Reference Stack Traces

Windows Vista™ x86 Complete Memory Dump

Dmitry Vostokov

1/28/2008

First Edition

Table of Contents

Version

```
Windows Vista Kernel Version 6000 MP (2 procs) Free x86 compatible
Product: WinNt, suite: TerminalServer SingleUserTS Personal
Built by: 6000.16575.x86fre.vista_gdr.071009-1548
Kernel base = 0x81c00000 PsLoadedModuleList = 0x81d11e10
Debug session time: Sat Jan 26 19:18:24.739 2008 (GMT+0)
System Uptime: 0 days 0:11:18.594
```

Virtual Memory

```
0: kd> !vm

*** Virtual Memory Usage ***
       Physical Memory:      253893 (   1015572 Kb)
       Page File: \??\C:\pagefile.sys
         Current:   1322772 Kb  Free Space:   1227612 Kb
         Minimum:   1322772 Kb  Maximum:      4194304 Kb
       Available Pages:      114802 (    459208 Kb)
       ResAvail Pages:       185450 (    741800 Kb)
       Locked IO Pages:           0 (         0 Kb)
       Free System PTEs:     334133 (   1336532 Kb)
       Modified Pages:         6981 (     27924 Kb)
       Modified PF Pages:      6937 (     27748 Kb)
       NonPagedPool Usage:    10013 (     40052 Kb)
       NonPagedPool Max:     185977 (    743908 Kb)
       PagedPool 0 Usage:      7283 (     29132 Kb)
       PagedPool 1 Usage:      4841 (     19364 Kb)
       PagedPool 2 Usage:       534 (      2136 Kb)
       PagedPool 3 Usage:       549 (      2196 Kb)
       PagedPool 4 Usage:       553 (      2212 Kb)
       PagedPool Usage:       13760 (     55040 Kb)
       PagedPool Maximum:    523264 (   2093056 Kb)
       Shared Commit:          9883 (     39532 Kb)
       Special Pool:              0 (         0 Kb)
       Shared Process:         2195 (      8780 Kb)
       PagedPool Commit:      13763 (     55052 Kb)
       Driver Commit:          4362 (     17448 Kb)
       Committed pages:      173112 (    692448 Kb)
       Commit limit:         573293 (   2293172 Kb)

       Total Private:        118809 (    475236 Kb)
         0b48 dwm.exe          19248 (     76992 Kb)
         05a4 iexplore.exe     14371 (     57484 Kb)
         0ce4 sidebar.exe       8481 (     33924 Kb)
         0b90 explorer.exe      7780 (     31120 Kb)
         03bc svchost.exe       7734 (     30936 Kb)
         01e4 SearchIndexer.e   7371 (     29484 Kb)
         0350 svchost.exe       5090 (     20360 Kb)
         03cc svchost.exe       4723 (     18892 Kb)
         0600 svchost.exe       3971 (     15884 Kb)
         04c4 svchost.exe       3226 (     12904 Kb)
         03a4 svchost.exe       3119 (     12476 Kb)
         0420 audiodg.exe       3113 (     12452 Kb)
         0b14 taskeng.exe       2341 (      9364 Kb)
         0844 wmpnetwk.exe      2069 (      8276 Kb)
         078c stacsv.exe        2049 (      8196 Kb)
         0460 svchost.exe       2033 (      8132 Kb)
         0c9c KbdMgr.exe        1926 (      7704 Kb)
         05e8 spoolsv.exe       1497 (      5988 Kb)
         0440 SLsvc.exe         1360 (      5440 Kb)
         0c64 MSASCui.exe       1268 (      5072 Kb)
         0c8c sttray.exe        1068 (      4272 Kb)
         0910 ieuser.exe        1012 (      4048 Kb)
         0004 System             891 (      3564 Kb)
         0324 svchost.exe        873 (      3492 Kb)
         0220 lsass.exe          801 (      3204 Kb)
         0cfc GoogleToolbarNo    735 (      2940 Kb)
         0d40 WmiPrvSE.exe       709 (      2836 Kb)
         02ec svchost.exe        643 (      2572 Kb)
         0214 services.exe       623 (      2492 Kb)
         0734 svchost.exe        553 (      2212 Kb)
         0cf4 ehtray.exe         535 (      2140 Kb)
         0378 notepad.exe        509 (      2036 Kb)
         0294 winlogon.exe       490 (      1960 Kb)
         0228 lsm.exe            479 (      1916 Kb)
```

```
0768 svchost.exe        478 (      1912 Kb)
01f8 taskeng.exe        454 (      1816 Kb)
0cd8 realsched.exe      440 (      1760 Kb)
0de8 wmpnscfg.exe       439 (      1756 Kb)
0ddc igfxsrvc.exe       397 (      1588 Kb)
0c78 hkcmd.exe          392 (      1568 Kb)
01bc csrss.exe          389 (      1556 Kb)
01f4 csrss.exe          388 (      1552 Kb)
0ab8 FlashUtil9e.exe    339 (      1356 Kb)
0c6c igfxtray.exe       335 (      1340 Kb)
01e8 wininit.exe        328 (      1312 Kb)
0724 AppleTimeSrv.ex    288 (      1152 Kb)
0c94 IRW.exe            269 (      1076 Kb)
0ca4 jusched.exe        262 (      1048 Kb)
0c84 igfxpers.exe       260 (      1040 Kb)
0e24 ehmsas.exe         259 (      1036 Kb)
0704 AppleOSSMgr.exe    184 (       736 Kb)
000c svchost.exe        146 (       584 Kb)
0164 smss.exe            71 (       284 Kb)
0920 realplay.exe         0 (         0 Kb)
```

Processes and Threads

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

System process

```
PROCESS 82f14d90  SessionId: none  Cid: 0004    Peb: 00000000  ParentCid: 0000
    DirBase: 00122000  ObjectTable: 85a00358  HandleCount: 517.
    Image: System
    VadRoot 8484d108 Vads 327 Clone 0 Private 880. Modified 10893. Locked 64.
    DeviceMap 85a03048
    Token                             85a039b0
    ElapsedTime                       00:11:19.083
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.327
    QuotaPoolUsage[PagedPool]         0
    QuotaPoolUsage[NonPagedPool]      0
    Working Set Sizes (now,min,max)  (1471, 0, 0) (5884KB, 0KB, 0KB)
    PeakWorkingSetSize                3897
    VirtualSize                       10 Mb
    PeakVirtualSize                   16 Mb
    PageFaultCount                    15272
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      891

    Setting context for this process...
.process /p /r ffffffff82f14d90

    !peb

        THREAD 82f14ae8  Cid 0004.0008  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrFreePage)
KernelMode Non-Alertable
            81d12180  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      43383          Ticks: 116 (0:00:00:01.809)
        Context Switch Count      1992
        UserTime                  00:00:00.000
        KernelTime                00:00:01.560
        Win32 Start Address nt!Phase1Initialization (0x81d3300b)
        Stack Init 84e69000 Current 84e68c60 Base 84e69000 Limit 84e66000 Call 0
        Priority 0 BasePriority 0 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        84e68c78 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        84e68cb4 81c293a7 nt!KiSwapThread+0x389
        84e68d14 81cba246 nt!KeWaitForSingleObject+0x414
        84e68d74 81d3301d nt!MmZeroPageThread+0x123
        84e68d7c 81e254e0 nt!Phase1Initialization+0x12
        84e68dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 82f14348  Cid 0004.0010  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            81d09570  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      18             Ticks: 43481 (0:00:11:18.307)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!PopIrpWorkerControl (0x81c50688)
        Stack Init 84e3d000 Current 84e3cc98 Base 84e3d000 Limit 84e3a000 Call 0
        Priority 15 BasePriority 13 PriorityDecrement 2 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        84e3ccb0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        84e3ccec 81c293a7 nt!KiSwapThread+0x389
        84e3cd4c 81c506ad nt!KeWaitForSingleObject+0x414
        84e3cd7c 81e254e0 nt!PopIrpWorkerControl+0x25
        84e3cdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 82f38020  Cid 0004.0014  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            81d09ac0  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      10180          Ticks: 33319 (0:00:08:39.779)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!PopIrpWorker (0x81c5075b)
        Stack Init 84e39000 Current 84e38c60 Base 84e39000 Limit 84e36000 Call 0
        Priority 15 BasePriority 13 PriorityDecrement 2 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        84e38c78 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        84e38cb4 81c293a7 nt!KiSwapThread+0x389
        84e38d14 81c50884 nt!KeWaitForSingleObject+0x414
        84e38d7c 81e254e0 nt!PopIrpWorker+0x129
        84e38dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 82f38d78  Cid 0004.0018  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            81d09ac0  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      10180          Ticks: 33319 (0:00:08:39.779)
        Context Switch Count      16
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!PopIrpWorker (0x81c5075b)
        Stack Init 84e35000 Current 84e34c60 Base 84e35000 Limit 84e32000 Call 0
        Priority 15 BasePriority 13 PriorityDecrement 2 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        84e34c78 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        84e34cb4 81c293a7 nt!KiSwapThread+0x389
        84e34d14 81c50884 nt!KeWaitForSingleObject+0x414
        84e34d7c 81e254e0 nt!PopIrpWorker+0x129
        84e34dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 82f389c0  Cid 0004.001c  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            81cfde40  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      18             Ticks: 43481 (0:00:11:18.307)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!ExpWorkerThread (0x81c78ea3)
        Stack Init 84e6d000 Current 84e6cc90 Base 84e6d000 Limit 84e6a000 Call 0
        Priority 13 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        84e6cca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        84e6cce4 81cad431 nt!KiSwapThread+0x389
        84e6cd30 81c78f78 nt!KeRemoveQueueEx+0x568
        84e6cd7c 81e254e0 nt!ExpWorkerThread+0xd5
        84e6cdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 82f38718  Cid 0004.0020  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            81cfde40  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      18             Ticks: 43481 (0:00:11:18.307)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!ExpWorkerThread (0x81c78ea3)
        Stack Init 84e71000 Current 84e70c90 Base 84e71000 Limit 84e6e000 Call 0
        Priority 13 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        84e70ca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        84e70ce4 81cad431 nt!KiSwapThread+0x389
        84e70d30 81c78f78 nt!KeRemoveQueueEx+0x568
        84e70d7c 81e254e0 nt!ExpWorkerThread+0xd5
        84e70dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 82f38470  Cid 0004.0024  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            81cfde40  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      680            Ticks: 42819 (0:00:11:07.980)
        Context Switch Count      860
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!ExpWorkerThread (0x81c78ea3)
        Stack Init 859f0000 Current 859efc90 Base 859f0000 Limit 859ed000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        859efca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        859efce4 81cad431 nt!KiSwapThread+0x389
        859efd30 81c78f78 nt!KeRemoveQueueEx+0x568
        859efd7c 81e254e0 nt!ExpWorkerThread+0xd5
        859efdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 82f3a020  Cid 0004.0028  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            81cfde40  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      680            Ticks: 42819 (0:00:11:07.980)
        Context Switch Count      1456
        UserTime                  00:00:00.000
        KernelTime                00:00:00.436
        Win32 Start Address nt!ExpWorkerThread (0x81c78ea3)
        Stack Init 859ec000 Current 859ebc90 Base 859ec000 Limit 859e9000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        859ebca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        859ebce4 81cad431 nt!KiSwapThread+0x389
        859ebd30 81c78f78 nt!KeRemoveQueueEx+0x568
        859ebd7c 81e254e0 nt!ExpWorkerThread+0xd5
        859ebdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16


        THREAD 82f3ad78  Cid 0004.002c  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            81cfde40  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      658            Ticks: 42841 (0:00:11:08.323)
        Context Switch Count      159
        UserTime                  00:00:00.000
        KernelTime                00:00:00.265
        Win32 Start Address nt!ExpWorkerThread (0x81c78ea3)
        Stack Init 859e8000 Current 859e7c90 Base 859e8000 Limit 859e5000 Call 0
        Priority 13 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        859e7ca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        859e7ce4 81cad431 nt!KiSwapThread+0x389
        859e7d30 81c78f78 nt!KeRemoveQueueEx+0x568
        859e7d7c 81e254e0 nt!ExpWorkerThread+0xd5
        859e7dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 82f3aad0  Cid 0004.0030  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            81cfde7c  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      765            Ticks: 42734 (0:00:11:06.654)
        Context Switch Count      204
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!ExpWorkerThread (0x81c78ea3)
        Stack Init 859e4000 Current 859e3c90 Base 859e4000 Limit 859e1000 Call 0
        Priority 13 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        859e3ca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        859e3ce4 81cad431 nt!KiSwapThread+0x389
        859e3d30 81c78f78 nt!KeRemoveQueueEx+0x568
        859e3d7c 81e254e0 nt!ExpWorkerThread+0xd5
        859e3dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 82f3a828  Cid 0004.0034  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            81cfde7c  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      8861           Ticks: 34638 (0:00:09:00.356)
        Context Switch Count      1966
        UserTime                  00:00:00.000
        KernelTime                00:00:02.449
        Win32 Start Address nt!ExpWorkerThread (0x81c78ea3)
        Stack Init 859e0000 Current 859dfc90 Base 859e0000 Limit 859dd000 Call 0
        Priority 15 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        859dfca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        859dfce4 81cad431 nt!KiSwapThread+0x389
        859dfd30 81c78f78 nt!KeRemoveQueueEx+0x568
        859dfd7c 81e254e0 nt!ExpWorkerThread+0xd5
        859dfdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 82f3a580  Cid 0004.0038  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            81cfde7c  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      29798          Ticks: 13701 (0:00:03:33.736)
        Context Switch Count      5908
        UserTime                  00:00:00.000
        KernelTime                00:00:00.249
        Win32 Start Address nt!ExpWorkerThread (0x81c78ea3)
        Stack Init 859dc000 Current 859dbc90 Base 859dc000 Limit 859d9000 Call 0
        Priority 13 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        859dbca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        859dbce4 81cad431 nt!KiSwapThread+0x389
        859dbd30 81c78f78 nt!KeRemoveQueueEx+0x568
        859dbd7c 81e254e0 nt!ExpWorkerThread+0xd5
        859dbdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 82f3a2d8  Cid 0004.003c  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            81cfde7c  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      8861           Ticks: 34638 (0:00:09:00.356)
        Context Switch Count      554
        UserTime                  00:00:00.000
        KernelTime                00:00:00.062
        Win32 Start Address nt!ExpWorkerThread (0x81c78ea3)
        Stack Init 859d8000 Current 859d7c90 Base 859d8000 Limit 859d5000 Call 0
        Priority 14 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        859d7ca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        859d7ce4 81cad431 nt!KiSwapThread+0x389
        859d7d30 81c78f78 nt!KeRemoveQueueEx+0x568
        859d7d7c 81e254e0 nt!ExpWorkerThread+0xd5
        859d7dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 82f3b020  Cid 0004.0040  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            81cfde7c  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      9807           Ticks: 33692 (0:00:08:45.598)
        Context Switch Count      1402
        UserTime                  00:00:00.000
        KernelTime                00:00:00.187
        Win32 Start Address nt!ExpWorkerThread (0x81c78ea3)
        Stack Init 859d4000 Current 859d3c90 Base 859d4000 Limit 859d1000 Call 0
        Priority 14 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        859d3ca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        859d3ce4 81cad431 nt!KiSwapThread+0x389
        859d3d30 81c78f78 nt!KeRemoveQueueEx+0x568
        859d3d7c 81e254e0 nt!ExpWorkerThread+0xd5
        859d3dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 82f3bd78  Cid 0004.0044  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            81cfde7c  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      43496          Ticks: 3 (0:00:00:00.046)
        Context Switch Count      5183
        UserTime                  00:00:00.000
        KernelTime                00:00:00.202
        Win32 Start Address nt!ExpWorkerThread (0x81c78ea3)
        Stack Init 859d0000 Current 859cfc90 Base 859d0000 Limit 859cd000 Call 0
        Priority 13 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        859cfca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        859cfce4 81cad431 nt!KiSwapThread+0x389
        859cfd30 81c78f78 nt!KeRemoveQueueEx+0x568
        859cfd7c 81e254e0 nt!ExpWorkerThread+0xd5
        859cfdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 82f3bad0  Cid 0004.0048  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            81cfde7c  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      43384          Ticks: 115 (0:00:00:01.794)
        Context Switch Count      9947
        UserTime                  00:00:00.000
        KernelTime                00:00:01.466
        Win32 Start Address nt!ExpWorkerThread (0x81c78ea3)
        Stack Init 859cc000 Current 859cbc90 Base 859cc000 Limit 859c9000 Call 0
        Priority 12 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        859cbca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        859cbce4 81cad431 nt!KiSwapThread+0x389
        859cbd30 81c78f78 nt!KeRemoveQueueEx+0x568
        859cbd7c 81e254e0 nt!ExpWorkerThread+0xd5
        859cbdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 82f3b828  Cid 0004.004c  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
KernelMode Non-Alertable
            81cfdeb8  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      43448          Ticks: 51 (0:00:00:00.795)
        Context Switch Count      1208
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!ExpWorkerThread (0x81c78ea3)
        Stack Init 859c8000 Current 859c7c90 Base 859c8000 Limit 859c5000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        859c7ca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        859c7ce4 81cad431 nt!KiSwapThread+0x389
        859c7d30 81c78f78 nt!KeRemoveQueueEx+0x568
        859c7d7c 81e254e0 nt!ExpWorkerThread+0xd5
        859c7dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 82f3b580  Cid 0004.0050  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            859c3d50  NotificationTimer
            81cfde20  SynchronizationEvent
            81cfde10  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      43455          Ticks: 44 (0:00:00:00.686)
        Context Switch Count      684
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!ExpWorkerThreadBalanceManager (0x81e877d6)
        Stack Init 859c4000 Current 859c3c68 Base 859c4000 Limit 859c1000 Call 0
        Priority 14 BasePriority 14 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        859c3c80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        859c3cbc 81c28c64 nt!KiSwapThread+0x389
        859c3d08 81e8783e nt!KeWaitForMultipleObjects+0x47d
        859c3d7c 81e254e0 nt!ExpWorkerThreadBalanceManager+0x68
        859c3dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 82f3d4d8  Cid 0004.0054  Teb: 00000000 Win32Thread: 00000000 WAIT: (Suspended)
KernelMode Non-Alertable
            81cf61d0  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      43306          Ticks: 193 (0:00:00:03.010)
        Context Switch Count      48
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!KiExecuteDpc (0x81c276cd)
        Stack Init 859c0000 Current 859bfc70 Base 859c0000 Limit 859bd000 Call 0
        Priority 31 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        859bfc88 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        859bfcc4 81c293a7 nt!KiSwapThread+0x389
        859bfd24 81c27827 nt!KeWaitForSingleObject+0x414
        859bfd7c 81e254e0 nt!KiExecuteDpc+0x15a
        859bfdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 82f3d230  Cid 0004.0058  Teb: 00000000 Win32Thread: 00000000 WAIT: (Suspended)
KernelMode Non-Alertable
            84e29ad0  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      43316          Ticks: 183 (0:00:00:02.854)
        Context Switch Count      47
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!KiExecuteDpc (0x81c276cd)
        Stack Init 859bc000 Current 859bbc70 Base 859bc000 Limit 859b9000 Call 0
        Priority 31 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        859bbc88 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        859bbcc4 81c293a7 nt!KiSwapThread+0x389
        859bbd24 81c27827 nt!KeWaitForSingleObject+0x414
        859bbd7c 81e254e0 nt!KiExecuteDpc+0x15a
        859bbdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 82f40020  Cid 0004.005c  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrVirtualMemory)
UserMode Non-Alertable
            81d121a0  Semaphore Limit 0x7fffffff
            81d12210  NotificationEvent
            81d122b0  NotificationEvent
            81d11c30  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      18468          Ticks: 25031 (0:00:06:30.486)
        Context Switch Count      212
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!MiDereferenceSegmentThread (0x81c11492)
        Stack Init 859b8000 Current 859b7c98 Base 859b8000 Limit 859b5000 Call 0
        Priority 18 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        859b7cb0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        859b7cec 81c28c64 nt!KiSwapThread+0x389
        859b7d38 81c114ef nt!KeWaitForMultipleObjects+0x47d
        859b7d7c 81e254e0 nt!MiDereferenceSegmentThread+0x5d
        859b7dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 82f40d78  Cid 0004.0060  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrFreePage)
KernelMode Non-Alertable
            81d113d0  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      43319          Ticks: 180 (0:00:00:02.808)
        Context Switch Count      261
        UserTime                  00:00:00.000
        KernelTime                00:00:00.078
        Win32 Start Address nt!MiModifiedPageWriter (0x81c218ca)
        Stack Init 859b4000 Current 859b3c88 Base 859b4000 Limit 859b1000 Call 0
        Priority 17 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        859b3ca0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        859b3cdc 81c293a7 nt!KiSwapThread+0x389
        859b3d3c 81c2190a nt!KeWaitForSingleObject+0x414
        859b3d7c 81e254e0 nt!MiModifiedPageWriter+0x40
        859b3dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 82f40898  Cid 0004.0064  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrFreePage)
KernelMode Non-Alertable
            81d11ee0  SynchronizationEvent
            81d11ef0  SynchronizationEvent
            81d11f00  SynchronizationEvent
            81d11f10  SynchronizationEvent
            81d11f20  SynchronizationEvent
            81d11f30  SynchronizationEvent
            81d11f40  SynchronizationEvent
            81d11f50  SynchronizationEvent
            81d11f60  SynchronizationEvent
            81d11f70  SynchronizationEvent
            81d11f80  SynchronizationEvent
            81d11f90  SynchronizationEvent
            81d11fa0  SynchronizationEvent
            81d11fb0  SynchronizationEvent
            81d11fc0  SynchronizationEvent
            81d11fd0  SynchronizationEvent
            81d11fe0  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      23             Ticks: 43476 (0:00:11:18.229)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!MiMappedPageWriter (0x81c39e30)
        Stack Init 859b0000 Current 859afc58 Base 859b0000 Limit 859ad000 Call 0
        Priority 17 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        859afc70 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        859afcac 81c28c64 nt!KiSwapThread+0x389
        859afcf8 81c39e96 nt!KeWaitForMultipleObjects+0x47d
        859afd7c 81e254e0 nt!MiMappedPageWriter+0x66
        859afdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 82f40390  Cid 0004.0068  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            859abd20  SynchronizationTimer
            81d11d10  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      43447          Ticks: 52 (0:00:00:00.811)
        Context Switch Count      768
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!KeBalanceSetManager (0x81cafd5e)
        Stack Init 859ac000 Current 859abc18 Base 859ac000 Limit 859a9000 Call 0
        Priority 16 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        859abc30 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        859abc6c 81c28c64 nt!KiSwapThread+0x389
        859abcb8 81cafe2a nt!KeWaitForMultipleObjects+0x47d
        859abd7c 81e254e0 nt!KeBalanceSetManager+0xcc
        859abdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 82f3f020  Cid 0004.006c  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            81d28db0  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      43447          Ticks: 52 (0:00:00:00.811)
        Context Switch Count      3041
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address nt!KeSwapProcessOrStack (0x81cb38d4)
        Stack Init 859a8000 Current 859a7ca8 Base 859a8000 Limit 859a5000 Call 0
        Priority 23 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        859a7cc0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        859a7cfc 81c293a7 nt!KiSwapThread+0x389
        859a7d5c 81cb3907 nt!KeWaitForSingleObject+0x414
        859a7d7c 81e254e0 nt!KeSwapProcessOrStack+0x33
        859a7dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 82f3faf0  Cid 0004.0070  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrFreePage)
KernelMode Non-Alertable
            81d301f0  SynchronizationEvent
            81d301e0  SynchronizationEvent
            81d301d0  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      42744          Ticks: 755 (0:00:00:11.778)
        Context Switch Count      543
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!CcQueueLazyWriteScanThread (0x81cbc009)
        Stack Init 85894000 Current 85893c90 Base 85894000 Limit 85891000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        85893ca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85893ce4 81c28c64 nt!KiSwapThread+0x389
        85893d30 81cbc04b nt!KeWaitForMultipleObjects+0x47d
        85893d7c 81e254e0 nt!CcQueueLazyWriteScanThread+0x42
        85893dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 82f35830  Cid 0004.0074  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
KernelMode Non-Alertable
            81d2f200  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      32             Ticks: 43467 (0:00:11:18.089)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!FsRtlWorkerThread (0x81c01468)
        Stack Init 85890000 Current 8588fcb0 Base 85890000 Limit 8588d000 Call 0
        Priority 16 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        8588fcc8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        8588fd04 81cad431 nt!KiSwapThread+0x389
        8588fd50 81c014a9 nt!KeRemoveQueueEx+0x568
        8588fd7c 81e254e0 nt!FsRtlWorkerThread+0x41
        8588fdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 82f35588  Cid 0004.0078  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
KernelMode Non-Alertable
            81d2f228  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      28             Ticks: 43471 (0:00:11:18.151)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!FsRtlWorkerThread (0x81c01468)
        Stack Init 8588c000 Current 8588bcb0 Base 8588c000 Limit 85889000 Call 0
        Priority 17 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        8588bcc8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        8588bd04 81cad431 nt!KiSwapThread+0x389
        8588bd50 81c014a9 nt!KeRemoveQueueEx+0x568
        8588bd7c 81e254e0 nt!FsRtlWorkerThread+0x41
        8588bdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 82f0cd78  Cid 0004.0080  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            82f0b2a4  SynchronizationEvent
            82f0ce00  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      43485          Ticks: 14 (0:00:00:00.218)
        Context Switch Count      688
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!EtwpLogger (0x81e708a2)
        Stack Init 85884000 Current 85883c78 Base 85884000 Limit 85881000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        85883c90 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85883ccc 81c293a7 nt!KiSwapThread+0x389
        85883d2c 81e70969 nt!KeWaitForSingleObject+0x414
        85883d7c 81e254e0 nt!EtwpLogger+0xc7
        85883dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 82f0c730  Cid 0004.0084  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            82f0cbe4  SynchronizationEvent
            82f0c7b8  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      43442          Ticks: 57 (0:00:00:00.889)
        Context Switch Count      692
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!EtwpLogger (0x81e708a2)
        Stack Init 85880000 Current 8587fc78 Base 85880000 Limit 8587d000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        8587fc90 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        8587fccc 81c293a7 nt!KiSwapThread+0x389
        8587fd2c 81e70969 nt!KeWaitForSingleObject+0x414
        8587fd7c 81e254e0 nt!EtwpLogger+0xc7
        8587fdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 83352d78  Cid 0004.0088  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            83352164  SynchronizationEvent
            83352e00  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      43488          Ticks: 11 (0:00:00:00.171)
        Context Switch Count      681
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!EtwpLogger (0x81e708a2)
        Stack Init 8587c000 Current 8587bc78 Base 8587c000 Limit 85879000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        8587bc90 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        8587bccc 81c293a7 nt!KiSwapThread+0x389
        8587bd2c 81e70969 nt!KeWaitForSingleObject+0x414
        8587bd7c 81e254e0 nt!EtwpLogger+0xc7
        8587bdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 833527d0  Cid 0004.008c  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            83352be4  SynchronizationEvent
            83352858  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      43469          Ticks: 30 (0:00:00:00.468)
        Context Switch Count      681
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!EtwpLogger (0x81e708a2)
        Stack Init 85878000 Current 85877c78 Base 85878000 Limit 85875000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        85877c90 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85877ccc 81c293a7 nt!KiSwapThread+0x389
        85877d2c 81e70969 nt!KeWaitForSingleObject+0x414
        85877d7c 81e254e0 nt!EtwpLogger+0xc7
        85877dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 833d64f8  Cid 0004.0090  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            833d68e4  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      33             Ticks: 43466 (0:00:11:18.073)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!EtwpLogger (0x81e708a2)
        Stack Init 85874000 Current 85873c78 Base 85874000 Limit 85871000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        85873c90 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85873ccc 81c293a7 nt!KiSwapThread+0x389
        85873d2c 81e70908 nt!KeWaitForSingleObject+0x414
        85873d7c 81e254e0 nt!EtwpLogger+0x66
        85873dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 833dbd78  Cid 0004.0094  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            833db164  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      33             Ticks: 43466 (0:00:11:18.073)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!EtwpLogger (0x81e708a2)
        Stack Init 85870000 Current 8586fc78 Base 85870000 Limit 8586d000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        8586fc90 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        8586fccc 81c293a7 nt!KiSwapThread+0x389
        8586fd2c 81e70908 nt!KeWaitForSingleObject+0x414
        8586fd7c 81e254e0 nt!EtwpLogger+0x66
        8586fdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 833db7d0  Cid 0004.0098  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            833dbbe4  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      33             Ticks: 43466 (0:00:11:18.073)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!EtwpLogger (0x81e708a2)
        Stack Init 8586c000 Current 8586bc78 Base 8586c000 Limit 85869000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        8586bc90 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        8586bccc 81c293a7 nt!KiSwapThread+0x389
        8586bd2c 81e70908 nt!KeWaitForSingleObject+0x414
        8586bd7c 81e254e0 nt!EtwpLogger+0x66
        8586bdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 83a5c370  Cid 0004.00a0  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            83a5c824  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      15151          Ticks: 28348 (0:00:07:22.231)
        Context Switch Count      33
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!EtwpLogger (0x81e708a2)
        Stack Init 85864000 Current 85863c78 Base 85864000 Limit 85861000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        85863c90 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85863ccc 81c293a7 nt!KiSwapThread+0x389
        85863d2c 81e70969 nt!KeWaitForSingleObject+0x414
        85863d7c 81e254e0 nt!EtwpLogger+0xc7
        85863dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 83c6d278  Cid 0004.00a4  Teb: 00000000 Win32Thread: 00000000 WAIT: (DelayExecution)
KernelMode Non-Alertable
            83c6d300  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      42343          Ticks: 1156 (0:00:00:18.033)
        Context Switch Count      12
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!WdipSemCheckTimeout (0x81e64737)
        Stack Init 85860000 Current 8585fc40 Base 85860000 Limit 8585d000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        8585fc58 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        8585fc94 81cac48e nt!KiSwapThread+0x389
        8585fcf4 81e6495d nt!KeDelayExecutionThread+0x397
        8585fd7c 81e254e0 nt!WdipSemCheckTimeout+0x226
        8585fdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 83c8a020  Cid 0004.00a8  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            80489600  NotificationEvent
            804895f0  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      784            Ticks: 42715 (0:00:11:06.358)
        Context Switch Count      343
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address acpi!ACPIWorkerThread (0x8047606e)
        Stack Init 85856000 Current 85855c98 Base 85856000 Limit 85853000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        85855cb0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85855cec 81c28c64 nt!KiSwapThread+0x389
        85855d3c 804760b5 nt!KeWaitForMultipleObjects+0x47d
        85855d7c 81e254e0 acpi!ACPIWorkerThread+0x47 (FPO: [Non-Fpo])
        85855dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 83c9d020  Cid 0004.00b0  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            833375d0  SynchronizationEvent
            833375e0  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      41             Ticks: 43458 (0:00:11:17.949)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address pci!ExpressRootComplexPmeEventDispatcher (0x8043be80)
        Stack Init 8584e000 Current 8584dca0 Base 8584e000 Limit 8584b000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        8584dcb8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        8584dcf4 81c28c64 nt!KiSwapThread+0x389
        8584dd40 8043beb4 nt!KeWaitForMultipleObjects+0x47d
        8584dd7c 81e254e0 pci!ExpressRootComplexPmeEventDispatcher+0x34 (FPO: [Non-Fpo])
        8584ddc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 83c9dd78  Cid 0004.00b4  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            83319a0c  SynchronizationEvent
            833199fc  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      41             Ticks: 43458 (0:00:11:17.949)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address acpi!PciRootBusBiosMethodDispatcherOnResume (0x804709fc)
        Stack Init 8584a000 Current 85849ca0 Base 8584a000 Limit 85847000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        85849cb8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85849cf4 81c28c64 nt!KiSwapThread+0x389
        85849d44 80470a2c nt!KeWaitForMultipleObjects+0x47d
        85849d7c 81e254e0 acpi!PciRootBusBiosMethodDispatcherOnResume+0x30 (FPO: [Non-Fpo])
        85849dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 83cbd880  Cid 0004.00b8  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
KernelMode Non-Alertable
            80680da8  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      1086           Ticks: 42413 (0:00:11:01.647)
        Context Switch Count      14
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ndis!ndisWorkerThread (0x80724690)
        Stack Init 85814000 Current 85813ca0 Base 85814000 Limit 85811000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        85813cb8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85813cf4 81cad431 nt!KiSwapThread+0x389
        85813d40 81cc26f6 nt!KeRemoveQueueEx+0x568
        85813d60 807246ce nt!KeRemoveQueue+0x1b
        85813d7c 81e254e0 ndis!ndisWorkerThread+0x3e (FPO: [Non-Fpo])
        85813dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 83cd7aa0  Cid 0004.00bc  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            80681530  NotificationEvent
            83cd7b28  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      42474          Ticks: 1025 (0:00:00:15.990)
        Context Switch Count      23
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ndis!ndisCmWaitThread (0x8064caa0)
        Stack Init 85810000 Current 8580fc98 Base 85810000 Limit 8580d000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        8580fcb0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        8580fcec 81c293a7 nt!KiSwapThread+0x389
        8580fd4c 8064cafb nt!KeWaitForSingleObject+0x414
        8580fd7c 81e254e0 ndis!ndisCmWaitThread+0x5b (FPO: [Non-Fpo])
        8580fdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 83cd77f8  Cid 0004.00c0  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            84fed41c  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      5024           Ticks: 38475 (0:00:10:00.213)
        Context Switch Count      15289
        UserTime                  00:00:00.000
        KernelTime                00:00:02.854
        Win32 Start Address ecache!EcCacheIoWorker (0x84fe76fa)
        Stack Init 8580c000 Current 8580bbe0 Base 8580c000 Limit 85809000 Call 0
        Priority 13 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        8580bbf8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        8580bc34 81c293a7 nt!KiSwapThread+0x389
        8580bc90 84fe773b nt!KeWaitForSingleObject+0x414
        8580bd7c 81e254e0 ecache!EcCacheIoWorker+0x41 (FPO: [Non-Fpo])
        8580bdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 83cd7550  Cid 0004.00c4  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            84fed480  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      5023           Ticks: 38476 (0:00:10:00.229)
        Context Switch Count      12936
        UserTime                  00:00:00.000
        KernelTime                00:00:00.093
        Win32 Start Address ecache!EcCacheIoWatchdog (0x84fe608c)
        Stack Init 85808000 Current 85807c50 Base 85808000 Limit 85805000 Call 0
        Priority 13 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        85807c68 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85807ca4 81c293a7 nt!KiSwapThread+0x389
        85807d04 84fe6459 nt!KeWaitForSingleObject+0x414
        85807d7c 81e254e0 ecache!EcCacheIoWatchdog+0x3cd (FPO: [Non-Fpo])
        85807dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 847a7968  Cid 0004.00cc  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            83cd722c  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      182            Ticks: 43317 (0:00:11:15.749)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address volsnap!VspWorkerThread (0x81a3432a)
        Stack Init 85df4000 Current 85df3ca0 Base 85df4000 Limit 85df1000 Call 0
        Priority 20 BasePriority 8 PriorityDecrement 0 IoPriority 3 PagePriority 5
        ChildEBP RetAddr
        85df3cb8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85df3cf4 81c293a7 nt!KiSwapThread+0x389
        85df3d50 81a3437b nt!KeWaitForSingleObject+0x414
        85df3d7c 81e254e0 volsnap!VspWorkerThread+0x51 (FPO: [Non-Fpo])
        85df3dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 84651558  Cid 0004.00d0  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            83cd7240  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      32052          Ticks: 11447 (0:00:02:58.574)
        Context Switch Count      185
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address volsnap!VspWorkerThread (0x81a3432a)
        Stack Init 85df0000 Current 85defca0 Base 85df0000 Limit 85ded000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        85defcb8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85defcf4 81c293a7 nt!KiSwapThread+0x389
        85defd50 81a343b9 nt!KeWaitForSingleObject+0x414
        85defd7c 81e254e0 volsnap!VspWorkerThread+0x8f (FPO: [Non-Fpo])
        85defdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 846512b0  Cid 0004.00d4  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            83cd7254  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      32052          Ticks: 11447 (0:00:02:58.574)
        Context Switch Count      2644
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address volsnap!VspWorkerThread (0x81a3432a)
        Stack Init 85dec000 Current 85debca0 Base 85dec000 Limit 85de9000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        85debcb8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85debcf4 81c293a7 nt!KiSwapThread+0x389
        85debd50 81a343b9 nt!KeWaitForSingleObject+0x414
        85debd7c 81e254e0 volsnap!VspWorkerThread+0x8f (FPO: [Non-Fpo])
        85debdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 8444bb98  Cid 0004.00d8  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            83cd7268  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      283            Ticks: 43216 (0:00:11:14.173)
        Context Switch Count      6
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address volsnap!VspWorkerThread (0x81a3432a)
        Stack Init 85de8000 Current 85de7ca0 Base 85de8000 Limit 85de5000 Call 0
        Priority 20 BasePriority 8 PriorityDecrement 0 IoPriority 3 PagePriority 5
        ChildEBP RetAddr
        85de7cb8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85de7cf4 81c293a7 nt!KiSwapThread+0x389
        85de7d50 81a343b9 nt!KeWaitForSingleObject+0x414
        85de7d7c 81e254e0 volsnap!VspWorkerThread+0x8f (FPO: [Non-Fpo])
        85de7dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 8444b8f0  Cid 0004.00dc  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            83cd727c  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      182            Ticks: 43317 (0:00:11:15.749)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address volsnap!VspWorkerThread (0x81a3432a)
        Stack Init 85de4000 Current 85de3ca0 Base 85de4000 Limit 85de1000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        85de3cb8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85de3cf4 81c293a7 nt!KiSwapThread+0x389
        85de3d50 81a3437b nt!KeWaitForSingleObject+0x414
        85de3d7c 81e254e0 volsnap!VspWorkerThread+0x51 (FPO: [Non-Fpo])
        85de3dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 8480d3b8  Cid 0004.00e0  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            81afc698  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      41739          Ticks: 1760 (0:00:00:27.456)
        Context Switch Count      913
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address Ntfs!TxfPrivateThreadWorkerRoutine (0x81ada1db)
        Stack Init 85dd4000 Current 85dd3ca8 Base 85dd4000 Limit 85dd1000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        85dd3cc0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85dd3cfc 81c293a7 nt!KiSwapThread+0x389
        85dd3d58 81ada1fb nt!KeWaitForSingleObject+0x414
        85dd3d7c 81e254e0 Ntfs!TxfPrivateThreadWorkerRoutine+0x20 (FPO: [Non-Fpo])
        85dd3dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 84902d78  Cid 0004.00e8  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            8857f0a0  SynchronizationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      482            Ticks: 43017 (0:00:11:11.069)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address dxgkrnl!DpiPdoPollingThread (0x885cbea5)
        Stack Init 85dd8000 Current 85dd7c90 Base 85dd8000 Limit 85dd5000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        85dd7ca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85dd7ce4 81c293a7 nt!KiSwapThread+0x389
        85dd7d40 885cbede nt!KeWaitForSingleObject+0x414
        85dd7d7c 81e254e0 dxgkrnl!DpiPdoPollingThread+0x39 (FPO: [Non-Fpo])
        85dd7dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 84902ad0  Cid 0004.00ec  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            85c0e1c0  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      482            Ticks: 43017 (0:00:11:11.069)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address watchdog!SMgrGdiCalloutThread (0x85c0a4e2)
        Stack Init 85d40000 Current 85d3fc78 Base 85d40000 Limit 85d3d000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        85d3fc90 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85d3fccc 81c293a7 nt!KiSwapThread+0x389
        85d3fd28 85c0a527 nt!KeWaitForSingleObject+0x414
        85d3fd7c 81e254e0 watchdog!SMgrGdiCalloutThread+0x45 (FPO: [Non-Fpo])
        85d3fdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 84902828  Cid 0004.00f0  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            84903f90  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      482            Ticks: 43017 (0:00:11:11.069)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address dxgkrnl!DpiPowerArbiterThread (0x885c95e7)
        Stack Init 85dc8000 Current 85dc7c90 Base 85dc8000 Limit 85dc5000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        85dc7ca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85dc7ce4 81c293a7 nt!KiSwapThread+0x389
        85dc7d40 885c9627 nt!KeWaitForSingleObject+0x414
        85dc7d7c 81e254e0 dxgkrnl!DpiPowerArbiterThread+0x40 (FPO: [Non-Fpo])
        85dc7dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 84cdd660  Cid 0004.0110  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            88053490  SynchronizationEvent
            88053470  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      9417           Ticks: 34082 (0:00:08:51.682)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address raspptp!MainPassiveLevelThread (0x880467d7)
        Stack Init 85d44000 Current 85d43c98 Base 85d44000 Limit 85d41000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        85d43cb0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85d43cec 81c28c64 nt!KiSwapThread+0x389
        85d43d3c 88046845 nt!KeWaitForMultipleObjects+0x47d
        85d43d7c 81e254e0 raspptp!MainPassiveLevelThread+0x6e (FPO: [Non-Fpo])
        85d43dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 84b60af8  Cid 0004.0114  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            84bfd3e4  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      1075           Ticks: 42424 (0:00:11:01.818)
        Context Switch Count      14
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address stwrt (0x88df1580)
        Stack Init 85d3c000 Current 85d3bca0 Base 85d3c000 Limit 85d39000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        85d3bcb8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85d3bcf4 81c293a7 nt!KiSwapThread+0x389
        85d3bd50 88df152d nt!KeWaitForSingleObject+0x414
        85d3bd7c 81e254e0 stwrt+0x9452d
        85d3bdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 84c6b020  Cid 0004.0118  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            85c73060  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      655            Ticks: 42844 (0:00:11:08.370)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address rasacd!AcdNotificationRequestThread (0x85c70f6c)
        Stack Init 85ddc000 Current 85ddbc98 Base 85ddc000 Limit 85dd9000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        85ddbcb0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85ddbcec 81c293a7 nt!KiSwapThread+0x389
        85ddbd4c 85c7104c nt!KeWaitForSingleObject+0x414
        85ddbd7c 81e254e0 rasacd!AcdNotificationRequestThread+0xe0 (FPO: [Non-Fpo])
        85ddbdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 84dc0760  Cid 0004.0134  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
KernelMode Non-Alertable
            88ee101c  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      658            Ticks: 42841 (0:00:11:08.323)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address rdbss!RxBootstrapWorkerThreadDispatcher (0x88ef9bf6)
        Stack Init 85d08000 Current 85d07c48 Base 85d08000 Limit 85d05000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        85d07c60 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85d07c9c 81cad431 nt!KiSwapThread+0x389
        85d07cec 81cc26f6 nt!KeRemoveQueueEx+0x568
        85d07d0c 88ecc15e nt!KeRemoveQueue+0x1b
        85d07d6c 88ef9c05 rdbss!RxpWorkerThreadDispatcher+0x84 (FPO: [Non-Fpo])
        85d07d7c 81e254e0 rdbss!RxBootstrapWorkerThreadDispatcher+0xf (FPO: [Non-Fpo])
        85d07dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 84dbb5f0  Cid 0004.0138  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
KernelMode Non-Alertable
            88ee101c  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      658            Ticks: 42841 (0:00:11:08.323)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address rdbss!RxBootstrapWorkerThreadDispatcher (0x88ef9bf6)
        Stack Init 85d00000 Current 85cffc48 Base 85d00000 Limit 85cfd000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        85cffc60 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85cffc9c 81cad431 nt!KiSwapThread+0x389
        85cffcec 81cc26f6 nt!KeRemoveQueueEx+0x568
        85cffd0c 88ecc15e nt!KeRemoveQueue+0x1b
        85cffd6c 88ef9c05 rdbss!RxpWorkerThreadDispatcher+0x84 (FPO: [Non-Fpo])
        85cffd7c 81e254e0 rdbss!RxBootstrapWorkerThreadDispatcher+0xf (FPO: [Non-Fpo])
        85cffdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 84dc5810  Cid 0004.013c  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
KernelMode Non-Alertable
            88ee10c4  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      658            Ticks: 42841 (0:00:11:08.323)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address rdbss!RxBootstrapWorkerThreadDispatcher (0x88ef9bf6)
        Stack Init 85cfc000 Current 85cfbc48 Base 85cfc000 Limit 85cf9000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        85cfbc60 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85cfbc9c 81cad431 nt!KiSwapThread+0x389
        85cfbcec 81cc26f6 nt!KeRemoveQueueEx+0x568
        85cfbd0c 88ecc15e nt!KeRemoveQueue+0x1b
        85cfbd6c 88ef9c05 rdbss!RxpWorkerThreadDispatcher+0x84 (FPO: [Non-Fpo])
        85cfbd7c 81e254e0 rdbss!RxBootstrapWorkerThreadDispatcher+0xf (FPO: [Non-Fpo])
        85cfbdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 84dc5568  Cid 0004.0140  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
KernelMode Non-Alertable
            88ee10c4  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      658            Ticks: 42841 (0:00:11:08.323)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address rdbss!RxBootstrapWorkerThreadDispatcher (0x88ef9bf6)
        Stack Init 85d04000 Current 85d03c48 Base 85d04000 Limit 85d01000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        85d03c60 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85d03c9c 81cad431 nt!KiSwapThread+0x389
        85d03cec 81cc26f6 nt!KeRemoveQueueEx+0x568
        85d03d0c 88ecc15e nt!KeRemoveQueue+0x1b
        85d03d6c 88ef9c05 rdbss!RxpWorkerThreadDispatcher+0x84 (FPO: [Non-Fpo])
        85d03d7c 81e254e0 rdbss!RxBootstrapWorkerThreadDispatcher+0xf (FPO: [Non-Fpo])
        85d03dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 84dca020  Cid 0004.0144  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
KernelMode Non-Alertable
            88ee0d7c  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      42241          Ticks: 1258 (0:00:00:19.624)
        Context Switch Count      34
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address rdbss!RxBootstrapWorkerThreadDispatcher (0x88ef9bf6)
        Stack Init 85d0c000 Current 85d0bc48 Base 85d0c000 Limit 85d09000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        85d0bc60 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85d0bc9c 81cad431 nt!KiSwapThread+0x389
        85d0bcec 81cc26f6 nt!KeRemoveQueueEx+0x568
        85d0bd0c 88ecc15e nt!KeRemoveQueue+0x1b
        85d0bd6c 88ef9c05 rdbss!RxpWorkerThreadDispatcher+0x84 (FPO: [Non-Fpo])
        85d0bd7c 81e254e0 rdbss!RxBootstrapWorkerThreadDispatcher+0xf (FPO: [Non-Fpo])
        85d0bdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 84dcad78  Cid 0004.0148  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
KernelMode Non-Alertable
            88ee0e24  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      658            Ticks: 42841 (0:00:11:08.323)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address rdbss!RxBootstrapWorkerThreadDispatcher (0x88ef9bf6)
        Stack Init 85d18000 Current 85d17c48 Base 85d18000 Limit 85d15000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        85d17c60 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85d17c9c 81cad431 nt!KiSwapThread+0x389
        85d17cec 81cc26f6 nt!KeRemoveQueueEx+0x568
        85d17d0c 88ecc15e nt!KeRemoveQueue+0x1b
        85d17d6c 88ef9c05 rdbss!RxpWorkerThreadDispatcher+0x84 (FPO: [Non-Fpo])
        85d17d7c 81e254e0 rdbss!RxBootstrapWorkerThreadDispatcher+0xf (FPO: [Non-Fpo])
        85d17dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 84dcaad0  Cid 0004.014c  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
KernelMode Non-Alertable
            88ee0ecc  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      658            Ticks: 42841 (0:00:11:08.323)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address rdbss!RxBootstrapWorkerThreadDispatcher (0x88ef9bf6)
        Stack Init 85d1c000 Current 85d1bc48 Base 85d1c000 Limit 85d19000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        85d1bc60 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85d1bc9c 81cad431 nt!KiSwapThread+0x389
        85d1bcec 81cc26f6 nt!KeRemoveQueueEx+0x568
        85d1bd0c 88ecc15e nt!KeRemoveQueue+0x1b
        85d1bd6c 88ef9c05 rdbss!RxpWorkerThreadDispatcher+0x84 (FPO: [Non-Fpo])
        85d1bd7c 81e254e0 rdbss!RxBootstrapWorkerThreadDispatcher+0xf (FPO: [Non-Fpo])
        85d1bdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 84dca828  Cid 0004.0150  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
KernelMode Non-Alertable
            88ee0f74  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      658            Ticks: 42841 (0:00:11:08.323)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address rdbss!RxBootstrapWorkerThreadDispatcher (0x88ef9bf6)
        Stack Init 85d20000 Current 85d1fc48 Base 85d20000 Limit 85d1d000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        85d1fc60 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85d1fc9c 81cad431 nt!KiSwapThread+0x389
        85d1fcec 81cc26f6 nt!KeRemoveQueueEx+0x568
        85d1fd0c 88ecc15e nt!KeRemoveQueue+0x1b
        85d1fd6c 88ef9c05 rdbss!RxpWorkerThreadDispatcher+0x84 (FPO: [Non-Fpo])
        85d1fd7c 81e254e0 rdbss!RxBootstrapWorkerThreadDispatcher+0xf (FPO: [Non-Fpo])
        85d1fdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 84dca580  Cid 0004.0154  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
KernelMode Non-Alertable
            88ee0f74  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      42914          Ticks: 585 (0:00:00:09.126)
        Context Switch Count      66
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address rdbss!RxBootstrapWorkerThreadDispatcher (0x88ef9bf6)
        Stack Init 85d24000 Current 85d23c48 Base 85d24000 Limit 85d21000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        85d23c60 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85d23c9c 81cad431 nt!KiSwapThread+0x389
        85d23cec 81cc26f6 nt!KeRemoveQueueEx+0x568
        85d23d0c 88ecc15e nt!KeRemoveQueue+0x1b
        85d23d6c 88ef9c05 rdbss!RxpWorkerThreadDispatcher+0x84 (FPO: [Non-Fpo])
        85d23d7c 81e254e0 rdbss!RxBootstrapWorkerThreadDispatcher+0xf (FPO: [Non-Fpo])
        85d23dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 84dca2d8  Cid 0004.0158  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            88ee111c  NotificationEvent
            84dca360  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      42967          Ticks: 532 (0:00:00:08.299)
        Context Switch Count      12
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address rdbss!RxSpinUpRequestsDispatcher (0x88ed091c)
        Stack Init 85d2c000 Current 85d2bc98 Base 85d2c000 Limit 85d29000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        85d2bcb0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85d2bcec 81c293a7 nt!KiSwapThread+0x389
        85d2bd48 88ed09a3 nt!KeWaitForSingleObject+0x414
        85d2bd7c 81e254e0 rdbss!RxSpinUpRequestsDispatcher+0x87 (FPO: [Non-Fpo])
        85d2bdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 84d9f3b8  Cid 0004.0160  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrLpcReceive)
UserMode Non-Alertable
            84d9f5cc  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      14206          Ticks: 29293 (0:00:07:36.973)
        Context Switch Count      51
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!SepRmCommandServerThread (0x81e3e360)
        Stack Init 85cf8000 Current 85cf78b8 Base 85cf8000 Limit 85cf5000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        85cf78d0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85cf790c 81c293a7 nt!KiSwapThread+0x389
        85cf7968 81dc3dac nt!KeWaitForSingleObject+0x414
        85cf79a0 81dc486e nt!AlpcpReceiveMessagePort+0x221
        85cf7a08 81dbe7b6 nt!AlpcpReceiveLegacyMessage+0x197
        85cf7a74 81dbe69c nt!NtReplyWaitReceivePortEx+0x100
        85cf7a90 81c8caaa nt!NtReplyWaitReceivePort+0x18
        85cf7a90 81c7f1d9 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 85cf7aa8)
        85cf7b18 81e3e428 nt!ZwReplyWaitReceivePort+0x11 (FPO: [4,0,0])
        85cf7d7c 81e254e0 nt!SepRmCommandServerThread+0xc8
        85cf7dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 84875d78  Cid 0004.017c  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            81cfde40  QueueObject
            84875e00  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      43385          Ticks: 114 (0:00:00:01.778)
        Context Switch Count      5878
        UserTime                  00:00:00.000
        KernelTime                00:00:00.717
        Win32 Start Address nt!ExpWorkerThread (0x81c78ea3)
        Stack Init 88ea5000 Current 88ea4c90 Base 88ea5000 Limit 88ea2000 Call 0
        Priority 15 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        88ea4ca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        88ea4ce4 81cad431 nt!KiSwapThread+0x389
        88ea4d30 81c78f78 nt!KeRemoveQueueEx+0x568
        88ea4d7c 81e254e0 nt!ExpWorkerThread+0xd5
        88ea4dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 84875ad0  Cid 0004.0180  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            81cfde40  QueueObject
            84875b58  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      42680          Ticks: 819 (0:00:00:12.776)
        Context Switch Count      3349
        UserTime                  00:00:00.000
        KernelTime                00:00:00.655
        Win32 Start Address nt!ExpWorkerThread (0x81c78ea3)
        Stack Init 88e89000 Current 88e88c90 Base 88e89000 Limit 88e86000 Call 0
        Priority 13 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        88e88ca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        88e88ce4 81cad431 nt!KiSwapThread+0x389
        88e88d30 81c78f78 nt!KeRemoveQueueEx+0x568
        88e88d7c 81e254e0 nt!ExpWorkerThread+0xd5
        88e88dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 84875580  Cid 0004.0188  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            81cfde40  QueueObject
            84875608  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      15262          Ticks: 28237 (0:00:07:20.500)
        Context Switch Count      2575
        UserTime                  00:00:00.000
        KernelTime                00:00:00.171
        Win32 Start Address nt!ExpWorkerThread (0x81c78ea3)
        Stack Init 88ead000 Current 88eacc90 Base 88ead000 Limit 88eaa000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        88eacca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        88eacce4 81cad431 nt!KiSwapThread+0x389
        88eacd30 81c78f78 nt!KeRemoveQueueEx+0x568
        88eacd7c 81e254e0 nt!ExpWorkerThread+0xd5
        88eacdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 848752d8  Cid 0004.018c  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            81cfde40  QueueObject
            84875360  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      17820          Ticks: 25679 (0:00:06:40.594)
        Context Switch Count      1268
        UserTime                  00:00:00.000
        KernelTime                00:00:00.202
        Win32 Start Address nt!ExpWorkerThread (0x81c78ea3)
        Stack Init 88eb1000 Current 88eb0c90 Base 88eb1000 Limit 88eae000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        88eb0ca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        88eb0ce4 81cad431 nt!KiSwapThread+0x389
        88eb0d30 81c78f78 nt!KeRemoveQueueEx+0x568
        88eb0d7c 81e254e0 nt!ExpWorkerThread+0xd5
        88eb0dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 89844d78  Cid 0004.01c4  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            89842d8c  SynchronizationEvent
            89842d7c  SynchronizationEvent
            89842dac  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      25429          Ticks: 18070 (0:00:04:41.893)
        Context Switch Count      3169
        UserTime                  00:00:00.000
        KernelTime                00:00:00.109
        Win32 Start Address dxgkrnl!VidSchiWorkerThread (0x885c8c81)
        Stack Init 84e41000 Current 84e40be0 Base 84e41000 Limit 84e3e000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        84e40bf8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        84e40c34 81c28c64 nt!KiSwapThread+0x389
        84e40c80 88588b69 nt!KeWaitForMultipleObjects+0x47d
        84e40cc8 88565193 dxgkrnl!VidSchiWaitForSchedulerEvents+0x109 (FPO: [Non-Fpo])
        84e40d58 88589093 dxgkrnl!VidSchiScheduleCommandToRun+0xac (FPO: [Non-Fpo])
        84e40d6c 885c8ce2 dxgkrnl!VidSchiRun_PriorityTable+0xf (FPO: [Non-Fpo])
        84e40d7c 81e254e0 dxgkrnl!VidSchiWorkerThread+0x61 (FPO: [Non-Fpo])
        84e40dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 89966080  Cid 0004.01c8  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            89966fbc  NotificationEvent
            89966fcc  NotificationEvent
            89966fdc  NotificationEvent
            89966fec  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      784            Ticks: 42715 (0:00:11:06.358)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address IRFilter (0x87d4cee8)
        Stack Init 88e99000 Current 88e98c98 Base 88e99000 Limit 88e96000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        88e98cb0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        88e98cec 81c28c64 nt!KiSwapThread+0x389
        88e98d38 87d4cfac nt!KeWaitForMultipleObjects+0x47d
        88e98d7c 81e254e0 IRFilter+0xfac
        88e98dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 89945030  Cid 0004.0200  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
KernelMode Alertable
            899442f0  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      29067          Ticks: 14432 (0:00:03:45.140)
        Context Switch Count      174
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address msrpc!LrpcKernelBaseRoutine (0x8062a40f)
        Stack Init 85d10000 Current 85d0fb38 Base 85d10000 Limit 85d0d000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        85d0fb50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85d0fb8c 81cad431 nt!KiSwapThread+0x389
        85d0fbdc 81d8b982 nt!KeRemoveQueueEx+0x568
        85d0fc34 81d8b8e9 nt!IoRemoveIoCompletion+0x23
        85d0fcac 81c8caaa nt!NtRemoveIoCompletionEx+0x151
        85d0fcac 81c7fa0d nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 85d0fccc)
        85d0fd3c 8062a433 nt!ZwRemoveIoCompletionEx+0x11 (FPO: [6,0,0])
        85d0fd7c 81e254e0 msrpc!LrpcKernelBaseRoutine+0x24 (FPO: [Non-Fpo])
        85d0fdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 8997fcf8  Cid 0004.023c  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            8996cae4  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      9649           Ticks: 33850 (0:00:08:48.063)
        Context Switch Count      15
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!EtwpLogger (0x81e708a2)
        Stack Init 9e9f0000 Current 9e9efc78 Base 9e9f0000 Limit 9e9ed000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9e9efc90 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e9efccc 81c293a7 nt!KiSwapThread+0x389
        9e9efd2c 81e70969 nt!KeWaitForSingleObject+0x414
        9e9efd7c 81e254e0 nt!EtwpLogger+0xc7
        9e9efdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 899ca020  Cid 0004.0270  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            899b967c  NotificationEvent
            899b968c  NotificationEvent
            899b969c  NotificationEvent
            899b96ac  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      10213          Ticks: 33286 (0:00:08:39.264)
        Context Switch Count      69
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address bthport!HCI_ThreadFunction (0x9e92ec92)
        Stack Init 88e24000 Current 88e23c20 Base 88e24000 Limit 88e21000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        88e23c38 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        88e23c74 81c28c64 nt!KiSwapThread+0x389
        88e23cc4 9e92ed1b nt!KeWaitForMultipleObjects+0x47d
        88e23d7c 81e254e0 bthport!HCI_ThreadFunction+0x89 (FPO: [Non-Fpo])
        88e23dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 899f1510  Cid 0004.0274  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            899ffb50  NotificationEvent
            899ffb60  NotificationEvent
            899ffb70  NotificationEvent
            899ffb80  NotificationEvent
            899ffb90  NotificationEvent
            899ffba0  NotificationEvent
            899ffbb0  NotificationEvent
            899ffbc0  NotificationEvent
            899ffbd0  NotificationEvent
            899ffc00  NotificationEvent
            899ffbe0  NotificationEvent
            899ffbf0  NotificationEvent
            899ffc10  NotificationEvent
            899ffc20  NotificationEvent
            899ffc30  NotificationEvent
            899ffc40  NotificationEvent
            899ffc50  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      848            Ticks: 42651 (0:00:11:05.359)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address KeyMagic (0x89ad0542)
        Stack Init 88e18000 Current 88e17c60 Base 88e18000 Limit 88e15000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        88e17c78 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        88e17cb4 81c28c64 nt!KiSwapThread+0x389
        88e17d04 89ad06dd nt!KeWaitForMultipleObjects+0x47d
        88e17d7c 81e254e0 KeyMagic+0x26dd
        88e17dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 9e1ffd78  Cid 0004.0310  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            9e1fc1fc  NotificationEvent
            9e1fc20c  SynchronizationEvent
            9e1fc23c  NotificationEvent
        IRP List:
            89871008: (0006,01d8) Flags: 00060800  Mdl: 836992c0
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      32052          Ticks: 11447 (0:00:02:58.574)
        Context Switch Count      803
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address luafv!UsnThread (0x9e883263)
        Stack Init 9e8cf000 Current 9e8cec28 Base 9e8cf000 Limit 9e8cc000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9e8cec40 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e8cec7c 81c28c64 nt!KiSwapThread+0x389
        9e8cecc8 9e8834c0 nt!KeWaitForMultipleObjects+0x47d
        9e8ced08 9e8833e3 luafv!SynchronousFsControl+0xa3 (FPO: [Non-Fpo])
        9e8ced7c 81e254e0 luafv!UsnThread+0x180 (FPO: [Non-Fpo])
        9e8cedc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 9fcd7d78  Cid 0004.0494  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            a02d4994  NotificationEvent
            9fccf018  NotificationEvent
            9fcd1048  NotificationEvent
            9fcd3078  NotificationEvent
            9fcd50a8  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      1078           Ticks: 42421 (0:00:11:01.771)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address spsys!SPVersion (0xa02e9204)
        Stack Init 9f2a8000 Current 9f2a7c80 Base 9f2a8000 Limit 9f2a5000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f2a7c98 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f2a7cd4 81c28c64 nt!KiSwapThread+0x389
        9f2a7d24 a02e90d3 nt!KeWaitForMultipleObjects+0x47d
        9f2a7d74 a02e9211 spsys!SPVersion+0x1489b
        9f2a7d7c 81e254e0 spsys!SPVersion+0x149d9
        9f2a7dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 9fd37918  Cid 0004.05c8  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            9fd37bd0  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      43486          Ticks: 13 (0:00:00:00.202)
        Context Switch Count      183
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address HTTP!UlpThreadPoolWorker (0xa08c4005)
        Stack Init a0925000 Current a0924c90 Base a0925000 Limit a0922000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a0924ca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0924ce4 81c293a7 nt!KiSwapThread+0x389
        a0924d44 a08c40eb nt!KeWaitForSingleObject+0x414
        a0924d7c 81e254e0 HTTP!UlpThreadPoolWorker+0xe6 (FPO: [Non-Fpo])
        a0924dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 9fd54020  Cid 0004.05cc  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            9fd37c10  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      14648          Ticks: 28851 (0:00:07:30.078)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address HTTP!UlpThreadPoolWorker (0xa08c4005)
        Stack Init a0941000 Current a0940c90 Base a0941000 Limit a093e000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a0940ca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0940ce4 81c293a7 nt!KiSwapThread+0x389
        a0940d44 a08c40eb nt!KeWaitForSingleObject+0x414
        a0940d7c 81e254e0 HTTP!UlpThreadPoolWorker+0xe6 (FPO: [Non-Fpo])
        a0940dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 9fd54d78  Cid 0004.05d0  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            9fd37c50  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      43467          Ticks: 32 (0:00:00:00.499)
        Context Switch Count      13
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address HTTP!UlpThreadPoolWorker (0xa08c4005)
        Stack Init a0989000 Current a0988c90 Base a0989000 Limit a0986000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a0988ca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0988ce4 81c293a7 nt!KiSwapThread+0x389
        a0988d44 a08c40eb nt!KeWaitForSingleObject+0x414
        a0988d7c 81e254e0 HTTP!UlpThreadPoolWorker+0xe6 (FPO: [Non-Fpo])
        a0988dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 9fd54ad0  Cid 0004.05d4  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            9fd37c90  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      1158           Ticks: 42341 (0:00:11:00.523)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address HTTP!UlpThreadPoolWorker (0xa08c4005)
        Stack Init a0919000 Current a0918c90 Base a0919000 Limit a0916000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a0918ca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0918ce4 81c293a7 nt!KiSwapThread+0x389
        a0918d44 a08c40eb nt!KeWaitForSingleObject+0x414
        a0918d7c 81e254e0 HTTP!UlpThreadPoolWorker+0xe6 (FPO: [Non-Fpo])
        a0918dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 9fd54828  Cid 0004.05d8  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            9fd37cd0  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      14067          Ticks: 29432 (0:00:07:39.142)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address HTTP!UlpThreadPoolWorker (0xa08c4005)
        Stack Init a091d000 Current a091cc90 Base a091d000 Limit a091a000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a091cca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a091cce4 81c293a7 nt!KiSwapThread+0x389
        a091cd44 a08c40eb nt!KeWaitForSingleObject+0x414
        a091cd7c 81e254e0 HTTP!UlpThreadPoolWorker+0xe6 (FPO: [Non-Fpo])
        a091cdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 9fd54580  Cid 0004.05dc  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            9fd37d10  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      1158           Ticks: 42341 (0:00:11:00.523)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address HTTP!UlpThreadPoolWorker (0xa08c4005)
        Stack Init a092d000 Current a092cc90 Base a092d000 Limit a092a000 Call 0
        Priority 11 BasePriority 11 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a092cca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a092cce4 81c293a7 nt!KiSwapThread+0x389
        a092cd44 a08c40eb nt!KeWaitForSingleObject+0x414
        a092cd7c 81e254e0 HTTP!UlpThreadPoolWorker+0xe6 (FPO: [Non-Fpo])
        a092cdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 9fd4a020  Cid 0004.05e0  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            a08c27e0  NotificationEvent
            a08c27d0  NotificationEvent
            82f40bf8  NotificationEvent
            a08c27f0  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      39877          Ticks: 3622 (0:00:00:56.503)
        Context Switch Count      12
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address HTTP!UlpScavengerThread (0xa08c4435)
        Stack Init a0931000 Current a0930c40 Base a0931000 Limit a092e000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a0930c58 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0930c94 81c28c64 nt!KiSwapThread+0x389
        a0930ce4 a08c4493 nt!KeWaitForMultipleObjects+0x47d
        a0930d7c 81e254e0 HTTP!UlpScavengerThread+0x5e (FPO: [Non-Fpo])
        a0930dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 9fd7b9f8  Cid 0004.0644  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            a0ccf810  SynchronizationEvent
            a0ccf870  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      9808           Ticks: 33691 (0:00:08:45.582)
        Context Switch Count      48
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address mpsdrv!AuditSuccessEvent (0xa0cccbe0)
        Stack Init a086f000 Current a086ec90 Base a086f000 Limit a086c000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 3 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a086eca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a086ece4 81c28c64 nt!KiSwapThread+0x389
        a086ed34 a0cccceb nt!KeWaitForMultipleObjects+0x47d
        a086ed7c 81e254e0 mpsdrv!AuditSuccessEvent+0x19b (FPO: [Non-Fpo])
        a086edc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 9fd97b00  Cid 0004.065c  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            a0ca8200  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      42241          Ticks: 1258 (0:00:00:19.624)
        Context Switch Count      33
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address mrxdav!MRxDAVContextTimerThread (0xa0ca30ca)
        Stack Init a0840000 Current a083fc98 Base a0840000 Limit a083d000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a083fcb0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a083fcec 81c293a7 nt!KiSwapThread+0x389
        a083fd4c a0ca3134 nt!KeWaitForSingleObject+0x414
        a083fd7c 81e254e0 mrxdav!MRxDAVContextTimerThread+0x6a (FPO: [Non-Fpo])
        a083fdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 9fd9a020  Cid 0004.068c  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
KernelMode Non-Alertable
            9fd96170  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      1221           Ticks: 42278 (0:00:10:59.541)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address srv2!SrvProcWorkerThread (0xa0c30005)
        Stack Init a080c000 Current a080bc98 Base a080c000 Limit a0809000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a080bcb0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a080bcec 81cad431 nt!KiSwapThread+0x389
        a080bd3c 81cc26f6 nt!KeRemoveQueueEx+0x568
        a080bd5c a0c3006b nt!KeRemoveQueue+0x1b
        a080bd7c 81e254e0 srv2!SrvProcWorkerThread+0x66 (FPO: [Non-Fpo])
        a080bdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 9fd9ab90  Cid 0004.0690  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
KernelMode Non-Alertable
            9fd96230  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      1226           Ticks: 42273 (0:00:10:59.463)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address srv2!SrvProcWorkerThread (0xa0c30005)
        Stack Init a0820000 Current a081fc98 Base a0820000 Limit a081d000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a081fcb0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a081fcec 81cad431 nt!KiSwapThread+0x389
        a081fd3c 81cc26f6 nt!KeRemoveQueueEx+0x568
        a081fd5c a0c3006b nt!KeRemoveQueue+0x1b
        a081fd7c 81e254e0 srv2!SrvProcWorkerThread+0x66 (FPO: [Non-Fpo])
        a081fdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 9fd9b918  Cid 0004.0698  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
KernelMode Non-Alertable
            9fd99498  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      1227           Ticks: 42272 (0:00:10:59.447)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address srv2!SrvProcWorkerThread (0xa0c30005)
        Stack Init a1b78000 Current a1b77c98 Base a1b78000 Limit a1b75000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a1b77cb0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1b77cec 81cad431 nt!KiSwapThread+0x389
        a1b77d3c 81cc26f6 nt!KeRemoveQueueEx+0x568
        a1b77d5c a0c3006b nt!KeRemoveQueue+0x1b
        a1b77d7c 81e254e0 srv2!SrvProcWorkerThread+0x66 (FPO: [Non-Fpo])
        a1b77dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 9fda2020  Cid 0004.06b4  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
KernelMode Non-Alertable
            9fd99558  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      1229           Ticks: 42270 (0:00:10:59.416)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address srv2!SrvProcWorkerThread (0xa0c30005)
        Stack Init a1bb0000 Current a1bafc98 Base a1bb0000 Limit a1bad000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a1bafcb0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1bafcec 81cad431 nt!KiSwapThread+0x389
        a1bafd3c 81cc26f6 nt!KeRemoveQueueEx+0x568
        a1bafd5c a0c3006b nt!KeRemoveQueue+0x1b
        a1bafd7c 81e254e0 srv2!SrvProcWorkerThread+0x66 (FPO: [Non-Fpo])
        a1bafdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 9fda3020  Cid 0004.06b8  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
KernelMode Non-Alertable
            9fd993d0  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      1229           Ticks: 42270 (0:00:10:59.416)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address srv2!SrvProcWorkerThread (0xa0c30005)
        Stack Init a0824000 Current a0823c98 Base a0824000 Limit a0821000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a0823cb0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0823cec 81cad431 nt!KiSwapThread+0x389
        a0823d3c 81cc26f6 nt!KeRemoveQueueEx+0x568
        a0823d5c a0c3006b nt!KeRemoveQueue+0x1b
        a0823d7c 81e254e0 srv2!SrvProcWorkerThread+0x66 (FPO: [Non-Fpo])
        a0823dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 9fda5978  Cid 0004.06bc  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            9fda46a4  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      1230           Ticks: 42269 (0:00:10:59.400)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address srv!WorkerThread (0xa1bc8d61)
        Stack Init a1bac000 Current a1babc88 Base a1bac000 Limit a1ba9000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1babca0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1babcdc 81cad431 nt!KiSwapThread+0x389
        a1babd28 81cc26f6 nt!KeRemoveQueueEx+0x568
        a1babd48 a1bc8ddb nt!KeRemoveQueue+0x1b
        a1babd7c 81e254e0 srv!WorkerThread+0x7a (FPO: [Non-Fpo])
        a1babdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 9fda5290  Cid 0004.06c0  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            9fda48e4  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      1231           Ticks: 42268 (0:00:10:59.385)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address srv!WorkerThread (0xa1bc8d61)
        Stack Init a1bb4000 Current a1bb3c88 Base a1bb4000 Limit a1bb1000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1bb3ca0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1bb3cdc 81cad431 nt!KiSwapThread+0x389
        a1bb3d28 81cc26f6 nt!KeRemoveQueueEx+0x568
        a1bb3d48 a1bc8ddb nt!KeRemoveQueue+0x1b
        a1bb3d7c 81e254e0 srv!WorkerThread+0x7a (FPO: [Non-Fpo])
        a1bb3dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 9fda8d78  Cid 0004.06c8  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            9fd9b424  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      1232           Ticks: 42267 (0:00:10:59.369)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address srv!WorkerThread (0xa1bc8d61)
        Stack Init a1b84000 Current a1b83c88 Base a1b84000 Limit a1b81000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1b83ca0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1b83cdc 81cad431 nt!KiSwapThread+0x389
        a1b83d28 81cc26f6 nt!KeRemoveQueueEx+0x568
        a1b83d48 a1bc8ddb nt!KeRemoveQueue+0x1b
        a1b83d7c 81e254e0 srv!WorkerThread+0x7a (FPO: [Non-Fpo])
        a1b83dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 9fdb5a98  Cid 0004.06d0  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            a1bc4b2c  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      1233           Ticks: 42266 (0:00:10:59.353)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address srv!WorkerThread (0xa1bc8d61)
        Stack Init a1b8c000 Current a1b8bc88 Base a1b8c000 Limit a1b89000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1b8bca0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1b8bcdc 81cad431 nt!KiSwapThread+0x389
        a1b8bd28 81cc26f6 nt!KeRemoveQueueEx+0x568
        a1b8bd48 a1bc8ddb nt!KeRemoveQueue+0x1b
        a1b8bd7c 81e254e0 srv!WorkerThread+0x7a (FPO: [Non-Fpo])
        a1b8bdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD a18e3d78  Cid 0004.0524  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            a18a85e4  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      1864           Ticks: 41635 (0:00:10:49.510)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!EtwpLogger (0x81e708a2)
        Stack Init a1eb2000 Current a1eb1c78 Base a1eb2000 Limit a1eaf000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a1eb1c90 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1eb1ccc 81c293a7 nt!KiSwapThread+0x389
        a1eb1d2c 81e70969 nt!KeWaitForSingleObject+0x414
        a1eb1d7c 81e254e0 nt!EtwpLogger+0xc7
        a1eb1dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 9fcbf808  Cid 0004.0890  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            81cfae94  NotificationEvent
            81cfae84  NotificationEvent
            81cfae0c  NotificationEvent
            81cfaeb8  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      43326          Ticks: 173 (0:00:00:02.698)
        Context Switch Count      1286
        UserTime                  00:00:00.000
        KernelTime                00:00:00.171
        Win32 Start Address nt!PfTLoggingWorker (0x81dffce3)
        Stack Init 9e9e8000 Current 9e9e7c28 Base 9e9e8000 Limit 9e9e5000 Call 0
        Priority 7 BasePriority 7 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9e9e7c40 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e9e7c7c 81c28c64 nt!KiSwapThread+0x389
        9e9e7cc8 81dffd4a nt!KeWaitForMultipleObjects+0x47d
        9e9e7d7c 81e254e0 nt!PfTLoggingWorker+0x67
        9e9e7dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD a194f7e0  Cid 0004.08bc  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            a1941b64  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      5010           Ticks: 38489 (0:00:10:00.432)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!EtwpLogger (0x81e708a2)
        Stack Init a0911000 Current a0910c78 Base a0911000 Limit a090e000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a0910c90 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0910ccc 81c293a7 nt!KiSwapThread+0x389
        a0910d2c 81e70969 nt!KeWaitForSingleObject+0x414
        a0910d7c 81e254e0 nt!EtwpLogger+0xc7
        a0910dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 8345c030  Cid 0004.08c4  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            83d326a4  SynchronizationEvent
            8345c0b8  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      43479          Ticks: 20 (0:00:00:00.312)
        Context Switch Count      600
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!EtwpLogger (0x81e708a2)
        Stack Init a310c000 Current a310bc78 Base a310c000 Limit a3109000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a310bc90 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a310bccc 81c293a7 nt!KiSwapThread+0x389
        a310bd2c 81e70969 nt!KeWaitForSingleObject+0x414
        a310bd7c 81e254e0 nt!EtwpLogger+0xc7
        a310bdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 835a9490  Cid 0004.0a10  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            835a82a4  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      8856           Ticks: 34643 (0:00:09:00.434)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!EtwpLogger (0x81e708a2)
        Stack Init a3110000 Current a310fc78 Base a3110000 Limit a310d000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a310fc90 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a310fccc 81c293a7 nt!KiSwapThread+0x389
        a310fd2c 81e70969 nt!KeWaitForSingleObject+0x414
        a310fd7c 81e254e0 nt!EtwpLogger+0xc7
        a310fdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 838e6020  Cid 0004.01a8  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            83677164  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      15066          Ticks: 28433 (0:00:07:23.557)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nt!EtwpLogger (0x81e708a2)
        Stack Init 85888000 Current 85887c78 Base 85888000 Limit 85885000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        85887c90 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85887ccc 81c293a7 nt!KiSwapThread+0x389
        85887d2c 81e70908 nt!KeWaitForSingleObject+0x414
        85887d7c 81e254e0 nt!EtwpLogger+0x66
        85887dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 83670b98  Cid 0004.051c  Teb: 00000000 Win32Thread: 00000000 RUNNING on processor 0
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f14d90       Image:         System
        Wait Start TickCount      24268          Ticks: 19231 (0:00:05:00.005)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address SystemDump!BSODThread (0x9f659558)
        Stack Init 9f298000 Current 9f297ca0 Base 9f298000 Limit 9f295000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f297d54 9f6595a9 nt!KeBugCheckEx+0x1e
        9f297d7c 81e254e0 SystemDump!BSODThread+0x51 (FPO: [Non-Fpo]) (CONV: stdcall)
[c:\wddk\src\general\ctxbsod\sys\ctxbsod.c @ 115]
        9f297dc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16
```

Smss process

```
PROCESS 84d9f128  SessionId: none  Cid: 0164    Peb: 7ffd9000  ParentCid: 0004
    DirBase: 29a01020  ObjectTable: 882184c0  HandleCount:  28.
    Image: smss.exe
    VadRoot 84dc6468 Vads 15 Clone 0 Private 51. Modified 28. Locked 0.
    DeviceMap 85a03048
    Token                             873f2348
    ElapsedTime                       00:11:09.177
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         8648
    QuotaPoolUsage[NonPagedPool]      720
    Working Set Sizes (now,min,max)  (138, 50, 345) (552KB, 200KB, 1380KB)
    PeakWorkingSetSize                178
    VirtualSize                       4 Mb
    PeakVirtualSize                   14 Mb
    PageFaultCount                    262
    MemoryPriority                    BACKGROUND
    BasePriority                      11
    CommitCharge                      71

    Setting context for this process...
.process /p /r ffffffff84d9f128

    !peb
PEB at 7ffd9000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         47ce0000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 002717c0 . 002717c0
    Ldr.InLoadOrderModuleList:           00271740 . 002717b0
    Ldr.InMemoryOrderModuleList:         00271748 . 002717b8
            Base TimeStamp                     Module
        47ce0000 4549ad41 Nov 02 08:33:05 2006 \SystemRoot\System32\smss.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
    SubSystemData:     00000000
    ProcessHeap:       00270000
    ProcessParameters: 00270870
    WindowTitle:  '< Name not readable >'
    ImageFile:    '\SystemRoot\System32\smss.exe'
    CommandLine:  '\SystemRoot\System32\smss.exe'
    DllPath:      'C:\Windows\System32'
    Environment:  002707e8
        Path=C:\Windows\System32
        SystemDrive=C:
        SystemRoot=C:\Windows
```

```
        THREAD 84dbed78  Cid 0164.0168  Teb: 7ffdf000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            84d32d90  ProcessObject
            8983e1b0  ProcessObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            84d9f128       Image:         smss.exe
        Wait Start TickCount      792            Ticks: 42707 (0:00:11:06.233)
        Context Switch Count      394
        UserTime                  00:00:00.000
        KernelTime                00:00:00.046
        Win32 Start Address smss!NtProcessStartupW (0x47ced757)
        Stack Init 85d38000 Current 85d378d0 Base 85d38000 Limit 85d35000 Call 0
        Priority 13 BasePriority 11 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        85d378e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85d37924 81c28c64 nt!KiSwapThread+0x389
        85d37970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        85d37bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        85d37d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        85d37d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 85d37d64)
        0024fe20 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0024fe24 47ceb583 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0024febc 47ced73d smss!wmain+0x211 (FPO: [Non-Fpo])
        0024ff00 77446329 smss!NtProcessStartupW_AfterSecurityCookieInitialized+0x1fe (FPO: [Non-
Fpo])
        0024ff40 00000000 ntdll!_RtlUserThreadStart+0x35 (FPO: [Non-Fpo])

        THREAD 84881030  Cid 0164.01ac  Teb: 7ffde000 Win32Thread: 00000000 WAIT: (WrLpcReceive)
UserMode Non-Alertable
            84881244  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            84d9f128       Image:         smss.exe
        Wait Start TickCount      1000           Ticks: 42499 (0:00:11:02.988)
        Context Switch Count      9
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address smss!SmpCreateInitialSession (0x47ceb2a2)
        Stack Init 88ea1000 Current 88ea0b78 Base 88ea1000 Limit 88e9e000 Call 0
        Priority 12 BasePriority 11 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        88ea0b90 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        88ea0bcc 81c293a7 nt!KiSwapThread+0x389
        88ea0c2c 81dc3dac nt!KeWaitForSingleObject+0x414
        88ea0c64 81dc436e nt!AlpcpReceiveMessagePort+0x221
        88ea0ce0 81dc6211 nt!AlpcpReceiveMessage+0x163
        88ea0d3c 81c8caaa nt!NtAlpcSendWaitReceivePort+0x11c
        88ea0d3c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 88ea0d64)
        0045f6d8 7748f2c0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0045f6dc 47ce9f99 ntdll!NtAlpcSendWaitReceivePort+0xc (FPO: [8,0,0])
        0045f8a0 47ceb365 smss!SmpApiLoop+0x103 (FPO: [Non-Fpo])
        0045fa20 77446329 smss!SmpCreateInitialSession+0xc3 (FPO: [Non-Fpo])
        0045fa60 00000000 ntdll!_RtlUserThreadStart+0x35 (FPO: [Non-Fpo])
```

```
        THREAD 84d9e970  Cid 0164.01b8  Teb: 7ffdd000 Win32Thread: 00000000 WAIT: (WrLpcReceive)
UserMode Non-Alertable
            84d9eb84  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            84d9f128       Image:         smss.exe
        Wait Start TickCount      1000           Ticks: 42499 (0:00:11:02.988)
        Context Switch Count      11
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address smss!SmpApiLoop (0x47ce9e96)
        Stack Init 88e95000 Current 88e94b78 Base 88e95000 Limit 88e92000 Call 0
        Priority 12 BasePriority 11 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        88e94b90 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        88e94bcc 81c293a7 nt!KiSwapThread+0x389
        88e94c2c 81dc3dac nt!KeWaitForSingleObject+0x414
        88e94c64 81dc436e nt!AlpcpReceiveMessagePort+0x221
        88e94ce0 81dc6211 nt!AlpcpReceiveMessage+0x163
        88e94d3c 81c8caaa nt!NtAlpcSendWaitReceivePort+0x11c
        88e94d3c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 88e94d64)
        0015f60c 7748f2c0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0015f610 47ce9f99 ntdll!NtAlpcSendWaitReceivePort+0xc (FPO: [8,0,0])
        0015f7d4 77446329 smss!SmpApiLoop+0x103 (FPO: [Non-Fpo])
        0015f814 00000000 ntdll!_RtlUserThreadStart+0x35 (FPO: [Non-Fpo])

        THREAD 89940918  Cid 0164.01dc  Teb: 7ffdc000 Win32Thread: 00000000 WAIT: (WrLpcReceive)
UserMode Non-Alertable
            89940b2c  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            84d9f128       Image:         smss.exe
        Wait Start TickCount      1000           Ticks: 42499 (0:00:11:02.988)
        Context Switch Count      10
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address smss!SmpCreateInitialSession (0x47ceb2a2)
        Stack Init 88e85000 Current 88e84b78 Base 88e85000 Limit 88e82000 Call 0
        Priority 12 BasePriority 11 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        88e84b90 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        88e84bcc 81c293a7 nt!KiSwapThread+0x389
        88e84c2c 81dc3dac nt!KeWaitForSingleObject+0x414
        88e84c64 81dc436e nt!AlpcpReceiveMessagePort+0x221
        88e84ce0 81dc6211 nt!AlpcpReceiveMessage+0x163
        88e84d3c 81c8caaa nt!NtAlpcSendWaitReceivePort+0x11c
        88e84d3c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 88e84d64)
        0040fbe0 7748f2c0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0040fbe4 47ce9f99 ntdll!NtAlpcSendWaitReceivePort+0xc (FPO: [8,0,0])
        0040fda8 47ceb365 smss!SmpApiLoop+0x103 (FPO: [Non-Fpo])
        0040ff28 77446329 smss!SmpCreateInitialSession+0xc3 (FPO: [Non-Fpo])
        0040ff68 00000000 ntdll!_RtlUserThreadStart+0x35 (FPO: [Non-Fpo])
```

Csrss process (session 0)

```
PROCESS 84d32d90  SessionId: 0  Cid: 01bc    Peb: 7ffda000  ParentCid: 01b0
    DirBase: 29a01060  ObjectTable: 8b93dd78  HandleCount: 453.
    Image: csrss.exe
    VadRoot 8994edc8 Vads 99 Clone 0 Private 264. Modified 177. Locked 0.
    DeviceMap 85a03048
    Token                             8b9bf440
    ElapsedTime                       00:11:08.194
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.624
    QuotaPoolUsage[PagedPool]         179016
    QuotaPoolUsage[NonPagedPool]      4824
    Working Set Sizes (now,min,max)  (1029, 50, 345) (4116KB, 200KB, 1380KB)
    PeakWorkingSetSize                1222
    VirtualSize                       77 Mb
    PeakVirtualSize                   86 Mb
    PageFaultCount                    3178
    MemoryPriority                    BACKGROUND
    BasePriority                      13
    CommitCharge                      389

    Setting context for this process...
.process /p /r ffffffff84d32d90

    !peb
PEB at 7ffda000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         49dd0000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 004d1548 . 004ed3e0
    Ldr.InLoadOrderModuleList:           004d14c8 . 004ed3d0
    Ldr.InMemoryOrderModuleList:         004d14d0 . 004ed3d8
            Base TimeStamp                     Module
        49dd0000 4549ad3f Nov 02 08:33:03 2006 C:\Windows\system32\csrss.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75c40000 45dfad13 Feb 24 03:12:19 2007 C:\Windows\system32\CSRSRV.dll
        75c20000 4549bcb4 Nov 02 09:39:00 2006 C:\Windows\system32\basesrv.dll
        75bc0000 45dfad61 Feb 24 03:13:37 2007 C:\Windows\system32\winsrv.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\KERNEL32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        75a60000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\sxs.dll
    SubSystemData:     00000000
    ProcessHeap:       004d0000
    ProcessParameters: 004d0cd8
    WindowTitle:  '< Name not readable >'
    ImageFile:    'C:\Windows\system32\csrss.exe'
    CommandLine:  'C:\Windows\system32\csrss.exe ObjectDirectory=\Windows
SharedSection=1024,3072,512 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;C:\Program
Files\QuickTime\QTSystem\'
    Environment:  004d07e8
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        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;C:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\TEMP
        TMP=C:\Windows\TEMP
        USERNAME=SYSTEM
        windir=C:\Windows


        THREAD 89943398  Cid 01bc.01cc  Teb: 7ffde000 Win32Thread: ff502558 WAIT: (WrLpcReply)
UserMode Non-Alertable
            899435ac  Semaphore Limit 0x1
        Waiting for reply to ALPC Message a77ce2b8
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            84d32d90       Image:         csrss.exe
        Wait Start TickCount      8892           Ticks: 34607 (0:00:08:59.872)
        Context Switch Count      9
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address winsrv!TerminalServerRequestThread (0x75bcfc43)
        Stack Init 88e91000 Current 88e90b48 Base 88e91000 Limit 88e8e000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        88e90b60 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        88e90b9c 81c293a7 nt!KiSwapThread+0x389
        88e90bf8 81cc0275 nt!KeWaitForSingleObject+0x414
        88e90c20 81dc3818 nt!AlpcpSignalAndWait+0x7e
        88e90c44 81dc5c29 nt!AlpcpReceiveSynchronousReply+0x2b
        88e90ccc 81dbe18a nt!AlpcpProcessSynchronousRequest+0x201
        88e90d2c 81dbe324 nt!LpcpRequestWaitReplyPort+0x66
        88e90d50 81c8caaa nt!NtRequestWaitReplyPort+0x4c
        88e90d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 88e90d64)
        00d2f84c 77490190 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00d2f850 75bcfe80 ntdll!NtRequestWaitReplyPort+0xc (FPO: [3,0,0])
        00d2f9a4 77446329 winsrv!TerminalServerRequestThread+0x251 (FPO: [Non-Fpo])
        00d2f9e4 00000000 ntdll!_RtlUserThreadStart+0x35 (FPO: [Non-Fpo])
```

```
        THREAD 89939d78  Cid 01bc.01d0  Teb: 7ffdd000 Win32Thread: ff524e98 WAIT: (UserRequest)
UserMode Alertable
            84d344e0  SynchronizationEvent
            84d34678  SynchronizationEvent
            84d34648  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            84d32d90       Image:         csrss.exe
        Wait Start TickCount      1825           Ticks: 41674 (0:00:10:50.118)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address winsrv!NotificationThread (0x75bcb56b)
        Stack Init 88ec1000 Current 88ec08d0 Base 88ec1000 Limit 88ebe000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        88ec08e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        88ec0924 81c28c64 nt!KiSwapThread+0x389
        88ec0970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        88ec0bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        88ec0d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        88ec0d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 88ec0d64)
        00dcfbcc 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00dcfbd0 75bcb6ae ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00dcfe38 77446329 winsrv!NotificationThread+0x149 (FPO: [Non-Fpo])
        00dcfe78 00000000 ntdll!_RtlUserThreadStart+0x35 (FPO: [Non-Fpo])

        THREAD 8993f238  Cid 01bc.01d4  Teb: 7ffdc000 Win32Thread: ffa90ba8 WAIT: (WrLpcReceive)
UserMode Non-Alertable
            8993f44c  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            84d32d90       Image:         csrss.exe
        Wait Start TickCount      43448          Ticks: 51 (0:00:00:00.795)
        Context Switch Count      890
        UserTime                  00:00:00.046
        KernelTime                00:00:00.031
        Win32 Start Address CSRSRV!CsrApiRequestThread (0x75c4563d)
        Stack Init 88e1c000 Current 88e1bb78 Base 88e1c000 Limit 88e19000 Call 0
        Priority 15 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        88e1bb90 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        88e1bbcc 81c293a7 nt!KiSwapThread+0x389
        88e1bc2c 81dc3dac nt!KeWaitForSingleObject+0x414
        88e1bc64 81dc436e nt!AlpcpReceiveMessagePort+0x221
        88e1bce0 81dc6211 nt!AlpcpReceiveMessage+0x163
        88e1bd3c 81c8caaa nt!NtAlpcSendWaitReceivePort+0x11c
        88e1bd3c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 88e1bd64)
        00e2fcfc 7748f2c0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00e2fd00 75c45720 ntdll!NtAlpcSendWaitReceivePort+0xc (FPO: [8,0,0])
        00e2fe8c 77446329 CSRSRV!CsrApiRequestThread+0xe3 (FPO: [Non-Fpo])
        00e2fecc 00000000 ntdll!_RtlUserThreadStart+0x35 (FPO: [Non-Fpo])
```

```
        THREAD 89940030  Cid 01bc.01d8  Teb: 7ffdb000 Win32Thread: 00000000 WAIT: (WrLpcReceive)
UserMode Non-Alertable
            89940244  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            84d32d90       Image:         csrss.exe
        Wait Start TickCount      792            Ticks: 42707 (0:00:11:06.233)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address CSRSRV!CsrSbApiRequestThread (0x75c44530)
        Stack Init 88e20000 Current 88e1fb70 Base 88e20000 Limit 88e1d000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        88e1fb88 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        88e1fbc4 81c293a7 nt!KiSwapThread+0x389
        88e1fc24 81dc3dac nt!KeWaitForSingleObject+0x414
        88e1fc5c 81dc486e nt!AlpcpReceiveMessagePort+0x221
        88e1fcc4 81dbe7b6 nt!AlpcpReceiveLegacyMessage+0x197
        88e1fd30 81dbe69c nt!NtReplyWaitReceivePortEx+0x100
        88e1fd4c 81c8caaa nt!NtReplyWaitReceivePort+0x18
        88e1fd4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 88e1fd64)
        00effa80 77490140 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00effa84 75c44578 ntdll!ZwReplyWaitReceivePort+0xc (FPO: [4,0,0])
        00effbc4 77446329 CSRSRV!CsrSbApiRequestThread+0x48 (FPO: [Non-Fpo])
        00effc04 00000000 ntdll!_RtlUserThreadStart+0x35 (FPO: [Non-Fpo])

        THREAD 89941400  Cid 01bc.01f0  Teb: 7ffdf000 Win32Thread: ff452db8 WAIT: (WrLpcReceive)
UserMode Non-Alertable
            89941614  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            84d32d90       Image:         csrss.exe
        Wait Start TickCount      43413          Ticks: 86 (0:00:00:01.341)
        Context Switch Count      801
        UserTime                  00:00:00.046
        KernelTime                00:00:00.000
        Win32 Start Address CSRSRV!CsrApiRequestThread (0x75c4563d)
        Stack Init 88e08000 Current 88e07b78 Base 88e08000 Limit 88e05000 Call 0
        Priority 15 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        88e07b90 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        88e07bcc 81c293a7 nt!KiSwapThread+0x389
        88e07c2c 81dc3dac nt!KeWaitForSingleObject+0x414
        88e07c64 81dc436e nt!AlpcpReceiveMessagePort+0x221
        88e07ce0 81dc6211 nt!AlpcpReceiveMessage+0x163
        88e07d3c 81c8caaa nt!NtAlpcSendWaitReceivePort+0x11c
        88e07d3c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 88e07d64)
        0100f820 7748f2c0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0100f824 75c45720 ntdll!NtAlpcSendWaitReceivePort+0xc (FPO: [8,0,0])
        0100f9b0 77446329 CSRSRV!CsrApiRequestThread+0xe3 (FPO: [Non-Fpo])
        0100f9f0 00000000 ntdll!_RtlUserThreadStart+0x35 (FPO: [Non-Fpo])
```

```
        THREAD 8994d568  Cid 01bc.0204  Teb: 7ffd9000 Win32Thread: ffaa94f8 WAIT: (WrUserRequest)
KernelMode Alertable
            8994d4b8  SynchronizationEvent
            8994d408  NotificationTimer
            8994d3d8  SynchronizationTimer
            81d09fc0  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            84d32d90       Image:         csrss.exe
        Wait Start TickCount      43497          Ticks: 2 (0:00:00:00.031)
        Context Switch Count      35846
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address winsrv!StartCreateSystemThreads (0x75bcbde0)
        Stack Init 88e34000 Current 88e33c38 Base 88e34000 Limit 88e31000 Call 0
        Priority 15 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        88e33c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        88e33c8c 81c28c64 nt!KiSwapThread+0x389
        88e33cd8 8ce0861a nt!KeWaitForMultipleObjects+0x47d
        88e33d34 8ce05145 win32k!RawInputThread+0x474 (FPO: [Non-Fpo])
        88e33d48 8ced8d19 win32k!xxxCreateSystemThreads+0x4a (FPO: [Non-Fpo])
        88e33d58 81c8caaa win32k!NtUserCallNoParam+0x1b (FPO: [Non-Fpo])
        88e33d58 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 88e33d64)
        00fafd40 75bc612e ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00fafd44 75bcbdf2 winsrv!NtUserCallNoParam+0xc (FPO: [Non-Fpo])
        00fafd50 77446329 winsrv!StartCreateSystemThreads+0x12 (FPO: [Non-Fpo])
        00fafd90 00000000 ntdll!_RtlUserThreadStart+0x35 (FPO: [Non-Fpo])

        THREAD 8994d118  Cid 01bc.0208  Teb: 7ffd8000 Win32Thread: ffad1768 WAIT: (WrUserRequest)
UserMode Non-Alertable
            898466a8  SynchronizationEvent
            8994eff0  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            84d32d90       Image:         csrss.exe
        Wait Start TickCount      17260          Ticks: 26239 (0:00:06:49.331)
        Context Switch Count      24
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address winsrv!StartCreateSystemThreads (0x75bcbde0)
        Stack Init 88e40000 Current 88e3fbf8 Base 88e40000 Limit 88e3d000 Call 0
        Priority 15 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        88e3fc10 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        88e3fc4c 81c28c64 nt!KiSwapThread+0x389
        88e3fc9c 8ceb093b nt!KeWaitForMultipleObjects+0x47d
        88e3fcf4 8ce16737 win32k!xxxMsgWaitForMultipleObjects+0xcb (FPO: [Non-Fpo])
        88e3fd34 8ce0514f win32k!xxxDesktopThread+0x18f (FPO: [Non-Fpo])
        88e3fd48 8ced8d19 win32k!xxxCreateSystemThreads+0x54 (FPO: [Non-Fpo])
        88e3fd58 81c8caaa win32k!NtUserCallNoParam+0x1b (FPO: [Non-Fpo])
        88e3fd58 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 88e3fd64)
        0108fb28 75bc612e ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0108fb2c 75bcbdf2 winsrv!NtUserCallNoParam+0xc (FPO: [Non-Fpo])
        0108fb38 77446329 winsrv!StartCreateSystemThreads+0x12 (FPO: [Non-Fpo])
        0108fb78 00000000 ntdll!_RtlUserThreadStart+0x35 (FPO: [Non-Fpo])
```

```
        THREAD 89964470  Cid 01bc.0230  Teb: 7ffd7000 Win32Thread: ff4d0a78 WAIT: (WrLpcReceive)
UserMode Non-Alertable
            89964684  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            84d32d90       Image:         csrss.exe
        Wait Start TickCount      43411          Ticks: 88 (0:00:00:01.372)
        Context Switch Count      796
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address CSRSRV!CsrApiRequestThread (0x75c4563d)
        Stack Init 9e9c8000 Current 9e9c7b78 Base 9e9c8000 Limit 9e9c5000 Call 0
        Priority 15 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9e9c7b90 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e9c7bcc 81c293a7 nt!KiSwapThread+0x389
        9e9c7c2c 81dc3dac nt!KeWaitForSingleObject+0x414
        9e9c7c64 81dc436e nt!AlpcpReceiveMessagePort+0x221
        9e9c7ce0 81dc6211 nt!AlpcpReceiveMessage+0x163
        9e9c7d3c 81c8caaa nt!NtAlpcSendWaitReceivePort+0x11c
        9e9c7d3c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9e9c7d64)
        0464f6e4 7748f2c0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0464f6e8 75c45720 ntdll!NtAlpcSendWaitReceivePort+0xc (FPO: [8,0,0])
        0464f874 77446329 CSRSRV!CsrApiRequestThread+0xe3 (FPO: [Non-Fpo])
        0464f8b4 00000000 ntdll!_RtlUserThreadStart+0x35 (FPO: [Non-Fpo])

        THREAD 89967030  Cid 01bc.0234  Teb: 7ffd6000 Win32Thread: ff41c848 WAIT: (WrUserRequest)
UserMode Non-Alertable
            89964350  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            84d32d90       Image:         csrss.exe
        Wait Start TickCount      807            Ticks: 42692 (0:00:11:05.999)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address winsrv!StartCreateSystemThreads (0x75bcbde0)
        Stack Init 9e9c4000 Current 9e9c3bf8 Base 9e9c4000 Limit 9e9c1000 Call 0
        Priority 12 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9e9c3c10 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e9c3c4c 81c28c64 nt!KiSwapThread+0x389
        9e9c3c9c 8ceb093b nt!KeWaitForMultipleObjects+0x47d
        9e9c3cf4 8ce16737 win32k!xxxMsgWaitForMultipleObjects+0xcb (FPO: [Non-Fpo])
        9e9c3d34 8ce0514f win32k!xxxDesktopThread+0x18f (FPO: [Non-Fpo])
        9e9c3d48 8ced8d19 win32k!xxxCreateSystemThreads+0x54 (FPO: [Non-Fpo])
        9e9c3d58 81c8caaa win32k!NtUserCallNoParam+0x1b (FPO: [Non-Fpo])
        9e9c3d58 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9e9c3d64)
        00d7fb64 75bc612e ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00d7fb68 75bcbdf2 winsrv!NtUserCallNoParam+0xc (FPO: [Non-Fpo])
        00d7fb74 77446329 winsrv!StartCreateSystemThreads+0x12 (FPO: [Non-Fpo])
        00d7fbb4 00000000 ntdll!_RtlUserThreadStart+0x35 (FPO: [Non-Fpo])
```

```
        THREAD 89967c28  Cid 01bc.0238  Teb: 7ffd5000 Win32Thread: ff41c4e8 WAIT: (WrUserRequest)
UserMode Non-Alertable
            89967b78  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            84d32d90       Image:         csrss.exe
        Wait Start TickCount      808            Ticks: 42691 (0:00:11:05.983)
        Context Switch Count      7
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address winsrv!ConsoleInputThread (0x75bc2f42)
        Stack Init 85d14000 Current 85d13b68 Base 85d14000 Limit 85d11000 Call 0
        Priority 13 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        85d13b80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85d13bbc 81c293a7 nt!KiSwapThread+0x389
        85d13c18 8cedb8ed nt!KeWaitForSingleObject+0x414
        85d13c74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        85d13c90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        85d13ce8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        85d13d4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        85d13d4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 85d13d64)
        0047f9f0 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0047f9f4 761e19cd USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        0047fa10 75bc306e USER32!GetMessageW+0x33 (FPO: [Non-Fpo])
        0047fa7c 77446329 winsrv!ConsoleInputThread+0x21c (FPO: [Non-Fpo])
        0047fabc 00000000 ntdll!_RtlUserThreadStart+0x35 (FPO: [Non-Fpo])
```

Wininit process

```
PROCESS 8983e1b0  SessionId: 0  Cid: 01e8    Peb: 7ffd8000  ParentCid: 01b0
    DirBase: 29a010a0  ObjectTable: 873da8b8  HandleCount:  98.
    Image: wininit.exe
    VadRoot 899585d0 Vads 55 Clone 0 Private 260. Modified 118. Locked 3.
    DeviceMap 85a03048
    Token                             89c7adb0
    ElapsedTime                       00:11:07.164
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.046
    QuotaPoolUsage[PagedPool]         57080
    QuotaPoolUsage[NonPagedPool]      4304
    Working Set Sizes (now,min,max)  (795, 50, 345) (3180KB, 200KB, 1380KB)
    PeakWorkingSetSize                993
    VirtualSize                       26 Mb
    PeakVirtualSize                   51 Mb
    PageFaultCount                    1640
    MemoryPriority                    BACKGROUND
    BasePriority                      13
    CommitCharge                      328

    Setting context for this process...
.process /p /r ffffffff8983e1b0

    !peb
PEB at 7ffd8000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00f80000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 001d1348 . 001f1c18
    Ldr.InLoadOrderModuleList:           001d12c8 . 001f1ce8
    Ldr.InMemoryOrderModuleList:         001d12d0 . 001f1cf0
            Base TimeStamp                     Module
          f80000 4549aff9 Nov 02 08:44:41 2006 C:\Windows\system32\wininit.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        75ba0000 4549bde2 Nov 02 09:44:02 2006 C:\Windows\system32\USERENV.dll
        75b80000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\Secur32.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        75b20000 4549bcaf Nov 02 09:38:55 2006 C:\Windows\system32\apphelp.dll
        75fe0000 4549be0e Nov 02 09:44:46 2006 C:\Windows\system32\WS2_32.dll
        77550000 4549bdc7 Nov 02 09:43:35 2006 C:\Windows\system32\NSI.dll
        75250000 4549bd69 Nov 02 09:42:01 2006 C:\Windows\system32\mswsock.dll
        752c0000 4549be27 Nov 02 09:45:11 2006 C:\Windows\System32\wshtcpip.dll
        752b0000 4549be21 Nov 02 09:45:05 2006 C:\Windows\System32\wship6.dll
        75480000 4549bd20 Nov 02 09:40:48 2006 C:\Windows\system32\credssp.dll
        75650000 45b96fde Jan 26 03:05:02 2007 C:\Windows\system32\CRYPT32.dll
        75820000 4549bd41 Nov 02 09:41:21 2006 C:\Windows\system32\MSASN1.dll
        75050000 46773a78 Jun 19 03:07:52 2007 C:\Windows\system32\schannel.dll
        75840000 4549bd53 Nov 02 09:41:39 2006 C:\Windows\system32\NETAPI32.dll
        75ce0000 4549bd99 Nov 02 09:42:49 2006 C:\Windows\system32\PSAPI.DLL
    SubSystemData:     00000000
    ProcessHeap:       001d0000
    ProcessParameters: 001d0cd8
    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;C:\Program
Files\QuickTime\QTSystem\'
    Environment:  001f5f08
        ALLUSERSPROFILE=C:\ProgramData
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        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;C:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        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 899429f8  Cid 01e8.01ec  Teb: 7ffdf000 Win32Thread: ffabbe98 WAIT: (UserRequest)
UserMode Non-Alertable
            89955840  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            8983e1b0       Image:         wininit.exe
        Wait Start TickCount      824            Ticks: 42675 (0:00:11:05.734)
        Context Switch Count      339
        UserTime                  00:00:00.031
        KernelTime                00:00:00.140
        Win32 Start Address wininit!WinMainCRTStartup (0x00f85c70)
        Stack Init 88e14000 Current 88e13c38 Base 88e14000 Limit 88e11000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        88e13c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        88e13c8c 81c293a7 nt!KiSwapThread+0x389
        88e13ce8 81df5057 nt!KeWaitForSingleObject+0x414
        88e13d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        88e13d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 88e13d64)
        0009fcf8 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0009fcfc 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0009fd6c 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        0009fd80 00f82b8a kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0009fd90 00f825ca wininit!WaitForShutdown+0x14 (FPO: [Non-Fpo])
        0009fdf4 00f85dd9 wininit!WinMain+0x962 (FPO: [Non-Fpo])
        0009fe84 75f33833 wininit!_initterm_e+0x1a1 (FPO: [Non-Fpo])
        0009fe90 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0009fed0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 8995e788  Cid 01e8.021c  Teb: 7ffdb000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            8995ea30  SynchronizationTimer
            89956238  ProcessObject
            8995e4a0  ProcessObject
            8995ab30  ProcessObject
            89999020  SynchronizationTimer
            89999ee8  SynchronizationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            8983e1b0       Image:         wininit.exe
        Wait Start TickCount      1466           Ticks: 42033 (0:00:10:55.719)
        Context Switch Count      7
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x7744b49a)
        Stack Init 88e44000 Current 88e438d0 Base 88e44000 Limit 88e41000 Call 0
        Priority 15 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        88e438e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        88e43924 81c28c64 nt!KiSwapThread+0x389
        88e43970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        88e43bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        88e43d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        88e43d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 88e43d64)
        0132fc3c 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0132fc40 7744b65b ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0132fddc 75f33833 ntdll!TppWaiterpThread+0x294 (FPO: [Non-Fpo])
        0132fde8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0132fe28 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9e1cc710  Cid 01e8.085c  Teb: 7ffdd000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            84873238  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            8983e1b0       Image:         wininit.exe
        Wait Start TickCount      6773           Ticks: 36726 (0:00:09:32.929)
        Context Switch Count      6
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init a1e82000 Current a1e81bc8 Base a1e82000 Limit a1e7f000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1e81be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1e81c1c 81cad431 nt!KiSwapThread+0x389
        a1e81c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a1e81cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a1e81d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a1e81d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1e81d64)
        00f7fbc0 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00f7fbc4 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        00f7fbf0 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        00f7fc2c 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        00f7fc98 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        00f7fca4 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        00f7fccc 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        00f7fcd8 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        00f7fce4 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00f7fd24 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Csrss process (session 1)

```
PROCESS 84d33020  SessionId: 1  Cid: 01f4    Peb: 7ffd8000  ParentCid: 01e0
    DirBase: 29a01040  ObjectTable: 89ca7ea8  HandleCount: 316.
    Image: csrss.exe
    VadRoot 899aa4a0 Vads 93 Clone 0 Private 249. Modified 285. Locked 0.
    DeviceMap 85a03048
    Token                             8b9bfdb0
    ElapsedTime                       00:11:07.164
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.421
    QuotaPoolUsage[PagedPool]         175936
    QuotaPoolUsage[NonPagedPool]      7816
    Working Set Sizes (now,min,max)  (1448, 50, 345) (5792KB, 200KB, 1380KB)
    PeakWorkingSetSize                4333
    VirtualSize                       78 Mb
    PeakVirtualSize                   139 Mb
    PageFaultCount                    15970
    MemoryPriority                    BACKGROUND
    BasePriority                      13
    CommitCharge                      388

    Setting context for this process...
.process /p /r ffffffff84d33020

    !peb
PEB at 7ffd8000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         49dd0000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 002d1548 . 002ebe98
    Ldr.InLoadOrderModuleList:           002d14c8 . 002ebe88
    Ldr.InMemoryOrderModuleList:         002d14d0 . 002ebe90
            Base TimeStamp                     Module
        49dd0000 4549ad3f Nov 02 08:33:03 2006 C:\Windows\system32\csrss.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75c40000 45dfad13 Feb 24 03:12:19 2007 C:\Windows\system32\CSRSRV.dll
        75c20000 4549bcb4 Nov 02 09:39:00 2006 C:\Windows\system32\basesrv.dll
        75bc0000 45dfad61 Feb 24 03:13:37 2007 C:\Windows\system32\winsrv.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\KERNEL32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        75a60000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\sxs.dll
    SubSystemData:     00000000
    ProcessHeap:       002d0000
    ProcessParameters: 002d0cd8
    WindowTitle:  '< Name not readable >'
    ImageFile:    'C:\Windows\system32\csrss.exe'
    CommandLine:  'C:\Windows\system32\csrss.exe ObjectDirectory=\Windows
SharedSection=1024,3072,512 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;C:\Program
Files\QuickTime\QTSystem\'
    Environment:  002d07e8
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        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;C:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\TEMP
        TMP=C:\Windows\TEMP
        USERNAME=SYSTEM
        windir=C:\Windows


        THREAD 89979aa0  Cid 01f4.0244  Teb: 00000000 Win32Thread: 00000000 WAIT: (Executive)
KernelMode Non-Alertable
            8996c390  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            84d33020       Image:         csrss.exe
        Wait Start TickCount      18552          Ticks: 24947 (0:00:06:29.175)
        Context Switch Count      4656
        UserTime                  00:00:00.000
        KernelTime                00:00:00.234
        Win32 Start Address cdd!PresentWorkerThread (0x9e61309e)
        Stack Init 9e9dc000 Current 9e9dbc10 Base 9e9dc000 Limit 9e9d9000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9e9dbc28 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e9dbc64 81c293a7 nt!KiSwapThread+0x389
        9e9dbcc4 9e613470 nt!KeWaitForSingleObject+0x414
        9e9dbd7c 81e254e0 cdd!PresentWorkerThread+0x3d2 (FPO: [Non-Fpo])
        9e9dbdc0 81c9159e nt!PspSystemThreadStartup+0x9d
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 899550d0  Cid 01f4.0258  Teb: 7ffde000 Win32Thread: ff34ad80 WAIT: (WrLpcReply)
UserMode Non-Alertable
            899552e4  Semaphore Limit 0x1
        Waiting for reply to ALPC Message a9b46b78
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            84d33020       Image:         csrss.exe
        Wait Start TickCount      14133          Ticks: 29366 (0:00:07:38.112)
        Context Switch Count      35
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address winsrv!TerminalServerRequestThread (0x75bcfc43)
        Stack Init 9e9d0000 Current 9e9cfb48 Base 9e9d0000 Limit 9e9cd000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9e9cfb60 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e9cfb9c 81c293a7 nt!KiSwapThread+0x389
        9e9cfbf8 81cc0275 nt!KeWaitForSingleObject+0x414
        9e9cfc20 81dc3818 nt!AlpcpSignalAndWait+0x7e
        9e9cfc44 81dc5c29 nt!AlpcpReceiveSynchronousReply+0x2b
        9e9cfccc 81dbe18a nt!AlpcpProcessSynchronousRequest+0x201
        9e9cfd2c 81dbe324 nt!LpcpRequestWaitReplyPort+0x66
        9e9cfd50 81c8caaa nt!NtRequestWaitReplyPort+0x4c
        9e9cfd50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9e9cfd64)
        0093fb20 77490190 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0093fb24 75bcfe80 ntdll!NtRequestWaitReplyPort+0xc (FPO: [3,0,0])
        0093fc78 77446329 winsrv!TerminalServerRequestThread+0x251 (FPO: [Non-Fpo])
        0093fcb8 00000000 ntdll!_RtlUserThreadStart+0x35 (FPO: [Non-Fpo])
```

```
        THREAD 89999a70  Cid 01f4.025c  Teb: 7ffdd000 Win32Thread: ff357968 WAIT: (UserRequest)
UserMode Alertable
            84881980  SynchronizationEvent
            8993edd8  SynchronizationEvent
            84d9ec40  SynchronizationEvent
            89999e20  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            84d33020       Image:         csrss.exe
        Wait Start TickCount      9156           Ticks: 34343 (0:00:08:55.754)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address winsrv!NotificationThread (0x75bcb56b)
        Stack Init 88e3c000 Current 88e3b8d0 Base 88e3c000 Limit 88e39000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        88e3b8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        88e3b924 81c28c64 nt!KiSwapThread+0x389
        88e3b970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        88e3bbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        88e3bd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        88e3bd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 88e3bd64)
        0024f8c4 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0024f8c8 75bcb6ae ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0024fb30 77446329 winsrv!NotificationThread+0x149 (FPO: [Non-Fpo])
        0024fb70 00000000 ntdll!_RtlUserThreadStart+0x35 (FPO: [Non-Fpo])

        THREAD 899ab030  Cid 01f4.0264  Teb: 7ffdc000 Win32Thread: ffa91ba8 WAIT: (WrLpcReceive)
UserMode Non-Alertable
            899ab244  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            84d33020       Image:         csrss.exe
        Wait Start TickCount      40753          Ticks: 2746 (0:00:00:42.837)
        Context Switch Count      1002
        UserTime                  00:00:00.124
        KernelTime                00:00:00.062
        Win32 Start Address CSRSRV!CsrApiRequestThread (0x75c4563d)
        Stack Init 9e9fc000 Current 9e9fbb78 Base 9e9fc000 Limit 9e9f9000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9e9fbb90 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e9fbbcc 81c293a7 nt!KiSwapThread+0x389
        9e9fbc2c 81dc3dac nt!KeWaitForSingleObject+0x414
        9e9fbc64 81dc436e nt!AlpcpReceiveMessagePort+0x221
        9e9fbce0 81dc6211 nt!AlpcpReceiveMessage+0x163
        9e9fbd3c 81c8caaa nt!NtAlpcSendWaitReceivePort+0x11c
        9e9fbd3c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9e9fbd64)
        01a6f62c 7748f2c0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01a6f630 75c45720 ntdll!NtAlpcSendWaitReceivePort+0xc (FPO: [8,0,0])
        01a6f7bc 77446329 CSRSRV!CsrApiRequestThread+0xe3 (FPO: [Non-Fpo])
        01a6f7fc 00000000 ntdll!_RtlUserThreadStart+0x35 (FPO: [Non-Fpo])
```

```
        THREAD 899991b0  Cid 01f4.026c  Teb: 7ffdb000 Win32Thread: 00000000 WAIT: (WrLpcReceive)
UserMode Non-Alertable
            899993c4  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            84d33020       Image:         csrss.exe
        Wait Start TickCount      864            Ticks: 42635 (0:00:11:05.110)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address CSRSRV!CsrSbApiRequestThread (0x75c44530)
        Stack Init 88e2c000 Current 88e2bb70 Base 88e2c000 Limit 88e29000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        88e2bb88 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        88e2bbc4 81c293a7 nt!KiSwapThread+0x389
        88e2bc24 81dc3dac nt!KeWaitForSingleObject+0x414
        88e2bc5c 81dc486e nt!AlpcpReceiveMessagePort+0x221
        88e2bcc4 81dbe7b6 nt!AlpcpReceiveLegacyMessage+0x197
        88e2bd30 81dbe69c nt!NtReplyWaitReceivePortEx+0x100
        88e2bd4c 81c8caaa nt!NtReplyWaitReceivePort+0x18
        88e2bd4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 88e2bd64)
        008efa7c 77490140 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        008efa80 75c44578 ntdll!ZwReplyWaitReceivePort+0xc (FPO: [4,0,0])
        008efbc0 77446329 CSRSRV!CsrSbApiRequestThread+0x48 (FPO: [Non-Fpo])
        008efc00 00000000 ntdll!_RtlUserThreadStart+0x35 (FPO: [Non-Fpo])

        THREAD 9e1e7030  Cid 01f4.029c  Teb: 7ffdf000 Win32Thread: ff77e330 WAIT: (WrLpcReceive)
UserMode Non-Alertable
            9e1e7244  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            84d33020       Image:         csrss.exe
        Wait Start TickCount      42676          Ticks: 823 (0:00:00:12.838)
        Context Switch Count      910
        UserTime                  00:00:00.093
        KernelTime                00:00:00.046
        Win32 Start Address CSRSRV!CsrApiRequestThread (0x75c4563d)
        Stack Init 88ebd000 Current 88ebcb78 Base 88ebd000 Limit 88eba000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        88ebcb90 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        88ebcbcc 81c293a7 nt!KiSwapThread+0x389
        88ebcc2c 81dc3dac nt!KeWaitForSingleObject+0x414
        88ebcc64 81dc436e nt!AlpcpReceiveMessagePort+0x221
        88ebcce0 81dc6211 nt!AlpcpReceiveMessage+0x163
        88ebcd3c 81c8caaa nt!NtAlpcSendWaitReceivePort+0x11c
        88ebcd3c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 88ebcd64)
        01ccfbac 7748f2c0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01ccfbb0 75c45720 ntdll!NtAlpcSendWaitReceivePort+0xc (FPO: [8,0,0])
        01ccfd3c 77446329 CSRSRV!CsrApiRequestThread+0xe3 (FPO: [Non-Fpo])
        01ccfd7c 00000000 ntdll!_RtlUserThreadStart+0x35 (FPO: [Non-Fpo])
```

```
        THREAD 899eaaa8  Cid 01f4.02a4  Teb: 7ffda000 Win32Thread: ffabde28 WAIT: (WrUserRequest)
KernelMode Alertable
            84dc6298  SynchronizationEvent
            899ea928  NotificationTimer
            899ea8f8  SynchronizationTimer
            899be928  SynchronizationEvent
        IRP List:
            83a20d00: (0006,01fc) Flags: 00060970  Mdl: 00000000
            8371a6f0: (0006,01d8) Flags: 00060900  Mdl: 83697008
            84d321e8: (0006,01d8) Flags: 00060970  Mdl: 00000000
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            84d33020       Image:         csrss.exe
        Wait Start TickCount      43499          Ticks: 0
        Context Switch Count      157620
        UserTime                  00:00:00.000
        KernelTime                00:00:00.327
        Win32 Start Address winsrv!StartCreateSystemThreads (0x75bcbde0)
        Stack Init 85d34000 Current 85d33c38 Base 85d34000 Limit 85d31000 Call 0
        Priority 15 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        85d33c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85d33c8c 81c28c64 nt!KiSwapThread+0x389
        85d33cd8 8ce0861a nt!KeWaitForMultipleObjects+0x47d
        85d33d34 8ce05145 win32k!RawInputThread+0x474 (FPO: [Non-Fpo])
        85d33d48 8ced8d19 win32k!xxxCreateSystemThreads+0x4a (FPO: [Non-Fpo])
        85d33d58 81c8caaa win32k!NtUserCallNoParam+0x1b (FPO: [Non-Fpo])
        85d33d58 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 85d33d64)
        01d2f9b4 75bc612e ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01d2f9b8 75bcbdf2 winsrv!NtUserCallNoParam+0xc (FPO: [Non-Fpo])
        01d2f9c4 77446329 winsrv!StartCreateSystemThreads+0x12 (FPO: [Non-Fpo])
        01d2fa04 00000000 ntdll!_RtlUserThreadStart+0x35 (FPO: [Non-Fpo])

        THREAD 899b4630  Cid 01f4.02a8  Teb: 7ffd9000 Win32Thread: ffac2c78 WAIT: (WrUserRequest)
UserMode Non-Alertable
            9e1e6ac8  SynchronizationEvent
            9e1ddac0  SynchronizationEvent
        IRP List:
            8371d710: (0006,02d4) Flags: 00060970  Mdl: 00000000
            899c1008: (0006,01d8) Flags: 00060970  Mdl: 00000000
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            84d33020       Image:         csrss.exe
        Wait Start TickCount      25627          Ticks: 17872 (0:00:04:38.804)
        Context Switch Count      4310
        UserTime                  00:00:00.000
        KernelTime                00:00:00.187
        Win32 Start Address winsrv!StartCreateSystemThreads (0x75bcbde0)
        Stack Init 9e990000 Current 9e98fbf8 Base 9e990000 Limit 9e98d000 Call 0
        Priority 15 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9e98fc10 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e98fc4c 81c28c64 nt!KiSwapThread+0x389
        9e98fc9c 8ceb093b nt!KeWaitForMultipleObjects+0x47d
        9e98fcf4 8ce16737 win32k!xxxMsgWaitForMultipleObjects+0xcb (FPO: [Non-Fpo])
        9e98fd34 8ce0514f win32k!xxxDesktopThread+0x18f (FPO: [Non-Fpo])
        9e98fd48 8ced8d19 win32k!xxxCreateSystemThreads+0x54 (FPO: [Non-Fpo])
        9e98fd58 81c8caaa win32k!NtUserCallNoParam+0x1b (FPO: [Non-Fpo])
        9e98fd58 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9e98fd64)
        01c2fad8 75bc612e ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01c2fadc 75bcbdf2 winsrv!NtUserCallNoParam+0xc (FPO: [Non-Fpo])
        01c2fae8 77446329 winsrv!StartCreateSystemThreads+0x12 (FPO: [Non-Fpo])
        01c2fb28 00000000 ntdll!_RtlUserThreadStart+0x35 (FPO: [Non-Fpo])
```

```
        THREAD 836053c8  Cid 01f4.0b34  Teb: 7ffd7000 Win32Thread: ff375840 WAIT: (WrLpcReceive)
UserMode Non-Alertable
            836055dc  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            84d33020       Image:         csrss.exe
        Wait Start TickCount      42703          Ticks: 796 (0:00:00:12.417)
        Context Switch Count      841
        UserTime                  00:00:00.062
        KernelTime                00:00:00.062
        Win32 Start Address CSRSRV!CsrApiRequestThread (0x75c4563d)
        Stack Init 9e8bb000 Current 9e8bab78 Base 9e8bb000 Limit 9e8b8000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9e8bab90 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e8babcc 81c293a7 nt!KiSwapThread+0x389
        9e8bac2c 81dc3dac nt!KeWaitForSingleObject+0x414
        9e8bac64 81dc436e nt!AlpcpReceiveMessagePort+0x221
        9e8bace0 81dc6211 nt!AlpcpReceiveMessage+0x163
        9e8bad3c 81c8caaa nt!NtAlpcSendWaitReceivePort+0x11c
        9e8bad3c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9e8bad64)
        052afb4c 7748f2c0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        052afb50 75c45720 ntdll!NtAlpcSendWaitReceivePort+0xc (FPO: [8,0,0])
        052afcdc 77446329 CSRSRV!CsrApiRequestThread+0xe3 (FPO: [Non-Fpo])
        052afd1c 00000000 ntdll!_RtlUserThreadStart+0x35 (FPO: [Non-Fpo])
```

Services process

```
PROCESS 89956238  SessionId: 0  Cid: 0214    Peb: 7ffde000  ParentCid: 01e8
    DirBase: 29a010c0  ObjectTable: 89d1ade0  HandleCount: 231.
    Image: services.exe
    VadRoot 899b70e0 Vads 68 Clone 0 Private 516. Modified 134. Locked 2.
    DeviceMap 85a03048
    Token                             89d1c840
    ElapsedTime                       00:11:07.024
    UserTime                          00:00:00.187
    KernelTime                        00:00:01.092
    QuotaPoolUsage[PagedPool]         58848
    QuotaPoolUsage[NonPagedPool]      7112
    Working Set Sizes (now,min,max)  (1118, 50, 345) (4472KB, 200KB, 1380KB)
    PeakWorkingSetSize                1320
    VirtualSize                       27 Mb
    PeakVirtualSize                   32 Mb
    PageFaultCount                    5637
    MemoryPriority                    BACKGROUND
    BasePriority                      9
    CommitCharge                      623

    Setting context for this process...
.process /p /r ffffffff89956238

    !peb
PEB at 7ffde000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00850000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00241620 . 00258748
    Ldr.InLoadOrderModuleList:           002415a0 . 00258738
    Ldr.InMemoryOrderModuleList:         002415a8 . 00258740
            Base TimeStamp                     Module
          850000 4549add1 Nov 02 08:35:29 2006 C:\Windows\system32\services.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        75ba0000 4549bde2 Nov 02 09:44:02 2006 C:\Windows\system32\USERENV.dll
        75b80000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\Secur32.dll
        757d0000 4549bdb2 Nov 02 09:43:14 2006 C:\Windows\system32\SCESRV.dll
        757b0000 4549bccf Nov 02 09:39:27 2006 C:\Windows\system32\AUTHZ.dll
        75840000 4549bd53 Nov 02 09:41:39 2006 C:\Windows\system32\NETAPI32.dll
        75ce0000 4549bd99 Nov 02 09:42:49 2006 C:\Windows\system32\PSAPI.DLL
        75b50000 4549bd46 Nov 02 09:41:26 2006 C:\Windows\system32\NCObjAPI.DLL
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        75480000 4549bd20 Nov 02 09:40:48 2006 C:\Windows\system32\credssp.dll
        75650000 45b96fde Jan 26 03:05:02 2007 C:\Windows\system32\CRYPT32.dll
        75820000 4549bd41 Nov 02 09:41:21 2006 C:\Windows\system32\MSASN1.dll
        75050000 46773a78 Jun 19 03:07:52 2007 C:\Windows\system32\schannel.dll
        75b20000 4549bcaf Nov 02 09:38:55 2006 C:\Windows\system32\apphelp.dll
        75020000 4549bddb Nov 02 09:43:55 2006 C:\Windows\system32\NTMARTA.DLL
        76310000 4549be44 Nov 02 09:45:40 2006 C:\Windows\system32\WLDAP32.dll
        75fe0000 4549be0e Nov 02 09:44:46 2006 C:\Windows\system32\WS2_32.dll
        77550000 4549bdc7 Nov 02 09:43:35 2006 C:\Windows\system32\NSI.dll
        75ad0000 4549bda8 Nov 02 09:43:04 2006 C:\Windows\system32\SAMLIB.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
```

```
        75250000 4549bd69 Nov 02 09:42:01 2006 C:\Windows\system32\mswsock.dll
        752c0000 4549be27 Nov 02 09:45:11 2006 C:\Windows\System32\wshtcpip.dll
        752b0000 4549be21 Nov 02 09:45:05 2006 C:\Windows\System32\wship6.dll
    SubSystemData:     00000000
    ProcessHeap:       00240000
    ProcessParameters: 00240ea8
    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;C:\Program Files\QuickTime\QTSystem\'
    Environment:  002407e8
        ALLUSERSPROFILE=C:\ProgramData
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        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;C:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        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 9e1de030  Cid 0214.02b0  Teb: 7ffdd000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            9e1deda0  SynchronizationTimer
            899b8d20  SynchronizationEvent
            9e1f2020  ProcessObject
            9e1fd468  ProcessObject
            9fc4a020  ProcessObject
            8485e910  ProcessObject
            9fc38a48  ProcessObject
            9fc3dd90  ProcessObject
            9fc70d90  ProcessObject
            9fc9c020  ProcessObject
            9fcb2858  ProcessObject
            9fd42790  ProcessObject
            9fd50418  ProcessObject
            89870020  ProcessObject
            89871718  ProcessObject
            89877258  ProcessObject
            89881d28  ProcessObject
            9fde0020  ProcessObject
            a18b73a0  ProcessObject
            a18bd670  ProcessObject
            8997fb18  NotificationEvent
            83a0bc70  ProcessObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            89956238       Image:         services.exe
        Wait Start TickCount      14192          Ticks: 29307 (0:00:07:37.192)
        Context Switch Count      33
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x7744b49a)
        Stack Init 9e994000 Current 9e9938d0 Base 9e994000 Limit 9e991000 Call 0
        Priority 11 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9e9938e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e993924 81c28c64 nt!KiSwapThread+0x389
        9e993970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9e993bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9e993d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9e993d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9e993d64)
        00d6f848 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00d6f84c 7744b65b ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00d6f9e8 75f33833 ntdll!TppWaiterpThread+0x294 (FPO: [Non-Fpo])
        00d6f9f4 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00d6fa34 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 898559c0  Cid 0214.0878  Teb: 7ffdf000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Alertable
            9e1fa280  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            89956238       Image:         services.exe
        Wait Start TickCount      3983           Ticks: 39516 (0:00:10:16.453)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init a0360000 Current a035fbc8 Base a0360000 Limit a035d000 Call 0
        Priority 10 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a035fbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a035fc1c 81cad431 nt!KiSwapThread+0x389
        a035fc68 81d8b982 nt!KeRemoveQueueEx+0x568
        a035fcc0 81c7a036 nt!IoRemoveIoCompletion+0x23
        a035fd54 81c8caaa nt!NtWaitForWorkViaWorkerFactory+0x1a1
        a035fd54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a035fd64)
        00dffdf0 77490850 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00dffdf4 7749a1b4 ntdll!NtWaitForWorkViaWorkerFactory+0xc (FPO: [2,0,0])
        00dfff1c 75f33833 ntdll!TppWorkerThread+0x1f6 (FPO: [Non-Fpo])
        00dfff28 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00dfff68 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 83583030  Cid 0214.09e4  Teb: 7ffda000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            8356bc68  NotificationEvent
            83583ff0  NotificationEvent
        IRP List:
            9e1cb820: (0006,0094) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            89956238       Image:         services.exe
        Wait Start TickCount      7707           Ticks: 35792 (0:00:09:18.358)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address NCObjAPI!CNamedPipeClient::CallbackListenThreadProc (0x75b55515)
        Stack Init a1a7f000 Current a1a7e8d0 Base a1a7f000 Limit a1a7c000 Call 0
        Priority 11 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1a7e8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1a7e924 81c28c64 nt!KiSwapThread+0x389
        a1a7e970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1a7ebfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1a7ed48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1a7ed48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1a7ed64)
        00f3f2b4 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00f3f2b8 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00f3f354 75b555a8 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        00f3fbb4 75f33833 NCObjAPI!CNamedPipeClient::CallbackListenThreadProc+0x8f (FPO: [Non-Fpo])
        00f3fbc0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00f3fc00 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD a190fd78  Cid 0214.09e8  Teb: 7ffd9000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9e1e8ac8  NotificationEvent
            89944b10  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            89956238       Image:         services.exe
        Wait Start TickCount      18403          Ticks: 25096 (0:00:06:31.500)
        Context Switch Count      24
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address NCObjAPI!CConnection::SendThreadProc (0x75b51905)
        Stack Init 9e8b7000 Current 9e8b68d0 Base 9e8b7000 Limit 9e8b4000 Call 0
        Priority 10 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9e8b68e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e8b6924 81c28c64 nt!KiSwapThread+0x389
        9e8b6970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9e8b6bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9e8b6d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9e8b6d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9e8b6d64)
        00f8f90c 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00f8f910 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00f8f9ac 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        00f8f9c8 75b51969 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        00f8fa28 75f33833 NCObjAPI!CConnection::SendThreadProc+0x64 (FPO: [Non-Fpo])
        00f8fa34 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00f8fa74 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 8372ad38  Cid 0214.012c  Teb: 7ffdb000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            899c7140  QueueObject
            8372adc0  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            89956238       Image:         services.exe
        Wait Start TickCount      42017          Ticks: 1482 (0:00:00:23.119)
        Context Switch Count      18
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init a3104000 Current a3103bc8 Base a3104000 Limit a3101000 Call 0
        Priority 11 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a3103be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a3103c1c 81cad431 nt!KiSwapThread+0x389
        a3103c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a3103cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a3103d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a3103d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a3103d64)
        0020f998 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0020f99c 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        0020f9c8 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        0020fa04 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        0020fa70 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        0020fa7c 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        0020faa0 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        0020faac 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        0020fab8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0020faf8 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 83605d78  Cid 0214.06d8  Teb: 7ffdc000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            899c7140  QueueObject
            83605e00  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            89956238       Image:         services.exe
        Wait Start TickCount      42017          Ticks: 1482 (0:00:00:23.119)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init 9f7d8000 Current 9f7d7bc8 Base 9f7d8000 Limit 9f7d5000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f7d7be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f7d7c1c 81cad431 nt!KiSwapThread+0x389
        9f7d7c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        9f7d7cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        9f7d7d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        9f7d7d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f7d7d64)
        0103f9d0 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0103f9d4 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        0103fa00 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        0103fa3c 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        0103faa8 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        0103fab4 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        0103fad8 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        0103fae4 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        0103faf0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0103fb30 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Lsass process

```
PROCESS 8995e4a0  SessionId: 0  Cid: 0220    Peb: 7ffdc000  ParentCid: 01e8
    DirBase: 29a010e0  ObjectTable: 89d35740  HandleCount: 580.
    Image: lsass.exe
    VadRoot 89976f98 Vads 112 Clone 0 Private 635. Modified 968. Locked 2.
    DeviceMap 85a03048
    Token                             89d369c8
    ElapsedTime                       00:11:06.977
    UserTime                          00:00:00.577
    KernelTime                        00:00:00.468
    QuotaPoolUsage[PagedPool]         81104
    QuotaPoolUsage[NonPagedPool]      9168
    Working Set Sizes (now,min,max)  (392, 50, 345) (1568KB, 200KB, 1380KB)
    PeakWorkingSetSize                1791
    VirtualSize                       37 Mb
    PeakVirtualSize                   38 Mb
    PageFaultCount                    3795
    MemoryPriority                    BACKGROUND
    BasePriority                      9
    CommitCharge                      801

    Setting context for this process...
.process /p /r ffffffff8995e4a0

    !peb
PEB at 7ffdc000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00f80000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00151608 . 001af9a8
    Ldr.InLoadOrderModuleList:           00151588 . 001af998
    Ldr.InMemoryOrderModuleList:         00151590 . 001af9a0
            Base TimeStamp                     Module
          f80000 4549afbe Nov 02 08:43:42 2006 C:\Windows\system32\lsass.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        75930000 4549bd04 Nov 02 09:40:20 2006 C:\Windows\system32\LSASRV.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        75b80000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\Secur32.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        758b0000 4549bdaa Nov 02 09:43:06 2006 C:\Windows\system32\SAMSRV.dll
        75b60000 4549bd26 Nov 02 09:40:54 2006 C:\Windows\system32\cryptdll.dll
        75af0000 4549bcf1 Nov 02 09:40:01 2006 C:\Windows\system32\DNSAPI.dll
        75fe0000 4549be0e Nov 02 09:44:46 2006 C:\Windows\system32\WS2_32.dll
        77550000 4549bdc7 Nov 02 09:43:35 2006 C:\Windows\system32\NSI.dll
        75840000 4549bd53 Nov 02 09:41:39 2006 C:\Windows\system32\NETAPI32.dll
        75ce0000 4549bd99 Nov 02 09:42:49 2006 C:\Windows\system32\PSAPI.DLL
        75ad0000 4549bda8 Nov 02 09:43:04 2006 C:\Windows\system32\SAMLIB.dll
        75820000 4549bd41 Nov 02 09:41:21 2006 C:\Windows\system32\MSASN1.dll
        75780000 4549bdcc Nov 02 09:43:40 2006 C:\Windows\system32\NTDSAPI.dll
        76310000 4549be44 Nov 02 09:45:40 2006 C:\Windows\system32\WLDAP32.dll
        75770000 4549bce3 Nov 02 09:39:47 2006 C:\Windows\system32\FeClient.dll
        75750000 4549bd14 Nov 02 09:40:36 2006 C:\Windows\system32\MPR.dll
        75ba0000 4549bde2 Nov 02 09:44:02 2006 C:\Windows\system32\USERENV.dll
        75650000 45b96fde Jan 26 03:05:02 2007 C:\Windows\system32\CRYPT32.dll
        75610000 4679de70 Jun 21 03:12:00 2007 C:\Windows\system32\slc.dll
        75ac0000 4549bddd Nov 02 09:43:57 2006 C:\Windows\system32\SYSNTFY.dll
        755d0000 4549bdf6 Nov 02 09:44:22 2006 C:\Windows\system32\wevtapi.dll
        755b0000 4549bd3f Nov 02 09:41:19 2006 C:\Windows\system32\IPHLPAPI.DLL
        75570000 46807ea6 Jun 26 03:49:10 2007 C:\Windows\system32\dhcpcsvc.DLL
```

```
        75560000 4549be1e Nov 02 09:45:02 2006 C:\Windows\system32\WINNSI.DLL
        75540000 46807ea7 Jun 26 03:49:11 2007 C:\Windows\system32\dhcpcsvc6.DLL
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        75530000 4549bcf8 Nov 02 09:40:08 2006 C:\Windows\system32\cngaudit.dll
        757b0000 4549bccf Nov 02 09:39:27 2006 C:\Windows\system32\AUTHZ.dll
        754f0000 4549bd49 Nov 02 09:41:29 2006 C:\Windows\system32\ncrypt.dll
        754a0000 4549bcb9 Nov 02 09:39:05 2006 C:\Windows\system32\BCRYPT.dll
        75480000 4549bd20 Nov 02 09:40:48 2006 C:\Windows\system32\credssp.dll
        75490000 45499bc4 Nov 02 07:18:28 2006 C:\Windows\system32\msprivs.dll
        75400000 4549bd7f Nov 02 09:42:23 2006 C:\Windows\system32\kerberos.dll
        75250000 4549bd69 Nov 02 09:42:01 2006 C:\Windows\system32\mswsock.dll
        752b0000 4549be21 Nov 02 09:45:05 2006 C:\Windows\System32\wship6.dll
        75210000 4549bd5d Nov 02 09:41:49 2006 C:\Windows\system32\msv1_0.dll
        75180000 4549bd5e Nov 02 09:41:50 2006 C:\Windows\system32\netlogon.dll
        750a0000 4549be0a Nov 02 09:44:42 2006 C:\Windows\system32\WINBRAND.dll
        75050000 46773a78 Jun 19 03:07:52 2007 C:\Windows\system32\schannel.dll
        753c0000 4549bde2 Nov 02 09:44:02 2006 C:\Windows\system32\wdigest.dll
        75350000 4549bdae Nov 02 09:43:10 2006 C:\Windows\system32\rsaenh.dll
        753a0000 4549be09 Nov 02 09:44:41 2006 C:\Windows\system32\tspkg.dll
        75330000 4549bcd7 Nov 02 09:39:35 2006 C:\Windows\system32\GPAPI.dll
        77030000 4549bdb0 Nov 02 09:43:12 2006 C:\Windows\system32\setupapi.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        752d0000 4549bdb1 Nov 02 09:43:13 2006 C:\Windows\system32\scecli.dll
        74c80000 4549bd81 Nov 02 09:42:25 2006 C:\Windows\system32\keyiso.dll
        752c0000 4549be27 Nov 02 09:45:11 2006 C:\Windows\System32\wshtcpip.dll
        6db20000 4549bd1d Nov 02 09:40:45 2006 C:\Windows\system32\dssenh.dll
    SubSystemData:     00000000
    ProcessHeap:       00150000
    ProcessParameters: 00150ea8
    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;C:\Program Files\QuickTime\QTSystem\'
    Environment:  001507e8
        ALLUSERSPROFILE=C:\ProgramData
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        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=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        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 89977030  Cid 0220.0240  Teb: 7ffde000 Win32Thread: 00000000 WAIT: (Executive)
UserMode Non-Alertable
            9fc8d914  NotificationEvent
        IRP List:
            9e1cd758: (0006,0094) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            8995e4a0       Image:         lsass.exe
        Wait Start TickCount      1087           Ticks: 42412 (0:00:11:01.631)
        Context Switch Count      11
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address LSASRV!ServiceDispatcherThread (0x7595bffc)
        Stack Init 9ea00000 Current 9e9ffbc8 Base 9ea00000 Limit 9e9fd000 Call 0
        Priority 11 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9e9ffbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e9ffc1c 81c293a7 nt!KiSwapThread+0x389
        9e9ffc78 81d88faf nt!KeWaitForSingleObject+0x414
        9e9ffcac 81d93669 nt!IopSynchronousServiceTail+0x258
        9e9ffd38 81c8caaa nt!NtReadFile+0x646
        9e9ffd38 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9e9ffd64)
        00eff9a4 77490080 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00eff9a8 75f3853f ntdll!ZwReadFile+0xc (FPO: [9,0,0])
        00effa20 775cffe2 kernel32!ReadFile+0x20e (FPO: [Non-Fpo])
        00effa4c 775cfdfb ADVAPI32!ScGetPipeInput+0x2a (FPO: [Non-Fpo])
        00effab4 775cbdd2 ADVAPI32!ScDispatcherLoop+0x6c (FPO: [Non-Fpo])
        00effd2c 7595c047 ADVAPI32!StartServiceCtrlDispatcherW+0xce (FPO: [Non-Fpo])
        00effd40 75f33833 LSASRV!ServiceDispatcherThread+0xab (FPO: [Non-Fpo])
        00effd4c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00effd8c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 8995dae0  Cid 0220.0248  Teb: 7ffdd000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            8997a848  SynchronizationTimer
            83873a38  SynchronizationEvent
            899afd70  SynchronizationTimer
            9e1d8520  Thread
            899d83a0  SynchronizationEvent
            899d8c90  SynchronizationEvent
            89991848  SynchronizationEvent
            847d5e00  SynchronizationEvent
            899e1ab8  NotificationEvent
            899d3450  SynchronizationEvent
            8997a740  SynchronizationEvent
            899afc88  SynchronizationEvent
            89991570  SynchronizationEvent
            899aa4e0  SynchronizationEvent
            89969528  SynchronizationEvent
            8997a1f0  SynchronizationEvent
            899ab948  SynchronizationEvent
            899df200  SynchronizationEvent
            89951bc8  SynchronizationEvent
            899daa20  SynchronizationEvent
            9e1ce800  SynchronizationEvent
            9e1d8df8  SynchronizationEvent
            9fca69a0  NotificationEvent
            9fd19378  SynchronizationEvent
            899dc340  SynchronizationEvent
            9fd923e8  SynchronizationEvent
            8383b6f8  SynchronizationEvent
            899afcb8  SynchronizationTimer
            838370c0  SynchronizationEvent
            8387d580  SynchronizationEvent
            9fc89458  SynchronizationEvent
            8387ed60  SynchronizationEvent
            838355e8  SynchronizationEvent
            8995db68  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            8995e4a0       Image:         lsass.exe
        Wait Start TickCount      31158          Ticks: 12341 (0:00:03:12.520)
        Context Switch Count      112
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x7744b49a)
        Stack Init 88eb5000 Current 88eb48d0 Base 88eb5000 Limit 88eb2000 Call 0
        Priority 11 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        88eb48e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        88eb4924 81c28c64 nt!KiSwapThread+0x389
        88eb4970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        88eb4bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        88eb4d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        88eb4d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 88eb4d64)
        00dbf6b0 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00dbf6b4 7744b65b ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00dbf850 75f33833 ntdll!TppWaiterpThread+0x294 (FPO: [Non-Fpo])
        00dbf85c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00dbf89c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 899380d8  Cid 0220.0250  Teb: 7ffda000 Win32Thread: 00000000 WAIT: (WrLpcReceive)
UserMode Non-Alertable
            899382ec  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            8995e4a0       Image:         lsass.exe
        Wait Start TickCount      1825           Ticks: 41674 (0:00:10:50.118)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address LSASRV!LsapRmServerThread (0x7597fbf0)
        Stack Init 9e9d4000 Current 9e9d3b70 Base 9e9d4000 Limit 9e9d1000 Call 0
        Priority 10 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9e9d3b88 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e9d3bc4 81c293a7 nt!KiSwapThread+0x389
        9e9d3c24 81dc3dac nt!KeWaitForSingleObject+0x414
        9e9d3c5c 81dc486e nt!AlpcpReceiveMessagePort+0x221
        9e9d3cc4 81dbe7b6 nt!AlpcpReceiveLegacyMessage+0x197
        9e9d3d30 81dbe69c nt!NtReplyWaitReceivePortEx+0x100
        9e9d3d4c 81c8caaa nt!NtReplyWaitReceivePort+0x18
        9e9d3d4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9e9d3d64)
        0102f76c 77490140 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0102f770 7597fc6e ntdll!ZwReplyWaitReceivePort+0xc (FPO: [4,0,0])
        0102f8a0 75f33833 LSASRV!LsapRmServerThread+0x84 (FPO: [Non-Fpo])
        0102f8ac 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0102f8ec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9e1d8520  Cid 0220.0280  Teb: 7ffd7000 Win32Thread: 00000000 WAIT: (WrLpcReceive)
UserMode Non-Alertable
            9e1d8734  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            8995e4a0       Image:         lsass.exe
        Wait Start TickCount      19969          Ticks: 23530 (0:00:06:07.070)
        Context Switch Count      614
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address LSASRV!LsapThreadBase (0x7597d271)
        Stack Init 9e9bc000 Current 9e9bbb70 Base 9e9bc000 Limit 9e9b9000 Call 0
        Priority 10 BasePriority 9 PriorityDecrement 1 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9e9bbb88 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e9bbbc4 81c293a7 nt!KiSwapThread+0x389
        9e9bbc24 81dc3dac nt!KeWaitForSingleObject+0x414
        9e9bbc5c 81dc486e nt!AlpcpReceiveMessagePort+0x221
        9e9bbcc4 81dbe7b6 nt!AlpcpReceiveLegacyMessage+0x197
        9e9bbd30 81dbe69c nt!NtReplyWaitReceivePortEx+0x100
        9e9bbd4c 81c8caaa nt!NtReplyWaitReceivePort+0x18
        9e9bbd4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9e9bbd64)
        011efd90 77490140 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        011efd94 759403eb ntdll!ZwReplyWaitReceivePort+0xc (FPO: [4,0,0])
        011efee0 7597d2d5 LSASRV!LpcServerThread+0x123 (FPO: [Non-Fpo])
        011eff24 75f33833 LSASRV!LsapThreadBase+0xaf (FPO: [Non-Fpo])
        011eff30 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        011eff70 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 899d80f8  Cid 0220.0288  Teb: 7ffd5000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            899d83d0  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            8995e4a0       Image:         lsass.exe
        Wait Start TickCount      853            Ticks: 42646 (0:00:11:05.281)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address LSASRV!LsapThreadBase (0x7597d271)
        Stack Init 88e30000 Current 88e2fc38 Base 88e30000 Limit 88e2d000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        88e2fc50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        88e2fc8c 81c293a7 nt!KiSwapThread+0x389
        88e2fce8 81df5057 nt!KeWaitForSingleObject+0x414
        88e2fd50 81c8caaa nt!NtWaitForSingleObject+0xbe
        88e2fd50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 88e2fd64)
        0125f70c 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0125f710 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0125f780 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        0125f794 7593ffee kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0125f7b0 7593ff7b LSASRV!WaitForThreadTask+0x4e (FPO: [Non-Fpo])
        0125f7d8 7597d2d5 LSASRV!SpmPoolThreadBase+0xbc (FPO: [Non-Fpo])
        0125f81c 75f33833 LSASRV!LsapThreadBase+0xaf (FPO: [Non-Fpo])
        0125f828 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0125f868 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 899e17a8  Cid 0220.0290  Teb: 7ffd3000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            899e1a80  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            8995e4a0       Image:         lsass.exe
        Wait Start TickCount      1599           Ticks: 41900 (0:00:10:53.644)
        Context Switch Count      38
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address LSASRV!LsapThreadBase (0x7597d271)
        Stack Init 9e9d8000 Current 9e9d7c38 Base 9e9d8000 Limit 9e9d5000 Call 0
        Priority 10 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9e9d7c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e9d7c8c 81c293a7 nt!KiSwapThread+0x389
        9e9d7ce8 81df5057 nt!KeWaitForSingleObject+0x414
        9e9d7d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        9e9d7d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9e9d7d64)
        013ff998 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        013ff99c 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        013ffa0c 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        013ffa20 7593ffee kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        013ffa3c 7593ff7b LSASRV!WaitForThreadTask+0x4e (FPO: [Non-Fpo])
        013ffa64 7597d2d5 LSASRV!SpmPoolThreadBase+0xbc (FPO: [Non-Fpo])
        013ffaa8 75f33833 LSASRV!LsapThreadBase+0xaf (FPO: [Non-Fpo])
        013ffab4 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        013ffaf4 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9e1f8030  Cid 0220.02b8  Teb: 7ffae000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Alertable
            89991fa0  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            8995e4a0       Image:         lsass.exe
        Wait Start TickCount      23815          Ticks: 19684 (0:00:05:07.072)
        Context Switch Count      45
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init 9e89f000 Current 9e89ebc8 Base 9e89f000 Limit 9e89c000 Call 0
        Priority 10 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9e89ebe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e89ec1c 81cad431 nt!KiSwapThread+0x389
        9e89ec68 81d8b982 nt!KeRemoveQueueEx+0x568
        9e89ecc0 81c7a036 nt!IoRemoveIoCompletion+0x23
        9e89ed54 81c8caaa nt!NtWaitForWorkViaWorkerFactory+0x1a1
        9e89ed54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9e89ed64)
        010bfad0 77490850 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        010bfad4 7749a1b4 ntdll!NtWaitForWorkViaWorkerFactory+0xc (FPO: [2,0,0])
        010bfbfc 75f33833 ntdll!TppWorkerThread+0x1f6 (FPO: [Non-Fpo])
        010bfc08 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        010bfc48 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 8356fa40  Cid 0220.09dc  Teb: 7ffdb000 Win32Thread: 00000000 WAIT: (DelayExecution)
UserMode Alertable
            8356fac8  NotificationTimer
        IRP List:
            835e6e20: (0006,01d8) Flags: 00060000  Mdl: 00000000
            834da618: (0006,01d8) Flags: 00060000  Mdl: 00000000
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            8995e4a0       Image:         lsass.exe
        Wait Start TickCount      42379          Ticks: 1120 (0:00:00:17.472)
        Context Switch Count      1455
        UserTime                  00:00:00.093
        KernelTime                00:00:00.093
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init 9e8ab000 Current 9e8aac58 Base 9e8ab000 Limit 9e8a8000 Call 0
        Priority 11 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9e8aac70 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e8aacac 81cac48e nt!KiSwapThread+0x389
        9e8aad08 81e90bf1 nt!KeDelayExecutionThread+0x397
        9e8aad54 81c8caaa nt!NtDelayExecution+0x8d
        9e8aad54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9e8aad64)
        0119f90c 7748f7c0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0119f910 75d0a0e4 ntdll!NtDelayExecution+0xc (FPO: [2,0,0])
        0119f928 75d0a062 RPCRT4!TIMER::Wait+0x2c
        0119f948 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0xbd
        0119f954 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        0119f960 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0119f9a0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD a18b5030  Cid 0220.0bd4  Teb: 7ffdf000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            89977c98  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            8995e4a0       Image:         lsass.exe
        Wait Start TickCount      42379          Ticks: 1120 (0:00:00:17.472)
        Context Switch Count      11
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init a0959000 Current a0958bc8 Base a0959000 Limit a0956000 Call 0
        Priority 11 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a0958be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0958c1c 81cad431 nt!KiSwapThread+0x389
        a0958c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a0958cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a0958d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a0958d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0958d64)
        00d5f8e8 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00d5f8ec 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        00d5f918 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        00d5f954 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        00d5f9c0 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        00d5f9cc 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        00d5f9f4 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        00d5fa00 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        00d5fa0c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00d5fa4c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Lsm process

```
PROCESS 8995ab30  SessionId: 0  Cid: 0228    Peb: 7ffdb000  ParentCid: 01e8
    DirBase: 29a01100  ObjectTable: 89d39620  HandleCount: 165.
    Image: lsm.exe
    VadRoot 8996c8d8 Vads 62 Clone 0 Private 368. Modified 108. Locked 0.
    DeviceMap 85a03048
    Token                             89d397f0
    ElapsedTime                       00:11:06.962
    UserTime                          00:00:00.015
    KernelTime                        00:00:00.062
    QuotaPoolUsage[PagedPool]         45840
    QuotaPoolUsage[NonPagedPool]      3352
    Working Set Sizes (now,min,max)  (843, 50, 345) (3372KB, 200KB, 1380KB)
    PeakWorkingSetSize                1017
    VirtualSize                       23 Mb
    PeakVirtualSize                   24 Mb
    PageFaultCount                    1107
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      479

    Setting context for this process...
.process /p /r ffffffff8995ab30

    !peb
PEB at 7ffdb000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         005a0000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 001c15f8 . 001e6e60
    Ldr.InLoadOrderModuleList:           001c1578 . 001e6f30
    Ldr.InMemoryOrderModuleList:         001c1580 . 001e6f38
            Base TimeStamp                     Module
          5a0000 4549b436 Nov 02 09:02:46 2006 C:\Windows\system32\lsm.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        75ac0000 4549bddd Nov 02 09:43:57 2006 C:\Windows\system32\SYSNTFY.dll
        757a0000 4549be18 Nov 02 09:44:56 2006 C:\Windows\system32\WMsgAPI.dll
        75b80000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\secur32.dll
        75480000 4549bd20 Nov 02 09:40:48 2006 C:\Windows\system32\credssp.dll
        75650000 45b96fde Jan 26 03:05:02 2007 C:\Windows\system32\CRYPT32.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        75820000 4549bd41 Nov 02 09:41:21 2006 C:\Windows\system32\MSASN1.dll
        75ba0000 4549bde2 Nov 02 09:44:02 2006 C:\Windows\system32\USERENV.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        75050000 46773a78 Jun 19 03:07:52 2007 C:\Windows\system32\schannel.dll
        75840000 4549bd53 Nov 02 09:41:39 2006 C:\Windows\system32\NETAPI32.dll
        75ce0000 4549bd99 Nov 02 09:42:49 2006 C:\Windows\system32\PSAPI.DLL
    SubSystemData:     00000000
    ProcessHeap:       001c0000
    ProcessParameters: 001c0ea8
    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;C:\Program Files\QuickTime\QTSystem\'
    Environment:  001c07e8
        ALLUSERSPROFILE=C:\ProgramData
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        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;C:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        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 8995a5f0  Cid 0228.022c  Teb: 7ffdf000 Win32Thread: ff4e6668 WAIT: (UserRequest)
UserMode Non-Alertable
            899d6888  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            8995ab30       Image:         lsm.exe
        Wait Start TickCount      1002           Ticks: 42497 (0:00:11:02.957)
        Context Switch Count      117
        UserTime                  00:00:00.015
        KernelTime                00:00:00.015
        Win32 Start Address lsm!mainCRTStartup (0x005b3acb)
        Stack Init 88e8d000 Current 88e8cc38 Base 88e8d000 Limit 88e8a000 Call 0
        Priority 13 BasePriority 8 PriorityDecrement 4 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        88e8cc50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        88e8cc8c 81c293a7 nt!KiSwapThread+0x389
        88e8cce8 81df5057 nt!KeWaitForSingleObject+0x414
        88e8cd50 81c8caaa nt!NtWaitForSingleObject+0xbe
        88e8cd50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 88e8cd64)
        0011fd80 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0011fd84 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0011fdf4 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        0011fe08 75d02ba5 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0011fe18 75cf1fd2 RPCRT4!EVENT::Wait+0x13
        0011fe2c 75cf1fb3 RPCRT4!RPC_SERVER::WaitForStopServerListening+0x17
        0011fe3c 005b0381 RPCRT4!RPC_SERVER::WaitServerListen+0x48 (FPO: [0,0,0])
        0011fe4c 005b3b8f lsm!main+0xa9 (FPO: [Non-Fpo])
        0011fe90 75f33833 lsm!_initterm_e+0x163 (FPO: [Non-Fpo])
        0011fe9c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0011fedc 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fc481f0  Cid 0228.0344  Teb: 7ffdd000 Win32Thread: 00000000 WAIT: (WrLpcReceive)
UserMode Non-Alertable
            9fc48404  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            8995ab30       Image:         lsm.exe
        Wait Start TickCount      9330           Ticks: 34169 (0:00:08:53.039)
        Context Switch Count      16
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init 9f2ec000 Current 9f2ebb70 Base 9f2ec000 Limit 9f2e9000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f2ebb88 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f2ebbc4 81c293a7 nt!KiSwapThread+0x389
        9f2ebc24 81dc3dac nt!KeWaitForSingleObject+0x414
        9f2ebc5c 81dc486e nt!AlpcpReceiveMessagePort+0x221
        9f2ebcc4 81dbe7b6 nt!AlpcpReceiveLegacyMessage+0x197
        9f2ebd30 81dbe69c nt!NtReplyWaitReceivePortEx+0x100
        9f2ebd4c 81c8caaa nt!NtReplyWaitReceivePort+0x18
        9f2ebd4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f2ebd64)
        0018fc08 77490140 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0018fc0c 005a6e4d ntdll!ZwReplyWaitReceivePort+0xc (FPO: [4,0,0])
        0018fd1c 005b0ba2 lsm!CCsrMgr::LpcWorker+0x44 (FPO: [Non-Fpo])
        0018fd24 7746fe6d lsm!CCsrMgr::staticLpcWorker+0xd (FPO: [Non-Fpo])
        0018fd88 7749a2b8 ntdll!RtlpTpWorkCallback+0xbf (FPO: [Non-Fpo])
        0018feb0 75f33833 ntdll!TppWorkerThread+0x522 (FPO: [Non-Fpo])
        0018febc 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0018fefc 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fc49c98  Cid 0228.0348  Teb: 7ffdc000 Win32Thread: 00000000 WAIT: (WrLpcReceive)
UserMode Non-Alertable
            9fc49eac  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            8995ab30       Image:         lsm.exe
        Wait Start TickCount      9811           Ticks: 33688 (0:00:08:45.536)
        Context Switch Count      8
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init 9f2e8000 Current 9f2e7b70 Base 9f2e8000 Limit 9f2e5000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f2e7b88 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f2e7bc4 81c293a7 nt!KiSwapThread+0x389
        9f2e7c24 81dc3dac nt!KeWaitForSingleObject+0x414
        9f2e7c5c 81dc486e nt!AlpcpReceiveMessagePort+0x221
        9f2e7cc4 81dbe7b6 nt!AlpcpReceiveLegacyMessage+0x197
        9f2e7d30 81dbe69c nt!NtReplyWaitReceivePortEx+0x100
        9f2e7d4c 81c8caaa nt!NtReplyWaitReceivePort+0x18
        9f2e7d4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f2e7d64)
        004df784 77490140 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        004df788 005a6e4d ntdll!ZwReplyWaitReceivePort+0xc (FPO: [4,0,0])
        004df898 005b0ba2 lsm!CCsrMgr::LpcWorker+0x44 (FPO: [Non-Fpo])
        004df8a0 7746fe6d lsm!CCsrMgr::staticLpcWorker+0xd (FPO: [Non-Fpo])
        004df904 7749a2b8 ntdll!RtlpTpWorkCallback+0xbf (FPO: [Non-Fpo])
        004dfa2c 75f33833 ntdll!TppWorkerThread+0x522 (FPO: [Non-Fpo])
        004dfa38 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        004dfa78 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fc49868  Cid 0228.034c  Teb: 7ffda000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            9fc49b10  SynchronizationTimer
            84d32d90  ProcessObject
            8983e1b0  ProcessObject
            84d33020  ProcessObject
            899e3020  ProcessObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            8995ab30       Image:         lsm.exe
        Wait Start TickCount      1000           Ticks: 42499 (0:00:11:02.988)
        Context Switch Count      7
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x7744b49a)
        Stack Init 9f2f0000 Current 9f2ef8d0 Base 9f2f0000 Limit 9f2ed000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f2ef8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f2ef924 81c28c64 nt!KiSwapThread+0x389
        9f2ef970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f2efbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f2efd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f2efd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f2efd64)
        0034fc2c 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0034fc30 7744b65b ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0034fdcc 75f33833 ntdll!TppWaiterpThread+0x294 (FPO: [Non-Fpo])
        0034fdd8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0034fe18 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fc53178  Cid 0228.035c  Teb: 7ffd9000 Win32Thread: 00000000 WAIT: (WrLpcReceive)
UserMode Non-Alertable
            9fc5338c  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            8995ab30       Image:         lsm.exe
        Wait Start TickCount      9811           Ticks: 33688 (0:00:08:45.536)
        Context Switch Count      11
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init 9f2fc000 Current 9f2fbb70 Base 9f2fc000 Limit 9f2f9000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f2fbb88 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f2fbbc4 81c293a7 nt!KiSwapThread+0x389
        9f2fbc24 81dc3dac nt!KeWaitForSingleObject+0x414
        9f2fbc5c 81dc486e nt!AlpcpReceiveMessagePort+0x221
        9f2fbcc4 81dbe7b6 nt!AlpcpReceiveLegacyMessage+0x197
        9f2fbd30 81dbe69c nt!NtReplyWaitReceivePortEx+0x100
        9f2fbd4c 81c8caaa nt!NtReplyWaitReceivePort+0x18
        9f2fbd4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f2fbd64)
        0053f970 77490140 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0053f974 005a6e4d ntdll!ZwReplyWaitReceivePort+0xc (FPO: [4,0,0])
        0053fa84 005b0ba2 lsm!CCsrMgr::LpcWorker+0x44 (FPO: [Non-Fpo])
        0053fa8c 7746fe6d lsm!CCsrMgr::staticLpcWorker+0xd (FPO: [Non-Fpo])
        0053faf0 7749a2b8 ntdll!RtlpTpWorkCallback+0xbf (FPO: [Non-Fpo])
        0053fc18 75f33833 ntdll!TppWorkerThread+0x522 (FPO: [Non-Fpo])
        0053fc24 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0053fc64 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fc40030  Cid 0228.0364  Teb: 7ffd8000 Win32Thread: 00000000 WAIT: (WrLpcReceive)
UserMode Non-Alertable
            9fc40244  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            8995ab30       Image:         lsm.exe
        Wait Start TickCount      14133          Ticks: 29366 (0:00:07:38.112)
        Context Switch Count      12
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init 9e9b8000 Current 9e9b7b70 Base 9e9b8000 Limit 9e9b5000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9e9b7b88 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e9b7bc4 81c293a7 nt!KiSwapThread+0x389
        9e9b7c24 81dc3dac nt!KeWaitForSingleObject+0x414
        9e9b7c5c 81dc486e nt!AlpcpReceiveMessagePort+0x221
        9e9b7cc4 81dbe7b6 nt!AlpcpReceiveLegacyMessage+0x197
        9e9b7d30 81dbe69c nt!NtReplyWaitReceivePortEx+0x100
        9e9b7d4c 81c8caaa nt!NtReplyWaitReceivePort+0x18
        9e9b7d4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9e9b7d64)
        0099fc84 77490140 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0099fc88 005a6e4d ntdll!ZwReplyWaitReceivePort+0xc (FPO: [4,0,0])
        0099fd98 005b0ba2 lsm!CCsrMgr::LpcWorker+0x44 (FPO: [Non-Fpo])
        0099fda0 7746fe6d lsm!CCsrMgr::staticLpcWorker+0xd (FPO: [Non-Fpo])
        0099fe04 7749a2b8 ntdll!RtlpTpWorkCallback+0xbf (FPO: [Non-Fpo])
        0099ff2c 75f33833 ntdll!TppWorkerThread+0x522 (FPO: [Non-Fpo])
        0099ff38 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0099ff78 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fc40d78  Cid 0228.0368  Teb: 7ffd7000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fc497b0  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            8995ab30       Image:         lsm.exe
        Wait Start TickCount      9163           Ticks: 34336 (0:00:08:55.645)
        Context Switch Count      19
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init 9f300000 Current 9f2ffc38 Base 9f300000 Limit 9f2fd000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f2ffc50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f2ffc8c 81c293a7 nt!KiSwapThread+0x389
        9f2ffce8 81df5057 nt!KeWaitForSingleObject+0x414
        9f2ffd50 81c8caaa nt!NtWaitForSingleObject+0xbe
        9f2ffd50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f2ffd64)
        0047fc28 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0047fc2c 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0047fc9c 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        0047fcb0 005a7536 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0047fcd8 005b2aa1 lsm!CSCMNotify::SCMNotificationWorker+0xae (FPO: [Non-Fpo])
        0047fce0 7746fe6d lsm!CSCMNotify::staticSCMNotificationThread+0xd (FPO: [Non-Fpo])
        0047fd44 7749a2b8 ntdll!RtlpTpWorkCallback+0xbf (FPO: [Non-Fpo])
        0047fe6c 75f33833 ntdll!TppWorkerThread+0x522 (FPO: [Non-Fpo])
        0047fe78 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0047feb8 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fc4f060  Cid 0228.0374  Teb: 7ffd5000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            9fc4d630  SynchronizationEvent
            9fc4fe30  SynchronizationEvent
            9fc4e098  SynchronizationEvent
            9fc4d9e8  SynchronizationEvent
            9fc4d9b8  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            8995ab30       Image:         lsm.exe
        Wait Start TickCount      1855           Ticks: 41644 (0:00:10:49.650)
        Context Switch Count      19
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init 9f29c000 Current 9f29b8d0 Base 9f29c000 Limit 9f299000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f29b8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f29b924 81c28c64 nt!KiSwapThread+0x389
        9f29b970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f29bbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f29bd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f29bd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f29bd64)
        00c8f604 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00c8f608 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00c8f6a4 005ae9ca kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        00c8f6c4 005ae5e4 lsm!CPolicyMonitor::WaitForTSConnectionsPolicyChanges+0x36 (FPO: [Non-
Fpo])
        00c8f6fc 005b09bd lsm!CPolicyMonitor::PolicyMonitorWorker+0x139 (FPO: [Non-Fpo])
        00c8f704 7746fe6d lsm!CPolicyMonitor::staticPolicyMonitorWorker+0xd (FPO: [Non-Fpo])
        00c8f768 7749a2b8 ntdll!RtlpTpWorkCallback+0xbf (FPO: [Non-Fpo])
        00c8f890 75f33833 ntdll!TppWorkerThread+0x522 (FPO: [Non-Fpo])
        00c8f89c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00c8f8dc 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 89995d78  Cid 0228.0a88  Teb: 7ffd6000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            9fc16ba0  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            8995ab30       Image:         lsm.exe
        Wait Start TickCount      30322          Ticks: 13177 (0:00:03:25.562)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init a0965000 Current a0964bc8 Base a0965000 Limit a0962000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a0964be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0964c1c 81cad431 nt!KiSwapThread+0x389
        a0964c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a0964cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a0964d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a0964d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0964d64)
        0111f808 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0111f80c 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        0111f838 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        0111f874 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        0111f8e0 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        0111f8ec 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        0111f914 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        0111f920 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        0111f92c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0111f96c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Winlogon process

```
PROCESS 899e3020  SessionId: 1  Cid: 0294    Peb: 7ffdf000  ParentCid: 01e0
    DirBase: 29a01120  ObjectTable: 89d15c90  HandleCount: 123.
    Image: winlogon.exe
    VadRoot 9e1e4b28 Vads 69 Clone 0 Private 379. Modified 361. Locked 0.
    DeviceMap 85a03048
    Token                             89d5e808
    ElapsedTime                       00:11:06.041
    UserTime                          00:00:00.109
    KernelTime                        00:00:00.187
    QuotaPoolUsage[PagedPool]         60152
    QuotaPoolUsage[NonPagedPool]      3352
    Working Set Sizes (now,min,max)  (1125, 50, 345) (4500KB, 200KB, 1380KB)
    PeakWorkingSetSize                1618
    VirtualSize                       31 Mb
    PeakVirtualSize                   52 Mb
    PageFaultCount                    2531
    MemoryPriority                    BACKGROUND
    BasePriority                      13
    CommitCharge                      490

    Setting context for this process...
.process /p /r ffffffff899e3020

    !peb
PEB at 7ffdf000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00820000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00351348 . 003698c8
    Ldr.InLoadOrderModuleList:           003512c8 . 003698b8
    Ldr.InMemoryOrderModuleList:         003512d0 . 003698c0
            Base TimeStamp                     Module
          820000 4549aff7 Nov 02 08:44:39 2006 C:\Windows\system32\winlogon.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        75b80000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\Secur32.dll
        75300000 4549be2e Nov 02 09:45:18 2006 C:\Windows\system32\WINSTA.dll
        75ce0000 4549bd99 Nov 02 09:42:49 2006 C:\Windows\system32\PSAPI.DLL
        75ba0000 4549bde2 Nov 02 09:44:02 2006 C:\Windows\system32\USERENV.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        75b20000 4549bcaf Nov 02 09:38:55 2006 C:\Windows\system32\apphelp.dll
        75020000 4549bddb Nov 02 09:43:55 2006 C:\Windows\system32\NTMARTA.DLL
        76310000 4549be44 Nov 02 09:45:40 2006 C:\Windows\system32\WLDAP32.dll
        75fe0000 4549be0e Nov 02 09:44:46 2006 C:\Windows\system32\WS2_32.dll
        77550000 4549bdc7 Nov 02 09:43:35 2006 C:\Windows\system32\NSI.dll
        75ad0000 4549bda8 Nov 02 09:43:04 2006 C:\Windows\system32\SAMLIB.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        74c40000 4549bdbe Nov 02 09:43:26 2006 C:\Windows\system32\SHSVCS.dll
        746d0000 4549bde7 Nov 02 09:44:07 2006 C:\Windows\system32\uxtheme.dll
        75350000 4549bdae Nov 02 09:43:10 2006 C:\Windows\system32\rsaenh.dll
        73240000 4654f735 May 24 03:23:49 2007 C:\Windows\system32\WindowsCodecs.dll
        75840000 4549bd53 Nov 02 09:41:39 2006 C:\Windows\system32\NETAPI32.dll
        75610000 4679de70 Jun 21 03:12:00 2007 C:\Windows\system32\slc.dll
        75750000 4549bd14 Nov 02 09:40:36 2006 C:\Windows\system32\MPR.dll
```

```
    SubSystemData:     00000000
    ProcessHeap:       00350000
    ProcessParameters: 00350cd8
    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;C:\Program
Files\QuickTime\QTSystem\'
    Environment:  0036cce0
        ALLUSERSPROFILE=C:\ProgramData
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        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;C:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        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 9e1e7d78  Cid 0294.0298  Teb: 7ffde000 Win32Thread: ffab9e98 WAIT: (UserRequest)
UserMode Non-Alertable
            89962cc8  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            899e3020       Image:         winlogon.exe
        Wait Start TickCount      18555          Ticks: 24944 (0:00:06:29.128)
        Context Switch Count      454
        UserTime                  00:00:00.000
        KernelTime                00:00:00.124
        Win32 Start Address winlogon!WinMainCRTStartup (0x008457e2)
        Stack Init 9e988000 Current 9e987c38 Base 9e988000 Limit 9e985000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9e987c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e987c8c 81c293a7 nt!KiSwapThread+0x389
        9e987ce8 81df5057 nt!KeWaitForSingleObject+0x414
        9e987d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        9e987d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9e987d64)
        0018f8c4 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0018f8c8 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0018f938 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        0018f94c 00846bf8 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0018f96c 00846525 winlogon!SignalManagerWaitForSignal+0xd5 (FPO: [Non-Fpo])
        0018fb04 0082c03d winlogon!StateMachineRun+0x276 (FPO: [Non-Fpo])
        0018fb18 0082a339 winlogon!WlStateMachineRun+0x16 (FPO: [Non-Fpo])
        0018fb7c 0084566c winlogon!WinMain+0xa74 (FPO: [Non-Fpo])
        0018fc0c 75f33833 winlogon!_initterm_e+0x1a1 (FPO: [Non-Fpo])
        0018fc18 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0018fc58 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 899e7030  Cid 0294.02a0  Teb: 7ffdd000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            9e1e6368  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            899e3020       Image:         winlogon.exe
        Wait Start TickCount      20478          Ticks: 23021 (0:00:05:59.129)
        Context Switch Count      20
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init 9e984000 Current 9e983bc8 Base 9e984000 Limit 9e981000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9e983be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e983c1c 81cad431 nt!KiSwapThread+0x389
        9e983c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        9e983cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        9e983d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        9e983d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9e983d64)
        00e5f798 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00e5f79c 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        00e5f7c8 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        00e5f804 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        00e5f870 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        00e5f87c 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        00e5f8a4 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        00e5f8b0 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        00e5f8bc 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00e5f8fc 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fc36d10  Cid 0294.038c  Teb: 7ffda000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            9fc35310  SynchronizationTimer
            9fc35408  SynchronizationTimer
            9fdaa898  NotificationEvent
            9fc36418  SynchronizationTimer
            835f6ba8  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            899e3020       Image:         winlogon.exe
        Wait Start TickCount      11090          Ticks: 32409 (0:00:08:25.583)
        Context Switch Count      7
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x7744b49a)
        Stack Init 9f2b0000 Current 9f2af8d0 Base 9f2b0000 Limit 9f2ad000 Call 0
        Priority 15 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f2af8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f2af924 81c28c64 nt!KiSwapThread+0x389
        9f2af970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f2afbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f2afd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f2afd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f2afd64)
        0105facc 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0105fad0 7744b65b ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0105fc6c 75f33833 ntdll!TppWaiterpThread+0x294 (FPO: [Non-Fpo])
        0105fc78 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0105fcb8 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Svchost process (DcomLaunch)

```
PROCESS 9e1f2020  SessionId: 0  Cid: 02ec    Peb: 7ffda000  ParentCid: 0214
    DirBase: 29a01080  ObjectTable: 85ae1458  HandleCount: 301.
    Image: svchost.exe
    VadRoot 9e1ea840 Vads 80 Clone 0 Private 509. Modified 132. Locked 0.
    DeviceMap 85a03048
    Token                             9f94f8f0
    ElapsedTime                       00:11:04.200
    UserTime                          00:00:00.546
    KernelTime                        00:00:01.669
    QuotaPoolUsage[PagedPool]         59208
    QuotaPoolUsage[NonPagedPool]      4392
    Working Set Sizes (now,min,max)  (1251, 50, 345) (5004KB, 200KB, 1380KB)
    PeakWorkingSetSize                1449
    VirtualSize                       31 Mb
    PeakVirtualSize                   35 Mb
    PageFaultCount                    34644
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      643

    Setting context for this process...
.process /p /r ffffffff9e1f2020

    !peb
PEB at 7ffda000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00dd0000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00231728 . 0024ed00
    Ldr.InLoadOrderModuleList:           002316a8 . 0024ecf0
    Ldr.InMemoryOrderModuleList:         002316b0 . 0024ecf8
            Base TimeStamp                     Module
          dd0000 4549adc4 Nov 02 08:35:16 2006 C:\Windows\system32\svchost.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        74fa0000 4549bdd7 Nov 02 09:43:51 2006 c:\windows\system32\umpnpmgr.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        75ba0000 4549bde2 Nov 02 09:44:02 2006 c:\windows\system32\USERENV.dll
        75b80000 4549bdd2 Nov 02 09:43:46 2006 c:\windows\system32\Secur32.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        75290000 4549bdd0 Nov 02 09:43:44 2006 C:\Windows\system32\POWRPROF.dll
        75330000 4549bcd7 Nov 02 09:39:35 2006 C:\Windows\system32\GPAPI.dll
        75610000 4679de70 Jun 21 03:12:00 2007 C:\Windows\system32\slc.dll
        74e80000 4549bdac Nov 02 09:43:08 2006 c:\windows\system32\rpcss.dll
        75fe0000 4549be0e Nov 02 09:44:46 2006 C:\Windows\system32\WS2_32.dll
        77550000 4549bdc7 Nov 02 09:43:35 2006 C:\Windows\system32\NSI.dll
        74f30000 46677f3a Jun 07 04:44:58 2007 c:\windows\system32\FirewallAPI.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        753f0000 4549bde4 Nov 02 09:44:04 2006 c:\windows\system32\VERSION.dll
        75480000 4549bd20 Nov 02 09:40:48 2006 C:\Windows\system32\credssp.dll
        75650000 45b96fde Jan 26 03:05:02 2007 C:\Windows\system32\CRYPT32.dll
        75820000 4549bd41 Nov 02 09:41:21 2006 C:\Windows\system32\MSASN1.dll
        75050000 46773a78 Jun 19 03:07:52 2007 C:\Windows\system32\schannel.dll
        75840000 4549bd53 Nov 02 09:41:39 2006 C:\Windows\system32\NETAPI32.dll
```

```
        75ce0000 4549bd99 Nov 02 09:42:49 2006 C:\Windows\system32\PSAPI.DLL
        77030000 4549bdb0 Nov 02 09:43:12 2006 C:\Windows\system32\SETUPAPI.dll
        74f10000 4549bcb8 Nov 02 09:39:04 2006 C:\Windows\system32\Cabinet.dll
        75020000 4549bddb Nov 02 09:43:55 2006 C:\Windows\system32\NTMARTA.DLL
        76310000 4549be44 Nov 02 09:45:40 2006 C:\Windows\system32\WLDAP32.dll
        75ad0000 4549bda8 Nov 02 09:43:04 2006 C:\Windows\system32\SAMLIB.dll
        75300000 4549be2e Nov 02 09:45:18 2006 C:\Windows\system32\WINSTA.dll
        773a0000 4549bce9 Nov 02 09:39:53 2006 C:\Windows\system32\CLBCatQ.DLL
        75b20000 4549bcaf Nov 02 09:38:55 2006 C:\Windows\system32\apphelp.dll
        74fe0000 46d779a1 Aug 31 03:14:57 2007 C:\Windows\system32\WTSAPI32.dll
    SubSystemData:     00000000
    ProcessHeap:       00230000
    ProcessParameters: 00230fd8
    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;C:\Program Files\QuickTime\QTSystem\'
    Environment:  002307e8
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\system32\config\systemprofile\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        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:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\TEMP
        TMP=C:\Windows\TEMP
        USERDOMAIN=WORKGROUP
        USERNAME=HOME$
        USERPROFILE=C:\Windows\system32\config\systemprofile
        windir=C:\Windows
```

```
        THREAD 9e1f2d78  Cid 02ec.02f0  Teb: 7ffdf000 Win32Thread: 00000000 WAIT: (Executive)
UserMode Non-Alertable
            9e1f3b34  NotificationEvent
        IRP List:
            835f4398: (0006,0094) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9e1f2020       Image:         svchost.exe
        Wait Start TickCount      9162           Ticks: 34337 (0:00:08:55.660)
        Context Switch Count      82
        UserTime                  00:00:00.031
        KernelTime                00:00:00.109
        Win32 Start Address svchost!wmainCRTStartup (0x00dd20bf)
        Stack Init 9e8cb000 Current 9e8cabc8 Base 9e8cb000 Limit 9e8c8000 Call 0
        Priority 13 BasePriority 8 PriorityDecrement 5 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9e8cabe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e8cac1c 81c293a7 nt!KiSwapThread+0x389
        9e8cac78 81d88faf nt!KeWaitForSingleObject+0x414
        9e8cacac 81d93669 nt!IopSynchronousServiceTail+0x258
        9e8cad38 81c8caaa nt!NtReadFile+0x646
        9e8cad38 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9e8cad64)
        000df7b8 77490080 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        000df7bc 75f3853f ntdll!ZwReadFile+0xc (FPO: [9,0,0])
        000df834 775cffe2 kernel32!ReadFile+0x20e (FPO: [Non-Fpo])
        000df860 775cfdfb ADVAPI32!ScGetPipeInput+0x2a (FPO: [Non-Fpo])
        000df8c8 775cbdd2 ADVAPI32!ScDispatcherLoop+0x6c (FPO: [Non-Fpo])
        000dfb40 00dd241d ADVAPI32!StartServiceCtrlDispatcherW+0xce (FPO: [Non-Fpo])
        000dfb48 00dd2401 svchost!SvcHostMain+0x12 (FPO: [Non-Fpo])
        000dfb4c 00dd2183 svchost!wmain+0x5 (FPO: [Non-Fpo])
        000dfb90 75f33833 svchost!_initterm_e+0x163 (FPO: [Non-Fpo])
        000dfb9c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        000dfbdc 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 899e5250  Cid 02ec.02fc  Teb: 7ffdc000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            9e1f2b10  SynchronizationTimer
            9e1f3628  SynchronizationEvent
            899c23e8  SynchronizationEvent
            84da0a00  SynchronizationTimer
            84da0948  SynchronizationTimer
            9fc09210  SynchronizationEvent
            9e1ffc88  SynchronizationEvent
            9e1ff0b0  SynchronizationEvent
            9e1f3550  SynchronizationEvent
            9e1ffc50  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9e1f2020       Image:         svchost.exe
        Wait Start TickCount      996            Ticks: 42503 (0:00:11:03.051)
        Context Switch Count      24
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x7744b49a)
        Stack Init 9e9e4000 Current 9e9e38d0 Base 9e9e4000 Limit 9e9e1000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9e9e38e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e9e3924 81c28c64 nt!KiSwapThread+0x389
        9e9e3970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9e9e3bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9e9e3d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9e9e3d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9e9e3d64)
        008dfd6c 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        008dfd70 7744b65b ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        008dff0c 75f33833 ntdll!TppWaiterpThread+0x294 (FPO: [Non-Fpo])
        008dff18 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        008dff58 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9e1fa8b0  Cid 02ec.0308  Teb: 7ffd8000 Win32Thread: ff4e2760 WAIT: (UserRequest)
UserMode Alertable
            82f41fd0  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9e1f2020       Image:         svchost.exe
        Wait Start TickCount      42017          Ticks: 1482 (0:00:00:23.119)
        Context Switch Count      267
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address umpnpmgr!DeviceEventThreadProc (0x74fa174f)
        Stack Init 9e9a8000 Current 9e9a7c70 Base 9e9a8000 Limit 9e9a5000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9e9a7c88 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e9a7cc4 81c293a7 nt!KiSwapThread+0x389
        9e9a7d24 81db9e52 nt!KeWaitForSingleObject+0x414
        9e9a7d4c 81c8caaa nt!NtGetPlugPlayEvent+0x11c
        9e9a7d4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9e9a7d64)
        0095f360 7748fa00 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0095f364 74fa17bb ntdll!NtGetPlugPlayEvent+0xc (FPO: [4,0,0])
        0095f7d4 75f33833 umpnpmgr!DeviceEventThreadProc+0x9a (FPO: [Non-Fpo])
        0095f7e0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0095f820 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fc08b98  Cid 02ec.0318  Teb: 7ffde000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Alertable
            9e1ea198  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9e1f2020       Image:         svchost.exe
        Wait Start TickCount      996            Ticks: 42503 (0:00:11:03.051)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init 9e9b4000 Current 9e9b3bc8 Base 9e9b4000 Limit 9e9b1000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9e9b3be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e9b3c1c 81cad431 nt!KiSwapThread+0x389
        9e9b3c68 81d8b982 nt!KeRemoveQueueEx+0x568
        9e9b3cc0 81c7a036 nt!IoRemoveIoCompletion+0x23
        9e9b3d54 81c8caaa nt!NtWaitForWorkViaWorkerFactory+0x1a1
        9e9b3d54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9e9b3d64)
        00e3fa78 77490850 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00e3fa7c 7749a1b4 ntdll!NtWaitForWorkViaWorkerFactory+0xc (FPO: [2,0,0])
        00e3fba4 75f33833 ntdll!TppWorkerThread+0x1f6 (FPO: [Non-Fpo])
        00e3fbb0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00e3fbf0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fc088e0  Cid 02ec.031c  Teb: 7ffd6000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Alertable
            9fc09d68  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9e1f2020       Image:         svchost.exe
        Wait Start TickCount      996            Ticks: 42503 (0:00:11:03.051)
        Context Switch Count      14
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init 9e98c000 Current 9e98bbc8 Base 9e98c000 Limit 9e989000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9e98bbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e98bc1c 81cad431 nt!KiSwapThread+0x389
        9e98bc68 81d8b982 nt!KeRemoveQueueEx+0x568
        9e98bcc0 81c7a036 nt!IoRemoveIoCompletion+0x23
        9e98bd54 81c8caaa nt!NtWaitForWorkViaWorkerFactory+0x1a1
        9e98bd54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9e98bd64)
        0112fafc 77490850 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0112fb00 7749a1b4 ntdll!NtWaitForWorkViaWorkerFactory+0xc (FPO: [2,0,0])
        0112fc28 75f33833 ntdll!TppWorkerThread+0x1f6 (FPO: [Non-Fpo])
        0112fc34 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0112fc74 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 83789d28  Cid 02ec.08f0  Teb: 7ffdd000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            9e1ead10  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9e1f2020       Image:         svchost.exe
        Wait Start TickCount      30990          Ticks: 12509 (0:00:03:15.141)
        Context Switch Count      172
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init a0939000 Current a0938bc8 Base a0939000 Limit a0936000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a0938be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0938c1c 81cad431 nt!KiSwapThread+0x389
        a0938c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a0938cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a0938d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a0938d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0938d64)
        010bfe18 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        010bfe1c 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        010bfe48 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        010bfe84 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        010bfef0 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        010bfefc 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        010bff20 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        010bff2c 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        010bff38 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        010bff78 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Svchost process (rpcss)

```
PROCESS 9e1fd468  SessionId: 0  Cid: 0324    Peb: 7ffdc000  ParentCid: 0214
    DirBase: 29a01140  ObjectTable: 9f9a44b8  HandleCount: 343.
    Image: svchost.exe
    VadRoot 9fc10bf0 Vads 76 Clone 0 Private 738. Modified 131. Locked 3.
    DeviceMap 9f999328
    Token                             9f9a8030
    ElapsedTime                       00:11:03.982
    UserTime                          00:00:00.124
    KernelTime                        00:00:00.093
    QuotaPoolUsage[PagedPool]         64800
    QuotaPoolUsage[NonPagedPool]      7952
    Working Set Sizes (now,min,max)  (1380, 50, 345) (5520KB, 200KB, 1380KB)
    PeakWorkingSetSize                1459
    VirtualSize                       31 Mb
    PeakVirtualSize                   31 Mb
    PageFaultCount                    1862
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      873

    Setting context for this process...
.process /p /r ffffffff9e1fd468

    !peb
PEB at 7ffdc000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00dd0000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 001a17a8 . 001bdeb0
    Ldr.InLoadOrderModuleList:           001a1728 . 001bdea0
    Ldr.InMemoryOrderModuleList:         001a1730 . 001bdea8
            Base TimeStamp                     Module
          dd0000 4549adc4 Nov 02 08:35:16 2006 C:\Windows\system32\svchost.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        74e80000 4549bdac Nov 02 09:43:08 2006 c:\windows\system32\rpcss.dll
        75fe0000 4549be0e Nov 02 09:44:46 2006 C:\Windows\system32\WS2_32.dll
        77550000 4549bdc7 Nov 02 09:43:35 2006 C:\Windows\system32\NSI.dll
        75b80000 4549bdd2 Nov 02 09:43:46 2006 c:\windows\system32\Secur32.dll
        74f30000 46677f3a Jun 07 04:44:58 2007 c:\windows\system32\FirewallAPI.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        753f0000 4549bde4 Nov 02 09:44:04 2006 c:\windows\system32\VERSION.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        75480000 4549bd20 Nov 02 09:40:48 2006 C:\Windows\system32\credssp.dll
        75650000 45b96fde Jan 26 03:05:02 2007 C:\Windows\system32\CRYPT32.dll
        75820000 4549bd41 Nov 02 09:41:21 2006 C:\Windows\system32\MSASN1.dll
        75ba0000 4549bde2 Nov 02 09:44:02 2006 C:\Windows\system32\USERENV.dll
        75050000 46773a78 Jun 19 03:07:52 2007 C:\Windows\system32\schannel.dll
        75840000 4549bd53 Nov 02 09:41:39 2006 C:\Windows\system32\NETAPI32.dll
        75ce0000 4549bd99 Nov 02 09:42:49 2006 C:\Windows\system32\PSAPI.DLL
        75350000 4549bdae Nov 02 09:43:10 2006 C:\Windows\system32\rsaenh.dll
        75250000 4549bd69 Nov 02 09:42:01 2006 C:\Windows\system32\mswsock.dll
        752c0000 4549be27 Nov 02 09:45:11 2006 C:\Windows\System32\wshtcpip.dll
```

```
        752b0000 4549be21 Nov 02 09:45:05 2006 C:\Windows\System32\wship6.dll
        773a0000 4549bce9 Nov 02 09:39:53 2006 C:\Windows\system32\CLBCatQ.DLL
        735b0000 4549bce0 Nov 02 09:39:44 2006 C:\Windows\system32\fwpuclnt.dll
    SubSystemData:     00000000
    ProcessHeap:       001a0000
    ProcessParameters: 001a1060
    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;C:\Program Files\QuickTime\QTSystem\'
    Environment:  001a07e8
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        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;C:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        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=WORKGROUP
        USERNAME=HOME$
        USERPROFILE=C:\Windows\ServiceProfiles\NetworkService
        windir=C:\Windows
```

```
        THREAD 9e1fd1c0  Cid 0324.0328  Teb: 7ffdf000 Win32Thread: 00000000 WAIT: (Executive)
UserMode Non-Alertable
            9e1fd794  NotificationEvent
        IRP List:
            899593e0: (0006,0094) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            9e1fd468       Image:         svchost.exe
        Wait Start TickCount      997            Ticks: 42502 (0:00:11:03.035)
        Context Switch Count      11
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address svchost!wmainCRTStartup (0x00dd20bf)
        Stack Init 9f2d0000 Current 9f2cfbc8 Base 9f2d0000 Limit 9f2cd000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f2cfbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f2cfc1c 81c293a7 nt!KiSwapThread+0x389
        9f2cfc78 81d88faf nt!KeWaitForSingleObject+0x414
        9f2cfcac 81d93669 nt!IopSynchronousServiceTail+0x258
        9f2cfd38 81c8caaa nt!NtReadFile+0x646
        9f2cfd38 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f2cfd64)
        000efaac 77490080 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        000efab0 75f3853f ntdll!ZwReadFile+0xc (FPO: [9,0,0])
        000efb28 775cffe2 kernel32!ReadFile+0x20e (FPO: [Non-Fpo])
        000efb54 775cfdfb ADVAPI32!ScGetPipeInput+0x2a (FPO: [Non-Fpo])
        000efbbc 775cbdd2 ADVAPI32!ScDispatcherLoop+0x6c (FPO: [Non-Fpo])
        000efe34 00dd241d ADVAPI32!StartServiceCtrlDispatcherW+0xce (FPO: [Non-Fpo])
        000efe3c 00dd2401 svchost!SvcHostMain+0x12 (FPO: [Non-Fpo])
        000efe40 00dd2183 svchost!wmain+0x5 (FPO: [Non-Fpo])
        000efe84 75f33833 svchost!_initterm_e+0x163 (FPO: [Non-Fpo])
        000efe90 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        000efed0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fc0d748  Cid 0324.032c  Teb: 7ffde000 Win32Thread: ff4e08c0 WAIT: (DelayExecution)
UserMode Non-Alertable
            9fc0d7d0  NotificationTimer
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            9e1fd468       Image:         svchost.exe
        Wait Start TickCount      42972          Ticks: 527 (0:00:00:08.221)
        Context Switch Count      105
        UserTime                  00:00:00.015
        KernelTime                00:00:00.015
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x775cb9d5)
        Stack Init 9f2cc000 Current 9f2cbc58 Base 9f2cc000 Limit 9f2c9000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f2cbc70 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f2cbcac 81cac48e nt!KiSwapThread+0x389
        9f2cbd08 81e90bf1 nt!KeDelayExecutionThread+0x397
        9f2cbd54 81c8caaa nt!NtDelayExecution+0x8d
        9f2cbd54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f2cbd64)
        0068f8b4 7748f7c0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0068f8b8 75f378e0 ntdll!NtDelayExecution+0xc (FPO: [2,0,0])
        0068f920 74e81a4f kernel32!SleepEx+0x62 (FPO: [Non-Fpo])
        0068f92c 74ea8da2 rpcss!CTime::Sleep+0x2a (FPO: [Non-Fpo])
        0068f978 74ea0220 rpcss!ObjectExporterWorkerThread+0x322 (FPO: [Non-Fpo])
        0068f988 74ea1c6e rpcss!ScmServiceMain+0xb8 (FPO: [Non-Fpo])
        0068f9b8 00dd148a rpcss!ServiceMain+0x117 (FPO: [Non-Fpo])
        0068f9e4 775cb9f6 svchost!ServiceStarter+0x17a (FPO: [Non-Fpo])
        0068f9f8 75f33833 ADVAPI32!ScSvcctrlThreadA+0x21 (FPO: [Non-Fpo])
        0068fa04 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0068fa44 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fc0c030  Cid 0324.0330  Teb: 7ffdd000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            9fc0d530  SynchronizationTimer
            9fc0d3e8  SynchronizationEvent
            9fc10f60  SynchronizationEvent
            9fc10ee8  SynchronizationEvent
            9fc10c48  SynchronizationEvent
            9fd00368  SynchronizationTimer
            9fd53678  SynchronizationEvent
            9fc0f7b8  SynchronizationEvent
            9fd28c20  SynchronizationTimer
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            9e1fd468       Image:         svchost.exe
        Wait Start TickCount      39562          Ticks: 3937 (0:00:01:01.417)
        Context Switch Count      23
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x7744b49a)
        Stack Init 9f2d4000 Current 9f2d38d0 Base 9f2d4000 Limit 9f2d1000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f2d38e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f2d3924 81c28c64 nt!KiSwapThread+0x389
        9f2d3970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f2d3bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f2d3d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f2d3d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f2d3d64)
        006ffd58 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        006ffd5c 7744b65b ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        006ffef8 75f33833 ntdll!TppWaiterpThread+0x294 (FPO: [Non-Fpo])
        006fff04 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        006fff44 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fd00d78  Cid 0324.0534  Teb: 7ffd7000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Alertable
            9fc0d6e8  QueueObject
        IRP List:
            83606df0: (0006,0100) Flags: 00060030  Mdl: 00000000
            84daca68: (0006,01d8) Flags: 00060030  Mdl: 00000000
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            9e1fd468       Image:         svchost.exe
        Wait Start TickCount      9805           Ticks: 33694 (0:00:08:45.629)
        Context Switch Count      29
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init a09b1000 Current a09b0bc8 Base a09b1000 Limit a09ae000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 3 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a09b0be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a09b0c1c 81cad431 nt!KiSwapThread+0x389
        a09b0c68 81d8b982 nt!KeRemoveQueueEx+0x568
        a09b0cc0 81c7a036 nt!IoRemoveIoCompletion+0x23
        a09b0d54 81c8caaa nt!NtWaitForWorkViaWorkerFactory+0x1a1
        a09b0d54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a09b0d64)
        009ffc1c 77490850 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        009ffc20 7749a1b4 ntdll!NtWaitForWorkViaWorkerFactory+0xc (FPO: [2,0,0])
        009ffd48 75f33833 ntdll!TppWorkerThread+0x1f6 (FPO: [Non-Fpo])
        009ffd54 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        009ffd94 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 835e67e0  Cid 0324.0adc  Teb: 7ffd8000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            9fc0c800  QueueObject
            835e6868  NotificationTimer
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            9e1fd468       Image:         svchost.exe
        Wait Start TickCount      42898          Ticks: 601 (0:00:00:09.375)
        Context Switch Count      1639
        UserTime                  00:00:00.046
        KernelTime                00:00:00.062
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init a1eda000 Current a1ed9bc8 Base a1eda000 Limit a1ed7000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a1ed9be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1ed9c1c 81cad431 nt!KiSwapThread+0x389
        a1ed9c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a1ed9cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a1ed9d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a1ed9d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1ed9d64)
        0134fe18 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0134fe1c 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        0134fe48 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        0134fe84 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        0134fef0 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        0134fefc 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        0134ff20 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        0134ff2c 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        0134ff38 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0134ff78 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 838efd78  Cid 0324.04e8  Teb: 7ffdb000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            9fc0c800  QueueObject
            838efe00  NotificationTimer
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            9e1fd468       Image:         svchost.exe
        Wait Start TickCount      43483          Ticks: 16 (0:00:00:00.249)
        Context Switch Count      541
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init a09a5000 Current a09a4bc8 Base a09a5000 Limit a09a2000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a09a4be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a09a4c1c 81cad431 nt!KiSwapThread+0x389
        a09a4c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a09a4cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a09a4d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a09a4d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a09a4d64)
        0121fd20 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0121fd24 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        0121fd50 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        0121fd8c 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        0121fdf8 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        0121fe04 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        0121fe2c 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        0121fe38 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        0121fe44 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0121fe84 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 8366f2a0  Cid 0324.0ae4  Teb: 7ffd9000 Win32Thread: 00000000 WAIT: (DelayExecution)
UserMode Non-Alertable
            8366f328  NotificationTimer
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            9e1fd468       Image:         svchost.exe
        Wait Start TickCount      41690          Ticks: 1809 (0:00:00:28.220)
        Context Switch Count      81
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address rpcss!ObjectExporterTaskThread (0x74ea94ea)
        Stack Init a09ad000 Current a09acc58 Base a09ad000 Limit a09aa000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a09acc70 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a09accac 81cac48e nt!KiSwapThread+0x389
        a09acd08 81e90bf1 nt!KeDelayExecutionThread+0x397
        a09acd54 81c8caaa nt!NtDelayExecution+0x8d
        a09acd54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a09acd64)
        00f2fc5c 7748f7c0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00f2fc60 75f378e0 ntdll!NtDelayExecution+0xc (FPO: [2,0,0])
        00f2fcc8 74e81a4f kernel32!SleepEx+0x62 (FPO: [Non-Fpo])
        00f2fcd4 74ea9599 rpcss!CTime::Sleep+0x2a (FPO: [Non-Fpo])
        00f2fcf0 75f33833 rpcss!ObjectExporterTaskThread+0xe5 (FPO: [Non-Fpo])
        00f2fcfc 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00f2fd3c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 83715cd0  Cid 0324.02c8  Teb: 7ffda000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            9fc0c800  QueueObject
            83715d58  NotificationTimer
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            9e1fd468       Image:         svchost.exe
        Wait Start TickCount      41598          Ticks: 1901 (0:00:00:29.655)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init a6883000 Current a6882bc8 Base a6883000 Limit a6880000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a6882be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a6882c1c 81cad431 nt!KiSwapThread+0x389
        a6882c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a6882cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a6882d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a6882d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a6882d64)
        00e7f708 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00e7f70c 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        00e7f738 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        00e7f774 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        00e7f7e0 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        00e7f7ec 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        00e7f814 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        00e7f820 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        00e7f82c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00e7f86c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Svchost process (secsvcs)

```
PROCESS 9fc4a020  SessionId: 0  Cid: 0350    Peb: 7ffd8000  ParentCid: 0214
    DirBase: 29a01160  ObjectTable: 9f9d2f80  HandleCount: 323.
    Image: svchost.exe
    VadRoot 9fcc4b80 Vads 161 Clone 0 Private 4405. Modified 5479. Locked 0.
    DeviceMap 85a03048
    Token                             9f9d7ab8
    ElapsedTime                       00:11:03.920
    UserTime                          00:00:07.612
    KernelTime                        00:00:01.263
    QuotaPoolUsage[PagedPool]         93504
    QuotaPoolUsage[NonPagedPool]      9568
    Working Set Sizes (now,min,max)  (1727, 50, 345) (6908KB, 200KB, 1380KB)
    PeakWorkingSetSize                9267
    VirtualSize                       66 Mb
    PeakVirtualSize                   77 Mb
    PageFaultCount                    56406
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      5090

    Setting context for this process...
.process /p /r ffffffff9fc4a020

    !peb
PEB at 7ffd8000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00dd0000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00351720 . 003b2f40
    Ldr.InLoadOrderModuleList:           003516a0 . 003b2f30
    Ldr.InMemoryOrderModuleList:         003516a8 . 003b2f38
            Base TimeStamp                     Module
          dd0000 4549adc4 Nov 02 08:35:16 2006 C:\Windows\System32\svchost.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        74de0000 45ad8fe9 Jan 17 02:54:33 2007 c:\program files\windows defender\mpsvc.dll
        753f0000 4549bde4 Nov 02 09:44:04 2006 C:\Windows\system32\VERSION.dll
        75650000 45b96fde Jan 26 03:05:02 2007 C:\Windows\system32\CRYPT32.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        75820000 4549bd41 Nov 02 09:41:21 2006 C:\Windows\system32\MSASN1.dll
        75ba0000 4549bde2 Nov 02 09:44:02 2006 C:\Windows\system32\USERENV.dll
        75b80000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\Secur32.dll
        74ff0000 4549be2f Nov 02 09:45:19 2006 C:\Windows\system32\WINTRUST.dll
        77580000 462434a3 Apr 17 03:44:51 2007 C:\Windows\system32\imagehlp.dll
        74e30000 45ad8fe2 Jan 17 02:54:26 2007 c:\program files\windows defender\MpClient.dll
        76560000 4681c95d Jun 27 03:20:13 2007 C:\Windows\system32\SHELL32.dll
        763b0000 4549bdb9 Nov 02 09:43:21 2006 C:\Windows\system32\SHLWAPI.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        74aa0000 4549bd09 Nov 02 09:40:25 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_5d07289e07e1d100\comctl32.dll
        75330000 4549bcd7 Nov 02 09:39:35 2006 C:\Windows\System32\GPAPI.dll
        75610000 4679de70 Jun 21 03:12:00 2007 C:\Windows\System32\slc.dll
        75020000 4549bddb Nov 02 09:43:55 2006 C:\Windows\System32\NTMARTA.DLL
```

```
        76310000 4549be44 Nov 02 09:45:40 2006 C:\Windows\system32\WLDAP32.dll
        75fe0000 4549be0e Nov 02 09:44:46 2006 C:\Windows\system32\WS2_32.dll
        77550000 4549bdc7 Nov 02 09:43:35 2006 C:\Windows\system32\NSI.dll
        75ce0000 4549bd99 Nov 02 09:42:49 2006 C:\Windows\system32\PSAPI.DLL
        75ad0000 4549bda8 Nov 02 09:43:04 2006 C:\Windows\System32\SAMLIB.dll
        75350000 4549bdae Nov 02 09:43:10 2006 C:\Windows\System32\rsaenh.dll
        754f0000 4549bd49 Nov 02 09:41:29 2006 C:\Windows\System32\ncrypt.dll
        754a0000 4549bcb9 Nov 02 09:39:05 2006 C:\Windows\System32\BCRYPT.dll
        740d0000 4754dff4 Dec 04 05:04:52 2007 C:\ProgramData\Microsoft\Windows Defender\Definition
Updates\{F85625E4-AA62-4A95-9603-5727C94F2B85}\mpengine.dll
        75840000 4549bd53 Nov 02 09:41:39 2006 C:\Windows\system32\NETAPI32.DLL
        74d20000 4549bd8c Nov 02 09:42:36 2006 C:\Windows\system32\KTMW32.DLL
        755b0000 4549bd3f Nov 02 09:41:19 2006 C:\Windows\system32\iphlpapi.dll
        75570000 46807ea6 Jun 26 03:49:10 2007 C:\Windows\System32\dhcpcsvc.DLL
        75af0000 4549bcf1 Nov 02 09:40:01 2006 C:\Windows\System32\DNSAPI.dll
        75560000 4549be1e Nov 02 09:45:02 2006 C:\Windows\System32\WINNSI.DLL
        75540000 46807ea7 Jun 26 03:49:11 2007 C:\Windows\System32\dhcpcsvc6.DLL
        736a0000 45ad8fe6 Jan 17 02:54:30 2007 c:\program files\windows defender\mprtplug.dll
        73480000 4549bde5 Nov 02 09:44:05 2006 C:\Windows\System32\tdh.dll
        75480000 4549bd20 Nov 02 09:40:48 2006 C:\Windows\System32\credssp.dll
        75050000 46773a78 Jun 19 03:07:52 2007 C:\Windows\system32\schannel.dll
        773a0000 4549bce9 Nov 02 09:39:53 2006 C:\Windows\system32\CLBCatQ.DLL
    SubSystemData:     00000000
    ProcessHeap:       00350000
    ProcessParameters: 00350fd8
    WindowTitle:  'C:\Windows\System32\svchost.exe'
    ImageFile:    'C:\Windows\System32\svchost.exe'
    CommandLine:  'C:\Windows\System32\svchost.exe -k secsvcs'
    DllPath:
'C:\Windows\System32;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Wind
ows;C:\Windows\System32\Wbem;C:\Program Files\QuickTime\QTSystem\'
    Environment:  0037c080
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\system32\config\systemprofile\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        LOCALAPPDATA=C:\Windows\system32\config\systemprofile\AppData\Local
        MpConfig_ProductAppDataPath=C:\ProgramData\Microsoft\Windows Defender
        MpConfig_ProductCodeName=AntiSpyware
        MpConfig_ProductPath=c:\program files\windows defender

MpConfig_ProductUserAppDataPath=C:\Windows\system32\config\systemprofile\AppData\Local\Microsoft\Wi
ndows Defender
        MpConfig_ReportingGUID=9E105B54-307A-4903-9E49-E8DE56BD66B8
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\TEMP
        TMP=C:\Windows\TEMP
        USERDOMAIN=WORKGROUP
        USERNAME=HOME$
        USERPROFILE=C:\Windows\system32\config\systemprofile
        windir=C:\Windows
```

```
        THREAD 9fc4a598  Cid 0350.0354  Teb: 7ffdf000 Win32Thread: 00000000 WAIT: (Executive)
UserMode Non-Alertable
            9fc4beb4  NotificationEvent
        IRP List:
            9fc4a8d8: (0006,0094) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc4a020       Image:         svchost.exe
        Wait Start TickCount      1000           Ticks: 42499 (0:00:11:02.988)
        Context Switch Count      15
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address svchost!wmainCRTStartup (0x00dd20bf)
        Stack Init 9f2f4000 Current 9f2f3bc8 Base 9f2f4000 Limit 9f2f1000 Call 0
        Priority 13 BasePriority 8 PriorityDecrement 4 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f2f3be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f2f3c1c 81c293a7 nt!KiSwapThread+0x389
        9f2f3c78 81d88faf nt!KeWaitForSingleObject+0x414
        9f2f3cac 81d93669 nt!IopSynchronousServiceTail+0x258
        9f2f3d38 81c8caaa nt!NtReadFile+0x646
        9f2f3d38 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f2f3d64)
        0017f71c 77490080 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0017f720 75f3853f ntdll!ZwReadFile+0xc (FPO: [9,0,0])
        0017f798 775cffe2 kernel32!ReadFile+0x20e (FPO: [Non-Fpo])
        0017f7c4 775cfdfb ADVAPI32!ScGetPipeInput+0x2a (FPO: [Non-Fpo])
        0017f82c 775cbdd2 ADVAPI32!ScDispatcherLoop+0x6c (FPO: [Non-Fpo])
        0017faa4 00dd241d ADVAPI32!StartServiceCtrlDispatcherW+0xce (FPO: [Non-Fpo])
        0017faac 00dd2401 svchost!SvcHostMain+0x12 (FPO: [Non-Fpo])
        0017fab0 00dd2183 svchost!wmain+0x5 (FPO: [Non-Fpo])
        0017faf4 75f33833 svchost!_initterm_e+0x163 (FPO: [Non-Fpo])
        0017fb00 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0017fb40 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fc21030  Cid 0350.0390  Teb: 7ffdd000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            9fc280f8  SynchronizationTimer
            899e3a90  SynchronizationEvent
            9fc22510  SynchronizationEvent
            9fc21400  SynchronizationEvent
            9fc4d788  NotificationEvent
            899f51f0  SynchronizationEvent
            9fc39488  SynchronizationEvent
            9fd4aaa8  SynchronizationEvent
            9fd4ac10  SynchronizationEvent
            9fd6e9b0  SynchronizationEvent
            9fd6ec38  SynchronizationTimer
            9fd6e5f8  SynchronizationTimer
            9fc2f944  NotificationEvent
            9fc3d568  SynchronizationEvent
            9fc3d6c0  SynchronizationEvent
            9fc3d798  SynchronizationEvent
            9fc39708  SynchronizationEvent
            9fc3ac88  SynchronizationEvent
            9fc42060  SynchronizationEvent
            9fc3a828  SynchronizationEvent
            9fc41c18  SynchronizationEvent
            9fc45428  SynchronizationEvent
            9fc45548  SynchronizationEvent
            9fc3a5d0  SynchronizationEvent
            9fc3ab90  SynchronizationEvent
            9fc41c48  SynchronizationEvent
            9fc2efa8  SynchronizationEvent
            9fc412f0  SynchronizationEvent
            9fc3a8a0  SynchronizationEvent
            9fc3aa48  SynchronizationEvent
            9fc3aaf0  SynchronizationEvent
            9fc3aed0  SynchronizationEvent
            9fc38898  SynchronizationEvent
            9fc25088  SynchronizationEvent
            8363ed00  NotificationEvent
            836149c0  NotificationEvent
            9fd6e760  SynchronizationTimer
            9fd8a680  SynchronizationEvent
            9fdb9468  SynchronizationTimer
            9fc210b8  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc4a020       Image:         svchost.exe
        Wait Start TickCount      39659          Ticks: 3840 (0:00:00:59.904)
        Context Switch Count      1080
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address ntdll!TppWaiterpThread (0x7744b49a)
        Stack Init 9f2b4000 Current 9f2b38d0 Base 9f2b4000 Limit 9f2b1000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f2b38e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f2b3924 81c28c64 nt!KiSwapThread+0x389
        9f2b3970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f2b3bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f2b3d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f2b3d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f2b3d64)
        0099f6e4 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0099f6e8 7744b65b ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0099f884 75f33833 ntdll!TppWaiterpThread+0x294 (FPO: [Non-Fpo])
        0099f890 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0099f8d0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fc23d78  Cid 0350.039c  Teb: 7ffde000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Alertable
            9fc226d0  QueueObject
        IRP List:
            847ce868: (0006,01d8) Flags: 00060000  Mdl: 00000000
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc4a020       Image:         svchost.exe
        Wait Start TickCount      39659          Ticks: 3840 (0:00:00:59.904)
        Context Switch Count      43
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init 9e9c0000 Current 9e9bfbc8 Base 9e9c0000 Limit 9e9bd000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9e9bfbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e9bfc1c 81cad431 nt!KiSwapThread+0x389
        9e9bfc68 81d8b982 nt!KeRemoveQueueEx+0x568
        9e9bfcc0 81c7a036 nt!IoRemoveIoCompletion+0x23
        9e9bfd54 81c8caaa nt!NtWaitForWorkViaWorkerFactory+0x1a1
        9e9bfd54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9e9bfd64)
        002df6cc 77490850 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        002df6d0 7749a1b4 ntdll!NtWaitForWorkViaWorkerFactory+0xc (FPO: [2,0,0])
        002df7f8 75f33833 ntdll!TppWorkerThread+0x1f6 (FPO: [Non-Fpo])
        002df804 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        002df844 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fc46030  Cid 0350.03dc  Teb: 7ffd9000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fc2a528  NotificationEvent
            9fc3e3d0  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc4a020       Image:         svchost.exe
        Wait Start TickCount      22067          Ticks: 21432 (0:00:05:34.341)
        Context Switch Count      9
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address mpsvc!HealthMonitor (0x74dec756)
        Stack Init 9f2c4000 Current 9f2c38d0 Base 9f2c4000 Limit 9f2c1000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f2c38e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f2c3924 81c28c64 nt!KiSwapThread+0x389
        9f2c3970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f2c3bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f2c3d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f2c3d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f2c3d64)
        0127fa58 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0127fa5c 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0127faf8 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0127fb14 74dec80a kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0127fda4 75f33833 mpsvc!HealthMonitor+0xb4 (FPO: [Non-Fpo])
        0127fdb0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0127fdf0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fc469f0  Cid 0350.03e0  Teb: 7ffd7000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fd2291c  NotificationEvent
            9fc3fe88  NotificationEvent
        IRP List:
            9fd52bd8: (0006,01d8) Flags: 00060000  Mdl: 00000000
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc4a020       Image:         svchost.exe
        Wait Start TickCount      20439          Ticks: 23060 (0:00:05:59.738)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address mpsvc!UpdateXcopyWorker (0x74df9baa)
        Stack Init 9f27c000 Current 9f27b8d0 Base 9f27c000 Limit 9f279000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f27b8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f27b924 81c28c64 nt!KiSwapThread+0x389
        9f27b970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f27bbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f27bd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f27bd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f27bd64)
        0133f924 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0133f928 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0133f9c4 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0133f9e0 74df9dbb kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0133fe8c 75f33833 mpsvc!UpdateXcopyWorker+0x211 (FPO: [Non-Fpo])
        0133fe98 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0133fed8 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fd6d660  Cid 0350.063c  Teb: 7ffdc000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fd6eb48  NotificationEvent
            9fd6eb78  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc4a020       Image:         svchost.exe
        Wait Start TickCount      10001          Ticks: 33498 (0:00:08:42.572)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address mpsvc!EventDispatcher (0x74defa8f)
        Stack Init 9e897000 Current 9e8968d0 Base 9e897000 Limit 9e894000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9e8968e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e896924 81c28c64 nt!KiSwapThread+0x389
        9e896970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9e896bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9e896d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9e896d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9e896d64)
        016ff794 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        016ff798 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        016ff834 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        016ff850 74defae3 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        016ff884 75f33833 mpsvc!EventDispatcher+0x54 (FPO: [Non-Fpo])
        016ff890 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        016ff8d0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fdb9030  Cid 0350.0640  Teb: 7ffd5000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fd6ea90  NotificationEvent
            9fd6ea20  NotificationEvent
            9fd6d620  NotificationEvent
            9fd6d5b0  NotificationEvent
            9fd6d540  NotificationEvent
            9fd6d4d0  NotificationEvent
            9fd6d460  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc4a020       Image:         svchost.exe
        Wait Start TickCount      18671          Ticks: 24828 (0:00:06:27.319)
        Context Switch Count      242
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address mpsvc!WorkDispatcher (0x74dee944)
        Stack Init a0808000 Current a08078d0 Base a0808000 Limit a0805000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a08078e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0807924 81c28c64 nt!KiSwapThread+0x389
        a0807970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a0807bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a0807d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a0807d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0807d64)
        0162fc34 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0162fc38 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0162fcd4 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0162fcf0 74e45890 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0162fd18 74dee9aa MpClient!InternalMpWaitForMultipleObjects+0x2a (FPO: [Non-Fpo])
        0162fd80 75f33833 mpsvc!WorkDispatcher+0x66 (FPO: [Non-Fpo])
        0162fd8c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0162fdcc 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fd22ac0  Cid 0350.0650  Teb: 7ffd4000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fd89bf0  NotificationEvent
            9fd87dc8  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc4a020       Image:         svchost.exe
        Wait Start TickCount      18671          Ticks: 24828 (0:00:06:27.319)
        Context Switch Count      90
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address mprtplug!RTPNotificationWorker (0x736a2458)
        Stack Init a0828000 Current a08278d0 Base a0828000 Limit a0825000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a08278e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0827924 81c28c64 nt!KiSwapThread+0x389
        a0827970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a0827bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a0827d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a0827d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0827d64)
        0187fb4c 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0187fb50 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0187fbec 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0187fc08 736a24c1 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0187fc48 75f33833 mprtplug!RTPNotificationWorker+0x69 (FPO: [Non-Fpo])
        0187fc54 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0187fc94 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 8345cd78  Cid 0350.08c8  Teb: 7ffaf000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            899e80e8  NotificationEvent
        IRP List:
            8379dc60: (0006,0094) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc4a020       Image:         svchost.exe
        Wait Start TickCount      29247          Ticks: 14252 (0:00:03:42.332)
        Context Switch Count      75
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address mprtplug!ProcessEventsThread (0x736a876f)
        Stack Init 9e998000 Current 9e997c38 Base 9e998000 Limit 9e995000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9e997c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e997c8c 81c293a7 nt!KiSwapThread+0x389
        9e997ce8 81df5057 nt!KeWaitForSingleObject+0x414
        9e997d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        9e997d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9e997d64)
        018bf94c 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        018bf950 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        018bf9c0 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        018bf9d4 775d126c kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        018bfa14 775c0a06 ADVAPI32!EtwpProcessRealTimeTraces+0x9e (FPO: [Non-Fpo])
        018bfd5c 736a87c9 ADVAPI32!ProcessTrace+0x30a (FPO: [Non-Fpo])
        018bfd84 75f33833 mprtplug!ProcessEventsThread+0x5a (FPO: [Non-Fpo])
        018bfd90 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        018bfdd0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fdbcd30  Cid 0350.040c  Teb: 7ffda000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            89962890  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc4a020       Image:         svchost.exe
        Wait Start TickCount      28862          Ticks: 14637 (0:00:03:48.338)
        Context Switch Count      7
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init 9f724000 Current 9f723bc8 Base 9f724000 Limit 9f721000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f723be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f723c1c 81cad431 nt!KiSwapThread+0x389
        9f723c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        9f723cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        9f723d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        9f723d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f723d64)
        01baf7a0 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01baf7a4 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        01baf7d0 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        01baf80c 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        01baf878 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        01baf884 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        01baf8ac 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        01baf8b8 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        01baf8c4 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01baf904 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 839f2ac0  Cid 0350.0370  Teb: 7ffd6000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fd6e6b0  NotificationEvent
            839f2b48  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc4a020       Image:         svchost.exe
        Wait Start TickCount      39659          Ticks: 3840 (0:00:00:59.904)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address mpsvc!PurgeThreadProc (0x74dfe3e0)
        Stack Init a1ed2000 Current a1ed1c38 Base a1ed2000 Limit a1ecf000 Call 0
        Priority 4 BasePriority 4 PriorityDecrement 0 IoPriority 0 PagePriority 1
        ChildEBP RetAddr
        a1ed1c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1ed1c8c 81c293a7 nt!KiSwapThread+0x389
        a1ed1ce8 81df5057 nt!KeWaitForSingleObject+0x414
        a1ed1d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a1ed1d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1ed1d64)
        01cbfc28 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01cbfc2c 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        01cbfc9c 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        01cbfcb0 74dfe4af kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        01cbfcd0 75f33833 mpsvc!PurgeThreadProc+0xcf (FPO: [Non-Fpo])
        01cbfcdc 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01cbfd1c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Svchost process (LocalServiceNetworkRestricted)

```
PROCESS 8485e910  SessionId: 0  Cid: 03a4    Peb: 7ffdd000  ParentCid: 0214
    DirBase: 29a011a0  ObjectTable: a00386c8  HandleCount: 432.
    Image: svchost.exe
    VadRoot 899d5bf8 Vads 157 Clone 0 Private 1104. Modified 262. Locked 6.
    DeviceMap a00699b8
    Token                             a004d8e8
    ElapsedTime                       00:11:03.748
    UserTime                          00:00:00.296
    KernelTime                        00:00:00.296
    QuotaPoolUsage[PagedPool]         83384
    QuotaPoolUsage[NonPagedPool]      12264
    Working Set Sizes (now,min,max)  (2309, 50, 345) (9236KB, 200KB, 1380KB)
    PeakWorkingSetSize                2578
    VirtualSize                       53 Mb
    PeakVirtualSize                   69 Mb
    PageFaultCount                    3676
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      3119

    Setting context for this process...
.process /p /r ffffffff8485e910

    !peb
PEB at 7ffdd000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00dd0000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 002017e0 . 02093fa0
    Ldr.InLoadOrderModuleList:           00201760 . 02093f90
    Ldr.InMemoryOrderModuleList:         00201768 . 02093f98
            Base TimeStamp                     Module
          dd0000 4549adc4 Nov 02 08:35:16 2006 C:\Windows\System32\svchost.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        747b0000 4549bdf8 Nov 02 09:44:24 2006 c:\windows\system32\wevtsvc.dll
        75ba0000 4549bde2 Nov 02 09:44:02 2006 c:\windows\system32\USERENV.dll
        75b80000 4549bdd2 Nov 02 09:43:46 2006 c:\windows\system32\Secur32.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        753f0000 4549bde4 Nov 02 09:44:04 2006 c:\windows\system32\VERSION.dll
        75330000 4549bcd7 Nov 02 09:39:35 2006 c:\windows\system32\GPAPI.dll
        75610000 4679de70 Jun 21 03:12:00 2007 c:\windows\system32\slc.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        75480000 4549bd20 Nov 02 09:40:48 2006 C:\Windows\System32\credssp.dll
        75650000 45b96fde Jan 26 03:05:02 2007 C:\Windows\System32\CRYPT32.dll
        75820000 4549bd41 Nov 02 09:41:21 2006 C:\Windows\System32\MSASN1.dll
        75050000 46773a78 Jun 19 03:07:52 2007 C:\Windows\system32\schannel.dll
        75840000 4549bd53 Nov 02 09:41:39 2006 C:\Windows\System32\NETAPI32.dll
        75ce0000 4549bd99 Nov 02 09:42:49 2006 C:\Windows\system32\PSAPI.DLL
        75fe0000 4549be0e Nov 02 09:44:46 2006 C:\Windows\system32\WS2_32.dll
        77550000 4549bdc7 Nov 02 09:43:35 2006 C:\Windows\system32\NSI.dll
        75250000 4549bd69 Nov 02 09:42:01 2006 C:\Windows\system32\mswsock.dll
        752c0000 4549be27 Nov 02 09:45:11 2006 C:\Windows\System32\wshtcpip.dll
        752b0000 4549be21 Nov 02 09:45:05 2006 C:\Windows\System32\wship6.dll
        74d40000 4549bcc3 Nov 02 09:39:15 2006 c:\windows\system32\audiosrv.dll
```

```
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        74d90000 4549bd03 Nov 02 09:40:19 2006 c:\windows\system32\MMDevAPI.DLL
        763b0000 4549bdb9 Nov 02 09:43:21 2006 C:\Windows\system32\SHLWAPI.dll
        74fe0000 46d779a1 Aug 31 03:14:57 2007 c:\windows\system32\WTSAPI32.dll
        75300000 4549be2e Nov 02 09:45:18 2006 c:\windows\system32\WINSTA.dll
        74aa0000 4549bd09 Nov 02 09:40:25 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_5d07289e07e1d100\comctl32.dll
        773a0000 4549bce9 Nov 02 09:39:53 2006 C:\Windows\system32\CLBCatQ.DLL
        77030000 4549bdb0 Nov 02 09:43:12 2006 C:\Windows\system32\SETUPAPI.dll
        74ff0000 4549be2f Nov 02 09:45:19 2006 C:\Windows\System32\WINTRUST.dll
        77580000 462434a3 Apr 17 03:44:51 2007 C:\Windows\system32\imagehlp.dll
        746c0000 4549bcf3 Nov 02 09:40:03 2006 c:\windows\system32\lmhsvc.dll
        755b0000 4549bd3f Nov 02 09:41:19 2006 c:\windows\system32\IPHLPAPI.DLL
        75570000 46807ea6 Jun 26 03:49:10 2007 c:\windows\system32\dhcpcsvc.DLL
        75af0000 4549bcf1 Nov 02 09:40:01 2006 c:\windows\system32\DNSAPI.dll
        75560000 4549be1e Nov 02 09:45:02 2006 c:\windows\system32\WINNSI.DLL
        75540000 46807ea7 Jun 26 03:49:11 2007 c:\windows\system32\dhcpcsvc6.DLL
        75350000 4549bdae Nov 02 09:43:10 2006 C:\Windows\System32\rsaenh.dll
        736d0000 4549bcc2 Nov 02 09:39:14 2006 C:\Windows\System32\audioses.dll
        73540000 4549bcc0 Nov 02 09:39:12 2006 C:\Windows\System32\audioeng.dll
        75390000 4549bcdc Nov 02 09:39:40 2006 C:\Windows\System32\AVRT.dll
        6f620000 4549be13 Nov 02 09:44:51 2006 c:\windows\system32\wscsvc.dll
        74f30000 46677f3a Jun 07 04:44:58 2007 c:\windows\system32\FirewallAPI.dll
        72090000 4549bdef Nov 02 09:44:15 2006 C:\Windows\system32\wbem\wbemprox.dll
        71fe0000 46d7799a Aug 31 03:14:50 2007 C:\Windows\system32\wbem\wbemcomn.dll
        71ef0000 4549bdf0 Nov 02 09:44:16 2006 C:\Windows\system32\wbem\wbemsvc.dll
        71b40000 4549bcd4 Nov 02 09:39:32 2006 C:\Windows\system32\wbem\fastprox.dll
        75780000 4549bdcc Nov 02 09:43:40 2006 C:\Windows\system32\NTDSAPI.dll
        76310000 4549be44 Nov 02 09:45:40 2006 C:\Windows\system32\WLDAP32.dll
        6dcb0000 46ae8eee Jul 31 02:22:54 2007 C:\Windows\system32\wuapi.dll
        74f10000 4549bcb8 Nov 02 09:39:04 2006 C:\Windows\system32\Cabinet.dll
        73c50000 4549bcb0 Nov 02 09:38:56 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.6000.16386_none_87e0cb09378714f1\COMCTL32.dll
    SubSystemData:     00000000
    ProcessHeap:       00200000
    ProcessParameters: 00201068
    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;C:\Program Files\QuickTime\QTSystem\'
    Environment:  002007e8
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\ServiceProfiles\LocalService\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        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;C:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        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 899d5948  Cid 03a4.03a8  Teb: 7ffdf000 Win32Thread: 00000000 WAIT: (Executive)
UserMode Non-Alertable
            9fc52404  NotificationEvent
        IRP List:
            836ae300: (0006,0094) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            8485e910       Image:         svchost.exe
        Wait Start TickCount      42017          Ticks: 1482 (0:00:00:23.119)
        Context Switch Count      47
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address svchost!wmainCRTStartup (0x00dd20bf)
        Stack Init 9f2ac000 Current 9f2abbc8 Base 9f2ac000 Limit 9f2a9000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f2abbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f2abc1c 81c293a7 nt!KiSwapThread+0x389
        9f2abc78 81d88faf nt!KeWaitForSingleObject+0x414
        9f2abcac 81d93669 nt!IopSynchronousServiceTail+0x258
        9f2abd38 81c8caaa nt!NtReadFile+0x646
        9f2abd38 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f2abd64)
        000dfbb4 77490080 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        000dfbb8 75f3853f ntdll!ZwReadFile+0xc (FPO: [9,0,0])
        000dfc30 775cffe2 kernel32!ReadFile+0x20e (FPO: [Non-Fpo])
        000dfc5c 775cfdfb ADVAPI32!ScGetPipeInput+0x2a (FPO: [Non-Fpo])
        000dfcc4 775cbdd2 ADVAPI32!ScDispatcherLoop+0x6c (FPO: [Non-Fpo])
        000dff3c 00dd241d ADVAPI32!StartServiceCtrlDispatcherW+0xce (FPO: [Non-Fpo])
        000dff44 00dd2401 svchost!SvcHostMain+0x12 (FPO: [Non-Fpo])
        000dff48 00dd2183 svchost!wmain+0x5 (FPO: [Non-Fpo])
        000dff8c 75f33833 svchost!_initterm_e+0x163 (FPO: [Non-Fpo])
        000dff98 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        000dffd8 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fc2b6c0  Cid 03a4.03b0  Teb: 7ffdc000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fc081b8  SynchronizationEvent
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            8485e910       Image:         svchost.exe
        Wait Start TickCount      1015           Ticks: 42484 (0:00:11:02.754)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wevtsvc!RegistryMonitor::WaitThreadRoutine (0x747dc224)
        Stack Init 9f2b8000 Current 9f2b7c38 Base 9f2b8000 Limit 9f2b5000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f2b7c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f2b7c8c 81c293a7 nt!KiSwapThread+0x389
        9f2b7ce8 81df5057 nt!KeWaitForSingleObject+0x414
        9f2b7d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        9f2b7d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f2b7d64)
        00eefc30 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00eefc34 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        00eefca4 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        00eefcb8 747dc28a kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        00eefd1c 75f33833 wevtsvc!RegistryMonitor::WaitThreadRoutine+0xaf (FPO: [Non-Fpo])
        00eefd28 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00eefd68 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fc2e768  Cid 03a4.03b4  Teb: 7ffdb000 Win32Thread: ff4f03a8 WAIT: (UserRequest)
UserMode Non-Alertable
            9fc2a8a8  SynchronizationEvent
            9fc2acc0  SynchronizationEvent
            9fc2eea0  SynchronizationEvent
            9fc2a9b8  SynchronizationTimer
            9fc524b8  SynchronizationEvent
            9fc2eb00  SynchronizationTimer
            9fc2ac90  SynchronizationEvent
            9fc2e7f0  NotificationTimer
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            8485e910       Image:         svchost.exe
        Wait Start TickCount      42017          Ticks: 1482 (0:00:00:23.119)
        Context Switch Count      104
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wevtsvc!OsEventsCleanup (0x747e7cf0)
        Stack Init 9e89b000 Current 9e89a8d0 Base 9e89b000 Limit 9e898000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9e89a8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e89a924 81c28c64 nt!KiSwapThread+0x389
        9e89a970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9e89abfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9e89ad48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9e89ad48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9e89ad64)
        00f5fc84 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00f5fc88 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00f5fd24 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        00f5fd40 747e7e3f kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        00f5fd98 75f33833 wevtsvc!OsEventsCleanup+0x308 (FPO: [Non-Fpo])
        00f5fda4 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00f5fde4 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fc3c030  Cid 03a4.03c4  Teb: 7ffd9000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            899d5680  SynchronizationTimer
            9fc42f68  SynchronizationTimer
            9fc42f00  SynchronizationEvent
            9fc3ac58  SynchronizationEvent
            9fc702f0  NotificationEvent
            9fc2a278  SynchronizationEvent
            9fc69b20  NotificationEvent
            9fca0c18  NotificationEvent
            9fd4aba0  NotificationEvent
            9fd790b8  NotificationEvent
            9fc2a428  NotificationEvent
            9fd79088  NotificationEvent
            89851de8  NotificationEvent
            89878430  NotificationEvent
            9fce7518  SynchronizationEvent
            83488b50  NotificationEvent
            836cf668  SynchronizationEvent
            8373fff0  SynchronizationEvent
            837263e0  SynchronizationEvent
            9fce27d8  SynchronizationEvent
            9fc42ad8  SynchronizationTimer
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            8485e910       Image:         svchost.exe
        Wait Start TickCount      43326          Ticks: 173 (0:00:00:02.698)
        Context Switch Count      157
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x7744b49a)
        Stack Init 9f260000 Current 9f25f8d0 Base 9f260000 Limit 9f25d000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f25f8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f25f924 81c28c64 nt!KiSwapThread+0x389
        9f25f970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f25fbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f25fd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f25fd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f25fd64)
        010dfd50 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        010dfd54 7744b65b ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        010dfef0 75f33833 ntdll!TppWaiterpThread+0x294 (FPO: [Non-Fpo])
        010dfefc 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        010dff3c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fc3e630  Cid 03a4.03d8  Teb: 7ffd7000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fc3eea8  NotificationEvent
        IRP List:
            9fd94508: (0006,0094) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            8485e910       Image:         svchost.exe
        Wait Start TickCount      40520          Ticks: 2979 (0:00:00:46.472)
        Context Switch Count      326
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address wevtsvc!ProcessEventsThread (0x747d0cc9)
        Stack Init 9f278000 Current 9f277c38 Base 9f278000 Limit 9f275000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f277c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f277c8c 81c293a7 nt!KiSwapThread+0x389
        9f277ce8 81df5057 nt!KeWaitForSingleObject+0x414
        9f277d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        9f277d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f277d64)
        0100f7cc 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0100f7d0 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0100f840 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        0100f854 775d126c kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0100f894 775c0a06 ADVAPI32!EtwpProcessRealTimeTraces+0x9e (FPO: [Non-Fpo])
        0100fbdc 747d0d16 ADVAPI32!ProcessTrace+0x30a (FPO: [Non-Fpo])
        0100fc04 75f33833 wevtsvc!ProcessEventsThread+0x4d (FPO: [Non-Fpo])
        0100fc10 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0100fc50 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fc6e7f8  Cid 03a4.0400  Teb: 7ffd6000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fc6adc8  NotificationEvent
        IRP List:
            838160f8: (0006,0094) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            8485e910       Image:         svchost.exe
        Wait Start TickCount      12992          Ticks: 30507 (0:00:07:55.912)
        Context Switch Count      180
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wevtsvc!ProcessEventsThread (0x747d0cc9)
        Stack Init 9f220000 Current 9f21fc38 Base 9f220000 Limit 9f21d000 Call 0
        Priority 13 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f21fc50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f21fc8c 81c293a7 nt!KiSwapThread+0x389
        9f21fce8 81df5057 nt!KeWaitForSingleObject+0x414
        9f21fd50 81c8caaa nt!NtWaitForSingleObject+0xbe
        9f21fd50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f21fd64)
        0126f388 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0126f38c 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0126f3fc 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        0126f410 775d126c kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0126f450 775c0a06 ADVAPI32!EtwpProcessRealTimeTraces+0x9e (FPO: [Non-Fpo])
        0126f798 747d0d16 ADVAPI32!ProcessTrace+0x30a (FPO: [Non-Fpo])
        0126f7c0 75f33833 wevtsvc!ProcessEventsThread+0x4d (FPO: [Non-Fpo])
        0126f7cc 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0126f80c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fc6bd78  Cid 03a4.041c  Teb: 7ffd5000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            9fc704f8  QueueObject
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            8485e910       Image:         svchost.exe
        Wait Start TickCount      9155           Ticks: 34344 (0:00:08:55.769)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address audiosrv!EventWorkerThread (0x74d4f449)
        Stack Init 9f2c8000 Current 9f2c7bc8 Base 9f2c8000 Limit 9f2c5000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f2c7be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f2c7c1c 81cad431 nt!KiSwapThread+0x389
        9f2c7c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        9f2c7cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        9f2c7d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        9f2c7d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f2c7d64)
        013cf7cc 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        013cf7d0 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        013cf7fc 74d4f48b kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        013cf828 75f33833 audiosrv!EventWorkerThread+0x66 (FPO: [Non-Fpo])
        013cf834 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        013cf874 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fc7c3a8  Cid 03a4.042c  Teb: 7ffd3000 Win32Thread: ff4fe3a8 WAIT: (WrUserRequest)
UserMode Non-Alertable
            9fc7c328  SynchronizationEvent
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            8485e910       Image:         svchost.exe
        Wait Start TickCount      8892           Ticks: 34607 (0:00:08:59.872)
        Context Switch Count      33
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address MMDevAPI!CDeviceEnumerator::PnpNotificationThreadWrapper (0x74d94902)
        Stack Init 9f26c000 Current 9f26bb68 Base 9f26c000 Limit 9f269000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f26bb80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f26bbbc 81c293a7 nt!KiSwapThread+0x389
        9f26bc18 8cedb8ed nt!KeWaitForSingleObject+0x414
        9f26bc74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        9f26bc90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        9f26bce8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        9f26bd4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        9f26bd4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f26bd64)
        00e5fd34 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00e5fd38 761e19cd USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        00e5fd54 74d91b32 USER32!GetMessageW+0x33 (FPO: [Non-Fpo])
        00e5fde4 74d9490f MMDevAPI!CDeviceEnumerator::PnpNotificationThread+0x1ad (FPO: [Non-Fpo])
        00e5fdec 75f33833 MMDevAPI!CDeviceEnumerator::PnpNotificationThreadWrapper+0xd (FPO: [Non-
Fpo])
        00e5fdf8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00e5fe38 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fc85030  Cid 03a4.0430  Teb: 7ffaf000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fca0108  SynchronizationEvent
            9fca1620  SynchronizationEvent
            9fca1c30  SynchronizationEvent
            9fc854b8  SynchronizationEvent
            9fc33e88  SynchronizationEvent
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            8485e910       Image:         svchost.exe
        Wait Start TickCount      1069           Ticks: 42430 (0:00:11:01.912)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address MMDevAPI!CNotificationDelegator::HardwarePollingThreadProc (0x74d9ffc4)
        Stack Init 9f204000 Current 9f2038d0 Base 9f204000 Limit 9f201000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f2038e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f203924 81c28c64 nt!KiSwapThread+0x389
        9f203970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f203bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f203d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f203d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f203d64)
        0109fa78 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0109fa7c 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0109fb18 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0109fb34 74d9ffee kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0109fb58 75f33833 MMDevAPI!CNotificationDelegator::HardwarePollingThreadProc+0x2a (FPO:
[Non-Fpo])
        0109fb64 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0109fba4 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fce03b8  Cid 03a4.04d4  Teb: 7ffd8000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fcdc498  SynchronizationEvent
            9fcdef10  SynchronizationEvent
        IRP List:
            9fc9ddd8: (0006,0094) Flags: 00060000  Mdl: 9fc359e8
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            8485e910       Image:         svchost.exe
        Wait Start TickCount      1087           Ticks: 42412 (0:00:11:01.631)
        Context Switch Count      21
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x775cb9d5)
        Stack Init a0266000 Current a02658d0 Base a0266000 Limit a0263000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 3 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a02658e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0265924 81c28c64 nt!KiSwapThread+0x389
        a0265970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a0265bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a0265d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a0265d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0265d64)
        0155f8c4 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0155f8c8 746c170e ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0155fa9c 00dd148a lmhsvc!ServiceMain+0x20d (FPO: [Non-Fpo])
        0155fac8 775cb9f6 svchost!ServiceStarter+0x17a (FPO: [Non-Fpo])
        0155fadc 75f33833 ADVAPI32!ScSvcctrlThreadA+0x21 (FPO: [Non-Fpo])
        0155fae8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0155fb28 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fca6030  Cid 03a4.04dc  Teb: 7ffad000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fcdeee0  SynchronizationEvent
            9fcdeeb0  SynchronizationEvent
        IRP List:
            9fc8a770: (0006,0094) Flags: 00060000  Mdl: 899c6ec8
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            8485e910       Image:         svchost.exe
        Wait Start TickCount      1087           Ticks: 42412 (0:00:11:01.631)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address lmhsvc!CheckIPAddrWorkerRtn (0x746c268c)
        Stack Init a026a000 Current a02698d0 Base a026a000 Limit a0267000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a02698e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0269924 81c28c64 nt!KiSwapThread+0x389
        a0269970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a0269bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a0269d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a0269d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0269d64)
        0104f778 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0104f77c 746c2705 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0104f7b8 75f33833 lmhsvc!CheckIPAddrWorkerRtn+0x96 (FPO: [Non-Fpo])
        0104f7c4 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0104f804 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fca6d78  Cid 03a4.04e0  Teb: 7ffac000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fcdc9a0  NotificationEvent
            9fca6464  NotificationEvent
        IRP List:
            9fc47df0: (0006,01d8) Flags: 00060030  Mdl: 84b86408
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            8485e910       Image:         svchost.exe
        Wait Start TickCount      1087           Ticks: 42412 (0:00:11:01.631)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address lmhsvc!SmbGetHostThread (0x746c1115)
        Stack Init a027e000 Current a027d8d0 Base a027e000 Limit a027b000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a027d8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a027d924 81c28c64 nt!KiSwapThread+0x389
        a027d970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a027dbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a027dd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a027dd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a027dd64)
        011ff928 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        011ff92c 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        011ff9c8 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        011ff9e4 746c11d9 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        011ffdbc 75f33833 lmhsvc!SmbGetHostThread+0xfa (FPO: [Non-Fpo])
        011ffdc8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        011ffe08 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fca6ac0  Cid 03a4.04e4  Teb: 7ffab000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fcdc9a0  NotificationEvent
            9fcc77cc  NotificationEvent
        IRP List:
            89991a48: (0006,01d8) Flags: 00060030  Mdl: 899c5998
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            8485e910       Image:         svchost.exe
        Wait Start TickCount      1087           Ticks: 42412 (0:00:11:01.631)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address lmhsvc!SmbGetHostThread (0x746c1115)
        Stack Init a0282000 Current a02818d0 Base a0282000 Limit a027f000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a02818e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0281924 81c28c64 nt!KiSwapThread+0x389
        a0281970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a0281bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a0281d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a0281d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0281d64)
        0151f374 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0151f378 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0151f414 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0151f430 746c11d9 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0151f808 75f33833 lmhsvc!SmbGetHostThread+0xfa (FPO: [Non-Fpo])
        0151f814 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0151f854 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fcc93e0  Cid 03a4.04f4  Teb: 7ffaa000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            849cbff0  NotificationEvent
            9fcc8530  SynchronizationEvent
            9fccb168  NotificationEvent
            9fccb198  SynchronizationEvent
            9fcc9468  NotificationTimer
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            8485e910       Image:         svchost.exe
        Wait Start TickCount      1302           Ticks: 42197 (0:00:10:58.277)
        Context Switch Count      52
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x775cb9d5)
        Stack Init a028e000 Current a028d8d0 Base a028e000 Limit a028b000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a028d8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a028d924 81c28c64 nt!KiSwapThread+0x389
        a028d970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a028dbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a028dd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a028dd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a028dd64)
        0174fa9c 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0174faa0 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0174fb3c 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0174fb58 75575982 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0174fba4 755822d0 dhcpcsvc!ProcessDhcpRequestForever+0x245 (FPO: [Non-Fpo])
        0174fbd8 00dd148a dhcpcsvc!ServiceMain+0x107 (FPO: [Non-Fpo])
        0174fc04 775cb9f6 svchost!ServiceStarter+0x17a (FPO: [Non-Fpo])
        0174fc18 75f33833 ADVAPI32!ScSvcctrlThreadA+0x21 (FPO: [Non-Fpo])
        0174fc24 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0174fc64 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fce1a70  Cid 03a4.0510  Teb: 7ffa9000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            849cbff0  NotificationEvent
            9fc6d660  SynchronizationEvent
            9fcc4810  NotificationEvent
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            8485e910       Image:         svchost.exe
        Wait Start TickCount      9789           Ticks: 33710 (0:00:08:45.879)
        Context Switch Count      19
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address dhcpcsvc6!Dhcpv6Main (0x75545df4)
        Stack Init a0364000 Current a03638d0 Base a0364000 Limit a0361000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a03638e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0363924 81c28c64 nt!KiSwapThread+0x389
        a0363970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a0363bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a0363d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a0363d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0363d64)
        0149f8ac 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0149f8b0 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0149f94c 755441da kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0149f994 75545e8a dhcpcsvc6!ProcessDhcpv6RequestForever+0x108 (FPO: [Non-Fpo])
        0149f9b4 75f33833 dhcpcsvc6!Dhcpv6Main+0xa8 (FPO: [Non-Fpo])
        0149f9c0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0149fa00 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fd01030  Cid 03a4.0540  Teb: 7ffa5000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fd2eba8  NotificationEvent
        IRP List:
            9fc961d8: (0006,0094) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            8485e910       Image:         svchost.exe
        Wait Start TickCount      24448          Ticks: 19051 (0:00:04:57.197)
        Context Switch Count      71
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wevtsvc!ProcessEventsThread (0x747d0cc9)
        Stack Init a09bd000 Current a09bcc38 Base a09bd000 Limit a09ba000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a09bcc50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a09bcc8c 81c293a7 nt!KiSwapThread+0x389
        a09bcce8 81df5057 nt!KeWaitForSingleObject+0x414
        a09bcd50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a09bcd50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a09bcd64)
        0159f3a0 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0159f3a4 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0159f414 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        0159f428 775d126c kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0159f468 775c0a06 ADVAPI32!EtwpProcessRealTimeTraces+0x9e (FPO: [Non-Fpo])
        0159f7b0 747d0d16 ADVAPI32!ProcessTrace+0x30a (FPO: [Non-Fpo])
        0159f7d8 75f33833 wevtsvc!ProcessEventsThread+0x4d (FPO: [Non-Fpo])
        0159f7e4 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0159f824 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 83491840  Cid 03a4.0f58  Teb: 7ffa2000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            83634ff0  SynchronizationEvent
            836cf7b0  SynchronizationTimer
            83634fc0  SynchronizationEvent
            837dc2f8  SynchronizationEvent
            836cf638  SynchronizationEvent
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            8485e910       Image:         svchost.exe
        Wait Start TickCount      9783           Ticks: 33716 (0:00:08:45.972)
        Context Switch Count      46
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wscsvc!CThirdPartyMonitoring::MonitoringThreadProcEntry (0x6f624930)
        Stack Init 9f7cc000 Current 9f7cb8d0 Base 9f7cc000 Limit 9f7c9000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f7cb8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f7cb924 81c28c64 nt!KiSwapThread+0x389
        9f7cb970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f7cbbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f7cbd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f7cbd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f7cbd64)
        024ffb88 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        024ffb8c 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        024ffc28 6f62381e kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        024ffc6c 6f624959 wscsvc!CThirdPartyMonitoring::MonitoringThreadProc+0xf1 (FPO: [Non-Fpo])
        024ffc78 75f33833 wscsvc!CThirdPartyMonitoring::MonitoringThreadProcEntry+0x2d (FPO: [Non-
Fpo])
        024ffc84 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        024ffcc4 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 83725840  Cid 03a4.0f5c  Teb: 7ffa0000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Alertable
            837d6ca8  QueueObject
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            8485e910       Image:         svchost.exe
        Wait Start TickCount      9781           Ticks: 33718 (0:00:08:46.004)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init 9f7d4000 Current 9f7d3bc8 Base 9f7d4000 Limit 9f7d1000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f7d3be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f7d3c1c 81cad431 nt!KiSwapThread+0x389
        9f7d3c68 81d8b982 nt!KeRemoveQueueEx+0x568
        9f7d3cc0 81c7a036 nt!IoRemoveIoCompletion+0x23
        9f7d3d54 81c8caaa nt!NtWaitForWorkViaWorkerFactory+0x1a1
        9f7d3d54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f7d3d64)
        0237fa58 77490850 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0237fa5c 7749a1b4 ntdll!NtWaitForWorkViaWorkerFactory+0xc (FPO: [2,0,0])
        0237fb84 75f33833 ntdll!TppWorkerThread+0x1f6 (FPO: [Non-Fpo])
        0237fb90 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0237fbd0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 83726538  Cid 03a4.0f64  Teb: 7ff9f000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            837dc6c0  NotificationEvent
            83569788  SynchronizationEvent
            899c0230  SynchronizationEvent
            83634188  SynchronizationEvent
            836db9a0  SynchronizationEvent
            83634020  SynchronizationTimer
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            8485e910       Image:         svchost.exe
        Wait Start TickCount      9859           Ticks: 33640 (0:00:08:44.787)
        Context Switch Count      35
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wscsvc!SystemMonitoringThreadProc (0x6f62254d)
        Stack Init 9f7e0000 Current 9f7df8d0 Base 9f7e0000 Limit 9f7dd000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f7df8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f7df924 81c28c64 nt!KiSwapThread+0x389
        9f7df970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f7dfbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f7dfd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f7dfd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f7dfd64)
        022dfc80 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        022dfc84 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        022dfd20 6f622749 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        022dfdcc 75f33833 wscsvc!SystemMonitoringThreadProc+0x27b (FPO: [Non-Fpo])
        022dfdd8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        022dfe18 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 8374c440  Cid 03a4.080c  Teb: 7ffde000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            9fc2ab28  QueueObject
            8374c4c8  NotificationTimer
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            8485e910       Image:         svchost.exe
        Wait Start TickCount      42379          Ticks: 1120 (0:00:00:17.472)
        Context Switch Count      17
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init 9f3b4000 Current 9f3b3bc8 Base 9f3b4000 Limit 9f3b1000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f3b3be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f3b3c1c 81cad431 nt!KiSwapThread+0x389
        9f3b3c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        9f3b3cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        9f3b3d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        9f3b3d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f3b3d64)
        01bbf690 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01bbf694 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        01bbf6c0 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        01bbf6fc 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        01bbf768 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        01bbf774 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        01bbf79c 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        01bbf7a8 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        01bbf7b4 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01bbf7f4 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 8360b920  Cid 03a4.0af8  Teb: 7ffda000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Alertable
            9fc3b0e0  QueueObject
            8360b9a8  NotificationTimer
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            8485e910       Image:         svchost.exe
        Wait Start TickCount      43326          Ticks: 173 (0:00:00:02.698)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init 9f7fc000 Current 9f7fbbc8 Base 9f7fc000 Limit 9f7f9000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f7fbbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f7fbc1c 81cad431 nt!KiSwapThread+0x389
        9f7fbc68 81d8b982 nt!KeRemoveQueueEx+0x568
        9f7fbcc0 81c7a036 nt!IoRemoveIoCompletion+0x23
        9f7fbd54 81c8caaa nt!NtWaitForWorkViaWorkerFactory+0x1a1
        9f7fbd54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f7fbd64)
        017dfdf0 77490850 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        017dfdf4 7749a1b4 ntdll!NtWaitForWorkViaWorkerFactory+0xc (FPO: [2,0,0])
        017dff1c 75f33833 ntdll!TppWorkerThread+0x1f6 (FPO: [Non-Fpo])
        017dff28 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        017dff68 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 835d1930  Cid 03a4.05ac  Teb: 7ffd4000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Alertable
            9fc3b0e0  QueueObject
            835d19b8  NotificationTimer
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            8485e910       Image:         svchost.exe
        Wait Start TickCount      43326          Ticks: 173 (0:00:00:02.698)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init 9f79c000 Current 9f79bbc8 Base 9f79c000 Limit 9f799000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f79bbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f79bc1c 81cad431 nt!KiSwapThread+0x389
        9f79bc68 81d8b982 nt!KeRemoveQueueEx+0x568
        9f79bcc0 81c7a036 nt!IoRemoveIoCompletion+0x23
        9f79bd54 81c8caaa nt!NtWaitForWorkViaWorkerFactory+0x1a1
        9f79bd54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f79bd64)
        00e9f75c 77490850 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00e9f760 7749a1b4 ntdll!NtWaitForWorkViaWorkerFactory+0xc (FPO: [2,0,0])
        00e9f888 75f33833 ntdll!TppWorkerThread+0x1f6 (FPO: [Non-Fpo])
        00e9f894 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00e9f8d4 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Svchost process (LocalSystemNetworkRestricted)

```
PROCESS 9fc38a48  SessionId: 0  Cid: 03bc    Peb: 7ffd8000  ParentCid: 0214
    DirBase: 29a011c0  ObjectTable: a00811e8  HandleCount: 479.
    Image: svchost.exe
    VadRoot 9fc41098 Vads 250 Clone 0 Private 6433. Modified 884. Locked 2.
    DeviceMap 85a03048
    Token                             a0087a20
    ElapsedTime                       00:11:03.670
    UserTime                          00:00:00.124
    KernelTime                        00:00:00.358
    QuotaPoolUsage[PagedPool]         118648
    QuotaPoolUsage[NonPagedPool]      12256
    Working Set Sizes (now,min,max)  (7751, 50, 345) (31004KB, 200KB, 1380KB)
    PeakWorkingSetSize                13810
    VirtualSize                       113 Mb
    PeakVirtualSize                   120 Mb
    PageFaultCount                    25574
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      7734

    Setting context for this process...
.process /p /r ffffffff9fc38a48

    !peb
PEB at 7ffd8000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00dd0000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 002c1748 . 0476d858
    Ldr.InLoadOrderModuleList:           002c16c8 . 0476d8b8
    Ldr.InMemoryOrderModuleList:         002c16d0 . 0476d8c0
            Base TimeStamp                     Module
          dd0000 4549adc4 Nov 02 08:35:16 2006 C:\Windows\System32\svchost.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        75020000 4549bddb Nov 02 09:43:55 2006 C:\Windows\System32\NTMARTA.DLL
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        76310000 4549be44 Nov 02 09:45:40 2006 C:\Windows\system32\WLDAP32.dll
        75fe0000 4549be0e Nov 02 09:44:46 2006 C:\Windows\system32\WS2_32.dll
        77550000 4549bdc7 Nov 02 09:43:35 2006 C:\Windows\system32\NSI.dll
        75ce0000 4549bd99 Nov 02 09:42:49 2006 C:\Windows\system32\PSAPI.DLL
        75ad0000 4549bda8 Nov 02 09:43:04 2006 C:\Windows\System32\SAMLIB.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        74d40000 4549bcc3 Nov 02 09:39:15 2006 c:\windows\system32\audiosrv.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        74d90000 4549bd03 Nov 02 09:40:19 2006 c:\windows\system32\MMDevAPI.DLL
        763b0000 4549bdb9 Nov 02 09:43:21 2006 C:\Windows\system32\SHLWAPI.dll
        74fe0000 46d779a1 Aug 31 03:14:57 2007 c:\windows\system32\WTSAPI32.dll
        75300000 4549be2e Nov 02 09:45:18 2006 c:\windows\system32\WINSTA.dll
        74aa0000 4549bd09 Nov 02 09:40:25 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_5d07289e07e1d100\comctl32.dll
        773a0000 4549bce9 Nov 02 09:39:53 2006 C:\Windows\system32\CLBCatQ.DLL
        77030000 4549bdb0 Nov 02 09:43:12 2006 C:\Windows\system32\SETUPAPI.dll
        74ff0000 4549be2f Nov 02 09:45:19 2006 C:\Windows\System32\WINTRUST.dll
```

```
    75650000 45b96fde Jan 26 03:05:02 2007 C:\Windows\System32\CRYPT32.dll
    75820000 4549bd41 Nov 02 09:41:21 2006 C:\Windows\System32\MSASN1.dll
    75ba0000 4549bde2 Nov 02 09:44:02 2006 C:\Windows\System32\USERENV.dll
    75b80000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\System32\Secur32.dll
    77580000 462434a3 Apr 17 03:44:51 2007 C:\Windows\system32\imagehlp.dll
    74c90000 4549bde6 Nov 02 09:44:06 2006 c:\windows\system32\uxsms.dll
    74690000 4549bdcf Nov 02 09:43:43 2006 c:\windows\system32\tabsvc.dll
    74cb0000 4549bcde Nov 02 09:39:42 2006 c:\windows\system32\HID.DLL
    75610000 4679de70 Jun 21 03:12:00 2007 c:\windows\system32\slc.dll
    73fd0000 46d4e27e Aug 29 04:05:34 2007 c:\windows\system32\wlansvc.dll
    75840000 4549bd53 Nov 02 09:41:39 2006 c:\windows\system32\NETAPI32.dll
    76560000 4681c95d Jun 27 03:20:13 2007 C:\Windows\system32\SHELL32.dll
    74080000 46d4e27b Aug 29 04:05:31 2007 c:\windows\system32\WLANMSM.DLL
    73f70000 46d4e27d Aug 29 04:05:33 2007 c:\windows\system32\WLANSEC.dll
    74050000 4549bda1 Nov 02 09:42:57 2006 c:\windows\system32\OneX.DLL
    74680000 4549bccc Nov 02 09:39:24 2006 c:\windows\system32\eappprxy.dll
    73f40000 4549bcc9 Nov 02 09:39:21 2006 c:\windows\system32\eappcfg.dll
    757b0000 4549bccf Nov 02 09:39:27 2006 c:\windows\system32\AUTHZ.dll
    75570000 46807ea6 Jun 26 03:49:10 2007 c:\windows\system32\dhcpcsvc.DLL
    75af0000 4549bcf1 Nov 02 09:40:01 2006 c:\windows\system32\DNSAPI.dll
    75560000 4549be1e Nov 02 09:45:02 2006 c:\windows\system32\WINNSI.DLL
    74440000 4549be45 Nov 02 09:45:41 2006 c:\windows\system32\wlgpclnt.dll
    744c0000 4549bce0 Nov 02 09:39:44 2006 c:\windows\system32\l2gpstore.dll
    73f30000 4549be41 Nov 02 09:45:37 2006 c:\windows\system32\wlanutil.dll
    75ac0000 4549bddd Nov 02 09:43:57 2006 c:\windows\system32\SYSNTFY.dll
    74d30000 4549bd6b Nov 02 09:42:03 2006 c:\windows\system32\nlaapi.dll
    755b0000 4549bd3f Nov 02 09:41:19 2006 c:\windows\system32\IPHLPAPI.DLL
    75540000 46807ea7 Jun 26 03:49:11 2007 c:\windows\system32\dhcpcsvc6.DLL
    754a0000 4549bcb9 Nov 02 09:39:05 2006 c:\windows\system32\bcrypt.dll
    73ad0000 46289734 Apr 20 11:34:28 2007 C:\Windows\System32\msxml6.dll
    75350000 4549bdae Nov 02 09:43:10 2006 C:\Windows\System32\rsaenh.dll
    75480000 4549bd20 Nov 02 09:40:48 2006 C:\Windows\System32\credssp.dll
    75050000 46773a78 Jun 19 03:07:52 2007 C:\Windows\system32\schannel.dll
    75400000 4549bd7f Nov 02 09:42:23 2006 C:\Windows\system32\kerberos.dll
    75b60000 4549bd26 Nov 02 09:40:54 2006 C:\Windows\System32\cryptdll.dll
    73d00000 4689b047 Jul 03 03:11:19 2007 C:\Windows\system32\netcfgx.dll
    74f10000 4549bcb8 Nov 02 09:39:04 2006 C:\Windows\System32\Cabinet.dll
    72db0000 4549bcfc Nov 02 09:40:12 2006 c:\windows\system32\emdmgmt.dll
    72bb0000 4549bde4 Nov 02 09:44:04 2006 c:\windows\system32\WDSCORE.dll
    72f50000 4549bdb6 Nov 02 09:43:18 2006 c:\windows\system32\SLWGA.dll
    75dc0000 470c4de2 Oct 10 04:58:26 2007 C:\Windows\system32\urlmon.dll
    76360000 4549bcfb Nov 02 09:40:11 2006 C:\Windows\system32\iertutil.dll
    72c30000 4549bd91 Nov 02 09:42:41 2006 c:\windows\system32\pcasvc.dll
    75b20000 4549bcaf Nov 02 09:38:55 2006 c:\windows\system32\apphelp.dll
    72bf0000 4549bce0 Nov 02 09:39:44 2006 c:\windows\system32\hidserv.dll
    72630000 46d4e22c Aug 29 04:04:12 2007 c:\windows\system32\sysmain.dll
    728c0000 4549bdfe Nov 02 09:44:30 2006 c:\windows\system32\trkwks.dll
    728a0000 4549bdff Nov 02 09:44:31 2006 c:\windows\system32\wpdbusenum.dll
    75330000 4549bcd7 Nov 02 09:39:35 2006 C:\Windows\System32\GPAPI.dll
    72040000 4549bdc8 Nov 02 09:43:36 2006 C:\Windows\system32\PortableDeviceApi.dll
    72e70000 4549bde1 Nov 02 09:44:01 2006 c:\windows\system32\wdi.dll
    71b20000 4549bd90 Nov 02 09:42:40 2006 C:\Windows\system32\pcadm.dll
    6f5c0000 4549bd5f Nov 02 09:41:51 2006 c:\windows\system32\netman.dll
    73a20000 4549bda3 Nov 02 09:42:59 2006 c:\windows\system32\RASAPI32.dll
    73a00000 4549bdab Nov 02 09:43:07 2006 c:\windows\system32\rasman.dll
    73960000 4549bdd1 Nov 02 09:43:45 2006 c:\windows\system32\TAPI32.dll
    73950000 4549bdba Nov 02 09:43:22 2006 c:\windows\system32\rtutils.dll
    738c0000 4549be1d Nov 02 09:45:01 2006 c:\windows\system32\WINMM.dll
    73880000 4549bd93 Nov 02 09:42:43 2006 c:\windows\system32\OLEACC.dll
    6f200000 4549bd66 Nov 02 09:41:58 2006 C:\Windows\System32\netshell.dll
    6f130000 4549bda9 Nov 02 09:43:05 2006 C:\Windows\System32\RASDLG.dll
    73840000 4549bd15 Nov 02 09:40:37 2006 C:\Windows\System32\MPRAPI.dll
    731d0000 4549bcbd Nov 02 09:39:09 2006 C:\Windows\System32\ACTIVEDS.dll
    73190000 4549bcce Nov 02 09:39:26 2006 C:\Windows\System32\adsldpc.dll
    73160000 4549bd21 Nov 02 09:40:49 2006 C:\Windows\System32\credui.dll
    74d00000 4549bcbc Nov 02 09:39:08 2006 C:\Windows\System32\ATL.DLL
    6ea60000 4549bd9a Nov 02 09:42:50 2006 C:\Windows\system32\radardt.dll
    753f0000 4549bde4 Nov 02 09:44:04 2006 C:\Windows\System32\VERSION.dll
SubSystemData:     00000000
ProcessHeap:       002c0000
```

```
    ProcessParameters: 002c0fd8
    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;C:\Program Files\QuickTime\QTSystem\'
    Environment:  002c07e8
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\system32\config\systemprofile\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        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:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\TEMP
        TMP=C:\Windows\TEMP
        USERDOMAIN=WORKGROUP
        USERNAME=HOME$
        USERPROFILE=C:\Windows\system32\config\systemprofile
        windir=C:\Windows


        THREAD 9fc382c8  Cid 03bc.03c0  Teb: 7ffdf000 Win32Thread: ff4f2e98 WAIT: (Executive)
UserMode Non-Alertable
            9fc3b194  NotificationEvent
        IRP List:
            9fd92708: (0006,0094) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      9648           Ticks: 33851 (0:00:08:48.078)
        Context Switch Count      249
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address svchost!wmainCRTStartup (0x00dd20bf)
        Stack Init 9f25c000 Current 9f25bbc8 Base 9f25c000 Limit 9f259000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f25bbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f25bc1c 81c293a7 nt!KiSwapThread+0x389
        9f25bc78 81d88faf nt!KeWaitForSingleObject+0x414
        9f25bcac 81d93669 nt!IopSynchronousServiceTail+0x258
        9f25bd38 81c8caaa nt!NtReadFile+0x646
        9f25bd38 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f25bd64)
        001efb54 77490080 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        001efb58 75f3853f ntdll!ZwReadFile+0xc (FPO: [9,0,0])
        001efbd0 775cffe2 kernel32!ReadFile+0x20e (FPO: [Non-Fpo])
        001efbfc 775cfdfb ADVAPI32!ScGetPipeInput+0x2a (FPO: [Non-Fpo])
        001efc64 775cbdd2 ADVAPI32!ScDispatcherLoop+0x6c (FPO: [Non-Fpo])
        001efedc 00dd241d ADVAPI32!StartServiceCtrlDispatcherW+0xce (FPO: [Non-Fpo])
        001efee4 00dd2401 svchost!SvcHostMain+0x12 (FPO: [Non-Fpo])
        001efee8 00dd2183 svchost!wmain+0x5 (FPO: [Non-Fpo])
```

```
        001eff2c 75f33833 svchost!_initterm_e+0x163 (FPO: [Non-Fpo])
        001eff38 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        001eff78 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fc6b030  Cid 03bc.03ec  Teb: 7ffdd000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            9fc42e48  SynchronizationTimer
            9fc58b60  NotificationEvent
            9fc6c530  SynchronizationTimer
            9fc3e2f0  NotificationEvent
            9fd08188  NotificationEvent
            9fc271e8  NotificationEvent
            a18a6668  SynchronizationTimer
            a18b58f0  SynchronizationEvent
            a18a5bd0  SynchronizationEvent
            9fc221e0  Semaphore Limit 0x7fffffff
            a18a5100  SynchronizationEvent
            9fc25d40  SynchronizationEvent
            a18aa5c8  SynchronizationEvent
            a18ad880  SynchronizationEvent
            a18b97f0  SynchronizationEvent
            9fdfcee8  NotificationEvent
            8995e0a8  NotificationEvent
            8346fd90  ProcessObject
            83635980  SynchronizationEvent
            8374c9c0  SynchronizationEvent
            9fc55020  SynchronizationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      43413          Ticks: 86 (0:00:00:01.341)
        Context Switch Count      135
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x7744b49a)
        Stack Init 9f28c000 Current 9f28b8d0 Base 9f28c000 Limit 9f289000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f28b8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f28b924 81c28c64 nt!KiSwapThread+0x389
        9f28b970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f28bbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f28bd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f28bd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f28bd64)
        00e3f628 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00e3f62c 7744b65b ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00e3f7c8 75f33833 ntdll!TppWaiterpThread+0x294 (FPO: [Non-Fpo])
        00e3f7d4 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00e3f814 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fc6bac0  Cid 03bc.03f4  Teb: 7ffde000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            9fc58248  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      1021           Ticks: 42478 (0:00:11:02.661)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address audiosrv!EventWorkerThread (0x74d4f449)
        Stack Init 9f210000 Current 9f20fbc8 Base 9f210000 Limit 9f20d000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f20fbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f20fc1c 81cad431 nt!KiSwapThread+0x389
        9f20fc6c 81d8b982 nt!KeRemoveQueueEx+0x568
        9f20fcc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        9f20fd48 81c8caaa nt!NtRemoveIoCompletion+0x106
        9f20fd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f20fd64)
        00d6f914 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00d6f918 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        00d6f944 74d4f48b kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        00d6f970 75f33833 audiosrv!EventWorkerThread+0x66 (FPO: [Non-Fpo])
        00d6f97c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00d6f9bc 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fc57030  Cid 03bc.03f8  Teb: 7ffdb000 Win32Thread: ff454918 WAIT: (WrUserRequest)
UserMode Non-Alertable
            9fc6c880  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      8892           Ticks: 34607 (0:00:08:59.872)
        Context Switch Count      35
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address MMDevAPI!CDeviceEnumerator::PnpNotificationThreadWrapper (0x74d94902)
        Stack Init 9f264000 Current 9f263b68 Base 9f264000 Limit 9f261000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f263b80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f263bbc 81c293a7 nt!KiSwapThread+0x389
        9f263c18 8cedb8ed nt!KeWaitForSingleObject+0x414
        9f263c74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        9f263c90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        9f263ce8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        9f263d4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        9f263d4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f263d64)
        00faf7e4 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00faf7e8 761e19cd USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        00faf804 74d91b32 USER32!GetMessageW+0x33 (FPO: [Non-Fpo])
        00faf894 74d9490f MMDevAPI!CDeviceEnumerator::PnpNotificationThread+0x1ad (FPO: [Non-Fpo])
        00faf89c 75f33833 MMDevAPI!CDeviceEnumerator::PnpNotificationThreadWrapper+0xd (FPO: [Non-
Fpo])
        00faf8a8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00faf8e8 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fc7ad78  Cid 03bc.0404  Teb: 7ffda000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fc71e48  SynchronizationEvent
            9fc6a970  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      1062           Ticks: 42437 (0:00:11:02.021)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address MMDevAPI!CNotificationDelegator::HardwarePollingThreadProc (0x74d9ffc4)
        Stack Init 9f238000 Current 9f2378d0 Base 9f238000 Limit 9f235000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f2378e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f237924 81c28c64 nt!KiSwapThread+0x389
        9f237970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f237bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f237d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f237d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f237d64)
        00ebf9e8 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00ebf9ec 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00ebfa88 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        00ebfaa4 74d9ffee kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        00ebfac8 75f33833 MMDevAPI!CNotificationDelegator::HardwarePollingThreadProc+0x2a (FPO:
[Non-Fpo])
        00ebfad4 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00ebfb14 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fc8e030  Cid 03bc.04ac  Teb: 7ffd5000 Win32Thread: 00000000 WAIT: (WrLpcReceive)
UserMode Non-Alertable
            9fc8e244  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      18450          Ticks: 25049 (0:00:06:30.766)
        Context Switch Count      53
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address uxsms!CPortBase::PortThread (0x74c92bf9)
        Stack Init 9f230000 Current 9f22fb70 Base 9f230000 Limit 9f22d000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f22fb88 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f22fbc4 81c293a7 nt!KiSwapThread+0x389
        9f22fc24 81dc3dac nt!KeWaitForSingleObject+0x414
        9f22fc5c 81dc486e nt!AlpcpReceiveMessagePort+0x221
        9f22fcc4 81dbe7b6 nt!AlpcpReceiveLegacyMessage+0x197
        9f22fd30 81dbe69c nt!NtReplyWaitReceivePortEx+0x100
        9f22fd4c 81c8caaa nt!NtReplyWaitReceivePort+0x18
        9f22fd4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f22fd64)
        011cf7bc 77490140 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        011cf7c0 74c911f7 ntdll!ZwReplyWaitReceivePort+0xc (FPO: [4,0,0])
        011cf7f4 74c92c07 uxsms!CPortBase::PortThreadInternal+0x95
        011cf800 75f33833 uxsms!CPortBase::PortThread+0xe
        011cf80c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        011cf84c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fc8dd78  Cid 03bc.04b4  Teb: 7ffdc000 Win32Thread: ff502230 WAIT: (WrUserRequest)
UserMode Non-Alertable
            849cdbc0  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      1087           Ticks: 42412 (0:00:11:01.631)
        Context Switch Count      78
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x775cb9d5)
        Stack Init 9f23c000 Current 9f23bb68 Base 9f23c000 Limit 9f239000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f23bb80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f23bbbc 81c293a7 nt!KiSwapThread+0x389
        9f23bc18 8cedb8ed nt!KeWaitForSingleObject+0x414
        9f23bc74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        9f23bc90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        9f23bce8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        9f23bd4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        9f23bd4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f23bd64)
        0137fe7c 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0137fe80 761e19cd USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        0137fe9c 746966bf USER32!GetMessageW+0x33 (FPO: [Non-Fpo])
        0137fedc 7469661e tabsvc!CServiceModule::ServiceMainLoop+0x53 (FPO: [Non-Fpo])
        0137fee4 00dd148a tabsvc!CServiceModule::ServiceMain+0x61 (FPO: [Non-Fpo])
        0137ff10 775cb9f6 svchost!ServiceStarter+0x17a (FPO: [Non-Fpo])
        0137ff24 75f33833 ADVAPI32!ScSvcctrlThreadA+0x21 (FPO: [Non-Fpo])
        0137ff30 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0137ff70 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fcdcd78  Cid 03bc.04cc  Teb: 7ffd4000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            9fc8da98  SynchronizationEvent
            9fc15288  SynchronizationEvent
            9fc97910  SynchronizationEvent
            835f47b8  SynchronizationEvent
            835f6250  SynchronizationEvent
            835f64b0  SynchronizationEvent
            835f4fc0  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      9163           Ticks: 34336 (0:00:08:55.645)
        Context Switch Count      7
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address msvcrt!_endthreadex (0x7628639b)
        Stack Init 9f248000 Current 9f2478d0 Base 9f248000 Limit 9f245000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f2478e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f247924 81c28c64 nt!KiSwapThread+0x389
        9f247970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f247bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f247d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f247d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f247d64)
        012ff590 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        012ff594 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        012ff630 74691b37 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        012ff9a8 762862b6 tabsvc!CServiceModule::MonitorThreadProc+0x43d (FPO: [Non-Fpo])
        012ff9e0 762863de msvcrt!_endthreadex+0x44 (FPO: [Non-Fpo])
        012ff9e8 75f33833 msvcrt!_endthreadex+0xce (FPO: [Non-Fpo])
        012ff9f4 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        012ffa34 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fd02880  Cid 03bc.054c  Teb: 7ffae000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fd01858  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      1104           Ticks: 42395 (0:00:11:01.366)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address msvcrt!_endthreadex (0x7628639b)
        Stack Init a09c1000 Current a09c0c38 Base a09c1000 Limit a09be000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a09c0c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a09c0c8c 81c293a7 nt!KiSwapThread+0x389
        a09c0ce8 81df5057 nt!KeWaitForSingleObject+0x414
        a09c0d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a09c0d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a09c0d64)
        0179f7cc 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0179f7d0 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0179f840 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        0179f854 74683658 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0179f874 762862b6 eappprxy!EapHost::Peer::PeerProxy::InitUninitComEnvProc+0x98 (FPO: [Non-
Fpo])
        0179f8ac 762863de msvcrt!_endthreadex+0x44 (FPO: [Non-Fpo])
        0179f8b4 75f33833 msvcrt!_endthreadex+0xce (FPO: [Non-Fpo])
        0179f8c0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0179f900 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fd07808  Cid 03bc.0550  Teb: 7ffad000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fd02690  SynchronizationEvent
            9fd01500  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      1103           Ticks: 42396 (0:00:11:01.381)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wlgpclnt!MainGPAProc (0x74444bd4)
        Stack Init a09c5000 Current a09c48d0 Base a09c5000 Limit a09c2000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a09c48e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a09c4924 81c28c64 nt!KiSwapThread+0x389
        a09c4970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a09c4bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a09c4d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a09c4d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a09c4d64)
        0174f780 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0174f784 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0174f820 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0174f83c 74444c7e kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0174f87c 75f33833 wlgpclnt!MainGPAProc+0xaa (FPO: [Non-Fpo])
        0174f888 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0174f8c8 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fce1030  Cid 03bc.0564  Teb: 7ffaa000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Alertable
            9fc58510  QueueObject
        IRP List:
            9fde17a8: (0006,01d8) Flags: 00060800  Mdl: 00000000
            8985a830: (0006,01d8) Flags: 00060000  Mdl: 00000000
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      43413          Ticks: 86 (0:00:00:01.341)
        Context Switch Count      140
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init a0969000 Current a0968bc8 Base a0969000 Limit a0966000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a0968be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0968c1c 81cad431 nt!KiSwapThread+0x389
        a0968c68 81d8b982 nt!KeRemoveQueueEx+0x568
        a0968cc0 81c7a036 nt!IoRemoveIoCompletion+0x23
        a0968d54 81c8caaa nt!NtWaitForWorkViaWorkerFactory+0x1a1
        a0968d54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0968d64)
        0145f798 77490850 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0145f79c 7749a1b4 ntdll!NtWaitForWorkViaWorkerFactory+0xc (FPO: [2,0,0])
        0145f8c4 75f33833 ntdll!TppWorkerThread+0x1f6 (FPO: [Non-Fpo])
        0145f8d0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0145f910 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 89872970  Cid 03bc.0748  Teb: 7ffd6000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            8994acd8  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      1820           Ticks: 41679 (0:00:10:50.196)
        Context Switch Count      320
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x775cb9d5)
        Stack Init a1b38000 Current a1b37c38 Base a1b38000 Limit a1b35000 Call 0
        Priority 12 BasePriority 8 PriorityDecrement 3 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1b37c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1b37c8c 81c293a7 nt!KiSwapThread+0x389
        a1b37ce8 81df5057 nt!KeWaitForSingleObject+0x414
        a1b37d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a1b37d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1b37d64)
        013cfb4c 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        013cfb50 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        013cfbc0 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        013cfbd4 72dbf052 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        013cfbf4 72dbef9c emdmgmt!EcSvcMainThread+0x71 (FPO: [Non-Fpo])
        013cfc1c 00dd148a emdmgmt!EMDMgmtServiceMain+0xaa (FPO: [Non-Fpo])
        013cfc48 775cb9f6 svchost!ServiceStarter+0x17a (FPO: [Non-Fpo])
        013cfc5c 75f33833 ADVAPI32!ScSvcctrlThreadA+0x21 (FPO: [Non-Fpo])
        013cfc68 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        013cfca8 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 898748d0  Cid 03bc.0750  Teb: 7ffd3000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            89881a80  Thread
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      1807           Ticks: 41692 (0:00:10:50.399)
        Context Switch Count      10
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x775cb9d5)
        Stack Init a1b3c000 Current a1b3bc38 Base a1b3c000 Limit a1b39000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1b3bc50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1b3bc8c 81c293a7 nt!KiSwapThread+0x389
        a1b3bce8 81df5057 nt!KeWaitForSingleObject+0x414
        a1b3bd50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a1b3bd50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1b3bd64)
        0186fe50 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0186fe54 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0186fec4 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        0186fed8 72bf1c0c kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0186fef0 00dd148a hidserv!ServiceMain+0xf2 (FPO: [Non-Fpo])
        0186ff1c 775cb9f6 svchost!ServiceStarter+0x17a (FPO: [Non-Fpo])
        0186ff30 75f33833 ADVAPI32!ScSvcctrlThreadA+0x21 (FPO: [Non-Fpo])
        0186ff3c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0186ff7c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 89881a80  Cid 03bc.0770  Teb: 7ffa9000 Win32Thread: ff516120 WAIT: (WrUserRequest)
UserMode Non-Alertable
            9fc24320  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      9155           Ticks: 34344 (0:00:08:55.769)
        Context Switch Count      83
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address hidserv!HidServMain (0x72bf1c31)
        Stack Init a1ae5000 Current a1ae4b68 Base a1ae5000 Limit a1ae2000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1ae4b80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1ae4bbc 81c293a7 nt!KiSwapThread+0x389
        a1ae4c18 8cedb8ed nt!KeWaitForSingleObject+0x414
        a1ae4c74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        a1ae4c90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        a1ae4ce8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        a1ae4d4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        a1ae4d4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1ae4d64)
        0170fa18 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0170fa1c 761e19cd USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        0170fa38 72bf1e85 USER32!GetMessageW+0x33 (FPO: [Non-Fpo])
        0170fac8 75f33833 hidserv!HidServMain+0x25f (FPO: [Non-Fpo])
        0170fad4 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0170fb14 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fd9faf8  Cid 03bc.0778  Teb: 7ffab000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            89958878  NotificationEvent
            899dd8a8  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      1811           Ticks: 41688 (0:00:10:50.336)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address hidserv!HidThreadInputProc (0x72bf21b1)
        Stack Init a1ae9000 Current a1ae88d0 Base a1ae9000 Limit a1ae6000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1ae88e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1ae8924 81c28c64 nt!KiSwapThread+0x389
        a1ae8970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1ae8bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1ae8d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1ae8d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1ae8d64)
        0124f9d8 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0124f9dc 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0124fa78 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0124fa94 72bf2216 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0124fb10 75f33833 hidserv!HidThreadInputProc+0x65 (FPO: [Non-Fpo])
        0124fb1c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0124fb5c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fdc2d78  Cid 03bc.0788  Teb: 7ffa8000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fda0670  NotificationEvent
            9fda0b10  SynchronizationEvent
            9fdc2e00  NotificationTimer
        IRP List:
            9fc46428: (0006,01d8) Flags: 00060900  Mdl: 89875210
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      43492          Ticks: 7 (0:00:00:00.109)
        Context Switch Count      132
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address hidserv!HidThreadProc (0x72bf235c)
        Stack Init a1afd000 Current a1afc8d0 Base a1afd000 Limit a1afa000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a1afc8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1afc924 81c28c64 nt!KiSwapThread+0x389
        a1afc970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1afcbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1afcd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1afcd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1afcd64)
        0192fda4 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0192fda8 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0192fe44 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0192fe60 72bf240d kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0192fe9c 75f33833 hidserv!HidThreadProc+0xb6 (FPO: [Non-Fpo])
        0192fea8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0192fee8 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD a1805b68  Cid 03bc.07f4  Teb: 7ffa7000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            a1802980  SynchronizationEvent
            9fc69a00  SynchronizationEvent
            8987c248  SynchronizationEvent
            8987c1e0  SynchronizationEvent
            9fd90408  SynchronizationTimer
            9fde96a0  SynchronizationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      42203          Ticks: 1296 (0:00:00:20.217)
        Context Switch Count      1489
        UserTime                  00:00:02.808
        KernelTime                00:00:01.388
        Win32 Start Address emdmgmt!EcSvcWorkThread (0x72db146d)
        Stack Init a1acd000 Current a1acc8d0 Base a1acd000 Limit a1aca000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a1acc8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1acc924 81c28c64 nt!KiSwapThread+0x389
        a1acc970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1accbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1accd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1accd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1accd64)
        01e3fa6c 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01e3fa70 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        01e3fb0c 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        01e3fb28 72db1488 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        01e3fb44 75f33833 emdmgmt!EcSvcWorkThread+0x1b (FPO: [Non-Fpo])
        01e3fb50 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01e3fb90 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD a18a33b8  Cid 03bc.019c  Teb: 7ffa6000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            a18a61b0  NotificationEvent
            82f35f38  NotificationEvent
            82f35eb8  SynchronizationEvent
            9fd11f00  SynchronizationTimer
            9fd97a48  SynchronizationTimer
            9fd1fde8  NotificationEvent
            82f35ef8  SynchronizationEvent
            82f35f78  SynchronizationEvent
        Impersonation token:  a2839a20 (Level Impersonation)
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      43438          Ticks: 61 (0:00:00:00.951)
        Context Switch Count      1891
        UserTime                  00:00:01.606
        KernelTime                00:00:00.561
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x775cb9d5)
        Stack Init a082c000 Current a082b8d0 Base a082c000 Limit a0829000 Call 0
        Priority 7 BasePriority 7 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a082b8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a082b924 81c28c64 nt!KiSwapThread+0x389
        a082b970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a082bbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a082bd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a082bd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a082bd64)
        0133f110 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0133f114 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0133f1b0 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0133f1cc 72631810 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0133f914 7264ff33 sysmain!PfSvcMainThread+0x3d0 (FPO: [Non-Fpo])
        0133f93c 00dd148a sysmain!SysMtServiceMain+0xba (FPO: [Non-Fpo])
        0133f968 775cb9f6 svchost!ServiceStarter+0x17a (FPO: [Non-Fpo])
        0133f97c 75f33833 ADVAPI32!ScSvcctrlThreadA+0x21 (FPO: [Non-Fpo])
        0133f988 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0133f9c8 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fdf2d78  Cid 03bc.0358  Teb: 7ffa5000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fd92da8  Semaphore Limit 0x7fffffff
            9fdb0b20  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      40344          Ticks: 3155 (0:00:00:49.218)
        Context Switch Count      38
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x775cb9d5)
        Stack Init 85df8000 Current 85df78d0 Base 85df8000 Limit 85df5000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        85df78e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85df7924 81c28c64 nt!KiSwapThread+0x389
        85df7970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        85df7bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        85df7d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        85df7d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 85df7d64)
        0206fc04 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0206fc08 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0206fca4 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0206fcc0 72e72ffd kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0206fd10 72e731e2 wdi!WdipHostListener+0xbd (FPO: [Non-Fpo])
        0206fd38 72e73d43 wdi!WdipTriggerHost+0x179 (FPO: [Non-Fpo])
        0206fd50 00dd148a wdi!ServiceMain+0xe3 (FPO: [Non-Fpo])
        0206fd7c 775cb9f6 svchost!ServiceStarter+0x17a (FPO: [Non-Fpo])
        0206fd90 75f33833 ADVAPI32!ScSvcctrlThreadA+0x21 (FPO: [Non-Fpo])
        0206fd9c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0206fddc 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 89856540  Cid 03bc.06e8  Teb: 7ffa4000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            8988a280  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      9869           Ticks: 33630 (0:00:08:44.631)
        Context Switch Count      22
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdi!WdipSessionListener (0x72e71277)
        Stack Init 9f290000 Current 9f28fbc8 Base 9f290000 Limit 9f28d000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f28fbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f28fc1c 81cad431 nt!KiSwapThread+0x389
        9f28fc6c 81d8b982 nt!KeRemoveQueueEx+0x568
        9f28fcc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        9f28fd48 81c8caaa nt!NtRemoveIoCompletion+0x106
        9f28fd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f28fd64)
        0221fecc 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0221fed0 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        0221fefc 72e712f3 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        0221ff50 75f33833 wdi!WdipSessionListener+0xaa (FPO: [Non-Fpo])
        0221ff5c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0221ff9c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 89856288  Cid 03bc.0278  Teb: 7ffa3000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            8988a280  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      2058           Ticks: 41441 (0:00:10:46.483)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdi!WdipSessionListener (0x72e71277)
        Stack Init a1e2e000 Current a1e2dbc8 Base a1e2e000 Limit a1e2b000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1e2dbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1e2dc1c 81cad431 nt!KiSwapThread+0x389
        a1e2dc6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a1e2dcc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a1e2dd48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a1e2dd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1e2dd64)
        020dfd28 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        020dfd2c 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        020dfd58 72e712f3 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        020dfdac 75f33833 wdi!WdipSessionListener+0xaa (FPO: [Non-Fpo])
        020dfdb8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        020dfdf8 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD a1800030  Cid 03bc.02e8  Teb: 7ffa2000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            8988a280  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      40344          Ticks: 3155 (0:00:00:49.218)
        Context Switch Count      37
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdi!WdipSessionListener (0x72e71277)
        Stack Init a1e3e000 Current a1e3dbc8 Base a1e3e000 Limit a1e3b000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a1e3dbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1e3dc1c 81cad431 nt!KiSwapThread+0x389
        a1e3dc6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a1e3dcc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a1e3dd48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a1e3dd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1e3dd64)
        01dffbbc 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01dffbc0 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        01dffbec 72e712f3 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        01dffc40 75f33833 wdi!WdipSessionListener+0xaa (FPO: [Non-Fpo])
        01dffc4c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01dffc8c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD a1800770  Cid 03bc.045c  Teb: 7ffa1000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            8988a280  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      2058           Ticks: 41441 (0:00:10:46.483)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdi!WdipSessionListener (0x72e71277)
        Stack Init a1e42000 Current a1e41bc8 Base a1e42000 Limit a1e3f000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1e41be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1e41c1c 81cad431 nt!KiSwapThread+0x389
        a1e41c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a1e41cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a1e41d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a1e41d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1e41d64)
        0108fdd4 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0108fdd8 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        0108fe04 72e712f3 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        0108fe58 75f33833 wdi!WdipSessionListener+0xaa (FPO: [Non-Fpo])
        0108fe64 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0108fea4 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD a18004b8  Cid 03bc.02bc  Teb: 7ffa0000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            8988a280  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      40344          Ticks: 3155 (0:00:00:49.218)
        Context Switch Count      26
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdi!WdipSessionListener (0x72e71277)
        Stack Init a1e46000 Current a1e45bc8 Base a1e46000 Limit a1e43000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a1e45be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1e45c1c 81cad431 nt!KiSwapThread+0x389
        a1e45c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a1e45cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a1e45d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a1e45d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1e45d64)
        0141f948 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0141f94c 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        0141f978 72e712f3 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        0141f9cc 75f33833 wdi!WdipSessionListener+0xaa (FPO: [Non-Fpo])
        0141f9d8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0141fa18 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD a1d3a030  Cid 03bc.06e0  Teb: 7ff9f000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            8988a280  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      2058           Ticks: 41441 (0:00:10:46.483)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdi!WdipSessionListener (0x72e71277)
        Stack Init a1e4a000 Current a1e49bc8 Base a1e4a000 Limit a1e47000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1e49be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1e49c1c 81cad431 nt!KiSwapThread+0x389
        a1e49c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a1e49cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a1e49d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a1e49d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1e49d64)
        0227f8e0 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0227f8e4 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        0227f910 72e712f3 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        0227f964 75f33833 wdi!WdipSessionListener+0xaa (FPO: [Non-Fpo])
        0227f970 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0227f9b0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD a1d3a8d8  Cid 03bc.06dc  Teb: 7ff9e000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            8988a280  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      9869           Ticks: 33630 (0:00:08:44.631)
        Context Switch Count      19
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdi!WdipSessionListener (0x72e71277)
        Stack Init a1e4e000 Current a1e4dbc8 Base a1e4e000 Limit a1e4b000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1e4dbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1e4dc1c 81cad431 nt!KiSwapThread+0x389
        a1e4dc6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a1e4dcc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a1e4dd48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a1e4dd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1e4dd64)
        021bfbdc 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        021bfbe0 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        021bfc0c 72e712f3 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        021bfc60 75f33833 wdi!WdipSessionListener+0xaa (FPO: [Non-Fpo])
        021bfc6c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        021bfcac 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD a1d3a620  Cid 03bc.0384  Teb: 7ff9d000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            8988a280  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      2058           Ticks: 41441 (0:00:10:46.483)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdi!WdipSessionListener (0x72e71277)
        Stack Init a1e52000 Current a1e51bc8 Base a1e52000 Limit a1e4f000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1e51be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1e51c1c 81cad431 nt!KiSwapThread+0x389
        a1e51c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a1e51cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a1e51d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a1e51d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1e51d64)
        022cf83c 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        022cf840 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        022cf86c 72e712f3 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        022cf8c0 75f33833 wdi!WdipSessionListener+0xaa (FPO: [Non-Fpo])
        022cf8cc 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        022cf90c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD a1d3a368  Cid 03bc.0380  Teb: 7ff9c000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            8988a280  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      9869           Ticks: 33630 (0:00:08:44.631)
        Context Switch Count      11
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdi!WdipSessionListener (0x72e71277)
        Stack Init a1e56000 Current a1e55bc8 Base a1e56000 Limit a1e53000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1e55be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1e55c1c 81cad431 nt!KiSwapThread+0x389
        a1e55c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a1e55cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a1e55d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a1e55d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1e55d64)
        0234f938 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0234f93c 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        0234f968 72e712f3 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        0234f9bc 75f33833 wdi!WdipSessionListener+0xaa (FPO: [Non-Fpo])
        0234f9c8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0234fa08 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 847a8030  Cid 03bc.070c  Teb: 7ff9b000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            8988a280  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      2058           Ticks: 41441 (0:00:10:46.483)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdi!WdipSessionListener (0x72e71277)
        Stack Init a1e5e000 Current a1e5dbc8 Base a1e5e000 Limit a1e5b000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1e5dbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1e5dc1c 81cad431 nt!KiSwapThread+0x389
        a1e5dc6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a1e5dcc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a1e5dd48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a1e5dd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1e5dd64)
        0239f7a0 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0239f7a4 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        0239f7d0 72e712f3 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        0239f824 75f33833 wdi!WdipSessionListener+0xaa (FPO: [Non-Fpo])
        0239f830 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0239f870 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fc88d78  Cid 03bc.08a0  Teb: 7ff98000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            a18a8278  SynchronizationEvent
        Impersonation token:  a28b8a20 (Level Impersonation)
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      33630          Ticks: 9869 (0:00:02:33.957)
        Context Switch Count      13315
        UserTime                  00:00:00.046
        KernelTime                00:00:03.650
        Win32 Start Address sysmain!PfRbPrefetchWorker (0x72644b78)
        Stack Init 9e8af000 Current 9e8aec38 Base 9e8af000 Limit 9e8ac000 Call 0
        Priority 8 BasePriority 7 PriorityDecrement 0 IoPriority 0 PagePriority 5
        ChildEBP RetAddr
        9e8aec50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e8aec8c 81c293a7 nt!KiSwapThread+0x389
        9e8aece8 81df5057 nt!KeWaitForSingleObject+0x414
        9e8aed50 81c8caaa nt!NtWaitForSingleObject+0xbe
        9e8aed50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9e8aed64)
        0295f900 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0295f904 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0295f974 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        0295f988 72644be0 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0295f9a4 75f33833 sysmain!PfRbPrefetchWorker+0x68 (FPO: [Non-Fpo])
        0295f9b0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0295f9f0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 8369a588  Cid 03bc.08cc  Teb: 7ffd7000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            9e1e0b90  QueueObject
            8369a610  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      43357          Ticks: 142 (0:00:00:02.215)
        Context Switch Count      138
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address pcasvc!PcapProcessChainThread (0x72c33b0c)
        Stack Init a8e5e000 Current a8e5dbc8 Base a8e5e000 Limit a8e5b000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a8e5dbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8e5dc1c 81cad431 nt!KiSwapThread+0x389
        a8e5dc6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a8e5dcc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a8e5dd48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a8e5dd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8e5dd64)
        02b0f7fc 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        02b0f800 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        02b0f82c 72c33b44 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        02b0f854 75f33833 pcasvc!PcapProcessChainThread+0x38 (FPO: [Non-Fpo])
        02b0f860 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        02b0f8a0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 83687d78  Cid 03bc.009c  Teb: 7ff95000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Alertable
            a18b7f28  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      18561          Ticks: 24938 (0:00:06:29.035)
        Context Switch Count      4
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init 9f394000 Current 9f393bc8 Base 9f394000 Limit 9f391000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f393be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f393c1c 81cad431 nt!KiSwapThread+0x389
        9f393c68 81d8b982 nt!KeRemoveQueueEx+0x568
        9f393cc0 81c7a036 nt!IoRemoveIoCompletion+0x23
        9f393d54 81c8caaa nt!NtWaitForWorkViaWorkerFactory+0x1a1
        9f393d54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f393d64)
        02c7f6dc 77490850 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        02c7f6e0 7749a1b4 ntdll!NtWaitForWorkViaWorkerFactory+0xc (FPO: [2,0,0])
        02c7f808 75f33833 ntdll!TppWorkerThread+0x1f6 (FPO: [Non-Fpo])
        02c7f814 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        02c7f854 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fc427f8  Cid 03bc.090c  Teb: 7ff9a000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            9fc45390  QueueObject
            9fc42880  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      43413          Ticks: 86 (0:00:00:01.341)
        Context Switch Count      45
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init a1ac5000 Current a1ac4bc8 Base a1ac5000 Limit a1ac2000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a1ac4be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1ac4c1c 81cad431 nt!KiSwapThread+0x389
        a1ac4c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a1ac4cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a1ac4d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a1ac4d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1ac4d64)
        00fef8c8 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00fef8cc 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        00fef8f8 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        00fef934 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        00fef9a0 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        00fef9ac 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        00fef9d0 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        00fef9dc 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        00fef9e8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00fefa28 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fc7aac0  Cid 03bc.0f74  Teb: 7ff99000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            9fc45390  QueueObject
            9fc7ab48  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      43413          Ticks: 86 (0:00:00:01.341)
        Context Switch Count      11
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init 9e9cc000 Current 9e9cbbc8 Base 9e9cc000 Limit 9e9c9000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9e9cbbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e9cbc1c 81cad431 nt!KiSwapThread+0x389
        9e9cbc6c 81d8b982 nt!KeRemoveQueueEx+0x568
        9e9cbcc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        9e9cbd48 81c8caaa nt!NtRemoveIoCompletion+0x106
        9e9cbd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9e9cbd64)
        0197fa78 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0197fa7c 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        0197faa8 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        0197fae4 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        0197fb50 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        0197fb5c 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        0197fb84 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        0197fb90 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        0197fb9c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0197fbdc 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fce2d78  Cid 03bc.0a94  Teb: 7ff97000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            83512998  NotificationEvent
            82f406c8  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      40344          Ticks: 3155 (0:00:00:49.218)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address radardt!RdrpMonitorResources (0x6ea688fc)
        Stack Init a6853000 Current a68528d0 Base a6853000 Limit a6850000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a68528e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a6852924 81c28c64 nt!KiSwapThread+0x389
        a6852970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a6852bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a6852d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a6852d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a6852d64)
        02acf978 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        02acf97c 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        02acfa18 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        02acfa34 6ea68378 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        02acfa5c 6ea68a28 radardt!RdrpWaitForHighCommit+0x9c (FPO: [Non-Fpo])
        02acfaac 75f33833 radardt!RdrpMonitorResources+0x12c (FPO: [Non-Fpo])
        02acfab8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        02acfaf8 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 835d8d78  Cid 03bc.0b54  Teb: 7ff96000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            836535e8  NotificationEvent
            83586bf8  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      40344          Ticks: 3155 (0:00:00:49.218)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address radardt!RdrpMonitorCommitCharge (0x6ea6b5c7)
        Stack Init a8f14000 Current a8f138d0 Base a8f14000 Limit a8f11000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a8f138e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8f13924 81c28c64 nt!KiSwapThread+0x389
        a8f13970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a8f13bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a8f13d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a8f13d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8f13d64)
        02a7fb3c 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        02a7fb40 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        02a7fbdc 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        02a7fbf8 6ea6b6b3 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        02a7fc2c 75f33833 radardt!RdrpMonitorCommitCharge+0xec (FPO: [Non-Fpo])
        02a7fc38 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        02a7fc78 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 83920af8  Cid 03bc.056c  Teb: 7ffaf000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Alertable
            9fc58510  QueueObject
            83920b80  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      43411          Ticks: 88 (0:00:00:01.372)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init 9e8a3000 Current 9e8a2bc8 Base 9e8a3000 Limit 9e8a0000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9e8a2be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e8a2c1c 81cad431 nt!KiSwapThread+0x389
        9e8a2c68 81d8b982 nt!KeRemoveQueueEx+0x568
        9e8a2cc0 81c7a036 nt!IoRemoveIoCompletion+0x23
        9e8a2d54 81c8caaa nt!NtWaitForWorkViaWorkerFactory+0x1a1
        9e8a2d54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9e8a2d64)
        018bf938 77490850 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        018bf93c 7749a1b4 ntdll!NtWaitForWorkViaWorkerFactory+0xc (FPO: [2,0,0])
        018bfa64 75f33833 ntdll!TppWorkerThread+0x1f6 (FPO: [Non-Fpo])
        018bfa70 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        018bfab0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 836b8578  Cid 03bc.0304  Teb: 7ffd9000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Alertable
            9fc58510  QueueObject
            836b8600  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      43413          Ticks: 86 (0:00:00:01.341)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init 9f71c000 Current 9f71bbc8 Base 9f71c000 Limit 9f719000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f71bbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f71bc1c 81cad431 nt!KiSwapThread+0x389
        9f71bc68 81d8b982 nt!KeRemoveQueueEx+0x568
        9f71bcc0 81c7a036 nt!IoRemoveIoCompletion+0x23
        9f71bd54 81c8caaa nt!NtWaitForWorkViaWorkerFactory+0x1a1
        9f71bd54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f71bd64)
        02cef814 77490850 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        02cef818 7749a1b4 ntdll!NtWaitForWorkViaWorkerFactory+0xc (FPO: [2,0,0])
        02cef940 75f33833 ntdll!TppWorkerThread+0x1f6 (FPO: [Non-Fpo])
        02cef94c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        02cef98c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fc99030  Cid 03bc.0a30  Teb: 7ffac000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            9fc45390  QueueObject
            9fc990b8  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc38a48       Image:         svchost.exe
        Wait Start TickCount      43413          Ticks: 86 (0:00:00:01.341)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init a1ba0000 Current a1b9fbc8 Base a1ba0000 Limit a1b9d000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a1b9fbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1b9fc1c 81cad431 nt!KiSwapThread+0x389
        a1b9fc6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a1b9fcc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a1b9fd48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a1b9fd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1b9fd64)
        02b4f788 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        02b4f78c 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        02b4f7b8 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        02b4f7f4 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        02b4f860 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        02b4f86c 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        02b4f894 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        02b4f8a0 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        02b4f8ac 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        02b4f8ec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Svchost process (netsvcs)

```
PROCESS 9fc3dd90  SessionId: 0  Cid: 03cc    Peb: 7ffd7000  ParentCid: 0214
    DirBase: 29a011e0  ObjectTable: a008a458  HandleCount: 1138.
    Image: svchost.exe
    VadRoot a18ce2e8 Vads 330 Clone 0 Private 3196. Modified 1398. Locked 9.
    DeviceMap 85a03048
    Token                             a0092960
    ElapsedTime                       00:11:03.654
    UserTime                          00:00:00.686
    KernelTime                        00:00:00.468
    QuotaPoolUsage[PagedPool]         180952
    QuotaPoolUsage[NonPagedPool]      39848
    Working Set Sizes (now,min,max)  (5233, 50, 345) (20932KB, 200KB, 1380KB)
    PeakWorkingSetSize                6004
    VirtualSize                       103 Mb
    PeakVirtualSize                   133 Mb
    PageFaultCount                    12166
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      4723

    Setting context for this process...
.process /p /r ffffffff9fc3dd90

    !peb
PEB at 7ffd7000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00dd0000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00161720 . 01d46c78
    Ldr.InLoadOrderModuleList:           001616a0 . 01d46c68
    Ldr.InMemoryOrderModuleList:         001616a8 . 01d46c70
            Base TimeStamp                     Module
          dd0000 4549adc4 Nov 02 08:35:16 2006 C:\Windows\system32\svchost.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        75020000 4549bddb Nov 02 09:43:55 2006 C:\Windows\system32\NTMARTA.DLL
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        76310000 4549be44 Nov 02 09:45:40 2006 C:\Windows\system32\WLDAP32.dll
        75fe0000 4549be0e Nov 02 09:44:46 2006 C:\Windows\system32\WS2_32.dll
        77550000 4549bdc7 Nov 02 09:43:35 2006 C:\Windows\system32\NSI.dll
        75ce0000 4549bd99 Nov 02 09:42:49 2006 C:\Windows\system32\PSAPI.DLL
        75ad0000 4549bda8 Nov 02 09:43:04 2006 C:\Windows\system32\SAMLIB.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        74dc0000 4549bd02 Nov 02 09:40:18 2006 c:\windows\system32\mmcss.dll
        75390000 4549bcdc Nov 02 09:39:40 2006 c:\windows\system32\AVRT.dll
        74cc0000 4549bd95 Nov 02 09:42:45 2006 c:\windows\system32\profsvc.dll
        75ac0000 4549bddd Nov 02 09:43:57 2006 c:\windows\system32\SYSNTFY.dll
        75ba0000 4549bde2 Nov 02 09:44:02 2006 c:\windows\system32\USERENV.dll
        75b80000 4549bdd2 Nov 02 09:43:46 2006 c:\windows\system32\Secur32.dll
        74d30000 4549bd6b Nov 02 09:42:03 2006 c:\windows\system32\nlaapi.dll
        755b0000 4549bd3f Nov 02 09:41:19 2006 c:\windows\system32\IPHLPAPI.DLL
        75570000 46807ea6 Jun 26 03:49:10 2007 c:\windows\system32\dhcpcsvc.DLL
        75af0000 4549bcf1 Nov 02 09:40:01 2006 c:\windows\system32\DNSAPI.dll
        75560000 4549be1e Nov 02 09:45:02 2006 c:\windows\system32\WINNSI.DLL
```

```
        75540000 46807ea7 Jun 26 03:49:11 2007 c:\windows\system32\dhcpcsvc6.DLL
        74d00000 4549bcbc Nov 02 09:39:08 2006 c:\windows\system32\ATL.DLL
        745f0000 4549bce1 Nov 02 09:39:45 2006 c:\windows\system32\gpsvc.dll
        75840000 4549bd53 Nov 02 09:41:39 2006 c:\windows\system32\NETAPI32.dll
        75780000 4549bdcc Nov 02 09:43:40 2006 c:\windows\system32\NTDSAPI.dll
        74fe0000 46d779a1 Aug 31 03:14:57 2007 c:\windows\system32\WTSAPI32.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        75330000 4549bcd7 Nov 02 09:39:35 2006 c:\windows\system32\GPAPI.dll
        75610000 4679de70 Jun 21 03:12:00 2007 c:\windows\system32\slc.dll
        757b0000 4549bccf Nov 02 09:39:27 2006 c:\windows\system32\AUTHZ.dll
        75300000 4549be2e Nov 02 09:45:18 2006 c:\windows\system32\WINSTA.dll
        74c40000 4549bdbe Nov 02 09:43:26 2006 c:\windows\system32\shsvcs.dll
        74ca0000 4549bdd5 Nov 02 09:43:49 2006 c:\windows\system32\sens.dll
        744d0000 4549bcce Nov 02 09:39:26 2006 c:\windows\system32\eapsvc.dll
        74460000 4549bccb Nov 02 09:39:23 2006 C:\Windows\system32\eapphost.dll
        75350000 4549bdae Nov 02 09:43:10 2006 C:\Windows\system32\rsaenh.dll
        773a0000 4549bce9 Nov 02 09:39:53 2006 C:\Windows\system32\CLBCatQ.DLL
        73c50000 4549bcb0 Nov 02 09:38:56 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.6000.16386_none_87e0cb09378714f1\COMCTL32.dll
        74710000 4549bdb5 Nov 02 09:43:17 2006 c:\windows\system32\schedsvc.dll
        74d20000 4549bd8c Nov 02 09:42:36 2006 c:\windows\system32\ktmw32.dll
        763b0000 4549bdb9 Nov 02 09:43:21 2006 C:\Windows\system32\SHLWAPI.dll
        755d0000 4549bdf6 Nov 02 09:44:22 2006 c:\windows\system32\wevtapi.dll
        74aa0000 4549bd09 Nov 02 09:40:25 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_5d07289e07e1d100\comctl32.dll
        77030000 4549bdb0 Nov 02 09:43:12 2006 C:\Windows\system32\SETUPAPI.dll
        75480000 4549bd20 Nov 02 09:40:48 2006 C:\Windows\system32\credssp.dll
        75650000 45b96fde Jan 26 03:05:02 2007 C:\Windows\system32\CRYPT32.dll
        75820000 4549bd41 Nov 02 09:41:21 2006 C:\Windows\system32\MSASN1.dll
        75050000 46773a78 Jun 19 03:07:52 2007 C:\Windows\system32\schannel.dll
        74ff0000 4549be2f Nov 02 09:45:19 2006 C:\Windows\system32\WINTRUST.dll
        77580000 462434a3 Apr 17 03:44:51 2007 C:\Windows\system32\imagehlp.dll
        73f20000 4549be01 Nov 02 09:44:33 2006 C:\Windows\system32\wiarpc.dll
        73900000 4549bdd9 Nov 02 09:43:53 2006 C:\Windows\system32\taskcomp.dll
        753f0000 4549bde4 Nov 02 09:44:04 2006 C:\Windows\system32\VERSION.dll
        75250000 4549bd69 Nov 02 09:42:01 2006 C:\Windows\system32\mswsock.dll
        752c0000 4549be27 Nov 02 09:45:11 2006 C:\Windows\System32\wshtcpip.dll
        752b0000 4549be21 Nov 02 09:45:05 2006 C:\Windows\System32\wship6.dll
        746d0000 4549bde7 Nov 02 09:44:07 2006 C:\Windows\system32\UxTheme.dll
        73210000 4549bdc4 Nov 02 09:43:32 2006 c:\windows\system32\srvsvc.dll
        736b0000 4549bdc6 Nov 02 09:43:34 2006 C:\Windows\system32\SSCORE.DLL
        74f30000 46677f3a Jun 07 04:44:58 2007 C:\Windows\system32\FirewallAPI.DLL
        73340000 4549bcee Nov 02 09:39:58 2006 C:\Windows\system32\CLUSAPI.DLL
        731d0000 4549bcbd Nov 02 09:39:09 2006 C:\Windows\system32\ACTIVEDS.dll
        73190000 4549bcce Nov 02 09:39:26 2006 C:\Windows\system32\adsldpc.dll
        73160000 4549bd21 Nov 02 09:40:49 2006 C:\Windows\system32\credui.dll
        76560000 4681c95d Jun 27 03:20:13 2007 C:\Windows\system32\SHELL32.dll
        73140000 4549bdc8 Nov 02 09:43:36 2006 C:\Windows\system32\RESUTILS.DLL
        72f70000 4549bcd5 Nov 02 09:39:33 2006 c:\windows\system32\aelupsvc.dll
        75b20000 4549bcaf Nov 02 09:38:55 2006 c:\windows\system32\apphelp.dll
        72b10000 4549bd1c Nov 02 09:40:44 2006 c:\windows\system32\ikeext.dll
        735b0000 4549bce0 Nov 02 09:39:44 2006 c:\windows\system32\fwpuclnt.dll
        754f0000 4549bd49 Nov 02 09:41:29 2006 C:\Windows\system32\ncrypt.dll
        754a0000 4549bcb9 Nov 02 09:39:05 2006 C:\Windows\system32\BCRYPT.dll
        72b80000 4549bdcc Nov 02 09:43:40 2006 c:\windows\system32\seclogon.dll
        727d0000 4549be69 Nov 02 09:46:17 2006 c:\windows\system32\wbem\wmisvc.dll
        71fe0000 46d7799a Aug 31 03:14:50 2007 c:\windows\system32\wbem\wbemcomn.dll
        72590000 46677faf Jun 07 04:46:55 2007 c:\windows\system32\iphlpsvc.dll
        73950000 4549bdba Nov 02 09:43:22 2006 c:\windows\system32\rtutils.dll
        72830000 4549bdf0 Nov 02 09:44:16 2006 c:\windows\system32\sqmapi.dll
        74f10000 4549bcb8 Nov 02 09:39:04 2006 C:\Windows\system32\Cabinet.dll
        73420000 4549be18 Nov 02 09:44:56 2006 C:\Windows\system32\WINHTTP.dll
        72cb0000 4549bded Nov 02 09:44:13 2006 C:\Windows\system32\VSSAPI.DLL
        72e50000 4549bdef Nov 02 09:44:15 2006 C:\Windows\system32\vsstrace.dll
        73a70000 4549be05 Nov 02 09:44:37 2006 C:\Windows\system32\XmlLite.dll
        75750000 4549bd14 Nov 02 09:40:36 2006 C:\Windows\system32\MPR.dll
        744e0000 4549bd96 Nov 02 09:42:46 2006 C:\Windows\system32\PROPSYS.dll
        71be0000 4549bdec Nov 02 09:44:12 2006 C:\Windows\System32\Wbem\wbemcore.dll
        71cf0000 4549bcfb Nov 02 09:40:11 2006 C:\Windows\System32\Wbem\esscli.dll
        71b40000 4549bcd4 Nov 02 09:39:32 2006 C:\Windows\System32\Wbem\FastProx.dll
```

```
        71ef0000 4549bdf0 Nov 02 09:44:16 2006 C:\Windows\system32\wbem\wbemsvc.dll
        71b00000 4549be6b Nov 02 09:46:19 2006 C:\Windows\system32\wbem\wmiutils.dll
        71a60000 4549bdc5 Nov 02 09:43:33 2006 C:\Windows\system32\wbem\repdrvfs.dll
        717b0000 4549be67 Nov 02 09:46:15 2006 C:\Windows\system32\wbem\wmiprvsd.dll
        75b50000 4549bd46 Nov 02 09:41:26 2006 C:\Windows\system32\NCObjAPI.DLL
        71750000 4549bdee Nov 02 09:44:14 2006 C:\Windows\system32\wbem\wbemess.dll
        72f40000 4549be1f Nov 02 09:45:03 2006 C:\Windows\System32\winrnr.dll
        72f30000 4549bd3b Nov 02 09:41:15 2006 C:\Windows\system32\napinsp.dll
        72c10000 4549bdc0 Nov 02 09:43:28 2006 C:\Windows\system32\pnrpnsp.dll
        72c40000 4549be1d Nov 02 09:45:01 2006 C:\Windows\system32\wshbth.dll
        72a60000 4549bda2 Nov 02 09:42:58 2006 C:\Windows\system32\rasadhlp.dll
        71af0000 4549be04 Nov 02 09:44:36 2006 C:\Windows\system32\tschannel.dll
        71ee0000 4549be10 Nov 02 09:44:48 2006 C:\Windows\system32\wscapi.dll
        75dc0000 470c4de2 Oct 10 04:58:26 2007 C:\Windows\system32\urlmon.dll
        76360000 4549bcfb Nov 02 09:40:11 2006 C:\Windows\system32\iertutil.dll
        71ad0000 4549bd48 Nov 02 09:41:28 2006 C:\Windows\system32\wbem\ncprov.dll
        75a60000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\SXS.DLL
        70970000 4549bdac Nov 02 09:43:08 2006 c:\windows\system32\rasmans.dll
        75b60000 4549bd26 Nov 02 09:40:54 2006 c:\windows\system32\cryptdll.dll
        70a70000 4549bdb6 Nov 02 09:43:18 2006 C:\Windows\system32\rastapi.dll
        73960000 4549bdd1 Nov 02 09:43:45 2006 C:\Windows\system32\TAPI32.dll
        738c0000 4549be1d Nov 02 09:45:01 2006 C:\Windows\system32\WINMM.dll
        73880000 4549bd93 Nov 02 09:42:43 2006 C:\Windows\system32\OLEACC.dll
        739a0000 4549bdb2 Nov 02 09:43:14 2006 C:\Windows\system32\rasppp.dll
        73840000 4549bd15 Nov 02 09:40:37 2006 C:\Windows\system32\MPRAPI.dll
        73a20000 4549bda3 Nov 02 09:42:59 2006 C:\Windows\system32\RASAPI32.dll
        73a00000 4549bdab Nov 02 09:43:07 2006 C:\Windows\system32\rasman.dll
        75400000 4549bd7f Nov 02 09:42:23 2006 C:\Windows\system32\kerberos.dll
        70a10000 4549bdb3 Nov 02 09:43:15 2006 C:\Windows\system32\RASQEC.DLL
        709f0000 4549bda5 Nov 02 09:43:01 2006 C:\Windows\system32\QUtil.dll
        70430000 4549bda6 Nov 02 09:43:02 2006 C:\Windows\System32\raschap.dll
        70760000 4549bdb7 Nov 02 09:43:19 2006 C:\Windows\System32\rastls.dll
        70340000 4549bd2a Nov 02 09:40:58 2006 C:\Windows\system32\CRYPTUI.dll
        74cf0000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\MSIMG32.dll
        73ce0000 4549be24 Nov 02 09:45:08 2006 C:\Windows\system32\WinSCard.dll
        6e090000 46a6c0fe Jul 25 04:18:22 2007 c:\windows\system32\qmgr.dll
        70aa0000 4549bdb5 Nov 02 09:43:17 2006 c:\windows\system32\SHFOLDER.dll
        70a90000 4549bcc1 Nov 02 09:39:13 2006 c:\windows\system32\bitsperf.dll
        6fa70000 4549bcbf Nov 02 09:39:11 2006 C:\Windows\system32\bitsigd.dll
        6e850000 4549bdd6 Nov 02 09:43:50 2006 C:\Windows\system32\upnp.dll
        72a70000 4549bdc7 Nov 02 09:43:35 2006 C:\Windows\system32\SSDPAPI.dll
        72460000 4666193b Jun 06 03:17:31 2007 C:\Windows\System32\msxml3.dll
        6d950000 46ae8ef5 Jul 31 02:23:01 2007 c:\windows\system32\wuaueng.dll
        718b0000 4549bcf9 Nov 02 09:40:09 2006 c:\windows\system32\ESENT.dll
        715a0000 4549be2a Nov 02 09:45:14 2006 c:\windows\system32\WINSPOOL.DRV
        6f5b0000 4549bd36 Nov 02 09:41:10 2006 c:\windows\system32\mspatcha.dll
        757a0000 4549be18 Nov 02 09:44:56 2006 C:\Windows\system32\WMsgAPI.dll
        6db20000 4549bd1d Nov 02 09:40:45 2006 C:\Windows\system32\dssenh.dll
        6e8b0000 4549bcb1 Nov 02 09:38:57 2006 c:\windows\system32\appinfo.dll
    SubSystemData:     00000000
    ProcessHeap:       00160000
    ProcessParameters: 00160fd8
    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;C:\Program Files\QuickTime\QTSystem\'
    Environment:  001607e8
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\system32\config\systemprofile\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        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:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\TEMP
        TMP=C:\Windows\TEMP
        USERDOMAIN=WORKGROUP
        USERNAME=HOME$
        USERPROFILE=C:\Windows\system32\config\systemprofile
        windir=C:\Windows


        THREAD 9fc3d030  Cid 03cc.03d0  Teb: 7ffdf000 Win32Thread: ff4f20c0 WAIT: (Executive)
UserMode Non-Alertable
            9fc37bb4  NotificationEvent
        IRP List:
            9fce77f8: (0006,0094) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      18395          Ticks: 25104 (0:00:06:31.624)
        Context Switch Count      217
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address svchost!wmainCRTStartup (0x00dd20bf)
        Stack Init 9f274000 Current 9f273bc8 Base 9f274000 Limit 9f271000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f273be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f273c1c 81c293a7 nt!KiSwapThread+0x389
        9f273c78 81d88faf nt!KeWaitForSingleObject+0x414
        9f273cac 81d93669 nt!IopSynchronousServiceTail+0x258
        9f273d38 81c8caaa nt!NtReadFile+0x646
        9f273d38 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f273d64)
        000ef6e0 77490080 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        000ef6e4 75f3853f ntdll!ZwReadFile+0xc (FPO: [9,0,0])
        000ef75c 775cffe2 kernel32!ReadFile+0x20e (FPO: [Non-Fpo])
        000ef788 775cfdfb ADVAPI32!ScGetPipeInput+0x2a (FPO: [Non-Fpo])
        000ef7f0 775cbdd2 ADVAPI32!ScDispatcherLoop+0x6c (FPO: [Non-Fpo])
        000efa68 00dd241d ADVAPI32!StartServiceCtrlDispatcherW+0xce (FPO: [Non-Fpo])
        000efa70 00dd2401 svchost!SvcHostMain+0x12 (FPO: [Non-Fpo])
        000efa74 00dd2183 svchost!wmain+0x5 (FPO: [Non-Fpo])
        000efab8 75f33833 svchost!_initterm_e+0x163 (FPO: [Non-Fpo])
        000efac4 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        000efb04 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fc56b88  Cid 03cc.03e4  Teb: 7ffde000 Win32Thread: 00000000 WAIT: (DelayExecution)
UserMode Alertable
            9fc56c10  NotificationTimer
        Impersonation token:  a00b7030 (Level Delegation)
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      24701          Ticks: 18798 (0:00:04:53.250)
        Context Switch Count      4325
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x775cb9d5)
        Stack Init 9f288000 Current 9f287c58 Base 9f288000 Limit 9f285000 Call 0
        Priority 27 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f287c70 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f287cac 81cac48e nt!KiSwapThread+0x389
        9f287d08 81e90bf1 nt!KeDelayExecutionThread+0x397
        9f287d54 81c8caaa nt!NtDelayExecution+0x8d
        9f287d54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f287d64)
        00d8fa88 7748f7c0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00d8fa8c 74dc195a ntdll!NtDelayExecution+0xc (FPO: [2,0,0])
        00d8fa98 74dc3a2d mmcss!CiSchedulerStart+0x31 (FPO: [Non-Fpo])
        00d8faf0 74dc3964 mmcss!CiSchedulerInitiailize+0xbf (FPO: [Non-Fpo])
        00d8faf8 00dd148a mmcss!CsServiceMain+0x4a (FPO: [Non-Fpo])
        00d8fb24 775cb9f6 svchost!ServiceStarter+0x17a (FPO: [Non-Fpo])
        00d8fb38 75f33833 ADVAPI32!ScSvcctrlThreadA+0x21 (FPO: [Non-Fpo])
        00d8fb44 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00d8fb84 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fc56668  Cid 03cc.03e8  Teb: 7ffdd000 Win32Thread: 00000000 WAIT: (WrLpcReceive)
UserMode Non-Alertable
            9fc5687c  Semaphore Limit 0x1
            9fc566f0  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      43274          Ticks: 225 (0:00:00:03.510)
        Context Switch Count      320
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address mmcss!CsServerApiLoop (0x74dc344a)
        Stack Init 9f284000 Current 9f283b78 Base 9f284000 Limit 9f281000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f283b90 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f283bcc 81c293a7 nt!KiSwapThread+0x389
        9f283c2c 81dc3dac nt!KeWaitForSingleObject+0x414
        9f283c64 81dc436e nt!AlpcpReceiveMessagePort+0x221
        9f283ce0 81dc6211 nt!AlpcpReceiveMessage+0x163
        9f283d3c 81c8caaa nt!NtAlpcSendWaitReceivePort+0x11c
        9f283d3c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f283d64)
        00d1fc5c 7748f2c0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00d1fc60 74dc120d ntdll!NtAlpcSendWaitReceivePort+0xc (FPO: [8,0,0])
        00d1fe0c 74dc3463 mmcss!CiServerApiLoop+0x9f (FPO: [Non-Fpo])
        00d1fe44 75f33833 mmcss!CsServerApiLoop+0x3e (FPO: [Non-Fpo])
        00d1fe50 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00d1fe90 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fc87030  Cid 03cc.043c  Teb: 7ffdb000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fc9c560  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      1075           Ticks: 42424 (0:00:11:01.818)
        Context Switch Count      69
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x775cb9d5)
        Stack Init 9f208000 Current 9f207c38 Base 9f208000 Limit 9f205000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f207c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f207c8c 81c293a7 nt!KiSwapThread+0x389
        9f207ce8 81df5057 nt!KeWaitForSingleObject+0x414
        9f207d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        9f207d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f207d64)
        00e6fb28 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00e6fb2c 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        00e6fb9c 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        00e6fbb0 74cc7964 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        00e6fbc0 74cc7926 profsvc!CUserProfileService::ServiceMain+0x2c (FPO: [Non-Fpo])
        00e6fbcc 00dd148a profsvc!UserProfileServiceMain+0x52 (FPO: [Non-Fpo])
        00e6fbf8 775cb9f6 svchost!ServiceStarter+0x17a (FPO: [Non-Fpo])
        00e6fc0c 75f33833 ADVAPI32!ScSvcctrlThreadA+0x21 (FPO: [Non-Fpo])
        00e6fc18 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00e6fc58 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fc896c0  Cid 03cc.044c  Teb: 7ffda000 Win32Thread: 00000000 WAIT: (WrLpcReceive)
UserMode Non-Alertable
            9fc898d4  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      29067          Ticks: 14432 (0:00:03:45.140)
        Context Switch Count      233
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x775cb9d5)
        Stack Init a033c000 Current a033bb70 Base a033c000 Limit a0339000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a033bb88 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a033bbc4 81c293a7 nt!KiSwapThread+0x389
        a033bc24 81dc3dac nt!KeWaitForSingleObject+0x414
        a033bc5c 81dc486e nt!AlpcpReceiveMessagePort+0x221
        a033bcc4 81dbe7b6 nt!AlpcpReceiveLegacyMessage+0x197
        a033bd30 81dbe69c nt!NtReplyWaitReceivePortEx+0x100
        a033bd4c 81c8caaa nt!NtReplyWaitReceivePort+0x18
        a033bd4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a033bd64)
        0012f978 77490140 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0012f97c 74c41569 ntdll!ZwReplyWaitReceivePort+0xc (FPO: [4,0,0])
        0012faac 74c41517 shsvcs!CAPIConnection::ListenToServerConnectionPort+0x42 (FPO: [Non-Fpo])
        0012fab8 74c4fbc3 shsvcs!CAPIConnection::Listen+0x1b (FPO: [Non-Fpo])
        0012fac8 74c4faf7 shsvcs!CService::Start+0x8b (FPO: [Non-Fpo])
        0012fad8 00dd148a shsvcs!ThemeServiceMain+0x84 (FPO: [Non-Fpo])
        0012fb04 775cb9f6 svchost!ServiceStarter+0x17a (FPO: [Non-Fpo])
        0012fb18 75f33833 ADVAPI32!ScSvcctrlThreadA+0x21 (FPO: [Non-Fpo])
        0012fb24 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0012fb64 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fc964d8  Cid 03cc.047c  Teb: 7ffd6000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fd10360  SynchronizationEvent
            9fd0f8d0  SynchronizationEvent
        IRP List:
            9fd068f8: (0006,01d8) Flags: 00060970  Mdl: 00000000
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      1125           Ticks: 42374 (0:00:11:01.038)
        Context Switch Count      19
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init 9f234000 Current 9f2338d0 Base 9f234000 Limit 9f231000 Call 0
        Priority 13 BasePriority 8 PriorityDecrement 5 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f2338e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f233924 81c28c64 nt!KiSwapThread+0x389
        9f233970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f233bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f233d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f233d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f233d64)
        0143fc28 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0143fc2c 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0143fcc8 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0143fce4 74c49f40 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0143fd44 74c43029 shsvcs!Wia::MailslotServer::_DoStuff+0xae (FPO: [Non-Fpo])
        0143fd60 74c42fca shsvcs!CThreadTask::_CallDoStuff+0x42 (FPO: [Non-Fpo])
        0143fd70 7746fe6d shsvcs!CThreadTask::_ThreadProc+0x11 (FPO: [Non-Fpo])
        0143fdd4 7749a2b8 ntdll!RtlpTpWorkCallback+0xbf (FPO: [Non-Fpo])
        0143fefc 75f33833 ntdll!TppWorkerThread+0x522 (FPO: [Non-Fpo])
        0143ff08 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0143ff48 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fc98ad0  Cid 03cc.0480  Teb: 7ffd5000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            9fc98e50  SynchronizationTimer
            9fc9d2d8  SynchronizationEvent
            9fc92550  SynchronizationTimer
            9fc92750  SynchronizationEvent
            9fd1b358  SynchronizationEvent
            9fd13970  SynchronizationEvent
            9fd15a10  SynchronizationEvent
            9fd14578  SynchronizationEvent
            9fd19530  SynchronizationEvent
            9fd34980  SynchronizationEvent
            899e3020  ProcessObject
            9fd4abd0  SynchronizationEvent
            9fc48868  SynchronizationEvent
            9fdca1b8  SynchronizationEvent
            9fd79020  SynchronizationEvent
            9fc2b1d8  NotificationEvent
            9fde3050  SynchronizationEvent
            9fde3370  SynchronizationEvent
            9fdff020  SynchronizationEvent
            8987ac78  SynchronizationEvent
            899e7358  SynchronizationEvent
            9fc547a8  SynchronizationEvent
            a18f7438  SynchronizationEvent
            a18d3bf0  SynchronizationEvent
            a18dec70  SynchronizationEvent
            a18ddce8  SynchronizationEvent
            a18df518  SynchronizationEvent
            a18f7090  SynchronizationEvent
            89878470  SynchronizationEvent
            a18f50c8  SynchronizationEvent
            a18d3698  SynchronizationTimer
            a18f56b0  SynchronizationEvent
            a18cafb8  SynchronizationEvent
            a18caf88  SynchronizationEvent
            a18c0990  SynchronizationEvent
            a18c0960  SynchronizationEvent
            a18f7798  SynchronizationEvent
            9fdb3458  NotificationEvent
            a18a8150  NotificationEvent
            a18d0bc8  SynchronizationTimer
            9fd35ad8  SynchronizationEvent
            9fdba3e0  SynchronizationEvent
            89860020  ProcessObject
            899fa3d8  SynchronizationEvent
            a18adff0  SynchronizationEvent
            9fd24630  SynchronizationEvent
            9fd6bd98  SynchronizationEvent
            9fd93a38  SynchronizationEvent
            8346d618  ProcessObject
            a1805898  SynchronizationEvent
            837d6c60  SynchronizationEvent
            9fdb5240  SynchronizationEvent
            9fc14830  SynchronizationEvent
            a18de390  SynchronizationEvent
            847b2320  SynchronizationEvent
            9fdede68  SynchronizationEvent
            8373f318  SynchronizationEvent
            9fc8aee8  SynchronizationEvent
            a18c2f60  SynchronizationEvent
            a18de9f0  SynchronizationEvent
            a18d0a80  SynchronizationTimer
            a18f56e0  SynchronizationTimer
            9fc92498  SynchronizationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      42252          Ticks: 1247 (0:00:00:19.453)
        Context Switch Count      820
```

```
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x7744b49a)
        Stack Init a0334000 Current a03338d0 Base a0334000 Limit a0331000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a03338e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0333924 81c28c64 nt!KiSwapThread+0x389
        a0333970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a0333bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a0333d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a0333d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0333d64)
        0113fcb4 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0113fcb8 7744b65b ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0113fe54 75f33833 ntdll!TppWaiterpThread+0x294 (FPO: [Non-Fpo])
        0113fe60 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0113fea0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fcc8d78  Cid 03cc.04ec  Teb: 7ffd4000 Win32Thread: ff506668 WAIT: (UserRequest)
UserMode Non-Alertable
            9fcdca18  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      1094           Ticks: 42405 (0:00:11:01.522)
        Context Switch Count      94
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x775cb9d5)
        Stack Init a0286000 Current a0285c38 Base a0286000 Limit a0283000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a0285c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0285c8c 81c293a7 nt!KiSwapThread+0x389
        a0285ce8 81df5057 nt!KeWaitForSingleObject+0x414
        a0285d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a0285d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0285d64)
        0130fa68 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0130fa6c 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0130fadc 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        0130faf0 744d45cb kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0130fb00 744d509c eapsvc!ObjectHandle::Wait+0x11 (FPO: [Non-Fpo])
        0130fb38 744d32be eapsvc!ServiceManager::ExecuteService+0x55 (FPO: [Non-Fpo])
        0130fbc0 00dd148a eapsvc!ServiceMain+0x29 (FPO: [Non-Fpo])
        0130fbec 775cb9f6 svchost!ServiceStarter+0x17a (FPO: [Non-Fpo])
        0130fc00 75f33833 ADVAPI32!ScSvcctrlThreadA+0x21 (FPO: [Non-Fpo])
        0130fc0c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0130fc4c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fd05d78  Cid 03cc.0558  Teb: 7ffaf000 Win32Thread: ff506168 WAIT: (UserRequest)
UserMode Non-Alertable
            9fd03250  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      9162           Ticks: 34337 (0:00:08:55.660)
        Context Switch Count      315
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x775cb9d5)
        Stack Init a09cd000 Current a09ccc38 Base a09cd000 Limit a09ca000 Call 0
        Priority 12 BasePriority 8 PriorityDecrement 3 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a09ccc50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a09ccc8c 81c293a7 nt!KiSwapThread+0x389
        a09ccce8 81df5057 nt!KeWaitForSingleObject+0x414
        a09ccd50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a09ccd50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a09ccd64)
        015af5fc 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        015af600 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        015af670 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        015af684 74c42991 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        015af698 74c4c97a shsvcs!GSM::_RunService+0x30 (FPO: [Non-Fpo])
        015af6b8 74c4c85a shsvcs!GSM::_ServiceMainHelper+0x129 (FPO: [Non-Fpo])
        015af6c0 74c43029 shsvcs!GSM::CServiceMainTask::_DoStuff+0x9 (FPO: [Non-Fpo])
        015af6dc 74c4aa55 shsvcs!CThreadTask::_CallDoStuff+0x42 (FPO: [Non-Fpo])
        015af6e4 74c4c834 shsvcs!CThreadTask::RunSynchronously+0xa (FPO: [Non-Fpo])
        015af780 00dd148a shsvcs!GSM::ServiceMain+0x58 (FPO: [Non-Fpo])
        015af7ac 775cb9f6 svchost!ServiceStarter+0x17a (FPO: [Non-Fpo])
        015af7c0 75f33833 ADVAPI32!ScSvcctrlThreadA+0x21 (FPO: [Non-Fpo])
        015af7cc 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        015af80c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fd09388  Cid 03cc.055c  Teb: 7ffae000 Win32Thread: ff508128 WAIT: (UserRequest)
UserMode Non-Alertable
            9fd0f0d0  SynchronizationEvent
            9fd46a90  SynchronizationEvent
            9fce1818  SynchronizationEvent
            9fd09410  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      1825           Ticks: 41674 (0:00:10:50.118)
        Context Switch Count      264
        UserTime                  00:00:00.015
        KernelTime                00:00:00.015
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x775cb9d5)
        Stack Init a035c000 Current a035b8d0 Base a035c000 Limit a0359000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a035b8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a035b924 81c28c64 nt!KiSwapThread+0x389
        a035b970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a035bbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a035bd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a035bd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a035bd64)
        00e2f924 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00e2f928 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00e2f9c4 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        00e2f9e0 747239d8 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        00e2fb48 74729949 schedsvc!Scheduler::TimerThreadFunction+0x1dd (FPO: [Non-Fpo])
        00e2fb90 7472be6d schedsvc!JobsService::WorkerThread+0xa3 (FPO: [Non-Fpo])
        00e2fba8 7472bd7a schedsvc!CNtService::Run+0xd1 (FPO: [Non-Fpo])
        00e2fc54 00dd148a schedsvc!ServiceMain+0x3a (FPO: [Non-Fpo])
        00e2fc80 775cb9f6 svchost!ServiceStarter+0x17a (FPO: [Non-Fpo])
        00e2fc94 75f33833 ADVAPI32!ScSvcctrlThreadA+0x21 (FPO: [Non-Fpo])
        00e2fca0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00e2fce0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fd1ba00  Cid 03cc.0568  Teb: 7ffad000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Alertable
            9fd1b308  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      25158          Ticks: 18341 (0:00:04:46.121)
        Context Switch Count      45
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init a0979000 Current a0978bc8 Base a0979000 Limit a0976000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a0978be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0978c1c 81cad431 nt!KiSwapThread+0x389
        a0978c68 81d8b982 nt!KeRemoveQueueEx+0x568
        a0978cc0 81c7a036 nt!IoRemoveIoCompletion+0x23
        a0978d54 81c8caaa nt!NtWaitForWorkViaWorkerFactory+0x1a1
        a0978d54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0978d64)
        015efb84 77490850 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        015efb88 7749a1b4 ntdll!NtWaitForWorkViaWorkerFactory+0xc (FPO: [2,0,0])
        015efcb0 75f33833 ntdll!TppWorkerThread+0x1f6 (FPO: [Non-Fpo])
        015efcbc 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        015efcfc 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fc6f3d8  Cid 03cc.0570  Teb: 7ffac000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fd1add0  SynchronizationEvent
            9fce17e8  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      9488           Ticks: 34011 (0:00:08:50.575)
        Context Switch Count      277
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address schedsvc!CSessionMgr::StartJobsCallback (0x7472c8d1)
        Stack Init a0272000 Current a02718d0 Base a0272000 Limit a026f000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a02718e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0271924 81c28c64 nt!KiSwapThread+0x389
        a0271970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a0271bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a0271d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a0271d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0271d64)
        006ffc70 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        006ffc74 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        006ffd10 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        006ffd2c 747139ab kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        006ffd6c 7472c916 schedsvc!CSessionMgr::LaunchLoop+0x44 (FPO: [Non-Fpo])
        006ffdb4 75f33833 schedsvc!CSessionMgr::StartJobsCallback+0x7c (FPO: [Non-Fpo])
        006ffdc0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        006ffe00 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fd199c8  Cid 03cc.0590  Teb: 7ffab000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            89947e70  SynchronizationEvent
            9fc54748  SynchronizationEvent
            899bc648  SynchronizationEvent
            899bc020  SynchronizationTimer
            9fcd85c8  SynchronizationTimer
        IRP List:
            9fc355b8: (0006,01d8) Flags: 00060000  Mdl: 00000000
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      1230           Ticks: 42269 (0:00:10:59.400)
        Context Switch Count      10
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address taskcomp!CompatibilityAdapter::MonitorThread (0x73902c56)
        Stack Init a0975000 Current a09748d0 Base a0975000 Limit a0972000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a09748e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0974924 81c28c64 nt!KiSwapThread+0x389
        a0974970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a0974bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a0974d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a0974d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0974d64)
        018cfcf0 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        018cfcf4 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        018cfd90 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        018cfdac 73902cd3 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        018cfdf8 75f33833 taskcomp!CompatibilityAdapter::MonitorThread+0xa0 (FPO: [Non-Fpo])
        018cfe04 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        018cfe44 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fd21030  Cid 03cc.0594  Teb: 7ffaa000 Win32Thread: ff4e02b8 WAIT: (UserRequest)
UserMode Non-Alertable
            9fce17e8  NotificationEvent
            9fc50a80  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      8892           Ticks: 34607 (0:00:08:59.872)
        Context Switch Count      34
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address schedsvc!JobsService::MsgPumpThread (0x74718ae9)
        Stack Init a097d000 Current a097c8d0 Base a097d000 Limit a097a000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a097c8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a097c924 81c28c64 nt!KiSwapThread+0x389
        a097c970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a097cbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a097cd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a097cd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a097cd64)
        014bfb18 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        014bfb1c 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        014bfbb8 761dc4b7 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        014bfc0c 761d8b83 USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
        014bfc28 74718b9f USER32!MsgWaitForMultipleObjects+0x1f (FPO: [Non-Fpo])
        014bfc94 75f33833 schedsvc!JobsService::MsgPumpThread+0x119 (FPO: [Non-Fpo])
        014bfca0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        014bfce0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fd4ad78  Cid 03cc.05e4  Teb: 7ffa7000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fd321a0  NotificationEvent
            9fd52b30  SynchronizationEvent
            9fd52b00  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      1194           Ticks: 42305 (0:00:10:59.962)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address gpsvc!GPOThread (0x745fad8b)
        Stack Init a0935000 Current a09348d0 Base a0935000 Limit a0932000 Call 0
        Priority 1 BasePriority 1 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a09348e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0934924 81c28c64 nt!KiSwapThread+0x389
        a0934970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a0934bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a0934d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a0934d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0934d64)
        0136f654 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0136f658 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0136f6f4 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0136f710 745fafed kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0136f828 75f33833 gpsvc!GPOThread+0x2d1 (FPO: [Non-Fpo])
        0136f834 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0136f874 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9e1f1b18  Cid 03cc.0680  Teb: 7ffa8000 Win32Thread: ff5063e8 WAIT: (UserRequest)
UserMode Non-Alertable
            9fd8dd38  SynchronizationEvent
            9fd6c100  SynchronizationEvent
            9fdcc148  SynchronizationEvent
            9fdb6ff0  SynchronizationEvent
            9fdaa6e8  SynchronizationEvent
            9fdcd380  SynchronizationEvent
            9fdb0b98  SynchronizationEvent
            9e1f1ba0  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      32552          Ticks: 10947 (0:00:02:50.774)
        Context Switch Count      454
        UserTime                  00:00:00.062
        KernelTime                00:00:00.015
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x775cb9d5)
        Stack Init a0810000 Current a080f8d0 Base a0810000 Limit a080d000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a080f8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a080f924 81c28c64 nt!KiSwapThread+0x389
        a080f970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a080fbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a080fd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a080fd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a080fd64)
        00dcf830 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00dcf834 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00dcf8d0 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        00dcf8ec 7321433f kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        00dcf974 73214e2d srvsvc!SsScavengerThread+0x368 (FPO: [Non-Fpo])
        00dcf994 00dd148a srvsvc!ServiceMain+0x186 (FPO: [Non-Fpo])
        00dcf9c0 775cb9f6 svchost!ServiceStarter+0x17a (FPO: [Non-Fpo])
        00dcf9d4 75f33833 ADVAPI32!ScSvcctrlThreadA+0x21 (FPO: [Non-Fpo])
        00dcf9e0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00dcfa20 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 899f7d78  Cid 03cc.06f4  Teb: 7ffa4000 Win32Thread: 00000000 WAIT: (WrLpcReceive)
UserMode Non-Alertable
            899f7f8c  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      3719           Ticks: 39780 (0:00:10:20.571)
        Context Switch Count      6
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address srvsvc!XsProcessApisWrapper (0x7321462f)
        Stack Init 9e8c7000 Current 9e8c6b88 Base 9e8c7000 Limit 9e8c4000 Call 0
        Priority 11 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9e8c6ba0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e8c6bdc 81c293a7 nt!KiSwapThread+0x389
        9e8c6c3c 81dc3dac nt!KeWaitForSingleObject+0x414
        9e8c6c74 81dc486e nt!AlpcpReceiveMessagePort+0x221
        9e8c6cdc 81dbe7b6 nt!AlpcpReceiveLegacyMessage+0x197
        9e8c6d48 81c8caaa nt!NtReplyWaitReceivePortEx+0x100
        9e8c6d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9e8c6d64)
        0147fcd0 77490150 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0147fcd4 732146f0 ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        0147fe14 7321465a srvsvc!XsProcessApis+0x73 (FPO: [Non-Fpo])
        0147fe90 75f33833 srvsvc!XsProcessApisWrapper+0x2b (FPO: [Non-Fpo])
        0147fe9c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0147fedc 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 898548f8  Cid 03cc.0710  Teb: 7ffa2000 Win32Thread: 00000000 WAIT: (WrLpcReceive)
UserMode Non-Alertable
            89854b0c  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      18559          Ticks: 24940 (0:00:06:29.066)
        Context Switch Count      25
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address aelupsvc!AelpProcessLPCCalls (0x72f73fa2)
        Stack Init 9f24c000 Current 9f24bb78 Base 9f24c000 Limit 9f249000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f24bb90 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f24bbcc 81c293a7 nt!KiSwapThread+0x389
        9f24bc2c 81dc3dac nt!KeWaitForSingleObject+0x414
        9f24bc64 81dc436e nt!AlpcpReceiveMessagePort+0x221
        9f24bce0 81dc6211 nt!AlpcpReceiveMessage+0x163
        9f24bd3c 81c8caaa nt!NtAlpcSendWaitReceivePort+0x11c
        9f24bd3c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f24bd64)
        0197fef4 7748f2c0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0197fef8 72f74036 ntdll!NtAlpcSendWaitReceivePort+0xc (FPO: [8,0,0])
        0197ff5c 75f33833 aelupsvc!AelpProcessLPCCalls+0x94 (FPO: [Non-Fpo])
        0197ff68 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0197ffa8 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 89854640  Cid 03cc.0714  Teb: 7ffa0000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            89846890  SynchronizationEvent
            899b4d40  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      18560          Ticks: 24939 (0:00:06:29.050)
        Context Switch Count      61
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address aelupsvc!AelTppDispatcherThreadRoutine (0x72f7482d)
        Stack Init 9e9ec000 Current 9e9eb8d0 Base 9e9ec000 Limit 9e9e9000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9e9eb8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e9eb924 81c28c64 nt!KiSwapThread+0x389
        9e9eb970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9e9ebbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9e9ebd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9e9ebd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9e9ebd64)
        01d9f980 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01d9f984 72f74865 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        01d9f9ac 75f33833 aelupsvc!AelTppDispatcherThreadRoutine+0x38 (FPO: [Non-Fpo])
        01d9f9b8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01d9f9f8 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 89854388  Cid 03cc.0718  Teb: 7ff9f000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            899b4d10  NotificationEvent
            847d4990  NotificationEvent
            89854410  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      41637          Ticks: 1862 (0:00:00:29.047)
        Context Switch Count      69
        UserTime                  00:00:00.046
        KernelTime                00:00:00.015
        Win32 Start Address aelupsvc!AelTppWorkerThreadRoutine (0x72f74526)
        Stack Init 9e99c000 Current 9e99b8d0 Base 9e99c000 Limit 9e999000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9e99b8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e99b924 81c28c64 nt!KiSwapThread+0x389
        9e99b970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9e99bbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9e99bd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9e99bd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9e99bd64)
        01a9fe3c 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01a9fe40 72f7455e ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        01a9fe70 75f33833 aelupsvc!AelTppWorkerThreadRoutine+0x38 (FPO: [Non-Fpo])
        01a9fe7c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01a9febc 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fde6d78  Cid 03cc.07b0  Teb: 7ff9c000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fdfdff0  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      1815           Ticks: 41684 (0:00:10:50.274)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address AUTHZ!AuthzpDeQueueThreadWorker (0x757b68c9)
        Stack Init a1aed000 Current a1aecc38 Base a1aed000 Limit a1aea000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1aecc50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1aecc8c 81c293a7 nt!KiSwapThread+0x389
        a1aecce8 81df5057 nt!KeWaitForSingleObject+0x414
        a1aecd50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a1aecd50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1aecd64)
        020ffb1c 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        020ffb20 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        020ffb90 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        020ffba4 757b68ef kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        020ffbc0 75f33833 AUTHZ!AuthzpDeQueueThreadWorker+0xa2 (FPO: [Non-Fpo])
        020ffbcc 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        020ffc0c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD a1806d78  Cid 03cc.07f8  Teb: 7ff9d000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            9fdffe90  NotificationEvent
            9fdeb140  SynchronizationEvent
            9fdfcff0  SynchronizationEvent
            9fde42c0  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      1815           Ticks: 41684 (0:00:10:50.274)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ikeext!IkeReceiveThread (0x72b11ea0)
        Stack Init a1ac9000 Current a1ac88d0 Base a1ac9000 Limit a1ac6000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1ac88e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1ac8924 81c28c64 nt!KiSwapThread+0x389
        a1ac8970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1ac8bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1ac8d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1ac8d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1ac8d64)
        020bfc88 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        020bfc8c 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        020bfd28 72b11f47 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        020bfe24 75f33833 ikeext!IkeReceiveThread+0xa7 (FPO: [Non-Fpo])
        020bfe30 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        020bfe70 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD a18b4898  Cid 03cc.015c  Teb: 7ffa1000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            a18ddc80  NotificationEvent
            a18c2660  SynchronizationEvent
            a18c2358  SynchronizationEvent
            a18d3d24  NotificationEvent
        IRP List:
            a18bbe20: (0006,01d8) Flags: 00060000  Mdl: 00000000
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      28020          Ticks: 15479 (0:00:04:01.473)
        Context Switch Count      202
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x775cb9d5)
        Stack Init a1a4b000 Current a1a4a8d0 Base a1a4b000 Limit a1a48000 Call 0
        Priority 11 BasePriority 10 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a1a4a8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1a4a924 81c28c64 nt!KiSwapThread+0x389
        a1a4a970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1a4abfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1a4ad48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1a4ad48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1a4ad64)
        012cfa90 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        012cfa94 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        012cfb30 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        012cfb4c 727d1865 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        012cfba4 727d828a wmisvc!WaitingFunction+0xd2 (FPO: [Non-Fpo])
        012cfbf8 727d80bc wmisvc!MyService::WorkerThread+0x178 (FPO: [Non-Fpo])
        012cfc38 727d7fe6 wmisvc!CNtService::Run+0xd7 (FPO: [Non-Fpo])
        012cfca0 00dd148a wmisvc!RunService+0x30 (FPO: [Non-Fpo])
        012cfccc 775cb9f6 svchost!ServiceStarter+0x17a (FPO: [Non-Fpo])
        012cfce0 75f33833 ADVAPI32!ScSvcctrlThreadA+0x21 (FPO: [Non-Fpo])
        012cfcec 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        012cfd2c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD a18f87a8  Cid 03cc.0528  Teb: 7ff97000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            a18c9460  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      1868           Ticks: 41631 (0:00:10:49.447)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address AUTHZ!AuthzpDeQueueThreadWorker (0x757b68c9)
        Stack Init a1a4f000 Current a1a4ec38 Base a1a4f000 Limit a1a4c000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1a4ec50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1a4ec8c 81c293a7 nt!KiSwapThread+0x389
        a1a4ece8 81df5057 nt!KeWaitForSingleObject+0x414
        a1a4ed50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a1a4ed50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1a4ed64)
        0186f930 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0186f934 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0186f9a4 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        0186f9b8 757b68ef kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0186f9d4 75f33833 AUTHZ!AuthzpDeQueueThreadWorker+0xa2 (FPO: [Non-Fpo])
        0186f9e0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0186fa20 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 8356e568  Cid 03cc.09cc  Teb: 7ff8f000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            8356bcc0  NotificationEvent
            835692b0  NotificationEvent
        IRP List:
            9fd85930: (0006,0094) Flags: 00060900  Mdl: 00000000
            9fd33708: (0006,0094) Flags: 00060800  Mdl: 00000000
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      18403          Ticks: 25096 (0:00:06:31.500)
        Context Switch Count      47
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ncprov!CNCProvider::ConnectThreadProc (0x71ad4031)
        Stack Init a1f0e000 Current a1f0d8d0 Base a1f0e000 Limit a1f0b000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1f0d8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1f0d924 81c28c64 nt!KiSwapThread+0x389
        a1f0d970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1f0dbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1f0dd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1f0dd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1f0dd64)
        01aefbb0 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01aefbb4 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        01aefc50 71ad1767 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        01aefcb0 71ad405d ncprov!CNCProvider::ConnectLoop+0x157 (FPO: [Non-Fpo])
        01aefcdc 75f33833 ncprov!CNCProvider::ConnectThreadProc+0x28 (FPO: [Non-Fpo])
        01aefce8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01aefd28 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 8356f030  Cid 03cc.09d4  Teb: 7ff8e000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fd20780  NotificationEvent
            835676c8  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      7700           Ticks: 35799 (0:00:09:18.467)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address NCObjAPI!CNamedPipeClient::ProviderReadyThreadProc (0x75b517a5)
        Stack Init a1a33000 Current a1a328d0 Base a1a33000 Limit a1a30000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1a328e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1a32924 81c28c64 nt!KiSwapThread+0x389
        a1a32970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1a32bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1a32d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1a32d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1a32d64)
        0301fbe4 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0301fbe8 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0301fc84 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0301fca0 75b51808 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0301fcf0 75f33833 NCObjAPI!CNamedPipeClient::ProviderReadyThreadProc+0x102 (FPO: [Non-Fpo])
        0301fcfc 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0301fd3c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 8356fd78  Cid 03cc.09d8  Teb: 7ff95000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            8356bc38  NotificationEvent
            8356bb38  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      7700           Ticks: 35799 (0:00:09:18.467)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address NCObjAPI!CNamedPipeClient::ProviderReadyThreadProc (0x75b517a5)
        Stack Init a1f16000 Current a1f158d0 Base a1f16000 Limit a1f13000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1f158e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1f15924 81c28c64 nt!KiSwapThread+0x389
        a1f15970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1f15bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1f15d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1f15d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1f15d64)
        02fdfa18 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        02fdfa1c 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        02fdfab8 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        02fdfad4 75b51808 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        02fdfb24 75f33833 NCObjAPI!CNamedPipeClient::ProviderReadyThreadProc+0x102 (FPO: [Non-Fpo])
        02fdfb30 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        02fdfb70 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 83608568  Cid 03cc.0b00  Teb: 7ffa5000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            835e7398  NotificationEvent
            835e7308  SynchronizationEvent
            835e72d8  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      9156           Ticks: 34343 (0:00:08:55.754)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address gpsvc!GPOThread (0x745fad8b)
        Stack Init a1ea6000 Current a1ea58d0 Base a1ea6000 Limit a1ea3000 Call 0
        Priority 1 BasePriority 1 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1ea58e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1ea5924 81c28c64 nt!KiSwapThread+0x389
        a1ea5970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1ea5bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1ea5d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1ea5d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1ea5d64)
        024df628 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        024df62c 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        024df6c8 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        024df6e4 745fafed kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        024df7fc 75f33833 gpsvc!GPOThread+0x2d1 (FPO: [Non-Fpo])
        024df808 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        024df848 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 836e0b48  Cid 03cc.0d74  Teb: 7ff96000 Win32Thread: ff532170 WAIT: (WrQueue)
UserMode Non-Alertable
            9fd28b68  QueueObject
            836e0bd0  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      43491          Ticks: 8 (0:00:00:00.124)
        Context Switch Count      616
        UserTime                  00:00:00.000
        KernelTime                00:00:00.046
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x775cb9d5)
        Stack Init a8fa0000 Current a8f9fbc8 Base a8fa0000 Limit a8f9d000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a8f9fbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8f9fc1c 81cad431 nt!KiSwapThread+0x389
        a8f9fc6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a8f9fcc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a8f9fd48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a8f9fd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8f9fd64)
        02cbf968 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        02cbf96c 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        02cbf998 70971468 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        02cbfa04 7097687f rasmans!RequestThread+0x63 (FPO: [Non-Fpo])
        02cbfa0c 7097685e rasmans!_RasmanEngine+0x7 (FPO: [Non-Fpo])
        02cbfa44 00dd148a rasmans!ServiceMain+0xae (FPO: [Non-Fpo])
        02cbfa70 775cb9f6 svchost!ServiceStarter+0x17a (FPO: [Non-Fpo])
        02cbfa84 75f33833 ADVAPI32!ScSvcctrlThreadA+0x21 (FPO: [Non-Fpo])
        02cbfa90 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        02cbfad0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fce7978  Cid 03cc.0d78  Teb: 7ff94000 Win32Thread: ff52fe98 WAIT: (WrUserRequest)
UserMode Non-Alertable
            836d98e0  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      9419           Ticks: 34080 (0:00:08:51.651)
        Context Switch Count      48
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address rastapi!EnumerateTapiPorts (0x70a72bcb)
        Stack Init a8fa4000 Current a8fa3b68 Base a8fa4000 Limit a8fa1000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a8fa3b80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8fa3bbc 81c293a7 nt!KiSwapThread+0x389
        a8fa3c18 8cedb8ed nt!KeWaitForSingleObject+0x414
        a8fa3c74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        a8fa3c90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        a8fa3ce8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        a8fa3d4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        a8fa3d4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8fa3d64)
        02d0fe38 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        02d0fe3c 761d3ad1 USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        02d0fe60 70a72d10 USER32!GetMessageA+0x8a (FPO: [Non-Fpo])
        02d0fec0 75f33833 rastapi!EnumerateTapiPorts+0x152 (FPO: [Non-Fpo])
        02d0fecc 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        02d0ff0c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fd4dbd8  Cid 03cc.0da8  Teb: 7ff92000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            835c4208  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      9419           Ticks: 34080 (0:00:08:51.651)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address TAPI32!AsyncEventsThread (0x73965fc6)
        Stack Init a8fa8000 Current a8fa7c38 Base a8fa8000 Limit a8fa5000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a8fa7c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8fa7c8c 81c293a7 nt!KiSwapThread+0x389
        a8fa7ce8 81df5057 nt!KeWaitForSingleObject+0x414
        a8fa7d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a8fa7d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8fa7d64)
        0202fda4 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0202fda8 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0202fe18 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        0202fe2c 73966097 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0202ff0c 75f33833 TAPI32!AsyncEventsThread+0x107 (FPO: [Non-Fpo])
        0202ff18 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0202ff58 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fc51af0  Cid 03cc.0dac  Teb: 7ff91000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            9fd184d0  SynchronizationEvent
            9fda32d0  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      9422           Ticks: 34077 (0:00:08:51.604)
        Context Switch Count      10
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RASQEC!RasQecHelper::WorkerThread (0x70a11bf1)
        Stack Init a0981000 Current a09808d0 Base a0981000 Limit a097e000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a09808e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0980924 81c28c64 nt!KiSwapThread+0x389
        a0980970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a0980bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a0980d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a0980d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0980d64)
        02f1f744 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        02f1f748 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        02f1f7e4 70a11d92 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        02f1f86c 75f33833 RASQEC!RasQecHelper::WorkerThread+0x4c3 (FPO: [Non-Fpo])
        02f1f878 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        02f1f8b8 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 836ed5e0  Cid 03cc.0db0  Teb: 7ff8d000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            9fd6a4b0  NotificationEvent
            9fd09a70  SynchronizationEvent
            9fc7bb00  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      9425           Ticks: 34074 (0:00:08:51.557)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address rasppp!WorkerThread (0x739a2801)
        Stack Init a8fac000 Current a8fab8d0 Base a8fac000 Limit a8fa9000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a8fab8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8fab924 81c28c64 nt!KiSwapThread+0x389
        a8fab970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a8fabbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a8fabd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a8fabd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8fabd64)
        0308fe84 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0308fe88 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0308ff24 739a2859 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0308ff60 75f33833 rasppp!WorkerThread+0x58 (FPO: [Non-Fpo])
        0308ff6c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0308ffac 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 8349c4d8  Cid 03cc.0ef8  Teb: 7ff8c000 Win32Thread: ff535bb8 WAIT: (UserRequest)
UserMode Alertable
            8350c020  SynchronizationTimer
            8368bd70  NotificationEvent
            834845c8  SynchronizationEvent
        IRP List:
            83714b00: (0006,01d8) Flags: 00060030  Mdl: 00000000
            8374c308: (0006,0100) Flags: 00060030  Mdl: 00000000
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      10400          Ticks: 33099 (0:00:08:36.347)
        Context Switch Count      520
        UserTime                  00:00:00.000
        KernelTime                00:00:00.062
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x775cb9d5)
        Stack Init a8fd0000 Current a8fcf8d0 Base a8fd0000 Limit a8fcd000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a8fcf8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8fcf924 81c28c64 nt!KiSwapThread+0x389
        a8fcf970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a8fcfbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a8fcfd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a8fcfd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8fcfd64)
        02f8f4fc 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        02f8f500 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        02f8f59c 761dc4b7 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        02f8f5f0 6e09192e USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
        02f8f640 6e097f15 qmgr!CJobManager::TaskThread+0x3c (FPO: [Non-Fpo])
        02f8f6bc 6e097ddd qmgr!InitQmgr+0x178 (FPO: [Non-Fpo])
        02f8f780 6e097ba4 qmgr!BITSServiceMainProc+0x495 (FPO: [Non-Fpo])
        02f8f7bc 6e097b6d qmgr!BITSServiceMain+0x2c (FPO: [Non-Fpo])
        02f8f7dc 00dd148a qmgr!ServiceMain+0x50 (FPO: [Non-Fpo])
        02f8f808 775cb9f6 svchost!ServiceStarter+0x17a (FPO: [Non-Fpo])
        02f8f81c 75f33833 ADVAPI32!ScSvcctrlThreadA+0x21 (FPO: [Non-Fpo])
        02f8f828 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        02f8f868 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 836b7b88  Cid 03cc.0efc  Teb: 7ff8b000 Win32Thread: ff535a48 WAIT: (WrUserRequest)
UserMode Non-Alertable
            835fac90  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      32891          Ticks: 10608 (0:00:02:45.485)
        Context Switch Count      85
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address ole32!CRpcThreadCache::RpcWorkerThreadEntry (0x7644fc53)
        Stack Init a6867000 Current a6866b68 Base a6867000 Limit a6864000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a6866b80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a6866bbc 81c293a7 nt!KiSwapThread+0x389
        a6866c18 8cedb8ed nt!KeWaitForSingleObject+0x414
        a6866c74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        a6866c90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        a6866ce8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        a6866d4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        a6866d4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a6866d64)
        0206fea0 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0206fea4 761e19cd USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        0206fec0 76458155 USER32!GetMessageW+0x33 (FPO: [Non-Fpo])
        0206ff00 7645258c ole32!CDllHost::STAWorkerLoop+0x81 (FPO: [Non-Fpo])
        0206ff1c 764524ce ole32!CDllHost::WorkerThread+0xce (FPO: [Non-Fpo])
        0206ff24 7644fc0d ole32!DLLHostThreadEntry+0xd (FPO: [Non-Fpo])
        0206ff40 7644fc73 ole32!CRpcThread::WorkerLoop+0x26 (FPO: [Non-Fpo])
        0206ff4c 75f33833 ole32!CRpcThreadCache::RpcWorkerThreadEntry+0x20 (FPO: [Non-Fpo])
        0206ff58 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0206ff98 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 835e4b58  Cid 03cc.0f0c  Teb: 7ff88000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            83713378  NotificationEvent
            835e4be0  NotificationTimer
        IRP List:
            83673008: (0006,01d8) Flags: 00060070  Mdl: 00000000
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      43449          Ticks: 50 (0:00:00:00.780)
        Context Switch Count      230
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address WINHTTP!ICAsyncThread::SelectThreadWrapper (0x73436286)
        Stack Init a8f08000 Current a8f07c38 Base a8f08000 Limit a8f05000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a8f07c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8f07c8c 81c293a7 nt!KiSwapThread+0x389
        a8f07ce8 81df5057 nt!KeWaitForSingleObject+0x414
        a8f07d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a8f07d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8f07d64)
        0325faa8 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0325faac 75253b28 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0325faec 75252690 mswsock!SockWaitForSingleObject+0x19f (FPO: [Non-Fpo])
        0325fbd8 75fe3781 mswsock!WSPSelect+0x38c (FPO: [Non-Fpo])
        0325fc54 73436217 WS2_32!select+0x456 (FPO: [Non-Fpo])
        0325fcdc 7343629e WINHTTP!ICAsyncThread::SelectThread+0x27d (FPO: [Non-Fpo])
        0325fcf0 75f33833 WINHTTP!ICAsyncThread::SelectThreadWrapper+0x18 (FPO: [Non-Fpo])
        0325fcfc 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0325fd3c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 835e48a0  Cid 03cc.0f10  Teb: 7ff87000 Win32Thread: ff5357c8 WAIT: (WrQueue)
UserMode Non-Alertable
            8357fc30  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      9759           Ticks: 33740 (0:00:08:46.347)
        Context Switch Count      37
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address WINHTTP!IOCompletionThreadFunc (0x7343642a)
        Stack Init a8f0c000 Current a8f0bbc8 Base a8f0c000 Limit a8f09000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a8f0bbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8f0bc1c 81cad431 nt!KiSwapThread+0x389
        a8f0bc6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a8f0bcc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a8f0bd48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a8f0bd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8f0bd64)
        0316fcc0 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0316fcc4 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        0316fcf0 73436467 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        0316fd70 75f33833 WINHTTP!IOCompletionThreadFunc+0x47 (FPO: [Non-Fpo])
        0316fd7c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0316fdbc 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 835e44d8  Cid 03cc.0f14  Teb: 7ff86000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            8357fc30  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      9755           Ticks: 33744 (0:00:08:46.409)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address WINHTTP!IOCompletionThreadFunc (0x7343642a)
        Stack Init a8f10000 Current a8f0fbc8 Base a8f10000 Limit a8f0d000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a8f0fbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8f0fc1c 81cad431 nt!KiSwapThread+0x389
        a8f0fc6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a8f0fcc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a8f0fd48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a8f0fd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8f0fd64)
        0358fd84 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0358fd88 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        0358fdb4 73436467 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        0358fe34 75f33833 WINHTTP!IOCompletionThreadFunc+0x47 (FPO: [Non-Fpo])
        0358fe40 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0358fe80 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 836cfac0  Cid 03cc.0f60  Teb: 7ff7f000 Win32Thread: ff536d88 WAIT: (UserRequest)
UserMode Alertable
            9fc6a9b8  SynchronizationEvent
            83738ff0  NotificationEvent
            847ad860  SynchronizationEvent
            836cfb48  NotificationTimer
        IRP List:
            83728de8: (0006,0100) Flags: 00060030  Mdl: 00000000
            83728ef8: (0006,0100) Flags: 00060030  Mdl: 00000000
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      13183          Ticks: 30316 (0:00:07:52.932)
        Context Switch Count      362
        UserTime                  00:00:00.078
        KernelTime                00:00:00.078
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x775cb9d5)
        Stack Init 9f7dc000 Current 9f7db8d0 Base 9f7dc000 Limit 9f7d9000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f7db8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f7db924 81c28c64 nt!KiSwapThread+0x389
        9f7db970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f7dbbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f7dbd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f7dbd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f7dbd64)
        02b7f8d8 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        02b7f8dc 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        02b7f978 6d9d707f kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        02b7f9c4 6daa257f wuaueng!DllInstall+0xac04
        02b7f9f8 6d9cba84 wuaueng!WUAutoUpdateAtShutdown+0x20418
        02b7fa9c 6d9cbb82 wuaueng!ServiceMain+0x303
        02b7fab4 00dd148a wuaueng!WUServiceMain+0x17
        02b7fae0 775cb9f6 svchost!ServiceStarter+0x17a (FPO: [Non-Fpo])
        02b7faf4 75f33833 ADVAPI32!ScSvcctrlThreadA+0x21 (FPO: [Non-Fpo])
        02b7fb00 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        02b7fb40 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 83727030  Cid 03cc.0478  Teb: 7ff8a000 Win32Thread: 00000000 WAIT: (WrLpcReply)
UserMode Non-Alertable
            83727244  Semaphore Limit 0x1
        Waiting for reply to ALPC Message a9be5ae0
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      10330          Ticks: 33169 (0:00:08:37.439)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address SSDPAPI!GetNotificationLoop (0x72a73289)
        Stack Init a8f68000 Current a8f67b48 Base a8f68000 Limit a8f65000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a8f67b60 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8f67b9c 81c293a7 nt!KiSwapThread+0x389
        a8f67bfc 81cc0275 nt!KeWaitForSingleObject+0x414
        a8f67c24 81dc3818 nt!AlpcpSignalAndWait+0x7e
        a8f67c48 81dc5c29 nt!AlpcpReceiveSynchronousReply+0x2b
        a8f67cd0 81dc61c5 nt!AlpcpProcessSynchronousRequest+0x201
        a8f67d3c 81c8caaa nt!NtAlpcSendWaitReceivePort+0xd0
        a8f67d3c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8f67d64)
        0421f67c 7748f2c0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0421f680 75d27f41 ntdll!NtAlpcSendWaitReceivePort+0xc (FPO: [8,0,0])
        0421f6ac 75da37a0 RPCRT4!LRPC_CASSOCIATION::AlpcSendWaitReceivePort+0x24
        0421fbac 72a7331b RPCRT4!NdrClientCall2+0x76e
        0421fbc8 72a732d4 SSDPAPI!GetNotificationRpc+0x1a (FPO: [Non-Fpo])
        0421fc0c 75f33833 SSDPAPI!GetNotificationLoop+0x59 (FPO: [Non-Fpo])
        0421fc18 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0421fc58 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 83919788  Cid 03cc.0d08  Teb: 7ff82000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            8373e9c0  NotificationEvent
            837e1520  NotificationEvent
            83919810  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      13183          Ticks: 30316 (0:00:07:52.932)
        Context Switch Count      110
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wuaueng!DllInstall (0x6d9e854b)
        Stack Init a8f94000 Current a8f938d0 Base a8f94000 Limit a8f91000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a8f938e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8f93924 81c28c64 nt!KiSwapThread+0x389
        a8f93970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a8f93bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a8f93d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a8f93d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8f93d64)
        0354fe20 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0354fe24 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0354fec0 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0354fedc 6d9e7f62 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0354ff14 6d9e8586 wuaueng!DllInstall+0x1bae7
        0354ff28 75f33833 wuaueng!DllInstall+0x1c10b
        0354ff34 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0354ff74 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 8345c570  Cid 03cc.0838  Teb: 7ffa9000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            8359da58  SynchronizationTimer
            82f0bd10  ProcessObject
            83831da8  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      18396          Ticks: 25103 (0:00:06:31.609)
        Context Switch Count      7
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x7744b49a)
        Stack Init a8ff0000 Current a8fef8d0 Base a8ff0000 Limit a8fed000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a8fef8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8fef924 81c28c64 nt!KiSwapThread+0x389
        a8fef970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a8fefbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a8fefd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a8fefd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8fefd64)
        0251fae0 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0251fae4 7744b65b ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0251fc80 75f33833 ntdll!TppWaiterpThread+0x294 (FPO: [Non-Fpo])
        0251fc8c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0251fccc 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 83685030  Cid 03cc.0bec  Teb: 7ffa6000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Alertable
            a18f7eb0  QueueObject
            836850b8  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      43375          Ticks: 124 (0:00:00:01.934)
        Context Switch Count      14
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init 9f687000 Current 9f686bc8 Base 9f687000 Limit 9f684000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f686be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f686c1c 81cad431 nt!KiSwapThread+0x389
        9f686c68 81d8b982 nt!KeRemoveQueueEx+0x568
        9f686cc0 81c7a036 nt!IoRemoveIoCompletion+0x23
        9f686d54 81c8caaa nt!NtWaitForWorkViaWorkerFactory+0x1a1
        9f686d54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f686d64)
        0236f708 77490850 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0236f70c 7749a1b4 ntdll!NtWaitForWorkViaWorkerFactory+0xc (FPO: [2,0,0])
        0236f834 75f33833 ntdll!TppWorkerThread+0x1f6 (FPO: [Non-Fpo])
        0236f840 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0236f880 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 836cdd78  Cid 03cc.0bf0  Teb: 7ffd3000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            9fc37088  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fc3dd90       Image:         svchost.exe
        Wait Start TickCount      43448          Ticks: 51 (0:00:00:00.795)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init a8fec000 Current a8febbc8 Base a8fec000 Limit a8fe9000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a8febbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8febc1c 81cad431 nt!KiSwapThread+0x389
        a8febc6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a8febcc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a8febd48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a8febd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8febd64)
        027bfb28 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        027bfb2c 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        027bfb58 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        027bfb94 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        027bfc00 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        027bfc0c 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        027bfc34 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        027bfc40 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        027bfc4c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        027bfc8c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Audiodg process

```
PROCESS 9fca1800  SessionId: 0  Cid: 0420    Peb: 7ffd8000  ParentCid: 03a4
    DirBase: 29a01200  ObjectTable: 89df4ea8  HandleCount: 110.
    Image: audiodg.exe
    VadRoot 9fc7a430 Vads 73 Clone 0 Private 2443. Modified 2184. Locked 0.
    DeviceMap a00699b8
    Token                             a00ddb10
    ElapsedTime                       00:11:02.921
    UserTime                          00:00:00.093
    KernelTime                        00:00:00.140
    QuotaPoolUsage[PagedPool]         60640
    QuotaPoolUsage[NonPagedPool]      3544
    Working Set Sizes (now,min,max)  (2295, 3371, 3887) (9180KB, 13484KB, 15548KB)
    PeakWorkingSetSize                3645
    VirtualSize                       38 Mb
    PeakVirtualSize                   41 Mb
    PageFaultCount                    7284
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      3113

    Setting context for this process...
.process /p /r ffffffff9fca1800

    !peb
PEB at 7ffd8000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00340000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00200e90 . 00219520
    Ldr.InLoadOrderModuleList:           00200e10 . 00219510
    Ldr.InMemoryOrderModuleList:         00200e18 . 00219518
            Base TimeStamp                     Module
          340000 4549b44e Nov 02 09:03:10 2006 C:\Windows\system32\AUDIODG.EXE
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\System32\kernel32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\System32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\System32\RPCRT4.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\System32\msvcrt.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\System32\ole32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\System32\GDI32.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\System32\USER32.dll
        74d90000 4549bd03 Nov 02 09:40:19 2006 C:\Windows\System32\MMDevAPI.DLL
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\System32\OLEAUT32.dll
        763b0000 4549bdb9 Nov 02 09:43:21 2006 C:\Windows\System32\SHLWAPI.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        75020000 4549bddb Nov 02 09:43:55 2006 C:\Windows\system32\NTMARTA.DLL
        76310000 4549be44 Nov 02 09:45:40 2006 C:\Windows\system32\WLDAP32.dll
        75fe0000 4549be0e Nov 02 09:44:46 2006 C:\Windows\system32\WS2_32.dll
        77550000 4549bdc7 Nov 02 09:43:35 2006 C:\Windows\system32\NSI.dll
        75ce0000 4549bd99 Nov 02 09:42:49 2006 C:\Windows\system32\PSAPI.DLL
        75ad0000 4549bda8 Nov 02 09:43:04 2006 C:\Windows\system32\SAMLIB.dll
        773a0000 4549bce9 Nov 02 09:39:53 2006 C:\Windows\system32\CLBCatQ.DLL
        75350000 4549bdae Nov 02 09:43:10 2006 C:\Windows\system32\rsaenh.dll
        736d0000 4549bcc2 Nov 02 09:39:14 2006 C:\Windows\System32\audioses.dll
        73540000 4549bcc0 Nov 02 09:39:12 2006 C:\Windows\System32\audioeng.dll
        75390000 4549bcdc Nov 02 09:39:40 2006 C:\Windows\System32\AVRT.dll
        734f0000 4549bcc1 Nov 02 09:39:13 2006 C:\Windows\System32\audiokse.dll
        77030000 4549bdb0 Nov 02 09:43:12 2006 C:\Windows\System32\SETUPAPI.dll
        75650000 45b96fde Jan 26 03:05:02 2007 C:\Windows\System32\CRYPT32.dll
```

```
        75820000 4549bd41 Nov 02 09:41:21 2006 C:\Windows\System32\MSASN1.dll
        75ba0000 4549bde2 Nov 02 09:44:02 2006 C:\Windows\System32\USERENV.dll
        75b80000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\System32\Secur32.dll
        74ff0000 4549be2f Nov 02 09:45:19 2006 C:\Windows\System32\WINTRUST.dll
        77580000 462434a3 Apr 17 03:44:51 2007 C:\Windows\System32\imagehlp.dll
        73870000 4549bd89 Nov 02 09:42:33 2006 C:\Windows\System32\ksuser.dll
        72fc0000 4549be4a Nov 02 09:45:46 2006 C:\Windows\system32\WMALFXGFXDSP.dll
        72f80000 4549bd0c Nov 02 09:40:28 2006 C:\Windows\system32\mfplat.dll
        74fe0000 46d779a1 Aug 31 03:14:57 2007 C:\Windows\system32\WTSAPI32.dll
        75300000 4549be2e Nov 02 09:45:18 2006 C:\Windows\system32\WINSTA.dll
    SubSystemData:     00000000
    ProcessHeap:       00200000
    ProcessParameters: 00200870
    WindowTitle:  'C:\Windows\system32\AUDIODG.EXE'
    ImageFile:    'C:\Windows\system32\AUDIODG.EXE'
    CommandLine:  'C:\Windows\system32\AUDIODG.EXE 0x2c8'
    DllPath:      'C:\Windows\System32'
    Environment:  002007e8
        Path=C:\Windows\System32
        SystemDrive=C:
        SystemRoot=C:\Windows


        THREAD 9fc7b030  Cid 0420.0424  Teb: 7ffdf000 Win32Thread: ff4dae98 WAIT: (UserRequest)
UserMode Non-Alertable
            9fca0080  NotificationEvent
            8485e910  ProcessObject
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fca1800       Image:         audiodg.exe
        Wait Start TickCount      1069           Ticks: 42430 (0:00:11:01.912)
        Context Switch Count      243
        UserTime                  00:00:00.031
        KernelTime                00:00:00.031
        Win32 Start Address AUDIODG!wWinMainCRTStartup (0x0034932f)
        Stack Init 9f254000 Current 9f2538d0 Base 9f254000 Limit 9f251000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f2538e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f253924 81c28c64 nt!KiSwapThread+0x389
        9f253970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f253bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f253d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f253d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f253d64)
        0017fcb4 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0017fcb8 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0017fd54 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0017fd70 00349662 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0017fd9c 00349616 AUDIODG!CAudioDGModule::RunMessageLoop+0x4e (FPO: [Non-Fpo])
        0017fdac 003495ea AUDIODG!ATL::CAtlExeModuleT<CAudioDGModule>::Run+0x1e (FPO: [Non-Fpo])
        0017fdbc 00349579 AUDIODG!ATL::CAtlExeModuleT<CAudioDGModule>::WinMain+0x26 (FPO: [Non-
Fpo])
        0017fdd8 003494ce AUDIODG!wWinMain+0xf1 (FPO: [Non-Fpo])
        0017fe6c 75f33833 AUDIODG!_initterm_e+0x1b1 (FPO: [Non-Fpo])
        0017fe78 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0017feb8 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fdb02d8  Cid 0420.06c4  Teb: 7ffd9000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            9fdaa188  SynchronizationTimer
            9fd6f520  SynchronizationTimer
            9fd22020  SynchronizationTimer
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fca1800       Image:         audiodg.exe
        Wait Start TickCount      24648          Ticks: 18851 (0:00:04:54.077)
        Context Switch Count      28
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x7744b49a)
        Stack Init a0834000 Current a08338d0 Base a0834000 Limit a0831000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a08338e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0833924 81c28c64 nt!KiSwapThread+0x389
        a0833970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a0833bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a0833d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a0833d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0833d64)
        013cfcc8 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        013cfccc 7744b65b ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        013cfe68 75f33833 ntdll!TppWaiterpThread+0x294 (FPO: [Non-Fpo])
        013cfe74 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        013cfeb4 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 83885ac0  Cid 0420.0c44  Teb: 7ffde000 Win32Thread: ff538938 WAIT: (WrQueue)
UserMode Non-Alertable
            9fca05d0  QueueObject
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fca1800       Image:         audiodg.exe
        Wait Start TickCount      36288          Ticks: 7211 (0:00:01:52.492)
        Context Switch Count      461
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init a6897000 Current a6896bc8 Base a6897000 Limit a6894000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a6896be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a6896c1c 81cad431 nt!KiSwapThread+0x389
        a6896c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a6896cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a6896d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a6896d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a6896d64)
        00d0fb68 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00d0fb6c 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        00d0fb98 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        00d0fbd4 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        00d0fc40 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        00d0fc4c 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        00d0fc74 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        00d0fc80 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        00d0fc8c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00d0fccc 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

SLsvc process

```
PROCESS 9fc70d90  SessionId: 0  Cid: 0440    Peb: 7ffd3000  ParentCid: 0214
    DirBase: 29a01220  ObjectTable: 9f8d2db0  HandleCount:  96.
    Image: SLsvc.exe
    VadRoot 9fca0328 Vads 59 Clone 0 Private 950. Modified 692. Locked 0.
    DeviceMap 9f999328
    Token                             a00df3c0
    ElapsedTime                       00:11:02.843
    UserTime                          00:00:00.780
    KernelTime                        00:00:00.717
    QuotaPoolUsage[PagedPool]         57000
    QuotaPoolUsage[NonPagedPool]      2912
    Working Set Sizes (now,min,max)  (810, 50, 345) (3240KB, 200KB, 1380KB)
    PeakWorkingSetSize                2334
    VirtualSize                       33 Mb
    PeakVirtualSize                   34 Mb
    PageFaultCount                    4775
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      1360

    Setting context for this process...
.process /p /r ffffffff9fc70d90

    !peb
PEB at 7ffd3000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00710000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 002a1788 . 002b9e70
    Ldr.InLoadOrderModuleList:           002a1708 . 002ba090
    Ldr.InMemoryOrderModuleList:         002a1710 . 002ba098
            Base TimeStamp                     Module
          710000 4679d9fe Jun 21 02:53:02 2007 C:\Windows\system32\SLsvc.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        75610000 4679de70 Jun 21 03:12:00 2007 C:\Windows\system32\slc.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        75af0000 4549bcf1 Nov 02 09:40:01 2006 C:\Windows\system32\DNSAPI.dll
        75fe0000 4549be0e Nov 02 09:44:46 2006 C:\Windows\system32\WS2_32.dll
        77550000 4549bdc7 Nov 02 09:43:35 2006 C:\Windows\system32\NSI.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        75350000 4549bdae Nov 02 09:43:10 2006 C:\Windows\system32\rsaenh.dll
        77030000 4549bdb0 Nov 02 09:43:12 2006 C:\Windows\system32\SETUPAPI.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        74ff0000 4549be2f Nov 02 09:45:19 2006 C:\Windows\system32\WINTRUST.dll
        75650000 45b96fde Jan 26 03:05:02 2007 C:\Windows\system32\CRYPT32.dll
        75820000 4549bd41 Nov 02 09:41:21 2006 C:\Windows\system32\MSASN1.dll
        75ba0000 4549bde2 Nov 02 09:44:02 2006 C:\Windows\system32\USERENV.dll
        75b80000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\Secur32.dll
        77580000 462434a3 Apr 17 03:44:51 2007 C:\Windows\system32\imagehlp.dll
    SubSystemData:     00000000
    ProcessHeap:       002a0000
    ProcessParameters: 002a1060
    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;C:\Program Files\QuickTime\QTSystem\'
    Environment:  002a07e8
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        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;C:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        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=WORKGROUP
        USERNAME=HOME$
        USERPROFILE=C:\Windows\ServiceProfiles\NetworkService
        windir=C:\Windows

        THREAD 9fc87580  Cid 0440.0444  Teb: 7ffdf000 Win32Thread: ff4c6e28 WAIT: (Executive)
UserMode Non-Alertable
            8995c774  NotificationEvent
        IRP List:
            9fc24ec0: (0006,0094) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            9fc70d90       Image:         SLsvc.exe
        Wait Start TickCount      1073           Ticks: 42426 (0:00:11:01.849)
        Context Switch Count      92
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address SLsvc (0x007be756)
        Stack Init 9f21c000 Current 9f21bbc8 Base 9f21c000 Limit 9f219000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f21bbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f21bc1c 81c293a7 nt!KiSwapThread+0x389
        9f21bc78 81d88faf nt!KeWaitForSingleObject+0x414
        9f21bcac 81d93669 nt!IopSynchronousServiceTail+0x258
        9f21bd38 81c8caaa nt!NtReadFile+0x646
        9f21bd38 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f21bd64)
        001af538 77490080 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        001af53c 75f3853f ntdll!ZwReadFile+0xc (FPO: [9,0,0])
        001af5b4 775cffe2 kernel32!ReadFile+0x20e (FPO: [Non-Fpo])
        001af5e0 775cfdfb ADVAPI32!ScGetPipeInput+0x2a (FPO: [Non-Fpo])
        001af648 775cbdd2 ADVAPI32!ScDispatcherLoop+0x6c (FPO: [Non-Fpo])
        001af8c0 0072edac ADVAPI32!StartServiceCtrlDispatcherW+0xce (FPO: [Non-Fpo])
        001af8f0 007b9afa SLsvc+0x1edac
        001af934 007be7cd SLsvc+0xa9afa
        001af94c 75f33833 SLsvc+0xae7cd
        001af958 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        001af998 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fc88ac0  Cid 0440.0454  Teb: 7ffdd000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            9fc87a38  SynchronizationTimer
            9fc89638  NotificationEvent
            9fc88188  SynchronizationTimer
            9fc8a020  SynchronizationTimer
            9fc70d90  ProcessObject
            9fd1a440  SynchronizationEvent
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            9fc70d90       Image:         SLsvc.exe
        Wait Start TickCount      1127           Ticks: 42372 (0:00:11:01.007)
        Context Switch Count      7
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x7744b49a)
        Stack Init a0340000 Current a033f8d0 Base a0340000 Limit a033d000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a033f8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a033f924 81c28c64 nt!KiSwapThread+0x389
        a033f970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a033fbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a033fd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a033fd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a033fd64)
        0050f93c 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0050f940 7744b65b ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0050fadc 75f33833 ntdll!TppWaiterpThread+0x294 (FPO: [Non-Fpo])
        0050fae8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0050fb28 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fc886e0  Cid 0440.0458  Teb: 7ffdc000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            9e1e85f0  QueueObject
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            9fc70d90       Image:         SLsvc.exe
        Wait Start TickCount      4921           Ticks: 38578 (0:00:10:01.820)
        Context Switch Count      6
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init a0344000 Current a0343bc8 Base a0344000 Limit a0341000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a0343be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0343c1c 81cad431 nt!KiSwapThread+0x389
        a0343c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a0343cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a0343d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a0343d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0343d64)
        013bfd78 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        013bfd7c 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        013bfda8 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        013bfde4 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        013bfe50 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        013bfe5c 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        013bfe84 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        013bfe90 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        013bfe9c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        013bfedc 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fc95030  Cid 0440.0470  Teb: 7ffde000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fc9b3b0  SynchronizationEvent
            9fc9b830  NotificationEvent
            9fc950b8  NotificationTimer
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            9fc70d90       Image:         SLsvc.exe
        Wait Start TickCount      1076           Ticks: 42423 (0:00:11:01.803)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address msvcrt!_endthreadex (0x7628639b)
        Stack Init 9f22c000 Current 9f22b8d0 Base 9f22c000 Limit 9f229000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 0 PagePriority 1
        Kernel stack not resident.
        ChildEBP RetAddr
        9f22b8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f22b924 81c28c64 nt!KiSwapThread+0x389
        9f22b970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f22bbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f22bd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f22bd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f22bd64)
        012cf5dc 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        012cf5e0 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        012cf67c 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        012cf698 008fcebb kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        012cf8e4 762862b6 SLsvc+0x1ecebb
        012cf91c 762863de msvcrt!_endthreadex+0x44 (FPO: [Non-Fpo])
        012cf924 75f33833 msvcrt!_endthreadex+0xce (FPO: [Non-Fpo])
        012cf930 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        012cf970 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Svchost process (LocalService)

```
PROCESS 9fc9c020  SessionId: 0  Cid: 0460    Peb: 7ffde000  ParentCid: 0214
    DirBase: 29a01240  ObjectTable: 89dd33c8  HandleCount: 563.
    Image: svchost.exe
    VadRoot 9fc8a130 Vads 200 Clone 0 Private 1309. Modified 308. Locked 133.
    DeviceMap a00699b8
    Token                             a00e95d0
    ElapsedTime                       00:11:02.765
    UserTime                          00:00:00.156
    KernelTime                        00:00:00.265
    QuotaPoolUsage[PagedPool]         128648
    QuotaPoolUsage[NonPagedPool]      24952
    Working Set Sizes (now,min,max)  (2707, 50, 345) (10828KB, 200KB, 1380KB)
    PeakWorkingSetSize                2933
    VirtualSize                       70 Mb
    PeakVirtualSize                   72 Mb
    PageFaultCount                    4075
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      2033

    Setting context for this process...
.process /p /r ffffffff9fc9c020

    !peb
PEB at 7ffde000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00dd0000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 002217b8 . 002fa188
    Ldr.InLoadOrderModuleList:           00221738 . 002fa178
    Ldr.InMemoryOrderModuleList:         00221740 . 002fa180
            Base TimeStamp                     Module
          dd0000 4549adc4 Nov 02 08:35:16 2006 C:\Windows\system32\svchost.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        75020000 4549bddb Nov 02 09:43:55 2006 C:\Windows\system32\NTMARTA.DLL
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        76310000 4549be44 Nov 02 09:45:40 2006 C:\Windows\system32\WLDAP32.dll
        75fe0000 4549be0e Nov 02 09:44:46 2006 C:\Windows\system32\WS2_32.dll
        77550000 4549bdc7 Nov 02 09:43:35 2006 C:\Windows\system32\NSI.dll
        75ce0000 4549bd99 Nov 02 09:42:49 2006 C:\Windows\system32\PSAPI.DLL
        75ad0000 4549bda8 Nov 02 09:43:04 2006 C:\Windows\system32\SAMLIB.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        745a0000 4549bcf8 Nov 02 09:40:08 2006 c:\windows\system32\es.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        744e0000 4549bd96 Nov 02 09:42:46 2006 c:\windows\system32\PROPSYS.dll
        75350000 4549bdae Nov 02 09:43:10 2006 C:\Windows\system32\rsaenh.dll
        773a0000 4549bce9 Nov 02 09:39:53 2006 C:\Windows\system32\CLBCatQ.DLL
        746b0000 4549bdc8 Nov 02 09:43:36 2006 c:\windows\system32\nsisvc.dll
        75250000 4549bd69 Nov 02 09:42:01 2006 C:\Windows\system32\mswsock.dll
        752c0000 4549be27 Nov 02 09:45:11 2006 C:\Windows\System32\wshtcpip.dll
        752b0000 4549be21 Nov 02 09:45:05 2006 C:\Windows\System32\wship6.dll
        75b80000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\secur32.dll
        75480000 4549bd20 Nov 02 09:40:48 2006 C:\Windows\system32\credssp.dll
```

```
        75650000 45b96fde Jan 26 03:05:02 2007 C:\Windows\system32\CRYPT32.dll
        75820000 4549bd41 Nov 02 09:41:21 2006 C:\Windows\system32\MSASN1.dll
        75ba0000 4549bde2 Nov 02 09:44:02 2006 C:\Windows\system32\USERENV.dll
        75050000 46773a78 Jun 19 03:07:52 2007 C:\Windows\system32\schannel.dll
        75840000 4549bd53 Nov 02 09:41:39 2006 C:\Windows\system32\NETAPI32.dll
        73360000 4549bded Nov 02 09:44:13 2006 c:\windows\system32\webclnt.dll
        73420000 4549be18 Nov 02 09:44:56 2006 c:\windows\system32\WINHTTP.dll
        763b0000 4549bdb9 Nov 02 09:43:21 2006 C:\Windows\system32\SHLWAPI.dll
        75dc0000 470c4de2 Oct 10 04:58:26 2007 C:\Windows\system32\urlmon.dll
        76360000 4549bcfb Nov 02 09:40:11 2006 C:\Windows\system32\iertutil.dll
        74aa0000 4549bd09 Nov 02 09:40:25 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_5d07289e07e1d100\comctl32.dll
        76560000 4681c95d Jun 27 03:20:13 2007 C:\Windows\system32\shell32.dll
        76020000 470c4e1e Oct 10 04:59:26 2007 C:\Windows\system32\WinInet.dll
        76010000 4549ad42 Nov 02 08:33:06 2006 C:\Windows\system32\Normaliz.dll
        73300000 4549be31 Nov 02 09:45:21 2006 c:\windows\system32\wkssvc.dll
        755b0000 4549bd3f Nov 02 09:41:19 2006 c:\windows\system32\IPHLPAPI.DLL
        75570000 46807ea6 Jun 26 03:49:10 2007 c:\windows\system32\dhcpcsvc.DLL
        75af0000 4549bcf1 Nov 02 09:40:01 2006 c:\windows\system32\DNSAPI.dll
        75560000 4549be1e Nov 02 09:45:02 2006 c:\windows\system32\WINNSI.DLL
        75540000 46807ea7 Jun 26 03:49:11 2007 c:\windows\system32\dhcpcsvc6.DLL
        75780000 4549bdcc Nov 02 09:43:40 2006 c:\windows\system32\NTDSAPI.dll
        750a0000 4549be0a Nov 02 09:44:42 2006 c:\windows\system32\WINBRAND.dll
        73330000 4549bcde Nov 02 09:39:42 2006 c:\windows\system32\fdrespub.dll
        72c50000 4549be15 Nov 02 09:44:53 2006 c:\windows\system32\wsdapi.dll
        72e40000 4549bcd7 Nov 02 09:39:35 2006 c:\windows\system32\HTTPAPI.dll
        74ff0000 4549be2f Nov 02 09:45:19 2006 c:\windows\system32\WINTRUST.dll
        77580000 462434a3 Apr 17 03:44:51 2007 C:\Windows\system32\imagehlp.dll
        73a70000 4549be05 Nov 02 09:44:37 2006 c:\windows\system32\XmlLite.dll
        74f30000 46677f3a Jun 07 04:44:58 2007 c:\windows\system32\FirewallAPI.dll
        753f0000 4549bde4 Nov 02 09:44:04 2006 c:\windows\system32\VERSION.dll
        72a20000 4549bcda Nov 02 09:39:38 2006 C:\Windows\system32\FunDisc.dll
        74d00000 4549bcbc Nov 02 09:39:08 2006 C:\Windows\system32\ATL.DLL
        77030000 4549bdb0 Nov 02 09:43:12 2006 C:\Windows\system32\SETUPAPI.dll
        729c0000 4549bdc8 Nov 02 09:43:36 2006 c:\windows\system32\ssdpsrv.dll
        72460000 4666193b Jun 06 03:17:31 2007 C:\Windows\System32\msxml3.dll
        75a60000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\SXS.DLL
        72410000 4549bdd7 Nov 02 09:43:51 2006 c:\windows\system32\upnphost.dll
        72a70000 4549bdc7 Nov 02 09:43:35 2006 c:\windows\system32\SSDPAPI.dll
        723c0000 4549bddb Nov 02 09:43:55 2006 c:\windows\system32\w32time.dll
        75b60000 4549bd26 Nov 02 09:40:54 2006 c:\windows\system32\cryptdll.dll
        75330000 4549bcd7 Nov 02 09:39:35 2006 C:\Windows\system32\GPAPI.dll
        75610000 4679de70 Jun 21 03:12:00 2007 C:\Windows\system32\slc.dll
        71ea0000 4549bd63 Nov 02 09:41:55 2006 c:\windows\system32\netprofm.dll
        74d30000 4549bd6b Nov 02 09:42:03 2006 c:\windows\system32\nlaapi.dll
        720c0000 4549bdc3 Nov 02 09:43:31 2006 C:\Windows\System32\npmproxy.dll
        6fa80000 4549bcdc Nov 02 09:39:40 2006 c:\windows\system32\fdphost.dll
        6f9a0000 4549bce2 Nov 02 09:39:46 2006 C:\Windows\system32\fdwsd.dll
        6f630000 4549bcf7 Nov 02 09:40:07 2006 C:\Windows\system32\MLANG.dll
        6f980000 4549bcdf Nov 02 09:39:43 2006 C:\Windows\system32\fdssdp.dll
        70b10000 4549bcdd Nov 02 09:39:41 2006 C:\Windows\system32\fdproxy.dll
        72f40000 4549be1f Nov 02 09:45:03 2006 C:\Windows\System32\winrnr.dll
        72f30000 4549bd3b Nov 02 09:41:15 2006 C:\Windows\system32\napinsp.dll
        72c10000 4549bdc0 Nov 02 09:43:28 2006 C:\Windows\system32\pnrpnsp.dll
        72c40000 4549be1d Nov 02 09:45:01 2006 C:\Windows\system32\wshbth.dll
        72a60000 4549bda2 Nov 02 09:42:58 2006 C:\Windows\system32\rasadhlp.dll
        6e8a0000 4549bdd6 Nov 02 09:43:50 2006 C:\Windows\system32\udhisapi.dll
    SubSystemData:     00000000
    ProcessHeap:       00220000
    ProcessParameters: 00221068
    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;C:\Program Files\QuickTime\QTSystem\'
    Environment:  002207e8
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\ServiceProfiles\LocalService\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
```

```
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        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;C:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        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 9fc9c890  Cid 0460.0464  Teb: 7ffdf000 Win32Thread: ff4ea210 WAIT: (Executive)
UserMode Non-Alertable
            9fc97fdc  NotificationEvent
        IRP List:
            9fc34e08: (0006,0094) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fc9c020       Image:         svchost.exe
        Wait Start TickCount      14206          Ticks: 29293 (0:00:07:36.973)
        Context Switch Count      96
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address svchost!wmainCRTStartup (0x00dd20bf)
        Stack Init a034c000 Current a034bbc8 Base a034c000 Limit a0349000 Call 0
        Priority 13 BasePriority 8 PriorityDecrement 4 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a034bbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a034bc1c 81c293a7 nt!KiSwapThread+0x389
        a034bc78 81d88faf nt!KeWaitForSingleObject+0x414
        a034bcac 81d93669 nt!IopSynchronousServiceTail+0x258
        a034bd38 81c8caaa nt!NtReadFile+0x646
        a034bd38 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a034bd64)
        000df9ac 77490080 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        000df9b0 75f3853f ntdll!ZwReadFile+0xc (FPO: [9,0,0])
        000dfa28 775cffe2 kernel32!ReadFile+0x20e (FPO: [Non-Fpo])
        000dfa54 775cfdfb ADVAPI32!ScGetPipeInput+0x2a (FPO: [Non-Fpo])
        000dfabc 775cbdd2 ADVAPI32!ScDispatcherLoop+0x6c (FPO: [Non-Fpo])
        000dfd34 00dd241d ADVAPI32!StartServiceCtrlDispatcherW+0xce (FPO: [Non-Fpo])
        000dfd3c 00dd2401 svchost!SvcHostMain+0x12 (FPO: [Non-Fpo])
        000dfd40 00dd2183 svchost!wmain+0x5 (FPO: [Non-Fpo])
        000dfd84 75f33833 svchost!_initterm_e+0x163 (FPO: [Non-Fpo])
        000dfd90 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        000dfdd0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fc9f2c8  Cid 0460.049c  Teb: 7ffd9000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            9fc9ff68  SynchronizationTimer
            8996a1c0  SynchronizationEvent
            9fcd78b0  SynchronizationEvent
            9fca6970  SynchronizationEvent
            9fca65d8  SynchronizationEvent
            9fd8cf10  SynchronizationEvent
            9fda1a50  NotificationEvent
            898651c0  SynchronizationEvent
            a1805aa0  SynchronizationTimer
            8987c3a0  SynchronizationEvent
            9fde4208  SynchronizationEvent
            9fdb42c0  SynchronizationEvent
            84b677a8  SynchronizationEvent
            9fdb3350  SynchronizationTimer
            9fda0960  NotificationEvent
            a18abc40  SynchronizationEvent
            a18b71e0  SynchronizationEvent
            a18aa7f0  NotificationEvent
            a18aa820  SynchronizationEvent
            a18a7720  SynchronizationEvent
            a18aba68  SynchronizationEvent
            a18acbb8  Thread
            a18abac8  SynchronizationEvent
            a18aba98  SynchronizationEvent
            a18aba38  SynchronizationEvent
            a18aba08  SynchronizationEvent
            a18dd428  SynchronizationEvent
            a18beff0  SynchronizationEvent
            a18d3c50  SynchronizationEvent
            9fd83620  SynchronizationEvent
            9e1f9798  SynchronizationEvent
            898740f8  SynchronizationEvent
            9fc282d0  SynchronizationEvent
            9fde0318  SynchronizationEvent
            9fd93d50  Semaphore Limit 0x7fffffff
            89857660  SynchronizationTimer
            9fdbb520  SynchronizationEvent
            a1c2f2f8  SynchronizationTimer
            a1c3d668  SynchronizationEvent
            a1811530  Semaphore Limit 0x7fffffff
            8987c278  SynchronizationTimer
            a18024c0  SynchronizationEvent
            83702178  NotificationEvent
            9fd35a40  SynchronizationEvent
            a18a7640  NotificationEvent
            837e6b20  SynchronizationEvent
            837dc8d8  SynchronizationEvent
            a18a7640  NotificationEvent
            a18a5808  SynchronizationEvent
            89870860  Semaphore Limit 0x5
            a18a6de8  SynchronizationEvent
            a18a76e0  NotificationEvent
            a1805958  SynchronizationEvent
            9fdb3d08  SynchronizationEvent
            83726c70  SynchronizationEvent
            8373f2e0  SynchronizationEvent
            8371d3c0  SynchronizationEvent
            a18f5680  SynchronizationEvent
            89856880  SynchronizationTimer
            a18f7c70  SynchronizationEvent
            a180cf40  SynchronizationTimer
            9fda2db8  SynchronizationEvent
            9fce7ee8  SynchronizationEvent
            83736a30  SynchronizationEvent
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fc9c020       Image:         svchost.exe
        Wait Start TickCount      35703          Ticks: 7796 (0:00:02:01.618)
```

```
        Context Switch Count      772
        UserTime                  00:00:00.015
        KernelTime                00:00:00.031
        Win32 Start Address ntdll!TppWaiterpThread (0x7744b49a)
        Stack Init 9f224000 Current 9f2238d0 Base 9f224000 Limit 9f221000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f2238e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f223924 81c28c64 nt!KiSwapThread+0x389
        9f223970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f223bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f223d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f223d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f223d64)
        00d4f694 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00d4f698 7744b65b ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00d4f834 75f33833 ntdll!TppWaiterpThread+0x294 (FPO: [Non-Fpo])
        00d4f840 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00d4f880 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 8995f960  Cid 0460.04a4  Teb: 7ffd8000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Alertable
            9fcd7860  QueueObject
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fc9c020       Image:         svchost.exe
        Wait Start TickCount      1883           Ticks: 41616 (0:00:10:49.213)
        Context Switch Count      22
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init 9f244000 Current 9f243bc8 Base 9f244000 Limit 9f241000 Call 0
        Priority 12 BasePriority 8 PriorityDecrement 3 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f243be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f243c1c 81cad431 nt!KiSwapThread+0x389
        9f243c68 81d8b982 nt!KeRemoveQueueEx+0x568
        9f243cc0 81c7a036 nt!IoRemoveIoCompletion+0x23
        9f243d54 81c8caaa nt!NtWaitForWorkViaWorkerFactory+0x1a1
        9f243d54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f243d64)
        010cfaa4 77490850 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        010cfaa8 7749a1b4 ntdll!NtWaitForWorkViaWorkerFactory+0xc (FPO: [2,0,0])
        010cfbd0 75f33833 ntdll!TppWorkerThread+0x1f6 (FPO: [Non-Fpo])
        010cfbdc 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        010cfc1c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fd97240  Cid 0460.0660  Teb: 7ffd5000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fda1560  NotificationEvent
            9fd972c8  NotificationTimer
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fc9c020       Image:         svchost.exe
        Wait Start TickCount      41598          Ticks: 1901 (0:00:00:29.655)
        Context Switch Count      33
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address webclnt!TfsScavengerThread (0x73361402)
        Stack Init 9f2c0000 Current 9f2bfc38 Base 9f2c0000 Limit 9f2bd000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f2bfc50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f2bfc8c 81c293a7 nt!KiSwapThread+0x389
        9f2bfce8 81df5057 nt!KeWaitForSingleObject+0x414
        9f2bfd50 81c8caaa nt!NtWaitForSingleObject+0xbe
        9f2bfd50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f2bfd64)
        0103fbcc 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0103fbd0 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0103fc40 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        0103fc54 73361484 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0103fc6c 75f33833 webclnt!TfsScavengerThread+0x138 (FPO: [Non-Fpo])
        0103fc78 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0103fcb8 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fd92030  Cid 0460.0664  Teb: 7ffd4000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            9fd9c558  QueueObject
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fc9c020       Image:         svchost.exe
        Wait Start TickCount      1211           Ticks: 42288 (0:00:10:59.697)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address webclnt!DavWorkerThread (0x73361ca6)
        Stack Init a087f000 Current a087ea58 Base a087f000 Limit a087c000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a087ea70 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a087eaac 81cad431 nt!KiSwapThread+0x389
        a087eaf8 81cc26f6 nt!KeRemoveQueueEx+0x568
        a087eb18 a0caaec2 nt!KeRemoveQueue+0x1b
        a087eb3c a0ca97f0 mrxdav!UMRxAssignWork+0x2d5 (FPO: [Non-Fpo])
        a087eba0 81a17912 mrxdav!MRxDAVFastIoDeviceControl+0x1eb (FPO: [Non-Fpo])
        a087ebd0 80763917 mup!MupFastIoDeviceControl+0x3f (FPO: [Non-Fpo])
        a087ec08 8077589e fltmgr!FltpPerformFastIoCall+0x151 (FPO: [Non-Fpo])
        a087ec58 81d89aff fltmgr!FltpFastIoDeviceControl+0x96 (FPO: [Non-Fpo])
        a087ed00 81d8ee55 nt!IopXxxControlFile+0x2cf
        a087ed34 81c8caaa nt!NtDeviceIoControlFile+0x2a
        a087ed34 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a087ed64)
        008ef6f0 7748f850 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        008ef6f4 75f37c92 ntdll!ZwDeviceIoControlFile+0xc (FPO: [10,0,0])
        008ef754 73361e34 kernel32!DeviceIoControl+0x14a (FPO: [Non-Fpo])
        008ef788 73361d55 webclnt!UMReflectorGetRequest+0x94 (FPO: [Non-Fpo])
        008ef7c8 75f33833 webclnt!DavWorkerThread+0x112 (FPO: [Non-Fpo])
        008ef7d4 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        008ef814 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fd92b18  Cid 0460.0668  Teb: 7ffd3000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            9fd9c558  QueueObject
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fc9c020       Image:         svchost.exe
        Wait Start TickCount      1210           Ticks: 42289 (0:00:10:59.712)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address webclnt!DavWorkerThread (0x73361ca6)
        Stack Init a0844000 Current a0843a58 Base a0844000 Limit a0841000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a0843a70 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0843aac 81cad431 nt!KiSwapThread+0x389
        a0843af8 81cc26f6 nt!KeRemoveQueueEx+0x568
        a0843b18 a0caaec2 nt!KeRemoveQueue+0x1b
        a0843b3c a0ca97f0 mrxdav!UMRxAssignWork+0x2d5 (FPO: [Non-Fpo])
        a0843ba0 81a17912 mrxdav!MRxDAVFastIoDeviceControl+0x1eb (FPO: [Non-Fpo])
        a0843bd0 80763917 mup!MupFastIoDeviceControl+0x3f (FPO: [Non-Fpo])
        a0843c08 8077589e fltmgr!FltpPerformFastIoCall+0x151 (FPO: [Non-Fpo])
        a0843c58 81d89aff fltmgr!FltpFastIoDeviceControl+0x96 (FPO: [Non-Fpo])
        a0843d00 81d8ee55 nt!IopXxxControlFile+0x2cf
        a0843d34 81c8caaa nt!NtDeviceIoControlFile+0x2a
        a0843d34 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0843d64)
        013af80c 7748f850 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        013af810 75f37c92 ntdll!ZwDeviceIoControlFile+0xc (FPO: [10,0,0])
        013af870 73361e34 kernel32!DeviceIoControl+0x14a (FPO: [Non-Fpo])
        013af8a4 73361d55 webclnt!UMReflectorGetRequest+0x94 (FPO: [Non-Fpo])
        013af8e4 75f33833 webclnt!DavWorkerThread+0x112 (FPO: [Non-Fpo])
        013af8f0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        013af930 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD a1806ac0  Cid 0460.07fc  Teb: 7ffae000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            a180aff0  NotificationEvent
            9fd90d98  NotificationEvent
        IRP List:
            89872cd8: (0006,01d8) Flags: 00060030  Mdl: 89879ac8
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fc9c020       Image:         svchost.exe
        Wait Start TickCount      1816           Ticks: 41683 (0:00:10:50.258)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init a1b6c000 Current a1b6b8d0 Base a1b6c000 Limit a1b69000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1b6b8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1b6b924 81c28c64 nt!KiSwapThread+0x389
        a1b6b970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1b6bbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1b6bd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1b6bd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1b6bd64)
        0141f348 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0141f34c 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0141f3e8 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0141f404 72c6f1ae kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0141f77c 7746fe6d wsdapi!CWSDHttpListener::Listener+0x16b (FPO: [Non-Fpo])
        0141f7e0 7749a2b8 ntdll!RtlpTpWorkCallback+0xbf (FPO: [Non-Fpo])
        0141f908 75f33833 ntdll!TppWorkerThread+0x522 (FPO: [Non-Fpo])
        0141f914 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0141f954 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 8985aa38  Cid 0460.0104  Teb: 7ffac000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            a1806930  SynchronizationEvent
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fc9c020       Image:         svchost.exe
        Wait Start TickCount      1817           Ticks: 41682 (0:00:10:50.243)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address FunDisc!CNotificationQueue::ThreadProc (0x72a2154d)
        Stack Init a1a9f000 Current a1a9ec38 Base a1a9f000 Limit a1a9c000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1a9ec50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1a9ec8c 81c293a7 nt!KiSwapThread+0x389
        a1a9ece8 81df5057 nt!KeWaitForSingleObject+0x414
        a1a9ed50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a1a9ed50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1a9ed64)
        0134fe18 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0134fe1c 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0134fe8c 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        0134fea0 72a215ed kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0134fec4 75f33833 FunDisc!CNotificationQueue::ThreadProc+0x24f (FPO: [Non-Fpo])
        0134fed0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0134ff10 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD a180b820  Cid 0460.010c  Teb: 7ffab000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            a180bac8  SynchronizationEvent
            898741b0  SynchronizationEvent
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fc9c020       Image:         svchost.exe
        Wait Start TickCount      1820           Ticks: 41679 (0:00:10:50.196)
        Context Switch Count      21
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address FunDisc!CRegProvider::ThreadProc (0x72a22cdd)
        Stack Init a1a53000 Current a1a528d0 Base a1a53000 Limit a1a50000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1a528e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1a52924 81c28c64 nt!KiSwapThread+0x389
        a1a52970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1a52bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1a52d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1a52d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1a52d64)
        0171f774 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0171f778 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0171f814 72a22dce kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0171fc80 72a22cea FunDisc!CRegProvider::MemberThreadProc+0x136 (FPO: [Non-Fpo])
        0171fc88 75f33833 FunDisc!CRegProvider::ThreadProc+0xd (FPO: [Non-Fpo])
        0171fc94 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0171fcd4 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD a18b6030  Cid 0460.0130  Teb: 7ffaa000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fd90918  SynchronizationEvent
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fc9c020       Image:         svchost.exe
        Wait Start TickCount      22303          Ticks: 21196 (0:00:05:30.659)
        Context Switch Count      109
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address ssdpsrv!CSsdpSearchRequestManager::DwSearchThreadProc (0x729c9a48)
        Stack Init a1b60000 Current a1b5fc38 Base a1b60000 Limit a1b5d000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1b5fc50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1b5fc8c 81c293a7 nt!KiSwapThread+0x389
        a1b5fce8 81df5057 nt!KeWaitForSingleObject+0x414
        a1b5fd50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a1b5fd50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1b5fd64)
        0190f614 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0190f618 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0190f688 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        0190f69c 729c4662 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0190f8ac 729c9a52 ssdpsrv!CSsdpSearchRequestManager::DwThreadFunc+0xfc (FPO: [Non-Fpo])
        0190f8b0 75f33833 ssdpsrv!CSsdpSearchRequestManager::DwSearchThreadProc+0xa (FPO: [Non-
Fpo])
        0190f8bc 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0190f8fc 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fdb3a60  Cid 0460.0174  Teb: 7ffa9000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fdb2ff0  SynchronizationEvent
            a18b62d8  NotificationEvent
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fc9c020       Image:         svchost.exe
        Wait Start TickCount      35703          Ticks: 7796 (0:00:02:01.618)
        Context Switch Count      126
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ssdpsrv!CReceiveDataManager::ThreadFunc (0x729c996c)
        Stack Init a1a2b000 Current a1a2a8d0 Base a1a2b000 Limit a1a28000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a1a2a8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1a2a924 81c28c64 nt!KiSwapThread+0x389
        a1a2a970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1a2abfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1a2ad48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1a2ad48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1a2ad64)
        019bfa50 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        019bfa54 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        019bfaf0 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        019bfb0c 729c2b4f kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        019bfb3c 729c9976 ssdpsrv!CReceiveDataManager::ThreadMember+0x7b (FPO: [Non-Fpo])
        019bfb40 75f33833 ssdpsrv!CReceiveDataManager::ThreadFunc+0xa (FPO: [Non-Fpo])
        019bfb4c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        019bfb8c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD a180cc98  Cid 0460.016c  Teb: 7ffaf000 Win32Thread: ff52f998 WAIT: (WrQueue)
UserMode Alertable
            9fc22748  QueueObject
        IRP List:
            9fc4faa8: (0006,0100) Flags: 00060030  Mdl: 00000000
            a18aa948: (0006,01d8) Flags: 00060030  Mdl: 00000000
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fc9c020       Image:         svchost.exe
        Wait Start TickCount      14452          Ticks: 29047 (0:00:07:33.136)
        Context Switch Count      546
        UserTime                  00:00:00.046
        KernelTime                00:00:00.062
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init a1a83000 Current a1a82bc8 Base a1a83000 Limit a1a80000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1a82be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1a82c1c 81cad431 nt!KiSwapThread+0x389
        a1a82c68 81d8b982 nt!KeRemoveQueueEx+0x568
        a1a82cc0 81c7a036 nt!IoRemoveIoCompletion+0x23
        a1a82d54 81c8caaa nt!NtWaitForWorkViaWorkerFactory+0x1a1
        a1a82d54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1a82d64)
        0169f800 77490850 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0169f804 7749a1b4 ntdll!NtWaitForWorkViaWorkerFactory+0xc (FPO: [2,0,0])
        0169f92c 75f33833 ntdll!TppWorkerThread+0x1f6 (FPO: [Non-Fpo])
        0169f938 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0169f978 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD a18acbb8  Cid 0460.02f4  Teb: 7ffa7000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            a18b7f90  NotificationEvent
            a18bda30  SynchronizationEvent
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fc9c020       Image:         svchost.exe
        Wait Start TickCount      1856           Ticks: 41643 (0:00:10:49.634)
        Context Switch Count      14
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address w32time!ClockDisciplineThread (0x723ce7db)
        Stack Init a1a3f000 Current a1a3e8d0 Base a1a3f000 Limit a1a3c000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1a3e8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1a3e924 81c28c64 nt!KiSwapThread+0x389
        a1a3e970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1a3ebfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1a3ed48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1a3ed48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1a3ed64)
        01c2fae0 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01c2fae4 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        01c2fb80 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        01c2fb9c 723c1a17 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        01c2fde4 75f33833 w32time!ClockDisciplineThread+0x2b5 (FPO: [Non-Fpo])
        01c2fdf0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01c2fe30 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD a18c2030  Cid 0460.0414  Teb: 7ffa8000 Win32Thread: ff5121b8 WAIT: (WrUserRequest)
UserMode Non-Alertable
            a18f7558  SynchronizationEvent
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fc9c020       Image:         svchost.exe
        Wait Start TickCount      9413           Ticks: 34086 (0:00:08:51.745)
        Context Switch Count      9
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address netprofm!CImplINetworkListManager::EventMgrThreadProc (0x71ea5d06)
        Stack Init a1af1000 Current a1af0b68 Base a1af1000 Limit a1aee000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1af0b80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1af0bbc 81c293a7 nt!KiSwapThread+0x389
        a1af0c18 8cedb8ed nt!KeWaitForSingleObject+0x414
        a1af0c74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        a1af0c90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        a1af0ce8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        a1af0d4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        a1af0d4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1af0d64)
        01a6fd18 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01a6fd1c 761e19cd USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        01a6fd38 71ea5d81 USER32!GetMessageW+0x33 (FPO: [Non-Fpo])
        01a6fda0 75f33833 netprofm!CImplINetworkListManager::EventMgrThreadProc+0x1f7 (FPO: [Non-
Fpo])
        01a6fdac 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01a6fdec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD a18d3d78  Cid 0460.04b0  Teb: 7ffa6000 Win32Thread: ff41bd88 WAIT: (UserRequest)
UserMode Non-Alertable
            a180dff0  NotificationEvent
            9fdb3748  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fc9c020       Image:         svchost.exe
        Wait Start TickCount      1900           Ticks: 41599 (0:00:10:48.948)
        Context Switch Count      151
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init a1eee000 Current a1eed8d0 Base a1eee000 Limit a1eeb000 Call 0
        Priority 12 BasePriority 8 PriorityDecrement 4 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1eed8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1eed924 81c28c64 nt!KiSwapThread+0x389
        a1eed970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1eedbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1eedd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1eedd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1eedd64)
        01cbf564 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01cbf568 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        01cbf604 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        01cbf620 729c5951 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        01cbf64c 75d26d7e ssdpsrv!_GetNotificationRpc+0x62 (FPO: [Non-Fpo])
        01cbf668 75da03a2 RPCRT4!Invoke+0x2a
        01cbfa94 75d9f44c RPCRT4!NdrStubCall2+0x27b
        01cbfab0 75d273cb RPCRT4!NdrServerCall2+0x1e
        01cbfaec 75d27279 RPCRT4!DispatchToStubInCNoAvrf+0x41
        01cbfb60 75d2770a RPCRT4!RPC_INTERFACE::DispatchToStubWorker+0xdf
        01cbfba0 75d275d5 RPCRT4!LRPC_SCALL::DispatchRequest+0xa2
        01cbfc0c 75d2618a RPCRT4!LRPC_SCALL::HandleRequest+0x1d2
        01cbfcb4 75d3b062 RPCRT4!LRPC_ADDRESS::ProcessIO+0x216
        01cbfd08 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x162
        01cbfd14 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        01cbfd38 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        01cbfd44 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        01cbfd50 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01cbfd90 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fdf33f0  Cid 0460.06fc  Teb: 7ffa3000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Alertable
            89856fd0  QueueObject
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fc9c020       Image:         svchost.exe
        Wait Start TickCount      9807           Ticks: 33692 (0:00:08:45.598)
        Context Switch Count      27
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init a1ebe000 Current a1ebdbc8 Base a1ebe000 Limit a1ebb000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1ebdbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1ebdc1c 81cad431 nt!KiSwapThread+0x389
        a1ebdc68 81d8b982 nt!KeRemoveQueueEx+0x568
        a1ebdcc0 81c7a036 nt!IoRemoveIoCompletion+0x23
        a1ebdd54 81c8caaa nt!NtWaitForWorkViaWorkerFactory+0x1a1
        a1ebdd54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1ebdd64)
        0176fe00 77490850 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0176fe04 7749a1b4 ntdll!NtWaitForWorkViaWorkerFactory+0xc (FPO: [2,0,0])
        0176ff2c 75f33833 ntdll!TppWorkerThread+0x1f6 (FPO: [Non-Fpo])
        0176ff38 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0176ff78 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD a1938030  Cid 0460.0700  Teb: 7ffa2000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            9fd7e680  SynchronizationTimer
            83a0b840  SynchronizationEvent
            a19ad178  SynchronizationTimer
            a18c0c08  SynchronizationEvent
            9fdb09d8  SynchronizationEvent
            89857b40  SynchronizationEvent
            83930358  SynchronizationEvent
            a19380b8  NotificationTimer
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fc9c020       Image:         svchost.exe
        Wait Start TickCount      43052          Ticks: 447 (0:00:00:06.973)
        Context Switch Count      65
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x7744b49a)
        Stack Init a1ec6000 Current a1ec58d0 Base a1ec6000 Limit a1ec3000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a1ec58e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1ec5924 81c28c64 nt!KiSwapThread+0x389
        a1ec5970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1ec5bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1ec5d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1ec5d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1ec5d64)
        01c7f928 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01c7f92c 7744b65b ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        01c7fac8 75f33833 ntdll!TppWaiterpThread+0x294 (FPO: [Non-Fpo])
        01c7fad4 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01c7fb14 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD a1c2f650  Cid 0460.0720  Teb: 7ffa1000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Alertable
            89856fd0  QueueObject
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fc9c020       Image:         svchost.exe
        Wait Start TickCount      9821           Ticks: 33678 (0:00:08:45.380)
        Context Switch Count      13
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init a1e66000 Current a1e65bc8 Base a1e66000 Limit a1e63000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1e65be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1e65c1c 81cad431 nt!KiSwapThread+0x389
        a1e65c68 81d8b982 nt!KeRemoveQueueEx+0x568
        a1e65cc0 81c7a036 nt!IoRemoveIoCompletion+0x23
        a1e65d54 81c8caaa nt!NtWaitForWorkViaWorkerFactory+0x1a1
        a1e65d54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1e65d64)
        022afd58 77490850 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        022afd5c 7749a1b4 ntdll!NtWaitForWorkViaWorkerFactory+0xc (FPO: [2,0,0])
        022afe84 75f33833 ntdll!TppWorkerThread+0x1f6 (FPO: [Non-Fpo])
        022afe90 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        022afed0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 835aa890  Cid 0460.0a1c  Teb: 7ffdc000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            a180dff0  NotificationEvent
            8368fd10  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fc9c020       Image:         svchost.exe
        Wait Start TickCount      9654           Ticks: 33845 (0:00:08:47.985)
        Context Switch Count      10
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init a0929000 Current a09288d0 Base a0929000 Limit a0926000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a09288e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0928924 81c28c64 nt!KiSwapThread+0x389
        a0928970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a0928bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a0928d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a0928d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0928d64)
        01a2efc4 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01a2efc8 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        01a2f064 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        01a2f080 729c5951 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        01a2f0ac 75d26d7e ssdpsrv!_GetNotificationRpc+0x62 (FPO: [Non-Fpo])
        01a2f0c8 75da03a2 RPCRT4!Invoke+0x2a
        01a2f4f4 75d9f44c RPCRT4!NdrStubCall2+0x27b
        01a2f510 75d273cb RPCRT4!NdrServerCall2+0x1e
        01a2f54c 75d27279 RPCRT4!DispatchToStubInCNoAvrf+0x41
        01a2f5c0 75d2770a RPCRT4!RPC_INTERFACE::DispatchToStubWorker+0xdf
        01a2f600 75d275d5 RPCRT4!LRPC_SCALL::DispatchRequest+0xa2
        01a2f66c 75d2618a RPCRT4!LRPC_SCALL::HandleRequest+0x1d2
        01a2f714 75d3b062 RPCRT4!LRPC_ADDRESS::ProcessIO+0x216
        01a2f768 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x162
        01a2f774 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        01a2f798 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        01a2f7a4 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        01a2f7b0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01a2f7f0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 835e8738  Cid 0460.0b44  Teb: 7ffd6000 Win32Thread: ff535008 WAIT: (UserRequest)
UserMode Non-Alertable
            a180dff0  NotificationEvent
            899786d8  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fc9c020       Image:         svchost.exe
        Wait Start TickCount      10330          Ticks: 33169 (0:00:08:37.439)
        Context Switch Count      108
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init a1ba4000 Current a1ba38d0 Base a1ba4000 Limit a1ba1000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1ba38e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1ba3924 81c28c64 nt!KiSwapThread+0x389
        a1ba3970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1ba3bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1ba3d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1ba3d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1ba3d64)
        0237f334 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0237f338 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0237f3d4 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0237f3f0 729c5951 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0237f41c 75d26d7e ssdpsrv!_GetNotificationRpc+0x62 (FPO: [Non-Fpo])
        0237f438 75da03a2 RPCRT4!Invoke+0x2a
        0237f864 75d9f44c RPCRT4!NdrStubCall2+0x27b
        0237f880 75d273cb RPCRT4!NdrServerCall2+0x1e
        0237f8bc 75d27279 RPCRT4!DispatchToStubInCNoAvrf+0x41
        0237f930 75d2770a RPCRT4!RPC_INTERFACE::DispatchToStubWorker+0xdf
        0237f970 75d275d5 RPCRT4!LRPC_SCALL::DispatchRequest+0xa2
        0237f9dc 75d2618a RPCRT4!LRPC_SCALL::HandleRequest+0x1d2
        0237fa84 75d3b062 RPCRT4!LRPC_ADDRESS::ProcessIO+0x216
        0237fad8 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x162
        0237fae4 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        0237fb08 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        0237fb14 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        0237fb20 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0237fb60 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 835dc790  Cid 0460.0d88  Teb: 7ffa5000 Win32Thread: ff530e98 WAIT: (WrUserRequest)
UserMode Non-Alertable
            9fc52ae8  SynchronizationEvent
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fc9c020       Image:         svchost.exe
        Wait Start TickCount      9413           Ticks: 34086 (0:00:08:51.745)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address netprofm!CImplINetworkListManager::EventWorkerThreadProc (0x71ea60b0)
        Stack Init a1ef6000 Current a1ef5b68 Base a1ef6000 Limit a1ef3000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1ef5b80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1ef5bbc 81c293a7 nt!KiSwapThread+0x389
        a1ef5c18 8cedb8ed nt!KeWaitForSingleObject+0x414
        a1ef5c74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        a1ef5c90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        a1ef5ce8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        a1ef5d4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        a1ef5d4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1ef5d64)
        0130fcdc 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0130fce0 761e19cd USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        0130fcfc 71ea611a USER32!GetMessageW+0x33 (FPO: [Non-Fpo])
        0130fd58 75f33833 netprofm!CImplINetworkListManager::EventWorkerThreadProc+0x77 (FPO: [Non-
Fpo])
        0130fd64 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0130fda4 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 8374abb0  Cid 0460.0e94  Teb: 7ffa4000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            837020a8  SynchronizationEvent
            836a9510  NotificationEvent
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fc9c020       Image:         svchost.exe
        Wait Start TickCount      9654           Ticks: 33845 (0:00:08:47.985)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address fdssdp!CSsdpWorker::WorkerStart (0x6f98890f)
        Stack Init 9f3c4000 Current 9f3c38d0 Base 9f3c4000 Limit 9f3c1000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f3c38e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f3c3924 81c28c64 nt!KiSwapThread+0x389
        9f3c3970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f3c3bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f3c3d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f3c3d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f3c3d64)
        01d0f638 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01d0f63c 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        01d0f6d8 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        01d0f6f4 6f9884ea kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        01d0f8c0 6f9885be fdssdp!CSsdpWorker::WorkerMain+0x195 (FPO: [Non-Fpo])
        01d0f8d4 7642e04e fdssdp!WorkerMainWithComContext+0x40 (FPO: [Non-Fpo])
        01d0f948 7641e300 ole32!EnterForCallback+0xcf (FPO: [Non-Fpo])
        01d0faa8 7641e3be ole32!SwitchForCallback+0x1a8 (FPO: [Non-Fpo])
        01d0fafc 76451336 ole32!PerformCallback+0xa3 (FPO: [Non-Fpo])
        01d0fb94 76420a58 ole32!CObjectContext::InternalContextCallback+0x15b (FPO: [Non-Fpo])
        01d0fbe4 7641d7ab ole32!CObjectContext::ContextCallback+0x87 (FPO: [Non-Fpo])
        01d0fc08 6f9889ae ole32!CContextSwitcher::ContextCallback+0x45 (FPO: [Non-Fpo])
        01d0fc40 75f33833 fdssdp!CSsdpWorker::WorkerStart+0x9f (FPO: [Non-Fpo])
        01d0fc4c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01d0fc8c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 8367dd78  Cid 0460.0e98  Teb: 7ffa0000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            837020a8  SynchronizationEvent
            836a9510  NotificationEvent
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fc9c020       Image:         svchost.exe
        Wait Start TickCount      10233          Ticks: 33266 (0:00:08:38.952)
        Context Switch Count      10
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address fdssdp!CSsdpWorker::WorkerStart (0x6f98890f)
        Stack Init 9f39c000 Current 9f39b8d0 Base 9f39c000 Limit 9f399000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f39b8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f39b924 81c28c64 nt!KiSwapThread+0x389
        9f39b970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f39bbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f39bd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f39bd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f39bd64)
        0110f300 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0110f304 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0110f3a0 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0110f3bc 6f9884ea kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0110f588 6f9885be fdssdp!CSsdpWorker::WorkerMain+0x195 (FPO: [Non-Fpo])
        0110f59c 7642e04e fdssdp!WorkerMainWithComContext+0x40 (FPO: [Non-Fpo])
        0110f610 7641e300 ole32!EnterForCallback+0xcf (FPO: [Non-Fpo])
        0110f770 7641e3be ole32!SwitchForCallback+0x1a8 (FPO: [Non-Fpo])
        0110f7c4 76451336 ole32!PerformCallback+0xa3 (FPO: [Non-Fpo])
        0110f85c 76420a58 ole32!CObjectContext::InternalContextCallback+0x15b (FPO: [Non-Fpo])
        0110f8ac 7641d7ab ole32!CObjectContext::ContextCallback+0x87 (FPO: [Non-Fpo])
        0110f8d0 6f9889ae ole32!CContextSwitcher::ContextCallback+0x45 (FPO: [Non-Fpo])
        0110f908 75f33833 fdssdp!CSsdpWorker::WorkerStart+0x9f (FPO: [Non-Fpo])
        0110f914 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0110f954 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 83677b88  Cid 0460.0e9c  Teb: 7ff9f000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            837020a8  SynchronizationEvent
            836a9510  NotificationEvent
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fc9c020       Image:         svchost.exe
        Wait Start TickCount      9654           Ticks: 33845 (0:00:08:47.985)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address fdssdp!CSsdpWorker::WorkerStart (0x6f98890f)
        Stack Init 9f3ac000 Current 9f3ab8d0 Base 9f3ac000 Limit 9f3a9000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f3ab8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f3ab924 81c28c64 nt!KiSwapThread+0x389
        9f3ab970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f3abbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f3abd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f3abd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f3abd64)
        0244f334 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0244f338 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0244f3d4 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0244f3f0 6f9884ea kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0244f5bc 6f9885be fdssdp!CSsdpWorker::WorkerMain+0x195 (FPO: [Non-Fpo])
        0244f5d0 7642e04e fdssdp!WorkerMainWithComContext+0x40 (FPO: [Non-Fpo])
        0244f644 7641e300 ole32!EnterForCallback+0xcf (FPO: [Non-Fpo])
        0244f7a4 7641e3be ole32!SwitchForCallback+0x1a8 (FPO: [Non-Fpo])
        0244f7f8 76451336 ole32!PerformCallback+0xa3 (FPO: [Non-Fpo])
        0244f890 76420a58 ole32!CObjectContext::InternalContextCallback+0x15b (FPO: [Non-Fpo])
        0244f8e0 7641d7ab ole32!CObjectContext::ContextCallback+0x87 (FPO: [Non-Fpo])
        0244f904 6f9889ae ole32!CContextSwitcher::ContextCallback+0x45 (FPO: [Non-Fpo])
        0244f93c 75f33833 fdssdp!CSsdpWorker::WorkerStart+0x9f (FPO: [Non-Fpo])
        0244f948 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0244f988 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 83697780  Cid 0460.0ea0  Teb: 7ff9e000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            837020a8  SynchronizationEvent
            836a9510  NotificationEvent
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fc9c020       Image:         svchost.exe
        Wait Start TickCount      10233          Ticks: 33266 (0:00:08:38.952)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address fdssdp!CSsdpWorker::WorkerStart (0x6f98890f)
        Stack Init 9f3b8000 Current 9f3b78d0 Base 9f3b8000 Limit 9f3b5000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f3b78e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f3b7924 81c28c64 nt!KiSwapThread+0x389
        9f3b7970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f3b7bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f3b7d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f3b7d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f3b7d64)
        0248f744 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0248f748 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0248f7e4 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0248f800 6f9884ea kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0248f9cc 6f9885be fdssdp!CSsdpWorker::WorkerMain+0x195 (FPO: [Non-Fpo])
        0248f9e0 7642e04e fdssdp!WorkerMainWithComContext+0x40 (FPO: [Non-Fpo])
        0248fa54 7641e300 ole32!EnterForCallback+0xcf (FPO: [Non-Fpo])
        0248fbb4 7641e3be ole32!SwitchForCallback+0x1a8 (FPO: [Non-Fpo])
        0248fc08 76451336 ole32!PerformCallback+0xa3 (FPO: [Non-Fpo])
        0248fca0 76420a58 ole32!CObjectContext::InternalContextCallback+0x15b (FPO: [Non-Fpo])
        0248fcf0 7641d7ab ole32!CObjectContext::ContextCallback+0x87 (FPO: [Non-Fpo])
        0248fd14 6f9889ae ole32!CContextSwitcher::ContextCallback+0x45 (FPO: [Non-Fpo])
        0248fd4c 75f33833 fdssdp!CSsdpWorker::WorkerStart+0x9f (FPO: [Non-Fpo])
        0248fd58 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0248fd98 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 836cdac0  Cid 0460.0ea4  Teb: 7ff9d000 Win32Thread: 00000000 WAIT: (WrLpcReply)
UserMode Non-Alertable
            836cdcd4  Semaphore Limit 0x1
        Waiting for reply to ALPC Message a9ba6020
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fc9c020       Image:         svchost.exe
        Wait Start TickCount      9654           Ticks: 33845 (0:00:08:47.985)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address SSDPAPI!GetNotificationLoop (0x72a73289)
        Stack Init 9f3c0000 Current 9f3bfb48 Base 9f3c0000 Limit 9f3bd000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f3bfb60 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f3bfb9c 81c293a7 nt!KiSwapThread+0x389
        9f3bfbfc 81cc0275 nt!KeWaitForSingleObject+0x414
        9f3bfc24 81dc3818 nt!AlpcpSignalAndWait+0x7e
        9f3bfc48 81dc5c29 nt!AlpcpReceiveSynchronousReply+0x2b
        9f3bfcd0 81dc61c5 nt!AlpcpProcessSynchronousRequest+0x201
        9f3bfd3c 81c8caaa nt!NtAlpcSendWaitReceivePort+0xd0
        9f3bfd3c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f3bfd64)
        022ef320 7748f2c0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        022ef324 75d27f41 ntdll!NtAlpcSendWaitReceivePort+0xc (FPO: [8,0,0])
        022ef350 75da37a0 RPCRT4!LRPC_CASSOCIATION::AlpcSendWaitReceivePort+0x24
        022ef850 72a7331b RPCRT4!NdrClientCall2+0x76e
        022ef86c 72a732d4 SSDPAPI!GetNotificationRpc+0x1a (FPO: [Non-Fpo])
        022ef8b0 75f33833 SSDPAPI!GetNotificationLoop+0x59 (FPO: [Non-Fpo])
        022ef8bc 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        022ef8fc 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD a1d3ad78  Cid 0460.0f80  Teb: 7ff94000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Alertable
            9fc22748  QueueObject
        IRP List:
            836d6628: (0006,0100) Flags: 00060030  Mdl: 00000000
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fc9c020       Image:         svchost.exe
        Wait Start TickCount      43052          Ticks: 447 (0:00:00:06.973)
        Context Switch Count      443
        UserTime                  00:00:00.015
        KernelTime                00:00:00.062
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init 9f7f0000 Current 9f7efbc8 Base 9f7f0000 Limit 9f7ed000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f7efbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f7efc1c 81cad431 nt!KiSwapThread+0x389
        9f7efc68 81d8b982 nt!KeRemoveQueueEx+0x568
        9f7efcc0 81c7a036 nt!IoRemoveIoCompletion+0x23
        9f7efd54 81c8caaa nt!NtWaitForWorkViaWorkerFactory+0x1a1
        9f7efd54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f7efd64)
        0150f84c 77490850 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0150f850 7749a1b4 ntdll!NtWaitForWorkViaWorkerFactory+0xc (FPO: [2,0,0])
        0150f978 75f33833 ntdll!TppWorkerThread+0x1f6 (FPO: [Non-Fpo])
        0150f984 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0150f9c4 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 834a9740  Cid 0460.0f84  Teb: 7ff93000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Alertable
            9fc22748  QueueObject
        IRP List:
            837d94d0: (0006,0100) Flags: 00060030  Mdl: 00000000
            837e84f0: (0006,0100) Flags: 00060030  Mdl: 00000000
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fc9c020       Image:         svchost.exe
        Wait Start TickCount      15063          Ticks: 28436 (0:00:07:23.604)
        Context Switch Count      219
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init 9f7ec000 Current 9f7ebbc8 Base 9f7ec000 Limit 9f7e9000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f7ebbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f7ebc1c 81cad431 nt!KiSwapThread+0x389
        9f7ebc68 81d8b982 nt!KeRemoveQueueEx+0x568
        9f7ebcc0 81c7a036 nt!IoRemoveIoCompletion+0x23
        9f7ebd54 81c8caaa nt!NtWaitForWorkViaWorkerFactory+0x1a1
        9f7ebd54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f7ebd64)
        0265f6e0 77490850 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0265f6e4 7749a1b4 ntdll!NtWaitForWorkViaWorkerFactory+0xc (FPO: [2,0,0])
        0265f80c 75f33833 ntdll!TppWorkerThread+0x1f6 (FPO: [Non-Fpo])
        0265f818 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0265f858 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 83885d78  Cid 0460.0fe0  Teb: 7ffdd000 Win32Thread: ff52aa30 WAIT: (UserRequest)
UserMode Non-Alertable
            a180dff0  NotificationEvent
            8392d880  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fc9c020       Image:         svchost.exe
        Wait Start TickCount      14773          Ticks: 28726 (0:00:07:28.128)
        Context Switch Count      81
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init 9f677000 Current 9f6768d0 Base 9f677000 Limit 9f674000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f6768e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f676924 81c28c64 nt!KiSwapThread+0x389
        9f676970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f676bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f676d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f676d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f676d64)
        024cf6cc 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        024cf6d0 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        024cf76c 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        024cf788 729c5951 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        024cf7b4 75d26d7e ssdpsrv!_GetNotificationRpc+0x62 (FPO: [Non-Fpo])
        024cf7d0 75da03a2 RPCRT4!Invoke+0x2a
        024cfbfc 75d9f44c RPCRT4!NdrStubCall2+0x27b
        024cfc18 75d273cb RPCRT4!NdrServerCall2+0x1e
        024cfc54 75d27279 RPCRT4!DispatchToStubInCNoAvrf+0x41
        024cfcc8 75d2770a RPCRT4!RPC_INTERFACE::DispatchToStubWorker+0xdf
        024cfd08 75d275d5 RPCRT4!LRPC_SCALL::DispatchRequest+0xa2
        024cfd74 75d2618a RPCRT4!LRPC_SCALL::HandleRequest+0x1d2
        024cfe1c 75d3b062 RPCRT4!LRPC_ADDRESS::ProcessIO+0x216
        024cfe70 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x162
        024cfe7c 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        024cfea4 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        024cfeb0 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        024cfebc 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        024cfefc 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 83a14030  Cid 0460.09fc  Teb: 7ff97000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            83885628  SynchronizationEvent
            83a140b8  NotificationTimer
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fc9c020       Image:         svchost.exe
        Wait Start TickCount      41316          Ticks: 2183 (0:00:00:34.055)
        Context Switch Count      14
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address upnphost!SVSThreadPool::SVSThreadPoolWorkerThread (0x7243f3db)
        Stack Init a8e76000 Current a8e75c38 Base a8e76000 Limit a8e73000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a8e75c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8e75c8c 81c293a7 nt!KiSwapThread+0x389
        a8e75ce8 81df5057 nt!KeWaitForSingleObject+0x414
        a8e75d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a8e75d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8e75d64)
        0297f898 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0297f89c 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0297f90c 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        0297f920 7243f317 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0297f948 7243f3e8 upnphost!SVSThreadPool::Worker+0x61 (FPO: [Non-Fpo])
        0297f950 75f33833 upnphost!SVSThreadPool::SVSThreadPoolWorkerThread+0xd (FPO: [Non-Fpo])
        0297f95c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0297f99c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 83739b10  Cid 0460.0f7c  Teb: 7ffd7000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            8395d9e8  SynchronizationEvent
            83739b98  NotificationTimer
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fc9c020       Image:         svchost.exe
        Wait Start TickCount      41316          Ticks: 2183 (0:00:00:34.055)
        Context Switch Count      11
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address upnphost!SVSThreadPool::SVSThreadPoolWorkerThread (0x7243f3db)
        Stack Init a0945000 Current a0944c38 Base a0945000 Limit a0942000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a0944c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0944c8c 81c293a7 nt!KiSwapThread+0x389
        a0944ce8 81df5057 nt!KeWaitForSingleObject+0x414
        a0944d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a0944d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0944d64)
        00dcfb58 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00dcfb5c 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        00dcfbcc 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        00dcfbe0 7243f317 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        00dcfc08 7243f3e8 upnphost!SVSThreadPool::Worker+0x61 (FPO: [Non-Fpo])
        00dcfc10 75f33833 upnphost!SVSThreadPool::SVSThreadPoolWorkerThread+0xd (FPO: [Non-Fpo])
        00dcfc1c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00dcfc5c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 836843c0  Cid 0460.0d30  Teb: 7ffdb000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            9fc29d90  QueueObject
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fc9c020       Image:         svchost.exe
        Wait Start TickCount      34814          Ticks: 8685 (0:00:02:15.486)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init 9f2d8000 Current 9f2d7bc8 Base 9f2d8000 Limit 9f2d5000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f2d7be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f2d7c1c 81cad431 nt!KiSwapThread+0x389
        9f2d7c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        9f2d7cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        9f2d7d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        9f2d7d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f2d7d64)
        011afb58 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        011afb5c 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        011afb88 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        011afbc4 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        011afc30 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        011afc3c 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        011afc64 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        011afc70 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        011afc7c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        011afcbc 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Svchost process (NetworkService)

```
PROCESS 9fcb2858  SessionId: 0  Cid: 04c4    Peb: 7ffdf000  ParentCid: 0214
    DirBase: 29a01260  ObjectTable: a0130fa0  HandleCount: 505.
    Image: svchost.exe
    VadRoot 8987f190 Vads 206 Clone 0 Private 1658. Modified 471. Locked 0.
    DeviceMap 9f999328
    Token                             a012a030
    ElapsedTime                       00:11:02.578
    UserTime                          00:00:00.171
    KernelTime                        00:00:00.483
    QuotaPoolUsage[PagedPool]         116872
    QuotaPoolUsage[NonPagedPool]      16024
    Working Set Sizes (now,min,max)  (2641, 50, 345) (10564KB, 200KB, 1380KB)
    PeakWorkingSetSize                3306
    VirtualSize                       73 Mb
    PeakVirtualSize                   76 Mb
    PageFaultCount                    4293
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      3226

    Setting context for this process...
.process /p /r ffffffff9fcb2858

    !peb
PEB at 7ffdf000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00dd0000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 002d17b8 . 003176f0
    Ldr.InLoadOrderModuleList:           002d1738 . 01bea140
    Ldr.InMemoryOrderModuleList:         002d1740 . 01bea148
            Base TimeStamp                     Module
          dd0000 4549adc4 Nov 02 08:35:16 2006 C:\Windows\system32\svchost.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        75020000 4549bddb Nov 02 09:43:55 2006 C:\Windows\system32\NTMARTA.DLL
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        76310000 4549be44 Nov 02 09:45:40 2006 C:\Windows\system32\WLDAP32.dll
        75fe0000 4549be0e Nov 02 09:44:46 2006 C:\Windows\system32\WS2_32.dll
        77550000 4549bdc7 Nov 02 09:43:35 2006 C:\Windows\system32\NSI.dll
        75ce0000 4549bd99 Nov 02 09:42:49 2006 C:\Windows\system32\PSAPI.DLL
        75ad0000 4549bda8 Nov 02 09:43:04 2006 C:\Windows\system32\SAMLIB.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        744a0000 4549bcf6 Nov 02 09:40:06 2006 c:\windows\system32\dnsrslvr.dll
        75af0000 4549bcf1 Nov 02 09:40:01 2006 c:\windows\system32\DNSAPI.dll
        75570000 46807ea6 Jun 26 03:49:10 2007 c:\windows\system32\dhcpcsvc.DLL
        75b80000 4549bdd2 Nov 02 09:43:46 2006 c:\windows\system32\Secur32.dll
        75560000 4549be1e Nov 02 09:45:02 2006 c:\windows\system32\WINNSI.DLL
        75540000 46807ea7 Jun 26 03:49:11 2007 c:\windows\system32\dhcpcsvc6.DLL
        755b0000 4549bd3f Nov 02 09:41:19 2006 c:\windows\system32\IPHLPAPI.DLL
        75250000 4549bd69 Nov 02 09:42:01 2006 C:\Windows\system32\mswsock.dll
        752b0000 4549be21 Nov 02 09:45:05 2006 C:\Windows\System32\wship6.dll
        752c0000 4549be27 Nov 02 09:45:11 2006 C:\Windows\System32\wshtcpip.dll
        72f00000 4549bd29 Nov 02 09:40:57 2006 c:\windows\system32\cryptsvc.dll
```

```
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        72cb0000 4549bded Nov 02 09:44:13 2006 c:\windows\system32\VSSAPI.DLL
        74d00000 4549bcbc Nov 02 09:39:08 2006 c:\windows\system32\ATL.DLL
        72e50000 4549bdef Nov 02 09:44:15 2006 c:\windows\system32\vsstrace.dll
        757b0000 4549bccf Nov 02 09:39:27 2006 c:\windows\system32\AUTHZ.dll
        73a70000 4549be05 Nov 02 09:44:37 2006 c:\windows\system32\XmlLite.dll
        75840000 4549bd53 Nov 02 09:41:39 2006 c:\windows\system32\NETAPI32.dll
        75750000 4549bd14 Nov 02 09:40:36 2006 c:\windows\system32\MPR.dll
        77030000 4549bdb0 Nov 02 09:43:12 2006 C:\Windows\system32\SETUPAPI.dll
        75650000 45b96fde Jan 26 03:05:02 2007 c:\windows\system32\CRYPT32.dll
        75820000 4549bd41 Nov 02 09:41:21 2006 c:\windows\system32\MSASN1.dll
        75ba0000 4549bde2 Nov 02 09:44:02 2006 c:\windows\system32\USERENV.dll
        72a80000 4549bd6c Nov 02 09:42:04 2006 c:\windows\system32\nlasvc.dll
        755d0000 4549bdf6 Nov 02 09:44:22 2006 c:\windows\system32\wevtapi.dll
        72b90000 4549bd4b Nov 02 09:41:31 2006 c:\windows\system32\ncsi.dll
        73420000 4549be18 Nov 02 09:44:56 2006 c:\windows\system32\WINHTTP.dll
        763b0000 4549bdb9 Nov 02 09:43:21 2006 C:\Windows\system32\SHLWAPI.dll
        74fe0000 46d779a1 Aug 31 03:14:57 2007 c:\windows\system32\WTSAPI32.dll
        754a0000 4549bcb9 Nov 02 09:39:05 2006 c:\windows\system32\bcrypt.dll
        74aa0000 4549bd09 Nov 02 09:40:25 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_5d07289e07e1d100\comctl32.dll
        75480000 4549bd20 Nov 02 09:40:48 2006 C:\Windows\system32\credssp.dll
        75050000 46773a78 Jun 19 03:07:52 2007 C:\Windows\system32\schannel.dll
        72a70000 4549bdc7 Nov 02 09:43:35 2006 C:\Windows\system32\ssdpapi.dll
        75350000 4549bdae Nov 02 09:43:10 2006 C:\Windows\system32\rsaenh.dll
        773a0000 4549bce9 Nov 02 09:39:53 2006 C:\Windows\system32\CLBCatQ.DLL
        745a0000 4549bcf8 Nov 02 09:40:08 2006 C:\Windows\system32\es.dll
        744e0000 4549bd96 Nov 02 09:42:46 2006 C:\Windows\system32\PROPSYS.dll
        75300000 4549be2e Nov 02 09:45:18 2006 C:\Windows\system32\WINSTA.dll
        725c0000 4549bde8 Nov 02 09:44:08 2006 c:\windows\system32\termsrv.dll
        72a50000 4549bce5 Nov 02 09:39:49 2006 c:\windows\system32\ICAAPI.dll
        74ff0000 4549be2f Nov 02 09:45:19 2006 c:\windows\system32\WINTRUST.dll
        77580000 462434a3 Apr 17 03:44:51 2007 C:\Windows\system32\imagehlp.dll
        76560000 4681c95d Jun 27 03:20:13 2007 C:\Windows\system32\SHELL32.dll
        718b0000 4549bcf9 Nov 02 09:40:09 2006 C:\Windows\system32\ESENT.dll
        709b0000 4549bdd6 Nov 02 09:43:50 2006 c:\windows\system32\tapisrv.dll
        731d0000 4549bcbd Nov 02 09:39:09 2006 c:\windows\system32\ACTIVEDS.dll
        73190000 4549bcce Nov 02 09:39:26 2006 c:\windows\system32\adsldpc.dll
        73160000 4549bd21 Nov 02 09:40:49 2006 c:\windows\system32\credui.dll
        73950000 4549bdba Nov 02 09:43:22 2006 c:\windows\system32\rtutils.dll
        738c0000 4549be1d Nov 02 09:45:01 2006 c:\windows\system32\WINMM.dll
        73880000 4549bd93 Nov 02 09:42:43 2006 c:\windows\system32\OLEACC.dll
        707e0000 4549bddb Nov 02 09:43:55 2006 C:\Windows\system32\unimdm.tsp
        73ac0000 4549bddd Nov 02 09:43:57 2006 C:\Windows\system32\uniplat.dll
        73ab0000 468b03d2 Jul 04 03:20:02 2007 C:\Windows\system32\kmddsp.tsp
        73aa0000 468b0393 Jul 04 03:18:59 2007 C:\Windows\system32\ndptsp.tsp
        739f0000 4549bcdf Nov 02 09:39:43 2006 C:\Windows\system32\hidphone.tsp
        74cb0000 4549bcde Nov 02 09:39:42 2006 C:\Windows\system32\HID.DLL
        6e170000 4549bd69 Nov 02 09:42:01 2006 c:\windows\system32\msdtckrm.dll
        753f0000 4549bde4 Nov 02 09:44:04 2006 c:\windows\system32\VERSION.dll
        74d20000 4549bd8c Nov 02 09:42:36 2006 c:\windows\system32\ktmw32.dll
    SubSystemData:     00000000
    ProcessHeap:       002d0000
    ProcessParameters: 002d1060
    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;C:\Program Files\QuickTime\QTSystem\'
    Environment:  002d07e8
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        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;C:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        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=WORKGROUP
        USERNAME=HOME$
        USERPROFILE=C:\Windows\ServiceProfiles\NetworkService
        windir=C:\Windows


        THREAD 849cc770  Cid 04c4.04c8  Teb: 7ffde000 Win32Thread: ff5020c0 WAIT: (Executive)
UserMode Non-Alertable
            9fcdefa4  NotificationEvent
        IRP List:
            835b90d0: (0006,0094) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            9fcb2858       Image:         svchost.exe
        Wait Start TickCount      9766           Ticks: 33733 (0:00:08:46.238)
        Context Switch Count      71
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address svchost!wmainCRTStartup (0x00dd20bf)
        Stack Init a0368000 Current a0367bc8 Base a0368000 Limit a0365000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a0367be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0367c1c 81c293a7 nt!KiSwapThread+0x389
        a0367c78 81d88faf nt!KeWaitForSingleObject+0x414
        a0367cac 81d93669 nt!IopSynchronousServiceTail+0x258
        a0367d38 81c8caaa nt!NtReadFile+0x646
        a0367d38 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0367d64)
        0015f4b4 77490080 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0015f4b8 75f3853f ntdll!ZwReadFile+0xc (FPO: [9,0,0])
        0015f530 775cffe2 kernel32!ReadFile+0x20e (FPO: [Non-Fpo])
        0015f55c 775cfdfb ADVAPI32!ScGetPipeInput+0x2a (FPO: [Non-Fpo])
        0015f5c4 775cbdd2 ADVAPI32!ScDispatcherLoop+0x6c (FPO: [Non-Fpo])
        0015f83c 00dd241d ADVAPI32!StartServiceCtrlDispatcherW+0xce (FPO: [Non-Fpo])
        0015f844 00dd2401 svchost!SvcHostMain+0x12 (FPO: [Non-Fpo])
        0015f848 00dd2183 svchost!wmain+0x5 (FPO: [Non-Fpo])
        0015f88c 75f33833 svchost!_initterm_e+0x163 (FPO: [Non-Fpo])
        0015f898 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0015f8d8 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fcc9030  Cid 04c4.04f0  Teb: 7ffdc000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fcc84e8  NotificationEvent
            9fcc7254  NotificationEvent
            9fcc93a0  SynchronizationEvent
            9fcc9328  SynchronizationEvent
        IRP List:
            9fc467e8: (0006,01d8) Flags: 00060000  Mdl: 00000000
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            9fcb2858       Image:         svchost.exe
        Wait Start TickCount      1090           Ticks: 42409 (0:00:11:01.584)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address dnsrslvr!NotifyThread (0x744aad6a)
        Stack Init a026e000 Current a026d8d0 Base a026e000 Limit a026b000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a026d8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a026d924 81c28c64 nt!KiSwapThread+0x389
        a026d970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a026dbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a026dd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a026dd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a026dd64)
        00e4f8c4 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00e4f8c8 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00e4f964 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        00e4f980 744aaddd kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        00e4f9b4 75f33833 dnsrslvr!NotifyThread+0x73 (FPO: [Non-Fpo])
        00e4f9c0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00e4fa00 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fcbfd78  Cid 04c4.04f8  Teb: 7ffdb000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fccb3a8  NotificationEvent
            9fcc84e8  NotificationEvent
        IRP List:
            836476b0: (0006,0100) Flags: 00060030  Mdl: 00000000
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            9fcb2858       Image:         svchost.exe
        Wait Start TickCount      10305          Ticks: 33194 (0:00:08:37.829)
        Context Switch Count      182
        UserTime                  00:00:00.031
        KernelTime                00:00:00.046
        Win32 Start Address dnsrslvr!Ip_NotifyThread (0x744a85aa)
        Stack Init a027a000 Current a02798d0 Base a027a000 Limit a0277000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a02798e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0279924 81c28c64 nt!KiSwapThread+0x389
        a0279970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a0279bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a0279d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a0279d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0279d64)
        0086f874 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0086f878 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0086f914 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0086f930 744a8673 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0086f984 75f33833 dnsrslvr!Ip_NotifyThread+0xdb (FPO: [Non-Fpo])
        0086f990 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0086f9d0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fcbfac0  Cid 04c4.04fc  Teb: 7ffda000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fcc8630  NotificationEvent
            9fcc8600  NotificationEvent
            9fcc85d0  NotificationEvent
            9fcbfb48  NotificationTimer
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            9fcb2858       Image:         svchost.exe
        Wait Start TickCount      10086          Ticks: 33413 (0:00:08:41.246)
        Context Switch Count      226
        UserTime                  00:00:00.031
        KernelTime                00:00:00.031
        Win32 Start Address dnsrslvr!Mcast_Thread (0x744a515b)
        Stack Init a028a000 Current a02898d0 Base a028a000 Limit a0287000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a02898e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0289924 81c28c64 nt!KiSwapThread+0x389
        a0289970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a0289bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a0289d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a0289d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0289d64)
        00daf99c 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00daf9a0 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00dafa3c 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        00dafa58 744a51ae kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        00dafa94 75f33833 dnsrslvr!Mcast_Thread+0x94 (FPO: [Non-Fpo])
        00dafaa0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00dafae0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fcc26e0  Cid 04c4.0504  Teb: 7ffd8000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            9fcc2988  SynchronizationTimer
            9fcc2b10  SynchronizationEvent
            9e1f96d8  NotificationEvent
            89881ff0  NotificationEvent
            9fdfcae8  SynchronizationTimer
            9fd93658  SynchronizationEvent
            9fd904f0  SynchronizationEvent
            89851a68  SynchronizationEvent
            9fd96540  SynchronizationEvent
            a18bdf20  SynchronizationEvent
            a18dc090  SynchronizationEvent
            835c4d78  NotificationEvent
            a194d738  SynchronizationEvent
            9fd93980  SynchronizationEvent
            9fd93de8  SynchronizationEvent
            9fdfca88  SynchronizationEvent
            9fdec470  SynchronizationEvent
            89976250  SynchronizationEvent
            9fdfd278  SynchronizationEvent
            835ffcbc  NotificationEvent
            83a0bc70  ProcessObject
            83952da4  NotificationEvent
            a189b350  SynchronizationEvent
            9fdfc9b0  SynchronizationTimer
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            9fcb2858       Image:         svchost.exe
        Wait Start TickCount      43257          Ticks: 242 (0:00:00:03.775)
        Context Switch Count      273
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x7744b49a)
        Stack Init a029e000 Current a029d8d0 Base a029e000 Limit a029b000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a029d8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a029d924 81c28c64 nt!KiSwapThread+0x389
        a029d970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a029dbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a029dd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a029dd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a029dd64)
        00e8f738 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00e8f73c 7744b65b ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00e8f8d8 75f33833 ntdll!TppWaiterpThread+0x294 (FPO: [Non-Fpo])
        00e8f8e4 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00e8f924 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fdfdbc0  Cid 04c4.07e4  Teb: 7ffd7000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Alertable
            a189b3e0  QueueObject
        IRP List:
            83855c50: (0006,01d8) Flags: 00060000  Mdl: 00000000
            83a0ae20: (0006,01d8) Flags: 00060000  Mdl: 00000000
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            9fcb2858       Image:         svchost.exe
        Wait Start TickCount      17269          Ticks: 26230 (0:00:06:49.190)
        Context Switch Count      61
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init 9e9e0000 Current 9e9dfbc8 Base 9e9e0000 Limit 9e9dd000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9e9dfbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e9dfc1c 81cad431 nt!KiSwapThread+0x389
        9e9dfc68 81d8b982 nt!KeRemoveQueueEx+0x568
        9e9dfcc0 81c7a036 nt!IoRemoveIoCompletion+0x23
        9e9dfd54 81c8caaa nt!NtWaitForWorkViaWorkerFactory+0x1a1
        9e9dfd54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9e9dfd64)
        0120f93c 77490850 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0120f940 7749a1b4 ntdll!NtWaitForWorkViaWorkerFactory+0xc (FPO: [2,0,0])
        0120fa68 75f33833 ntdll!TppWorkerThread+0x1f6 (FPO: [Non-Fpo])
        0120fa74 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0120fab4 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fd936d0  Cid 04c4.07e8  Teb: 7ffaf000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fdfd630  SynchronizationEvent
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            9fcb2858       Image:         svchost.exe
        Wait Start TickCount      9939           Ticks: 33560 (0:00:08:43.539)
        Context Switch Count      103
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address nlasvc!QueueMonitor (0x72a8d131)
        Stack Init a1b5c000 Current a1b5bc38 Base a1b5c000 Limit a1b59000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1b5bc50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1b5bc8c 81c293a7 nt!KiSwapThread+0x389
        a1b5bce8 81df5057 nt!KeWaitForSingleObject+0x414
        a1b5bd50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a1b5bd50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1b5bd64)
        0189f864 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0189f868 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0189f8d8 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        0189f8ec 72a8d19a kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0189f91c 75f33833 nlasvc!QueueMonitor+0x265 (FPO: [Non-Fpo])
        0189f928 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0189f968 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fdb37a8  Cid 04c4.0170  Teb: 7ffd3000 Win32Thread: 00000000 WAIT: (WrLpcReply)
UserMode Non-Alertable
            9fdb39bc  Semaphore Limit 0x1
        Waiting for reply to ALPC Message a1318b28
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            9fcb2858       Image:         svchost.exe
        Wait Start TickCount      1900           Ticks: 41599 (0:00:10:48.948)
        Context Switch Count      8
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ssdpapi!GetNotificationLoop (0x72a73289)
        Stack Init a1add000 Current a1adcb48 Base a1add000 Limit a1ada000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1adcb60 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1adcb9c 81c293a7 nt!KiSwapThread+0x389
        a1adcbfc 81cc0275 nt!KeWaitForSingleObject+0x414
        a1adcc24 81dc3818 nt!AlpcpSignalAndWait+0x7e
        a1adcc48 81dc5c29 nt!AlpcpReceiveSynchronousReply+0x2b
        a1adccd0 81dc61c5 nt!AlpcpProcessSynchronousRequest+0x201
        a1adcd3c 81c8caaa nt!NtAlpcSendWaitReceivePort+0xd0
        a1adcd3c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1adcd64)
        0118f578 7748f2c0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0118f57c 75d27f41 ntdll!NtAlpcSendWaitReceivePort+0xc (FPO: [8,0,0])
        0118f5a8 75da37a0 RPCRT4!LRPC_CASSOCIATION::AlpcSendWaitReceivePort+0x24
        0118faa8 72a7331b RPCRT4!NdrClientCall2+0x76e
        0118fac4 72a732d4 ssdpapi!GetNotificationRpc+0x1a (FPO: [Non-Fpo])
        0118fb08 75f33833 ssdpapi!GetNotificationLoop+0x59 (FPO: [Non-Fpo])
        0118fb14 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0118fb54 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD a18ab760  Cid 04c4.02e4  Teb: 7ffa8000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            a18bdf50  SynchronizationEvent
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            9fcb2858       Image:         svchost.exe
        Wait Start TickCount      1854           Ticks: 41645 (0:00:10:49.666)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address termsrv!CService::staticMiscThread (0x725d2701)
        Stack Init a1f02000 Current a1f01c38 Base a1f02000 Limit a1eff000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1f01c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1f01c8c 81c293a7 nt!KiSwapThread+0x389
        a1f01ce8 81df5057 nt!KeWaitForSingleObject+0x414
        a1f01d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a1f01d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1f01d64)
        019ffc68 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        019ffc6c 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        019ffcdc 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        019ffcf0 725d1fb4 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        019ffd08 725d270e termsrv!CService::MiscThread+0x48 (FPO: [Non-Fpo])
        019ffd10 75f33833 termsrv!CService::staticMiscThread+0xd (FPO: [Non-Fpo])
        019ffd1c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        019ffd5c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD a18d3030  Cid 04c4.04a0  Teb: 7ffaa000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            a18dc060  SynchronizationEvent
            a18bbaf0  NotificationEvent
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            9fcb2858       Image:         svchost.exe
        Wait Start TickCount      1860           Ticks: 41639 (0:00:10:49.572)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address msvcrt!_endthreadex (0x7628639b)
        Stack Init a1aa7000 Current a1aa68d0 Base a1aa7000 Limit a1aa4000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1aa68e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1aa6924 81c28c64 nt!KiSwapThread+0x389
        a1aa6970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1aa6bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1aa6d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1aa6d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1aa6d64)
        00f8fb28 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00f8fb2c 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00f8fbc8 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        00f8fbe4 72b98855 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        00f8fc10 762862b6 ncsi!CNcsiConfigData::MonitorRegistry+0x114 (FPO: [Non-Fpo])
        00f8fc48 762863de msvcrt!_endthreadex+0x44 (FPO: [Non-Fpo])
        00f8fc50 75f33833 msvcrt!_endthreadex+0xce (FPO: [Non-Fpo])
        00f8fc5c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00f8fc9c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD a18d33b8  Cid 04c4.04a8  Teb: 7ffa7000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            a18bb7c0  SynchronizationEvent
            9fc4f830  SynchronizationEvent
            9fc4c268  SynchronizationEvent
        IRP List:
            847ae7a0: (0006,0094) Flags: 00060000  Mdl: 00000000
            9fc34f28: (0006,0094) Flags: 00060000  Mdl: 00000000
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            9fcb2858       Image:         svchost.exe
        Wait Start TickCount      9807           Ticks: 33692 (0:00:08:45.598)
        Context Switch Count      144
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address msvcrt!_endthreadex (0x7628639b)
        Stack Init a1eea000 Current a1ee98d0 Base a1eea000 Limit a1ee7000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1ee98e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1ee9924 81c28c64 nt!KiSwapThread+0x389
        a1ee9970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1ee9bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1ee9d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1ee9d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1ee9d64)
        019bf6a4 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        019bf6a8 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        019bf744 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        019bf760 72b95d5c kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        019bf818 762862b6 ncsi!NcsiMediaChange+0x218 (FPO: [Non-Fpo])
        019bf850 762863de msvcrt!_endthreadex+0x44 (FPO: [Non-Fpo])
        019bf858 75f33833 msvcrt!_endthreadex+0xce (FPO: [Non-Fpo])
        019bf864 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        019bf8a4 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD a1969a88  Cid 04c4.0bcc  Teb: 7ffd6000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Alertable
            9fcc25e0  QueueObject
            a1969b10  NotificationTimer
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            9fcb2858       Image:         svchost.exe
        Wait Start TickCount      43257          Ticks: 242 (0:00:00:03.775)
        Context Switch Count      259
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init 88e0c000 Current 88e0bbc8 Base 88e0c000 Limit 88e09000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        88e0bbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        88e0bc1c 81cad431 nt!KiSwapThread+0x389
        88e0bc68 81d8b982 nt!KeRemoveQueueEx+0x568
        88e0bcc0 81c7a036 nt!IoRemoveIoCompletion+0x23
        88e0bd54 81c8caaa nt!NtWaitForWorkViaWorkerFactory+0x1a1
        88e0bd54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 88e0bd64)
        0192fa7c 77490850 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0192fa80 7749a1b4 ntdll!NtWaitForWorkViaWorkerFactory+0xc (FPO: [2,0,0])
        0192fba8 75f33833 ntdll!TppWorkerThread+0x1f6 (FPO: [Non-Fpo])
        0192fbb4 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0192fbf4 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 835c4870  Cid 04c4.0d6c  Teb: 7ffa9000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            836ed888  NotificationEvent
            835c48f8  NotificationTimer
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            9fcb2858       Image:         svchost.exe
        Wait Start TickCount      42097          Ticks: 1402 (0:00:00:21.871)
        Context Switch Count      19
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address tapisrv!SPEventHandlerThread (0x709b134d)
        Stack Init a9000000 Current a8fffc38 Base a9000000 Limit a8ffd000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a8fffc50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8fffc8c 81c293a7 nt!KiSwapThread+0x389
        a8fffce8 81df5057 nt!KeWaitForSingleObject+0x414
        a8fffd50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a8fffd50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8fffd64)
        0174fa40 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0174fa44 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0174fab4 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        0174fac8 709b13a2 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0174faf8 75f33833 tapisrv!SPEventHandlerThread+0x64 (FPO: [Non-Fpo])
        0174fb04 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0174fb44 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 835c4540  Cid 04c4.0d70  Teb: 7ffa5000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            835c47e8  NotificationEvent
            835c45c8  NotificationTimer
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            9fcb2858       Image:         svchost.exe
        Wait Start TickCount      42097          Ticks: 1402 (0:00:00:21.871)
        Context Switch Count      19
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address tapisrv!SPEventHandlerThread (0x709b134d)
        Stack Init a8f9c000 Current a8f9bc38 Base a8f9c000 Limit a8f99000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a8f9bc50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8f9bc8c 81c293a7 nt!KiSwapThread+0x389
        a8f9bce8 81df5057 nt!KeWaitForSingleObject+0x414
        a8f9bd50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a8f9bd50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8f9bd64)
        01aafd68 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01aafd6c 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        01aafddc 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        01aafdf0 709b13a2 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        01aafe20 75f33833 tapisrv!SPEventHandlerThread+0x64 (FPO: [Non-Fpo])
        01aafe2c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01aafe6c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fd14888  Cid 04c4.0d84  Teb: 7ffab000 Win32Thread: 00000000 WAIT: (DelayExecution)
UserMode Alertable
            9fd14910  NotificationTimer
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            9fcb2858       Image:         svchost.exe
        Wait Start TickCount      9413           Ticks: 34086 (0:00:08:51.745)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address unimdm!tepAPC (0x707fda43)
        Stack Init a0887000 Current a0886c58 Base a0887000 Limit a0884000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a0886c70 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0886cac 81cac48e nt!KiSwapThread+0x389
        a0886d08 81e90bf1 nt!KeDelayExecutionThread+0x397
        a0886d54 81c8caaa nt!NtDelayExecution+0x8d
        a0886d54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0886d64)
        0298fee8 7748f7c0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0298feec 75f378e0 ntdll!NtDelayExecution+0xc (FPO: [2,0,0])
        0298ff54 707fda78 kernel32!SleepEx+0x62 (FPO: [Non-Fpo])
        0298ff68 75f33833 unimdm!tepAPC+0x35 (FPO: [Non-Fpo])
        0298ff74 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0298ffb4 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 835fb030  Cid 04c4.0d98  Teb: 7ffa3000 Win32Thread: ff530c18 WAIT: (UserRequest)
UserMode Non-Alertable
            9fd24170  NotificationEvent
            9fc4fc78  SynchronizationEvent
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            9fcb2858       Image:         svchost.exe
        Wait Start TickCount      9415           Ticks: 34084 (0:00:08:51.713)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address uniplat!MonitorWorkerThread (0x73ac1d37)
        Stack Init 9f2a4000 Current 9f2a38d0 Base 9f2a4000 Limit 9f2a1000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f2a38e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f2a3924 81c28c64 nt!KiSwapThread+0x389
        9f2a3970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f2a3bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f2a3d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f2a3d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f2a3d64)
        01d0fb40 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01d0fb44 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        01d0fbe0 761dc4b7 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        01d0fc34 761d8b83 USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
        01d0fc50 73ac129c USER32!MsgWaitForMultipleObjects+0x1f (FPO: [Non-Fpo])
        01d0fcbc 73ac1d48 uniplat!DllWinMain+0xd9 (FPO: [Non-Fpo])
        01d0fcd0 75f33833 uniplat!MonitorWorkerThread+0x11 (FPO: [Non-Fpo])
        01d0fcdc 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01d0fd1c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 899bed78  Cid 04c4.0d9c  Teb: 7ffa2000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            9fd21388  QueueObject
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            9fcb2858       Image:         svchost.exe
        Wait Start TickCount      9418           Ticks: 34081 (0:00:08:51.667)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address kmddsp!AsyncEventsThread (0x73ab76ca)
        Stack Init a8fe8000 Current a8fe7bc8 Base a8fe8000 Limit a8fe5000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a8fe7be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8fe7c1c 81cad431 nt!KiSwapThread+0x389
        a8fe7c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a8fe7cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a8fe7d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a8fe7d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8fe7d64)
        00fdfda0 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00fdfda4 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        00fdfdd0 73ab7759 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        00fdfe34 75f33833 kmddsp!AsyncEventsThread+0x8f (FPO: [Non-Fpo])
        00fdfe40 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00fdfe80 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fd536b8  Cid 04c4.0da0  Teb: 7ffa1000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            9fd30128  QueueObject
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            9fcb2858       Image:         svchost.exe
        Wait Start TickCount      9418           Ticks: 34081 (0:00:08:51.667)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ndptsp!AsyncEventsThread (0x73aa9d8d)
        Stack Init a8fb0000 Current a8fafbc8 Base a8fb0000 Limit a8fad000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a8fafbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8fafc1c 81cad431 nt!KiSwapThread+0x389
        a8fafc6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a8fafcc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a8fafd48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a8fafd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8fafd64)
        02b7fae0 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        02b7fae4 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        02b7fb10 73aa9e1c kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        02b7fb70 75f33833 ndptsp!AsyncEventsThread+0x8f (FPO: [Non-Fpo])
        02b7fb7c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        02b7fbbc 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9e1cf728  Cid 04c4.0da4  Teb: 7ffa0000 Win32Thread: ff5341f8 WAIT: (UserRequest)
UserMode Non-Alertable
            9fd04a78  NotificationEvent
            9fd04fc8  SynchronizationEvent
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            9fcb2858       Image:         svchost.exe
        Wait Start TickCount      9419           Ticks: 34080 (0:00:08:51.651)
        Context Switch Count      6
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address hidphone!AsyncEventQueueServiceThread (0x739f4140)
        Stack Init a09a9000 Current a09a88d0 Base a09a9000 Limit a09a6000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a09a88e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a09a8924 81c28c64 nt!KiSwapThread+0x389
        a09a8970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a09a8bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a09a8d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a09a8d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a09a8d64)
        02c2f8ec 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        02c2f8f0 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        02c2f98c 761dc4b7 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        02c2f9e0 739f4209 USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
        02c2fa5c 75f33833 hidphone!AsyncEventQueueServiceThread+0xc9 (FPO: [Non-Fpo])
        02c2fa68 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        02c2faa8 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 837dc030  Cid 04c4.0f30  Teb: 7ff9e000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            83689300  QueueObject
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            9fcb2858       Image:         svchost.exe
        Wait Start TickCount      14313          Ticks: 29186 (0:00:07:35.304)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address msdtckrm!ProcessNotification (0x6e19ce0a)
        Stack Init a8f20000 Current a8f1fbc8 Base a8f20000 Limit a8f1d000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a8f1fbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8f1fc1c 81cad431 nt!KiSwapThread+0x389
        a8f1fc6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a8f1fcc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a8f1fd48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a8f1fd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8f1fd64)
        02bcf968 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        02bcf96c 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        02bcf998 6e19cef0 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        02bcf9f8 75f33833 msdtckrm!ProcessNotification+0xe6 (FPO: [Non-Fpo])
        02bcfa04 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        02bcfa44 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 83699d30  Cid 04c4.0120  Teb: 7ff9d000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Alertable
            9fcc25e0  QueueObject
            83699db8  NotificationTimer
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            9fcb2858       Image:         svchost.exe
        Wait Start TickCount      43257          Ticks: 242 (0:00:00:03.775)
        Context Switch Count      159
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init 9f77c000 Current 9f77bbc8 Base 9f77c000 Limit 9f779000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f77bbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f77bc1c 81cad431 nt!KiSwapThread+0x389
        9f77bc68 81d8b982 nt!KeRemoveQueueEx+0x568
        9f77bcc0 81c7a036 nt!IoRemoveIoCompletion+0x23
        9f77bd54 81c8caaa nt!NtWaitForWorkViaWorkerFactory+0x1a1
        9f77bd54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f77bd64)
        02aafccc 77490850 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        02aafcd0 7749a1b4 ntdll!NtWaitForWorkViaWorkerFactory+0xc (FPO: [2,0,0])
        02aafdf8 75f33833 ntdll!TppWorkerThread+0x1f6 (FPO: [Non-Fpo])
        02aafe04 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        02aafe44 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 847b2ac0  Cid 04c4.0194  Teb: 7ffdd000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            8371d390  NotificationEvent
            836d5a48  NotificationEvent
            9fcc40c0  NotificationEvent
            847b2b48  NotificationTimer
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            9fcb2858       Image:         svchost.exe
        Wait Start TickCount      10046          Ticks: 33453 (0:00:08:41.870)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address dnsrslvr!Responder_Thread (0x744a51f2)
        Stack Init 9f78c000 Current 9f78b8d0 Base 9f78c000 Limit 9f789000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f78b8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f78b924 81c28c64 nt!KiSwapThread+0x389
        9f78b970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f78bbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f78bd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f78bd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f78bd64)
        02a3fa74 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        02a3fa78 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        02a3fb14 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        02a3fb30 744a5267 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        02a3fb5c 75f33833 dnsrslvr!Responder_Thread+0xbf (FPO: [Non-Fpo])
        02a3fb68 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        02a3fba8 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 83702550  Cid 04c4.09a4  Teb: 7ffd5000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            9fcdc170  QueueObject
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            9fcb2858       Image:         svchost.exe
        Wait Start TickCount      26879          Ticks: 16620 (0:00:04:19.273)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init a0338000 Current a0337bc8 Base a0338000 Limit a0335000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a0337be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0337c1c 81cad431 nt!KiSwapThread+0x389
        a0337c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a0337cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a0337d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a0337d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0337d64)
        01b7fc78 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01b7fc7c 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        01b7fca8 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        01b7fce4 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        01b7fd50 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        01b7fd5c 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        01b7fd80 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        01b7fd8c 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        01b7fd98 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01b7fdd8 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Spoolsv process

```
PROCESS 9fd42790  SessionId: 0  Cid: 05e8    Peb: 7ffd9000  ParentCid: 0214
    DirBase: 29a01280  ObjectTable: a0072d98  HandleCount: 310.
    Image: spoolsv.exe
    VadRoot 9fd4e1e8 Vads 179 Clone 0 Private 735. Modified 59. Locked 0.
    DeviceMap 85a03048
    Token                             a01e1c10
    ElapsedTime                       00:11:01.439
    UserTime                          00:00:00.015
    KernelTime                        00:00:00.078
    QuotaPoolUsage[PagedPool]         106736
    QuotaPoolUsage[NonPagedPool]      9032
    Working Set Sizes (now,min,max)  (2197, 50, 345) (8788KB, 200KB, 1380KB)
    PeakWorkingSetSize                2306
    VirtualSize                       68 Mb
    PeakVirtualSize                   71 Mb
    PageFaultCount                    3960
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      1497

    Setting context for this process...
.process /p /r ffffffff9fd42790

    !peb
PEB at 7ffd9000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00e00000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00361728 . 003a6318
    Ldr.InLoadOrderModuleList:           003616a8 . 003a6308
    Ldr.InMemoryOrderModuleList:         003616b0 . 003a6310
            Base TimeStamp                     Module
          e00000 4549b734 Nov 02 09:15:32 2006 C:\Windows\System32\spoolsv.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        75610000 4679de70 Jun 21 03:12:00 2007 C:\Windows\System32\slc.dll
        75b80000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\System32\secur32.dll
        75480000 4549bd20 Nov 02 09:40:48 2006 C:\Windows\System32\credssp.dll
        75650000 45b96fde Jan 26 03:05:02 2007 C:\Windows\System32\CRYPT32.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        75820000 4549bd41 Nov 02 09:41:21 2006 C:\Windows\System32\MSASN1.dll
        75ba0000 4549bde2 Nov 02 09:44:02 2006 C:\Windows\System32\USERENV.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        75050000 46773a78 Jun 19 03:07:52 2007 C:\Windows\system32\schannel.dll
        75840000 4549bd53 Nov 02 09:41:39 2006 C:\Windows\System32\NETAPI32.dll
        75ce0000 4549bd99 Nov 02 09:42:49 2006 C:\Windows\system32\PSAPI.DLL
        737c0000 4549bdde Nov 02 09:43:58 2006 C:\Windows\System32\SPOOLSS.DLL
        74fe0000 46d779a1 Aug 31 03:14:57 2007 C:\Windows\System32\WTSAPI32.dll
        755b0000 4549bd3f Nov 02 09:41:19 2006 C:\Windows\System32\IPHLPAPI.DLL
        75570000 46807ea6 Jun 26 03:49:10 2007 C:\Windows\System32\dhcpcsvc.DLL
        75af0000 4549bcf1 Nov 02 09:40:01 2006 C:\Windows\System32\DNSAPI.dll
        75fe0000 4549be0e Nov 02 09:44:46 2006 C:\Windows\system32\WS2_32.dll
        77550000 4549bdc7 Nov 02 09:43:35 2006 C:\Windows\system32\NSI.dll
        75560000 4549be1e Nov 02 09:45:02 2006 C:\Windows\System32\WINNSI.DLL
        75540000 46807ea7 Jun 26 03:49:11 2007 C:\Windows\System32\dhcpcsvc6.DLL
```

```
        75250000 4549bd69 Nov 02 09:42:01 2006 C:\Windows\system32\mswsock.dll
        72a60000 4549bda2 Nov 02 09:42:58 2006 C:\Windows\System32\rasadhlp.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        773a0000 4549bce9 Nov 02 09:39:53 2006 C:\Windows\system32\CLBCatQ.DLL
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        74ff0000 4549be2f Nov 02 09:45:19 2006 C:\Windows\System32\WINTRUST.dll
        77580000 462434a3 Apr 17 03:44:51 2007 C:\Windows\system32\imagehlp.dll
        714e0000 46846bec Jun 29 03:18:20 2007 C:\Windows\System32\localspl.dll
        753f0000 4549bde4 Nov 02 09:44:04 2006 C:\Windows\System32\VERSION.dll
        71840000 4549bdb4 Nov 02 09:43:16 2006 C:\Windows\System32\sfc.dll
        763b0000 4549bdb9 Nov 02 09:43:21 2006 C:\Windows\system32\SHLWAPI.dll
        76560000 4681c95d Jun 27 03:20:13 2007 C:\Windows\system32\SHELL32.dll
        77030000 4549bdb0 Nov 02 09:43:12 2006 C:\Windows\system32\SETUPAPI.dll
        74aa0000 4549bd09 Nov 02 09:40:25 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_5d07289e07e1d100\comctl32.dll
        715a0000 4549be2a Nov 02 09:45:14 2006 C:\Windows\System32\winspool.drv
        71610000 453038aa Oct 14 02:08:58 2006 C:\Windows\System32\CNBLM3_2.DLL
        714b0000 4549bde2 Nov 02 09:44:02 2006 C:\Windows\System32\tcpmon.dll
        71ac0000 4549bdca Nov 02 09:43:38 2006 C:\Windows\System32\snmpapi.dll
        71830000 4549be31 Nov 02 09:45:21 2006 C:\Windows\System32\wsnmp32.dll
        73ad0000 46289734 Apr 20 11:34:28 2007 C:\Windows\System32\msxml6.dll
        71600000 4549bde1 Nov 02 09:44:01 2006 C:\Windows\System32\tcpmib.dll
        715f0000 4549bd10 Nov 02 09:40:32 2006 C:\Windows\System32\mgmtapi.dll
        71590000 4549bddd Nov 02 09:43:57 2006 C:\Windows\System32\usbmon.dll
        71420000 4549be46 Nov 02 09:45:42 2006 C:\Windows\system32\wls0wndh.dll
        713f0000 4549be17 Nov 02 09:44:55 2006 C:\Windows\System32\WSDMon.dll
        72c50000 4549be15 Nov 02 09:44:53 2006 C:\Windows\System32\wsdapi.dll
        72e40000 4549bcd7 Nov 02 09:39:35 2006 C:\Windows\System32\HTTPAPI.dll
        73420000 4549be18 Nov 02 09:44:56 2006 C:\Windows\System32\WINHTTP.dll
        73a70000 4549be05 Nov 02 09:44:37 2006 C:\Windows\System32\XmlLite.dll
        72a20000 4549bcda Nov 02 09:39:38 2006 C:\Windows\system32\FunDisc.dll
        74d00000 4549bcbc Nov 02 09:39:08 2006 C:\Windows\system32\ATL.DLL
        72460000 4666193b Jun 06 03:17:31 2007 C:\Windows\System32\msxml3.dll
        713b0000 451cd364 Sep 29 09:03:48 2006 C:\Windows\system32\spool\PRTPROCS\W32X86\CNBPP3.DLL
        75020000 4549bddb Nov 02 09:43:55 2006 C:\Windows\System32\NTMARTA.DLL
        76310000 4549be44 Nov 02 09:45:40 2006 C:\Windows\system32\WLDAP32.dll
        75ad0000 4549bda8 Nov 02 09:43:04 2006 C:\Windows\System32\SAMLIB.dll
        71340000 4549be09 Nov 02 09:44:41 2006 C:\Windows\System32\win32spl.dll
        71430000 4549bd65 Nov 02 09:41:57 2006 C:\Windows\System32\NETRAP.dll
        713d0000 4549bdd4 Nov 02 09:43:48 2006 C:\Windows\system32\printcom.dll
        713e0000 4549bdd6 Nov 02 09:43:50 2006 C:\Windows\system32\SensApi.dll
        75330000 4549bcd7 Nov 02 09:39:35 2006 C:\Windows\System32\GPAPI.dll
        71320000 4549bd2e Nov 02 09:41:02 2006 C:\Windows\System32\inetpp.dll
        752c0000 4549be27 Nov 02 09:45:11 2006 C:\Windows\System32\wshtcpip.dll
        752b0000 4549be21 Nov 02 09:45:05 2006 C:\Windows\System32\wship6.dll
        74d30000 4549bd6b Nov 02 09:42:03 2006 C:\Windows\system32\NLAapi.dll
        72f40000 4549be1f Nov 02 09:45:03 2006 C:\Windows\System32\winrnr.dll
        72f30000 4549bd3b Nov 02 09:41:15 2006 C:\Windows\system32\napinsp.dll
        72c10000 4549bdc0 Nov 02 09:43:28 2006 C:\Windows\system32\pnrpnsp.dll
        72c40000 4549be1d Nov 02 09:45:01 2006 C:\Windows\system32\wshbth.dll
        75300000 4549be2e Nov 02 09:45:18 2006 C:\Windows\System32\WINSTA.dll
        75350000 4549bdae Nov 02 09:43:10 2006 C:\Windows\System32\rsaenh.dll
    SubSystemData:     00000000
    ProcessHeap:       00360000
    ProcessParameters: 00360fd8
    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;C:\Program Files\QuickTime\QTSystem\'
    Environment:  003607e8
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\system32\config\systemprofile\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        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:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\TEMP
        TMP=C:\Windows\TEMP
        USERDOMAIN=WORKGROUP
        USERNAME=HOME$
        USERPROFILE=C:\Windows\system32\config\systemprofile
        windir=C:\Windows


        THREAD 9fd420b8  Cid 05e8.05ec  Teb: 7ffdf000 Win32Thread: 00000000 WAIT: (Executive)
UserMode Non-Alertable
            9fc416dc  NotificationEvent
        IRP List:
            9e1e2cc8: (0006,0094) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fd42790       Image:         spoolsv.exe
        Wait Start TickCount      9162           Ticks: 34337 (0:00:08:55.660)
        Context Switch Count      28
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address spoolsv!mainCRTStartup (0x00e09a45)
        Stack Init a0915000 Current a0914bc8 Base a0915000 Limit a0912000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a0914be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0914c1c 81c293a7 nt!KiSwapThread+0x389
        a0914c78 81d88faf nt!KeWaitForSingleObject+0x414
        a0914cac 81d93669 nt!IopSynchronousServiceTail+0x258
        a0914d38 81c8caaa nt!NtReadFile+0x646
        a0914d38 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0914d64)
        0022f7f0 77490080 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0022f7f4 75f3853f ntdll!ZwReadFile+0xc (FPO: [9,0,0])
        0022f86c 775cffe2 kernel32!ReadFile+0x20e (FPO: [Non-Fpo])
        0022f898 775cfdfb ADVAPI32!ScGetPipeInput+0x2a (FPO: [Non-Fpo])
        0022f900 775cbdd2 ADVAPI32!ScDispatcherLoop+0x6c (FPO: [Non-Fpo])
        0022fb78 00e08a3b ADVAPI32!StartServiceCtrlDispatcherW+0xce (FPO: [Non-Fpo])
        0022fb80 00e09b09 spoolsv!main+0x19 (FPO: [Non-Fpo])
        0022fbc4 75f33833 spoolsv!_initterm_e+0x163 (FPO: [Non-Fpo])
        0022fbd0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0022fc10 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fd424e8  Cid 05e8.05f0  Teb: 7ffde000 Win32Thread: ff4f83a0 WAIT: (UserRequest)
UserMode Non-Alertable
            8483b310  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fd42790       Image:         spoolsv.exe
        Wait Start TickCount      1161           Ticks: 42338 (0:00:11:00.477)
        Context Switch Count      54
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x775cb9d5)
        Stack Init a093d000 Current a093cc38 Base a093d000 Limit a093a000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a093cc50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a093cc8c 81c293a7 nt!KiSwapThread+0x389
        a093cce8 81df5057 nt!KeWaitForSingleObject+0x414
        a093cd50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a093cd50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a093cd64)
        0029faa4 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0029faa8 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0029fb18 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        0029fb2c 00e0958e kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0029fb40 775cb9f6 spoolsv!SPOOLER_main+0x45 (FPO: [Non-Fpo])
        0029fb54 75f33833 ADVAPI32!ScSvcctrlThreadA+0x21 (FPO: [Non-Fpo])
        0029fb60 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0029fba0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fd4c030  Cid 05e8.05f4  Teb: 7ffdd000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            9fc6a730  SynchronizationTimer
            9fd09668  SynchronizationEvent
            835aa528  SynchronizationEvent
            835ad608  SynchronizationEvent
            835b66e8  SynchronizationEvent
            835b65d8  SynchronizationEvent
            835b5708  SynchronizationEvent
            83533308  SynchronizationTimer
            835a9bd8  SynchronizationEvent
            835b1288  SynchronizationEvent
            835b1258  SynchronizationEvent
            835aa148  SynchronizationEvent
            835c9950  SynchronizationEvent
            835fb350  SynchronizationEvent
            835aa408  SynchronizationEvent
            835b92b8  SynchronizationTimer
            835a9920  SynchronizationEvent
            835ace88  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fd42790       Image:         spoolsv.exe
        Wait Start TickCount      16595          Ticks: 26904 (0:00:06:59.705)
        Context Switch Count      61
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x7744b49a)
        Stack Init a0292000 Current a02918d0 Base a0292000 Limit a028f000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a02918e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0291924 81c28c64 nt!KiSwapThread+0x389
        a0291970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a0291bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a0291d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a0291d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0291d64)
        0035fdb0 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0035fdb4 7744b65b ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0035ff50 75f33833 ntdll!TppWaiterpThread+0x294 (FPO: [Non-Fpo])
        0035ff5c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0035ff9c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fd4cc60  Cid 05e8.05fc  Teb: 7ffdb000 Win32Thread: ff50cbd8 WAIT: (UserRequest)
UserMode Non-Alertable
            9fd4e7e8  SynchronizationEvent
            835acd98  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fd42790       Image:         spoolsv.exe
        Wait Start TickCount      8892           Ticks: 34607 (0:00:08:59.872)
        Context Switch Count      267
        UserTime                  00:00:00.031
        KernelTime                00:00:00.202
        Win32 Start Address spoolsv!PreInitializeRouter (0x00e085bb)
        Stack Init a0867000 Current a08668d0 Base a0867000 Limit a0864000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a08668e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0866924 81c28c64 nt!KiSwapThread+0x389
        a0866970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a0866bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a0866d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a0866d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0866d64)
        0092fb74 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0092fb78 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0092fc14 761dc4b7 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0092fc68 761d8b83 USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
        0092fc84 737ccf34 USER32!MsgWaitForMultipleObjects+0x1f (FPO: [Non-Fpo])
        0092fcd4 737cbc5f SPOOLSS!HandlePollNotifications+0x38 (FPO: [Non-Fpo])
        0092fce8 00e085f8 SPOOLSS!InitializeRouter+0x1b3 (FPO: [Non-Fpo])
        0092fcf8 75f33833 spoolsv!PreInitializeRouter+0x3d (FPO: [Non-Fpo])
        0092fd04 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0092fd44 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 835b62a0  Cid 05e8.0a38  Teb: 7ffda000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            835b6548  NotificationEvent
            835b6328  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fd42790       Image:         spoolsv.exe
        Wait Start TickCount      43466          Ticks: 33 (0:00:00:00.514)
        Context Switch Count      555
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address msvcrt!_endthreadex (0x7628639b)
        Stack Init a3130000 Current a312fc38 Base a3130000 Limit a312d000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a312fc50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a312fc8c 81c293a7 nt!KiSwapThread+0x389
        a312fce8 81df5057 nt!KeWaitForSingleObject+0x414
        a312fd50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a312fd50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a312fd64)
        0141fa10 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0141fa14 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0141fa84 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        0141fa98 7183120b kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0141fac0 762862b6 wsnmp32!thrTimer+0x206 (FPO: [Non-Fpo])
        0141faf8 762863de msvcrt!_endthreadex+0x44 (FPO: [Non-Fpo])
        0141fb00 75f33833 msvcrt!_endthreadex+0xce (FPO: [Non-Fpo])
        0141fb0c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0141fb4c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 835ae030  Cid 05e8.0a3c  Teb: 7ffd8000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            835b61e8  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fd42790       Image:         spoolsv.exe
        Wait Start TickCount      8875           Ticks: 34624 (0:00:09:00.137)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address msvcrt!_endthreadex (0x7628639b)
        Stack Init a3134000 Current a3133c38 Base a3134000 Limit a3131000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a3133c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a3133c8c 81c293a7 nt!KiSwapThread+0x389
        a3133ce8 81df5057 nt!KeWaitForSingleObject+0x414
        a3133d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a3133d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a3133d64)
        0165f7d4 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0165f7d8 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0165f848 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        0165f85c 71832d2c kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0165f884 762862b6 wsnmp32!thrNotify+0x5d (FPO: [Non-Fpo])
        0165f8bc 762863de msvcrt!_endthreadex+0x44 (FPO: [Non-Fpo])
        0165f8c4 75f33833 msvcrt!_endthreadex+0xce (FPO: [Non-Fpo])
        0165f8d0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0165f910 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 835aed78  Cid 05e8.0a40  Teb: 7ffd7000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            835b6140  SynchronizationEvent
            835b6110  SynchronizationEvent
            835b60e0  NotificationEvent
            835aee00  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fd42790       Image:         spoolsv.exe
        Wait Start TickCount      8877           Ticks: 34622 (0:00:09:00.106)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address tcpmon!TBidiServer::PollingThread (0x714b1730)
        Stack Init a3138000 Current a31378d0 Base a3138000 Limit a3135000 Call 0
        Priority 7 BasePriority 6 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a31378e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a3137924 81c28c64 nt!KiSwapThread+0x389
        a3137970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a3137bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a3137d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a3137d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a3137d64)
        0178f970 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0178f974 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0178fa10 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0178fa2c 714b1828 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0178fa68 75f33833 tcpmon!TBidiServer::PollingThread+0xe7 (FPO: [Non-Fpo])
        0178fa74 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0178fab4 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 835b3030  Cid 05e8.0a44  Teb: 7ffd6000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            835ae430  SynchronizationEvent
            835b30b8  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fd42790       Image:         spoolsv.exe
        Wait Start TickCount      43493          Ticks: 6 (0:00:00:00.093)
        Context Switch Count      21
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address tcpmon!CDeviceStatus::StatusThread (0x714b1628)
        Stack Init a313c000 Current a313bc38 Base a313c000 Limit a3139000 Call 0
        Priority 7 BasePriority 6 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a313bc50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a313bc8c 81c293a7 nt!KiSwapThread+0x389
        a313bce8 81df5057 nt!KeWaitForSingleObject+0x414
        a313bd50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a313bd50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a313bd64)
        0171fe5c 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0171fe60 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0171fed0 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        0171fee4 714b165d kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0171fefc 75f33833 tcpmon!CDeviceStatus::StatusThread+0x2a (FPO: [Non-Fpo])
        0171ff08 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0171ff48 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 835b3a18  Cid 05e8.0a48  Teb: 7ffd5000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            835ae2d8  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fd42790       Image:         spoolsv.exe
        Wait Start TickCount      8877           Ticks: 34622 (0:00:09:00.106)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address msvcrt!_endthreadex (0x7628639b)
        Stack Init a09b5000 Current a09b4c38 Base a09b5000 Limit a09b2000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a09b4c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a09b4c8c 81c293a7 nt!KiSwapThread+0x389
        a09b4ce8 81df5057 nt!KeWaitForSingleObject+0x414
        a09b4d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a09b4d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a09b4d64)
        01b0f898 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01b0f89c 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        01b0f90c 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        01b0f920 71832d2c kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        01b0f948 762862b6 wsnmp32!thrNotify+0x5d (FPO: [Non-Fpo])
        01b0f980 762863de msvcrt!_endthreadex+0x44 (FPO: [Non-Fpo])
        01b0f988 75f33833 msvcrt!_endthreadex+0xce (FPO: [Non-Fpo])
        01b0f994 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01b0f9d4 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 835b3490  Cid 05e8.0a4c  Teb: 7ffd4000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            835b3880  SynchronizationEvent
            835b3738  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fd42790       Image:         spoolsv.exe
        Wait Start TickCount      8891           Ticks: 34608 (0:00:08:59.888)
        Context Switch Count      7
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address usbmon!UpdateThread (0x7159185c)
        Stack Init a1eca000 Current a1ec98d0 Base a1eca000 Limit a1ec7000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1ec98e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1ec9924 81c28c64 nt!KiSwapThread+0x389
        a1ec9970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1ec9bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1ec9d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1ec9d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1ec9d64)
        0098f990 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0098f994 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0098fa30 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0098fa4c 7159189d kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0098fa88 75f33833 usbmon!UpdateThread+0x4f (FPO: [Non-Fpo])
        0098fa94 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0098fad4 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 835b5d48  Cid 05e8.0a50  Teb: 7ffd3000 Win32Thread: ff529688 WAIT: (WrUserRequest)
UserMode Non-Alertable
            835ae858  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fd42790       Image:         spoolsv.exe
        Wait Start TickCount      8892           Ticks: 34607 (0:00:08:59.872)
        Context Switch Count      23
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address usbmon!CPNPNotifications::WindowMessageThread (0x71591211)
        Stack Init a1a9b000 Current a1a9ab68 Base a1a9b000 Limit a1a98000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1a9ab80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1a9abbc 81c293a7 nt!KiSwapThread+0x389
        a1a9ac18 8cedb8ed nt!KeWaitForSingleObject+0x414
        a1a9ac74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        a1a9ac90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        a1a9ace8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        a1a9ad4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        a1a9ad4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1a9ad64)
        01bdf8f4 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01bdf8f8 761e19cd USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        01bdf914 715912cc USER32!GetMessageW+0x33 (FPO: [Non-Fpo])
        01bdf978 75f33833 usbmon!CPNPNotifications::WindowMessageThread+0x11c (FPO: [Non-Fpo])
        01bdf984 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01bdf9c4 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 835b51c8  Cid 05e8.0a54  Teb: 7ffaf000 Win32Thread: ff526cc8 WAIT: (WrUserRequest)
UserMode Non-Alertable
            835b5110  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fd42790       Image:         spoolsv.exe
        Wait Start TickCount      8892           Ticks: 34607 (0:00:08:59.872)
        Context Switch Count      16
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address WSDMon!Ncd::TPower::WindowMessageThread (0x713f2a91)
        Stack Init a0909000 Current a0908b68 Base a0909000 Limit a0906000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a0908b80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0908bbc 81c293a7 nt!KiSwapThread+0x389
        a0908c18 8cedb8ed nt!KeWaitForSingleObject+0x414
        a0908c74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        a0908c90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        a0908ce8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        a0908d4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        a0908d4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0908d64)
        019ef98c 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        019ef990 761e19cd USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        019ef9ac 713f2b1a USER32!GetMessageW+0x33 (FPO: [Non-Fpo])
        019ef9ec 75f33833 WSDMon!Ncd::TPower::WindowMessageThread+0xa5 (FPO: [Non-Fpo])
        019ef9f8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        019efa38 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 835b9d78  Cid 05e8.0a58  Teb: 7ffae000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            835b9020  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fd42790       Image:         spoolsv.exe
        Wait Start TickCount      8882           Ticks: 34617 (0:00:09:00.028)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address FunDisc!CNotificationQueue::ThreadProc (0x72a2154d)
        Stack Init a1ece000 Current a1ecdc38 Base a1ece000 Limit a1ecb000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1ecdc50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1ecdc8c 81c293a7 nt!KiSwapThread+0x389
        a1ecdce8 81df5057 nt!KeWaitForSingleObject+0x414
        a1ecdd50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a1ecdd50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1ecdd64)
        01c1f8a0 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01c1f8a4 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        01c1f914 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        01c1f928 72a215ed kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        01c1f94c 75f33833 FunDisc!CNotificationQueue::ThreadProc+0x24f (FPO: [Non-Fpo])
        01c1f958 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01c1f998 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 835b9808  Cid 05e8.0a5c  Teb: 7ffad000 Win32Thread: ff4eeac8 WAIT: (UserRequest)
UserMode Non-Alertable
            835b9ab0  SynchronizationEvent
            835b9758  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fd42790       Image:         spoolsv.exe
        Wait Start TickCount      8882           Ticks: 34617 (0:00:09:00.028)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address FunDisc!ListenerThread (0x72a219c4)
        Stack Init a1b48000 Current a1b478d0 Base a1b48000 Limit a1b45000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1b478e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1b47924 81c28c64 nt!KiSwapThread+0x389
        a1b47970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1b47bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1b47d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1b47d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1b47d64)
        00defcfc 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00defd00 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00defd9c 761dc4b7 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        00defdf0 761d8b83 USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
        00defe0c 72a21ab2 USER32!MsgWaitForMultipleObjects+0x1f (FPO: [Non-Fpo])
        00defe88 75f33833 FunDisc!ListenerThread+0x12b (FPO: [Non-Fpo])
        00defe94 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00defed4 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 835b9420  Cid 05e8.0a60  Teb: 7ffac000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            835b96c8  SynchronizationEvent
            835b9370  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fd42790       Image:         spoolsv.exe
        Wait Start TickCount      8882           Ticks: 34617 (0:00:09:00.028)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address FunDisc!CRegProvider::ThreadProc (0x72a22cdd)
        Stack Init a0348000 Current a03478d0 Base a0348000 Limit a0345000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a03478e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0347924 81c28c64 nt!KiSwapThread+0x389
        a0347970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a0347bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a0347d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a0347d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0347d64)
        01a7f8b4 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01a7f8b8 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        01a7f954 72a22dce kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        01a7fdc0 72a22cea FunDisc!CRegProvider::MemberThreadProc+0x136 (FPO: [Non-Fpo])
        01a7fdc8 75f33833 FunDisc!CRegProvider::ThreadProc+0xd (FPO: [Non-Fpo])
        01a7fdd4 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01a7fe14 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 835b12f8  Cid 05e8.0a68  Teb: 7ffaa000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            835bb348  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fd42790       Image:         spoolsv.exe
        Wait Start TickCount      9162           Ticks: 34337 (0:00:08:55.660)
        Context Switch Count      7
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address localspl!SchedulerThread (0x714ee922)
        Stack Init 88e10000 Current 88e0fc38 Base 88e10000 Limit 88e0d000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        88e0fc50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        88e0fc8c 81c293a7 nt!KiSwapThread+0x389
        88e0fce8 81df5057 nt!KeWaitForSingleObject+0x414
        88e0fd50 81c8caaa nt!NtWaitForSingleObject+0xbe
        88e0fd50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 88e0fd64)
        01cffa40 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01cffa44 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        01cffab4 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        01cffac8 714ee96a kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        01cffaec 75f33833 localspl!SchedulerThread+0x8c (FPO: [Non-Fpo])
        01cffaf8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01cffb38 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 835c0148  Cid 05e8.0a7c  Teb: 7ffab000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            9fd423f8  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fd42790       Image:         spoolsv.exe
        Wait Start TickCount      36601          Ticks: 6898 (0:00:01:47.609)
        Context Switch Count      28
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init a3140000 Current a313fbc8 Base a3140000 Limit a313d000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a313fbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a313fc1c 81cad431 nt!KiSwapThread+0x389
        a313fc6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a313fcc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a313fd48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a313fd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a313fd64)
        01c6fcf8 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01c6fcfc 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        01c6fd28 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        01c6fd64 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        01c6fdd0 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        01c6fddc 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        01c6fe00 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        01c6fe0c 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        01c6fe18 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01c6fe58 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Svchost process (LocalServiceNoNetwork)

```
PROCESS 9fd50418  SessionId: 0  Cid: 0600    Peb: 7ffd7000  ParentCid: 0214
    DirBase: 29a012a0  ObjectTable: a01e7b60  HandleCount: 296.
    Image: svchost.exe
    VadRoot 9fd81450 Vads 163 Clone 0 Private 3144. Modified 3419. Locked 0.
    DeviceMap a00699b8
    Token                             a01ed5f0
    ElapsedTime                       00:11:01.408
    UserTime                          00:00:00.202
    KernelTime                        00:00:00.218
    QuotaPoolUsage[PagedPool]         94656
    QuotaPoolUsage[NonPagedPool]      24640
    Working Set Sizes (now,min,max)  (2010, 50, 345) (8040KB, 200KB, 1380KB)
    PeakWorkingSetSize                11760
    VirtualSize                       77 Mb
    PeakVirtualSize                   111 Mb
    PageFaultCount                    28402
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      3971

    Setting context for this process...
.process /p /r ffffffff9fd50418

    !peb
PEB at 7ffd7000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00dd0000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 000c17d0 . 015d00d0
    Ldr.InLoadOrderModuleList:           000c1750 . 015d0130
    Ldr.InMemoryOrderModuleList:         000c1758 . 015d0138
            Base TimeStamp                     Module
          dd0000 4549adc4 Nov 02 08:35:16 2006 C:\Windows\system32\svchost.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        73640000 4549bcbc Nov 02 09:39:08 2006 c:\windows\system32\bfe.dll
        757b0000 4549bccf Nov 02 09:39:27 2006 c:\windows\system32\AUTHZ.dll
        75b80000 4549bdd2 Nov 02 09:43:46 2006 c:\windows\system32\Secur32.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        733a0000 46677f80 Jun 07 04:46:08 2007 c:\windows\system32\mpssvc.dll
        74f30000 46677f3a Jun 07 04:44:58 2007 c:\windows\system32\FirewallAPI.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        753f0000 4549bde4 Nov 02 09:44:04 2006 c:\windows\system32\VERSION.dll
        74d30000 4549bd6b Nov 02 09:42:03 2006 c:\windows\system32\nlaapi.dll
        755b0000 4549bd3f Nov 02 09:41:19 2006 c:\windows\system32\IPHLPAPI.DLL
        75570000 46807ea6 Jun 26 03:49:10 2007 c:\windows\system32\dhcpcsvc.DLL
        75af0000 4549bcf1 Nov 02 09:40:01 2006 c:\windows\system32\DNSAPI.dll
        75fe0000 4549be0e Nov 02 09:44:46 2006 C:\Windows\system32\WS2_32.dll
        77550000 4549bdc7 Nov 02 09:43:35 2006 C:\Windows\system32\NSI.dll
        75560000 4549be1e Nov 02 09:45:02 2006 c:\windows\system32\WINNSI.DLL
        75540000 46807ea7 Jun 26 03:49:11 2007 c:\windows\system32\dhcpcsvc6.DLL
        75650000 45b96fde Jan 26 03:05:02 2007 c:\windows\system32\CRYPT32.dll
        75820000 4549bd41 Nov 02 09:41:21 2006 c:\windows\system32\MSASN1.dll
```

```
        75ba0000 4549bde2 Nov 02 09:44:02 2006 c:\windows\system32\USERENV.dll
        754a0000 4549bcb9 Nov 02 09:39:05 2006 c:\windows\system32\bcrypt.dll
        74fe0000 46d779a1 Aug 31 03:14:57 2007 c:\windows\system32\WTSAPI32.dll
        763b0000 4549bdb9 Nov 02 09:43:21 2006 C:\Windows\system32\SHLWAPI.dll
        735b0000 4549bce0 Nov 02 09:39:44 2006 c:\windows\system32\fwpuclnt.dll
        74aa0000 4549bd09 Nov 02 09:40:25 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_5d07289e07e1d100\comctl32.dll
        75480000 4549bd20 Nov 02 09:40:48 2006 C:\Windows\system32\credssp.dll
        75050000 46773a78 Jun 19 03:07:52 2007 C:\Windows\system32\schannel.dll
        75840000 4549bd53 Nov 02 09:41:39 2006 C:\Windows\system32\NETAPI32.dll
        75ce0000 4549bd99 Nov 02 09:42:49 2006 C:\Windows\system32\PSAPI.DLL
        75330000 4549bcd7 Nov 02 09:39:35 2006 C:\Windows\system32\GPAPI.dll
        75610000 4679de70 Jun 21 03:12:00 2007 C:\Windows\system32\slc.dll
        73410000 46677fd3 Jun 07 04:47:31 2007 C:\Windows\system32\wfapigp.dll
        72ed0000 46846bed Jun 29 03:18:21 2007 c:\windows\system32\dps.dll
        72e70000 4549bde1 Nov 02 09:44:01 2006 c:\windows\system32\wdi.dll
        773a0000 4549bce9 Nov 02 09:39:53 2006 C:\Windows\system32\CLBCatQ.DLL
        72ab0000 4549bdda Nov 02 09:43:54 2006 C:\Windows\system32\taskschd.dll
        73a70000 4549be05 Nov 02 09:44:37 2006 C:\Windows\system32\XmlLite.dll
        726c0000 4549bcd1 Nov 02 09:39:29 2006 C:\Windows\system32\diagperf.dll
        76560000 4681c95d Jun 27 03:20:13 2007 C:\Windows\system32\SHELL32.dll
        72a10000 4549bdbc Nov 02 09:43:24 2006 C:\Windows\system32\pnpts.dll
        75250000 4549bd69 Nov 02 09:42:01 2006 C:\Windows\system32\mswsock.dll
        752c0000 4549be27 Nov 02 09:45:11 2006 C:\Windows\System32\wshtcpip.dll
        752b0000 4549be21 Nov 02 09:45:05 2006 C:\Windows\System32\wship6.dll
        75350000 4549bdae Nov 02 09:43:10 2006 C:\Windows\system32\rsaenh.dll
        720c0000 4549bdc3 Nov 02 09:43:31 2006 C:\Windows\System32\npmproxy.dll
        77030000 4549bdb0 Nov 02 09:43:12 2006 C:\Windows\system32\SETUPAPI.dll
        74ff0000 4549be2f Nov 02 09:45:19 2006 C:\Windows\system32\WINTRUST.dll
        77580000 462434a3 Apr 17 03:44:51 2007 C:\Windows\system32\imagehlp.dll
    SubSystemData:     00000000
    ProcessHeap:       000c0000
    ProcessParameters: 000c1068
    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;C:\Program Files\QuickTime\QTSystem\'
    Environment:  000c07e8
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\ServiceProfiles\LocalService\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        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;C:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        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 9fd50030  Cid 0600.0604  Teb: 7ffdf000 Win32Thread: 00000000 WAIT: (Executive)
UserMode Non-Alertable
            9fd3d084  NotificationEvent
        IRP List:
            9fc4dec0: (0006,0094) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fd50418       Image:         svchost.exe
        Wait Start TickCount      9758           Ticks: 33741 (0:00:08:46.362)
        Context Switch Count      25
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address svchost!wmainCRTStartup (0x00dd20bf)
        Stack Init a086b000 Current a086abc8 Base a086b000 Limit a0868000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a086abe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a086ac1c 81c293a7 nt!KiSwapThread+0x389
        a086ac78 81d88faf nt!KeWaitForSingleObject+0x414
        a086acac 81d93669 nt!IopSynchronousServiceTail+0x258
        a086ad38 81c8caaa nt!NtReadFile+0x646
        a086ad38 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a086ad64)
        0008f514 77490080 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0008f518 75f3853f ntdll!ZwReadFile+0xc (FPO: [9,0,0])
        0008f590 775cffe2 kernel32!ReadFile+0x20e (FPO: [Non-Fpo])
        0008f5bc 775cfdfb ADVAPI32!ScGetPipeInput+0x2a (FPO: [Non-Fpo])
        0008f624 775cbdd2 ADVAPI32!ScDispatcherLoop+0x6c (FPO: [Non-Fpo])
        0008f89c 00dd241d ADVAPI32!StartServiceCtrlDispatcherW+0xce (FPO: [Non-Fpo])
        0008f8a4 00dd2401 svchost!SvcHostMain+0x12 (FPO: [Non-Fpo])
        0008f8a8 00dd2183 svchost!wmain+0x5 (FPO: [Non-Fpo])
        0008f8ec 75f33833 svchost!_initterm_e+0x163 (FPO: [Non-Fpo])
        0008f8f8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0008f938 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fd452c0  Cid 0600.060c  Teb: 7ffdd000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            9fd45568  SynchronizationTimer
            9fd440b0  SynchronizationTimer
            9fd3d7c8  SynchronizationEvent
            9fd46d50  SynchronizationEvent
            9fd44cf0  SynchronizationEvent
            9fd9dfb8  SynchronizationEvent
            9fd89cb0  SynchronizationEvent
            9fd926f0  SynchronizationEvent
            9fd86258  SynchronizationEvent
            9fda1380  SynchronizationEvent
            8995e4a0  ProcessObject
            9fd46d20  SynchronizationEvent
            a1818a10  SynchronizationTimer
            a1818958  SynchronizationTimer
            9fd96140  SynchronizationEvent
            9fd90ca0  SynchronizationEvent
            9fd8ddb8  SynchronizationEvent
            9fd9ae90  SynchronizationEvent
            9fd43020  SynchronizationTimer
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fd50418       Image:         svchost.exe
        Wait Start TickCount      15054          Ticks: 28445 (0:00:07:23.744)
        Context Switch Count      46
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x7744b49a)
        Stack Init a0873000 Current a08728d0 Base a0873000 Limit a0870000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a08728e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0872924 81c28c64 nt!KiSwapThread+0x389
        a0872970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a0872bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a0872d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a0872d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0872d64)
        006cf6a4 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        006cf6a8 7744b65b ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        006cf844 75f33833 ntdll!TppWaiterpThread+0x294 (FPO: [Non-Fpo])
        006cf850 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        006cf890 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fd46030  Cid 0600.0610  Teb: 7ffdc000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fd43148  NotificationEvent
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fd50418       Image:         svchost.exe
        Wait Start TickCount      1162           Ticks: 42337 (0:00:11:00.461)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address AUTHZ!AuthzpDeQueueThreadWorker (0x757b68c9)
        Stack Init a0877000 Current a0876c38 Base a0877000 Limit a0874000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a0876c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0876c8c 81c293a7 nt!KiSwapThread+0x389
        a0876ce8 81df5057 nt!KeWaitForSingleObject+0x414
        a0876d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a0876d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0876d64)
        009ef9f8 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        009ef9fc 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        009efa6c 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        009efa80 757b68ef kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        009efa9c 75f33833 AUTHZ!AuthzpDeQueueThreadWorker+0xa2 (FPO: [Non-Fpo])
        009efaa8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        009efae8 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fd7e030  Cid 0600.062c  Teb: 7ffd9000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fd6c3e0  NotificationEvent
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fd50418       Image:         svchost.exe
        Wait Start TickCount      1174           Ticks: 42325 (0:00:11:00.274)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address AUTHZ!AuthzpDeQueueThreadWorker (0x757b68c9)
        Stack Init a0893000 Current a0892c38 Base a0893000 Limit a0890000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a0892c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0892c8c 81c293a7 nt!KiSwapThread+0x389
        a0892ce8 81df5057 nt!KeWaitForSingleObject+0x414
        a0892d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a0892d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0892d64)
        00cafaa8 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00cafaac 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        00cafb1c 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        00cafb30 757b68ef kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        00cafb4c 75f33833 AUTHZ!AuthzpDeQueueThreadWorker+0xa2 (FPO: [Non-Fpo])
        00cafb58 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00cafb98 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fd22d78  Cid 0600.066c  Teb: 7ffd8000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fd8c200  NotificationEvent
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fd50418       Image:         svchost.exe
        Wait Start TickCount      1883           Ticks: 41616 (0:00:10:49.213)
        Context Switch Count      67
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address AUTHZ!AuthzpDeQueueThreadWorker (0x757b68c9)
        Stack Init a083c000 Current a083bc38 Base a083c000 Limit a0839000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a083bc50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a083bc8c 81c293a7 nt!KiSwapThread+0x389
        a083bce8 81df5057 nt!KeWaitForSingleObject+0x414
        a083bd50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a083bd50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a083bd64)
        013cfc48 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        013cfc4c 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        013cfcbc 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        013cfcd0 757b68ef kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        013cfcec 75f33833 AUTHZ!AuthzpDeQueueThreadWorker+0xa2 (FPO: [Non-Fpo])
        013cfcf8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        013cfd38 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fd86338  Cid 0600.0678  Teb: 7ffde000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fd847a8  NotificationEvent
            9fd84688  NotificationEvent
            9fd86e48  NotificationEvent
            9fd85b78  NotificationEvent
            9fd6f240  SynchronizationEvent
        IRP List:
            89880698: (0006,0094) Flags: 00060070  Mdl: 00000000
            a18aa6b0: (0006,0094) Flags: 00060070  Mdl: 00000000
            9fd24f68: (0006,0094) Flags: 00060070  Mdl: 00000000
            9fd6fcb8: (0006,0094) Flags: 00060070  Mdl: 00000000
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fd50418       Image:         svchost.exe
        Wait Start TickCount      9808           Ticks: 33691 (0:00:08:45.582)
        Context Switch Count      66
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address mpssvc!FwUpcall2ndPhaseShutdown (0x733a4a62)
        Stack Init a081c000 Current a081b8d0 Base a081c000 Limit a0819000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a081b8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a081b924 81c28c64 nt!KiSwapThread+0x389
        a081b970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a081bbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a081bd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a081bd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a081bd64)
        011af778 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        011af77c 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        011af818 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        011af834 733a4b8f kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        011af8a0 75f33833 mpssvc!FwUpcall2ndPhaseShutdown+0x269 (FPO: [Non-Fpo])
        011af8ac 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        011af8ec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fd94030  Cid 0600.0684  Teb: 7ffd4000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            9fd85e10  NotificationEvent
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fd50418       Image:         svchost.exe
        Wait Start TickCount      1818           Ticks: 41681 (0:00:10:50.227)
        Context Switch Count      103
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address mpssvc!Nla::CNlaServiceState::WaitForNotifications (0x733bc7b7)
        Stack Init a0814000 Current a0813c38 Base a0814000 Limit a0811000 Call 0
        Priority 13 BasePriority 8 PriorityDecrement 4 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a0813c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0813c8c 81c293a7 nt!KiSwapThread+0x389
        a0813ce8 81df5057 nt!KeWaitForSingleObject+0x414
        a0813d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a0813d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0813d64)
        0095fc58 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0095fc5c 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0095fccc 733b66f6 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        0095fce8 733bc7da mpssvc!Nla::CNlaServiceState::WaitForNotifications+0x80 (FPO: [Non-Fpo])
        0095fcf0 75f33833 mpssvc!Nla::CNlaServiceState::WaitForNotifications+0x33 (FPO: [Non-Fpo])
        0095fcfc 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0095fd3c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fd9a328  Cid 0600.0694  Teb: 7ffd3000 Win32Thread: ff4fc2d8 WAIT: (UserRequest)
UserMode Alertable
            9fd24140  SynchronizationEvent
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fd50418       Image:         svchost.exe
        Wait Start TickCount      1863           Ticks: 41636 (0:00:10:49.525)
        Context Switch Count      132
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address mpssvc!FwDynDataNotifySinkProc (0x733b3b0d)
        Stack Init a0991000 Current a0990c38 Base a0991000 Limit a098e000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a0990c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0990c8c 81c293a7 nt!KiSwapThread+0x389
        a0990ce8 81df5057 nt!KeWaitForSingleObject+0x414
        a0990d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a0990d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0990d64)
        00d3f980 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00d3f984 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        00d3f9f4 733b3ca8 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        00d3fa70 75f33833 mpssvc!FwDynDataNotifySinkProc+0x35a (FPO: [Non-Fpo])
        00d3fa7c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00d3fabc 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fd9b138  Cid 0600.06a0  Teb: 7ffaf000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Alertable
            9fd8d1b8  QueueObject
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fd50418       Image:         svchost.exe
        Wait Start TickCount      1227           Ticks: 42272 (0:00:10:59.447)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init a1b9c000 Current a1b9bbc8 Base a1b9c000 Limit a1b99000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1b9bbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1b9bc1c 81cad431 nt!KiSwapThread+0x389
        a1b9bc68 81d8b982 nt!KeRemoveQueueEx+0x568
        a1b9bcc0 81c7a036 nt!IoRemoveIoCompletion+0x23
        a1b9bd54 81c8caaa nt!NtWaitForWorkViaWorkerFactory+0x1a1
        a1b9bd54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1b9bd64)
        0149fb48 77490850 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0149fb4c 7749a1b4 ntdll!NtWaitForWorkViaWorkerFactory+0xc (FPO: [2,0,0])
        0149fc74 75f33833 ntdll!TppWorkerThread+0x1f6 (FPO: [Non-Fpo])
        0149fc80 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0149fcc0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 89872030  Cid 0600.0744  Teb: 7ffd6000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fde7430  NotificationEvent
        IRP List:
            9fd8d228: (0006,0094) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fd50418       Image:         svchost.exe
        Wait Start TickCount      40408          Ticks: 3091 (0:00:00:48.219)
        Context Switch Count      186
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x775cb9d5)
        Stack Init a1b90000 Current a1b8fc38 Base a1b90000 Limit a1b8d000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a1b8fc50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1b8fc8c 81c293a7 nt!KiSwapThread+0x389
        a1b8fce8 81df5057 nt!KeWaitForSingleObject+0x414
        a1b8fd50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a1b8fd50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1b8fd64)
        0145f93c 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0145f940 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0145f9b0 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        0145f9c4 775d126c kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0145fa04 775c0a06 ADVAPI32!EtwpProcessRealTimeTraces+0x9e (FPO: [Non-Fpo])
        0145fd4c 72ed8590 ADVAPI32!ProcessTrace+0x30a (FPO: [Non-Fpo])
        0145ff10 72ed84ac dps!DpsRun+0xb8 (FPO: [Non-Fpo])
        0145ff24 00dd148a dps!ServiceMain+0x183 (FPO: [Non-Fpo])
        0145ff50 775cb9f6 svchost!ServiceStarter+0x17a (FPO: [Non-Fpo])
        0145ff64 75f33833 ADVAPI32!ScSvcctrlThreadA+0x21 (FPO: [Non-Fpo])
        0145ff70 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0145ffb0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fde0498  Cid 0600.0794  Teb: 7ffad000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fde92a8  NotificationEvent
            9fde9278  SynchronizationEvent
            9fde9248  NotificationEvent
            9fde0520  NotificationTimer
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fd50418       Image:         svchost.exe
        Wait Start TickCount      40275          Ticks: 3224 (0:00:00:50.294)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address dps!DpspBackgroundControl (0x72ed3405)
        Stack Init a1ae1000 Current a1ae08d0 Base a1ae1000 Limit a1ade000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a1ae08e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1ae0924 81c28c64 nt!KiSwapThread+0x389
        a1ae0970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1ae0bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1ae0d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1ae0d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1ae0d64)
        0140fc34 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0140fc38 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0140fcd4 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0140fcf0 72ed34c1 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0140fd3c 75f33833 dps!DpspBackgroundControl+0x303 (FPO: [Non-Fpo])
        0140fd48 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0140fd88 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fde2c50  Cid 0600.0798  Teb: 7ffac000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            847fd160  Semaphore Limit 0x7fffffff
            9fde92a8  NotificationEvent
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fd50418       Image:         svchost.exe
        Wait Start TickCount      40344          Ticks: 3155 (0:00:00:49.218)
        Context Switch Count      47
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address dps!DpspSetThreadToken (0x72ed13cb)
        Stack Init a087b000 Current a087a8d0 Base a087b000 Limit a0878000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a087a8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a087a924 81c28c64 nt!KiSwapThread+0x389
        a087a970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a087abfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a087ad48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a087ad48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a087ad64)
        0171fe28 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0171fe2c 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0171fec8 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0171fee4 72ed1484 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0171ff34 75f33833 dps!DpspSetThreadToken+0x557 (FPO: [Non-Fpo])
        0171ff40 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0171ff80 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fde12f0  Cid 0600.079c  Teb: 7ffab000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            847fd160  Semaphore Limit 0x7fffffff
            9fde92a8  NotificationEvent
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fd50418       Image:         svchost.exe
        Wait Start TickCount      40344          Ticks: 3155 (0:00:00:49.218)
        Context Switch Count      35
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address dps!DpspSetThreadToken (0x72ed13cb)
        Stack Init a1b7c000 Current a1b7b8d0 Base a1b7c000 Limit a1b79000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a1b7b8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1b7b924 81c28c64 nt!KiSwapThread+0x389
        a1b7b970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1b7bbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1b7bd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1b7bd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1b7bd64)
        0152fcf4 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0152fcf8 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0152fd94 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0152fdb0 72ed1484 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0152fe00 75f33833 dps!DpspSetThreadToken+0x557 (FPO: [Non-Fpo])
        0152fe0c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0152fe4c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fde2490  Cid 0600.07a0  Teb: 7ffaa000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            847fd160  Semaphore Limit 0x7fffffff
            9fde92a8  NotificationEvent
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fd50418       Image:         svchost.exe
        Wait Start TickCount      40344          Ticks: 3155 (0:00:00:49.218)
        Context Switch Count      59
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address dps!DpspSetThreadToken (0x72ed13cb)
        Stack Init a1b74000 Current a1b738d0 Base a1b74000 Limit a1b71000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a1b738e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1b73924 81c28c64 nt!KiSwapThread+0x389
        a1b73970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1b73bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1b73d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1b73d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1b73d64)
        017dfdb0 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        017dfdb4 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        017dfe50 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        017dfe6c 72ed1484 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        017dfebc 75f33833 dps!DpspSetThreadToken+0x557 (FPO: [Non-Fpo])
        017dfec8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        017dff08 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fde7030  Cid 0600.07a4  Teb: 7ffa9000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            847fd160  Semaphore Limit 0x7fffffff
            9fde92a8  NotificationEvent
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fd50418       Image:         svchost.exe
        Wait Start TickCount      18676          Ticks: 24823 (0:00:06:27.241)
        Context Switch Count      42
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address dps!DpspSetThreadToken (0x72ed13cb)
        Stack Init a1b88000 Current a1b878d0 Base a1b88000 Limit a1b85000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1b878e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1b87924 81c28c64 nt!KiSwapThread+0x389
        a1b87970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1b87bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1b87d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1b87d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1b87d64)
        009afe34 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        009afe38 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        009afed4 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        009afef0 72ed1484 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        009aff40 75f33833 dps!DpspSetThreadToken+0x557 (FPO: [Non-Fpo])
        009aff4c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        009aff8c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fde7d78  Cid 0600.07a8  Teb: 7ffa8000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            847fd160  Semaphore Limit 0x7fffffff
            9fde92a8  NotificationEvent
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fd50418       Image:         svchost.exe
        Wait Start TickCount      40344          Ticks: 3155 (0:00:00:49.218)
        Context Switch Count      48
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address dps!DpspSetThreadToken (0x72ed13cb)
        Stack Init a1b58000 Current a1b578d0 Base a1b58000 Limit a1b55000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a1b578e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1b57924 81c28c64 nt!KiSwapThread+0x389
        a1b57970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1b57bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1b57d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1b57d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1b57d64)
        016bf6c0 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        016bf6c4 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        016bf760 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        016bf77c 72ed1484 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        016bf7cc 75f33833 dps!DpspSetThreadToken+0x557 (FPO: [Non-Fpo])
        016bf7d8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        016bf818 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fde7ac0  Cid 0600.07ac  Teb: 7ffa7000 Win32Thread: ff51ee98 WAIT: (UserRequest)
UserMode Non-Alertable
            898557b0  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fd50418       Image:         svchost.exe
        Wait Start TickCount      12650          Ticks: 30849 (0:00:08:01.247)
        Context Switch Count      111
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address dps!WdipLaunchLocalHost (0x72ed5a43)
        Stack Init a09b9000 Current a09b88d0 Base a09b9000 Limit a09b6000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a09b88e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a09b8924 81c28c64 nt!KiSwapThread+0x389
        a09b8970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a09b8bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a09b8d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a09b8d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a09b8d64)
        018bfc94 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        018bfc98 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        018bfd34 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        018bfd50 72e72ffd kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        018bfda0 72e731e2 wdi!WdipHostListener+0xbd (FPO: [Non-Fpo])
        018bfdc8 72e73240 wdi!WdipTriggerHost+0x179 (FPO: [Non-Fpo])
        018bfddc 75f33833 wdi!WdipLaunchLocalHost+0x1c (FPO: [Non-Fpo])
        018bfde8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        018bfe28 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fdff928  Cid 0600.07b4  Teb: 7ffa6000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            89990a40  QueueObject
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fd50418       Image:         svchost.exe
        Wait Start TickCount      1812           Ticks: 41687 (0:00:10:50.321)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdi!WdipSessionListener (0x72e71277)
        Stack Init a1af9000 Current a1af8bc8 Base a1af9000 Limit a1af6000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1af8be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1af8c1c 81cad431 nt!KiSwapThread+0x389
        a1af8c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a1af8cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a1af8d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a1af8d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1af8d64)
        00bcfefc 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00bcff00 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        00bcff2c 72e712f3 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        00bcff80 75f33833 wdi!WdipSessionListener+0xaa (FPO: [Non-Fpo])
        00bcff8c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00bcffcc 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fdff670  Cid 0600.07b8  Teb: 7ffa5000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            89990a40  QueueObject
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fd50418       Image:         svchost.exe
        Wait Start TickCount      1816           Ticks: 41683 (0:00:10:50.258)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdi!WdipSessionListener (0x72e71277)
        Stack Init a1b80000 Current a1b7fbc8 Base a1b80000 Limit a1b7d000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1b7fbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1b7fc1c 81cad431 nt!KiSwapThread+0x389
        a1b7fc6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a1b7fcc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a1b7fd48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a1b7fd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1b7fd64)
        01bafa94 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01bafa98 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        01bafac4 72e712f3 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        01bafb18 75f33833 wdi!WdipSessionListener+0xaa (FPO: [Non-Fpo])
        01bafb24 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01bafb64 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fdff3b8  Cid 0600.07bc  Teb: 7ffa4000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            89990a40  QueueObject
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fd50418       Image:         svchost.exe
        Wait Start TickCount      1812           Ticks: 41687 (0:00:10:50.321)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdi!WdipSessionListener (0x72e71277)
        Stack Init a1a73000 Current a1a72bc8 Base a1a73000 Limit a1a70000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1a72be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1a72c1c 81cad431 nt!KiSwapThread+0x389
        a1a72c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a1a72cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a1a72d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a1a72d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1a72d64)
        01bffc68 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01bffc6c 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        01bffc98 72e712f3 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        01bffcec 75f33833 wdi!WdipSessionListener+0xaa (FPO: [Non-Fpo])
        01bffcf8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01bffd38 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fdff100  Cid 0600.07c0  Teb: 7ffa3000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            89990a40  QueueObject
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fd50418       Image:         svchost.exe
        Wait Start TickCount      1816           Ticks: 41683 (0:00:10:50.258)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdi!WdipSessionListener (0x72e71277)
        Stack Init a1a77000 Current a1a76bc8 Base a1a77000 Limit a1a74000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1a76be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1a76c1c 81cad431 nt!KiSwapThread+0x389
        a1a76c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a1a76cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a1a76d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a1a76d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1a76d64)
        011efd54 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        011efd58 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        011efd84 72e712f3 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        011efdd8 75f33833 wdi!WdipSessionListener+0xaa (FPO: [Non-Fpo])
        011efde4 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        011efe24 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD a189b030  Cid 0600.07c4  Teb: 7ffa2000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            89990a40  QueueObject
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fd50418       Image:         svchost.exe
        Wait Start TickCount      1812           Ticks: 41687 (0:00:10:50.321)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdi!WdipSessionListener (0x72e71277)
        Stack Init a1a7b000 Current a1a7abc8 Base a1a7b000 Limit a1a78000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1a7abe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1a7ac1c 81cad431 nt!KiSwapThread+0x389
        a1a7ac6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a1a7acc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a1a7ad48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a1a7ad48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1a7ad64)
        01c5f9c4 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01c5f9c8 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        01c5f9f4 72e712f3 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        01c5fa48 75f33833 wdi!WdipSessionListener+0xaa (FPO: [Non-Fpo])
        01c5fa54 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01c5fa94 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD a189b440  Cid 0600.07d0  Teb: 7ffa1000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            89990a40  QueueObject
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fd50418       Image:         svchost.exe
        Wait Start TickCount      15313          Ticks: 28186 (0:00:07:19.704)
        Context Switch Count      749
        UserTime                  00:00:01.029
        KernelTime                00:00:00.218
        Win32 Start Address wdi!WdipSessionListener (0x72e71277)
        Stack Init a1a87000 Current a1a86bc8 Base a1a87000 Limit a1a84000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1a86be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1a86c1c 81cad431 nt!KiSwapThread+0x389
        a1a86c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a1a86cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a1a86d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a1a86d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1a86d64)
        0182f784 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0182f788 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        0182f7b4 72e712f3 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        0182f808 75f33833 wdi!WdipSessionListener+0xaa (FPO: [Non-Fpo])
        0182f814 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0182f854 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fdec030  Cid 0600.07d4  Teb: 7ffa0000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            89990a40  QueueObject
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fd50418       Image:         svchost.exe
        Wait Start TickCount      1812           Ticks: 41687 (0:00:10:50.321)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdi!WdipSessionListener (0x72e71277)
        Stack Init a1a8b000 Current a1a8abc8 Base a1a8b000 Limit a1a88000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1a8abe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1a8ac1c 81cad431 nt!KiSwapThread+0x389
        a1a8ac6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a1a8acc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a1a8ad48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a1a8ad48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1a8ad64)
        0177fcd0 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0177fcd4 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        0177fd00 72e712f3 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        0177fd54 75f33833 wdi!WdipSessionListener+0xaa (FPO: [Non-Fpo])
        0177fd60 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0177fda0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fdecd48  Cid 0600.07d8  Teb: 7ff9f000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            89990a40  QueueObject
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fd50418       Image:         svchost.exe
        Wait Start TickCount      15186          Ticks: 28313 (0:00:07:21.685)
        Context Switch Count      44
        UserTime                  00:00:00.109
        KernelTime                00:00:00.046
        Win32 Start Address wdi!WdipSessionListener (0x72e71277)
        Stack Init a1a8f000 Current a1a8ebc8 Base a1a8f000 Limit a1a8c000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1a8ebe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1a8ec1c 81cad431 nt!KiSwapThread+0x389
        a1a8ec6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a1a8ecc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a1a8ed48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a1a8ed48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1a8ed64)
        01d8fc14 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01d8fc18 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        01d8fc44 72e712f3 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        01d8fc98 75f33833 wdi!WdipSessionListener+0xaa (FPO: [Non-Fpo])
        01d8fca4 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01d8fce4 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fdeca90  Cid 0600.07dc  Teb: 7ff9e000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            89990a40  QueueObject
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fd50418       Image:         svchost.exe
        Wait Start TickCount      1812           Ticks: 41687 (0:00:10:50.321)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdi!WdipSessionListener (0x72e71277)
        Stack Init a1a93000 Current a1a92bc8 Base a1a93000 Limit a1a90000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1a92be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1a92c1c 81cad431 nt!KiSwapThread+0x389
        a1a92c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a1a92cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a1a92d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a1a92d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1a92d64)
        01b0f8b4 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01b0f8b8 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        01b0f8e4 72e712f3 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        01b0f938 75f33833 wdi!WdipSessionListener+0xaa (FPO: [Non-Fpo])
        01b0f944 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01b0f984 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fdec7d8  Cid 0600.07e0  Teb: 7ff9d000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            89990a40  QueueObject
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fd50418       Image:         svchost.exe
        Wait Start TickCount      14894          Ticks: 28605 (0:00:07:26.240)
        Context Switch Count      137
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address wdi!WdipSessionListener (0x72e71277)
        Stack Init a1a97000 Current a1a96bc8 Base a1a97000 Limit a1a94000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1a96be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1a96c1c 81cad431 nt!KiSwapThread+0x389
        a1a96c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a1a96cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a1a96d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a1a96d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1a96d64)
        01c9fa68 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01c9fa6c 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        01c9fa98 72e712f3 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        01c9faec 75f33833 wdi!WdipSessionListener+0xaa (FPO: [Non-Fpo])
        01c9faf8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01c9fb38 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 83890138  Cid 0600.075c  Teb: 7ffda000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            9fd43b18  QueueObject
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            9fd50418       Image:         svchost.exe
        Wait Start TickCount      34475          Ticks: 9024 (0:00:02:20.775)
        Context Switch Count      48
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init 9f7e8000 Current 9f7e7bc8 Base 9f7e8000 Limit 9f7e5000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f7e7be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f7e7c1c 81cad431 nt!KiSwapThread+0x389
        9f7e7c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        9f7e7cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        9f7e7d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        9f7e7d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f7e7d64)
        01ebfae8 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01ebfaec 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        01ebfb18 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        01ebfb54 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        01ebfbc0 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        01ebfbcc 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        01ebfbf0 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        01ebfbfc 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        01ebfc08 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01ebfc48 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

AppleOSSMgr process

```
PROCESS 89870020  SessionId: 0  Cid: 0704    Peb: 7ffdc000  ParentCid: 0214
    DirBase: 29a012c0  ObjectTable: 89df9f48  HandleCount:  34.
    Image: AppleOSSMgr.exe
    VadRoot 89875188 Vads 36 Clone 0 Private 122. Modified 75. Locked 0.
    DeviceMap 85a03048
    Token                             a1280030
    ElapsedTime                       00:10:51.511
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         46880
    QuotaPoolUsage[NonPagedPool]      1768
    Working Set Sizes (now,min,max)  (541, 50, 345) (2164KB, 200KB, 1380KB)
    PeakWorkingSetSize                632
    VirtualSize                       22 Mb
    PeakVirtualSize                   24 Mb
    PageFaultCount                    631
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      184

    Setting context for this process...
.process /p /r ffffffff89870020

    !peb
PEB at 7ffdc000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00400000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00281720 . 00282738
    Ldr.InLoadOrderModuleList:           002816a0 . 002991c0
    Ldr.InMemoryOrderModuleList:         002816a8 . 002991c8
            Base TimeStamp                     Module
          400000 46aa6ef8 Jul 27 23:17:28 2007 C:\Windows\system32\AppleOSSMgr.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        75290000 4549bdd0 Nov 02 09:43:44 2006 C:\Windows\system32\POWRPROF.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        77030000 4549bdb0 Nov 02 09:43:12 2006 C:\Windows\system32\SETUPAPI.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
    SubSystemData:     00000000
    ProcessHeap:       00280000
    ProcessParameters: 00280fd8
    WindowTitle:  'C:\Windows\system32\AppleOSSMgr.exe'
    ImageFile:    'C:\Windows\system32\AppleOSSMgr.exe'
    CommandLine:  'C:\Windows\system32\AppleOSSMgr.exe'
    DllPath:
'C:\Windows\system32;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Wind
ows;C:\Windows\System32\Wbem;C:\Program Files\QuickTime\QTSystem\'
    Environment:  002807e8
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\system32\config\systemprofile\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
```

```
        COMPUTERNAME=HOME
        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:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\TEMP
        TMP=C:\Windows\TEMP
        USERDOMAIN=WORKGROUP
        USERNAME=HOME$
        USERPROFILE=C:\Windows\system32\config\systemprofile
        windir=C:\Windows


        THREAD 89870d78  Cid 0704.0708  Teb: 7ffdf000 Win32Thread: ff5141d8 WAIT: (Executive)
UserMode Non-Alertable
            89871e24  NotificationEvent
        IRP List:
            9fd86270: (0006,0094) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            89870020       Image:         AppleOSSMgr.exe
        Wait Start TickCount      1797           Ticks: 41702 (0:00:10:50.555)
        Context Switch Count      20
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address AppleOSSMgr (0x00407ad9)
        Stack Init a0370000 Current a036fbc8 Base a0370000 Limit a036d000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a036fbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a036fc1c 81c293a7 nt!KiSwapThread+0x389
        a036fc78 81d88faf nt!KeWaitForSingleObject+0x414
        a036fcac 81d93669 nt!IopSynchronousServiceTail+0x258
        a036fd38 81c8caaa nt!NtReadFile+0x646
        a036fd38 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a036fd64)
        0012f95c 77490080 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0012f960 75f3853f ntdll!ZwReadFile+0xc (FPO: [9,0,0])
        0012f9d8 775cffe2 kernel32!ReadFile+0x20e (FPO: [Non-Fpo])
        0012fa04 775cfdfb ADVAPI32!ScGetPipeInput+0x2a (FPO: [Non-Fpo])
        0012fa6c 775cbdd2 ADVAPI32!ScDispatcherLoop+0x6c (FPO: [Non-Fpo])
        0012fce4 004023e3 ADVAPI32!StartServiceCtrlDispatcherW+0xce (FPO: [Non-Fpo])
        0012ffa0 75f33833 AppleOSSMgr+0x23e3
        0012ffac 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0012ffec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

AppleTimeSrv process

```
PROCESS 89871718  SessionId: 0  Cid: 0724    Peb: 7ffda000  ParentCid: 0214
    DirBase: 29a012e0  ObjectTable: 89c98008  HandleCount:  74.
    Image: AppleTimeSrv.exe
    VadRoot 89854f98 Vads 60 Clone 0 Private 217. Modified 143. Locked 0.
    DeviceMap 85a03048
    Token                             a12802d0
    ElapsedTime                       00:10:51.480
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.078
    QuotaPoolUsage[PagedPool]         50336
    QuotaPoolUsage[NonPagedPool]      2952
    Working Set Sizes (now,min,max)  (681, 50, 345) (2724KB, 200KB, 1380KB)
    PeakWorkingSetSize                867
    VirtualSize                       26 Mb
    PeakVirtualSize                   27 Mb
    PageFaultCount                    1057
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      288

    Setting context for this process...
.process /p /r ffffffff89871718

    !peb
PEB at 7ffda000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00400000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 002b1728 . 002cc070
    Ldr.InLoadOrderModuleList:           002b16a8 . 002cc060
    Ldr.InMemoryOrderModuleList:         002b16b0 . 002cc068
            Base TimeStamp                     Module
          400000 46b10814 Aug 01 23:24:20 2007 C:\Windows\system32\AppleTimeSrv.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        75fe0000 4549be0e Nov 02 09:44:46 2006 C:\Windows\system32\WS2_32.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        77550000 4549bdc7 Nov 02 09:43:35 2006 C:\Windows\system32\NSI.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        75250000 4549bd69 Nov 02 09:42:01 2006 C:\Windows\system32\mswsock.dll
        752c0000 4549be27 Nov 02 09:45:11 2006 C:\Windows\System32\wshtcpip.dll
        752b0000 4549be21 Nov 02 09:45:05 2006 C:\Windows\System32\wship6.dll
        74d30000 4549bd6b Nov 02 09:42:03 2006 C:\Windows\system32\NLAapi.dll
        755b0000 4549bd3f Nov 02 09:41:19 2006 C:\Windows\system32\IPHLPAPI.DLL
        75570000 46807ea6 Jun 26 03:49:10 2007 C:\Windows\system32\dhcpcsvc.DLL
        75af0000 4549bcf1 Nov 02 09:40:01 2006 C:\Windows\system32\DNSAPI.dll
        75b80000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\Secur32.dll
        75560000 4549be1e Nov 02 09:45:02 2006 C:\Windows\system32\WINNSI.DLL
        75540000 46807ea7 Jun 26 03:49:11 2007 C:\Windows\system32\dhcpcsvc6.DLL
        72f40000 4549be1f Nov 02 09:45:03 2006 C:\Windows\System32\winrnr.dll
        76310000 4549be44 Nov 02 09:45:40 2006 C:\Windows\system32\WLDAP32.dll
        75ce0000 4549bd99 Nov 02 09:42:49 2006 C:\Windows\system32\PSAPI.DLL
        72f30000 4549bd3b Nov 02 09:41:15 2006 C:\Windows\system32\napinsp.dll
        72c10000 4549bdc0 Nov 02 09:43:28 2006 C:\Windows\system32\pnrpnsp.dll
        72c40000 4549be1d Nov 02 09:45:01 2006 C:\Windows\system32\wshbth.dll
```

```
        77030000 4549bdb0 Nov 02 09:43:12 2006 C:\Windows\system32\SETUPAPI.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        72a60000 4549bda2 Nov 02 09:42:58 2006 C:\Windows\system32\rasadhlp.dll
    SubSystemData:     00000000
    ProcessHeap:       002b0000
    ProcessParameters: 002b0fd8
    WindowTitle:  'C:\Windows\system32\AppleTimeSrv.exe'
    ImageFile:    'C:\Windows\system32\AppleTimeSrv.exe'
    CommandLine:  'C:\Windows\system32\AppleTimeSrv.exe'
    DllPath:
'C:\Windows\system32;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Wind
ows;C:\Windows\System32\Wbem;C:\Program Files\QuickTime\QTSystem\'
    Environment:  002b07e8
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\system32\config\systemprofile\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        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:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\TEMP
        TMP=C:\Windows\TEMP
        USERDOMAIN=WORKGROUP
        USERNAME=HOME$
        USERPROFILE=C:\Windows\system32\config\systemprofile
        windir=C:\Windows
```

```
        THREAD 89871470  Cid 0724.0728  Teb: 7ffdf000 Win32Thread: ff50c0c8 WAIT: (Executive)
UserMode Non-Alertable
            898738ec  NotificationEvent
        IRP List:
            9fccb798: (0006,0094) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            89871718       Image:         AppleTimeSrv.exe
        Wait Start TickCount      1798           Ticks: 41701 (0:00:10:50.539)
        Context Switch Count      20
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address AppleTimeSrv (0x004027b7)
        Stack Init a088f000 Current a088ebc8 Base a088f000 Limit a088c000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a088ebe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a088ec1c 81c293a7 nt!KiSwapThread+0x389
        a088ec78 81d88faf nt!KeWaitForSingleObject+0x414
        a088ecac 81d93669 nt!IopSynchronousServiceTail+0x258
        a088ed38 81c8caaa nt!NtReadFile+0x646
        a088ed38 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a088ed64)
        0012f95c 77490080 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0012f960 75f3853f ntdll!ZwReadFile+0xc (FPO: [9,0,0])
        0012f9d8 775cffe2 kernel32!ReadFile+0x20e (FPO: [Non-Fpo])
        0012fa04 775cfdfb ADVAPI32!ScGetPipeInput+0x2a (FPO: [Non-Fpo])
        0012fa6c 775cbdd2 ADVAPI32!ScDispatcherLoop+0x6c (FPO: [Non-Fpo])
        0012fce4 00401740 ADVAPI32!StartServiceCtrlDispatcherW+0xce (FPO: [Non-Fpo])
        0012ff04 00401785 AppleTimeSrv+0x1740
        0012ffa0 75f33833 AppleTimeSrv+0x1785
        0012ffac 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0012ffec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Svchost process (bthsvcs)

```
PROCESS 89877258  SessionId: 0  Cid: 0734    Peb: 7ffd9000  ParentCid: 0214
    DirBase: 29a01300  ObjectTable: 9f8d2970  HandleCount:  94.
    Image: svchost.exe
    VadRoot 89854070 Vads 60 Clone 0 Private 216. Modified 98. Locked 0.
    DeviceMap a00699b8
    Token                             a01d7568
    ElapsedTime                       00:10:51.464
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.015
    QuotaPoolUsage[PagedPool]         52432
    QuotaPoolUsage[NonPagedPool]      2920
    Working Set Sizes (now,min,max)  (782, 50, 345) (3128KB, 200KB, 1380KB)
    PeakWorkingSetSize                885
    VirtualSize                       27 Mb
    PeakVirtualSize                   28 Mb
    PageFaultCount                    928
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      553

    Setting context for this process...
.process /p /r ffffffff89877258

    !peb
PEB at 7ffd9000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00dd0000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 003a17b0 . 003bdbe0
    Ldr.InLoadOrderModuleList:           003a1730 . 003bdd20
    Ldr.InMemoryOrderModuleList:         003a1738 . 003bdd28
            Base TimeStamp                     Module
          dd0000 4549adc4 Nov 02 08:35:16 2006 C:\Windows\system32\svchost.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        72f60000 4549bce4 Nov 02 09:39:48 2006 c:\windows\system32\bthserv.dll
        77030000 4549bdb0 Nov 02 09:43:12 2006 C:\Windows\system32\SETUPAPI.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        74ff0000 4549be2f Nov 02 09:45:19 2006 C:\Windows\system32\WINTRUST.dll
        75650000 45b96fde Jan 26 03:05:02 2007 C:\Windows\system32\CRYPT32.dll
        75820000 4549bd41 Nov 02 09:41:21 2006 C:\Windows\system32\MSASN1.dll
        75ba0000 4549bde2 Nov 02 09:44:02 2006 C:\Windows\system32\USERENV.dll
        75b80000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\Secur32.dll
        77580000 462434a3 Apr 17 03:44:51 2007 C:\Windows\system32\imagehlp.dll
        75480000 4549bd20 Nov 02 09:40:48 2006 C:\Windows\system32\credssp.dll
        75050000 46773a78 Jun 19 03:07:52 2007 C:\Windows\system32\schannel.dll
        75840000 4549bd53 Nov 02 09:41:39 2006 C:\Windows\system32\NETAPI32.dll
        75ce0000 4549bd99 Nov 02 09:42:49 2006 C:\Windows\system32\PSAPI.DLL
        75210000 4549bd5d Nov 02 09:41:49 2006 C:\Windows\system32\msv1_0.dll
        75b60000 4549bd26 Nov 02 09:40:54 2006 C:\Windows\system32\cryptdll.dll
        75fe0000 4549be0e Nov 02 09:44:46 2006 C:\Windows\system32\WS2_32.dll
        77550000 4549bdc7 Nov 02 09:43:35 2006 C:\Windows\system32\NSI.dll
```

```
    SubSystemData:     00000000
    ProcessHeap:       003a0000
    ProcessParameters: 003a1068
    WindowTitle:  'C:\Windows\system32\svchost.exe'
    ImageFile:    'C:\Windows\system32\svchost.exe'
    CommandLine:  'C:\Windows\system32\svchost.exe -k bthsvcs'
    DllPath:
'C:\Windows\system32;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Wind
ows;C:\Windows\System32\Wbem;C:\Program Files\QuickTime\QTSystem\'
    Environment:  003a07e8
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\ServiceProfiles\LocalService\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        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;C:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        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 898776d8  Cid 0734.0738  Teb: 7ffdf000 Win32Thread: 00000000 WAIT: (Executive)
UserMode Non-Alertable
            89878504  NotificationEvent
        IRP List:
            9fdabb60: (0006,0094) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            89877258       Image:         svchost.exe
        Wait Start TickCount      1799           Ticks: 41700 (0:00:10:50.524)
        Context Switch Count      15
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address svchost!wmainCRTStartup (0x00dd20bf)
        Stack Init a1b50000 Current a1b4fbc8 Base a1b50000 Limit a1b4d000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1b4fbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1b4fc1c 81c293a7 nt!KiSwapThread+0x389
        a1b4fc78 81d88faf nt!KeWaitForSingleObject+0x414
        a1b4fcac 81d93669 nt!IopSynchronousServiceTail+0x258
        a1b4fd38 81c8caaa nt!NtReadFile+0x646
        a1b4fd38 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1b4fd64)
        001df990 77490080 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        001df994 75f3853f ntdll!ZwReadFile+0xc (FPO: [9,0,0])
        001dfa0c 775cffe2 kernel32!ReadFile+0x20e (FPO: [Non-Fpo])
        001dfa38 775cfdfb ADVAPI32!ScGetPipeInput+0x2a (FPO: [Non-Fpo])
        001dfaa0 775cbdd2 ADVAPI32!ScDispatcherLoop+0x6c (FPO: [Non-Fpo])
        001dfd18 00dd241d ADVAPI32!StartServiceCtrlDispatcherW+0xce (FPO: [Non-Fpo])
        001dfd20 00dd2401 svchost!SvcHostMain+0x12 (FPO: [Non-Fpo])
        001dfd24 00dd2183 svchost!wmain+0x5 (FPO: [Non-Fpo])
        001dfd68 75f33833 svchost!_initterm_e+0x163 (FPO: [Non-Fpo])
        001dfd74 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        001dfdb4 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 89879210  Cid 0734.0758  Teb: 7ffdd000 Win32Thread: ff5125a8 WAIT: (WrUserRequest)
UserMode Non-Alertable
            9fc21478  SynchronizationEvent
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            89877258       Image:         svchost.exe
        Wait Start TickCount      10202          Ticks: 33297 (0:00:08:39.436)
        Context Switch Count      99
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address bthserv!BthServMainThread (0x72f636a5)
        Stack Init a1b54000 Current a1b53b68 Base a1b54000 Limit a1b51000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1b53b80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1b53bbc 81c293a7 nt!KiSwapThread+0x389
        a1b53c18 8cedb8ed nt!KeWaitForSingleObject+0x414
        a1b53c74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        a1b53c90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        a1b53ce8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        a1b53d4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        a1b53d4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1b53d64)
        00abfc10 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00abfc14 761e19cd USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        00abfc30 72f6375f USER32!GetMessageW+0x33 (FPO: [Non-Fpo])
        00abfca0 75f33833 bthserv!BthServMainThread+0xba (FPO: [Non-Fpo])
        00abfcac 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00abfcec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 8988e420  Cid 0734.0774  Teb: 7ffdc000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            9fc22c88  NotificationEvent
            9fde8d80  SynchronizationTimer
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            89877258       Image:         svchost.exe
        Wait Start TickCount      1811           Ticks: 41688 (0:00:10:50.336)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address bthserv!BthServAsyncThread (0x72f62ac2)
        Stack Init a1ad5000 Current a1ad48d0 Base a1ad5000 Limit a1ad2000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1ad48e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1ad4924 81c28c64 nt!KiSwapThread+0x389
        a1ad4970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1ad4bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1ad4d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1ad4d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1ad4d64)
        00b1fdcc 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00b1fdd0 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00b1fe6c 72f62953 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        00b1feb8 75f33833 bthserv!BthServAsyncEventsThread+0xb7 (FPO: [Non-Fpo])
        00b1fec4 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00b1ff04 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 838f4a08  Cid 0734.0b1c  Teb: 7ffde000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            9fde0438  QueueObject
        Not impersonating
        DeviceMap                 a00699b8
        Owning Process            89877258       Image:         svchost.exe
        Wait Start TickCount      21532          Ticks: 21967 (0:00:05:42.687)
        Context Switch Count      6
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init a8fc8000 Current a8fc7bc8 Base a8fc8000 Limit a8fc5000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a8fc7be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8fc7c1c 81cad431 nt!KiSwapThread+0x389
        a8fc7c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a8fc7cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a8fc7d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a8fc7d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8fc7d64)
        00cbf6f8 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00cbf6fc 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        00cbf728 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        00cbf764 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        00cbf7d0 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        00cbf7dc 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        00cbf800 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        00cbf80c 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        00cbf818 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00cbf858 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Svchost process (NetworkServiceNetworkRestricted)

```
PROCESS 89881d28  SessionId: 0  Cid: 0768    Peb: 7ffdf000  ParentCid: 0214
    DirBase: 29a01320  ObjectTable: 9f8813f0  HandleCount: 108.
    Image: svchost.exe
    VadRoot 9fc41e80 Vads 72 Clone 0 Private 380. Modified 111. Locked 0.
    DeviceMap 9f999328
    Token                             a123f5e0
    ElapsedTime                       00:10:51.355
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         54840
    QuotaPoolUsage[NonPagedPool]      4440
    Working Set Sizes (now,min,max)  (946, 50, 345) (3784KB, 200KB, 1380KB)
    PeakWorkingSetSize                1155
    VirtualSize                       27 Mb
    PeakVirtualSize                   28 Mb
    PageFaultCount                    1364
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      478

    Setting context for this process...
.process /p /r ffffffff89881d28

    !peb
PEB at 7ffdf000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00dd0000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 002417d8 . 0025e630
    Ldr.InLoadOrderModuleList:           00241758 . 0025e690
    Ldr.InMemoryOrderModuleList:         00241760 . 0025e698
            Base TimeStamp                     Module
          dd0000 4549adc4 Nov 02 08:35:16 2006 C:\Windows\system32\svchost.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        72960000 4549bd4d Nov 02 09:41:33 2006 c:\windows\system32\ipsecsvc.dll
        757b0000 4549bccf Nov 02 09:39:27 2006 c:\windows\system32\AUTHZ.dll
        755b0000 4549bd3f Nov 02 09:41:19 2006 c:\windows\system32\IPHLPAPI.DLL
        75570000 46807ea6 Jun 26 03:49:10 2007 c:\windows\system32\dhcpcsvc.DLL
        75af0000 4549bcf1 Nov 02 09:40:01 2006 c:\windows\system32\DNSAPI.dll
        75fe0000 4549be0e Nov 02 09:44:46 2006 C:\Windows\system32\WS2_32.dll
        77550000 4549bdc7 Nov 02 09:43:35 2006 C:\Windows\system32\NSI.dll
        75b80000 4549bdd2 Nov 02 09:43:46 2006 c:\windows\system32\Secur32.dll
        75560000 4549be1e Nov 02 09:45:02 2006 c:\windows\system32\WINNSI.DLL
        75540000 46807ea7 Jun 26 03:49:11 2007 c:\windows\system32\dhcpcsvc6.DLL
        75650000 45b96fde Jan 26 03:05:02 2007 c:\windows\system32\CRYPT32.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        75820000 4549bd41 Nov 02 09:41:21 2006 c:\windows\system32\MSASN1.dll
        75ba0000 4549bde2 Nov 02 09:44:02 2006 c:\windows\system32\USERENV.dll
        735b0000 4549bce0 Nov 02 09:39:44 2006 c:\windows\system32\fwpuclnt.dll
        74f30000 46677f3a Jun 07 04:44:58 2007 c:\windows\system32\FirewallAPI.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        753f0000 4549bde4 Nov 02 09:44:04 2006 c:\windows\system32\VERSION.dll
        72c00000 4549bce1 Nov 02 09:39:45 2006 c:\windows\system32\FwRemoteSvr.DLL
        76310000 4549be44 Nov 02 09:45:40 2006 C:\Windows\system32\WLDAP32.dll
        75ce0000 4549bd99 Nov 02 09:42:49 2006 C:\Windows\system32\PSAPI.DLL
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
```

```
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        75250000 4549bd69 Nov 02 09:42:01 2006 C:\Windows\system32\mswsock.dll
        752c0000 4549be27 Nov 02 09:45:11 2006 C:\Windows\System32\wshtcpip.dll
        752b0000 4549be21 Nov 02 09:45:05 2006 C:\Windows\System32\wship6.dll
        75480000 4549bd20 Nov 02 09:40:48 2006 C:\Windows\system32\credssp.dll
        75050000 46773a78 Jun 19 03:07:52 2007 C:\Windows\system32\schannel.dll
        75840000 4549bd53 Nov 02 09:41:39 2006 C:\Windows\system32\NETAPI32.dll
    SubSystemData:     00000000
    ProcessHeap:       00240000
    ProcessParameters: 00241060
    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;C:\Program Files\QuickTime\QTSystem\'
    Environment:  002407e8
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        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;C:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        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=WORKGROUP
        USERNAME=HOME$
        USERPROFILE=C:\Windows\ServiceProfiles\NetworkService
        windir=C:\Windows
```

```
        THREAD 89881650  Cid 0768.076c  Teb: 7ffde000 Win32Thread: 00000000 WAIT: (Executive)
UserMode Non-Alertable
            9fc276d4  NotificationEvent
        IRP List:
            9fcf4340: (0006,0094) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            89881d28       Image:         svchost.exe
        Wait Start TickCount      1807           Ticks: 41692 (0:00:10:50.399)
        Context Switch Count      67
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address svchost!wmainCRTStartup (0x00dd20bf)
        Stack Init a1ad9000 Current a1ad8bc8 Base a1ad9000 Limit a1ad6000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1ad8be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1ad8c1c 81c293a7 nt!KiSwapThread+0x389
        a1ad8c78 81d88faf nt!KeWaitForSingleObject+0x414
        a1ad8cac 81d93669 nt!IopSynchronousServiceTail+0x258
        a1ad8d38 81c8caaa nt!NtReadFile+0x646
        a1ad8d38 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1ad8d64)
        0018f9c4 77490080 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0018f9c8 75f3853f ntdll!ZwReadFile+0xc (FPO: [9,0,0])
        0018fa40 775cffe2 kernel32!ReadFile+0x20e (FPO: [Non-Fpo])
        0018fa6c 775cfdfb ADVAPI32!ScGetPipeInput+0x2a (FPO: [Non-Fpo])
        0018fad4 775cbdd2 ADVAPI32!ScDispatcherLoop+0x6c (FPO: [Non-Fpo])
        0018fd4c 00dd241d ADVAPI32!StartServiceCtrlDispatcherW+0xce (FPO: [Non-Fpo])
        0018fd54 00dd2401 svchost!SvcHostMain+0x12 (FPO: [Non-Fpo])
        0018fd58 00dd2183 svchost!wmain+0x5 (FPO: [Non-Fpo])
        0018fd9c 75f33833 svchost!_initterm_e+0x163 (FPO: [Non-Fpo])
        0018fda8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0018fde8 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fd9f840  Cid 0768.077c  Teb: 7ffdd000 Win32Thread: ff51de98 WAIT: (UserRequest)
UserMode Non-Alertable
            a181a6f8  NotificationEvent
            9fda3640  NotificationEvent
            899e6e20  NotificationEvent
            8485e7f8  NotificationEvent
            898512c8  NotificationEvent
            89878318  NotificationEvent
            a1811ac0  SynchronizationEvent
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            89881d28       Image:         svchost.exe
        Wait Start TickCount      9806           Ticks: 33693 (0:00:08:45.614)
        Context Switch Count      670
        UserTime                  00:00:00.031
        KernelTime                00:00:00.078
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x775cb9d5)
        Stack Init a1b64000 Current a1b638d0 Base a1b64000 Limit a1b61000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1b638e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1b63924 81c28c64 nt!KiSwapThread+0x389
        a1b63970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1b63bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1b63d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1b63d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1b63d64)
        0072fdf0 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0072fdf4 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0072fe90 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0072feac 729616b4 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0072ff00 7296a2c3 ipsecsvc!ServiceWait+0x156 (FPO: [Non-Fpo])
        0072ff10 00dd148a ipsecsvc!SpdServiceMain+0x321 (FPO: [Non-Fpo])
        0072ff3c 775cb9f6 svchost!ServiceStarter+0x17a (FPO: [Non-Fpo])
        0072ff50 75f33833 ADVAPI32!ScSvcctrlThreadA+0x21 (FPO: [Non-Fpo])
        0072ff5c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0072ff9c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fcf5af0  Cid 0768.00f8  Teb: 7ffdc000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            9fcf5d98  SynchronizationTimer
            9fc28918  SynchronizationEvent
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            89881d28       Image:         svchost.exe
        Wait Start TickCount      1883           Ticks: 41616 (0:00:10:49.213)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x7744b49a)
        Stack Init a1ad1000 Current a1ad08d0 Base a1ad1000 Limit a1ace000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1ad08e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1ad0924 81c28c64 nt!KiSwapThread+0x389
        a1ad0970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1ad0bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1ad0d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1ad0d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1ad0d64)
        009ef824 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        009ef828 7744b65b ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        009ef9c4 75f33833 ntdll!TppWaiterpThread+0x294 (FPO: [Non-Fpo])
        009ef9d0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        009efa10 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 8985acf0  Cid 0768.0108  Teb: 7ffdb000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Alertable
            a1803768  QueueObject
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            89881d28       Image:         svchost.exe
        Wait Start TickCount      1884           Ticks: 41615 (0:00:10:49.198)
        Context Switch Count      11
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init a0921000 Current a0920bc8 Base a0921000 Limit a091e000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a0920be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0920c1c 81cad431 nt!KiSwapThread+0x389
        a0920c68 81d8b982 nt!KeRemoveQueueEx+0x568
        a0920cc0 81c7a036 nt!IoRemoveIoCompletion+0x23
        a0920d54 81c8caaa nt!NtWaitForWorkViaWorkerFactory+0x1a1
        a0920d54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0920d64)
        00cef790 77490850 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00cef794 7749a1b4 ntdll!NtWaitForWorkViaWorkerFactory+0xc (FPO: [2,0,0])
        00cef8bc 75f33833 ntdll!TppWorkerThread+0x1f6 (FPO: [Non-Fpo])
        00cef8c8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00cef908 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD a180c418  Cid 0768.0190  Teb: 7ffda000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            9fd4d948  QueueObject
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            89881d28       Image:         svchost.exe
        Wait Start TickCount      13632          Ticks: 29867 (0:00:07:45.928)
        Context Switch Count      16
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init 9f228000 Current 9f227bc8 Base 9f228000 Limit 9f225000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f227be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f227c1c 81cad431 nt!KiSwapThread+0x389
        9f227c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        9f227cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        9f227d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        9f227d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f227d64)
        00bbfa48 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00bbfa4c 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        00bbfa78 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        00bbfab4 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        00bbfb20 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        00bbfb2c 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        00bbfb54 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        00bbfb60 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        00bbfb6c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00bbfbac 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Stacsv process

```
PROCESS 9fde0020  SessionId: 0  Cid: 078c    Peb: 7ffde000  ParentCid: 0214
    DirBase: 29a01340  ObjectTable: a012eeb8  HandleCount: 140.
    Image: stacsv.exe
    VadRoot 9fc6cac8 Vads 77 Clone 0 Private 513. Modified 242. Locked 0.
    DeviceMap 85a03048
    Token                             873fe620
    ElapsedTime                       00:10:51.324
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.015
    QuotaPoolUsage[PagedPool]         60920
    QuotaPoolUsage[NonPagedPool]      3768
    Working Set Sizes (now,min,max)  (1086, 50, 345) (4344KB, 200KB, 1380KB)
    PeakWorkingSetSize                1444
    VirtualSize                       41 Mb
    PeakVirtualSize                   48 Mb
    PageFaultCount                    1552
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      2049

    Setting context for this process...
.process /p /r ffffffff9fde0020

    !peb
PEB at 7ffde000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00400000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 001917c8 . 001a9428
    Ldr.InLoadOrderModuleList:           00191748 . 001a9568
    Ldr.InMemoryOrderModuleList:         00191750 . 001a9570
            Base TimeStamp                     Module
          400000 4592b2f3 Dec 27 17:52:51 2006 C:\Program Files\SigmaTel\C-Major
Audio\WDM\STacSV.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        77030000 4549bdb0 Nov 02 09:43:12 2006 C:\Windows\system32\SETUPAPI.dll
        728e0000 4549bd18 Nov 02 09:40:40 2006 C:\Windows\system32\DSOUND.dll
        738c0000 4549be1d Nov 02 09:45:01 2006 C:\Windows\system32\WINMM.dll
        73880000 4549bd93 Nov 02 09:42:43 2006 C:\Windows\system32\OLEACC.dll
        75290000 4549bdd0 Nov 02 09:43:44 2006 C:\Windows\system32\POWRPROF.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        75b80000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\Secur32.dll
        74ff0000 4549be2f Nov 02 09:45:19 2006 C:\Windows\system32\WINTRUST.dll
        75650000 45b96fde Jan 26 03:05:02 2007 C:\Windows\system32\CRYPT32.dll
        75820000 4549bd41 Nov 02 09:41:21 2006 C:\Windows\system32\MSASN1.dll
        75ba0000 4549bde2 Nov 02 09:44:02 2006 C:\Windows\system32\USERENV.dll
        77580000 462434a3 Apr 17 03:44:51 2007 C:\Windows\system32\imagehlp.dll
        773a0000 4549bce9 Nov 02 09:39:53 2006 C:\Windows\system32\CLBCatQ.DLL
        72860000 4592b297 Dec 27 17:51:19 2006 C:\Windows\system32\stapi32.dll
        75350000 4549bdae Nov 02 09:43:10 2006 C:\Windows\system32\rsaenh.dll
        74d90000 4549bd03 Nov 02 09:40:19 2006 C:\Windows\System32\MMDevApi.dll
```

```
        763b0000 4549bdb9 Nov 02 09:43:21 2006 C:\Windows\system32\SHLWAPI.dll
        74aa0000 4549bd09 Nov 02 09:40:25 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_5d07289e07e1d100\comctl32.dll
        736d0000 4549bcc2 Nov 02 09:39:14 2006 C:\Windows\System32\audioses.dll
        73540000 4549bcc0 Nov 02 09:39:12 2006 C:\Windows\System32\audioeng.dll
        75390000 4549bcdc Nov 02 09:39:40 2006 C:\Windows\System32\AVRT.dll
        75ce0000 4549bd99 Nov 02 09:42:49 2006 C:\Windows\system32\PSAPI.DLL
    SubSystemData:     00000000
    ProcessHeap:       00190000
    ProcessParameters: 00190fd8
    WindowTitle:  'C:\Program Files\SigmaTel\C-Major Audio\WDM\STacSV.exe'
    ImageFile:    'C:\Program Files\SigmaTel\C-Major Audio\WDM\STacSV.exe'
    CommandLine:  '"C:\Program Files\SigmaTel\C-Major Audio\WDM\STacSV.exe"'
    DllPath:      'C:\Program Files\SigmaTel\C-Major
Audio\WDM;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Windows;C:\Wind
ows\System32\Wbem;C:\Program Files\QuickTime\QTSystem\'
    Environment:  001907e8
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\system32\config\systemprofile\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        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:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\TEMP
        TMP=C:\Windows\TEMP
        USERDOMAIN=WORKGROUP
        USERNAME=HOME$
        USERPROFILE=C:\Windows\system32\config\systemprofile
        windir=C:\Windows
```

```
        THREAD 9fde0cd8  Cid 078c.0790  Teb: 7ffdf000 Win32Thread: ff41b7a0 WAIT: (Executive)
UserMode Non-Alertable
            a18055ac  NotificationEvent
        IRP List:
            899e7af8: (0006,0094) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fde0020       Image:         stacsv.exe
        Wait Start TickCount      8861           Ticks: 34638 (0:00:09:00.356)
        Context Switch Count      3964
        UserTime                  00:00:00.062
        KernelTime                00:00:00.046
        Win32 Start Address STacSV (0x0040f014)
        Stack Init a1b01000 Current a1b00bc8 Base a1b01000 Limit a1afe000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1b00be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1b00c1c 81c293a7 nt!KiSwapThread+0x389
        a1b00c78 81d88faf nt!KeWaitForSingleObject+0x414
        a1b00cac 81d93669 nt!IopSynchronousServiceTail+0x258
        a1b00d38 81c8caaa nt!NtReadFile+0x646
        a1b00d38 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1b00d64)
        0012d578 77490080 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0012d57c 75f3853f ntdll!ZwReadFile+0xc (FPO: [9,0,0])
        0012d5f4 775cffe2 kernel32!ReadFile+0x20e (FPO: [Non-Fpo])
        0012d620 775cfdfb ADVAPI32!ScGetPipeInput+0x2a (FPO: [Non-Fpo])
        0012d688 775b2949 ADVAPI32!ScDispatcherLoop+0x6c (FPO: [Non-Fpo])
        0012d8dc 0040393f ADVAPI32!StartServiceCtrlDispatcherA+0x8a (FPO: [Non-Fpo])
        0012da30 004125f8 STacSV+0x393f
        004103d8 0040f104 STacSV+0x125f8
        004103dc 0040f118 STacSV+0xf104
        004103e0 00000000 STacSV+0xf118
```

```
        THREAD 9fd78d78  Cid 078c.01a4  Teb: 7ffdd000 Win32Thread: ff524d28 WAIT: (UserRequest)
UserMode Non-Alertable
            9e1f28f0  NotificationEvent
            a18a4ec8  NotificationEvent
            a18a4020  NotificationEvent
            a18a4458  NotificationEvent
            9fdfe470  NotificationEvent
            a18a5dc0  NotificationEvent
            a18a5d90  NotificationEvent
            a18a5ea0  NotificationEvent
            a18a5e70  NotificationEvent
            a18a5e40  NotificationEvent
            a18a4738  NotificationEvent
            a18a4708  NotificationEvent
            a18a46d8  NotificationEvent
            a18a46a8  NotificationEvent
            a18a4678  NotificationEvent
            8988ead0  NotificationEvent
            8988eaa0  NotificationEvent
            8988ea70  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fde0020       Image:         stacsv.exe
        Wait Start TickCount      1895           Ticks: 41604 (0:00:10:49.026)
        Context Switch Count      3344
        UserTime                  00:00:00.078
        KernelTime                00:00:00.015
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x775cb9d5)
        Stack Init a0838000 Current a08378d0 Base a0838000 Limit a0835000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a08378e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0837924 81c28c64 nt!KiSwapThread+0x389
        a0837970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a0837bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a0837d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a0837d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0837d64)
        00f1fa54 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00f1fa58 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00f1faf4 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        00f1fb10 00407152 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        00f1fb98 77492d96 STacSV+0x7152
        00f1fb9c 7745ec63 ntdll!_SEH_epilog4_GS+0xa
        77492d96 909090ff ntdll!LdrLoadDll+0x23a (FPO: [Non-Fpo])
        77492daa 900004c2 0x909090ff
        77492dae 90909090 0x900004c2
        77492db2 8b55ff8b 0x90909090
        77492db6 90ec81ec 0x8b55ff8b
        77492dba 83000000 0x90ec81ec
        77492dbe 4fcf4c3d 0x83000000
        77492dc2 850f0077 0x4fcf4c3d
        77492dc6 00020aca 0x850f0077
        77492dca c2c9c033 0x20aca
        77492dce 90900004 0xc2c9c033
        77492dd2 8b909090 0x90900004
        77492dd6 ec8b55ff 0x8b909090
        77492dda 8310458b 0xec8b55ff
        77492dde 00a928ec 0x8310458b
        77492de2 0ff80000 0xa928ec
        77492de6 013afc85 0xff80000
        77492dea 0c4d8b00 0x13afc85
        77492dee 00000000 0xc4d8b00
```

```
        THREAD a1c3dd78  Cid 078c.06ec  Teb: 7ffda000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            a1c3c108  SynchronizationEvent
            a1c3de00  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fde0020       Image:         stacsv.exe
        Wait Start TickCount      40343          Ticks: 3156 (0:00:00:49.233)
        Context Switch Count      12
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ole32!CRpcThreadCache::RpcWorkerThreadEntry (0x7644fc53)
        Stack Init a1ee2000 Current a1ee1c38 Base a1ee2000 Limit a1edf000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a1ee1c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1ee1c8c 81c293a7 nt!KiSwapThread+0x389
        a1ee1ce8 81df5057 nt!KeWaitForSingleObject+0x414
        a1ee1d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a1ee1d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1ee1d64)
        015ffeac 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        015ffeb0 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        015fff20 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        015fff34 76455251 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        015fff50 76422104 ole32!CDllHost::MTAWorkerLoop+0x2b (FPO: [Non-Fpo])
        015fff70 764524ce ole32!CDllHost::WorkerThread+0xc7 (FPO: [Non-Fpo])
        015fff78 7644fc0d ole32!DLLHostThreadEntry+0xd (FPO: [Non-Fpo])
        015fff94 7644fc73 ole32!CRpcThread::WorkerLoop+0x26 (FPO: [Non-Fpo])
        015fffa0 75f33833 ole32!CRpcThreadCache::RpcWorkerThreadEntry+0x20 (FPO: [Non-Fpo])
        015fffac 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        015fffec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9e1dc7a0  Cid 078c.072c  Teb: 7ffd5000 Win32Thread: 00000000 WAIT: (Executive)
UserMode Non-Alertable
            898518d4  NotificationEvent
        IRP List:
            a18deb28: (0006,0094) Flags: 00060800  Mdl: 00000000
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fde0020       Image:         stacsv.exe
        Wait Start TickCount      10068          Ticks: 33431 (0:00:08:41.526)
        Context Switch Count      8
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address STacSV (0x004088f0)
        Stack Init 88eb9000 Current 88eb8b80 Base 88eb9000 Limit 88eb6000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        88eb8b98 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        88eb8bd4 81c293a7 nt!KiSwapThread+0x389
        88eb8c30 81d88faf nt!KeWaitForSingleObject+0x414
        88eb8c64 81d89efb nt!IopSynchronousServiceTail+0x258
        88eb8d00 81d8ee8f nt!IopXxxControlFile+0x6b7
        88eb8d34 81c8caaa nt!NtFsControlFile+0x2a
        88eb8d34 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 88eb8d64)
        01f0f6f8 7748f9c0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01f0f6fc 75eff00d ntdll!NtFsControlFile+0xc (FPO: [10,0,0])
        01f0f740 004089c9 kernel32!ConnectNamedPipe+0x52 (FPO: [Non-Fpo])
        01f0f790 75f3b6ce STacSV+0x89c9
        01f0fbd8 7749a604 kernel32!_BaseDllInitialize+0x92 (FPO: [Non-Fpo])
        01f0fc00 7746ab6c ntdll!LdrpCallInitRoutine+0x14
        01f0fc98 774905a0 ntdll!LdrpInitializeThread+0x1e9 (FPO: [SEH])
        01f0fc9c 7746a968 ntdll!NtTestAlert+0xc (FPO: [0,0,0])
        7746a9ea 90909090 ntdll!_LdrpInitialize+0x29c (FPO: [Non-Fpo])
        7746a9f6 00000000 0x90909090
```

```
        THREAD a180a6c0  Cid 078c.0760  Teb: 7ffd4000 Win32Thread: 00000000 WAIT: (DelayExecution)
UserMode Non-Alertable
            a180a748  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fde0020       Image:         stacsv.exe
        Wait Start TickCount      43468          Ticks: 31 (0:00:00:00.483)
        Context Switch Count      5781
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address STacSV (0x00409830)
        Stack Init a1e6e000 Current a1e6dc58 Base a1e6e000 Limit a1e6b000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a1e6dc70 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1e6dcac 81cac48e nt!KiSwapThread+0x389
        a1e6dd08 81e90bf1 nt!KeDelayExecutionThread+0x397
        a1e6dd54 81c8caaa nt!NtDelayExecution+0x8d
        a1e6dd54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1e6dd64)
        0200fb08 7748f7c0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0200fb0c 75f378e0 ntdll!NtDelayExecution+0xc (FPO: [2,0,0])
        0200fb74 75ef1da0 kernel32!SleepEx+0x62 (FPO: [Non-Fpo])
        0200fb84 004098e8 kernel32!Sleep+0xf (FPO: [Non-Fpo])
        0200fbd8 7749a604 STacSV+0x98e8
        0200fc00 7746ab6c ntdll!LdrpCallInitRoutine+0x14
        0200fc98 774905a0 ntdll!LdrpInitializeThread+0x1e9 (FPO: [SEH])
        0200fc9c 7746a968 ntdll!NtTestAlert+0xc (FPO: [0,0,0])
        7746a9ea 90909090 ntdll!_LdrpInitialize+0x29c (FPO: [Non-Fpo])
        7746a9f6 00000000 0x90909090

        THREAD 9fdbc030  Cid 078c.0764  Teb: 7ffd3000 Win32Thread: 00000000 WAIT: (DelayExecution)
UserMode Non-Alertable
            9fdbc0b8  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fde0020       Image:         stacsv.exe
        Wait Start TickCount      43489          Ticks: 10 (0:00:00:00.156)
        Context Switch Count      1424
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address STacSV (0x00409b60)
        Stack Init a1e72000 Current a1e71c58 Base a1e72000 Limit a1e6f000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a1e71c70 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1e71cac 81cac48e nt!KiSwapThread+0x389
        a1e71d08 81e90bf1 nt!KeDelayExecutionThread+0x397
        a1e71d54 81c8caaa nt!NtDelayExecution+0x8d
        a1e71d54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1e71d64)
        0210fb0c 7748f7c0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0210fb10 75f378e0 ntdll!NtDelayExecution+0xc (FPO: [2,0,0])
        0210fb78 75ef1da0 kernel32!SleepEx+0x62 (FPO: [Non-Fpo])
        0210fb88 00409bb6 kernel32!Sleep+0xf (FPO: [Non-Fpo])
        0210fbb4 7626a6fc STacSV+0x9bb6
        0210fbd8 7749a604 msvcrt!_core_crt_dll_init+0x24b (FPO: [Non-Fpo])
        0210fc00 7746ab6c ntdll!LdrpCallInitRoutine+0x14
        0210fc98 774905a0 ntdll!LdrpInitializeThread+0x1e9 (FPO: [SEH])
        0210fc9c 7746a968 ntdll!NtTestAlert+0xc (FPO: [0,0,0])
        7746a9ea 90909090 ntdll!_LdrpInitialize+0x29c (FPO: [Non-Fpo])
        7746a9f6 00000000 0x90909090
```

```
        THREAD 8346f030  Cid 078c.0fc4  Teb: 7ffdb000 Win32Thread: ff535e98 WAIT: (WrQueue)
UserMode Non-Alertable
            a1807c38  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            9fde0020       Image:         stacsv.exe
        Wait Start TickCount      26946          Ticks: 16553 (0:00:04:18.228)
        Context Switch Count      7
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init a1aa3000 Current a1aa2bc8 Base a1aa3000 Limit a1aa0000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a1aa2be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1aa2c1c 81cad431 nt!KiSwapThread+0x389
        a1aa2c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a1aa2cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a1aa2d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a1aa2d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1aa2d64)
        014ffe88 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        014ffe8c 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        014ffeb8 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        014ffef4 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        014fff60 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        014fff6c 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        014fff94 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        014fffa0 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        014fffac 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        014fffec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Svchost process (WerSvcGroup)

```
PROCESS a18b73a0  SessionId: 0  Cid: 000c    Peb: 7ffd6000  ParentCid: 0214
    DirBase: 29a01360  ObjectTable: a13361b8  HandleCount:  45.
    Image: svchost.exe
    VadRoot a18b7350 Vads 29 Clone 0 Private 112. Modified 28. Locked 0.
    DeviceMap 85a03048
    Token                             a133b8f0
    ElapsedTime                       00:10:49.669
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         30232
    QuotaPoolUsage[NonPagedPool]      1472
    Working Set Sizes (now,min,max)  (511, 50, 345) (2044KB, 200KB, 1380KB)
    PeakWorkingSetSize                546
    VirtualSize                       14 Mb
    PeakVirtualSize                   15 Mb
    PageFaultCount                    567
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      146

    Setting context for this process...
.process /p /r ffffffffa18b73a0

    !peb
PEB at 7ffd6000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00dd0000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 000c1728 . 000df620
    Ldr.InLoadOrderModuleList:           000c16a8 . 000df610
    Ldr.InMemoryOrderModuleList:         000c16b0 . 000df618
            Base TimeStamp                     Module
          dd0000 4549adc4 Nov 02 08:35:16 2006 C:\Windows\System32\svchost.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        72800000 4549bdf4 Nov 02 09:44:20 2006 c:\windows\system32\wersvc.dll
        74fe0000 46d779a1 Aug 31 03:14:57 2007 C:\Windows\System32\WTSAPI32.dll
        75300000 4549be2e Nov 02 09:45:18 2006 C:\Windows\System32\WINSTA.dll
    SubSystemData:     00000000
    ProcessHeap:       000c0000
    ProcessParameters: 000c0fd8
    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;C:\Program Files\QuickTime\QTSystem\'
    Environment:  000c07e8
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\system32\config\systemprofile\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        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:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\TEMP
        TMP=C:\Windows\TEMP
        USERDOMAIN=WORKGROUP
        USERNAME=HOME$
        USERPROFILE=C:\Windows\system32\config\systemprofile
        windir=C:\Windows


        THREAD a18b5d78  Cid 000c.01c0  Teb: 7ffdf000 Win32Thread: 00000000 WAIT: (Executive)
UserMode Non-Alertable
            a18a7994  NotificationEvent
        IRP List:
            9fd235e8: (0006,0094) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            a18b73a0       Image:         svchost.exe
        Wait Start TickCount      9163           Ticks: 34336 (0:00:08:55.645)
        Context Switch Count      61
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address svchost!wmainCRTStartup (0x00dd20bf)
        Stack Init a1a5f000 Current a1a5ebc8 Base a1a5f000 Limit a1a5c000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1a5ebe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1a5ec1c 81c293a7 nt!KiSwapThread+0x389
        a1a5ec78 81d88faf nt!KeWaitForSingleObject+0x414
        a1a5ecac 81d93669 nt!IopSynchronousServiceTail+0x258
        a1a5ed38 81c8caaa nt!NtReadFile+0x646
        a1a5ed38 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1a5ed64)
        000bfa34 77490080 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        000bfa38 75f3853f ntdll!ZwReadFile+0xc (FPO: [9,0,0])
        000bfab0 775cffe2 kernel32!ReadFile+0x20e (FPO: [Non-Fpo])
        000bfadc 775cfdfb ADVAPI32!ScGetPipeInput+0x2a (FPO: [Non-Fpo])
        000bfb44 775cbdd2 ADVAPI32!ScDispatcherLoop+0x6c (FPO: [Non-Fpo])
        000bfdbc 00dd241d ADVAPI32!StartServiceCtrlDispatcherW+0xce (FPO: [Non-Fpo])
        000bfdc4 00dd2401 svchost!SvcHostMain+0x12 (FPO: [Non-Fpo])
        000bfdc8 00dd2183 svchost!wmain+0x5 (FPO: [Non-Fpo])
        000bfe0c 75f33833 svchost!_initterm_e+0x163 (FPO: [Non-Fpo])
        000bfe18 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        000bfe58 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD a18aad78  Cid 000c.02e0  Teb: 7ffdd000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            a18bd300  SynchronizationTimer
            a18bdab8  NotificationEvent
            a18b8250  SynchronizationEvent
            a18b81dc  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            a18b73a0       Image:         svchost.exe
        Wait Start TickCount      17983          Ticks: 25516 (0:00:06:38.052)
        Context Switch Count      29
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x7744b49a)
        Stack Init a1ee6000 Current a1ee58d0 Base a1ee6000 Limit a1ee3000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1ee58e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1ee5924 81c28c64 nt!KiSwapThread+0x389
        a1ee5970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1ee5bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1ee5d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1ee5d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1ee5d64)
        007cfaa8 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        007cfaac 7744b65b ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        007cfc48 75f33833 ntdll!TppWaiterpThread+0x294 (FPO: [Non-Fpo])
        007cfc54 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        007cfc94 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD a18a9030  Cid 000c.0224  Teb: 7ffdc000 Win32Thread: 00000000 WAIT: (WrLpcReceive)
UserMode Non-Alertable
            a18a9244  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            a18b73a0       Image:         svchost.exe
        Wait Start TickCount      1854           Ticks: 41645 (0:00:10:49.666)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wersvc!CWerService::StaticLpcServerThread (0x728063b7)
        Stack Init a1efa000 Current a1ef9b78 Base a1efa000 Limit a1ef7000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1ef9b90 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1ef9bcc 81c293a7 nt!KiSwapThread+0x389
        a1ef9c2c 81dc3dac nt!KeWaitForSingleObject+0x414
        a1ef9c64 81dc436e nt!AlpcpReceiveMessagePort+0x221
        a1ef9ce0 81dc6211 nt!AlpcpReceiveMessage+0x163
        a1ef9d3c 81c8caaa nt!NtAlpcSendWaitReceivePort+0x11c
        a1ef9d3c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1ef9d64)
        006af68c 7748f2c0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        006af690 72801545 ntdll!NtAlpcSendWaitReceivePort+0xc (FPO: [8,0,0])
        006afbac 728063c4 wersvc!CWerService::LpcServerThread+0x9c (FPO: [Non-Fpo])
        006afbb4 75f33833 wersvc!CWerService::StaticLpcServerThread+0xd (FPO: [Non-Fpo])
        006afbc0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        006afc00 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD a18a9d78  Cid 000c.028c  Teb: 7ffdb000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Alertable
            a18b43d8  QueueObject
        IRP List:
            8367e560: (0006,01d8) Flags: 00060000  Mdl: 00000000
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            a18b73a0       Image:         svchost.exe
        Wait Start TickCount      17983          Ticks: 25516 (0:00:06:38.052)
        Context Switch Count      56
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init a1f12000 Current a1f11bc8 Base a1f12000 Limit a1f0f000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1f11be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1f11c1c 81cad431 nt!KiSwapThread+0x389
        a1f11c68 81d8b982 nt!KeRemoveQueueEx+0x568
        a1f11cc0 81c7a036 nt!IoRemoveIoCompletion+0x23
        a1f11d54 81c8caaa nt!NtWaitForWorkViaWorkerFactory+0x1a1
        a1f11d54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1f11d64)
        0071f6b4 77490850 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0071f6b8 7749a1b4 ntdll!NtWaitForWorkViaWorkerFactory+0xc (FPO: [2,0,0])
        0071f7e0 75f33833 ntdll!TppWorkerThread+0x1f6 (FPO: [Non-Fpo])
        0071f7ec 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0071f82c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

SearchIndexer process

```
PROCESS a18bd670  SessionId: 0  Cid: 01e4    Peb: 7ffd5000  ParentCid: 0214
    DirBase: 29a01380  ObjectTable: a1341848  HandleCount: 595.
    Image: SearchIndexer.exe
    VadRoot 9fdfe2a8 Vads 210 Clone 0 Private 2261. Modified 1656. Locked 1.
    DeviceMap 85a03048
    Token                             a1345ab8
    ElapsedTime                       00:10:49.653
    UserTime                          00:00:00.046
    KernelTime                        00:00:00.062
    QuotaPoolUsage[PagedPool]         124208
    QuotaPoolUsage[NonPagedPool]      10424
    Working Set Sizes (now,min,max)  (2107, 50, 345) (8428KB, 200KB, 1380KB)
    PeakWorkingSetSize                2903
    VirtualSize                       102 Mb
    PeakVirtualSize                   114 Mb
    PageFaultCount                    6323
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      7371

    Setting context for this process...
.process /p /r ffffffffa18bd670
    !peb
PEB at 7ffd5000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00b00000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 001e1748 . 01b52250
    Ldr.InLoadOrderModuleList:           001e16c8 . 01b52240
    Ldr.InMemoryOrderModuleList:         001e16d0 . 01b52248
            Base TimeStamp                     Module
          b00000 4549b667 Nov 02 09:12:07 2006 C:\Windows\system32\SearchIndexer.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        72240000 4549bdfb Nov 02 09:44:27 2006 C:\Windows\system32\TQUERY.DLL
        744e0000 4549bd96 Nov 02 09:42:46 2006 C:\Windows\system32\PROPSYS.dll
        75840000 4549bd53 Nov 02 09:41:39 2006 C:\Windows\system32\NETAPI32.dll
        75ce0000 4549bd99 Nov 02 09:42:49 2006 C:\Windows\system32\PSAPI.DLL
        74ff0000 4549be2f Nov 02 09:45:19 2006 C:\Windows\system32\WINTRUST.dll
        75650000 45b96fde Jan 26 03:05:02 2007 C:\Windows\system32\CRYPT32.dll
        75820000 4549bd41 Nov 02 09:41:21 2006 C:\Windows\system32\MSASN1.dll
        75ba0000 4549bde2 Nov 02 09:44:02 2006 C:\Windows\system32\USERENV.dll
        75b80000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\Secur32.dll
        77580000 462434a3 Apr 17 03:44:51 2007 C:\Windows\system32\imagehlp.dll
        763b0000 4549bdb9 Nov 02 09:43:21 2006 C:\Windows\system32\SHLWAPI.dll
        720e0000 4549bda4 Nov 02 09:43:00 2006 C:\Windows\system32\query.dll
        76560000 4681c95d Jun 27 03:20:13 2007 C:\Windows\system32\SHELL32.dll
        75750000 4549bd14 Nov 02 09:40:36 2006 C:\Windows\system32\MPR.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        74aa0000 4549bd09 Nov 02 09:40:25 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_5d07289e07e1d100\comctl32.dll
        773a0000 4549bce9 Nov 02 09:39:53 2006 C:\Windows\system32\CLBCatQ.DLL
```

```
        729f0000 4549bd4c Nov 02 09:41:32 2006 C:\Windows\system32\msstrc.dll
        75480000 4549bd20 Nov 02 09:40:48 2006 C:\Windows\system32\credssp.dll
        75050000 46773a78 Jun 19 03:07:52 2007 C:\Windows\system32\schannel.dll
        71d40000 4549bd4b Nov 02 09:41:31 2006 C:\Windows\system32\mssrch.dll
        74fe0000 46d779a1 Aug 31 03:14:57 2007 C:\Windows\system32\WTSAPI32.dll
        71f00000 4549bcc9 Nov 02 09:39:21 2006 C:\Windows\system32\dbghelp.dll
        753f0000 4549bde4 Nov 02 09:44:04 2006 C:\Windows\system32\VERSION.dll
        72a00000 4549bd8c Nov 02 09:42:36 2006 C:\Windows\system32\Msidle.dll
        75300000 4549be2e Nov 02 09:45:18 2006 C:\Windows\system32\WINSTA.dll
        75350000 4549bdae Nov 02 09:43:10 2006 C:\Windows\system32\rsaenh.dll
        720a0000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\propdefs.dll
        71a20000 4549b647 Nov 02 09:11:35 2006 C:\Windows\system32\en-us\tQuery.dll.mui
        718b0000 4549bcf9 Nov 02 09:40:09 2006 C:\Windows\system32\esent.dll
        720d0000 4549bd3d Nov 02 09:41:17 2006 C:\Windows\system32\msscb.dll
        75610000 4679de70 Jun 21 03:12:00 2007 C:\Windows\system32\slc.dll
        72cb0000 4549bded Nov 02 09:44:13 2006 C:\Windows\system32\VSSAPI.DLL
        74d00000 4549bcbc Nov 02 09:39:08 2006 C:\Windows\system32\ATL.DLL
        72e50000 4549bdef Nov 02 09:44:15 2006 C:\Windows\system32\vsstrace.dll
        757b0000 4549bccf Nov 02 09:39:27 2006 C:\Windows\system32\AUTHZ.dll
        73a70000 4549be05 Nov 02 09:44:37 2006 C:\Windows\system32\XmlLite.dll
        77030000 4549bdb0 Nov 02 09:43:12 2006 C:\Windows\system32\SETUPAPI.dll
        75ad0000 4549bda8 Nov 02 09:43:04 2006 C:\Windows\system32\SAMLIB.dll
        745a0000 4549bcf8 Nov 02 09:40:08 2006 C:\Windows\system32\es.dll
        75b20000 4549bcaf Nov 02 09:38:55 2006 C:\Windows\system32\apphelp.dll
        75020000 4549bddb Nov 02 09:43:55 2006 C:\Windows\system32\NTMARTA.DLL
        76310000 4549be44 Nov 02 09:45:40 2006 C:\Windows\system32\WLDAP32.dll
        75fe0000 4549be0e Nov 02 09:44:46 2006 C:\Windows\system32\WS2_32.dll
        77550000 4549bdc7 Nov 02 09:43:35 2006 C:\Windows\system32\NSI.dll
        70690000 4549bd41 Nov 02 09:41:21 2006 C:\Windows\System32\NaturalLanguage6.dll
        70e10000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\mssprxy.dll
        75a60000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\SXS.DLL
    SubSystemData:     00000000
    ProcessHeap:       001e0000
    ProcessParameters: 001e0fd8
    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;C:\Program Files\QuickTime\QTSystem\'
    Environment:  0021c268
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\system32\config\systemprofile\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        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:\Program
Files\QuickTime\QTSystem\;C:\Windows\system32
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\ProgramData\Microsoft\Search\Data\Temp\usgthrsvc
        TMP=C:\ProgramData\Microsoft\Search\Data\Temp\usgthrsvc
        USERDOMAIN=WORKGROUP
        USERNAME=HOME$
        USERPROFILE=C:\Windows\system32\config\systemprofile
        windir=C:\Windows
```

```
        THREAD a18bd3c8  Cid 01e4.01e0  Teb: 7ffdf000 Win32Thread: ff525e98 WAIT: (Executive)
UserMode Non-Alertable
            a18ba44c  NotificationEvent
        IRP List:
            835d7a40: (0006,0094) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            a18bd670       Image:         SearchIndexer.exe
        Wait Start TickCount      9163           Ticks: 34336 (0:00:08:55.645)
        Context Switch Count      260
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address SearchIndexer!WinMainCRTStartup (0x00b0b112)
        Stack Init a1ef2000 Current a1ef1bc8 Base a1ef2000 Limit a1eef000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1ef1be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1ef1c1c 81c293a7 nt!KiSwapThread+0x389
        a1ef1c78 81d88faf nt!KeWaitForSingleObject+0x414
        a1ef1cac 81d93669 nt!IopSynchronousServiceTail+0x258
        a1ef1d38 81c8caaa nt!NtReadFile+0x646
        a1ef1d38 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1ef1d64)
        001af6c0 77490080 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        001af6c4 75f3853f ntdll!ZwReadFile+0xc (FPO: [9,0,0])
        001af73c 775cffe2 kernel32!ReadFile+0x20e (FPO: [Non-Fpo])
        001af768 775cfdfb ADVAPI32!ScGetPipeInput+0x2a (FPO: [Non-Fpo])
        001af7d0 775cbdd2 ADVAPI32!ScDispatcherLoop+0x6c (FPO: [Non-Fpo])
        001afa48 00b0b72c ADVAPI32!StartServiceCtrlDispatcherW+0xce (FPO: [Non-Fpo])
        001afa54 00b0b6ad SearchIndexer!CDcomService::ServiceStart+0x12 (FPO: [Non-Fpo])
        001afd00 00b0b355 SearchIndexer!WinMain+0x550 (FPO: [Non-Fpo])
        001afd90 75f33833 SearchIndexer!_initterm_e+0x1a1 (FPO: [Non-Fpo])
        001afd9c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        001afddc 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD a18dc7c0  Cid 01e4.0314  Teb: 7ffde000 Win32Thread: ff50ca68 WAIT: (UserRequest)
UserMode Non-Alertable
            a18ae570  SynchronizationEvent
            a18b9790  SynchronizationEvent
            a18bf1a0  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            a18bd670       Image:         SearchIndexer.exe
        Wait Start TickCount      2057           Ticks: 41442 (0:00:10:46.499)
        Context Switch Count      1166
        UserTime                  00:00:00.078
        KernelTime                00:00:00.046
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x775cb9d5)
        Stack Init a1a47000 Current a1a468d0 Base a1a47000 Limit a1a44000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1a468e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1a46924 81c28c64 nt!KiSwapThread+0x389
        a1a46970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1a46bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1a46d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1a46d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1a46d64)
        0101ecf8 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0101ecfc 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0101ed98 761dc4b7 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0101edec 761d8b83 USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
        0101ee08 00b08416 USER32!MsgWaitForMultipleObjects+0x1f (FPO: [Non-Fpo])
        0101ee48 00b08086 SearchIndexer!MessageLoop+0x47 (FPO: [Non-Fpo])
        0101f7c4 00b08c8d SearchIndexer!CDcomService::Listen+0x14d (FPO: [Non-Fpo])
        0101fc24 775cb9f6 SearchIndexer!CDcomService::ServiceMain+0x1ea (FPO: [Non-Fpo])
        0101fc38 75f33833 ADVAPI32!ScSvcctrlThreadA+0x21 (FPO: [Non-Fpo])
        0101fc44 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0101fc84 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD a18d0420  Cid 01e4.0608  Teb: 7ffdb000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            a18c6f20  SynchronizationEvent
            a18d03e0  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            a18bd670       Image:         SearchIndexer.exe
        Wait Start TickCount      1871           Ticks: 41628 (0:00:10:49.400)
        Context Switch Count      8
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address esent!UtilThreadIThreadBase (0x718da8cd)
        Stack Init a1eae000 Current a1ead8d0 Base a1eae000 Limit a1eab000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1ead8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1ead924 81c28c64 nt!KiSwapThread+0x389
        a1ead970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1eadbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1eadd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1eadd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1eadd64)
        01b0f81c 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01b0f820 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        01b0f8bc 718dc49d kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        01b0f930 718da921 esent!UtilPerfThread+0x9c (FPO: [Non-Fpo])
        01b0f968 75f33833 esent!UtilThreadIThreadBase+0x50 (FPO: [Non-Fpo])
        01b0f974 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01b0f9b4 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 8995e1f8  Cid 01e4.0548  Teb: 7ffda000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            a18f5a40  SynchronizationTimer
            9fdee430  SynchronizationTimer
            9fd327a8  SynchronizationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            a18bd670       Image:         SearchIndexer.exe
        Wait Start TickCount      43271          Ticks: 228 (0:00:00:03.556)
        Context Switch Count      460
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x7744b49a)
        Stack Init 88e38000 Current 88e378d0 Base 88e38000 Limit 88e35000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        88e378e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        88e37924 81c28c64 nt!KiSwapThread+0x389
        88e37970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        88e37bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        88e37d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        88e37d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 88e37d64)
        037bf9bc 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        037bf9c0 7744b65b ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        037bfb5c 75f33833 ntdll!TppWaiterpThread+0x294 (FPO: [Non-Fpo])
        037bfb68 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        037bfba8 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 89856ca8  Cid 01e4.05c0  Teb: 7ffd9000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            a18d0868  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            a18bd670       Image:         SearchIndexer.exe
        Wait Start TickCount      19298          Ticks: 24201 (0:00:06:17.538)
        Context Switch Count      210
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address esent!UtilThreadIThreadBase (0x718da8cd)
        Stack Init a1e7e000 Current a1e7dbc8 Base a1e7e000 Limit a1e7b000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1e7dbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1e7dc1c 81cad431 nt!KiSwapThread+0x389
        a1e7dc6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a1e7dcc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a1e7dd48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a1e7dd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1e7dd64)
        0387fd1c 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0387fd20 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        0387fd4c 718fce15 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        0387fd84 718dd405 esent!CTaskManager::TMIDispatch+0x59 (FPO: [Non-Fpo])
        0387fd90 718da921 esent!CTaskManager::TMDispatch+0x14 (FPO: [Non-Fpo])
        0387fdc8 75f33833 esent!UtilThreadIThreadBase+0x50 (FPO: [Non-Fpo])
        0387fdd4 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0387fe14 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD a1d3d6f0  Cid 01e4.061c  Teb: 7ffd8000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fdf1d70  NotificationEvent
            898629a0  NotificationEvent
        IRP List:
            9fdf1a48: (0006,0094) Flags: 00060800  Mdl: 00000000
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            a18bd670       Image:         SearchIndexer.exe
        Wait Start TickCount      1925           Ticks: 41574 (0:00:10:48.558)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address TQUERY!CThread::_ThreadFunction (0x72295195)
        Stack Init a1e92000 Current a1e918d0 Base a1e92000 Limit a1e8f000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1e918e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1e91924 81c28c64 nt!KiSwapThread+0x389
        a1e91970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1e91bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1e91d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1e91d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1e91d64)
        0396f67c 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0396f680 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0396f71c 7226958e kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0396f7c4 72295dfb TQUERY!CRequestQueue::DoWork+0xf4 (FPO: [Non-Fpo])
        0396f7f8 722951c4 TQUERY!CCiQueryServer::QueryServerThreadProc+0x26 (FPO: [Non-Fpo])
        0396f830 75f33833 TQUERY!CThread::_ThreadFunction+0x2f (FPO: [Non-Fpo])
        0396f83c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0396f87c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fdc4d78  Cid 01e4.07cc  Teb: 7ffd6000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            a18bfe78  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            a18bd670       Image:         SearchIndexer.exe
        Wait Start TickCount      1934           Ticks: 41565 (0:00:10:48.418)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address mssrch!CHostHitTimingThread::Thread (0x71d976d0)
        Stack Init a1ea2000 Current a1ea1c38 Base a1ea2000 Limit a1e9f000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1ea1c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1ea1c8c 81c293a7 nt!KiSwapThread+0x389
        a1ea1ce8 81df5057 nt!KeWaitForSingleObject+0x414
        a1ea1d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a1ea1d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1ea1d64)
        03c7f814 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        03c7f818 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        03c7f888 71d97719 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        03c7f8bc 75f33833 mssrch!CHostHitTimingThread::Thread+0x41 (FPO: [Non-Fpo])
        03c7f8c8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        03c7f908 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fdc4a78  Cid 01e4.073c  Teb: 7ffd4000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            a18bfe48  SynchronizationEvent
            9fdc4b00  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            a18bd670       Image:         SearchIndexer.exe
        Wait Start TickCount      42966          Ticks: 533 (0:00:00:08.314)
        Context Switch Count      85
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address mssrch!CTimerThread::Thread (0x71d45446)
        Stack Init a1e6a000 Current a1e69c38 Base a1e6a000 Limit a1e67000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a1e69c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1e69c8c 81c293a7 nt!KiSwapThread+0x389
        a1e69ce8 81df5057 nt!KeWaitForSingleObject+0x414
        a1e69d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a1e69d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1e69d64)
        03b6f7cc 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        03b6f7d0 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        03b6f840 71d455a2 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        03b6f878 75f33833 mssrch!CTimerThread::Thread+0x1a8 (FPO: [Non-Fpo])
        03b6f884 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        03b6f8c4 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fdc4750  Cid 01e4.0124  Teb: 7ffd3000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            a18bfa10  SynchronizationEvent
            9fdc47d8  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            a18bd670       Image:         SearchIndexer.exe
        Wait Start TickCount      43497          Ticks: 2 (0:00:00:00.031)
        Context Switch Count      1169
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address mssrch!CBackoffTimerThread::Thread (0x71d42e5f)
        Stack Init a1e76000 Current a1e75c38 Base a1e76000 Limit a1e73000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a1e75c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1e75c8c 81c293a7 nt!KiSwapThread+0x389
        a1e75ce8 81df5057 nt!KeWaitForSingleObject+0x414
        a1e75d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a1e75d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1e75d64)
        03d5eeac 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        03d5eeb0 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        03d5ef20 71d42ee2 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        03d5f8a8 75f33833 mssrch!CBackoffTimerThread::Thread+0x83 (FPO: [Non-Fpo])
        03d5f8b4 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        03d5f8f4 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD a1801030  Cid 01e4.074c  Teb: 7ffaf000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            a18c08c0  NotificationEvent
            a18c0890  NotificationEvent
            89862300  NotificationEvent
        IRP List:
            83688e28: (0006,01d8) Flags: 00060800  Mdl: 836d3630
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            a18bd670       Image:         SearchIndexer.exe
        Wait Start TickCount      40456          Ticks: 3043 (0:00:00:47.471)
        Context Switch Count      386
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address mssrch!CUsnMonitorNotifier::MonitorThreadStatic (0x71d7ac27)
        Stack Init a1e86000 Current a1e858d0 Base a1e86000 Limit a1e83000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a1e858e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1e85924 81c28c64 nt!KiSwapThread+0x389
        a1e85970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1e85bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1e85d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1e85d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1e85d64)
        03e1e4f0 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        03e1e4f4 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        03e1e590 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        03e1e5ac 71d46640 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        03e1e5c4 71d464bd mssrch!CWaitForMultipleObjects::Wait+0x15 (FPO: [Non-Fpo])
        03e1f7e4 71d7ac4e mssrch!CUsnMonitorNotifier::Thread+0x382 (FPO: [Non-Fpo])
        03e1f814 75f33833 mssrch!CUsnMonitorNotifier::MonitorThreadStatic+0x27 (FPO: [Non-Fpo])
        03e1f820 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        03e1f860 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9e1d45f8  Cid 01e4.0ee4  Teb: 7ffa8000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            a18ad6d0  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            a18bd670       Image:         SearchIndexer.exe
        Wait Start TickCount      34678          Ticks: 8821 (0:00:02:17.608)
        Context Switch Count      77
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init a8f7c000 Current a8f7bbc8 Base a8f7c000 Limit a8f79000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a8f7bbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8f7bc1c 81cad431 nt!KiSwapThread+0x389
        a8f7bc6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a8f7bcc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a8f7bd48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a8f7bd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8f7bd64)
        046bfc18 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        046bfc1c 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        046bfc48 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        046bfc84 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        046bfcf0 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        046bfcfc 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        046bfd24 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        046bfd30 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        046bfd3c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        046bfd7c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 834bcd78  Cid 01e4.0bac  Teb: 7ffd7000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Alertable
            9fdc5c88  QueueObject
            834bce00  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            a18bd670       Image:         SearchIndexer.exe
        Wait Start TickCount      43271          Ticks: 228 (0:00:00:03.556)
        Context Switch Count      14
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init a089f000 Current a089ebc8 Base a089f000 Limit a089c000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a089ebe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a089ec1c 81cad431 nt!KiSwapThread+0x389
        a089ec68 81d8b982 nt!KeRemoveQueueEx+0x568
        a089ecc0 81c7a036 nt!IoRemoveIoCompletion+0x23
        a089ed54 81c8caaa nt!NtWaitForWorkViaWorkerFactory+0x1a1
        a089ed54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a089ed64)
        03e9f8d0 77490850 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        03e9f8d4 7749a1b4 ntdll!NtWaitForWorkViaWorkerFactory+0xc (FPO: [2,0,0])
        03e9f9fc 75f33833 ntdll!TppWorkerThread+0x1f6 (FPO: [Non-Fpo])
        03e9fa08 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        03e9fa48 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 8371b2c0  Cid 01e4.0b08  Teb: 7ffdc000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Alertable
            9fdc5c88  QueueObject
            8371b348  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            a18bd670       Image:         SearchIndexer.exe
        Wait Start TickCount      43271          Ticks: 228 (0:00:00:03.556)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init 9e8bf000 Current 9e8bebc8 Base 9e8bf000 Limit 9e8bc000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9e8bebe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e8bec1c 81cad431 nt!KiSwapThread+0x389
        9e8bec68 81d8b982 nt!KeRemoveQueueEx+0x568
        9e8becc0 81c7a036 nt!IoRemoveIoCompletion+0x23
        9e8bed54 81c8caaa nt!NtWaitForWorkViaWorkerFactory+0x1a1
        9e8bed54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9e8bed64)
        042afcf0 77490850 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        042afcf4 7749a1b4 ntdll!NtWaitForWorkViaWorkerFactory+0xc (FPO: [2,0,0])
        042afe1c 75f33833 ntdll!TppWorkerThread+0x1f6 (FPO: [Non-Fpo])
        042afe28 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        042afe68 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Taskeng process (session 0)

```
PROCESS 89860020  SessionId: 0  Cid: 01f8    Peb: 7ffd7000  ParentCid: 03cc
    DirBase: 29a013a0  ObjectTable: a1325d40  HandleCount: 123.
    Image: taskeng.exe
    VadRoot 9fdeebe0 Vads 86 Clone 0 Private 332. Modified 161. Locked 0.
    DeviceMap 85a03048
    Token                             a2846030
    ElapsedTime                       00:10:46.440
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.015
    QuotaPoolUsage[PagedPool]         84784
    QuotaPoolUsage[NonPagedPool]      4424
    Working Set Sizes (now,min,max)  (1082, 50, 345) (4328KB, 200KB, 1380KB)
    PeakWorkingSetSize                1271
    VirtualSize                       43 Mb
    PeakVirtualSize                   45 Mb
    PageFaultCount                    1383
    MemoryPriority                    BACKGROUND
    BasePriority                      6
    CommitCharge                      454

    Setting context for this process...
.process /p /r ffffffff89860020

    !peb
PEB at 7ffd7000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00e90000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 000b1758 . 000c8f78
    Ldr.InLoadOrderModuleList:           000b16d8 . 000c9668
    Ldr.InMemoryOrderModuleList:         000b16e0 . 000c9670
            Base TimeStamp                     Module
          e90000 4549af28 Nov 02 08:41:12 2006 C:\Windows\system32\taskeng.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        76560000 4681c95d Jun 27 03:20:13 2007 C:\Windows\system32\SHELL32.dll
        763b0000 4549bdb9 Nov 02 09:43:21 2006 C:\Windows\system32\SHLWAPI.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        75b80000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\Secur32.dll
        73a70000 4549be05 Nov 02 09:44:37 2006 C:\Windows\system32\XmlLite.dll
        75750000 4549bd14 Nov 02 09:40:36 2006 C:\Windows\system32\MPR.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        74aa0000 4549bd09 Nov 02 09:40:25 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_5d07289e07e1d100\comctl32.dll
        75350000 4549bdae Nov 02 09:43:10 2006 C:\Windows\system32\rsaenh.dll
        773a0000 4549bce9 Nov 02 09:39:53 2006 C:\Windows\system32\CLBCatQ.DLL
        71af0000 4549be04 Nov 02 09:44:36 2006 C:\Windows\system32\tschannel.dll
        737b0000 4549bcd4 Nov 02 09:39:32 2006 C:\Windows\system32\dimsjob.dll
        75ba0000 4549bde2 Nov 02 09:44:02 2006 C:\Windows\system32\USERENV.dll
        754f0000 4549bd49 Nov 02 09:41:29 2006 C:\Windows\system32\ncrypt.dll
        75650000 45b96fde Jan 26 03:05:02 2007 C:\Windows\system32\CRYPT32.dll
        75820000 4549bd41 Nov 02 09:41:21 2006 C:\Windows\system32\MSASN1.dll
        75330000 4549bcd7 Nov 02 09:39:35 2006 C:\Windows\system32\GPAPI.dll
```

```
        75610000 4679de70 Jun 21 03:12:00 2007 C:\Windows\system32\slc.dll
        71ae0000 4549bd8e Nov 02 09:42:38 2006 C:\Windows\system32\pautoenr.dll
        75840000 4549bd53 Nov 02 09:41:39 2006 C:\Windows\system32\NETAPI32.dll
        75ce0000 4549bd99 Nov 02 09:42:49 2006 C:\Windows\system32\PSAPI.DLL
        76310000 4549be44 Nov 02 09:45:40 2006 C:\Windows\system32\WLDAP32.dll
        75fe0000 4549be0e Nov 02 09:44:46 2006 C:\Windows\system32\WS2_32.dll
        77550000 4549bdc7 Nov 02 09:43:35 2006 C:\Windows\system32\NSI.dll
        71850000 4549bccc Nov 02 09:39:24 2006 C:\Windows\system32\certcli.dll
        74d00000 4549bcbc Nov 02 09:39:08 2006 C:\Windows\system32\ATL.DLL
        76020000 470c4e1e Oct 10 04:59:26 2007 C:\Windows\system32\WININET.dll
        76010000 4549ad42 Nov 02 08:33:06 2006 C:\Windows\system32\Normaliz.dll
        76360000 4549bcfb Nov 02 09:40:11 2006 C:\Windows\system32\iertutil.dll
        71640000 4549bccf Nov 02 09:39:27 2006 C:\Windows\system32\certenroll.dll
        75780000 4549bdcc Nov 02 09:43:40 2006 C:\Windows\system32\NTDSAPI.dll
        75af0000 4549bcf1 Nov 02 09:40:01 2006 C:\Windows\system32\DNSAPI.dll
        73ce0000 4549be24 Nov 02 09:45:08 2006 C:\Windows\system32\WinSCard.dll
        74fe0000 46d779a1 Aug 31 03:14:57 2007 C:\Windows\system32\WTSAPI32.dll
        75300000 4549be2e Nov 02 09:45:18 2006 C:\Windows\system32\WINSTA.dll
    SubSystemData:     00000000
    ProcessHeap:       000b0000
    ProcessParameters: 000b0fd8
    WindowTitle:  'taskeng.exe'
    ImageFile:    'C:\Windows\system32\taskeng.exe'
    CommandLine:  'taskeng.exe {73A0C1B4-D81F-4C69-859A-175F136E995E}'
    DllPath:
'C:\Windows\system32;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Wind
ows;C:\Windows\System32\Wbem;C:\Program Files\QuickTime\QTSystem\'
    Environment:  000b07e8
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\system32\config\systemprofile\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        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:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\TEMP
        TMP=C:\Windows\TEMP
        USERDOMAIN=WORKGROUP
        USERNAME=HOME$
        USERPROFILE=C:\Windows\system32\config\systemprofile
        windir=C:\Windows
```

```
        THREAD 89854cd8  Cid 01f8.05b0  Teb: 7ffdf000 Win32Thread: ff529250 WAIT: (UserRequest)
UserMode Non-Alertable
            9fde9520  SynchronizationEvent
            847ac660  SynchronizationTimer
            847ac5a8  SynchronizationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            89860020       Image:         taskeng.exe
        Wait Start TickCount      30914          Ticks: 12585 (0:00:03:16.327)
        Context Switch Count      121
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address taskeng!wWinMainCRTStartup (0x00e9adb0)
        Stack Init a1e9e000 Current a1e9d8d0 Base a1e9e000 Limit a1e9b000 Call 0
        Priority 8 BasePriority 6 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1e9d8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1e9d924 81c28c64 nt!KiSwapThread+0x389
        a1e9d970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1e9dbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1e9dd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1e9dd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1e9dd64)
        0025fa34 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0025fa38 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0025fad4 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0025faf0 00e91806 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0025fb80 00e9919c taskeng!Session::CentralControlLoop+0x7a (FPO: [Non-Fpo])
        0025fc38 00e992e4 taskeng!RunSession+0x5f (FPO: [Non-Fpo])
        0025fc88 00e99456 taskeng!wWinMain+0x157 (FPO: [Non-Fpo])
        0025fd1c 75f33833 taskeng!_initterm_e+0x1b1 (FPO: [Non-Fpo])
        0025fd28 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0025fd68 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 847ab030  Cid 01f8.0804  Teb: 7ffde000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            847a9408  SynchronizationTimer
            847aab30  SynchronizationEvent
            847aed78  Thread
            8987ef68  SynchronizationTimer
            8987fab8  SynchronizationTimer
            847abd00  SynchronizationEvent
            847ac2a0  SynchronizationEvent
            847acbb0  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            89860020       Image:         taskeng.exe
        Wait Start TickCount      2711           Ticks: 40788 (0:00:10:36.296)
        Context Switch Count      13
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x7744b49a)
        Stack Init a1e5a000 Current a1e598d0 Base a1e5a000 Limit a1e57000 Call 0
        Priority 10 BasePriority 6 PriorityDecrement 4 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1e598e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1e59924 81c28c64 nt!KiSwapThread+0x389
        a1e59970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1e59bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1e59d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1e59d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1e59d64)
        00e4fd04 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00e4fd08 7744b65b ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00e4fea4 75f33833 ntdll!TppWaiterpThread+0x294 (FPO: [Non-Fpo])
        00e4feb0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00e4fef0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 847abd78  Cid 01f8.0808  Teb: 7ffdd000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Alertable
            89862020  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            89860020       Image:         taskeng.exe
        Wait Start TickCount      2711           Ticks: 40788 (0:00:10:36.296)
        Context Switch Count      6
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init a1e62000 Current a1e61bc8 Base a1e62000 Limit a1e5f000 Call 0
        Priority 7 BasePriority 6 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1e61be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1e61c1c 81cad431 nt!KiSwapThread+0x389
        a1e61c68 81d8b982 nt!KeRemoveQueueEx+0x568
        a1e61cc0 81c7a036 nt!IoRemoveIoCompletion+0x23
        a1e61d54 81c8caaa nt!NtWaitForWorkViaWorkerFactory+0x1a1
        a1e61d54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1e61d64)
        008efe1c 77490850 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        008efe20 7749a1b4 ntdll!NtWaitForWorkViaWorkerFactory+0xc (FPO: [2,0,0])
        008eff48 75f33833 ntdll!TppWorkerThread+0x1f6 (FPO: [Non-Fpo])
        008eff54 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        008eff94 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 847aed78  Cid 01f8.081c  Teb: 7ffd9000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            8994df98  NotificationEvent
            9fc9b1f8  SynchronizationEvent
            8988a360  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            89860020       Image:         taskeng.exe
        Wait Start TickCount      2068           Ticks: 41431 (0:00:10:46.327)
        Context Switch Count      36
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address taskeng!Job::RunCallback (0x00e91fbf)
        Stack Init a1e2a000 Current a1e298d0 Base a1e2a000 Limit a1e27000 Call 0
        Priority 8 BasePriority 6 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1e298e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1e29924 81c28c64 nt!KiSwapThread+0x389
        a1e29970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1e29bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1e29d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1e29d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1e29d64)
        0110f830 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0110f834 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0110f8d0 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0110f8ec 00e91b6e kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0110f968 00e91fed taskeng!Job::Run+0x179 (FPO: [Non-Fpo])
        0110f9ac 75f33833 taskeng!Job::RunCallback+0x8c (FPO: [Non-Fpo])
        0110f9b8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0110f9f8 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 837d3778  Cid 01f8.0fc8  Teb: 7ffd8000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            847ac200  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            89860020       Image:         taskeng.exe
        Wait Start TickCount      27131          Ticks: 16368 (0:00:04:15.342)
        Context Switch Count      6
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init a1e96000 Current a1e95bc8 Base a1e96000 Limit a1e93000 Call 0
        Priority 7 BasePriority 6 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1e95be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1e95c1c 81cad431 nt!KiSwapThread+0x389
        a1e95c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a1e95cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a1e95d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a1e95d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1e95d64)
        012ff950 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        012ff954 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        012ff980 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        012ff9bc 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        012ffa28 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        012ffa34 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        012ffa58 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        012ffa64 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        012ffa70 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        012ffab0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Taskeng process (session 1)

```
PROCESS 8346d618  SessionId: 1  Cid: 0b14    Peb: 7ffd5000  ParentCid: 03cc
    DirBase: 29a013e0  ObjectTable: a8a766e8  HandleCount: 338.
    Image: taskeng.exe
    VadRoot 83606cd8 Vads 167 Clone 0 Private 814. Modified 0. Locked 0.
    DeviceMap a7766db8
    Token                             a83fa030
    ElapsedTime                       00:08:55.586
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         116496
    QuotaPoolUsage[NonPagedPool]      9392
    Working Set Sizes (now,min,max)  (2412, 50, 345) (9648KB, 200KB, 1380KB)
    PeakWorkingSetSize                2436
    VirtualSize                       67 Mb
    PeakVirtualSize                   73 Mb
    PageFaultCount                    3318
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      2341

    Setting context for this process...
.process /p /r ffffffff8346d618

    !peb
PEB at 7ffd5000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00e90000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 001517c0 . 001ae8e0
    Ldr.InLoadOrderModuleList:           00151740 . 001aea20
    Ldr.InMemoryOrderModuleList:         00151748 . 001aea28
            Base TimeStamp                     Module
          e90000 4549af28 Nov 02 08:41:12 2006 C:\Windows\system32\taskeng.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        76560000 4681c95d Jun 27 03:20:13 2007 C:\Windows\system32\SHELL32.dll
        763b0000 4549bdb9 Nov 02 09:43:21 2006 C:\Windows\system32\SHLWAPI.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        75b80000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\Secur32.dll
        73a70000 4549be05 Nov 02 09:44:37 2006 C:\Windows\system32\XmlLite.dll
        75750000 4549bd14 Nov 02 09:40:36 2006 C:\Windows\system32\MPR.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        74aa0000 4549bd09 Nov 02 09:40:25 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_5d07289e07e1d100\comctl32.dll
        75350000 4549bdae Nov 02 09:43:10 2006 C:\Windows\system32\rsaenh.dll
        773a0000 4549bce9 Nov 02 09:39:53 2006 C:\Windows\system32\CLBCatQ.DLL
        71af0000 4549be04 Nov 02 09:44:36 2006 C:\Windows\system32\tschannel.dll
        746d0000 4549bde7 Nov 02 09:44:07 2006 C:\Windows\system32\uxtheme.dll
        71450000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\System32\HotStartUserAgent.dll
        75610000 4679de70 Jun 21 03:12:00 2007 C:\Windows\System32\slc.dll
        71480000 4549bdb7 Nov 02 09:43:19 2006 C:\Windows\System32\PlaySndSrv.dll
        738c0000 4549be1d Nov 02 09:45:01 2006 C:\Windows\System32\WINMM.dll
        73880000 4549bd93 Nov 02 09:42:43 2006 C:\Windows\System32\OLEACC.dll
```

```
        737b0000 4549bcd4 Nov 02 09:39:32 2006 C:\Windows\system32\dimsjob.dll
        75ba0000 4549bde2 Nov 02 09:44:02 2006 C:\Windows\system32\USERENV.dll
        754f0000 4549bd49 Nov 02 09:41:29 2006 C:\Windows\system32\ncrypt.dll
        75650000 45b96fde Jan 26 03:05:02 2007 C:\Windows\system32\CRYPT32.dll
        75820000 4549bd41 Nov 02 09:41:21 2006 C:\Windows\system32\MSASN1.dll
        71460000 4549bd4d Nov 02 09:41:33 2006 C:\Windows\system32\MsCtfMonitor.dll
        70f20000 4549bd5c Nov 02 09:41:48 2006 C:\Windows\system32\MSUTB.dll
        71490000 4549bd24 Nov 02 09:40:52 2006 C:\Windows\system32\dwmapi.dll
        75330000 4549bcd7 Nov 02 09:39:35 2006 C:\Windows\system32\GPAPI.dll
        71ae0000 4549bd8e Nov 02 09:42:38 2006 C:\Windows\system32\pautoenr.dll
        75840000 4549bd53 Nov 02 09:41:39 2006 C:\Windows\system32\NETAPI32.dll
        75ce0000 4549bd99 Nov 02 09:42:49 2006 C:\Windows\system32\PSAPI.DLL
        76310000 4549be44 Nov 02 09:45:40 2006 C:\Windows\system32\WLDAP32.dll
        75fe0000 4549be0e Nov 02 09:44:46 2006 C:\Windows\system32\WS2_32.dll
        77550000 4549bdc7 Nov 02 09:43:35 2006 C:\Windows\system32\NSI.dll
        71850000 4549bccc Nov 02 09:39:24 2006 C:\Windows\system32\certcli.dll
        74d00000 4549bcbc Nov 02 09:39:08 2006 C:\Windows\system32\ATL.DLL
        76020000 470c4e1e Oct 10 04:59:26 2007 C:\Windows\system32\WININET.dll
        76010000 4549ad42 Nov 02 08:33:06 2006 C:\Windows\system32\Normaliz.dll
        76360000 4549bcfb Nov 02 09:40:11 2006 C:\Windows\system32\iertutil.dll
        71640000 4549bccf Nov 02 09:39:27 2006 C:\Windows\system32\certenroll.dll
        75780000 4549bdcc Nov 02 09:43:40 2006 C:\Windows\system32\NTDSAPI.dll
        75af0000 4549bcf1 Nov 02 09:40:01 2006 C:\Windows\system32\DNSAPI.dll
        73ce0000 4549be24 Nov 02 09:45:08 2006 C:\Windows\system32\WinSCard.dll
        74fe0000 46d779a1 Aug 31 03:14:57 2007 C:\Windows\system32\WTSAPI32.dll
        75300000 4549be2e Nov 02 09:45:18 2006 C:\Windows\system32\WINSTA.dll
        737f0000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\wdmaud.drv
        73870000 4549bd89 Nov 02 09:42:33 2006 C:\Windows\system32\ksuser.dll
        75390000 4549bcdc Nov 02 09:39:40 2006 C:\Windows\system32\AVRT.dll
        74d90000 4549bd03 Nov 02 09:40:19 2006 C:\Windows\system32\MMDevAPI.DLL
        77030000 4549bdb0 Nov 02 09:43:12 2006 C:\Windows\system32\SETUPAPI.dll
        74ff0000 4549be2f Nov 02 09:45:19 2006 C:\Windows\system32\WINTRUST.dll
        77580000 462434a3 Apr 17 03:44:51 2007 C:\Windows\system32\imagehlp.dll
        736d0000 4549bcc2 Nov 02 09:39:14 2006 C:\Windows\System32\audioses.dll
        73540000 4549bcc0 Nov 02 09:39:12 2006 C:\Windows\System32\audioeng.dll
        73860000 4549bd2f Nov 02 09:41:03 2006 C:\Windows\system32\msacm32.drv
        73790000 4549bd2e Nov 02 09:41:02 2006 C:\Windows\system32\MSACM32.dll
        736c0000 4549bd27 Nov 02 09:40:55 2006 C:\Windows\system32\miUserNamep.dll
        70830000 4549bdf7 Nov 02 09:44:23 2006 C:\Windows\System32\TMM.dll
        75290000 4549bdd0 Nov 02 09:43:44 2006 C:\Windows\System32\POWRPROF.dll
        70f50000 4549bcc1 Nov 02 09:39:13 2006 C:\Windows\System32\d3d9.dll
        753f0000 4549bde4 Nov 02 09:44:04 2006 C:\Windows\System32\VERSION.dll
        71470000 4549bcc0 Nov 02 09:39:12 2006 C:\Windows\System32\d3d8thk.dll
        10000000 468136d2 Jun 26 16:54:58 2007 C:\Windows\system32\igfxTMM.dll
        6e9b0000 4549bd97 Nov 02 09:42:47 2006 C:\Windows\System32\QAgent.dll
        709f0000 4549bda5 Nov 02 09:43:01 2006 C:\Windows\System32\QUtil.dll
        755d0000 4549bdf6 Nov 02 09:44:22 2006 C:\Windows\System32\wevtapi.dll
        735b0000 4549bce0 Nov 02 09:39:44 2006 C:\Windows\System32\fwpuclnt.dll
    SubSystemData:     00000000
    ProcessHeap:       00150000
    ProcessParameters: 00150fd8
    WindowTitle:  'taskeng.exe'
    ImageFile:    'C:\Windows\system32\taskeng.exe'
    CommandLine:  'taskeng.exe {34007B7D-784F-48E6-963B-9797164C4676}'
    DllPath:
'C:\Windows\system32;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Wind
ows;C:\Windows\System32\Wbem;C:\Program Files\QuickTime\QTSystem\'
    Environment:  001507e8
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\UserName\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        HOMEDRIVE=C:
        HOMEPATH=\Users\UserName
        LOCALAPPDATA=C:\Users\UserName\AppData\Local
        LOGONSERVER=\\HOME
        NUMBER_OF_PROCESSORS=2
```

```
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Users\UserName\AppData\Local\Temp
        TMP=C:\Users\UserName\AppData\Local\Temp
        USERDOMAIN=home
        USERNAME=UserName
        USERPROFILE=C:\Users\UserName
        windir=C:\Windows


        THREAD 83485030  Cid 0b14.0b18  Teb: 7ffdf000 Win32Thread: ff7786b8 WAIT: (UserRequest)
UserMode Non-Alertable
            836218e8  SynchronizationEvent
            83621800  SynchronizationTimer
            83621748  SynchronizationTimer
            835680b8  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8346d618       Image:         taskeng.exe
        Wait Start TickCount      38021          Ticks: 5478 (0:00:01:25.457)
        Context Switch Count      174
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address taskeng!wWinMainCRTStartup (0x00e9adb0)
        Stack Init a098d000 Current a098c8d0 Base a098d000 Limit a098a000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a098c8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a098c924 81c28c64 nt!KiSwapThread+0x389
        a098c970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a098cbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a098cd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a098cd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a098cd64)
        000cf554 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        000cf558 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        000cf5f4 761dc4b7 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        000cf648 761d8b83 USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
        000cf664 00e9148d USER32!MsgWaitForMultipleObjects+0x1f (FPO: [Non-Fpo])
        000cf6f8 00e9919c taskeng!Session::CentralControlLoop+0x7a (FPO: [Non-Fpo])
        000cf7b0 00e992e4 taskeng!RunSession+0x5f (FPO: [Non-Fpo])
        000cf800 00e99456 taskeng!wWinMain+0x157 (FPO: [Non-Fpo])
        000cf894 75f33833 taskeng!_initterm_e+0x1b1 (FPO: [Non-Fpo])
        000cf8a0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        000cf8e0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 83604a58  Cid 0b14.0b38  Teb: 7ffde000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            83606070  SynchronizationTimer
            83605210  SynchronizationEvent
            8360ed78  Thread
            835d4850  Thread
            835f85c0  Thread
            835bf760  SynchronizationTimer
            835bf6a8  SynchronizationTimer
            835f8580  SynchronizationEvent
            83592da8  SynchronizationEvent
            835d7030  Thread
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8346d618       Image:         taskeng.exe
        Wait Start TickCount      9681           Ticks: 33818 (0:00:08:47.564)
        Context Switch Count      37
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x7744b49a)
        Stack Init 9f2e0000 Current 9f2df8d0 Base 9f2e0000 Limit 9f2dd000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f2df8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f2df924 81c28c64 nt!KiSwapThread+0x389
        9f2df970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f2dfbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f2dfd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f2dfd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f2dfd64)
        00c8f624 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00c8f628 7744b65b ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00c8f7c4 75f33833 ntdll!TppWaiterpThread+0x294 (FPO: [Non-Fpo])
        00c8f7d0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00c8f810 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 835e8ca8  Cid 0b14.0b3c  Teb: 7ffdd000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Alertable
            83604d00  QueueObject
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8346d618       Image:         taskeng.exe
        Wait Start TickCount      9167           Ticks: 34332 (0:00:08:55.582)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init a3120000 Current a311fbc8 Base a3120000 Limit a311d000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a311fbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a311fc1c 81cad431 nt!KiSwapThread+0x389
        a311fc68 81d8b982 nt!KeRemoveQueueEx+0x568
        a311fcc0 81c7a036 nt!IoRemoveIoCompletion+0x23
        a311fd54 81c8caaa nt!NtWaitForWorkViaWorkerFactory+0x1a1
        a311fd54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a311fd64)
        00dcf6cc 77490850 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00dcf6d0 7749a1b4 ntdll!NtWaitForWorkViaWorkerFactory+0xc (FPO: [2,0,0])
        00dcf7f8 75f33833 ntdll!TppWorkerThread+0x1f6 (FPO: [Non-Fpo])
        00dcf804 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00dcf844 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 83622030  Cid 0b14.0b50  Teb: 7ffdc000 Win32Thread: ff35f860 WAIT: (WrQueue)
UserMode Non-Alertable
            836073f0  QueueObject
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8346d618       Image:         taskeng.exe
        Wait Start TickCount      34218          Ticks: 9281 (0:00:02:24.784)
        Context Switch Count      870
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init a3114000 Current a3113bc8 Base a3114000 Limit a3111000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a3113be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a3113c1c 81cad431 nt!KiSwapThread+0x389
        a3113c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a3113cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a3113d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a3113d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a3113d64)
        00d8f908 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00d8f90c 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        00d8f938 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        00d8f974 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        00d8f9e0 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        00d8f9ec 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        00d8fa14 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        00d8fa20 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        00d8fa2c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00d8fa6c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 8360ed78  Cid 0b14.0b68  Teb: 7ffd8000 Win32Thread: ff288b48 WAIT: (UserRequest)
UserMode Non-Alertable
            9fcce410  NotificationEvent
            8360dc68  SynchronizationEvent
            9fc71c90  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8346d618       Image:         taskeng.exe
        Wait Start TickCount      9187           Ticks: 34312 (0:00:08:55.270)
        Context Switch Count      23
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address taskeng!Job::RunCallback (0x00e91fbf)
        Stack Init a1af5000 Current a1af48d0 Base a1af5000 Limit a1af2000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1af48e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1af4924 81c28c64 nt!KiSwapThread+0x389
        a1af4970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1af4bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1af4d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1af4d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1af4d64)
        0013fc14 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0013fc18 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0013fcb4 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0013fcd0 00e91b6e kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0013fd4c 00e91fed taskeng!Job::Run+0x179 (FPO: [Non-Fpo])
        0013fd90 75f33833 taskeng!Job::RunCallback+0x8c (FPO: [Non-Fpo])
        0013fd9c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0013fddc 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 835d4850  Cid 0b14.0b78  Teb: 7ffd7000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            835e8100  NotificationEvent
            83618b18  SynchronizationEvent
            83618b70  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8346d618       Image:         taskeng.exe
        Wait Start TickCount      9190           Ticks: 34309 (0:00:08:55.223)
        Context Switch Count      121
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address taskeng!Job::RunCallback (0x00e91fbf)
        Stack Init a1b4c000 Current a1b4b8d0 Base a1b4c000 Limit a1b49000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1b4b8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1b4b924 81c28c64 nt!KiSwapThread+0x389
        a1b4b970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1b4bbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1b4bd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1b4bd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1b4bd64)
        012af918 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        012af91c 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        012af9b8 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        012af9d4 00e91b6e kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        012afa50 00e91fed taskeng!Job::Run+0x179 (FPO: [Non-Fpo])
        012afa94 75f33833 taskeng!Job::RunCallback+0x8c (FPO: [Non-Fpo])
        012afaa0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        012afae0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 835f85c0  Cid 0b14.0b80  Teb: 7ffd6000 Win32Thread: ff351430 WAIT: (UserRequest)
UserMode Non-Alertable
            835e8160  NotificationEvent
            83618270  SynchronizationEvent
            83606558  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8346d618       Image:         taskeng.exe
        Wait Start TickCount      9189           Ticks: 34310 (0:00:08:55.239)
        Context Switch Count      8
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address taskeng!Job::RunCallback (0x00e91fbf)
        Stack Init 85868000 Current 858678d0 Base 85868000 Limit 85865000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        858678e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        85867924 81c28c64 nt!KiSwapThread+0x389
        85867970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        85867bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        85867d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        85867d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 85867d64)
        015af758 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        015af75c 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        015af7f8 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        015af814 00e91b6e kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        015af890 00e91fed taskeng!Job::Run+0x179 (FPO: [Non-Fpo])
        015af8d4 75f33833 taskeng!Job::RunCallback+0x8c (FPO: [Non-Fpo])
        015af8e0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        015af920 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 8360d8d8  Cid 0b14.0b84  Teb: 7ffd4000 Win32Thread: ff77c330 WAIT: (UserRequest)
UserMode Non-Alertable
            8360b460  NotificationEvent
            8360b490  NotificationEvent
            8360b628  NotificationEvent
            83621478  NotificationEvent
            8362c440  NotificationEvent
            8362c3c8  NotificationEvent
            8362c350  NotificationEvent
            8362c2d8  NotificationEvent
            8362c260  NotificationEvent
            8362c1e8  NotificationEvent
            8362c170  NotificationEvent
            8362c0f8  NotificationEvent
            8362c080  NotificationEvent
            8362ab60  NotificationEvent
            8362aae8  NotificationEvent
            8362aa70  NotificationEvent
            9e1e3ff0  NotificationEvent
            835e8190  SynchronizationEvent
            8360dc38  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8346d618       Image:         taskeng.exe
        Wait Start TickCount      29067          Ticks: 14432 (0:00:03:45.140)
        Context Switch Count      4893
        UserTime                  00:00:00.031
        KernelTime                00:00:00.046
        Win32 Start Address MsCtfMonitor!MsCtfMonitor::ThreadProc (0x71463075)
        Stack Init 9f20c000 Current 9f20b8d0 Base 9f20c000 Limit 9f209000 Call 0
        Priority 12 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f20b8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f20b924 81c28c64 nt!KiSwapThread+0x389
        9f20b970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f20bbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f20bd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f20bd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f20bd64)
        0167fa74 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0167fa78 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0167fb14 761dc4b7 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0167fb68 761d8b83 USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
        0167fb84 714612de USER32!MsgWaitForMultipleObjects+0x1f (FPO: [Non-Fpo])
        0167fc0c 714630c5 MsCtfMonitor!DoMsCtfMonitor+0x180 (FPO: [Non-Fpo])
        0167fe2c 75f33833 MsCtfMonitor!MsCtfMonitor::ThreadProc+0x57 (FPO: [Non-Fpo])
        0167fe38 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0167fe78 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 83628620  Cid 0b14.0b8c  Teb: 7ffd3000 Win32Thread: ff781c08 WAIT: (WrLpcReceive)
UserMode Non-Alertable
            83628834  Semaphore Limit 0x1
            836286a8  NotificationTimer
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8346d618       Image:         taskeng.exe
        Wait Start TickCount      43490          Ticks: 9 (0:00:00:00.140)
        Context Switch Count      1800
        UserTime                  00:00:00.015
        KernelTime                00:00:00.078
        Win32 Start Address MSCTF!CCtfServerPort::StaticServerThread (0x771dd079)
        Stack Init a1a2f000 Current a1a2eb78 Base a1a2f000 Limit a1a2c000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a1a2eb90 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1a2ebcc 81c293a7 nt!KiSwapThread+0x389
        a1a2ec2c 81dc3dac nt!KeWaitForSingleObject+0x414
        a1a2ec64 81dc436e nt!AlpcpReceiveMessagePort+0x221
        a1a2ece0 81dc6211 nt!AlpcpReceiveMessage+0x163
        a1a2ed3c 81c8caaa nt!NtAlpcSendWaitReceivePort+0x11c
        a1a2ed3c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1a2ed64)
        0176e638 7748f2c0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0176e63c 771c262c ntdll!NtAlpcSendWaitReceivePort+0xc (FPO: [8,0,0])
        0176f6f4 771dd190 MSCTF!CCtfServerPort::ServerLoop+0x131 (FPO: [Non-Fpo])
        0176f960 771dd097 MSCTF!CCtfServerPort::ServerThread+0xdc (FPO: [Non-Fpo])
        0176f970 75f33833 MSCTF!CCtfServerPort::StaticServerThread+0x22 (FPO: [Non-Fpo])
        0176f97c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0176f9bc 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 8366a888  Cid 0b14.0bd8  Teb: 7ffaf000 Win32Thread: ff365860 WAIT: (WrQueue)
UserMode Non-Alertable
            83648fd0  QueueObject
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8346d618       Image:         taskeng.exe
        Wait Start TickCount      9292           Ticks: 34207 (0:00:08:53.632)
        Context Switch Count      136
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdmaud!mxdMessageThreadProc (0x737f42d7)
        Stack Init a693f000 Current a693ebc8 Base a693f000 Limit a693c000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a693ebe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a693ec1c 81cad431 nt!KiSwapThread+0x389
        a693ec6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a693ecc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a693ed48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a693ed48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a693ed64)
        01e4fa14 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01e4fa18 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        01e4fa44 737f4354 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        01e4fa74 75f33833 wdmaud!mxdMessageThreadProc+0x7d (FPO: [Non-Fpo])
        01e4fa80 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01e4fac0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 83678b98  Cid 0b14.0bdc  Teb: 7ffae000 Win32Thread: ff363860 WAIT: (WrUserRequest)
UserMode Non-Alertable
            836548d8  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8346d618       Image:         taskeng.exe
        Wait Start TickCount      9285           Ticks: 34214 (0:00:08:53.741)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdmaud!CTaskThread::TaskThreadProc (0x737f8675)
        Stack Init a6943000 Current a6942b68 Base a6943000 Limit a6940000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a6942b80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a6942bbc 81c293a7 nt!KiSwapThread+0x389
        a6942c18 8cedb8ed nt!KeWaitForSingleObject+0x414
        a6942c74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        a6942c90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        a6942ce8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        a6942d4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        a6942d4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a6942d64)
        016ffa3c 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        016ffa40 761e19cd USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        016ffa5c 737f8712 USER32!GetMessageW+0x33 (FPO: [Non-Fpo])
        016ffa9c 75f33833 wdmaud!CTaskThread::TaskThreadProc+0x9d (FPO: [Non-Fpo])
        016ffaa8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        016ffae8 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 83655568  Cid 0b14.0be0  Teb: 7ffad000 Win32Thread: fe69a9f0 WAIT: (UserRequest)
UserMode Non-Alertable
            83655850  SynchronizationEvent
            836546c8  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8346d618       Image:         taskeng.exe
        Wait Start TickCount      24684          Ticks: 18815 (0:00:04:53.515)
        Context Switch Count      623
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdmaud!CWorker::_StaticThreadProc (0x737f8544)
        Stack Init a6947000 Current a69468d0 Base a6947000 Limit a6944000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a69468e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a6946924 81c28c64 nt!KiSwapThread+0x389
        a6946970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a6946bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a6946d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a6946d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a6946d64)
        018af880 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        018af884 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        018af920 737f5111 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        018af958 737f855c wdmaud!CWorker::_ThreadProc+0x5e (FPO: [Non-Fpo])
        018af964 75f33833 wdmaud!CWorker::_StaticThreadProc+0x18 (FPO: [Non-Fpo])
        018af970 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        018af9b0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 835fbcc0  Cid 0b14.0c08  Teb: 7ffab000 Win32Thread: fe6f69d8 WAIT: (WrUserRequest)
UserMode Non-Alertable
            83662940  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8346d618       Image:         taskeng.exe
        Wait Start TickCount      29067          Ticks: 14432 (0:00:03:45.140)
        Context Switch Count      215
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address WINMM!mciwindow (0x738c1385)
        Stack Init a68d3000 Current a68d2b68 Base a68d3000 Limit a68d0000 Call 0
        Priority 12 BasePriority 10 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a68d2b80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a68d2bbc 81c293a7 nt!KiSwapThread+0x389
        a68d2c18 8cedb8ed nt!KeWaitForSingleObject+0x414
        a68d2c74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        a68d2c90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        a68d2ce8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        a68d2d4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        a68d2d4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a68d2d64)
        0140fe30 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0140fe34 761d3ad1 USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        0140fe58 738c1404 USER32!GetMessageA+0x8a (FPO: [Non-Fpo])
        0140fe90 75f33833 WINMM!mciwindow+0x102 (FPO: [Non-Fpo])
        0140fe9c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0140fedc 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 835d7030  Cid 0b14.0c0c  Teb: 7ffaa000 Win32Thread: ff3512c0 WAIT: (UserRequest)
UserMode Non-Alertable
            83660918  NotificationEvent
            8348c110  SynchronizationEvent
            8357b560  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8346d618       Image:         taskeng.exe
        Wait Start TickCount      9309           Ticks: 34190 (0:00:08:53.367)
        Context Switch Count      171
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address taskeng!Job::RunCallback (0x00e91fbf)
        Stack Init a68cf000 Current a68ce8d0 Base a68cf000 Limit a68cc000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a68ce8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a68ce924 81c28c64 nt!KiSwapThread+0x389
        a68ce970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a68cebfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a68ced48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a68ced48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a68ced64)
        01a1fbbc 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01a1fbc0 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        01a1fc5c 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        01a1fc78 00e91b6e kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        01a1fcf4 00e91fed taskeng!Job::Run+0x179 (FPO: [Non-Fpo])
        01a1fd38 75f33833 taskeng!Job::RunCallback+0x8c (FPO: [Non-Fpo])
        01a1fd44 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01a1fd84 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 8366bd78  Cid 0b14.0c4c  Teb: 7ffa9000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            83591ea8  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8346d618       Image:         taskeng.exe
        Wait Start TickCount      9308           Ticks: 34191 (0:00:08:53.383)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address TMM!CTMMJob::ThreadProc (0x7083a4fb)
        Stack Init a688f000 Current a688ec38 Base a688f000 Limit a688c000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a688ec50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a688ec8c 81c293a7 nt!KiSwapThread+0x389
        a688ece8 81df5057 nt!KeWaitForSingleObject+0x414
        a688ed50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a688ed50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a688ed64)
        0136fa1c 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0136fa20 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0136fa90 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        0136faa4 7083a554 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0136fac8 75f33833 TMM!CTMMJob::ThreadProc+0x75 (FPO: [Non-Fpo])
        0136fad4 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0136fb14 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Dwm process

```
PROCESS 8346fd90  SessionId: 1  Cid: 0b48    Peb: 7ffdc000  ParentCid: 03bc
    DirBase: 29a01420  ObjectTable: a8a5ae38  HandleCount: 147.
    Image: dwm.exe
    VadRoot 835f5558 Vads 140 Clone 0 Private 16700. Modified 9180. Locked 12584.
    DeviceMap a7766db8
    Token                             a8a72be8
    ElapsedTime                       00:08:55.446
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         113424
    QuotaPoolUsage[NonPagedPool]      6760
    Working Set Sizes (now,min,max)  (21855, 12800, 524272) (87420KB, 51200KB, 2097088KB)
    PeakWorkingSetSize                25415
    VirtualSize                       130 Mb
    PeakVirtualSize                   145 Mb
    PageFaultCount                    40547
    MemoryPriority                    BACKGROUND
    BasePriority                      13
    CommitCharge                      19248

    Setting context for this process...
.process /p /r ffffffff8346fd90

    !peb
PEB at 7ffdc000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00fe0000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 001a1718 . 001b8b58
    Ldr.InLoadOrderModuleList:           001a1698 . 001b8bb8
    Ldr.InMemoryOrderModuleList:         001a16a0 . 001b8bc0
            Base TimeStamp                     Module
          fe0000 4549aed1 Nov 02 08:39:45 2006 C:\Windows\system32\Dwm.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        746d0000 4549bde7 Nov 02 09:44:07 2006 C:\Windows\system32\UxTheme.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.dll
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        71300000 4549bd25 Nov 02 09:40:53 2006 C:\Windows\system32\dwmredir.dll
        72f50000 4549bdb6 Nov 02 09:43:18 2006 C:\Windows\system32\SLWGA.dll
        75dc0000 470c4de2 Oct 10 04:58:26 2007 C:\Windows\system32\urlmon.dll
        763b0000 4549bdb9 Nov 02 09:43:21 2006 C:\Windows\system32\SHLWAPI.dll
        76360000 4549bcfb Nov 02 09:40:11 2006 C:\Windows\system32\iertutil.dll
        74fe0000 46d779a1 Aug 31 03:14:57 2007 C:\Windows\system32\WTSAPI32.dll
        75610000 4679de70 Jun 21 03:12:00 2007 C:\Windows\system32\slc.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        74aa0000 4549bd09 Nov 02 09:40:25 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_5d07289e07e1d100\comctl32.dll
        75020000 4549bddb Nov 02 09:43:55 2006 C:\Windows\system32\NTMARTA.DLL
        76310000 4549be44 Nov 02 09:45:40 2006 C:\Windows\system32\WLDAP32.dll
        75fe0000 4549be0e Nov 02 09:44:46 2006 C:\Windows\system32\WS2_32.dll
        77550000 4549bdc7 Nov 02 09:43:35 2006 C:\Windows\system32\NSI.dll
        75ce0000 4549bd99 Nov 02 09:42:49 2006 C:\Windows\system32\PSAPI.DLL
        75ad0000 4549bda8 Nov 02 09:43:04 2006 C:\Windows\system32\SAMLIB.dll
```

```
        71110000 4549bcf5 Nov 02 09:40:05 2006 C:\Windows\system32\milcore.dll
        70f50000 4549bcc1 Nov 02 09:39:13 2006 C:\Windows\system32\d3d9.dll
        753f0000 4549bde4 Nov 02 09:44:04 2006 C:\Windows\system32\VERSION.dll
        71470000 4549bcc0 Nov 02 09:39:12 2006 C:\Windows\system32\d3d8thk.dll
        71490000 4549bd24 Nov 02 09:40:52 2006 C:\Windows\system32\dwmapi.dll
        10000000 4681449e Jun 26 17:53:50 2007 C:\Windows\system32\igdumd32.dll
        70ee0000 4549bdd7 Nov 02 09:43:51 2006 C:\Windows\system32\uDWM.dll
        73240000 4654f735 May 24 03:23:49 2007 C:\Windows\system32\WindowsCodecs.dll
    SubSystemData:     00000000
    ProcessHeap:       001a0000
    ProcessParameters: 001a0fd8
    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;C:\Program Files\QuickTime\QTSystem\'
    Environment:  001a07e8
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\UserName\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        HOMEDRIVE=C:
        HOMEPATH=\Users\UserName
        LOCALAPPDATA=C:\Users\UserName\AppData\Local
        LOGONSERVER=\\HOME
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Users\UserName\AppData\Local\Temp
        TMP=C:\Users\UserName\AppData\Local\Temp
        USERDOMAIN=home
        USERNAME=UserName
        USERPROFILE=C:\Users\UserName
        windir=C:\Windows
```

```
        THREAD 835f9ad8  Cid 0b48.0b4c  Teb: 7ffdf000 Win32Thread: ff34a840 WAIT: (UserRequest)
UserMode Non-Alertable
            8346d470  SynchronizationEvent
            8346d4a0  SynchronizationEvent
            835f8c20  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8346fd90       Image:         dwm.exe
        Wait Start TickCount      11132          Ticks: 32367 (0:00:08:24.928)
        Context Switch Count      141
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address Dwm!_WinMainStartup (0x00fe55ed)
        Stack Init a1b44000 Current a1b438d0 Base a1b44000 Limit a1b41000 Call 0
        Priority 15 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1b438e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1b43924 81c28c64 nt!KiSwapThread+0x389
        a1b43970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1b43bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1b43d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1b43d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1b43d64)
        000af964 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        000af968 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        000afa04 761dc4b7 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        000afa58 00fe1ad5 USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
        000afa84 00fe1a8a Dwm!CDwmAppHost::WaitForAndProcessEvent+0x3a
        000afab8 00fe4ec7 Dwm!CDwmAppHost::Run+0x65
        000afac8 00fe45bd Dwm!WinMain+0x46
        000afb58 00fe5602 Dwm!_initterm_e+0x1a1 (FPO: [Non-Fpo])
        000afb60 75f33833 Dwm!_WinMainStartup+0x11 (FPO: [Non-Fpo])
        000afb6c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        000afbac 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 8362b030  Cid 0b48.0b6c  Teb: 7ffde000 Win32Thread: ff77ca08 WAIT: (UserRequest)
UserMode Non-Alertable
            835a3040  Semaphore Limit 0x7fffffff
            8362a080  SynchronizationEvent
            8362b0b8  NotificationTimer
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8346fd90       Image:         dwm.exe
        Wait Start TickCount      43269          Ticks: 230 (0:00:00:03.588)
        Context Switch Count      13605
        UserTime                  00:00:00.171
        KernelTime                00:00:00.109
        Win32 Start Address Dwm!CPortBase::PortThread (0x00fe53af)
        Stack Init a1a6f000 Current a1a6e8d0 Base a1a6f000 Limit a1a6c000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a1a6e8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1a6e924 81c28c64 nt!KiSwapThread+0x389
        a1a6e970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1a6ebfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1a6ed48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1a6ed48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1a6ed64)
        00fdf764 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00fdf768 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00fdf804 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        00fdf820 71112d91 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        00fdf948 71112ce6 milcore!CMilChannel::WaitForNextMessage+0xac
        00fdf968 713014a7 milcore!MilComposition_WaitForNextMessage+0x5d
        00fdf9d8 71301447 dwmredir!CMilWindowManager::WaitForMultipleObjects+0xa1
        00fdf9ec 00fe14a3 dwmredir!DwmRedirectionManagerWaitForMultipleObjects+0x14
        00fdfa08 00fe1607 Dwm!CSessionPort::WaitForMultipleObjects+0x1b
        00fdfa30 00fe53bd Dwm!CPortBase::PortThreadInternal+0x42
        00fdfa3c 75f33833 Dwm!CPortBase::PortThread+0xe
        00fdfa48 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00fdfa88 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 8362bb80  Cid 0b48.0b70  Teb: 7ffdd000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            83568200  SynchronizationTimer
            9fc38a48  ProcessObject
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8346fd90       Image:         dwm.exe
        Wait Start TickCount      9188           Ticks: 34311 (0:00:08:55.255)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x7744b49a)
        Stack Init a02a2000 Current a02a18d0 Base a02a2000 Limit a029f000 Call 0
        Priority 13 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a02a18e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a02a1924 81c28c64 nt!KiSwapThread+0x389
        a02a1970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a02a1bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a02a1d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a02a1d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a02a1d64)
        011efa4c 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        011efa50 7744b65b ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        011efbec 75f33833 ntdll!TppWaiterpThread+0x294 (FPO: [Non-Fpo])
        011efbf8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        011efc38 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 83628910  Cid 0b48.0b88  Teb: 7ffdb000 Win32Thread: ff77ce98 WAIT: (UserRequest)
UserMode Non-Alertable
            83606738  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8346fd90       Image:         dwm.exe
        Wait Start TickCount      43270          Ticks: 229 (0:00:00:03.572)
        Context Switch Count      9232
        UserTime                  00:00:04.165
        KernelTime                00:00:01.653
        Win32 Start Address milcore!CPartitionThread::ThreadMain (0x71189e87)
        Stack Init a0985000 Current a0984c38 Base a0985000 Limit a0982000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a0984c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0984c8c 81c293a7 nt!KiSwapThread+0x389
        a0984ce8 81df5057 nt!KeWaitForSingleObject+0x414
        a0984d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a0984d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0984d64)
        0156fb14 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0156fb18 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0156fb88 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        0156fb9c 711136ac kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0156fbcc 711155be milcore!CPartitionManager::GetWork+0x159
        0156fbe4 7111570c milcore!CPartitionVerticalBlankScheduler::WaitForWork+0x42
        0156fc0c 71189ea5 milcore!CPartitionVerticalBlankScheduler::Run+0x3a
        0156fc24 75f33833 milcore!CPartitionThread::ThreadMain+0x1e
        0156fc30 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0156fc70 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 83629d78  Cid 0b48.0b98  Teb: 7ffda000 Win32Thread: ff36f410 WAIT: (UserRequest)
UserMode Non-Alertable
            8362a1f8  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8346fd90       Image:         dwm.exe
        Wait Start TickCount      24714          Ticks: 18785 (0:00:04:53.047)
        Context Switch Count      756
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address uDWM!CDesktopManager::DwmEventThreadProc (0x70eeb532)
        Stack Init a1b70000 Current a1b6f8d0 Base a1b70000 Limit a1b6d000 Call 0
        Priority 15 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1b6f8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1b6f924 81c28c64 nt!KiSwapThread+0x389
        a1b6f970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a1b6fbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a1b6fd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a1b6fd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1b6fd64)
        0119f9f0 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0119f9f4 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0119fa90 761dc4b7 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0119fae4 70eeb6eb USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
        0119fb8c 75f33833 uDWM!CDesktopManager::DwmEventThreadProc+0x309
        0119fb98 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0119fbd8 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 83641768  Cid 0b48.0b9c  Teb: 7ffd9000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            83641a40  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8346fd90       Image:         dwm.exe
        Wait Start TickCount      9195           Ticks: 34304 (0:00:08:55.145)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address d3d9!wmt_CSSEShaderCode::ProcessPositionAndColors (0x7106a100)
        Stack Init a1a57000 Current a1a56c38 Base a1a57000 Limit a1a54000 Call 0
        Priority 13 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a1a56c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1a56c8c 81c293a7 nt!KiSwapThread+0x389
        a1a56ce8 81df5057 nt!KeWaitForSingleObject+0x414
        a1a56d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a1a56d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1a56d64)
        046aeb68 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        046aeb6c 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        046aebdc 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        046aebf0 7106a17f kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        046afc30 75f33833 d3d9!wmt_CSSEShaderCode::ProcessPositionAndColors+0x9ef (FPO: [Non-Fpo])
        046afc3c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        046afc7c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Explorer process

```
PROCESS 8362a638  SessionId: 1  Cid: 0b90    Peb: 7ffd7000  ParentCid: 0b2c
    DirBase: 29a01440  ObjectTable: a8a865d8  HandleCount: 674.
    Image: explorer.exe
    VadRoot 83474580 Vads 399 Clone 0 Private 4240. Modified 8997. Locked 0.
    DeviceMap a7766db8
    Token                             a8a928b0
    ElapsedTime                       00:08:55.118
    UserTime                          00:00:00.748
    KernelTime                        00:00:00.982
    QuotaPoolUsage[PagedPool]         303672
    QuotaPoolUsage[NonPagedPool]      29352
    Working Set Sizes (now,min,max)  (10022, 50, 345) (40088KB, 200KB, 1380KB)
    PeakWorkingSetSize                10917
    VirtualSize                       175 Mb
    PeakVirtualSize                   204 Mb
    PageFaultCount                    32212
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      7780

    Setting context for this process...
.process /p /r ffffffff8362a638

    !peb
PEB at 7ffd7000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00510000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 001b1740 . 063f6cb0
    Ldr.InLoadOrderModuleList:           001b16c0 . 063f6ca0
    Ldr.InMemoryOrderModuleList:         001b16c8 . 063f6ca8
            Base TimeStamp                     Module
          510000 46d230c5 Aug 27 03:02:45 2007 C:\Windows\Explorer.EXE
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        763b0000 4549bdb9 Nov 02 09:43:21 2006 C:\Windows\system32\SHLWAPI.dll
        76560000 4681c95d Jun 27 03:20:13 2007 C:\Windows\system32\SHELL32.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        70cc0000 4549bdb3 Nov 02 09:43:15 2006 C:\Windows\system32\SHDOCVW.dll
        746d0000 4549bde7 Nov 02 09:44:07 2006 C:\Windows\system32\UxTheme.dll
        75290000 4549bdd0 Nov 02 09:43:44 2006 C:\Windows\system32\POWRPROF.dll
        71490000 4549bd24 Nov 02 09:40:52 2006 C:\Windows\system32\dwmapi.dll
        73d70000 4549bcaf Nov 02 09:38:55 2006
C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.0.6000.16386_none_9ea0ac9ec96e71
27\gdiplus.dll
        75610000 4679de70 Jun 21 03:12:00 2007 C:\Windows\system32\slc.dll
        744e0000 4549bd96 Nov 02 09:42:46 2006 C:\Windows\system32\PROPSYS.dll
        70b70000 4549bcde Nov 02 09:39:42 2006 C:\Windows\system32\BROWSEUI.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.dll
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        73c20000 4549bd23 Nov 02 09:40:51 2006 C:\Windows\system32\DUser.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        74aa0000 4549bd09 Nov 02 09:40:25 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_5d07289e07e1d100\comctl32.dll
        73240000 4654f735 May 24 03:23:49 2007 C:\Windows\system32\WindowsCodecs.dll
```

```
714a0000 4549bcec Nov 02 09:39:56 2006 C:\Windows\system32\IconCodecService.dll
75b80000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\Secur32.dll
773a0000 4549bce9 Nov 02 09:39:53 2006 C:\Windows\system32\CLBCatQ.DLL
75350000 4549bdae Nov 02 09:43:10 2006 C:\Windows\system32\rsaenh.dll
70e20000 46d24086 Aug 27 04:09:58 2007 C:\Windows\system32\timedate.cpl
74d00000 4549bcbc Nov 02 09:39:08 2006 C:\Windows\system32\ATL.DLL
75840000 4549bd53 Nov 02 09:41:39 2006 C:\Windows\system32\NETAPI32.dll
75ce0000 4549bd99 Nov 02 09:42:49 2006 C:\Windows\system32\PSAPI.DLL
73880000 4549bd93 Nov 02 09:42:43 2006 C:\Windows\system32\OLEACC.dll
70ab0000 4549bcbf Nov 02 09:39:11 2006 C:\Windows\system32\actxprxy.dll
75ba0000 4549bde2 Nov 02 09:44:02 2006 C:\Windows\system32\USERENV.dll
70f20000 4549bd5c Nov 02 09:41:48 2006 C:\Windows\system32\msutb.dll
750a0000 4549be0a Nov 02 09:44:42 2006 C:\Windows\system32\WINBRAND.dll
73820000 4549bdb3 Nov 02 09:43:15 2006 C:\Windows\System32\shacct.dll
75ad0000 4549bda8 Nov 02 09:43:04 2006 C:\Windows\System32\SAMLIB.dll
75b20000 4549bcaf Nov 02 09:38:55 2006 C:\Windows\system32\apphelp.dll
70a30000 4549bd43 Nov 02 09:41:23 2006 C:\Windows\System32\msshsq.dll
70690000 4549bd41 Nov 02 09:41:21 2006 C:\Windows\System32\NaturalLanguage6.dll
75650000 45b96fde Jan 26 03:05:02 2007 C:\Windows\System32\CRYPT32.dll
75820000 4549bd41 Nov 02 09:41:21 2006 C:\Windows\System32\MSASN1.dll
6fd30000 4549bd76 Nov 02 09:42:14 2006 C:\Windows\System32\NLSData0009.dll
6faa0000 4549aaad Nov 02 08:22:05 2006 C:\Windows\System32\NLSLexicons0009.dll
748b0000 4681c8b2 Jun 27 03:17:22 2007 C:\Windows\system32\authui.dll
74cf0000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\MSIMG32.dll
70e00000 4549bcef Nov 02 09:39:59 2006 C:\Windows\system32\LINKINFO.dll
70df0000 4549bd91 Nov 02 09:42:41 2006 C:\Windows\system32\msiltcfg.dll
753f0000 4549bde4 Nov 02 09:44:04 2006 C:\Windows\system32\VERSION.dll
70480000 4549bd89 Nov 02 09:42:33 2006 C:\Windows\system32\msi.dll
6eaa0000 470c4d6e Oct 10 04:56:30 2007 C:\Windows\system32\ieframe.dll
76360000 4549bcfb Nov 02 09:40:11 2006 C:\Windows\system32\iertutil.dll
75020000 4549bddb Nov 02 09:43:55 2006 C:\Windows\system32\NTMARTA.DLL
76310000 4549be44 Nov 02 09:45:40 2006 C:\Windows\system32\WLDAP32.dll
75fe0000 4549be0e Nov 02 09:44:46 2006 C:\Windows\system32\WS2_32.dll
77550000 4549bdc7 Nov 02 09:43:35 2006 C:\Windows\system32\NSI.dll
75dc0000 470c4de2 Oct 10 04:58:26 2007 C:\Windows\system32\urlmon.dll
70de0000 4549bd00 Nov 02 09:40:16 2006 C:\Windows\system32\ExplorerFrame.dll
76020000 470c4e1e Oct 10 04:59:26 2007 C:\Windows\system32\WININET.dll
76010000 4549ad42 Nov 02 08:33:06 2006 C:\Windows\system32\Normaliz.dll
738c0000 4549be1d Nov 02 09:45:01 2006 C:\Windows\system32\WINMM.dll
737f0000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\wdmaud.drv
73870000 4549bd89 Nov 02 09:42:33 2006 C:\Windows\system32\ksuser.dll
75390000 4549bcdc Nov 02 09:39:40 2006 C:\Windows\system32\AVRT.dll
74d90000 4549bd03 Nov 02 09:40:19 2006 C:\Windows\system32\MMDevAPI.DLL
71440000 4549bd2c Nov 02 09:41:00 2006 C:\Windows\system32\cscapi.dll
71840000 4549bdb4 Nov 02 09:43:16 2006 C:\Windows\system32\SFC.DLL
70dd0000 4549bdb5 Nov 02 09:43:17 2006 C:\Windows\system32\sfc_os.dll
77030000 4549bdb0 Nov 02 09:43:12 2006 C:\Windows\system32\SETUPAPI.dll
74ff0000 4549be2f Nov 02 09:45:19 2006 C:\Windows\system32\WINTRUST.dll
77580000 462434a3 Apr 17 03:44:51 2007 C:\Windows\system32\imagehlp.dll
736d0000 4549bcc2 Nov 02 09:39:14 2006 C:\Windows\System32\audioses.dll
73540000 4549bcc0 Nov 02 09:39:12 2006 C:\Windows\System32\audioeng.dll
73860000 4549bd2f Nov 02 09:41:03 2006 C:\Windows\system32\msacm32.drv
73790000 4549bd2e Nov 02 09:41:02 2006 C:\Windows\system32\MSACM32.dll
736c0000 4549bd27 Nov 02 09:40:55 2006 C:\Windows\system32\miUserNamep.dll
6f8e0000 4549bdca Nov 02 09:43:38 2006 C:\Windows\system32\stobject.dll
6f820000 4549bcb5 Nov 02 09:39:01 2006 C:\Windows\system32\BatMeter.dll
74fe0000 46d779a1 Aug 31 03:14:57 2007 C:\Windows\system32\WTSAPI32.dll
75300000 4549be2e Nov 02 09:45:18 2006 C:\Windows\system32\WINSTA.dll
745a0000 4549bcf8 Nov 02 09:40:08 2006 C:\Windows\system32\es.dll
6f9f0000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\System32\SndVolSSO.dll
6f9c0000 4549bcf5 Nov 02 09:40:05 2006 C:\Windows\ehome\ehSSO.dll
74cb0000 4549bcde Nov 02 09:39:42 2006 C:\Windows\system32\HID.DLL
74f30000 46677f3a Jun 07 04:44:58 2007 C:\Windows\system32\FirewallAPI.dll
6f200000 4549bd66 Nov 02 09:41:58 2006 C:\Windows\System32\netshell.dll
755b0000 4549bd3f Nov 02 09:41:19 2006 C:\Windows\System32\IPHLPAPI.DLL
75570000 46807ea6 Jun 26 03:49:10 2007 C:\Windows\System32\dhcpcsvc.DLL
75af0000 4549bcf1 Nov 02 09:40:01 2006 C:\Windows\System32\DNSAPI.dll
75560000 4549be1e Nov 02 09:45:02 2006 C:\Windows\System32\WINNSI.DLL
75540000 46807ea7 Jun 26 03:49:11 2007 C:\Windows\System32\dhcpcsvc6.DLL
74d30000 4549bd6b Nov 02 09:42:03 2006 C:\Windows\System32\nlaapi.dll
```

```
        6f660000 4549bdba Nov 02 09:43:22 2006 C:\Windows\system32\pnidui.dll
        709f0000 4549bda5 Nov 02 09:43:01 2006 C:\Windows\system32\QUtil.dll
        755d0000 4549bdf6 Nov 02 09:44:22 2006 C:\Windows\system32\wevtapi.dll
        73f30000 4549be41 Nov 02 09:45:37 2006 C:\Windows\system32\wlanutil.dll
        72a20000 4549bcda Nov 02 09:39:38 2006 C:\Windows\system32\FunDisc.dll
        70b10000 4549bcdd Nov 02 09:39:41 2006 C:\Windows\system32\fdproxy.dll
        72460000 4666193b Jun 06 03:17:31 2007 C:\Windows\System32\msxml3.dll
        720c0000 4549bdc3 Nov 02 09:43:31 2006 C:\Windows\System32\npmproxy.dll
        6fa90000 46d4e271 Aug 29 04:05:21 2007 C:\Windows\system32\Wlanapi.dll
        74050000 4549bda1 Nov 02 09:42:57 2006 C:\Windows\system32\OneX.DLL
        74680000 4549bccc Nov 02 09:39:24 2006 C:\Windows\system32\eappprxy.dll
        73f40000 4549bcc9 Nov 02 09:39:21 2006 C:\Windows\system32\eappcfg.dll
        754a0000 4549bcb9 Nov 02 09:39:05 2006 C:\Windows\system32\bcrypt.dll
        6fa60000 4549bce0 Nov 02 09:39:44 2006 C:\Windows\System32\AltTab.dll
        6f560000 4549be08 Nov 02 09:44:40 2006 C:\Windows\system32\wpdshserviceobj.dll
        73420000 4549be18 Nov 02 09:44:56 2006 C:\Windows\system32\WINHTTP.dll
        6f0f0000 4549bdf1 Nov 02 09:44:17 2006 C:\Windows\System32\srchadmin.dll
        6f0b0000 4549bdec Nov 02 09:44:12 2006 C:\Windows\system32\webcheck.dll
        6ddd0000 4549bdd5 Nov 02 09:43:49 2006 C:\Windows\System32\SyncCenter.dll
        70e10000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\mssprxy.dll
        6f520000 4549be12 Nov 02 09:44:50 2006 C:\Windows\system32\wscntfy.dll
        71ee0000 4549be10 Nov 02 09:44:48 2006 C:\Windows\system32\WSCAPI.dll
        70b20000 4549bde2 Nov 02 09:44:02 2006 C:\Windows\system32\ntshrui.dll
        6e9b0000 4549bd97 Nov 02 09:42:47 2006 C:\Windows\System32\QAgent.dll
        735b0000 4549bce0 Nov 02 09:39:44 2006 C:\Windows\System32\fwpuclnt.dll
        75a60000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\SXS.DLL
        6f080000 4549bdca Nov 02 09:43:38 2006 C:\Windows\system32\PortableDeviceTypes.dll
        72040000 4549bdc8 Nov 02 09:43:36 2006 C:\Windows\system32\PortableDeviceApi.dll
        6e490000 4549bd24 Nov 02 09:40:52 2006 C:\Windows\system32\imapi2.dll
        6d850000 4549bce3 Nov 02 09:39:47 2006 C:\Windows\system32\bthprops.cpl
        6d7f0000 4549bdf3 Nov 02 09:44:19 2006 C:\Program Files\Common Files\microsoft
shared\ink\tiptsf.dll
        10000000 453c6a72 Oct 23 08:08:34 2006 C:\Program Files\Common
Files\Adobe\Acrobat\ActiveX\AcroIEHelper.dll
        6e210000 4536eb78 Oct 19 04:05:28 2006
C:\Windows\WinSxS\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.312_none_10b2ee7b9bffc2c7\MSVCR
80.dll
        73a70000 4549be05 Nov 02 09:44:37 2006 C:\Windows\system32\xmllite.dll
        6e670000 4549bdec Nov 02 09:44:12 2006 C:\Windows\system32\thumbcache.dll
        75750000 4549bd14 Nov 02 09:40:36 2006 C:\Windows\system32\MPR.dll
        6f630000 4549bcf7 Nov 02 09:40:07 2006 C:\Windows\system32\MLANG.dll
        6e890000 4549bccc Nov 02 09:39:24 2006 C:\Windows\system32\dciman32.dll
        6e430000 4549bdd7 Nov 02 09:43:51 2006 C:\Windows\system32\syncui.dll
        6e900000 4549bdd6 Nov 02 09:43:50 2006 C:\Windows\system32\SYNCENG.dll
        74f10000 4549bcb8 Nov 02 09:39:04 2006 C:\Windows\system32\Cabinet.dll
    SubSystemData:     00000000
    ProcessHeap:       001b0000
    ProcessParameters: 001b1000
    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;C:\Program Files\QuickTime\QTSystem\'
    Environment:  024aa360
        =::=::\
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\UserName\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        HOMEDRIVE=C:
        HOMEPATH=\Users\UserName
        LOCALAPPDATA=C:\Users\UserName\AppData\Local
        LOGONSERVER=\\HOME
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
```

```
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        SESSIONNAME=Console
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Users\UserName\AppData\Local\Temp
        TMP=C:\Users\UserName\AppData\Local\Temp
        USERDOMAIN=home
        USERNAME=UserName
        USERPROFILE=C:\Users\UserName
        windir=C:\Windows


        THREAD 8362a390  Cid 0b90.0b94  Teb: 7ffdf000 Win32Thread: ff34c848 WAIT: (WrUserRequest)
UserMode Non-Alertable
            83656de0  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8362a638       Image:         explorer.exe
        Wait Start TickCount      43496          Ticks: 3 (0:00:00:00.046)
        Context Switch Count      14502
        UserTime                  00:00:00.436
        KernelTime                00:00:00.608
        Win32 Start Address Explorer!wWinMainCRTStartup (0x0052d070)
        Stack Init 9e8b3000 Current 9e8b2c10 Base 9e8b3000 Limit 9e8b0000 Call 0
        Priority 12 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9e8b2c28 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e8b2c64 81c293a7 nt!KiSwapThread+0x389
        9e8b2cc0 8cedb8ed nt!KeWaitForSingleObject+0x414
        9e8b2d1c 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        9e8b2d38 8ced573c win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        9e8b2d4c 8ced5759 win32k!xxxRealWaitMessageEx+0x12 (FPO: [Non-Fpo])
        9e8b2d5c 81c8caaa win32k!NtUserWaitMessage+0x14 (FPO: [Non-Fpo])
        9e8b2d5c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9e8b2d64)
        000ffb94 761db5bc ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        000ffb98 765e07f6 USER32!NtUserWaitMessage+0xc (FPO: [Non-Fpo])
        000ffbb0 76566f4e SHELL32!CDesktopBrowser::_MessageLoop+0x4c (FPO: [Non-Fpo])
        000ffbbc 00529039 SHELL32!SHDesktopMessageLoop+0x24 (FPO: [Non-Fpo])
        000ffea8 0052d1e0 Explorer!wWinMain+0x447 (FPO: [Non-Fpo])
        000fff3c 75f33833 Explorer!_initterm_e+0x1b1 (FPO: [Non-Fpo])
        000fff48 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        000fff88 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 8354e030  Cid 0b90.0c00  Teb: 7ffdc000 Win32Thread: ff36b860 WAIT: (WrUserRequest)
UserMode Non-Alertable
            a191c6e0  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8362a638       Image:         explorer.exe
        Wait Start TickCount      41945          Ticks: 1554 (0:00:00:24.242)
        Context Switch Count      13657
        UserTime                  00:00:00.530
        KernelTime                00:00:00.795
        Win32 Start Address SHLWAPI!WrapperThreadProc (0x763cb09a)
        Stack Init a68bb000 Current a68bac10 Base a68bb000 Limit a68b8000 Call 0
        Priority 13 BasePriority 9 PriorityDecrement 2 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a68bac28 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a68bac64 81c293a7 nt!KiSwapThread+0x389
        a68bacc0 8cedb8ed nt!KeWaitForSingleObject+0x414
        a68bad1c 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        a68bad38 8ced573c win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        a68bad4c 8ced5759 win32k!xxxRealWaitMessageEx+0x12 (FPO: [Non-Fpo])
        a68bad5c 81c8caaa win32k!NtUserWaitMessage+0x14 (FPO: [Non-Fpo])
        a68bad5c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a68bad64)
        01a8fb98 761db5bc ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01a8fb9c 00511c8e USER32!NtUserWaitMessage+0xc (FPO: [Non-Fpo])
        01a8fbcc 0052a684 Explorer!CTray::_MessageLoop+0x140 (FPO: [Non-Fpo])
        01a8fbd8 763cb132 Explorer!CTray::MainThreadProc+0x27 (FPO: [Non-Fpo])
        01a8fc54 75f33833 SHLWAPI!WrapperThreadProc+0x10f (FPO: [Non-Fpo])
        01a8fc60 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01a8fca0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD a1950380  Cid 0b90.0c10  Teb: 7ffdb000 Win32Thread: ff369860 WAIT: (UserRequest)
UserMode Alertable
            83794020  NotificationEvent
            837419e0  NotificationEvent
            837413d8  NotificationEvent
            837413a8  NotificationEvent
            837cc918  NotificationEvent
            837db2d8  NotificationEvent
            8370c220  NotificationEvent
            8370c288  NotificationEvent
            836738d8  NotificationEvent
            83684e08  NotificationEvent
            83644ab8  NotificationEvent
            83644a88  NotificationEvent
            83644b18  NotificationEvent
            83644ae8  NotificationEvent
            8362cb60  NotificationEvent
            835a7768  NotificationEvent
            836721e8  NotificationEvent
            8367f168  NotificationEvent
            83584300  NotificationEvent
            83672418  NotificationEvent
            8357d5d8  NotificationEvent
            8364ec58  NotificationEvent
            8357d548  SynchronizationEvent
        IRP List:
            83794a38: (0006,01d8) Flags: 00060000  Mdl: 00000000
            83794c20: (0006,01d8) Flags: 00060000  Mdl: 00000000
            8370b008: (0006,01d8) Flags: 00060000  Mdl: 00000000
            83674008: (0006,01d8) Flags: 00060000  Mdl: 00000000
            8379c7f8: (0006,01d8) Flags: 00060000  Mdl: 00000000
            837de8c0: (0006,01d8) Flags: 00060000  Mdl: 00000000
            835ee458: (0006,01d8) Flags: 00060000  Mdl: 00000000
            835f17a0: (0006,01d8) Flags: 00060000  Mdl: 00000000
            83704e20: (0006,01d8) Flags: 00060000  Mdl: 00000000
            83684c08: (0006,01d8) Flags: 00060000  Mdl: 00000000
            83684e20: (0006,01d8) Flags: 00060000  Mdl: 00000000
            83645e20: (0006,01d8) Flags: 00060000  Mdl: 00000000
            83671b28: (0006,01d8) Flags: 00060000  Mdl: 00000000
            8351e008: (0006,01d8) Flags: 00060000  Mdl: 00000000
            8368a528: (0006,01d8) Flags: 00060000  Mdl: 00000000
            83686e20: (0006,01d8) Flags: 00060000  Mdl: 00000000
            83667ac0: (0006,01d8) Flags: 00060000  Mdl: 00000000
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8362a638       Image:         explorer.exe
        Wait Start TickCount      14648          Ticks: 28851 (0:00:07:30.078)
        Context Switch Count      597
        UserTime                  00:00:00.062
        KernelTime                00:00:00.031
        Win32 Start Address SHLWAPI!WrapperThreadProc (0x763cb09a)
        Stack Init a68cb000 Current a68ca8d0 Base a68cb000 Limit a68c8000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a68ca8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a68ca924 81c28c64 nt!KiSwapThread+0x389
        a68ca970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a68cabfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a68cad48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a68cad48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a68cad64)
        0223f9e4 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0223f9e8 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0223fa84 761dc4b7 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0223fad8 765dcd55 USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
        0223fbfc 7656596f SHELL32!CChangeNotify::_MessagePump+0x3b (FPO: [Non-Fpo])
        0223fc08 763cb132 SHELL32!CChangeNotify::ThreadProc+0x21 (FPO: [Non-Fpo])
        0223fc84 75f33833 SHLWAPI!WrapperThreadProc+0x10f (FPO: [Non-Fpo])
        0223fc90 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0223fcd0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 83699030  Cid 0b90.0c3c  Teb: 7ffda000 Win32Thread: ff35b848 WAIT: (UserRequest)
UserMode Non-Alertable
            834f86b8  NotificationEvent
            8368aff0  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8362a638       Image:         explorer.exe
        Wait Start TickCount      11132          Ticks: 32367 (0:00:08:24.928)
        Context Switch Count      77
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address gdiplus!BackgroundThreadProc (0x73d81909)
        Stack Init a6877000 Current a68768d0 Base a6877000 Limit a6874000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a68768e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a6876924 81c28c64 nt!KiSwapThread+0x389
        a6876970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a6876bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a6876d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a6876d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a6876d64)
        022ffa20 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        022ffa24 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        022ffac0 761dc4b7 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        022ffb14 761d8b83 USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
        022ffb30 73d81965 USER32!MsgWaitForMultipleObjects+0x1f (FPO: [Non-Fpo])
        022ffb7c 75f33833 gdiplus!BackgroundThreadProc+0x59 (FPO: [Non-Fpo])
        022ffb88 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        022ffbc8 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 8367ba90  Cid 0b90.0c5c  Teb: 7ffd3000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            835a8868  NotificationEvent
            83663430  NotificationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8362a638       Image:         explorer.exe
        Wait Start TickCount      9312           Ticks: 34187 (0:00:08:53.320)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address msiltcfg!WorkerThread (0x70df17ae)
        Stack Init a68f3000 Current a68f28d0 Base a68f3000 Limit a68f0000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a68f28e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a68f2924 81c28c64 nt!KiSwapThread+0x389
        a68f2970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a68f2bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a68f2d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a68f2d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a68f2d64)
        01dcf9d4 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01dcf9d8 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        01dcfa74 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        01dcfa90 70df1883 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        01dcfac0 75f33833 msiltcfg!WorkerThread+0xd5 (FPO: [Non-Fpo])
        01dcfacc 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01dcfb0c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 83688410  Cid 0b90.0c80  Teb: 7ffae000 Win32Thread: ff7fabe0 WAIT: (WrUserRequest)
UserMode Non-Alertable
            8357bc70  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8362a638       Image:         explorer.exe
        Wait Start TickCount      11132          Ticks: 32367 (0:00:08:24.928)
        Context Switch Count      58
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address SHLWAPI!WrapperThreadProc (0x763cb09a)
        Stack Init a68b3000 Current a68b2b68 Base a68b3000 Limit a68b0000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a68b2b80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a68b2bbc 81c293a7 nt!KiSwapThread+0x389
        a68b2c18 8cedb8ed nt!KeWaitForSingleObject+0x414
        a68b2c74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        a68b2c90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        a68b2ce8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        a68b2d4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        a68b2d4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a68b2d64)
        01eafe3c 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01eafe40 761e19cd USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        01eafe5c 00517385 USER32!GetMessageW+0x33 (FPO: [Non-Fpo])
        01eafe9c 763cb132 Explorer!CSoundWnd::s_ThreadProc+0x3a (FPO: [Non-Fpo])
        01eaff18 75f33833 SHLWAPI!WrapperThreadProc+0x10f (FPO: [Non-Fpo])
        01eaff24 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01eaff64 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 8367a380  Cid 0b90.0cc0  Teb: 7ffac000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            8352cbf8  QueueObject
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8362a638       Image:         explorer.exe
        Wait Start TickCount      9362           Ticks: 34137 (0:00:08:52.540)
        Context Switch Count      183
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdmaud!mxdMessageThreadProc (0x737f42d7)
        Stack Init a684b000 Current a684abc8 Base a684b000 Limit a6848000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a684abe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a684ac1c 81cad431 nt!KiSwapThread+0x389
        a684ac6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a684acc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a684ad48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a684ad48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a684ad64)
        0228fe7c 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0228fe80 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        0228feac 737f4354 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        0228fedc 75f33833 wdmaud!mxdMessageThreadProc+0x7d (FPO: [Non-Fpo])
        0228fee8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0228ff28 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 83646c40  Cid 0b90.0cc4  Teb: 7ffab000 Win32Thread: ff2ca4c0 WAIT: (WrUserRequest)
UserMode Non-Alertable
            8365ede0  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8362a638       Image:         explorer.exe
        Wait Start TickCount      9346           Ticks: 34153 (0:00:08:52.790)
        Context Switch Count      8
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdmaud!CTaskThread::TaskThreadProc (0x737f8675)
        Stack Init a6933000 Current a6932b68 Base a6933000 Limit a6930000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a6932b80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a6932bbc 81c293a7 nt!KiSwapThread+0x389
        a6932c18 8cedb8ed nt!KeWaitForSingleObject+0x414
        a6932c74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        a6932c90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        a6932ce8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        a6932d4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        a6932d4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a6932d64)
        0253fcb0 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0253fcb4 761e19cd USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        0253fcd0 737f8712 USER32!GetMessageW+0x33 (FPO: [Non-Fpo])
        0253fd10 75f33833 wdmaud!CTaskThread::TaskThreadProc+0x9d (FPO: [Non-Fpo])
        0253fd1c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0253fd5c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 83692d78  Cid 0b90.0cd4  Teb: 7ffa8000 Win32Thread: fed0ce98 WAIT: (UserRequest)
UserMode Non-Alertable
            83697460  SynchronizationEvent
            a1927328  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8362a638       Image:         explorer.exe
        Wait Start TickCount      11437          Ticks: 32062 (0:00:08:20.170)
        Context Switch Count      561
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdmaud!CWorker::_StaticThreadProc (0x737f8544)
        Stack Init a685f000 Current a685e8d0 Base a685f000 Limit a685c000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a685e8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a685e924 81c28c64 nt!KiSwapThread+0x389
        a685e970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a685ebfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a685ed48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a685ed48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a685ed64)
        01f3f878 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01f3f87c 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        01f3f918 737f5111 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        01f3f950 737f855c wdmaud!CWorker::_ThreadProc+0x5e (FPO: [Non-Fpo])
        01f3f95c 75f33833 wdmaud!CWorker::_StaticThreadProc+0x18 (FPO: [Non-Fpo])
        01f3f968 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01f3f9a8 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 834a2d78  Cid 0b90.0e38  Teb: 7ffd4000 Win32Thread: ff36f9f0 WAIT: (UserRequest)
UserMode Non-Alertable
            83710760  SynchronizationEvent
            836252d8  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8362a638       Image:         explorer.exe
        Wait Start TickCount      42621          Ticks: 878 (0:00:00:13.696)
        Context Switch Count      1144
        UserTime                  00:00:00.046
        KernelTime                00:00:00.062
        Win32 Start Address stobject!CSysTray::SysTrayThreadProc (0x6f8e7170)
        Stack Init a8e65fe0 Current a8e658b0 Base a8e66000 Limit a8e63000 Call 3ec
        Priority 12 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a8e658c8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8e65904 81c28c64 nt!KiSwapThread+0x389
        a8e65950 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a8e65bdc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a8e65d28 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a8e65d28 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8e65d44)
        026cfaa0 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        026cfaa4 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        026cfb40 761dc4b7 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        026cfb94 73c2161a USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
        026cfbb4 73c21642 DUser!CoreSC::Wait+0x59 (FPO: [Non-Fpo])
        026cfbe8 73c216f6 DUser!CoreSC::xwProcessNL+0xaa (FPO: [Non-Fpo])
        026cfc0c 761daff1 DUser!MphProcessMessage+0x33 (FPO: [Non-Fpo])
        026cfc54 77490e6e USER32!__ClientGetMessageMPH+0x30 (FPO: [Non-Fpo])
        026cfc7c 761e199a ntdll!KiUserCallbackDispatcher+0x2e (FPO: [0,0,0])
        026cfc80 761e19cd USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        026cfc9c 6f8e195b USER32!GetMessageW+0x33 (FPO: [Non-Fpo])
        026cfd18 6f8e7187 stobject!SysTrayMain+0x211 (FPO: [Non-Fpo])
        026cfd30 75f33833 stobject!CSysTray::SysTrayThreadProc+0x17 (FPO: [Non-Fpo])
        026cfd3c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        026cfd7c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 836d0030  Cid 0b90.0e3c  Teb: 7ffad000 Win32Thread: ff3639f0 WAIT: (UserRequest)
UserMode Non-Alertable
            83633e20  SynchronizationEvent
            83633df0  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8362a638       Image:         explorer.exe
        Wait Start TickCount      11147          Ticks: 32352 (0:00:08:24.694)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address msvcrt!_endthreadex (0x7628639b)
        Stack Init 9f3fc000 Current 9f3fb8d0 Base 9f3fc000 Limit 9f3f9000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f3fb8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f3fb924 81c28c64 nt!KiSwapThread+0x389
        9f3fb970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f3fbbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f3fbd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f3fbd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f3fbd64)
        040ef7cc 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        040ef7d0 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        040ef86c 761dc4b7 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        040ef8c0 73c2161a USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
        040ef8e0 73c21642 DUser!CoreSC::Wait+0x59 (FPO: [Non-Fpo])
        040ef914 73c2c442 DUser!CoreSC::xwProcessNL+0xaa (FPO: [Non-Fpo])
        040ef934 73c2c3a2 DUser!GetMessageExA+0x44 (FPO: [Non-Fpo])
        040ef988 762862b6 DUser!ResourceManager::SharedThreadProc+0xb6 (FPO: [Non-Fpo])
        040ef9c0 762863de msvcrt!_endthreadex+0x44 (FPO: [Non-Fpo])
        040ef9c8 75f33833 msvcrt!_endthreadex+0xce (FPO: [Non-Fpo])
        040ef9d4 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        040efa14 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 836cd778  Cid 0b90.0e4c  Teb: 7ffa5000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            836d05b0  SynchronizationTimer
            83651e58  NotificationEvent
            8374b0b8  SynchronizationEvent
            83757af0  SynchronizationEvent
            83749678  SynchronizationEvent
            8374b418  SynchronizationEvent
            83678620  SynchronizationEvent
            838ed130  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8362a638       Image:         explorer.exe
        Wait Start TickCount      18192          Ticks: 25307 (0:00:06:34.791)
        Context Switch Count      19
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x7744b49a)
        Stack Init a099d000 Current a099c8d0 Base a099d000 Limit a099a000 Call 0
        Priority 12 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a099c8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a099c924 81c28c64 nt!KiSwapThread+0x389
        a099c970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a099cbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a099cd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a099cd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a099cd64)
        040afa90 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        040afa94 7744b65b ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        040afc30 75f33833 ntdll!TppWaiterpThread+0x294 (FPO: [Non-Fpo])
        040afc3c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        040afc7c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 835fa698  Cid 0b90.0e54  Teb: 7ffa4000 Win32Thread: ff35f9f0 WAIT: (WrUserRequest)
UserMode Non-Alertable
            835ee658  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8362a638       Image:         explorer.exe
        Wait Start TickCount      11132          Ticks: 32367 (0:00:08:24.928)
        Context Switch Count      43
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address MMDevAPI!CDeviceEnumerator::PnpNotificationThreadWrapper (0x74d94902)
        Stack Init a088b000 Current a088ab68 Base a088b000 Limit a0888000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a088ab80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a088abbc 81c293a7 nt!KiSwapThread+0x389
        a088ac18 8cedb8ed nt!KeWaitForSingleObject+0x414
        a088ac74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        a088ac90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        a088ace8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        a088ad4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        a088ad4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a088ad64)
        044af864 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        044af868 761e19cd USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        044af884 74d91b32 USER32!GetMessageW+0x33 (FPO: [Non-Fpo])
        044af914 74d9490f MMDevAPI!CDeviceEnumerator::PnpNotificationThread+0x1ad (FPO: [Non-Fpo])
        044af91c 75f33833 MMDevAPI!CDeviceEnumerator::PnpNotificationThreadWrapper+0xd (FPO: [Non-
Fpo])
        044af928 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        044af968 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 835fa3e0  Cid 0b90.0e58  Teb: 7ffa3000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            8370a148  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8362a638       Image:         explorer.exe
        Wait Start TickCount      9639           Ticks: 33860 (0:00:08:48.219)
        Context Switch Count      9
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address SndVolSSO!CServiceMonitor::Run (0x6f9f25c2)
        Stack Init 9f384000 Current 9f383c38 Base 9f384000 Limit 9f381000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f383c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f383c8c 81c293a7 nt!KiSwapThread+0x389
        9f383ce8 81df5057 nt!KeWaitForSingleObject+0x414
        9f383d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        9f383d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f383d64)
        0436fb18 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0436fb1c 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0436fb8c 6f9f2652 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        0436fbe8 75f33833 SndVolSSO!CServiceMonitor::Run+0x91 (FPO: [Non-Fpo])
        0436fbf4 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0436fc34 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 8350f800  Cid 0b90.0e5c  Teb: 7ffa2000 Win32Thread: ffbfe928 WAIT: (WrUserRequest)
UserMode Non-Alertable
            8350faa8  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8362a638       Image:         explorer.exe
        Wait Start TickCount      25364          Ticks: 18135 (0:00:04:42.907)
        Context Switch Count      42
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address SndVolSSO!CAudioVolumeShellService::VolumeThreadProc (0x6f9f15a2)
        Stack Init 9f388000 Current 9f387c10 Base 9f388000 Limit 9f385000 Call 0
        Priority 12 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f387c28 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f387c64 81c293a7 nt!KiSwapThread+0x389
        9f387cc0 8cedb8ed nt!KeWaitForSingleObject+0x414
        9f387d1c 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        9f387d38 8ced573c win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        9f387d4c 8ced5759 win32k!xxxRealWaitMessageEx+0x12 (FPO: [Non-Fpo])
        9f387d5c 81c8caaa win32k!NtUserWaitMessage+0x14 (FPO: [Non-Fpo])
        9f387d5c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f387d64)
        03f5f9bc 761db5bc ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        03f5f9c0 6f9f161a USER32!NtUserWaitMessage+0xc (FPO: [Non-Fpo])
        03f5f9e8 75f33833 SndVolSSO!CAudioVolumeShellService::VolumeThreadProc+0x80 (FPO: [Non-
Fpo])
        03f5f9f4 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        03f5fa34 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 8350f500  Cid 0b90.0e60  Teb: 7ffa1000 Win32Thread: ffbfbbf0 WAIT: (UserRequest)
UserMode Non-Alertable
            8370ac68  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8362a638       Image:         explorer.exe
        Wait Start TickCount      32755          Ticks: 10744 (0:00:02:47.607)
        Context Switch Count      182
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address SHLWAPI!WrapperThreadProc (0x763cb09a)
        Stack Init 9f38c000 Current 9f38b8d0 Base 9f38c000 Limit 9f389000 Call 0
        Priority 12 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f38b8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f38b924 81c28c64 nt!KiSwapThread+0x389
        9f38b970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f38bbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f38bd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f38bd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f38bd64)
        0456f874 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0456f878 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0456f914 761dc4b7 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0456f968 761d8b83 USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
        0456f984 6f9c14ce USER32!MsgWaitForMultipleObjects+0x1f (FPO: [Non-Fpo])
        0456f9cc 6f9c156b ehSSO!CMediaCenterSSOThread::MessagePump+0x2c (FPO: [Non-Fpo])
        0456f9dc 6f9c31e2 ehSSO!CMediaCenterSSOThread::ThreadProc+0x7c (FPO: [Non-Fpo])
        0456f9ec 763cb132 ehSSO!CMediaCenterSSOThread::s_ThreadProc+0x1e (FPO: [Non-Fpo])
        0456fa68 75f33833 SHLWAPI!WrapperThreadProc+0x10f (FPO: [Non-Fpo])
        0456fa74 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0456fab4 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 8374da20  Cid 0b90.0e64  Teb: 7ffa0000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            8374dd28  SynchronizationEvent
            8374daa8  NotificationTimer
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8362a638       Image:         explorer.exe
        Wait Start TickCount      28877          Ticks: 14622 (0:00:03:48.104)
        Context Switch Count      6
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ole32!CRpcThreadCache::RpcWorkerThreadEntry (0x7644fc53)
        Stack Init 9f398000 Current 9f397c38 Base 9f398000 Limit 9f395000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f397c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f397c8c 81c293a7 nt!KiSwapThread+0x389
        9f397ce8 81df5057 nt!KeWaitForSingleObject+0x414
        9f397d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        9f397d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f397d64)
        0257fa40 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0257fa44 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0257fab4 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        0257fac8 76455251 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0257fae4 76422104 ole32!CDllHost::MTAWorkerLoop+0x2b (FPO: [Non-Fpo])
        0257fb04 764524ce ole32!CDllHost::WorkerThread+0xc7 (FPO: [Non-Fpo])
        0257fb0c 7644fc0d ole32!DLLHostThreadEntry+0xd (FPO: [Non-Fpo])
        0257fb28 7644fc73 ole32!CRpcThread::WorkerLoop+0x26 (FPO: [Non-Fpo])
        0257fb34 75f33833 ole32!CRpcThreadCache::RpcWorkerThreadEntry+0x20 (FPO: [Non-Fpo])
        0257fb40 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0257fb80 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 836bbd78  Cid 0b90.0e6c  Teb: 7ff9e000 Win32Thread: ff77d190 WAIT: (UserRequest)
UserMode Non-Alertable
            83706f48  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8362a638       Image:         explorer.exe
        Wait Start TickCount      10233          Ticks: 33266 (0:00:08:38.952)
        Context Switch Count      6
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address FunDisc!CNotificationQueue::ThreadProc (0x72a2154d)
        Stack Init 9f3a0000 Current 9f39fc38 Base 9f3a0000 Limit 9f39d000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 3 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f39fc50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f39fc8c 81c293a7 nt!KiSwapThread+0x389
        9f39fce8 81df5057 nt!KeWaitForSingleObject+0x414
        9f39fd50 81c8caaa nt!NtWaitForSingleObject+0xbe
        9f39fd50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f39fd64)
        04a3febc 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        04a3fec0 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        04a3ff30 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        04a3ff44 72a215ed kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        04a3ff68 75f33833 FunDisc!CNotificationQueue::ThreadProc+0x24f (FPO: [Non-Fpo])
        04a3ff74 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        04a3ffb4 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 83746d78  Cid 0b90.0eb8  Teb: 7ff9c000 Win32Thread: fe6f21c0 WAIT: (UserRequest)
UserMode Alertable
            8360ad28  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8362a638       Image:         explorer.exe
        Wait Start TickCount      43413          Ticks: 86 (0:00:00:01.341)
        Context Switch Count      81
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address Wlanapi!NotificationApcThreadProc (0x6fa94619)
        Stack Init a8f54000 Current a8f53c38 Base a8f54000 Limit a8f51000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a8f53c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8f53c8c 81c293a7 nt!KiSwapThread+0x389
        a8f53ce8 81df5057 nt!KeWaitForSingleObject+0x414
        a8f53d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a8f53d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8f53d64)
        042ef83c 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        042ef840 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        042ef8b0 6fa9466d kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        042ef8d4 75f33833 Wlanapi!NotificationApcThreadProc+0x54 (FPO: [Non-Fpo])
        042ef8e0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        042ef920 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 837457c0  Cid 0b90.0ec0  Teb: 7ff9b000 Win32Thread: ff32e290 WAIT: (WrUserRequest)
UserMode Non-Alertable
            83635a20  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8362a638       Image:         explorer.exe
        Wait Start TickCount      18553          Ticks: 24946 (0:00:06:29.160)
        Context Switch Count      167
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address SHLWAPI!WrapperThreadProc (0x763cb09a)
        Stack Init a8f58000 Current a8f57b68 Base a8f58000 Limit a8f55000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a8f57b80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8f57bbc 81c293a7 nt!KiSwapThread+0x389
        a8f57c18 8cedb8ed nt!KeWaitForSingleObject+0x414
        a8f57c74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        a8f57c90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        a8f57ce8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        a8f57d4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        a8f57d4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8f57d64)
        04defe98 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        04defe9c 761e19cd USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        04defeb8 6fa61549 USER32!GetMessageW+0x33 (FPO: [Non-Fpo])
        04defef4 6fa65607 AltTab!RunMessagePump+0x31 (FPO: [Non-Fpo])
        04deff08 6fa65589 AltTab!AltTabRun+0x68 (FPO: [Non-Fpo])
        04deff1c 763cb132 AltTab!CAltTabSSO::_ThreadProc+0x24 (FPO: [Non-Fpo])
        04deff98 75f33833 SHLWAPI!WrapperThreadProc+0x10f (FPO: [Non-Fpo])
        04deffa4 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        04deffe4 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 836aab00  Cid 0b90.0ec4  Teb: 7ff9a000 Win32Thread: ffac5568 WAIT: (WrUserRequest)
UserMode Non-Alertable
            836aaac0  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8362a638       Image:         explorer.exe
        Wait Start TickCount      43498          Ticks: 1 (0:00:00:00.015)
        Context Switch Count      13110
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address SHLWAPI!WrapperThreadProc (0x763cb09a)
        Stack Init a8f64000 Current a8f63b68 Base a8f64000 Limit a8f61000 Call 0
        Priority 12 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a8f63b80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8f63bbc 81c293a7 nt!KiSwapThread+0x389
        a8f63c18 8cedb8ed nt!KeWaitForSingleObject+0x414
        a8f63c74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        a8f63c90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        a8f63ce8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        a8f63d4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        a8f63d4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8f63d64)
        0442f92c 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0442f930 761e19cd USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        0442f94c 6f56a8fc USER32!GetMessageW+0x33 (FPO: [Non-Fpo])
        0442fab0 763cb132 wpdshserviceobj!CWPDShServiceObj::_SvcObjThreadProc+0x15d (FPO: [Non-
Fpo])
        0442fb2c 75f33833 SHLWAPI!WrapperThreadProc+0x10f (FPO: [Non-Fpo])
        0442fb38 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0442fb78 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 836aa818  Cid 0b90.0ec8  Teb: 7ff99000 Win32Thread: ffa96618 WAIT: (UserRequest)
UserMode Alertable
            8364c6b4  NotificationEvent
            836aa720  SynchronizationEvent
        IRP List:
            836ba008: (0006,01d8) Flags: 00060000  Mdl: 00000000
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8362a638       Image:         explorer.exe
        Wait Start TickCount      9661           Ticks: 33838 (0:00:08:47.876)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address SHLWAPI!WrapperThreadProc (0x763cb09a)
        Stack Init a8f5c000 Current a8f5b8d0 Base a8f5c000 Limit a8f59000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a8f5b8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8f5b924 81c28c64 nt!KiSwapThread+0x389
        a8f5b970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a8f5bbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a8f5bd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a8f5bd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8f5bd64)
        053ff624 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        053ff628 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        053ff6c4 761dc4b7 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        053ff718 6f569c5b USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
        053ff88c 763cb132 wpdshserviceobj!CWPDShServiceObj::_SqmUploadThreadProc+0xf0 (FPO: [Non-
Fpo])
        053ff908 75f33833 SHLWAPI!WrapperThreadProc+0x10f (FPO: [Non-Fpo])
        053ff914 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        053ff954 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 836bad40  Cid 0b90.0ecc  Teb: 7ff98000 Win32Thread: ff2f8ad0 WAIT: (UserRequest)
UserMode Alertable
            83488a30  SynchronizationEvent
            836bab70  SynchronizationEvent
            836bab08  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8362a638       Image:         explorer.exe
        Wait Start TickCount      32755          Ticks: 10744 (0:00:02:47.607)
        Context Switch Count      117
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address SHLWAPI!WrapperThreadProc (0x763cb09a)
        Stack Init a8f60000 Current a8f5f8d0 Base a8f60000 Limit a8f5d000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a8f5f8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8f5f924 81c28c64 nt!KiSwapThread+0x389
        a8f5f970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a8f5fbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a8f5fd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a8f5fd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8f5fd64)
        04f1f604 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        04f1f608 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        04f1f6a4 761dc4b7 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        04f1f6f8 6f0f1615 USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
        04f1f784 6f0f35d1 srchadmin!CSrchAdminSSO::_SvcObjThreadProc+0x136 (FPO: [Non-Fpo])
        04f1f794 763cb132 srchadmin!CSrchAdminSSO::s_SvcObjThreadProc+0x11 (FPO: [Non-Fpo])
        04f1f810 75f33833 SHLWAPI!WrapperThreadProc+0x10f (FPO: [Non-Fpo])
        04f1f81c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        04f1f85c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 8374b748  Cid 0b90.0ed4  Teb: 7ff96000 Win32Thread: ff330860 WAIT: (UserRequest)
UserMode Non-Alertable
            8374b678  SynchronizationEvent
            8374b9f0  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8362a638       Image:         explorer.exe
        Wait Start TickCount      11132          Ticks: 32367 (0:00:08:24.928)
        Context Switch Count      89
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address SHLWAPI!WrapperThreadProc (0x763cb09a)
        Stack Init a8f70000 Current a8f6f8d0 Base a8f70000 Limit a8f6d000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a8f6f8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8f6f924 81c28c64 nt!KiSwapThread+0x389
        a8f6f970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a8f6fbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a8f6fd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a8f6fd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8f6fd64)
        04c9f6fc 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        04c9f700 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        04c9f79c 761dc4b7 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        04c9f7f0 761d8b83 USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
        04c9f80c 6f5215b7 USER32!MsgWaitForMultipleObjects+0x1f (FPO: [Non-Fpo])
        04c9f854 6f524a78 wscntfy!CNotifyWindow::WinMain+0x97 (FPO: [Non-Fpo])
        04c9fc7c 763cb132 wscntfy!CWscNotify::_ExecThread+0x37 (FPO: [Non-Fpo])
        04c9fcf8 75f33833 SHLWAPI!WrapperThreadProc+0x10f (FPO: [Non-Fpo])
        04c9fd04 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        04c9fd44 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 8374b140  Cid 0b90.0ed8  Teb: 7ff95000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Alertable
            8370dbf8  QueueObject
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8362a638       Image:         explorer.exe
        Wait Start TickCount      18192          Ticks: 25307 (0:00:06:34.791)
        Context Switch Count      40
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init a8f74000 Current a8f73bc8 Base a8f74000 Limit a8f71000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a8f73be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8f73c1c 81cad431 nt!KiSwapThread+0x389
        a8f73c68 81d8b982 nt!KeRemoveQueueEx+0x568
        a8f73cc0 81c7a036 nt!IoRemoveIoCompletion+0x23
        a8f73d54 81c8caaa nt!NtWaitForWorkViaWorkerFactory+0x1a1
        a8f73d54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8f73d64)
        058ffc70 77490850 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        058ffc74 7749a1b4 ntdll!NtWaitForWorkViaWorkerFactory+0xc (FPO: [2,0,0])
        058ffd9c 75f33833 ntdll!TppWorkerThread+0x1f6 (FPO: [Non-Fpo])
        058ffda8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        058ffde8 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 8361d5f8  Cid 0b90.0210  Teb: 7ff97000 Win32Thread: fe743b80 WAIT: (WrUserRequest)
UserMode Non-Alertable
            83739eb0  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8362a638       Image:         explorer.exe
        Wait Start TickCount      11132          Ticks: 32367 (0:00:08:24.928)
        Context Switch Count      73
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address SHLWAPI!WrapperThreadProc (0x763cb09a)
        Stack Init a8f04000 Current a8f03b68 Base a8f04000 Limit a8f01000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a8f03b80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8f03bbc 81c293a7 nt!KiSwapThread+0x389
        a8f03c18 8cedb8ed nt!KeWaitForSingleObject+0x414
        a8f03c74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        a8f03c90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        a8f03ce8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        a8f03d4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        a8f03d4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8f03d64)
        049ef858 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        049ef85c 761e19cd USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        049ef878 6d855470 USER32!GetMessageW+0x33 (FPO: [Non-Fpo])
        049ef920 763cb132 bthprops!BluetoothAuthenticationAgent+0x11a (FPO: [Non-Fpo])
        049ef99c 75f33833 SHLWAPI!WrapperThreadProc+0x10f (FPO: [Non-Fpo])
        049ef9a8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        049ef9e8 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 837c9ab0  Cid 0b90.01b0  Teb: 7ffd6000 Win32Thread: fe6e8bb8 WAIT: (WrUserRequest)
UserMode Non-Alertable
            836cf480  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8362a638       Image:         explorer.exe
        Wait Start TickCount      34253          Ticks: 9246 (0:00:02:24.238)
        Context Switch Count      30
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address SHLWAPI!WrapperThreadProc (0x763cb09a)
        Stack Init a8fd4000 Current a8fd3b68 Base a8fd4000 Limit a8fd1000 Call 0
        Priority 12 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a8fd3b80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8fd3bbc 81c293a7 nt!KiSwapThread+0x389
        a8fd3c18 8cedb8ed nt!KeWaitForSingleObject+0x414
        a8fd3c74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        a8fd3c90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        a8fd3ce8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        a8fd3d4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        a8fd3d4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8fd3d64)
        04edfa38 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        04edfa3c 761e19cd USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        04edfa58 765b0c40 USER32!GetMessageW+0x33 (FPO: [Non-Fpo])
        04edfa98 763cb132 SHELL32!_LocalServerThread+0x3a (FPO: [Non-Fpo])
        04edfb14 75f33833 SHLWAPI!WrapperThreadProc+0x10f (FPO: [Non-Fpo])
        04edfb20 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        04edfb60 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 837c64c8  Cid 0b90.00fc  Teb: 7ffd5000 Win32Thread: ff6d30d0 WAIT: (UserRequest)
UserMode Non-Alertable
            835b1660  SynchronizationEvent
            835c4178  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8362a638       Image:         explorer.exe
        Wait Start TickCount      34750          Ticks: 8749 (0:00:02:16.485)
        Context Switch Count      7625
        UserTime                  00:00:00.546
        KernelTime                00:00:01.014
        Win32 Start Address BROWSEUI!BrowserNewThreadProc (0x70bacc4d)
        Stack Init a8f47fe0 Current a8f478b0 Base a8f48000 Limit a8f45000 Call 374
        Priority 11 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a8f478c8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8f47904 81c28c64 nt!KiSwapThread+0x389
        a8f47950 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a8f47bdc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a8f47d28 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a8f47d28 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8f47d44)
        055dfcbc 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        055dfcc0 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        055dfd5c 761dc4b7 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        055dfdb0 73c2161a USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
        055dfdd0 73c22cb6 DUser!CoreSC::Wait+0x59 (FPO: [Non-Fpo])
        055dfdf8 73c22c55 DUser!CoreSC::WaitMessage+0x54 (FPO: [Non-Fpo])
        055dfe08 761d15c0 DUser!MphWaitMessageEx+0x22 (FPO: [Non-Fpo])
        055dfe24 77490e6e USER32!__ClientWaitMessageExMPH+0x1e (FPO: [Non-Fpo])
        055dfe40 761db5bc ntdll!KiUserCallbackDispatcher+0x2e (FPO: [0,0,0])
        055dfe44 70bab93e USER32!NtUserWaitMessage+0xc (FPO: [Non-Fpo])
        055dfe7c 70bacb0b BROWSEUI!CBrowserFrame::FrameMessagePump+0x14f (FPO: [Non-Fpo])
        055dfe90 70bacc90 BROWSEUI!BrowserThreadProc+0x5e (FPO: [Non-Fpo])
        055dfea8 75f33833 BROWSEUI!BrowserNewThreadProc+0x43 (FPO: [Non-Fpo])
        055dfeb4 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        055dfef4 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 837c4388  Cid 0b90.0418  Teb: 7ff92000 Win32Thread: fe6e8208 WAIT: (WrUserRequest)
UserMode Non-Alertable
            83685660  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8362a638       Image:         explorer.exe
        Wait Start TickCount      11437          Ticks: 32062 (0:00:08:20.170)
        Context Switch Count      94
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address WINMM!mciwindow (0x738c1385)
        Stack Init 9f7a0000 Current 9f79fb68 Base 9f7a0000 Limit 9f79d000 Call 0
        Priority 13 BasePriority 10 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f79fb80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f79fbbc 81c293a7 nt!KiSwapThread+0x389
        9f79fc18 8cedb8ed nt!KeWaitForSingleObject+0x414
        9f79fc74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        9f79fc90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        9f79fce8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        9f79fd4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        9f79fd4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f79fd64)
        0627fa48 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0627fa4c 761d3ad1 USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        0627fa70 738c1404 USER32!GetMessageA+0x8a (FPO: [Non-Fpo])
        0627faa8 75f33833 WINMM!mciwindow+0x102 (FPO: [Non-Fpo])
        0627fab4 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0627faf4 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 835d9090  Cid 0b90.0484  Teb: 7ffde000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            8368f380  QueueObject
            835d9118  NotificationTimer
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8362a638       Image:         explorer.exe
        Wait Start TickCount      43413          Ticks: 86 (0:00:00:01.341)
        Context Switch Count      24
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init 9f73c000 Current 9f73bbc8 Base 9f73c000 Limit 9f739000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f73bbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f73bc1c 81cad431 nt!KiSwapThread+0x389
        9f73bc6c 81d8b982 nt!KeRemoveQueueEx+0x568
        9f73bcc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        9f73bd48 81c8caaa nt!NtRemoveIoCompletion+0x106
        9f73bd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f73bd64)
        01b3f9f8 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01b3f9fc 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        01b3fa28 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        01b3fa64 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        01b3fad0 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        01b3fadc 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        01b3fb00 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        01b3fb0c 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        01b3fb18 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01b3fb58 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

MSASCui process

```
PROCESS 836999f8  SessionId: 1  Cid: 0c64    Peb: 7ffdd000  ParentCid: 0b90
    DirBase: 29a014a0  ObjectTable: a8b87520  HandleCount: 329.
    Image: MSASCui.exe
    VadRoot 9fd10dc0 Vads 104 Clone 0 Private 1039. Modified 795. Locked 0.
    DeviceMap a7766db8
    Token                             a8bc7030
    ElapsedTime                       00:08:53.199
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         135744
    QuotaPoolUsage[NonPagedPool]      11056
    Working Set Sizes (now,min,max)  (1085, 50, 345) (4340KB, 200KB, 1380KB)
    PeakWorkingSetSize                2013
    VirtualSize                       69 Mb
    PeakVirtualSize                   74 Mb
    PageFaultCount                    3718
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      1268
    Job                               83658020

    Setting context for this process...
.process /p /r ffffffff836999f8

    !peb
PEB at 7ffdd000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         000d0000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 003c17e0 . 003faa98
    Ldr.InLoadOrderModuleList:           003c1760 . 003faaf8
    Ldr.InMemoryOrderModuleList:         003c1768 . 003fab00
            Base TimeStamp                     Module
           d0000 45ad82d9 Jan 17 01:58:49 2007 C:\Program Files\Windows Defender\MSASCui.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        76560000 4681c95d Jun 27 03:20:13 2007 C:\Windows\system32\SHELL32.dll
        763b0000 4549bdb9 Nov 02 09:43:21 2006 C:\Windows\system32\SHLWAPI.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        74e30000 45ad8fe2 Jan 17 02:54:26 2007 C:\Program Files\Windows Defender\MpClient.dll
        75ba0000 4549bde2 Nov 02 09:44:02 2006 C:\Windows\system32\USERENV.dll
        75b80000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\Secur32.dll
        73d70000 4549bcaf Nov 02 09:38:55 2006
C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.0.6000.16386_none_9ea0ac9ec96e71
27\gdiplus.dll
        74aa0000 4549bd09 Nov 02 09:40:25 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_5d07289e07e1d100\COMCTL32.dll
        73880000 4549bd93 Nov 02 09:42:43 2006 C:\Windows\system32\OLEACC.dll
        70290000 45ad8feb Jan 17 02:54:35 2007 C:\Program Files\Windows Defender\MsMpRes.dll
        701e0000 45ad8fe5 Jan 17 02:54:29 2007 C:\Program Files\Windows Defender\MpRtMon.DLL
        75840000 4549bd53 Nov 02 09:41:39 2006 C:\Windows\system32\NETAPI32.dll
        75ce0000 4549bd99 Nov 02 09:42:49 2006 C:\Windows\system32\PSAPI.DLL
        73420000 4549be18 Nov 02 09:44:56 2006 C:\Windows\system32\WINHTTP.dll
        75dc0000 470c4de2 Oct 10 04:58:26 2007 C:\Windows\system32\urlmon.dll
        76360000 4549bcfb Nov 02 09:40:11 2006 C:\Windows\system32\iertutil.dll
        753f0000 4549bde4 Nov 02 09:44:04 2006 C:\Windows\system32\VERSION.dll
```

```
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        746d0000 4549bde7 Nov 02 09:44:07 2006 C:\Windows\system32\uxtheme.dll
        6e000000 4689b074 Jul 03 03:12:04 2007 C:\Windows\system32\MSFTEDIT.DLL
        75350000 4549bdae Nov 02 09:43:10 2006 C:\Windows\system32\rsaenh.dll
        75480000 4549bd20 Nov 02 09:40:48 2006 C:\Windows\system32\credssp.dll
        75650000 45b96fde Jan 26 03:05:02 2007 C:\Windows\system32\CRYPT32.dll
        75820000 4549bd41 Nov 02 09:41:21 2006 C:\Windows\system32\MSASN1.dll
        75050000 46773a78 Jun 19 03:07:52 2007 C:\Windows\system32\schannel.dll
        75330000 4549bcd7 Nov 02 09:39:35 2006 C:\Windows\system32\GPAPI.dll
        75610000 4679de70 Jun 21 03:12:00 2007 C:\Windows\system32\slc.dll
    SubSystemData:     00000000
    ProcessHeap:       003c0000
    ProcessParameters: 003c1010
    WindowTitle:  'C:\Program Files\Windows Defender\MSASCui.exe'
    ImageFile:    'C:\Program Files\Windows Defender\MSASCui.exe'
    CommandLine:  '"C:\Program Files\Windows Defender\MSASCui.exe" -hide'
    DllPath:      'C:\Program Files\Windows
Defender;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Windows;C:\Windo
ws\System32\Wbem;C:\Program Files\QuickTime\QTSystem\'
    Environment:  003e91d8
        =::=::\
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\UserName\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        HOMEDRIVE=C:
        HOMEPATH=\Users\UserName
        LOCALAPPDATA=C:\Users\UserName\AppData\Local
        LOGONSERVER=\\HOME
        MpConfig_ProductAppDataPath=C:\ProgramData\Microsoft\Windows Defender
        MpConfig_ProductCodeName=AntiSpyware
        MpConfig_ProductPath=C:\Program Files\Windows Defender
        MpConfig_ProductUserAppDataPath=C:\Users\UserName\AppData\Local\Microsoft\Windows Defender
        MpConfig_ReportingGUID=9E105B54-307A-4903-9E49-E8DE56BD66B8
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        SESSIONNAME=Console
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Users\UserName\AppData\Local\Temp
        TMP=C:\Users\UserName\AppData\Local\Temp
        USERDOMAIN=home
        USERNAME=UserName
        USERPROFILE=C:\Users\UserName
        windir=C:\Windows
```

```
        THREAD 836735e8  Cid 0c64.0c68  Teb: 7ffdf000 Win32Thread: ff2f6bb8 WAIT: (WrUserRequest)
UserMode Non-Alertable
            9fd13b18  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            836999f8       Image:         MSASCui.exe
        Wait Start TickCount      11132          Ticks: 32367 (0:00:08:24.928)
        Context Switch Count      1003
        UserTime                  00:00:00.124
        KernelTime                00:00:00.109
        Win32 Start Address MSASCui!wWinMainCRTStartup (0x00132b27)
        Stack Init a68ab000 Current a68aab68 Base a68ab000 Limit a68a8000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a68aab80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a68aabbc 81c293a7 nt!KiSwapThread+0x389
        a68aac18 8cedb8ed nt!KeWaitForSingleObject+0x414
        a68aac74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        a68aac90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        a68aace8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        a68aad4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        a68aad4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a68aad64)
        0028fca4 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0028fca8 761e19cd USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        0028fcc4 000ee0b5 USER32!GetMessageW+0x33 (FPO: [Non-Fpo])
        0028fd50 000ee295 MSASCui!CAntiSpywareUIModule::DisplayUI+0x2d2 (FPO: [Non-Fpo])
        0028fd7c 001329c2 MSASCui!wWinMain+0x157 (FPO: [Non-Fpo])
        0028fe10 75f33833 MSASCui!_initterm_e+0x1b1 (FPO: [Non-Fpo])
        0028fe1c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0028fe5c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 847b2808  Cid 0c64.0fb0  Teb: 7ffde000 Win32Thread: ff32edf8 WAIT: (UserRequest)
UserMode Non-Alertable
            84df02e8  NotificationEvent
            837d9a30  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            836999f8       Image:         MSASCui.exe
        Wait Start TickCount      11132          Ticks: 32367 (0:00:08:24.928)
        Context Switch Count      61
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address gdiplus!BackgroundThreadProc (0x73d81909)
        Stack Init a8f40000 Current a8f3f8d0 Base a8f40000 Limit a8f3d000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a8f3f8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8f3f924 81c28c64 nt!KiSwapThread+0x389
        a8f3f970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a8f3fbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a8f3fd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a8f3fd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8f3fd64)
        012afc60 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        012afc64 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        012afd00 761dc4b7 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        012afd54 761d8b83 USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
        012afd70 73d81965 USER32!MsgWaitForMultipleObjects+0x1f (FPO: [Non-Fpo])
        012afdbc 75f33833 gdiplus!BackgroundThreadProc+0x59 (FPO: [Non-Fpo])
        012afdc8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        012afe08 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 835fca28  Cid 0c64.0670  Teb: 7ffdc000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            83584530  SynchronizationEvent
            836951e0  Semaphore Limit 0x9c4
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            836999f8       Image:         MSASCui.exe
        Wait Start TickCount      10001          Ticks: 33498 (0:00:08:42.572)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address
MpRtMon!Realtime::CEventQueue<Realtime::CFsWatcher::CFsEvent>::_WorkerThread (0x7023da0c)
        Stack Init 9f76c000 Current 9f76b8d0 Base 9f76c000 Limit 9f769000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f76b8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f76b924 81c28c64 nt!KiSwapThread+0x389
        9f76b970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f76bbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f76bd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f76bd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f76bd64)
        0177f71c 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0177f720 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0177f7bc 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0177f7d8 7023da40 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0177f80c 75f33833
MpRtMon!Realtime::CEventQueue<Realtime::CFsWatcher::CFsEvent>::_WorkerThread+0x34 (FPO: [Non-Fpo])
        0177f818 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0177f858 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 835fc5d8  Cid 0c64.06a4  Teb: 7ffdb000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            835fc880  SynchronizationTimer
            8363de30  SynchronizationEvent
            835fc938  SynchronizationTimer
            835fc510  SynchronizationTimer
            837d3020  SynchronizationEvent
            837d31e0  SynchronizationEvent
            8363e0a0  SynchronizationEvent
            8363dcf8  SynchronizationEvent
            8363dcc8  SynchronizationEvent
            8363dc98  SynchronizationEvent
            836b0270  SynchronizationEvent
            836b0240  SynchronizationEvent
            8368bf08  SynchronizationEvent
            836af3d8  SynchronizationEvent
            8363b670  SynchronizationEvent
            8363dd98  SynchronizationEvent
            83617950  SynchronizationEvent
            9fd16720  SynchronizationEvent
            836bf5f8  SynchronizationEvent
            836bf4b8  SynchronizationEvent
            836bf488  SynchronizationEvent
            836bf428  SynchronizationEvent
            836ab498  SynchronizationEvent
            836ab468  SynchronizationEvent
            835fd190  SynchronizationEvent
            835fd160  SynchronizationEvent
            836925f8  SynchronizationEvent
            836925c8  SynchronizationEvent
            836bf6a8  SynchronizationEvent
            8363d368  SynchronizationEvent
            8363d338  SynchronizationEvent
            836af598  SynchronizationEvent
            835d84a8  SynchronizationEvent
            836926c0  SynchronizationEvent
            83692690  SynchronizationEvent
            8366e238  SynchronizationEvent
            8366e208  SynchronizationEvent
            836bf640  SynchronizationEvent
            836a0268  SynchronizationEvent
            836ab508  SynchronizationEvent
            836a3638  SynchronizationEvent
            9e1e9510  SynchronizationEvent
            8363b500  SynchronizationEvent
            837d5b68  SynchronizationEvent
            836cf278  SynchronizationEvent
            836cf2a8  SynchronizationEvent
            836cf2d8  SynchronizationEvent
            8363a468  SynchronizationEvent
            8361ba00  SynchronizationEvent
            8363a438  SynchronizationEvent
            8361b9d0  SynchronizationEvent
            8363b640  SynchronizationEvent
            836af408  SynchronizationEvent
            8361b9a0  SynchronizationEvent
            835fd210  SynchronizationEvent
            835fd240  SynchronizationEvent
            836147b8  SynchronizationEvent
            836b0210  SynchronizationEvent
            836147f0  SynchronizationEvent
            8363a498  SynchronizationEvent
            836af5d8  SynchronizationEvent
            836bf458  SynchronizationEvent
            9fd16800  SynchronizationEvent
            8363b4d0  SynchronizationEvent
            835fc660  NotificationTimer
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            836999f8       Image:         MSASCui.exe
```

```
        Wait Start TickCount      24251          Ticks: 19248 (0:00:05:00.270)
        Context Switch Count      199
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x7744b49a)
        Stack Init 9f754000 Current 9f7538d0 Base 9f754000 Limit 9f751000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f7538e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f753924 81c28c64 nt!KiSwapThread+0x389
        9f753970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f753bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f753d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f753d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f753d64)
        0122f80c 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0122f810 7744b65b ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0122f9ac 75f33833 ntdll!TppWaiterpThread+0x294 (FPO: [Non-Fpo])
        0122f9b8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0122f9f8 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 835fc230  Cid 0c64.0128  Teb: 7ffda000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            83617660  SynchronizationEvent
            8363d258  Semaphore Limit 0x400
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            836999f8       Image:         MSASCui.exe
        Wait Start TickCount      10001          Ticks: 33498 (0:00:08:42.572)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address MpRtMon!Realtime::CEventQueue<Realtime::CMpEventWatcher>::_WorkerThread
(0x70245c78)
        Stack Init 9f74c000 Current 9f74b8d0 Base 9f74c000 Limit 9f749000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f74b8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f74b924 81c28c64 nt!KiSwapThread+0x389
        9f74b970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f74bbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f74bd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f74bd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f74bd64)
        017ef8fc 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        017ef900 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        017ef99c 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        017ef9b8 70245cac kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        017ef9ec 75f33833
MpRtMon!Realtime::CEventQueue<Realtime::CMpEventWatcher>::_WorkerThread+0x34 (FPO: [Non-Fpo])
        017ef9f8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        017efa38 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 8363ea58  Cid 0c64.0508  Teb: 7ffd9000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            9fc34568  SynchronizationEvent
            9fc4d808  NotificationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            836999f8       Image:         MSASCui.exe
        Wait Start TickCount      10001          Ticks: 33498 (0:00:08:42.572)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address MpClient!MpEventWorker (0x74e3bb6f)
        Stack Init 9f774000 Current 9f7738d0 Base 9f774000 Limit 9f771000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f7738e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f773924 81c28c64 nt!KiSwapThread+0x389
        9f773970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f773bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f773d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f773d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f773d64)
        0039f804 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0039f808 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0039f8a4 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0039f8c0 74e3bc49 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0039f930 75f33833 MpClient!MpEventWorker+0xda (FPO: [Non-Fpo])
        0039f93c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0039f97c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 8363e6b8  Cid 0c64.053c  Teb: 7ffd8000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            836a6618  SynchronizationEvent
            8363e9c8  Semaphore Limit 0x2710
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            836999f8       Image:         MSASCui.exe
        Wait Start TickCount      14164          Ticks: 29335 (0:00:07:37.628)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address
MpRtMon!Realtime::CEventQueue<Realtime::CRegWatcher::CRegEvent>::_WorkerThread (0x70248a1d)
        Stack Init 9f7a8000 Current 9f7a78d0 Base 9f7a8000 Limit 9f7a5000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f7a78e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f7a7924 81c28c64 nt!KiSwapThread+0x389
        9f7a7970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f7a7bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f7a7d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f7a7d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f7a7d64)
        018afd68 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        018afd6c 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        018afe08 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        018afe24 70248ab7 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        018afe58 75f33833
MpRtMon!Realtime::CEventQueue<Realtime::CRegWatcher::CRegEvent>::_WorkerThread+0x9a (FPO: [Non-
Fpo])
        018afe64 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        018afea4 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 8363e358  Cid 0c64.04b8  Teb: 7ffd7000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            836aba08  QueueObject
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            836999f8       Image:         MSASCui.exe
        Wait Start TickCount      17693          Ticks: 25806 (0:00:06:42.576)
        Context Switch Count      20
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init 9f768000 Current 9f767bc8 Base 9f768000 Limit 9f765000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f767be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f767c1c 81cad431 nt!KiSwapThread+0x389
        9f767c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        9f767cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        9f767d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        9f767d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f767d64)
        0195fe80 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0195fe84 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        0195feb0 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        0195feec 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        0195ff58 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        0195ff64 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        0195ff88 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        0195ff94 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        0195ffa0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0195ffe0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 836929e0  Cid 0c64.0834  Teb: 7ffd6000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Alertable
            8363e178  QueueObject
        IRP List:
            8363b688: (0006,01d8) Flags: 00020000  Mdl: 00000000
            8363d580: (0006,01d8) Flags: 00020000  Mdl: 00000000
            836bfa18: (0006,01d8) Flags: 00020000  Mdl: 00000000
            836cf008: (0006,01d8) Flags: 00020000  Mdl: 00000000
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            836999f8       Image:         MSASCui.exe
        Wait Start TickCount      24252          Ticks: 19247 (0:00:05:00.255)
        Context Switch Count      264
        UserTime                  00:00:00.046
        KernelTime                00:00:00.031
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init 9f778000 Current 9f777bc8 Base 9f778000 Limit 9f775000 Call 0
        Priority 12 BasePriority 8 PriorityDecrement 3 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f777be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f777c1c 81cad431 nt!KiSwapThread+0x389
        9f777c68 81d8b982 nt!KeRemoveQueueEx+0x568
        9f777cc0 81c7a036 nt!IoRemoveIoCompletion+0x23
        9f777d54 81c8caaa nt!NtWaitForWorkViaWorkerFactory+0x1a1
        9f777d54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f777d64)
        0164f8a4 77490850 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0164f8a8 7749a1b4 ntdll!NtWaitForWorkViaWorkerFactory+0xc (FPO: [2,0,0])
        0164f9d0 75f33833 ntdll!TppWorkerThread+0x1f6 (FPO: [Non-Fpo])
        0164f9dc 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0164fa1c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 836826f0  Cid 0c64.0780  Teb: 7ffd5000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            836a3768  SynchronizationTimer
            836a0a78  SynchronizationEvent
            83682778  NotificationTimer
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            836999f8       Image:         MSASCui.exe
        Wait Start TickCount      10028          Ticks: 33471 (0:00:08:42.150)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x7744b49a)
        Stack Init 9f764000 Current 9f7638d0 Base 9f764000 Limit 9f761000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f7638e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f763924 81c28c64 nt!KiSwapThread+0x389
        9f763970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f763bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f763d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f763d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f763d64)
        0182fa70 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0182fa74 7744b65b ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0182fc10 75f33833 ntdll!TppWaiterpThread+0x294 (FPO: [Non-Fpo])
        0182fc1c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0182fc5c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 836a39c8  Cid 0c64.0740  Teb: 7ffd4000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            836b0150  SynchronizationEvent
            836b0180  NotificationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            836999f8       Image:         MSASCui.exe
        Wait Start TickCount      10028          Ticks: 33471 (0:00:08:42.150)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address MpClient!MpEventWorker (0x74e3bb6f)
        Stack Init 9f770000 Current 9f76f8d0 Base 9f770000 Limit 9f76d000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f76f8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f76f924 81c28c64 nt!KiSwapThread+0x389
        9f76f970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f76fbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f76fd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f76fd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f76fd64)
        01c3f6a8 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01c3f6ac 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        01c3f748 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        01c3f764 74e3bc49 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        01c3f7d4 75f33833 MpClient!MpEventWorker+0xda (FPO: [Non-Fpo])
        01c3f7e0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01c3f820 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Igfxtray process

```
PROCESS 8364a488  SessionId: 1  Cid: 0c6c    Peb: 7ffd8000  ParentCid: 0b90
    DirBase: 29a014c0  ObjectTable: a7695278  HandleCount:  66.
    Image: igfxtray.exe
    VadRoot 836fc958 Vads 57 Clone 0 Private 246. Modified 158. Locked 0.
    DeviceMap a7766db8
    Token                             a8bfcca0
    ElapsedTime                       00:08:53.137
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         85656
    QuotaPoolUsage[NonPagedPool]      2736
    Working Set Sizes (now,min,max)  (922, 50, 345) (3688KB, 200KB, 1380KB)
    PeakWorkingSetSize                1131
    VirtualSize                       42 Mb
    PeakVirtualSize                   45 Mb
    PageFaultCount                    1244
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      335
    Job                               83658020

    Setting context for this process...
.process /p /r ffffffff8364a488

    !peb
PEB at 7ffd8000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00400000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00291770 . 002a9d78
    Ldr.InLoadOrderModuleList:           002916f0 . 002a9d68
    Ldr.InMemoryOrderModuleList:         002916f8 . 002a9d70
            Base TimeStamp                     Module
          400000 468136d9 Jun 26 16:55:05 2007 C:\Windows\System32\igfxtray.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        10000000 46813690 Jun 26 16:53:52 2007 C:\Windows\System32\hccutils.DLL
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        76560000 4681c95d Jun 27 03:20:13 2007 C:\Windows\system32\SHELL32.dll
        763b0000 4549bdb9 Nov 02 09:43:21 2006 C:\Windows\system32\SHLWAPI.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        74aa0000 4549bd09 Nov 02 09:40:25 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_5d07289e07e1d100\comctl32.dll
        746d0000 4549bde7 Nov 02 09:44:07 2006 C:\Windows\System32\uxtheme.dll
        773a0000 4549bce9 Nov 02 09:39:53 2006 C:\Windows\system32\CLBCatQ.DLL
        75350000 4549bdae Nov 02 09:43:10 2006 C:\Windows\System32\rsaenh.dll
          3a0000 468136a8 Jun 26 16:54:16 2007 C:\Windows\system32\igfxsrvc.dll
          3c0000 4681367f Jun 26 16:53:35 2007 C:\Intel\ExtremeGraphics\CUI\Resource\igfxres.dll
         1380000 4681367f Jun 26 16:53:35 2007 C:\Windows\System32\igfxress.dll
    SubSystemData:     00000000
    ProcessHeap:       00290000
    ProcessParameters: 00291010
    WindowTitle:  'C:\Windows\System32\igfxtray.exe'
```

```
    ImageFile:    'C:\Windows\System32\igfxtray.exe'
    CommandLine:  '"C:\Windows\System32\igfxtray.exe" '
    DllPath:
'C:\Windows\System32;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Wind
ows;C:\Windows\System32\Wbem;C:\Program Files\QuickTime\QTSystem\'
    Environment:  002907e8
        =::=::\
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\UserName\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        HOMEDRIVE=C:
        HOMEPATH=\Users\UserName
        LOCALAPPDATA=C:\Users\UserName\AppData\Local
        LOGONSERVER=\\HOME
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        SESSIONNAME=Console
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Users\UserName\AppData\Local\Temp
        TMP=C:\Users\UserName\AppData\Local\Temp
        USERDOMAIN=home
        USERNAME=UserName
        USERPROFILE=C:\Users\UserName
        windir=C:\Windows


        THREAD 8367d030  Cid 0c6c.0c70  Teb: 7ffdf000 Win32Thread: ff7b09a0 WAIT: (WrUserRequest)
UserMode Non-Alertable
            835f0c40  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8364a488       Image:         igfxtray.exe
        Wait Start TickCount      32687          Ticks: 10812 (0:00:02:48.668)
        Context Switch Count      284
        UserTime                  00:00:00.046
        KernelTime                00:00:00.046
        Win32 Start Address igfxtray (0x0040b40a)
        Stack Init a68a7000 Current a68a6b68 Base a68a7000 Limit a68a4000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a68a6b80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a68a6bbc 81c293a7 nt!KiSwapThread+0x389
        a68a6c18 8cedb8ed nt!KeWaitForSingleObject+0x414
        a68a6c74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        a68a6c90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        a68a6ce8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        a68a6d4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        a68a6d4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a68a6d64)
        0012fd44 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0012fd48 761d3ad1 USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        0012fd6c 00405978 USER32!GetMessageA+0x8a (FPO: [Non-Fpo])
        0012ff08 0040b3a1 igfxtray+0x5978
        00000000 00000000 igfxtray+0xb3a1
```

```
        THREAD 83a23ac0  Cid 0c6c.0284  Teb: 7ffde000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            8370ce48  QueueObject
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8364a488       Image:         igfxtray.exe
        Wait Start TickCount      34610          Ticks: 8889 (0:00:02:18.669)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init a8f24000 Current a8f23bc8 Base a8f24000 Limit a8f21000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a8f23be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8f23c1c 81cad431 nt!KiSwapThread+0x389
        a8f23c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a8f23cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a8f23d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a8f23d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8f23d64)
        011efe88 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        011efe8c 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        011efeb8 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        011efef4 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        011eff60 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        011eff6c 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        011eff94 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        011effa0 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        011effac 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        011effec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Hkcmd process

```
PROCESS 8369d8b8  SessionId: 1  Cid: 0c78    Peb: 7ffde000  ParentCid: 0b90
    DirBase: 29a014e0  ObjectTable: a8bfc400  HandleCount:  76.
    Image: hkcmd.exe
    VadRoot 83576df8 Vads 60 Clone 0 Private 301. Modified 168. Locked 0.
    DeviceMap a7766db8
    Token                             a9a0c030
    ElapsedTime                       00:08:52.997
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.015
    QuotaPoolUsage[PagedPool]         79144
    QuotaPoolUsage[NonPagedPool]      2880
    Working Set Sizes (now,min,max)  (948, 50, 345) (3792KB, 200KB, 1380KB)
    PeakWorkingSetSize                1156
    VirtualSize                       42 Mb
    PeakVirtualSize                   43 Mb
    PageFaultCount                    1250
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      392
    Job                               83658020

    Setting context for this process...
.process /p /r ffffffff8369d8b8

    !peb
PEB at 7ffde000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00400000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00261758 . 00279cf0
    Ldr.InLoadOrderModuleList:           002616d8 . 00279ce0
    Ldr.InMemoryOrderModuleList:         002616e0 . 00279ce8
            Base TimeStamp                     Module
          400000 468136c2 Jun 26 16:54:42 2007 C:\Windows\System32\hkcmd.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        10000000 46813690 Jun 26 16:53:52 2007 C:\Windows\System32\hccutils.DLL
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        76560000 4681c95d Jun 27 03:20:13 2007 C:\Windows\system32\SHELL32.dll
        763b0000 4549bdb9 Nov 02 09:43:21 2006 C:\Windows\system32\SHLWAPI.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        74aa0000 4549bd09 Nov 02 09:40:25 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_5d07289e07e1d100\comctl32.dll
        746d0000 4549bde7 Nov 02 09:44:07 2006 C:\Windows\System32\uxtheme.dll
        773a0000 4549bce9 Nov 02 09:39:53 2006 C:\Windows\system32\CLBCatQ.DLL
        75350000 4549bdae Nov 02 09:43:10 2006 C:\Windows\System32\rsaenh.dll
          390000 468136a8 Jun 26 16:54:16 2007 C:\Windows\system32\igfxsrvc.dll
          3c0000 4681367f Jun 26 16:53:35 2007 C:\Intel\ExtremeGraphics\CUI\Resource\igfxres.dll
    SubSystemData:     00000000
    ProcessHeap:       00260000
    ProcessParameters: 00261010
    WindowTitle:  'C:\Windows\System32\hkcmd.exe'
    ImageFile:    'C:\Windows\System32\hkcmd.exe'
```

```
    CommandLine:  '"C:\Windows\System32\hkcmd.exe" '
    DllPath:
'C:\Windows\System32;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Wind
ows;C:\Windows\System32\Wbem;C:\Program Files\QuickTime\QTSystem\'
    Environment:  002607e8
        =::=::\
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\UserName\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        HOMEDRIVE=C:
        HOMEPATH=\Users\UserName
        LOCALAPPDATA=C:\Users\UserName\AppData\Local
        LOGONSERVER=\\HOME
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        SESSIONNAME=Console
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Users\UserName\AppData\Local\Temp
        TMP=C:\Users\UserName\AppData\Local\Temp
        USERDOMAIN=home
        USERNAME=UserName
        USERPROFILE=C:\Users\UserName
        windir=C:\Windows


        THREAD 8369d610  Cid 0c78.0c7c  Teb: 7ffdf000 Win32Thread: ffa96390 WAIT: (WrUserRequest)
UserMode Non-Alertable
            835cbdb0  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8369d8b8       Image:         hkcmd.exe
        Wait Start TickCount      43483          Ticks: 16 (0:00:00:00.249)
        Context Switch Count      3101
        UserTime                  00:00:00.062
        KernelTime                00:00:00.031
        Win32 Start Address hkcmd (0x0040c78d)
        Stack Init a6887000 Current a6886b68 Base a6887000 Limit a6884000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a6886b80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a6886bbc 81c293a7 nt!KiSwapThread+0x389
        a6886c18 8cedb8ed nt!KeWaitForSingleObject+0x414
        a6886c74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        a6886c90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        a6886ce8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        a6886d4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        a6886d4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a6886d64)
        0012fe48 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0012fe4c 761d3ad1 USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        0012fe70 00406706 USER32!GetMessageA+0x8a (FPO: [Non-Fpo])
        0012ff08 0040c724 hkcmd+0x6706
        0012ffa0 75f33833 hkcmd+0xc724
        0012ffac 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0012ffec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 83483d78  Cid 0c78.0e0c  Teb: 7ffdc000 Win32Thread: 00000000 WAIT: (DelayExecution)
UserMode Non-Alertable
            83483e00  NotificationTimer
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8369d8b8       Image:         hkcmd.exe
        Wait Start TickCount      40378          Ticks: 3121 (0:00:00:48.687)
        Context Switch Count      18
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ole32!CRpcThreadCache::RpcWorkerThreadEntry (0x7644fc53)
        Stack Init a1a37000 Current a1a36c58 Base a1a37000 Limit a1a34000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a1a36c70 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1a36cac 81cac48e nt!KiSwapThread+0x389
        a1a36d08 81e90bf1 nt!KeDelayExecutionThread+0x397
        a1a36d54 81c8caaa nt!NtDelayExecution+0x8d
        a1a36d54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1a36d64)
        0154fef0 7748f7c0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0154fef4 75f378e0 ntdll!NtDelayExecution+0xc (FPO: [2,0,0])
        0154ff5c 75ef1da0 kernel32!SleepEx+0x62 (FPO: [Non-Fpo])
        0154ff6c 764640f4 kernel32!Sleep+0xf (FPO: [Non-Fpo])
        0154ff78 7644fc0d ole32!CROIDTable::WorkerThreadLoop+0x14 (FPO: [Non-Fpo])
        0154ff94 7644fc73 ole32!CRpcThread::WorkerLoop+0x26 (FPO: [Non-Fpo])
        0154ffa0 75f33833 ole32!CRpcThreadCache::RpcWorkerThreadEntry+0x20 (FPO: [Non-Fpo])
        0154ffac 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0154ffec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 83c8a3b0  Cid 0c78.0810  Teb: 7ffdd000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            83670eb8  QueueObject
            83c8a438  NotificationTimer
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8369d8b8       Image:         hkcmd.exe
        Wait Start TickCount      43483          Ticks: 16 (0:00:00:00.249)
        Context Switch Count      511
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init a0883000 Current a0882bc8 Base a0883000 Limit a0880000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a0882be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0882c1c 81cad431 nt!KiSwapThread+0x389
        a0882c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a0882cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a0882d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a0882d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0882d64)
        0144fe88 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0144fe8c 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        0144feb8 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        0144fef4 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        0144ff60 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        0144ff6c 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        0144ff94 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        0144ffa0 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        0144ffac 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0144ffec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Igfxpers process

```
PROCESS 83688020  SessionId: 1  Cid: 0c84    Peb: 7ffda000  ParentCid: 0b90
    DirBase: 29a01500  ObjectTable: a8bf7288  HandleCount:  64.
    Image: igfxpers.exe
    VadRoot 8364a268 Vads 46 Clone 0 Private 203. Modified 127. Locked 0.
    DeviceMap a7766db8
    Token                             a9a18030
    ElapsedTime                       00:08:52.887
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         53328
    QuotaPoolUsage[NonPagedPool]      2208
    Working Set Sizes (now,min,max)  (844, 50, 345) (3376KB, 200KB, 1380KB)
    PeakWorkingSetSize                973
    VirtualSize                       26 Mb
    PeakVirtualSize                   28 Mb
    PageFaultCount                    1082
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      260
    Job                               83658020

    Setting context for this process...
.process /p /r ffffffff83688020

    !peb
PEB at 7ffda000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00400000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00241770 . 00259fa8
    Ldr.InLoadOrderModuleList:           002416f0 . 00259f98
    Ldr.InMemoryOrderModuleList:         002416f8 . 00259fa0
            Base TimeStamp                     Module
          400000 468136ae Jun 26 16:54:22 2007 C:\Windows\System32\igfxpers.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        746d0000 4549bde7 Nov 02 09:44:07 2006 C:\Windows\System32\uxtheme.dll
        773a0000 4549bce9 Nov 02 09:39:53 2006 C:\Windows\system32\CLBCatQ.DLL
        75350000 4549bdae Nov 02 09:43:10 2006 C:\Windows\System32\rsaenh.dll
        10000000 468136a8 Jun 26 16:54:16 2007 C:\Windows\system32\igfxsrvc.dll
        74fe0000 46d779a1 Aug 31 03:14:57 2007 C:\Windows\System32\wtsapi32.dll
        75300000 4549be2e Nov 02 09:45:18 2006 C:\Windows\System32\WINSTA.dll
    SubSystemData:     00000000
    ProcessHeap:       00240000
    ProcessParameters: 00241010
    WindowTitle:  'C:\Windows\System32\igfxpers.exe'
    ImageFile:    'C:\Windows\System32\igfxpers.exe'
    CommandLine:  '"C:\Windows\System32\igfxpers.exe" '
    DllPath:
'C:\Windows\System32;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Wind
ows;C:\Windows\System32\Wbem;C:\Program Files\QuickTime\QTSystem\'
    Environment:  002407e8
        =::=::\
```

```
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\UserName\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        HOMEDRIVE=C:
        HOMEPATH=\Users\UserName
        LOCALAPPDATA=C:\Users\UserName\AppData\Local
        LOGONSERVER=\\HOME
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        SESSIONNAME=Console
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Users\UserName\AppData\Local\Temp
        TMP=C:\Users\UserName\AppData\Local\Temp
        USERDOMAIN=home
        USERNAME=UserName
        USERPROFILE=C:\Users\UserName
        windir=C:\Windows


        THREAD 8367f870  Cid 0c84.0c88  Teb: 7ffdf000 Win32Thread: fe69c0d0 WAIT: (WrUserRequest)
UserMode Non-Alertable
            8364dcc8  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            83688020       Image:         igfxpers.exe
        Wait Start TickCount      32687          Ticks: 10812 (0:00:02:48.668)
        Context Switch Count      330
        UserTime                  00:00:00.031
        KernelTime                00:00:00.046
        Win32 Start Address igfxpers (0x0040c4ad)
        Stack Init a68d7000 Current a68d6b68 Base a68d7000 Limit a68d4000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a68d6b80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a68d6bbc 81c293a7 nt!KiSwapThread+0x389
        a68d6c18 8cedb8ed nt!KeWaitForSingleObject+0x414
        a68d6c74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        a68d6c90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        a68d6ce8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        a68d6d4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        a68d6d4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a68d6d64)
        0012fe44 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0012fe48 761d3ad1 USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        0012fe6c 00408a8c USER32!GetMessageA+0x8a (FPO: [Non-Fpo])
        0012ff08 0040c444 igfxpers+0x8a8c
        0012ffa0 75f33833 igfxpers+0xc444
        0012ffac 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0012ffec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 838fed78  Cid 0c84.0d80  Teb: 7ffde000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            8368c310  QueueObject
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            83688020       Image:         igfxpers.exe
        Wait Start TickCount      34610          Ticks: 8889 (0:00:02:18.669)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init 9f734000 Current 9f733bc8 Base 9f734000 Limit 9f731000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f733be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f733c1c 81cad431 nt!KiSwapThread+0x389
        9f733c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        9f733cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        9f733d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        9f733d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f733d64)
        011cfe88 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        011cfe8c 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        011cfeb8 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        011cfef4 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        011cff60 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        011cff6c 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        011cff94 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        011cffa0 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        011cffac 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        011cffec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Stray process

```
PROCESS 83665b10  SessionId: 1  Cid: 0c8c    Peb: 7ffd6000  ParentCid: 0b90
    DirBase: 29a01520  ObjectTable: a8acc008  HandleCount: 105.
    Image: sttray.exe
    VadRoot 83627fd0 Vads 79 Clone 0 Private 900. Modified 628. Locked 0.
    DeviceMap a7766db8
    Token                             a9a13ca0
    ElapsedTime                       00:08:52.856
    UserTime                          00:00:00.015
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         95616
    QuotaPoolUsage[NonPagedPool]      3840
    Working Set Sizes (now,min,max)  (1192, 50, 345) (4768KB, 200KB, 1380KB)
    PeakWorkingSetSize                2340
    VirtualSize                       53 Mb
    PeakVirtualSize                   60 Mb
    PageFaultCount                    2847
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      1068
    Job                               83658020

    Setting context for this process...
.process /p /r ffffffff83665b10

    !peb
PEB at 7ffd6000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00400000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00271718 . 00288938
    Ldr.InLoadOrderModuleList:           00271698 . 00288a78
    Ldr.InMemoryOrderModuleList:         002716a0 . 00288a80
            Base TimeStamp                     Module
          400000 4592b31a Dec 27 17:53:30 2006 C:\Windows\sttray.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        10000000 4592b1bb Dec 27 17:47:39 2006 C:\Windows\system32\STLang.dll
        6e4f0000 4549bd08 Nov 02 09:40:24 2006 C:\Windows\system32\MFC42u.DLL
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        76020000 470c4e1e Oct 10 04:59:26 2007 C:\Windows\system32\WININET.dll
        763b0000 4549bdb9 Nov 02 09:43:21 2006 C:\Windows\system32\SHLWAPI.dll
        76010000 4549ad42 Nov 02 08:33:06 2006 C:\Windows\system32\Normaliz.dll
        76360000 4549bcfb Nov 02 09:40:11 2006 C:\Windows\system32\iertutil.dll
        75fe0000 4549be0e Nov 02 09:44:46 2006 C:\Windows\system32\WS2_32.dll
        77550000 4549bdc7 Nov 02 09:43:35 2006 C:\Windows\system32\NSI.dll
        6e940000 4549bd7d Nov 02 09:42:21 2006 C:\Windows\system32\ODBC32.dll
        73c50000 4549bcb0 Nov 02 09:38:56 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.6000.16386_none_87e0cb09378714f1\COMCTL32.dll
        76560000 4681c95d Jun 27 03:20:13 2007 C:\Windows\system32\SHELL32.dll
        76140000 4549bd09 Nov 02 09:40:25 2006 C:\Windows\system32\COMDLG32.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        74aa0000 4549bd09 Nov 02 09:40:25 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_5d07289e07e1d100\comctl32.dll
```

```
        6fa20000 4549bd84 Nov 02 09:42:28 2006 C:\Windows\system32\odbcint.dll
        746d0000 4549bde7 Nov 02 09:44:07 2006 C:\Windows\system32\uxtheme.dll
        773a0000 4549bce9 Nov 02 09:39:53 2006 C:\Windows\system32\CLBCatQ.DLL
        75350000 4549bdae Nov 02 09:43:10 2006 C:\Windows\system32\rsaenh.dll
        72860000 4592b297 Dec 27 17:51:19 2006 C:\Windows\system32\stapi32.dll
        738c0000 4549be1d Nov 02 09:45:01 2006 C:\Windows\system32\WINMM.dll
        73880000 4549bd93 Nov 02 09:42:43 2006 C:\Windows\system32\OLEACC.dll
        77030000 4549bdb0 Nov 02 09:43:12 2006 C:\Windows\system32\SETUPAPI.dll
    SubSystemData:     00000000
    ProcessHeap:       00270000
    ProcessParameters: 00271010
    WindowTitle:  'C:\Windows\sttray.exe'
    ImageFile:    'C:\Windows\sttray.exe'
    CommandLine:  '"C:\Windows\sttray.exe" '
    DllPath:
'C:\Windows;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Windows;C:\Wi
ndows\System32\Wbem;C:\Program Files\QuickTime\QTSystem\'
    Environment:  002707e8
        =::=::\
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\UserName\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        HOMEDRIVE=C:
        HOMEPATH=\Users\UserName
        LOCALAPPDATA=C:\Users\UserName\AppData\Local
        LOGONSERVER=\\HOME
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        SESSIONNAME=Console
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Users\UserName\AppData\Local\Temp
        TMP=C:\Users\UserName\AppData\Local\Temp
        USERDOMAIN=home
        USERNAME=UserName
        USERPROFILE=C:\Users\UserName
        windir=C:\Windows
```

```
        THREAD 8366d6a0  Cid 0c8c.0c90  Teb: 7ffdf000 Win32Thread: ff2a83d8 WAIT: (WrUserRequest)
UserMode Non-Alertable
            835f2348  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            83665b10       Image:         sttray.exe
        Wait Start TickCount      33196          Ticks: 10303 (0:00:02:40.727)
        Context Switch Count      1196
        UserTime                  00:00:00.062
        KernelTime                00:00:00.062
        Win32 Start Address sttray (0x00409f5a)
        Stack Init a683b000 Current a683ab68 Base a683b000 Limit a6838000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a683ab80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a683abbc 81c293a7 nt!KiSwapThread+0x389
        a683ac18 8cedb8ed nt!KeWaitForSingleObject+0x414
        a683ac74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        a683ac90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        a683ace8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        a683ad4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        a683ad4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a683ad64)
        0012fe88 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0012fe8c 761e19cd USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        0012fea8 6e50db70 USER32!GetMessageW+0x33 (FPO: [Non-Fpo])
        0012fec4 6e50e8fe MFC42u!CWinThread::PumpMessage+0x16 (FPO: [Non-Fpo])
        0012fedc 6e50f63b MFC42u!CWinThread::Run+0x50 (FPO: [Non-Fpo])
        0012fef0 0040a329 MFC42u!AfxWinMain+0x84 (FPO: [Non-Fpo])
        0012ffa0 75f33833 sttray+0xa329
        0012ffac 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0012ffec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 8374fb10  Cid 0c8c.0820  Teb: 7ffde000 Win32Thread: fe694550 WAIT: (WrQueue)
UserMode Non-Alertable
            9fd166d0  QueueObject
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            83665b10       Image:         sttray.exe
        Wait Start TickCount      35119          Ticks: 8380 (0:00:02:10.728)
        Context Switch Count      10
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init a8f98000 Current a8f97bc8 Base a8f98000 Limit a8f95000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a8f97be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8f97c1c 81cad431 nt!KiSwapThread+0x389
        a8f97c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a8f97cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a8f97d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a8f97d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8f97d64)
        01d9fe88 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01d9fe8c 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        01d9feb8 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        01d9fef4 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        01d9ff60 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        01d9ff6c 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        01d9ff94 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        01d9ffa0 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        01d9ffac 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01d9ffec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 8372aa50  Cid 0c8c.02d0  Teb: 7ffdc000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            83725728  SynchronizationEvent
            8372aad8  NotificationTimer
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            83665b10       Image:         sttray.exe
        Wait Start TickCount      29285          Ticks: 14214 (0:00:03:41.739)
        Context Switch Count      7
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ole32!CRpcThreadCache::RpcWorkerThreadEntry (0x7644fc53)
        Stack Init 9f704000 Current 9f703c38 Base 9f704000 Limit 9f701000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f703c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f703c8c 81c293a7 nt!KiSwapThread+0x389
        9f703ce8 81df5057 nt!KeWaitForSingleObject+0x414
        9f703d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        9f703d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f703d64)
        01f9feac 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01f9feb0 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        01f9ff20 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        01f9ff34 76455251 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        01f9ff50 76422104 ole32!CDllHost::MTAWorkerLoop+0x2b (FPO: [Non-Fpo])
        01f9ff70 764524ce ole32!CDllHost::WorkerThread+0xc7 (FPO: [Non-Fpo])
        01f9ff78 7644fc0d ole32!DLLHostThreadEntry+0xd (FPO: [Non-Fpo])
        01f9ff94 7644fc73 ole32!CRpcThread::WorkerLoop+0x26 (FPO: [Non-Fpo])
        01f9ffa0 75f33833 ole32!CRpcThreadCache::RpcWorkerThreadEntry+0x20 (FPO: [Non-Fpo])
        01f9ffac 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01f9ffec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 836a0d78  Cid 0c8c.03a0  Teb: 7ffda000 Win32Thread: 00000000 WAIT: (Executive)
UserMode Non-Alertable
            836b0084  NotificationEvent
        IRP List:
            82efff68: (0006,0094) Flags: 00020800  Mdl: 00000000
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            83665b10       Image:         sttray.exe
        Wait Start TickCount      10068          Ticks: 33431 (0:00:08:41.526)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address stapi32!DllUnregisterServer (0x72874f88)
        Stack Init 9f2a0000 Current 9f29fb80 Base 9f2a0000 Limit 9f29d000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f29fb98 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f29fbd4 81c293a7 nt!KiSwapThread+0x389
        9f29fc30 81d88faf nt!KeWaitForSingleObject+0x414
        9f29fc64 81d89efb nt!IopSynchronousServiceTail+0x258
        9f29fd00 81d8ee8f nt!IopXxxControlFile+0x6b7
        9f29fd34 81c8caaa nt!NtFsControlFile+0x2a
        9f29fd34 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f29fd64)
        0219f908 7748f9c0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0219f90c 75eff00d ntdll!NtFsControlFile+0xc (FPO: [10,0,0])
        0219f950 72875045 kernel32!ConnectNamedPipe+0x52 (FPO: [Non-Fpo])
        0219ffa0 75f33833 stapi32!DllUnregisterServer+0x3755
        0219ffac 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0219ffec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

IRW process

```
PROCESS 83644b48  SessionId: 1  Cid: 0c94    Peb: 7ffd5000  ParentCid: 0b90
    DirBase: 29a01540  ObjectTable: a8bc1358  HandleCount:  48.
    Image: IRW.exe
    VadRoot 835950a8 Vads 48 Clone 0 Private 174. Modified 118. Locked 0.
    DeviceMap a7766db8
    Token                             a9a11910
    ElapsedTime                       00:08:52.841
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         79304
    QuotaPoolUsage[NonPagedPool]      2304
    Working Set Sizes (now,min,max)  (687, 50, 345) (2748KB, 200KB, 1380KB)
    PeakWorkingSetSize                829
    VirtualSize                       40 Mb
    PeakVirtualSize                   41 Mb
    PageFaultCount                    840
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      269
    Job                               83658020

    Setting context for this process...
.process /p /r ffffffff83644b48

    !peb
PEB at 7ffd5000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00400000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00221750 . 00239598
    Ldr.InLoadOrderModuleList:           002216d0 . 00239588
    Ldr.InMemoryOrderModuleList:         002216d8 . 00239590
            Base TimeStamp                     Module
          400000 469c0caf Jul 17 01:26:23 2007 C:\Windows\System32\IRW.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        73d70000 4549bcaf Nov 02 09:38:55 2006
C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.0.6000.16386_none_9ea0ac9ec96e71
27\gdiplus.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        76560000 4681c95d Jun 27 03:20:13 2007 C:\Windows\system32\SHELL32.dll
        763b0000 4549bdb9 Nov 02 09:43:21 2006 C:\Windows\system32\SHLWAPI.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        74aa0000 4549bd09 Nov 02 09:40:25 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_5d07289e07e1d100\comctl32.dll
        746d0000 4549bde7 Nov 02 09:44:07 2006 C:\Windows\System32\uxtheme.dll
    SubSystemData:     00000000
    ProcessHeap:       00220000
    ProcessParameters: 00221010
    WindowTitle:  'C:\Windows\System32\IRW.exe'
    ImageFile:    'C:\Windows\System32\IRW.exe'
    CommandLine:  '"C:\Windows\System32\IRW.exe" '
```

```
    DllPath:
'C:\Windows\System32;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Wind
ows;C:\Windows\System32\Wbem;C:\Program Files\QuickTime\QTSystem\'
    Environment:  002207e8
        =::=::\
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\UserName\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        HOMEDRIVE=C:
        HOMEPATH=\Users\UserName
        LOCALAPPDATA=C:\Users\UserName\AppData\Local
        LOGONSERVER=\\HOME
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        SESSIONNAME=Console
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Users\UserName\AppData\Local\Temp
        TMP=C:\Users\UserName\AppData\Local\Temp
        USERDOMAIN=home
        USERNAME=UserName
        USERPROFILE=C:\Users\UserName
        windir=C:\Windows


        THREAD 8366d2c8  Cid 0c94.0c98  Teb: 7ffdf000 Win32Thread: ff34fa68 WAIT: (WrUserRequest)
UserMode Non-Alertable
            9fd4d120  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            83644b48       Image:         IRW.exe
        Wait Start TickCount      11132          Ticks: 32367 (0:00:08:24.928)
        Context Switch Count      95
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address IRW (0x0040253d)
        Stack Init a68a3000 Current a68a2b68 Base a68a3000 Limit a68a0000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a68a2b80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a68a2bbc 81c293a7 nt!KiSwapThread+0x389
        a68a2c18 8cedb8ed nt!KeWaitForSingleObject+0x414
        a68a2c74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        a68a2c90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        a68a2ce8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        a68a2d4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        a68a2d4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a68a2d64)
        0012fe80 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0012fe84 761e19cd USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        0012fea0 004012a4 USER32!GetMessageW+0x33 (FPO: [Non-Fpo])
        0012ff08 004024d4 IRW+0x12a4
        0012ffa0 75f33833 IRW+0x24d4
        0012ffac 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0012ffec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 83486810  Cid 0c94.0df4  Teb: 7ffde000 Win32Thread: fe7399d0 WAIT: (UserRequest)
UserMode Non-Alertable
            83666730  NotificationEvent
            8346b2d0  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            83644b48       Image:         IRW.exe
        Wait Start TickCount      11132          Ticks: 32367 (0:00:08:24.928)
        Context Switch Count      26
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address gdiplus!BackgroundThreadProc (0x73d81909)
        Stack Init 9f3c8000 Current 9f3c78d0 Base 9f3c8000 Limit 9f3c5000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f3c78e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f3c7924 81c28c64 nt!KiSwapThread+0x389
        9f3c7970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f3c7bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f3c7d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f3c7d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f3c7d64)
        011dfe44 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        011dfe48 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        011dfee4 761dc4b7 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        011dff38 761d8b83 USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
        011dff54 73d81965 USER32!MsgWaitForMultipleObjects+0x1f (FPO: [Non-Fpo])
        011dffa0 75f33833 gdiplus!BackgroundThreadProc+0x59 (FPO: [Non-Fpo])
        011dffac 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        011dffec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 8371b648  Cid 0c94.0df8  Teb: 7ffdd000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            8371be08  SynchronizationEvent
            9fd12a98  SynchronizationEvent
            9fd12a68  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            83644b48       Image:         IRW.exe
        Wait Start TickCount      9573           Ticks: 33926 (0:00:08:49.248)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address IRW (0x00401780)
        Stack Init 9f3d4000 Current 9f3d38d0 Base 9f3d4000 Limit 9f3d1000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f3d38e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f3d3924 81c28c64 nt!KiSwapThread+0x389
        9f3d3970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f3d3bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f3d3d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f3d3d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f3d3d64)
        013dfca4 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        013dfca8 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        013dfd44 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        013dfd60 0040181d kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        013dffa0 75f33833 IRW+0x181d
        013dffac 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        013dffec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

KbdMgr process

```
PROCESS 83683d90  SessionId: 1  Cid: 0c9c    Peb: 7ffd5000  ParentCid: 0b90
    DirBase: 29a01560  ObjectTable: a8bfa440  HandleCount: 135.
    Image: KbdMgr.exe
    VadRoot 83486560 Vads 102 Clone 0 Private 444. Modified 365. Locked 0.
    DeviceMap a7766db8
    Token                             a9a2b030
    ElapsedTime                       00:08:52.825
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         96472
    QuotaPoolUsage[NonPagedPool]      4968
    Working Set Sizes (now,min,max)  (1195, 50, 345) (4780KB, 200KB, 1380KB)
    PeakWorkingSetSize                1612
    VirtualSize                       60 Mb
    PeakVirtualSize                   61 Mb
    PageFaultCount                    1640
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      1926
    Job                               83658020

    Setting context for this process...
.process /p /r ffffffff83683d90

    !peb
PEB at 7ffd5000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00400000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00631798 . 00649330
    Ldr.InLoadOrderModuleList:           00631718 . 00649320
    Ldr.InMemoryOrderModuleList:         00631720 . 00649328
            Base TimeStamp                     Module
          400000 46d36bee Aug 28 01:27:26 2007 C:\Program Files\Boot Camp\KbdMgr.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        738c0000 4549be1d Nov 02 09:45:01 2006 C:\Windows\system32\WINMM.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        73880000 4549bd93 Nov 02 09:42:43 2006 C:\Windows\system32\OLEACC.dll
        73d70000 4549bcaf Nov 02 09:38:55 2006
C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.0.6000.16386_none_9ea0ac9ec96e71
27\gdiplus.dll
        76140000 4549bd09 Nov 02 09:40:25 2006 C:\Windows\system32\COMDLG32.dll
        763b0000 4549bdb9 Nov 02 09:43:21 2006 C:\Windows\system32\SHLWAPI.dll
        73c50000 4549bcb0 Nov 02 09:38:56 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.6000.16386_none_87e0cb09378714f1\COMCTL32.dll
        76560000 4681c95d Jun 27 03:20:13 2007 C:\Windows\system32\SHELL32.dll
        715a0000 4549be2a Nov 02 09:45:14 2006 C:\Windows\system32\WINSPOOL.DRV
        707c0000 4549bd99 Nov 02 09:42:49 2006 C:\Windows\system32\oledlg.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        74aa0000 4549bd09 Nov 02 09:40:25 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_5d07289e07e1d100\comctl32.dll
        746d0000 4549bde7 Nov 02 09:44:07 2006 C:\Windows\system32\uxtheme.dll
```

```
        10000000 46d36be5 Aug 28 01:27:17 2007 C:\Program Files\Boot Camp\Boot
Camp.Resources\en.lproj\Resources.dll
        737f0000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\wdmaud.drv
        73870000 4549bd89 Nov 02 09:42:33 2006 C:\Windows\system32\ksuser.dll
        75390000 4549bcdc Nov 02 09:39:40 2006 C:\Windows\system32\AVRT.dll
        74d90000 4549bd03 Nov 02 09:40:19 2006 C:\Windows\system32\MMDevAPI.DLL
        773a0000 4549bce9 Nov 02 09:39:53 2006 C:\Windows\system32\CLBCatQ.DLL
        77030000 4549bdb0 Nov 02 09:43:12 2006 C:\Windows\system32\SETUPAPI.dll
        74ff0000 4549be2f Nov 02 09:45:19 2006 C:\Windows\system32\WINTRUST.dll
        75650000 45b96fde Jan 26 03:05:02 2007 C:\Windows\system32\CRYPT32.dll
        75820000 4549bd41 Nov 02 09:41:21 2006 C:\Windows\system32\MSASN1.dll
        75ba0000 4549bde2 Nov 02 09:44:02 2006 C:\Windows\system32\USERENV.dll
        75b80000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\Secur32.dll
        77580000 462434a3 Apr 17 03:44:51 2007 C:\Windows\system32\imagehlp.dll
        736d0000 4549bcc2 Nov 02 09:39:14 2006 C:\Windows\System32\audioses.dll
        73540000 4549bcc0 Nov 02 09:39:12 2006 C:\Windows\System32\audioeng.dll
        75ce0000 4549bd99 Nov 02 09:42:49 2006 C:\Windows\system32\PSAPI.DLL
        73860000 4549bd2f Nov 02 09:41:03 2006 C:\Windows\system32\msacm32.drv
        73790000 4549bd2e Nov 02 09:41:02 2006 C:\Windows\system32\MSACM32.dll
        736c0000 4549bd27 Nov 02 09:40:55 2006 C:\Windows\system32\miUserNamep.dll
    SubSystemData:     00000000
    ProcessHeap:       00630000
    ProcessParameters: 00631010
    WindowTitle:  'C:\Program Files\Boot Camp\KbdMgr.exe'
    ImageFile:    'C:\Program Files\Boot Camp\KbdMgr.exe'
    CommandLine:  '"C:\Program Files\Boot Camp\KbdMgr.exe" '
    DllPath:      'C:\Program Files\Boot
Camp;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Windows;C:\Windows\S
ystem32\Wbem;C:\Program Files\QuickTime\QTSystem\'
    Environment:  006307e8
        =::=::\
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\UserName\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        HOMEDRIVE=C:
        HOMEPATH=\Users\UserName
        LOCALAPPDATA=C:\Users\UserName\AppData\Local
        LOGONSERVER=\\HOME
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        SESSIONNAME=Console
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Users\UserName\AppData\Local\Temp
        TMP=C:\Users\UserName\AppData\Local\Temp
        USERDOMAIN=home
        USERNAME=UserName
        USERPROFILE=C:\Users\UserName
        windir=C:\Windows
```

```
        THREAD 83691838  Cid 0c9c.0ca0  Teb: 7ffdf000 Win32Thread: ff2533f0 WAIT: (WrUserRequest)
UserMode Non-Alertable
            83666620  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            83683d90       Image:         KbdMgr.exe
        Wait Start TickCount      11132          Ticks: 32367 (0:00:08:24.928)
        Context Switch Count      566
        UserTime                  00:00:00.031
        KernelTime                00:00:00.015
        Win32 Start Address KbdMgr (0x0042dfd4)
        Stack Init a689f000 Current a689eb68 Base a689f000 Limit a689c000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a689eb80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a689ebbc 81c293a7 nt!KiSwapThread+0x389
        a689ec18 8cedb8ed nt!KeWaitForSingleObject+0x414
        a689ec74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        a689ec90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        a689ece8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        a689ed4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        a689ed4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a689ed64)
        0012fea0 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0012fea4 761e19cd USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        0012fec0 004142e8 USER32!GetMessageW+0x33 (FPO: [Non-Fpo])
        00000000 00000000 KbdMgr+0x142e8

        THREAD 83723710  Cid 0c9c.0ef0  Teb: 7ffde000 Win32Thread: fe68c3d8 WAIT: (UserRequest)
UserMode Non-Alertable
            835e3bd8  NotificationEvent
            83484820  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            83683d90       Image:         KbdMgr.exe
        Wait Start TickCount      11132          Ticks: 32367 (0:00:08:24.928)
        Context Switch Count      58
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address gdiplus!BackgroundThreadProc (0x73d81909)
        Stack Init a8fcc000 Current a8fcb8d0 Base a8fcc000 Limit a8fc9000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a8fcb8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8fcb924 81c28c64 nt!KiSwapThread+0x389
        a8fcb970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a8fcbbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a8fcbd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a8fcbd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8fcbd64)
        0122fe44 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0122fe48 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0122fee4 761dc4b7 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0122ff38 761d8b83 USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
        0122ff54 73d81965 USER32!MsgWaitForMultipleObjects+0x1f (FPO: [Non-Fpo])
        0122ffa0 75f33833 gdiplus!BackgroundThreadProc+0x59 (FPO: [Non-Fpo])
        0122ffac 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0122ffec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 83491af8  Cid 0c9c.0f48  Teb: 7ffdd000 Win32Thread: ff32a4d8 WAIT: (WrQueue)
UserMode Non-Alertable
            836a8220  QueueObject
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            83683d90       Image:         KbdMgr.exe
        Wait Start TickCount      9786           Ticks: 33713 (0:00:08:45.926)
        Context Switch Count      199
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address wdmaud!mxdMessageThreadProc (0x737f42d7)
        Stack Init a8f3c000 Current a8f3bbc8 Base a8f3c000 Limit a8f39000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a8f3bbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8f3bc1c 81cad431 nt!KiSwapThread+0x389
        a8f3bc6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a8f3bcc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a8f3bd48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a8f3bd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8f3bd64)
        019eff40 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        019eff44 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        019eff70 737f4354 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        019effa0 75f33833 wdmaud!mxdMessageThreadProc+0x7d (FPO: [Non-Fpo])
        019effac 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        019effec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 83725af8  Cid 0c9c.0f4c  Teb: 7ffdc000 Win32Thread: ff32a968 WAIT: (WrUserRequest)
UserMode Non-Alertable
            837d6d50  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            83683d90       Image:         KbdMgr.exe
        Wait Start TickCount      9778           Ticks: 33721 (0:00:08:46.050)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdmaud!CTaskThread::TaskThreadProc (0x737f8675)
        Stack Init 9f7c8000 Current 9f7c7b68 Base 9f7c8000 Limit 9f7c5000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f7c7b80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f7c7bbc 81c293a7 nt!KiSwapThread+0x389
        9f7c7c18 8cedb8ed nt!KeWaitForSingleObject+0x414
        9f7c7c74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        9f7c7c90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        9f7c7ce8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        9f7c7d4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        9f7c7d4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f7c7d64)
        01aeff40 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01aeff44 761e19cd USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        01aeff60 737f8712 USER32!GetMessageW+0x33 (FPO: [Non-Fpo])
        01aeffa0 75f33833 wdmaud!CTaskThread::TaskThreadProc+0x9d (FPO: [Non-Fpo])
        01aeffac 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01aeffec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 836cfd78  Cid 0c9c.0f54  Teb: 7ffdb000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            836ced90  SynchronizationEvent
            83753d98  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            83683d90       Image:         KbdMgr.exe
        Wait Start TickCount      9785           Ticks: 33714 (0:00:08:45.941)
        Context Switch Count      566
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address wdmaud!CWorker::_StaticThreadProc (0x737f8544)
        Stack Init 9f7d0000 Current 9f7cf8d0 Base 9f7d0000 Limit 9f7cd000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f7cf8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f7cf924 81c28c64 nt!KiSwapThread+0x389
        9f7cf970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f7cfbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f7cfd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f7cfd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f7cfd64)
        014afebc 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        014afec0 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        014aff5c 737f5111 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        014aff94 737f855c wdmaud!CWorker::_ThreadProc+0x5e (FPO: [Non-Fpo])
        014affa0 75f33833 wdmaud!CWorker::_StaticThreadProc+0x18 (FPO: [Non-Fpo])
        014affac 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        014affec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 837e1ad8  Cid 0c9c.0f9c  Teb: 7ffda000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            a194d5c0  SynchronizationEvent
            9fd4d848  SynchronizationEvent
            9fd4d878  SynchronizationEvent
            9fd4d8a8  SynchronizationEvent
            9fd4d8d8  SynchronizationEvent
            9fdb30a8  SynchronizationEvent
            9fdb3078  SynchronizationEvent
            a194d560  SynchronizationEvent
            a194d590  SynchronizationEvent
            a194d530  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            83683d90       Image:         KbdMgr.exe
        Wait Start TickCount      9791           Ticks: 33708 (0:00:08:45.848)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address KbdMgr (0x00404d30)
        Stack Init 9f784000 Current 9f7838d0 Base 9f784000 Limit 9f781000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f7838e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f783924 81c28c64 nt!KiSwapThread+0x389
        9f783970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f783bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f783d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f783d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f783d64)
        0185fea0 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0185fea4 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0185ff40 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0185ff5c 00404db0 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0185ffac 7746a9bd KbdMgr+0x4db0
        0185ffec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 837d9030  Cid 0c9c.0fa0  Teb: 7ffd9000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            a194d500  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            83683d90       Image:         KbdMgr.exe
        Wait Start TickCount      9787           Ticks: 33712 (0:00:08:45.910)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address KbdMgr (0x00403de0)
        Stack Init 9f790000 Current 9f78fc38 Base 9f790000 Limit 9f78d000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f78fc50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f78fc8c 81c293a7 nt!KiSwapThread+0x389
        9f78fce8 81df5057 nt!KeWaitForSingleObject+0x414
        9f78fd50 81c8caaa nt!NtWaitForSingleObject+0xbe
        9f78fd50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f78fd64)
        01ffff00 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01ffff04 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        01ffff74 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        01ffff88 00403dfe kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        01ffffac 7746a9bd KbdMgr+0x3dfe
        01ffffec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Jusched process

```
PROCESS 83679bb0  SessionId: 1  Cid: 0ca4    Peb: 7ffd3000  ParentCid: 0b90
    DirBase: 29a01580  ObjectTable: a8bcd5f8  HandleCount:  47.
    Image: jusched.exe
    VadRoot 836576a8 Vads 47 Clone 0 Private 175. Modified 112. Locked 0.
    DeviceMap a7766db8
    Token                             a8bc1c48
    ElapsedTime                       00:08:52.809
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         78824
    QuotaPoolUsage[NonPagedPool]      2328
    Working Set Sizes (now,min,max)  (723, 50, 345) (2892KB, 200KB, 1380KB)
    PeakWorkingSetSize                818
    VirtualSize                       38 Mb
    PeakVirtualSize                   40 Mb
    PageFaultCount                    956
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      262
    Job                               83658020

    Setting context for this process...
.process /p /r ffffffff83679bb0

    !peb
PEB at 7ffd3000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00400000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 001b17f8 . 001c7ee0
    Ldr.InLoadOrderModuleList:           001b1778 . 001c7ed0
    Ldr.InMemoryOrderModuleList:         001b1780 . 001c7ed8
            Base TimeStamp                     Module
          400000 46f8aa61 Sep 25 07:27:45 2007 C:\Program Files\Java\jre1.6.0_03\bin\jusched.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        76020000 470c4e1e Oct 10 04:59:26 2007 C:\Windows\system32\WININET.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        763b0000 4549bdb9 Nov 02 09:43:21 2006 C:\Windows\system32\SHLWAPI.dll
        76010000 4549ad42 Nov 02 08:33:06 2006 C:\Windows\system32\Normaliz.dll
        76360000 4549bcfb Nov 02 09:40:11 2006 C:\Windows\system32\iertutil.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        76560000 4681c95d Jun 27 03:20:13 2007 C:\Windows\system32\SHELL32.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        74aa0000 4549bd09 Nov 02 09:40:25 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_5d07289e07e1d100\comctl32.dll
        746d0000 4549bde7 Nov 02 09:44:07 2006 C:\Windows\system32\uxtheme.dll
    SubSystemData:     00000000
    ProcessHeap:       001b0000
    ProcessParameters: 001b1010
    WindowTitle:  'C:\Program Files\Java\jre1.6.0_03\bin\jusched.exe'
    ImageFile:    'C:\Program Files\Java\jre1.6.0_03\bin\jusched.exe'
    CommandLine:  '"C:\Program Files\Java\jre1.6.0_03\bin\jusched.exe" '
```

```
    DllPath:      'C:\Program
Files\Java\jre1.6.0_03\bin;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C
:\Windows;C:\Windows\System32\Wbem;C:\Program Files\QuickTime\QTSystem\'
    Environment:  001b07e8
        =::=::\
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\UserName\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        HOMEDRIVE=C:
        HOMEPATH=\Users\UserName
        LOCALAPPDATA=C:\Users\UserName\AppData\Local
        LOGONSERVER=\\HOME
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        SESSIONNAME=Console
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Users\UserName\AppData\Local\Temp
        TMP=C:\Users\UserName\AppData\Local\Temp
        USERDOMAIN=home
        USERNAME=UserName
        USERPROFILE=C:\Users\UserName
        windir=C:\Windows


        THREAD 83691580  Cid 0ca4.0ca8  Teb: 7ffdf000 Win32Thread: ff25f7c0 WAIT: (UserRequest)
UserMode Non-Alertable
            836a9138  NotificationEvent
            8394bfb0  SynchronizationEvent
            83691608  NotificationTimer
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            83679bb0       Image:         jusched.exe
        Wait Start TickCount      28805          Ticks: 14694 (0:00:03:49.227)
        Context Switch Count      37
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address jusched (0x0040b4a4)
        Stack Init a683f000 Current a683e8d0 Base a683f000 Limit a683c000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a683e8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a683e924 81c28c64 nt!KiSwapThread+0x389
        a683e970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a683ebfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a683ed48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a683ed48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a683ed64)
        0012f95c 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0012f960 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0012f9fc 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0012fa18 00401b25 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0012fe78 0040b628 jusched+0x1b25
        0012ffa0 75f33833 jusched+0xb628
        0012ffac 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0012ffec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Realsched process

```
PROCESS 836466e8  SessionId: 1  Cid: 0cd8    Peb: 7ffdd000  ParentCid: 0b90
    DirBase: 29a015e0  ObjectTable: a9a38610  HandleCount:  99.
    Image: realsched.exe
    VadRoot 8365d668 Vads 72 Clone 0 Private 250. Modified 824. Locked 0.
    DeviceMap a7766db8
    Token                             a9a45ca0
    ElapsedTime                       00:08:52.716
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         85720
    QuotaPoolUsage[NonPagedPool]      3456
    Working Set Sizes (now,min,max)  (154, 50, 345) (616KB, 200KB, 1380KB)
    PeakWorkingSetSize                1090
    VirtualSize                       47 Mb
    PeakVirtualSize                   49 Mb
    PageFaultCount                    3441
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      440
    Job                               83658020

    Setting context for this process...
.process /p /r ffffffff836466e8

    !peb
PEB at 7ffdd000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00400000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 001d08f0 . 001e9920
    Ldr.InLoadOrderModuleList:           001d0870 . 001e9910
    Ldr.InMemoryOrderModuleList:         001d0878 . 001e9918
            Base TimeStamp                     Module
          400000 47323519 Nov 07 21:58:49 2007 C:\Program Files\Common
Files\Real\Update_OB\realsched.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        753f0000 4549bde4 Nov 02 09:44:04 2006 C:\Windows\system32\VERSION.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        76560000 4681c95d Jun 27 03:20:13 2007 C:\Windows\system32\shell32.dll
        763b0000 4549bdb9 Nov 02 09:43:21 2006 C:\Windows\system32\SHLWAPI.dll
        74aa0000 4549bd09 Nov 02 09:40:25 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_5d07289e07e1d100\comctl32.dll
        746d0000 4549bde7 Nov 02 09:44:07 2006 C:\Windows\system32\uxtheme.dll
        77030000 4549bdb0 Nov 02 09:43:12 2006 C:\Windows\system32\SETUPAPI.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        75ba0000 4549bde2 Nov 02 09:44:02 2006 C:\Windows\system32\USERENV.dll
        75b80000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\Secur32.dll
        744e0000 4549bd96 Nov 02 09:42:46 2006 C:\Windows\system32\PROPSYS.dll
```

```
        773a0000 4549bce9 Nov 02 09:39:53 2006 C:\Windows\system32\CLBCatQ.DLL
        75350000 4549bdae Nov 02 09:43:10 2006 C:\Windows\system32\rsaenh.dll
        75020000 4549bddb Nov 02 09:43:55 2006 C:\Windows\system32\NTMARTA.DLL
        76310000 4549be44 Nov 02 09:45:40 2006 C:\Windows\system32\WLDAP32.dll
        75fe0000 4549be0e Nov 02 09:44:46 2006 C:\Windows\system32\WS2_32.dll
        77550000 4549bdc7 Nov 02 09:43:35 2006 C:\Windows\system32\NSI.dll
        75ce0000 4549bd99 Nov 02 09:42:49 2006 C:\Windows\system32\PSAPI.DLL
        75ad0000 4549bda8 Nov 02 09:43:04 2006 C:\Windows\system32\SAMLIB.dll
        75300000 4549be2e Nov 02 09:45:18 2006 C:\Windows\system32\WINSTA.dll
    SubSystemData:     00000000
    ProcessHeap:       001c0000
    ProcessParameters: 001c07e8
    WindowTitle:  'C:\Program Files\Common Files\Real\Update_OB\realsched.exe'
    ImageFile:    'C:\Program Files\Common Files\Real\Update_OB\realsched.exe'
    CommandLine:  '"C:\Program Files\Common Files\Real\Update_OB\realsched.exe"  -osboot'
    DllPath:      'C:\Program Files\Common
Files\Real\Update_OB;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Wind
ows;C:\Windows\System32\Wbem;C:\Program Files\QuickTime\QTSystem\'
    Environment:  001d0048
        =::=::\
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\UserName\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        HOMEDRIVE=C:
        HOMEPATH=\Users\UserName
        LOCALAPPDATA=C:\Users\UserName\AppData\Local
        LOGONSERVER=\\HOME
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        SESSIONNAME=Console
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Users\UserName\AppData\Local\Temp
        TMP=C:\Users\UserName\AppData\Local\Temp
        USERDOMAIN=home
        USERNAME=UserName
        USERPROFILE=C:\Users\UserName
        windir=C:\Windows
```

```
        THREAD 83646440  Cid 0cd8.0cdc  Teb: 7ffdf000 Win32Thread: ff2ac1c0 WAIT: (WrUserRequest)
UserMode Non-Alertable
            836fe808  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            836466e8       Image:         realsched.exe
        Wait Start TickCount      32687          Ticks: 10812 (0:00:02:48.668)
        Context Switch Count      145
        UserTime                  00:00:00.031
        KernelTime                00:00:00.062
        Win32 Start Address realsched (0x004165fd)
        Stack Init a6863000 Current a6862b68 Base a6863000 Limit a6860000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a6862b80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a6862bbc 81c293a7 nt!KiSwapThread+0x389
        a6862c18 8cedb8ed nt!KeWaitForSingleObject+0x414
        a6862c74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        a6862c90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        a6862ce8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        a6862d4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        a6862d4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a6862d64)
        0012fd70 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0012fd74 761d3ad1 USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        0012fd98 00402f54 USER32!GetMessageA+0x8a (FPO: [Non-Fpo])
        0012fde4 004031ff realsched+0x2f54
        0012fe00 004010b2 realsched+0x31ff
        0012fe78 00416781 realsched+0x10b2
        0012ffa0 75f33833 realsched+0x16781
        0012ffac 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0012ffec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 837142f0  Cid 0cd8.0dc4  Teb: 7ffde000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            83651518  NotificationEvent
            83648bf0  NotificationEvent
            836535b8  NotificationEvent
            83714378  NotificationTimer
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            836466e8       Image:         realsched.exe
        Wait Start TickCount      9547           Ticks: 33952 (0:00:08:49.654)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address realsched (0x00402f81)
        Stack Init a8fdc000 Current a8fdb8d0 Base a8fdc000 Limit a8fd9000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a8fdb8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8fdb924 81c28c64 nt!KiSwapThread+0x389
        a8fdb970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a8fdbbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a8fdbd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a8fdbd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8fdbd64)
        012ffe90 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        012ffe94 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        012fff30 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        012fff4c 00402b85 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        012fff9c 00402f94 realsched+0x2b85
        012fffac 7746a9bd realsched+0x2f94
        012fffec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 9fdb9bd8  Cid 0cd8.0dd0  Teb: 7ffda000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            836eee70  NotificationEvent
            835f47e8  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            836466e8       Image:         realsched.exe
        Wait Start TickCount      9550           Ticks: 33949 (0:00:08:49.607)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address realsched (0x00412fc0)
        Stack Init a036c000 Current a036b8d0 Base a036c000 Limit a0369000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a036b8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a036b924 81c28c64 nt!KiSwapThread+0x389
        a036b970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a036bbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a036bd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a036bd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a036bd64)
        018dfec4 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        018dfec8 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        018dff64 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        018dff80 00413001 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        018dffa0 75f33833 realsched+0x13001
        018dffac 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        018dffec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 9fd6c630  Cid 0cd8.0320  Teb: 7ffdc000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            836eea78  QueueObject
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            836466e8       Image:         realsched.exe
        Wait Start TickCount      34610          Ticks: 8889 (0:00:02:18.669)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init a6927000 Current a6926bc8 Base a6927000 Limit a6924000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a6926be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a6926c1c 81cad431 nt!KiSwapThread+0x389
        a6926c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a6926cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a6926d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a6926d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a6926d64)
        014cfe88 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        014cfe8c 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        014cfeb8 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        014cfef4 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        014cff60 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        014cff6c 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        014cff94 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        014cffa0 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        014cffac 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        014cffec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Sidebar process

```
PROCESS 8364b2f0  SessionId: 1  Cid: 0ce4    Peb: 7ffdb000  ParentCid: 0b90
    DirBase: 29a01600  ObjectTable: a9a44fc8  HandleCount: 418.
    Image: sidebar.exe
    VadRoot 8370f250 Vads 240 Clone 0 Private 2936. Modified 1787. Locked 0.
    DeviceMap a7766db8
    Token                             a9a13030
    ElapsedTime                       00:08:52.685
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         160800
    QuotaPoolUsage[NonPagedPool]      12000
    Working Set Sizes (now,min,max)  (4091, 50, 345) (16364KB, 200KB, 1380KB)
    PeakWorkingSetSize                6304
    VirtualSize                       116 Mb
    PeakVirtualSize                   118 Mb
    PageFaultCount                    130388
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      8481
    Job                               83658020

    Setting context for this process...
.process /p /r ffffffff8364b2f0

    !peb
PEB at 7ffdb000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00050000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 003217e0 . 0433d6c0
    Ldr.InLoadOrderModuleList:           00321760 . 0433d6b0
    Ldr.InMemoryOrderModuleList:         00321768 . 0433d6b8
            Base TimeStamp                     Module
           50000 4764fba1 Dec 16 10:19:13 2007 C:\Program Files\Windows Sidebar\sidebar.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        74d00000 4549bcbc Nov 02 09:39:08 2006 C:\Windows\system32\ATL.DLL
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        74aa0000 4549bd09 Nov 02 09:40:25 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_5d07289e07e1d100\COMCTL32.dll
        763b0000 4549bdb9 Nov 02 09:43:21 2006 C:\Windows\system32\SHLWAPI.dll
        73d70000 4549bcaf Nov 02 09:38:55 2006
C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.0.6000.16386_none_9ea0ac9ec96e71
27\gdiplus.dll
        76560000 4681c95d Jun 27 03:20:13 2007 C:\Windows\system32\SHELL32.dll
        75dc0000 470c4de2 Oct 10 04:58:26 2007 C:\Windows\system32\urlmon.dll
        76360000 4549bcfb Nov 02 09:40:11 2006 C:\Windows\system32\iertutil.dll
        75650000 45b96fde Jan 26 03:05:02 2007 C:\Windows\system32\CRYPT32.dll
        75820000 4549bd41 Nov 02 09:41:21 2006 C:\Windows\system32\MSASN1.dll
        75ba0000 4549bde2 Nov 02 09:44:02 2006 C:\Windows\system32\USERENV.dll
        75b80000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\Secur32.dll
        71840000 4549bdb4 Nov 02 09:43:16 2006 C:\Windows\system32\sfc.dll
        70dd0000 4549bdb5 Nov 02 09:43:17 2006 C:\Windows\system32\sfc_os.DLL
        77030000 4549bdb0 Nov 02 09:43:12 2006 C:\Windows\system32\SETUPAPI.dll
        71490000 4549bd24 Nov 02 09:40:52 2006 C:\Windows\system32\dwmapi.dll
        70340000 4549bd2a Nov 02 09:40:58 2006 C:\Windows\system32\CRYPTUI.dll
```

```
        74ff0000 4549be2f Nov 02 09:45:19 2006 C:\Windows\system32\WINTRUST.dll
        77580000 462434a3 Apr 17 03:44:51 2007 C:\Windows\system32\imagehlp.dll
        75840000 4549bd53 Nov 02 09:41:39 2006 C:\Windows\system32\NETAPI32.dll
        75ce0000 4549bd99 Nov 02 09:42:49 2006 C:\Windows\system32\PSAPI.DLL
        76310000 4549be44 Nov 02 09:45:40 2006 C:\Windows\system32\WLDAP32.dll
        75fe0000 4549be0e Nov 02 09:44:46 2006 C:\Windows\system32\WS2_32.dll
        77550000 4549bdc7 Nov 02 09:43:35 2006 C:\Windows\system32\NSI.dll
        753f0000 4549bde4 Nov 02 09:44:04 2006 C:\Windows\system32\VERSION.dll
        74cf0000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\MSIMG32.dll
        746d0000 4549bde7 Nov 02 09:44:07 2006 C:\Windows\system32\UxTheme.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        773a0000 4549bce9 Nov 02 09:39:53 2006 C:\Windows\system32\CLBCatQ.DLL
        75a60000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\SXS.DLL
        75350000 4549bdae Nov 02 09:43:10 2006 C:\Windows\system32\rsaenh.dll
        74fe0000 46d779a1 Aug 31 03:14:57 2007 C:\Windows\system32\WTSAPI32.dll
        75300000 4549be2e Nov 02 09:45:18 2006 C:\Windows\system32\WINSTA.dll
        6fa90000 46d4e271 Aug 29 04:05:21 2007 C:\Windows\system32\Wlanapi.dll
        74050000 4549bda1 Nov 02 09:42:57 2006 C:\Windows\system32\OneX.DLL
        74680000 4549bccc Nov 02 09:39:24 2006 C:\Windows\system32\eappprxy.dll
        73f40000 4549bcc9 Nov 02 09:39:21 2006 C:\Windows\system32\eappcfg.dll
        754a0000 4549bcb9 Nov 02 09:39:05 2006 C:\Windows\system32\bcrypt.dll
        72460000 4666193b Jun 06 03:17:31 2007 C:\Windows\System32\msxml3.dll
        76020000 470c4e1e Oct 10 04:59:26 2007 C:\Windows\system32\WININET.dll
        76010000 4549ad42 Nov 02 08:33:06 2006 C:\Windows\system32\Normaliz.dll
        6d250000 4722d0fd Oct 27 06:47:41 2007 C:\Windows\system32\mshtml.dll
        6e9e0000 4549bd98 Nov 02 09:42:48 2006 C:\Windows\system32\msls31.dll
        6f630000 4549bcf7 Nov 02 09:40:07 2006 C:\Windows\system32\MLANG.dll
        6f590000 4549bd94 Nov 02 09:42:44 2006 C:\Windows\system32\msimtf.dll
        6eaa0000 470c4d6e Oct 10 04:56:30 2007 C:\Windows\system32\ieframe.dll
        6dc30000 4549bce2 Nov 02 09:39:46 2006 C:\Windows\system32\jscript.dll
        6f5a0000 4549bd27 Nov 02 09:40:55 2006 C:\Windows\system32\ImgUtil.dll
        6e1d0000 470c4d7f Oct 10 04:56:47 2007 C:\Windows\system32\Dxtrans.dll
        6f070000 4549bcd1 Nov 02 09:39:29 2006 C:\Windows\system32\ddrawex.dll
        6e6d0000 4549bcd0 Nov 02 09:39:28 2006 C:\Windows\system32\DDRAW.dll
        6e890000 4549bccc Nov 02 09:39:24 2006 C:\Windows\system32\DCIMAN32.dll
        75020000 4549bddb Nov 02 09:43:55 2006 C:\Windows\system32\NTMARTA.DLL
        75ad0000 4549bda8 Nov 02 09:43:04 2006 C:\Windows\system32\SAMLIB.dll
        10000000 4681449e Jun 26 17:53:50 2007 C:\Windows\system32\igdumd32.dll
        6e840000 4549bdb9 Nov 02 09:43:21 2006 C:\Windows\system32\pngfilt.dll
        6dbd0000 470c4d7e Oct 10 04:56:46 2007 C:\Windows\system32\Dxtmsft.dll
        6e670000 4549bdec Nov 02 09:44:12 2006 C:\Windows\system32\thumbcache.dll
        75b20000 4549bcaf Nov 02 09:38:55 2006 C:\Windows\system32\apphelp.dll
        70cc0000 4549bdb3 Nov 02 09:43:15 2006 C:\Windows\System32\shdocvw.dll
        744e0000 4549bd96 Nov 02 09:42:46 2006 C:\Windows\system32\PROPSYS.dll
        73240000 4654f735 May 24 03:23:49 2007 C:\Windows\system32\windowscodecs.dll
        6e7c0000 4549bd47 Nov 02 09:41:27 2006 C:\Windows\system32\mscms.dll
        715a0000 4549be2a Nov 02 09:45:14 2006 C:\Windows\system32\WINSPOOL.DRV
        6db50000 470c4dea Oct 10 04:58:34 2007 C:\Windows\system32\mshtmled.dll
        6dd90000 4549bce9 Nov 02 09:39:53 2006 C:\Windows\system32\icm32.dll
    SubSystemData:     00000000
    ProcessHeap:       00320000
    ProcessParameters: 00321010
    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;C:\Program Files\QuickTime\QTSystem\'
    Environment:  003207e8
        =::=::\
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\UserName\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
```

```
        HOMEDRIVE=C:
        HOMEPATH=\Users\UserName
        LOCALAPPDATA=C:\Users\UserName\AppData\Local
        LOGONSERVER=\\HOME
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        SESSIONNAME=Console
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Users\UserName\AppData\Local\Temp
        TMP=C:\Users\UserName\AppData\Local\Temp
        USERDOMAIN=home
        USERNAME=UserName
        USERPROFILE=C:\Users\UserName
        windir=C:\Windows


        THREAD 83681d78  Cid 0ce4.0ce8  Teb: 7ffdf000 Win32Thread: ff2e6908 WAIT: (UserRequest)
UserMode Alertable
            837571c8  SynchronizationEvent
            83627290  SynchronizationEvent
        IRP List:
            899c9f68: (0006,0094) Flags: 00020900  Mdl: 00000000
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8364b2f0       Image:         sidebar.exe
        Wait Start TickCount      43462          Ticks: 37 (0:00:00:00.577)
        Context Switch Count      4967
        UserTime                  00:00:02.792
        KernelTime                00:00:00.717
        Win32 Start Address sidebar!WinMainCRTStartup (0x0006f549)
        Stack Init a686b000 Current a686a8d0 Base a686b000 Limit a6868000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a686a8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a686a924 81c28c64 nt!KiSwapThread+0x389
        a686a970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a686abfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a686ad48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a686ad48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a686ad64)
        001bf694 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        001bf698 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        001bf734 761dc4b7 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        001bf788 00051bff USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
        001bf7d0 00069e9f sidebar!PresentationHost::Run+0x42 (FPO: [Non-Fpo])
        001bf7dc 00067be7 sidebar!SBClientApplication::Run+0x12 (FPO: [Non-Fpo])
        001bf9dc 0006f0ef sidebar!SidebarMain+0x2b3 (FPO: [Non-Fpo])
        001bf9f0 0006f354 sidebar!WinMain+0x18f (FPO: [Non-Fpo])
        001bfa80 75f33833 sidebar!_initterm_e+0x1a1 (FPO: [Non-Fpo])
        001bfa8c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        001bfacc 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 83635030  Cid 0ce4.0dfc  Teb: 7ffde000 Win32Thread: ff3101c0 WAIT: (UserRequest)
UserMode Non-Alertable
            836ad858  NotificationEvent
            9fd1ca80  NotificationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8364b2f0       Image:         sidebar.exe
        Wait Start TickCount      42621          Ticks: 878 (0:00:00:13.696)
        Context Switch Count      58
        UserTime                  00:00:00.031
        KernelTime                00:00:00.062
        Win32 Start Address sidebar!GThumbnailThreadProc (0x0008c8b6)
        Stack Init 9f3cc000 Current 9f3cb8d0 Base 9f3cc000 Limit 9f3c9000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f3cb8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f3cb924 81c28c64 nt!KiSwapThread+0x389
        9f3cb970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f3cbbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f3cbd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f3cbd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f3cbd64)
        0109fe10 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0109fe14 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0109feb0 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0109fecc 0008c8f2 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0109ff0c 75f33833 sidebar!GThumbnailThreadProc+0x3c (FPO: [Non-Fpo])
        0109ff18 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0109ff58 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 83694d78  Cid 0ce4.0e00  Teb: 7ffdd000 Win32Thread: ff735928 WAIT: (UserRequest)
UserMode Non-Alertable
            8368b430  NotificationEvent
            847b5048  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8364b2f0       Image:         sidebar.exe
        Wait Start TickCount      11132          Ticks: 32367 (0:00:08:24.928)
        Context Switch Count      18
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address gdiplus!BackgroundThreadProc (0x73d81909)
        Stack Init a6843000 Current a68428d0 Base a6843000 Limit a6840000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a68428e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a6842924 81c28c64 nt!KiSwapThread+0x389
        a6842970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a6842bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a6842d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a6842d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a6842d64)
        00fbfd48 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00fbfd4c 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00fbfde8 761dc4b7 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        00fbfe3c 761d8b83 USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
        00fbfe58 73d81965 USER32!MsgWaitForMultipleObjects+0x1f (FPO: [Non-Fpo])
        00fbfea4 75f33833 gdiplus!BackgroundThreadProc+0x59 (FPO: [Non-Fpo])
        00fbfeb0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00fbfef0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 836db2b0  Cid 0ce4.0eec  Teb: 7ffd9000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            83484738  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8364b2f0       Image:         sidebar.exe
        Wait Start TickCount      43413          Ticks: 86 (0:00:00:01.341)
        Context Switch Count      131
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address Wlanapi!NotificationApcThreadProc (0x6fa94619)
        Stack Init a8fe0000 Current a8fdfc38 Base a8fe0000 Limit a8fdd000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a8fdfc50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8fdfc8c 81c293a7 nt!KiSwapThread+0x389
        a8fdfce8 81df5057 nt!KeWaitForSingleObject+0x414
        a8fdfd50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a8fdfd50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8fdfd64)
        017bf958 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        017bf95c 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        017bf9cc 6fa9466d kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        017bf9f0 75f33833 Wlanapi!NotificationApcThreadProc+0x54 (FPO: [Non-Fpo])
        017bf9fc 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        017bfa3c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 837e2788  Cid 0ce4.0f8c  Teb: 7ffd8000 Win32Thread: fe96ea40 WAIT: (WrQueue)
UserMode Non-Alertable
            83710208  QueueObject
            837e2810  NotificationTimer
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8364b2f0       Image:         sidebar.exe
        Wait Start TickCount      43413          Ticks: 86 (0:00:00:01.341)
        Context Switch Count      98
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init 9f7f8000 Current 9f7f7bc8 Base 9f7f8000 Limit 9f7f5000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f7f7be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f7f7c1c 81cad431 nt!KiSwapThread+0x389
        9f7f7c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        9f7f7cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        9f7f7d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        9f7f7d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f7f7d64)
        01f5fd88 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01f5fd8c 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        01f5fdb8 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        01f5fdf4 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        01f5fe60 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        01f5fe6c 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        01f5fe94 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        01f5fea0 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        01f5feac 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01f5feec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 8346bd78  Cid 0ce4.0fcc  Teb: 7ffd7000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            837539a0  NotificationEvent
            837e6db0  NotificationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8364b2f0       Image:         sidebar.exe
        Wait Start TickCount      9813           Ticks: 33686 (0:00:08:45.504)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address sidebar!Killbits::KillbitsChangeWaitProc (0x0008d9c5)
        Stack Init 9f7b4000 Current 9f7b38d0 Base 9f7b4000 Limit 9f7b1000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f7b38e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f7b3924 81c28c64 nt!KiSwapThread+0x389
        9f7b3970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f7b3bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f7b3d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f7b3d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f7b3d64)
        0173fdc4 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0173fdc8 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0173fe64 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0173fe80 0008d986 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0173feb4 0008d9dd sidebar!Killbits::KillbitsMonitorProc+0x60 (FPO: [Non-Fpo])
        0173febc 75f33833 sidebar!Killbits::KillbitsChangeWaitProc+0x18 (FPO: [Non-Fpo])
        0173fec8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0173ff08 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 83738550  Cid 0ce4.0fd4  Teb: 7ffd6000 Win32Thread: fe751c08 WAIT: (UserRequest)
UserMode Alertable
            a1800c68  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8364b2f0       Image:         sidebar.exe
        Wait Start TickCount      42622          Ticks: 877 (0:00:00:13.681)
        Context Switch Count      1385
        UserTime                  00:00:00.390
        KernelTime                00:00:00.202
        Win32 Start Address sidebar!StockLib::Utility::t_ObjectThreadProc<PartInstance>
(0x0005e0c1)
        Stack Init 9f294000 Current 9f2938d0 Base 9f294000 Limit 9f291000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f2938e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f293924 81c28c64 nt!KiSwapThread+0x389
        9f293970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f293bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f293d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f293d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f293d64)
        01abf8d4 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01abf8d8 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        01abf974 761dc4b7 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        01abf9c8 00051bff USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
        01abfa10 0005f3a4 sidebar!PresentationHost::Run+0x42 (FPO: [Non-Fpo])
        01abfa1c 0005e11a sidebar!PartInstance::Run+0xc (FPO: [Non-Fpo])
        01abfa4c 75f33833 sidebar!StockLib::Utility::t_ObjectThreadProc<PartInstance>+0x59 (FPO:
[Non-Fpo])
        01abfa58 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01abfa98 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 83735360  Cid 0ce4.0fd8  Teb: 7ffd5000 Win32Thread: fe694228 WAIT: (UserRequest)
UserMode Alertable
            847ad818  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8364b2f0       Image:         sidebar.exe
        Wait Start TickCount      33037          Ticks: 10462 (0:00:02:43.208)
        Context Switch Count      1778
        UserTime                  00:00:00.140
        KernelTime                00:00:00.109
        Win32 Start Address sidebar!StockLib::Utility::t_ObjectThreadProc<PartInstance>
(0x0005e0c1)
        Stack Init 9f7c0000 Current 9f7bf8d0 Base 9f7c0000 Limit 9f7bd000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f7bf8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f7bf924 81c28c64 nt!KiSwapThread+0x389
        9f7bf970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f7bfbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f7bfd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f7bfd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f7bfd64)
        01c9faa8 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01c9faac 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        01c9fb48 761dc4b7 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        01c9fb9c 00051bff USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
        01c9fbe4 0005f3a4 sidebar!PresentationHost::Run+0x42 (FPO: [Non-Fpo])
        01c9fbf0 0005e11a sidebar!PartInstance::Run+0xc (FPO: [Non-Fpo])
        01c9fc20 75f33833 sidebar!StockLib::Utility::t_ObjectThreadProc<PartInstance>+0x59 (FPO:
[Non-Fpo])
        01c9fc2c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01c9fc6c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 837d3c78  Cid 0ce4.0fdc  Teb: 7ffd4000 Win32Thread: fe6c40d0 WAIT: (UserRequest)
UserMode Alertable
            83651d08  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8364b2f0       Image:         sidebar.exe
        Wait Start TickCount      43276          Ticks: 223 (0:00:00:03.478)
        Context Switch Count      2733
        UserTime                  00:00:01.216
        KernelTime                00:00:00.218
        Win32 Start Address sidebar!StockLib::Utility::t_ObjectThreadProc<PartInstance>
(0x0005e0c1)
        Stack Init 9f7bc000 Current 9f7bb8d0 Base 9f7bc000 Limit 9f7b9000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f7bb8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f7bb924 81c28c64 nt!KiSwapThread+0x389
        9f7bb970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f7bbbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f7bbd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f7bbd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f7bbd64)
        01a6fbdc 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01a6fbe0 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        01a6fc7c 761dc4b7 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        01a6fcd0 00051bff USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
        01a6fd18 0005f3a4 sidebar!PresentationHost::Run+0x42 (FPO: [Non-Fpo])
        01a6fd24 0005e11a sidebar!PartInstance::Run+0xc (FPO: [Non-Fpo])
        01a6fd54 75f33833 sidebar!StockLib::Utility::t_ObjectThreadProc<PartInstance>+0x59 (FPO:
[Non-Fpo])
        01a6fd60 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01a6fda0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 83620788  Cid 0ce4.0fe8  Teb: 7ffd3000 Win32Thread: ffbfac78 WAIT: (UserRequest)
UserMode Non-Alertable
            83725658  SynchronizationEvent
            83620810  NotificationTimer
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8364b2f0       Image:         sidebar.exe
        Wait Start TickCount      9975           Ticks: 33524 (0:00:08:42.977)
        Context Switch Count      16
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address mshtml!CExecFT::StaticThreadProc (0x6d26da47)
        Stack Init 9f748000 Current 9f747c38 Base 9f748000 Limit 9f745000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f747c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f747c8c 81c293a7 nt!KiSwapThread+0x389
        9f747ce8 81df5057 nt!KeWaitForSingleObject+0x414
        9f747d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        9f747d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f747d64)
        02cbfe20 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        02cbfe24 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        02cbfe94 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        02cbfea8 6d2ef525 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        02cbfec0 6d2e6c1a mshtml!CDwnTaskExec::ThreadExec+0x127 (FPO: [Non-Fpo])
        02cbfecc 6d26da54 mshtml!CExecFT::ThreadProc+0x3c (FPO: [Non-Fpo])
        02cbfed4 75f33833 mshtml!CExecFT::StaticThreadProc+0xd (FPO: [Non-Fpo])
        02cbfee0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        02cbff20 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 8361b0c8  Cid 0ce4.0fec  Teb: 7ffaf000 Win32Thread: ff308148 WAIT: (UserRequest)
UserMode Non-Alertable
            836527c0  SynchronizationEvent
            8361b150  NotificationTimer
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8364b2f0       Image:         sidebar.exe
        Wait Start TickCount      42622          Ticks: 877 (0:00:00:13.681)
        Context Switch Count      139
        UserTime                  00:00:00.140
        KernelTime                00:00:00.046
        Win32 Start Address mshtml!CExecFT::StaticThreadProc (0x6d26da47)
        Stack Init 9f744000 Current 9f743c38 Base 9f744000 Limit 9f741000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f743c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f743c8c 81c293a7 nt!KiSwapThread+0x389
        9f743ce8 81df5057 nt!KeWaitForSingleObject+0x414
        9f743d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        9f743d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f743d64)
        0177f728 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0177f72c 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0177f79c 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        0177f7b0 6d2ef525 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0177f7c8 6d2e6c1a mshtml!CDwnTaskExec::ThreadExec+0x127 (FPO: [Non-Fpo])
        0177f7d4 6d26da54 mshtml!CExecFT::ThreadProc+0x3c (FPO: [Non-Fpo])
        0177f7dc 75f33833 mshtml!CExecFT::StaticThreadProc+0xd (FPO: [Non-Fpo])
        0177f7e8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0177f828 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 83616188  Cid 0ce4.0ff0  Teb: 7ffae000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            835fd560  QueueObject
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8364b2f0       Image:         sidebar.exe
        Wait Start TickCount      9910           Ticks: 33589 (0:00:08:43.991)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address Dxtrans!TMThreadProc (0x6e1d1c1d)
        Stack Init 9f7b8000 Current 9f7b7bc8 Base 9f7b8000 Limit 9f7b5000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f7b7be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f7b7c1c 81cad431 nt!KiSwapThread+0x389
        9f7b7c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        9f7b7cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        9f7b7d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        9f7b7d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f7b7d64)
        02f6fa28 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        02f6fa2c 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        02f6fa58 6e1d1c5f kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        02f6fad0 75f33833 Dxtrans!TMThreadProc+0x4d (FPO: [Non-Fpo])
        02f6fadc 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        02f6fb1c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 836a1030  Cid 0ce4.0ff4  Teb: 7ffad000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            835fd560  QueueObject
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8364b2f0       Image:         sidebar.exe
        Wait Start TickCount      9910           Ticks: 33589 (0:00:08:43.991)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address Dxtrans!TMThreadProc (0x6e1d1c1d)
        Stack Init 9f758000 Current 9f757bc8 Base 9f758000 Limit 9f755000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f757be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f757c1c 81cad431 nt!KiSwapThread+0x389
        9f757c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        9f757cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        9f757d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        9f757d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f757d64)
        0423fa6c 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0423fa70 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        0423fa9c 6e1d1c5f kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        0423fb14 75f33833 Dxtrans!TMThreadProc+0x4d (FPO: [Non-Fpo])
        0423fb20 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0423fb60 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 836a1d78  Cid 0ce4.0ff8  Teb: 7ffac000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            835fd560  QueueObject
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8364b2f0       Image:         sidebar.exe
        Wait Start TickCount      42622          Ticks: 877 (0:00:00:13.681)
        Context Switch Count      68
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address Dxtrans!TMThreadProc (0x6e1d1c1d)
        Stack Init 9f7ac000 Current 9f7abbc8 Base 9f7ac000 Limit 9f7a9000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f7abbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f7abc1c 81cad431 nt!KiSwapThread+0x389
        9f7abc6c 81d8b982 nt!KeRemoveQueueEx+0x568
        9f7abcc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        9f7abd48 81c8caaa nt!NtRemoveIoCompletion+0x106
        9f7abd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f7abd64)
        01d9fcd8 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01d9fcdc 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        01d9fd08 6e1d1c5f kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        01d9fd80 75f33833 Dxtrans!TMThreadProc+0x4d (FPO: [Non-Fpo])
        01d9fd8c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01d9fdcc 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 836a1ac0  Cid 0ce4.0ffc  Teb: 7ffab000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            835fd560  QueueObject
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8364b2f0       Image:         sidebar.exe
        Wait Start TickCount      9987           Ticks: 33512 (0:00:08:42.790)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address Dxtrans!TMThreadProc (0x6e1d1c1d)
        Stack Init 9f75c000 Current 9f75bbc8 Base 9f75c000 Limit 9f759000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f75bbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f75bc1c 81cad431 nt!KiSwapThread+0x389
        9f75bc6c 81d8b982 nt!KeRemoveQueueEx+0x568
        9f75bcc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        9f75bd48 81c8caaa nt!NtRemoveIoCompletion+0x106
        9f75bd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f75bd64)
        01c2fe88 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01c2fe8c 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        01c2feb8 6e1d1c5f kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        01c2ff30 75f33833 Dxtrans!TMThreadProc+0x4d (FPO: [Non-Fpo])
        01c2ff3c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01c2ff7c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Ehtray process

```
PROCESS 8354dd90  SessionId: 1  Cid: 0cf4    Peb: 7ffd9000  ParentCid: 0b90
    DirBase: 29a01640  ObjectTable: a9a40088  HandleCount:  86.
    Image: ehtray.exe
    VadRoot 8370b5d0 Vads 62 Clone 0 Private 222. Modified 213. Locked 0.
    DeviceMap a7766db8
    Token                             a9a64910
    ElapsedTime                       00:08:52.653
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         105128
    QuotaPoolUsage[NonPagedPool]      3120
    Working Set Sizes (now,min,max)  (337, 50, 345) (1348KB, 200KB, 1380KB)
    PeakWorkingSetSize                1232
    VirtualSize                       50 Mb
    PeakVirtualSize                   51 Mb
    PageFaultCount                    1672
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      535
    Job                               83658020

    Setting context for this process...
.process /p /r ffffffff8354dd90

    !peb
PEB at 7ffd9000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         010a0000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 001a1748 . 001b8578
    Ldr.InLoadOrderModuleList:           001a16c8 . 001b8568
    Ldr.InMemoryOrderModuleList:         001a16d0 . 001b8570
            Base TimeStamp                     Module
         10a0000 4549b563 Nov 02 09:07:47 2006 C:\Windows\ehome\ehtray.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        76560000 4681c95d Jun 27 03:20:13 2007 C:\Windows\system32\SHELL32.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        763b0000 4549bdb9 Nov 02 09:43:21 2006 C:\Windows\system32\SHLWAPI.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        74fe0000 46d779a1 Aug 31 03:14:57 2007 C:\Windows\system32\WTSAPI32.dll
        75610000 4679de70 Jun 21 03:12:00 2007 C:\Windows\system32\slc.dll
        74cb0000 4549bcde Nov 02 09:39:42 2006 C:\Windows\system32\HID.DLL
        77030000 4549bdb0 Nov 02 09:43:12 2006 C:\Windows\system32\SETUPAPI.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        74aa0000 4549bd09 Nov 02 09:40:25 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_5d07289e07e1d100\comctl32.dll
        746d0000 4549bde7 Nov 02 09:44:07 2006 C:\Windows\system32\uxtheme.dll
        75300000 4549be2e Nov 02 09:45:18 2006 C:\Windows\system32\WINSTA.dll
        773a0000 4549bce9 Nov 02 09:39:53 2006 C:\Windows\system32\CLBCatQ.DLL
        75350000 4549bdae Nov 02 09:43:10 2006 C:\Windows\system32\rsaenh.dll
        707a0000 4549bcef Nov 02 09:39:59 2006 C:\Windows\eHome\ehProxy.dll
    SubSystemData:     00000000
    ProcessHeap:       001a0000
```

```
    ProcessParameters: 001a1010
    WindowTitle:  'C:\Windows\ehome\ehtray.exe'
    ImageFile:    'C:\Windows\ehome\ehtray.exe'
    CommandLine:  '"C:\Windows\ehome\ehtray.exe" '
    DllPath:
'C:\Windows\ehome;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Windows
;C:\Windows\System32\Wbem;C:\Program Files\QuickTime\QTSystem\'
    Environment:  001a07e8
        =::=::\
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\UserName\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        HOMEDRIVE=C:
        HOMEPATH=\Users\UserName
        LOCALAPPDATA=C:\Users\UserName\AppData\Local
        LOGONSERVER=\\HOME
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        SESSIONNAME=Console
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Users\UserName\AppData\Local\Temp
        TMP=C:\Users\UserName\AppData\Local\Temp
        USERDOMAIN=home
        USERNAME=UserName
        USERPROFILE=C:\Users\UserName
        windir=C:\Windows
```

```
        THREAD 8354dae8  Cid 0cf4.0cf8  Teb: 7ffdf000 Win32Thread: ff34ec08 WAIT: (UserRequest)
UserMode Alertable
            836ac0f0  SynchronizationEvent
            8370f188  SynchronizationEvent
            835e0a40  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8354dd90       Image:         ehtray.exe
        Wait Start TickCount      32755          Ticks: 10744 (0:00:02:47.607)
        Context Switch Count      141
        UserTime                  00:00:00.031
        KernelTime                00:00:00.000
        Win32 Start Address ehtray!WinMainCRTStartup (0x010a5b34)
        Stack Init a686f000 Current a686e8d0 Base a686f000 Limit a686c000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a686e8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a686e924 81c28c64 nt!KiSwapThread+0x389
        a686e970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a686ebfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a686ed48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a686ed48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a686ed64)
        0009f5e4 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0009f5e8 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0009f684 761dc4b7 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0009f6d8 010a14da USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
        0009f774 010a5c75 ehtray!WinMain+0x1b1 (FPO: [Non-Fpo])
        0009f89c 75f33833 ehtray!ATL::CAtlStringMgr::Reallocate+0x228 (FPO: [Non-Fpo])
        0009f8a8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0009f8e8 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 8388d030  Cid 0cf4.0574  Teb: 7ffde000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            83483d18  QueueObject
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8354dd90       Image:         ehtray.exe
        Wait Start TickCount      34678          Ticks: 8821 (0:00:02:17.608)
        Context Switch Count      6
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init a8f34000 Current a8f33bc8 Base a8f34000 Limit a8f31000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a8f33be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8f33c1c 81cad431 nt!KiSwapThread+0x389
        a8f33c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a8f33cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a8f33d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a8f33d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8f33d64)
        01bafa70 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01bafa74 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        01bafaa0 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        01bafadc 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        01bafb48 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        01bafb54 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        01bafb78 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        01bafb84 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        01bafb90 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        01bafbd0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

GoogleToolbarNotifier process

```
PROCESS 836d3d90  SessionId: 1  Cid: 0cfc    Peb: 7ffd8000  ParentCid: 0b90
    DirBase: 29a01660  ObjectTable: a9a27088  HandleCount:  98.
    Image: GoogleToolbarNotifier.exe
    VadRoot 836275c8 Vads 72 Clone 0 Private 316. Modified 331. Locked 0.
    DeviceMap a7766db8
    Token                             a9a28698
    ElapsedTime                       00:08:52.638
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         85944
    QuotaPoolUsage[NonPagedPool]      3600
    Working Set Sizes (now,min,max)  (394, 50, 345) (1576KB, 200KB, 1380KB)
    PeakWorkingSetSize                1312
    VirtualSize                       47 Mb
    PeakVirtualSize                   50 Mb
    PageFaultCount                    1855
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      735
    Job                               83658020

    Setting context for this process...
.process /p /r ffffffff836d3d90

    !peb
PEB at 7ffd8000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00400000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 002218f8 . 002390f0
    Ldr.InLoadOrderModuleList:           00221878 . 002393f0
    Ldr.InMemoryOrderModuleList:         00221880 . 002393f8
            Base TimeStamp                     Module
          400000 459ee9bb Jan 06 00:13:47 2007 C:\Program
Files\Google\GoogleToolbarNotifier\1.2.1128.5462\GoogleToolbarNotifier.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        76020000 470c4e1e Oct 10 04:59:26 2007 C:\Windows\system32\WININET.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        763b0000 4549bdb9 Nov 02 09:43:21 2006 C:\Windows\system32\SHLWAPI.dll
        76010000 4549ad42 Nov 02 08:33:06 2006 C:\Windows\system32\Normaliz.dll
        76360000 4549bcfb Nov 02 09:40:11 2006 C:\Windows\system32\iertutil.dll
        75ce0000 4549bd99 Nov 02 09:42:49 2006 C:\Windows\system32\PSAPI.DLL
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        74aa0000 4549bd09 Nov 02 09:40:25 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_5d07289e07e1d100\comctl32.dll
        746d0000 4549bde7 Nov 02 09:44:07 2006 C:\Windows\system32\uxtheme.dll
        773a0000 4549bce9 Nov 02 09:39:53 2006 C:\Windows\system32\CLBCatQ.DLL
        75350000 4549bdae Nov 02 09:43:10 2006 C:\Windows\system32\rsaenh.dll
        10000000 459eeacc Jan 06 00:18:20 2007 C:\Program
Files\Google\GoogleToolbarNotifier\1.2.1128.5462\res_en.dll
        75a60000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\SXS.DLL
```

```
         1130000 459ee9f9 Jan 06 00:14:49 2007 C:\Program
Files\Google\GoogleToolbarNotifier\1.2.1128.5462\swg.dll
        75650000 45b96fde Jan 26 03:05:02 2007 C:\Windows\system32\CRYPT32.dll
        75820000 4549bd41 Nov 02 09:41:21 2006 C:\Windows\system32\MSASN1.dll
        75ba0000 4549bde2 Nov 02 09:44:02 2006 C:\Windows\system32\USERENV.dll
        75b80000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\Secur32.dll
        76560000 4681c95d Jun 27 03:20:13 2007 C:\Windows\system32\SHELL32.dll
        74ff0000 4549be2f Nov 02 09:45:19 2006 C:\Windows\system32\WINTRUST.dll
        77580000 462434a3 Apr 17 03:44:51 2007 C:\Windows\system32\imagehlp.dll
    SubSystemData:     00000000
    ProcessHeap:       00220000
    ProcessParameters: 00221010
    WindowTitle:  'C:\Program
Files\Google\GoogleToolbarNotifier\1.2.1128.5462\GoogleToolbarNotifier.exe'
    ImageFile:    'C:\Program
Files\Google\GoogleToolbarNotifier\1.2.1128.5462\GoogleToolbarNotifier.exe'
    CommandLine:  '"C:\Program
Files\Google\GoogleToolbarNotifier\1.2.1128.5462\GoogleToolbarNotifier.exe" '
    DllPath:      'C:\Program
Files\Google\GoogleToolbarNotifier\1.2.1128.5462;C:\Windows\system32;C:\Windows\system;C:\Windows;.
;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Program Files\QuickTime\QTSystem\'
    Environment:  002207e8
        =::=::\
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\UserName\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        HOMEDRIVE=C:
        HOMEPATH=\Users\UserName
        LOCALAPPDATA=C:\Users\UserName\AppData\Local
        LOGONSERVER=\\HOME
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        SESSIONNAME=Console
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Users\UserName\AppData\Local\Temp
        TMP=C:\Users\UserName\AppData\Local\Temp
        USERDOMAIN=home
        USERNAME=UserName
        USERPROFILE=C:\Users\UserName
        windir=C:\Windows
```

```
        THREAD 83681ac0  Cid 0cfc.0d00  Teb: 7ffdf000 Win32Thread: ff3400f0 WAIT: (UserRequest)
UserMode Non-Alertable
            835f9d90  SynchronizationEvent
            836da690  NotificationEvent
            83627688  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            836d3d90       Image:         GoogleToolbarNotifier.exe
        Wait Start TickCount      32687          Ticks: 10812 (0:00:02:48.668)
        Context Switch Count      140
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address GoogleToolbarNotifier (0x0040db8c)
        Stack Init a8fc4000 Current a8fc38d0 Base a8fc4000 Limit a8fc1000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a8fc38e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8fc3924 81c28c64 nt!KiSwapThread+0x389
        a8fc3970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a8fc3bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a8fc3d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a8fc3d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8fc3d64)
        0012fd04 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0012fd08 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0012fda4 761dc4b7 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0012fdf8 761d8b83 USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
        0012fe14 00404994 USER32!MsgWaitForMultipleObjects+0x1f (FPO: [Non-Fpo])
        0012fe54 004050f5 GoogleToolbarNotifier+0x4994
        00000000 00000000 GoogleToolbarNotifier+0x50f5

        THREAD 83719610  Cid 0cfc.0dc0  Teb: 7ffdc000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            835616a8  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            836d3d90       Image:         GoogleToolbarNotifier.exe
        Wait Start TickCount      9547           Ticks: 33952 (0:00:08:49.654)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address GoogleToolbarNotifier (0x004053e0)
        Stack Init 9f2e4000 Current 9f2e3c38 Base 9f2e4000 Limit 9f2e1000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f2e3c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f2e3c8c 81c293a7 nt!KiSwapThread+0x389
        9f2e3ce8 81df5057 nt!KeWaitForSingleObject+0x414
        9f2e3d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        9f2e3d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f2e3d64)
        0142fefc 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0142ff00 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0142ff70 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        0142ff84 00405408 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0142ffac 7746a9bd GoogleToolbarNotifier+0x5408
        0142ffec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 8373c030  Cid 0cfc.0f24  Teb: 7ffdb000 Win32Thread: fe694398 WAIT: (UserRequest)
UserMode Non-Alertable
            83749470  SynchronizationEvent
            836d0f50  SynchronizationEvent
            836d0f80  SynchronizationEvent
            83475568  SynchronizationTimer
            83753968  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            836d3d90       Image:         GoogleToolbarNotifier.exe
        Wait Start TickCount      11132          Ticks: 32367 (0:00:08:24.928)
        Context Switch Count      29
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address swg (0x0113b6e0)
        Stack Init a8f2c000 Current a8f2b8d0 Base a8f2c000 Limit a8f29000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a8f2b8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8f2b924 81c28c64 nt!KiSwapThread+0x389
        a8f2b970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a8f2bbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a8f2bd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a8f2bd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8f2bd64)
        0173fe40 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0173fe44 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0173fee0 761dc4b7 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0173ff34 761d8b83 USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
        0173ff50 0113b947 USER32!MsgWaitForMultipleObjects+0x1f (FPO: [Non-Fpo])
        0173ffac 7746a9bd swg+0xb947
        0173ffec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 8394dc90  Cid 0cfc.09f0  Teb: 7ffde000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            837552d8  QueueObject
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            836d3d90       Image:         GoogleToolbarNotifier.exe
        Wait Start TickCount      34610          Ticks: 8889 (0:00:02:18.669)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init a8e92000 Current a8e91bc8 Base a8e92000 Limit a8e8f000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a8e91be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8e91c1c 81cad431 nt!KiSwapThread+0x389
        a8e91c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a8e91cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a8e91d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a8e91d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8e91d64)
        00d9fe88 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00d9fe8c 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        00d9feb8 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        00d9fef4 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        00d9ff60 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        00d9ff6c 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        00d9ff94 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        00d9ffa0 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        00d9ffac 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00d9ffec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Igfxsrvc process

```
PROCESS 8354c7a0  SessionId: 1  Cid: 0ddc    Peb: 7ffdc000  ParentCid: 02ec
    DirBase: 29a013c0  ObjectTable: a83f6790  HandleCount:  68.
    Image: igfxsrvc.exe
    VadRoot 8370d630 Vads 61 Clone 0 Private 329. Modified 2. Locked 0.
    DeviceMap a7766db8
    Token                             a9af4030
    ElapsedTime                       00:08:49.441
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         54720
    QuotaPoolUsage[NonPagedPool]      2928
    Working Set Sizes (now,min,max)  (1118, 50, 345) (4472KB, 200KB, 1380KB)
    PeakWorkingSetSize                1118
    VirtualSize                       32 Mb
    PeakVirtualSize                   33 Mb
    PageFaultCount                    1225
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      397

    Setting context for this process...
.process /p /r ffffffff8354c7a0

    !peb
PEB at 7ffdc000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00400000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00631780 . 00649f50
    Ldr.InLoadOrderModuleList:           00631700 . 0064a170
    Ldr.InMemoryOrderModuleList:         00631708 . 0064a178
            Base TimeStamp                     Module
          400000 468136a6 Jun 26 16:54:14 2007 C:\Windows\system32\igfxsrvc.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        746d0000 4549bde7 Nov 02 09:44:07 2006 C:\Windows\system32\uxtheme.dll
        773a0000 4549bce9 Nov 02 09:39:53 2006 C:\Windows\system32\CLBCatQ.DLL
        75350000 4549bdae Nov 02 09:43:10 2006 C:\Windows\system32\rsaenh.dll
        10000000 468136a8 Jun 26 16:54:16 2007 C:\Windows\system32\igfxsrvc.dll
          3a0000 4681368b Jun 26 16:53:47 2007 C:\Windows\system32\igfxdev.dll
        75020000 4549bddb Nov 02 09:43:55 2006 C:\Windows\system32\NTMARTA.DLL
        76310000 4549be44 Nov 02 09:45:40 2006 C:\Windows\system32\WLDAP32.dll
        75fe0000 4549be0e Nov 02 09:44:46 2006 C:\Windows\system32\WS2_32.dll
        77550000 4549bdc7 Nov 02 09:43:35 2006 C:\Windows\system32\NSI.dll
        75ce0000 4549bd99 Nov 02 09:42:49 2006 C:\Windows\system32\PSAPI.DLL
        75ad0000 4549bda8 Nov 02 09:43:04 2006 C:\Windows\system32\SAMLIB.dll
    SubSystemData:     00000000
    ProcessHeap:       00630000
    ProcessParameters: 00631010
    WindowTitle:  'C:\Windows\system32\igfxsrvc.exe'
    ImageFile:    'C:\Windows\system32\igfxsrvc.exe'
```

```
    CommandLine:  'C:\Windows\system32\igfxsrvc.exe -Embedding'
    DllPath:
'C:\Windows\system32;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Wind
ows;C:\Windows\System32\Wbem;C:\Program Files\QuickTime\QTSystem\'
    Environment:  006307e8
        =::=::\
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\UserName\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        HOMEDRIVE=C:
        HOMEPATH=\Users\UserName
        LOCALAPPDATA=C:\Users\UserName\AppData\Local
        LOGONSERVER=\\HOME
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        SESSIONNAME=Console
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Users\UserName\AppData\Local\Temp
        TMP=C:\Users\UserName\AppData\Local\Temp
        USERDOMAIN=home
        USERNAME=UserName
        USERPROFILE=C:\Users\UserName
        windir=C:\Windows


        THREAD 83561400  Cid 0ddc.0de0  Teb: 7ffdf000 Win32Thread: ff23b868 WAIT: (WrUserRequest)
UserMode Non-Alertable
            847b50f8  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8354c7a0       Image:         igfxsrvc.exe
        Wait Start TickCount      43483          Ticks: 16 (0:00:00:00.249)
        Context Switch Count      3089
        UserTime                  00:00:00.031
        KernelTime                00:00:00.296
        Win32 Start Address igfxsrvc (0x004132b2)
        Stack Init a8fbc000 Current a8fbbb68 Base a8fbc000 Limit a8fb9000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a8fbbb80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8fbbbbc 81c293a7 nt!KiSwapThread+0x389
        a8fbbc18 8cedb8ed nt!KeWaitForSingleObject+0x414
        a8fbbc74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        a8fbbc90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        a8fbbce8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        a8fbbd4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        a8fbbd4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8fbbd64)
        0012fea0 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0012fea4 761d3ad1 USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        0012fec8 0040c544 USER32!GetMessageA+0x8a (FPO: [Non-Fpo])
        0012ffa0 75f33833 igfxsrvc+0xc544
        0012ffac 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0012ffec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 837128a0  Cid 0ddc.0de4  Teb: 7ffde000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            837028a0  SynchronizationEvent
            83712928  NotificationTimer
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8354c7a0       Image:         igfxsrvc.exe
        Wait Start TickCount      43483          Ticks: 16 (0:00:00:00.249)
        Context Switch Count      544
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address igfxsrvc (0x00406870)
        Stack Init a8fb8000 Current a8fb7c38 Base a8fb8000 Limit a8fb5000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a8fb7c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8fb7c8c 81c293a7 nt!KiSwapThread+0x389
        a8fb7ce8 81df5057 nt!KeWaitForSingleObject+0x414
        a8fb7d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a8fb7d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8fb7d64)
        00eafefc 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00eaff00 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        00eaff70 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        00eaff84 004061fe kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        00eaffac 7746a9bd igfxsrvc+0x61fe
        00eaffec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 836a4478  Cid 0ddc.0360  Teb: 7ffdd000 Win32Thread: fede7e98 WAIT: (WrQueue)
UserMode Non-Alertable
            83703eb8  QueueObject
            836a4500  NotificationTimer
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8354c7a0       Image:         igfxsrvc.exe
        Wait Start TickCount      43483          Ticks: 16 (0:00:00:00.249)
        Context Switch Count      1179
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init a8e62000 Current a8e61bc8 Base a8e62000 Limit a8e5f000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a8e61be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8e61c1c 81cad431 nt!KiSwapThread+0x389
        a8e61c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a8e61cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a8e61d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a8e61d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8e61d64)
        0142fe88 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0142fe8c 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        0142feb8 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        0142fef4 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        0142ff60 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        0142ff6c 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        0142ff94 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        0142ffa0 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        0142ffac 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0142ffec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
THREAD 83a09a90  Cid 0ddc.0828  Teb: 7ffdb000 Win32Thread: 00000000 WAIT: (WrQueue) UserMode Non-
Alertable
            83703eb8  QueueObject
            83a09b18  NotificationTimer
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8354c7a0       Image:         igfxsrvc.exe
        Wait Start TickCount      42703          Ticks: 796 (0:00:00:12.417)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init a1e9a000 Current a1e99bc8 Base a1e9a000 Limit a1e97000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a1e99be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1e99c1c 81cad431 nt!KiSwapThread+0x389
        a1e99c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a1e99cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a1e99d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a1e99d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1e99d64)
        0152fe88 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0152fe8c 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        0152feb8 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        0152fef4 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        0152ff60 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        0152ff6c 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        0152ff94 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        0152ffa0 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        0152ffac 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0152ffec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Ehmsas process

```
PROCESS 83687850  SessionId: 1  Cid: 0e24    Peb: 7ffde000  ParentCid: 02ec
    DirBase: 29a015c0  ObjectTable: a838a428  HandleCount:  53.
    Image: ehmsas.exe
    VadRoot 8371dde8 Vads 47 Clone 0 Private 200. Modified 1. Locked 0.
    DeviceMap a7766db8
    Token                             a77f0ca0
    ElapsedTime                       00:08:48.520
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         52360
    QuotaPoolUsage[NonPagedPool]      2256
    Working Set Sizes (now,min,max)  (910, 50, 345) (3640KB, 200KB, 1380KB)
    PeakWorkingSetSize                913
    VirtualSize                       25 Mb
    PeakVirtualSize                   26 Mb
    PageFaultCount                    989
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      259

    Setting context for this process...
.process /p /r ffffffff83687850

    !peb
PEB at 7ffde000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00260000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 003e1758 . 003f9b18
    Ldr.InLoadOrderModuleList:           003e16d8 . 003f9b08
    Ldr.InMemoryOrderModuleList:         003e16e0 . 003f9b10
            Base TimeStamp                     Module
          260000 4549b566 Nov 02 09:07:50 2006 C:\Windows\ehome\ehmsas.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        74d00000 4549bcbc Nov 02 09:39:08 2006 C:\Windows\system32\ATL.DLL
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        746d0000 4549bde7 Nov 02 09:44:07 2006 C:\Windows\system32\uxtheme.dll
        773a0000 4549bce9 Nov 02 09:39:53 2006 C:\Windows\system32\CLBCatQ.DLL
        75350000 4549bdae Nov 02 09:43:10 2006 C:\Windows\system32\rsaenh.dll
        707a0000 4549bcef Nov 02 09:39:59 2006 C:\Windows\eHome\ehProxy.dll
    SubSystemData:     00000000
    ProcessHeap:       003e0000
    ProcessParameters: 003e1010
    WindowTitle:  'C:\Windows\ehome\ehmsas.exe'
    ImageFile:    'C:\Windows\ehome\ehmsas.exe'
    CommandLine:  'C:\Windows\ehome\ehmsas.exe -Embedding'
    DllPath:
'C:\Windows\ehome;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Windows
;C:\Windows\System32\Wbem;C:\Program Files\QuickTime\QTSystem\'
    Environment:  003e07e8
        =::=::\
```

```
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\UserName\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        HOMEDRIVE=C:
        HOMEPATH=\Users\UserName
        LOCALAPPDATA=C:\Users\UserName\AppData\Local
        LOGONSERVER=\\HOME
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        SESSIONNAME=Console
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Users\UserName\AppData\Local\Temp
        TMP=C:\Users\UserName\AppData\Local\Temp
        USERDOMAIN=home
        USERNAME=UserName
        USERPROFILE=C:\Users\UserName
        windir=C:\Windows


        THREAD 83625030  Cid 0e24.0e28  Teb: 7ffdf000 Win32Thread: ff36b9f0 WAIT: (WrUserRequest)
UserMode Non-Alertable
            8368fa80  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            83687850       Image:         ehmsas.exe
        Wait Start TickCount      32755          Ticks: 10744 (0:00:02:47.607)
        Context Switch Count      141
        UserTime                  00:00:00.031
        KernelTime                00:00:00.187
        Win32 Start Address ehmsas!wWinMainCRTStartup (0x0026188d)
        Stack Init 9f3dc000 Current 9f3dbb68 Base 9f3dc000 Limit 9f3d9000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f3dbb80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f3dbbbc 81c293a7 nt!KiSwapThread+0x389
        9f3dbc18 8cedb8ed nt!KeWaitForSingleObject+0x414
        9f3dbc74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        9f3dbc90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        9f3dbce8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        9f3dbd4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        9f3dbd4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f3dbd64)
        0007fce4 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0007fce8 761e19cd USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        0007fd04 00261288 USER32!GetMessageW+0x33 (FPO: [Non-Fpo])
        0007fd58 00261a1e ehmsas!wWinMain+0x12b (FPO: [Non-Fpo])
        0007fdec 75f33833 ehmsas!_initterm_e+0x1b1 (FPO: [Non-Fpo])
        0007fdf8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0007fe38 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 83625338  Cid 0e24.0e2c  Teb: 7ffdd000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            83713320  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            83687850       Image:         ehmsas.exe
        Wait Start TickCount      9623           Ticks: 33876 (0:00:08:48.468)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address
ehmsas!ATL::CComObjectRootEx<ATL::CComMultiThreadModel>::~CComObjectRootEx<ATL::CComMultiThreadMode
l> (0x00261fc4)
        Stack Init 9f3f4000 Current 9f3f3c38 Base 9f3f4000 Limit 9f3f1000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f3f3c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f3f3c8c 81c293a7 nt!KiSwapThread+0x389
        9f3f3ce8 81df5057 nt!KeWaitForSingleObject+0x414
        9f3f3d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        9f3f3d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f3f3d64)
        0116feac 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0116feb0 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0116ff20 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        0116ff34 00261ff5 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0116ff4c 00261fd1 ehmsas!CExeModule::MonitorShutdown+0x19 (FPO: [Non-Fpo])
        0116ff54 75f33833
ehmsas!ATL::CComObjectRootEx<ATL::CComMultiThreadModel>::~CComObjectRootEx<ATL::CComMultiThreadMode
l>+0x27 (FPO: [Non-Fpo])
        0116ff60 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0116ffa0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 8389d458  Cid 0e24.0a74  Teb: 7ffdc000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            83486160  QueueObject
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            83687850       Image:         ehmsas.exe
        Wait Start TickCount      34678          Ticks: 8821 (0:00:02:17.608)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init a68e3000 Current a68e2bc8 Base a68e3000 Limit a68e0000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a68e2be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a68e2c1c 81cad431 nt!KiSwapThread+0x389
        a68e2c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a68e2cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a68e2d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a68e2d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a68e2d64)
        00fef810 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00fef814 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        00fef840 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        00fef87c 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        00fef8e8 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        00fef8f4 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        00fef918 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        00fef924 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        00fef930 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00fef970 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Ieuser process

```
PROCESS 8380c398  SessionId: 1  Cid: 0910    Peb: 7ffd7000  ParentCid: 08b4
    DirBase: 29a01680  ObjectTable: a8b69ab8  HandleCount: 222.
    Image: ieuser.exe
    VadRoot 9fc7a7f8 Vads 116 Clone 0 Private 566. Modified 3. Locked 0.
    DeviceMap a7766db8
    Token                             aa43aca0
    ElapsedTime                       00:08:15.431
    UserTime                          00:00:00.093
    KernelTime                        00:00:00.046
    QuotaPoolUsage[PagedPool]         117240
    QuotaPoolUsage[NonPagedPool]      5640
    Working Set Sizes (now,min,max)  (2072, 50, 345) (8288KB, 200KB, 1380KB)
    PeakWorkingSetSize                2096
    VirtualSize                       59 Mb
    PeakVirtualSize                   61 Mb
    PageFaultCount                    2354
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      1012

    Setting context for this process...
.process /p /r ffffffff8380c398

    !peb
PEB at 7ffd7000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00b10000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 000a1908 . 000ed870
    Ldr.InLoadOrderModuleList:           000a1888 . 000ed860
    Ldr.InMemoryOrderModuleList:         000a1890 . 000ed868
            Base TimeStamp                     Module
          b10000 470c3335 Oct 10 03:04:37 2007 C:\Program Files\Internet Explorer\ieuser.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        75ce0000 4549bd99 Nov 02 09:42:49 2006 C:\Windows\system32\PSAPI.DLL
        74cf0000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\MSIMG32.dll
        76560000 4681c95d Jun 27 03:20:13 2007 C:\Windows\system32\SHELL32.dll
        763b0000 4549bdb9 Nov 02 09:43:21 2006 C:\Windows\system32\SHLWAPI.dll
        75650000 45b96fde Jan 26 03:05:02 2007 C:\Windows\system32\CRYPT32.dll
        75820000 4549bd41 Nov 02 09:41:21 2006 C:\Windows\system32\MSASN1.dll
        75ba0000 4549bde2 Nov 02 09:44:02 2006 C:\Windows\system32\USERENV.dll
        75b80000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\Secur32.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        753f0000 4549bde4 Nov 02 09:44:04 2006 C:\Windows\system32\VERSION.dll
        74ff0000 4549be2f Nov 02 09:45:19 2006 C:\Windows\system32\WINTRUST.dll
        77580000 462434a3 Apr 17 03:44:51 2007 C:\Windows\system32\imagehlp.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        74aa0000 4549bd09 Nov 02 09:40:25 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_5d07289e07e1d100\comctl32.dll
        773a0000 4549bce9 Nov 02 09:39:53 2006 C:\Windows\system32\CLBCatQ.DLL
        75350000 4549bdae Nov 02 09:43:10 2006 C:\Windows\system32\rsaenh.dll
        746d0000 4549bde7 Nov 02 09:44:07 2006 C:\Windows\system32\uxtheme.dll
```

```
        70ab0000 4549bcbf Nov 02 09:39:11 2006 C:\Windows\system32\actxprxy.dll
        6eaa0000 470c4d6e Oct 10 04:56:30 2007 C:\Windows\system32\ieframe.dll
        76360000 4549bcfb Nov 02 09:40:11 2006 C:\Windows\system32\iertutil.dll
        76020000 470c4e1e Oct 10 04:59:26 2007 C:\Windows\system32\WININET.dll
        76010000 4549ad42 Nov 02 08:33:06 2006 C:\Windows\system32\Normaliz.dll
        75fe0000 4549be0e Nov 02 09:44:46 2006 C:\Windows\system32\ws2_32.dll
        77550000 4549bdc7 Nov 02 09:43:35 2006 C:\Windows\system32\NSI.dll
        73a20000 4549bda3 Nov 02 09:42:59 2006 C:\Windows\system32\RASAPI32.dll
        73a00000 4549bdab Nov 02 09:43:07 2006 C:\Windows\system32\rasman.dll
        75840000 4549bd53 Nov 02 09:41:39 2006 C:\Windows\system32\NETAPI32.dll
        73960000 4549bdd1 Nov 02 09:43:45 2006 C:\Windows\system32\TAPI32.dll
        73950000 4549bdba Nov 02 09:43:22 2006 C:\Windows\system32\rtutils.dll
        738c0000 4549be1d Nov 02 09:45:01 2006 C:\Windows\system32\WINMM.dll
        73880000 4549bd93 Nov 02 09:42:43 2006 C:\Windows\system32\OLEACC.dll
        75480000 4549bd20 Nov 02 09:40:48 2006 C:\Windows\system32\credssp.dll
        75050000 46773a78 Jun 19 03:07:52 2007 C:\Windows\system32\schannel.dll
        713e0000 4549bdd6 Nov 02 09:43:50 2006 C:\Windows\system32\sensapi.dll
        74d30000 4549bd6b Nov 02 09:42:03 2006 C:\Windows\system32\NLAapi.dll
        755b0000 4549bd3f Nov 02 09:41:19 2006 C:\Windows\system32\IPHLPAPI.DLL
        75570000 46807ea6 Jun 26 03:49:10 2007 C:\Windows\system32\dhcpcsvc.DLL
        75af0000 4549bcf1 Nov 02 09:40:01 2006 C:\Windows\system32\DNSAPI.dll
        75560000 4549be1e Nov 02 09:45:02 2006 C:\Windows\system32\WINNSI.DLL
        75540000 46807ea7 Jun 26 03:49:11 2007 C:\Windows\system32\dhcpcsvc6.DLL
        72a60000 4549bda2 Nov 02 09:42:58 2006 C:\Windows\system32\rasadhlp.dll
        75b20000 4549bcaf Nov 02 09:38:55 2006 C:\Windows\system32\apphelp.dll
        75a60000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\SXS.DLL
        75dc0000 470c4de2 Oct 10 04:58:26 2007 C:\Windows\system32\urlmon.dll
        6d660000 4549bd70 Nov 02 09:42:08 2006 C:\Windows\system32\msfeeds.dll
        6f630000 4549bcf7 Nov 02 09:40:07 2006 C:\Windows\system32\MLANG.dll
        77030000 4549bdb0 Nov 02 09:43:12 2006 C:\Windows\system32\SETUPAPI.dll
    SubSystemData:     00000000
    ProcessHeap:       000a0000
    ProcessParameters: 000a10e0
    WindowTitle:  'C:\Program Files\Internet Explorer\ieuser.exe'
    ImageFile:    'C:\Program Files\Internet Explorer\ieuser.exe'
    CommandLine:  '"C:\Program Files\Internet Explorer\ieuser.exe" -Embedding'
    DllPath:      'C:\Program Files\Internet
Explorer;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Program Files\Internet
Explorer;;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Program
Files\QuickTime\QTSystem\'
    Environment:  000a07e8
        =::=::\
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\UserName\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        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=\\HOME
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Program Files\Internet
Explorer;;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        SESSIONNAME=Console
```

```
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Users\UserName\AppData\Local\Temp
        TMP=C:\Users\UserName\AppData\Local\Temp
        USERDOMAIN=home
        USERNAME=UserName
        USERPROFILE=C:\Users\UserName
        windir=C:\Windows


        THREAD 8358fd78  Cid 0910.0938  Teb: 7ffdf000 Win32Thread: ff3303d0 WAIT: (UserRequest)
UserMode Non-Alertable
            83824170  NotificationEvent
            8382d5e0  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8380c398       Image:         ieuser.exe
        Wait Start TickCount      11744          Ticks: 31755 (0:00:08:15.381)
        Context Switch Count      68
        UserTime                  00:00:00.046
        KernelTime                00:00:00.015
        Win32 Start Address ieuser!wWinMainCRTStartup (0x00b15301)
        Stack Init a8f6c000 Current a8f6b8d0 Base a8f6c000 Limit a8f69000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a8f6b8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8f6b924 81c28c64 nt!KiSwapThread+0x389
        a8f6b970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a8f6bbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a8f6bd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a8f6bd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8f6bd64)
        0007fc9c 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0007fca0 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0007fd3c 761dc4b7 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0007fd90 761d8b83 USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
        0007fdac 00b1140b USER32!MsgWaitForMultipleObjects+0x1f (FPO: [Non-Fpo])
        0007fdf0 00b14623 ieuser!_MyMiniPump+0x52 (FPO: [Non-Fpo])
        0007fe30 00b144c7 ieuser!wWinMain+0x1a1 (FPO: [Non-Fpo])
        0007fec4 75f33833 ieuser!_initterm_e+0x1b1 (FPO: [Non-Fpo])
        0007fed0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0007ff10 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 838388e0  Cid 0910.0934  Teb: 7ffda000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            83807b30  SynchronizationTimer
            837201f0  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8380c398       Image:         ieuser.exe
        Wait Start TickCount      11977          Ticks: 31522 (0:00:08:11.746)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x7744b49a)
        Stack Init a8f8c000 Current a8f8b8d0 Base a8f8c000 Limit a8f89000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a8f8b8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8f8b924 81c28c64 nt!KiSwapThread+0x389
        a8f8b970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a8f8bbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a8f8bd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a8f8bd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8f8bd64)
        0183f838 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0183f83c 7744b65b ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0183f9d8 75f33833 ntdll!TppWaiterpThread+0x294 (FPO: [Non-Fpo])
        0183f9e4 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0183fa24 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 8371e4f0  Cid 0910.0b60  Teb: 7ffd9000 Win32Thread: fe8969f0 WAIT: (WrUserRequest)
UserMode Non-Alertable
            83875da0  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8380c398       Image:         ieuser.exe
        Wait Start TickCount      35032          Ticks: 8467 (0:00:02:12.086)
        Context Switch Count      32
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ole32!CRpcThreadCache::RpcWorkerThreadEntry (0x7644fc53)
        Stack Init a0863000 Current a0862b68 Base a0863000 Limit a0860000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a0862b80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0862bbc 81c293a7 nt!KiSwapThread+0x389
        a0862c18 8cedb8ed nt!KeWaitForSingleObject+0x414
        a0862c74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        a0862c90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        a0862ce8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        a0862d4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        a0862d4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0862d64)
        0178fcb8 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0178fcbc 761e19cd USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        0178fcd8 76458155 USER32!GetMessageW+0x33 (FPO: [Non-Fpo])
        0178fd18 7645258c ole32!CDllHost::STAWorkerLoop+0x81 (FPO: [Non-Fpo])
        0178fd34 764524ce ole32!CDllHost::WorkerThread+0xce (FPO: [Non-Fpo])
        0178fd3c 7644fc0d ole32!DLLHostThreadEntry+0xd (FPO: [Non-Fpo])
        0178fd58 7644fc73 ole32!CRpcThread::WorkerLoop+0x26 (FPO: [Non-Fpo])
        0178fd64 75f33833 ole32!CRpcThreadCache::RpcWorkerThreadEntry+0x20 (FPO: [Non-Fpo])
        0178fd70 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0178fdb0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 8367cd48  Cid 0910.092c  Teb: 7ffdd000 Win32Thread: fede9b80 WAIT: (WrQueue)
UserMode Non-Alertable
            837fc830  QueueObject
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8380c398       Image:         ieuser.exe
        Wait Start TickCount      36955          Ticks: 6544 (0:00:01:42.087)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init 9f800000 Current 9f7ffbc8 Base 9f800000 Limit 9f7fd000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f7ffbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f7ffc1c 81cad431 nt!KiSwapThread+0x389
        9f7ffc6c 81d8b982 nt!KeRemoveQueueEx+0x568
        9f7ffcc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        9f7ffd48 81c8caaa nt!NtRemoveIoCompletion+0x106
        9f7ffd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f7ffd64)
        010ef7e0 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        010ef7e4 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        010ef810 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        010ef84c 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        010ef8b8 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        010ef8c4 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        010ef8e8 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        010ef8f4 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        010ef900 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        010ef940 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Iexplore process

```
PROCESS 8380fd90  SessionId: 1  Cid: 05a4    Peb: 7ffde000  ParentCid: 08b4
    DirBase: 29a01620  ObjectTable: a9a5cd90  HandleCount: 604.
    Image: iexplore.exe
    VadRoot 837ebab0 Vads 428 Clone 0 Private 6177. Modified 357. Locked 0.
    DeviceMap a7766db8
    Token                             aa43c030
    ElapsedTime                       00:08:15.321
    UserTime                          00:00:00.265
    KernelTime                        00:00:00.109
    QuotaPoolUsage[PagedPool]         244424
    QuotaPoolUsage[NonPagedPool]      28312
    Working Set Sizes (now,min,max)  (12404, 50, 345) (49616KB, 200KB, 1380KB)
    PeakWorkingSetSize                13942
    VirtualSize                       195 Mb
    PeakVirtualSize                   222 Mb
    PageFaultCount                    17155
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      14371

    Setting context for this process...
.process /p /r ffffffff8380fd90

    !peb
PEB at 7ffde000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00a20000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00451900 . 054f8040
    Ldr.InLoadOrderModuleList:           00451880 . 054f8030
    Ldr.InMemoryOrderModuleList:         00451888 . 054f8038
            Base TimeStamp                     Module
          a20000 470c3339 Oct 10 03:04:41 2007 C:\Program Files\Internet Explorer\iexplore.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        763b0000 4549bdb9 Nov 02 09:43:21 2006 C:\Windows\system32\SHLWAPI.dll
        76560000 4681c95d Jun 27 03:20:13 2007 C:\Windows\system32\SHELL32.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        75dc0000 470c4de2 Oct 10 04:58:26 2007 C:\Windows\system32\urlmon.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        76360000 4549bcfb Nov 02 09:40:11 2006 C:\Windows\system32\iertutil.dll
        753f0000 4549bde4 Nov 02 09:44:04 2006 C:\Windows\system32\VERSION.dll
        6e920000 4549bdb7 Nov 02 09:43:19 2006 C:\Windows\system32\ShimEng.dll
        75b20000 4549bcaf Nov 02 09:38:55 2006 C:\Windows\system32\apphelp.dll
        71ce0000 470c4d6b Oct 10 04:56:27 2007 C:\Windows\AppPatch\iebrshim.dll
        71ca0000 4549bcb8 Nov 02 09:39:04 2006 C:\Windows\AppPatch\AcRedir.DLL
        6d760000 4718255c Oct 19 04:32:44 2007 C:\Windows\AppPatch\AcLayers.DLL
        75ba0000 4549bde2 Nov 02 09:44:02 2006 C:\Windows\system32\USERENV.dll
        75b80000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\Secur32.dll
        715a0000 4549be2a Nov 02 09:45:14 2006 C:\Windows\system32\WINSPOOL.DRV
        75750000 4549bd14 Nov 02 09:40:36 2006 C:\Windows\system32\MPR.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        74aa0000 4549bd09 Nov 02 09:40:25 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_5d07289e07e1d100\comctl32.dll
```

```
        76020000 470c4e1e Oct 10 04:59:26 2007 C:\Windows\system32\WININET.dll
        76010000 4549ad42 Nov 02 08:33:06 2006 C:\Windows\system32\Normaliz.dll
        75fe0000 4549be0e Nov 02 09:44:46 2006 C:\Windows\system32\ws2_32.dll
        77550000 4549bdc7 Nov 02 09:43:35 2006 C:\Windows\system32\NSI.dll
        73a20000 4549bda3 Nov 02 09:42:59 2006 C:\Windows\system32\RASAPI32.dll
        73a00000 4549bdab Nov 02 09:43:07 2006 C:\Windows\system32\rasman.dll
        75840000 4549bd53 Nov 02 09:41:39 2006 C:\Windows\system32\NETAPI32.dll
        75ce0000 4549bd99 Nov 02 09:42:49 2006 C:\Windows\system32\PSAPI.DLL
        73960000 4549bdd1 Nov 02 09:43:45 2006 C:\Windows\system32\TAPI32.dll
        73950000 4549bdba Nov 02 09:43:22 2006 C:\Windows\system32\rtutils.dll
        738c0000 4549be1d Nov 02 09:45:01 2006 C:\Windows\system32\WINMM.dll
        73880000 4549bd93 Nov 02 09:42:43 2006 C:\Windows\system32\OLEACC.dll
        75480000 4549bd20 Nov 02 09:40:48 2006 C:\Windows\system32\credssp.dll
        75650000 45b96fde Jan 26 03:05:02 2007 C:\Windows\system32\CRYPT32.dll
        75820000 4549bd41 Nov 02 09:41:21 2006 C:\Windows\system32\MSASN1.dll
        75050000 46773a78 Jun 19 03:07:52 2007 C:\Windows\system32\schannel.dll
        713e0000 4549bdd6 Nov 02 09:43:50 2006 C:\Windows\system32\sensapi.dll
        74d30000 4549bd6b Nov 02 09:42:03 2006 C:\Windows\system32\NLAapi.dll
        755b0000 4549bd3f Nov 02 09:41:19 2006 C:\Windows\system32\IPHLPAPI.DLL
        75570000 46807ea6 Jun 26 03:49:10 2007 C:\Windows\system32\dhcpcsvc.DLL
        75af0000 4549bcf1 Nov 02 09:40:01 2006 C:\Windows\system32\DNSAPI.dll
        75560000 4549be1e Nov 02 09:45:02 2006 C:\Windows\system32\WINNSI.DLL
        75540000 46807ea7 Jun 26 03:49:11 2007 C:\Windows\system32\dhcpcsvc6.DLL
        72a60000 4549bda2 Nov 02 09:42:58 2006 C:\Windows\system32\rasadhlp.dll
        6eaa0000 470c4d6e Oct 10 04:56:30 2007 C:\Windows\system32\IEFRAME.dll
        746d0000 4549bde7 Nov 02 09:44:07 2006 C:\Windows\system32\UxTheme.dll
        773a0000 4549bce9 Nov 02 09:39:53 2006 C:\Windows\system32\CLBCatQ.DLL
        75350000 4549bdae Nov 02 09:43:10 2006 C:\Windows\system32\rsaenh.dll
        70ab0000 4549bcbf Nov 02 09:39:11 2006 C:\Windows\system32\actxprxy.dll
        6e460000 470c4d74 Oct 10 04:56:36 2007 C:\Windows\system32\IEUI.dll
        74cf0000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\MSIMG32.dll
        73d70000 4549bcaf Nov 02 09:38:55 2006
C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.0.6000.16386_none_9ea0ac9ec96e71
27\gdiplus.dll
        73a70000 4549be05 Nov 02 09:44:37 2006 C:\Windows\system32\xmllite.dll
        73240000 4654f735 May 24 03:23:49 2007 C:\Windows\system32\WindowsCodecs.dll
        6d7f0000 4549bdf3 Nov 02 09:44:19 2006 C:\Program Files\Common Files\microsoft
shared\ink\tiptsf.dll
        71490000 4549bd24 Nov 02 09:40:52 2006 C:\Windows\system32\dwmapi.dll
        6f630000 4549bcf7 Nov 02 09:40:07 2006 C:\Windows\system32\MLANG.dll
        10000000 45b1bc45 Jan 20 06:52:53 2007 c:\program files\google\googletoolbar1.dll
        70480000 4549bd89 Nov 02 09:42:33 2006 C:\Windows\system32\msi.dll
        77580000 462434a3 Apr 17 03:44:51 2007 C:\Windows\system32\imagehlp.dll
        74ff0000 4549be2f Nov 02 09:45:19 2006 C:\Windows\system32\WINTRUST.dll
        6f510000 4549be32 Nov 02 09:45:22 2006 C:\Windows\system32\WSOCK32.dll
        75a60000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\SXS.DLL
        72460000 4666193b Jun 06 03:17:31 2007 C:\Windows\System32\msxml3.dll
        77030000 4549bdb0 Nov 02 09:43:12 2006 C:\Windows\system32\SETUPAPI.dll
        75ad0000 4549bda8 Nov 02 09:43:04 2006 C:\Windows\system32\SAMLIB.dll
        6e150000 4549bdd9 Nov 02 09:43:53 2006 C:\Windows\System32\ntlanman.dll
        6e830000 4549bd0f Nov 02 09:40:31 2006 C:\Windows\System32\drprov.dll
        6e6a0000 4549bcc7 Nov 02 09:39:19 2006 C:\Windows\System32\davclnt.dll
        71440000 4549bd2c Nov 02 09:41:00 2006 C:\Windows\system32\cscapi.dll
        73c50000 4549bcb0 Nov 02 09:38:56 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.6000.16386_none_87e0cb09378714f1\COMCTL32.dll
        72040000 4549bdc8 Nov 02 09:43:36 2006 C:\Windows\system32\PortableDeviceApi.dll
         2bb0000 453c6a72 Oct 23 08:08:34 2006 C:\Program Files\Common
Files\Adobe\Acrobat\ActiveX\AcroIEHelper.dll
        6e210000 4536eb78 Oct 19 04:05:28 2006
C:\Windows\WinSxS\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.312_none_10b2ee7b9bffc2c7\MSVCR
80.dll
        655e0000 473249c3 Nov 07 23:26:59 2007 C:\Program
Files\Real\RealPlayer\rpbrowserrecordplugin.dll
        76140000 4549bd09 Nov 02 09:40:25 2006 C:\Windows\system32\comdlg32.dll
        7c3a0000 3e77eebb Mar 19 04:14:51 2003 C:\Windows\system32\MSVCP71.dll
        7c340000 3e561eac Feb 21 12:42:20 2003 C:\Windows\system32\MSVCR71.dll
        744e0000 4549bd96 Nov 02 09:42:46 2006 C:\Windows\system32\PROPSYS.dll
        70b20000 4549bde2 Nov 02 09:44:02 2006 C:\Windows\system32\ntshrui.dll
        75610000 4679de70 Jun 21 03:12:00 2007 C:\Windows\system32\slc.dll
         3490000 46f8ab4d Sep 25 07:31:41 2007 C:\Program Files\Java\jre1.6.0_03\bin\ssv.dll
```

```
        75250000 4549bd69 Nov 02 09:42:01 2006 C:\Windows\system32\mswsock.dll
        752c0000 4549be27 Nov 02 09:45:11 2006 C:\Windows\System32\wshtcpip.dll
        752b0000 4549be21 Nov 02 09:45:05 2006 C:\Windows\System32\wship6.dll
        72f40000 4549be1f Nov 02 09:45:03 2006 C:\Windows\System32\winrnr.dll
        76310000 4549be44 Nov 02 09:45:40 2006 C:\Windows\system32\WLDAP32.dll
        72f30000 4549bd3b Nov 02 09:41:15 2006 C:\Windows\system32\napinsp.dll
        72c10000 4549bdc0 Nov 02 09:43:28 2006 C:\Windows\system32\pnrpnsp.dll
        72c40000 4549be1d Nov 02 09:45:01 2006 C:\Windows\system32\wshbth.dll
        6d250000 4722d0fd Oct 27 06:47:41 2007 C:\Windows\system32\mshtml.dll
        6e9e0000 4549bd98 Nov 02 09:42:48 2006 C:\Windows\system32\msls31.dll
        6d600000 470c4d6a Oct 10 04:56:26 2007 C:\Windows\system32\ieapfltr.dll
        75020000 4549bddb Nov 02 09:43:55 2006 C:\Windows\system32\NTMARTA.DLL
        6f590000 4549bd94 Nov 02 09:42:44 2006 C:\Windows\system32\msimtf.dll
        6dc30000 4549bce2 Nov 02 09:39:46 2006 C:\Windows\system32\jscript.dll
        6dd50000 4549bcf9 Nov 02 09:40:09 2006 C:\Windows\system32\iepeers.dll
        6db50000 470c4dea Oct 10 04:58:34 2007 C:\Windows\system32\mshtmled.dll
        6e1d0000 470c4d7f Oct 10 04:56:47 2007 C:\Windows\system32\Dxtrans.dll
        74d00000 4549bcbc Nov 02 09:39:08 2006 C:\Windows\system32\ATL.DLL
        6f070000 4549bcd1 Nov 02 09:39:29 2006 C:\Windows\system32\ddrawex.dll
        6e6d0000 4549bcd0 Nov 02 09:39:28 2006 C:\Windows\system32\DDRAW.dll
        6e890000 4549bccc Nov 02 09:39:24 2006 C:\Windows\system32\DCIMAN32.dll
         5fe0000 4681449e Jun 26 17:53:50 2007 C:\Windows\system32\igdumd32.dll
        6c2c0000 4549bddb Nov 02 09:43:55 2006 C:\Windows\system32\vbscript.dll
        30000000 474375f3 Nov 21 00:04:03 2007 C:\Windows\system32\Macromed\Flash\Flash9e.ocx
        737f0000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\wdmaud.drv
        73870000 4549bd89 Nov 02 09:42:33 2006 C:\Windows\system32\ksuser.dll
        75390000 4549bcdc Nov 02 09:39:40 2006 C:\Windows\system32\AVRT.dll
        74d90000 4549bd03 Nov 02 09:40:19 2006 C:\Windows\system32\MMDevAPI.DLL
        736d0000 4549bcc2 Nov 02 09:39:14 2006 C:\Windows\System32\audioses.dll
        73540000 4549bcc0 Nov 02 09:39:12 2006 C:\Windows\System32\audioeng.dll
        73860000 4549bd2f Nov 02 09:41:03 2006 C:\Windows\system32\msacm32.drv
        73790000 4549bd2e Nov 02 09:41:02 2006 C:\Windows\system32\MSACM32.dll
        736c0000 4549bd27 Nov 02 09:40:55 2006 C:\Windows\system32\miUserNamep.dll
        6f5a0000 4549bd27 Nov 02 09:40:55 2006 C:\Windows\system32\ImgUtil.dll
        6e840000 4549bdb9 Nov 02 09:43:21 2006 C:\Windows\system32\pngfilt.dll
        6db20000 4549bd1d Nov 02 09:40:45 2006 C:\Windows\system32\dssenh.dll
        754f0000 4549bd49 Nov 02 09:41:29 2006 C:\Windows\system32\ncrypt.dll
        754a0000 4549bcb9 Nov 02 09:39:05 2006 C:\Windows\system32\bcrypt.dll
        75330000 4549bcd7 Nov 02 09:39:35 2006 C:\Windows\system32\GPAPI.dll
        6db00000 4549bd28 Nov 02 09:40:56 2006 C:\Windows\system32\cryptnet.dll
        74f10000 4549bcb8 Nov 02 09:39:04 2006 C:\Windows\system32\Cabinet.dll
    SubSystemData:     00000000
    ProcessHeap:       00450000
    ProcessParameters: 004510e0
    WindowTitle:  'C:\Program Files\Internet Explorer\iexplore.exe'
    ImageFile:    'C:\Program Files\Internet Explorer\iexplore.exe'
    CommandLine:  '"C:\Program Files\Internet Explorer\iexplore.exe" '
    DllPath:      'C:\Program Files\Internet
Explorer;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Program Files\Internet
Explorer;;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Program
Files\QuickTime\QTSystem\'
    Environment:  0370db60
        =::=::\
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\UserName\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        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=\\HOME
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
```

```
        Path=C:\Program Files\Internet
Explorer;;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        RNLOG_BASEKEY=Software\RealNetworks\RealPlayer\6.0\Preferences\BrowserRecordPluginLog
        SESSIONNAME=Console
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Users\UserName\AppData\Local\Temp\Low
        TMP=C:\Users\UserName\AppData\Local\Temp\Low
        USERDOMAIN=home
        USERNAME=UserName
        USERPROFILE=C:\Users\UserName
        windir=C:\Windows


        THREAD 837231d0  Cid 05a4.094c  Teb: 7ffdf000 Win32Thread: ff32a290 WAIT: (UserRequest)
UserMode Non-Alertable
            8380e1b0  SynchronizationEvent
            83829b18  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8380fd90       Image:         iexplore.exe
        Wait Start TickCount      34898          Ticks: 8601 (0:00:02:14.176)
        Context Switch Count      3996
        UserTime                  00:00:00.218
        KernelTime                00:00:00.436
        Win32 Start Address iexplore!wWinMainCRTStartup (0x00a22e2d)
        Stack Init 9f2dc000 Current 9f2db8d0 Base 9f2dc000 Limit 9f2d9000 Call 0
        Priority 14 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f2db8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f2db924 81c28c64 nt!KiSwapThread+0x389
        9f2db970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f2dbbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f2dbd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f2dbd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f2dbd64)
        0031e290 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0031e294 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0031e330 761dc4b7 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0031e384 6e46605c USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
        0031e3a4 6e46634e IEUI!CoreSC::Wait+0x49 (FPO: [Non-Fpo])
        0031e3cc 6e466178 IEUI!CoreSC::WaitMessage+0x54 (FPO: [Non-Fpo])
        0031e3d8 6eb5994d IEUI!WaitMessageEx+0x33 (FPO: [Non-Fpo])
        0031e408 6eb4abcc IEFRAME!CBrowserFrame::FrameMessagePump+0x199 (FPO: [Non-Fpo])
        0031e414 6eb4bc3b IEFRAME!BrowserThreadProc+0x3f (FPO: [Non-Fpo])
        0031e438 6eb4bb89 IEFRAME!BrowserNewThreadProc+0x7b (FPO: [Non-Fpo])
        0031f4a8 6eb4ba39 IEFRAME!SHOpenFolderWindow+0x188 (FPO: [Non-Fpo])
        0031f6d8 00a21464 IEFRAME!IEWinMain+0x2d9 (FPO: [Non-Fpo])
        0031fb1c 00a212ff iexplore!wWinMain+0x2c1 (FPO: [Non-Fpo])
        0031fbb0 75f33833 iexplore!_initterm_e+0x1b1 (FPO: [Non-Fpo])
        0031fbbc 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0031fbfc 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 83838b98  Cid 05a4.0964  Teb: 7ffdb000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            8352cd58  SynchronizationTimer
            838306e0  SynchronizationEvent
            837ccb60  SynchronizationEvent
            838934ec  NotificationEvent
            83893208  SynchronizationEvent
            83894280  SynchronizationEvent
            8369a340  SynchronizationEvent
            83876410  SynchronizationEvent
            838b5a50  SynchronizationEvent
            83853220  SynchronizationEvent
            838569b8  SynchronizationEvent
            83862218  SynchronizationEvent
            838a9d88  SynchronizationEvent
            837ee7d0  SynchronizationEvent
            83487c40  SynchronizationEvent
            838119d0  SynchronizationEvent
            836af788  SynchronizationEvent
            8383e290  SynchronizationEvent
            836cab58  SynchronizationEvent
            83481ed8  SynchronizationEvent
            83481bd4  NotificationEvent
            83855ee0  SynchronizationEvent
            837dbe70  SynchronizationEvent
            8361db10  SynchronizationEvent
            835e4220  SynchronizationEvent
            838b6d90  SynchronizationEvent
            83866ed8  SynchronizationEvent
            838b6348  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8380fd90       Image:         iexplore.exe
        Wait Start TickCount      12255          Ticks: 31244 (0:00:08:07.409)
        Context Switch Count      39
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x7744b49a)
        Stack Init a8f50000 Current a8f4f8d0 Base a8f50000 Limit a8f4d000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a8f4f8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8f4f924 81c28c64 nt!KiSwapThread+0x389
        a8f4f970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a8f4fbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a8f4fd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a8f4fd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8f4fd64)
        0260f85c 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0260f860 7744b65b ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0260f9fc 75f33833 ntdll!TppWaiterpThread+0x294 (FPO: [Non-Fpo])
        0260fa08 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0260fa48 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 83813d78  Cid 05a4.0930  Teb: 7ffd9000 Win32Thread: ffbffe98 WAIT: (UserRequest)
UserMode Non-Alertable
            8351e588  SynchronizationEvent
            8354cc70  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8380fd90       Image:         iexplore.exe
        Wait Start TickCount      11771          Ticks: 31728 (0:00:08:14.959)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address msvcrt!_endthreadex (0x7628639b)
        Stack Init a8f84000 Current a8f838d0 Base a8f84000 Limit a8f81000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a8f838e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8f83924 81c28c64 nt!KiSwapThread+0x389
        a8f83970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a8f83bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a8f83d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a8f83d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8f83d64)
        02affbf8 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        02affbfc 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        02affc98 761dc4b7 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        02affcec 6e46605c USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
        02affd0c 6e469441 IEUI!CoreSC::Wait+0x49 (FPO: [Non-Fpo])
        02affd40 6e469982 IEUI!CoreSC::xwProcessNL+0xa4 (FPO: [Non-Fpo])
        02affd60 6e4698e0 IEUI!GetMessageExA+0x44 (FPO: [Non-Fpo])
        02affdb4 762862b6 IEUI!ResourceManager::SharedThreadProc+0xb6 (FPO: [Non-Fpo])
        02affdec 762863de msvcrt!_endthreadex+0x44 (FPO: [Non-Fpo])
        02affdf4 75f33833 msvcrt!_endthreadex+0xce (FPO: [Non-Fpo])
        02affe00 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        02affe40 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 83809598  Cid 05a4.0968  Teb: 7ffd8000 Win32Thread: fed0e008 WAIT: (WrUserRequest)
UserMode Non-Alertable
            8381d2e0  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8380fd90       Image:         iexplore.exe
        Wait Start TickCount      43497          Ticks: 2 (0:00:00:00.031)
        Context Switch Count      25487
        UserTime                  00:00:00.904
        KernelTime                00:00:00.530
        Win32 Start Address IEFRAME!CTabWindow::_TabWindowThreadProc (0x6eb3e424)
        Stack Init a6893000 Current a6892c10 Base a6893000 Limit a6890000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a6892c28 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a6892c64 81c293a7 nt!KiSwapThread+0x389
        a6892cc0 8cedb8ed nt!KeWaitForSingleObject+0x414
        a6892d1c 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        a6892d38 8ced573c win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        a6892d4c 8ced5759 win32k!xxxRealWaitMessageEx+0x12 (FPO: [Non-Fpo])
        a6892d5c 81c8caaa win32k!NtUserWaitMessage+0x14 (FPO: [Non-Fpo])
        a6892d5c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a6892d64)
        0348fa60 761db5bc ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0348fa64 6eb3f324 USER32!NtUserWaitMessage+0xc (FPO: [Non-Fpo])
        0348fac8 75f33833 IEFRAME!CTabWindow::_TabWindowThreadProc+0x2d0 (FPO: [Non-Fpo])
        0348fad4 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0348fb14 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 838174d8  Cid 05a4.08b0  Teb: 7ffd7000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            838653d0  NotificationEvent
            83817560  NotificationTimer
        IRP List:
            838df428: (0006,0100) Flags: 00060070  Mdl: 00000000
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8380fd90       Image:         iexplore.exe
        Wait Start TickCount      12646          Ticks: 30853 (0:00:08:01.309)
        Context Switch Count      131
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address WININET!ICAsyncThread::SelectThreadWrapper (0x76042a8b)
        Stack Init 9f718000 Current 9f717c38 Base 9f718000 Limit 9f715000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f717c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f717c8c 81c293a7 nt!KiSwapThread+0x389
        9f717ce8 81df5057 nt!KeWaitForSingleObject+0x414
        9f717d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        9f717d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f717d64)
        048ff394 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        048ff398 75253b28 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        048ff3d8 75252690 mswsock!SockWaitForSingleObject+0x19f (FPO: [Non-Fpo])
        048ff4c4 75fe3781 mswsock!WSPSelect+0x38c (FPO: [Non-Fpo])
        048ff540 7604611d ws2_32!select+0x456 (FPO: [Non-Fpo])
        048ff898 76042a98 WININET!ICAsyncThread::SelectThread+0x242 (FPO: [Non-Fpo])
        048ff8a0 75f33833 WININET!ICAsyncThread::SelectThreadWrapper+0xd (FPO: [Non-Fpo])
        048ff8ac 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        048ff8ec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 838633f8  Cid 05a4.059c  Teb: 7ffd4000 Win32Thread: fedf49d0 WAIT: (UserRequest)
UserMode Non-Alertable
            8382f5f8  SynchronizationEvent
            83863480  NotificationTimer
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8380fd90       Image:         iexplore.exe
        Wait Start TickCount      12274          Ticks: 31225 (0:00:08:07.113)
        Context Switch Count      50
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address mshtml!CExecFT::StaticThreadProc (0x6d26da47)
        Stack Init 9f69b000 Current 9f69ac38 Base 9f69b000 Limit 9f698000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f69ac50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f69ac8c 81c293a7 nt!KiSwapThread+0x389
        9f69ace8 81df5057 nt!KeWaitForSingleObject+0x414
        9f69ad50 81c8caaa nt!NtWaitForSingleObject+0xbe
        9f69ad50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f69ad64)
        04f3f98c 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        04f3f990 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        04f3fa00 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        04f3fa14 6d2ef525 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        04f3fa2c 6d2e6c1a mshtml!CDwnTaskExec::ThreadExec+0x127 (FPO: [Non-Fpo])
        04f3fa38 6d26da54 mshtml!CExecFT::ThreadProc+0x3c (FPO: [Non-Fpo])
        04f3fa40 75f33833 mshtml!CExecFT::StaticThreadProc+0xd (FPO: [Non-Fpo])
        04f3fa4c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        04f3fa8c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 83868308  Cid 05a4.02ac  Teb: 7ffd3000 Win32Thread: fedfdcf0 WAIT: (UserRequest)
UserMode Non-Alertable
            8480c5e8  SynchronizationEvent
            83868390  NotificationTimer
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8380fd90       Image:         iexplore.exe
        Wait Start TickCount      12293          Ticks: 31206 (0:00:08:06.816)
        Context Switch Count      91
        UserTime                  00:00:00.078
        KernelTime                00:00:00.062
        Win32 Start Address mshtml!CExecFT::StaticThreadProc (0x6d26da47)
        Stack Init 9f69f000 Current 9f69ec38 Base 9f69f000 Limit 9f69c000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f69ec50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f69ec8c 81c293a7 nt!KiSwapThread+0x389
        9f69ece8 81df5057 nt!KeWaitForSingleObject+0x414
        9f69ed50 81c8caaa nt!NtWaitForSingleObject+0xbe
        9f69ed50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f69ed64)
        0549f9f0 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0549f9f4 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0549fa64 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        0549fa78 6d2ef525 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0549fa90 6d2e6c1a mshtml!CDwnTaskExec::ThreadExec+0x127 (FPO: [Non-Fpo])
        0549fa9c 6d26da54 mshtml!CExecFT::ThreadProc+0x3c (FPO: [Non-Fpo])
        0549faa4 75f33833 mshtml!CExecFT::StaticThreadProc+0xd (FPO: [Non-Fpo])
        0549fab0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0549faf0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 83863030  Cid 05a4.046c  Teb: 7ffaf000 Win32Thread: ff246468 WAIT: (WrQueue)
UserMode Alertable
            83809c70  QueueObject
        IRP List:
            83853008: (0006,01d8) Flags: 00060000  Mdl: 00000000
            83894008: (0006,01d8) Flags: 00060000  Mdl: 00000000
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8380fd90       Image:         iexplore.exe
        Wait Start TickCount      12293          Ticks: 31206 (0:00:08:06.816)
        Context Switch Count      357
        UserTime                  00:00:00.187
        KernelTime                00:00:00.156
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init 9f6a3000 Current 9f6a2bc8 Base 9f6a3000 Limit 9f6a0000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f6a2be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f6a2c1c 81cad431 nt!KiSwapThread+0x389
        9f6a2c68 81d8b982 nt!KeRemoveQueueEx+0x568
        9f6a2cc0 81c7a036 nt!IoRemoveIoCompletion+0x23
        9f6a2d54 81c8caaa nt!NtWaitForWorkViaWorkerFactory+0x1a1
        9f6a2d54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f6a2d64)
        059bfaf0 77490850 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        059bfaf4 7749a1b4 ntdll!NtWaitForWorkViaWorkerFactory+0xc (FPO: [2,0,0])
        059bfc1c 75f33833 ntdll!TppWorkerThread+0x1f6 (FPO: [Non-Fpo])
        059bfc28 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        059bfc68 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 83744c30  Cid 05a4.0870  Teb: 7ffaa000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            9e1e0720  QueueObject
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8380fd90       Image:         iexplore.exe
        Wait Start TickCount      11899          Ticks: 31600 (0:00:08:12.963)
        Context Switch Count      99
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdmaud!mxdMessageThreadProc (0x737f42d7)
        Stack Init 9f720000 Current 9f71fbc8 Base 9f720000 Limit 9f71d000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f71fbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f71fc1c 81cad431 nt!KiSwapThread+0x389
        9f71fc6c 81d8b982 nt!KeRemoveQueueEx+0x568
        9f71fcc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        9f71fd48 81c8caaa nt!NtRemoveIoCompletion+0x106
        9f71fd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f71fd64)
        08c1fe24 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        08c1fe28 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        08c1fe54 737f4354 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        08c1fe84 75f33833 wdmaud!mxdMessageThreadProc+0x7d (FPO: [Non-Fpo])
        08c1fe90 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        08c1fed0 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 83744978  Cid 05a4.0998  Teb: 7ffa9000 Win32Thread: fe89da40 WAIT: (WrUserRequest)
UserMode Non-Alertable
            8382fc68  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8380fd90       Image:         iexplore.exe
        Wait Start TickCount      11892          Ticks: 31607 (0:00:08:13.072)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wdmaud!CTaskThread::TaskThreadProc (0x737f8675)
        Stack Init a8ff8000 Current a8ff7b68 Base a8ff8000 Limit a8ff5000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a8ff7b80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8ff7bbc 81c293a7 nt!KiSwapThread+0x389
        a8ff7c18 8cedb8ed nt!KeWaitForSingleObject+0x414
        a8ff7c74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        a8ff7c90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        a8ff7ce8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        a8ff7d4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        a8ff7d4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8ff7d64)
        08f0fe10 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        08f0fe14 761e19cd USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        08f0fe30 737f8712 USER32!GetMessageW+0x33 (FPO: [Non-Fpo])
        08f0fe70 75f33833 wdmaud!CTaskThread::TaskThreadProc+0x9d (FPO: [Non-Fpo])
        08f0fe7c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        08f0febc 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 83744490  Cid 05a4.099c  Teb: 7ffa8000 Win32Thread: ff34ca08 WAIT: (UserRequest)
UserMode Non-Alertable
            8382fc98  SynchronizationEvent
            8382f688  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8380fd90       Image:         iexplore.exe
        Wait Start TickCount      12176          Ticks: 31323 (0:00:08:08.641)
        Context Switch Count      468
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address wdmaud!CWorker::_StaticThreadProc (0x737f8544)
        Stack Init a691f000 Current a691e8d0 Base a691f000 Limit a691c000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a691e8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a691e924 81c28c64 nt!KiSwapThread+0x389
        a691e970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a691ebfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a691ed48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a691ed48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a691ed64)
        0904fd6c 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0904fd70 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0904fe0c 737f5111 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0904fe44 737f855c wdmaud!CWorker::_ThreadProc+0x5e (FPO: [Non-Fpo])
        0904fe50 75f33833 wdmaud!CWorker::_StaticThreadProc+0x18 (FPO: [Non-Fpo])
        0904fe5c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0904fe9c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 8383ea38  Cid 05a4.0b5c  Teb: 7ffa7000 Win32Thread: fecf5008 WAIT: (UserRequest)
UserMode Non-Alertable
            834b0288  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8380fd90       Image:         iexplore.exe
        Wait Start TickCount      12202          Ticks: 31297 (0:00:08:08.236)
        Context Switch Count      427
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address mshtml!CExecFT::StaticThreadProc (0x6d26da47)
        Stack Init 9f738000 Current 9f737c38 Base 9f738000 Limit 9f735000 Call 0
        Priority 13 BasePriority 8 PriorityDecrement 4 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f737c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f737c8c 81c293a7 nt!KiSwapThread+0x389
        9f737ce8 81df5057 nt!KeWaitForSingleObject+0x414
        9f737d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        9f737d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f737d64)
        098cfdc0 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        098cfdc4 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        098cfe34 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        098cfe48 6d34960c kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        098cfe6c 6d2e6c1a mshtml!CTimerMan::ThreadExec+0x90 (FPO: [Non-Fpo])
        098cfe78 6d26da54 mshtml!CExecFT::ThreadProc+0x3c (FPO: [Non-Fpo])
        098cfe80 75f33833 mshtml!CExecFT::StaticThreadProc+0xd (FPO: [Non-Fpo])
        098cfe8c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        098cfecc 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 838a8548  Cid 05a4.0c74  Teb: 7ffa6000 Win32Thread: fe89c468 WAIT: (WrUserRequest)
UserMode Non-Alertable
            838b4d80  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8380fd90       Image:         iexplore.exe
        Wait Start TickCount      12176          Ticks: 31323 (0:00:08:08.641)
        Context Switch Count      26
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address WINMM!mciwindow (0x738c1385)
        Stack Init a8f44000 Current a8f43b68 Base a8f44000 Limit a8f41000 Call 0
        Priority 13 BasePriority 10 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a8f43b80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8f43bbc 81c293a7 nt!KiSwapThread+0x389
        a8f43c18 8cedb8ed nt!KeWaitForSingleObject+0x414
        a8f43c74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        a8f43c90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        a8f43ce8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        a8f43d4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        a8f43d4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8f43d64)
        03e8fc48 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        03e8fc4c 761d3ad1 USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        03e8fc70 738c1404 USER32!GetMessageA+0x8a (FPO: [Non-Fpo])
        03e8fca8 75f33833 WINMM!mciwindow+0x102 (FPO: [Non-Fpo])
        03e8fcb4 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        03e8fcf4 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 83499d78  Cid 05a4.0578  Teb: 7ffab000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            83866e18  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8380fd90       Image:         iexplore.exe
        Wait Start TickCount      12267          Ticks: 31232 (0:00:08:07.222)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address Flash9e!DllUnregisterServer (0x3010ebf1)
        Stack Init a8f88000 Current a8f87c38 Base a8f88000 Limit a8f85000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a8f87c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8f87c8c 81c293a7 nt!KiSwapThread+0x389
        a8f87ce8 81df5057 nt!KeWaitForSingleObject+0x414
        a8f87d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a8f87d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8f87d64)
        0893fdbc 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0893fdc0 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0893fe30 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        0893fe44 3010ebca kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0893fe84 7746a9bd Flash9e!DllUnregisterServer+0x5594f
        0893fec4 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 83887368  Cid 05a4.0588  Teb: 7ffa5000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            834bbb88  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8380fd90       Image:         iexplore.exe
        Wait Start TickCount      12267          Ticks: 31232 (0:00:08:07.222)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address Flash9e!DllUnregisterServer (0x3010ebf1)
        Stack Init a8fd8000 Current a8fd7c38 Base a8fd8000 Limit a8fd5000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a8fd7c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8fd7c8c 81c293a7 nt!KiSwapThread+0x389
        a8fd7ce8 81df5057 nt!KeWaitForSingleObject+0x414
        a8fd7d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a8fd7d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8fd7d64)
        08adf864 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        08adf868 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        08adf8d8 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        08adf8ec 3010ebca kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        08adf92c 7746a9bd Flash9e!DllUnregisterServer+0x5594f
        08adf96c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 83702d78  Cid 05a4.06f0  Teb: 7ffdc000 Win32Thread: fe7941c0 WAIT: (WrQueue)
UserMode Non-Alertable
            837e5428  QueueObject
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            8380fd90       Image:         iexplore.exe
        Wait Start TickCount      37337          Ticks: 6162 (0:00:01:36.127)
        Context Switch Count      8
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init a09d1000 Current a09d0bc8 Base a09d1000 Limit a09ce000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a09d0be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a09d0c1c 81cad431 nt!KiSwapThread+0x389
        a09d0c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a09d0cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a09d0d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a09d0d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a09d0d64)
        03c2fdf8 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        03c2fdfc 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        03c2fe28 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        03c2fe64 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        03c2fed0 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        03c2fedc 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        03c2ff04 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        03c2ff10 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        03c2ff1c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        03c2ff5c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Realplay process

```
PROCESS 835ff588  SessionId: 1  Cid: 0920    Peb: 7ffdd000  ParentCid: 05a4
    DirBase: 29a01180  ObjectTable: 00000000  HandleCount:   0.
    Image: realplay.exe
    VadRoot 00000000 Vads 0 Clone 0 Private 0. Modified 0. Locked 0.
    DeviceMap a7766db8
    Token                             aa45e910
    ElapsedTime                       00:08:14.526
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.015
    QuotaPoolUsage[PagedPool]         0
    QuotaPoolUsage[NonPagedPool]      0
    Working Set Sizes (now,min,max)  (7, 50, 345) (28KB, 200KB, 1380KB)
    PeakWorkingSetSize                21
    VirtualSize                       2 Mb
    PeakVirtualSize                   2 Mb
    PageFaultCount                    14
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      0

    Setting context for this process...
.process /p /r ffffffff835ff588

    !peb
PEB at 7ffdd000


No active threads
```

FlashUtil9e process

```
PROCESS 838806e8  SessionId: 1  Cid: 0ab8    Peb: 7ffdf000  ParentCid: 02ec
    DirBase: 29a016c0  ObjectTable: aa57b7d8  HandleCount:  77.
    Image: FlashUtil9e.exe
    VadRoot 838a3af8 Vads 61 Clone 0 Private 235. Modified 0. Locked 0.
    DeviceMap a7766db8
    Token                             aa5d8ca0
    ElapsedTime                       00:08:07.130
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         84456
    QuotaPoolUsage[NonPagedPool]      2928
    Working Set Sizes (now,min,max)  (1098, 50, 345) (4392KB, 200KB, 1380KB)
    PeakWorkingSetSize                1106
    VirtualSize                       42 Mb
    PeakVirtualSize                   44 Mb
    PageFaultCount                    1169
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      339

    Setting context for this process...
.process /p /r ffffffff838806e8

    !peb
PEB at 7ffdf000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00400000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00261920 . 00278a28
    Ldr.InLoadOrderModuleList:           002618a0 . 00278a18
    Ldr.InMemoryOrderModuleList:         002618a8 . 00278a20
            Base TimeStamp                     Module
          400000 47437368 Nov 20 23:53:12 2007 C:\Windows\system32\Macromed\Flash\FlashUtil9e.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        753f0000 4549bde4 Nov 02 09:44:04 2006 C:\Windows\system32\VERSION.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        76020000 470c4e1e Oct 10 04:59:26 2007 C:\Windows\system32\WININET.dll
        763b0000 4549bdb9 Nov 02 09:43:21 2006 C:\Windows\system32\SHLWAPI.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        76010000 4549ad42 Nov 02 08:33:06 2006 C:\Windows\system32\Normaliz.dll
        76360000 4549bcfb Nov 02 09:40:11 2006 C:\Windows\system32\iertutil.dll
        75650000 45b96fde Jan 26 03:05:02 2007 C:\Windows\system32\CRYPT32.dll
        75820000 4549bd41 Nov 02 09:41:21 2006 C:\Windows\system32\MSASN1.dll
        75ba0000 4549bde2 Nov 02 09:44:02 2006 C:\Windows\system32\USERENV.dll
        75b80000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\Secur32.dll
        76560000 4681c95d Jun 27 03:20:13 2007 C:\Windows\system32\SHELL32.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        74aa0000 4549bd09 Nov 02 09:40:25 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_5d07289e07e1d100\comctl32.dll
        746d0000 4549bde7 Nov 02 09:44:07 2006 C:\Windows\system32\uxtheme.dll
        773a0000 4549bce9 Nov 02 09:39:53 2006 C:\Windows\system32\CLBCatQ.DLL
        75350000 4549bdae Nov 02 09:43:10 2006 C:\Windows\system32\rsaenh.dll
        75a60000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\SXS.DLL
```

```
    SubSystemData:     00000000
    ProcessHeap:       00260000
    ProcessParameters: 002610e0
    WindowTitle:  'C:\Windows\system32\Macromed\Flash\FlashUtil9e.exe'
    ImageFile:    'C:\Windows\system32\Macromed\Flash\FlashUtil9e.exe'
    CommandLine:  'C:\Windows\system32\Macromed\Flash\FlashUtil9e.exe -Embedding'
    DllPath:
'C:\Windows\system32\Macromed\Flash;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Program
Files\Internet Explorer;;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Program
Files\QuickTime\QTSystem\'
    Environment:  002607e8
        =::=::\
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\UserName\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        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=\\HOME
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Program Files\Internet
Explorer;;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        SESSIONNAME=Console
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Users\UserName\AppData\Local\Temp
        TMP=C:\Users\UserName\AppData\Local\Temp
        USERDOMAIN=home
        USERNAME=UserName
        USERPROFILE=C:\Users\UserName
        windir=C:\Windows
```

```
        THREAD 83855598  Cid 0ab8.0620  Teb: 7ffde000 Win32Thread: feceec80 WAIT: (WrUserRequest)
UserMode Non-Alertable
            83855440  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            838806e8       Image:         FlashUtil9e.exe
        Wait Start TickCount      35414          Ticks: 8085 (0:00:02:06.126)
        Context Switch Count      55
        UserTime                  00:00:00.031
        KernelTime                00:00:00.015
        Win32 Start Address FlashUtil9e (0x00407e33)
        Stack Init 9e9a0000 Current 9e99fb68 Base 9e9a0000 Limit 9e99d000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9e99fb80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e99fbbc 81c293a7 nt!KiSwapThread+0x389
        9e99fc18 8cedb8ed nt!KeWaitForSingleObject+0x414
        9e99fc74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        9e99fc90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        9e99fce8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        9e99fd4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        9e99fd4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9e99fd64)
        0012ff14 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0012ff18 761d3ad1 USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        0012ff3c 00407965 USER32!GetMessageA+0x8a (FPO: [Non-Fpo])
        0012ff7c 00407e65 FlashUtil9e+0x7965
        0012ffa0 75f33833 FlashUtil9e+0x7e65
        0012ffac 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0012ffec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 8369a030  Cid 0ab8.057c  Teb: 7ffdd000 Win32Thread: feceee98 WAIT: (WrQueue)
UserMode Non-Alertable
            83746138  QueueObject
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            838806e8       Image:         FlashUtil9e.exe
        Wait Start TickCount      37337          Ticks: 6162 (0:00:01:36.127)
        Context Switch Count      29
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init a6857000 Current a6856bc8 Base a6857000 Limit a6854000 Call 0
        Priority 13 BasePriority 8 PriorityDecrement 4 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a6856be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a6856c1c 81cad431 nt!KiSwapThread+0x389
        a6856c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a6856cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a6856d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a6856d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a6856d64)
        0121fe88 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0121fe8c 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        0121feb8 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        0121fef4 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        0121ff60 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        0121ff6c 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        0121ff94 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        0121ffa0 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        0121ffac 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0121ffec 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Notepad process

```
PROCESS 838e25a0  SessionId: 1  Cid: 0378    Peb: 7ffd8000  ParentCid: 0b90
    DirBase: 29a01400  ObjectTable: 9f5e67a0  HandleCount:  52.
    Image: notepad.exe
    VadRoot 838ed688 Vads 53 Clone 0 Private 241. Modified 221. Locked 0.
    DeviceMap a7766db8
    Token                             9f5e3928
    ElapsedTime                       00:07:59.971
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         79896
    QuotaPoolUsage[NonPagedPool]      2544
    Working Set Sizes (now,min,max)  (925, 50, 345) (3700KB, 200KB, 1380KB)
    PeakWorkingSetSize                1812
    VirtualSize                       39 Mb
    PeakVirtualSize                   47 Mb
    PageFaultCount                    1855
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      509

    Setting context for this process...
.process /p /r ffffffff838e25a0

    !peb
PEB at 7ffd8000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00360000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 001917e0 . 001a8c40
    Ldr.InLoadOrderModuleList:           00191760 . 001a8c30
    Ldr.InMemoryOrderModuleList:         00191768 . 001a8c38
            Base TimeStamp                     Module
          360000 4549b0be Nov 02 08:47:58 2006 C:\Windows\System32\notepad.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        76140000 4549bd09 Nov 02 09:40:25 2006 C:\Windows\system32\COMDLG32.dll
        763b0000 4549bdb9 Nov 02 09:43:21 2006 C:\Windows\system32\SHLWAPI.dll
        74aa0000 4549bd09 Nov 02 09:40:25 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_5d07289e07e1d100\COMCTL32.dll
        76560000 4681c95d Jun 27 03:20:13 2007 C:\Windows\system32\SHELL32.dll
        715a0000 4549be2a Nov 02 09:45:14 2006 C:\Windows\System32\WINSPOOL.DRV
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        746d0000 4549bde7 Nov 02 09:44:07 2006 C:\Windows\System32\uxtheme.dll
    SubSystemData:     00000000
    ProcessHeap:       00190000
    ProcessParameters: 00191010
    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;C:\Program Files\QuickTime\QTSystem\'
    Environment:  001907e8
        =::=::\
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\UserName\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        HOMEDRIVE=C:
        HOMEPATH=\Users\UserName
        LOCALAPPDATA=C:\Users\UserName\AppData\Local
        LOGONSERVER=\\HOME
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        SESSIONNAME=Console
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Users\UserName\AppData\Local\Temp
        TMP=C:\Users\UserName\AppData\Local\Temp
        USERDOMAIN=home
        USERNAME=UserName
        USERPROFILE=C:\Users\UserName
        windir=C:\Windows


        THREAD 838edd78  Cid 0378.0d3c  Teb: 7ffdf000 Win32Thread: fed7e848 WAIT: (WrUserRequest)
UserMode Non-Alertable
            838c84a0  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            838e25a0       Image:         notepad.exe
        Wait Start TickCount      12967          Ticks: 30532 (0:00:07:56.302)
        Context Switch Count      490
        UserTime                  00:00:00.000
        KernelTime                00:00:00.109
        Win32 Start Address notepad!WinMainCRTStartup (0x003631f8)
        Stack Init a691b000 Current a691ab68 Base a691b000 Limit a6918000 Call 0
        Priority 12 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a691ab80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a691abbc 81c293a7 nt!KiSwapThread+0x389
        a691ac18 8cedb8ed nt!KeWaitForSingleObject+0x414
        a691ac74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        a691ac90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        a691ace8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        a691ad4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        a691ad4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a691ad64)
        0006f6d0 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0006f6d4 761e19cd USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        0006f6f0 0036149c USER32!GetMessageW+0x33 (FPO: [Non-Fpo])
        0006f730 00361971 notepad!WinMain+0xec (FPO: [Non-Fpo])
        0006f7c0 75f33833 notepad!_initterm_e+0x1a1 (FPO: [Non-Fpo])
        0006f7cc 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0006f80c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Wmpnscfg process

```
PROCESS 83862d90  SessionId: 1  Cid: 0de8    Peb: 7ffd3000  ParentCid: 0388
    DirBase: 29a01460  ObjectTable: aa487af8  HandleCount: 106.
    Image: wmpnscfg.exe
    VadRoot 8395d878 Vads 72 Clone 0 Private 300. Modified 4. Locked 0.
    DeviceMap a7766db8
    Token                             a9be7910
    ElapsedTime                       00:07:37.691
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.015
    QuotaPoolUsage[PagedPool]         63560
    QuotaPoolUsage[NonPagedPool]      3456
    Working Set Sizes (now,min,max)  (1211, 50, 345) (4844KB, 200KB, 1380KB)
    PeakWorkingSetSize                1217
    VirtualSize                       33 Mb
    PeakVirtualSize                   38 Mb
    PageFaultCount                    1304
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      439

    Setting context for this process...
.process /p /r ffffffff83862d90

    !peb
PEB at 7ffd3000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00420000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 001c1898 . 001d9480
    Ldr.InLoadOrderModuleList:           001c1818 . 001d9630
    Ldr.InMemoryOrderModuleList:         001c1820 . 001d9638
            Base TimeStamp                     Module
          420000 4549b53f Nov 02 09:07:11 2006 C:\Program Files\Windows Media Player\WMPNSCFG.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        73d70000 4549bcaf Nov 02 09:38:55 2006
C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.0.6000.16386_none_9ea0ac9ec96e71
27\gdiplus.dll
        763b0000 4549bdb9 Nov 02 09:43:21 2006 C:\Windows\system32\SHLWAPI.dll
        75b80000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\Secur32.dll
        75840000 4549bd53 Nov 02 09:41:39 2006 C:\Windows\system32\NETAPI32.dll
        75ce0000 4549bd99 Nov 02 09:42:49 2006 C:\Windows\system32\PSAPI.DLL
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        74aa0000 4549bd09 Nov 02 09:40:25 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_5d07289e07e1d100\comctl32.dll
        746d0000 4549bde7 Nov 02 09:44:07 2006 C:\Windows\system32\uxtheme.dll
        773a0000 4549bce9 Nov 02 09:39:53 2006 C:\Windows\system32\CLBCatQ.DLL
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        75350000 4549bdae Nov 02 09:43:10 2006 C:\Windows\system32\rsaenh.dll
```

```
        6e2c0000 4549be7a Nov 02 09:46:34 2006 C:\Program Files\Windows Media Player\wmpnssci.dll
        75020000 4549bddb Nov 02 09:43:55 2006 C:\Windows\system32\NTMARTA.DLL
        76310000 4549be44 Nov 02 09:45:40 2006 C:\Windows\system32\WLDAP32.dll
        75fe0000 4549be0e Nov 02 09:44:46 2006 C:\Windows\system32\WS2_32.dll
        77550000 4549bdc7 Nov 02 09:43:35 2006 C:\Windows\system32\NSI.dll
        75ad0000 4549bda8 Nov 02 09:43:04 2006 C:\Windows\system32\SAMLIB.dll
    SubSystemData:     00000000
    ProcessHeap:       001c0000
    ProcessParameters: 001c1060
    WindowTitle:  'C:\Program Files\Windows Media Player\WMPNSCFG.exe'
    ImageFile:    'C:\Program Files\Windows Media Player\WMPNSCFG.exe'
    CommandLine:  '"C:\Program Files\Windows Media Player\WMPNSCFG.exe" '
    DllPath:      'C:\Program Files\Windows Media
Player;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Program Files\Windows Media
Player;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Program
Files\QuickTime\QTSystem\'
    Environment:  001c07e8
        =::=::\
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\UserName\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        HOMEDRIVE=C:
        HOMEPATH=\Users\UserName
        LOCALAPPDATA=C:\Users\UserName\AppData\Local
        LOGONSERVER=\\HOME
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Program Files\Windows Media
Player;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Program Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        SESSIONNAME=Console
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Users\UserName\AppData\Local\Temp
        TMP=C:\Users\UserName\AppData\Local\Temp
        USERDOMAIN=home
        USERNAME=UserName
        USERPROFILE=C:\Users\UserName
        windir=C:\Windows
```

```
        THREAD 839f0380  Cid 0de8.0c34  Teb: 7ffdf000 Win32Thread: fe9838c0 WAIT: (WrUserRequest)
UserMode Non-Alertable
            839301d8  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            83862d90       Image:         wmpnscfg.exe
        Wait Start TickCount      37306          Ticks: 6193 (0:00:01:36.611)
        Context Switch Count      121
        UserTime                  00:00:00.031
        KernelTime                00:00:00.000
        Win32 Start Address WMPNSCFG!wWinMainCRTStartup (0x004317a1)
        Stack Init a1e3a000 Current a1e39b68 Base a1e3a000 Limit a1e37000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a1e39b80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1e39bbc 81c293a7 nt!KiSwapThread+0x389
        a1e39c18 8cedb8ed nt!KeWaitForSingleObject+0x414
        a1e39c74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        a1e39c90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        a1e39ce8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        a1e39d4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        a1e39d4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1e39d64)
        000cf300 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        000cf304 761e19cd USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        000cf320 004237a5 USER32!GetMessageW+0x33 (FPO: [Non-Fpo])
        000cf34c 00426f1f WMPNSCFG!WTL::CMessageLoop::Run+0x4f (FPO: [Non-Fpo])
        000cf844 0043163c WMPNSCFG!wWinMain+0x765 (FPO: [Non-Fpo])
        000cf8d8 75f33833 WMPNSCFG!_initterm_e+0x1b1 (FPO: [Non-Fpo])
        000cf8e4 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        000cf924 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 83968880  Cid 0de8.0ad4  Teb: 7ffde000 Win32Thread: fe96ee98 WAIT: (UserRequest)
UserMode Non-Alertable
            83950a18  NotificationEvent
            83862b70  SynchronizationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            83862d90       Image:         wmpnscfg.exe
        Wait Start TickCount      14165          Ticks: 29334 (0:00:07:37.613)
        Context Switch Count      46
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address gdiplus!BackgroundThreadProc (0x73d81909)
        Stack Init a68e7000 Current a68e68d0 Base a68e7000 Limit a68e4000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a68e68e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a68e6924 81c28c64 nt!KiSwapThread+0x389
        a68e6970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a68e6bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a68e6d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a68e6d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a68e6d64)
        00fff9cc 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00fff9d0 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00fffa6c 761dc4b7 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        00fffac0 761d8b83 USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
        00fffadc 73d81965 USER32!MsgWaitForMultipleObjects+0x1f (FPO: [Non-Fpo])
        00fffb28 75f33833 gdiplus!BackgroundThreadProc+0x59 (FPO: [Non-Fpo])
        00fffb34 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00fffb74 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 839f2d78  Cid 0de8.0ee0  Teb: 7ffdb000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            83954af0  SynchronizationEvent
            839f2e00  NotificationTimer
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            83862d90       Image:         wmpnscfg.exe
        Wait Start TickCount      33396          Ticks: 10103 (0:00:02:37.607)
        Context Switch Count      6
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ole32!CRpcThreadCache::RpcWorkerThreadEntry (0x7644fc53)
        Stack Init a693b000 Current a693ac38 Base a693b000 Limit a6938000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a693ac50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a693ac8c 81c293a7 nt!KiSwapThread+0x389
        a693ace8 81df5057 nt!KeWaitForSingleObject+0x414
        a693ad50 81c8caaa nt!NtWaitForSingleObject+0xbe
        a693ad50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a693ad64)
        0104fd24 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0104fd28 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0104fd98 75f37742 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        0104fdac 76455251 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0104fdc8 76422104 ole32!CDllHost::MTAWorkerLoop+0x2b (FPO: [Non-Fpo])
        0104fde8 764524ce ole32!CDllHost::WorkerThread+0xc7 (FPO: [Non-Fpo])
        0104fdf0 7644fc0d ole32!DLLHostThreadEntry+0xd (FPO: [Non-Fpo])
        0104fe0c 7644fc73 ole32!CRpcThread::WorkerLoop+0x26 (FPO: [Non-Fpo])
        0104fe18 75f33833 ole32!CRpcThreadCache::RpcWorkerThreadEntry+0x20 (FPO: [Non-Fpo])
        0104fe24 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0104fe64 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 839f2808  Cid 0de8.0840  Teb: 7ffd9000 Win32Thread: fe9b5890 WAIT: (UserRequest)
UserMode Non-Alertable
            83481e20  SynchronizationEvent
            83481e50  SynchronizationEvent
            838bf468  NotificationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            83862d90       Image:         wmpnscfg.exe
        Wait Start TickCount      14397          Ticks: 29102 (0:00:07:33.994)
        Context Switch Count      86
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address wmpnssci!ATL::CWorkerThread<ATL::Win32ThreadTraits>::_WorkerThreadProc
(0x6e2ce843)
        Stack Init a687b000 Current a687a8d0 Base a687b000 Limit a6878000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a687a8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a687a924 81c28c64 nt!KiSwapThread+0x389
        a687a970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a687abfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a687ad48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a687ad48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a687ad64)
        012cf8e4 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        012cf8e8 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        012cf984 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        012cf9a0 6e2ce5ee kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        012cfcd0 6e2ce85b
wmpnssci!ATL::CWorkerThread<ATL::Win32ThreadTraits>::WorkerThreadProc+0x9f (FPO: [Non-Fpo])
        012cfcf8 75f33833
wmpnssci!ATL::CWorkerThread<ATL::Win32ThreadTraits>::_WorkerThreadProc+0x18 (FPO: [Non-Fpo])
        012cfd04 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        012cfd44 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 839f2550  Cid 0de8.0e68  Teb: 7ffd8000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            83963b80  SynchronizationEvent
            8371f368  SynchronizationEvent
            8388dac0  NotificationEvent
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            83862d90       Image:         wmpnscfg.exe
        Wait Start TickCount      14166          Ticks: 29333 (0:00:07:37.597)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address WMPNSCFG!ATL::CWorkerThread<ATL::Win32ThreadTraits>::_WorkerThreadProc
(0x00428e99)
        Stack Init a692b000 Current a692a8d0 Base a692b000 Limit a6928000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a692a8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a692a924 81c28c64 nt!KiSwapThread+0x389
        a692a970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a692abfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a692ad48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a692ad48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a692ad64)
        0143f4c0 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0143f4c4 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0143f560 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        0143f57c 004289f2 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0143f8ac 00428eb1
WMPNSCFG!ATL::CWorkerThread<ATL::Win32ThreadTraits>::WorkerThreadProc+0x9f (FPO: [Non-Fpo])
        0143f8d4 75f33833
WMPNSCFG!ATL::CWorkerThread<ATL::Win32ThreadTraits>::_WorkerThreadProc+0x18 (FPO: [Non-Fpo])
        0143f8e0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0143f920 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 83820590  Cid 0de8.0fb8  Teb: 7ffdc000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            83951638  QueueObject
        Not impersonating
        DeviceMap                 a7766db8
        Owning Process            83862d90       Image:         wmpnscfg.exe
        Wait Start TickCount      39229          Ticks: 4270 (0:00:01:06.612)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init 9f67f000 Current 9f67ebc8 Base 9f67f000 Limit 9f67c000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f67ebe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f67ec1c 81cad431 nt!KiSwapThread+0x389
        9f67ec6c 81d8b982 nt!KeRemoveQueueEx+0x568
        9f67ecc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        9f67ed48 81c8caaa nt!NtRemoveIoCompletion+0x106
        9f67ed48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f67ed64)
        0109f910 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0109f914 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        0109f940 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        0109f97c 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        0109f9e8 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        0109f9f4 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        0109fa18 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        0109fa24 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        0109fa30 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0109fa70 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Wmpnetwk process

```
PROCESS 83a0bc70  SessionId: 0  Cid: 0844    Peb: 7ffda000  ParentCid: 0214
    DirBase: 29a016e0  ObjectTable: a8bd77c0  HandleCount: 351.
    Image: wmpnetwk.exe
    VadRoot 838731d0 Vads 165 Clone 0 Private 961. Modified 8. Locked 0.
    DeviceMap 9f999328
    Token                             aaf811a0
    ElapsedTime                       00:07:37.568
    UserTime                          00:00:00.140
    KernelTime                        00:00:00.124
    QuotaPoolUsage[PagedPool]         169712
    QuotaPoolUsage[NonPagedPool]      11064
    Working Set Sizes (now,min,max)  (3014, 50, 345) (12056KB, 200KB, 1380KB)
    PeakWorkingSetSize                3426
    VirtualSize                       92 Mb
    PeakVirtualSize                   95 Mb
    PageFaultCount                    4601
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      2069

    Setting context for this process...
.process /p /r ffffffff83a0bc70

    !peb
PEB at 7ffda000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00440000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00261830 . 017e7018
    Ldr.InLoadOrderModuleList:           002617b0 . 017e7008
    Ldr.InMemoryOrderModuleList:         002617b8 . 017e7010
            Base TimeStamp                     Module
          440000 4549b540 Nov 02 09:07:12 2006 C:\Program Files\Windows Media Player\wmpnetwk.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        6f510000 4549be32 Nov 02 09:45:22 2006 C:\Windows\system32\WSOCK32.dll
        75fe0000 4549be0e Nov 02 09:44:46 2006 C:\Windows\system32\WS2_32.dll
        77550000 4549bdc7 Nov 02 09:43:35 2006 C:\Windows\system32\NSI.dll
        755b0000 4549bd3f Nov 02 09:41:19 2006 C:\Windows\system32\IPHLPAPI.DLL
        75570000 46807ea6 Jun 26 03:49:10 2007 C:\Windows\system32\dhcpcsvc.DLL
        75af0000 4549bcf1 Nov 02 09:40:01 2006 C:\Windows\system32\DNSAPI.dll
        75b80000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\Secur32.dll
        75560000 4549be1e Nov 02 09:45:02 2006 C:\Windows\system32\WINNSI.DLL
        75540000 46807ea7 Jun 26 03:49:11 2007 C:\Windows\system32\dhcpcsvc6.DLL
        763b0000 4549bdb9 Nov 02 09:43:21 2006 C:\Windows\system32\SHLWAPI.dll
        6bdc0000 4549be79 Nov 02 09:46:33 2006 C:\Windows\system32\wmpmde.dll
        6bb00000 4549bd03 Nov 02 09:40:19 2006 C:\Windows\system32\MF.dll
        74d00000 4549bcbc Nov 02 09:39:08 2006 C:\Windows\system32\ATL.DLL
        72f80000 4549bd0c Nov 02 09:40:28 2006 C:\Windows\system32\MFPlat.DLL
        75390000 4549bcdc Nov 02 09:39:40 2006 C:\Windows\system32\AVRT.dll
        6ba80000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\EVR.dll
        738c0000 4549be1d Nov 02 09:45:01 2006 C:\Windows\system32\WINMM.dll
        73880000 4549bd93 Nov 02 09:42:43 2006 C:\Windows\system32\OLEACC.dll
        75290000 4549bdd0 Nov 02 09:43:44 2006 C:\Windows\system32\POWRPROF.dll
        6b960000 4549be52 Nov 02 09:45:54 2006 C:\Windows\system32\WMDRMSDK.DLL
```

```
        75ba0000 4549bde2 Nov 02 09:44:02 2006 C:\Windows\system32\USERENV.dll
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        74aa0000 4549bd09 Nov 02 09:40:25 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_5d07289e07e1d100\comctl32.dll
        6e6b0000 4549bd2a Nov 02 09:40:58 2006 C:\Windows\system32\DXVA2.DLL
        75020000 4549bddb Nov 02 09:43:55 2006 C:\Windows\system32\NTMARTA.DLL
        76310000 4549be44 Nov 02 09:45:40 2006 C:\Windows\system32\WLDAP32.dll
        75ce0000 4549bd99 Nov 02 09:42:49 2006 C:\Windows\system32\PSAPI.DLL
        75ad0000 4549bda8 Nov 02 09:43:04 2006 C:\Windows\system32\SAMLIB.dll
        773a0000 4549bce9 Nov 02 09:39:53 2006 C:\Windows\system32\CLBCatQ.DLL
        75350000 4549bdae Nov 02 09:43:10 2006 C:\Windows\system32\rsaenh.dll
        6e850000 4549bdd6 Nov 02 09:43:50 2006 C:\Windows\system32\upnp.dll
        73420000 4549be18 Nov 02 09:44:56 2006 C:\Windows\system32\WINHTTP.dll
        72a70000 4549bdc7 Nov 02 09:43:35 2006 C:\Windows\system32\SSDPAPI.dll
        75a60000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\SXS.DLL
        6ad10000 46e5fb76 Sep 11 03:20:38 2007 C:\Windows\system32\wmp.dll
        73c50000 4549bcb0 Nov 02 09:38:56 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.6000.16386_none_87e0cb09378714f1\COMCTL32.dll
        753f0000 4549bde4 Nov 02 09:44:04 2006 C:\Windows\system32\VERSION.dll
        6e8c0000 4681c94e Jun 27 03:19:58 2007 C:\Windows\system32\MSVFW32.dll
        76560000 4681c95d Jun 27 03:20:13 2007 C:\Windows\system32\SHELL32.dll
        71f00000 4549bcc9 Nov 02 09:39:21 2006 C:\Windows\system32\dbghelp.dll
        6a540000 46e5f131 Sep 11 02:36:49 2007 C:\Windows\system32\wmploc.dll
        73d70000 4549bcaf Nov 02 09:38:55 2006
C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.0.6000.16386_none_9ea0ac9ec96e71
27\gdiplus.dll
        70ab0000 4549bcbf Nov 02 09:39:11 2006 C:\Windows\system32\actxprxy.dll
        73240000 4654f735 May 24 03:23:49 2007 C:\Windows\system32\windowscodecs.dll
        74ff0000 4549be2f Nov 02 09:45:19 2006 C:\Windows\system32\WINTRUST.dll
        75650000 45b96fde Jan 26 03:05:02 2007 C:\Windows\system32\CRYPT32.dll
        75820000 4549bd41 Nov 02 09:41:21 2006 C:\Windows\system32\MSASN1.dll
        77580000 462434a3 Apr 17 03:44:51 2007 C:\Windows\system32\imagehlp.dll
        754f0000 4549bd49 Nov 02 09:41:29 2006 C:\Windows\system32\ncrypt.dll
        754a0000 4549bcb9 Nov 02 09:39:05 2006 C:\Windows\system32\BCRYPT.dll
        75250000 4549bd69 Nov 02 09:42:01 2006 C:\Windows\system32\mswsock.dll
        752c0000 4549be27 Nov 02 09:45:11 2006 C:\Windows\System32\wshtcpip.dll
        75330000 4549bcd7 Nov 02 09:39:35 2006 C:\Windows\system32\GPAPI.dll
        75610000 4679de70 Jun 21 03:12:00 2007 C:\Windows\system32\slc.dll
        6db00000 4549bd28 Nov 02 09:40:56 2006 C:\Windows\system32\cryptnet.dll
        713e0000 4549bdd6 Nov 02 09:43:50 2006 C:\Windows\system32\SensApi.dll
        75840000 4549bd53 Nov 02 09:41:39 2006 C:\Windows\system32\NETAPI32.dll
        752b0000 4549be21 Nov 02 09:45:05 2006 C:\Windows\System32\wship6.dll
        6e340000 4549be7b Nov 02 09:46:35 2006 C:\Windows\System32\wmpps.dll
        72460000 4666193b Jun 06 03:17:31 2007 C:\Windows\System32\msxml3.dll
        75dc0000 470c4de2 Oct 10 04:58:26 2007 C:\Windows\system32\urlmon.dll
        76360000 4549bcfb Nov 02 09:40:11 2006 C:\Windows\system32\iertutil.dll
        71ea0000 4549bd63 Nov 02 09:41:55 2006 C:\Windows\System32\netprofm.dll
        74d30000 4549bd6b Nov 02 09:42:03 2006 C:\Windows\System32\nlaapi.dll
        720c0000 4549bdc3 Nov 02 09:43:31 2006 C:\Windows\System32\npmproxy.dll
        72f40000 4549be1f Nov 02 09:45:03 2006 C:\Windows\System32\winrnr.dll
        72f30000 4549bd3b Nov 02 09:41:15 2006 C:\Windows\system32\napinsp.dll
        72c10000 4549bdc0 Nov 02 09:43:28 2006 C:\Windows\system32\pnrpnsp.dll
        72c40000 4549be1d Nov 02 09:45:01 2006 C:\Windows\system32\wshbth.dll
        77030000 4549bdb0 Nov 02 09:43:12 2006 C:\Windows\system32\SETUPAPI.dll
        72a60000 4549bda2 Nov 02 09:42:58 2006 C:\Windows\system32\rasadhlp.dll
    SubSystemData:     00000000
    ProcessHeap:       00260000
    ProcessParameters: 00261060
    WindowTitle:  'C:\Program Files\Windows Media Player\wmpnetwk.exe'
    ImageFile:    'C:\Program Files\Windows Media Player\wmpnetwk.exe'
    CommandLine:  '"C:\Program Files\Windows Media Player\wmpnetwk.exe"'
    DllPath:      'C:\Program Files\Windows Media
Player;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Windows;C:\Windows
\System32\Wbem;C:\Program Files\QuickTime\QTSystem\'
    Environment:  002891a0
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming
```

```
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        LOCALAPPDATA=C:\Windows\ServiceProfiles\NetworkService\AppData\Local
        NUMBER_OF_PROCESSORS=2
        OANOCACHE=1
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        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=WORKGROUP
        USERNAME=HOME$
        USERPROFILE=C:\Windows\ServiceProfiles\NetworkService
        windir=C:\Windows


        THREAD 83a0b598  Cid 0844.0f70  Teb: 7ffdf000 Win32Thread: ff514638 WAIT: (Executive)
UserMode Non-Alertable
            836c8d34  NotificationEvent
        IRP List:
            836bb5a0: (0006,0094) Flags: 00060900  Mdl: 00000000
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            83a0bc70       Image:         wmpnetwk.exe
        Wait Start TickCount      14192          Ticks: 29307 (0:00:07:37.192)
        Context Switch Count      63
        UserTime                  00:00:00.015
        KernelTime                00:00:00.015
        Win32 Start Address wmpnetwk!TrackerWinMainW (0x004df364)
        Stack Init a68df000 Current a68debc8 Base a68df000 Limit a68dc000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a68debe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a68dec1c 81c293a7 nt!KiSwapThread+0x389
        a68dec78 81d88faf nt!KeWaitForSingleObject+0x414
        a68decac 81d93669 nt!IopSynchronousServiceTail+0x258
        a68ded38 81c8caaa nt!NtReadFile+0x646
        a68ded38 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a68ded64)
        001cf28c 77490080 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        001cf290 75f3853f ntdll!ZwReadFile+0xc (FPO: [9,0,0])
        001cf308 775cffe2 kernel32!ReadFile+0x20e (FPO: [Non-Fpo])
        001cf334 775cfdfb ADVAPI32!ScGetPipeInput+0x2a (FPO: [Non-Fpo])
        001cf39c 775cbdd2 ADVAPI32!ScDispatcherLoop+0x6c (FPO: [Non-Fpo])
        001cf614 0046a976 ADVAPI32!StartServiceCtrlDispatcherW+0xce (FPO: [Non-Fpo])
        001cf640 004680e2 wmpnetwk!CNTService::StartServiceW+0xd6 (FPO: [Non-Fpo])
        001cf764 004df352 wmpnetwk!wWinMain+0x537 (FPO: [Non-Fpo])
        001cf7c8 004df369 wmpnetwk!wWinMainTrackerCRTStartup+0x7d (FPO: [Non-Fpo])
        001cf7cc 75f33833 wmpnetwk!TrackerWinMainW+0x5 (FPO: [Non-Fpo])
        001cf7d8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        001cf818 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 839f5888  Cid 0844.0814  Teb: 7ffde000 Win32Thread: ff52ec80 WAIT: (UserRequest)
UserMode Alertable
            839304c0  SynchronizationEvent
            8362e968  SynchronizationEvent
            839f67b8  SynchronizationEvent
            839f5910  NotificationTimer
        IRP List:
            838fc458: (0006,0094) Flags: 00060000  Mdl: 00000000
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            83a0bc70       Image:         wmpnetwk.exe
        Wait Start TickCount      43240          Ticks: 259 (0:00:00:04.040)
        Context Switch Count      243
        UserTime                  00:00:00.015
        KernelTime                00:00:00.015
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x775cb9d5)
        Stack Init 9e9f8000 Current 9e9f78d0 Base 9e9f8000 Limit 9e9f5000 Call 0
        Priority 13 BasePriority 8 PriorityDecrement 3 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9e9f78e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9e9f7924 81c28c64 nt!KiSwapThread+0x389
        9e9f7970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9e9f7bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9e9f7d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9e9f7d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9e9f7d64)
        003ffcec 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        003ffcf0 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        003ffd8c 761dc4b7 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        003ffde0 00472154 USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
        003ffe9c 0046a7d2 wmpnetwk!CWMCService::Run+0x6c2 (FPO: [Non-Fpo])
        003ffec4 775cb9f6 wmpnetwk!CNTService::ServiceMain+0x16e (FPO: [Non-Fpo])
        003ffed8 75f33833 ADVAPI32!ScSvcctrlThreadA+0x21 (FPO: [Non-Fpo])
        003ffee4 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        003fff24 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 839f63c8  Cid 0844.0860  Teb: 7ffdd000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            8396c150  SynchronizationEvent
            83a1d210  SynchronizationEvent
            8396c5b8  NotificationEvent
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            83a0bc70       Image:         wmpnetwk.exe
        Wait Start TickCount      14397          Ticks: 29102 (0:00:07:33.994)
        Context Switch Count      84
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wmpnetwk!ATL::CWorkerThread<ATL::Win32ThreadTraits>::_WorkerThreadProc
(0x00492d35)
        Stack Init a8f28000 Current a8f278d0 Base a8f28000 Limit a8f25000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a8f278e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a8f27924 81c28c64 nt!KiSwapThread+0x389
        a8f27970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a8f27bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a8f27d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a8f27d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a8f27d64)
        003af8a0 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        003af8a4 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        003af940 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        003af95c 004927cb kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        003afc8c 00492d4d
wmpnetwk!ATL::CWorkerThread<ATL::Win32ThreadTraits>::WorkerThreadProc+0x9f (FPO: [Non-Fpo])
        003afcb4 75f33833
wmpnetwk!ATL::CWorkerThread<ATL::Win32ThreadTraits>::_WorkerThreadProc+0x18 (FPO: [Non-Fpo])
        003afcc0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        003afd00 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 83a24a60  Cid 0844.0e18  Teb: 7ffd9000 Win32Thread: ff536008 WAIT: (WrUserRequest)
UserMode Non-Alertable
            8388bd48  SynchronizationEvent
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            83a0bc70       Image:         wmpnetwk.exe
        Wait Start TickCount      43497          Ticks: 2 (0:00:00:00.031)
        Context Switch Count      7876
        UserTime                  00:00:00.031
        KernelTime                00:00:00.031
        Win32 Start Address ole32!CRpcThreadCache::RpcWorkerThreadEntry (0x7644fc53)
        Stack Init a1e7a000 Current a1e79b68 Base a1e7a000 Limit a1e77000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a1e79b80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a1e79bbc 81c293a7 nt!KiSwapThread+0x389
        a1e79c18 8cedb8ed nt!KeWaitForSingleObject+0x414
        a1e79c74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        a1e79c90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        a1e79ce8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        a1e79d4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        a1e79d4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a1e79d64)
        0124f780 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0124f784 761e19cd USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        0124f7a0 76458155 USER32!GetMessageW+0x33 (FPO: [Non-Fpo])
        0124f7e0 7645258c ole32!CDllHost::STAWorkerLoop+0x81 (FPO: [Non-Fpo])
        0124f7fc 764524ce ole32!CDllHost::WorkerThread+0xce (FPO: [Non-Fpo])
        0124f804 7644fc0d ole32!DLLHostThreadEntry+0xd (FPO: [Non-Fpo])
        0124f820 7644fc73 ole32!CRpcThread::WorkerLoop+0x26 (FPO: [Non-Fpo])
        0124f82c 75f33833 ole32!CRpcThreadCache::RpcWorkerThreadEntry+0x20 (FPO: [Non-Fpo])
        0124f838 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0124f878 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 837512a8  Cid 0844.0dc8  Teb: 7ffd6000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            839ed5f8  SynchronizationTimer
            8396c6f8  SynchronizationEvent
            83832760  SynchronizationEvent
            839152a8  SynchronizationEvent
            837a8890  SynchronizationEvent
            83751240  SynchronizationEvent
            83a1d570  SynchronizationEvent
            838d8614  NotificationEvent
            836d5c10  SynchronizationEvent
            9fd819b0  SynchronizationEvent
            83901480  SynchronizationEvent
            8390c228  SynchronizationEvent
            838853e8  SynchronizationEvent
            838854a8  SynchronizationEvent
            838fc1f8  SynchronizationEvent
            83963618  SynchronizationEvent
            8390eac0  SynchronizationEvent
            83a1f1c0  SynchronizationEvent
            8362eb80  SynchronizationEvent
            835ec890  SynchronizationEvent
            83500088  SynchronizationEvent
            83a1eb68  SynchronizationEvent
            83a21d90  SynchronizationEvent
            839f0da8  SynchronizationEvent
            8393cc78  SynchronizationEvent
            8393cbd0  SynchronizationEvent
            83a0b348  SynchronizationEvent
            83a0b318  SynchronizationEvent
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            83a0bc70       Image:         wmpnetwk.exe
        Wait Start TickCount      15282          Ticks: 28217 (0:00:07:20.188)
        Context Switch Count      105
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWaiterpThread (0x7744b49a)
        Stack Init 9f68f000 Current 9f68e8d0 Base 9f68f000 Limit 9f68c000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f68e8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f68e924 81c28c64 nt!KiSwapThread+0x389
        9f68e970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f68ebfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f68ed48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f68ed48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f68ed64)
        012dfb8c 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        012dfb90 7744b65b ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        012dfd2c 75f33833 ntdll!TppWaiterpThread+0x294 (FPO: [Non-Fpo])
        012dfd38 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        012dfd78 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 8395f4d0  Cid 0844.0e14  Teb: 7ffd5000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            839f66b0  QueueObject
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            83a0bc70       Image:         wmpnetwk.exe
        Wait Start TickCount      14195          Ticks: 29304 (0:00:07:37.145)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address msvcrt!_endthreadex (0x7628639b)
        Stack Init 9f710000 Current 9f70fbc8 Base 9f710000 Limit 9f70d000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f70fbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f70fc1c 81cad431 nt!KiSwapThread+0x389
        9f70fc6c 81d8b982 nt!KeRemoveQueueEx+0x568
        9f70fcc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        9f70fd48 81c8caaa nt!NtRemoveIoCompletion+0x106
        9f70fd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f70fd64)
        0105f634 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0105f638 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        0105f664 72f83582 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        0105f69c 72f82887 MFPlat!CCompletionPortNT::Get+0x43 (FPO: [Non-Fpo])
        0105f7a4 72f889d7 MFPlat!CWorkQueue::CThread::ThreadMain+0x80 (FPO: [Non-Fpo])
        0105f7ac 762862b6 MFPlat!CWorkQueue::CThread::ThreadFunc+0xd (FPO: [Non-Fpo])
        0105f7e4 762863de msvcrt!_endthreadex+0x44 (FPO: [Non-Fpo])
        0105f7ec 75f33833 msvcrt!_endthreadex+0xce (FPO: [Non-Fpo])
        0105f7f8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0105f838 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 83a1e420  Cid 0844.083c  Teb: 7ffd4000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            83915ba0  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            83a0bc70       Image:         wmpnetwk.exe
        Wait Start TickCount      14195          Ticks: 29304 (0:00:07:37.145)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address msvcrt!_endthreadex (0x7628639b)
        Stack Init 9f728000 Current 9f727c38 Base 9f728000 Limit 9f725000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f727c50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f727c8c 81c293a7 nt!KiSwapThread+0x389
        9f727ce8 81df5057 nt!KeWaitForSingleObject+0x414
        9f727d50 81c8caaa nt!NtWaitForSingleObject+0xbe
        9f727d50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f727d64)
        0133fcd0 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0133fcd4 75f377d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0133fd44 72f82e54 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        0133fd68 72f82da1 MFPlat!LFQueueGetWaitEx+0xec (FPO: [Non-Fpo])
        0133fd88 72f82d63 MFPlat!LFQueueGetWait+0x22 (FPO: [Non-Fpo])
        0133fdb0 72f82887 MFPlat!CCompletionPortQ::Get+0x1f (FPO: [Non-Fpo])
        0133feb8 72f889d7 MFPlat!CWorkQueue::CThread::ThreadMain+0x80 (FPO: [Non-Fpo])
        0133fec0 762862b6 MFPlat!CWorkQueue::CThread::ThreadFunc+0xd (FPO: [Non-Fpo])
        0133fef8 762863de msvcrt!_endthreadex+0x44 (FPO: [Non-Fpo])
        0133ff00 75f33833 msvcrt!_endthreadex+0xce (FPO: [Non-Fpo])
        0133ff0c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0133ff4c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 83a14b50  Cid 0844.0628  Teb: 7ffd3000 Win32Thread: ff52c998 WAIT: (UserRequest)
UserMode Non-Alertable
            83a0b268  NotificationEvent
            83930ed8  SynchronizationEvent
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            83a0bc70       Image:         wmpnetwk.exe
        Wait Start TickCount      14196          Ticks: 29303 (0:00:07:37.129)
        Context Switch Count      9
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address gdiplus!BackgroundThreadProc (0x73d81909)
        Stack Init 9f3bc000 Current 9f3bb8d0 Base 9f3bc000 Limit 9f3b9000 Call 0
        Priority 13 BasePriority 8 PriorityDecrement 4 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f3bb8e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f3bb924 81c28c64 nt!KiSwapThread+0x389
        9f3bb970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        9f3bbbfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        9f3bbd48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        9f3bbd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f3bbd64)
        011cf788 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        011cf78c 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        011cf828 761dc4b7 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        011cf87c 761d8b83 USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
        011cf898 73d81965 USER32!MsgWaitForMultipleObjects+0x1f (FPO: [Non-Fpo])
        011cf8e4 75f33833 gdiplus!BackgroundThreadProc+0x59 (FPO: [Non-Fpo])
        011cf8f0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        011cf930 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 83a14410  Cid 0844.09ac  Teb: 7ffaa000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Alertable
            8371f3c0  NotificationEvent
            83a14498  NotificationTimer
        IRP List:
            837079c0: (0006,01d8) Flags: 00060070  Mdl: 00000000
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            83a0bc70       Image:         wmpnetwk.exe
        Wait Start TickCount      43271          Ticks: 228 (0:00:00:03.556)
        Context Switch Count      193
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address WINHTTP!ICAsyncThread::SelectThreadWrapper (0x73436286)
        Stack Init 9f760000 Current 9f75fc38 Base 9f760000 Limit 9f75d000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f75fc50 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f75fc8c 81c293a7 nt!KiSwapThread+0x389
        9f75fce8 81df5057 nt!KeWaitForSingleObject+0x414
        9f75fd50 81c8caaa nt!NtWaitForSingleObject+0xbe
        9f75fd50 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f75fd64)
        00fdf894 774906a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00fdf898 75253b28 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        00fdf8d8 75252690 mswsock!SockWaitForSingleObject+0x19f (FPO: [Non-Fpo])
        00fdf9c4 75fe3781 mswsock!WSPSelect+0x38c (FPO: [Non-Fpo])
        00fdfa40 73436217 WS2_32!select+0x456 (FPO: [Non-Fpo])
        00fdfac8 7343629e WINHTTP!ICAsyncThread::SelectThread+0x27d (FPO: [Non-Fpo])
        00fdfadc 75f33833 WINHTTP!ICAsyncThread::SelectThreadWrapper+0x18 (FPO: [Non-Fpo])
        00fdfae8 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        00fdfb28 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 83a0ab90  Cid 0844.09b0  Teb: 7ffa9000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            839efb70  QueueObject
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            83a0bc70       Image:         wmpnetwk.exe
        Wait Start TickCount      14390          Ticks: 29109 (0:00:07:34.103)
        Context Switch Count      18
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address WINHTTP!IOCompletionThreadFunc (0x7343642a)
        Stack Init a687f000 Current a687ebc8 Base a687f000 Limit a687c000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a687ebe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a687ec1c 81cad431 nt!KiSwapThread+0x389
        a687ec6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a687ecc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a687ed48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a687ed48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a687ed64)
        0146fcf8 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0146fcfc 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        0146fd28 73436467 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        0146fda8 75f33833 WINHTTP!IOCompletionThreadFunc+0x47 (FPO: [Non-Fpo])
        0146fdb4 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0146fdf4 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 83709030  Cid 0844.0824  Teb: 7ffa8000 Win32Thread: ff5268e8 WAIT: (WrQueue)
UserMode Non-Alertable
            839efb70  QueueObject
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            83a0bc70       Image:         wmpnetwk.exe
        Wait Start TickCount      14398          Ticks: 29101 (0:00:07:33.978)
        Context Switch Count      26
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address WINHTTP!IOCompletionThreadFunc (0x7343642a)
        Stack Init a0897000 Current a0896bc8 Base a0897000 Limit a0894000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a0896be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0896c1c 81cad431 nt!KiSwapThread+0x389
        a0896c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a0896cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a0896d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a0896d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0896d64)
        0139f934 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0139f938 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        0139f964 73436467 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        0139f9e4 75f33833 WINHTTP!IOCompletionThreadFunc+0x47 (FPO: [Non-Fpo])
        0139f9f0 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0139fa30 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 837a9580  Cid 0844.0a78  Teb: 7ffd7000 Win32Thread: 00000000 WAIT: (WrLpcReply)
UserMode Non-Alertable
            837a9794  Semaphore Limit 0x1
        Waiting for reply to ALPC Message aaf94ad8
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            83a0bc70       Image:         wmpnetwk.exe
        Wait Start TickCount      14773          Ticks: 28726 (0:00:07:28.128)
        Context Switch Count      6
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address SSDPAPI!GetNotificationLoop (0x72a73289)
        Stack Init 9f693000 Current 9f692b48 Base 9f693000 Limit 9f690000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f692b60 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f692b9c 81c293a7 nt!KiSwapThread+0x389
        9f692bfc 81cc0275 nt!KeWaitForSingleObject+0x414
        9f692c24 81dc3818 nt!AlpcpSignalAndWait+0x7e
        9f692c48 81dc5c29 nt!AlpcpReceiveSynchronousReply+0x2b
        9f692cd0 81dc61c5 nt!AlpcpProcessSynchronousRequest+0x201
        9f692d3c 81c8caaa nt!NtAlpcSendWaitReceivePort+0xd0
        9f692d3c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f692d64)
        022bfa08 7748f2c0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        022bfa0c 75d27f41 ntdll!NtAlpcSendWaitReceivePort+0xc (FPO: [8,0,0])
        022bfa38 75da37a0 RPCRT4!LRPC_CASSOCIATION::AlpcSendWaitReceivePort+0x24
        022bff38 72a7331b RPCRT4!NdrClientCall2+0x76e
        022bff54 72a732d4 SSDPAPI!GetNotificationRpc+0x1a (FPO: [Non-Fpo])
        022bff98 75f33833 SSDPAPI!GetNotificationLoop+0x59 (FPO: [Non-Fpo])
        022bffa4 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        022bffe4 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 835e17d0  Cid 0844.0874  Teb: 7ffaf000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Alertable
            83915948  QueueObject
        IRP List:
            839208e8: (0006,01d8) Flags: 00060000  Mdl: 00000000
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            83a0bc70       Image:         wmpnetwk.exe
        Wait Start TickCount      15282          Ticks: 28217 (0:00:07:20.188)
        Context Switch Count      43
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!TppWorkerThread (0x7749a044)
        Stack Init 9f72c000 Current 9f72bbc8 Base 9f72c000 Limit 9f729000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        9f72bbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f72bc1c 81cad431 nt!KiSwapThread+0x389
        9f72bc68 81d8b982 nt!KeRemoveQueueEx+0x568
        9f72bcc0 81c7a036 nt!IoRemoveIoCompletion+0x23
        9f72bd54 81c8caaa nt!NtWaitForWorkViaWorkerFactory+0x1a1
        9f72bd54 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f72bd64)
        0141f73c 77490850 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0141f740 7749a1b4 ntdll!NtWaitForWorkViaWorkerFactory+0xc (FPO: [2,0,0])
        0141f868 75f33833 ntdll!TppWorkerThread+0x1f6 (FPO: [Non-Fpo])
        0141f874 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        0141f8b4 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 8374cc60  Cid 0844.0fc0  Teb: 7ffdb000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            83751550  QueueObject
        Not impersonating
        DeviceMap                 9f999328
        Owning Process            83a0bc70       Image:         wmpnetwk.exe
        Wait Start TickCount      39229          Ticks: 4270 (0:00:01:06.612)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init a0995000 Current a0994bc8 Base a0995000 Limit a0992000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a0994be0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a0994c1c 81cad431 nt!KiSwapThread+0x389
        a0994c6c 81d8b982 nt!KeRemoveQueueEx+0x568
        a0994cc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        a0994d48 81c8caaa nt!NtRemoveIoCompletion+0x106
        a0994d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a0994d64)
        018ffc78 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        018ffc7c 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        018ffca8 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        018ffce4 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        018ffd50 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        018ffd5c 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        018ffd80 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        018ffd8c 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        018ffd98 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        018ffdd8 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

WmiPrvSE process

```
PROCESS 82f0bd10  SessionId: 0  Cid: 0d40    Peb: 7ffd5000  ParentCid: 02ec
    DirBase: 29a01700  ObjectTable: a9bd3498  HandleCount: 105.
    Image: WmiPrvSE.exe
    VadRoot 8395da28 Vads 69 Clone 0 Private 371. Modified 1. Locked 0.
    DeviceMap 85a03048
    Token                             a820e030
    ElapsedTime                       00:06:49.315
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         52120
    QuotaPoolUsage[NonPagedPool]      3312
    Working Set Sizes (now,min,max)  (1294, 50, 345) (5176KB, 200KB, 1380KB)
    PeakWorkingSetSize                1311
    VirtualSize                       27 Mb
    PeakVirtualSize                   29 Mb
    PageFaultCount                    1607
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      709
    Job                               9fcf49b0

    Setting context for this process...
.process /p /r ffffffff82f0bd10

    !peb
PEB at 7ffd5000
    InheritedAddressSpace:    No
    ReaUserNamegeFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00660000
    Ldr                       774f5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00171780 . 00189308
    Ldr.InLoadOrderModuleList:           00171700 . 00189368
    Ldr.InMemoryOrderModuleList:         00171708 . 00189370
            Base TimeStamp                     Module
          660000 4549af45 Nov 02 08:41:41 2006 C:\Windows\system32\wbem\wmiprvse.exe
        77430000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        75ef0000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\kernel32.dll
        775b0000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        75cf0000 469c344c Jul 17 04:15:24 2007 C:\Windows\system32\RPCRT4.dll
        761c0000 45d3dc0e Feb 15 04:05:34 2007 C:\Windows\system32\USER32.dll
        760f0000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        76260000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        71fe0000 46d7799a Aug 31 03:14:50 2007 C:\Windows\system32\wbem\wbemcomn.dll
        77310000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        76410000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        71b40000 4549bcd4 Nov 02 09:39:32 2006 C:\Windows\system32\wbem\FastProx.dll
        75780000 4549bdcc Nov 02 09:43:40 2006 C:\Windows\system32\NTDSAPI.dll
        75af0000 4549bcf1 Nov 02 09:40:01 2006 C:\Windows\system32\DNSAPI.dll
        75fe0000 4549be0e Nov 02 09:44:46 2006 C:\Windows\system32\WS2_32.dll
        77550000 4549bdc7 Nov 02 09:43:35 2006 C:\Windows\system32\NSI.dll
        76310000 4549be44 Nov 02 09:45:40 2006 C:\Windows\system32\WLDAP32.dll
        75ce0000 4549bd99 Nov 02 09:42:49 2006 C:\Windows\system32\PSAPI.DLL
        75840000 4549bd53 Nov 02 09:41:39 2006 C:\Windows\system32\NETAPI32.dll
        75b80000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\Secur32.dll
        75b50000 4549bd46 Nov 02 09:41:26 2006 C:\Windows\system32\NCObjAPI.DLL
        77560000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        771c0000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        75fd0000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        77290000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        773a0000 4549bce9 Nov 02 09:39:53 2006 C:\Windows\system32\CLBCatQ.DLL
        75350000 4549bdae Nov 02 09:43:10 2006 C:\Windows\system32\rsaenh.dll
        71ef0000 4549bdf0 Nov 02 09:44:16 2006 C:\Windows\system32\wbem\wbemsvc.dll
        71b00000 4549be6b Nov 02 09:46:19 2006 C:\Windows\system32\wbem\wmiutils.dll
```

```
        6e620000 4549be66 Nov 02 09:46:14 2006 C:\Windows\system32\wbem\wmiprov.dll
        6f610000 46243562 Apr 17 03:48:02 2007 C:\Windows\system32\WMI.dll
    SubSystemData:     00000000
    ProcessHeap:       00170000
    ProcessParameters: 00170fd8
    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;C:\Program Files\QuickTime\QTSystem\'
    Environment:  001707e8
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Windows\system32\config\systemprofile\AppData\Roaming
        CLASSPATH=.;C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=HOME
        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:\Program
Files\QuickTime\QTSystem\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=0f02
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        QTJAVA=C:\Program Files\Java\jre1.6.0_03\lib\ext\QTJava.zip
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Windows\TEMP
        TMP=C:\Windows\TEMP
        USERDOMAIN=WORKGROUP
        USERNAME=HOME$
        USERPROFILE=C:\Windows\system32\config\systemprofile
        windir=C:\Windows
```

```
        THREAD 83962d78  Cid 0d40.0d28  Teb: 7ffdf000 Win32Thread: ff52bc18 WAIT: (WrUserRequest)
UserMode Non-Alertable
            837c1430  SynchronizationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f0bd10       Image:         WmiPrvSE.exe
        Wait Start TickCount      17262          Ticks: 26237 (0:00:06:49.299)
        Context Switch Count      59
        UserTime                  00:00:00.015
        KernelTime                00:00:00.031
        Win32 Start Address wmiprvse!WinMainCRTStartup (0x00671373)
        Stack Init a6917000 Current a6916b68 Base a6917000 Limit a6914000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a6916b80 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a6916bbc 81c293a7 nt!KiSwapThread+0x389
        a6916c18 8cedb8ed nt!KeWaitForSingleObject+0x414
        a6916c74 8cedb724 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        a6916c90 8ced9976 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        a6916ce8 8cedd983 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
        a6916d4c 81c8caaa win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        a6916d4c 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a6916d64)
        000ff7a8 761e199a ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        000ff7ac 761e19cd USER32!NtUserGetMessage+0xc (FPO: [Non-Fpo])
        000ff7c8 00666714 USER32!GetMessageW+0x33 (FPO: [Non-Fpo])
        000ff804 00666649 wmiprvse!WindowsDispatch+0x31 (FPO: [Non-Fpo])
        000ff898 0066682c wmiprvse!Process+0x1f4 (FPO: [Non-Fpo])
        000ff8a0 006667b9 wmiprvse!WinMain+0x55 (FPO: [Non-Fpo])
        000ff930 75f33833 wmiprvse!_initterm_e+0x1a1 (FPO: [Non-Fpo])
        000ff93c 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        000ff97c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 8383cd78  Cid 0d40.0e90  Teb: 7ffde000 Win32Thread: 00000000 WAIT: (UserRequest)
UserMode Non-Alertable
            836501f8  NotificationEvent
            8356bb38  NotificationEvent
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f0bd10       Image:         WmiPrvSE.exe
        Wait Start TickCount      17261          Ticks: 26238 (0:00:06:49.315)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address NCObjAPI!CNamedPipeClient::ProviderReadyThreadProc (0x75b517a5)
        Stack Init a09d5000 Current a09d48d0 Base a09d5000 Limit a09d2000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        a09d48e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a09d4924 81c28c64 nt!KiSwapThread+0x389
        a09d4970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a09d4bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a09d4d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a09d4d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a09d4d64)
        010cfa4c 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        010cfa50 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        010cfaec 75f38150 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        010cfb08 75b51808 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        010cfb58 75f33833 NCObjAPI!CNamedPipeClient::ProviderReadyThreadProc+0x102 (FPO: [Non-Fpo])
        010cfb64 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        010cfba4 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 835ac300  Cid 0d40.0618  Teb: 7ffdd000 Win32Thread: 00000000 WAIT: (WrQueue)
UserMode Non-Alertable
            8361d910  QueueObject
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f0bd10       Image:         WmiPrvSE.exe
        Wait Start TickCount      42326          Ticks: 1173 (0:00:00:18.298)
        Context Switch Count      1478
        UserTime                  00:00:00.093
        KernelTime                00:00:00.031
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x75d3ac65)
        Stack Init 9f750000 Current 9f74fbc8 Base 9f750000 Limit 9f74d000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9f74fbe0 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9f74fc1c 81cad431 nt!KiSwapThread+0x389
        9f74fc6c 81d8b982 nt!KeRemoveQueueEx+0x568
        9f74fcc4 81d8b705 nt!IoRemoveIoCompletion+0x23
        9f74fd48 81c8caaa nt!NtRemoveIoCompletion+0x106
        9f74fd48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9f74fd64)
        012dfb58 774900f0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        012dfb5c 75f17948 ntdll!NtRemoveIoCompletion+0xc (FPO: [5,0,0])
        012dfb88 75d3aeae kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        012dfbc4 75d3afe7 RPCRT4!COMMON_ProcessCalls+0xb5
        012dfc30 75d3abcf RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
        012dfc3c 75d3ac39 RPCRT4!ProcessIOEventsWrapper+0xe
        012dfc60 75d3ac83 RPCRT4!BaseCachedThreadRoutine+0x5c
        012dfc6c 75f33833 RPCRT4!ThreadStartRoutine+0x1e
        012dfc78 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        012dfcb8 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

        THREAD 8385b5a8  Cid 0d40.0d24  Teb: 7ffdb000 Win32Thread: ff53c008 WAIT: (UserRequest)
UserMode Alertable
            8379e698  SynchronizationEvent
            836d3ba0  SynchronizationEvent
            8994bf08  SynchronizationEvent
            837b4ff0  SynchronizationEvent
            83667a58  SynchronizationEvent
            8385b630  NotificationTimer
        Not impersonating
        DeviceMap                 85a03048
        Owning Process            82f0bd10       Image:         WmiPrvSE.exe
        Wait Start TickCount      40339          Ticks: 3160 (0:00:00:49.296)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wmiprvse!WmiThread<unsigned long>::ThreadProc (0x006663db)
        Stack Init a68c3000 Current a68c28d0 Base a68c3000 Limit a68c0000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        a68c28e8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        a68c2924 81c28c64 nt!KiSwapThread+0x389
        a68c2970 81df5519 nt!KeWaitForMultipleObjects+0x47d
        a68c2bfc 81df5181 nt!ObpWaitForMultipleObjects+0x256
        a68c2d48 81c8caaa nt!NtWaitForMultipleObjects+0xcc
        a68c2d48 77490f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ a68c2d64)
        009bfbb4 77490690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        009bfbb8 75f37e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
        009bfc54 761dc4b7 kernel32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
        009bfca8 0066158d USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
        009bfdf4 006654a6 wmiprvse!WmiThread<unsigned long>::ThreadWait+0x77 (FPO: [Non-Fpo])
        009bfe28 00666406 wmiprvse!WmiThread<unsigned long>::ThreadDispatch+0x9f (FPO: [Non-Fpo])
        009bfe38 75f33833 wmiprvse!WmiThread<unsigned long>::ThreadProc+0x2b (FPO: [Non-Fpo])
        009bfe44 7746a9bd kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        009bfe84 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Stacks Summary

```
0: kd> !stacks
Proc.Thread  .Thread  Ticks   ThreadState Blocker
                          [82f14d90 System]
   4.000010  82f14348 000a9d9 Blocked    nt!PopIrpWorkerControl+0x25
   4.000014  82f38020 0008227 Blocked    nt!PopIrpWorker+0x129
   4.000018  82f38d78 0008227 Blocked    nt!PopIrpWorker+0x129
   4.000038  82f3a580 0003585 Blocked    nt!KeRemoveQueueEx+0x568
   4.000044  82f3bd78 0000003 Blocked    nt!KeRemoveQueueEx+0x568
   4.000048  82f3bad0 0000073 Blocked    nt!KeRemoveQueueEx+0x568
   4.00004c  82f3b828 0000033 Blocked    nt!KeRemoveQueueEx+0x568
   4.000054  82f3d4d8 00000c1 Blocked    nt!KiExecuteDpc+0x15a
   4.000058  82f3d230 00000b7 Blocked    nt!KiExecuteDpc+0x15a
   4.000060  82f40d78 00000b4 Blocked    nt!MiModifiedPageWriter+0x40
   4.000070  82f3faf0 00002f3 Blocked    nt!CcQueueLazyWriteScanThread+0x42
   4.000074  82f35830 000a9cb Blocked    nt!KeRemoveQueueEx+0x568
   4.000078  82f35588 000a9cf Blocked    nt!KeRemoveQueueEx+0x568
   4.000080  82f0cd78 000000e Blocked    nt!EtwpLogger+0xc7
   4.000084  82f0c730 0000039 Blocked    nt!EtwpLogger+0xc7
   4.000088  83352d78 000000b Blocked    nt!EtwpLogger+0xc7
   4.00008c  833527d0 000001e Blocked    nt!EtwpLogger+0xc7
   4.000090  833d64f8 000a9ca Blocked    nt!EtwpLogger+0x66
   4.000094  833dbd78 000a9ca Blocked    nt!EtwpLogger+0x66
   4.000098  833db7d0 000a9ca Blocked    nt!EtwpLogger+0x66
   4.0000a0  83a5c370 0006ebc Blocked    nt!EtwpLogger+0xc7
   4.0000a4  83c6d278 0000484 Blocked    nt!WdipSemCheckTimeout+0x226
   4.0000a8  83c8a020 000a6db Blocked    acpi!ACPIWorkerThread+0x47
   4.0000b0  83c9d020 000a9c2 Blocked    pci!ExpressRootComplexPmeEventDispatcher+0x34
   4.0000b4  83c9dd78 000a9c2 Blocked    acpi!PciRootBusBiosMethodDispatcherOnResume+0x30
   4.0000b8  83cbd880 000a5ad Blocked    nt!KeRemoveQueueEx+0x568
   4.0000bc  83cd7aa0 0000401 Blocked    ndis!ndisCmWaitThread+0x5b
   4.0000c0  83cd77f8 000964b Blocked    ecache!EcCacheIoWorker+0x41
   4.0000c4  83cd7550 000964c Blocked    ecache!EcCacheIoWatchdog+0x3cd
   4.0000cc  847a7968 000a935 Blocked    volsnap!VspWorkerThread+0x51
   4.0000d0  84651558 0002cb7 Blocked    volsnap!VspWorkerThread+0x8f
   4.0000d4  846512b0 0002cb7 Blocked    volsnap!VspWorkerThread+0x8f
   4.0000d8  8444bb98 000a8d0 Blocked    volsnap!VspWorkerThread+0x8f
   4.0000dc  8444b8f0 000a935 Blocked    volsnap!VspWorkerThread+0x51
   4.0000e0  8480d3b8 00006e0 Blocked    Ntfs!TxfPrivateThreadWorkerRoutine+0x20
   4.0000e8  84902d78 000a809 Blocked    dxgkrnl!DpiPdoPollingThread+0x39
   4.0000ec  84902ad0 000a809 Blocked    watchdog!SMgrGdiCalloutThread+0x45
   4.0000f0  84902828 000a809 Blocked    dxgkrnl!DpiPowerArbiterThread+0x40
   4.000114  84b60af8 000a5b8 Blocked    stwrt+0x9452d
   4.000134  84dc0760 000a759 Blocked    nt!KeRemoveQueueEx+0x568
   4.000138  84dbb5f0 000a759 Blocked    nt!KeRemoveQueueEx+0x568
   4.00013c  84dc5810 000a759 Blocked    nt!KeRemoveQueueEx+0x568
   4.000140  84dc5568 000a759 Blocked    nt!KeRemoveQueueEx+0x568
   4.000144  84dca020 00004ea Blocked    nt!KeRemoveQueueEx+0x568
   4.000148  84dcad78 000a759 Blocked    nt!KeRemoveQueueEx+0x568
   4.00014c  84dcaad0 000a759 Blocked    nt!KeRemoveQueueEx+0x568
   4.000150  84dca828 000a759 Blocked    nt!KeRemoveQueueEx+0x568
   4.000154  84dca580 0000249 Blocked    nt!KeRemoveQueueEx+0x568
   4.00017c  84875d78 0000072 Blocked    nt!KeRemoveQueueEx+0x568
   4.000180  84875ad0 0000333 Blocked    nt!KeRemoveQueueEx+0x568
   4.0001c4  89844d78 0004696 Blocked    dxgkrnl!VidSchiWaitForSchedulerEvents+0x109
   4.0001c8  89966080 000a6db Blocked    IRFilter+0xfac
   4.000200  89945030 0003860 Blocked    nt!KeRemoveQueueEx+0x568
   4.00023c  8997fcf8 000843a Blocked    nt!EtwpLogger+0xc7
   4.000270  899ca020 0008206 Blocked    bthport!HCI_ThreadFunction+0x89
   4.000274  899f1510 000a69b Blocked    KeyMagic+0x26dd
   4.000310  9e1ffd78 0002cb7 Blocked    luafv!SynchronousFsControl+0xa3
   4.000494  9fcd7d78 000a5b5 Blocked    spsys!SPVersion+0x1489b
   4.0005e0  9fd4a020 0000e26 Blocked    HTTP!UlpScavengerThread+0x5e
   4.000644  9fd7b9f8 000839b Blocked    mpsdrv!AuditSuccessEvent+0x19b
   4.00068c  9fd9a020 000a526 Blocked    nt!KeRemoveQueueEx+0x568
   4.000690  9fd9ab90 000a521 Blocked    nt!KeRemoveQueueEx+0x568
```

```
  4.000698  9fd9b918 000a520 Blocked    nt!KeRemoveQueueEx+0x568
  4.0006b4  9fda2020 000a51e Blocked    nt!KeRemoveQueueEx+0x568
  4.0006b8  9fda3020 000a51e Blocked    nt!KeRemoveQueueEx+0x568
  4.000524  a18e3d78 000a2a3 Blocked    nt!EtwpLogger+0xc7
  4.000890  9fcbf808 00000ad Blocked    nt!PfTLoggingWorker+0x67
  4.0008bc  a194f7e0 0009659 Blocked    nt!EtwpLogger+0xc7
  4.0008c4  8345c030 0000014 Blocked    nt!EtwpLogger+0xc7
  4.000a10  835a9490 0008753 Blocked    nt!EtwpLogger+0xc7
  4.0001a8  838e6020 0006f11 Blocked    nt!EtwpLogger+0x66
  4.00051c  83670b98 0004b1f RUNNING    nt!KeBugCheckEx+0x1e

                          [84d9f128 smss.exe]

                          [84d32d90 csrss.exe]
1bc.0001d4  8993f238 0000033 Blocked    nt!AlpcpReceiveMessagePort+0x221
1bc.0001f0  89941400 0000056 Blocked    nt!AlpcpReceiveMessagePort+0x221
1bc.000230  89964470 0000058 Blocked    nt!AlpcpReceiveMessagePort+0x221

                          [8983e1b0 wininit.exe]

                          [84d33020 csrss.exe]
1f4.000244  89979aa0 0006173 Blocked    cdd!PresentWorkerThread+0x3d2
1f4.000264  899ab030 0000aba Blocked    nt!AlpcpReceiveMessagePort+0x221
1f4.00029c  9e1e7030 0000337 Blocked    nt!AlpcpReceiveMessagePort+0x221
1f4.000b34  836053c8 000031c Blocked    nt!AlpcpReceiveMessagePort+0x221

                          [89956238 services.exe]
214.00012c  8372ad38 00005ca Blocked    nt!KeRemoveQueueEx+0x568
214.0006d8  83605d78 00005ca Blocked    nt!KeRemoveQueueEx+0x568

                          [8995e4a0 lsass.exe]
220.0009dc  8356fa40 0000460 Blocked    nt!KiFastCallEntry+0x12a
220.000bd4  a18b5030 0000460 Blocked    nt!KeRemoveQueueEx+0x568

                          [8995ab30 lsm.exe]
228.000a88  89995d78 0003379 Blocked    nt!KeRemoveQueueEx+0x568

                          [899e3020 winlogon.exe]

                          [9e1f2020 svchost.exe]
2ec.0008f0  83789d28 00030dd Blocked    nt!KeRemoveQueueEx+0x568

                          [9e1fd468 svchost.exe]
324.00032c  9fc0d748 000020f Blocked    nt!KiFastCallEntry+0x12a
324.000330  9fc0c030 0000f61 Blocked    nt!ObpWaitForMultipleObjects+0x256
324.000adc  835e67e0 0000259 Blocked    nt!KeRemoveQueueEx+0x568
324.0004e8  838efd78 0000010 Blocked    nt!KeRemoveQueueEx+0x568
324.000ae4  8366f2a0 0000711 Blocked    nt!KiFastCallEntry+0x12a
324.0002c8  83715cd0 000076d Blocked    nt!KeRemoveQueueEx+0x568

                          [9fc4a020 svchost.exe]
350.000390  9fc21030 0000f00 Blocked    nt!ObpWaitForMultipleObjects+0x256
350.00039c  9fc23d78 0000f00 Blocked    nt!KeRemoveQueueEx+0x568
350.00040c  9fdbcd30 000392d Blocked    nt!KeRemoveQueueEx+0x568
350.000370  839f2ac0 0000f00 Blocked    nt!KiFastCallEntry+0x12a

                          [8485e910 svchost.exe]
3a4.0003a8  899d5948 00005ca Blocked    nt!NtReadFile+0x646
3a4.0003b4  9fc2e768 00005ca Blocked    nt!ObpWaitForMultipleObjects+0x256
3a4.0003c4  9fc3c030 00000ad Blocked    nt!ObpWaitForMultipleObjects+0x256
3a4.0003d8  9fc3e630 0000ba3 Blocked    nt!KiFastCallEntry+0x12a
3a4.00080c  8374c440 0000460 Blocked    nt!KeRemoveQueueEx+0x568
3a4.000af8  8360b920 00000ad Blocked    nt!KeRemoveQueueEx+0x568
3a4.0005ac  835d1930 00000ad Blocked    nt!KeRemoveQueueEx+0x568

                          [9fc38a48 svchost.exe]
3bc.0003ec  9fc6b030 0000056 Blocked    nt!ObpWaitForMultipleObjects+0x256
3bc.000564  9fce1030 0000056 Blocked    nt!KeRemoveQueueEx+0x568
3bc.000788  9fdc2d78 0000007 Blocked    nt!ObpWaitForMultipleObjects+0x256
3bc.0007f4  a1805b68 0000510 Blocked    nt!ObpWaitForMultipleObjects+0x256
```

```
3bc.00019c  a18a33b8 000003d Blocked    nt!ObpWaitForMultipleObjects+0x256
3bc.000358  9fdf2d78 0000c53 Blocked    nt!ObpWaitForMultipleObjects+0x256
3bc.0002e8  a1800030 0000c53 Blocked    nt!KeRemoveQueueEx+0x568
3bc.0002bc  a18004b8 0000c53 Blocked    nt!KeRemoveQueueEx+0x568
3bc.0008a0  9fc88d78 000268d Blocked    nt!KiFastCallEntry+0x12a
3bc.0008cc  8369a588 000008e Blocked    nt!KeRemoveQueueEx+0x568
3bc.00090c  9fc427f8 0000056 Blocked    nt!KeRemoveQueueEx+0x568
3bc.000f74  9fc7aac0 0000056 Blocked    nt!KeRemoveQueueEx+0x568
3bc.000a94  9fce2d78 0000c53 Blocked    nt!ObpWaitForMultipleObjects+0x256
3bc.000b54  835d8d78 0000c53 Blocked    nt!ObpWaitForMultipleObjects+0x256
3bc.00056c  83920af8 0000058 Blocked    nt!KeRemoveQueueEx+0x568
3bc.000304  836b8578 0000056 Blocked    nt!KeRemoveQueueEx+0x568
3bc.000a30  9fc99030 0000056 Blocked    nt!KeRemoveQueueEx+0x568

                          [9fc3dd90 svchost.exe]
3cc.0003e4  9fc56b88 000496e Blocked    nt!KiFastCallEntry+0x12a
3cc.0003e8  9fc56668 00000e1 Blocked    nt!AlpcpReceiveMessagePort+0x221
3cc.000480  9fc98ad0 00004df Blocked    nt!ObpWaitForMultipleObjects+0x256
3cc.000568  9fd1ba00 00047a5 Blocked    nt!KeRemoveQueueEx+0x568
3cc.000718  89854388 0000746 Blocked    nt!ObpWaitForMultipleObjects+0x256
3cc.00015c  a18b4898 0003c77 Blocked    nt!ObpWaitForMultipleObjects+0x256
3cc.000d74  836e0b48 0000008 Blocked    nt!KeRemoveQueueEx+0x568
3cc.000efc  836b7b88 0002970 Blocked    win32k!xxxRealSleepThread+0x1ad
3cc.000f0c  835e4b58 0000032 Blocked    nt!KiFastCallEntry+0x12a
3cc.000bec  83685030 000007c Blocked    nt!KeRemoveQueueEx+0x568
3cc.000bf0  836cdd78 0000033 Blocked    nt!KeRemoveQueueEx+0x568

                          [9fca1800 audiodg.exe]
420.0006c4  9fdb02d8 00049a3 Blocked    nt!ObpWaitForMultipleObjects+0x256
420.000c44  83885ac0 0001c2b Blocked    nt!KeRemoveQueueEx+0x568

                          [9fc70d90 SLsvc.exe]

                          [9fc9c020 svchost.exe]
460.00049c  9fc9f2c8 0001e74 Blocked    nt!ObpWaitForMultipleObjects+0x256
460.000660  9fd97240 000076d Blocked    nt!KiFastCallEntry+0x12a
460.000174  9fdb3a60 0001e74 Blocked    nt!ObpWaitForMultipleObjects+0x256
460.000700  a1938030 00001bf Blocked    nt!ObpWaitForMultipleObjects+0x256
460.000f80  a1d3ad78 00001bf Blocked    nt!KeRemoveQueueEx+0x568
460.0009fc  83a14030 0000887 Blocked    nt!KiFastCallEntry+0x12a
460.000f7c  83739b10 0000887 Blocked    nt!KiFastCallEntry+0x12a
460.000d30  836843c0 00021ed Blocked    nt!KeRemoveQueueEx+0x568

                          [9fcb2858 svchost.exe]
4c4.000504  9fcc26e0 00000f2 Blocked    nt!ObpWaitForMultipleObjects+0x256
4c4.000bcc  a1969a88 00000f2 Blocked    nt!KeRemoveQueueEx+0x568
4c4.000d6c  835c4870 000057a Blocked    nt!KiFastCallEntry+0x12a
4c4.000d70  835c4540 000057a Blocked    nt!KiFastCallEntry+0x12a
4c4.000120  83699d30 00000f2 Blocked    nt!KeRemoveQueueEx+0x568

                          [9fd42790 spoolsv.exe]
5e8.000a38  835b62a0 0000021 Blocked    nt!KiFastCallEntry+0x12a
5e8.000a44  835b3030 0000006 Blocked    nt!KiFastCallEntry+0x12a
5e8.000a7c  835c0148 0001af2 Blocked    nt!KeRemoveQueueEx+0x568

                          [9fd50418 svchost.exe]
600.000744  89872030 0000c13 Blocked    nt!KiFastCallEntry+0x12a
600.000794  9fde0498 0000c98 Blocked    nt!ObpWaitForMultipleObjects+0x256
600.000798  9fde2c50 0000c53 Blocked    nt!ObpWaitForMultipleObjects+0x256
600.00079c  9fde12f0 0000c53 Blocked    nt!ObpWaitForMultipleObjects+0x256
600.0007a0  9fde2490 0000c53 Blocked    nt!ObpWaitForMultipleObjects+0x256
600.0007a8  9fde7d78 0000c53 Blocked    nt!ObpWaitForMultipleObjects+0x256
600.00075c  83890138 0002340 Blocked    nt!KeRemoveQueueEx+0x568

                          [89870020 AppleOSSMgr.exe]

                          [89871718 AppleTimeSrv.ex]

                          [89877258 svchost.exe]
```

```
                          [89881d28 svchost.exe]

                          [9fde0020 stacsv.exe]
78c.0006ec  a1c3dd78 0000c54 Blocked    nt!KiFastCallEntry+0x12a
78c.000760  a180a6c0 000001f Blocked    nt!KiFastCallEntry+0x12a
78c.000764  9fdbc030 000000a Blocked    nt!KiFastCallEntry+0x12a
78c.000fc4  8346f030 00040a9 Blocked    nt!KeRemoveQueueEx+0x568

                          [a18b73a0 svchost.exe]

                          [a18bd670 SearchIndexer.e]
1e4.000548  8995e1f8 00000e4 Blocked    nt!ObpWaitForMultipleObjects+0x256
1e4.00073c  9fdc4a78 0000215 Blocked    nt!KiFastCallEntry+0x12a
1e4.000124  9fdc4750 0000002 Blocked    nt!KiFastCallEntry+0x12a
1e4.00074c  a1801030 0000be3 Blocked    nt!ObpWaitForMultipleObjects+0x256
1e4.000ee4  9e1d45f8 0002275 Blocked    nt!KeRemoveQueueEx+0x568
1e4.000bac  834bcd78 00000e4 Blocked    nt!KeRemoveQueueEx+0x568
1e4.000b08  8371b2c0 00000e4 Blocked    nt!KeRemoveQueueEx+0x568

                          [89860020 taskeng.exe]

                          [8346d618 taskeng.exe]
b14.000b18  83485030 0001566 Blocked    nt!ObpWaitForMultipleObjects+0x256
b14.000b50  83622030 0002441 Blocked    nt!KeRemoveQueueEx+0x568
b14.000b8c  83628620 0000009 Blocked    nt!AlpcpReceiveMessagePort+0x221
b14.000be0  83655568 000497f Blocked    nt!ObpWaitForMultipleObjects+0x256

                          [8346fd90 dwm.exe]
b48.000b6c  8362b030 00000e6 Blocked    nt!ObpWaitForMultipleObjects+0x256
b48.000b88  83628910 00000e5 Blocked    nt!KiFastCallEntry+0x12a

                          [8362a638 explorer.exe]
b90.000b94  8362a390 0000003 Blocked    win32k!xxxRealSleepThread+0x1ad
b90.000c00  8354e030 0000612 Blocked    win32k!xxxRealSleepThread+0x1ad
b90.000e38  834a2d78 000036e Blocked    nt!ObpWaitForMultipleObjects+0x256
b90.000e5c  8350f800 00046d7 Blocked    win32k!xxxRealSleepThread+0x1ad
b90.000e60  8350f500 00029f8 Blocked    nt!ObpWaitForMultipleObjects+0x256
b90.000e64  8374da20 000391e Blocked    nt!KiFastCallEntry+0x12a
b90.000eb8  83746d78 0000056 Blocked    nt!KiFastCallEntry+0x12a
b90.000ec4  836aab00 0000001 Blocked    win32k!xxxRealSleepThread+0x1ad
b90.000ecc  836bad40 00029f8 Blocked    nt!ObpWaitForMultipleObjects+0x256
b90.0001b0  837c9ab0 000241e Blocked    win32k!xxxRealSleepThread+0x1ad
b90.0000fc  837c64c8 000222d Blocked    nt!ObpWaitForMultipleObjects+0x256
b90.000484  835d9090 0000056 Blocked    nt!KeRemoveQueueEx+0x568

                          [836999f8 MSASCui.exe]
c64.000834  836929e0 0004b2f Blocked    nt!KeRemoveQueueEx+0x568

                          [8364a488 igfxtray.exe]
c6c.000c70  8367d030 0002a3c Blocked    win32k!xxxRealSleepThread+0x1ad
c6c.000284  83a23ac0 00022b9 Blocked    nt!KeRemoveQueueEx+0x568

                          [8369d8b8 hkcmd.exe]
c78.000c7c  8369d610 0000010 Blocked    win32k!xxxRealSleepThread+0x1ad
c78.000e0c  83483d78 0000c31 Blocked    nt!KiFastCallEntry+0x12a
c78.000810  83c8a3b0 0000010 Blocked    nt!KeRemoveQueueEx+0x568

                          [83688020 igfxpers.exe]
c84.000c88  8367f870 0002a3c Blocked    win32k!xxxRealSleepThread+0x1ad
c84.000d80  838fed78 00022b9 Blocked    nt!KeRemoveQueueEx+0x568

                          [83665b10 sttray.exe]
c8c.000c90  8366d6a0 000283f Blocked    win32k!xxxRealSleepThread+0x1ad
c8c.000820  8374fb10 00020bc Blocked    nt!KeRemoveQueueEx+0x568
c8c.0002d0  8372aa50 0003786 Blocked    nt!KiFastCallEntry+0x12a

                          [83644b48 IRW.exe]

                          [83683d90 KbdMgr.exe]
```

```
                          [83679bb0 jusched.exe]
 ca4.000ca8  83691580 0003966 Blocked    nt!ObpWaitForMultipleObjects+0x256

                          [836466e8 realsched.exe]
 cd8.000cdc  83646440 0002a3c Blocked    win32k!xxxRealSleepThread+0x1ad
 cd8.000320  9fd6c630 00022b9 Blocked    nt!KeRemoveQueueEx+0x568

                          [8364b2f0 sidebar.exe]
 ce4.000ce8  83681d78 0000025 Blocked    nt!ObpWaitForMultipleObjects+0x256
 ce4.000dfc  83635030 000036e Blocked    nt!ObpWaitForMultipleObjects+0x256
 ce4.000eec  836db2b0 0000056 Blocked    nt!KiFastCallEntry+0x12a
 ce4.000f8c  837e2788 0000056 Blocked    nt!KeRemoveQueueEx+0x568
 ce4.000fd4  83738550 000036d Blocked    nt!ObpWaitForMultipleObjects+0x256
 ce4.000fd8  83735360 00028de Blocked    nt!ObpWaitForMultipleObjects+0x256
 ce4.000fdc  837d3c78 00000df Blocked    nt!ObpWaitForMultipleObjects+0x256
 ce4.000fec  8361b0c8 000036d Blocked    nt!KiFastCallEntry+0x12a
 ce4.000ff8  836a1d78 000036d Blocked    nt!KeRemoveQueueEx+0x568

                          [8354dd90 ehtray.exe]
 cf4.000cf8  8354dae8 00029f8 Blocked    nt!ObpWaitForMultipleObjects+0x256
 cf4.000574  8388d030 0002275 Blocked    nt!KeRemoveQueueEx+0x568

                          [836d3d90 GoogleToolbarNo]
 cfc.0009f0  8394dc90 00022b9 Blocked    nt!KeRemoveQueueEx+0x568

                          [8354c7a0 igfxsrvc.exe]
 ddc.000de0  83561400 0000010 Blocked    win32k!xxxRealSleepThread+0x1ad
 ddc.000de4  837128a0 0000010 Blocked    nt!KiFastCallEntry+0x12a
 ddc.000360  836a4478 0000010 Blocked    nt!KeRemoveQueueEx+0x568
 ddc.000828  83a09a90 000031c Blocked    nt!KeRemoveQueueEx+0x568

                          [83687850 ehmsas.exe]
 e24.000e28  83625030 00029f8 Blocked    win32k!xxxRealSleepThread+0x1ad
 e24.000a74  8389d458 0002275 Blocked    nt!KeRemoveQueueEx+0x568

                          [8380c398 ieuser.exe]
 910.000b60  8371e4f0 0002113 Blocked    win32k!xxxRealSleepThread+0x1ad
 910.00092c  8367cd48 0001990 Blocked    nt!KeRemoveQueueEx+0x568

                          [8380fd90 iexplore.exe]
 5a4.00094c  837231d0 0002199 Blocked    nt!ObpWaitForMultipleObjects+0x256
 5a4.000968  83809598 0000002 Blocked    win32k!xxxRealSleepThread+0x1ad
 5a4.0006f0  83702d78 0001812 Blocked    nt!KeRemoveQueueEx+0x568

                          [835ff588 realplay.exe]

                          [838806e8 FlashUtil9e.exe]
 ab8.000620  83855598 0001f95 Blocked    win32k!xxxRealSleepThread+0x1ad
 ab8.00057c  8369a030 0001812 Blocked    nt!KeRemoveQueueEx+0x568

                          [838e25a0 notepad.exe]

                          [83862d90 wmpnscfg.exe]
 de8.000c34  839f0380 0001831 Blocked    win32k!xxxRealSleepThread+0x1ad
 de8.000ee0  839f2d78 0002777 Blocked    nt!KiFastCallEntry+0x12a
 de8.000fb8  83820590 00010ae Blocked    nt!KeRemoveQueueEx+0x568

                          [83a0bc70 wmpnetwk.exe]
 844.000814  839f5888 0000103 Blocked    nt!ObpWaitForMultipleObjects+0x256
 844.000e18  83a24a60 0000002 Blocked    win32k!xxxRealSleepThread+0x1ad
 844.0009ac  83a14410 00000e4 Blocked    nt!KiFastCallEntry+0x12a
 844.000fc0  8374cc60 00010ae Blocked    nt!KeRemoveQueueEx+0x568

                          [82f0bd10 WmiPrvSE.exe]
 d40.000618  835ac300 0000495 Blocked    nt!KeRemoveQueueEx+0x568
 d40.000d24  8385b5a8 0000c58 Blocked    nt!ObpWaitForMultipleObjects+0x256


Threads Processed: 597
```

Executive Queues

```
0: kd> !exqueue ff
Dumping ExWorkerQueue: 81CFDE40

**** Critical WorkQueue( current = 0 maximum = 2 )
THREAD 82f389c0  Cid 0004.001c  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue) UserMode Non-
Alertable
    81cfde40  QueueObject
Not impersonating
DeviceMap                 85a03048
Owning Process            82f14d90       Image:         System
Wait Start TickCount      18             Ticks: 43481 (0:00:11:18.307)
Context Switch Count      1
UserTime                  00:00:00.000
KernelTime                00:00:00.000
Win32 Start Address nt!ExpWorkerThread (0x81c78ea3)
Stack Init 84e6d000 Current 84e6cc90 Base 84e6d000 Limit 84e6a000 Call 0
Priority 13 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
Kernel stack not resident.
ChildEBP RetAddr
84e6cca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
84e6cce4 81cad431 nt!KiSwapThread+0x389
84e6cd30 81c78f78 nt!KeRemoveQueueEx+0x568
84e6cd7c 81e254e0 nt!ExpWorkerThread+0xd5
84e6cdc0 81c9159e nt!PspSystemThreadStartup+0x9d
00000000 00000000 nt!KiThreadStartup+0x16

THREAD 82f38718  Cid 0004.0020  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue) UserMode Non-
Alertable
    81cfde40  QueueObject
Not impersonating
DeviceMap                 85a03048
Owning Process            82f14d90       Image:         System
Wait Start TickCount      18             Ticks: 43481 (0:00:11:18.307)
Context Switch Count      1
UserTime                  00:00:00.000
KernelTime                00:00:00.000
Win32 Start Address nt!ExpWorkerThread (0x81c78ea3)
Stack Init 84e71000 Current 84e70c90 Base 84e71000 Limit 84e6e000 Call 0
Priority 13 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
Kernel stack not resident.
ChildEBP RetAddr
84e70ca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
84e70ce4 81cad431 nt!KiSwapThread+0x389
84e70d30 81c78f78 nt!KeRemoveQueueEx+0x568
84e70d7c 81e254e0 nt!ExpWorkerThread+0xd5
84e70dc0 81c9159e nt!PspSystemThreadStartup+0x9d
00000000 00000000 nt!KiThreadStartup+0x16
```

```
THREAD 82f38470  Cid 0004.0024  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue) UserMode Non-
Alertable
    81cfde40  QueueObject
Not impersonating
DeviceMap                 85a03048
Owning Process            82f14d90       Image:         System
Wait Start TickCount      680            Ticks: 42819 (0:00:11:07.980)
Context Switch Count      860
UserTime                  00:00:00.000
KernelTime                00:00:00.000
Win32 Start Address nt!ExpWorkerThread (0x81c78ea3)
Stack Init 859f0000 Current 859efc90 Base 859f0000 Limit 859ed000 Call 0
Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
Kernel stack not resident.
ChildEBP RetAddr
859efca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
859efce4 81cad431 nt!KiSwapThread+0x389
859efd30 81c78f78 nt!KeRemoveQueueEx+0x568
859efd7c 81e254e0 nt!ExpWorkerThread+0xd5
859efdc0 81c9159e nt!PspSystemThreadStartup+0x9d
00000000 00000000 nt!KiThreadStartup+0x16

THREAD 82f3a020  Cid 0004.0028  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue) UserMode Non-
Alertable
    81cfde40  QueueObject
Not impersonating
DeviceMap                 85a03048
Owning Process            82f14d90       Image:         System
Wait Start TickCount      680            Ticks: 42819 (0:00:11:07.980)
Context Switch Count      1456
UserTime                  00:00:00.000
KernelTime                00:00:00.436
Win32 Start Address nt!ExpWorkerThread (0x81c78ea3)
Stack Init 859ec000 Current 859ebc90 Base 859ec000 Limit 859e9000 Call 0
Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
Kernel stack not resident.
ChildEBP RetAddr
859ebca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
859ebce4 81cad431 nt!KiSwapThread+0x389
859ebd30 81c78f78 nt!KeRemoveQueueEx+0x568
859ebd7c 81e254e0 nt!ExpWorkerThread+0xd5
859ebdc0 81c9159e nt!PspSystemThreadStartup+0x9d
00000000 00000000 nt!KiThreadStartup+0x16

THREAD 82f3ad78  Cid 0004.002c  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue) UserMode Non-
Alertable
    81cfde40  QueueObject
Not impersonating
DeviceMap                 85a03048
Owning Process            82f14d90       Image:         System
Wait Start TickCount      658            Ticks: 42841 (0:00:11:08.323)
Context Switch Count      159
UserTime                  00:00:00.000
KernelTime                00:00:00.265
Win32 Start Address nt!ExpWorkerThread (0x81c78ea3)
Stack Init 859e8000 Current 859e7c90 Base 859e8000 Limit 859e5000 Call 0
Priority 13 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
Kernel stack not resident.
ChildEBP RetAddr
859e7ca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
859e7ce4 81cad431 nt!KiSwapThread+0x389
859e7d30 81c78f78 nt!KeRemoveQueueEx+0x568
859e7d7c 81e254e0 nt!ExpWorkerThread+0xd5
859e7dc0 81c9159e nt!PspSystemThreadStartup+0x9d
00000000 00000000 nt!KiThreadStartup+0x16
```

```
THREAD 84875d78  Cid 0004.017c  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue) UserMode Non-
Alertable
    81cfde40  QueueObject
    84875e00  NotificationTimer
Not impersonating
DeviceMap                 85a03048
Owning Process            82f14d90       Image:         System
Wait Start TickCount      43385          Ticks: 114 (0:00:00:01.778)
Context Switch Count      5878
UserTime                  00:00:00.000
KernelTime                00:00:00.717
Win32 Start Address nt!ExpWorkerThread (0x81c78ea3)
Stack Init 88ea5000 Current 88ea4c90 Base 88ea5000 Limit 88ea2000 Call 0
Priority 15 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
ChildEBP RetAddr
88ea4ca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
88ea4ce4 81cad431 nt!KiSwapThread+0x389
88ea4d30 81c78f78 nt!KeRemoveQueueEx+0x568
88ea4d7c 81e254e0 nt!ExpWorkerThread+0xd5
88ea4dc0 81c9159e nt!PspSystemThreadStartup+0x9d
00000000 00000000 nt!KiThreadStartup+0x16

THREAD 848752d8  Cid 0004.018c  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue) UserMode Non-
Alertable
    81cfde40  QueueObject
    84875360  NotificationTimer
Not impersonating
DeviceMap                 85a03048
Owning Process            82f14d90       Image:         System
Wait Start TickCount      17820          Ticks: 25679 (0:00:06:40.594)
Context Switch Count      1268
UserTime                  00:00:00.000
KernelTime                00:00:00.202
Win32 Start Address nt!ExpWorkerThread (0x81c78ea3)
Stack Init 88eb1000 Current 88eb0c90 Base 88eb1000 Limit 88eae000 Call 0
Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
Kernel stack not resident.
ChildEBP RetAddr
88eb0ca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
88eb0ce4 81cad431 nt!KiSwapThread+0x389
88eb0d30 81c78f78 nt!KeRemoveQueueEx+0x568
88eb0d7c 81e254e0 nt!ExpWorkerThread+0xd5
88eb0dc0 81c9159e nt!PspSystemThreadStartup+0x9d
00000000 00000000 nt!KiThreadStartup+0x16

THREAD 84875ad0  Cid 0004.0180  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue) UserMode Non-
Alertable
    81cfde40  QueueObject
    84875b58  NotificationTimer
Not impersonating
DeviceMap                 85a03048
Owning Process            82f14d90       Image:         System
Wait Start TickCount      42680          Ticks: 819 (0:00:00:12.776)
Context Switch Count      3349
UserTime                  00:00:00.000
KernelTime                00:00:00.655
Win32 Start Address nt!ExpWorkerThread (0x81c78ea3)
Stack Init 88e89000 Current 88e88c90 Base 88e89000 Limit 88e86000 Call 0
Priority 13 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
ChildEBP RetAddr
88e88ca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
88e88ce4 81cad431 nt!KiSwapThread+0x389
88e88d30 81c78f78 nt!KeRemoveQueueEx+0x568
88e88d7c 81e254e0 nt!ExpWorkerThread+0xd5
88e88dc0 81c9159e nt!PspSystemThreadStartup+0x9d
00000000 00000000 nt!KiThreadStartup+0x16
```

```
THREAD 84875580  Cid 0004.0188  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue) UserMode Non-
Alertable
    81cfde40  QueueObject
    84875608  NotificationTimer
Not impersonating
DeviceMap                 85a03048
Owning Process            82f14d90       Image:         System
Wait Start TickCount      15262          Ticks: 28237 (0:00:07:20.500)
Context Switch Count      2575
UserTime                  00:00:00.000
KernelTime                00:00:00.171
Win32 Start Address nt!ExpWorkerThread (0x81c78ea3)
Stack Init 88ead000 Current 88eacc90 Base 88ead000 Limit 88eaa000 Call 0
Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
Kernel stack not resident.
ChildEBP RetAddr
88eacca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
88eacce4 81cad431 nt!KiSwapThread+0x389
88eacd30 81c78f78 nt!KeRemoveQueueEx+0x568
88eacd7c 81e254e0 nt!ExpWorkerThread+0xd5
88eacdc0 81c9159e nt!PspSystemThreadStartup+0x9d
00000000 00000000 nt!KiThreadStartup+0x16


**** Delayed WorkQueue( current = 0 maximum = 2 )
THREAD 82f3aad0  Cid 0004.0030  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue) UserMode Non-
Alertable
    81cfde7c  QueueObject
Not impersonating
DeviceMap                 85a03048
Owning Process            82f14d90       Image:         System
Wait Start TickCount      765            Ticks: 42734 (0:00:11:06.654)
Context Switch Count      204
UserTime                  00:00:00.000
KernelTime                00:00:00.000
Win32 Start Address nt!ExpWorkerThread (0x81c78ea3)
Stack Init 859e4000 Current 859e3c90 Base 859e4000 Limit 859e1000 Call 0
Priority 13 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5
Kernel stack not resident.
ChildEBP RetAddr
859e3ca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
859e3ce4 81cad431 nt!KiSwapThread+0x389
859e3d30 81c78f78 nt!KeRemoveQueueEx+0x568
859e3d7c 81e254e0 nt!ExpWorkerThread+0xd5
859e3dc0 81c9159e nt!PspSystemThreadStartup+0x9d
00000000 00000000 nt!KiThreadStartup+0x16

THREAD 82f3a828  Cid 0004.0034  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue) UserMode Non-
Alertable
    81cfde7c  QueueObject
Not impersonating
DeviceMap                 85a03048
Owning Process            82f14d90       Image:         System
Wait Start TickCount      8861           Ticks: 34638 (0:00:09:00.356)
Context Switch Count      1966
UserTime                  00:00:00.000
KernelTime                00:00:02.449
Win32 Start Address nt!ExpWorkerThread (0x81c78ea3)
Stack Init 859e0000 Current 859dfc90 Base 859e0000 Limit 859dd000 Call 0
Priority 15 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5
Kernel stack not resident.
ChildEBP RetAddr
859dfca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
859dfce4 81cad431 nt!KiSwapThread+0x389
859dfd30 81c78f78 nt!KeRemoveQueueEx+0x568
859dfd7c 81e254e0 nt!ExpWorkerThread+0xd5
859dfdc0 81c9159e nt!PspSystemThreadStartup+0x9d
00000000 00000000 nt!KiThreadStartup+0x16
```

```
THREAD 82f3a580  Cid 0004.0038  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue) UserMode Non-
Alertable
    81cfde7c  QueueObject
Not impersonating
DeviceMap                 85a03048
Owning Process            82f14d90       Image:         System
Wait Start TickCount      29798          Ticks: 13701 (0:00:03:33.736)
Context Switch Count      5908
UserTime                  00:00:00.000
KernelTime                00:00:00.249
Win32 Start Address nt!ExpWorkerThread (0x81c78ea3)
Stack Init 859dc000 Current 859dbc90 Base 859dc000 Limit 859d9000 Call 0
Priority 13 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5
ChildEBP RetAddr
859dbca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
859dbce4 81cad431 nt!KiSwapThread+0x389
859dbd30 81c78f78 nt!KeRemoveQueueEx+0x568
859dbd7c 81e254e0 nt!ExpWorkerThread+0xd5
859dbdc0 81c9159e nt!PspSystemThreadStartup+0x9d
00000000 00000000 nt!KiThreadStartup+0x16

THREAD 82f3a2d8  Cid 0004.003c  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue) UserMode Non-
Alertable
    81cfde7c  QueueObject
Not impersonating
DeviceMap                 85a03048
Owning Process            82f14d90       Image:         System
Wait Start TickCount      8861           Ticks: 34638 (0:00:09:00.356)
Context Switch Count      554
UserTime                  00:00:00.000
KernelTime                00:00:00.062
Win32 Start Address nt!ExpWorkerThread (0x81c78ea3)
Stack Init 859d8000 Current 859d7c90 Base 859d8000 Limit 859d5000 Call 0
Priority 14 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5
Kernel stack not resident.
ChildEBP RetAddr
859d7ca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
859d7ce4 81cad431 nt!KiSwapThread+0x389
859d7d30 81c78f78 nt!KeRemoveQueueEx+0x568
859d7d7c 81e254e0 nt!ExpWorkerThread+0xd5
859d7dc0 81c9159e nt!PspSystemThreadStartup+0x9d
00000000 00000000 nt!KiThreadStartup+0x16

THREAD 82f3b020  Cid 0004.0040  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue) UserMode Non-
Alertable
    81cfde7c  QueueObject
Not impersonating
DeviceMap                 85a03048
Owning Process            82f14d90       Image:         System
Wait Start TickCount      9807           Ticks: 33692 (0:00:08:45.598)
Context Switch Count      1402
UserTime                  00:00:00.000
KernelTime                00:00:00.187
Win32 Start Address nt!ExpWorkerThread (0x81c78ea3)
Stack Init 859d4000 Current 859d3c90 Base 859d4000 Limit 859d1000 Call 0
Priority 14 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5
Kernel stack not resident.
ChildEBP RetAddr
859d3ca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
859d3ce4 81cad431 nt!KiSwapThread+0x389
859d3d30 81c78f78 nt!KeRemoveQueueEx+0x568
859d3d7c 81e254e0 nt!ExpWorkerThread+0xd5
859d3dc0 81c9159e nt!PspSystemThreadStartup+0x9d
00000000 00000000 nt!KiThreadStartup+0x16
```

```
THREAD 82f3bd78  Cid 0004.0044  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue) UserMode Non-
Alertable
    81cfde7c  QueueObject
Not impersonating
DeviceMap                 85a03048
Owning Process            82f14d90       Image:         System
Wait Start TickCount      43496          Ticks: 3 (0:00:00:00.046)
Context Switch Count      5183
UserTime                  00:00:00.000
KernelTime                00:00:00.202
Win32 Start Address nt!ExpWorkerThread (0x81c78ea3)
Stack Init 859d0000 Current 859cfc90 Base 859d0000 Limit 859cd000 Call 0
Priority 13 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5
ChildEBP RetAddr
859cfca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
859cfce4 81cad431 nt!KiSwapThread+0x389
859cfd30 81c78f78 nt!KeRemoveQueueEx+0x568
859cfd7c 81e254e0 nt!ExpWorkerThread+0xd5
859cfdc0 81c9159e nt!PspSystemThreadStartup+0x9d
00000000 00000000 nt!KiThreadStartup+0x16

THREAD 82f3bad0  Cid 0004.0048  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue) UserMode Non-
Alertable
    81cfde7c  QueueObject
Not impersonating
DeviceMap                 85a03048
Owning Process            82f14d90       Image:         System
Wait Start TickCount      43384          Ticks: 115 (0:00:00:01.794)
Context Switch Count      9947
UserTime                  00:00:00.000
KernelTime                00:00:01.466
Win32 Start Address nt!ExpWorkerThread (0x81c78ea3)
Stack Init 859cc000 Current 859cbc90 Base 859cc000 Limit 859c9000 Call 0
Priority 12 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5
ChildEBP RetAddr
859cbca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
859cbce4 81cad431 nt!KiSwapThread+0x389
859cbd30 81c78f78 nt!KeRemoveQueueEx+0x568
859cbd7c 81e254e0 nt!ExpWorkerThread+0xd5
859cbdc0 81c9159e nt!PspSystemThreadStartup+0x9d
00000000 00000000 nt!KiThreadStartup+0x16


**** HyperCritical WorkQueue( current = 0 maximum = 2 )
THREAD 82f3b828  Cid 0004.004c  Teb: 00000000 Win32Thread: 00000000 WAIT: (WrQueue) KernelMode Non-
Alertable
    81cfdeb8  QueueObject
Not impersonating
DeviceMap                 85a03048
Owning Process            82f14d90       Image:         System
Wait Start TickCount      43448          Ticks: 51 (0:00:00:00.795)
Context Switch Count      1208
UserTime                  00:00:00.000
KernelTime                00:00:00.000
Win32 Start Address nt!ExpWorkerThread (0x81c78ea3)
Stack Init 859c8000 Current 859c7c90 Base 859c8000 Limit 859c5000 Call 0
Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
ChildEBP RetAddr
859c7ca8 81cac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
859c7ce4 81cad431 nt!KiSwapThread+0x389
859c7d30 81c78f78 nt!KeRemoveQueueEx+0x568
859c7d7c 81e254e0 nt!ExpWorkerThread+0xd5
859c7dc0 81c9159e nt!PspSystemThreadStartup+0x9d
00000000 00000000 nt!KiThreadStartup+0x16
```

Root Objects

```
0: kd> !object \
Object: 85a07638  Type: (82efc1f8) Directory
    ObjectHeader: 85a07620 (old version)
    HandleCount: 0  PointerCount: 46
    Directory Object: 00000000  Name: \

    Hash Address  Type          Name
    ---- -------  ----          ----
     00  85a0ade8 Directory     ArcName
         83cb9698 Device        Ntfs
     01  89938870 ALPC Port     SeLsaCommandPort
         84d33ff0 Event         UniqueInteractiveSessionIdEvent
     03  85a09940 Key           \REGISTRY
     05  9fc96c20 ALPC Port     ThemeApiPort
     06  9fdcc030 ALPC Port     XactSrvLpcPort
     08  a18ab2b8 ALPC Port     WindowsErrorReportingServicePort
     09  85a5f030 Directory     NLS
     10  85a07748 SymbolicLink  DosDevices
     12  9fc8d5c8 ALPC Port     UxSmsApiPort
     13  84b9ddd8 ALPC Port     SeRmCommandPort
     14  899d8ad0 ALPC Port     LsaAuthenticationPort
         9fd6c100 Event         LanmanServerAnnounceEvent
         85a60ae0 SymbolicLink  Dfs
         85a573a8 Directory     UMDFCommunicationPorts
     16  85a62ea0 Directory     Driver
     18  83343aa0 Device        clfs
     19  85a12530 Directory     Device
     20  9fc557a8 ALPC Port     MmcssApiPort
         873d58e8 Directory     Windows
         8487e790 Event         CsrSbSyncEvent
     21  873d5f58 Directory     Sessions
         899d92a8 Event         SAM_SERVICE_STARTED
     22  873c1e50 Directory     RPC Control
         84dbe2f0 ALPC Port     SmApiPort
     23  89c00af8 Directory     BaseNamedObjects
         85a071d0 Directory     KernelObjects
     24  85a03288 Directory     GLOBAL??
         85a5d810 Directory     FileSystem
         89969f88 Event         DSYSDBG.Debug.Trace.Memory.220
     25  89d63f50 Section       LsaPerformance
     26  9fc48630 ALPC Port     SmSsWinStationApiPort
         85a035e8 Directory     ObjectTypes
     27  85a09868 Directory     Security
     30  89854bb0 ALPC Port     AELPort
         899e1e18 Event         EFSSrvInitEvent
     31  87264158 SymbolicLink  SystemRoot
         8485a2e8 Device        Cdfs
     32  85a08ee8 Directory     Callback
     33  899e1e58 Event         EFSSmbInitEvent
         84dcd628 Event         EFSInitEvent
         8487eef8 Event         UniqueSessionIdEvent
     35  873b5f58 Directory     KnownDlls
```

Device Objects

```
0: kd> !object \Device
Object: 85a12530  Type: (82efc1f8) Directory
    ObjectHeader: 85a12518 (old version)
    HandleCount: 0  PointerCount: 277
    Directory Object: 85a07638  Name: Device

    Hash Address  Type          Name
    ---- -------  ----          ----
     00  83db02f0 Device        KsecDD
         83ce3840 Device        Ndis
         82f086d8 Device        00000032
         9fd448b8 Device        SrvNet
         84b62030 Device        Beep
         87264f38 SymbolicLink  ScsiPort2
         85bb7208 SymbolicLink  HarddiskVolumeShadowCopy{c50194f6-c939-11dc-aa52-001b635fde5a}
         82f06b30 Device        00000025
         82f04c50 Device        00000019
     01  8987a1c8 Device        KeyAgent
         82f08418 Device        00000033
         84dbc030 Device        Netbios
         848f6030 Device        NDMP10
         87265f58 SymbolicLink  ScsiPort3
         82f068b0 Device        00000026
     02  848f7030 Device        NDMP11
         872493c8 SymbolicLink  {59ED4BC8-BE3E-49B7-8F12-52A80F13A10D}
         82f08168 Device        00000034
         87264528 SymbolicLink  Ip
         873bbe50 SymbolicLink  ScsiPort4
         85a53c38 SymbolicLink  HarddiskVolumeShadowCopy{8a678fba-ca05-11dc-928f-001b635fde5a}
         847a7c20 Device        HarddiskVolumeShadowCopy1
         8333f368 Device        00000040
         82f065f8 Device        00000027
     03  873b98f0 SymbolicLink  {E3FE0F52-6729-43AC-8488-5AC1FB2AE7A9}
         9fd6d158 Device        KSENUM#00000002
         82f09f10 Device        00000035
         84907030 Device        NDMP12
         84908298 Device        KeyboardClass0
         84b63040 Device        Video0
         847fe030 Device        HarddiskVolumeShadowCopy2
         8333f250 Device        00000041
         83c8abe8 Device        KMDF0
         82eff1c8 Device        WMIAdminDevice
         82f06338 Device        00000028
     04  84916e48 Device        Tun0
         84ccfc70 Device        NDProxy
         a01cbd18 SymbolicLink  MailslotRedirector
         8725e378 SymbolicLink  {6EA11ADB-6FEB-425D-A3CB-3CB73F334E62}
         899e0030 Device        NDMP13
         84859190 Device        KeyboardClass1
         899f04b8 Device        BthPan
         84c6cc58 Device        Video1
         847b6c20 Device        HarddiskVolumeShadowCopy3
         83c93d18 Device        VolMgrControl
         83344030 Device        00000042
         82f09c90 Device        00000036
         82f07030 Device        00000029
     05  84bf6338 Device        00000050
         9fd7c340 Device        NDMP14
         82f09a10 Device        00000037
         9fd44ba8 Device        SrvAdmin
         84909578 Device        PointerClass0
         84c6c460 Device        Video2
         873c4b78 SymbolicLink  Ip6
         85b08230 SymbolicLink  HarddiskVolumeShadowCopy{c50194ed-c939-11dc-aa52-001b635fde5a}
         847c97c0 Device        HarddiskVolumeShadowCopy4
```

```
    83344f18 Device        00000043
    82f01590 Device        0000000a
06  898462e0 Device        Video3
    9e1d9c60 Device        PointerClass1
    849c1028 Device        USBPDO-0
    84bf39f0 Device        00000051
    847c93b0 Device        HarddiskVolumeShadowCopy5
    82f09790 Device        00000038
    83344e00 Device        00000044
    82f012d8 Device        0000000b
07  82eff2e0 Device        WMIDataDevice
    899e8648 Device        MacHALDriver
    8486f580 Device        00000052
    83d91b60 Device        SpDevice
    85bb4260 SymbolicLink  {534467F1-4A60-4374-AB3A-F94FA338D23B}
    849bf028 Device        USBPDO-1
    847fe7e8 Device        HarddiskVolumeShadowCopy6
    83344ce8 Device        00000045
    83c70948 Device        RawTape
    82f092e0 Device        00000039
    82f02f10 Device        0000000c
08  89880030 Device        PEAuth
    a1237128 SymbolicLink  WebDavRedirector
    9f82a9a0 SymbolicLink  {93563980-2A26-408A-8A65-7A7BA760261B}
    849c6028 Device        USBPDO-2
    8984c558 Device        00000053
    847ff618 Device        HarddiskVolumeShadowCopy7
    83344bd0 Device        00000046
    83c9d300 Device        NTPNP_PCI0000
    82f049d0 Device        0000001a
    82f02c50 Device        0000000d
09  89952d48 Device        00000054
    9fdb9a18 Device        MPS
    84ad8028 Device        USBPDO-3
    83334030 Device        NTPNP_PCI0001
    84802030 Device        HarddiskVolumeShadowCopy8
    83344ab8 Device        00000047
    82f04710 Device        0000001b
    82f02998 Device        0000000e
10  84c6aa10 Device        RasAcd
    899bbec0 Device        00000055
    84b8f028 Device        USBPDO-4
    84d4da48 Device        Psched
    8480e6e0 Device        HarddiskVolumeShadowCopy9
    833449a0 Device        00000048
    83334b98 Device        NTPNP_PCI0002
    82f04458 Device        0000001c
    82f026d8 Device        0000000f
11  84dcd710 Device        DfsClient
    8996d818 Device        IRFilter
    84d865e0 Device        Tcp
    899bbd50 Device        00000056
    84880700 Device        USBPDO-5
    8333a030 Device        NTPNP_PCI0010
    83344888 Device        00000049
    83334700 Device        NTPNP_PCI0003
    82f041a0 Device        0000001d
12  899bbbe0 Device        00000057
    89847030 Device        USBPDO-6
    84d61aa8 Device        eQoS
    8333ab98 Device        NTPNP_PCI0011
    83338030 Device        NTPNP_PCI0004
    82f07db0 Device        0000002a
    82f05ed8 Device        0000001e
13  8394a6d0 Device        SystemDump
    a01d82a0 Directory     Http
    8997d030 Device        USBPDO-7
    84651e20 Device        HarddiskVolume1
    84840030 Device        NDMP1
    899ed698 Device        00000058
```

```
    8333a700 Device        NTPNP_PCI0012
    83338b98 Device        NTPNP_PCI0005
    82f07af0 Device        0000002b
    82f05c20 Device        0000001f
14  84988a60 Device        CdRom0
    83cd7ee8 Device        ECacheControl
    84651888 Device        HarddiskVolume2
    8484a030 Device        NDMP2
    899ef030 Device        00000059
    84dc5ac8 Device        FsWrap
    83338700 Device        NTPNP_PCI0006
    84908588 Device        Termdd
    8333b030 Device        NTPNP_PCI0013
    82f07830 Device        0000002c
15  8444b1c0 Device        HarddiskVolume3
    85bbd5a0 Directory     Ide
    8484b030 Device        NDMP3
    85affe98 SymbolicLink  {2C278182-E7C0-4F09-87DE-C7FEB61235AE}
    8487f948 Device        _HID00000000
    84d89808 Device        RawIp6
    83c8ff18 Device        0000003a
    83339030 Device        NTPNP_PCI0007
    8333bb98 Device        NTPNP_PCI0014
    82f07570 Device        0000002d
16  82f072b0 Device        0000002e
    8484c030 Device        NDMP4
    89958030 Device        _HID00000001
    8331e220 Device        0000003b
    83339b98 Device        NTPNP_PCI0008
    8333b700 Device        NTPNP_PCI0015
17  82f08f10 Device        0000002f
    83c8cb98 Device        NTPNP_PCI0016
    8484f030 Device        NDMP5
    899f9030 Device        _HID00000002
    82f35368 Event         VolumesSafeForWriteAccess
    83339700 Device        NTPNP_PCI0009
    8331d220 Device        0000003c
18  9fcb2220 Device        NetBT_Tcpip_{2C278182-E7C0-4F09-87DE-C7FEB61235AE}
    84910030 Device        NDMP6
    8480ec20 Device        HarddiskVolumeShadowCopy10
    9fda0a08 Device        Secdrv
    83c8eb98 Device        NTPNP_PCI0017
    899fb030 Device        _HID00000003
    899fe750 Device        BTHMS_RFCOMM
    84d91528 Device        Tcp6
    85bfb430 SymbolicLink  HarddiskVolumeShadowCopy{be08b27d-c1d2-11dc-8962-001b635fde5a}
    83c8f030 Device        0000003d
19  85bf8398 SymbolicLink  {034E5E83-07BF-438D-A902-4F7D975B6E1A}
    84911030 Device        NDMP7
    84da7030 Device        NetBt_Wins_Export
    83c8e700 Device        NTPNP_PCI0018
    849c3028 Device        0000004a
    83c8f778 Device        0000003e
20  84d66ea8 Device        WFP
    84935030 Device        NDMP8
    84b94028 Device        0000004b
    8331a1d8 Device        0000003f
21  84d8cb68 Device        NetbiosSmb
    849cd5f0 Device        nativewifip
    84831030 Device        NDMP9
    8498e028 Device        0000004c
22  85ba4488 SymbolicLink  {122CA9E8-FE91-47EB-AB70-2D45ADB79701}
    84add028 Device        0000004d
23  83c93a38 Device        MountPointManager
    9e1db030 Device        0000005b
    9fca5798 Device        rspndr
    84d87ed8 Device        Tdx
    84b8b028 Device        0000004e
24  84dcb6a8 Device        Nsi
    89d5f758 SymbolicLink  {541EFF09-BA28-42D1-A0BB-9342062D7CAE}
```

```
    85a63730 SymbolicLink  {852D1CB8-57E9-4A1E-A850-119CB69CD3EB}
    84dc2ed8 Device        WANARP
    835ab850 Device        0000005c
    9fd8ddf8 Device        LanmanServer
    9fd89a08 Device        Srv2
    83d914b8 Device        Mup
    84941998 Device        RaidPort0
25  873bedc8 SymbolicLink  {54950694-33A2-408C-9E06-ABBEB791E26F}
    84d87a20 Device        Udp
    85b11058 SymbolicLink  HarddiskVolumeShadowCopy{dfd6ace0-cc36-11dc-ab39-001b635fde5a}
    85b960b8 SymbolicLink  HarddiskVolumeShadowCopy{9c91b6f9-c701-11dc-921c-001b635fde5a}
26  85b15510 Directory     Harddisk0
    84d89958 Device        RawIp
    82f36250 Device        00000001
    873b56b0 SymbolicLink  NdisWanIp
27  84dc2dc0 Device        WANARPV6
    9fd7b0f0 Device        ASYNCMAC
    82effe70 Device        00000002
    9fc90db8 Device        lltdio
    83c70b78 Device        RawDisk
28  84904028 Device        USBFDO-0
    82effbf0 Device        00000003
    84b67ad8 Device        Null
    84985028 Device        1394BUS0
    85be9578 SymbolicLink  HarddiskVolumeShadowCopy{be08b2df-c1d2-11dc-8962-001b635fde5a}
    82f02420 Device        00000010
29  84dbb030 Device        NetBT_Tcpip_{852D1CB8-57E9-4A1E-A850-119CB69CD3EB}
    82eff970 Device        00000004
    84d48e78 Device        NXTIPSEC
    8490b028 Device        USBFDO-1
    82f02168 Device        00000011
30  9fd6cae8 Device        LanmanDatagramReceiver
    84830b30 Device        NdisTapi
    84cd6030 Device        NdisWan
    9fda0030 Device        AscKmd
    82eff6f0 Device        00000005
    85a129f8 Section       PhysicalMemory
    84d873f8 Device        Udp6
    8490d028 Device        USBFDO-2
    85af6d78 SymbolicLink  HarddiskVolumeShadowCopy{8a678ff3-ca05-11dc-928f-0016cbac5b3d}
    82f03f10 Device        00000012
31  9e1cf030 Device        NetBT_Tcpip_{93563980-2A26-408A-8A65-7A7BA760261B}
    84901ab8 Device        DxgKrnl
    a01f70c0 SymbolicLink  LanmanRedirector
    85bfba38 SymbolicLink  {0BB5FB04-E159-420F-9B86-0DF1BABFB53E}
    899fe5d0 Device        BthEnum0
    84940028 Device        USBFDO-3
    82f03c90 Device        00000013
    82f01030 Device        00000006
32  84c6aee8 Device        NamedPipe
    899fe228 Device        BthEnum1
    82f01db0 Device        00000007
    84942028 Device        USBFDO-4
    87249fe0 SymbolicLink  FtControl
    82f05968 Device        00000020
    82f03a10 Device        00000014
33  84c6c960 Device        Mailslot
    85bf5030 SymbolicLink  NdisWanIpv6
    82f056a8 Device        00000021
    82f03750 Device        00000015
    82f01b00 Device        00000008
34  84b64d28 Device        Afd
    83cd05c0 Device        FileInfo
    9fcb4ca8 Device        Ndisuio
    83c70a60 Device        RawCdRom
    82f053f0 Device        00000022
    82f03488 Device        00000016
    82f01848 Device        00000009
35  82f08c58 Device        00000030
    84d68f18 Device        WfpAle
```

```
    8725f678 SymbolicLink  ScsiPort0
    85af2a10 SymbolicLink  HarddiskVolumeShadowCopy{d6f7172a-b348-11dc-8e3d-001b635fde5a}
    82f06030 Device        00000023
    82f03208 Device        00000017
36  82f08998 Device        00000031
    87264030 SymbolicLink  ScsiPort1
    85a60ca8 SymbolicLink  HarddiskVolumeShadowCopy{f2961e0d-cc23-11dc-96da-001b635fde5a}
    82f06db0 Device        00000024
    82f04f10 Device        00000018
```

Driver Objects

```
0: kd> !object \Driver
Object: 85a62ea0  Type: (82efc1f8) Directory
    ObjectHeader: 85a62e88 (old version)
    HandleCount: 0  PointerCount: 89
    Directory Object: 85a07638  Name: Driver

    Hash Address  Type          Name
    ---- -------  ----          ----
     00  84b67150 Driver        Beep
         83db0408 Driver        KSecDD
         83343848 Driver        NDIS
     01  8987a968 Driver        KeyAgent
         84909d20 Driver        mouclass
     03  848f5eb0 Driver        kbdclass
     04  899bb310 Driver        BthPan
         8984c1c0 Driver        monitor
         84ccfea8 Driver        NDProxy
         84b62a38 Driver        VgaSave
         8331c1e0 Driver        msisadrv
     05  83ce1568 Driver        Ecache
         83c93c20 Driver        MountMgr
     06  8497c8f0 Driver        ohci1394
     07  9fc22d98 Driver        MacHALDriver
         9e1e8838 Driver        BTHUSB
     08  89880938 Driver        PEAUTH
         83c948c0 Driver        atapi
     09  83c94f38 Driver        volmgrx
     10  848386c8 Driver        tunmp
         84c6a1b8 Driver        RasAcd
         84da6e20 Driver        PSched
     11  8487e930 Driver        Win32k
         848f8528 Driver        usbuhci
         9e1dbf38 Driver        mouhid
         899bc828 Driver        BthEnum
     12  84838138 Driver        tunnel
         84921dc0 Driver        swenum
         849936f8 Driver        usbhub
     13  839353c8 Driver        SystemDump
         84cf0768 Driver        STHDA
         84b63c68 Driver        RDPCDD
         8490ef38 Driver        RasPppoe
         9fd23030 Driver        HTTP
     14  84908ad8 Driver        TermDD
     15  8490e550 Driver        Rasl2tp
     16  899c13b0 Driver        RFCOMM
     17  84929330 Driver        umbus
         899fecd0 Driver        KeyMagic
     18  9fda0cd8 Driver        secdrv
         83cd0030 Driver        CLFS
         84801338 Driver        crcdisk
         84d86d78 Driver        Smb
         848f5840 Driver        PptpMiniport
         82efe4b8 Driver        WMIxWDM
         82f09538 Driver        ACPI_HAL
     19  83d91c78 Driver        spldr
     20  8983e7e8 Driver        applebt
         89846758 Driver        IRRemoteFlt
     21  a18a5290 Driver        tcpipreg
         84d884f0 Driver        netbt
         9fc8fe60 Driver        NativeWifiP
     22  84b63a18 Driver        RDPENCDD
         849068e8 Driver        cdrom
         84929728 Driver        mssmbios
         848f8ad0 Driver        iScsiPrt
     23  84d91350 Driver        tdx
```

```
    9fca5680 Driver        rspndr
24  84c71b68 Driver        Tcpip
    84df3898 Driver        kbdhid
    9fd6ef38 Driver        mpsdrv
25  84dc04a8 Driver        nsiproxy
    83c93f38 Driver        volmgr
    83ce01c8 Driver        volsnap
26  847a31f8 Driver        intelppm
27  84dc28b0 Driver        Wanarpv6
    848fc6a0 Driver        yukonwlh
    9fc8e7d8 Driver        lltdio
    9fd7b4a8 Driver        AsyncMac
28  84b67bf0 Driver        Null
    848fc2a8 Driver        usbehci
29  83c8f658 Driver        pci
    83db0128 Driver        disk
30  83d91dd8 Driver        partmgr
    84830030 Driver        NdisTapi
    84830ca0 Driver        NdisWan
31  84906408 Driver        DXGKrnl
    84903858 Driver        HDAudBus
32  83c8ad50 Driver        Wdf01000
    83c8a668 Driver        ACPI
    899f1cd8 Driver        HidBth
33  82f3f300 Driver        PnpManager
34  8484fcf8 Driver        igfx
    84b64e40 Driver        AFD
    9fca21c8 Driver        Ndisuio
35  84df05a8 Driver        HidUsb
    84906518 Driver        athr
36  83c93940 Driver        intelide
```

FileSystem Objects

```
0: kd> !object \FileSystem
Object: 85a5d810  Type: (82efc1f8) Directory
    ObjectHeader: 85a5d7f8 (old version)
    HandleCount: 0  PointerCount: 29
    Directory Object: 85a07638  Name: FileSystem

    Hash Address  Type          Name
    ---- -------  ----          ----
     00  9fd3d430 Driver        srvnet
         83cb99e8 Driver        Ntfs
     01  84dbc2f0 Driver        NetBIOS
     03  84b664f8 Device        ExFatRecognizer
     05  84dc0180 Driver        rdbss
     10  9fd6c140 Driver        bowser
     15  84c6cab0 Driver        Msfs
     17  9fc692e0 Driver        mrxsmb
     18  84b66e60 Device        UdfsCdRomRecognizer
     19  9fd8df38 Driver        srv
     23  84dcd9b0 Driver        DfsC
     24  9fd89e90 Driver        srv2
         83d915d0 Driver        Mup
         83c70cc0 Driver        RAW
     25  84c6a460 Driver        Npfs
         84b60830 Driver        Fs_Rec
     26  85a5edd8 Directory     Filters
     30  9fd6df38 Driver        mrxsmb10
     31  8485a400 Driver        cdfs
     32  84b66620 Device        FatCdRomRecognizer
         84b60208 Device        CdfsRecognizer
         83cd0e98 Driver        FltMgr
     33  9fd872c8 Driver        mrxsmb20
     34  84b66748 Device        FatDiskRecognizer
         83cdeb18 Driver        FileInfo
     35  9fd7df38 Driver        MRxDAV
     36  84da0cc0 Driver        luafv
         84b66d38 Device        UdfsDiskRecognizer
```

Base Named Objects

```
0: kd> !object \BaseNamedObjects
Object: 89c00af8  Type: (82efc1f8) Directory
    ObjectHeader: 89c00ae0 (old version)
    HandleCount: 27  PointerCount: 148
    Directory Object: 85a07638  Name: BaseNamedObjects

    Hash Address  Type          Name
    ---- -------  ----          ----
     00  836a68b8 Mutant
C::Users:UserName:AppData:Local:Microsoft:Windows:Explorer:thumbcache_idx.db!ThumbnailCacheInit
         8b9cba70 SymbolicLink  Local
         9fd87958 Mutant        ZonesCacheCounterMutex
         89862928 Event         MSNRecoveryDone
         9fc52540 Event         AgentToWkssvcEvent
     01  89958d98 Event         TermSrvReadyEvent
         83753ab0 Mutant
C::Users:UserName:AppData:Local:Microsoft:Windows:Explorer:thumbcache_idx.db!rwWriterMutex
         9fd8c438 Mutant        ZonesLockedCacheCounterMutex
         a8b9ea68 Section       MMF_BITS_s
         a136f500 Section       UGATHERER
     02  836a6908 Mutant
C::Users:UserName:AppData:Local:Microsoft:Windows:Explorer:thumbcache_sr.db!dfMaintainer
         835676c8 Event         EVENT_READYROOT/CIMV2WMI SELF-INSTRUMENTATION EVENT PROVIDER
         9fd85b00 Event         BFE_Notify_Event_{f02e08c1-fbcf-4a2a-b4db-9f87edb5f3a9}
         899af7a0 Event         UMSServicesStarted
         89c00490 Directory     Restricted
     03  89ddec60 Section       __ComCatalogCache__
         8388dac0 Event         ad869ba1-7ad2-4712-a77e-a70ff958b125
         83663430 Event         ShutdownMSIDLLv262144.393232386
         9fd85738 Event         WkssvcToAgentStartEvent
         899b8d20 Event         ScNetDrvMsg
     04  a0002868 Section       windows_shell_global_counters
         835b2db0 Mutant        BJMON_MUTEX_INKLOW_USB001
         a1293320 Section       UrlZonesSM_SYSTEM
         89878318 Event         IPSEC_GP_REFRESH_EVENT
         8987ac78 Event         BFE_Notify_Event_{74f5d4ff-757f-4010-a964-4f899c7772d6}
         9fd03250 Event         {C2DB8232-E199-4AAF-A0A7-B86BFEA76BFC}ShellHWDetection
         9fd02690 Event         WLAN_POLICY_CHANGE_EVENT
     05  9e1d42b8 Event         WBEM_ESS_OPEN_FOR_BUSINESS
     06  83753a10 Mutant
C::Users:UserName:AppData:Local:Microsoft:Windows:Explorer:thumbcache_96.db!dfMaintainer
         835b2c20 Mutant        BJMON_MUTEX_PINIBIDI_USB001
         9fd2eea0 Event         NlaPrivatePort1
     07  838bf468 Event         {E540CA7A-9B37-495D-9979-274A3442B6D9}
         a01b88c0 Section       WSearchIdxPi
         899d9178 Event         NlaPrivatePort2
     08  8360ace8 Mutant        WindowsUpdateTracingMutex
         9fd2d220 Event         NlaPrivatePort3
         9e1d8848 Event         LSA_RPC_SERVER_ACTIVE
     09  9fc92618 Event         SENS Started Event
     10  83644768 Event         RestartMSIDLLv262144.393232386
         835b2b30 Mutant        BJMON_MUTEX_SENDRECVBIDIDATAFROMPORT_2_USB001
         a18b9b98 Mutant        SearchServiceMUT
     11  a18c2f60 Event         WMI_SysEvent_UnLodCtr
     12  9f8812e8 Section       mmGlobalPnpInfo
         83753a60 Mutant
C::Users:UserName:AppData:Local:Microsoft:Windows:Explorer:thumbcache_32.db!dfMaintainer
         836da690 Event         {B7F1F778-8315-4eb2-AC1E-5AFCAA603271}
         a18d03e0 Event         Go0:  ESENT Performance Data Schema Version 73
     13  a18f77d8 Event         WMI_RevAdap_ACK
         8997fb58 Event         SC_AutoStartComplete
         89877e90 Mutant        OOC State Mutex
     14  836a69a8 Mutant
C::Users:UserName:AppData:Local:Microsoft:Windows:Explorer:thumbcache_256.db!dfMaintainer
     15  9fc158f8 Event         ScmCreatedEvent
```

```
         9fd53678 Event         BFE_Notify_Event_{de0b5a43-2b41-44c2-8d45-5a0d8c91ef54}
     16  8b9fecd8 SymbolicLink  Global
         8360d298 ALPC Port     msctf.serverDefault1
         8396c5b8 Event         {BCB56B24-05BF-4C1C-92B4-0E6EDB63AD12}
         a18c2660 Event         WINMGMT_COREDLL_CANSHUTDOWN
     17  9fde2f08 ALPC Port     WDI_{24037b7f-9930-4807-9ac4-6229e9cad721}
         9f89cd98 Section       WseIdxPm
         a18f7798 Event         WMI_ProcessIdleTasksStart
     18  835b2d10 Mutant        BJMON_MUTEX_STARTDOC_USB001
     19  835b2c70 Mutant        BJMON_MUTEX_PORTEXCLUSIONINFO_USB001
         a282fb08 Section       IDA0:  ESENT Performance Data Schema Version 73
         a1350cf0 Section       UGthrSvcObj
         89958878 Event         WinSta0_DesktopSwitch
     20  835b2bd0 Mutant        BJMON_MUTEX_SENDRECVBIDIDATAFROMPORT_0_USB001
         9fdedcb0 Mutant        ZoneAttributeCacheCounterMutex
     21  899768c8 Event         SvcctrlStartEvent_A3752DX
         a189cdd0 Mutant        oleacc-msaa-loaded
         835b2d60 Mutant        BJMON_MUTEX_PRINTERNAME_USB001
         a18a7720 Event         W32TIME_NAMED_EVENT_SYSTIME_NOT_CORRECT
         89879d80 Event         BFE_Notify_Event_{bff40e3e-fd6e-442c-a744-bd66c6915392}
     22  835f6ba8 Event         000000000003812d_WlballoonKerberosNotificationEventName
         a18f5108 Mutant        FwtSqmSession10_S-1-5-18
         89878358 Event         IPSEC_POLICY_CHANGE_NOTIFY
         8994c730 Event         FirstWinlogonCheck
     23  835b2cc0 Mutant        BJMON_MUTEX_GETPRINTERDATAFROMPORT_USB001
     24  8363d180 Event
C::Users:UserName:AppData:Local:Microsoft:Windows:Explorer:thumbcache_idx.db!rwWriterEvent
         a00788a8 Section       SENS Information Cache
         89ddc4d8 Section       Debug.Trace.Memory.220
     25  836a6958 Mutant
C::Users:UserName:AppData:Local:Microsoft:Windows:Explorer:thumbcache_1024.db!dfMaintainer
         a2809520 Section       GDA:  ESENT Performance Data Schema Version 73
         9fd21e90 Mutant        RasPbFile
         a18f7758 Event         WMI_ProcessIdleTasksComplete
         9fd845c0 Event         BFE_Notify_Event_{feea4a79-8cb1-46d7-9f2c-c8af8ce7e38d}
     26  836eee70 Event         RNAdminShutdownEvent-75A2A39B-2537-418c-A295-D3DEF8F26C3B
         835bbbc8 Mutant        BJMON_MUTEX_USB001
         9fd6c030 Event         BFE_Notify_Event_{c1d41011-bda8-4c36-ae1d-105bbdce6494}
     28  a18c2358 Event         WINMGMT_PROVIDER_CANSHUTDOWN
         a18c2f20 Event         WMI_RevAdap_Set
         9fc97910 Event         ConsoleSessionCreation
         89d72c60 Section       Debug.Memory.220
     29  9fd971c8 Mutant        ZonesCounterMutex
         9f9cd4f8 Section       RotHintTable
         84da07b8 Event         PnP_No_Pending_Install_Clients
         9fcf49b0 Job           WmiProviderSubSystemHostJob
     30  a2827c60 Section       Wmi Provider Sub System Counters
         847fd2e8 Event         RouterPreInitEvent
         89c00610 SymbolicLink  Session
         84da07f8 Event         PnP_No_Pending_Install_Events
         a13a0138 Section       SqmData_FwtSqmSession10_S-1-5-18
         8485e7f8 Event         IPSEC_POLICY_CHANGE_EVENT
         9fd322f8 Event         WkssvcToAgentStopEvent
         9fd15a10 Event         WiaServiceStarted
         9fc17fe0 Mutant        {A3BD3259-3E4F-428a-84C8-F0463A9D3EB5}
     31  9fd7f558 Event         wkssvc:  MUP finished initializing event
     32  8356bb38 Event         EVENT_READYROOT/CIMV2PROVIDERSUBSYSTEM
         a18d1ed8 Mutant        Instance0:  ESENT Performance Data Schema Version 73
         a18d03a0 Event         Ready0:  ESENT Performance Data Schema Version 73
         9fd96540 Event         NlaPrivatePort
         9fca0208 Event         AudioSrv_CanAcceptMMCClient
     33  9fc92468 Event         TabletHardwarePresent
         8356bb78 Event         EVENT_READYROOT/CIMV2SCM EVENT PROVIDER
         a1350f88 Section       UGathererObj
     35  835b2b80 Mutant        BJMON_MUTEX_SENDRECVBIDIDATAFROMPORT_1_USB001
     36  a18de9f0 Event         WMI_SysEvent_LodCtr
         839417b0 Event         {325C9375-651F-4EAD-8778-0D47C6C9C5F6}
         83650750 Event         IGFXTRAY
         a136f430 Section       UGTHRSVC
         9fd7ed58 Event         BFE_Notify_Event_{9ff11d1b-1c35-4a4c-9d10-f8251fa2e02e}
```

```
         9f9d4478 Section       {A64C7F33-DA35-459b-96CA-63B51FB0CDB9}
```

Kernel Objects

```
0: kd> !object \KernelObjects
Object: 85a071d0  Type: (82efc1f8) Directory
    ObjectHeader: 85a071b8 (old version)
    HandleCount: 0  PointerCount: 19
    Directory Object: 85a07638  Name: KernelObjects

    Hash Address  Type          Name
    ---- -------  ----          ----
     02  82f406c8 Event         HighCommitCondition
     04  82f40848 Event         HighMemoryCondition
     10  82f40788 Event         LowNonPagedPoolCondition
     11  82f40748 Event         HighNonPagedPoolCondition
     17  82f40708 Event         LowCommitCondition
     20  82f35f78 Event         SuperfetchParametersChanged
         82f36d48 Event         BootLoaderTraceReady
     23  8487eb78 Session       Session0
         82f35ef8 Event         PrefetchTracesReady
     24  8993fa88 Session       Session1
     25  82f35f38 Event         SuperfetchScenarioNotify
         82f40808 Event         LowPagedPoolCondition
     26  82f407c8 Event         HighPagedPoolCondition
         82f40648 Event         MemoryErrors
     28  82f35eb8 Event         SuperfetchTracesReady
     32  82f40bf8 Event         LowMemoryCondition
         85a09030 KeyedEvent    CritSecOutOfMemoryEvent
     34  82f40688 Event         MaximumCommitCondition
```

Loaded System Modules

```
0: kd> lmv
start    end        module name
80204000 8020d000   WMILIB     (deferred)
    Image path: \SystemRoot\system32\drivers\WMILIB.SYS
    Image name: WMILIB.SYS
    Timestamp:        Thu Nov 02 08:54:53 2006 (4549B25D)
    CheckSum:         00004EA9
    ImageSize:        00009000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
8020d000 8021a000   WDFLDR     (deferred)
    Image path: \SystemRoot\system32\drivers\WDFLDR.SYS
    Image name: WDFLDR.SYS
    Timestamp:        Thu Nov 02 08:54:05 2006 (4549B22D)
    CheckSum:         000124C2
    ImageSize:        0000D000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
8021a000 80255000   CLFS       (deferred)
    Image path: \SystemRoot\system32\CLFS.SYS
    Image name: CLFS.SYS
    Timestamp:        Thu Nov 02 08:30:52 2006 (4549ACBC)
    CheckSum:         00041B8F
    ImageSize:        0003B000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
80255000 8025d000   BOOTVID    (deferred)
    Image path: \SystemRoot\system32\BOOTVID.dll
    Image name: BOOTVID.dll
    Timestamp:        Thu Nov 02 09:39:29 2006 (4549BCD1)
    CheckSum:         0000C572
    ImageSize:        00008000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
8025d000 80266000   PSHED      (deferred)
    Image path: \SystemRoot\system32\PSHED.dll
    Image name: PSHED.dll
    Timestamp:        Thu Nov 02 09:42:51 2006 (4549BD9B)
    CheckSum:         0001395B
    ImageSize:        00009000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
80266000 802c6000   mcupdate_GenuineIntel   (deferred)
    Image path: \SystemRoot\system32\mcupdate_GenuineIntel.dll
    Image name: mcupdate_GenuineIntel.dll
    Timestamp:        Tue Apr 24 04:40:05 2007 (462D7C15)
    CheckSum:         00065549
    ImageSize:        00060000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
802c6000 802ce000   kdcom      (deferred)
    Image path: kdcom.dll
    Image name: kdcom.dll
    Timestamp:        Thu Nov 02 09:42:20 2006 (4549BD7C)
    CheckSum:         00009994
    ImageSize:        00008000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
80400000 8040e000   PCIIDEX    (deferred)
    Image path: \SystemRoot\system32\drivers\PCIIDEX.SYS
    Image name: PCIIDEX.SYS
    Timestamp:        Wed Oct 24 03:02:39 2007 (471EA7BF)
    CheckSum:         0000DFE7
    ImageSize:        0000E000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
8040e000 80415000   intelide   (deferred)
    Image path: \SystemRoot\system32\drivers\intelide.sys
    Image name: intelide.sys
    Timestamp:        Wed Oct 24 03:02:40 2007 (471EA7C0)
    CheckSum:         0000BFB0
    ImageSize:        00007000
    File version:     6.0.6000.16584
    Product version:  6.0.6000.16584
    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:   6.0.6000.16584
    FileVersion:      6.0.6000.16584 (vista_gdr.071023-1545)
    FileDescription:  Intel PCI IDE Driver
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
80415000 80425000   mountmgr   (deferred)
    Image path: \SystemRoot\System32\drivers\mountmgr.sys
    Image name: mountmgr.sys
    Timestamp:        Thu Nov 02 08:51:06 2006 (4549B17A)
    CheckSum:         0000F0B3
    ImageSize:        00010000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
80425000 80434000   volmgr     (pdb symbols)
c:\mss\volmgr.pdb\3C43C06A961143719A6DF9F0B2A9699C1\volmgr.pdb
    Loaded symbol image file: volmgr.sys
    Image path: \SystemRoot\system32\drivers\volmgr.sys
    Image name: volmgr.sys
    Timestamp:        Thu Nov 02 08:51:44 2006 (4549B1A0)
    CheckSum:         00015FAA
    ImageSize:        0000F000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
80434000 80459000   pci        (pdb symbols)
c:\mss\pci.pdb\A5E895C861984D7393087EB0459E7FE01\pci.pdb
    Loaded symbol image file: pci.sys
    Image path: \SystemRoot\system32\drivers\pci.sys
    Image name: pci.sys
    Timestamp:        Thu Nov 02 08:35:13 2006 (4549ADC1)
    CheckSum:         0002E8CB
    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:        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.
80459000 80461000   msisadrv   (deferred)
    Image path: \SystemRoot\system32\drivers\msisadrv.sys
    Image name: msisadrv.sys
    Timestamp:        Thu Nov 02 08:35:08 2006 (4549ADBC)
    CheckSum:         0000D703
    ImageSize:        00008000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
80461000 804a4000   acpi       (pdb symbols)
c:\mss\acpi.pdb\55BB5363FCD842CE9CB57D88182AF8E61\acpi.pdb
    Loaded symbol image file: acpi.sys
    Image path: \SystemRoot\system32\drivers\acpi.sys
    Image name: acpi.sys
    Timestamp:        Fri Aug 31 01:57:46 2007 (46D7678A)
    CheckSum:         00042BC2
    ImageSize:        00043000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
804a4000 8051f000   Wdf01000   (pdb symbols)
c:\mss\Wdf01000.pdb\824746676E3E40DAB196832C3EA41D781\Wdf01000.pdb
    Loaded symbol image file: Wdf01000.sys
```

```
    Image path: \SystemRoot\system32\drivers\Wdf01000.sys
    Image name: Wdf01000.sys
    Timestamp:        Thu Nov 02 08:54:18 2006 (4549B23A)
    CheckSum:         0007DC5C
    ImageSize:        0007B000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
8051f000 80600000   CI         (deferred)
    Image path: \SystemRoot\system32\CI.dll
    Image name: CI.dll
    Timestamp:        Thu Nov 02 09:42:45 2006 (4549BD95)
    CheckSum:         000A28B7
    ImageSize:        000E1000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
80600000 80609000   crcdisk    (deferred)
    Image path: \SystemRoot\system32\drivers\crcdisk.sys
    Image name: crcdisk.sys
    Timestamp:        Thu Nov 02 08:52:27 2006 (4549B1CB)
    CheckSum:         00006D96
    ImageSize:        00009000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
80609000 80618000   partmgr    (deferred)
    Image path: \SystemRoot\System32\drivers\partmgr.sys
    Image name: partmgr.sys
    Timestamp:        Thu Nov 02 08:51:47 2006 (4549B1A3)
    CheckSum:         00015E29
    ImageSize:        0000F000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
80618000 80620000   spldr      (deferred)
    Image path: \SystemRoot\System32\Drivers\spldr.sys
    Image name: spldr.sys
    Timestamp:        Wed Oct 25 23:40:44 2006 (453FE7EC)
    CheckSum:         0000BC5E
    ImageSize:        00008000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
80620000 8064b000   msrpc      (pdb symbols)
c:\mss\msrpc.pdb\AE709AEDF7494AE2A33E2E7499F9777B1\msrpc.pdb
    Loaded symbol image file: msrpc.sys
    Image path: \SystemRoot\system32\drivers\msrpc.sys
    Image name: msrpc.sys
    Timestamp:        Thu Nov 02 08:50:16 2006 (4549B148)
    CheckSum:         00030F7F
    ImageSize:        0002B000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
8064b000 8074f000   ndis       (pdb symbols)
c:\mss\ndis.pdb\93E7C38CE3454B78AA882083F442C17A2\ndis.pdb
    Loaded symbol image file: ndis.sys
    Image path: \SystemRoot\system32\drivers\ndis.sys
    Image name: ndis.sys
    Timestamp:        Thu Nov 02 08:57:33 2006 (4549B2FD)
    CheckSum:         000889FD
    ImageSize:        00104000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
8074f000 8075f000   fileinfo   (deferred)
    Image path: \SystemRoot\system32\drivers\fileinfo.sys
    Image name: fileinfo.sys
    Timestamp:        Thu Nov 02 08:36:47 2006 (4549AE1F)
    CheckSum:         0001C10F
    ImageSize:        00010000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
8075f000 80790000   fltmgr     (pdb symbols)
c:\mss\fltMgr.pdb\FA42D1F108C1425599238F576CBDDE831\fltMgr.pdb
    Loaded symbol image file: fltmgr.sys
    Image path: \SystemRoot\system32\drivers\fltmgr.sys
    Image name: fltmgr.sys
    Timestamp:        Thu Nov 02 08:30:58 2006 (4549ACC2)
    CheckSum:         00035410
    ImageSize:        00031000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
80790000 807ae000   ataport    (deferred)
    Image path: \SystemRoot\system32\drivers\ataport.SYS
```

```
    Image name: ataport.SYS
    Timestamp:        Wed Oct 24 03:02:40 2007 (471EA7C0)
    CheckSum:         0001C121
    ImageSize:        0001E000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
807ae000 807b6000   atapi      (deferred)
    Image path: \SystemRoot\system32\drivers\atapi.sys
    Image name: atapi.sys
    Timestamp:        Wed Oct 24 03:02:39 2007 (471EA7BF)
    CheckSum:         00009360
    ImageSize:        00008000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
807b6000 80800000   volmgrx    (deferred)
    Image path: \SystemRoot\System32\drivers\volmgrx.sys
    Image name: volmgrx.sys
    Timestamp:        Thu Nov 02 08:51:54 2006 (4549B1AA)
    CheckSum:         0004955F
    ImageSize:        0004A000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
81a10000 81a1f000   mup        (pdb symbols)
c:\mss\mup.pdb\C00C2E9D8FB24D3C9ADA9A3DC6D718D02\mup.pdb
    Loaded symbol image file: mup.sys
    Image path: \SystemRoot\System32\Drivers\mup.sys
    Image name: mup.sys
    Timestamp:        Thu Nov 02 08:31:04 2006 (4549ACC8)
    CheckSum:         00019B87
    ImageSize:        0000F000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
81a1f000 81a55000   volsnap    (pdb symbols)
c:\mss\volsnap.pdb\9EDD0FABCC2E4E4098BB345F0F2656A41\volsnap.pdb
    Loaded symbol image file: volsnap.sys
    Image path: \SystemRoot\system32\drivers\volsnap.sys
    Image name: volsnap.sys
    Timestamp:        Fri Oct 26 03:04:17 2007 (47214B21)
    CheckSum:         0003B087
    ImageSize:        00036000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
81a55000 81abf000   ksecdd     (deferred)
    Image path: \SystemRoot\System32\Drivers\ksecdd.sys
    Image name: ksecdd.sys
    Timestamp:        Thu Nov 02 08:43:45 2006 (4549AFC1)
    CheckSum:         00064045
    ImageSize:        0006A000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
81abf000 81bc7000   Ntfs       (pdb symbols)
c:\mss\ntfs.pdb\8A183E745D464A3D831F8BE153F794AE2\ntfs.pdb
    Loaded symbol image file: Ntfs.sys
    Image path: \SystemRoot\System32\Drivers\Ntfs.sys
    Image name: Ntfs.sys
    Timestamp:        Fri Oct 26 02:40:39 2007 (47214597)
    CheckSum:         0010DD91
    ImageSize:        00108000
    File version:     6.0.6000.16586
    Product version:  6.0.6000.16586
    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:   6.0.6000.16586
    FileVersion:      6.0.6000.16586 (vista_gdr.071025-1510)
    FileDescription:  NT File System Driver
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
81bc7000 81c00000   NETIO      (deferred)
    Image path: \SystemRoot\system32\drivers\NETIO.SYS
    Image name: NETIO.SYS
```

```
    Timestamp:        Fri Sep 28 03:46:49 2007 (46FC6B19)
    CheckSum:         00044709
    ImageSize:        00039000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
81c00000 81fa1000   nt         (pdb symbols)
c:\mss\ntkrpamp.pdb\E42190E0396449A3882CB6F322CB176E2\ntkrpamp.pdb
    Loaded symbol image file: ntkrpamp.exe
    Image path: ntkrpamp.exe
    Image name: ntkrpamp.exe
    Timestamp:        Wed Oct 10 02:48:02 2007 (470C2F52)
    CheckSum:         00365AD7
    ImageSize:        003A1000
    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:     ntkrpamp.exe
    OriginalFilename: ntkrpamp.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.
81fa1000 81fd5000   hal        (deferred)
    Image path: halmacpi.dll
    Image name: halmacpi.dll
    Timestamp:        Thu Nov 02 08:30:18 2006 (4549AC9A)
    CheckSum:         00027A6F
    ImageSize:        00034000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
84e71000 84e80000   raspppoe   (deferred)
    Image path: \SystemRoot\system32\DRIVERS\raspppoe.sys
    Image name: raspppoe.sys
    Timestamp:        Thu Nov 02 08:58:12 2006 (4549B324)
    CheckSum:         00015C59
    ImageSize:        0000F000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
84e80000 84e89000   kbdhid     (deferred)
    Image path: \SystemRoot\system32\DRIVERS\kbdhid.sys
    Image name: kbdhid.sys
    Timestamp:        Thu Nov 02 08:51:12 2006 (4549B180)
    CheckSum:         0000FAC0
    ImageSize:        00009000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
84fa9000 84fca000   CLASSPNP   (deferred)
    Image path: \SystemRoot\system32\drivers\CLASSPNP.SYS
    Image name: CLASSPNP.SYS
    Timestamp:        Thu Nov 02 08:51:34 2006 (4549B196)
    CheckSum:         00028767
    ImageSize:        00021000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
84fca000 84fdb000   disk       (deferred)
    Image path: \SystemRoot\system32\drivers\disk.sys
    Image name: disk.sys
    Timestamp:        Thu Nov 02 08:51:40 2006 (4549B19C)
    CheckSum:         00016517
    ImageSize:        00011000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
84fdb000 85000000   ecache     (pdb symbols)
c:\mss\ecache.pdb\E083A5C0DE294A18A079F46C3AA36E561\ecache.pdb
    Loaded symbol image file: ecache.sys
    Image path: \SystemRoot\System32\drivers\ecache.sys
    Image name: ecache.sys
    Timestamp:        Thu Nov 02 08:52:42 2006 (4549B1DA)
    CheckSum:         0002A2CD
    ImageSize:        00025000
```

```
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
85838000 85846000   intelppm   (deferred)
    Image path: \SystemRoot\system32\DRIVERS\intelppm.sys
    Image name: intelppm.sys
    Timestamp:        Thu Nov 02 08:30:18 2006 (4549AC9A)
    CheckSum:         00013132
    ImageSize:        0000E000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
858a4000 858b4000   NDProxy    (pdb symbols)
c:\mss\ndproxy.pdb\4FDCCADCB2FF4BCF9FBBEDDA0BE20F3E1\ndproxy.pdb
    Loaded symbol image file: NDProxy.SYS
    Image path: \SystemRoot\System32\Drivers\NDProxy.SYS
    Image name: NDProxy.SYS
    Timestamp:        Wed Jul 04 02:28:13 2007 (468AF7AD)
    CheckSum:         00013454
    ImageSize:        00010000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
858d4000 858e4000   lltdio     (deferred)
    Image path: \SystemRoot\system32\DRIVERS\lltdio.sys
    Image name: lltdio.sys
    Timestamp:        Thu Nov 02 08:56:48 2006 (4549B2D0)
    CheckSum:         00010AFF
    ImageSize:        00010000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
85924000 85934000   HIDCLASS   (pdb symbols)
c:\mss\hidclass.pdb\93501CB539964D8AA0AA9E4183C4ED591\hidclass.pdb
    Loaded symbol image file: HIDCLASS.SYS
    Image path: \SystemRoot\system32\DRIVERS\HIDCLASS.SYS
    Image name: HIDCLASS.SYS
    Timestamp:        Thu Nov 02 08:55:00 2006 (4549B264)
    CheckSum:         00014363
    ImageSize:        00010000
    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.
85994000 859a3280   ohci1394   (deferred)
    Image path: \SystemRoot\system32\DRIVERS\ohci1394.sys
    Image name: ohci1394.sys
    Timestamp:        Thu Nov 02 08:55:16 2006 (4549B274)
    CheckSum:         0000FA1F
    ImageSize:        0000F280
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
85c09000 85c16000   watchdog   (pdb symbols)
c:\mss\watchdog.pdb\F21C61867E77408497C5C21F550BB8A41\watchdog.pdb
    Loaded symbol image file: watchdog.sys
    Image path: \SystemRoot\System32\drivers\watchdog.sys
    Image name: watchdog.sys
    Timestamp:        Thu Nov 02 08:37:44 2006 (4549AE58)
    CheckSum:         0000E618
    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:        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.
85c16000 85c21000   tunnel     (deferred)
    Image path: \SystemRoot\system32\DRIVERS\tunnel.sys
    Image name: tunnel.sys
    Timestamp:        Thu Jun 07 03:57:03 2007 (466773FF)
    CheckSum:         0000A64F
    ImageSize:        0000B000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
85c27000 85c32000   dump_dumpata   (deferred)
    Image path: \SystemRoot\System32\Drivers\dump_dumpata.sys
    Image name: dump_dumpata.sys
    Timestamp:        Thu Nov 02 08:51:34 2006 (4549B196)
    CheckSum:         0000C948
    ImageSize:        0000B000
    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.
85c35000 85c42000   crashdmp   (deferred)
    Image path: \SystemRoot\System32\Drivers\crashdmp.sys
    Image name: crashdmp.sys
    Timestamp:        Thu Nov 02 08:51:36 2006 (4549B198)
    CheckSum:         0001054E
    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:        3.7 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.
85c5d000 85c66000   Fs_Rec     (deferred)
    Image path: \SystemRoot\System32\Drivers\Fs_Rec.SYS
    Image name: Fs_Rec.SYS
    Timestamp:        Tue Apr 17 02:26:39 2007 (4624224F)
    CheckSum:         000083AB
    ImageSize:        00009000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
85c6f000 85c78000   rasacd     (pdb symbols)
c:\mss\rasacd.pdb\CF7B92EB750D4AEDB23C382FDC0901B91\rasacd.pdb
    Loaded symbol image file: rasacd.sys
    Image path: \SystemRoot\System32\DRIVERS\rasacd.sys
    Image name: rasacd.sys
    Timestamp:        Thu Nov 02 08:58:13 2006 (4549B325)
    CheckSum:         0000E90B
```

```
    ImageSize:        00009000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
85c78000 85c81000   asyncmac   (deferred)
    Image path: \SystemRoot\system32\DRIVERS\asyncmac.sys
    Image name: asyncmac.sys
    Timestamp:        Thu Nov 02 08:58:10 2006 (4549B322)
    CheckSum:         000085B4
    ImageSize:        00009000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
85cc0000 85cc9000   tunmp      (pdb symbols)
c:\mss\tunmp.pdb\B967B309486B4AC6A6408E35531A876B1\tunmp.pdb
    Loaded symbol image file: tunmp.sys
    Image path: \SystemRoot\system32\DRIVERS\tunmp.sys
    Image name: tunmp.sys
    Timestamp:        Thu Jun 07 03:56:53 2007 (466773F5)
    CheckSum:         0000774F
    ImageSize:        00009000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
85cc9000 85cd2000   hidusb     (pdb symbols)
c:\mss\hidusb.pdb\760200290AB0432D84FA9CF9BDAC46301\hidusb.pdb
    Loaded symbol image file: hidusb.sys
    Image path: \SystemRoot\system32\DRIVERS\hidusb.sys
    Image name: hidusb.sys
    Timestamp:        Thu Nov 02 08:55:01 2006 (4549B265)
    CheckSum:         0000C577
    ImageSize:        00009000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
85cd2000 85cd3980   MacHALDriver   (deferred)
    Image path: \??\C:\Windows\system32\drivers\MacHALDriver.sys
    Image name: MacHALDriver.sys
    Timestamp:        Tue Jul 10 07:18:11 2007 (469324A3)
    CheckSum:         00002473
    ImageSize:        00001980
    File version:     6.103.0.9
    Product version:  2.0.0.0
    File flags:       8 (Mask 3F) Private
    File OS:          40004 NT Win32
    File type:        0.0 Unknown
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      Apple Inc.
    InternalName:     MacHALDriver.sys
    OriginalFilename: MacHALDriver.sys
    ProductVersion:   2.0
    FileVersion:      6.103.0.9
    FileDescription:  Mac HAL Driver
    LegalCopyright:   Copyright © 2006-2007 Apple Inc. All Rights Reserved.
85cd6000 85cd7380   swenum     (deferred)
    Image path: \SystemRoot\system32\DRIVERS\swenum.sys
    Image name: swenum.sys
    Timestamp:        Thu Nov 02 08:51:15 2006 (4549B183)
    CheckSum:         00007AE5
    ImageSize:        00001380
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
85ce4000 85ce5700   USBD       (deferred)
    Image path: \SystemRoot\system32\DRIVERS\USBD.SYS
    Image name: USBD.SYS
    Timestamp:        Thu Nov 02 08:55:00 2006 (4549B264)
    CheckSum:         000034E1
    ImageSize:        00001700
    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.
85cec000 85ced300   KeyAgent   (deferred)
    Image path: \??\C:\Windows\system32\drivers\KeyAgent.sys
    Image name: KeyAgent.sys
    Timestamp:        Tue Aug 28 01:27:14 2007 (46D36BE2)
    CheckSum:         0000DB71
    ImageSize:        00001300
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
85cf0000 85cf1f80   applebt    (deferred)
    Image path: \SystemRoot\system32\DRIVERS\applebt.sys
    Image name: applebt.sys
    Timestamp:        Thu Jun 28 00:08:31 2007 (4682EDEF)
    CheckSum:         0000CB50
    ImageSize:        00001F80
    File version:     2.0.0.1
    Product version:  2.0.0.0
    File flags:       8 (Mask 3F) Private
    File OS:          40004 NT Win32
    File type:        0.0 Unknown
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      Apple Inc.
    ProductName:      Boot Camp
    InternalName:     AppleBt.sys
    OriginalFilename: AppleBt.sys
    ProductVersion:   2.0
    FileVersion:      2.0.0.1
    FileDescription:  Apple Bluetooth
    LegalCopyright:   Copyright © 2006-2007 Apple Inc. All Rights Reserved.
85d54000 85d5c000   dump_atapi   (deferred)
    Image path: \SystemRoot\System32\Drivers\dump_atapi.sys
    Image name: dump_atapi.sys
    Timestamp:        Wed Oct 24 03:02:39 2007 (471EA7BF)
    CheckSum:         00009360
    ImageSize:        00008000
    File version:     6.0.6000.16584
    Product version:  6.0.6000.16584
    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:   6.0.6000.16584
    FileVersion:      6.0.6000.16584 (vista_gdr.071023-1545)
    FileDescription:  ATAPI IDE Miniport Driver
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
85d5c000 85d64000   RDPCDD     (deferred)
    Image path: \SystemRoot\System32\DRIVERS\RDPCDD.sys
    Image name: RDPCDD.sys
    Timestamp:        Thu Nov 02 09:02:01 2006 (4549B409)
    CheckSum:         000095C6
    ImageSize:        00008000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
85d6c000 85d74000   rdpencdd   (deferred)
    Image path: \SystemRoot\system32\drivers\rdpencdd.sys
    Image name: rdpencdd.sys
    Timestamp:        Thu Nov 02 09:02:01 2006 (4549B409)
    CheckSum:         0000CDEE
    ImageSize:        00008000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
85d74000 85d7c000   mouhid     (deferred)
    Image path: \SystemRoot\system32\DRIVERS\mouhid.sys
```

```
    Image name: mouhid.sys
    Timestamp:        Thu Nov 02 08:51:12 2006 (4549B180)
    CheckSum:         00005315
    ImageSize:        00008000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
87c08000 87c13000   TDI        (deferred)
    Image path: \SystemRoot\system32\DRIVERS\TDI.SYS
    Image name: TDI.SYS
    Timestamp:        Thu Nov 02 08:58:46 2006 (4549B346)
    CheckSum:         0000B17F
    ImageSize:        0000B000
    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.
87c13000 87c1e000   usbuhci    (pdb symbols)
c:\mss\usbuhci.pdb\FEDB826FDB70437D9D0E8D2BD9E38C7D1\usbuhci.pdb
    Loaded symbol image file: usbuhci.sys
    Image path: \SystemRoot\system32\DRIVERS\usbuhci.sys
    Image name: usbuhci.sys
    Timestamp:        Thu Nov 02 08:55:04 2006 (4549B268)
    CheckSum:         0000F7F0
    ImageSize:        0000B000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
87c1e000 87c30000   HDAudBus   (deferred)
    Image path: \SystemRoot\system32\DRIVERS\HDAudBus.sys
    Image name: HDAudBus.sys
    Timestamp:        Sat Mar 24 18:54:34 2007 (460573EA)
    CheckSum:         0001A527
    ImageSize:        00012000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
87c30000 87c3e000   usbehci    (pdb symbols)
c:\mss\usbehci.pdb\5BEBE90C757648A9BB0311B6039BACE11\usbehci.pdb
    Loaded symbol image file: usbehci.sys
    Image path: \SystemRoot\system32\DRIVERS\usbehci.sys
    Image name: usbehci.sys
    Timestamp:        Thu Nov 02 08:55:04 2006 (4549B268)
    CheckSum:         00017319
    ImageSize:        0000E000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
87c3e000 87c4b080   1394BUS    (deferred)
    Image path: \SystemRoot\system32\DRIVERS\1394BUS.SYS
    Image name: 1394BUS.SYS
    Timestamp:        Thu Nov 02 08:55:12 2006 (4549B270)
    CheckSum:         0001A682
    ImageSize:        0000D080
    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:     1394bus.sys
    OriginalFilename: 1394bus.sys
    ProductVersion:   6.0.6000.16386
    FileVersion:      6.0.6000.16386 (vista_rtm.061101-2205)
```

```
    FileDescription:  1394 Bus Device Driver
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
87c4c000 87c5a000   Npfs       (pdb symbols)
c:\mss\npfs.pdb\449D383E08CB4766933BE4760B85AD4B1\npfs.pdb
    Loaded symbol image file: Npfs.SYS
    Image path: \SystemRoot\System32\Drivers\Npfs.SYS
    Image name: Npfs.SYS
    Timestamp:        Thu Nov 02 08:30:57 2006 (4549ACC1)
    CheckSum:         00016EA8
    ImageSize:        0000E000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
87c5a000 87c68000   netbios    (deferred)
    Image path: \SystemRoot\system32\DRIVERS\netbios.sys
    Image name: netbios.sys
    Timestamp:        Thu Nov 02 08:57:26 2006 (4549B2F6)
    CheckSum:         0000F480
    ImageSize:        0000E000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
87c68000 87c72000   mssmbios   (deferred)
    Image path: \SystemRoot\system32\DRIVERS\mssmbios.sys
    Image name: mssmbios.sys
    Timestamp:        Thu Nov 02 08:35:13 2006 (4549ADC1)
    CheckSum:         00010CCD
    ImageSize:        0000A000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
87c72000 87cb0000   yk60x86    (deferred)
    Image path: \SystemRoot\system32\DRIVERS\yk60x86.sys
    Image name: yk60x86.sys
    Timestamp:        Fri Mar 23 10:11:54 2007 (4603A7EA)
    CheckSum:         0004047A
    ImageSize:        0003E000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
87d4c000 87d50080   IRFilter   (no symbols)
    Loaded symbol image file: IRFilter.sys
    Image path: \SystemRoot\system32\DRIVERS\IRFilter.sys
    Image name: IRFilter.sys
    Timestamp:        Tue Jul 17 01:26:21 2007 (469C0CAD)
    CheckSum:         00009D5D
    ImageSize:        00004080
    File version:     2.0.0.1
    Product version:  2.0.0.0
    File flags:       0 (Mask 17)
    File OS:          4 Unknown Win32
    File type:        0.0 Unknown
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      Apple Inc.
    ProductName:      Boot Camp
    InternalName:     IRFilter
    OriginalFilename: IRFilter.sys
    ProductVersion:   2.0
    FileVersion:      2.0.0.1
    FileDescription:  IR Receiver Driver
    LegalCopyright:   Copyright © 2006-2007 Apple Inc. All Rights Reserved.
87dcf000 87dd6000   Null       (deferred)
    Image path: \SystemRoot\System32\Drivers\Null.SYS
    Image name: Null.SYS
    Timestamp:        Thu Nov 02 08:51:05 2006 (4549B179)
    CheckSum:         0000ED81
    ImageSize:        00007000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
87dd6000 87ddd000   Beep       (deferred)
    Image path: \SystemRoot\System32\Drivers\Beep.SYS
    Image name: Beep.SYS
    Timestamp:        Thu Nov 02 08:51:03 2006 (4549B177)
    CheckSum:         0000F272
    ImageSize:        00007000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
87ddd000 87de3380   HIDPARSE   (deferred)
    Image path: \SystemRoot\system32\DRIVERS\HIDPARSE.SYS
```

```
    Image name: HIDPARSE.SYS
    Timestamp:        Thu Nov 02 08:55:00 2006 (4549B264)
    CheckSum:         00008A44
    ImageSize:        00006380
    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.
88013000 8801e000   mouclass   (pdb symbols)
c:\mss\mouclass.pdb\D033CE0590EA470AB0A9E4BD547429391\mouclass.pdb
    Loaded symbol image file: mouclass.sys
    Image path: \SystemRoot\system32\DRIVERS\mouclass.sys
    Image name: mouclass.sys
    Timestamp:        Thu Nov 02 08:51:09 2006 (4549B17D)
    CheckSum:         0000DE48
    ImageSize:        0000B000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
8801e000 88029000   kbdclass   (pdb symbols)
c:\mss\kbdclass.pdb\C982444210F84B69BF2DC147CDCBCCAF1\kbdclass.pdb
    Loaded symbol image file: kbdclass.sys
    Image path: \SystemRoot\system32\DRIVERS\kbdclass.sys
    Image name: kbdclass.sys
    Timestamp:        Thu Nov 02 08:51:09 2006 (4549B17D)
    CheckSum:         00009F23
    ImageSize:        0000B000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
88029000 88038000   termdd     (deferred)
    Image path: \SystemRoot\system32\DRIVERS\termdd.sys
    Image name: termdd.sys
    Timestamp:        Thu Nov 02 09:02:00 2006 (4549B408)
    CheckSum:         00016581
    ImageSize:        0000F000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
88038000 88045000   umbus      (deferred)
    Image path: \SystemRoot\system32\DRIVERS\umbus.sys
    Image name: umbus.sys
    Timestamp:        Thu Nov 02 08:55:24 2006 (4549B27C)
    CheckSum:         0000A198
    ImageSize:        0000D000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
88045000 88058000   raspptp    (pdb symbols)
c:\mss\raspptp.pdb\B88F02B042D0402BAA9F7DE82A2040322\raspptp.pdb
    Loaded symbol image file: raspptp.sys
    Image path: \SystemRoot\system32\DRIVERS\raspptp.sys
    Image name: raspptp.sys
    Timestamp:        Thu Nov 02 08:58:14 2006 (4549B326)
    CheckSum:         00018677
    ImageSize:        00013000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
88058000 8807b000   ndiswan    (pdb symbols)
c:\mss\ndiswan.pdb\EEA80C8DD67249B882399832832A167C2\ndiswan.pdb
    Loaded symbol image file: ndiswan.sys
    Image path: \SystemRoot\system32\DRIVERS\ndiswan.sys
    Image name: ndiswan.sys
    Timestamp:        Thu Nov 02 08:58:13 2006 (4549B325)
    CheckSum:         00023D9F
    ImageSize:        00023000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
```

```
8807b000 88086000   ndistapi   (pdb symbols)
c:\mss\ndistapi.pdb\B3AC7F470DF047BEBC5A385939B7BB891\ndistapi.pdb
    Loaded symbol image file: ndistapi.sys
    Image path: \SystemRoot\system32\DRIVERS\ndistapi.sys
    Image name: ndistapi.sys
    Timestamp:        Wed Jul 04 02:28:09 2007 (468AF7A9)
    CheckSum:         0000E7EB
    ImageSize:        0000B000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
88086000 8809d000   rasl2tp    (deferred)
    Image path: \SystemRoot\system32\DRIVERS\rasl2tp.sys
    Image name: rasl2tp.sys
    Timestamp:        Thu Nov 02 08:58:13 2006 (4549B325)
    CheckSum:         0001283E
    ImageSize:        00017000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
8809d000 880dd000   storport   (deferred)
    Image path: \SystemRoot\system32\DRIVERS\storport.sys
    Image name: storport.sys
    Timestamp:        Thu Nov 02 08:51:45 2006 (4549B1A1)
    CheckSum:         0001ECB2
    ImageSize:        00040000
    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.
880dd000 88108000   msiscsi    (deferred)
    Image path: \SystemRoot\system32\DRIVERS\msiscsi.sys
    Image name: msiscsi.sys
    Timestamp:        Thu Nov 02 08:52:40 2006 (4549B1D8)
    CheckSum:         0002C426
    ImageSize:        0002B000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
88108000 88120000   cdrom      (deferred)
    Image path: \SystemRoot\system32\DRIVERS\cdrom.sys
    Image name: cdrom.sys
    Timestamp:        Thu Nov 02 08:51:44 2006 (4549B1A0)
    CheckSum:         0001BA75
    ImageSize:        00018000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
88407000 88413000   vga        (deferred)
    Image path: \SystemRoot\System32\drivers\vga.sys
    Image name: vga.sys
    Timestamp:        Thu Nov 02 08:53:56 2006 (4549B224)
    CheckSum:         0000AE5E
    ImageSize:        0000C000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
88413000 88447000   usbhub     (pdb symbols)
c:\mss\usbhub.pdb\CE688E0154334944B40E875BB6E2146C2\usbhub.pdb
    Loaded symbol image file: usbhub.sys
    Image path: \SystemRoot\system32\DRIVERS\usbhub.sys
    Image name: usbhub.sys
    Timestamp:        Thu Nov 02 08:55:20 2006 (4549B278)
    CheckSum:         000355FE
    ImageSize:        00034000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
88447000 88471000   ks         (deferred)
    Image path: \SystemRoot\system32\DRIVERS\ks.sys
    Image name: ks.sys
```

```
    Timestamp:        Thu Nov 02 08:51:18 2006 (4549B186)
    CheckSum:         000285FF
    ImageSize:        0002A000
    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.
88471000 884ae000   USBPORT    (pdb symbols)
c:\mss\usbport.pdb\148A292E1DA8491F91F82441FDDF70F72\usbport.pdb
    Loaded symbol image file: USBPORT.SYS
    Image path: \SystemRoot\system32\DRIVERS\USBPORT.SYS
    Image name: USBPORT.SYS
    Timestamp:        Thu Nov 02 08:55:09 2006 (4549B26D)
    CheckSum:         0003FA9C
    ImageSize:        0003D000
    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.
884ae000 8855f000   athr       (deferred)
    Image path: \SystemRoot\system32\DRIVERS\athr.sys
    Image name: athr.sys
    Timestamp:        Mon Apr 16 06:29:11 2007 (462309A7)
    CheckSum:         000BA5FB
    ImageSize:        000B1000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
8855f000 885fc000   dxgkrnl    (pdb symbols)
c:\mss\dxgkrnl.pdb\1D2CDBE804EC4F0BBB308A05F8BCD14C2\dxgkrnl.pdb
    Loaded symbol image file: dxgkrnl.sys
    Image path: \SystemRoot\System32\drivers\dxgkrnl.sys
    Image name: dxgkrnl.sys
    Timestamp:        Tue Jul 03 02:01:10 2007 (46899FD6)
    CheckSum:         000A2242
    ImageSize:        0009D000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
885fc000 88c00000   igdkmd32   (deferred)
    Image path: \SystemRoot\system32\DRIVERS\igdkmd32.sys
    Image name: igdkmd32.sys
    Timestamp:        Tue Jun 26 17:53:33 2007 (4681448D)
    CheckSum:         001B64EB
    ImageSize:        00604000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
88c04000 88c36000   netbt      (pdb symbols)
c:\mss\netbt.pdb\42B661CF61454494A2C450C4DB53B1CC2\netbt.pdb
    Loaded symbol image file: netbt.sys
    Image path: \SystemRoot\System32\DRIVERS\netbt.sys
    Image name: netbt.sys
    Timestamp:        Thu Nov 02 08:57:18 2006 (4549B2EE)
```

```
    CheckSum:         0002DCA1
    ImageSize:        00032000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
88c36000 88c7d000   afd        (pdb symbols)
c:\mss\afd.pdb\D7ADD0FFBDA6457C8AD64784806BBA1D2\afd.pdb
    Loaded symbol image file: afd.sys
    Image path: \SystemRoot\system32\drivers\afd.sys
    Image name: afd.sys
    Timestamp:        Thu Nov 02 08:58:41 2006 (4549B341)
    CheckSum:         00049FFB
    ImageSize:        00047000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
88c7d000 88c91000   smb        (pdb symbols)
c:\mss\smb.pdb\56F7FE005B104C1EBA97D5EAAECD9BEA1\smb.pdb
    Loaded symbol image file: smb.sys
    Image path: \SystemRoot\system32\DRIVERS\smb.sys
    Image name: smb.sys
    Timestamp:        Thu Nov 02 08:57:10 2006 (4549B2E6)
    CheckSum:         00010933
    ImageSize:        00014000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
88c91000 88ca6000   tdx        (deferred)
    Image path: \SystemRoot\system32\DRIVERS\tdx.sys
    Image name: tdx.sys
    Timestamp:        Thu Nov 02 08:57:34 2006 (4549B2FE)
    CheckSum:         0001FE16
    ImageSize:        00015000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
88ca6000 88cbf000   fwpkclnt   (deferred)
    Image path: \SystemRoot\System32\drivers\fwpkclnt.sys
    Image name: fwpkclnt.sys
    Timestamp:        Thu Nov 02 08:57:26 2006 (4549B2F6)
    CheckSum:         0002402A
    ImageSize:        00019000
    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.
88cbf000 88cca000   Msfs       (pdb symbols)
c:\mss\msfs.pdb\BAA6A8DF2BC6425CAC74B199E26C994A1\msfs.pdb
    Loaded symbol image file: Msfs.SYS
    Image path: \SystemRoot\System32\Drivers\Msfs.SYS
    Image name: Msfs.SYS
    Timestamp:        Thu Nov 02 08:30:56 2006 (4549ACC0)
    CheckSum:         0000FC5E
    ImageSize:        0000B000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
88cea000 88d0b000   VIDEOPRT   (deferred)
    Image path: \SystemRoot\System32\drivers\VIDEOPRT.SYS
    Image name: VIDEOPRT.SYS
    Timestamp:        Thu Nov 02 08:54:07 2006 (4549B22F)
    CheckSum:         0001DD84
    ImageSize:        00021000
    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.
88d0b000 88d30000   drmk       (deferred)
    Image path: \SystemRoot\system32\drivers\drmk.sys
    Image name: drmk.sys
    Timestamp:        Thu Nov 02 09:20:49 2006 (4549B871)
    CheckSum:         0002E713
    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:        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.
88d30000 88d5d000   portcls    (deferred)
    Image path: \SystemRoot\system32\drivers\portcls.sys
    Image name: portcls.sys
    Timestamp:        Thu Nov 02 08:55:02 2006 (4549B266)
    CheckSum:         00034F0F
    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:        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.
88d5d000 88e00000   stwrt      (no symbols)
    Loaded symbol image file: stwrt.sys
    Image path: \SystemRoot\system32\drivers\stwrt.sys
    Image name: stwrt.sys
    Timestamp:        Wed Dec 27 17:44:51 2006 (4592B113)
    CheckSum:         000AB66C
    ImageSize:        000A3000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
88e44000 88e5a000   cdfs       (deferred)
    Image path: \SystemRoot\system32\DRIVERS\cdfs.sys
    Image name: cdfs.sys
    Timestamp:        Thu Nov 02 08:30:50 2006 (4549ACBA)
    CheckSum:         0001EEB3
    ImageSize:        00016000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
88e6a000 88e81000   dfsc       (deferred)
    Image path: \SystemRoot\System32\Drivers\dfsc.sys
    Image name: dfsc.sys
    Timestamp:        Thu Nov 02 08:31:04 2006 (4549ACC8)
```

```
    CheckSum:         00015C96
    ImageSize:        00017000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
88ec1000 88ecb000   nsiproxy   (pdb symbols)
c:\mss\nsiproxy.pdb\79954EF52348493CB195FCA39F46AEFF1\nsiproxy.pdb
    Loaded symbol image file: nsiproxy.sys
    Image path: \SystemRoot\system32\drivers\nsiproxy.sys
    Image name: nsiproxy.sys
    Timestamp:        Thu Nov 02 08:57:30 2006 (4549B2FA)
    CheckSum:         0000D051
    ImageSize:        0000A000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
88ecb000 88f06000   rdbss      (pdb symbols)
c:\mss\rdbss.pdb\6BD820DCC9284AE69B371FBB0CD9836F2\rdbss.pdb
    Loaded symbol image file: rdbss.sys
    Image path: \SystemRoot\system32\DRIVERS\rdbss.sys
    Image name: rdbss.sys
    Timestamp:        Thu Nov 02 08:31:24 2006 (4549ACDC)
    CheckSum:         0003A186
    ImageSize:        0003B000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
88f06000 88f19000   wanarp     (deferred)
    Image path: \SystemRoot\system32\DRIVERS\wanarp.sys
    Image name: wanarp.sys
    Timestamp:        Wed Jul 04 02:28:16 2007 (468AF7B0)
    CheckSum:         0001CFF4
    ImageSize:        00013000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
88f19000 88f2f000   pacer      (deferred)
    Image path: \SystemRoot\system32\DRIVERS\pacer.sys
    Image name: pacer.sys
    Timestamp:        Wed Jul 04 02:27:33 2007 (468AF785)
    CheckSum:         0001981A
    ImageSize:        00016000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
88f2f000 89000000   tcpip      (deferred)
    Image path: \SystemRoot\System32\drivers\tcpip.sys
    Image name: tcpip.sys
    Timestamp:        Fri Sep 28 03:47:19 2007 (46FC6B37)
    CheckSum:         000C86AB
    ImageSize:        000D1000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
89a87000 89a96000   monitor    (deferred)
    Image path: \SystemRoot\system32\DRIVERS\monitor.sys
    Image name: monitor.sys
    Timestamp:        Thu Nov 02 08:54:05 2006 (4549B22D)
    CheckSum:         000126AD
    ImageSize:        0000F000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
89aba000 89ac4000   Dxapi      (deferred)
    Image path: \SystemRoot\System32\drivers\Dxapi.sys
    Image name: Dxapi.sys
    Timestamp:        Thu Nov 02 08:38:17 2006 (4549AE79)
    CheckSum:         0000C639
    ImageSize:        0000A000
    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.
```

```
89ac4000 89ace000   BthEnum    (deferred)
    Image path: \SystemRoot\system32\DRIVERS\BthEnum.sys
    Image name: BthEnum.sys
    Timestamp:        Thu Nov 02 08:55:22 2006 (4549B27A)
    CheckSum:         0000BFB3
    ImageSize:        0000A000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
89ace000 89ad8000   KeyMagic   (no symbols)
    Loaded symbol image file: KeyMagic.sys
    Image path: \SystemRoot\system32\DRIVERS\KeyMagic.sys
    Image name: KeyMagic.sys
    Timestamp:        Thu Aug 30 22:59:01 2007 (46D73DA5)
    CheckSum:         0000B906
    ImageSize:        0000A000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
89ad8000 89ae2000   ndisuio    (deferred)
    Image path: \SystemRoot\system32\DRIVERS\ndisuio.sys
    Image name: ndisuio.sys
    Timestamp:        Thu Nov 02 08:57:22 2006 (4549B2F2)
    CheckSum:         000086D8
    ImageSize:        0000A000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
89af6000 89b00000   secdrv     (deferred)
    Image path: \SystemRoot\System32\Drivers\secdrv.SYS
    Image name: secdrv.SYS
    Timestamp:        Wed Sep 13 14:18:32 2006 (45080528)
    CheckSum:         0000F9E8
    ImageSize:        0000A000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
89b5b000 89b66000   tcpipreg   (deferred)
    Image path: \SystemRoot\System32\drivers\tcpipreg.sys
    Image name: tcpipreg.sys
    Timestamp:        Thu Nov 02 08:57:46 2006 (4549B30A)
    CheckSum:         0000792D
    ImageSize:        0000B000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
8ce00000 8cfff000   win32k     (pdb symbols)
c:\mss\win32k.pdb\798F703BCE934F93A6D2C14E3066F4562\win32k.pdb
    Loaded symbol image file: win32k.sys
    Image path: \SystemRoot\System32\win32k.sys
    Image name: win32k.sys
    Timestamp:        Wed Aug 29 02:52:35 2007 (46D4D163)
    CheckSum:         001F53A2
    ImageSize:        001FF000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
9e600000 9e609000   TSDDD      (deferred)
    Image path: \SystemRoot\System32\TSDDD.dll
    Image name: TSDDD.dll
    Timestamp:        Thu Nov 02 09:02:02 2006 (4549B40A)
    CheckSum:         000133E7
    ImageSize:        00009000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
9e610000 9e61e000   cdd        (pdb symbols)
c:\mss\cdd.pdb\07C77AD315AD4FDCAAF3DEC553303D561\cdd.pdb
    Loaded symbol image file: cdd.dll
    Image path: \SystemRoot\System32\cdd.dll
    Image name: cdd.dll
    Timestamp:        Tue Jul 03 03:08:39 2007 (4689AFA7)
    CheckSum:         0000FC2E
    ImageSize:        0000E000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
9e878000 9e893000   luafv      (pdb symbols)
c:\mss\luafv.pdb\C177291432194CC8A5D6B9E0834207602\luafv.pdb
    Loaded symbol image file: luafv.sys
    Image path: \SystemRoot\system32\drivers\luafv.sys
    Image name: luafv.sys
    Timestamp:        Thu Nov 02 08:33:07 2006 (4549AD43)
    CheckSum:         0001BBEF
    ImageSize:        0001B000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
```

```
9e8e3000 9e8ef000   hidbth     (pdb symbols)
c:\mss\hidbth.pdb\D2978BBCDCA4469F9C6AF9CE6EA5C5A11\hidbth.pdb
    Loaded symbol image file: hidbth.sys
    Image path: \SystemRoot\system32\DRIVERS\hidbth.sys
    Image name: hidbth.sys
    Timestamp:        Thu Nov 02 08:55:21 2006 (4549B279)
    CheckSum:         0000A91E
    ImageSize:        0000C000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
9e8ef000 9e909000   bthpan     (deferred)
    Image path: \SystemRoot\system32\DRIVERS\bthpan.sys
    Image name: bthpan.sys
    Timestamp:        Thu Nov 02 08:55:27 2006 (4549B27F)
    CheckSum:         00024A60
    ImageSize:        0001A000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
9e909000 9e91a000   rfcomm     (deferred)
    Image path: \SystemRoot\system32\DRIVERS\rfcomm.sys
    Image name: rfcomm.sys
    Timestamp:        Thu Nov 02 08:55:22 2006 (4549B27A)
    CheckSum:         000172A6
    ImageSize:        00011000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
9e91a000 9e954000   bthport    (pdb symbols)
c:\mss\bthport.pdb\E531E2B7A1E94F3AAF0C77890C19D40D1\bthport.pdb
    Loaded symbol image file: bthport.sys
    Image path: \SystemRoot\System32\Drivers\bthport.sys
    Image name: bthport.sys
    Timestamp:        Thu Nov 02 08:55:21 2006 (4549B279)
    CheckSum:         00038041
    ImageSize:        0003A000
    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:     bthport.sys
    OriginalFilename: bthport.sys
    ProductVersion:   6.0.6000.16386
    FileVersion:      6.0.6000.16386 (vista_rtm.061101-2205)
    FileDescription:  Bluetooth Bus Driver
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
9e954000 9e960000   BTHUSB     (pdb symbols)
c:\mss\bthusb.pdb\22D18568CFC542048FB9039ADD893FD21\bthusb.pdb
    Loaded symbol image file: BTHUSB.sys
    Image path: \SystemRoot\System32\Drivers\BTHUSB.sys
    Image name: BTHUSB.sys
    Timestamp:        Thu Nov 02 08:55:19 2006 (4549B277)
    CheckSum:         0000AA57
    ImageSize:        0000C000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
9f659000 9f65a180   SystemDump   (private pdb symbols)
C:\dmitri\SystemDump31\x86\Symbols\SystemDump.pdb
    Loaded symbol image file: SystemDump.sys
    Image path: \??\C:\dmitri\SystemDump31\x86\SystemDump.sys
    Image name: SystemDump.sys
    Timestamp:        Mon Sep 11 17:38:23 2006 (450590FF)
    CheckSum:         000099A6
    ImageSize:        00001180
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
a024f000 a0262000   rspndr     (deferred)
    Image path: \SystemRoot\system32\DRIVERS\rspndr.sys
    Image name: rspndr.sys
    Timestamp:        Thu Nov 02 08:56:48 2006 (4549B2D0)
    CheckSum:         00016310
    ImageSize:        00013000
```

```
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
a02a2000 a0330000   spsys      (export symbols)       spsys.sys
    Loaded symbol image file: spsys.sys
    Image path: \SystemRoot\system32\drivers\spsys.sys
    Image name: spsys.sys
    Timestamp:        Wed Oct 25 23:43:28 2006 (453FE890)
    CheckSum:         00089D11
    ImageSize:        0008E000
    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).061025-1421)
    FileDescription:  security processor
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
a0844000 a085f000   srvnet     (pdb symbols)
c:\mss\srvnet.pdb\91A40D3CD78140A494724F2496D4F62D2\srvnet.pdb
    Loaded symbol image file: srvnet.sys
    Image path: \SystemRoot\System32\DRIVERS\srvnet.sys
    Image name: srvnet.sys
    Timestamp:        Fri Oct 26 02:40:43 2007 (4721459B)
    CheckSum:         0001DAE5
    ImageSize:        0001B000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
a089f000 a0905000   HTTP       (pdb symbols)
c:\mss\http.pdb\97890387C8654941B93C5F738D1827672\http.pdb
    Loaded symbol image file: HTTP.sys
    Image path: \SystemRoot\system32\drivers\HTTP.sys
    Image name: HTTP.sys
    Timestamp:        Thu Nov 02 08:57:06 2006 (4549B2E2)
    CheckSum:         0006169A
    ImageSize:        00066000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
a09d5000 a0a00000   nwifi      (pdb symbols)
c:\mss\nwifi.pdb\9C01B29DA66F4E21926D5DACB8FE343B1\nwifi.pdb
    Loaded symbol image file: nwifi.sys
    Image path: \SystemRoot\system32\DRIVERS\nwifi.sys
    Image name: nwifi.sys
    Timestamp:        Tue Oct 30 01:21:14 2007 (4726870A)
    CheckSum:         00028AE3
    ImageSize:        0002B000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
a0c15000 a0c39000   srv2       (pdb symbols)
c:\mss\srv2.pdb\26E8577A14FB4CD6B17CD080E166B0122\srv2.pdb
    Loaded symbol image file: srv2.sys
    Image path: \SystemRoot\System32\DRIVERS\srv2.sys
    Image name: srv2.sys
    Timestamp:        Fri Oct 26 02:40:47 2007 (4721459F)
    CheckSum:         0002B85A
    ImageSize:        00024000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
a0c39000 a0c4b000   mrxsmb20   (deferred)
    Image path: \SystemRoot\system32\DRIVERS\mrxsmb20.sys
    Image name: mrxsmb20.sys
    Timestamp:        Fri Oct 26 02:40:16 2007 (47214580)
    CheckSum:         00016BD9
    ImageSize:        00012000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
a0c4b000 a0c84000   mrxsmb10   (deferred)
    Image path: \SystemRoot\system32\DRIVERS\mrxsmb10.sys
    Image name: mrxsmb10.sys
    Timestamp:        Thu Nov 02 08:31:25 2006 (4549ACDD)
```

```
    CheckSum:         00042EE5
    ImageSize:        00039000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
a0c84000 a0ca2000   mrxsmb     (deferred)
    Image path: \SystemRoot\system32\DRIVERS\mrxsmb.sys
    Image name: mrxsmb.sys
    Timestamp:        Fri Oct 26 02:40:17 2007 (47214581)
    CheckSum:         0001962A
    ImageSize:        0001E000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
a0ca2000 a0cc1000   mrxdav     (pdb symbols)
c:\mss\mrxdav.pdb\3B6A2571BAEF46559335875A995F94E42\mrxdav.pdb
    Loaded symbol image file: mrxdav.sys
    Image path: \SystemRoot\system32\drivers\mrxdav.sys
    Image name: mrxdav.sys
    Timestamp:        Thu Nov 02 08:31:24 2006 (4549ACDC)
    CheckSum:         00020D0D
    ImageSize:        0001F000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
a0cc1000 a0cd5000   mpsdrv     (pdb symbols)
c:\mss\mpsdrv.pdb\ECFCC91F84A74026BDADE46C8D527FBC1\mpsdrv.pdb
    Loaded symbol image file: mpsdrv.sys
    Image path: \SystemRoot\System32\drivers\mpsdrv.sys
    Image name: mpsdrv.sys
    Timestamp:        Thu Jun 07 03:55:55 2007 (466773BB)
    CheckSum:         00017B0B
    ImageSize:        00014000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
a0de7000 a0e00000   bowser     (deferred)
    Image path: \SystemRoot\system32\DRIVERS\bowser.sys
    Image name: bowser.sys
    Timestamp:        Thu Nov 02 08:31:11 2006 (4549ACCF)
    CheckSum:         0001D6EC
    ImageSize:        00019000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
a1bb4000 a1c00000   srv        (pdb symbols)
c:\mss\srv.pdb\B15B5CF196634D978649C1BF6A132DEA2\srv.pdb
    Loaded symbol image file: srv.sys
    Image path: \SystemRoot\System32\DRIVERS\srv.sys
    Image name: srv.sys
    Timestamp:        Thu Nov 02 08:31:55 2006 (4549ACFB)
    CheckSum:         0005310D
    ImageSize:        0004C000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
a1f22000 a2000000   peauth     (deferred)
    Image path: \SystemRoot\system32\drivers\peauth.sys
    Image name: peauth.sys
    Timestamp:        Mon Oct 23 09:55:32 2006 (453C8384)
    CheckSum:         000DBD03
    ImageSize:        000DE000
    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.
```

```
Unloaded modules:
85d8c000 85d94000   drmkaud.sys
    Timestamp: unavailable (00000000)
    Checksum:  00000000
85cea000 85cec000   BthKicker.sys
    Timestamp: unavailable (00000000)
    Checksum:  00000000
85c35000 85c42000   crashdmp.sys
    Timestamp: unavailable (00000000)
    Checksum:  00000000
85c27000 85c32000   dump_ataport.sys
    Timestamp: unavailable (00000000)
    Checksum:  00000000
85d64000 85d6c000   dump_atapi.sys
    Timestamp: unavailable (00000000)
    Checksum:  00000000
85c66000 85c6f000   kbdhid.sys
    Timestamp: unavailable (00000000)
    Checksum:  00000000
```

IRP Distrubution

```
0: kd> !irpfind

  Irp    [ Thread ] irpStack: (Mj,Mn)   DevObj  [Driver]         MDL Process
82eecab0 [82f3b020] Irp is complete (CurrentLocation 8 > StackCount 7) 0x00000000
82efff68 [836a0d78] irpStack: ( d, 0)  84c6aee8 [ \FileSystem\Npfs]
82f003d0 [00000000] Irp is complete (CurrentLocation 21 > StackCount 20)
82f36690 [00000000] Irp is complete (CurrentLocation 21 > StackCount 20)
82f369d8 [00000000] Irp is complete (CurrentLocation 21 > StackCount 20)
82f418a0 [899abd78] irpStack: ( d, 0)  84c6aee8 [ \FileSystem\Npfs]
83306698 [9fc9a358] irpStack: ( e,20)  84b64d28 [ \Driver\AFD] 0x9fc9c020
833370f0 [00000000] irpStack: ( f, 0)  849c6028 [ \Driver\usbuhci]
83337b98 [89944770] irpStack: ( d, 0)  84c6aee8 [ \FileSystem\Npfs]
833458a8 [00000000] irpStack: ( f, 0)  00000000 [00000000: Could not read device object or
_DEVICE_OBJECT not found
]
834da618 [8356fa40] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
8351e008 [a1950380] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
8357e008 [8372a678] irpStack: ( 3, 0)  84916e48 [ \Driver\tunmp] 0x9fc3dd90
8358c2f8 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
8358c6d8 [8356fa40] irpStack: ( d, 0)  84c6aee8 [ \FileSystem\Npfs]
835ad4d0 [899bed78] irpStack: ( e, 0)  84830b30 [ \Driver\NdisTapi]
835b90d0 [849cc770] irpStack: ( 3, 0)  84c6aee8 [ \FileSystem\Npfs]
835c6990 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
835d7a40 [a18bd3c8] irpStack: ( 3, 0)  84c6aee8 [ \FileSystem\Npfs]
835e6e20 [8356fa40] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
835ee458 [a1950380] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
835f17a0 [a1950380] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
835f4398 [9e1f2d78] irpStack: ( 3, 0)  84c6aee8 [ \FileSystem\Npfs]
83606df0 [9fd00d78] irpStack: ( e,2d)  84b64d28 [ \Driver\AFD]
8363b688 [836929e0] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
8363d580 [836929e0] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
83645e20 [a1950380] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
836476b0 [9fcbfd78] irpStack: ( e,2d)  84b64d28 [ \Driver\AFD]
8364c008 [a1950380] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
8364e468 [8385b2f0] irpStack: ( d, 0)  84c6aee8 [ \FileSystem\Npfs]
83663a88 [a1950380] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
83663c70 [a1950380] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
83667ac0 [a1950380] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
8366b158 [a18c9d78] irpStack: ( d, 0)  84c6aee8 [ \FileSystem\Npfs]
83671b28 [a1950380] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
83673008 [835e4b58] irpStack: ( e, 9)  84b64d28 [ \Driver\AFD]
83674008 [a1950380] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
8367e560 [a18a9d78] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
83684c08 [a1950380] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
83684e20 [a1950380] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
836856b0 [9fd536b8] irpStack: ( e, 0)  84ccfc70 [ \Driver\NDProxy]
83686e20 [a1950380] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
83688e28 [a1801030] irpStack: ( d, 0)  847f7020 [ \FileSystem\Ntfs] 0xa18bd670
8368a528 [a1950380] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
83690420 [a1950380] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
836ae300 [899d5948] irpStack: ( 3, 0)  84c6aee8 [ \FileSystem\Npfs]
836ba008 [836aa818] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
836bb5a0 [83a0b598] irpStack: ( 3, 0)  84c6aee8 [ \FileSystem\Npfs]
836bfa18 [836929e0] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
836cd118 [8372a678] irpStack: ( 3, 0)  84916e48 [ \Driver\tunmp] 0x9fc3dd90
836cf008 [836929e0] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
836d6628 [a1d3ad78] irpStack: ( e,2d)  84b64d28 [ \Driver\AFD]
83704e20 [a1950380] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
837079c0 [83a14410] irpStack: ( e, 9)  84b64d28 [ \Driver\AFD]
83707ba0 [00000000] irpStack: (16, 0)  8997d030 [ \Driver\usbhub]
8370b008 [a1950380] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
83714b00 [8349c4d8] irpStack: ( e,2d)  84b64d28 [ \Driver\AFD]
83717e28 [00000000] irpStack: ( f, 0)  84ad8028 [ \Driver\usbuhci]
8371a6f0 [899eaaa8] irpStack: ( 3, 0)  89952d48 [ \Driver\HidUsb] 0x00000000
8371d710 [899b4630] irpStack: ( 3, 0)  9e1d9c60 [ \Driver\mouclass]
```

```
83728de8 [836cfac0] irpStack: ( e,2d)  84b64d28 [ \Driver\AFD]
83728ef8 [836cfac0] irpStack: ( e,2d)  84b64d28 [ \Driver\AFD]
83736cc0 [a1c2f650] irpStack: ( e, 6)  84b64d28 [ \Driver\AFD] 0x9fc9c020
83739008 [a1c2f650] irpStack: ( e, 6)  84b64d28 [ \Driver\AFD] 0x9fc9c020
8373e748 [a180cc98] irpStack: ( e, 6)  84b64d28 [ \Driver\AFD] 0x9fc9c020
8374c308 [8349c4d8] irpStack: ( e,2d)  84b64d28 [ \Driver\AFD]
8374ff68 [83885d78] irpStack: ( d, 0)  84c6aee8 [ \FileSystem\Npfs]
83794a38 [a1950380] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
83794c20 [a1950380] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
8379c7f8 [a1950380] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
8379dc60 [8345cd78] irpStack: ( 3, 0)  84c6aee8 [ \FileSystem\Npfs]
837d94d0 [834a9740] irpStack: ( e,2d)  84b64d28 [ \Driver\AFD]
837de8c0 [a1950380] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
837e84f0 [834a9740] irpStack: ( e,2d)  84b64d28 [ \Driver\AFD]
838160f8 [9fc6e7f8] irpStack: ( 3, 0)  84c6aee8 [ \FileSystem\Npfs]
83816438 [8372a678] irpStack: ( 3, 0)  84916e48 [ \Driver\tunmp] 0x9fc3dd90
83833e28 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3) 0x00000000
83853008 [83863030] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
83855c50 [9fdfdbc0] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
83894008 [83863030] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
838df428 [838174d8] irpStack: ( e, 9)  84b64d28 [ \Driver\AFD]
838fc458 [839f5888] irpStack: ( e, 0)  84dcb6a8 [ \Driver\nsiproxy]
839208e8 [835e17d0] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
83a0ae20 [9fdfdbc0] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
83a20d00 [899eaaa8] irpStack: ( 3, 0)  84859190 [ \Driver\kbdclass]
83c70008 [00000000] irpStack: ( e, 0)  8331d220 [ \Driver\ACPI]
83c703f0 [00000000] irpStack: ( e, 0)  83c8f778 [ \Driver\ACPI]
83c8a7e0 [9fc15c60] irpStack: ( d, 0)  84c6aee8 [ \FileSystem\Npfs]
84245980 [a1950380] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
8444be28 [836908b8] Irp is complete (CurrentLocation 8 > StackCount 7) 0x00000000
84797cd8 [00000000] irpStack: (16, 2)  83c94868 [83c94868: is not a device object
]
8479f9e0 [00000000] Irp is complete (CurrentLocation 5 > StackCount 4) 0x00000000
847a1618 [82f47828] irpStack: ( e, 0)  84321478 [84321478: is not a device object
]
847a4b30 [00000000] irpStack: ( f, 0)  849c6028 [ \Driver\usbuhci]
847a99d8 [89961030] irpStack: ( d, 0)  84c6aee8 [ \FileSystem\Npfs]
847aa9f0 [9e1cdb90] irpStack: ( e,20)  84b64d28 [ \Driver\AFD] 0x89956238
847aaef8 [9e1cdb90] irpStack: ( e,20)  84b64d28 [ \Driver\AFD] 0x89956238
847ae7a0 [a18d33b8] irpStack: ( e, 0)  84dcb6a8 [ \Driver\nsiproxy]
847c9bc8 [82f3bd78] irpStack: ( e, 0)  8444b1c0 [ \Driver\volmgr]
847ce868 [9fc23d78] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
847d5898 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
847f9290 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
847fe5e0 [00000000] Irp is complete (CurrentLocation 8 > StackCount 7) 0x00000000
8482f180 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
84836d48 [00000000] irpStack: ( f, 0)  849bf028 [ \Driver\usbuhci]
84837990 [00000000] irpStack: ( f, 0)  84b8f028 [ \Driver\usbehci]
84837b70 [00000000] irpStack: ( f, 0)  849c1028 [ \Driver\usbuhci]
8483cf68 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
8485b410 [00000000] irpStack: ( 3, 0)  8486f580 [ \Driver\HidUsb] 0x00000000
8486f840 [00000000] irpStack: ( f, 0)  849c6028 [ \Driver\usbuhci]
8486fbc8 [00000000] irpStack: (16, 0)  84880700 [ \Driver\usbhub]
8487fc80 [00000000] irpStack: ( f, 0)  84ad8028 [ \Driver\usbuhci]
84921008 [00000000] Irp is complete (CurrentLocation 5 > StackCount 4) 0x00000000
84952c68 [00000000] irpStack: ( 0, 0)  00000000 [00000000: Could not read device object or
_DEVICE_OBJECT not found
] 0x00000000
84adcca8 [00000000] irpStack: ( f, 0)  84ad8028 [ \Driver\usbuhci]
84b60340 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2)
84b62b08 [00000000] irpStack: ( f, 0)  849c1028 [ \Driver\usbuhci]
84d321e8 [899eaaa8] irpStack: ( 3, 0)  84908298 [ \Driver\kbdclass]
84d32458 [9fc0f218] irpStack: ( e,2d)  84b64d28 [ \Driver\AFD]
84d32a90 [00000000] irpStack: ( f, 0)  89966598 [ \Driver\IRRemoteFlt]
84daca68 [9fd00d78] irpStack: ( e,2d)  84b64d28 [ \Driver\AFD]
84dacc48 [00000000] irpStack: ( f, 0)  849c6028 [ \Driver\usbuhci]
84db1398 [9fc0f218] irpStack: ( e,20)  84b64d28 [ \Driver\AFD] 0x9e1fd468
84dcb4a0 [00000000] irpStack: ( f, 0)  84ad8028 [ \Driver\usbuhci]
84df1e28 [00000000] irpStack: ( f, 0)  84ad8028 [ \Driver\usbuhci]
84df3968 [84875d78] Irp is complete (CurrentLocation 8 > StackCount 7) 0x00000000
```

```
89847b60 [00000000] irpStack: ( f, 0)  84ad8028 [ \Driver\usbuhci]
89851770 [9fc9fcb8] irpStack: ( d, 0)  84c6aee8 [ \FileSystem\Npfs]
89857128 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
89858048 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
89858450 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
898584f0 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
89859600 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
89859838 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
89859a70 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
8985a830 [9fce1030] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
8985c008 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
8985c830 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
8985d5c8 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
89860648 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
898606e8 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
89865528 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
89865d88 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
89866260 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
89866348 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
898669c8 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
89867290 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
89867cc8 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
89868728 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
89869128 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
898699c8 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
89869cc0 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
8986a5d0 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
8986b7d0 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
8986c1a8 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
8986cc08 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
8986cf20 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
8986d4e8 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
8986df20 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
8986e920 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
8986f1d0 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
8986fc08 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
89871008 [9e1ffd78] irpStack: ( d, 0)  847f7020 [ \FileSystem\Ntfs] 0x00000000
89872cd8 [a1806ac0] irpStack: ( e, 0)  9fd52160 [ \Driver\HTTP] 0x9fc9c020
89880698 [9fd86338] irpStack: ( e, 0)  9fdb9a18 [ \Driver\mpsdrv]
899496c8 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
899524c0 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3) 0x00000000
899593e0 [9e1fd1c0] irpStack: ( 3, 0)  84c6aee8 [ \FileSystem\Npfs]
8995b9c0 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
8996b968 [89937030] irpStack: ( d, 0)  84c6aee8 [ \FileSystem\Npfs]
89991a48 [9fca6ac0] irpStack: ( e, 0)  84d8cb68 [ \Driver\Smb] 0x8485e910
899acac8 [00000000] irpStack: ( f, 0)  84ad8028 [ \Driver\usbuhci]
899af458 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
899bac80 [00000000] irpStack: ( 0, 0)  00000000 [00000000: Could not read device object or
_DEVICE_OBJECT not found
]
899bf618 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
899c0bc8 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
899c1008 [899b4630] irpStack: ( 3, 0)  84909578 [ \Driver\mouclass]
899c9f68 [83681d78] irpStack: ( 3, 0)  84c6aee8 [ \FileSystem\Npfs]
899d7858 [00000000] Irp is complete (CurrentLocation 10 > StackCount 9)
899d8bd0 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
899d8d98 [899bc290] irpStack: ( d, 0)  84c6aee8 [ \FileSystem\Npfs]
899df008 [00000000] irpStack: ( f, 0)  84ad8028 [ \Driver\usbuhci]
899df638 [00000000] irpStack: ( f, 0)  84ad8028 [ \Driver\usbuhci]
899e7af8 [9fde0cd8] irpStack: ( 3, 0)  84c6aee8 [ \FileSystem\Npfs]
899eeec8 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
899eef68 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
899f0688 [00000000] Irp is complete (CurrentLocation 14 > StackCount 13)
899f08d8 [00000000] Irp is complete (CurrentLocation 16 > StackCount 15)
899f0b70 [00000000] Irp is complete (CurrentLocation 16 > StackCount 15)
899fa008 [00000000] Irp is complete (CurrentLocation 14 > StackCount 13)
9e1cb820 [83583030] irpStack: ( 3, 0)  84c6aee8 [ \FileSystem\Npfs]
9e1cc5f0 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
9e1cd758 [89977030] irpStack: ( 3, 0)  84c6aee8 [ \FileSystem\Npfs]
9e1ce408 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
```

```
9e1cf9e0 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
9e1cfd70 [00000000] irpStack: ( 3, 0)  9e1db030 [ \Driver\HidBth] 0x00000000
9e1d0008 [00000000] irpStack: ( f, 0)  899f9030 [ \Driver\HidBth]
9e1d06e8 [00000000] irpStack: ( f, 0)  899f9030 [ \Driver\HidBth]
9e1d4340 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
9e1da008 [00000000] irpStack: ( f, 0)  899bbd50 [ \Driver\BTHUSB]
9e1dadb8 [00000000] irpStack: ( f, 0)  899bbd50 [ \Driver\BTHUSB]
9e1deba8 [89937030] irpStack: ( d, 0)  84c6aee8 [ \FileSystem\Npfs]
9e1e2cc8 [9fd420b8] irpStack: ( 3, 0)  84c6aee8 [ \FileSystem\Npfs]
9e1eda30 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
9e1f24f0 [9fc0f218] irpStack: ( e,20)  84b64d28 [ \Driver\AFD] 0x9e1fd468
9e1f88e0 [84da0030] irpStack: ( d, 0)  84c6aee8 [ \FileSystem\Npfs]
9e1f8b80 [9fc0d748] irpStack: ( d, 0)  84c6aee8 [ \FileSystem\Npfs]
9e1fb408 [89944770] irpStack: ( e,20)  84b64d28 [ \Driver\AFD] 0x8983e1b0
9fc09008 [899bc290] irpStack: ( e,20)  84b64d28 [ \Driver\AFD] 0x8995e4a0
9fc22530 [9fc2e268] irpStack: ( d, 0)  84c6aee8 [ \FileSystem\Npfs]
9fc24ec0 [9fc87580] irpStack: ( 3, 0)  84c6aee8 [ \FileSystem\Npfs]
9fc2a8e8 [899d5d78] irpStack: ( d, 0)  84c6aee8 [ \FileSystem\Npfs]
9fc2ab90 [89938d78] irpStack: ( d, 0)  84c6aee8 [ \FileSystem\Npfs]
9fc2ae28 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
9fc32d98 [89944770] irpStack: ( e,20)  84b64d28 [ \Driver\AFD] 0x8983e1b0
9fc33008 [9fc2e268] irpStack: ( e,20)  84b64d28 [ \Driver\AFD] 0x8485e910
9fc34e08 [9fc9c890] irpStack: ( 3, 0)  84c6aee8 [ \FileSystem\Npfs]
9fc34f28 [a18d33b8] irpStack: ( e, 0)  84dcb6a8 [ \Driver\nsiproxy]
9fc355b8 [9fd199c8] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
9fc39e48 [9fd08d78] irpStack: ( 3, 0)  849cd5f0 [ \Driver\NativeWifiP] 0x9fc38a48
9fc3be28 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
9fc3c8b0 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
9fc3f190 [9fc9a358] irpStack: ( e,20)  84b64d28 [ \Driver\AFD] 0x9fc9c020
9fc45150 [a18b5030] irpStack: ( 3, 0)  84c6aee8 [ \FileSystem\Npfs]
9fc46428 [9fdc2d78] irpStack: ( 3, 0)  89952d48 [ \Driver\HidUsb] 0x9fc38a48
9fc46608 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
9fc467e8 [9fcc9030] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
9fc47df0 [9fca6d78] irpStack: ( e, 0)  84d8cb68 [ \Driver\Smb] 0x8485e910
9fc48d58 [9fc8a4c0] irpStack: ( e,20)  84b64d28 [ \Driver\AFD] 0x9fc3dd90
9fc4a8d8 [9fc4a598] irpStack: ( 3, 0)  84c6aee8 [ \FileSystem\Npfs]
9fc4c690 [9fc2e268] irpStack: ( e,20)  84b64d28 [ \Driver\AFD] 0x8485e910
9fc4d3f8 [9fc16798] irpStack: ( d, 0)  84c6aee8 [ \FileSystem\Npfs]
9fc4dec0 [9fd50030] irpStack: ( 3, 0)  84c6aee8 [ \FileSystem\Npfs]
9fc4faa8 [a180cc98] irpStack: ( e,2d)  84b64d28 [ \Driver\AFD]
9fc52630 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
9fc6b378 [8372a678] irpStack: ( 3, 0)  84916e48 [ \Driver\tunmp] 0x9fc3dd90
9fc8a770 [9fca6030] irpStack: ( e, 0)  84da7030 [ \Driver\netbt] 0x8485e910
9fc961d8 [9fd01030] irpStack: ( 3, 0)  84c6aee8 [ \FileSystem\Npfs]
9fc9ddd8 [9fce03b8] irpStack: ( e, 0)  84da7030 [ \Driver\netbt] 0x8485e910
9fca1ed0 [9fd34d78] irpStack: ( d, 0)  84c6aee8 [ \FileSystem\Npfs]
9fca6870 [9fcde888] irpStack: ( d, 0)  84c6aee8 [ \FileSystem\Npfs]
9fcc4008 [9fd096d8] irpStack: ( d, 0)  84c6aee8 [ \FileSystem\Npfs]
9fcc9850 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
9fccb798 [89871470] irpStack: ( 3, 0)  84c6aee8 [ \FileSystem\Npfs]
9fce2368 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
9fce77f8 [9fc3d030] irpStack: ( 3, 0)  84c6aee8 [ \FileSystem\Npfs]
9fcf4340 [89881650] irpStack: ( 3, 0)  84c6aee8 [ \FileSystem\Npfs]
9fd03f68 [9fd09388] irpStack: ( d, 0)  84c6aee8 [ \FileSystem\Npfs]
9fd068f8 [9fc964d8] irpStack: ( 3, 0)  84c6c960 [ \FileSystem\Msfs]
9fd074d0 [9fc8a4c0] irpStack: ( d, 0)  84c6aee8 [ \FileSystem\Npfs]
9fd09970 [836e0b48] irpStack: ( e, 0)  84cd6030 [ \Driver\NdisWan]
9fd11160 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
9fd1aab8 [836e0b48] irpStack: ( e, 0)  84cd6030 [ \Driver\NdisWan]
9fd21f68 [8372a678] irpStack: ( 3, 0)  84916e48 [ \Driver\tunmp] 0x9fc3dd90
9fd235e8 [a18b5d78] irpStack: ( 3, 0)  84c6aee8 [ \FileSystem\Npfs]
9fd24f68 [9fd86338] irpStack: ( e, 0)  9fdb9a18 [ \Driver\mpsdrv]
9fd28008 [9fc8a4c0] irpStack: ( e,20)  84b64d28 [ \Driver\AFD] 0x9fc3dd90
9fd33708 [8356e568] irpStack: ( d, 0)  84c6aee8 [ \FileSystem\Npfs]
9fd33e00 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
9fd4a340 [899bc290] irpStack: ( e,20)  84b64d28 [ \Driver\AFD] 0x8995e4a0
9fd4a558 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
9fd52bd8 [9fc469f0] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
9fd6fcb8 [9fd86338] irpStack: ( e, 0)  9fdb9a18 [ \Driver\mpsdrv]
9fd79d68 [8366e760] irpStack: ( d, 0)  84c6aee8 [ \FileSystem\Npfs]
```

```
9fd85930 [8356e568] irpStack: ( 3, 0)  84c6aee8 [ \FileSystem\Npfs]
9fd86270 [89870d78] irpStack: ( 3, 0)  84c6aee8 [ \FileSystem\Npfs]
9fd8d228 [89872030] irpStack: ( 3, 0)  84c6aee8 [ \FileSystem\Npfs]
9fd92708 [9fc382c8] irpStack: ( 3, 0)  84c6aee8 [ \FileSystem\Npfs]
9fd94508 [9fc3e630] irpStack: ( 3, 0)  84c6aee8 [ \FileSystem\Npfs]
9fd9a8d0 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
9fd9bbf8 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
9fda45e8 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
9fdaa3b0 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
9fdab3b8 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
9fdabb60 [898776d8] irpStack: ( 3, 0)  84c6aee8 [ \FileSystem\Npfs]
9fde17a8 [9fce1030] irpStack: ( d, 0)  847f7020 [ \FileSystem\Ntfs]
9fde30e8 [9fcced78] irpStack: ( d, 0)  84c6aee8 [ \FileSystem\Npfs]
9fdf1a48 [a1d3d6f0] irpStack: ( d, 0)  84c6aee8 [ \FileSystem\Npfs]
9fdf3278 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
9fdfe138 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1)
a18aa6b0 [9fd86338] irpStack: ( e, 0)  9fdb9a18 [ \Driver\mpsdrv]
a18aa948 [a180cc98] irpStack: ( e,2d)  84b64d28 [ \Driver\AFD]
a18b6430 [a18de720] irpStack: ( e, 6)  84b64d28 [ \Driver\AFD] 0x9fc9c020
a18bbe20 [a18b4898] irpStack: ( c, 2)  847f7020 [ \FileSystem\Ntfs]
a18c0c20 [a180cc98] irpStack: ( e, 6)  84b64d28 [ \Driver\AFD] 0x9fc9c020
a18deb28 [9e1dc7a0] irpStack: ( d, 0)  84c6aee8 [ \FileSystem\Npfs]
a19acef8 [a18de720] irpStack: ( e, 6)  84b64d28 [ \Driver\AFD] 0x9fc9c020
```