Reference Stack Traces

Windows Vista™ x64 Complete Memory Dump

Dmitry Vostokov

1/29/2008

First Edition

Table of Contents

Version 4

Virtual Memory 5

Processes and Threads 7

System process 7

Smss process 49

Csrss process (session 0) 52

Csrss process (session 1) 59

Wininit process 65

Services process 68

Lsass process 74

Winlogon process 83

Lsm process 86

Svchost process (DcomLaunch) 92

Svchost process (rpcss) 99

Ati2evxx process (session 0) 105

Svchost process (LocalServiceNetworkRestricted) 112

Svchost process (LocalSystemNetworkRestricted) 125

Svchost process (netsvcs) 147

Audiodg process 177

SLsvc process 180

Svchost process (LocalService) 184

Svchost process (NetworkService) 199

Ati2evxx.exe process (session 0) 215

Spoolsv process 222

Svchost process (LocalServiceNoNetwork) 235

CcSvcHst process 252

DbgSvc process 266

DefWatch process 274

Svchost process (NetworkServiceNetworkRestricted) 279

Svchost process (WerSvcGroup) 284

SearchIndexer process 288

Rtvscan process 298

Taskeng process (session 0) 319

Taskeng process (session 1)....327
Dwm process....339
Explorer process....343
Sidebar process....363
Smax4pnp process....372
CcApp process....375
VPTray process....380
Issch process....387
CLI process....389
CLI process (second)....402
Dllhost process....412
Msdtc process....422
Ieuser process....431
Iexplore process....435
Notepad process....443
WmiPrvSE process....445
Stacks Summary....450
Executive Queues....456
Root Objects....463
Device Objects....464
Driver Objects....469
File System Objects....471
Base Named Objects....472
Kernel Objects....476
Loaded System Modules....477
IRP Distribution....500

Version

```
Windows Vista Kernel Version 6000 MP (2 procs) Free x64
Product: WinNt, suite: TerminalServer SingleUserTS
Built by: 6000.16575.amd64fre.vista_gdr.071009-1548
Kernel base = 0xfffff800`01c00000 PsLoadedModuleList = 0xfffff800`01d9af70
Debug session time: Tue Jan 29 11:03:52.572 2008 (GMT+0)
System Uptime: 0 days 0:12:06.648
64-bit Full kernel dump: C:\Windows\MEMORY.DMP
```

Virtual Memory

```
1: kd> !vm

*** Virtual Memory Usage ***
       Physical Memory:      523519 (   2094076 Kb)
       Page File: \??\C:\pagefile.sys
         Current:   2401276 Kb  Free Space:   2218208 Kb
         Minimum:   2401276 Kb  Maximum:      6282228 Kb
       Available Pages:      325512 (   1302048 Kb)
       ResAvail Pages:       465802 (   1863208 Kb)
       Locked IO Pages:           0 (         0 Kb)
       Free System PTEs:  268294650 (1073178600 Kb)
       Modified Pages:        15697 (     62788 Kb)
       Modified PF Pages:     15638 (     62552 Kb)
       NonPagedPool Usage:     9858 (     39432 Kb)
       NonPagedPool Max:     200192 (    800768 Kb)
       PagedPool 0 Usage:     16599 (     66396 Kb)
       PagedPool 1 Usage:     17117 (     68468 Kb)
       PagedPool 2 Usage:      1141 (      4564 Kb)
       PagedPool 3 Usage:      1110 (      4440 Kb)
       PagedPool 4 Usage:      1165 (      4660 Kb)
       PagedPool Usage:       37132 (    148528 Kb)
       PagedPool Maximum:  33554432 ( 134217728 Kb)
       Shared Commit:         16700 (     66800 Kb)
       Special Pool:              0 (         0 Kb)
       Shared Process:         6102 (     24408 Kb)
       PagedPool Commit:      37148 (    148592 Kb)
       Driver Commit:          7294 (     29176 Kb)
       Committed pages:      241777 (    967108 Kb)
       Commit limit:        1103187 (   4412748 Kb)

       Total Private:        151386 (    605544 Kb)
         018c svchost.exe      17591 (     70364 Kb)
         062c Rtvscan.exe      14306 (     57224 Kb)
         0b44 CLI.exe          13351 (     53404 Kb)
         0a34 CLI.exe          11487 (     45948 Kb)
         07c8 SearchIndexer.e  11253 (     45012 Kb)
         0a84 explorer.exe     10283 (     41132 Kb)
         0bac sidebar.exe       7012 (     28048 Kb)
         0d8c iexplore.exe      6230 (     24920 Kb)
         01a8 svchost.exe       5841 (     23364 Kb)
         022c csrss.exe         4358 (     17432 Kb)
         04cc svchost.exe       4046 (     16184 Kb)
         0114 svchost.exe       3738 (     14952 Kb)
         05f4 svchost.exe       3712 (     14848 Kb)
         032c audiodg.exe       2933 (     11732 Kb)
         0a14 taskeng.exe       2815 (     11260 Kb)
         0140 SLsvc.exe         2577 (     10308 Kb)
         05dc spoolsv.exe       2236 (      8944 Kb)
         0424 svchost.exe       2110 (      8440 Kb)
         0884 smax4pnp.exe      1991 (      7964 Kb)
         06fc DbgSvc.exe        1937 (      7748 Kb)
         041c dllhost.exe       1860 (      7440 Kb)
         06d4 ccSvcHst.exe      1668 (      6672 Kb)
         04e8 VPTray.exe        1456 (      5824 Kb)
         027c lsass.exe         1274 (      5096 Kb)
         0388 svchost.exe       1190 (      4760 Kb)
         03ec ccApp.exe         1175 (      4700 Kb)
         0958 ieuser.exe        1114 (      4456 Kb)
         0924 taskeng.exe       1056 (      4224 Kb)
         0004 System            1011 (      4044 Kb)
         03d8 WmiPrvSE.exe       904 (      3616 Kb)
         0ca4 msdtc.exe          882 (      3528 Kb)
         0338 svchost.exe        818 (      3272 Kb)
         025c services.exe       817 (      3268 Kb)
         0290 lsm.exe            739 (      2956 Kb)
```

```
0284 winlogon.exe       674 (      2696 Kb)
0760 svchost.exe        623 (      2492 Kb)
01f8 csrss.exe          603 (      2412 Kb)
0a44 dwm.exe            593 (      2372 Kb)
0528 Ati2evxx.exe       577 (      2308 Kb)
0720 DefWatch.exe       573 (      2292 Kb)
0ffc notepad.exe        473 (      1892 Kb)
0234 wininit.exe        433 (      1732 Kb)
0118 Ati2evxx.exe       427 (      1708 Kb)
07b4 svchost.exe        292 (      1168 Kb)
0868 issch.exe          230 (       920 Kb)
0184 smss.exe           117 (       468 Kb)
```

Processes and Threads

```
1: kd> !process 0 ff
```

System process

```
PROCESS fffffa8001860190
    SessionId: none  Cid: 0004    Peb: 00000000  ParentCid: 0000
    DirBase: 00124000  ObjectTable: fffff880000000e0  HandleCount: 589.
    Image: System
    VadRoot fffffa80038a1830 Vads 323 Clone 0 Private 987. Modified 27421. Locked 64.
    DeviceMap fffff88000007820
    Token                             fffff880000033b0
    ElapsedTime                       00:12:06.978
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.733
    QuotaPoolUsage[PagedPool]         0
    QuotaPoolUsage[NonPagedPool]      0
    Working Set Sizes (now,min,max)  (3590, 0, 0) (14360KB, 0KB, 0KB)
    PeakWorkingSetSize                5764
    VirtualSize                       23 Mb
    PeakVirtualSize                   29 Mb
    PageFaultCount                    36446
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      1011

    Setting context for this process...
.process /p /r fffffa8001860190

    !peb
        THREAD fffffa8001884060  Cid 0004.0008  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrFreePage) KernelMode Non-Alertable
            fffff80001d9bde0  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      46531          Ticks: 48 (0:00:00:00.748)
        Context Switch Count      5892
        UserTime                  00:00:00.000
        KernelTime                00:00:02.308
        Win32 Start Address nt!Phase1Initialization (0xfffff80001fff520)
        Stack Init fffff98000a36db0 Current fffff98000a36a30
        Base fffff98000a37000 Limit fffff98000a31000 Call 0
        Priority 0 BasePriority 0 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`00a36a70 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`00a36bb0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`00a36c10 fffff800`01c87ebd nt!KeWaitForSingleObject+0x5f5
        fffff980`00a36c90 fffff800`01fff52e nt!MmZeroPageThread+0x180
        fffff980`00a36d20 fffff800`01ee196b nt!Phase1Initialization+0xe
        fffff980`00a36d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`00a36d80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa8001885bb0  Cid 0004.0010  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffff80001d7b0a0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      17             Ticks: 46562 (0:00:12:06.371)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!PopIrpWorkerControl (0xfffff80001d00290)
        Stack Init fffff98000a08db0 Current fffff98000a08ab0
        Base fffff98000a09000 Limit fffff98000a03000 Call 0
        Priority 15 BasePriority 13 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`00a08af0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`00a08c30 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`00a08c90 fffff800`01d002b2 nt!KeWaitForSingleObject+0x5f5
        fffff980`00a08d10 fffff800`01ee196b nt!PopIrpWorkerControl+0x22
        fffff980`00a08d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`00a08d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa8001885720  Cid 0004.0014  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffff80001d7b740  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      568            Ticks: 46011 (0:00:11:57.776)
        Context Switch Count      6
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!PopIrpWorker (0xfffff80001c0d910)
        Stack Init fffff98000a56db0 Current fffff98000a56a40
        Base fffff98000a57000 Limit fffff98000a51000 Call 0
        Priority 15 BasePriority 13 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`00a56a80 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`00a56bc0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`00a56c20 fffff800`01c0da74 nt!KeWaitForSingleObject+0x5f5
        fffff980`00a56ca0 fffff800`01ee196b nt!PopIrpWorker+0x164
        fffff980`00a56d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`00a56d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa8001886040  Cid 0004.0018  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffff80001d7b740  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      825            Ticks: 45754 (0:00:11:53.766)
        Context Switch Count      7
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!PopIrpWorker (0xfffff80001c0d910)
        Stack Init fffff98000a4fdb0 Current fffff98000a4fa40
        Base fffff98000a50000 Limit fffff98000a4a000 Call 0
        Priority 15 BasePriority 13 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`00a4fa80 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`00a4fbc0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`00a4fc20 fffff800`01c0da74 nt!KeWaitForSingleObject+0x5f5
        fffff980`00a4fca0 fffff800`01ee196b nt!PopIrpWorker+0x164
        fffff980`00a4fd50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`00a4fd80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa8001897bb0  Cid 0004.001c  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffff80001d68980  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      17             Ticks: 46562 (0:00:12:06.371)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!ExpWorkerThread (0xfffff80001c59c80)
        Stack Init fffff98000c7adb0 Current fffff98000c7aa70
        Base fffff98000c7b000 Limit fffff98000c75000 Call 0
        Priority 13 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`00c7aab0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`00c7abf0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`00c7ac50 fffff800`01c59d7d nt!KeRemoveQueueEx+0x848
        fffff980`00c7ace0 fffff800`01ee196b nt!ExpWorkerThread+0x104
        fffff980`00c7ad50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`00c7ad80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa8001897720  Cid 0004.0020  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffff80001d68980  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      1071           Ticks: 45508 (0:00:11:49.929)
        Context Switch Count      250
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address nt!ExpWorkerThread (0xfffff80001c59c80)
        Stack Init fffff98000c73db0 Current fffff98000c73a70
        Base fffff98000c74000 Limit fffff98000c6e000 Call 0
        Priority 13 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`00c73ab0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`00c73bf0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`00c73c50 fffff800`01c59d7d nt!KeRemoveQueueEx+0x848
        fffff980`00c73ce0 fffff800`01ee196b nt!ExpWorkerThread+0x104
        fffff980`00c73d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`00c73d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa8001897290  Cid 0004.0024  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffff80001d68980  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      835            Ticks: 45744 (0:00:11:53.610)
        Context Switch Count      3586
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address nt!ExpWorkerThread (0xfffff80001c59c80)
        Stack Init fffff98000c6cdb0 Current fffff98000c6ca70
        Base fffff98000c6d000 Limit fffff98000c67000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`00c6cab0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`00c6cbf0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`00c6cc50 fffff800`01c59d7d nt!KeRemoveQueueEx+0x848
        fffff980`00c6cce0 fffff800`01ee196b nt!ExpWorkerThread+0x104
        fffff980`00c6cd50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`00c6cd80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa800188d040  Cid 0004.0028  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffff80001d68980  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      835            Ticks: 45744 (0:00:11:53.610)
        Context Switch Count      2860
        UserTime                  00:00:00.000
        KernelTime                00:00:01.123
        Win32 Start Address nt!ExpWorkerThread (0xfffff80001c59c80)
        Stack Init fffff98000c65db0 Current fffff98000c65a70
        Base fffff98000c66000 Limit fffff98000c60000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`00c65ab0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`00c65bf0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`00c65c50 fffff800`01c59d7d nt!KeRemoveQueueEx+0x848
        fffff980`00c65ce0 fffff800`01ee196b nt!ExpWorkerThread+0x104
        fffff980`00c65d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`00c65d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa800188dbb0  Cid 0004.002c  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffff80001d68980  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      1071           Ticks: 45508 (0:00:11:49.929)
        Context Switch Count      2699
        UserTime                  00:00:00.000
        KernelTime                00:00:00.577
        Win32 Start Address nt!ExpWorkerThread (0xfffff80001c59c80)
        Stack Init fffff98000c5edb0 Current fffff98000c5ea70
        Base fffff98000c5f000 Limit fffff98000c59000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`00c5eab0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`00c5ebf0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`00c5ec50 fffff800`01c59d7d nt!KeRemoveQueueEx+0x848
        fffff980`00c5ece0 fffff800`01ee196b nt!ExpWorkerThread+0x104
        fffff980`00c5ed50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`00c5ed80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa800188d720  Cid 0004.0030  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffff80001d689d8  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      46545          Ticks: 34 (0:00:00:00.530)
        Context Switch Count      34058
        UserTime                  00:00:00.000
        KernelTime                00:00:02.745
        Win32 Start Address nt!ExpWorkerThread (0xfffff80001c59c80)
        Stack Init fffff98000c57db0 Current fffff98000c57a70
        Base fffff98000c58000 Limit fffff98000c52000 Call 0
        Priority 13 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`00c57ab0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`00c57bf0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`00c57c50 fffff800`01c59d7d nt!KeRemoveQueueEx+0x848
        fffff980`00c57ce0 fffff800`01ee196b nt!ExpWorkerThread+0x104
        fffff980`00c57d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`00c57d80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa800188c040  Cid 0004.0034  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffff80001d689d8  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      1304           Ticks: 45275 (0:00:11:46.294)
        Context Switch Count      1277
        UserTime                  00:00:00.000
        KernelTime                00:00:00.639
        Win32 Start Address nt!ExpWorkerThread (0xfffff80001c59c80)
        Stack Init fffff98000c50db0 Current fffff98000c50a70
        Base fffff98000c51000 Limit fffff98000c4b000 Call 0
        Priority 15 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`00c50ab0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`00c50bf0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`00c50c50 fffff800`01c59d7d nt!KeRemoveQueueEx+0x848
        fffff980`00c50ce0 fffff800`01ee196b nt!ExpWorkerThread+0x104
        fffff980`00c50d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`00c50d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa800188cbb0  Cid 0004.0038  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffff80001d689d8  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      791            Ticks: 45788 (0:00:11:54.297)
        Context Switch Count      163
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!ExpWorkerThread (0xfffff80001c59c80)
        Stack Init fffff98000c49db0 Current fffff98000c49a70
        Base fffff98000c4a000 Limit fffff98000c44000 Call 0
        Priority 13 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`00c49ab0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`00c49bf0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`00c49c50 fffff800`01c59d7d nt!KeRemoveQueueEx+0x848
        fffff980`00c49ce0 fffff800`01ee196b nt!ExpWorkerThread+0x104
        fffff980`00c49d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`00c49d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa800188c720  Cid 0004.003c  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffff80001d689d8  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      46556          Ticks: 23 (0:00:00:00.358)
        Context Switch Count      8153
        UserTime                  00:00:00.000
        KernelTime                00:00:00.202
        Win32 Start Address nt!ExpWorkerThread (0xfffff80001c59c80)
        Stack Init fffff98000c42db0 Current fffff98000c42a70
        Base fffff98000c43000 Limit fffff98000c3d000 Call 0
        Priority 13 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`00c42ab0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`00c42bf0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`00c42c50 fffff800`01c59d7d nt!KeRemoveQueueEx+0x848
        fffff980`00c42ce0 fffff800`01ee196b nt!ExpWorkerThread+0x104
        fffff980`00c42d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`00c42d80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa800188b040  Cid 0004.0040  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffff80001d689d8  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      798            Ticks: 45781 (0:00:11:54.188)
        Context Switch Count      218
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address nt!ExpWorkerThread (0xfffff80001c59c80)
        Stack Init fffff98000c3bdb0 Current fffff98000c3ba70
        Base fffff98000c3c000 Limit fffff98000c36000 Call 0
        Priority 13 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`00c3bab0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`00c3bbf0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`00c3bc50 fffff800`01c59d7d nt!KeRemoveQueueEx+0x848
        fffff980`00c3bce0 fffff800`01ee196b nt!ExpWorkerThread+0x104
        fffff980`00c3bd50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`00c3bd80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa800188bbb0  Cid 0004.0044  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffff80001d689d8  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      29543          Ticks: 17036 (0:00:04:25.763)
        Context Switch Count      14311
        UserTime                  00:00:00.000
        KernelTime                00:00:00.951
        Win32 Start Address nt!ExpWorkerThread (0xfffff80001c59c80)
        Stack Init fffff98000c34db0 Current fffff98000c34a70
        Base fffff98000c35000 Limit fffff98000c2f000 Call 0
        Priority 13 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`00c34ab0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`00c34bf0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`00c34c50 fffff800`01c59d7d nt!KeRemoveQueueEx+0x848
        fffff980`00c34ce0 fffff800`01ee196b nt!ExpWorkerThread+0x104
        fffff980`00c34d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`00c34d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa800188b720  Cid 0004.0048  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffff80001d689d8  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      29543          Ticks: 17036 (0:00:04:25.763)
        Context Switch Count      1365
        UserTime                  00:00:00.000
        KernelTime                00:00:00.062
        Win32 Start Address nt!ExpWorkerThread (0xfffff80001c59c80)
        Stack Init fffff98000c2ddb0 Current fffff98000c2da70
        Base fffff98000c2e000 Limit fffff98000c28000 Call 0
        Priority 13 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`00c2dab0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`00c2dbf0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`00c2dc50 fffff800`01c59d7d nt!KeRemoveQueueEx+0x848
        fffff980`00c2dce0 fffff800`01ee196b nt!ExpWorkerThread+0x104
        fffff980`00c2dd50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`00c2dd80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa800188a040  Cid 0004.004c  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) KernelMode Non-Alertable
            fffff80001d68a30  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      46371          Ticks: 208 (0:00:00:03.244)
        Context Switch Count      1459
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!ExpWorkerThread (0xfffff80001c59c80)
        Stack Init fffff98000c26db0 Current fffff98000c26a70
        Base fffff98000c27000 Limit fffff98000c21000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`00c26ab0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`00c26bf0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`00c26c50 fffff800`01c59d7d nt!KeRemoveQueueEx+0x848
        fffff980`00c26ce0 fffff800`01ee196b nt!ExpWorkerThread+0x104
        fffff980`00c26d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`00c26d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa800188abb0  Cid 0004.0050  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffff98000c1fd00  NotificationTimer
            fffff80001d68940  SynchronizationEvent
            fffff80001d68920  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      46545          Ticks: 34 (0:00:00:00.530)
        Context Switch Count      730
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!ExpWorkerThreadBalanceManager (0xfffff80001e941a0)
        Stack Init fffff98000c1fdb0 Current fffff98000c1fa50
        Base fffff98000c20000 Limit fffff98000c1a000 Call 0
        Priority 15 BasePriority 14 PriorityDecrement 1 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`00c1fa90 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`00c1fbd0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`00c1fc30 fffff800`01e94228 nt!KeWaitForMultipleObjects+0x703
        fffff980`00c1fca0 fffff800`01ee196b nt!ExpWorkerThreadBalanceManager+0x85
        fffff980`00c1fd50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`00c1fd80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa80018983d0  Cid 0004.0054  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Suspended) KernelMode Non-Alertable
            fffff80001d4dd00  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      46203          Ticks: 376 (0:00:00:05.865)
        Context Switch Count      51
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!KiExecuteDpc (0xfffff80001c2d3e0)
        Stack Init fffff98000c18db0 Current fffff98000c18a80
        Base fffff98000c19000 Limit fffff98000c13000 Call 0
        Priority 31 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`00c18ac0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`00c18c00 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`00c18c60 fffff800`01c2d578 nt!KeWaitForSingleObject+0x5f5
        fffff980`00c18ce0 fffff800`01ee196b nt!KiExecuteDpc+0x198
        fffff980`00c18d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`00c18d80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa8001899040  Cid 0004.0058  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Suspended) KernelMode Non-Alertable
            fffff98000a40500  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      46213          Ticks: 366 (0:00:00:05.709)
        Context Switch Count      50
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!KiExecuteDpc (0xfffff80001c2d3e0)
        Stack Init fffff98000c11db0 Current fffff98000c11a80
        Base fffff98000c12000 Limit fffff98000c0c000 Call 0
        Priority 31 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`00c11ac0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`00c11c00 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`00c11c60 fffff800`01c2d578 nt!KeWaitForSingleObject+0x5f5
        fffff980`00c11ce0 fffff800`01ee196b nt!KiExecuteDpc+0x198
        fffff980`00c11d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`00c11d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa800189a910  Cid 0004.005c  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrVirtualMemory) UserMode Non-Alertable
            fffff80001d9b920  Semaphore Limit 0x7fffffff
            fffff80001d9b9e0  NotificationEvent
            fffff80001d9bb00  NotificationEvent
            fffff80001d889a0  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      43279          Ticks: 3300 (0:00:00:51.480)
        Context Switch Count      19
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!MiDereferenceSegmentThread (0xfffff80001c274f0)
        Stack Init fffff98000c0adb0 Current fffff98000c0aa90
        Base fffff98000c0b000 Limit fffff98000c05000 Call 0
        Priority 18 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`00c0aad0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`00c0ac10 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`00c0ac70 fffff800`01c27577 nt!KeWaitForMultipleObjects+0x703
        fffff980`00c0ace0 fffff800`01ee196b nt!MiDereferenceSegmentThread+0x87
        fffff980`00c0ad50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`00c0ad80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa800189b040  Cid 0004.0060  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrFreePage) KernelMode Non-Alertable
            fffff80001d865a0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      26712          Ticks: 19867 (0:00:05:09.927)
        Context Switch Count      468
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!MiModifiedPageWriter (0xfffff80001d11860)
        Stack Init fffff980012fddb0 Current fffff980012fda90
        Base fffff980012fe000 Limit fffff980012f8000 Call 0
        Priority 17 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`012fdad0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`012fdc10 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`012fdc70 fffff800`01d118b9 nt!KeWaitForSingleObject+0x5f5
        fffff980`012fdcf0 fffff800`01ee196b nt!MiModifiedPageWriter+0x59
        fffff980`012fdd50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`012fdd80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa800189b8d0  Cid 0004.0064  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrFreePage) KernelMode Non-Alertable
            fffff80001d9b0c0  SynchronizationEvent
            fffff80001d9b0d8  SynchronizationEvent
            fffff80001d9b0f0  SynchronizationEvent
            fffff80001d9b108  SynchronizationEvent
            fffff80001d9b120  SynchronizationEvent
            fffff80001d9b138  SynchronizationEvent
            fffff80001d9b150  SynchronizationEvent
            fffff80001d9b168  SynchronizationEvent
            fffff80001d9b180  SynchronizationEvent
            fffff80001d9b198  SynchronizationEvent
            fffff80001d9b1b0  SynchronizationEvent
            fffff80001d9b1c8  SynchronizationEvent
            fffff80001d9b1e0  SynchronizationEvent
            fffff80001d9b1f8  SynchronizationEvent
            fffff80001d9b210  SynchronizationEvent
            fffff80001d9b228  SynchronizationEvent
            fffff80001d9b240  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      6075           Ticks: 40504 (0:00:10:31.866)
        Context Switch Count      82
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!MiMappedPageWriter (0xfffff80001c1f280)
        Stack Init fffff980012f6db0 Current fffff980012f6a20
        Base fffff980012f7000 Limit fffff980012f1000 Call 0
        Priority 17 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`012f6a60 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`012f6ba0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`012f6c00 fffff800`01c1f32d nt!KeWaitForMultipleObjects+0x703
        fffff980`012f6c70 fffff800`01ee196b nt!MiMappedPageWriter+0xad
        fffff980`012f6d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`012f6d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa800189cbb0  Cid 0004.0068  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffff980012efca0  SynchronizationTimer
            fffff80001d9ae20  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      46531          Ticks: 48 (0:00:00:00.748)
        Context Switch Count      1476
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address nt!KeBalanceSetManager (0xfffff80001c67660)
        Stack Init fffff980012efdb0 Current fffff980012ef9c0
        Base fffff980012f0000 Limit fffff980012ea000 Call 0
        Priority 16 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`012efa00 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`012efb40 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`012efba0 fffff800`01c67764 nt!KeWaitForMultipleObjects+0x703
        fffff980`012efc10 fffff800`01ee196b nt!KeBalanceSetManager+0x101
        fffff980`012efd50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`012efd80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa800189c720  Cid 0004.006c  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffff80001dc81c0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      46531          Ticks: 48 (0:00:00:00.748)
        Context Switch Count      3036
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!KeSwapProcessOrStack (0xfffff80001c722b0)
        Stack Init fffff980012e8db0 Current fffff980012e8ab0
        Base fffff980012e9000 Limit fffff980012e3000 Call 0
        Priority 23 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`012e8af0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`012e8c30 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`012e8c90 fffff800`01c722f4 nt!KeWaitForSingleObject+0x5f5
        fffff980`012e8d10 fffff800`01ee196b nt!KeSwapProcessOrStack+0x44
        fffff980`012e8d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`012e8d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa8001881040  Cid 0004.0070  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrFreePage) KernelMode Non-Alertable
            fffff80001dd37e0  SynchronizationEvent
            fffff80001dd37c0  SynchronizationEvent
            fffff80001dd37a0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      46538          Ticks: 41 (0:00:00:00.639)
        Context Switch Count      708
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!CcQueueLazyWriteScanThread (0xfffff80001ca32c0)
        Stack Init fffff980012c1db0 Current fffff980012c1a90
        Base fffff980012c2000 Limit fffff980012bc000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`012c1ad0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`012c1c10 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`012c1c70 fffff800`01ca3333 nt!KeWaitForMultipleObjects+0x703
        fffff980`012c1ce0 fffff800`01ee196b nt!CcQueueLazyWriteScanThread+0x73
        fffff980`012c1d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`012c1d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa8001883320  Cid 0004.0074  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) KernelMode Non-Alertable
            fffff80001dd1c40  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      27             Ticks: 46552 (0:00:12:06.215)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!FsRtlWorkerThread (0xfffff80001ce1f30)
        Stack Init fffff980012badb0 Current fffff980012baaa0
        Base fffff980012bb000 Limit fffff980012b5000 Call 0
        Priority 16 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`012baae0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`012bac20 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`012bac80 fffff800`01ce1f7d nt!KeRemoveQueueEx+0x848
        fffff980`012bad10 fffff800`01ee196b nt!FsRtlWorkerThread+0x4d
        fffff980`012bad50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`012bad80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa800189d040  Cid 0004.0078  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) KernelMode Non-Alertable
            fffff80001dd1c80  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      23             Ticks: 46556 (0:00:12:06.278)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!FsRtlWorkerThread (0xfffff80001ce1f30)
        Stack Init fffff980012b3db0 Current fffff980012b3aa0
        Base fffff980012b4000 Limit fffff980012ae000 Call 0
        Priority 17 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`012b3ae0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`012b3c20 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`012b3c80 fffff800`01ce1f7d nt!KeRemoveQueueEx+0x848
        fffff980`012b3d10 fffff800`01ee196b nt!FsRtlWorkerThread+0x4d
        fffff980`012b3d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`012b3d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa8001cdc040  Cid 0004.0080  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffffa8001858a78  SynchronizationEvent
            fffffa8001cdc0f8  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      46561          Ticks: 18 (0:00:00:00.280)
        Context Switch Count      728
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!EtwpLogger (0xfffff80001e90370)
        Stack Init fffff980012a5db0 Current fffff980012a5a90
        Base fffff980012a6000 Limit fffff980012a0000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`012a5ad0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`012a5c10 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`012a5c70 fffff800`01e9044d nt!KeWaitForSingleObject+0x5f5
        fffff980`012a5cf0 fffff800`01ee196b nt!EtwpLogger+0xdd
        fffff980`012a5d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`012a5d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa8001cdc7b0  Cid 0004.0084  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffffa8001cdcdf8  SynchronizationEvent
            fffffa8001cdc868  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      46541          Ticks: 38 (0:00:00:00.592)
        Context Switch Count      747
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!EtwpLogger (0xfffff80001e90370)
        Stack Init fffff9800129edb0 Current fffff9800129ea90
        Base fffff9800129f000 Limit fffff98001299000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0129ead0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0129ec10 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0129ec70 fffff800`01e9044d nt!KeWaitForSingleObject+0x5f5
        fffff980`0129ecf0 fffff800`01ee196b nt!EtwpLogger+0xdd
        fffff980`0129ed50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0129ed80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa8001d22040  Cid 0004.0088  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffffa8001ce1678  SynchronizationEvent
            fffffa8001d220f8  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      46545          Ticks: 34 (0:00:00:00.530)
        Context Switch Count      742
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!EtwpLogger (0xfffff80001e90370)
        Stack Init fffff98001297db0 Current fffff98001297a90
        Base fffff98001298000 Limit fffff98001292000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`01297ad0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`01297c10 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`01297c70 fffff800`01e9044d nt!KeWaitForSingleObject+0x5f5
        fffff980`01297cf0 fffff800`01ee196b nt!EtwpLogger+0xdd
        fffff980`01297d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`01297d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa8001d227f0  Cid 0004.008c  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffffa8001d22e38  SynchronizationEvent
            fffffa8001d228a8  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      46545          Ticks: 34 (0:00:00:00.530)
        Context Switch Count      739
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!EtwpLogger (0xfffff80001e90370)
        Stack Init fffff98001290db0 Current fffff98001290a90
        Base fffff98001291000 Limit fffff9800128b000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`01290ad0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`01290c10 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`01290c70 fffff800`01e9044d nt!KeWaitForSingleObject+0x5f5
        fffff980`01290cf0 fffff800`01ee196b nt!EtwpLogger+0xdd
        fffff980`01290d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`01290d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa8001d6b040  Cid 0004.0090  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffffa8001d663b8  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      33             Ticks: 46546 (0:00:12:06.122)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!EtwpLogger (0xfffff80001e90370)
        Stack Init fffff98001289db0 Current fffff98001289a90
        Base fffff9800128a000 Limit fffff98001284000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`01289ad0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`01289c10 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`01289c70 fffff800`01e903f4 nt!KeWaitForSingleObject+0x5f5
        fffff980`01289cf0 fffff800`01ee196b nt!EtwpLogger+0x84
        fffff980`01289d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`01289d80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa8001d6b670  Cid 0004.0094  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffffa8001d6bcb8  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      33             Ticks: 46546 (0:00:12:06.122)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!EtwpLogger (0xfffff80001e90370)
        Stack Init fffff98001282db0 Current fffff98001282a90
        Base fffff98001283000 Limit fffff9800127d000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`01282ad0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`01282c10 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`01282c70 fffff800`01e903f4 nt!KeWaitForSingleObject+0x5f5
        fffff980`01282cf0 fffff800`01ee196b nt!EtwpLogger+0x84
        fffff980`01282d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`01282d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa8001dac8b0  Cid 0004.0098  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffffa8001dac1f8  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      33             Ticks: 46546 (0:00:12:06.122)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!EtwpLogger (0xfffff80001e90370)
        Stack Init fffff9800127bdb0 Current fffff9800127ba90
        Base fffff9800127c000 Limit fffff98001276000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0127bad0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0127bc10 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0127bc70 fffff800`01e903f4 nt!KeWaitForSingleObject+0x5f5
        fffff980`0127bcf0 fffff800`01ee196b nt!EtwpLogger+0x84
        fffff980`0127bd50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0127bd80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa8001dcdbb0  Cid 0004.009c  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffffa8001dcd1f8  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      33             Ticks: 46546 (0:00:12:06.122)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!EtwpLogger (0xfffff80001e90370)
        Stack Init fffff98001274db0 Current fffff98001274a90
        Base fffff98001275000 Limit fffff9800126f000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`01274ad0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`01274c10 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`01274c70 fffff800`01e903f4 nt!KeWaitForSingleObject+0x5f5
        fffff980`01274cf0 fffff800`01ee196b nt!EtwpLogger+0x84
        fffff980`01274d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`01274d80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa800185d040  Cid 0004.00a4  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffffa800230e4b8  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      13293          Ticks: 33286 (0:00:08:39.264)
        Context Switch Count      33
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address nt!EtwpLogger (0xfffff80001e90370)
        Stack Init fffff98001266db0 Current fffff98001266a90
        Base fffff98001267000 Limit fffff98001261000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`01266ad0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`01266c10 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`01266c70 fffff800`01e9044d nt!KeWaitForSingleObject+0x5f5
        fffff980`01266cf0 fffff800`01ee196b nt!EtwpLogger+0xdd
        fffff980`01266d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`01266d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa800185e8b0  Cid 0004.00a8  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (DelayExecution) KernelMode Non-Alertable
            fffffa800185e968  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      46197          Ticks: 382 (0:00:00:05.959)
        Context Switch Count      13
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!WdipSemCheckTimeout (0xfffff80001ea56c0)
        Stack Init fffff9800125fdb0 Current fffff9800125fac0
        Base fffff98001260000 Limit fffff9800125a000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0125fb00 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0125fc40 fffff800`01c5b5a9 nt!KiSwapThread+0x125
        fffff980`0125fca0 fffff800`01ea57e8 nt!KeDelayExecutionThread+0x339
        fffff980`0125fd20 fffff800`01ee196b nt!WdipSemCheckTimeout+0x128
        fffff980`0125fd50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0125fd80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa8002657040  Cid 0004.00ac  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffff9800024bb00  NotificationEvent
            fffff9800024bae0  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      825            Ticks: 45754 (0:00:11:53.766)
        Context Switch Count      75
        UserTime                  00:00:00.000
        KernelTime                00:00:00.093
        Win32 Start Address acpi!ACPIWorkerThread (0xfffff98000231964)
        Stack Init fffff98001258db0 Current fffff98001258aa0
        Base fffff98001259000 Limit fffff98001253000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`01258ae0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`01258c20 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`01258c80 fffff980`002319d8 nt!KeWaitForMultipleObjects+0x703
        fffff980`01258cf0 fffff800`01ee196b acpi!ACPIWorkerThread+0x74
        fffff980`01258d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`01258d80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa8001c92490  Cid 0004.00b4  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffffa8001c9f618  SynchronizationEvent
            fffffa8001c9f600  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      51             Ticks: 46528 (0:00:12:05.841)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address acpi!PciRootBusBiosMethodDispatcherOnResume (0xfffff9800022a990)
        Stack Init fffff98001231db0 Current fffff98001231aa0
        Base fffff98001232000 Limit fffff9800122c000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`01231ae0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`01231c20 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`01231c80 fffff980`0022a9e1 nt!KeWaitForMultipleObjects+0x703
        fffff980`01231cf0 fffff800`01ee196b acpi!PciRootBusBiosMethodDispatcherOnResume+0x51
        fffff980`01231d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`01231d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa8002777330  Cid 0004.00b8  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) KernelMode Non-Alertable
            fffff980006a3f00  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      1618           Ticks: 44961 (0:00:11:41.396)
        Context Switch Count      16
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ndis!ndisWorkerThread (0xfffff980007c8eb0)
        Stack Init fffff980014ffdb0 Current fffff980014ffa50
        Base fffff98001500000 Limit fffff980014fa000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`014ffa90 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`014ffbd0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`014ffc30 fffff800`01c34eb1 nt!KeRemoveQueueEx+0x848
        fffff980`014ffcc0 fffff980`007c8ef5 nt!KeRemoveQueue+0x21
        fffff980`014ffd00 fffff800`01ee196b ndis!ndisWorkerThread+0x45
        fffff980`014ffd50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`014ffd80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa800277a6a0  Cid 0004.00bc  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffff980006a4920  NotificationEvent
            fffffa800277a758  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      46271          Ticks: 308 (0:00:00:04.804)
        Context Switch Count      25
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ndis!ndisCmWaitThread (0xfffff9800065b590)
        Stack Init fffff9800148fdb0 Current fffff9800148fab0
        Base fffff98001490000 Limit fffff9800148a000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0148faf0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0148fc30 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0148fc90 fffff980`0065b5fe nt!KeWaitForSingleObject+0x5f5
        fffff980`0148fd10 fffff800`01ee196b ndis!ndisCmWaitThread+0x6e
        fffff980`0148fd50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0148fd80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa800277a210  Cid 0004.00c0  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffff98000bc6e08  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      5191           Ticks: 41388 (0:00:10:45.656)
        Context Switch Count      65447
        UserTime                  00:00:00.000
        KernelTime                00:00:07.191
        Win32 Start Address ecache!EcCacheIoWorker (0xfffff98000bbd328)
        Stack Init fffff98001496db0 Current fffff98001496a00
        Base fffff98001497000 Limit fffff98001491000 Call 0
        Priority 13 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`01496a40 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`01496b80 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`01496be0 fffff980`00bbd38b nt!KeWaitForSingleObject+0x5f5
        fffff980`01496c60 fffff800`01ee196b ecache!EcCacheIoWorker+0x63
        fffff980`01496d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`01496d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa8002791bb0  Cid 0004.00c4  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffff98000bc6eb8  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      5191           Ticks: 41388 (0:00:10:45.656)
        Context Switch Count      84971
        UserTime                  00:00:00.000
        KernelTime                00:00:00.202
        Win32 Start Address ecache!EcCacheIoWatchdog (0xfffff98000bbcb20)
        Stack Init fffff9800149ddb0 Current fffff9800149da50
        Base fffff9800149e000 Limit fffff98001498000 Call 0
        Priority 13 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0149da90 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0149dbd0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0149dc30 fffff980`00bbce8d nt!KeWaitForSingleObject+0x5f5
        fffff980`0149dcb0 fffff800`01ee196b ecache!EcCacheIoWatchdog+0x36d
        fffff980`0149dd50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0149dd80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa8002978b10  Cid 0004.00cc  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffffa80027f4220  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      1026           Ticks: 45553 (0:00:11:50.631)
        Context Switch Count      27
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address volsnap!VspWorkerThread (0xfffff9800043cf80)
        Stack Init fffff980014c0db0 Current fffff980014c0ab0
        Base fffff980014c1000 Limit fffff980014bb000 Call 0
        Priority 20 BasePriority 8 PriorityDecrement 0 IoPriority 3 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`014c0af0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`014c0c30 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`014c0c90 fffff980`0043d058 nt!KeWaitForSingleObject+0x5f5
        fffff980`014c0d10 fffff800`01ee196b volsnap!VspWorkerThread+0xd8
        fffff980`014c0d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`014c0d80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa80029785e0  Cid 0004.00d0  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffffa80027f4240  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      43361          Ticks: 3218 (0:00:00:50.201)
        Context Switch Count      360
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address volsnap!VspWorkerThread (0xfffff9800043cf80)
        Stack Init fffff980014c7db0 Current fffff980014c7ab0
        Base fffff980014c8000 Limit fffff980014c2000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`014c7af0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`014c7c30 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`014c7c90 fffff980`0043d058 nt!KeWaitForSingleObject+0x5f5
        fffff980`014c7d10 fffff800`01ee196b volsnap!VspWorkerThread+0xd8
        fffff980`014c7d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`014c7d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa800297d040  Cid 0004.00d4  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffffa80027f4260  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      46209          Ticks: 370 (0:00:00:05.772)
        Context Switch Count      1864
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address volsnap!VspWorkerThread (0xfffff9800043cf80)
        Stack Init fffff980014cedb0 Current fffff980014ceab0
        Base fffff980014cf000 Limit fffff980014c9000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`014ceaf0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`014cec30 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`014cec90 fffff980`0043d058 nt!KeWaitForSingleObject+0x5f5
        fffff980`014ced10 fffff800`01ee196b volsnap!VspWorkerThread+0xd8
        fffff980`014ced50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`014ced80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa800297dbb0  Cid 0004.00d8  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffffa80027f4280  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      373            Ticks: 46206 (0:00:12:00.818)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address volsnap!VspWorkerThread (0xfffff9800043cf80)
        Stack Init fffff980014d5db0 Current fffff980014d5ab0
        Base fffff980014d6000 Limit fffff980014d0000 Call 0
        Priority 20 BasePriority 8 PriorityDecrement 0 IoPriority 3 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`014d5af0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`014d5c30 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`014d5c90 fffff980`0043d058 nt!KeWaitForSingleObject+0x5f5
        fffff980`014d5d10 fffff800`01ee196b volsnap!VspWorkerThread+0xd8
        fffff980`014d5d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`014d5d80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa800297d720  Cid 0004.00dc  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffffa80027f42a0  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      113            Ticks: 46466 (0:00:12:04.874)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address volsnap!VspWorkerThread (0xfffff9800043cf80)
        Stack Init fffff980014dcdb0 Current fffff980014dcab0
        Base fffff980014dd000 Limit fffff980014d7000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`014dcaf0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`014dcc30 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`014dcc90 fffff980`0043cff6 nt!KeWaitForSingleObject+0x5f5
        fffff980`014dcd10 fffff800`01ee196b volsnap!VspWorkerThread+0x76
        fffff980`014dcd50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`014dcd80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa80038a6bb0  Cid 0004.00e0  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffff980008e5790  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      46469          Ticks: 110 (0:00:00:01.716)
        Context Switch Count      1534
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address Ntfs!TxfPrivateThreadWorkerRoutine (0xfffff9800089e040)
        Stack Init fffff980014eadb0 Current fffff980014eaab0
        Base fffff980014eb000 Limit fffff980014e5000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`014eaaf0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`014eac30 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`014eac90 fffff980`0089e07f nt!KeWaitForSingleObject+0x5f5
        fffff980`014ead10 fffff800`01ee196b Ntfs!TxfPrivateThreadWorkerRoutine+0x3f
        fffff980`014ead50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`014ead80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa800397dbb0  Cid 0004.00e8  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffff980038e9c28  SynchronizationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      489            Ticks: 46090 (0:00:11:59.008)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address dxgkrnl!DpiPdoPollingThread (0xfffff9800393c2a4)
        Stack Init fffff9800141fdb0 Current fffff9800141fa80
        Base fffff98001420000 Limit fffff9800141a000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0141fac0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0141fc00 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0141fc60 fffff980`0393c2f5 nt!KeWaitForSingleObject+0x5f5
        fffff980`0141fce0 fffff800`01ee196b dxgkrnl!DpiPdoPollingThread+0x51
        fffff980`0141fd50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0141fd80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa800397d720  Cid 0004.00ec  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffff98001215420  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      489            Ticks: 46090 (0:00:11:59.008)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address watchdog!SMgrGdiCalloutThread (0xfffff98001211588)
        Stack Init fffff980014f8db0 Current fffff980014f8a70
        Base fffff980014f9000 Limit fffff980014f3000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`014f8ab0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`014f8bf0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`014f8c50 fffff980`012115e5 nt!KeWaitForSingleObject+0x5f5
        fffff980`014f8cd0 fffff800`01ee196b watchdog!SMgrGdiCalloutThread+0x5d
        fffff980`014f8d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`014f8d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa80038f4bb0  Cid 0004.00f0  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffffa80038f4a48  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      489            Ticks: 46090 (0:00:11:59.008)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address dxgkrnl!DpiPowerArbiterThread (0xfffff9800393ccf8)
        Stack Init fffff98001426db0 Current fffff98001426a90
        Base fffff98001427000 Limit fffff98001421000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`01426ad0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`01426c10 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`01426c70 fffff980`0393cd43 nt!KeWaitForSingleObject+0x5f5
        fffff980`01426cf0 fffff800`01ee196b dxgkrnl!DpiPowerArbiterThread+0x4b
        fffff980`01426d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`01426d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa80039d7870  Cid 0004.00fc  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) KernelMode Non-Alertable
            fffff98004338a38  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      501            Ticks: 46078 (0:00:11:58.821)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address rdpdr!RxBootstrapWorkerThreadDispatcher (0xfffff98004352040)
        Stack Init fffff980014e3db0 Current fffff980014e3a40
        Base fffff980014e4000 Limit fffff980014de000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`014e3a80 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`014e3bc0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`014e3c20 fffff800`01c34eb1 nt!KeRemoveQueueEx+0x848
        fffff980`014e3cb0 fffff980`042e221f nt!KeRemoveQueue+0x21
        fffff980`014e3cf0 fffff800`01ee196b rdpdr!RxpWorkerThreadDispatcher+0x6f
        fffff980`014e3d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`014e3d80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa80039ac040  Cid 0004.0100  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) KernelMode Non-Alertable
            fffff98004338838  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      501            Ticks: 46078 (0:00:11:58.821)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address rdpdr!RxBootstrapWorkerThreadDispatcher (0xfffff98004352040)
        Stack Init fffff9800142ddb0 Current fffff9800142da40
        Base fffff9800142e000 Limit fffff98001428000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0142da80 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0142dbc0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0142dc20 fffff800`01c34eb1 nt!KeRemoveQueueEx+0x848
        fffff980`0142dcb0 fffff980`042e221f nt!KeRemoveQueue+0x21
        fffff980`0142dcf0 fffff800`01ee196b rdpdr!RxpWorkerThreadDispatcher+0x6f
        fffff980`0142dd50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0142dd80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa80039ac9f0  Cid 0004.0104  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) KernelMode Non-Alertable
            fffff98004338938  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      501            Ticks: 46078 (0:00:11:58.821)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address rdpdr!RxBootstrapWorkerThreadDispatcher (0xfffff98004352040)
        Stack Init fffff980014f1db0 Current fffff980014f1a40
        Base fffff980014f2000 Limit fffff980014ec000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`014f1a80 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`014f1bc0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`014f1c20 fffff800`01c34eb1 nt!KeRemoveQueueEx+0x848
        fffff980`014f1cb0 fffff980`042e221f nt!KeRemoveQueue+0x21
        fffff980`014f1cf0 fffff800`01ee196b rdpdr!RxpWorkerThreadDispatcher+0x6f
        fffff980`014f1d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`014f1d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa80039ac560  Cid 0004.0108  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffff98004338ad8  NotificationEvent
            fffffa80039ac618  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      42817          Ticks: 3762 (0:00:00:58.687)
        Context Switch Count      13
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address rdpdr!RxSpinUpRequestsDispatcher (0xfffff980042e1d80)
        Stack Init fffff98001434db0 Current fffff98001434a70
        Base fffff98001435000 Limit fffff9800142f000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`01434ab0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`01434bf0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`01434c50 fffff980`042e1dfc nt!KeWaitForSingleObject+0x5f5
        fffff980`01434cd0 fffff800`01ee196b rdpdr!RxSpinUpRequestsDispatcher+0x7c
        fffff980`01434d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`01434d80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa8003a84bb0  Cid 0004.010c  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffffa80039744c0  NotificationEvent
            fffffa8003a84c68  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      46461          Ticks: 118 (0:00:00:01.840)
        Context Switch Count      148
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address parport!P5FdoThread (0xfffff9800300b67c)
        Stack Init fffff9800143bdb0 Current fffff9800143ba60
        Base fffff9800143c000 Limit fffff98001436000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0143baa0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0143bbe0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0143bc40 fffff980`0300b6de nt!KeWaitForSingleObject+0x5f5
        fffff980`0143bcc0 fffff800`01ee196b parport!P5FdoThread+0x62
        fffff980`0143bd50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0143bd80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa8003c5b040  Cid 0004.0128  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffff9800436f5e0  SynchronizationEvent
            fffff9800436f5a0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      7643           Ticks: 38936 (0:00:10:07.405)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address raspptp!MainPassiveLevelThread (0xfffff9800435ee90)
        Stack Init fffff98001450db0 Current fffff98001450aa0
        Base fffff98001451000 Limit fffff9800144b000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`01450ae0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`01450c20 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`01450c80 fffff980`0435ef0d nt!KeWaitForMultipleObjects+0x703
        fffff980`01450cf0 fffff800`01ee196b raspptp!MainPassiveLevelThread+0x7d
        fffff980`01450d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`01450d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa8003dc0710  Cid 0004.012c  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffff9800145ed00  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      744            Ticks: 45835 (0:00:11:55.030)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address DLARTL_E!ThreadIsCriticalWaiting (0xfffff98002fd2e90)
        Stack Init fffff9800145edb0 Current fffff9800145e9f0
        Base fffff9800145f000 Limit fffff98001459000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0145ea30 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0145eb70 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0145ebd0 fffff980`02fd2b60 nt!KeWaitForSingleObject+0x5f5
        fffff980`0145ec50 fffff980`02fd304c DLARTL_E!ThreadBlock+0x60
        fffff980`0145eca0 fffff980`02fd2f04 DLARTL_E!GetTimer+0x70
        fffff980`0145ecd0 fffff800`01ee196b DLARTL_E!ThreadIsCriticalWaiting+0x84
        fffff980`0145ed50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0145ed80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa8003f17980  Cid 0004.0130  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffff980030c9180  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      753            Ticks: 45826 (0:00:11:54.890)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address rasacd!AcdNotificationRequestThread (0xfffff980030c73e4)
        Stack Init fffff98001465db0 Current fffff98001465ab0
        Base fffff98001466000 Limit fffff98001460000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`01465af0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`01465c30 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`01465c90 fffff980`030c74ff nt!KeWaitForSingleObject+0x5f5
        fffff980`01465d10 fffff800`01ee196b rasacd!AcdNotificationRequestThread+0x11b
        fffff980`01465d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`01465d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa8003f1d040  Cid 0004.014c  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) KernelMode Non-Alertable
            fffff98004dbcb50  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      46296          Ticks: 283 (0:00:00:04.414)
        Context Switch Count      16
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address rdbss!RxBootstrapWorkerThreadDispatcher (0xfffff98004ddbb60)
        Stack Init fffff980044c1db0 Current fffff980044c19f0
        Base fffff980044c2000 Limit fffff980044bc000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`044c1a30 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`044c1b70 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`044c1bd0 fffff800`01c34eb1 nt!KeRemoveQueueEx+0x848
        fffff980`044c1c60 fffff980`04d9e1f5 nt!KeRemoveQueue+0x21
        fffff980`044c1ca0 fffff800`01ee196b rdbss!RxpWorkerThreadDispatcher+0xc5
        fffff980`044c1d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`044c1d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa8003f1dbb0  Cid 0004.0150  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) KernelMode Non-Alertable
            fffff98004dbcb50  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      27408          Ticks: 19171 (0:00:04:59.069)
        Context Switch Count      46
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address rdbss!RxBootstrapWorkerThreadDispatcher (0xfffff98004ddbb60)
        Stack Init fffff9800452adb0 Current fffff9800452a9f0
        Base fffff9800452b000 Limit fffff98004525000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0452aa30 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0452ab70 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0452abd0 fffff800`01c34eb1 nt!KeRemoveQueueEx+0x848
        fffff980`0452ac60 fffff980`04d9e1f5 nt!KeRemoveQueue+0x21
        fffff980`0452aca0 fffff800`01ee196b rdbss!RxpWorkerThreadDispatcher+0xc5
        fffff980`0452ad50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0452ad80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa8003f1d720  Cid 0004.0154  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) KernelMode Non-Alertable
            fffff98004dbcc68  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      770            Ticks: 45809 (0:00:11:54.624)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address rdbss!RxBootstrapWorkerThreadDispatcher (0xfffff98004ddbb60)
        Stack Init fffff980044c8db0 Current fffff980044c89f0
        Base fffff980044c9000 Limit fffff980044c3000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`044c8a30 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`044c8b70 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`044c8bd0 fffff800`01c34eb1 nt!KeRemoveQueueEx+0x848
        fffff980`044c8c60 fffff980`04d9e1f5 nt!KeRemoveQueue+0x21
        fffff980`044c8ca0 fffff800`01ee196b rdbss!RxpWorkerThreadDispatcher+0xc5
        fffff980`044c8d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`044c8d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa8003f1e040  Cid 0004.0158  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) KernelMode Non-Alertable
            fffff98004dbcc68  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      2523           Ticks: 44056 (0:00:11:27.278)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address rdbss!RxBootstrapWorkerThreadDispatcher (0xfffff98004ddbb60)
        Stack Init fffff9800146cdb0 Current fffff9800146c9f0
        Base fffff9800146d000 Limit fffff98001467000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0146ca30 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0146cb70 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0146cbd0 fffff800`01c34eb1 nt!KeRemoveQueueEx+0x848
        fffff980`0146cc60 fffff980`04d9e1f5 nt!KeRemoveQueue+0x21
        fffff980`0146cca0 fffff800`01ee196b rdbss!RxpWorkerThreadDispatcher+0xc5
        fffff980`0146cd50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0146cd80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa8003f1ebb0  Cid 0004.015c  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) KernelMode Non-Alertable
            fffff98004dbc6f0  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      46296          Ticks: 283 (0:00:00:04.414)
        Context Switch Count      51
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address rdbss!RxBootstrapWorkerThreadDispatcher (0xfffff98004ddbb60)
        Stack Init fffff98001457db0 Current fffff980014579f0
        Base fffff98001458000 Limit fffff98001452000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`01457a30 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`01457b70 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`01457bd0 fffff800`01c34eb1 nt!KeRemoveQueueEx+0x848
        fffff980`01457c60 fffff980`04d9e1f5 nt!KeRemoveQueue+0x21
        fffff980`01457ca0 fffff800`01ee196b rdbss!RxpWorkerThreadDispatcher+0xc5
        fffff980`01457d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`01457d80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa8003f1e720  Cid 0004.0160  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) KernelMode Non-Alertable
            fffff98004dbc808  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      27065          Ticks: 19514 (0:00:05:04.420)
        Context Switch Count      11
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address rdbss!RxBootstrapWorkerThreadDispatcher (0xfffff98004ddbb60)
        Stack Init fffff980044e4db0 Current fffff980044e49f0
        Base fffff980044e5000 Limit fffff980044df000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`044e4a30 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`044e4b70 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`044e4bd0 fffff800`01c34eb1 nt!KeRemoveQueueEx+0x848
        fffff980`044e4c60 fffff980`04d9e1f5 nt!KeRemoveQueue+0x21
        fffff980`044e4ca0 fffff800`01ee196b rdbss!RxpWorkerThreadDispatcher+0xc5
        fffff980`044e4d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`044e4d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa8003f1f040  Cid 0004.0164  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) KernelMode Non-Alertable
            fffff98004dbc920  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      770            Ticks: 45809 (0:00:11:54.624)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address rdbss!RxBootstrapWorkerThreadDispatcher (0xfffff98004ddbb60)
        Stack Init fffff980044ebdb0 Current fffff980044eb9f0
        Base fffff980044ec000 Limit fffff980044e6000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`044eba30 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`044ebb70 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`044ebbd0 fffff800`01c34eb1 nt!KeRemoveQueueEx+0x848
        fffff980`044ebc60 fffff980`04d9e1f5 nt!KeRemoveQueue+0x21
        fffff980`044ebca0 fffff800`01ee196b rdbss!RxpWorkerThreadDispatcher+0xc5
        fffff980`044ebd50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`044ebd80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa8003f1fbb0  Cid 0004.0168  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) KernelMode Non-Alertable
            fffff98004dbca38  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      46296          Ticks: 283 (0:00:00:04.414)
        Context Switch Count      295
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address rdbss!RxBootstrapWorkerThreadDispatcher (0xfffff98004ddbb60)
        Stack Init fffff980044f2db0 Current fffff980044f29f0
        Base fffff980044f3000 Limit fffff980044ed000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`044f2a30 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`044f2b70 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`044f2bd0 fffff800`01c34eb1 nt!KeRemoveQueueEx+0x848
        fffff980`044f2c60 fffff980`04d9e1f5 nt!KeRemoveQueue+0x21
        fffff980`044f2ca0 fffff800`01ee196b rdbss!RxpWorkerThreadDispatcher+0xc5
        fffff980`044f2d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`044f2d80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa8003f1f720  Cid 0004.016c  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) KernelMode Non-Alertable
            fffff98004dbca38  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      46296          Ticks: 283 (0:00:00:04.414)
        Context Switch Count      78
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address rdbss!RxBootstrapWorkerThreadDispatcher (0xfffff98004ddbb60)
        Stack Init fffff980044f9db0 Current fffff980044f99f0
        Base fffff980044fa000 Limit fffff980044f4000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`044f9a30 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`044f9b70 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`044f9bd0 fffff800`01c34eb1 nt!KeRemoveQueueEx+0x848
        fffff980`044f9c60 fffff980`04d9e1f5 nt!KeRemoveQueue+0x21
        fffff980`044f9ca0 fffff800`01ee196b rdbss!RxpWorkerThreadDispatcher+0xc5
        fffff980`044f9d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`044f9d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa8003f20040  Cid 0004.0170  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffff98004dbccf8  NotificationEvent
            fffffa8003f200f8  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      43084          Ticks: 3495 (0:00:00:54.522)
        Context Switch Count      12
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address rdbss!RxSpinUpRequestsDispatcher (0xfffff98004da41e0)
        Stack Init fffff98004500db0 Current fffff98004500a80
        Base fffff98004501000 Limit fffff980044fb000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`04500ac0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`04500c00 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`04500c60 fffff980`04da42a5 nt!KeWaitForSingleObject+0x5f5
        fffff980`04500ce0 fffff800`01ee196b rdbss!RxSpinUpRequestsDispatcher+0xc5
        fffff980`04500d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`04500d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa8003f6fb30  Cid 0004.0174  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffffa8003f2a130  SynchronizationEvent
        IRP List:
            fffffa80018cb460: (0006,0118) Flags: 00060070  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      781            Ticks: 45798 (0:00:11:54.453)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address SYMEVENT64x86!SYMEvent_GetSubTask (0xfffff98004cd1be0)
        Stack Init fffff9800450edb0 Current fffff9800450ea60
        Base fffff9800450f000 Limit fffff98004509000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0450eaa0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0450ebe0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0450ec40 fffff980`04cd1e41 nt!KeWaitForSingleObject+0x5f5
        fffff980`0450ecc0 fffff800`01ee196b SYMEVENT64x86!SYMEvent_GetSubTask+0x23d1
        fffff980`0450ed50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0450ed80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa8003f28a10  Cid 0004.0178  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffffa8003f389d0  NotificationEvent
            fffffa8003f28ac8  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      45317          Ticks: 1262 (0:00:00:19.687)
        Context Switch Count      465
        UserTime                  00:00:00.000
        KernelTime                00:00:00.046
        Win32 Start Address eeCtrl64 (0xfffff98004d36bc4)
        Stack Init fffff98004507db0 Current fffff98004507980
        Base fffff98004508000 Limit fffff98004502000 Call 0
        Priority 13 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`045079c0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`04507b00 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`04507b60 fffff980`04d33755 nt!KeWaitForSingleObject+0x5f5
        fffff980`04507be0 fffff980`04d2c7de eeCtrl64+0xf755
        fffff980`04507c20 fffff980`04d36c04 eeCtrl64+0x87de
        fffff980`04507d20 fffff800`01ee196b eeCtrl64+0x12c04
        fffff980`04507d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`04507d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa8003f58570  Cid 0004.0180  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrLpcReceive) UserMode Non-Alertable
            fffffa8003f58900  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      16093          Ticks: 30486 (0:00:07:55.584)
        Context Switch Count      71
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!SepRmCommandServerThread (0xfffff80001e71b30)
        Stack Init fffff98001488db0 Current fffff980014882e0
        Base fffff98001489000 Limit fffff98001483000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`01488320 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`01488460 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`014884c0 fffff800`01eb3788 nt!KeWaitForSingleObject+0x5f5
        fffff980`01488540 fffff800`01e7e523 nt!AlpcpReceiveMessagePort+0x298
        fffff980`014885a0 fffff800`01e740d2 nt!AlpcpReceiveLegacyMessage+0x122
        fffff980`01488640 fffff800`01e724bf nt!NtReplyWaitReceivePortEx+0xc1
        fffff980`014886d0 fffff800`01c4d733 nt!NtReplyWaitReceivePort+0xf
        fffff980`01488710 fffff800`01c4dc40 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`01488710)
        fffff980`014888a8 fffff800`01e71c1f nt!KiServiceLinkage
        fffff980`014888b0 fffff800`01ee196b nt!SepRmCommandServerThread+0xef
        fffff980`01488d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`01488d80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa8002984bb0  Cid 0004.01c8  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffff80001d68980  QueueObject
            fffffa8002984c68  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      46569          Ticks: 10 (0:00:00:00.156)
        Context Switch Count      5069
        UserTime                  00:00:00.000
        KernelTime                00:00:00.140
        Win32 Start Address nt!ExpWorkerThread (0xfffff80001c59c80)
        Stack Init fffff98004f96db0 Current fffff98004f96a70
        Base fffff98004f97000 Limit fffff98004f91000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`04f96ab0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`04f96bf0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`04f96c50 fffff800`01c59d7d nt!KeRemoveQueueEx+0x848
        fffff980`04f96ce0 fffff800`01ee196b nt!ExpWorkerThread+0x104
        fffff980`04f96d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`04f96d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa80041b4800  Cid 0004.01d0  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffff80001d68980  QueueObject
            fffffa80041b48b8  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      13295          Ticks: 33284 (0:00:08:39.233)
        Context Switch Count      5596
        UserTime                  00:00:00.000
        KernelTime                00:00:00.296
        Win32 Start Address nt!ExpWorkerThread (0xfffff80001c59c80)
        Stack Init fffff98004fc7db0 Current fffff98004fc7a70
        Base fffff98004fc8000 Limit fffff98004fc2000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`04fc7ab0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`04fc7bf0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`04fc7c50 fffff800`01c59d7d nt!KeRemoveQueueEx+0x848
        fffff980`04fc7ce0 fffff800`01ee196b nt!ExpWorkerThread+0x104
        fffff980`04fc7d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`04fc7d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa8003bf1bb0  Cid 0004.01d8  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffff80001d68980  QueueObject
            fffffa8003bf1c68  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      38990          Ticks: 7589 (0:00:01:58.389)
        Context Switch Count      2932
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address nt!ExpWorkerThread (0xfffff80001c59c80)
        Stack Init fffff98004fb9db0 Current fffff98004fb9a70
        Base fffff98004fba000 Limit fffff98004fb4000 Call 0
        Priority 15 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`04fb9ab0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`04fb9bf0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`04fb9c50 fffff800`01c59d7d nt!KeRemoveQueueEx+0x848
        fffff980`04fb9ce0 fffff800`01ee196b nt!ExpWorkerThread+0x104
        fffff980`04fb9d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`04fb9d80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa80041b4040  Cid 0004.01e4  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffff80001d68980  QueueObject
            fffffa80041b40f8  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      46148          Ticks: 431 (0:00:00:06.723)
        Context Switch Count      10832
        UserTime                  00:00:00.000
        KernelTime                00:00:00.421
        Win32 Start Address nt!ExpWorkerThread (0xfffff80001c59c80)
        Stack Init fffff98004fe3db0 Current fffff98004fe3a70
        Base fffff98004fe4000 Limit fffff98004fde000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`04fe3ab0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`04fe3bf0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`04fe3c50 fffff800`01c59d7d nt!KeRemoveQueueEx+0x848
        fffff980`04fe3ce0 fffff800`01ee196b nt!ExpWorkerThread+0x104
        fffff980`04fe3d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`04fe3d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa8003fd1bb0  Cid 0004.0204  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Alertable
            fffffa8001885038  NotificationEvent
            fffffa80018850e0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      1205           Ticks: 45374 (0:00:11:47.838)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address atikmdag!xc_copp_agent (0xfffff980041cf984)
        Stack Init fffff98000a0fdb0 Current fffff98000a0fa90
        Base fffff98000a10000 Limit fffff98000a0a000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`00a0fad0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`00a0fc10 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`00a0fc70 fffff980`041cf9e0 nt!KeWaitForMultipleObjects+0x703
        fffff980`00a0fce0 fffff800`01ee196b atikmdag!xc_copp_agent+0x616890
        fffff980`00a0fd50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`00a0fd80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa8003d73890  Cid 0004.0208  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffffa80041c8570  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      1326           Ticks: 45253 (0:00:11:45.951)
        Context Switch Count      162
        UserTime                  00:00:00.000
        KernelTime                00:00:00.109
        Win32 Start Address atikmdag (0xfffff98003afd640)
        Stack Init fffff98001442db0 Current fffff98001442910
        Base fffff98001443000 Limit fffff9800143d000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`01442950 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`01442a90 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`01442af0 fffff980`03a7e5ce nt!KeWaitForSingleObject+0x5f5
        fffff980`01442b70 fffff980`03afe23f atikmdag+0x1f5ce
        fffff980`01442bb0 fffff980`03afd65d atikmdag+0x9f23f
        fffff980`01442d10 fffff800`01ee196b atikmdag+0x9e65d
        fffff980`01442d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`01442d80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa8004069a70  Cid 0004.020c  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffffa8003fd6558  SynchronizationEvent
            fffffa8003fd6540  SynchronizationEvent
            fffffa8003fd6588  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      16769          Ticks: 29810 (0:00:07:45.038)
        Context Switch Count      21
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address dxgkrnl!VidSchiWorkerThread (0xfffff9800399431c)
        Stack Init fffff98001449db0 Current fffff98001449920
        Base fffff9800144a000 Limit fffff98001444000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`01449960 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`01449aa0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`01449b00 fffff980`03994559 nt!KeWaitForMultipleObjects+0x703
        fffff980`01449b70 fffff980`038dccd8 dxgkrnl!VidSchiWaitForSchedulerEvents+0x161
        fffff980`01449bf0 fffff980`039943b1 dxgkrnl!VidSchiScheduleCommandToRun+0x398
        fffff980`01449d10 fffff800`01ee196b dxgkrnl!VidSchiWorkerThread+0x95
        fffff980`01449d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`01449d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa8004087060  Cid 0004.0248  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) KernelMode Alertable
            fffffa8004073830  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      45939          Ticks: 640 (0:00:00:09.984)
        Context Switch Count      362
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address msrpc!LrpcKernelBaseRoutine (0xfffff98000462a24)
        Stack Init fffff9800147adb0 Current fffff9800147a750
        Base fffff9800147b000 Limit fffff98001475000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0147a790 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0147a8d0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0147a930 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0147a9c0 fffff800`01e5b152 nt!IoRemoveIoCompletion+0x47
        fffff980`0147aa40 fffff800`01c4d733 nt!NtRemoveIoCompletionEx+0xf2
        fffff980`0147aae0 fffff800`01c4dc40 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0147ab50)
        fffff980`0147ace8 fffff980`00462a53 nt!KiServiceLinkage
        fffff980`0147acf0 fffff800`01ee196b msrpc!LrpcKernelBaseRoutine+0x2f
        fffff980`0147ad50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0147ad80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa80042a5060  Cid 0004.02ac  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffffa800422bb78  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      12684          Ticks: 33895 (0:00:08:48.765)
        Context Switch Count      18
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!EtwpLogger (0xfffff80001e90370)
        Stack Init fffff9800b3d5db0 Current fffff9800b3d5a90
        Base fffff9800b3d6000 Limit fffff9800b3d0000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0b3d5ad0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0b3d5c10 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0b3d5c70 fffff800`01e9044d nt!KeWaitForSingleObject+0x5f5
        fffff980`0b3d5cf0 fffff800`01ee196b nt!EtwpLogger+0xdd
        fffff980`0b3d5d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0b3d5d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa80043dabb0  Cid 0004.035c  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffffa80043a7a38  NotificationEvent
            fffffa80043a7a50  SynchronizationEvent
            fffffa80043a7a98  NotificationEvent
        IRP List:
            fffffa80025d38c0: (0006,03a0) Flags: 00060800  Mdl: fffffa80020707d0
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      38349          Ticks: 8230 (0:00:02:08.388)
        Context Switch Count      1369
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address luafv!UsnThread (0xfffff9800ba55a28)
        Stack Init fffff9800bac1db0 Current fffff9800bac19b0
        Base fffff9800bac2000 Limit fffff9800babc000 Call 0
        Priority 13 BasePriority 8 PriorityDecrement 4 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0bac19f0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0bac1b30 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0bac1b90 fffff980`0ba559be nt!KeWaitForMultipleObjects+0x703
        fffff980`0bac1c00 fffff980`0ba55afe luafv!SynchronousFsControl+0x102
        fffff980`0bac1c90 fffff800`01ee196b luafv!UsnThread+0xd6
        fffff980`0bac1d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0bac1d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa80043d9040  Cid 0004.0360  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffffa8004395690  Semaphore Limit 0xc8
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      1523           Ticks: 45056 (0:00:11:42.878)
        Context Switch Count      14
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address DRVEDDM (0xfffff980064a09b4)
        Stack Init fffff9800babadb0 Current fffff9800babaa70
        Base fffff9800babb000 Limit fffff9800bab5000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0babaab0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0bababf0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0babac50 fffff980`064a09eb nt!KeWaitForSingleObject+0x5f5
        fffff980`0babacd0 fffff800`01ee196b DRVEDDM+0x69eb
        fffff980`0babad50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0babad80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa80043ccbb0  Cid 0004.0368  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffffa8004375bd0  Semaphore Limit 0xc8
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      1513           Ticks: 45066 (0:00:11:43.034)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address DRVEDDM (0xfffff980064a0ad4)
        Stack Init fffff9800b694db0 Current fffff9800b694a60
        Base fffff9800b695000 Limit fffff9800b68f000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0b694aa0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0b694be0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0b694c40 fffff980`064a0b2d nt!KeWaitForSingleObject+0x5f5
        fffff980`0b694cc0 fffff800`01ee196b DRVEDDM+0x6b2d
        fffff980`0b694d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0b694d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa80043bdbb0  Cid 0004.0370  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffff9800ba89d00  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      1530           Ticks: 45049 (0:00:11:42.768)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address DLARTL_E!ThreadIsCriticalWaiting (0xfffff98002fd2e90)
        Stack Init fffff9800ba89db0 Current fffff9800ba89900
        Base fffff9800ba8a000 Limit fffff9800ba84000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0ba89940 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0ba89a80 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0ba89ae0 fffff980`02fd2b60 nt!KeWaitForSingleObject+0x5f5
        fffff980`0ba89b60 fffff980`02fd1fea DLARTL_E!ThreadBlock+0x60
        fffff980`0ba89bb0 fffff980`0ba300fe DLARTL_E!QueueReadTimeout+0x66
        fffff980`0ba89c30 fffff980`02fd2f04 DLAIFS_E!ReleaseDrive+0xa22
        fffff980`0ba89cd0 fffff800`01ee196b DLARTL_E!ThreadIsCriticalWaiting+0x84
        fffff980`0ba89d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0ba89d80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa80043cd5d0  Cid 0004.0374  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffff9800bac8d00  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      1530           Ticks: 45049 (0:00:11:42.768)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address DLARTL_E!ThreadIsCriticalWaiting (0xfffff98002fd2e90)
        Stack Init fffff9800bac8db0 Current fffff9800bac89d0
        Base fffff9800bac9000 Limit fffff9800bac3000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0bac8a10 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0bac8b50 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0bac8bb0 fffff980`02fd2b60 nt!KeWaitForSingleObject+0x5f5
        fffff980`0bac8c30 fffff980`030d14c6 DLARTL_E!ThreadBlock+0x60
        fffff980`0bac8c80 fffff980`02fd2f04 DLABOIOE+0x34c6
        fffff980`0bac8cd0 fffff800`01ee196b DLARTL_E!ThreadIsCriticalWaiting+0x84
        fffff980`0bac8d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0bac8d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa800474c060  Cid 0004.0254  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffff98004cb7260  NotificationEvent
            fffff98004cb7290  NotificationEvent
            fffff98004cb7278  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      1583           Ticks: 44996 (0:00:11:41.942)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address csc!CscEnpEvictAutoThread (0xfffff98004c9b8e8)
        Stack Init fffff9800cc1bdb0 Current fffff9800cc1ba70
        Base fffff9800cc1c000 Limit fffff9800cc16000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0cc1bab0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0cc1bbf0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0cc1bc50 fffff980`04c9ba80 nt!KeWaitForMultipleObjects+0x703
        fffff980`0cc1bcc0 fffff800`01ee196b csc!CscEnpEvictAutoThread+0x198
        fffff980`0cc1bd50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0cc1bd80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa800474cad0  Cid 0004.017c  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffff98004cb7260  NotificationEvent
            fffff98004cb72a8  NotificationEvent
            fffffa800474cb88  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      1583           Ticks: 44996 (0:00:11:41.942)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address csc!CscEnpEvictAutoThread (0xfffff98004c9b8e8)
        Stack Init fffff9800cc22db0 Current fffff9800cc22a70
        Base fffff9800cc23000 Limit fffff9800cc1d000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0cc22ab0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0cc22bf0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0cc22c50 fffff980`04c9ba80 nt!KeWaitForMultipleObjects+0x703
        fffff980`0cc22cc0 fffff800`01ee196b csc!CscEnpEvictAutoThread+0x198
        fffff980`0cc22d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0cc22d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa800453b4a0  Cid 0004.0474  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffff9800e3a5ea8  NotificationEvent
            fffffa800463d028  NotificationEvent
            fffffa800463f068  NotificationEvent
            fffffa80046410a8  NotificationEvent
            fffffa80046430e8  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      1598           Ticks: 44981 (0:00:11:41.708)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address spsys!SPVersion (0xfffff9800e3bed29)
        Stack Init fffff9800dabadb0 Current fffff9800dabaa80
        Base fffff9800dabb000 Limit fffff9800dab5000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0dabaac0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0dabac00 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0dabac60 fffff980`0e3bedc1 nt!KeWaitForMultipleObjects+0x703
        fffff980`0dabacd0 fffff800`01ee196b spsys!SPVersion+0x19491
        fffff980`0dabad50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0dabad80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa80045f82f0  Cid 0004.05c0  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffffa80045f8760  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      46294          Ticks: 285 (0:00:00:04.446)
        Context Switch Count      183
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address HTTP!UlpThreadPoolWorker (0xfffff9800e7aa010)
        Stack Init fffff9800e482db0 Current fffff9800e482a90
        Base fffff9800e483000 Limit fffff9800e47d000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0e482ad0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e482c10 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0e482c70 fffff980`0e7aa27d nt!KeWaitForSingleObject+0x5f5
        fffff980`0e482cf0 fffff800`01ee196b HTTP!UlpThreadPoolWorker+0x26c
        fffff980`0e482d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0e482d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa80045fa040  Cid 0004.05c4  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffffa80045f87e0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      5527           Ticks: 41052 (0:00:10:40.415)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address HTTP!UlpThreadPoolWorker (0xfffff9800e7aa010)
        Stack Init fffff9800e489db0 Current fffff9800e489a90
        Base fffff9800e48a000 Limit fffff9800e484000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0e489ad0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e489c10 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0e489c70 fffff980`0e7aa27d nt!KeWaitForSingleObject+0x5f5
        fffff980`0e489cf0 fffff800`01ee196b HTTP!UlpThreadPoolWorker+0x26c
        fffff980`0e489d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0e489d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa80045fabb0  Cid 0004.05c8  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffffa80045f8860  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      43994          Ticks: 2585 (0:00:00:40.326)
        Context Switch Count      13
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address HTTP!UlpThreadPoolWorker (0xfffff9800e7aa010)
        Stack Init fffff9800e49edb0 Current fffff9800e49ea90
        Base fffff9800e49f000 Limit fffff9800e499000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0e49ead0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e49ec10 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0e49ec70 fffff980`0e7aa27d nt!KeWaitForSingleObject+0x5f5
        fffff980`0e49ecf0 fffff800`01ee196b HTTP!UlpThreadPoolWorker+0x26c
        fffff980`0e49ed50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0e49ed80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa80045fa720  Cid 0004.05cc  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffffa80045f88e0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      1679           Ticks: 44900 (0:00:11:40.444)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address HTTP!UlpThreadPoolWorker (0xfffff9800e7aa010)
        Stack Init fffff9800e4a5db0 Current fffff9800e4a5a90
        Base fffff9800e4a6000 Limit fffff9800e4a0000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0e4a5ad0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e4a5c10 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0e4a5c70 fffff980`0e7aa27d nt!KeWaitForSingleObject+0x5f5
        fffff980`0e4a5cf0 fffff800`01ee196b HTTP!UlpThreadPoolWorker+0x26c
        fffff980`0e4a5d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0e4a5d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa80045fb040  Cid 0004.05d0  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffffa80045f8960  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      1871           Ticks: 44708 (0:00:11:37.449)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address HTTP!UlpThreadPoolWorker (0xfffff9800e7aa010)
        Stack Init fffff9800e4acdb0 Current fffff9800e4aca90
        Base fffff9800e4ad000 Limit fffff9800e4a7000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0e4acad0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e4acc10 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0e4acc70 fffff980`0e7aa27d nt!KeWaitForSingleObject+0x5f5
        fffff980`0e4accf0 fffff800`01ee196b HTTP!UlpThreadPoolWorker+0x26c
        fffff980`0e4acd50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0e4acd80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa80045fbbb0  Cid 0004.05d4  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffffa80045f89e0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      1679           Ticks: 44900 (0:00:11:40.444)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address HTTP!UlpThreadPoolWorker (0xfffff9800e7aa010)
        Stack Init fffff9800e4b3db0 Current fffff9800e4b3a90
        Base fffff9800e4b4000 Limit fffff9800e4ae000 Call 0
        Priority 11 BasePriority 11 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0e4b3ad0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e4b3c10 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0e4b3c70 fffff980`0e7aa27d nt!KeWaitForSingleObject+0x5f5
        fffff980`0e4b3cf0 fffff800`01ee196b HTTP!UlpThreadPoolWorker+0x26c
        fffff980`0e4b3d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0e4b3d80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa80045fc040  Cid 0004.05d8  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffff9800e7a2260  NotificationEvent
            fffff9800e7a2240  NotificationEvent
            fffffa800189bd80  NotificationEvent
            fffff9800e7a2280  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      40400          Ticks: 6179 (0:00:01:36.393)
        Context Switch Count      13
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address HTTP!UlpScavengerThread (0xfffff9800e7c2920)
        Stack Init fffff9800e4badb0 Current fffff9800e4ba9f0
        Base fffff9800e4bb000 Limit fffff9800e4b5000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0e4baa30 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e4bab70 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0e4babd0 fffff980`0e7c299e nt!KeWaitForMultipleObjects+0x703
        fffff980`0e4bac40 fffff800`01ee196b HTTP!UlpScavengerThread+0x81
        fffff980`0e4bad50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0e4bad80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa8004658600  Cid 0004.0614  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffff9800da18ec0  SynchronizationEvent
            fffff9800da18ee0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      7401           Ticks: 39178 (0:00:10:11.180)
        Context Switch Count      29
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address mpsdrv!IP6StringToAddress (0xfffff9800da140c0)
        Stack Init fffff9800e71fdb0 Current fffff9800e71fa80
        Base fffff9800e720000 Limit fffff9800e71a000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0e71fac0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e71fc00 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0e71fc60 fffff980`0da14228 nt!KeWaitForMultipleObjects+0x703
        fffff980`0e71fcd0 fffff800`01ee196b mpsdrv!IP6StringToAddress+0x738
        fffff980`0e71fd50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0e71fd80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa8004665040  Cid 0004.0634  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffff9800e442460  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      45338          Ticks: 1241 (0:00:00:19.359)
        Context Switch Count      36
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address mrxdav!MRxDAVContextTimerThread (0xfffff9800e43d8b8)
        Stack Init fffff9800e490db0 Current fffff9800e490ab0
        Base fffff9800e491000 Limit fffff9800e48b000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0e490af0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e490c30 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0e490c90 fffff980`0e43d92a nt!KeWaitForSingleObject+0x5f5
        fffff980`0e490d10 fffff800`01ee196b mrxdav!MRxDAVContextTimerThread+0x72
        fffff980`0e490d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0e490d80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa80046ad450  Cid 0004.0670  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) KernelMode Non-Alertable
            fffffa80046adb20  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      1742           Ticks: 44837 (0:00:11:39.461)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address srv2!SrvProcWorkerThread (0xfffff9800e682400)
        Stack Init fffff9800e726db0 Current fffff9800e726a60
        Base fffff9800e727000 Limit fffff9800e721000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0e726aa0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e726be0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0e726c40 fffff800`01c34eb1 nt!KeRemoveQueueEx+0x848
        fffff980`0e726cd0 fffff980`0e682474 nt!KeRemoveQueue+0x21
        fffff980`0e726d10 fffff800`01ee196b srv2!SrvProcWorkerThread+0x74
        fffff980`0e726d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0e726d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa80046b1bb0  Cid 0004.0674  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) KernelMode Non-Alertable
            fffffa80046adc40  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      1743           Ticks: 44836 (0:00:11:39.446)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address srv2!SrvProcWorkerThread (0xfffff9800e682400)
        Stack Init fffff9800e46ddb0 Current fffff9800e46da60
        Base fffff9800e46e000 Limit fffff9800e468000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0e46daa0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e46dbe0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0e46dc40 fffff800`01c34eb1 nt!KeRemoveQueueEx+0x848
        fffff980`0e46dcd0 fffff980`0e682474 nt!KeRemoveQueue+0x21
        fffff980`0e46dd10 fffff800`01ee196b srv2!SrvProcWorkerThread+0x74
        fffff980`0e46dd50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0e46dd80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa80046ae670  Cid 0004.0678  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) KernelMode Non-Alertable
            fffffa80046ad8d0  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      1744           Ticks: 44835 (0:00:11:39.430)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address srv2!SrvProcWorkerThread (0xfffff9800e682400)
        Stack Init fffff9800e497db0 Current fffff9800e497a60
        Base fffff9800e498000 Limit fffff9800e492000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0e497aa0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e497be0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0e497c40 fffff800`01c34eb1 nt!KeRemoveQueueEx+0x848
        fffff980`0e497cd0 fffff980`0e682474 nt!KeRemoveQueue+0x21
        fffff980`0e497d10 fffff800`01ee196b srv2!SrvProcWorkerThread+0x74
        fffff980`0e497d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0e497d80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa80046af040  Cid 0004.0680  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) KernelMode Non-Alertable
            fffffa80046ad9f0  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      1744           Ticks: 44835 (0:00:11:39.430)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address srv2!SrvProcWorkerThread (0xfffff9800e682400)
        Stack Init fffff9800ccbcdb0 Current fffff9800ccbca60
        Base fffff9800ccbd000 Limit fffff9800ccb7000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0ccbcaa0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0ccbcbe0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0ccbcc40 fffff800`01c34eb1 nt!KeRemoveQueueEx+0x848
        fffff980`0ccbccd0 fffff980`0e682474 nt!KeRemoveQueue+0x21
        fffff980`0ccbcd10 fffff800`01ee196b srv2!SrvProcWorkerThread+0x74
        fffff980`0ccbcd50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0ccbcd80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa80046afbb0  Cid 0004.068c  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) KernelMode Non-Alertable
            fffffa8004686390  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      1745           Ticks: 44834 (0:00:11:39.414)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address srv2!SrvProcWorkerThread (0xfffff9800e682400)
        Stack Init fffff9800e734db0 Current fffff9800e734a60
        Base fffff9800e735000 Limit fffff9800e72f000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0e734aa0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e734be0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0e734c40 fffff800`01c34eb1 nt!KeRemoveQueueEx+0x848
        fffff980`0e734cd0 fffff980`0e682474 nt!KeRemoveQueue+0x21
        fffff980`0e734d10 fffff800`01ee196b srv2!SrvProcWorkerThread+0x74
        fffff980`0e734d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0e734d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa80046e0bb0  Cid 0004.0694  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa80046db028  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      1746           Ticks: 44833 (0:00:11:39.399)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address srv!WorkerThread (0xfffff9800eb45d20)
        Stack Init fffff9800ebb9db0 Current fffff9800ebb9a50
        Base fffff9800ebba000 Limit fffff9800ebb4000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0ebb9a90 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0ebb9bd0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0ebb9c30 fffff800`01c34eb1 nt!KeRemoveQueueEx+0x848
        fffff980`0ebb9cc0 fffff980`0eb45dad nt!KeRemoveQueue+0x21
        fffff980`0ebb9d00 fffff800`01ee196b srv!WorkerThread+0x90
        fffff980`0ebb9d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0ebb9d80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa80046e2570  Cid 0004.0698  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa80046db348  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      1747           Ticks: 44832 (0:00:11:39.383)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address srv!WorkerThread (0xfffff9800eb45d20)
        Stack Init fffff9800ebc0db0 Current fffff9800ebc0a50
        Base fffff9800ebc1000 Limit fffff9800ebbb000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0ebc0a90 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0ebc0bd0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0ebc0c30 fffff800`01c34eb1 nt!KeRemoveQueueEx+0x848
        fffff980`0ebc0cc0 fffff980`0eb45dad nt!KeRemoveQueue+0x21
        fffff980`0ebc0d00 fffff800`01ee196b srv!WorkerThread+0x90
        fffff980`0ebc0d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0ebc0d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa80046e5770  Cid 0004.069c  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa80046b2188  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      1748           Ticks: 44831 (0:00:11:39.368)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address srv!WorkerThread (0xfffff9800eb45d20)
        Stack Init fffff9800ebc7db0 Current fffff9800ebc7a50
        Base fffff9800ebc8000 Limit fffff9800ebc2000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0ebc7a90 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0ebc7bd0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0ebc7c30 fffff800`01c34eb1 nt!KeRemoveQueueEx+0x848
        fffff980`0ebc7cc0 fffff980`0eb45dad nt!KeRemoveQueue+0x21
        fffff980`0ebc7d00 fffff800`01ee196b srv!WorkerThread+0x90
        fffff980`0ebc7d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0ebc7d80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa80046b5040  Cid 0004.06a0  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffff9800eb18e08  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      1749           Ticks: 44830 (0:00:11:39.352)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address srv!WorkerThread (0xfffff9800eb45d20)
        Stack Init fffff9800ebcedb0 Current fffff9800ebcea50
        Base fffff9800ebcf000 Limit fffff9800ebc9000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0ebcea90 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0ebcebd0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0ebcec30 fffff800`01c34eb1 nt!KeRemoveQueueEx+0x848
        fffff980`0ebcecc0 fffff980`0eb45dad nt!KeRemoveQueue+0x21
        fffff980`0ebced00 fffff800`01ee196b srv!WorkerThread+0x90
        fffff980`0ebced50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0ebced80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa80048cd060  Cid 0004.083c  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffffa80048b8cb8  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      1935           Ticks: 44644 (0:00:11:36.450)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!EtwpLogger (0xfffff80001e90370)
        Stack Init fffff98010388db0 Current fffff98010388a90
        Base fffff98010389000 Limit fffff98010383000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`10388ad0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`10388c10 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`10388c70 fffff800`01e9044d nt!KeWaitForSingleObject+0x5f5
        fffff980`10388cf0 fffff800`01ee196b nt!EtwpLogger+0xdd
        fffff980`10388d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`10388d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa8004b57ad0  Cid 0004.0a0c  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffffa8004b54df8  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      2777           Ticks: 43802 (0:00:11:23.315)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!EtwpLogger (0xfffff80001e90370)
        Stack Init fffff98010843db0 Current fffff98010843a90
        Base fffff98010844000 Limit fffff9801083e000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`10843ad0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`10843c10 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`10843c70 fffff800`01e9044d nt!KeWaitForSingleObject+0x5f5
        fffff980`10843cf0 fffff800`01ee196b nt!EtwpLogger+0xdd
        fffff980`10843d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`10843d80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa8004a1c7c0  Cid 0004.0540  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffff80001d542e8  NotificationEvent
            fffff80001d542d0  NotificationEvent
            fffff80001d54210  NotificationEvent
            fffff80001d54320  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      46515          Ticks: 64 (0:00:00:00.998)
        Context Switch Count      7376
        UserTime                  00:00:00.000
        KernelTime                00:00:00.343
        Win32 Start Address nt!PfTLoggingWorker (0xfffff80001fce8f0)
        Stack Init fffff98010781db0 Current fffff980107819d0
        Base fffff98010782000 Limit fffff9801077c000 Call 0
        Priority 7 BasePriority 7 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`10781a10 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`10781b50 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`10781bb0 fffff800`01fce971 nt!KeWaitForMultipleObjects+0x703
        fffff980`10781c20 fffff800`01ee196b nt!PfTLoggingWorker+0x81
        fffff980`10781d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`10781d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa80048990d0  Cid 0004.0438  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffffa800490f938  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      5531           Ticks: 41048 (0:00:10:40.352)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!EtwpLogger (0xfffff80001e90370)
        Stack Init fffff98012ff8db0 Current fffff98012ff8a90
        Base fffff98012ff9000 Limit fffff98012ff3000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`12ff8ad0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12ff8c10 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`12ff8c70 fffff800`01e9044d nt!KeWaitForSingleObject+0x5f5
        fffff980`12ff8cf0 fffff800`01ee196b nt!EtwpLogger+0xdd
        fffff980`12ff8d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`12ff8d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa8002097bb0  Cid 0004.0cec  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffffa80020b2ab8  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      7648           Ticks: 38931 (0:00:10:07.327)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!EtwpLogger (0xfffff80001e90370)
        Stack Init fffff9801dbd5db0 Current fffff9801dbd5a90
        Base fffff9801dbd6000 Limit fffff9801dbd0000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1dbd5ad0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1dbd5c10 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`1dbd5c70 fffff800`01e9044d nt!KeWaitForSingleObject+0x5f5
        fffff980`1dbd5cf0 fffff800`01ee196b nt!EtwpLogger+0xdd
        fffff980`1dbd5d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`1dbd5d80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
        THREAD fffffa800204c060  Cid 0004.0e20  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffffa800472d1f8  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      27065          Ticks: 19514 (0:00:05:04.420)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!EtwpLogger (0xfffff80001e90370)
        Stack Init fffff9801da46db0 Current fffff9801da46a90
        Base fffff9801da47000 Limit fffff9801da41000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1da46ad0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1da46c10 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`1da46c70 fffff800`01e9044d nt!KeWaitForSingleObject+0x5f5
        fffff980`1da46cf0 fffff800`01ee196b nt!EtwpLogger+0xdd
        fffff980`1da46d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`1da46d80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa8002425bb0  Cid 0004.06e0  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffffa8001857b78  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      13224          Ticks: 33355 (0:00:08:40.341)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!EtwpLogger (0xfffff80001e90370)
        Stack Init fffff980012acdb0 Current fffff980012aca90
        Base fffff980012ad000 Limit fffff980012a7000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`012acad0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`012acc10 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`012acc70 fffff800`01e903f4 nt!KeWaitForSingleObject+0x5f5
        fffff980`012accf0 fffff800`01ee196b nt!EtwpLogger+0x84
        fffff980`012acd50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`012acd80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa80048957f0  Cid 0004.0e9c  Teb: 0000000000000000 Win32Thread: 0000000000000000
RUNNING on processor 1
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8001860190       Image:         System
        Wait Start TickCount      27349          Ticks: 19230 (0:00:04:59.989)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address SystemDump64 (0xfffff9801da720f0)
        Stack Init fffff9800f3f8db0 Current fffff9800f3f8ab0
        Base fffff9800f3f9000 Limit fffff9800f3f3000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0f3f8d08 fffff980`1da72162 nt!KeBugCheckEx
        fffff980`0f3f8d10 fffff800`01ee196b SystemDump64+0x1162
        fffff980`0f3f8d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0f3f8d80 00000000`00000000 nt!KxStartSystemThread+0x16
```

Smss process

```
PROCESS fffffa8003f5b040
    SessionId: none  Cid: 0184    Peb: 7fffffd6000  ParentCid: 0004
    DirBase: 5d1fb000  ObjectTable: fffff8800012ed70  HandleCount:  28.
    Image: smss.exe
    VadRoot fffffa8003f58df0 Vads 17 Clone 0 Private 88. Modified 48. Locked 0.
    DeviceMap fffff88000007820
    Token                             fffff88002ff4c40
    ElapsedTime                       00:11:54.951
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         10184
    QuotaPoolUsage[NonPagedPool]      1536
    Working Set Sizes (now,min,max)  (166, 50, 345) (664KB, 200KB, 1380KB)
    PeakWorkingSetSize                236
    VirtualSize                       5 Mb
    PeakVirtualSize                   16 Mb
    PageFaultCount                    440
    MemoryPriority                    BACKGROUND
    BasePriority                      11
    CommitCharge                      117

    Setting context for this process...
.process /p /r fffffa8003f5b040

    !peb
PEB at 000007fffffd6000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00000000475b0000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00000000002324c0 . 00000000002324c0
    Ldr.InLoadOrderModuleList:           00000000002323d0 . 00000000002324a0
    Ldr.InMemoryOrderModuleList:         00000000002323e0 . 00000000002324b0
            Base TimeStamp                     Module
        475b0000 4549b4d2 Nov 02 09:05:22 2006 \SystemRoot\System32\smss.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       0000000000230000
    ProcessParameters: 00000000002313a0
    WindowTitle:  '< Name not readable >'
    ImageFile:    '\SystemRoot\System32\smss.exe'
    CommandLine:  '\SystemRoot\System32\smss.exe'
    DllPath:      'C:\Windows\System32'
    Environment:  0000000000231310
        Path=C:\Windows\System32
        SystemDrive=C:
        SystemRoot=C:\Windows
```

```
        THREAD fffffa8003f71ae0  Cid 0184.0188  Teb: 000007fffffde000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80040bc8e0  ProcessObject
            fffffa8003f56ad0  ProcessObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8003f5b040       Image:         smss.exe
        Wait Start TickCount      1333           Ticks: 45246 (0:00:11:45.842)
        Context Switch Count      10768
        UserTime                  00:00:00.000
        KernelTime                00:00:00.795
        Win32 Start Address smss!NtProcessStartupW (0x00000000475bfadc)
        Stack Init fffff980044cfdb0 Current fffff980044cf260
        Base fffff980044d0000 Limit fffff980044ca000 Call 0
        Priority 12 BasePriority 11 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`044cf2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`044cf3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`044cf440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`044cf4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`044cf960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`044cfbb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`044cfc20)
        00000000`0018fbf8 00000000`475bd7be ntdll!NtWaitForMultipleObjects+0xa
        00000000`0018fc00 00000000`475bfab4 smss!wmain+0x2f2
        00000000`0018fcf0 00000000`76dfb332
smss!NtProcessStartupW_AfterSecurityCookieInitialized+0x2fc
        00000000`0018fd80 00000000`00000000 ntdll!RtlUserThreadStart+0x29

        THREAD fffffa8003fab6b0  Cid 0184.01e8  Teb: 000007fffffdc000 Win32Thread: 0000000000000000
WAIT: (WrLpcReceive) UserMode Non-Alertable
            fffffa8003faba40  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8003f5b040       Image:         smss.exe
        Wait Start TickCount      1545           Ticks: 45034 (0:00:11:42.534)
        Context Switch Count      9
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address smss!SmpCreateInitialSession (0x00000000475bd9ec)
        Stack Init fffff98004feadb0 Current fffff98004fea7a0
        Base fffff98004feb000 Limit fffff98004fe5000 Call 0
        Priority 12 BasePriority 11 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`04fea7e0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`04fea920 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`04fea980 fffff800`01eb3788 nt!KeWaitForSingleObject+0x5f5
        fffff980`04feaa00 fffff800`01eb3eda nt!AlpcpReceiveMessagePort+0x298
        fffff980`04feaa60 fffff800`01eb74ba nt!AlpcpReceiveMessage+0x246
        fffff980`04feab00 fffff800`01c4d733 nt!NtAlpcSendWaitReceivePort+0x1da
        fffff980`04feabb0 00000000`76e20aca nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`04feac20)
        00000000`0046f998 00000000`475bb835 ntdll!NtAlpcSendWaitReceivePort+0xa
        00000000`0046f9a0 00000000`475bda8c smss!SmpApiLoop+0x149
        00000000`0046fc20 00000000`76dfb332 smss!SmpCreateInitialSession+0xa0
        00000000`0046fde0 00000000`00000000 ntdll!RtlUserThreadStart+0x29
```

```
        THREAD fffffa80038b5630  Cid 0184.01f4  Teb: 000007fffffda000 Win32Thread: 0000000000000000
WAIT: (WrLpcReceive) UserMode Non-Alertable
            fffffa80038b59c0  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8003f5b040       Image:         smss.exe
        Wait Start TickCount      1545           Ticks: 45034 (0:00:11:42.534)
        Context Switch Count      9
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address smss!SmpApiLoop (0x00000000475bb6ec)
        Stack Init fffff980044dddb0 Current fffff980044dd7a0
        Base fffff980044de000 Limit fffff980044d8000 Call 0
        Priority 12 BasePriority 11 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`044dd7e0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`044dd920 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`044dd980 fffff800`01eb3788 nt!KeWaitForSingleObject+0x5f5
        fffff980`044dda00 fffff800`01eb3eda nt!AlpcpReceiveMessagePort+0x298
        fffff980`044dda60 fffff800`01eb74ba nt!AlpcpReceiveMessage+0x246
        fffff980`044ddb00 fffff800`01c4d733 nt!NtAlpcSendWaitReceivePort+0x1da
        fffff980`044ddbb0 00000000`76e20aca nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`044ddc20)
        00000000`0062fb28 00000000`475bb835 ntdll!NtAlpcSendWaitReceivePort+0xa
        00000000`0062fb30 00000000`76dfb332 smss!SmpApiLoop+0x149
        00000000`0062fdb0 00000000`00000000 ntdll!RtlUserThreadStart+0x29

        THREAD fffffa8004065060  Cid 0184.0220  Teb: 000007fffffd8000 Win32Thread: 0000000000000000
WAIT: (WrLpcReceive) UserMode Non-Alertable
            fffffa80040653f0  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8003f5b040       Image:         smss.exe
        Wait Start TickCount      1546           Ticks: 45033 (0:00:11:42.519)
        Context Switch Count      76
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address smss!SmpCreateInitialSession (0x00000000475bd9ec)
        Stack Init fffff9800b3f8db0 Current fffff9800b3f87a0
        Base fffff9800b3f9000 Limit fffff9800b3f3000 Call 0
        Priority 12 BasePriority 11 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0b3f87e0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0b3f8920 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0b3f8980 fffff800`01eb3788 nt!KeWaitForSingleObject+0x5f5
        fffff980`0b3f8a00 fffff800`01eb3eda nt!AlpcpReceiveMessagePort+0x298
        fffff980`0b3f8a60 fffff800`01eb74ba nt!AlpcpReceiveMessage+0x246
        fffff980`0b3f8b00 fffff800`01c4d733 nt!NtAlpcSendWaitReceivePort+0x1da
        fffff980`0b3f8bb0 00000000`76e20aca nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0b3f8c20)
        00000000`0073f478 00000000`475bb835 ntdll!NtAlpcSendWaitReceivePort+0xa
        00000000`0073f480 00000000`475bda8c smss!SmpApiLoop+0x149
        00000000`0073f700 00000000`76dfb332 smss!SmpCreateInitialSession+0xa0
        00000000`0073f8c0 00000000`00000000 ntdll!RtlUserThreadStart+0x29
```

Csrss process (session 0)

```
PROCESS fffffa80040bc8e0
    SessionId: 0  Cid: 01f8    Peb: 7fffffd6000  ParentCid: 01ec
    DirBase: 55a93000  ObjectTable: fffff880050efdb0  HandleCount: 542.
    Image: csrss.exe
    VadRoot fffffa8004072130 Vads 106 Clone 0 Private 407. Modified 302. Locked 0.
    DeviceMap fffff88000007820
    Token                             fffff880050ef2c0
    ElapsedTime                       00:11:48.960
    UserTime                          00:00:00.000
    KernelTime                        00:00:01.950
    QuotaPoolUsage[PagedPool]         262568
    QuotaPoolUsage[NonPagedPool]      10208
    Working Set Sizes (now,min,max)  (1398, 50, 345) (5592KB, 200KB, 1380KB)
    PeakWorkingSetSize                1623
    VirtualSize                       110 Mb
    PeakVirtualSize                   116 Mb
    PageFaultCount                    3550
    MemoryPriority                    BACKGROUND
    BasePriority                      13
    CommitCharge                      603

    Setting context for this process...
.process /p /r fffffa80040bc8e0

    !peb
PEB at 000007fffffd6000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00000000499a0000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 0000000000272490 . 000000000029af20
    Ldr.InLoadOrderModuleList:           00000000002723a0 . 000000000029af00
    Ldr.InMemoryOrderModuleList:         00000000002723b0 . 000000000029af10
            Base TimeStamp                     Module
        499a0000 4549b4cc Nov 02 09:05:16 2006 C:\Windows\system32\csrss.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
     7fefd470000 45dfbfd9 Feb 24 04:32:25 2007 C:\Windows\system32\CSRSRV.dll
     7fefd450000 4549d24d Nov 02 11:11:09 2006 C:\Windows\system32\basesrv.dll
     7fefd3e0000 45dfc002 Feb 24 04:33:06 2007 C:\Windows\system32\winsrv.dll
        76d00000 45d3ee19 Feb 15 05:22:33 2007 C:\Windows\system32\USER32.dll
        76bc0000 4549d328 Nov 02 11:14:48 2006 C:\Windows\system32\KERNEL32.dll
     7fefec20000 4549d273 Nov 02 11:11:47 2006 C:\Windows\system32\GDI32.dll
     7fefea30000 4549d267 Nov 02 11:11:35 2006 C:\Windows\system32\ADVAPI32.dll
     7fefed90000 469c43bb Jul 17 05:21:15 2007 C:\Windows\system32\RPCRT4.dll
     7feff0c0000 4549d2a1 Nov 02 11:12:33 2006 C:\Windows\system32\LPK.DLL
     7fefd940000 4549d337 Nov 02 11:15:03 2006 C:\Windows\system32\USP10.dll
     7fefdd40000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\system32\msvcrt.dll
     7fefd1f0000 4549d32f Nov 02 11:14:55 2006 C:\Windows\system32\sxs.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       0000000000270000
    ProcessParameters: 0000000000271950
    WindowTitle:  '< Name not readable >'
    ImageFile:    'C:\Windows\system32\csrss.exe'
    CommandLine:  'C:\Windows\system32\csrss.exe ObjectDirectory=\Windows
SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1
ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2
ProfileControl=Off MaxRequestThreads=16'
    DllPath:      'C:\Windows\system32;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem'
    Environment:  0000000000271310
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
```

```
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\TEMP
        TMP=C:\Windows\TEMP
        USERNAME=SYSTEM
        windir=C:\Windows


        THREAD fffffa80041f2810  Cid 01f8.0210  Teb: 000007fffffdc000 Win32Thread: fffff900c07f6460
WAIT: (WrLpcReply) UserMode Non-Alertable
            fffffa80041f2ba0  Semaphore Limit 0x1
        Waiting for reply to ALPC Message fffff88002394350
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80040bc8e0       Image:         csrss.exe
        Wait Start TickCount      2941           Ticks: 43638 (0:00:11:20.757)
        Context Switch Count      9                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address winsrv!TerminalServerRequestThread (0x000007fefd3e9ad0)
        Stack Init fffff98012b0adb0 Current fffff98012b0a760
        Base fffff98012b0b000 Limit fffff98012b05000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`12b0a7a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12b0a8e0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`12b0a940 fffff800`01c8f857 nt!KeWaitForSingleObject+0x5f5
        fffff980`12b0a9c0 fffff800`01ebed64 nt!AlpcpSignalAndWait+0x97
        fffff980`12b0aa00 fffff800`01e9a80a nt!AlpcpReceiveSynchronousReply+0x44
        fffff980`12b0aa60 fffff800`01ea67b2 nt!AlpcpProcessSynchronousRequest+0x257
        fffff980`12b0ab80 fffff800`01e9ee9d nt!LpcpRequestWaitReplyPort+0x91
        fffff980`12b0abe0 fffff800`01c4d733 nt!NtRequestWaitReplyPort+0x6d
        fffff980`12b0ac20 00000000`76e2049a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12b0ac20)
        00000000`00ebf7e8 000007fe`fd3e9c40 ntdll!NtRequestWaitReplyPort+0xa
        00000000`00ebf7f0 00000000`76dfb332 winsrv!TerminalServerRequestThread+0x256
        00000000`00ebfa00 00000000`00000000 ntdll!RtlUserThreadStart+0x29
```

```
        THREAD fffffa80040aebb0  Cid 01f8.0214  Teb: 000007fffffda000 Win32Thread: fffff900c07bfd60
WAIT: (UserRequest) UserMode Alertable
            fffffa8003fce510  SynchronizationEvent
            fffffa8003fce5d0  SynchronizationEvent
            fffffa8003fce570  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80040bc8e0       Image:         csrss.exe
        Wait Start TickCount      1504           Ticks: 45075 (0:00:11:43.174)
        Context Switch Count      2                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address winsrv!NotificationThread (0x000007fefd3e9e20)
        Stack Init fffff9800d154db0 Current fffff9800d154260
        Base fffff9800d155000 Limit fffff9800d14f000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0d1542a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0d1543e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0d154440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0d1544b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0d154960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0d154bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0d154c20)
        00000000`00f1fb68 000007fe`fd3ea013 ntdll!NtWaitForMultipleObjects+0xa
        00000000`00f1fb70 00000000`76dfb332 winsrv!NotificationThread+0x1ee
        00000000`00f1fe80 00000000`00000000 ntdll!RtlUserThreadStart+0x29

        THREAD fffffa8003d7b060  Cid 01f8.0218  Teb: 000007fffffd8000 Win32Thread: fffff900c0092d60
WAIT: (WrLpcReceive) UserMode Non-Alertable
            fffffa8003d7b3f0  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80040bc8e0       Image:         csrss.exe
        Wait Start TickCount      46397          Ticks: 182 (0:00:00:02.839)
        Context Switch Count      1361                 LargeStack
        UserTime                  00:00:00.124
        KernelTime                00:00:00.078
        Win32 Start Address CSRSRV!CsrApiRequestThread (0x000007fefd475f8c)
        Stack Init fffff9800b23fdb0 Current fffff9800b23f7a0
        Base fffff9800b240000 Limit fffff9800b237000 Call 0
        Priority 15 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0b23f7e0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0b23f920 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0b23f980 fffff800`01eb3788 nt!KeWaitForSingleObject+0x5f5
        fffff980`0b23fa00 fffff800`01eb3eda nt!AlpcpReceiveMessagePort+0x298
        fffff980`0b23fa60 fffff800`01eb74ba nt!AlpcpReceiveMessage+0x246
        fffff980`0b23fb00 fffff800`01c4d733 nt!NtAlpcSendWaitReceivePort+0x1da
        fffff980`0b23fbb0 00000000`76e20aca nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0b23fc20)
        00000000`00a0f6d8 000007fe`fd4760d0 ntdll!NtAlpcSendWaitReceivePort+0xa
        00000000`00a0f6e0 00000000`76dfb332 CSRSRV!CsrApiRequestThread+0x144
        00000000`00a0f9e0 00000000`00000000 ntdll!RtlUserThreadStart+0x29
```

```
        THREAD fffffa800419fbb0  Cid 01f8.021c  Teb: 000007fffffd4000 Win32Thread: 0000000000000000
WAIT: (WrLpcReceive) UserMode Non-Alertable
            fffffa800419ff40  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80040bc8e0       Image:         csrss.exe
        Wait Start TickCount      1333           Ticks: 45246 (0:00:11:45.842)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address CSRSRV!CsrSbApiRequestThread (0x000007fefd47525c)
        Stack Init fffff9800b3eadb0 Current fffff9800b3ea7f0
        Base fffff9800b3eb000 Limit fffff9800b3e5000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0b3ea830 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0b3ea970 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0b3ea9d0 fffff800`01eb3788 nt!KeWaitForSingleObject+0x5f5
        fffff980`0b3eaa50 fffff800`01e7e523 nt!AlpcpReceiveMessagePort+0x298
        fffff980`0b3eaab0 fffff800`01e740d2 nt!AlpcpReceiveLegacyMessage+0x122
        fffff980`0b3eab50 fffff800`01e724bf nt!NtReplyWaitReceivePortEx+0xc1
        fffff980`0b3eabe0 fffff800`01c4d733 nt!NtReplyWaitReceivePort+0xf
        fffff980`0b3eac20 00000000`76e2032a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0b3eac20)
        00000000`0026fdd8 000007fe`fd4752a9 ntdll!NtReplyWaitReceivePort+0xa
        00000000`0026fde0 00000000`76dfb332 CSRSRV!CsrSbApiRequestThread+0x4d
        00000000`0026ff60 00000000`00000000 ntdll!RtlUserThreadStart+0x29

        THREAD fffffa8003fcd960  Cid 01f8.023c  Teb: 000007fffffde000 Win32Thread: fffff900c06ba6a0
WAIT: (WrLpcReceive) UserMode Non-Alertable
            fffffa8003fcdcf0  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80040bc8e0       Image:         csrss.exe
        Wait Start TickCount      46354          Ticks: 225 (0:00:00:03.510)
        Context Switch Count      1132                 LargeStack
        UserTime                  00:00:00.078
        KernelTime                00:00:00.109
        Win32 Start Address CSRSRV!CsrApiRequestThread (0x000007fefd475f8c)
        Stack Init fffff9800bb2edb0 Current fffff9800bb2e7a0
        Base fffff9800bb2f000 Limit fffff9800bb26000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0bb2e7e0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0bb2e920 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0bb2e980 fffff800`01eb3788 nt!KeWaitForSingleObject+0x5f5
        fffff980`0bb2ea00 fffff800`01eb3eda nt!AlpcpReceiveMessagePort+0x298
        fffff980`0bb2ea60 fffff800`01eb74ba nt!AlpcpReceiveMessage+0x246
        fffff980`0bb2eb00 fffff800`01c4d733 nt!NtAlpcSendWaitReceivePort+0x1da
        fffff980`0bb2ebb0 00000000`76e20aca nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0bb2ec20)
        00000000`001cfbb8 000007fe`fd4760d0 ntdll!NtAlpcSendWaitReceivePort+0xa
        00000000`001cfbc0 00000000`76dfb332 CSRSRV!CsrApiRequestThread+0x144
        00000000`001cfec0 00000000`00000000 ntdll!RtlUserThreadStart+0x29
```

```
        THREAD fffffa80040b1b10  Cid 01f8.024c  Teb: 000007fffffae000 Win32Thread: fffff900c00cb010
WAIT: (WrUserRequest) KernelMode Alertable
            fffffa8004088e20  SynchronizationEvent
            fffffa800409bca0  NotificationTimer
            fffffa8004099570  SynchronizationTimer
            fffff80001d7ba20  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80040bc8e0       Image:         csrss.exe
        Wait Start TickCount      46302          Ticks: 277 (0:00:00:04.321)
        Context Switch Count      97                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address winsrv!StartCreateSystemThreads (0x000007fefd3ec650)
        Stack Init fffff9800baf5db0 Current fffff9800baf58b0
        Base fffff9800baf6000 Limit fffff9800baf0000 Call 0
        Priority 15 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0baf58f0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0baf5a30 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0baf5a90 fffff960`000c1841 nt!KeWaitForMultipleObjects+0x703
        fffff980`0baf5b00 fffff960`00056838 win32k!RawInputThread+0x681
        fffff980`0baf5bc0 fffff960`000d1d80 win32k!xxxCreateSystemThreads+0x58
        fffff980`0baf5bf0 fffff800`01c4d733 win32k!NtUserCallNoParam+0x20
        fffff980`0baf5c20 000007fe`fd3ee02a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0baf5c20)
        00000000`0021fa28 000007fe`fd3ec669 winsrv!NtUserCallNoParam+0xa
        00000000`0021fa30 00000000`76dfb332 winsrv!StartCreateSystemThreads+0x19
        00000000`0021fa60 00000000`00000000 ntdll!RtlUserThreadStart+0x29

        THREAD fffffa80040b1660  Cid 01f8.0250  Teb: 000007fffffac000 Win32Thread: fffff900c00dea10
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa80041b1710  SynchronizationEvent
            fffffa8004097d30  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80040bc8e0       Image:         csrss.exe
        Wait Start TickCount      17281          Ticks: 29298 (0:00:07:37.051)
        Context Switch Count      26                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address winsrv!StartCreateSystemThreads (0x000007fefd3ec650)
        Stack Init fffff9800bb08db0 Current fffff9800bb08880
        Base fffff9800bb09000 Limit fffff9800bb03000 Call 0
        Priority 15 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0bb088c0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0bb08a00 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0bb08a60 fffff960`000996c3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0bb08ad0 fffff960`0009a531 win32k!xxxMsgWaitForMultipleObjects+0xf3
        fffff980`0bb08b50 fffff960`00056844 win32k!xxxDesktopThread+0x212
        fffff980`0bb08bc0 fffff960`000d1d80 win32k!xxxCreateSystemThreads+0x64
        fffff980`0bb08bf0 fffff800`01c4d733 win32k!NtUserCallNoParam+0x20
        fffff980`0bb08c20 000007fe`fd3ee02a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0bb08c20)
        00000000`00f9fb98 000007fe`fd3ec669 winsrv!NtUserCallNoParam+0xa
        00000000`00f9fba0 00000000`76dfb332 winsrv!StartCreateSystemThreads+0x19
        00000000`00f9fbd0 00000000`00000000 ntdll!RtlUserThreadStart+0x29
```

```
        THREAD fffffa80042a3060  Cid 01f8.0298  Teb: 000007fffffaa000 Win32Thread: fffff900c06c2d60
WAIT: (WrLpcReceive) UserMode Non-Alertable
            fffffa80042a33f0  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80040bc8e0       Image:         csrss.exe
        Wait Start TickCount      46371          Ticks: 208 (0:00:00:03.244)
        Context Switch Count      1065                 LargeStack
        UserTime                  00:00:00.031
        KernelTime                00:00:00.031
        Win32 Start Address CSRSRV!CsrApiRequestThread (0x000007fefd475f8c)
        Stack Init fffff9800bb8ddb0 Current fffff9800bb8d7a0
        Base fffff9800bb8e000 Limit fffff9800bb86000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0bb8d7e0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0bb8d920 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0bb8d980 fffff800`01eb3788 nt!KeWaitForSingleObject+0x5f5
        fffff980`0bb8da00 fffff800`01eb3eda nt!AlpcpReceiveMessagePort+0x298
        fffff980`0bb8da60 fffff800`01eb74ba nt!AlpcpReceiveMessage+0x246
        fffff980`0bb8db00 fffff800`01c4d733 nt!NtAlpcSendWaitReceivePort+0x1da
        fffff980`0bb8dbb0 00000000`76e20aca nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0bb8dc20)
        00000000`05e2fa88 000007fe`fd4760d0 ntdll!NtAlpcSendWaitReceivePort+0xa
        00000000`05e2fa90 00000000`76dfb332 CSRSRV!CsrApiRequestThread+0x144
        00000000`05e2fd90 00000000`00000000 ntdll!RtlUserThreadStart+0x29

        THREAD fffffa80042a3bb0  Cid 01f8.029c  Teb: 000007fffffa8000 Win32Thread: fffff900c06c0a60
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa8004298b10  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80040bc8e0       Image:         csrss.exe
        Wait Start TickCount      1364           Ticks: 45215 (0:00:11:45.358)
        Context Switch Count      4                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address winsrv!StartCreateSystemThreads (0x000007fefd3ec650)
        Stack Init fffff9800bb41db0 Current fffff9800bb41880
        Base fffff9800bb42000 Limit fffff9800bb3c000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0bb418c0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0bb41a00 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0bb41a60 fffff960`000996c3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0bb41ad0 fffff960`0009a531 win32k!xxxMsgWaitForMultipleObjects+0xf3
        fffff980`0bb41b50 fffff960`00056844 win32k!xxxDesktopThread+0x212
        fffff980`0bb41bc0 fffff960`000d1d80 win32k!xxxCreateSystemThreads+0x64
        fffff980`0bb41bf0 fffff800`01c4d733 win32k!NtUserCallNoParam+0x20
        fffff980`0bb41c20 000007fe`fd3ee02a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0bb41c20)
        00000000`05ddf9b8 000007fe`fd3ec669 winsrv!NtUserCallNoParam+0xa
        00000000`05ddf9c0 00000000`76dfb332 winsrv!StartCreateSystemThreads+0x19
        00000000`05ddf9f0 00000000`00000000 ntdll!RtlUserThreadStart+0x29
```

```
        THREAD fffffa80042aa060  Cid 01f8.02a0  Teb: 000007fffffa6000 Win32Thread: fffff900c06c07b0
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa80041a8220  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80040bc8e0       Image:         csrss.exe
        Wait Start TickCount      1364           Ticks: 45215 (0:00:11:45.358)
        Context Switch Count      6                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address winsrv!ConsoleInputThread (0x000007fefd3e3460)
        Stack Init fffff9800bb54db0 Current fffff9800bb54740
        Base fffff9800bb55000 Limit fffff9800bb4d000 Call 0
        Priority 15 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0bb54780 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0bb548c0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0bb54920 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`0bb549a0 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`0bb54a40 fffff960`000c7e1e win32k!xxxSleepThread+0x56
        fffff980`0bb54a70 fffff960`000c7f25 win32k!xxxRealInternalGetMessage+0x72e
        fffff980`0bb54b50 fffff960`000c97e4 win32k!xxxInternalGetMessage+0x35
        fffff980`0bb54b90 fffff800`01c4d733 win32k!NtUserGetMessage+0x64
        fffff980`0bb54c20 00000000`76d1e6aa nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0bb54c20)
        00000000`0602fa88 00000000`76d1e6ea USER32!ZwUserGetMessage+0xa
        00000000`0602fa90 000007fe`fd3e3566 USER32!GetMessageW+0x34
        00000000`0602fac0 00000000`76dfb332 winsrv!ConsoleInputThread+0x315
        00000000`0602fba0 00000000`00000000 ntdll!RtlUserThreadStart+0x29

        THREAD fffffa8004ac27f0  Cid 01f8.0990  Teb: 000007fffffa4000 Win32Thread: fffff900c2000590
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa8004b3f390  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80040bc8e0       Image:         csrss.exe
        Wait Start TickCount      2530           Ticks: 44049 (0:00:11:27.168)
        Context Switch Count      7                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address winsrv!ConsoleInputThread (0x000007fefd3e3460)
        Stack Init fffff9800db54db0 Current fffff9800db54740
        Base fffff9800db55000 Limit fffff9800db4d000 Call 0
        Priority 15 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0db54780 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0db548c0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0db54920 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`0db549a0 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`0db54a40 fffff960`000c7e1e win32k!xxxSleepThread+0x56
        fffff980`0db54a70 fffff960`000c7f25 win32k!xxxRealInternalGetMessage+0x72e
        fffff980`0db54b50 fffff960`000c97e4 win32k!xxxInternalGetMessage+0x35
        fffff980`0db54b90 fffff800`01c4d733 win32k!NtUserGetMessage+0x64
        fffff980`0db54c20 00000000`76d1e6aa nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0db54c20)
        00000000`067dfa38 00000000`76d1e6ea USER32!ZwUserGetMessage+0xa
        00000000`067dfa40 000007fe`fd3e3566 USER32!GetMessageW+0x34
        00000000`067dfa70 00000000`76dfb332 winsrv!ConsoleInputThread+0x315
        00000000`067dfb50 00000000`00000000 ntdll!RtlUserThreadStart+0x29
```

Csrss process (session 1)

```
PROCESS fffffa8003d72040
    SessionId: 1  Cid: 022c    Peb: 7fffffdc000  ParentCid: 0224
    DirBase: 545b3000  ObjectTable: fffff880051b9d80  HandleCount: 305.
    Image: csrss.exe
    VadRoot fffffa80041eaa90 Vads 94 Clone 0 Private 2283. Modified 2696. Locked 1875.
    DeviceMap fffff88000007820
    Token                             fffff88005767280
    ElapsedTime                       00:11:46.558
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.358
    QuotaPoolUsage[PagedPool]         243808
    QuotaPoolUsage[NonPagedPool]      11504
    Working Set Sizes (now,min,max)  (3521, 50, 345) (14084KB, 200KB, 1380KB)
    PeakWorkingSetSize                5450
    VirtualSize                       120 Mb
    PeakVirtualSize                   171 Mb
    PageFaultCount                    20629
    MemoryPriority                    BACKGROUND
    BasePriority                      13
    CommitCharge                      4358

    Setting context for this process...
.process /p /r fffffa8003d72040

    !peb
PEB at 000007fffffdc000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00000000499a0000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00000000002f2490 . 000000000031af00
    Ldr.InLoadOrderModuleList:           00000000002f23a0 . 000000000031aee0
    Ldr.InMemoryOrderModuleList:         00000000002f23b0 . 000000000031aef0
            Base TimeStamp                     Module
        499a0000 4549b4cc Nov 02 09:05:16 2006 C:\Windows\system32\csrss.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
     7fefd470000 45dfbfd9 Feb 24 04:32:25 2007 C:\Windows\system32\CSRSRV.dll
     7fefd450000 4549d24d Nov 02 11:11:09 2006 C:\Windows\system32\basesrv.dll
     7fefd3e0000 45dfc002 Feb 24 04:33:06 2007 C:\Windows\system32\winsrv.dll
        76d00000 45d3ee19 Feb 15 05:22:33 2007 C:\Windows\system32\USER32.dll
        76bc0000 4549d328 Nov 02 11:14:48 2006 C:\Windows\system32\KERNEL32.dll
     7fefec20000 4549d273 Nov 02 11:11:47 2006 C:\Windows\system32\GDI32.dll
     7fefea30000 4549d267 Nov 02 11:11:35 2006 C:\Windows\system32\ADVAPI32.dll
     7fefed90000 469c43bb Jul 17 05:21:15 2007 C:\Windows\system32\RPCRT4.dll
     7feff0c0000 4549d2a1 Nov 02 11:12:33 2006 C:\Windows\system32\LPK.DLL
     7fefd940000 4549d337 Nov 02 11:15:03 2006 C:\Windows\system32\USP10.dll
     7fefdd40000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\system32\msvcrt.dll
     7fefd1f0000 4549d32f Nov 02 11:14:55 2006 C:\Windows\system32\sxs.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       00000000002f0000
    ProcessParameters: 00000000002f1950
    WindowTitle:  '< Name not readable >'
    ImageFile:    'C:\Windows\system32\csrss.exe'
    CommandLine:  'C:\Windows\system32\csrss.exe ObjectDirectory=\Windows
SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1
ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2
ProfileControl=Off MaxRequestThreads=16'
    DllPath:      'C:\Windows\system32;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem'
    Environment:  00000000002f1310
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
```

```
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\TEMP
        TMP=C:\Windows\TEMP
        USERNAME=SYSTEM
        windir=C:\Windows


        THREAD fffffa80041b8480  Cid 022c.0264  Teb: 0000000000000000 Win32Thread: 0000000000000000
WAIT: (Executive) KernelMode Non-Alertable
            fffffa80041d7a60  SynchronizationEvent
            fffffa80041b8538  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8003d72040       Image:         csrss.exe
        Wait Start TickCount      46579          Ticks: 0
        Context Switch Count      14583
        UserTime                  00:00:00.000
        KernelTime                00:00:00.171
        Win32 Start Address cdd!PresentWorkerThread (0xfffff96000603c38)
        Stack Init fffff9800b39ddb0 Current fffff9800b39d9e0
        Base fffff9800b39e000 Limit fffff9800b398000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0b39da20 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0b39db60 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0b39dbc0 fffff960`006040ae nt!KeWaitForSingleObject+0x5f5
        fffff980`0b39dc40 fffff800`01ee196b cdd!PresentWorkerThread+0x476
        fffff980`0b39dd50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
        fffff980`0b39dd80 00000000`00000000 nt!KxStartSystemThread+0x16

        THREAD fffffa80041a7550  Cid 022c.026c  Teb: 000007fffffda000 Win32Thread: fffff900c06e6910
WAIT: (WrLpcReply) UserMode Non-Alertable
            fffffa80041a78e0  Semaphore Limit 0x1
        Waiting for reply to ALPC Message fffff880028ae870
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8003d72040       Image:         csrss.exe
        Wait Start TickCount      5138           Ticks: 41441 (0:00:10:46.483)
        Context Switch Count      29                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address winsrv!TerminalServerRequestThread (0x000007fefd3e9ad0)
        Stack Init fffff9800d1d9db0 Current fffff9800d1d9760
        Base fffff9800d1da000 Limit fffff9800d1d4000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0d1d97a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0d1d98e0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0d1d9940 fffff800`01c8f857 nt!KeWaitForSingleObject+0x5f5
        fffff980`0d1d99c0 fffff800`01ebed64 nt!AlpcpSignalAndWait+0x97
        fffff980`0d1d9a00 fffff800`01e9a80a nt!AlpcpReceiveSynchronousReply+0x44
        fffff980`0d1d9a60 fffff800`01ea67b2 nt!AlpcpProcessSynchronousRequest+0x257
        fffff980`0d1d9b80 fffff800`01e9ee9d nt!LpcpRequestWaitReplyPort+0x91
        fffff980`0d1d9be0 fffff800`01c4d733 nt!NtRequestWaitReplyPort+0x6d
        fffff980`0d1d9c20 00000000`76e2049a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0d1d9c20)
        00000000`0095f7f8 000007fe`fd3e9c40 ntdll!NtRequestWaitReplyPort+0xa
        00000000`0095f800 00000000`76dfb332 winsrv!TerminalServerRequestThread+0x256
        00000000`0095fa10 00000000`00000000 ntdll!RtlUserThreadStart+0x29
```

```
        THREAD fffffa8004209060  Cid 022c.0270  Teb: 000007fffffd8000 Win32Thread: fffff900c07fdd60
WAIT: (UserRequest) UserMode Alertable
            fffffa8003f539b0  SynchronizationEvent
            fffffa8003f53a70  SynchronizationEvent
            fffffa8003f53a10  SynchronizationEvent
            fffffa80041a83f0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8003d72040       Image:         csrss.exe
        Wait Start TickCount      2769           Ticks: 43810 (0:00:11:23.440)
        Context Switch Count      21                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address winsrv!NotificationThread (0x000007fefd3e9e20)
        Stack Init fffff9800d167db0 Current fffff9800d167260
        Base fffff9800d168000 Limit fffff9800d162000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0d1672a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0d1673e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0d167440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0d1674b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0d167960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0d167bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0d167c20)
        00000000`0234f878 000007fe`fd3ea013 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0234f880 00000000`76dfb332 winsrv!NotificationThread+0x1ee
        00000000`0234fb90 00000000`00000000 ntdll!RtlUserThreadStart+0x29

        THREAD fffffa8004209bb0  Cid 022c.0274  Teb: 000007fffffd6000 Win32Thread: fffff900c009dac0
WAIT: (WrLpcReceive) UserMode Non-Alertable
            fffffa8004209f40  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8003d72040       Image:         csrss.exe
        Wait Start TickCount      46084          Ticks: 495 (0:00:00:07.722)
        Context Switch Count      1334                 LargeStack
        UserTime                  00:00:00.140
        KernelTime                00:00:00.078
        Win32 Start Address CSRSRV!CsrApiRequestThread (0x000007fefd475f8c)
        Stack Init fffff9800bb1bdb0 Current fffff9800bb1b7a0
        Base fffff9800bb1c000 Limit fffff9800bb14000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0bb1b7e0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0bb1b920 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0bb1b980 fffff800`01eb3788 nt!KeWaitForSingleObject+0x5f5
        fffff980`0bb1ba00 fffff800`01eb3eda nt!AlpcpReceiveMessagePort+0x298
        fffff980`0bb1ba60 fffff800`01eb74ba nt!AlpcpReceiveMessage+0x246
        fffff980`0bb1bb00 fffff800`01c4d733 nt!NtAlpcSendWaitReceivePort+0x1da
        fffff980`0bb1bbb0 00000000`76e20aca nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0bb1bc20)
        00000000`023cfbe8 000007fe`fd4760d0 ntdll!NtAlpcSendWaitReceivePort+0xa
        00000000`023cfbf0 00000000`76dfb332 CSRSRV!CsrApiRequestThread+0x144
        00000000`023cfef0 00000000`00000000 ntdll!RtlUserThreadStart+0x29
```

```
        THREAD fffffa8004209700  Cid 022c.0278  Teb: 000007fffffd4000 Win32Thread: 0000000000000000
WAIT: (WrLpcReceive) UserMode Non-Alertable
            fffffa8004209a90  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8003d72040       Image:         csrss.exe
        Wait Start TickCount      1361           Ticks: 45218 (0:00:11:45.405)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address CSRSRV!CsrSbApiRequestThread (0x000007fefd47525c)
        Stack Init fffff9800b3c0db0 Current fffff9800b3c07f0
        Base fffff9800b3c1000 Limit fffff9800b3bb000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0b3c0830 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0b3c0970 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0b3c09d0 fffff800`01eb3788 nt!KeWaitForSingleObject+0x5f5
        fffff980`0b3c0a50 fffff800`01e7e523 nt!AlpcpReceiveMessagePort+0x298
        fffff980`0b3c0ab0 fffff800`01e740d2 nt!AlpcpReceiveLegacyMessage+0x122
        fffff980`0b3c0b50 fffff800`01e724bf nt!NtReplyWaitReceivePortEx+0xc1
        fffff980`0b3c0be0 fffff800`01c4d733 nt!NtReplyWaitReceivePort+0xf
        fffff980`0b3c0c20 00000000`76e2032a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0b3c0c20)
        00000000`00ddf828 000007fe`fd4752a9 ntdll!NtReplyWaitReceivePort+0xa
        00000000`00ddf830 00000000`76dfb332 CSRSRV!CsrSbApiRequestThread+0x4d
        00000000`00ddf9b0 00000000`00000000 ntdll!RtlUserThreadStart+0x29

        THREAD fffffa800429a560  Cid 022c.028c  Teb: 000007fffffde000 Win32Thread: fffff900c06e26c0
WAIT: (WrLpcReceive) UserMode Non-Alertable
            fffffa800429a8f0  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8003d72040       Image:         csrss.exe
        Wait Start TickCount      46518          Ticks: 61 (0:00:00:00.951)
        Context Switch Count      1534                 LargeStack
        UserTime                  00:00:00.187
        KernelTime                00:00:00.156
        Win32 Start Address CSRSRV!CsrApiRequestThread (0x000007fefd475f8c)
        Stack Init fffff98010652db0 Current fffff980106527a0
        Base fffff98010653000 Limit fffff9801064b000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`106527e0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`10652920 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`10652980 fffff800`01eb3788 nt!KeWaitForSingleObject+0x5f5
        fffff980`10652a00 fffff800`01eb3eda nt!AlpcpReceiveMessagePort+0x298
        fffff980`10652a60 fffff800`01eb74ba nt!AlpcpReceiveMessage+0x246
        fffff980`10652b00 fffff800`01c4d733 nt!NtAlpcSendWaitReceivePort+0x1da
        fffff980`10652bb0 00000000`76e20aca nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`10652c20)
        00000000`026dfbd8 000007fe`fd4760d0 ntdll!NtAlpcSendWaitReceivePort+0xa
        00000000`026dfbe0 00000000`76dfb332 CSRSRV!CsrApiRequestThread+0x144
        00000000`026dfee0 00000000`00000000 ntdll!RtlUserThreadStart+0x29
```

```
        THREAD fffffa80042b0bb0  Cid 022c.02a8  Teb: 000007fffffae000 Win32Thread: fffff900c00fe010
WAIT: (WrUserRequest) KernelMode Alertable
            fffffa80042a91d0  SynchronizationEvent
            fffffa80042969d0  NotificationTimer
            fffffa80042087e0  SynchronizationTimer
            fffffa8003d72e10  SynchronizationEvent
        IRP List:
            fffffa800260d820: (0006,0358) Flags: 00060970  Mdl: 00000000
            fffffa80041c75d0: (0006,03a0) Flags: 00060970  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8003d72040       Image:         csrss.exe
        Wait Start TickCount      46573          Ticks: 6 (0:00:00:00.093)
        Context Switch Count      32479                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.405
        Win32 Start Address winsrv!StartCreateSystemThreads (0x000007fefd3ec650)
        Stack Init fffff9800bb7adb0 Current fffff9800bb7a8b0
        Base fffff9800bb7b000 Limit fffff9800bb75000 Call 0
        Priority 15 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0bb7a8f0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0bb7aa30 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0bb7aa90 fffff960`000c1841 nt!KeWaitForMultipleObjects+0x703
        fffff980`0bb7ab00 fffff960`00056838 win32k!RawInputThread+0x681
        fffff980`0bb7abc0 fffff960`000d1d80 win32k!xxxCreateSystemThreads+0x58
        fffff980`0bb7abf0 fffff800`01c4d733 win32k!NtUserCallNoParam+0x20
        fffff980`0bb7ac20 000007fe`fd3ee02a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0bb7ac20)
        00000000`0246fd48 000007fe`fd3ec669 winsrv!NtUserCallNoParam+0xa
        00000000`0246fd50 00000000`76dfb332 winsrv!StartCreateSystemThreads+0x19
        00000000`0246fd80 00000000`00000000 ntdll!RtlUserThreadStart+0x29

        THREAD fffffa800431e060  Cid 022c.02d0  Teb: 000007fffffac000 Win32Thread: fffff900c00fd3d0
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa8004099980  SynchronizationEvent
            fffffa800431f310  SynchronizationEvent
        IRP List:
            fffffa8002216c60: (0006,03a0) Flags: 00060970  Mdl: 00000000
            fffffa8003faec60: (0006,03a0) Flags: 00060970  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8003d72040       Image:         csrss.exe
        Wait Start TickCount      45975          Ticks: 604 (0:00:00:09.422)
        Context Switch Count      9737                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.421
        Win32 Start Address winsrv!StartCreateSystemThreads (0x000007fefd3ec650)
        Stack Init fffff9800bbffdb0 Current fffff9800bbff880
        Base fffff9800bc00000 Limit fffff9800bbfa000 Call 0
        Priority 15 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0bbff8c0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0bbffa00 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0bbffa60 fffff960`000996c3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0bbffad0 fffff960`0009a531 win32k!xxxMsgWaitForMultipleObjects+0xf3
        fffff980`0bbffb50 fffff960`00056844 win32k!xxxDesktopThread+0x212
        fffff980`0bbffbc0 fffff960`000d1d80 win32k!xxxCreateSystemThreads+0x64
        fffff980`0bbffbf0 fffff800`01c4d733 win32k!NtUserCallNoParam+0x20
        fffff980`0bbffc20 000007fe`fd3ee02a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0bbffc20)
        00000000`0240f7c8 000007fe`fd3ec669 winsrv!NtUserCallNoParam+0xa
        00000000`0240f7d0 00000000`76dfb332 winsrv!StartCreateSystemThreads+0x19
        00000000`0240f800 00000000`00000000 ntdll!RtlUserThreadStart+0x29
```

```
        THREAD fffffa8004bf6ac0  Cid 022c.0aa4  Teb: 000007fffffaa000 Win32Thread: fffff900c1c3fd60
WAIT: (WrLpcReceive) UserMode Non-Alertable
            fffffa8004bf6e50  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8003d72040       Image:         csrss.exe
        Wait Start TickCount      46196          Ticks: 383 (0:00:00:05.974)
        Context Switch Count      1197                 LargeStack
        UserTime                  00:00:00.078
        KernelTime                00:00:00.109
        Win32 Start Address CSRSRV!CsrApiRequestThread (0x000007fefd475f8c)
        Stack Init fffff98012f8fdb0 Current fffff98012f8f7a0
        Base fffff98012f90000 Limit fffff98012f88000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`12f8f7e0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12f8f920 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`12f8f980 fffff800`01eb3788 nt!KeWaitForSingleObject+0x5f5
        fffff980`12f8fa00 fffff800`01eb3eda nt!AlpcpReceiveMessagePort+0x298
        fffff980`12f8fa60 fffff800`01eb74ba nt!AlpcpReceiveMessage+0x246
        fffff980`12f8fb00 fffff800`01c4d733 nt!NtAlpcSendWaitReceivePort+0x1da
        fffff980`12f8fbb0 00000000`76e20aca nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12f8fc20)
        00000000`06cdfc78 000007fe`fd4760d0 ntdll!NtAlpcSendWaitReceivePort+0xa
        00000000`06cdfc80 00000000`76dfb332 CSRSRV!CsrApiRequestThread+0x144
        00000000`06cdff80 00000000`00000000 ntdll!RtlUserThreadStart+0x29
```

Wininit process

```
PROCESS fffffa8003f56ad0
    SessionId: 0  Cid: 0234    Peb: 7fffffdb000  ParentCid: 01ec
    DirBase: 5461a000  ObjectTable: fffff880051c3fa0  HandleCount:  98.
    Image: wininit.exe
    VadRoot fffffa8003d72e40 Vads 60 Clone 0 Private 321. Modified 187. Locked 2.
    DeviceMap fffff88000007820
    Token                             fffff880056b36b0
    ElapsedTime                       00:11:46.542
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.390
    QuotaPoolUsage[PagedPool]         117440
    QuotaPoolUsage[NonPagedPool]      8192
    Working Set Sizes (now,min,max)  (959, 50, 345) (3836KB, 200KB, 1380KB)
    PeakWorkingSetSize                1215
    VirtualSize                       55 Mb
    PeakVirtualSize                   57 Mb
    PageFaultCount                    1690
    MemoryPriority                    BACKGROUND
    BasePriority                      13
    CommitCharge                      433

    Setting context for this process...
.process /p /r fffffa8003f56ad0

    !peb
PEB at 000007fffffdb000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00000000ff060000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00000000001f2290 . 000000000021c3e0
    Ldr.InLoadOrderModuleList:           00000000001f21a0 . 000000000021c560
    Ldr.InMemoryOrderModuleList:         00000000001f21b0 . 000000000021c570
            Base TimeStamp                     Module
        ff060000 4549b9f0 Nov 02 09:27:12 2006 C:\Windows\system32\wininit.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        76bc0000 4549d328 Nov 02 11:14:48 2006 C:\Windows\system32\kernel32.dll
     7fefea30000 4549d267 Nov 02 11:11:35 2006 C:\Windows\system32\ADVAPI32.dll
     7fefed90000 469c43bb Jul 17 05:21:15 2007 C:\Windows\system32\RPCRT4.dll
        76d00000 45d3ee19 Feb 15 05:22:33 2007 C:\Windows\system32\USER32.dll
     7fefec20000 4549d273 Nov 02 11:11:47 2006 C:\Windows\system32\GDI32.dll
     7fefdd40000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\system32\msvcrt.dll
     7fefd3b0000 4549d336 Nov 02 11:15:02 2006 C:\Windows\system32\USERENV.dll
     7fefd390000 4549d33f Nov 02 11:15:11 2006 C:\Windows\system32\Secur32.dll
     7fefd9e0000 4549d2cb Nov 02 11:13:15 2006 C:\Windows\system32\IMM32.DLL
     7fefdc30000 4549d2e6 Nov 02 11:13:42 2006 C:\Windows\system32\MSCTF.dll
     7feff0c0000 4549d2a1 Nov 02 11:12:33 2006 C:\Windows\system32\LPK.DLL
     7fefd940000 4549d337 Nov 02 11:15:03 2006 C:\Windows\system32\USP10.dll
     7fefd310000 4549d247 Nov 02 11:11:03 2006 C:\Windows\system32\apphelp.dll
     7fefd540000 4549d38a Nov 02 11:16:26 2006 C:\Windows\system32\WS2_32.dll
     7feff0b0000 4549d370 Nov 02 11:16:00 2006 C:\Windows\system32\NSI.dll
     7fefc8f0000 4549d2e7 Nov 02 11:13:43 2006 C:\Windows\system32\mswsock.dll
     7fefc560000 4549d3a3 Nov 02 11:16:51 2006 C:\Windows\system32\wshtcpip.dll
     7fefc980000 4549d39d Nov 02 11:16:45 2006 C:\Windows\System32\wship6.dll
     7fefca40000 4549d341 Nov 02 11:15:13 2006 C:\Windows\system32\credssp.dll
     7fefcc50000 4549d344 Nov 02 11:15:16 2006 C:\Windows\system32\CRYPT32.dll
     7fefce00000 4549d2df Nov 02 11:13:35 2006 C:\Windows\system32\MSASN1.dll
     7fefc670000 4549d321 Nov 02 11:14:41 2006 C:\Windows\system32\schannel.dll
     7fefcf70000 4549d2fc Nov 02 11:14:04 2006 C:\Windows\system32\NETAPI32.dll
     7fefd530000 4549d310 Nov 02 11:14:24 2006 C:\Windows\system32\PSAPI.DLL
    SubSystemData:     0000000000000000
    ProcessHeap:       00000000001f0000
    ProcessParameters: 00000000001f1950
```

```
    WindowTitle:  '< Name not readable >'
    ImageFile:    'C:\Windows\system32\wininit.exe'
    CommandLine:  'wininit.exe'
    DllPath:      'C:\Windows\system32;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem'
    Environment:  00000000002292b0
        ALLUSERSPROFILE=C:\ProgramData
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\TEMP
        TMP=C:\Windows\TEMP
        USERNAME=SYSTEM
        USERPROFILE=C:\Windows\system32\config\systemprofile
        windir=C:\Windows


        THREAD fffffa8003f56640  Cid 0234.0238  Teb: 000007fffffde000 Win32Thread: fffff900c00a65f0
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800409b620  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8003f56ad0       Image:         wininit.exe
        Wait Start TickCount      1388           Ticks: 45191 (0:00:11:44.984)
        Context Switch Count      2075                 LargeStack
        UserTime                  00:00:00.015
        KernelTime                00:00:00.218
        Win32 Start Address wininit!WinMainCRTStartup (0x00000000ff077c34)
        Stack Init fffff9800bae2db0 Current fffff9800bae2960
        Base fffff9800bae3000 Limit fffff9800bad8000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0bae29a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0bae2ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0bae2b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0bae2bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0bae2c20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0bae2c20)
        00000000`000af8f8 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`000af900 00000000`ff066779 kernel32!WaitForSingleObjectEx+0x9c
        00000000`000af9c0 00000000`ff077a8b wininit!WinMain+0xd8d
        00000000`000afb00 00000000`76bfcdcd wininit!LsaGetUserName+0x1eb
        00000000`000afbc0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`000afbf0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80041a7060  Cid 0234.0268  Teb: 000007fffffd5000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa800422aef0  SynchronizationTimer
            fffffa80041a2b50  ProcessObject
            fffffa8004298550  ProcessObject
            fffffa80042a4c10  ProcessObject
            fffffa80042b3930  SynchronizationTimer
            fffffa800435fef0  SynchronizationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8003f56ad0       Image:         wininit.exe
        Wait Start TickCount      2030           Ticks: 44549 (0:00:11:34.968)
        Context Switch Count      8
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x0000000076df6930)
        Stack Init fffff9800b3a4db0 Current fffff9800b3a4260
        Base fffff9800b3a5000 Limit fffff9800b39f000 Call 0
        Priority 15 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0b3a42a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0b3a43e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0b3a4440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0b3a44b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0b3a4960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0b3a4bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0b3a4c20)
        00000000`02fbf868 00000000`76df6b07 ntdll!NtWaitForMultipleObjects+0xa
        00000000`02fbf870 00000000`76bfcdcd ntdll!TppWaiterpThread+0x14d
        00000000`02fbfb10 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02fbfb40 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004063060  Cid 0234.0b90  Teb: 000007fffffd9000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8003d7bcc0  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8003f56ad0       Image:         wininit.exe
        Wait Start TickCount      5394           Ticks: 41185 (0:00:10:42.490)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff9800b396db0 Current fffff9800b396810
        Base fffff9800b397000 Limit fffff9800b391000 Call 0
        Priority 13 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0b396850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0b396990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0b3969f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0b396a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`0b396b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`0b396bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0b396c20)
        00000000`001bf8a8 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`001bf8b0 000007fe`fedce7a3 kernel32!GetQueuedCompletionStatus+0x48
        00000000`001bf910 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`001bf9a0 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`001bfa50 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`001bfa80 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`001bfac0 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`001bfaf0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`001bfb20 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

Services process

```
PROCESS fffffa80041a2b50
    SessionId: 0  Cid: 025c    Peb: 7fffffd4000  ParentCid: 0234
    DirBase: 53755000  ObjectTable: fffff880051b8b00  HandleCount: 247.
    Image: services.exe
    VadRoot fffffa80040b0c30 Vads 84 Clone 0 Private 646. Modified 906. Locked 2.
    DeviceMap fffff88000007820
    Token                             fffff880055faac0
    ElapsedTime                       00:11:46.183
    UserTime                          00:00:00.140
    KernelTime                        00:00:02.418
    QuotaPoolUsage[PagedPool]         125456
    QuotaPoolUsage[NonPagedPool]      13744
    Working Set Sizes (now,min,max)  (1898, 50, 345) (7592KB, 200KB, 1380KB)
    PeakWorkingSetSize                2241
    VirtualSize                       54 Mb
    PeakVirtualSize                   85 Mb
    PageFaultCount                    9009
    MemoryPriority                    BACKGROUND
    BasePriority                      9
    CommitCharge                      817

    Setting context for this process...
.process /p /r fffffa80041a2b50

    !peb
PEB at 000007fffffd4000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00000000ff310000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 0000000000152640 . 0000000002bc2460
    Ldr.InLoadOrderModuleList:           0000000000152550 . 0000000002bc2440
    Ldr.InMemoryOrderModuleList:         0000000000152560 . 0000000002bc2450
            Base TimeStamp                     Module
        ff310000 4549b60a Nov 02 09:10:34 2006 C:\Windows\system32\services.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        76bc0000 4549d328 Nov 02 11:14:48 2006 C:\Windows\system32\kernel32.dll
     7fefea30000 4549d267 Nov 02 11:11:35 2006 C:\Windows\system32\ADVAPI32.dll
     7fefed90000 469c43bb Jul 17 05:21:15 2007 C:\Windows\system32\RPCRT4.dll
        76d00000 45d3ee19 Feb 15 05:22:33 2007 C:\Windows\system32\USER32.dll
     7fefec20000 4549d273 Nov 02 11:11:47 2006 C:\Windows\system32\GDI32.dll
     7fefdd40000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\system32\msvcrt.dll
     7fefd3b0000 4549d336 Nov 02 11:15:02 2006 C:\Windows\system32\USERENV.dll
     7fefd390000 4549d33f Nov 02 11:15:11 2006 C:\Windows\system32\Secur32.dll
     7fefd2a0000 4549d31f Nov 02 11:14:39 2006 C:\Windows\system32\SCESRV.dll
     7fefd360000 4549d265 Nov 02 11:11:33 2006 C:\Windows\system32\AUTHZ.dll
     7fefcf70000 4549d2fc Nov 02 11:14:04 2006 C:\Windows\system32\NETAPI32.dll
     7fefd530000 4549d310 Nov 02 11:14:24 2006 C:\Windows\system32\PSAPI.DLL
     7fefcea0000 4549d2ef Nov 02 11:13:51 2006 C:\Windows\system32\NCObjAPI.DLL
     7fefd9e0000 4549d2cb Nov 02 11:13:15 2006 C:\Windows\system32\IMM32.DLL
     7fefdc30000 4549d2e6 Nov 02 11:13:42 2006 C:\Windows\system32\MSCTF.dll
     7feff0c0000 4549d2a1 Nov 02 11:12:33 2006 C:\Windows\system32\LPK.DLL
     7fefd940000 4549d337 Nov 02 11:15:03 2006 C:\Windows\system32\USP10.dll
     7fefca40000 4549d341 Nov 02 11:15:13 2006 C:\Windows\system32\credssp.dll
     7fefcc50000 4549d344 Nov 02 11:15:16 2006 C:\Windows\system32\CRYPT32.dll
     7fefce00000 4549d2df Nov 02 11:13:35 2006 C:\Windows\system32\MSASN1.dll
     7fefc670000 4549d321 Nov 02 11:14:41 2006 C:\Windows\system32\schannel.dll
     7fefd310000 4549d247 Nov 02 11:11:03 2006 C:\Windows\system32\apphelp.dll
     7fefc5b0000 4549d384 Nov 02 11:16:20 2006 C:\Windows\system32\NTMARTA.DLL
     7fefd590000 4549d396 Nov 02 11:16:38 2006 C:\Windows\system32\WLDAP32.dll
     7fefd540000 4549d38a Nov 02 11:16:26 2006 C:\Windows\system32\WS2_32.dll
     7feff0b0000 4549d370 Nov 02 11:16:00 2006 C:\Windows\system32\NSI.dll
     7fefce20000 4549d315 Nov 02 11:14:29 2006 C:\Windows\system32\SAMLIB.dll
```

```
     7fefd760000 4549d317 Nov 02 11:14:31 2006 C:\Windows\system32\ole32.dll
     7fefbe70000 4549d32b Nov 02 11:14:51 2006 C:\Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_1559f1c6f365a7fa\Comctl32.dll
     7fefda10000 4549d31f Nov 02 11:14:39 2006 C:\Windows\system32\SHLWAPI.dll
     7fefc8f0000 4549d2e7 Nov 02 11:13:43 2006 C:\Windows\system32\mswsock.dll
     7fefc560000 4549d3a3 Nov 02 11:16:51 2006 C:\Windows\system32\wshtcpip.dll
     7fefc980000 4549d39d Nov 02 11:16:45 2006 C:\Windows\System32\wship6.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       0000000000150000
    ProcessParameters: 0000000000151bf0
    WindowTitle:  'C:\Windows\system32\services.exe'
    ImageFile:    'C:\Windows\system32\services.exe'
    CommandLine:  'C:\Windows\system32\services.exe'
    DllPath:
'C:\Windows\system32;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Wind
ows;C:\Windows\System32\Wbem'
    Environment:  0000000002bcc080
        ALLUSERSPROFILE=C:\ProgramData
        commonfiles=C:\Program Files\Common Files
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        progfiles=C:\Program Files
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public
        systemdir=C:\Windows\system32
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\TEMP
        TMP=C:\Windows\TEMP
        USERNAME=SYSTEM
        USERPROFILE=C:\Windows\system32\config\systemprofile
        windir=C:\Windows
```

```
        THREAD fffffa80043948b0  Cid 025c.02f8  Teb: 000007fffffdc000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa80043dfc00  SynchronizationTimer
            fffffa8004394e80  SynchronizationEvent
            fffffa8004297040  ProcessObject
            fffffa80042d1c10  ProcessObject
            fffffa80044c0040  ProcessObject
            fffffa80044ff040  ProcessObject
            fffffa8004484c10  ProcessObject
            fffffa80044d9c10  ProcessObject
            fffffa80044fbc10  ProcessObject
            fffffa80045c38c0  ProcessObject
            fffffa8004567c10  ProcessObject
            fffffa800461e270  ProcessObject
            fffffa8004622180  ProcessObject
            fffffa8004a2fc10  ProcessObject
            fffffa800475d280  ProcessObject
            fffffa8004a31c10  ProcessObject
            fffffa80047fb780  ProcessObject
            fffffa800480ab70  ProcessObject
            fffffa8004812870  ProcessObject
            fffffa800486c230  ProcessObject
            fffffa8002004c10  ProcessObject
            fffffa8002043c10  ProcessObject
            fffffa80042b0240  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80041a2b50       Image:         services.exe
        Wait Start TickCount      15092          Ticks: 31487 (0:00:08:11.200)
        Context Switch Count      34
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x0000000076df6930)
        Stack Init fffff9800b68ddb0 Current fffff9800b68d260
        Base fffff9800b68e000 Limit fffff9800b688000 Call 0
        Priority 11 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0b68d2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0b68d3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0b68d440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0b68d4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0b68d960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0b68dbb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0b68dc20)
        00000000`00fffb08 00000000`76df6b07 ntdll!NtWaitForMultipleObjects+0xa
        00000000`00fffb10 00000000`76bfcdcd ntdll!TppWaiterpThread+0x14d
        00000000`00fffdb0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`00fffde0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8001f93700  Cid 025c.0df0  Teb: 000007fffffd6000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa80018a2240  NotificationEvent
            fffffa80018b3490  NotificationEvent
        IRP List:
            fffffa8001f93580: (0006,0118) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80041a2b50       Image:         services.exe
        Wait Start TickCount      7770           Ticks: 38809 (0:00:10:05.424)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address NCObjAPI!CNamedPipeClient::CallbackListenThreadProc
(0x000007fefcea50b0)
        Stack Init fffff9800b6e1db0 Current fffff9800b6e1260
        Base fffff9800b6e2000 Limit fffff9800b6dc000 Call 0
        Priority 11 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0b6e12a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0b6e13e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0b6e1440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0b6e14b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0b6e1960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0b6e1bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0b6e1c20)
        00000000`0169f548 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0169f550 000007fe`fcea517a kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0169f660 00000000`76bfcdcd
NCObjAPI!CNamedPipeClient::CallbackListenThreadProc+0xc6
        00000000`0169ff00 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0169ff30 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80020b9bb0  Cid 025c.0df8  Teb: 000007fffff9e000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004385040  NotificationEvent
            fffffa8004394f30  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80041a2b50       Image:         services.exe
        Wait Start TickCount      16242          Ticks: 30337 (0:00:07:53.260)
        Context Switch Count      16
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address NCObjAPI!CConnection::SendThreadProc (0x000007fefcea20c0)
        Stack Init fffff980103c7db0 Current fffff980103c7260
        Base fffff980103c8000 Limit fffff980103c2000 Call 0
        Priority 10 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`103c72a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`103c73e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`103c7440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`103c74b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`103c7960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`103c7bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`103c7c20)
        00000000`0261fa38 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0261fa40 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0261fb50 000007fe`fcea2161 kernel32!WaitForMultipleObjects+0x11
        00000000`0261fb90 00000000`76bfcdcd NCObjAPI!CConnection::SendThreadProc+0xa1
        00000000`0261fc60 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0261fc90 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8001e6a8f0  Cid 025c.0fdc  Teb: 000007fffffde000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Alertable
            fffffa80043c4040  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80041a2b50       Image:         services.exe
        Wait Start TickCount      9345           Ticks: 37234 (0:00:09:40.854)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x0000000076e17860)
        Stack Init fffff9801a6c2db0 Current fffff9801a6c2860
        Base fffff9801a6c3000 Limit fffff9801a6bd000 Call 0
        Priority 10 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1a6c28a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1a6c29e0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`1a6c2a40 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`1a6c2ad0 fffff800`01c8a722 nt!IoRemoveIoCompletion+0x47
        fffff980`1a6c2b50 fffff800`01c4d733 nt!NtWaitForWorkViaWorkerFactory+0x1f1
        fffff980`1a6c2c20 00000000`76e21b4a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1a6c2c20)
        00000000`02baf588 00000000`76e17a20 ntdll!NtWaitForWorkViaWorkerFactory+0xa
        00000000`02baf590 00000000`76bfcdcd ntdll!TppWorkerThread+0x23e
        00000000`02baf800 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02baf830 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80024f2590  Cid 025c.0acc  Teb: 000007fffffda000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8004395150  QueueObject
            fffffa80024f2648  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80041a2b50       Image:         services.exe
        Wait Start TickCount      46323          Ticks: 256 (0:00:00:03.993)
        Context Switch Count      51
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff980107f6db0 Current fffff980107f6810
        Base fffff980107f7000 Limit fffff980107f1000 Call 0
        Priority 11 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`107f6850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`107f6990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`107f69f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`107f6a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`107f6b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`107f6bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`107f6c20)
        00000000`0172f678 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`0172f680 000007fe`fedce7a3 kernel32!GetQueuedCompletionStatus+0x48
        00000000`0172f6e0 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`0172f770 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`0172f820 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`0172f850 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`0172f890 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`0172f8c0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0172f8f0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004482060  Cid 025c.0d78  Teb: 000007fffffd8000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8004395150  QueueObject
            fffffa8004482118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80041a2b50       Image:         services.exe
        Wait Start TickCount      45955          Ticks: 624 (0:00:00:09.734)
        Context Switch Count      23
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff98020c6ddb0 Current fffff98020c6d810
        Base fffff98020c6e000 Limit fffff98020c68000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`20c6d850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`20c6d990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`20c6d9f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`20c6da80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`20c6db00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`20c6dbb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`20c6dc20)
        00000000`024dfc68 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`024dfc70 000007fe`fedce7a3 kernel32!GetQueuedCompletionStatus+0x48
        00000000`024dfcd0 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`024dfd60 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`024dfe10 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`024dfe40 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`024dfe80 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`024dfeb0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`024dfee0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8002424700  Cid 025c.0fd8  Teb: 000007fffffae000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8004395150  QueueObject
            fffffa80024247b8  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80041a2b50       Image:         services.exe
        Wait Start TickCount      45955          Ticks: 624 (0:00:00:09.734)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff98004fdcdb0 Current fffff98004fdc810
        Base fffff98004fdd000 Limit fffff98004fd7000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`04fdc850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`04fdc990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`04fdc9f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`04fdca80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`04fdcb00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`04fdcbb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`04fdcc20)
        00000000`026bf878 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`026bf880 000007fe`fedce7a3 kernel32!GetQueuedCompletionStatus+0x48
        00000000`026bf8e0 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`026bf970 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`026bfa20 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`026bfa50 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`026bfa90 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`026bfac0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`026bfaf0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

Lsass process

```
PROCESS fffffa8004298550
    SessionId: 0  Cid: 027c    Peb: 7fffffde000  ParentCid: 0234
    DirBase: 52637000  ObjectTable: fffff880056ae3f0  HandleCount: 661.
    Image: lsass.exe
    VadRoot fffffa80042950b0 Vads 129 Clone 0 Private 1022. Modified 1324. Locked 3.
    DeviceMap fffff88000007820
    Token                             fffff88005843580
    ElapsedTime                       00:11:46.105
    UserTime                          00:00:01.045
    KernelTime                        00:00:00.499
    QuotaPoolUsage[PagedPool]         144456
    QuotaPoolUsage[NonPagedPool]      24560
    Working Set Sizes (now,min,max)  (440, 50, 345) (1760KB, 200KB, 1380KB)
    PeakWorkingSetSize                2962
    VirtualSize                       68 Mb
    PeakVirtualSize                   71 Mb
    PageFaultCount                    4980
    MemoryPriority                    BACKGROUND
    BasePriority                      9
    CommitCharge                      1274

    Setting context for this process...
.process /p /r fffffa8004298550

    !peb
PEB at 000007fffffde000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00000000ffa60000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00000000003f2620 . 00000000027f58e0
    Ldr.InLoadOrderModuleList:           00000000003f2530 . 00000000027f58c0
    Ldr.InMemoryOrderModuleList:         00000000003f2540 . 00000000027f58d0
            Base TimeStamp                     Module
        ffa60000 4549b97f Nov 02 09:25:19 2006 C:\Windows\system32\lsass.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        76bc0000 4549d328 Nov 02 11:14:48 2006 C:\Windows\system32\kernel32.dll
     7fefea30000 4549d267 Nov 02 11:11:35 2006 C:\Windows\system32\ADVAPI32.dll
     7fefed90000 469c43bb Jul 17 05:21:15 2007 C:\Windows\system32\RPCRT4.dll
     7fefd010000 4549d2a6 Nov 02 11:12:38 2006 C:\Windows\system32\LSASRV.dll
     7fefdd40000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\system32\msvcrt.dll
     7fefd390000 4549d33f Nov 02 11:15:11 2006 C:\Windows\system32\Secur32.dll
        76d00000 45d3ee19 Feb 15 05:22:33 2007 C:\Windows\system32\USER32.dll
     7fefec20000 4549d273 Nov 02 11:11:47 2006 C:\Windows\system32\GDI32.dll
     7fefcec0000 4549d317 Nov 02 11:14:31 2006 C:\Windows\system32\SAMSRV.dll
     7fefce80000 4549d346 Nov 02 11:15:18 2006 C:\Windows\system32\cryptdll.dll
     7fefce40000 4549d288 Nov 02 11:12:08 2006 C:\Windows\system32\DNSAPI.dll
     7fefd540000 4549d38a Nov 02 11:16:26 2006 C:\Windows\system32\WS2_32.dll
     7feff0b0000 4549d370 Nov 02 11:16:00 2006 C:\Windows\system32\NSI.dll
     7fefcf70000 4549d2fc Nov 02 11:14:04 2006 C:\Windows\system32\NETAPI32.dll
     7fefd530000 4549d310 Nov 02 11:14:24 2006 C:\Windows\system32\PSAPI.DLL
     7fefce20000 4549d315 Nov 02 11:14:29 2006 C:\Windows\system32\SAMLIB.dll
     7fefce00000 4549d2df Nov 02 11:13:35 2006 C:\Windows\system32\MSASN1.dll
     7fefcdd0000 4549d375 Nov 02 11:16:05 2006 C:\Windows\system32\NTDSAPI.dll
     7fefd590000 4549d396 Nov 02 11:16:38 2006 C:\Windows\system32\WLDAP32.dll
     7fefcdb0000 4549d283 Nov 02 11:12:03 2006 C:\Windows\system32\FeClient.dll
     7fefcd90000 4549d2b2 Nov 02 11:12:50 2006 C:\Windows\system32\MPR.dll
     7fefd3b0000 4549d336 Nov 02 11:15:02 2006 C:\Windows\system32\USERENV.dll
     7fefcc50000 4549d344 Nov 02 11:15:16 2006 C:\Windows\system32\CRYPT32.dll
     7fefcc20000 4549d32d Nov 02 11:14:53 2006 C:\Windows\system32\slc.dll
     7fefd350000 4549d33a Nov 02 11:15:06 2006 C:\Windows\system32\SYSNTFY.dll
     7fefcbb0000 4549d349 Nov 02 11:15:21 2006 C:\Windows\system32\wevtapi.dll
     7fefcb80000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\system32\IPHLPAPI.DLL
```

```
     7fefcb30000 4549d263 Nov 02 11:11:31 2006 C:\Windows\system32\dhcpcsvc.DLL
     7fefd280000 4549d370 Nov 02 11:16:00 2006 C:\Windows\system32\WINNSI.DLL
     7fefcb00000 4549d264 Nov 02 11:11:32 2006 C:\Windows\system32\dhcpcsvc6.DLL
     7fefd9e0000 4549d2cb Nov 02 11:13:15 2006 C:\Windows\system32\IMM32.DLL
     7fefdc30000 4549d2e6 Nov 02 11:13:42 2006 C:\Windows\system32\MSCTF.dll
     7feff0c0000 4549d2a1 Nov 02 11:12:33 2006 C:\Windows\system32\LPK.DLL
     7fefd940000 4549d337 Nov 02 11:15:03 2006 C:\Windows\system32\USP10.dll
     7fefcaf0000 4549d313 Nov 02 11:14:27 2006 C:\Windows\system32\cngaudit.dll
     7fefd360000 4549d265 Nov 02 11:11:33 2006 C:\Windows\system32\AUTHZ.dll
     7fefcab0000 4549d2f2 Nov 02 11:13:54 2006 C:\Windows\system32\ncrypt.dll
     7fefca60000 4549d252 Nov 02 11:11:14 2006 C:\Windows\system32\BCRYPT.dll
     7fefca40000 4549d341 Nov 02 11:15:13 2006 C:\Windows\system32\credssp.dll
        75170000 45499de2 Nov 02 07:27:30 2006 C:\Windows\system32\msprivs.dll
     7fefc990000 4549d327 Nov 02 11:14:47 2006 C:\Windows\system32\kerberos.dll
     7fefc8f0000 4549d2e7 Nov 02 11:13:43 2006 C:\Windows\system32\mswsock.dll
     7fefc980000 4549d39d Nov 02 11:16:45 2006 C:\Windows\System32\wship6.dll
     7fefc860000 4549d2de Nov 02 11:13:34 2006 C:\Windows\system32\msv1_0.dll
     7fefc7b0000 4549d307 Nov 02 11:14:15 2006 C:\Windows\system32\netlogon.dll
     7fefc6d0000 4549d35d Nov 02 11:15:41 2006 C:\Windows\system32\WINBRAND.dll
     7fefc670000 4549d321 Nov 02 11:14:41 2006 C:\Windows\system32\schannel.dll
     7fefc8b0000 4549d335 Nov 02 11:15:01 2006 C:\Windows\system32\wdigest.dll
     7fefc620000 4549d31d Nov 02 11:14:37 2006 C:\Windows\system32\rsaenh.dll
     7fefc960000 4549d363 Nov 02 11:15:47 2006 C:\Windows\system32\tspkg.dll
     7fefc940000 4549d277 Nov 02 11:11:51 2006 C:\Windows\system32\GPAPI.dll
     7fefeed0000 4549d318 Nov 02 11:14:32 2006 C:\Windows\system32\setupapi.dll
     7fefdab0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\OLEAUT32.dll
     7fefd760000 4549d317 Nov 02 11:14:31 2006 C:\Windows\system32\ole32.dll
     7fefc5e0000 4549d31e Nov 02 11:14:38 2006 C:\Windows\system32\scecli.dll
     7fefc560000 4549d3a3 Nov 02 11:16:51 2006 C:\Windows\system32\wshtcpip.dll
     7fefaab0000 4549d371 Nov 02 11:16:01 2006 C:\Windows\System32\winrnr.dll
     7fefc1a0000 4549d314 Nov 02 11:14:28 2006 C:\Windows\system32\NLAapi.dll
     7fefaa70000 4549d2e4 Nov 02 11:13:40 2006 C:\Windows\system32\napinsp.dll
     7fefaa50000 4549d341 Nov 02 11:15:13 2006 C:\Windows\system32\pnrpnsp.dll
     7fefaac0000 4549d317 Nov 02 11:14:31 2006 C:\Windows\system32\rasadhlp.dll
     7fefb3b0000 4549d2b1 Nov 02 11:12:49 2006 C:\Windows\system32\dssenh.dll
     7fef8150000 4549d329 Nov 02 11:14:49 2006 C:\Windows\system32\keyiso.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       00000000003f0000
    ProcessParameters: 00000000003f1bf0
    WindowTitle:  'C:\Windows\system32\lsass.exe'
    ImageFile:    'C:\Windows\system32\lsass.exe'
    CommandLine:  'C:\Windows\system32\lsass.exe'
    DllPath:
'C:\Windows\system32;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Wind
ows;C:\Windows\System32\Wbem'
    Environment:  00000000003f1310
        ALLUSERSPROFILE=C:\ProgramData
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\System32
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\TEMP
        TMP=C:\Windows\TEMP
        USERNAME=SYSTEM
        USERPROFILE=C:\Windows\system32\config\systemprofile
```

```
        windir=C:\Windows


        THREAD fffffa80042d4710  Cid 027c.02b4  Teb: 000007fffffda000 Win32Thread: 0000000000000000
WAIT: (Executive) UserMode Non-Alertable
            fffffa80045457b8  NotificationEvent
        IRP List:
            fffffa80044f20f0: (0006,0118) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004298550       Image:         lsass.exe
        Wait Start TickCount      7416           Ticks: 39163 (0:00:10:10.946)
        Context Switch Count      15
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address LSASRV!ServiceDispatcherThread (0x000007fefd03f450)
        Stack Init fffff98004ff1db0 Current fffff98004ff17f0
        Base fffff98004ff2000 Limit fffff98004fec000 Call 0
        Priority 11 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`04ff1830 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`04ff1970 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`04ff19d0 fffff800`01ebdf16 nt!KeWaitForSingleObject+0x5f5
        fffff980`04ff1a50 fffff800`01ea1a24 nt!IopSynchronousServiceTail+0x306
        fffff980`04ff1ac0 fffff800`01c4d733 nt!NtReadFile+0x583
        fffff980`04ff1bb0 00000000`76e202da nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`04ff1c20)
        00000000`0189f498 00000000`76bf26da ntdll!NtReadFile+0xa
        00000000`0189f4a0 000007fe`fea865aa kernel32!ReadFile+0x8a
        00000000`0189f530 000007fe`fea862e3 ADVAPI32!ScGetPipeInput+0x4a
        00000000`0189f610 000007fe`fea850f3 ADVAPI32!ScDispatcherLoop+0x9a
        00000000`0189f710 000007fe`fd03f4b4 ADVAPI32!StartServiceCtrlDispatcherW+0x176
        00000000`0189f9b0 00000000`76bfcdcd LSASRV!ServiceDispatcherThread+0xc7
        00000000`0189f9e0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0189fa10 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004325060  Cid 027c.02b8  Teb: 000007fffffd8000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa80042b8040  SynchronizationTimer
            fffffa80044c9110  SynchronizationEvent
            fffffa8004322e10  SynchronizationTimer
            fffffa800436f780  Thread
            fffffa8004387040  SynchronizationEvent
            fffffa800437cf60  SynchronizationEvent
            fffffa80042b6210  SynchronizationEvent
            fffffa800439e720  SynchronizationEvent
            fffffa8004387840  NotificationEvent
            fffffa800431ca60  SynchronizationEvent
            fffffa80043283d0  SynchronizationEvent
            fffffa80042d6240  SynchronizationEvent
            fffffa80042d4c40  SynchronizationEvent
            fffffa800435f7d0  SynchronizationEvent
            fffffa80042b5f00  SynchronizationEvent
            fffffa8004303d70  SynchronizationEvent
            fffffa8004305d60  SynchronizationEvent
            fffffa8004308a70  SynchronizationEvent
            fffffa8004314150  SynchronizationEvent
            fffffa800431f6f0  SynchronizationEvent
            fffffa800438eb00  SynchronizationEvent
            fffffa800435dc20  SynchronizationEvent
            fffffa800431e940  SynchronizationEvent
            fffffa8004674b60  SynchronizationEvent
            fffffa8004894dd0  SynchronizationEvent
            fffffa80048964d0  SynchronizationEvent
            fffffa8004904220  SynchronizationEvent
            fffffa8004cf91b0  SynchronizationEvent
            fffffa80043e8da0  NotificationEvent
            fffffa80043226e0  SynchronizationTimer
            fffffa8003ff0600  SynchronizationEvent
            fffffa800484ea50  SynchronizationEvent
            fffffa8004b8c330  SynchronizationEvent
            fffffa80049cf6a0  SynchronizationEvent
            fffffa8003ff03d0  SynchronizationEvent
            fffffa8004325118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004298550       Image:         lsass.exe
        Wait Start TickCount      42751          Ticks: 3828 (0:00:00:59.717)
        Context Switch Count      144
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x0000000076df6930)
        Stack Init fffff9800b3c7db0 Current fffff9800b3c7260
        Base fffff9800b3c8000 Limit fffff9800b3c2000 Call 0
        Priority 11 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0b3c72a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0b3c73e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0b3c7440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0b3c74b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0b3c7960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0b3c7bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0b3c7c20)
        00000000`0197f688 00000000`76df6b07 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0197f690 00000000`76bfcdcd ntdll!TppWaiterpThread+0x14d
        00000000`0197f930 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0197f960 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004322060  Cid 027c.02bc  Teb: 000007fffffd6000 Win32Thread: 0000000000000000
WAIT: (WrLpcReceive) UserMode Non-Alertable
            fffffa80043223f0  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004298550       Image:         lsass.exe
        Wait Start TickCount      7536           Ticks: 39043 (0:00:10:09.074)
        Context Switch Count      10
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address LSASRV!LsapRmServerThread (0x000007fefd031230)
        Stack Init fffff98004fffdb0 Current fffff98004fff7f0
        Base fffff98005000000 Limit fffff98004ffa000 Call 0
        Priority 10 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`04fff830 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`04fff970 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`04fff9d0 fffff800`01eb3788 nt!KeWaitForSingleObject+0x5f5
        fffff980`04fffa50 fffff800`01e7e523 nt!AlpcpReceiveMessagePort+0x298
        fffff980`04fffab0 fffff800`01e740d2 nt!AlpcpReceiveLegacyMessage+0x122
        fffff980`04fffb50 fffff800`01e724bf nt!NtReplyWaitReceivePortEx+0xc1
        fffff980`04fffbe0 fffff800`01c4d733 nt!NtReplyWaitReceivePort+0xf
        fffff980`04fffc20 00000000`76e2032a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`04fffc20)
        00000000`01e0f6e8 000007fe`fd0312a6 ntdll!NtReplyWaitReceivePort+0xa
        00000000`01e0f6f0 00000000`76bfcdcd LSASRV!LsapRmServerThread+0x7d
        00000000`01e0f930 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`01e0f960 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa800436e340  Cid 027c.02d8  Teb: 000007fffffac000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa80042d6720  QueueObject
            fffffa800436e3f8  NotificationTimer
        IRP List:
            fffffa80027f7ca0: (0006,0358) Flags: 00060000  Mdl: 00000000
            fffffa8004b45ca0: (0006,0358) Flags: 00060000  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004298550       Image:         lsass.exe
        Wait Start TickCount      46323          Ticks: 256 (0:00:00:03.993)
        Context Switch Count      2278
        UserTime                  00:00:00.062
        KernelTime                00:00:00.140
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff9800b6b7db0 Current fffff9800b6b7810
        Base fffff9800b6b8000 Limit fffff9800b6b2000 Call 0
        Priority 11 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0b6b7850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0b6b7990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0b6b79f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0b6b7a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`0b6b7b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`0b6b7bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0b6b7c20)
        00000000`01f6fa68 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`01f6fa70 000007fe`fedce7a3 kernel32!GetQueuedCompletionStatus+0x48
        00000000`01f6fad0 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`01f6fb60 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`01f6fc10 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`01f6fc40 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`01f6fc80 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`01f6fcb0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`01f6fce0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800436f780  Cid 027c.02dc  Teb: 000007fffffaa000 Win32Thread: 0000000000000000
WAIT: (WrLpcReceive) UserMode Non-Alertable
            fffffa800436fb10  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004298550       Image:         lsass.exe
        Wait Start TickCount      46296          Ticks: 283 (0:00:00:04.414)
        Context Switch Count      1394
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address LSASRV!LsapThreadBase (0x000007fefd0598b0)
        Stack Init fffff9800b6efdb0 Current fffff9800b6ef7f0
        Base fffff9800b6f0000 Limit fffff9800b6ea000 Call 0
        Priority 10 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0b6ef830 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0b6ef970 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0b6ef9d0 fffff800`01eb3788 nt!KeWaitForSingleObject+0x5f5
        fffff980`0b6efa50 fffff800`01e7e523 nt!AlpcpReceiveMessagePort+0x298
        fffff980`0b6efab0 fffff800`01e740d2 nt!AlpcpReceiveLegacyMessage+0x122
        fffff980`0b6efb50 fffff800`01e724bf nt!NtReplyWaitReceivePortEx+0xc1
        fffff980`0b6efbe0 fffff800`01c4d733 nt!NtReplyWaitReceivePort+0xf
        fffff980`0b6efc20 00000000`76e2032a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0b6efc20)
        00000000`0217fa08 000007fe`fd01c661 ntdll!NtReplyWaitReceivePort+0xa
        00000000`0217fa10 000007fe`fd05992e LSASRV!LpcServerThread+0x28f
        00000000`0217fcf0 00000000`76bfcdcd LSASRV!LsapThreadBase+0xaa
        00000000`0217fd40 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0217fd70 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80043873b0  Cid 027c.02e4  Teb: 000007fffffa6000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80043878a0  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004298550       Image:         lsass.exe
        Wait Start TickCount      1416           Ticks: 45163 (0:00:11:44.547)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address LSASRV!LsapThreadBase (0x000007fefd0598b0)
        Stack Init fffff9800b3abdb0 Current fffff9800b3ab960
        Base fffff9800b3ac000 Limit fffff9800b3a6000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0b3ab9a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0b3abae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0b3abb40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0b3abbc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0b3abc20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0b3abc20)
        00000000`0220fbb8 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`0220fbc0 000007fe`fd01b022 kernel32!WaitForSingleObjectEx+0x9c
        00000000`0220fc80 000007fe`fd05992e LSASRV!SpmPoolThreadBase+0x13e
        00000000`0220fcd0 00000000`76bfcdcd LSASRV!LsapThreadBase+0xaa
        00000000`0220fd20 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0220fd50 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80043697c0  Cid 027c.02ec  Teb: 000007fffffa2000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80043dfe00  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004298550       Image:         lsass.exe
        Wait Start TickCount      2699           Ticks: 43880 (0:00:11:24.532)
        Context Switch Count      115
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address LSASRV!LsapThreadBase (0x000007fefd0598b0)
        Stack Init fffff9800b686db0 Current fffff9800b686960
        Base fffff9800b687000 Limit fffff9800b681000 Call 0
        Priority 11 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0b6869a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0b686ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0b686b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0b686bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0b686c20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0b686c20)
        00000000`0169fa78 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`0169fa80 000007fe`fd01b022 kernel32!WaitForSingleObjectEx+0x9c
        00000000`0169fb40 000007fe`fd05992e LSASRV!SpmPoolThreadBase+0x13e
        00000000`0169fb90 00000000`76bfcdcd LSASRV!LsapThreadBase+0xaa
        00000000`0169fbe0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0169fc10 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004396060  Cid 027c.0300  Teb: 000007fffff9e000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Alertable
            fffffa80042d62a0  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004298550       Image:         lsass.exe
        Wait Start TickCount      22971          Ticks: 23608 (0:00:06:08.287)
        Context Switch Count      53
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x0000000076e17860)
        Stack Init fffff9800b6ccdb0 Current fffff9800b6cc860
        Base fffff9800b6cd000 Limit fffff9800b6c7000 Call 0
        Priority 10 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0b6cc8a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0b6cc9e0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0b6cca40 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0b6ccad0 fffff800`01c8a722 nt!IoRemoveIoCompletion+0x47
        fffff980`0b6ccb50 fffff800`01c4d733 nt!NtWaitForWorkViaWorkerFactory+0x1f1
        fffff980`0b6ccc20 00000000`76e21b4a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0b6ccc20)
        00000000`0247f978 00000000`76e17a20 ntdll!NtWaitForWorkViaWorkerFactory+0xa
        00000000`0247f980 00000000`76bfcdcd ntdll!TppWorkerThread+0x23e
        00000000`0247fbf0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0247fc20 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80041b5bb0  Cid 027c.06b4  Teb: 000007fffff9c000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80046b55d0  NotificationEvent
            fffffa8004701170  SynchronizationEvent
            fffffa80041b72c0  NotificationEvent
            fffffa800466af70  SynchronizationEvent
            fffffa80046e6e00  SynchronizationEvent
            fffffa8004310590  SynchronizationEvent
            fffffa80046b7680  NotificationEvent
            fffffa80042ae850  NotificationEvent
            fffffa80041b5c68  NotificationTimer
        IRP List:
            fffffa8004722010: (0006,01f0) Flags: 00060000  Mdl: fffffa80043100d0
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004298550       Image:         lsass.exe
        Wait Start TickCount      40222          Ticks: 6357 (0:00:01:39.169)
        Context Switch Count      102
        UserTime                  00:00:00.000
        KernelTime                00:00:00.046
        Win32 Start Address ADVAPI32!ScSvcctrlThreadW (0x000007fefea84bd0)
        Stack Init fffff9800ebf1db0 Current fffff9800ebf1260
        Base fffff9800ebf2000 Limit fffff9800ebec000 Call 0
        Priority 11 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0ebf12a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0ebf13e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0ebf1440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0ebf14b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0ebf1960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0ebf1bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0ebf1c20)
        00000000`02bdf788 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`02bdf790 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`02bdf8a0 000007fe`fc7c7aa7 kernel32!WaitForMultipleObjects+0x11
        00000000`02bdf8e0 000007fe`fc7bf873 netlogon!NlMainLoop+0x6b5
        00000000`02bdfdd0 000007fe`fd051753 netlogon!NlNetlogonMain+0x4d3
        00000000`02bdfe40 000007fe`fea84bf5 LSASRV!LsapStartService+0x17b
        00000000`02bdfea0 00000000`76bfcdcd ADVAPI32!ScSvcctrlThreadW+0x25
        00000000`02bdfed0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02bdff00 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8002583bb0  Cid 027c.09c0  Teb: 000007fffffdc000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa80042d6720  QueueObject
            fffffa8002583c68  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004298550       Image:         lsass.exe
        Wait Start TickCount      45141          Ticks: 1438 (0:00:00:22.432)
        Context Switch Count      35
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff9801db11db0 Current fffff9801db11810
        Base fffff9801db12000 Limit fffff9801db0c000 Call 0
        Priority 11 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1db11850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1db11990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`1db119f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`1db11a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`1db11b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`1db11bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1db11c20)
        00000000`017cf968 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`017cf970 000007fe`fedce7a3 kernel32!GetQueuedCompletionStatus+0x48
        00000000`017cf9d0 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`017cfa60 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`017cfb10 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`017cfb40 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`017cfb80 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`017cfbb0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`017cfbe0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80040a1060  Cid 027c.0db8  Teb: 000007fffffd4000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80042b5ea0  Semaphore Limit 0x7fffffff
            fffffa80040a1118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004298550       Image:         lsass.exe
        Wait Start TickCount      46296          Ticks: 283 (0:00:00:04.414)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address LSASRV!LsapThreadBase (0x000007fefd0598b0)
        Stack Init fffff9800daacdb0 Current fffff9800daac960
        Base fffff9800daad000 Limit fffff9800daa7000 Call 0
        Priority 10 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0daac9a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0daacae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0daacb40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0daacbc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0daacc20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0daacc20)
        00000000`022df648 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`022df650 000007fe`fd01b022 kernel32!WaitForSingleObjectEx+0x9c
        00000000`022df710 000007fe`fd05992e LSASRV!SpmPoolThreadBase+0x13e
        00000000`022df760 00000000`76bfcdcd LSASRV!LsapThreadBase+0xaa
        00000000`022df7b0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`022df7e0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

Winlogon process

```
PROCESS fffffa8004299660
    SessionId: 1  Cid: 0284    Peb: 7fffffde000  ParentCid: 0224
    DirBase: 523ba000  ObjectTable: fffff880057e8010  HandleCount: 125.
    Image: winlogon.exe
    VadRoot fffffa8004294120 Vads 75 Clone 0 Private 534. Modified 631. Locked 0.
    DeviceMap fffff88000007820
    Token                             fffff880057cac40
    ElapsedTime                       00:11:46.105
    UserTime                          00:00:00.093
    KernelTime                        00:00:00.234
    QuotaPoolUsage[PagedPool]         129352
    QuotaPoolUsage[NonPagedPool]      7168
    Working Set Sizes (now,min,max)  (1279, 50, 345) (5116KB, 200KB, 1380KB)
    PeakWorkingSetSize                1936
    VirtualSize                       66 Mb
    PeakVirtualSize                   68 Mb
    PageFaultCount                    3057
    MemoryPriority                    BACKGROUND
    BasePriority                      13
    CommitCharge                      674

    Setting context for this process...
.process /p /r fffffa8004299660

    !peb
PEB at 000007fffffde000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00000000ff180000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00000000001f2290 . 000000000021ceb0
    Ldr.InLoadOrderModuleList:           00000000001f21a0 . 000000000021ce90
    Ldr.InMemoryOrderModuleList:         00000000001f21b0 . 000000000021cea0
            Base TimeStamp                     Module
        ff180000 4549b9f4 Nov 02 09:27:16 2006 C:\Windows\system32\winlogon.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        76bc0000 4549d328 Nov 02 11:14:48 2006 C:\Windows\system32\kernel32.dll
     7fefea30000 4549d267 Nov 02 11:11:35 2006 C:\Windows\system32\ADVAPI32.dll
     7fefed90000 469c43bb Jul 17 05:21:15 2007 C:\Windows\system32\RPCRT4.dll
        76d00000 45d3ee19 Feb 15 05:22:33 2007 C:\Windows\system32\USER32.dll
     7fefec20000 4549d273 Nov 02 11:11:47 2006 C:\Windows\system32\GDI32.dll
     7fefdd40000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\system32\msvcrt.dll
     7fefd390000 4549d33f Nov 02 11:15:11 2006 C:\Windows\system32\Secur32.dll
     7fefd1b0000 4549d380 Nov 02 11:16:16 2006 C:\Windows\system32\WINSTA.dll
     7fefd530000 4549d310 Nov 02 11:14:24 2006 C:\Windows\system32\PSAPI.DLL
     7fefd3b0000 4549d336 Nov 02 11:15:02 2006 C:\Windows\system32\USERENV.dll
     7fefd9e0000 4549d2cb Nov 02 11:13:15 2006 C:\Windows\system32\IMM32.DLL
     7fefdc30000 4549d2e6 Nov 02 11:13:42 2006 C:\Windows\system32\MSCTF.dll
     7feff0c0000 4549d2a1 Nov 02 11:12:33 2006 C:\Windows\system32\LPK.DLL
     7fefd940000 4549d337 Nov 02 11:15:03 2006 C:\Windows\system32\USP10.dll
     7fefd310000 4549d247 Nov 02 11:11:03 2006 C:\Windows\system32\apphelp.dll
     7fefc5b0000 4549d384 Nov 02 11:16:20 2006 C:\Windows\system32\NTMARTA.DLL
     7fefd590000 4549d396 Nov 02 11:16:38 2006 C:\Windows\system32\WLDAP32.dll
     7fefd540000 4549d38a Nov 02 11:16:26 2006 C:\Windows\system32\WS2_32.dll
     7feff0b0000 4549d370 Nov 02 11:16:00 2006 C:\Windows\system32\NSI.dll
     7fefce20000 4549d315 Nov 02 11:14:29 2006 C:\Windows\system32\SAMLIB.dll
     7fefd760000 4549d317 Nov 02 11:14:31 2006 C:\Windows\system32\ole32.dll
     7fefb5c0000 4549d324 Nov 02 11:14:44 2006 C:\Windows\system32\SHSVCS.dll
     7fefc330000 4549d33b Nov 02 11:15:07 2006 C:\Windows\system32\uxtheme.dll
     7fefc620000 4549d31d Nov 02 11:14:37 2006 C:\Windows\system32\rsaenh.dll
     7fefb140000 4549d365 Nov 02 11:15:49 2006 C:\Windows\system32\WindowsCodecs.dll
     7fefcf70000 4549d2fc Nov 02 11:14:04 2006 C:\Windows\system32\NETAPI32.dll
     7fefcc20000 4549d32d Nov 02 11:14:53 2006 C:\Windows\system32\slc.dll
```

```
     7fefcd90000 4549d2b2 Nov 02 11:12:50 2006 C:\Windows\system32\MPR.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       00000000001f0000
    ProcessParameters: 00000000001f1950
    WindowTitle:  '< Name not readable >'
    ImageFile:    'C:\Windows\system32\winlogon.exe'
    CommandLine:  'winlogon.exe'
    DllPath:      'C:\Windows\system32;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem'
    Environment:  000000000021eea0
        ALLUSERSPROFILE=C:\ProgramData
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\TEMP
        TMP=C:\Windows\TEMP
        USERNAME=SYSTEM
        USERPROFILE=C:\Windows\system32\config\systemprofile
        windir=C:\Windows


        THREAD fffffa800429a060  Cid 0284.0288  Teb: 000007fffffdc000 Win32Thread: fffff900c00c6a60
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004491b50  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004299660       Image:         winlogon.exe
        Wait Start TickCount      16708          Ticks: 29871 (0:00:07:45.990)
        Context Switch Count      1249                 LargeStack
        UserTime                  00:00:00.015
        KernelTime                00:00:00.078
        Win32 Start Address winlogon!WinMainCRTStartup (0x00000000ff1ce3b8)
        Stack Init fffff9800bb67db0 Current fffff9800bb67960
        Base fffff9800bb68000 Limit fffff9800bb5e000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0bb679a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0bb67ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0bb67b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0bb67bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0bb67c20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0bb67c20)
        00000000`0012f1d8 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`0012f1e0 00000000`ff1b307b kernel32!WaitForSingleObjectEx+0x9c
        00000000`0012f2a0 00000000`ff18d862 winlogon!StateMachineRun+0x4c7
        00000000`0012f590 00000000`ff1ce20f winlogon!WinMain+0x12a2
        00000000`0012f6d0 00000000`76bfcdcd winlogon!ConvertSidToStringSidW+0x1ed
        00000000`0012f790 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0012f7c0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004490740  Cid 0284.03f4  Teb: 000007fffffd4000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa8004490ef0  SynchronizationTimer
            fffffa80044bf3a0  SynchronizationTimer
            fffffa8004242760  NotificationEvent
            fffffa8004490da0  SynchronizationTimer
            fffffa80048ffe50  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004299660       Image:         winlogon.exe
        Wait Start TickCount      4710           Ticks: 41869 (0:00:10:53.160)
        Context Switch Count      8
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x0000000076df6930)
        Stack Init fffff9800cca0db0 Current fffff9800cca0260
        Base fffff9800cca1000 Limit fffff9800cc9b000 Call 0
        Priority 15 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0cca02a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0cca03e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0cca0440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0cca04b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0cca0960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0cca0bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0cca0c20)
        00000000`00fff718 00000000`76df6b07 ntdll!NtWaitForMultipleObjects+0xa
        00000000`00fff720 00000000`76bfcdcd ntdll!TppWaiterpThread+0x14d
        00000000`00fff9c0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`00fff9f0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa800294fa80  Cid 0284.0870  Teb: 000007fffffda000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa80042a4040  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004299660       Image:         winlogon.exe
        Wait Start TickCount      18631          Ticks: 27948 (0:00:07:15.991)
        Context Switch Count      21
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff98004f9ddb0 Current fffff98004f9d810
        Base fffff98004f9e000 Limit fffff98004f98000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`04f9d850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`04f9d990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`04f9d9f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`04f9da80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`04f9db00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`04f9dbb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`04f9dc20)
        00000000`01d2f7d8 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`01d2f7e0 000007fe`fedce7a3 kernel32!GetQueuedCompletionStatus+0x48
        00000000`01d2f840 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`01d2f8d0 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`01d2f980 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`01d2f9b0 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`01d2f9f0 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`01d2fa20 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`01d2fa50 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

Lsm process

```
PROCESS fffffa80042a4c10
    SessionId: 0  Cid: 0290    Peb: 7fffffdc000  ParentCid: 0234
    DirBase: 52141000  ObjectTable: fffff880055fd870  HandleCount: 160.
    Image: lsm.exe
    VadRoot fffffa8004299c70 Vads 66 Clone 0 Private 471. Modified 143. Locked 0.
    DeviceMap fffff88000007820
    Token                             fffff880057f4c40
    ElapsedTime                       00:11:46.059
    UserTime                          00:00:00.046
    KernelTime                        00:00:00.015
    QuotaPoolUsage[PagedPool]         68640
    QuotaPoolUsage[NonPagedPool]      6880
    Working Set Sizes (now,min,max)  (1069, 50, 345) (4276KB, 200KB, 1380KB)
    PeakWorkingSetSize                1314
    VirtualSize                       35 Mb
    PeakVirtualSize                   36 Mb
    PageFaultCount                    1394
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      739

    Setting context for this process...
.process /p /r fffffa80042a4c10

    !peb
PEB at 000007fffffdc000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00000000ff090000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00000000001c2610 . 00000000001faeb0
    Ldr.InLoadOrderModuleList:           00000000001c2520 . 00000000001fb030
    Ldr.InMemoryOrderModuleList:         00000000001c2530 . 00000000001fb040
            Base TimeStamp                     Module
        ff090000 4549c010 Nov 02 09:53:20 2006 C:\Windows\system32\lsm.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        76bc0000 4549d328 Nov 02 11:14:48 2006 C:\Windows\system32\kernel32.dll
     7fefea30000 4549d267 Nov 02 11:11:35 2006 C:\Windows\system32\ADVAPI32.dll
     7fefed90000 469c43bb Jul 17 05:21:15 2007 C:\Windows\system32\RPCRT4.dll
     7fefdd40000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\system32\msvcrt.dll
     7fefd350000 4549d33a Nov 02 11:15:06 2006 C:\Windows\system32\SYSNTFY.dll
     7fefd290000 4549d366 Nov 02 11:15:50 2006 C:\Windows\system32\WMsgAPI.dll
     7fefd390000 4549d33f Nov 02 11:15:11 2006 C:\Windows\system32\secur32.dll
     7fefca40000 4549d341 Nov 02 11:15:13 2006 C:\Windows\system32\credssp.dll
     7fefcc50000 4549d344 Nov 02 11:15:16 2006 C:\Windows\system32\CRYPT32.dll
        76d00000 45d3ee19 Feb 15 05:22:33 2007 C:\Windows\system32\USER32.dll
     7fefec20000 4549d273 Nov 02 11:11:47 2006 C:\Windows\system32\GDI32.dll
     7fefce00000 4549d2df Nov 02 11:13:35 2006 C:\Windows\system32\MSASN1.dll
     7fefd3b0000 4549d336 Nov 02 11:15:02 2006 C:\Windows\system32\USERENV.dll
     7fefd9e0000 4549d2cb Nov 02 11:13:15 2006 C:\Windows\system32\IMM32.DLL
     7fefdc30000 4549d2e6 Nov 02 11:13:42 2006 C:\Windows\system32\MSCTF.dll
     7feff0c0000 4549d2a1 Nov 02 11:12:33 2006 C:\Windows\system32\LPK.DLL
     7fefd940000 4549d337 Nov 02 11:15:03 2006 C:\Windows\system32\USP10.dll
     7fefc670000 4549d321 Nov 02 11:14:41 2006 C:\Windows\system32\schannel.dll
     7fefcf70000 4549d2fc Nov 02 11:14:04 2006 C:\Windows\system32\NETAPI32.dll
     7fefd530000 4549d310 Nov 02 11:14:24 2006 C:\Windows\system32\PSAPI.DLL
    SubSystemData:     0000000000000000
    ProcessHeap:       00000000001c0000
    ProcessParameters: 00000000001c1bf0
    WindowTitle:  'C:\Windows\system32\lsm.exe'
    ImageFile:    'C:\Windows\system32\lsm.exe'
    CommandLine:  'C:\Windows\system32\lsm.exe'
```

```
    DllPath:
'C:\Windows\system32;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Wind
ows;C:\Windows\System32\Wbem'
    Environment:  00000000001c1310
        ALLUSERSPROFILE=C:\ProgramData
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\TEMP
        TMP=C:\Windows\TEMP
        USERNAME=SYSTEM
        USERPROFILE=C:\Windows\system32\config\systemprofile
        windir=C:\Windows


        THREAD fffffa80042a4780  Cid 0290.0294  Teb: 000007fffffde000 Win32Thread: fffff900c07c3a60
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004386770  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80042a4c10       Image:         lsm.exe
        Wait Start TickCount      1547           Ticks: 45032 (0:00:11:42.503)
        Context Switch Count      454                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address lsm!mainCRTStartup (0x00000000ff0c3e0c)
        Stack Init fffff9800d1c6db0 Current fffff9800d1c6960
        Base fffff9800d1c7000 Limit fffff9800d1c0000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0d1c69a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0d1c6ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0d1c6b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0d1c6bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0d1c6c20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0d1c6c20)
        00000000`000df6a8 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`000df6b0 000007fe`feda0e9d kernel32!WaitForSingleObjectEx+0x9c
        00000000`000df770 000007fe`fee056bc RPCRT4!EVENT::Wait+0xd
        00000000`000df7a0 000007fe`fede6cf5 RPCRT4!RPC_SERVER::WaitForStopServerListening+0x1c
        00000000`000df7d0 000007fe`fede6c9d RPCRT4!RPC_SERVER::WaitServerListen+0x55
        00000000`000df800 00000000`ff0a060c RPCRT4!RpcMgmtWaitServerListen+0x22
        00000000`000df830 00000000`ff0c3ca1 lsm!main+0x158
        00000000`000df890 00000000`76bfcdcd lsm!AuditFree+0x19b
        00000000`000df8d0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`000df900 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80041bc060  Cid 0290.03b8  Teb: 000007fffffd8000 Win32Thread: 0000000000000000
WAIT: (WrLpcReceive) UserMode Non-Alertable
            fffffa80041bc3f0  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80042a4c10       Image:         lsm.exe
        Wait Start TickCount      5135           Ticks: 41444 (0:00:10:46.530)
        Context Switch Count      13
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x0000000076e17860)
        Stack Init fffff9800c243db0 Current fffff9800c2437f0
        Base fffff9800c244000 Limit fffff9800c23e000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0c243830 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0c243970 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0c2439d0 fffff800`01eb3788 nt!KeWaitForSingleObject+0x5f5
        fffff980`0c243a50 fffff800`01e7e523 nt!AlpcpReceiveMessagePort+0x298
        fffff980`0c243ab0 fffff800`01e740d2 nt!AlpcpReceiveLegacyMessage+0x122
        fffff980`0c243b50 fffff800`01e724bf nt!NtReplyWaitReceivePortEx+0xc1
        fffff980`0c243be0 fffff800`01c4d733 nt!NtReplyWaitReceivePort+0xf
        fffff980`0c243c20 00000000`76e2032a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0c243c20)
        00000000`00a2f6d8 00000000`ff0b2221 ntdll!NtReplyWaitReceivePort+0xa
        00000000`00a2f6e0 00000000`ff0b1909 lsm!CCsrMgr::LpcWorker+0x59
        00000000`00a2f850 00000000`76df6500 lsm!CCsrMgr::staticLpcWorker+0x9
        00000000`00a2f880 00000000`76e17b59 ntdll!RtlpTpWorkCallback+0xf0
        00000000`00a2f930 00000000`76bfcdcd ntdll!TppWorkerThread+0x3ad
        00000000`00a2fba0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`00a2fbd0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80041bca60  Cid 0290.03bc  Teb: 000007fffffd6000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa80041bcef0  SynchronizationTimer
            fffffa80040bc8e0  ProcessObject
            fffffa8003f56ad0  ProcessObject
            fffffa8003d72040  ProcessObject
            fffffa8004299660  ProcessObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80042a4c10       Image:         lsm.exe
        Wait Start TickCount      1546           Ticks: 45033 (0:00:11:42.519)
        Context Switch Count      7
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x0000000076df6930)
        Stack Init fffff9800bacfdb0 Current fffff9800bacf260
        Base fffff9800bad0000 Limit fffff9800baca000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0bacf2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0bacf3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0bacf440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0bacf4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0bacf960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0bacfbb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0bacfc20)
        00000000`0082f8a8 00000000`76df6b07 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0082f8b0 00000000`76bfcdcd ntdll!TppWaiterpThread+0x14d
        00000000`0082fb50 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0082fb80 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800442b060  Cid 0290.03c0  Teb: 000007fffffd4000 Win32Thread: 0000000000000000
WAIT: (WrLpcReceive) UserMode Non-Alertable
            fffffa800442b3f0  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80042a4c10       Image:         lsm.exe
        Wait Start TickCount      5138           Ticks: 41441 (0:00:10:46.483)
        Context Switch Count      10
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x0000000076e17860)
        Stack Init fffff9800c24adb0 Current fffff9800c24a7f0
        Base fffff9800c24b000 Limit fffff9800c245000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0c24a830 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0c24a970 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0c24a9d0 fffff800`01eb3788 nt!KeWaitForSingleObject+0x5f5
        fffff980`0c24aa50 fffff800`01e7e523 nt!AlpcpReceiveMessagePort+0x298
        fffff980`0c24aab0 fffff800`01e740d2 nt!AlpcpReceiveLegacyMessage+0x122
        fffff980`0c24ab50 fffff800`01e724bf nt!NtReplyWaitReceivePortEx+0xc1
        fffff980`0c24abe0 fffff800`01c4d733 nt!NtReplyWaitReceivePort+0xf
        fffff980`0c24ac20 00000000`76e2032a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0c24ac20)
        00000000`0016fa58 00000000`ff0b2221 ntdll!NtReplyWaitReceivePort+0xa
        00000000`0016fa60 00000000`ff0b1909 lsm!CCsrMgr::LpcWorker+0x59
        00000000`0016fbd0 00000000`76df6500 lsm!CCsrMgr::staticLpcWorker+0x9
        00000000`0016fc00 00000000`76e17b59 ntdll!RtlpTpWorkCallback+0xf0
        00000000`0016fcb0 00000000`76bfcdcd ntdll!TppWorkerThread+0x3ad
        00000000`0016ff20 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0016ff50 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa800442bbb0  Cid 0290.03c4  Teb: 000007fffffae000 Win32Thread: 0000000000000000
WAIT: (WrLpcReceive) UserMode Non-Alertable
            fffffa800442bf40  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80042a4c10       Image:         lsm.exe
        Wait Start TickCount      5135           Ticks: 41444 (0:00:10:46.530)
        Context Switch Count      9
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x0000000076e17860)
        Stack Init fffff9800c251db0 Current fffff9800c2517f0
        Base fffff9800c252000 Limit fffff9800c24c000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0c251830 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0c251970 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0c2519d0 fffff800`01eb3788 nt!KeWaitForSingleObject+0x5f5
        fffff980`0c251a50 fffff800`01e7e523 nt!AlpcpReceiveMessagePort+0x298
        fffff980`0c251ab0 fffff800`01e740d2 nt!AlpcpReceiveLegacyMessage+0x122
        fffff980`0c251b50 fffff800`01e724bf nt!NtReplyWaitReceivePortEx+0xc1
        fffff980`0c251be0 fffff800`01c4d733 nt!NtReplyWaitReceivePort+0xf
        fffff980`0c251c20 00000000`76e2032a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0c251c20)
        00000000`00baf708 00000000`ff0b2221 ntdll!NtReplyWaitReceivePort+0xa
        00000000`00baf710 00000000`ff0b1909 lsm!CCsrMgr::LpcWorker+0x59
        00000000`00baf880 00000000`76df6500 lsm!CCsrMgr::staticLpcWorker+0x9
        00000000`00baf8b0 00000000`76e17b59 ntdll!RtlpTpWorkCallback+0xf0
        00000000`00baf960 00000000`76bfcdcd ntdll!TppWorkerThread+0x3ad
        00000000`00bafbd0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`00bafc00 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80044c43b0  Cid 0290.03cc  Teb: 000007fffffac000 Win32Thread: 0000000000000000
WAIT: (WrLpcReceive) UserMode Non-Alertable
            fffffa80044c4740  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80042a4c10       Image:         lsm.exe
        Wait Start TickCount      3732           Ticks: 42847 (0:00:11:08.417)
        Context Switch Count      12
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x0000000076e17860)
        Stack Init fffff9800c258db0 Current fffff9800c2587f0
        Base fffff9800c259000 Limit fffff9800c253000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0c258830 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0c258970 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0c2589d0 fffff800`01eb3788 nt!KeWaitForSingleObject+0x5f5
        fffff980`0c258a50 fffff800`01e7e523 nt!AlpcpReceiveMessagePort+0x298
        fffff980`0c258ab0 fffff800`01e740d2 nt!AlpcpReceiveLegacyMessage+0x122
        fffff980`0c258b50 fffff800`01e724bf nt!NtReplyWaitReceivePortEx+0xc1
        fffff980`0c258be0 fffff800`01c4d733 nt!NtReplyWaitReceivePort+0xf
        fffff980`0c258c20 00000000`76e2032a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0c258c20)
        00000000`00c6f6c8 00000000`ff0b2221 ntdll!NtReplyWaitReceivePort+0xa
        00000000`00c6f6d0 00000000`ff0b1909 lsm!CCsrMgr::LpcWorker+0x59
        00000000`00c6f840 00000000`76df6500 lsm!CCsrMgr::staticLpcWorker+0x9
        00000000`00c6f870 00000000`76e17b59 ntdll!RtlpTpWorkCallback+0xf0
        00000000`00c6f920 00000000`76bfcdcd ntdll!TppWorkerThread+0x3ad
        00000000`00c6fb90 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`00c6fbc0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80044c3bb0  Cid 0290.03d0  Teb: 000007fffffaa000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80044c5390  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80042a4c10       Image:         lsm.exe
        Wait Start TickCount      2778           Ticks: 43801 (0:00:11:23.299)
        Context Switch Count      18
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x0000000076e17860)
        Stack Init fffff9800c274db0 Current fffff9800c274960
        Base fffff9800c275000 Limit fffff9800c26f000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0c2749a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0c274ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0c274b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0c274bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0c274c20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0c274c20)
        00000000`00cff588 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`00cff590 00000000`ff09ff3d kernel32!WaitForSingleObjectEx+0x9c
        00000000`00cff650 00000000`76df6500 lsm!CSCMNotify::staticSCMNotificationThread+0xf1
        00000000`00cff6a0 00000000`76e17b59 ntdll!RtlpTpWorkCallback+0xf0
        00000000`00cff750 00000000`76bfcdcd ntdll!TppWorkerThread+0x3ad
        00000000`00cff9c0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`00cff9f0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80044c7960  Cid 0290.03dc  Teb: 000007fffffa6000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa80044a3650  SynchronizationEvent
            fffffa80043eddb0  SynchronizationEvent
            fffffa80043edd50  SynchronizationEvent
            fffffa80043edcf0  SynchronizationEvent
            fffffa80043edc90  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80042a4c10       Image:         lsm.exe
        Wait Start TickCount      1874           Ticks: 44705 (0:00:11:37.402)
        Context Switch Count      40
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x0000000076e17860)
        Stack Init fffff9800b3b2db0 Current fffff9800b3b2260
        Base fffff9800b3b3000 Limit fffff9800b3ad000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0b3b22a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0b3b23e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0b3b2440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0b3b24b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0b3b2960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0b3b2bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0b3b2c20)
        00000000`01d3f758 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`01d3f760 00000000`ff0a1a0b kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`01d3f870 00000000`76df6500 lsm!CPolicyMonitor::PolicyMonitorWorker+0x26f
        00000000`01d3f8d0 00000000`76e17b59 ntdll!RtlpTpWorkCallback+0xf0
        00000000`01d3f980 00000000`76bfcdcd ntdll!TppWorkerThread+0x3ad
        00000000`01d3fbf0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`01d3fc20 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8002174200  Cid 0290.030c  Teb: 000007fffffa8000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa80043e77c0  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80042a4c10       Image:         lsm.exe
        Wait Start TickCount      46345          Ticks: 234 (0:00:00:03.650)
        Context Switch Count      8
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff980157cadb0 Current fffff980157ca810
        Base fffff980157cb000 Limit fffff980157c5000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`157ca850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`157ca990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`157ca9f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`157caa80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`157cab00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`157cabb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`157cac20)
        00000000`0154f9a8 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`0154f9b0 000007fe`fedce7a3 kernel32!GetQueuedCompletionStatus+0x48
        00000000`0154fa10 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`0154faa0 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`0154fb50 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`0154fb80 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`0154fbc0 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`0154fbf0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0154fc20 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

Svchost process (DcomLaunch)

```
PROCESS fffffa8004297040
    SessionId: 0  Cid: 0338    Peb: 7fffffdf000  ParentCid: 025c
    DirBase: 4f414000  ObjectTable: fffff8800589ceb0  HandleCount: 305.
    Image: svchost.exe
    VadRoot fffffa8004297440 Vads 94 Clone 0 Private 601. Modified 327. Locked 0.
    DeviceMap fffff88000007820
    Token                             fffff8800598daa0
    ElapsedTime                       00:11:43.906
    UserTime                          00:00:00.265
    KernelTime                        00:00:01.216
    QuotaPoolUsage[PagedPool]         109120
    QuotaPoolUsage[NonPagedPool]      9872
    Working Set Sizes (now,min,max)  (1635, 50, 345) (6540KB, 200KB, 1380KB)
    PeakWorkingSetSize                1961
    VirtualSize                       52 Mb
    PeakVirtualSize                   56 Mb
    PageFaultCount                    17109
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      818

    Setting context for this process...
.process /p /r fffffa8004297040

    !peb
PEB at 000007fffffdf000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00000000ff910000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 0000000000172740 . 00000000001fcc50
    Ldr.InLoadOrderModuleList:           0000000000172650 . 00000000001fcc30
    Ldr.InMemoryOrderModuleList:         0000000000172660 . 00000000001fcc40
            Base TimeStamp                     Module
        ff910000 4549b5f5 Nov 02 09:10:13 2006 C:\Windows\system32\svchost.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        76bc0000 4549d328 Nov 02 11:14:48 2006 C:\Windows\system32\kernel32.dll
     7fefdd40000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\system32\msvcrt.dll
     7fefea30000 4549d267 Nov 02 11:11:35 2006 C:\Windows\system32\ADVAPI32.dll
     7fefed90000 469c43bb Jul 17 05:21:15 2007 C:\Windows\system32\RPCRT4.dll
     7fefc510000 4549d32c Nov 02 11:14:52 2006 c:\windows\system32\umpnpmgr.dll
        76d00000 45d3ee19 Feb 15 05:22:33 2007 C:\Windows\system32\USER32.dll
     7fefec20000 4549d273 Nov 02 11:11:47 2006 C:\Windows\system32\GDI32.dll
     7fefd3b0000 4549d336 Nov 02 11:15:02 2006 c:\windows\system32\USERENV.dll
     7fefd390000 4549d33f Nov 02 11:15:11 2006 c:\windows\system32\Secur32.dll
     7fefd9e0000 4549d2cb Nov 02 11:13:15 2006 C:\Windows\system32\IMM32.DLL
     7fefdc30000 4549d2e6 Nov 02 11:13:42 2006 C:\Windows\system32\MSCTF.dll
     7feff0c0000 4549d2a1 Nov 02 11:12:33 2006 C:\Windows\system32\LPK.DLL
     7fefd940000 4549d337 Nov 02 11:15:03 2006 C:\Windows\system32\USP10.dll
     7fefc580000 4549d351 Nov 02 11:15:29 2006 C:\Windows\system32\POWRPROF.dll
     7fefc940000 4549d277 Nov 02 11:11:51 2006 C:\Windows\system32\GPAPI.dll
     7fefcc20000 4549d32d Nov 02 11:14:53 2006 C:\Windows\system32\slc.dll
     7fefc390000 4549d31b Nov 02 11:14:35 2006 c:\windows\system32\rpcss.dll
     7fefd540000 4549d38a Nov 02 11:16:26 2006 C:\Windows\system32\WS2_32.dll
     7feff0b0000 4549d370 Nov 02 11:16:00 2006 C:\Windows\system32\NSI.dll
     7fefc460000 466785ee Jun 07 05:13:34 2007 c:\windows\system32\FirewallAPI.dll
     7fefdab0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\OLEAUT32.dll
     7fefd760000 4549d317 Nov 02 11:14:31 2006 C:\Windows\system32\ole32.dll
     7fefca50000 4549d336 Nov 02 11:15:02 2006 c:\windows\system32\VERSION.dll
     7fefca40000 4549d341 Nov 02 11:15:13 2006 C:\Windows\system32\credssp.dll
     7fefcc50000 4549d344 Nov 02 11:15:16 2006 C:\Windows\system32\CRYPT32.dll
     7fefce00000 4549d2df Nov 02 11:13:35 2006 C:\Windows\system32\MSASN1.dll
     7fefc670000 4549d321 Nov 02 11:14:41 2006 C:\Windows\system32\schannel.dll
```

```
     7fefcf70000 4549d2fc Nov 02 11:14:04 2006 C:\Windows\system32\NETAPI32.dll
     7fefd530000 4549d310 Nov 02 11:14:24 2006 C:\Windows\system32\PSAPI.DLL
     7fefeed0000 4549d318 Nov 02 11:14:32 2006 C:\Windows\system32\SETUPAPI.dll
     7fefc1c0000 4549d251 Nov 02 11:11:13 2006 C:\Windows\system32\Cabinet.dll
     7fefc5b0000 4549d384 Nov 02 11:16:20 2006 C:\Windows\system32\NTMARTA.DLL
     7fefd590000 4549d396 Nov 02 11:16:38 2006 C:\Windows\system32\WLDAP32.dll
     7fefce20000 4549d315 Nov 02 11:14:29 2006 C:\Windows\system32\SAMLIB.dll
     7fefd1b0000 4549d380 Nov 02 11:16:16 2006 C:\Windows\system32\WINSTA.dll
     7fefdb90000 4549d282 Nov 02 11:12:02 2006 C:\Windows\system32\CLBCatQ.DLL
     7fefd310000 4549d247 Nov 02 11:11:03 2006 C:\Windows\system32\apphelp.dll
     7fefc450000 4549d34e Nov 02 11:15:26 2006 C:\Windows\system32\WTSAPI32.dll
     7fef8830000 4549d31b Nov 02 11:14:35 2006 C:\Windows\system32\msi.dll
     7fef9e10000 4549d323 Nov 02 11:14:43 2006 C:\Windows\system32\msiltcfg.dll
     7fef9770000 4549d31c Nov 02 11:14:36 2006 C:\Windows\system32\SFC.DLL
     7fef97e0000 4549d31d Nov 02 11:14:37 2006 C:\Windows\system32\sfc_os.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       0000000000170000
    ProcessParameters: 0000000000171d20
    WindowTitle:  'C:\Windows\system32\svchost.exe'
    ImageFile:    'C:\Windows\system32\svchost.exe'
    CommandLine:  'C:\Windows\system32\svchost.exe -k DcomLaunch'
    DllPath:
'C:\Windows\system32;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Wind
ows;C:\Windows\System32\Wbem'
    Environment:  0000000000171310
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\system32\config\systemprofile\AppData\Roaming
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        LOCALAPPDATA=C:\Windows\system32\config\systemprofile\AppData\Local
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\TEMP
        TMP=C:\Windows\TEMP
        USERDOMAIN=DOMAIN
        USERNAME=COMPUTERNAME$
        USERPROFILE=C:\Windows\system32\config\systemprofile
        windir=C:\Windows
```

```
        THREAD fffffa80043a2bb0  Cid 0338.033c  Teb: 000007fffffdd000 Win32Thread: 0000000000000000
WAIT: (Executive) UserMode Non-Alertable
            fffffa80043a5a58  NotificationEvent
        IRP List:
            fffffa80043a2470: (0006,0118) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004297040       Image:         svchost.exe
        Wait Start TickCount      2774           Ticks: 43805 (0:00:11:23.362)
        Context Switch Count      308
        UserTime                  00:00:00.015
        KernelTime                00:00:00.093
        Win32 Start Address svchost!wmainCRTStartup (0x00000000ff912550)
        Stack Init fffff9800ba74db0 Current fffff9800ba747f0
        Base fffff9800ba75000 Limit fffff9800ba6f000 Call 0
        Priority 13 BasePriority 8 PriorityDecrement 3 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0ba74830 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0ba74970 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0ba749d0 fffff800`01ebdf16 nt!KeWaitForSingleObject+0x5f5
        fffff980`0ba74a50 fffff800`01ea1a24 nt!IopSynchronousServiceTail+0x306
        fffff980`0ba74ac0 fffff800`01c4d733 nt!NtReadFile+0x583
        fffff980`0ba74bb0 00000000`76e202da nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0ba74c20)
        00000000`0016f758 00000000`76bf26da ntdll!NtReadFile+0xa
        00000000`0016f760 000007fe`fea865aa kernel32!ReadFile+0x8a
        00000000`0016f7f0 000007fe`fea862e3 ADVAPI32!ScGetPipeInput+0x4a
        00000000`0016f8d0 000007fe`fea850f3 ADVAPI32!ScDispatcherLoop+0x9a
        00000000`0016f9d0 00000000`ff91283c ADVAPI32!StartServiceCtrlDispatcherW+0x176
        00000000`0016fc70 00000000`ff912666 svchost!wmain+0xe5
        00000000`0016fca0 00000000`76bfcdcd svchost!ScCreateWellKnownSids+0x301
        00000000`0016fce0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0016fd10 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80043de060  Cid 0338.0348  Teb: 000007fffffd7000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa800430e040  SynchronizationTimer
            fffffa800430ae10  SynchronizationEvent
            fffffa80042cb5f0  SynchronizationEvent
            fffffa80043aacb0  SynchronizationTimer
            fffffa80043aab60  SynchronizationTimer
            fffffa80043c3cd0  SynchronizationEvent
            fffffa80043cfb60  SynchronizationEvent
            fffffa80043cf920  SynchronizationEvent
            fffffa80043db790  SynchronizationEvent
            fffffa80043dba30  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004297040       Image:         svchost.exe
        Wait Start TickCount      1534           Ticks: 45045 (0:00:11:42.706)
        Context Switch Count      17
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x0000000076df6930)
        Stack Init fffff9800b3cedb0 Current fffff9800b3ce260
        Base fffff9800b3cf000 Limit fffff9800b3c9000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0b3ce2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0b3ce3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0b3ce440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0b3ce4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0b3ce960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0b3cebb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0b3cec20)
        00000000`00c2fbf8 00000000`76df6b07 ntdll!NtWaitForMultipleObjects+0xa
        00000000`00c2fc00 00000000`76bfcdcd ntdll!TppWaiterpThread+0x14d
        00000000`00c2fea0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`00c2fed0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004383bb0  Cid 0338.0354  Teb: 000007fffffae000 Win32Thread: fffff900c07d38d0
WAIT: (UserRequest) UserMode Alertable
            fffffa8001840748  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004297040       Image:         svchost.exe
        Wait Start TickCount      43120          Ticks: 3459 (0:00:00:53.960)
        Context Switch Count      199                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address umpnpmgr!DeviceEventThreadProc (0x000007fefc51d4b0)
        Stack Init fffff9800d0f5db0 Current fffff9800d0f5980
        Base fffff9800d0f6000 Limit fffff9800d0ef000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0d0f59c0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0d0f5b00 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0d0f5b60 fffff800`01e77fc2 nt!KeWaitForSingleObject+0x5f5
        fffff980`0d0f5be0 fffff800`01c4d733 nt!NtGetPlugPlayEvent+0xc2
        fffff980`0d0f5c20 00000000`76e20fba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0d0f5c20)
        00000000`010bf5a8 000007fe`fc51d541 ntdll!ZwGetPlugPlayEvent+0xa
        00000000`010bf5b0 00000000`76bfcdcd umpnpmgr!DeviceEventThreadProc+0xc0
        00000000`010bfa50 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`010bfa80 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80043d0060  Cid 0338.037c  Teb: 000007fffffdb000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Alertable
            fffffa80043dbbd0  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004297040       Image:         svchost.exe
        Wait Start TickCount      1534           Ticks: 45045 (0:00:11:42.706)
        Context Switch Count      6
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x0000000076e17860)
        Stack Init fffff9800baacdb0 Current fffff9800baac860
        Base fffff9800baad000 Limit fffff9800baa7000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0baac8a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0baac9e0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0baaca40 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0baacad0 fffff800`01c8a722 nt!IoRemoveIoCompletion+0x47
        fffff980`0baacb50 fffff800`01c4d733 nt!NtWaitForWorkViaWorkerFactory+0x1f1
        fffff980`0baacc20 00000000`76e21b4a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0baacc20)
        00000000`0188fa68 00000000`76e17a20 ntdll!NtWaitForWorkViaWorkerFactory+0xa
        00000000`0188fa70 00000000`76bfcdcd ntdll!TppWorkerThread+0x23e
        00000000`0188fce0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0188fd10 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80043d09f0  Cid 0338.0380  Teb: 000007fffffaa000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Alertable
            fffffa80043c3c40  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004297040       Image:         svchost.exe
        Wait Start TickCount      1534           Ticks: 45045 (0:00:11:42.706)
        Context Switch Count      6
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x0000000076e17860)
        Stack Init fffff9800c25fdb0 Current fffff9800c25f860
        Base fffff9800c260000 Limit fffff9800c25a000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0c25f8a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0c25f9e0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0c25fa40 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0c25fad0 fffff800`01c8a722 nt!IoRemoveIoCompletion+0x47
        fffff980`0c25fb50 fffff800`01c4d733 nt!NtWaitForWorkViaWorkerFactory+0x1f1
        fffff980`0c25fc20 00000000`76e21b4a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0c25fc20)
        00000000`01aff5a8 00000000`76e17a20 ntdll!NtWaitForWorkViaWorkerFactory+0xa
        00000000`01aff5b0 00000000`76bfcdcd ntdll!TppWorkerThread+0x23e
        00000000`01aff820 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`01aff850 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8003dcc720  Cid 0338.0b80  Teb: 000007fffffa8000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8003d8fdf0  NotificationEvent
            fffffa80048c5880  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004297040       Image:         svchost.exe
        Wait Start TickCount      3450           Ticks: 43129 (0:00:11:12.816)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address msiltcfg!WorkerThread (0x000007fef9e12148)
        Stack Init fffff9800ba82db0 Current fffff9800ba82260
        Base fffff9800ba83000 Limit fffff9800ba7d000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0ba822a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0ba823e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0ba82440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0ba824b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0ba82960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0ba82bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0ba82c20)
        00000000`0240f7b8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0240f7c0 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0240f8d0 000007fe`f9e121ce kernel32!WaitForMultipleObjects+0x11
        00000000`0240f910 00000000`76bfcdcd msiltcfg!WorkerThread+0x86
        00000000`0240f9a0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0240f9d0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004b3c4f0  Cid 0338.0b24  Teb: 000007fffffd9000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa80043a6fb0  QueueObject
            fffffa8004b3c5a8  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004297040       Image:         svchost.exe
        Wait Start TickCount      45573          Ticks: 1006 (0:00:00:15.693)
        Context Switch Count      17
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff980014b9db0 Current fffff980014b9810
        Base fffff980014ba000 Limit fffff980014b4000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`014b9850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`014b9990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`014b99f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`014b9a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`014b9b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`014b9bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`014b9c20)
        00000000`011afbf8 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`011afc00 000007fe`fedce7a3 kernel32!GetQueuedCompletionStatus+0x48
        00000000`011afc60 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`011afcf0 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`011afda0 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`011afdd0 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`011afe10 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`011afe40 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`011afe70 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80023a3a50  Cid 0338.08b0  Teb: 000007fffffd5000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa80043a6fb0  QueueObject
            fffffa80023a3b08  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004297040       Image:         svchost.exe
        Wait Start TickCount      45573          Ticks: 1006 (0:00:00:15.693)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff9801db7adb0 Current fffff9801db7a810
        Base fffff9801db7b000 Limit fffff9801db75000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1db7a850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1db7a990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`1db7a9f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`1db7aa80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`1db7ab00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`1db7abb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1db7ac20)
        00000000`01b9fa98 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`01b9faa0 000007fe`fedce7a3 kernel32!GetQueuedCompletionStatus+0x48
        00000000`01b9fb00 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`01b9fb90 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`01b9fc40 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`01b9fc70 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`01b9fcb0 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`01b9fce0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`01b9fd10 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

Svchost process (rpcss)

```
PROCESS fffffa80042d1c10
    SessionId: 0  Cid: 0388    Peb: 7fffffda000  ParentCid: 025c
    DirBase: 4ebe5000  ObjectTable: fffff8800497eda0  HandleCount: 331.
    Image: svchost.exe
    VadRoot fffffa80043dd330 Vads 90 Clone 0 Private 962. Modified 367. Locked 2.
    DeviceMap fffff8800598a680
    Token                             fffff880058c7a30
    ElapsedTime                       00:11:43.282
    UserTime                          00:00:00.234
    KernelTime                        00:00:00.546
    QuotaPoolUsage[PagedPool]         120312
    QuotaPoolUsage[NonPagedPool]      15600
    Working Set Sizes (now,min,max)  (1845, 50, 345) (7380KB, 200KB, 1380KB)
    PeakWorkingSetSize                2232
    VirtualSize                       54 Mb
    PeakVirtualSize                   56 Mb
    PageFaultCount                    2967
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      1190

    Setting context for this process...
.process /p /r fffffa80042d1c10

    !peb
PEB at 000007fffffda000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00000000ff910000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00000000002727b0 . 00000000020616d0
    Ldr.InLoadOrderModuleList:           00000000002726c0 . 0000000002061780
    Ldr.InMemoryOrderModuleList:         00000000002726d0 . 0000000002061790
            Base TimeStamp                     Module
        ff910000 4549b5f5 Nov 02 09:10:13 2006 C:\Windows\system32\svchost.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        76bc0000 4549d328 Nov 02 11:14:48 2006 C:\Windows\system32\kernel32.dll
     7fefdd40000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\system32\msvcrt.dll
     7fefea30000 4549d267 Nov 02 11:11:35 2006 C:\Windows\system32\ADVAPI32.dll
     7fefed90000 469c43bb Jul 17 05:21:15 2007 C:\Windows\system32\RPCRT4.dll
     7fefc390000 4549d31b Nov 02 11:14:35 2006 c:\windows\system32\rpcss.dll
     7fefd540000 4549d38a Nov 02 11:16:26 2006 C:\Windows\system32\WS2_32.dll
     7feff0b0000 4549d370 Nov 02 11:16:00 2006 C:\Windows\system32\NSI.dll
     7fefd390000 4549d33f Nov 02 11:15:11 2006 c:\windows\system32\Secur32.dll
     7fefc460000 466785ee Jun 07 05:13:34 2007 c:\windows\system32\FirewallAPI.dll
        76d00000 45d3ee19 Feb 15 05:22:33 2007 C:\Windows\system32\USER32.dll
     7fefec20000 4549d273 Nov 02 11:11:47 2006 C:\Windows\system32\GDI32.dll
     7fefdab0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\OLEAUT32.dll
     7fefd760000 4549d317 Nov 02 11:14:31 2006 C:\Windows\system32\ole32.dll
     7fefca50000 4549d336 Nov 02 11:15:02 2006 c:\windows\system32\VERSION.dll
     7fefd9e0000 4549d2cb Nov 02 11:13:15 2006 C:\Windows\system32\IMM32.DLL
     7fefdc30000 4549d2e6 Nov 02 11:13:42 2006 C:\Windows\system32\MSCTF.dll
     7feff0c0000 4549d2a1 Nov 02 11:12:33 2006 C:\Windows\system32\LPK.DLL
     7fefd940000 4549d337 Nov 02 11:15:03 2006 C:\Windows\system32\USP10.dll
     7fefca40000 4549d341 Nov 02 11:15:13 2006 C:\Windows\system32\credssp.dll
     7fefcc50000 4549d344 Nov 02 11:15:16 2006 C:\Windows\system32\CRYPT32.dll
     7fefce00000 4549d2df Nov 02 11:13:35 2006 C:\Windows\system32\MSASN1.dll
     7fefd3b0000 4549d336 Nov 02 11:15:02 2006 C:\Windows\system32\USERENV.dll
     7fefc670000 4549d321 Nov 02 11:14:41 2006 C:\Windows\system32\schannel.dll
     7fefcf70000 4549d2fc Nov 02 11:14:04 2006 C:\Windows\system32\NETAPI32.dll
     7fefd530000 4549d310 Nov 02 11:14:24 2006 C:\Windows\system32\PSAPI.DLL
     7fefc620000 4549d31d Nov 02 11:14:37 2006 C:\Windows\system32\rsaenh.dll
     7fefc8f0000 4549d2e7 Nov 02 11:13:43 2006 C:\Windows\system32\mswsock.dll
```

```
     7fefc560000 4549d3a3 Nov 02 11:16:51 2006 C:\Windows\system32\wshtcpip.dll
     7fefc980000 4549d39d Nov 02 11:16:45 2006 C:\Windows\System32\wship6.dll
     7fefdb90000 4549d282 Nov 02 11:12:02 2006 C:\Windows\system32\CLBCatQ.DLL
     7fefac60000 4549d280 Nov 02 11:12:00 2006 C:\Windows\system32\fwpuclnt.dll
     7fef8830000 4549d31b Nov 02 11:14:35 2006 C:\Windows\system32\msi.dll
     7fef9e10000 4549d323 Nov 02 11:14:43 2006 C:\Windows\system32\msiltcfg.dll
     7fefc5b0000 4549d384 Nov 02 11:16:20 2006 C:\Windows\system32\NTMARTA.DLL
     7fefd590000 4549d396 Nov 02 11:16:38 2006 C:\Windows\system32\WLDAP32.dll
     7fefce20000 4549d315 Nov 02 11:14:29 2006 C:\Windows\system32\SAMLIB.dll
     7fef9770000 4549d31c Nov 02 11:14:36 2006 C:\Windows\system32\SFC.DLL
     7fef97e0000 4549d31d Nov 02 11:14:37 2006 C:\Windows\system32\sfc_os.dll
     7fefeed0000 4549d318 Nov 02 11:14:32 2006 C:\Windows\system32\SETUPAPI.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       0000000000270000
    ProcessParameters: 0000000000271da0
    WindowTitle:  'C:\Windows\system32\svchost.exe'
    ImageFile:    'C:\Windows\system32\svchost.exe'
    CommandLine:  'C:\Windows\system32\svchost.exe -k rpcss'
    DllPath:
'C:\Windows\system32;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Wind
ows;C:\Windows\System32\Wbem'
    Environment:  0000000000271310
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        LOCALAPPDATA=C:\Windows\ServiceProfiles\NetworkService\AppData\Local
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\SERVIC~2\NETWOR~1\AppData\Local\Temp
        TMP=C:\Windows\SERVIC~2\NETWOR~1\AppData\Local\Temp
        USERDOMAIN=DOMAIN
        USERNAME=COMPUTERNAME$
        USERPROFILE=C:\Windows\ServiceProfiles\NetworkService
        windir=C:\Windows
```

```
        THREAD fffffa80043e2060  Cid 0388.038c  Teb: 000007fffffde000 Win32Thread: 0000000000000000
WAIT: (Executive) UserMode Non-Alertable
            fffffa800442cfb8  NotificationEvent
        IRP List:
            fffffa80043c44f0: (0006,0118) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa80042d1c10       Image:         svchost.exe
        Wait Start TickCount      1542           Ticks: 45037 (0:00:11:42.581)
        Context Switch Count      12
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address svchost!wmainCRTStartup (0x00000000ff912550)
        Stack Init fffff9800c282db0 Current fffff9800c2827f0
        Base fffff9800c283000 Limit fffff9800c27d000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0c282830 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0c282970 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0c2829d0 fffff800`01ebdf16 nt!KeWaitForSingleObject+0x5f5
        fffff980`0c282a50 fffff800`01ea1a24 nt!IopSynchronousServiceTail+0x306
        fffff980`0c282ac0 fffff800`01c4d733 nt!NtReadFile+0x583
        fffff980`0c282bb0 00000000`76e202da nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0c282c20)
        00000000`000cf7d8 00000000`76bf26da ntdll!NtReadFile+0xa
        00000000`000cf7e0 000007fe`fea865aa kernel32!ReadFile+0x8a
        00000000`000cf870 000007fe`fea862e3 ADVAPI32!ScGetPipeInput+0x4a
        00000000`000cf950 000007fe`fea850f3 ADVAPI32!ScDispatcherLoop+0x9a
        00000000`000cfa50 00000000`ff91283c ADVAPI32!StartServiceCtrlDispatcherW+0x176
        00000000`000cfcf0 00000000`ff912666 svchost!wmain+0xe5
        00000000`000cfd20 00000000`76bfcdcd svchost!ScCreateWellKnownSids+0x301
        00000000`000cfd60 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`000cfd90 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80042d1780  Cid 0388.0390  Teb: 000007fffffdc000 Win32Thread: fffff900c07c24e0
WAIT: (DelayExecution) UserMode Non-Alertable
            fffffa80042d1838  NotificationTimer
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa80042d1c10       Image:         svchost.exe
        Wait Start TickCount      45292          Ticks: 1287 (0:00:00:20.077)
        Context Switch Count      97                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address ADVAPI32!ScSvcctrlThreadW (0x000007fefea84bd0)
        Stack Init fffff9800d1a0db0 Current fffff9800d1a0990
        Base fffff9800d1a1000 Limit fffff9800d19a000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0d1a09d0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0d1a0b10 fffff800`01c5b5a9 nt!KiSwapThread+0x125
        fffff980`0d1a0b70 fffff800`01e8ae9d nt!KeDelayExecutionThread+0x339
        fffff980`0d1a0bf0 fffff800`01c4d733 nt!NtDelayExecution+0x5c
        fffff980`0d1a0c20 00000000`76e205ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0d1a0c20)
        00000000`0083f318 00000000`76bfd908 ntdll!NtDelayExecution+0xa
        00000000`0083f320 000007fe`fc3ba8c0 kernel32!SleepEx+0x84
        00000000`0083f3a0 000007fe`fc3b17bd rpcss!ObjectExporterWorkerThread+0x50b
        00000000`0083f470 000007fe`fc3b27f2 rpcss!ScmServiceMain+0xe4
        00000000`0083f4a0 00000000`ff911771 rpcss!ServiceMain+0x251
        00000000`0083f760 000007fe`fea84bf5 svchost!ServiceStarter+0x1ea
        00000000`0083f7f0 00000000`76bfcdcd ADVAPI32!ScSvcctrlThreadW+0x25
        00000000`0083f820 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0083f850 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80043e4060  Cid 0388.0394  Teb: 000007fffffd8000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa800442c320  SynchronizationTimer
            fffffa80043ce290  SynchronizationEvent
            fffffa80043e7bf0  SynchronizationEvent
            fffffa80043e7b10  SynchronizationEvent
            fffffa8004422260  SynchronizationEvent
            fffffa8004645820  SynchronizationEvent
            fffffa8004423b60  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa80042d1c10       Image:         svchost.exe
        Wait Start TickCount      40111          Ticks: 6468 (0:00:01:40.901)
        Context Switch Count      22
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x0000000076df6930)
        Stack Init fffff9800c289db0 Current fffff9800c289260
        Base fffff9800c28a000 Limit fffff9800c284000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0c2892a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0c2893e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0c289440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0c2894b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0c289960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0c289bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0c289c20)
        00000000`0188fca8 00000000`76df6b07 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0188fcb0 00000000`76bfcdcd ntdll!TppWaiterpThread+0x14d
        00000000`0188ff50 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0188ff80 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80043571f0  Cid 0388.0584  Teb: 000007fffffa8000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Alertable
            fffffa800442cc20  QueueObject
        IRP List:
            fffffa8004865e10: (0006,01f0) Flags: 00060030  Mdl: 00000000
            fffffa8004233830: (0006,01f0) Flags: 00060030  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa80042d1c10       Image:         svchost.exe
        Wait Start TickCount      1983           Ticks: 44596 (0:00:11:35.702)
        Context Switch Count      29
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x0000000076e17860)
        Stack Init fffff9800e2c8db0 Current fffff9800e2c8860
        Base fffff9800e2c9000 Limit fffff9800e2c3000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e2c88a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e2c89e0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0e2c8a40 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0e2c8ad0 fffff800`01c8a722 nt!IoRemoveIoCompletion+0x47
        fffff980`0e2c8b50 fffff800`01c4d733 nt!NtWaitForWorkViaWorkerFactory+0x1f1
        fffff980`0e2c8c20 00000000`76e21b4a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e2c8c20)
        00000000`0229f838 00000000`76e17a20 ntdll!NtWaitForWorkViaWorkerFactory+0xa
        00000000`0229f840 00000000`76bfcdcd ntdll!TppWorkerThread+0x23e
        00000000`0229fab0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0229fae0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800491fbb0  Cid 0388.089c  Teb: 000007fffffa6000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800468a5b0  NotificationEvent
            fffffa80048c5880  NotificationEvent
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa80042d1c10       Image:         svchost.exe
        Wait Start TickCount      2015           Ticks: 44564 (0:00:11:35.202)
        Context Switch Count      15
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address msiltcfg!WorkerThread (0x000007fef9e12148)
        Stack Init fffff9801031fdb0 Current fffff9801031f260
        Base fffff98010320000 Limit fffff9801031a000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1031f2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1031f3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`1031f440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`1031f4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`1031f960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`1031fbb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1031fc20)
        00000000`00cdfd08 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`00cdfd10 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`00cdfe20 000007fe`f9e121ce kernel32!WaitForMultipleObjects+0x11
        00000000`00cdfe60 00000000`76bfcdcd msiltcfg!WorkerThread+0x86
        00000000`00cdfef0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`00cdff20 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004890bb0  Cid 0388.0e48  Teb: 000007fffffae000 Win32Thread: 0000000000000000
WAIT: (DelayExecution) UserMode Non-Alertable
            fffffa8004890c68  NotificationTimer
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa80042d1c10       Image:         svchost.exe
        Wait Start TickCount      44010          Ticks: 2569 (0:00:00:40.076)
        Context Switch Count      80
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address rpcss!ObjectExporterTaskThread (0x000007fefc3c5ec0)
        Stack Init fffff98012f9ddb0 Current fffff98012f9d990
        Base fffff98012f9e000 Limit fffff98012f98000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`12f9d9d0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12f9db10 fffff800`01c5b5a9 nt!KiSwapThread+0x125
        fffff980`12f9db70 fffff800`01e8ae9d nt!KeDelayExecutionThread+0x339
        fffff980`12f9dbf0 fffff800`01c4d733 nt!NtDelayExecution+0x5c
        fffff980`12f9dc20 00000000`76e205ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12f9dc20)
        00000000`0200fa68 00000000`76bfd908 ntdll!NtDelayExecution+0xa
        00000000`0200fa70 000007fe`fc3c5fa3 kernel32!SleepEx+0x84
        00000000`0200faf0 00000000`76bfcdcd rpcss!ObjectExporterTaskThread+0x115
        00000000`0200fb30 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0200fb60 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004513740  Cid 0388.0a3c  Teb: 000007fffffd6000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa80043e2590  QueueObject
            fffffa80045137f8  NotificationTimer
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa80042d1c10       Image:         svchost.exe
        Wait Start TickCount      46323          Ticks: 256 (0:00:00:03.993)
        Context Switch Count      123
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff98012fabdb0 Current fffff98012fab810
        Base fffff98012fac000 Limit fffff98012fa6000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`12fab850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12fab990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`12fab9f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`12faba80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`12fabb00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`12fabbb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12fabc20)
        00000000`00c5fd08 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`00c5fd10 000007fe`fedce7a3 kernel32!GetQueuedCompletionStatus+0x48
        00000000`00c5fd70 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`00c5fe00 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`00c5feb0 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`00c5fee0 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`00c5ff20 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`00c5ff50 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`00c5ff80 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80025b5700  Cid 0388.0e80  Teb: 000007fffffd4000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa80043e2590  QueueObject
            fffffa80025b57b8  NotificationTimer
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa80042d1c10       Image:         svchost.exe
        Wait Start TickCount      46323          Ticks: 256 (0:00:00:03.993)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff98004fc0db0 Current fffff98004fc0810
        Base fffff98004fc1000 Limit fffff98004fbb000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`04fc0850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`04fc0990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`04fc09f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`04fc0a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`04fc0b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`04fc0bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`04fc0c20)
        00000000`01f5f6f8 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`01f5f700 000007fe`fedce7a3 kernel32!GetQueuedCompletionStatus+0x48
        00000000`01f5f760 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`01f5f7f0 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`01f5f8a0 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`01f5f8d0 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`01f5f910 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`01f5f940 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`01f5f970 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

Ati2evxx process (session 0)

```
PROCESS fffffa80044c0040
    SessionId: 0  Cid: 0118    Peb: 7fffffd9000  ParentCid: 025c
    DirBase: 4e067000  ObjectTable: fffff8800586a4d0  HandleCount:  97.
    Image: Ati2evxx.exe
    VadRoot fffffa800438fe00 Vads 58 Clone 0 Private 333. Modified 247. Locked 0.
    DeviceMap fffff88000007820
    Token                             fffff88005a09c40
    ElapsedTime                       00:11:43.017
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         99920
    QuotaPoolUsage[NonPagedPool]      5600
    Working Set Sizes (now,min,max)  (831, 50, 345) (3324KB, 200KB, 1380KB)
    PeakWorkingSetSize                1213
    VirtualSize                       51 Mb
    PeakVirtualSize                   52 Mb
    PageFaultCount                    1275
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      427

    Setting context for this process...
.process /p /r fffffa80044c0040

    !peb
PEB at 000007fffffd9000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         0000000000400000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 0000000000692740 . 00000000006bc490
    Ldr.InLoadOrderModuleList:           0000000000692650 . 00000000006bc7b0
    Ldr.InMemoryOrderModuleList:         0000000000692660 . 00000000006bc7c0
            Base TimeStamp                     Module
          400000 453ec111 Oct 25 02:42:41 2006 C:\Windows\system32\Ati2evxx.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        76bc0000 4549d328 Nov 02 11:14:48 2006 C:\Windows\system32\kernel32.dll
        76d00000 45d3ee19 Feb 15 05:22:33 2007 C:\Windows\system32\USER32.dll
     7fefec20000 4549d273 Nov 02 11:11:47 2006 C:\Windows\system32\GDI32.dll
     7fefea30000 4549d267 Nov 02 11:11:35 2006 C:\Windows\system32\ADVAPI32.dll
     7fefed90000 469c43bb Jul 17 05:21:15 2007 C:\Windows\system32\RPCRT4.dll
     7fefd760000 4549d317 Nov 02 11:14:31 2006 C:\Windows\system32\ole32.dll
     7fefdd40000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\system32\msvcrt.dll
     7fefdab0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\OLEAUT32.dll
     7fefd9e0000 4549d2cb Nov 02 11:13:15 2006 C:\Windows\system32\IMM32.DLL
     7fefdc30000 4549d2e6 Nov 02 11:13:42 2006 C:\Windows\system32\MSCTF.dll
     7feff0c0000 4549d2a1 Nov 02 11:12:33 2006 C:\Windows\system32\LPK.DLL
     7fefd940000 4549d337 Nov 02 11:15:03 2006 C:\Windows\system32\USP10.dll
     7fefd3b0000 4549d336 Nov 02 11:15:02 2006 C:\Windows\system32\userenv.dll
     7fefd390000 4549d33f Nov 02 11:15:11 2006 C:\Windows\system32\Secur32.dll
     7fefc580000 4549d351 Nov 02 11:15:29 2006 C:\Windows\system32\powrprof.dll
     7fefd530000 4549d310 Nov 02 11:14:24 2006 C:\Windows\system32\psapi.dll
     7fefc320000 4549d398 Nov 02 11:16:40 2006 C:\Windows\system32\wls0wndh.dll
     7fefd1b0000 4549d380 Nov 02 11:16:16 2006 C:\Windows\system32\WINSTA.dll
     7fefd310000 4549d247 Nov 02 11:11:03 2006 C:\Windows\system32\apphelp.dll
     7fefc5b0000 4549d384 Nov 02 11:16:20 2006 C:\Windows\system32\NTMARTA.DLL
     7fefd590000 4549d396 Nov 02 11:16:38 2006 C:\Windows\system32\WLDAP32.dll
     7fefd540000 4549d38a Nov 02 11:16:26 2006 C:\Windows\system32\WS2_32.dll
     7feff0b0000 4549d370 Nov 02 11:16:00 2006 C:\Windows\system32\NSI.dll
     7fefce20000 4549d315 Nov 02 11:14:29 2006 C:\Windows\system32\SAMLIB.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       0000000000690000
    ProcessParameters: 0000000000691d20
```

```
    WindowTitle:  'C:\Windows\system32\Ati2evxx.exe'
    ImageFile:    'C:\Windows\system32\Ati2evxx.exe'
    CommandLine:  'C:\Windows\system32\Ati2evxx.exe'
    DllPath:
'C:\Windows\system32;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Wind
ows;C:\Windows\System32\Wbem'
    Environment:  0000000000691310
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\system32\config\systemprofile\AppData\Roaming
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        LOCALAPPDATA=C:\Windows\system32\config\systemprofile\AppData\Local
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\TEMP
        TMP=C:\Windows\TEMP
        USERDOMAIN=DOMAIN
        USERNAME=COMPUTERNAME$
        USERPROFILE=C:\Windows\system32\config\systemprofile
        windir=C:\Windows
```

```
        THREAD fffffa8004490060  Cid 0118.0120  Teb: 000007fffffde000 Win32Thread: fffff900c07c9a60
WAIT: (Executive) UserMode Non-Alertable
            fffffa800437ed58  NotificationEvent
        IRP List:
            fffffa8004363010: (0006,0118) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044c0040       Image:         Ati2evxx.exe
        Wait Start TickCount      2768           Ticks: 43811 (0:00:11:23.455)
        Context Switch Count      68                 LargeStack
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address Ati2evxx (0x0000000000456a30)
        Stack Init fffff9800d108db0 Current fffff9800d1087f0
        Base fffff9800d109000 Limit fffff9800d102000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0d108830 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0d108970 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0d1089d0 fffff800`01ebdf16 nt!KeWaitForSingleObject+0x5f5
        fffff980`0d108a50 fffff800`01ea1a24 nt!IopSynchronousServiceTail+0x306
        fffff980`0d108ac0 fffff800`01c4d733 nt!NtReadFile+0x583
        fffff980`0d108bb0 00000000`76e202da nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0d108c20)
        00000000`0012f5e8 00000000`76bf26da ntdll!NtReadFile+0xa
        00000000`0012f5f0 000007fe`fea865aa kernel32!ReadFile+0x8a
        00000000`0012f680 000007fe`fea862e3 ADVAPI32!ScGetPipeInput+0x4a
        00000000`0012f760 000007fe`feadea5d ADVAPI32!ScDispatcherLoop+0x9a
        00000000`0012f860 00000000`0041219e ADVAPI32!StartServiceCtrlDispatcherA+0x8d
        00000000`0012fae0 00000000`00130012 Ati2evxx+0x1219e
        00000000`0012fae8 00000000`00692be0 0x130012
        00000000`0012faf0 00000000`ffffffd3 0x692be0
        00000000`0012faf8 00000000`00692be1 0xffffffd3
        00000000`0012fb00 00000000`0012fb78 0x692be1
        00000000`0012fb08 00000000`00411f90 0x12fb78
        00000000`0012fb10 00000000`00000000 Ati2evxx+0x11f90
        00000000`0012fb18 00000000`00000000 0x0
        00000000`0012fb20 00000000`00692be0 0x0
        00000000`0012fb28 00000000`0041097f 0x692be0
        00000000`0012fb30 00000000`00000000 Ati2evxx+0x1097f
        00000000`0012fb38 00000000`00692be0 0x0
        00000000`0012fb40 00000000`00692be1 0x692be0
        00000000`0012fb48 00000000`0047994d 0x692be1
        00000000`0012fb50 00000000`00000001 Ati2evxx+0x7994d
        00000000`0012fb58 00000000`76c201d8 0x1
        00000000`0012fb60 00000000`00479928 kernel32!SxsPolicySuffix+0x140
        00000000`0012fb68 00000000`00692be0 Ati2evxx+0x79928
        00000000`0012fb70 00000000`00475608 0x692be0
        00000000`0012fb78 4b746f48`20697441 Ati2evxx+0x75608
        00000000`0012fb80 656c6c6f`50207965 0x4b746f48`20697441
        00000000`0012fb88 00000000`00000072 0x656c6c6f`50207965
        00000000`0012fb90 00000000`00000000 0x72
        00000000`0012fb98 00000000`00000000 0x0
        00000000`0012fba0 00000000`00000000 0x0
        00000000`0012fba8 00000000`00000000 0x0
        00000000`0012fbb0 00000000`00000000 0x0
        00000000`0012fbb8 00000000`00000001 0x0
        00000000`0012fbc0 00000000`006c1290 0x1
```

```
        THREAD fffffa800449d060  Cid 0118.011c  Teb: 000007fffffdc000 Win32Thread: fffff900c07c9330
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa800448a0c0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044c0040       Image:         Ati2evxx.exe
        Wait Start TickCount      2961           Ticks: 43618 (0:00:11:20.445)
        Context Switch Count      118                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ADVAPI32!ScSvcctrlThreadW (0x000007fefea84bd0)
        Stack Init fffff9800d11bdb0 Current fffff9800d11b740
        Base fffff9800d11c000 Limit fffff9800d113000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0d11b780 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0d11b8c0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0d11b920 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`0d11b9a0 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`0d11ba40 fffff960`000c7e1e win32k!xxxSleepThread+0x56
        fffff980`0d11ba70 fffff960`000c7f25 win32k!xxxRealInternalGetMessage+0x72e
        fffff980`0d11bb50 fffff960`000c97e4 win32k!xxxInternalGetMessage+0x35
        fffff980`0d11bb90 fffff800`01c4d733 win32k!NtUserGetMessage+0x64
        fffff980`0d11bc20 00000000`76d1e6aa nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0d11bc20)
        00000000`0268fdc8 00000000`76d1bf4e USER32!ZwUserGetMessage+0xa
        00000000`0268fdd0 00000000`0040fce9 USER32!GetMessageA+0xc3
        00000000`0268fe00 00000000`00400000 Ati2evxx+0xfce9
        00000000`0268fe08 00000000`0012fb78 Ati2evxx
        00000000`0268fe10 00000000`00000000 0x12fb78
        00000000`0268fe18 00000000`00000000 0x0
        00000000`0268fe20 00000000`00000001 0x0
        00000000`0268fe28 00000000`00000000 0x1
        00000000`0268fe30 00000000`00010022 0x0
        00000000`0268fe38 00000000`00000113 0x10022
        00000000`0268fe40 00000000`000014ca 0x113
        00000000`0268fe48 00000000`00000000 0x14ca
        00000000`0268fe50 00000200`0000b46f 0x0
        00000000`0268fe58 00000000`00000180 0x200`0000b46f
        00000000`0268fe60 00000000`0012fb70 0x180
        00000000`0268fe68 00000000`004033a0 0x12fb70
        00000000`0268fe70 00000000`00000000 Ati2evxx+0x33a0
        00000000`0268fe78 00000000`00000000 0x0
        00000000`0268fe80 00000000`00000000 0x0
        00000000`0268fe88 00000000`00000002 0x0
        00000000`0268fe90 00000000`00000000 0x2
        00000000`0268fe98 00000000`004120fd 0x0
        00000000`0268fea0 00000000`0012fb70 Ati2evxx+0x120fd
        00000000`0268fea8 00000000`0012fb78 0x12fb70
        00000000`0268feb0 00000000`00000000 0x12fb78
        00000000`0268feb8 00000000`00000000 0x0
        00000000`0268fec0 00000000`00000000 0x0
        00000000`0268fec8 00000000`00000000 0x0
        00000000`0268fed0 00000000`00000000 0x0
        00000000`0268fed8 00000000`00000000 0x0
        00000000`0268fee0 00000000`00000000 0x0
```

```
        THREAD fffffa800448abb0  Cid 0118.0124  Teb: 000007fffffda000 Win32Thread: fffff900c07ddab0
WAIT: (Executive) UserMode Non-Alertable
            fffffa800438e988  NotificationEvent
        IRP List:
            fffffa8004576110: (0006,0118) Flags: 00060800  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044c0040       Image:         Ati2evxx.exe
        Wait Start TickCount      1653           Ticks: 44926 (0:00:11:40.850)
        Context Switch Count      72                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address Ati2evxx (0x000000000042ee90)
        Stack Init fffff9800e51bdb0 Current fffff9800e51b7a0
        Base fffff9800e51c000 Limit fffff9800e515000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e51b7e0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e51b920 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0e51b980 fffff800`01e8e6ee nt!KeWaitForSingleObject+0x5f5
        fffff980`0e51ba00 fffff800`01eab906 nt!IopXxxControlFile+0xe29
        fffff980`0e51bb40 fffff800`01c4d733 nt!NtFsControlFile+0x56
        fffff980`0e51bbb0 00000000`76e2060a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e51bc20)
        00000000`0278fe88 00000000`76bc7330 ntdll!NtFsControlFile+0xa
        00000000`0278fe90 00000000`0042ef3b kernel32!ConnectNamedPipe+0x60
        00000000`0278ff00 00000000`000000bc Ati2evxx+0x2ef3b
        00000000`0278ff08 00000000`00000188 0xbc
        00000000`0278ff10 00000000`0278ff40 0x188
        00000000`0278ff18 00000000`000000bc 0x278ff40
        00000000`0278ff20 00000000`00007a80 0xbc
        00000000`0278ff28 00000000`00007a80 0x7a80
        00000000`0278ff30 00000000`00000fa0 0x7a80
        00000000`0278ff38 00000000`00000000 0xfa0
        00000000`0278ff40 00000000`00000000 0x0
        00000000`0278ff48 00000000`00000000 0x0
        00000000`0278ff50 00000000`00000000 0x0
        00000000`0278ff58 00000000`76bfcdcd 0x0
        00000000`0278ff60 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0278ff90 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80045b5060  Cid 0118.0560  Teb: 000007fffffd7000 Win32Thread: fffff900c07c4b20
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800448ffe0  NotificationEvent
            fffffa80041eafe0  NotificationEvent
            fffffa8004558d40  NotificationEvent
            fffffa8004558bd0  NotificationEvent
            fffffa80041eafe0  NotificationEvent
            fffffa80041eafe0  NotificationEvent
            fffffa80041eafe0  NotificationEvent
            fffffa80041eafe0  NotificationEvent
            fffffa80041eafe0  NotificationEvent
            fffffa80041eafe0  NotificationEvent
            fffffa80041eafe0  NotificationEvent
            fffffa8004558cc0  NotificationEvent
            fffffa80045cfe00  NotificationEvent
            fffffa80041eafe0  NotificationEvent
            fffffa80041eafe0  NotificationEvent
            fffffa80041eafe0  NotificationEvent
            fffffa80041eafe0  NotificationEvent
            fffffa80041eafe0  NotificationEvent
            fffffa80041eafe0  NotificationEvent
            fffffa80041eafe0
```

```
00000000`0288fe58 00000000`00000000 0x0
00000000`0288fe60 00000000`021abb10 0x0
00000000`0288fe68 00000000`021ab9c0 0x21abb10
00000000`0288fe70 00000000`00000068 0x21ab9c0
00000000`0288fe78 ffffffff`fffffffe 0x68
00000000`0288fe80 00000000`00000000 0xffffffff`fffffffe
00000000`0288fe88 00000000`00000000 0x0
00000000`0288fe90 00000000`00000028 0x0
00000000`0288fe98 00000000`020bfe50 0x28
00000000`0288fea0 00000000`021a83b0 0x20bfe50
00000000`0288fea8 00000000`00000000 0x21a83b0
00000000`0288feb0 00000000`00000068 0x0
00000000`0288feb8 00000000`0040253e 0x68
00000000`0288fec0 00000000`020bfe70 Ati2evxx+0x253e
00000000`0288fec8 00000000`00000000 0x20bfe70
00000000`0288fed0 00000000`00000000 0x0
00000000`0288fed8 000000ff`ffffffff 0x0
00000000`0288fee0 00000015`00320024 0xff`ffffffff
00000000`0288fee8 00000000`00000000 0x15`00320024
00000000`0288fef0 00000000`00000000 0x0
00000000`0288fef8 00000000`0040296e 0x0
00000000`0288ff00 00000000`021a83b0 Ati2evxx+0x296e
00000000`0288ff08 00000000`00000000 0x21a83b0
00000000`0288ff10 00000000`00000000 0x0
00000000`0288ff18 00000000`00000000 0x0
00000000`0288ff20 00000000`00000000 0x0
00000000`0288ff28 00000000`0040bdb5 0x0
00000000`0288ff30 00000000`00000000 Ati2evxx+0xbdb5
```

Svchost process (LocalServiceNetworkRestricted)

```
PROCESS fffffa80044ff040
    SessionId: 0  Cid: 0114    Peb: 7fffffd7000  ParentCid: 025c
    DirBase: 4de3f000  ObjectTable: fffff88005a06140  HandleCount: 450.
    Image: svchost.exe
    VadRoot fffffa800448b6c0 Vads 168 Clone 0 Private 1530. Modified 487. Locked 6.
    DeviceMap fffff88005a30830
    Token                             fffff88005a82060
    ElapsedTime                       00:11:42.985
    UserTime                          00:00:00.124
    KernelTime                        00:00:00.452
    QuotaPoolUsage[PagedPool]         146664
    QuotaPoolUsage[NonPagedPool]      23600
    Working Set Sizes (now,min,max)  (3244, 50, 345) (12976KB, 200KB, 1380KB)
    PeakWorkingSetSize                3373
    VirtualSize                       84 Mb
    PeakVirtualSize                   102 Mb
    PageFaultCount                    5138
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      3738

    Setting context for this process...
.process /p /r fffffa80044ff040

    !peb
PEB at 000007fffffd7000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00000000ff910000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00000000003a27f0 . 00000000039a8040
    Ldr.InLoadOrderModuleList:           00000000003a2700 . 00000000039a8020
    Ldr.InMemoryOrderModuleList:         00000000003a2710 . 00000000039a8030
            Base TimeStamp                     Module
        ff910000 4549b5f5 Nov 02 09:10:13 2006 C:\Windows\System32\svchost.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        76bc0000 4549d328 Nov 02 11:14:48 2006 C:\Windows\system32\kernel32.dll
     7fefdd40000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\system32\msvcrt.dll
     7fefea30000 4549d267 Nov 02 11:11:35 2006 C:\Windows\system32\ADVAPI32.dll
     7fefed90000 469c43bb Jul 17 05:21:15 2007 C:\Windows\system32\RPCRT4.dll
     7fefbad0000 4549d34b Nov 02 11:15:23 2006 c:\windows\system32\wevtsvc.dll
     7fefd3b0000 4549d336 Nov 02 11:15:02 2006 c:\windows\system32\USERENV.dll
     7fefd390000 4549d33f Nov 02 11:15:11 2006 c:\windows\system32\Secur32.dll
        76d00000 45d3ee19 Feb 15 05:22:33 2007 C:\Windows\system32\USER32.dll
     7fefec20000 4549d273 Nov 02 11:11:47 2006 C:\Windows\system32\GDI32.dll
     7fefca50000 4549d336 Nov 02 11:15:02 2006 c:\windows\system32\VERSION.dll
     7fefc940000 4549d277 Nov 02 11:11:51 2006 c:\windows\system32\GPAPI.dll
     7fefcc20000 4549d32d Nov 02 11:14:53 2006 c:\windows\system32\slc.dll
     7fefd9e0000 4549d2cb Nov 02 11:13:15 2006 C:\Windows\system32\IMM32.DLL
     7fefdc30000 4549d2e6 Nov 02 11:13:42 2006 C:\Windows\system32\MSCTF.dll
     7feff0c0000 4549d2a1 Nov 02 11:12:33 2006 C:\Windows\system32\LPK.DLL
     7fefd940000 4549d337 Nov 02 11:15:03 2006 C:\Windows\system32\USP10.dll
     7fefca40000 4549d341 Nov 02 11:15:13 2006 C:\Windows\System32\credssp.dll
     7fefcc50000 4549d344 Nov 02 11:15:16 2006 C:\Windows\System32\CRYPT32.dll
     7fefce00000 4549d2df Nov 02 11:13:35 2006 C:\Windows\System32\MSASN1.dll
     7fefc670000 4549d321 Nov 02 11:14:41 2006 C:\Windows\system32\schannel.dll
     7fefcf70000 4549d2fc Nov 02 11:14:04 2006 C:\Windows\System32\NETAPI32.dll
     7fefd530000 4549d310 Nov 02 11:14:24 2006 C:\Windows\system32\PSAPI.DLL
     7fefd540000 4549d38a Nov 02 11:16:26 2006 C:\Windows\system32\WS2_32.dll
     7feff0b0000 4549d370 Nov 02 11:16:00 2006 C:\Windows\system32\NSI.dll
     7fefc8f0000 4549d2e7 Nov 02 11:13:43 2006 C:\Windows\system32\mswsock.dll
     7fefc560000 4549d3a3 Nov 02 11:16:51 2006 C:\Windows\system32\wshtcpip.dll
     7fefc980000 4549d39d Nov 02 11:16:45 2006 C:\Windows\System32\wship6.dll
```

```
     7fefc220000 4549d259 Nov 02 11:11:21 2006 c:\windows\system32\audiosrv.dll
     7fefd760000 4549d317 Nov 02 11:14:31 2006 C:\Windows\system32\ole32.dll
     7fefdab0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\OLEAUT32.dll
     7fefc2e0000 4549d2a1 Nov 02 11:12:33 2006 c:\windows\system32\MMDevAPI.DLL
     7fefda10000 4549d31f Nov 02 11:14:39 2006 C:\Windows\system32\SHLWAPI.dll
     7fefc450000 4549d34e Nov 02 11:15:26 2006 c:\windows\system32\WTSAPI32.dll
     7fefd1b0000 4549d380 Nov 02 11:16:16 2006 c:\windows\system32\WINSTA.dll
     7fefbe70000 4549d32b Nov 02 11:14:51 2006 C:\Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_1559f1c6f365a7fa\comctl32.dll
     7fefdb90000 4549d282 Nov 02 11:12:02 2006 C:\Windows\system32\CLBCatQ.DLL
     7fefeed0000 4549d318 Nov 02 11:14:32 2006 C:\Windows\system32\SETUPAPI.dll
     7fefc1e0000 4549d381 Nov 02 11:16:17 2006 C:\Windows\System32\WINTRUST.dll
     7fefda90000 462443ee Apr 17 04:50:06 2007 C:\Windows\system32\imagehlp.dll
     7fefb260000 4549d295 Nov 02 11:12:21 2006 c:\windows\system32\lmhsvc.dll
     7fefcb80000 4549d2e1 Nov 02 11:13:37 2006 c:\windows\system32\IPHLPAPI.DLL
     7fefcb30000 4549d263 Nov 02 11:11:31 2006 c:\windows\system32\dhcpcsvc.DLL
     7fefce40000 4549d288 Nov 02 11:12:08 2006 c:\windows\system32\DNSAPI.dll
     7fefd280000 4549d370 Nov 02 11:16:00 2006 c:\windows\system32\WINNSI.DLL
     7fefcb00000 4549d264 Nov 02 11:11:32 2006 c:\windows\system32\dhcpcsvc6.DLL
     7fefc620000 4549d31d Nov 02 11:14:37 2006 C:\Windows\System32\rsaenh.dll
     7fefb0c0000 4549d258 Nov 02 11:11:20 2006 C:\Windows\System32\audioses.dll
     7fefb040000 4549d256 Nov 02 11:11:18 2006 C:\Windows\System32\audioeng.dll
     7fefc2d0000 4549d273 Nov 02 11:11:47 2006 C:\Windows\System32\AVRT.dll
     7fefaab0000 4549d371 Nov 02 11:16:01 2006 C:\Windows\System32\winrnr.dll
     7fefd590000 4549d396 Nov 02 11:16:38 2006 C:\Windows\system32\WLDAP32.dll
     7fefc1a0000 4549d314 Nov 02 11:14:28 2006 C:\Windows\system32\NLAapi.dll
     7fefaa70000 4549d2e4 Nov 02 11:13:40 2006 C:\Windows\system32\napinsp.dll
     7fefaa50000 4549d341 Nov 02 11:15:13 2006 C:\Windows\system32\pnrpnsp.dll
     7fefaac0000 4549d317 Nov 02 11:14:31 2006 C:\Windows\System32\rasadhlp.dll
     7fef7130000 4549d38f Nov 02 11:16:31 2006 c:\windows\system32\wscsvc.dll
     7fefc460000 466785ee Jun 07 05:13:34 2007 c:\windows\system32\FirewallAPI.dll
     7fef9e20000 4549d342 Nov 02 11:15:14 2006 C:\Windows\system32\wbem\wbemprox.dll
     7fef9f50000 4549d33d Nov 02 11:15:09 2006 C:\Windows\system32\wbem\wbemcomn.dll
     7fef96d0000 4549d343 Nov 02 11:15:15 2006 C:\Windows\system32\wbem\wbemsvc.dll
     7fef9040000 4549d274 Nov 02 11:11:48 2006 C:\Windows\system32\wbem\fastprox.dll
     7fefcdd0000 4549d375 Nov 02 11:16:05 2006 C:\Windows\system32\NTDSAPI.dll
     7fef3390000 46ae95af Jul 31 02:51:43 2007 C:\Windows\system32\wuapi.dll
     7fefc1c0000 4549d251 Nov 02 11:11:13 2006 C:\Windows\system32\Cabinet.dll
     7fefaf00000 4549d246 Nov 02 11:11:02 2006 C:\Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.6000.16386_none_40339432230aebeb\COMCTL32.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       00000000003a0000
    ProcessParameters: 00000000003a1db0
    WindowTitle:  'C:\Windows\System32\svchost.exe'
    ImageFile:    'C:\Windows\System32\svchost.exe'
    CommandLine:  'C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted'
    DllPath:
'C:\Windows\System32;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Wind
ows;C:\Windows\System32\Wbem'
    Environment:  00000000003a1310
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\ServiceProfiles\LocalService\AppData\Roaming
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        LOCALAPPDATA=C:\Windows\ServiceProfiles\LocalService\AppData\Local
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public
```

```
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\SERVIC~2\LOCALS~1\AppData\Local\Temp
        TMP=C:\Windows\SERVIC~2\LOCALS~1\AppData\Local\Temp
        USERDOMAIN=NT AUTHORITY
        USERNAME=LOCAL SERVICE
        USERPROFILE=C:\Windows\ServiceProfiles\LocalService
        windir=C:\Windows


        THREAD fffffa80042d8bb0  Cid 0114.0134  Teb: 000007fffffde000 Win32Thread: 0000000000000000
WAIT: (Executive) UserMode Non-Alertable
            fffffa80044c1fb8  NotificationEvent
        IRP List:
            fffffa80044bd2c0: (0006,0118) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80044ff040       Image:         svchost.exe
        Wait Start TickCount      43120          Ticks: 3459 (0:00:00:53.960)
        Context Switch Count      45
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address svchost!wmainCRTStartup (0x00000000ff912550)
        Stack Init fffff9800cc99db0 Current fffff9800cc997f0
        Base fffff9800cc9a000 Limit fffff9800cc94000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0cc99830 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0cc99970 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0cc999d0 fffff800`01ebdf16 nt!KeWaitForSingleObject+0x5f5
        fffff980`0cc99a50 fffff800`01ea1a24 nt!IopSynchronousServiceTail+0x306
        fffff980`0cc99ac0 fffff800`01c4d733 nt!NtReadFile+0x583
        fffff980`0cc99bb0 00000000`76e202da nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0cc99c20)
        00000000`0023f628 00000000`76bf26da ntdll!NtReadFile+0xa
        00000000`0023f630 000007fe`fea865aa kernel32!ReadFile+0x8a
        00000000`0023f6c0 000007fe`fea862e3 ADVAPI32!ScGetPipeInput+0x4a
        00000000`0023f7a0 000007fe`fea850f3 ADVAPI32!ScDispatcherLoop+0x9a
        00000000`0023f8a0 00000000`ff91283c ADVAPI32!StartServiceCtrlDispatcherW+0x176
        00000000`0023fb40 00000000`ff912666 svchost!wmain+0xe5
        00000000`0023fb70 00000000`76bfcdcd svchost!ScCreateWellKnownSids+0x301
        00000000`0023fbb0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0023fbe0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80044c1a20  Cid 0114.0138  Teb: 000007fffffda000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80044ff5e0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80044ff040       Image:         svchost.exe
        Wait Start TickCount      1914           Ticks: 44665 (0:00:11:36.778)
        Context Switch Count      2770
        UserTime                  00:00:00.109
        KernelTime                00:00:00.624
        Win32 Start Address wevtsvc!RegistryMonitor::WaitThreadRoutine (0x000007fefbbab7f0)
        Stack Init fffff9800c26ddb0 Current fffff9800c26d960
        Base fffff9800c26e000 Limit fffff9800c268000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0c26d9a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0c26dae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0c26db40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0c26dbc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0c26dc20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0c26dc20)
        00000000`00d8f9b8 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`00d8f9c0 000007fe`fbbab8d8 kernel32!WaitForSingleObjectEx+0x9c
        00000000`00d8fa80 00000000`76bfcdcd wevtsvc!RegistryMonitor::WaitThreadRoutine+0xe8
        00000000`00d8fb10 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
```

```
        00000000`00d8fb40 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80044fe340  Cid 0114.0148  Teb: 000007fffffd8000 Win32Thread: fffff900c07ce010
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80044c2320  SynchronizationEvent
            fffffa80044c11f0  SynchronizationEvent
            fffffa80044e5170  SynchronizationEvent
            fffffa80044fe920  SynchronizationTimer
            fffffa80044b9730  SynchronizationEvent
            fffffa80044fe7d0  SynchronizationTimer
            fffffa80044c1190  SynchronizationEvent
            fffffa80044fe3f8  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80044ff040       Image:         svchost.exe
        Wait Start TickCount      43120          Ticks: 3459 (0:00:00:53.960)
        Context Switch Count      77                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address wevtsvc!OsEventsPowerEvent (0x000007fefbbc82e0)
        Stack Init fffff9800d141db0 Current fffff9800d141260
        Base fffff9800d142000 Limit fffff9800d139000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0d1412a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0d1413e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0d141440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0d1414b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0d141960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0d141bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0d141c20)
        00000000`01e2f668 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`01e2f670 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`01e2f780 000007fe`fbbc852a kernel32!WaitForMultipleObjects+0x11
        00000000`01e2f7c0 00000000`76bfcdcd wevtsvc!OsEventsPowerEvent+0x33e
        00000000`01e2f870 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`01e2f8a0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80044dd870  Cid 0114.01a0  Teb: 000007fffffd3000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa80044dcb80  SynchronizationTimer
            fffffa80044e51d0  NotificationEvent
            fffffa80044ddef0  SynchronizationTimer
            fffffa80044dfdd0  SynchronizationEvent
            fffffa80044d9a80  SynchronizationEvent
            fffffa80044e5fe0  SynchronizationEvent
            fffffa80040923d0  NotificationEvent
            fffffa80045e7fe0  NotificationEvent
            fffffa800451fbe0  NotificationEvent
            fffffa800451fd80  NotificationEvent
            fffffa80045e0c10  NotificationEvent
            fffffa80045f4510  NotificationEvent
            fffffa80044e4110  NotificationEvent
            fffffa8004823940  NotificationEvent
            fffffa8004892d50  NotificationEvent
            fffffa80045b5dc0  SynchronizationEvent
            fffffa80045a9b70  SynchronizationEvent
            fffffa80020b6190  NotificationEvent
            fffffa8002b1b5e0  SynchronizationEvent
            fffffa80020f73b0  SynchronizationEvent
            fffffa8002a01ae0  SynchronizationEvent
            fffffa80044ddd00  SynchronizationTimer
            fffffa80044dd928  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80044ff040       Image:         svchost.exe
        Wait Start TickCount      46021          Ticks: 558 (0:00:00:08.704)
        Context Switch Count      191
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x0000000076df6930)
        Stack Init fffff9800ccd8db0 Current fffff9800ccd8260
        Base fffff9800ccd9000 Limit fffff9800ccd3000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0ccd82a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0ccd83e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0ccd8440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0ccd84b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0ccd8960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0ccd8bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0ccd8c20)
        00000000`024efb28 00000000`76df6b07 ntdll!NtWaitForMultipleObjects+0xa
        00000000`024efb30 00000000`76bfcdcd ntdll!TppWaiterpThread+0x14d
        00000000`024efdd0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`024efe00 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004519110  Cid 0114.02f0  Teb: 000007fffffdc000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa80045195a0  QueueObject
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80044ff040       Image:         svchost.exe
        Wait Start TickCount      2768           Ticks: 43811 (0:00:11:23.455)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address audiosrv!EventWorkerThread (0x000007fefc232fb0)
        Stack Init fffff9800cc14db0 Current fffff9800cc14810
        Base fffff9800cc15000 Limit fffff9800cc0f000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0cc14850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0cc14990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0cc149f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0cc14a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`0cc14b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`0cc14bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0cc14c20)
        00000000`01d9fbe8 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`01d9fbf0 000007fe`fc232ff8 kernel32!GetQueuedCompletionStatus+0x48
        00000000`01d9fc50 00000000`76bfcdcd audiosrv!EventWorkerThread+0x75
        00000000`01d9fc90 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`01d9fcc0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004525ab0  Cid 0114.02e8  Teb: 000007fffffa4000 Win32Thread: fffff900c07bfab0
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa80045255c0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80044ff040       Image:         svchost.exe
        Wait Start TickCount      2941           Ticks: 43638 (0:00:11:20.757)
        Context Switch Count      28                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address MMDevAPI!CDeviceEnumerator::PnpNotificationThreadWrapper
(0x000007fefc2eade0)
        Stack Init fffff9800daf5db0 Current fffff9800daf5740
        Base fffff9800daf6000 Limit fffff9800daee000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0daf5780 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0daf58c0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0daf5920 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`0daf59a0 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`0daf5a40 fffff960`000c7e1e win32k!xxxSleepThread+0x56
        fffff980`0daf5a70 fffff960`000c7f25 win32k!xxxRealInternalGetMessage+0x72e
        fffff980`0daf5b50 fffff960`000c97e4 win32k!xxxInternalGetMessage+0x35
        fffff980`0daf5b90 fffff800`01c4d733 win32k!NtUserGetMessage+0x64
        fffff980`0daf5c20 00000000`76d1e6aa nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0daf5c20)
        00000000`0285f7e8 00000000`76d1e6ea USER32!ZwUserGetMessage+0xa
        00000000`0285f7f0 000007fe`fc2e19f2 USER32!GetMessageW+0x34
        00000000`0285f820 00000000`76bfcdcd MMDevAPI!CDeviceEnumerator::PnpNotificationThread+0x25d
        00000000`0285f940 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0285f970 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800457a790  Cid 0114.0378  Teb: 000007fffffa2000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004525f40  SynchronizationEvent
            fffffa800451f890  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80044ff040       Image:         svchost.exe
        Wait Start TickCount      1580           Ticks: 44999 (0:00:11:41.988)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address MMDevAPI!CNotificationDelegator::HardwarePollingThreadProc
(0x000007fefc3016a0)
        Stack Init fffff9800cc7ddb0 Current fffff9800cc7d260
        Base fffff9800cc7e000 Limit fffff9800cc78000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0cc7d2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0cc7d3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0cc7d440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0cc7d4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0cc7d960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0cc7dbb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0cc7dc20)
        00000000`02b7f918 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`02b7f920 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`02b7fa30 000007fe`fc3016dd kernel32!WaitForMultipleObjects+0x11
        00000000`02b7fa70 00000000`76bfcdcd
MMDevAPI!CNotificationDelegator::HardwarePollingThreadProc+0x3d
        00000000`02b7fab0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02b7fae0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80045c0bb0  Cid 0114.04f8  Teb: 000007fffff9c000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004577480  SynchronizationEvent
            fffffa800456b210  SynchronizationEvent
        IRP List:
            fffffa8004487980: (0006,0118) Flags: 00060000  Mdl: fffffa800472d4c0
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80044ff040       Image:         svchost.exe
        Wait Start TickCount      46296          Ticks: 283 (0:00:00:04.414)
        Context Switch Count      50
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ADVAPI32!ScSvcctrlThreadW (0x000007fefea84bd0)
        Stack Init fffff9800e30edb0 Current fffff9800e30e260
        Base fffff9800e30f000 Limit fffff9800e309000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0e30e2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e30e3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0e30e440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0e30e4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0e30e960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0e30ebb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e30ec20)
        00000000`02c0f7d8 000007fe`fb261a14 ntdll!NtWaitForMultipleObjects+0xa
        00000000`02c0f7e0 00000000`ff911771 lmhsvc!ServiceMain+0x272
        00000000`02c0fa00 000007fe`fea84bf5 svchost!ServiceStarter+0x1ea
        00000000`02c0fa90 00000000`76bfcdcd ADVAPI32!ScSvcctrlThreadW+0x25
        00000000`02c0fac0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02c0faf0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800456ebb0  Cid 0114.0500  Teb: 000007fffff9a000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80045734b0  SynchronizationEvent
            fffffa80045bf6b0  SynchronizationEvent
        IRP List:
            fffffa800458a1e0: (0006,0118) Flags: 00060000  Mdl: fffffa8003fa9290
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80044ff040       Image:         svchost.exe
        Wait Start TickCount      1624           Ticks: 44955 (0:00:11:41.302)
        Context Switch Count      6
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address lmhsvc!CheckIPAddrWorkerRtn (0x000007fefb262980)
        Stack Init fffff9800e32adb0 Current fffff9800e32a260
        Base fffff9800e32b000 Limit fffff9800e325000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e32a2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e32a3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0e32a440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0e32a4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0e32a960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0e32abb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e32ac20)
        00000000`02eff918 000007fe`fb262a24 ntdll!NtWaitForMultipleObjects+0xa
        00000000`02eff920 00000000`76bfcdcd lmhsvc!CheckIPAddrWorkerRtn+0xbf
        00000000`02eff990 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02eff9c0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa800456dbb0  Cid 0114.0504  Teb: 000007fffff98000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80045bd0a0  NotificationEvent
            fffffa80045bf0e8  NotificationEvent
        IRP List:
            fffffa800458a840: (0006,0160) Flags: 00060030  Mdl: fffffa80044c05f0
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80044ff040       Image:         svchost.exe
        Wait Start TickCount      1624           Ticks: 44955 (0:00:11:41.302)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address lmhsvc!SmbGetHostThread (0x000007fefb261230)
        Stack Init fffff9800e338db0 Current fffff9800e338260
        Base fffff9800e339000 Limit fffff9800e333000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e3382a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e3383e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0e338440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0e3384b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0e338960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0e338bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e338c20)
        00000000`0245f328 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0245f330 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0245f440 000007fe`fb2613d6 kernel32!WaitForMultipleObjects+0x11
        00000000`0245f480 00000000`76bfcdcd lmhsvc!SmbGetHostThread+0x1f5
        00000000`0245f920 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0245f950 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800456d700  Cid 0114.0508  Teb: 000007fffff96000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80045bd0a0  NotificationEvent
            fffffa80045a0528  NotificationEvent
        IRP List:
            fffffa8002849010: (0006,0160) Flags: 00060030  Mdl: fffffa8004350ea0
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80044ff040       Image:         svchost.exe
        Wait Start TickCount      46296          Ticks: 283 (0:00:00:04.414)
        Context Switch Count      16
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address lmhsvc!SmbGetHostThread (0x000007fefb261230)
        Stack Init fffff9800e331db0 Current fffff9800e331260
        Base fffff9800e332000 Limit fffff9800e32c000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0e3312a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e3313e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0e331440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0e3314b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0e331960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0e331bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e331c20)
        00000000`0290f528 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0290f530 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0290f640 000007fe`fb2613d6 kernel32!WaitForMultipleObjects+0x11
        00000000`0290f680 00000000`76bfcdcd lmhsvc!SmbGetHostThread+0x1f5
        00000000`0290fb20 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0290fb50 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80045cf060  Cid 0114.0544  Teb: 000007fffff94000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80045cf560  NotificationEvent
            fffffa80045c1b10  SynchronizationEvent
            fffffa80045a8e00  NotificationEvent
            fffffa80045ac460  SynchronizationEvent
            fffffa80045cf118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80044ff040       Image:         svchost.exe
        Wait Start TickCount      1865           Ticks: 44714 (0:00:11:37.542)
        Context Switch Count      54
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ADVAPI32!ScSvcctrlThreadW (0x000007fefea84bd0)
        Stack Init fffff9800da89db0 Current fffff9800da89260
        Base fffff9800da8a000 Limit fffff9800da84000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0da892a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0da893e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0da89440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0da894b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0da89960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0da89bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0da89c20)
        00000000`0314fbc8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0314fbd0 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0314fce0 000007fe`fcb3458c kernel32!WaitForMultipleObjects+0x11
        00000000`0314fd20 000007fe`fcb3e022 dhcpcsvc!ProcessDhcpRequestForever+0x2e7
        00000000`0314fdd0 00000000`ff911771 dhcpcsvc!ServiceMain+0x14c
        00000000`0314fe30 000007fe`fea84bf5 svchost!ServiceStarter+0x1ea
        00000000`0314fec0 00000000`76bfcdcd ADVAPI32!ScSvcctrlThreadW+0x25
        00000000`0314fef0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0314ff20 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80045b9060  Cid 0114.0550  Teb: 000007fffff92000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa80045cf560  NotificationEvent
            fffffa80045b7690  SynchronizationEvent
            fffffa80045b7630  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80044ff040       Image:         svchost.exe
        Wait Start TickCount      1985           Ticks: 44594 (0:00:11:35.670)
        Context Switch Count      12
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address dhcpcsvc6!Dhcpv6Main (0x000007fefcb068cc)
        Stack Init fffff9800cc8bdb0 Current fffff9800cc8b260
        Base fffff9800cc8c000 Limit fffff9800cc86000 Call 0
        Priority 13 BasePriority 8 PriorityDecrement 5 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0cc8b2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0cc8b3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0cc8b440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0cc8b4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0cc8b960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0cc8bbb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0cc8bc20)
        00000000`031ef558 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`031ef560 000007fe`fcb0615f kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`031ef670 000007fe`fcb0698c dhcpcsvc6!ProcessDhcpv6RequestForever+0x143
        00000000`031ef730 00000000`76bfcdcd dhcpcsvc6!Dhcpv6Main+0xc0
        00000000`031ef770 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`031ef7a0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa800489ebb0  Cid 0114.0828  Teb: 000007fffffaa000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80048758e0  NotificationEvent
        IRP List:
            fffffa800477d530: (0006,0118) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80044ff040       Image:         svchost.exe
        Wait Start TickCount      46086          Ticks: 493 (0:00:00:07.690)
        Context Switch Count      132
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wevtsvc!ProcessEventsThread (0x000007fefbb724a0)
        Stack Init fffff9800ccc3db0 Current fffff9800ccc3960
        Base fffff9800ccc4000 Limit fffff9800ccbe000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0ccc39a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0ccc3ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0ccc3b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0ccc3bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0ccc3c20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0ccc3c20)
        00000000`03d6f2b8 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`03d6f2c0 000007fe`fea89b0e kernel32!WaitForSingleObjectEx+0x9c
        00000000`03d6f380 000007fe`fea8a6a5 ADVAPI32!EtwpProcessRealTimeTraces+0xf4
        00000000`03d6f400 000007fe`fbb724f5 ADVAPI32!ProcessTrace+0x480
        00000000`03d6f870 00000000`76bfcdcd wevtsvc!ProcessEventsThread+0x55
        00000000`03d6f8a0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`03d6f8d0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004880060  Cid 0114.082c  Teb: 000007fffffa8000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80047f0590  NotificationEvent
        IRP List:
            fffffa80042fd5c0: (0006,0118) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80044ff040       Image:         svchost.exe
        Wait Start TickCount      27503          Ticks: 19076 (0:00:04:57.587)
        Context Switch Count      13
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wevtsvc!ProcessEventsThread (0x000007fefbb724a0)
        Stack Init fffff9800e73bdb0 Current fffff9800e73b960
        Base fffff9800e73c000 Limit fffff9800e736000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e73b9a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e73bae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0e73bb40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0e73bbc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0e73bc20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e73bc20)
        00000000`0326f548 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`0326f550 000007fe`fea89b0e kernel32!WaitForSingleObjectEx+0x9c
        00000000`0326f610 000007fe`fea8a6a5 ADVAPI32!EtwpProcessRealTimeTraces+0xf4
        00000000`0326f690 000007fe`fbb724f5 ADVAPI32!ProcessTrace+0x480
        00000000`0326fb00 00000000`76bfcdcd wevtsvc!ProcessEventsThread+0x55
        00000000`0326fb30 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0326fb60 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80048a1bb0  Cid 0114.0830  Teb: 000007fffffac000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800486a6a0  NotificationEvent
        IRP List:
            fffffa80043eaee0: (0006,0118) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80044ff040       Image:         svchost.exe
        Wait Start TickCount      40630          Ticks: 5949 (0:00:01:32.804)
        Context Switch Count      163
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address wevtsvc!ProcessEventsThread (0x000007fefbb724a0)
        Stack Init fffff980103d5db0 Current fffff980103d5960
        Base fffff980103d6000 Limit fffff980103d0000 Call 0
        Priority 13 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`103d59a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`103d5ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`103d5b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`103d5bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`103d5c20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`103d5c20)
        00000000`03aaf4e8 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`03aaf4f0 000007fe`fea89b0e kernel32!WaitForSingleObjectEx+0x9c
        00000000`03aaf5b0 000007fe`fea8a6a5 ADVAPI32!EtwpProcessRealTimeTraces+0xf4
        00000000`03aaf630 000007fe`fbb724f5 ADVAPI32!ProcessTrace+0x480
        00000000`03aafaa0 00000000`76bfcdcd wevtsvc!ProcessEventsThread+0x55
        00000000`03aafad0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`03aafb00 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80024f5060  Cid 0114.0e74  Teb: 000007fffff8a000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8002b1b580  SynchronizationEvent
            fffffa8002addef0  SynchronizationTimer
            fffffa8002568c50  SynchronizationEvent
            fffffa8002adec90  SynchronizationEvent
            fffffa8002160450  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80044ff040       Image:         svchost.exe
        Wait Start TickCount      16102          Ticks: 30477 (0:00:07:55.444)
        Context Switch Count      56
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wscsvc!CThirdPartyMonitoring::MonitoringThreadProcEntry
(0x000007fef7136e6c)
        Stack Init fffff9800e4c8db0 Current fffff9800e4c8260
        Base fffff9800e4c9000 Limit fffff9800e4c3000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e4c82a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e4c83e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0e4c8440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0e4c84b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0e4c8960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0e4c8bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e4c8c20)
        00000000`0303f7c8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0303f7d0 000007fe`f7137015 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0303f8e0 000007fe`f7136e9a
wscsvc!CThirdPartyMonitoring::MonitoringThreadProc+0x165
        00000000`0303f930 00000000`76bfcdcd
wscsvc!CThirdPartyMonitoring::MonitoringThreadProcEntry+0x2e
        00000000`0303f960 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0303f990 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80028a8710  Cid 0114.0b7c  Teb: 000007fffff86000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Alertable
            fffffa8002132aa0  QueueObject
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80044ff040       Image:         svchost.exe
        Wait Start TickCount      16100          Ticks: 30479 (0:00:07:55.475)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x0000000076e17860)
        Stack Init fffff98020c90db0 Current fffff98020c90860
        Base fffff98020c91000 Limit fffff98020c8b000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`20c908a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`20c909e0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`20c90a40 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`20c90ad0 fffff800`01c8a722 nt!IoRemoveIoCompletion+0x47
        fffff980`20c90b50 fffff800`01c4d733 nt!NtWaitForWorkViaWorkerFactory+0x1f1
        fffff980`20c90c20 00000000`76e21b4a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`20c90c20)
        00000000`02e5fba8 00000000`76e17a20 ntdll!NtWaitForWorkViaWorkerFactory+0xa
        00000000`02e5fbb0 00000000`76bfcdcd ntdll!TppWorkerThread+0x23e
        00000000`02e5fe20 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02e5fe50 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8001eca1e0  Cid 0114.04c8  Teb: 000007fffff84000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa80020f7410  NotificationEvent
            fffffa8002b00e30  SynchronizationEvent
            fffffa8002ae7460  SynchronizationEvent
            fffffa80025cb6a0  SynchronizationEvent
            fffffa8001ff35e0  SynchronizationEvent
            fffffa8002a3e8c0  SynchronizationTimer
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80044ff040       Image:         svchost.exe
        Wait Start TickCount      16235          Ticks: 30344 (0:00:07:53.369)
        Context Switch Count      33
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wscsvc!SystemMonitoringThreadProc (0x000007fef7133388)
        Stack Init fffff9801daafdb0 Current fffff9801daaf260
        Base fffff9801dab0000 Limit fffff9801daaa000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1daaf2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1daaf3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`1daaf440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`1daaf4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`1daaf960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`1daafbb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1daafc20)
        00000000`0405f6d8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0405f6e0 000007fe`f71336ab kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0405f7f0 00000000`76bfcdcd wscsvc!SystemMonitoringThreadProc+0x323
        00000000`0405f8f0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0405f920 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8002b1e620  Cid 0114.0d84  Teb: 000007fffffae000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa80044e5cc0  QueueObject
            fffffa8002b1e6d8  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80044ff040       Image:         svchost.exe
        Wait Start TickCount      45939          Ticks: 640 (0:00:00:09.984)
        Context Switch Count      107
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff9800e749db0 Current fffff9800e749810
        Base fffff9800e74a000 Limit fffff9800e744000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0e749850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e749990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0e7499f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0e749a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`0e749b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`0e749bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e749c20)
        00000000`0236fcb8 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`0236fcc0 000007fe`fedce7a3 kernel32!GetQueuedCompletionStatus+0x48
        00000000`0236fd20 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`0236fdb0 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`0236fe60 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`0236fe90 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`0236fed0 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`0236ff00 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0236ff30 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

Svchost process (LocalSystemNetworkRestricted)

```
PROCESS fffffa8004484c10
    SessionId: 0  Cid: 018c    Peb: 7fffffd4000  ParentCid: 025c
    DirBase: 4d307000  ObjectTable: fffff88005a43f00  HandleCount: 495.
    Image: svchost.exe
    VadRoot fffffa8004484a20 Vads 241 Clone 0 Private 16169. Modified 2352. Locked 0.
    DeviceMap fffff88000007820
    Token                             fffff88005b84060
    ElapsedTime                       00:11:42.939
    UserTime                          00:00:00.078
    KernelTime                        00:00:00.546
    QuotaPoolUsage[PagedPool]         188648
    QuotaPoolUsage[NonPagedPool]      27136
    Working Set Sizes (now,min,max)  (18165, 50, 345) (72660KB, 200KB, 1380KB)
    PeakWorkingSetSize                38659
    VirtualSize                       184 Mb
    PeakVirtualSize                   233 Mb
    PageFaultCount                    71705
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      17591

    Setting context for this process...
.process /p /r fffffa8004484c10

    !peb
PEB at 000007fffffd4000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00000000ff910000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 0000000000172760 . 000000000989a110
    Ldr.InLoadOrderModuleList:           0000000000172670 . 00000000001e5630
    Ldr.InMemoryOrderModuleList:         0000000000172680 . 00000000001e5640
            Base TimeStamp                     Module
        ff910000 4549b5f5 Nov 02 09:10:13 2006 C:\Windows\System32\svchost.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        76bc0000 4549d328 Nov 02 11:14:48 2006 C:\Windows\system32\kernel32.dll
     7fefdd40000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\system32\msvcrt.dll
     7fefea30000 4549d267 Nov 02 11:11:35 2006 C:\Windows\system32\ADVAPI32.dll
     7fefed90000 469c43bb Jul 17 05:21:15 2007 C:\Windows\system32\RPCRT4.dll
     7fefc5b0000 4549d384 Nov 02 11:16:20 2006 C:\Windows\System32\NTMARTA.DLL
        76d00000 45d3ee19 Feb 15 05:22:33 2007 C:\Windows\system32\USER32.dll
     7fefec20000 4549d273 Nov 02 11:11:47 2006 C:\Windows\system32\GDI32.dll
     7fefd590000 4549d396 Nov 02 11:16:38 2006 C:\Windows\system32\WLDAP32.dll
     7fefd540000 4549d38a Nov 02 11:16:26 2006 C:\Windows\system32\WS2_32.dll
     7feff0b0000 4549d370 Nov 02 11:16:00 2006 C:\Windows\system32\NSI.dll
     7fefd530000 4549d310 Nov 02 11:14:24 2006 C:\Windows\system32\PSAPI.DLL
     7fefce20000 4549d315 Nov 02 11:14:29 2006 C:\Windows\System32\SAMLIB.dll
     7fefd760000 4549d317 Nov 02 11:14:31 2006 C:\Windows\system32\ole32.dll
     7fefd9e0000 4549d2cb Nov 02 11:13:15 2006 C:\Windows\system32\IMM32.DLL
     7fefdc30000 4549d2e6 Nov 02 11:13:42 2006 C:\Windows\system32\MSCTF.dll
     7feff0c0000 4549d2a1 Nov 02 11:12:33 2006 C:\Windows\system32\LPK.DLL
     7fefd940000 4549d337 Nov 02 11:15:03 2006 C:\Windows\system32\USP10.dll
     7fefc220000 4549d259 Nov 02 11:11:21 2006 c:\windows\system32\audiosrv.dll
     7fefdab0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\OLEAUT32.dll
     7fefc2e0000 4549d2a1 Nov 02 11:12:33 2006 c:\windows\system32\MMDevAPI.DLL
     7fefda10000 4549d31f Nov 02 11:14:39 2006 C:\Windows\system32\SHLWAPI.dll
     7fefc450000 4549d34e Nov 02 11:15:26 2006 c:\windows\system32\WTSAPI32.dll
     7fefd1b0000 4549d380 Nov 02 11:16:16 2006 c:\windows\system32\WINSTA.dll
     7fefbe70000 4549d32b Nov 02 11:14:51 2006 C:\Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_1559f1c6f365a7fa\comctl32.dll
     7fefdb90000 4549d282 Nov 02 11:12:02 2006 C:\Windows\system32\CLBCatQ.DLL
     7fefeed0000 4549d318 Nov 02 11:14:32 2006 C:\Windows\system32\SETUPAPI.dll
```

```
 7fefc1e0000 4549d381 Nov 02 11:16:17 2006 C:\Windows\System32\WINTRUST.dll
 7fefcc50000 4549d344 Nov 02 11:15:16 2006 C:\Windows\System32\CRYPT32.dll
 7fefce00000 4549d2df Nov 02 11:13:35 2006 C:\Windows\System32\MSASN1.dll
 7fefd3b0000 4549d336 Nov 02 11:15:02 2006 C:\Windows\System32\USERENV.dll
 7fefd390000 4549d33f Nov 02 11:15:11 2006 C:\Windows\System32\Secur32.dll
 7fefda90000 462443ee Apr 17 04:50:06 2007 C:\Windows\system32\imagehlp.dll
 7fefb9b0000 4549d350 Nov 02 11:15:28 2006 c:\windows\system32\cscsvc.dll
 7fefddf0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\SHELL32.dll
 7fefcd90000 4549d2b2 Nov 02 11:12:50 2006 c:\windows\system32\MPR.dll
 7fefc620000 4549d31d Nov 02 11:14:37 2006 C:\Windows\System32\rsaenh.dll
 7fefc940000 4549d277 Nov 02 11:11:51 2006 C:\Windows\System32\GPAPI.dll
 7fefcc20000 4549d32d Nov 02 11:14:53 2006 C:\Windows\System32\slc.dll
 7fefc170000 4549d33a Nov 02 11:15:06 2006 c:\windows\system32\uxsms.dll
 7fefb4b0000 4549d32a Nov 02 11:14:50 2006 c:\windows\system32\tabsvc.dll
 7fefb2c0000 4549d281 Nov 02 11:12:01 2006 c:\windows\system32\HID.DLL
 7fefa540000 4549d28b Nov 02 11:12:11 2006 c:\windows\system32\emdmgmt.dll
 7fefa6b0000 4549d337 Nov 02 11:15:03 2006 c:\windows\system32\WDSCORE.dll
 7fefaaa0000 4549d31e Nov 02 11:14:38 2006 c:\windows\system32\SLWGA.dll
 7fefd5f0000 470c5dac Oct 10 06:05:48 2007 C:\Windows\system32\urlmon.dll
 7fefebc0000 4549d29c Nov 02 11:12:28 2006 C:\Windows\system32\iertutil.dll
 7fefa690000 4549d312 Nov 02 11:14:26 2006 c:\windows\system32\pcasvc.dll
 7fefd310000 4549d247 Nov 02 11:11:03 2006 c:\windows\system32\apphelp.dll
 7fefa110000 4549d338 Nov 02 11:15:04 2006 c:\windows\system32\sysmain.dll
 7fefa260000 4549d358 Nov 02 11:15:36 2006 c:\windows\system32\trkwks.dll
 7fefcf70000 4549d2fc Nov 02 11:14:04 2006 c:\windows\system32\NETAPI32.dll
 7fefca40000 4549d341 Nov 02 11:15:13 2006 C:\Windows\System32\credssp.dll
 7fefc670000 4549d321 Nov 02 11:14:41 2006 C:\Windows\system32\schannel.dll
 7fef7170000 4549d34f Nov 02 11:15:27 2006 C:\Windows\system32\cscobj.dll
 7fef80a0000 4549d34c Nov 02 11:15:24 2006 C:\Windows\system32\CSCAPI.dll
 7fefa700000 4549d334 Nov 02 11:15:00 2006 c:\windows\system32\wdi.dll
 7fef74f0000 4549d311 Nov 02 11:14:25 2006 C:\Windows\system32\pcadm.dll
 7fef4350000 4549d308 Nov 02 11:14:16 2006 c:\windows\system32\netman.dll
 7fef4410000 4549d318 Nov 02 11:14:32 2006 c:\windows\system32\RASAPI32.dll
 7fef7150000 4549d320 Nov 02 11:14:40 2006 c:\windows\system32\rasman.dll
 7fef6ea0000 4549d32c Nov 02 11:14:52 2006 c:\windows\system32\TAPI32.dll
 7fefc2c0000 4549d329 Nov 02 11:14:49 2006 c:\windows\system32\rtutils.dll
 7fefb360000 4549d36f Nov 02 11:15:59 2006 c:\windows\system32\WINMM.dll
 7fefb310000 4549d318 Nov 02 11:14:32 2006 c:\windows\system32\OLEACC.dll
 7fefd280000 4549d370 Nov 02 11:16:00 2006 c:\windows\system32\WINNSI.DLL
 7fef5540000 4549d30f Nov 02 11:14:23 2006 C:\Windows\System32\netshell.dll
 7fefcb80000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\System32\IPHLPAPI.DLL
 7fefcb30000 4549d263 Nov 02 11:11:31 2006 C:\Windows\System32\dhcpcsvc.DLL
 7fefce40000 4549d288 Nov 02 11:12:08 2006 C:\Windows\System32\DNSAPI.dll
 7fefcb00000 4549d264 Nov 02 11:11:32 2006 C:\Windows\System32\dhcpcsvc6.DLL
 7fefc1a0000 4549d314 Nov 02 11:14:28 2006 C:\Windows\System32\nlaapi.dll
 7fef4470000 4549d31e Nov 02 11:14:38 2006 C:\Windows\System32\RASDLG.dll
 7fef6d00000 4549d2b3 Nov 02 11:12:51 2006 C:\Windows\System32\MPRAPI.dll
 7fefaad0000 4549d254 Nov 02 11:11:16 2006 C:\Windows\System32\ACTIVEDS.dll
 7fefaa00000 4549d263 Nov 02 11:11:31 2006 C:\Windows\System32\adsldpc.dll
 7fefa9c0000 4549d342 Nov 02 11:15:14 2006 C:\Windows\System32\credui.dll
 7fefc180000 4549d253 Nov 02 11:11:15 2006 C:\Windows\System32\ATL.DLL
 7fef9250000 4549d286 Nov 02 11:12:06 2006 C:\Windows\System32\hnetcfg.dll
 7fefae90000 4549d36a Nov 02 11:15:54 2006 C:\Windows\System32\WINHTTP.dll
 7fefc8f0000 4549d2e7 Nov 02 11:13:43 2006 C:\Windows\system32\mswsock.dll
 7fefc560000 4549d3a3 Nov 02 11:16:51 2006 C:\Windows\system32\wshtcpip.dll
 7fef3a20000 4549d32a Nov 02 11:14:50 2006 C:\Windows\system32\upnp.dll
 7fefa990000 4549d324 Nov 02 11:14:44 2006 C:\Windows\system32\SSDPAPI.dll
 7fefd1f0000 4549d32f Nov 02 11:14:55 2006 C:\Windows\System32\SXS.DLL
 7fef92c0000 4549d2ff Nov 02 11:14:07 2006 C:\Windows\system32\netcfgx.dll
 7fefc1c0000 4549d251 Nov 02 11:11:13 2006 C:\Windows\System32\Cabinet.dll
 7fef9e20000 4549d342 Nov 02 11:15:14 2006 C:\Windows\system32\wbem\wbemprox.dll
 7fef9f50000 4549d33d Nov 02 11:15:09 2006 C:\Windows\system32\wbem\wbemcomn.dll
 7fef96d0000 4549d343 Nov 02 11:15:15 2006 C:\Windows\system32\wbem\wbemsvc.dll
 7fef9040000 4549d274 Nov 02 11:11:48 2006 C:\Windows\system32\wbem\fastprox.dll
 7fefcdd0000 4549d375 Nov 02 11:16:05 2006 C:\Windows\system32\NTDSAPI.dll
 7fef65c0000 4549d30f Nov 02 11:14:23 2006 C:\Windows\system32\radardt.dll
 7fefca50000 4549d336 Nov 02 11:15:02 2006 C:\Windows\System32\VERSION.dll
SubSystemData:     0000000000000000
ProcessHeap:       0000000000170000
ProcessParameters: 0000000000171d20
```

```
    WindowTitle:  'C:\Windows\System32\svchost.exe'
    ImageFile:    'C:\Windows\System32\svchost.exe'
    CommandLine:  'C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted'
    DllPath:
'C:\Windows\System32;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Wind
ows;C:\Windows\System32\Wbem'
    Environment:  0000000000171310
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\system32\config\systemprofile\AppData\Roaming
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        LOCALAPPDATA=C:\Windows\system32\config\systemprofile\AppData\Local
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\TEMP
        TMP=C:\Windows\TEMP
        USERDOMAIN=DOMAIN
        USERNAME=COMPUTERNAME$
        USERPROFILE=C:\Windows\system32\config\systemprofile
        windir=C:\Windows


        THREAD fffffa8004480bb0  Cid 018c.0110  Teb: 000007fffffde000 Win32Thread: fffff900c07cea60
WAIT: (Executive) UserMode Non-Alertable
            fffffa80044810e8  NotificationEvent
        IRP List:
            fffffa80041a68f0: (0006,0118) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004484c10       Image:         svchost.exe
        Wait Start TickCount      7418           Ticks: 39161 (0:00:10:10.915)
        Context Switch Count      141                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address svchost!wmainCRTStartup (0x00000000ff912550)
        Stack Init fffff9800d17adb0 Current fffff9800d17a7f0
        Base fffff9800d17b000 Limit fffff9800d174000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0d17a830 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0d17a970 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0d17a9d0 fffff800`01ebdf16 nt!KeWaitForSingleObject+0x5f5
        fffff980`0d17aa50 fffff800`01ea1a24 nt!IopSynchronousServiceTail+0x306
        fffff980`0d17aac0 fffff800`01c4d733 nt!NtReadFile+0x583
        fffff980`0d17abb0 00000000`76e202da nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0d17ac20)
        00000000`000af748 00000000`76bf26da ntdll!NtReadFile+0xa
        00000000`000af750 000007fe`fea865aa kernel32!ReadFile+0x8a
        00000000`000af7e0 000007fe`fea862e3 ADVAPI32!ScGetPipeInput+0x4a
        00000000`000af8c0 000007fe`fea850f3 ADVAPI32!ScDispatcherLoop+0x9a
        00000000`000af9c0 00000000`ff91283c ADVAPI32!StartServiceCtrlDispatcherW+0x176
        00000000`000afc60 00000000`ff912666 svchost!wmain+0xe5
        00000000`000afc90 00000000`76bfcdcd svchost!ScCreateWellKnownSids+0x301
        00000000`000afcd0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
```

```
        00000000`000afd00 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80044fc700  Cid 018c.01f0  Teb: 000007fffffda000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa80044f1040  SynchronizationTimer
            fffffa80044f3170  NotificationEvent
            fffffa80044eed50  SynchronizationTimer
            fffffa8004580ba0  SynchronizationEvent
            fffffa8004520700  NotificationEvent
            fffffa8004576440  NotificationEvent
            fffffa80044ee340  SynchronizationTimer
            fffffa8002966220  NotificationEvent
            fffffa800480a110  SynchronizationTimer
            fffffa800480c040  SynchronizationEvent
            fffffa8002945820  Semaphore Limit 0x7fffffff
            fffffa80048035d0  SynchronizationEvent
            fffffa8004803040  SynchronizationEvent
            fffffa80048134b0  SynchronizationEvent
            fffffa8004b3e8e0  SynchronizationEvent
            fffffa8004569260  NotificationEvent
            fffffa8004b8a9c0  ProcessObject
            fffffa8004abb870  NotificationEvent
            fffffa8004bf7840  NotificationEvent
            fffffa80039ddf80  SynchronizationEvent
            fffffa800206fd90  SynchronizationEvent
            fffffa800495a170  SynchronizationEvent
            fffffa8001efe930  SynchronizationEvent
            fffffa80047711d0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004484c10       Image:         svchost.exe
        Wait Start TickCount      27354          Ticks: 19225 (0:00:04:59.911)
        Context Switch Count      57
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x0000000076df6930)
        Stack Init fffff9800cc29db0 Current fffff9800cc29260
        Base fffff9800cc2a000 Limit fffff9800cc24000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0cc292a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0cc293e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0cc29440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0cc294b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0cc29960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0cc29bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0cc29c20)
        00000000`0189fbb8 00000000`76df6b07 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0189fbc0 00000000`76bfcdcd ntdll!TppWaiterpThread+0x14d
        00000000`0189fe60 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0189fe90 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004481bb0  Cid 018c.01ec  Teb: 000007fffffdc000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa80044873c0  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004484c10       Image:         svchost.exe
        Wait Start TickCount      1569           Ticks: 45010 (0:00:11:42.160)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address audiosrv!EventWorkerThread (0x000007fefc232fb0)
        Stack Init fffff9800cc37db0 Current fffff9800cc37810
        Base fffff9800cc38000 Limit fffff9800cc32000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0cc37850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0cc37990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0cc379f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0cc37a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`0cc37b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`0cc37bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0cc37c20)
        00000000`0167f958 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`0167f960 000007fe`fc232ff8 kernel32!GetQueuedCompletionStatus+0x48
        00000000`0167f9c0 00000000`76bfcdcd audiosrv!EventWorkerThread+0x75
        00000000`0167fa00 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0167fa30 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80044f8540  Cid 018c.0230  Teb: 000007fffffd6000 Win32Thread: fffff900c07d1a50
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa80044f83e0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004484c10       Image:         svchost.exe
        Wait Start TickCount      2941           Ticks: 43638 (0:00:11:20.757)
        Context Switch Count      26                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address MMDevAPI!CDeviceEnumerator::PnpNotificationThreadWrapper
(0x000007fefc2eade0)
        Stack Init fffff9800d1ffdb0 Current fffff9800d1ff740
        Base fffff9800d200000 Limit fffff9800d1f8000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0d1ff780 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0d1ff8c0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0d1ff920 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`0d1ff9a0 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`0d1ffa40 fffff960`000c7e1e win32k!xxxSleepThread+0x56
        fffff980`0d1ffa70 fffff960`000c7f25 win32k!xxxRealInternalGetMessage+0x72e
        fffff980`0d1ffb50 fffff960`000c97e4 win32k!xxxInternalGetMessage+0x35
        fffff980`0d1ffb90 fffff800`01c4d733 win32k!NtUserGetMessage+0x64
        fffff980`0d1ffc20 00000000`76d1e6aa nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0d1ffc20)
        00000000`01eff758 00000000`76d1e6ea USER32!ZwUserGetMessage+0xa
        00000000`01eff760 000007fe`fc2e19f2 USER32!GetMessageW+0x34
        00000000`01eff790 00000000`76bfcdcd MMDevAPI!CDeviceEnumerator::PnpNotificationThread+0x25d
        00000000`01eff8b0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`01eff8e0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80044fdbb0  Cid 018c.0224  Teb: 000007fffffac000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80044f8e90  SynchronizationEvent
            fffffa80044f7cc0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004484c10       Image:         svchost.exe
        Wait Start TickCount      1577           Ticks: 45002 (0:00:11:42.035)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address MMDevAPI!CNotificationDelegator::HardwarePollingThreadProc
(0x000007fefc3016a0)
        Stack Init fffff9800ba97db0 Current fffff9800ba97260
        Base fffff9800ba98000 Limit fffff9800ba92000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0ba972a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0ba973e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0ba97440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0ba974b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0ba97960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0ba97bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0ba97c20)
        00000000`0204f958 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0204f960 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0204fa70 000007fe`fc3016dd kernel32!WaitForMultipleObjects+0x11
        00000000`0204fab0 00000000`76bfcdcd
MMDevAPI!CNotificationDelegator::HardwarePollingThreadProc+0x3d
        00000000`0204faf0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0204fb20 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa800457fbb0  Cid 018c.03c8  Teb: 000007fffffd8000 Win32Thread: fffff900c07d4d60
WAIT: (UserRequest) UserMode Alertable
            fffffa800457c830  NotificationEvent
            fffffa800450b5d0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004484c10       Image:         svchost.exe
        Wait Start TickCount      43898          Ticks: 2681 (0:00:00:41.823)
        Context Switch Count      139                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address ADVAPI32!ScSvcctrlThreadW (0x000007fefea84bd0)
        Stack Init fffff9800db1bdb0 Current fffff9800db1b260
        Base fffff9800db1c000 Limit fffff9800db12000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0db1b2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0db1b3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0db1b440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0db1b4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0db1b960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0db1bbb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0db1bc20)
        00000000`0214f788 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0214f790 00000000`76d1e96d kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0214f8a0 00000000`76d1e85e USER32!RealMsgWaitForMultipleObjectsEx+0x129
        00000000`0214f940 000007fe`fba05e76 USER32!MsgWaitForMultipleObjectsEx+0x46
        00000000`0214f980 000007fe`fb9e9236 cscsvc!CscUtil_WaitAndProcessThreadMessages+0x56
        00000000`0214fa00 000007fe`fb9e997d cscsvc!CscService_MainLoop+0x66
        00000000`0214fb30 00000000`ff911771 cscsvc!CscServiceMain+0x4b1
        00000000`0214fd70 000007fe`fea84bf5 svchost!ServiceStarter+0x1ea
        00000000`0214fe00 00000000`76bfcdcd ADVAPI32!ScSvcctrlThreadW+0x25
        00000000`0214fe30 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0214fe60 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800457d710  Cid 018c.0240  Teb: 000007fffffa8000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa80044fb880  NotificationEvent
            fffffa80044fba90  NotificationEvent
            fffffa80045790c0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004484c10       Image:         svchost.exe
        Wait Start TickCount      1649           Ticks: 44930 (0:00:11:40.912)
        Context Switch Count      139
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address cscsvc!SettingsChgMon_ThreadProc (0x000007fefb9f22ec)
        Stack Init fffff9800cc61db0 Current fffff9800cc61260
        Base fffff9800cc62000 Limit fffff9800cc5c000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0cc612a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0cc613e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0cc61440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0cc614b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0cc61960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0cc61bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0cc61c20)
        00000000`00f0f978 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`00f0f980 000007fe`fb9f24d1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`00f0fa90 00000000`76bfcdcd cscsvc!SettingsChgMon_ThreadProc+0x1e5
        00000000`00f0fb20 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`00f0fb50 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80045e00d0  Cid 018c.0404  Teb: 000007fffffa6000 Win32Thread: fffff900c07d8010
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80045c4290  NotificationEvent
            fffffa800474dfe0  NotificationEvent
            fffffa800451f040  NotificationEvent
            fffffa80045c37a0  NotificationEvent
            fffffa800474ca50  NotificationEvent
            fffffa800474c9f0  NotificationEvent
            fffffa800457ade0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004484c10       Image:         svchost.exe
        Wait Start TickCount      2770           Ticks: 43809 (0:00:11:23.424)
        Context Switch Count      22                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address cscsvc!CscAgentp_ThreadProc (0x000007fefb9d2078)
        Stack Init fffff9800db41db0 Current fffff9800db41260
        Base fffff9800db42000 Limit fffff9800db3b000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0db412a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0db413e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0db41440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0db414b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0db41960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0db41bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0db41c20)
        00000000`01fcf958 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`01fcf960 00000000`76d1e96d kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`01fcfa70 00000000`76d1e85e USER32!RealMsgWaitForMultipleObjectsEx+0x129
        00000000`01fcfb10 000007fe`fba05e76 USER32!MsgWaitForMultipleObjectsEx+0x46
        00000000`01fcfb50 000007fe`fb9d219b cscsvc!CscUtil_WaitAndProcessThreadMessages+0x56
        00000000`01fcfbd0 00000000`76bfcdcd cscsvc!CscAgentp_ThreadProc+0x123
        00000000`01fcfc50 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`01fcfc80 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800474d370  Cid 018c.0408  Teb: 000007fffffa4000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8004787058  QueueObject
        IRP List:
            fffffa80046ae010: (0006,01f0) Flags: 00060800  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004484c10       Image:         svchost.exe
        Wait Start TickCount      1743           Ticks: 44836 (0:00:11:39.446)
        Context Switch Count      12
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address cscsvc!CscDriverpUpcallThreadRoutine (0x000007fefba0a950)
        Stack Init fffff9800d097db0 Current fffff9800d096dc0
        Base fffff9800d098000 Limit fffff9800d092000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0d096e00 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0d096f40 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0d096fa0 fffff800`01c34eb1 nt!KeRemoveQueueEx+0x848
        fffff980`0d097030 fffff980`04caf18a nt!KeRemoveQueue+0x21
        fffff980`0d097070 fffff980`04cad808 csc!UpCallRemoveQueueRequest+0x46
        fffff980`0d0970f0 fffff980`04cac935 csc!CscDclInternalFsControl+0x2068
        fffff980`0d097180 fffff980`04c78dbe csc!CscDclInternalFsControl+0x1195
        fffff980`0d0972e0 fffff980`04dc934c csc!CscFsCtl+0x18e
        fffff980`0d097350 fffff980`04dd1ff2 rdbss!RxLowIoSubmit+0x29c
        fffff980`0d0973b0 fffff980`04dd2b19 rdbss!RxLowIoFsCtlShell+0x1c2
        fffff980`0d097420 fffff980`04da063c rdbss!RxCommonFileSystemControl+0xac9
        fffff980`0d097550 fffff980`04dc219a rdbss!RxFsdCommonDispatch+0x77c
        fffff980`0d097640 fffff980`04c67f90 rdbss!RxFsdDispatch+0x21a
        fffff980`0d0976b0 fffff980`04c6e4e2 csc!CscFsdDispatch+0x2e0
        fffff980`0d097730 fffff980`00be23db csc!CscSurrogatePreProcess+0x802
        fffff980`0d097840 fffff980`00be218f mup!MupCallSurrogatePrePost+0x10b
        fffff980`0d0978a0 fffff980`00be424f mup!MupStateMachine+0x13f
        fffff980`0d0978f0 fffff980`004d721a mup!MupFsControl+0x7f
        fffff980`0d097930 fffff980`004f39e2
fltmgr!FltpLegacyProcessingAfterPreCallbacksCompleted+0x20a
        fffff980`0d0979a0 fffff800`01e8dee7 fltmgr!FltpFsControl+0x102
        fffff980`0d097a00 fffff800`01eab906 nt!IopXxxControlFile+0x626
        fffff980`0d097b40 fffff800`01c4d733 nt!NtFsControlFile+0x56
        fffff980`0d097bb0 00000000`76e2060a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0d097c20)
        00000000`022ef848 000007fe`fba09782 ntdll!NtFsControlFile+0xa
        00000000`022ef850 000007fe`fba0aa8c cscsvc!CscDriverOpenItem+0x31a
        00000000`022ef8e0 00000000`76bfcdcd cscsvc!CscDriverpUpcallThreadRoutine+0x13c
        00000000`022ef9d0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`022efa00 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004562060  Cid 018c.049c  Teb: 000007fffff9a000 Win32Thread: 0000000000000000
WAIT: (WrLpcReceive) UserMode Non-Alertable
            fffffa80045623f0  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004484c10       Image:         svchost.exe
        Wait Start TickCount      15650          Ticks: 30929 (0:00:08:02.495)
        Context Switch Count      62
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address uxsms!CPortBase::PortThread (0x000007fefc175088)
        Stack Init fffff9800da97db0 Current fffff9800da977f0
        Base fffff9800da98000 Limit fffff9800da92000 Call 0
        Priority 13 BasePriority 8 PriorityDecrement 3 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0da97830 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0da97970 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0da979d0 fffff800`01eb3788 nt!KeWaitForSingleObject+0x5f5
        fffff980`0da97a50 fffff800`01e7e523 nt!AlpcpReceiveMessagePort+0x298
        fffff980`0da97ab0 fffff800`01e740d2 nt!AlpcpReceiveLegacyMessage+0x122
        fffff980`0da97b50 fffff800`01e724bf nt!NtReplyWaitReceivePortEx+0xc1
        fffff980`0da97be0 fffff800`01c4d733 nt!NtReplyWaitReceivePort+0xf
        fffff980`0da97c20 00000000`76e2032a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0da97c20)
        00000000`0265fc58 000007fe`fc174ff7 ntdll!NtReplyWaitReceivePort+0xa
        00000000`0265fc60 000007fe`fc175091 uxsms!CPortBase::PortThreadInternal+0xbf
        00000000`0265fcc0 00000000`76bfcdcd uxsms!CPortBase::PortThread+0x9
        00000000`0265fcf0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0265fd20 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004562700  Cid 018c.04a4  Teb: 000007fffff9e000 Win32Thread: fffff900c07db010
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa800408f4c0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004484c10       Image:         svchost.exe
        Wait Start TickCount      1618           Ticks: 44961 (0:00:11:41.396)
        Context Switch Count      145                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ADVAPI32!ScSvcctrlThreadW (0x000007fefea84bd0)
        Stack Init fffff9800bbb3db0 Current fffff9800bbb3740
        Base fffff9800bbb4000 Limit fffff9800bbad000 Call 0
        Priority 13 BasePriority 8 PriorityDecrement 5 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0bbb3780 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0bbb38c0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0bbb3920 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`0bbb39a0 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`0bbb3a40 fffff960`000c7e1e win32k!xxxSleepThread+0x56
        fffff980`0bbb3a70 fffff960`000c7f25 win32k!xxxRealInternalGetMessage+0x72e
        fffff980`0bbb3b50 fffff960`000c97e4 win32k!xxxInternalGetMessage+0x35
        fffff980`0bbb3b90 fffff800`01c4d733 win32k!NtUserGetMessage+0x64
        fffff980`0bbb3c20 00000000`76d1e6aa nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0bbb3c20)
        00000000`0282fc38 00000000`76d1e6ea USER32!ZwUserGetMessage+0xa
        00000000`0282fc40 000007fe`fb4b7aac USER32!GetMessageW+0x34
        00000000`0282fc70 00000000`ff911771 tabsvc!CServiceModule::ServiceMain+0x17c
        00000000`0282fd00 000007fe`fea84bf5 svchost!ServiceStarter+0x1ea
        00000000`0282fd90 00000000`76bfcdcd ADVAPI32!ScSvcctrlThreadW+0x25
        00000000`0282fdc0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0282fdf0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004550870  Cid 018c.04a8  Teb: 000007fffff98000 Win32Thread: fffff900c07fcab0
WAIT: (WrQueue) UserMode Alertable
            fffffa80044e39a0  QueueObject
        IRP List:
            fffffa8004815010: (0006,0358) Flags: 00060800  Mdl: 00000000
            fffffa8004809b20: (0006,0358) Flags: 00060000  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004484c10       Image:         svchost.exe
        Wait Start TickCount      43898          Ticks: 2681 (0:00:00:41.823)
        Context Switch Count      146                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address ntdll!TppWorkerThread (0x0000000076e17860)
        Stack Init fffff980108e2db0 Current fffff980108e2860
        Base fffff980108e3000 Limit fffff980108da000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`108e28a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`108e29e0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`108e2a40 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`108e2ad0 fffff800`01c8a722 nt!IoRemoveIoCompletion+0x47
        fffff980`108e2b50 fffff800`01c4d733 nt!NtWaitForWorkViaWorkerFactory+0x1f1
        fffff980`108e2c20 00000000`76e21b4a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`108e2c20)
        00000000`0240f7d8 00000000`76e17a20 ntdll!NtWaitForWorkViaWorkerFactory+0xa
        00000000`0240f7e0 00000000`76bfcdcd ntdll!TppWorkerThread+0x23e
        00000000`0240fa50 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0240fa80 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004569bb0  Cid 018c.04d4  Teb: 000007fffff96000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa8004391c20  SynchronizationEvent
            fffffa8003f9d210  SynchronizationEvent
            fffffa80043702c0  SynchronizationEvent
            fffffa8004b5f9c0  SynchronizationEvent
            fffffa8004b48bf0  SynchronizationEvent
            fffffa8004b48b70  SynchronizationEvent
            fffffa8004b5fa40  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004484c10       Image:         svchost.exe
        Wait Start TickCount      2776           Ticks: 43803 (0:00:11:23.331)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address msvcrt!endthreadex (0x000007fefdd59620)
        Stack Init fffff9800da6ddb0 Current fffff9800da6d260
        Base fffff9800da6e000 Limit fffff9800da68000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0da6d2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0da6d3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0da6d440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0da6d4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0da6d960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0da6dbb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0da6dc20)
        00000000`028df028 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`028df030 000007fe`fb4b8c65 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`028df140 000007fe`fdd594e7 tabsvc!CServiceModule::MonitorThreadProc+0x669
        00000000`028df770 000007fe`fdd5967d msvcrt!endthreadex+0x47
        00000000`028df7a0 00000000`76bfcdcd msvcrt!endthreadex+0x100
        00000000`028df7d0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`028df800 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8002963bb0  Cid 018c.0738  Teb: 000007fffff92000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8002966cd0  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004484c10       Image:         svchost.exe
        Wait Start TickCount      1985           Ticks: 44594 (0:00:11:35.670)
        Context Switch Count      2743
        UserTime                  00:00:00.000
        KernelTime                00:00:00.187
        Win32 Start Address ADVAPI32!ScSvcctrlThreadW (0x000007fefea84bd0)
        Stack Init fffff9800eaeddb0 Current fffff9800eaed960
        Base fffff9800eaee000 Limit fffff9800eae8000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0eaed9a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0eaedae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0eaedb40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0eaedbc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0eaedc20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0eaedc20)
        00000000`02abfb98 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`02abfba0 000007fe`fa5562ea kernel32!WaitForSingleObjectEx+0x9c
        00000000`02abfc60 000007fe`fa54c12c emdmgmt!EcSvcMainThread+0x7e
        00000000`02abfca0 00000000`ff911771 emdmgmt!EMDMgmtServiceMain+0xd4
        00000000`02abfcf0 000007fe`fea84bf5 svchost!ServiceStarter+0x1ea
        00000000`02abfd80 00000000`76bfcdcd ADVAPI32!ScSvcctrlThreadW+0x25
        00000000`02abfdb0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02abfde0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80047f0060  Cid 018c.0768  Teb: 000007fffff8e000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Alertable
            fffffa8004771230  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004484c10       Image:         svchost.exe
        Wait Start TickCount      27354          Ticks: 19225 (0:00:04:59.911)
        Context Switch Count      12
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x0000000076e17860)
        Stack Init fffff9800eb9ddb0 Current fffff9800eb9d860
        Base fffff9800eb9e000 Limit fffff9800eb98000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0eb9d8a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0eb9d9e0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0eb9da40 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0eb9dad0 fffff800`01c8a722 nt!IoRemoveIoCompletion+0x47
        fffff980`0eb9db50 fffff800`01c4d733 nt!NtWaitForWorkViaWorkerFactory+0x1f1
        fffff980`0eb9dc20 00000000`76e21b4a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0eb9dc20)
        00000000`02ebfb58 00000000`76e17a20 ntdll!NtWaitForWorkViaWorkerFactory+0xa
        00000000`02ebfb60 00000000`76bfcdcd ntdll!TppWorkerThread+0x23e
        00000000`02ebfdd0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02ebfe00 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004800060  Cid 018c.07a0  Teb: 000007fffff90000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004619bf0  NotificationEvent
            fffffa8001883fe0  NotificationEvent
            fffffa8001883ee0  SynchronizationEvent
            fffffa8004904900  SynchronizationTimer
            fffffa800494d040  SynchronizationTimer
            fffffa8004904790  NotificationEvent
            fffffa8001883f60  SynchronizationEvent
            fffffa80018814f0  SynchronizationEvent
        Impersonation token:  fffff88001cae060 (Level Impersonation)
        Owning Process            fffffa8004484c10       Image:         svchost.exe
        Wait Start TickCount      46556          Ticks: 23 (0:00:00:00.358)
        Context Switch Count      5543
        UserTime                  00:00:03.010
        KernelTime                00:00:01.263
        Win32 Start Address ADVAPI32!ScSvcctrlThreadW (0x000007fefea84bd0)
        Stack Init fffff9800ead8db0 Current fffff9800ead8260
        Base fffff9800ead9000 Limit fffff9800ead3000 Call 0
        Priority 7 BasePriority 7 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0ead82a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0ead83e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0ead8440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0ead84b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0ead8960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0ead8bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0ead8c20)
        00000000`0297f128 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0297f130 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0297f240 000007fe`fa12bdc4 kernel32!WaitForMultipleObjects+0x11
        00000000`0297f280 000007fe`fa115c58 sysmain!PfSvcMainThread+0x994
        00000000`0297fd10 00000000`ff911771 sysmain!SysMtServiceMain+0xe0
        00000000`0297fd60 000007fe`fea84bf5 svchost!ServiceStarter+0x1ea
        00000000`0297fdf0 00000000`76bfcdcd ADVAPI32!ScSvcctrlThreadW+0x25
        00000000`0297fe20 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0297fe50 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004918a40  Cid 018c.0874  Teb: 000007fffff8c000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80043ab630  SynchronizationEvent
            fffffa800431b390  SynchronizationEvent
            fffffa8004929b50  SynchronizationEvent
            fffffa8004929af0  SynchronizationEvent
            fffffa800491cef0  SynchronizationTimer
            fffffa800491cca0  SynchronizationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004484c10       Image:         svchost.exe
        Wait Start TickCount      46232          Ticks: 347 (0:00:00:05.413)
        Context Switch Count      1728
        UserTime                  00:00:05.803
        KernelTime                00:00:01.045
        Win32 Start Address emdmgmt!EcSvcWorkThread (0x000007fefa557d1c)
        Stack Init fffff9800e362db0 Current fffff9800e362260
        Base fffff9800e363000 Limit fffff9800e35d000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0e3622a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e3623e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0e362440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0e3624b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0e362960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0e362bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e362c20)
        00000000`02b3f648 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`02b3f650 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`02b3f760 000007fe`fa557d55 kernel32!WaitForMultipleObjects+0x11
        00000000`02b3f7a0 00000000`76bfcdcd emdmgmt!EcSvcWorkThread+0x39
        00000000`02b3f880 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02b3f8b0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004bc4060  Cid 018c.08a8  Teb: 000007fffffaa000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80043b68b0  SynchronizationEvent
        Impersonation token:  fffff880025ba720 (Level Impersonation)
        Owning Process            fffffa8004484c10       Image:         svchost.exe
        Wait Start TickCount      43633          Ticks: 2946 (0:00:00:45.957)
        Context Switch Count      34357
        UserTime                  00:00:00.109
        KernelTime                00:00:03.900
        Win32 Start Address sysmain!PfRbPrefetchWorker (0x000007fefa155530)
        Stack Init fffff98012bd5db0 Current fffff98012bd5960
        Base fffff98012bd6000 Limit fffff98012bd0000 Call 0
        Priority 8 BasePriority 7 PriorityDecrement 0 IoPriority 0 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`12bd59a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12bd5ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`12bd5b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`12bd5bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`12bd5c20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12bd5c20)
        00000000`0279fb28 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`0279fb30 000007fe`fa1555fd kernel32!WaitForSingleObjectEx+0x9c
        00000000`0279fbf0 00000000`76bfcdcd sysmain!PfRbPrefetchWorker+0xcd
        00000000`0279fc20 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0279fc50 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8001e9b6c0  Cid 018c.0790  Teb: 000007fffff9c000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8001e71400  Semaphore Limit 0x7fffffff
            fffffa8004721710  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004484c10       Image:         svchost.exe
        Wait Start TickCount      40451          Ticks: 6128 (0:00:01:35.597)
        Context Switch Count      38
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ADVAPI32!ScSvcctrlThreadW (0x000007fefea84bd0)
        Stack Init fffff980102e0db0 Current fffff980102e0260
        Base fffff980102e1000 Limit fffff980102db000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`102e02a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`102e03e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`102e0440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`102e04b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`102e0960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`102e0bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`102e0c20)
        00000000`02bdf7f8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`02bdf800 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`02bdf910 000007fe`fa70883a kernel32!WaitForMultipleObjects+0x11
        00000000`02bdf950 000007fe`fa70e2e6 wdi!WdipHostListener+0xe6
        00000000`02bdfa00 000007fe`fa70e974 wdi!WdipTriggerHost+0x25a
        00000000`02bdfa60 00000000`ff911771 wdi!ServiceMain+0x108
        00000000`02bdfaa0 000007fe`fea84bf5 svchost!ServiceStarter+0x1ea
        00000000`02bdfb30 00000000`76bfcdcd ADVAPI32!ScSvcctrlThreadW+0x25
        00000000`02bdfb60 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02bdfb90 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8002004060  Cid 018c.0a90  Teb: 000007fffff8a000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8004b4c830  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004484c10       Image:         svchost.exe
        Wait Start TickCount      16796          Ticks: 29783 (0:00:07:44.617)
        Context Switch Count      65
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdi!WdipSessionListener (0x000007fefa708ad0)
        Stack Init fffff980108c1db0 Current fffff980108c1810
        Base fffff980108c2000 Limit fffff980108bc000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`108c1850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`108c1990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`108c19f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`108c1a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`108c1b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`108c1bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`108c1c20)
        00000000`02a3fa08 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`02a3fa10 000007fe`fa708b94 kernel32!GetQueuedCompletionStatus+0x48
        00000000`02a3fa70 00000000`76bfcdcd wdi!WdipSessionListener+0xc4
        00000000`02a3fb10 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02a3fb40 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800200abb0  Cid 018c.042c  Teb: 000007fffff88000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8004b4c830  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004484c10       Image:         svchost.exe
        Wait Start TickCount      7401           Ticks: 39178 (0:00:10:11.180)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdi!WdipSessionListener (0x000007fefa708ad0)
        Stack Init fffff9800d0acdb0 Current fffff9800d0ac810
        Base fffff9800d0ad000 Limit fffff9800d0a7000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0d0ac850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0d0ac990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0d0ac9f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0d0aca80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`0d0acb00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`0d0acbb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0d0acc20)
        00000000`02cbf888 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`02cbf890 000007fe`fa708b94 kernel32!GetQueuedCompletionStatus+0x48
        00000000`02cbf8f0 00000000`76bfcdcd wdi!WdipSessionListener+0xc4
        00000000`02cbf990 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02cbf9c0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa800201a060  Cid 018c.0844  Teb: 000007fffff86000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8004b4c830  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004484c10       Image:         svchost.exe
        Wait Start TickCount      40451          Ticks: 6128 (0:00:01:35.597)
        Context Switch Count      99
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdi!WdipSessionListener (0x000007fefa708ad0)
        Stack Init fffff980107fddb0 Current fffff980107fd810
        Base fffff980107fe000 Limit fffff980107f8000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`107fd850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`107fd990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`107fd9f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`107fda80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`107fdb00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`107fdbb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`107fdc20)
        00000000`03e3fa98 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`03e3faa0 000007fe`fa708b94 kernel32!GetQueuedCompletionStatus+0x48
        00000000`03e3fb00 00000000`76bfcdcd wdi!WdipSessionListener+0xc4
        00000000`03e3fba0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`03e3fbd0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800201abb0  Cid 018c.08a4  Teb: 000007fffff84000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8004b4c830  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004484c10       Image:         svchost.exe
        Wait Start TickCount      7401           Ticks: 39178 (0:00:10:11.180)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdi!WdipSessionListener (0x000007fefa708ad0)
        Stack Init fffff980159cedb0 Current fffff980159ce810
        Base fffff980159cf000 Limit fffff980159c9000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`159ce850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`159ce990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`159ce9f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`159cea80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`159ceb00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`159cebb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`159cec20)
        00000000`03d3f8a8 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`03d3f8b0 000007fe`fa708b94 kernel32!GetQueuedCompletionStatus+0x48
        00000000`03d3f910 00000000`76bfcdcd wdi!WdipSessionListener+0xc4
        00000000`03d3f9b0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`03d3f9e0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa800201a700  Cid 018c.0bb4  Teb: 000007fffff82000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8004b4c830  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004484c10       Image:         svchost.exe
        Wait Start TickCount      16796          Ticks: 29783 (0:00:07:44.617)
        Context Switch Count      165
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address wdi!WdipSessionListener (0x000007fefa708ad0)
        Stack Init fffff98012ba4db0 Current fffff98012ba4810
        Base fffff98012ba5000 Limit fffff98012b9f000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`12ba4850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12ba4990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`12ba49f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`12ba4a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`12ba4b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`12ba4bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12ba4c20)
        00000000`03f4fac8 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`03f4fad0 000007fe`fa708b94 kernel32!GetQueuedCompletionStatus+0x48
        00000000`03f4fb30 00000000`76bfcdcd wdi!WdipSessionListener+0xc4
        00000000`03f4fbd0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`03f4fc00 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800201c060  Cid 018c.08f8  Teb: 000007fffff80000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8004b4c830  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004484c10       Image:         svchost.exe
        Wait Start TickCount      7412           Ticks: 39167 (0:00:10:11.009)
        Context Switch Count      52
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdi!WdipSessionListener (0x000007fefa708ad0)
        Stack Init fffff980159b2db0 Current fffff980159b2810
        Base fffff980159b3000 Limit fffff980159ad000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`159b2850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`159b2990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`159b29f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`159b2a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`159b2b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`159b2bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`159b2c20)
        00000000`06ccfd08 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`06ccfd10 000007fe`fa708b94 kernel32!GetQueuedCompletionStatus+0x48
        00000000`06ccfd70 00000000`76bfcdcd wdi!WdipSessionListener+0xc4
        00000000`06ccfe10 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`06ccfe40 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa800201cbb0  Cid 018c.08dc  Teb: 000007fffff7e000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8004b4c830  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004484c10       Image:         svchost.exe
        Wait Start TickCount      40451          Ticks: 6128 (0:00:01:35.597)
        Context Switch Count      93
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdi!WdipSessionListener (0x000007fefa708ad0)
        Stack Init fffff980157d1db0 Current fffff980157d1810
        Base fffff980157d2000 Limit fffff980157cc000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`157d1850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`157d1990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`157d19f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`157d1a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`157d1b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`157d1bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`157d1c20)
        00000000`03fefd08 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`03fefd10 000007fe`fa708b94 kernel32!GetQueuedCompletionStatus+0x48
        00000000`03fefd70 00000000`76bfcdcd wdi!WdipSessionListener+0xc4
        00000000`03fefe10 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`03fefe40 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800201c700  Cid 018c.07a4  Teb: 000007fffff7c000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8004b4c830  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004484c10       Image:         svchost.exe
        Wait Start TickCount      7411           Ticks: 39168 (0:00:10:11.024)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdi!WdipSessionListener (0x000007fefa708ad0)
        Stack Init fffff980157d8db0 Current fffff980157d8810
        Base fffff980157d9000 Limit fffff980157d3000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`157d8850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`157d8990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`157d89f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`157d8a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`157d8b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`157d8bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`157d8c20)
        00000000`0407f788 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`0407f790 000007fe`fa708b94 kernel32!GetQueuedCompletionStatus+0x48
        00000000`0407f7f0 00000000`76bfcdcd wdi!WdipSessionListener+0xc4
        00000000`0407f890 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0407f8c0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa800201d060  Cid 018c.0814  Teb: 000007fffff7a000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8004b4c830  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004484c10       Image:         svchost.exe
        Wait Start TickCount      7412           Ticks: 39167 (0:00:10:11.009)
        Context Switch Count      52
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address wdi!WdipSessionListener (0x000007fefa708ad0)
        Stack Init fffff980157dfdb0 Current fffff980157df810
        Base fffff980157e0000 Limit fffff980157da000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`157df850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`157df990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`157df9f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`157dfa80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`157dfb00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`157dfbb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`157dfc20)
        00000000`0238fc68 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`0238fc70 000007fe`fa708b94 kernel32!GetQueuedCompletionStatus+0x48
        00000000`0238fcd0 00000000`76bfcdcd wdi!WdipSessionListener+0xc4
        00000000`0238fd70 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0238fda0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800201dbb0  Cid 018c.06ac  Teb: 000007fffff78000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8004b4c830  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004484c10       Image:         svchost.exe
        Wait Start TickCount      16796          Ticks: 29783 (0:00:07:44.617)
        Context Switch Count      110
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdi!WdipSessionListener (0x000007fefa708ad0)
        Stack Init fffff980157e6db0 Current fffff980157e6810
        Base fffff980157e7000 Limit fffff980157e1000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`157e6850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`157e6990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`157e69f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`157e6a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`157e6b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`157e6bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`157e6c20)
        00000000`016ffae8 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`016ffaf0 000007fe`fa708b94 kernel32!GetQueuedCompletionStatus+0x48
        00000000`016ffb50 00000000`76bfcdcd wdi!WdipSessionListener+0xc4
        00000000`016ffbf0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`016ffc20 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80022783e0  Cid 018c.0eb4  Teb: 000007fffff72000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa80020926b0  QueueObject
            fffffa8002278498  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004484c10       Image:         svchost.exe
        Wait Start TickCount      46388          Ticks: 191 (0:00:00:02.979)
        Context Switch Count      223
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address pcasvc!PcapProcessChainThread (0x000007fefa695c50)
        Stack Init fffff9800da82db0 Current fffff9800da82810
        Base fffff9800da83000 Limit fffff9800da7d000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0da82850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0da82990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0da829f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0da82a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`0da82b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`0da82bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0da82c20)
        00000000`0759fcd8 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`0759fce0 000007fe`fa695c98 kernel32!GetQueuedCompletionStatus+0x48
        00000000`0759fd40 00000000`76bfcdcd pcasvc!PcapProcessChainThread+0x48
        00000000`0759fd80 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0759fdb0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80020c9bb0  Cid 018c.0da8  Teb: 000007fffff74000 Win32Thread: fffff900c2011530
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa8001f01540  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004484c10       Image:         svchost.exe
        Wait Start TickCount      32834          Ticks: 13745 (0:00:03:34.423)
        Context Switch Count      45                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address ole32!CRpcThreadCache::RpcWorkerThreadEntry (0x000007fefd7a3be0)
        Stack Init fffff980109ecdb0 Current fffff980109ec740
        Base fffff980109ed000 Limit fffff980109e5000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`109ec780 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`109ec8c0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`109ec920 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`109ec9a0 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`109eca40 fffff960`000c7e1e win32k!xxxSleepThread+0x56
        fffff980`109eca70 fffff960`000c7f25 win32k!xxxRealInternalGetMessage+0x72e
        fffff980`109ecb50 fffff960`000c97e4 win32k!xxxInternalGetMessage+0x35
        fffff980`109ecb90 fffff800`01c4d733 win32k!NtUserGetMessage+0x64
        fffff980`109ecc20 00000000`76d1e6aa nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`109ecc20)
        00000000`06e2f6d8 00000000`76d1e6ea USER32!ZwUserGetMessage+0xa
        00000000`06e2f6e0 000007fe`fd779d72 USER32!GetMessageW+0x34
        00000000`06e2f710 000007fe`fd77a0dd ole32!CDllHost::STAWorkerLoop+0x8a
        00000000`06e2f770 000007fe`fd7a3b7e ole32!CDllHost::WorkerThread+0xd7
        00000000`06e2f7b0 000007fe`fd7a3c0a ole32!CRpcThread::WorkerLoop+0x1e
        00000000`06e2f7f0 00000000`76bfcdcd ole32!CRpcThreadCache::RpcWorkerThreadEntry+0x2a
        00000000`06e2f820 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`06e2f850 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8002200b30  Cid 018c.0b20  Teb: 000007fffff70000 Win32Thread: 0000000000000000
WAIT: (WrLpcReply) UserMode Non-Alertable
            fffffa8002200ec0  Semaphore Limit 0x1
        Waiting for reply to ALPC Message fffff88000bcc030
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004484c10       Image:         svchost.exe
        Wait Start TickCount      10275          Ticks: 36304 (0:00:09:26.346)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address SSDPAPI!GetNotificationLoop (0x000007fefa995000)
        Stack Init fffff980102d9db0 Current fffff980102d96e0
        Base fffff980102da000 Limit fffff980102d4000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`102d9720 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`102d9860 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`102d98c0 fffff800`01c8f857 nt!KeWaitForSingleObject+0x5f5
        fffff980`102d9940 fffff800`01ebed64 nt!AlpcpSignalAndWait+0x97
        fffff980`102d9980 fffff800`01e9a80a nt!AlpcpReceiveSynchronousReply+0x44
        fffff980`102d99e0 fffff800`01eb747f nt!AlpcpProcessSynchronousRequest+0x257
        fffff980`102d9b00 fffff800`01c4d733 nt!NtAlpcSendWaitReceivePort+0x19f
        fffff980`102d9bb0 00000000`76e20aca nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`102d9c20)
        00000000`070df818 000007fe`fedba66b ntdll!NtAlpcSendWaitReceivePort+0xa
        00000000`070df820 000007fe`fedbd422 RPCRT4!LRPC_CCALL::SendReceive+0xbb
        00000000`070df8a0 000007fe`fedbd472 RPCRT4!I_RpcSendReceive+0x42
        00000000`070df8d0 000007fe`fee9a2bc RPCRT4!NdrSendReceive+0x32
        00000000`070df900 000007fe`fee9a3d0 RPCRT4!NdrpClientCall3+0x11c
        00000000`070dfb50 000007fe`fa995086 RPCRT4!NdrClientCall3+0x7c
        00000000`070dfec0 00000000`76bfcdcd SSDPAPI!GetNotificationLoop+0x86
        00000000`070dff40 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`070dff70 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004b35bb0  Cid 018c.0c8c  Teb: 000007fffffae000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa80044876c0  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004484c10       Image:         svchost.exe
        Wait Start TickCount      45934          Ticks: 645 (0:00:00:10.062)
        Context Switch Count      10
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff9800e29edb0 Current fffff9800e29e810
        Base fffff9800e29f000 Limit fffff9800e299000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0e29e850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e29e990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0e29e9f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0e29ea80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`0e29eb00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`0e29ebb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e29ec20)
        00000000`019af9e8 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`019af9f0 000007fe`fedce7a3 kernel32!GetQueuedCompletionStatus+0x48
        00000000`019afa50 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`019afae0 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`019afb90 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`019afbc0 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`019afc00 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`019afc30 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`019afc60 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8002011bb0  Cid 018c.0974  Teb: 000007fffffa0000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800249b2f0  NotificationEvent
            fffffa800189b570  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004484c10       Image:         svchost.exe
        Wait Start TickCount      40451          Ticks: 6128 (0:00:01:35.597)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address radardt!RdrpMonitorResources (0x000007fef65c9bec)
        Stack Init fffff9800b6a2db0 Current fffff9800b6a2260
        Base fffff9800b6a3000 Limit fffff9800b69d000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0b6a22a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0b6a23e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0b6a2440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0b6a24b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0b6a2960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0b6a2bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0b6a2c20)
        00000000`0259fbf8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0259fc00 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0259fd10 000007fe`f65c9a9d kernel32!WaitForMultipleObjects+0x11
        00000000`0259fd50 000007fe`f65c9d26 radardt!RdrpWaitForHighCommit+0xa5
        00000000`0259fd80 00000000`76bfcdcd radardt!RdrpMonitorResources+0x13a
        00000000`0259fe40 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0259fe70 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004383520  Cid 018c.09ac  Teb: 000007fffff94000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8002b1b780  NotificationEvent
            fffffa80020c3610  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004484c10       Image:         svchost.exe
        Wait Start TickCount      40451          Ticks: 6128 (0:00:01:35.597)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address radardt!RdrpMonitorCommitCharge (0x000007fef65cc3fc)
        Stack Init fffff9800b6c5db0 Current fffff9800b6c5260
        Base fffff9800b6c6000 Limit fffff9800b6c0000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0b6c52a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0b6c53e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0b6c5440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0b6c54b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0b6c5960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0b6c5bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0b6c5c20)
        00000000`0191f9c8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0191f9d0 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0191fae0 000007fe`f65cc4f3 kernel32!WaitForMultipleObjects+0x11
        00000000`0191fb20 00000000`76bfcdcd radardt!RdrpMonitorCommitCharge+0xf7
        00000000`0191fb70 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0191fba0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

Svchost process (netsvcs)

```
PROCESS fffffa80044d9c10
    SessionId: 0  Cid: 01a8    Peb: 7fffffd3000  ParentCid: 025c
    DirBase: 4d80d000  ObjectTable: fffff880051c8260  HandleCount: 1045.
    Image: svchost.exe
    VadRoot fffffa80044d9600 Vads 313 Clone 0 Private 4035. Modified 1822. Locked 3.
    DeviceMap fffff88000007820
    Token                             fffff880055f9060
    ElapsedTime                       00:11:42.923
    UserTime                          00:00:00.842
    KernelTime                        00:00:01.107
    QuotaPoolUsage[PagedPool]         261176
    QuotaPoolUsage[NonPagedPool]      70048
    Working Set Sizes (now,min,max)  (6854, 50, 345) (27416KB, 200KB, 1380KB)
    PeakWorkingSetSize                7627
    VirtualSize                       401 Mb
    PeakVirtualSize                   711 Mb
    PageFaultCount                    23665
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      5841

    Setting context for this process...
.process /p /r fffffa80044d9c10

    !peb
PEB at 000007fffffd3000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00000000ff910000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 0000000000312740 . 0000000002cfbfd0
    Ldr.InLoadOrderModuleList:           0000000000312650 . 0000000002cfbfb0
    Ldr.InMemoryOrderModuleList:         0000000000312660 . 0000000002cfbfc0
            Base TimeStamp                     Module
        ff910000 4549b5f5 Nov 02 09:10:13 2006 C:\Windows\system32\svchost.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        76bc0000 4549d328 Nov 02 11:14:48 2006 C:\Windows\system32\kernel32.dll
     7fefdd40000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\system32\msvcrt.dll
     7fefea30000 4549d267 Nov 02 11:11:35 2006 C:\Windows\system32\ADVAPI32.dll
     7fefed90000 469c43bb Jul 17 05:21:15 2007 C:\Windows\system32\RPCRT4.dll
     7fefc5b0000 4549d384 Nov 02 11:16:20 2006 C:\Windows\system32\NTMARTA.DLL
        76d00000 45d3ee19 Feb 15 05:22:33 2007 C:\Windows\system32\USER32.dll
     7fefec20000 4549d273 Nov 02 11:11:47 2006 C:\Windows\system32\GDI32.dll
     7fefd590000 4549d396 Nov 02 11:16:38 2006 C:\Windows\system32\WLDAP32.dll
     7fefd540000 4549d38a Nov 02 11:16:26 2006 C:\Windows\system32\WS2_32.dll
     7feff0b0000 4549d370 Nov 02 11:16:00 2006 C:\Windows\system32\NSI.dll
     7fefd530000 4549d310 Nov 02 11:14:24 2006 C:\Windows\system32\PSAPI.DLL
     7fefce20000 4549d315 Nov 02 11:14:29 2006 C:\Windows\system32\SAMLIB.dll
     7fefd760000 4549d317 Nov 02 11:14:31 2006 C:\Windows\system32\ole32.dll
     7fefd9e0000 4549d2cb Nov 02 11:13:15 2006 C:\Windows\system32\IMM32.DLL
     7fefdc30000 4549d2e6 Nov 02 11:13:42 2006 C:\Windows\system32\MSCTF.dll
     7feff0c0000 4549d2a1 Nov 02 11:12:33 2006 C:\Windows\system32\LPK.DLL
     7fefd940000 4549d337 Nov 02 11:15:03 2006 C:\Windows\system32\USP10.dll
     7fefc2a0000 4549d2a0 Nov 02 11:12:32 2006 c:\windows\system32\mmcss.dll
     7fefc2d0000 4549d273 Nov 02 11:11:47 2006 c:\windows\system32\AVRT.dll
     7fefb830000 4549d281 Nov 02 11:12:01 2006 c:\windows\system32\gpsvc.dll
     7fefd390000 4549d33f Nov 02 11:15:11 2006 c:\windows\system32\Secur32.dll
     7fefcf70000 4549d2fc Nov 02 11:14:04 2006 c:\windows\system32\NETAPI32.dll
     7fefcdd0000 4549d375 Nov 02 11:16:05 2006 c:\windows\system32\NTDSAPI.dll
     7fefce40000 4549d288 Nov 02 11:12:08 2006 c:\windows\system32\DNSAPI.dll
     7fefc450000 4549d34e Nov 02 11:15:26 2006 c:\windows\system32\WTSAPI32.dll
     7fefdab0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\OLEAUT32.dll
     7fefd3b0000 4549d336 Nov 02 11:15:02 2006 c:\windows\system32\USERENV.dll
```

```
     7fefc940000 4549d277 Nov 02 11:11:51 2006 c:\windows\system32\GPAPI.dll
     7fefcc20000 4549d32d Nov 02 11:14:53 2006 c:\windows\system32\slc.dll
     7fefd360000 4549d265 Nov 02 11:11:33 2006 c:\windows\system32\AUTHZ.dll
     7fefd350000 4549d33a Nov 02 11:15:06 2006 c:\windows\system32\SYSNTFY.dll
     7fefd1b0000 4549d380 Nov 02 11:16:16 2006 c:\windows\system32\WINSTA.dll
     7fefc1a0000 4549d314 Nov 02 11:14:28 2006 c:\windows\system32\nlaapi.dll
     7fefcb80000 4549d2e1 Nov 02 11:13:37 2006 c:\windows\system32\IPHLPAPI.DLL
     7fefcb30000 4549d263 Nov 02 11:11:31 2006 c:\windows\system32\dhcpcsvc.DLL
     7fefd280000 4549d370 Nov 02 11:16:00 2006 c:\windows\system32\WINNSI.DLL
     7fefcb00000 4549d264 Nov 02 11:11:32 2006 c:\windows\system32\dhcpcsvc6.DLL
     7fefc140000 4549d30c Nov 02 11:14:20 2006 c:\windows\system32\profsvc.dll
     7fefc180000 4549d253 Nov 02 11:11:15 2006 c:\windows\system32\ATL.DLL
     7fefb5c0000 4549d324 Nov 02 11:14:44 2006 c:\windows\system32\shsvcs.dll
     7fefb910000 4549d342 Nov 02 11:15:14 2006 c:\windows\system32\sens.dll
     7fefc330000 4549d33b Nov 02 11:15:07 2006 C:\Windows\system32\UxTheme.dll
     7fefc620000 4549d31d Nov 02 11:14:37 2006 C:\Windows\system32\rsaenh.dll
     7fefdb90000 4549d282 Nov 02 11:12:02 2006 C:\Windows\system32\CLBCatQ.DLL
     7fefaf00000 4549d246 Nov 02 11:11:02 2006 C:\Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.6000.16386_none_40339432230aebeb\COMCTL32.dll
     7fefeed0000 4549d318 Nov 02 11:14:32 2006 C:\Windows\system32\SETUPAPI.dll
     7fefc1e0000 4549d381 Nov 02 11:16:17 2006 C:\Windows\system32\WINTRUST.dll
     7fefcc50000 4549d344 Nov 02 11:15:16 2006 C:\Windows\system32\CRYPT32.dll
     7fefce00000 4549d2df Nov 02 11:13:35 2006 C:\Windows\system32\MSASN1.dll
     7fefda90000 462443ee Apr 17 04:50:06 2007 C:\Windows\system32\imagehlp.dll
     7fefc060000 4549d322 Nov 02 11:14:42 2006 c:\windows\system32\schedsvc.dll
     7fefb110000 4549d334 Nov 02 11:15:00 2006 c:\windows\system32\ktmw32.dll
     7fefda10000 4549d31f Nov 02 11:14:39 2006 C:\Windows\system32\SHLWAPI.dll
     7fefcbb0000 4549d349 Nov 02 11:15:21 2006 c:\windows\system32\wevtapi.dll
     7fefbe70000 4549d32b Nov 02 11:14:51 2006 C:\Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_1559f1c6f365a7fa\comctl32.dll
     7fefca40000 4549d341 Nov 02 11:15:13 2006 C:\Windows\system32\credssp.dll
     7fefc670000 4549d321 Nov 02 11:14:41 2006 C:\Windows\system32\schannel.dll
     7fefb100000 4549d354 Nov 02 11:15:32 2006 C:\Windows\system32\wiarpc.dll
     7fefae20000 4549d334 Nov 02 11:15:00 2006 C:\Windows\system32\taskcomp.dll
     7fefca50000 4549d336 Nov 02 11:15:02 2006 C:\Windows\system32\VERSION.dll
     7fefc8f0000 4549d2e7 Nov 02 11:13:43 2006 C:\Windows\system32\mswsock.dll
     7fefc560000 4549d3a3 Nov 02 11:16:51 2006 C:\Windows\system32\wshtcpip.dll
     7fefc980000 4549d39d Nov 02 11:16:45 2006 C:\Windows\System32\wship6.dll
     7fefabf0000 4549d321 Nov 02 11:14:41 2006 c:\windows\system32\srvsvc.dll
     7fefadc0000 4549d323 Nov 02 11:14:43 2006 C:\Windows\system32\SSCORE.DLL
     7fefc460000 466785ee Jun 07 05:13:34 2007 C:\Windows\system32\FirewallAPI.DLL
     7fefabc0000 4549d287 Nov 02 11:12:07 2006 C:\Windows\system32\CLUSAPI.DLL
     7fefaad0000 4549d254 Nov 02 11:11:16 2006 C:\Windows\system32\ACTIVEDS.dll
     7fefaa00000 4549d263 Nov 02 11:11:31 2006 C:\Windows\system32\adsldpc.dll
     7fefa9c0000 4549d342 Nov 02 11:15:14 2006 C:\Windows\system32\credui.dll
     7fefddf0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\SHELL32.dll
     7fefada0000 4549d33d Nov 02 11:15:09 2006 C:\Windows\system32\RESUTILS.DLL
     7fefaa90000 4549d26a Nov 02 11:11:38 2006 c:\windows\system32\aelupsvc.dll
     7fefd310000 4549d247 Nov 02 11:11:03 2006 c:\windows\system32\apphelp.dll
     7fefa4c0000 4549d2be Nov 02 11:13:02 2006 c:\windows\system32\ikeext.dll
     7fefac60000 4549d280 Nov 02 11:12:00 2006 c:\windows\system32\fwpuclnt.dll
     7fefcab0000 4549d2f2 Nov 02 11:13:54 2006 C:\Windows\system32\ncrypt.dll
     7fefca60000 4549d252 Nov 02 11:11:14 2006 C:\Windows\system32\BCRYPT.dll
     7fefa7d0000 4549d339 Nov 02 11:15:05 2006 c:\windows\system32\seclogon.dll
     7fef9fe0000 4549d3bb Nov 02 11:17:15 2006 c:\windows\system32\wbem\wmisvc.dll
     7fef9f50000 4549d33d Nov 02 11:15:09 2006 c:\windows\system32\wbem\wbemcomn.dll
     7fef97a0000 46678661 Jun 07 05:15:29 2007 c:\windows\system32\iphlpsvc.dll
     7fefc2c0000 4549d329 Nov 02 11:14:49 2006 c:\windows\system32\rtutils.dll
     7fef97f0000 4549d358 Nov 02 11:15:36 2006 c:\windows\system32\sqmapi.dll
     7fefc1c0000 4549d251 Nov 02 11:11:13 2006 C:\Windows\system32\Cabinet.dll
     7fefa800000 4549d33f Nov 02 11:15:11 2006 C:\Windows\system32\VSSAPI.DLL
     7fefa9a0000 4549d341 Nov 02 11:15:13 2006 C:\Windows\system32\vsstrace.dll
     7fefb930000 4549d350 Nov 02 11:15:28 2006 C:\Windows\system32\XmlLite.dll
     7fefcd90000 4549d2b2 Nov 02 11:12:50 2006 C:\Windows\system32\MPR.dll
     7fefb4d0000 4549d30d Nov 02 11:14:21 2006 C:\Windows\system32\PROPSYS.dll
     7fef9120000 4549d33f Nov 02 11:15:11 2006 C:\Windows\System32\Wbem\wbemcore.dll
     7fef9350000 4549d2ea Nov 02 11:13:46 2006 C:\Windows\System32\Wbem\esscli.dll
     7fef9040000 4549d274 Nov 02 11:11:48 2006 C:\Windows\System32\Wbem\FastProx.dll
     7fef96d0000 4549d343 Nov 02 11:15:15 2006 C:\Windows\system32\wbem\wbemsvc.dll
     7fef96a0000 4549d3bd Nov 02 11:17:17 2006 C:\Windows\system32\wbem\wmiutils.dll
```

```
     7fef8f60000 4549d33a Nov 02 11:15:06 2006 C:\Windows\system32\wbem\repdrvfs.dll
     7fef8b90000 4549d3b9 Nov 02 11:17:13 2006 C:\Windows\system32\wbem\wmiprvsd.dll
     7fefcea0000 4549d2ef Nov 02 11:13:51 2006 C:\Windows\system32\NCObjAPI.DLL
     7fef8b00000 4549d341 Nov 02 11:15:13 2006 C:\Windows\system32\wbem\wbemess.dll
     7fefaab0000 4549d371 Nov 02 11:16:01 2006 C:\Windows\System32\winrnr.dll
     7fefaa70000 4549d2e4 Nov 02 11:13:40 2006 C:\Windows\system32\napinsp.dll
     7fefaa50000 4549d341 Nov 02 11:15:13 2006 C:\Windows\system32\pnrpnsp.dll
     7fefaac0000 4549d317 Nov 02 11:14:31 2006 C:\Windows\system32\rasadhlp.dll
     7fefc990000 4549d327 Nov 02 11:14:47 2006 C:\Windows\system32\kerberos.dll
     7fefce80000 4549d346 Nov 02 11:15:18 2006 C:\Windows\system32\cryptdll.dll
     7fef9750000 4549d35e Nov 02 11:15:42 2006 C:\Windows\system32\tschannel.dll
     7fefd1f0000 4549d32f Nov 02 11:14:55 2006 C:\Windows\system32\SXS.DLL
     7fef6ff0000 4549d321 Nov 02 11:14:41 2006 c:\windows\system32\rasmans.dll
     7fef6a80000 4549d32b Nov 02 11:14:51 2006 C:\Windows\system32\rastapi.dll
     7fef6ea0000 4549d32c Nov 02 11:14:52 2006 C:\Windows\system32\TAPI32.dll
     7fefb360000 4549d36f Nov 02 11:15:59 2006 C:\Windows\system32\WINMM.dll
     7fefb310000 4549d318 Nov 02 11:14:32 2006 C:\Windows\system32\OLEACC.dll
     7fef3e30000 4549d327 Nov 02 11:14:47 2006 C:\Windows\system32\rasppp.dll
     7fef6d00000 4549d2b3 Nov 02 11:12:51 2006 C:\Windows\system32\MPRAPI.dll
     7fef4410000 4549d318 Nov 02 11:14:32 2006 C:\Windows\system32\RASAPI32.dll
     7fef7150000 4549d320 Nov 02 11:14:40 2006 C:\Windows\system32\rasman.dll
     7fef4eb0000 4549d328 Nov 02 11:14:48 2006 C:\Windows\system32\RASQEC.DLL
     7fef79c0000 4549d31b Nov 02 11:14:35 2006 C:\Windows\system32\QUtil.dll
     7fef3d90000 4549d31b Nov 02 11:14:35 2006 C:\Windows\System32\raschap.dll
     7fef3d40000 4549d32c Nov 02 11:14:52 2006 C:\Windows\System32\rastls.dll
     7fef6d90000 4549d34a Nov 02 11:15:22 2006 C:\Windows\system32\CRYPTUI.dll
     7fefc570000 4549d324 Nov 02 11:14:44 2006 C:\Windows\system32\MSIMG32.dll
     7fefb2d0000 4549d376 Nov 02 11:16:06 2006 C:\Windows\system32\WinSCard.dll
     7fef3b40000 4549d2f1 Nov 02 11:13:53 2006 C:\Windows\system32\wbem\ncprov.dll
     7fef46f0000 46a6d0eb Jul 25 05:26:19 2007 c:\windows\system32\qmgr.dll
     7fef75f0000 4549d31b Nov 02 11:14:35 2006 c:\windows\system32\SHFOLDER.dll
     7fefae90000 4549d36a Nov 02 11:15:54 2006 c:\windows\system32\WINHTTP.dll
     7fefb900000 4549d25a Nov 02 11:11:22 2006 c:\windows\system32\bitsperf.dll
     7fef81d0000 4549d249 Nov 02 11:11:05 2006 c:\windows\system32\appinfo.dll
     7fef8190000 4549d258 Nov 02 11:11:20 2006 C:\Windows\system32\bitsigd.dll
     7fef3a20000 4549d32a Nov 02 11:14:50 2006 C:\Windows\system32\upnp.dll
     7fefa990000 4549d324 Nov 02 11:14:44 2006 C:\Windows\system32\SSDPAPI.dll
     7fef2bf0000 46ae9639 Jul 31 02:54:01 2007 c:\windows\system32\wuaueng.dll
     7fef8cf0000 4549d2e8 Nov 02 11:13:44 2006 c:\windows\system32\ESENT.dll
     7fef8520000 4549d37c Nov 02 11:16:12 2006 c:\windows\system32\WINSPOOL.DRV
     7fef70a0000 4549d2b9 Nov 02 11:12:57 2006 c:\windows\system32\mspatcha.dll
     7fefd290000 4549d366 Nov 02 11:15:50 2006 C:\Windows\system32\WMsgAPI.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       0000000000310000
    ProcessParameters: 0000000000311d20
    WindowTitle:  'C:\Windows\system32\svchost.exe'
    ImageFile:    'C:\Windows\system32\svchost.exe'
    CommandLine:  'C:\Windows\system32\svchost.exe -k netsvcs'
    DllPath:
'C:\Windows\system32;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Wind
ows;C:\Windows\System32\Wbem'
    Environment:  0000000000311310
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\system32\config\systemprofile\AppData\Roaming
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        LOCALAPPDATA=C:\Windows\system32\config\systemprofile\AppData\Local
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
```

```
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\TEMP
        TMP=C:\Windows\TEMP
        USERDOMAIN=DOMAIN
        USERNAME=COMPUTERNAME$
        USERPROFILE=C:\Windows\system32\config\systemprofile
        windir=C:\Windows


        THREAD fffffa80044df060  Cid 01a8.01b0  Teb: 000007fffffde000 Win32Thread: fffff900c07d0a60
WAIT: (Executive) UserMode Non-Alertable
            fffffa80045000e8  NotificationEvent
        IRP List:
            fffffa8003d7f780: (0006,0118) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      19121          Ticks: 27458 (0:00:07:08.347)
        Context Switch Count      258                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address svchost!wmainCRTStartup (0x00000000ff912550)
        Stack Init fffff9800d18ddb0 Current fffff9800d18d7f0
        Base fffff9800d18e000 Limit fffff9800d187000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0d18d830 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0d18d970 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0d18d9d0 fffff800`01ebdf16 nt!KeWaitForSingleObject+0x5f5
        fffff980`0d18da50 fffff800`01ea1a24 nt!IopSynchronousServiceTail+0x306
        fffff980`0d18dac0 fffff800`01c4d733 nt!NtReadFile+0x583
        fffff980`0d18dbb0 00000000`76e202da nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0d18dc20)
        00000000`0013f378 00000000`76bf26da ntdll!NtReadFile+0xa
        00000000`0013f380 000007fe`fea865aa kernel32!ReadFile+0x8a
        00000000`0013f410 000007fe`fea862e3 ADVAPI32!ScGetPipeInput+0x4a
        00000000`0013f4f0 000007fe`fea850f3 ADVAPI32!ScDispatcherLoop+0x9a
        00000000`0013f5f0 00000000`ff91283c ADVAPI32!StartServiceCtrlDispatcherW+0x176
        00000000`0013f890 00000000`ff912666 svchost!wmain+0xe5
        00000000`0013f8c0 00000000`76bfcdcd svchost!ScCreateWellKnownSids+0x301
        00000000`0013f900 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0013f930 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800450e060  Cid 01a8.000c  Teb: 000007fffffdc000 Win32Thread: 0000000000000000
WAIT: (DelayExecution) UserMode Alertable
            fffffa800450e118  NotificationTimer
        Impersonation token:  fffff88005a80660 (Level Delegation)
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      27827          Ticks: 18752 (0:00:04:52.533)
        Context Switch Count      5317
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address ADVAPI32!ScSvcctrlThreadW (0x000007fefea84bd0)
        Stack Init fffff9800cc0ddb0 Current fffff9800cc0d990
        Base fffff9800cc0e000 Limit fffff9800cc08000 Call 0
        Priority 27 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0cc0d9d0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0cc0db10 fffff800`01c5b5a9 nt!KiSwapThread+0x125
        fffff980`0cc0db70 fffff800`01e8ae9d nt!KeDelayExecutionThread+0x339
        fffff980`0cc0dbf0 fffff800`01c4d733 nt!NtDelayExecution+0x5c
        fffff980`0cc0dc20 00000000`76e205ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0cc0dc20)
        00000000`00c1f8b8 000007fe`fc2a3d20 ntdll!NtDelayExecution+0xa
        00000000`00c1f8c0 000007fe`fc2a2602 mmcss!CiSchedulerInitiailize+0x120
        00000000`00c1f930 00000000`ff911771 mmcss!CsServiceMain+0x17a
        00000000`00c1f9a0 000007fe`fea84bf5 svchost!ServiceStarter+0x1ea
        00000000`00c1fa30 00000000`76bfcdcd ADVAPI32!ScSvcctrlThreadW+0x25
        00000000`00c1fa60 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`00c1fa90 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80044fcbb0  Cid 01a8.01fc  Teb: 000007fffffda000 Win32Thread: 0000000000000000
WAIT: (WrLpcReceive) UserMode Non-Alertable
            fffffa80044fcf40  Semaphore Limit 0x1
            fffffa80044fcc68  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      46371          Ticks: 208 (0:00:00:03.244)
        Context Switch Count      355
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address mmcss!CsServerApiLoop (0x000007fefc2a5154)
        Stack Init fffff9800ccd1db0 Current fffff9800ccd17a0
        Base fffff9800ccd2000 Limit fffff9800cccc000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0ccd17e0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0ccd1920 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0ccd1980 fffff800`01eb3788 nt!KeWaitForSingleObject+0x5f5
        fffff980`0ccd1a00 fffff800`01eb3eda nt!AlpcpReceiveMessagePort+0x298
        fffff980`0ccd1a60 fffff800`01eb74ba nt!AlpcpReceiveMessage+0x246
        fffff980`0ccd1b00 fffff800`01c4d733 nt!NtAlpcSendWaitReceivePort+0x1da
        fffff980`0ccd1bb0 00000000`76e20aca nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0ccd1c20)
        00000000`00d1f968 000007fe`fc2a4f68 ntdll!NtAlpcSendWaitReceivePort+0xa
        00000000`00d1f970 000007fe`fc2a5161 mmcss!CiServerApiLoop+0xc4
        00000000`00d1fb80 00000000`76bfcdcd mmcss!CsServerApiLoop+0xd
        00000000`00d1fbd0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`00d1fc00 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004578bb0  Cid 01a8.03f8  Teb: 000007fffffd6000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800452b850  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      1589           Ticks: 44990 (0:00:11:41.848)
        Context Switch Count      267
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address ADVAPI32!ScSvcctrlThreadW (0x000007fefea84bd0)
        Stack Init fffff9800cc06db0 Current fffff9800cc06960
        Base fffff9800cc07000 Limit fffff9800cc01000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0cc069a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0cc06ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0cc06b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0cc06bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0cc06c20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0cc06c20)
        00000000`01a1f638 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`01a1f640 000007fe`fc1578fa kernel32!WaitForSingleObjectEx+0x9c
        00000000`01a1f700 00000000`ff911771 profsvc!UserProfileServiceMain+0xde
        00000000`01a1f740 000007fe`fea84bf5 svchost!ServiceStarter+0x1ea
        00000000`01a1f7d0 00000000`76bfcdcd ADVAPI32!ScSvcctrlThreadW+0x25
        00000000`01a1f800 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`01a1f830 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80045c2690  Cid 01a8.0420  Teb: 000007fffffd4000 Win32Thread: 0000000000000000
WAIT: (WrLpcReceive) UserMode Non-Alertable
            fffffa80045c2a20  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      45939          Ticks: 640 (0:00:00:09.984)
        Context Switch Count      299
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ADVAPI32!ScSvcctrlThreadW (0x000007fefea84bd0)
        Stack Init fffff9800d0c8db0 Current fffff9800d0c87f0
        Base fffff9800d0c9000 Limit fffff9800d0c3000 Call 0
        Priority 13 BasePriority 8 PriorityDecrement 4 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0d0c8830 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0d0c8970 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0d0c89d0 fffff800`01eb3788 nt!KeWaitForSingleObject+0x5f5
        fffff980`0d0c8a50 fffff800`01e7e523 nt!AlpcpReceiveMessagePort+0x298
        fffff980`0d0c8ab0 fffff800`01e740d2 nt!AlpcpReceiveLegacyMessage+0x122
        fffff980`0d0c8b50 fffff800`01e724bf nt!NtReplyWaitReceivePortEx+0xc1
        fffff980`0d0c8be0 fffff800`01c4d733 nt!NtReplyWaitReceivePort+0xf
        fffff980`0d0c8c20 00000000`76e2032a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0d0c8c20)
        00000000`01b8f548 000007fe`fb5cd944 ntdll!NtReplyWaitReceivePort+0xa
        00000000`01b8f550 000007fe`fb5ce140 shsvcs!CAPIConnection::Listen+0x7c
        00000000`01b8f7b0 000007fe`fb5c7aa1 shsvcs!CService::Start+0x140
        00000000`01b8f7e0 00000000`ff911771 shsvcs!ThemeServiceMain+0x285
        00000000`01b8f860 000007fe`fea84bf5 svchost!ServiceStarter+0x1ea
        00000000`01b8f8f0 00000000`76bfcdcd ADVAPI32!ScSvcctrlThreadW+0x25
        00000000`01b8f920 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`01b8f950 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004527bb0  Cid 01a8.0440  Teb: 000007fffffaa000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa800452b500  SynchronizationTimer
            fffffa80044ef410  SynchronizationEvent
            fffffa8004530550  SynchronizationTimer
            fffffa800452e410  SynchronizationEvent
            fffffa8004299660  ProcessObject
            fffffa8004628a70  SynchronizationEvent
            fffffa80045e8c20  SynchronizationEvent
            fffffa80045e2fe0  SynchronizationEvent
            fffffa80045e2a80  SynchronizationEvent
            fffffa800453dcb0  SynchronizationEvent
            fffffa8004614680  SynchronizationEvent
            fffffa800451cd80  SynchronizationEvent
            fffffa80045fa640  SynchronizationEvent
            fffffa8004547640  SynchronizationEvent
            fffffa80041b60b0  NotificationEvent
            fffffa8004781650  SynchronizationEvent
            fffffa8004804ab0  SynchronizationEvent
            fffffa8004804a50  SynchronizationEvent
            fffffa8002967790  SynchronizationEvent
            fffffa80046697b0  SynchronizationEvent
            fffffa8004801530  SynchronizationEvent
            fffffa80046b0ae0  SynchronizationEvent
            fffffa8004862d10  NotificationEvent
            fffffa800485f300  NotificationEvent
            fffffa8004897370  SynchronizationEvent
            fffffa8004728590  SynchronizationEvent
            fffffa8004888a30  SynchronizationEvent
            fffffa8004837660  SynchronizationEvent
            fffffa8004878750  SynchronizationEvent
            fffffa8004897940  SynchronizationEvent
            fffffa8004862600  SynchronizationEvent
            fffffa8004862800  SynchronizationEvent
            fffffa800489c7c0  SynchronizationTimer
            fffffa80048966d0  SynchronizationTimer
            fffffa8004864730  SynchronizationEvent
            fffffa800489a540  SynchronizationEvent
            fffffa8004295160  SynchronizationEvent
            fffffa80047f0530  SynchronizationEvent
            fffffa8004899fe0  SynchronizationEvent
            fffffa80048bd4e0  SynchronizationEvent
            fffffa80048e9ef0  SynchronizationTimer
            fffffa80048ed660  SynchronizationEvent
            fffffa800491cb30  SynchronizationEvent
            fffffa8004545a10  SynchronizationEvent
            fffffa800296cc40  SynchronizationEvent
            fffffa80047002a0  SynchronizationEvent
            fffffa8004899ae0  SynchronizationEvent
            fffffa80046a5d10  SynchronizationEvent
            fffffa800492d330  ProcessObject
            fffffa8004b32040  SynchronizationEvent
            fffffa8004b1d220  SynchronizationEvent
            fffffa8004b4a040  ProcessObject
            fffffa800209fe30  SynchronizationEvent
            fffffa80021979b0  NotificationEvent
            fffffa800237e610  SynchronizationEvent
            fffffa8004cd8040  SynchronizationEvent
            fffffa80025b7500  ProcessObject
            fffffa8004861490  SynchronizationEvent
            fffffa8004861510  SynchronizationEvent
            fffffa80048e9a40  SynchronizationTimer
            fffffa800452fb10  SynchronizationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      46184          Ticks: 395 (0:00:00:06.162)
        Context Switch Count      580
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
```

```
        Win32 Start Address ntdll!TppWaiterpThread (0x0000000076df6930)
        Stack Init fffff9800cc68db0 Current fffff9800cc68260
        Base fffff9800cc69000 Limit fffff9800cc63000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0cc682a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0cc683e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0cc68440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0cc684b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0cc68960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0cc68bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0cc68c20)
        00000000`01eef7f8 00000000`76df6b07 ntdll!NtWaitForMultipleObjects+0xa
        00000000`01eef800 00000000`76bfcdcd ntdll!TppWaiterpThread+0x14d
        00000000`01eefaa0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`01eefad0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80045a45b0  Cid 01a8.053c  Teb: 000007fffffa4000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80045e2d80  SynchronizationEvent
            fffffa80045f3930  SynchronizationEvent
        IRP List:
            fffffa8003fcec60: (0006,03a0) Flags: 00060970  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      1661           Ticks: 44918 (0:00:11:40.725)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x0000000076e17860)
        Stack Init fffff9800e35bdb0 Current fffff9800e35b260
        Base fffff9800e35c000 Limit fffff9800e356000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e35b2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e35b3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0e35b440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0e35b4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0e35b960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0e35bbb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e35bc20)
        00000000`0271f7b8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0271f7c0 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0271f8d0 000007fe`fb5e51d6 kernel32!WaitForMultipleObjects+0x11
        00000000`0271f910 000007fe`fb5cbf5c shsvcs!Wia::MailslotServer::_DoStuff+0x162
        00000000`0271f9c0 000007fe`fb5cbe56 shsvcs!CThreadTask::_CallDoStuff+0x78
        00000000`0271f9f0 00000000`76df6500 shsvcs!CThreadTask::_ThreadProc+0x12
        00000000`0271fa20 00000000`76e17b59 ntdll!RtlpTpWorkCallback+0xf0
        00000000`0271fad0 00000000`76bfcdcd ntdll!TppWorkerThread+0x3ad
        00000000`0271fd40 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0271fd70 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80045a8060  Cid 01a8.0564  Teb: 000007fffffa2000 Win32Thread: fffff900c07e2540
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80045a8bb0  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      19121          Ticks: 27458 (0:00:07:08.347)
        Context Switch Count      674                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.046
        Win32 Start Address ADVAPI32!ScSvcctrlThreadW (0x000007fefea84bd0)
        Stack Init fffff9800e541db0 Current fffff9800e541960
        Base fffff9800e542000 Limit fffff9800e53a000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e5419a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e541ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0e541b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0e541bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0e541c20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e541c20)
        00000000`0286f648 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`0286f650 000007fe`fb5cfb62 kernel32!WaitForSingleObjectEx+0x9c
        00000000`0286f710 000007fe`fb5cfe5d shsvcs!GSM::_RunService+0x4a
        00000000`0286f750 000007fe`fb5cfeed shsvcs!GSM::_ServiceMainHelper+0x225
        00000000`0286f7a0 000007fe`fb5cbf5c shsvcs!GSM::CServiceMainTask::_DoStuff+0xd
        00000000`0286f7d0 000007fe`fb5cff9e shsvcs!CThreadTask::_CallDoStuff+0x78
        00000000`0286f800 00000000`ff911771 shsvcs!GSM::ServiceMain+0xa2
        00000000`0286f8e0 000007fe`fea84bf5 svchost!ServiceStarter+0x1ea
        00000000`0286f970 00000000`76bfcdcd ADVAPI32!ScSvcctrlThreadW+0x25
        00000000`0286f9a0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0286f9d0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80045f2060  Cid 01a8.0578  Teb: 000007fffff9e000 Win32Thread: fffff900c07e0670
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80046084f0  SynchronizationEvent
            fffffa80046011e0  SynchronizationEvent
            fffffa800460a450  SynchronizationEvent
            fffffa80045f2118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      1680           Ticks: 44899 (0:00:11:40.428)
        Context Switch Count      369                 LargeStack
        UserTime                  00:00:00.015
        KernelTime                00:00:00.046
        Win32 Start Address ADVAPI32!ScSvcctrlThreadW (0x000007fefea84bd0)
        Stack Init fffff9800e567db0 Current fffff9800e567260
        Base fffff9800e568000 Limit fffff9800e55f000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e5672a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e5673e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0e567440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0e5674b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0e567960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0e567bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e567c20)
        00000000`0217f2c8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0217f2d0 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0217f3e0 000007fe`fc08c280 kernel32!WaitForMultipleObjects+0x11
        00000000`0217f420 000007fe`fc06ff0b schedsvc!Scheduler::TimerThreadFunction+0x2b8
        00000000`0217f660 000007fe`fc072a35 schedsvc!JobsService::WorkerThread+0x15f
        00000000`0217f700 000007fe`fc06fb1c schedsvc!CNtService::Run+0x16d
        00000000`0217f750 00000000`ff911771 schedsvc!ServiceMain+0x7c
        00000000`0217f870 000007fe`fea84bf5 svchost!ServiceStarter+0x1ea
        00000000`0217f900 00000000`76bfcdcd ADVAPI32!ScSvcctrlThreadW+0x25
        00000000`0217f930 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0217f960 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004608bb0  Cid 01a8.05a0  Teb: 000007fffff9c000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Alertable
            fffffa8004607d00  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      25260          Ticks: 21319 (0:00:05:32.578)
        Context Switch Count      22
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x0000000076e17860)
        Stack Init fffff9800e300db0 Current fffff9800e300860
        Base fffff9800e301000 Limit fffff9800e2fb000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e3008a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e3009e0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0e300a40 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0e300ad0 fffff800`01c8a722 nt!IoRemoveIoCompletion+0x47
        fffff980`0e300b50 fffff800`01c4d733 nt!NtWaitForWorkViaWorkerFactory+0x1f1
        fffff980`0e300c20 00000000`76e21b4a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e300c20)
        00000000`01fcf968 00000000`76e17a20 ntdll!NtWaitForWorkViaWorkerFactory+0xa
        00000000`01fcf970 00000000`76bfcdcd ntdll!TppWorkerThread+0x23e
        00000000`01fcfbe0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`01fcfc10 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80045e25f0  Cid 01a8.05b4  Teb: 000007fffff9a000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80045e5cc0  SynchronizationEvent
            fffffa800460a350  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      41241          Ticks: 5338 (0:00:01:23.273)
        Context Switch Count      350
        UserTime                  00:00:00.015
        KernelTime                00:00:00.031
        Win32 Start Address schedsvc!CSessionMgr::StartJobsCallback (0x000007fefc0a12b8)
        Stack Init fffff9800e2f2db0 Current fffff9800e2f2260
        Base fffff9800e2f3000 Limit fffff9800e2ed000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e2f22a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e2f23e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0e2f2440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0e2f24b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0e2f2960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0e2f2bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e2f2c20)
        00000000`02aefc38 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`02aefc40 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`02aefd50 000007fe`fc0a15a3 kernel32!WaitForMultipleObjects+0x11
        00000000`02aefd90 000007fe`fc0a134a schedsvc!CSessionMgr::LaunchLoop+0x6b
        00000000`02aefde0 00000000`76bfcdcd schedsvc!CSessionMgr::StartJobsCallback+0x92
        00000000`02aefe50 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02aefe80 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80045e7a10  Cid 01a8.05b8  Teb: 000007fffff98000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800460b600  SynchronizationEvent
            fffffa8004529160  SynchronizationEvent
            fffffa80044ef660  SynchronizationEvent
            fffffa80045e1250  SynchronizationTimer
            fffffa8004557b60  SynchronizationTimer
        IRP List:
            fffffa80045f7a00: (0006,0358) Flags: 00060000  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      1762           Ticks: 44817 (0:00:11:39.149)
        Context Switch Count      25
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address taskcomp!CompatibilityAdapter::MonitorThread (0x000007fefae38454)
        Stack Init fffff9800d074db0 Current fffff9800d074260
        Base fffff9800d075000 Limit fffff9800d06f000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0d0742a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0d0743e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0d074440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0d0744b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0d074960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0d074bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0d074c20)
        00000000`02fff858 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`02fff860 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`02fff970 000007fe`fae38541 kernel32!WaitForMultipleObjects+0x11
        00000000`02fff9b0 00000000`76bfcdcd taskcomp!CompatibilityAdapter::MonitorThread+0xed
        00000000`02fffa20 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02fffa50 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80045f4060  Cid 01a8.05bc  Teb: 000007fffff96000 Win32Thread: fffff900c07e2010
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800460a350  NotificationEvent
            fffffa80044f9390  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      2941           Ticks: 43638 (0:00:11:20.757)
        Context Switch Count      24                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address schedsvc!JobsService::MsgPumpThread (0x000007fefc0701d0)
        Stack Init fffff9800e5a0db0 Current fffff9800e5a0260
        Base fffff9800e5a1000 Limit fffff9800e599000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e5a02a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e5a03e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0e5a0440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0e5a04b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0e5a0960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0e5a0bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e5a0c20)
        00000000`02b7f818 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`02b7f820 00000000`76d1e96d kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`02b7f930 00000000`76d1e85e USER32!RealMsgWaitForMultipleObjectsEx+0x129
        00000000`02b7f9d0 00000000`76d13680 USER32!MsgWaitForMultipleObjectsEx+0x46
        00000000`02b7fa10 000007fe`fc07035c USER32!MsgWaitForMultipleObjects+0x20
        00000000`02b7fa50 00000000`76bfcdcd schedsvc!JobsService::MsgPumpThread+0x18c
        00000000`02b7fb40 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02b7fb70 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800468b960  Cid 01a8.0650  Teb: 000007fffff94000 Win32Thread: fffff900c07e6010
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800468aa40  SynchronizationEvent
            fffffa80046785b0  SynchronizationEvent
            fffffa80040976f0  SynchronizationEvent
            fffffa80046e1fe0  SynchronizationEvent
            fffffa80040989e0  SynchronizationEvent
            fffffa80043e09a0  SynchronizationEvent
            fffffa800408dbc0  SynchronizationEvent
            fffffa800468ba18  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      17293          Ticks: 29286 (0:00:07:36.864)
        Context Switch Count      1332                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.062
        Win32 Start Address ADVAPI32!ScSvcctrlThreadW (0x000007fefea84bd0)
        Stack Init fffff9800e5ffdb0 Current fffff9800e5ff260
        Base fffff9800e600000 Limit fffff9800e5f9000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e5ff2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e5ff3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0e5ff440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0e5ff4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0e5ff960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0e5ffbb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e5ffc20)
        00000000`027bf848 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`027bf850 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`027bf960 000007fe`fabf22dd kernel32!WaitForMultipleObjects+0x11
        00000000`027bf9a0 000007fe`fabf865d srvsvc!SsScavengerThread+0x48b
        00000000`027bfa90 00000000`ff911771 srvsvc!ServiceMain+0x241
        00000000`027bfae0 000007fe`fea84bf5 svchost!ServiceStarter+0x1ea
        00000000`027bfb70 00000000`76bfcdcd ADVAPI32!ScSvcctrlThreadW+0x25
        00000000`027bfba0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`027bfbd0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80046e4530  Cid 01a8.06a8  Teb: 000007fffff90000 Win32Thread: 0000000000000000
WAIT: (WrLpcReceive) UserMode Non-Alertable
            fffffa80046e48c0  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      3703           Ticks: 42876 (0:00:11:08.869)
        Context Switch Count      6
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address srvsvc!XsProcessApisWrapper (0x000007fefabf2aa0)
        Stack Init fffff9800ebdcdb0 Current fffff9800ebdc7c0
        Base fffff9800ebdd000 Limit fffff9800ebd7000 Call 0
        Priority 11 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0ebdc800 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0ebdc940 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0ebdc9a0 fffff800`01eb3788 nt!KeWaitForSingleObject+0x5f5
        fffff980`0ebdca20 fffff800`01e7e523 nt!AlpcpReceiveMessagePort+0x298
        fffff980`0ebdca80 fffff800`01e740d2 nt!AlpcpReceiveLegacyMessage+0x122
        fffff980`0ebdcb20 fffff800`01c4d733 nt!NtReplyWaitReceivePortEx+0xc1
        fffff980`0ebdcbb0 00000000`76e2052a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0ebdcc20)
        00000000`00c9f7d8 000007fe`fabf2ba9 ntdll!NtReplyWaitReceivePortEx+0xa
        00000000`00c9f7e0 000007fe`fabf2ad9 srvsvc!XsProcessApis+0x99
        00000000`00c9fa30 00000000`76bfcdcd srvsvc!XsProcessApisWrapper+0x39
        00000000`00c9fb00 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`00c9fb30 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80046f4060  Cid 01a8.06c0  Teb: 000007fffff88000 Win32Thread: 0000000000000000
WAIT: (WrLpcReceive) UserMode Non-Alertable
            fffffa80046f43f0  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      16115          Ticks: 30464 (0:00:07:55.241)
        Context Switch Count      27
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address aelupsvc!AelpProcessLPCCalls (0x000007fefaa94298)
        Stack Init fffff9800ebeadb0 Current fffff9800ebea7a0
        Base fffff9800ebeb000 Limit fffff9800ebe5000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0ebea7e0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0ebea920 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0ebea980 fffff800`01eb3788 nt!KeWaitForSingleObject+0x5f5
        fffff980`0ebeaa00 fffff800`01eb3eda nt!AlpcpReceiveMessagePort+0x298
        fffff980`0ebeaa60 fffff800`01eb74ba nt!AlpcpReceiveMessage+0x246
        fffff980`0ebeab00 fffff800`01c4d733 nt!NtAlpcSendWaitReceivePort+0x1da
        fffff980`0ebeabb0 00000000`76e20aca nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0ebeac20)
        00000000`033efa88 000007fe`faa9440e ntdll!NtAlpcSendWaitReceivePort+0xa
        00000000`033efa90 00000000`76bfcdcd aelupsvc!AelpProcessLPCCalls+0x176
        00000000`033efb40 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`033efb70 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80046f45a0  Cid 01a8.06c4  Teb: 000007fffff86000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80041b5ad0  SynchronizationEvent
            fffffa80046a6c60  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      16115          Ticks: 30464 (0:00:07:55.241)
        Context Switch Count      78
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address aelupsvc!AelTppDispatcherThreadRoutine (0x000007fefaa94f54)
        Stack Init fffff9800ebf8db0 Current fffff9800ebf8260
        Base fffff9800ebf9000 Limit fffff9800ebf3000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0ebf82a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0ebf83e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0ebf8440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0ebf84b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0ebf8960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0ebf8bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0ebf8c20)
        00000000`035bfe08 000007fe`faa94fa5 ntdll!NtWaitForMultipleObjects+0xa
        00000000`035bfe10 00000000`76bfcdcd aelupsvc!AelTppDispatcherThreadRoutine+0x51
        00000000`035bfe60 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`035bfe90 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80046f5060  Cid 01a8.06c8  Teb: 000007fffff84000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80046a6c00  NotificationEvent
            fffffa80041b5a70  NotificationEvent
            fffffa80046f5118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      39192          Ticks: 7387 (0:00:01:55.237)
        Context Switch Count      62
        UserTime                  00:00:00.031
        KernelTime                00:00:00.000
        Win32 Start Address aelupsvc!AelTppWorkerThreadRoutine (0x000007fefaa94c48)
        Stack Init fffff9800e70adb0 Current fffff9800e70a260
        Base fffff9800e70b000 Limit fffff9800e705000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e70a2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e70a3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0e70a440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0e70a4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0e70a960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0e70abb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e70ac20)
        00000000`0372f978 000007fe`faa94c9b ntdll!NtWaitForMultipleObjects+0xa
        00000000`0372f980 00000000`76bfcdcd aelupsvc!AelTppWorkerThreadRoutine+0x53
        00000000`0372f9d0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0372fa00 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004783bb0  Cid 01a8.0750  Teb: 000007fffff8a000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800476fc30  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      1856           Ticks: 44723 (0:00:11:37.683)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address AUTHZ!AuthzpDeQueueThreadWorker (0x000007fefd364660)
        Stack Init fffff9800eaa7db0 Current fffff9800eaa7960
        Base fffff9800eaa8000 Limit fffff9800eaa2000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0eaa79a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0eaa7ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0eaa7b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0eaa7bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0eaa7c20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0eaa7c20)
        00000000`0346fb18 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`0346fb20 000007fe`fd364689 kernel32!WaitForSingleObjectEx+0x9c
        00000000`0346fbe0 00000000`76bfcdcd AUTHZ!AuthzpDeQueueThreadWorker+0x29
        00000000`0346fc10 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0346fc40 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800477ebb0  Cid 01a8.076c  Teb: 000007fffff80000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa8004779b50  NotificationEvent
            fffffa80029664c0  SynchronizationEvent
            fffffa800296bc50  SynchronizationEvent
            fffffa8004778d80  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      1861           Ticks: 44718 (0:00:11:37.605)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ikeext!IkeReceiveThread (0x000007fefa4dc9b4)
        Stack Init fffff9800e6fcdb0 Current fffff9800e6fc260
        Base fffff9800e6fd000 Limit fffff9800e6f7000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e6fc2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e6fc3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0e6fc440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0e6fc4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0e6fc960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0e6fcbb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e6fcc20)
        00000000`0367f9c8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0367f9d0 000007fe`fa4dcba9 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0367fae0 00000000`76bfcdcd ikeext!IkeReceiveThread+0x1f5
        00000000`0367fc40 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0367fc70 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004813bb0  Cid 01a8.07c4  Teb: 000007fffff8c000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80046624f0  NotificationEvent
            fffffa8004860330  SynchronizationEvent
            fffffa8004860700  SynchronizationEvent
            fffffa80048617d8  NotificationEvent
            fffffa8004813c68  NotificationTimer
        IRP List:
            fffffa80046b0b90: (0006,0358) Flags: 00060000  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      45141          Ticks: 1438 (0:00:00:22.432)
        Context Switch Count      221
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address ADVAPI32!ScSvcctrlThreadW (0x000007fefea84bd0)
        Stack Init fffff9800f3abdb0 Current fffff9800f3ab260
        Base fffff9800f3ac000 Limit fffff9800f3a6000 Call 0
        Priority 11 BasePriority 10 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0f3ab2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0f3ab3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0f3ab440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0f3ab4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0f3ab960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0f3abbb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0f3abc20)
        00000000`03bff3c8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`03bff3d0 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`03bff4e0 000007fe`f9fea141 kernel32!WaitForMultipleObjects+0x11
        00000000`03bff520 000007fe`f9fea8c5 wmisvc!WaitingFunction+0x179
        00000000`03bff5d0 000007fe`f9feb520 wmisvc!MyService::WorkerThread+0x2e9
        00000000`03bff750 000007fe`f9feaf94 wmisvc!CNtService::Run+0x174
        00000000`03bff8d0 00000000`ff911771 wmisvc!ServiceMain+0x11c
        00000000`03bff970 000007fe`fea84bf5 svchost!ServiceStarter+0x1ea
        00000000`03bffa00 00000000`76bfcdcd ADVAPI32!ScSvcctrlThreadW+0x25
        00000000`03bffa30 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`03bffa60 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80048eb560  Cid 01a8.0854  Teb: 000007fffff74000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80048eabb0  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      1952           Ticks: 44627 (0:00:11:36.185)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address AUTHZ!AuthzpDeQueueThreadWorker (0x000007fefd364660)
        Stack Init fffff98010381db0 Current fffff98010381960
        Base fffff98010382000 Limit fffff9801037c000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`103819a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`10381ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`10381b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`10381bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`10381c20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`10381c20)
        00000000`03c9fcf8 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`03c9fd00 000007fe`fd364689 kernel32!WaitForSingleObjectEx+0x9c
        00000000`03c9fdc0 00000000`76bfcdcd AUTHZ!AuthzpDeQueueThreadWorker+0x29
        00000000`03c9fdf0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`03c9fe20 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004393440  Cid 01a8.0960  Teb: 000007fffff60000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004811240  NotificationEvent
            fffffa800483da40  SynchronizationEvent
            fffffa80048dc4c0  SynchronizationEvent
            fffffa80048dc460  SynchronizationEvent
            fffffa8004b2cd40  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      2501           Ticks: 44078 (0:00:11:27.621)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address gpsvc!GPOThread (0x000007fefb86b904)
        Stack Init fffff9800b6d3db0 Current fffff9800b6d3260
        Base fffff9800b6d4000 Limit fffff9800b6ce000 Call 0
        Priority 2 BasePriority 1 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0b6d32a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0b6d33e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0b6d3440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0b6d34b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0b6d3960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0b6d3bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0b6d3c20)
        00000000`0595faa8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0595fab0 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0595fbc0 000007fe`fb86bd3a kernel32!WaitForMultipleObjects+0x11
        00000000`0595fc00 00000000`76bfcdcd gpsvc!GPOThread+0x436
        00000000`0595fde0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0595fe10 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004b4cbb0  Cid 01a8.0a04  Teb: 000007fffff6c000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80044e50b0  NotificationEvent
            fffffa80046a6e10  SynchronizationEvent
            fffffa8004859530  SynchronizationEvent
            fffffa8004b50700  SynchronizationEvent
            fffffa8004b4c9c0  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      2770           Ticks: 43809 (0:00:11:23.424)
        Context Switch Count      16
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address gpsvc!GPOThread (0x000007fefb86b904)
        Stack Init fffff9800dac1db0 Current fffff9800dac1260
        Base fffff9800dac2000 Limit fffff9800dabc000 Call 0
        Priority 11 BasePriority 1 PriorityDecrement 10 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0dac12a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0dac13e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0dac1440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0dac14b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0dac1960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0dac1bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0dac1c20)
        00000000`0548fa08 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0548fa10 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0548fb20 000007fe`fb86bd3a kernel32!WaitForMultipleObjects+0x11
        00000000`0548fb60 00000000`76bfcdcd gpsvc!GPOThread+0x436
        00000000`0548fd40 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0548fd70 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004b997c0  Cid 01a8.0bc8  Teb: 000007fffff7a000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80046a6c00  NotificationEvent
            fffffa80041b5a70  NotificationEvent
            fffffa8004b99878  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      39192          Ticks: 7387 (0:00:01:55.237)
        Context Switch Count      26
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address aelupsvc!AelTppWorkerThreadRoutine (0x000007fefaa94c48)
        Stack Init fffff98010765db0 Current fffff98010765260
        Base fffff98010766000 Limit fffff98010760000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`107652a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`107653e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`10765440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`107654b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`10765960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`10765bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`10765c20)
        00000000`04f3fc88 000007fe`faa94c9b ntdll!NtWaitForMultipleObjects+0xa
        00000000`04f3fc90 00000000`76bfcdcd aelupsvc!AelTppWorkerThreadRoutine+0x53
        00000000`04f3fce0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`04f3fd10 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa800200e840  Cid 01a8.06d0  Teb: 000007fffffd8000 Win32Thread: fffff900c200a320
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8001ec2450  QueueObject
            fffffa800200e8f8  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      46535          Ticks: 44 (0:00:00:00.686)
        Context Switch Count      940                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.062
        Win32 Start Address ADVAPI32!ScSvcctrlThreadW (0x000007fefea84bd0)
        Stack Init fffff98012e98db0 Current fffff98012e98810
        Base fffff98012e99000 Limit fffff98012e91000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`12e98850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12e98990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`12e989f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`12e98a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`12e98b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`12e98bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12e98c20)
        00000000`020bf658 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`020bf660 000007fe`f700dfa8 kernel32!GetQueuedCompletionStatus+0x48
        00000000`020bf6c0 000007fe`f701a6ad rasmans!RequestThread+0x88
        00000000`020bf760 00000000`ff911771 rasmans!ServiceMain+0xf1
        00000000`020bf7d0 000007fe`fea84bf5 svchost!ServiceStarter+0x1ea
        00000000`020bf860 00000000`76bfcdcd ADVAPI32!ScSvcctrlThreadW+0x25
        00000000`020bf890 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`020bf8c0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8001f7f550  Cid 01a8.0cd8  Teb: 000007fffffa8000 Win32Thread: fffff900c2009010
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa8004837580  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      7648           Ticks: 38931 (0:00:10:07.327)
        Context Switch Count      41                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address rastapi!EnumerateTapiPorts (0x000007fef6a8802c)
        Stack Init fffff9800db67db0 Current fffff9800db67740
        Base fffff9800db68000 Limit fffff9800db60000 Call 0
        Priority 13 BasePriority 8 PriorityDecrement 5 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0db67780 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0db678c0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0db67920 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`0db679a0 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`0db67a40 fffff960`000c7e1e win32k!xxxSleepThread+0x56
        fffff980`0db67a70 fffff960`000c7f25 win32k!xxxRealInternalGetMessage+0x72e
        fffff980`0db67b50 fffff960`000c97e4 win32k!xxxInternalGetMessage+0x35
        fffff980`0db67b90 fffff800`01c4d733 win32k!NtUserGetMessage+0x64
        fffff980`0db67c20 00000000`76d1e6aa nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0db67c20)
        00000000`0523fdc8 00000000`76d1bf4e USER32!ZwUserGetMessage+0xa
        00000000`0523fdd0 000007fe`f6a88346 USER32!GetMessageA+0xc3
        00000000`0523fe00 00000000`76bfcdcd rastapi!EnumerateTapiPorts+0x31a
        00000000`0523ff40 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0523ff70 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8001ffdbb0  Cid 01a8.0d00  Teb: 000007fffffa6000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800206fe90  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      7651           Ticks: 38928 (0:00:10:07.280)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address TAPI32!AsyncEventsThread (0x000007fef6ea7ec0)
        Stack Init fffff9801dbffdb0 Current fffff9801dbff960
        Base fffff9801dc00000 Limit fffff9801dbfa000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1dbff9a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1dbffae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`1dbffb40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`1dbffbc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`1dbffc20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1dbffc20)
        00000000`04ebf768 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`04ebf770 000007fe`f6ea8048 kernel32!WaitForSingleObjectEx+0x9c
        00000000`04ebf830 00000000`76bfcdcd TAPI32!AsyncEventsThread+0x188
        00000000`04ebf9c0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`04ebf9f0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800207bbb0  Cid 01a8.0d1c  Teb: 000007fffff8e000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa8002053d00  SynchronizationEvent
            fffffa80020a1af0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      7656           Ticks: 38923 (0:00:10:07.202)
        Context Switch Count      10
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RASQEC!RasQecHelper::WorkerThread (0x000007fef4ebdb3c)
        Stack Init fffff9801db49db0 Current fffff9801db49260
        Base fffff9801db4a000 Limit fffff9801db44000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1db492a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1db493e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`1db49440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`1db494b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`1db49960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`1db49bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1db49c20)
        00000000`0577fd18 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0577fd20 000007fe`f4ebdd72 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0577fe30 00000000`76bfcdcd RASQEC!RasQecHelper::WorkerThread+0x236
        00000000`0577ff00 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0577ff30 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80021f6bb0  Cid 01a8.0d24  Teb: 000007fffff6a000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa800207b850  NotificationEvent
            fffffa800209ca80  SynchronizationEvent
            fffffa80020a2ca0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      7654           Ticks: 38925 (0:00:10:07.233)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address rasppp!WorkerThread (0x000007fef3e52fdc)
        Stack Init fffff9801db50db0 Current fffff9801db50260
        Base fffff9801db51000 Limit fffff9801db4b000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1db502a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1db503e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`1db50440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`1db504b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`1db50960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`1db50bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1db50c20)
        00000000`052df678 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`052df680 000007fe`f3e5305b kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`052df790 00000000`76bfcdcd rasppp!WorkerThread+0x7f
        00000000`052df800 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`052df830 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80020a3400  Cid 01a8.0d80  Teb: 000007fffff68000 Win32Thread: fffff900c200c370
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa8003d8fb60  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      46149          Ticks: 430 (0:00:00:06.708)
        Context Switch Count      57                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ole32!CRpcThreadCache::RpcWorkerThreadEntry (0x000007fefd7a3be0)
        Stack Init fffff98015770db0 Current fffff98015770740
        Base fffff98015771000 Limit fffff98015769000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`15770780 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`157708c0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`15770920 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`157709a0 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`15770a40 fffff960`000c7e1e win32k!xxxSleepThread+0x56
        fffff980`15770a70 fffff960`000c7f25 win32k!xxxRealInternalGetMessage+0x72e
        fffff980`15770b50 fffff960`000c97e4 win32k!xxxInternalGetMessage+0x35
        fffff980`15770b90 fffff800`01c4d733 win32k!NtUserGetMessage+0x64
        fffff980`15770c20 00000000`76d1e6aa nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`15770c20)
        00000000`02e0f978 00000000`76d1e6ea USER32!ZwUserGetMessage+0xa
        00000000`02e0f980 000007fe`fd779d72 USER32!GetMessageW+0x34
        00000000`02e0f9b0 000007fe`fd77a0dd ole32!CDllHost::STAWorkerLoop+0x8a
        00000000`02e0fa10 000007fe`fd7a3b7e ole32!CDllHost::WorkerThread+0xd7
        00000000`02e0fa50 000007fe`fd7a3c0a ole32!CRpcThread::WorkerLoop+0x1e
        00000000`02e0fa90 00000000`76bfcdcd ole32!CRpcThreadCache::RpcWorkerThreadEntry+0x2a
        00000000`02e0fac0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02e0faf0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8001f4b060  Cid 01a8.0ddc  Teb: 000007fffff54000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa80018a2570  NotificationEvent
            fffffa80020c3aa0  NotificationEvent
        IRP List:
            fffffa8004ab8db0: (0006,0118) Flags: 00060900  Mdl: 00000000
            fffffa8001f4b580: (0006,0118) Flags: 00060800  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      16242          Ticks: 30337 (0:00:07:53.260)
        Context Switch Count      28
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ncprov!CNCProvider::ConnectThreadProc (0x000007fef3b4552c)
        Stack Init fffff9801dafcdb0 Current fffff9801dafc260
        Base fffff9801dafd000 Limit fffff9801daf7000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1dafc2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1dafc3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`1dafc440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`1dafc4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`1dafc960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`1dafcbb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1dafcc20)
        00000000`0626fad8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0626fae0 000007fe`f3b45893 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0626fbf0 000007fe`f3b4555b ncprov!CNCProvider::ConnectLoop+0x237
        00000000`0626fc80 00000000`76bfcdcd ncprov!CNCProvider::ConnectThreadProc+0x2f
        00000000`0626fcc0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0626fcf0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8001f4b700  Cid 01a8.0de4  Teb: 000007fffff52000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80020b7d60  NotificationEvent
            fffffa80020c09e0  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      7765           Ticks: 38814 (0:00:10:05.502)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address NCObjAPI!CNamedPipeClient::ProviderReadyThreadProc (0x000007fefcea2010)
        Stack Init fffff9801db03db0 Current fffff9801db03260
        Base fffff9801db04000 Limit fffff9801dafe000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1db032a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1db033e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`1db03440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`1db034b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`1db03960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`1db03bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1db03c20)
        00000000`0269fb18 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0269fb20 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0269fc30 000007fe`fcea208b kernel32!WaitForMultipleObjects+0x11
        00000000`0269fc70 00000000`76bfcdcd
NCObjAPI!CNamedPipeClient::ProviderReadyThreadProc+0x147
        00000000`0269fcd0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0269fd00 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8001f93bb0  Cid 01a8.0dec  Teb: 000007fffff72000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80020d80b0  NotificationEvent
            fffffa80020e0350  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      7765           Ticks: 38814 (0:00:10:05.502)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address NCObjAPI!CNamedPipeClient::ProviderReadyThreadProc (0x000007fefcea2010)
        Stack Init fffff9800ead1db0 Current fffff9800ead1260
        Base fffff9800ead2000 Limit fffff9800eacc000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0ead12a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0ead13e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0ead1440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0ead14b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0ead1960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0ead1bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0ead1c20)
        00000000`05c5f6f8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`05c5f700 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`05c5f810 000007fe`fcea208b kernel32!WaitForMultipleObjects+0x11
        00000000`05c5f850 00000000`76bfcdcd
NCObjAPI!CNamedPipeClient::ProviderReadyThreadProc+0x147
        00000000`05c5f8b0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`05c5f8e0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8002424bb0  Cid 01a8.0e54  Teb: 000007fffff92000 Win32Thread: fffff900c07e0920
WAIT: (UserRequest) UserMode Alertable
            fffffa80022255f0  SynchronizationTimer
            fffffa80025c2f80  NotificationEvent
            fffffa8001fd1c40  SynchronizationEvent
        IRP List:
            fffffa80025fd010: (0006,01f0) Flags: 00060030  Mdl: 00000000
            fffffa8002186710: (0006,03a0) Flags: 00060030  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      16322          Ticks: 30257 (0:00:07:52.012)
        Context Switch Count      838                 LargeStack
        UserTime                  00:00:00.015
        KernelTime                00:00:00.062
        Win32 Start Address ADVAPI32!ScSvcctrlThreadW (0x000007fefea84bd0)
        Stack Init fffff98012f30db0 Current fffff98012f30260
        Base fffff98012f31000 Limit fffff98012f29000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`12f302a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12f303e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`12f30440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`12f304b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`12f30960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`12f30bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12f30c20)
        00000000`0326f888 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0326f890 00000000`76d1e96d kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0326f9a0 00000000`76d1e85e USER32!RealMsgWaitForMultipleObjectsEx+0x129
        00000000`0326fa40 000007fe`f471960f USER32!MsgWaitForMultipleObjectsEx+0x46
        00000000`0326fa80 000007fe`f4715c92 qmgr!CJobManager::TaskThread+0x4b
        00000000`0326fb00 000007fe`f470429a qmgr!InitQmgr+0x202
        00000000`0326fbc0 000007fe`f4703ba5 qmgr!BITSServiceMainProc+0x6b2
        00000000`0326fd00 000007fe`f4703558 qmgr!BITSServiceMain+0x9
        00000000`0326fd40 00000000`ff911771 qmgr!ServiceMain+0x64
        00000000`0326fd70 000007fe`fea84bf5 svchost!ServiceStarter+0x1ea
        00000000`0326fe00 00000000`76bfcdcd ADVAPI32!ScSvcctrlThreadW+0x25
        00000000`0326fe30 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0326fe60 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8002af7bb0  Cid 01a8.0b4c  Teb: 000007fffff4e000 Win32Thread: fffff900c2009ab0
WAIT: (UserRequest) UserMode Alertable
            fffffa8004cd8110  SynchronizationEvent
            fffffa8004cd80b0  NotificationEvent
            fffffa80025a7580  SynchronizationEvent
            fffffa8002af7c68  NotificationTimer
        IRP List:
            fffffa8002b47cc0: (0006,01f0) Flags: 00060030  Mdl: 00000000
            fffffa80028492c0: (0006,01f0) Flags: 00060030  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      19445          Ticks: 27134 (0:00:07:03.293)
        Context Switch Count      397                 LargeStack
        UserTime                  00:00:00.015
        KernelTime                00:00:00.078
        Win32 Start Address ADVAPI32!ScSvcctrlThreadW (0x000007fefea84bd0)
        Stack Init fffff9801e54fdb0 Current fffff9801e54f260
        Base fffff9801e550000 Limit fffff9801e548000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1e54f2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1e54f3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`1e54f440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`1e54f4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`1e54f960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`1e54fbb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1e54fc20)
        00000000`05d5f4b8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`05d5f4c0 000007fe`f2d94c64 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`05d5f5d0 01c862bc`bb8cce00 wuaueng!WUAutoUpdateAtShutdown+0x24e88
        00000000`05d5f5d8 00000000`00260078 0x1c862bc`bb8cce00
        00000000`05d5f5e0 00000000`00000000 0x260078
        00000000`05d5f5e8 000007fe`f2c1e0f0 0x0
        00000000`05d5f5f0 00000000`00000001 wuaueng+0x2e0f0
        00000000`05d5f5f8 000007fe`f2bfd3d0 0x1
        00000000`05d5f600 00000000`002603c8 wuaueng+0xd3d0
        00000000`05d5f608 00000000`00000000 0x2603c8
        00000000`05d5f610 00000000`00000000 0x0
        00000000`05d5f618 ffffffff`80000002 0x0
        00000000`05d5f620 00000000`00000003 0xffffffff`80000002
        00000000`05d5f628 00000000`00000000 0x3
        00000000`05d5f630 00000000`00000001 0x0
        00000000`05d5f638 00000000`00000002 0x1
        00000000`05d5f640 00000000`00000001 0x2
        00000000`05d5f648 00000000`00000000 0x1
        00000000`05d5f650 00000000`00000000 0x0
        00000000`05d5f658 000007fe`f2c7761d 0x0
        00000000`05d5f660 00000001`00000000 wuaueng!ServiceMain+0x39d
        00000000`05d5f668 00000000`00000001 0x1`00000000
        00000000`05d5f670 01c86265`a5a0d6e8 0x1
        00000000`05d5f678 01c862bc`bb8cce00 0x1c86265`a5a0d6e8
        00000000`05d5f680 00000000`00000000 0x1c862bc`bb8cce00
        00000000`05d5f688 00000000`00000000 0x0
        00000000`05d5f690 00000002`00000000 0x0
        00000000`05d5f698 00000000`0002020e 0x2`00000000
        00000000`05d5f6a0 00000000`00000000 0x2020e
        00000000`05d5f6a8 00000000`00000000 0x0
        00000000`05d5f6b0 00000000`00000000 0x0
        00000000`05d5f6b8 00000000`00000000 0x0
        00000000`05d5f6c0 00000000`02caf168 0x0
        00000000`05d5f6c8 00000000`00000000 0x2caf168
```

```
        THREAD fffffa800254ebb0  Cid 01a8.0d88  Teb: 000007fffff6e000 Win32Thread: 0000000000000000
WAIT: (WrLpcReply) UserMode Non-Alertable
            fffffa800254ef40  Semaphore Limit 0x1
        Waiting for reply to ALPC Message fffff880020f32f0
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      16235          Ticks: 30344 (0:00:07:53.369)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address SSDPAPI!GetNotificationLoop (0x000007fefa995000)
        Stack Init fffff9800e2d6db0 Current fffff9800e2d66e0
        Base fffff9800e2d7000 Limit fffff9800e2d1000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e2d6720 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e2d6860 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0e2d68c0 fffff800`01c8f857 nt!KeWaitForSingleObject+0x5f5
        fffff980`0e2d6940 fffff800`01ebed64 nt!AlpcpSignalAndWait+0x97
        fffff980`0e2d6980 fffff800`01e9a80a nt!AlpcpReceiveSynchronousReply+0x44
        fffff980`0e2d69e0 fffff800`01eb747f nt!AlpcpProcessSynchronousRequest+0x257
        fffff980`0e2d6b00 fffff800`01c4d733 nt!NtAlpcSendWaitReceivePort+0x19f
        fffff980`0e2d6bb0 00000000`76e20aca nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e2d6c20)
        00000000`03eef278 000007fe`fedba66b ntdll!NtAlpcSendWaitReceivePort+0xa
        00000000`03eef280 000007fe`fedbd422 RPCRT4!LRPC_CCALL::SendReceive+0xbb
        00000000`03eef300 000007fe`fedbd472 RPCRT4!I_RpcSendReceive+0x42
        00000000`03eef330 000007fe`fee9a2bc RPCRT4!NdrSendReceive+0x32
        00000000`03eef360 000007fe`fee9a3d0 RPCRT4!NdrpClientCall3+0x11c
        00000000`03eef5b0 000007fe`fa995086 RPCRT4!NdrClientCall3+0x7c
        00000000`03eef920 00000000`76bfcdcd SSDPAPI!GetNotificationLoop+0x86
        00000000`03eef9a0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`03eef9d0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800202a060  Cid 01a8.0ea4  Teb: 000007fffff56000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8002aed970  NotificationEvent
            fffffa8002b49b30  NotificationEvent
            fffffa800202a118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      19445          Ticks: 27134 (0:00:07:03.293)
        Context Switch Count      105
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wuaueng!DllInstall (0x000007fef2c9c5b8)
        Stack Init fffff98020cbadb0 Current fffff98020cba260
        Base fffff98020cbb000 Limit fffff98020cb5000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`20cba2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`20cba3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`20cba440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`20cba4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`20cba960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`20cbabb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`20cbac20)
        00000000`03a8f968 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`03a8f970 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`03a8fa80 000007fe`f2c9c631 kernel32!WaitForMultipleObjects+0x11
        00000000`03a8fac0 00000000`00261860 wuaueng!DllInstall+0x23efd
        00000000`03a8fac8 00000000`00000000 0x261860
        00000000`03a8fad0 00000000`00000001 0x0
        00000000`03a8fad8 00000000`00000001 0x1
        00000000`03a8fae0 00000000`00000000 0x1
        00000000`03a8fae8 00000000`00000000 0x0
        00000000`03a8faf0 00000000`00001134 0x0
        00000000`03a8faf8 00000000`00001138 0x1134
        00000000`03a8fb00 00000000`00000000 0x1138
        00000000`03a8fb08 00000000`00000000 0x0
        00000000`03a8fb10 00000000`00000000 0x0
        00000000`03a8fb18 00000000`00000000 0x0
        00000000`03a8fb20 00000000`00000000 0x0
        00000000`03a8fb28 00000000`76bfcdcd 0x0
        00000000`03a8fb30 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`03a8fb60 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004b3a060  Cid 01a8.09bc  Teb: 000007fffffae000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa80044e2750  QueueObject
            fffffa8004b3a118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      46527          Ticks: 52 (0:00:00:00.811)
        Context Switch Count      115
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff9800ba7bdb0 Current fffff9800ba7b810
        Base fffff9800ba7c000 Limit fffff9800ba76000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0ba7b850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0ba7b990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0ba7b9f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0ba7ba80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`0ba7bb00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`0ba7bbb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0ba7bc20)
        00000000`0351f9f8 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`0351fa00 000007fe`fedce7a3 kernel32!GetQueuedCompletionStatus+0x48
        00000000`0351fa60 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`0351faf0 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`0351fba0 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`0351fbd0 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`0351fc10 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`0351fc40 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0351fc70 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa800437abb0  Cid 01a8.0318  Teb: 000007fffff7e000 Win32Thread: 0000000000000000
WAIT: (DelayExecution) UserMode Non-Alertable
            fffffa800437ac68  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      45141          Ticks: 1438 (0:00:00:22.432)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ole32!CRpcThreadCache::RpcWorkerThreadEntry (0x000007fefd7a3be0)
        Stack Init fffff98010858db0 Current fffff98010858990
        Base fffff98010859000 Limit fffff98010853000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`108589d0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`10858b10 fffff800`01c5b5a9 nt!KiSwapThread+0x125
        fffff980`10858b70 fffff800`01e8ae9d nt!KeDelayExecutionThread+0x339
        fffff980`10858bf0 fffff800`01c4d733 nt!NtDelayExecution+0x5c
        fffff980`10858c20 00000000`76e205ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`10858c20)
        00000000`0446f968 00000000`76bfd908 ntdll!NtDelayExecution+0xa
        00000000`0446f970 000007fe`fd7acdc0 kernel32!SleepEx+0x84
        00000000`0446f9f0 000007fe`fd7a3b7e ole32!CROIDTable::WorkerThreadLoop+0x10
        00000000`0446fa20 000007fe`fd7a3c0a ole32!CRpcThread::WorkerLoop+0x1e
        00000000`0446fa60 00000000`76bfcdcd ole32!CRpcThreadCache::RpcWorkerThreadEntry+0x2a
        00000000`0446fa90 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0446fac0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80020ab060  Cid 01a8.00b0  Teb: 000007fffffa0000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Alertable
            fffffa80044c24d0  QueueObject
            fffffa80020ab118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      46184          Ticks: 395 (0:00:00:06.162)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x0000000076e17860)
        Stack Init fffff9800e369db0 Current fffff9800e369860
        Base fffff9800e36a000 Limit fffff9800e364000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0e3698a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e3699e0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0e369a40 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0e369ad0 fffff800`01c8a722 nt!IoRemoveIoCompletion+0x47
        fffff980`0e369b50 fffff800`01c4d733 nt!NtWaitForWorkViaWorkerFactory+0x1f1
        fffff980`0e369c20 00000000`76e21b4a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e369c20)
        00000000`0400fb08 00000000`76e17a20 ntdll!NtWaitForWorkViaWorkerFactory+0xa
        00000000`0400fb10 00000000`76bfcdcd ntdll!TppWorkerThread+0x23e
        00000000`0400fd80 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0400fdb0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8002847060  Cid 01a8.0620  Teb: 000007fffff82000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Alertable
            fffffa80044c24d0  QueueObject
            fffffa8002847118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      46184          Ticks: 395 (0:00:00:06.162)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x0000000076e17860)
        Stack Init fffff9800f293db0 Current fffff9800f293860
        Base fffff9800f294000 Limit fffff9800f28e000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0f2938a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0f2939e0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0f293a40 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0f293ad0 fffff800`01c8a722 nt!IoRemoveIoCompletion+0x47
        fffff980`0f293b50 fffff800`01c4d733 nt!NtWaitForWorkViaWorkerFactory+0x1f1
        fffff980`0f293c20 00000000`76e21b4a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0f293c20)
        00000000`02f6fb38 00000000`76e17a20 ntdll!NtWaitForWorkViaWorkerFactory+0xa
        00000000`02f6fb40 00000000`76bfcdcd ntdll!TppWorkerThread+0x23e
        00000000`02f6fdb0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02f6fde0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80048fb060  Cid 01a8.0d34  Teb: 000007fffffac000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa80044e2750  QueueObject
            fffffa80048fb118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80044d9c10       Image:         svchost.exe
        Wait Start TickCount      46397          Ticks: 182 (0:00:00:02.839)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff9800ba66db0 Current fffff9800ba66810
        Base fffff9800ba67000 Limit fffff9800ba61000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0ba66850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0ba66990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0ba669f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0ba66a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`0ba66b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`0ba66bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0ba66c20)
        00000000`045df888 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`045df890 000007fe`fedce7a3 kernel32!GetQueuedCompletionStatus+0x48
        00000000`045df8f0 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`045df980 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`045dfa30 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`045dfa60 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`045dfaa0 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`045dfad0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`045dfb00 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

Audiodg process

```
PROCESS fffffa800451dc10
    SessionId: 0  Cid: 032c    Peb: 7fffffd6000  ParentCid: 0114
    DirBase: 4d37c000  ObjectTable: fffff88005c1ec40  HandleCount: 100.
    Image: audiodg.exe
    VadRoot fffffa80045197b0 Vads 73 Clone 0 Private 2534. Modified 1393. Locked 0.
    DeviceMap fffff88005a30830
    Token                             fffff88005ace060
    ElapsedTime                       00:11:42.720
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.062
    QuotaPoolUsage[PagedPool]         80896
    QuotaPoolUsage[NonPagedPool]      6912
    Working Set Sizes (now,min,max)  (3586, 2863, 3379) (14344KB, 11452KB, 13516KB)
    PeakWorkingSetSize                4031
    VirtualSize                       48 Mb
    PeakVirtualSize                   51 Mb
    PageFaultCount                    8876
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      2933

    Setting context for this process...
.process /p /r fffffa800451dc10

    !peb
PEB at 000007fffffd6000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00000000ff8a0000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00000000001f1b90 . 000000000021c150
    Ldr.InLoadOrderModuleList:           00000000001f1aa0 . 000000000021c7b0
    Ldr.InMemoryOrderModuleList:         00000000001f1ab0 . 000000000021c7c0
            Base TimeStamp                     Module
        ff8a0000 4549c02f Nov 02 09:53:51 2006 C:\Windows\system32\AUDIODG.EXE
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        76bc0000 4549d328 Nov 02 11:14:48 2006 C:\Windows\System32\kernel32.dll
     7fefea30000 4549d267 Nov 02 11:11:35 2006 C:\Windows\System32\ADVAPI32.dll
     7fefed90000 469c43bb Jul 17 05:21:15 2007 C:\Windows\System32\RPCRT4.dll
     7fefdd40000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\System32\msvcrt.dll
     7fefd760000 4549d317 Nov 02 11:14:31 2006 C:\Windows\System32\ole32.dll
     7fefec20000 4549d273 Nov 02 11:11:47 2006 C:\Windows\System32\GDI32.dll
        76d00000 45d3ee19 Feb 15 05:22:33 2007 C:\Windows\System32\USER32.dll
     7fefc2e0000 4549d2a1 Nov 02 11:12:33 2006 C:\Windows\System32\MMDevAPI.DLL
     7fefdab0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\System32\OLEAUT32.dll
     7fefda10000 4549d31f Nov 02 11:14:39 2006 C:\Windows\System32\SHLWAPI.dll
     7fefd9e0000 4549d2cb Nov 02 11:13:15 2006 C:\Windows\system32\IMM32.DLL
     7fefdc30000 4549d2e6 Nov 02 11:13:42 2006 C:\Windows\system32\MSCTF.dll
     7feff0c0000 4549d2a1 Nov 02 11:12:33 2006 C:\Windows\system32\LPK.DLL
     7fefd940000 4549d337 Nov 02 11:15:03 2006 C:\Windows\system32\USP10.dll
     7fefc5b0000 4549d384 Nov 02 11:16:20 2006 C:\Windows\system32\NTMARTA.DLL
     7fefd590000 4549d396 Nov 02 11:16:38 2006 C:\Windows\system32\WLDAP32.dll
     7fefd540000 4549d38a Nov 02 11:16:26 2006 C:\Windows\system32\WS2_32.dll
     7feff0b0000 4549d370 Nov 02 11:16:00 2006 C:\Windows\system32\NSI.dll
     7fefd530000 4549d310 Nov 02 11:14:24 2006 C:\Windows\system32\PSAPI.DLL
     7fefce20000 4549d315 Nov 02 11:14:29 2006 C:\Windows\system32\SAMLIB.dll
     7fefdb90000 4549d282 Nov 02 11:12:02 2006 C:\Windows\system32\CLBCatQ.DLL
     7fefc620000 4549d31d Nov 02 11:14:37 2006 C:\Windows\system32\rsaenh.dll
     7fefb0c0000 4549d258 Nov 02 11:11:20 2006 C:\Windows\System32\audioses.dll
     7fefb040000 4549d256 Nov 02 11:11:18 2006 C:\Windows\System32\audioeng.dll
     7fefc2d0000 4549d273 Nov 02 11:11:47 2006 C:\Windows\System32\AVRT.dll
     7fefafe0000 4549d257 Nov 02 11:11:19 2006 C:\Windows\System32\audiokse.dll
     7fefeed0000 4549d318 Nov 02 11:14:32 2006 C:\Windows\System32\SETUPAPI.dll
```

```
     7fefcc50000 4549d344 Nov 02 11:15:16 2006 C:\Windows\System32\CRYPT32.dll
     7fefce00000 4549d2df Nov 02 11:13:35 2006 C:\Windows\System32\MSASN1.dll
     7fefd3b0000 4549d336 Nov 02 11:15:02 2006 C:\Windows\System32\USERENV.dll
     7fefd390000 4549d33f Nov 02 11:15:11 2006 C:\Windows\System32\Secur32.dll
     7fefc1e0000 4549d381 Nov 02 11:16:17 2006 C:\Windows\System32\WINTRUST.dll
     7fefda90000 462443ee Apr 17 04:50:06 2007 C:\Windows\System32\imagehlp.dll
        75160000 4549d331 Nov 02 11:14:57 2006 C:\Windows\System32\ksuser.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       00000000001f0000
    ProcessParameters: 00000000001f13a0
    WindowTitle:  'C:\Windows\system32\AUDIODG.EXE'
    ImageFile:    'C:\Windows\system32\AUDIODG.EXE'
    CommandLine:  'C:\Windows\system32\AUDIODG.EXE 0x2c4'
    DllPath:      'C:\Windows\System32'
    Environment:  00000000001f1310
        Path=C:\Windows\System32
        SystemDrive=C:
        SystemRoot=C:\Windows


        THREAD fffffa800451b060  Cid 032c.0330  Teb: 000007fffffde000 Win32Thread: fffff900c07ba3b0
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800451a1a0  NotificationEvent
            fffffa80044ff040  ProcessObject
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa800451dc10       Image:         audiodg.exe
        Wait Start TickCount      1581           Ticks: 44998 (0:00:11:41.973)
        Context Switch Count      98                 LargeStack
        UserTime                  00:00:00.015
        KernelTime                00:00:00.031
        Win32 Start Address AUDIODG!wWinMainCRTStartup (0x00000000ff8b4ddc)
        Stack Init fffff9800dae2db0 Current fffff9800dae2260
        Base fffff9800dae3000 Limit fffff9800dada000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0dae22a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0dae23e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0dae2440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0dae24b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0dae2960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0dae2bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0dae2c20)
        00000000`0018f858 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0018f860 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0018f970 00000000`ff8a4236 kernel32!WaitForMultipleObjects+0x11
        00000000`0018f9b0 00000000`ff8a4bbd AUDIODG!CAudioDGModule::RunMessageLoop+0x6a
        00000000`0018f9f0 00000000`ff8b4c4a AUDIODG!wWinMain+0x1d5
        00000000`0018fa60 00000000`76bfcdcd AUDIODG!TraceMessage+0x204
        00000000`0018fb20 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0018fb50 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8002137ad0  Cid 032c.0f50  Teb: 000007fffffd4000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa80044f6d00  QueueObject
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa800451dc10       Image:         audiodg.exe
        Wait Start TickCount      38126          Ticks: 8453 (0:00:02:11.867)
        Context Switch Count      503
        UserTime                  00:00:00.015
        KernelTime                00:00:00.062
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff9800e307db0 Current fffff9800e307810
        Base fffff9800e308000 Limit fffff9800e302000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e307850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e307990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0e3079f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0e307a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`0e307b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`0e307bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e307c20)
        00000000`0203f728 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`0203f730 000007fe`fedce7a3 kernel32!GetQueuedCompletionStatus+0x48
        00000000`0203f790 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`0203f820 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`0203f8d0 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`0203f900 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`0203f940 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`0203f970 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0203f9a0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

SLsvc process

```
PROCESS fffffa80044fbc10
    SessionId: 0  Cid: 0140    Peb: 7fffffd3000  ParentCid: 025c
    DirBase: 4ccda000  ObjectTable: fffff88005c4e6a0  HandleCount: 148.
    Image: SLsvc.exe
    VadRoot fffffa80044fb700 Vads 89 Clone 0 Private 2005. Modified 668. Locked 0.
    DeviceMap fffff8800598a680
    Token                             fffff8800598b060
    ElapsedTime                       00:11:42.673
    UserTime                          00:00:03.619
    KernelTime                        00:00:09.890
    QuotaPoolUsage[PagedPool]         123064
    QuotaPoolUsage[NonPagedPool]      9024
    Working Set Sizes (now,min,max)  (2718, 50, 345) (10872KB, 200KB, 1380KB)
    PeakWorkingSetSize                3784
    VirtualSize                       71 Mb
    PeakVirtualSize                   73 Mb
    PageFaultCount                    78979
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      2577

    Setting context for this process...
.process /p /r fffffa80044fbc10

    !peb
PEB at 000007fffffd3000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00000000ff420000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00000000000c2790 . 0000000001d225d0
    Ldr.InLoadOrderModuleList:           00000000000c26a0 . 0000000001d225b0
    Ldr.InMemoryOrderModuleList:         00000000000c26b0 . 0000000001d225c0
            Base TimeStamp                     Module
        ff420000 4549d080 Nov 02 11:03:28 2006 C:\Windows\system32\SLsvc.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        76bc0000 4549d328 Nov 02 11:14:48 2006 C:\Windows\system32\kernel32.dll
     7fefea30000 4549d267 Nov 02 11:11:35 2006 C:\Windows\system32\ADVAPI32.dll
     7fefed90000 469c43bb Jul 17 05:21:15 2007 C:\Windows\system32\RPCRT4.dll
     7fefdd40000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\system32\msvcrt.dll
     7fefcc20000 4549d32d Nov 02 11:14:53 2006 C:\Windows\system32\slc.dll
        76d00000 45d3ee19 Feb 15 05:22:33 2007 C:\Windows\system32\USER32.dll
     7fefec20000 4549d273 Nov 02 11:11:47 2006 C:\Windows\system32\GDI32.dll
     7fefce40000 4549d288 Nov 02 11:12:08 2006 C:\Windows\system32\DNSAPI.dll
     7fefd540000 4549d38a Nov 02 11:16:26 2006 C:\Windows\system32\WS2_32.dll
     7feff0b0000 4549d370 Nov 02 11:16:00 2006 C:\Windows\system32\NSI.dll
     7fefd9e0000 4549d2cb Nov 02 11:13:15 2006 C:\Windows\system32\IMM32.DLL
     7fefdc30000 4549d2e6 Nov 02 11:13:42 2006 C:\Windows\system32\MSCTF.dll
     7feff0c0000 4549d2a1 Nov 02 11:12:33 2006 C:\Windows\system32\LPK.DLL
     7fefd940000 4549d337 Nov 02 11:15:03 2006 C:\Windows\system32\USP10.dll
     7fefc620000 4549d31d Nov 02 11:14:37 2006 C:\Windows\system32\rsaenh.dll
     7fefddf0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\SHELL32.dll
     7fefda10000 4549d31f Nov 02 11:14:39 2006 C:\Windows\system32\SHLWAPI.dll
     7fefbe70000 4549d32b Nov 02 11:14:51 2006 C:\Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_1559f1c6f365a7fa\comctl32.dll
     7fefd760000 4549d317 Nov 02 11:14:31 2006 C:\Windows\system32\ole32.dll
     7fefd3b0000 4549d336 Nov 02 11:15:02 2006 C:\Windows\system32\USERENV.dll
     7fefd390000 4549d33f Nov 02 11:15:11 2006 C:\Windows\system32\Secur32.dll
     7fefeed0000 4549d318 Nov 02 11:14:32 2006 C:\Windows\system32\SETUPAPI.dll
     7fefdab0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\OLEAUT32.dll
     7fefc1e0000 4549d381 Nov 02 11:16:17 2006 C:\Windows\system32\WINTRUST.dll
     7fefcc50000 4549d344 Nov 02 11:15:16 2006 C:\Windows\system32\CRYPT32.dll
     7fefce00000 4549d2df Nov 02 11:13:35 2006 C:\Windows\system32\MSASN1.dll
```

```
     7fefda90000 462443ee Apr 17 04:50:06 2007 C:\Windows\system32\imagehlp.dll
     7fefc8f0000 4549d2e7 Nov 02 11:13:43 2006 C:\Windows\system32\mswsock.dll
     7fefc560000 4549d3a3 Nov 02 11:16:51 2006 C:\Windows\system32\wshtcpip.dll
     7fefc980000 4549d39d Nov 02 11:16:45 2006 C:\Windows\System32\wship6.dll
     7fefaab0000 4549d371 Nov 02 11:16:01 2006 C:\Windows\System32\winrnr.dll
     7fefd590000 4549d396 Nov 02 11:16:38 2006 C:\Windows\system32\WLDAP32.dll
     7fefd530000 4549d310 Nov 02 11:14:24 2006 C:\Windows\system32\PSAPI.DLL
     7fefc1a0000 4549d314 Nov 02 11:14:28 2006 C:\Windows\system32\NLAapi.dll
     7fefcb80000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\system32\IPHLPAPI.DLL
     7fefcb30000 4549d263 Nov 02 11:11:31 2006 C:\Windows\system32\dhcpcsvc.DLL
     7fefd280000 4549d370 Nov 02 11:16:00 2006 C:\Windows\system32\WINNSI.DLL
     7fefcb00000 4549d264 Nov 02 11:11:32 2006 C:\Windows\system32\dhcpcsvc6.DLL
     7fefaa70000 4549d2e4 Nov 02 11:13:40 2006 C:\Windows\system32\napinsp.dll
     7fefaa50000 4549d341 Nov 02 11:15:13 2006 C:\Windows\system32\pnrpnsp.dll
     7fefaac0000 4549d317 Nov 02 11:14:31 2006 C:\Windows\system32\rasadhlp.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       00000000000c0000
    ProcessParameters: 00000000000c1da0
    WindowTitle:  'C:\Windows\system32\SLsvc.exe'
    ImageFile:    'C:\Windows\system32\SLsvc.exe'
    CommandLine:  'C:\Windows\system32\SLsvc.exe'
    DllPath:
'C:\Windows\system32;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Wind
ows;C:\Windows\System32\Wbem'
    Environment:  00000000000c1310
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        LOCALAPPDATA=C:\Windows\ServiceProfiles\NetworkService\AppData\Local
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\SERVIC~2\NETWOR~1\AppData\Local\Temp
        TMP=C:\Windows\SERVIC~2\NETWOR~1\AppData\Local\Temp
        USERDOMAIN=DOMAIN
        USERNAME=COMPUTERNAME$
        USERPROFILE=C:\Windows\ServiceProfiles\NetworkService
        windir=C:\Windows
```

```
        THREAD fffffa800457c060  Cid 0140.019c  Teb: 000007fffffde000 Win32Thread: fffff900c07d6010
WAIT: (Executive) UserMode Non-Alertable
            fffffa800457ea18  NotificationEvent
        IRP List:
            fffffa80044f7720: (0006,0118) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa80044fbc10       Image:         SLsvc.exe
        Wait Start TickCount      1584           Ticks: 44995 (0:00:11:41.926)
        Context Switch Count      80                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address SLsvc (0x00000000ff4b0397)
        Stack Init fffff9800db2edb0 Current fffff9800db2e7f0
        Base fffff9800db2f000 Limit fffff9800db28000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0db2e830 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0db2e970 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0db2e9d0 fffff800`01ebdf16 nt!KeWaitForSingleObject+0x5f5
        fffff980`0db2ea50 fffff800`01ea1a24 nt!IopSynchronousServiceTail+0x306
        fffff980`0db2eac0 fffff800`01c4d733 nt!NtReadFile+0x583
        fffff980`0db2ebb0 00000000`76e202da nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0db2ec20)
        00000000`0028f1c8 00000000`76bf26da ntdll!NtReadFile+0xa
        00000000`0028f1d0 000007fe`fea865aa kernel32!ReadFile+0x8a
        00000000`0028f260 000007fe`fea862e3 ADVAPI32!ScGetPipeInput+0x4a
        00000000`0028f340 000007fe`fea850f3 ADVAPI32!ScDispatcherLoop+0x9a
        00000000`0028f440 00000000`ff43e6d5 ADVAPI32!StartServiceCtrlDispatcherW+0x176
        00000000`0028f6e0 00000000`ff4aaf7f SLsvc+0x1e6d5
        00000000`0028f740 00000000`ff4b0503 SLsvc+0x8af7f
        00000000`0028f780 00000000`76bfcdcd SLsvc+0x90503
        00000000`0028f800 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0028f830 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004766060  Cid 0140.044c  Teb: 000007fffffda000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa8004766870  SynchronizationTimer
            fffffa8004546560  NotificationEvent
            fffffa8004545040  SynchronizationTimer
            fffffa8004545590  SynchronizationTimer
            fffffa80044fbc10  ProcessObject
            fffffa80045c38c0  ProcessObject
            fffffa8004677f10  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa80044fbc10       Image:         SLsvc.exe
        Wait Start TickCount      9978           Ticks: 36601 (0:00:09:30.979)
        Context Switch Count      13
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x0000000076df6930)
        Stack Init fffff9800b3b9db0 Current fffff9800b3b9260
        Base fffff9800b3ba000 Limit fffff9800b3b4000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0b3b92a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0b3b93e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0b3b9440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0b3b94b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0b3b9960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0b3b9bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0b3b9c20)
        00000000`01b0f838 00000000`76df6b07 ntdll!NtWaitForMultipleObjects+0xa
        00000000`01b0f840 00000000`76bfcdcd ntdll!TppWaiterpThread+0x14d
        00000000`01b0fae0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`01b0fb10 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004531bb0  Cid 0140.0468  Teb: 000007fffffdc000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800388f1c0  SynchronizationEvent
            fffffa800389de00  NotificationEvent
            fffffa8004531c68  NotificationTimer
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa80044fbc10       Image:         SLsvc.exe
        Wait Start TickCount      1591           Ticks: 44988 (0:00:11:41.817)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address msvcrt!endthreadex (0x000007fefdd59620)
        Stack Init fffff9800d0c1db0 Current fffff9800d0c1260
        Base fffff9800d0c2000 Limit fffff9800d0bc000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 0 PagePriority 1
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0d0c12a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0d0c13e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0d0c1440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0d0c14b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0d0c1960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0d0c1bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0d0c1c20)
        00000000`018df608 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`018df610 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`018df720 00000000`ff596c2a kernel32!WaitForMultipleObjects+0x11
        00000000`018df760 000007fe`fdd594e7 SLsvc+0x176c2a
        00000000`018df9f0 000007fe`fdd5967d msvcrt!endthreadex+0x47
        00000000`018dfa20 00000000`76bfcdcd msvcrt!endthreadex+0x100
        00000000`018dfa50 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`018dfa80 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8002193060  Cid 0140.0e64  Teb: 000007fffffd8000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa80044ef530  QueueObject
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa80044fbc10       Image:         SLsvc.exe
        Wait Start TickCount      21767          Ticks: 24812 (0:00:06:27.069)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff98020cc8db0 Current fffff98020cc8810
        Base fffff98020cc9000 Limit fffff98020cc3000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`20cc8850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`20cc8990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`20cc89f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`20cc8a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`20cc8b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`20cc8bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`20cc8c20)
        00000000`00b6f8c8 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`00b6f8d0 000007fe`fedce7a3 kernel32!GetQueuedCompletionStatus+0x48
        00000000`00b6f930 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`00b6f9c0 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`00b6fa70 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`00b6faa0 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`00b6fae0 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`00b6fb10 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`00b6fb40 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

Svchost process (LocalService)

```
PROCESS fffffa80045c38c0
    SessionId: 0  Cid: 0424    Peb: 7fffffde000  ParentCid: 025c
    DirBase: 4c829000  ObjectTable: fffff880059c6a70  HandleCount: 642.
    Image: svchost.exe
    VadRoot fffffa80045c2420 Vads 172 Clone 0 Private 1478. Modified 654. Locked 20.
    DeviceMap fffff88005a30830
    Token                             fffff8800576f060
    ElapsedTime                       00:11:42.627
    UserTime                          00:00:00.249
    KernelTime                        00:00:00.312
    QuotaPoolUsage[PagedPool]         197552
    QuotaPoolUsage[NonPagedPool]      33328
    Working Set Sizes (now,min,max)  (3047, 50, 345) (12188KB, 200KB, 1380KB)
    PeakWorkingSetSize                3889
    VirtualSize                       97 Mb
    PeakVirtualSize                   101 Mb
    PageFaultCount                    4656
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      2110

    Setting context for this process...
.process /p /r fffffa80045c38c0

    !peb
PEB at 000007fffffde000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00000000ff910000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00000000003127d0 . 00000000020494e0
    Ldr.InLoadOrderModuleList:           00000000003126e0 . 00000000020494c0
    Ldr.InMemoryOrderModuleList:         00000000003126f0 . 00000000020494d0
            Base TimeStamp                     Module
        ff910000 4549b5f5 Nov 02 09:10:13 2006 C:\Windows\system32\svchost.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        76bc0000 4549d328 Nov 02 11:14:48 2006 C:\Windows\system32\kernel32.dll
     7fefdd40000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\system32\msvcrt.dll
     7fefea30000 4549d267 Nov 02 11:11:35 2006 C:\Windows\system32\ADVAPI32.dll
     7fefed90000 469c43bb Jul 17 05:21:15 2007 C:\Windows\system32\RPCRT4.dll
     7fefc5b0000 4549d384 Nov 02 11:16:20 2006 C:\Windows\system32\NTMARTA.DLL
        76d00000 45d3ee19 Feb 15 05:22:33 2007 C:\Windows\system32\USER32.dll
     7fefec20000 4549d273 Nov 02 11:11:47 2006 C:\Windows\system32\GDI32.dll
     7fefd590000 4549d396 Nov 02 11:16:38 2006 C:\Windows\system32\WLDAP32.dll
     7fefd540000 4549d38a Nov 02 11:16:26 2006 C:\Windows\system32\WS2_32.dll
     7feff0b0000 4549d370 Nov 02 11:16:00 2006 C:\Windows\system32\NSI.dll
     7fefd530000 4549d310 Nov 02 11:14:24 2006 C:\Windows\system32\PSAPI.DLL
     7fefce20000 4549d315 Nov 02 11:14:29 2006 C:\Windows\system32\SAMLIB.dll
     7fefd760000 4549d317 Nov 02 11:14:31 2006 C:\Windows\system32\ole32.dll
     7fefd9e0000 4549d2cb Nov 02 11:13:15 2006 C:\Windows\system32\IMM32.DLL
     7fefdc30000 4549d2e6 Nov 02 11:13:42 2006 C:\Windows\system32\MSCTF.dll
     7feff0c0000 4549d2a1 Nov 02 11:12:33 2006 C:\Windows\system32\LPK.DLL
     7fefd940000 4549d337 Nov 02 11:15:03 2006 C:\Windows\system32\USP10.dll
     7fefba70000 4549d2e7 Nov 02 11:13:43 2006 c:\windows\system32\es.dll
     7fefdab0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\OLEAUT32.dll
     7fefb4d0000 4549d30d Nov 02 11:14:21 2006 c:\windows\system32\PROPSYS.dll
     7fefc620000 4549d31d Nov 02 11:14:37 2006 C:\Windows\system32\rsaenh.dll
     7fefdb90000 4549d282 Nov 02 11:12:02 2006 C:\Windows\system32\CLBCatQ.DLL
     7fefb250000 4549d371 Nov 02 11:16:01 2006 c:\windows\system32\nsisvc.dll
     7fefc8f0000 4549d2e7 Nov 02 11:13:43 2006 C:\Windows\system32\mswsock.dll
     7fefc560000 4549d3a3 Nov 02 11:16:51 2006 C:\Windows\system32\wshtcpip.dll
     7fefc980000 4549d39d Nov 02 11:16:45 2006 C:\Windows\System32\wship6.dll
     7fefd390000 4549d33f Nov 02 11:15:11 2006 C:\Windows\system32\secur32.dll
```

```
     7fefca40000 4549d341 Nov 02 11:15:13 2006 C:\Windows\system32\credssp.dll
     7fefcc50000 4549d344 Nov 02 11:15:16 2006 C:\Windows\system32\CRYPT32.dll
     7fefce00000 4549d2df Nov 02 11:13:35 2006 C:\Windows\system32\MSASN1.dll
     7fefd3b0000 4549d336 Nov 02 11:15:02 2006 C:\Windows\system32\USERENV.dll
     7fefc670000 4549d321 Nov 02 11:14:41 2006 C:\Windows\system32\schannel.dll
     7fefcf70000 4549d2fc Nov 02 11:14:04 2006 C:\Windows\system32\NETAPI32.dll
     7fefade0000 4549d340 Nov 02 11:15:12 2006 c:\windows\system32\webclnt.dll
     7fefae90000 4549d36a Nov 02 11:15:54 2006 c:\windows\system32\WINHTTP.dll
     7fefda10000 4549d31f Nov 02 11:14:39 2006 C:\Windows\system32\SHLWAPI.dll
     7fefd5f0000 470c5dac Oct 10 06:05:48 2007 C:\Windows\system32\urlmon.dll
     7fefebc0000 4549d29c Nov 02 11:12:28 2006 C:\Windows\system32\iertutil.dll
     7fefbe70000 4549d32b Nov 02 11:14:51 2006 C:\Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_1559f1c6f365a7fa\comctl32.dll
     7fefddf0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\shell32.dll
     7fefec90000 470c5de6 Oct 10 06:06:46 2007 C:\Windows\system32\WinInet.dll
        76f70000 4549b4d2 Nov 02 09:05:22 2006 C:\Windows\system32\Normaliz.dll
     7fefac20000 4549d383 Nov 02 11:16:19 2006 c:\windows\system32\wkssvc.dll
     7fefcb80000 4549d2e1 Nov 02 11:13:37 2006 c:\windows\system32\IPHLPAPI.DLL
     7fefcb30000 4549d263 Nov 02 11:11:31 2006 c:\windows\system32\dhcpcsvc.DLL
     7fefce40000 4549d288 Nov 02 11:12:08 2006 c:\windows\system32\DNSAPI.dll
     7fefd280000 4549d370 Nov 02 11:16:00 2006 c:\windows\system32\WINNSI.DLL
     7fefcb00000 4549d264 Nov 02 11:11:32 2006 c:\windows\system32\dhcpcsvc6.DLL
     7fefcdd0000 4549d375 Nov 02 11:16:05 2006 c:\windows\system32\NTDSAPI.dll
     7fefc6d0000 4549d35d Nov 02 11:15:41 2006 c:\windows\system32\WINBRAND.dll
     7fefaab0000 4549d371 Nov 02 11:16:01 2006 C:\Windows\System32\winrnr.dll
     7fefc1a0000 4549d314 Nov 02 11:14:28 2006 C:\Windows\system32\NLAapi.dll
     7fefaa70000 4549d2e4 Nov 02 11:13:40 2006 C:\Windows\system32\napinsp.dll
     7fefaa50000 4549d341 Nov 02 11:15:13 2006 C:\Windows\system32\pnrpnsp.dll
     7fefaac0000 4549d317 Nov 02 11:14:31 2006 C:\Windows\system32\rasadhlp.dll
     7fefd1f0000 4549d32f Nov 02 11:14:55 2006 C:\Windows\system32\SXS.DLL
     7fefaa40000 4549d27e Nov 02 11:11:58 2006 c:\windows\system32\fdrespub.dll
     7fefa450000 4549d391 Nov 02 11:16:33 2006 c:\windows\system32\wsdapi.dll
     7fefa680000 4549d28c Nov 02 11:12:12 2006 c:\windows\system32\HTTPAPI.dll
     7fefc1e0000 4549d381 Nov 02 11:16:17 2006 c:\windows\system32\WINTRUST.dll
     7fefda90000 462443ee Apr 17 04:50:06 2007 C:\Windows\system32\imagehlp.dll
     7fefb930000 4549d350 Nov 02 11:15:28 2006 c:\windows\system32\XmlLite.dll
     7fefc460000 466785ee Jun 07 05:13:34 2007 c:\windows\system32\FirewallAPI.dll
     7fefca50000 4549d336 Nov 02 11:15:02 2006 c:\windows\system32\VERSION.dll
     7fefa290000 4549d325 Nov 02 11:14:45 2006 c:\windows\system32\ssdpsrv.dll
     7fefa020000 4549d32e Nov 02 11:14:54 2006 c:\windows\system32\w32time.dll
     7fefce80000 4549d346 Nov 02 11:15:18 2006 c:\windows\system32\cryptdll.dll
     7fefa230000 4549d27a Nov 02 11:11:54 2006 C:\Windows\system32\FunDisc.dll
     7fefc180000 4549d253 Nov 02 11:11:15 2006 C:\Windows\system32\ATL.DLL
     7fefeed0000 4549d318 Nov 02 11:14:32 2006 C:\Windows\system32\SETUPAPI.dll
     7fefc940000 4549d277 Nov 02 11:11:51 2006 C:\Windows\system32\GPAPI.dll
     7fefcc20000 4549d32d Nov 02 11:14:53 2006 C:\Windows\system32\slc.dll
     7fef9c40000 46662887 Jun 06 04:22:47 2007 C:\Windows\System32\msxml3.dll
     7fef9700000 4549d30c Nov 02 11:14:20 2006 c:\windows\system32\netprofm.dll
     7fef9640000 4549d32b Nov 02 11:14:51 2006 c:\windows\system32\upnphost.dll
     7fefa990000 4549d324 Nov 02 11:14:44 2006 c:\windows\system32\SSDPAPI.dll
     7fefa1f0000 4549d36c Nov 02 11:15:56 2006 C:\Windows\System32\npmproxy.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       0000000000310000
    ProcessParameters: 0000000000311db0
    WindowTitle:  'C:\Windows\system32\svchost.exe'
    ImageFile:    'C:\Windows\system32\svchost.exe'
    CommandLine:  'C:\Windows\system32\svchost.exe -k LocalService'
    DllPath:
'C:\Windows\system32;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Wind
ows;C:\Windows\System32\Wbem'
    Environment:  0000000000311310
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\ServiceProfiles\LocalService\AppData\Roaming
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        LOCALAPPDATA=C:\Windows\ServiceProfiles\LocalService\AppData\Local
        NUMBER_OF_PROCESSORS=2
```

```
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\SERVIC~2\LOCALS~1\AppData\Local\Temp
        TMP=C:\Windows\SERVIC~2\LOCALS~1\AppData\Local\Temp
        USERDOMAIN=NT AUTHORITY
        USERNAME=LOCAL SERVICE
        USERPROFILE=C:\Windows\ServiceProfiles\LocalService
        windir=C:\Windows


        THREAD fffffa80045793c0  Cid 0424.0428  Teb: 000007fffffdc000 Win32Thread: fffff900c07d8500
WAIT: (Executive) UserMode Non-Alertable
            fffffa8004578b08  NotificationEvent
        IRP List:
            fffffa8004b3b610: (0006,0118) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80045c38c0       Image:         svchost.exe
        Wait Start TickCount      7416           Ticks: 39163 (0:00:10:10.946)
        Context Switch Count      87                 LargeStack
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address svchost!wmainCRTStartup (0x00000000ff912550)
        Stack Init fffff9800db7adb0 Current fffff9800db7a7f0
        Base fffff9800db7b000 Limit fffff9800db74000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0db7a830 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0db7a970 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0db7a9d0 fffff800`01ebdf16 nt!KeWaitForSingleObject+0x5f5
        fffff980`0db7aa50 fffff800`01ea1a24 nt!IopSynchronousServiceTail+0x306
        fffff980`0db7aac0 fffff800`01c4d733 nt!NtReadFile+0x583
        fffff980`0db7abb0 00000000`76e202da nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0db7ac20)
        00000000`0025f688 00000000`76bf26da ntdll!NtReadFile+0xa
        00000000`0025f690 000007fe`fea865aa kernel32!ReadFile+0x8a
        00000000`0025f720 000007fe`fea862e3 ADVAPI32!ScGetPipeInput+0x4a
        00000000`0025f800 000007fe`fea850f3 ADVAPI32!ScDispatcherLoop+0x9a
        00000000`0025f900 00000000`ff91283c ADVAPI32!StartServiceCtrlDispatcherW+0x176
        00000000`0025fba0 00000000`ff912666 svchost!wmain+0xe5
        00000000`0025fbd0 00000000`76bfcdcd svchost!ScCreateWellKnownSids+0x301
        00000000`0025fc10 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0025fc40 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004554bb0  Cid 0424.045c  Teb: 000007fffffd8000 Win32Thread: fffff900c07f1010
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800477f6e0  NotificationEvent
            fffffa80021d9af0  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80045c38c0       Image:         svchost.exe
        Wait Start TickCount      10275          Ticks: 36304 (0:00:09:26.346)
        Context Switch Count      2147                 LargeStack
        UserTime                  00:00:00.078
        KernelTime                00:00:00.015
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff9800efb3db0 Current fffff9800efb3260
        Base fffff9800efb4000 Limit fffff9800efac000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0efb32a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0efb33e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0efb3440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0efb34b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0efb3960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0efb3bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0efb3c20)
        00000000`018ef198 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`018ef1a0 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`018ef2b0 000007fe`fa294b50 kernel32!WaitForMultipleObjects+0x11
        00000000`018ef2f0 000007fe`fedcb255 ssdpsrv!GetNotificationRpc+0x84
        00000000`018ef330 000007fe`fee9889d RPCRT4!Invoke+0x65
        00000000`018ef380 000007fe`fed97450 RPCRT4!Ndr64StubWorker+0x560
        00000000`018ef950 000007fe`fedcb4f4 RPCRT4!NdrServerCallAll+0x40
        00000000`018ef9a0 000007fe`fedcb365 RPCRT4!DispatchToStubInCNoAvrf+0x14
        00000000`018ef9d0 000007fe`fedcb606 RPCRT4!RPC_INTERFACE::DispatchToStubWorker+0xe9
        00000000`018efac0 000007fe`fedcb977 RPCRT4!LRPC_SCALL::DispatchRequest+0x1c2
        00000000`018efb30 000007fe`fedcb062 RPCRT4!LRPC_SCALL::HandleRequest+0x1fb
        00000000`018efc60 000007fe`fedce6f1 RPCRT4!LRPC_ADDRESS::ProcessIO+0x322
        00000000`018efd80 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x257
        00000000`018efe30 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`018efe60 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`018efea0 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`018efed0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`018eff00 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80045328a0  Cid 0424.0464  Teb: 000007fffffd4000 Win32Thread: fffff900c07ded60
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800477f6e0  NotificationEvent
            fffffa8004805960  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80045c38c0       Image:         svchost.exe
        Wait Start TickCount      1881           Ticks: 44698 (0:00:11:37.293)
        Context Switch Count      366                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff9800ef08db0 Current fffff9800ef08260
        Base fffff9800ef09000 Limit fffff9800ef02000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0ef082a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0ef083e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0ef08440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0ef084b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0ef08960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0ef08bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0ef08c20)
        00000000`0182f1e8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0182f1f0 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0182f300 000007fe`fa294b50 kernel32!WaitForMultipleObjects+0x11
        00000000`0182f340 000007fe`fedcb255 ssdpsrv!GetNotificationRpc+0x84
        00000000`0182f380 000007fe`fee9889d RPCRT4!Invoke+0x65
        00000000`0182f3d0 000007fe`fed97450 RPCRT4!Ndr64StubWorker+0x560
        00000000`0182f9a0 000007fe`fedcb4f4 RPCRT4!NdrServerCallAll+0x40
        00000000`0182f9f0 000007fe`fedcb365 RPCRT4!DispatchToStubInCNoAvrf+0x14
        00000000`0182fa20 000007fe`fedcb606 RPCRT4!RPC_INTERFACE::DispatchToStubWorker+0xe9
        00000000`0182fb10 000007fe`fedcb977 RPCRT4!LRPC_SCALL::DispatchRequest+0x1c2
        00000000`0182fb80 000007fe`fedcb062 RPCRT4!LRPC_SCALL::HandleRequest+0x1fb
        00000000`0182fcb0 000007fe`fedce6f1 RPCRT4!LRPC_ADDRESS::ProcessIO+0x322
        00000000`0182fdd0 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x257
        00000000`0182fe80 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`0182feb0 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`0182fef0 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`0182ff20 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0182ff50 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004530060  Cid 0424.046c  Teb: 000007fffffae000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa800452c430  SynchronizationTimer
            fffffa8004667c20  SynchronizationEvent
            fffffa80038a39b0  SynchronizationEvent
            fffffa800452ec10  SynchronizationEvent
            fffffa800453d130  SynchronizationEvent
            fffffa8004572e50  SynchronizationEvent
            fffffa80044e3430  SynchronizationEvent
            fffffa80046553f0  NotificationEvent
            fffffa800468ad30  SynchronizationEvent
            fffffa8004812740  Semaphore Limit 0x5
            fffffa8004812040  SynchronizationTimer
            fffffa8004812200  SynchronizationEvent
            fffffa800480ea90  SynchronizationEvent
            fffffa8004821190  SynchronizationEvent
            fffffa80048319d0  SynchronizationEvent
            fffffa800483ddf0  SynchronizationEvent
            fffffa800483eba0  SynchronizationEvent
            fffffa800483eb40  SynchronizationEvent
            fffffa800483e230  SynchronizationEvent
            fffffa800481ffe0  SynchronizationEvent
            fffffa8002955f80  NotificationEvent
            fffffa8002955fe0  SynchronizationEvent
            fffffa8004803430  SynchronizationEvent
            fffffa80048051f0  SynchronizationEvent
            fffffa8004835580  Thread
            fffffa8004807f20  SynchronizationEvent
            fffffa8004805190  SynchronizationEvent
            fffffa8004849620  SynchronizationTimer
            fffffa8004806a70  SynchronizationEvent
            fffffa80048069b0  NotificationEvent
            fffffa80044b7140  SynchronizationEvent
            fffffa800487d460  SynchronizationEvent
            fffffa8004884a10  SynchronizationEvent
            fffffa8004879230  SynchronizationEvent
            fffffa80046b7540  SynchronizationEvent
            fffffa800469bcd0  SynchronizationEvent
            fffffa800483edf0  NotificationEvent
            fffffa80048a2710  SynchronizationEvent
            fffffa800483edf0  NotificationEvent
            fffffa8004829a90  SynchronizationEvent
            fffffa80048033b0  NotificationEvent
            fffffa800480e200  SynchronizationEvent
            fffffa8004736560  SynchronizationEvent
            fffffa800477b110  SynchronizationEvent
            fffffa80048419f0  SynchronizationEvent
            fffffa80048074c0  SynchronizationEvent
            fffffa8004849d60  SynchronizationEvent
            fffffa800483b110  SynchronizationEvent
            fffffa80040a0eb0  SynchronizationEvent
            fffffa8004805250  SynchronizationEvent
            fffffa800477ba20  SynchronizationTimer
            fffffa80048118e0  SynchronizationEvent
            fffffa800483deb0  SynchronizationEvent
            fffffa8004839790  SynchronizationTimer
            fffffa8004891670  SynchronizationEvent
            fffffa8004530118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80045c38c0       Image:         svchost.exe
        Wait Start TickCount      44051          Ticks: 2528 (0:00:00:39.437)
        Context Switch Count      226
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x0000000076df6930)
        Stack Init fffff9800d0a5db0 Current fffff9800d0a5260
        Base fffff9800d0a6000 Limit fffff9800d0a0000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
```

```
        fffff980`0d0a52a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0d0a53e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0d0a5440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0d0a54b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0d0a5960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0d0a5bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0d0a5c20)
        00000000`01e0f718 00000000`76df6b07 ntdll!NtWaitForMultipleObjects+0xa
        00000000`01e0f720 00000000`76bfcdcd ntdll!TppWaiterpThread+0x14d
        00000000`01e0f9c0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`01e0f9f0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004539060  Cid 0424.047c  Teb: 000007fffffda000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Alertable
            fffffa800452eb80  QueueObject
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80045c38c0       Image:         svchost.exe
        Wait Start TickCount      2045           Ticks: 44534 (0:00:11:34.734)
        Context Switch Count      14
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x0000000076e17860)
        Stack Init fffff9800daa5db0 Current fffff9800daa5860
        Base fffff9800daa6000 Limit fffff9800daa0000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0daa58a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0daa59e0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0daa5a40 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0daa5ad0 fffff800`01c8a722 nt!IoRemoveIoCompletion+0x47
        fffff980`0daa5b50 fffff800`01c4d733 nt!NtWaitForWorkViaWorkerFactory+0x1f1
        fffff980`0daa5c20 00000000`76e21b4a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0daa5c20)
        00000000`01ecfa98 00000000`76e17a20 ntdll!NtWaitForWorkViaWorkerFactory+0xa
        00000000`01ecfaa0 00000000`76bfcdcd ntdll!TppWorkerThread+0x23e
        00000000`01ecfd10 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`01ecfd40 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004670bb0  Cid 0424.0638  Teb: 000007fffffa8000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80046695f0  NotificationEvent
            fffffa8004670c68  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80045c38c0       Image:         svchost.exe
        Wait Start TickCount      45971          Ticks: 608 (0:00:00:09.484)
        Context Switch Count      50
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address webclnt!TfsScavengerThread (0x000007fefae0ba14)
        Stack Init fffff9800e711db0 Current fffff9800e711960
        Base fffff9800e712000 Limit fffff9800e70c000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0e7119a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e711ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0e711b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0e711bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0e711c20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e711c20)
        00000000`00f7fdf8 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`00f7fe00 000007fe`fae0bbb3 kernel32!WaitForSingleObjectEx+0x9c
        00000000`00f7fec0 00000000`76bfcdcd webclnt!TfsScavengerThread+0x19f
        00000000`00f7fef0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`00f7ff20 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800467a060  Cid 0424.0644  Teb: 000007fffffa4000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa800465b980  QueueObject
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80045c38c0       Image:         svchost.exe
        Wait Start TickCount      1722           Ticks: 44857 (0:00:11:39.773)
        Context Switch Count      21
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address webclnt!DavWorkerThread (0x000007fefadedd80)
        Stack Init fffff9800e750db0 Current fffff9800e750500
        Base fffff9800e751000 Limit fffff9800e74b000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 3 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e750540 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e750680 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0e7506e0 fffff800`01c34eb1 nt!KeRemoveQueueEx+0x848
        fffff980`0e750770 fffff980`0e45a60d nt!KeRemoveQueue+0x21
        fffff980`0e7507b0 fffff980`0e444ff8 mrxdav!UMRxAssignWork+0x379
        fffff980`0e750810 fffff980`00be531b mrxdav!MRxDAVFastIoDeviceControl+0x2c8
        fffff980`0e750890 fffff980`004d9c0f mup!MupFastIoDeviceControl+0x8b
        fffff980`0e750900 fffff980`004f4a3e fltmgr! ?? ::FNODOBFM::`string'+0x10e
        fffff980`0e750960 fffff800`01e8dc75 fltmgr! ?? ::NNGAKEGL::`string'+0x433
        fffff980`0e750a00 fffff800`01e94136 nt!IopXxxControlFile+0x3b4
        fffff980`0e750b40 fffff800`01c4d733 nt!NtDeviceIoControlFile+0x56
        fffff980`0e750bb0 00000000`76e202ea nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e750c20)
        00000000`0225fe18 00000000`76be21da ntdll!ZwDeviceIoControlFile+0xa
        00000000`0225fe20 000007fe`fadee0a6 kernel32!DeviceIoControl+0xaa
        00000000`0225fea0 00000000`76bfcdcd webclnt!DavWorkerThread+0x326
        00000000`0225ff50 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0225ff80 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa800467abb0  Cid 0424.0648  Teb: 000007fffffa2000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa800465b980  QueueObject
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80045c38c0       Image:         svchost.exe
        Wait Start TickCount      1722           Ticks: 44857 (0:00:11:39.773)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address webclnt!DavWorkerThread (0x000007fefadedd80)
        Stack Init fffff9800e75edb0 Current fffff9800e75e500
        Base fffff9800e75f000 Limit fffff9800e759000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e75e540 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e75e680 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0e75e6e0 fffff800`01c34eb1 nt!KeRemoveQueueEx+0x848
        fffff980`0e75e770 fffff980`0e45a60d nt!KeRemoveQueue+0x21
        fffff980`0e75e7b0 fffff980`0e444ff8 mrxdav!UMRxAssignWork+0x379
        fffff980`0e75e810 fffff980`00be531b mrxdav!MRxDAVFastIoDeviceControl+0x2c8
        fffff980`0e75e890 fffff980`004d9c0f mup!MupFastIoDeviceControl+0x8b
        fffff980`0e75e900 fffff980`004f4a3e fltmgr! ?? ::FNODOBFM::`string'+0x10e
        fffff980`0e75e960 fffff800`01e8dc75 fltmgr! ?? ::NNGAKEGL::`string'+0x433
        fffff980`0e75ea00 fffff800`01e94136 nt!IopXxxControlFile+0x3b4
        fffff980`0e75eb40 fffff800`01c4d733 nt!NtDeviceIoControlFile+0x56
        fffff980`0e75ebb0 00000000`76e202ea nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e75ec20)
        00000000`0234f8b8 00000000`76be21da ntdll!ZwDeviceIoControlFile+0xa
        00000000`0234f8c0 000007fe`fadee0a6 kernel32!DeviceIoControl+0xaa
        00000000`0234f940 00000000`76bfcdcd webclnt!DavWorkerThread+0x326
        00000000`0234f9f0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0234fa20 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80046b0060  Cid 0424.067c  Teb: 000007fffffaa000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004811ea0  NotificationEvent
            fffffa8004820d30  NotificationEvent
        IRP List:
            fffffa8004820b00: (0006,01f0) Flags: 00060030  Mdl: fffffa80048209b0
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80045c38c0       Image:         svchost.exe
        Wait Start TickCount      1871           Ticks: 44708 (0:00:11:37.449)
        Context Switch Count      275
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address ntdll!TppWorkerThread (0x0000000076e17860)
        Stack Init fffff9800e4cfdb0 Current fffff9800e4cf260
        Base fffff9800e4d0000 Limit fffff9800e4ca000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e4cf2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e4cf3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0e4cf440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0e4cf4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0e4cf960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0e4cfbb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e4cfc20)
        00000000`0250f258 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0250f260 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0250f370 000007fe`fa4796e4 kernel32!WaitForMultipleObjects+0x11
        00000000`0250f3b0 00000000`76df6500 wsdapi!CWSDHttpListener::Listener+0x19c
        00000000`0250f8c0 00000000`76e17b59 ntdll!RtlpTpWorkCallback+0xf0
        00000000`0250f970 00000000`76bfcdcd ntdll!TppWorkerThread+0x3ad
        00000000`0250fbe0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0250fc10 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa800482f060  Cid 0424.07e0  Teb: 000007fffff9a000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800481f5c0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80045c38c0       Image:         svchost.exe
        Wait Start TickCount      19503          Ticks: 27076 (0:00:07:02.388)
        Context Switch Count      13
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ssdpsrv!CSsdpSearchRequestManager::DwSearchThreadProc
(0x000007fefa29a06c)
        Stack Init fffff9800f29adb0 Current fffff9800f29a960
        Base fffff9800f29b000 Limit fffff9800f295000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0f29a9a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0f29aae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0f29ab40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0f29abc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0f29ac20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0f29ac20)
        00000000`0210f698 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`0210f6a0 000007fe`fa29aab2 kernel32!WaitForSingleObjectEx+0x9c
        00000000`0210f760 00000000`76bfcdcd ssdpsrv!CSsdpSearchRequestManager::DwThreadFunc+0x2be
        00000000`0210f9e0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0210fa10 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800482ebb0  Cid 0424.07e4  Teb: 000007fffff98000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004828a60  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80045c38c0       Image:         svchost.exe
        Wait Start TickCount      1876           Ticks: 44703 (0:00:11:37.371)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address FunDisc!CNotificationQueue::ThreadProc (0x000007fefa23ace4)
        Stack Init fffff9800f2a1db0 Current fffff9800f2a1960
        Base fffff9800f2a2000 Limit fffff9800f29c000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0f2a19a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0f2a1ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0f2a1b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0f2a1bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0f2a1c20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0f2a1c20)
        00000000`02ecfc28 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`02ecfc30 000007fe`fa23afd0 kernel32!WaitForSingleObjectEx+0x9c
        00000000`02ecfcf0 00000000`76bfcdcd FunDisc!CNotificationQueue::ThreadProc+0x2ec
        00000000`02ecfd50 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02ecfd80 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004835580  Cid 0424.07ec  Teb: 000007fffff96000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004808fe0  NotificationEvent
            fffffa80047759d0  SynchronizationEvent
            fffffa8004835638  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80045c38c0       Image:         svchost.exe
        Wait Start TickCount      41405          Ticks: 5174 (0:00:01:20.714)
        Context Switch Count      19
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address w32time!ClockDisciplineThread (0x000007fefa02ce90)
        Stack Init fffff9800f2afdb0 Current fffff9800f2af260
        Base fffff9800f2b0000 Limit fffff9800f2aa000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0f2af2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0f2af3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0f2af440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0f2af4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0f2af960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0f2afbb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0f2afc20)
        00000000`0284f2f8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0284f300 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0284f410 000007fe`fa021b26 kernel32!WaitForMultipleObjects+0x11
        00000000`0284f450 00000000`76bfcdcd w32time!ClockDisciplineThread+0x761
        00000000`0284fa40 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0284fa70 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800483fbb0  Cid 0424.07f4  Teb: 000007fffff94000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800483b6d0  SynchronizationEvent
            fffffa8004835a90  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80045c38c0       Image:         svchost.exe
        Wait Start TickCount      16042          Ticks: 30537 (0:00:07:56.380)
        Context Switch Count      19
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ssdpsrv!CReceiveDataManager::ThreadFunc (0x000007fefa2a2038)
        Stack Init fffff9800f3b9db0 Current fffff9800f3b9260
        Base fffff9800f3ba000 Limit fffff9800f3b4000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0f3b92a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0f3b93e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0f3b9440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0f3b94b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0f3b9960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0f3b9bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0f3b9c20)
        00000000`028efbf8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`028efc00 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`028efd10 000007fe`fa2a2081 kernel32!WaitForMultipleObjects+0x11
        00000000`028efd50 00000000`76bfcdcd ssdpsrv!CReceiveDataManager::ThreadFunc+0x49
        00000000`028efea0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`028efed0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004829060  Cid 0424.07f8  Teb: 000007fffff9e000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa800482e530  SynchronizationEvent
            fffffa800485ce00  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80045c38c0       Image:         svchost.exe
        Wait Start TickCount      1880           Ticks: 44699 (0:00:11:37.308)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address FunDisc!CRegProvider::ThreadProc (0x000007fefa2443d8)
        Stack Init fffff9800f277db0 Current fffff9800f277260
        Base fffff9800f278000 Limit fffff9800f272000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0f2772a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0f2773e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0f277440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0f2774b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0f277960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0f277bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0f277c20)
        00000000`0327f5c8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0327f5d0 000007fe`fa24628f kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0327f6e0 00000000`76bfcdcd FunDisc!CRegProvider::MemberThreadProc+0x16f
        00000000`0327fba0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0327fbd0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004663060  Cid 0424.007c  Teb: 000007fffff9c000 Win32Thread: fffff900c07f2ab0
WAIT: (WrQueue) UserMode Alertable
            fffffa8004531730  QueueObject
        IRP List:
            fffffa80048b0230: (0006,01f0) Flags: 00060030  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80045c38c0       Image:         svchost.exe
        Wait Start TickCount      44051          Ticks: 2528 (0:00:00:39.437)
        Context Switch Count      221                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x0000000076e17860)
        Stack Init fffff980108f5db0 Current fffff980108f5860
        Base fffff980108f6000 Limit fffff980108ef000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`108f58a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`108f59e0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`108f5a40 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`108f5ad0 fffff800`01c8a722 nt!IoRemoveIoCompletion+0x47
        fffff980`108f5b50 fffff800`01c4d733 nt!NtWaitForWorkViaWorkerFactory+0x1f1
        fffff980`108f5c20 00000000`76e21b4a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`108f5c20)
        00000000`0247fa38 00000000`76e17a20 ntdll!NtWaitForWorkViaWorkerFactory+0xa
        00000000`0247fa40 00000000`76bfcdcd ntdll!TppWorkerThread+0x23e
        00000000`0247fcb0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0247fce0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004864060  Cid 0424.0594  Teb: 000007fffff8c000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Alertable
            fffffa8004531730  QueueObject
        IRP List:
            fffffa80048bfe10: (0006,01f0) Flags: 00060030  Mdl: 00000000
            fffffa80048b31f0: (0006,01f0) Flags: 00060030  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80045c38c0       Image:         svchost.exe
        Wait Start TickCount      16235          Ticks: 30344 (0:00:07:53.369)
        Context Switch Count      135
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x0000000076e17860)
        Stack Init fffff98010396db0 Current fffff98010396860
        Base fffff98010397000 Limit fffff98010391000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`103968a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`103969e0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`10396a40 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`10396ad0 fffff800`01c8a722 nt!IoRemoveIoCompletion+0x47
        fffff980`10396b50 fffff800`01c4d733 nt!NtWaitForWorkViaWorkerFactory+0x1f1
        fffff980`10396c20 00000000`76e21b4a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`10396c20)
        00000000`0340fcb8 00000000`76e17a20 ntdll!NtWaitForWorkViaWorkerFactory+0xa
        00000000`0340fcc0 00000000`76bfcdcd ntdll!TppWorkerThread+0x23e
        00000000`0340ff30 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0340ff60 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004882060  Cid 0424.0520  Teb: 000007fffff90000 Win32Thread: fffff900c07f12c0
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa8004884b30  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80045c38c0       Image:         svchost.exe
        Wait Start TickCount      3026           Ticks: 43553 (0:00:11:19.431)
        Context Switch Count      20                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address netprofm!CImplINetworkListManager::EventMgrThreadProc
(0x000007fef9713598)
        Stack Init fffff9800efa0db0 Current fffff9800efa0740
        Base fffff9800efa1000 Limit fffff9800ef9a000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0efa0780 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0efa08c0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0efa0920 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`0efa09a0 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`0efa0a40 fffff960`000c7e1e win32k!xxxSleepThread+0x56
        fffff980`0efa0a70 fffff960`000c7f25 win32k!xxxRealInternalGetMessage+0x72e
        fffff980`0efa0b50 fffff960`000c97e4 win32k!xxxInternalGetMessage+0x35
        fffff980`0efa0b90 fffff800`01c4d733 win32k!NtUserGetMessage+0x64
        fffff980`0efa0c20 00000000`76d1e6aa nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0efa0c20)
        00000000`026bf8b8 00000000`76d1e6ea USER32!ZwUserGetMessage+0xa
        00000000`026bf8c0 000007fe`f97137fc USER32!GetMessageW+0x34
        00000000`026bf8f0 00000000`76bfcdcd
netprofm!CImplINetworkListManager::EventMgrThreadProc+0x264
        00000000`026bf9a0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`026bf9d0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80048c1060  Cid 0424.084c  Teb: 000007fffff86000 Win32Thread: fffff900c07f1d60
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa800489fbc0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80045c38c0       Image:         svchost.exe
        Wait Start TickCount      3026           Ticks: 43553 (0:00:11:19.431)
        Context Switch Count      15                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address netprofm!CImplINetworkListManager::EventWorkerThreadProc
(0x000007fef9715e34)
        Stack Init fffff98010908db0 Current fffff98010908740
        Base fffff98010909000 Limit fffff98010902000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`10908780 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`109088c0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`10908920 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`109089a0 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`10908a40 fffff960`000c7e1e win32k!xxxSleepThread+0x56
        fffff980`10908a70 fffff960`000c7f25 win32k!xxxRealInternalGetMessage+0x72e
        fffff980`10908b50 fffff960`000c97e4 win32k!xxxInternalGetMessage+0x35
        fffff980`10908b90 fffff800`01c4d733 win32k!NtUserGetMessage+0x64
        fffff980`10908c20 00000000`76d1e6aa nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`10908c20)
        00000000`03eafa38 00000000`76d1e6ea USER32!ZwUserGetMessage+0xa
        00000000`03eafa40 000007fe`f9715ef3 USER32!GetMessageW+0x34
        00000000`03eafa70 00000000`76bfcdcd
netprofm!CImplINetworkListManager::EventWorkerThreadProc+0xbf
        00000000`03eafb00 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`03eafb30 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8002b05bb0  Cid 0424.0754  Teb: 000007fffffd6000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800477f6e0  NotificationEvent
            fffffa8002187810  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80045c38c0       Image:         svchost.exe
        Wait Start TickCount      16235          Ticks: 30344 (0:00:07:53.369)
        Context Switch Count      10
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff9801da9adb0 Current fffff9801da9a260
        Base fffff9801da9b000 Limit fffff9801da95000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1da9a2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1da9a3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`1da9a440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`1da9a4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`1da9a960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`1da9abb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1da9ac20)
        00000000`03b8f018 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`03b8f020 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`03b8f130 000007fe`fa294b50 kernel32!WaitForMultipleObjects+0x11
        00000000`03b8f170 000007fe`fedcb255 ssdpsrv!GetNotificationRpc+0x84
        00000000`03b8f1b0 000007fe`fee9889d RPCRT4!Invoke+0x65
        00000000`03b8f200 000007fe`fed97450 RPCRT4!Ndr64StubWorker+0x560
        00000000`03b8f7d0 000007fe`fedcb4f4 RPCRT4!NdrServerCallAll+0x40
        00000000`03b8f820 000007fe`fedcb365 RPCRT4!DispatchToStubInCNoAvrf+0x14
        00000000`03b8f850 000007fe`fedcb606 RPCRT4!RPC_INTERFACE::DispatchToStubWorker+0xe9
        00000000`03b8f940 000007fe`fedcb977 RPCRT4!LRPC_SCALL::DispatchRequest+0x1c2
        00000000`03b8f9b0 000007fe`fedcb062 RPCRT4!LRPC_SCALL::HandleRequest+0x1fb
        00000000`03b8fae0 000007fe`fedce6f1 RPCRT4!LRPC_ADDRESS::ProcessIO+0x322
        00000000`03b8fc00 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x257
        00000000`03b8fcb0 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`03b8fce0 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`03b8fd20 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`03b8fd50 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`03b8fd80 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80040b0060  Cid 0424.0bf4  Teb: 000007fffffac000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa800457dcb0  QueueObject
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa80045c38c0       Image:         svchost.exe
        Wait Start TickCount      45975          Ticks: 604 (0:00:00:09.422)
        Context Switch Count      7
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff98020c74db0 Current fffff98020c74810
        Base fffff98020c75000 Limit fffff98020c6f000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`20c74850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`20c74990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`20c749f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`20c74a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`20c74b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`20c74bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`20c74c20)
        00000000`0274f6f8 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`0274f700 000007fe`fedce7a3 kernel32!GetQueuedCompletionStatus+0x48
        00000000`0274f760 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`0274f7f0 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`0274f8a0 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`0274f8d0 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`0274f910 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`0274f940 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0274f970 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

Svchost process (NetworkService)

```
PROCESS fffffa8004567c10
    SessionId: 0  Cid: 04cc    Peb: 7fffffde000  ParentCid: 025c
    DirBase: 4a04f000  ObjectTable: fffff88005771a10  HandleCount: 525.
    Image: svchost.exe
    VadRoot fffffa800438a140 Vads 222 Clone 0 Private 2135. Modified 1139. Locked 0.
    DeviceMap fffff8800598a680
    Token                             fffff88005a8c060
    ElapsedTime                       00:11:42.096
    UserTime                          00:00:00.109
    KernelTime                        00:00:00.390
    QuotaPoolUsage[PagedPool]         178856
    QuotaPoolUsage[NonPagedPool]      31536
    Working Set Sizes (now,min,max)  (3404, 50, 345) (13616KB, 200KB, 1380KB)
    PeakWorkingSetSize                4511
    VirtualSize                       373 Mb
    PeakVirtualSize                   376 Mb
    PageFaultCount                    5339
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      4046

    Setting context for this process...
.process /p /r fffffa8004567c10

    !peb
PEB at 000007fffffde000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00000000ff910000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00000000002d27c0 . 00000000032cd770
    Ldr.InLoadOrderModuleList:           00000000002d26d0 . 00000000032cd8f0
    Ldr.InMemoryOrderModuleList:         00000000002d26e0 . 00000000032cd900
            Base TimeStamp                     Module
        ff910000 4549b5f5 Nov 02 09:10:13 2006 C:\Windows\system32\svchost.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        76bc0000 4549d328 Nov 02 11:14:48 2006 C:\Windows\system32\kernel32.dll
     7fefdd40000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\system32\msvcrt.dll
     7fefea30000 4549d267 Nov 02 11:11:35 2006 C:\Windows\system32\ADVAPI32.dll
     7fefed90000 469c43bb Jul 17 05:21:15 2007 C:\Windows\system32\RPCRT4.dll
     7fefc5b0000 4549d384 Nov 02 11:16:20 2006 C:\Windows\system32\NTMARTA.DLL
        76d00000 45d3ee19 Feb 15 05:22:33 2007 C:\Windows\system32\USER32.dll
     7fefec20000 4549d273 Nov 02 11:11:47 2006 C:\Windows\system32\GDI32.dll
     7fefd590000 4549d396 Nov 02 11:16:38 2006 C:\Windows\system32\WLDAP32.dll
     7fefd540000 4549d38a Nov 02 11:16:26 2006 C:\Windows\system32\WS2_32.dll
     7feff0b0000 4549d370 Nov 02 11:16:00 2006 C:\Windows\system32\NSI.dll
     7fefd530000 4549d310 Nov 02 11:14:24 2006 C:\Windows\system32\PSAPI.DLL
     7fefce20000 4549d315 Nov 02 11:14:29 2006 C:\Windows\system32\SAMLIB.dll
     7fefd760000 4549d317 Nov 02 11:14:31 2006 C:\Windows\system32\ole32.dll
     7fefd9e0000 4549d2cb Nov 02 11:13:15 2006 C:\Windows\system32\IMM32.DLL
     7fefdc30000 4549d2e6 Nov 02 11:13:42 2006 C:\Windows\system32\MSCTF.dll
     7feff0c0000 4549d2a1 Nov 02 11:12:33 2006 C:\Windows\system32\LPK.DLL
     7fefd940000 4549d337 Nov 02 11:15:03 2006 C:\Windows\system32\USP10.dll
     7fefb220000 4549d28d Nov 02 11:12:13 2006 c:\windows\system32\dnsrslvr.dll
     7fefce40000 4549d288 Nov 02 11:12:08 2006 c:\windows\system32\DNSAPI.dll
     7fefcb30000 4549d263 Nov 02 11:11:31 2006 c:\windows\system32\dhcpcsvc.DLL
     7fefd390000 4549d33f Nov 02 11:15:11 2006 c:\windows\system32\Secur32.dll
     7fefd280000 4549d370 Nov 02 11:16:00 2006 c:\windows\system32\WINNSI.DLL
     7fefcb00000 4549d264 Nov 02 11:11:32 2006 c:\windows\system32\dhcpcsvc6.DLL
     7fefcb80000 4549d2e1 Nov 02 11:13:37 2006 c:\windows\system32\IPHLPAPI.DLL
     7fefc8f0000 4549d2e7 Nov 02 11:13:43 2006 C:\Windows\system32\mswsock.dll
     7fefc980000 4549d39d Nov 02 11:16:45 2006 C:\Windows\System32\wship6.dll
     7fefc560000 4549d3a3 Nov 02 11:16:51 2006 C:\Windows\system32\wshtcpip.dll
```

```
     7fefa960000 4549d349 Nov 02 11:15:21 2006 c:\windows\system32\cryptsvc.dll
     7fefdab0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\OLEAUT32.dll
     7fefa800000 4549d33f Nov 02 11:15:11 2006 c:\windows\system32\VSSAPI.DLL
     7fefc180000 4549d253 Nov 02 11:11:15 2006 c:\windows\system32\ATL.DLL
     7fefa9a0000 4549d341 Nov 02 11:15:13 2006 c:\windows\system32\vsstrace.dll
     7fefd360000 4549d265 Nov 02 11:11:33 2006 c:\windows\system32\AUTHZ.dll
     7fefb930000 4549d350 Nov 02 11:15:28 2006 c:\windows\system32\XmlLite.dll
     7fefcf70000 4549d2fc Nov 02 11:14:04 2006 c:\windows\system32\NETAPI32.dll
     7fefcd90000 4549d2b2 Nov 02 11:12:50 2006 c:\windows\system32\MPR.dll
     7fefeed0000 4549d318 Nov 02 11:14:32 2006 C:\Windows\system32\SETUPAPI.dll
     7fefcc50000 4549d344 Nov 02 11:15:16 2006 c:\windows\system32\CRYPT32.dll
     7fefce00000 4549d2df Nov 02 11:13:35 2006 c:\windows\system32\MSASN1.dll
     7fefd3b0000 4549d336 Nov 02 11:15:02 2006 c:\windows\system32\USERENV.dll
     7fefc620000 4549d31d Nov 02 11:14:37 2006 C:\Windows\system32\rsaenh.dll
     7fefdb90000 4549d282 Nov 02 11:12:02 2006 C:\Windows\system32\CLBCatQ.DLL
     7fefba70000 4549d2e7 Nov 02 11:13:43 2006 C:\Windows\system32\es.dll
     7fefb4d0000 4549d30d Nov 02 11:14:21 2006 C:\Windows\system32\PROPSYS.dll
     7fefa630000 4549d315 Nov 02 11:14:29 2006 c:\windows\system32\nlasvc.dll
     7fefcbb0000 4549d349 Nov 02 11:15:21 2006 c:\windows\system32\wevtapi.dll
     7fefa7e0000 4549d2f4 Nov 02 11:13:56 2006 c:\windows\system32\ncsi.dll
     7fefae90000 4549d36a Nov 02 11:15:54 2006 c:\windows\system32\WINHTTP.dll
     7fefda10000 4549d31f Nov 02 11:14:39 2006 C:\Windows\system32\SHLWAPI.dll
     7fefc450000 4549d34e Nov 02 11:15:26 2006 c:\windows\system32\WTSAPI32.dll
     7fefca60000 4549d252 Nov 02 11:11:14 2006 c:\windows\system32\bcrypt.dll
     7fefbe70000 4549d32b Nov 02 11:14:51 2006 C:\Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_1559f1c6f365a7fa\comctl32.dll
     7fefca40000 4549d341 Nov 02 11:15:13 2006 C:\Windows\system32\credssp.dll
     7fefc670000 4549d321 Nov 02 11:14:41 2006 C:\Windows\system32\schannel.dll
     7fefa990000 4549d324 Nov 02 11:14:44 2006 C:\Windows\system32\ssdpapi.dll
     7fefa080000 4549d342 Nov 02 11:15:14 2006 c:\windows\system32\termsrv.dll
     7fefa670000 4549d287 Nov 02 11:12:07 2006 c:\windows\system32\ICAAPI.dll
     7fefc1e0000 4549d381 Nov 02 11:16:17 2006 c:\windows\system32\WINTRUST.dll
     7fefda90000 462443ee Apr 17 04:50:06 2007 C:\Windows\system32\imagehlp.dll
     7fefddf0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\SHELL32.dll
     7fefd1b0000 4549d380 Nov 02 11:16:16 2006 C:\Windows\system32\WINSTA.dll
     7fefaab0000 4549d371 Nov 02 11:16:01 2006 C:\Windows\System32\winrnr.dll
     7fefc1a0000 4549d314 Nov 02 11:14:28 2006 C:\Windows\system32\NLAapi.dll
     7fefaa70000 4549d2e4 Nov 02 11:13:40 2006 C:\Windows\system32\napinsp.dll
     7fefaa50000 4549d341 Nov 02 11:15:13 2006 C:\Windows\system32\pnrpnsp.dll
     7fefaac0000 4549d317 Nov 02 11:14:31 2006 C:\Windows\system32\rasadhlp.dll
     7fefcdd0000 4549d375 Nov 02 11:16:05 2006 C:\Windows\system32\NTDSAPI.DLL
     7fefc990000 4549d327 Nov 02 11:14:47 2006 C:\Windows\system32\kerberos.dll
     7fefce80000 4549d346 Nov 02 11:15:18 2006 C:\Windows\system32\cryptdll.dll
     7fef43b0000 4549d331 Nov 02 11:14:57 2006 c:\windows\system32\tapisrv.dll
     7fefaad0000 4549d254 Nov 02 11:11:16 2006 c:\windows\system32\ACTIVEDS.dll
     7fefaa00000 4549d263 Nov 02 11:11:31 2006 c:\windows\system32\adsldpc.dll
     7fefa9c0000 4549d342 Nov 02 11:15:14 2006 c:\windows\system32\credui.dll
     7fefc2c0000 4549d329 Nov 02 11:14:49 2006 c:\windows\system32\rtutils.dll
     7fefb360000 4549d36f Nov 02 11:15:59 2006 c:\windows\system32\WINMM.dll
     7fefb310000 4549d318 Nov 02 11:14:32 2006 c:\windows\system32\OLEACC.dll
     7fef3e80000 4549d330 Nov 02 11:14:56 2006 C:\Windows\system32\unimdm.tsp
     7fef7580000 4549d332 Nov 02 11:14:58 2006 C:\Windows\system32\uniplat.dll
     7fef8160000 4549d32b Nov 02 11:14:51 2006 C:\Windows\system32\kmddsp.tsp
     7fef6570000 4549d2fb Nov 02 11:14:03 2006 C:\Windows\system32\ndptsp.tsp
     7fef6cf0000 4549d282 Nov 02 11:12:02 2006 C:\Windows\system32\hidphone.tsp
     7fefb2c0000 4549d281 Nov 02 11:12:01 2006 C:\Windows\system32\HID.DLL
     7fef8cf0000 4549d2e8 Nov 02 11:13:44 2006 C:\Windows\system32\ESENT.dll
     7fef50a0000 4549d2fb Nov 02 11:14:03 2006 c:\windows\system32\msdtckrm.dll
     7fefca50000 4549d336 Nov 02 11:15:02 2006 c:\windows\system32\VERSION.dll
     7fefb110000 4549d334 Nov 02 11:15:00 2006 c:\windows\system32\ktmw32.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       00000000002d0000
    ProcessParameters: 00000000002d1da0
    WindowTitle:  'C:\Windows\system32\svchost.exe'
    ImageFile:    'C:\Windows\system32\svchost.exe'
    CommandLine:  'C:\Windows\system32\svchost.exe -k NetworkService'
    DllPath:
'C:\Windows\system32;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Wind
ows;C:\Windows\System32\Wbem'
    Environment:  00000000002d1310
```

```
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        LOCALAPPDATA=C:\Windows\ServiceProfiles\NetworkService\AppData\Local
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\SERVIC~2\NETWOR~1\AppData\Local\Temp
        TMP=C:\Windows\SERVIC~2\NETWOR~1\AppData\Local\Temp
        USERDOMAIN=DOMAIN
        USERNAME=COMPUTERNAME$
        USERPROFILE=C:\Windows\ServiceProfiles\NetworkService
        windir=C:\Windows


        THREAD fffffa8004242260  Cid 04cc.04d0  Teb: 000007fffffdc000 Win32Thread: fffff900c07dba60
WAIT: (Executive) UserMode Non-Alertable
            fffffa80045bed68  NotificationEvent
        IRP List:
            fffffa80045810d0: (0006,0118) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa8004567c10       Image:         svchost.exe
        Wait Start TickCount      15653          Ticks: 30926 (0:00:08:02.448)
        Context Switch Count      123                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address svchost!wmainCRTStartup (0x00000000ff912550)
        Stack Init fffff9800d1ecdb0 Current fffff9800d1ec7f0
        Base fffff9800d1ed000 Limit fffff9800d1e6000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0d1ec830 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0d1ec970 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0d1ec9d0 fffff800`01ebdf16 nt!KeWaitForSingleObject+0x5f5
        fffff980`0d1eca50 fffff800`01ea1a24 nt!IopSynchronousServiceTail+0x306
        fffff980`0d1ecac0 fffff800`01c4d733 nt!NtReadFile+0x583
        fffff980`0d1ecbb0 00000000`76e202da nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0d1ecc20)
        00000000`0018f778 00000000`76bf26da ntdll!NtReadFile+0xa
        00000000`0018f780 000007fe`fea865aa kernel32!ReadFile+0x8a
        00000000`0018f810 000007fe`fea862e3 ADVAPI32!ScGetPipeInput+0x4a
        00000000`0018f8f0 000007fe`fea850f3 ADVAPI32!ScDispatcherLoop+0x9a
        00000000`0018f9f0 00000000`ff91283c ADVAPI32!StartServiceCtrlDispatcherW+0x176
        00000000`0018fc90 00000000`ff912666 svchost!wmain+0xe5
        00000000`0018fcc0 00000000`76bfcdcd svchost!ScCreateWellKnownSids+0x301
        00000000`0018fd00 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0018fd30 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004570060  Cid 04cc.050c  Teb: 000007fffffd8000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80045bd240  NotificationEvent
            fffffa80045a03f8  NotificationEvent
            fffffa8004594be0  SynchronizationEvent
            fffffa8004594b00  SynchronizationEvent
        IRP List:
            fffffa80044c5a10: (0006,03a0) Flags: 00060000  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa8004567c10       Image:         svchost.exe
        Wait Start TickCount      1626           Ticks: 44953 (0:00:11:41.271)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address dnsrslvr!NotifyThread (0x000007fefb227860)
        Stack Init fffff9800e33fdb0 Current fffff9800e33f260
        Base fffff9800e340000 Limit fffff9800e33a000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e33f2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e33f3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0e33f440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0e33f4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0e33f960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0e33fbb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e33fc20)
        00000000`018bf338 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`018bf340 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`018bf450 000007fe`fb227a75 kernel32!WaitForMultipleObjects+0x11
        00000000`018bf490 00000000`76bfcdcd dnsrslvr!NotifyThread+0x283
        00000000`018bf920 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`018bf950 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa800456f060  Cid 04cc.0510  Teb: 000007fffffd6000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004375720  NotificationEvent
            fffffa80045bd240  NotificationEvent
        IRP List:
            fffffa80049a6e10: (0006,01f0) Flags: 00060030  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa8004567c10       Image:         svchost.exe
        Wait Start TickCount      2397           Ticks: 44182 (0:00:11:29.243)
        Context Switch Count      55
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address dnsrslvr!Ip_NotifyThread (0x000007fefb224ed0)
        Stack Init fffff9800e34ddb0 Current fffff9800e34d260
        Base fffff9800e34e000 Limit fffff9800e348000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e34d2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e34d3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0e34d440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0e34d4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0e34d960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0e34dbb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e34dc20)
        00000000`0174f808 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0174f810 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0174f920 000007fe`fb22509d kernel32!WaitForMultipleObjects+0x11
        00000000`0174f960 00000000`76bfcdcd dnsrslvr!Ip_NotifyThread+0x249
        00000000`0174fa20 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0174fa50 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800456e060  Cid 04cc.0514  Teb: 000007fffffd4000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80045bf4f0  NotificationEvent
            fffffa80045bf490  NotificationEvent
            fffffa8004375830  NotificationEvent
            fffffa800456e118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa8004567c10       Image:         svchost.exe
        Wait Start TickCount      2179           Ticks: 44400 (0:00:11:32.644)
        Context Switch Count      88
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address dnsrslvr!Mcast_Thread (0x000007fefb223830)
        Stack Init fffff9800e354db0 Current fffff9800e354260
        Base fffff9800e355000 Limit fffff9800e34f000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e3542a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e3543e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0e354440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0e3544b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0e354960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0e354bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e354c20)
        00000000`0194f9a8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0194f9b0 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0194fac0 000007fe`fb223899 kernel32!WaitForMultipleObjects+0x11
        00000000`0194fb00 00000000`76bfcdcd dnsrslvr!Mcast_Thread+0x1b7
        00000000`0194fb60 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0194fb90 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004570990  Cid 04cc.051c  Teb: 000007fffffac000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa8004577270  SynchronizationTimer
            fffffa80045c0860  SynchronizationEvent
            fffffa80047603d0  NotificationEvent
            fffffa800472eab0  NotificationEvent
            fffffa8004816a10  SynchronizationTimer
            fffffa8004806770  SynchronizationEvent
            fffffa800480a400  SynchronizationEvent
            fffffa800480f2e0  SynchronizationEvent
            fffffa8004802c10  SynchronizationEvent
            fffffa800480b040  SynchronizationEvent
            fffffa800480e890  SynchronizationEvent
            fffffa8004823290  SynchronizationEvent
            fffffa8004813630  SynchronizationEvent
            fffffa800492d330  ProcessObject
            fffffa80047ee640  SynchronizationEvent
            fffffa8004a30d00  SynchronizationEvent
            fffffa80045d2600  SynchronizationEvent
            fffffa80048117f0  SynchronizationEvent
            fffffa8004b2c4f8  NotificationEvent
            fffffa80044c6a90  NotificationEvent
            fffffa800467e998  NotificationEvent
            fffffa800404ee30  SynchronizationEvent
            fffffa80047ffa40  SynchronizationEvent
            fffffa8004816ef0  SynchronizationTimer
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa8004567c10       Image:         svchost.exe
        Wait Start TickCount      46486          Ticks: 93 (0:00:00:01.450)
        Context Switch Count      290
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x0000000076df6930)
        Stack Init fffff9800e370db0 Current fffff9800e370260
        Base fffff9800e371000 Limit fffff9800e36b000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0e3702a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e3703e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0e370440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0e3704b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0e370960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0e370bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e370c20)
        00000000`00bffa78 00000000`76df6b07 ntdll!NtWaitForMultipleObjects+0xa
        00000000`00bffa80 00000000`76bfcdcd ntdll!TppWaiterpThread+0x14d
        00000000`00bffd20 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`00bffd50 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80047ff060  Cid 04cc.079c  Teb: 000007fffffa0000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80047fddf0  SynchronizationEvent
            fffffa80047ff118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa8004567c10       Image:         svchost.exe
        Wait Start TickCount      2187           Ticks: 44392 (0:00:11:32.519)
        Context Switch Count      9
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address dnsrslvr!Areg_RegistrationThread (0x000007fefb223af0)
        Stack Init fffff9800ea92db0 Current fffff9800ea92960
        Base fffff9800ea93000 Limit fffff9800ea8d000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0ea929a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0ea92ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0ea92b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0ea92bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0ea92c20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0ea92c20)
        00000000`0168f948 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`0168f950 000007fe`fb223b85 kernel32!WaitForSingleObjectEx+0x9c
        00000000`0168fa10 00000000`76bfcdcd dnsrslvr!Areg_RegistrationThread+0xa1
        00000000`0168fa60 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0168fa90 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004808060  Cid 04cc.07b0  Teb: 000007fffff9c000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Alertable
            fffffa800477e6c0  QueueObject
        IRP List:
            fffffa800222cca0: (0006,0358) Flags: 00060000  Mdl: 00000000
            fffffa8004a5cca0: (0006,0358) Flags: 00060000  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa8004567c10       Image:         svchost.exe
        Wait Start TickCount      9839           Ticks: 36740 (0:00:09:33.147)
        Context Switch Count      58
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x0000000076e17860)
        Stack Init fffff9800eafbdb0 Current fffff9800eafb860
        Base fffff9800eafc000 Limit fffff9800eaf6000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0eafb8a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0eafb9e0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0eafba40 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0eafbad0 fffff800`01c8a722 nt!IoRemoveIoCompletion+0x47
        fffff980`0eafbb50 fffff800`01c4d733 nt!NtWaitForWorkViaWorkerFactory+0x1f1
        fffff980`0eafbc20 00000000`76e21b4a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0eafbc20)
        00000000`01e7fcd8 00000000`76e17a20 ntdll!NtWaitForWorkViaWorkerFactory+0xa
        00000000`01e7fce0 00000000`76bfcdcd ntdll!TppWorkerThread+0x23e
        00000000`01e7ff50 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`01e7ff80 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800480bbb0  Cid 04cc.07c0  Teb: 000007fffff9a000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004810200  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa8004567c10       Image:         svchost.exe
        Wait Start TickCount      1872           Ticks: 44707 (0:00:11:37.433)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address termsrv!CService::staticMiscThread (0x000007fefa0a515c)
        Stack Init fffff9800e2acdb0 Current fffff9800e2ac960
        Base fffff9800e2ad000 Limit fffff9800e2a7000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e2ac9a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e2acae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0e2acb40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0e2acbc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0e2acc20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e2acc20)
        00000000`02c5fa98 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`02c5faa0 000007fe`fa0a51bc kernel32!WaitForSingleObjectEx+0x9c
        00000000`02c5fb60 00000000`76bfcdcd termsrv!CService::staticMiscThread+0x60
        00000000`02c5fb90 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02c5fbc0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80048148f0  Cid 04cc.07d0  Teb: 000007fffff98000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800480c670  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa8004567c10       Image:         svchost.exe
        Wait Start TickCount      2115           Ticks: 44464 (0:00:11:33.642)
        Context Switch Count      60
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nlasvc!QueueMonitor (0x000007fefa644ee8)
        Stack Init fffff9800f285db0 Current fffff9800f285960
        Base fffff9800f286000 Limit fffff9800f280000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0f2859a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0f285ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0f285b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0f285bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0f285c20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0f285c20)
        00000000`02eef8a8 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`02eef8b0 000007fe`fa6451ad kernel32!WaitForSingleObjectEx+0x9c
        00000000`02eef970 00000000`76bfcdcd nlasvc!QueueMonitor+0x2c5
        00000000`02eef9e0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02eefa10 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004837bb0  Cid 04cc.0598  Teb: 000007fffff9e000 Win32Thread: 0000000000000000
WAIT: (WrLpcReply) UserMode Non-Alertable
            fffffa8004837f40  Semaphore Limit 0x1
        Waiting for reply to ALPC Message fffff8800600ecf0
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa8004567c10       Image:         svchost.exe
        Wait Start TickCount      1881           Ticks: 44698 (0:00:11:37.293)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ssdpapi!GetNotificationLoop (0x000007fefa995000)
        Stack Init fffff9801039ddb0 Current fffff9801039d6e0
        Base fffff9801039e000 Limit fffff98010398000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1039d720 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1039d860 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`1039d8c0 fffff800`01c8f857 nt!KeWaitForSingleObject+0x5f5
        fffff980`1039d940 fffff800`01ebed64 nt!AlpcpSignalAndWait+0x97
        fffff980`1039d980 fffff800`01e9a80a nt!AlpcpReceiveSynchronousReply+0x44
        fffff980`1039d9e0 fffff800`01eb747f nt!AlpcpProcessSynchronousRequest+0x257
        fffff980`1039db00 fffff800`01c4d733 nt!NtAlpcSendWaitReceivePort+0x19f
        fffff980`1039dbb0 00000000`76e20aca nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1039dc20)
        00000000`0335f068 000007fe`fedba66b ntdll!NtAlpcSendWaitReceivePort+0xa
        00000000`0335f070 000007fe`fedbd422 RPCRT4!LRPC_CCALL::SendReceive+0xbb
        00000000`0335f0f0 000007fe`fedbd472 RPCRT4!I_RpcSendReceive+0x42
        00000000`0335f120 000007fe`fee9a2bc RPCRT4!NdrSendReceive+0x32
        00000000`0335f150 000007fe`fee9a3d0 RPCRT4!NdrpClientCall3+0x11c
        00000000`0335f3a0 000007fe`fa995086 RPCRT4!NdrClientCall3+0x7c
        00000000`0335f710 00000000`76bfcdcd ssdpapi!GetNotificationLoop+0x86
        00000000`0335f790 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0335f7c0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004887bb0  Cid 04cc.04f0  Teb: 000007fffff8c000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80044beaa0  SynchronizationEvent
            fffffa80044bd8e0  NotificationEvent
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa8004567c10       Image:         svchost.exe
        Wait Start TickCount      1897           Ticks: 44682 (0:00:11:37.043)
        Context Switch Count      18
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address msvcrt!endthreadex (0x000007fefdd59620)
        Stack Init fffff98010357db0 Current fffff98010357260
        Base fffff98010358000 Limit fffff98010352000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`103572a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`103573e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`10357440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`103574b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`10357960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`10357bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`10357c20)
        00000000`035bfd58 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`035bfd60 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`035bfe70 000007fe`fa7e7bd8 kernel32!WaitForMultipleObjects+0x11
        00000000`035bfeb0 000007fe`fdd594e7 ncsi!CNcsiConfigData::MonitorRegistry+0x14c
        00000000`035bff00 000007fe`fdd5967d msvcrt!endthreadex+0x47
        00000000`035bff30 00000000`76bfcdcd msvcrt!endthreadex+0x100
        00000000`035bff60 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`035bff90 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004887700  Cid 04cc.0524  Teb: 000007fffff88000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004892f60  SynchronizationEvent
            fffffa8004815510  SynchronizationEvent
            fffffa8004893f00  SynchronizationEvent
        IRP List:
            fffffa800489ddb0: (0006,0118) Flags: 00060000  Mdl: 00000000
            fffffa8004893da0: (0006,0118) Flags: 00060000  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa8004567c10       Image:         svchost.exe
        Wait Start TickCount      1985           Ticks: 44594 (0:00:11:35.670)
        Context Switch Count      66
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address msvcrt!endthreadex (0x000007fefdd59620)
        Stack Init fffff9800eab5db0 Current fffff9800eab5260
        Base fffff9800eab6000 Limit fffff9800eab0000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0eab52a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0eab53e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0eab5440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0eab54b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0eab5960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0eab5bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0eab5c20)
        00000000`01c4f5a8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`01c4f5b0 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`01c4f6c0 000007fe`fa7f0d74 kernel32!WaitForMultipleObjects+0x11
        00000000`01c4f700 000007fe`fdd594e7 ncsi!NcsiMediaChange+0x294
        00000000`01c4f7e0 000007fe`fdd5967d msvcrt!endthreadex+0x47
        00000000`01c4f810 00000000`76bfcdcd msvcrt!endthreadex+0x100
        00000000`01c4f840 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`01c4f870 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80049a6280  Cid 04cc.08f4  Teb: 000007fffffaa000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80046d3ca0  NotificationEvent
            fffffa8004860d80  NotificationEvent
            fffffa80044e23f0  NotificationEvent
            fffffa80049a6338  NotificationTimer
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa8004567c10       Image:         svchost.exe
        Wait Start TickCount      2139           Ticks: 44440 (0:00:11:33.268)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address dnsrslvr!Responder_Thread (0x000007fefb223910)
        Stack Init fffff9800cc92db0 Current fffff9800cc92260
        Base fffff9800cc93000 Limit fffff9800cc8d000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0cc922a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0cc923e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0cc92440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0cc924b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0cc92960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0cc92bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0cc92c20)
        00000000`03a1f998 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`03a1f9a0 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`03a1fab0 000007fe`fb2239bc kernel32!WaitForMultipleObjects+0x11
        00000000`03a1faf0 00000000`76bfcdcd dnsrslvr!Responder_Thread+0x259
        00000000`03a1fb70 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`03a1fba0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80044c0730  Cid 04cc.03b4  Teb: 000007fffff94000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004320160  NotificationEvent
            fffffa80044c07e8  NotificationTimer
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa8004567c10       Image:         svchost.exe
        Wait Start TickCount      45895          Ticks: 684 (0:00:00:10.670)
        Context Switch Count      23
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address tapisrv!SPEventHandlerThread (0x000007fef43b1690)
        Stack Init fffff9800baa5db0 Current fffff9800baa5960
        Base fffff9800baa6000 Limit fffff9800baa0000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0baa59a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0baa5ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0baa5b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0baa5bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0baa5c20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0baa5c20)
        00000000`0349fac8 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`0349fad0 000007fe`f43b16f1 kernel32!WaitForSingleObjectEx+0x9c
        00000000`0349fb90 00000000`76bfcdcd tapisrv!SPEventHandlerThread+0x6e
        00000000`0349fc00 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0349fc30 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8002016bb0  Cid 04cc.09d0  Teb: 000007fffff92000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80043e5bc0  NotificationEvent
            fffffa8002016c68  NotificationTimer
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa8004567c10       Image:         svchost.exe
        Wait Start TickCount      45898          Ticks: 681 (0:00:00:10.623)
        Context Switch Count      22
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address tapisrv!SPEventHandlerThread (0x000007fef43b1690)
        Stack Init fffff9800ebffdb0 Current fffff9800ebff960
        Base fffff9800ec00000 Limit fffff9800ebfa000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0ebff9a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0ebffae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0ebffb40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0ebffbc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0ebffc20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0ebffc20)
        00000000`031bf9d8 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`031bf9e0 000007fe`f43b16f1 kernel32!WaitForSingleObjectEx+0x9c
        00000000`031bfaa0 00000000`76bfcdcd tapisrv!SPEventHandlerThread+0x6e
        00000000`031bfb10 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`031bfb40 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800203e060  Cid 04cc.0cdc  Teb: 000007fffff90000 Win32Thread: 0000000000000000
WAIT: (DelayExecution) UserMode Alertable
            fffffa800203e118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa8004567c10       Image:         svchost.exe
        Wait Start TickCount      7641           Ticks: 38938 (0:00:10:07.436)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address unimdm!tepAPC (0x000007fef3ea3dec)
        Stack Init fffff980159c7db0 Current fffff980159c7990
        Base fffff980159c8000 Limit fffff980159c2000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`159c79d0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`159c7b10 fffff800`01c5b5a9 nt!KiSwapThread+0x125
        fffff980`159c7b70 fffff800`01e8ae9d nt!KeDelayExecutionThread+0x339
        fffff980`159c7bf0 fffff800`01c4d733 nt!NtDelayExecution+0x5c
        fffff980`159c7c20 00000000`76e205ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`159c7c20)
        00000000`033df7f8 00000000`76bfd908 ntdll!NtDelayExecution+0xa
        00000000`033df800 000007fe`f3ea3e2a kernel32!SleepEx+0x84
        00000000`033df880 00000000`76bfcdcd unimdm!tepAPC+0x3e
        00000000`033df8b0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`033df8e0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa800205d770  Cid 04cc.0ce0  Teb: 000007fffff8e000 Win32Thread: fffff900c07c3d60
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80048c73b0  NotificationEvent
            fffffa8001f113c0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa8004567c10       Image:         svchost.exe
        Wait Start TickCount      7643           Ticks: 38936 (0:00:10:07.405)
        Context Switch Count      5                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address uniplat!MonitorWorkerThread (0x000007fef7581820)
        Stack Init fffff980158bedb0 Current fffff980158be260
        Base fffff980158bf000 Limit fffff980158b7000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`158be2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`158be3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`158be440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`158be4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`158be960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`158bebb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`158bec20)
        00000000`03cffbd8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`03cffbe0 00000000`76d1e96d kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`03cffcf0 00000000`76d1e85e USER32!RealMsgWaitForMultipleObjectsEx+0x129
        00000000`03cffd90 00000000`76d13680 USER32!MsgWaitForMultipleObjectsEx+0x46
        00000000`03cffdd0 000007fe`f7581960 USER32!MsgWaitForMultipleObjects+0x20
        00000000`03cffe10 00000000`76bfcdcd uniplat!MonitorWorkerThread+0x14e
        00000000`03cfff00 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`03cfff30 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8001fe13a0  Cid 04cc.0ce4  Teb: 000007fffff8a000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8002002670  QueueObject
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa8004567c10       Image:         svchost.exe
        Wait Start TickCount      7646           Ticks: 38933 (0:00:10:07.358)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address kmddsp!AsyncEventsThread (0x000007fef8165354)
        Stack Init fffff9801dbc7db0 Current fffff9801dbc7810
        Base fffff9801dbc8000 Limit fffff9801dbc2000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1dbc7850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1dbc7990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`1dbc79f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`1dbc7a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`1dbc7b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`1dbc7bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1dbc7c20)
        00000000`03b7fa58 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`03b7fa60 000007fe`f8165423 kernel32!GetQueuedCompletionStatus+0x48
        00000000`03b7fac0 00000000`76bfcdcd kmddsp!AsyncEventsThread+0xcf
        00000000`03b7fb80 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`03b7fbb0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8001e67bb0  Cid 04cc.0ce8  Teb: 000007fffff84000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8003d85eb0  QueueObject
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa8004567c10       Image:         svchost.exe
        Wait Start TickCount      7648           Ticks: 38931 (0:00:10:07.327)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ndptsp!AsyncEventsThread (0x000007fef6577624)
        Stack Init fffff9801a691db0 Current fffff9801a691810
        Base fffff9801a692000 Limit fffff9801a68c000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1a691850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1a691990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`1a6919f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`1a691a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`1a691b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`1a691bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1a691c20)
        00000000`01bafcb8 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`01bafcc0 000007fe`f65776ef kernel32!GetQueuedCompletionStatus+0x48
        00000000`01bafd20 00000000`76bfcdcd ndptsp!AsyncEventsThread+0xcb
        00000000`01bafde0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`01bafe10 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8002087bb0  Cid 04cc.0cf8  Teb: 000007fffff80000 Win32Thread: fffff900c2003ab0
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800206e6c0  NotificationEvent
            fffffa8002079850  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa8004567c10       Image:         svchost.exe
        Wait Start TickCount      7652           Ticks: 38927 (0:00:10:07.265)
        Context Switch Count      2                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address hidphone!AsyncEventQueueServiceThread (0x000007fef6cf2084)
        Stack Init fffff98012f7cdb0 Current fffff98012f7c260
        Base fffff98012f7d000 Limit fffff98012f75000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`12f7c2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12f7c3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`12f7c440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`12f7c4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`12f7c960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`12f7cbb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12f7cc20)
        00000000`03e1fbc8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`03e1fbd0 00000000`76d1e96d kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`03e1fce0 00000000`76d1e85e USER32!RealMsgWaitForMultipleObjectsEx+0x129
        00000000`03e1fd80 000007fe`f6cf21d2 USER32!MsgWaitForMultipleObjectsEx+0x46
        00000000`03e1fdc0 00000000`76bfcdcd hidphone!AsyncEventQueueServiceThread+0x14e
        00000000`03e1fee0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`03e1ff10 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa800260f500  Cid 04cc.060c  Teb: 000007fffffa2000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa80025ac5f0  QueueObject
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa8004567c10       Image:         svchost.exe
        Wait Start TickCount      16091          Ticks: 30488 (0:00:07:55.615)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address msdtckrm!ProcessNotification (0x000007fef50cf124)
        Stack Init fffff9801581edb0 Current fffff9801581e810
        Base fffff9801581f000 Limit fffff98015819000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1581e850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1581e990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`1581e9f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`1581ea80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`1581eb00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`1581ebb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1581ec20)
        00000000`03d7f798 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`03d7f7a0 000007fe`f50cf27e kernel32!GetQueuedCompletionStatus+0x48
        00000000`03d7f800 00000000`76bfcdcd msdtckrm!ProcessNotification+0x15a
        00000000`03d7f8a0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`03d7f8d0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8002032800  Cid 04cc.0f68  Teb: 000007fffffa8000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Alertable
            fffffa80045c12c0  QueueObject
            fffffa80020328b8  NotificationTimer
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa8004567c10       Image:         svchost.exe
        Wait Start TickCount      46486          Ticks: 93 (0:00:00:01.450)
        Context Switch Count      113
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x0000000076e17860)
        Stack Init fffff9800cc6fdb0 Current fffff9800cc6f860
        Base fffff9800cc70000 Limit fffff9800cc6a000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0cc6f8a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0cc6f9e0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0cc6fa40 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0cc6fad0 fffff800`01c8a722 nt!IoRemoveIoCompletion+0x47
        fffff980`0cc6fb50 fffff800`01c4d733 nt!NtWaitForWorkViaWorkerFactory+0x1f1
        fffff980`0cc6fc20 00000000`76e21b4a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0cc6fc20)
        00000000`01dcfbd8 00000000`76e17a20 ntdll!NtWaitForWorkViaWorkerFactory+0xa
        00000000`01dcfbe0 00000000`76bfcdcd ntdll!TppWorkerThread+0x23e
        00000000`01dcfe50 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`01dcfe80 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004d14060  Cid 04cc.0f04  Teb: 000007fffffae000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Alertable
            fffffa80045c12c0  QueueObject
            fffffa8004d14118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa8004567c10       Image:         svchost.exe
        Wait Start TickCount      46486          Ticks: 93 (0:00:00:01.450)
        Context Switch Count      27
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x0000000076e17860)
        Stack Init fffff9800e72ddb0 Current fffff9800e72d860
        Base fffff9800e72e000 Limit fffff9800e728000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0e72d8a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e72d9e0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0e72da40 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0e72dad0 fffff800`01c8a722 nt!IoRemoveIoCompletion+0x47
        fffff980`0e72db50 fffff800`01c4d733 nt!NtWaitForWorkViaWorkerFactory+0x1f1
        fffff980`0e72dc20 00000000`76e21b4a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e72dc20)
        00000000`01b1f5a8 00000000`76e17a20 ntdll!NtWaitForWorkViaWorkerFactory+0xa
        00000000`01b1f5b0 00000000`76bfcdcd ntdll!TppWorkerThread+0x23e
        00000000`01b1f820 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`01b1f850 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8002486060  Cid 04cc.09fc  Teb: 000007fffffa4000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa80045bd5c0  QueueObject
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa8004567c10       Image:         svchost.exe
        Wait Start TickCount      45975          Ticks: 604 (0:00:00:09.422)
        Context Switch Count      7
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff9800eaf4db0 Current fffff9800eaf4810
        Base fffff9800eaf5000 Limit fffff9800eaef000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0eaf4850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0eaf4990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0eaf49f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0eaf4a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`0eaf4b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`0eaf4bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0eaf4c20)
        00000000`0309f538 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`0309f540 000007fe`fedce7a3 kernel32!GetQueuedCompletionStatus+0x48
        00000000`0309f5a0 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`0309f630 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`0309f6e0 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`0309f710 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`0309f750 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`0309f780 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0309f7b0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

Ati2evxx.exe process (session 0)

```
PROCESS fffffa80045a53d0
    SessionId: 1  Cid: 0528    Peb: 7fffffde000  ParentCid: 0118
    DirBase: 484ed000  ObjectTable: fffff88005d21c00  HandleCount:  92.
    Image: Ati2evxx.exe
    VadRoot fffffa80045a5350 Vads 64 Clone 0 Private 489. Modified 381. Locked 0.
    DeviceMap fffff88000007820
    Token                             fffff88005d5d7d0
    ElapsedTime                       00:11:41.846
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         100336
    QuotaPoolUsage[NonPagedPool]      6112
    Working Set Sizes (now,min,max)  (943, 50, 345) (3772KB, 200KB, 1380KB)
    PeakWorkingSetSize                1434
    VirtualSize                       56 Mb
    PeakVirtualSize                   57 Mb
    PageFaultCount                    1482
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      577

    Setting context for this process...
.process /p /r fffffa80045a53d0

    !peb
PEB at 000007fffffde000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         0000000000400000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00000000002f2730 . 000000000031c6f0
    Ldr.InLoadOrderModuleList:           00000000002f2640 . 000000000031c6d0
    Ldr.InMemoryOrderModuleList:         00000000002f2650 . 000000000031c6e0
            Base TimeStamp                     Module
          400000 453ec111 Oct 25 02:42:41 2006 C:\Windows\system32\Ati2evxx.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        76bc0000 4549d328 Nov 02 11:14:48 2006 C:\Windows\system32\kernel32.dll
        76d00000 45d3ee19 Feb 15 05:22:33 2007 C:\Windows\system32\USER32.dll
     7fefec20000 4549d273 Nov 02 11:11:47 2006 C:\Windows\system32\GDI32.dll
     7fefea30000 4549d267 Nov 02 11:11:35 2006 C:\Windows\system32\ADVAPI32.dll
     7fefed90000 469c43bb Jul 17 05:21:15 2007 C:\Windows\system32\RPCRT4.dll
     7fefd760000 4549d317 Nov 02 11:14:31 2006 C:\Windows\system32\ole32.dll
     7fefdd40000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\system32\msvcrt.dll
     7fefdab0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\OLEAUT32.dll
     7fefd9e0000 4549d2cb Nov 02 11:13:15 2006 C:\Windows\system32\IMM32.DLL
     7fefdc30000 4549d2e6 Nov 02 11:13:42 2006 C:\Windows\system32\MSCTF.dll
     7feff0c0000 4549d2a1 Nov 02 11:12:33 2006 C:\Windows\system32\LPK.DLL
     7fefd940000 4549d337 Nov 02 11:15:03 2006 C:\Windows\system32\USP10.dll
     7fefd3b0000 4549d336 Nov 02 11:15:02 2006 C:\Windows\system32\userenv.dll
     7fefd390000 4549d33f Nov 02 11:15:11 2006 C:\Windows\system32\Secur32.dll
     7fefc580000 4549d351 Nov 02 11:15:29 2006 C:\Windows\system32\powrprof.dll
     7fefd530000 4549d310 Nov 02 11:14:24 2006 C:\Windows\system32\psapi.dll
     7fefc330000 4549d33b Nov 02 11:15:07 2006 C:\Windows\system32\uxtheme.dll
     7fefd1b0000 4549d380 Nov 02 11:16:16 2006 C:\Windows\system32\WINSTA.dll
          950000 453ec141 Oct 25 02:43:29 2006 C:\Windows\system32\Atiedu64.dll
        10000000 453ec159 Oct 25 02:43:53 2006 C:\Windows\system32\atipdl64.dll
         1fd0000 453ec11d Oct 25 02:42:53 2006 C:\Windows\system32\ati2evxx.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       00000000002f0000
    ProcessParameters: 00000000002f1d20
    WindowTitle:  'C:\Windows\system32\Ati2evxx.exe'
    ImageFile:    'C:\Windows\system32\Ati2evxx.exe'
    CommandLine:  'Ati2evxx.exe -Client'
```

```
    DllPath:
'C:\Windows\system32;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Wind
ows;C:\Windows\System32\Wbem'
    Environment:  00000000002f1310
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\system32\config\systemprofile\AppData\Roaming
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        LOCALAPPDATA=C:\Windows\system32\config\systemprofile\AppData\Local
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\TEMP
        TMP=C:\Windows\TEMP
        USERDOMAIN=DOMAIN
        USERNAME=COMPUTERNAME$
        USERPROFILE=C:\Windows\system32\config\systemprofile
        windir=C:\Windows
```

```
        THREAD fffffa800453e710  Cid 0528.052c  Teb: 000007fffffdc000 Win32Thread: fffff900c206d010
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa800453dde0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80045a53d0       Image:         Ati2evxx.exe
        Wait Start TickCount      13619          Ticks: 32960 (0:00:08:34.179)
        Context Switch Count      831                 LargeStack
        UserTime                  00:00:00.031
        KernelTime                00:00:00.078
        Win32 Start Address Ati2evxx (0x0000000000456a30)
        Stack Init fffff9800e508db0 Current fffff9800e508740
        Base fffff9800e509000 Limit fffff9800e500000 Call 0
        Priority 14 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e508780 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e5088c0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0e508920 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`0e5089a0 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`0e508a40 fffff960`000c7e1e win32k!xxxSleepThread+0x56
        fffff980`0e508a70 fffff960`000c7f25 win32k!xxxRealInternalGetMessage+0x72e
        fffff980`0e508b50 fffff960`000c97e4 win32k!xxxInternalGetMessage+0x35
        fffff980`0e508b90 fffff800`01c4d733 win32k!NtUserGetMessage+0x64
        fffff980`0e508c20 00000000`76d1e6aa nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e508c20)
        00000000`0012f3a8 00000000`76d1bf4e USER32!ZwUserGetMessage+0xa
        00000000`0012f3b0 00000000`00410672 USER32!GetMessageA+0xc3
        00000000`0012f3e0 00000000`00000000 Ati2evxx+0x10672
        00000000`0012f3e8 00000000`00400000 0x0
        00000000`0012f3f0 00000000`00000000 Ati2evxx
        00000000`0012f3f8 00000000`00000000 0x0
        00000000`0012f400 00000000`00000001 0x0
        00000000`0012f408 00000000`0012f420 0x1
        00000000`0012f410 00000000`00000000 0x12f420
        00000000`0012f418 00000000`00000000 0x0
        00000000`0012f420 00000000`000005a8 0x0
        00000000`0012f428 00000000`00000000 0x5a8
        00000000`0012f430 ffffffff`00000000 0x0
        00000000`0012f438 ffffffff`ffffffff 0xffffffff`00000000
        00000000`0012f440 ffffffff`ffffffff 0xffffffff`ffffffff
        00000000`0012f448 00000000`00000000 0xffffffff`ffffffff
        00000000`0012f450 00000000`00000000 0x0
        00000000`0012f458 0000002c`00000000 0x0
        00000000`0012f460 00000000`00000000 0x2c`00000000
        00000000`0012f468 00000000`00000000 0x0
        00000000`0012f470 00000000`00000000 0x0
        00000000`0012f478 00000000`00000000 0x0
        00000000`0012f480 00000000`00000001 0x0
        00000000`0012f488 ffffffff`fffffffe 0x1
        00000000`0012f490 0000002c`00000000 0xffffffff`fffffffe
        00000000`0012f498 00000000`00000000 0x2c`00000000
        00000000`0012f4a0 00000000`00000000 0x0
        00000000`0012f4a8 00000000`00000000 0x0
        00000000`0012f4b0 00000000`00000000 0x0
        00000000`0012f4b8 00000000`00000001 0x0
        00000000`0012f4c0 00000000`0001003e 0x1
```

```
        THREAD fffffa80045adbb0  Cid 0528.056c  Teb: 000007fffffda000 Win32Thread: 0000000000000000
WAIT: (Executive) UserMode Non-Alertable
            fffffa80045b6fb8  NotificationEvent
        IRP List:
            fffffa8004490c40: (0006,0118) Flags: 00060800  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80045a53d0       Image:         Ati2evxx.exe
        Wait Start TickCount      13619          Ticks: 32960 (0:00:08:34.179)
        Context Switch Count      13
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address Ati2evxx (0x000000000042fdd0)
        Stack Init fffff9800e2b3db0 Current fffff9800e2b37a0
        Base fffff9800e2b4000 Limit fffff9800e2ae000 Call 0
        Priority 12 BasePriority 10 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e2b37e0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e2b3920 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0e2b3980 fffff800`01e8e6ee nt!KeWaitForSingleObject+0x5f5
        fffff980`0e2b3a00 fffff800`01eab906 nt!IopXxxControlFile+0xe29
        fffff980`0e2b3b40 fffff800`01c4d733 nt!NtFsControlFile+0x56
        fffff980`0e2b3bb0 00000000`76e2060a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e2b3c20)
        00000000`025ffd88 00000000`76bc7330 ntdll!NtFsControlFile+0xa
        00000000`025ffd90 00000000`0042ff2b kernel32!ConnectNamedPipe+0x60
        00000000`025ffe00 00000000`000000d8 Ati2evxx+0x2ff2b
        00000000`025ffe08 00000000`0000017c 0xd8
        00000000`025ffe10 00000000`000000d8 0x17c
        00000000`025ffe18 00000000`024f5f90 0xd8
        00000000`025ffe20 00000000`00007a80 0x24f5f90
        00000000`025ffe28 00000000`00007a80 0x7a80
        00000000`025ffe30 00000000`00000fa0 0x7a80
        00000000`025ffe38 00000000`00000000 0xfa0
        00000000`025ffe40 65706970`5c2e5c5c 0x0
        00000000`025ffe48 6e657645`7478455c 0x65706970`5c2e5c5c
        00000000`025ffe50 31735f65`70695074 0x6e657645`7478455c
        00000000`025ffe58 00000000`00000000 0x31735f65`70695074
        00000000`025ffe60 00000000`00000000 0x0
        00000000`025ffe68 00000000`00000000 0x0
        00000000`025ffe70 00000000`00000000 0x0
        00000000`025ffe78 00000000`00000000 0x0
        00000000`025ffe80 00000000`00000000 0x0
        00000000`025ffe88 00000000`00000000 0x0
        00000000`025ffe90 00000000`00000000 0x0
        00000000`025ffe98 00000000`00000000 0x0
        00000000`025ffea0 00000000`00000000 0x0
        00000000`025ffea8 00000000`00000000 0x0
        00000000`025ffeb0 00000000`00000000 0x0
        00000000`025ffeb8 00000000`00000000 0x0
        00000000`025ffec0 00000000`00000000 0x0
        00000000`025ffec8 00000000`00000000 0x0
        00000000`025ffed0 00000000`00000000 0x0
        00000000`025ffed8 00000000`00000000 0x0
        00000000`025ffee0 00000000`00000000 0x0
        00000000`025ffee8 00000000`00000000 0x0
        00000000`025ffef0 00000000`00000000 0x0
        00000000`025ffef8 00000000`00000000 0x0
```

```
        THREAD fffffa80045f1bb0  Cid 0528.0570  Teb: 000007fffffd8000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80045b0220  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80045a53d0       Image:         Ati2evxx.exe
        Wait Start TickCount      2961           Ticks: 43618 (0:00:11:20.445)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address Ati2evxx (0x000000000042f240)
        Stack Init fffff9800e2badb0 Current fffff9800e2ba960
        Base fffff9800e2bb000 Limit fffff9800e2b5000 Call 0
        Priority 11 BasePriority 10 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e2ba9a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e2baae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0e2bab40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0e2babc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0e2bac20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e2bac20)
        00000000`0279f7e8 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`0279f7f0 00000000`0042f2b4 kernel32!WaitForSingleObjectEx+0x9c
        00000000`0279f8b0 00000000`000000cc Ati2evxx+0x2f2b4
        00000000`0279f8b8 00000000`0042f382 0xcc
        00000000`0279f8c0 00000000`00000000 Ati2evxx+0x2f382
        00000000`0279f8c8 00000000`000000cc 0x0
        00000000`0279f8d0 00000000`002f3e00 0xcc
        00000000`0279f8d8 000007fe`fdd42203 0x2f3e00
        00000000`0279f8e0 00000000`76e1c8ef msvcrt!core_crt_dll_init+0x228
        00000000`0279f910 00000000`76e1c5c0 ntdll!LdrpInitializeThread+0x265
        00000000`0279fa10 00000000`76e1c4f8 ntdll!LdrpInitialize+0xb0
        00000000`0279fab0 00000000`00000000 ntdll!LdrInitializeThunk+0x18
```

```
        THREAD fffffa80045e6910  Cid 0528.05a4  Teb: 000007fffffd6000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004609a90  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80045a53d0       Image:         Ati2evxx.exe
        Wait Start TickCount      13619          Ticks: 32960 (0:00:08:34.179)
        Context Switch Count      6
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ati2evxx_1fd0000 (0x0000000001fd3760)
        Stack Init fffff9800e2f9db0 Current fffff9800e2f9960
        Base fffff9800e2fa000 Limit fffff9800e2f4000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e2f99a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e2f9ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0e2f9b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0e2f9bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0e2f9c20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e2f9c20)
        00000000`02c2f728 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`02c2f730 00000000`01fd3792 kernel32!WaitForSingleObjectEx+0x9c
        00000000`02c2f7f0 00000000`00000144 ati2evxx_1fd0000+0x3792
        00000000`02c2f7f8 00000000`00000000 0x144
        00000000`02c2f800 00000000`00000000 0x0
        00000000`02c2f808 00000000`00000144 0x0
        00000000`02c2f810 ffffffff`fffffffe 0x144
        00000000`02c2f818 00000000`00000000 0xffffffff`fffffffe
        00000000`02c2f820 65706970`5c2e5c5c 0x0
        00000000`02c2f828 6e657645`7478455c 0x65706970`5c2e5c5c
        00000000`02c2f830 31735f65`70695074 0x6e657645`7478455c
        00000000`02c2f838 00000000`00000000 0x31735f65`70695074
        00000000`02c2f840 00000000`00000000 0x0
        00000000`02c2f848 00000000`00000000 0x0
        00000000`02c2f850 00000000`00000000 0x0
        00000000`02c2f858 00000000`00000000 0x0
        00000000`02c2f860 00000000`00000000 0x0
        00000000`02c2f868 00000000`00000000 0x0
        00000000`02c2f870 00000000`00000000 0x0
        00000000`02c2f878 00000000`00000000 0x0
        00000000`02c2f880 00000000`00000000 0x0
        00000000`02c2f888 00000000`00000000 0x0
        00000000`02c2f890 00000000`00000000 0x0
        00000000`02c2f898 00000000`00000000 0x0
        00000000`02c2f8a0 00000000`00000000 0x0
        00000000`02c2f8a8 00000000`00000000 0x0
        00000000`02c2f8b0 00000000`00000000 0x0
        00000000`02c2f8b8 00000000`00000000 0x0
        00000000`02c2f8c0 00000000`00000000 0x0
        00000000`02c2f8c8 00000000`00000000 0x0
        00000000`02c2f8d0 00000000`00000000 0x0
        00000000`02c2f8d8 00000000`00000000 0x0
        00000000`02c2f8e0 00000000`00000000 0x0
        00000000`02c2f8e8 00000000`00000000 0x0
        00000000`02c2f8f0 00000000`00000000 0x0
```

```
        THREAD fffffa80045e8530  Cid 0528.05ac  Teb: 000007fffffae000 Win32Thread: fffff900c20634d0
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa80045d4b50  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80045a53d0       Image:         Ati2evxx.exe
        Wait Start TickCount      4692           Ticks: 41887 (0:00:10:53.441)
        Context Switch Count      6                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff9800bbecdb0 Current fffff9800bbec810
        Base fffff9800bbed000 Limit fffff9800bbe6000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0bbec850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0bbec990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0bbec9f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0bbeca80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`0bbecb00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`0bbecbb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0bbecc20)
        00000000`02e2fd18 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`02e2fd20 000007fe`fedce7a3 kernel32!GetQueuedCompletionStatus+0x48
        00000000`02e2fd80 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`02e2fe10 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`02e2fec0 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`02e2fef0 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`02e2ff30 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`02e2ff60 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02e2ff90 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

Spoolsv process

```
PROCESS fffffa800461e270
    SessionId: 0  Cid: 05dc    Peb: 7fffffde000  ParentCid: 025c
    DirBase: 47899000  ObjectTable: fffff880057aa580  HandleCount: 339.
    Image: spoolsv.exe
    VadRoot fffffa80045f64f0 Vads 187 Clone 0 Private 1460. Modified 1079. Locked 0.
    DeviceMap fffff88000007820
    Token                             fffff88005ce4aa0
    ElapsedTime                       00:11:41.170
    UserTime                          00:00:00.031
    KernelTime                        00:00:00.093
    QuotaPoolUsage[PagedPool]         204608
    QuotaPoolUsage[NonPagedPool]      19072
    Working Set Sizes (now,min,max)  (2569, 50, 345) (10276KB, 200KB, 1380KB)
    PeakWorkingSetSize                3951
    VirtualSize                       120 Mb
    PeakVirtualSize                   125 Mb
    PageFaultCount                    5595
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      2236

    Setting context for this process...
.process /p /r fffffa800461e270

    !peb
PEB at 000007fffffde000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00000000ffb10000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00000000001b2740 . 0000000000278470
    Ldr.InLoadOrderModuleList:           00000000001b2650 . 0000000000278450
    Ldr.InMemoryOrderModuleList:         00000000001b2660 . 0000000000278460
            Base TimeStamp                     Module
        ffb10000 4549c865 Nov 02 10:28:53 2006 C:\Windows\System32\spoolsv.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        76bc0000 4549d328 Nov 02 11:14:48 2006 C:\Windows\system32\kernel32.dll
     7fefea30000 4549d267 Nov 02 11:11:35 2006 C:\Windows\system32\ADVAPI32.dll
     7fefed90000 469c43bb Jul 17 05:21:15 2007 C:\Windows\system32\RPCRT4.dll
     7fefdd40000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\system32\msvcrt.dll
     7fefcc20000 4549d32d Nov 02 11:14:53 2006 C:\Windows\System32\slc.dll
     7fefd390000 4549d33f Nov 02 11:15:11 2006 C:\Windows\System32\secur32.dll
     7fefca40000 4549d341 Nov 02 11:15:13 2006 C:\Windows\System32\credssp.dll
     7fefcc50000 4549d344 Nov 02 11:15:16 2006 C:\Windows\System32\CRYPT32.dll
        76d00000 45d3ee19 Feb 15 05:22:33 2007 C:\Windows\system32\USER32.dll
     7fefec20000 4549d273 Nov 02 11:11:47 2006 C:\Windows\system32\GDI32.dll
     7fefce00000 4549d2df Nov 02 11:13:35 2006 C:\Windows\System32\MSASN1.dll
     7fefd3b0000 4549d336 Nov 02 11:15:02 2006 C:\Windows\System32\USERENV.dll
     7fefd9e0000 4549d2cb Nov 02 11:13:15 2006 C:\Windows\system32\IMM32.DLL
     7fefdc30000 4549d2e6 Nov 02 11:13:42 2006 C:\Windows\system32\MSCTF.dll
     7feff0c0000 4549d2a1 Nov 02 11:12:33 2006 C:\Windows\system32\LPK.DLL
     7fefd940000 4549d337 Nov 02 11:15:03 2006 C:\Windows\system32\USP10.dll
     7fefc670000 4549d321 Nov 02 11:14:41 2006 C:\Windows\system32\schannel.dll
     7fefcf70000 4549d2fc Nov 02 11:14:04 2006 C:\Windows\System32\NETAPI32.dll
     7fefd530000 4549d310 Nov 02 11:14:24 2006 C:\Windows\system32\PSAPI.DLL
     7fefafa0000 4549d347 Nov 02 11:15:19 2006 C:\Windows\System32\SPOOLSS.DLL
     7fefc450000 4549d34e Nov 02 11:15:26 2006 C:\Windows\System32\WTSAPI32.dll
     7fefd1b0000 4549d380 Nov 02 11:16:16 2006 C:\Windows\System32\WINSTA.dll
     7fefcb80000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\System32\IPHLPAPI.DLL
     7fefcb30000 4549d263 Nov 02 11:11:31 2006 C:\Windows\System32\dhcpcsvc.DLL
     7fefce40000 4549d288 Nov 02 11:12:08 2006 C:\Windows\System32\DNSAPI.dll
     7fefd540000 4549d38a Nov 02 11:16:26 2006 C:\Windows\system32\WS2_32.dll
     7feff0b0000 4549d370 Nov 02 11:16:00 2006 C:\Windows\system32\NSI.dll
```

```
     7fefd280000 4549d370 Nov 02 11:16:00 2006 C:\Windows\System32\WINNSI.DLL
     7fefcb00000 4549d264 Nov 02 11:11:32 2006 C:\Windows\System32\dhcpcsvc6.DLL
     7fefc8f0000 4549d2e7 Nov 02 11:13:43 2006 C:\Windows\system32\mswsock.dll
     7fefaac0000 4549d317 Nov 02 11:14:31 2006 C:\Windows\System32\rasadhlp.dll
     7fefd760000 4549d317 Nov 02 11:14:31 2006 C:\Windows\system32\ole32.dll
     7fefdb90000 4549d282 Nov 02 11:12:02 2006 C:\Windows\system32\CLBCatQ.DLL
     7fefdab0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\OLEAUT32.dll
     7fefc1e0000 4549d381 Nov 02 11:16:17 2006 C:\Windows\System32\WINTRUST.dll
     7fefda90000 462443ee Apr 17 04:50:06 2007 C:\Windows\system32\imagehlp.dll
     7fef8580000 4549d299 Nov 02 11:12:25 2006 C:\Windows\System32\localspl.dll
     7fefca50000 4549d336 Nov 02 11:15:02 2006 C:\Windows\System32\VERSION.dll
     7fef9770000 4549d31c Nov 02 11:14:36 2006 C:\Windows\System32\sfc.dll
     7fefda10000 4549d31f Nov 02 11:14:39 2006 C:\Windows\system32\SHLWAPI.dll
     7fefddf0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\SHELL32.dll
     7fefeed0000 4549d318 Nov 02 11:14:32 2006 C:\Windows\system32\SETUPAPI.dll
     7fefbe70000 4549d32b Nov 02 11:14:51 2006 C:\Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_1559f1c6f365a7fa\comctl32.dll
     7fef8520000 4549d37c Nov 02 11:16:12 2006 C:\Windows\System32\winspool.drv
     7fef95f0000 4549d28a Nov 02 11:12:10 2006 C:\Windows\System32\FXSMON.DLL
        73e70000 4549aea9 Nov 02 08:39:05 2006 C:\Windows\System32\FXSRESM.DLL
     7fef8380000 4549d33c Nov 02 11:15:08 2006 C:\Windows\System32\tcpmon.dll
     7fef8130000 4549d333 Nov 02 11:14:59 2006 C:\Windows\System32\snmpapi.dll
     7fef8110000 4549d3ad Nov 02 11:17:01 2006 C:\Windows\System32\wsnmp32.dll
     7fef7d50000 4628a4b9 Apr 20 12:32:09 2007 C:\Windows\System32\msxml6.dll
     7fef80c0000 4549d33b Nov 02 11:15:07 2006 C:\Windows\System32\tcpmib.dll
     7fef8090000 4549d2b0 Nov 02 11:12:48 2006 C:\Windows\System32\mgmtapi.dll
     7fef8080000 4549d331 Nov 02 11:14:57 2006 C:\Windows\System32\usbmon.dll
     7fefc320000 4549d398 Nov 02 11:16:40 2006 C:\Windows\system32\wls0wndh.dll
     7fefc560000 4549d3a3 Nov 02 11:16:51 2006 C:\Windows\system32\wshtcpip.dll
     7fef8040000 4549d393 Nov 02 11:16:35 2006 C:\Windows\System32\WSDMon.dll
     7fefa450000 4549d391 Nov 02 11:16:33 2006 C:\Windows\System32\wsdapi.dll
     7fefa680000 4549d28c Nov 02 11:12:12 2006 C:\Windows\System32\HTTPAPI.dll
     7fefae90000 4549d36a Nov 02 11:15:54 2006 C:\Windows\System32\WINHTTP.dll
     7fefb930000 4549d350 Nov 02 11:15:28 2006 C:\Windows\System32\XmlLite.dll
     7fefa230000 4549d27a Nov 02 11:11:54 2006 C:\Windows\system32\FunDisc.dll
     7fefc180000 4549d253 Nov 02 11:11:15 2006 C:\Windows\system32\ATL.DLL
     7fef9c40000 46662887 Jun 06 04:22:47 2007 C:\Windows\System32\msxml3.dll
        74010000 45382208 Oct 20 02:10:32 2006 C:\Windows\system32\spool\PRTPROCS\x64\hpzpplhn.dll
     7fefc5b0000 4549d384 Nov 02 11:16:20 2006 C:\Windows\System32\NTMARTA.DLL
     7fefd590000 4549d396 Nov 02 11:16:38 2006 C:\Windows\system32\WLDAP32.dll
     7fefce20000 4549d315 Nov 02 11:14:29 2006 C:\Windows\System32\SAMLIB.dll
     7fef7820000 4549d35c Nov 02 11:15:40 2006 C:\Windows\System32\win32spl.dll
     7fef8030000 4549d30e Nov 02 11:14:22 2006 C:\Windows\System32\NETRAP.dll
     7fef8010000 4549d356 Nov 02 11:15:34 2006 C:\Windows\system32\printcom.dll
     7fef9760000 4549d343 Nov 02 11:15:15 2006 C:\Windows\system32\SensApi.dll
     7fefc940000 4549d277 Nov 02 11:11:51 2006 C:\Windows\System32\GPAPI.dll
     7fef7f30000 4549d2d0 Nov 02 11:13:20 2006 C:\Windows\System32\inetpp.dll
     7fefc980000 4549d39d Nov 02 11:16:45 2006 C:\Windows\System32\wship6.dll
     7fefaab0000 4549d371 Nov 02 11:16:01 2006 C:\Windows\System32\winrnr.dll
     7fefc1a0000 4549d314 Nov 02 11:14:28 2006 C:\Windows\system32\NLAapi.dll
     7fefaa70000 4549d2e4 Nov 02 11:13:40 2006 C:\Windows\system32\napinsp.dll
     7fefaa50000 4549d341 Nov 02 11:15:13 2006 C:\Windows\system32\pnrpnsp.dll
     7fefc620000 4549d31d Nov 02 11:14:37 2006 C:\Windows\System32\rsaenh.dll
     7fef7640000 4549d2da Nov 02 11:13:30 2006 C:\Windows\system32\spool\DRIVERS\x64\3\UNIDRVUI.DLL
    SubSystemData:     0000000000000000
    ProcessHeap:       00000000001b0000
    ProcessParameters: 00000000001b1d20
    WindowTitle:  'C:\Windows\System32\spoolsv.exe'
    ImageFile:    'C:\Windows\System32\spoolsv.exe'
    CommandLine:  'C:\Windows\System32\spoolsv.exe'
    DllPath:
'C:\Windows\System32;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Wind
ows;C:\Windows\System32\Wbem'
    Environment:  00000000001b1310
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\system32\config\systemprofile\AppData\Roaming
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\Windows\system32\cmd.exe
```

```
        FP_NO_HOST_CHECK=NO
        LOCALAPPDATA=C:\Windows\system32\config\systemprofile\AppData\Local
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\TEMP
        TMP=C:\Windows\TEMP
        USERDOMAIN=DOMAIN
        USERNAME=COMPUTERNAME$
        USERPROFILE=C:\Windows\system32\config\systemprofile
        windir=C:\Windows


        THREAD fffffa80045f9bb0  Cid 05dc.05e0  Teb: 000007fffffdc000 Win32Thread: 0000000000000000
WAIT: (Executive) UserMode Non-Alertable
            fffffa80045f80e8  NotificationEvent
        IRP List:
            fffffa8004609010: (0006,0118) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800461e270       Image:         spoolsv.exe
        Wait Start TickCount      2775           Ticks: 43804 (0:00:11:23.346)
        Context Switch Count      53
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address spoolsv!mainCRTStartup (0x00000000ffb12d50)
        Stack Init fffff9800e4c1db0 Current fffff9800e4c17f0
        Base fffff9800e4c2000 Limit fffff9800e4bc000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e4c1830 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e4c1970 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0e4c19d0 fffff800`01ebdf16 nt!KeWaitForSingleObject+0x5f5
        fffff980`0e4c1a50 fffff800`01ea1a24 nt!IopSynchronousServiceTail+0x306
        fffff980`0e4c1ac0 fffff800`01c4d733 nt!NtReadFile+0x583
        fffff980`0e4c1bb0 00000000`76e202da nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e4c1c20)
        00000000`0016f3d8 00000000`76bf26da ntdll!NtReadFile+0xa
        00000000`0016f3e0 000007fe`fea865aa kernel32!ReadFile+0x8a
        00000000`0016f470 000007fe`fea862e3 ADVAPI32!ScGetPipeInput+0x4a
        00000000`0016f550 000007fe`fea850f3 ADVAPI32!ScDispatcherLoop+0x9a
        00000000`0016f650 00000000`ffb123a3 ADVAPI32!StartServiceCtrlDispatcherW+0x176
        00000000`0016f8f0 00000000`ffb12e66 spoolsv!main+0x23
        00000000`0016f920 00000000`76bfcdcd
spoolsv!ConvertStringSecurityDescriptorToSecurityDescriptorW+0x19b
        00000000`0016f960 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0016f990 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80045438a0  Cid 05dc.05e4  Teb: 000007fffffda000 Win32Thread: fffff900c07df010
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80045f99f0  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800461e270       Image:         spoolsv.exe
        Wait Start TickCount      1681           Ticks: 44898 (0:00:11:40.413)
        Context Switch Count      46                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address ADVAPI32!ScSvcctrlThreadW (0x000007fefea84bd0)
        Stack Init fffff9800e5b3db0 Current fffff9800e5b3960
        Base fffff9800e5b4000 Limit fffff9800e5ad000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e5b39a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e5b3ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0e5b3b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0e5b3bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0e5b3c20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e5b3c20)
        00000000`008af798 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`008af7a0 00000000`ffb1307f kernel32!WaitForSingleObjectEx+0x9c
        00000000`008af860 000007fe`fea84bf5 spoolsv!SPOOLER_main+0x80
        00000000`008af890 00000000`76bfcdcd ADVAPI32!ScSvcctrlThreadW+0x25
        00000000`008af8c0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`008af8f0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004602060  Cid 05dc.05e8  Teb: 000007fffffd8000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa800461e120  SynchronizationTimer
            fffffa80045f6620  SynchronizationEvent
            fffffa800409da40  SynchronizationEvent
            fffffa8004b70500  SynchronizationEvent
            fffffa8004ba9ce0  SynchronizationEvent
            fffffa8004b1f9f0  SynchronizationEvent
            fffffa8004baddc0  SynchronizationTimer
            fffffa8004c01040  SynchronizationEvent
            fffffa80046b6940  SynchronizationEvent
            fffffa8004782320  SynchronizationEvent
            fffffa80045dfab0  SynchronizationEvent
            fffffa8004c00d00  SynchronizationEvent
            fffffa8004c00190  SynchronizationEvent
            fffffa8004bdb940  SynchronizationEvent
            fffffa8004b711e0  SynchronizationEvent
            fffffa8004bbcfe0  SynchronizationEvent
            fffffa8004bc3a60  SynchronizationEvent
            fffffa8004b4d040  SynchronizationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800461e270       Image:         spoolsv.exe
        Wait Start TickCount      41371          Ticks: 5208 (0:00:01:21.245)
        Context Switch Count      82
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x0000000076df6930)
        Stack Init fffff9800e323db0 Current fffff9800e323260
        Base fffff9800e324000 Limit fffff9800e31e000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e3232a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e3233e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0e323440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0e3234b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0e323960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0e323bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e323c20)
        00000000`0082f8a8 00000000`76df6b07 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0082f8b0 00000000`76bfcdcd ntdll!TppWaiterpThread+0x14d
        00000000`0082fb50 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0082fb80 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80046225d0  Cid 05dc.05f0  Teb: 000007fffffd4000 Win32Thread: fffff900c07f7d60
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800450c280  SynchronizationEvent
            fffffa8004b76120  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800461e270       Image:         spoolsv.exe
        Wait Start TickCount      2941           Ticks: 43638 (0:00:11:20.757)
        Context Switch Count      4388                 LargeStack
        UserTime                  00:00:00.078
        KernelTime                00:00:00.358
        Win32 Start Address spoolsv!PreInitializeRouter (0x00000000ffb121f0)
        Stack Init fffff98010665db0 Current fffff98010665260
        Base fffff98010666000 Limit fffff9801065d000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`106652a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`106653e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`10665440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`106654b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`10665960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`10665bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`10665c20)
        00000000`0086f348 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0086f350 00000000`76d1e96d kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0086f460 00000000`76d1e85e USER32!RealMsgWaitForMultipleObjectsEx+0x129
        00000000`0086f500 00000000`76d13680 USER32!MsgWaitForMultipleObjectsEx+0x46
        00000000`0086f540 000007fe`fafab8f6 USER32!MsgWaitForMultipleObjects+0x20
        00000000`0086f580 000007fe`fafa821b SPOOLSS!HandlePollNotifications+0x46
        00000000`0086f600 00000000`ffb1223e SPOOLSS!InitializeRouter+0x623
        00000000`0086f7d0 00000000`76bfcdcd spoolsv!PreInitializeRouter+0x4e
        00000000`0086f800 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0086f830 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004b992c0  Cid 05dc.0ab0  Teb: 000007fffffac000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004bca5c0  NotificationEvent
            fffffa8004b99378  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800461e270       Image:         spoolsv.exe
        Wait Start TickCount      46567          Ticks: 12 (0:00:00:00.187)
        Context Switch Count      714
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address msvcrt!endthreadex (0x000007fefdd59620)
        Stack Init fffff98012b96db0 Current fffff98012b96960
        Base fffff98012b97000 Limit fffff98012b91000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`12b969a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12b96ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`12b96b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`12b96bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`12b96c20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12b96c20)
        00000000`021bf9a8 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`021bf9b0 000007fe`f81186e7 kernel32!WaitForSingleObjectEx+0x9c
        00000000`021bfa70 000007fe`fdd594e7 wsnmp32!thrTimer+0x2a3
        00000000`021bfac0 000007fe`fdd5967d msvcrt!endthreadex+0x47
        00000000`021bfaf0 00000000`76bfcdcd msvcrt!endthreadex+0x100
        00000000`021bfb20 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`021bfb50 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800409c060  Cid 05dc.0ab4  Teb: 000007fffffaa000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004784710  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800461e270       Image:         spoolsv.exe
        Wait Start TickCount      41360          Ticks: 5219 (0:00:01:21.416)
        Context Switch Count      16
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address msvcrt!endthreadex (0x000007fefdd59620)
        Stack Init fffff98012bb9db0 Current fffff98012bb9960
        Base fffff98012bba000 Limit fffff98012bb4000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`12bb99a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12bb9ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`12bb9b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`12bb9bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`12bb9c20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12bb9c20)
        00000000`008ef6a8 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`008ef6b0 000007fe`f8118084 kernel32!WaitForSingleObjectEx+0x9c
        00000000`008ef770 000007fe`fdd594e7 wsnmp32!thrNotify+0x9c
        00000000`008ef7d0 000007fe`fdd5967d msvcrt!endthreadex+0x47
        00000000`008ef800 00000000`76bfcdcd msvcrt!endthreadex+0x100
        00000000`008ef830 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`008ef860 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004bd5060  Cid 05dc.0ab8  Teb: 000007fffffa8000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004784580  SynchronizationEvent
            fffffa8004ba41d0  SynchronizationEvent
            fffffa8004ba4170  NotificationEvent
            fffffa8004bd5118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800461e270       Image:         spoolsv.exe
        Wait Start TickCount      41354          Ticks: 5225 (0:00:01:21.510)
        Context Switch Count      9
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address tcpmon!TBidiServer::PollingThread (0x000007fef8381b10)
        Stack Init fffff9801076cdb0 Current fffff9801076c260
        Base fffff9801076d000 Limit fffff98010767000 Call 0
        Priority 7 BasePriority 6 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1076c2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1076c3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`1076c440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`1076c4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`1076c960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`1076cbb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1076cc20)
        00000000`02c3fb38 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`02c3fb40 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`02c3fc50 000007fe`f8381c3c kernel32!WaitForMultipleObjects+0x11
        00000000`02c3fc90 00000000`76bfcdcd tcpmon!TBidiServer::PollingThread+0x11b
        00000000`02c3fcf0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02c3fd20 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004bce9d0  Cid 05dc.0ad0  Teb: 000007fffffa6000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004be1f10  SynchronizationEvent
            fffffa8004bcea88  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800461e270       Image:         spoolsv.exe
        Wait Start TickCount      45225          Ticks: 1354 (0:00:00:21.122)
        Context Switch Count      32
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address tcpmon!CDeviceStatus::StatusThread (0x000007fef83816a0)
        Stack Init fffff98012bffdb0 Current fffff98012bff960
        Base fffff98012c00000 Limit fffff98012bfa000 Call 0
        Priority 10 BasePriority 6 PriorityDecrement 3 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`12bff9a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12bffae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`12bffb40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`12bffbc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`12bffc20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12bffc20)
        00000000`02d1fd78 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`02d1fd80 000007fe`f8381707 kernel32!WaitForSingleObjectEx+0x9c
        00000000`02d1fe40 00000000`76bfcdcd tcpmon!CDeviceStatus::StatusThread+0x161
        00000000`02d1fe90 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02d1fec0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004bd6270  Cid 05dc.0adc  Teb: 000007fffffa4000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80048e8dc0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800461e270       Image:         spoolsv.exe
        Wait Start TickCount      45226          Ticks: 1353 (0:00:00:21.106)
        Context Switch Count      49
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address msvcrt!endthreadex (0x000007fefdd59620)
        Stack Init fffff98012be3db0 Current fffff98012be3960
        Base fffff98012be4000 Limit fffff98012bde000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`12be39a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12be3ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`12be3b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`12be3bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`12be3c20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12be3c20)
        00000000`0077f768 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`0077f770 000007fe`f8118084 kernel32!WaitForSingleObjectEx+0x9c
        00000000`0077f830 000007fe`fdd594e7 wsnmp32!thrNotify+0x9c
        00000000`0077f890 000007fe`fdd5967d msvcrt!endthreadex+0x47
        00000000`0077f8c0 00000000`76bfcdcd msvcrt!endthreadex+0x100
        00000000`0077f8f0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0077f920 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004c32300  Cid 05dc.0ae8  Teb: 000007fffffa0000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004bfd450  SynchronizationEvent
            fffffa8004bfd3f0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800461e270       Image:         spoolsv.exe
        Wait Start TickCount      2901           Ticks: 43678 (0:00:11:21.381)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address usbmon!UpdateThread (0x000007fef80819e0)
        Stack Init fffff98012beadb0 Current fffff98012bea260
        Base fffff98012beb000 Limit fffff98012be5000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`12bea2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12bea3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`12bea440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`12bea4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`12bea960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`12beabb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12beac20)
        00000000`0349fb18 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0349fb20 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0349fc30 000007fe`f8081a56 kernel32!WaitForMultipleObjects+0x11
        00000000`0349fc70 00000000`76bfcdcd usbmon!UpdateThread+0x86
        00000000`0349fcf0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0349fd20 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004bd7530  Cid 05dc.0aec  Teb: 000007fffff9e000 Win32Thread: fffff900c07f3940
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa8004bd3bb0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800461e270       Image:         spoolsv.exe
        Wait Start TickCount      2941           Ticks: 43638 (0:00:11:20.757)
        Context Switch Count      25                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address usbmon!CPNPNotifications::WindowMessageThread (0x000007fef80822d0)
        Stack Init fffff98012a72db0 Current fffff98012a72740
        Base fffff98012a73000 Limit fffff98012a69000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`12a72780 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12a728c0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`12a72920 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`12a729a0 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`12a72a40 fffff960`000c7e1e win32k!xxxSleepThread+0x56
        fffff980`12a72a70 fffff960`000c7f25 win32k!xxxRealInternalGetMessage+0x72e
        fffff980`12a72b50 fffff960`000c97e4 win32k!xxxInternalGetMessage+0x35
        fffff980`12a72b90 fffff800`01c4d733 win32k!NtUserGetMessage+0x64
        fffff980`12a72c20 00000000`76d1e6aa nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12a72c20)
        00000000`02e9f958 00000000`76d1e6ea USER32!ZwUserGetMessage+0xa
        00000000`02e9f960 000007fe`f80823f0 USER32!GetMessageW+0x34
        00000000`02e9f990 00000000`76bfcdcd usbmon!CPNPNotifications::WindowMessageThread+0x1a0
        00000000`02e9fa60 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02e9fa90 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004bdbbb0  Cid 05dc.0af4  Teb: 000007fffff9a000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004c21cf0  NotificationEvent
            fffffa8004bca5c0  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800461e270       Image:         spoolsv.exe
        Wait Start TickCount      45226          Ticks: 1353 (0:00:00:21.106)
        Context Switch Count      34
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address msvcrt!endthreadex (0x000007fefdd59620)
        Stack Init fffff9801075edb0 Current fffff9801075e260
        Base fffff9801075f000 Limit fffff98010759000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1075e2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1075e3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`1075e440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`1075e4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`1075e960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`1075ebb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1075ec20)
        00000000`02f7fc08 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`02f7fc10 000007fe`fd54ca72 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`02f7fd20 000007fe`f8118400 WS2_32!WSAWaitForMultipleEvents+0x12
        00000000`02f7fd60 000007fe`fdd594e7 wsnmp32!thrManager+0x1a4
        00000000`02f7fe80 000007fe`fdd5967d msvcrt!endthreadex+0x47
        00000000`02f7feb0 00000000`76bfcdcd msvcrt!endthreadex+0x100
        00000000`02f7fee0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02f7ff10 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004bfcbb0  Cid 05dc.0b04  Teb: 000007fffff98000 Win32Thread: fffff900c07d8d60
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa8004bfcad0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800461e270       Image:         spoolsv.exe
        Wait Start TickCount      2941           Ticks: 43638 (0:00:11:20.757)
        Context Switch Count      16                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address WSDMon!Ncd::TPower::WindowMessageThread (0x000007fef8050c54)
        Stack Init fffff98012a98db0 Current fffff98012a98740
        Base fffff98012a99000 Limit fffff98012a91000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`12a98780 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12a988c0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`12a98920 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`12a989a0 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`12a98a40 fffff960`000c7e1e win32k!xxxSleepThread+0x56
        fffff980`12a98a70 fffff960`000c7f25 win32k!xxxRealInternalGetMessage+0x72e
        fffff980`12a98b50 fffff960`000c97e4 win32k!xxxInternalGetMessage+0x35
        fffff980`12a98b90 fffff800`01c4d733 win32k!NtUserGetMessage+0x64
        fffff980`12a98c20 00000000`76d1e6aa nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12a98c20)
        00000000`0399fc68 00000000`76d1e6ea USER32!ZwUserGetMessage+0xa
        00000000`0399fc70 000007fe`f8050d3a USER32!GetMessageW+0x34
        00000000`0399fca0 00000000`76bfcdcd WSDMon!Ncd::TPower::WindowMessageThread+0xe6
        00000000`0399fd40 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0399fd70 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800409ebb0  Cid 05dc.0b08  Teb: 000007fffff96000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80043978e0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800461e270       Image:         spoolsv.exe
        Wait Start TickCount      2909           Ticks: 43670 (0:00:11:21.256)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address FunDisc!CNotificationQueue::ThreadProc (0x000007fefa23ace4)
        Stack Init fffff98012bf8db0 Current fffff98012bf8960
        Base fffff98012bf9000 Limit fffff98012bf3000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`12bf89a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12bf8ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`12bf8b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`12bf8bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`12bf8c20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12bf8c20)
        00000000`035bfac8 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`035bfad0 000007fe`fa23afd0 kernel32!WaitForSingleObjectEx+0x9c
        00000000`035bfb90 00000000`76bfcdcd FunDisc!CNotificationQueue::ThreadProc+0x2ec
        00000000`035bfbf0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`035bfc20 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004b43700  Cid 05dc.0b0c  Teb: 000007fffff94000 Win32Thread: fffff900c2000ab0
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004b8ff10  SynchronizationEvent
            fffffa8004badd10  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800461e270       Image:         spoolsv.exe
        Wait Start TickCount      2910           Ticks: 43669 (0:00:11:21.240)
        Context Switch Count      4                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address FunDisc!ListenerThread (0x000007fefa23b464)
        Stack Init fffff98012abedb0 Current fffff98012abe260
        Base fffff98012abf000 Limit fffff98012ab7000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`12abe2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12abe3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`12abe440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`12abe4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`12abe960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`12abebb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12abec20)
        00000000`038cf808 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`038cf810 00000000`76d1e96d kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`038cf920 00000000`76d1e85e USER32!RealMsgWaitForMultipleObjectsEx+0x129
        00000000`038cf9c0 00000000`76d13680 USER32!MsgWaitForMultipleObjectsEx+0x46
        00000000`038cfa00 000007fe`fa23b60a USER32!MsgWaitForMultipleObjects+0x20
        00000000`038cfa40 00000000`76bfcdcd FunDisc!ListenerThread+0x1a6
        00000000`038cfb30 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`038cfb60 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004b46630  Cid 05dc.0b10  Teb: 000007fffff92000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa80048ee740  SynchronizationEvent
            fffffa8004b90150  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800461e270       Image:         spoolsv.exe
        Wait Start TickCount      2910           Ticks: 43669 (0:00:11:21.240)
        Context Switch Count      7
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address FunDisc!CRegProvider::ThreadProc (0x000007fefa2443d8)
        Stack Init fffff98012bcedb0 Current fffff98012bce260
        Base fffff98012bcf000 Limit fffff98012bc9000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`12bce2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12bce3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`12bce440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`12bce4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`12bce960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`12bcebb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12bcec20)
        00000000`035ff6f8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`035ff700 000007fe`fa24628f kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`035ff810 00000000`76bfcdcd FunDisc!CRegProvider::MemberThreadProc+0x16f
        00000000`035ffcd0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`035ffd00 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004be3bb0  Cid 05dc.0b18  Teb: 000007fffff8e000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8003fa6f10  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800461e270       Image:         spoolsv.exe
        Wait Start TickCount      2939           Ticks: 43640 (0:00:11:20.788)
        Context Switch Count      7
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address localspl!SchedulerThread (0x000007fef858b660)
        Stack Init fffff98012f96db0 Current fffff98012f96960
        Base fffff98012f97000 Limit fffff98012f91000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`12f969a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12f96ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`12f96b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`12f96bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`12f96c20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12f96c20)
        00000000`03bffa18 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`03bffa20 000007fe`f858b77f kernel32!WaitForSingleObjectEx+0x9c
        00000000`03bffae0 00000000`76bfcdcd localspl!SchedulerThread+0x180
        00000000`03bffb90 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`03bffbc0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80020eabb0  Cid 05dc.0b30  Teb: 000007fffffd6000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa800461e7d0  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800461e270       Image:         spoolsv.exe
        Wait Start TickCount      28009          Ticks: 18570 (0:00:04:49.693)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff98020ccfdb0 Current fffff98020ccf810
        Base fffff98020cd0000 Limit fffff98020cca000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`20ccf850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`20ccf990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`20ccf9f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`20ccfa80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`20ccfb00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`20ccfbb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`20ccfc20)
        00000000`02fcfc18 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`02fcfc20 000007fe`fedce7a3 kernel32!GetQueuedCompletionStatus+0x48
        00000000`02fcfc80 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`02fcfd10 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`02fcfdc0 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`02fcfdf0 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`02fcfe30 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`02fcfe60 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02fcfe90 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

Svchost process (LocalServiceNoNetwork)

```
PROCESS fffffa8004622180
    SessionId: 0  Cid: 05f4    Peb: 7fffffde000  ParentCid: 025c
    DirBase: 471a0000  ObjectTable: fffff88005885850  HandleCount: 275.
    Image: svchost.exe
    VadRoot fffffa80046200b0 Vads 162 Clone 0 Private 2958. Modified 2611. Locked 0.
    DeviceMap fffff88005a30830
    Token                             fffff88005dd38d0
    ElapsedTime                       00:11:41.146
    UserTime                          00:00:00.171
    KernelTime                        00:00:00.171
    QuotaPoolUsage[PagedPool]         141696
    QuotaPoolUsage[NonPagedPool]      32784
    Working Set Sizes (now,min,max)  (2597, 50, 345) (10388KB, 200KB, 1380KB)
    PeakWorkingSetSize                16375
    VirtualSize                       103 Mb
    PeakVirtualSize                   158 Mb
    PageFaultCount                    37999
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      3712

    Setting context for this process...
.process /p /r fffffa8004622180

    !peb
PEB at 000007fffffde000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00000000ff910000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00000000003c27e0 . 00000000026e6770
    Ldr.InLoadOrderModuleList:           00000000003c26f0 . 00000000026e6750
    Ldr.InMemoryOrderModuleList:         00000000003c2700 . 00000000026e6760
            Base TimeStamp                     Module
        ff910000 4549b5f5 Nov 02 09:10:13 2006 C:\Windows\system32\svchost.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        76bc0000 4549d328 Nov 02 11:14:48 2006 C:\Windows\system32\kernel32.dll
     7fefdd40000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\system32\msvcrt.dll
     7fefea30000 4549d267 Nov 02 11:11:35 2006 C:\Windows\system32\ADVAPI32.dll
     7fefed90000 469c43bb Jul 17 05:21:15 2007 C:\Windows\system32\RPCRT4.dll
     7fefad20000 4549d255 Nov 02 11:11:17 2006 c:\windows\system32\bfe.dll
     7fefd360000 4549d265 Nov 02 11:11:33 2006 c:\windows\system32\AUTHZ.dll
     7fefd390000 4549d33f Nov 02 11:15:11 2006 c:\windows\system32\Secur32.dll
        76d00000 45d3ee19 Feb 15 05:22:33 2007 C:\Windows\system32\USER32.dll
     7fefec20000 4549d273 Nov 02 11:11:47 2006 C:\Windows\system32\GDI32.dll
     7fefd9e0000 4549d2cb Nov 02 11:13:15 2006 C:\Windows\system32\IMM32.DLL
     7fefdc30000 4549d2e6 Nov 02 11:13:42 2006 C:\Windows\system32\MSCTF.dll
     7feff0c0000 4549d2a1 Nov 02 11:12:33 2006 C:\Windows\system32\LPK.DLL
     7fefd940000 4549d337 Nov 02 11:15:03 2006 C:\Windows\system32\USP10.dll
     7fefab20000 46678630 Jun 07 05:14:40 2007 c:\windows\system32\mpssvc.dll
     7fefc460000 466785ee Jun 07 05:13:34 2007 c:\windows\system32\FirewallAPI.dll
     7fefdab0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\OLEAUT32.dll
     7fefd760000 4549d317 Nov 02 11:14:31 2006 C:\Windows\system32\ole32.dll
     7fefca50000 4549d336 Nov 02 11:15:02 2006 c:\windows\system32\VERSION.dll
     7fefc1a0000 4549d314 Nov 02 11:14:28 2006 c:\windows\system32\nlaapi.dll
     7fefcb80000 4549d2e1 Nov 02 11:13:37 2006 c:\windows\system32\IPHLPAPI.DLL
     7fefcb30000 4549d263 Nov 02 11:11:31 2006 c:\windows\system32\dhcpcsvc.DLL
     7fefce40000 4549d288 Nov 02 11:12:08 2006 c:\windows\system32\DNSAPI.dll
     7fefd540000 4549d38a Nov 02 11:16:26 2006 C:\Windows\system32\WS2_32.dll
     7feff0b0000 4549d370 Nov 02 11:16:00 2006 C:\Windows\system32\NSI.dll
     7fefd280000 4549d370 Nov 02 11:16:00 2006 c:\windows\system32\WINNSI.DLL
     7fefcb00000 4549d264 Nov 02 11:11:32 2006 c:\windows\system32\dhcpcsvc6.DLL
     7fefcc50000 4549d344 Nov 02 11:15:16 2006 c:\windows\system32\CRYPT32.dll
```

```
     7fefce00000 4549d2df Nov 02 11:13:35 2006 c:\windows\system32\MSASN1.dll
     7fefd3b0000 4549d336 Nov 02 11:15:02 2006 c:\windows\system32\USERENV.dll
     7fefca60000 4549d252 Nov 02 11:11:14 2006 c:\windows\system32\bcrypt.dll
     7fefc450000 4549d34e Nov 02 11:15:26 2006 c:\windows\system32\WTSAPI32.dll
     7fefda10000 4549d31f Nov 02 11:14:39 2006 C:\Windows\system32\SHLWAPI.dll
     7fefac60000 4549d280 Nov 02 11:12:00 2006 c:\windows\system32\fwpuclnt.dll
     7fefbe70000 4549d32b Nov 02 11:14:51 2006 C:\Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_1559f1c6f365a7fa\comctl32.dll
     7fefca40000 4549d341 Nov 02 11:15:13 2006 C:\Windows\system32\credssp.dll
     7fefc670000 4549d321 Nov 02 11:14:41 2006 C:\Windows\system32\schannel.dll
     7fefcf70000 4549d2fc Nov 02 11:14:04 2006 C:\Windows\system32\NETAPI32.dll
     7fefd530000 4549d310 Nov 02 11:14:24 2006 C:\Windows\system32\PSAPI.DLL
     7fefc940000 4549d277 Nov 02 11:11:51 2006 C:\Windows\system32\GPAPI.dll
     7fefcc20000 4549d32d Nov 02 11:14:53 2006 C:\Windows\system32\slc.dll
     7fefadd0000 46678689 Jun 07 05:16:09 2007 C:\Windows\system32\wfapigp.dll
     7fefa7a0000 4549d29f Nov 02 11:12:31 2006 c:\windows\system32\dps.dll
     7fefa700000 4549d334 Nov 02 11:15:00 2006 c:\windows\system32\wdi.dll
     7fefdb90000 4549d282 Nov 02 11:12:02 2006 C:\Windows\system32\CLBCatQ.DLL
     7fefa360000 4549d335 Nov 02 11:15:01 2006 C:\Windows\system32\taskschd.dll
     7fefb930000 4549d350 Nov 02 11:15:28 2006 C:\Windows\system32\XmlLite.dll
     7fefc8f0000 4549d2e7 Nov 02 11:13:43 2006 C:\Windows\system32\mswsock.dll
     7fefc560000 4549d3a3 Nov 02 11:16:51 2006 C:\Windows\system32\wshtcpip.dll
     7fefc980000 4549d39d Nov 02 11:16:45 2006 C:\Windows\System32\wship6.dll
     7fefc620000 4549d31d Nov 02 11:14:37 2006 C:\Windows\system32\rsaenh.dll
     7fefa1f0000 4549d36c Nov 02 11:15:56 2006 C:\Windows\System32\npmproxy.dll
     7fef4090000 4549d26e Nov 02 11:11:42 2006 C:\Windows\system32\diagperf.dll
     7fefddf0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\SHELL32.dll
     7fef75b0000 4549d33d Nov 02 11:15:09 2006 C:\Windows\system32\pnpts.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       00000000003c0000
    ProcessParameters: 00000000003c1db0
    WindowTitle:  'C:\Windows\system32\svchost.exe'
    ImageFile:    'C:\Windows\system32\svchost.exe'
    CommandLine:  'C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork'
    DllPath:
'C:\Windows\system32;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Wind
ows;C:\Windows\System32\Wbem'
    Environment:  00000000003c1310
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\ServiceProfiles\LocalService\AppData\Roaming
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        LOCALAPPDATA=C:\Windows\ServiceProfiles\LocalService\AppData\Local
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public

        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\SERVIC~2\LOCALS~1\AppData\Local\Temp
        TMP=C:\Windows\SERVIC~2\LOCALS~1\AppData\Local\Temp
        USERDOMAIN=NT AUTHORITY
        USERNAME=LOCAL SERVICE
        USERPROFILE=C:\Windows\ServiceProfiles\LocalService

        windir=C:\Windows
```

```
        THREAD fffffa8004620750  Cid 05f4.05f8  Teb: 000007fffffdc000 Win32Thread: 0000000000000000
WAIT: (Executive) UserMode Non-Alertable
            fffffa8004620f48  NotificationEvent
        IRP List:
            fffffa80045d4ee0: (0006,0118) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa8004622180       Image:         svchost.exe
        Wait Start TickCount      1851           Ticks: 44728 (0:00:11:37.761)
        Context Switch Count      24
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address svchost!wmainCRTStartup (0x00000000ff912550)
        Stack Init fffff9800e2dddb0 Current fffff9800e2dd7f0
        Base fffff9800e2de000 Limit fffff9800e2d8000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e2dd830 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e2dd970 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0e2dd9d0 fffff800`01ebdf16 nt!KeWaitForSingleObject+0x5f5
        fffff980`0e2dda50 fffff800`01ea1a24 nt!IopSynchronousServiceTail+0x306
        fffff980`0e2ddac0 fffff800`01c4d733 nt!NtReadFile+0x583
        fffff980`0e2ddbb0 00000000`76e202da nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e2ddc20)
        00000000`0020f408 00000000`76bf26da ntdll!NtReadFile+0xa
        00000000`0020f410 000007fe`fea865aa kernel32!ReadFile+0x8a
        00000000`0020f4a0 000007fe`fea862e3 ADVAPI32!ScGetPipeInput+0x4a
        00000000`0020f580 000007fe`fea850f3 ADVAPI32!ScDispatcherLoop+0x9a
        00000000`0020f680 00000000`ff91283c ADVAPI32!StartServiceCtrlDispatcherW+0x176
        00000000`0020f920 00000000`ff912666 svchost!wmain+0xe5
        00000000`0020f950 00000000`76bfcdcd svchost!ScCreateWellKnownSids+0x301
        00000000`0020f990 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0020f9c0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800450c360  Cid 05f4.0600  Teb: 000007fffffd8000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa800450def0  SynchronizationTimer
            fffffa800461fc40  SynchronizationTimer
            fffffa80045ba9f0  SynchronizationEvent
            fffffa800459e290  SynchronizationEvent
            fffffa800461f740  SynchronizationEvent
            fffffa800465a250  SynchronizationEvent
            fffffa80046617e0  SynchronizationEvent
            fffffa80044e0ef0  SynchronizationEvent
            fffffa8004655380  SynchronizationEvent
            fffffa800468f540  SynchronizationEvent
            fffffa80047810b0  SynchronizationEvent
            fffffa80048520c0  SynchronizationTimer
            fffffa8004855710  SynchronizationTimer
            fffffa800467bad0  SynchronizationEvent
            fffffa8004829690  SynchronizationEvent
            fffffa800468afe0  SynchronizationEvent
            fffffa800468a9e0  SynchronizationEvent
            fffffa8004624930  SynchronizationTimer
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa8004622180       Image:         svchost.exe
        Wait Start TickCount      13211          Ticks: 33368 (0:00:08:40.544)
        Context Switch Count      50
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x0000000076df6930)
        Stack Init fffff9800e31cdb0 Current fffff9800e31c260
        Base fffff9800e31d000 Limit fffff9800e317000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e31c2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e31c3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0e31c440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0e31c4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0e31c960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0e31cbb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e31cc20)
        00000000`0095f908 00000000`76df6b07 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0095f910 00000000`76bfcdcd ntdll!TppWaiterpThread+0x14d
        00000000`0095fbb0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0095fbe0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004633bb0  Cid 05f4.0604  Teb: 000007fffffd6000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004631820  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa8004622180       Image:         svchost.exe
        Wait Start TickCount      1684           Ticks: 44895 (0:00:11:40.366)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address AUTHZ!AuthzpDeQueueThreadWorker (0x000007fefd364660)
        Stack Init fffff9800e2e4db0 Current fffff9800e2e4960
        Base fffff9800e2e5000 Limit fffff9800e2df000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e2e49a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e2e4ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0e2e4b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0e2e4bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0e2e4c20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e2e4c20)
        00000000`0135fb88 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`0135fb90 000007fe`fd364689 kernel32!WaitForSingleObjectEx+0x9c
        00000000`0135fc50 00000000`76bfcdcd AUTHZ!AuthzpDeQueueThreadWorker+0x29
        00000000`0135fc80 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0135fcb0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004677060  Cid 05f4.0610  Teb: 000007fffffac000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800467c490  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa8004622180       Image:         svchost.exe
        Wait Start TickCount      1688           Ticks: 44891 (0:00:11:40.304)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address AUTHZ!AuthzpDeQueueThreadWorker (0x000007fefd364660)
        Stack Init fffff9800e47bdb0 Current fffff9800e47b960
        Base fffff9800e47c000 Limit fffff9800e476000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e47b9a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e47bae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0e47bb40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0e47bbc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0e47bc20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e47bc20)
        00000000`01fff908 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`01fff910 000007fe`fd364689 kernel32!WaitForSingleObjectEx+0x9c
        00000000`01fff9d0 00000000`76bfcdcd AUTHZ!AuthzpDeQueueThreadWorker+0x29
        00000000`01fffa00 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`01fffa30 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80046611f0  Cid 05f4.061c  Teb: 000007fffffaa000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004679e60  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa8004622180       Image:         svchost.exe
        Wait Start TickCount      2045           Ticks: 44534 (0:00:11:34.734)
        Context Switch Count      122
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address AUTHZ!AuthzpDeQueueThreadWorker (0x000007fefd364660)
        Stack Init fffff9800e742db0 Current fffff9800e742960
        Base fffff9800e743000 Limit fffff9800e73d000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e7429a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e742ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0e742b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0e742bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0e742c20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e742c20)
        00000000`0225fd88 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`0225fd90 000007fe`fd364689 kernel32!WaitForSingleObjectEx+0x9c
        00000000`0225fe50 00000000`76bfcdcd AUTHZ!AuthzpDeQueueThreadWorker+0x29
        00000000`0225fe80 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0225feb0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8003eed060  Cid 05f4.0630  Teb: 000007fffffda000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004665780  NotificationEvent
            fffffa8004667a20  NotificationEvent
            fffffa8004667bb0  NotificationEvent
            fffffa8004667890  NotificationEvent
            fffffa8004698ef0  SynchronizationEvent
        IRP List:
            fffffa8003fecee0: (0006,0118) Flags: 00060070  Mdl: 00000000
            fffffa8002947c70: (0006,0118) Flags: 00060070  Mdl: 00000000
            fffffa8004836ee0: (0006,0118) Flags: 00060070  Mdl: 00000000
            fffffa8004480360: (0006,0118) Flags: 00060070  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa8004622180       Image:         svchost.exe
        Wait Start TickCount      7401           Ticks: 39178 (0:00:10:11.180)
        Context Switch Count      106
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address mpssvc!WPP_SF_qd (0x000007fefab4d430)
        Stack Init fffff9800e765db0 Current fffff9800e765260
        Base fffff9800e766000 Limit fffff9800e760000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e7652a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e7653e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0e765440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0e7654b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0e765960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0e765bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e765c20)
        00000000`00edf8a8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`00edf8b0 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`00edf9c0 000007fe`fab4d68e kernel32!WaitForMultipleObjects+0x11
        00000000`00edfa00 00000000`76bfcdcd mpssvc!WPP_SF_qd+0x2be
        00000000`00edfb00 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`00edfb30 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800467a510  Cid 05f4.064c  Teb: 000007fffffa4000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa8004668bf0  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa8004622180       Image:         svchost.exe
        Wait Start TickCount      1878           Ticks: 44701 (0:00:11:37.340)
        Context Switch Count      108
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address mpssvc!Nla::CNlaServiceState::WaitForNotifications (0x000007fefab71bc0)
        Stack Init fffff9800e757db0 Current fffff9800e757960
        Base fffff9800e758000 Limit fffff9800e752000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e7579a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e757ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0e757b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0e757bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0e757c20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e757c20)
        00000000`025ffbe8 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`025ffbf0 000007fe`fab71cb7 kernel32!WaitForSingleObjectEx+0x9c
        00000000`025ffcb0 00000000`76bfcdcd mpssvc!Nla::CNlaServiceState::WaitForNotifications+0xa7
        00000000`025ffd10 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`025ffd40 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004690060  Cid 05f4.0654  Teb: 000007fffffa2000 Win32Thread: fffff900c07e5ab0
WAIT: (UserRequest) UserMode Alertable
            fffffa800468f9e0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa8004622180       Image:         svchost.exe
        Wait Start TickCount      1917           Ticks: 44662 (0:00:11:36.731)
        Context Switch Count      80                 LargeStack
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address mpssvc!FwDynDataNotifySinkProc (0x000007fefab3fab0)
        Stack Init fffff9800ef8ddb0 Current fffff9800ef8d960
        Base fffff9800ef8e000 Limit fffff9800ef87000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0ef8d9a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0ef8dae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0ef8db40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0ef8dbc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0ef8dc20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0ef8dc20)
        00000000`008cfd98 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`008cfda0 000007fe`fab3fe73 kernel32!WaitForSingleObjectEx+0x9c
        00000000`008cfe60 00000000`76bfcdcd mpssvc!FwDynDataNotifySinkProc+0x3c3
        00000000`008cff10 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`008cff40 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004693bb0  Cid 05f4.065c  Teb: 000007fffffa0000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Alertable
            fffffa8004690740  QueueObject
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa8004622180       Image:         svchost.exe
        Wait Start TickCount      1726           Ticks: 44853 (0:00:11:39.711)
        Context Switch Count      9
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x0000000076e17860)
        Stack Init fffff9800e703db0 Current fffff9800e703860
        Base fffff9800e704000 Limit fffff9800e6fe000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e7038a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e7039e0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0e703a40 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0e703ad0 fffff800`01c8a722 nt!IoRemoveIoCompletion+0x47
        fffff980`0e703b50 fffff800`01c4d733 nt!NtWaitForWorkViaWorkerFactory+0x1f1
        fffff980`0e703c20 00000000`76e21b4a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e703c20)
        00000000`020cfb18 00000000`76e17a20 ntdll!NtWaitForWorkViaWorkerFactory+0xa
        00000000`020cfb20 00000000`76bfcdcd ntdll!TppWorkerThread+0x23e
        00000000`020cfd90 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`020cfdc0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8002963060  Cid 05f4.0734  Teb: 000007fffffa8000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80047fe1e0  NotificationEvent
        IRP List:
            fffffa800439aaa0: (0006,0118) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa8004622180       Image:         svchost.exe
        Wait Start TickCount      40516          Ticks: 6063 (0:00:01:34.583)
        Context Switch Count      241
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ADVAPI32!ScSvcctrlThreadW (0x000007fefea84bd0)
        Stack Init fffff9800eabcdb0 Current fffff9800eabc960
        Base fffff9800eabd000 Limit fffff9800eab7000 Call 0
        Priority 13 BasePriority 8 PriorityDecrement 5 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0eabc9a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0eabcae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0eabcb40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0eabcbc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0eabcc20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0eabcc20)
        00000000`0244f0f8 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`0244f100 000007fe`fea89b0e kernel32!WaitForSingleObjectEx+0x9c
        00000000`0244f1c0 000007fe`fea8a6a5 ADVAPI32!EtwpProcessRealTimeTraces+0xf4
        00000000`0244f240 000007fe`fa7a5913 ADVAPI32!ProcessTrace+0x480
        00000000`0244f6b0 000007fe`fa7a57a6 dps!DpsRun+0xcb
        00000000`0244f8c0 00000000`ff911771 dps!ServiceMain+0x202
        00000000`0244f900 000007fe`fea84bf5 svchost!ServiceStarter+0x1ea
        00000000`0244f990 00000000`76bfcdcd ADVAPI32!ScSvcctrlThreadW+0x25
        00000000`0244f9c0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0244f9f0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80047ed060  Cid 05f4.0778  Teb: 000007fffff9e000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004729340  NotificationEvent
            fffffa80047292e0  SynchronizationEvent
            fffffa800296b900  NotificationEvent
            fffffa80047ed118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa8004622180       Image:         svchost.exe
        Wait Start TickCount      40325          Ticks: 6254 (0:00:01:37.563)
        Context Switch Count      7
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address dps!DpspBackgroundControl (0x000007fefa7b7cdc)
        Stack Init fffff9800eaa0db0 Current fffff9800eaa0260
        Base fffff9800eaa1000 Limit fffff9800ea9b000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0eaa02a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0eaa03e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0eaa0440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0eaa04b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0eaa0960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0eaa0bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0eaa0c20)
        00000000`02a9f588 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`02a9f590 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`02a9f6a0 000007fe`fa7b7ffb kernel32!WaitForMultipleObjects+0x11
        00000000`02a9f6e0 00000000`76bfcdcd dps!DpspBackgroundControl+0x31f
        00000000`02a9f770 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02a9f7a0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80047edbb0  Cid 05f4.077c  Teb: 000007fffff9c000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80044d8320  Semaphore Limit 0x7fffffff
            fffffa8004729340  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa8004622180       Image:         svchost.exe
        Wait Start TickCount      40451          Ticks: 6128 (0:00:01:35.597)
        Context Switch Count      82
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address dps!DpspSetThreadToken (0x000007fefa7ae8e0)
        Stack Init fffff9800f39ddb0 Current fffff9800f39d260
        Base fffff9800f39e000 Limit fffff9800f398000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0f39d2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0f39d3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0f39d440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0f39d4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0f39d960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0f39dbb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0f39dc20)
        00000000`02bef888 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`02bef890 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`02bef9a0 000007fe`fa7aea37 kernel32!WaitForMultipleObjects+0x11
        00000000`02bef9e0 00000000`76bfcdcd dps!DpspSetThreadToken+0xad7
        00000000`02befa70 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02befaa0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80047ed700  Cid 05f4.0780  Teb: 000007fffff9a000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80044d8320  Semaphore Limit 0x7fffffff
            fffffa8004729340  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa8004622180       Image:         svchost.exe
        Wait Start TickCount      16796          Ticks: 29783 (0:00:07:44.617)
        Context Switch Count      55
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address dps!DpspSetThreadToken (0x000007fefa7ae8e0)
        Stack Init fffff9800f3dcdb0 Current fffff9800f3dc260
        Base fffff9800f3dd000 Limit fffff9800f3d7000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0f3dc2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0f3dc3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0f3dc440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0f3dc4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0f3dc960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0f3dcbb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0f3dcc20)
        00000000`02b6fb88 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`02b6fb90 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`02b6fca0 000007fe`fa7aea37 kernel32!WaitForMultipleObjects+0x11
        00000000`02b6fce0 00000000`76bfcdcd dps!DpspSetThreadToken+0xad7
        00000000`02b6fd70 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02b6fda0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80047ef060  Cid 05f4.0784  Teb: 000007fffff98000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80044d8320  Semaphore Limit 0x7fffffff
            fffffa8004729340  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa8004622180       Image:         svchost.exe
        Wait Start TickCount      40451          Ticks: 6128 (0:00:01:35.597)
        Context Switch Count      81
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address dps!DpspSetThreadToken (0x000007fefa7ae8e0)
        Stack Init fffff9800f3e3db0 Current fffff9800f3e3260
        Base fffff9800f3e4000 Limit fffff9800f3de000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0f3e32a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0f3e33e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0f3e3440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0f3e34b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0f3e3960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0f3e3bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0f3e3c20)
        00000000`02d1fa78 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`02d1fa80 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`02d1fb90 000007fe`fa7aea37 kernel32!WaitForMultipleObjects+0x11
        00000000`02d1fbd0 00000000`76bfcdcd dps!DpspSetThreadToken+0xad7
        00000000`02d1fc60 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02d1fc90 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80047efbb0  Cid 05f4.0788  Teb: 000007fffff96000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80044d8320  Semaphore Limit 0x7fffffff
            fffffa8004729340  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa8004622180       Image:         svchost.exe
        Wait Start TickCount      40451          Ticks: 6128 (0:00:01:35.597)
        Context Switch Count      49
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address dps!DpspSetThreadToken (0x000007fefa7ae8e0)
        Stack Init fffff9800f3eadb0 Current fffff9800f3ea260
        Base fffff9800f3eb000 Limit fffff9800f3e5000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0f3ea2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0f3ea3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0f3ea440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0f3ea4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0f3ea960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0f3eabb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0f3eac20)
        00000000`0237f8f8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0237f900 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0237fa10 000007fe`fa7aea37 kernel32!WaitForMultipleObjects+0x11
        00000000`0237fa50 00000000`76bfcdcd dps!DpspSetThreadToken+0xad7
        00000000`0237fae0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0237fb10 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80047ef700  Cid 05f4.078c  Teb: 000007fffff94000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80044d8320  Semaphore Limit 0x7fffffff
            fffffa8004729340  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa8004622180       Image:         svchost.exe
        Wait Start TickCount      40451          Ticks: 6128 (0:00:01:35.597)
        Context Switch Count      82
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address dps!DpspSetThreadToken (0x000007fefa7ae8e0)
        Stack Init fffff9800f3f1db0 Current fffff9800f3f1260
        Base fffff9800f3f2000 Limit fffff9800f3ec000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0f3f12a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0f3f13e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0f3f1440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0f3f14b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0f3f1960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0f3f1bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0f3f1c20)
        00000000`02eafb68 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`02eafb70 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`02eafc80 000007fe`fa7aea37 kernel32!WaitForMultipleObjects+0x11
        00000000`02eafcc0 00000000`76bfcdcd dps!DpspSetThreadToken+0xad7
        00000000`02eafd50 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02eafd80 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8001f7b060  Cid 05f4.03f0  Teb: 000007fffffd4000 Win32Thread: fffff900c07e6500
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004871750  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa8004622180       Image:         svchost.exe
        Wait Start TickCount      11862          Ticks: 34717 (0:00:09:01.588)
        Context Switch Count      88                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address dps!WdipLaunchLocalHost (0x000007fefa7bc898)
        Stack Init fffff98012b43db0 Current fffff98012b43260
        Base fffff98012b44000 Limit fffff98012b3c000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`12b432a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12b433e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`12b43440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`12b434b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`12b43960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`12b43bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12b43c20)
        00000000`0300f618 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0300f620 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0300f730 000007fe`fa70883a kernel32!WaitForMultipleObjects+0x11
        00000000`0300f770 000007fe`fa70e2e6 wdi!WdipHostListener+0xe6
        00000000`0300f820 000007fe`fa70de32 wdi!WdipTriggerHost+0x25a
        00000000`0300f880 00000000`76bfcdcd wdi!WdipLaunchLocalHost+0x16
        00000000`0300f8c0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0300f8f0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8001fc1060  Cid 05f4.0340  Teb: 000007fffffae000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8002009bb0  QueueObject
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa8004622180       Image:         svchost.exe
        Wait Start TickCount      7401           Ticks: 39178 (0:00:10:11.180)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdi!WdipSessionListener (0x000007fefa708ad0)
        Stack Init fffff980157f4db0 Current fffff980157f4810
        Base fffff980157f5000 Limit fffff980157ef000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`157f4850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`157f4990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`157f49f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`157f4a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`157f4b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`157f4bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`157f4c20)
        00000000`01eff748 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`01eff750 000007fe`fa708b94 kernel32!GetQueuedCompletionStatus+0x48
        00000000`01eff7b0 00000000`76bfcdcd wdi!WdipSessionListener+0xc4
        00000000`01eff850 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`01eff880 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8001fc1bb0  Cid 05f4.0590  Teb: 000007fffff90000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8002009bb0  QueueObject
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa8004622180       Image:         svchost.exe
        Wait Start TickCount      7401           Ticks: 39178 (0:00:10:11.180)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdi!WdipSessionListener (0x000007fefa708ad0)
        Stack Init fffff980157fbdb0 Current fffff980157fb810
        Base fffff980157fc000 Limit fffff980157f6000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`157fb850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`157fb990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`157fb9f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`157fba80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`157fbb00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`157fbbb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`157fbc20)
        00000000`0352fd68 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`0352fd70 000007fe`fa708b94 kernel32!GetQueuedCompletionStatus+0x48
        00000000`0352fdd0 00000000`76bfcdcd wdi!WdipSessionListener+0xc4
        00000000`0352fe70 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0352fea0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8001fc1700  Cid 05f4.06e8  Teb: 000007fffff8c000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8002009bb0  QueueObject
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa8004622180       Image:         svchost.exe
        Wait Start TickCount      7432           Ticks: 39147 (0:00:10:10.697)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdi!WdipSessionListener (0x000007fefa708ad0)
        Stack Init fffff98015802db0 Current fffff98015802810
        Base fffff98015803000 Limit fffff980157fd000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`15802850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`15802990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`158029f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`15802a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`15802b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`15802bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`15802c20)
        00000000`02c8f8a8 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`02c8f8b0 000007fe`fa708b94 kernel32!GetQueuedCompletionStatus+0x48
        00000000`02c8f910 00000000`76bfcdcd wdi!WdipSessionListener+0xc4
        00000000`02c8f9b0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02c8f9e0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8001fc0060  Cid 05f4.02a4  Teb: 000007fffff8a000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8002009bb0  QueueObject
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa8004622180       Image:         svchost.exe
        Wait Start TickCount      7401           Ticks: 39178 (0:00:10:11.180)
        Context Switch Count      7
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdi!WdipSessionListener (0x000007fefa708ad0)
        Stack Init fffff9801582cdb0 Current fffff9801582c810
        Base fffff9801582d000 Limit fffff98015827000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1582c850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1582c990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`1582c9f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`1582ca80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`1582cb00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`1582cbb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1582cc20)
        00000000`035dfd88 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`035dfd90 000007fe`fa708b94 kernel32!GetQueuedCompletionStatus+0x48
        00000000`035dfdf0 00000000`76bfcdcd wdi!WdipSessionListener+0xc4
        00000000`035dfe90 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`035dfec0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8001fc0bb0  Cid 05f4.0ac8  Teb: 000007fffff86000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8002009bb0  QueueObject
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa8004622180       Image:         svchost.exe
        Wait Start TickCount      7442           Ticks: 39137 (0:00:10:10.541)
        Context Switch Count      97
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdi!WdipSessionListener (0x000007fefa708ad0)
        Stack Init fffff980159c0db0 Current fffff980159c0810
        Base fffff980159c1000 Limit fffff980159bb000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`159c0850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`159c0990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`159c09f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`159c0a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`159c0b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`159c0bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`159c0c20)
        00000000`0370f7a8 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`0370f7b0 000007fe`fa708b94 kernel32!GetQueuedCompletionStatus+0x48
        00000000`0370f810 00000000`76bfcdcd wdi!WdipSessionListener+0xc4
        00000000`0370f8b0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0370f8e0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8001fc0700  Cid 05f4.040c  Teb: 000007fffff84000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8002009bb0  QueueObject
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa8004622180       Image:         svchost.exe
        Wait Start TickCount      7432           Ticks: 39147 (0:00:10:10.697)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdi!WdipSessionListener (0x000007fefa708ad0)
        Stack Init fffff98015809db0 Current fffff98015809810
        Base fffff9801580a000 Limit fffff98015804000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`15809850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`15809990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`158099f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`15809a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`15809b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`15809bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`15809c20)
        00000000`0367fb88 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`0367fb90 000007fe`fa708b94 kernel32!GetQueuedCompletionStatus+0x48
        00000000`0367fbf0 00000000`76bfcdcd wdi!WdipSessionListener+0xc4
        00000000`0367fc90 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0367fcc0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8001f38060  Cid 05f4.0444  Teb: 000007fffff82000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8002009bb0  QueueObject
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa8004622180       Image:         svchost.exe
        Wait Start TickCount      13319          Ticks: 33260 (0:00:08:38.859)
        Context Switch Count      45
        UserTime                  00:00:00.046
        KernelTime                00:00:00.031
        Win32 Start Address wdi!WdipSessionListener (0x000007fefa708ad0)
        Stack Init fffff98015810db0 Current fffff98015810810
        Base fffff98015811000 Limit fffff9801580b000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`15810850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`15810990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`158109f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`15810a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`15810b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`15810bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`15810c20)
        00000000`038af978 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`038af980 000007fe`fa708b94 kernel32!GetQueuedCompletionStatus+0x48
        00000000`038af9e0 00000000`76bfcdcd wdi!WdipSessionListener+0xc4
        00000000`038afa80 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`038afab0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8001f38bb0  Cid 05f4.048c  Teb: 000007fffff80000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8002009bb0  QueueObject
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa8004622180       Image:         svchost.exe
        Wait Start TickCount      7432           Ticks: 39147 (0:00:10:10.697)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdi!WdipSessionListener (0x000007fefa708ad0)
        Stack Init fffff98015817db0 Current fffff98015817810
        Base fffff98015818000 Limit fffff98015812000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`15817850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`15817990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`158179f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`15817a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`15817b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`15817bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`15817c20)
        00000000`0393fcf8 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`0393fd00 000007fe`fa708b94 kernel32!GetQueuedCompletionStatus+0x48
        00000000`0393fd60 00000000`76bfcdcd wdi!WdipSessionListener+0xc4
        00000000`0393fe00 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0393fe30 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8001f38700  Cid 05f4.0450  Teb: 000007fffff7e000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8002009bb0  QueueObject
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa8004622180       Image:         svchost.exe
        Wait Start TickCount      15563          Ticks: 31016 (0:00:08:03.852)
        Context Switch Count      823
        UserTime                  00:00:00.655
        KernelTime                00:00:01.060
        Win32 Start Address wdi!WdipSessionListener (0x000007fefa708ad0)
        Stack Init fffff98015825db0 Current fffff98015825810
        Base fffff98015826000 Limit fffff98015820000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`15825850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`15825990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`158259f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`15825a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`15825b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`15825bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`15825c20)
        00000000`0379f6c8 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`0379f6d0 000007fe`fa708b94 kernel32!GetQueuedCompletionStatus+0x48
        00000000`0379f730 00000000`76bfcdcd wdi!WdipSessionListener+0xc4
        00000000`0379f7d0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0379f800 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8002003060  Cid 05f4.0660  Teb: 000007fffff7c000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8002009bb0  QueueObject
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa8004622180       Image:         svchost.exe
        Wait Start TickCount      7432           Ticks: 39147 (0:00:10:10.697)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdi!WdipSessionListener (0x000007fefa708ad0)
        Stack Init fffff980157c3db0 Current fffff980157c3810
        Base fffff980157c4000 Limit fffff980157be000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`157c3850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`157c3990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`157c39f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`157c3a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`157c3b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`157c3bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`157c3c20)
        00000000`034afb18 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`034afb20 000007fe`fa708b94 kernel32!GetQueuedCompletionStatus+0x48
        00000000`034afb80 00000000`76bfcdcd wdi!WdipSessionListener+0xc4
        00000000`034afc20 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`034afc50 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004561060  Cid 05f4.0e6c  Teb: 000007fffff92000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa800450d8f0  QueueObject
        Not impersonating
        DeviceMap                 fffff88005a30830
        Owning Process            fffffa8004622180       Image:         svchost.exe
        Wait Start TickCount      26903          Ticks: 19676 (0:00:05:06.947)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff980103b9db0 Current fffff980103b9810
        Base fffff980103ba000 Limit fffff980103b4000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`103b9850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`103b9990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`103b99f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`103b9a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`103b9b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`103b9bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`103b9c20)
        00000000`009ef7e8 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`009ef7f0 000007fe`fedce7a3 kernel32!GetQueuedCompletionStatus+0x48
        00000000`009ef850 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`009ef8e0 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`009ef990 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`009ef9c0 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`009efa00 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`009efa30 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`009efa60 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

CcSvcHst process

```
PROCESS fffffa8004a2fc10
    SessionId: 0  Cid: 06d4    Peb: 7efdf000  ParentCid: 025c
    DirBase: 45f8c000  ObjectTable: fffff880057fa9e0  HandleCount: 356.
    Image: ccSvcHst.exe
    VadRoot fffffa800436ddb0 Vads 172 Clone 0 Private 882. Modified 4741. Locked 0.
    DeviceMap fffff88000007820
    Token                             fffff88005e8ac40
    ElapsedTime                       00:11:39.941
    UserTime                          00:00:00.031
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         119104
    QuotaPoolUsage[NonPagedPool]      20208
    Working Set Sizes (now,min,max)  (780, 50, 345) (3120KB, 200KB, 1380KB)
    PeakWorkingSetSize                2825
    VirtualSize                       67 Mb
    PeakVirtualSize                   69 Mb
    PageFaultCount                    15520
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      1668

    Setting context for this process...
.process /p /r fffffa8004a2fc10

    !peb
PEB at 000000007efdf000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         0000000000400000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00000000002c2840 . 00000000002c2ba0
    Ldr.InLoadOrderModuleList:           00000000002c2750 . 00000000002c2d00
    Ldr.InMemoryOrderModuleList:         00000000002c2760 . 00000000002c2d10
            Base TimeStamp                     Module
          400000 4578a2a1 Dec 07 23:24:17 2006 c:\Program Files (x86)\Common Files\Symantec
Shared\ccSvcHst.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        75110000 4549d371 Nov 02 11:16:01 2006 C:\Windows\system32\wow64.dll
        75000000 4549d374 Nov 02 11:16:04 2006 C:\Windows\system32\wow64win.dll
        75100000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\wow64cpu.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       00000000002c0000
    ProcessParameters: 00000000002c1d20
    WindowTitle:  'c:\Program Files (x86)\Common Files\Symantec Shared\ccSvcHst.exe'
    ImageFile:    'c:\Program Files (x86)\Common Files\Symantec Shared\ccSvcHst.exe'
    CommandLine:  '"c:\Program Files (x86)\Common Files\Symantec Shared\ccSvcHst.exe" /h ccCommon'
    DllPath:      'c:\Program Files (x86)\Common Files\Symantec
Shared;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Windows;C:\Windows
\System32\Wbem'
    Environment:  00000000002c1310
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\system32\config\systemprofile\AppData\Roaming
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        LOCALAPPDATA=C:\Windows\system32\config\systemprofile\AppData\Local
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
```

```
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\TEMP
        TMP=C:\Windows\TEMP
        USERDOMAIN=DOMAIN
        USERNAME=COMPUTERNAME$
        USERPROFILE=C:\Windows\system32\config\systemprofile
        windir=C:\Windows


        THREAD fffffa8004a2f780  Cid 06d4.06d8  Teb: 000000007efdb000 Win32Thread: fffff900c07e0010
WAIT: (Executive) UserMode Non-Alertable
            fffffa80047577a8  NotificationEvent
        IRP List:
            fffffa80044be010: (0006,0118) Flags: 00060900  Mdl: 00000000
            fffffa8004757800: (0006,0358) Flags: 00060000  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004a2fc10       Image:         ccSvcHst.exe
        Wait Start TickCount      1879           Ticks: 44700 (0:00:11:37.324)
        Context Switch Count      2426                 LargeStack
        UserTime                  00:00:00.078
        KernelTime                00:00:00.265
        Win32 Start Address ccSvcHst (0x000000000040ae9d)
        Stack Init fffff9800e5d9db0 Current fffff9800e5d97f0
        Base fffff9800e5da000 Limit fffff9800e5d1000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e5d9830 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e5d9970 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0e5d99d0 fffff800`01ebdf16 nt!KeWaitForSingleObject+0x5f5
        fffff980`0e5d9a50 fffff800`01ea1a24 nt!IopSynchronousServiceTail+0x306
        fffff980`0e5d9ac0 fffff800`01c4d733 nt!NtReadFile+0x583
        fffff980`0e5d9bb0 00000000`75103907 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e5d9c20)
        00000000`0007ee38 00000000`7511abfe wow64cpu!ReadWriteFileFault+0x35
        00000000`0007ef10 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0007ef40 00000000`76e0e23d wow64!Wow64LdrpInitialize+0x492
        00000000`0007f4a0 00000000`76e7e974 ntdll!LdrpInitializeProcess+0x1333
        00000000`0007f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d641
        00000000`0007f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa8004753a30  Cid 06d4.06dc  Teb: 000000007efd8000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa8004753620  SynchronizationTimer
            fffffa800473add0  SynchronizationEvent
            fffffa8004754aa0  SynchronizationEvent
            fffffa8004755040  SynchronizationEvent
            fffffa8004764ae0  SynchronizationEvent
            fffffa800474b1d0  SynchronizationEvent
            fffffa8004754d80  SynchronizationEvent
            fffffa80047584f0  SynchronizationEvent
            fffffa8004758220  SynchronizationEvent
            fffffa8004759d70  SynchronizationEvent
            fffffa8004759a40  SynchronizationEvent
            fffffa8004755fe0  SynchronizationEvent
            fffffa80047587b0  SynchronizationEvent
            fffffa8004764980  SynchronizationEvent
            fffffa80045e6f80  SynchronizationEvent
            fffffa80047653e0  SynchronizationEvent
            fffffa8004754cc0  SynchronizationEvent
            fffffa80047585f0  SynchronizationEvent
            fffffa80047650e8  NotificationEvent
            fffffa80047544c0  SynchronizationEvent
            fffffa8004759b60  SynchronizationEvent
            fffffa8004764270  SynchronizationEvent
            fffffa8004765bb0  SynchronizationEvent
            fffffa8004765a10  SynchronizationEvent
            fffffa8004757310  SynchronizationEvent
            fffffa8004757230  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004a2fc10       Image:         ccSvcHst.exe
        Wait Start TickCount      7661           Ticks: 38918 (0:00:10:07.124)
        Context Switch Count      186
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x0000000077046235
        Stack Init fffff9800ebabdb0 Current fffff9800ebab260
        Base fffff9800ebac000 Limit fffff9800eba6000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0ebab2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0ebab3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0ebab440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0ebab4b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`0ebab960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`0ebabbb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0ebabc20)
        00000000`0027f0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`0027f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0027f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0027f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0027f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa800475a060  Cid 06d4.06ec  Teb: 000000007efaa000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004757d00  NotificationEvent
            fffffa800475a118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004a2fc10       Image:         ccSvcHst.exe
        Wait Start TickCount      43804          Ticks: 2775 (0:00:00:43.290)
        Context Switch Count      630
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3494f6
        Stack Init fffff9800eac3db0 Current fffff9800eac3960
        Base fffff9800eac4000 Limit fffff9800eabe000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0eac39a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0eac3ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0eac3b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0eac3bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0eac3c20 00000000`75103cf9 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0eac3c20)
        00000000`011cf128 00000000`75103af6 wow64cpu!CpupSyscallStub+0x9
        00000000`011cf130 00000000`7511abfe wow64cpu!Thunk0ArgReloadState+0x1a
        00000000`011cf1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`011cf1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`011cf730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`011cf7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa8004762060  Cid 06d4.06f0  Teb: 000000007efa7000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800475c510  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004a2fc10       Image:         ccSvcHst.exe
        Wait Start TickCount      1844           Ticks: 44735 (0:00:11:37.870)
        Context Switch Count      1727
        UserTime                  00:00:00.000
        KernelTime                00:00:00.093
        Win32 Start Address 0x00000000767fb9d5
        Stack Init fffff9800eacadb0 Current fffff9800eaca960
        Base fffff9800eacb000 Limit fffff9800eac5000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0eaca9a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0eacaae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0eacab40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0eacabc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0eacac20 00000000`75103cf9 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0eacac20)
        00000000`0124f128 00000000`75103af6 wow64cpu!CpupSyscallStub+0x9
        00000000`0124f130 00000000`7511abfe wow64cpu!Thunk0ArgReloadState+0x1a
        00000000`0124f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0124f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0124f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0124f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa800295b060  Cid 06d4.0710  Teb: 000000007efa4000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80043a92d0  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004a2fc10       Image:         ccSvcHst.exe
        Wait Start TickCount      1848           Ticks: 44731 (0:00:11:37.808)
        Context Switch Count      122
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address 0x000000007c3494f6
        Stack Init fffff9800eae6db0 Current fffff9800eae6960
        Base fffff9800eae7000 Limit fffff9800eae1000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0eae69a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0eae6ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0eae6b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0eae6bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0eae6c20 00000000`75103cf9 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0eae6c20)
        00000000`0140f128 00000000`75103af6 wow64cpu!CpupSyscallStub+0x9
        00000000`0140f130 00000000`7511abfe wow64cpu!Thunk0ArgReloadState+0x1a
        00000000`0140f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0140f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0140f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0140f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa800485b840  Cid 06d4.04d8  Teb: 000000007efa1000 Win32Thread: fffff900c07ed460
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80046a7400  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004a2fc10       Image:         ccSvcHst.exe
        Wait Start TickCount      1885           Ticks: 44694 (0:00:11:37.230)
        Context Switch Count      305                 LargeStack
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address 0x00000000767fb9d5
        Stack Init fffff9800efffdb0 Current fffff9800efff960
        Base fffff9800f000000 Limit fffff9800eff7000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0efff9a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0efffae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0efffb40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0efffbc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0efffc20 00000000`75103cf9 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0efffc20)
        00000000`0161f128 00000000`75103af6 wow64cpu!CpupSyscallStub+0x9
        00000000`0161f130 00000000`7511abfe wow64cpu!Thunk0ArgReloadState+0x1a
        00000000`0161f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0161f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0161f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0161f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa8004869bb0  Cid 06d4.0664  Teb: 000000007ef9e000 Win32Thread: fffff900c07ead60
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80048597b0  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004a2fc10       Image:         ccSvcHst.exe
        Wait Start TickCount      1931           Ticks: 44648 (0:00:11:36.513)
        Context Switch Count      3593                 LargeStack
        UserTime                  00:00:00.046
        KernelTime                00:00:00.031
        Win32 Start Address 0x000000007c3494f6
        Stack Init fffff9800e57adb0 Current fffff9800e57a960
        Base fffff9800e57b000 Limit fffff9800e572000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e57a9a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e57aae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0e57ab40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0e57abc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0e57ac20 00000000`75103cf9 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e57ac20)
        00000000`0169f128 00000000`75103af6 wow64cpu!CpupSyscallStub+0x9
        00000000`0169f130 00000000`7511abfe wow64cpu!Thunk0ArgReloadState+0x1a
        00000000`0169f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0169f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0169f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0169f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa800487a060  Cid 06d4.06b0  Teb: 000000007ef9b000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004888400  NotificationEvent
            fffffa8004869850  NotificationEvent
            fffffa8004874990  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004a2fc10       Image:         ccSvcHst.exe
        Wait Start TickCount      46515          Ticks: 64 (0:00:00:00.998)
        Context Switch Count      3684
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3494f6
        Stack Init fffff980103eadb0 Current fffff980103ea260
        Base fffff980103eb000 Limit fffff980103e5000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`103ea2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`103ea3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`103ea440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`103ea4b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`103ea960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`103eabb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`103eac20)
        00000000`0171f0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`0171f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0171f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0171f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0171f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa800487b060  Cid 06d4.0328  Teb: 000000007ef98000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80048372c0  NotificationEvent
            fffffa8004869850  NotificationEvent
            fffffa8004874990  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004a2fc10       Image:         ccSvcHst.exe
        Wait Start TickCount      46515          Ticks: 64 (0:00:00:00.998)
        Context Switch Count      3498
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3494f6
        Stack Init fffff980103f1db0 Current fffff980103f1260
        Base fffff980103f2000 Limit fffff980103ec000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`103f12a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`103f13e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`103f1440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`103f14b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`103f1960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`103f1bb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`103f1c20)
        00000000`0179f0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`0179f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0179f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0179f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0179f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa800487bbb0  Cid 06d4.066c  Teb: 000000007ef95000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004878fe0  NotificationEvent
            fffffa8004869850  NotificationEvent
            fffffa8004874990  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004a2fc10       Image:         ccSvcHst.exe
        Wait Start TickCount      46515          Ticks: 64 (0:00:00:00.998)
        Context Switch Count      3740
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3494f6
        Stack Init fffff980103b2db0 Current fffff980103b2260
        Base fffff980103b3000 Limit fffff980103ad000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`103b22a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`103b23e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`103b2440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`103b24b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`103b2960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`103b2bb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`103b2c20)
        00000000`0181f0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`0181f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0181f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0181f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0181f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa800487b700  Cid 06d4.06f8  Teb: 000000007ef92000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004878f30  NotificationEvent
            fffffa8004869850  NotificationEvent
            fffffa8004874990  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004a2fc10       Image:         ccSvcHst.exe
        Wait Start TickCount      46515          Ticks: 64 (0:00:00:00.998)
        Context Switch Count      3442
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3494f6
        Stack Init fffff980103ffdb0 Current fffff980103ff260
        Base fffff98010400000 Limit fffff980103fa000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`103ff2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`103ff3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`103ff440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`103ff4b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`103ff960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`103ffbb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`103ffc20)
        00000000`0189f0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`0189f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0189f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0189f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0189f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa800487c060  Cid 06d4.0708  Teb: 000000007ef8f000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800487d260  NotificationEvent
            fffffa8004869850  NotificationEvent
            fffffa8004874990  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004a2fc10       Image:         ccSvcHst.exe
        Wait Start TickCount      46515          Ticks: 64 (0:00:00:00.998)
        Context Switch Count      3708
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3494f6
        Stack Init fffff9800f3cedb0 Current fffff9800f3ce260
        Base fffff9800f3cf000 Limit fffff9800f3c9000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0f3ce2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0f3ce3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0f3ce440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0f3ce4b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`0f3ce960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`0f3cebb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0f3cec20)
        00000000`0191f0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`0191f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0191f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0191f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0191f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa800487cbb0  Cid 06d4.074c  Teb: 000000007ef8c000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800487d880  NotificationEvent
            fffffa8004869850  NotificationEvent
            fffffa8004874990  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004a2fc10       Image:         ccSvcHst.exe
        Wait Start TickCount      46515          Ticks: 64 (0:00:00:00.998)
        Context Switch Count      3428
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3494f6
        Stack Init fffff980103cedb0 Current fffff980103ce260
        Base fffff980103cf000 Limit fffff980103c9000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`103ce2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`103ce3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`103ce440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`103ce4b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`103ce960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`103cebb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`103cec20)
        00000000`0199f0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`0199f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0199f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0199f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0199f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa800487c700  Cid 06d4.0748  Teb: 000000007ef89000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800487b620  NotificationEvent
            fffffa800486c040  NotificationEvent
            fffffa800487b680  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004a2fc10       Image:         ccSvcHst.exe
        Wait Start TickCount      19121          Ticks: 27458 (0:00:07:08.347)
        Context Switch Count      54
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3494f6
        Stack Init fffff980103dcdb0 Current fffff980103dc260
        Base fffff980103dd000 Limit fffff980103d7000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`103dc2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`103dc3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`103dc440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`103dc4b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`103dc960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`103dcbb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`103dcc20)
        00000000`01a1f0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`01a1f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`01a1f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`01a1f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`01a1f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa800487e060  Cid 06d4.075c  Teb: 000000007ef86000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800487c680  NotificationEvent
            fffffa800486c040  NotificationEvent
            fffffa800487b680  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004a2fc10       Image:         ccSvcHst.exe
        Wait Start TickCount      19121          Ticks: 27458 (0:00:07:08.347)
        Context Switch Count      56
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3494f6
        Stack Init fffff98010326db0 Current fffff98010326260
        Base fffff98010327000 Limit fffff98010321000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`103262a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`103263e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`10326440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`103264b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`10326960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`10326bb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`10326c20)
        00000000`01a9f0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`01a9f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`01a9f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`01a9f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`01a9f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa800487ebb0  Cid 06d4.0758  Teb: 000000007ef83000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800487c4f0  NotificationEvent
            fffffa800486c040  NotificationEvent
            fffffa800487b680  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004a2fc10       Image:         ccSvcHst.exe
        Wait Start TickCount      19121          Ticks: 27458 (0:00:07:08.347)
        Context Switch Count      54
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3494f6
        Stack Init fffff9801032ddb0 Current fffff9801032d260
        Base fffff9801032e000 Limit fffff98010328000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1032d2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1032d3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`1032d440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`1032d4b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`1032d960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`1032dbb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1032dc20)
        00000000`01b1f0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`01b1f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`01b1f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`01b1f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`01b1f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa800487e700  Cid 06d4.0568  Teb: 000000007ef80000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004879570  NotificationEvent
            fffffa800486c040  NotificationEvent
            fffffa800487b680  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004a2fc10       Image:         ccSvcHst.exe
        Wait Start TickCount      19121          Ticks: 27458 (0:00:07:08.347)
        Context Switch Count      58
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3494f6
        Stack Init fffff98010334db0 Current fffff98010334260
        Base fffff98010335000 Limit fffff9801032f000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`103342a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`103343e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`10334440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`103344b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`10334960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`10334bb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`10334c20)
        00000000`01b9f0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`01b9f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`01b9f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`01b9f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`01b9f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa800487f060  Cid 06d4.0794  Teb: 000000007ef7d000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800487e5f0  NotificationEvent
            fffffa800486c040  NotificationEvent
            fffffa800487b680  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004a2fc10       Image:         ccSvcHst.exe
        Wait Start TickCount      19121          Ticks: 27458 (0:00:07:08.347)
        Context Switch Count      54
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3494f6
        Stack Init fffff9801033bdb0 Current fffff9801033b260
        Base fffff9801033c000 Limit fffff98010336000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1033b2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1033b3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`1033b440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`1033b4b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`1033b960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`1033bbb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1033bc20)
        00000000`01c1f0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`01c1f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`01c1f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`01c1f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`01c1f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa800487fb20  Cid 06d4.07a8  Teb: 000000007ef7a000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800487e4f0  NotificationEvent
            fffffa800486c040  NotificationEvent
            fffffa800487b680  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004a2fc10       Image:         ccSvcHst.exe
        Wait Start TickCount      19121          Ticks: 27458 (0:00:07:08.347)
        Context Switch Count      55
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3494f6
        Stack Init fffff98010342db0 Current fffff98010342260
        Base fffff98010343000 Limit fffff9801033d000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`103422a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`103423e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`10342440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`103424b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`10342960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`10342bb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`10342c20)
        00000000`01c9f0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`01c9f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`01c9f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`01c9f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`01c9f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa80048ab060  Cid 06d4.0838  Teb: 000000007ef71000 Win32Thread: fffff900c07f2d60
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800296d3a0  SynchronizationEvent
            fffffa80047fd4f0  SynchronizationEvent
            fffffa8003d5dad0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004a2fc10       Image:         ccSvcHst.exe
        Wait Start TickCount      46515          Ticks: 64 (0:00:00:00.998)
        Context Switch Count      2477                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:01.544
        Win32 Start Address 0x000000006fa37d78
        Stack Init fffff9800e4f5db0 Current fffff9800e4f5260
        Base fffff9800e4f6000 Limit fffff9800e4ee000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0e4f52a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e4f53e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0e4f5440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0e4f54b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`0e4f5960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`0e4f5bb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e4f5c20)
        00000000`01f5f0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`01f5f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`01f5f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`01f5f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`01f5f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa800204a210  Cid 06d4.0c40  Teb: 000000007efad000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8001f91d80  NotificationEvent
            fffffa8001f7c7f0  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004a2fc10       Image:         ccSvcHst.exe
        Wait Start TickCount      19121          Ticks: 27458 (0:00:07:08.347)
        Context Switch Count      41
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000006fa37d78
        Stack Init fffff9800ccaedb0 Current fffff9800ccae260
        Base fffff9800ccaf000 Limit fffff9800cca9000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0ccae2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0ccae3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0ccae440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0ccae4b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`0ccae960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`0ccaebb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0ccaec20)
        00000000`003ff0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`003ff1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`003ff1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`003ff730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`003ff7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa80039d8550  Cid 06d4.0f34  Teb: 000000007efd5000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8004726700  QueueObject
            fffffa80039d8608  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004a2fc10       Image:         ccSvcHst.exe
        Wait Start TickCount      46515          Ticks: 64 (0:00:00:00.998)
        Context Switch Count      146
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x00000000762f3242
        Stack Init fffff9800e346db0 Current fffff9800e346810
        Base fffff9800e347000 Limit fffff9800e341000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0e346850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e346990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0e3469f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0e346a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`0e346b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`0e346bb0 00000000`751039a2 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e346c20)
        00000000`0037f0c8 00000000`7511abfe wow64cpu!RemoveIoCompletionFault+0x41
        00000000`0037f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0037f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0037f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0037f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa8002858bb0  Cid 06d4.0728  Teb: 000000007ef77000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8004726700  QueueObject
            fffffa8002858c68  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004a2fc10       Image:         ccSvcHst.exe
        Wait Start TickCount      45002          Ticks: 1577 (0:00:00:24.601)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x00000000762f3242
        Stack Init fffff9801daa1db0 Current fffff9801daa1810
        Base fffff9801daa2000 Limit fffff9801da9c000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1daa1850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1daa1990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`1daa19f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`1daa1a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`1daa1b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`1daa1bb0 00000000`751039a2 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1daa1c20)
        00000000`01e5f0c8 00000000`7511abfe wow64cpu!RemoveIoCompletionFault+0x41
        00000000`01e5f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`01e5f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`01e5f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`01e5f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

DbgSvc process

```
PROCESS fffffa800475d280
    SessionId: 0  Cid: 06fc    Peb: 7efdf000  ParentCid: 025c
    DirBase: 445e2000  ObjectTable: fffff880059b0250  HandleCount: 323.
    Image: DbgSvc.exe
    VadRoot fffffa8002961860 Vads 177 Clone 0 Private 1242. Modified 174. Locked 0.
    DeviceMap fffff88000007820
    Token                             fffff880059567f0
    ElapsedTime                       00:11:38.792
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         102488
    QuotaPoolUsage[NonPagedPool]      17568
    Working Set Sizes (now,min,max)  (2992, 50, 345) (11968KB, 200KB, 1380KB)
    PeakWorkingSetSize                3156
    VirtualSize                       74 Mb
    PeakVirtualSize                   74 Mb
    PageFaultCount                    4377
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      1937

    Setting context for this process...
.process /p /r fffffa800475d280

    !peb
PEB at 000000007efdf000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         0000000001000000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 0000000000112790 . 0000000000112af0
    Ldr.InLoadOrderModuleList:           00000000001126a0 . 0000000000112c50
    Ldr.InMemoryOrderModuleList:         00000000001126b0 . 0000000000112c60
            Base TimeStamp                     Module
         1000000 45ac45bd Jan 16 03:25:49 2007 C:\Program Files (x86)\DebugDiag\DbgSvc.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        75110000 4549d371 Nov 02 11:16:01 2006 C:\Windows\system32\wow64.dll
        75000000 4549d374 Nov 02 11:16:04 2006 C:\Windows\system32\wow64win.dll
        75100000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\wow64cpu.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       0000000000110000
    ProcessParameters: 0000000000111d20
    WindowTitle:  'C:\Program Files (x86)\DebugDiag\DbgSvc.exe'
    ImageFile:    'C:\Program Files (x86)\DebugDiag\DbgSvc.exe'
    CommandLine:  '"C:\Program Files (x86)\DebugDiag\DbgSvc.exe"'
    DllPath:      'C:\Program Files
(x86)\DebugDiag;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Windows;C
:\Windows\System32\Wbem'
    Environment:  0000000000111310
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\system32\config\systemprofile\AppData\Roaming
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        LOCALAPPDATA=C:\Windows\system32\config\systemprofile\AppData\Local
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
```

```
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\TEMP
        TMP=C:\Windows\TEMP
        USERDOMAIN=DOMAIN
        USERNAME=COMPUTERNAME$
        USERPROFILE=C:\Windows\system32\config\systemprofile
        windir=C:\Windows


        THREAD fffffa800474f950  Cid 06fc.0700  Teb: 000000007efdb000 Win32Thread: fffff900c07deab0
WAIT: (Executive) UserMode Non-Alertable
            fffffa8002953b68  NotificationEvent
        IRP List:
            fffffa8004751700: (0006,0118) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800475d280       Image:         DbgSvc.exe
        Wait Start TickCount      7450           Ticks: 39129 (0:00:10:10.416)
        Context Switch Count      1725                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.046
        Win32 Start Address DbgSvc (0x00000000010252d1)
        Stack Init fffff9800eee2db0 Current fffff9800eee27f0
        Base fffff9800eee3000 Limit fffff9800eedb000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0eee2830 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0eee2970 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0eee29d0 fffff800`01ebdf16 nt!KeWaitForSingleObject+0x5f5
        fffff980`0eee2a50 fffff800`01ea1a24 nt!IopSynchronousServiceTail+0x306
        fffff980`0eee2ac0 fffff800`01c4d733 nt!NtReadFile+0x583
        fffff980`0eee2bb0 00000000`75103907 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0eee2c20)
        00000000`0007ee38 00000000`7511abfe wow64cpu!ReadWriteFileFault+0x35
        00000000`0007ef10 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0007ef40 00000000`76e0e23d wow64!Wow64LdrpInitialize+0x492
        00000000`0007f4a0 00000000`76e7e974 ntdll!LdrpInitializeProcess+0x1333
        00000000`0007f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d641
        00000000`0007f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa800295c900  Cid 06fc.0718  Teb: 000000007efd8000 Win32Thread: fffff900c07e6d60
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa8004759350  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800475d280       Image:         DbgSvc.exe
        Wait Start TickCount      7450           Ticks: 39129 (0:00:10:10.416)
        Context Switch Count      114                 LargeStack
        UserTime                  00:00:00.031
        KernelTime                00:00:00.000
        Win32 Start Address 0x00000000767fb9d5
        Stack Init fffff9800ef2edb0 Current fffff9800ef2e740
        Base fffff9800ef2f000 Limit fffff9800ef28000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0ef2e780 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0ef2e8c0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0ef2e920 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`0ef2e9a0 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`0ef2ea40 fffff960`000c7e1e win32k!xxxSleepThread+0x56
        fffff980`0ef2ea70 fffff960`000c7f25 win32k!xxxRealInternalGetMessage+0x72e
        fffff980`0ef2eb50 fffff960`000c97e4 win32k!xxxInternalGetMessage+0x35
        fffff980`0ef2eb90 fffff800`01c4d733 win32k!NtUserGetMessage+0x64
        fffff980`0ef2ec20 00000000`75039f7a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0ef2ec20)
        00000000`001ce7f8 00000000`75023160 wow64win!ZwUserGetMessage+0xa
        00000000`001ce800 00000000`7511aa4e wow64win!whNtUserGetMessage+0x30
        00000000`001ce860 00000000`75103678 wow64!Wow64SystemServiceEx+0xca
        00000000`001cf110 00000000`7511abfe wow64cpu!TurboDispatchJumpAddressEnd+0x28
        00000000`001cf1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`001cf1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`001cf730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`001cf7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa8004a30820  Cid 06fc.072c  Teb: 000000007efaa000 Win32Thread: fffff900c07e4a60
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa80042ae420  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800475d280       Image:         DbgSvc.exe
        Wait Start TickCount      45955          Ticks: 624 (0:00:00:09.734)
        Context Switch Count      9865                LargeStack
        UserTime                  00:00:00.078
        KernelTime                00:00:00.452
        Win32 Start Address DbgSvc (0x0000000001013424)
        Stack Init fffff9800ef41db0 Current fffff9800ef41740
        Base fffff9800ef42000 Limit fffff9800ef39000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0ef41780 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0ef418c0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0ef41920 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`0ef419a0 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`0ef41a40 fffff960`000c7e1e win32k!xxxSleepThread+0x56
        fffff980`0ef41a70 fffff960`000c7f25 win32k!xxxRealInternalGetMessage+0x72e
        fffff980`0ef41b50 fffff960`000c97e4 win32k!xxxInternalGetMessage+0x35
        fffff980`0ef41b90 fffff800`01c4d733 win32k!NtUserGetMessage+0x64
        fffff980`0ef41c20 00000000`75039f7a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0ef41c20)
        00000000`0120e7f8 00000000`75023160 wow64win!ZwUserGetMessage+0xa
        00000000`0120e800 00000000`7511aa4e wow64win!whNtUserGetMessage+0x30
        00000000`0120e860 00000000`75103678 wow64!Wow64SystemServiceEx+0xca
        00000000`0120f110 00000000`7511abfe wow64cpu!TurboDispatchJumpAddressEnd+0x28
        00000000`0120f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0120f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0120f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0120f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa800485c360  Cid 06fc.0530  Teb: 000000007efa7000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004857a20  NotificationEvent
            fffffa800485c418  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800475d280       Image:         DbgSvc.exe
        Wait Start TickCount      46522          Ticks: 57 (0:00:00:00.889)
        Context Switch Count      725
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address DbgSvc (0x000000000101f955)
        Stack Init fffff9800f2cbdb0 Current fffff9800f2cb960
        Base fffff9800f2cc000 Limit fffff9800f2c6000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0f2cb9a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0f2cbae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0f2cbb40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0f2cbbc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0f2cbc20 00000000`75103cf9 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0f2cbc20)
        00000000`0150f128 00000000`75103af6 wow64cpu!CpupSyscallStub+0x9
        00000000`0150f130 00000000`7511abfe wow64cpu!Thunk0ArgReloadState+0x1a
        00000000`0150f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0150f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0150f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0150f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa800485d060  Cid 06fc.055c  Teb: 000000007efa4000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80046d1d80  NotificationEvent
            fffffa800485d118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800475d280       Image:         DbgSvc.exe
        Wait Start TickCount      46497          Ticks: 82 (0:00:00:01.279)
        Context Switch Count      156
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address DbgSvc (0x000000000101a642)
        Stack Init fffff9800f2d9db0 Current fffff9800f2d9960
        Base fffff9800f2da000 Limit fffff9800f2d4000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0f2d99a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0f2d9ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0f2d9b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0f2d9bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0f2d9c20 00000000`75103cf9 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0f2d9c20)
        00000000`0175f128 00000000`75103af6 wow64cpu!CpupSyscallStub+0x9
        00000000`0175f130 00000000`7511abfe wow64cpu!Thunk0ArgReloadState+0x1a
        00000000`0175f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0175f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0175f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0175f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa80048c1bb0  Cid 06fc.0850  Teb: 000000007efa1000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80048c3a90  NotificationEvent
            fffffa80048c1c68  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800475d280       Image:         DbgSvc.exe
        Wait Start TickCount      46518          Ticks: 61 (0:00:00:00.951)
        Context Switch Count      729
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address DbgSvc (0x0000000001015056)
        Stack Init fffff9800f27edb0 Current fffff9800f27e960
        Base fffff9800f27f000 Limit fffff9800f279000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0f27e9a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0f27eae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0f27eb40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0f27ebc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0f27ec20 00000000`75103cf9 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0f27ec20)
        00000000`017df128 00000000`75103af6 wow64cpu!CpupSyscallStub+0x9
        00000000`017df130 00000000`7511abfe wow64cpu!Thunk0ArgReloadState+0x1a
        00000000`017df1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`017df1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`017df730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`017df7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa80020ae700  Cid 06fc.0dd8  Teb: 000000007efd5000 Win32Thread: 0000000000000000
WAIT: (DelayExecution) UserMode Non-Alertable
            fffffa80020ae7b8  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800475d280       Image:         DbgSvc.exe
        Wait Start TickCount      46209          Ticks: 370 (0:00:00:05.772)
        Context Switch Count      31
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007600fc53
        Stack Init fffff9801daf5db0 Current fffff9801daf5990
        Base fffff9801daf6000 Limit fffff9801daf0000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1daf59d0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1daf5b10 fffff800`01c5b5a9 nt!KiSwapThread+0x125
        fffff980`1daf5b70 fffff800`01e8ae9d nt!KeDelayExecutionThread+0x339
        fffff980`1daf5bf0 fffff800`01c4d733 nt!NtDelayExecution+0x5c
        fffff980`1daf5c20 00000000`75103cf9 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1daf5c20)
        00000000`010af128 00000000`75103bad wow64cpu!CpupSyscallStub+0x9
        00000000`010af130 00000000`7511abfe wow64cpu!Thunk2ArgNSpNSpReloadState+0x21
        00000000`010af1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`010af1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`010af730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`010af7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa80020af730  Cid 06fc.0e0c  Teb: 000000007efad000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80018b20d0  NotificationEvent
            fffffa80020af7e8  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800475d280       Image:         DbgSvc.exe
        Wait Start TickCount      46323          Ticks: 256 (0:00:00:03.993)
        Context Switch Count      1040
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address DbgSvc (0x000000000101e9a0)
        Stack Init fffff9801db0adb0 Current fffff9801db0a960
        Base fffff9801db0b000 Limit fffff9801db05000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1db0a9a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1db0aae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`1db0ab40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`1db0abc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`1db0ac20 00000000`75103cf9 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1db0ac20)
        00000000`0112f128 00000000`75103af6 wow64cpu!CpupSyscallStub+0x9
        00000000`0112f130 00000000`7511abfe wow64cpu!Thunk0ArgReloadState+0x1a
        00000000`0112f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0112f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0112f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0112f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa80020ffbb0  Cid 06fc.0e10  Teb: 000000007ef98000 Win32Thread: fffff900c2015d60
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80020b8230  NotificationEvent
            fffffa80020ffc68  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800475d280       Image:         DbgSvc.exe
        Wait Start TickCount      46540          Ticks: 39 (0:00:00:00.608)
        Context Switch Count      1230                 LargeStack
        UserTime                  00:00:00.031
        KernelTime                00:00:00.000
        Win32 Start Address DbgSvc (0x000000000101e5cf)
        Stack Init fffff98020dd9db0 Current fffff98020dd9960
        Base fffff98020dda000 Limit fffff98020dd3000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`20dd99a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`20dd9ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`20dd9b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`20dd9bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`20dd9c20 00000000`75103cf9 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`20dd9c20)
        00000000`01d9f128 00000000`75103af6 wow64cpu!CpupSyscallStub+0x9
        00000000`01d9f130 00000000`7511abfe wow64cpu!Thunk0ArgReloadState+0x1a
        00000000`01d9f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`01d9f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`01d9f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`01d9f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa800211ca00  Cid 06fc.0e24  Teb: 000000007ef95000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8002101540  NotificationEvent
            fffffa800211cab8  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800475d280       Image:         DbgSvc.exe
        Wait Start TickCount      46296          Ticks: 283 (0:00:00:04.414)
        Context Switch Count      20
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address DbgSvc (0x0000000001018b8b)
        Stack Init fffff9801da4ddb0 Current fffff9801da4d960
        Base fffff9801da4e000 Limit fffff9801da48000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1da4d9a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1da4dae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`1da4db40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`1da4dbc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`1da4dc20 00000000`75103cf9 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1da4dc20)
        00000000`01e3f128 00000000`75103af6 wow64cpu!CpupSyscallStub+0x9
        00000000`01e3f130 00000000`7511abfe wow64cpu!Thunk0ArgReloadState+0x1a
        00000000`01e3f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`01e3f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`01e3f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`01e3f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa8002577a80  Cid 06fc.0d58  Teb: 000000007ef9b000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa800295ea50  QueueObject
            fffffa8002577b38  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800475d280       Image:         DbgSvc.exe
        Wait Start TickCount      46242          Ticks: 337 (0:00:00:05.257)
        Context Switch Count      8
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x00000000762f3242
        Stack Init fffff9800e2cfdb0 Current fffff9800e2cf810
        Base fffff9800e2d0000 Limit fffff9800e2ca000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0e2cf850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e2cf990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0e2cf9f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0e2cfa80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`0e2cfb00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`0e2cfbb0 00000000`751039a2 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e2cfc20)
        00000000`01d1f0c8 00000000`7511abfe wow64cpu!RemoveIoCompletionFault+0x41
        00000000`01d1f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`01d1f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`01d1f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`01d1f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa8001fe1930  Cid 06fc.0fa8  Teb: 000000007ef92000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa800295ea50  QueueObject
            fffffa8001fe19e8  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800475d280       Image:         DbgSvc.exe
        Wait Start TickCount      46242          Ticks: 337 (0:00:00:05.257)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x00000000762f3242
        Stack Init fffff9801a6ecdb0 Current fffff9801a6ec810
        Base fffff9801a6ed000 Limit fffff9801a6e7000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1a6ec850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1a6ec990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`1a6ec9f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`1a6eca80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`1a6ecb00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`1a6ecbb0 00000000`751039a2 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1a6ecc20)
        00000000`02bef0c8 00000000`7511abfe wow64cpu!RemoveIoCompletionFault+0x41
        00000000`02bef1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`02bef1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`02bef730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`02bef7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

DefWatch process

```
PROCESS fffffa8004a31c10
    SessionId: 0  Cid: 0720    Peb: 7efdf000  ParentCid: 025c
    DirBase: 43d6e000  ObjectTable: fffff88005865a40  HandleCount: 180.
    Image: DefWatch.exe
    VadRoot fffffa8004735640 Vads 87 Clone 0 Private 433. Modified 332. Locked 0.
    DeviceMap fffff88000007820
    Token                             fffff88005d60820
    ElapsedTime                       00:11:38.566
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         95832
    QuotaPoolUsage[NonPagedPool]      12048
    Working Set Sizes (now,min,max)  (1356, 50, 345) (5424KB, 200KB, 1380KB)
    PeakWorkingSetSize                1910
    VirtualSize                       52 Mb
    PeakVirtualSize                   58 Mb
    PageFaultCount                    2492
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      573

    Setting context for this process...
.process /p /r fffffa8004a31c10

    !peb
PEB at 000000007efdf000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         0000000000400000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00000000001d27e0 . 00000000001d2b40
    Ldr.InLoadOrderModuleList:           00000000001d26f0 . 00000000001d2ca0
    Ldr.InMemoryOrderModuleList:         00000000001d2700 . 00000000001d2cb0
            Base TimeStamp                     Module
          400000 4580ac4f Dec 14 01:43:43 2006 c:\Program Files (x86)\Symantec
AntiVirus\DefWatch.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        75110000 4549d371 Nov 02 11:16:01 2006 C:\Windows\system32\wow64.dll
        75000000 4549d374 Nov 02 11:16:04 2006 C:\Windows\system32\wow64win.dll
        75100000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\wow64cpu.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       00000000001d0000
    ProcessParameters: 00000000001d1d20
    WindowTitle:  'c:\Program Files (x86)\Symantec AntiVirus\DefWatch.exe'
    ImageFile:    'c:\Program Files (x86)\Symantec AntiVirus\DefWatch.exe'
    CommandLine:  '"c:\Program Files (x86)\Symantec AntiVirus\DefWatch.exe"'
    DllPath:      'c:\Program Files (x86)\Symantec
AntiVirus;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Windows;C:\Wind
ows\System32\Wbem'
    Environment:  00000000001d1310
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\system32\config\systemprofile\AppData\Roaming
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        LOCALAPPDATA=C:\Windows\system32\config\systemprofile\AppData\Local
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
```

```
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\TEMP
        TMP=C:\Windows\TEMP
        USERDOMAIN=DOMAIN
        USERNAME=COMPUTERNAME$
        USERPROFILE=C:\Windows\system32\config\systemprofile
        windir=C:\Windows


        THREAD fffffa8002968820  Cid 0720.0724  Teb: 000000007efdb000 Win32Thread: fffff900c07e5d60
WAIT: (Executive) UserMode Non-Alertable
            fffffa80047317a8  NotificationEvent
        IRP List:
            fffffa8004602850: (0006,0118) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004a31c10       Image:         DefWatch.exe
        Wait Start TickCount      1850           Ticks: 44729 (0:00:11:37.776)
        Context Switch Count      94                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address DefWatch (0x0000000000403751)
        Stack Init fffff9800ef54db0 Current fffff9800ef547f0
        Base fffff9800ef55000 Limit fffff9800ef4e000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0ef54830 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0ef54970 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0ef549d0 fffff800`01ebdf16 nt!KeWaitForSingleObject+0x5f5
        fffff980`0ef54a50 fffff800`01ea1a24 nt!IopSynchronousServiceTail+0x306
        fffff980`0ef54ac0 fffff800`01c4d733 nt!NtReadFile+0x583
        fffff980`0ef54bb0 00000000`75103907 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0ef54c20)
        00000000`0007ee38 00000000`7511abfe wow64cpu!ReadWriteFileFault+0x35
        00000000`0007ef10 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0007ef40 00000000`76e0e23d wow64!Wow64LdrpInitialize+0x492
        00000000`0007f4a0 00000000`76e7e974 ntdll!LdrpInitializeProcess+0x1333
        00000000`0007f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d641
        00000000`0007f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa80029625c0  Cid 0720.0730  Teb: 000000007efd8000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8002965e40  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004a31c10       Image:         DefWatch.exe
        Wait Start TickCount      1851           Ticks: 44728 (0:00:11:37.761)
        Context Switch Count      14
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x00000000767fb9d5
        Stack Init fffff9800da9edb0 Current fffff9800da9e960
        Base fffff9800da9f000 Limit fffff9800da99000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0da9e9a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0da9eae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0da9eb40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0da9ebc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0da9ec20 00000000`75103cf9 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0da9ec20)
        00000000`003bf128 00000000`75103af6 wow64cpu!CpupSyscallStub+0x9
        00000000`003bf130 00000000`7511abfe wow64cpu!Thunk0ArgReloadState+0x1a
        00000000`003bf1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`003bf1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`003bf730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`003bf7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa8002967060  Cid 0720.0744  Teb: 000000007efd5000 Win32Thread: fffff900c07ea920
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8002965cc0  SynchronizationEvent
            fffffa8002965de0  NotificationEvent
        IRP List:
            fffffa8004886010: (0006,0358) Flags: 00060000  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004a31c10       Image:         DefWatch.exe
        Wait Start TickCount      2069           Ticks: 44510 (0:00:11:34.360)
        Context Switch Count      4606                 LargeStack
        UserTime                  00:00:00.390
        KernelTime                00:00:00.499
        Win32 Start Address DefWatch (0x0000000000402570)
        Stack Init fffff9800ef67db0 Current fffff9800ef67260
        Base fffff9800ef68000 Limit fffff9800ef5f000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0ef672a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0ef673e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0ef67440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0ef674b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`0ef67960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`0ef67bb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0ef67c20)
        00000000`003ff0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`003ff1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`003ff1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`003ff730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`003ff7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa80047ec5f0  Cid 0720.0774  Teb: 000000007efad000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa80047eca80  SynchronizationTimer
            fffffa800480d140  SynchronizationEvent
            fffffa800487adf0  SynchronizationEvent
            fffffa8004765670  SynchronizationEvent
            fffffa8004883900  SynchronizationEvent
            fffffa8004880540  SynchronizationEvent
            fffffa8004883720  SynchronizationEvent
            fffffa8004891530  SynchronizationEvent
            fffffa80048830d0  SynchronizationEvent
            fffffa800481f390  SynchronizationEvent
            fffffa8004883e10  SynchronizationEvent
            fffffa8004892a80  SynchronizationEvent
            fffffa8004892b60  SynchronizationEvent
            fffffa8004892b00  SynchronizationEvent
            fffffa8004892de0  SynchronizationEvent
            fffffa80048834c0  SynchronizationEvent
            fffffa80048833e0  SynchronizationEvent
            fffffa80048157f0  SynchronizationEvent
            fffffa80048929f8  NotificationEvent
            fffffa8004884510  SynchronizationEvent
            fffffa80048922e0  SynchronizationEvent
            fffffa8004847d00  SynchronizationEvent
            fffffa8004884930  SynchronizationEvent
            fffffa80048939c0  SynchronizationEvent
            fffffa8004828e20  SynchronizationEvent
            fffffa8004883fe0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004a31c10       Image:         DefWatch.exe
        Wait Start TickCount      1898           Ticks: 44681 (0:00:11:37.028)
        Context Switch Count      42
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x0000000077046235
        Stack Init fffff9800ea99db0 Current fffff9800ea99260
        Base fffff9800ea9a000 Limit fffff9800ea94000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0ea992a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0ea993e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0ea99440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0ea994b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`0ea99960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`0ea99bb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0ea99c20)
        00000000`00aef0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`00aef1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`00aef1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`00aef730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`00aef7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa8004885480  Cid 0720.0688  Teb: 000000007efa7000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8004882c70  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004a31c10       Image:         DefWatch.exe
        Wait Start TickCount      3820           Ticks: 42759 (0:00:11:07.044)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x00000000762f3242
        Stack Init fffff9800d0cfdb0 Current fffff9800d0cf810
        Base fffff9800d0d0000 Limit fffff9800d0ca000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0d0cf850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0d0cf990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0d0cf9f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0d0cfa80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`0d0cfb00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`0d0cfbb0 00000000`751039a2 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0d0cfc20)
        00000000`00c4f0c8 00000000`7511abfe wow64cpu!RemoveIoCompletionFault+0x41
        00000000`00c4f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`00c4f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`00c4f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`00c4f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

Svchost process (NetworkServiceNetworkRestricted)

```
PROCESS fffffa80047fb780
    SessionId: 0  Cid: 0760    Peb: 7fffffde000  ParentCid: 025c
    DirBase: 437fb000  ObjectTable: fffff88005e3a4d0  HandleCount: 108.
    Image: svchost.exe
    VadRoot fffffa80048043c0 Vads 76 Clone 0 Private 464. Modified 291. Locked 0.
    DeviceMap fffff8800598a680
    Token                             fffff88005d91060
    ElapsedTime                       00:11:38.385
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         81208
    QuotaPoolUsage[NonPagedPool]      8816
    Working Set Sizes (now,min,max)  (1126, 50, 345) (4504KB, 200KB, 1380KB)
    PeakWorkingSetSize                1474
    VirtualSize                       41 Mb
    PeakVirtualSize                   41 Mb
    PageFaultCount                    1676
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      623

    Setting context for this process...
.process /p /r fffffa80047fb780

    !peb
PEB at 000007fffffde000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00000000ff910000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00000000003b27f0 . 00000000003e10c0
    Ldr.InLoadOrderModuleList:           00000000003b2700 . 000000000040c0c0
    Ldr.InMemoryOrderModuleList:         00000000003b2710 . 000000000040c0d0
            Base TimeStamp                     Module
        ff910000 4549b5f5 Nov 02 09:10:13 2006 C:\Windows\system32\svchost.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        76bc0000 4549d328 Nov 02 11:14:48 2006 C:\Windows\system32\kernel32.dll
     7fefdd40000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\system32\msvcrt.dll
     7fefea30000 4549d267 Nov 02 11:11:35 2006 C:\Windows\system32\ADVAPI32.dll
     7fefed90000 469c43bb Jul 17 05:21:15 2007 C:\Windows\system32\RPCRT4.dll
     7fefa2d0000 4549d2ee Nov 02 11:13:50 2006 c:\windows\system32\ipsecsvc.dll
     7fefd360000 4549d265 Nov 02 11:11:33 2006 c:\windows\system32\AUTHZ.dll
     7fefcb80000 4549d2e1 Nov 02 11:13:37 2006 c:\windows\system32\IPHLPAPI.DLL
     7fefcb30000 4549d263 Nov 02 11:11:31 2006 c:\windows\system32\dhcpcsvc.DLL
     7fefce40000 4549d288 Nov 02 11:12:08 2006 c:\windows\system32\DNSAPI.dll
     7fefd540000 4549d38a Nov 02 11:16:26 2006 C:\Windows\system32\WS2_32.dll
     7feff0b0000 4549d370 Nov 02 11:16:00 2006 C:\Windows\system32\NSI.dll
     7fefd390000 4549d33f Nov 02 11:15:11 2006 c:\windows\system32\Secur32.dll
     7fefd280000 4549d370 Nov 02 11:16:00 2006 c:\windows\system32\WINNSI.DLL
     7fefcb00000 4549d264 Nov 02 11:11:32 2006 c:\windows\system32\dhcpcsvc6.DLL
     7fefcc50000 4549d344 Nov 02 11:15:16 2006 c:\windows\system32\CRYPT32.dll
        76d00000 45d3ee19 Feb 15 05:22:33 2007 C:\Windows\system32\USER32.dll
     7fefec20000 4549d273 Nov 02 11:11:47 2006 C:\Windows\system32\GDI32.dll
     7fefce00000 4549d2df Nov 02 11:13:35 2006 c:\windows\system32\MSASN1.dll
     7fefd3b0000 4549d336 Nov 02 11:15:02 2006 c:\windows\system32\USERENV.dll
     7fefac60000 4549d280 Nov 02 11:12:00 2006 c:\windows\system32\fwpuclnt.dll
     7fefc460000 466785ee Jun 07 05:13:34 2007 c:\windows\system32\FirewallAPI.dll
     7fefdab0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\OLEAUT32.dll
     7fefd760000 4549d317 Nov 02 11:14:31 2006 C:\Windows\system32\ole32.dll
     7fefca50000 4549d336 Nov 02 11:15:02 2006 c:\windows\system32\VERSION.dll
     7fefa620000 4549d281 Nov 02 11:12:01 2006 c:\windows\system32\FwRemoteSvr.DLL
     7fefd590000 4549d396 Nov 02 11:16:38 2006 C:\Windows\system32\WLDAP32.dll
     7fefd530000 4549d310 Nov 02 11:14:24 2006 C:\Windows\system32\PSAPI.DLL
```

```
     7fefd9e0000 4549d2cb Nov 02 11:13:15 2006 C:\Windows\system32\IMM32.DLL
     7fefdc30000 4549d2e6 Nov 02 11:13:42 2006 C:\Windows\system32\MSCTF.dll
     7feff0c0000 4549d2a1 Nov 02 11:12:33 2006 C:\Windows\system32\LPK.DLL
     7fefd940000 4549d337 Nov 02 11:15:03 2006 C:\Windows\system32\USP10.dll
     7fefc8f0000 4549d2e7 Nov 02 11:13:43 2006 C:\Windows\system32\mswsock.dll
     7fefc560000 4549d3a3 Nov 02 11:16:51 2006 C:\Windows\system32\wshtcpip.dll
     7fefc980000 4549d39d Nov 02 11:16:45 2006 C:\Windows\System32\wship6.dll
     7fefca40000 4549d341 Nov 02 11:15:13 2006 C:\Windows\system32\credssp.dll
     7fefc670000 4549d321 Nov 02 11:14:41 2006 C:\Windows\system32\schannel.dll
     7fefcf70000 4549d2fc Nov 02 11:14:04 2006 C:\Windows\system32\NETAPI32.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       00000000003b0000
    ProcessParameters: 00000000003b1da0
    WindowTitle:  'C:\Windows\system32\svchost.exe'
    ImageFile:    'C:\Windows\system32\svchost.exe'
    CommandLine:  'C:\Windows\system32\svchost.exe -k NetworkServiceNetworkRestricted'
    DllPath:
'C:\Windows\system32;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Wind
ows;C:\Windows\System32\Wbem'
    Environment:  00000000003b1310
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        LOCALAPPDATA=C:\Windows\ServiceProfiles\NetworkService\AppData\Local
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\SERVIC~2\NETWOR~1\AppData\Local\Temp
        TMP=C:\Windows\SERVIC~2\NETWOR~1\AppData\Local\Temp
        USERDOMAIN=DOMAIN
        USERNAME=COMPUTERNAME$
        USERPROFILE=C:\Windows\ServiceProfiles\NetworkService
        windir=C:\Windows
```

```
        THREAD fffffa8004771760  Cid 0760.0764  Teb: 000007fffffdc000 Win32Thread: 0000000000000000
WAIT: (Executive) UserMode Non-Alertable
            fffffa80047fc898  NotificationEvent
        IRP List:
            fffffa80047713d0: (0006,0118) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa80047fb780       Image:         svchost.exe
        Wait Start TickCount      1861           Ticks: 44718 (0:00:11:37.605)
        Context Switch Count      35
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address svchost!wmainCRTStartup (0x00000000ff912550)
        Stack Init fffff9800e718db0 Current fffff9800e7187f0
        Base fffff9800e719000 Limit fffff9800e713000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e718830 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e718970 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0e7189d0 fffff800`01ebdf16 nt!KeWaitForSingleObject+0x5f5
        fffff980`0e718a50 fffff800`01ea1a24 nt!IopSynchronousServiceTail+0x306
        fffff980`0e718ac0 fffff800`01c4d733 nt!NtReadFile+0x583
        fffff980`0e718bb0 00000000`76e202da nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e718c20)
        00000000`0025f5d8 00000000`76bf26da ntdll!NtReadFile+0xa
        00000000`0025f5e0 000007fe`fea865aa kernel32!ReadFile+0x8a
        00000000`0025f670 000007fe`fea862e3 ADVAPI32!ScGetPipeInput+0x4a
        00000000`0025f750 000007fe`fea850f3 ADVAPI32!ScDispatcherLoop+0x9a
        00000000`0025f850 00000000`ff91283c ADVAPI32!StartServiceCtrlDispatcherW+0x176
        00000000`0025faf0 00000000`ff912666 svchost!wmain+0xe5
        00000000`0025fb20 00000000`76bfcdcd svchost!ScCreateWellKnownSids+0x301
        00000000`0025fb60 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0025fb90 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800477f7b0  Cid 0760.0770  Teb: 000007fffffda000 Win32Thread: fffff900c07eca60
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004865b20  NotificationEvent
            fffffa8004831970  NotificationEvent
            fffffa8004846170  NotificationEvent
            fffffa8004888150  NotificationEvent
            fffffa8002954680  NotificationEvent
            fffffa8004874150  NotificationEvent
            fffffa800485c0b0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa80047fb780       Image:         svchost.exe
        Wait Start TickCount      2048           Ticks: 44531 (0:00:11:34.688)
        Context Switch Count      819                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.062
        Win32 Start Address ADVAPI32!ScSvcctrlThreadW (0x000007fefea84bd0)
        Stack Init fffff9800efecdb0 Current fffff9800efec260
        Base fffff9800efed000 Limit fffff9800efe6000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0efec2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0efec3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0efec440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0efec4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0efec960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0efecbb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0efecc20)
        00000000`0094f528 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0094f530 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0094f640 000007fe`fa2d198c kernel32!WaitForMultipleObjects+0x11
        00000000`0094f680 000007fe`fa2d442d ipsecsvc!ServiceWait+0x1c7
        00000000`0094f730 00000000`ff911771 ipsecsvc!SpdServiceMain+0x479
        00000000`0094f790 000007fe`fea84bf5 svchost!ServiceStarter+0x1ea
        00000000`0094f820 00000000`76bfcdcd ADVAPI32!ScSvcctrlThreadW+0x25
        00000000`0094f850 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0094f880 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa800485d5b0  Cid 0760.0588  Teb: 000007fffffd8000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa800485dcc0  SynchronizationTimer
            fffffa800485dfe0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa80047fb780       Image:         svchost.exe
        Wait Start TickCount      2048           Ticks: 44531 (0:00:11:34.688)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x0000000076df6930)
        Stack Init fffff9800f270db0 Current fffff9800f270260
        Base fffff9800f271000 Limit fffff9800f26b000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0f2702a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0f2703e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0f270440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0f2704b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0f270960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0f270bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0f270c20)
        00000000`013dfc78 00000000`76df6b07 ntdll!NtWaitForMultipleObjects+0xa
        00000000`013dfc80 00000000`76bfcdcd ntdll!TppWaiterpThread+0x14d
        00000000`013dff20 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`013dff50 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800485e9b0  Cid 0760.0624  Teb: 000007fffffd6000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Alertable
            fffffa800485df50  QueueObject
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa80047fb780       Image:         svchost.exe
        Wait Start TickCount      2048           Ticks: 44531 (0:00:11:34.688)
        Context Switch Count      10
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x0000000076e17860)
        Stack Init fffff980103c0db0 Current fffff980103c0860
        Base fffff980103c1000 Limit fffff980103bb000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`103c08a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`103c09e0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`103c0a40 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`103c0ad0 fffff800`01c8a722 nt!IoRemoveIoCompletion+0x47
        fffff980`103c0b50 fffff800`01c4d733 nt!NtWaitForWorkViaWorkerFactory+0x1f1
        fffff980`103c0c20 00000000`76e21b4a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`103c0c20)
        00000000`01affa88 00000000`76e17a20 ntdll!NtWaitForWorkViaWorkerFactory+0xa
        00000000`01affa90 00000000`76bfcdcd ntdll!TppWorkerThread+0x23e
        00000000`01affd00 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`01affd30 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004879bb0  Cid 0760.06bc  Teb: 000007fffffd4000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8004856380  QueueObject
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa80047fb780       Image:         svchost.exe
        Wait Start TickCount      5741           Ticks: 40838 (0:00:10:37.076)
        Context Switch Count      12
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff980103e3db0 Current fffff980103e3810
        Base fffff980103e4000 Limit fffff980103de000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`103e3850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`103e3990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`103e39f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`103e3a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`103e3b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`103e3bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`103e3c20)
        00000000`01baf998 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`01baf9a0 000007fe`fedce7a3 kernel32!GetQueuedCompletionStatus+0x48
        00000000`01bafa00 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`01bafa90 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`01bafb40 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`01bafb70 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`01bafbb0 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`01bafbe0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`01bafc10 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

Svchost process (WerSvcGroup)

```
PROCESS fffffa800480ab70
    SessionId: 0  Cid: 07b4    Peb: 7fffffd5000  ParentCid: 025c
    DirBase: 42a82000  ObjectTable: fffff88005cec890  HandleCount:  44.
    Image: svchost.exe
    VadRoot fffffa80048064a0 Vads 34 Clone 0 Private 225. Modified 139. Locked 0.
    DeviceMap fffff88000007820
    Token                             fffff88005de2490
    ElapsedTime                       00:11:38.248
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         33456
    QuotaPoolUsage[NonPagedPool]      3296
    Working Set Sizes (now,min,max)  (598, 50, 345) (2392KB, 200KB, 1380KB)
    PeakWorkingSetSize                757
    VirtualSize                       18 Mb
    PeakVirtualSize                   18 Mb
    PageFaultCount                    782
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      292

    Setting context for this process...
.process /p /r fffffa800480ab70

    !peb
PEB at 000007fffffd5000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00000000ff910000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00000000002a2740 . 00000000002d20d0
    Ldr.InLoadOrderModuleList:           00000000002a2650 . 00000000002d20b0
    Ldr.InMemoryOrderModuleList:         00000000002a2660 . 00000000002d20c0
            Base TimeStamp                     Module
        ff910000 4549b5f5 Nov 02 09:10:13 2006 C:\Windows\System32\svchost.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        76bc0000 4549d328 Nov 02 11:14:48 2006 C:\Windows\system32\kernel32.dll
     7fefdd40000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\system32\msvcrt.dll
     7fefea30000 4549d267 Nov 02 11:11:35 2006 C:\Windows\system32\ADVAPI32.dll
     7fefed90000 469c43bb Jul 17 05:21:15 2007 C:\Windows\system32\RPCRT4.dll
     7fefa200000 4549d347 Nov 02 11:15:19 2006 c:\windows\system32\wersvc.dll
     7fefc450000 4549d34e Nov 02 11:15:26 2006 C:\Windows\System32\WTSAPI32.dll
     7fefd1b0000 4549d380 Nov 02 11:16:16 2006 C:\Windows\System32\WINSTA.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       00000000002a0000
    ProcessParameters: 00000000002a1d20
    WindowTitle:  'C:\Windows\System32\svchost.exe'
    ImageFile:    'C:\Windows\System32\svchost.exe'
    CommandLine:  'C:\Windows\System32\svchost.exe -k WerSvcGroup'
    DllPath:
'C:\Windows\System32;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Wind
ows;C:\Windows\System32\Wbem'
    Environment:  00000000002a1310
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\system32\config\systemprofile\AppData\Roaming
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        LOCALAPPDATA=C:\Windows\system32\config\systemprofile\AppData\Local
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
```

```
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public

        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\TEMP
        TMP=C:\Windows\TEMP
        USERDOMAIN=DOMAIN
        USERNAME=COMPUTERNAME$
        USERPROFILE=C:\Windows\system32\config\systemprofile

        windir=C:\Windows


        THREAD fffffa800477c740  Cid 07b4.07b8  Teb: 000007fffffde000 Win32Thread: 0000000000000000
WAIT: (Executive) UserMode Non-Alertable
            fffffa80048031d8  NotificationEvent
        IRP List:
            fffffa800296c120: (0006,0118) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800480ab70       Image:         svchost.exe
        Wait Start TickCount      2776           Ticks: 43803 (0:00:11:23.331)
        Context Switch Count      63
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address svchost!wmainCRTStartup (0x00000000ff912550)
        Stack Init fffff9800f3b2db0 Current fffff9800f3b27f0
        Base fffff9800f3b3000 Limit fffff9800f3ad000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0f3b2830 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0f3b2970 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0f3b29d0 fffff800`01ebdf16 nt!KeWaitForSingleObject+0x5f5
        fffff980`0f3b2a50 fffff800`01ea1a24 nt!IopSynchronousServiceTail+0x306
        fffff980`0f3b2ac0 fffff800`01c4d733 nt!NtReadFile+0x583
        fffff980`0f3b2bb0 00000000`76e202da nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0f3b2c20)
        00000000`0016f568 00000000`76bf26da ntdll!NtReadFile+0xa
        00000000`0016f570 000007fe`fea865aa kernel32!ReadFile+0x8a
        00000000`0016f600 000007fe`fea862e3 ADVAPI32!ScGetPipeInput+0x4a
        00000000`0016f6e0 000007fe`fea850f3 ADVAPI32!ScDispatcherLoop+0x9a
        00000000`0016f7e0 00000000`ff91283c ADVAPI32!StartServiceCtrlDispatcherW+0x176
        00000000`0016fa80 00000000`ff912666 svchost!wmain+0xe5
        00000000`0016fab0 00000000`76bfcdcd svchost!ScCreateWellKnownSids+0x301
        00000000`0016faf0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0016fb20 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004834a30  Cid 07b4.07e8  Teb: 000007fffffda000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa800481f9e0  SynchronizationTimer
            fffffa800482e250  NotificationEvent
            fffffa8004859d40  SynchronizationEvent
            fffffa8004860228  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800480ab70       Image:         svchost.exe
        Wait Start TickCount      21851          Ticks: 24728 (0:00:06:25.759)
        Context Switch Count      70
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x0000000076df6930)
        Stack Init fffff9800f2a8db0 Current fffff9800f2a8260
        Base fffff9800f2a9000 Limit fffff9800f2a3000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0f2a82a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0f2a83e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0f2a8440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0f2a84b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0f2a8960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0f2a8bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0f2a8c20)
        00000000`000cfc88 00000000`76df6b07 ntdll!NtWaitForMultipleObjects+0xa
        00000000`000cfc90 00000000`76bfcdcd ntdll!TppWaiterpThread+0x14d
        00000000`000cff30 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`000cff60 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004666590  Cid 07b4.0470  Teb: 000007fffffd8000 Win32Thread: 0000000000000000
WAIT: (WrLpcReceive) UserMode Non-Alertable
            fffffa8004666920  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800480ab70       Image:         svchost.exe
        Wait Start TickCount      1880           Ticks: 44699 (0:00:11:37.308)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wersvc!CWerService::StaticLpcServerThread (0x000007fefa206cac)
        Stack Init fffff9800f3ffdb0 Current fffff9800f3ff7a0
        Base fffff9800f400000 Limit fffff9800f3fa000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0f3ff7e0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0f3ff920 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0f3ff980 fffff800`01eb3788 nt!KeWaitForSingleObject+0x5f5
        fffff980`0f3ffa00 fffff800`01eb3eda nt!AlpcpReceiveMessagePort+0x298
        fffff980`0f3ffa60 fffff800`01eb74ba nt!AlpcpReceiveMessage+0x246
        fffff980`0f3ffb00 fffff800`01c4d733 nt!NtAlpcSendWaitReceivePort+0x1da
        fffff980`0f3ffbb0 00000000`76e20aca nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0f3ffc20)
        00000000`0029f458 000007fe`fa206d8d ntdll!NtAlpcSendWaitReceivePort+0xa
        00000000`0029f460 000007fe`fa206cb5 wersvc!CWerService::LpcServerThread+0xc9
        00000000`0029fa00 00000000`76bfcdcd wersvc!CWerService::StaticLpcServerThread+0x9
        00000000`0029fa30 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0029fa60 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80046a77f0  Cid 07b4.0430  Teb: 000007fffffd6000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Alertable
            fffffa800481f950  QueueObject
        IRP List:
            fffffa80046128b0: (0006,03a0) Flags: 00060000  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800480ab70       Image:         svchost.exe
        Wait Start TickCount      21851          Ticks: 24728 (0:00:06:25.759)
        Context Switch Count      94
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x0000000076e17860)
        Stack Init fffff9800f2bddb0 Current fffff9800f2bd860
        Base fffff9800f2be000 Limit fffff9800f2b8000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0f2bd8a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0f2bd9e0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0f2bda40 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0f2bdad0 fffff800`01c8a722 nt!IoRemoveIoCompletion+0x47
        fffff980`0f2bdb50 fffff800`01c4d733 nt!NtWaitForWorkViaWorkerFactory+0x1f1
        fffff980`0f2bdc20 00000000`76e21b4a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0f2bdc20)
        00000000`00a4f8e8 00000000`76e17a20 ntdll!NtWaitForWorkViaWorkerFactory+0xa
        00000000`00a4f8f0 00000000`76bfcdcd ntdll!TppWorkerThread+0x23e
        00000000`00a4fb60 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`00a4fb90 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

SearchIndexer process

```
PROCESS fffffa8004812870
    SessionId: 0  Cid: 07c8    Peb: 7fffffd3000  ParentCid: 025c
    DirBase: 42f48000  ObjectTable: fffff880060280e0  HandleCount: 716.
    Image: SearchIndexer.exe
    VadRoot fffffa80048e7ca0 Vads 242 Clone 0 Private 3508. Modified 2063. Locked 1.
    DeviceMap fffff88000007820
    Token                             fffff88005cecaa0
    ElapsedTime                       00:11:38.213
    UserTime                          00:00:00.249
    KernelTime                        00:00:00.265
    QuotaPoolUsage[PagedPool]         195008
    QuotaPoolUsage[NonPagedPool]      23744
    Working Set Sizes (now,min,max)  (4528, 50, 345) (18112KB, 200KB, 1380KB)
    PeakWorkingSetSize                5476
    VirtualSize                       160 Mb
    PeakVirtualSize                   185 Mb
    PageFaultCount                    10490
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      11253

    Setting context for this process...
.process /p /r fffffa8004812870

    !peb
PEB at 000007fffffd3000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00000000ffa70000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 0000000000302760 . 00000000072be1c0
    Ldr.InLoadOrderModuleList:           0000000000302670 . 00000000072be1a0
    Ldr.InMemoryOrderModuleList:         0000000000302680 . 00000000072be1b0
            Base TimeStamp                     Module
        ffa70000 4549c44a Nov 02 10:11:22 2006 C:\Windows\system32\SearchIndexer.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        76bc0000 4549d328 Nov 02 11:14:48 2006 C:\Windows\system32\kernel32.dll
     7fefea30000 4549d267 Nov 02 11:11:35 2006 C:\Windows\system32\ADVAPI32.dll
     7fefed90000 469c43bb Jul 17 05:21:15 2007 C:\Windows\system32\RPCRT4.dll
        76d00000 45d3ee19 Feb 15 05:22:33 2007 C:\Windows\system32\USER32.dll
     7fefec20000 4549d273 Nov 02 11:11:47 2006 C:\Windows\system32\GDI32.dll
     7fefdd40000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\system32\msvcrt.dll
     7fefd760000 4549d317 Nov 02 11:14:31 2006 C:\Windows\system32\ole32.dll
     7fefdab0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\OLEAUT32.dll
     7fef9a30000 4549d355 Nov 02 11:15:33 2006 C:\Windows\system32\TQUERY.DLL
     7fefb4d0000 4549d30d Nov 02 11:14:21 2006 C:\Windows\system32\PROPSYS.dll
     7fefcf70000 4549d2fc Nov 02 11:14:04 2006 C:\Windows\system32\NETAPI32.dll
     7fefd530000 4549d310 Nov 02 11:14:24 2006 C:\Windows\system32\PSAPI.DLL
     7fefc1e0000 4549d381 Nov 02 11:16:17 2006 C:\Windows\system32\WINTRUST.dll
     7fefcc50000 4549d344 Nov 02 11:15:16 2006 C:\Windows\system32\CRYPT32.dll
     7fefce00000 4549d2df Nov 02 11:13:35 2006 C:\Windows\system32\MSASN1.dll
     7fefd3b0000 4549d336 Nov 02 11:15:02 2006 C:\Windows\system32\USERENV.dll
     7fefd390000 4549d33f Nov 02 11:15:11 2006 C:\Windows\system32\Secur32.dll
     7fefda90000 462443ee Apr 17 04:50:06 2007 C:\Windows\system32\imagehlp.dll
     7fefda10000 4549d31f Nov 02 11:14:39 2006 C:\Windows\system32\SHLWAPI.dll
     7fef9820000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\query.dll
     7fefddf0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\SHELL32.dll
     7fefcd90000 4549d2b2 Nov 02 11:12:50 2006 C:\Windows\system32\MPR.dll
     7fefd9e0000 4549d2cb Nov 02 11:13:15 2006 C:\Windows\system32\IMM32.DLL
     7fefdc30000 4549d2e6 Nov 02 11:13:42 2006 C:\Windows\system32\MSCTF.dll
     7feff0c0000 4549d2a1 Nov 02 11:12:33 2006 C:\Windows\system32\LPK.DLL
     7fefd940000 4549d337 Nov 02 11:15:03 2006 C:\Windows\system32\USP10.dll
```

```
     7fefbe70000 4549d32b Nov 02 11:14:51 2006 C:\Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_1559f1c6f365a7fa\comctl32.dll
     7fefdb90000 4549d282 Nov 02 11:12:02 2006 C:\Windows\system32\CLBCatQ.DLL
     7fefa410000 4549d2ce Nov 02 11:13:18 2006 C:\Windows\system32\msstrc.dll
     7fefca40000 4549d341 Nov 02 11:15:13 2006 C:\Windows\system32\credssp.dll
     7fefc670000 4549d321 Nov 02 11:14:41 2006 C:\Windows\system32\schannel.dll
     7fef93c0000 4549d2cd Nov 02 11:13:17 2006 C:\Windows\system32\mssrch.dll
     7fefc450000 4549d34e Nov 02 11:15:26 2006 C:\Windows\system32\WTSAPI32.dll
     7fef9e30000 4549d262 Nov 02 11:11:30 2006 C:\Windows\system32\dbghelp.dll
     7fefca50000 4549d336 Nov 02 11:15:02 2006 C:\Windows\system32\VERSION.dll
     7fefa440000 4549d31e Nov 02 11:14:38 2006 C:\Windows\system32\Msidle.dll
     7fefd1b0000 4549d380 Nov 02 11:16:16 2006 C:\Windows\system32\WINSTA.dll
     7fefc620000 4549d31d Nov 02 11:14:37 2006 C:\Windows\system32\rsaenh.dll
     7fef9780000 4549d30c Nov 02 11:14:20 2006 C:\Windows\system32\propdefs.dll
     7fef9000000 4549c411 Nov 02 10:10:25 2006 C:\Windows\system32\en-us\tQuery.dll.mui
     7fef8cf0000 4549d2e8 Nov 02 11:13:44 2006 C:\Windows\system32\esent.dll
     7fefa430000 4549d2c0 Nov 02 11:13:04 2006 C:\Windows\system32\msscb.dll
     7fefcc20000 4549d32d Nov 02 11:14:53 2006 C:\Windows\system32\slc.dll
     7fefa800000 4549d33f Nov 02 11:15:11 2006 C:\Windows\system32\VSSAPI.DLL
     7fefc180000 4549d253 Nov 02 11:11:15 2006 C:\Windows\system32\ATL.DLL
     7fefa9a0000 4549d341 Nov 02 11:15:13 2006 C:\Windows\system32\vsstrace.dll
     7fefd360000 4549d265 Nov 02 11:11:33 2006 C:\Windows\system32\AUTHZ.dll
     7fefb930000 4549d350 Nov 02 11:15:28 2006 C:\Windows\system32\XmlLite.dll
     7fefeed0000 4549d318 Nov 02 11:14:32 2006 C:\Windows\system32\SETUPAPI.dll
     7fefce20000 4549d315 Nov 02 11:14:29 2006 C:\Windows\system32\SAMLIB.dll
     7fefba70000 4549d2e7 Nov 02 11:13:43 2006 C:\Windows\system32\es.dll
     7fefd310000 4549d247 Nov 02 11:11:03 2006 C:\Windows\system32\apphelp.dll
     7fefc5b0000 4549d384 Nov 02 11:16:20 2006 C:\Windows\system32\NTMARTA.DLL
     7fefd590000 4549d396 Nov 02 11:16:38 2006 C:\Windows\system32\WLDAP32.dll
     7fefd540000 4549d38a Nov 02 11:16:26 2006 C:\Windows\system32\WS2_32.dll
     7feff0b0000 4549d370 Nov 02 11:16:00 2006 C:\Windows\system32\NSI.dll
     7fef6b90000 4549d2ea Nov 02 11:13:46 2006 C:\Windows\System32\NaturalLanguage6.dll
     7fefb3a0000 4549d2cc Nov 02 11:13:16 2006 C:\Windows\system32\mssprxy.dll
     7fefd1f0000 4549d32f Nov 02 11:14:55 2006 C:\Windows\system32\SXS.DLL
     7fef83b0000 4549d319 Nov 02 11:14:33 2006 C:\Windows\System32\shdocvw.dll
     7fef7720000 4549d256 Nov 02 11:11:18 2006 C:\Windows\system32\actxprxy.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       0000000000300000
    ProcessParameters: 0000000000301d20
    WindowTitle:  'C:\Windows\system32\SearchIndexer.exe'
    ImageFile:    'C:\Windows\system32\SearchIndexer.exe'
    CommandLine:  'C:\Windows\system32\SearchIndexer.exe /Embedding'
    DllPath:
'C:\Windows\system32;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Wind
ows;C:\Windows\System32\Wbem'
    Environment:  000000000035c630
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\system32\config\systemprofile\AppData\Roaming
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        LOCALAPPDATA=C:\Windows\system32\config\systemprofile\AppData\Local
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\system32
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\ProgramData\Microsoft\Search\Data\Temp\usgthrsvc
        TMP=C:\ProgramData\Microsoft\Search\Data\Temp\usgthrsvc
```

```
        USERDOMAIN=DOMAIN
        USERNAME=COMPUTERNAME$
        USERPROFILE=C:\Windows\system32\config\systemprofile
        windir=C:\Windows


        THREAD fffffa800480f470  Cid 07c8.07cc  Teb: 000007fffffde000 Win32Thread: fffff900c07ee640
WAIT: (Executive) UserMode Non-Alertable
            fffffa8004858e98  NotificationEvent
        IRP List:
            fffffa80043dd4f0: (0006,0118) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004812870       Image:         SearchIndexer.exe
        Wait Start TickCount      2778           Ticks: 43801 (0:00:11:23.299)
        Context Switch Count      468                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.046
        Win32 Start Address SearchIndexer!WinMainCRTStartup (0x00000000ffab9994)
        Stack Init fffff9800efd9db0 Current fffff9800efd97f0
        Base fffff9800efda000 Limit fffff9800efd2000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0efd9830 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0efd9970 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0efd99d0 fffff800`01ebdf16 nt!KeWaitForSingleObject+0x5f5
        fffff980`0efd9a50 fffff800`01ea1a24 nt!IopSynchronousServiceTail+0x306
        fffff980`0efd9ac0 fffff800`01c4d733 nt!NtReadFile+0x583
        fffff980`0efd9bb0 00000000`76e202da nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0efd9c20)
        00000000`0012f258 00000000`76bf26da ntdll!NtReadFile+0xa
        00000000`0012f260 000007fe`fea865aa kernel32!ReadFile+0x8a
        00000000`0012f2f0 000007fe`fea862e3 ADVAPI32!ScGetPipeInput+0x4a
        00000000`0012f3d0 000007fe`fea850f3 ADVAPI32!ScDispatcherLoop+0x9a
        00000000`0012f4d0 00000000`ffa89e50 ADVAPI32!StartServiceCtrlDispatcherW+0x176
        00000000`0012f770 00000000`ffab97eb SearchIndexer!WinMain+0x62c
        00000000`0012fac0 00000000`76bfcdcd SearchIndexer!ATL::CAtlBaseModule::CAtlBaseModule+0x2e7
        00000000`0012fb80 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0012fbb0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004857060  Cid 07c8.04bc  Teb: 000007fffffdc000 Win32Thread: fffff900c07ec640
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80048564e0  SynchronizationEvent
            fffffa8004856480  SynchronizationEvent
            fffffa800449aa00  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004812870       Image:         SearchIndexer.exe
        Wait Start TickCount      2255           Ticks: 44324 (0:00:11:31.458)
        Context Switch Count      9451                 LargeStack
        UserTime                  00:00:00.078
        KernelTime                00:00:00.780
        Win32 Start Address ADVAPI32!ScSvcctrlThreadW (0x000007fefea84bd0)
        Stack Init fffff9800ef7adb0 Current fffff9800ef7a260
        Base fffff9800ef7b000 Limit fffff9800ef73000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0ef7a2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0ef7a3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0ef7a440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0ef7a4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0ef7a960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0ef7abb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0ef7ac20)
        00000000`016eed18 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`016eed20 00000000`76d1e96d kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`016eee30 00000000`76d1e85e USER32!RealMsgWaitForMultipleObjectsEx+0x129
        00000000`016eeed0 00000000`76d13680 USER32!MsgWaitForMultipleObjectsEx+0x46
        00000000`016eef10 00000000`ffa966fe USER32!MsgWaitForMultipleObjects+0x20
        00000000`016eef50 00000000`ffa96241 SearchIndexer!CDcomService::Listen+0x2ba
        00000000`016ef970 000007fe`fea84bf5 SearchIndexer!CDcomService::ServiceMain+0x2ed
        00000000`016efea0 00000000`76bfcdcd ADVAPI32!ScSvcctrlThreadW+0x25
        00000000`016efed0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`016eff00 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80048e5bb0  Cid 07c8.0860  Teb: 000007fffffd6000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80048de6c0  SynchronizationEvent
            fffffa80048e5af0  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004812870       Image:         SearchIndexer.exe
        Wait Start TickCount      1958           Ticks: 44621 (0:00:11:36.092)
        Context Switch Count      9
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address esent!UtilThreadIThreadBase (0x000007fef8cf8db0)
        Stack Init fffff980102c4db0 Current fffff980102c4260
        Base fffff980102c5000 Limit fffff980102bf000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`102c42a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`102c43e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`102c4440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`102c44b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`102c4960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`102c4bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`102c4c20)
        00000000`0292f458 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0292f460 000007fe`f8cf86e3 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0292f570 000007fe`f8cf8dd5 esent!UtilPerfThread+0xa8
        00000000`0292f860 00000000`76bfcdcd esent!UtilThreadIThreadBase+0x21
        00000000`0292f8a0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0292f8d0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004689bb0  Cid 07c8.08c0  Teb: 000007fffffae000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa80046e95b0  SynchronizationTimer
            fffffa80048e6360  SynchronizationTimer
            fffffa80046993e0  SynchronizationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004812870       Image:         SearchIndexer.exe
        Wait Start TickCount      46354          Ticks: 225 (0:00:00:03.510)
        Context Switch Count      553
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x0000000076df6930)
        Stack Init fffff98010866db0 Current fffff98010866260
        Base fffff98010867000 Limit fffff98010861000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`108662a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`108663e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`10866440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`108664b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`10866960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`10866bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`10866c20)
        00000000`05e4fc58 00000000`76df6b07 ntdll!NtWaitForMultipleObjects+0xa
        00000000`05e4fc60 00000000`76bfcdcd ntdll!TppWaiterpThread+0x14d
        00000000`05e4ff00 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`05e4ff30 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80046d4af0  Cid 07c8.08d4  Teb: 000007fffffac000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa80048de450  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004812870       Image:         SearchIndexer.exe
        Wait Start TickCount      22296          Ticks: 24283 (0:00:06:18.817)
        Context Switch Count      404
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address esent!UtilThreadIThreadBase (0x000007fef8cf8db0)
        Stack Init fffff980108c8db0 Current fffff980108c8810
        Base fffff980108c9000 Limit fffff980108c3000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`108c8850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`108c8990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`108c89f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`108c8a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`108c8b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`108c8bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`108c8c20)
        00000000`05bbf688 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`05bbf690 000007fe`f8d3c543 kernel32!GetQueuedCompletionStatus+0x48
        00000000`05bbf6f0 000007fe`f8cf8fb1 esent!CTaskManager::TMIDispatch+0x81
        00000000`05bbf770 000007fe`f8cf8dd5 esent!CTaskManager::TMDispatch+0x11
        00000000`05bbf7a0 00000000`76bfcdcd esent!UtilThreadIThreadBase+0x21
        00000000`05bbf7e0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`05bbf810 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800493e510  Cid 07c8.08d8  Teb: 000007fffffaa000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80049664a0  NotificationEvent
            fffffa8004966300  NotificationEvent
        IRP List:
            fffffa800493e260: (0006,0118) Flags: 00060800  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004812870       Image:         SearchIndexer.exe
        Wait Start TickCount      2123           Ticks: 44456 (0:00:11:33.518)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address TQUERY!CThread::_ThreadFunction (0x000007fef9b33870)
        Stack Init fffff980108cfdb0 Current fffff980108cf260
        Base fffff980108d0000 Limit fffff980108ca000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`108cf2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`108cf3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`108cf440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`108cf4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`108cf960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`108cfbb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`108cfc20)
        00000000`05faf4b8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`05faf4c0 000007fe`f9b4411b kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`05faf5d0 000007fe`f9b37d67 TQUERY!CRequestQueue::DoWork+0x2fb
        00000000`05faf760 000007fe`f9b338ad TQUERY!CCiQueryServer::QueryServerThreadProc+0x28
        00000000`05faf7a0 00000000`76bfcdcd TQUERY!CThread::_ThreadFunction+0x3e
        00000000`05faf7e0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`05faf810 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80049657d0  Cid 07c8.08e0  Teb: 000007fffffa6000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004866bc0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004812870       Image:         SearchIndexer.exe
        Wait Start TickCount      2129           Ticks: 44450 (0:00:11:33.424)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address mssrch!CHostHitTimingThread::Thread (0x000007fef945f106)
        Stack Init fffff9801086ddb0 Current fffff9801086d960
        Base fffff9801086e000 Limit fffff98010868000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1086d9a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1086dae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`1086db40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`1086dbc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`1086dc20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1086dc20)
        00000000`0602fbd8 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`0602fbe0 000007fe`f945f39d kernel32!WaitForSingleObjectEx+0x9c
        00000000`0602fca0 00000000`76bfcdcd mssrch!CHostHitTimingThread::Thread+0x298
        00000000`0602fd40 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0602fd70 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004952060  Cid 07c8.08e4  Teb: 000007fffffa4000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa8004866b60  SynchronizationEvent
            fffffa8004952118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004812870       Image:         SearchIndexer.exe
        Wait Start TickCount      46414          Ticks: 165 (0:00:00:02.574)
        Context Switch Count      110
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address mssrch!CTimerThread::Thread (0x000007fef945f47d)
        Stack Init fffff98010874db0 Current fffff98010874960
        Base fffff98010875000 Limit fffff9801086f000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`108749a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`10874ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`10874b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`10874bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`10874c20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`10874c20)
        00000000`061efce8 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`061efcf0 000007fe`f945fc9c kernel32!WaitForSingleObjectEx+0x9c
        00000000`061efdb0 00000000`76bfcdcd mssrch!CTimerThread::Thread+0x820
        00000000`061eff60 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`061eff90 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004952bb0  Cid 07c8.08e8  Teb: 000007fffffa2000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa8004356930  SynchronizationEvent
            fffffa8004952c68  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004812870       Image:         SearchIndexer.exe
        Wait Start TickCount      46578          Ticks: 1 (0:00:00:00.015)
        Context Switch Count      1310
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address mssrch!CBackoffTimerThread::Thread (0x000007fef9444626)
        Stack Init fffff9801087bdb0 Current fffff9801087b960
        Base fffff9801087c000 Limit fffff98010876000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1087b9a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1087bae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`1087bb40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`1087bbc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`1087bc20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1087bc20)
        00000000`060bf048 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`060bf050 000007fe`f94447be kernel32!WaitForSingleObjectEx+0x9c
        00000000`060bf110 00000000`76bfcdcd mssrch!CBackoffTimerThread::Thread+0x198
        00000000`060bfb00 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`060bfb30 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80049a8bb0  Cid 07c8.08ec  Teb: 000007fffffa0000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800489f890  NotificationEvent
            fffffa800489f830  NotificationEvent
            fffffa8004952680  NotificationEvent
        IRP List:
            fffffa8002ac3520: (0006,03a0) Flags: 00060800  Mdl: fffffa800434f770
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004812870       Image:         SearchIndexer.exe
        Wait Start TickCount      40565          Ticks: 6014 (0:00:01:33.819)
        Context Switch Count      737
        UserTime                  00:00:00.015
        KernelTime                00:00:00.031
        Win32 Start Address mssrch!CUsnMonitorNotifier::MonitorThreadStatic (0x000007fef953ba9e)
        Stack Init fffff98010882db0 Current fffff98010882260
        Base fffff98010883000 Limit fffff9801087d000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`108822a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`108823e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`10882440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`108824b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`10882960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`10882bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`10882c20)
        00000000`0633e608 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0633e610 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0633e720 000007fe`f953c8aa kernel32!WaitForMultipleObjects+0x11
        00000000`0633e760 000007fe`f953bacd mssrch!CUsnMonitorNotifier::Thread+0x52b
        00000000`0633fa20 00000000`76bfcdcd mssrch!CUsnMonitorNotifier::MonitorThreadStatic+0x30
        00000000`0633fa60 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0633fa90 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8002118930  Cid 07c8.0e28  Teb: 000007fffff96000 Win32Thread: fffff900c07e7010
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa8001e9f040  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004812870       Image:         SearchIndexer.exe
        Wait Start TickCount      46302          Ticks: 277 (0:00:00:04.321)
        Context Switch Count      26                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address ole32!CRpcThreadCache::RpcWorkerThreadEntry (0x000007fefd7a3be0)
        Stack Init fffff98020d8ddb0 Current fffff98020d8d740
        Base fffff98020d8e000 Limit fffff98020d86000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`20d8d780 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`20d8d8c0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`20d8d920 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`20d8d9a0 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`20d8da40 fffff960`000c7e1e win32k!xxxSleepThread+0x56
        fffff980`20d8da70 fffff960`000c7f25 win32k!xxxRealInternalGetMessage+0x72e
        fffff980`20d8db50 fffff960`000c97e4 win32k!xxxInternalGetMessage+0x35
        fffff980`20d8db90 fffff800`01c4d733 win32k!NtUserGetMessage+0x64
        fffff980`20d8dc20 00000000`76d1e6aa nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`20d8dc20)
        00000000`0753fc08 00000000`76d1e6ea USER32!ZwUserGetMessage+0xa
        00000000`0753fc10 000007fe`fd779d72 USER32!GetMessageW+0x34
        00000000`0753fc40 000007fe`fd77a0dd ole32!CDllHost::STAWorkerLoop+0x8a
        00000000`0753fca0 000007fe`fd7a3b7e ole32!CDllHost::WorkerThread+0xd7
        00000000`0753fce0 000007fe`fd7a3c0a ole32!CRpcThread::WorkerLoop+0x1e
        00000000`0753fd20 00000000`76bfcdcd ole32!CRpcThreadCache::RpcWorkerThreadEntry+0x2a
        00000000`0753fd50 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0753fd80 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8002ad5770  Cid 07c8.03a0  Teb: 000007fffffa8000 Win32Thread: fffff900c2009d60
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8004510f10  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004812870       Image:         SearchIndexer.exe
        Wait Start TickCount      32905          Ticks: 13674 (0:00:03:33.315)
        Context Switch Count      3                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff9801598fdb0 Current fffff9801598f810
        Base fffff98015990000 Limit fffff98015989000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1598f850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1598f990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`1598f9f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`1598fa80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`1598fb00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`1598fbb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1598fc20)
        00000000`0651fc48 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`0651fc50 000007fe`fedce7a3 kernel32!GetQueuedCompletionStatus+0x48
        00000000`0651fcb0 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`0651fd40 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`0651fdf0 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`0651fe20 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`0651fe60 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`0651fe90 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0651fec0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8002b1bbb0  Cid 07c8.0e70  Teb: 000007fffffda000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Alertable
            fffffa8003d5a5c0  QueueObject
            fffffa8002b1bc68  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004812870       Image:         SearchIndexer.exe
        Wait Start TickCount      46354          Ticks: 225 (0:00:00:03.510)
        Context Switch Count      10
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x0000000076e17860)
        Stack Init fffff9800b6bedb0 Current fffff9800b6be860
        Base fffff9800b6bf000 Limit fffff9800b6b9000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0b6be8a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0b6be9e0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0b6bea40 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0b6bead0 fffff800`01c8a722 nt!IoRemoveIoCompletion+0x47
        fffff980`0b6beb50 fffff800`01c4d733 nt!NtWaitForWorkViaWorkerFactory+0x1f1
        fffff980`0b6bec20 00000000`76e21b4a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0b6bec20)
        00000000`0662fc68 00000000`76e17a20 ntdll!NtWaitForWorkViaWorkerFactory+0xa
        00000000`0662fc70 00000000`76bfcdcd ntdll!TppWorkerThread+0x23e
        00000000`0662fee0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0662ff10 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80025adbb0  Cid 07c8.0e90  Teb: 000007fffffd8000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Alertable
            fffffa8003d5a5c0  QueueObject
            fffffa80025adc68  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004812870       Image:         SearchIndexer.exe
        Wait Start TickCount      46354          Ticks: 225 (0:00:00:03.510)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x0000000076e17860)
        Stack Init fffff98012bb2db0 Current fffff98012bb2860
        Base fffff98012bb3000 Limit fffff98012bad000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`12bb28a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12bb29e0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`12bb2a40 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`12bb2ad0 fffff800`01c8a722 nt!IoRemoveIoCompletion+0x47
        fffff980`12bb2b50 fffff800`01c4d733 nt!NtWaitForWorkViaWorkerFactory+0x1f1
        fffff980`12bb2c20 00000000`76e21b4a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12bb2c20)
        00000000`0648f6b8 00000000`76e17a20 ntdll!NtWaitForWorkViaWorkerFactory+0xa
        00000000`0648f6c0 00000000`76bfcdcd ntdll!TppWorkerThread+0x23e
        00000000`0648f930 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0648f960 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80025a76c0  Cid 07c8.0fa4  Teb: 000007fffffd4000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Alertable
            fffffa8003d5a5c0  QueueObject
            fffffa80025a7778  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8004812870       Image:         SearchIndexer.exe
        Wait Start TickCount      46354          Ticks: 225 (0:00:00:03.510)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x0000000076e17860)
        Stack Init fffff9801db65db0 Current fffff9801db65860
        Base fffff9801db66000 Limit fffff9801db60000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1db658a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1db659e0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`1db65a40 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`1db65ad0 fffff800`01c8a722 nt!IoRemoveIoCompletion+0x47
        fffff980`1db65b50 fffff800`01c4d733 nt!NtWaitForWorkViaWorkerFactory+0x1f1
        fffff980`1db65c20 00000000`76e21b4a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1db65c20)
        00000000`0626f748 00000000`76e17a20 ntdll!NtWaitForWorkViaWorkerFactory+0xa
        00000000`0626f750 00000000`76bfcdcd ntdll!TppWorkerThread+0x23e
        00000000`0626f9c0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0626f9f0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

Rtvscan process

```
PROCESS fffffa800486c230
    SessionId: 0  Cid: 062c    Peb: 7efdf000  ParentCid: 025c
    DirBase: 41b5c000  ObjectTable: fffff88005e9ded0  HandleCount: 570.
    Image: Rtvscan.exe
    VadRoot fffffa8003fb05c0 Vads 317 Clone 0 Private 13369. Modified 11198. Locked 0.
    DeviceMap fffff88000007820
    Token                             fffff88005e3f5c0
    ElapsedTime                       00:11:37.933
    UserTime                          00:00:08.252
    KernelTime                        00:00:09.656
    QuotaPoolUsage[PagedPool]         166536
    QuotaPoolUsage[NonPagedPool]      37344
    Working Set Sizes (now,min,max)  (8392, 50, 345) (33568KB, 200KB, 1380KB)
    PeakWorkingSetSize                17634
    VirtualSize                       181 Mb
    PeakVirtualSize                   191 Mb
    PageFaultCount                    327907
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      14306

    Setting context for this process...
.process /p /r fffffa800486c230

    !peb
PEB at 000000007efdf000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         0000000000400000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00000000002d27d0 . 00000000002d2b30
    Ldr.InLoadOrderModuleList:           00000000002d26e0 . 00000000002d2c90
    Ldr.InMemoryOrderModuleList:         00000000002d26f0 . 00000000002d2ca0
            Base TimeStamp                     Module
          400000 4580ab9c Dec 14 01:40:44 2006 c:\Program Files (x86)\Symantec
AntiVirus\Rtvscan.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        75110000 4549d371 Nov 02 11:16:01 2006 C:\Windows\system32\wow64.dll
        75000000 4549d374 Nov 02 11:16:04 2006 C:\Windows\system32\wow64win.dll
        75100000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\wow64cpu.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       00000000002d0000
    ProcessParameters: 00000000002d1d20
    WindowTitle:  'c:\Program Files (x86)\Symantec AntiVirus\Rtvscan.exe'
    ImageFile:    'c:\Program Files (x86)\Symantec AntiVirus\Rtvscan.exe'
    CommandLine:  '"c:\Program Files (x86)\Symantec AntiVirus\Rtvscan.exe"'
    DllPath:      'c:\Program Files (x86)\Symantec
AntiVirus;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Windows;C:\Wind
ows\System32\Wbem'
    Environment:  00000000002d1310
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\system32\config\systemprofile\AppData\Roaming
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        LOCALAPPDATA=C:\Windows\system32\config\systemprofile\AppData\Local
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
```

```
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\TEMP
        TMP=C:\Windows\TEMP
        USERDOMAIN=DOMAIN
        USERNAME=COMPUTERNAME$
        USERPROFILE=C:\Windows\system32\config\systemprofile
        windir=C:\Windows


        THREAD fffffa800482b530  Cid 062c.0668  Teb: 000000007efdb000 Win32Thread: fffff900c07f4010
WAIT: (Executive) UserMode Non-Alertable
            fffffa80048db778  NotificationEvent
        IRP List:
            fffffa8004ac6930: (0006,0118) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800486c230       Image:         Rtvscan.exe
        Wait Start TickCount      2775           Ticks: 43804 (0:00:11:23.346)
        Context Switch Count      10097                 LargeStack
        UserTime                  00:00:00.015
        KernelTime                00:00:00.280
        Win32 Start Address Rtvscan!NTSGetComputerName (0x000000000051ca48)
        Stack Init fffff9801098ddb0 Current fffff9801098d7f0
        Base fffff9801098e000 Limit fffff98010985000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1098d830 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1098d970 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`1098d9d0 fffff800`01ebdf16 nt!KeWaitForSingleObject+0x5f5
        fffff980`1098da50 fffff800`01ea1a24 nt!IopSynchronousServiceTail+0x306
        fffff980`1098dac0 fffff800`01c4d733 nt!NtReadFile+0x583
        fffff980`1098dbb0 00000000`75103907 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1098dc20)
        00000000`0007ee38 00000000`7511abfe wow64cpu!ReadWriteFileFault+0x35
        00000000`0007ef10 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0007ef40 00000000`76e0e23d wow64!Wow64LdrpInitialize+0x492
        00000000`0007f4a0 00000000`76e7e974 ntdll!LdrpInitializeProcess+0x1333
        00000000`0007f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d641
        00000000`0007f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa800437a6b0  Cid 062c.0890  Teb: 000000007efd8000 Win32Thread: fffff900c07f7920
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004957970  NotificationEvent
            fffffa800437a768  NotificationTimer
        IRP List:
            fffffa80042d2c70: (0006,0118) Flags: 00060000  Mdl: 00000000
            fffffa8004685590: (0006,0118) Flags: 00060000  Mdl: 00000000
            fffffa80046d7060: (0006,0358) Flags: 00060000  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800486c230       Image:         Rtvscan.exe
        Wait Start TickCount      7694           Ticks: 38885 (0:00:10:06.609)
        Context Switch Count      5024                 LargeStack
        UserTime                  00:00:01.622
        KernelTime                00:00:01.388
        Win32 Start Address 0x00000000767fb9d5
        Stack Init fffff980109a0db0 Current fffff980109a0960
        Base fffff980109a1000 Limit fffff98010998000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`109a09a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`109a0ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`109a0b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`109a0bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`109a0c20 00000000`75103cf9 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`109a0c20)
        00000000`0038f128 00000000`75103af6 wow64cpu!CpupSyscallStub+0x9
        00000000`0038f130 00000000`7511abfe wow64cpu!Thunk0ArgReloadState+0x1a
        00000000`0038f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0038f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0038f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0038f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa800497c060  Cid 062c.08a0  Teb: 000000007efaa000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa800497d2f0  SynchronizationTimer
            fffffa800497d690  SynchronizationEvent
            fffffa8004919770  SynchronizationEvent
            fffffa80048e1040  SynchronizationEvent
            fffffa800466a8a0  SynchronizationEvent
            fffffa8004772270  SynchronizationEvent
            fffffa80044c6770  SynchronizationEvent
            fffffa800295e040  SynchronizationEvent
            fffffa8004880e10  SynchronizationEvent
            fffffa80046d9560  SynchronizationEvent
            fffffa800469a7d0  SynchronizationEvent
            fffffa800295e0b0  SynchronizationEvent
            fffffa80048b7b80  SynchronizationEvent
            fffffa80048d2560  SynchronizationEvent
            fffffa80046b1220  SynchronizationEvent
            fffffa8004905270  SynchronizationEvent
            fffffa8004833e30  SynchronizationEvent
            fffffa80046d7b00  SynchronizationEvent
            fffffa800468c9d8  NotificationEvent
            fffffa80049b4570  SynchronizationEvent
            fffffa800496db90  SynchronizationEvent
            fffffa80049175d0  SynchronizationEvent
            fffffa800469d230  SynchronizationEvent
            fffffa80046d79b0  SynchronizationEvent
            fffffa8004691f50  SynchronizationEvent
            fffffa80046d1770  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800486c230       Image:         Rtvscan.exe
        Wait Start TickCount      7663           Ticks: 38916 (0:00:10:07.093)
        Context Switch Count      406
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address 0x0000000077046235
        Stack Init fffff9800ba6ddb0 Current fffff9800ba6d260
        Base fffff9800ba6e000 Limit fffff9800ba68000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0ba6d2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0ba6d3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0ba6d440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0ba6d4b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`0ba6d960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`0ba6dbb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0ba6dc20)
        00000000`015ef0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`015ef1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`015ef1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`015ef730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`015ef7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa80046d1800  Cid 062c.08b8  Teb: 000000007efa4000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8003d62b90  SynchronizationEvent
            fffffa80046d18b8  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800486c230       Image:         Rtvscan.exe
        Wait Start TickCount      40523          Ticks: 6056 (0:00:01:34.474)
        Context Switch Count      7
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3493a3
        Stack Init fffff9800ebb2db0 Current fffff9800ebb2960
        Base fffff9800ebb3000 Limit fffff9800ebad000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0ebb29a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0ebb2ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0ebb2b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0ebb2bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0ebb2c20 00000000`75103cf9 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0ebb2c20)
        00000000`0166f128 00000000`75103af6 wow64cpu!CpupSyscallStub+0x9
        00000000`0166f130 00000000`7511abfe wow64cpu!Thunk0ArgReloadState+0x1a
        00000000`0166f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0166f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0166f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0166f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa8004853060  Cid 062c.08c4  Teb: 000000007efa1000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80042ac940  NotificationEvent
            fffffa80042ac8e0  NotificationEvent
            fffffa8004853118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800486c230       Image:         Rtvscan.exe
        Wait Start TickCount      44416          Ticks: 2163 (0:00:00:33.743)
        Context Switch Count      17
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3494f6
        Stack Init fffff98010889db0 Current fffff98010889260
        Base fffff9801088a000 Limit fffff98010884000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`108892a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`108893e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`10889440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`108894b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`10889960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`10889bb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`10889c20)
        00000000`01bdf0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`01bdf1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`01bdf1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`01bdf730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`01bdf7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa80046c62c0  Cid 062c.08c8  Teb: 000000007ef9e000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80046c6ce0  NotificationEvent
            fffffa80046c6378  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800486c230       Image:         Rtvscan.exe
        Wait Start TickCount      46577          Ticks: 2 (0:00:00:00.031)
        Context Switch Count      6846
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address 0x000000007c3494f6
        Stack Init fffff98010897db0 Current fffff98010897960
        Base fffff98010898000 Limit fffff98010892000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`108979a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`10897ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`10897b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`10897bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`10897c20 00000000`75103cf9 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`10897c20)
        00000000`01c1f128 00000000`75103af6 wow64cpu!CpupSyscallStub+0x9
        00000000`01c1f130 00000000`7511abfe wow64cpu!Thunk0ArgReloadState+0x1a
        00000000`01c1f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`01c1f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`01c1f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`01c1f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa80045e5830  Cid 062c.08cc  Teb: 000000007ef9b000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80046e8640  SynchronizationEvent
            fffffa80045e58e8  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800486c230       Image:         Rtvscan.exe
        Wait Start TickCount      46570          Ticks: 9 (0:00:00:00.140)
        Context Switch Count      3857
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3494f6
        Stack Init fffff9801089edb0 Current fffff9801089e960
        Base fffff9801089f000 Limit fffff98010899000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1089e9a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1089eae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`1089eb40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`1089ebc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`1089ec20 00000000`75103cf9 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1089ec20)
        00000000`01c5f128 00000000`75103af6 wow64cpu!CpupSyscallStub+0x9
        00000000`01c5f130 00000000`7511abfe wow64cpu!Thunk0ArgReloadState+0x1a
        00000000`01c5f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`01c5f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`01c5f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`01c5f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa80046c7420  Cid 062c.08d0  Teb: 000000007ef98000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004959920  NotificationEvent
            fffffa80042acac0  SynchronizationEvent
            fffffa80046c74d8  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800486c230       Image:         Rtvscan.exe
        Wait Start TickCount      2105           Ticks: 44474 (0:00:11:33.798)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3493a3
        Stack Init fffff98010890db0 Current fffff98010890260
        Base fffff98010891000 Limit fffff9801088b000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`108902a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`108903e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`10890440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`108904b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`10890960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`10890bb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`10890c20)
        00000000`01ccf0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`01ccf1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`01ccf1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`01ccf730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`01ccf7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa8004a1f060  Cid 062c.0914  Teb: 000000007ef92000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800491f610  SynchronizationEvent
            fffffa8004a1f118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800486c230       Image:         Rtvscan.exe
        Wait Start TickCount      46539          Ticks: 40 (0:00:00:00.624)
        Context Switch Count      372
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3493a3
        Stack Init fffff9800d089db0 Current fffff9800d089960
        Base fffff9800d08a000 Limit fffff9800d084000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0d0899a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0d089ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0d089b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0d089bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0d089c20 00000000`75103cf9 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0d089c20)
        00000000`028bf128 00000000`75103af6 wow64cpu!CpupSyscallStub+0x9
        00000000`028bf130 00000000`7511abfe wow64cpu!Thunk0ArgReloadState+0x1a
        00000000`028bf1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`028bf1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`028bf730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`028bf7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa8004a3cbb0  Cid 062c.0918  Teb: 000000007ef8f000 Win32Thread: 0000000000000000
WAIT: (DelayExecution) UserMode Non-Alertable
            fffffa8004a3cc68  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800486c230       Image:         Rtvscan.exe
        Wait Start TickCount      46539          Ticks: 40 (0:00:00:00.624)
        Context Switch Count      366
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3493a3
        Stack Init fffff9800cc53db0 Current fffff9800cc53990
        Base fffff9800cc54000 Limit fffff9800cc4e000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0cc539d0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0cc53b10 fffff800`01c5b5a9 nt!KiSwapThread+0x125
        fffff980`0cc53b70 fffff800`01e8ae9d nt!KeDelayExecutionThread+0x339
        fffff980`0cc53bf0 fffff800`01c4d733 nt!NtDelayExecution+0x5c
        fffff980`0cc53c20 00000000`75103cf9 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0cc53c20)
        00000000`02c4f128 00000000`75103bad wow64cpu!CpupSyscallStub+0x9
        00000000`02c4f130 00000000`7511abfe wow64cpu!Thunk2ArgNSpNSpReloadState+0x21
        00000000`02c4f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`02c4f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`02c4f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`02c4f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa8004a3c700  Cid 062c.091c  Teb: 000000007ef8c000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8003d5ec90  SynchronizationEvent
            fffffa8004a3c7b8  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800486c230       Image:         Rtvscan.exe
        Wait Start TickCount      46553          Ticks: 26 (0:00:00:00.405)
        Context Switch Count      736
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3493a3
        Stack Init fffff9800e315db0 Current fffff9800e315960
        Base fffff9800e316000 Limit fffff9800e310000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0e3159a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e315ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0e315b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0e315bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0e315c20 00000000`75103cf9 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e315c20)
        00000000`05a5f128 00000000`75103af6 wow64cpu!CpupSyscallStub+0x9
        00000000`05a5f130 00000000`7511abfe wow64cpu!Thunk0ArgReloadState+0x1a
        00000000`05a5f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`05a5f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`05a5f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`05a5f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa8004203bb0  Cid 062c.0a08  Teb: 000000007ef86000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004c2ceb0  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800486c230       Image:         Rtvscan.exe
        Wait Start TickCount      3406           Ticks: 43173 (0:00:11:13.503)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3494f6
        Stack Init fffff980159ffdb0 Current fffff980159ff960
        Base fffff98015a00000 Limit fffff980159fa000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`159ff9a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`159ffae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`159ffb40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`159ffbc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`159ffc20 00000000`75103cf9 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`159ffc20)
        00000000`05cdf128 00000000`75103af6 wow64cpu!CpupSyscallStub+0x9
        00000000`05cdf130 00000000`7511abfe wow64cpu!Thunk0ArgReloadState+0x1a
        00000000`05cdf1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`05cdf1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`05cdf730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`05cdf7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa8003d7d9d0  Cid 062c.0480  Teb: 000000007ef80000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800407f8c0  Semaphore Limit 0x1
            fffffa8003d7da88  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800486c230       Image:         Rtvscan.exe
        Wait Start TickCount      46546          Ticks: 33 (0:00:00:00.514)
        Context Switch Count      729
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3493a3
        Stack Init fffff980159dcdb0 Current fffff980159dc960
        Base fffff980159dd000 Limit fffff980159d7000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`159dc9a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`159dcae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`159dcb40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`159dcbc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`159dcc20 00000000`75103cf9 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`159dcc20)
        00000000`05f5f128 00000000`75103af6 wow64cpu!CpupSyscallStub+0x9
        00000000`05f5f130 00000000`7511abfe wow64cpu!Thunk0ArgReloadState+0x1a
        00000000`05f5f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`05f5f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`05f5f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`05f5f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa8004960bb0  Cid 062c.071c  Teb: 000000007efa7000 Win32Thread: fffff900c07fc010
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80049fc0e0  NotificationEvent
            fffffa80049cee40  SynchronizationEvent
            fffffa800494d360  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800486c230       Image:         Rtvscan.exe
        Wait Start TickCount      5049           Ticks: 41530 (0:00:10:47.872)
        Context Switch Count      633                 LargeStack
        UserTime                  00:00:00.015
        KernelTime                00:00:00.046
        Win32 Start Address 0x0000000073cd2923
        Stack Init fffff9800d0e2db0 Current fffff9800d0e2260
        Base fffff9800d0e3000 Limit fffff9800d0db000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0d0e22a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0d0e23e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0d0e2440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0d0e24b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`0d0e2960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`0d0e2bb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0d0e2c20)
        00000000`0162f0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`0162f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0162f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0162f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0162f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa8003d86060  Cid 062c.093c  Teb: 000000007ef7d000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004371c30  NotificationEvent
            fffffa80048c5880  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800486c230       Image:         Rtvscan.exe
        Wait Start TickCount      5039           Ticks: 41540 (0:00:10:48.028)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x0000000073f717ae
        Stack Init fffff9800d090db0 Current fffff9800d090260
        Base fffff9800d091000 Limit fffff9800d08b000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0d0902a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0d0903e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0d090440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0d0904b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`0d090960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`0d090bb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0d090c20)
        00000000`0629f0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`0629f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0629f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0629f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0629f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa80020aa410  Cid 062c.0c38  Teb: 000000007ef7a000 Win32Thread: 0000000000000000
WAIT: (DelayExecution) UserMode Non-Alertable
            fffffa80020aa4c8  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800486c230       Image:         Rtvscan.exe
        Wait Start TickCount      46515          Ticks: 64 (0:00:00:00.998)
        Context Switch Count      3225
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address 0x000000007c3493a3
        Stack Init fffff9801a6bbdb0 Current fffff9801a6bb990
        Base fffff9801a6bc000 Limit fffff9801a6b6000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1a6bb9d0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1a6bbb10 fffff800`01c5b5a9 nt!KiSwapThread+0x125
        fffff980`1a6bbb70 fffff800`01e8ae9d nt!KeDelayExecutionThread+0x339
        fffff980`1a6bbbf0 fffff800`01c4d733 nt!NtDelayExecution+0x5c
        fffff980`1a6bbc20 00000000`75103cf9 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1a6bbc20)
        00000000`06bdf128 00000000`75103bad wow64cpu!CpupSyscallStub+0x9
        00000000`06bdf130 00000000`7511abfe wow64cpu!Thunk2ArgNSpNSpReloadState+0x21
        00000000`06bdf1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`06bdf1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`06bdf730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`06bdf7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa800448cbb0  Cid 062c.0c3c  Teb: 000000007ef77000 Win32Thread: fffff900c2005ab0
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80020655b0  SynchronizationEvent
            fffffa8001ffa6b0  SynchronizationEvent
            fffffa8004b38120  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800486c230       Image:         Rtvscan.exe
        Wait Start TickCount      19121          Ticks: 27458 (0:00:07:08.347)
        Context Switch Count      88                 LargeStack
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000006fa37d78
        Stack Init fffff980106eadb0 Current fffff980106ea260
        Base fffff980106eb000 Limit fffff980106e4000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`106ea2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`106ea3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`106ea440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`106ea4b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`106ea960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`106eabb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`106eac20)
        00000000`06e1f0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`06e1f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`06e1f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`06e1f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`06e1f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa8002035060  Cid 062c.0c48  Teb: 000000007ef71000 Win32Thread: 0000000000000000
WAIT: (Executive) UserMode Alertable
            fffffa8002792690  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800486c230       Image:         Rtvscan.exe
        Wait Start TickCount      7665           Ticks: 38914 (0:00:10:07.062)
        Context Switch Count      254
        UserTime                  00:00:00.046
        KernelTime                00:00:00.109
        Win32 Start Address 0x000000007c3493a3
        Stack Init fffff9801a701db0 Current fffff9801a7017c0
        Base fffff9801a702000 Limit fffff9801a6fc000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1a701800 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1a701940 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`1a7019a0 fffff800`01e702bb nt!KeWaitForSingleObject+0x5f5
        fffff980`1a701a20 fffff800`01e70aa0 nt! ?? ::NNGAKEGL::`string'+0x2ac4c
        fffff980`1a701b40 fffff800`01c4d733 nt!NtNotifyChangeKey+0x60
        fffff980`1a701bb0 00000000`76e2116a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1a701c20)
        00000000`0709e7f8 00000000`7512d824 ntdll!ZwNotifyChangeKey+0xa
        00000000`0709e800 00000000`7511aa4e wow64!whNtNotifyChangeKey+0x6c
        00000000`0709e860 00000000`75103678 wow64!Wow64SystemServiceEx+0xca
        00000000`0709f110 00000000`7511abfe wow64cpu!TurboDispatchJumpAddressEnd+0x28
        00000000`0709f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0709f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0709f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0709f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa8002038bb0  Cid 062c.0c50  Teb: 000000007ef6b000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80041b9cd0  NotificationEvent
            fffffa80042fd210  NotificationEvent
            fffffa8001f7c790  Semaphore Limit 0x400
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800486c230       Image:         Rtvscan.exe
        Wait Start TickCount      7515           Ticks: 39064 (0:00:10:09.402)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3494f6
        Stack Init fffff9801a62fdb0 Current fffff9801a62f260
        Base fffff9801a630000 Limit fffff9801a62a000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1a62f2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1a62f3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`1a62f440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`1a62f4b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`1a62f960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`1a62fbb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1a62fc20)
        00000000`0731f0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`0731f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0731f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0731f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0731f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa8002030060  Cid 062c.0c54  Teb: 000000007ef68000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8001ffaf90  NotificationEvent
            fffffa8002031560  NotificationEvent
            fffffa8001f7c790  Semaphore Limit 0x400
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800486c230       Image:         Rtvscan.exe
        Wait Start TickCount      7516           Ticks: 39063 (0:00:10:09.386)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3494f6
        Stack Init fffff9801a636db0 Current fffff9801a636260
        Base fffff9801a637000 Limit fffff9801a631000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1a6362a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1a6363e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`1a636440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`1a6364b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`1a636960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`1a636bb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1a636c20)
        00000000`0745f0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`0745f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0745f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0745f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0745f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa80020a9060  Cid 062c.0c58  Teb: 000000007ef65000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8001f35d90  NotificationEvent
            fffffa8001f35d30  NotificationEvent
            fffffa8001f7c790  Semaphore Limit 0x400
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800486c230       Image:         Rtvscan.exe
        Wait Start TickCount      7515           Ticks: 39064 (0:00:10:09.402)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3494f6
        Stack Init fffff9801a63ddb0 Current fffff9801a63d260
        Base fffff9801a63e000 Limit fffff9801a638000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1a63d2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1a63d3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`1a63d440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`1a63d4b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`1a63d960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`1a63dbb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1a63dc20)
        00000000`0759f0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`0759f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0759f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0759f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0759f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa8002069bb0  Cid 062c.0c5c  Teb: 000000007ef62000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8002031cd0  NotificationEvent
            fffffa8004c21090  NotificationEvent
            fffffa8001f7c790  Semaphore Limit 0x400
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800486c230       Image:         Rtvscan.exe
        Wait Start TickCount      7516           Ticks: 39063 (0:00:10:09.386)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3494f6
        Stack Init fffff9801a64bdb0 Current fffff9801a64b260
        Base fffff9801a64c000 Limit fffff9801a646000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1a64b2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1a64b3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`1a64b440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`1a64b4b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`1a64b960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`1a64bbb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1a64bc20)
        00000000`076df0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`076df1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`076df1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`076df730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`076df7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa8004b21bb0  Cid 062c.0c64  Teb: 000000007ef5c000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8001e124f0  NotificationEvent
            fffffa8002064fe0  NotificationEvent
            fffffa8001f7c790  Semaphore Limit 0x400
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800486c230       Image:         Rtvscan.exe
        Wait Start TickCount      7516           Ticks: 39063 (0:00:10:09.386)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3494f6
        Stack Init fffff9801a652db0 Current fffff9801a652260
        Base fffff9801a653000 Limit fffff9801a64d000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1a6522a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1a6523e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`1a652440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`1a6524b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`1a652960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`1a652bb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1a652c20)
        00000000`0795f0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`0795f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0795f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0795f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0795f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa8001ff6bb0  Cid 062c.0c74  Teb: 000000007ef50000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004957970  NotificationEvent
            fffffa8004cb33a0  SynchronizationEvent
            fffffa8004cb3340  SynchronizationEvent
            fffffa8004cb3920  SynchronizationEvent
            fffffa8004cb3260  SynchronizationEvent
            fffffa8004cb38c0  SynchronizationEvent
            fffffa8004cb3860  SynchronizationEvent
            fffffa8004cb3800  SynchronizationEvent
            fffffa8002061680  SynchronizationEvent
            fffffa8002061620  SynchronizationEvent
            fffffa80020615c0  SynchronizationEvent
            fffffa8002061560  SynchronizationEvent
            fffffa800204a040  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800486c230       Image:         Rtvscan.exe
        Wait Start TickCount      7694           Ticks: 38885 (0:00:10:06.609)
        Context Switch Count      9
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3493a3
        Stack Init fffff9801a66edb0 Current fffff9801a66e260
        Base fffff9801a66f000 Limit fffff9801a669000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1a66e2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1a66e3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`1a66e440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`1a66e4b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`1a66e960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`1a66ebb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1a66ec20)
        00000000`0815f0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`0815f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0815f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0815f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0815f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa8001ff6700  Cid 062c.0c78  Teb: 000000007ef4d000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800205e4b0  SynchronizationEvent
            fffffa800202fe30  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800486c230       Image:         Rtvscan.exe
        Wait Start TickCount      7516           Ticks: 39063 (0:00:10:09.386)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3493a3
        Stack Init fffff9801a675db0 Current fffff9801a675260
        Base fffff9801a676000 Limit fffff9801a670000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1a6752a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1a6753e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`1a675440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`1a6754b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`1a675960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`1a675bb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1a675c20)
        00000000`0829f0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`0829f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0829f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0829f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0829f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa80020af060  Cid 062c.0c7c  Teb: 000000007ef4a000 Win32Thread: 0000000000000000
WAIT: (DelayExecution) UserMode Non-Alertable
            fffffa80020af118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800486c230       Image:         Rtvscan.exe
        Wait Start TickCount      46555          Ticks: 24 (0:00:00:00.374)
        Context Switch Count      1233
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3493a3
        Stack Init fffff9801a67cdb0 Current fffff9801a67c990
        Base fffff9801a67d000 Limit fffff9801a677000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1a67c9d0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1a67cb10 fffff800`01c5b5a9 nt!KiSwapThread+0x125
        fffff980`1a67cb70 fffff800`01e8ae9d nt!KeDelayExecutionThread+0x339
        fffff980`1a67cbf0 fffff800`01c4d733 nt!NtDelayExecution+0x5c
        fffff980`1a67cc20 00000000`75103cf9 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1a67cc20)
        00000000`083df128 00000000`75103bad wow64cpu!CpupSyscallStub+0x9
        00000000`083df130 00000000`7511abfe wow64cpu!Thunk2ArgNSpNSpReloadState+0x21
        00000000`083df1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`083df1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`083df730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`083df7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa8001e12610  Cid 062c.0c80  Teb: 000000007ef53000 Win32Thread: 0000000000000000
WAIT: (Executive) UserMode Alertable
            fffffa800202fb20  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800486c230       Image:         Rtvscan.exe
        Wait Start TickCount      7694           Ticks: 38885 (0:00:10:06.609)
        Context Switch Count      10
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3493a3
        Stack Init fffff9801a667db0 Current fffff9801a6677c0
        Base fffff9801a668000 Limit fffff9801a662000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1a667800 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1a667940 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`1a6679a0 fffff800`01e702bb nt!KeWaitForSingleObject+0x5f5
        fffff980`1a667a20 fffff800`01e70aa0 nt! ?? ::NNGAKEGL::`string'+0x2ac4c
        fffff980`1a667b40 fffff800`01c4d733 nt!NtNotifyChangeKey+0x60
        fffff980`1a667bb0 00000000`76e2116a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1a667c20)
        00000000`0801e7f8 00000000`7512d824 ntdll!ZwNotifyChangeKey+0xa
        00000000`0801e800 00000000`7511aa4e wow64!whNtNotifyChangeKey+0x6c
        00000000`0801e860 00000000`75103678 wow64!Wow64SystemServiceEx+0xca
        00000000`0801f110 00000000`7511abfe wow64cpu!TurboDispatchJumpAddressEnd+0x28
        00000000`0801f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0801f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0801f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0801f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa8002064660  Cid 062c.0c84  Teb: 000000007ef47000 Win32Thread: 0000000000000000
WAIT: (Executive) UserMode Alertable
            fffffa800205e670  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800486c230       Image:         Rtvscan.exe
        Wait Start TickCount      7516           Ticks: 39063 (0:00:10:09.386)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3493a3
        Stack Init fffff9801a683db0 Current fffff9801a6837c0
        Base fffff9801a684000 Limit fffff9801a67e000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1a683800 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1a683940 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`1a6839a0 fffff800`01e702bb nt!KeWaitForSingleObject+0x5f5
        fffff980`1a683a20 fffff800`01e70aa0 nt! ?? ::NNGAKEGL::`string'+0x2ac4c
        fffff980`1a683b40 fffff800`01c4d733 nt!NtNotifyChangeKey+0x60
        fffff980`1a683bb0 00000000`76e2116a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1a683c20)
        00000000`0851e7f8 00000000`7512d824 ntdll!ZwNotifyChangeKey+0xa
        00000000`0851e800 00000000`7511aa4e wow64!whNtNotifyChangeKey+0x6c
        00000000`0851e860 00000000`75103678 wow64!Wow64SystemServiceEx+0xca
        00000000`0851f110 00000000`7511abfe wow64cpu!TurboDispatchJumpAddressEnd+0x28
        00000000`0851f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0851f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0851f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0851f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa800206c060  Cid 062c.0c88  Teb: 000000007ef44000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80048bc510  SynchronizationEvent
            fffffa8001ec4de0  NotificationEvent
            fffffa800206c118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800486c230       Image:         Rtvscan.exe
        Wait Start TickCount      7608           Ticks: 38971 (0:00:10:07.951)
        Context Switch Count      9
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3493a3
        Stack Init fffff9801a68adb0 Current fffff9801a68a260
        Base fffff9801a68b000 Limit fffff9801a685000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1a68a2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1a68a3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`1a68a440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`1a68a4b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`1a68a960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`1a68abb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1a68ac20)
        00000000`0865f0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`0865f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0865f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0865f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0865f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa8001f7b890  Cid 062c.0cb0  Teb: 000000007ef6e000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004c1bf90  SynchronizationEvent
            fffffa8001f7b948  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800486c230       Image:         Rtvscan.exe
        Wait Start TickCount      46363          Ticks: 216 (0:00:00:03.369)
        Context Switch Count      136
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3493a3
        Stack Init fffff9801dba4db0 Current fffff9801dba4260
        Base fffff9801dba5000 Limit fffff9801db9f000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1dba42a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1dba43e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`1dba4440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`1dba44b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`1dba4960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`1dba4bb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1dba4c20)
        00000000`071df0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`071df1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`071df1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`071df730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`071df7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa800203d060  Cid 062c.0cbc  Teb: 000000007ef3e000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004b13230  SynchronizationEvent
            fffffa8001f09230  SynchronizationEvent
            fffffa800206e170  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800486c230       Image:         Rtvscan.exe
        Wait Start TickCount      7609           Ticks: 38970 (0:00:10:07.935)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3493a3
        Stack Init fffff9801dbb9db0 Current fffff9801dbb9260
        Base fffff9801dbba000 Limit fffff9801dbb4000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1dbb92a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1dbb93e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`1dbb9440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`1dbb94b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`1dbb9960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`1dbb9bb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1dbb9c20)
        00000000`088df0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`088df1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`088df1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`088df730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`088df7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa8002051060  Cid 062c.0cc0  Teb: 000000007ef3b000 Win32Thread: fffff900c2018200
WAIT: (DelayExecution) UserMode Non-Alertable
            fffffa8002051118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800486c230       Image:         Rtvscan.exe
        Wait Start TickCount      46573          Ticks: 6 (0:00:00:00.093)
        Context Switch Count      1522                 LargeStack
        UserTime                  00:00:01.248
        KernelTime                00:00:00.764
        Win32 Start Address 0x000000007c3493a3
        Stack Init fffff98020db3db0 Current fffff98020db3990
        Base fffff98020db4000 Limit fffff98020dac000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`20db39d0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`20db3b10 fffff800`01c5b5a9 nt!KiSwapThread+0x125
        fffff980`20db3b70 fffff800`01e8ae9d nt!KeDelayExecutionThread+0x339
        fffff980`20db3bf0 fffff800`01c4d733 nt!NtDelayExecution+0x5c
        fffff980`20db3c20 00000000`75103cf9 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`20db3c20)
        00000000`08a1f128 00000000`75103bad wow64cpu!CpupSyscallStub+0x9
        00000000`08a1f130 00000000`7511abfe wow64cpu!Thunk2ArgNSpNSpReloadState+0x21
        00000000`08a1f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`08a1f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`08a1f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`08a1f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa8002054840  Cid 062c.0cc4  Teb: 000000007ef38000 Win32Thread: 0000000000000000
WAIT: (DelayExecution) UserMode Non-Alertable
            fffffa80020548f8  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800486c230       Image:         Rtvscan.exe
        Wait Start TickCount      46527          Ticks: 52 (0:00:00:00.811)
        Context Switch Count      1286
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3493a3
        Stack Init fffff9801dbc0db0 Current fffff9801dbc0990
        Base fffff9801dbc1000 Limit fffff9801dbbb000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1dbc09d0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1dbc0b10 fffff800`01c5b5a9 nt!KiSwapThread+0x125
        fffff980`1dbc0b70 fffff800`01e8ae9d nt!KeDelayExecutionThread+0x339
        fffff980`1dbc0bf0 fffff800`01c4d733 nt!NtDelayExecution+0x5c
        fffff980`1dbc0c20 00000000`75103cf9 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1dbc0c20)
        00000000`08b5f128 00000000`75103bad wow64cpu!CpupSyscallStub+0x9
        00000000`08b5f130 00000000`7511abfe wow64cpu!Thunk2ArgNSpNSpReloadState+0x21
        00000000`08b5f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`08b5f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`08b5f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`08b5f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa80020b33b0  Cid 062c.0d90  Teb: 000000007ef41000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8001f25780  SynchronizationEvent
            fffffa8004957970  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800486c230       Image:         Rtvscan.exe
        Wait Start TickCount      7694           Ticks: 38885 (0:00:10:06.609)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3493a3
        Stack Init fffff9801dad2db0 Current fffff9801dad2260
        Base fffff9801dad3000 Limit fffff9801dacd000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1dad22a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1dad23e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`1dad2440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`1dad24b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`1dad2960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`1dad2bb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1dad2c20)
        00000000`0879f0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`0879f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0879f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0879f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0879f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa80020f5340  Cid 062c.0488  Teb: 000000007efd5000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8004846370  QueueObject
            fffffa80020f53f8  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800486c230       Image:         Rtvscan.exe
        Wait Start TickCount      46515          Ticks: 64 (0:00:00:00.998)
        Context Switch Count      564
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x00000000762f3242
        Stack Init fffff9800eadfdb0 Current fffff9800eadf810
        Base fffff9800eae0000 Limit fffff9800eada000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0eadf850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0eadf990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0eadf9f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0eadfa80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`0eadfb00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`0eadfbb0 00000000`751039a2 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0eadfc20)
        00000000`0141f0c8 00000000`7511abfe wow64cpu!RemoveIoCompletionFault+0x41
        00000000`0141f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0141f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0141f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0141f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa8002915060  Cid 062c.0fec  Teb: 000000007efad000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8004846370  QueueObject
            fffffa8002915118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800486c230       Image:         Rtvscan.exe
        Wait Start TickCount      44825          Ticks: 1754 (0:00:00:27.362)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x00000000762f3242
        Stack Init fffff9800dac8db0 Current fffff9800dac8810
        Base fffff9800dac9000 Limit fffff9800dac3000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0dac8850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0dac8990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0dac89f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0dac8a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`0dac8b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`0dac8bb0 00000000`751039a2 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0dac8c20)
        00000000`019df0c8 00000000`7511abfe wow64cpu!RemoveIoCompletionFault+0x41
        00000000`019df1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`019df1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`019df730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`019df7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

Taskeng process (session 0)

```
PROCESS fffffa800492d330
    SessionId: 0  Cid: 0924    Peb: 7fffffdf000  ParentCid: 01a8
    DirBase: 38f1a000  ObjectTable: fffff88005e8dbd0  HandleCount: 278.
    Image: taskeng.exe
    VadRoot fffffa80049a78f0 Vads 119 Clone 0 Private 892. Modified 357. Locked 0.
    DeviceMap fffff88000007820
    Token                             fffff880024d3660
    ElapsedTime                       00:11:31.167
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         152800
    QuotaPoolUsage[NonPagedPool]      17120
    Working Set Sizes (now,min,max)  (2475, 50, 345) (9900KB, 200KB, 1380KB)
    PeakWorkingSetSize                2881
    VirtualSize                       72 Mb
    PeakVirtualSize                   75 Mb
    PageFaultCount                    3341
    MemoryPriority                    BACKGROUND
    BasePriority                      6
    CommitCharge                      1056

    Setting context for this process...
.process /p /r fffffa800492d330

    !peb
PEB at 000007fffffdf000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00000000ff050000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 0000000000192770 . 000000000027cb00
    Ldr.InLoadOrderModuleList:           0000000000192680 . 000000000027cae0
    Ldr.InMemoryOrderModuleList:         0000000000192690 . 000000000027caf0
            Base TimeStamp                     Module
        ff050000 4549b8ad Nov 02 09:21:49 2006 C:\Windows\system32\taskeng.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        76bc0000 4549d328 Nov 02 11:14:48 2006 C:\Windows\system32\kernel32.dll
     7fefea30000 4549d267 Nov 02 11:11:35 2006 C:\Windows\system32\ADVAPI32.dll
     7fefed90000 469c43bb Jul 17 05:21:15 2007 C:\Windows\system32\RPCRT4.dll
        76d00000 45d3ee19 Feb 15 05:22:33 2007 C:\Windows\system32\USER32.dll
     7fefec20000 4549d273 Nov 02 11:11:47 2006 C:\Windows\system32\GDI32.dll
     7fefdd40000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\system32\msvcrt.dll
     7fefddf0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\SHELL32.dll
     7fefda10000 4549d31f Nov 02 11:14:39 2006 C:\Windows\system32\SHLWAPI.dll
     7fefd760000 4549d317 Nov 02 11:14:31 2006 C:\Windows\system32\ole32.dll
     7fefdab0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\OLEAUT32.dll
     7fefd390000 4549d33f Nov 02 11:15:11 2006 C:\Windows\system32\Secur32.dll
     7fefb930000 4549d350 Nov 02 11:15:28 2006 C:\Windows\system32\XmlLite.dll
     7fefcd90000 4549d2b2 Nov 02 11:12:50 2006 C:\Windows\system32\MPR.dll
     7fefd9e0000 4549d2cb Nov 02 11:13:15 2006 C:\Windows\system32\IMM32.DLL
     7fefdc30000 4549d2e6 Nov 02 11:13:42 2006 C:\Windows\system32\MSCTF.dll
     7feff0c0000 4549d2a1 Nov 02 11:12:33 2006 C:\Windows\system32\LPK.DLL
     7fefd940000 4549d337 Nov 02 11:15:03 2006 C:\Windows\system32\USP10.dll
     7fefbe70000 4549d32b Nov 02 11:14:51 2006 C:\Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_1559f1c6f365a7fa\comctl32.dll
     7fefc620000 4549d31d Nov 02 11:14:37 2006 C:\Windows\system32\rsaenh.dll
     7fefdb90000 4549d282 Nov 02 11:12:02 2006 C:\Windows\system32\CLBCatQ.DLL
     7fef9750000 4549d35e Nov 02 11:15:42 2006 C:\Windows\system32\tschannel.dll
     7fef9610000 4549d272 Nov 02 11:11:46 2006 C:\Windows\system32\dimsjob.dll
     7fefd3b0000 4549d336 Nov 02 11:15:02 2006 C:\Windows\system32\USERENV.dll
     7fefcab0000 4549d2f2 Nov 02 11:13:54 2006 C:\Windows\system32\ncrypt.dll
     7fefcc50000 4549d344 Nov 02 11:15:16 2006 C:\Windows\system32\CRYPT32.dll
     7fefce00000 4549d2df Nov 02 11:13:35 2006 C:\Windows\system32\MSASN1.dll
```

```
     7fefc940000 4549d277 Nov 02 11:11:51 2006 C:\Windows\system32\GPAPI.dll
     7fefcc20000 4549d32d Nov 02 11:14:53 2006 C:\Windows\system32\slc.dll
     7fef9600000 4549d30f Nov 02 11:14:23 2006 C:\Windows\system32\pautoenr.dll
     7fefcf70000 4549d2fc Nov 02 11:14:04 2006 C:\Windows\system32\NETAPI32.dll
     7fefd530000 4549d310 Nov 02 11:14:24 2006 C:\Windows\system32\PSAPI.DLL
     7fefd590000 4549d396 Nov 02 11:16:38 2006 C:\Windows\system32\WLDAP32.dll
     7fefd540000 4549d38a Nov 02 11:16:26 2006 C:\Windows\system32\WS2_32.dll
     7feff0b0000 4549d370 Nov 02 11:16:00 2006 C:\Windows\system32\NSI.dll
     7fef8c70000 4549d265 Nov 02 11:11:33 2006 C:\Windows\system32\certcli.dll
     7fefc180000 4549d253 Nov 02 11:11:15 2006 C:\Windows\system32\ATL.DLL
     7fef8690000 4549d268 Nov 02 11:11:36 2006 C:\Windows\system32\certenroll.dll
     7fefcdd0000 4549d375 Nov 02 11:16:05 2006 C:\Windows\system32\NTDSAPI.dll
     7fefce40000 4549d288 Nov 02 11:12:08 2006 C:\Windows\system32\DNSAPI.dll
     7fefb2d0000 4549d376 Nov 02 11:16:06 2006 C:\Windows\system32\WinSCard.dll
     7fefc450000 4549d34e Nov 02 11:15:26 2006 C:\Windows\system32\WTSAPI32.dll
     7fefd1b0000 4549d380 Nov 02 11:16:16 2006 C:\Windows\system32\WINSTA.dll
     7fefec90000 470c5de6 Oct 10 06:06:46 2007 C:\Windows\system32\WININET.dll
        76f70000 4549b4d2 Nov 02 09:05:22 2006 C:\Windows\system32\Normaliz.dll
     7fefebc0000 4549d29c Nov 02 11:12:28 2006 C:\Windows\system32\iertutil.dll
     7fefc8f0000 4549d2e7 Nov 02 11:13:43 2006 C:\Windows\system32\mswsock.dll
     7fefc560000 4549d3a3 Nov 02 11:16:51 2006 C:\Windows\system32\wshtcpip.dll
     7fefca40000 4549d341 Nov 02 11:15:13 2006 C:\Windows\system32\credssp.dll
     7fefc670000 4549d321 Nov 02 11:14:41 2006 C:\Windows\system32\schannel.dll
     7fefc990000 4549d327 Nov 02 11:14:47 2006 C:\Windows\system32\kerberos.dll
     7fefce80000 4549d346 Nov 02 11:15:18 2006 C:\Windows\system32\cryptdll.dll
     7fefca60000 4549d252 Nov 02 11:11:14 2006 C:\Windows\system32\bcrypt.dll
     7fef8fd0000 4549d348 Nov 02 11:15:20 2006 C:\Windows\system32\cryptnet.dll
     7fef9760000 4549d343 Nov 02 11:15:15 2006 C:\Windows\system32\SensApi.dll
     7fefc5b0000 4549d384 Nov 02 11:16:20 2006 C:\Windows\system32\NTMARTA.DLL
     7fefce20000 4549d315 Nov 02 11:14:29 2006 C:\Windows\system32\SAMLIB.dll
     7fefc1c0000 4549d251 Nov 02 11:11:13 2006 C:\Windows\system32\Cabinet.dll
     7fefb3b0000 4549d2b1 Nov 02 11:12:49 2006 C:\Windows\system32\dssenh.dll
     7fef4560000 4549d24d Nov 02 11:11:09 2006 C:\Windows\system32\basecsp.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       0000000000190000
    ProcessParameters: 0000000000191d20
    WindowTitle:  'taskeng.exe'
    ImageFile:    'C:\Windows\system32\taskeng.exe'
    CommandLine:  'taskeng.exe {391890BE-7511-4EF4-B4D9-259CE26FF0C1}'
    DllPath:
'C:\Windows\system32;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Wind
ows;C:\Windows\System32\Wbem'
    Environment:  0000000000191310
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\system32\config\systemprofile\AppData\Roaming
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        LOCALAPPDATA=C:\Windows\system32\config\systemprofile\AppData\Local
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\TEMP
        TMP=C:\Windows\TEMP
        USERDOMAIN=DOMAIN
        USERNAME=COMPUTERNAME$
        USERPROFILE=C:\Windows\system32\config\systemprofile
```

```
        windir=C:\Windows

        THREAD fffffa80045718a0  Cid 0924.0928  Teb: 000007fffffdd000 Win32Thread: fffff900c07f9010
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004a0d520  SynchronizationEvent
            fffffa8004a6f040  SynchronizationTimer
            fffffa8004abcd30  SynchronizationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800492d330       Image:         taskeng.exe
        Wait Start TickCount      31173          Ticks: 15406 (0:00:04:00.335)
        Context Switch Count      81                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address taskeng!wWinMainCRTStartup (0x00000000ff078730)
        Stack Init fffff980109d9db0 Current fffff980109d9260
        Base fffff980109da000 Limit fffff980109d4000 Call 0
        Priority 7 BasePriority 6 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`109d92a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`109d93e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`109d9440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`109d94b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`109d9960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`109d9bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`109d9c20)
        00000000`000ef2d8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`000ef2e0 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`000ef3f0 00000000`ff05ea0e kernel32!WaitForMultipleObjects+0x11
        00000000`000ef430 00000000`ff05b5cf taskeng!Session::CentralControlLoop+0xaa
        00000000`000ef4d0 00000000`ff05b848 taskeng!RunSession+0x173
        00000000`000ef620 00000000`ff07859e taskeng!wWinMain+0x22c
        00000000`000ef6c0 00000000`76bfcdcd taskeng!std::_String_base::_Xran+0x266
        00000000`000ef780 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`000ef7b0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004a6f290  Cid 0924.092c  Teb: 000007fffffdb000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa8004a6f720  SynchronizationTimer
            fffffa8004a6fc20  SynchronizationEvent
            fffffa8004abfa20  SynchronizationTimer
            fffffa8004af8490  Thread
            fffffa8004a713d0  SynchronizationTimer
            fffffa8004b04750  SynchronizationEvent
            fffffa8004af8340  SynchronizationEvent
            fffffa8004b1d750  SynchronizationEvent
            fffffa8004b1e870  SynchronizationEvent
            fffffa8004a3c2a0  SynchronizationEvent
            fffffa8004b21af0  SynchronizationEvent
            fffffa8004a3c100  SynchronizationEvent
            fffffa80044a1e00  SynchronizationEvent
            fffffa8004b1d360  SynchronizationEvent
            fffffa8004b07cb0  SynchronizationEvent
            fffffa8004b141d0  SynchronizationEvent
            fffffa8004b1ec50  SynchronizationEvent
            fffffa8004b13a70  SynchronizationEvent
            fffffa800493ef00  SynchronizationEvent
            fffffa8004959f80  SynchronizationEvent
            fffffa8004a3c490  SynchronizationEvent
            fffffa8004b214b0  SynchronizationEvent
            fffffa8004b200e0  SynchronizationEvent
            fffffa8004b204b0  SynchronizationEvent
            fffffa8004785450  SynchronizationEvent
            fffffa8004785310  SynchronizationEvent
            fffffa80047851d0  SynchronizationEvent
            fffffa8004840ba0  SynchronizationEvent
            fffffa8004b30c10  SynchronizationEvent
            fffffa8004b31c50  SynchronizationEvent
            fffffa8004b2d858  NotificationEvent
            fffffa8004b318b0  SynchronizationEvent
            fffffa8004785040  SynchronizationEvent
            fffffa80047850f0  SynchronizationEvent
            fffffa80020aab70  SynchronizationEvent
            fffffa8002067140  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800492d330       Image:         taskeng.exe
        Wait Start TickCount      7531           Ticks: 39048 (0:00:10:09.152)
        Context Switch Count      53
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x0000000076df6930)
        Stack Init fffff9800b69bdb0 Current fffff9800b69b260
        Base fffff9800b69c000 Limit fffff9800b696000 Call 0
        Priority 8 BasePriority 6 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0b69b2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0b69b3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0b69b440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0b69b4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0b69b960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0b69bbb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0b69bc20)
        00000000`011dfa78 00000000`76df6b07 ntdll!NtWaitForMultipleObjects+0xa
        00000000`011dfa80 00000000`76bfcdcd ntdll!TppWaiterpThread+0x14d
        00000000`011dfd20 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`011dfd50 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004abe060  Cid 0924.0930  Teb: 000007fffffd9000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Alertable
            fffffa8004a6f9b0  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800492d330       Image:         taskeng.exe
        Wait Start TickCount      2320           Ticks: 44259 (0:00:11:30.444)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x0000000076e17860)
        Stack Init fffff980102e7db0 Current fffff980102e7860
        Base fffff980102e8000 Limit fffff980102e2000 Call 0
        Priority 7 BasePriority 6 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`102e78a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`102e79e0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`102e7a40 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`102e7ad0 fffff800`01c8a722 nt!IoRemoveIoCompletion+0x47
        fffff980`102e7b50 fffff800`01c4d733 nt!NtWaitForWorkViaWorkerFactory+0x1f1
        fffff980`102e7c20 00000000`76e21b4a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`102e7c20)
        00000000`00b6f5c8 00000000`76e17a20 ntdll!NtWaitForWorkViaWorkerFactory+0xa
        00000000`00b6f5d0 00000000`76bfcdcd ntdll!TppWorkerThread+0x23e
        00000000`00b6f840 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`00b6f870 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004af8bb0  Cid 0924.0934  Teb: 000007fffffd7000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8004ab3040  QueueObject
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800492d330       Image:         taskeng.exe
        Wait Start TickCount      27392          Ticks: 19187 (0:00:04:59.319)
        Context Switch Count      39
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff980102fcdb0 Current fffff980102fc810
        Base fffff980102fd000 Limit fffff980102f7000 Call 0
        Priority 7 BasePriority 6 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`102fc850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`102fc990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`102fc9f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`102fca80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`102fcb00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`102fcbb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`102fcc20)
        00000000`0199f968 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`0199f970 000007fe`fedce7a3 kernel32!GetQueuedCompletionStatus+0x48
        00000000`0199f9d0 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`0199fa60 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`0199fb10 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`0199fb40 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`0199fb80 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`0199fbb0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0199fbe0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004af8490  Cid 0924.0940  Teb: 000007fffffae000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80049cf940  NotificationEvent
            fffffa8004a4dda0  SynchronizationEvent
            fffffa8004a4dd40  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800492d330       Image:         taskeng.exe
        Wait Start TickCount      2328           Ticks: 44251 (0:00:11:30.320)
        Context Switch Count      54
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address taskeng!Job::RunCallback (0x00000000ff06d0bc)
        Stack Init fffff980102d2db0 Current fffff980102d2260
        Base fffff980102d3000 Limit fffff980102cd000 Call 0
        Priority 7 BasePriority 6 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`102d22a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`102d23e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`102d2440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`102d24b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`102d2960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`102d2bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`102d2c20)
        00000000`01ebfa58 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`01ebfa60 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`01ebfb70 00000000`ff06c93e kernel32!WaitForMultipleObjects+0x11
        00000000`01ebfbb0 00000000`ff06d106 taskeng!Job::Run+0x212
        00000000`01ebfcb0 00000000`76bfcdcd taskeng!Job::RunCallback+0x4a
        00000000`01ebfd20 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`01ebfd50 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004b04b10  Cid 0924.0944  Teb: 000007fffffac000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Alertable
            fffffa8004ab3950  QueueObject
        IRP List:
            fffffa8004687330: (0006,0358) Flags: 00060000  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa800492d330       Image:         taskeng.exe
        Wait Start TickCount      7536           Ticks: 39043 (0:00:10:09.074)
        Context Switch Count      773
        UserTime                  00:00:00.062
        KernelTime                00:00:00.171
        Win32 Start Address ntdll!TppWorkerThread (0x0000000076e17860)
        Stack Init fffff980108acdb0 Current fffff980108ac860
        Base fffff980108ad000 Limit fffff980108a7000 Call 0
        Priority 7 BasePriority 6 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`108ac8a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`108ac9e0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`108aca40 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`108acad0 fffff800`01c8a722 nt!IoRemoveIoCompletion+0x47
        fffff980`108acb50 fffff800`01c4d733 nt!NtWaitForWorkViaWorkerFactory+0x1f1
        fffff980`108acc20 00000000`76e21b4a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`108acc20)
        00000000`0210fbb8 00000000`76e17a20 ntdll!NtWaitForWorkViaWorkerFactory+0xa
        00000000`0210fbc0 00000000`76bfcdcd ntdll!TppWorkerThread+0x23e
        00000000`0210fe30 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0210fe60 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800200dbb0  Cid 0924.0c94  Teb: 000007fffffa8000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8001f7e6b0  SynchronizationEvent
            fffffa8001f7e650  SynchronizationEvent
            fffffa8001f7e6b0  SynchronizationEvent
            fffffa8001f7e6b0  SynchronizationEvent
            fffffa8001f7e6b0
```

```
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x0000000076e17860)
        Stack Init fffff980159f8db0 Current fffff980159f8260
        Base fffff980159f9000 Limit fffff980159f3000 Call 0
        Priority 7 BasePriority 6 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`159f82a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`159f83e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`159f8440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`159f84b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`159f8960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`159f8bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`159f8c20)
        00000000`029af8f8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`029af900 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`029afa10 000007fe`f456f97e kernel32!WaitForMultipleObjects+0x11
        00000000`029afa50 00000000`76dddd60 basecsp!I_TransactionManagerThreadProc+0xba
        00000000`029afaa0 00000000`76e17b59 ntdll!TppWorkpExecuteCallback+0x90
        00000000`029afb00 00000000`76bfcdcd ntdll!TppWorkerThread+0x3ad
        00000000`029afd70 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`029afda0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

Taskeng process (session 1)

```
PROCESS fffffa8004b4a040
    SessionId: 1  Cid: 0a14    Peb: 7fffffd6000  ParentCid: 01a8
    DirBase: 36d85000  ObjectTable: fffff88000fcdd80  HandleCount: 355.
    Image: taskeng.exe
    VadRoot fffffa800459d3b0 Vads 183 Clone 0 Private 1231. Modified 603. Locked 0.
    DeviceMap fffff88006100250
    Token                             fffff88000feea20
    ElapsedTime                       00:11:24.006
    UserTime                          00:00:00.062
    KernelTime                        00:00:00.171
    QuotaPoolUsage[PagedPool]         211336
    QuotaPoolUsage[NonPagedPool]      20032
    Working Set Sizes (now,min,max)  (2921, 50, 345) (11684KB, 200KB, 1380KB)
    PeakWorkingSetSize                3487
    VirtualSize                       113 Mb
    PeakVirtualSize                   117 Mb
    PageFaultCount                    4739
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      2815

    Setting context for this process...
.process /p /r fffffa8004b4a040

    !peb
PEB at 000007fffffd6000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00000000ff050000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00000000002a2810 . 0000000003bebcb0
    Ldr.InLoadOrderModuleList:           00000000002a2720 . 0000000003bebc90
    Ldr.InMemoryOrderModuleList:         00000000002a2730 . 0000000003bebca0
            Base TimeStamp                     Module
        ff050000 4549b8ad Nov 02 09:21:49 2006 C:\Windows\system32\taskeng.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        76bc0000 4549d328 Nov 02 11:14:48 2006 C:\Windows\system32\kernel32.dll
     7fefea30000 4549d267 Nov 02 11:11:35 2006 C:\Windows\system32\ADVAPI32.dll
     7fefed90000 469c43bb Jul 17 05:21:15 2007 C:\Windows\system32\RPCRT4.dll
        76d00000 45d3ee19 Feb 15 05:22:33 2007 C:\Windows\system32\USER32.dll
     7fefec20000 4549d273 Nov 02 11:11:47 2006 C:\Windows\system32\GDI32.dll
     7fefdd40000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\system32\msvcrt.dll
     7fefddf0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\SHELL32.dll
     7fefda10000 4549d31f Nov 02 11:14:39 2006 C:\Windows\system32\SHLWAPI.dll
     7fefd760000 4549d317 Nov 02 11:14:31 2006 C:\Windows\system32\ole32.dll
     7fefdab0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\OLEAUT32.dll
     7fefd390000 4549d33f Nov 02 11:15:11 2006 C:\Windows\system32\Secur32.dll
     7fefb930000 4549d350 Nov 02 11:15:28 2006 C:\Windows\system32\XmlLite.dll
     7fefcd90000 4549d2b2 Nov 02 11:12:50 2006 C:\Windows\system32\MPR.dll
     7fefd9e0000 4549d2cb Nov 02 11:13:15 2006 C:\Windows\system32\IMM32.DLL
     7fefdc30000 4549d2e6 Nov 02 11:13:42 2006 C:\Windows\system32\MSCTF.dll
     7feff0c0000 4549d2a1 Nov 02 11:12:33 2006 C:\Windows\system32\LPK.DLL
     7fefd940000 4549d337 Nov 02 11:15:03 2006 C:\Windows\system32\USP10.dll
     7fefbe70000 4549d32b Nov 02 11:14:51 2006 C:\Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_1559f1c6f365a7fa\comctl32.dll
     7fefc620000 4549d31d Nov 02 11:14:37 2006 C:\Windows\system32\rsaenh.dll
     7fefdb90000 4549d282 Nov 02 11:12:02 2006 C:\Windows\system32\CLBCatQ.DLL
     7fef9750000 4549d35e Nov 02 11:15:42 2006 C:\Windows\system32\tschannel.dll
     7fefc330000 4549d33b Nov 02 11:15:07 2006 C:\Windows\system32\uxtheme.dll
     7fef8650000 4549d338 Nov 02 11:15:04 2006 C:\Windows\System32\PlaySndSrv.dll
     7fefb360000 4549d36f Nov 02 11:15:59 2006 C:\Windows\System32\WINMM.dll
     7fefb310000 4549d318 Nov 02 11:14:32 2006 C:\Windows\System32\OLEACC.dll
     7fef9340000 4549d275 Nov 02 11:11:49 2006 C:\Windows\System32\HotStartUserAgent.dll
```

```
     7fefcc20000 4549d32d Nov 02 11:14:53 2006 C:\Windows\System32\slc.dll
     7fef8c40000 4549d2e9 Nov 02 11:13:45 2006 C:\Windows\system32\MsCtfMonitor.dll
     7fef84e0000 4549d2dd Nov 02 11:13:33 2006 C:\Windows\system32\MSUTB.dll
     7fef8c50000 4549d2b7 Nov 02 11:12:55 2006 C:\Windows\system32\dwmapi.dll
     7fef9610000 4549d272 Nov 02 11:11:46 2006 C:\Windows\system32\dimsjob.dll
     7fefd3b0000 4549d336 Nov 02 11:15:02 2006 C:\Windows\system32\USERENV.dll
     7fefcab0000 4549d2f2 Nov 02 11:13:54 2006 C:\Windows\system32\ncrypt.dll
     7fefcc50000 4549d344 Nov 02 11:15:16 2006 C:\Windows\system32\CRYPT32.dll
     7fefce00000 4549d2df Nov 02 11:13:35 2006 C:\Windows\system32\MSASN1.dll
     7fefc940000 4549d277 Nov 02 11:11:51 2006 C:\Windows\system32\GPAPI.dll
     7fef9600000 4549d30f Nov 02 11:14:23 2006 C:\Windows\system32\pautoenr.dll
     7fefcf70000 4549d2fc Nov 02 11:14:04 2006 C:\Windows\system32\NETAPI32.dll
     7fefd530000 4549d310 Nov 02 11:14:24 2006 C:\Windows\system32\PSAPI.DLL
     7fefd590000 4549d396 Nov 02 11:16:38 2006 C:\Windows\system32\WLDAP32.dll
     7fefd540000 4549d38a Nov 02 11:16:26 2006 C:\Windows\system32\WS2_32.dll
     7feff0b0000 4549d370 Nov 02 11:16:00 2006 C:\Windows\system32\NSI.dll
     7fef8c70000 4549d265 Nov 02 11:11:33 2006 C:\Windows\system32\certcli.dll
     7fefc180000 4549d253 Nov 02 11:11:15 2006 C:\Windows\system32\ATL.DLL
     7fef8690000 4549d268 Nov 02 11:11:36 2006 C:\Windows\system32\certenroll.dll
     7fefcdd0000 4549d375 Nov 02 11:16:05 2006 C:\Windows\system32\NTDSAPI.dll
     7fefce40000 4549d288 Nov 02 11:12:08 2006 C:\Windows\system32\DNSAPI.dll
     7fefb2d0000 4549d376 Nov 02 11:16:06 2006 C:\Windows\system32\WinSCard.dll
     7fefc450000 4549d34e Nov 02 11:15:26 2006 C:\Windows\system32\WTSAPI32.dll
     7fefd1b0000 4549d380 Nov 02 11:16:16 2006 C:\Windows\system32\WINSTA.dll
     7fefec90000 470c5de6 Oct 10 06:06:46 2007 C:\Windows\system32\WININET.dll
        76f70000 4549b4d2 Nov 02 09:05:22 2006 C:\Windows\system32\Normaliz.dll
     7fefebc0000 4549d29c Nov 02 11:12:28 2006 C:\Windows\system32\iertutil.dll
     7fefb280000 4549d336 Nov 02 11:15:02 2006 C:\Windows\system32\wdmaud.drv
        75160000 4549d331 Nov 02 11:14:57 2006 C:\Windows\system32\ksuser.dll
     7fefc2d0000 4549d273 Nov 02 11:11:47 2006 C:\Windows\system32\AVRT.dll
     7fefc2e0000 4549d2a1 Nov 02 11:12:33 2006 C:\Windows\system32\MMDevAPI.DLL
     7fefeed0000 4549d318 Nov 02 11:14:32 2006 C:\Windows\system32\SETUPAPI.dll
     7fefc1e0000 4549d381 Nov 02 11:16:17 2006 C:\Windows\system32\WINTRUST.dll
     7fefda90000 462443ee Apr 17 04:50:06 2007 C:\Windows\system32\imagehlp.dll
     7fefb0c0000 4549d258 Nov 02 11:11:20 2006 C:\Windows\System32\audioses.dll
     7fefb040000 4549d256 Nov 02 11:11:18 2006 C:\Windows\System32\audioeng.dll
     7fefb270000 4549d2cd Nov 02 11:13:17 2006 C:\Windows\system32\msacm32.drv
     7fefb120000 4549d2cc Nov 02 11:13:16 2006 C:\Windows\system32\MSACM32.dll
     7fefb240000 4549d2bf Nov 02 11:13:03 2006 C:\Windows\system32\midimap.dll
     7fef73a0000 4549d351 Nov 02 11:15:29 2006 C:\Windows\System32\TMM.dll
     7fefc580000 4549d351 Nov 02 11:15:29 2006 C:\Windows\System32\POWRPROF.dll
     7fef71b0000 4549d25d Nov 02 11:11:25 2006 C:\Windows\System32\d3d9.dll
     7fefca50000 4549d336 Nov 02 11:15:02 2006 C:\Windows\System32\VERSION.dll
     7fef8020000 4549d25c Nov 02 11:11:24 2006 C:\Windows\System32\d3d8thk.dll
     7fefc5b0000 4549d384 Nov 02 11:16:20 2006 C:\Windows\system32\NTMARTA.DLL
     7fefce20000 4549d315 Nov 02 11:14:29 2006 C:\Windows\system32\SAMLIB.dll
        10000000 453ec166 Oct 25 02:44:06 2006 C:\Windows\system32\atitmm64.dll
     7fef7600000 4549d30d Nov 02 11:14:21 2006 C:\Windows\System32\QAgent.dll
     7fef79c0000 4549d31b Nov 02 11:14:35 2006 C:\Windows\System32\QUtil.dll
     7fefcbb0000 4549d349 Nov 02 11:15:21 2006 C:\Windows\System32\wevtapi.dll
     7fefac60000 4549d280 Nov 02 11:12:00 2006 C:\Windows\System32\fwpuclnt.dll
     7fef7040000 4549d26c Nov 02 11:11:40 2006 C:\Windows\System32\AuxiliaryDisplayServices.dll
     7fefba40000 4549d384 Nov 02 11:16:20 2006 C:\Windows\System32\Wlanapi.dll
     7fef7900000 4549d322 Nov 02 11:14:42 2006 C:\Windows\System32\OneX.DLL
     7fef78e0000 4549d26a Nov 02 11:11:38 2006 C:\Windows\System32\eappprxy.dll
     7fef7540000 4549d267 Nov 02 11:11:35 2006 C:\Windows\System32\eappcfg.dll
     7fefca60000 4549d252 Nov 02 11:11:14 2006 C:\Windows\System32\bcrypt.dll
     7fefd310000 4549d247 Nov 02 11:11:03 2006 C:\Windows\system32\apphelp.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       00000000002a0000
    ProcessParameters: 00000000002a1d50
    WindowTitle:  'taskeng.exe'
    ImageFile:    'C:\Windows\system32\taskeng.exe'
    CommandLine:  'taskeng.exe {1C6D6556-073A-4078-B11A-03C2A9B6E6CE}'
    DllPath:
'C:\Windows\system32;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Wind
ows;C:\Windows\System32\Wbem'
    Environment:  00000000002a1310
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\UserName\AppData\Roaming
```

```
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        HOMEDRIVE=C:
        HOMEPATH=\Users\UserName
        LOCALAPPDATA=C:\Users\UserName\AppData\Local
        LOGONSERVER=\\COMPUTERNAME
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Users\UserName\AppData\Local\Temp
        TMP=C:\Users\UserName\AppData\Local\Temp
        USERDOMAIN=COMPUTERNAME
        USERNAME=UserName
        USERPROFILE=C:\Users\UserName
        windir=C:\Windows


        THREAD fffffa8004b43bb0  Cid 0a14.0a18  Teb: 000007fffffde000 Win32Thread: fffff900c207f010
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004b6ffe0  SynchronizationEvent
            fffffa8004b6fe30  SynchronizationTimer
            fffffa8004b6fce0  SynchronizationTimer
            fffffa8004b4ab60  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004b4a040       Image:         taskeng.exe
        Wait Start TickCount      31634          Ticks: 14945 (0:00:03:53.143)
        Context Switch Count      593                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address taskeng!wWinMainCRTStartup (0x00000000ff078730)
        Stack Init fffff9801062cdb0 Current fffff9801062c260
        Base fffff9801062d000 Limit fffff98010624000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1062c2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1062c3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`1062c440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`1062c4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`1062c960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`1062cbb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1062cc20)
        00000000`0011f418 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0011f420 00000000`76d1e96d kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0011f530 00000000`76d1e85e USER32!RealMsgWaitForMultipleObjectsEx+0x129
        00000000`0011f5d0 00000000`76d13680 USER32!MsgWaitForMultipleObjectsEx+0x46
        00000000`0011f610 00000000`ff05e9f6 USER32!MsgWaitForMultipleObjects+0x20
        00000000`0011f650 00000000`ff05b5cf taskeng!Session::CentralControlLoop+0x92
        00000000`0011f6f0 00000000`ff05b848 taskeng!RunSession+0x173
        00000000`0011f840 00000000`ff07859e taskeng!wWinMain+0x22c
        00000000`0011f8e0 00000000`76bfcdcd taskeng!std::_String_base::_Xran+0x266
        00000000`0011f9a0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0011f9d0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004b36310  Cid 0a14.0a1c  Teb: 000007fffffdc000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa8004b71b60  SynchronizationTimer
            fffffa8004b4dbe0  SynchronizationEvent
            fffffa8004b8d060  Thread
            fffffa8004b98bb0  Thread
            fffffa8004b93060  Thread
            fffffa8004b35040  SynchronizationTimer
            fffffa8004780b50  SynchronizationTimer
            fffffa80041f6850  SynchronizationEvent
            fffffa8004b77a90  SynchronizationEvent
            fffffa8004c45060  Thread
            fffffa8001fe84c0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004b4a040       Image:         taskeng.exe
        Wait Start TickCount      45939          Ticks: 640 (0:00:00:09.984)
        Context Switch Count      64
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x0000000076df6930)
        Stack Init fffff98010851db0 Current fffff98010851260
        Base fffff98010852000 Limit fffff9801084c000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`108512a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`108513e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`10851440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`108514b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`10851960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`10851bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`10851c20)
        00000000`0024f8e8 00000000`76df6b07 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0024f8f0 00000000`76bfcdcd ntdll!TppWaiterpThread+0x14d
        00000000`0024fb90 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0024fbc0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004b72a50  Cid 0a14.0a20  Teb: 000007fffffda000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Alertable
            fffffa8004a2aae0  QueueObject
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004b4a040       Image:         taskeng.exe
        Wait Start TickCount      7948           Ticks: 38631 (0:00:10:02.647)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x0000000076e17860)
        Stack Init fffff98010750db0 Current fffff98010750860
        Base fffff98010751000 Limit fffff9801074b000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`107508a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`107509e0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`10750a40 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`10750ad0 fffff800`01c8a722 nt!IoRemoveIoCompletion+0x47
        fffff980`10750b50 fffff800`01c4d733 nt!NtWaitForWorkViaWorkerFactory+0x1f1
        fffff980`10750c20 00000000`76e21b4a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`10750c20)
        00000000`020ef838 00000000`76e17a20 ntdll!NtWaitForWorkViaWorkerFactory+0xa
        00000000`020ef840 00000000`76bfcdcd ntdll!TppWorkerThread+0x23e
        00000000`020efab0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`020efae0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004b8d060  Cid 0a14.0a4c  Teb: 000007fffffac000 Win32Thread: fffff900c06dc280
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004b88f40  NotificationEvent
            fffffa8004b6ed80  SynchronizationEvent
            fffffa8004b6ed20  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004b4a040       Image:         taskeng.exe
        Wait Start TickCount      2794           Ticks: 43785 (0:00:11:23.050)
        Context Switch Count      70                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address taskeng!Job::RunCallback (0x00000000ff06d0bc)
        Stack Init fffff9801068bdb0 Current fffff9801068b260
        Base fffff9801068c000 Limit fffff98010685000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1068b2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1068b3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`1068b440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`1068b4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`1068b960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`1068bbb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1068bc20)
        00000000`0348f748 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0348f750 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0348f860 00000000`ff06c93e kernel32!WaitForMultipleObjects+0x11
        00000000`0348f8a0 00000000`ff06d106 taskeng!Job::Run+0x212
        00000000`0348f9a0 00000000`76bfcdcd taskeng!Job::RunCallback+0x4a
        00000000`0348fa10 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0348fa40 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004b98bb0  Cid 0a14.0a54  Teb: 000007fffffa8000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004baecb0  NotificationEvent
            fffffa8004b8e860  SynchronizationEvent
            fffffa8004b8de10  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004b4a040       Image:         taskeng.exe
        Wait Start TickCount      2805           Ticks: 43774 (0:00:11:22.878)
        Context Switch Count      62
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address taskeng!Job::RunCallback (0x00000000ff06d0bc)
        Stack Init fffff98010788db0 Current fffff98010788260
        Base fffff98010789000 Limit fffff98010783000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`107882a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`107883e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`10788440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`107884b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`10788960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`10788bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`10788c20)
        00000000`0364f958 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0364f960 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0364fa70 00000000`ff06c93e kernel32!WaitForMultipleObjects+0x11
        00000000`0364fab0 00000000`ff06d106 taskeng!Job::Run+0x212
        00000000`0364fbb0 00000000`76bfcdcd taskeng!Job::RunCallback+0x4a
        00000000`0364fc20 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0364fc50 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004b93060  Cid 0a14.0a58  Teb: 000007fffffa6000 Win32Thread: fffff900c2081780
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004ba67e0  NotificationEvent
            fffffa8004b98410  SynchronizationEvent
            fffffa8004b8b460  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004b4a040       Image:         taskeng.exe
        Wait Start TickCount      2804           Ticks: 43775 (0:00:11:22.894)
        Context Switch Count      301                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address taskeng!Job::RunCallback (0x00000000ff06d0bc)
        Stack Init fffff980106d7db0 Current fffff980106d7260
        Base fffff980106d8000 Limit fffff980106d1000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`106d72a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`106d73e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`106d7440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`106d74b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`106d7960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`106d7bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`106d7c20)
        00000000`0383fb08 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0383fb10 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0383fc20 00000000`ff06c93e kernel32!WaitForMultipleObjects+0x11
        00000000`0383fc60 00000000`ff06d106 taskeng!Job::Run+0x212
        00000000`0383fd60 00000000`76bfcdcd taskeng!Job::RunCallback+0x4a
        00000000`0383fdd0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0383fe00 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004b77bb0  Cid 0a14.0a74  Teb: 000007fffffa2000 Win32Thread: fffff900c1c212b0
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004bc1f30  NotificationEvent
            fffffa8004745040  NotificationEvent
            fffffa8004327ae0  NotificationEvent
            fffffa800460abb0  NotificationEvent
            fffffa8004bf5a70  NotificationEvent
            fffffa8004bf5990  NotificationEvent
            fffffa8004b9ae10  NotificationEvent
            fffffa8004b9ad30  NotificationEvent
            fffffa8004b5d200  NotificationEvent
            fffffa8004b894c0  NotificationEvent
            fffffa8004bcab40  NotificationEvent
            fffffa8004b48730  NotificationEvent
            fffffa8004b48650  NotificationEvent
            fffffa800459df90  NotificationEvent
            fffffa800459deb0  NotificationEvent
            fffffa800409c9b0  NotificationEvent
            fffffa800439b8d0  NotificationEvent
            fffffa8004ba5820  SynchronizationEvent
            fffffa8004bc4a30  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004b4a040       Image:         taskeng.exe
        Wait Start TickCount      45975          Ticks: 604 (0:00:00:09.422)
        Context Switch Count      9996                LargeStack
        UserTime                  00:00:00.031
        KernelTime                00:00:00.062
        Win32 Start Address MsCtfMonitor!MsCtfMonitor::ThreadProc (0x000007fef8c428c0)
        Stack Init fffff980106fddb0 Current fffff980106fd260
        Base fffff980106fe000 Limit fffff980106f6000 Call 0
        Priority 12 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`106fd2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`106fd3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`106fd440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`106fd4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`106fd960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`106fdbb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`106fdc20)
        00000000`0350f8f8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0350f900 00000000`76d1e96d kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0350fa10 00000000`76d1e85e USER32!RealMsgWaitForMultipleObjectsEx+0x129
        00000000`0350fab0 00000000`76d13680 USER32!MsgWaitForMultipleObjectsEx+0x46
        00000000`0350faf0 000007fe`f8c43459 USER32!MsgWaitForMultipleObjects+0x20
        00000000`0350fb30 000007fe`f8c429de MsCtfMonitor!DoMsCtfMonitor+0x321
        00000000`0350fcc0 00000000`76bfcdcd MsCtfMonitor!MsCtfMonitor::ThreadProc+0x11e
        00000000`0350ff00 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0350ff30 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004bf5460  Cid 0a14.0a94  Teb: 000007fffffa0000 Win32Thread: fffff900c20814d0
WAIT: (WrLpcReceive) UserMode Non-Alertable
            fffffa8004bf57f0  Semaphore Limit 0x1
            fffffa8004bf5518  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004b4a040       Image:         taskeng.exe
        Wait Start TickCount      45968          Ticks: 611 (0:00:00:09.531)
        Context Switch Count      3384                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address MSCTF!CCtfServerPort::StaticServerThread (0x000007fefdc498d0)
        Stack Init fffff98010710db0 Current fffff980107107a0
        Base fffff98010711000 Limit fffff9801070a000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`107107e0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`10710920 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`10710980 fffff800`01eb3788 nt!KeWaitForSingleObject+0x5f5
        fffff980`10710a00 fffff800`01eb3eda nt!AlpcpReceiveMessagePort+0x298
        fffff980`10710a60 fffff800`01eb74ba nt!AlpcpReceiveMessage+0x246
        fffff980`10710b00 fffff800`01c4d733 nt!NtAlpcSendWaitReceivePort+0x1da
        fffff980`10710bb0 00000000`76e20aca nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`10710c20)
        00000000`039ae338 000007fe`fdc320c1 ntdll!NtAlpcSendWaitReceivePort+0xa
        00000000`039ae340 000007fe`fdc49a56 MSCTF!CCtfServerPort::ServerLoop+0x15a
        00000000`039af4b0 000007fe`fdc498f2 MSCTF!CCtfServerPort::ServerThread+0x136
        00000000`039af790 00000000`76bfcdcd MSCTF!CCtfServerPort::StaticServerThread+0x28
        00000000`039af7c0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`039af7f0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004c2a060  Cid 0a14.0a98  Teb: 000007fffff9e000 Win32Thread: fffff900c06e0230
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8004c125b0  QueueObject
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004b4a040       Image:         taskeng.exe
        Wait Start TickCount      2832           Ticks: 43747 (0:00:11:22.457)
        Context Switch Count      138                  LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address wdmaud!mxdMessageThreadProc (0x000007fefb286f50)
        Stack Init fffff98010749db0 Current fffff98010749810
        Base fffff9801074a000 Limit fffff98010741000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`10749850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`10749990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`107499f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`10749a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`10749b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`10749bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`10749c20)
        00000000`03b5fab8 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`03b5fac0 000007fe`fb286fc1 kernel32!GetQueuedCompletionStatus+0x48
        00000000`03b5fb20 00000000`76bfcdcd wdmaud!mxdMessageThreadProc+0x71
        00000000`03b5fb60 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`03b5fb90 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004c2abb0  Cid 0a14.0a9c  Teb: 000007fffff9c000 Win32Thread: fffff900c1c1f520
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa8004b99f40  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004b4a040       Image:         taskeng.exe
        Wait Start TickCount      2825           Ticks: 43754 (0:00:11:22.566)
        Context Switch Count      4                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdmaud!CTaskThread::TaskThreadProc (0x000007fefb295e94)
        Stack Init fffff98010723db0 Current fffff98010723740
        Base fffff98010724000 Limit fffff9801071d000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`10723780 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`107238c0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`10723920 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`107239a0 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`10723a40 fffff960`000c7e1e win32k!xxxSleepThread+0x56
        fffff980`10723a70 fffff960`000c7f25 win32k!xxxRealInternalGetMessage+0x72e
        fffff980`10723b50 fffff960`000c97e4 win32k!xxxInternalGetMessage+0x35
        fffff980`10723b90 fffff800`01c4d733 win32k!NtUserGetMessage+0x64
        fffff980`10723c20 00000000`76d1e6aa nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`10723c20)
        00000000`036cfd38 00000000`76d1e6ea USER32!ZwUserGetMessage+0xa
        00000000`036cfd40 000007fe`fb295f46 USER32!GetMessageW+0x34
        00000000`036cfd70 00000000`76bfcdcd wdmaud!CTaskThread::TaskThreadProc+0xb2
        00000000`036cfde0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`036cfe10 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004b976c0  Cid 0a14.0aa0  Teb: 000007fffff9a000 Win32Thread: fffff900c1ec1ab0
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004bcae20  SynchronizationEvent
            fffffa8004c21eb0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004b4a040       Image:         taskeng.exe
        Wait Start TickCount      27753          Ticks: 18826 (0:00:04:53.687)
        Context Switch Count      747                LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address wdmaud!CWorker::_StaticThreadProc (0x000007fefb291a18)
        Stack Init fffff98012ad1db0 Current fffff98012ad1260
        Base fffff98012ad2000 Limit fffff98012acb000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`12ad12a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12ad13e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`12ad1440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`12ad14b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`12ad1960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`12ad1bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12ad1c20)
        00000000`038df7b8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`038df7c0 000007fe`fb291aa8 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`038df8d0 00000000`76bfcdcd wdmaud!CWorker::_StaticThreadProc+0x90
        00000000`038df920 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`038df950 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80047723a0  Cid 0a14.0aac  Teb: 000007fffff98000 Win32Thread: fffff900c06e0820
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa8004b23630  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004b4a040       Image:         taskeng.exe
        Wait Start TickCount      45939          Ticks: 640 (0:00:00:09.984)
        Context Switch Count      392                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address WINMM!mciwindow (0x000007fefb3616c0)
        Stack Init fffff9801097adb0 Current fffff9801097a740
        Base fffff9801097b000 Limit fffff98010973000 Call 0
        Priority 12 BasePriority 10 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1097a780 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1097a8c0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`1097a920 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`1097a9a0 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`1097aa40 fffff960`000c7e1e win32k!xxxSleepThread+0x56
        fffff980`1097aa70 fffff960`000c7f25 win32k!xxxRealInternalGetMessage+0x72e
        fffff980`1097ab50 fffff960`000c97e4 win32k!xxxInternalGetMessage+0x35
        fffff980`1097ab90 fffff800`01c4d733 win32k!NtUserGetMessage+0x64
        fffff980`1097ac20 00000000`76d1e6aa nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1097ac20)
        00000000`03cdf6f8 00000000`76d1bf4e USER32!ZwUserGetMessage+0xa
        00000000`03cdf700 000007fe`fb361785 USER32!GetMessageA+0xc3
        00000000`03cdf730 00000000`76bfcdcd WINMM!mciwindow+0x174
        00000000`03cdf7d0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`03cdf800 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004c45060  Cid 0a14.0b6c  Teb: 000007fffff96000 Win32Thread: fffff900c1ec1d60
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004bb1100  NotificationEvent
            fffffa8004baa6d0  SynchronizationEvent
            fffffa8004c30770  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004b4a040       Image:         taskeng.exe
        Wait Start TickCount      2981           Ticks: 43598 (0:00:11:20.133)
        Context Switch Count      30                 LargeStack
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address taskeng!Job::RunCallback (0x00000000ff06d0bc)
        Stack Init fffff98012aabdb0 Current fffff98012aab260
        Base fffff98012aac000 Limit fffff98012aa4000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`12aab2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12aab3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`12aab440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`12aab4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`12aab960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`12aabbb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12aabc20)
        00000000`03d8fb18 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`03d8fb20 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`03d8fc30 00000000`ff06c93e kernel32!WaitForMultipleObjects+0x11
        00000000`03d8fc70 00000000`ff06d106 taskeng!Job::Run+0x212
        00000000`03d8fd70 00000000`76bfcdcd taskeng!Job::RunCallback+0x4a
        00000000`03d8fde0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`03d8fe10 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004c47060  Cid 0a14.0b70  Teb: 000007fffff94000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80047598a0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004b4a040       Image:         taskeng.exe
        Wait Start TickCount      2981           Ticks: 43598 (0:00:11:20.133)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address TMM!CTMMJob::ThreadProc (0x000007fef73aa284)
        Stack Init fffff9800d09edb0 Current fffff9800d09e960
        Base fffff9800d09f000 Limit fffff9800d099000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0d09e9a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0d09eae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0d09eb40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0d09ebc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0d09ec20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0d09ec20)
        00000000`0460fac8 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`0460fad0 000007fe`f73aa303 kernel32!WaitForSingleObjectEx+0x9c
        00000000`0460fb90 00000000`76bfcdcd TMM!CTMMJob::ThreadProc+0x7f
        00000000`0460fbc0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0460fbf0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8001f01060  Cid 0a14.0864  Teb: 000007fffffd4000 Win32Thread: fffff900c1fbfd60
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa800409ddd0  QueueObject
            fffffa8001f01118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004b4a040       Image:         taskeng.exe
        Wait Start TickCount      45939          Ticks: 640 (0:00:00:09.984)
        Context Switch Count      59                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff9801e458db0 Current fffff9801e458810
        Base fffff9801e459000 Limit fffff9801e452000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1e458850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1e458990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`1e4589f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`1e458a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`1e458b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`1e458bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1e458c20)
        00000000`046ef908 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`046ef910 000007fe`fedce7a3 kernel32!GetQueuedCompletionStatus+0x48
        00000000`046ef970 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`046efa00 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`046efab0 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`046efae0 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`046efb20 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`046efb50 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`046efb80 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8002a6cbb0  Cid 0a14.0d4c  Teb: 000007fffffd8000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa800409ddd0  QueueObject
            fffffa8002a6cc68  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004b4a040       Image:         taskeng.exe
        Wait Start TickCount      45885          Ticks: 694 (0:00:00:10.826)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff9801db9ddb0 Current fffff9801db9d810
        Base fffff9801db9e000 Limit fffff9801db98000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1db9d850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1db9d990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`1db9d9f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`1db9da80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`1db9db00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`1db9dbb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1db9dc20)
        00000000`035cf958 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`035cf960 000007fe`fedce7a3 kernel32!GetQueuedCompletionStatus+0x48
        00000000`035cf9c0 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`035cfa50 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`035cfb00 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`035cfb30 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`035cfb70 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`035cfba0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`035cfbd0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8002089bb0  Cid 0a14.0ef4  Teb: 000007fffffae000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Alertable
            fffffa8004b8d8e0  QueueObject
            fffffa8002089c68  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004b4a040       Image:         taskeng.exe
        Wait Start TickCount      45939          Ticks: 640 (0:00:00:09.984)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x0000000076e17860)
        Stack Init fffff98004523db0 Current fffff98004523860
        Base fffff98004524000 Limit fffff9800451e000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`045238a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`045239e0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`04523a40 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`04523ad0 fffff800`01c8a722 nt!IoRemoveIoCompletion+0x47
        fffff980`04523b50 fffff800`01c4d733 nt!NtWaitForWorkViaWorkerFactory+0x1f1
        fffff980`04523c20 00000000`76e21b4a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`04523c20)
        00000000`02d5f5c8 00000000`76e17a20 ntdll!NtWaitForWorkViaWorkerFactory+0xa
        00000000`02d5f5d0 00000000`76bfcdcd ntdll!TppWorkerThread+0x23e
        00000000`02d5f840 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02d5f870 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

Dwm process

```
PROCESS fffffa8004b8a9c0
    SessionId: 1  Cid: 0a44    Peb: 7fffffdb000  ParentCid: 018c
    DirBase: 36d1c000  ObjectTable: fffff88002436a10  HandleCount:  96.
    Image: dwm.exe
    VadRoot fffffa8004b5ef80 Vads 78 Clone 0 Private 446. Modified 230. Locked 0.
    DeviceMap fffff88006100250
    Token                             fffff88000c13ab0
    ElapsedTime                       00:11:23.835
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         136048
    QuotaPoolUsage[NonPagedPool]      7456
    Working Set Sizes (now,min,max)  (1440, 50, 345) (5760KB, 200KB, 1380KB)
    PeakWorkingSetSize                2109
    VirtualSize                       68 Mb
    PeakVirtualSize                   80 Mb
    PageFaultCount                    2220
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      593

    Setting context for this process...
.process /p /r fffffa8004b8a9c0

    !peb
PEB at 000007fffffdb000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00000000ff350000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00000000002d2760 . 00000000002f9cc0
    Ldr.InLoadOrderModuleList:           00000000002d2670 . 00000000002f9ca0
    Ldr.InMemoryOrderModuleList:         00000000002d2680 . 00000000002f9cb0
            Base TimeStamp                     Module
        ff350000 4549b7e9 Nov 02 09:18:33 2006 C:\Windows\system32\Dwm.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        76bc0000 4549d328 Nov 02 11:14:48 2006 C:\Windows\system32\kernel32.dll
     7fefea30000 4549d267 Nov 02 11:11:35 2006 C:\Windows\system32\ADVAPI32.dll
     7fefed90000 469c43bb Jul 17 05:21:15 2007 C:\Windows\system32\RPCRT4.dll
     7fefec20000 4549d273 Nov 02 11:11:47 2006 C:\Windows\system32\GDI32.dll
        76d00000 45d3ee19 Feb 15 05:22:33 2007 C:\Windows\system32\USER32.dll
     7fefdd40000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\system32\msvcrt.dll
     7fefd760000 4549d317 Nov 02 11:14:31 2006 C:\Windows\system32\ole32.dll
     7fefdab0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\OLEAUT32.dll
     7fefc330000 4549d33b Nov 02 11:15:07 2006 C:\Windows\system32\UxTheme.dll
     7fefd9e0000 4549d2cb Nov 02 11:13:15 2006 C:\Windows\system32\IMM32.dll
     7fefdc30000 4549d2e6 Nov 02 11:13:42 2006 C:\Windows\system32\MSCTF.dll
     7fef8670000 4549d2b8 Nov 02 11:12:56 2006 C:\Windows\system32\dwmredir.dll
     7fefaaa0000 4549d31e Nov 02 11:14:38 2006 C:\Windows\system32\SLWGA.dll
     7fefd5f0000 470c5dac Oct 10 06:05:48 2007 C:\Windows\system32\urlmon.dll
     7fefda10000 4549d31f Nov 02 11:14:39 2006 C:\Windows\system32\SHLWAPI.dll
     7fefebc0000 4549d29c Nov 02 11:12:28 2006 C:\Windows\system32\iertutil.dll
     7fefc450000 4549d34e Nov 02 11:15:26 2006 C:\Windows\system32\WTSAPI32.dll
     7fefcc20000 4549d32d Nov 02 11:14:53 2006 C:\Windows\system32\slc.dll
     7feff0c0000 4549d2a1 Nov 02 11:12:33 2006 C:\Windows\system32\LPK.DLL
     7fefd940000 4549d337 Nov 02 11:15:03 2006 C:\Windows\system32\USP10.dll
     7fefbe70000 4549d32b Nov 02 11:14:51 2006 C:\Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_1559f1c6f365a7fa\comctl32.dll
     7fefc5b0000 4549d384 Nov 02 11:16:20 2006 C:\Windows\system32\NTMARTA.DLL
     7fefd590000 4549d396 Nov 02 11:16:38 2006 C:\Windows\system32\WLDAP32.dll
     7fefd540000 4549d38a Nov 02 11:16:26 2006 C:\Windows\system32\WS2_32.dll
     7feff0b0000 4549d370 Nov 02 11:16:00 2006 C:\Windows\system32\NSI.dll
     7fefd530000 4549d310 Nov 02 11:14:24 2006 C:\Windows\system32\PSAPI.DLL
```

```
     7fefce20000 4549d315 Nov 02 11:14:29 2006 C:\Windows\system32\SAMLIB.dll
     7fefd1b0000 4549d380 Nov 02 11:16:16 2006 C:\Windows\system32\WINSTA.dll
     7fefdb90000 4549d282 Nov 02 11:12:02 2006 C:\Windows\system32\CLBCatQ.DLL
     7fefc620000 4549d31d Nov 02 11:14:37 2006 C:\Windows\system32\rsaenh.dll
     7fefd1f0000 4549d32f Nov 02 11:14:55 2006 C:\Windows\system32\SXS.DLL
     7fef7ac0000 4549d295 Nov 02 11:12:21 2006 C:\Windows\system32\milcore.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       00000000002d0000
    ProcessParameters: 00000000002d1d50
    WindowTitle:  'C:\Windows\system32\Dwm.exe'
    ImageFile:    'C:\Windows\system32\Dwm.exe'
    CommandLine:  '"C:\Windows\system32\Dwm.exe"'
    DllPath:
'C:\Windows\system32;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Wind
ows;C:\Windows\System32\Wbem'
    Environment:  00000000002d1310
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\UserName\AppData\Roaming
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        HOMEDRIVE=C:
        HOMEPATH=\Users\UserName
        LOCALAPPDATA=C:\Users\UserName\AppData\Local
        LOGONSERVER=\\COMPUTERNAME
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Users\UserName\AppData\Local\Temp
        TMP=C:\Users\UserName\AppData\Local\Temp
        USERDOMAIN=COMPUTERNAME
        USERNAME=UserName
        USERPROFILE=C:\Users\UserName
        windir=C:\Windows


        THREAD fffffa8004b5e8f0  Cid 0a44.0a48  Teb: 000007fffffde000 Win32Thread: fffff900c20f29f0
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004b91110  SynchronizationEvent
            fffffa8004b910b0  SynchronizationEvent
            fffffa8004bb3580  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004b8a9c0       Image:         dwm.exe
        Wait Start TickCount      15650          Ticks: 30929 (0:00:08:02.495)
        Context Switch Count      506                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address Dwm!WinMainStartup (0x00000000ff35b01c)
        Stack Init fffff9801069edb0 Current fffff9801069e260
        Base fffff9801069f000 Limit fffff98010696000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1069e2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1069e3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`1069e440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
```

```
        fffff980`1069e4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`1069e960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`1069ebb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1069ec20)
        00000000`0012f9c8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0012f9d0 00000000`76d1e96d kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0012fae0 00000000`76d1e85e USER32!RealMsgWaitForMultipleObjectsEx+0x129
        00000000`0012fb80 00000000`ff35433d USER32!MsgWaitForMultipleObjectsEx+0x46
        00000000`0012fbc0 00000000`ff355b20 Dwm!CDwmAppHost::WaitForAndProcessEvent+0x51
        00000000`0012fc00 00000000`ff355bbc Dwm!CDwmAppHost::Run+0x7c
        00000000`0012fc70 00000000`ff363223 Dwm!WinMain+0x54
        00000000`0012fcb0 00000000`ff35b036 Dwm!LocalAlloc+0x1eb
        00000000`0012fd70 00000000`76bfcdcd Dwm!WinMainStartup+0x1a
        00000000`0012fda0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0012fdd0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004ba92f0  Cid 0a44.0a60  Teb: 000007fffffdc000 Win32Thread: fffff900c2081a30
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80045a59d0  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004b8a9c0       Image:         dwm.exe
        Wait Start TickCount      16704          Ticks: 29875 (0:00:07:46.052)
        Context Switch Count      245                 LargeStack
        UserTime                  00:00:00.015
        KernelTime                00:00:00.015
        Win32 Start Address Dwm!CPortBase::PortThread (0x00000000ff35c688)
        Stack Init fffff980106c4db0 Current fffff980106c4260
        Base fffff980106c5000 Limit fffff980106bd000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`106c42a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`106c43e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`106c4440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`106c44b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`106c4960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`106c4bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`106c4c20)
        00000000`02abfb98 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`02abfba0 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`02abfcb0 000007fe`f868199e kernel32!WaitForMultipleObjects+0x11
        00000000`02abfcf0 00000000`ff3590b5
dwmredir!CMilWindowManager::WaitForMultipleObjects+0x116
        00000000`02abfd90 00000000`ff35c581 Dwm!CSessionPort::WaitForMultipleObjects+0x21
        00000000`02abfdd0 00000000`ff35c691 Dwm!CPortBase::PortThreadInternal+0x49
        00000000`02abfe30 00000000`76bfcdcd Dwm!CPortBase::PortThread+0x9
        00000000`02abfe60 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02abfe90 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004b929d0  Cid 0a44.0a64  Teb: 000007fffffd9000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa8004b94670  SynchronizationTimer
            fffffa8004484c10  ProcessObject
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004b8a9c0       Image:         dwm.exe
        Wait Start TickCount      2802           Ticks: 43777 (0:00:11:22.925)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x0000000076df6930)
        Stack Init fffff980107b9db0 Current fffff980107b9260
        Base fffff980107ba000 Limit fffff980107b4000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`107b92a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`107b93e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`107b9440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`107b94b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`107b9960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`107b9bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`107b9c20)
        00000000`02d7fb18 00000000`76df6b07 ntdll!NtWaitForMultipleObjects+0xa
        00000000`02d7fb20 00000000`76bfcdcd ntdll!TppWaiterpThread+0x14d
        00000000`02d7fdc0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02d7fdf0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80044f1a80  Cid 0a44.0a6c  Teb: 000007fffffd7000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8004b94a80  QueueObject
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004b8a9c0       Image:         dwm.exe
        Wait Start TickCount      4802           Ticks: 41777 (0:00:10:51.725)
        Context Switch Count      7
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff98010773db0 Current fffff98010773810
        Base fffff98010774000 Limit fffff9801076e000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`10773850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`10773990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`107739f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`10773a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`10773b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`10773bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`10773c20)
        00000000`02edfa48 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`02edfa50 000007fe`fedce7a3 kernel32!GetQueuedCompletionStatus+0x48
        00000000`02edfab0 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`02edfb40 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`02edfbf0 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`02edfc20 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`02edfc60 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`02edfc90 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02edfcc0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

Explorer process

```
PROCESS fffffa8004ba4c10
    SessionId: 1  Cid: 0a84    Peb: 7fffffd9000  ParentCid: 0a30
    DirBase: 361bd000  ObjectTable: fffff88001f224b0  HandleCount: 744.
    Image: explorer.exe
    VadRoot fffffa8004bafcd0 Vads 418 Clone 0 Private 6347. Modified 38865. Locked 0.
    DeviceMap fffff88006100250
    Token                             fffff88001fc2ab0
    ElapsedTime                       00:11:23.554
    UserTime                          00:00:02.745
    KernelTime                        00:00:06.037
    QuotaPoolUsage[PagedPool]         447000
    QuotaPoolUsage[NonPagedPool]      60960
    Working Set Sizes (now,min,max)  (11821, 6321, 6837) (47284KB, 25284KB, 27348KB)
    PeakWorkingSetSize                14210
    VirtualSize                       257 Mb
    PeakVirtualSize                   300 Mb
    PageFaultCount                    69184
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      10283

    Setting context for this process...
.process /p /r fffffa8004ba4c10

    !peb
PEB at 000007fffffd9000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00000000ff570000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 0000000000292790 . 0000000005f48830
    Ldr.InLoadOrderModuleList:           00000000002926a0 . 0000000005f488e0
    Ldr.InMemoryOrderModuleList:         00000000002926b0 . 0000000005f488f0
            Base TimeStamp                     Module
        ff570000 4549bacb Nov 02 09:30:51 2006 C:\Windows\Explorer.EXE
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        76bc0000 4549d328 Nov 02 11:14:48 2006 C:\Windows\system32\kernel32.dll
     7fefea30000 4549d267 Nov 02 11:11:35 2006 C:\Windows\system32\ADVAPI32.dll
     7fefed90000 469c43bb Jul 17 05:21:15 2007 C:\Windows\system32\RPCRT4.dll
     7fefec20000 4549d273 Nov 02 11:11:47 2006 C:\Windows\system32\GDI32.dll
        76d00000 45d3ee19 Feb 15 05:22:33 2007 C:\Windows\system32\USER32.dll
     7fefdd40000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\system32\msvcrt.dll
     7fefda10000 4549d31f Nov 02 11:14:39 2006 C:\Windows\system32\SHLWAPI.dll
     7fefddf0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\SHELL32.dll
     7fefd760000 4549d317 Nov 02 11:14:31 2006 C:\Windows\system32\ole32.dll
     7fefdab0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\OLEAUT32.dll
     7fef83b0000 4549d319 Nov 02 11:14:33 2006 C:\Windows\system32\SHDOCVW.dll
     7fefc330000 4549d33b Nov 02 11:15:07 2006 C:\Windows\system32\UxTheme.dll
     7fefc580000 4549d351 Nov 02 11:15:29 2006 C:\Windows\system32\POWRPROF.dll
     7fef8c50000 4549d2b7 Nov 02 11:12:55 2006 C:\Windows\system32\dwmapi.dll
     7fefb610000 4549d245 Nov 02 11:11:01 2006
C:\Windows\WinSxS\amd64_microsoft.windows.gdiplus_6595b64144ccf1df_1.0.6000.16386_none_56f375c7b4f2
4821\gdiplus.dll
     7fefcc20000 4549d32d Nov 02 11:14:53 2006 C:\Windows\system32\slc.dll
     7fefb4d0000 4549d30d Nov 02 11:14:21 2006 C:\Windows\system32\PROPSYS.dll
     7fef81e0000 4549d27b Nov 02 11:11:55 2006 C:\Windows\system32\BROWSEUI.dll
     7fefd9e0000 4549d2cb Nov 02 11:13:15 2006 C:\Windows\system32\IMM32.dll
     7fefdc30000 4549d2e6 Nov 02 11:13:42 2006 C:\Windows\system32\MSCTF.dll
     7fefb960000 4549d2b6 Nov 02 11:12:54 2006 C:\Windows\system32\DUser.dll
     7feff0c0000 4549d2a1 Nov 02 11:12:33 2006 C:\Windows\system32\LPK.DLL
     7fefd940000 4549d337 Nov 02 11:15:03 2006 C:\Windows\system32\USP10.dll
     7fefbe70000 4549d32b Nov 02 11:14:51 2006 C:\Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_1559f1c6f365a7fa\comctl32.dll
```

```
7fefb140000 4549d365 Nov 02 11:15:49 2006 C:\Windows\system32\WindowsCodecs.dll
7fefd310000 4549d247 Nov 02 11:11:03 2006 C:\Windows\system32\apphelp.dll
7fefdb90000 4549d282 Nov 02 11:12:02 2006 C:\Windows\system32\CLBCatQ.DLL
7fef7f60000 4549d351 Nov 02 11:15:29 2006 C:\Windows\System32\cscui.dll
7fef80b0000 4549d34d Nov 02 11:15:25 2006 C:\Windows\System32\CSCDLL.dll
7fef80a0000 4549d34c Nov 02 11:15:24 2006 C:\Windows\System32\CSCAPI.dll
7fef8070000 4549d28d Nov 02 11:12:13 2006 C:\Windows\system32\IconCodecService.dll
7fefd390000 4549d33f Nov 02 11:15:11 2006 C:\Windows\system32\Secur32.dll
7fefc620000 4549d31d Nov 02 11:14:37 2006 C:\Windows\system32\rsaenh.dll
7fef79e0000 4549d347 Nov 02 11:15:19 2006 C:\Windows\system32\timedate.cpl
7fefc180000 4549d253 Nov 02 11:11:15 2006 C:\Windows\system32\ATL.DLL
7fefcf70000 4549d2fc Nov 02 11:14:04 2006 C:\Windows\system32\NETAPI32.dll
7fefd530000 4549d310 Nov 02 11:14:24 2006 C:\Windows\system32\PSAPI.DLL
7fefb310000 4549d318 Nov 02 11:14:32 2006 C:\Windows\system32\OLEACC.dll
7fef7720000 4549d256 Nov 02 11:11:18 2006 C:\Windows\system32\actxprxy.dll
7fefd3b0000 4549d336 Nov 02 11:15:02 2006 C:\Windows\system32\USERENV.dll
7fef84e0000 4549d2dd Nov 02 11:13:33 2006 C:\Windows\system32\msutb.dll
7fefc6d0000 4549d35d Nov 02 11:15:41 2006 C:\Windows\system32\WINBRAND.dll
7fef9620000 4549d319 Nov 02 11:14:33 2006 C:\Windows\System32\shacct.dll
7fefce20000 4549d315 Nov 02 11:14:29 2006 C:\Windows\System32\SAMLIB.dll
7fef7940000 4549d2c5 Nov 02 11:13:09 2006 C:\Windows\System32\msshsq.dll
7fef6b90000 4549d2ea Nov 02 11:13:46 2006 C:\Windows\System32\NaturalLanguage6.dll
7fefcc50000 4549d344 Nov 02 11:15:16 2006 C:\Windows\System32\CRYPT32.dll
7fefce00000 4549d2df Nov 02 11:13:35 2006 C:\Windows\System32\MSASN1.dll
7fef5f50000 4549d31f Nov 02 11:14:39 2006 C:\Windows\System32\NLSData0009.dll
   73670000 4549b2e3 Nov 02 08:57:07 2006 C:\Windows\System32\NLSLexicons0009.dll
7fefbc40000 4549d264 Nov 02 11:11:32 2006 C:\Windows\system32\authui.dll
7fefc570000 4549d324 Nov 02 11:14:44 2006 C:\Windows\system32\MSIMG32.dll
7fefd5f0000 470c5dac Oct 10 06:05:48 2007 C:\Windows\system32\urlmon.dll
7fefebc0000 4549d29c Nov 02 11:12:28 2006 C:\Windows\system32\iertutil.dll
7fefc5b0000 4549d384 Nov 02 11:16:20 2006 C:\Windows\system32\NTMARTA.DLL
7fefd590000 4549d396 Nov 02 11:16:38 2006 C:\Windows\system32\WLDAP32.dll
7fefd540000 4549d38a Nov 02 11:16:26 2006 C:\Windows\system32\WS2_32.dll
7feff0b0000 4549d370 Nov 02 11:16:00 2006 C:\Windows\system32\NSI.dll
7fef5880000 470c5d32 Oct 10 06:03:46 2007 C:\Windows\system32\ieframe.dll
7fef7f20000 4549d291 Nov 02 11:12:17 2006 C:\Windows\system32\LINKINFO.dll
7fefec90000 470c5de6 Oct 10 06:06:46 2007 C:\Windows\system32\WININET.dll
   76f70000 4549b4d2 Nov 02 09:05:22 2006 C:\Windows\system32\Normaliz.dll
7fef9e10000 4549d323 Nov 02 11:14:43 2006 C:\Windows\system32\msiltcfg.dll
7fefca50000 4549d336 Nov 02 11:15:02 2006 C:\Windows\system32\VERSION.dll
7fef8830000 4549d31b Nov 02 11:14:35 2006 C:\Windows\system32\msi.dll
7fef9770000 4549d31c Nov 02 11:14:36 2006 C:\Windows\system32\SFC.DLL
7fef97e0000 4549d31d Nov 02 11:14:37 2006 C:\Windows\system32\sfc_os.dll
7fefeed0000 4549d318 Nov 02 11:14:32 2006 C:\Windows\system32\SETUPAPI.dll
7fef7f10000 4549d2ee Nov 02 11:13:50 2006 C:\Windows\system32\ExplorerFrame.dll
7fefb360000 4549d36f Nov 02 11:15:59 2006 C:\Windows\system32\WINMM.dll
7fefb280000 4549d336 Nov 02 11:15:02 2006 C:\Windows\system32\wdmaud.drv
   75160000 4549d331 Nov 02 11:14:57 2006 C:\Windows\system32\ksuser.dll
7fefc2d0000 4549d273 Nov 02 11:11:47 2006 C:\Windows\system32\AVRT.dll
7fefc2e0000 4549d2a1 Nov 02 11:12:33 2006 C:\Windows\system32\MMDevAPI.DLL
7fefc1e0000 4549d381 Nov 02 11:16:17 2006 C:\Windows\system32\WINTRUST.dll
7fefda90000 462443ee Apr 17 04:50:06 2007 C:\Windows\system32\imagehlp.dll
7fefb0c0000 4549d258 Nov 02 11:11:20 2006 C:\Windows\System32\audioses.dll
7fefb040000 4549d256 Nov 02 11:11:18 2006 C:\Windows\System32\audioeng.dll
7fefb270000 4549d2cd Nov 02 11:13:17 2006 C:\Windows\system32\msacm32.drv
7fefb120000 4549d2cc Nov 02 11:13:16 2006 C:\Windows\system32\MSACM32.dll
7fefb240000 4549d2bf Nov 02 11:13:03 2006 C:\Windows\system32\midimap.dll
7fef6900000 4549d327 Nov 02 11:14:47 2006 C:\Windows\system32\stobject.dll
7fef69c0000 4549d24e Nov 02 11:11:10 2006 C:\Windows\system32\BatMeter.dll
7fefc450000 4549d34e Nov 02 11:15:26 2006 C:\Windows\system32\WTSAPI32.dll
7fefd1b0000 4549d380 Nov 02 11:16:16 2006 C:\Windows\system32\WINSTA.dll
7fefba70000 4549d2e7 Nov 02 11:13:43 2006 C:\Windows\system32\es.dll
7fefb480000 4549d332 Nov 02 11:14:58 2006 C:\Windows\System32\SndVolSSO.dll
7fef5540000 4549d30f Nov 02 11:14:23 2006 C:\Windows\System32\netshell.dll
7fefcb80000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\System32\IPHLPAPI.DLL
7fefcb30000 4549d263 Nov 02 11:11:31 2006 C:\Windows\System32\dhcpcsvc.DLL
7fefce40000 4549d288 Nov 02 11:12:08 2006 C:\Windows\System32\DNSAPI.dll
7fefd280000 4549d370 Nov 02 11:16:00 2006 C:\Windows\System32\WINNSI.DLL
7fefcb00000 4549d264 Nov 02 11:11:32 2006 C:\Windows\System32\dhcpcsvc6.DLL
7fefc1a0000 4549d314 Nov 02 11:14:28 2006 C:\Windows\System32\nlaapi.dll
```

```
     7fef6700000 4549d33b Nov 02 11:15:07 2006 C:\Windows\system32\pnidui.dll
     7fef79c0000 4549d31b Nov 02 11:14:35 2006 C:\Windows\system32\QUtil.dll
     7fefcbb0000 4549d349 Nov 02 11:15:21 2006 C:\Windows\system32\wevtapi.dll
     7fefba60000 4549d393 Nov 02 11:16:35 2006 C:\Windows\system32\wlanutil.dll
     7fefd1f0000 4549d32f Nov 02 11:14:55 2006 C:\Windows\system32\SXS.DLL
     7fef52e0000 4549d323 Nov 02 11:14:43 2006 C:\Windows\system32\oobefldr.dll
     7fef9c40000 46662887 Jun 06 04:22:47 2007 C:\Windows\System32\msxml3.dll
     7fefb440000 4549d297 Nov 02 11:12:23 2006 C:\Windows\system32\MLANG.dll
     7fef6f70000 4549d375 Nov 02 11:16:05 2006 C:\Windows\system32\WinSATAPI.dll
     7fef6ee0000 4549d2e5 Nov 02 11:13:41 2006 C:\Windows\system32\mscms.dll
     7fef8520000 4549d37c Nov 02 11:16:12 2006 C:\Windows\system32\WINSPOOL.DRV
     7fefc1c0000 4549d251 Nov 02 11:11:13 2006 C:\Windows\system32\Cabinet.dll
     7fefcab0000 4549d2f2 Nov 02 11:13:54 2006 C:\Windows\system32\ncrypt.dll
     7fefca60000 4549d252 Nov 02 11:11:14 2006 C:\Windows\system32\BCRYPT.dll
     7fefc940000 4549d277 Nov 02 11:11:51 2006 C:\Windows\system32\GPAPI.dll
     7fef8fd0000 4549d348 Nov 02 11:15:20 2006 C:\Windows\system32\cryptnet.dll
     7fef9760000 4549d343 Nov 02 11:15:15 2006 C:\Windows\system32\SensApi.dll
     7fefcd90000 4549d2b2 Nov 02 11:12:50 2006 C:\Windows\system32\MPR.dll
     7fef4db0000 4549d282 Nov 02 11:12:02 2006 C:\Windows\system32\bthprops.cpl
     7fef4ed0000 4549d28f Nov 02 11:12:15 2006 C:\Windows\system32\fxsst.dll
     7fef4590000 4549d283 Nov 02 11:12:03 2006 C:\Windows\system32\FXSAPI.dll
        73e70000 4549aea9 Nov 02 08:39:05 2006 C:\Windows\system32\FXSRESM.DLL
     7fefa1f0000 4549d36c Nov 02 11:15:56 2006 C:\Windows\System32\npmproxy.dll
     7fefba40000 4549d384 Nov 02 11:16:20 2006 C:\Windows\system32\Wlanapi.dll
     7fef7900000 4549d322 Nov 02 11:14:42 2006 C:\Windows\system32\OneX.DLL
     7fef78e0000 4549d26a Nov 02 11:11:38 2006 C:\Windows\system32\eappprxy.dll
     7fef7540000 4549d267 Nov 02 11:11:35 2006 C:\Windows\system32\eappcfg.dll
     7fef3e20000 4549d275 Nov 02 11:11:49 2006 C:\Windows\System32\AltTab.dll
     7fef3ae0000 4549d359 Nov 02 11:15:37 2006 C:\Windows\System32\srchadmin.dll
     7fef7170000 4549d34f Nov 02 11:15:27 2006 C:\Windows\System32\cscobj.dll
     7fef3a90000 4549d33f Nov 02 11:15:11 2006 C:\Windows\system32\webcheck.dll
     7fef3590000 4549d332 Nov 02 11:14:58 2006 C:\Windows\System32\SyncCenter.dll
     7fefb3a0000 4549d2cc Nov 02 11:13:16 2006 C:\Windows\system32\mssprxy.dll
     7fef3de0000 4549d38e Nov 02 11:16:30 2006 C:\Windows\system32\wscntfy.dll
     7fef4d70000 4549d38c Nov 02 11:16:28 2006 C:\Windows\system32\WSCAPI.dll
     7fef39b0000 4549d2c6 Nov 02 11:13:10 2006 C:\Windows\system32\imapi2.dll
     7fef7600000 4549d30d Nov 02 11:14:21 2006 C:\Windows\System32\QAgent.dll
     7fefac60000 4549d280 Nov 02 11:12:00 2006 C:\Windows\System32\fwpuclnt.dll
     7fef5100000 4549d34d Nov 02 11:15:25 2006 C:\Program Files\Common Files\microsoft
shared\ink\tiptsf.dll
     7fefb930000 4549d350 Nov 02 11:15:28 2006 C:\Windows\system32\xmllite.dll
     7fef79a0000 4549d346 Nov 02 11:15:18 2006 C:\Windows\system32\thumbcache.dll
     7fef65e0000 4549d38b Nov 02 11:16:27 2006 C:\Windows\system32\ntshrui.dll
     7fef7990000 4549d265 Nov 02 11:11:33 2006 C:\Windows\system32\dciman32.dll
     7fef81b0000 4549d36f Nov 02 11:15:59 2006 C:\Windows\system32\twext.dll
     7fef80d0000 4549d334 Nov 02 11:15:00 2006 C:\Windows\system32\syncui.dll
     7fef8170000 4549d333 Nov 02 11:14:59 2006 C:\Windows\system32\SYNCENG.dll
     7fef3240000 4549d33d Nov 02 11:15:09 2006 C:\Windows\System32\systemcpl.dll
     7fefaaa0000 4549d31e Nov 02 11:14:38 2006 C:\Windows\System32\SLWGA.dll
     7fef9e20000 4549d342 Nov 02 11:15:14 2006 C:\Windows\system32\wbem\wbemprox.dll
     7fef9f50000 4549d33d Nov 02 11:15:09 2006 C:\Windows\system32\wbem\wbemcomn.dll
     7fef96d0000 4549d343 Nov 02 11:15:15 2006 C:\Windows\system32\wbem\wbemsvc.dll
     7fef9040000 4549d274 Nov 02 11:11:48 2006 C:\Windows\system32\wbem\fastprox.dll
     7fefcdd0000 4549d375 Nov 02 11:16:05 2006 C:\Windows\system32\NTDSAPI.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       0000000000290000
    ProcessParameters: 0000000000291d80
    WindowTitle:  'C:\Windows\Explorer.EXE'
    ImageFile:    'C:\Windows\Explorer.EXE'
    CommandLine:  'C:\Windows\Explorer.EXE'
    DllPath:
'C:\Windows;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Windows;C:\Wi
ndows\System32\Wbem'
    Environment:  0000000000389820
        =::=::\
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\UserName\AppData\Roaming
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
```

```
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        HOMEDRIVE=C:
        HOMEPATH=\Users\UserName
        LOCALAPPDATA=C:\Users\UserName\AppData\Local
        LOGONSERVER=\\COMPUTERNAME
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public
        SESSIONNAME=Console
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Users\UserName\AppData\Local\Temp
        TMP=C:\Users\UserName\AppData\Local\Temp
        USERDOMAIN=COMPUTERNAME
        USERNAME=UserName
        USERPROFILE=C:\Users\UserName
        windir=C:\Windows


        THREAD fffffa8004ba4780  Cid 0a84.0a88  Teb: 000007fffffde000 Win32Thread: fffff900c077b2e0
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa8004b5d510  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004ba4c10       Image:         explorer.exe
        Wait Start TickCount      45988          Ticks: 591 (0:00:00:09.219)
        Context Switch Count      13540                 LargeStack
        UserTime                  00:00:00.421
        KernelTime                00:00:00.436
        Win32 Start Address Explorer!wWinMainCRTStartup (0x00000000ff5983f0)
        Stack Init fffff980106b1db0 Current fffff980106b18c0
        Base fffff980106b2000 Limit fffff980106a7000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`106b1900 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`106b1a40 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`106b1aa0 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`106b1b20 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`106b1bc0 fffff960`000dc057 win32k!xxxSleepThread+0x56
        fffff980`106b1bf0 fffff800`01c4d733 win32k!NtUserWaitMessage+0x37
        fffff980`106b1c20 00000000`76d1df2a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`106b1c20)
        00000000`0020f6a8 000007fe`fde72e23 USER32!ZwUserWaitMessage+0xa
        00000000`0020f6b0 00000000`ff592ee2 SHELL32!SHDesktopMessageLoop+0x9f
        00000000`0020f6e0 00000000`ff598575 Explorer!wWinMain+0x9a3
        00000000`0020fd80 00000000`76bfcdcd Explorer!TraceMessage+0x204
        00000000`0020fe40 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0020fe70 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004b46060  Cid 0a84.0b00  Teb: 000007fffffd7000 Win32Thread: fffff900c1ed9a00
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa8004bfab30  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004ba4c10       Image:         explorer.exe
        Wait Start TickCount      46293          Ticks: 286 (0:00:00:04.461)
        Context Switch Count      24945                 LargeStack
        UserTime                  00:00:00.436
        KernelTime                00:00:00.951
        Win32 Start Address SHLWAPI!WrapperThreadProc (0x000007fefda24f20)
        Stack Init fffff98012a85db0 Current fffff98012a858c0
        Base fffff98012a86000 Limit fffff98012a7a000 Call 0
        Priority 13 BasePriority 9 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`12a85900 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12a85a40 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`12a85aa0 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`12a85b20 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`12a85bc0 fffff960`000dc057 win32k!xxxSleepThread+0x56
        fffff980`12a85bf0 fffff800`01c4d733 win32k!NtUserWaitMessage+0x37
        fffff980`12a85c20 00000000`76d1df2a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12a85c20)
        00000000`032ffbc8 00000000`ff5728f0 USER32!ZwUserWaitMessage+0xa
        00000000`032ffbd0 00000000`ff5949dc Explorer!CTray::_MessageLoop+0x3fb
        00000000`032ffc70 00000000`00000000 Explorer!CTray::MainThreadProc+0x62
```

```
        THREAD fffffa8004c075d0  Cid 0a84.0b3c  Teb: 000007fffffd5000 Win32Thread: fffff900c0763460
WAIT: (UserRequest) UserMode Alertable
            fffffa80025a1a50  NotificationEvent
            fffffa800481d1a0  NotificationEvent
            fffffa80029ff6a0  NotificationEvent
            fffffa8002a6f330  NotificationEvent
            fffffa80025783e0  NotificationEvent
            fffffa8001e7c680  NotificationEvent
            fffffa800496b960  NotificationEvent
            fffffa800474f040  NotificationEvent
            fffffa8004bfa830  NotificationEvent
            fffffa8004c2e0d0  NotificationEvent
            fffffa8004b8c1d0  NotificationEvent
            fffffa800475e950  NotificationEvent
            fffffa8004b6ced0  NotificationEvent
            fffffa800451e9a0  NotificationEvent
            fffffa800451e940  NotificationEvent
            fffffa800469aa10  NotificationEvent
            fffffa8004c2e780  NotificationEvent
            fffffa8004c023d0  NotificationEvent
            fffffa8004c10760  NotificationEvent
            fffffa8004c1ba60  NotificationEvent
            fffffa8004c07470  SynchronizationEvent
        IRP List:
            fffffa8002a62010: (0006,0358) Flags: 00060000  Mdl: 00000000
            fffffa8002a6c1c0: (0006,0358) Flags: 00060000  Mdl: 00000000
            fffffa800259d820: (0006,0358) Flags: 00060000  Mdl: 00000000
            fffffa8002ad6ca0: (0006,0358) Flags: 00060000  Mdl: 00000000
            fffffa8002904ca0: (0006,0358) Flags: 00060000  Mdl: 00000000
            fffffa80029034c0: (0006,0358) Flags: 00060000  Mdl: 00000000
            fffffa800220d370: (0006,0358) Flags: 00060000  Mdl: 00000000
            fffffa8004bdec60: (0006,03a0) Flags: 00060000  Mdl: 00000000
            fffffa80020beca0: (0006,0358) Flags: 00060000  Mdl: 00000000
            fffffa80039a7ca0: (0006,0358) Flags: 00060000  Mdl: 00000000
            fffffa80039ab4e0: (0006,0358) Flags: 00060000  Mdl: 00000000
            fffffa8004c635c0: (0006,0358) Flags: 00060000  Mdl: 00000000
            fffffa8004c63010: (0006,0358) Flags: 00060000  Mdl: 00000000
            fffffa8004c3e2c0: (0006,0358) Flags: 00060000  Mdl: 00000000
            fffffa8004ba8010: (0006,0358) Flags: 00060000  Mdl: 00000000
            fffffa8004c41930: (0006,0358) Flags: 00060000  Mdl: 00000000
            fffffa8004c41ca0: (0006,0358) Flags: 00060000  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004ba4c10       Image:         explorer.exe
        Wait Start TickCount      19796          Ticks: 26783 (0:00:06:57.817)
        Context Switch Count      2553                 LargeStack
        UserTime                  00:00:00.171
        KernelTime                00:00:00.124
        Win32 Start Address SHLWAPI!WrapperThreadProc (0x000007fefda24f20)
        Stack Init fffff98012b1ddb0 Current fffff98012b1d260
        Base fffff98012b1e000 Limit fffff98012b15000 Call 0
        Priority 12 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`12b1d2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12b1d3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`12b1d440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`12b1d4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`12b1d960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`12b1dbb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12b1dc20)
        00000000`0327f668 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0327f670 00000000`76d1e96d kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0327f780 00000000`76d1e85e USER32!RealMsgWaitForMultipleObjectsEx+0x129
        00000000`0327f820 000007fe`fde67a9a USER32!MsgWaitForMultipleObjectsEx+0x46
        00000000`0327f860 000007fe`fda24d48 SHELL32!CChangeNotify::ThreadProc+0xba
        00000000`0327fae0 00000000`76bfcdcd SHLWAPI!WrapperThreadProc+0xfc
        00000000`0327fbc0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0327fbf0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004c30bb0  Cid 0a84.0b5c  Teb: 000007fffffd3000 Win32Thread: fffff900c1ebbd60
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004bfa7d0  NotificationEvent
            fffffa8004bb29b0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004ba4c10       Image:         explorer.exe
        Wait Start TickCount      15650          Ticks: 30929 (0:00:08:02.495)
        Context Switch Count      68                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address gdiplus!BackgroundThreadProc (0x000007fefb672410)
        Stack Init fffff98012b56db0 Current fffff98012b56260
        Base fffff98012b57000 Limit fffff98012b4f000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`12b562a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12b563e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`12b56440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`12b564b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`12b56960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`12b56bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12b56c20)
        00000000`03f9fa08 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`03f9fa10 00000000`76d1e96d kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`03f9fb20 00000000`76d1e85e USER32!RealMsgWaitForMultipleObjectsEx+0x129
        00000000`03f9fbc0 00000000`76d13680 USER32!MsgWaitForMultipleObjectsEx+0x46
        00000000`03f9fc00 000007fe`fb672478 USER32!MsgWaitForMultipleObjects+0x20
        00000000`03f9fc40 00000000`76bfcdcd gdiplus!BackgroundThreadProc+0x68
        00000000`03f9fcb0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`03f9fce0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004c95bb0  Cid 0a84.0bd4  Teb: 000007fffffa0000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004c3c210  NotificationEvent
            fffffa80048c5880  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004ba4c10       Image:         explorer.exe
        Wait Start TickCount      3137           Ticks: 43442 (0:00:11:17.699)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address msiltcfg!WorkerThread (0x000007fef9e12148)
        Stack Init fffff98012fa4db0 Current fffff98012fa4260
        Base fffff98012fa5000 Limit fffff98012f9f000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`12fa42a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12fa43e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`12fa4440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`12fa44b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`12fa4960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`12fa4bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12fa4c20)
        00000000`0693f7b8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0693f7c0 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0693f8d0 000007fe`f9e121ce kernel32!WaitForMultipleObjects+0x11
        00000000`0693f910 00000000`76bfcdcd msiltcfg!WorkerThread+0x86
        00000000`0693f9a0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0693f9d0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004cbb3e0  Cid 0a84.0bd8  Teb: 000007fffff9e000 Win32Thread: fffff900c1e81260
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa8004c9dfe0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004ba4c10       Image:         explorer.exe
        Wait Start TickCount      15650          Ticks: 30929 (0:00:08:02.495)
        Context Switch Count      47                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address SHLWAPI!WrapperThreadProc (0x000007fefda24f20)
        Stack Init fffff98012ed1db0 Current fffff98012ed1740
        Base fffff98012ed2000 Limit fffff98012eca000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`12ed1780 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12ed18c0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`12ed1920 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`12ed19a0 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`12ed1a40 fffff960`000c7e1e win32k!xxxSleepThread+0x56
        fffff980`12ed1a70 fffff960`000c7f25 win32k!xxxRealInternalGetMessage+0x72e
        fffff980`12ed1b50 fffff960`000c97e4 win32k!xxxInternalGetMessage+0x35
        fffff980`12ed1b90 fffff800`01c4d733 win32k!NtUserGetMessage+0x64
        fffff980`12ed1c20 00000000`76d1e6aa nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12ed1c20)
        00000000`0456fa58 00000000`76d1e6ea USER32!ZwUserGetMessage+0xa
        00000000`0456fa60 00000000`ff5792a9 USER32!GetMessageW+0x34
        00000000`0456fa90 000007fe`fda24d48 Explorer!CSoundWnd::s_ThreadProc+0x3b
        00000000`0456faf0 00000000`76bfcdcd SHLWAPI!WrapperThreadProc+0xfc
        00000000`0456fbd0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0456fc00 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004ce9bb0  Cid 0a84.0be0  Teb: 000007fffff9a000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8004c9ae50  QueueObject
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004ba4c10       Image:         explorer.exe
        Wait Start TickCount      3157           Ticks: 43422 (0:00:11:17.387)
        Context Switch Count      99
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address wdmaud!mxdMessageThreadProc (0x000007fefb286f50)
        Stack Init fffff98010835db0 Current fffff98010835810
        Base fffff98010836000 Limit fffff98010830000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`10835850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`10835990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`108359f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`10835a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`10835b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`10835bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`10835c20)
        00000000`058bfb78 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`058bfb80 000007fe`fb286fc1 kernel32!GetQueuedCompletionStatus+0x48
        00000000`058bfbe0 00000000`76bfcdcd wdmaud!mxdMessageThreadProc+0x71
        00000000`058bfc20 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`058bfc50 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004ce9510  Cid 0a84.0be4  Teb: 000007fffff98000 Win32Thread: fffff900c1e99d60
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa80045a5c00  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004ba4c10       Image:         explorer.exe
        Wait Start TickCount      3154           Ticks: 43425 (0:00:11:17.434)
        Context Switch Count      4                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdmaud!CTaskThread::TaskThreadProc (0x000007fefb295e94)
        Stack Init fffff98012ee4db0 Current fffff98012ee4740
        Base fffff98012ee5000 Limit fffff98012ede000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`12ee4780 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12ee48c0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`12ee4920 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`12ee49a0 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`12ee4a40 fffff960`000c7e1e win32k!xxxSleepThread+0x56
        fffff980`12ee4a70 fffff960`000c7f25 win32k!xxxRealInternalGetMessage+0x72e
        fffff980`12ee4b50 fffff960`000c97e4 win32k!xxxInternalGetMessage+0x35
        fffff980`12ee4b90 fffff800`01c4d733 win32k!NtUserGetMessage+0x64
        fffff980`12ee4c20 00000000`76d1e6aa nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12ee4c20)
        00000000`0612f6d8 00000000`76d1e6ea USER32!ZwUserGetMessage+0xa
        00000000`0612f6e0 000007fe`fb295f46 USER32!GetMessageW+0x34
        00000000`0612f710 00000000`76bfcdcd wdmaud!CTaskThread::TaskThreadProc+0xb2
        00000000`0612f780 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0612f7b0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004cc36f0  Cid 0a84.0be8  Teb: 000007fffff96000 Win32Thread: fffff900c07a0d60
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004ca0fe0  SynchronizationEvent
            fffffa8004cbc710  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004ba4c10       Image:         explorer.exe
        Wait Start TickCount      15992          Ticks: 30587 (0:00:07:57.160)
        Context Switch Count      532                LargeStack
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address wdmaud!CWorker::_StaticThreadProc (0x000007fefb291a18)
        Stack Init fffff9800ef1bdb0 Current fffff9800ef1b260
        Base fffff9800ef1c000 Limit fffff9800ef15000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0ef1b2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0ef1b3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0ef1b440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0ef1b4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0ef1b960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0ef1bbb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0ef1bc20)
        00000000`05a3fda8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`05a3fdb0 000007fe`fb291aa8 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`05a3fec0 00000000`76bfcdcd wdmaud!CWorker::_StaticThreadProc+0x90
        00000000`05a3ff10 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`05a3ff40 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8003a47060  Cid 0a84.0a10  Teb: 000007fffff92000 Win32Thread: fffff900c1f50d60
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800496d090  SynchronizationEvent
            fffffa8004c43160  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004ba4c10       Image:         explorer.exe
        Wait Start TickCount      46535          Ticks: 44 (0:00:00:00.686)
        Context Switch Count      3037                 LargeStack
        UserTime                  00:00:00.062
        KernelTime                00:00:00.156
        Win32 Start Address stobject!CSysTray::SysTrayThreadProc (0x000007fef6907630)
        Stack Init fffff9800dbff6d0 Current fffff9800dbfeb80
        Base fffff9800dc00000 Limit fffff9800dbf5000 Call fffff9800dbff920
        Priority 11 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0dbfebc0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0dbfed00 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0dbfed60 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0dbfedd0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0dbff280 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0dbff4d0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0dbff540)
        00000000`0599f4c8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0599f4d0 00000000`76d1e96d kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0599f5e0 000007fe`fb961ab6 USER32!RealMsgWaitForMultipleObjectsEx+0x129
        00000000`0599f680 000007fe`fb961aef DUser!CoreSC::Wait+0x62
        00000000`0599f6d0 000007fe`fb961b8a DUser!CoreSC::xwProcessNL+0xd5
        00000000`0599f740 00000000`76d1c78d DUser!MphProcessMessage+0x6a
        00000000`0599f790 00000000`76e22016 USER32!_ClientGetMessageMPH+0x3d
        00000000`0599f820 00000000`76d1e6aa ntdll!KiUserCallbackDispatcherContinue (TrapFrame @
00000000`0599f6e8)
        00000000`0599f898 00000000`76d1e6ea USER32!ZwUserGetMessage+0xa
        00000000`0599f8a0 000007fe`f690225f USER32!GetMessageW+0x34
        00000000`0599f8d0 000007fe`f690764f stobject!SysTrayMain+0x3a0
        00000000`0599f9e0 00000000`76bfcdcd stobject!CSysTray::SysTrayThreadProc+0x1f
        00000000`0599fa10 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0599fa40 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800294a3a0  Cid 0a84.0a68  Teb: 000007fffff90000 Win32Thread: fffff900c1f3cab0
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8002949e00  SynchronizationEvent
            fffffa8004cf63d0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004ba4c10       Image:         explorer.exe
        Wait Start TickCount      15996          Ticks: 30583 (0:00:07:57.097)
        Context Switch Count      11                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address msvcrt!endthreadex (0x000007fefdd59620)
        Stack Init fffff9800dba0db0 Current fffff9800dba0260
        Base fffff9800dba1000 Limit fffff9800db9a000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0dba02a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0dba03e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0dba0440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0dba04b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0dba0960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0dba0bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0dba0c20)
        00000000`069efad8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`069efae0 00000000`76d1e96d kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`069efbf0 000007fe`fb961ab6 USER32!RealMsgWaitForMultipleObjectsEx+0x129
        00000000`069efc90 000007fe`fb961aef DUser!CoreSC::Wait+0x62
        00000000`069efce0 000007fe`fb96e4ad DUser!CoreSC::xwProcessNL+0xd5
        00000000`069efd50 000007fe`fb96e3cc DUser!GetMessageExA+0x7b
        00000000`069efda0 000007fe`fdd594e7 DUser!ResourceManager::SharedThreadProc+0xe8
        00000000`069efe30 000007fe`fdd5967d msvcrt!endthreadex+0x47
        00000000`069efe60 00000000`76bfcdcd msvcrt!endthreadex+0x100
        00000000`069efe90 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`069efec0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80039a7060  Cid 0a84.0a50  Teb: 000007fffff8e000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa800294e4a0  SynchronizationTimer
            fffffa800294d230  NotificationEvent
            fffffa8004d156a0  SynchronizationEvent
            fffffa80045d01b0  SynchronizationEvent
            fffffa8003fea1b0  SynchronizationEvent
            fffffa8003df98a0  SynchronizationEvent
            fffffa8003fea308  NotificationEvent
            fffffa8003d806b0  SynchronizationEvent
            fffffa8003fe0630  SynchronizationEvent
            fffffa8003dc91a0  SynchronizationEvent
            fffffa8003df5320  SynchronizationEvent
            fffffa8003fece50  SynchronizationEvent
            fffffa8003e07930  SynchronizationEvent
            fffffa80038ee610  SynchronizationEvent
            fffffa800405e140  SynchronizationEvent
            fffffa8003dc9360  SynchronizationEvent
            fffffa8003d59fe0  SynchronizationEvent
            fffffa8003e07c50  SynchronizationEvent
            fffffa800405e360  SynchronizationEvent
            fffffa8003fecbf0  SynchronizationEvent
            fffffa8004c2a880  SynchronizationEvent
            fffffa8004c2a8e0  SynchronizationEvent
            fffffa80038ee8a0  SynchronizationEvent
            fffffa80038ee410  SynchronizationEvent
            fffffa8004d0b3b0  SynchronizationEvent
            fffffa8003dca630  SynchronizationEvent
            fffffa80041ffbe0  SynchronizationEvent
            fffffa8002104bf0  SynchronizationEvent
            fffffa8002086780  SynchronizationEvent
            fffffa800206b480  SynchronizationEvent
            fffffa800206b420  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004ba4c10       Image:         explorer.exe
        Wait Start TickCount      16235          Ticks: 30344 (0:00:07:53.369)
        Context Switch Count      151
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x0000000076df6930)
        Stack Init fffff98012fd5db0 Current fffff98012fd5260
        Base fffff98012fd6000 Limit fffff98012fd0000 Call 0
        Priority 12 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`12fd52a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12fd53e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`12fd5440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`12fd54b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`12fd5960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`12fd5bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12fd5c20)
        00000000`06c3f598 00000000`76df6b07 ntdll!NtWaitForMultipleObjects+0xa
        00000000`06c3f5a0 00000000`76bfcdcd ntdll!TppWaiterpThread+0x14d
        00000000`06c3f840 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`06c3f870 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80039db060  Cid 0a84.0334  Teb: 000007fffff8c000 Win32Thread: fffff900c06d8430
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa8004c90540  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004ba4c10       Image:         explorer.exe
        Wait Start TickCount      15650          Ticks: 30929 (0:00:08:02.495)
        Context Switch Count      44                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address MMDevAPI!CDeviceEnumerator::PnpNotificationThreadWrapper
(0x000007fefc2eade0)
        Stack Init fffff9800dbecdb0 Current fffff9800dbec740
        Base fffff9800dbed000 Limit fffff9800dbe5000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0dbec780 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0dbec8c0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0dbec920 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`0dbec9a0 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`0dbeca40 fffff960`000c7e1e win32k!xxxSleepThread+0x56
        fffff980`0dbeca70 fffff960`000c7f25 win32k!xxxRealInternalGetMessage+0x72e
        fffff980`0dbecb50 fffff960`000c97e4 win32k!xxxInternalGetMessage+0x35
        fffff980`0dbecb90 fffff800`01c4d733 win32k!NtUserGetMessage+0x64
        fffff980`0dbecc20 00000000`76d1e6aa nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0dbecc20)
        00000000`06cefd88 00000000`76d1e6ea USER32!ZwUserGetMessage+0xa
        00000000`06cefd90 000007fe`fc2e19f2 USER32!GetMessageW+0x34
        00000000`06cefdc0 00000000`76bfcdcd MMDevAPI!CDeviceEnumerator::PnpNotificationThread+0x25d
        00000000`06cefee0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`06ceff10 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80039dbbb0  Cid 0a84.0ac0  Teb: 000007fffff8a000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa800294d110  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004ba4c10       Image:         explorer.exe
        Wait Start TickCount      3361           Ticks: 43218 (0:00:11:14.205)
        Context Switch Count      6
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address SndVolSSO!CServiceMonitor::Run (0x000007fefb485ce8)
        Stack Init fffff980159a4db0 Current fffff980159a4960
        Base fffff980159a5000 Limit fffff9801599f000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`159a49a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`159a4ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`159a4b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`159a4bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`159a4c20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`159a4c20)
        00000000`06a6fcb8 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`06a6fcc0 000007fe`fb485d43 kernel32!WaitForSingleObjectEx+0x9c
        00000000`06a6fd80 00000000`76bfcdcd SndVolSSO!CServiceMonitor::Run+0x5b
        00000000`06a6fe00 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`06a6fe30 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004be28e0  Cid 0a84.0abc  Teb: 000007fffff88000 Win32Thread: fffff900c1f6ad60
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa8004c7e430  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004ba4c10       Image:         explorer.exe
        Wait Start TickCount      15650          Ticks: 30929 (0:00:08:02.495)
        Context Switch Count      208                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address SndVolSSO!CAudioVolumeShellService::VolumeThreadProc
(0x000007fefb484460)
        Stack Init fffff9800db08db0 Current fffff9800db088c0
        Base fffff9800db09000 Limit fffff9800db01000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0db08900 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0db08a40 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0db08aa0 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`0db08b20 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`0db08bc0 fffff960`000dc057 win32k!xxxSleepThread+0x56
        fffff980`0db08bf0 fffff800`01c4d733 win32k!NtUserWaitMessage+0x37
        fffff980`0db08c20 00000000`76d1df2a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0db08c20)
        00000000`0609fcf8 000007fe`fb4844d5 USER32!ZwUserWaitMessage+0xa
        00000000`0609fd00 00000000`76bfcdcd
SndVolSSO!CAudioVolumeShellService::VolumeThreadProc+0x75
        00000000`0609fd70 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0609fda0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80044d28c0  Cid 0a84.04a0  Teb: 000007fffff7c000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Alertable
            fffffa8004ccf690  QueueObject
        IRP List:
            fffffa80043d7ca0: (0006,0358) Flags: 00060000  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004ba4c10       Image:         explorer.exe
        Wait Start TickCount      16102          Ticks: 30477 (0:00:07:55.444)
        Context Switch Count      94
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x0000000076e17860)
        Stack Init fffff980107b2db0 Current fffff980107b2860
        Base fffff980107b3000 Limit fffff980107ad000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`107b28a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`107b29e0 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`107b2a40 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`107b2ad0 fffff800`01c8a722 nt!IoRemoveIoCompletion+0x47
        fffff980`107b2b50 fffff800`01c4d733 nt!NtWaitForWorkViaWorkerFactory+0x1f1
        fffff980`107b2c20 00000000`76e21b4a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`107b2c20)
        00000000`087ef6f8 00000000`76e17a20 ntdll!NtWaitForWorkViaWorkerFactory+0xa
        00000000`087ef700 00000000`76bfcdcd ntdll!TppWorkerThread+0x23e
        00000000`087ef970 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`087ef9a0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8001fb8060  Cid 0a84.0494  Teb: 000007fffffae000 Win32Thread: fffff900c1f2f010
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa8001fb55b0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004ba4c10       Image:         explorer.exe
        Wait Start TickCount      45573          Ticks: 1006 (0:00:00:15.693)
        Context Switch Count      49                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address SHLWAPI!WrapperThreadProc (0x000007fefda24f20)
        Stack Init fffff98015930db0 Current fffff98015930740
        Base fffff98015931000 Limit fffff9801592b000 Call 0
        Priority 13 BasePriority 8 PriorityDecrement 3 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`15930780 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`159308c0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`15930920 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`159309a0 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`15930a40 fffff960`000c7e1e win32k!xxxSleepThread+0x56
        fffff980`15930a70 fffff960`000c7f25 win32k!xxxRealInternalGetMessage+0x72e
        fffff980`15930b50 fffff960`000c97e4 win32k!xxxInternalGetMessage+0x35
        fffff980`15930b90 fffff800`01c4d733 win32k!NtUserGetMessage+0x64
        fffff980`15930c20 00000000`76d1e6aa nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`15930c20)
        00000000`067afba8 00000000`76d1e6ea USER32!ZwUserGetMessage+0xa
        00000000`067afbb0 000007fe`f4db6d26 USER32!GetMessageW+0x34
        00000000`067afbe0 000007fe`fda24d48 bthprops!BluetoothAuthenticationAgent+0x1de
        00000000`067afd30 00000000`76bfcdcd SHLWAPI!WrapperThreadProc+0xfc
        00000000`067afe10 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`067afe40 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8001e6a350  Cid 0a84.0ad4  Teb: 000007fffffac000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8001fb74e0  SynchronizationEvent
            fffffa8001f0f1c0  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004ba4c10       Image:         explorer.exe
        Wait Start TickCount      7112           Ticks: 39467 (0:00:10:15.689)
        Context Switch Count      13
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address fxsst!WaitForRestartThread (0x000007fef4ed4af0)
        Stack Init fffff98012ff1db0 Current fffff98012ff1260
        Base fffff98012ff2000 Limit fffff98012fec000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`12ff12a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12ff13e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`12ff1440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`12ff14b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`12ff1960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`12ff1bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12ff1c20)
        00000000`076df6e8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`076df6f0 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`076df800 000007fe`f4ed4bdd kernel32!WaitForMultipleObjects+0x11
        00000000`076df840 00000000`76bfcdcd fxsst!WaitForRestartThread+0xed
        00000000`076df890 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`076df8c0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8001eb5bb0  Cid 0a84.0d44  Teb: 000007fffffa8000 Win32Thread: fffff900c1eb3ad0
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa8001eaa560  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004ba4c10       Image:         explorer.exe
        Wait Start TickCount      16706          Ticks: 29873 (0:00:07:46.021)
        Context Switch Count      131                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address SHLWAPI!WrapperThreadProc (0x000007fefda24f20)
        Stack Init fffff98010941db0 Current fffff98010941740
        Base fffff98010942000 Limit fffff98010938000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`10941780 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`109418c0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`10941920 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`109419a0 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`10941a40 fffff960`000c7e1e win32k!xxxSleepThread+0x56
        fffff980`10941a70 fffff960`000c7f25 win32k!xxxRealInternalGetMessage+0x72e
        fffff980`10941b50 fffff960`000c97e4 win32k!xxxInternalGetMessage+0x35
        fffff980`10941b90 fffff800`01c4d733 win32k!NtUserGetMessage+0x64
        fffff980`10941c20 00000000`76d1e6aa nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`10941c20)
        00000000`044cf878 00000000`76d1e6ea USER32!ZwUserGetMessage+0xa
        00000000`044cf880 000007fe`f3e22ef0 USER32!GetMessageW+0x34
        00000000`044cf8b0 000007fe`fda24d48 AltTab!CAltTabSSO::_ThreadProc+0x124
        00000000`044cf950 00000000`76bfcdcd SHLWAPI!WrapperThreadProc+0xfc
        00000000`044cfa30 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`044cfa60 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8002093060  Cid 0a84.0d48  Teb: 000007fffffa6000 Win32Thread: fffff900c1f66d60
WAIT: (UserRequest) UserMode Alertable
            fffffa8002095f10  NotificationEvent
            fffffa8002079720  NotificationEvent
            fffffa80020a3c20  SynchronizationTimer
            fffffa8004c6a730  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004ba4c10       Image:         explorer.exe
        Wait Start TickCount      30809          Ticks: 15770 (0:00:04:06.013)
        Context Switch Count      68                  LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address SHLWAPI!WrapperThreadProc (0x000007fefda24f20)
        Stack Init fffff980109c6db0 Current fffff980109c6260
        Base fffff980109c7000 Limit fffff980109bf000 Call 0
        Priority 12 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`109c62a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`109c63e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`109c6440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`109c64b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`109c6960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`109c6bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`109c6c20)
        00000000`0784f9d8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0784f9e0 00000000`76d1e96d kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0784faf0 00000000`76d1e85e USER32!RealMsgWaitForMultipleObjectsEx+0x129
        00000000`0784fb90 000007fe`f7f62bc5 USER32!MsgWaitForMultipleObjectsEx+0x46
        00000000`0784fbd0 000007fe`fda24d48 cscui!CCSCShellServiceObject::_SvcObjThreadProc+0x10d
        00000000`0784fc80 00000000`76bfcdcd SHLWAPI!WrapperThreadProc+0xfc
        00000000`0784fd60 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0784fd90 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800201d700  Cid 0a84.0d50  Teb: 000007fffffa4000 Win32Thread: fffff900c009b010
WAIT: (UserRequest) UserMode Alertable
            fffffa800203f500  SynchronizationEvent
            fffffa800204f4c0  SynchronizationEvent
            fffffa800201fba0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004ba4c10       Image:         explorer.exe
        Wait Start TickCount      30809          Ticks: 15770 (0:00:04:06.013)
        Context Switch Count      227                 LargeStack
        UserTime                  00:00:00.046
        KernelTime                00:00:00.015
        Win32 Start Address SHLWAPI!WrapperThreadProc (0x000007fefda24f20)
        Stack Init fffff98012f43db0 Current fffff98012f43260
        Base fffff98012f44000 Limit fffff98012f3e000 Call 0
        Priority 12 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`12f432a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12f433e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`12f43440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`12f434b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`12f43960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`12f43bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12f43c20)
        00000000`07a6f898 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`07a6f8a0 00000000`76d1e96d kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`07a6f9b0 00000000`76d1e85e USER32!RealMsgWaitForMultipleObjectsEx+0x129
        00000000`07a6fa50 000007fe`f3aeb259 USER32!MsgWaitForMultipleObjectsEx+0x46
        00000000`07a6fa90 000007fe`f3aeb08e srchadmin!CSrchAdminSSO::_SvcObjThreadProc+0x1ad
        00000000`07a6fb90 000007fe`fda24d48 srchadmin!CSrchAdminSSO::s_SvcObjThreadProc+0x12
        00000000`07a6fbc0 00000000`76bfcdcd SHLWAPI!WrapperThreadProc+0xfc
        00000000`07a6fca0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`07a6fcd0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80020403e0  Cid 0a84.0d74  Teb: 000007fffff94000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800205b530  SynchronizationEvent
            fffffa8002040498  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004ba4c10       Image:         explorer.exe
        Wait Start TickCount      46142          Ticks: 437 (0:00:00:06.817)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ole32!CRpcThreadCache::RpcWorkerThreadEntry (0x000007fefd7a3be0)
        Stack Init fffff9801dac4db0 Current fffff9801dac4960
        Base fffff9801dac5000 Limit fffff9801dabf000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1dac49a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1dac4ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`1dac4b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`1dac4bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`1dac4c20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1dac4c20)
        00000000`0726fc58 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`0726fc60 000007fe`fd7ac9b9 kernel32!WaitForSingleObjectEx+0x9c
        00000000`0726fd20 000007fe`fd7657f6 ole32!CDllHost::MTAWorkerLoop+0x23
        00000000`0726fd50 000007fe`fd7a3b7e ole32!CDllHost::WorkerThread+0xd0
        00000000`0726fd90 000007fe`fd7a3c0a ole32!CRpcThread::WorkerLoop+0x1e
        00000000`0726fdd0 00000000`76bfcdcd ole32!CRpcThreadCache::RpcWorkerThreadEntry+0x2a
        00000000`0726fe00 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0726fe30 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800204ebb0  Cid 0a84.0da0  Teb: 000007fffff84000 Win32Thread: fffff900c1ffa310
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8001e66650  SynchronizationEvent
            fffffa8001e666b0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004ba4c10       Image:         explorer.exe
        Wait Start TickCount      16235          Ticks: 30344 (0:00:07:53.369)
        Context Switch Count      65                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address SHLWAPI!WrapperThreadProc (0x000007fefda24f20)
        Stack Init fffff98020cf5db0 Current fffff98020cf5260
        Base fffff98020cf6000 Limit fffff98020cee000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`20cf52a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`20cf53e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`20cf5440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`20cf54b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`20cf5960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`20cf5bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`20cf5c20)
        00000000`088bf018 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`088bf020 00000000`76d1e96d kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`088bf130 00000000`76d1e85e USER32!RealMsgWaitForMultipleObjectsEx+0x129
        00000000`088bf1d0 00000000`76d13680 USER32!MsgWaitForMultipleObjectsEx+0x46
        00000000`088bf210 000007fe`f3de64b3 USER32!MsgWaitForMultipleObjects+0x20
        00000000`088bf250 000007fe`fda24d48 wscntfy!CWscNotify::_ExecThread+0xeb
        00000000`088bf6f0 00000000`76bfcdcd SHLWAPI!WrapperThreadProc+0xfc
        00000000`088bf7d0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`088bf800 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80028e6060  Cid 0a84.0ff4  Teb: 000007fffff82000 Win32Thread: fffff900c265cad0
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa80025b9200  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004ba4c10       Image:         explorer.exe
        Wait Start TickCount      36751          Ticks: 9828 (0:00:02:33.317)
        Context Switch Count      20                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address SHLWAPI!WrapperThreadProc (0x000007fefda24f20)
        Stack Init fffff98012b8fdb0 Current fffff98012b8f740
        Base fffff98012b90000 Limit fffff98012b8a000 Call 0
        Priority 12 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`12b8f780 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12b8f8c0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`12b8f920 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`12b8f9a0 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`12b8fa40 fffff960`000c7e1e win32k!xxxSleepThread+0x56
        fffff980`12b8fa70 fffff960`000c7f25 win32k!xxxRealInternalGetMessage+0x72e
        fffff980`12b8fb50 fffff960`000c97e4 win32k!xxxInternalGetMessage+0x35
        fffff980`12b8fb90 fffff800`01c4d733 win32k!NtUserGetMessage+0x64
        fffff980`12b8fc20 00000000`76d1e6aa nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12b8fc20)
        00000000`08c5fdd8 00000000`76d1e6ea USER32!ZwUserGetMessage+0xa
        00000000`08c5fde0 000007fe`fdf545b7 USER32!GetMessageW+0x34
        00000000`08c5fe10 000007fe`fda24d48 SHELL32!_LocalServerThread+0x3a
        00000000`08c5fe70 00000000`76bfcdcd SHLWAPI!WrapperThreadProc+0xfc
        00000000`08c5ff50 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`08c5ff80 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8002613b30  Cid 0a84.0314  Teb: 000007fffff7e000 Win32Thread: fffff900c1f0ed60
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800219b420  SynchronizationEvent
            fffffa80021402a0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004ba4c10       Image:         explorer.exe
        Wait Start TickCount      38393          Ticks: 8186 (0:00:02:07.702)
        Context Switch Count      7998                 LargeStack
        UserTime                  00:00:00.733
        KernelTime                00:00:00.795
        Win32 Start Address BROWSEUI!BrowserNewThreadProc (0x000007fef821c330)
        Stack Init fffff98012b69790 Current fffff98012b68c40
        Base fffff98012b6a000 Limit fffff98012b5e000 Call fffff98012b699e0
        Priority 10 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`12b68c80 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12b68dc0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`12b68e20 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`12b68e90 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`12b69340 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`12b69590 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12b69600)
        00000000`08e2f3d8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`08e2f3e0 00000000`76d1e96d kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`08e2f4f0 000007fe`fb961ab6 USER32!RealMsgWaitForMultipleObjectsEx+0x129
        00000000`08e2f590 000007fe`fb96371f DUser!CoreSC::Wait+0x62
        00000000`08e2f5e0 000007fe`fb963696 DUser!CoreSC::WaitMessage+0x6f
        00000000`08e2f620 00000000`76d0bd1a DUser!MphWaitMessageEx+0x36
        00000000`08e2f650 00000000`76e22016 USER32!_ClientWaitMessageExMPH+0x1a
        00000000`08e2f6a0 00000000`76d1df2a ntdll!KiUserCallbackDispatcherContinue (TrapFrame @
00000000`08e2f568)
        00000000`08e2f708 000007fe`f8218b33 USER32!ZwUserWaitMessage+0xa
        00000000`08e2f710 000007fe`f821c3e4 BROWSEUI!CBrowserFrame::FrameMessagePump+0x29f
        00000000`08e2f7a0 00000000`76bfcdcd BROWSEUI!BrowserNewThreadProc+0xb4
        00000000`08e2f7e0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`08e2f810 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8002a48650  Cid 0a84.0efc  Teb: 000007fffff6a000 Win32Thread: fffff900c07e02b0
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa8002a485d0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004ba4c10       Image:         explorer.exe
        Wait Start TickCount      15992          Ticks: 30587 (0:00:07:57.160)
        Context Switch Count      119                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address WINMM!mciwindow (0x000007fefb3616c0)
        Stack Init fffff9800e5c6db0 Current fffff9800e5c6740
        Base fffff9800e5c7000 Limit fffff9800e5bf000 Call 0
        Priority 11 BasePriority 10 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e5c6780 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e5c68c0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0e5c6920 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`0e5c69a0 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`0e5c6a40 fffff960`000c7e1e win32k!xxxSleepThread+0x56
        fffff980`0e5c6a70 fffff960`000c7f25 win32k!xxxRealInternalGetMessage+0x72e
        fffff980`0e5c6b50 fffff960`000c97e4 win32k!xxxInternalGetMessage+0x35
        fffff980`0e5c6b90 fffff800`01c4d733 win32k!NtUserGetMessage+0x64
        fffff980`0e5c6c20 00000000`76d1e6aa nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e5c6c20)
        00000000`09a6fb78 00000000`76d1bf4e USER32!ZwUserGetMessage+0xa
        00000000`09a6fb80 000007fe`fb361785 USER32!GetMessageA+0xc3
        00000000`09a6fbb0 00000000`76bfcdcd WINMM!mciwindow+0x174
        00000000`09a6fc50 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`09a6fc80 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80020e6bb0  Cid 0a84.03e0  Teb: 000007fffffdc000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8004bcf8d0  QueueObject
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004ba4c10       Image:         explorer.exe
        Wait Start TickCount      41192          Ticks: 5387 (0:00:01:24.037)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff98012bf1db0 Current fffff98012bf1810
        Base fffff98012bf2000 Limit fffff98012bec000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`12bf1850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12bf1990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`12bf19f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`12bf1a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`12bf1b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`12bf1bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12bf1c20)
        00000000`0312fc48 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`0312fc50 000007fe`fedce7a3 kernel32!GetQueuedCompletionStatus+0x48
        00000000`0312fcb0 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`0312fd40 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`0312fdf0 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`0312fe20 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`0312fe60 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`0312fe90 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0312fec0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

Sidebar process

```
PROCESS fffffa8004c8f270
    SessionId: 1  Cid: 0bac    Peb: 7fffffd8000  ParentCid: 0a84
    DirBase: 330bb000  ObjectTable: fffff88002954190  HandleCount: 395.
    Image: sidebar.exe
    VadRoot fffffa8004c8d340 Vads 238 Clone 0 Private 3730. Modified 3276. Locked 0.
    DeviceMap fffff88006100250
    Token                             fffff88002516060
    ElapsedTime                       00:11:19.297
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         275432
    QuotaPoolUsage[NonPagedPool]      23584
    Working Set Sizes (now,min,max)  (4724, 50, 345) (18896KB, 200KB, 1380KB)
    PeakWorkingSetSize                7453
    VirtualSize                       170 Mb
    PeakVirtualSize                   173 Mb
    PageFaultCount                    126910
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      7012
    Job                               fffffa8004c32850

    Setting context for this process...
.process /p /r fffffa8004c8f270

    !peb
PEB at 000007fffffd8000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00000000ff630000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 0000000000262830 . 0000000003ad9c70
    Ldr.InLoadOrderModuleList:           0000000000262740 . 0000000003ad9c50
    Ldr.InMemoryOrderModuleList:         0000000000262750 . 0000000003ad9c60
            Base TimeStamp                     Module
        ff630000 476507e0 Dec 16 11:11:28 2007 C:\Program Files\Windows Sidebar\sidebar.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        76bc0000 4549d328 Nov 02 11:14:48 2006 C:\Windows\system32\kernel32.dll
     7fefea30000 4549d267 Nov 02 11:11:35 2006 C:\Windows\system32\ADVAPI32.dll
     7fefed90000 469c43bb Jul 17 05:21:15 2007 C:\Windows\system32\RPCRT4.dll
     7fefec20000 4549d273 Nov 02 11:11:47 2006 C:\Windows\system32\GDI32.dll
        76d00000 45d3ee19 Feb 15 05:22:33 2007 C:\Windows\system32\USER32.dll
     7fefdd40000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\system32\msvcrt.dll
     7fefc180000 4549d253 Nov 02 11:11:15 2006 C:\Windows\system32\ATL.DLL
     7fefd760000 4549d317 Nov 02 11:14:31 2006 C:\Windows\system32\ole32.dll
     7fefdab0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\OLEAUT32.dll
     7fefbe70000 4549d32b Nov 02 11:14:51 2006 C:\Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_1559f1c6f365a7fa\COMCTL32.dll
     7fefda10000 4549d31f Nov 02 11:14:39 2006 C:\Windows\system32\SHLWAPI.dll
     7fefb610000 4549d245 Nov 02 11:11:01 2006
C:\Windows\WinSxS\amd64_microsoft.windows.gdiplus_6595b64144ccf1df_1.0.6000.16386_none_56f375c7b4f2
4821\gdiplus.dll
     7fefddf0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\SHELL32.dll
     7fefd5f0000 470c5dac Oct 10 06:05:48 2007 C:\Windows\system32\urlmon.dll
     7fefebc0000 4549d29c Nov 02 11:12:28 2006 C:\Windows\system32\iertutil.dll
     7fefcc50000 4549d344 Nov 02 11:15:16 2006 C:\Windows\system32\CRYPT32.dll
     7fefce00000 4549d2df Nov 02 11:13:35 2006 C:\Windows\system32\MSASN1.dll
     7fefd3b0000 4549d336 Nov 02 11:15:02 2006 C:\Windows\system32\USERENV.dll
     7fefd390000 4549d33f Nov 02 11:15:11 2006 C:\Windows\system32\Secur32.dll
     7fef9770000 4549d31c Nov 02 11:14:36 2006 C:\Windows\system32\sfc.dll
     7fef97e0000 4549d31d Nov 02 11:14:37 2006 C:\Windows\system32\sfc_os.DLL
     7fefeed0000 4549d318 Nov 02 11:14:32 2006 C:\Windows\system32\SETUPAPI.dll
     7fef8c50000 4549d2b7 Nov 02 11:12:55 2006 C:\Windows\system32\dwmapi.dll
```

```
     7fef6d90000 4549d34a Nov 02 11:15:22 2006 C:\Windows\system32\CRYPTUI.dll
     7fefc1e0000 4549d381 Nov 02 11:16:17 2006 C:\Windows\system32\WINTRUST.dll
     7fefda90000 462443ee Apr 17 04:50:06 2007 C:\Windows\system32\imagehlp.dll
     7fefcf70000 4549d2fc Nov 02 11:14:04 2006 C:\Windows\system32\NETAPI32.dll
     7fefd530000 4549d310 Nov 02 11:14:24 2006 C:\Windows\system32\PSAPI.DLL
     7fefd590000 4549d396 Nov 02 11:16:38 2006 C:\Windows\system32\WLDAP32.dll
     7fefd540000 4549d38a Nov 02 11:16:26 2006 C:\Windows\system32\WS2_32.dll
     7feff0b0000 4549d370 Nov 02 11:16:00 2006 C:\Windows\system32\NSI.dll
     7fefca50000 4549d336 Nov 02 11:15:02 2006 C:\Windows\system32\VERSION.dll
     7fefc570000 4549d324 Nov 02 11:14:44 2006 C:\Windows\system32\MSIMG32.dll
     7fefc330000 4549d33b Nov 02 11:15:07 2006 C:\Windows\system32\UxTheme.dll
     7fefd9e0000 4549d2cb Nov 02 11:13:15 2006 C:\Windows\system32\IMM32.DLL
     7fefdc30000 4549d2e6 Nov 02 11:13:42 2006 C:\Windows\system32\MSCTF.dll
     7feff0c0000 4549d2a1 Nov 02 11:12:33 2006 C:\Windows\system32\LPK.DLL
     7fefd940000 4549d337 Nov 02 11:15:03 2006 C:\Windows\system32\USP10.dll
     7fefdb90000 4549d282 Nov 02 11:12:02 2006 C:\Windows\system32\CLBCatQ.DLL
     7fefd1f0000 4549d32f Nov 02 11:14:55 2006 C:\Windows\system32\SXS.DLL
     7fefc620000 4549d31d Nov 02 11:14:37 2006 C:\Windows\system32\rsaenh.dll
     7fefc450000 4549d34e Nov 02 11:15:26 2006 C:\Windows\system32\WTSAPI32.dll
     7fefd1b0000 4549d380 Nov 02 11:16:16 2006 C:\Windows\system32\WINSTA.dll
     7fefba40000 4549d384 Nov 02 11:16:20 2006 C:\Windows\system32\Wlanapi.dll
     7fef7900000 4549d322 Nov 02 11:14:42 2006 C:\Windows\system32\OneX.DLL
     7fef78e0000 4549d26a Nov 02 11:11:38 2006 C:\Windows\system32\eappprxy.dll
     7fef7540000 4549d267 Nov 02 11:11:35 2006 C:\Windows\system32\eappcfg.dll
     7fefca60000 4549d252 Nov 02 11:11:14 2006 C:\Windows\system32\bcrypt.dll
     7fef9c40000 46662887 Jun 06 04:22:47 2007 C:\Windows\System32\msxml3.dll
     7fefec90000 470c5de6 Oct 10 06:06:46 2007 C:\Windows\system32\WININET.dll
        76f70000 4549b4d2 Nov 02 09:05:22 2006 C:\Windows\system32\Normaliz.dll
     7fef4800000 4722dd92 Oct 27 07:41:22 2007 C:\Windows\system32\mshtml.dll
     7fef7500000 4549d329 Nov 02 11:14:49 2006 C:\Windows\system32\msls31.dll
     7fefb440000 4549d297 Nov 02 11:12:23 2006 C:\Windows\system32\MLANG.dll
     7fef78d0000 4549d326 Nov 02 11:14:46 2006 C:\Windows\system32\msimtf.dll
     7fef5880000 470c5d32 Oct 10 06:03:46 2007 C:\Windows\system32\ieframe.dll
     7fef6640000 4549d28a Nov 02 11:12:10 2006 C:\Windows\system32\jscript.dll
     7fef75d0000 4549d2c9 Nov 02 11:13:13 2006 C:\Windows\system32\ImgUtil.dll
     7fef6d30000 470c5d3f Oct 10 06:03:59 2007 C:\Windows\system32\Dxtrans.dll
     7fef7590000 4549d33a Nov 02 11:15:06 2006 C:\Windows\system32\pngfilt.dll
     7fef75c0000 4549d26a Nov 02 11:11:38 2006 C:\Windows\system32\ddrawex.dll
     7fef6aa0000 4549d269 Nov 02 11:11:37 2006 C:\Windows\system32\DDRAW.dll
     7fef7990000 4549d265 Nov 02 11:11:33 2006 C:\Windows\system32\DCIMAN32.dll
     7fefc5b0000 4549d384 Nov 02 11:16:20 2006 C:\Windows\system32\NTMARTA.DLL
     7fefce20000 4549d315 Nov 02 11:14:29 2006 C:\Windows\system32\SAMLIB.dll
        71e00000 453ebf88 Oct 25 02:36:08 2006 C:\Windows\system32\atiumd64.dll
         4f30000 453ebe3e Oct 25 02:30:38 2006 C:\Windows\system32\atiumd6a.dll
     7fef70b0000 470c5d3e Oct 10 06:03:58 2007 C:\Windows\system32\Dxtmsft.dll
     7fef79a0000 4549d346 Nov 02 11:15:18 2006 C:\Windows\system32\thumbcache.dll
     7fefd310000 4549d247 Nov 02 11:11:03 2006 C:\Windows\system32\apphelp.dll
     7fef83b0000 4549d319 Nov 02 11:14:33 2006 C:\Windows\System32\shdocvw.dll
     7fefb4d0000 4549d30d Nov 02 11:14:21 2006 C:\Windows\system32\PROPSYS.dll
     7fefb140000 4549d365 Nov 02 11:15:49 2006 C:\Windows\system32\windowscodecs.dll
     7fef6ee0000 4549d2e5 Nov 02 11:13:41 2006 C:\Windows\system32\mscms.dll
     7fef8520000 4549d37c Nov 02 11:16:12 2006 C:\Windows\system32\WINSPOOL.DRV
     7fefb3f0000 4549d28a Nov 02 11:12:10 2006 C:\Windows\system32\icm32.dll
     7fef5220000 470c5da5 Oct 10 06:05:41 2007 C:\Windows\system32\mshtmled.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       0000000000260000
    ProcessParameters: 0000000000261d90
    WindowTitle:  'C:\Program Files\Windows Sidebar\sidebar.exe'
    ImageFile:    'C:\Program Files\Windows Sidebar\sidebar.exe'
    CommandLine:  '"C:\Program Files\Windows Sidebar\sidebar.exe" /autoRun'
    DllPath:      'C:\Program Files\Windows
Sidebar;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Windows;C:\Window
s\System32\Wbem'
    Environment:  0000000000261310
        =::=::\
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\UserName\AppData\Roaming
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
```

```
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        HOMEDRIVE=C:
        HOMEPATH=\Users\UserName
        LOCALAPPDATA=C:\Users\UserName\AppData\Local
        LOGONSERVER=\\COMPUTERNAME
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public
        SESSIONNAME=Console
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Users\UserName\AppData\Local\Temp
        TMP=C:\Users\UserName\AppData\Local\Temp
        USERDOMAIN=COMPUTERNAME
        USERNAME=UserName
        USERPROFILE=C:\Users\UserName
        windir=C:\Windows


        THREAD fffffa8004c89bb0  Cid 0bac.0bb0  Teb: 000007fffffde000 Win32Thread: fffff900c078d950
WAIT: (UserRequest) UserMode Alertable
            fffffa8004bf7210  SynchronizationEvent
            fffffa8003fe22b0  SynchronizationEvent
        IRP List:
            fffffa80045c93c0: (0006,0118) Flags: 00020900  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004c8f270       Image:         sidebar.exe
        Wait Start TickCount      46526          Ticks: 53 (0:00:00:00.826)
        Context Switch Count      123806                 LargeStack
        UserTime                  00:00:00.686
        KernelTime                00:00:04.602
        Win32 Start Address sidebar!WinMainCRTStartup (0x00000000ff6f9238)
        Stack Init fffff98012f1ddb0 Current fffff98012f1d260
        Base fffff98012f1e000 Limit fffff98012f14000 Call 0
        Priority 12 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`12f1d2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12f1d3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`12f1d440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`12f1d4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`12f1d960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`12f1dbb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12f1dc20)
        00000000`000eed38 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`000eed40 00000000`76d1e96d kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`000eee50 00000000`76d1e85e USER32!RealMsgWaitForMultipleObjectsEx+0x129
        00000000`000eeef0 00000000`ff69014d USER32!MsgWaitForMultipleObjectsEx+0x46
        00000000`000eef30 00000000`ff64e478 sidebar!PresentationHost::Run+0x85
        00000000`000ef440 00000000`ff64ebaa sidebar!SidebarMain+0x644
        00000000`000efa90 00000000`ff6f908f sidebar!WinMain+0x28a
        00000000`000efad0 00000000`76bfcdcd sidebar!CComStdCallThunkHelper+0x1ef
        00000000`000efb90 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`000efbc0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8003fe5bb0  Cid 0bac.08b4  Teb: 000007fffffdc000 Win32Thread: fffff900c1eab460
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80047705f0  NotificationEvent
            fffffa8004770650  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004c8f270       Image:         sidebar.exe
        Wait Start TickCount      46535          Ticks: 44 (0:00:00:00.686)
        Context Switch Count      93                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.062
        Win32 Start Address sidebar!GThumbnailThreadProc (0x00000000ff66c94c)
        Stack Init fffff9801574adb0 Current fffff9801574a260
        Base fffff9801574b000 Limit fffff98015744000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1574a2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1574a3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`1574a440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`1574a4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`1574a960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`1574abb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1574ac20)
        00000000`02b2fc88 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`02b2fc90 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`02b2fda0 00000000`ff66c997 kernel32!WaitForMultipleObjects+0x11
        00000000`02b2fde0 00000000`76bfcdcd sidebar!GThumbnailThreadProc+0x4b
        00000000`02b2fe30 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02b2fe60 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80042063c0  Cid 0bac.09e4  Teb: 000007fffffda000 Win32Thread: fffff900c2097d60
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8003dd0e40  NotificationEvent
            fffffa80042062b0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004c8f270       Image:         sidebar.exe
        Wait Start TickCount      15650          Ticks: 30929 (0:00:08:02.495)
        Context Switch Count      44                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address gdiplus!BackgroundThreadProc (0x000007fefb672410)
        Stack Init fffff980158d1db0 Current fffff980158d1260
        Base fffff980158d2000 Limit fffff980158ca000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`158d12a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`158d13e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`158d1440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`158d14b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`158d1960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`158d1bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`158d1c20)
        00000000`02e1f9d8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`02e1f9e0 00000000`76d1e96d kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`02e1faf0 00000000`76d1e85e USER32!RealMsgWaitForMultipleObjectsEx+0x129
        00000000`02e1fb90 00000000`76d13680 USER32!MsgWaitForMultipleObjectsEx+0x46
        00000000`02e1fbd0 000007fe`fb672478 USER32!MsgWaitForMultipleObjects+0x20
        00000000`02e1fc10 00000000`76bfcdcd gdiplus!BackgroundThreadProc+0x68
        00000000`02e1fc80 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02e1fcb0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8003df7060  Cid 0bac.09dc  Teb: 000007fffffd6000 Win32Thread: fffff900c1c11d60
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8004205120  QueueObject
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004c8f270       Image:         sidebar.exe
        Wait Start TickCount      29245          Ticks: 17334 (0:00:04:30.412)
        Context Switch Count      17                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff98020d1bdb0 Current fffff98020d1b810
        Base fffff98020d1c000 Limit fffff98020d15000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`20d1b850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`20d1b990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`20d1b9f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`20d1ba80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`20d1bb00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`20d1bbb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`20d1bc20)
        00000000`02c3f668 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`02c3f670 000007fe`fedce7a3 kernel32!GetQueuedCompletionStatus+0x48
        00000000`02c3f6d0 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`02c3f760 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`02c3f810 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`02c3f840 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`02c3f880 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`02c3f8b0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02c3f8e0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80046a87f0  Cid 0bac.0a2c  Teb: 000007fffffae000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8003d53290  NotificationEvent
            fffffa8004300250  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004c8f270       Image:         sidebar.exe
        Wait Start TickCount      3815           Ticks: 42764 (0:00:11:07.122)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address sidebar!Killbits::KillbitsChangeWaitProc (0x00000000ff66fd04)
        Stack Init fffff9800f3c0db0 Current fffff9800f3c0260
        Base fffff9800f3c1000 Limit fffff9800f3bb000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0f3c02a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0f3c03e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0f3c0440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0f3c04b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0f3c0960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0f3c0bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0f3c0c20)
        00000000`02a8f888 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`02a8f890 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`02a8f9a0 00000000`ff66fda8 kernel32!WaitForMultipleObjects+0x11
        00000000`02a8f9e0 00000000`76bfcdcd sidebar!Killbits::KillbitsChangeWaitProc+0xa4
        00000000`02a8fa30 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02a8fa60 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004b68bb0  Cid 0bac.01a4  Teb: 000007fffffac000 Win32Thread: fffff900c2228780
WAIT: (UserRequest) UserMode Alertable
            fffffa800296dcd0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004c8f270       Image:         sidebar.exe
        Wait Start TickCount      27322          Ticks: 19257 (0:00:05:00.411)
        Context Switch Count      117434                 LargeStack
        UserTime                  00:00:00.046
        KernelTime                00:00:00.296
        Win32 Start Address sidebar!StockLib::Utility::t_ObjectThreadProc<PartInstance>
(0x00000000ff65e76c)
        Stack Init fffff980156b2db0 Current fffff980156b2260
        Base fffff980156b3000 Limit fffff980156a8000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`156b22a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`156b23e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`156b2440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`156b24b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`156b2960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`156b2bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`156b2c20)
        00000000`03cbf7a8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`03cbf7b0 00000000`76d1e96d kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`03cbf8c0 00000000`76d1e85e USER32!RealMsgWaitForMultipleObjectsEx+0x129
        00000000`03cbf960 00000000`ff69014d USER32!MsgWaitForMultipleObjectsEx+0x46
        00000000`03cbf9a0 00000000`ff65e931 sidebar!PresentationHost::Run+0x85
        00000000`03cbfeb0 00000000`76bfcdcd
sidebar!StockLib::Utility::t_ObjectThreadProc<PartInstance>+0x1c5
        00000000`03cbff10 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`03cbff40 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004874bb0  Cid 0bac.09ec  Teb: 000007fffffaa000 Win32Thread: fffff900c1f962e0
WAIT: (UserRequest) UserMode Alertable
            fffffa8004499240  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004c8f270       Image:         sidebar.exe
        Wait Start TickCount      46535          Ticks: 44 (0:00:00:00.686)
        Context Switch Count      2050                 LargeStack
        UserTime                  00:00:00.062
        KernelTime                00:00:00.171
        Win32 Start Address sidebar!StockLib::Utility::t_ObjectThreadProc<PartInstance>
(0x00000000ff65e76c)
        Stack Init fffff980156c5db0 Current fffff980156c5260
        Base fffff980156c6000 Limit fffff980156bc000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`156c52a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`156c53e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`156c5440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`156c54b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`156c5960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`156c5bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`156c5c20)
        00000000`03e8f3a8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`03e8f3b0 00000000`76d1e96d kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`03e8f4c0 00000000`76d1e85e USER32!RealMsgWaitForMultipleObjectsEx+0x129
        00000000`03e8f560 00000000`ff69014d USER32!MsgWaitForMultipleObjectsEx+0x46
        00000000`03e8f5a0 00000000`ff65e931 sidebar!PresentationHost::Run+0x85
        00000000`03e8fab0 00000000`76bfcdcd
sidebar!StockLib::Utility::t_ObjectThreadProc<PartInstance>+0x1c5
        00000000`03e8fb10 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`03e8fb40 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004a5c060  Cid 0bac.0b74  Teb: 000007fffffa8000 Win32Thread: fffff900c2239d60
WAIT: (UserRequest) UserMode Alertable
            fffffa800405bce0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004c8f270       Image:         sidebar.exe
        Wait Start TickCount      46566          Ticks: 13 (0:00:00:00.202)
        Context Switch Count      3257                 LargeStack
        UserTime                  00:00:00.202
        KernelTime                00:00:00.249
        Win32 Start Address sidebar!StockLib::Utility::t_ObjectThreadProc<PartInstance>
(0x00000000ff65e76c)
        Stack Init fffff980156d8db0 Current fffff980156d8260
        Base fffff980156d9000 Limit fffff980156cf000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`156d82a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`156d83e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`156d8440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`156d84b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`156d8960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`156d8bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`156d8c20)
        00000000`03fef188 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`03fef190 00000000`76d1e96d kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`03fef2a0 00000000`76d1e85e USER32!RealMsgWaitForMultipleObjectsEx+0x129
        00000000`03fef340 00000000`ff69014d USER32!MsgWaitForMultipleObjectsEx+0x46
        00000000`03fef380 00000000`ff65e931 sidebar!PresentationHost::Run+0x85
        00000000`03fef890 00000000`76bfcdcd
sidebar!StockLib::Utility::t_ObjectThreadProc<PartInstance>+0x1c5
        00000000`03fef8f0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`03fef920 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80045ac850  Cid 0bac.0684  Teb: 000007fffffa4000 Win32Thread: fffff900c2243c70
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800475e100  SynchronizationEvent
            fffffa80045ac908  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004c8f270       Image:         sidebar.exe
        Wait Start TickCount      46535          Ticks: 44 (0:00:00:00.686)
        Context Switch Count      282                  LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address mshtml!CExecFT::StaticThreadProc (0x000007fef4834ea0)
        Stack Init fffff980156fedb0 Current fffff980156fe960
        Base fffff980156ff000 Limit fffff980156f7000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`156fe9a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`156feae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`156feb40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`156febc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`156fec20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`156fec20)
        00000000`04d2f778 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`04d2f780 000007fe`f48dc07f kernel32!WaitForSingleObjectEx+0x9c
        00000000`04d2f840 000007fe`f4897bba mshtml!CDwnTaskExec::ThreadExec+0x2ac
        00000000`04d2f8b0 00000000`76bfcdcd mshtml!CExecFT::ThreadProc+0x4c
        00000000`04d2f8e0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`04d2f910 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800407a950  Cid 0bac.07d8  Teb: 000007fffffa2000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8003fe3b80  QueueObject
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004c8f270       Image:         sidebar.exe
        Wait Start TickCount      4026           Ticks: 42553 (0:00:11:03.831)
        Context Switch Count      6
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address Dxtrans!TMThreadProc (0x000007fef6d31670)
        Stack Init fffff980102cbdb0 Current fffff980102cb810
        Base fffff980102cc000 Limit fffff980102c6000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`102cb850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`102cb990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`102cb9f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`102cba80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`102cbb00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`102cbbb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`102cbc20)
        00000000`05ecfa68 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`05ecfa70 000007fe`f6d316dc kernel32!GetQueuedCompletionStatus+0x48
        00000000`05ecfad0 00000000`76bfcdcd Dxtrans!TMThreadProc+0x6c
        00000000`05ecfb90 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`05ecfbc0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004655bb0  Cid 0bac.081c  Teb: 000007fffffa0000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8003fe3b80  QueueObject
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004c8f270       Image:         sidebar.exe
        Wait Start TickCount      46535          Ticks: 44 (0:00:00:00.686)
        Context Switch Count      87
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address Dxtrans!TMThreadProc (0x000007fef6d31670)
        Stack Init fffff9800e466db0 Current fffff9800e466810
        Base fffff9800e467000 Limit fffff9800e461000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0e466850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e466990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0e4669f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0e466a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`0e466b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`0e466bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e466c20)
        00000000`05e2fbb8 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`05e2fbc0 000007fe`f6d316dc kernel32!GetQueuedCompletionStatus+0x48
        00000000`05e2fc20 00000000`76bfcdcd Dxtrans!TMThreadProc+0x6c
        00000000`05e2fce0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`05e2fd10 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80046c8bb0  Cid 0bac.0bb8  Teb: 000007fffff9e000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8003fe3b80  QueueObject
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004c8f270       Image:         sidebar.exe
        Wait Start TickCount      4026           Ticks: 42553 (0:00:11:03.831)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address Dxtrans!TMThreadProc (0x000007fef6d31670)
        Stack Init fffff98010365db0 Current fffff98010365810
        Base fffff98010366000 Limit fffff98010360000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`10365850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`10365990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`103659f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`10365a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`10365b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`10365bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`10365c20)
        00000000`05f4fe38 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`05f4fe40 000007fe`f6d316dc kernel32!GetQueuedCompletionStatus+0x48
        00000000`05f4fea0 00000000`76bfcdcd Dxtrans!TMThreadProc+0x6c
        00000000`05f4ff60 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`05f4ff90 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa800497c7c0  Cid 0bac.0b48  Teb: 000007fffff9c000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8003fe3b80  QueueObject
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004c8f270       Image:         sidebar.exe
        Wait Start TickCount      4120           Ticks: 42459 (0:00:11:02.364)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address Dxtrans!TMThreadProc (0x000007fef6d31670)
        Stack Init fffff9800c27bdb0 Current fffff9800c27b810
        Base fffff9800c27c000 Limit fffff9800c276000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0c27b850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0c27b990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0c27b9f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0c27ba80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`0c27bb00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`0c27bbb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0c27bc20)
        00000000`0408f6c8 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`0408f6d0 000007fe`f6d316dc kernel32!GetQueuedCompletionStatus+0x48
        00000000`0408f730 00000000`76bfcdcd Dxtrans!TMThreadProc+0x6c
        00000000`0408f7f0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0408f820 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

Smax4pnp process

```
PROCESS fffffa80045424e0
    SessionId: 1  Cid: 0884    Peb: 7efdf000  ParentCid: 0bcc
    DirBase: 2e185000  ObjectTable: fffff88005f48580  HandleCount: 126.
    Image: smax4pnp.exe
    VadRoot fffffa8003f6d940 Vads 103 Clone 0 Private 470. Modified 415. Locked 0.
    DeviceMap fffff88006100250
    Token                             fffff88001ff1ab0
    ElapsedTime                       00:11:16.783
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.031
    QuotaPoolUsage[PagedPool]         138048
    QuotaPoolUsage[NonPagedPool]      9760
    Working Set Sizes (now,min,max)  (1801, 50, 345) (7204KB, 200KB, 1380KB)
    PeakWorkingSetSize                2968
    VirtualSize                       80 Mb
    PeakVirtualSize                   86 Mb
    PageFaultCount                    3357
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      1991

    Setting context for this process...
.process /p /r fffffa80045424e0

    !peb
PEB at 000000007efdf000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         0000000000400000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00000000001a2a10 . 00000000001a2d70
    Ldr.InLoadOrderModuleList:           00000000001a2920 . 00000000001a2ed0
    Ldr.InMemoryOrderModuleList:         00000000001a2930 . 00000000001a2ee0
            Base TimeStamp                     Module
          400000 452bb8dc Oct 10 16:14:36 2006 C:\Program Files (x86)\Analog
Devices\Core\smax4pnp.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        75110000 4549d371 Nov 02 11:16:01 2006 C:\Windows\system32\wow64.dll
        75000000 4549d374 Nov 02 11:16:04 2006 C:\Windows\system32\wow64win.dll
        75100000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\wow64cpu.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       00000000001a0000
    ProcessParameters: 00000000001a1ed0
    WindowTitle:  'C:\Program Files (x86)\Analog Devices\Core\smax4pnp.exe'
    ImageFile:    'C:\Program Files (x86)\Analog Devices\Core\smax4pnp.exe'
    CommandLine:  '"C:\Program Files (x86)\Analog Devices\Core\smax4pnp.exe" '
    DllPath:      'C:\Program Files (x86)\Analog
Devices\Core;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Program Files (x86)\Analog
Devices\Core;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem'
    Environment:  00000000001a1310
        =::=::\
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\UserName\AppData\Roaming
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        HOMEDRIVE=C:
        HOMEPATH=\Users\UserName
        LOCALAPPDATA=C:\Users\UserName\AppData\Local
        LOGONSERVER=\\COMPUTERNAME
        NUMBER_OF_PROCESSORS=2
```

```
        OS=Windows_NT
        Path=C:\Program Files (x86)\Analog
Devices\Core;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public
        SESSIONNAME=Console
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Users\UserName\AppData\Local\Temp
        TMP=C:\Users\UserName\AppData\Local\Temp
        USERDOMAIN=COMPUTERNAME
        USERNAME=UserName
        USERPROFILE=C:\Users\UserName
        windir=C:\Windows


        THREAD fffffa800455a060  Cid 0884.02c4  Teb: 000000007efdb000 Win32Thread: fffff900c1c55010
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa800496a1e0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa80045424e0       Image:         smax4pnp.exe
        Wait Start TickCount      15650          Ticks: 30929 (0:00:08:02.495)
        Context Switch Count      1872                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.234
        Win32 Start Address smax4pnp (0x000000000042e470)
        Stack Init fffff98012e72db0 Current fffff98012e72740
        Base fffff98012e73000 Limit fffff98012e6a000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`12e72780 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12e728c0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`12e72920 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`12e729a0 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`12e72a40 fffff960`000c7e1e win32k!xxxSleepThread+0x56
        fffff980`12e72a70 fffff960`000c7f25 win32k!xxxRealInternalGetMessage+0x72e
        fffff980`12e72b50 fffff960`000c97e4 win32k!xxxInternalGetMessage+0x35
        fffff980`12e72b90 fffff800`01c4d733 win32k!NtUserGetMessage+0x64
        fffff980`12e72c20 00000000`75039f7a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12e72c20)
        00000000`0007e568 00000000`75023160 wow64win!ZwUserGetMessage+0xa
        00000000`0007e570 00000000`7511aa4e wow64win!whNtUserGetMessage+0x30
        00000000`0007e5d0 00000000`75103678 wow64!Wow64SystemServiceEx+0xca
        00000000`0007ee80 00000000`7511abfe wow64cpu!TurboDispatchJumpAddressEnd+0x28
        00000000`0007ef10 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0007ef40 00000000`76e0e23d wow64!Wow64LdrpInitialize+0x492
        00000000`0007f4a0 00000000`76e7e974 ntdll!LdrpInitializeProcess+0x1333
        00000000`0007f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d641
        00000000`0007f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa80039dabb0  Cid 0884.0978  Teb: 000000007efad000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004d2d9b0  SynchronizationEvent
            fffffa8004cf7d80  SynchronizationEvent
            fffffa8004d42b20  SynchronizationEvent
            fffffa80039a8c90  SynchronizationEvent
            fffffa8004d18350  SynchronizationEvent
            fffffa8004d182d0  SynchronizationEvent
            fffffa80039a6060  SynchronizationEvent
            fffffa80039a6120  SynchronizationEvent
            fffffa8004cc8780  SynchronizationEvent
            fffffa8004cc8700  SynchronizationEvent
            fffffa80039a9710  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa80045424e0       Image:         smax4pnp.exe
        Wait Start TickCount      3342           Ticks: 43237 (0:00:11:14.501)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000001000109b
        Stack Init fffff98012fffdb0 Current fffff98012fff260
        Base fffff98013000000 Limit fffff98012ffa000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`12fff2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12fff3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`12fff440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`12fff4b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`12fff960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`12fffbb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12fffc20)
        00000000`026df0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`026df1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`026df1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`026df730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`026df7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa8004cf78d0  Cid 0884.0980  Teb: 000000007efa7000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa8004351c00  SynchronizationTimer
            fffffa8002950ef0  SynchronizationTimer
            fffffa8004354550  SynchronizationTimer
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa80045424e0       Image:         smax4pnp.exe
        Wait Start TickCount      3444           Ticks: 43135 (0:00:11:12.910)
        Context Switch Count      6
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x0000000077046235
        Stack Init fffff98012b9ddb0 Current fffff98012b9d260
        Base fffff98012b9e000 Limit fffff98012b98000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`12b9d2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12b9d3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`12b9d440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`12b9d4b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`12b9d960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`12b9dbb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12b9dc20)
        00000000`029cf0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`029cf1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`029cf1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`029cf730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`029cf7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

CcApp process

```
PROCESS fffffa8004320c10
    SessionId: 1  Cid: 03ec    Peb: 7efdf000  ParentCid: 0bcc
    DirBase: 2e457000  ObjectTable: fffff880024355a0  HandleCount: 203.
    Image: ccApp.exe
    VadRoot fffffa8004d0cd40 Vads 104 Clone 0 Private 482. Modified 1097. Locked 0.
    DeviceMap fffff88006100250
    Token                             fffff880025bb480
    ElapsedTime                       00:11:16.111
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         144792
    QuotaPoolUsage[NonPagedPool]      13616
    Working Set Sizes (now,min,max)  (189, 50, 345) (756KB, 200KB, 1380KB)
    PeakWorkingSetSize                2131
    VirtualSize                       74 Mb
    PeakVirtualSize                   76 Mb
    PageFaultCount                    4709
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      1175

    Setting context for this process...
.process /p /r fffffa8004320c10

    !peb
PEB at 000000007efdf000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         0000000000400000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 0000000000252a70 . 0000000000252dd0
    Ldr.InLoadOrderModuleList:           0000000000252980 . 0000000000252f30
    Ldr.InMemoryOrderModuleList:         0000000000252990 . 0000000000252f40
            Base TimeStamp                     Module
          400000 4578a447 Dec 07 23:31:19 2006 C:\Program Files (x86)\Common Files\Symantec
Shared\ccApp.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        75110000 4549d371 Nov 02 11:16:01 2006 C:\Windows\system32\wow64.dll
        75000000 4549d374 Nov 02 11:16:04 2006 C:\Windows\system32\wow64win.dll
        75100000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\wow64cpu.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       0000000000250000
    ProcessParameters: 0000000000251ee0
    WindowTitle:  'C:\Program Files (x86)\Common Files\Symantec Shared\ccApp.exe'
    ImageFile:    'C:\Program Files (x86)\Common Files\Symantec Shared\ccApp.exe'
    CommandLine:  '"C:\Program Files (x86)\Common Files\Symantec Shared\ccApp.exe" '
    DllPath:      'C:\Program Files (x86)\Common Files\Symantec
Shared;C:\Windows\system32;C:\Windows\system;C:\Windows;.;c:\Program Files (x86)\Common
Files\Symantec Shared\;;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem'
    Environment:  0000000000251310
        =::=::\
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\UserName\AppData\Roaming
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        HOMEDRIVE=C:
        HOMEPATH=\Users\UserName
        LOCALAPPDATA=C:\Users\UserName\AppData\Local
        LOGONSERVER=\\COMPUTERNAME
        NUMBER_OF_PROCESSORS=2
```

```
        OS=Windows_NT
        Path=c:\Program Files (x86)\Common Files\Symantec
Shared\;;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public
        SESSIONNAME=Console
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Users\UserName\AppData\Local\Temp
        TMP=C:\Users\UserName\AppData\Local\Temp
        USERDOMAIN=COMPUTERNAME
        USERNAME=UserName
        USERPROFILE=C:\Users\UserName
        windir=C:\Windows


        THREAD fffffa80047457d0  Cid 03ec.00e4  Teb: 000000007efdb000 Win32Thread: fffff900c1c47d60
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800452f190  SynchronizationEvent
            fffffa8004b541c0  SynchronizationEvent
            fffffa8004745888  NotificationTimer
        IRP List:
            fffffa8004d72010: (0006,0358) Flags: 00060000  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004320c10       Image:         ccApp.exe
        Wait Start TickCount      46331          Ticks: 248 (0:00:00:03.868)
        Context Switch Count      972                 LargeStack
        UserTime                  00:00:00.062
        KernelTime                00:00:00.280
        Win32 Start Address ccApp (0x000000000040ac55)
        Stack Init fffff98010967db0 Current fffff98010967260
        Base fffff98010968000 Limit fffff9801095f000 Call 0
        Priority 13 BasePriority 8 PriorityDecrement 3 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`109672a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`109673e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`10967440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`109674b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`10967960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`10967bb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`10967c20)
        00000000`0007ee68 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`0007ef10 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0007ef40 00000000`76e0e23d wow64!Wow64LdrpInitialize+0x492
        00000000`0007f4a0 00000000`76e7e974 ntdll!LdrpInitializeProcess+0x1333
        00000000`0007f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d641
        00000000`0007f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa80045bcbb0  Cid 03ec.0418  Teb: 000000007efd8000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa8003d76990  SynchronizationTimer
            fffffa8004bfd1a0  SynchronizationEvent
            fffffa8004852d50  SynchronizationEvent
            fffffa8004576720  SynchronizationEvent
            fffffa80045765e0  SynchronizationEvent
            fffffa800455ae90  SynchronizationEvent
            fffffa8004551790  SynchronizationEvent
            fffffa80044a3cc0  SynchronizationEvent
            fffffa8004917fe0  SynchronizationEvent
            fffffa8004c87590  SynchronizationEvent
            fffffa8004551040  SynchronizationEvent
            fffffa8004d0d450  SynchronizationEvent
            fffffa8004538200  SynchronizationEvent
            fffffa80048c2c20  SynchronizationEvent
            fffffa8004551560  SynchronizationEvent
            fffffa8004b9a240  SynchronizationEvent
            fffffa800455f2b0  SynchronizationEvent
            fffffa8004d72940  SynchronizationEvent
            fffffa8004d72468  NotificationEvent
            fffffa8004d72eb0  SynchronizationEvent
            fffffa8004d0d3f0  SynchronizationEvent
            fffffa8004d6fa60  SynchronizationEvent
            fffffa8004d6f920  SynchronizationEvent
            fffffa80044a3e60  SynchronizationEvent
            fffffa8004cbf410  SynchronizationEvent
            fffffa8004cbf3b0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004320c10       Image:         ccApp.exe
        Wait Start TickCount      3322           Ticks: 43257 (0:00:11:14.813)
        Context Switch Count      70
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x0000000077046235
        Stack Init fffff980107a4db0 Current fffff980107a4260
        Base fffff980107a5000 Limit fffff9801079f000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`107a42a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`107a43e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`107a4440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`107a44b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`107a4960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`107a4bb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`107a4c20)
        00000000`0055f0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`0055f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0055f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0055f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0055f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa800455f5e0  Cid 03ec.02b0  Teb: 000000007efad000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa800455a5c0  QueueObject
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004320c10       Image:         ccApp.exe
        Wait Start TickCount      7157           Ticks: 39422 (0:00:10:14.987)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x00000000762f3242
        Stack Init fffff9800dab3db0 Current fffff9800dab3810
        Base fffff9800dab4000 Limit fffff9800daae000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0dab3850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0dab3990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0dab39f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0dab3a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`0dab3b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`0dab3bb0 00000000`751039a2 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0dab3c20)
        00000000`022bf0c8 00000000`7511abfe wow64cpu!RemoveIoCompletionFault+0x41
        00000000`022bf1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`022bf1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`022bf730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`022bf7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa8004d22060  Cid 03ec.0968  Teb: 000000007efaa000 Win32Thread: fffff900c1e8fab0
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa8004d4f440  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004320c10       Image:         ccApp.exe
        Wait Start TickCount      15651          Ticks: 30928 (0:00:08:02.479)
        Context Switch Count      65                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3494f6
        Stack Init fffff9800d1b3db0 Current fffff9800d1b3740
        Base fffff9800d1b4000 Limit fffff9800d1ac000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0d1b3780 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0d1b38c0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0d1b3920 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`0d1b39a0 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`0d1b3a40 fffff960`000c7e1e win32k!xxxSleepThread+0x56
        fffff980`0d1b3a70 fffff960`000c7f25 win32k!xxxRealInternalGetMessage+0x72e
        fffff980`0d1b3b50 fffff960`000c97e4 win32k!xxxInternalGetMessage+0x35
        fffff980`0d1b3b90 fffff800`01c4d733 win32k!NtUserGetMessage+0x64
        fffff980`0d1b3c20 00000000`75039f7a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0d1b3c20)
        00000000`028de7f8 00000000`75023160 wow64win!ZwUserGetMessage+0xa
        00000000`028de800 00000000`7511aa4e wow64win!whNtUserGetMessage+0x30
        00000000`028de860 00000000`75103678 wow64!Wow64SystemServiceEx+0xca
        00000000`028df110 00000000`7511abfe wow64cpu!TurboDispatchJumpAddressEnd+0x28
        00000000`028df1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`028df1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`028df730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`028df7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa8004d225b0  Cid 03ec.0964  Teb: 000000007efa7000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004d4fbd0  NotificationEvent
            fffffa8004d22668  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004320c10       Image:         ccApp.exe
        Wait Start TickCount      45293          Ticks: 1286 (0:00:00:20.061)
        Context Switch Count      578
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3494f6
        Stack Init fffff9800da66db0 Current fffff9800da66960
        Base fffff9800da67000 Limit fffff9800da61000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0da669a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0da66ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0da66b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0da66bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0da66c20 00000000`75103cf9 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0da66c20)
        00000000`0295f128 00000000`75103af6 wow64cpu!CpupSyscallStub+0x9
        00000000`0295f130 00000000`7511abfe wow64cpu!Thunk0ArgReloadState+0x1a
        00000000`0295f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0295f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0295f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0295f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

VPTray process

```
PROCESS fffffa8004541040
    SessionId: 1  Cid: 04e8    Peb: 7efdf000  ParentCid: 0bcc
    DirBase: 2e6e6000  ObjectTable: fffff880028bb560  HandleCount: 367.
    Image: VPTray.exe
    VadRoot fffffa8004b47900 Vads 160 Clone 0 Private 828. Modified 382. Locked 0.
    DeviceMap fffff88006100250
    Token                             fffff88002801670
    ElapsedTime                       00:11:15.861
    UserTime                          00:00:00.015
    KernelTime                        00:00:00.046
    QuotaPoolUsage[PagedPool]         171472
    QuotaPoolUsage[NonPagedPool]      19376
    Working Set Sizes (now,min,max)  (2626, 50, 345) (10504KB, 200KB, 1380KB)
    PeakWorkingSetSize                3417
    VirtualSize                       95 Mb
    PeakVirtualSize                   101 Mb
    PageFaultCount                    5062
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      1456

    Setting context for this process...
.process /p /r fffffa8004541040

    !peb
PEB at 000000007efdf000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         0000000000400000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00000000001f2960 . 00000000001f2cc0
    Ldr.InLoadOrderModuleList:           00000000001f2870 . 00000000001f2e20
    Ldr.InMemoryOrderModuleList:         00000000001f2880 . 00000000001f2e30
            Base TimeStamp                     Module
          400000 4580a5d7 Dec 14 01:16:07 2006 C:\Program Files (x86)\Symantec AntiVirus\VPTray.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        75110000 4549d371 Nov 02 11:16:01 2006 C:\Windows\system32\wow64.dll
        75000000 4549d374 Nov 02 11:16:04 2006 C:\Windows\system32\wow64win.dll
        75100000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\wow64cpu.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       00000000001f0000
    ProcessParameters: 00000000001f1e80
    WindowTitle:  'C:\Program Files (x86)\Symantec AntiVirus\VPTray.exe'
    ImageFile:    'C:\Program Files (x86)\Symantec AntiVirus\VPTray.exe'
    CommandLine:  '"C:\Program Files (x86)\Symantec AntiVirus\VPTray.exe" '
    DllPath:      'C:\Program Files (x86)\Symantec
AntiVirus;C:\Windows\system32;C:\Windows\system;C:\Windows;.;;C:\Windows\system32;C:\Windows;C:\Win
dows\System32\Wbem'
    Environment:  00000000001f1310
        =::=::\
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\UserName\AppData\Roaming
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        HOMEDRIVE=C:
        HOMEPATH=\Users\UserName
        LOCALAPPDATA=C:\Users\UserName\AppData\Local
        LOGONSERVER=\\COMPUTERNAME
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
```

```
        Path=;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public
        SESSIONNAME=Console
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Users\UserName\AppData\Local\Temp
        TMP=C:\Users\UserName\AppData\Local\Temp
        USERDOMAIN=COMPUTERNAME
        USERNAME=UserName
        USERPROFILE=C:\Users\UserName
        windir=C:\Windows


        THREAD fffffa800455b060  Cid 04e8.0448  Teb: 000000007efdb000 Win32Thread: fffff900c070c570
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa8004530b00  SynchronizationEvent
        IRP List:
            fffffa8004d2e010: (0006,0358) Flags: 00060000  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004541040       Image:         VPTray.exe
        Wait Start TickCount      26450          Ticks: 20129 (0:00:05:14.014)
        Context Switch Count      1954                LargeStack
        UserTime                  00:00:00.109
        KernelTime                00:00:00.312
        Win32 Start Address VPTray (0x0000000000411fe4)
        Stack Init fffff9800bbd9db0 Current fffff9800bbd9740
        Base fffff9800bbda000 Limit fffff9800bbd1000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0bbd9780 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0bbd98c0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0bbd9920 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`0bbd99a0 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`0bbd9a40 fffff960`000c7e1e win32k!xxxSleepThread+0x56
        fffff980`0bbd9a70 fffff960`000c7f25 win32k!xxxRealInternalGetMessage+0x72e
        fffff980`0bbd9b50 fffff960`000c97e4 win32k!xxxInternalGetMessage+0x35
        fffff980`0bbd9b90 fffff800`01c4d733 win32k!NtUserGetMessage+0x64
        fffff980`0bbd9c20 00000000`75039f7a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0bbd9c20)
        00000000`0007e568 00000000`75023160 wow64win!ZwUserGetMessage+0xa
        00000000`0007e570 00000000`7511aa4e wow64win!whNtUserGetMessage+0x30
        00000000`0007e5d0 00000000`75103678 wow64!Wow64SystemServiceEx+0xca
        00000000`0007ee80 00000000`7511abfe wow64cpu!TurboDispatchJumpAddressEnd+0x28
        00000000`0007ef10 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0007ef40 00000000`76e0e23d wow64!Wow64LdrpInitialize+0x492
        00000000`0007f4a0 00000000`76e7e974 ntdll!LdrpInitializeProcess+0x1333
        00000000`0007f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d641
        00000000`0007f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa8004ccb680  Cid 04e8.0304  Teb: 000000007efad000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa8004ccbb10  SynchronizationTimer
            fffffa8004ccbeb0  SynchronizationEvent
            fffffa8004ca3eb0  SynchronizationEvent
            fffffa8004ca3770  SynchronizationEvent
            fffffa8004c4d280  SynchronizationEvent
            fffffa8004d24900  SynchronizationEvent
            fffffa8004cf27c0  SynchronizationEvent
            fffffa8004d3fc60  SynchronizationEvent
            fffffa8004d3f990  SynchronizationEvent
            fffffa8004ccbf80  SynchronizationEvent
            fffffa8004d23f60  SynchronizationEvent
            fffffa8004d24610  SynchronizationEvent
            fffffa8004d24670  SynchronizationEvent
            fffffa8004d24160  SynchronizationEvent
            fffffa8004d423e0  SynchronizationEvent
            fffffa8004d3f2c0  SynchronizationEvent
            fffffa8004551260  SynchronizationEvent
            fffffa80045529e0  SynchronizationEvent
            fffffa8004d24ac8  NotificationEvent
            fffffa8004d24960  SynchronizationEvent
            fffffa8004cc8040  SynchronizationEvent
            fffffa8004cc8aa0  SynchronizationEvent
            fffffa8004cc8530  SynchronizationEvent
            fffffa8004cc8390  SynchronizationEvent
            fffffa8004cc81f0  SynchronizationEvent
            fffffa8004cc8110  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004541040       Image:         VPTray.exe
        Wait Start TickCount      3408           Ticks: 43171 (0:00:11:13.471)
        Context Switch Count      85
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x0000000077046235
        Stack Init fffff98012bc0db0 Current fffff98012bc0260
        Base fffff98012bc1000 Limit fffff98012bbb000 Call 0
        Priority 12 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`12bc02a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12bc03e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`12bc0440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`12bc04b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`12bc0960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`12bc0bb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12bc0c20)
        00000000`024df0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`024df1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`024df1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`024df730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`024df7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa8004d17bb0  Cid 04e8.0988  Teb: 000000007efa1000 Win32Thread: fffff900c0734b20
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004cdbdc0  NotificationEvent
            fffffa8004d725a0  SynchronizationEvent
            fffffa8004cf8170  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004541040       Image:         VPTray.exe
        Wait Start TickCount      3326           Ticks: 43253 (0:00:11:14.751)
        Context Switch Count      2                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3494f6
        Stack Init fffff98012eabdb0 Current fffff98012eab260
        Base fffff98012eac000 Limit fffff98012ea5000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`12eab2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12eab3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`12eab440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`12eab4b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`12eab960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`12eabbb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12eabc20)
        00000000`0265f0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`0265f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0265f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0265f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0265f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa8004ccebb0  Cid 04e8.0998  Teb: 000000007ef9e000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004d15040  NotificationEvent
            fffffa80048c5880  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004541040       Image:         VPTray.exe
        Wait Start TickCount      3351           Ticks: 43228 (0:00:11:14.361)
        Context Switch Count      2
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address 0x0000000073f717ae
        Stack Init fffff98012fcedb0 Current fffff98012fce260
        Base fffff98012fcf000 Limit fffff98012fc9000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`12fce2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12fce3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`12fce440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`12fce4b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`12fce960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`12fcebb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12fcec20)
        00000000`026df0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`026df1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`026df1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`026df730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`026df7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa8003dcf3f0  Cid 04e8.0a7c  Teb: 000000007efa4000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8003d59880  NotificationEvent
            fffffa8003fe4c30  NotificationEvent
            fffffa8003dcf4a8  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004541040       Image:         VPTray.exe
        Wait Start TickCount      45701          Ticks: 878 (0:00:00:13.696)
        Context Switch Count      13
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3494f6
        Stack Init fffff98012babdb0 Current fffff98012bab260
        Base fffff98012bac000 Limit fffff98012ba6000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`12bab2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12bab3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`12bab440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`12bab4b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`12bab960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`12babbb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12babc20)
        00000000`0261f0f8 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`0261f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0261f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0261f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0261f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa8003fe6060  Cid 04e8.0ae4  Teb: 000000007ef9b000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8003d93df0  NotificationEvent
            fffffa8003fe6118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004541040       Image:         VPTray.exe
        Wait Start TickCount      46577          Ticks: 2 (0:00:00:00.031)
        Context Switch Count      6699
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007c3494f6
        Stack Init fffff980159abdb0 Current fffff980159ab960
        Base fffff980159ac000 Limit fffff980159a6000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`159ab9a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`159abae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`159abb40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`159abbc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`159abc20 00000000`75103cf9 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`159abc20)
        00000000`0271f128 00000000`75103af6 wow64cpu!CpupSyscallStub+0x9
        00000000`0271f130 00000000`7511abfe wow64cpu!Thunk0ArgReloadState+0x1a
        00000000`0271f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0271f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0271f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0271f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa8003e0d060  Cid 04e8.04ac  Teb: 000000007ef95000 Win32Thread: fffff900c1f66ab0
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8004b4aa90  NotificationEvent
            fffffa8003e0d118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004541040       Image:         VPTray.exe
        Wait Start TickCount      46451          Ticks: 128 (0:00:00:01.996)
        Context Switch Count      1011                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address VPTray (0x0000000000410540)
        Stack Init fffff9800e5ecdb0 Current fffff9800e5ec960
        Base fffff9800e5ed000 Limit fffff9800e5e5000 Call 0
        Priority 13 BasePriority 8 PriorityDecrement 4 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0e5ec9a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e5ecae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0e5ecb40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`0e5ecbc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`0e5ecc20 00000000`75103cf9 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e5ecc20)
        00000000`029ef128 00000000`75103af6 wow64cpu!CpupSyscallStub+0x9
        00000000`029ef130 00000000`7511abfe wow64cpu!Thunk0ArgReloadState+0x1a
        00000000`029ef1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`029ef1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`029ef730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`029ef7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa8004242bb0  Cid 04e8.0dcc  Teb: 000000007efd8000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa80044a3d90  QueueObject
            fffffa8004242c68  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004541040       Image:         VPTray.exe
        Wait Start TickCount      46451          Ticks: 128 (0:00:00:01.996)
        Context Switch Count      139
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x00000000762f3242
        Stack Init fffff980108badb0 Current fffff980108ba810
        Base fffff980108bb000 Limit fffff980108b5000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`108ba850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`108ba990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`108ba9f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`108baa80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`108bab00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`108babb0 00000000`751039a2 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`108bac20)
        00000000`003ff0c8 00000000`7511abfe wow64cpu!RemoveIoCompletionFault+0x41
        00000000`003ff1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`003ff1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`003ff730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`003ff7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa8004919060  Cid 04e8.0d68  Teb: 000000007efd5000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa80044a3d90  QueueObject
            fffffa8004919118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8004541040       Image:         VPTray.exe
        Wait Start TickCount      45968          Ticks: 611 (0:00:00:09.531)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x00000000762f3242
        Stack Init fffff9800cc4cdb0 Current fffff9800cc4c810
        Base fffff9800cc4d000 Limit fffff9800cc47000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0cc4c850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0cc4c990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0cc4c9f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0cc4ca80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`0cc4cb00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`0cc4cbb0 00000000`751039a2 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0cc4cc20)
        00000000`0249f0c8 00000000`7511abfe wow64cpu!RemoveIoCompletionFault+0x41
        00000000`0249f1a0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0249f1d0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0249f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0249f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

Issch process

```
PROCESS fffffa8003a48040
    SessionId: 1  Cid: 0868    Peb: 7efdf000  ParentCid: 0bcc
    DirBase: 2ce44000  ObjectTable: fffff880008bb530  HandleCount:  21.
    Image: issch.exe
    VadRoot fffffa80049a4e50 Vads 44 Clone 0 Private 151. Modified 75. Locked 0.
    DeviceMap fffff88006100250
    Token                             fffff880028e9a10
    ElapsedTime                       00:11:15.033
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         90184
    QuotaPoolUsage[NonPagedPool]      4032
    Working Set Sizes (now,min,max)  (726, 50, 345) (2904KB, 200KB, 1380KB)
    PeakWorkingSetSize                804
    VirtualSize                       45 Mb
    PeakVirtualSize                   47 Mb
    PageFaultCount                    941
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      230

    Setting context for this process...
.process /p /r fffffa8003a48040

    !peb
PEB at 000000007efdf000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         0000000000400000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 0000000000312a10 . 0000000000312d70
    Ldr.InLoadOrderModuleList:           0000000000312920 . 0000000000312ed0
    Ldr.InMemoryOrderModuleList:         0000000000312930 . 0000000000312ee0
            Base TimeStamp                     Module
          400000 4106ce18 Jul 27 22:50:16 2004 C:\Program Files (x86)\Common
Files\InstallShield\UpdateService\issch.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        75110000 4549d371 Nov 02 11:16:01 2006 C:\Windows\system32\wow64.dll
        75000000 4549d374 Nov 02 11:16:04 2006 C:\Windows\system32\wow64win.dll
        75100000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\wow64cpu.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       0000000000310000
    ProcessParameters: 0000000000311e80
    WindowTitle:  'C:\Program Files (x86)\Common Files\InstallShield\UpdateService\issch.exe'
    ImageFile:    'C:\Program Files (x86)\Common Files\InstallShield\UpdateService\issch.exe'
    CommandLine:  '"C:\Program Files (x86)\Common Files\InstallShield\UpdateService\issch.exe" -
start'
    DllPath:      'C:\Program Files (x86)\Common
Files\InstallShield\UpdateService;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\sys
tem32;C:\Windows;C:\Windows\System32\Wbem'
    Environment:  0000000000311310
        =::=::\
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\UserName\AppData\Roaming
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        HOMEDRIVE=C:
        HOMEPATH=\Users\UserName
        LOCALAPPDATA=C:\Users\UserName\AppData\Local
        LOGONSERVER=\\COMPUTERNAME
```

```
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public
        SESSIONNAME=Console
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Users\UserName\AppData\Local\Temp
        TMP=C:\Users\UserName\AppData\Local\Temp
        USERDOMAIN=COMPUTERNAME
        USERNAME=UserName
        USERPROFILE=C:\Users\UserName
        windir=C:\Windows


        THREAD fffffa8003a47bb0  Cid 0868.09e8  Teb: 000000007efdb000 Win32Thread: fffff900c1e873e0
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa80038f03f0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8003a48040       Image:         issch.exe
        Wait Start TickCount      45713          Ticks: 866 (0:00:00:13.509)
        Context Switch Count      124                LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address issch (0x000000000040847d)
        Stack Init fffff9800dbb3db0 Current fffff9800dbb3740
        Base fffff9800dbb4000 Limit fffff9800dbac000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0dbb3780 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0dbb38c0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0dbb3920 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`0dbb39a0 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`0dbb3a40 fffff960`000c7e1e win32k!xxxSleepThread+0x56
        fffff980`0dbb3a70 fffff960`000c7f25 win32k!xxxRealInternalGetMessage+0x72e
        fffff980`0dbb3b50 fffff960`000c97e4 win32k!xxxInternalGetMessage+0x35
        fffff980`0dbb3b90 fffff800`01c4d733 win32k!NtUserGetMessage+0x64
        fffff980`0dbb3c20 00000000`75039f7a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0dbb3c20)
        00000000`0007e568 00000000`75023160 wow64win!ZwUserGetMessage+0xa
        00000000`0007e570 00000000`7511aa4e wow64win!whNtUserGetMessage+0x30
        00000000`0007e5d0 00000000`75103678 wow64!Wow64SystemServiceEx+0xca
        00000000`0007ee80 00000000`7511abfe wow64cpu!TurboDispatchJumpAddressEnd+0x28
        00000000`0007ef10 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0007ef40 00000000`76e0e23d wow64!Wow64LdrpInitialize+0x492
        00000000`0007f4a0 00000000`76e7e974 ntdll!LdrpInitializeProcess+0x1333
        00000000`0007f730 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d641
        00000000`0007f7d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

CLI process

```
PROCESS fffffa8003e0cb50
    SessionId: 1  Cid: 0b44    Peb: 7fffffdd000  ParentCid: 0ba4
    DirBase: 2c7d5000  ObjectTable: fffff880058b0300  HandleCount: 497.
    Image: CLI.exe
    VadRoot fffffa8003d92650 Vads 347 Clone 0 Private 4785. Modified 27335. Locked 1.
    DeviceMap fffff88006100250
    Token                             fffff8800290a060
    ElapsedTime                       00:11:14.127
    UserTime                          00:00:00.655
    KernelTime                        00:00:00.327
    QuotaPoolUsage[PagedPool]         419832
    QuotaPoolUsage[NonPagedPool]      47676
    Working Set Sizes (now,min,max)  (847, 50, 345) (3388KB, 200KB, 1380KB)
    PeakWorkingSetSize                10494
    VirtualSize                       621 Mb
    PeakVirtualSize                   631 Mb
    PageFaultCount                    105091
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      13351
    Job                               fffffa8004c32850

    Setting context for this process...
.process /p /r fffffa8003e0cb50

    !peb
PEB at 000007fffffdd000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         0000000010570000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00000000003f2900 . 00000000058be4b0
    Ldr.InLoadOrderModuleList:           00000000003f2810 . 00000000058be490
    Ldr.InMemoryOrderModuleList:         00000000003f2820 . 00000000058be4a0
            Base TimeStamp                     Module
        10570000 4433d218 Apr 05 15:20:08 2006 C:\Program Files\ATI Technologies\ATI.ACE\CLI.EXE
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
     6427ee50000 453712fa Oct 19 06:54:02 2006 C:\Windows\system32\mscoree.dll
        76bc0000 4549d328 Nov 02 11:14:48 2006 C:\Windows\system32\KERNEL32.dll
     7fefea30000 4549d267 Nov 02 11:11:35 2006 C:\Windows\system32\ADVAPI32.dll
     7fefed90000 469c43bb Jul 17 05:21:15 2007 C:\Windows\system32\RPCRT4.dll
     7fefda10000 4549d31f Nov 02 11:14:39 2006 C:\Windows\system32\SHLWAPI.dll
     7fefec20000 4549d273 Nov 02 11:11:47 2006 C:\Windows\system32\GDI32.dll
        76d00000 45d3ee19 Feb 15 05:22:33 2007 C:\Windows\system32\USER32.dll
     7fefdd40000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\system32\msvcrt.dll
     7fefd9e0000 4549d2cb Nov 02 11:13:15 2006 C:\Windows\system32\IMM32.DLL
     7fefdc30000 4549d2e6 Nov 02 11:13:42 2006 C:\Windows\system32\MSCTF.dll
     7feff0c0000 4549d2a1 Nov 02 11:12:33 2006 C:\Windows\system32\LPK.DLL
     7fefd940000 4549d337 Nov 02 11:15:03 2006 C:\Windows\system32\USP10.dll
     7fefbe70000 4549d32b Nov 02 11:14:51 2006 C:\Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_1559f1c6f365a7fa\comctl32.dll
     6427f330000 45371492 Oct 19 07:00:50 2006
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorwks.dll
        72170000 4536ee36 Oct 19 04:17:10 2006
C:\Windows\WinSxS\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.312_none_c905b7a4878399c1\MSV
CR80.dll
     7fefddf0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\shell32.dll
     7fefd760000 4549d317 Nov 02 11:14:31 2006 C:\Windows\system32\ole32.dll
     64278000000 4537154e Oct 19 07:03:58 2006
C:\Windows\assembly\NativeImages_v2.0.50727_64\mscorlib\c211d8638f8461ef03ab23671688fda7\mscorlib.n
i.dll
     7fefc330000 4549d33b Nov 02 11:15:07 2006 C:\Windows\system32\uxtheme.dll
```

```
     6427eed0000 45371528 Oct 19 07:03:20 2006
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorjit.dll
     64274880000 4536f31b Oct 19 04:38:03 2006
C:\Windows\assembly\NativeImages_v2.0.50727_64\System\72f2ba64b66428349d531c716015936e\System.ni.dl
l
     64275bc0000 4536f335 Oct 19 04:38:29 2006
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Drawing\0c51eaefe61bd045154a4a71b6921985\Syst
em.Drawing.ni.dll
     64275fa0000 4536f34f Oct 19 04:38:55 2006
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Windows.Forms\eb6e9e31d20fa25914584378d589e4a
c\System.Windows.Forms.ni.dll
     7fefc620000 4549d31d Nov 02 11:14:37 2006 C:\Windows\system32\rsaenh.dll
        73ff0000 453eba8c Oct 25 02:14:52 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Implementation.dll
        74000000 453eba85 Oct 25 02:14:45 2006 C:\Program Files\ATI
Technologies\ATI.ACE\LOG.Foundation.dll
        73aa0000 453eba88 Oct 25 02:14:48 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Foundation.dll
        73ad0000 453eba8d Oct 25 02:14:53 2006 C:\Program Files\ATI
Technologies\ATI.ACE\LOG.Foundation.Service.dll
        73ac0000 453eba8c Oct 25 02:14:52 2006 C:\Program Files\ATI
Technologies\ATI.ACE\LOG.Foundation.Shared.dll
     7fef75f0000 4549d31b Nov 02 11:14:35 2006 C:\Windows\system32\shfolder.dll
        73a80000 453eba8f Oct 25 02:14:55 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Foundation.XManifestation.dll
     64246f40000 4536f317 Oct 19 04:37:59 2006
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Xml\874dae5d812627145a41a14b122bb0ee\System.X
ml.ni.dll
     6424eee0000 4536f2f1 Oct 19 04:37:21 2006
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Runtime.Remo#\e0cc672a21d5ea9053256eb3e2e9e91
b\System.Runtime.Remoting.ni.dll
     7fefd540000 4549d38a Nov 02 11:16:26 2006 C:\Windows\system32\ws2_32.dll
     7feff0b0000 4549d370 Nov 02 11:16:00 2006 C:\Windows\system32\NSI.dll
     7fefc8f0000 4549d2e7 Nov 02 11:13:43 2006 C:\Windows\system32\mswsock.dll
     7fefc560000 4549d3a3 Nov 02 11:16:51 2006 C:\Windows\system32\wshtcpip.dll
     7fefc980000 4549d39d Nov 02 11:16:45 2006 C:\Windows\System32\wship6.dll
     64249120000 4536f318 Oct 19 04:38:00 2006
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Configuration\1b7409c5c3b532cc35f174a22dd45b8
4\System.Configuration.ni.dll
        732a0000 453eba8e Oct 25 02:14:54 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Component.Runtime.dll
        73a90000 453eba88 Oct 25 02:14:48 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Component.Runtime.Shared.dll
        73a70000 453eba8d Oct 25 02:14:53 2006 C:\Program Files\ATI
Technologies\ATI.ACE\ATICCCom.dll
        73a60000 453eba86 Oct 25 02:14:46 2006 C:\Program Files\ATI
Technologies\ATI.ACE\AEM.Foundation.dll
        73a50000 453eba8b Oct 25 02:14:51 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Caste.Graphics.Shared.dll
        73220000 453ebaa1 Oct 25 02:15:13 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Caste.Graphics.Runtime.dll
        73900000 453eba8b Oct 25 02:14:51 2006 C:\Program Files\ATI
Technologies\ATI.ACE\ACE.Graphics.DisplaysManager.Shared.dll
        73290000 453eba9c Oct 25 02:15:08 2006 C:\Program Files\ATI
Technologies\ATI.ACE\DEM.OS.I0602.dll
        73280000 453eba87 Oct 25 02:14:47 2006 C:\Program Files\ATI
Technologies\ATI.ACE\DEM.Foundation.dll
        73270000 453eba9f Oct 25 02:15:11 2006 C:\Program Files\ATI
Technologies\ATI.ACE\DEM.Graphics.I0601.dll
     642bc680000 46203b59 Apr 14 03:24:25 2007
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Web\c915380299000c3202f933a022f9c8d6\System.W
eb.ni.dll
        73260000 453eba9d Oct 25 02:15:09 2006 C:\Program Files\ATI Technologies\ATI.ACE\DEM.OS.dll
        73210000 453eba9e Oct 25 02:15:10 2006 C:\Program Files\ATI
Technologies\ATI.ACE\DEM.Graphics.dll
        731f0000 453eba9d Oct 25 02:15:09 2006 C:\Program Files\ATI
Technologies\ATI.ACE\ATIDEMOS.dll
     6424ea20000 4536f344 Oct 19 04:38:44 2006
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Management\b732bd782bd9d48633330d1ce07b14ad\S
ystem.Management.ni.dll
```

```
     7fefdb90000 4549d282 Nov 02 11:12:02 2006 C:\Windows\system32\CLBCatQ.DLL
     7fefdab0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\OLEAUT32.dll
     642fffd0000 4536f28b Oct 19 04:35:39 2006
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\WMINet_Utils.dll
     7fef96a0000 4549d3bd Nov 02 11:17:17 2006 C:\Windows\system32\wbem\wmiutils.dll
     7fef9f50000 4549d33d Nov 02 11:15:09 2006 C:\Windows\system32\wbem\wbemcomn.dll
     7fef9e20000 4549d342 Nov 02 11:15:14 2006 C:\Windows\system32\wbem\wbemprox.dll
     7fef96d0000 4549d343 Nov 02 11:15:15 2006 C:\Windows\system32\wbem\wbemsvc.dll
     7fef9040000 4549d274 Nov 02 11:11:48 2006 C:\Windows\system32\wbem\fastprox.dll
     7fefcdd0000 4549d375 Nov 02 11:16:05 2006 C:\Windows\system32\NTDSAPI.dll
     7fefce40000 4549d288 Nov 02 11:12:08 2006 C:\Windows\system32\DNSAPI.dll
     7fefd590000 4549d396 Nov 02 11:16:38 2006 C:\Windows\system32\WLDAP32.dll
     7fefd530000 4549d310 Nov 02 11:14:24 2006 C:\Windows\system32\PSAPI.DLL
     7fefcf70000 4549d2fc Nov 02 11:14:04 2006 C:\Windows\system32\NETAPI32.dll
     7fefd390000 4549d33f Nov 02 11:15:11 2006 C:\Windows\system32\Secur32.dll
        73140000 453ebda0 Oct 25 02:28:00 2006 C:\Program Files\ATI
Technologies\ATI.ACE\ATIDEMGX.dll
     7fefeed0000 4549d318 Nov 02 11:14:32 2006 C:\Windows\system32\setupapi.dll
     7fefb8f0000 4549d276 Nov 02 11:11:50 2006 C:\Windows\system32\cfgmgr32.dll
        10000000 453ec159 Oct 25 02:43:53 2006 C:\Windows\system32\atipdl64.dll
        731d0000 453eba9f Oct 25 02:15:11 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DisplaysColour2.Graphics.Shared.dll
        731b0000 453ebcc7 Oct 25 02:24:23 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.Radeon3D.Graphics.Runtime.dll
        731a0000 453ebb05 Oct 25 02:16:53 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Caste.Graphics.Runtime.Shared.dll
        73190000 453ebcc6 Oct 25 02:24:22 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.Radeon3D.Graphics.Shared.dll
        73130000 453ebb3c Oct 25 02:17:48 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DisplaysColour2.Graphics.Runtime.dll
        73120000 453ebc00 Oct 25 02:21:04 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.MMVideo.Graphics.Runtime.dll
        73110000 453ebbff Oct 25 02:21:03 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.MMVideo.Graphics.Shared.dll
        73100000 453ebbff Oct 25 02:21:03 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DeviceCRT.Graphics.Runtime.dll
        730f0000 453ebbef Oct 25 02:20:47 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DeviceCRT.Graphics.Shared.dll
        730e0000 453ebc2d Oct 25 02:21:49 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DeviceCRT2.Graphics.Runtime.dll
        730d0000 453ebc1f Oct 25 02:21:35 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DeviceCRT2.Graphics.Shared.dll
        730c0000 453ebc88 Oct 25 02:23:20 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DeviceLCD.Graphics.Runtime.dll
        730b0000 453ebaca Oct 25 02:15:54 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DeviceLCD.Graphics.Shared.dll
        730a0000 453ebcf8 Oct 25 02:25:12 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DeviceLCD2.Graphics.Runtime.dll
        73090000 453ebac9 Oct 25 02:15:53 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DeviceLCD2.Graphics.Shared.dll
        73070000 453ebcb3 Oct 25 02:24:03 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DeviceCV.Graphics.Runtime.dll
        73060000 453ebcb2 Oct 25 02:24:02 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DeviceCV.Graphics.Shared.dll
        73050000 453ebbdd Oct 25 02:20:29 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.CustomFormats.Graphics.Shared.dll
        73030000 453ebcd8 Oct 25 02:24:40 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DeviceCV2.Graphics.Runtime.dll
        73020000 453ebcd7 Oct 25 02:24:39 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DeviceCV2.Graphics.Shared.dll
        73000000 453ebd18 Oct 25 02:25:44 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DeviceTV2.Graphics.Runtime.dll
        72fe0000 453ebd64 Oct 25 02:27:00 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DeviceTV.Graphics.Runtime.dll
        72fd0000 453ebbef Oct 25 02:20:47 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DeviceDFP.Graphics.Runtime.dll
        72fc0000 453ebbe0 Oct 25 02:20:32 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DeviceDFP.Graphics.Shared.dll
        72fb0000 453ebc5b Oct 25 02:22:35 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DeviceDFP2.Graphics.Runtime.dll
```

```
        72fa0000 453ebc4d Oct 25 02:22:21 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DeviceDFP2.Graphics.Shared.dll
        72f80000 453ebba1 Oct 25 02:19:29 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.OverDrive3.Graphics.Runtime.dll
        72f70000 453ebba0 Oct 25 02:19:28 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.OverDrive3.Graphics.Shared.dll
        72f60000 453ebb84 Oct 25 02:19:00 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.OverDrive2.Graphics.Runtime.dll
        72f50000 453ebda5 Oct 25 02:28:05 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.PowerPlayDPPE.Graphics.Runtime.dll
        72f40000 453ebd4e Oct 25 02:26:38 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.PowerPlayDPPE.Graphics.Shared.dll
        72f30000 453ebca2 Oct 25 02:23:46 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.PowerPlay3.Graphics.Runtime.dll
        72f20000 453ebc94 Oct 25 02:23:32 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.PowerPlay3.Graphics.Shared.dll
        72f10000 453ebc5d Oct 25 02:22:37 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DisplaysOptions.Graphics.Runtime.dll
        72f00000 453ebb13 Oct 25 02:17:07 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.InfoCentre.Graphics.Runtime.dll
        72ef0000 453ebb13 Oct 25 02:17:07 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.InfoCentre.Graphics.Shared.dll
        72ee0000 453ebacb Oct 25 02:15:55 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.HotkeysHandling.Graphics.Runtime.dll
        72ed0000 453ebaa0 Oct 25 02:15:12 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.HotkeysHandling.Graphics.Shared.dll
        72ec0000 453ebaca Oct 25 02:15:54 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DeviceProperty.Graphics.Shared.dll
        72eb0000 453ebac9 Oct 25 02:15:53 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DeviceProperty2.Graphics.Shared.dll
        72ea0000 453ebc12 Oct 25 02:21:22 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DeviceProperty2.Graphics.Runtime.dll
        72e80000 453ebd17 Oct 25 02:25:43 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DeviceTV2.Graphics.Shared.dll
        72e60000 453ebd63 Oct 25 02:26:59 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DeviceTV.Graphics.Shared.dll
        72e50000 453ebb84 Oct 25 02:19:00 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.OverDrive2.Graphics.Shared.dll
     7fefb610000 4549d245 Nov 02 11:11:01 2006
C:\Windows\WinSxS\amd64_microsoft.windows.gdiplus_6595b64144ccf1df_1.0.6000.16386_none_56f375c7b4f2
4821\gdiplus.dll
        72e40000 453ebc5c Oct 25 02:22:36 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DisplaysOptions.Graphics.Shared.dll
     7fefc580000 4549d351 Nov 02 11:15:29 2006 C:\Windows\system32\powrprof.dll
        72e30000 453eba87 Oct 25 02:14:47 2006 C:\Program Files\ATI
Technologies\ATI.ACE\APM.Foundation.dll
     7fefb4d0000 4549d30d Nov 02 11:14:21 2006 C:\Windows\system32\PROPSYS.dll
     7fefd310000 4549d247 Nov 02 11:11:03 2006 C:\Windows\system32\apphelp.dll
     7fef5880000 470c5d32 Oct 10 06:03:46 2007 C:\Windows\system32\ieframe.dll
     7fefebc0000 4549d29c Nov 02 11:12:28 2006 C:\Windows\system32\iertutil.dll
     7fefd3b0000 4549d336 Nov 02 11:15:02 2006 C:\Windows\system32\USERENV.dll
     7fefd5f0000 470c5dac Oct 10 06:05:48 2007 C:\Windows\system32\urlmon.dll
       516f00000 4536ffb5 Oct 19 05:31:49 2006
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\diasymreader.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       00000000003f0000
    ProcessParameters: 00000000003f1e80
    WindowTitle:  'C:\Program Files\ATI Technologies\ATI.ACE\CLI.EXE'
    ImageFile:    'C:\Program Files\ATI Technologies\ATI.ACE\CLI.EXE'
    CommandLine:  'CLI.EXE Runtime'
    DllPath:      'C:\Program Files\ATI
Technologies\ATI.ACE;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Wind
ows;C:\Windows\System32\Wbem'
    Environment:  00000000003f1310
        =::=::\
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\UserName\AppData\Roaming
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
```

```
ComSpec=C:\Windows\system32\cmd.exe
FP_NO_HOST_CHECK=NO
HOMEDRIVE=C:
HOMEPATH=\Users\UserName
LOCALAPPDATA=C:\Users\UserName\AppData\Local
LOGONSERVER=\\COMPUTERNAME
NUMBER_OF_PROCESSORS=2
OS=Windows_NT
Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE=AMD64
PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=0f02
ProgramData=C:\ProgramData
ProgramFiles=C:\Program Files
ProgramFiles(x86)=C:\Program Files (x86)
PUBLIC=C:\Users\Public
SESSIONNAME=Console
SystemDrive=C:
SystemRoot=C:\Windows
TEMP=C:\Users\UserName\AppData\Local\Temp
TMP=C:\Users\UserName\AppData\Local\Temp
USERDOMAIN=COMPUTERNAME
USERNAME=UserName
USERPROFILE=C:\Users\UserName
windir=C:\Windows
```

```
        THREAD fffffa80039a9bb0  Cid 0b44.0b40  Teb: 000007fffffde000 Win32Thread: fffff900c1c05010
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa8004abd590  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8003e0cb50       Image:         CLI.exe
        Wait Start TickCount      27056          Ticks: 19523 (0:00:05:04.560)
        Context Switch Count      8978                 LargeStack
        UserTime                  00:00:03.697
        KernelTime                00:00:01.045
        Win32 Start Address CLI (0x000000001057286e)
        Stack Init fffff9801569fdb0 Current fffff9801569f8c0
        Base fffff980156a0000 Limit fffff98015697000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1569f900 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1569fa40 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`1569faa0 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`1569fb20 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`1569fbc0 fffff960`000dc057 win32k!xxxSleepThread+0x56
        fffff980`1569fbf0 fffff800`01c4d733 win32k!NtUserWaitMessage+0x37
        fffff980`1569fc20 00000000`76d1df2a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1569fc20)
        00000000`0029db78 00000642`7f66bf32 USER32!ZwUserWaitMessage+0xa
        00000000`0029db80 00000642`75fada2a mscorwks!DoNDirectCallWorker+0x62
        00000000`0029dc10 00000000`105f9948 System_Windows_Forms_ni+0xda2a
        00000000`0029dc18 00000000`0029dc60 0x105f9948
        00000000`0029dc20 00000000`00000000 0x29dc60
        00000000`0029dc28 00000000`00000000 0x0
        00000000`0029dc30 00000000`00000000 0x0
        00000000`0029dc38 00000000`00437860 0x0
        00000000`0029dc40 00000000`0029dc10 0x437860
        00000000`0029dc48 00000000`00000000 0x29dc10
        00000000`0029dc50 00000000`00000000 0x0
        00000000`0029dc58 00000095`0000000b 0x0
        00000000`0029dc60 00000000`00000000 0x95`0000000b
        00000000`0029dc68 00000000`00000000 0x0
        00000000`0029dc70 00000000`00000000 0x0
        00000000`0029dc78 00000000`00000000 0x0
        00000000`0029dc80 00000000`00000000 0x0
        00000000`0029dc88 00000000`00000000 0x0
        00000000`0029dc90 00006265`27321646 0x0
        00000000`0029dc98 00000000`00000000 0x6265`27321646
        00000000`0029dca0 00000000`01000000 0x0
        00000000`0029dca8 00000642`7f3d2550 0x1000000
        00000000`0029dcb0 00000000`0029e7c8 mscorwks!NDirectMethodFrameStandalone::`vftable'
        00000000`0029dcb8 00000000`0029dc10 0x29e7c8
        00000000`0029dcc0 00000000`105f9948 0x29dc10
        00000000`0029dcc8 00000000`10887c01 0x105f9948
        00000000`0029dcd0 00000000`00000000 0x10887c01
        00000000`0029dcd8 00000000`0029dc40 0x0
        00000000`0029dce0 00000000`0029dcc0 0x29dc40
        00000000`0029dce8 00000000`00000001 0x29dcc0
        00000000`0029dcf0 00000000`00000000 0x1
        00000000`0029dcf8 00000000`00000000 0x0
        00000000`0029dd00 00000642`76c1b3b0 0x0
```

```
        THREAD fffffa8004c1c630  Cid 0b44.097c  Teb: 000007fffffdb000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80048661c0  SynchronizationEvent
            fffffa80043df610  SynchronizationEvent
            fffffa8004828f70  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8003e0cb50       Image:         CLI.exe
        Wait Start TickCount      3877           Ticks: 42702 (0:00:11:06.155)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address mscorwks!DebuggerRCThread::ThreadProcStatic (0x000006427f45e464)
        Stack Init fffff98012feadb0 Current fffff98012fea260
        Base fffff98012feb000 Limit fffff98012fe5000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`12fea2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12fea3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`12fea440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`12fea4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`12fea960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`12feabb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12feac20)
        00000000`0273f778 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0273f780 00000000`76bfedf1 KERNEL32!WaitForMultipleObjectsEx+0x10b
        00000000`0273f890 00000642`7f60634e KERNEL32!WaitForMultipleObjects+0x11
        00000000`0273f8d0 00000642`7f45e626 mscorwks!DebuggerRCThread::MainLoop+0xb6
        00000000`0273f980 00000642`7f45e4b8 mscorwks!DebuggerRCThread::ThreadProc+0xf2
        00000000`0273f9e0 00000000`76bfcdcd mscorwks!DebuggerRCThread::ThreadProcStatic+0x54
        00000000`0273fa30 00000000`76e1c6e1 KERNEL32!BaseThreadInitThunk+0xd
        00000000`0273fa60 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004607060  Cid 0b44.02c0  Teb: 000007fffffd9000 Win32Thread: fffff900c06dad60
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800189bd80  NotificationEvent
            fffffa8004cde670  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8003e0cb50       Image:         CLI.exe
        Wait Start TickCount      43237          Ticks: 3342 (0:00:00:52.135)
        Context Switch Count      323                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address mscorwks!Thread::intermediateThreadProc (0x000006427f5e3718)
        Stack Init fffff98015783db0 Current fffff98015783260
        Base fffff98015784000 Limit fffff9801577d000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`157832a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`157833e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`15783440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`157834b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`15783960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`15783bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`15783c20)
        00000000`0313f568 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0313f570 00000000`76bfedf1 KERNEL32!WaitForMultipleObjectsEx+0x10b
        00000000`0313f680 00000642`7f5fc463 KERNEL32!WaitForMultipleObjects+0x11
        00000000`0313f6c0 00000642`7f47aeba mscorwks!WKS::WaitForFinalizerEvent+0x93
        00000000`0313f6f0 00000642`7f585a1c mscorwks!WKS::GCHeap::FinalizerThreadWorker+0x5a
        00000000`0313f730 00000642`7f58585d mscorwks!ThreadpoolMgr::FlushQueueOfTimerInfos+0x298
        00000000`0313f840 00000642`7f44fdd6 mscorwks!ThreadpoolMgr::FlushQueueOfTimerInfos+0xd9
        00000000`0313f880 00000642`7f475684 mscorwks!ManagedThreadBase_NoADTransition+0x42
        00000000`0313f8e0 00000642`7f5e3790 mscorwks!WKS::GCHeap::FinalizerThreadStart+0x74
        00000000`0313f920 00000000`76bfcdcd mscorwks!Thread::intermediateThreadProc+0x78
        00000000`0313f9f0 00000000`76e1c6e1 KERNEL32!BaseThreadInitThunk+0xd
        00000000`0313fa20 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004884bb0  Cid 0b44.0820  Teb: 000007fffffd7000 Win32Thread: fffff900c06e0d60
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8004c83fb0  QueueObject
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8003e0cb50       Image:         CLI.exe
        Wait Start TickCount      29245          Ticks: 17334 (0:00:04:30.412)
        Context Switch Count      804                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff98012e85db0 Current fffff98012e85810
        Base fffff98012e86000 Limit fffff98012e7f000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`12e85850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12e85990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`12e859f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`12e85a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`12e85b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`12e85bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12e85c20)
        00000000`03d7fba8 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`03d7fbb0 000007fe`fedce7a3 KERNEL32!GetQueuedCompletionStatus+0x48
        00000000`03d7fc10 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`03d7fca0 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`03d7fd50 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`03d7fd80 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`03d7fdc0 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`03d7fdf0 00000000`76e1c6e1 KERNEL32!BaseThreadInitThunk+0xd
        00000000`03d7fe20 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004c67060  Cid 0b44.0834  Teb: 000007fffffd3000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa800486f240  SynchronizationEvent
            fffffa8004c67118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8003e0cb50       Image:         CLI.exe
        Wait Start TickCount      46518          Ticks: 61 (0:00:00:00.951)
        Context Switch Count      235
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address mscorwks!ThreadpoolMgr::WaitThreadStart (0x000006427fabbb10)
        Stack Init fffff980157eddb0 Current fffff980157ed260
        Base fffff980157ee000 Limit fffff980157e8000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`157ed2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`157ed3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`157ed440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`157ed4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`157ed960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`157edbb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`157edc20)
        00000000`0482f768 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0482f770 00000642`7fabbbce KERNEL32!WaitForMultipleObjectsEx+0x10b
        00000000`0482f880 00000000`76bfcdcd mscorwks!ThreadpoolMgr::WaitThreadStart+0xbe
        00000000`0482f910 00000000`76e1c6e1 KERNEL32!BaseThreadInitThunk+0xd
        00000000`0482f940 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8003d54bb0  Cid 0b44.0658  Teb: 000007fffff0e000 Win32Thread: 0000000000000000
WAIT: (DelayExecution) UserMode Alertable
            fffffa8003d54c68  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8003e0cb50       Image:         CLI.exe
        Wait Start TickCount      46514          Ticks: 65 (0:00:00:01.014)
        Context Switch Count      236
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address mscorwks!Thread::intermediateThreadProc (0x000006427f5e3718)
        Stack Init fffff9800e2ebdb0 Current fffff9800e2eb990
        Base fffff9800e2ec000 Limit fffff9800e2e6000 Call 0
        Priority 7 BasePriority 7 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0e2eb9d0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e2ebb10 fffff800`01c5b5a9 nt!KiSwapThread+0x125
        fffff980`0e2ebb70 fffff800`01e8ae9d nt!KeDelayExecutionThread+0x339
        fffff980`0e2ebbf0 fffff800`01c4d733 nt!NtDelayExecution+0x5c
        fffff980`0e2ebc20 00000000`76e205ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e2ebc20)
        00000000`0462eea8 00000000`76bfd908 ntdll!NtDelayExecution+0xa
        00000000`0462eeb0 00000642`7f57bab9 KERNEL32!SleepEx+0x84
        00000000`0462ef30 00000642`7f4d8185 mscorwks!CExecutionEngine::ClrSleepEx+0x35
        00000000`0462efb0 00000642`7f4c7e86 mscorwks!Thread::UserSleep+0x79
        00000000`0462f010 00000642`8015ac1b mscorwks!ThreadNative::Sleep+0x116
        00000000`0462f1c0 00000000`00002710 0x642`8015ac1b
        00000000`0462f1c8 00000000`00032000 0x2710
        00000000`0462f1d0 00000000`0462e628 0x32000
        00000000`0462f1d8 00000000`0462e6a0 0x462e628
        00000000`0462f1e0 00000000`0462f1c0 0x462e6a0
        00000000`0462f1e8 00000000`0000bacc 0x462f1c0
        00000000`0462f1f0 00000000`0000bacc 0xbacc
        00000000`0462f1f8 00000000`10632e40 0xbacc
        00000000`0462f200 00000000`00000001 0x10632e40
        00000000`0462f208 00000000`105c2300 0x1
        00000000`0462f210 00000000`00000000 0x105c2300
        00000000`0462f218 00000000`10632e40 0x0
        00000000`0462f220 00000000`10632ea8 0x10632e40
        00000000`0462f228 00000642`782e7f1e 0x10632ea8
        00000000`0462f230 00000000`1058a1d8 mscorlib_ni+0x2e7f1e
        00000000`0462f238 00000000`10632d98 0x1058a1d8
        00000000`0462f240 00000000`10632e40 0x10632d98
        00000000`0462f248 0000018b`0080000f 0x10632e40
        00000000`0462f250 00000000`00000000 0x18b`0080000f
        00000000`0462f258 00000000`10632ea8 0x0
        00000000`0462f260 00000000`0462f460 0x10632ea8
        00000000`0462f268 00000000`0462f2a0 0x462f460
        00000000`0462f270 00000000`10632e40 0x462f2a0
        00000000`0462f278 00000642`782eb76f 0x10632e40
        00000000`0462f280 00000642`80012020 mscorlib_ni+0x2eb76f
        00000000`0462f288 00000000`00000165 0x642`80012020
        00000000`0462f290 00000000`00000000 0x165
        00000000`0462f298 00000000`0462f300 0x0
        00000000`0462f2a0 00000000`0462f280 0x462f300
        00000000`0462f2a8 00000000`00000000 0x462f280
```

```
        THREAD fffffa80042ca060  Cid 0b44.0ad8  Teb: 000007fffff0a000 Win32Thread: 0000000000000000
WAIT: (DelayExecution) UserMode Non-Alertable
            fffffa80042ca118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8003e0cb50       Image:         CLI.exe
        Wait Start TickCount      46571          Ticks: 8 (0:00:00:00.124)
        Context Switch Count      1424
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address mscorwks!ThreadpoolMgr::GateThreadStart (0x000006427f4aed08)
        Stack Init fffff9800f2b6db0 Current fffff9800f2b6990
        Base fffff9800f2b7000 Limit fffff9800f2b1000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0f2b69d0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0f2b6b10 fffff800`01c5b5a9 nt!KiSwapThread+0x125
        fffff980`0f2b6b70 fffff800`01e8ae9d nt!KeDelayExecutionThread+0x339
        fffff980`0f2b6bf0 fffff800`01c4d733 nt!NtDelayExecution+0x5c
        fffff980`0f2b6c20 00000000`76e205ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0f2b6c20)
        00000000`04ecf8d8 00000000`76bfd908 ntdll!NtDelayExecution+0xa
        00000000`04ecf8e0 00000642`7f47ad61 KERNEL32!SleepEx+0x84
        00000000`04ecf960 00000642`7f59f8dd mscorwks!EESleepEx+0x31
        00000000`04ecf9e0 00000642`7f4aedcb mscorwks!__DangerousSwitchToThread+0x9d
        00000000`04ecfa30 00000000`76bfcdcd mscorwks!ThreadpoolMgr::GateThreadStart+0xc3
        00000000`04ecfb60 00000000`76e1c6e1 KERNEL32!BaseThreadInitThunk+0xd
        00000000`04ecfb90 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004d14bb0  Cid 0b44.0bc0  Teb: 000007fffff06000 Win32Thread: fffff900c1f8c460
WAIT: (UserRequest) UserMode Alertable
            fffffa800462bbf0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8003e0cb50       Image:         CLI.exe
        Wait Start TickCount      5166           Ticks: 41413 (0:00:10:46.046)
        Context Switch Count      352                 LargeStack
        UserTime                  00:00:00.015
        KernelTime                00:00:00.015
        Win32 Start Address mscorwks!Thread::intermediateThreadProc (0x000006427f5e3718)
        Stack Init fffff9801597cdb0 Current fffff9801597c260
        Base fffff9801597d000 Limit fffff98015976000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1597c2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1597c3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`1597c440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`1597c4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`1597c960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`1597cbb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1597cc20)
        00000000`0518ec48 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0518ec50 00000642`7f4a06c5 KERNEL32!WaitForMultipleObjectsEx+0x10b
        00000000`0518ed60 00000642`7f4a30d9 mscorwks!WaitForMultipleObjectsEx_SO_TOLERANT+0xc1
        00000000`0518ee00 00000642`7f4ef6dd mscorwks!Thread::DoAppropriateAptStateWait+0x41
        00000000`0518ee60 00000642`7f4bca30 mscorwks!Thread::DoAppropriateWaitWorker+0x195
        00000000`0518ef60 00000642`7f46846f mscorwks!Thread::DoAppropriateWait+0x5c
        00000000`0518efd0 00000642`782f181f mscorwks!WaitHandleNative::CorWaitOneNative+0x19f
        00000000`0518f210 00000000`001a0018 mscorlib_ni+0x2f181f
        00000000`0518f218 00000000`ffffffff 0x1a0018
        00000000`0518f220 00000000`0518f200 0xffffffff
        00000000`0518f228 00000000`00000000 0x518f200
        00000000`0518f230 00000000`105c3338 0x0
        00000000`0518f238 00000000`105c3338 0x105c3338
        00000000`0518f240 00000000`205967f0 0x105c3338
        00000000`0518f248 00000642`4ea23989 0x205967f0
        00000000`0518f250 00000000`0518f728 System_Management_ni+0x3989
        00000000`0518f258 00000000`0518f2b0 0x518f728
        00000000`0518f260 00000000`105c3338 0x518f2b0
        00000000`0518f268 00000000`00000000 0x105c3338
        00000000`0518f270 00000000`0518f250 0x0
        00000000`0518f278 00000000`00000000 0x518f250
        00000000`0518f280 00000000`00000000 0x0
        00000000`0518f288 00000000`205967f0 0x0
        00000000`0518f290 00000000`105c2300 0x205967f0
        00000000`0518f298 00000000`106c29f0 0x105c2300
        00000000`0518f2a0 00000000`106c2a58 0x106c29f0
        00000000`0518f2a8 00000642`782e7f1e 0x106c2a58
        00000000`0518f2b0 00000000`106c2948 mscorlib_ni+0x2e7f1e
        00000000`0518f2b8 00000000`106c2948 0x106c2948
        00000000`0518f2c0 00000000`106c29f0 0x106c2948
        00000000`0518f2c8 00000037`02781318 0x106c29f0
        00000000`0518f2d0 00000000`00000000 0x37`02781318
        00000000`0518f2d8 00000000`106c2a58 0x0
        00000000`0518f2e0 00000000`0518f4e0 0x106c2a58
```

```
        THREAD fffffa800462e060  Cid 0b44.0200  Teb: 000007fffff00000 Win32Thread: fffff900c1e73460
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8003d8b950  NotificationEvent
            fffffa80048f7ae0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8003e0cb50       Image:         CLI.exe
        Wait Start TickCount      15651          Ticks: 30928 (0:00:08:02.479)
        Context Switch Count      55                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address gdiplus!BackgroundThreadProc (0x000007fefb672410)
        Stack Init fffff9800bbc6db0 Current fffff9800bbc6260
        Base fffff9800bbc7000 Limit fffff9800bbbf000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0bbc62a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0bbc63e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0bbc6440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0bbc64b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0bbc6960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0bbc6bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0bbc6c20)
        00000000`05fef688 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`05fef690 00000000`76d1e96d KERNEL32!WaitForMultipleObjectsEx+0x10b
        00000000`05fef7a0 00000000`76d1e85e USER32!RealMsgWaitForMultipleObjectsEx+0x129
        00000000`05fef840 00000000`76d13680 USER32!MsgWaitForMultipleObjectsEx+0x46
        00000000`05fef880 000007fe`fb672478 USER32!MsgWaitForMultipleObjects+0x20
        00000000`05fef8c0 00000000`76bfcdcd gdiplus!BackgroundThreadProc+0x68
        00000000`05fef930 00000000`76e1c6e1 KERNEL32!BaseThreadInitThunk+0xd
        00000000`05fef960 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8002b33bb0  Cid 0b44.04f4  Teb: 000007fffff0c000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa800483b460  QueueObject
            fffffa8002b33c68  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8003e0cb50       Image:         CLI.exe
        Wait Start TickCount      46518          Ticks: 61 (0:00:00:00.951)
        Context Switch Count      13
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address mscorwks!Thread::intermediateThreadProc (0x000006427f5e3718)
        Stack Init fffff980159eadb0 Current fffff980159ea810
        Base fffff980159eb000 Limit fffff980159e5000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`159ea850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`159ea990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`159ea9f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`159eaa80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`159eab00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`159eabb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`159eac20)
        00000000`0503f8b8 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`0503f8c0 00000642`7f45557f KERNEL32!GetQueuedCompletionStatus+0x48
        00000000`0503f920 00000642`7f5e3790 mscorwks!ThreadpoolMgr::CompletionPortThreadStart+0xbf
        00000000`0503f9c0 00000000`76bfcdcd mscorwks!Thread::intermediateThreadProc+0x78
        00000000`0503fe90 00000000`76e1c6e1 KERNEL32!BaseThreadInitThunk+0xd
        00000000`0503fec0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800254e700  Cid 0b44.039c  Teb: 000007fffffd5000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa800483b460  QueueObject
            fffffa800254e7b8  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa8003e0cb50       Image:         CLI.exe
        Wait Start TickCount      46518          Ticks: 61 (0:00:00:00.951)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address mscorwks!Thread::intermediateThreadProc (0x000006427f5e3718)
        Stack Init fffff9801a6a6db0 Current fffff9801a6a6810
        Base fffff9801a6a7000 Limit fffff9801a6a1000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1a6a6850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1a6a6990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`1a6a69f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`1a6a6a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`1a6a6b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`1a6a6bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1a6a6c20)
        00000000`05e6f8a8 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`05e6f8b0 00000642`7f45557f KERNEL32!GetQueuedCompletionStatus+0x48
        00000000`05e6f910 00000642`7f5e3790 mscorwks!ThreadpoolMgr::CompletionPortThreadStart+0xbf
        00000000`05e6f9b0 00000000`76bfcdcd mscorwks!Thread::intermediateThreadProc+0x78
        00000000`05e6ff00 00000000`76e1c6e1 KERNEL32!BaseThreadInitThunk+0xd
        00000000`05e6ff30 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

CLI process (second)

```
PROCESS fffffa800499dc10
    SessionId: 1  Cid: 0a34    Peb: 7fffffd3000  ParentCid: 0b44
    DirBase: 07b83000  ObjectTable: fffff880025e54d0  HandleCount: 329.
    Image: CLI.exe
    VadRoot fffffa8004cf82a0 Vads 228 Clone 0 Private 3196. Modified 16226. Locked 1.
    DeviceMap fffff88006100250
    Token                             fffff88002859060
    ElapsedTime                       00:10:40.468
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.015
    QuotaPoolUsage[PagedPool]         372816
    QuotaPoolUsage[NonPagedPool]      36252
    Working Set Sizes (now,min,max)  (489, 50, 345) (1956KB, 200KB, 1380KB)
    PeakWorkingSetSize                9973
    VirtualSize                       601 Mb
    PeakVirtualSize                   603 Mb
    PageFaultCount                    54053
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      11487
    Job                               fffffa8004c32850

    Setting context for this process...
.process /p /r fffffa800499dc10

    !peb
PEB at 000007fffffd3000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         0000000010570000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 0000000000342860 . 00000000041e1ec0
    Ldr.InLoadOrderModuleList:           0000000000342770 . 00000000041e1ea0
    Ldr.InMemoryOrderModuleList:         0000000000342780 . 00000000041e1eb0
            Base TimeStamp                     Module
        10570000 4433d218 Apr 05 15:20:08 2006 C:\Program Files\ATI Technologies\ATI.ACE\CLI.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
     6427ee50000 453712fa Oct 19 06:54:02 2006 C:\Windows\system32\mscoree.dll
        76bc0000 4549d328 Nov 02 11:14:48 2006 C:\Windows\system32\KERNEL32.dll
     7fefea30000 4549d267 Nov 02 11:11:35 2006 C:\Windows\system32\ADVAPI32.dll
     7fefed90000 469c43bb Jul 17 05:21:15 2007 C:\Windows\system32\RPCRT4.dll
     7fefda10000 4549d31f Nov 02 11:14:39 2006 C:\Windows\system32\SHLWAPI.dll
     7fefec20000 4549d273 Nov 02 11:11:47 2006 C:\Windows\system32\GDI32.dll
        76d00000 45d3ee19 Feb 15 05:22:33 2007 C:\Windows\system32\USER32.dll
     7fefdd40000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\system32\msvcrt.dll
     7fefd9e0000 4549d2cb Nov 02 11:13:15 2006 C:\Windows\system32\IMM32.DLL
     7fefdc30000 4549d2e6 Nov 02 11:13:42 2006 C:\Windows\system32\MSCTF.dll
     7feff0c0000 4549d2a1 Nov 02 11:12:33 2006 C:\Windows\system32\LPK.DLL
     7fefd940000 4549d337 Nov 02 11:15:03 2006 C:\Windows\system32\USP10.dll
     7fefbe70000 4549d32b Nov 02 11:14:51 2006 C:\Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_1559f1c6f365a7fa\comctl32.dll
     6427f330000 45371492 Oct 19 07:00:50 2006
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorwks.dll
        72170000 4536ee36 Oct 19 04:17:10 2006
C:\Windows\WinSxS\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.312_none_c905b7a4878399c1\MSV
CR80.dll
     7fefddf0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\shell32.dll
     7fefd760000 4549d317 Nov 02 11:14:31 2006 C:\Windows\system32\ole32.dll
     64278000000 4537154e Oct 19 07:03:58 2006
C:\Windows\assembly\NativeImages_v2.0.50727_64\mscorlib\c211d8638f8461ef03ab23671688fda7\mscorlib.n
i.dll
     7fefc330000 4549d33b Nov 02 11:15:07 2006 C:\Windows\system32\uxtheme.dll
     6427eed0000 45371528 Oct 19 07:03:20 2006
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorjit.dll
```

```
     64274880000 4536f31b Oct 19 04:38:03 2006
C:\Windows\assembly\NativeImages_v2.0.50727_64\System\72f2ba64b66428349d531c716015936e\System.ni.dl
l
     64275bc0000 4536f335 Oct 19 04:38:29 2006
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Drawing\0c51eaefe61bd045154a4a71b6921985\Syst
em.Drawing.ni.dll
     64275fa0000 4536f34f Oct 19 04:38:55 2006
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Windows.Forms\eb6e9e31d20fa25914584378d589e4a
c\System.Windows.Forms.ni.dll
     7fefc620000 4549d31d Nov 02 11:14:37 2006 C:\Windows\system32\rsaenh.dll
        73ff0000 453eba8c Oct 25 02:14:52 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Implementation.dll
        74000000 453eba85 Oct 25 02:14:45 2006 C:\Program Files\ATI
Technologies\ATI.ACE\LOG.Foundation.dll
        73aa0000 453eba88 Oct 25 02:14:48 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Foundation.dll
        73ad0000 453eba8d Oct 25 02:14:53 2006 C:\Program Files\ATI
Technologies\ATI.ACE\LOG.Foundation.Service.dll
        73ac0000 453eba8c Oct 25 02:14:52 2006 C:\Program Files\ATI
Technologies\ATI.ACE\LOG.Foundation.Shared.dll
     7fef75f0000 4549d31b Nov 02 11:14:35 2006 C:\Windows\system32\shfolder.dll
        73a80000 453eba8f Oct 25 02:14:55 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Foundation.XManifestation.dll
     64246f40000 4536f317 Oct 19 04:37:59 2006
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Xml\874dae5d812627145a41a14b122bb0ee\System.X
ml.ni.dll
     6424eee0000 4536f2f1 Oct 19 04:37:21 2006
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Runtime.Remo#\e0cc672a21d5ea9053256eb3e2e9e91
b\System.Runtime.Remoting.ni.dll
     7fefd540000 4549d38a Nov 02 11:16:26 2006 C:\Windows\system32\ws2_32.dll
     7feff0b0000 4549d370 Nov 02 11:16:00 2006 C:\Windows\system32\NSI.dll
     7fefc8f0000 4549d2e7 Nov 02 11:13:43 2006 C:\Windows\system32\mswsock.dll
     7fefc560000 4549d3a3 Nov 02 11:16:51 2006 C:\Windows\system32\wshtcpip.dll
     7fefc980000 4549d39d Nov 02 11:16:45 2006 C:\Windows\System32\wship6.dll
     64249120000 4536f318 Oct 19 04:38:00 2006
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Configuration\1b7409c5c3b532cc35f174a22dd45b8
4\System.Configuration.ni.dll
        72c50000 453ebade Oct 25 02:16:14 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Component.Wizard.dll
        72e10000 453eba89 Oct 25 02:14:49 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Component.Client.Shared.dll
        72e20000 453eba8a Oct 25 02:14:50 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Component.Wizard.Shared.dll
        732a0000 453eba8e Oct 25 02:14:54 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Component.Runtime.dll
        73a90000 453eba88 Oct 25 02:14:48 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Component.Runtime.Shared.dll
        73a70000 453eba8d Oct 25 02:14:53 2006 C:\Program Files\ATI
Technologies\ATI.ACE\ATICCCom.dll
        73a50000 453eba8b Oct 25 02:14:51 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Caste.Graphics.Shared.dll
        73a60000 453eba86 Oct 25 02:14:46 2006 C:\Program Files\ATI
Technologies\ATI.ACE\AEM.Foundation.dll
        73900000 453eba8b Oct 25 02:14:51 2006 C:\Program Files\ATI
Technologies\ATI.ACE\ACE.Graphics.DisplaysManager.Shared.dll
        72e00000 453ebae7 Oct 25 02:16:23 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Caste.Graphics.Wizard.dll
        72de0000 453ebae6 Oct 25 02:16:22 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Caste.Graphics.Wizard.Shared.dll
        72b90000 453ebd0d Oct 25 02:25:33 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DeviceCV.Graphics.Wizard.dll
        72ae0000 453ebd35 Oct 25 02:26:13 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DeviceCV2.Graphics.Wizard.dll
        72d00000 453ebb3f Oct 25 02:17:51 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DeviceLCD.Graphics.Wizard.dll
        72a90000 453ebb6c Oct 25 02:18:36 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DeviceLCD2.Graphics.Wizard.dll
        72dc0000 453ebd88 Oct 25 02:27:36 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DeviceTV.Graphics.Wizard.dll
```

```
        72ce0000 453ebd7d Oct 25 02:27:25 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DeviceTV2.Graphics.Wizard.dll
        728f0000 453ebafa Oct 25 02:16:42 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DisplaysManager.Graphics.Wizard.dll
        728d0000 453ebcfb Oct 25 02:25:15 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.Radeon3D.Graphics.Wizard.dll
        72860000 453ebd44 Oct 25 02:26:28 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.MMVideo.Graphics.Wizard.dll
        727e0000 453ebca9 Oct 25 02:23:53 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.TransCode.Local.Wizard.dll
        727b0000 453ebb16 Oct 25 02:17:10 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.InfoCentre.Graphics.Wizard.dll
        73060000 453ebcb2 Oct 25 02:24:02 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DeviceCV.Graphics.Shared.dll
        72ec0000 453ebaca Oct 25 02:15:54 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DeviceProperty.Graphics.Shared.dll
        73020000 453ebcd7 Oct 25 02:24:39 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DeviceCV2.Graphics.Shared.dll
        72eb0000 453ebac9 Oct 25 02:15:53 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DeviceProperty2.Graphics.Shared.dll
        73050000 453ebbdd Oct 25 02:20:29 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.CustomFormats.Graphics.Shared.dll
        730b0000 453ebaca Oct 25 02:15:54 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DeviceLCD.Graphics.Shared.dll
        73090000 453ebac9 Oct 25 02:15:53 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DeviceLCD2.Graphics.Shared.dll
        72e60000 453ebd63 Oct 25 02:26:59 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DeviceTV.Graphics.Shared.dll
        72e80000 453ebd17 Oct 25 02:25:43 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.DeviceTV2.Graphics.Shared.dll
        73190000 453ebcc6 Oct 25 02:24:22 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.Radeon3D.Graphics.Shared.dll
        73110000 453ebbff Oct 25 02:21:03 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.MMVideo.Graphics.Shared.dll
        72df0000 453ebca3 Oct 25 02:23:47 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.TransCode.Local.Shared.dll
        72cd0000 44906cde Jun 14 21:09:02 2006 C:\Program Files\ATI
Technologies\ATI.ACE\atixclib.dll
     7fefdb90000 4549d282 Nov 02 11:12:02 2006 C:\Windows\system32\CLBCatQ.DLL
     7fefdab0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\OLEAUT32.dll
        72ef0000 453ebb13 Oct 25 02:17:07 2006 C:\Program Files\ATI
Technologies\ATI.ACE\CLI.Aspect.InfoCentre.Graphics.Shared.dll
     642bc680000 46203b59 Apr 14 03:24:25 2007
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Web\c915380299000c3202f933a022f9c8d6\System.W
eb.ni.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       0000000000340000
    ProcessParameters: 0000000000341d90
    WindowTitle:  'C:\Program Files\ATI Technologies\ATI.ACE\CLI.exe'
    ImageFile:    'C:\Program Files\ATI Technologies\ATI.ACE\CLI.exe'
    CommandLine:  '"C:\Program Files\ATI Technologies\ATI.ACE\CLI.exe" -hide Wizard'
    DllPath:      'C:\Program Files\ATI
Technologies\ATI.ACE;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Wind
ows;C:\Windows\System32\Wbem'
    Environment:  0000000000341310
        =::=::\
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\UserName\AppData\Roaming
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        HOMEDRIVE=C:
        HOMEPATH=\Users\UserName
        LOCALAPPDATA=C:\Users\UserName\AppData\Local
        LOGONSERVER=\\COMPUTERNAME
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
```

```
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE=AMD64
PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=0f02
ProgramData=C:\ProgramData
ProgramFiles=C:\Program Files
ProgramFiles(x86)=C:\Program Files (x86)
PUBLIC=C:\Users\Public
SESSIONNAME=Console
SystemDrive=C:
SystemRoot=C:\Windows
TEMP=C:\Users\UserName\AppData\Local\Temp
TMP=C:\Users\UserName\AppData\Local\Temp
USERDOMAIN=COMPUTERNAME
USERNAME=UserName
USERPROFILE=C:\Users\UserName
windir=C:\Windows
```

```
        THREAD fffffa8003d85060  Cid 0a34.0a30  Teb: 000007fffffde000 Win32Thread: fffff900c1eadd60
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa8004892440  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa800499dc10       Image:         CLI.exe
        Wait Start TickCount      28728          Ticks: 17851 (0:00:04:38.477)
        Context Switch Count      577                 LargeStack
        UserTime                  00:00:00.702
        KernelTime                00:00:00.171
        Win32 Start Address CLI (0x000000001057286e)
        Stack Init fffff980158e4db0 Current fffff980158e48c0
        Base fffff980158e5000 Limit fffff980158df000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`158e4900 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`158e4a40 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`158e4aa0 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`158e4b20 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`158e4bc0 fffff960`000dc057 win32k!xxxSleepThread+0x56
        fffff980`158e4bf0 fffff800`01c4d733 win32k!NtUserWaitMessage+0x37
        fffff980`158e4c20 00000000`76d1df2a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`158e4c20)
        00000000`0018d808 00000642`7f66bf32 USER32!ZwUserWaitMessage+0xa
        00000000`0018d810 00000642`75fada2a mscorwks!DoNDirectCallWorker+0x62
        00000000`0018d8a0 00000000`0018da38 System_Windows_Forms_ni+0xda2a
        00000000`0018d8a8 00000000`0018d8f0 0x18da38
        00000000`0018d8b0 00000000`00000400 0x18d8f0
        00000000`0018d8b8 00000000`0018d6b0 0x400
        00000000`0018d8c0 00000000`00000000 0x18d6b0
        00000000`0018d8c8 00000000`003875a0 0x0
        00000000`0018d8d0 00000000`0018d8a0 0x3875a0
        00000000`0018d8d8 00000000`00000000 0x18d8a0
        00000000`0018d8e0 00000000`00000000 0x0
        00000000`0018d8e8 00000045`0000000b 0x0
        00000000`0018d8f0 00000000`00000000 0x45`0000000b
        00000000`0018d8f8 00000000`00000000 0x0
        00000000`0018d900 00000000`00000000 0x0
        00000000`0018d908 00000000`00000000 0x0
        00000000`0018d910 00000000`00000000 0x0
        00000000`0018d918 00000000`00000000 0x0
        00000000`0018d920 00006265`6eeb1335 0x0
        00000000`0018d928 00000000`00000000 0x6265`6eeb1335
        00000000`0018d930 00000000`01000000 0x0
        00000000`0018d938 00000642`7f3d2550 0x1000000
        00000000`0018d940 00000000`0018e418 mscorwks!NDirectMethodFrameStandalone::`vftable'
        00000000`0018d948 00000000`0018d8a0 0x18e418
        00000000`0018d950 00000000`10705180 0x18d8a0
        00000000`0018d958 00000000`10776301 0x10705180
        00000000`0018d960 00000000`00000000 0x10776301
        00000000`0018d968 00000000`0018d8d0 0x0
        00000000`0018d970 00000000`0018d950 0x18d8d0
        00000000`0018d978 00000000`00000000 0x18d950
        00000000`0018d980 00000000`00000000 0x0
        00000000`0018d988 00000000`00000000 0x0
        00000000`0018d990 00000642`76c1b3b0 0x0
```

```
        THREAD fffffa8001e87060  Cid 0a34.087c  Teb: 000007fffffdc000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80045eee70  SynchronizationEvent
            fffffa8003d58330  SynchronizationEvent
            fffffa80045eeed0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa800499dc10       Image:         CLI.exe
        Wait Start TickCount      5585           Ticks: 40994 (0:00:10:39.510)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address mscorwks!DebuggerRCThread::ThreadProcStatic (0x000006427f45e464)
        Stack Init fffff980159d5db0 Current fffff980159d5260
        Base fffff980159d6000 Limit fffff980159d0000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`159d52a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`159d53e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`159d5440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`159d54b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`159d5960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`159d5bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`159d5c20)
        00000000`0278fc88 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0278fc90 00000000`76bfedf1 KERNEL32!WaitForMultipleObjectsEx+0x10b
        00000000`0278fda0 00000642`7f60634e KERNEL32!WaitForMultipleObjects+0x11
        00000000`0278fde0 00000642`7f45e626 mscorwks!DebuggerRCThread::MainLoop+0xb6
        00000000`0278fe90 00000642`7f45e4b8 mscorwks!DebuggerRCThread::ThreadProc+0xf2
        00000000`0278fef0 00000000`76bfcdcd mscorwks!DebuggerRCThread::ThreadProcStatic+0x54
        00000000`0278ff40 00000000`76e1c6e1 KERNEL32!BaseThreadInitThunk+0xd
        00000000`0278ff70 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8001e83bb0  Cid 0a34.0ac4  Teb: 000007fffffda000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800189bd80  NotificationEvent
            fffffa8002596950  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa800499dc10       Image:         CLI.exe
        Wait Start TickCount      12161          Ticks: 34418 (0:00:08:56.924)
        Context Switch Count      18
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address mscorwks!Thread::intermediateThreadProc (0x000006427f5e3718)
        Stack Init fffff9800ba90db0 Current fffff9800ba90260
        Base fffff9800ba91000 Limit fffff9800ba8b000 Call 0
        Priority 11 BasePriority 10 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0ba902a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0ba903e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0ba90440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0ba904b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0ba90960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0ba90bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0ba90c20)
        00000000`030ef878 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`030ef880 00000000`76bfedf1 KERNEL32!WaitForMultipleObjectsEx+0x10b
        00000000`030ef990 00000642`7f5fc463 KERNEL32!WaitForMultipleObjects+0x11
        00000000`030ef9d0 00000642`7f47aeba mscorwks!WKS::WaitForFinalizerEvent+0x93
        00000000`030efa00 00000642`7f585a1c mscorwks!WKS::GCHeap::FinalizerThreadWorker+0x5a
        00000000`030efa40 00000642`7f58585d mscorwks!ThreadpoolMgr::FlushQueueOfTimerInfos+0x298
        00000000`030efb50 00000642`7f44fdd6 mscorwks!ThreadpoolMgr::FlushQueueOfTimerInfos+0xd9
        00000000`030efb90 00000642`7f475684 mscorwks!ManagedThreadBase_NoADTransition+0x42
        00000000`030efbf0 00000642`7f5e3790 mscorwks!WKS::GCHeap::FinalizerThreadStart+0x74
        00000000`030efc30 00000000`76bfcdcd mscorwks!Thread::intermediateThreadProc+0x78
        00000000`030efd00 00000000`76e1c6e1 KERNEL32!BaseThreadInitThunk+0xd
        00000000`030efd30 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8001e82060  Cid 0a34.0bf0  Teb: 000007fffffd4000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa800294ed90  SynchronizationEvent
            fffffa8001e82118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa800499dc10       Image:         CLI.exe
        Wait Start TickCount      46084          Ticks: 495 (0:00:00:07.722)
        Context Switch Count      219
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address mscorwks!ThreadpoolMgr::WaitThreadStart (0x000006427fabbb10)
        Stack Init fffff9800ebd5db0 Current fffff9800ebd5260
        Base fffff9800ebd6000 Limit fffff9800ebd0000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0ebd52a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0ebd53e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0ebd5440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0ebd54b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0ebd5960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0ebd5bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0ebd5c20)
        00000000`0453fd58 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0453fd60 00000642`7fabbbce KERNEL32!WaitForMultipleObjectsEx+0x10b
        00000000`0453fe70 00000000`76bfcdcd mscorwks!ThreadpoolMgr::WaitThreadStart+0xbe
        00000000`0453ff00 00000000`76e1c6e1 KERNEL32!BaseThreadInitThunk+0xd
        00000000`0453ff30 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8001e87660  Cid 0a34.0548  Teb: 000007fffff0e000 Win32Thread: 0000000000000000
WAIT: (DelayExecution) UserMode Alertable
            fffffa8001e87718  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa800499dc10       Image:         CLI.exe
        Wait Start TickCount      46476          Ticks: 103 (0:00:00:01.606)
        Context Switch Count      189
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address mscorwks!Thread::intermediateThreadProc (0x000006427f5e3718)
        Stack Init fffff9800eb96db0 Current fffff9800eb96990
        Base fffff9800eb97000 Limit fffff9800eb91000 Call 0
        Priority 7 BasePriority 7 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0eb969d0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0eb96b10 fffff800`01c5b5a9 nt!KiSwapThread+0x125
        fffff980`0eb96b70 fffff800`01e8ae9d nt!KeDelayExecutionThread+0x339
        fffff980`0eb96bf0 fffff800`01c4d733 nt!NtDelayExecution+0x5c
        fffff980`0eb96c20 00000000`76e205ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0eb96c20)
        00000000`0464edd8 00000000`76bfd908 ntdll!NtDelayExecution+0xa
        00000000`0464ede0 00000642`7f57bab9 KERNEL32!SleepEx+0x84
        00000000`0464ee60 00000642`7f4d8185 mscorwks!CExecutionEngine::ClrSleepEx+0x35
        00000000`0464eee0 00000642`7f4c7e86 mscorwks!Thread::UserSleep+0x79
        00000000`0464ef40 00000642`8015aa4b mscorwks!ThreadNative::Sleep+0x116
        00000000`0464f0f0 00000000`00002710 0x642`8015aa4b
        00000000`0464f0f8 00000000`00032000 0x2710
        00000000`0464f100 00000000`0464e558 0x32000
        00000000`0464f108 00000000`0464e5d0 0x464e558
        00000000`0464f110 00000000`0464f0f0 0x464e5d0
        00000000`0464f118 00000000`00008eec 0x464f0f0
        00000000`0464f120 00000000`00008eec 0x8eec
        00000000`0464f128 00000000`10632970 0x8eec
        00000000`0464f130 00000000`00000001 0x10632970
        00000000`0464f138 00000000`105c2f28 0x1
        00000000`0464f140 00000000`00000000 0x105c2f28
        00000000`0464f148 00000000`10632970 0x0
        00000000`0464f150 00000000`106329d8 0x10632970
        00000000`0464f158 00000642`782e7f1e 0x106329d8
        00000000`0464f160 00000000`1058a208 mscorlib_ni+0x2e7f1e
        00000000`0464f168 00000000`106328c8 0x1058a208
        00000000`0464f170 00000000`10632970 0x106328c8
        00000000`0464f178 00000177`00640002 0x10632970
        00000000`0464f180 00000000`00000000 0x177`00640002
        00000000`0464f188 00000000`106329d8 0x0
        00000000`0464f190 00000000`0464f390 0x106329d8
        00000000`0464f198 00000000`0464f1d0 0x464f390
        00000000`0464f1a0 00000000`10632970 0x464f1d0
        00000000`0464f1a8 00000642`782eb76f 0x10632970
        00000000`0464f1b0 00000642`80012020 mscorlib_ni+0x2eb76f
        00000000`0464f1b8 00000000`00000165 0x642`80012020
        00000000`0464f1c0 00000000`00000000 0x165
        00000000`0464f1c8 00000000`0464f230 0x0
        00000000`0464f1d0 00000000`0464f1b0 0x464f230
        00000000`0464f1d8 00000000`00000000 0x464f1b0
```

```
        THREAD fffffa8001ed9530  Cid 0a34.03a4  Teb: 000007fffff0a000 Win32Thread: 0000000000000000
WAIT: (DelayExecution) UserMode Non-Alertable
            fffffa8001ed95e8  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa800499dc10       Image:         CLI.exe
        Wait Start TickCount      46555          Ticks: 24 (0:00:00:00.374)
        Context Switch Count      1332
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address mscorwks!ThreadpoolMgr::GateThreadStart (0x000006427f4aed08)
        Stack Init fffff980108b3db0 Current fffff980108b3990
        Base fffff980108b4000 Limit fffff980108ae000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`108b39d0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`108b3b10 fffff800`01c5b5a9 nt!KiSwapThread+0x125
        fffff980`108b3b70 fffff800`01e8ae9d nt!KeDelayExecutionThread+0x339
        fffff980`108b3bf0 fffff800`01c4d733 nt!NtDelayExecution+0x5c
        fffff980`108b3c20 00000000`76e205ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`108b3c20)
        00000000`05c5f708 00000000`76bfd908 ntdll!NtDelayExecution+0xa
        00000000`05c5f710 00000642`7f47ad61 KERNEL32!SleepEx+0x84
        00000000`05c5f790 00000642`7f59f8dd mscorwks!EESleepEx+0x31
        00000000`05c5f810 00000642`7f4aedcb mscorwks!__DangerousSwitchToThread+0x9d
        00000000`05c5f860 00000000`76bfcdcd mscorwks!ThreadpoolMgr::GateThreadStart+0xc3
        00000000`05c5f990 00000000`76e1c6e1 KERNEL32!BaseThreadInitThunk+0xd
        00000000`05c5f9c0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa800499c060  Cid 0a34.0c08  Teb: 000007fffff08000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8001e21510  QueueObject
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa800499dc10       Image:         CLI.exe
        Wait Start TickCount      30652          Ticks: 15927 (0:00:04:08.462)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff9801db1fdb0 Current fffff9801db1f810
        Base fffff9801db20000 Limit fffff9801db1a000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1db1f850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1db1f990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`1db1f9f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`1db1fa80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`1db1fb00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`1db1fbb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1db1fc20)
        00000000`060af898 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`060af8a0 000007fe`fedce7a3 KERNEL32!GetQueuedCompletionStatus+0x48
        00000000`060af900 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`060af990 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`060afa40 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`060afa70 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`060afab0 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`060afae0 00000000`76e1c6e1 KERNEL32!BaseThreadInitThunk+0xd
        00000000`060afb10 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8002610710  Cid 0a34.0fd0  Teb: 000007fffffd6000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8001e1a880  QueueObject
            fffffa80026107c8  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa800499dc10       Image:         CLI.exe
        Wait Start TickCount      46084          Ticks: 495 (0:00:00:07.722)
        Context Switch Count      15
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address mscorwks!Thread::intermediateThreadProc (0x000006427f5e3718)
        Stack Init fffff98010827db0 Current fffff98010827810
        Base fffff98010828000 Limit fffff98010822000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`10827850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`10827990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`108279f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`10827a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`10827b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`10827bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`10827c20)
        00000000`05edfc98 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`05edfca0 00000642`7f45557f KERNEL32!GetQueuedCompletionStatus+0x48
        00000000`05edfd00 00000642`7f5e3790 mscorwks!ThreadpoolMgr::CompletionPortThreadStart+0xbf
        00000000`05edfda0 00000000`76bfcdcd mscorwks!Thread::intermediateThreadProc+0x78
        00000000`05edfdf0 00000000`76e1c6e1 KERNEL32!BaseThreadInitThunk+0xd
        00000000`05edfe20 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80025d1060  Cid 0a34.0280  Teb: 000007fffffd8000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa8001e1a880  QueueObject
            fffffa80025d1118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa800499dc10       Image:         CLI.exe
        Wait Start TickCount      46084          Ticks: 495 (0:00:00:07.722)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address mscorwks!Thread::intermediateThreadProc (0x000006427f5e3718)
        Stack Init fffff98020c82db0 Current fffff98020c82810
        Base fffff98020c83000 Limit fffff98020c7d000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`20c82850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`20c82990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`20c829f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`20c82a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`20c82b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`20c82bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`20c82c20)
        00000000`05aff528 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`05aff530 00000642`7f45557f KERNEL32!GetQueuedCompletionStatus+0x48
        00000000`05aff590 00000642`7f5e3790 mscorwks!ThreadpoolMgr::CompletionPortThreadStart+0xbf
        00000000`05aff630 00000000`76bfcdcd mscorwks!Thread::intermediateThreadProc+0x78
        00000000`05aff780 00000000`76e1c6e1 KERNEL32!BaseThreadInitThunk+0xd
        00000000`05aff7b0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

Dllhost process

```
PROCESS fffffa8002004c10
    SessionId: 0  Cid: 041c    Peb: 7fffffd8000  ParentCid: 025c
    DirBase: 202fb000  ObjectTable: fffff880016b4c20  HandleCount: 241.
    Image: dllhost.exe
    VadRoot fffffa8004318650 Vads 155 Clone 0 Private 1547. Modified 0. Locked 0.
    DeviceMap fffff88000007820
    Token                             fffff880030c4c40
    ElapsedTime                       00:10:11.793
    UserTime                          00:00:00.078
    KernelTime                        00:00:00.156
    QuotaPoolUsage[PagedPool]         157120
    QuotaPoolUsage[NonPagedPool]      15152
    Working Set Sizes (now,min,max)  (3697, 50, 345) (14788KB, 200KB, 1380KB)
    PeakWorkingSetSize                3703
    VirtualSize                       96 Mb
    PeakVirtualSize                   100 Mb
    PageFaultCount                    4097
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      1860

    Setting context for this process...
.process /p /r fffffa8002004c10

    !peb
PEB at 000007fffffd8000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00000000fff60000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 0000000000232840 . 000000000139ebe0
    Ldr.InLoadOrderModuleList:           0000000000232750 . 000000000139f0a0
    Ldr.InMemoryOrderModuleList:         0000000000232760 . 000000000139f0b0
            Base TimeStamp                     Module
        fff60000 4549bbff Nov 02 09:35:59 2006 C:\Windows\system32\dllhost.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        76bc0000 4549d328 Nov 02 11:14:48 2006 C:\Windows\system32\kernel32.dll
     7fefdd40000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\system32\msvcrt.dll
     7fefd760000 4549d317 Nov 02 11:14:31 2006 C:\Windows\system32\ole32.dll
     7fefec20000 4549d273 Nov 02 11:11:47 2006 C:\Windows\system32\GDI32.dll
        76d00000 45d3ee19 Feb 15 05:22:33 2007 C:\Windows\system32\USER32.dll
     7fefea30000 4549d267 Nov 02 11:11:35 2006 C:\Windows\system32\ADVAPI32.dll
     7fefed90000 469c43bb Jul 17 05:21:15 2007 C:\Windows\system32\RPCRT4.dll
     7fefd9e0000 4549d2cb Nov 02 11:13:15 2006 C:\Windows\system32\IMM32.DLL
     7fefdc30000 4549d2e6 Nov 02 11:13:42 2006 C:\Windows\system32\MSCTF.dll
     7feff0c0000 4549d2a1 Nov 02 11:12:33 2006 C:\Windows\system32\LPK.DLL
     7fefd940000 4549d337 Nov 02 11:15:03 2006 C:\Windows\system32\USP10.dll
     7fefdb90000 4549d282 Nov 02 11:12:02 2006 C:\Windows\system32\CLBCatQ.DLL
     7fefdab0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\OLEAUT32.dll
     7fefc620000 4549d31d Nov 02 11:14:37 2006 C:\Windows\system32\rsaenh.dll
     7fef3ee0000 4549d336 Nov 02 11:15:02 2006 C:\Windows\system32\COMSVCS.DLL
     7fefda10000 4549d31f Nov 02 11:14:39 2006 C:\Windows\system32\SHLWAPI.dll
     7fefbe70000 4549d32b Nov 02 11:14:51 2006 C:\Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_1559f1c6f365a7fa\comctl32.dll
     7fefba70000 4549d2e7 Nov 02 11:13:43 2006 C:\Windows\system32\ES.DLL
     7fefb4d0000 4549d30d Nov 02 11:14:21 2006 C:\Windows\system32\PROPSYS.dll
     7fefd1f0000 4549d32f Nov 02 11:14:55 2006 C:\Windows\system32\SXS.DLL
     7fef6590000 4549d370 Nov 02 11:16:00 2006 C:\Windows\system32\txflog.dll
     7fefca50000 4549d336 Nov 02 11:15:02 2006 C:\Windows\system32\VERSION.dll
     7fef8140000 4549d352 Nov 02 11:15:30 2006 C:\Windows\system32\XOLEHLP.dll
     7fefcf70000 4549d2fc Nov 02 11:14:04 2006 C:\Windows\system32\NETAPI32.dll
     7fefd530000 4549d310 Nov 02 11:14:24 2006 C:\Windows\system32\PSAPI.DLL
     7fef42a0000 4549d2fd Nov 02 11:14:05 2006 C:\Windows\system32\MSDTCPRX.DLL
```

```
     7fef4250000 4549d2ee Nov 02 11:13:50 2006 C:\Windows\system32\MTXCLU.DLL
     7fefd540000 4549d38a Nov 02 11:16:26 2006 C:\Windows\system32\WS2_32.dll
     7feff0b0000 4549d370 Nov 02 11:16:00 2006 C:\Windows\system32\NSI.dll
     7fefabc0000 4549d287 Nov 02 11:12:07 2006 C:\Windows\system32\CLUSAPI.dll
     7fefcdd0000 4549d375 Nov 02 11:16:05 2006 C:\Windows\system32\NTDSAPI.dll
     7fefce40000 4549d288 Nov 02 11:12:08 2006 C:\Windows\system32\DNSAPI.dll
     7fefd590000 4549d396 Nov 02 11:16:38 2006 C:\Windows\system32\WLDAP32.dll
     7fefd390000 4549d33f Nov 02 11:15:11 2006 C:\Windows\system32\Secur32.dll
     7fefaad0000 4549d254 Nov 02 11:11:16 2006 C:\Windows\system32\ACTIVEDS.dll
     7fefaa00000 4549d263 Nov 02 11:11:31 2006 C:\Windows\system32\adsldpc.dll
     7fefa9c0000 4549d342 Nov 02 11:15:14 2006 C:\Windows\system32\credui.dll
     7fefddf0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\SHELL32.dll
     7fefc180000 4549d253 Nov 02 11:11:15 2006 C:\Windows\system32\ATL.DLL
     7fefada0000 4549d33d Nov 02 11:15:09 2006 C:\Windows\system32\RESUTILS.dll
     7fefd3b0000 4549d336 Nov 02 11:15:02 2006 C:\Windows\system32\USERENV.dll
     7fefca60000 4549d252 Nov 02 11:11:14 2006 C:\Windows\system32\bcrypt.dll
     7fefb110000 4549d334 Nov 02 11:15:00 2006 C:\Windows\system32\ktmw32.dll
     7fefca40000 4549d341 Nov 02 11:15:13 2006 C:\Windows\system32\credssp.dll
     7fefcc50000 4549d344 Nov 02 11:15:16 2006 C:\Windows\system32\CRYPT32.dll
     7fefce00000 4549d2df Nov 02 11:13:35 2006 C:\Windows\system32\MSASN1.dll
     7fefc670000 4549d321 Nov 02 11:14:41 2006 C:\Windows\system32\schannel.dll
     7fefc8f0000 4549d2e7 Nov 02 11:13:43 2006 C:\Windows\System32\mswsock.dll
     7fefaab0000 4549d371 Nov 02 11:16:01 2006 C:\Windows\System32\winrnr.dll
     7fefc1a0000 4549d314 Nov 02 11:14:28 2006 C:\Windows\system32\NLAapi.dll
     7fefcb80000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\system32\IPHLPAPI.DLL
     7fefcb30000 4549d263 Nov 02 11:11:31 2006 C:\Windows\system32\dhcpcsvc.DLL
     7fefd280000 4549d370 Nov 02 11:16:00 2006 C:\Windows\system32\WINNSI.DLL
     7fefcb00000 4549d264 Nov 02 11:11:32 2006 C:\Windows\system32\dhcpcsvc6.DLL
     7fefaa70000 4549d2e4 Nov 02 11:13:40 2006 C:\Windows\system32\napinsp.dll
     7fefaa50000 4549d341 Nov 02 11:15:13 2006 C:\Windows\system32\pnrpnsp.dll
     7fefaac0000 4549d317 Nov 02 11:14:31 2006 C:\Windows\system32\rasadhlp.dll
     7fefc980000 4549d39d Nov 02 11:16:45 2006 C:\Windows\System32\wship6.dll
     7fef38b0000 4549d25a Nov 02 11:11:22 2006 C:\Windows\system32\catsrv.dll
     7fef3d30000 4549d2aa Nov 02 11:12:42 2006 C:\Windows\system32\MfcSubs.dll
     7fef3b60000 4549d25b Nov 02 11:11:23 2006 C:\Windows\system32\catsrvps.dll
     7fef3820000 4549d25c Nov 02 11:11:24 2006 C:\Windows\system32\catsrvut.dll
     7fefa800000 4549d33f Nov 02 11:15:11 2006 C:\Windows\system32\VSSAPI.DLL
     7fefa9a0000 4549d341 Nov 02 11:15:13 2006 C:\Windows\system32\vsstrace.dll
     7fefd360000 4549d265 Nov 02 11:11:33 2006 C:\Windows\system32\AUTHZ.dll
     7fefb930000 4549d350 Nov 02 11:15:28 2006 C:\Windows\system32\XmlLite.dll
     7fefcd90000 4549d2b2 Nov 02 11:12:50 2006 C:\Windows\system32\MPR.dll
     7fefeed0000 4549d318 Nov 02 11:14:32 2006 C:\Windows\system32\SETUPAPI.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       0000000000230000
    ProcessParameters: 0000000000231de0
    WindowTitle:  'C:\Windows\system32\dllhost.exe'
    ImageFile:    'C:\Windows\system32\dllhost.exe'
    CommandLine:  'C:\Windows\system32\dllhost.exe /Processid:{02D4B3F1-FD88-11D1-960D-
00805FC79235}'
    DllPath:
'C:\Windows\system32;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Wind
ows;C:\Windows\System32\Wbem'
    Environment:  0000000000231310
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\system32\config\systemprofile\AppData\Roaming
        commonfiles=C:\Program Files\Common Files
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        LOCALAPPDATA=C:\Windows\system32\config\systemprofile\AppData\Local
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
```

```
        progfiles=C:\Program Files
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public
        systemdir=C:\Windows\system32
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\TEMP
        TMP=C:\Windows\TEMP
        USERDOMAIN=DOMAIN
        USERNAME=COMPUTERNAME$
        USERPROFILE=C:\Windows\system32\config\systemprofile
        windir=C:\Windows


        THREAD fffffa8002004780  Cid 041c.0b68  Teb: 000007fffffde000 Win32Thread: fffff900c200bb20
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8001ff9220  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8002004c10       Image:         dllhost.exe
        Wait Start TickCount      7502           Ticks: 39077 (0:00:10:09.605)
        Context Switch Count      147                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.046
        Win32 Start Address dllhost!WinMainCRTStartup (0x00000000fff61818)
        Stack Init fffff98012b30db0 Current fffff98012b30960
        Base fffff98012b31000 Limit fffff98012b28000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`12b309a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12b30ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`12b30b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`12b30bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`12b30c20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12b30c20)
        00000000`001af898 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`001af8a0 000007fe`fd77a326 kernel32!WaitForSingleObjectEx+0x9c
        00000000`001af960 000007fe`fd779fb5
ole32!CSurrogateProcessActivator::WaitForSurrogateTimeout+0x6b
        00000000`001af990 00000000`fff6144f ole32!CoRegisterSurrogateEx+0x24c
        00000000`001af9d0 00000000`fff6166f dllhost!WinMain+0x207
        00000000`001afcd0 00000000`76bfcdcd dllhost!WinMain+0x427
        00000000`001afd90 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`001afdc0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800202ea60  Cid 041c.0b14  Teb: 000007fffffdc000 Win32Thread: 0000000000000000
WAIT: (Executive) UserMode Non-Alertable
            fffffa8001f080e8  NotificationEvent
        IRP List:
            fffffa80043ebdb0: (0006,0118) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8002004c10       Image:         dllhost.exe
        Wait Start TickCount      7416           Ticks: 39163 (0:00:10:10.946)
        Context Switch Count      12
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ole32!CSurrogateProcessActivator::StartNTService (0x000007fefd859f60)
        Stack Init fffff9800f28cdb0 Current fffff9800f28c7f0
        Base fffff9800f28d000 Limit fffff9800f287000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0f28c830 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0f28c970 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0f28c9d0 fffff800`01ebdf16 nt!KeWaitForSingleObject+0x5f5
        fffff980`0f28ca50 fffff800`01ea1a24 nt!IopSynchronousServiceTail+0x306
        fffff980`0f28cac0 fffff800`01c4d733 nt!NtReadFile+0x583
        fffff980`0f28cbb0 00000000`76e202da nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0f28cc20)
        00000000`00d0f268 00000000`76bf26da ntdll!NtReadFile+0xa
        00000000`00d0f270 000007fe`fea865aa kernel32!ReadFile+0x8a
        00000000`00d0f300 000007fe`fea862e3 ADVAPI32!ScGetPipeInput+0x4a
        00000000`00d0f3e0 000007fe`fea850f3 ADVAPI32!ScDispatcherLoop+0x9a
        00000000`00d0f4e0 000007fe`fd859f9d ADVAPI32!StartServiceCtrlDispatcherW+0x176
        00000000`00d0f780 00000000`76bfcdcd ole32!CSurrogateProcessActivator::StartNTService+0x3d
        00000000`00d0f7e0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`00d0f810 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8002014a30  Cid 041c.0350  Teb: 000007fffffd4000 Win32Thread: fffff900c07f8d60
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa8002003a60  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8002004c10       Image:         dllhost.exe
        Wait Start TickCount      45879          Ticks: 700 (0:00:00:10.920)
        Context Switch Count      19                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ole32!CRpcThreadCache::RpcWorkerThreadEntry (0x000007fefd7a3be0)
        Stack Init fffff98012f69db0 Current fffff98012f69740
        Base fffff98012f6a000 Limit fffff98012f62000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`12f69780 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12f698c0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`12f69920 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`12f699a0 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`12f69a40 fffff960`000c7e1e win32k!xxxSleepThread+0x56
        fffff980`12f69a70 fffff960`000c7f25 win32k!xxxRealInternalGetMessage+0x72e
        fffff980`12f69b50 fffff960`000c97e4 win32k!xxxInternalGetMessage+0x35
        fffff980`12f69b90 fffff800`01c4d733 win32k!NtUserGetMessage+0x64
        fffff980`12f69c20 00000000`76d1e6aa nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12f69c20)
        00000000`01d7f668 00000000`76d1e6ea USER32!ZwUserGetMessage+0xa
        00000000`01d7f670 000007fe`fd779d72 USER32!GetMessageW+0x34
        00000000`01d7f6a0 000007fe`fd77a0dd ole32!CDllHost::STAWorkerLoop+0x8a
        00000000`01d7f700 000007fe`fd7a3b7e ole32!CDllHost::WorkerThread+0xd7
        00000000`01d7f740 000007fe`fd7a3c0a ole32!CRpcThread::WorkerLoop+0x1e
        00000000`01d7f780 00000000`76bfcdcd ole32!CRpcThreadCache::RpcWorkerThreadEntry+0x2a
        00000000`01d7f7b0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`01d7f7e0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8004507bb0  Cid 041c.0c10  Teb: 000007fffffaa000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800202b180  SynchronizationEvent
            fffffa8004520530  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8002004c10       Image:         dllhost.exe
        Wait Start TickCount      7506           Ticks: 39073 (0:00:10:09.542)
        Context Switch Count      57
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address msvcrt!endthreadex (0x000007fefdd59620)
        Stack Init fffff98012fe3db0 Current fffff98012fe3260
        Base fffff98012fe4000 Limit fffff98012fde000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`12fe32a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12fe33e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`12fe3440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`12fe34b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`12fe3960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`12fe3bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12fe3c20)
        00000000`011def78 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`011def80 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`011df090 000007fe`f3f36003 kernel32!WaitForMultipleObjects+0x11
        00000000`011df0d0 000007fe`f3f244e1 COMSVCS!CRMRecoveryClerk::RecoveryThread+0x2c3
        00000000`011df890 000007fe`fdd594e7 COMSVCS!RecoveryThreadFunction+0x131
        00000000`011df8f0 000007fe`fdd5967d msvcrt!endthreadex+0x47
        00000000`011df920 00000000`76bfcdcd msvcrt!endthreadex+0x100
        00000000`011df950 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`011df980 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8004503060  Cid 041c.0c14  Teb: 000007fffffa8000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa8003d55040  SynchronizationTimer
            fffffa80043e78a0  SynchronizationTimer
            fffffa8001f7b700  SynchronizationTimer
            fffffa8002004c10  ProcessObject
            fffffa800200efe0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8002004c10       Image:         dllhost.exe
        Wait Start TickCount      7438           Ticks: 39141 (0:00:10:10.603)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x0000000076df6930)
        Stack Init fffff9800e2a5db0 Current fffff9800e2a5260
        Base fffff9800e2a6000 Limit fffff9800e2a0000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e2a52a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e2a53e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0e2a5440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0e2a54b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`0e2a5960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`0e2a5bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e2a5c20)
        00000000`0217f778 00000000`76df6b07 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0217f780 00000000`76bfcdcd ntdll!TppWaiterpThread+0x14d
        00000000`0217fa20 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0217fa50 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8001e6c360  Cid 041c.0c18  Teb: 000007fffffa6000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa800201a650  QueueObject
            fffffa8001e6c418  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8002004c10       Image:         dllhost.exe
        Wait Start TickCount      42059          Ticks: 4520 (0:00:01:10.512)
        Context Switch Count      47
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address msvcrt!endthreadex (0x000007fefdd59620)
        Stack Init fffff98012bc7db0 Current fffff98012bc7810
        Base fffff98012bc8000 Limit fffff98012bc2000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`12bc7850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12bc7990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`12bc79f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`12bc7a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`12bc7b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`12bc7bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12bc7c20)
        00000000`0227f758 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`0227f760 000007fe`f3fd6c02 kernel32!GetQueuedCompletionStatus+0x48
        00000000`0227f7c0 000007fe`f3fd6fde COMSVCS!WORK_QUEUE::WorkerLoop+0xb2
        00000000`0227f8b0 000007fe`fdd594e7 COMSVCS!WORK_QUEUE::ThreadLoop+0xe
        00000000`0227f8e0 000007fe`fdd5967d msvcrt!endthreadex+0x47
        00000000`0227f910 00000000`76bfcdcd msvcrt!endthreadex+0x100
        00000000`0227f940 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0227f970 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8002014060  Cid 041c.0c20  Teb: 000007fffffa2000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800200e190  SynchronizationEvent
            fffffa8002012fe0  SynchronizationEvent
            fffffa8002014118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8002004c10       Image:         dllhost.exe
        Wait Start TickCount      46551          Ticks: 28 (0:00:00:00.436)
        Context Switch Count      1708
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address COMSVCS!CEventServer::DispatchEvents (0x000007fef3f42400)
        Stack Init fffff9801a6d7db0 Current fffff9801a6d7260
        Base fffff9801a6d8000 Limit fffff9801a6d2000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1a6d72a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1a6d73e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`1a6d7440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`1a6d74b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`1a6d7960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`1a6d7bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1a6d7c20)
        00000000`0264f8e8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0264f8f0 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0264fa00 000007fe`f3f5205a kernel32!WaitForMultipleObjects+0x11
        00000000`0264fa40 000007fe`f3f42491 COMSVCS!CLceDisp::DoWork+0x18a
        00000000`0264fb20 00000000`76bfcdcd COMSVCS!CEventServer::DispatchEvents+0x91
        00000000`0264fb60 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0264fb90 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80020a9bb0  Cid 041c.0c2c  Teb: 000007fffff9e000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800205e8b0  SynchronizationEvent
            fffffa8004310e00  NotificationEvent
            fffffa8002009060  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8002004c10       Image:         dllhost.exe
        Wait Start TickCount      7439           Ticks: 39140 (0:00:10:10.587)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address COMSVCS!PostData (0x000007fef3f88020)
        Stack Init fffff9801a6dedb0 Current fffff9801a6de260
        Base fffff9801a6df000 Limit fffff9801a6d9000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1a6de2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1a6de3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`1a6de440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`1a6de4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`1a6de960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`1a6debb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1a6dec20)
        00000000`02adfcb8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`02adfcc0 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`02adfdd0 000007fe`f3f881ff kernel32!WaitForMultipleObjects+0x11
        00000000`02adfe10 00000000`76bfcdcd COMSVCS!PostData+0x1df
        00000000`02adfec0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02adfef0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa800202e060  Cid 041c.0c30  Teb: 000007fffff9c000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8001ec4c60  SynchronizationEvent
            fffffa800202b6a0  NotificationEvent
            fffffa8001e1b940  SynchronizationEvent
            fffffa800202e118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8002004c10       Image:         dllhost.exe
        Wait Start TickCount      45983          Ticks: 596 (0:00:00:09.297)
        Context Switch Count      70
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address msvcrt!endthreadex (0x000007fefdd59620)
        Stack Init fffff9801a6f3db0 Current fffff9801a6f3260
        Base fffff9801a6f4000 Limit fffff9801a6ee000 Call 0
        Priority 13 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1a6f32a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1a6f33e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`1a6f3440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`1a6f34b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`1a6f3960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`1a6f3bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1a6f3c20)
        00000000`02d3fbd8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`02d3fbe0 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`02d3fcf0 000007fe`f3f3d81a kernel32!WaitForMultipleObjects+0x11
        00000000`02d3fd30 000007fe`f3f244e1 COMSVCS!CRecoveryClerk2::RecoveryThread+0x4ca
        00000000`02d3fe60 000007fe`fdd594e7 COMSVCS!RecoveryThreadFunction+0x131
        00000000`02d3fec0 000007fe`fdd5967d msvcrt!endthreadex+0x47
        00000000`02d3fef0 00000000`76bfcdcd msvcrt!endthreadex+0x100
        00000000`02d3ff20 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02d3ff50 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80020678b0  Cid 041c.0ca0  Teb: 000007fffffae000 Win32Thread: 0000000000000000
WAIT: (DelayExecution) UserMode Non-Alertable
            fffffa8002067968  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8002004c10       Image:         dllhost.exe
        Wait Start TickCount      46574          Ticks: 5 (0:00:00:00.078)
        Context Switch Count      5810
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address MSDTCPRX!CConnectionManager::TimerProc (0x000007fef42e14b0)
        Stack Init fffff9801a698db0 Current fffff9801a698990
        Base fffff9801a699000 Limit fffff9801a693000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1a6989d0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1a698b10 fffff800`01c5b5a9 nt!KiSwapThread+0x125
        fffff980`1a698b70 fffff800`01e8ae9d nt!KeDelayExecutionThread+0x339
        fffff980`1a698bf0 fffff800`01c4d733 nt!NtDelayExecution+0x5c
        fffff980`1a698c20 00000000`76e205ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1a698c20)
        00000000`0391f7b8 00000000`76bfd908 ntdll!NtDelayExecution+0xa
        00000000`0391f7c0 000007fe`f42e15a3 kernel32!SleepEx+0x84
        00000000`0391f840 000007fe`f42e14cb
MSDTCPRX!CConnectionManager::TimerProcForNonGuardedUser+0xc3
        00000000`0391f8a0 00000000`76bfcdcd MSDTCPRX!CConnectionManager::TimerProc+0x1b
        00000000`0391f8d0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0391f900 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80020b0bb0  Cid 041c.0d30  Teb: 000007fffff9a000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80020a3a30  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8002004c10       Image:         dllhost.exe
        Wait Start TickCount      46371          Ticks: 208 (0:00:00:03.244)
        Context Switch Count      240
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address MSDTCPRX!CSessionObject::MaintainSession (0x000007fef42eb840)
        Stack Init fffff9801dbcedb0 Current fffff9801dbce960
        Base fffff9801dbcf000 Limit fffff9801dbc9000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1dbce9a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1dbceae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`1dbceb40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`1dbcebc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`1dbcec20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1dbcec20)
        00000000`036ef598 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`036ef5a0 000007fe`f42edd79 kernel32!WaitForSingleObjectEx+0x9c
        00000000`036ef660 000007fe`f42eba8f MSDTCPRX!CSessionObject::MaintainItInUpState+0x359
        00000000`036ef920 000007fe`f42eb84e MSDTCPRX!CSessionObject::MaintainIt+0x22f
        00000000`036ef990 00000000`76bfcdcd MSDTCPRX!CSessionObject::MaintainSession+0xe
        00000000`036ef9c0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`036ef9f0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8002052060  Cid 041c.0dd0  Teb: 000007fffff96000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800202da30  SynchronizationEvent
            fffffa8002052118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8002004c10       Image:         dllhost.exe
        Wait Start TickCount      46202          Ticks: 377 (0:00:00:05.881)
        Context Switch Count      22
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address msvcrt!endthreadex (0x000007fefdd59620)
        Stack Init fffff98010373db0 Current fffff98010373960
        Base fffff98010374000 Limit fffff9801036e000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`103739a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`10373ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`10373b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`10373bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`10373c20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`10373c20)
        00000000`0352f7e8 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`0352f7f0 000007fe`f38d959c kernel32!WaitForSingleObjectEx+0x9c
        00000000`0352f8b0 000007fe`f38bf444 catsrv!RegSrvrPump+0x9c
        00000000`0352f8e0 000007fe`fdd594e7 catsrv!RunService+0xf4
        00000000`0352f930 000007fe`fdd5967d msvcrt!endthreadex+0x47
        00000000`0352f960 00000000`76bfcdcd msvcrt!endthreadex+0x100
        00000000`0352f990 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0352f9c0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80048cdbb0  Cid 041c.0fc4  Teb: 000007fffffda000 Win32Thread: fffff900c07f3d60
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa80044f5040  QueueObject
            fffffa80048cdc68  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8002004c10       Image:         dllhost.exe
        Wait Start TickCount      46507          Ticks: 72 (0:00:00:01.123)
        Context Switch Count      571                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff9801063fdb0 Current fffff9801063f810
        Base fffff98010640000 Limit fffff98010639000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1063f850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1063f990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`1063f9f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`1063fa80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`1063fb00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`1063fbb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1063fc20)
        00000000`0206f768 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`0206f770 000007fe`fedce7a3 kernel32!GetQueuedCompletionStatus+0x48
        00000000`0206f7d0 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`0206f860 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`0206f910 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`0206f940 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`0206f980 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`0206f9b0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0206f9e0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa800452c9d0  Cid 041c.0fb4  Teb: 000007fffffd6000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa80044f5040  QueueObject
            fffffa800452ca88  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa8002004c10       Image:         dllhost.exe
        Wait Start TickCount      45039          Ticks: 1540 (0:00:00:24.024)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff980102eedb0 Current fffff980102ee810
        Base fffff980102ef000 Limit fffff980102e9000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`102ee850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`102ee990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`102ee9f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`102eea80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`102eeb00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`102eebb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`102eec20)
        00000000`0244f878 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`0244f880 000007fe`fedce7a3 kernel32!GetQueuedCompletionStatus+0x48
        00000000`0244f8e0 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`0244f970 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`0244fa20 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`0244fa50 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`0244fa90 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`0244fac0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0244faf0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

Msdtc process

```
PROCESS fffffa8002043c10
    SessionId: 0  Cid: 0ca4    Peb: 7fffffde000  ParentCid: 025c
    DirBase: 22f00000  ObjectTable: fffff880031b0970  HandleCount: 159.
    Image: msdtc.exe
    VadRoot fffffa8004425440 Vads 153 Clone 0 Private 664. Modified 2. Locked 0.
    DeviceMap fffff8800598a680
    Token                             fffff8800310e400
    ElapsedTime                       00:10:09.887
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         109824
    QuotaPoolUsage[NonPagedPool]      14784
    Working Set Sizes (now,min,max)  (1956, 50, 345) (7824KB, 200KB, 1380KB)
    PeakWorkingSetSize                1970
    VirtualSize                       81 Mb
    PeakVirtualSize                   82 Mb
    PageFaultCount                    2103
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      882

    Setting context for this process...
.process /p /r fffffa8002043c10

    !peb
PEB at 000007fffffde000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         0000000000ca0000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 0000000000282790 . 00000000002b75d0
    Ldr.InLoadOrderModuleList:           00000000002826a0 . 00000000002b7680
    Ldr.InMemoryOrderModuleList:         00000000002826b0 . 00000000002b7690
            Base TimeStamp                     Module
          ca0000 4549bc1e Nov 02 09:36:30 2006 C:\Windows\System32\msdtc.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        76bc0000 4549d328 Nov 02 11:14:48 2006 C:\Windows\system32\kernel32.dll
     7fefd760000 4549d317 Nov 02 11:14:31 2006 C:\Windows\system32\ole32.dll
     7fefdd40000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\system32\msvcrt.dll
     7fefec20000 4549d273 Nov 02 11:11:47 2006 C:\Windows\system32\GDI32.dll
        76d00000 45d3ee19 Feb 15 05:22:33 2007 C:\Windows\system32\USER32.dll
     7fefea30000 4549d267 Nov 02 11:11:35 2006 C:\Windows\system32\ADVAPI32.dll
     7fefed90000 469c43bb Jul 17 05:21:15 2007 C:\Windows\system32\RPCRT4.dll
     7fef3b80000 4549d2ff Nov 02 11:14:07 2006 C:\Windows\System32\MSDTCTM.dll
     7fef42a0000 4549d2fd Nov 02 11:14:05 2006 C:\Windows\System32\MSDTCPRX.dll
     7fefcf70000 4549d2fc Nov 02 11:14:04 2006 C:\Windows\System32\NETAPI32.dll
     7fefd530000 4549d310 Nov 02 11:14:24 2006 C:\Windows\system32\PSAPI.DLL
     7fef4250000 4549d2ee Nov 02 11:13:50 2006 C:\Windows\System32\MTXCLU.DLL
     7fefd540000 4549d38a Nov 02 11:16:26 2006 C:\Windows\system32\WS2_32.dll
     7feff0b0000 4549d370 Nov 02 11:16:00 2006 C:\Windows\system32\NSI.dll
     7fefabc0000 4549d287 Nov 02 11:12:07 2006 C:\Windows\System32\CLUSAPI.dll
     7fefcdd0000 4549d375 Nov 02 11:16:05 2006 C:\Windows\System32\NTDSAPI.dll
     7fefce40000 4549d288 Nov 02 11:12:08 2006 C:\Windows\System32\DNSAPI.dll
     7fefd590000 4549d396 Nov 02 11:16:38 2006 C:\Windows\system32\WLDAP32.dll
     7fefd390000 4549d33f Nov 02 11:15:11 2006 C:\Windows\System32\Secur32.dll
     7fefdab0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\OLEAUT32.dll
     7fefaad0000 4549d254 Nov 02 11:11:16 2006 C:\Windows\System32\ACTIVEDS.dll
     7fefaa00000 4549d263 Nov 02 11:11:31 2006 C:\Windows\System32\adsldpc.dll
     7fefa9c0000 4549d342 Nov 02 11:15:14 2006 C:\Windows\System32\credui.dll
     7fefddf0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\SHELL32.dll
     7fefda10000 4549d31f Nov 02 11:14:39 2006 C:\Windows\system32\SHLWAPI.dll
     7fefc180000 4549d253 Nov 02 11:11:15 2006 C:\Windows\System32\ATL.DLL
     7fefada0000 4549d33d Nov 02 11:15:09 2006 C:\Windows\System32\RESUTILS.dll
```

```
     7fefd3b0000 4549d336 Nov 02 11:15:02 2006 C:\Windows\System32\USERENV.dll
     7fefca50000 4549d336 Nov 02 11:15:02 2006 C:\Windows\System32\VERSION.dll
     7fefca60000 4549d252 Nov 02 11:11:14 2006 C:\Windows\System32\bcrypt.dll
     7fefb110000 4549d334 Nov 02 11:15:00 2006 C:\Windows\System32\ktmw32.dll
     7fef4d80000 4549d2fc Nov 02 11:14:04 2006 C:\Windows\System32\MSDTCLOG.dll
     7fefb360000 4549d36f Nov 02 11:15:59 2006 C:\Windows\System32\WINMM.dll
     7fefb310000 4549d318 Nov 02 11:14:32 2006 C:\Windows\System32\OLEACC.dll
     7fef8140000 4549d352 Nov 02 11:15:30 2006 C:\Windows\System32\XOLEHLP.dll
     7fefc8f0000 4549d2e7 Nov 02 11:13:43 2006 C:\Windows\System32\MSWSOCK.dll
     7fefd9e0000 4549d2cb Nov 02 11:13:15 2006 C:\Windows\system32\IMM32.DLL
     7fefdc30000 4549d2e6 Nov 02 11:13:42 2006 C:\Windows\system32\MSCTF.dll
     7feff0c0000 4549d2a1 Nov 02 11:12:33 2006 C:\Windows\system32\LPK.DLL
     7fefd940000 4549d337 Nov 02 11:15:03 2006 C:\Windows\system32\USP10.dll
     7fefbe70000 4549d32b Nov 02 11:14:51 2006 C:\Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_1559f1c6f365a7fa\comctl32.dll
        72680000 4549bc13 Nov 02 09:36:19 2006 C:\Windows\System32\COMRES.DLL
     7fef4220000 4549d2f1 Nov 02 11:13:53 2006 C:\Windows\System32\MTxOCI.Dll
     7fefca40000 4549d341 Nov 02 11:15:13 2006 C:\Windows\System32\credssp.dll
     7fefcc50000 4549d344 Nov 02 11:15:16 2006 C:\Windows\System32\CRYPT32.dll
     7fefce00000 4549d2df Nov 02 11:13:35 2006 C:\Windows\System32\MSASN1.dll
     7fefc670000 4549d321 Nov 02 11:14:41 2006 C:\Windows\system32\schannel.dll
     7fefc5b0000 4549d384 Nov 02 11:16:20 2006 C:\Windows\System32\NTMARTA.DLL
     7fefce20000 4549d315 Nov 02 11:14:29 2006 C:\Windows\System32\SAMLIB.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       0000000000280000
    ProcessParameters: 0000000000281da0
    WindowTitle:  'C:\Windows\System32\msdtc.exe'
    ImageFile:    'C:\Windows\System32\msdtc.exe'
    CommandLine:  'C:\Windows\System32\msdtc.exe'
    DllPath:
'C:\Windows\System32;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Wind
ows;C:\Windows\System32\Wbem'
    Environment:  0000000000281310
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        LOCALAPPDATA=C:\Windows\ServiceProfiles\NetworkService\AppData\Local
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\SERVIC~2\NETWOR~1\AppData\Local\Temp
        TMP=C:\Windows\SERVIC~2\NETWOR~1\AppData\Local\Temp
        USERDOMAIN=DOMAIN
        USERNAME=COMPUTERNAME$
        USERPROFILE=C:\Windows\ServiceProfiles\NetworkService
        windir=C:\Windows
```

```
        THREAD fffffa8002045bb0  Cid 0ca4.0ca8  Teb: 000007fffffdc000 Win32Thread: fffff900c200d010
WAIT: (Executive) UserMode Non-Alertable
            fffffa8001ec2d58  NotificationEvent
        IRP List:
            fffffa80039de5e0: (0006,0118) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa8002043c10       Image:         msdtc.exe
        Wait Start TickCount      7530           Ticks: 39049 (0:00:10:09.168)
        Context Switch Count      30                 LargeStack
        UserTime                  00:00:00.031
        KernelTime                00:00:00.031
        Win32 Start Address msdtc!wWinMainCRTStartup (0x0000000000ca207c)
        Stack Init fffff9800e4e2db0 Current fffff9800e4e27f0
        Base fffff9800e4e3000 Limit fffff9800e4db000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 3 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0e4e2830 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0e4e2970 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`0e4e29d0 fffff800`01ebdf16 nt!KeWaitForSingleObject+0x5f5
        fffff980`0e4e2a50 fffff800`01ea1a24 nt!IopSynchronousServiceTail+0x306
        fffff980`0e4e2ac0 fffff800`01c4d733 nt!NtReadFile+0x583
        fffff980`0e4e2bb0 00000000`76e202da nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0e4e2c20)
        00000000`0010f418 00000000`76bf26da ntdll!NtReadFile+0xa
        00000000`0010f420 000007fe`fea865aa kernel32!ReadFile+0x8a
        00000000`0010f4b0 000007fe`fea862e3 ADVAPI32!ScGetPipeInput+0x4a
        00000000`0010f590 000007fe`fea850f3 ADVAPI32!ScDispatcherLoop+0x9a
        00000000`0010f690 000007fe`f3bf2eaf ADVAPI32!StartServiceCtrlDispatcherW+0x176
        00000000`0010f930 000007fe`f3befaf4 MSDTCTM!CDtcService::Start+0x6f
        00000000`0010f9b0 00000000`00ca1719 MSDTCTM!DtcMainExt+0x994
        00000000`0010fa70 00000000`00ca1eea msdtc!wWinMain+0x1e1
        00000000`0010fab0 00000000`76bfcdcd msdtc!operator new+0x296
        00000000`0010fb70 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0010fba0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8002048060  Cid 0ca4.0cb4  Teb: 000007fffffda000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8001ffcbb0  Thread
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa8002043c10       Image:         msdtc.exe
        Wait Start TickCount      7655           Ticks: 38924 (0:00:10:07.218)
        Context Switch Count      186
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ADVAPI32!ScSvcctrlThreadW (0x000007fefea84bd0)
        Stack Init fffff9801db96db0 Current fffff9801db96960
        Base fffff9801db97000 Limit fffff9801db91000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1db969a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1db96ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`1db96b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`1db96bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`1db96c20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1db96c20)
        00000000`02eff868 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`02eff870 000007fe`f3bf3d75 kernel32!WaitForSingleObjectEx+0x9c
        00000000`02eff930 000007fe`fea84bf5 MSDTCTM!ServiceMain+0x3d5
        00000000`02eff9f0 00000000`76bfcdcd ADVAPI32!ScSvcctrlThreadW+0x25
        00000000`02effa20 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02effa50 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8001ffcbb0  Cid 0ca4.0cd4  Teb: 000007fffffd8000 Win32Thread: fffff900c07f7010
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa80020abab0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa8002043c10       Image:         msdtc.exe
        Wait Start TickCount      7655           Ticks: 38924 (0:00:10:07.218)
        Context Switch Count      161                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.046
        Win32 Start Address MSDTCTM!DTCDummy (0x000007fef3bf3960)
        Stack Init fffff980158f7db0 Current fffff980158f7740
        Base fffff980158f8000 Limit fffff980158f1000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`158f7780 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`158f78c0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`158f7920 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`158f79a0 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`158f7a40 fffff960`000c7e1e win32k!xxxSleepThread+0x56
        fffff980`158f7a70 fffff960`000c7f25 win32k!xxxRealInternalGetMessage+0x72e
        fffff980`158f7b50 fffff960`000c97e4 win32k!xxxInternalGetMessage+0x35
        fffff980`158f7b90 fffff800`01c4d733 win32k!NtUserGetMessage+0x64
        fffff980`158f7c20 00000000`76d1e6aa nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`158f7c20)
        00000000`02bffc98 00000000`76d1bf4e USER32!ZwUserGetMessage+0xa
        00000000`02bffca0 000007fe`f3bf0cc7 USER32!GetMessageA+0xc3
        00000000`02bffcd0 000007fe`f3bf397a MSDTCTM!DtcMain+0x867
        00000000`02bffe10 00000000`76bfcdcd MSDTCTM!DTCDummy+0x1a
        00000000`02bffe40 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02bffe70 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8002088bb0  Cid 0ca4.0cf4  Teb: 000007fffffd4000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800208f8f0  SynchronizationEvent
            fffffa800208f890  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa8002043c10       Image:         msdtc.exe
        Wait Start TickCount      7652           Ticks: 38927 (0:00:10:07.265)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address MSDTCTM!ThreadProc (0x000007fef3c152d0)
        Stack Init fffff9801dbeadb0 Current fffff9801dbea260
        Base fffff9801dbeb000 Limit fffff9801dbe5000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1dbea2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1dbea3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`1dbea440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`1dbea4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`1dbea960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`1dbeabb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1dbeac20)
        00000000`032efd78 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`032efd80 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`032efe90 000007fe`f3c1539b kernel32!WaitForMultipleObjects+0x11
        00000000`032efed0 00000000`76bfcdcd MSDTCTM!ThreadProc+0xcb
        00000000`032eff40 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`032eff70 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8002046bb0  Cid 0ca4.0cfc  Teb: 000007fffffae000 Win32Thread: 0000000000000000
WAIT: (DelayExecution) UserMode Non-Alertable
            fffffa8002046c68  NotificationTimer
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa8002043c10       Image:         msdtc.exe
        Wait Start TickCount      46577          Ticks: 2 (0:00:00:00.031)
        Context Switch Count      5734
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address MSDTCPRX!CConnectionManager::TimerProc (0x000007fef42e14b0)
        Stack Init fffff9801dbf8db0 Current fffff9801dbf8990
        Base fffff9801dbf9000 Limit fffff9801dbf3000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1dbf89d0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1dbf8b10 fffff800`01c5b5a9 nt!KiSwapThread+0x125
        fffff980`1dbf8b70 fffff800`01e8ae9d nt!KeDelayExecutionThread+0x339
        fffff980`1dbf8bf0 fffff800`01c4d733 nt!NtDelayExecution+0x5c
        fffff980`1dbf8c20 00000000`76e205ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1dbf8c20)
        00000000`024cf798 00000000`76bfd908 ntdll!NtDelayExecution+0xa
        00000000`024cf7a0 000007fe`f42e1a25 kernel32!SleepEx+0x84
        00000000`024cf820 000007fe`f42e14c4
MSDTCPRX!CConnectionManager::TimerProcForGuardedUser+0x3b5
        00000000`024cf8d0 00000000`76bfcdcd MSDTCPRX!CConnectionManager::TimerProc+0x14
        00000000`024cf900 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`024cf930 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa8002050bb0  Cid 0ca4.0d08  Teb: 000007fffffaa000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800204cd00  NotificationEvent
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa8002043c10       Image:         msdtc.exe
        Wait Start TickCount      7651           Ticks: 38928 (0:00:10:07.280)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address MSDTCPRX!CConnectionManager::TimerProc (0x000007fef42e14b0)
        Stack Init fffff9801db2ddb0 Current fffff9801db2d960
        Base fffff9801db2e000 Limit fffff9801db28000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1db2d9a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1db2dae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`1db2db40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`1db2dbc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`1db2dc20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1db2dc20)
        00000000`0352f778 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`0352f780 000007fe`f42e15f6 kernel32!WaitForSingleObjectEx+0x9c
        00000000`0352f840 000007fe`f42e14cb
MSDTCPRX!CConnectionManager::TimerProcForNonGuardedUser+0x116
        00000000`0352f8a0 00000000`76bfcdcd MSDTCPRX!CConnectionManager::TimerProc+0x1b
        00000000`0352f8d0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0352f900 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80020529f0  Cid 0ca4.0d10  Teb: 000007fffffa8000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8002052e80  NotificationEvent
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa8002043c10       Image:         msdtc.exe
        Wait Start TickCount      7973           Ticks: 38606 (0:00:10:02.257)
        Context Switch Count      9
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address MSDTCTM!UIServerThread (0x000007fef3c2bf30)
        Stack Init fffff9801dbe3db0 Current fffff9801dbe3960
        Base fffff9801dbe4000 Limit fffff9801dbde000 Call 0
        Priority 13 BasePriority 8 PriorityDecrement 5 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1dbe39a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1dbe3ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`1dbe3b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`1dbe3bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`1dbe3c20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1dbe3c20)
        00000000`0366f628 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`0366f630 000007fe`f3c2c50c kernel32!WaitForSingleObjectEx+0x9c
        00000000`0366f6f0 00000000`76bfcdcd MSDTCTM!UIServerThread+0x5dc
        00000000`0366f7a0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0366f7d0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa800205c9e0  Cid 0ca4.0d14  Teb: 000007fffffa6000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800205ce70  NotificationEvent
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa8002043c10       Image:         msdtc.exe
        Wait Start TickCount      7651           Ticks: 38928 (0:00:10:07.280)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address MSDTCPRX!CConnectionManager::TimerProc (0x000007fef42e14b0)
        Stack Init fffff9801db3bdb0 Current fffff9801db3b960
        Base fffff9801db3c000 Limit fffff9801db36000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1db3b9a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1db3bae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`1db3bb40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`1db3bbc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`1db3bc20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1db3bc20)
        00000000`036ef678 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`036ef680 000007fe`f42e15f6 kernel32!WaitForSingleObjectEx+0x9c
        00000000`036ef740 000007fe`f42e14cb
MSDTCPRX!CConnectionManager::TimerProcForNonGuardedUser+0x116
        00000000`036ef7a0 00000000`76bfcdcd MSDTCPRX!CConnectionManager::TimerProc+0x1b
        00000000`036ef7d0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`036ef800 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8002079a70  Cid 0ca4.0d18  Teb: 000007fffffa4000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8002079f00  NotificationEvent
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa8002043c10       Image:         msdtc.exe
        Wait Start TickCount      7656           Ticks: 38923 (0:00:10:07.202)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address MSDTCPRX!CConnectionManager::TimerProc (0x000007fef42e14b0)
        Stack Init fffff9801db42db0 Current fffff9801db42960
        Base fffff9801db43000 Limit fffff9801db3d000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1db429a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1db42ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`1db42b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`1db42bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`1db42c20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1db42c20)
        00000000`0323fc58 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`0323fc60 000007fe`f42e1a13 kernel32!WaitForSingleObjectEx+0x9c
        00000000`0323fd20 000007fe`f42e14c4
MSDTCPRX!CConnectionManager::TimerProcForGuardedUser+0x3a3
        00000000`0323fdd0 00000000`76bfcdcd MSDTCPRX!CConnectionManager::TimerProc+0x14
        00000000`0323fe00 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0323fe30 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80020acbb0  Cid 0ca4.0d28  Teb: 000007fffffa2000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80020abd40  SynchronizationEvent
            fffffa80020abce0  SynchronizationEvent
            fffffa80020abc80  SynchronizationEvent
            fffffa80020abc20  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa8002043c10       Image:         msdtc.exe
        Wait Start TickCount      8432           Ticks: 38147 (0:00:09:55.097)
        Context Switch Count      1128
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address MSDTCLOG!_FlushThread (0x000007fef4d8af90)
        Stack Init fffff9801db57db0 Current fffff9801db57260
        Base fffff9801db58000 Limit fffff9801db52000 Call 0
        Priority 10 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1db572a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1db573e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`1db57440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`1db574b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`1db57960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`1db57bb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1db57c20)
        00000000`0392f0f8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0392f100 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0392f210 000007fe`f4d8b0ad kernel32!WaitForMultipleObjects+0x11
        00000000`0392f250 00000000`76bfcdcd MSDTCLOG!_FlushThread+0x11d
        00000000`0392fac0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0392faf0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80020b3bb0  Cid 0ca4.0d38  Teb: 000007fffff9c000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8002067270  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa8002043c10       Image:         msdtc.exe
        Wait Start TickCount      46507          Ticks: 72 (0:00:00:01.123)
        Context Switch Count      226
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address MSDTCPRX!CSessionObject::MaintainSession (0x000007fef42eb840)
        Stack Init fffff9801db6cdb0 Current fffff9801db6c960
        Base fffff9801db6d000 Limit fffff9801db67000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1db6c9a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1db6cae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`1db6cb40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`1db6cbc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`1db6cc20 00000000`76e202ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1db6cc20)
        00000000`0389faa8 00000000`76bfd820 ntdll!NtWaitForSingleObject+0xa
        00000000`0389fab0 000007fe`f42edd79 kernel32!WaitForSingleObjectEx+0x9c
        00000000`0389fb70 000007fe`f42eba8f MSDTCPRX!CSessionObject::MaintainItInUpState+0x359
        00000000`0389fe30 000007fe`f42eb84e MSDTCPRX!CSessionObject::MaintainIt+0x22f
        00000000`0389fea0 00000000`76bfcdcd MSDTCPRX!CSessionObject::MaintainSession+0xe
        00000000`0389fed0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0389ff00 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa800202abb0  Cid 0ca4.0eb8  Teb: 000007fffffd6000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa80020434c0  QueueObject
            fffffa800202ac68  NotificationTimer
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa8002043c10       Image:         msdtc.exe
        Wait Start TickCount      45951          Ticks: 628 (0:00:00:09.796)
        Context Switch Count      9
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff9801085fdb0 Current fffff9801085f810
        Base fffff98010860000 Limit fffff9801085a000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1085f850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1085f990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`1085f9f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`1085fa80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`1085fb00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`1085fbb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1085fc20)
        00000000`0312f8f8 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`0312f900 000007fe`fedce7a3 kernel32!GetQueuedCompletionStatus+0x48
        00000000`0312f960 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`0312f9f0 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`0312faa0 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`0312fad0 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`0312fb10 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`0312fb40 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0312fb70 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80045b37f0  Cid 0ca4.0dc0  Teb: 000007fffffac000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa80020434c0  QueueObject
            fffffa80045b38a8  NotificationTimer
        Not impersonating
        DeviceMap                 fffff8800598a680
        Owning Process            fffffa8002043c10       Image:         msdtc.exe
        Wait Start TickCount      46371          Ticks: 208 (0:00:00:03.244)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff9801036cdb0 Current fffff9801036c810
        Base fffff9801036d000 Limit fffff98010367000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1036c850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1036c990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`1036c9f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`1036ca80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`1036cb00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`1036cbb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1036cc20)
        00000000`02f9fa98 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`02f9faa0 000007fe`fedce7a3 kernel32!GetQueuedCompletionStatus+0x48
        00000000`02f9fb00 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`02f9fb90 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`02f9fc40 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`02f9fc70 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`02f9fcb0 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`02f9fce0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`02f9fd10 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

Ieuser process

```
PROCESS fffffa800253fae0
    SessionId: 1  Cid: 0958    Peb: 7efdf000  ParentCid: 0880
    DirBase: 4afd4000  ObjectTable: fffff880079b80f0  HandleCount: 257.
    Image: ieuser.exe
    VadRoot fffffa800229e6c0 Vads 142 Clone 0 Private 659. Modified 4. Locked 0.
    DeviceMap fffff88006100250
    Token                             fffff880079b1060
    ElapsedTime                       00:08:49.458
    UserTime                          00:00:00.046
    KernelTime                        00:00:00.124
    QuotaPoolUsage[PagedPool]         172160
    QuotaPoolUsage[NonPagedPool]      13984
    Working Set Sizes (now,min,max)  (2646, 50, 345) (10584KB, 200KB, 1380KB)
    PeakWorkingSetSize                2708
    VirtualSize                       83 Mb
    PeakVirtualSize                   92 Mb
    PageFaultCount                    3045
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      1114

    Setting context for this process...
.process /p /r fffffa800253fae0

    !peb
PEB at 000000007efdf000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         0000000000640000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00000000002e2a70 . 00000000002e2dd0
    Ldr.InLoadOrderModuleList:           00000000002e2980 . 00000000002e2f30
    Ldr.InMemoryOrderModuleList:         00000000002e2990 . 00000000002e2f40
            Base TimeStamp                     Module
          640000 470c3335 Oct 10 03:04:37 2007 C:\Program Files (x86)\Internet Explorer\ieuser.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        75110000 4549d371 Nov 02 11:16:01 2006 C:\Windows\system32\wow64.dll
        75000000 4549d374 Nov 02 11:16:04 2006 C:\Windows\system32\wow64win.dll
        75100000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\wow64cpu.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       00000000002e0000
    ProcessParameters: 00000000002e1f40
    WindowTitle:  'C:\Program Files (x86)\Internet Explorer\ieuser.exe'
    ImageFile:    'C:\Program Files (x86)\Internet Explorer\ieuser.exe'
    CommandLine:  '"C:\Program Files (x86)\Internet Explorer\ieuser.exe" -Embedding'
    DllPath:      'C:\Program Files (x86)\Internet
Explorer;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Program Files\Internet
Explorer;;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem'
    Environment:  00000000002e1310
        =::=::\
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\UserName\AppData\Roaming
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        HKCU_S=\REGISTRY\CUSER\Software
        HKLM_S=\REGISTRY\MACHINE\Software
        HOMEDRIVE=C:
        HOMEPATH=\Users\UserName
        LOCALAPPDATA=C:\Users\UserName\AppData\Local
        LOGONSERVER=\\COMPUTERNAME
```

```
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Program Files\Internet
Explorer;;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public
        SESSIONNAME=Console
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Users\UserName\AppData\Local\Temp
        TMP=C:\Users\UserName\AppData\Local\Temp
        USERDOMAIN=COMPUTERNAME
        USERNAME=UserName
        USERPROFILE=C:\Users\UserName
        windir=C:\Windows


        THREAD fffffa80025a49c0  Cid 0958.0878  Teb: 000000007efdb000 Win32Thread: fffff900c1e8d2e0
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800405e430  NotificationEvent
            fffffa8001e1c490  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa800253fae0       Image:         ieuser.exe
        Wait Start TickCount      15650          Ticks: 30929 (0:00:08:02.495)
        Context Switch Count      77                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.078
        Win32 Start Address ieuser!wWinMainCRTStartup (0x0000000000645301)
        Stack Init fffff98004e7bdb0 Current fffff98004e7b260
        Base fffff98004e7c000 Limit fffff98004e73000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`04e7b2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`04e7b3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`04e7b440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`04e7b4b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`04e7b960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`04e7bbb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`04e7bc20)
        00000000`0011e808 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`0011e8b0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0011e8e0 00000000`76e0e23d wow64!Wow64LdrpInitialize+0x492
        00000000`0011ee40 00000000`76e7e974 ntdll!LdrpInitializeProcess+0x1333
        00000000`0011f0d0 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d641
        00000000`0011f170 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa80025d96b0  Cid 0958.0ec0  Teb: 000000007efa7000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa80025c4820  SynchronizationTimer
            fffffa8001f015a0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa800253fae0       Image:         ieuser.exe
        Wait Start TickCount      44051          Ticks: 2528 (0:00:00:39.437)
        Context Switch Count      24
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x0000000077046235
        Stack Init fffff9801db5edb0 Current fffff9801db5e260
        Base fffff9801db5f000 Limit fffff9801db59000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1db5e2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1db5e3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`1db5e440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`1db5e4b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`1db5e960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`1db5ebb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1db5ec20)
        00000000`022def18 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`022defc0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`022deff0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`022df550 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`022df5f0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa8002583700  Cid 0958.0f24  Teb: 000000007efa4000 Win32Thread: fffff900c22d1820
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa80043eecf0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa800253fae0       Image:         ieuser.exe
        Wait Start TickCount      36304          Ticks: 10275 (0:00:02:40.291)
        Context Switch Count      12                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000000007600fc53
        Stack Init fffff98020d54db0 Current fffff98020d54740
        Base fffff98020d55000 Limit fffff98020d4d000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`20d54780 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`20d548c0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`20d54920 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`20d549a0 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`20d54a40 fffff960`000c7e1e win32k!xxxSleepThread+0x56
        fffff980`20d54a70 fffff960`000c7f25 win32k!xxxRealInternalGetMessage+0x72e
        fffff980`20d54b50 fffff960`000c97e4 win32k!xxxInternalGetMessage+0x35
        fffff980`20d54b90 fffff800`01c4d733 win32k!NtUserGetMessage+0x64
        fffff980`20d54c20 00000000`75039f7a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`20d54c20)
        00000000`0279e4f8 00000000`75023160 wow64win!ZwUserGetMessage+0xa
        00000000`0279e500 00000000`7511aa4e wow64win!whNtUserGetMessage+0x30
        00000000`0279e560 00000000`75103678 wow64!Wow64SystemServiceEx+0xca
        00000000`0279ee10 00000000`7511abfe wow64cpu!TurboDispatchJumpAddressEnd+0x28
        00000000`0279eea0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0279eed0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0279f430 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0279f4d0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa8004bd6bb0  Cid 0958.0d70  Teb: 000000007efd5000 Win32Thread: fffff900c223f580
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa80020da9b0  QueueObject
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa800253fae0       Image:         ieuser.exe
        Wait Start TickCount      45975          Ticks: 604 (0:00:00:09.422)
        Context Switch Count      13                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x00000000762f3242
        Stack Init fffff9801e4b7db0 Current fffff9801e4b7810
        Base fffff9801e4b8000 Limit fffff9801e4b1000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1e4b7850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1e4b7990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`1e4b79f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`1e4b7a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`1e4b7b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`1e4b7bb0 00000000`751039a2 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1e4b7c20)
        00000000`02b2e9f8 00000000`7511abfe wow64cpu!RemoveIoCompletionFault+0x41
        00000000`02b2ead0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`02b2eb00 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`02b2f060 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`02b2f100 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

Iexplore process

```
PROCESS fffffa80025aac10
    SessionId: 1  Cid: 0d8c    Peb: 7efdf000  ParentCid: 0880
    DirBase: 3ece5000  ObjectTable: fffff8800283fd30  HandleCount: 421.
    Image: iexplore.exe
    VadRoot fffffa80025c93a0 Vads 337 Clone 0 Private 2385. Modified 416. Locked 0.
    DeviceMap fffff88006100250
    Token                             fffff880079d5060
    ElapsedTime                       00:08:49.364
    UserTime                          00:00:00.140
    KernelTime                        00:00:00.109
    QuotaPoolUsage[PagedPool]         240120
    QuotaPoolUsage[NonPagedPool]      36064
    Working Set Sizes (now,min,max)  (7660, 50, 345) (30640KB, 200KB, 1380KB)
    PeakWorkingSetSize                7830
    VirtualSize                       157 Mb
    PeakVirtualSize                   181 Mb
    PageFaultCount                    9467
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      6230

    Setting context for this process...
.process /p /r fffffa80025aac10

    !peb
PEB at 000000007efdf000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         0000000000ca0000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00000000003d2a60 . 00000000003d2dc0
    Ldr.InLoadOrderModuleList:           00000000003d2970 . 00000000003d2f20
    Ldr.InMemoryOrderModuleList:         00000000003d2980 . 00000000003d2f30
            Base TimeStamp                     Module
          ca0000 470c3339 Oct 10 03:04:41 2007 C:\Program Files (x86)\Internet
Explorer\iexplore.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        75110000 4549d371 Nov 02 11:16:01 2006 C:\Windows\system32\wow64.dll
        75000000 4549d374 Nov 02 11:16:04 2006 C:\Windows\system32\wow64win.dll
        75100000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\wow64cpu.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       00000000003d0000
    ProcessParameters: 00000000003d1f40
    WindowTitle:  'C:\Program Files (x86)\Internet Explorer\iexplore.exe'
    ImageFile:    'C:\Program Files (x86)\Internet Explorer\iexplore.exe'
    CommandLine:  '"C:\Program Files (x86)\Internet Explorer\iexplore.exe" '
    DllPath:      'C:\Program Files (x86)\Internet
Explorer;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Program Files\Internet
Explorer;;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem'
    Environment:  00000000003d1310
        =::=::\
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\UserName\AppData\Roaming
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        HKCU_S=\REGISTRY\CUSER\Software
        HKLM_S=\REGISTRY\MACHINE\Software
        HOMEDRIVE=C:
        HOMEPATH=\Users\UserName
        LOCALAPPDATA=C:\Users\UserName\AppData\Local
```

```
        LOGONSERVER=\\COMPUTERNAME
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Program Files\Internet
Explorer;;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public
        SESSIONNAME=Console
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Users\UserName\AppData\Local\Temp
        TMP=C:\Users\UserName\AppData\Local\Temp
        USERDOMAIN=COMPUTERNAME
        USERNAME=UserName
        USERPROFILE=C:\Users\UserName
        windir=C:\Windows


        THREAD fffffa800259d060  Cid 0d8c.0dc8  Teb: 000000007efdb000 Win32Thread: fffff900c1e53460
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800229fd10  SynchronizationEvent
            fffffa80025c31d0  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa80025aac10       Image:         iexplore.exe
        Wait Start TickCount      35815          Ticks: 10764 (0:00:02:47.919)
        Context Switch Count      3239                 LargeStack
        UserTime                  00:00:00.171
        KernelTime                00:00:00.468
        Win32 Start Address iexplore!wWinMainCRTStartup (0x0000000000ca2e2d)
        Stack Init fffff9800d12edb0 Current fffff9800d12e260
        Base fffff9800d12f000 Limit fffff9800d124000 Call 0
        Priority 14 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0d12e2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0d12e3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0d12e440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0d12e4b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`0d12e960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`0d12ebb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0d12ec20)
        00000000`000fe848 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`000fe8f0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`000fe920 00000000`76e0e23d wow64!Wow64LdrpInitialize+0x492
        00000000`000fee80 00000000`76e7e974 ntdll!LdrpInitializeProcess+0x1333
        00000000`000ff110 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d641
        00000000`000ff1b0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa80025d17c0  Cid 0d8c.03b0  Teb: 000000007efad000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa80023ad310  SynchronizationTimer
            fffffa80021dbd70  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa80025aac10       Image:         iexplore.exe
        Wait Start TickCount      44051          Ticks: 2528 (0:00:00:39.437)
        Context Switch Count      34
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x0000000077046235
        Stack Init fffff9800b6a9db0 Current fffff9800b6a9260
        Base fffff9800b6aa000 Limit fffff9800b6a4000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0b6a92a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0b6a93e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0b6a9440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0b6a94b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`0b6a9960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`0b6a9bb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0b6a9c20)
        00000000`004cee28 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`004ceed0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`004cef00 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`004cf460 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`004cf500 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa80021b8bb0  Cid 0d8c.0ed4  Teb: 000000007efa7000 Win32Thread: fffff900c06d8d60
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80022baba0  SynchronizationEvent
            fffffa8002279600  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa80025aac10       Image:         iexplore.exe
        Wait Start TickCount      12709          Ticks: 33870 (0:00:08:48.375)
        Context Switch Count      3                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x00000000768c639b
        Stack Init fffff9800dbd9db0 Current fffff9800dbd9260
        Base fffff9800dbda000 Limit fffff9800dbd3000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`0dbd92a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0dbd93e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`0dbd9440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`0dbd94b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`0dbd9960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`0dbd9bb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0dbd9c20)
        00000000`0051ed48 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`0051edf0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0051ee20 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0051f380 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0051f420 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa80023fe480  Cid 0d8c.0ec8  Teb: 000000007efa4000 Win32Thread: fffff900c26bbd60
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa8001eae760  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa80025aac10       Image:         iexplore.exe
        Wait Start TickCount      35815          Ticks: 10764 (0:00:02:47.919)
        Context Switch Count      2714                 LargeStack
        UserTime                  00:00:00.249
        KernelTime                00:00:00.577
        Win32 Start Address 0x00000000718ce424
        Stack Init fffff98012f0adb0 Current fffff98012f0a8c0
        Base fffff98012f0b000 Limit fffff98012f01000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`12f0a900 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`12f0aa40 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`12f0aaa0 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`12f0ab20 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`12f0abc0 fffff960`000dc057 win32k!xxxSleepThread+0x56
        fffff980`12f0abf0 fffff800`01c4d733 win32k!NtUserWaitMessage+0x37
        fffff980`12f0ac20 00000000`75103cf9 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`12f0ac20)
        00000000`03e0e998 00000000`75103cb5 wow64cpu!CpupSyscallStub+0x9
        00000000`03e0e9a0 00000000`7511abfe wow64cpu!Thunk0Arg+0x5
        00000000`03e0ea10 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`03e0ea40 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`03e0efa0 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`03e0f040 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa800249dbb0  Cid 0d8c.0ec4  Teb: 000000007efa1000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Alertable
            fffffa80025d4de0  NotificationEvent
            fffffa800249dc68  NotificationTimer
        IRP List:
            fffffa800218a420: (0006,03a0) Flags: 00060070  Mdl: 00000000
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa80025aac10       Image:         iexplore.exe
        Wait Start TickCount      13514          Ticks: 33065 (0:00:08:35.817)
        Context Switch Count      68
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x0000000076602a8b
        Stack Init fffff98001481db0 Current fffff98001481960
        Base fffff98001482000 Limit fffff9800147c000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`014819a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`01481ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`01481b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`01481bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`01481c20 00000000`75103cf9 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`01481c20)
        00000000`03dbeb88 00000000`75103af6 wow64cpu!CpupSyscallStub+0x9
        00000000`03dbeb90 00000000`7511abfe wow64cpu!Thunk0ArgReloadState+0x1a
        00000000`03dbec00 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`03dbec30 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`03dbf190 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`03dbf230 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa80025d7bb0  Cid 0d8c.0f14  Teb: 000000007ef98000 Win32Thread: fffff900c06f9370
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8001fb2ae0  SynchronizationEvent
            fffffa80025d7c68  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa80025aac10       Image:         iexplore.exe
        Wait Start TickCount      13116          Ticks: 33463 (0:00:08:42.026)
        Context Switch Count      30                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address 0x0000000070deda47
        Stack Init fffff98020dffdb0 Current fffff98020dff960
        Base fffff98020e00000 Limit fffff98020df8000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`20dff9a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`20dffae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`20dffb40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`20dffbc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`20dffc20 00000000`75103cf9 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`20dffc20)
        00000000`0448ea18 00000000`75103af6 wow64cpu!CpupSyscallStub+0x9
        00000000`0448ea20 00000000`7511abfe wow64cpu!Thunk0ArgReloadState+0x1a
        00000000`0448ea90 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0448eac0 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0448f020 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0448f0c0 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa8002586060  Cid 0d8c.0f3c  Teb: 000000007ef92000 Win32Thread: fffff900c1e9d460
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa80025de240  SynchronizationEvent
            fffffa8002586118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa80025aac10       Image:         iexplore.exe
        Wait Start TickCount      13160          Ticks: 33419 (0:00:08:41.339)
        Context Switch Count      76                 LargeStack
        UserTime                  00:00:00.031
        KernelTime                00:00:00.031
        Win32 Start Address 0x0000000070deda47
        Stack Init fffff980109b3db0 Current fffff980109b3960
        Base fffff980109b4000 Limit fffff980109ac000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`109b39a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`109b3ae0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`109b3b40 fffff800`01e8af4b nt!KeWaitForSingleObject+0x5f5
        fffff980`109b3bc0 fffff800`01c4d733 nt!NtWaitForSingleObject+0x9b
        fffff980`109b3c20 00000000`75103cf9 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`109b3c20)
        00000000`03fdf0d8 00000000`75103af6 wow64cpu!CpupSyscallStub+0x9
        00000000`03fdf0e0 00000000`7511abfe wow64cpu!Thunk0ArgReloadState+0x1a
        00000000`03fdf150 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`03fdf180 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`03fdf6e0 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`03fdf780 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa8001ffb700  Cid 0d8c.0f54  Teb: 000000007ef8f000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa800253d360  QueueObject
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa80025aac10       Image:         iexplore.exe
        Wait Start TickCount      13038          Ticks: 33541 (0:00:08:43.242)
        Context Switch Count      76
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address 0x00000000714742d7
        Stack Init fffff9801a69fdb0 Current fffff9801a69f810
        Base fffff9801a6a0000 Limit fffff9801a69a000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1a69f850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1a69f990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`1a69f9f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`1a69fa80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`1a69fb00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`1a69fbb0 00000000`751039a2 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1a69fc20)
        00000000`0510ee88 00000000`7511abfe wow64cpu!RemoveIoCompletionFault+0x41
        00000000`0510ef60 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0510ef90 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0510f4f0 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0510f590 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa800260fbb0  Cid 0d8c.0f48  Teb: 000000007ef8c000 Win32Thread: fffff900c0134690
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa8002142220  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa80025aac10       Image:         iexplore.exe
        Wait Start TickCount      13032          Ticks: 33547 (0:00:08:43.336)
        Context Switch Count      4                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x0000000071478675
        Stack Init fffff98020d08db0 Current fffff98020d08740
        Base fffff98020d09000 Limit fffff98020d02000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`20d08780 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`20d088c0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`20d08920 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`20d089a0 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`20d08a40 fffff960`000c7e1e win32k!xxxSleepThread+0x56
        fffff980`20d08a70 fffff960`000c7f25 win32k!xxxRealInternalGetMessage+0x72e
        fffff980`20d08b50 fffff960`000c97e4 win32k!xxxInternalGetMessage+0x35
        fffff980`20d08b90 fffff800`01c4d733 win32k!NtUserGetMessage+0x64
        fffff980`20d08c20 00000000`75039f7a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`20d08c20)
        00000000`04c0e778 00000000`75023160 wow64win!ZwUserGetMessage+0xa
        00000000`04c0e780 00000000`7511aa4e wow64win!whNtUserGetMessage+0x30
        00000000`04c0e7e0 00000000`75103678 wow64!Wow64SystemServiceEx+0xca
        00000000`04c0f090 00000000`7511abfe wow64cpu!TurboDispatchJumpAddressEnd+0x28
        00000000`04c0f120 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`04c0f150 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`04c0f6b0 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`04c0f750 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

```
        THREAD fffffa80028ad260  Cid 0d8c.0f58  Teb: 000000007ef89000 Win32Thread: fffff900c0129ad0
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa8002579b80  SynchronizationEvent
            fffffa80021c1290  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa80025aac10       Image:         iexplore.exe
        Wait Start TickCount      13105          Ticks: 33474 (0:00:08:42.197)
        Context Switch Count      411                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address 0x0000000071478544
        Stack Init fffff98020d2edb0 Current fffff98020d2e260
        Base fffff98020d2f000 Limit fffff98020d28000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`20d2e2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`20d2e3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`20d2e440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`20d2e4b0 fffff800`01fa52fa nt!ObpWaitForMultipleObjects+0x216
        fffff980`20d2e960 fffff800`01c4d733 nt!NtWaitForMultipleObjects32+0xd9
        fffff980`20d2ebb0 00000000`7510373f nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`20d2ec20)
        00000000`0442f028 00000000`7511abfe wow64cpu!WaitForMultipleObjects32+0x3a
        00000000`0442f0d0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`0442f100 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`0442f660 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`0442f700 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa8001ec7bb0  Cid 0d8c.0f44  Teb: 000000007ef86000 Win32Thread: fffff900c1e9f820
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa80044d7610  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa80025aac10       Image:         iexplore.exe
        Wait Start TickCount      15651          Ticks: 30928 (0:00:08:02.479)
        Context Switch Count      49                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x0000000073f81385
        Stack Init fffff98020d41db0 Current fffff98020d41740
        Base fffff98020d42000 Limit fffff98020d3a000 Call 0
        Priority 12 BasePriority 10 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`20d41780 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`20d418c0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`20d41920 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`20d419a0 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`20d41a40 fffff960`000c7e1e win32k!xxxSleepThread+0x56
        fffff980`20d41a70 fffff960`000c7f25 win32k!xxxRealInternalGetMessage+0x72e
        fffff980`20d41b50 fffff960`000c97e4 win32k!xxxInternalGetMessage+0x35
        fffff980`20d41b90 fffff800`01c4d733 win32k!NtUserGetMessage+0x64
        fffff980`20d41c20 00000000`75039f7a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`20d41c20)
        00000000`051fe1b8 00000000`75023160 wow64win!ZwUserGetMessage+0xa
        00000000`051fe1c0 00000000`7511aa4e wow64win!whNtUserGetMessage+0x30
        00000000`051fe220 00000000`75103678 wow64!Wow64SystemServiceEx+0xca
        00000000`051fead0 00000000`7511abfe wow64cpu!TurboDispatchJumpAddressEnd+0x28
        00000000`051feb60 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`051feb90 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`051ff0f0 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`051ff190 00000000`00000000 ntdll!LdrInitializeThunk+0xe

        THREAD fffffa8004526060  Cid 0d8c.0a8c  Teb: 000000007efd8000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa80042da940  QueueObject
        Not impersonating
        DeviceMap                 fffff88006100250
```

```
        Owning Process            fffffa80025aac10       Image:         iexplore.exe
        Wait Start TickCount      45975          Ticks: 604 (0:00:00:09.422)
        Context Switch Count      18
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x00000000762f3242
        Stack Init fffff98020c89db0 Current fffff98020c89810
        Base fffff98020c8a000 Limit fffff98020c84000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`20c89850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`20c89990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`20c899f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`20c89a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`20c89b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`20c89bb0 00000000`751039a2 nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`20c89c20)
        00000000`031aee18 00000000`7511abfe wow64cpu!RemoveIoCompletionFault+0x41
        00000000`031aeef0 00000000`7511a202 wow64!RunCpuSimulation+0xa
        00000000`031aef20 00000000`76df894c wow64!Wow64LdrpInitialize+0x492
        00000000`031af480 00000000`76e1c4ee ntdll! ?? ::FNODOBFM::`string'+0x1d777
        00000000`031af520 00000000`00000000 ntdll!LdrInitializeThunk+0xe
```

Notepad process

```
PROCESS fffffa800293d040
    SessionId: 1  Cid: 0ffc    Peb: 7fffffd3000  ParentCid: 0a84
    DirBase: 6a7fa000  ObjectTable: fffff88001834db0  HandleCount:  48.
    Image: notepad.exe
    VadRoot fffffa800499ed40 Vads 56 Clone 0 Private 340. Modified 2. Locked 0.
    DeviceMap fffff88006100250
    Token                             fffff88007b1b060
    ElapsedTime                       00:08:31.445
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         155672
    QuotaPoolUsage[NonPagedPool]      5280
    Working Set Sizes (now,min,max)  (1379, 50, 345) (5516KB, 200KB, 1380KB)
    PeakWorkingSetSize                1379
    VirtualSize                       77 Mb
    PeakVirtualSize                   77 Mb
    PageFaultCount                    1400
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      473

    Setting context for this process...
.process /p /r fffffa800293d040

    !peb
PEB at 000007fffffd3000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00000000ffec0000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 0000000000122830 . 000000000014a890
    Ldr.InLoadOrderModuleList:           0000000000122740 . 000000000014a870
    Ldr.InMemoryOrderModuleList:         0000000000122750 . 000000000014a880
            Base TimeStamp                     Module
        ffec0000 4549bb19 Nov 02 09:32:09 2006 C:\Windows\System32\notepad.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        76bc0000 4549d328 Nov 02 11:14:48 2006 C:\Windows\system32\kernel32.dll
     7fefea30000 4549d267 Nov 02 11:11:35 2006 C:\Windows\system32\ADVAPI32.dll
     7fefed90000 469c43bb Jul 17 05:21:15 2007 C:\Windows\system32\RPCRT4.dll
     7fefec20000 4549d273 Nov 02 11:11:47 2006 C:\Windows\system32\GDI32.dll
        76d00000 45d3ee19 Feb 15 05:22:33 2007 C:\Windows\system32\USER32.dll
     7fefdd40000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\system32\msvcrt.dll
     7fefeb30000 4549d32b Nov 02 11:14:51 2006 C:\Windows\system32\COMDLG32.dll
     7fefda10000 4549d31f Nov 02 11:14:39 2006 C:\Windows\system32\SHLWAPI.dll
     7fefbe70000 4549d32b Nov 02 11:14:51 2006 C:\Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_1559f1c6f365a7fa\COMCTL32.dll
     7fefddf0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\SHELL32.dll
     7fef8520000 4549d37c Nov 02 11:16:12 2006 C:\Windows\System32\WINSPOOL.DRV
     7fefd760000 4549d317 Nov 02 11:14:31 2006 C:\Windows\system32\ole32.dll
     7fefdab0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\OLEAUT32.dll
     7fefd9e0000 4549d2cb Nov 02 11:13:15 2006 C:\Windows\system32\IMM32.DLL
     7fefdc30000 4549d2e6 Nov 02 11:13:42 2006 C:\Windows\system32\MSCTF.dll
     7feff0c0000 4549d2a1 Nov 02 11:12:33 2006 C:\Windows\system32\LPK.DLL
     7fefd940000 4549d337 Nov 02 11:15:03 2006 C:\Windows\system32\USP10.dll
     7fefc330000 4549d33b Nov 02 11:15:07 2006 C:\Windows\System32\uxtheme.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       0000000000120000
    ProcessParameters: 0000000000121d90
    WindowTitle:  'C:\Users\UserName\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Accessories\Notepad.lnk'
    ImageFile:    'C:\Windows\System32\notepad.exe'
    CommandLine:  '"C:\Windows\System32\notepad.exe" '
```

```
    DllPath:
'C:\Windows\System32;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Wind
ows;C:\Windows\System32\Wbem'
    Environment:  0000000000121310
        =::=::\
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\UserName\AppData\Roaming
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        HOMEDRIVE=C:
        HOMEPATH=\Users\UserName
        LOCALAPPDATA=C:\Users\UserName\AppData\Local
        LOGONSERVER=\\COMPUTERNAME
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public
        SESSIONNAME=Console
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Users\UserName\AppData\Local\Temp
        TMP=C:\Users\UserName\AppData\Local\Temp
        USERDOMAIN=COMPUTERNAME
        USERNAME=UserName
        USERPROFILE=C:\Users\UserName
        windir=C:\Windows


        THREAD fffffa800293dbb0  Cid 0ffc.0ff8  Teb: 000007fffffde000 Win32Thread: fffff900c07aa7f0
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa8002916d70  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88006100250
        Owning Process            fffffa800293d040       Image:         notepad.exe
        Wait Start TickCount      15651          Ticks: 30928 (0:00:08:02.479)
        Context Switch Count      622                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.093
        Win32 Start Address notepad!WinMainCRTStartup (0x00000000ffecd134)
        Stack Init fffff98015711db0 Current fffff98015711740
        Base fffff98015712000 Limit fffff98015709000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`15711780 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`157118c0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`15711920 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`157119a0 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`15711a40 fffff960`000c7e1e win32k!xxxSleepThread+0x56
        fffff980`15711a70 fffff960`000c7f25 win32k!xxxRealInternalGetMessage+0x72e
        fffff980`15711b50 fffff960`000c97e4 win32k!xxxInternalGetMessage+0x35
        fffff980`15711b90 fffff800`01c4d733 win32k!NtUserGetMessage+0x64
        fffff980`15711c20 00000000`76d1e6aa nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`15711c20)
        00000000`0011f768 00000000`76d1e6ea USER32!ZwUserGetMessage+0xa
        00000000`0011f770 00000000`ffec6eca USER32!GetMessageW+0x34
        00000000`0011f7a0 00000000`ffeccf8b notepad!WinMain+0x176
        00000000`0011f820 00000000`76bfcdcd notepad!IsTextUTF8+0x24f
        00000000`0011f8e0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
```

```
        00000000`0011f910 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

WmiPrvSE process

```
PROCESS fffffa80025b7500
    SessionId: 0  Cid: 03d8    Peb: 7fffffde000  ParentCid: 0338
    DirBase: 2fcc3000  ObjectTable: fffff88006251630  HandleCount: 107.
    Image: WmiPrvSE.exe
    VadRoot fffffa8002092090 Vads 81 Clone 0 Private 504. Modified 2. Locked 0.
    DeviceMap fffff88000007820
    Token                             fffff880021e5060
    ElapsedTime                       00:07:37.397
    UserTime                          00:00:00.046
    KernelTime                        00:00:00.093
    QuotaPoolUsage[PagedPool]         93784
    QuotaPoolUsage[NonPagedPool]      7680
    Working Set Sizes (now,min,max)  (1808, 50, 345) (7232KB, 200KB, 1380KB)
    PeakWorkingSetSize                1808
    VirtualSize                       49 Mb
    PeakVirtualSize                   50 Mb
    PageFaultCount                    2079
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      904
    Job                               fffffa80048dfab0

    Setting context for this process...
.process /p /r fffffa80025b7500

    !peb
PEB at 000007fffffde000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00000000ffcf0000
    Ldr                       0000000076edf980
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00000000000e2790 . 000000000013c0e0
    Ldr.InLoadOrderModuleList:           00000000000e26a0 . 000000000013c190
    Ldr.InMemoryOrderModuleList:         00000000000e26b0 . 000000000013c1a0
            Base TimeStamp                     Module
        ffcf0000 4549b8cd Nov 02 09:22:21 2006 C:\Windows\system32\wbem\wmiprvse.exe
        76dd0000 4549d372 Nov 02 11:16:02 2006 C:\Windows\system32\ntdll.dll
        76bc0000 4549d328 Nov 02 11:14:48 2006 C:\Windows\system32\kernel32.dll
     7fefea30000 4549d267 Nov 02 11:11:35 2006 C:\Windows\system32\ADVAPI32.dll
     7fefed90000 469c43bb Jul 17 05:21:15 2007 C:\Windows\system32\RPCRT4.dll
        76d00000 45d3ee19 Feb 15 05:22:33 2007 C:\Windows\system32\USER32.dll
     7fefec20000 4549d273 Nov 02 11:11:47 2006 C:\Windows\system32\GDI32.dll
     7fefdd40000 4549d2e1 Nov 02 11:13:37 2006 C:\Windows\system32\msvcrt.dll
     7fef9f50000 4549d33d Nov 02 11:15:09 2006 C:\Windows\system32\wbem\wbemcomn.dll
     7fefdab0000 4549d31a Nov 02 11:14:34 2006 C:\Windows\system32\OLEAUT32.dll
     7fefd760000 4549d317 Nov 02 11:14:31 2006 C:\Windows\system32\ole32.dll
     7fef9040000 4549d274 Nov 02 11:11:48 2006 C:\Windows\system32\wbem\FastProx.dll
     7fefcdd0000 4549d375 Nov 02 11:16:05 2006 C:\Windows\system32\NTDSAPI.dll
     7fefce40000 4549d288 Nov 02 11:12:08 2006 C:\Windows\system32\DNSAPI.dll
     7fefd540000 4549d38a Nov 02 11:16:26 2006 C:\Windows\system32\WS2_32.dll
     7feff0b0000 4549d370 Nov 02 11:16:00 2006 C:\Windows\system32\NSI.dll
     7fefd590000 4549d396 Nov 02 11:16:38 2006 C:\Windows\system32\WLDAP32.dll
     7fefd530000 4549d310 Nov 02 11:14:24 2006 C:\Windows\system32\PSAPI.DLL
     7fefcf70000 4549d2fc Nov 02 11:14:04 2006 C:\Windows\system32\NETAPI32.dll
     7fefd390000 4549d33f Nov 02 11:15:11 2006 C:\Windows\system32\Secur32.dll
     7fefcea0000 4549d2ef Nov 02 11:13:51 2006 C:\Windows\system32\NCObjAPI.DLL
     7fefd9e0000 4549d2cb Nov 02 11:13:15 2006 C:\Windows\system32\IMM32.DLL
     7fefdc30000 4549d2e6 Nov 02 11:13:42 2006 C:\Windows\system32\MSCTF.dll
     7feff0c0000 4549d2a1 Nov 02 11:12:33 2006 C:\Windows\system32\LPK.DLL
```

```
     7fefd940000 4549d337 Nov 02 11:15:03 2006 C:\Windows\system32\USP10.dll
     7fefdb90000 4549d282 Nov 02 11:12:02 2006 C:\Windows\system32\CLBCatQ.DLL
     7fefc620000 4549d31d Nov 02 11:14:37 2006 C:\Windows\system32\rsaenh.dll
     7fef96d0000 4549d343 Nov 02 11:15:15 2006 C:\Windows\system32\wbem\wbemsvc.dll
     7fef96a0000 4549d3bd Nov 02 11:17:17 2006 C:\Windows\system32\wbem\wmiutils.dll
     7fef5010000 4549d3b8 Nov 02 11:17:12 2006 C:\Windows\system32\wbem\wmiprov.dll
        72540000 462444be Apr 17 04:53:34 2007 C:\Windows\system32\WMI.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       00000000000e0000
    ProcessParameters: 00000000000e1d20
    WindowTitle:  'C:\Windows\system32\wbem\wmiprvse.exe'
    ImageFile:    'C:\Windows\system32\wbem\wmiprvse.exe'
    CommandLine:  'C:\Windows\system32\wbem\wmiprvse.exe'
    DllPath:
'C:\Windows\system32\wbem;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:
\Windows;C:\Windows\System32\Wbem'
    Environment:  00000000000e1310
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\system32\config\systemprofile\AppData\Roaming
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        LOCALAPPDATA=C:\Windows\system32\config\systemprofile\AppData\Local
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=EM64T Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        PUBLIC=C:\Users\Public
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\TEMP
        TMP=C:\Windows\TEMP
        USERDOMAIN=DOMAIN
        USERNAME=COMPUTERNAME$
        USERPROFILE=C:\Windows\system32\config\systemprofile
        windir=C:\Windows
```

```
        THREAD fffffa8002a8cbb0  Cid 03d8.0ecc  Teb: 000007fffffdc000 Win32Thread: fffff900c200d460
WAIT: (WrUserRequest) UserMode Non-Alertable
            fffffa8001eaaf00  SynchronizationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80025b7500       Image:         WmiPrvSE.exe
        Wait Start TickCount      17282          Ticks: 29297 (0:00:07:37.036)
        Context Switch Count      59                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address wmiprvse!WinMainCRTStartup (0x00000000ffd3686c)
        Stack Init fffff9801e516db0 Current fffff9801e516740
        Base fffff9801e517000 Limit fffff9801e50f000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1e516780 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1e5168c0 fffff800`01c5cd9d nt!KiSwapThread+0x125
        fffff980`1e516920 fffff960`000c9638 nt!KeWaitForSingleObject+0x5f5
        fffff980`1e5169a0 fffff960`000c96c6 win32k!xxxRealSleepThread+0x278
        fffff980`1e516a40 fffff960`000c7e1e win32k!xxxSleepThread+0x56
        fffff980`1e516a70 fffff960`000c7f25 win32k!xxxRealInternalGetMessage+0x72e
        fffff980`1e516b50 fffff960`000c97e4 win32k!xxxInternalGetMessage+0x35
        fffff980`1e516b90 fffff800`01c4d733 win32k!NtUserGetMessage+0x64
        fffff980`1e516c20 00000000`76d1e6aa nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1e516c20)
        00000000`0028f5d8 00000000`76d1e6ea USER32!ZwUserGetMessage+0xa
        00000000`0028f5e0 00000000`ffcff414 USER32!GetMessageW+0x34
        00000000`0028f610 00000000`ffcff7d3 wmiprvse!Process+0x494
        00000000`0028f770 00000000`ffd366c3 wmiprvse!WinMain+0x63
        00000000`0028f7a0 00000000`76bfcdcd wmiprvse!TraceMessage+0x1ed
        00000000`0028f860 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0028f890 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80020e8b50  Cid 03d8.0dc4  Teb: 000007fffffda000 Win32Thread: 0000000000000000
WAIT: (UserRequest) UserMode Non-Alertable
            fffffa800207c150  NotificationEvent
            fffffa80020c09e0  NotificationEvent
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80025b7500       Image:         WmiPrvSE.exe
        Wait Start TickCount      17281          Ticks: 29298 (0:00:07:37.051)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address NCObjAPI!CNamedPipeClient::ProviderReadyThreadProc (0x000007fefcea2010)
        Stack Init fffff9801dacbdb0 Current fffff9801dacb260
        Base fffff9801dacc000 Limit fffff9801dac6000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        Child-SP          RetAddr           Call Site
        fffff980`1dacb2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1dacb3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`1dacb440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`1dacb4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`1dacb960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`1dacbbb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1dacbc20)
        00000000`01abfc68 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`01abfc70 00000000`76bfedf1 kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`01abfd80 000007fe`fcea208b kernel32!WaitForMultipleObjects+0x11
        00000000`01abfdc0 00000000`76bfcdcd
NCObjAPI!CNamedPipeClient::ProviderReadyThreadProc+0x147
        00000000`01abfe20 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`01abfe50 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa80021746b0  Cid 03d8.0f1c  Teb: 000007fffffd4000 Win32Thread: fffff900c20043a0
WAIT: (UserRequest) UserMode Alertable
            fffffa800254e5c0  SynchronizationEvent
            fffffa80026105b0  SynchronizationEvent
            fffffa8002610550  SynchronizationEvent
            fffffa8002a447d0  SynchronizationEvent
            fffffa8002a08df0  SynchronizationEvent
            fffffa8002174768  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80025b7500       Image:         WmiPrvSE.exe
        Wait Start TickCount      45141          Ticks: 1438 (0:00:00:22.432)
        Context Switch Count      7                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wmiprvse!WmiThread<unsigned long>::ThreadProc (0x00000000ffd0107c)
        Stack Init fffff9801e53cdb0 Current fffff9801e53c260
        Base fffff9801e53d000 Limit fffff9801e537000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1e53c2a0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1e53c3e0 fffff800`01c5a6ef nt!KiSwapThread+0x125
        fffff980`1e53c440 fffff800`01ec17e3 nt!KeWaitForMultipleObjects+0x703
        fffff980`1e53c4b0 fffff800`01ec19d3 nt!ObpWaitForMultipleObjects+0x216
        fffff980`1e53c960 fffff800`01c4d733 nt!NtWaitForMultipleObjects+0xe2
        fffff980`1e53cbb0 00000000`76e2082a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1e53cc20)
        00000000`0217f2b8 00000000`76bfed73 ntdll!NtWaitForMultipleObjects+0xa
        00000000`0217f2c0 00000000`76d1e96d kernel32!WaitForMultipleObjectsEx+0x10b
        00000000`0217f3d0 00000000`76d1e85e USER32!RealMsgWaitForMultipleObjectsEx+0x129
        00000000`0217f470 00000000`ffd0296d USER32!MsgWaitForMultipleObjectsEx+0x46
        00000000`0217f4b0 00000000`ffd024bc wmiprvse!WmiThread<unsigned long>::ThreadWait+0x91
        00000000`0217f730 00000000`ffd010ac wmiprvse!WmiThread<unsigned long>::ThreadDispatch+0xf4
        00000000`0217f790 00000000`76bfcdcd wmiprvse!WmiThread<unsigned long>::ThreadProc+0x30
        00000000`0217f7c0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0217f7f0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa80021e6060  Cid 03d8.0840  Teb: 000007fffffd8000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa80028ab040  QueueObject
            fffffa80021e6118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80025b7500       Image:         WmiPrvSE.exe
        Wait Start TickCount      45141          Ticks: 1438 (0:00:00:22.432)
        Context Switch Count      17
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff9800d0b3db0 Current fffff9800d0b3810
        Base fffff9800d0b4000 Limit fffff9800d0ae000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`0d0b3850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`0d0b3990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`0d0b39f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`0d0b3a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`0d0b3b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`0d0b3bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`0d0b3c20)
        00000000`0105f978 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`0105f980 000007fe`fedce7a3 kernel32!GetQueuedCompletionStatus+0x48
        00000000`0105f9e0 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`0105fa70 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`0105fb20 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`0105fb50 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`0105fb90 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`0105fbc0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0105fbf0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
        THREAD fffffa8002ac8060  Cid 03d8.0eec  Teb: 000007fffffd6000 Win32Thread: 0000000000000000
WAIT: (WrQueue) UserMode Non-Alertable
            fffffa80028ab040  QueueObject
            fffffa8002ac8118  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80025b7500       Image:         WmiPrvSE.exe
        Wait Start TickCount      45141          Ticks: 1438 (0:00:00:22.432)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x000007fefedce900)
        Stack Init fffff9801dab6db0 Current fffff9801dab6810
        Base fffff9801dab7000 Limit fffff9801dab1000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1dab6850 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1dab6990 fffff800`01c686e0 nt!KiSwapThread+0x125
        fffff980`1dab69f0 fffff800`01e94317 nt!KeRemoveQueueEx+0x848
        fffff980`1dab6a80 fffff800`01ec1b4d nt!IoRemoveIoCompletion+0x47
        fffff980`1dab6b00 fffff800`01c4d733 nt!NtRemoveIoCompletion+0x13d
        fffff980`1dab6bb0 00000000`76e2030a nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1dab6c20)
        00000000`0222f928 00000000`76bf8c5c ntdll!ZwRemoveIoCompletion+0xa
        00000000`0222f930 000007fe`fedce7a3 kernel32!GetQueuedCompletionStatus+0x48
        00000000`0222f990 000007fe`fedce66a RPCRT4!COMMON_ProcessCalls+0x101
        00000000`0222fa20 000007fe`fedce8e9 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x148
        00000000`0222fad0 000007fe`fedce89d RPCRT4!ProcessIOEventsWrapper+0x9
        00000000`0222fb00 000007fe`fedce924 RPCRT4!BaseCachedThreadRoutine+0x9b
        00000000`0222fb40 00000000`76bfcdcd RPCRT4!ThreadStartRoutine+0x24
        00000000`0222fb70 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`0222fba0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

        THREAD fffffa800489cbb0  Cid 03d8.0ae0  Teb: 000007fffffae000 Win32Thread: 0000000000000000
WAIT: (DelayExecution) UserMode Non-Alertable
            fffffa800489cc68  NotificationTimer
        Not impersonating
        DeviceMap                 fffff88000007820
        Owning Process            fffffa80025b7500       Image:         WmiPrvSE.exe
        Wait Start TickCount      45141          Ticks: 1438 (0:00:00:22.432)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ole32!CRpcThreadCache::RpcWorkerThreadEntry (0x000007fefd7a3be0)
        Stack Init fffff9801db88db0 Current fffff9801db88990
        Base fffff9801db89000 Limit fffff9801db83000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr           Call Site
        fffff980`1db889d0 fffff800`01c5d055 nt!KiSwapContext+0x84
        fffff980`1db88b10 fffff800`01c5b5a9 nt!KiSwapThread+0x125
        fffff980`1db88b70 fffff800`01e8ae9d nt!KeDelayExecutionThread+0x339
        fffff980`1db88bf0 fffff800`01c4d733 nt!NtDelayExecution+0x5c
        fffff980`1db88c20 00000000`76e205ba nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @
fffff980`1db88c20)
        00000000`01b3f7b8 00000000`76bfd908 ntdll!NtDelayExecution+0xa
        00000000`01b3f7c0 000007fe`fd7acdc0 kernel32!SleepEx+0x84
        00000000`01b3f840 000007fe`fd7a3b7e ole32!CROIDTable::WorkerThreadLoop+0x10
        00000000`01b3f870 000007fe`fd7a3c0a ole32!CRpcThread::WorkerLoop+0x1e
        00000000`01b3f8b0 00000000`76bfcdcd ole32!CRpcThreadCache::RpcWorkerThreadEntry+0x2a
        00000000`01b3f8e0 00000000`76e1c6e1 kernel32!BaseThreadInitThunk+0xd
        00000000`01b3f910 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

Stacks Summary

```
1: kd> !stacks
Proc.Thread  .Thread  Ticks   ThreadState Blocker
                            [fffffa8001860190 System]
   4.000010  fffffa8001885bb0 fffffef Blocked    nt!PopIrpWorkerControl+0x22
   4.000014  fffffa8001885720 fffffdc8 Blocked    nt!PopIrpWorker+0x164
   4.000018  fffffa8001886040 fffffcc7 Blocked    nt!PopIrpWorker+0x164
   4.000030  fffffa800188d720 ffff4a2f Blocked    nt!KeRemoveQueueEx+0x848
   4.00003c  fffffa800188c720 ffff4a24 Blocked    nt!KeRemoveQueueEx+0x848
   4.000044  fffffa800188bbb0 ffff8c99 Blocked    nt!KeRemoveQueueEx+0x848
   4.000048  fffffa800188b720 ffff8c99 Blocked    nt!KeRemoveQueueEx+0x848
   4.00004c  fffffa800188a040 ffff4add Blocked    nt!KeRemoveQueueEx+0x848
   4.000054  fffffa80018983d0 ffff4b85 Blocked    nt!KiExecuteDpc+0x198
   4.000058  fffffa8001899040 ffff4b7b Blocked    nt!KiExecuteDpc+0x198
   4.000060  fffffa800189b040 ffff97a8 Blocked    nt!MiModifiedPageWriter+0x59
   4.000070  fffffa8001881040 ffff4a36 Blocked    nt!CcQueueLazyWriteScanThread+0x73
   4.000074  fffffa8001883320 ffffffe5 Blocked    nt!KeRemoveQueueEx+0x848
   4.000078  fffffa800189d040 ffffffe9 Blocked    nt!KeRemoveQueueEx+0x848
   4.000080  fffffa8001cdc040 ffff4a1f Blocked    nt!EtwpLogger+0xdd
   4.000084  fffffa8001cdc7b0 ffff4a33 Blocked    nt!EtwpLogger+0xdd
   4.000088  fffffa8001d22040 ffff4a2f Blocked    nt!EtwpLogger+0xdd
   4.00008c  fffffa8001d227f0 ffff4a2f Blocked    nt!EtwpLogger+0xdd
   4.000090  fffffa8001d6b040 fffffdf Blocked    nt!EtwpLogger+0x84
   4.000094  fffffa8001d6b670 fffffdf Blocked    nt!EtwpLogger+0x84
   4.000098  fffffa8001dac8b0 fffffdf Blocked    nt!EtwpLogger+0x84
   4.00009c  fffffa8001dcdbb0 fffffdf Blocked    nt!EtwpLogger+0x84
   4.0000a4  fffffa800185d040 ffffcc13 Blocked    nt!EtwpLogger+0xdd
   4.0000a8  fffffa800185e8b0 ffff4b8b Blocked    nt!WdipSemCheckTimeout+0x128
   4.0000ac  fffffa8002657040 fffffcc7 Blocked    acpi!ACPIWorkerThread+0x74
   4.0000b4  fffffa8001c92490 fffffcd Blocked    acpi!PciRootBusBiosMethodDispatcherOnResume+0x51
   4.0000b8  fffffa8002777330 fffff9ae Blocked    nt!KeRemoveQueueEx+0x848
   4.0000bc  fffffa800277a6a0 ffff4b41 Blocked    ndis!ndisCmWaitThread+0x6e
   4.0000c0  fffffa800277a210 ffffebb9 Blocked    ecache!EcCacheIoWorker+0x63
   4.0000c4  fffffa8002791bb0 ffffebb9 Blocked    ecache!EcCacheIoWatchdog+0x36d
   4.0000cc  fffffa8002978b10 fffffbfe Blocked    volsnap!VspWorkerThread+0xd8
   4.0000d0  fffffa80029785e0 ffff569f Blocked    volsnap!VspWorkerThread+0xd8
   4.0000d4  fffffa800297d040 ffff4b7f Blocked    volsnap!VspWorkerThread+0xd8
   4.0000d8  fffffa800297dbb0 fffffe8b Blocked    volsnap!VspWorkerThread+0xd8
   4.0000dc  fffffa800297d720 ffffff8f Blocked    volsnap!VspWorkerThread+0x76
   4.0000e0  fffffa80038a6bb0 ffff4a7b Blocked    Ntfs!TxfPrivateThreadWorkerRoutine+0x3f
   4.0000e8  fffffa800397dbb0 fffffe17 Blocked    dxgkrnl!DpiPdoPollingThread+0x51
   4.0000ec  fffffa800397d720 fffffe17 Blocked    watchdog!SMgrGdiCalloutThread+0x5d
   4.0000f0  fffffa80038f4bb0 fffffe17 Blocked    dxgkrnl!DpiPowerArbiterThread+0x4b
   4.0000fc  fffffa80039d7870 fffffe0b Blocked    nt!KeRemoveQueueEx+0x848
   4.000100  fffffa80039ac040 fffffe0b Blocked    nt!KeRemoveQueueEx+0x848
   4.000104  fffffa80039ac9f0 fffffe0b Blocked    nt!KeRemoveQueueEx+0x848
   4.00012c  fffffa8003dc0710 fffffd18 Blocked    DLARTL_E!ThreadBlock+0x60
   4.00014c  fffffa8003f1d040 ffff4b28 Blocked    nt!KeRemoveQueueEx+0x848
   4.000150  fffffa8003f1dbb0 ffff94f0 Blocked    nt!KeRemoveQueueEx+0x848
   4.000154  fffffa8003f1d720 fffffcfe Blocked    nt!KeRemoveQueueEx+0x848
   4.000158  fffffa8003f1e040 fffff625 Blocked    nt!KeRemoveQueueEx+0x848
   4.00015c  fffffa8003f1ebb0 ffff4b28 Blocked    nt!KeRemoveQueueEx+0x848
   4.000160  fffffa8003f1e720 ffff9647 Blocked    nt!KeRemoveQueueEx+0x848
   4.000164  fffffa8003f1f040 fffffcfe Blocked    nt!KeRemoveQueueEx+0x848
   4.000168  fffffa8003f1fbb0 ffff4b28 Blocked    nt!KeRemoveQueueEx+0x848
   4.00016c  fffffa8003f1f720 ffff4b28 Blocked    nt!KeRemoveQueueEx+0x848
   4.000174  fffffa8003f6fb30 fffffcf3 Blocked    SYMEVENT64x86!SYMEvent_GetSubTask+0x23d1
   4.000178  fffffa8003f28a10 ffff4efb Blocked    eeCtrl64+0xf755
   4.0001c8  fffffa8002984bb0 ffff4a17 Blocked    nt!KeRemoveQueueEx+0x848
   4.0001e4  fffffa80041b4040 ffff4bbc Blocked    nt!KeRemoveQueueEx+0x848
   4.000204  fffffa8003fd1bb0 fffffb4b Blocked    atikmdag!xc_copp_agent+0x616890
   4.000208  fffffa8003d73890 fffffad2 Blocked    atikmdag+0x1f5ce
   4.00020c  fffffa8004069a70 ffffbe7f Blocked    dxgkrnl!VidSchiWaitForSchedulerEvents+0x161
   4.000248  fffffa8004087060 ffff4c8d Blocked    nt!KeRemoveQueueEx+0x848
   4.0002ac  fffffa80042a5060 ffffce74 Blocked    nt!EtwpLogger+0xdd
   4.00035c  fffffa80043dabb0 ffff6a33 Blocked    luafv!SynchronousFsControl+0x102
```

```
  4.000360  fffffa80043d9040 fffffa0d Blocked    DRVEDDM+0x69eb
  4.000368  fffffa80043ccbb0 fffffa17 Blocked    DRVEDDM+0x6b2d
  4.000370  fffffa80043bdbb0 fffffa06 Blocked    DLARTL_E!ThreadBlock+0x60
  4.000374  fffffa80043cd5d0 fffffa06 Blocked    DLARTL_E!ThreadBlock+0x60
  4.000254  fffffa800474c060 fffff9d1 Blocked    csc!CscEnpEvictAutoThread+0x198
  4.00017c  fffffa800474cad0 fffff9d1 Blocked    csc!CscEnpEvictAutoThread+0x198
  4.000474  fffffa800453b4a0 fffff9c2 Blocked    spsys!SPVersion+0x19491
  4.0005d8  fffffa80045fc040 ffff6230 Blocked    HTTP!UlpScavengerThread+0x81
  4.000614  fffffa8004658600 ffffe317 Blocked    mpsdrv!IP6StringToAddress+0x738
  4.000670  fffffa80046ad450 fffff932 Blocked    nt!KeRemoveQueueEx+0x848
  4.000674  fffffa80046b1bb0 fffff931 Blocked    nt!KeRemoveQueueEx+0x848
  4.000678  fffffa80046ae670 fffff930 Blocked    nt!KeRemoveQueueEx+0x848
  4.000680  fffffa80046af040 fffff930 Blocked    nt!KeRemoveQueueEx+0x848
  4.00068c  fffffa80046afbb0 fffff92f Blocked    nt!KeRemoveQueueEx+0x848
  4.00083c  fffffa80048cd060 fffff871 Blocked    nt!EtwpLogger+0xdd
  4.000a0c  fffffa8004b57ad0 fffff527 Blocked    nt!EtwpLogger+0xdd
  4.000540  fffffa8004a1c7c0 ffff4a4d Blocked    nt!PfTLoggingWorker+0x81
  4.000438  fffffa80048990d0 ffffea65 Blocked    nt!EtwpLogger+0xdd
  4.000cec  fffffa8002097bb0 ffffe220 Blocked    nt!EtwpLogger+0xdd
  4.000e20  fffffa800204c060 ffff9647 Blocked    nt!EtwpLogger+0xdd
  4.0006e0  fffffa8002425bb0 ffffcc58 Blocked    nt!EtwpLogger+0x84
  4.000e9c  fffffa80048957f0 ffff952b RUNNING    nt!KeBugCheckEx

                          [fffffa8003f5b040 smss.exe]

                          [fffffa80040bc8e0 csrss.exe]
1f8.000218  fffffa8003d7b060 ffff4ac3 Blocked    nt!AlpcpReceiveMessagePort+0x298
1f8.00023c  fffffa8003fcd960 ffff4aee Blocked    nt!AlpcpReceiveMessagePort+0x298
1f8.000298  fffffa80042a3060 ffff4add Blocked    nt!AlpcpReceiveMessagePort+0x298

                          [fffffa8003d72040 csrss.exe]
22c.000264  fffffa80041b8480 ffff4a0d Blocked    cdd!PresentWorkerThread+0x476
22c.000274  fffffa8004209bb0 ffff4bfc Blocked    nt!AlpcpReceiveMessagePort+0x298
22c.00028c  fffffa800429a560 ffff4a4a Blocked    nt!AlpcpReceiveMessagePort+0x298
22c.0002d0  fffffa800431e060 ffff4c69 Blocked    win32k!xxxMsgWaitForMultipleObjects+0xf3
22c.000aa4  fffffa8004bf6ac0 ffff4b8c Blocked    nt!AlpcpReceiveMessagePort+0x298

                          [fffffa8003f56ad0 wininit.exe]

                          [fffffa80041a2b50 services.exe]
25c.000acc  fffffa80024f2590 ffff4b0d Blocked    nt!KeRemoveQueueEx+0x848
25c.000d78  fffffa8004482060 ffff4c7d Blocked    nt!KeRemoveQueueEx+0x848
25c.000fd8  fffffa8002424700 ffff4c7d Blocked    nt!KeRemoveQueueEx+0x848

                          [fffffa8004298550 lsass.exe]
27c.0002b8  fffffa8004325060 ffff5901 Blocked    nt!ObpWaitForMultipleObjects+0x216
27c.0002d8  fffffa800436e340 ffff4b0d Blocked    nt!KeRemoveQueueEx+0x848
27c.0002dc  fffffa800436f780 ffff4b28 Blocked    nt!AlpcpReceiveMessagePort+0x298
27c.0009c0  fffffa8002583bb0 ffff4fab Blocked    nt!KeRemoveQueueEx+0x848
27c.000db8  fffffa80040a1060 ffff4b28 Blocked    nt!KiSystemServiceCopyEnd+0x13

                          [fffffa8004299660 winlogon.exe]

                          [fffffa80042a4c10 lsm.exe]
290.00030c  fffffa8002174200 ffff4af7 Blocked    nt!KeRemoveQueueEx+0x848

                          [fffffa8004297040 svchost.exe]
338.000b24  fffffa8004b3c4f0 ffff4dfb Blocked    nt!KeRemoveQueueEx+0x848
338.0008b0  fffffa80023a3a50 ffff4dfb Blocked    nt!KeRemoveQueueEx+0x848

                          [fffffa80042d1c10 svchost.exe]
388.000390  fffffa80042d1780 ffff4f14 Blocked    nt!KiSystemServiceCopyEnd+0x13
388.000e48  fffffa8004890bb0 ffff5416 Blocked    nt!KiSystemServiceCopyEnd+0x13
388.000a3c  fffffa8004513740 ffff4b0d Blocked    nt!KeRemoveQueueEx+0x848
388.000e80  fffffa80025b5700 ffff4b0d Blocked    nt!KeRemoveQueueEx+0x848

                          [fffffa80044c0040 Ati2evxx.exe]

                          [fffffa80044ff040 svchost.exe]
114.000134  fffffa80042d8bb0 ffff5790 Blocked    nt!NtReadFile+0x583
```

```
114.000148  fffffa80044fe340 ffff5790 Blocked    nt!ObpWaitForMultipleObjects+0x216
114.0001a0  fffffa80044dd870 ffff4c3b Blocked    nt!ObpWaitForMultipleObjects+0x216
114.0004f8  fffffa80045c0bb0 ffff4b28 Blocked    nt!ObpWaitForMultipleObjects+0x216
114.000508  fffffa800456d700 ffff4b28 Blocked    nt!ObpWaitForMultipleObjects+0x216
114.000828  fffffa800489ebb0 ffff4bfa Blocked    nt!KiSystemServiceCopyEnd+0x13
114.000830  fffffa80048a1bb0 ffff614a Blocked    nt!KiSystemServiceCopyEnd+0x13
114.000d84  fffffa8002b1e620 ffff4c8d Blocked    nt!KeRemoveQueueEx+0x848

                            [fffffa8004484c10 svchost.exe]
18c.0003c8  fffffa800457fbb0 ffff5486 Blocked    nt!ObpWaitForMultipleObjects+0x216
18c.0004a8  fffffa8004550870 ffff5486 Blocked    nt!KeRemoveQueueEx+0x848
18c.0007a0  fffffa8004800060 ffff4a24 Blocked    nt!ObpWaitForMultipleObjects+0x216
18c.000874  fffffa8004918a40 ffff4b68 Blocked    nt!ObpWaitForMultipleObjects+0x216
18c.0008a8  fffffa8004bc4060 ffff558f Blocked    nt!KiSystemServiceCopyEnd+0x13
18c.0008dc  fffffa800201cbb0 ffff61fd Blocked    nt!KeRemoveQueueEx+0x848
18c.000eb4  fffffa80022783e0 ffff4acc Blocked    nt!KeRemoveQueueEx+0x848
18c.000da8  fffffa80020c9bb0 ffff7fbe Blocked    win32k!xxxRealSleepThread+0x278
18c.000c8c  fffffa8004b35bb0 ffff4c92 Blocked    nt!KeRemoveQueueEx+0x848

                            [fffffa80044d9c10 svchost.exe]
1a8.00000c  fffffa800450e060 ffff934d Blocked    nt!KiSystemServiceCopyEnd+0x13
1a8.0001fc  fffffa80044fcbb0 ffff4add Blocked    nt!AlpcpReceiveMessagePort+0x298
1a8.000420  fffffa80045c2690 ffff4c8d Blocked    nt!AlpcpReceiveMessagePort+0x298
1a8.000440  fffffa8004527bb0 ffff4b98 Blocked    nt!ObpWaitForMultipleObjects+0x216
1a8.0007c4  fffffa8004813bb0 ffff4fab Blocked    nt!ObpWaitForMultipleObjects+0x216
1a8.0006d0  fffffa800200e840 ffff4a39 Blocked    nt!KeRemoveQueueEx+0x848
1a8.000d80  fffffa80020a3400 ffff4bbb Blocked    win32k!xxxRealSleepThread+0x278
1a8.0009bc  fffffa8004b3a060 ffff4a41 Blocked    nt!KeRemoveQueueEx+0x848
1a8.000318  fffffa800437abb0 ffff4fab Blocked    nt!KiSystemServiceCopyEnd+0x13
1a8.0000b0  fffffa80020ab060 ffff4b98 Blocked    nt!KeRemoveQueueEx+0x848
1a8.000620  fffffa8002847060 ffff4b98 Blocked    nt!KeRemoveQueueEx+0x848
1a8.000d34  fffffa80048fb060 ffff4ac3 Blocked    nt!KeRemoveQueueEx+0x848

                            [fffffa800451dc10 audiodg.exe]

                            [fffffa80044fbc10 SLsvc.exe]

                            [fffffa80045c38c0 svchost.exe]
424.00046c  fffffa8004530060 ffff53ed Blocked    nt!ObpWaitForMultipleObjects+0x216
424.000638  fffffa8004670bb0 ffff4c6d Blocked    nt!KiSystemServiceCopyEnd+0x13
424.0007ec  fffffa8004835580 ffff5e43 Blocked    nt!ObpWaitForMultipleObjects+0x216
424.00007c  fffffa8004663060 ffff53ed Blocked    nt!KeRemoveQueueEx+0x848
424.000bf4  fffffa80040b0060 ffff4c69 Blocked    nt!KeRemoveQueueEx+0x848

                            [fffffa8004567c10 svchost.exe]
4cc.00051c  fffffa8004570990 ffff4a6a Blocked    nt!ObpWaitForMultipleObjects+0x216
4cc.0003b4  fffffa80044c0730 ffff4cb9 Blocked    nt!KiSystemServiceCopyEnd+0x13
4cc.0009d0  fffffa8002016bb0 ffff4cb6 Blocked    nt!KiSystemServiceCopyEnd+0x13
4cc.000f68  fffffa8002032800 ffff4a6a Blocked    nt!KeRemoveQueueEx+0x848
4cc.000f04  fffffa8004d14060 ffff4a6a Blocked    nt!KeRemoveQueueEx+0x848
4cc.0009fc  fffffa8002486060 ffff4c69 Blocked    nt!KeRemoveQueueEx+0x848

                            [fffffa80045a53d0 Ati2evxx.exe]

                            [fffffa800461e270 spoolsv.exe]
5dc.000ab0  fffffa8004b992c0 ffff4a19 Blocked    nt!KiSystemServiceCopyEnd+0x13
5dc.000ab4  fffffa800409c060 ffff5e70 Blocked    nt!KiSystemServiceCopyEnd+0x13
5dc.000ad0  fffffa8004bce9d0 ffff4f57 Blocked    nt!KiSystemServiceCopyEnd+0x13
5dc.000adc  fffffa8004bd6270 ffff4f56 Blocked    nt!KiSystemServiceCopyEnd+0x13
5dc.000af4  fffffa8004bdbbb0 ffff4f56 Blocked    nt!ObpWaitForMultipleObjects+0x216

                            [fffffa8004622180 svchost.exe]
5f4.00077c  fffffa80047edbb0 ffff61fd Blocked    nt!ObpWaitForMultipleObjects+0x216
5f4.000784  fffffa80047ef060 ffff61fd Blocked    nt!ObpWaitForMultipleObjects+0x216
5f4.000788  fffffa80047efbb0 ffff61fd Blocked    nt!ObpWaitForMultipleObjects+0x216

                            [fffffa8004a2fc10 ccSvcHst.exe]
6d4.0006ec  fffffa800475a060 ffff54e4 Blocked    nt!KiSystemServiceCopyEnd+0x13
6d4.0006b0  fffffa800487a060 ffff4a4d Blocked    nt!ObpWaitForMultipleObjects+0x216
6d4.000328  fffffa800487b060 ffff4a4d Blocked    nt!ObpWaitForMultipleObjects+0x216
```

```
6d4.00066c  fffffa800487bbb0 ffff4a4d Blocked    nt!ObpWaitForMultipleObjects+0x216
6d4.0006f8  fffffa800487b700 ffff4a4d Blocked    nt!ObpWaitForMultipleObjects+0x216
6d4.000708  fffffa800487c060 ffff4a4d Blocked    nt!ObpWaitForMultipleObjects+0x216
6d4.00074c  fffffa800487cbb0 ffff4a4d Blocked    nt!ObpWaitForMultipleObjects+0x216
6d4.000838  fffffa80048ab060 ffff4a4d Blocked    nt!ObpWaitForMultipleObjects+0x216
6d4.000f34  fffffa80039d8550 ffff4a4d Blocked    nt!KeRemoveQueueEx+0x848
6d4.000728  fffffa8002858bb0 ffff5036 Blocked    nt!KeRemoveQueueEx+0x848

                            [fffffa800475d280 DbgSvc.exe]
6fc.00072c  fffffa8004a30820 ffff4c7d Blocked    win32k!xxxRealSleepThread+0x278
6fc.000530  fffffa800485c360 ffff4a46 Blocked    nt!KiSystemServiceCopyEnd+0x13
6fc.00055c  fffffa800485d060 ffff4a5f Blocked    nt!KiSystemServiceCopyEnd+0x13
6fc.000850  fffffa80048c1bb0 ffff4a4a Blocked    nt!KiSystemServiceCopyEnd+0x13
6fc.000dd8  fffffa80020ae700 ffff4b7f Blocked    nt!KiSystemServiceCopyEnd+0x13
6fc.000e0c  fffffa80020af730 ffff4b0d Blocked    nt!KiSystemServiceCopyEnd+0x13
6fc.000e10  fffffa80020ffbb0 ffff4a34 Blocked    nt!KiSystemServiceCopyEnd+0x13
6fc.000e24  fffffa800211ca00 ffff4b28 Blocked    nt!KiSystemServiceCopyEnd+0x13
6fc.000d58  fffffa8002577a80 ffff4b5e Blocked    nt!KeRemoveQueueEx+0x848
6fc.000fa8  fffffa8001fe1930 ffff4b5e Blocked    nt!KeRemoveQueueEx+0x848

                            [fffffa8004a31c10 DefWatch.exe]

                            [fffffa80047fb780 svchost.exe]

                            [fffffa800480ab70 svchost.exe]

                            [fffffa8004812870 SearchIndexer.e]
7c8.0008c0  fffffa8004689bb0 ffff4aee Blocked    nt!ObpWaitForMultipleObjects+0x216
7c8.0008e4  fffffa8004952060 ffff4ab2 Blocked    nt!KiSystemServiceCopyEnd+0x13
7c8.0008e8  fffffa8004952bb0 ffff4a0e Blocked    nt!KiSystemServiceCopyEnd+0x13
7c8.000e28  fffffa8002118930 ffff4b22 Blocked    win32k!xxxRealSleepThread+0x278
7c8.0003a0  fffffa8002ad5770 ffff7f77 Blocked    nt!KeRemoveQueueEx+0x848
7c8.000e70  fffffa8002b1bbb0 ffff4aee Blocked    nt!KeRemoveQueueEx+0x848
7c8.000e90  fffffa80025adbb0 ffff4aee Blocked    nt!KeRemoveQueueEx+0x848
7c8.000fa4  fffffa80025a76c0 ffff4aee Blocked    nt!KeRemoveQueueEx+0x848

                            [fffffa800486c230 Rtvscan.exe]
62c.0008b8  fffffa80046d1800 ffff61b5 Blocked    nt!KiSystemServiceCopyEnd+0x13
62c.0008c4  fffffa8004853060 ffff5280 Blocked    nt!ObpWaitForMultipleObjects+0x216
62c.0008c8  fffffa80046c62c0 ffff4a0f Blocked    nt!KiSystemServiceCopyEnd+0x13
62c.0008cc  fffffa80045e5830 ffff4a16 Blocked    nt!KiSystemServiceCopyEnd+0x13
62c.000914  fffffa8004a1f060 ffff4a35 Blocked    nt!KiSystemServiceCopyEnd+0x13
62c.000918  fffffa8004a3cbb0 ffff4a35 Blocked    nt!KiSystemServiceCopyEnd+0x13
62c.00091c  fffffa8004a3c700 ffff4a27 Blocked    nt!KiSystemServiceCopyEnd+0x13
62c.000480  fffffa8003d7d9d0 ffff4a2e Blocked    nt!KiSystemServiceCopyEnd+0x13
62c.000c38  fffffa80020aa410 ffff4a4d Blocked    nt!KiSystemServiceCopyEnd+0x13
62c.000c7c  fffffa80020af060 ffff4a25 Blocked    nt!KiSystemServiceCopyEnd+0x13
62c.000cb0  fffffa8001f7b890 ffff4ae5 Blocked    nt!ObpWaitForMultipleObjects+0x216
62c.000cc0  fffffa8002051060 ffff4a13 Blocked    nt!KiSystemServiceCopyEnd+0x13
62c.000cc4  fffffa8002054840 ffff4a41 Blocked    nt!KiSystemServiceCopyEnd+0x13
62c.000488  fffffa80020f5340 ffff4a4d Blocked    nt!KeRemoveQueueEx+0x848
62c.000fec  fffffa8002915060 ffff50e7 Blocked    nt!KeRemoveQueueEx+0x848

                            [fffffa800492d330 taskeng.exe]
924.000928  fffffa80045718a0 ffff863b Blocked    nt!ObpWaitForMultipleObjects+0x216

                            [fffffa8004b4a040 taskeng.exe]
a14.000a18  fffffa8004b43bb0 ffff846e Blocked    nt!ObpWaitForMultipleObjects+0x216
a14.000a1c  fffffa8004b36310 ffff4c8d Blocked    nt!ObpWaitForMultipleObjects+0x216
a14.000a74  fffffa8004b77bb0 ffff4c69 Blocked    nt!ObpWaitForMultipleObjects+0x216
a14.000a94  fffffa8004bf5460 ffff4c70 Blocked    nt!AlpcpReceiveMessagePort+0x298
a14.000aac  fffffa80047723a0 ffff4c8d Blocked    win32k!xxxRealSleepThread+0x278
a14.000864  fffffa8001f01060 ffff4c8d Blocked    nt!KeRemoveQueueEx+0x848
a14.000d4c  fffffa8002a6cbb0 ffff4cc3 Blocked    nt!KeRemoveQueueEx+0x848
a14.000ef4  fffffa8002089bb0 ffff4c8d Blocked    nt!KeRemoveQueueEx+0x848

                            [fffffa8004b8a9c0 dwm.exe]

                            [fffffa8004ba4c10 explorer.exe]
a84.000a88  fffffa8004ba4780 ffff4c5c Blocked    win32k!xxxRealSleepThread+0x278
```

```
a84.000b00  fffffa8004b46060 ffff4b2b Blocked    win32k!xxxRealSleepThread+0x278
a84.000a10  fffffa8003a47060 ffff4a39 Blocked    nt!ObpWaitForMultipleObjects+0x216
a84.000494  fffffa8001fb8060 ffff4dfb Blocked    win32k!xxxRealSleepThread+0x278
a84.000d48  fffffa8002093060 ffff87a7 Blocked    nt!ObpWaitForMultipleObjects+0x216
a84.000d74  fffffa80020403e0 ffff4bc2 Blocked    nt!KiSystemServiceCopyEnd+0x13
a84.000ff4  fffffa80028e6060 ffff7071 Blocked    win32k!xxxRealSleepThread+0x278
a84.000314  fffffa8002613b30 ffff6a07 Blocked    nt!ObpWaitForMultipleObjects+0x216

                            [fffffa8004c8f270 sidebar.exe]
bac.000bb0  fffffa8004c89bb0 ffff4a42 Blocked    nt!ObpWaitForMultipleObjects+0x216
bac.0008b4  fffffa8003fe5bb0 ffff4a39 Blocked    nt!ObpWaitForMultipleObjects+0x216
bac.0009dc  fffffa8003df7060 ffff8dc3 Blocked    nt!KeRemoveQueueEx+0x848
bac.0009ec  fffffa8004874bb0 ffff4a39 Blocked    nt!ObpWaitForMultipleObjects+0x216
bac.000b74  fffffa8004a5c060 ffff4a1a Blocked    nt!ObpWaitForMultipleObjects+0x216
bac.000684  fffffa80045ac850 ffff4a39 Blocked    nt!KiSystemServiceCopyEnd+0x13
bac.00081c  fffffa8004655bb0 ffff4a39 Blocked    nt!KeRemoveQueueEx+0x848

                            [fffffa80045424e0 smax4pnp.exe]

                            [fffffa8004320c10 ccApp.exe]
3ec.0000e4  fffffa80047457d0 ffff4b05 Blocked    nt!ObpWaitForMultipleObjects+0x216
3ec.000964  fffffa8004d225b0 ffff4f13 Blocked    nt!KiSystemServiceCopyEnd+0x13

                            [fffffa8004541040 VPTray.exe]
4e8.000a7c  fffffa8003dcf3f0 ffff4d7b Blocked    nt!ObpWaitForMultipleObjects+0x216
4e8.000ae4  fffffa8003fe6060 ffff4a0f Blocked    nt!KiSystemServiceCopyEnd+0x13
4e8.0004ac  fffffa8003e0d060 ffff4a8d Blocked    nt!KiSystemServiceCopyEnd+0x13
4e8.000dcc  fffffa8004242bb0 ffff4a8d Blocked    nt!KeRemoveQueueEx+0x848
4e8.000d68  fffffa8004919060 ffff4c70 Blocked    nt!KeRemoveQueueEx+0x848

                            [fffffa8003a48040 issch.exe]
868.0009e8  fffffa8003a47bb0 ffff4d6f Blocked    win32k!xxxRealSleepThread+0x278

                            [fffffa8003e0cb50 CLI.exe]
b44.0002c0  fffffa8004607060 ffff571b Blocked    nt!ObpWaitForMultipleObjects+0x216
b44.000820  fffffa8004884bb0 ffff8dc3 Blocked    nt!KeRemoveQueueEx+0x848
b44.000834  fffffa8004c67060 ffff4a4a Blocked    nt!ObpWaitForMultipleObjects+0x216
b44.000658  fffffa8003d54bb0 ffff4a4e Blocked    nt!KiSystemServiceCopyEnd+0x13
b44.000ad8  fffffa80042ca060 ffff4a15 Blocked    nt!KiSystemServiceCopyEnd+0x13
b44.0004f4  fffffa8002b33bb0 ffff4a4a Blocked    nt!KeRemoveQueueEx+0x848
b44.00039c  fffffa800254e700 ffff4a4a Blocked    nt!KeRemoveQueueEx+0x848

                            [fffffa800499dc10 CLI.exe]
a34.000a30  fffffa8003d85060 ffff8fc8 Blocked    win32k!xxxRealSleepThread+0x278
a34.000bf0  fffffa8001e82060 ffff4bfc Blocked    nt!ObpWaitForMultipleObjects+0x216
a34.000548  fffffa8001e87660 ffff4a74 Blocked    nt!KiSystemServiceCopyEnd+0x13
a34.0003a4  fffffa8001ed9530 ffff4a25 Blocked    nt!KiSystemServiceCopyEnd+0x13
a34.000fd0  fffffa8002610710 ffff4bfc Blocked    nt!KeRemoveQueueEx+0x848
a34.000280  fffffa80025d1060 ffff4bfc Blocked    nt!KeRemoveQueueEx+0x848

                            [fffffa8002004c10 dllhost.exe]
41c.000350  fffffa8002014a30 ffff4cc9 Blocked    win32k!xxxRealSleepThread+0x278
41c.000c18  fffffa8001e6c360 ffff5bb5 Blocked    nt!KeRemoveQueueEx+0x848
41c.000c20  fffffa8002014060 ffff4a29 Blocked    nt!ObpWaitForMultipleObjects+0x216
41c.000c30  fffffa800202e060 ffff4c61 Blocked    nt!ObpWaitForMultipleObjects+0x216
41c.000ca0  fffffa80020678b0 ffff4a12 Blocked    nt!KiSystemServiceCopyEnd+0x13
41c.000d30  fffffa80020b0bb0 ffff4add Blocked    nt!KiSystemServiceCopyEnd+0x13
41c.000dd0  fffffa8002052060 ffff4b86 Blocked    nt!KiSystemServiceCopyEnd+0x13
41c.000fc4  fffffa80048cdbb0 ffff4a55 Blocked    nt!KeRemoveQueueEx+0x848
41c.000fb4  fffffa800452c9d0 ffff5011 Blocked    nt!KeRemoveQueueEx+0x848

                            [fffffa8002043c10 msdtc.exe]
ca4.000cfc  fffffa8002046bb0 ffff4a0f Blocked    nt!KiSystemServiceCopyEnd+0x13
ca4.000d38  fffffa80020b3bb0 ffff4a55 Blocked    nt!KiSystemServiceCopyEnd+0x13
ca4.000eb8  fffffa800202abb0 ffff4c81 Blocked    nt!KeRemoveQueueEx+0x848
ca4.000dc0  fffffa80045b37f0 ffff4add Blocked    nt!KeRemoveQueueEx+0x848

                            [fffffa800253fae0 ieuser.exe]
958.000ec0  fffffa80025d96b0 ffff53ed Blocked    nt!ObpWaitForMultipleObjects+0x216
958.000f24  fffffa8002583700 ffff7230 Blocked    win32k!xxxRealSleepThread+0x278
```

```
 958.000d70  fffffa8004bd6bb0 ffff4c69 Blocked    nt!KeRemoveQueueEx+0x848

                            [fffffa80025aac10 iexplore.exe]
 d8c.0003b0  fffffa80025d17c0 ffff53ed Blocked    nt!ObpWaitForMultipleObjects+0x216
 d8c.000a8c  fffffa8004526060 ffff4c69 Blocked    nt!KeRemoveQueueEx+0x848

                            [fffffa800293d040 notepad.exe]

                            [fffffa80025b7500 WmiPrvSE.exe]
 3d8.000f1c  fffffa80021746b0 ffff4fab Blocked    nt!ObpWaitForMultipleObjects+0x216
 3d8.000840  fffffa80021e6060 ffff4fab Blocked    nt!KeRemoveQueueEx+0x848
 3d8.000eec  fffffa8002ac8060 ffff4fab Blocked    nt!KeRemoveQueueEx+0x848
 3d8.000ae0  fffffa800489cbb0 ffff4fab Blocked    nt!KiSystemServiceCopyEnd+0x13


Threads Processed: 649
```

Executive Queues

```
1: kd> !exqueue ff
Dumping ExWorkerQueue: FFFFF80001D68980

**** Critical WorkQueue( current = 0 maximum = 2 )
THREAD fffffa8001897bb0  Cid 0004.001c  Teb: 0000000000000000 Win32Thread: 0000000000000000 WAIT:
(WrQueue) UserMode Non-Alertable
    fffff80001d68980  QueueObject
Not impersonating
DeviceMap                 fffff88000007820
Owning Process            fffffa8001860190       Image:         System
Wait Start TickCount      17             Ticks: 46562 (0:00:12:06.371)
Context Switch Count      1
UserTime                  00:00:00.000
KernelTime                00:00:00.000
Win32 Start Address nt!ExpWorkerThread (0xfffff80001c59c80)
Stack Init fffff98000c7adb0 Current fffff98000c7aa70
Base fffff98000c7b000 Limit fffff98000c75000 Call 0
Priority 13 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
Kernel stack not resident.
Child-SP          RetAddr           Call Site
fffff980`00c7aab0 fffff800`01c5d055 nt!KiSwapContext+0x84
fffff980`00c7abf0 fffff800`01c686e0 nt!KiSwapThread+0x125
fffff980`00c7ac50 fffff800`01c59d7d nt!KeRemoveQueueEx+0x848
fffff980`00c7ace0 fffff800`01ee196b nt!ExpWorkerThread+0x104
fffff980`00c7ad50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
fffff980`00c7ad80 00000000`00000000 nt!KxStartSystemThread+0x16

THREAD fffffa8001897720  Cid 0004.0020  Teb: 0000000000000000 Win32Thread: 0000000000000000 WAIT:
(WrQueue) UserMode Non-Alertable
    fffff80001d68980  QueueObject
Not impersonating
DeviceMap                 fffff88000007820
Owning Process            fffffa8001860190       Image:         System
Wait Start TickCount      1071           Ticks: 45508 (0:00:11:49.929)
Context Switch Count      250
UserTime                  00:00:00.000
KernelTime                00:00:00.015
Win32 Start Address nt!ExpWorkerThread (0xfffff80001c59c80)
Stack Init fffff98000c73db0 Current fffff98000c73a70
Base fffff98000c74000 Limit fffff98000c6e000 Call 0
Priority 13 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
Kernel stack not resident.
Child-SP          RetAddr           Call Site
fffff980`00c73ab0 fffff800`01c5d055 nt!KiSwapContext+0x84
fffff980`00c73bf0 fffff800`01c686e0 nt!KiSwapThread+0x125
fffff980`00c73c50 fffff800`01c59d7d nt!KeRemoveQueueEx+0x848
fffff980`00c73ce0 fffff800`01ee196b nt!ExpWorkerThread+0x104
fffff980`00c73d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
fffff980`00c73d80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
THREAD fffffa8001897290  Cid 0004.0024  Teb: 0000000000000000 Win32Thread: 0000000000000000 WAIT:
(WrQueue) UserMode Non-Alertable
    fffff80001d68980  QueueObject
Not impersonating
DeviceMap                 fffff88000007820
Owning Process            fffffa8001860190       Image:         System
Wait Start TickCount      835            Ticks: 45744 (0:00:11:53.610)
Context Switch Count      3586
UserTime                  00:00:00.000
KernelTime                00:00:00.015
Win32 Start Address nt!ExpWorkerThread (0xfffff80001c59c80)
Stack Init fffff98000c6cdb0 Current fffff98000c6ca70
Base fffff98000c6d000 Limit fffff98000c67000 Call 0
Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
Kernel stack not resident.
Child-SP          RetAddr           Call Site
fffff980`00c6cab0 fffff800`01c5d055 nt!KiSwapContext+0x84
fffff980`00c6cbf0 fffff800`01c686e0 nt!KiSwapThread+0x125
fffff980`00c6cc50 fffff800`01c59d7d nt!KeRemoveQueueEx+0x848
fffff980`00c6cce0 fffff800`01ee196b nt!ExpWorkerThread+0x104
fffff980`00c6cd50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
fffff980`00c6cd80 00000000`00000000 nt!KxStartSystemThread+0x16

THREAD fffffa800188d040  Cid 0004.0028  Teb: 0000000000000000 Win32Thread: 0000000000000000 WAIT:
(WrQueue) UserMode Non-Alertable
    fffff80001d68980  QueueObject
Not impersonating
DeviceMap                 fffff88000007820
Owning Process            fffffa8001860190       Image:         System
Wait Start TickCount      835            Ticks: 45744 (0:00:11:53.610)
Context Switch Count      2860
UserTime                  00:00:00.000
KernelTime                00:00:01.123
Win32 Start Address nt!ExpWorkerThread (0xfffff80001c59c80)
Stack Init fffff98000c65db0 Current fffff98000c65a70
Base fffff98000c66000 Limit fffff98000c60000 Call 0
Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
Kernel stack not resident.
Child-SP          RetAddr           Call Site
fffff980`00c65ab0 fffff800`01c5d055 nt!KiSwapContext+0x84
fffff980`00c65bf0 fffff800`01c686e0 nt!KiSwapThread+0x125
fffff980`00c65c50 fffff800`01c59d7d nt!KeRemoveQueueEx+0x848
fffff980`00c65ce0 fffff800`01ee196b nt!ExpWorkerThread+0x104
fffff980`00c65d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
fffff980`00c65d80 00000000`00000000 nt!KxStartSystemThread+0x16

THREAD fffffa800188dbb0  Cid 0004.002c  Teb: 0000000000000000 Win32Thread: 0000000000000000 WAIT:
(WrQueue) UserMode Non-Alertable
    fffff80001d68980  QueueObject
Not impersonating
DeviceMap                 fffff88000007820
Owning Process            fffffa8001860190       Image:         System
Wait Start TickCount      1071           Ticks: 45508 (0:00:11:49.929)
Context Switch Count      2699
UserTime                  00:00:00.000
KernelTime                00:00:00.577
Win32 Start Address nt!ExpWorkerThread (0xfffff80001c59c80)
Stack Init fffff98000c5edb0 Current fffff98000c5ea70
Base fffff98000c5f000 Limit fffff98000c59000 Call 0
Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
Kernel stack not resident.
Child-SP          RetAddr           Call Site
fffff980`00c5eab0 fffff800`01c5d055 nt!KiSwapContext+0x84
fffff980`00c5ebf0 fffff800`01c686e0 nt!KiSwapThread+0x125
fffff980`00c5ec50 fffff800`01c59d7d nt!KeRemoveQueueEx+0x848
fffff980`00c5ece0 fffff800`01ee196b nt!ExpWorkerThread+0x104
fffff980`00c5ed50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
fffff980`00c5ed80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
THREAD fffffa8002984bb0  Cid 0004.01c8  Teb: 0000000000000000 Win32Thread: 0000000000000000 WAIT:
(WrQueue) UserMode Non-Alertable
    fffff80001d68980  QueueObject
    fffffa8002984c68  NotificationTimer
Not impersonating
DeviceMap                 fffff88000007820
Owning Process            fffffa8001860190       Image:         System
Wait Start TickCount      46569          Ticks: 10 (0:00:00:00.156)
Context Switch Count      5069
UserTime                  00:00:00.000
KernelTime                00:00:00.140
Win32 Start Address nt!ExpWorkerThread (0xfffff80001c59c80)
Stack Init fffff98004f96db0 Current fffff98004f96a70
Base fffff98004f97000 Limit fffff98004f91000 Call 0
Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
Child-SP          RetAddr           Call Site
fffff980`04f96ab0 fffff800`01c5d055 nt!KiSwapContext+0x84
fffff980`04f96bf0 fffff800`01c686e0 nt!KiSwapThread+0x125
fffff980`04f96c50 fffff800`01c59d7d nt!KeRemoveQueueEx+0x848
fffff980`04f96ce0 fffff800`01ee196b nt!ExpWorkerThread+0x104
fffff980`04f96d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
fffff980`04f96d80 00000000`00000000 nt!KxStartSystemThread+0x16

THREAD fffffa80041b4040  Cid 0004.01e4  Teb: 0000000000000000 Win32Thread: 0000000000000000 WAIT:
(WrQueue) UserMode Non-Alertable
    fffff80001d68980  QueueObject
    fffffa80041b40f8  NotificationTimer
Not impersonating
DeviceMap                 fffff88000007820
Owning Process            fffffa8001860190       Image:         System
Wait Start TickCount      46148          Ticks: 431 (0:00:00:06.723)
Context Switch Count      10832
UserTime                  00:00:00.000
KernelTime                00:00:00.421
Win32 Start Address nt!ExpWorkerThread (0xfffff80001c59c80)
Stack Init fffff98004fe3db0 Current fffff98004fe3a70
Base fffff98004fe4000 Limit fffff98004fde000 Call 0
Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
Child-SP          RetAddr           Call Site
fffff980`04fe3ab0 fffff800`01c5d055 nt!KiSwapContext+0x84
fffff980`04fe3bf0 fffff800`01c686e0 nt!KiSwapThread+0x125
fffff980`04fe3c50 fffff800`01c59d7d nt!KeRemoveQueueEx+0x848
fffff980`04fe3ce0 fffff800`01ee196b nt!ExpWorkerThread+0x104
fffff980`04fe3d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
fffff980`04fe3d80 00000000`00000000 nt!KxStartSystemThread+0x16

THREAD fffffa80041b4800  Cid 0004.01d0  Teb: 0000000000000000 Win32Thread: 0000000000000000 WAIT:
(WrQueue) UserMode Non-Alertable
    fffff80001d68980  QueueObject
    fffffa80041b48b8  NotificationTimer
Not impersonating
DeviceMap                 fffff88000007820
Owning Process            fffffa8001860190       Image:         System
Wait Start TickCount      13295          Ticks: 33284 (0:00:08:39.233)
Context Switch Count      5596
UserTime                  00:00:00.000
KernelTime                00:00:00.296
Win32 Start Address nt!ExpWorkerThread (0xfffff80001c59c80)
Stack Init fffff98004fc7db0 Current fffff98004fc7a70
Base fffff98004fc8000 Limit fffff98004fc2000 Call 0
Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
Kernel stack not resident.
Child-SP          RetAddr           Call Site
fffff980`04fc7ab0 fffff800`01c5d055 nt!KiSwapContext+0x84
fffff980`04fc7bf0 fffff800`01c686e0 nt!KiSwapThread+0x125
fffff980`04fc7c50 fffff800`01c59d7d nt!KeRemoveQueueEx+0x848
fffff980`04fc7ce0 fffff800`01ee196b nt!ExpWorkerThread+0x104
fffff980`04fc7d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
fffff980`04fc7d80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
THREAD fffffa8003bf1bb0  Cid 0004.01d8  Teb: 0000000000000000 Win32Thread: 0000000000000000 WAIT:
(WrQueue) UserMode Non-Alertable
    fffff80001d68980  QueueObject
    fffffa8003bf1c68  NotificationTimer
Not impersonating
DeviceMap                 fffff88000007820
Owning Process            fffffa8001860190       Image:         System
Wait Start TickCount      38990          Ticks: 7589 (0:00:01:58.389)
Context Switch Count      2932
UserTime                  00:00:00.000
KernelTime                00:00:00.031
Win32 Start Address nt!ExpWorkerThread (0xfffff80001c59c80)
Stack Init fffff98004fb9db0 Current fffff98004fb9a70
Base fffff98004fba000 Limit fffff98004fb4000 Call 0
Priority 15 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
Kernel stack not resident.
Child-SP          RetAddr           Call Site
fffff980`04fb9ab0 fffff800`01c5d055 nt!KiSwapContext+0x84
fffff980`04fb9bf0 fffff800`01c686e0 nt!KiSwapThread+0x125
fffff980`04fb9c50 fffff800`01c59d7d nt!KeRemoveQueueEx+0x848
fffff980`04fb9ce0 fffff800`01ee196b nt!ExpWorkerThread+0x104
fffff980`04fb9d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
fffff980`04fb9d80 00000000`00000000 nt!KxStartSystemThread+0x16


**** Delayed WorkQueue( current = 0 maximum = 2 )
THREAD fffffa800188d720  Cid 0004.0030  Teb: 0000000000000000 Win32Thread: 0000000000000000 WAIT:
(WrQueue) UserMode Non-Alertable
    fffff80001d689d8  QueueObject
Not impersonating
DeviceMap                 fffff88000007820
Owning Process            fffffa8001860190       Image:         System
Wait Start TickCount      46545          Ticks: 34 (0:00:00:00.530)
Context Switch Count      34058
UserTime                  00:00:00.000
KernelTime                00:00:02.745
Win32 Start Address nt!ExpWorkerThread (0xfffff80001c59c80)
Stack Init fffff98000c57db0 Current fffff98000c57a70
Base fffff98000c58000 Limit fffff98000c52000 Call 0
Priority 13 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5
Child-SP          RetAddr           Call Site
fffff980`00c57ab0 fffff800`01c5d055 nt!KiSwapContext+0x84
fffff980`00c57bf0 fffff800`01c686e0 nt!KiSwapThread+0x125
fffff980`00c57c50 fffff800`01c59d7d nt!KeRemoveQueueEx+0x848
fffff980`00c57ce0 fffff800`01ee196b nt!ExpWorkerThread+0x104
fffff980`00c57d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
fffff980`00c57d80 00000000`00000000 nt!KxStartSystemThread+0x16

THREAD fffffa800188c040  Cid 0004.0034  Teb: 0000000000000000 Win32Thread: 0000000000000000 WAIT:
(WrQueue) UserMode Non-Alertable
    fffff80001d689d8  QueueObject
Not impersonating
DeviceMap                 fffff88000007820
Owning Process            fffffa8001860190       Image:         System
Wait Start TickCount      1304           Ticks: 45275 (0:00:11:46.294)
Context Switch Count      1277
UserTime                  00:00:00.000
KernelTime                00:00:00.639
Win32 Start Address nt!ExpWorkerThread (0xfffff80001c59c80)
Stack Init fffff98000c50db0 Current fffff98000c50a70
Base fffff98000c51000 Limit fffff98000c4b000 Call 0
Priority 15 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5
Kernel stack not resident.
Child-SP          RetAddr           Call Site
fffff980`00c50ab0 fffff800`01c5d055 nt!KiSwapContext+0x84
fffff980`00c50bf0 fffff800`01c686e0 nt!KiSwapThread+0x125
fffff980`00c50c50 fffff800`01c59d7d nt!KeRemoveQueueEx+0x848
fffff980`00c50ce0 fffff800`01ee196b nt!ExpWorkerThread+0x104
fffff980`00c50d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
fffff980`00c50d80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
THREAD fffffa800188cbb0  Cid 0004.0038  Teb: 0000000000000000 Win32Thread: 0000000000000000 WAIT:
(WrQueue) UserMode Non-Alertable
    fffff80001d689d8  QueueObject
Not impersonating
DeviceMap                 fffff88000007820
Owning Process            fffffa8001860190       Image:         System
Wait Start TickCount      791            Ticks: 45788 (0:00:11:54.297)
Context Switch Count      163
UserTime                  00:00:00.000
KernelTime                00:00:00.000
Win32 Start Address nt!ExpWorkerThread (0xfffff80001c59c80)
Stack Init fffff98000c49db0 Current fffff98000c49a70
Base fffff98000c4a000 Limit fffff98000c44000 Call 0
Priority 13 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5
Kernel stack not resident.
Child-SP          RetAddr           Call Site
fffff980`00c49ab0 fffff800`01c5d055 nt!KiSwapContext+0x84
fffff980`00c49bf0 fffff800`01c686e0 nt!KiSwapThread+0x125
fffff980`00c49c50 fffff800`01c59d7d nt!KeRemoveQueueEx+0x848
fffff980`00c49ce0 fffff800`01ee196b nt!ExpWorkerThread+0x104
fffff980`00c49d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
fffff980`00c49d80 00000000`00000000 nt!KxStartSystemThread+0x16

THREAD fffffa800188c720  Cid 0004.003c  Teb: 0000000000000000 Win32Thread: 0000000000000000 WAIT:
(WrQueue) UserMode Non-Alertable
    fffff80001d689d8  QueueObject
Not impersonating
DeviceMap                 fffff88000007820
Owning Process            fffffa8001860190       Image:         System
Wait Start TickCount      46556          Ticks: 23 (0:00:00:00.358)
Context Switch Count      8153
UserTime                  00:00:00.000
KernelTime                00:00:00.202
Win32 Start Address nt!ExpWorkerThread (0xfffff80001c59c80)
Stack Init fffff98000c42db0 Current fffff98000c42a70
Base fffff98000c43000 Limit fffff98000c3d000 Call 0
Priority 13 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5
Child-SP          RetAddr           Call Site
fffff980`00c42ab0 fffff800`01c5d055 nt!KiSwapContext+0x84
fffff980`00c42bf0 fffff800`01c686e0 nt!KiSwapThread+0x125
fffff980`00c42c50 fffff800`01c59d7d nt!KeRemoveQueueEx+0x848
fffff980`00c42ce0 fffff800`01ee196b nt!ExpWorkerThread+0x104
fffff980`00c42d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
fffff980`00c42d80 00000000`00000000 nt!KxStartSystemThread+0x16

THREAD fffffa800188b040  Cid 0004.0040  Teb: 0000000000000000 Win32Thread: 0000000000000000 WAIT:
(WrQueue) UserMode Non-Alertable
    fffff80001d689d8  QueueObject
Not impersonating
DeviceMap                 fffff88000007820
Owning Process            fffffa8001860190       Image:         System
Wait Start TickCount      798            Ticks: 45781 (0:00:11:54.188)
Context Switch Count      218
UserTime                  00:00:00.000
KernelTime                00:00:00.015
Win32 Start Address nt!ExpWorkerThread (0xfffff80001c59c80)
Stack Init fffff98000c3bdb0 Current fffff98000c3ba70
Base fffff98000c3c000 Limit fffff98000c36000 Call 0
Priority 13 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5
Kernel stack not resident.
Child-SP          RetAddr           Call Site
fffff980`00c3bab0 fffff800`01c5d055 nt!KiSwapContext+0x84
fffff980`00c3bbf0 fffff800`01c686e0 nt!KiSwapThread+0x125
fffff980`00c3bc50 fffff800`01c59d7d nt!KeRemoveQueueEx+0x848
fffff980`00c3bce0 fffff800`01ee196b nt!ExpWorkerThread+0x104
fffff980`00c3bd50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
fffff980`00c3bd80 00000000`00000000 nt!KxStartSystemThread+0x16
```

```
THREAD fffffa800188bbb0  Cid 0004.0044  Teb: 0000000000000000 Win32Thread: 0000000000000000 WAIT:
(WrQueue) UserMode Non-Alertable
    fffff80001d689d8  QueueObject
Not impersonating
DeviceMap                 fffff88000007820
Owning Process            fffffa8001860190       Image:         System
Wait Start TickCount      29543          Ticks: 17036 (0:00:04:25.763)
Context Switch Count      14311
UserTime                  00:00:00.000
KernelTime                00:00:00.951
Win32 Start Address nt!ExpWorkerThread (0xfffff80001c59c80)
Stack Init fffff98000c34db0 Current fffff98000c34a70
Base fffff98000c35000 Limit fffff98000c2f000 Call 0
Priority 13 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5
Child-SP          RetAddr           Call Site
fffff980`00c34ab0 fffff800`01c5d055 nt!KiSwapContext+0x84
fffff980`00c34bf0 fffff800`01c686e0 nt!KiSwapThread+0x125
fffff980`00c34c50 fffff800`01c59d7d nt!KeRemoveQueueEx+0x848
fffff980`00c34ce0 fffff800`01ee196b nt!ExpWorkerThread+0x104
fffff980`00c34d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
fffff980`00c34d80 00000000`00000000 nt!KxStartSystemThread+0x16

THREAD fffffa800188b720  Cid 0004.0048  Teb: 0000000000000000 Win32Thread: 0000000000000000 WAIT:
(WrQueue) UserMode Non-Alertable
    fffff80001d689d8  QueueObject
Not impersonating
DeviceMap                 fffff88000007820
Owning Process            fffffa8001860190       Image:         System
Wait Start TickCount      29543          Ticks: 17036 (0:00:04:25.763)
Context Switch Count      1365
UserTime                  00:00:00.000
KernelTime                00:00:00.062
Win32 Start Address nt!ExpWorkerThread (0xfffff80001c59c80)
Stack Init fffff98000c2ddb0 Current fffff98000c2da70
Base fffff98000c2e000 Limit fffff98000c28000 Call 0
Priority 13 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5
Child-SP          RetAddr           Call Site
fffff980`00c2dab0 fffff800`01c5d055 nt!KiSwapContext+0x84
fffff980`00c2dbf0 fffff800`01c686e0 nt!KiSwapThread+0x125
fffff980`00c2dc50 fffff800`01c59d7d nt!KeRemoveQueueEx+0x848
fffff980`00c2dce0 fffff800`01ee196b nt!ExpWorkerThread+0x104
fffff980`00c2dd50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
fffff980`00c2dd80 00000000`00000000 nt!KxStartSystemThread+0x16


**** HyperCritical WorkQueue( current = 0 maximum = 2 )
THREAD fffffa800188a040  Cid 0004.004c  Teb: 0000000000000000 Win32Thread: 0000000000000000 WAIT:
(WrQueue) KernelMode Non-Alertable
    fffff80001d68a30  QueueObject
Not impersonating
DeviceMap                 fffff88000007820
Owning Process            fffffa8001860190       Image:         System
Wait Start TickCount      46371          Ticks: 208 (0:00:00:03.244)
Context Switch Count      1459
UserTime                  00:00:00.000
KernelTime                00:00:00.000
Win32 Start Address nt!ExpWorkerThread (0xfffff80001c59c80)
Stack Init fffff98000c26db0 Current fffff98000c26a70
Base fffff98000c27000 Limit fffff98000c21000 Call 0
Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
Child-SP          RetAddr           Call Site
fffff980`00c26ab0 fffff800`01c5d055 nt!KiSwapContext+0x84
fffff980`00c26bf0 fffff800`01c686e0 nt!KiSwapThread+0x125
fffff980`00c26c50 fffff800`01c59d7d nt!KeRemoveQueueEx+0x848
fffff980`00c26ce0 fffff800`01ee196b nt!ExpWorkerThread+0x104
fffff980`00c26d50 fffff800`01c34656 nt!PspSystemThreadStartup+0x5b
fffff980`00c26d80 00000000`00000000 nt!KxStartSystemThread+0x16
```

Root Objects

```
1: kd> !object \
Object: fffff88000005610  Type: (fffffa800183fb40) Directory
    ObjectHeader: fffff880000055e0 (old version)
    HandleCount: 0  PointerCount: 51
    Directory Object: 00000000  Name: \

    Hash Address          Type          Name
    ---- -------          ----          ----
     01  fffff88000005460 Directory     ObjectTypes
     03  fffffa80046d86d0 Event         NETLOGON_SERVICE_STARTED
     05  fffff88000075a40 SymbolicLink  SystemRoot
     06  fffff88002ff4200 Directory     Sessions
     07  fffffa80044f4170 ALPC Port     MmcssApiPort
     08  fffff8800000aaa0 Directory     ArcName
     09  fffff88000076060 Directory     NLS
         fffffa80046e2ba0 ALPC Port     XactSrvLpcPort
     10  fffffa80043ef060 ALPC Port     ThemeApiPort
         fffff88002fdf2f0 Directory     Windows
         fffff880000057f0 Directory     GLOBAL??
         fffffa80046785b0 Event         LanmanServerAnnounceEvent
     11  fffff88000138500 Directory     RPC Control
     13  fffffa8003f24c50 Event         EFSInitEvent
     14  fffffa8002777bd0 Device        clfs
         fffff88002fe8370 SymbolicLink  Dfs
     15  fffffa8003f5b910 ALPC Port     SeRmCommandPort
         fffffa80040b89d0 Event         CsrSbSyncEvent
     16  fffff88000005120 SymbolicLink  DosDevices
         fffffa800209f690 Device        Cdfs
     17  fffff880049ae9f0 Directory     KnownDlls32
         fffffa80046f4bc0 ALPC Port     AELPort
         fffffa80043dff20 Event         EFSSrvInitEvent
     18  fffff88000013620 Key           \REGISTRY
         fffffa80046a7e60 ALPC Port     WindowsErrorReportingServicePort
     19  fffff8800518a060 Directory     BaseNamedObjects
     21  fffffa80043e5970 ALPC Port     SmSsWinStationApiPort
         fffffa8003d7adc0 Event         UniqueInteractiveSessionIdEvent
         fffff8800009d420 Directory     UMDFCommunicationPorts
     22  fffff880024fd060 Directory     KnownDlls
         fffffa8003d60d30 Device        FatCdrom
         fffffa8003f9fd50 Device        Fat
     23  fffff88000076230 Directory     FileSystem
         fffff88000007060 Directory     KernelObjects
         fffffa8002826620 Device        Ntfs
     26  fffff88000007c30 Directory     Callback
         fffffa8004325e60 ALPC Port     SeLsaCommandPort
     27  fffffa80043175b0 Event         DSYSDBG.Debug.Trace.Memory.27c
     28  fffff880000095d0 Directory     Security
         fffffa80043cc9d0 Device        TfsCd
     29  fffffa8004557500 ALPC Port     UxSmsApiPort
     30  fffff88000013840 Directory     Device
         fffffa800437c060 Event         EFSSmbInitEvent
     32  fffffa8004370e60 ALPC Port     LsaAuthenticationPort
     34  fffffa8003f74060 ALPC Port     SmApiPort
         fffff880057f9140 Section       LsaPerformance
         fffffa8003fd3df0 Event         UniqueSessionIdEvent
     36  fffff880000763e0 Directory     Driver
         fffffa800437c780 Event         SAM_SERVICE_STARTED
```

Device Objects

```
1: kd> !object \Device
Object: fffff88000013840  Type: (fffffa800183fb40) Directory
    ObjectHeader: fffff88000013810 (old version)
    HandleCount: 0  PointerCount: 290
    Directory Object: fffff88000005610  Name: Device

    Hash Address          Type          Name
    ---- -------          ----          ----
     00  fffffa8001854e50 Device        00000030
         fffffa80038f2050 Device        NDMP2
         fffffa8001c96a80 Device        NTPNP_PCI0002
         fffff88000908eb0 SymbolicLink  {EEA73716-0C42-465F-B4ED-067C52C7ECAF}
         fffffa8001cad6b0 Device        00000044
     01  fffffa8003971050 Device        NDMP3
         fffff88005e91c90 SymbolicLink  {A2461C02-9298-40EA-9980-8F8C32C2D972}
         fffffa8002596cc0 Device        00000054
         fffffa8001c97060 Device        NTPNP_PCI0003
         fffff880001419d0 SymbolicLink  HarddiskVolumeShadowCopy{6c6b4490-c91c-11dc-af78-
001aa0c5dcdf}
         fffffa8001c90a40 Device        00000040
     02  fffffa8003f4eb50 Device        NetBT_Tcpip_{D1BC5D97-61EC-45A0-B1B4-97E83B0CFA0C}
         fffffa800399d050 Device        NDMP4
         fffff88000c37430 SymbolicLink  Ip
         fffffa8003b64050 Device        USBPDO-5
         fffffa8003c40050 Device        00000050
         fffffa8003977050 Device        USBFDO-3
         fffffa8001c97a80 Device        NTPNP_PCI0004
         fffff880001513e0 SymbolicLink  HarddiskVolumeShadowCopy{2d6e066a-cb49-11dc-97e3-
001aa0c5dcdf}
         fffff8800014d2c0 SymbolicLink  HarddiskVolumeShadowCopy{6c6b4496-c91c-11dc-af78-
001aa0c5dcdf}
         fffffa800184a5d0 Device        0000000f
     03  fffffa8003bcfdf0 Device        NDProxy
         fffffa80039d6050 Device        NDMP5
         fffffa8004561670 Device        lltdio
         fffffa80043c4670 Device        drvnddm
         fffff88000013510 Section       PhysicalMemory
         fffffa8003fb6cd0 Device        Psched
         fffffa8003f41e50 Device        Tcp6
         fffffa80039ee050 Device        USBPDO-1
         fffff88000153fc0 SymbolicLink  HarddiskVolumeShadowCopy{6c6b44a9-c91c-11dc-af78-
001aa0c5dcdf}
         fffffa8001c98060 Device        NTPNP_PCI0005
         fffffa800184fc20 Device        0000001f
         fffffa80018497e0 Device        0000000b
     04  fffffa80018533a0 Device        0000002f
         fffff88005bd7690 Directory     Http
         fffffa80047fd060 Device        AscKmd
         fffffa800399f050 Device        NDMP6
         fffffa80039b0580 Device        RaidPort0
         fffff880001f2bc0 SymbolicLink  HarddiskVolumeShadowCopy{6c6b447e-c91c-11dc-af78-
001aa0c5dcdf}
         fffffa8001c98a80 Device        NTPNP_PCI0006
         fffffa800184ee50 Device        0000001b
         fffffa8001849060 Device        00000009
     05  fffffa8003a0c750 Device        CdRom0
         fffffa80039c0050 Device        NDMP7
         fffffa800461f2f0 Device        SrvAdmin
         fffff88002fb8e60 SymbolicLink  Ip6
         fffffa8001c99060 Device        NTPNP_PCI0007
         fffffa8001c90c40 Device        0000003f
         fffffa80018525d0 Device        0000002b
         fffffa800184d7e0 Device        00000019
         fffffa8001847a10 Device        00000005
     06  fffffa80018cb620 Device        00000001
```

```
         fffffa80039c2050 Device        NDMP8
         fffffa8001ca1360 Device        0000003b
         fffffa8003b66050 Device        0000004f
         fffffa8001c99a80 Device        NTPNP_PCI0008
         fffff880001f26b0 SymbolicLink  HarddiskVolumeShadowCopy{f194dbfa-c99e-11dc-a0a4-
001aa0c5dcdf}
         fffffa8001852e50 Device        00000029
         fffffa800184ca10 Device        00000015
     07  fffffa8004a32050 Device        NDMP9
         fffffa800468be10 Device        LanmanServer
         fffff88000625ad0 SymbolicLink  CDR4_XP
         fffffa8003d9bb90 Device        _HID00000001
         fffffa8001c9a060 Device        NTPNP_PCI0009
         fffffa8003a49050 Device        0000004b
         fffffa8001cbaa10 Device        00000039
         fffffa8001851060 Device        00000025
         fffffa800184bc20 Device        00000011
     08  fffffa8001847160 Device        WMIDataDevice
         fffffa80047fac70 Device        PEAuth
         fffffa8001cae860 Device        00000049
         fffffa80018557e0 Device        00000035
         fffffa800184f3a0 Device        00000021
     09  fffffa8004b87980 Device        00000059
         fffffa8004658080 Device        MPS
         fffffa8001cae060 Device        00000045
         fffffa8001854a10 Device        00000031
     10  fffffa8003d5b250 Device        00000055
         fffffa8003f29330 Device        EraserUtilDrv10741
         fffffa8004655870 Device        LanmanDatagramReceiver
         fffff8800084a620 SymbolicLink  NdisWanIp
         fffffa8002980990 Device        HarddiskVolumeShadowCopy10
         fffff88000153160 SymbolicLink  HarddiskVolumeShadowCopy{6c6b44af-c91c-11dc-af78-
001aa0c5dcdf}
         fffffa8001cac540 Device        00000041
     11  fffffa8003f41060 Device        Tcp
         fffffa800284f620 Device        SpDevice
         fffffa80038b6ab0 Device        DxgKrnl
         fffff88005b49d70 SymbolicLink  LanmanRedirector
         fffffa8004737060 Device        ASYNCMAC
         fffffa8003a83050 Device        USBPDO-6
         fffffa8001c9aa80 Device        NTPNP_PCI0010
         fffffa8003979050 Device        USBFDO-4
         fffffa80039eabb0 Device        RdpDrPort
         fffffa800297e990 Device        HarddiskVolumeShadowCopy11
     12  fffffa8002766050 Device        USBFDO-0
         fffff88005bef500 SymbolicLink  MailslotRedirector
         fffffa8003dc5600 Device        Null
         fffffa8003a55050 Device        USBPDO-2
         fffffa8001c9b060 Device        NTPNP_PCI0011
         fffffa80039ea490 Device        RdpDr
         fffffa800298a060 Device        HarddiskVolumeShadowCopy12
         fffffa80018493a0 Device        0000000c
     13  fffffa8003dc1060 Device        NamedPipe
         fffffa8003fe9300 Device        WANARP
         fffffa8003f414a0 Device        Udp6
         fffffa8002983990 Device        HarddiskVolumeShadowCopy13
         fffffa8001c9ba80 Device        NTPNP_PCI0012
         fffffa800184ea10 Device        0000001c
     14  fffffa8001853060 Device        0000002c
         fffffa8004b2f5d0 Device        NAVENG
         fffffa8002772050 Device        PxHelperDevice0
         fffffa8003fe88d0 Device        EraserCtrlDrv
         fffffa8003f16080 Device        Video0
         fffffa80039c8880 Device        RdpDrDvMgr
         fffffa8002994990 Device        HarddiskVolumeShadowCopy14
         fffffa8001c9c060 Device        NTPNP_PCI0013
         fffffa8001848e50 Device        00000006
     15  fffffa800285ec70 Device        KsecDD
         fffff880005f28d0 Directory     Ide
         fffffa80018b65a0 Device        00000002
```

```
         fffffa8003e60580 Device        NXTIPSEC
         fffffa8003dc19e0 Device        Video1
         fffffa8002976060 Device        HarddiskVolumeShadowCopy15
         fffff880001f5a00 SymbolicLink  HarddiskVolumeShadowCopy{6c6b44b6-c91c-11dc-af78-
001aa0c5dcdf}
         fffff8800014de00 SymbolicLink  HarddiskVolumeShadowCopy{6c6b449d-c91c-11dc-af78-
001aa0c5dcdf}
         fffffa8001c9ca80 Device        NTPNP_PCI0014
         fffffa8001ca9890 Device        0000003c
         fffffa800184c5d0 Device        00000016
     16  fffffa8001cb6650 Device        MountPointManager
         fffffa80027713e0 Device        drvmcdb
         fffffa8003e049e0 Device        Video2
         fffffa8003a5c050 Device        0000004c
         fffffa8002971990 Device        HarddiskVolumeShadowCopy16
         fffffa8001c9d060 Device        NTPNP_PCI0015
         fffffa8001851c20 Device        00000026
         fffffa800184b7e0 Device        00000012
     17  fffffa800406c7b0 Device        Video3
         fffffa8002981990 Device        HarddiskVolumeShadowCopy17
         fffffa80018553a0 Device        00000036
         fffffa8004631bd0 Device        SrvNet
         fffffa80038c1370 Device        sscdbhook1
         fffffa8001c9da80 Device        NTPNP_PCI0016
         fffffa8002656e60 Device        KMDF0
         fffffa8001856a20 Device        WMIAdminDevice
         fffffa8001850e50 Device        00000022
     18  fffffa8001cb2060 Device        NTPNP_PCI0017
         fffffa8001f11060 Device        NAVEX15
         fffffa800298f060 Device        HarddiskVolumeShadowCopy18
         fffffa80018545d0 Device        00000032
         fffffa8004095d90 Device        Video4
         fffffa8001caee60 Device        00000046
     19  fffffa8003d99b90 Device        00000056
         fffffa8002993060 Device        HarddiskVolumeShadowCopy19
         fffff880007e4df0 SymbolicLink  {3CAC835F-95BB-4CCF-95F1-8BE8920A3C2F}
         fffff88000032da0 SymbolicLink  HarddiskVolumeShadowCopy{2d6e067c-cb49-11dc-97e3-
001aa0c5dcdf}
         fffffa8001cb2a80 Device        NTPNP_PCI0018
         fffffa8001cadab0 Device        00000042
     20  fffffa8003d42060 Device        00000052
         fffffa8001cb6060 Device        NTPNP_PCI0019
         fffffa8003eaa5c0 Device        WFP
         fffffa8003d4e060 Device        USBPDO-7
         fffffa800397b050 Device        USBFDO-5
     21  fffffa80039fd050 Device        USBPDO-3
         fffffa8003893050 Device        USBFDO-1
         fffffa8003974060 Device        ParallelPort0
         fffffa800184ae50 Device        0000000d
     22  fffffa8002af85f0 Device        SystemDump
         fffffa8003beb5f0 Device        SRTSPX
         fffffa8002891ce0 Device        HarddiskVolume1
         fffffa8003e04790 Device        Mailslot
         fffffa80039eadb0 Device        DrDynVc
         fffffa800262a840 Device        RawCdRom
         fffff88000647b90 SymbolicLink  FtControl
         fffffa800184e5d0 Device        0000001d
     23  fffffa80028912d0 Device        HarddiskVolume2
         fffffa8003f139c0 Device        RasAcd
         fffff880001f0a30 Directory     Harddisk0
         fffffa800473b060 Device        KSENUM#00000002
         fffffa8001853c20 Device        0000002d
         fffffa8003f6b9c0 Device        WANARPV6
         fffffa8003f32e50 Device        RawIp
         fffffa8003f32060 Device        RawIp6
         fffffa8003eea7f0 Device        Tdx
         fffff880001f62d0 SymbolicLink  HarddiskVolumeShadowCopy{f194dbf4-c99e-11dc-a0a4-
001aa0c5dcdf}
         fffffa8002977290 Device        HarddiskVolumeShadowCopy1
         fffffa8001cb0620 Device        VolMgrControl
```

```
         fffffa8001848a10 Device        00000007
     24  fffffa80028549f0 Device        Mup
         fffffa8003f1f540 Device        Nsi
         fffff880007ef680 SymbolicLink  {D1BC5D97-61EC-45A0-B1B4-97E83B0CFA0C}
         fffffa8003f006c0 Device        FsWrap
         fffffa8003a04a90 Device        PointerClass0
         fffff88000153060 SymbolicLink  HarddiskVolumeShadowCopy{6c6b44c4-c91c-11dc-af78-
001aa0c5dcdf}
         fffffa8002892060 Device        HarddiskVolumeShadowCopy2
         fffffa8001ca8620 Device        0000003d
         fffffa800184d060 Device        00000017
         fffffa8001843c20 Device        00000003
     25  fffff88000849a40 SymbolicLink  {515E420A-241B-4616-8F36-A36B1627FA86}
         fffffa8003f416b0 Device        Udp
         fffffa8003d989c0 Device        PointerClass1
         fffffa8003a72050 Device        0000004d
         fffffa800296f990 Device        HarddiskVolumeShadowCopy3
         fffff8800065a6a0 SymbolicLink  HarddiskVolumeShadowCopy{6c6b448a-c91c-11dc-af78-
001aa0c5dcdf}
         fffffa800262a640 Device        RawTape
         fffffa80018517e0 Device        00000027
         fffffa800184b3a0 Device        00000013
     26  fffffa8004802350 Device        Secdrv
         fffffa80039ed3f0 Device        Serial0
         fffffa800297f990 Device        HarddiskVolumeShadowCopy4
         fffffa8001856e50 Device        00000037
         fffffa8001850a10 Device        00000023
     27  fffff880008497a0 SymbolicLink  {F30C6E8D-89CC-44B9-A103-6F2DCAE75CEC}
         fffffa8001855060 Device        00000033
         fffff88000151f20 SymbolicLink  HarddiskVolumeShadowCopy{f194dc01-c99e-11dc-a0a4-
001aa0c5dcdf}
         fffffa8002970990 Device        HarddiskVolumeShadowCopy5
         fffffa8001caec60 Device        00000047
     28  fffffa8002771060 Device        FileInfo
         fffffa8003f36320 Device        NetBt_Wins_Export
         fffffa800455b700 Device        rspndr
         fffffa8004090060 Device        00000057
         fffffa80039fc060 Device        Termdd
         fffff88000153b30 SymbolicLink  HarddiskVolumeShadowCopy{6c6b44a3-c91c-11dc-af78-
001aa0c5dcdf}
         fffffa800299a990 Device        HarddiskVolumeShadowCopy6
         fffffa8001cad8b0 Device        00000043
     29  fffff88002fe88e0 SymbolicLink  Csc
         fffffa8003d9c060 Device        USBPDO-8
         fffffa8003c5e7c0 Device        00000053
         fffffa8003999050 Device        USBFDO-6
         fffffa8002975060 Device        HarddiskVolumeShadowCopy7
         fffff8800006ae00 SymbolicLink  MbDlDp32
     30  fffffa80027777e0 Device        Ndis
         fffffa8003ec6a10 Device        WfpAle
         fffffa8001883220 Event         VolumesSafeForWriteAccess
         fffffa8003a85050 Device        USBPDO-4
         fffffa80039c7660 Device        KeyboardClass0
         fffff88000651220 SymbolicLink  ScsiPort0
         fffffa8003975050 Device        USBFDO-2
         fffff88000151d50 SymbolicLink  HarddiskVolumeShadowCopy{2d6e0670-cb49-11dc-97e3-
001aa0c5dcdf}
         fffffa8002986990 Device        HarddiskVolumeShadowCopy8
         fffffa800184aa10 Device        0000000e
     31  fffffa8003f96460 Device        DfsClient
         fffff88000848060 SymbolicLink  {34E2D8A0-75A6-435D-9E42-2C8948763B5F}
         fffffa80039f0050 Device        USBPDO-0
         fffffa8003d5bd00 Device        KeyboardClass1
         fffff8800064f820 SymbolicLink  ScsiPort1
         fffffa8002972990 Device        HarddiskVolumeShadowCopy9
         fffffa800184f060 Device        0000001e
         fffffa8001849c20 Device        0000000a
     32  fffffa80018537e0 Device        0000002e
         fffffa8003f2a6c0 Device        SymEvent
         fffff880008423b0 SymbolicLink  ScsiPort2
```

```
         fffff88000141880 SymbolicLink  HarddiskVolumeShadowCopy{6c6b4484-c91c-11dc-af78-
001aa0c5dcdf}
         fffffa800184d3a0 Device        0000001a
         fffffa80018485d0 Device        00000008
     33  fffffa8003f4f490 Device        Netbios
         fffffa8004658c70 Device        Srv2
         fffffa8003fe9c40 Device        NetbiosSmb
         fffff8800084a7f0 SymbolicLink  NdisWanIpv6
         fffffa8003ecaa10 Device        eQoS
         fffffa8001847e50 Device        00000004
         fffffa800262aa40 Device        RawDisk
         fffffa8001c90060 Device        0000003e
         fffffa8001852a10 Device        0000002a
         fffffa800184dc20 Device        00000018
     34  fffffa8003f75300 Device        Afd
         fffffa80039ca290 Device        NdisTapi
         fffffa8003d46520 Device        SRTSP
         fffffa8003a75810 Device        Parallel0
         fffffa8001ca2360 Device        0000003a
         fffffa8003a87050 Device        0000004e
         fffff88000151060 SymbolicLink  HarddiskVolumeShadowCopy{2d6e0664-cb49-11dc-97e3-
001aa0c5dcdf}
         fffffa80018513a0 Device        00000028
         fffffa800184ce50 Device        00000014
     35  fffffa8002792c40 Device        ECacheControl
         fffff88005befae0 SymbolicLink  WebDavRedirector
         fffffa8003d5d2b0 Device        _HID00000000
         fffffa8003a38050 Device        0000004a
         fffffa80039e8060 Device        Tun0
         fffff88000151200 SymbolicLink  HarddiskVolumeShadowCopy{f194dc0b-c99e-11dc-a0a4-
001aa0c5dcdf}
         fffffa8001c95a80 Device        NTPNP_PCI0000
         fffffa8001843460 Device        00000038
         fffffa80018505d0 Device        00000024
         fffffa800184b060 Device        00000010
     36  fffffa8001855c20 Device        00000034
         fffffa8003bd1cd0 Device        NdisWan
         fffffa800396c050 Device        NDMP1
         fffffa8001caea60 Device        00000048
         fffffa8001c96060 Device        NTPNP_PCI0001
         fffffa800184f7e0 Device        00000020
```

Driver Objects

```
1: kd> !object \Driver
Object: fffff880000763e0  Type: (fffffa800183fb40) Directory
    ObjectHeader: fffff880000763b0 (old version)
    HandleCount: 0  PointerCount: 88
    Directory Object: fffff88000005610  Name: Driver

    Hash Address          Type          Name
    ---- -------          ----          ----
     00  fffffa80027715e0 Driver        DRVECDB
     01  fffffa8002653510 Driver        Wdf01000
         fffffa800399ee70 Driver        PptpMiniport
         fffffa80039a1530 Driver        usbuhci
         fffffa8003f758d0 Driver        netbt
     02  fffffa8004660060 Driver        mpsdrv
     03  fffffa8004536e70 Driver        lltdio
         fffffa800285e430 Driver        disk
         fffffa8003a75600 Driver        NDProxy
         fffffa8003f00090 Driver        PSched
     04  fffffa80045f5960 Driver        HTTP
     06  fffffa800298d420 Driver        usbehci
         fffffa8003980480 Driver        R300
         fffffa8003fca9e0 Driver        monitor
         fffffa80038acc10 Driver        tunnel
     07  fffffa800284f430 Driver        partmgr
     08  fffffa8004777c70 Driver        PEAUTH
         fffffa8001843060 Driver        ACPI_HAL
         fffffa80039a3060 Driver        b57nd60a
         fffffa80039aee70 Driver        iScsiPrt
     09  fffffa800284a1b0 Driver        spldr
         fffffa8003d43c00 Driver        RDPENCDD
     10  fffffa80039b02d0 Driver        Rasl2tp
         fffffa8003d4f500 Driver        HidUsb
     11  fffffa8004747270 Driver        AsyncMac
         fffffa8003dc4e70 Driver        EraserUtilRebootDrv
         fffffa80018407f0 Driver        PnpManager
         fffffa80038e6060 Driver        DXGKrnl
     12  fffffa8003dc5060 Driver        Null
         fffffa80039a07b0 Driver        rdpdr
     14  fffffa8002777e70 Driver        CLFS
         fffffa800397d310 Driver        Serenum
         fffffa80020567b0 Driver        NAVENG
     15  fffffa8003e05830 Driver        RDPCDD
         fffffa80038e3250 Driver        Serial
         fffffa80038f17b0 Driver        tunmp
         fffffa800285ee70 Driver        KSecDD
         fffffa8001cb37d0 Driver        volmgr
     16  fffffa80027717d0 Driver        PxHlpa64
         fffffa80029b9c40 Driver        crcdisk
         fffffa8003a0dda0 Driver        umbus
     17  fffffa80041b9ac0 Driver        Win32k
     18  fffffa8003a03760 Driver        mouclass
         fffffa8003f75530 Driver        Smb
         fffffa8003f6d630 Driver        eeCtrl
         fffffa8003bf09e0 Driver        NAVEX15
     19  fffffa8001cba5c0 Driver        msisadrv
     20  fffffa80039fc320 Driver        kbdclass
     21  fffffa8002942d80 Driver        volsnap
         fffffa8003d99500 Driver        mouhid
     22  fffffa8001ef0590 Driver        SystemDump
         fffffa8003f13530 Driver        VgaSave
         fffffa8003dc5d30 Driver        nsiproxy
         fffffa8001847670 Driver        WMIxWDM
         fffffa8003dbe490 Driver        SRTSPX
     23  fffffa8003f335b0 Driver        tdx
         fffffa8003dc03a0 Driver        RasAcd
```

```
     fffffa8003f13250 Driver        Wanarpv6
25   fffffa80039e9830 Driver        RasPppoe
     fffffa8003980060 Driver        HDAudBus
26   fffffa80047fde70 Driver        secdrv
27   fffffa80038e3660 Driver        Parport
     fffffa8003d62940 Driver        kbdhid
     fffffa8003d42460 Driver        ADIHdAudAddService
28   fffffa8004098bc0 Driver        rspndr
     fffffa80039c6e70 Driver        TermDD
29   fffffa8001cbb060 Driver        volmgrx
     fffffa8001ca8430 Driver        pci
     fffffa8003f2b530 Driver        CSC
     fffffa80039fc700 Driver        mssmbios
30   fffffa8001846d60 Driver        Ecache
     fffffa80039a1770 Driver        cdrom
     fffffa80027779e0 Driver        NDIS
31   fffffa80039c38b0 Driver        swenum
32   fffffa8003e042c0 Driver        Tcpip
     fffffa8003f24720 Driver        SymEvent
     fffffa8003a64110 Driver        usbhub
33   fffffa80038ba060 Driver        intelppm
     fffffa8001cbb9d0 Driver        atapi
34   fffffa8003f75060 Driver        AFD
     fffffa8001cb0430 Driver        MountMgr
     fffffa8001cb57d0 Driver        intelide
     fffffa8003978bd0 Driver        NdisTapi
35   fffffa8004802de0 Driver        tcpipreg
     fffffa80025958e0 Driver        ksthunk
36   fffffa8002657e70 Driver        ACPI
     fffffa80039a1ce0 Driver        NdisWan
```

File System Objects

```
1: kd> !object \FileSystem
Object: fffff88000076230  Type: (fffffa800183fb40) Directory
    ObjectHeader: fffff88000076200 (old version)
    HandleCount: 0  PointerCount: 42
    Directory Object: fffff88000005610  Name: FileSystem

    Hash Address          Type          Name
    ---- -------          ----          ----
     01  fffffa8003980be0 Driver        DLACDBHE
     02  fffffa8004661990 Driver        mrxsmb10
         fffffa800465e0e0 Driver        mrxsmb
     03  fffffa8004679600 Driver        mrxsmb20
     04  fffffa800436b9d0 Driver        luafv
     05  fffffa80042d5980 Driver        DLAUDFAE
     06  fffffa80043a86a0 Driver        DLAPoolE
     07  fffffa80043cdc90 Driver        DLABMFSE
     11  fffffa8003fd7b00 Driver        rdbss
         fffffa8003d98e50 Device        CdfsRecognizer
     12  fffffa8003dc47a0 Device        UdfsDiskRecognizer
         fffffa8003d43610 Driver        Fs_Rec
     13  fffffa8003dc4060 Driver        Msfs
     15  fffffa8003f72060 Driver        DfsC
     16  fffffa80020a03c0 Driver        cdfs
     17  fffffa8004535790 Driver        srvnet
         fffffa80043bd060 Driver        DLAOPIOE
     19  fffffa800467b900 Driver        srv
         fffffa80046593d0 Driver        MRxDAV
         fffff8800009d5d0 Directory     Filters
     21  fffffa8004658e70 Driver        bowser
         fffffa80028997e0 Driver        FltMgr
     22  fffffa80043c4870 Driver        DRVEDDM
         fffffa8003dc2060 Device        FatCdRomRecognizer
     23  fffffa8002792e70 Driver        Ntfs
     24  fffffa8003dc42a0 Driver        Npfs
         fffffa8002854c90 Driver        Mup
         fffffa800262ac40 Driver        RAW
     27  fffffa80041b1060 Driver        fastfat
     28  fffffa800276d500 Driver        FileInfo
     29  fffffa80043bce70 Driver        DLADResE
         fffffa8003d43360 Driver        DLARTL_E
     31  fffffa8003dc4590 Device        FatDiskRecognizer
     32  fffffa80042d56e0 Driver        DLABOIOE
     33  fffffa800466da10 Driver        srv2
         fffffa8003fe85f0 Driver        NetBIOS
         fffffa8003dc2e50 Device        ExFatRecognizer
     34  fffffa8003bf1730 Driver        SRTSP
     35  fffffa80043cec50 Driver        DLAUDF_E
         fffffa80043c12f0 Driver        DLAIFS_E
         fffffa8003dc49b0 Device        UdfsCdRomRecognizer
```

Base Named Objects

```
1: kd> !object \BaseNamedObjects
Object: fffff8800518a060  Type: (fffffa800183fb40) Directory
    ObjectHeader: fffff8800518a030 (old version)
    HandleCount: 28  PointerCount: 222
    Directory Object: fffff88000005610  Name: BaseNamedObjects

    Hash Address          Type          Name
    ---- -------          ----          ----
     00  fffffa8004853df0 Event         LDVP_LPC_13
         fffffa8004a2b960 Mutant        Symantec.EraserSvc.SingleAccess
         fffffa800467cfe0 Event         BFE_Notify_Event_{7c0ed2b5-868e-49fd-a5d7-6a55ad939653}
     01  fffffa800475f660 Mutant        usbhub_Perf_Library_Lock_PID_6fc
         fffffa80020b9620 Mutant        ServiceModelEndpoint 3.0.0.0_Perf_Library_Lock_PID_6fc
         fffffa80020d3970 Mutant        BITS_Perf_Library_Lock_PID_6fc
         fffffa8002953c10 Mutant        oleacc-msaa-loaded
         fffffa8004853d70 Event         LDVP_LPC_14
     02  fffffa8004089b00 Mutant
C::Users:UserName:AppData:Local:Microsoft:Windows:Explorer:thumbcache_32.db!dfMaintainer
         fffffa80020fcde0 Mutant        ServiceModelService 3.0.0.0_Perf_Library_Lock_PID_6fc
         fffff8800292a2c0 Section       netfxcustomperfcounters.1.0.net clr networking
         fffffa8004853cf0 Event         LDVP_LPC_15
         fffffa800475c510 Event         ccSetMgr_Terminate_Lock
         fffffa8004374bc0 Mutant        ATI_ExtEventMiscMutex
     03  fffffa8002096870 Mutant        MSDTC_STATS_EVENT
     04  fffffa8004861510 Event         WMI_SysEvent_LodCtr
         fffffa8004204250 Mutant
C::Users:UserName:AppData:Local:Microsoft:Windows:Explorer:thumbcache_sr.db!dfMaintainer
         fffffa800475f700 Mutant        UGTHRSVC_Perf_Library_Lock_PID_6fc
         fffffa8004558bd0 Event         AtiDrvMsgEvent_1
     05  fffffa8004800b30 Event         NlaPrivatePort1
         fffffa80043702c0 Event         ConsoleSessionCreation
     06  fffffa80047ec1e0 ALPC Port     WDI_{32c083d7-3e87-40fa-996d-19a9cd926281}
         fffffa8004ce8fc0 Mutant
C::Users:UserName:AppData:Local:Microsoft:Windows:Explorer:thumbcache_256.db!dfMaintainer
         fffff88004973a20 SymbolicLink  Local
         fffffa8001fff290 Mutant        PolicyAgent_Perf_Library_Lock_PID_6fc
         fffffa8001fff510 Mutant        PerfNet_Perf_Library_Lock_PID_6fc
         fffffa800475ba00 Mutant        ccSetMgr_Running
         fffffa8004290260 Mutant        LDVPNTLogMutex
         fffffa8004544c20 Event         RouterPreInitEvent
         fffffa800430e1e0 Event         PnP_No_Pending_Install_Clients
         fffffa80047ff9d0 Event         NlaPrivatePort2
         fffffa80045e2fe0 Event         WiaServiceStarted
     07  fffff88008bbf780 Section       MMF_BITS_s
         fffffa80047ff700 Event         NlaPrivatePort3
     08  fffffa80020d3c70 Mutant        .NETFramework_Perf_Library_Lock_PID_6fc
         fffffa8004cdb0d0 Event         CorDBIPCSetupSyncEvent_2884
         fffffa80048e5060 Event         Ready0:  ESENT Performance Data Schema Version 73
         fffffa80048e5af0 Event         Go0:  ESENT Performance Data Schema Version 73
         fffffa8004662570 Event         BFE_Notify_Event_{d1178e0d-dab7-484f-8722-10c5273adbf6}
         fffffa80045a8bb0 Event         {B3FFC4BE-2FCA-492E-AC6A-6549DEB751B6}ShellHWDetection
         fffffa800451f660 Event         AudioSrv_CanAcceptMMCClient
     09  fffff88002e4efc0 Section       Cor_Private_IPCBlock_2612
         fffff880060ca410 Section       UGTHRSVC
     10  fffffa8001ffff20 Mutant        MSDTC Bridge 3.0.0.0_Perf_Library_Lock_PID_6fc
         fffffa80049688b0 Mutant        I1_LDVP Load VDB
         fffff88005a33fc0 Section       WseIdxPm
         fffff880060b9790 Section       UGathererObj
     11  fffffa80048e2a20 Mutant        Instance0:  ESENT Performance Data Schema Version 73
         fffff88005c08920 Section       mmGlobalPnpInfo
         fffffa80020e0350 Event         EVENT_READYROOT/CIMV2WMI SELF-INSTRUMENTATION EVENT
PROVIDER
         fffffa80046d62b0 Event         LDVP_LPC_0
         fffffa8004804a50 Event         BFE_Notify_Event_{7264a790-b479-4b02-ab47-baf1809248df}
     12  fffffa8002009060 Event         COM+ Tracker Push Event
```

```
         fffffa80048a1470 Event         LDVP_LPC_1
         fffff8800518a5c0 SymbolicLink  Session
         fffff88005ad2600 Section       AtiEeuSharedAdapterData_420b000
     13  fffffa8004861490 Event         WMI_SysEvent_UnLodCtr
         fffffa80020fcca0 Mutant        Spooler_Perf_Library_Lock_PID_6fc
         fffffa80048a13f0 Event         LDVP_LPC_2
         fffffa80046e8640 Event         LDVP_LPC_SEM
         fffffa800430e260 Event         PnP_No_Pending_Install_Events
         fffffa8004874150 Event         IPSEC_GP_REFRESH_EVENT
     14  fffffa80020d38d0 Mutant        DFSR_Perf_Library_Lock_PID_6fc
         fffffa80046b05c0 Event         LDVP_LPC_3
         fffffa8004838c30 Mutant        SearchServiceMUT
         fffffa8004802c10 Event         NlaPrivatePort
         fffffa80046797f0 Event         WkssvcToAgentStopEvent
     15  fffffa8004088a90 Event         TermSrvReadyEvent
         fffff8800623e300 Section       GDA:  ESENT Performance Data Schema Version 73
         fffffa800205a250 Mutant        WindowsUpdateTracingMutex
         fffffa8002114fc0 Mutant        PSched_Perf_Library_Lock_PID_6fc
         fffff88000950dd0 Section       MSDTC_STATS_FILE
         fffffa80046b0540 Event         LDVP_LPC_4
         fffffa8004965dc0 Event         MSNRecoveryDone
     16  fffffa8004940370 Event         LDVP_LPC_5
         fffffa800466e680 Mutant        ZonesCounterMutex
         fffffa80048dfab0 Job           WmiProviderSubSystemHostJob
         fffffa80046a7400 Event         ccEvtMgr_Terminate_Lock
     17  fffffa8003d8e370 Mutant
C::Users:UserName:AppData:Local:Microsoft:Windows:Explorer:thumbcache_1024.db!dfMaintainer
         fffffa8004292c30 Mutant
C::Users:UserName:AppData:Local:Microsoft:Windows:Explorer:thumbcache_96.db!dfMaintainer
         fffffa80049402f0 Event         LDVP_LPC_6
         fffffa80048b7fc0 Mutant        sMsGsYs.Mb
         fffffa800466a370 Event         wkssvc:  MUP finished initializing event
         fffffa80044f8a50 Event         SENS Started Event
     18  fffff8800518a240 SymbolicLink  Global
         fffffa800495b8e0 Event         LDVP_LPC_7
     19  fffffa8003d594a0 Mutant
C::Users:UserName:AppData:Local:Microsoft:Windows:Explorer:thumbcache_idx.db!ThumbnailCacheInit
         fffffa8004c5fd80 Mutant
C::Users:UserName:AppData:Local:Microsoft:Windows:Explorer:thumbcache_idx.db!rwWriterMutex
         fffffa80020d3830 Mutant        EmdCache_Perf_Library_Lock_PID_6fc
         fffffa800495b860 Event         LDVP_LPC_8
         fffffa8004544060 Mutant        ZonesLockedCacheCounterMutex
         fffffa800422cb50 Mutant        DBWinMutex
         fffffa8004558cc0 Event         AtiOvrDrvMsgEvent_0
         fffffa80043eac30 Mutant        ATI_ExtEventApp_StartupMutex
     20  fffffa80020fc820 Mutant        LOADPERF_MUTEX
         fffffa8001fff880 Mutant        PerfDisk_Perf_Library_Lock_PID_6fc
         fffffa8004310e00 Event         COM+ Tracker Init Event
         fffffa8004853fe0 Event         LDVP_LPC_9
         fffffa80046d1170 Mutant        LDVP_LPC_LOCK
         fffffa80046b0ae0 Event         WMI_ProcessIdleTasksStart
         fffffa80045cfe00 Event         AtiOvrDrvMsgEvent_1
     21  fffffa8004860700 Event         WINMGMT_PROVIDER_CANSHUTDOWN
         fffffa800439c520 Event         WBEM_ESS_OPEN_FOR_BUSINESS
         fffffa800475f5c0 Mutant        Windows Workflow Foundation
3.0.0.0_Perf_Library_Lock_PID_6fc
         fffffa8001fffe80 Mutant        MSSCNTRS_Perf_Library_Lock_PID_6fc
         fffffa80020d3fc0 Mutant        .NET Data Provider for Oracle_Perf_Library_Lock_PID_6fc
         fffff88004decac0 Section       RotHintTable
         fffff8800252d900 Section       Cor_Public_IPCBlock_2612
         fffffa80046c70b0 Event         WkssvcToAgentStartEvent
         fffffa80042d54c0 Event         UMSServicesStarted
     22  fffffa80042a9470 Event         SvcctrlStartEvent_A3752DX
         fffffa80046b0b60 Event         WMI_RevAdap_ACK
         fffffa80040bbcf0 Event         SC_AutoStartComplete
         fffffa800201b730 Mutant        RasPbFile
         fffff880050e99e0 Section       {A64C7F33-DA35-459b-96CA-63B51FB0CDB9}
     23  fffffa8002067140 Event         Microsoft Smart Card Resource Manager Started
         fffffa800475f7a0 Mutant        UGatherer_Perf_Library_Lock_PID_6fc
         fffffa8002060130 Mutant        TermService_Perf_Library_Lock_PID_6fc
```

```
        fffffa80020c0fe0 Event         EVENT_READYROOT/CIMV2SCM EVENT PROVIDER
        fffffa8002965de0 Event         HawkingCheckDefs
        fffffa8004678e50 Event         BFE_Notify_Event_{05b95242-d8cc-47e3-9176-c69de74dc462}
        fffffa8004073ca0 Event         FirstWinlogonCheck
    24  fffffa80020601d0 Mutant        Tcpip_Perf_Library_Lock_PID_6fc
        fffffa80020214c0 Mutant        PscanClientMutex
    25  fffff8800592b3d0 Section       __ComCatalogCache__
        fffffa80020d7150 Mutant        ServiceModelOperation 3.0.0.0_Perf_Library_Lock_PID_6fc
        fffffa80020d3730 Mutant        ESENT_Perf_Library_Lock_PID_6fc
        fffffa800211a640 Mutant        .NET CLR Networking_Perf_Library_Lock_PID_6fc
        fffffa8004874060 Event         IPSEC_POLICY_CHANGE_NOTIFY
    26  fffffa80048bb940 Event         RestartMSIDLLv262144.393232386
        fffffa80048c5880 Event         ShutdownMSIDLLv262144.393232386
        fffffa800207c320 Mutant        WSearchIdxPi_Perf_Library_Lock_PID_6fc
        fffffa80020d74b0 Mutant        .NET CLR Data_Perf_Library_Lock_PID_6fc
        fffffa80020b8ba0 Event         FastTrack
        fffffa8004645820 Event         BFE_Notify_Event_{373ac276-57eb-4038-adde-99f10ad269c4}
    27  fffff880060e5e40 Section       PscanStatBlock
        fffff88002454320 Section       Cor_Public_IPCBlock_2884
        fffff88006368750 Section       LDVP_LPC_BLOCKS
        fffffa800487a6f0 Mutant        XLogAccessMutex
        fffff88005e20a20 Section       IDA0:  ESENT Performance Data Schema Version 73
        fffffa8004862fe0 Event         WMI_ProcessIdleTasksComplete
    28  fffffa8004838e00 Event
C::Users:UserName:AppData:Local:Microsoft:Windows:Explorer:thumbcache_idx.db!rwWriterEvent
        fffffa80020c09e0 Event         EVENT_READYROOT/CIMV2PROVIDERSUBSYSTEM
        fffff88005ccfce0 Section       Wmi Provider Sub System Counters
        fffffa800207c060 Mutant        WmiApRpl_Perf_Library_Lock_PID_6fc
        fffffa8002060270 Mutant        TapiSrv_Perf_Library_Lock_PID_6fc
        fffffa8001fff3d0 Mutant        PerfProc_Perf_Library_Lock_PID_6fc
        fffffa80020d3f20 Mutant        .NET Data Provider for SqlServer_Perf_Library_Lock_PID_6fc
        fffffa80048c04a0 Mutant        ccEvtMgr_Running
        fffffa800205e530 Mutant        APEnablerThread_Mutex
        fffff88005a18830 Section       SENS Information Cache
        fffffa800486d8d0 Mutant        ccEvtMgr_Single_Instance_Lock
        fffff88005ab6160 Section       AtiEeuSharedAdapterHeader
    29  fffffa8001fffb80 Mutant        MSSQL$SQLEXPRESS_Perf_Library_Lock_PID_6fc
        fffff880024f5a50 Section       SqmData_FwtSqmSession10_S-1-5-18
    30  fffff880060ae3e0 Section       WSearchIdxPi
        fffffa8004860330 Event         WINMGMT_COREDLL_CANSHUTDOWN
        fffff88005902230 Section       Debug.Trace.Memory.27c
        fffff880049c2240 Directory     Restricted
    31  fffffa8002114b00 Mutant        RemoteAccess_Perf_Library_Lock_PID_6fc
        fffffa80020d3690 Mutant        Lsa_Perf_Library_Lock_PID_6fc
        fffffa8004c8b110 Event         CorDBIPCSetupSyncEvent_2612
        fffffa8004661760 Mutant        ZonesCacheCounterMutex
        fffff88005e75930 Section       UGATHERER
        fffffa8004859a50 Event         BFE_Notify_Event_{f5d94a5d-09ca-4891-a9b8-c34da3343a59}
        fffffa8004803430 Event         W32TIME_NAMED_EVENT_SYSTIME_NOT_CORRECT
        fffffa8002953780 Mutant        ccSetMgr_Single_Instance_Lock
        fffffa80045a50e0 Event         AtiSafeEscapeEvent_0
    32  fffffa80020fcd40 Mutant        SMSvcHost 3.0.0.0_Perf_Library_Lock_PID_6fc
        fffffa8001fff470 Mutant        PerfOS_Perf_Library_Lock_PID_6fc
        fffffa8004782ef0 Mutant        FwtSqmSession10_S-1-5-18
        fffff88005ebf580 Section       UGthrSvcObj
        fffffa8004558d40 Event         AtiDrvMsgEvent_0
        fffffa80043e7a10 Mutant        {A3BD3259-3E4F-428a-84C8-F0463A9D3EB5}
        fffffa8004389570 Event         LSA_RPC_SERVER_ACTIVE
        fffff880057e0550 Section       Debug.Memory.27c
    33  fffffa8004bf5260 ALPC Port     msctf.serverDefault1
        fffffa800408fde0 Event         TabletHardwarePresent
        fffffa8001ffffc0 Mutant        MSDTC_Perf_Library_Lock_PID_6fc
        fffffa8004394e80 Event         ScNetDrvMsg
    34  fffffa8004853f60 Event         LDVP_LPC_10
        fffffa80048ffe50 Event         000000000002fb84_WlballoonKerberosNotificationEventName
    35  fffff880058d3080 Section       windows_shell_global_counters
        fffffa8001fff330 Mutant        PNRPsvc_Perf_Library_Lock_PID_6fc
        fffff8800609c9f0 Section       Cor_Private_IPCBlock_2884
        fffffa80042349a0 Event         LDVP_LPC_11
        fffffa8004429f50 Event         ScmCreatedEvent
```

```
36  fffffa8004861410 Event         WMI_RevAdap_Set
    fffffa8004234920 Event         LDVP_LPC_12
    fffffa8004888150 Event         IPSEC_POLICY_CHANGE_EVENT
    fffffa80044e02c0 Event         AgentToWkssvcEvent
    fffffa8004661d60 Event         BFE_Notify_Event_{9da795a1-d54d-4970-8174-be55c7c90b6c}
    fffffa80040988e0 Event         WinSta0_DesktopSwitch
```

Kernel Objects

```
1: kd> !object \KernelObjects
Object: fffff88000007060  Type: (fffffa800183fb40) Directory
    ObjectHeader: fffff88000007030 (old version)
    HandleCount: 0  PointerCount: 19
    Directory Object: fffff88000005610  Name: KernelObjects

    Hash Address          Type          Name
    ---- -------          ----          ----
     00  fffffa800189c060 Event         MemoryErrors
     02  fffffa800189b6f0 Event         LowNonPagedPoolCondition
     04  fffffa80041ed130 Session       Session1
     05  fffffa80018814f0 Event         SuperfetchParametersChanged
         fffffa8001883fe0 Event         SuperfetchScenarioNotify
     06  fffffa8001898370 Event         BootLoaderTraceReady
     09  fffffa8001883ee0 Event         SuperfetchTracesReady
     12  fffffa800189b570 Event         HighCommitCondition
     14  fffffa800189b670 Event         HighNonPagedPoolCondition
         fffffa800189b870 Event         HighMemoryCondition
     21  fffff880000082b0 KeyedEvent    CritSecOutOfMemoryEvent
     23  fffffa800189b4f0 Event         MaximumCommitCondition
     25  fffffa800189b5f0 Event         LowCommitCondition
     26  fffffa800189b770 Event         HighPagedPoolCondition
     28  fffffa800189bd80 Event         LowMemoryCondition
     32  fffffa8003fd2fe0 Session       Session0
         fffffa800189b7f0 Event         LowPagedPoolCondition
     34  fffffa8001883f60 Event         PrefetchTracesReady
```

Loaded System Modules

```
1: kd> lmv
start             end                 module name
fffff800`01c00000 fffff800`020d4000   nt         (pdb symbols)
c:\mss\ntkrnlmp.pdb\AD2A616388564BA49EEA0A8070C32B1D2\ntkrnlmp.pdb
    Loaded symbol image file: ntkrnlmp.exe
    Image path: ntkrnlmp.exe
    Image name: ntkrnlmp.exe
    Timestamp:        Wed Oct 10 03:15:16 2007 (470C35B4)
    CheckSum:         0044825D
    ImageSize:        004D4000
    File version:     6.0.6000.16575
    Product version:  6.0.6000.16575
    File flags:       0 (Mask 3F)
    File OS:          40004 NT Win32
    File type:        1.0 App
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      Microsoft Corporation
    ProductName:      Microsoft® Windows® Operating System
    InternalName:     ntkrnlmp.exe
    OriginalFilename: ntkrnlmp.exe
    ProductVersion:   6.0.6000.16575
    FileVersion:      6.0.6000.16575 (vista_gdr.071009-1548)
    FileDescription:  NT Kernel & System
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
fffff800`020d4000 fffff800`02125000   hal        (deferred)
    Image path: hal.dll
    Image name: hal.dll
    Timestamp:        Thu Nov 02 11:11:46 2006 (4549D272)
    CheckSum:         0004BE3C
    ImageSize:        00051000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff960`00000000 fffff960`002b2000   win32k     (pdb symbols)
c:\mss\win32k.pdb\16D90565D4FB4D148677ED97151315E42\win32k.pdb
    Loaded symbol image file: win32k.sys
    Image path: \SystemRoot\System32\win32k.sys
    Image name: win32k.sys
    Timestamp:        Thu Feb 15 03:27:40 2007 (45D3D32C)
    CheckSum:         002A1B51
    ImageSize:        002B2000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff960`00400000 fffff960`0040a000   TSDDD      (deferred)
    Image path: \SystemRoot\System32\TSDDD.dll
    Image name: TSDDD.dll
    Timestamp:        Thu Nov 02 09:52:10 2006 (4549BFCA)
    CheckSum:         00006486
    ImageSize:        0000A000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff960`00600000 fffff960`00611000   cdd        (pdb symbols)
c:\mss\cdd.pdb\024033BD2FD94FB0919B5C310435216A1\cdd.pdb
    Loaded symbol image file: cdd.dll
    Image path: \SystemRoot\System32\cdd.dll
    Image name: cdd.dll
    Timestamp:        Thu Nov 02 11:11:29 2006 (4549D261)
    CheckSum:         00016FFE
    ImageSize:        00011000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`00000000 fffff980`00009000   WMILIB     (deferred)
    Image path: \SystemRoot\system32\drivers\WMILIB.SYS
    Image name: WMILIB.SYS
    Timestamp:        Thu Nov 02 09:43:26 2006 (4549BDBE)
    CheckSum:         0000D492
    ImageSize:        00009000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`00009000 fffff980`00060000   CLFS       (deferred)
```

```
    Image path: \SystemRoot\system32\CLFS.SYS
    Image name: CLFS.SYS
    Timestamp:        Thu Nov 02 09:01:05 2006 (4549B3D1)
    CheckSum:         000577E4
    ImageSize:        00057000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`00060000 fffff980`00069000   PSHED      (deferred)
    Image path: \SystemRoot\system32\PSHED.dll
    Image name: PSHED.dll
    Timestamp:        Thu Nov 02 11:14:26 2006 (4549D312)
    CheckSum:         0000B13A
    ImageSize:        00009000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`00069000 fffff980`00095000   mcupdate_GenuineIntel   (deferred)
    Image path: \SystemRoot\system32\mcupdate_GenuineIntel.dll
    Image name: mcupdate_GenuineIntel.dll
    Timestamp:        Tue Apr 24 05:49:44 2007 (462D8C68)
    CheckSum:         0003798D
    ImageSize:        0002C000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`00095000 fffff980`0009e000   kdcom      (deferred)
    Image path: kdcom.dll
    Image name: kdcom.dll
    Timestamp:        Thu Nov 02 11:14:44 2006 (4549D324)
    CheckSum:         00011D98
    ImageSize:        00009000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`00205000 fffff980`0020d000   intelide   (deferred)
    Image path: \SystemRoot\system32\drivers\intelide.sys
    Image name: intelide.sys
    Timestamp:        Thu Nov 02 09:38:13 2006 (4549BC85)
    CheckSum:         0000BAA6
    ImageSize:        00008000
    File version:     6.0.6000.16386
    Product version:  6.0.6000.16386
    File flags:       0 (Mask 3F)
    File OS:          40004 NT Win32
    File type:        3.7 Driver
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      Microsoft Corporation
    ProductName:      Microsoft® Windows® Operating System
    InternalName:     intelide.sys
    OriginalFilename: intelide.sys
    ProductVersion:   6.0.6000.16386
    FileVersion:      6.0.6000.16386 (vista_rtm.061101-2205)
    FileDescription:  Intel PCI IDE Driver
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
fffff980`0020d000 fffff980`00217000   msisadrv   (deferred)
    Image path: \SystemRoot\system32\drivers\msisadrv.sys
    Image name: msisadrv.sys
    Timestamp:        Thu Nov 02 09:10:06 2006 (4549B5EE)
    CheckSum:         0000C1BA
    ImageSize:        0000A000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`00217000 fffff980`0026a000   acpi       (pdb symbols)
c:\mss\acpi.pdb\7CB6842C78D9400590E5AA62744246E31\acpi.pdb
    Loaded symbol image file: acpi.sys
    Image path: \SystemRoot\system32\drivers\acpi.sys
    Image name: acpi.sys
    Timestamp:        Thu Nov 02 09:10:04 2006 (4549B5EC)
    CheckSum:         00050A17
    ImageSize:        00053000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`0026a000 fffff980`00278000   WDFLDR     (deferred)
    Image path: \SystemRoot\system32\drivers\WDFLDR.SYS
    Image name: WDFLDR.SYS
    Timestamp:        Thu Nov 02 09:42:06 2006 (4549BD6E)
    CheckSum:         00015DDD
    ImageSize:        0000E000
```

```
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`00278000 fffff980`0034e000   Wdf01000   (deferred)
    Image path: \SystemRoot\system32\drivers\Wdf01000.sys
    Image name: Wdf01000.sys
    Timestamp:        Thu Nov 02 09:43:35 2006 (4549BDC7)
    CheckSum:         000D6DBC
    ImageSize:        000D6000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`0034e000 fffff980`00400000   CI         (deferred)
    Image path: \SystemRoot\system32\CI.dll
    Image name: CI.dll
    Timestamp:        Thu Nov 02 11:14:20 2006 (4549D30C)
    CheckSum:         00063848
    ImageSize:        000B2000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`00401000 fffff980`00409000   spldr      (deferred)
    Image path: \SystemRoot\System32\Drivers\spldr.sys
    Image name: spldr.sys
    Timestamp:        Thu Oct 26 00:10:19 2006 (453FEEDB)
    CheckSum:         0000A2A3
    ImageSize:        00008000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`00409000 fffff980`00449000   volsnap    (pdb symbols)
c:\mss\volsnap.pdb\9468F4BEDA5143489F5653787308D68C1\volsnap.pdb
    Loaded symbol image file: volsnap.sys
    Image path: \SystemRoot\system32\drivers\volsnap.sys
    Image name: volsnap.sys
    Timestamp:        Thu Nov 02 09:39:09 2006 (4549BCBD)
    CheckSum:         0003FE6A
    ImageSize:        00040000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`00449000 fffff980`00499000   msrpc      (pdb symbols)
c:\mss\msrpc.pdb\3DE1CDD9259748F0B18D2A8F2BE9E58B1\msrpc.pdb
    Loaded symbol image file: msrpc.sys
    Image path: \SystemRoot\system32\drivers\msrpc.sys
    Image name: msrpc.sys
    Timestamp:        Thu Nov 02 09:36:03 2006 (4549BC03)
    CheckSum:         0005A57C
    ImageSize:        00050000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`00499000 fffff980`004a42c0   PxHlpa64   (deferred)
    Image path: \SystemRoot\System32\Drivers\PxHlpa64.sys
    Image name: PxHlpa64.sys
    Timestamp:        Tue Jul 25 01:18:43 2006 (44C56363)
    CheckSum:         00013DE7
    ImageSize:        0000B2C0
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`004a5000 fffff980`004c14a0   DRVECDB    (deferred)
    Image path: \SystemRoot\System32\Drivers\DRVECDB.SYS
    Image name: DRVECDB.SYS
    Timestamp:        Fri Jul 21 19:21:08 2006 (44C11B14)
    CheckSum:         0002C497
    ImageSize:        0001C4A0
    File version:     8.10.42.0
    Product version:  1.0.0.1
    File flags:       0 (Mask 3F)
    File OS:          4 Unknown Win32
    File type:        3.7 Driver
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      Sonic Solutions
    FileVersion:      8.10.42a
    FileDescription:  Device Driver
    LegalCopyright:   Copyright © Sonic Solutions
fffff980`004c2000 fffff980`004d6000   fileinfo   (deferred)
    Image path: \SystemRoot\system32\drivers\fileinfo.sys
    Image name: fileinfo.sys
    Timestamp:        Thu Nov 02 09:12:51 2006 (4549B693)
    CheckSum:         0001F84D
    ImageSize:        00014000
```

```
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`004d6000 fffff980`00519000   fltmgr     (pdb symbols)
c:\mss\fltMgr.pdb\A35A4E9939754866A8FB3EC3B80C83772\fltMgr.pdb
    Loaded symbol image file: fltmgr.sys
    Image path: \SystemRoot\system32\drivers\fltmgr.sys
    Image name: fltmgr.sys
    Timestamp:        Thu Nov 02 09:01:19 2006 (4549B3DF)
    CheckSum:         00048A13
    ImageSize:        00043000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`00519000 fffff980`0053d000   ataport    (deferred)
    Image path: \SystemRoot\system32\drivers\ataport.SYS
    Image name: ataport.SYS
    Timestamp:        Thu Nov 02 09:38:12 2006 (4549BC84)
    CheckSum:         000259E4
    ImageSize:        00024000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`0053d000 fffff980`00545000   atapi      (deferred)
    Image path: \SystemRoot\system32\drivers\atapi.sys
    Image name: atapi.sys
    Timestamp:        Thu Nov 02 09:38:10 2006 (4549BC82)
    CheckSum:         00012C68
    ImageSize:        00008000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`00545000 fffff980`0059e000   volmgrx    (deferred)
    Image path: \SystemRoot\System32\drivers\volmgrx.sys
    Image name: volmgrx.sys
    Timestamp:        Thu Nov 02 09:38:40 2006 (4549BCA0)
    CheckSum:         0005E26D
    ImageSize:        00059000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`0059e000 fffff980`005ae000   PCIIDEX    (deferred)
    Image path: \SystemRoot\system32\drivers\PCIIDEX.SYS
    Image name: PCIIDEX.SYS
    Timestamp:        Thu Nov 02 09:38:10 2006 (4549BC82)
    CheckSum:         000166B9
    ImageSize:        00010000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`005ae000 fffff980`005c1000   mountmgr   (pdb symbols)
c:\mss\mountmgr.pdb\6992B444C898403692253049AAD44A451\mountmgr.pdb
    Loaded symbol image file: mountmgr.sys
    Image path: \SystemRoot\System32\drivers\mountmgr.sys
    Image name: mountmgr.sys
    Timestamp:        Thu Nov 02 09:37:17 2006 (4549BC4D)
    CheckSum:         0001B535
    ImageSize:        00013000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`005c1000 fffff980`005d3000   volmgr     (pdb symbols)
c:\mss\volmgr.pdb\1E016C79E2794A15BEB82F498BE6D40B1\volmgr.pdb
    Loaded symbol image file: volmgr.sys
    Image path: \SystemRoot\system32\drivers\volmgr.sys
    Image name: volmgr.sys
    Timestamp:        Thu Nov 02 09:38:28 2006 (4549BC94)
    CheckSum:         0001CC6C
    ImageSize:        00012000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`005d3000 fffff980`00600000   pci        (deferred)
    Image path: \SystemRoot\system32\drivers\pci.sys
    Image name: pci.sys
    Timestamp:        Thu Nov 02 09:10:11 2006 (4549B5F3)
    CheckSum:         00037ADA
    ImageSize:        0002D000
    File version:     6.0.6000.16386
    Product version:  6.0.6000.16386
    File flags:       0 (Mask 3F)
    File OS:          40004 NT Win32
    File type:        2.0 Dll
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      Microsoft Corporation
```

```
    ProductName:      Microsoft® Windows® Operating System
    InternalName:     pci.sys
    OriginalFilename: pci.sys
    ProductVersion:   6.0.6000.16386
    FileVersion:      6.0.6000.16386 (vista_rtm.061101-2205)
    FileDescription:  NT Plug and Play PCI Enumerator
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
fffff980`00606000 fffff980`0065a000   NETIO      (deferred)
    Image path: \SystemRoot\system32\drivers\NETIO.SYS
    Image name: NETIO.SYS
    Timestamp:        Fri Sep 28 04:16:58 2007 (46FC722A)
    CheckSum:         00050AF1
    ImageSize:        00054000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`0065a000 fffff980`00800000   ndis       (pdb symbols)
c:\mss\ndis.pdb\EEB96C56FAEB4CD5840C13CBD50CF0492\ndis.pdb
    Loaded symbol image file: ndis.sys
    Image path: \SystemRoot\system32\drivers\ndis.sys
    Image name: ndis.sys
    Timestamp:        Thu Nov 02 09:46:57 2006 (4549BE91)
    CheckSum:         000A83B7
    ImageSize:        001A6000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`00804000 fffff980`0080e000   crcdisk    (deferred)
    Image path: \SystemRoot\system32\drivers\crcdisk.sys
    Image name: crcdisk.sys
    Timestamp:        Thu Nov 02 09:39:40 2006 (4549BCDC)
    CheckSum:         00015FC7
    ImageSize:        0000A000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`0080e000 fffff980`0088a000   ksecdd     (deferred)
    Image path: \SystemRoot\System32\Drivers\ksecdd.sys
    Image name: ksecdd.sys
    Timestamp:        Thu Nov 02 09:25:31 2006 (4549B98B)
    CheckSum:         00083E5F
    ImageSize:        0007C000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`0088a000 fffff980`00a00000   Ntfs       (pdb symbols)
c:\mss\ntfs.pdb\E4B2AB28F0FD4BCA83DE23C9E02AE3362\ntfs.pdb
    Loaded symbol image file: Ntfs.sys
    Image path: \SystemRoot\System32\Drivers\Ntfs.sys
    Image name: Ntfs.sys
    Timestamp:        Thu Nov 02 09:02:04 2006 (4549B40C)
    CheckSum:         0017164C
    ImageSize:        00176000
    File version:     6.0.6000.16386
    Product version:  6.0.6000.16386
    File flags:       0 (Mask 3F)
    File OS:          40004 NT Win32
    File type:        3.7 Driver
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      Microsoft Corporation
    ProductName:      Microsoft® Windows® Operating System
    InternalName:     ntfs.sys
    OriginalFilename: ntfs.sys
    ProductVersion:   6.0.6000.16386
    FileVersion:      6.0.6000.16386 (vista_rtm.061101-2205)
    FileDescription:  NT File System Driver
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
fffff980`00a37000 fffff980`00a39b80   DLAPoolE   (deferred)
    Image path: \SystemRoot\System32\DLA\DLAPoolE.SYS
    Image name: DLAPoolE.SYS
    Timestamp:        Fri Aug 18 21:15:03 2006 (44E61FC7)
    CheckSum:         000057EA
    ImageSize:        00002B80
    File version:     9.1.5.0
    Product version:  1.0.0.1
    File flags:       0 (Mask 3F)
    File OS:          4 Unknown Win32
```

```
    File type:        2.0 Dll
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      Roxio
    FileVersion:      9.01.05a
    FileDescription:  Drive Letter Access Component
    LegalCopyright:   Copyright © 2006 Roxio
fffff980`00b77000 fffff980`00b9f000   CLASSPNP   (pdb symbols)
c:\mss\classpnp.pdb\FB007C1437294488BBCA7C2F2B1103341\classpnp.pdb
    Loaded symbol image file: CLASSPNP.SYS
    Image path: \SystemRoot\system32\drivers\CLASSPNP.SYS
    Image name: CLASSPNP.SYS
    Timestamp:        Thu Nov 02 09:38:10 2006 (4549BC82)
    CheckSum:         0002B329
    ImageSize:        00028000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`00b9f000 fffff980`00bb3000   disk       (deferred)
    Image path: \SystemRoot\system32\drivers\disk.sys
    Image name: disk.sys
    Timestamp:        Thu Nov 02 09:38:20 2006 (4549BC8C)
    CheckSum:         0001B5D7
    ImageSize:        00014000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`00bb3000 fffff980`00bdc000   ecache     (pdb symbols)
c:\mss\ecache.pdb\047868C8DD30461C93A69B62125AFA491\ecache.pdb
    Loaded symbol image file: ecache.sys
    Image path: \SystemRoot\System32\drivers\ecache.sys
    Image name: ecache.sys
    Timestamp:        Thu Nov 02 09:40:11 2006 (4549BCFB)
    CheckSum:         00030550
    ImageSize:        00029000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`00bdc000 fffff980`00bee000   mup        (pdb symbols)
c:\mss\mup.pdb\5877D6B1CEE54C0CAABCF5E2227412452\mup.pdb
    Loaded symbol image file: mup.sys
    Image path: \SystemRoot\System32\Drivers\mup.sys
    Image name: mup.sys
    Timestamp:        Thu Nov 02 09:01:24 2006 (4549B3E4)
    CheckSum:         0000FD93
    ImageSize:        00012000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`00bee000 fffff980`00c00000   partmgr    (deferred)
    Image path: \SystemRoot\System32\drivers\partmgr.sys
    Image name: partmgr.sys
    Timestamp:        Thu Nov 02 09:38:30 2006 (4549BC96)
    CheckSum:         00015CEF
    ImageSize:        00012000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`01210000 fffff980`0121f000   watchdog   (pdb symbols)
c:\mss\watchdog.pdb\C6F947E78226424B8D9A627525F43C321\watchdog.pdb
    Loaded symbol image file: watchdog.sys
    Image path: \SystemRoot\System32\drivers\watchdog.sys
    Image name: watchdog.sys
    Timestamp:        Thu Nov 02 09:15:27 2006 (4549B72F)
    CheckSum:         0000F9FE
    ImageSize:        0000F000
    File version:     6.0.6000.16386
    Product version:  6.0.6000.16386
    File flags:       0 (Mask 3F)
    File OS:          40004 NT Win32
    File type:        2.0 Dll
    File date:        00000000.00000000
    Translations:     0000.04b0
    CompanyName:      Microsoft Corporation
    ProductName:      Microsoft® Windows® Operating System
    InternalName:     watchdog.sys
    OriginalFilename: watchdog.sys
    ProductVersion:   6.0.6000.16386
    FileVersion:      6.0.6000.16386 (vista_rtm.061101-2205)
    FileDescription:  Watchdog Driver
```

```
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
fffff980`0123e000 fffff980`0123f480   swenum     (deferred)
    Image path: \SystemRoot\system32\DRIVERS\swenum.sys
    Image name: swenum.sys
    Timestamp:        Thu Nov 02 09:37:33 2006 (4549BC5D)
    CheckSum:         0000447A
    ImageSize:        00001480
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`01250000 fffff980`01251d80   USBD       (deferred)
    Image path: \SystemRoot\system32\DRIVERS\USBD.SYS
    Image name: USBD.SYS
    Timestamp:        Thu Nov 02 09:43:35 2006 (4549BDC7)
    CheckSum:         0000EE3E
    ImageSize:        00001D80
    File version:     6.0.6000.16386
    Product version:  6.0.6000.16386
    File flags:       0 (Mask 3F)
    File OS:          40004 NT Win32
    File type:        2.0 Dll
    File date:        00000000.00000000
    Translations:     0000.04b0
    CompanyName:      Microsoft Corporation
    ProductName:      Microsoft® Windows® Operating System
    InternalName:     usbd.sys
    OriginalFilename: usbd.sys
    ProductVersion:   6.0.6000.16386
    FileVersion:      6.0.6000.16386 (vista_rtm.061101-2205)
    FileDescription:  Universal Serial Bus Driver
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
fffff980`012d2000 fffff980`012e2000   usbehci    (pdb symbols)
c:\mss\usbehci.pdb\C035065118AF49A2B50A6BFA09578B531\usbehci.pdb
    Loaded symbol image file: usbehci.sys
    Image path: \SystemRoot\system32\DRIVERS\usbehci.sys
    Image name: usbehci.sys
    Timestamp:        Thu Nov 02 09:43:41 2006 (4549BDCD)
    CheckSum:         00018AD2
    ImageSize:        00010000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`01500000 fffff980`01510000   umbus      (deferred)
    Image path: \SystemRoot\system32\DRIVERS\umbus.sys
    Image name: umbus.sys
    Timestamp:        Thu Nov 02 09:44:03 2006 (4549BDE3)
    CheckSum:         0000BE1B
    ImageSize:        00010000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`015c0000 fffff980`015d0000   raspppoe   (deferred)
    Image path: \SystemRoot\system32\DRIVERS\raspppoe.sys
    Image name: raspppoe.sys
    Timestamp:        Thu Nov 02 09:47:32 2006 (4549BEB4)
    CheckSum:         000187F3
    ImageSize:        00010000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`02e05000 fffff980`02e11000   tunnel     (deferred)
    Image path: \SystemRoot\system32\DRIVERS\tunnel.sys
    Image name: tunnel.sys
    Timestamp:        Thu Jun 07 03:46:08 2007 (46677170)
    CheckSum:         000086B0
    ImageSize:        0000C000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`02e16000 fffff980`02e22000   Dxapi      (deferred)
    Image path: \SystemRoot\System32\drivers\Dxapi.sys
    Image name: Dxapi.sys
    Timestamp:        Thu Nov 02 09:16:03 2006 (4549B753)
    CheckSum:         0000E35F
    ImageSize:        0000C000
    File version:     6.0.6000.16386
    Product version:  6.0.6000.16386
    File flags:       0 (Mask 3F)
    File OS:          40004 NT Win32
    File type:        3.7 Driver
```

```
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      Microsoft Corporation
    ProductName:      Microsoft® Windows® Operating System
    InternalName:     dxapi.sys
    OriginalFilename: dxapi.sys
    ProductVersion:   6.0.6000.16386
    FileVersion:      6.0.6000.16386 (vista_rtm.061101-2205)
    FileDescription:  DirectX API Driver
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
fffff980`02e55000 fffff980`02e67000   intelppm   (deferred)
    Image path: \SystemRoot\system32\DRIVERS\intelppm.sys
    Image name: intelppm.sys
    Timestamp:        Thu Nov 02 09:00:15 2006 (4549B39F)
    CheckSum:         00010B1D
    ImageSize:        00012000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`02e67000 fffff980`02e70000   tunmp      (deferred)
    Image path: \SystemRoot\system32\DRIVERS\tunmp.sys
    Image name: tunmp.sys
    Timestamp:        Thu Jun 07 03:45:55 2007 (46677163)
    CheckSum:         00013012
    ImageSize:        00009000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`02ec5000 fffff980`02ed6000   Npfs       (pdb symbols)
c:\mss\npfs.pdb\6E087C3561CA494B978F18443B1CC75F1\npfs.pdb
    Loaded symbol image file: Npfs.SYS
    Image path: \SystemRoot\System32\Drivers\Npfs.SYS
    Image name: Npfs.SYS
    Timestamp:        Thu Nov 02 09:01:04 2006 (4549B3D0)
    CheckSum:         00017ED5
    ImageSize:        00011000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`02fa8000 fffff980`02fafb80   HIDPARSE   (deferred)
    Image path: \SystemRoot\system32\DRIVERS\HIDPARSE.SYS
    Image name: HIDPARSE.SYS
    Timestamp:        Thu Nov 02 09:43:35 2006 (4549BDC7)
    CheckSum:         000153EC
    ImageSize:        00007B80
    File version:     6.0.6000.16386
    Product version:  6.0.6000.16386
    File flags:       0 (Mask 3F)
    File OS:          40004 NT Win32
    File type:        2.0 Dll
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      Microsoft Corporation
    ProductName:      Microsoft® Windows® Operating System
    InternalName:     hidparse.sys
    OriginalFilename: hidparse.sys
    ProductVersion:   6.0.6000.16386
    FileVersion:      6.0.6000.16386 (vista_rtm.061101-2205)
    FileDescription:  Hid Parsing Library
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
fffff980`02fc8000 fffff980`02fd0000   dump_atapi   (deferred)
    Image path: \SystemRoot\System32\Drivers\dump_atapi.sys
    Image name: dump_atapi.sys
    Timestamp:        Thu Nov 02 09:38:10 2006 (4549BC82)
    CheckSum:         00012C68
    ImageSize:        00008000
    File version:     6.0.6000.16386
    Product version:  6.0.6000.16386
    File flags:       0 (Mask 3F)
    File OS:          40004 NT Win32
    File type:        3.7 Driver
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      Microsoft Corporation
    ProductName:      Microsoft® Windows® Operating System
    InternalName:     atapi.sys
```

```
    OriginalFilename: atapi.sys
    ProductVersion:   6.0.6000.16386
    FileVersion:      6.0.6000.16386 (vista_rtm.061101-2205)
    FileDescription:  ATAPI IDE Miniport Driver
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
fffff980`02fd0000 fffff980`02fd7e80   DLARTL_E   (export symbols)       DLARTL_E.SYS
    Loaded symbol image file: DLARTL_E.SYS
    Image path: \SystemRoot\System32\Drivers\DLARTL_E.SYS
    Image name: DLARTL_E.SYS
    Timestamp:        Fri Aug 11 18:33:47 2006 (44DCBF7B)
    CheckSum:         000102A9
    ImageSize:        00007E80
    File version:     0.0.0.0
    Product version:  1.0.0.1
    File flags:       0 (Mask 3F)
    File OS:          4 Unknown Win32
    File type:        2.0 Dll
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      Roxio
    FileVersion:      local_build
    FileDescription:  Shared Driver Component
    LegalCopyright:   Copyright © 2006 Roxio
fffff980`03006000 fffff980`03022000   parport    (pdb symbols)
c:\mss\parport.pdb\3A595972408E4D2B8680F39D8441A4521\parport.pdb
    Loaded symbol image file: parport.sys
    Image path: \SystemRoot\system32\DRIVERS\parport.sys
    Image name: parport.sys
    Timestamp:        Thu Nov 02 09:37:57 2006 (4549BC75)
    CheckSum:         0001A267
    ImageSize:        0001C000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`03022000 fffff980`03035000   HDAudBus   (deferred)
    Image path: \SystemRoot\system32\DRIVERS\HDAudBus.sys
    Image name: HDAudBus.sys
    Timestamp:        Mon Oct 16 17:33:33 2006 (4533B45D)
    CheckSum:         0000F37C
    ImageSize:        00013000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`03035000 fffff980`03041000   usbuhci    (pdb symbols)
c:\mss\usbuhci.pdb\DEBFBF62E37B4F818F6ECE18B8E22FA71\usbuhci.pdb
    Loaded symbol image file: usbuhci.sys
    Image path: \SystemRoot\system32\DRIVERS\usbuhci.sys
    Image name: usbuhci.sys
    Timestamp:        Thu Nov 02 09:43:40 2006 (4549BDCC)
    CheckSum:         0000D8B2
    ImageSize:        0000C000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`03074000 fffff980`0307d000   hidusb     (pdb symbols)
c:\mss\hidusb.pdb\5E300317E8A44F418A3EECB71D7396E31\hidusb.pdb
    Loaded symbol image file: hidusb.sys
    Image path: \SystemRoot\system32\DRIVERS\hidusb.sys
    Image name: hidusb.sys
    Timestamp:        Thu Nov 02 09:43:36 2006 (4549BDC8)
    CheckSum:         000095B2
    ImageSize:        00009000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`030aa000 fffff980`030b3000   Null       (deferred)
    Image path: \SystemRoot\System32\Drivers\Null.SYS
    Image name: Null.SYS
    Timestamp:        Thu Nov 02 09:37:15 2006 (4549BC4B)
    CheckSum:         0000B49D
    ImageSize:        00009000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`030b3000 fffff980`030bc000   RDPCDD     (deferred)
    Image path: \SystemRoot\System32\DRIVERS\RDPCDD.sys
    Image name: RDPCDD.sys
    Timestamp:        Thu Nov 02 09:52:09 2006 (4549BFC9)
    CheckSum:         0000231D
    ImageSize:        00009000
```

```
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`030bc000 fffff980`030c5000   rdpencdd   (deferred)
    Image path: \SystemRoot\system32\drivers\rdpencdd.sys
    Image name: rdpencdd.sys
    Timestamp:        Thu Nov 02 09:52:10 2006 (4549BFCA)
    CheckSum:         0000C9EE
    ImageSize:        00009000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`030c5000 fffff980`030ce000   rasacd     (pdb symbols)
c:\mss\rasacd.pdb\AA80C81F9CBA4F1DB467D81D96AF28C81\rasacd.pdb
    Loaded symbol image file: rasacd.sys
    Image path: \SystemRoot\System32\DRIVERS\rasacd.sys
    Image name: rasacd.sys
    Timestamp:        Thu Nov 02 09:47:34 2006 (4549BEB6)
    CheckSum:         0000B7D6
    ImageSize:        00009000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`030ce000 fffff980`030d6900   DLABOIOE   (no symbols)
    Loaded symbol image file: DLABOIOE.SYS
    Image path: \SystemRoot\System32\DLA\DLABOIOE.SYS
    Image name: DLABOIOE.SYS
    Timestamp:        Fri Aug 18 21:15:40 2006 (44E61FEC)
    CheckSum:         000150C3
    ImageSize:        00008900
    File version:     9.1.5.0
    Product version:  1.0.0.1
    File flags:       0 (Mask 3F)
    File OS:          4 Unknown Win32
    File type:        2.0 Dll
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      Roxio
    FileVersion:      9.01.05a
    FileDescription:  Drive Letter Access Component
    LegalCopyright:   Copyright © 2006 Roxio
fffff980`0313f000 fffff980`03141380   DLACDBHE   (deferred)
    Image path: \SystemRoot\System32\Drivers\DLACDBHE.SYS
    Image name: DLACDBHE.SYS
    Timestamp:        Fri Aug 11 18:34:57 2006 (44DCBFC1)
    CheckSum:         00013C57
    ImageSize:        00002380
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`03174000 fffff980`0317e000   kbdhid     (deferred)
    Image path: \SystemRoot\system32\DRIVERS\kbdhid.sys
    Image name: kbdhid.sys
    Timestamp:        Thu Nov 02 09:37:27 2006 (4549BC57)
    CheckSum:         0000F32D
    ImageSize:        0000A000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`0317e000 fffff980`03188000   Fs_Rec     (deferred)
    Image path: \SystemRoot\System32\Drivers\Fs_Rec.SYS
    Image name: Fs_Rec.SYS
    Timestamp:        Tue Apr 17 02:37:50 2007 (462424EE)
    CheckSum:         000123EA
    ImageSize:        0000A000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`03188000 fffff980`03191180   DLABMFSE   (deferred)
    Image path: \SystemRoot\System32\DLA\DLABMFSE.SYS
    Image name: DLABMFSE.SYS
    Timestamp:        Fri Aug 18 21:15:45 2006 (44E61FF1)
    CheckSum:         00011164
    ImageSize:        00009180
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`03806000 fffff980`03822000   cdrom      (pdb symbols)
c:\mss\cdrom.pdb\ADFDE370A5A245959C96D401AFAF077B1\cdrom.pdb
    Loaded symbol image file: cdrom.sys
    Image path: \SystemRoot\system32\DRIVERS\cdrom.sys
    Image name: cdrom.sys
    Timestamp:        Thu Nov 02 09:38:24 2006 (4549BC90)
    CheckSum:         00022C12
```

```
    ImageSize:        0001C000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`03822000 fffff980`0382e000   serenum    (deferred)
    Image path: \SystemRoot\system32\DRIVERS\serenum.sys
    Image name: serenum.sys
    Timestamp:        Thu Nov 02 09:37:58 2006 (4549BC76)
    CheckSum:         000119F1
    ImageSize:        0000C000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`0382e000 fffff980`0384b000   serial     (deferred)
    Image path: \SystemRoot\system32\DRIVERS\serial.sys
    Image name: serial.sys
    Timestamp:        Thu Nov 02 09:38:02 2006 (4549BC7A)
    CheckSum:         000254F5
    ImageSize:        0001D000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`0384b000 fffff980`0387f000   b57nd60a   (deferred)
    Image path: \SystemRoot\system32\DRIVERS\b57nd60a.sys
    Image name: b57nd60a.sys
    Timestamp:        Fri Aug 18 07:46:59 2006 (44E56263)
    CheckSum:         0003040C
    ImageSize:        00034000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`0387f000 fffff980`038c4000   USBPORT    (pdb symbols)
c:\mss\usbport.pdb\D32FD0E49915414E972075182B4CF2B01\usbport.pdb
    Loaded symbol image file: USBPORT.SYS
    Image path: \SystemRoot\system32\DRIVERS\USBPORT.SYS
    Image name: USBPORT.SYS
    Timestamp:        Thu Nov 02 09:43:47 2006 (4549BDD3)
    CheckSum:         00041D26
    ImageSize:        00045000
    File version:     6.0.6000.16386
    Product version:  6.0.6000.16386
    File flags:       0 (Mask 3F)
    File OS:          40004 NT Win32
    File type:        2.0 Dll
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      Microsoft Corporation
    ProductName:      Microsoft® Windows® Operating System
    InternalName:     usbport.sys
    OriginalFilename: usbport.sys
    ProductVersion:   6.0.6000.16386
    FileVersion:      6.0.6000.16386 (vista_rtm.061101-2205)
    FileDescription:  USB 1.1 & 2.0 Port Driver
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
fffff980`038c4000 fffff980`039a0000   dxgkrnl    (pdb symbols)
c:\mss\dxgkrnl.pdb\CBB59D3CA0C54796BACC0476BF4294D61\dxgkrnl.pdb
    Loaded symbol image file: dxgkrnl.sys
    Image path: \SystemRoot\System32\drivers\dxgkrnl.sys
    Image name: dxgkrnl.sys
    Timestamp:        Thu Nov 02 09:16:36 2006 (4549B774)
    CheckSum:         000DE4E9
    ImageSize:        000DC000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`039e8000 fffff980`039ed100   ksthunk    (deferred)
    Image path: \SystemRoot\system32\drivers\ksthunk.sys
    Image name: ksthunk.sys
    Timestamp:        Thu Nov 02 09:37:32 2006 (4549BC5C)
    CheckSum:         000055BF
    ImageSize:        00005100
    File version:     6.0.6000.16386
    Product version:  6.0.6000.16386
    File flags:       0 (Mask 3F)
    File OS:          40004 NT Win32
    File type:        3.0 Driver
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      Microsoft Corporation
    ProductName:      Microsoft® Windows® Operating System
```

```
    InternalName:     ksthunk.sys
    OriginalFilename: ksthunk.sys
    ProductVersion:   6.0.6000.16386
    FileVersion:      6.0.6000.16386 (vista_rtm.061101-2205)
    FileDescription:  Kernel Streaming WOW Thunk Service
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
fffff980`03a01000 fffff980`03a1f000   rasl2tp    (deferred)
    Image path: \SystemRoot\system32\DRIVERS\rasl2tp.sys
    Image name: rasl2tp.sys
    Timestamp:        Thu Nov 02 09:47:36 2006 (4549BEB8)
    CheckSum:         0001C626
    ImageSize:        0001E000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`03a1f000 fffff980`03a2c000   TDI         (deferred)
    Image path: \SystemRoot\system32\DRIVERS\TDI.SYS
    Image name: TDI.SYS
    Timestamp:        Thu Nov 02 09:48:18 2006 (4549BEE2)
    CheckSum:         0000C89E
    ImageSize:        0000D000
    File version:     6.0.6000.16386
    Product version:  6.0.6000.16386
    File flags:       0 (Mask 3F)
    File OS:          40004 NT Win32
    File type:        3.6 Driver
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      Microsoft Corporation
    ProductName:      Microsoft® Windows® Operating System
    InternalName:     tdi.sys
    OriginalFilename: tdi.sys
    ProductVersion:   6.0.6000.16386
    FileVersion:      6.0.6000.16386 (vista_rtm.061101-2205)
    FileDescription:  TDI Wrapper
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
fffff980`03a2c000 fffff980`03a5f000   msiscsi    (deferred)
    Image path: \SystemRoot\system32\DRIVERS\msiscsi.sys
    Image name: msiscsi.sys
    Timestamp:        Thu Nov 02 09:40:03 2006 (4549BCF3)
    CheckSum:         000368B5
    ImageSize:        00033000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`03a5f000 fffff980`04200000   atikmdag   (export symbols)       atikmdag.sys
    Loaded symbol image file: atikmdag.sys
    Image path: \SystemRoot\system32\DRIVERS\atikmdag.sys
    Image name: atikmdag.sys
    Timestamp:        Wed Oct 25 02:55:03 2006 (453EC3F7)
    CheckSum:         0027D96C
    ImageSize:        007A1000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`04204000 fffff980`0424a000   usbhub     (pdb symbols)
c:\mss\usbhub.pdb\84D343AEC732448F94DF1A9C49CE56021\usbhub.pdb
    Loaded symbol image file: usbhub.sys
    Image path: \SystemRoot\system32\DRIVERS\usbhub.sys
    Image name: usbhub.sys
    Timestamp:        Thu Nov 02 09:43:55 2006 (4549BDDB)
    CheckSum:         0004BD8B
    ImageSize:        00046000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`0424a000 fffff980`04255000   mssmbios   (deferred)
    Image path: \SystemRoot\system32\DRIVERS\mssmbios.sys
    Image name: mssmbios.sys
    Timestamp:        Thu Nov 02 09:10:10 2006 (4549B5F2)
    CheckSum:         0001514F
    ImageSize:        0000B000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`04255000 fffff980`0428a000   ks         (deferred)
    Image path: \SystemRoot\system32\DRIVERS\ks.sys
    Image name: ks.sys
    Timestamp:        Thu Nov 02 09:37:43 2006 (4549BC67)
    CheckSum:         00039E07
```

```
    ImageSize:        00035000
    File version:     6.0.6000.16386
    Product version:  6.0.6000.16386
    File flags:       0 (Mask 3F)
    File OS:          40004 NT Win32
    File type:        3.0 Driver
    File date:        00000000.00000000
    Translations:     0000.04b0
    CompanyName:      Microsoft Corporation
    ProductName:      Microsoft® Windows® Operating System
    InternalName:     ks.sys
    OriginalFilename: ks.sys
    ProductVersion:   6.0.6000.16386
    FileVersion:      6.0.6000.16386 (vista_rtm.061101-2205)
    FileDescription:  Kernel CSA Library
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
fffff980`0428a000 fffff980`04296000   mouclass   (pdb symbols)
c:\mss\mouclass.pdb\8BE426D68BD3432EB225C22D6D4DB6411\mouclass.pdb
    Loaded symbol image file: mouclass.sys
    Image path: \SystemRoot\system32\DRIVERS\mouclass.sys
    Image name: mouclass.sys
    Timestamp:        Thu Nov 02 09:37:22 2006 (4549BC52)
    CheckSum:         000168D2
    ImageSize:        0000C000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`04296000 fffff980`042a4000   kbdclass   (pdb symbols)
c:\mss\kbdclass.pdb\39B94B09A3CB4C31AB098C2B1D796EF41\kbdclass.pdb
    Loaded symbol image file: kbdclass.sys
    Image path: \SystemRoot\system32\DRIVERS\kbdclass.sys
    Image name: kbdclass.sys
    Timestamp:        Thu Nov 02 09:37:21 2006 (4549BC51)
    CheckSum:         00014EFA
    ImageSize:        0000E000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`042a4000 fffff980`042b6000   termdd     (deferred)
    Image path: \SystemRoot\system32\DRIVERS\termdd.sys
    Image name: termdd.sys
    Timestamp:        Thu Nov 02 09:52:08 2006 (4549BFC8)
    CheckSum:         0001699B
    ImageSize:        00012000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`042b6000 fffff980`042c5000   netbios    (deferred)
    Image path: \SystemRoot\system32\DRIVERS\netbios.sys
    Image name: netbios.sys
    Timestamp:        Thu Nov 02 09:46:38 2006 (4549BE7E)
    CheckSum:         00016B99
    ImageSize:        0000F000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`042c5000 fffff980`0435d000   rdpdr      (pdb symbols)
c:\mss\rdpdr.pdb\9F562EA9AF2D4128A626FEE847271B111\rdpdr.pdb
    Loaded symbol image file: rdpdr.sys
    Image path: \SystemRoot\system32\DRIVERS\rdpdr.sys
    Image name: rdpdr.sys
    Timestamp:        Thu Nov 02 09:53:43 2006 (4549C027)
    CheckSum:         00058EF8
    ImageSize:        00098000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`0435d000 fffff980`04375000   raspptp    (pdb symbols)
c:\mss\raspptp.pdb\95285CF5CE154884B76A6748C9ABA2DA2\raspptp.pdb
    Loaded symbol image file: raspptp.sys
    Image path: \SystemRoot\system32\DRIVERS\raspptp.sys
    Image name: raspptp.sys
    Timestamp:        Thu Nov 02 09:47:36 2006 (4549BEB8)
    CheckSum:         00022B61
    ImageSize:        00018000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`04375000 fffff980`0439e000   ndiswan    (pdb symbols)
c:\mss\ndiswan.pdb\BB654C93D7AB4F6EB8D64A8C698C75F92\ndiswan.pdb
    Loaded symbol image file: ndiswan.sys
    Image path: \SystemRoot\system32\DRIVERS\ndiswan.sys
```

```
    Image name: ndiswan.sys
    Timestamp:        Thu Nov 02 09:47:35 2006 (4549BEB7)
    CheckSum:         00027668
    ImageSize:        00029000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`0439e000 fffff980`043aa000   ndistapi   (pdb symbols)
c:\mss\ndistapi.pdb\463A1616E203466381C8859581549A6C1\ndistapi.pdb
    Loaded symbol image file: ndistapi.sys
    Image path: \SystemRoot\system32\DRIVERS\ndistapi.sys
    Image name: ndistapi.sys
    Timestamp:        Thu Nov 02 09:47:26 2006 (4549BEAE)
    CheckSum:         00008F1B
    ImageSize:        0000C000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`043aa000 fffff980`04400000   storport   (deferred)
    Image path: \SystemRoot\system32\DRIVERS\storport.sys
    Image name: storport.sys
    Timestamp:        Thu Nov 02 09:38:25 2006 (4549BC91)
    CheckSum:         00025342
    ImageSize:        00056000
    File version:     6.0.6000.16386
    Product version:  6.0.6000.16386
    File flags:       0 (Mask 3F)
    File OS:          40004 NT Win32
    File type:        3.7 Driver
    File date:        00000000.00000000
    Translations:     0000.04b0
    CompanyName:      Microsoft Corporation
    ProductName:      Microsoft® Windows® Operating System
    InternalName:     storport.sys
    OriginalFilename: storport.sys
    ProductVersion:   6.0.6000.16386
    FileVersion:      6.0.6000.16386 (vista_rtm.061101-2205)
    FileDescription:  Microsoft Storage Port Driver
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
fffff980`04402000 fffff980`0440d000   mouhid     (deferred)
    Image path: \SystemRoot\system32\DRIVERS\mouhid.sys
    Image name: mouhid.sys
    Timestamp:        Thu Nov 02 09:37:27 2006 (4549BC57)
    CheckSum:         00012A33
    ImageSize:        0000B000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`0440d000 fffff980`0442f000   ENG64      (deferred)
    Image path: \??\C:\PROGRA~3\Symantec\DEFINI~1\VIRUSD~1\20080125.004\ENG64.SYS
    Image name: ENG64.SYS
    Timestamp:        Fri Jan 18 14:16:52 2008 (4790B4D4)
    CheckSum:         00025D4A
    ImageSize:        00022000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`0442f000 fffff980`04447000   SRTSPX64   (deferred)
    Image path: \SystemRoot\System32\Drivers\SRTSPX64.SYS
    Image name: SRTSPX64.SYS
    Timestamp:        Sat Nov 18 06:03:57 2006 (455EA24D)
    CheckSum:         0000D7D7
    ImageSize:        00018000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`04447000 fffff980`044bb000   SRTSP64    (deferred)
    Image path: \SystemRoot\System32\Drivers\SRTSP64.SYS
    Image name: SRTSP64.SYS
    Timestamp:        Sat Nov 18 06:03:57 2006 (455EA24D)
    CheckSum:         00066BBE
    ImageSize:        00074000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`0452b000 fffff980`0454e000   drmk       (deferred)
    Image path: \SystemRoot\system32\drivers\drmk.sys
    Image name: drmk.sys
    Timestamp:        Thu Nov 02 10:52:47 2006 (4549CDFF)
    CheckSum:         0002B94E
    ImageSize:        00023000
    File version:     6.0.6000.16386
```

```
    Product version:  6.0.6000.16386
    File flags:       0 (Mask 3F)
    File OS:          40004 NT Win32
    File type:        2.0 Dll
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      Microsoft Corporation
    ProductName:      Microsoft® Windows® Operating System
    InternalName:     drmk.sys
    OriginalFilename: drmk.sys
    ProductVersion:   6.0.6000.16386
    FileVersion:      6.0.6000.16386 (vista_rtm.061101-2205)
    FileDescription:  Microsoft Kernel DRM Descrambler Filter
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
fffff980`0454e000 fffff980`04589000   portcls    (deferred)
    Image path: \SystemRoot\system32\drivers\portcls.sys
    Image name: portcls.sys
    Timestamp:        Thu Nov 02 09:43:42 2006 (4549BDCE)
    CheckSum:         0003D954
    ImageSize:        0003B000
    File version:     6.0.6000.16386
    Product version:  6.0.6000.16386
    File flags:       0 (Mask 3F)
    File OS:          40004 NT Win32
    File type:        3.9 Driver
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      Microsoft Corporation
    ProductName:      Microsoft® Windows® Operating System
    InternalName:     portcls.sys
    OriginalFilename: portcls.sys
    ProductVersion:   6.0.6000.16386
    FileVersion:      6.0.6000.16386 (vista_rtm.061101-2205)
    FileDescription:  Port Class (Class Driver for Port/Miniport Devices)
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
fffff980`04589000 fffff980`045ec000   ADIHdAud   (deferred)
    Image path: \SystemRoot\system32\drivers\ADIHdAud.sys
    Image name: ADIHdAud.sys
    Timestamp:        Wed Sep 27 22:15:41 2006 (451AE9FD)
    CheckSum:         0006047B
    ImageSize:        00063000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`045ec000 fffff980`04600000   NDProxy    (pdb symbols)
c:\mss\ndproxy.pdb\1E6588D4B5DE4A118859564F8DEE56421\ndproxy.pdb
    Loaded symbol image file: NDProxy.SYS
    Image path: \SystemRoot\System32\Drivers\NDProxy.SYS
    Image name: NDProxy.SYS
    Timestamp:        Thu Nov 02 09:47:30 2006 (4549BEB2)
    CheckSum:         00017578
    ImageSize:        00014000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`04835000 fffff980`0485a000   VIDEOPRT   (deferred)
    Image path: \SystemRoot\System32\drivers\VIDEOPRT.SYS
    Image name: VIDEOPRT.SYS
    Timestamp:        Thu Nov 02 09:42:04 2006 (4549BD6C)
    CheckSum:         0002BA27
    ImageSize:        00025000
    File version:     6.0.6000.16386
    Product version:  6.0.6000.16386
    File flags:       0 (Mask 3F)
    File OS:          40004 NT Win32
    File type:        3.4 Driver
    File date:        00000000.00000000
    Translations:     0000.04b0
    CompanyName:      Microsoft Corporation
    ProductName:      Microsoft® Windows® Operating System
    InternalName:     videoprt.sys
    OriginalFilename: videoprt.sys
    ProductVersion:   6.0.6000.16386
    FileVersion:      6.0.6000.16386 (vista_rtm.061101-2205)
```

```
    FileDescription:  Video Port Driver
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
fffff980`04867000 fffff980`04875000   vga        (deferred)
    Image path: \SystemRoot\System32\drivers\vga.sys
    Image name: vga.sys
    Timestamp:        Thu Nov 02 09:41:53 2006 (4549BD61)
    CheckSum:         0001199E
    ImageSize:        0000E000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`04875000 fffff980`04881000   nsiproxy   (pdb symbols)
c:\mss\nsiproxy.pdb\FEDF66ED29E944099E9061891C846E291\nsiproxy.pdb
    Loaded symbol image file: nsiproxy.sys
    Image path: \SystemRoot\system32\drivers\nsiproxy.sys
    Image name: nsiproxy.sys
    Timestamp:        Thu Nov 02 09:46:47 2006 (4549BE87)
    CheckSum:         0000F22A
    ImageSize:        0000C000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`04881000 fffff980`04893000   HIDCLASS   (pdb symbols)
c:\mss\hidclass.pdb\9552798607044C03801658C280A7C5BE1\hidclass.pdb
    Loaded symbol image file: HIDCLASS.SYS
    Image path: \SystemRoot\system32\DRIVERS\HIDCLASS.SYS
    Image name: HIDCLASS.SYS
    Timestamp:        Thu Nov 02 09:43:36 2006 (4549BDC8)
    CheckSum:         00016B0D
    ImageSize:        00012000
    File version:     6.0.6000.16386
    Product version:  6.0.6000.16386
    File flags:       0 (Mask 3F)
    File OS:          40004 NT Win32
    File type:        2.0 Dll
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      Microsoft Corporation
    ProductName:      Microsoft® Windows® Operating System
    InternalName:     hidclass.sys
    OriginalFilename: hidclass.sys
    ProductVersion:   6.0.6000.16386
    FileVersion:      6.0.6000.16386 (vista_rtm.061101-2205)
    FileDescription:  Hid Class Library
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
fffff980`048a3000 fffff980`04a00000   EX64       (deferred)
    Image path: \??\C:\PROGRA~3\Symantec\DEFINI~1\VIRUSD~1\20080125.004\EX64.SYS
    Image name: EX64.SYS
    Timestamp:        Fri Jan 18 13:35:48 2008 (4790AB34)
    CheckSum:         0016A366
    ImageSize:        0015D000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`04a00000 fffff980`04a6a000   afd        (pdb symbols)
c:\mss\afd.pdb\4454D557A71040CFBBB0A664E5E9BAA02\afd.pdb
    Loaded symbol image file: afd.sys
    Image path: \SystemRoot\system32\drivers\afd.sys
    Image name: afd.sys
    Timestamp:        Thu Nov 02 09:48:12 2006 (4549BEDC)
    CheckSum:         0006FD4D
    ImageSize:        0006A000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`04a6a000 fffff980`04a85000   smb        (pdb symbols)
c:\mss\smb.pdb\2E4AA01275B64ED3BC522390DA9C98CE1\smb.pdb
    Loaded symbol image file: smb.sys
    Image path: \SystemRoot\system32\DRIVERS\smb.sys
    Image name: smb.sys
    Timestamp:        Thu Nov 02 09:46:20 2006 (4549BE6C)
    CheckSum:         0001C14B
    ImageSize:        0001B000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`04a85000 fffff980`04aa0000   tdx        (deferred)
    Image path: \SystemRoot\system32\DRIVERS\tdx.sys
    Image name: tdx.sys
    Timestamp:        Thu Nov 02 09:46:56 2006 (4549BE90)
```

```
    CheckSum:         0001B54C
    ImageSize:        0001B000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`04aa0000 fffff980`04ac8000   fwpkclnt   (deferred)
    Image path: \SystemRoot\System32\drivers\fwpkclnt.sys
    Image name: fwpkclnt.sys
    Timestamp:        Thu Nov 02 09:46:48 2006 (4549BE88)
    CheckSum:         0002685E
    ImageSize:        00028000
    File version:     6.0.6000.16386
    Product version:  6.0.6000.16386
    File flags:       0 (Mask 3F)
    File OS:          40004 NT Win32
    File type:        2.0 Dll
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      Microsoft Corporation
    ProductName:      Microsoft® Windows® Operating System
    InternalName:     fwpkclnt.sys
    OriginalFilename: fwpkclnt.sys
    ProductVersion:   6.0.6000.16386
    FileVersion:      6.0.6000.16386 (vista_rtm.061101-2205)
    FileDescription:  FWP/IPsec Kernel-Mode API
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
fffff980`04ac8000 fffff980`04c00000   tcpip      (deferred)
    Image path: \SystemRoot\System32\drivers\tcpip.sys
    Image name: tcpip.sys
    Timestamp:        Fri Sep 28 04:17:45 2007 (46FC7259)
    CheckSum:         00125C82
    ImageSize:        00138000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`04c10000 fffff980`04c10d80   DLADResE   (deferred)
    Image path: \SystemRoot\System32\DLA\DLADResE.SYS
    Image name: DLADResE.SYS
    Timestamp:        Fri Aug 18 21:16:46 2006 (44E6202E)
    CheckSum:         0000C6A1
    ImageSize:        00000D80
    File version:     9.1.5.0
    Product version:  1.0.0.1
    File flags:       0 (Mask 3F)
    File OS:          4 Unknown Win32
    File type:        2.0 Dll
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      Roxio
    FileVersion:      9.01.05a
    FileDescription:  Drive Letter Access Component
    LegalCopyright:   Copyright © 2006 Roxio
fffff980`04c39000 fffff980`04c45000   dump_dumpata   (deferred)
    Image path: \SystemRoot\System32\Drivers\dump_dumpata.sys
    Image name: dump_dumpata.sys
    Timestamp:        Thu Nov 02 09:38:11 2006 (4549BC83)
    CheckSum:         0000E7BD
    ImageSize:        0000C000
    File version:     6.0.6000.16386
    Product version:  6.0.6000.16386
    File flags:       0 (Mask 3F)
    File OS:          40004 NT Win32
    File type:        3.7 Driver
    File date:        00000000.00000000
    Translations:     0000.04b0
    CompanyName:      Microsoft Corporation
    ProductName:      Microsoft® Windows® Operating System
    InternalName:     dumpata.sys
    OriginalFilename: dumpata.sys
    ProductVersion:   6.0.6000.16386
    FileVersion:      6.0.6000.16386 (vista_rtm.061101-2205)
    FileDescription:  ATAPI Dump Driver
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
fffff980`04c45000 fffff980`04c62000   dfsc       (deferred)
```

```
    Image path: \SystemRoot\System32\Drivers\dfsc.sys
    Image name: dfsc.sys
    Timestamp:        Thu Nov 02 09:01:23 2006 (4549B3E3)
    CheckSum:         0001DF3C
    ImageSize:        0001D000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`04c62000 fffff980`04cce000   csc        (pdb symbols)
c:\mss\csc.pdb\3982C8BDECEC4CAF8C51E7C0DE15FA681\csc.pdb
    Loaded symbol image file: csc.sys
    Image path: \SystemRoot\system32\drivers\csc.sys
    Image name: csc.sys
    Timestamp:        Thu Nov 02 09:02:05 2006 (4549B40D)
    CheckSum:         00072441
    ImageSize:        0006C000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`04cce000 fffff980`04cff000   SYMEVENT64x86   (export symbols)       SYMEVENT64x86.SYS
    Loaded symbol image file: SYMEVENT64x86.SYS
    Image path: \??\C:\Windows\system32\Drivers\SYMEVENT64x86.SYS
    Image name: SYMEVENT64x86.SYS
    Timestamp:        Wed Oct 18 05:14:17 2006 (4535AA19)
    CheckSum:         000304C7
    ImageSize:        00031000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`04cff000 fffff980`04d24000   EraserUtilRebootDrv   (deferred)
    Image path: \??\C:\Program Files (x86)\Common Files\Symantec
Shared\EENGINE\EraserUtilRebootDrv.sys
    Image name: EraserUtilRebootDrv.sys
    Timestamp:        Fri Jan 18 02:44:19 2008 (47901283)
    CheckSum:         000288E3
    ImageSize:        00025000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`04d24000 fffff980`04d9d000   eeCtrl64   (no symbols)
    Loaded symbol image file: eeCtrl64.sys
    Image path: \??\C:\Program Files (x86)\Common Files\Symantec Shared\EENGINE\eeCtrl64.sys
    Image name: eeCtrl64.sys
    Timestamp:        Fri Jan 18 02:44:19 2008 (47901283)
    CheckSum:         0007E2A5
    ImageSize:        00079000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`04d9d000 fffff980`04dea000   rdbss      (pdb symbols)
c:\mss\rdbss.pdb\8D5A79655CAC4ACF84B13A616AEEAB082\rdbss.pdb
    Loaded symbol image file: rdbss.sys
    Image path: \SystemRoot\system32\DRIVERS\rdbss.sys
    Image name: rdbss.sys
    Timestamp:        Thu Nov 02 09:01:51 2006 (4549B3FF)
    CheckSum:         0004D329
    ImageSize:        0004D000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`04dea000 fffff980`04e00000   wanarp     (deferred)
    Image path: \SystemRoot\system32\DRIVERS\wanarp.sys
    Image name: wanarp.sys
    Timestamp:        Thu Nov 02 09:47:34 2006 (4549BEB6)
    CheckSum:         00015101
    ImageSize:        00016000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`04e16000 fffff980`04e29000   monitor    (deferred)
    Image path: \SystemRoot\system32\DRIVERS\monitor.sys
    Image name: monitor.sys
    Timestamp:        Thu Nov 02 09:42:06 2006 (4549BD6E)
    CheckSum:         0000C155
    ImageSize:        00013000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`04e7c000 fffff980`04eb0000   fastfat    (deferred)
    Image path: \SystemRoot\System32\Drivers\fastfat.SYS
    Image name: fastfat.SYS
    Timestamp:        Thu Nov 02 09:00:54 2006 (4549B3C6)
    CheckSum:         00039AC0
    ImageSize:        00034000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`06414000 fffff980`06431000   pacer      (deferred)
```

```
    Image path: \SystemRoot\system32\DRIVERS\pacer.sys
    Image name: pacer.sys
    Timestamp:        Thu Nov 02 09:46:53 2006 (4549BE8D)
    CheckSum:         0001C97E
    ImageSize:        0001D000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`06431000 fffff980`06470000   netbt      (pdb symbols)
c:\mss\netbt.pdb\6BEEAA1CFC7849F1B744E41A9D0F0D0A1\netbt.pdb
    Loaded symbol image file: netbt.sys
    Image path: \SystemRoot\System32\DRIVERS\netbt.sys
    Image name: netbt.sys
    Timestamp:        Thu Nov 02 09:46:24 2006 (4549BE70)
    CheckSum:         0003D412
    ImageSize:        0003F000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`06470000 fffff980`0647e000   crashdmp   (deferred)
    Image path: \SystemRoot\System32\Drivers\crashdmp.sys
    Image name: crashdmp.sys
    Timestamp:        Thu Nov 02 09:38:17 2006 (4549BC89)
    CheckSum:         0000D338
    ImageSize:        0000E000
    File version:     6.0.6000.16386
    Product version:  6.0.6000.16386
    File flags:       0 (Mask 3F)
    File OS:          40004 NT Win32
    File type:        3.7 Driver
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      Microsoft Corporation
    ProductName:      Microsoft® Windows® Operating System
    InternalName:     crashdmp.sys
    OriginalFilename: crashdmp.sys
    ProductVersion:   6.0.6000.16386
    FileVersion:      6.0.6000.16386 (vista_rtm.061101-2205)
    FileDescription:  Crash Dump Driver
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
fffff980`0649a000 fffff980`064a7d80   DRVEDDM    (export symbols)       DRVEDDM.SYS
    Loaded symbol image file: DRVEDDM.SYS
    Image path: \SystemRoot\System32\Drivers\DRVEDDM.SYS
    Image name: DRVEDDM.SYS
    Timestamp:        Fri Aug 11 19:05:44 2006 (44DCC6F8)
    CheckSum:         0000FF44
    ImageSize:        0000DD80
    File version:     3.0.0.0
    Product version:  1.0.0.1
    File flags:       0 (Mask 3F)
    File OS:          4 Unknown Win32
    File type:        2.0 Dll
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      Roxio
    FileVersion:      9.01.01a
    FileDescription:  Device Driver Manager
    LegalCopyright:   Copyright © Roxio
fffff980`06542000 fffff980`06550000   tcpipreg   (deferred)
    Image path: \SystemRoot\System32\drivers\tcpipreg.sys
    Image name: tcpipreg.sys
    Timestamp:        Thu Nov 02 09:47:05 2006 (4549BE99)
    CheckSum:         0000B25E
    ImageSize:        0000E000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`0655b000 fffff980`06566000   Msfs       (pdb symbols)
c:\mss\msfs.pdb\CCB8B994CB8040B18F03E690DE2E55721\msfs.pdb
    Loaded symbol image file: Msfs.SYS
    Image path: \SystemRoot\System32\Drivers\Msfs.SYS
    Image name: Msfs.SYS
    Timestamp:        Thu Nov 02 09:01:08 2006 (4549B3D4)
    CheckSum:         0001216C
    ImageSize:        0000B000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
```

```
fffff980`0659d000 fffff980`065a8000   asyncmac   (deferred)
    Image path: \SystemRoot\system32\DRIVERS\asyncmac.sys
    Image name: asyncmac.sys
    Timestamp:        Thu Nov 02 09:47:31 2006 (4549BEB3)
    CheckSum:         000141C6
    ImageSize:        0000B000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`065f5000 fffff980`06600000   secdrv     (deferred)
    Image path: \SystemRoot\System32\Drivers\secdrv.SYS
    Image name: secdrv.SYS
    Timestamp:        Wed Sep 13 14:18:38 2006 (4508052E)
    CheckSum:         00010B40
    ImageSize:        0000B000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`0b620000 fffff980`0b63fc00   DLAUDFAE   (deferred)
    Image path: \SystemRoot\System32\DLA\DLAUDFAE.SYS
    Image name: DLAUDFAE.SYS
    Timestamp:        Fri Aug 18 21:15:38 2006 (44E61FEA)
    CheckSum:         000280F5
    ImageSize:        0001FC00
    File version:     9.1.5.0
    Product version:  1.0.0.1
    File flags:       0 (Mask 3F)
    File OS:          4 Unknown Win32
    File type:        2.0 Dll
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      Roxio
    FileVersion:      9.01.05a
    FileDescription:  Drive Letter Access Component
    LegalCopyright:   Copyright © 2006 Roxio
fffff980`0ba1d000 fffff980`0ba3dd80   DLAIFS_E   (export symbols)       DLAIFS_E.SYS
    Loaded symbol image file: DLAIFS_E.SYS
    Image path: \SystemRoot\System32\DLA\DLAIFS_E.SYS
    Image name: DLAIFS_E.SYS
    Timestamp:        Fri Aug 18 21:14:40 2006 (44E61FB0)
    CheckSum:         00030257
    ImageSize:        00020D80
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`0ba3e000 fffff980`0ba60000   luafv      (pdb symbols)
c:\mss\luafv.pdb\579CB5DA0BCE466C86ED5DB73A4E7BC11\luafv.pdb
    Loaded symbol image file: luafv.sys
    Image path: \SystemRoot\system32\drivers\luafv.sys
    Image name: luafv.sys
    Timestamp:        Thu Nov 02 09:05:17 2006 (4549B4CD)
    CheckSum:         0001F862
    ImageSize:        00022000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`0ba98000 fffff980`0ba9e880   DLAOPIOE   (deferred)
    Image path: \SystemRoot\System32\DLA\DLAOPIOE.SYS
    Image name: DLAOPIOE.SYS
    Timestamp:        Fri Aug 18 21:16:17 2006 (44E62011)
    CheckSum:         0000D340
    ImageSize:        00006880
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`0c21b000 fffff980`0c23c400   DLAUDF_E   (deferred)
    Image path: \SystemRoot\System32\DLA\DLAUDF_E.SYS
    Image name: DLAUDF_E.SYS
    Timestamp:        Fri Aug 18 21:15:22 2006 (44E61FDA)
    CheckSum:         0002DDA2
    ImageSize:        00021400
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`0d001000 fffff980`0d019000   mrxsmb20   (deferred)
    Image path: \SystemRoot\system32\DRIVERS\mrxsmb20.sys
    Image name: mrxsmb20.sys
    Timestamp:        Fri Oct 26 02:59:25 2007 (472149FD)
    CheckSum:         000189B8
    ImageSize:        00018000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`0d034000 fffff980`0d04c000   rspndr     (deferred)
```

```
    Image path: \SystemRoot\system32\DRIVERS\rspndr.sys
    Image name: rspndr.sys
    Timestamp:        Thu Nov 02 09:45:52 2006 (4549BE50)
    CheckSum:         00015E43
    ImageSize:        00018000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`0d04c000 fffff980`0d060000   lltdio     (deferred)
    Image path: \SystemRoot\system32\DRIVERS\lltdio.sys
    Image name: lltdio.sys
    Timestamp:        Thu Nov 02 09:45:51 2006 (4549BE4F)
    CheckSum:         0000ED81
    ImageSize:        00014000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`0da05000 fffff980`0da1f000   mpsdrv     (pdb symbols)
c:\mss\mpsdrv.pdb\414BB976A0F44771B37BFACC4A6429831\mpsdrv.pdb
    Loaded symbol image file: mpsdrv.sys
    Image path: \SystemRoot\System32\drivers\mpsdrv.sys
    Image name: mpsdrv.sys
    Timestamp:        Thu Jun 07 03:44:52 2007 (46677124)
    CheckSum:         0001F51E
    ImageSize:        0001A000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`0da1f000 fffff980`0da3d000   bowser     (pdb symbols)
c:\mss\bowser.pdb\A7D097ED186543B0AC41D98F0AAAF0B01\bowser.pdb
    Loaded symbol image file: bowser.sys
    Image path: \SystemRoot\system32\DRIVERS\bowser.sys
    Image name: bowser.sys
    Timestamp:        Thu Nov 02 09:01:30 2006 (4549B3EA)
    CheckSum:         0001DD85
    ImageSize:        0001E000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`0da3d000 fffff980`0da60000   srvnet     (deferred)
    Image path: \SystemRoot\System32\DRIVERS\srvnet.sys
    Image name: srvnet.sys
    Timestamp:        Fri Oct 26 03:01:18 2007 (47214A6E)
    CheckSum:         0002C7AF
    ImageSize:        00023000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`0e378000 fffff980`0e400000   spsys      (export symbols)       spsys.sys
    Loaded symbol image file: spsys.sys
    Image path: \SystemRoot\system32\drivers\spsys.sys
    Image name: spsys.sys
    Timestamp:        Thu Oct 26 00:13:33 2006 (453FEF9D)
    CheckSum:         0008ED91
    ImageSize:        00088000
    File version:     6.0.5840.16389
    Product version:  6.0.5840.16389
    File flags:       8 (Mask 3F) Private
    File OS:          40004 NT Win32
    File type:        3.0 Driver
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      Microsoft Corporation
    ProductName:      Microsoft® Windows® Operating System
    InternalName:     spsys.sys
    OriginalFilename: spsys.sys
    ProductVersion:   6.0.5840.16389
    FileVersion:      6.0.5840.16389 (VISTA_RTM(sepbld-s).061025-1429)
    FileDescription:  security processor
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
fffff980`0e412000 fffff980`0e43a000   mrxsmb     (deferred)
    Image path: \SystemRoot\system32\DRIVERS\mrxsmb.sys
    Image name: mrxsmb.sys
    Timestamp:        Fri Oct 26 03:00:50 2007 (47214A52)
    CheckSum:         00021564
    ImageSize:        00028000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`0e43a000 fffff980`0e460000   mrxdav     (pdb symbols)
c:\mss\mrxdav.pdb\B41023BDD4F340E1AFC28F40A9AC309D1\mrxdav.pdb
    Loaded symbol image file: mrxdav.sys
```

```
    Image path: \SystemRoot\system32\drivers\mrxdav.sys
    Image name: mrxdav.sys
    Timestamp:        Thu Nov 02 09:01:48 2006 (4549B3FC)
    CheckSum:         0002EDA4
    ImageSize:        00026000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`0e65d000 fffff980`0e68b000   srv2       (pdb symbols)
c:\mss\srv2.pdb\02DDDE094A6B462C8DC6090F2B43EB381\srv2.pdb
    Loaded symbol image file: srv2.sys
    Image path: \SystemRoot\System32\DRIVERS\srv2.sys
    Image name: srv2.sys
    Timestamp:        Fri Oct 26 03:01:14 2007 (47214A6A)
    CheckSum:         00029590
    ImageSize:        0002E000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`0e6ad000 fffff980`0e6f6000   mrxsmb10   (deferred)
    Image path: \SystemRoot\system32\DRIVERS\mrxsmb10.sys
    Image name: mrxsmb10.sys
    Timestamp:        Thu Nov 02 09:01:44 2006 (4549B3F8)
    CheckSum:         0004B7C7
    ImageSize:        00049000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`0e766000 fffff980`0e800000   HTTP       (pdb symbols)
c:\mss\http.pdb\09D9A267AF8D41E8B323F4495982C9612\http.pdb
    Loaded symbol image file: HTTP.sys
    Image path: \SystemRoot\system32\drivers\HTTP.sys
    Image name: HTTP.sys
    Timestamp:        Thu Nov 02 09:46:18 2006 (4549BE6A)
    CheckSum:         00093F7B
    ImageSize:        0009A000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`0eafc000 fffff980`0eb90000   srv        (pdb symbols)
c:\mss\srv.pdb\93029554063744268F298E16FBC5FDDF2\srv.pdb
    Loaded symbol image file: srv.sys
    Image path: \SystemRoot\System32\DRIVERS\srv.sys
    Image name: srv.sys
    Timestamp:        Thu Nov 02 09:02:50 2006 (4549B43A)
    CheckSum:         0006F928
    ImageSize:        00094000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`0f2da000 fffff980`0f390000   peauth     (deferred)
    Image path: \SystemRoot\system32\drivers\peauth.sys
    Image name: peauth.sys
    Timestamp:        Mon Oct 23 12:57:00 2006 (453CAE0C)
    CheckSum:         000AE0B2
    ImageSize:        000B6000
    File version:     6.0.5840.16385
    Product version:  6.0.5840.16385
    File flags:       0 (Mask 3F)
    File OS:          40004 NT Win32
    File type:        3.7 Driver
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      Microsoft Corporation
    ProductName:      Microsoft® Windows® Operating System
    InternalName:     PEAuth.sys
    OriginalFilename: PEAuth.sys
    ProductVersion:   6.0.5840.16385
    FileVersion:      6.0.5840.16385 (VISTA_RTM_CLIENT_akaDMD.061022-1800)
    FileDescription:  Protected Environment Authentication and Authorization Export Driver
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
fffff980`10213000 fffff980`10230000   cdfs       (deferred)
    Image path: \SystemRoot\system32\DRIVERS\cdfs.sys
    Image name: cdfs.sys
    Timestamp:        Thu Nov 02 09:00:53 2006 (4549B3C5)
    CheckSum:         0001F626
    ImageSize:        0001D000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
fffff980`1da71000 fffff980`1da78000   SystemDump64   (no symbols)
    Loaded symbol image file: SystemDump64.sys
```

```
    Image path: \??\C:\dmitri\CtxBSOD\x64\release\SystemDump64.sys
    Image name: SystemDump64.sys
    Timestamp:        Mon Sep 11 17:41:08 2006 (450591A4)
    CheckSum:         0000944A
    ImageSize:        00007000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0

Unloaded modules:
fffff980`0440d000 fffff980`0442f000   ENG64.SYS
    Timestamp: unavailable (00000000)
    Checksum:  00000000
fffff980`048a3000 fffff980`04a00000   EX64.SYS
    Timestamp: unavailable (00000000)
    Checksum:  00000000
fffff980`03059000 fffff980`03062000   drmkaud.sys
    Timestamp: unavailable (00000000)
    Checksum:  00000000
fffff980`0440d000 fffff980`0442f000   ENG64.SYS
    Timestamp: unavailable (00000000)
    Checksum:  00000000
fffff980`048a3000 fffff980`04a00000   EX64.SYS
    Timestamp: unavailable (00000000)
    Checksum:  00000000
fffff980`0440d000 fffff980`0442f000   ENG64.SYS
    Timestamp: unavailable (00000000)
    Checksum:  00000000
fffff980`048a3000 fffff980`04a00000   EX64.SYS
    Timestamp: unavailable (00000000)
    Checksum:  00000000
fffff980`02e22000 fffff980`02e30000   crashdmp.sys
    Timestamp: unavailable (00000000)
    Checksum:  00000000
fffff980`02e16000 fffff980`02e22000   dump_ataport.sys
    Timestamp: unavailable (00000000)
    Checksum:  00000000
fffff980`02fc8000 fffff980`02fd0000   dump_atapi.sys
    Timestamp: unavailable (00000000)
    Checksum:  00000000
```

IRP Distribution

```
1: kd> !irpfind

Scanning large pool allocation table for Tag: Irp? (fffffa8002bdb000 : fffffa8002d5b000)



Searching NonPaged pool (fffffa80017fc000 : ffffffe000000000) for Tag: Irp?


  Irp    [ Thread ] irpStack: (Mj,Mn)   DevObj  [Driver]         MDL Process
fffffa8001840010 [00000000] Irp is complete (CurrentLocation 21 > StackCount 20)
fffffa8001840990 [00000000] Irp is complete (CurrentLocation 21 > StackCount 20)
fffffa80018b6990 [00000000] Irp is complete (CurrentLocation 21 > StackCount 20)
fffffa80018bd250 [fffffa80048b9060] irpStack: ( d, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa80018cb460 [fffffa8003f6fb30] irpStack: ( e, 0)  fffffa8001cb6650 [ \Driver\MountMgr]
fffffa8001c8ec60 [00000000] irpStack: (16, 0)  fffffa8003d9c060 [ \Driver\usbhub]
fffffa8001c92010 [00000000] irpStack: ( e, 0)  fffffa8001c90a40 [ \Driver\ACPI]
fffffa8001c92c60 [00000000] irpStack: ( e, 0)  fffffa8001cbaa10 [ \Driver\ACPI]
fffffa8001cadc60 [00000000] irpStack: ( f, 0)  00000000 [00000000: Could not read device object or
_DEVICE_OBJECT not found
]
fffffa8001cbb320 [fffffa800188bbb0] Irp is complete (CurrentLocation 7 > StackCount 6)
0x0000000000000000
fffffa8001cca010 [00000000] Irp is complete (CurrentLocation 7 > StackCount 6) 0x0000000000000000
fffffa8001e1b650 [fffffa8002138ac0] irpStack: ( e,20)  fffffa8003f75300 [ \Driver\AFD]
0xfffffa8003e0cb50
fffffa8001eede10 [fffffa8001ee3bb0] irpStack: ( e,20)  fffffa8003f75300 [ \Driver\AFD]
0xfffffa800499dc10
fffffa8001f08e10 [fffffa8004398060] irpStack: ( e,20)  fffffa8003f75300 [ \Driver\AFD]
0xfffffa80041a2b50
fffffa8001f395d0 [fffffa8004398060] irpStack: ( e,20)  fffffa8003f75300 [ \Driver\AFD]
0xfffffa80041a2b50
fffffa8001f4b580 [fffffa8001f4b060] irpStack: ( d, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa8001f93580 [fffffa8001f93700] irpStack: ( 3, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa8002045010 [fffffa8001fe13a0] irpStack: ( e, 0)  fffffa80039ca290 [ \Driver\NdisTapi]
fffffa80020538f0 [fffffa80041fb060] irpStack: ( d, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa800208fee0 [fffffa8001e67bb0] irpStack: ( e, 0)  fffffa8003bcfdf0 [ \Driver\NDProxy]
fffffa80020a3860 [fffffa800200e840] irpStack: ( e, 0)  fffffa8003bd1cd0 [ \Driver\NdisWan]
fffffa80020a3ac0 [fffffa800200e840] irpStack: ( e, 0)  fffffa8003bd1cd0 [ \Driver\NdisWan]
fffffa80020beca0 [fffffa8004c075d0] irpStack: ( c, 2)  fffffa8002990030 [ \FileSystem\Ntfs]
fffffa8002186710 [fffffa8002424bb0] irpStack: ( e,2d)  fffffa8003f75300 [ \Driver\AFD]
fffffa800218a420 [fffffa800249dbb0] irpStack: ( e, 9)  fffffa8003f75300 [ \Driver\AFD]
fffffa80021c4580 [fffffa80020473a0] irpStack: ( d, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa800220d370 [fffffa8004c075d0] irpStack: ( c, 2)  fffffa8002990030 [ \FileSystem\Ntfs]
fffffa8002216c60 [fffffa800431e060] irpStack: ( 3, 0)  fffffa8003d989c0 [ \Driver\mouclass]
fffffa800222cca0 [fffffa8004808060] irpStack: ( c, 2)  fffffa8002990030 [ \FileSystem\Ntfs]
fffffa8002596510 [00000000] irpStack: ( f, 0)  fffffa80039fd050 [ \Driver\usbuhci]
fffffa8002597010 [00000000] irpStack: ( f, 0)  fffffa8003a55050 [ \Driver\usbehci]
fffffa800259d820 [fffffa8004c075d0] irpStack: ( c, 2)  fffffa8002990030 [ \FileSystem\Ntfs]
fffffa80025d38c0 [fffffa80043dabb0] irpStack: ( d, 0)  fffffa8002990030 [ \FileSystem\Ntfs]
0x0000000000000000
fffffa80025fd010 [fffffa8002424bb0] irpStack: ( e,2d)  fffffa8003f75300 [ \Driver\AFD]
fffffa800260d820 [fffffa80042b0bb0] irpStack: ( 3, 0)  fffffa8003d5bd00 [ \Driver\kbdclass]
fffffa800262a010 [00000000] irpStack: (16, 0)  fffffa8001cbaa10 [ \Driver\ACPI]
fffffa800262b010 [fffffa800188d720] irpStack: ( e, 0)  fffffa80028912d0 [ \Driver\volmgr]
fffffa80026567e0 [fffffa8004073060] irpStack: ( d, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa80027f7ca0 [fffffa800436e340] irpStack: ( c, 2)  fffffa8002990030 [ \FileSystem\Ntfs]
fffffa8002849010 [fffffa800456d700] irpStack: ( e, 0)  fffffa8003fe9c40 [ \Driver\Smb]
0xfffffa80044ff040
fffffa80028492c0 [fffffa8002af7bb0] irpStack: ( e,2d)  fffffa8003f75300 [ \Driver\AFD]
fffffa80028929e0 [00000000] irpStack: ( f, 0)  fffffa8003a85050 [ \Driver\usbuhci]
fffffa80029034c0 [fffffa8004c075d0] irpStack: ( c, 2)  fffffa8002990030 [ \FileSystem\Ntfs]
fffffa8002904ca0 [fffffa8004c075d0] irpStack: ( c, 2)  fffffa8002990030 [ \FileSystem\Ntfs]
fffffa8002947c70 [fffffa8003eed060] irpStack: ( e, 0)  fffffa8004658080 [ \Driver\mpsdrv]
fffffa800296c120 [fffffa800477c740] irpStack: ( 3, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
```

```
fffffa800296ec60 [00000000] Irp is complete (CurrentLocation 7 > StackCount 6) 0x0000000000000000
fffffa80029738b0 [fffffa80041b4040] Irp is complete (CurrentLocation 7 > StackCount 6)
0x0000000000000000
fffffa8002974010 [00000000] irpStack: ( f, 0)  fffffa8003a85050 [ \Driver\usbuhci]
fffffa8002981180 [00000000] irpStack: (16, 0)  fffffa8003d99b90 [ \Driver\HidUsb]
fffffa8002995010 [00000000] irpStack: ( 3, 0)  fffffa8003d5b250 [ \Driver\HidUsb]
0x0000000000000000
fffffa800299a350 [00000000] irpStack: ( f, 0)  fffffa80039f0050 [ \Driver\usbuhci]
fffffa8002a06430 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x0000000000000000
fffffa8002a62010 [fffffa8004c075d0] irpStack: ( c, 2)  fffffa8002990030 [ \FileSystem\Ntfs]
fffffa8002a6c1c0 [fffffa8004c075d0] irpStack: ( c, 2)  fffffa8002990030 [ \FileSystem\Ntfs]
fffffa8002ac3520 [fffffa80049a8bb0] irpStack: ( d, 0)  fffffa8002990030 [ \FileSystem\Ntfs]
0xfffffa8004812870
fffffa8002ad6ca0 [fffffa8004c075d0] irpStack: ( c, 2)  fffffa8002990030 [ \FileSystem\Ntfs]
fffffa8002b47cc0 [fffffa8002af7bb0] irpStack: ( e,2d)  fffffa8003f75300 [ \Driver\AFD]
fffffa80038ac010 [00000000] irpStack: (16, 0)  fffffa8003d4e060 [ \Driver\usbhub]
fffffa80038aeee0 [fffffa800439c060] irpStack: ( d, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa80038b0010 [fffffa800436e340] irpStack: ( d, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa80038b0e00 [fffffa800435f930] irpStack: ( d, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa80038e7010 [00000000] irpStack: ( f, 0)  fffffa80039fd050 [ \Driver\usbuhci]
fffffa80039a7ca0 [fffffa8004c075d0] irpStack: ( c, 2)  fffffa8002990030 [ \FileSystem\Ntfs]
fffffa80039ab4e0 [fffffa8004c075d0] irpStack: ( c, 2)  fffffa8002990030 [ \FileSystem\Ntfs]
fffffa80039de5e0 [fffffa8002045bb0] irpStack: ( 3, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa80039e8510 [00000000] irpStack: ( 0, 0)  00000000 [00000000: Could not read device object or
_DEVICE_OBJECT not found
] 0x0000000000000000
fffffa8003b63010 [00000000] irpStack: ( 3, 0)  fffffa8003d99b90 [ \Driver\HidUsb]
0x0000000000000000
fffffa8003b6ac60 [00000000] irpStack: ( 0, 0)  fffffa8003a0c750 [ \Driver\cdrom] 0x0000000000000000
fffffa8003b6bc60 [00000000] irpStack: ( 0, 0)  00000000 [00000000: Could not read device object or
_DEVICE_OBJECT not found
] 0x0000000000000000
fffffa8003d448b0 [00000000] irpStack: (16, 0)  fffffa8003d5b250 [ \Driver\HidUsb]
fffffa8003d44c60 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2)
fffffa8003d5f680 [00000000] irpStack: ( f, 0)  fffffa80039f0050 [ \Driver\usbuhci]
fffffa8003d60010 [00000000] irpStack: ( f, 0)  fffffa8003a85050 [ \Driver\usbuhci]
fffffa8003d606f0 [00000000] irpStack: ( f, 0)  fffffa8003a85050 [ \Driver\usbuhci]
fffffa8003d7f780 [fffffa80044df060] irpStack: ( 3, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa8003d96010 [00000000] irpStack: ( f, 0)  fffffa8003a83050 [ \Driver\usbehci]
fffffa8003e05010 [00000000] irpStack: ( f, 0)  fffffa8003a55050 [ \Driver\usbehci]
fffffa8003e05c60 [00000000] irpStack: ( f, 0)  fffffa80039ee050 [ \Driver\usbuhci]
fffffa8003f17010 [00000000] irpStack: ( f, 0)  fffffa8003a85050 [ \Driver\usbuhci]
fffffa8003faec60 [fffffa800431e060] irpStack: ( 3, 0)  fffffa8003a04a90 [ \Driver\mouclass]
fffffa8003fcec60 [fffffa80045a45b0] irpStack: ( 3, 0)  fffffa8003e04790 [ \FileSystem\Msfs]
fffffa8003fecee0 [fffffa8003eed060] irpStack: ( e, 0)  fffffa8004658080 [ \Driver\mpsdrv]
fffffa8004065c60 [fffffa8004429060] irpStack: ( e,2d)  fffffa8003f75300 [ \Driver\AFD]
fffffa80041a68f0 [fffffa8004480bb0] irpStack: ( 3, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa80041bb010 [fffffa80041b4040] Irp is complete (CurrentLocation 7 > StackCount 6)
0x0000000000000000
fffffa80041c75d0 [fffffa80042b0bb0] irpStack: ( 3, 0)  fffffa80039c7660 [ \Driver\kbdclass]
fffffa80041ebac0 [fffffa8004073060] irpStack: ( e,20)  fffffa8003f75300 [ \Driver\AFD]
0xfffffa8003f56ad0
fffffa8004208a60 [fffffa8001e12bb0] irpStack: ( d, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa8004233830 [fffffa80043571f0] irpStack: ( e,2d)  fffffa8003f75300 [ \Driver\AFD]
fffffa80042955c0 [fffffa8004486460] irpStack: ( e,20)  fffffa8003f75300 [ \Driver\AFD]
0xfffffa80044ff040
fffffa80042978b0 [fffffa8004073060] irpStack: ( e,20)  fffffa8003f75300 [ \Driver\AFD]
0xfffffa8003f56ad0
fffffa80042d2c70 [fffffa800437a6b0] irpStack: ( e, 0)  fffffa8003f1f540 [ \Driver\nsiproxy]
fffffa80042fd5c0 [fffffa8004880060] irpStack: ( 3, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa8004308010 [fffffa80043e6060] irpStack: ( e,20)  fffffa8003f75300 [ \Driver\AFD]
0xfffffa80042d1c10
fffffa8004363010 [fffffa8004490060] irpStack: ( 3, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa80043678f0 [fffffa80044a44e0] irpStack: ( d, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa8004387ad0 [fffffa800439c060] irpStack: ( d, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa80043932c0 [fffffa800436e340] irpStack: ( 3, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa800439a280 [fffffa80043a6570] irpStack: ( d, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa800439aaa0 [fffffa8002963060] irpStack: ( 3, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa800439fee0 [fffffa80043e6060] irpStack: ( d, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa80043a2470 [fffffa80043a2bb0] irpStack: ( 3, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
```

```
fffffa80043c44f0 [fffffa80043e2060] irpStack: ( 3, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa80043c4cd0 [fffffa80043e4ad0] irpStack: ( d, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa80043d7ca0 [fffffa80044d28c0] irpStack: ( c, 2)  fffffa8002990030 [ \FileSystem\Ntfs]
fffffa80043dd4f0 [fffffa800480f470] irpStack: ( 3, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa80043eaee0 [fffffa80048a1bb0] irpStack: ( 3, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa80043ebdb0 [fffffa800202ea60] irpStack: ( 3, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa80043ed3f0 [fffffa8004486460] irpStack: ( e,20)  fffffa8003f75300 [ \Driver\AFD]
0xfffffa80044ff040
fffffa800442cc80 [fffffa80042d1780] irpStack: ( d, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa8004480360 [fffffa8003eed060] irpStack: ( e, 0)  fffffa8004658080 [ \Driver\mpsdrv]
fffffa8004487980 [fffffa80045c0bb0] irpStack: ( e, 0)  fffffa8003f36320 [ \Driver\netbt]
0xfffffa80044ff040
fffffa8004490c40 [fffffa80045adbb0] irpStack: ( d, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa80044a2ee0 [fffffa8004486460] irpStack: ( d, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa80044bd2c0 [fffffa80042d8bb0] irpStack: ( 3, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa80044be010 [fffffa8004a2f780] irpStack: ( 3, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa80044c5a10 [fffffa8004570060] irpStack: ( c, 2)  fffffa8002990030 [ \FileSystem\Ntfs]
fffffa80044c5dc0 [fffffa800436e340] irpStack: ( 3, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa80044d8e00 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
fffffa80044f20f0 [fffffa80042d4710] irpStack: ( 3, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa80044f7720 [fffffa800457c060] irpStack: ( 3, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa80044ff750 [fffffa8004489430] irpStack: ( d, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa8004500d10 [fffffa8004b3a060] irpStack: ( 3, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa8004573320 [fffffa8002935060] irpStack: ( d, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa8004576110 [fffffa800448abb0] irpStack: ( d, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa8004577820 [fffffa80045be250] irpStack: ( d, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa80045810d0 [fffffa8004242260] irpStack: ( 3, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa800458a1e0 [fffffa800456ebb0] irpStack: ( e, 0)  fffffa8003f36320 [ \Driver\netbt]
0xfffffa80044ff040
fffffa800458a840 [fffffa800456dbb0] irpStack: ( e, 0)  fffffa8003fe9c40 [ \Driver\Smb]
0xfffffa80044ff040
fffffa8004593440 [fffffa8004554bb0] irpStack: ( e,20)  fffffa8003f75300 [ \Driver\AFD]
0xfffffa80045c38c0
fffffa800459f790 [fffffa8004554bb0] irpStack: ( e,20)  fffffa8003f75300 [ \Driver\AFD]
0xfffffa80045c38c0
fffffa80045b9b50 [fffffa800452b060] irpStack: ( d, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa80045bc010 [fffffa80045f2060] irpStack: ( d, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa80045c93c0 [fffffa8004c89bb0] irpStack: ( 3, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa80045d4ee0 [fffffa8004620750] irpStack: ( 3, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa80045f6e10 [fffffa800452b060] irpStack: ( e,20)  fffffa8003f75300 [ \Driver\AFD]
0xfffffa80044d9c10
fffffa80045f7a00 [fffffa80045e7a10] irpStack: ( c, 2)  fffffa8002990030 [ \FileSystem\Ntfs]
fffffa8004602850 [fffffa8002968820] irpStack: ( 3, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa8004609010 [fffffa80045f9bb0] irpStack: ( 3, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa80046128b0 [fffffa80046a77f0] irpStack: ( c, 2)  fffffa8002990030 [ \FileSystem\Ntfs]
fffffa80046146b0 [fffffa800452b060] irpStack: ( e,20)  fffffa8003f75300 [ \Driver\AFD]
0xfffffa80044d9c10
fffffa80046235c0 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
fffffa800462aee0 [fffffa80048c5060] irpStack: ( d, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa8004685590 [fffffa800437a6b0] irpStack: ( e, 0)  fffffa8003f1f540 [ \Driver\nsiproxy]
fffffa8004687330 [fffffa8004b04b10] irpStack: ( c, 2)  fffffa8002990030 [ \FileSystem\Ntfs]
fffffa80046ae010 [fffffa800474d370] irpStack: ( d, 0)  fffffa8003f95040 [ \Driver\CSC]
fffffa80046b0b90 [fffffa8004813bb0] irpStack: ( c, 2)  fffffa8002990030 [ \FileSystem\Ntfs]
fffffa80046d7060 [fffffa800437a6b0] irpStack: ( c, 2)  fffffa8002990030 [ \FileSystem\Ntfs]
fffffa80046db930 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
fffffa80046e6bc0 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
fffffa80046e7140 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
fffffa80046e7270 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
fffffa80046f67c0 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
fffffa80046fa2d0 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
fffffa80046fa400 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
fffffa80046fa750 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
fffffa80046faaa0 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
fffffa80046ff2d0 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
fffffa80046ff620 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
fffffa80046ff970 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
fffffa80046ffcc0 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
fffffa80047004f0 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
fffffa8004700840 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
fffffa8004700b90 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
```

```
fffffa8004700ee0 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
fffffa8004701010 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
fffffa80047011a0 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
fffffa80047012d0 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
fffffa8004701620 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
fffffa8004701970 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
fffffa8004701cc0 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
fffffa80047022d0 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
fffffa8004702620 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
fffffa8004702970 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
fffffa8004702cc0 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
fffffa80047034f0 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
fffffa8004703840 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
fffffa8004703b90 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
fffffa8004703ee0 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
fffffa8004704010 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
fffffa8004704a20 [fffffa8002583bb0] irpStack: ( d, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa8004704cc0 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
fffffa8004705010 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
fffffa8004705ac0 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
fffffa8004706950 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
fffffa8004707460 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
fffffa8004707870 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
fffffa80047081e0 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
fffffa800470ac30 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
fffffa800470bac0 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
fffffa800470c010 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
fffffa800470c950 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
fffffa800470d6c0 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
fffffa800470e590 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
fffffa800470ebc0 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
fffffa800470f190 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
fffffa8004711240 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
fffffa8004711e50 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
fffffa8004712390 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
fffffa8004712e50 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
fffffa8004713e50 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
fffffa8004714010 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
fffffa8004716010 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
fffffa8004716c30 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
fffffa8004717ac0 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
fffffa8004718950 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
fffffa8004719460 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
fffffa800471b010 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
fffffa800471c010 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
fffffa800471cc30 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
fffffa800471d4c0 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
fffffa800471e220 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
fffffa8004722010 [fffffa80041b5bb0] irpStack: ( e, 0)  fffffa8004655870 [ \FileSystem\bowser]
0xfffffa8004298550
fffffa8004751700 [fffffa800474f950] irpStack: ( 3, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa8004757800 [fffffa8004a2f780] irpStack: ( c, 2)  fffffa8002990030 [ \FileSystem\Ntfs]
fffffa800475ebc0 [fffffa80046af720] irpStack: ( d, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa80047713d0 [fffffa8004771760] irpStack: ( 3, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa800477d530 [fffffa800489ebb0] irpStack: ( 3, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa8004809b20 [fffffa8004550870] irpStack: ( c, 2)  fffffa8002990030 [ \FileSystem\Ntfs]
fffffa8004811270 [fffffa8004359480] irpStack: ( d, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa8004815010 [fffffa8004550870] irpStack: ( d, 0)  fffffa8002990030 [ \FileSystem\Ntfs]
fffffa8004820b00 [fffffa80046b0060] irpStack: ( e, 0)  fffffa80045f8b20 [ \Driver\HTTP]
0xfffffa80045c38c0
fffffa8004836ee0 [fffffa8003eed060] irpStack: ( e, 0)  fffffa8004658080 [ \Driver\mpsdrv]
fffffa8004845c80 [fffffa80045b7bb0] irpStack: ( d, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa8004861ce0 [fffffa800452b060] irpStack: ( d, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa8004865e10 [fffffa80043571f0] irpStack: ( e,2d)  fffffa8003f75300 [ \Driver\AFD]
fffffa8004886010 [fffffa8002967060] irpStack: ( c, 2)  fffffa8002990030 [ \FileSystem\Ntfs]
fffffa8004893da0 [fffffa8004887700] irpStack: ( e, 0)  fffffa8003f1f540 [ \Driver\nsiproxy]
fffffa800489ddb0 [fffffa8004887700] irpStack: ( e, 0)  fffffa8003f1f540 [ \Driver\nsiproxy]
fffffa80048b0230 [fffffa8004663060] irpStack: ( e,2d)  fffffa8003f75300 [ \Driver\AFD]
fffffa80048b31f0 [fffffa8004864060] irpStack: ( e,2d)  fffffa8003f75300 [ \Driver\AFD]
fffffa80048bfe10 [fffffa8004864060] irpStack: ( e,2d)  fffffa8003f75300 [ \Driver\AFD]
```

```
fffffa800493e260 [fffffa800493e510] irpStack: ( d, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa80049a6e10 [fffffa800456f060] irpStack: ( e,2d)  fffffa8003f75300 [ \Driver\AFD]
fffffa80049a7460 [fffffa800436e340] irpStack: ( e,20)  fffffa8003f75300 [ \Driver\AFD]
0xfffffa8004298550
fffffa80049aaa10 [fffffa800436e340] irpStack: ( e,20)  fffffa8003f75300 [ \Driver\AFD]
0xfffffa8004298550
fffffa8004a2f010 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
fffffa8004a5cca0 [fffffa8004808060] irpStack: ( c, 2)  fffffa8002990030 [ \FileSystem\Ntfs]
fffffa8004ab8db0 [fffffa8001f4b060] irpStack: ( 3, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa8004ac6930 [fffffa800482b530] irpStack: ( 3, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa8004b3b610 [fffffa80045793c0] irpStack: ( 3, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa8004b45ca0 [fffffa800436e340] irpStack: ( c, 2)  fffffa8002990030 [ \FileSystem\Ntfs]
fffffa8004b71ee0 [fffffa80041a26c0] irpStack: ( d, 0)  fffffa8003dc1060 [ \FileSystem\Npfs]
fffffa8004ba8010 [fffffa8004c075d0] irpStack: ( c, 2)  fffffa8002990030 [ \FileSystem\Ntfs]
fffffa8004bdec60 [fffffa8004c075d0] irpStack: ( c, 2)  fffffa8002990030 [ \FileSystem\Ntfs]
fffffa8004c1d680 [fffffa8004c075d0] irpStack: ( c, 2)  fffffa8002990030 [ \FileSystem\Ntfs]
fffffa8004c3d150 [fffffa8004c075d0] irpStack: ( c, 2)  fffffa8002990030 [ \FileSystem\Ntfs]
fffffa8004c3d4c0 [fffffa8004c075d0] irpStack: ( c, 2)  fffffa8002990030 [ \FileSystem\Ntfs]
fffffa8004c3e2c0 [fffffa8004c075d0] irpStack: ( c, 2)  fffffa8002990030 [ \FileSystem\Ntfs]
fffffa8004c41930 [fffffa8004c075d0] irpStack: ( c, 2)  fffffa8002990030 [ \FileSystem\Ntfs]
fffffa8004c41ca0 [fffffa8004c075d0] irpStack: ( c, 2)  fffffa8002990030 [ \FileSystem\Ntfs]
fffffa8004c63010 [fffffa8004c075d0] irpStack: ( c, 2)  fffffa8002990030 [ \FileSystem\Ntfs]
fffffa8004c635c0 [fffffa8004c075d0] irpStack: ( c, 2)  fffffa8002990030 [ \FileSystem\Ntfs]
fffffa8004d2e010 [fffffa800455b060] irpStack: ( c, 2)  fffffa8002990030 [ \FileSystem\Ntfs]
fffffa8004d72010 [fffffa80047457d0] irpStack: ( c, 2)  fffffa8002990030 [ \FileSystem\Ntfs]
```