Reference Stack Traces

Windows Server 2003™ x86 Complete Memory Dump

Dmitry Vostokov

1/31/2008

First Edition

Table of Contents

Version

```
kd> version
Windows Server 2003 Kernel Version 3790 (Service Pack 2) UP Free x86 compatible
Product: Server, suite: Enterprise TerminalServer SingleUserTS
Built by: 3790.srv03_sp2_rtm.070216-1710
Kernel base = 0x80800000 PsLoadedModuleList = 0x8089ffa8
Debug session time: Wed Jan 30 17:54:13.390 2008 (GMT+0)
System Uptime: 0 days 0:30:12.000
32-bit Full kernel dump: c:\dmitri\MEMORY_Windows2003SP2_x86.DMP
```

Virtual Memory

```
kd> !vm

*** Virtual Memory Usage ***
       Physical Memory:      262003 (   1048012 Kb)
       Page File: \??\C:\pagefile.sys
         Current:   1126400 Kb  Free Space:   1113376 Kb
         Minimum:   1126400 Kb  Maximum:      1126400 Kb
       Available Pages:      205257 (    821028 Kb)
       ResAvail Pages:       199908 (    799632 Kb)
       Locked IO Pages:          64 (       256 Kb)
       Free System PTEs:      47381 (    189524 Kb)
       Free NP PTEs:          32766 (    131064 Kb)
       Free Special NP:           0 (         0 Kb)
       Modified Pages:          137 (       548 Kb)
       Modified PF Pages:       137 (       548 Kb)
       NonPagedPool Usage:     2144 (      8576 Kb)
       NonPagedPool Max:      51967 (    207868 Kb)
       PagedPool 0 Usage:      4766 (     19064 Kb)
       PagedPool 1 Usage:       483 (      1932 Kb)
       PagedPool 2 Usage:       491 (      1964 Kb)
       PagedPool Usage:        5740 (     22960 Kb)
       PagedPool Maximum:     70656 (    282624 Kb)
       Shared Commit:           754 (      3016 Kb)
       Special Pool:              0 (         0 Kb)
       Shared Process:         1939 (      7756 Kb)
       PagedPool Commit:       5744 (     22976 Kb)
       Driver Commit:          1575 (      6300 Kb)
       Committed pages:       27929 (    111716 Kb)
       Commit limit:         520702 (   2082808 Kb)

       Total Private:         16502 (     66008 Kb)
         0350 svchost.exe       3217 (     12868 Kb)
         035c explorer.exe      2262 (      9048 Kb)
         01a4 lsass.exe         1684 (      6736 Kb)
         0168 winlogon.exe      1536 (      6144 Kb)
         0840 iexplore.exe      1510 (      6040 Kb)
         0314 svchost.exe        890 (      3560 Kb)
         03dc spoolsv.exe        765 (      3060 Kb)
         0434 SpntSvc.exe        538 (      2152 Kb)
         04ec msdtc.exe          451 (      1804 Kb)
         0730 wmiprvse.exe       399 (      1596 Kb)
         0150 csrss.exe          372 (      1488 Kb)
         0198 services.exe       347 (      1388 Kb)
         065c svchost.exe        341 (      1364 Kb)
         0328 svchost.exe        309 (      1236 Kb)
         02d4 svchost.exe        274 (      1096 Kb)
         0610 VMwareUser.exe     214 (       856 Kb)
         05dc VMwareTray.exe     204 (       816 Kb)
         056c mdm.exe            194 (       776 Kb)
         0280 svchost.exe        193 (       772 Kb)
         04d4 StOPP.exe          177 (       708 Kb)
         0884 notepad.exe        155 (       620 Kb)
         05ec VMwareService.e    142 (       568 Kb)
         0550 svchost.exe        122 (       488 Kb)
         04b8 StWatchDog.exe      94 (       376 Kb)
         0584 svchost.exe         67 (       268 Kb)
         011c smss.exe            37 (       148 Kb)
         0004 System               8 (        32 Kb)
         06ec wmiprvse.exe         0 (         0 Kb)
         0300 userinit.exe         0 (         0 Kb)
```

Processes and Threads

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

System process

```
PROCESS 865a1818  SessionId: none  Cid: 0004    Peb: 00000000  ParentCid: 0000
    DirBase: 003b6000  ObjectTable: e1001ca8  HandleCount: 400.
    Image: System
    VadRoot 862d3320 Vads 4 Clone 0 Private 3. Modified 2942. Locked 0.
    DeviceMap e1000170
    Token                             e1000808
    ElapsedTime                       00:30:12.000
    UserTime                          00:00:00.000
    KernelTime                        00:04:01.140
    QuotaPoolUsage[PagedPool]         0
    QuotaPoolUsage[NonPagedPool]      0
    Working Set Sizes (now,min,max)  (59, 0, 345) (236KB, 0KB, 1380KB)
    PeakWorkingSetSize                524
    VirtualSize                       1 Mb
    PeakVirtualSize                   2 Mb
    PageFaultCount                    7039
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      8

    Setting context for this process...
.process /p /r ffffffff865a1818

    !peb
PEB NULL...


        THREAD 865a15a8  Cid 0004.0008  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            808a4920  SynchronizationEvent
            808a5a80  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      115817         Ticks: 151 (0:00:00:02.359)
        Context Switch Count      8361
        UserTime                  00:00:00.000
        KernelTime                00:03:47.812
        Start Address nt!Phase1Initialization (0x808e0982)
        Stack Init f78a7000 Current f78a6cdc Base f78a7000 Limit f78a4000 Call 0
        Priority 0 BasePriority 0 PriorityDecrement 0
        ChildEBP RetAddr
        f78a6cf4 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f78a6d0c 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f78a6d40 80856202 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f78a6da4 808e0994 nt!MmZeroPageThread+0x74 (FPO: [Non-Fpo])
        f78a6dac 809418f4 nt!Phase1Initialization+0x12 (FPO: [Non-Fpo])
        f78a6ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 865a0b40  Cid 0004.0010  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            808a76c0  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      20             Ticks: 115948 (0:00:30:11.687)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address nt!ExpWorkerThread (0x8087acd6)
        Stack Init f78b7000 Current f78b6d00 Base f78b7000 Limit f78b4000 Call 0
        Priority 13 BasePriority 13 PriorityDecrement 0
        ChildEBP RetAddr
        f78b6d18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f78b6d30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f78b6d78 8087ad9e nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f78b6dac 809418f4 nt!ExpWorkerThread+0xc8 (FPO: [Non-Fpo])
        f78b6ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 865a08d0  Cid 0004.0014  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            808a76c0  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      20             Ticks: 115948 (0:00:30:11.687)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address nt!ExpWorkerThread (0x8087acd6)
        Stack Init f78bb000 Current f78bad00 Base f78bb000 Limit f78b8000 Call 0
        Priority 13 BasePriority 13 PriorityDecrement 0
        ChildEBP RetAddr
        f78bad18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f78bad30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f78bad78 8087ad9e nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f78badac 809418f4 nt!ExpWorkerThread+0xc8 (FPO: [Non-Fpo])
        f78baddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 8659f020  Cid 0004.0018  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            808a76c0  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      4800           Ticks: 111168 (0:00:28:57.000)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address nt!ExpWorkerThread (0x8087acd6)
        Stack Init f78bf000 Current f78bed00 Base f78bf000 Limit f78bc000 Call 0
        Priority 13 BasePriority 13 PriorityDecrement 0
        ChildEBP RetAddr
        f78bed18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f78bed30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f78bed78 8087ad9e nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f78bedac 809418f4 nt!ExpWorkerThread+0xc8 (FPO: [Non-Fpo])
        f78beddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 8659fdb0  Cid 0004.001c  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            808a76c0  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      115952         Ticks: 16 (0:00:00:00.250)
        Context Switch Count      6313
        UserTime                  00:00:00.000
        KernelTime                00:00:01.406
        Start Address nt!ExpWorkerThread (0x8087acd6)
        Stack Init f78c3000 Current f78c2d00 Base f78c3000 Limit f78c0000 Call 0
        Priority 13 BasePriority 13 PriorityDecrement 0
        ChildEBP RetAddr
        f78c2d18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f78c2d30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f78c2d78 8087ad9e nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f78c2dac 809418f4 nt!ExpWorkerThread+0xc8 (FPO: [Non-Fpo])
        f78c2ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 8659fb40  Cid 0004.0020  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            808a76c0  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      97025          Ticks: 18943 (0:00:04:55.984)
        Context Switch Count      4800
        UserTime                  00:00:00.000
        KernelTime                00:00:00.421
        Start Address nt!ExpWorkerThread (0x8087acd6)
        Stack Init f78c7000 Current f78c6d00 Base f78c7000 Limit f78c4000 Call 0
        Priority 13 BasePriority 13 PriorityDecrement 0
        ChildEBP RetAddr
        f78c6d18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f78c6d30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f78c6d78 8087ad9e nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f78c6dac 809418f4 nt!ExpWorkerThread+0xc8 (FPO: [Non-Fpo])
        f78c6ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 8659f8d0  Cid 0004.0024  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            808a76c0  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      115941         Ticks: 27 (0:00:00:00.421)
        Context Switch Count      5086
        UserTime                  00:00:00.000
        KernelTime                00:00:00.343
        Start Address nt!ExpWorkerThread (0x8087acd6)
        Stack Init f78cb000 Current f78cad00 Base f78cb000 Limit f78c8000 Call 0
        Priority 13 BasePriority 13 PriorityDecrement 0
        ChildEBP RetAddr
        f78cad18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f78cad30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f78cad78 8087ad9e nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f78cadac 809418f4 nt!ExpWorkerThread+0xc8 (FPO: [Non-Fpo])
        f78caddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 8659f660  Cid 0004.0028  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            808a76c0  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      112613         Ticks: 3355 (0:00:00:52.421)
        Context Switch Count      810
        UserTime                  00:00:00.000
        KernelTime                00:00:00.125
        Start Address nt!ExpWorkerThread (0x8087acd6)
        Stack Init f78cf000 Current f78ced00 Base f78cf000 Limit f78cc000 Call 0
        Priority 13 BasePriority 13 PriorityDecrement 0
        ChildEBP RetAddr
        f78ced18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f78ced30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f78ced78 8087ad9e nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f78cedac 809418f4 nt!ExpWorkerThread+0xc8 (FPO: [Non-Fpo])
        f78ceddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 8659f3f0  Cid 0004.002c  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            808a76c0  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      4800           Ticks: 111168 (0:00:28:57.000)
        Context Switch Count      555
        UserTime                  00:00:00.000
        KernelTime                00:00:00.093
        Start Address nt!ExpWorkerThread (0x8087acd6)
        Stack Init f78d3000 Current f78d2d00 Base f78d3000 Limit f78d0000 Call 0
        Priority 13 BasePriority 13 PriorityDecrement 0
        ChildEBP RetAddr
        f78d2d18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f78d2d30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f78d2d78 8087ad9e nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f78d2dac 809418f4 nt!ExpWorkerThread+0xc8 (FPO: [Non-Fpo])
        f78d2ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 8659e020  Cid 0004.0030  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            808a76c0  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      97025          Ticks: 18943 (0:00:04:55.984)
        Context Switch Count      1645
        UserTime                  00:00:00.000
        KernelTime                00:00:00.140
        Start Address nt!ExpWorkerThread (0x8087acd6)
        Stack Init f78d7000 Current f78d6d00 Base f78d7000 Limit f78d4000 Call 0
        Priority 13 BasePriority 13 PriorityDecrement 0
        ChildEBP RetAddr
        f78d6d18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f78d6d30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f78d6d78 8087ad9e nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f78d6dac 809418f4 nt!ExpWorkerThread+0xc8 (FPO: [Non-Fpo])
        f78d6ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 8659edb0  Cid 0004.0034  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            808a76c0  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      95717          Ticks: 20251 (0:00:05:16.421)
        Context Switch Count      121
        UserTime                  00:00:00.000
        KernelTime                00:00:00.171
        Start Address nt!ExpWorkerThread (0x8087acd6)
        Stack Init f78db000 Current f78dad00 Base f78db000 Limit f78d8000 Call 0
        Priority 13 BasePriority 13 PriorityDecrement 0
        ChildEBP RetAddr
        f78dad18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f78dad30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f78dad78 8087ad9e nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f78dadac 809418f4 nt!ExpWorkerThread+0xc8 (FPO: [Non-Fpo])
        f78daddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 8659eb40  Cid 0004.0038  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            808a76fc  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      20             Ticks: 115948 (0:00:30:11.687)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address nt!ExpWorkerThread (0x8087acd6)
        Stack Init f78df000 Current f78ded00 Base f78df000 Limit f78dc000 Call 0
        Priority 12 BasePriority 12 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f78ded18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f78ded30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f78ded78 8087ad9e nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f78dedac 809418f4 nt!ExpWorkerThread+0xc8 (FPO: [Non-Fpo])
        f78deddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 8659e8d0  Cid 0004.003c  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            808a76fc  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      20             Ticks: 115948 (0:00:30:11.687)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address nt!ExpWorkerThread (0x8087acd6)
        Stack Init f78e3000 Current f78e2d00 Base f78e3000 Limit f78e0000 Call 0
        Priority 12 BasePriority 12 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f78e2d18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f78e2d30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f78e2d78 8087ad9e nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f78e2dac 809418f4 nt!ExpWorkerThread+0xc8 (FPO: [Non-Fpo])
        f78e2ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 8659e660  Cid 0004.0040  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            808a76fc  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      3081           Ticks: 112887 (0:00:29:23.859)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address nt!ExpWorkerThread (0x8087acd6)
        Stack Init f78e7000 Current f78e6d00 Base f78e7000 Limit f78e4000 Call 0
        Priority 12 BasePriority 12 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f78e6d18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f78e6d30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f78e6d78 8087ad9e nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f78e6dac 809418f4 nt!ExpWorkerThread+0xc8 (FPO: [Non-Fpo])
        f78e6ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 8659e3f0  Cid 0004.0044  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            808a76fc  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      115952         Ticks: 16 (0:00:00:00.250)
        Context Switch Count      17561
        UserTime                  00:00:00.000
        KernelTime                00:00:01.593
        Start Address nt!ExpWorkerThread (0x8087acd6)
        Stack Init f78eb000 Current f78ead00 Base f78eb000 Limit f78e8000 Call 0
        Priority 12 BasePriority 12 PriorityDecrement 0
        ChildEBP RetAddr
        f78ead18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f78ead30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f78ead78 8087ad9e nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f78eadac 809418f4 nt!ExpWorkerThread+0xc8 (FPO: [Non-Fpo])
        f78eaddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 8659d020  Cid 0004.0048  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            808a76fc  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      4302           Ticks: 111666 (0:00:29:04.781)
        Context Switch Count      21
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address nt!ExpWorkerThread (0x8087acd6)
        Stack Init f78ef000 Current f78eed00 Base f78ef000 Limit f78ec000 Call 0
        Priority 13 BasePriority 12 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f78eed18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f78eed30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f78eed78 8087ad9e nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f78eedac 809418f4 nt!ExpWorkerThread+0xc8 (FPO: [Non-Fpo])
        f78eeddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 8659ddb0  Cid 0004.004c  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            808a76fc  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      111781         Ticks: 4187 (0:00:01:05.421)
        Context Switch Count      442
        UserTime                  00:00:00.000
        KernelTime                00:00:00.625
        Start Address nt!ExpWorkerThread (0x8087acd6)
        Stack Init f78f3000 Current f78f2d00 Base f78f3000 Limit f78f0000 Call 0
        Priority 12 BasePriority 12 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f78f2d18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f78f2d30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f78f2d78 8087ad9e nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f78f2dac 809418f4 nt!ExpWorkerThread+0xc8 (FPO: [Non-Fpo])
        f78f2ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 8659db40  Cid 0004.0050  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            808a76fc  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      3534           Ticks: 112434 (0:00:29:16.781)
        Context Switch Count      460
        UserTime                  00:00:00.000
        KernelTime                00:00:00.921
        Start Address nt!ExpWorkerThread (0x8087acd6)
        Stack Init f78f7000 Current f78f6d00 Base f78f7000 Limit f78f4000 Call 0
        Priority 12 BasePriority 12 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f78f6d18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f78f6d30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f78f6d78 8087ad9e nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f78f6dac 809418f4 nt!ExpWorkerThread+0xc8 (FPO: [Non-Fpo])
        f78f6ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 8659d8d0  Cid 0004.0054  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            808a7738  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      114509         Ticks: 1459 (0:00:00:22.796)
        Context Switch Count      290
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Start Address nt!ExpWorkerThread (0x8087acd6)
        Stack Init f78fb000 Current f78fad00 Base f78fb000 Limit f78f8000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0
        ChildEBP RetAddr
        f78fad18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f78fad30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f78fad78 8087ad9e nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f78fadac 809418f4 nt!ExpWorkerThread+0xc8 (FPO: [Non-Fpo])
        f78faddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 8659d660  Cid 0004.0058  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f78fed78  NotificationTimer
            808a76a0  SynchronizationEvent
            808a7690  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      115952         Ticks: 16 (0:00:00:00.250)
        Context Switch Count      1812
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address nt!ExpWorkerThreadBalanceManager (0x80988daa)
        Stack Init f78ff000 Current f78fece0 Base f78ff000 Limit f78fc000 Call 0
        Priority 15 BasePriority 14 PriorityDecrement 1
        ChildEBP RetAddr
        f78fecf8 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f78fed10 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f78fed44 80988e08 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f78fedac 809418f4 nt!ExpWorkerThreadBalanceManager+0x5e (FPO: [Non-Fpo])
        f78feddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 86596020  Cid 0004.005c  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            808a45c0  Semaphore Limit 0x7fffffff
            808a4590  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      91             Ticks: 115877 (0:00:30:10.578)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address nt!MiDereferenceSegmentThread (0x808400b0)
        Stack Init f7903000 Current f7902d0c Base f7903000 Limit f7900000 Call 0
        Priority 18 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f7902d24 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f7902d3c 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f7902d70 80840103 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f7902dac 809418f4 nt!MiDereferenceSegmentThread+0x53 (FPO: [Non-Fpo])
        f7902ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 86596db0  Cid 0004.0060  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            808a4480  NotificationEvent
            8089fe80  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      115009         Ticks: 959 (0:00:00:14.984)
        Context Switch Count      255
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Start Address nt!MiModifiedPageWriter (0x809a2ebc)
        Stack Init f7907000 Current f7906ccc Base f7907000 Limit f7904000 Call 0
        Priority 17 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f7906ce4 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f7906cfc 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f7906d30 808446a3 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f7906d78 809a3035 nt!MiModifiedPageWriterWorker+0x45 (FPO: [Non-Fpo])
        f7906dac 809418f4 nt!MiModifiedPageWriter+0x179 (FPO: [Non-Fpo])
        f7906ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 86596b40  Cid 0004.0064  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f790ad78  SynchronizationTimer
            808a4470  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      115945         Ticks: 23 (0:00:00:00.359)
        Context Switch Count      1814
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address nt!KeBalanceSetManager (0x80882626)
        Stack Init f790b000 Current f790ac90 Base f790b000 Limit f7908000 Call 0
        Priority 16 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f790aca8 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f790acc0 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f790acf4 808826d3 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f790adac 809418f4 nt!KeBalanceSetManager+0xad (FPO: [Non-Fpo])
        f790addc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 865968d0  Cid 0004.0068  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            8089f2e0  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      115932         Ticks: 36 (0:00:00:00.562)
        Context Switch Count      9262
        UserTime                  00:00:00.000
        KernelTime                00:00:00.546
        Start Address nt!KeSwapProcessOrStack (0x80882730)
        Stack Init f790f000 Current f790ed20 Base f790f000 Limit f790c000 Call 0
        Priority 23 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f790ed38 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f790ed50 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f790ed94 8088275b nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f790edac 809418f4 nt!KeSwapProcessOrStack+0x2b (FPO: [1,0,0])
        f790eddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 865979b8  Cid 0004.006c  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            8089db40  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      91             Ticks: 115877 (0:00:30:10.578)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address nt!FsRtlWorkerThread (0x80819dea)
        Stack Init f7913000 Current f7912d14 Base f7913000 Limit f7910000 Call 0
        Priority 16 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f7912d2c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f7912d44 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f7912d8c 80819e1f nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f7912dac 809418f4 nt!FsRtlWorkerThread+0x35 (FPO: [Non-Fpo])
        f7912ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 86597748  Cid 0004.0070  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            8089db68  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      91             Ticks: 115877 (0:00:30:10.578)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address nt!FsRtlWorkerThread (0x80819dea)
        Stack Init f7917000 Current f7916d14 Base f7917000 Limit f7914000 Call 0
        Priority 17 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f7916d2c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f7916d44 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f7916d8c 80819e1f nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f7916dac 809418f4 nt!FsRtlWorkerThread+0x35 (FPO: [Non-Fpo])
        f7916ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 86574988  Cid 0004.0074  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f7372290  NotificationEvent
            f7372280  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      3262           Ticks: 112706 (0:00:29:21.031)
        Context Switch Count      609
        UserTime                  00:00:00.000
        KernelTime                00:00:01.515
        Start Address ACPI!ACPIWorker (0xf7363d22)
        Stack Init f7927000 Current f7926d08 Base f7927000 Limit f7924000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f7926d20 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f7926d38 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f7926d6c f7363d69 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f7926dac 809418f4 ACPI!ACPIWorker+0x47 (FPO: [Non-Fpo])
        f7926ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 8656b020  Cid 0004.0078  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            808a40c0  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      95478          Ticks: 20490 (0:00:05:20.156)
        Context Switch Count      10
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Start Address nt!MiMappedPageWriter (0x808444fe)
        Stack Init f792b000 Current f792acfc Base f792b000 Limit f7928000 Call 0
        Priority 17 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f792ad14 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f792ad2c 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f792ad70 80844552 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f792adac 809418f4 nt!MiMappedPageWriter+0x54 (FPO: [Non-Fpo])
        f792addc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 865a59a0  Cid 0004.007c  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f730bbe0  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      261            Ticks: 115707 (0:00:30:07.921)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address dmio!voliod_loop (0xf72f5f8e)
        Stack Init f792f000 Current f792ed0c Base f792f000 Limit f792c000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f792ed24 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f792ed3c 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f792ed80 f72f6327 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f792edac 809418f4 dmio!voliod_loop+0x399 (FPO: [Non-Fpo])
        f792eddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 864f0020  Cid 0004.0080  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f717d32c  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      4024           Ticks: 111944 (0:00:29:09.125)
        Context Switch Count      9
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address NDIS!ndisWorkerThread (0xf7180a41)
        Stack Init f7933000 Current f7932d18 Base f7933000 Limit f7930000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f7932d30 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f7932d48 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f7932d90 f7180a0e nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f7932dac 809418f4 NDIS!ndisWorkerThread+0x2f (FPO: [Non-Fpo])
        f7932ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 863feb50  Cid 0004.0088  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            86403b50  SynchronizationEvent
            86403b60  SynchronizationEvent
            86403b70  SynchronizationEvent
            86403b80  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      3008           Ticks: 112960 (0:00:29:25.000)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address redbook!RedBookSystemThread (0xf70a8830)
        Stack Init f793f000 Current f793ec88 Base f793f000 Limit f793c000 Call 0
        Priority 16 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f793eca0 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f793ecb8 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f793ecec f70a8937 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f793edac 809418f4 redbook!RedBookSystemThread+0x107 (FPO: [Non-Fpo])
        f793eddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 864aaa08  Cid 0004.0094  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f6ecf1c8  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      2889           Ticks: 113079 (0:00:29:26.859)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address rdpdr!RxBootstrapWorkerThreadDispatcher (0xf6ee1b82)
        Stack Init f794b000 Current f794acec Base f794b000 Limit f7948000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f794ad04 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f794ad1c 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f794ad64 f6ec8449 nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f794ad9c f6ee1b91 rdpdr!RxpWorkerThreadDispatcher+0x4b (FPO: [Non-Fpo])
        f794adac 809418f4 rdpdr!RxBootstrapWorkerThreadDispatcher+0xf (FPO: [Non-Fpo])
        f794addc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 863fe2d8  Cid 0004.0098  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f6ecf090  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      2889           Ticks: 113079 (0:00:29:26.859)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address rdpdr!RxBootstrapWorkerThreadDispatcher (0xf6ee1b82)
        Stack Init f7953000 Current f7952cec Base f7953000 Limit f7950000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f7952d04 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f7952d1c 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f7952d64 f6ec8449 nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f7952d9c f6ee1b91 rdpdr!RxpWorkerThreadDispatcher+0x4b (FPO: [Non-Fpo])
        f7952dac 809418f4 rdpdr!RxBootstrapWorkerThreadDispatcher+0xf (FPO: [Non-Fpo])
        f7952ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 863fddb0  Cid 0004.009c  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f6ecf090  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      2889           Ticks: 113079 (0:00:29:26.859)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address rdpdr!RxBootstrapWorkerThreadDispatcher (0xf6ee1b82)
        Stack Init f7957000 Current f7956cec Base f7957000 Limit f7954000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f7956d04 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f7956d1c 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f7956d64 f6ec8449 nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f7956d9c f6ee1b91 rdpdr!RxpWorkerThreadDispatcher+0x4b (FPO: [Non-Fpo])
        f7956dac 809418f4 rdpdr!RxBootstrapWorkerThreadDispatcher+0xf (FPO: [Non-Fpo])
        f7956ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 8639cdb0  Cid 0004.00a0  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f6ecf090  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      2889           Ticks: 113079 (0:00:29:26.859)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address rdpdr!RxBootstrapWorkerThreadDispatcher (0xf6ee1b82)
        Stack Init f795b000 Current f795acec Base f795b000 Limit f7958000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f795ad04 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f795ad1c 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f795ad64 f6ec8449 nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f795ad9c f6ee1b91 rdpdr!RxpWorkerThreadDispatcher+0x4b (FPO: [Non-Fpo])
        f795adac 809418f4 rdpdr!RxBootstrapWorkerThreadDispatcher+0xf (FPO: [Non-Fpo])
        f795addc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 863fc870  Cid 0004.00a4  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f6ecf090  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      2889           Ticks: 113079 (0:00:29:26.859)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address rdpdr!RxBootstrapWorkerThreadDispatcher (0xf6ee1b82)
        Stack Init f795f000 Current f795ecec Base f795f000 Limit f795c000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f795ed04 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f795ed1c 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f795ed64 f6ec8449 nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f795ed9c f6ee1b91 rdpdr!RxpWorkerThreadDispatcher+0x4b (FPO: [Non-Fpo])
        f795edac 809418f4 rdpdr!RxBootstrapWorkerThreadDispatcher+0xf (FPO: [Non-Fpo])
        f795eddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 86467b00  Cid 0004.00a8  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f6ecf090  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      2889           Ticks: 113079 (0:00:29:26.859)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address rdpdr!RxBootstrapWorkerThreadDispatcher (0xf6ee1b82)
        Stack Init f7963000 Current f7962cec Base f7963000 Limit f7960000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f7962d04 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f7962d1c 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f7962d64 f6ec8449 nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f7962d9c f6ee1b91 rdpdr!RxpWorkerThreadDispatcher+0x4b (FPO: [Non-Fpo])
        f7962dac 809418f4 rdpdr!RxBootstrapWorkerThreadDispatcher+0xf (FPO: [Non-Fpo])
        f7962ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 863d9298  Cid 0004.00ac  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f6ecf12c  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      2889           Ticks: 113079 (0:00:29:26.859)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address rdpdr!RxBootstrapWorkerThreadDispatcher (0xf6ee1b82)
        Stack Init f7967000 Current f7966cec Base f7967000 Limit f7964000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f7966d04 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f7966d1c 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f7966d64 f6ec8449 nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f7966d9c f6ee1b91 rdpdr!RxpWorkerThreadDispatcher+0x4b (FPO: [Non-Fpo])
        f7966dac 809418f4 rdpdr!RxBootstrapWorkerThreadDispatcher+0xf (FPO: [Non-Fpo])
        f7966ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 863fe6f0  Cid 0004.00b0  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f6ecf21c  NotificationEvent
            863fe768  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      114251         Ticks: 1717 (0:00:00:26.828)
        Context Switch Count      30
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address rdpdr!RxSpinUpRequestsDispatcher (0xf6ec8238)
        Stack Init f796b000 Current f796ad00 Base f796b000 Limit f7968000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f796ad18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f796ad30 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f796ad74 f6ec8290 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f796adac 809418f4 rdpdr!RxSpinUpRequestsDispatcher+0x58 (FPO: [Non-Fpo])
        f796addc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 862d5340  Cid 0004.00b8  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f6f9c3d0  SynchronizationEvent
            f6f9c3b0  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      2930           Ticks: 113038 (0:00:29:26.218)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address raspptp!MainPassiveLevelThread (0xf6f8fdee)
        Stack Init f7977000 Current f7976d08 Base f7977000 Limit f7974000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f7976d20 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f7976d38 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f7976d6c f6f8fe1c nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f7976dac 809418f4 raspptp!MainPassiveLevelThread+0x2e (FPO: [Non-Fpo])
        f7976ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 86413020  Cid 0004.00d8  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            862ae604  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      3008           Ticks: 112960 (0:00:29:25.000)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address USBPORT!USBPORT_WorkerThread (0xf7055d44)
        Stack Init f7125000 Current f7124cf8 Base f7125000 Limit f7122000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f7124d10 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f7124d28 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f7124d6c f7055d80 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f7124dac 809418f4 USBPORT!USBPORT_WorkerThread+0x3c (FPO: [Non-Fpo])
        f7124ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 863fd2e8  Cid 0004.00e8  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            863c6a58  NotificationEvent
            863fd360  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      115963         Ticks: 5 (0:00:00:00.078)
        Context Switch Count      355
        UserTime                  00:00:00.000
        KernelTime                00:00:00.046
        Start Address parport!P5FdoThread (0xf70e3324)
        Stack Init f7983000 Current f7982cf0 Base f7983000 Limit f7980000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f7982d08 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f7982d20 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f7982d64 f70e3377 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f7982dac 809418f4 parport!P5FdoThread+0x53 (FPO: [Non-Fpo])
        f7982ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 86453a70  Cid 0004.00ec  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f7792050  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      2972           Ticks: 112996 (0:00:29:25.562)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address rasacd!AcdNotificationRequestThread (0xf7790d38)
        Stack Init f797f000 Current f797ed08 Base f797f000 Limit f797c000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f797ed20 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f797ed38 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f797ed7c f7790e1a nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f797edac 809418f4 rasacd!AcdNotificationRequestThread+0xe2 (FPO: [Uses EBP] [1,2,0])
        f797eddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 8638d020  Cid 0004.00f8  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f6c20908  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      115363         Ticks: 605 (0:00:00:09.453)
        Context Switch Count      90
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address rdbss!RxBootstrapWorkerThreadDispatcher (0xf6c2e4f7)
        Stack Init f797b000 Current f797acec Base f797b000 Limit f7978000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f797ad04 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f797ad1c 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f797ad64 f6c151aa nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f797ad9c f6c2e506 rdbss!RxpWorkerThreadDispatcher+0x4b (FPO: [Non-Fpo])
        f797adac 809418f4 rdbss!RxBootstrapWorkerThreadDispatcher+0xf (FPO: [Non-Fpo])
        f797addc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 8632a1e8  Cid 0004.00fc  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f6c207d0  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      2998           Ticks: 112970 (0:00:29:25.156)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address rdbss!RxBootstrapWorkerThreadDispatcher (0xf6c2e4f7)
        Stack Init f7121000 Current f7120cec Base f7121000 Limit f711e000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f7120d04 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f7120d1c 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f7120d64 f6c151aa nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f7120d9c f6c2e506 rdbss!RxpWorkerThreadDispatcher+0x4b (FPO: [Non-Fpo])
        f7120dac 809418f4 rdbss!RxBootstrapWorkerThreadDispatcher+0xf (FPO: [Non-Fpo])
        f7120ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 863858d8  Cid 0004.0100  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f6c207d0  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      2998           Ticks: 112970 (0:00:29:25.156)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address rdbss!RxBootstrapWorkerThreadDispatcher (0xf6c2e4f7)
        Stack Init f711d000 Current f711ccec Base f711d000 Limit f711a000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f711cd04 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f711cd1c 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f711cd64 f6c151aa nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f711cd9c f6c2e506 rdbss!RxpWorkerThreadDispatcher+0x4b (FPO: [Non-Fpo])
        f711cdac 809418f4 rdbss!RxBootstrapWorkerThreadDispatcher+0xf (FPO: [Non-Fpo])
        f711cddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 862db598  Cid 0004.0104  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f6c207d0  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      115645         Ticks: 323 (0:00:00:05.046)
        Context Switch Count      331
        UserTime                  00:00:00.000
        KernelTime                00:00:00.093
        Start Address rdbss!RxBootstrapWorkerThreadDispatcher (0xf6c2e4f7)
        Stack Init f7119000 Current f7118cec Base f7119000 Limit f7116000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f7118d04 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f7118d1c 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f7118d64 f6c151aa nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f7118d9c f6c2e506 rdbss!RxpWorkerThreadDispatcher+0x4b (FPO: [Non-Fpo])
        f7118dac 809418f4 rdbss!RxBootstrapWorkerThreadDispatcher+0xf (FPO: [Non-Fpo])
        f7118ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 862d5b70  Cid 0004.0108  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f6c207d0  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      5468           Ticks: 110500 (0:00:28:46.562)
        Context Switch Count      13
        UserTime                  00:00:00.000
        KernelTime                00:00:00.078
        Start Address rdbss!RxBootstrapWorkerThreadDispatcher (0xf6c2e4f7)
        Stack Init f7115000 Current f7114cec Base f7115000 Limit f7112000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f7114d04 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f7114d1c 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f7114d64 f6c151aa nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f7114d9c f6c2e506 rdbss!RxpWorkerThreadDispatcher+0x4b (FPO: [Non-Fpo])
        f7114dac 809418f4 rdbss!RxBootstrapWorkerThreadDispatcher+0xf (FPO: [Non-Fpo])
        f7114ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 86371db0  Cid 0004.010c  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f6c207d0  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      115645         Ticks: 323 (0:00:00:05.046)
        Context Switch Count      319
        UserTime                  00:00:00.000
        KernelTime                00:00:00.312
        Start Address rdbss!RxBootstrapWorkerThreadDispatcher (0xf6c2e4f7)
        Stack Init f7111000 Current f7110cec Base f7111000 Limit f710e000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f7110d04 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f7110d1c 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f7110d64 f6c151aa nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f7110d9c f6c2e506 rdbss!RxpWorkerThreadDispatcher+0x4b (FPO: [Non-Fpo])
        f7110dac 809418f4 rdbss!RxBootstrapWorkerThreadDispatcher+0xf (FPO: [Non-Fpo])
        f7110ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 86355d08  Cid 0004.0110  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f6c2086c  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      115203         Ticks: 765 (0:00:00:11.953)
        Context Switch Count      92
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Start Address rdbss!RxBootstrapWorkerThreadDispatcher (0xf6c2e4f7)
        Stack Init f710d000 Current f710ccec Base f710d000 Limit f710a000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f710cd04 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f710cd1c 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f710cd64 f6c151aa nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f710cd9c f6c2e506 rdbss!RxpWorkerThreadDispatcher+0x4b (FPO: [Non-Fpo])
        f710cdac 809418f4 rdbss!RxBootstrapWorkerThreadDispatcher+0xf (FPO: [Non-Fpo])
        f710cddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 86363400  Cid 0004.0114  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f6c2095c  NotificationEvent
            86363478  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      113081         Ticks: 2887 (0:00:00:45.109)
        Context Switch Count      32
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Start Address rdbss!RxSpinUpRequestsDispatcher (0xf6c1562c)
        Stack Init f791b000 Current f791ad00 Base f791b000 Limit f7918000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f791ad18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f791ad30 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f791ad74 f6c15684 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f791adac 809418f4 rdbss!RxSpinUpRequestsDispatcher+0x58 (FPO: [Non-Fpo])
        f791addc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 8633c168  Cid 0004.0118  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            863df760  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      13419          Ticks: 102549 (0:00:26:42.328)
        Context Switch Count      15
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Start Address nt!SepRmCommandServerThread (0x8096ca04)
        Stack Init f791f000 Current f791e9a8 Base f791f000 Limit f791c000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f791e9c0 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f791e9d8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f791ea1c 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f791eacc 8091a8d8 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f791eae8 80883908 nt!NtReplyWaitReceivePort+0x18 (FPO: [Non-Fpo])
        f791eae8 8082d69d nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f791eb00)
        f791eb70 8096ca99 nt!ZwReplyWaitReceivePort+0x11 (FPO: [4,0,0])
        f791edac 809418f4 nt!SepRmCommandServerThread+0x95 (FPO: [Non-Fpo])
        f791eddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 862eadb0  Cid 0004.0264  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f69ea8c8  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      3886           Ticks: 112082 (0:00:29:11.281)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address VsapiNT!IsVsapiWT (0xf69c5f11)
        Stack Init f6a73000 Current f6a72d14 Base f6a73000 Limit f6a70000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f6a72d2c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6a72d44 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6a72d88 f69c5f3e nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6a72dac 809418f4 VsapiNT!IsVsapiWT+0x153
        f6a72ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 8644e740  Cid 0004.0268  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f69ea8c8  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      3886           Ticks: 112082 (0:00:29:11.281)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address VsapiNT!IsVsapiWT (0xf69c5f11)
        Stack Init f6a6f000 Current f6a6ed14 Base f6a6f000 Limit f6a6c000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f6a6ed2c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6a6ed44 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6a6ed88 f69c5f3e nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6a6edac 809418f4 VsapiNT!IsVsapiWT+0x153
        f6a6eddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 8641fb18  Cid 0004.026c  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f69ea8c8  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      3886           Ticks: 112082 (0:00:29:11.281)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address VsapiNT!IsVsapiWT (0xf69c5f11)
        Stack Init f6a6b000 Current f6a6ad14 Base f6a6b000 Limit f6a68000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f6a6ad2c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6a6ad44 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6a6ad88 f69c5f3e nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6a6adac 809418f4 VsapiNT!IsVsapiWT+0x153
        f6a6addc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 8636adb0  Cid 0004.0270  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f6901e28  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      114462         Ticks: 1506 (0:00:00:23.531)
        Context Switch Count      15
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address TmXPFlt (0xf68e5014)
        Stack Init f6a67000 Current f6a66d18 Base f6a67000 Limit f6a64000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f6a66d30 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6a66d48 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6a66d8c f68e504b nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6a66ddc 80887f4a TmXPFlt+0x704b
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 862ff6b0  Cid 0004.0274  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f6901e28  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      102942         Ticks: 13026 (0:00:03:23.531)
        Context Switch Count      25
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Start Address TmXPFlt (0xf68e5014)
        Stack Init f6a5f000 Current f6a5ed18 Base f6a5f000 Limit f6a5c000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f6a5ed30 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6a5ed48 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6a5ed8c f68e504b nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6a5eddc 80887f4a TmXPFlt+0x704b
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 862b4218  Cid 0004.0278  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f6901e28  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      108702         Ticks: 7266 (0:00:01:53.531)
        Context Switch Count      15
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Start Address TmXPFlt (0xf68e5014)
        Stack Init f6a5b000 Current f6a5ad18 Base f6a5b000 Limit f6a58000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f6a5ad30 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6a5ad48 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6a5ad8c f68e504b nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6a5addc 80887f4a TmXPFlt+0x704b
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 864469f0  Cid 0004.027c  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f6901d30  SynchronizationEvent
            f6a56d6c  SynchronizationEvent
            863b6ea8  SynchronizationEvent
            863b4290  SynchronizationEvent
            86446a68  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      115934         Ticks: 34 (0:00:00:00.531)
        Context Switch Count      1756
        UserTime                  00:00:00.000
        KernelTime                00:00:00.046
        Start Address TmXPFlt (0xf68e5641)
        Stack Init f6a57000 Current f6a56c74 Base f6a57000 Limit f6a54000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f6a56c8c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6a56ca4 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6a56cd8 f68e5873 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6a56dac 809418f4 TmXPFlt+0x7873
        f6a56ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 862f50f8  Cid 0004.041c  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            8632cbe4  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      4329           Ticks: 111639 (0:00:29:04.359)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address srv!WorkerThread (0xf66cb602)
        Stack Init f684e000 Current f684dd00 Base f684e000 Limit f684b000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0
        ChildEBP RetAddr
        f684dd18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f684dd30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f684dd78 f66cb67b nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f684ddac 809418f4 srv!WorkerThread+0x7c (FPO: [Non-Fpo])
        f684dddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 860e5db0  Cid 0004.0420  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            8632c984  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      4330           Ticks: 111638 (0:00:29:04.343)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address srv!WorkerThread (0xf66cb602)
        Stack Init f684a000 Current f6849d00 Base f684a000 Limit f6847000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0
        ChildEBP RetAddr
        f6849d18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6849d30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6849d78 f66cb67b nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f6849dac 809418f4 srv!WorkerThread+0x7c (FPO: [Non-Fpo])
        f6849ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
        THREAD 85e09db0  Cid 0004.0424  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f66c8cac  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      4331           Ticks: 111637 (0:00:29:04.328)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address srv!WorkerThread (0xf66cb602)
        Stack Init f685a000 Current f6859d00 Base f685a000 Limit f6857000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0
        ChildEBP RetAddr
        f6859d18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6859d30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6859d78 f66cb67b nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f6859dac 809418f4 srv!WorkerThread+0x7c (FPO: [Non-Fpo])
        f6859ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16

        THREAD 85da9db0  Cid 0004.0470  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f690493c  SynchronizationEvent
            f6902290  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      95290          Ticks: 20678 (0:00:05:23.093)
        Context Switch Count      69
        UserTime                  00:00:00.000
        KernelTime                00:00:02.015
        Start Address TmXPFlt (0xf68e7d2a)
        Stack Init f676e000 Current f676dcec Base f676e000 Limit f676b000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f676dd04 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f676dd1c 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f676dd50 f68e78a3 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f676dd84 f68e7b2d TmXPFlt+0x98a3
        f69023d4 8636adb0 TmXPFlt+0x9b2d
        00000000 00000000 0x8636adb0

        THREAD 862cf7b0  Cid 0004.0474  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f690493c  SynchronizationEvent
            f6902290  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      95297          Ticks: 20671 (0:00:05:22.984)
        Context Switch Count      31
        UserTime                  00:00:00.000
        KernelTime                00:00:00.140
        Start Address TmXPFlt (0xf68e7cc6)
        Stack Init f6782000 Current f6781cf4 Base f6782000 Limit f677f000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f6781d0c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6781d24 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6781d58 f68e78a3 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6781d8c f68e7b2d TmXPFlt+0x98a3
        f69027ac 8636adb0 TmXPFlt+0x9b2d
        00000000 00000000 0x8636adb0
```

```
        THREAD 86304bf0  Cid 0004.0478  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f690493c  SynchronizationEvent
            f6902290  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      95298          Ticks: 20670 (0:00:05:22.968)
        Context Switch Count      45
        UserTime                  00:00:00.000
        KernelTime                00:00:00.375
        Start Address TmXPFlt (0xf68e7cc6)
        Stack Init f6766000 Current f6765cf4 Base f6766000 Limit f6763000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f6765d0c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6765d24 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6765d58 f68e78a3 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6765d8c f68e7b2d TmXPFlt+0x98a3
        f6902b84 8636adb0 TmXPFlt+0x9b2d
        00000000 00000000 0x8636adb0

        THREAD 863e88f8  Cid 0004.047c  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f690493c  SynchronizationEvent
            f6902290  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      95304          Ticks: 20664 (0:00:05:22.875)
        Context Switch Count      31
        UserTime                  00:00:00.000
        KernelTime                00:00:00.234
        Start Address TmXPFlt (0xf68e7cc6)
        Stack Init f6762000 Current f6761cf4 Base f6762000 Limit f675f000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f6761d0c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6761d24 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6761d58 f68e78a3 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6761d8c f68e7b2d TmXPFlt+0x98a3
        f6902f5c 8636adb0 TmXPFlt+0x9b2d
        00000000 00000000 0x8636adb0

        THREAD 86304980  Cid 0004.0480  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f690493c  SynchronizationEvent
            f6902290  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      95308          Ticks: 20660 (0:00:05:22.812)
        Context Switch Count      49
        UserTime                  00:00:00.000
        KernelTime                00:00:00.140
        Start Address TmXPFlt (0xf68e7cc6)
        Stack Init f675e000 Current f675dcf4 Base f675e000 Limit f675b000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f675dd0c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f675dd24 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f675dd58 f68e78a3 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f675dd8c f68e7b2d TmXPFlt+0x98a3
        f6903334 8636adb0 TmXPFlt+0x9b2d
        00000000 00000000 0x8636adb0
```

```
        THREAD 863d0db0  Cid 0004.0484  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f690493c  SynchronizationEvent
            f6902290  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      95308          Ticks: 20660 (0:00:05:22.812)
        Context Switch Count      28
        UserTime                  00:00:00.000
        KernelTime                00:00:00.062
        Start Address TmXPFlt (0xf68e7cc6)
        Stack Init f675a000 Current f6759cf4 Base f675a000 Limit f6757000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f6759d0c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6759d24 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6759d58 f68e78a3 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6759d8c f68e7b2d TmXPFlt+0x98a3
        f690370c 8636adb0 TmXPFlt+0x9b2d
        00000000 00000000 0x8636adb0

        THREAD 8634b938  Cid 0004.0488  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f690493c  SynchronizationEvent
            f6902290  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      95310          Ticks: 20658 (0:00:05:22.781)
        Context Switch Count      31
        UserTime                  00:00:00.000
        KernelTime                00:00:00.062
        Start Address TmXPFlt (0xf68e7cc6)
        Stack Init f6756000 Current f6755cf4 Base f6756000 Limit f6753000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f6755d0c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6755d24 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6755d58 f68e78a3 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6755d8c f68e7b2d TmXPFlt+0x98a3
        f6903ae4 8636adb0 TmXPFlt+0x9b2d
        00000000 00000000 0x8636adb0

        THREAD 86331db0  Cid 0004.048c  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f690493c  SynchronizationEvent
            f6902290  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      95310          Ticks: 20658 (0:00:05:22.781)
        Context Switch Count      42
        UserTime                  00:00:00.000
        KernelTime                00:00:00.140
        Start Address TmXPFlt (0xf68e7cc6)
        Stack Init f6752000 Current f6751cf4 Base f6752000 Limit f674f000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f6751d0c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6751d24 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6751d58 f68e78a3 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6751d8c f68e7b2d TmXPFlt+0x98a3
        f6903ebc 8636adb0 TmXPFlt+0x9b2d
        00000000 00000000 0x8636adb0
```

```
        THREAD 86331600  Cid 0004.0490  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f690493c  SynchronizationEvent
            f6902290  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      95312          Ticks: 20656 (0:00:05:22.750)
        Context Switch Count      40
        UserTime                  00:00:00.000
        KernelTime                00:00:00.218
        Start Address TmXPFlt (0xf68e7cc6)
        Stack Init f673a000 Current f6739cf4 Base f673a000 Limit f6737000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f6739d0c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6739d24 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6739d58 f68e78a3 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6739d8c f68e7b2d TmXPFlt+0x98a3
        f6904294 8636adb0 TmXPFlt+0x9b2d
        00000000 00000000 0x8636adb0

        THREAD 863d0b40  Cid 0004.0494  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            f690493c  SynchronizationEvent
            f6902290  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      95808          Ticks: 20160 (0:00:05:15.000)
        Context Switch Count      27
        UserTime                  00:00:00.000
        KernelTime                00:00:00.156
        Start Address TmXPFlt (0xf68e7cc6)
        Stack Init f6736000 Current f6735cf4 Base f6736000 Limit f6733000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f6735d0c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6735d24 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6735d58 f68e78a3 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6735d8c f68e7b2d TmXPFlt+0x98a3
        f690466c 8636adb0 TmXPFlt+0x9b2d
        00000000 00000000 0x8636adb0

        THREAD 85d78db0  Cid 0004.0500  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown)
KernelMode Non-Alertable
            85d74014  Semaphore Limit 0x400
            85d78e28  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            865a1818       Image:         System
        Wait Start TickCount      115906         Ticks: 62 (0:00:00:00.968)
        Context Switch Count      1734
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address nt!WmipLogger (0x80975000)
        Stack Init f65b5000 Current f65b4cfc Base f65b5000 Limit f65b2000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0
        ChildEBP RetAddr
        f65b4d14 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f65b4d2c 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f65b4d70 809750f4 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f65b4dac 809418f4 nt!WmipLogger+0xf4 (FPO: [Non-Fpo])
        f65b4ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
        00000000 00000000 nt!KiThreadStartup+0x16
```

```
THREAD 85da11e8  Cid 0004.088c  Teb: 00000000 Win32Thread: 00000000 RUNNING on processor 0
Not impersonating
DeviceMap                 e1000170
Owning Process            865a1818       Image:         System
Wait Start TickCount      96768          Ticks: 19200 (0:00:05:00.000)
Context Switch Count      2
UserTime                  00:00:00.000
KernelTime                00:00:00.000
Start Address SystemDump (0xf7991558)
Stack Init f7129000 Current f7128d10 Base f7129000 Limit f7126000 Call 0
Priority 8 BasePriority 8 PriorityDecrement 0
ChildEBP RetAddr
f7128d84 f79915a9 nt!KeBugCheckEx+0x1b (FPO: [Non-Fpo])
f7128dac 809418f4 SystemDump+0x5a9
f7128ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
00000000 00000000 nt!KiThreadStartup+0x16
```

Smss process

```
PROCESS 8631ad88  SessionId: none  Cid: 011c    Peb: 7ffde000  ParentCid: 0004
    DirBase: 3af1a020  ObjectTable: e16e1988  HandleCount:  19.
    Image: smss.exe
    VadRoot 8640f2c0 Vads 15 Clone 0 Private 27. Modified 11. Locked 0.
    DeviceMap e1000170
    Token                             e13f4020
    ElapsedTime                       00:39:20.155
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.187
    QuotaPoolUsage[PagedPool]         6308
    QuotaPoolUsage[NonPagedPool]      600
    Working Set Sizes (now,min,max)  (115, 50, 345) (460KB, 200KB, 1380KB)
    PeakWorkingSetSize                117
    VirtualSize                       3 Mb
    PeakVirtualSize                   11 Mb
    PageFaultCount                    182
    MemoryPriority                    BACKGROUND
    BasePriority                      11
    CommitCharge                      37

    Setting context for this process...
.process /p /r ffffffff8631ad88

    !peb
PEB at 7ffde000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         48580000
    Ldr                       7c8877e0
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00161f18 . 00161f18
    Ldr.InLoadOrderModuleList:           00161eb0 . 00161f08
    Ldr.InMemoryOrderModuleList:         00161eb8 . 00161f10
            Base TimeStamp                     Module
        48580000 45d698f5 Feb 17 05:56:05 2007 \SystemRoot\System32\smss.exe
        7c800000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\ntdll.dll
    SubSystemData:     00000000
    ProcessHeap:       00160000
    ProcessParameters: 00110000
    WindowTitle:  '< Name not readable >'
    ImageFile:    '\SystemRoot\System32\smss.exe'
    CommandLine:  '\SystemRoot\System32\smss.exe'
    DllPath:      'C:\WINDOWS\System32'
    Environment:  00100000
        CommonProgramFiles=
        Path=C:\WINDOWS\System32
        ProgramFiles=
        SystemDrive=C:
        SystemRoot=C:\WINDOWS
```

```
        THREAD 86347518  Cid 011c.0120  Teb: 7ffdd000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            862d0248  ProcessObject
            862dd218  ProcessObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            8631ad88       Image:         smss.exe
        Wait Start TickCount      3540           Ticks: 112428 (0:00:29:16.687)
        Context Switch Count      115
        UserTime                  00:00:00.000
        KernelTime                00:00:00.187
        Start Address smss!NtProcessStartupForGS (0x4858ad8c)
        Stack Init f7923000 Current f7922914 Base f7923000 Limit f7920000 Call 0
        Priority 12 BasePriority 11 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f792292c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f7922944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f7922978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f7922bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f7922d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f7922d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f7922d64)
        0015ff04 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0015ff08 4858a5b4 ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0015ffa4 4858b68b smss!main+0x1cb (FPO: [Non-Fpo])
        0015fff4 00000000 smss!NtProcessStartup+0x236 (FPO: [Non-Fpo])

        THREAD 862d0a70  Cid 011c.0124  Teb: 7ffdc000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            863e0228  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            8631ad88       Image:         smss.exe
        Wait Start TickCount      6299           Ticks: 109669 (0:00:28:33.578)
        Context Switch Count      7
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address smss!SmpApiLoop (0x48589bb3)
        Stack Init f6ff5000 Current f6ff4c0c Base f6ff5000 Limit f6ff2000 Call 0
        Priority 12 BasePriority 11 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6ff4c24 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6ff4c3c 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6ff4c80 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6ff4d30 8091a8d8 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f6ff4d4c 80883908 nt!NtReplyWaitReceivePort+0x18 (FPO: [Non-Fpo])
        f6ff4d4c 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6ff4d64)
        0029fe3c 7c82782b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0029fe40 48589cdc ntdll!ZwReplyWaitReceivePort+0xc (FPO: [4,0,0])
        0029fff4 00000000 smss!SmpApiLoop+0x129 (FPO: [Non-Fpo])
```

```
        THREAD 8633f730  Cid 011c.0128  Teb: 7ffdb000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            863e0228  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            8631ad88       Image:         smss.exe
        Wait Start TickCount      6282           Ticks: 109686 (0:00:28:33.843)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x00000a70
        LPC Server thread working on message Id a70
        Start Address smss!SmpApiLoop (0x48589bb3)
        Stack Init f6ff1000 Current f6ff0c0c Base f6ff1000 Limit f6fee000 Call 0
        Priority 12 BasePriority 11 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6ff0c24 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6ff0c3c 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6ff0c80 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6ff0d30 8091a8d8 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f6ff0d4c 80883908 nt!NtReplyWaitReceivePort+0x18 (FPO: [Non-Fpo])
        f6ff0d4c 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6ff0d64)
        002dfe3c 7c82782b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        002dfe40 48589cdc ntdll!ZwReplyWaitReceivePort+0xc (FPO: [4,0,0])
        002dfff4 00000000 smss!SmpApiLoop+0x129 (FPO: [Non-Fpo])
```

Csrss process

```
PROCESS 862d0248  SessionId: 0  Cid: 0150    Peb: 7ffd4000  ParentCid: 011c
    DirBase: 3af1a040  ObjectTable: e169b530  HandleCount: 384.
    Image: csrss.exe
    VadRoot 862b3248 Vads 104 Clone 0 Private 347. Modified 200. Locked 0.
    DeviceMap e1000170
    Token                             e16f9de0
    ElapsedTime                       00:39:15.484
    UserTime                          00:00:00.140
    KernelTime                        00:00:03.640
    QuotaPoolUsage[PagedPool]         57764
    QuotaPoolUsage[NonPagedPool]      5136
    Working Set Sizes (now,min,max)  (1649, 50, 345) (6596KB, 200KB, 1380KB)
    PeakWorkingSetSize                1651
    VirtualSize                       23 Mb
    PeakVirtualSize                   23 Mb
    PageFaultCount                    3353
    MemoryPriority                    BACKGROUND
    BasePriority                      13
    CommitCharge                      372

    Setting context for this process...
.process /p /r ffffffff862d0248

    !peb
PEB at 7ffd4000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         4a680000
    Ldr                       7c8877e0
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00161f18 . 001672a8
    Ldr.InLoadOrderModuleList:           00161eb0 . 00167298
    Ldr.InMemoryOrderModuleList:         00161eb8 . 001672a0
            Base TimeStamp                     Module
        4a680000 3e800160 Mar 25 07:12:32 2003 \??\C:\WINDOWS\system32\csrss.exe
        7c800000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\ntdll.dll
        75a50000 45d70a89 Feb 17 14:00:41 2007 C:\WINDOWS\system32\CSRSRV.dll
        75a60000 45d70a14 Feb 17 13:58:44 2007 C:\WINDOWS\system32\basesrv.dll
        75a80000 45d70acc Feb 17 14:01:48 2007 C:\WINDOWS\system32\winsrv.dll
        77380000 45d70ac7 Feb 17 14:01:43 2007 C:\WINDOWS\system32\USER32.dll
        77e40000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\KERNEL32.dll
        77c00000 45d70a3e Feb 17 13:59:26 2007 C:\WINDOWS\system32\GDI32.dll
        77f50000 45d70a26 Feb 17 13:59:02 2007 C:\WINDOWS\system32\ADVAPI32.dll
        77c50000 45d70aaa Feb 17 14:01:14 2007 C:\WINDOWS\system32\RPCRT4.dll
        76f50000 45d70ac3 Feb 17 14:01:39 2007 C:\WINDOWS\system32\Secur32.dll
        75da0000 45d70afe Feb 17 14:02:38 2007 C:\WINDOWS\system32\sxs.dll
    SubSystemData:     00000000
    ProcessHeap:       00160000
    ProcessParameters: 00110000
    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'
    Environment:  00100000
        ClusterLog=C:\WINDOWS\Cluster\cluster.log
        ComSpec=C:\WINDOWS\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        NUMBER_OF_PROCESSORS=1
        OS=Windows_NT
        Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
```

```
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 15 Model 5 Stepping 10, AuthenticAMD
        PROCESSOR_LEVEL=15
        PROCESSOR_REVISION=050a
        SystemDrive=C:
        SystemRoot=C:\WINDOWS
        TEMP=C:\WINDOWS\TEMP
        TMP=C:\WINDOWS\TEMP
        windir=C:\WINDOWS


        THREAD 862c6db0  Cid 0150.0158  Teb: 7ffde000 Win32Thread: e10379e8 WAIT: (Unknown)
UserMode Non-Alertable
            862c6f9c  Semaphore Limit 0x1
        Waiting for reply to LPC MessageId 000014be:
        Current LPC port e2519d48
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            862d0248       Image:         csrss.exe
        Wait Start TickCount      19006          Ticks: 96962 (0:00:25:15.031)
        Context Switch Count      6                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.062
        Start Address winsrv!TerminalServerRequestThread (0x75a8e679)
        Stack Init f62f5000 Current f62f4c20 Base f62f5000 Limit f62f2000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f62f4c38 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f62f4c50 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f62f4c94 80916b4c nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f62f4d50 80883908 nt!NtRequestWaitReplyPort+0x776 (FPO: [Non-Fpo])
        f62f4d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f62f4d64)
        0049fe94 7c82787b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0049fe98 75a8e7c2 ntdll!NtRequestWaitReplyPort+0xc (FPO: [3,0,0])
        0049fff4 00000000 winsrv!TerminalServerRequestThread+0x25a (FPO: [Non-Fpo])

        THREAD 863153f0  Cid 0150.015c  Teb: 7ffdd000 Win32Thread: e1988b78 WAIT: (Unknown)
UserMode Alertable
            86343cf8  SynchronizationEvent
            86363348  SynchronizationEvent
            862c18c8  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            862d0248       Image:         csrss.exe
        Wait Start TickCount      24720          Ticks: 91248 (0:00:23:45.750)
        Context Switch Count      21                LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.062
        Start Address winsrv!NotificationThread (0x75a8e877)
        Stack Init f6f0e000 Current f6f0d914 Base f6f0e000 Limit f6f0b000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6f0d92c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6f0d944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6f0d978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6f0dbf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6f0dd48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6f0dd48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6f0dd64)
        004dfd88 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        004dfd8c 75a8e90f ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        004dfff4 00000000 winsrv!NotificationThread+0x142 (FPO: [Non-Fpo])
```

```
        THREAD 864b2db0  Cid 0150.0160  Teb: 7ffdc000 Win32Thread: e16ed8a8 WAIT: (Unknown)
UserMode Non-Alertable
            863e3688  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            862d0248       Image:         csrss.exe
        Wait Start TickCount      113044         Ticks: 2924 (0:00:00:45.687)
        Context Switch Count      396                 LargeStack
        UserTime                  00:00:00.031
        KernelTime                00:00:00.500
        Start Address CSRSRV!CsrApiRequestThread (0x75a548d8)
        Stack Init f7587000 Current f7586c0c Base f7587000 Limit f7584000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f7586c24 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f7586c3c 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f7586c80 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f7586d30 8091a8d8 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f7586d4c 80883908 nt!NtReplyWaitReceivePort+0x18 (FPO: [Non-Fpo])
        f7586d4c 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f7586d64)
        0052feb0 7c82782b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0052feb4 75a54980 ntdll!ZwReplyWaitReceivePort+0xc (FPO: [4,0,0])
        0052fff4 00000000 CSRSRV!CsrApiRequestThread+0xa8 (FPO: [Non-Fpo])

        THREAD 864b2498  Cid 0150.0164  Teb: 7ffdb000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            8640ac60  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            862d0248       Image:         csrss.exe
        Wait Start TickCount      3540           Ticks: 112428 (0:00:29:16.687)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address CSRSRV!CsrSbApiRequestThread (0x75a53b6e)
        Stack Init f6fdd000 Current f6fdcc0c Base f6fdd000 Limit f6fda000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6fdcc24 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6fdcc3c 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6fdcc80 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6fdcd30 8091a8d8 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f6fdcd4c 80883908 nt!NtReplyWaitReceivePort+0x18 (FPO: [Non-Fpo])
        f6fdcd4c 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6fdcd64)
        0064feb0 7c82782b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0064feb4 75a53bb6 ntdll!ZwReplyWaitReceivePort+0xc (FPO: [4,0,0])
        0064fff4 00000000 CSRSRV!CsrSbApiRequestThread+0x48 (FPO: [Non-Fpo])
```

```
        THREAD 862d2db0  Cid 0150.0170  Teb: 7ffda000 Win32Thread: e177bb78 WAIT: (Unknown)
UserMode Non-Alertable
            863e3688  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            862d0248       Image:         csrss.exe
        Wait Start TickCount      114509         Ticks: 1459 (0:00:00:22.796)
        Context Switch Count      587                 LargeStack
        UserTime                  00:00:00.093
        KernelTime                00:00:01.093
        Win32 Start Address 0x000027a6
        LPC Server thread working on message Id 27a6
        Start Address CSRSRV!CsrApiRequestThread (0x75a548d8)
        Stack Init f7597000 Current f7596c0c Base f7597000 Limit f7594000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0
        ChildEBP RetAddr
        f7596c24 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f7596c3c 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f7596c80 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f7596d30 8091a8d8 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f7596d4c 80883908 nt!NtReplyWaitReceivePort+0x18 (FPO: [Non-Fpo])
        f7596d4c 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f7596d64)
        0069feb0 7c82782b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0069feb4 75a54980 ntdll!ZwReplyWaitReceivePort+0xc (FPO: [4,0,0])
        0069fff4 00000000 CSRSRV!CsrApiRequestThread+0xa8 (FPO: [Non-Fpo])

        THREAD 863b3258  Cid 0150.0174  Teb: 7ffd9000 Win32Thread: e1545008 WAIT: (Unknown)
KernelMode Alertable
            8638aca8  SynchronizationEvent
            86445cf0  SynchronizationEvent
            86423170  NotificationTimer
            862cf0a0  SynchronizationEvent
            808a6060  NotificationEvent
            86462ef8  SynchronizationEvent
            8634d288  SynchronizationTimer
        IRP List:
            86359e48: (0006,01b4) Flags: 00000970  Mdl: 00000000
            86341dc8: (0006,0190) Flags: 00000970  Mdl: 00000000
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            862d0248       Image:         csrss.exe
        Wait Start TickCount      115907         Ticks: 61 (0:00:00:00.953)
        Context Switch Count      16622                LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.328
        Start Address winsrv!StartCreateSystemThreads (0x75a8e96c)
        Stack Init f6f7e000 Current f6f7da50 Base f6f7e000 Limit f6f7b000 Call 0
        Priority 13 BasePriority 13 PriorityDecrement 0
        ChildEBP RetAddr
        f6f7da68 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6f7da80 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6f7dab4 bf815345 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6f7dd30 bf870354 win32k!RawInputThread+0x4e0 (FPO: [Non-Fpo])
        f6f7dd40 bf8990c2 win32k!xxxCreateSystemThreads+0x60 (FPO: [Non-Fpo])
        f6f7dd54 80883908 win32k!NtUserCallOneParam+0x23 (FPO: [Non-Fpo])
        f6f7dd54 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6f7dd64)
        006dffe0 75a85298 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00000000 f000ff53 winsrv!NtUserCallOneParam+0xc
        00000000 00000000 0xf000ff53
```

```
        THREAD 862d90f8  Cid 0150.0178  Teb: 7ffd8000 Win32Thread: e1551ea8 WAIT: (Unknown)
UserMode Non-Alertable
            8630f558  SynchronizationEvent
            863af140  SynchronizationEvent
            863454a8  SynchronizationEvent
        IRP List:
            860c60b0: (0006,01b4) Flags: 00000970  Mdl: 00000000
            862e64b8: (0006,0190) Flags: 00000970  Mdl: 00000000
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            862d0248       Image:         csrss.exe
        Wait Start TickCount      97124          Ticks: 18844 (0:00:04:54.437)
        Context Switch Count      4298                LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.765
        Start Address winsrv!StartCreateSystemThreads (0x75a8e96c)
        Stack Init f6f6e000 Current f6f6d9a4 Base f6f6e000 Limit f6f6b000 Call 0
        Priority 15 BasePriority 13 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6f6d9bc 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6f6d9d4 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6f6da08 bf8409e2 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6f6da5c bf817c7b win32k!xxxMsgWaitForMultipleObjects+0xc5 (FPO: [Non-Fpo])
        f6f6dd30 bf87035e win32k!xxxDesktopThread+0x346 (FPO: [Non-Fpo])
        f6f6dd40 bf8990c2 win32k!xxxCreateSystemThreads+0x6a (FPO: [Non-Fpo])
        f6f6dd54 80883908 win32k!NtUserCallOneParam+0x23 (FPO: [Non-Fpo])
        f6f6dd54 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6f6dd64)
        0071ffe0 75a85298 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00000000 f000ff53 winsrv!NtUserCallOneParam+0xc
        00000000 00000000 0xf000ff53

        THREAD 8642bc28  Cid 0150.01ac  Teb: 7ffd7000 Win32Thread: e154f5a8 WAIT: (Unknown)
UserMode Non-Alertable
            865c13d8  SynchronizationEvent
            8642bbf8  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            862d0248       Image:         csrss.exe
        Wait Start TickCount      3726           Ticks: 112242 (0:00:29:13.781)
        Context Switch Count      3                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address winsrv!StartCreateSystemThreads (0x75a8e96c)
        Stack Init f6f4e000 Current f6f4d9a4 Base f6f4e000 Limit f6f4b000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6f4d9bc 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6f4d9d4 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6f4da08 bf8409e2 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6f4da5c bf817c7b win32k!xxxMsgWaitForMultipleObjects+0xc5 (FPO: [Non-Fpo])
        f6f4dd30 bf87035e win32k!xxxDesktopThread+0x346 (FPO: [Non-Fpo])
        f6f4dd40 bf8990c2 win32k!xxxCreateSystemThreads+0x6a (FPO: [Non-Fpo])
        f6f4dd54 80883908 win32k!NtUserCallOneParam+0x23 (FPO: [Non-Fpo])
        f6f4dd54 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6f4dd64)
        00b9ffe0 75a85298 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00000000 f000ff53 winsrv!NtUserCallOneParam+0xc
        00000000 00000000 0xf000ff53
```

```
        THREAD 86387b18  Cid 0150.01d8  Teb: 7ffd6000 Win32Thread: e1837328 WAIT: (Unknown)
UserMode Non-Alertable
            863e3688  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            862d0248       Image:         csrss.exe
        Wait Start TickCount      114484         Ticks: 1484 (0:00:00:23.187)
        Context Switch Count      351                 LargeStack
        UserTime                  00:00:00.015
        KernelTime                00:00:00.343
        Win32 Start Address 0x000027a5
        LPC Server thread working on message Id 27a5
        Start Address CSRSRV!CsrApiRequestThread (0x75a548d8)
        Stack Init f6de8000 Current f6de7c0c Base f6de8000 Limit f6de5000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0
        ChildEBP RetAddr
        f6de7c24 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6de7c3c 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6de7c80 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6de7d30 8091a8d8 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f6de7d4c 80883908 nt!NtReplyWaitReceivePort+0x18 (FPO: [Non-Fpo])
        f6de7d4c 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6de7d64)
        00c5feb0 7c82782b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00c5feb4 75a54980 ntdll!ZwReplyWaitReceivePort+0xc (FPO: [4,0,0])
        00c5fff4 00000000 CSRSRV!CsrApiRequestThread+0xa8 (FPO: [Non-Fpo])

        THREAD 85d7b020  Cid 0150.00bc  Teb: 7ffd5000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d50704  NotificationEvent
        IRP List:
            85d5fda8: (0006,0094) Flags: 00000900  Mdl: 00000000
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            862d0248       Image:         csrss.exe
        Wait Start TickCount      19007          Ticks: 96961 (0:00:25:15.015)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Start Address winsrv!Win32CommandChannelThread (0x75a8c879)
        Stack Init f7987000 Current f7986c78 Base f7987000 Limit f7984000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f7986c90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f7986ca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f7986cec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f7986d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f7986d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f7986d64)
        00fbf6fc 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00fbf700 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        00fbf770 77e61c8d KERNEL32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        00fbf784 77e43a2c KERNEL32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        00fbf798 75a8c8ea KERNEL32!GetOverlappedResult+0x29 (FPO: [Non-Fpo])
        00fbfff4 00000000 winsrv!Win32CommandChannelThread+0x71 (FPO: [Non-Fpo])
```

Winlogon process

```
PROCESS 862dd218  SessionId: 0  Cid: 0168    Peb: 7ffdc000  ParentCid: 011c
    DirBase: 3af1a060  ObjectTable: e145f958  HandleCount: 510.
    Image: winlogon.exe
    VadRoot 86374450 Vads 142 Clone 0 Private 1396. Modified 1803. Locked 0.
    DeviceMap e1000170
    Token                             e1516de0
    ElapsedTime                       00:39:11.859
    UserTime                          00:00:00.890
    KernelTime                        00:00:07.578
    QuotaPoolUsage[PagedPool]         82548
    QuotaPoolUsage[NonPagedPool]      64112
    Working Set Sizes (now,min,max)  (492, 50, 345) (1968KB, 200KB, 1380KB)
    PeakWorkingSetSize                3169
    VirtualSize                       43 Mb
    PeakVirtualSize                   46 Mb
    PageFaultCount                    4157
    MemoryPriority                    BACKGROUND
    BasePriority                      13
    CommitCharge                      1536

    Setting context for this process...
.process /p /r ffffffff862dd218

    !peb
PEB at 7ffdc000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         01000000
    Ldr                       7c8877e0
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00071f18 . 00bfe7d8
    Ldr.InLoadOrderModuleList:           00071eb0 . 00bfe7c8
    Ldr.InMemoryOrderModuleList:         00071eb8 . 00bfe7d0
            Base TimeStamp                     Module
         1000000 45d6c2c2 Feb 17 08:54:26 2007 \??\C:\WINDOWS\system32\winlogon.exe
        7c800000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\ntdll.dll
        77e40000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\kernel32.dll
        77f50000 45d70a26 Feb 17 13:59:02 2007 C:\WINDOWS\system32\ADVAPI32.dll
        77c50000 45d70aaa Feb 17 14:01:14 2007 C:\WINDOWS\system32\RPCRT4.dll
        76f50000 45d70ac3 Feb 17 14:01:39 2007 C:\WINDOWS\system32\Secur32.dll
        761b0000 45d70a80 Feb 17 14:00:32 2007 C:\WINDOWS\system32\CRYPT32.dll
        77ba0000 45d70b06 Feb 17 14:02:46 2007 C:\WINDOWS\system32\msvcrt.dll
        77380000 45d70ac7 Feb 17 14:01:43 2007 C:\WINDOWS\system32\USER32.dll
        77c00000 45d70a3e Feb 17 13:59:26 2007 C:\WINDOWS\system32\GDI32.dll
        76190000 45d70aac Feb 17 14:01:16 2007 C:\WINDOWS\system32\MSASN1.dll
        75810000 45d70a7e Feb 17 14:00:30 2007 C:\WINDOWS\system32\NDdeApi.dll
        75800000 45d70ab2 Feb 17 14:01:22 2007 C:\WINDOWS\system32\PROFMAP.dll
        71c40000 45d70a82 Feb 17 14:00:34 2007 C:\WINDOWS\system32\NETAPI32.dll
        76920000 45d70ac8 Feb 17 14:01:44 2007 C:\WINDOWS\system32\USERENV.dll
        76b70000 45d70ab5 Feb 17 14:01:25 2007 C:\WINDOWS\system32\PSAPI.DLL
        77910000 45d70ab1 Feb 17 14:01:21 2007 C:\WINDOWS\system32\REGAPI.dll
        770e0000 45d70ab3 Feb 17 14:01:23 2007 C:\WINDOWS\system32\SETUPAPI.dll
        77b90000 45d70ac8 Feb 17 14:01:44 2007 C:\WINDOWS\system32\VERSION.dll
        771f0000 45d70ace Feb 17 14:01:50 2007 C:\WINDOWS\system32\WINSTA.dll
        71c00000 45d70ae9 Feb 17 14:02:17 2007 C:\WINDOWS\system32\WS2_32.dll
        71bf0000 45d70aea Feb 17 14:02:18 2007 C:\WINDOWS\system32\WS2HELP.dll
        75840000 45d70ace Feb 17 14:01:50 2007 C:\WINDOWS\system32\MSGINA.dll
        76b40000 45d70ac3 Feb 17 14:01:39 2007 C:\WINDOWS\system32\SHSVCS.dll
        77da0000 45d70ac0 Feb 17 14:01:36 2007 C:\WINDOWS\system32\SHLWAPI.dll
        76b10000 3e80249c Mar 25 09:42:52 2003 C:\WINDOWS\system32\sfc.dll
        76be0000 45d70ab5 Feb 17 14:01:25 2007 C:\WINDOWS\system32\sfc_os.dll
        76bb0000 45d70acf Feb 17 14:01:51 2007 C:\WINDOWS\system32\WINTRUST.dll
        76c10000 45d70a5d Feb 17 13:59:57 2007 C:\WINDOWS\system32\imagehlp.dll
        77670000 45d70aa5 Feb 17 14:01:09 2007 C:\WINDOWS\system32\ole32.dll
```

```
        77420000 45d70a05 Feb 17 13:58:29 2007 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.3790.3959_x-ww_D8713E55\Comctl32.dll
        72430000 45d70ac8 Feb 17 14:01:44 2007 C:\WINDOWS\system32\WINSCARD.DLL
        76f00000 45d70af7 Feb 17 14:02:31 2007 C:\WINDOWS\system32\WTSAPI32.dll
        75da0000 45d70afe Feb 17 14:02:38 2007 C:\WINDOWS\system32\sxs.dll
        76aa0000 45d70af0 Feb 17 14:02:24 2007 C:\WINDOWS\system32\WINMM.dll
        7c8d0000 45d70abb Feb 17 14:01:31 2007 C:\WINDOWS\system32\shell32.dll
        68000000 45d69786 Feb 17 05:49:58 2007 C:\WINDOWS\system32\rsaenh.dll
        76f10000 45d70ad5 Feb 17 14:01:57 2007 C:\WINDOWS\system32\wldap32.dll
        76520000 45d70a87 Feb 17 14:00:39 2007 C:\WINDOWS\system32\cscdll.dll
        5a120000 45d70a4e Feb 17 13:59:42 2007 C:\WINDOWS\system32\dimsntfy.dll
        75820000 45d70ad6 Feb 17 14:01:58 2007 C:\WINDOWS\system32\WlNotify.dll
        73070000 45d70acb Feb 17 14:01:47 2007 C:\WINDOWS\system32\WINSPOOL.DRV
        71bd0000 45d70a84 Feb 17 14:00:36 2007 C:\WINDOWS\system32\MPR.dll
        77d00000 45d70aa6 Feb 17 14:01:10 2007 C:\WINDOWS\system32\OLEAUT32.dll
        77530000 45d70a06 Feb 17 13:58:30 2007 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_5.82.3790.3959_x-ww_78FCF8D0\COMCTL32.dll
        71b70000 45d70acb Feb 17 14:01:47 2007 C:\WINDOWS\system32\UxTheme.dll
        7e020000 45d70aa8 Feb 17 14:01:12 2007 C:\WINDOWS\system32\SAMLIB.dll
        77b00000 45d70a88 Feb 17 14:00:40 2007 C:\WINDOWS\system32\cscui.dll
        777b0000 45d70a3b Feb 17 13:59:23 2007 C:\WINDOWS\system32\CLBCatQ.DLL
        77010000 45d70a76 Feb 17 14:00:22 2007 C:\WINDOWS\system32\COMRes.dll
        77e00000 45d70aab Feb 17 14:01:15 2007 C:\WINDOWS\system32\NTMARTA.DLL
         1330000 45d69418 Feb 17 05:35:20 2007 C:\WINDOWS\system32\xpsp2res.dll
    SubSystemData:     00000000
    ProcessHeap:       00070000
    ProcessParameters: 00020000
    WindowTitle:  '< Name not readable >'
    ImageFile:    '\??\C:\WINDOWS\system32\winlogon.exe'
    CommandLine:  'winlogon.exe'
    DllPath:      'C:\WINDOWS\system32;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem'
    Environment:  00010000
        ALLUSERSPROFILE=C:\Documents and Settings\All Users
        APPDATA=C:\Documents and Settings\Administrator\Application Data
        ClusterLog=C:\WINDOWS\Cluster\cluster.log
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\WINDOWS\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        LOGONSERVER=\\COMPUTERNAME
        NUMBER_OF_PROCESSORS=1
        OS=Windows_NT
        Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 15 Model 5 Stepping 10, AuthenticAMD
        PROCESSOR_LEVEL=15
        PROCESSOR_REVISION=050a
        ProgramFiles=C:\Program Files
        SystemDrive=C:
        SystemRoot=C:\WINDOWS
        TEMP=C:\WINDOWS\TEMP
        TMP=C:\WINDOWS\TEMP
        USERPROFILE=C:\Documents and Settings\Administrator
        windir=C:\WINDOWS
```

```
        THREAD 8640e1b0  Cid 0168.016c  Teb: 7ffdf000 Win32Thread: e177b770 WAIT: (Unknown)
UserMode Non-Alertable
            863b6d28  SynchronizationEvent
        IRP List:
            86547200: (0006,0094) Flags: 00000800  Mdl: 00000000
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            862dd218       Image:         winlogon.exe
        Wait Start TickCount      97056          Ticks: 18912 (0:00:04:55.500)
        Context Switch Count      825                 LargeStack
        UserTime                  00:00:00.734
        KernelTime                00:00:04.250
        Start Address winlogon!__report_gsfailure (0x0103e1b0)
        Stack Init f6f8e000 Current f6f8dc68 Base f6f8e000 Limit f6f8b000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6f8dc80 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6f8dc98 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6f8dcdc bf89b1c3 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6f8dd38 bf89e033 win32k!xxxSleepThread+0x1be (FPO: [Non-Fpo])
        f6f8dd4c bf89e9f1 win32k!xxxRealWaitMessageEx+0x12 (FPO: [Non-Fpo])
        f6f8dd5c 80883908 win32k!NtUserWaitMessage+0x14 (FPO: [0,0,0])
        f6f8dd5c 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6f8dd64)
        0006fd88 7739bf53 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0006fdc0 7738969d USER32!NtUserWaitMessage+0xc
        0006fde8 773896df USER32!InternalDialogBox+0xd0 (FPO: [Non-Fpo])
        0006fe08 77389727 USER32!DialogBoxIndirectParamAorW+0x37 (FPO: [Non-Fpo])
        0006fe2c 0103de0a USER32!DialogBoxParamW+0x3f (FPO: [Non-Fpo])
        0006fe50 0102d838 winlogon!Fusion_DialogBoxParam+0x24 (FPO: [Non-Fpo])
        0006fe8c 0103b6e0 winlogon!TimeoutDialogBoxParam+0x28 (FPO: [Non-Fpo])
        0006fec4 0103746e winlogon!WlxDialogBoxParam+0x80 (FPO: [Non-Fpo])
        0006fee4 01038042 winlogon!BlockWaitForUserAction+0x3a (FPO: [Non-Fpo])
        0006ff08 01031b33 winlogon!MainLoop+0x42d (FPO: [Non-Fpo])
        0006ff50 0103e33b winlogon!WUNotify+0x515 (FPO: [Non-Fpo])
        0006fff4 00000000 winlogon!__report_gsfailure+0x267 (FPO: [Non-Fpo])

        THREAD 8630dc18  Cid 0168.018c  Teb: 7ffd9000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            8630dc90  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            862dd218       Image:         winlogon.exe
        Wait Start TickCount      19251          Ticks: 96717 (0:00:25:11.203)
        Context Switch Count      12
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!RtlpTimerThread (0x7c83d3dd)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6e6d000 Current f6e6cc98 Base f6e6d000 Limit f6e6a000 Call 0
        Priority 13 BasePriority 13 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6e6ccb0 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6e6ccc8 80827e1e nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6e6cd0c 8098c418 nt!KeDelayExecutionThread+0x254 (FPO: [Non-Fpo])
        f6e6cd54 80883908 nt!NtDelayExecution+0x84 (FPO: [Non-Fpo])
        f6e6cd54 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6e6cd64)
        007dff9c 7c826f4b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        007dffa0 7c83d424 ntdll!NtDelayExecution+0xc (FPO: [2,0,0])
        007dffb8 77e64829 ntdll!RtlpTimerThread+0x47 (FPO: [Non-Fpo])
        007dffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 86359698  Cid 0168.0194  Teb: 7ffd7000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            86359710  NotificationTimer
        IRP List:
            865c5100: (0006,0094) Flags: 00000800  Mdl: 00000000
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            862dd218       Image:         winlogon.exe
        Wait Start TickCount      107354         Ticks: 8614 (0:00:02:14.593)
        Context Switch Count      9
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x77c7b0f5)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6e65000 Current f6e64c98 Base f6e65000 Limit f6e62000 Call 0
        Priority 13 BasePriority 13 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6e64cb0 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6e64cc8 80827e1e nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6e64d0c 8098c418 nt!KeDelayExecutionThread+0x254 (FPO: [Non-Fpo])
        f6e64d54 80883908 nt!NtDelayExecution+0x84 (FPO: [Non-Fpo])
        f6e64d54 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6e64d64)
        0086ff70 7c826f4b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0086ff74 77c8884c ntdll!NtDelayExecution+0xc (FPO: [2,0,0])
        0086ff8c 77c88768 RPCRT4!TIMER::Wait+0x2b (FPO: [Non-Fpo])
        0086ffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0xe8 (FPO: [Non-Fpo])
        0086ffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        0086ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 8642fdb0  Cid 0168.01a0  Teb: 7ffd6000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            86307260  NotificationTimer
            8638ed88  ProcessObject
            86342988  ProcessObject
            863f1650  NotificationEvent
            862eeb60  NotificationEvent
            8644d4a8  NotificationEvent
            8645bc18  SynchronizationEvent
            863b5268  SynchronizationEvent
            86421ab0  NotificationEvent
            85d5f9e8  SynchronizationEvent
            85d47e58  SynchronizationEvent
            860bb190  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            862dd218       Image:         winlogon.exe
        Wait Start TickCount      19180          Ticks: 96788 (0:00:25:12.312)
        Context Switch Count      28
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address ntdll!RtlpWaitThread (0x7c83c643)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6e5d000 Current f6e5c914 Base f6e5d000 Limit f6e5a000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6e5c92c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6e5c944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6e5c978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6e5cbf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6e5cd48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6e5cd48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6e5cd64)
        008afcec 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        008afcf0 7c83c78e ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        008affb8 77e64829 ntdll!RtlpWaitThread+0x161 (FPO: [Non-Fpo])
        008affec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 8630fdb0  Cid 0168.0298  Teb: 7ffdd000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            863234d8  Thread
            8630b7d8  Thread
            8631a558  Thread
        IRP List:
            863446b0: (0006,01b4) Flags: 00000000  Mdl: 00000000
            862f08a0: (0006,01b4) Flags: 00000000  Mdl: 00000000
            862f0a60: (0006,01b4) Flags: 00000000  Mdl: 00000000
            863b0888: (0006,01b4) Flags: 00000000  Mdl: 00000000
            863b0a48: (0006,01b4) Flags: 00000000  Mdl: 00000000
            8644d5a0: (0006,01b4) Flags: 00000000  Mdl: 00000000
            8644d760: (0006,01b4) Flags: 00000000  Mdl: 00000000
            862eec88: (0006,01b4) Flags: 00000000  Mdl: 00000000
            862eee48: (0006,01b4) Flags: 00000000  Mdl: 00000000
            86349be0: (0006,01b4) Flags: 00000000  Mdl: 00000000
            86349da0: (0006,01b4) Flags: 00000000  Mdl: 00000000
            86316830: (0006,01b4) Flags: 00000000  Mdl: 00000000
            863169f0: (0006,01b4) Flags: 00000000  Mdl: 00000000
            862f9c88: (0006,01b4) Flags: 00000000  Mdl: 00000000
            862f9e48: (0006,01b4) Flags: 00000000  Mdl: 00000000
            8639c790: (0006,01b4) Flags: 00000000  Mdl: 00000000
            8639c950: (0006,01b4) Flags: 00000000  Mdl: 00000000
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            862dd218       Image:         winlogon.exe
        Wait Start TickCount      11392          Ticks: 104576 (0:00:27:14.000)
        Context Switch Count      9
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address sfc_os!SfcWatchProtectedDirectoriesThread (0x76becac1)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6a47000 Current f6a46914 Base f6a47000 Limit f6a44000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6a4692c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6a46944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6a46978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6a46bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6a46d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6a46d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6a46d64)
        008eff64 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        008eff68 76bece84 ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        008effb8 77e64829 sfc_os!SfcWatchProtectedDirectoriesThread+0x3c3 (FPO: [Non-Fpo])
        008effec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 863234d8  Cid 0168.02a0  Teb: 7ffae000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            86409d28  NotificationEvent
            8630fd80  NotificationEvent
            8630fd50  NotificationEvent
            8630fd20  NotificationEvent
            8630fcf0  NotificationEvent
            86438020  NotificationEvent
            862ed7c0  NotificationEvent
            862ed790  NotificationEvent
            862ed760  NotificationEvent
            862ed730  NotificationEvent
            862ed700  NotificationEvent
            862ed6d0  NotificationEvent
            862ed6a0  NotificationEvent
            862ed670  NotificationEvent
            86443648  NotificationEvent
            86443618  NotificationEvent
            864435e8  NotificationEvent
            864435b8  NotificationEvent
            86443588  NotificationEvent
            86443558  NotificationEvent
            86443528  NotificationEvent
            864434f8  NotificationEvent
            862d8e30  NotificationEvent
            862d8e00  NotificationEvent
            862d8dd0  NotificationEvent
            862d8da0  NotificationEvent
            862d8d70  NotificationEvent
            862d8d40  NotificationEvent
            862d8d10  NotificationEvent
            862d8ce0  NotificationEvent
            86442460  NotificationEvent
            86442430  NotificationEvent
            86442400  NotificationEvent
            864423d0  NotificationEvent
            864423a0  NotificationEvent
            86442370  NotificationEvent
            86442340  NotificationEvent
            86442310  NotificationEvent
            86359a60  NotificationEvent
            86359a30  NotificationEvent
            86359a00  NotificationEvent
            863599d0  NotificationEvent
            863599a0  NotificationEvent
            86359970  NotificationEvent
            86359940  NotificationEvent
            86359910  NotificationEvent
            8634d588  NotificationEvent
            8634d558  NotificationEvent
            8638ca58  NotificationEvent
            8634d528  NotificationEvent
            8638d5e8  NotificationEvent
            8634d4f8  NotificationEvent
            862ff218  NotificationEvent
            8634d4c8  NotificationEvent
            862da930  NotificationEvent
            8634d498  NotificationEvent
            8630c240  NotificationEvent
            8634d468  NotificationEvent
            8634d438  NotificationEvent
            8644b830  NotificationEvent
            862da458  NotificationEvent
            86431bf8  NotificationEvent
            8639b4c0  NotificationEvent
            8639b490  NotificationEvent
        IRP List:
            85d45d50: (0006,01b4) Flags: 00000000  Mdl: 00000000
            860ca478: (0006,01b4) Flags: 00000000  Mdl: 00000000
            860e67c0: (0006,01b4) Flags: 00000000  Mdl: 00000000
```

```
Not impersonating
DeviceMap                 e1000170
Owning Process            862dd218       Image:         winlogon.exe
Wait Start TickCount      92451          Ticks: 23517 (0:00:06:07.453)
Context Switch Count      42
UserTime                  00:00:00.000
KernelTime                00:00:00.015
Win32 Start Address sfc_os!SfcWatchProtectedDirectoriesWorkerThread (0x76bec805)
Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
Stack Init f6a3f000 Current f6a3e914 Base f6a3f000 Limit f6a3c000 Call 0
Priority 14 BasePriority 13 PriorityDecrement 0
Kernel stack not resident.
ChildEBP RetAddr
f6a3e92c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
f6a3e944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
f6a3e978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
f6a3ebf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
f6a3ed48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
f6a3ed48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6a3ed64)
009eff54 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
009eff58 76beca80 ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
009effb8 77e64829 sfc_os!SfcWatchProtectedDirectoriesWorkerThread+0x27b (FPO: [Non-Fpo])
009effec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 8630b7d8  Cid 0168.02a4  Teb: 7ffad000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            86409d28  NotificationEvent
            864030f0  NotificationEvent
            864030c0  NotificationEvent
            862cbc70  NotificationEvent
            862cbc40  NotificationEvent
            863be5c0  NotificationEvent
            863be590  NotificationEvent
            862f2698  NotificationEvent
            862f2668  NotificationEvent
            862f7258  NotificationEvent
            862f7228  NotificationEvent
            86457c70  NotificationEvent
            86457c40  NotificationEvent
            863a0c70  NotificationEvent
            863a0c40  NotificationEvent
            8641c4e8  NotificationEvent
            8641c4b8  NotificationEvent
            8641c488  NotificationEvent
            863862c0  NotificationEvent
            86386290  NotificationEvent
            86386260  NotificationEvent
            8637ec70  NotificationEvent
            8637ec40  NotificationEvent
            8637ec10  NotificationEvent
            86321c70  NotificationEvent
            86321c40  NotificationEvent
            86321c10  NotificationEvent
            86366c70  NotificationEvent
            86366c40  NotificationEvent
            86366c10  NotificationEvent
            8637b2c0  NotificationEvent
            8637b290  NotificationEvent
            8637b260  NotificationEvent
            8637b230  NotificationEvent
            86416958  NotificationEvent
            86416928  NotificationEvent
            864168f8  NotificationEvent
            864168c8  NotificationEvent
            8632f290  NotificationEvent
            8632f260  NotificationEvent
            8632f230  NotificationEvent
            8632f200  NotificationEvent
            8646b290  NotificationEvent
            8646b260  NotificationEvent
            8646b230  NotificationEvent
            8646b200  NotificationEvent
            863fcbf8  NotificationEvent
            863fcbc8  NotificationEvent
            863fcb98  NotificationEvent
            863fcb68  NotificationEvent
            86410298  NotificationEvent
            86410268  NotificationEvent
            86410238  NotificationEvent
            86410208  NotificationEvent
            86405298  NotificationEvent
            86405268  NotificationEvent
            86405238  NotificationEvent
            86405208  NotificationEvent
            8640b8d8  NotificationEvent
            8640b8a8  NotificationEvent
            8640b878  NotificationEvent
            8640b848  NotificationEvent
            8640b818  NotificationEvent
            8640b7e8  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            862dd218       Image:         winlogon.exe
        Wait Start TickCount      3920           Ticks: 112048 (0:00:29:10.750)
```

```
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address sfc_os!SfcWatchProtectedDirectoriesWorkerThread (0x76bec805)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6a3b000 Current f6a3a914 Base f6a3b000 Limit f6a38000 Call 0
        Priority 13 BasePriority 13 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6a3a92c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6a3a944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6a3a978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6a3abf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6a3ad48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6a3ad48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6a3ad64)
        00c5ff54 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00c5ff58 76beca80 ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00c5ffb8 77e64829 sfc_os!SfcWatchProtectedDirectoriesWorkerThread+0x27b (FPO: [Non-Fpo])
        00c5ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 8631a558  Cid 0168.02a8  Teb: 7ffac000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            86409d28  NotificationEvent
            863bca88  NotificationEvent
            863bca58  NotificationEvent
            863bca28  NotificationEvent
            863bc9f8  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            862dd218       Image:         winlogon.exe
        Wait Start TickCount      3920           Ticks: 112048 (0:00:29:10.750)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address sfc_os!SfcWatchProtectedDirectoriesWorkerThread (0x76bec805)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6a37000 Current f6a36914 Base f6a37000 Limit f6a34000 Call 0
        Priority 13 BasePriority 13 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6a3692c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6a36944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6a36978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6a36bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6a36d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6a36d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6a36d64)
        00c9ff54 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00c9ff58 76beca80 ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00c9ffb8 77e64829 sfc_os!SfcWatchProtectedDirectoriesWorkerThread+0x27b (FPO: [Non-Fpo])
        00c9ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 862d1020  Cid 0168.03e8  Teb: 7ffa9000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            862d19c0  NotificationEvent
            862fdeb0  NotificationEvent
            862fd030  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            862dd218       Image:         winlogon.exe
        Wait Start TickCount      19140          Ticks: 96828 (0:00:25:12.937)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address USERENV!NotificationThread (0x76929dd9)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6866000 Current f6865914 Base f6866000 Limit f6863000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f686592c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6865944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6865978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6865bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6865d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6865d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6865d64)
        00e5fec0 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00e5fec4 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00e5ff6c 77e62fbe kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        00e5ff88 76929e35 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        00e5ffb8 77e64829 USERENV!NotificationThread+0x5f (FPO: [Non-Fpo])
        00e5ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 863147a0  Cid 0168.03f8  Teb: 7ffa8000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            86422758  NotificationEvent
            862d1990  SynchronizationEvent
            862d1950  SynchronizationEvent
            8633b640  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            862dd218       Image:         winlogon.exe
        Wait Start TickCount      4306           Ticks: 111662 (0:00:29:04.718)
        Context Switch Count      6
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address USERENV!GPOThread (0x7693d5dd)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6876000 Current f6875914 Base f6876000 Limit f6873000 Call 0
        Priority 13 BasePriority 1 PriorityDecrement 12
        Kernel stack not resident.
        ChildEBP RetAddr
        f687592c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6875944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6875978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6875bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6875d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6875d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6875d64)
        00eafe74 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00eafe78 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00eaff20 77e62fbe kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        00eaff3c 7693d78e kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        00eaffb8 77e64829 USERENV!GPOThread+0x1c2 (FPO: [Non-Fpo])
        00eaffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 863ed670  Cid 0168.0404  Teb: 7ffaa000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            86322d80  SynchronizationEvent
            862f7be8  SynchronizationEvent
            86422988  SynchronizationEvent
            86322d40  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            862dd218       Image:         winlogon.exe
        Wait Start TickCount      4302           Ticks: 111666 (0:00:29:04.781)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address winlogon!WlpExecuteNotify (0x010390b7)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6852000 Current f6851914 Base f6852000 Limit f684f000 Call 0
        Priority 13 BasePriority 13 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f685192c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6851944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6851978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6851bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6851d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6851d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6851d64)
        00ddfe44 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00ddfe48 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00ddfef0 77e62fbe kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        00ddff0c 76522d75 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        00ddff40 76522cb6 cscdll!ReInt_WinMain+0xa6 (FPO: [Non-Fpo])
        00ddff58 76522c8a cscdll!MprServiceProc+0x2d (FPO: [Non-Fpo])
        00ddff60 0103917b cscdll!WinlogonStartupEvent+0x40 (FPO: [1,0,0])
        00ddffb8 77e64829 winlogon!WlpExecuteNotify+0xc4 (FPO: [Non-Fpo])
        00ddffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 8633b768  Cid 0168.0418  Teb: 7ffa4000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            86322d00  SynchronizationEvent
            863033b8  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            862dd218       Image:         winlogon.exe
        Wait Start TickCount      4302           Ticks: 111666 (0:00:29:04.781)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address cscdll!ReInt_AttemptCacheFill (0x765229b0)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6846000 Current f6845914 Base f6846000 Limit f6843000 Call 0
        Priority 11 BasePriority 11 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f684592c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6845944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6845978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6845bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6845d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6845d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6845d64)
        00fbfeb4 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00fbfeb8 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00fbff60 77e62fbe kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        00fbff7c 76522a1c kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        00fbffb8 77e64829 cscdll!ReInt_AttemptCacheFill+0x73 (FPO: [Non-Fpo])
        00fbffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 86394bf0  Cid 0168.06bc  Teb: 7ffd5000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            862dadc8  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            862dd218       Image:         winlogon.exe
        Wait Start TickCount      46162          Ticks: 69806 (0:00:18:10.718)
        Context Switch Count      6
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x77c7b0f5)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6435000 Current f6434c24 Base f6435000 Limit f6432000 Call 0
        Priority 13 BasePriority 13 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6434c3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6434c54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6434c98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6434d48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f6434d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6434d64)
        00e1fe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00e1fe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        00e1ff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        00e1ff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        00e1ffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        00e1ffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        00e1ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 862e2638  Cid 0168.07e0  Teb: 7ffa7000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            863db618  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            862dd218       Image:         winlogon.exe
        Wait Start TickCount      45915          Ticks: 70053 (0:00:18:14.578)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x77c7b0f5)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6399000 Current f6398c24 Base f6399000 Limit f6396000 Call 0
        Priority 13 BasePriority 13 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6398c3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6398c54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6398c98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6398d48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f6398d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6398d64)
        00f3fe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00f3fe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        00f3ff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        00f3ff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        00f3ffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        00f3ffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        00f3ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d41db0  Cid 0168.07e4  Teb: 7ffa6000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            86334c68  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            862dd218       Image:         winlogon.exe
        Wait Start TickCount      26714          Ticks: 89254 (0:00:23:14.593)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x77c7b0f5)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6251000 Current f6250c4c Base f6251000 Limit f624e000 Call 0
        Priority 13 BasePriority 13 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6250c64 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6250c7c 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6250cc4 808e55e2 nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f6250d48 80883908 nt!NtRemoveIoCompletion+0xdc (FPO: [Non-Fpo])
        f6250d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6250d64)
        00f7feac 7c8277db ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00f7feb0 77e5bea2 ntdll!ZwRemoveIoCompletion+0xc (FPO: [5,0,0])
        00f7fedc 77c7b900 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        00f7ff18 77c7b703 RPCRT4!COMMON_ProcessCalls+0xa1 (FPO: [Non-Fpo])
        00f7ff84 77c7b9b5 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x117 (FPO: [Non-Fpo])
        00f7ff8c 77c8872d RPCRT4!ProcessIOEventsWrapper+0xd (FPO: [Non-Fpo])
        00f7ffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        00f7ffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        00f7ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85d7edb0  Cid 0168.07ec  Teb: 7ffa5000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            863db870  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            862dd218       Image:         winlogon.exe
        Wait Start TickCount      50059          Ticks: 65909 (0:00:17:09.828)
        Context Switch Count      7
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x00001c7c
        LPC Server thread working on message Id 1c7c
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6a0b000 Current f6a0ac24 Base f6a0b000 Limit f6a08000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6a0ac3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6a0ac54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6a0ac98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6a0ad48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f6a0ad48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6a0ad64)
        00fffe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00fffe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        00ffff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        00ffff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        00ffffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        00ffffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        00ffffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 860b6a30  Cid 0168.00c8  Teb: 7ffa2000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d5f9b8  NotificationEvent
            85d88d10  SynchronizationEvent
            863539c0  SynchronizationEvent
            863772b0  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            862dd218       Image:         winlogon.exe
        Wait Start TickCount      19495          Ticks: 96473 (0:00:25:07.390)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address USERENV!GPOThread (0x7693d5dd)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6e69000 Current f6e68914 Base f6e69000 Limit f6e66000 Call 0
        Priority 15 BasePriority 1 PriorityDecrement 14
        Kernel stack not resident.
        ChildEBP RetAddr
        f6e6892c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6e68944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6e68978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6e68bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6e68d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6e68d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6e68d64)
        0110fe74 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0110fe78 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0110ff20 77e62fbe kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        0110ff3c 7693d78e kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0110ffb8 77e64829 USERENV!GPOThread+0x1c2 (FPO: [Non-Fpo])
        0110ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85d44020  Cid 0168.0084  Teb: 7ff9b000 Win32Thread: e253d008 WAIT: (Unknown)
UserMode Non-Alertable
            863671a8  QueueObject
            85d44098  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            862dd218       Image:         winlogon.exe
        Wait Start TickCount      114976         Ticks: 992 (0:00:00:15.500)
        Context Switch Count      125                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.265
        Win32 Start Address ntdll!RtlpWorkerThread (0x7c839efb)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f64dd000 Current f64dcc4c Base f64dd000 Limit f64da000 Call 0
        Priority 14 BasePriority 13 PriorityDecrement 0
        ChildEBP RetAddr
        f64dcc64 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f64dcc7c 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f64dccc4 808e55e2 nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f64dcd48 80883908 nt!NtRemoveIoCompletion+0xdc (FPO: [Non-Fpo])
        f64dcd48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f64dcd64)
        0132ff70 7c8277db ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0132ff74 7c839f38 ntdll!ZwRemoveIoCompletion+0xc (FPO: [5,0,0])
        0132ffb8 77e64829 ntdll!RtlpWorkerThread+0x3d (FPO: [Non-Fpo])
        0132ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d7b720  Cid 0168.0288  Teb: 7ffa3000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            86319ee8  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            862dd218       Image:         winlogon.exe
        Wait Start TickCount      50006          Ticks: 65962 (0:00:17:10.656)
        Context Switch Count      5
        UserTime                  00:00:00.031
        KernelTime                00:00:00.031
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x77c7b0f5)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f623d000 Current f623cc24 Base f623d000 Limit f623a000 Call 0
        Priority 13 BasePriority 13 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f623cc3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f623cc54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f623cc98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f623cd48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f623cd48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f623cd64)
        011cfe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        011cfe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        011cff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        011cff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        011cffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        011cffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        011cffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

Services process

```
PROCESS 8638ed88  SessionId: 0  Cid: 0198    Peb: 7ffd7000  ParentCid: 0168
    DirBase: 3af1a080  ObjectTable: e158a3e0  HandleCount: 268.
    Image: services.exe
    VadRoot 86359610 Vads 83 Clone 0 Private 301. Modified 13. Locked 0.
    DeviceMap e1000170
    Token                             e1566630
    ElapsedTime                       00:39:09.780
    UserTime                          00:00:00.078
    KernelTime                        00:00:04.796
    QuotaPoolUsage[PagedPool]         33036
    QuotaPoolUsage[NonPagedPool]      6344
    Working Set Sizes (now,min,max)  (1377, 50, 345) (5508KB, 200KB, 1380KB)
    PeakWorkingSetSize                1377
    VirtualSize                       18 Mb
    PeakVirtualSize                   20 Mb
    PageFaultCount                    1450
    MemoryPriority                    BACKGROUND
    BasePriority                      9
    CommitCharge                      347

    Setting context for this process...
.process /p /r ffffffff8638ed88

    !peb
PEB at 7ffd7000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         01000000
    Ldr                       7c8877e0
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00081f18 . 000b59d8
    Ldr.InLoadOrderModuleList:           00081eb0 . 000b59c8
    Ldr.InMemoryOrderModuleList:         00081eb8 . 000b59d0
            Base TimeStamp                     Module
         1000000 45d6a04e Feb 17 06:27:26 2007 C:\WINDOWS\system32\services.exe
        7c800000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\ntdll.dll
        77e40000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\kernel32.dll
        77ba0000 45d70b06 Feb 17 14:02:46 2007 C:\WINDOWS\system32\msvcrt.dll
        77f50000 45d70a26 Feb 17 13:59:02 2007 C:\WINDOWS\system32\ADVAPI32.dll
        77c50000 45d70aaa Feb 17 14:01:14 2007 C:\WINDOWS\system32\RPCRT4.dll
        76f50000 45d70ac3 Feb 17 14:01:39 2007 C:\WINDOWS\system32\Secur32.dll
        77380000 45d70ac7 Feb 17 14:01:43 2007 C:\WINDOWS\system32\USER32.dll
        77c00000 45d70a3e Feb 17 13:59:26 2007 C:\WINDOWS\system32\GDI32.dll
        76920000 45d70ac8 Feb 17 14:01:44 2007 C:\WINDOWS\system32\USERENV.dll
        757a0000 45d70aaa Feb 17 14:01:14 2007 C:\WINDOWS\system32\SCESRV.dll
        76c40000 45d70a49 Feb 17 13:59:37 2007 C:\WINDOWS\system32\AUTHZ.dll
        71c40000 45d70a82 Feb 17 14:00:34 2007 C:\WINDOWS\system32\NETAPI32.dll
        75770000 45d70ac8 Feb 17 14:01:44 2007 C:\WINDOWS\system32\umpnpmgr.dll
        771f0000 45d70ace Feb 17 14:01:50 2007 C:\WINDOWS\system32\WINSTA.dll
        5fb10000 45d70a7a Feb 17 14:00:26 2007 C:\WINDOWS\system32\NCObjAPI.DLL
          400000 45d6a071 Feb 17 06:28:01 2007 C:\WINDOWS\system32\msvcp60.dll
        75750000 45d70a3a Feb 17 13:59:22 2007 C:\WINDOWS\system32\eventlog.dll
        71c00000 45d70ae9 Feb 17 14:02:17 2007 C:\WINDOWS\system32\WS2_32.dll
        71bf0000 45d70aea Feb 17 14:02:18 2007 C:\WINDOWS\system32\WS2HELP.dll
        76b70000 45d70ab5 Feb 17 14:01:25 2007 C:\WINDOWS\system32\PSAPI.DLL
        76f00000 45d70af7 Feb 17 14:02:31 2007 C:\WINDOWS\system32\wtsapi32.dll
    SubSystemData:     00000000
    ProcessHeap:       00080000
    ProcessParameters: 00020000
    WindowTitle:  'C:\WINDOWS\system32\services.exe'
    ImageFile:    'C:\WINDOWS\system32\services.exe'
    CommandLine:  'C:\WINDOWS\system32\services.exe'
```

```
    DllPath:
'C:\WINDOWS\system32;C:\WINDOWS\system32;C:\WINDOWS\system;C:\WINDOWS;.;C:\WINDOWS\system32;C:\WIND
OWS;C:\WINDOWS\System32\Wbem'
    Environment:  00010000
        ALLUSERSPROFILE=C:\Documents and Settings\All Users
        ClusterLog=C:\WINDOWS\Cluster\cluster.log
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\WINDOWS\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        NUMBER_OF_PROCESSORS=1
        OS=Windows_NT
        Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 15 Model 5 Stepping 10, AuthenticAMD
        PROCESSOR_LEVEL=15
        PROCESSOR_REVISION=050a
        ProgramFiles=C:\Program Files
        SystemDrive=C:
        SystemRoot=C:\WINDOWS
        TEMP=C:\WINDOWS\TEMP
        TMP=C:\WINDOWS\TEMP
        USERPROFILE=C:\Documents and Settings\NetworkService
        windir=C:\WINDOWS


        THREAD 862ecdb0  Cid 0198.01b4  Teb: 7ffde000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            862ece28  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            8638ed88       Image:         services.exe
        Wait Start TickCount      115301         Ticks: 667 (0:00:00:10.421)
        Context Switch Count      30
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address ntdll!RtlpTimerThread (0x7c83d3dd)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6e61000 Current f6e60c98 Base f6e61000 Limit f6e5e000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0
        ChildEBP RetAddr
        f6e60cb0 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6e60cc8 80827e1e nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6e60d0c 8098c418 nt!KeDelayExecutionThread+0x254 (FPO: [Non-Fpo])
        f6e60d54 80883908 nt!NtDelayExecution+0x84 (FPO: [Non-Fpo])
        f6e60d54 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6e60d64)
        005bff9c 7c826f4b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        005bffa0 7c83d424 ntdll!NtDelayExecution+0xc (FPO: [2,0,0])
        005bffb8 77e64829 ntdll!RtlpTimerThread+0x47 (FPO: [Non-Fpo])
        005bffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 862ea730  Cid 0198.01b8  Teb: 7ffdd000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            862ea7a8  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            8638ed88       Image:         services.exe
        Wait Start TickCount      115435         Ticks: 533 (0:00:00:08.328)
        Context Switch Count      56
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address ntdll!RtlpIOWorkerThread (0x7c8193fb)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6e55000 Current f6e54c98 Base f6e55000 Limit f6e52000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0
        ChildEBP RetAddr
        f6e54cb0 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6e54cc8 80827e1e nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6e54d0c 8098c418 nt!KeDelayExecutionThread+0x254 (FPO: [Non-Fpo])
        f6e54d54 80883908 nt!NtDelayExecution+0x84 (FPO: [Non-Fpo])
        f6e54d54 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6e54d64)
        005fff8c 7c826f4b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        005fff90 7c81943a ntdll!NtDelayExecution+0xc (FPO: [2,0,0])
        005fffb8 77e64829 ntdll!RtlpIOWorkerThread+0x3f (FPO: [Non-Fpo])
        005fffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 862b2020  Cid 0198.01bc  Teb: 7ffdc000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            86391aa0  NotificationTimer
            862fbeb0  SynchronizationEvent
            8633a298  ProcessObject
            86316798  NotificationEvent
            862c1c08  ProcessObject
            862d6b30  ProcessObject
            862fdbf0  ProcessObject
            86433518  ProcessObject
            86444d88  ProcessObject
            85de8d88  ProcessObject
            85d7f770  ProcessObject
            85d71020  ProcessObject
            85d6ed88  ProcessObject
            85d6b5f0  ProcessObject
            85d56d88  ProcessObject
            863208c0  NotificationEvent
            85dc8d88  ProcessObject
            86458518  NotificationEvent
            863ae558  NotificationEvent
            86316798  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            8638ed88       Image:         services.exe
        Wait Start TickCount      115301         Ticks: 667 (0:00:00:10.421)
        Context Switch Count      137
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!RtlpWaitThread (0x7c83c643)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6e51000 Current f6e50914 Base f6e51000 Limit f6e4e000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0
        ChildEBP RetAddr
        f6e5092c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6e50944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6e50978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6e50bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6e50d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6e50d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6e50d64)
        0063fcec 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0063fcf0 7c83c78e ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0063ffb8 77e64829 ntdll!RtlpWaitThread+0x161 (FPO: [Non-Fpo])
        0063ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 86443288  Cid 0198.0240  Teb: 7ffdb000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            8632e2b8  QueueObject
            86443300  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            8638ed88       Image:         services.exe
        Wait Start TickCount      115301         Ticks: 667 (0:00:00:10.421)
        Context Switch Count      104
        UserTime                  00:00:00.000
        KernelTime                00:00:00.046
        Win32 Start Address ntdll!RtlpWorkerThread (0x7c839efb)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6a8b000 Current f6a8ac4c Base f6a8b000 Limit f6a88000 Call 0
        Priority 10 BasePriority 9 PriorityDecrement 0
        ChildEBP RetAddr
        f6a8ac64 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6a8ac7c 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6a8acc4 808e55e2 nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f6a8ad48 80883908 nt!NtRemoveIoCompletion+0xdc (FPO: [Non-Fpo])
        f6a8ad48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6a8ad64)
        006aff70 7c8277db ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        006aff74 7c839f38 ntdll!ZwRemoveIoCompletion+0xc (FPO: [5,0,0])
        006affb8 77e64829 ntdll!RtlpWorkerThread+0x3d (FPO: [Non-Fpo])
        006affec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 862bedb0  Cid 0198.0248  Teb: 7ffd9000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            862bee28  NotificationTimer
        IRP List:
            85d5fb28: (0006,0094) Flags: 00000900  Mdl: 00000000
            863d24c8: (0006,0094) Flags: 00000800  Mdl: 00000000
            863d2690: (0006,0094) Flags: 00000800  Mdl: 00000000
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            8638ed88       Image:         services.exe
        Wait Start TickCount      109174         Ticks: 6794 (0:00:01:46.156)
        Context Switch Count      16
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x77c7b0f5)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6a83000 Current f6a82c98 Base f6a83000 Limit f6a80000 Call 0
        Priority 11 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6a82cb0 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6a82cc8 80827e1e nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6a82d0c 8098c418 nt!KeDelayExecutionThread+0x254 (FPO: [Non-Fpo])
        f6a82d54 80883908 nt!NtDelayExecution+0x84 (FPO: [Non-Fpo])
        f6a82d54 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6a82d64)
        0073ff70 7c826f4b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0073ff74 77c8884c ntdll!NtDelayExecution+0xc (FPO: [2,0,0])
        0073ff8c 77c88768 RPCRT4!TIMER::Wait+0x2b (FPO: [Non-Fpo])
        0073ffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0xe8 (FPO: [Non-Fpo])
        0073ffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        0073ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 86303bf0  Cid 0198.0250  Teb: 7ffd8000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            86356de8  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            8638ed88       Image:         services.exe
        Wait Start TickCount      3873           Ticks: 112095 (0:00:29:11.484)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address AUTHZ!AuthzpDeQueueThreadWorker (0x76c44d89)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f7973000 Current f7972c78 Base f7973000 Limit f7970000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f7972c90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f7972ca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f7972cec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f7972d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f7972d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f7972d64)
        0077ff14 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0077ff18 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0077ff88 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        0077ff9c 76c44daf kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0077ffb8 77e64829 AUTHZ!AuthzpDeQueueThreadWorker+0x26 (FPO: [Non-Fpo])
        0077ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 863b52d8  Cid 0198.0258  Teb: 7ffd6000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            862b4498  Semaphore Limit 0x7fffffff
            863b5350  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            8638ed88       Image:         services.exe
        Wait Start TickCount      115949         Ticks: 19 (0:00:00:00.296)
        Context Switch Count      2352
        UserTime                  00:00:00.000
        KernelTime                00:00:00.671
        Win32 Start Address 0x000027d1
        LPC Server thread working on message Id 27d1
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6a8f000 Current f6a8ec24 Base f6a8f000 Limit f6a8c000 Call 0
        Priority 10 BasePriority 9 PriorityDecrement 0
        ChildEBP RetAddr
        f6a8ec3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6a8ec54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6a8ec98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6a8ed48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f6a8ed48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6a8ed64)
        007bfe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        007bfe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        007bff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        007bff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        007bffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        007bffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        007bffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 8645d4c8  Cid 0198.028c  Teb: 7ffd4000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            86447884  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            8638ed88       Image:         services.exe
        Wait Start TickCount      19251          Ticks: 96717 (0:00:25:11.203)
        Context Switch Count      16
        UserTime                  00:00:00.000
        KernelTime                00:00:00.046
        Win32 Start Address services!DispatcherThread (0x0100bfa0)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6a4f000 Current f6a4ec04 Base f6a4f000 Limit f6a4c000 Call 0
        Priority 10 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6a4ec1c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6a4ec34 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6a4ec78 808ed456 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6a4eca0 808ea5ad nt!IopSynchronousServiceTail+0x180 (FPO: [Non-Fpo])
        f6a4ed38 80883908 nt!NtReadFile+0x5d5 (FPO: [Non-Fpo])
        f6a4ed38 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6a4ed64)
        0094fc3c 7c82776b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0094fc40 77e418b2 ntdll!NtReadFile+0xc (FPO: [9,0,0])
        0094fca8 77f65edb kernel32!ReadFile+0x16c (FPO: [Non-Fpo])
        0094fcd4 77f65f82 ADVAPI32!ScGetPipeInput+0x2a (FPO: [Non-Fpo])
        0094fd48 77f51ed9 ADVAPI32!ScDispatcherLoop+0x51 (FPO: [Non-Fpo])
        0094ffac 0100bfb0 ADVAPI32!StartServiceCtrlDispatcherW+0xe3 (FPO: [Non-Fpo])
        0094ffb8 77e64829 services!DispatcherThread+0x10 (FPO: [0,0,1])
        0094ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 86372230  Cid 0198.02ac  Teb: 7ffae000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            862f2630  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            8638ed88       Image:         services.exe
        Wait Start TickCount      5339           Ticks: 110629 (0:00:28:48.578)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000006c5
        LPC Server thread working on message Id 6c5
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6e31000 Current f6e30c0c Base f6e31000 Limit f6e2e000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6e30c24 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6e30c3c 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6e30c80 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6e30d30 8091a8d8 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f6e30d4c 80883908 nt!NtReplyWaitReceivePort+0x18 (FPO: [Non-Fpo])
        f6e30d4c 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6e30d64)
        00a1ff64 7c82782b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00a1ff68 75754a2f ntdll!ZwReplyWaitReceivePort+0xc (FPO: [4,0,0])
        00a1ffb4 757572e9 eventlog!ElfProcessLPCCalls+0x139 (FPO: [Non-Fpo])
        00a1ffb8 77e64829 eventlog!MainLPCThread+0xe (FPO: [1,0,0])
        00a1ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 86369a70  Cid 0198.030c  Teb: 7ffac000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            865c5d98  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            8638ed88       Image:         services.exe
        Wait Start TickCount      11496          Ticks: 104472 (0:00:27:12.375)
        Context Switch Count      6
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address umpnpmgr!ThreadProc_DeviceEvent (0x75776949)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f69ff000 Current f69fecb8 Base f69ff000 Limit f69fc000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f69fecd0 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f69fece8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f69fed2c 80908090 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f69fed4c 80883908 nt!NtGetPlugPlayEvent+0x9a (FPO: [Non-Fpo])
        f69fed4c 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f69fed64)
        00a9fb20 7c82712b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00a9fb24 757769cb ntdll!ZwGetPlugPlayEvent+0xc (FPO: [4,0,0])
        00a9ffb8 77e64829 umpnpmgr!ThreadProc_DeviceEvent+0x7e (FPO: [Non-Fpo])
        00a9ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 86369800  Cid 0198.0310  Teb: 7ffaa000 Win32Thread: e18078f8 WAIT: (Unknown)
UserMode Non-Alertable
            86313250  NotificationEvent
            86390ff0  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            8638ed88       Image:         services.exe
        Wait Start TickCount      20460          Ticks: 95508 (0:00:24:52.312)
        Context Switch Count      10                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.062
        Win32 Start Address umpnpmgr!ThreadProc_DeviceInstall (0x75775458)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f647d000 Current f647c914 Base f647d000 Limit f647a000 Call 0
        Priority 10 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f647c92c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f647c944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f647c978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f647cbf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f647cd48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f647cd48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f647cd64)
        00b1fe58 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00b1fe5c 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00b1ff04 77e62fbe kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        00b1ff20 75774045 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        00b1ffb8 77e64829 umpnpmgr!ThreadProc_DeviceInstall+0x2c3 (FPO: [Non-Fpo])
        00b1ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d5c938  Cid 0198.0614  Teb: 7ffa8000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            8636f4a8  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            8638ed88       Image:         services.exe
        Wait Start TickCount      17018          Ticks: 98950 (0:00:25:46.093)
        Context Switch Count      7
        UserTime                  00:00:00.015
        KernelTime                00:00:00.015
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x77c7b0f5)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6535000 Current f6534c4c Base f6535000 Limit f6532000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6534c64 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6534c7c 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6534cc4 808e55e2 nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f6534d48 80883908 nt!NtRemoveIoCompletion+0xdc (FPO: [Non-Fpo])
        f6534d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6534d64)
        00cafeac 7c8277db ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00cafeb0 77e5bea2 ntdll!ZwRemoveIoCompletion+0xc (FPO: [5,0,0])
        00cafedc 77c7b900 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        00caff18 77c7b703 RPCRT4!COMMON_ProcessCalls+0xa1 (FPO: [Non-Fpo])
        00caff84 77c7b9b5 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x117 (FPO: [Non-Fpo])
        00caff8c 77c8872d RPCRT4!ProcessIOEventsWrapper+0xd (FPO: [Non-Fpo])
        00caffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        00caffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        00caffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85d51650  Cid 0198.064c  Teb: 7ffa7000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            862b4498  Semaphore Limit 0x7fffffff
            85d516c8  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            8638ed88       Image:         services.exe
        Wait Start TickCount      115949         Ticks: 19 (0:00:00:00.296)
        Context Switch Count      1513
        UserTime                  00:00:00.000
        KernelTime                00:00:02.765
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6501000 Current f6500c24 Base f6501000 Limit f64fe000 Call 0
        Priority 10 BasePriority 9 PriorityDecrement 0
        ChildEBP RetAddr
        f6500c3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6500c54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6500c98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6500d48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f6500d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6500d64)
        00cefe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00cefe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        00ceff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        00ceff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        00ceffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        00ceffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        00ceffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d48b40  Cid 0198.0760  Teb: 7ffaf000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            86363ff0  NotificationEvent
            862bf3c0  NotificationEvent
        IRP List:
            8641c880: (0006,0094) Flags: 00000900  Mdl: 00000000
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            8638ed88       Image:         services.exe
        Wait Start TickCount      11267          Ticks: 104701 (0:00:27:15.953)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address NCObjAPI!CNamedPipeClient::CallbackListenThreadProc (0x5fb1459c)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f63e1000 Current f63e0914 Base f63e1000 Limit f63de000 Call 0
        Priority 10 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f63e092c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f63e0944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f63e0978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f63e0bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f63e0d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f63e0d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f63e0d64)
        0006f6a4 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0006f6a8 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0006f750 5fb1464a kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        0006ffb8 77e64829 NCObjAPI!CNamedPipeClient::CallbackListenThreadProc+0xaa (FPO: [Non-Fpo])
        0006ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 860b5db0  Cid 0198.0774  Teb: 7ffa9000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            863b6660  NotificationEvent
            86302250  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            8638ed88       Image:         services.exe
        Wait Start TickCount      96775          Ticks: 19193 (0:00:04:59.890)
        Context Switch Count      13
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address NCObjAPI!CConnection::SendThreadProc (0x5fb11fcb)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f687e000 Current f687d914 Base f687e000 Limit f687b000 Call 0
        Priority 10 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f687d92c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f687d944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f687d978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f687dbf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f687dd48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f687dd48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f687dd64)
        0098fe94 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0098fe98 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0098ff40 77e62fbe kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        0098ff5c 5fb12036 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0098ffb8 77e64829 NCObjAPI!CConnection::SendThreadProc+0x6b (FPO: [Non-Fpo])
        0098ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d44db0  Cid 0198.0154  Teb: 7ffda000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            862b4498  Semaphore Limit 0x7fffffff
            85d44e28  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            8638ed88       Image:         services.exe
        Wait Start TickCount      115949         Ticks: 19 (0:00:00:00.296)
        Context Switch Count      1287
        UserTime                  00:00:00.000
        KernelTime                00:00:00.187
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6411000 Current f6410c24 Base f6411000 Limit f640e000 Call 0
        Priority 10 BasePriority 9 PriorityDecrement 0
        ChildEBP RetAddr
        f6410c3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6410c54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6410c98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6410d48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f6410d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6410d64)
        006ffe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        006ffe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        006fff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        006fff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        006fffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        006fffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        006fffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

Lsass process

```
PROCESS 86342988  SessionId: 0  Cid: 01a4    Peb: 7ffd8000  ParentCid: 0168
    DirBase: 3af1a0a0  ObjectTable: e1553870  HandleCount: 411.
    Image: lsass.exe
    VadRoot 86370848 Vads 152 Clone 0 Private 711. Modified 1. Locked 1.
    DeviceMap e1000170
    Token                             e15932d8
    ElapsedTime                       00:39:09.296
    UserTime                          00:00:00.281
    KernelTime                        00:00:01.921
    QuotaPoolUsage[PagedPool]         56508
    QuotaPoolUsage[NonPagedPool]      13640
    Working Set Sizes (now,min,max)  (2196, 50, 345) (8784KB, 200KB, 1380KB)
    PeakWorkingSetSize                2241
    VirtualSize                       38 Mb
    PeakVirtualSize                   39 Mb
    PageFaultCount                    2484
    MemoryPriority                    BACKGROUND
    BasePriority                      9
    CommitCharge                      1684

    Setting context for this process...
.process /p /r ffffffff86342988

    !peb
PEB at 7ffd8000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         01000000
    Ldr                       7c8877e0
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00081f18 . 000f3508
    Ldr.InLoadOrderModuleList:           00081eb0 . 000f3550
    Ldr.InMemoryOrderModuleList:         00081eb8 . 000f3558
            Base TimeStamp                     Module
         1000000 3e7fffba Mar 25 07:05:30 2003 C:\WINDOWS\system32\lsass.exe
        7c800000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\ntdll.dll
        77e40000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\kernel32.dll
        77f50000 45d70a26 Feb 17 13:59:02 2007 C:\WINDOWS\system32\ADVAPI32.dll
        77c50000 45d70aaa Feb 17 14:01:14 2007 C:\WINDOWS\system32\RPCRT4.dll
        76f50000 45d70ac3 Feb 17 14:01:39 2007 C:\WINDOWS\system32\Secur32.dll
        4ab70000 45d70a62 Feb 17 14:00:02 2007 C:\WINDOWS\system32\LSASRV.dll
        77ba0000 45d70b06 Feb 17 14:02:46 2007 C:\WINDOWS\system32\msvcrt.dll
        77380000 45d70ac7 Feb 17 14:01:43 2007 C:\WINDOWS\system32\USER32.dll
        77c00000 45d70a3e Feb 17 13:59:26 2007 C:\WINDOWS\system32\GDI32.dll
        741d0000 45d70aa9 Feb 17 14:01:13 2007 C:\WINDOWS\system32\SAMSRV.dll
        766e0000 45d70a81 Feb 17 14:00:33 2007 C:\WINDOWS\system32\cryptdll.dll
        76ed0000 45d70a64 Feb 17 14:00:04 2007 C:\WINDOWS\system32\DNSAPI.dll
        71c00000 45d70ae9 Feb 17 14:02:17 2007 C:\WINDOWS\system32\WS2_32.dll
        71bf0000 45d70aea Feb 17 14:02:18 2007 C:\WINDOWS\system32\WS2HELP.dll
        76190000 45d70aac Feb 17 14:01:16 2007 C:\WINDOWS\system32\MSASN1.dll
        71c40000 45d70a82 Feb 17 14:00:34 2007 C:\WINDOWS\system32\NETAPI32.dll
        7e020000 45d70aa8 Feb 17 14:01:12 2007 C:\WINDOWS\system32\SAMLIB.dll
        71bd0000 45d70a84 Feb 17 14:00:36 2007 C:\WINDOWS\system32\MPR.dll
        766f0000 45d70a9f Feb 17 14:01:03 2007 C:\WINDOWS\system32\NTDSAPI.dll
        76f10000 45d70ad5 Feb 17 14:01:57 2007 C:\WINDOWS\system32\WLDAP32.dll
        74130000 3e8024ad Mar 25 09:43:09 2003 C:\WINDOWS\system32\msprivs.dll
        71ca0000 45d70a5d Feb 17 13:59:57 2007 C:\WINDOWS\system32\kerberos.dll
        76c90000 45d70b03 Feb 17 14:02:43 2007 C:\WINDOWS\system32\msv1_0.dll
        76cf0000 45d70a6c Feb 17 14:00:12 2007 C:\WINDOWS\system32\iphlpapi.dll
        76b70000 45d70ab5 Feb 17 14:01:25 2007 C:\WINDOWS\system32\PSAPI.DLL
        74250000 45d70a85 Feb 17 14:00:37 2007 C:\WINDOWS\system32\netlogon.dll
        76710000 45d70ac2 Feb 17 14:01:38 2007 C:\WINDOWS\system32\w32time.dll
          8c0000 45d6a071 Feb 17 06:28:01 2007 C:\WINDOWS\system32\msvcp60.dll
        76920000 45d70ac8 Feb 17 14:01:44 2007 C:\WINDOWS\system32\USERENV.dll
```

```
        76c40000 45d70a49 Feb 17 13:59:37 2007 C:\WINDOWS\system32\AUTHZ.dll
        76750000 45d70aab Feb 17 14:01:15 2007 C:\WINDOWS\system32\schannel.dll
        761b0000 45d70a80 Feb 17 14:00:32 2007 C:\WINDOWS\system32\CRYPT32.dll
        74100000 45d70adc Feb 17 14:02:04 2007 C:\WINDOWS\system32\wdigest.dll
        68000000 45d69786 Feb 17 05:49:58 2007 C:\WINDOWS\system32\rsaenh.dll
        5d9f0000 45d70aa8 Feb 17 14:01:12 2007 C:\WINDOWS\system32\RASSFM.dll
        770e0000 45d70ab3 Feb 17 14:01:23 2007 C:\WINDOWS\system32\setupapi.dll
        63a80000 45d70a5c Feb 17 13:59:56 2007 C:\WINDOWS\system32\KDCSVC.dll
        720e0000 45d70a9e Feb 17 14:01:02 2007 C:\WINDOWS\system32\NTDSA.dll
        71fd0000 45d70aa0 Feb 17 14:01:04 2007 C:\WINDOWS\system32\NTDSATQ.dll
        71b20000 45d70b0d Feb 17 14:02:53 2007 C:\WINDOWS\system32\MSWSOCK.dll
        4b180000 45d70a3c Feb 17 13:59:24 2007 C:\WINDOWS\system32\ESENT.dll
        760f0000 45d70aa9 Feb 17 14:01:13 2007 C:\WINDOWS\system32\scecli.dll
        10000000 45d69413 Feb 17 05:35:15 2007 C:\WINDOWS\system32\WS03RES.DLL
        5f270000 45d70a4a Feb 17 13:59:38 2007 C:\WINDOWS\system32\hnetcfg.dll
        71ae0000 45d70af3 Feb 17 14:02:27 2007 C:\WINDOWS\System32\wshtcpip.dll
        7fe40000 45d70ad9 Feb 17 14:02:01 2007 C:\WINDOWS\system32\ipsecsvc.dll
        4a630000 45d70ad9 Feb 17 14:02:01 2007 C:\WINDOWS\system32\oakley.DLL
        740f0000 45d70aef Feb 17 14:02:23 2007 C:\WINDOWS\system32\WINIPSEC.DLL
        77da0000 45d70ac0 Feb 17 14:01:36 2007 C:\WINDOWS\system32\SHLWAPI.dll
        74120000 45d70abc Feb 17 14:01:32 2007 C:\WINDOWS\system32\pstorsvc.dll
        74140000 45d70ab6 Feb 17 14:01:26 2007 C:\WINDOWS\system32\psbase.dll
        68100000 45d6978b Feb 17 05:50:03 2007 C:\WINDOWS\system32\dssenh.dll
        58f40000 45d70ad3 Feb 17 14:01:55 2007 C:\WINDOWS\system32\wlbsctrl.dll
        77670000 45d70aa5 Feb 17 14:01:09 2007 C:\WINDOWS\system32\ole32.dll
    SubSystemData:     00000000
    ProcessHeap:       00080000
    ProcessParameters: 00020000
    WindowTitle:  'C:\WINDOWS\system32\lsass.exe'
    ImageFile:    'C:\WINDOWS\system32\lsass.exe'
    CommandLine:  'C:\WINDOWS\system32\lsass.exe'
    DllPath:
'C:\WINDOWS\system32;C:\WINDOWS\system32;C:\WINDOWS\system;C:\WINDOWS;.;C:\WINDOWS\system32;C:\WIND
OWS;C:\WINDOWS\System32\Wbem'
    Environment:  00010000
        ALLUSERSPROFILE=C:\Documents and Settings\All Users
        ClusterLog=C:\WINDOWS\Cluster\cluster.log
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\WINDOWS\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        NUMBER_OF_PROCESSORS=1
        OS=Windows_NT
        Path=C:\WINDOWS\System32
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 15 Model 5 Stepping 10, AuthenticAMD
        PROCESSOR_LEVEL=15
        PROCESSOR_REVISION=050a
        ProgramFiles=C:\Program Files
        SystemDrive=C:
        SystemRoot=C:\WINDOWS
        TEMP=C:\WINDOWS\TEMP
        TMP=C:\WINDOWS\TEMP
        USERPROFILE=C:\WINDOWS\system32\config\systemprofile
        windir=C:\WINDOWS
```

```
        THREAD 86351db0  Cid 01a4.01b0  Teb: 7ffde000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            863ffb2c  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86342988       Image:         lsass.exe
        Wait Start TickCount      5322           Ticks: 110646 (0:00:28:48.843)
        Context Switch Count      17
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address LSASRV!ServiceDispatcherThread (0x4ab97323)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6e59000 Current f6e58c04 Base f6e59000 Limit f6e56000 Call 0
        Priority 10 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6e58c1c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6e58c34 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6e58c78 808ed456 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6e58ca0 808ea5ad nt!IopSynchronousServiceTail+0x180 (FPO: [Non-Fpo])
        f6e58d38 80883908 nt!NtReadFile+0x5d5 (FPO: [Non-Fpo])
        f6e58d38 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6e58d64)
        0058fc34 7c82776b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0058fc38 77e418b2 ntdll!NtReadFile+0xc (FPO: [9,0,0])
        0058fca0 77f65edb kernel32!ReadFile+0x16c (FPO: [Non-Fpo])
        0058fccc 77f65f82 ADVAPI32!ScGetPipeInput+0x2a (FPO: [Non-Fpo])
        0058fd40 77f51ed9 ADVAPI32!ScDispatcherLoop+0x51 (FPO: [Non-Fpo])
        0058ffa4 4ab9736e ADVAPI32!StartServiceCtrlDispatcherW+0xe3 (FPO: [Non-Fpo])
        0058ffb8 77e64829 LSASRV!ServiceDispatcherThread+0x6d (FPO: [1,0,0])
        0058ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 86456380  Cid 01a4.01c0  Teb: 7ffdd000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            864563f8  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86342988       Image:         lsass.exe
        Wait Start TickCount      114806         Ticks: 1162 (0:00:00:18.156)
        Context Switch Count      44
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!RtlpTimerThread (0x7c83d3dd)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6e4d000 Current f6e4cc98 Base f6e4d000 Limit f6e4a000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0
        ChildEBP RetAddr
        f6e4ccb0 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6e4ccc8 80827e1e nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6e4cd0c 8098c418 nt!KeDelayExecutionThread+0x254 (FPO: [Non-Fpo])
        f6e4cd54 80883908 nt!NtDelayExecution+0x84 (FPO: [Non-Fpo])
        f6e4cd54 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6e4cd64)
        0060ff9c 7c826f4b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0060ffa0 7c83d424 ntdll!NtDelayExecution+0xc (FPO: [2,0,0])
        0060ffb8 77e64829 ntdll!RtlpTimerThread+0x47 (FPO: [Non-Fpo])
        0060ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 862dbdb0  Cid 01a4.01c4  Teb: 7ffdc000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            8632eed8  QueueObject
            862dbe28  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86342988       Image:         lsass.exe
        Wait Start TickCount      114806         Ticks: 1162 (0:00:00:18.156)
        Context Switch Count      102
        UserTime                  00:00:00.015
        KernelTime                00:00:00.031
        Win32 Start Address ntdll!RtlpWorkerThread (0x7c839efb)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6e49000 Current f6e48c4c Base f6e49000 Limit f6e46000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0
        ChildEBP RetAddr
        f6e48c64 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6e48c7c 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6e48cc4 808e55e2 nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f6e48d48 80883908 nt!NtRemoveIoCompletion+0xdc (FPO: [Non-Fpo])
        f6e48d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6e48d64)
        0064ff70 7c8277db ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0064ff74 7c839f38 ntdll!ZwRemoveIoCompletion+0xc (FPO: [5,0,0])
        0064ffb8 77e64829 ntdll!RtlpWorkerThread+0x3d (FPO: [Non-Fpo])
        0064ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 864559b0  Cid 01a4.01c8  Teb: 7ffdb000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            86469f68  NotificationTimer
            8644b120  Thread
            862ee130  SynchronizationEvent
            863e1b90  SynchronizationEvent
            862c3108  SynchronizationEvent
            863ba130  SynchronizationEvent
            862d3128  SynchronizationEvent
            863826c8  SynchronizationTimer
            8630f178  SynchronizationEvent
            862f93d0  SynchronizationEvent
            86431188  SynchronizationEvent
            862b2320  SynchronizationEvent
            85d6a8d0  NotificationEvent
            85d65d70  SynchronizationEvent
            863351a0  SynchronizationEvent
            85d53130  SynchronizationEvent
            862f8960  SynchronizationEvent
            86431058  SynchronizationEvent
            86371108  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86342988       Image:         lsass.exe
        Wait Start TickCount      107433         Ticks: 8535 (0:00:02:13.359)
        Context Switch Count      43
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!RtlpWaitThread (0x7c83c643)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6e45000 Current f6e44914 Base f6e45000 Limit f6e42000 Call 0
        Priority 10 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6e4492c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6e44944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6e44978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6e44bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6e44d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6e44d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6e44d64)
        0068fcec 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0068fcf0 7c83c78e ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0068ffb8 77e64829 ntdll!RtlpWaitThread+0x161 (FPO: [Non-Fpo])
        0068ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 862dfa58  Cid 01a4.01cc  Teb: 7ffda000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            86436048  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86342988       Image:         lsass.exe
        Wait Start TickCount      3759           Ticks: 112209 (0:00:29:13.265)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address LSASRV!LsapRmServerThread (0x4ab8a05f)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6e41000 Current f6e40c0c Base f6e41000 Limit f6e3e000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6e40c24 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6e40c3c 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6e40c80 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6e40d30 8091a8d8 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f6e40d4c 80883908 nt!NtReplyWaitReceivePort+0x18 (FPO: [Non-Fpo])
        f6e40d4c 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6e40d64)
        006dfe84 7c82782b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        006dfe88 4ab8a0d7 ntdll!ZwReplyWaitReceivePort+0xc (FPO: [4,0,0])
        006dffb8 77e64829 LSASRV!LsapRmServerThread+0x82 (FPO: [Non-Fpo])
        006dffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 862de830  Cid 01a4.01d0  Teb: 7ffd9000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            862d3190  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86342988       Image:         lsass.exe
        Wait Start TickCount      13437          Ticks: 102531 (0:00:26:42.046)
        Context Switch Count      21
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address LSASRV!LsapThreadBase (0x4ab8f39e)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f712d000 Current f712cc78 Base f712d000 Limit f712a000 Call 0
        Priority 10 BasePriority 9 PriorityDecrement 1
        Kernel stack not resident.
        ChildEBP RetAddr
        f712cc90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f712cca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f712ccec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f712cd50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f712cd50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f712cd64)
        0071ff44 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0071ff48 4ab7e6cb ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0071ff78 4ab8f3f5 LSASRV!LsapAdtDequeueThreadWorker+0x36 (FPO: [Non-Fpo])
        0071ffb8 77e64829 LSASRV!LsapThreadBase+0x91 (FPO: [Non-Fpo])
        0071ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 863b1c20  Cid 01a4.01d4  Teb: 7ffd7000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            863b1c98  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86342988       Image:         lsass.exe
        Wait Start TickCount      114037         Ticks: 1931 (0:00:00:30.171)
        Context Switch Count      51
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!RtlpIOWorkerThread (0x7c8193fb)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6e3d000 Current f6e3cc98 Base f6e3d000 Limit f6e3a000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0
        ChildEBP RetAddr
        f6e3ccb0 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6e3ccc8 80827e1e nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6e3cd0c 8098c418 nt!KeDelayExecutionThread+0x254 (FPO: [Non-Fpo])
        f6e3cd54 80883908 nt!NtDelayExecution+0x84 (FPO: [Non-Fpo])
        f6e3cd54 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6e3cd64)
        0076ff8c 7c826f4b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0076ff90 7c81943a ntdll!NtDelayExecution+0xc (FPO: [2,0,0])
        0076ffb8 77e64829 ntdll!RtlpIOWorkerThread+0x3f (FPO: [Non-Fpo])
        0076ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 86344db0  Cid 01a4.01f0  Teb: 7ffd4000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            864f04f0  Semaphore Limit 0x7fffffff
            86344e28  NotificationTimer
        IRP List:
            86444cd0: (0006,0094) Flags: 00000800  Mdl: 00000000
            86348658: (0006,0190) Flags: 00000000  Mdl: 85db2e10
            863d27d0: (0006,0094) Flags: 00000800  Mdl: 00000000
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86342988       Image:         lsass.exe
        Wait Start TickCount      102527         Ticks: 13441 (0:00:03:30.015)
        Context Switch Count      1348
        UserTime                  00:00:00.000
        KernelTime                00:00:00.500
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6e25000 Current f6e24c24 Base f6e25000 Limit f6e22000 Call 0
        Priority 11 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6e24c3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6e24c54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6e24c98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6e24d48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f6e24d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6e24d64)
        009cfe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        009cfe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        009cff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        009cff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        009cffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        009cffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        009cffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 8644b120  Cid 01a4.01fc  Teb: 7ffad000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            86325270  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86342988       Image:         lsass.exe
        Wait Start TickCount      97721          Ticks: 18247 (0:00:04:45.109)
        Context Switch Count      301
        UserTime                  00:00:00.000
        KernelTime                00:00:00.062
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6b8d000 Current f6b8cc0c Base f6b8d000 Limit f6b8a000 Call 0
        Priority 10 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6b8cc24 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6b8cc3c 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6b8cc80 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6b8cd30 8091a8d8 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f6b8cd4c 80883908 nt!NtReplyWaitReceivePort+0x18 (FPO: [Non-Fpo])
        f6b8cd4c 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6b8cd64)
        00a8fe38 7c82782b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00a8fe3c 4ab7a5e6 ntdll!ZwReplyWaitReceivePort+0xc (FPO: [4,0,0])
        00a8ff78 4ab8f3f5 LSASRV!LpcServerThread+0xaf (FPO: [Non-Fpo])
        00a8ffb8 77e64829 LSASRV!LsapThreadBase+0x91 (FPO: [Non-Fpo])
        00a8ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 8634cc20  Cid 01a4.0200  Teb: 7ffac000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            86455978  Semaphore Limit 0x7fffffff
            8634cc98  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86342988       Image:         lsass.exe
        Wait Start TickCount      97719          Ticks: 18249 (0:00:04:45.140)
        Context Switch Count      41
        UserTime                  00:00:00.015
        KernelTime                00:00:00.015
        Win32 Start Address LSASRV!LsapThreadBase (0x4ab8f39e)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6b89000 Current f6b88c78 Base f6b89000 Limit f6b86000 Call 0
        Priority 10 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6b88c90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6b88ca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6b88cec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6b88d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f6b88d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6b88d64)
        00acfea8 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00acfeac 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        00acff1c 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        00acff30 4ab7a7d2 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        00acff50 4ab7a74e LSASRV!WaitForThreadTask+0x49 (FPO: [Non-Fpo])
        00acff78 4ab8f3f5 LSASRV!SpmPoolThreadBase+0xa2 (FPO: [Non-Fpo])
        00acffb8 77e64829 LSASRV!LsapThreadBase+0x91 (FPO: [Non-Fpo])
        00acffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 862bfc38  Cid 01a4.0204  Teb: 7ffab000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            86455978  Semaphore Limit 0x7fffffff
            862bfcb0  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86342988       Image:         lsass.exe
        Wait Start TickCount      97719          Ticks: 18249 (0:00:04:45.140)
        Context Switch Count      58
        UserTime                  00:00:00.015
        KernelTime                00:00:00.109
        Win32 Start Address LSASRV!LsapThreadBase (0x4ab8f39e)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6b85000 Current f6b84c78 Base f6b85000 Limit f6b82000 Call 0
        Priority 10 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6b84c90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6b84ca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6b84cec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6b84d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f6b84d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6b84d64)
        00b0fea8 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00b0feac 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        00b0ff1c 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        00b0ff30 4ab7a7d2 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        00b0ff50 4ab7a74e LSASRV!WaitForThreadTask+0x49 (FPO: [Non-Fpo])
        00b0ff78 4ab8f3f5 LSASRV!SpmPoolThreadBase+0xa2 (FPO: [Non-Fpo])
        00b0ffb8 77e64829 LSASRV!LsapThreadBase+0x91 (FPO: [Non-Fpo])
        00b0ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 863af508  Cid 01a4.0208  Teb: 7ffaa000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            86455978  Semaphore Limit 0x7fffffff
            863af580  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86342988       Image:         lsass.exe
        Wait Start TickCount      97721          Ticks: 18247 (0:00:04:45.109)
        Context Switch Count      31
        UserTime                  00:00:00.015
        KernelTime                00:00:00.031
        Win32 Start Address LSASRV!LsapThreadBase (0x4ab8f39e)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6b81000 Current f6b80c78 Base f6b81000 Limit f6b7e000 Call 0
        Priority 10 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6b80c90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6b80ca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6b80cec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6b80d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f6b80d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6b80d64)
        00b4fea8 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00b4feac 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        00b4ff1c 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        00b4ff30 4ab7a7d2 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        00b4ff50 4ab7a74e LSASRV!WaitForThreadTask+0x49 (FPO: [Non-Fpo])
        00b4ff78 4ab8f3f5 LSASRV!SpmPoolThreadBase+0xa2 (FPO: [Non-Fpo])
        00b4ffb8 77e64829 LSASRV!LsapThreadBase+0x91 (FPO: [Non-Fpo])
        00b4ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 863b9718  Cid 01a4.020c  Teb: 7ffa9000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            86455978  Semaphore Limit 0x7fffffff
            863b9790  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86342988       Image:         lsass.exe
        Wait Start TickCount      97721          Ticks: 18247 (0:00:04:45.109)
        Context Switch Count      29
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address LSASRV!LsapThreadBase (0x4ab8f39e)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6b7d000 Current f6b7cc78 Base f6b7d000 Limit f6b7a000 Call 0
        Priority 10 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6b7cc90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6b7cca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6b7ccec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6b7cd50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f6b7cd50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6b7cd64)
        00b8fea8 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00b8feac 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        00b8ff1c 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        00b8ff30 4ab7a7d2 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        00b8ff50 4ab7a74e LSASRV!WaitForThreadTask+0x49 (FPO: [Non-Fpo])
        00b8ff78 4ab8f3f5 LSASRV!SpmPoolThreadBase+0xa2 (FPO: [Non-Fpo])
        00b8ffb8 77e64829 LSASRV!LsapThreadBase+0x91 (FPO: [Non-Fpo])
        00b8ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 86454730  Cid 01a4.0210  Teb: 7ffa8000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            86455978  Semaphore Limit 0x7fffffff
            864547a8  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86342988       Image:         lsass.exe
        Wait Start TickCount      94706          Ticks: 21262 (0:00:05:32.218)
        Context Switch Count      34
        UserTime                  00:00:00.015
        KernelTime                00:00:00.125
        Win32 Start Address LSASRV!LsapThreadBase (0x4ab8f39e)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6b79000 Current f6b78c78 Base f6b79000 Limit f6b76000 Call 0
        Priority 10 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6b78c90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6b78ca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6b78cec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6b78d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f6b78d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6b78d64)
        00bcfea8 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00bcfeac 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        00bcff1c 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        00bcff30 4ab7a7d2 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        00bcff50 4ab7a74e LSASRV!WaitForThreadTask+0x49 (FPO: [Non-Fpo])
        00bcff78 4ab8f3f5 LSASRV!SpmPoolThreadBase+0xa2 (FPO: [Non-Fpo])
        00bcffb8 77e64829 LSASRV!LsapThreadBase+0x91 (FPO: [Non-Fpo])
        00bcffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 863b57d8  Cid 01a4.0214  Teb: 7ffa7000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            86455978  Semaphore Limit 0x7fffffff
            863b5850  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86342988       Image:         lsass.exe
        Wait Start TickCount      97721          Ticks: 18247 (0:00:04:45.109)
        Context Switch Count      30
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address LSASRV!LsapThreadBase (0x4ab8f39e)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6b75000 Current f6b74c78 Base f6b75000 Limit f6b72000 Call 0
        Priority 10 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6b74c90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6b74ca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6b74cec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6b74d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f6b74d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6b74d64)
        00c0fea8 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00c0feac 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        00c0ff1c 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        00c0ff30 4ab7a7d2 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        00c0ff50 4ab7a74e LSASRV!WaitForThreadTask+0x49 (FPO: [Non-Fpo])
        00c0ff78 4ab8f3f5 LSASRV!SpmPoolThreadBase+0xa2 (FPO: [Non-Fpo])
        00c0ffb8 77e64829 LSASRV!LsapThreadBase+0x91 (FPO: [Non-Fpo])
        00c0ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 862dd580  Cid 01a4.0224  Teb: 7ffa3000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            86455978  Semaphore Limit 0x7fffffff
            862dd5f8  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86342988       Image:         lsass.exe
        Wait Start TickCount      97719          Ticks: 18249 (0:00:04:45.140)
        Context Switch Count      28
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address LSASRV!LsapThreadBase (0x4ab8f39e)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6fd9000 Current f6fd8c78 Base f6fd9000 Limit f6fd6000 Call 0
        Priority 10 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6fd8c90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6fd8ca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6fd8cec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6fd8d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f6fd8d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6fd8d64)
        00d0fea8 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00d0feac 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        00d0ff1c 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        00d0ff30 4ab7a7d2 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        00d0ff50 4ab7a74e LSASRV!WaitForThreadTask+0x49 (FPO: [Non-Fpo])
        00d0ff78 4ab8f3f5 LSASRV!SpmPoolThreadBase+0xa2 (FPO: [Non-Fpo])
        00d0ffb8 77e64829 LSASRV!LsapThreadBase+0x91 (FPO: [Non-Fpo])
        00d0ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 8635a3d8  Cid 01a4.0228  Teb: 7ffa2000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            862de268  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86342988       Image:         lsass.exe
        Wait Start TickCount      3850           Ticks: 112118 (0:00:29:11.843)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address LSASRV!LsapThreadBase (0x4ab8f39e)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6fe1000 Current f6fe0c78 Base f6fe1000 Limit f6fde000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6fe0c90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6fe0ca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6fe0cec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6fe0d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f6fe0d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6fe0d64)
        00d4fea8 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00d4feac 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        00d4ff1c 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        00d4ff30 4ab7a7d2 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        00d4ff50 4ab7a74e LSASRV!WaitForThreadTask+0x49 (FPO: [Non-Fpo])
        00d4ff78 4ab9c401 LSASRV!SpmPoolThreadBase+0xa2 (FPO: [Non-Fpo])
        00d4ffb8 77e64829 LSASRV!LsapThreadBase+0x57 (FPO: [Non-Fpo])
        00d4ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 863ba860  Cid 01a4.022c  Teb: 7ffa1000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            8643c4e0  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86342988       Image:         lsass.exe
        Wait Start TickCount      50419          Ticks: 65549 (0:00:17:04.203)
        Context Switch Count      15
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6fed000 Current f6fecc24 Base f6fed000 Limit f6fea000 Call 0
        Priority 10 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6fecc3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6fecc54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6fecc98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6fecd48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f6fecd48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6fecd64)
        00d8fe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00d8fe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        00d8ff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        00d8ff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        00d8ffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        00d8ffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        00d8ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 862be400  Cid 01a4.0238  Teb: 7ff9e000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            863b1228  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86342988       Image:         lsass.exe
        Wait Start TickCount      34590          Ticks: 81378 (0:00:21:11.531)
        Context Switch Count      6
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x77c7b0f5)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6a93000 Current f6a92c24 Base f6a93000 Limit f6a90000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6a92c3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6a92c54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6a92c98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6a92d48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f6a92d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6a92d64)
        00f4fe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00f4fe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        00f4ff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        00f4ff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        00f4ffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        00f4ffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        00f4ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 86305330  Cid 01a4.024c  Teb: 7ff9c000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            862fc020  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86342988       Image:         lsass.exe
        Wait Start TickCount      97721          Ticks: 18247 (0:00:04:45.109)
        Context Switch Count      41
        UserTime                  00:00:00.000
        KernelTime                00:00:00.046
        Win32 Start Address LSASRV!LsapThreadBase (0x4ab8f39e)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6a7f000 Current f6a7ec78 Base f6a7f000 Limit f6a7c000 Call 0
        Priority 10 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6a7ec90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6a7eca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6a7ecec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6a7ed50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f6a7ed50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6a7ed64)
        00fdfea8 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00fdfeac 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        00fdff1c 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        00fdff30 4ab7a7d2 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        00fdff50 4ab7a74e LSASRV!WaitForThreadTask+0x49 (FPO: [Non-Fpo])
        00fdff78 4ab8f3f5 LSASRV!SpmPoolThreadBase+0xa2 (FPO: [Non-Fpo])
        00fdffb8 77e64829 LSASRV!LsapThreadBase+0x91 (FPO: [Non-Fpo])
        00fdffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 863b4db0  Cid 01a4.0254  Teb: 7ff9d000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            864f04f0  Semaphore Limit 0x7fffffff
            863b4e28  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86342988       Image:         lsass.exe
        Wait Start TickCount      102527         Ticks: 13441 (0:00:03:30.015)
        Context Switch Count      13
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f793b000 Current f793ac24 Base f793b000 Limit f7938000 Call 0
        Priority 10 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f793ac3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f793ac54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f793ac98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f793ad48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f793ad48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f793ad64)
        00f8fe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00f8fe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        00f8ff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        00f8ff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        00f8ffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        00f8ffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        00f8ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85d6e478  Cid 01a4.057c  Teb: 7ff9f000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d6cf50  NotificationEvent
            85d6cd28  NotificationEvent
            85d6cff0  NotificationEvent
            85d6a778  NotificationEvent
            85d6cfc0  NotificationEvent
            85d6cf20  NotificationEvent
        IRP List:
            862c9c30: (0006,0190) Flags: 00000030  Mdl: 00000000
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86342988       Image:         lsass.exe
        Wait Start TickCount      5363           Ticks: 110605 (0:00:28:48.203)
        Context Switch Count      64
        UserTime                  00:00:00.046
        KernelTime                00:00:00.109
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x77f65e70)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f65d5000 Current f65d4914 Base f65d5000 Limit f65d2000 Call 0
        Priority 10 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f65d492c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f65d4944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f65d4978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f65d4bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f65d4d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f65d4d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f65d4d64)
        013cfe28 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        013cfe2c 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        013cfed4 77e62fbe kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        013cfef0 7fe48003 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        013cff3c 7fe50422 ipsecsvc!ServiceWait+0xce (FPO: [Non-Fpo])
        013cff54 4ab96199 ipsecsvc!SPDServiceMain+0x1dd (FPO: [Non-Fpo])
        013cff8c 4ab96633 LSASRV!LsapStartService+0xc0 (FPO: [Non-Fpo])
        013cffa4 77f65e91 LSASRV!SrvLoadIPSecSvcs+0x14 (FPO: [Non-Fpo])
        013cffb8 77e64829 ADVAPI32!ScSvcctrlThreadW+0x21 (FPO: [Non-Fpo])
        013cffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d65400  Cid 01a4.05a8  Teb: 7ff9a000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            85d65e00  NotificationEvent
            85d6b450  SynchronizationEvent
        IRP List:
            85d7d348: (0006,0094) Flags: 00000070  Mdl: 00000000
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86342988       Image:         lsass.exe
        Wait Start TickCount      5359           Ticks: 110609 (0:00:28:48.265)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address msvcrt!_endthreadex (0x77bcb4bc)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6571000 Current f6570914 Base f6571000 Limit f656e000 Call 0
        Priority 11 BasePriority 11 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f657092c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6570944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6570978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6570bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6570d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6570d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6570d64)
        014bfdb0 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        014bfdb4 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        014bfe5c 4a63567d kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        014bff84 77bcb530 oakley!AcquireThread+0x24a (FPO: [Non-Fpo])
        014bffb8 77e64829 msvcrt!_endthreadex+0xa3 (FPO: [Non-Fpo])
        014bffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85d69b40  Cid 01a4.05ac  Teb: 7ff98000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            85d65dd0  NotificationEvent
            85d76320  SynchronizationEvent
            85d6a350  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86342988       Image:         lsass.exe
        Wait Start TickCount      5359           Ticks: 110609 (0:00:28:48.265)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address msvcrt!_endthreadex (0x77bcb4bc)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f656d000 Current f656c914 Base f656d000 Limit f656a000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f656c92c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f656c944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f656c978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f656cbf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f656cd48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f656cd48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f656cd64)
        014ffdf4 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        014ffdf8 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        014ffea0 4a6323b6 kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        014fff84 77bcb530 oakley!ReceiveThread+0x176 (FPO: [Non-Fpo])
        014fffb8 77e64829 msvcrt!_endthreadex+0xa3 (FPO: [Non-Fpo])
        014fffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d698d0  Cid 01a4.05b0  Teb: 7ff97000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            85d65da0  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86342988       Image:         lsass.exe
        Wait Start TickCount      115905         Ticks: 63 (0:00:00:00.984)
        Context Switch Count      1725
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address msvcrt!_endthreadex (0x77bcb4bc)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6569000 Current f6568914 Base f6569000 Limit f6566000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0
        ChildEBP RetAddr
        f656892c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6568944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6568978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6568bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6568d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6568d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6568d64)
        0153feb8 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0153febc 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0153ff64 4a631333 kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        0153ff84 77bcb530 oakley!TimerThread+0x36 (FPO: [Non-Fpo])
        0153ffb8 77e64829 msvcrt!_endthreadex+0xa3 (FPO: [Non-Fpo])
        0153ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85d4da10  Cid 01a4.06b8  Teb: 7ffd5000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            863b7e70  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86342988       Image:         lsass.exe
        Wait Start TickCount      34572          Ticks: 81396 (0:00:21:11.812)
        Context Switch Count      4
        UserTime                  00:00:00.015
        KernelTime                00:00:00.015
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x77c7b0f5)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6441000 Current f6440c24 Base f6441000 Limit f643e000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6440c3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6440c54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6440c98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6440d48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f6440d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6440d64)
        0096fe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0096fe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        0096ff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        0096ff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        0096ffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        0096ffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        0096ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d8d020  Cid 01a4.0780  Teb: 7ff9b000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            862dd0a0  NotificationEvent
            862fdeb0  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86342988       Image:         lsass.exe
        Wait Start TickCount      11433          Ticks: 104535 (0:00:27:13.359)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address USERENV!NotificationThread (0x76929dd9)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6a77000 Current f6a76914 Base f6a77000 Limit f6a74000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6a7692c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6a76944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6a76978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6a76bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6a76d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6a76d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6a76d64)
        0108fec0 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0108fec4 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0108ff6c 77e62fbe kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        0108ff88 76929e35 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0108ffb8 77e64829 USERENV!NotificationThread+0x5f (FPO: [Non-Fpo])
        0108ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 860cadb0  Cid 01a4.03a0  Teb: 7ffd6000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            860cae28  NotificationTimer
        IRP List:
            863d2ab0: (0006,0094) Flags: 00000800  Mdl: 00000000
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86342988       Image:         lsass.exe
        Wait Start TickCount      111913         Ticks: 4055 (0:00:01:03.359)
        Context Switch Count      175
        UserTime                  00:00:00.015
        KernelTime                00:00:00.062
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x77c7b0f5)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f68c2000 Current f68c1c98 Base f68c2000 Limit f68bf000 Call 0
        Priority 10 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f68c1cb0 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f68c1cc8 80827e1e nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f68c1d0c 8098c418 nt!KeDelayExecutionThread+0x254 (FPO: [Non-Fpo])
        f68c1d54 80883908 nt!NtDelayExecution+0x84 (FPO: [Non-Fpo])
        f68c1d54 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f68c1d64)
        008aff70 7c826f4b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        008aff74 77c8884c ntdll!NtDelayExecution+0xc (FPO: [2,0,0])
        008aff8c 77c88768 RPCRT4!TIMER::Wait+0x2b (FPO: [Non-Fpo])
        008affac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0xe8 (FPO: [Non-Fpo])
        008affb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        008affec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d3f520  Cid 01a4.0898  Teb: 7ffaf000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            8644be68  QueueObject
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86342988       Image:         lsass.exe
        Wait Start TickCount      111913         Ticks: 4055 (0:00:01:03.359)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x77c7b0f5)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6215000 Current f6214c4c Base f6215000 Limit f6212000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6214c64 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6214c7c 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6214cc4 808e55e2 nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f6214d48 80883908 nt!NtRemoveIoCompletion+0xdc (FPO: [Non-Fpo])
        f6214d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6214d64)
        0006feac 7c8277db ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0006feb0 77e5bea2 ntdll!ZwRemoveIoCompletion+0xc (FPO: [5,0,0])
        0006fedc 77c7b900 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        0006ff18 77c7b703 RPCRT4!COMMON_ProcessCalls+0xa1 (FPO: [Non-Fpo])
        0006ff84 77c7b9b5 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x117 (FPO: [Non-Fpo])
        0006ff8c 77c8872d RPCRT4!ProcessIOEventsWrapper+0xd (FPO: [Non-Fpo])
        0006ffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        0006ffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        0006ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

Svchost process (DcomLaunch)

```
PROCESS 8633a298  SessionId: 0  Cid: 0280    Peb: 7ffd9000  ParentCid: 0198
    DirBase: 3af1a0c0  ObjectTable: e182f750  HandleCount:  88.
    Image: svchost.exe
    VadRoot 863040d8 Vads 54 Clone 0 Private 133. Modified 2. Locked 0.
    DeviceMap e1000170
    Token                             e1832030
    ElapsedTime                       00:39:06.312
    UserTime                          00:00:00.171
    KernelTime                        00:00:00.359
    QuotaPoolUsage[PagedPool]         36588
    QuotaPoolUsage[NonPagedPool]      2776
    Working Set Sizes (now,min,max)  (1758, 50, 345) (7032KB, 200KB, 1380KB)
    PeakWorkingSetSize                1775
    VirtualSize                       18 Mb
    PeakVirtualSize                   19 Mb
    PageFaultCount                    1839
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      193

    Setting context for this process...
.process /p /r ffffffff8633a298

    !peb
PEB at 7ffd9000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         01000000
    Ldr                       7c8877e0
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00081f18 . 00085fc8
    Ldr.InLoadOrderModuleList:           00081eb0 . 00092c78
    Ldr.InMemoryOrderModuleList:         00081eb8 . 00092c80
            Base TimeStamp                     Module
         1000000 45d6a03c Feb 17 06:27:08 2007 C:\WINDOWS\system32\svchost.exe
        7c800000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\ntdll.dll
        77e40000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\kernel32.dll
        77f50000 45d70a26 Feb 17 13:59:02 2007 C:\WINDOWS\system32\ADVAPI32.dll
        77c50000 45d70aaa Feb 17 14:01:14 2007 C:\WINDOWS\system32\RPCRT4.dll
        76f50000 45d70ac3 Feb 17 14:01:39 2007 C:\WINDOWS\system32\Secur32.dll
        7fd80000 45d70ad8 Feb 17 14:02:00 2007 c:\windows\system32\rpcss.dll
        77ba0000 45d70b06 Feb 17 14:02:46 2007 C:\WINDOWS\system32\msvcrt.dll
        71c00000 45d70ae9 Feb 17 14:02:17 2007 c:\windows\system32\WS2_32.dll
        71bf0000 45d70aea Feb 17 14:02:18 2007 c:\windows\system32\WS2HELP.dll
        77380000 45d70ac7 Feb 17 14:01:43 2007 C:\WINDOWS\system32\USER32.dll
        77c00000 45d70a3e Feb 17 13:59:26 2007 C:\WINDOWS\system32\GDI32.dll
          680000 45d69418 Feb 17 05:35:20 2007 C:\WINDOWS\system32\xpsp2res.dll
        68000000 45d69786 Feb 17 05:49:58 2007 C:\WINDOWS\system32\rsaenh.dll
        76b70000 45d70ab5 Feb 17 14:01:25 2007 C:\WINDOWS\system32\PSAPI.DLL
        777b0000 45d70a3b Feb 17 13:59:23 2007 C:\WINDOWS\system32\CLBCatQ.DLL
        77d00000 45d70aa6 Feb 17 14:01:10 2007 C:\WINDOWS\system32\OLEAUT32.dll
        77670000 45d70aa5 Feb 17 14:01:09 2007 C:\WINDOWS\system32\ole32.dll
        77010000 45d70a76 Feb 17 14:00:22 2007 C:\WINDOWS\system32\COMRes.dll
        77b90000 45d70ac8 Feb 17 14:01:44 2007 C:\WINDOWS\system32\VERSION.dll
    SubSystemData:     00000000
    ProcessHeap:       00080000
    ProcessParameters: 00020000
    WindowTitle:  'C:\WINDOWS\system32\svchost.exe'
    ImageFile:    'C:\WINDOWS\system32\svchost.exe'
    CommandLine:  'C:\WINDOWS\system32\svchost.exe -k DcomLaunch'
    DllPath:
'C:\WINDOWS\system32;C:\WINDOWS\system32;C:\WINDOWS\system;C:\WINDOWS;.;C:\WINDOWS\system32;C:\WIND
OWS;C:\WINDOWS\System32\Wbem'
    Environment:  00010000
```

```
        ALLUSERSPROFILE=C:\Documents and Settings\All Users
        ClusterLog=C:\WINDOWS\Cluster\cluster.log
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\WINDOWS\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        NUMBER_OF_PROCESSORS=1
        OS=Windows_NT
        Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 15 Model 5 Stepping 10, AuthenticAMD
        PROCESSOR_LEVEL=15
        PROCESSOR_REVISION=050a
        ProgramFiles=C:\Program Files
        SystemDrive=C:
        SystemRoot=C:\WINDOWS
        TEMP=C:\WINDOWS\TEMP
        TMP=C:\WINDOWS\TEMP
        USERPROFILE=C:\Documents and Settings\Default User
        windir=C:\WINDOWS


        THREAD 86331240  Cid 0280.0284  Teb: 7ffdf000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            862e60f4  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            8633a298       Image:         svchost.exe
        Wait Start TickCount      3899           Ticks: 112069 (0:00:29:11.078)
        Context Switch Count      13
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address svchost!wmainCRTStartup (0x010020b9)
        Start Address kernel32!BaseProcessStartThunk (0x77e617f8)
        Stack Init f6a53000 Current f6a52c04 Base f6a53000 Limit f6a50000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6a52c1c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6a52c34 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6a52c78 808ed456 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6a52ca0 808ea5ad nt!IopSynchronousServiceTail+0x180 (FPO: [Non-Fpo])
        f6a52d38 80883908 nt!NtReadFile+0x5d5 (FPO: [Non-Fpo])
        f6a52d38 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6a52d64)
        0006fc40 7c82776b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0006fc44 77e418b2 ntdll!NtReadFile+0xc (FPO: [9,0,0])
        0006fcac 77f65edb kernel32!ReadFile+0x16c (FPO: [Non-Fpo])
        0006fcd8 77f65f82 ADVAPI32!ScGetPipeInput+0x2a (FPO: [Non-Fpo])
        0006fd4c 77f51ed9 ADVAPI32!ScDispatcherLoop+0x51 (FPO: [Non-Fpo])
        0006ffb0 0100213d ADVAPI32!StartServiceCtrlDispatcherW+0xe3 (FPO: [Non-Fpo])
        0006ffc0 77e6f23b svchost!_wmainCRTStartup+0x7f (FPO: [0,0,2])
        0006fff0 00000000 kernel32!BaseProcessStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 8642f8d8  Cid 0280.02b0  Teb: 7ffdc000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            8642f950  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            8633a298       Image:         svchost.exe
        Wait Start TickCount      3938           Ticks: 112030 (0:00:29:10.468)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!RtlpTimerThread (0x7c83d3dd)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6e39000 Current f6e38c98 Base f6e39000 Limit f6e36000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6e38cb0 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6e38cc8 80827e1e nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6e38d0c 8098c418 nt!KeDelayExecutionThread+0x254 (FPO: [Non-Fpo])
        f6e38d54 80883908 nt!NtDelayExecution+0x84 (FPO: [Non-Fpo])
        f6e38d54 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6e38d64)
        0098ff9c 7c826f4b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0098ffa0 7c83d424 ntdll!NtDelayExecution+0xc (FPO: [2,0,0])
        0098ffb8 77e64829 ntdll!RtlpTimerThread+0x47 (FPO: [Non-Fpo])
        0098ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 86454a70  Cid 0280.02b4  Teb: 7ffdb000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            86378b90  QueueObject
            86454ae8  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            8633a298       Image:         svchost.exe
        Wait Start TickCount      114036         Ticks: 1932 (0:00:00:30.187)
        Context Switch Count      45
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!RtlpWorkerThread (0x7c839efb)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6a33000 Current f6a32c4c Base f6a33000 Limit f6a30000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f6a32c64 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6a32c7c 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6a32cc4 808e55e2 nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f6a32d48 80883908 nt!NtRemoveIoCompletion+0xdc (FPO: [Non-Fpo])
        f6a32d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6a32d64)
        009cff70 7c8277db ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        009cff74 7c839f38 ntdll!ZwRemoveIoCompletion+0xc (FPO: [5,0,0])
        009cffb8 77e64829 ntdll!RtlpWorkerThread+0x3d (FPO: [Non-Fpo])
        009cffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 8642c750  Cid 0280.02b8  Teb: 7ffda000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            86309b40  NotificationTimer
            862e3238  SynchronizationEvent
            8639c680  SynchronizationEvent
            8639c748  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            8633a298       Image:         svchost.exe
        Wait Start TickCount      3937           Ticks: 112031 (0:00:29:10.484)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!RtlpWaitThread (0x7c83c643)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6a2f000 Current f6a2e914 Base f6a2f000 Limit f6a2c000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6a2e92c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6a2e944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6a2e978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6a2ebf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6a2ed48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6a2ed48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6a2ed64)
        00a0fcec 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00a0fcf0 7c83c78e ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00a0ffb8 77e64829 ntdll!RtlpWaitThread+0x161 (FPO: [Non-Fpo])
        00a0ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 86421b88  Cid 0280.02bc  Teb: 7ffd8000 Win32Thread: e198c9f8 WAIT: (Unknown)
UserMode Non-Alertable
            8646b1c8  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            8633a298       Image:         svchost.exe
        Wait Start TickCount      45338          Ticks: 70630 (0:00:18:23.593)
        Context Switch Count      104                 LargeStack
        UserTime                  00:00:00.031
        KernelTime                00:00:00.031
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6aa3000 Current f6aa2c24 Base f6aa3000 Limit f6aa0000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6aa2c3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6aa2c54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6aa2c98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6aa2d48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f6aa2d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6aa2d64)
        00a5fe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00a5fe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        00a5ff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        00a5ff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        00a5ffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        00a5ffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        00a5ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

Svchost process (rpcss)

```
PROCESS 862c1c08  SessionId: 0  Cid: 02d4    Peb: 7ffd4000  ParentCid: 0198
    DirBase: 3af1a0e0  ObjectTable: e16bb5e8  HandleCount: 229.
    Image: svchost.exe
    VadRoot 86421428 Vads 69 Clone 0 Private 203. Modified 0. Locked 1.
    DeviceMap e16b5d18
    Token                             e1903030
    ElapsedTime                       00:39:04.734
    UserTime                          00:00:00.281
    KernelTime                        00:00:01.343
    QuotaPoolUsage[PagedPool]         40772
    QuotaPoolUsage[NonPagedPool]      20856
    Working Set Sizes (now,min,max)  (1900, 50, 345) (7600KB, 200KB, 1380KB)
    PeakWorkingSetSize                1900
    VirtualSize                       20 Mb
    PeakVirtualSize                   20 Mb
    PageFaultCount                    1979
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      274

    Setting context for this process...
.process /p /r ffffffff862c1c08

    !peb
PEB at 7ffd4000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         01000000
    Ldr                       7c8877e0
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00081f18 . 0009f0e8
    Ldr.InLoadOrderModuleList:           00081eb0 . 0009f368
    Ldr.InMemoryOrderModuleList:         00081eb8 . 0009f370
            Base TimeStamp                     Module
         1000000 45d6a03c Feb 17 06:27:08 2007 C:\WINDOWS\system32\svchost.exe
        7c800000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\ntdll.dll
        77e40000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\kernel32.dll
        77f50000 45d70a26 Feb 17 13:59:02 2007 C:\WINDOWS\system32\ADVAPI32.dll
        77c50000 45d70aaa Feb 17 14:01:14 2007 C:\WINDOWS\system32\RPCRT4.dll
        76f50000 45d70ac3 Feb 17 14:01:39 2007 C:\WINDOWS\system32\Secur32.dll
        7fd80000 45d70ad8 Feb 17 14:02:00 2007 c:\windows\system32\rpcss.dll
        77ba0000 45d70b06 Feb 17 14:02:46 2007 C:\WINDOWS\system32\msvcrt.dll
        71c00000 45d70ae9 Feb 17 14:02:17 2007 c:\windows\system32\WS2_32.dll
        71bf0000 45d70aea Feb 17 14:02:18 2007 c:\windows\system32\WS2HELP.dll
        77380000 45d70ac7 Feb 17 14:01:43 2007 C:\WINDOWS\system32\USER32.dll
        77c00000 45d70a3e Feb 17 13:59:26 2007 C:\WINDOWS\system32\GDI32.dll
          680000 45d69418 Feb 17 05:35:20 2007 C:\WINDOWS\system32\xpsp2res.dll
        68000000 45d69786 Feb 17 05:49:58 2007 C:\WINDOWS\system32\rsaenh.dll
        76b70000 45d70ab5 Feb 17 14:01:25 2007 C:\WINDOWS\system32\PSAPI.DLL
        71b20000 45d70b0d Feb 17 14:02:53 2007 C:\WINDOWS\system32\mswsock.dll
        5f270000 45d70a4a Feb 17 13:59:38 2007 C:\WINDOWS\system32\hnetcfg.dll
        71ae0000 45d70af3 Feb 17 14:02:27 2007 C:\WINDOWS\System32\wshtcpip.dll
        777b0000 45d70a3b Feb 17 13:59:23 2007 C:\WINDOWS\system32\CLBCatQ.DLL
        77d00000 45d70aa6 Feb 17 14:01:10 2007 C:\WINDOWS\system32\OLEAUT32.dll
        77670000 45d70aa5 Feb 17 14:01:09 2007 C:\WINDOWS\system32\ole32.dll
        77010000 45d70a76 Feb 17 14:00:22 2007 C:\WINDOWS\system32\COMRes.dll
        77b90000 45d70ac8 Feb 17 14:01:44 2007 C:\WINDOWS\system32\VERSION.dll
    SubSystemData:     00000000
    ProcessHeap:       00080000
    ProcessParameters: 00020000
    WindowTitle:  'C:\WINDOWS\system32\svchost.exe'
    ImageFile:    'C:\WINDOWS\system32\svchost.exe'
    CommandLine:  'C:\WINDOWS\system32\svchost.exe -k rpcss'
```

```
    DllPath:
'C:\WINDOWS\system32;C:\WINDOWS\system32;C:\WINDOWS\system;C:\WINDOWS;.;C:\WINDOWS\system32;C:\WIND
OWS;C:\WINDOWS\System32\Wbem'
    Environment:  00010000
        ALLUSERSPROFILE=C:\Documents and Settings\All Users
        ClusterLog=C:\WINDOWS\Cluster\cluster.log
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\WINDOWS\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        NUMBER_OF_PROCESSORS=1
        OS=Windows_NT
        Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 15 Model 5 Stepping 10, AuthenticAMD
        PROCESSOR_LEVEL=15
        PROCESSOR_REVISION=050a
        ProgramFiles=C:\Program Files
        SystemDrive=C:
        SystemRoot=C:\WINDOWS
        TEMP=C:\DOCUME~1\NETWOR~1\LOCALS~1\Temp
        TMP=C:\DOCUME~1\NETWOR~1\LOCALS~1\Temp
        USERDOMAIN=NT AUTHORITY
        USERNAME=NETWORK SERVICE
        USERPROFILE=C:\Documents and Settings\NetworkService
        windir=C:\WINDOWS


        THREAD 862e9db0  Cid 02d4.02d8  Teb: 7ffdf000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            863ade04  NotificationEvent
        Not impersonating
        DeviceMap                 e16b5d18
        Owning Process            862c1c08       Image:         svchost.exe
        Wait Start TickCount      3999           Ticks: 111969 (0:00:29:09.515)
        Context Switch Count      14
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address svchost!wmainCRTStartup (0x010020b9)
        Start Address kernel32!BaseProcessStartThunk (0x77e617f8)
        Stack Init f6fd5000 Current f6fd4c04 Base f6fd5000 Limit f6fd2000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6fd4c1c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6fd4c34 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6fd4c78 808ed456 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6fd4ca0 808ea5ad nt!IopSynchronousServiceTail+0x180 (FPO: [Non-Fpo])
        f6fd4d38 80883908 nt!NtReadFile+0x5d5 (FPO: [Non-Fpo])
        f6fd4d38 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6fd4d64)
        0006fc40 7c82776b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0006fc44 77e418b2 ntdll!NtReadFile+0xc (FPO: [9,0,0])
        0006fcac 77f65edb kernel32!ReadFile+0x16c (FPO: [Non-Fpo])
        0006fcd8 77f65f82 ADVAPI32!ScGetPipeInput+0x2a (FPO: [Non-Fpo])
        0006fd4c 77f51ed9 ADVAPI32!ScDispatcherLoop+0x51 (FPO: [Non-Fpo])
        0006ffb0 0100213d ADVAPI32!StartServiceCtrlDispatcherW+0xe3 (FPO: [Non-Fpo])
        0006ffc0 77e6f23b svchost!_wmainCRTStartup+0x7f (FPO: [0,0,2])
        0006fff0 00000000 kernel32!BaseProcessStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 8645adb0  Cid 02d4.02dc  Teb: 7ffde000 Win32Thread: e17d5678 WAIT: (Unknown)
UserMode Non-Alertable
            8645ae28  NotificationTimer
        IRP List:
            8641cbd8: (0006,0094) Flags: 00000800  Mdl: 00000000
        Not impersonating
        DeviceMap                 e16b5d18
        Owning Process            862c1c08       Image:         svchost.exe
        Wait Start TickCount      108687         Ticks: 7281 (0:00:01:53.765)
        Context Switch Count      126                 LargeStack
        UserTime                  00:00:00.078
        KernelTime                00:00:00.109
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x77f65e70)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6d98000 Current f6d97c98 Base f6d98000 Limit f6d95000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6d97cb0 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6d97cc8 80827e1e nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6d97d0c 8098c418 nt!KeDelayExecutionThread+0x254 (FPO: [Non-Fpo])
        f6d97d54 80883908 nt!NtDelayExecution+0x84 (FPO: [Non-Fpo])
        f6d97d54 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6d97d64)
        0029fdb4 7c826f4b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0029fdb8 77e41ed1 ntdll!NtDelayExecution+0xc (FPO: [2,0,0])
        0029fe20 7fd85a63 kernel32!SleepEx+0x68 (FPO: [Non-Fpo])
        0029fe2c 7fd8698c rpcss!CTime::Sleep+0x2a (FPO: [0,0,0])
        0029fe78 7fd9e3c1 rpcss!ObjectExporterWorkerThread+0x305 (FPO: [Non-Fpo])
        0029ff44 7fd9bb80 rpcss!ScmServiceMain+0x240 (FPO: [Non-Fpo])
        0029ff70 010012a4 rpcss!ServiceMain+0xd0 (FPO: [Non-Fpo])
        0029ffa4 77f65e91 svchost!ServiceStarter+0x9e (FPO: [Non-Fpo])
        0029ffb8 77e64829 ADVAPI32!ScSvcctrlThreadW+0x21 (FPO: [Non-Fpo])
        0029ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 862db8e0  Cid 02d4.02e4  Teb: 7ffdc000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            862db958  NotificationTimer
        Not impersonating
        DeviceMap                 e16b5d18
        Owning Process            862c1c08       Image:         svchost.exe
        Wait Start TickCount      42612          Ticks: 73356 (0:00:19:06.187)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!RtlpTimerThread (0x7c83d3dd)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f78b3000 Current f78b2c98 Base f78b3000 Limit f78b0000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f78b2cb0 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f78b2cc8 80827e1e nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f78b2d0c 8098c418 nt!KeDelayExecutionThread+0x254 (FPO: [Non-Fpo])
        f78b2d54 80883908 nt!NtDelayExecution+0x84 (FPO: [Non-Fpo])
        f78b2d54 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f78b2d64)
        0098ff9c 7c826f4b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0098ffa0 7c83d424 ntdll!NtDelayExecution+0xc (FPO: [2,0,0])
        0098ffb8 77e64829 ntdll!RtlpTimerThread+0x47 (FPO: [Non-Fpo])
        0098ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 8631b4f0  Cid 02d4.02e8  Teb: 7ffdb000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            862ffc90  QueueObject
            8631b568  NotificationTimer
        IRP List:
            8638a008: (0006,0190) Flags: 00000030  Mdl: 00000000
        Not impersonating
        DeviceMap                 e16b5d18
        Owning Process            862c1c08       Image:         svchost.exe
        Wait Start TickCount      114294         Ticks: 1674 (0:00:00:26.156)
        Context Switch Count      48
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address ntdll!RtlpWorkerThread (0x7c839efb)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6a17000 Current f6a16c4c Base f6a17000 Limit f6a14000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f6a16c64 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6a16c7c 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6a16cc4 808e55e2 nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f6a16d48 80883908 nt!NtRemoveIoCompletion+0xdc (FPO: [Non-Fpo])
        f6a16d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6a16d64)
        009cff70 7c8277db ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        009cff74 7c839f38 ntdll!ZwRemoveIoCompletion+0xc (FPO: [5,0,0])
        009cffb8 77e64829 ntdll!RtlpWorkerThread+0x3d (FPO: [Non-Fpo])
        009cffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 8631aa58  Cid 02d4.02ec  Teb: 7ffda000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            862db828  NotificationTimer
            86322440  SynchronizationEvent
            86323328  SynchronizationEvent
            863372e8  SynchronizationEvent
            86419a90  SynchronizationEvent
        Not impersonating
        DeviceMap                 e16b5d18
        Owning Process            862c1c08       Image:         svchost.exe
        Wait Start TickCount      4210           Ticks: 111758 (0:00:29:06.218)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!RtlpWaitThread (0x7c83c643)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6a13000 Current f6a12914 Base f6a13000 Limit f6a10000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6a1292c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6a12944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6a12978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6a12bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6a12d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6a12d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6a12d64)
        00a0fcec 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00a0fcf0 7c83c78e ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00a0ffb8 77e64829 ntdll!RtlpWaitThread+0x161 (FPO: [Non-Fpo])
        00a0ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 8641e820  Cid 02d4.02f8  Teb: 7ffd8000 Win32Thread: e1979510 WAIT: (Unknown)
UserMode Non-Alertable
            863b02a0  Semaphore Limit 0x7fffffff
            8641e898  NotificationTimer
        Not impersonating
        DeviceMap                 e16b5d18
        Owning Process            862c1c08       Image:         svchost.exe
        Wait Start TickCount      114447         Ticks: 1521 (0:00:00:23.765)
        Context Switch Count      387                 LargeStack
        UserTime                  00:00:00.062
        KernelTime                00:00:00.312
        Win32 Start Address 0x0000270a
        LPC Server thread working on message Id 270a
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6ab3000 Current f6ab2c24 Base f6ab3000 Limit f6ab0000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f6ab2c3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6ab2c54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6ab2c98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6ab2d48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f6ab2d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6ab2d64)
        00a9fe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00a9fe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        00a9ff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        00a9ff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        00a9ffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        00a9ffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        00a9ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 86374db0  Cid 02d4.02fc  Teb: 7ffd7000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            8638c820  QueueObject
            86374e28  NotificationTimer
        IRP List:
            862b94c0: (0006,0190) Flags: 00000030  Mdl: 00000000
            862d6578: (0006,0094) Flags: 00000800  Mdl: 00000000
        Not impersonating
        DeviceMap                 e16b5d18
        Owning Process            862c1c08       Image:         svchost.exe
        Wait Start TickCount      114460         Ticks: 1508 (0:00:00:23.562)
        Context Switch Count      32
        UserTime                  00:00:00.015
        KernelTime                00:00:00.046
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x77c7b0f5)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6a03000 Current f6a02c4c Base f6a03000 Limit f6a00000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f6a02c64 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6a02c7c 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6a02cc4 808e55e2 nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f6a02d48 80883908 nt!NtRemoveIoCompletion+0xdc (FPO: [Non-Fpo])
        f6a02d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6a02d64)
        00adfeac 7c8277db ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00adfeb0 77e5bea2 ntdll!ZwRemoveIoCompletion+0xc (FPO: [5,0,0])
        00adfedc 77c7b900 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        00adff18 77c7b703 RPCRT4!COMMON_ProcessCalls+0xa1 (FPO: [Non-Fpo])
        00adff84 77c7b9b5 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x117 (FPO: [Non-Fpo])
        00adff8c 77c8872d RPCRT4!ProcessIOEventsWrapper+0xd (FPO: [Non-Fpo])
        00adffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        00adffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        00adffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 8635cdb0  Cid 02d4.04a8  Teb: 7ffd5000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            863b02a0  Semaphore Limit 0x7fffffff
            8635ce28  NotificationTimer
        Not impersonating
        DeviceMap                 e16b5d18
        Owning Process            862c1c08       Image:         svchost.exe
        Wait Start TickCount      114460         Ticks: 1508 (0:00:00:23.562)
        Context Switch Count      361
        UserTime                  00:00:00.062
        KernelTime                00:00:00.437
        Win32 Start Address 0x0000270d
        LPC Server thread working on message Id 270d
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f671a000 Current f6719c24 Base f671a000 Limit f6717000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f6719c3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6719c54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6719c98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6719d48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f6719d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6719d64)
        00b7fe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00b7fe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        00b7ff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        00b7ff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        00b7ffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        00b7ffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        00b7ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 864a9db0  Cid 02d4.0714  Teb: 7ffd6000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            863b02a0  Semaphore Limit 0x7fffffff
            864a9e28  NotificationTimer
        Not impersonating
        DeviceMap                 e16b5d18
        Owning Process            862c1c08       Image:         svchost.exe
        Wait Start TickCount      105199         Ticks: 10769 (0:00:02:48.265)
        Context Switch Count      149
        UserTime                  00:00:00.015
        KernelTime                00:00:00.093
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6419000 Current f6418c24 Base f6419000 Limit f6416000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6418c3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6418c54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6418c98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6418d48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f6418d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6418d64)
        00b3fe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00b3fe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        00b3ff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        00b3ff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        00b3ffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        00b3ffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        00b3ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d49690  Cid 02d4.05a4  Teb: 7ffd9000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            8638c820  QueueObject
            85d49708  NotificationTimer
        IRP List:
            860c9798: (0006,01b4) Flags: 00000000  Mdl: 8638cdf0
        Not impersonating
        DeviceMap                 e16b5d18
        Owning Process            862c1c08       Image:         svchost.exe
        Wait Start TickCount      114460         Ticks: 1508 (0:00:00:23.562)
        Context Switch Count      21
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x77c7b0f5)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6415000 Current f6414c4c Base f6415000 Limit f6412000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f6414c64 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6414c7c 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6414cc4 808e55e2 nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f6414d48 80883908 nt!NtRemoveIoCompletion+0xdc (FPO: [Non-Fpo])
        f6414d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6414d64)
        00a5feac 7c8277db ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00a5feb0 77e5bea2 ntdll!ZwRemoveIoCompletion+0xc (FPO: [5,0,0])
        00a5fedc 77c7b900 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        00a5ff18 77c7b703 RPCRT4!COMMON_ProcessCalls+0xa1 (FPO: [Non-Fpo])
        00a5ff84 77c7b9b5 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x117 (FPO: [Non-Fpo])
        00a5ff8c 77c8872d RPCRT4!ProcessIOEventsWrapper+0xd (FPO: [Non-Fpo])
        00a5ffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        00a5ffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        00a5ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 863fda48  Cid 02d4.089c  Teb: 7ffdd000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            863fdac0  NotificationTimer
        Not impersonating
        DeviceMap                 e16b5d18
        Owning Process            862c1c08       Image:         svchost.exe
        Wait Start TickCount      108687         Ticks: 7281 (0:00:01:53.765)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address rpcss!ObjectExporterTaskThread (0x7fda30df)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6241000 Current f6240c98 Base f6241000 Limit f623e000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6240cb0 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6240cc8 80827e1e nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6240d0c 8098c418 nt!KeDelayExecutionThread+0x254 (FPO: [Non-Fpo])
        f6240d54 80883908 nt!NtDelayExecution+0x84 (FPO: [Non-Fpo])
        f6240d54 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6240d64)
        00bbff24 7c826f4b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00bbff28 77e41ed1 ntdll!NtDelayExecution+0xc (FPO: [2,0,0])
        00bbff90 7fd85a63 kernel32!SleepEx+0x68 (FPO: [Non-Fpo])
        00bbff9c 7fd9fd83 rpcss!CTime::Sleep+0x2a (FPO: [0,0,0])
        00bbffb8 77e64829 rpcss!ObjectExporterTaskThread+0xe5 (FPO: [Non-Fpo])
        00bbffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

Svchost process (NetworkService)

```
PROCESS 862d6b30  SessionId: 0  Cid: 0314    Peb: 7ffd8000  ParentCid: 0198
    DirBase: 3af1a100  ObjectTable: e1840008  HandleCount: 140.
    Image: svchost.exe
    VadRoot 863904e0 Vads 109 Clone 0 Private 771. Modified 0. Locked 0.
    DeviceMap e16b5d18
    Token                             e1914240
    ElapsedTime                       00:39:04.296
    UserTime                          00:00:00.046
    KernelTime                        00:00:00.656
    QuotaPoolUsage[PagedPool]         65316
    QuotaPoolUsage[NonPagedPool]      5992
    Working Set Sizes (now,min,max)  (1925, 50, 345) (7700KB, 200KB, 1380KB)
    PeakWorkingSetSize                1942
    VirtualSize                       37 Mb
    PeakVirtualSize                   39 Mb
    PageFaultCount                    2171
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      890

    Setting context for this process...
.process /p /r ffffffff862d6b30

    !peb
PEB at 7ffd8000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         01000000
    Ldr                       7c8877e0
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00081f18 . 00096bf8
    Ldr.InLoadOrderModuleList:           00081eb0 . 00096be8
    Ldr.InMemoryOrderModuleList:         00081eb8 . 00096bf0
            Base TimeStamp                     Module
         1000000 45d6a03c Feb 17 06:27:08 2007 C:\WINDOWS\system32\svchost.exe
        7c800000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\ntdll.dll
        77e40000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\kernel32.dll
        77f50000 45d70a26 Feb 17 13:59:02 2007 C:\WINDOWS\system32\ADVAPI32.dll
        77c50000 45d70aaa Feb 17 14:01:14 2007 C:\WINDOWS\system32\RPCRT4.dll
        76f50000 45d70ac3 Feb 17 14:01:39 2007 C:\WINDOWS\system32\Secur32.dll
        76d10000 45d70a45 Feb 17 13:59:33 2007 c:\windows\system32\dhcpcsvc.dll
        77ba0000 45d70b06 Feb 17 14:02:46 2007 C:\WINDOWS\system32\msvcrt.dll
        76ed0000 45d70a64 Feb 17 14:00:04 2007 c:\windows\system32\DNSAPI.dll
        71c00000 45d70ae9 Feb 17 14:02:17 2007 c:\windows\system32\WS2_32.dll
        71bf0000 45d70aea Feb 17 14:02:18 2007 c:\windows\system32\WS2HELP.dll
        76cf0000 45d70a6c Feb 17 14:00:12 2007 c:\windows\system32\iphlpapi.dll
        76b70000 45d70ab5 Feb 17 14:01:25 2007 c:\windows\system32\PSAPI.DLL
        77380000 45d70ac7 Feb 17 14:01:43 2007 C:\WINDOWS\system32\USER32.dll
        77c00000 45d70a3e Feb 17 13:59:26 2007 C:\WINDOWS\system32\GDI32.dll
        766c0000 45d70a68 Feb 17 14:00:08 2007 c:\windows\system32\dnsrslvr.dll
        71b20000 45d70b0d Feb 17 14:02:53 2007 C:\WINDOWS\system32\mswsock.dll
        5f270000 45d70a4a Feb 17 13:59:38 2007 C:\WINDOWS\system32\hnetcfg.dll
        71ae0000 45d70af3 Feb 17 14:02:27 2007 C:\WINDOWS\System32\wshtcpip.dll
        77840000 45d70a86 Feb 17 14:00:38 2007 C:\WINDOWS\system32\netman.dll
        76300000 45d70a8a Feb 17 14:00:42 2007 C:\WINDOWS\system32\netshell.dll
        76e30000 45d70abb Feb 17 14:01:31 2007 C:\WINDOWS\system32\rtutils.dll
        76b80000 45d70a7f Feb 17 14:00:31 2007 C:\WINDOWS\system32\credui.dll
        7c8d0000 45d70abb Feb 17 14:01:31 2007 C:\WINDOWS\system32\SHELL32.dll
        77da0000 45d70ac0 Feb 17 14:01:36 2007 C:\WINDOWS\system32\SHLWAPI.dll
        77670000 45d70aa5 Feb 17 14:01:09 2007 C:\WINDOWS\system32\ole32.dll
        77d00000 45d70aa6 Feb 17 14:01:10 2007 C:\WINDOWS\system32\OLEAUT32.dll
        76a80000 3e80249c Mar 25 09:42:52 2003 C:\WINDOWS\system32\ATL.DLL
        74de0000 45d70a43 Feb 17 13:59:31 2007 C:\WINDOWS\system32\CLUSAPI.dll
        76cd0000 45d70a85 Feb 17 14:00:37 2007 C:\WINDOWS\system32\MPRAPI.dll
```

```
        76df0000 45d70a11 Feb 17 13:58:41 2007 C:\WINDOWS\system32\ACTIVEDS.dll
        76dc0000 45d70a22 Feb 17 13:58:58 2007 C:\WINDOWS\system32\adsldpc.dll
        71c40000 45d70a82 Feb 17 14:00:34 2007 C:\WINDOWS\system32\NETAPI32.dll
        76f10000 45d70ad5 Feb 17 14:01:57 2007 C:\WINDOWS\system32\WLDAP32.dll
        7e020000 45d70aa8 Feb 17 14:01:12 2007 C:\WINDOWS\system32\SAMLIB.dll
        770e0000 45d70ab3 Feb 17 14:01:23 2007 C:\WINDOWS\system32\SETUPAPI.dll
        76e90000 45d70a9e Feb 17 14:01:02 2007 C:\WINDOWS\system32\RASAPI32.dll
        76e40000 45d70aa3 Feb 17 14:01:07 2007 C:\WINDOWS\system32\rasman.dll
        76e60000 45d70abc Feb 17 14:01:32 2007 C:\WINDOWS\system32\TAPI32.dll
        76aa0000 45d70af0 Feb 17 14:02:24 2007 C:\WINDOWS\system32\WINMM.dll
        761b0000 45d70a80 Feb 17 14:00:32 2007 C:\WINDOWS\system32\CRYPT32.dll
        76190000 45d70aac Feb 17 14:01:16 2007 C:\WINDOWS\system32\MSASN1.dll
        7fcf0000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\WZCSvc.DLL
        76cc0000 3e80249b Mar 25 09:42:51 2003 C:\WINDOWS\system32\WMI.dll
        76f00000 45d70af7 Feb 17 14:02:31 2007 C:\WINDOWS\system32\WTSAPI32.dll
        771f0000 45d70ace Feb 17 14:01:50 2007 C:\WINDOWS\system32\WINSTA.dll
        4b180000 45d70a3c Feb 17 13:59:24 2007 C:\WINDOWS\system32\ESENT.dll
        77210000 45d70aee Feb 17 14:02:22 2007 C:\WINDOWS\system32\WININET.dll
        730a0000 45d70af9 Feb 17 14:02:33 2007 C:\WINDOWS\system32\WZCSAPI.DLL
        77420000 45d70a05 Feb 17 13:58:29 2007 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.3790.3959_x-ww_D8713E55\comctl32.dll
    SubSystemData:     00000000
    ProcessHeap:       00080000
    ProcessParameters: 00020000
    WindowTitle:  'C:\WINDOWS\system32\svchost.exe'
    ImageFile:    'C:\WINDOWS\system32\svchost.exe'
    CommandLine:  'C:\WINDOWS\system32\svchost.exe -k NetworkService'
    DllPath:
'C:\WINDOWS\system32;C:\WINDOWS\system32;C:\WINDOWS\system;C:\WINDOWS;.;C:\WINDOWS\system32;C:\WIND
OWS;C:\WINDOWS\System32\Wbem'
    Environment:  00010000
        ALLUSERSPROFILE=C:\Documents and Settings\All Users
        ClusterLog=C:\WINDOWS\Cluster\cluster.log
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\WINDOWS\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        NUMBER_OF_PROCESSORS=1
        OS=Windows_NT
        Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 15 Model 5 Stepping 10, AuthenticAMD
        PROCESSOR_LEVEL=15
        PROCESSOR_REVISION=050a
        ProgramFiles=C:\Program Files
        SystemDrive=C:
        SystemRoot=C:\WINDOWS
        TEMP=C:\DOCUME~1\NETWOR~1\LOCALS~1\Temp
        TMP=C:\DOCUME~1\NETWOR~1\LOCALS~1\Temp
        USERDOMAIN=NT AUTHORITY
        USERNAME=NETWORK SERVICE
        USERPROFILE=C:\Documents and Settings\NetworkService
        windir=C:\WINDOWS
```

```
        THREAD 865a0020  Cid 0314.0318  Teb: 7ffdf000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            86380b3c  NotificationEvent
        Not impersonating
        DeviceMap                 e16b5d18
        Owning Process            862d6b30       Image:         svchost.exe
        Wait Start TickCount      4030           Ticks: 111938 (0:00:29:09.031)
        Context Switch Count      19
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address svchost!wmainCRTStartup (0x010020b9)
        Start Address kernel32!BaseProcessStartThunk (0x77e617f8)
        Stack Init f69f7000 Current f69f6c04 Base f69f7000 Limit f69f4000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f69f6c1c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f69f6c34 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f69f6c78 808ed456 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f69f6ca0 808ea5ad nt!IopSynchronousServiceTail+0x180 (FPO: [Non-Fpo])
        f69f6d38 80883908 nt!NtReadFile+0x5d5 (FPO: [Non-Fpo])
        f69f6d38 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f69f6d64)
        0006fc40 7c82776b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0006fc44 77e418b2 ntdll!NtReadFile+0xc (FPO: [9,0,0])
        0006fcac 77f65edb kernel32!ReadFile+0x16c (FPO: [Non-Fpo])
        0006fcd8 77f65f82 ADVAPI32!ScGetPipeInput+0x2a (FPO: [Non-Fpo])
        0006fd4c 77f51ed9 ADVAPI32!ScDispatcherLoop+0x51 (FPO: [Non-Fpo])
        0006ffb0 0100213d ADVAPI32!StartServiceCtrlDispatcherW+0xe3 (FPO: [Non-Fpo])
        0006ffc0 77e6f23b svchost!_wmainCRTStartup+0x7f (FPO: [0,0,2])
        0006fff0 00000000 kernel32!BaseProcessStart+0x23 (FPO: [Non-Fpo])

        THREAD 86390260  Cid 0314.0320  Teb: 7ffde000 Win32Thread: e1915530 WAIT: (Unknown)
UserMode Non-Alertable
            862f65f0  NotificationEvent
            862b4ae8  SynchronizationEvent
            862b4c08  NotificationEvent
            862f6580  SynchronizationEvent
            863902d8  NotificationTimer
        Not impersonating
        DeviceMap                 e16b5d18
        Owning Process            862d6b30       Image:         svchost.exe
        Wait Start TickCount      4210           Ticks: 111758 (0:00:29:06.218)
        Context Switch Count      36                 LargeStack
        UserTime                  00:00:00.015
        KernelTime                00:00:00.031
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x77f65e70)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6d78000 Current f6d77914 Base f6d78000 Limit f6d74000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6d7792c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6d77944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6d77978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6d77bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6d77d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6d77d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6d77d64)
        0029fe4c 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0029fe50 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0029fef8 77e62fbe kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        0029ff14 76d138e1 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0029ff5c 76d194c5 dhcpcsvc!ProcessDhcpRequestForever+0xcc (FPO: [Non-Fpo])
        0029ff70 010012a4 dhcpcsvc!ServiceMain+0x7e (FPO: [Non-Fpo])
        0029ffa4 77f65e91 svchost!ServiceStarter+0x9e (FPO: [Non-Fpo])
        0029ffb8 77e64829 ADVAPI32!ScSvcctrlThreadW+0x21 (FPO: [Non-Fpo])
        0029ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 862dcdb0  Cid 0314.0330  Teb: 7ffdc000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            862d6dd8  NotificationEvent
            862b4c9c  NotificationEvent
            862f67f0  SynchronizationEvent
        IRP List:
            863717d8: (0006,01b4) Flags: 00000000  Mdl: 00000000
        Not impersonating
        DeviceMap                 e16b5d18
        Owning Process            862d6b30       Image:         svchost.exe
        Wait Start TickCount      4047           Ticks: 111921 (0:00:29:08.765)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address dnsrslvr!NotifyThread (0x766c549e)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f68da000 Current f68d9914 Base f68da000 Limit f68d7000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f68d992c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f68d9944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f68d9978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f68d9bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f68d9d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f68d9d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f68d9d64)
        0060fec0 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0060fec4 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0060ff6c 77e62fbe kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        0060ff88 766c54ff kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0060ffb8 77e64829 dnsrslvr!NotifyThread+0x61 (FPO: [Non-Fpo])
        0060ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 86338db0  Cid 0314.0334  Teb: 7ffdb000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            862dcd80  NotificationEvent
        IRP List:
            85d8fcb8: (0006,0094) Flags: 00000000  Mdl: 00000000
        Not impersonating
        DeviceMap                 e16b5d18
        Owning Process            862d6b30       Image:         svchost.exe
        Wait Start TickCount      5967           Ticks: 110001 (0:00:28:38.765)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address dnsrslvr!IpNotifyThread (0x766c480c)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f68d6000 Current f68d5c78 Base f68d6000 Limit f68d3000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f68d5c90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f68d5ca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f68d5cec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f68d5d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f68d5d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f68d5d64)
        0064fee4 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0064fee8 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0064ff58 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        0064ff6c 77e43a2c kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0064ff80 766c48d2 kernel32!GetOverlappedResult+0x29 (FPO: [Non-Fpo])
        0064ffb8 77e64829 dnsrslvr!IpNotifyThread+0xe4 (FPO: [Non-Fpo])
        0064ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 86323b70  Cid 0314.0338  Teb: 7ffda000 Win32Thread: e1953298 WAIT: (Unknown)
UserMode Non-Alertable
            862dcc88  Semaphore Limit 0x7fffffff
            86323be8  NotificationTimer
        Not impersonating
        DeviceMap                 e16b5d18
        Owning Process            862d6b30       Image:         svchost.exe
        Wait Start TickCount      115363         Ticks: 605 (0:00:00:09.453)
        Context Switch Count      101                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.234
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f665d000 Current f665cc24 Base f665d000 Limit f665a000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f665cc3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f665cc54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f665cc98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f665cd48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f665cd48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f665cd64)
        0069fe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0069fe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        0069ff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        0069ff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        0069ffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        0069ffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        0069ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 862b4d10  Cid 0314.033c  Teb: 7ffdd000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            862f65f0  NotificationEvent
            86433850  SynchronizationEvent
        IRP List:
            863e2e28: (0006,0094) Flags: 00000070  Mdl: 00000000
        Not impersonating
        DeviceMap                 e16b5d18
        Owning Process            862d6b30       Image:         svchost.exe
        Wait Start TickCount      4049           Ticks: 111919 (0:00:29:08.734)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address dhcpcsvc!MediaSenseDetectionLoop (0x76d18f3b)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f68d2000 Current f68d1914 Base f68d2000 Limit f68cf000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f68d192c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f68d1944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f68d1978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f68d1bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f68d1d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f68d1d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f68d1d64)
        006dfeb8 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        006dfebc 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        006dff64 77e62fbe kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        006dff80 76d18fde kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        006dffb8 77e64829 dhcpcsvc!MediaSenseDetectionLoop+0xa7 (FPO: [Non-Fpo])
        006dffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 862f6880  Cid 0314.0340  Teb: 7ffd9000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            862f6b28  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 e16b5d18
        Owning Process            862d6b30       Image:         svchost.exe
        Wait Start TickCount      29012          Ticks: 86956 (0:00:22:38.687)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x77c7b0f5)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f68c6000 Current f68c5c24 Base f68c6000 Limit f68c3000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f68c5c3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f68c5c54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f68c5c98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f68c5d48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f68c5d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f68c5d64)
        0071fe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0071fe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        0071ff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        0071ff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        0071ffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        0071ffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        0071ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 863396b0  Cid 0314.04c8  Teb: 7ffd7000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            862dcc88  Semaphore Limit 0x7fffffff
            86339728  NotificationTimer
        Not impersonating
        DeviceMap                 e16b5d18
        Owning Process            862d6b30       Image:         svchost.exe
        Wait Start TickCount      115043         Ticks: 925 (0:00:00:14.453)
        Context Switch Count      75
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f66b1000 Current f66b0c24 Base f66b1000 Limit f66ae000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f66b0c3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f66b0c54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f66b0c98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f66b0d48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f66b0d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f66b0d64)
        0075fe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0075fe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        0075ff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        0075ff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        0075ffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        0075ffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        0075ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d8a6b0  Cid 0314.04d0  Teb: 7ffd5000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            862dcc88  Semaphore Limit 0x7fffffff
            85d8a728  NotificationTimer
        Not impersonating
        DeviceMap                 e16b5d18
        Owning Process            862d6b30       Image:         svchost.exe
        Wait Start TickCount      115203         Ticks: 765 (0:00:00:11.953)
        Context Switch Count      54
        UserTime                  00:00:00.015
        KernelTime                00:00:00.156
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6691000 Current f6690c24 Base f6691000 Limit f668e000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f6690c3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6690c54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6690c98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6690d48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f6690d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6690d64)
        00d4fe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00d4fe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        00d4ff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        00d4ff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        00d4ffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        00d4ffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        00d4ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

Svchost process (LocalService)

```
PROCESS 862fdbf0  SessionId: 0  Cid: 0328    Peb: 7ffde000  ParentCid: 0198
    DirBase: 3af1a120  ObjectTable: e17de9c8  HandleCount: 162.
    Image: svchost.exe
    VadRoot 865a02f8 Vads 83 Clone 0 Private 238. Modified 0. Locked 2.
    DeviceMap e159ad18
    Token                             e1978de8
    ElapsedTime                       00:39:04.155
    UserTime                          00:00:00.031
    KernelTime                        00:00:00.687
    QuotaPoolUsage[PagedPool]         38340
    QuotaPoolUsage[NonPagedPool]      4376
    Working Set Sizes (now,min,max)  (1911, 50, 345) (7644KB, 200KB, 1380KB)
    PeakWorkingSetSize                1915
    VirtualSize                       21 Mb
    PeakVirtualSize                   21 Mb
    PageFaultCount                    1927
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      309

    Setting context for this process...
.process /p /r ffffffff862fdbf0

    !peb
PEB at 7ffde000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         01000000
    Ldr                       7c8877e0
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00081f18 . 0009d618
    Ldr.InLoadOrderModuleList:           00081eb0 . 0009d608
    Ldr.InMemoryOrderModuleList:         00081eb8 . 0009d610
            Base TimeStamp                     Module
         1000000 45d6a03c Feb 17 06:27:08 2007 C:\WINDOWS\system32\svchost.exe
        7c800000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\ntdll.dll
        77e40000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\kernel32.dll
        77f50000 45d70a26 Feb 17 13:59:02 2007 C:\WINDOWS\system32\ADVAPI32.dll
        77c50000 45d70aaa Feb 17 14:01:14 2007 C:\WINDOWS\system32\RPCRT4.dll
        76f50000 45d70ac3 Feb 17 14:01:39 2007 C:\WINDOWS\system32\Secur32.dll
        77e00000 45d70aab Feb 17 14:01:15 2007 C:\WINDOWS\system32\NTMARTA.DLL
        77ba0000 45d70b06 Feb 17 14:02:46 2007 C:\WINDOWS\system32\msvcrt.dll
        77380000 45d70ac7 Feb 17 14:01:43 2007 C:\WINDOWS\system32\USER32.dll
        77c00000 45d70a3e Feb 17 13:59:26 2007 C:\WINDOWS\system32\GDI32.dll
        76f10000 45d70ad5 Feb 17 14:01:57 2007 C:\WINDOWS\system32\WLDAP32.dll
        7e020000 45d70aa8 Feb 17 14:01:12 2007 C:\WINDOWS\system32\SAMLIB.dll
        77670000 45d70aa5 Feb 17 14:01:09 2007 C:\WINDOWS\system32\ole32.dll
          650000 45d69418 Feb 17 05:35:20 2007 C:\WINDOWS\system32\xpsp2res.dll
        74a40000 45d70a55 Feb 17 13:59:49 2007 c:\windows\system32\lmhsvc.dll
        76cf0000 45d70a6c Feb 17 14:00:12 2007 c:\windows\system32\iphlpapi.dll
        76b70000 45d70ab5 Feb 17 14:01:25 2007 c:\windows\system32\PSAPI.DLL
        71c00000 45d70ae9 Feb 17 14:02:17 2007 c:\windows\system32\WS2_32.dll
        71bf0000 45d70aea Feb 17 14:02:18 2007 c:\windows\system32\WS2HELP.dll
        71b20000 45d70b0d Feb 17 14:02:53 2007 C:\WINDOWS\System32\mswsock.dll
        76ed0000 45d70a64 Feb 17 14:00:04 2007 C:\WINDOWS\system32\DNSAPI.dll
        76f80000 45d70a9d Feb 17 14:01:01 2007 C:\WINDOWS\system32\rasadhlp.dll
        76710000 45d70ac2 Feb 17 14:01:38 2007 c:\windows\system32\w32time.dll
          ab0000 45d6a071 Feb 17 06:28:01 2007 c:\windows\system32\msvcp60.dll
        71c40000 45d70a82 Feb 17 14:00:34 2007 C:\WINDOWS\system32\NETAPI32.dll
        76920000 45d70ac8 Feb 17 14:01:44 2007 c:\windows\system32\USERENV.dll
        5f270000 45d70a4a Feb 17 13:59:38 2007 C:\WINDOWS\system32\hnetcfg.dll
        71ae0000 45d70af3 Feb 17 14:02:27 2007 C:\WINDOWS\System32\wshtcpip.dll
        76f70000 45d70ac7 Feb 17 14:01:43 2007 C:\WINDOWS\System32\winrnr.dll
    SubSystemData:     00000000
```

```
    ProcessHeap:       00080000
    ProcessParameters: 00020000
    WindowTitle:  'C:\WINDOWS\system32\svchost.exe'
    ImageFile:    'C:\WINDOWS\system32\svchost.exe'
    CommandLine:  'C:\WINDOWS\system32\svchost.exe -k LocalService'
    DllPath:
'C:\WINDOWS\system32;C:\WINDOWS\system32;C:\WINDOWS\system;C:\WINDOWS;.;C:\WINDOWS\system32;C:\WIND
OWS;C:\WINDOWS\System32\Wbem'
    Environment:  00010000
        ALLUSERSPROFILE=C:\Documents and Settings\All Users
        ClusterLog=C:\WINDOWS\Cluster\cluster.log
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\WINDOWS\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        NUMBER_OF_PROCESSORS=1
        OS=Windows_NT
        Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 15 Model 5 Stepping 10, AuthenticAMD
        PROCESSOR_LEVEL=15
        PROCESSOR_REVISION=050a
        ProgramFiles=C:\Program Files
        SystemDrive=C:
        SystemRoot=C:\WINDOWS
        TEMP=C:\DOCUME~1\LOCALS~1\LOCALS~1\Temp
        TMP=C:\DOCUME~1\LOCALS~1\LOCALS~1\Temp
        USERDOMAIN=NT AUTHORITY
        USERNAME=LOCAL SERVICE
        USERPROFILE=C:\Documents and Settings\LocalService
        windir=C:\WINDOWS


        THREAD 862e7a70  Cid 0328.032c  Teb: 7ffdd000 Win32Thread: e1833008 WAIT: (Unknown)
UserMode Non-Alertable
            863665dc  NotificationEvent
        Not impersonating
        DeviceMap                 e159ad18
        Owning Process            862fdbf0       Image:         svchost.exe
        Wait Start TickCount      5488           Ticks: 110480 (0:00:28:46.250)
        Context Switch Count      47                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.109
        Win32 Start Address svchost!wmainCRTStartup (0x010020b9)
        Start Address kernel32!BaseProcessStartThunk (0x77e617f8)
        Stack Init f7547000 Current f7546c04 Base f7547000 Limit f7543000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f7546c1c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f7546c34 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f7546c78 808ed456 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f7546ca0 808ea5ad nt!IopSynchronousServiceTail+0x180 (FPO: [Non-Fpo])
        f7546d38 80883908 nt!NtReadFile+0x5d5 (FPO: [Non-Fpo])
        f7546d38 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f7546d64)
        0006fc40 7c82776b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0006fc44 77e418b2 ntdll!NtReadFile+0xc (FPO: [9,0,0])
        0006fcac 77f65edb kernel32!ReadFile+0x16c (FPO: [Non-Fpo])
        0006fcd8 77f65f82 ADVAPI32!ScGetPipeInput+0x2a (FPO: [Non-Fpo])
        0006fd4c 77f51ed9 ADVAPI32!ScDispatcherLoop+0x51 (FPO: [Non-Fpo])
        0006ffb0 0100213d ADVAPI32!StartServiceCtrlDispatcherW+0xe3 (FPO: [Non-Fpo])
        0006ffc0 77e6f23b svchost!_wmainCRTStartup+0x7f (FPO: [0,0,2])
        0006fff0 00000000 kernel32!BaseProcessStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 862cab28  Cid 0328.034c  Teb: 7ffdb000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            86300960  SynchronizationEvent
            8633fba0  SynchronizationEvent
        IRP List:
            863713e8: (0006,0094) Flags: 00000000  Mdl: 85df1cd8
        Not impersonating
        DeviceMap                 e159ad18
        Owning Process            862fdbf0       Image:         svchost.exe
        Wait Start TickCount      115363         Ticks: 605 (0:00:00:09.453)
        Context Switch Count      253
        UserTime                  00:00:00.015
        KernelTime                00:00:00.109
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x77f65e70)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f68ba000 Current f68b9914 Base f68ba000 Limit f68b7000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f68b992c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f68b9944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f68b9978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f68b9bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f68b9d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f68b9d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f68b9d64)
        0095fd98 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0095fd9c 74a430d8 ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0095ff70 010012a4 lmhsvc!ServiceMain+0x20a (FPO: [Non-Fpo])
        0095ffa4 77f65e91 svchost!ServiceStarter+0x9e (FPO: [Non-Fpo])
        0095ffb8 77e64829 ADVAPI32!ScSvcctrlThreadW+0x21 (FPO: [Non-Fpo])
        0095ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 8637bc20  Cid 0328.0360  Teb: 7ffda000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            863008b8  SynchronizationEvent
            86300888  SynchronizationEvent
        IRP List:
            86433798: (0006,0094) Flags: 00000000  Mdl: 8630f0d8
        Not impersonating
        DeviceMap                 e159ad18
        Owning Process            862fdbf0       Image:         svchost.exe
        Wait Start TickCount      4060           Ticks: 111908 (0:00:29:08.562)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address lmhsvc!CheckIPAddrWorkerRtn (0x74a42dcb)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f68b2000 Current f68b1914 Base f68b2000 Limit f68af000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f68b192c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f68b1944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f68b1978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f68b1bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f68b1d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f68b1d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f68b1d64)
        009aff78 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        009aff7c 74a42e61 ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        009affb8 77e64829 lmhsvc!CheckIPAddrWorkerRtn+0x96 (FPO: [Non-Fpo])
        009affec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 8637b9b0  Cid 0328.0364  Teb: 7ffd9000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            863005b8  NotificationEvent
            8637ba28  NotificationTimer
        Not impersonating
        DeviceMap                 e159ad18
        Owning Process            862fdbf0       Image:         svchost.exe
        Wait Start TickCount      115478         Ticks: 490 (0:00:00:07.656)
        Context Switch Count      30
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address lmhsvc!SmbGetHostThread (0x74a44003)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f68ae000 Current f68adc78 Base f68ae000 Limit f68ab000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f68adc90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f68adca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f68adcec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f68add50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f68add50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f68add64)
        009efb68 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        009efb6c 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        009efbdc 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        009efbf0 74a44064 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        009effb8 77e64829 lmhsvc!SmbGetHostThread+0x61 (FPO: [Non-Fpo])
        009effec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 86350db0  Cid 0328.0368  Teb: 7ffd8000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            863005b8  NotificationEvent
            86350e28  NotificationTimer
        Not impersonating
        DeviceMap                 e159ad18
        Owning Process            862fdbf0       Image:         svchost.exe
        Wait Start TickCount      115478         Ticks: 490 (0:00:00:07.656)
        Context Switch Count      31
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address lmhsvc!SmbGetHostThread (0x74a44003)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f68aa000 Current f68a9c78 Base f68aa000 Limit f68a7000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f68a9c90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f68a9ca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f68a9cec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f68a9d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f68a9d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f68a9d64)
        00a2fb68 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00a2fb6c 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        00a2fbdc 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        00a2fbf0 74a44064 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        00a2ffb8 77e64829 lmhsvc!SmbGetHostThread+0x61 (FPO: [Non-Fpo])
        00a2ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d546b0  Cid 0328.0618  Teb: 7ffd6000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d5c900  Semaphore Limit 0x7fffffff
            85d54728  NotificationTimer
        Not impersonating
        DeviceMap                 e159ad18
        Owning Process            862fdbf0       Image:         svchost.exe
        Wait Start TickCount      114964         Ticks: 1004 (0:00:00:15.687)
        Context Switch Count      24
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x77c7b0f5)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f654d000 Current f654cc24 Base f654d000 Limit f654a000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f654cc3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f654cc54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f654cc98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f654cd48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f654cd48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f654cd64)
        00b6fe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00b6fe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        00b6ff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        00b6ff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        00b6ffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        00b6ffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        00b6ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85d54440  Cid 0328.061c  Teb: 7ffd5000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            86338b58  QueueObject
            85d544b8  NotificationTimer
        IRP List:
            85d5fa48: (0006,0094) Flags: 00000800  Mdl: 00000000
        Not impersonating
        DeviceMap                 e159ad18
        Owning Process            862fdbf0       Image:         svchost.exe
        Wait Start TickCount      114965         Ticks: 1003 (0:00:00:15.671)
        Context Switch Count      37
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x77c7b0f5)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f652d000 Current f652cc4c Base f652d000 Limit f652a000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f652cc64 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f652cc7c 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f652ccc4 808e55e2 nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f652cd48 80883908 nt!NtRemoveIoCompletion+0xdc (FPO: [Non-Fpo])
        f652cd48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f652cd64)
        00bafeac 7c8277db ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00bafeb0 77e5bea2 ntdll!ZwRemoveIoCompletion+0xc (FPO: [5,0,0])
        00bafedc 77c7b900 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        00baff18 77c7b703 RPCRT4!COMMON_ProcessCalls+0xa1 (FPO: [Non-Fpo])
        00baff84 77c7b9b5 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x117 (FPO: [Non-Fpo])
        00baff8c 77c8872d RPCRT4!ProcessIOEventsWrapper+0xd (FPO: [Non-Fpo])
        00baffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        00baffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        00baffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 860bc330  Cid 0328.0620  Teb: 7ffd4000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d5f130  NotificationEvent
            862fdeb0  NotificationEvent
        Not impersonating
        DeviceMap                 e159ad18
        Owning Process            862fdbf0       Image:         svchost.exe
        Wait Start TickCount      5515           Ticks: 110453 (0:00:28:45.828)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address USERENV!NotificationThread (0x76929dd9)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6529000 Current f6528914 Base f6529000 Limit f6526000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f652892c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6528944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6528978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6528bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6528d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6528d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6528d64)
        00bffec0 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00bffec4 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00bfff6c 77e62fbe kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        00bfff88 76929e35 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        00bfffb8 77e64829 USERENV!NotificationThread+0x5f (FPO: [Non-Fpo])
        00bfffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85d54bf0  Cid 0328.0624  Teb: 7ffaf000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d78840  NotificationEvent
            85d78810  SynchronizationEvent
        Not impersonating
        DeviceMap                 e159ad18
        Owning Process            862fdbf0       Image:         svchost.exe
        Wait Start TickCount      5517           Ticks: 110451 (0:00:28:45.796)
        Context Switch Count      9
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address w32time!ClockDisciplineThread (0x767198ef)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6525000 Current f6524914 Base f6525000 Limit f6522000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f652492c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6524944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6524978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6524bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6524d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6524d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6524d64)
        00c3fcfc 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00c3fd00 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00c3fda8 77e62fbe kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        00c3fdc4 767116d5 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        00c3ffb8 77e64829 w32time!ClockDisciplineThread+0x27c (FPO: [Non-Fpo])
        00c3ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 860bc870  Cid 0328.062c  Teb: 7ffae000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            860bc8e8  NotificationTimer
        Not impersonating
        DeviceMap                 e159ad18
        Owning Process            862fdbf0       Image:         svchost.exe
        Wait Start TickCount      72107          Ticks: 43861 (0:00:11:25.328)
        Context Switch Count      13
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!RtlpTimerThread (0x7c83d3dd)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f651d000 Current f651cc98 Base f651d000 Limit f651a000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f651ccb0 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f651ccc8 80827e1e nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f651cd0c 8098c418 nt!KeDelayExecutionThread+0x254 (FPO: [Non-Fpo])
        f651cd54 80883908 nt!NtDelayExecution+0x84 (FPO: [Non-Fpo])
        f651cd54 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f651cd64)
        00c7ff9c 7c826f4b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00c7ffa0 7c83d424 ntdll!NtDelayExecution+0xc (FPO: [2,0,0])
        00c7ffb8 77e64829 ntdll!RtlpTimerThread+0x47 (FPO: [Non-Fpo])
        00c7ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85d558a0  Cid 0328.0634  Teb: 7ffad000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d63b90  QueueObject
            85d55918  NotificationTimer
        IRP List:
            85d55bf0: (0006,0094) Flags: 00000000  Mdl: 00000000
        Not impersonating
        DeviceMap                 e159ad18
        Owning Process            862fdbf0       Image:         svchost.exe
        Wait Start TickCount      115932         Ticks: 36 (0:00:00:00.562)
        Context Switch Count      76
        UserTime                  00:00:00.000
        KernelTime                00:00:00.093
        Win32 Start Address ntdll!RtlpWorkerThread (0x7c839efb)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6515000 Current f6514c4c Base f6515000 Limit f6512000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f6514c64 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6514c7c 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6514cc4 808e55e2 nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f6514d48 80883908 nt!NtRemoveIoCompletion+0xdc (FPO: [Non-Fpo])
        f6514d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6514d64)
        00cbff70 7c8277db ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00cbff74 7c839f38 ntdll!ZwRemoveIoCompletion+0xc (FPO: [5,0,0])
        00cbffb8 77e64829 ntdll!RtlpWorkerThread+0x3d (FPO: [Non-Fpo])
        00cbffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d51a80  Cid 0328.0638  Teb: 7ffac000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            862ef690  NotificationTimer
            85d518e0  NotificationEvent
            860bcb10  SynchronizationEvent
            85d518e0  NotificationEvent
            85d51910  SynchronizationEvent
            85d71540  NotificationEvent
            85d71570  SynchronizationEvent
            85d5fb10  SynchronizationEvent
            85d54bf0  Thread
            85d63c68  SynchronizationEvent
            85d63c38  SynchronizationEvent
            85d5fea0  SynchronizationEvent
            85d714b0  NotificationEvent
            85d51940  SynchronizationEvent
        Not impersonating
        DeviceMap                 e159ad18
        Owning Process            862fdbf0       Image:         svchost.exe
        Wait Start TickCount      115932         Ticks: 36 (0:00:00:00.562)
        Context Switch Count      50
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!RtlpWaitThread (0x7c83c643)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6511000 Current f6510914 Base f6511000 Limit f650e000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f651092c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6510944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6510978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6510bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6510d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6510d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6510d64)
        00cffcec 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00cffcf0 7c83c78e ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00cfffb8 77e64829 ntdll!RtlpWaitThread+0x161 (FPO: [Non-Fpo])
        00cfffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 86380b70  Cid 0328.07f0  Teb: 7ffd7000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d5c900  Semaphore Limit 0x7fffffff
            86380be8  NotificationTimer
        Not impersonating
        DeviceMap                 e159ad18
        Owning Process            862fdbf0       Image:         svchost.exe
        Wait Start TickCount      114967         Ticks: 1001 (0:00:00:15.640)
        Context Switch Count      18
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x77c7b0f5)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f65d1000 Current f65d0c24 Base f65d1000 Limit f65ce000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f65d0c3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f65d0c54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f65d0c98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f65d0d48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f65d0d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f65d0d64)
        00d3fe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00d3fe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        00d3ff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        00d3ff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        00d3ffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        00d3ffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        00d3ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d41478  Cid 0328.07f4  Teb: 7ffab000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            86338b58  QueueObject
            85d414f0  NotificationTimer
        Not impersonating
        DeviceMap                 e159ad18
        Owning Process            862fdbf0       Image:         svchost.exe
        Wait Start TickCount      114965         Ticks: 1003 (0:00:00:15.671)
        Context Switch Count      34
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x77c7b0f5)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6519000 Current f6518c4c Base f6519000 Limit f6516000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f6518c64 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6518c7c 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6518cc4 808e55e2 nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f6518d48 80883908 nt!NtRemoveIoCompletion+0xdc (FPO: [Non-Fpo])
        f6518d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6518d64)
        00d7feac 7c8277db ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00d7feb0 77e5bea2 ntdll!ZwRemoveIoCompletion+0xc (FPO: [5,0,0])
        00d7fedc 77c7b900 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        00d7ff18 77c7b703 RPCRT4!COMMON_ProcessCalls+0xa1 (FPO: [Non-Fpo])
        00d7ff84 77c7b9b5 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x117 (FPO: [Non-Fpo])
        00d7ff8c 77c8872d RPCRT4!ProcessIOEventsWrapper+0xd (FPO: [Non-Fpo])
        00d7ffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        00d7ffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        00d7ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

Svchost process (netsvcs)

```
PROCESS 86433518  SessionId: 0  Cid: 0350    Peb: 7ffdb000  ParentCid: 0198
    DirBase: 3af1a140  ObjectTable: e17ec890  HandleCount: 871.
    Image: svchost.exe
    VadRoot 862e09c8 Vads 308 Clone 0 Private 2036. Modified 30. Locked 3.
    DeviceMap e1000170
    Token                             e1985978
    ElapsedTime                       00:39:03.843
    UserTime                          00:00:03.171
    KernelTime                        00:00:19.812
    QuotaPoolUsage[PagedPool]         130076
    QuotaPoolUsage[NonPagedPool]      25984
    Working Set Sizes (now,min,max)  (4627, 50, 345) (18508KB, 200KB, 1380KB)
    PeakWorkingSetSize                5501
    VirtualSize                       78 Mb
    PeakVirtualSize                   112 Mb
    PageFaultCount                    45300
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      3217

    Setting context for this process...
.process /p /r ffffffff86433518

    !peb
PEB at 7ffdb000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         01000000
    Ldr                       7c8877e0
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00081f18 . 04799590
    Ldr.InLoadOrderModuleList:           00081eb0 . 04799580
    Ldr.InMemoryOrderModuleList:         00081eb8 . 04799588
            Base TimeStamp                     Module
         1000000 45d6a03c Feb 17 06:27:08 2007 C:\WINDOWS\System32\svchost.exe
        7c800000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\ntdll.dll
        77e40000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\kernel32.dll
        77f50000 45d70a26 Feb 17 13:59:02 2007 C:\WINDOWS\system32\ADVAPI32.dll
        77c50000 45d70aaa Feb 17 14:01:14 2007 C:\WINDOWS\system32\RPCRT4.dll
        76f50000 45d70ac3 Feb 17 14:01:39 2007 C:\WINDOWS\system32\Secur32.dll
        77e00000 45d70aab Feb 17 14:01:15 2007 C:\WINDOWS\System32\NTMARTA.DLL
        77ba0000 45d70b06 Feb 17 14:02:46 2007 C:\WINDOWS\system32\msvcrt.dll
        77380000 45d70ac7 Feb 17 14:01:43 2007 C:\WINDOWS\system32\USER32.dll
        77c00000 45d70a3e Feb 17 13:59:26 2007 C:\WINDOWS\system32\GDI32.dll
        76f10000 45d70ad5 Feb 17 14:01:57 2007 C:\WINDOWS\system32\WLDAP32.dll
        7e020000 45d70aa8 Feb 17 14:01:12 2007 C:\WINDOWS\System32\SAMLIB.dll
        77670000 45d70aa5 Feb 17 14:01:09 2007 C:\WINDOWS\system32\ole32.dll
          650000 45d69418 Feb 17 05:35:20 2007 C:\WINDOWS\System32\xpsp2res.dll
        7fcf0000 45d70ad8 Feb 17 14:02:00 2007 c:\windows\system32\wzcsvc.dll
        76e30000 45d70abb Feb 17 14:01:31 2007 c:\windows\system32\rtutils.dll
        76cc0000 3e80249b Mar 25 09:42:51 2003 c:\windows\system32\WMI.dll
        76d10000 45d70a45 Feb 17 13:59:33 2007 c:\windows\system32\DHCPCSVC.DLL
        76ed0000 45d70a64 Feb 17 14:00:04 2007 c:\windows\system32\DNSAPI.dll
        71c00000 45d70ae9 Feb 17 14:02:17 2007 c:\windows\system32\WS2_32.dll
        71bf0000 45d70aea Feb 17 14:02:18 2007 c:\windows\system32\WS2HELP.dll
        76cf0000 45d70a6c Feb 17 14:00:12 2007 c:\windows\system32\iphlpapi.dll
        76b70000 45d70ab5 Feb 17 14:01:25 2007 c:\windows\system32\PSAPI.DLL
        77d00000 45d70aa6 Feb 17 14:01:10 2007 C:\WINDOWS\system32\OLEAUT32.dll
        761b0000 45d70a80 Feb 17 14:00:32 2007 C:\WINDOWS\system32\CRYPT32.dll
        76190000 45d70aac Feb 17 14:01:16 2007 C:\WINDOWS\system32\MSASN1.dll
        76f00000 45d70af7 Feb 17 14:02:31 2007 c:\windows\system32\WTSAPI32.dll
        771f0000 45d70ace Feb 17 14:01:50 2007 c:\windows\system32\WINSTA.dll
        71c40000 45d70a82 Feb 17 14:00:34 2007 C:\WINDOWS\system32\NETAPI32.dll
        77da0000 45d70ac0 Feb 17 14:01:36 2007 C:\WINDOWS\system32\SHLWAPI.dll
```

```
        4b180000 45d70a3c Feb 17 13:59:24 2007 c:\windows\system32\ESENT.dll
        76a80000 3e80249c Mar 25 09:42:52 2003 c:\windows\system32\ATL.DLL
        76b40000 45d70ac3 Feb 17 14:01:39 2007 c:\windows\system32\shsvcs.dll
        68000000 45d69786 Feb 17 05:49:58 2007 C:\WINDOWS\System32\rsaenh.dll
        777b0000 45d70a3b Feb 17 13:59:23 2007 C:\WINDOWS\System32\CLBCatQ.DLL
        77010000 45d70a76 Feb 17 14:00:22 2007 C:\WINDOWS\System32\COMRes.dll
        77b90000 45d70ac8 Feb 17 14:01:44 2007 C:\WINDOWS\system32\VERSION.dll
        74d10000 45d70aaa Feb 17 14:01:14 2007 C:\WINDOWS\System32\rastls.dll
        75360000 45d70a85 Feb 17 14:00:37 2007 C:\WINDOWS\system32\CRYPTUI.dll
        76bb0000 45d70acf Feb 17 14:01:51 2007 C:\WINDOWS\system32\WINTRUST.dll
        76c10000 45d70a5d Feb 17 13:59:57 2007 C:\WINDOWS\system32\imagehlp.dll
        76cd0000 45d70a85 Feb 17 14:00:37 2007 C:\WINDOWS\System32\MPRAPI.dll
        76df0000 45d70a11 Feb 17 13:58:41 2007 C:\WINDOWS\System32\ACTIVEDS.dll
        76dc0000 45d70a22 Feb 17 13:58:58 2007 C:\WINDOWS\System32\adsldpc.dll
        76b80000 45d70a7f Feb 17 14:00:31 2007 C:\WINDOWS\System32\credui.dll
        7c8d0000 45d70abb Feb 17 14:01:31 2007 C:\WINDOWS\system32\SHELL32.dll
        770e0000 45d70ab3 Feb 17 14:01:23 2007 C:\WINDOWS\System32\SETUPAPI.dll
        76e90000 45d70a9e Feb 17 14:01:02 2007 C:\WINDOWS\System32\RASAPI32.dll
        76e40000 45d70aa3 Feb 17 14:01:07 2007 C:\WINDOWS\System32\rasman.dll
        76e60000 45d70abc Feb 17 14:01:32 2007 C:\WINDOWS\System32\TAPI32.dll
        76aa0000 45d70af0 Feb 17 14:02:24 2007 C:\WINDOWS\System32\WINMM.dll
        72430000 45d70ac8 Feb 17 14:01:44 2007 C:\WINDOWS\System32\WinSCard.dll
        77530000 45d70a06 Feb 17 13:58:30 2007 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_5.82.3790.3959_x-ww_78FCF8D0\COMCTL32.dll
        77420000 45d70a05 Feb 17 13:58:29 2007 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.3790.3959_x-ww_D8713E55\Comctl32.dll
        76670000 45d70aa0 Feb 17 14:01:04 2007 C:\WINDOWS\System32\raschap.dll
        76ad0000 45d70aac Feb 17 14:01:16 2007 c:\windows\system32\schedsvc.dll
        766f0000 45d70a9f Feb 17 14:01:03 2007 c:\windows\system32\NTDSAPI.dll
        76c40000 45d70a49 Feb 17 13:59:37 2007 c:\windows\system32\AUTHZ.dll
        76920000 45d70ac8 Feb 17 14:01:44 2007 c:\windows\system32\USERENV.dll
        74d70000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\System32\MSIDLE.DLL
        74fc0000 45d70ad1 Feb 17 14:01:53 2007 c:\windows\system32\wkssvc.dll
        59ec0000 45d70ae4 Feb 17 14:02:12 2007 C:\WINDOWS\System32\wiarpc.dll
        74ed0000 45d70aec Feb 17 14:02:20 2007 c:\windows\system32\srvsvc.dll
        5f270000 45d70a4a Feb 17 13:59:38 2007 C:\WINDOWS\System32\HNETCFG.DLL
        4c590000 45d70a28 Feb 17 13:59:04 2007 c:\windows\system32\aelupsvc.dll
        75e60000 45d70a36 Feb 17 13:59:18 2007 c:\windows\system32\apphelp.dll
        73c70000 45d70ac1 Feb 17 14:01:37 2007 c:\windows\system32\seclogon.dll
        74d60000 45d70a97 Feb 17 14:00:55 2007 c:\windows\pchealth\helpctr\binaries\pchsvc.dll
        77930000 45d70a3b Feb 17 13:59:23 2007 c:\windows\system32\es.dll
        74db0000 45d70a5e Feb 17 13:59:58 2007 c:\windows\system32\dmserver.dll
        76da0000 45d70a84 Feb 17 14:00:36 2007 c:\windows\system32\cryptsvc.dll
        751c0000 45d70a27 Feb 17 13:59:03 2007 c:\windows\system32\certcli.dll
        5b890000 45d70ad7 Feb 17 14:01:59 2007 c:\windows\system32\VSSAPI.DLL
        71bd0000 45d70a84 Feb 17 14:00:36 2007 C:\WINDOWS\system32\MPR.dll
        76b10000 3e80249c Mar 25 09:42:52 2003 c:\windows\system32\sfc.dll
        76be0000 45d70ab5 Feb 17 14:01:25 2007 c:\windows\system32\sfc_os.dll
        74e00000 45d70a18 Feb 17 13:58:48 2007 c:\windows\system32\browser.dll
        5f8c0000 3e80253c Mar 25 09:45:32 2003 C:\WINDOWS\System32\NETRAP.dll
        75da0000 45d70afe Feb 17 14:02:38 2007 C:\WINDOWS\System32\SXS.DLL
        74eb0000 45d70aca Feb 17 14:01:46 2007 c:\windows\system32\trkwks.dll
        4a710000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\System32\comsvcs.dll
        72310000 45d70aad Feb 17 14:01:17 2007 c:\windows\system32\sens.dll
        5fb50000 45d70aa0 Feb 17 14:01:04 2007 c:\windows\system32\qmgr.dll
        766d0000 45d70abc Feb 17 14:01:32 2007 c:\windows\system32\SHFOLDER.dll
        4e7c0000 45d70a04 Feb 17 13:58:28 2007
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.WinHTTP_6595b64144ccf1df_5.1.3790.3959_x-
ww_D1A2C081\WINHTTP.dll
        50000000 45d6a097 Feb 17 06:28:39 2007 c:\windows\system32\wuauserv.dll
        58af0000 45d70aed Feb 17 14:02:21 2007 c:\windows\system32\wbem\wmisvc.dll
        50040000 46ae8ef5 Jul 31 02:23:01 2007 C:\WINDOWS\system32\wuaueng.dll
        73070000 45d70acb Feb 17 14:01:47 2007 C:\WINDOWS\System32\WINSPOOL.DRV
        74fa0000 45d70a19 Feb 17 13:58:49 2007 C:\WINDOWS\System32\Cabinet.dll
        60410000 3e802590 Mar 25 09:46:56 2003 C:\WINDOWS\System32\mspatcha.dll
        71b20000 45d70b0d Feb 17 14:02:53 2007 C:\WINDOWS\system32\mswsock.dll
        71ae0000 45d70af3 Feb 17 14:02:27 2007 C:\WINDOWS\System32\wshtcpip.dll
        68100000 45d6978b Feb 17 05:50:03 2007 C:\WINDOWS\System32\dssenh.dll
        750f0000 45d70ad3 Feb 17 14:01:55 2007 C:\WINDOWS\system32\wbem\wbemcomn.dll
        752e0000 45d70ad5 Feb 17 14:01:57 2007 C:\WINDOWS\System32\Wbem\wbemcore.dll
```

```
         3de0000 45d6a071 Feb 17 06:28:01 2007 C:\WINDOWS\System32\msvcp60.dll
        769f0000 45d70a3f Feb 17 13:59:27 2007 C:\WINDOWS\System32\Wbem\esscli.dll
        75550000 45d70a3a Feb 17 13:59:22 2007 C:\WINDOWS\System32\Wbem\FastProx.dll
        74ce0000 3e8024a8 Mar 25 09:43:04 2003 C:\WINDOWS\system32\wbem\wbemsvc.dll
        74e60000 45d70aef Feb 17 14:02:23 2007 C:\WINDOWS\system32\wbem\wmiutils.dll
        75060000 45d70ab7 Feb 17 14:01:27 2007 C:\WINDOWS\system32\wbem\repdrvfs.dll
        58b50000 45d70aeb Feb 17 14:02:19 2007 C:\WINDOWS\system32\wbem\wmiprvsd.dll
        5fb10000 45d70a7a Feb 17 14:00:26 2007 C:\WINDOWS\system32\NCObjAPI.DLL
        75200000 45d70ad7 Feb 17 14:01:59 2007 C:\WINDOWS\system32\wbem\wbemess.dll
        5faf0000 45d70a7c Feb 17 14:00:28 2007 C:\WINDOWS\system32\wbem\ncprov.dll
        77840000 45d70a86 Feb 17 14:00:38 2007 c:\windows\system32\netman.dll
        76300000 45d70a8a Feb 17 14:00:42 2007 c:\windows\system32\netshell.dll
        74de0000 45d70a43 Feb 17 13:59:31 2007 c:\windows\system32\CLUSAPI.dll
        77210000 45d70aee Feb 17 14:02:22 2007 C:\WINDOWS\system32\WININET.dll
        730a0000 45d70af9 Feb 17 14:02:33 2007 c:\windows\system32\WZCSAPI.DLL
        753e0000 45d70aa2 Feb 17 14:01:06 2007 C:\WINDOWS\System32\RASDLG.dll
        76f80000 45d70a9d Feb 17 14:01:01 2007 C:\WINDOWS\System32\rasadhlp.dll
        73c80000 45d70ad4 Feb 17 14:01:56 2007 C:\WINDOWS\system32\wbem\wbemcons.dll
    SubSystemData:     00000000
    ProcessHeap:       00080000
    ProcessParameters: 00020000
    WindowTitle:  'C:\WINDOWS\System32\svchost.exe'
    ImageFile:    'C:\WINDOWS\System32\svchost.exe'
    CommandLine:  'C:\WINDOWS\System32\svchost.exe -k netsvcs'
    DllPath:
'C:\WINDOWS\System32;C:\WINDOWS\system32;C:\WINDOWS\system;C:\WINDOWS;.;C:\WINDOWS\system32;C:\WIND
OWS;C:\WINDOWS\System32\Wbem'
    Environment:  00010000
        ALLUSERSPROFILE=C:\Documents and Settings\All Users
        ClusterLog=C:\WINDOWS\Cluster\cluster.log
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\WINDOWS\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        NUMBER_OF_PROCESSORS=1
        OS=Windows_NT
        Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 15 Model 5 Stepping 10, AuthenticAMD
        PROCESSOR_LEVEL=15
        PROCESSOR_REVISION=050a
        ProgramFiles=C:\Program Files
        SystemDrive=C:
        SystemRoot=C:\WINDOWS
        TEMP=C:\WINDOWS\TEMP
        TMP=C:\WINDOWS\TEMP
        USERPROFILE=C:\Documents and Settings\Default User
        windir=C:\WINDOWS
```

```
        THREAD 8633c468  Cid 0350.0354  Teb: 7ffdf000 Win32Thread: e19150e0 WAIT: (Unknown)
UserMode Non-Alertable
            863796dc  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      20713          Ticks: 95255 (0:00:24:48.359)
        Context Switch Count      154                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.156
        Win32 Start Address svchost!wmainCRTStartup (0x010020b9)
        Start Address kernel32!BaseProcessStartThunk (0x77e617f8)
        Stack Init f6b23000 Current f6b22c04 Base f6b23000 Limit f6b20000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6b22c1c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6b22c34 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6b22c78 808ed456 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6b22ca0 808ea5ad nt!IopSynchronousServiceTail+0x180 (FPO: [Non-Fpo])
        f6b22d38 80883908 nt!NtReadFile+0x5d5 (FPO: [Non-Fpo])
        f6b22d38 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6b22d64)
        0006fc40 7c82776b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0006fc44 77e418b2 ntdll!NtReadFile+0xc (FPO: [9,0,0])
        0006fcac 77f65edb kernel32!ReadFile+0x16c (FPO: [Non-Fpo])
        0006fcd8 77f65f82 ADVAPI32!ScGetPipeInput+0x2a (FPO: [Non-Fpo])
        0006fd4c 77f51ed9 ADVAPI32!ScDispatcherLoop+0x51 (FPO: [Non-Fpo])
        0006ffb0 0100213d ADVAPI32!StartServiceCtrlDispatcherW+0xe3 (FPO: [Non-Fpo])
        0006ffc0 77e6f23b svchost!_wmainCRTStartup+0x7f (FPO: [0,0,2])
        0006fff0 00000000 kernel32!BaseProcessStart+0x23 (FPO: [Non-Fpo])

        THREAD 8632ad08  Cid 0350.0370  Teb: 7ffdc000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            8632ad80  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      113685         Ticks: 2283 (0:00:00:35.671)
        Context Switch Count      73
        UserTime                  00:00:00.000
        KernelTime                00:00:00.046
        Win32 Start Address ntdll!RtlpTimerThread (0x7c83d3dd)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f68a6000 Current f68a5c98 Base f68a6000 Limit f68a3000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f68a5cb0 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f68a5cc8 80827e1e nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f68a5d0c 8098c418 nt!KeDelayExecutionThread+0x254 (FPO: [Non-Fpo])
        f68a5d54 80883908 nt!NtDelayExecution+0x84 (FPO: [Non-Fpo])
        f68a5d54 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f68a5d64)
        00d2ff9c 7c826f4b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00d2ffa0 7c83d424 ntdll!NtDelayExecution+0xc (FPO: [2,0,0])
        00d2ffb8 77e64829 ntdll!RtlpTimerThread+0x47 (FPO: [Non-Fpo])
        00d2ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 863fc020  Cid 0350.0374  Teb: 7ffda000 Win32Thread: e197b008 WAIT: (Unknown)
UserMode Non-Alertable
            862fda98  QueueObject
            863fc098  NotificationTimer
        IRP List:
            86300a98: (0006,0094) Flags: 00000900  Mdl: 86315298
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      115428         Ticks: 540 (0:00:00:08.437)
        Context Switch Count      410                 LargeStack
        UserTime                  00:00:00.156
        KernelTime                00:00:00.406
        Win32 Start Address ntdll!RtlpWorkerThread (0x7c839efb)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6ac3000 Current f6ac2c4c Base f6ac3000 Limit f6ac0000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f6ac2c64 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6ac2c7c 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6ac2cc4 808e55e2 nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f6ac2d48 80883908 nt!NtRemoveIoCompletion+0xdc (FPO: [Non-Fpo])
        f6ac2d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6ac2d64)
        00d6ff70 7c8277db ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00d6ff74 7c839f38 ntdll!ZwRemoveIoCompletion+0xc (FPO: [5,0,0])
        00d6ffb8 77e64829 ntdll!RtlpWorkerThread+0x3d (FPO: [Non-Fpo])
        00d6ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 862fa740  Cid 0350.0378  Teb: 7ffd9000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            862fda98  QueueObject
            862fa7b8  NotificationTimer
        IRP List:
            864288e8: (0006,01b4) Flags: 00000800  Mdl: 00000000
            865a04b0: (0006,01b4) Flags: 00000000  Mdl: 00000000
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      114982         Ticks: 986 (0:00:00:15.406)
        Context Switch Count      191
        UserTime                  00:00:00.031
        KernelTime                00:00:00.531
        Win32 Start Address ntdll!RtlpWorkerThread (0x7c839efb)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f689e000 Current f689dc4c Base f689e000 Limit f689b000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f689dc64 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f689dc7c 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f689dcc4 808e55e2 nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f689dd48 80883908 nt!NtRemoveIoCompletion+0xdc (FPO: [Non-Fpo])
        f689dd48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f689dd64)
        00daff70 7c8277db ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00daff74 7c839f38 ntdll!ZwRemoveIoCompletion+0xc (FPO: [5,0,0])
        00daffb8 77e64829 ntdll!RtlpWorkerThread+0x3d (FPO: [Non-Fpo])
        00daffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 8637cca0  Cid 0350.0380  Teb: 7ffd7000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            86350a68  NotificationEvent
            862fa2c0  NotificationEvent
            862fa260  NotificationEvent
            86375a08  NotificationEvent
            8637cd18  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      4089           Ticks: 111879 (0:00:29:08.109)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wzcsvc!ServiceStart (0x7fd52038)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6896000 Current f6895914 Base f6896000 Limit f6893000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f689592c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6895944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6895978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6895bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6895d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6895d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6895d64)
        00e3feac 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00e3feb0 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00e3ff58 77e62fbe kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        00e3ff74 7fd520cf kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        00e3ffb8 77e64829 wzcsvc!ServiceStart+0x97 (FPO: [Non-Fpo])
        00e3ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 862e4a48  Cid 0350.0384  Teb: 7ffd6000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            862f48f0  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      19259          Ticks: 96709 (0:00:25:11.078)
        Context Switch Count      162
        UserTime                  00:00:00.015
        KernelTime                00:00:00.140
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x77f65e70)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6892000 Current f6891c78 Base f6892000 Limit f688f000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6891c90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6891ca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6891cec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6891d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f6891d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6891d64)
        00e7fec4 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00e7fec8 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        00e7ff38 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        00e7ff4c 76b4bf88 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        00e7ff70 010012a4 shsvcs!CGenericServiceManager::_ServiceMain+0xea (FPO: [Non-Fpo])
        00e7ffa4 77f65e91 svchost!ServiceStarter+0x9e (FPO: [Non-Fpo])
        00e7ffb8 77e64829 ADVAPI32!ScSvcctrlThreadW+0x21 (FPO: [Non-Fpo])
        00e7ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 8634adb0  Cid 0350.0388  Teb: 7ffd5000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            862e4990  NotificationTimer
            86366810  SynchronizationEvent
            865e94a0  SynchronizationEvent
            86436f80  NotificationEvent
            8645b880  SynchronizationEvent
            86421340  SynchronizationEvent
            8645bbc0  SynchronizationEvent
            85de2ce8  SynchronizationEvent
            85d79d80  NotificationEvent
            85d62424  NotificationEvent
            85d64088  SynchronizationEvent
            865c0ff0  SynchronizationEvent
            85d6a070  NotificationEvent
            863fc82c  NotificationEvent
            860bc2c0  SynchronizationEvent
            85d78020  SynchronizationEvent
            85d5cf58  SynchronizationEvent
            862e7590  NotificationEvent
            85d46b18  ProcessObject
            85d62208  SynchronizationEvent
            85d4fc20  NotificationEvent
            863388d0  SynchronizationTimer
            86351548  SynchronizationEvent
            864a1810  SynchronizationEvent
            85da4ff0  SynchronizationEvent
            85d87da8  SynchronizationEvent
            863cb46c  NotificationEvent
            85da3ca0  SynchronizationEvent
            85da3cd0  SynchronizationEvent
            864630c4  NotificationEvent
            863bfdd8  SynchronizationEvent
            85d51a50  SynchronizationEvent
            85d557d0  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      62948          Ticks: 53020 (0:00:13:48.437)
        Context Switch Count      49
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address 0x00001b04
        LPC Server thread working on message Id 1b04
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f688e000 Current f688d914 Base f688e000 Limit f688b000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f688d92c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f688d944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f688d978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f688dbf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f688dd48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f688dd48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f688dd64)
        00ebfcec 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00ebfcf0 7c83c78e ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00ebffb8 77e64829 ntdll!RtlpWaitThread+0x161 (FPO: [Non-Fpo])
        00ebffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 862d6740  Cid 0350.038c  Teb: 7ffdd000 Win32Thread: e1028828 WAIT: (Unknown)
UserMode Non-Alertable
            8632a820  Semaphore Limit 0x7fffffff
            862d67b8  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      106020         Ticks: 9948 (0:00:02:35.437)
        Context Switch Count      1189                LargeStack
        UserTime                  00:00:00.031
        KernelTime                00:00:01.031
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6ad3000 Current f6ad2c24 Base f6ad3000 Limit f6ad0000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6ad2c3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6ad2c54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6ad2c98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6ad2d48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f6ad2d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6ad2d64)
        010cfe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        010cfe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        010cff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        010cff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        010cffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        010cffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        010cffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 8630cdb0  Cid 0350.0394  Teb: 7ffaf000 Win32Thread: e1833d30 WAIT: (Unknown)
UserMode Non-Alertable
            86390e10  SynchronizationEvent
            8631b7f8  SynchronizationEvent
            86367524  NotificationEvent
            8631b7c8  SynchronizationEvent
            862f4ad8  SynchronizationTimer
            8630ce28  NotificationTimer
        IRP List:
            862d4280: (0006,01b4) Flags: 00000000  Mdl: 00000000
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      84611          Ticks: 31357 (0:00:08:09.953)
        Context Switch Count      90                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.140
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x77f65e70)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6f2e000 Current f6f2d914 Base f6f2e000 Limit f6f2b000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6f2d92c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6f2d944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6f2d978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6f2dbf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6f2dd48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6f2dd48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6f2dd64)
        0114fd9c 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0114fda0 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0114fe48 77e62fbe kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        0114fe64 76ae1948 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0114ff28 76ae1f62 schedsvc!CSchedWorker::MainServiceLoop+0x16e (FPO: [Non-Fpo])
        0114ff2c 76adc5ac schedsvc!SchedMain+0xb (FPO: [1,0,0])
        0114ff5c 76adc6e9 schedsvc!SchedStart+0x266 (FPO: [Non-Fpo])
        0114ff70 010012a4 schedsvc!SchedServiceMain+0x63 (FPO: [Non-Fpo])
        0114ffa4 77f65e91 svchost!ServiceStarter+0x9e (FPO: [Non-Fpo])
        0114ffb8 77e64829 ADVAPI32!ScSvcctrlThreadW+0x21 (FPO: [Non-Fpo])
        0114ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 862d4458  Cid 0350.0398  Teb: 7ffae000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            8645ce40  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      4197           Ticks: 111771 (0:00:29:06.421)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address AUTHZ!AuthzpDeQueueThreadWorker (0x76c44d89)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6a07000 Current f6a06c78 Base f6a07000 Limit f6a04000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6a06c90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6a06ca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6a06cec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6a06d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f6a06d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6a06d64)
        0125ff14 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0125ff18 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0125ff88 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        0125ff9c 76c44daf kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0125ffb8 77e64829 AUTHZ!AuthzpDeQueueThreadWorker+0x26 (FPO: [Non-Fpo])
        0125ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 864258d8  Cid 0350.039c  Teb: 7ffad000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            86425950  NotificationTimer
        IRP List:
            863846f0: (0006,0094) Flags: 00000800  Mdl: 00000000
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      114788         Ticks: 1180 (0:00:00:18.437)
        Context Switch Count      19
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x77c7b0f5)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6a2b000 Current f6a2ac98 Base f6a2b000 Limit f6a28000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f6a2acb0 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6a2acc8 80827e1e nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6a2ad0c 8098c418 nt!KeDelayExecutionThread+0x254 (FPO: [Non-Fpo])
        f6a2ad54 80883908 nt!NtDelayExecution+0x84 (FPO: [Non-Fpo])
        f6a2ad54 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6a2ad64)
        0129ff70 7c826f4b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0129ff74 77c8884c ntdll!NtDelayExecution+0xc (FPO: [2,0,0])
        0129ff8c 77c88768 RPCRT4!TIMER::Wait+0x2b (FPO: [Non-Fpo])
        0129ffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0xe8 (FPO: [Non-Fpo])
        0129ffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        0129ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 862d47d8  Cid 0350.03a4  Teb: 7ffab000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            863714a0  QueueObject
        IRP List:
            862d1848: (0006,0094) Flags: 00000800  Mdl: 00000000
            86305800: (0006,0094) Flags: 00000800  Mdl: 00000000
            85d5fd08: (0006,0094) Flags: 00000800  Mdl: 00000000
            85d72b68: (0006,0094) Flags: 00000800  Mdl: 00000000
            85d65918: (0006,0094) Flags: 00000800  Mdl: 00000000
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      111913         Ticks: 4055 (0:00:01:03.359)
        Context Switch Count      114
        UserTime                  00:00:00.000
        KernelTime                00:00:00.171
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x77c7b0f5)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6882000 Current f6881c4c Base f6882000 Limit f687f000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6881c64 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6881c7c 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6881cc4 808e55e2 nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f6881d48 80883908 nt!NtRemoveIoCompletion+0xdc (FPO: [Non-Fpo])
        f6881d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6881d64)
        0131feac 7c8277db ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0131feb0 77e5bea2 ntdll!ZwRemoveIoCompletion+0xc (FPO: [5,0,0])
        0131fedc 77c7b900 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        0131ff18 77c7b703 RPCRT4!COMMON_ProcessCalls+0xa1 (FPO: [Non-Fpo])
        0131ff84 77c7b9b5 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x117 (FPO: [Non-Fpo])
        0131ff8c 77c8872d RPCRT4!ProcessIOEventsWrapper+0xd (FPO: [Non-Fpo])
        0131ffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        0131ffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        0131ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 8631bb78  Cid 0350.03a8  Teb: 7ffaa000 Win32Thread: e1813008 WAIT: (Unknown)
UserMode Non-Alertable
            865e9378  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      115331         Ticks: 637 (0:00:00:09.953)
        Context Switch Count      158                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address schedsvc!WindowMsgFcn (0x76adc1cd)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6f1e000 Current f6f1dbc4 Base f6f1e000 Limit f6f1b000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f6f1dbdc 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6f1dbf4 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6f1dc38 bf89b1c3 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6f1dc94 bf89b986 win32k!xxxSleepThread+0x1be (FPO: [Non-Fpo])
        f6f1dcec bf89da22 win32k!xxxRealInternalGetMessage+0x46a (FPO: [Non-Fpo])
        f6f1dd4c 80883908 win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        f6f1dd4c 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6f1dd64)
        0135ff30 7739c811 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0135ff50 76adc30e USER32!NtUserGetMessage+0xc
        0135ffb8 77e64829 schedsvc!WindowMsgFcn+0x141 (FPO: [Non-Fpo])
        0135ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 8631b908  Cid 0350.03ac  Teb: 7ffa9000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            86384578  NotificationEvent
            865e97e8  SynchronizationEvent
            865e97a8  SynchronizationEvent
            863ff6e8  SynchronizationEvent
        Impersonation token:  e198d590 (Level Impersonation)
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      8195           Ticks: 107773 (0:00:28:03.953)
        Context Switch Count      16
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address schedsvc!PfSvcMainThread (0x76adb25a)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f687a000 Current f6879914 Base f687a000 Limit f6877000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f687992c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6879944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6879978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6879bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6879d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6879d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6879d64)
        0139feac 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0139feb0 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0139ff58 77e62fbe kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        0139ff74 76adb43b kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0139ffb8 77e64829 schedsvc!PfSvcMainThread+0x1e1 (FPO: [Non-Fpo])
        0139ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 862d2300  Cid 0350.03c4  Teb: 7ffa5000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            86303190  NotificationEvent
            863ff718  SynchronizationEvent
            86444730  NotificationEvent
        Impersonation token:  e1905360 (Level Impersonation)
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      11419          Ticks: 104549 (0:00:27:13.578)
        Context Switch Count      88
        UserTime                  00:00:00.296
        KernelTime                00:00:00.609
        Win32 Start Address schedsvc!PfSvProcessTraceThread (0x76adaf57)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f7131000 Current f7130914 Base f7131000 Limit f712e000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f713092c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f7130944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f7130978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f7130bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f7130d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f7130d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f7130d64)
        0149fe48 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0149fe4c 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0149fef4 77e62fbe kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        0149ff10 76adb180 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0149ffb8 77e64829 schedsvc!PfSvProcessTraceThread+0x229 (FPO: [Non-Fpo])
        0149ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 862d2730  Cid 0350.03d4  Teb: 7ffa3000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            862d27a8  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      113727         Ticks: 2241 (0:00:00:35.015)
        Context Switch Count      46
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!RtlpIOWorkerThread (0x7c8193fb)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f686e000 Current f686dc98 Base f686e000 Limit f686b000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f686dcb0 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f686dcc8 80827e1e nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f686dd0c 8098c418 nt!KeDelayExecutionThread+0x254 (FPO: [Non-Fpo])
        f686dd54 80883908 nt!NtDelayExecution+0x84 (FPO: [Non-Fpo])
        f686dd54 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f686dd64)
        0151ff8c 7c826f4b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0151ff90 7c81943a ntdll!NtDelayExecution+0xc (FPO: [2,0,0])
        0151ffb8 77e64829 ntdll!RtlpIOWorkerThread+0x3f (FPO: [Non-Fpo])
        0151ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 86354728  Cid 0350.0400  Teb: 7ffa8000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            863226c8  SynchronizationEvent
            86541d38  SynchronizationEvent
            86343640  SynchronizationEvent
            86343538  SynchronizationEvent
            85de3d00  SynchronizationEvent
            85debf80  SynchronizationEvent
            863547a0  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      96428          Ticks: 19540 (0:00:05:05.312)
        Context Switch Count      67
        UserTime                  00:00:00.000
        KernelTime                00:00:00.046
        Win32 Start Address 0x00000323
        LPC Server thread working on message Id 323
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6856000 Current f6855914 Base f6856000 Limit f6853000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f685592c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6855944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6855978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6855bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6855d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6855d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6855d64)
        013dfdd4 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        013dfdd8 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        013dfe80 77e62fbe kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        013dfe9c 74ed4651 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        013dff28 74ed4b12 srvsvc!SsScavengerThread+0x322 (FPO: [Non-Fpo])
        013dff70 010012a4 srvsvc!ServiceMain+0x214 (FPO: [Non-Fpo])
        013dffa4 77f65e91 svchost!ServiceStarter+0x9e (FPO: [Non-Fpo])
        013dffb8 77e64829 ADVAPI32!ScSvcctrlThreadW+0x21 (FPO: [Non-Fpo])
        013dffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85e08db0  Cid 0350.0428  Teb: 7ffa2000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            86303410  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      6266           Ticks: 109702 (0:00:28:34.093)
        Context Switch Count      11
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6842000 Current f6841c24 Base f6842000 Limit f683f000 Call 0
        Priority 11 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6841c3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6841c54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6841c98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6841d48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f6841d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6841d64)
        0165fde4 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0165fde8 74ed3a7a ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        0165ff38 74ed39d3 srvsvc!XsProcessApis+0x84 (FPO: [Non-Fpo])
        0165ffb8 77e64829 srvsvc!XsProcessApisWrapper+0x2a (FPO: [Non-Fpo])
        0165ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85d76db0  Cid 0350.0544  Teb: 7ff9e000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            85d63140  Semaphore Limit 0x7fffffff
            860db810  NotificationEvent
            85d71510  NotificationEvent
        IRP List:
            8638dcd8: (0006,0190) Flags: 00000030  Mdl: 8630ef88
            862df618: (0006,0190) Flags: 00000070  Mdl: 00000000
            86393318: (0006,0190) Flags: 00000070  Mdl: 00000000
            862f2008: (0006,0190) Flags: 00000070  Mdl: 00000000
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      97721          Ticks: 18247 (0:00:04:45.109)
        Context Switch Count      101
        UserTime                  00:00:00.000
        KernelTime                00:00:00.109
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x77f65e70)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6579000 Current f6578914 Base f6579000 Limit f6576000 Call 0
        Priority 11 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f657892c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6578944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6578978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6578bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6578d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6578d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6578d64)
        0175fe6c 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0175fe70 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0175ff18 74e01a1c kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        0175ff5c 74e03bea browser!BrWorkerThread+0xea (FPO: [Non-Fpo])
        0175ff70 010012a4 browser!ServiceMain+0x43 (FPO: [Non-Fpo])
        0175ffa4 77f65e91 svchost!ServiceStarter+0x9e (FPO: [Non-Fpo])
        0175ffb8 77e64829 ADVAPI32!ScSvcctrlThreadW+0x21 (FPO: [Non-Fpo])
        0175ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d783f0  Cid 0350.0568  Teb: 7ff9a000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d640e8  NotificationEvent
            85d640b8  NotificationEvent
            85d64e00  NotificationEvent
        IRP List:
            85d66e48: (0006,01b4) Flags: 00000000  Mdl: 00000000
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      5383           Ticks: 110585 (0:00:28:47.890)
        Context Switch Count      15
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x77f65e70)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f65e9000 Current f65e8914 Base f65e9000 Limit f65e6000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 1
        Kernel stack not resident.
        ChildEBP RetAddr
        f65e892c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f65e8944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f65e8978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f65e8bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f65e8d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f65e8d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f65e8d64)
        0186fe4c 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0186fe50 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0186fef8 77e62fbe kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        0186ff14 74d61303 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0186ff4c 74d62cc1 pchsvc!MonitorRAPolicyChange+0xe2 (FPO: [Non-Fpo])
        0186ff54 74d62ca7 pchsvc!ServiceHandler::WaitUntilStopped+0xd (FPO: [0,0,0])
        0186ff5c 74d62c7c pchsvc!ServiceHandler::Run+0x14 (FPO: [0,0,0])
        0186ff70 010012a4 pchsvc!ServiceMain+0x41 (FPO: [Non-Fpo])
        0186ffa4 77f65e91 svchost!ServiceStarter+0x9e (FPO: [Non-Fpo])
        0186ffb8 77e64829 ADVAPI32!ScSvcctrlThreadW+0x21 (FPO: [Non-Fpo])
        0186ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 860dbdb0  Cid 0350.05b4  Teb: 7ff98000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d69320  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      95811          Ticks: 20157 (0:00:05:14.953)
        Context Switch Count      47
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address 0x00002584
        LPC Server thread working on message Id 2584
        Start Address aelupsvc!AelpProcessLPCCalls (0x4c594a20)
        Stack Init f6565000 Current f6564c0c Base f6565000 Limit f6562000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6564c24 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6564c3c 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6564c80 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6564d30 8091a8d8 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f6564d4c 80883908 nt!NtReplyWaitReceivePort+0x18 (FPO: [Non-Fpo])
        f6564d4c 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6564d64)
        018effc8 7c82782b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        018effcc 4c594a76 ntdll!ZwReplyWaitReceivePort+0xc (FPO: [4,0,0])
        018efff4 00000000 aelupsvc!AelpProcessLPCCalls+0x56 (FPO: [Non-Fpo])
```

```
        THREAD 860dba00  Cid 0350.05b8  Teb: 7ff97000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d79d50  SynchronizationEvent
            860dbd80  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      95811          Ticks: 20157 (0:00:05:14.953)
        Context Switch Count      40
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Start Address aelupsvc!AelTppDispatcherThreadRoutine (0x4c5953a9)
        Stack Init f6561000 Current f6560914 Base f6561000 Limit f655e000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f656092c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6560944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6560978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6560bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6560d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6560d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6560d64)
        0192ffc8 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0192ffcc 4c5953e1 ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0192fff4 00000000 aelupsvc!AelTppDispatcherThreadRoutine+0x38 (FPO: [Non-Fpo])

        THREAD 85d63328  Cid 0350.05c0  Teb: 7ff95000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d65080  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      47615          Ticks: 68353 (0:00:17:48.015)
        Context Switch Count      8
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x77c7b0f5)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6559000 Current f6558c24 Base f6559000 Limit f6556000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 1
        Kernel stack not resident.
        ChildEBP RetAddr
        f6558c3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6558c54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6558c98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6558d48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f6558d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6558d64)
        019afe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        019afe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        019aff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        019aff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        019affac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        019affb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        019affec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d626f8  Cid 0350.05c8  Teb: 7ff9f000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            85d63140  Semaphore Limit 0x7fffffff
            860db810  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      97712          Ticks: 18256 (0:00:04:45.250)
        Context Switch Count      30
        UserTime                  00:00:00.000
        KernelTime                00:00:00.046
        Win32 Start Address msvcrt!_endthreadex (0x77bcb4bc)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f657d000 Current f657c914 Base f657d000 Limit f657a000 Call 0
        Priority 10 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f657c92c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f657c944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f657c978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f657cbf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f657cd48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f657cd48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f657cd64)
        0171fe94 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0171fe98 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0171ff40 74e01a1c kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        0171ff84 77bcb530 browser!BrWorkerThread+0xea (FPO: [Non-Fpo])
        0171ffb8 77e64829 msvcrt!_endthreadex+0xa3 (FPO: [Non-Fpo])
        0171ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85d5adb0  Cid 0350.0604  Teb: 7ff94000 Win32Thread: e2519008 WAIT: (Unknown)
UserMode Non-Alertable
            85d67548  NotificationEvent
            85d4e310  SynchronizationEvent
            85d4d200  SynchronizationEvent
            85d5cfec  NotificationEvent
        IRP List:
            85d52c88: (0006,01b4) Flags: 00000000  Mdl: 00000000
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      114964         Ticks: 1004 (0:00:00:15.687)
        Context Switch Count      93                 LargeStack
        UserTime                  00:00:00.015
        KernelTime                00:00:00.203
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x77f65e70)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f646d000 Current f646c914 Base f646d000 Limit f646a000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f646c92c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f646c944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f646c978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f646cbf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f646cd48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f646cd48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f646cd64)
        01a6fddc 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01a6fde0 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        01a6fe88 77e62fbe kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        01a6fea4 58af6839 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        01a6fef8 58af6f19 wmisvc!WaitingFunction+0xac (FPO: [Non-Fpo])
        01a6ff04 58af72d1 wmisvc!MyService::WorkerThread+0x27 (FPO: [0,0,0])
        01a6ff18 58af6cdc wmisvc!CNtService::Run+0xb2 (FPO: [Non-Fpo])
        01a6ff70 010012a4 wmisvc!RunService+0x32 (FPO: [Non-Fpo])
        01a6ffa4 77f65e91 svchost!ServiceStarter+0x9e (FPO: [Non-Fpo])
        01a6ffb8 77e64829 ADVAPI32!ScSvcctrlThreadW+0x21 (FPO: [Non-Fpo])
        01a6ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d5a7b8  Cid 0350.0608  Teb: 7ff93000 Win32Thread: e253f468 WAIT: (Unknown)
UserMode Alertable
            85de9f70  SynchronizationEvent
            85deae78  NotificationEvent
            85de9f40  SynchronizationEvent
            85d5a830  NotificationTimer
        IRP List:
            86386e70: (0006,0190) Flags: 00000030  Mdl: 00000000
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      19259          Ticks: 96709 (0:00:25:11.078)
        Context Switch Count      1240                LargeStack
        UserTime                  00:00:01.500
        KernelTime                00:00:09.578
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x77f65e70)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f64fd000 Current f64fc914 Base f64fd000 Limit f64f9000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f64fc92c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f64fc944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f64fc978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f64fcbf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f64fcd48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f64fcd48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f64fcd64)
        01aafd4c 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01aafd50 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        01aafdf8 500c707f kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        01aafe44 5019257f wuaueng!DllInstall+0xac04
        01aafe78 500bba84 wuaueng!WUAutoUpdateAtShutdown+0x20418
        01aaff1c 50001223 wuaueng!ServiceMain+0x303
        01aaff70 010012a4 wuauserv!ServiceMain+0xaf (FPO: [Non-Fpo])
        01aaffa4 77f65e91 svchost!ServiceStarter+0x9e (FPO: [Non-Fpo])
        01aaffb8 77e64829 ADVAPI32!ScSvcctrlThreadW+0x21 (FPO: [Non-Fpo])
        01aaffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d5a548  Cid 0350.060c  Teb: 7ff92000 Win32Thread: e2503008 WAIT: (Unknown)
UserMode Alertable
            86367a90  SynchronizationTimer
            85d4e3b0  NotificationEvent
            85d501c8  SynchronizationEvent
        IRP List:
            862c6328: (0006,0190) Flags: 00000030  Mdl: 00000000
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      24720          Ticks: 91248 (0:00:23:45.750)
        Context Switch Count      167                 LargeStack
        UserTime                  00:00:00.031
        KernelTime                00:00:00.500
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x77f65e70)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6af3000 Current f6af2914 Base f6af3000 Limit f6aef000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6af292c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6af2944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6af2978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6af2bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6af2d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6af2d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6af2d64)
        01aefcbc 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01aefcc0 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        01aefd68 7739bbd1 kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        01aefdc4 5fb5fc08 USER32!RealMsgWaitForMultipleObjectsEx+0x141 (FPO: [Non-Fpo])
        01aefe14 5fb653e5 qmgr!CJobManager::TaskThread+0x3c (FPO: [Non-Fpo])
        01aefe88 5fb574e7 qmgr!InitQmgr+0x14f (FPO: [Non-Fpo])
        01aeff24 5fb57915 qmgr!BITSServiceMainProc+0x32c (FPO: [Non-Fpo])
        01aeff5c 5fb5796d qmgr!BITSServiceMain+0x1e (FPO: [Non-Fpo])
        01aeff70 010012a4 qmgr!ServiceMain+0x39 (FPO: [Non-Fpo])
        01aeffa4 77f65e91 svchost!ServiceStarter+0x9e (FPO: [Non-Fpo])
        01aeffb8 77e64829 ADVAPI32!ScSvcctrlThreadW+0x21 (FPO: [Non-Fpo])
        01aeffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 860bc020  Cid 0350.0628  Teb: 7ff90000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d7cfe8  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      47860          Ticks: 68108 (0:00:17:44.187)
        Context Switch Count      13
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x77c7b0f5)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6521000 Current f6520c24 Base f6521000 Limit f651e000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6520c3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6520c54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6520c98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6520d48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f6520d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6520d64)
        01b6fe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01b6fe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        01b6ff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        01b6ff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        01b6ffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        01b6ffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        01b6ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d54980  Cid 0350.0640  Teb: 7ff8e000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d62a40  QueueObject
            85d549f8  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      109948         Ticks: 6020 (0:00:01:34.062)
        Context Switch Count      188
        UserTime                  00:00:00.000
        KernelTime                00:00:00.156
        Win32 Start Address msvcrt!_endthreadex (0x77bcb4bc)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f650d000 Current f650cc4c Base f650d000 Limit f650a000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f650cc64 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f650cc7c 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f650ccc4 808e55e2 nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f650cd48 80883908 nt!NtRemoveIoCompletion+0xdc (FPO: [Non-Fpo])
        f650cd48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f650cd64)
        01d1fec8 7c8277db ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01d1fecc 77e5bea2 ntdll!ZwRemoveIoCompletion+0xc (FPO: [5,0,0])
        01d1fef8 77958cd3 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        01d1ff74 77958f24 es!WORK_QUEUE::WorkerLoop+0x66 (FPO: [Non-Fpo])
        01d1ff84 77bcb530 es!WORK_QUEUE::ThreadLoop+0x19 (FPO: [Non-Fpo])
        01d1ffb8 77e64829 msvcrt!_endthreadex+0xa3 (FPO: [Non-Fpo])
        01d1ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85d5c2c0  Cid 0350.0650  Teb: 7ff9c000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d4d300  Semaphore Limit 0x7fffffff
            85d5c338  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      106016         Ticks: 9952 (0:00:02:35.500)
        Context Switch Count      24
        UserTime                  00:00:00.015
        KernelTime                00:00:00.015
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6545000 Current f6544c24 Base f6545000 Limit f6542000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6544c3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6544c54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6544c98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6544d48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f6544d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6544d64)
        01ecfe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01ecfe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        01ecff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        01ecff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        01ecffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        01ecffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        01ecffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 862f8538  Cid 0350.0658  Teb: 7ff8c000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85da8d38  NotificationEvent
            862fdeb0  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      6176           Ticks: 109792 (0:00:28:35.500)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address USERENV!NotificationThread (0x76929dd9)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f66a5000 Current f66a4914 Base f66a5000 Limit f66a2000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f66a492c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f66a4944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f66a4978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f66a4bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f66a4d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f66a4d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f66a4d64)
        0207fec0 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0207fec4 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0207ff6c 77e62fbe kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        0207ff88 76929e35 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0207ffb8 77e64829 USERENV!NotificationThread+0x5f (FPO: [Non-Fpo])
        0207ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85d48db0  Cid 0350.066c  Teb: 7ff8b000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            8633c808  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      53375          Ticks: 62593 (0:00:16:18.015)
        Context Switch Count      15
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address 0x00001cde
        LPC Server thread working on message Id 1cde
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f645d000 Current f645cc24 Base f645d000 Limit f645a000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f645cc3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f645cc54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f645cc98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f645cd48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f645cd48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f645cd64)
        020bfe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        020bfe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        020bff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        020bff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        020bffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        020bffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        020bffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d42660  Cid 0350.0708  Teb: 7ff7f000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            86353600  NotificationEvent
            86352640  NotificationEvent
        IRP List:
            85d54e78: (0006,0094) Flags: 00000900  Mdl: 00000000
            85d4f4b8: (0006,0094) Flags: 00000800  Mdl: 00000000
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      96775          Ticks: 19193 (0:00:04:59.890)
        Context Switch Count      25
        UserTime                  00:00:00.000
        KernelTime                00:00:00.062
        Win32 Start Address ncprov!CNCProvider::ConnectThreadProc (0x5faf3cce)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6429000 Current f6428914 Base f6429000 Limit f6426000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f642892c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6428944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6428978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6428bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6428d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6428d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6428d64)
        0441fe88 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0441fe8c 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0441ff34 5faf3c73 kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        0441ff90 5faf3cfc ncprov!CNCProvider::ConnectLoop+0x15e (FPO: [Non-Fpo])
        0441ffb8 77e64829 ncprov!CNCProvider::ConnectThreadProc+0x2e (FPO: [Non-Fpo])
        0441ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85d4e840  Cid 0350.075c  Teb: 7ff7b000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d63040  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      47744          Ticks: 68224 (0:00:17:46.000)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x77c7b0f5)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f63f9000 Current f63f8c24 Base f63f9000 Limit f63f6000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f63f8c3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f63f8c54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f63f8c98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f63f8d48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f63f8d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f63f8d64)
        044dfe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        044dfe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        044dff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        044dff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        044dffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        044dffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        044dffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 860badb0  Cid 0350.0764  Teb: 7ff7a000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            8636c320  NotificationEvent
            86312240  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      11264          Ticks: 104704 (0:00:27:16.000)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address NCObjAPI!CNamedPipeClient::ProviderReadyThreadProc (0x5fb1168d)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f63dd000 Current f63dc914 Base f63dd000 Limit f63da000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f63dc92c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f63dc944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f63dc978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f63dcbf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f63dcd48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f63dcd48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f63dcd64)
        0451fe9c 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0451fea0 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0451ff48 77e62fbe kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        0451ff64 5fb116db kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0451ffb8 77e64829 NCObjAPI!CNamedPipeClient::ProviderReadyThreadProc+0xb3 (FPO: [Non-Fpo])
        0451ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 860bbdb0  Cid 0350.0768  Teb: 7ff8a000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            864515a8  NotificationEvent
            862e67b0  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      11265          Ticks: 104703 (0:00:27:15.984)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address NCObjAPI!CNamedPipeClient::ProviderReadyThreadProc (0x5fb1168d)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6431000 Current f6430914 Base f6431000 Limit f642e000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f643092c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6430944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6430978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6430bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6430d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6430d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6430d64)
        03edfe9c 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        03edfea0 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        03edff48 77e62fbe kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        03edff64 5fb116db kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        03edffb8 77e64829 NCObjAPI!CNamedPipeClient::ProviderReadyThreadProc+0xb3 (FPO: [Non-Fpo])
        03edffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d85020  Cid 0350.05e0  Teb: 7ff86000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            865ac2a8  QueueObject
        IRP List:
            8641cd18: (0006,0094) Flags: 00000800  Mdl: 00000000
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      20395          Ticks: 95573 (0:00:24:53.328)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address mswsock!SockAsyncThread (0x71b258ab)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f63cd000 Current f63ccc4c Base f63cd000 Limit f63ca000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f63ccc64 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f63ccc7c 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f63cccc4 808e55e2 nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f63ccd48 80883908 nt!NtRemoveIoCompletion+0xdc (FPO: [Non-Fpo])
        f63ccd48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f63ccd64)
        0421ff7c 7c8277db ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0421ff80 71b25914 ntdll!ZwRemoveIoCompletion+0xc (FPO: [5,0,0])
        0421ffb8 77e64829 mswsock!SockAsyncThread+0x69 (FPO: [Non-Fpo])
        0421ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85da3db0  Cid 0350.05e8  Teb: 7ff88000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            8632a820  Semaphore Limit 0x7fffffff
            85da3e28  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      106020         Ticks: 9948 (0:00:02:35.437)
        Context Switch Count      86
        UserTime                  00:00:00.015
        KernelTime                00:00:00.046
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f621d000 Current f621cc24 Base f621d000 Limit f621a000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f621cc3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f621cc54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f621cc98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f621cd48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f621cd48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f621cd64)
        0415fe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0415fe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        0415ff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        0415ff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        0415ffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        0415ffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        0415ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d3fa30  Cid 0350.07c4  Teb: 7ffde000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            860dbd50  NotificationEvent
            85d79d20  NotificationEvent
            85d3faa8  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      111171         Ticks: 4797 (0:00:01:14.953)
        Context Switch Count      10
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address aelupsvc!AelTppWorkerThreadRoutine (0x4c59507a)
        Stack Init f63b9000 Current f63b8914 Base f63b9000 Limit f63b6000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f63b892c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f63b8944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f63b8978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f63b8bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f63b8d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f63b8d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f63b8d64)
        0064ffbc 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0064ffc0 4c5950b8 ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0064fff4 00000000 aelupsvc!AelTppWorkerThreadRoutine+0x3e (FPO: [Non-Fpo])

        THREAD 85d68db0  Cid 0350.0838  Teb: 7ffa6000 Win32Thread: e11297e0 WAIT: (Unknown)
UserMode Non-Alertable
            862c4100  SynchronizationEvent
            862ce118  SynchronizationEvent
            85d68e28  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      113045         Ticks: 2923 (0:00:00:45.671)
        Context Switch Count      8                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address wbemcomn!CTimerGenerator::SchedulerThread (0x75105293)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6b33000 Current f6b32914 Base f6b33000 Limit f6b30000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6b3292c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6b32944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6b32978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6b32bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6b32d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6b32d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6b32d64)
        0179fdb4 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0179fdb8 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0179fe60 7739bbd1 kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        0179febc 7739ce36 USER32!RealMsgWaitForMultipleObjectsEx+0x141 (FPO: [Non-Fpo])
        0179fed8 750fe734 USER32!MsgWaitForMultipleObjects+0x1f (FPO: [Non-Fpo])
        0179ff18 750fe70b wbemcomn!WbemWaitForMultipleObjects+0x20 (FPO: [Non-Fpo])
        0179ff2c 7510516e wbemcomn!WbemWaitForSingleObject+0x13 (FPO: [Non-Fpo])
        0179ff50 751052d5 wbemcomn!CInstructionQueue::WaitAndPeek+0x46 (FPO: [Non-Fpo])
        0179ffb8 77e64829 wbemcomn!CTimerGenerator::SchedulerThread+0x42 (FPO: [Non-Fpo])
        0179ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d89db0  Cid 0350.0868  Teb: 7ffa4000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d4d300  Semaphore Limit 0x7fffffff
            85d89e28  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      106017         Ticks: 9951 (0:00:02:35.484)
        Context Switch Count      22
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f63f1000 Current f63f0c24 Base f63f1000 Limit f63ee000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f63f0c3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f63f0c54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f63f0c98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f63f0d48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f63f0d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f63f0d64)
        0182fe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0182fe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        0182ff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        0182ff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        0182ffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        0182ffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        0182ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 862e3b70  Cid 0350.08a0  Teb: 7ffd8000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            863b1020  SynchronizationEvent
            862c7070  SynchronizationEvent
            862e3be8  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86433518       Image:         svchost.exe
        Wait Start TickCount      113045         Ticks: 2923 (0:00:00:45.671)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address repdrvfs!CRepository::_FlusherThread (0x7507921b)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6235000 Current f6234914 Base f6235000 Limit f6232000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f623492c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6234944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6234978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6234bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6234d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6234d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6234d64)
        0110fea0 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0110fea4 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0110ff4c 77e62fbe kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        0110ff68 75079284 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0110ffb8 77e64829 repdrvfs!CRepository::_FlusherThread+0x69 (FPO: [Non-Fpo])
        0110ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

Spoolsv process

```
PROCESS 86444d88  SessionId: 0  Cid: 03dc    Peb: 7ffdd000  ParentCid: 0198
    DirBase: 3af1a160  ObjectTable: e1539870  HandleCount: 120.
    Image: spoolsv.exe
    VadRoot 862b6f70 Vads 101 Clone 0 Private 378. Modified 1. Locked 0.
    DeviceMap e1000170
    Token                             e1979de0
    ElapsedTime                       00:39:00.593
    UserTime                          00:00:00.015
    KernelTime                        00:00:01.109
    QuotaPoolUsage[PagedPool]         42380
    QuotaPoolUsage[NonPagedPool]      4272
    Working Set Sizes (now,min,max)  (1441, 50, 345) (5764KB, 200KB, 1380KB)
    PeakWorkingSetSize                1454
    VirtualSize                       25 Mb
    PeakVirtualSize                   26 Mb
    PageFaultCount                    1588
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      765

    Setting context for this process...
.process /p /r ffffffff86444d88

    !peb
PEB at 7ffdd000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         01000000
    Ldr                       7c8877e0
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00081f18 . 000b08b8
    Ldr.InLoadOrderModuleList:           00081eb0 . 000b0900
    Ldr.InMemoryOrderModuleList:         00081eb8 . 000b0908
            Base TimeStamp                     Module
         1000000 45d6a078 Feb 17 06:28:08 2007 C:\WINDOWS\system32\spoolsv.exe
        7c800000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\ntdll.dll
        77e40000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\kernel32.dll
        77ba0000 45d70b06 Feb 17 14:02:46 2007 C:\WINDOWS\system32\msvcrt.dll
        77f50000 45d70a26 Feb 17 13:59:02 2007 C:\WINDOWS\system32\ADVAPI32.dll
        77c50000 45d70aaa Feb 17 14:01:14 2007 C:\WINDOWS\system32\RPCRT4.dll
        76f50000 45d70ac3 Feb 17 14:01:39 2007 C:\WINDOWS\system32\Secur32.dll
        77c00000 45d70a3e Feb 17 13:59:26 2007 C:\WINDOWS\system32\GDI32.dll
        77380000 45d70ac7 Feb 17 14:01:43 2007 C:\WINDOWS\system32\USER32.dll
        74060000 45d70adf Feb 17 14:02:07 2007 C:\WINDOWS\system32\SPOOLSS.DLL
        71c00000 45d70ae9 Feb 17 14:02:17 2007 C:\WINDOWS\system32\WS2_32.dll
        71bf0000 45d70aea Feb 17 14:02:18 2007 C:\WINDOWS\system32\WS2HELP.dll
        71c40000 45d70a82 Feb 17 14:00:34 2007 C:\WINDOWS\system32\NETAPI32.dll
        76cf0000 45d70a6c Feb 17 14:00:12 2007 C:\WINDOWS\system32\iphlpapi.dll
        76b70000 45d70ab5 Feb 17 14:01:25 2007 C:\WINDOWS\system32\PSAPI.DLL
        76ed0000 45d70a64 Feb 17 14:00:04 2007 C:\WINDOWS\system32\DNSAPI.dll
        76f80000 45d70a9d Feb 17 14:01:01 2007 C:\WINDOWS\system32\rasadhlp.dll
        76130000 45d70a59 Feb 17 13:59:53 2007 C:\WINDOWS\system32\localspl.dll
        77670000 45d70aa5 Feb 17 14:01:09 2007 C:\WINDOWS\system32\ole32.dll
        77d00000 45d70aa6 Feb 17 14:01:10 2007 C:\WINDOWS\system32\OLEAUT32.dll
        77b90000 45d70ac8 Feb 17 14:01:44 2007 C:\WINDOWS\system32\VERSION.dll
        76be0000 45d70ab5 Feb 17 14:01:25 2007 C:\WINDOWS\system32\sfc_os.dll
        76bb0000 45d70acf Feb 17 14:01:51 2007 C:\WINDOWS\system32\WINTRUST.dll
        761b0000 45d70a80 Feb 17 14:00:32 2007 C:\WINDOWS\system32\CRYPT32.dll
        76190000 45d70aac Feb 17 14:01:16 2007 C:\WINDOWS\system32\MSASN1.dll
        76c10000 45d70a5d Feb 17 13:59:57 2007 C:\WINDOWS\system32\imagehlp.dll
        76920000 45d70ac8 Feb 17 14:01:44 2007 C:\WINDOWS\system32\USERENV.dll
        73070000 45d70acb Feb 17 14:01:47 2007 C:\WINDOWS\system32\winspool.drv
        74020000 45d70a68 Feb 17 14:00:08 2007 C:\WINDOWS\system32\cnbjmon.dll
        74000000 45d70aa4 Feb 17 14:01:08 2007 C:\WINDOWS\system32\pjlmon.dll
```

```
        72460000 45d70ac0 Feb 17 14:01:36 2007 C:\WINDOWS\system32\tcpmon.dll
        71ff0000 45d70af4 Feb 17 14:02:28 2007 C:\WINDOWS\system32\wsnmp32.dll
        72010000 45d70abf Feb 17 14:01:35 2007 C:\WINDOWS\system32\tcpmib.dll
        71bb0000 3e8024be Mar 25 09:43:26 2003 C:\WINDOWS\system32\WSOCK32.dll
        72000000 45d70a66 Feb 17 14:00:06 2007 C:\WINDOWS\system32\mgmtapi.dll
        71f50000 45d70ad6 Feb 17 14:01:58 2007 C:\WINDOWS\system32\snmpapi.dll
        72450000 45d70ac5 Feb 17 14:01:41 2007 C:\WINDOWS\system32\usbmon.dll
        71b20000 45d70b0d Feb 17 14:02:53 2007 C:\WINDOWS\System32\mswsock.dll
        76f70000 45d70ac7 Feb 17 14:01:43 2007 C:\WINDOWS\System32\winrnr.dll
        76f10000 45d70ad5 Feb 17 14:01:57 2007 C:\WINDOWS\system32\WLDAP32.dll
        5f270000 45d70a4a Feb 17 13:59:38 2007 C:\WINDOWS\system32\hnetcfg.dll
        57b60000 45d70af2 Feb 17 14:02:26 2007 C:\WINDOWS\System32\wshqos.dll
        71ae0000 45d70af3 Feb 17 14:02:27 2007 C:\WINDOWS\system32\wshtcpip.dll
        74030000 45d70aeb Feb 17 14:02:19 2007 C:\WINDOWS\system32\win32spl.dll
        5f8c0000 3e80253c Mar 25 09:45:32 2003 C:\WINDOWS\system32\NETRAP.dll
        766f0000 45d70a9f Feb 17 14:01:03 2007 C:\WINDOWS\system32\NTDSAPI.dll
        74080000 45d70a65 Feb 17 14:00:05 2007 C:\WINDOWS\system32\inetpp.dll
        74010000 3e8024ae Mar 25 09:43:10 2003 C:\WINDOWS\system32\icmp.dll
    SubSystemData:     00000000
    ProcessHeap:       00080000
    ProcessParameters: 00020000
    WindowTitle:  'C:\WINDOWS\system32\spoolsv.exe'
    ImageFile:    'C:\WINDOWS\system32\spoolsv.exe'
    CommandLine:  'C:\WINDOWS\system32\spoolsv.exe'
    DllPath:
'C:\WINDOWS\system32;C:\WINDOWS\system32;C:\WINDOWS\system;C:\WINDOWS;.;C:\WINDOWS\system32;C:\WIND
OWS;C:\WINDOWS\System32\Wbem'
    Environment:  00010000
        ALLUSERSPROFILE=C:\Documents and Settings\All Users
        ClusterLog=C:\WINDOWS\Cluster\cluster.log
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\WINDOWS\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        NUMBER_OF_PROCESSORS=1
        OS=Windows_NT
        Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 15 Model 5 Stepping 10, AuthenticAMD
        PROCESSOR_LEVEL=15
        PROCESSOR_REVISION=050a
        ProgramFiles=C:\Program Files
        SystemDrive=C:
        SystemRoot=C:\WINDOWS
        TEMP=C:\WINDOWS\TEMP
        TMP=C:\WINDOWS\TEMP
        USERPROFILE=C:\Documents and Settings\Default User
        windir=C:\WINDOWS
```

```
        THREAD 862ce870  Cid 03dc.03e0  Teb: 7ffdf000 Win32Thread: e17f0838 WAIT: (Unknown)
UserMode Non-Alertable
            862ceb4c  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86444d88       Image:         spoolsv.exe
        Wait Start TickCount      4280           Ticks: 111688 (0:00:29:05.125)
        Context Switch Count      19                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address spoolsv!mainCRTStartup (0x0100468c)
        Start Address kernel32!BaseProcessStartThunk (0x77e617f8)
        Stack Init f6dc8000 Current f6dc7c04 Base f6dc8000 Limit f6dc4000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6dc7c1c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6dc7c34 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6dc7c78 808ed456 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6dc7ca0 808ea5ad nt!IopSynchronousServiceTail+0x180 (FPO: [Non-Fpo])
        f6dc7d38 80883908 nt!NtReadFile+0x5d5 (FPO: [Non-Fpo])
        f6dc7d38 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6dc7d64)
        0006fbcc 7c82776b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0006fbd0 77e418b2 ntdll!NtReadFile+0xc (FPO: [9,0,0])
        0006fc38 77f65edb kernel32!ReadFile+0x16c (FPO: [Non-Fpo])
        0006fc64 77f65f82 ADVAPI32!ScGetPipeInput+0x2a (FPO: [Non-Fpo])
        0006fcd8 77f51ed9 ADVAPI32!ScDispatcherLoop+0x51 (FPO: [Non-Fpo])
        0006ff3c 01004019 ADVAPI32!StartServiceCtrlDispatcherW+0xe3 (FPO: [Non-Fpo])
        0006ff44 010047a2 spoolsv!main+0xb (FPO: [2,0,0])
        0006ffc0 77e6f23b spoolsv!mainCRTStartup+0x12f (FPO: [Non-Fpo])
        0006fff0 00000000 kernel32!BaseProcessStart+0x23 (FPO: [Non-Fpo])

        THREAD 8636f798  Cid 03dc.03ec  Teb: 7ffde000 Win32Thread: e1833bd0 WAIT: (Unknown)
UserMode Non-Alertable
            8636f628  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86444d88       Image:         spoolsv.exe
        Wait Start TickCount      4286           Ticks: 111682 (0:00:29:05.031)
        Context Switch Count      25                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x77f65e70)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6f5e000 Current f6f5dc78 Base f6f5e000 Limit f6f5a000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6f5dc90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6f5dca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6f5dcec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6f5dd50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f6f5dd50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6f5dd64)
        007bff08 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        007bff0c 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        007bff7c 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        007bff90 010043a3 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        007bffa4 77f65e91 spoolsv!SPOOLER_main+0x45 (FPO: [Non-Fpo])
        007bffb8 77e64829 ADVAPI32!ScSvcctrlThreadW+0x21 (FPO: [Non-Fpo])
        007bffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 863025c8  Cid 03dc.03fc  Teb: 7ffda000 Win32Thread: e17dfb98 WAIT: (Unknown)
UserMode Non-Alertable
            86304318  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86444d88       Image:         spoolsv.exe
        Wait Start TickCount      4292           Ticks: 111676 (0:00:29:04.937)
        Context Switch Count      2                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address spoolsv!SpoolerGetSpoolMessage (0x010045b9)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f681e000 Current f681dbfc Base f681e000 Limit f681a000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 1
        Kernel stack not resident.
        ChildEBP RetAddr
        f681dc14 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f681dc2c 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f681dc70 bf81ad1f nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f681dcdc bf81ac47 win32k!GreGetSpoolMessage+0x1d0 (FPO: [Non-Fpo])
        f681dd4c 80883908 win32k!NtGdiGetSpoolMessage+0x96 (FPO: [Non-Fpo])
        f681dd4c 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f681dd64)
        0088ff78 77c0c658 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0088ffb8 77e64829 GDI32!NtGdiGetSpoolMessage+0xc
        0088ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85d423f0  Cid 03dc.0798  Teb: 7ffd9000 Win32Thread: e253e830 WAIT: (Unknown)
UserMode Non-Alertable
            863144b8  SynchronizationEvent
            862f7998  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86444d88       Image:         spoolsv.exe
        Wait Start TickCount      12056          Ticks: 103912 (0:00:27:03.625)
        Context Switch Count      82                LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.296
        Win32 Start Address spoolsv!InitializeRouter (0x01003df8)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6325000 Current f6324914 Base f6325000 Limit f6321000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f632492c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6324944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6324978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6324bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6324d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6324d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6324d64)
        008ef7c8 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        008ef7cc 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        008ef874 7739bbd1 kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        008ef8d0 7739ce36 USER32!RealMsgWaitForMultipleObjectsEx+0x141 (FPO: [Non-Fpo])
        008ef8ec 740655f5 USER32!MsgWaitForMultipleObjects+0x1f (FPO: [Non-Fpo])
        008ef938 74064b43 SPOOLSS!HandlePollNotifications+0x38 (FPO: [Non-Fpo])
        008effb8 77e64829 SPOOLSS!InitializeRouter+0x49f (FPO: [Non-Fpo])
        008effec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d8eca0  Cid 03dc.07a0  Teb: 7ffd8000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            862d5a00  SynchronizationEvent
        IRP List:
            85d5fbc8: (0006,0094) Flags: 00000000  Mdl: 00000000
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86444d88       Image:         spoolsv.exe
        Wait Start TickCount      11976          Ticks: 103992 (0:00:27:04.875)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address SPOOLSS!PnpIPAddressChangeListener (0x740652c2)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f63b1000 Current f63b0914 Base f63b1000 Limit f63ae000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f63b092c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f63b0944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f63b0978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f63b0bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f63b0d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f63b0d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f63b0d64)
        0092feac 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0092feb0 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0092ff58 77e62fbe kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        0092ff74 7406532a kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0092ffb8 77e64829 SPOOLSS!PnpIPAddressChangeListener+0x64 (FPO: [Non-Fpo])
        0092ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85d532e8  Cid 03dc.07a8  Teb: 7ffdb000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            86373f20  SynchronizationEvent
            85d53360  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86444d88       Image:         spoolsv.exe
        Wait Start TickCount      115743         Ticks: 225 (0:00:00:03.515)
        Context Switch Count      57
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address tcpmon!CDeviceStatus::StatusThread (0x72461340)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f68a2000 Current f68a1c78 Base f68a2000 Limit f689f000 Call 0
        Priority 6 BasePriority 6 PriorityDecrement 0
        ChildEBP RetAddr
        f68a1c90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f68a1ca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f68a1cec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f68a1d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f68a1d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f68a1d64)
        00cbff18 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00cbff1c 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        00cbff8c 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        00cbffa0 72461375 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        00cbffb8 77e64829 tcpmon!CDeviceStatus::StatusThread+0x2a (FPO: [Non-Fpo])
        00cbffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d7aa58  Cid 03dc.07ac  Teb: 7ffd6000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            863bb8d8  NotificationEvent
            85d7aad0  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86444d88       Image:         spoolsv.exe
        Wait Start TickCount      115934         Ticks: 34 (0:00:00:00.531)
        Context Switch Count      1616
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address msvcrt!_endthreadex (0x77bcb4bc)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f63b5000 Current f63b4c78 Base f63b5000 Limit f63b2000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f63b4c90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f63b4ca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f63b4cec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f63b4d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f63b4d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f63b4d64)
        00cffed4 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00cffed8 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        00cfff48 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        00cfff5c 71ff5bf8 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        00cfff84 77bcb530 wsnmp32!thrTimer+0x1e5 (FPO: [Non-Fpo])
        00cfffb8 77e64829 msvcrt!_endthreadex+0xa3 (FPO: [Non-Fpo])
        00cfffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 86346d38  Cid 03dc.07b0  Teb: 7ffd5000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            863bb8a8  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86444d88       Image:         spoolsv.exe
        Wait Start TickCount      12041          Ticks: 103927 (0:00:27:03.859)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address msvcrt!_endthreadex (0x77bcb4bc)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6a0f000 Current f6a0ec78 Base f6a0f000 Limit f6a0c000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6a0ec90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6a0eca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6a0ecec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6a0ed50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f6a0ed50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6a0ed64)
        00d3fed4 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00d3fed8 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        00d3ff48 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        00d3ff5c 71ff5924 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        00d3ff84 77bcb530 wsnmp32!thrNotify+0x5d (FPO: [Non-Fpo])
        00d3ffb8 77e64829 msvcrt!_endthreadex+0xa3 (FPO: [Non-Fpo])
        00d3ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d7a020  Cid 03dc.07b4  Teb: 7ffd4000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            863bb848  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86444d88       Image:         spoolsv.exe
        Wait Start TickCount      12041          Ticks: 103927 (0:00:27:03.859)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address usbmon!UpdateThread (0x724515df)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6a87000 Current f6a86c78 Base f6a87000 Limit f6a84000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 2
        Kernel stack not resident.
        ChildEBP RetAddr
        f6a86c90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6a86ca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6a86cec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6a86d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f6a86d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6a86d64)
        00d7ff08 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00d7ff0c 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        00d7ff7c 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        00d7ff90 724515fa kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        00d7ffb8 77e64829 usbmon!UpdateThread+0x1b (FPO: [Non-Fpo])
        00d7ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85d53558  Cid 03dc.07b8  Teb: 7ffaf000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            862c55e0  SynchronizationEvent
            85d535d0  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86444d88       Image:         spoolsv.exe
        Wait Start TickCount      20108          Ticks: 95860 (0:00:24:57.812)
        Context Switch Count      49
        UserTime                  00:00:00.000
        KernelTime                00:00:00.468
        Win32 Start Address localspl!ServerThread (0x7616192f)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f685e000 Current f685dc78 Base f685e000 Limit f685b000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f685dc90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f685dca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f685dcec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f685dd50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f685dd50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f685dd64)
        00ddfdf4 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00ddfdf8 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        00ddfe68 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        00ddfe7c 76161b30 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        00ddffb8 77e64829 localspl!ServerThread+0x201 (FPO: [Non-Fpo])
        00ddffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d8ea30  Cid 03dc.07bc  Teb: 7ffae000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d472f0  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86444d88       Image:         spoolsv.exe
        Wait Start TickCount      12049          Ticks: 103919 (0:00:27:03.734)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address localspl!SchedulerThread (0x761344f0)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f639d000 Current f639cc78 Base f639d000 Limit f639a000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f639cc90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f639cca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f639ccec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f639cd50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f639cd50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f639cd64)
        00e1ff0c 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00e1ff10 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        00e1ff80 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        00e1ff94 7613451a kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        00e1ffb8 77e64829 localspl!SchedulerThread+0x2c (FPO: [Non-Fpo])
        00e1ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 860809d0  Cid 03dc.07f8  Teb: 7ffad000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            86354c70  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            86444d88       Image:         spoolsv.exe
        Wait Start TickCount      46608          Ticks: 69360 (0:00:18:03.750)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.078
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6509000 Current f6508c24 Base f6509000 Limit f6506000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6508c3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6508c54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6508c98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6508d48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f6508d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6508d64)
        00e5fe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00e5fe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        00e5ff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        00e5ff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        00e5ffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        00e5ffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        00e5ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

SpntSvc process

```
PROCESS 85de8d88  SessionId: 0  Cid: 0434    Peb: 7ffdf000  ParentCid: 0198
    DirBase: 3af1a180  ObjectTable: e17ecc38  HandleCount: 116.
    Image: SpntSvc.exe
    VadRoot 85de9d08 Vads 124 Clone 0 Private 423. Modified 0. Locked 1.
    DeviceMap e1000170
    Token                             e1991338
    ElapsedTime                       00:38:59.437
    UserTime                          00:00:00.140
    KernelTime                        00:00:01.062
    QuotaPoolUsage[PagedPool]         60004
    QuotaPoolUsage[NonPagedPool]      9968
    Working Set Sizes (now,min,max)  (1322, 50, 345) (5288KB, 200KB, 1380KB)
    PeakWorkingSetSize                1337
    VirtualSize                       59 Mb
    PeakVirtualSize                   61 Mb
    PageFaultCount                    10637
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      538

    Setting context for this process...
.process /p /r ffffffff85de8d88

    !peb
PEB at 7ffdf000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00400000
    Ldr                       7c8877e0
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00141f18 . 00165bc0
    Ldr.InLoadOrderModuleList:           00141eb0 . 00165bb0
    Ldr.InMemoryOrderModuleList:         00141eb8 . 00165bb8
            Base TimeStamp                     Module
          400000 3e9b8d46 Apr 15 05:40:38 2003 C:\Program Files\Trend\SProtect\SpntSvc.exe
        7c800000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\ntdll.dll
        77e40000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\kernel32.dll
        77c50000 45d70aaa Feb 17 14:01:14 2007 C:\WINDOWS\system32\RPCRT4.dll
        77f50000 45d70a26 Feb 17 13:59:02 2007 C:\WINDOWS\system32\ADVAPI32.dll
        76f50000 45d70ac3 Feb 17 14:01:39 2007 C:\WINDOWS\system32\Secur32.dll
        71bd0000 45d70a84 Feb 17 14:00:36 2007 C:\WINDOWS\system32\MPR.dll
        77380000 45d70ac7 Feb 17 14:01:43 2007 C:\WINDOWS\system32\USER32.dll
        77c00000 45d70a3e Feb 17 13:59:26 2007 C:\WINDOWS\system32\GDI32.dll
        71c40000 45d70a82 Feb 17 14:00:34 2007 C:\WINDOWS\system32\NETAPI32.dll
        77ba0000 45d70b06 Feb 17 14:02:46 2007 C:\WINDOWS\system32\msvcrt.dll
        77b90000 45d70ac8 Feb 17 14:01:44 2007 C:\WINDOWS\system32\VERSION.dll
        601e0000 3e9b8b37 Apr 15 05:31:51 2003 C:\Program Files\Trend\SProtect\CheckEVC.dll
        10000000 3e9b8c96 Apr 15 05:37:42 2003 C:\Program
Files\Trend\SProtect\CheckSecurityPatch.dll
        65630000 3e9b8c4d Apr 15 05:36:29 2003 C:\Program Files\Trend\SProtect\StCommon.dll
          320000 3383a3cf May 22 02:39:27 1997 C:\Program Files\Trend\SProtect\GENKEY32.dll
        71bb0000 3e8024be Mar 25 09:43:26 2003 C:\WINDOWS\system32\WSOCK32.dll
        71c00000 45d70ae9 Feb 17 14:02:17 2007 C:\WINDOWS\system32\WS2_32.dll
        71bf0000 45d70aea Feb 17 14:02:18 2007 C:\WINDOWS\system32\WS2HELP.dll
        620e0000 3e9b8c45 Apr 15 05:36:21 2003 C:\Program Files\Trend\SProtect\GetRemoteVer.dll
        65240000 3e9b8b35 Apr 15 05:31:49 2003 C:\Program Files\Trend\SProtect\SpTrace.dll
        76f70000 3850984a Dec 10 06:06:02 1999 C:\Program Files\Trend\SProtect\MFC42u.DLL
        7c8d0000 45d70abb Feb 17 14:01:31 2007 C:\WINDOWS\system32\SHELL32.dll
        77da0000 45d70ac0 Feb 17 14:01:36 2007 C:\WINDOWS\system32\SHLWAPI.dll
        77420000 45d70a05 Feb 17 13:58:29 2007 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.3790.3959_x-ww_D8713E55\comctl32.dll
        63270000 3e9b8cf1 Apr 15 05:39:13 2003 C:\Program Files\Trend\SProtect\LogMaster.dll
        63150000 3e9b8cd0 Apr 15 05:38:40 2003 C:\Program Files\Trend\SProtect\LogDb.dll
        640a0000 3e9b8c91 Apr 15 05:37:37 2003 C:\Program Files\Trend\SProtect\Notification.dll
```

```
        66040000 3ae64fa1 Apr 25 05:16:33 2001 C:\Program Files\Trend\SProtect\TMNotify.dll
        762b0000 45d70a72 Feb 17 14:00:18 2007 C:\WINDOWS\system32\comdlg32.dll
        77530000 45d70a06 Feb 17 13:58:30 2007 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_5.82.3790.3959_x-ww_78FCF8D0\COMCTL32.dll
        73070000 45d70acb Feb 17 14:01:47 2007 C:\WINDOWS\system32\WINSPOOL.DRV
        61180000 3e9b8d00 Apr 15 05:39:28 2003 C:\Program Files\Trend\SProtect\Eng50.dll
         17b0000 3a34b5a8 Dec 11 11:08:24 2000 C:\Program Files\Trend\SProtect\tmeng.dll
        76520000 45d70a87 Feb 17 14:00:39 2007 C:\WINDOWS\system32\cscdll.dll
        65670000 3e9b8d34 Apr 15 05:40:20 2003 C:\Program Files\Trend\SProtect\StRpcSrv.dll
        65740000 3e9b8c7b Apr 15 05:37:15 2003 C:\Program Files\Trend\SProtect\TmRpcSrv.dll
        60640000 3e9b8d2c Apr 15 05:40:12 2003 C:\Program Files\Trend\SProtect\AgRpcCln.dll
        71b20000 45d70b0d Feb 17 14:02:53 2007 C:\WINDOWS\system32\mswsock.dll
        5f270000 45d70a4a Feb 17 13:59:38 2007 C:\WINDOWS\system32\hnetcfg.dll
        71ae0000 45d70af3 Feb 17 14:02:27 2007 C:\WINDOWS\System32\wshtcpip.dll
        76ed0000 45d70a64 Feb 17 14:00:04 2007 C:\WINDOWS\system32\DNSAPI.dll
         2740000 45d70ac7 Feb 17 14:01:43 2007 C:\WINDOWS\System32\winrnr.dll
        76f10000 45d70ad5 Feb 17 14:01:57 2007 C:\WINDOWS\system32\WLDAP32.dll
         2770000 45d70a9d Feb 17 14:01:01 2007 C:\WINDOWS\system32\rasadhlp.dll
    SubSystemData:     00000000
    ProcessHeap:       00140000
    ProcessParameters: 00020000
    WindowTitle:  'C:\Program Files\Trend\SProtect\SpntSvc.exe'
    ImageFile:    'C:\Program Files\Trend\SProtect\SpntSvc.exe'
    CommandLine:  '"C:\Program Files\Trend\SProtect\SpntSvc.exe"'
    DllPath:      'C:\Program
Files\Trend\SProtect;C:\WINDOWS\system32;C:\WINDOWS\system;C:\WINDOWS;.;C:\WINDOWS\system32;C:\WIND
OWS;C:\WINDOWS\System32\Wbem'
    Environment:  00010000
        ALLUSERSPROFILE=C:\Documents and Settings\All Users
        ClusterLog=C:\WINDOWS\Cluster\cluster.log
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\WINDOWS\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        NUMBER_OF_PROCESSORS=1
        OS=Windows_NT
        Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 15 Model 5 Stepping 10, AuthenticAMD
        PROCESSOR_LEVEL=15
        PROCESSOR_REVISION=050a
        ProgramFiles=C:\Program Files
        SystemDrive=C:
        SystemRoot=C:\WINDOWS
        TEMP=C:\WINDOWS\TEMP
        TMP=C:\WINDOWS\TEMP
        USERPROFILE=C:\Documents and Settings\Default User
        windir=C:\WINDOWS
```

```
        THREAD 85de5db0  Cid 0434.0438  Teb: 7ffde000 Win32Thread: e1984090 WAIT: (Unknown)
UserMode Non-Alertable
            864079ec  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85de8d88       Image:         SpntSvc.exe
        Wait Start TickCount      4351           Ticks: 111617 (0:00:29:04.015)
        Context Switch Count      42                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.078
        Win32 Start Address SpntSvc (0x0040580e)
        Start Address kernel32!BaseProcessStartThunk (0x77e617f8)
        Stack Init f680e000 Current f680dc04 Base f680e000 Limit f680a000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f680dc1c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f680dc34 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f680dc78 808ed456 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f680dca0 808ea5ad nt!IopSynchronousServiceTail+0x180 (FPO: [Non-Fpo])
        f680dd38 80883908 nt!NtReadFile+0x5d5 (FPO: [Non-Fpo])
        f680dd38 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f680dd64)
        0012f928 7c82776b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0012f92c 77e418b2 ntdll!NtReadFile+0xc (FPO: [9,0,0])
        0012f994 77f65edb kernel32!ReadFile+0x16c (FPO: [Non-Fpo])
        0012f9c0 77f65f82 ADVAPI32!ScGetPipeInput+0x2a (FPO: [Non-Fpo])
        0012fa34 77f51ed9 ADVAPI32!ScDispatcherLoop+0x51 (FPO: [Non-Fpo])
        0012fc98 0040193c ADVAPI32!StartServiceCtrlDispatcherW+0xe3 (FPO: [Non-Fpo])
        0012ffc0 77e6f23b SpntSvc+0x193c
        0012fff0 00000000 kernel32!BaseProcessStart+0x23 (FPO: [Non-Fpo])

        THREAD 85de4db0  Cid 0434.043c  Teb: 7ffdd000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            85dcbcc0  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85de8d88       Image:         SpntSvc.exe
        Wait Start TickCount      4346           Ticks: 111622 (0:00:29:04.093)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address msvcrt!_endthreadex (0x77bcb4bc)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f679a000 Current f6799bb0 Base f679a000 Limit f6797000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6799bc8 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6799be0 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6799c24 808b3076 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6799cfc 808b43d2 nt!NtNotifyChangeMultipleKeys+0x838 (FPO: [Non-Fpo])
        f6799d34 80883908 nt!NtNotifyChangeKey+0x2c (FPO: [Non-Fpo])
        f6799d34 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6799d64)
        00defebc 7c8272cb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00defec0 77f786bf ntdll!NtNotifyChangeKey+0xc (FPO: [10,0,0])
        00defef8 65241530 ADVAPI32!RegNotifyChangeKeyValue+0x85 (FPO: [Non-Fpo])
        00000000 00000000 SpTrace!SpTraceGetCfgW+0x3b0
```

```
        THREAD 85dafdb0  Cid 0434.0440  Teb: 7ffdc000 Win32Thread: e1983770 WAIT: (Unknown)
UserMode Non-Alertable
            85debfc0  NotificationEvent
            85dafe28  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85de8d88       Image:         SpntSvc.exe
        Wait Start TickCount      115705         Ticks: 263 (0:00:00:04.109)
        Context Switch Count      976                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.140
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x77f65e70)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f682e000 Current f682dc78 Base f682e000 Limit f682a000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f682dc90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f682dca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f682dcec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f682dd50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f682dd50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f682dd64)
        00f6fab8 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00f6fabc 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        00f6fb2c 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        00f6fb40 0040226e kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        00f6fb4c 00000000 SpntSvc+0x226e

        THREAD 85db0db0  Cid 0434.0448  Teb: 7ffda000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85daae30  NotificationEvent
            85daacf8  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85de8d88       Image:         SpntSvc.exe
        Wait Start TickCount      4362           Ticks: 111606 (0:00:29:03.843)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address msvcrt!_endthreadex (0x77bcb4bc)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f678e000 Current f678d914 Base f678e000 Limit f678b000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f678d92c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f678d944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f678d978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f678dbf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f678dd48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f678dd48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f678dd64)
        0116fe9c 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0116fea0 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0116ff48 77e62fbe kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        0116ff64 631538b4 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0116ffb8 77e64829 LogDb!DB_ModifyTheRecord+0x2174
        0116ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 862c5a70  Cid 0434.044c  Teb: 7ffd9000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            863abf28  NotificationEvent
            862c5ae8  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85de8d88       Image:         SpntSvc.exe
        Wait Start TickCount      115743         Ticks: 225 (0:00:00:03.515)
        Context Switch Count      31
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address msvcrt!_endthreadex (0x77bcb4bc)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f678a000 Current f6789c78 Base f678a000 Limit f6787000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 1
        ChildEBP RetAddr
        f6789c90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6789ca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6789cec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6789d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f6789d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6789d64)
        0126fee0 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0126fee4 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0126ff54 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        0126ff68 632716ba kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0126ff84 77bcb530 LogMaster+0x16ba
        00364b20 ffffffff msvcrt!_endthreadex+0xa3 (FPO: [Non-Fpo])
        00364b28 00000000 0xffffffff

        THREAD 85daedb0  Cid 0434.0450  Teb: 7ffd8000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            862c5948  NotificationEvent
            85daee28  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85de8d88       Image:         SpntSvc.exe
        Wait Start TickCount      115923         Ticks: 45 (0:00:00:00.703)
        Context Switch Count      32
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address TMNotify!SendEMail (0x6604b7f0)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6792000 Current f6791c78 Base f6792000 Limit f678f000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f6791c90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6791ca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6791cec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6791d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f6791d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6791d64)
        0179fee0 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0179fee4 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0179ff54 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        0179ff68 6604550e kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0179ff84 6604b84d TMNotify!DoPagerNotifyEx+0x1abe
        0179ffa0 8082c3b2 TMNotify!SendEMail+0x3b4d
        0179ff90 00000000 nt!KiDeliverApc+0x11c (FPO: [Non-Fpo])
```

```
        THREAD 85da7db0  Cid 0434.0454  Teb: 7ffd7000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85daed30  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85de8d88       Image:         SpntSvc.exe
        Wait Start TickCount      4543           Ticks: 111425 (0:00:29:01.015)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address Notification!NTF_DoSNMPNotify (0x640a7948)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6786000 Current f6785c78 Base f6786000 Limit f6783000 Call 0
        Priority 7 BasePriority 7 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6785c90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6785ca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6785cec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6785d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f6785d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6785d64)
        01cefee8 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01cefeec 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        01ceff5c 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        01ceff70 640a1692 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        01ceffb8 77e64829 Notification!EndNotifyCriticalSection+0x132
        01ceffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85ddedb0  Cid 0434.0460  Teb: 7ffd6000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85dcdd20  NotificationEvent
            85dcdd80  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85de8d88       Image:         SpntSvc.exe
        Wait Start TickCount      95808          Ticks: 20160 (0:00:05:15.000)
        Context Switch Count      165
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address Eng50!ENG_GetTaskNextPerformTime (0x6118fa60)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f677e000 Current f677d914 Base f677e000 Limit f677b000 Call 0
        Priority 16 BasePriority 10 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f677d92c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f677d944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f677d978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f677dbf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f677dd48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f677dd48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f677dd64)
        01defec4 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01defec8 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        01deff70 6118fabc kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        01deffb0 7c8277ab Eng50!ENG_GetTaskNextPerformTime+0xdcc
        01deffb8 77e64829 ntdll!NtRegisterThreadTerminatePort+0xc (FPO: [1,0,0])
        01deffe4 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 8633a5e8  Cid 0434.0464  Teb: 7ffd5000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85de9ff0  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85de8d88       Image:         SpntSvc.exe
        Wait Start TickCount      95808          Ticks: 20160 (0:00:05:15.000)
        Context Switch Count      86
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address Eng50!ENG_GetTaskNextPerformTime (0x6118f730)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f677a000 Current f6779c78 Base f677a000 Limit f6777000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6779c90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6779ca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6779cec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6779d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f6779d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6779d64)
        01eeff08 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01eeff0c 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        01eeff7c 61193f8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        01eeffa4 6118f754 Eng50!ENG_GetTaskNextPerformTime+0x529d
        00000000 00000000 Eng50!ENG_GetTaskNextPerformTime+0xa64

        THREAD 85dabdb0  Cid 0434.0468  Teb: 7ffd4000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85de9fc0  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85de8d88       Image:         SpntSvc.exe
        Wait Start TickCount      4542           Ticks: 111426 (0:00:29:01.031)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address Eng50!ENG_GetTaskNextPerformTime (0x6118f730)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6776000 Current f6775c78 Base f6776000 Limit f6773000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6775c90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6775ca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6775cec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6775d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f6775d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6775d64)
        01feff08 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01feff0c 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        01feff7c 61193f8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        01feffa4 6118f754 Eng50!ENG_GetTaskNextPerformTime+0x529d
        00000000 00000000 Eng50!ENG_GetTaskNextPerformTime+0xa64
```

```
        THREAD 85daddb0  Cid 0434.046c  Teb: 7ffaf000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85dcdd20  NotificationEvent
            85dcdd50  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85de8d88       Image:         SpntSvc.exe
        Wait Start TickCount      4542           Ticks: 111426 (0:00:29:01.031)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address Eng50!ENG_GetTaskNextPerformTime (0x6118f9f0)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6772000 Current f6771914 Base f6772000 Limit f676f000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f677192c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6771944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6771978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6771bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6771d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6771d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6771d64)
        020ee20c 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        020ee210 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        020ee2b8 6118fa24 kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        020effec 00000000 Eng50!ENG_GetTaskNextPerformTime+0xd34

        THREAD 863a0718  Cid 0434.049c  Teb: 7ffae000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            8636c458  SynchronizationEvent
            863a0790  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85de8d88       Image:         SpntSvc.exe
        Wait Start TickCount      115923         Ticks: 45 (0:00:00:00.703)
        Context Switch Count      35
        UserTime                  00:00:00.000
        KernelTime                00:00:00.062
        Win32 Start Address Eng50!ENG_GetTaskNextPerformTime (0x6118eee0)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f672e000 Current f672dc78 Base f672e000 Limit f672b000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f672dc90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f672dca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f672dcec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f672dd50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f672dd50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f672dd64)
        021efeec 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        021efef0 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        021eff60 6118f164 kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        00000000 00000000 Eng50!ENG_GetTaskNextPerformTime+0x474
```

```
        THREAD 86304710  Cid 0434.04a0  Teb: 7ffad000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            863e8198  SynchronizationEvent
            86304788  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85de8d88       Image:         SpntSvc.exe
        Wait Start TickCount      115898         Ticks: 70 (0:00:00:01.093)
        Context Switch Count      348
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address Eng50!ENG_GetOutbreakAlertInfo (0x6118a520)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f672a000 Current f6729c78 Base f672a000 Limit f6727000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f6729c90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6729ca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6729cec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6729d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f6729d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6729d64)
        022efe88 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        022efe8c 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        022efefc 6118a56b kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        022eff24 80827bbe Eng50!ENG_GetOutbreakAlertInfo+0x6ab
        022effa0 8082c3b2 nt!KiAdjustQuantumThread+0xca (FPO: [Non-Fpo])
        f6729cc4 f6729ce8 nt!KiDeliverApc+0x11c (FPO: [Non-Fpo])
        f6729cec 80930ad8 0xf6729ce8
        f6729d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f6729d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6729d64)
        022efe88 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        022efe8c 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        022efefc 6118a56b kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        022eff24 80827bbe Eng50!ENG_GetOutbreakAlertInfo+0x6ab
        022effa0 8082c3b2 nt!KiAdjustQuantumThread+0xca (FPO: [Non-Fpo])
        f6729cc4 f6729ce8 nt!KiDeliverApc+0x11c (FPO: [Non-Fpo])
        f6729cec 80930ad8 0xf6729ce8
        f6729d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f6729d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6729d64)
        022efe88 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        022efe8c 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        022efefc 6118a56b kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        022eff24 80827bbe Eng50!ENG_GetOutbreakAlertInfo+0x6ab
        022effa0 8082c3b2 nt!KiAdjustQuantumThread+0xca (FPO: [Non-Fpo])
        f6729cc4 f6729ce8 nt!KiDeliverApc+0x11c (FPO: [Non-Fpo])
        f6729cec 80930ad8 0xf6729ce8
        f6729d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f6729d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6729d64)
        022efe88 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        022efe8c 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        022efefc 6118a56b kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        022eff24 80827bbe Eng50!ENG_GetOutbreakAlertInfo+0x6ab
        022effa0 8082c3b2 nt!KiAdjustQuantumThread+0xca (FPO: [Non-Fpo])
        f6729cc4 f6729ce8 nt!KiDeliverApc+0x11c (FPO: [Non-Fpo])
        f6729cec 80930ad8 0xf6729ce8
        f6729d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
```

```
        THREAD 8636cb98  Cid 0434.04a4  Teb: 7ffac000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            8636c428  SynchronizationEvent
            8636cc10  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85de8d88       Image:         SpntSvc.exe
        Wait Start TickCount      4543           Ticks: 111425 (0:00:29:01.015)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address Eng50!ENG_DoOBA_NotifySNMP_Trap (0x6118af20)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6726000 Current f6725c78 Base f6726000 Limit f6723000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6725c90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6725ca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6725cec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6725d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f6725d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6725d64)
        023efb90 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        023efb94 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        023efc04 6118b0f7 kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        00000000 00000000 Eng50!ENG_DoOBA_NotifySNMP_Trap+0x3b7

        THREAD 863d1af0  Cid 0434.04ac  Teb: 7ffab000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            863b8420  Semaphore Limit 0x7fffffff
            863d1b68  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85de8d88       Image:         SpntSvc.exe
        Wait Start TickCount      114086         Ticks: 1882 (0:00:00:29.406)
        Context Switch Count      22
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x77c7b0f5)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6a23000 Current f6a22c24 Base f6a23000 Limit f6a20000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f6a22c3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6a22c54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6a22c98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6a22d48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f6a22d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6a22d64)
        024ffe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        024ffe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        024fff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        024fff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        024fffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        024fffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        024fffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 863d1880  Cid 0434.04b0  Teb: 7ffaa000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            8633bd38  QueueObject
            863d18f8  NotificationTimer
        IRP List:
            86445ee8: (0006,0094) Flags: 00000800  Mdl: 00000000
            85de5cf8: (0006,0094) Flags: 00000800  Mdl: 00000000
            86392678: (0006,0190) Flags: 00000000  Mdl: 85db2d90
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85de8d88       Image:         SpntSvc.exe
        Wait Start TickCount      114442         Ticks: 1526 (0:00:00:23.843)
        Context Switch Count      40
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x77c7b0f5)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6716000 Current f6715c4c Base f6716000 Limit f6713000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f6715c64 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6715c7c 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6715cc4 808e55e2 nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f6715d48 80883908 nt!NtRemoveIoCompletion+0xdc (FPO: [Non-Fpo])
        f6715d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6715d64)
        025ffeac 7c8277db ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        025ffeb0 77e5bea2 ntdll!ZwRemoveIoCompletion+0xc (FPO: [5,0,0])
        025ffedc 77c7b900 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        025fff18 77c7b703 RPCRT4!COMMON_ProcessCalls+0xa1 (FPO: [Non-Fpo])
        025fff84 77c7b9b5 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x117 (FPO: [Non-Fpo])
        025fff8c 77c8872d RPCRT4!ProcessIOEventsWrapper+0xd (FPO: [Non-Fpo])
        025fffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        025fffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        025fffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 862b2c48  Cid 0434.04b4  Teb: 7ffa9000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            8639f398  NotificationEvent
            862b2cc0  NotificationTimer
        IRP List:
            863e7e48: (0006,01b4) Flags: 00000000  Mdl: 00000000
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85de8d88       Image:         SpntSvc.exe
        Wait Start TickCount      115363         Ticks: 605 (0:00:00:09.453)
        Context Switch Count      337
        UserTime                  00:00:00.015
        KernelTime                00:00:00.359
        Win32 Start Address msvcrt!_endthreadex (0x77bcb4bc)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f66b5000 Current f66b4c78 Base f66b5000 Limit f66b2000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f66b4c90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f66b4ca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f66b4cec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f66b4d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f66b4d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f66b4d64)
        026ff810 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        026ff814 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        026ff884 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        026ff898 77c5a767 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        026ff994 77c5a9c5 RPCRT4!WS_Open+0x321 (FPO: [Non-Fpo])
        026ffac8 77c5a8e0 RPCRT4!TCPOrHTTP_Open+0x1fc (FPO: [Non-Fpo])
        026ffb00 77c67e24 RPCRT4!TCP_Open+0x5c (FPO: [Non-Fpo])
        026ffb48 77c67cf2 RPCRT4!OSF_CCONNECTION::TransOpen+0x5e (FPO: [Non-Fpo])
        026ffbac 77c67c22 RPCRT4!OSF_CCONNECTION::OpenConnectionAndBind+0xbe (FPO: [Non-Fpo])
        026ffbf0 77c67b7a RPCRT4!OSF_CCALL::BindToServer+0xfa (FPO: [Non-Fpo])
        026ffc08 77c672d3 RPCRT4!OSF_BINDING_HANDLE::InitCCallWithAssociation+0x63 (FPO: [Non-Fpo])
        026ffc84 77c671cf RPCRT4!OSF_BINDING_HANDLE::AllocateCCall+0x49d (FPO: [Non-Fpo])
        026ffcb8 77c7f201 RPCRT4!OSF_BINDING_HANDLE::NegotiateTransferSyntax+0x2e (FPO: [Non-Fpo])
        026ffcd0 77c7ed14 RPCRT4!I_RpcGetBufferWithObject+0x5b (FPO: [Non-Fpo])
        026ffce0 77c7f464 RPCRT4!I_RpcGetBuffer+0xf (FPO: [Non-Fpo])
        026ffcf0 60641ae6 RPCRT4!NdrGetBuffer+0x2e (FPO: [Non-Fpo])
        026ffe18 60641961 AgRpcCln!CAgRpcClient::IO+0x6d6
        026ffef8 77e41ed1 AgRpcCln!CAgRpcClient::IO+0x551
        026fff60 77e424ed kernel32!SleepEx+0x68 (FPO: [Non-Fpo])
        77e41ef3 b44d8dd2 kernel32!Sleep+0xf (FPO: [Non-Fpo])
        77e41efb aceb77e4 0xb44d8dd2
        77e41eff c7d87589 0xaceb77e4
        77e41f03 00000000 0xc7d87589
```

```
        THREAD 85d48300  Cid 0434.06c0  Teb: 7ffa8000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            863b8420  Semaphore Limit 0x7fffffff
            85d48378  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85de8d88       Image:         SpntSvc.exe
        Wait Start TickCount      114087         Ticks: 1881 (0:00:00:29.390)
        Context Switch Count      20
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x77c7b0f5)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6549000 Current f6548c24 Base f6549000 Limit f6546000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f6548c3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6548c54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6548c98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6548d48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f6548d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6548d64)
        0287fe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0287fe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        0287ff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        0287ff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        0287ffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        0287ffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        0287ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 863383a0  Cid 0434.06cc  Teb: 7ffa7000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            8633bd38  QueueObject
            86338418  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85de8d88       Image:         SpntSvc.exe
        Wait Start TickCount      114442         Ticks: 1526 (0:00:00:23.843)
        Context Switch Count      37
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x77c7b0f5)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f688a000 Current f6889c4c Base f688a000 Limit f6887000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f6889c64 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6889c7c 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6889cc4 808e55e2 nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f6889d48 80883908 nt!NtRemoveIoCompletion+0xdc (FPO: [Non-Fpo])
        f6889d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6889d64)
        0297feac 7c8277db ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0297feb0 77e5bea2 ntdll!ZwRemoveIoCompletion+0xc (FPO: [5,0,0])
        0297fedc 77c7b900 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        0297ff18 77c7b703 RPCRT4!COMMON_ProcessCalls+0xa1 (FPO: [Non-Fpo])
        0297ff84 77c7b9b5 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x117 (FPO: [Non-Fpo])
        0297ff8c 77c8872d RPCRT4!ProcessIOEventsWrapper+0xd (FPO: [Non-Fpo])
        0297ffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        0297ffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        0297ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

StWatchDog process

```
PROCESS 8635fb50  SessionId: 0  Cid: 04b8    Peb: 7ffde000  ParentCid: 0434
    DirBase: 3af1a1c0  ObjectTable: e17c9e98  HandleCount:  50.
    Image: StWatchDog.exe
    VadRoot 86319590 Vads 41 Clone 0 Private 77. Modified 0. Locked 1.
    DeviceMap e1000170
    Token                             e1987de0
    ElapsedTime                       00:38:54.577
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.218
    QuotaPoolUsage[PagedPool]         30148
    QuotaPoolUsage[NonPagedPool]      5984
    Working Set Sizes (now,min,max)  (482, 50, 345) (1928KB, 200KB, 1380KB)
    PeakWorkingSetSize                484
    VirtualSize                       15 Mb
    PeakVirtualSize                   16 Mb
    PageFaultCount                    478
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      94

    Setting context for this process...
.process /p /r ffffffff8635fb50

    !peb
PEB at 7ffde000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00400000
    Ldr                       7c8877e0
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00141f18 . 0014d8b8
    Ldr.InLoadOrderModuleList:           00141eb0 . 0014d8a8
    Ldr.InMemoryOrderModuleList:         00141eb8 . 0014d8b0
            Base TimeStamp                     Module
          400000 3e9b8d50 Apr 15 05:40:48 2003 C:\Program Files\Trend\SProtect\StWatchDog.exe
        7c800000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\ntdll.dll
        77e40000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\kernel32.dll
        65740000 3e9b8c7b Apr 15 05:37:15 2003 C:\Program Files\Trend\SProtect\TmRpcSrv.dll
        77f50000 45d70a26 Feb 17 13:59:02 2007 C:\WINDOWS\system32\ADVAPI32.dll
        77c50000 45d70aaa Feb 17 14:01:14 2007 C:\WINDOWS\system32\RPCRT4.dll
        76f50000 45d70ac3 Feb 17 14:01:39 2007 C:\WINDOWS\system32\Secur32.dll
        77ba0000 45d70b06 Feb 17 14:02:46 2007 C:\WINDOWS\system32\MSVCRT.dll
        71b20000 45d70b0d Feb 17 14:02:53 2007 C:\WINDOWS\system32\mswsock.dll
        71c00000 45d70ae9 Feb 17 14:02:17 2007 C:\WINDOWS\system32\WS2_32.dll
        71bf0000 45d70aea Feb 17 14:02:18 2007 C:\WINDOWS\system32\WS2HELP.dll
        5f270000 45d70a4a Feb 17 13:59:38 2007 C:\WINDOWS\system32\hnetcfg.dll
        77c00000 45d70a3e Feb 17 13:59:26 2007 C:\WINDOWS\system32\GDI32.dll
        77380000 45d70ac7 Feb 17 14:01:43 2007 C:\WINDOWS\system32\USER32.dll
        71ae0000 45d70af3 Feb 17 14:02:27 2007 C:\WINDOWS\System32\wshtcpip.dll
    SubSystemData:     00000000
    ProcessHeap:       00140000
    ProcessParameters: 00020000
    WindowTitle:  'C:\Program Files\Trend\SProtect\StWatchDog.exe'
    ImageFile:    'C:\Program Files\Trend\SProtect\StWatchDog.exe'
    CommandLine:  'StWatchDog'
    DllPath:      'C:\Program
Files\Trend\SProtect;C:\WINDOWS\system32;C:\WINDOWS\system;C:\WINDOWS;.;C:\WINDOWS\system32;C:\WIND
OWS;C:\WINDOWS\System32\Wbem'
    Environment:  00010000
        ALLUSERSPROFILE=C:\Documents and Settings\All Users
        ClusterLog=C:\WINDOWS\Cluster\cluster.log
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\WINDOWS\system32\cmd.exe
```

```
        FP_NO_HOST_CHECK=NO
        NUMBER_OF_PROCESSORS=1
        OS=Windows_NT
        Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 15 Model 5 Stepping 10, AuthenticAMD
        PROCESSOR_LEVEL=15
        PROCESSOR_REVISION=050a
        ProgramFiles=C:\Program Files
        SystemDrive=C:
        SystemRoot=C:\WINDOWS
        TEMP=C:\WINDOWS\TEMP
        TMP=C:\WINDOWS\TEMP
        USERPROFILE=C:\Documents and Settings\Default User
        windir=C:\WINDOWS


        THREAD 86319870  Cid 04b8.04bc  Teb: 7ffdd000 Win32Thread: e17ecd18 WAIT: (Unknown)
UserMode Non-Alertable
            85debfc0  NotificationEvent
        IRP List:
            85dc4cd0: (0006,0094) Flags: 00000800  Mdl: 00000000
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            8635fb50       Image:         StWatchDog.exe
        Wait Start TickCount      4651           Ticks: 111317 (0:00:28:59.328)
        Context Switch Count      15                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.046
        Win32 Start Address StWatchDog (0x0040114a)
        Start Address kernel32!BaseProcessStartThunk (0x77e617f8)
        Stack Init f6dd8000 Current f6dd7c78 Base f6dd8000 Limit f6dd4000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6dd7c90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6dd7ca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6dd7cec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6dd7d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f6dd7d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6dd7d64)
        0012fe8c 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0012fe90 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0012ff00 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        0012ff14 00401105 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0012ffc0 77e6f23b StWatchDog+0x1105
        0012fff0 00000000 kernel32!BaseProcessStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 862b29d8  Cid 04b8.04c4  Teb: 7ffdb000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            862cf568  QueueObject
        IRP List:
            85d8f2f0: (0006,0094) Flags: 00000800  Mdl: 00000000
            86391b40: (0006,0190) Flags: 00000000  Mdl: 85de3f00
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            8635fb50       Image:         StWatchDog.exe
        Wait Start TickCount      10418          Ticks: 105550 (0:00:27:29.218)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x77c7b0f5)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f66a9000 Current f66a8c4c Base f66a9000 Limit f66a6000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f66a8c64 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f66a8c7c 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f66a8cc4 808e55e2 nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f66a8d48 80883908 nt!NtRemoveIoCompletion+0xdc (FPO: [Non-Fpo])
        f66a8d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f66a8d64)
        0060feac 7c8277db ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0060feb0 77e5bea2 ntdll!ZwRemoveIoCompletion+0xc (FPO: [5,0,0])
        0060fedc 77c7b900 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        0060ff18 77c7b703 RPCRT4!COMMON_ProcessCalls+0xa1 (FPO: [Non-Fpo])
        0060ff84 77c7b9b5 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x117 (FPO: [Non-Fpo])
        0060ff8c 77c8872d RPCRT4!ProcessIOEventsWrapper+0xd (FPO: [Non-Fpo])
        0060ffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        0060ffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        0060ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85d59db0  Cid 04b8.06c4  Teb: 7ffda000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            8634b5b8  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            8635fb50       Image:         StWatchDog.exe
        Wait Start TickCount      35383          Ticks: 80585 (0:00:20:59.140)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.046
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x77c7b0f5)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f68be000 Current f68bdc24 Base f68be000 Limit f68bb000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f68bdc3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f68bdc54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f68bdc98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f68bdd48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f68bdd48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f68bdd64)
        00befe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00befe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        00beff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        00beff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        00beffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        00beffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        00beffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

StOPP process

```
PROCESS 85d7fa08  SessionId: 0  Cid: 04d4    Peb: 7ffde000  ParentCid: 0434
    DirBase: 3af1a1e0  ObjectTable: e17f2050  HandleCount:  43.
    Image: StOPP.exe
    VadRoot 86319138 Vads 57 Clone 0 Private 148. Modified 0. Locked 0.
    DeviceMap e1000170
    Token                             e15427f0
    ElapsedTime                       00:38:49.390
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.125
    QuotaPoolUsage[PagedPool]         31644
    QuotaPoolUsage[NonPagedPool]      2440
    Working Set Sizes (now,min,max)  (607, 50, 345) (2428KB, 200KB, 1380KB)
    PeakWorkingSetSize                607
    VirtualSize                       22 Mb
    PeakVirtualSize                   22 Mb
    PageFaultCount                    600
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      177

    Setting context for this process...
.process /p /r ffffffff85d7fa08

    !peb
PEB at 7ffde000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00400000
    Ldr                       7c8877e0
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00141f18 . 00143460
    Ldr.InLoadOrderModuleList:           00141eb0 . 00143dc8
    Ldr.InMemoryOrderModuleList:         00141eb8 . 00143dd0
            Base TimeStamp                     Module
          400000 3e9b8d4b Apr 15 05:40:43 2003 C:\Program Files\Trend\SProtect\StOPP.exe
        7c800000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\ntdll.dll
        77e40000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\kernel32.dll
        77380000 45d70ac7 Feb 17 14:01:43 2007 C:\WINDOWS\system32\USER32.dll
        77c00000 45d70a3e Feb 17 13:59:26 2007 C:\WINDOWS\system32\GDI32.dll
        77f50000 45d70a26 Feb 17 13:59:02 2007 C:\WINDOWS\system32\ADVAPI32.dll
        77c50000 45d70aaa Feb 17 14:01:14 2007 C:\WINDOWS\system32\RPCRT4.dll
        76f50000 45d70ac3 Feb 17 14:01:39 2007 C:\WINDOWS\system32\Secur32.dll
        71c40000 45d70a82 Feb 17 14:00:34 2007 C:\WINDOWS\system32\NETAPI32.dll
        77ba0000 45d70b06 Feb 17 14:02:46 2007 C:\WINDOWS\system32\msvcrt.dll
        63270000 3e9b8cf1 Apr 15 05:39:13 2003 C:\Program Files\Trend\SProtect\LogMaster.dll
        63150000 3e9b8cd0 Apr 15 05:38:40 2003 C:\Program Files\Trend\SProtect\LogDb.dll
        65630000 3e9b8c4d Apr 15 05:36:29 2003 C:\Program Files\Trend\SProtect\StCommon.dll
        71bd0000 45d70a84 Feb 17 14:00:36 2007 C:\WINDOWS\system32\MPR.dll
        10000000 3383a3cf May 22 02:39:27 1997 C:\Program Files\Trend\SProtect\GENKEY32.dll
        77b90000 45d70ac8 Feb 17 14:01:44 2007 C:\WINDOWS\system32\VERSION.dll
        71bb0000 3e8024be Mar 25 09:43:26 2003 C:\WINDOWS\system32\WSOCK32.dll
        71c00000 45d70ae9 Feb 17 14:02:17 2007 C:\WINDOWS\system32\WS2_32.dll
        71bf0000 45d70aea Feb 17 14:02:18 2007 C:\WINDOWS\system32\WS2HELP.dll
        620e0000 3e9b8c45 Apr 15 05:36:21 2003 C:\Program Files\Trend\SProtect\GetRemoteVer.dll
        601e0000 3e9b8b37 Apr 15 05:31:51 2003 C:\Program Files\Trend\SProtect\CheckEVC.dll
        65240000 3e9b8b35 Apr 15 05:31:49 2003 C:\Program Files\Trend\SProtect\SpTrace.dll
        76f70000 3850984a Dec 10 06:06:02 1999 C:\Program Files\Trend\SProtect\MFC42u.DLL
    SubSystemData:     00000000
    ProcessHeap:       00140000
    ProcessParameters: 00020000
    WindowTitle:  'C:\Program Files\Trend\SProtect\StOPP.exe'
    ImageFile:    'C:\Program Files\Trend\SProtect\StOPP.exe'
    CommandLine:  'StOPP'
```

```
    DllPath:      'C:\Program
Files\Trend\SProtect;C:\WINDOWS\system32;C:\WINDOWS\system;C:\WINDOWS;.;C:\WINDOWS\system32;C:\WIND
OWS;C:\WINDOWS\System32\Wbem'
    Environment:  00010000
        ALLUSERSPROFILE=C:\Documents and Settings\All Users
        ClusterLog=C:\WINDOWS\Cluster\cluster.log
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\WINDOWS\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        NUMBER_OF_PROCESSORS=1
        OS=Windows_NT
        Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 15 Model 5 Stepping 10, AuthenticAMD
        PROCESSOR_LEVEL=15
        PROCESSOR_REVISION=050a
        ProgramFiles=C:\Program Files
        SystemDrive=C:
        SystemRoot=C:\WINDOWS
        TEMP=C:\WINDOWS\TEMP
        TMP=C:\WINDOWS\TEMP
        USERPROFILE=C:\Documents and Settings\Default User
        windir=C:\WINDOWS


        THREAD 85d83c80  Cid 04d4.04d8  Teb: 7ffdd000 Win32Thread: e198a418 WAIT: (Unknown)
UserMode Non-Alertable
            85d82428  SynchronizationEvent
            85debfc0  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85d7fa08       Image:         StOPP.exe
        Wait Start TickCount      5011           Ticks: 110957 (0:00:28:53.703)
        Context Switch Count      17                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.125
        Win32 Start Address StOPP (0x00401fcc)
        Start Address kernel32!BaseProcessStartThunk (0x77e617f8)
        Stack Init f662d000 Current f662c914 Base f662d000 Limit f6629000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f662c92c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f662c944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f662c978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f662cbf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f662cd48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f662cd48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f662cd64)
        0012f8e4 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0012f8e8 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0012f990 77e62fbe kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        0012f9ac 0040141c kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0012fa5c 7c829f59 StOPP+0x141c
        0012fb64 7c834345 ntdll!RtlFreeHeap+0x70f (FPO: [Non-Fpo])
        0012fcb8 7c827c3b ntdll!LdrpRunInitializeRoutines+0x403 (FPO: [Non-Fpo])
        0012fd14 7c826d9b ntdll!NtTestAlert+0xc (FPO: [0,0,0])
        0012fd18 7c8284da ntdll!NtContinue+0xc (FPO: [2,0,0])
        0012fdb4 7c829fb5 ntdll!KiUserApcDispatcher+0x3a
        0012fdc0 7c829f3d ntdll!RtlpFreeToHeapLookaside+0x22 (FPO: [Non-Fpo])
        0012fea0 00830000 ntdll!RtlFreeHeap+0x20e (FPO: [Non-Fpo])
        0012febc 7c82a0fc 0x830000
        001300d0 00000000 ntdll!RtlAllocateHeap+0xee7 (FPO: [Non-Fpo])
```

```
        THREAD 85d82c20  Cid 04d4.04dc  Teb: 7ffdc000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            85d7d3e8  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85d7fa08       Image:         StOPP.exe
        Wait Start TickCount      5011           Ticks: 110957 (0:00:28:53.703)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address msvcrt!_endthreadex (0x77bcb4bc)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f669d000 Current f669cbb0 Base f669d000 Limit f669a000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f669cbc8 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f669cbe0 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f669cc24 808b3076 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f669ccfc 808b43d2 nt!NtNotifyChangeMultipleKeys+0x838 (FPO: [Non-Fpo])
        f669cd34 80883908 nt!NtNotifyChangeKey+0x2c (FPO: [Non-Fpo])
        f669cd34 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f669cd64)
        00d8febc 7c8272cb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00d8fec0 77f786bf ntdll!NtNotifyChangeKey+0xc (FPO: [10,0,0])
        00d8fef8 65241530 ADVAPI32!RegNotifyChangeKeyValue+0x85 (FPO: [Non-Fpo])
        00000000 00000000 SpTrace!SpTraceGetCfgW+0x3b0

        THREAD 85d82520  Cid 04d4.04e0  Teb: 7ffdb000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d83990  NotificationEvent
            85d82bb0  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85d7fa08       Image:         StOPP.exe
        Wait Start TickCount      5011           Ticks: 110957 (0:00:28:53.703)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address msvcrt!_endthreadex (0x77bcb4bc)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f65dd000 Current f65dc914 Base f65dd000 Limit f65da000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f65dc92c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f65dc944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f65dc978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f65dcbf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f65dcd48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f65dcd48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f65dcd64)
        00f0fe9c 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00f0fea0 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00f0ff48 77e62fbe kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        00f0ff64 631538b4 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        00f0ffb8 77e64829 LogDb!DB_ModifyTheRecord+0x2174
        00f0ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d7d4f0  Cid 04d4.04e4  Teb: 7ffda000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d82458  NotificationEvent
            85d7d568  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85d7fa08       Image:         StOPP.exe
        Wait Start TickCount      112547         Ticks: 3421 (0:00:00:53.453)
        Context Switch Count      29
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address msvcrt!_endthreadex (0x77bcb4bc)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f65d9000 Current f65d8c78 Base f65d9000 Limit f65d6000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f65d8c90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f65d8ca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f65d8cec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f65d8d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f65d8d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f65d8d64)
        0101fee0 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0101fee4 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0101ff54 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        0101ff68 632716ba kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0101ff84 77bcb530 LogMaster+0x16ba
        00833e48 ffffffff msvcrt!_endthreadex+0xa3 (FPO: [Non-Fpo])
        00000000 00000000 0xffffffff
```

Msdtc process

```
PROCESS 85d7f770  SessionId: 0  Cid: 04ec    Peb: 7ffda000  ParentCid: 0198
    DirBase: 3af1a200  ObjectTable: e17e7e10  HandleCount: 161.
    Image: msdtc.exe
    VadRoot 85d7e888 Vads 140 Clone 0 Private 320. Modified 108. Locked 0.
    DeviceMap e16b5d18
    Token                             e197fc50
    ElapsedTime                       00:38:48.827
    UserTime                          00:00:00.031
    KernelTime                        00:00:00.375
    QuotaPoolUsage[PagedPool]         39340
    QuotaPoolUsage[NonPagedPool]      6216
    Working Set Sizes (now,min,max)  (1065, 50, 345) (4260KB, 200KB, 1380KB)
    PeakWorkingSetSize                1069
    VirtualSize                       24 Mb
    PeakVirtualSize                   25 Mb
    PageFaultCount                    1208
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      451

    Setting context for this process...
.process /p /r ffffffff85d7f770

    !peb
PEB at 7ffda000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00400000
    Ldr                       7c8877e0
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00081f18 . 000a85b8
    Ldr.InLoadOrderModuleList:           00081eb0 . 000a85a8
    Ldr.InMemoryOrderModuleList:         00081eb8 . 000a85b0
            Base TimeStamp                     Module
          400000 45d696b3 Feb 17 05:46:27 2007 C:\WINDOWS\system32\msdtc.exe
         7c800000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\ntdll.dll
         77e40000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\kernel32.dll
         77670000 45d70aa5 Feb 17 14:01:09 2007 C:\WINDOWS\system32\ole32.dll
         77ba0000 45d70b06 Feb 17 14:02:46 2007 C:\WINDOWS\system32\msvcrt.dll
         77c00000 45d70a3e Feb 17 13:59:26 2007 C:\WINDOWS\system32\GDI32.dll
         77380000 45d70ac7 Feb 17 14:01:43 2007 C:\WINDOWS\system32\USER32.dll
         77f50000 45d70a26 Feb 17 13:59:02 2007 C:\WINDOWS\system32\ADVAPI32.dll
         77c50000 45d70aaa Feb 17 14:01:14 2007 C:\WINDOWS\system32\RPCRT4.dll
         76f50000 45d70ac3 Feb 17 14:01:39 2007 C:\WINDOWS\system32\Secur32.dll
         48a60000 45d70ae0 Feb 17 14:02:08 2007 C:\WINDOWS\system32\MSDTCTM.dll
         76ed0000 45d70a64 Feb 17 14:00:04 2007 C:\WINDOWS\system32\DNSAPI.dll
         71c00000 45d70ae9 Feb 17 14:02:17 2007 C:\WINDOWS\system32\WS2_32.dll
         71bf0000 45d70aea Feb 17 14:02:18 2007 C:\WINDOWS\system32\WS2HELP.dll
           260000 45d6a071 Feb 17 06:28:01 2007 C:\WINDOWS\system32\msvcp60.dll
         61150000 45d70ac7 Feb 17 14:01:43 2007 C:\WINDOWS\system32\MSDTCPRX.dll
         77d00000 45d70aa6 Feb 17 14:01:10 2007 C:\WINDOWS\system32\OLEAUT32.dll
         71c40000 45d70a82 Feb 17 14:00:34 2007 C:\WINDOWS\system32\NETAPI32.dll
         74f40000 45d70b12 Feb 17 14:02:58 2007 C:\WINDOWS\system32\MTXCLU.DLL
         77b90000 45d70ac8 Feb 17 14:01:44 2007 C:\WINDOWS\system32\VERSION.dll
         71bb0000 3e8024be Mar 25 09:43:26 2003 C:\WINDOWS\system32\WSOCK32.dll
         611d0000 45d70ac6 Feb 17 14:01:42 2007 C:\WINDOWS\system32\MSDTCLOG.dll
         57b10000 45d70ad7 Feb 17 14:01:59 2007 C:\WINDOWS\system32\XOLEHLP.dll
         71b20000 45d70b0d Feb 17 14:02:53 2007 C:\WINDOWS\system32\MSWSOCK.dll
         76aa0000 45d70af0 Feb 17 14:02:24 2007 C:\WINDOWS\system32\WINMM.dll
         74de0000 45d70a43 Feb 17 13:59:31 2007 C:\WINDOWS\system32\CLUSAPI.DLL
         74ef0000 45d70aa1 Feb 17 14:01:05 2007 C:\WINDOWS\system32\RESUTILS.DLL
         76920000 45d70ac8 Feb 17 14:01:44 2007 C:\WINDOWS\system32\USERENV.dll
         77010000 45d70a76 Feb 17 14:00:22 2007 C:\WINDOWS\system32\COMRES.DLL
         76a40000 45d70b16 Feb 17 14:03:02 2007 C:\WINDOWS\system32\MTxOCI.Dll
```

```
        77e00000 45d70aab Feb 17 14:01:15 2007 C:\WINDOWS\system32\NTMARTA.DLL
        76f10000 45d70ad5 Feb 17 14:01:57 2007 C:\WINDOWS\system32\WLDAP32.dll
        7e020000 45d70aa8 Feb 17 14:01:12 2007 C:\WINDOWS\system32\SAMLIB.dll
        777b0000 45d70a3b Feb 17 13:59:23 2007 C:\WINDOWS\system32\CLBCatQ.DLL
    SubSystemData:     00000000
    ProcessHeap:       00080000
    ProcessParameters: 00020000
    WindowTitle:  'C:\WINDOWS\system32\msdtc.exe'
    ImageFile:    'C:\WINDOWS\system32\msdtc.exe'
    CommandLine:  'C:\WINDOWS\system32\msdtc.exe'
    DllPath:
'C:\WINDOWS\system32;C:\WINDOWS\system32;C:\WINDOWS\system;C:\WINDOWS;.;C:\WINDOWS\system32;C:\WIND
OWS;C:\WINDOWS\System32\Wbem'
    Environment:  00010000
        ALLUSERSPROFILE=C:\Documents and Settings\All Users
        ClusterLog=C:\WINDOWS\Cluster\cluster.log
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\WINDOWS\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        NUMBER_OF_PROCESSORS=1
        OS=Windows_NT
        Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 15 Model 5 Stepping 10, AuthenticAMD
        PROCESSOR_LEVEL=15
        PROCESSOR_REVISION=050a
        ProgramFiles=C:\Program Files
        SystemDrive=C:
        SystemRoot=C:\WINDOWS
        TEMP=C:\DOCUME~1\NETWOR~1\LOCALS~1\Temp
        TMP=C:\DOCUME~1\NETWOR~1\LOCALS~1\Temp
        USERDOMAIN=NT AUTHORITY
        USERNAME=NETWORK SERVICE
        USERPROFILE=C:\Documents and Settings\NetworkService
        windir=C:\WINDOWS


        THREAD 85d834b8  Cid 04ec.04f0  Teb: 7ffdf000 Win32Thread: e1953b28 WAIT: (Unknown)
UserMode Non-Alertable
            85d7db84  NotificationEvent
        Not impersonating
        DeviceMap                 e16b5d18
        Owning Process            85d7f770       Image:         msdtc.exe
        Wait Start TickCount      5195           Ticks: 110773 (0:00:28:50.828)
        Context Switch Count      64                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.156
        Win32 Start Address msdtc!wWinMainCRTStartup (0x004012aa)
        Start Address kernel32!BaseProcessStartThunk (0x77e617f8)
        Stack Init f67be000 Current f67bdc04 Base f67be000 Limit f67ba000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f67bdc1c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f67bdc34 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f67bdc78 808ed456 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f67bdca0 808ea5ad nt!IopSynchronousServiceTail+0x180 (FPO: [Non-Fpo])
        f67bdd38 80883908 nt!NtReadFile+0x5d5 (FPO: [Non-Fpo])
        f67bdd38 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f67bdd64)
        0006fab4 7c82776b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0006fab8 77e418b2 ntdll!NtReadFile+0xc (FPO: [9,0,0])
        0006fb20 77f65edb kernel32!ReadFile+0x16c (FPO: [Non-Fpo])
        0006fb4c 77f65f82 ADVAPI32!ScGetPipeInput+0x2a (FPO: [Non-Fpo])
        0006fbc0 77f51ed9 ADVAPI32!ScDispatcherLoop+0x51 (FPO: [Non-Fpo])
        0006fe24 48a9df52 ADVAPI32!StartServiceCtrlDispatcherW+0xe3 (FPO: [Non-Fpo])
        0006fe60 48a9dea6 MSDTCTM!CNtService::Start+0x35 (FPO: [Non-Fpo])
        0006fef0 0040127e MSDTCTM!DtcMainExt+0x778 (FPO: [Non-Fpo])
        0006ff1c 00401447 msdtc!wWinMain+0xbc (FPO: [Non-Fpo])
```

```
        0006ffc0 77e6f23b msdtc!wWinMainCRTStartup+0x19d (FPO: [Non-Fpo])
        0006fff0 00000000 kernel32!BaseProcessStart+0x23 (FPO: [Non-Fpo])

        THREAD 85d828a0  Cid 04ec.04f8  Teb: 7ffdd000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d8adb0  Thread
        Not impersonating
        DeviceMap                 e16b5d18
        Owning Process            85d7f770       Image:         msdtc.exe
        Wait Start TickCount      5297           Ticks: 110671 (0:00:28:49.234)
        Context Switch Count      71
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x77f65e70)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f65c1000 Current f65c0c78 Base f65c1000 Limit f65be000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f65c0c90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f65c0ca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f65c0cec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f65c0d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f65c0d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f65c0d64)
        007dfecc 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        007dfed0 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        007dff40 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        007dff54 48a916e2 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        007dffa4 77f65e91 MSDTCTM!Main+0x197 (FPO: [Non-Fpo])
        007dffb8 77e64829 ADVAPI32!ScSvcctrlThreadW+0x21 (FPO: [Non-Fpo])
        007dffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85d8adb0  Cid 04ec.04fc  Teb: 7ffdc000 Win32Thread: e154fea8 WAIT: (Unknown)
UserMode Non-Alertable
            86376a88  SynchronizationEvent
        Not impersonating
        DeviceMap                 e16b5d18
        Owning Process            85d7f770       Image:         msdtc.exe
        Wait Start TickCount      5362           Ticks: 110606 (0:00:28:48.218)
        Context Switch Count      238                 LargeStack
        UserTime                  00:00:00.015
        KernelTime                00:00:00.125
        Win32 Start Address MSDTCTM!DTCDummy (0x48a9cc7d)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f667d000 Current f667cbc4 Base f667d000 Limit f6679000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f667cbdc 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f667cbf4 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f667cc38 bf89b1c3 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f667cc94 bf89b986 win32k!xxxSleepThread+0x1be (FPO: [Non-Fpo])
        f667ccec bf89da22 win32k!xxxRealInternalGetMessage+0x46a (FPO: [Non-Fpo])
        f667cd4c 80883908 win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        f667cd4c 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f667cd64)
        0081ff08 7739c811 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0081ff30 48a9cf3b USER32!NtUserGetMessage+0xc
        0081ffa4 48a9cc92 MSDTCTM!DtcMain+0x5ac (FPO: [Non-Fpo])
        0081ffb8 77e64829 MSDTCTM!DTCDummy+0x15 (FPO: [Non-Fpo])
        0081ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d8ab40  Cid 04ec.0504  Teb: 7ffdb000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85da6e00  SynchronizationEvent
            85da6e30  SynchronizationEvent
        Not impersonating
        DeviceMap                 e16b5d18
        Owning Process            85d7f770       Image:         msdtc.exe
        Wait Start TickCount      5266           Ticks: 110702 (0:00:28:49.718)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address MSDTCTM!ThreadProc (0x48a9d8bb)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f65b1000 Current f65b0914 Base f65b1000 Limit f65ae000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f65b092c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f65b0944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f65b0978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f65b0bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f65b0d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f65b0d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f65b0d64)
        0085fbb8 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0085fbbc 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0085fc64 77e62fbe kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        0085fc80 48a9d97b kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0085ffb8 77e64829 MSDTCTM!ThreadProc+0x126 (FPO: [Non-Fpo])
        0085ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85d75020  Cid 04ec.0508  Teb: 7ffd9000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d781f0  NotificationEvent
        Not impersonating
        DeviceMap                 e16b5d18
        Owning Process            85d7f770       Image:         msdtc.exe
        Wait Start TickCount      8913           Ticks: 107055 (0:00:27:52.734)
        Context Switch Count      507
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address MSDTCPRX!CConnectionManager::TimerProc (0x6115ae8b)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f65ad000 Current f65acc78 Base f65ad000 Limit f65aa000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f65acc90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f65acca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f65accec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f65acd50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f65acd50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f65acd64)
        0089feec 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0089fef0 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0089ff60 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        0089ff74 6115359a kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        0089ffb0 6115aea2 MSDTCPRX!CConnectionManager::TimerProcForGuardedUser+0x131 (FPO: [Non-
Fpo])
        0089ffb8 77e64829 MSDTCPRX!CConnectionManager::TimerProc+0x1e (FPO: [Non-Fpo])
        0089ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d75b40  Cid 04ec.0510  Teb: 7ffd7000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            86354dd0  NotificationEvent
        Not impersonating
        DeviceMap                 e16b5d18
        Owning Process            85d7f770       Image:         msdtc.exe
        Wait Start TickCount      5268           Ticks: 110700 (0:00:28:49.687)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address MSDTCPRX!CConnectionManager::TimerProc (0x6115ae8b)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f65a5000 Current f65a4c78 Base f65a5000 Limit f65a2000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f65a4c90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f65a4ca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f65a4cec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f65a4d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f65a4d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f65a4d64)
        009afeec 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        009afef0 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        009aff60 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        009aff74 6115af47 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        009affb0 6115aeab MSDTCPRX!CConnectionManager::TimerProcForNonGuardedUser+0xb3 (FPO: [Non-
Fpo])
        009affb8 77e64829 MSDTCPRX!CConnectionManager::TimerProc+0x1e (FPO: [Non-Fpo])
        009affec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85d79860  Cid 04ec.0514  Teb: 7ffd6000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            862ce788  NotificationEvent
        Not impersonating
        DeviceMap                 e16b5d18
        Owning Process            85d7f770       Image:         msdtc.exe
        Wait Start TickCount      5588           Ticks: 110380 (0:00:28:44.687)
        Context Switch Count      15
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address MSDTCTM!UIServerThread (0x48a912a5)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f65a1000 Current f65a0c78 Base f65a1000 Limit f659e000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f65a0c90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f65a0ca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f65a0cec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f65a0d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f65a0d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f65a0d64)
        00a7fecc 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00a7fed0 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        00a7ff40 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        00a7ff54 48a914df kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        00a7ffb8 77e64829 MSDTCTM!UIServerThread+0x424 (FPO: [Non-Fpo])
        00a7ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d758d0  Cid 04ec.0518  Teb: 7ffd5000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            865ea450  NotificationEvent
        Not impersonating
        DeviceMap                 e16b5d18
        Owning Process            85d7f770       Image:         msdtc.exe
        Wait Start TickCount      5271           Ticks: 110697 (0:00:28:49.640)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address MSDTCPRX!CConnectionManager::TimerProc (0x6115ae8b)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6722000 Current f6721c78 Base f6722000 Limit f671f000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6721c90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6721ca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6721cec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6721d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f6721d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6721d64)
        00adfeec 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00adfef0 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        00adff60 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        00adff74 6115359a kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        00adffb0 6115aea2 MSDTCPRX!CConnectionManager::TimerProcForGuardedUser+0x131 (FPO: [Non-
Fpo])
        00adffb8 77e64829 MSDTCPRX!CConnectionManager::TimerProc+0x1e (FPO: [Non-Fpo])
        00adffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85d78b40  Cid 04ec.051c  Teb: 7ffd4000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            86454e30  NotificationEvent
        Not impersonating
        DeviceMap                 e16b5d18
        Owning Process            85d7f770       Image:         msdtc.exe
        Wait Start TickCount      5274           Ticks: 110694 (0:00:28:49.593)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address MSDTCPRX!CConnectionManager::TimerProc (0x6115ae8b)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f671e000 Current f671dc78 Base f671e000 Limit f671b000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f671dc90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f671dca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f671dcec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f671dd50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f671dd50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f671dd64)
        00bcfeec 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00bcfef0 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        00bcff60 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        00bcff74 6115af47 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        00bcffb0 6115aeab MSDTCPRX!CConnectionManager::TimerProcForNonGuardedUser+0xb3 (FPO: [Non-
Fpo])
        00bcffb8 77e64829 MSDTCPRX!CConnectionManager::TimerProc+0x1e (FPO: [Non-Fpo])
        00bcffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d88590  Cid 04ec.0520  Teb: 7ffaf000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            86390c60  SynchronizationEvent
            86390c30  SynchronizationEvent
            86390c00  SynchronizationEvent
            85dead38  SynchronizationEvent
        Not impersonating
        DeviceMap                 e16b5d18
        Owning Process            85d7f770       Image:         msdtc.exe
        Wait Start TickCount      6341           Ticks: 109627 (0:00:28:32.921)
        Context Switch Count      1016
        UserTime                  00:00:00.015
        KernelTime                00:00:00.000
        Win32 Start Address MSDTCLOG!_FlushThread (0x611d84fd)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f659d000 Current f659c914 Base f659d000 Limit f659a000 Call 0
        Priority 9 BasePriority 9 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f659c92c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f659c944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f659c978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f659cbf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f659cd48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f659cd48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f659cd64)
        00dbf69c 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00dbf6a0 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00dbf748 77e62fbe kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        00dbf764 611d85ce kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        00dbffb8 77e64829 MSDTCLOG!_FlushThread+0xd1 (FPO: [Non-Fpo])
        00dbffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85d76020  Cid 04ec.0524  Teb: 7ffae000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            85d76098  NotificationTimer
        Not impersonating
        DeviceMap                 e16b5d18
        Owning Process            85d7f770       Image:         msdtc.exe
        Wait Start TickCount      5281           Ticks: 110687 (0:00:28:49.484)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!RtlpTimerThread (0x7c83d3dd)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6599000 Current f6598c98 Base f6599000 Limit f6596000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6598cb0 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6598cc8 80827e1e nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6598d0c 8098c418 nt!KeDelayExecutionThread+0x254 (FPO: [Non-Fpo])
        f6598d54 80883908 nt!NtDelayExecution+0x84 (FPO: [Non-Fpo])
        f6598d54 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6598d64)
        00e1ff9c 7c826f4b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00e1ffa0 7c83d424 ntdll!NtDelayExecution+0xc (FPO: [2,0,0])
        00e1ffb8 77e64829 ntdll!RtlpTimerThread+0x47 (FPO: [Non-Fpo])
        00e1ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d81db0  Cid 04ec.0528  Teb: 7ffad000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            8642c190  SynchronizationEvent
            8642c160  NotificationEvent
            8641f648  SynchronizationEvent
        Not impersonating
        DeviceMap                 e16b5d18
        Owning Process            85d7f770       Image:         msdtc.exe
        Wait Start TickCount      5281           Ticks: 110687 (0:00:28:49.484)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address MSDTCTM!CTaskManager::ThreadRoutine (0x48af5021)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6595000 Current f6594914 Base f6595000 Limit f6592000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f659492c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6594944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6594978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6594bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6594d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6594d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6594d64)
        00e5feb4 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00e5feb8 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00e5ff60 48af5075 kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        00e5ffb8 77e64829 MSDTCTM!CTaskManager::ThreadRoutine+0x54 (FPO: [Non-Fpo])
        00e5ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85d81b40  Cid 04ec.052c  Teb: 7ffac000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            8642c190  SynchronizationEvent
            8642c160  NotificationEvent
            8643b238  SynchronizationEvent
        Not impersonating
        DeviceMap                 e16b5d18
        Owning Process            85d7f770       Image:         msdtc.exe
        Wait Start TickCount      5281           Ticks: 110687 (0:00:28:49.484)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address MSDTCTM!CTaskManager::ThreadRoutine (0x48af5021)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6591000 Current f6590914 Base f6591000 Limit f658e000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f659092c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6590944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6590978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6590bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6590d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6590d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6590d64)
        00e9feb4 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00e9feb8 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00e9ff60 48af5075 kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        00e9ffb8 77e64829 MSDTCTM!CTaskManager::ThreadRoutine+0x54 (FPO: [Non-Fpo])
        00e9ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d75660  Cid 04ec.0530  Teb: 7ffab000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            8642c190  SynchronizationEvent
            8642c160  NotificationEvent
            85d81b10  SynchronizationEvent
        Not impersonating
        DeviceMap                 e16b5d18
        Owning Process            85d7f770       Image:         msdtc.exe
        Wait Start TickCount      5281           Ticks: 110687 (0:00:28:49.484)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address MSDTCTM!CTaskManager::ThreadRoutine (0x48af5021)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f658d000 Current f658c914 Base f658d000 Limit f658a000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f658c92c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f658c944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f658c978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f658cbf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f658cd48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f658cd48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f658cd64)
        00edfeb4 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00edfeb8 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00edff60 48af5075 kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        00edffb8 77e64829 MSDTCTM!CTaskManager::ThreadRoutine+0x54 (FPO: [Non-Fpo])
        00edffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85d753f0  Cid 04ec.0534  Teb: 7ffaa000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            8642c130  SynchronizationEvent
            8644e370  NotificationEvent
        Not impersonating
        DeviceMap                 e16b5d18
        Owning Process            85d7f770       Image:         msdtc.exe
        Wait Start TickCount      5281           Ticks: 110687 (0:00:28:49.484)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address MSDTCTM!CTaskManager::SerialThreadRoutine (0x48af4437)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6589000 Current f6588914 Base f6589000 Limit f6586000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f658892c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6588944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6588978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6588bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6588d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6588d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6588d64)
        00f1feec 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00f1fef0 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00f1ff98 48af4454 kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        00f1ffb8 77e64829 MSDTCTM!CTaskManager::SerialThreadRoutine+0x1d (FPO: [Non-Fpo])
        00f1ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d79410  Cid 04ec.053c  Teb: 7ffa8000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            8644e340  SynchronizationEvent
            8644e310  NotificationEvent
        Not impersonating
        DeviceMap                 e16b5d18
        Owning Process            85d7f770       Image:         msdtc.exe
        Wait Start TickCount      5281           Ticks: 110687 (0:00:28:49.484)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address MSDTCTM!CTaskManager::ValidateThreadRoutine (0x48af44b0)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6581000 Current f6580914 Base f6581000 Limit f657e000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f658092c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6580944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6580978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6580bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6580d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6580d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6580d64)
        00f9feec 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00f9fef0 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00f9ff98 48af44cd kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        00f9ffb8 77e64829 MSDTCTM!CTaskManager::ValidateThreadRoutine+0x1d (FPO: [Non-Fpo])
        00f9ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85d76660  Cid 04ec.0558  Teb: 7ffa7000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85deeed8  SynchronizationEvent
        Not impersonating
        DeviceMap                 e16b5d18
        Owning Process            85d7f770       Image:         msdtc.exe
        Wait Start TickCount      5301           Ticks: 110667 (0:00:28:49.171)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address MSDTCTM!DCPromoThreadFunction (0x48a9cf58)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6695000 Current f6694c78 Base f6695000 Limit f6692000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6694c90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6694ca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6694cec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6694d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f6694d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6694d64)
        00feff1c 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00feff20 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        00feff90 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        00feffa4 48a9cfa8 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        00feffb8 77e64829 MSDTCTM!DCPromoThreadFunction+0x9a (FPO: [1,0,0])
        00feffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])


        THREAD 860e7660  Cid 04ec.0748  Teb: 7ffa9000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            86323f98  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 e16b5d18
        Owning Process            85d7f770       Image:         msdtc.exe
        Wait Start TickCount      35995          Ticks: 79973 (0:00:20:49.578)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x77c7b0f5)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
```

```
Stack Init f63fd000 Current f63fcc24 Base f63fd000 Limit f63fa000 Call 0
Priority 8 BasePriority 8 PriorityDecrement 0
Kernel stack not resident.
ChildEBP RetAddr
f63fcc3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
f63fcc54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
f63fcc98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
f63fcd48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
f63fcd48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f63fcd64)
00f5fe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
00f5fe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
00f5ff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
00f5ff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
00f5ffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
00f5ffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
00f5ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

Svchost process (WinErr)

```
PROCESS 85d71020  SessionId: 0  Cid: 0550    Peb: 7ffdd000  ParentCid: 0198
    DirBase: 3af1a220  ObjectTable: e183d140  HandleCount:  68.
    Image: svchost.exe
    VadRoot 85d712e8 Vads 43 Clone 0 Private 90. Modified 0. Locked 0.
    DeviceMap e1000170
    Token                             e1935c50
    ElapsedTime                       00:38:44.374
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.218
    QuotaPoolUsage[PagedPool]         33836
    QuotaPoolUsage[NonPagedPool]      2032
    Working Set Sizes (now,min,max)  (513, 50, 345) (2052KB, 200KB, 1380KB)
    PeakWorkingSetSize                515
    VirtualSize                       16 Mb
    PeakVirtualSize                   16 Mb
    PageFaultCount                    511
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      122

    Setting context for this process...
.process /p /r ffffffff85d71020

    !peb
PEB at 7ffdd000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         01000000
    Ldr                       7c8877e0
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00081f18 . 0008e518
    Ldr.InLoadOrderModuleList:           00081eb0 . 0008e6a0
    Ldr.InMemoryOrderModuleList:         00081eb8 . 0008e6a8
            Base TimeStamp                     Module
         1000000 45d6a03c Feb 17 06:27:08 2007 C:\WINDOWS\System32\svchost.exe
        7c800000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\ntdll.dll
        77e40000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\kernel32.dll
        77f50000 45d70a26 Feb 17 13:59:02 2007 C:\WINDOWS\system32\ADVAPI32.dll
        77c50000 45d70aaa Feb 17 14:01:14 2007 C:\WINDOWS\system32\RPCRT4.dll
        76f50000 45d70ac3 Feb 17 14:01:39 2007 C:\WINDOWS\system32\Secur32.dll
        77e00000 45d70aab Feb 17 14:01:15 2007 C:\WINDOWS\System32\NTMARTA.DLL
        77ba0000 45d70b06 Feb 17 14:02:46 2007 C:\WINDOWS\system32\msvcrt.dll
        77380000 45d70ac7 Feb 17 14:01:43 2007 C:\WINDOWS\system32\USER32.dll
        77c00000 45d70a3e Feb 17 13:59:26 2007 C:\WINDOWS\system32\GDI32.dll
        76f10000 45d70ad5 Feb 17 14:01:57 2007 C:\WINDOWS\system32\WLDAP32.dll
        7e020000 45d70aa8 Feb 17 14:01:12 2007 C:\WINDOWS\System32\SAMLIB.dll
        77670000 45d70aa5 Feb 17 14:01:09 2007 C:\WINDOWS\system32\ole32.dll
          650000 45d69418 Feb 17 05:35:20 2007 C:\WINDOWS\System32\xpsp2res.dll
        74da0000 45d70a3a Feb 17 13:59:22 2007 c:\windows\system32\ersvc.dll
        76920000 45d70ac8 Feb 17 14:01:44 2007 c:\windows\system32\USERENV.dll
        771f0000 45d70ace Feb 17 14:01:50 2007 c:\windows\system32\WINSTA.dll
        71c40000 45d70a82 Feb 17 14:00:34 2007 C:\WINDOWS\system32\NETAPI32.dll
    SubSystemData:     00000000
    ProcessHeap:       00080000
    ProcessParameters: 00020000
    WindowTitle:  'C:\WINDOWS\System32\svchost.exe'
    ImageFile:    'C:\WINDOWS\System32\svchost.exe'
    CommandLine:  'C:\WINDOWS\System32\svchost.exe -k WinErr'
    DllPath:
'C:\WINDOWS\System32;C:\WINDOWS\system32;C:\WINDOWS\system;C:\WINDOWS;.;C:\WINDOWS\system32;C:\WIND
OWS;C:\WINDOWS\System32\Wbem'
    Environment:  00010000
        ALLUSERSPROFILE=C:\Documents and Settings\All Users
        ClusterLog=C:\WINDOWS\Cluster\cluster.log
```

```
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\WINDOWS\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        NUMBER_OF_PROCESSORS=1
        OS=Windows_NT
        Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 15 Model 5 Stepping 10, AuthenticAMD
        PROCESSOR_LEVEL=15
        PROCESSOR_REVISION=050a
        ProgramFiles=C:\Program Files
        SystemDrive=C:
        SystemRoot=C:\WINDOWS
        TEMP=C:\WINDOWS\TEMP
        TMP=C:\WINDOWS\TEMP
        USERPROFILE=C:\Documents and Settings\Default User
        windir=C:\WINDOWS


        THREAD 85d72db0  Cid 0550.0554  Teb: 7ffdf000 Win32Thread: e1556cc0 WAIT: (Unknown)
UserMode Non-Alertable
            85d71624  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85d71020       Image:         svchost.exe
        Wait Start TickCount      5308           Ticks: 110660 (0:00:28:49.062)
        Context Switch Count      37                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.093
        Win32 Start Address svchost!wmainCRTStartup (0x010020b9)
        Start Address kernel32!BaseProcessStartThunk (0x77e617f8)
        Stack Init f666d000 Current f666cc04 Base f666d000 Limit f6669000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f666cc1c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f666cc34 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f666cc78 808ed456 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f666cca0 808ea5ad nt!IopSynchronousServiceTail+0x180 (FPO: [Non-Fpo])
        f666cd38 80883908 nt!NtReadFile+0x5d5 (FPO: [Non-Fpo])
        f666cd38 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f666cd64)
        0006fc40 7c82776b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0006fc44 77e418b2 ntdll!NtReadFile+0xc (FPO: [9,0,0])
        0006fcac 77f65edb kernel32!ReadFile+0x16c (FPO: [Non-Fpo])
        0006fcd8 77f65f82 ADVAPI32!ScGetPipeInput+0x2a (FPO: [Non-Fpo])
        0006fd4c 77f51ed9 ADVAPI32!ScDispatcherLoop+0x51 (FPO: [Non-Fpo])
        0006ffb0 0100213d ADVAPI32!StartServiceCtrlDispatcherW+0xe3 (FPO: [Non-Fpo])
        0006ffc0 77e6f23b svchost!_wmainCRTStartup+0x7f (FPO: [0,0,2])
        0006fff0 00000000 kernel32!BaseProcessStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 85d788d0  Cid 0550.0560  Teb: 7ffdc000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d6c060  NotificationEvent
            85d6c3e0  SynchronizationEvent
            85d6c510  SynchronizationEvent
        IRP List:
            85d7e480: (0006,0094) Flags: 00000800  Mdl: 00000000
            862b52f8: (0006,0094) Flags: 00000800  Mdl: 00000000
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85d71020       Image:         svchost.exe
        Wait Start TickCount      5320           Ticks: 110648 (0:00:28:48.875)
        Context Switch Count      15
        UserTime                  00:00:00.000
        KernelTime                00:00:00.093
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x77f65e70)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f65bd000 Current f65bc914 Base f65bd000 Limit f65ba000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f65bc92c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f65bc944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f65bc978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f65bcbf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f65bcd48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f65bcd48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f65bcd64)
        0095fdc0 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0095fdc4 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0095fe6c 77e62fbe kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        0095fe88 74da385b kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0095ff04 74da4031 ersvc!ProcessRequests+0x98 (FPO: [Non-Fpo])
        0095ff70 010012a4 ersvc!ServiceMain+0xdf (FPO: [Non-Fpo])
        0095ffa4 77f65e91 svchost!ServiceStarter+0x9e (FPO: [Non-Fpo])
        0095ffb8 77e64829 ADVAPI32!ScSvcctrlThreadW+0x21 (FPO: [Non-Fpo])
        0095ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

Mdm process

```
PROCESS 85d6ed88  SessionId: 0  Cid: 056c    Peb: 7ffd5000  ParentCid: 0198
    DirBase: 3af1a240  ObjectTable: e17e2cf0  HandleCount:  80.
    Image: mdm.exe
    VadRoot 85d79ba8 Vads 53 Clone 0 Private 132. Modified 0. Locked 0.
    DeviceMap e1000170
    Token                             e1552b10
    ElapsedTime                       00:38:44.249
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.312
    QuotaPoolUsage[PagedPool]         60044
    QuotaPoolUsage[NonPagedPool]      2448
    Working Set Sizes (now,min,max)  (750, 50, 345) (3000KB, 200KB, 1380KB)
    PeakWorkingSetSize                753
    VirtualSize                       32 Mb
    PeakVirtualSize                   34 Mb
    PageFaultCount                    805
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      194

    Setting context for this process...
.process /p /r ffffffff85d6ed88

    !peb
PEB at 7ffd5000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00400000
    Ldr                       7c8877e0
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00141f18 . 0014f9b8
    Ldr.InLoadOrderModuleList:           00141eb0 . 001500c0
    Ldr.InMemoryOrderModuleList:         00141eb8 . 001500c8
            Base TimeStamp                     Module
          400000 3a96365f Feb 23 10:07:27 2001 C:\Program Files\Common Files\Microsoft
Shared\VS7Debug\mdm.exe
        7c800000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\ntdll.dll
        77e40000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\kernel32.dll
        77670000 45d70aa5 Feb 17 14:01:09 2007 C:\WINDOWS\system32\ole32.dll
        77ba0000 45d70b06 Feb 17 14:02:46 2007 C:\WINDOWS\system32\msvcrt.dll
        77c00000 45d70a3e Feb 17 13:59:26 2007 C:\WINDOWS\system32\GDI32.dll
        77380000 45d70ac7 Feb 17 14:01:43 2007 C:\WINDOWS\system32\USER32.dll
        77f50000 45d70a26 Feb 17 13:59:02 2007 C:\WINDOWS\system32\ADVAPI32.dll
        77c50000 45d70aaa Feb 17 14:01:14 2007 C:\WINDOWS\system32\RPCRT4.dll
        76f50000 45d70ac3 Feb 17 14:01:39 2007 C:\WINDOWS\system32\Secur32.dll
        77d00000 45d70aa6 Feb 17 14:01:10 2007 C:\WINDOWS\system32\OLEAUT32.dll
        77b90000 45d70ac8 Feb 17 14:01:44 2007 C:\WINDOWS\system32\VERSION.dll
        7c8d0000 45d70abb Feb 17 14:01:31 2007 C:\WINDOWS\system32\SHELL32.dll
        77da0000 45d70ac0 Feb 17 14:01:36 2007 C:\WINDOWS\system32\SHLWAPI.dll
        77420000 45d70a05 Feb 17 13:58:29 2007 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.3790.3959_x-ww_D8713E55\comctl32.dll
        76b70000 45d70ab5 Feb 17 14:01:25 2007 C:\WINDOWS\system32\psapi.dll
          d30000 45d69418 Feb 17 05:35:20 2007 C:\WINDOWS\system32\xpsp2res.dll
        777b0000 45d70a3b Feb 17 13:59:23 2007 C:\WINDOWS\system32\CLBCatQ.DLL
        77010000 45d70a76 Feb 17 14:00:22 2007 C:\WINDOWS\system32\COMRes.dll
    SubSystemData:     00000000
    ProcessHeap:       00140000
    ProcessParameters: 00020000
    WindowTitle:  'C:\Program Files\Common Files\Microsoft Shared\VS7Debug\mdm.exe'
    ImageFile:    'C:\Program Files\Common Files\Microsoft Shared\VS7Debug\mdm.exe'
    CommandLine:  '"C:\Program Files\Common Files\Microsoft Shared\VS7Debug\mdm.exe"'
    DllPath:      'C:\Program Files\Common Files\Microsoft
Shared\VS7Debug;C:\WINDOWS\system32;C:\WINDOWS\system;C:\WINDOWS;.;C:\WINDOWS\system32;C:\WINDOWS;C
:\WINDOWS\System32\Wbem'
```

```
    Environment:  00010000
        ALLUSERSPROFILE=C:\Documents and Settings\All Users
        ClusterLog=C:\WINDOWS\Cluster\cluster.log
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\WINDOWS\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        NUMBER_OF_PROCESSORS=1
        OS=Windows_NT
        Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 15 Model 5 Stepping 10, AuthenticAMD
        PROCESSOR_LEVEL=15
        PROCESSOR_REVISION=050a
        ProgramFiles=C:\Program Files
        SystemDrive=C:
        SystemRoot=C:\WINDOWS
        TEMP=C:\WINDOWS\TEMP
        TMP=C:\WINDOWS\TEMP
        USERPROFILE=C:\Documents and Settings\Default User
        windir=C:\WINDOWS


        THREAD 85d6e758  Cid 056c.0570  Teb: 7ffdf000 Win32Thread: e194e8a0 WAIT: (Unknown)
UserMode Non-Alertable
            85d8c3ec  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85d6ed88       Image:         mdm.exe
        Wait Start TickCount      5324           Ticks: 110644 (0:00:28:48.812)
        Context Switch Count      31                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.046
        Win32 Start Address mdm (0x0042a443)
        Start Address kernel32!BaseProcessStartThunk (0x77e617f8)
        Stack Init f664d000 Current f664cc04 Base f664d000 Limit f6649000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f664cc1c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f664cc34 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f664cc78 808ed456 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f664cca0 808ea5ad nt!IopSynchronousServiceTail+0x180 (FPO: [Non-Fpo])
        f664cd38 80883908 nt!NtReadFile+0x5d5 (FPO: [Non-Fpo])
        f664cd38 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f664cd64)
        0012fae8 7c82776b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0012faec 77e418b2 ntdll!NtReadFile+0xc (FPO: [9,0,0])
        0012fb54 77f65edb kernel32!ReadFile+0x16c (FPO: [Non-Fpo])
        0012fb80 77f65f82 ADVAPI32!ScGetPipeInput+0x2a (FPO: [Non-Fpo])
        0012fbf4 77fb75af ADVAPI32!ScDispatcherLoop+0x51 (FPO: [Non-Fpo])
        0012fe38 0041259b ADVAPI32!StartServiceCtrlDispatcherA+0x93 (FPO: [Non-Fpo])
        0012fe58 00412774 mdm+0x1259b
        0012fea4 0042a5c1 mdm+0x12774
        0012ffc0 77e6f23b mdm+0x2a5c1
        0012fff0 00000000 kernel32!BaseProcessStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 85d6eb18  Cid 056c.0578  Teb: 7ffdd000 Win32Thread: e24f98e0 WAIT: (Unknown)
UserMode Non-Alertable
            85d6b0c8  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85d6ed88       Image:         mdm.exe
        Wait Start TickCount      115907         Ticks: 61 (0:00:00:00.953)
        Context Switch Count      1790                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.093
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x77f65e70)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f660d000 Current f660cbc4 Base f660d000 Limit f6609000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f660cbdc 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f660cbf4 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f660cc38 bf89b1c3 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f660cc94 bf89b986 win32k!xxxSleepThread+0x1be (FPO: [Non-Fpo])
        f660ccec bf89da22 win32k!xxxRealInternalGetMessage+0x46a (FPO: [Non-Fpo])
        f660cd4c 80883908 win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        f660cd4c 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f660cd64)
        00c2fed0 7739c811 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00c2fef8 0041246d USER32!NtUserGetMessage+0xc
        00c2ff98 00412553 mdm+0x1246d
        00c2ffb8 77e64829 mdm+0x12553
        00c2ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85d6a4f0  Cid 056c.058c  Teb: 7ffdc000 Win32Thread: e17f5450 WAIT: (Unknown)
UserMode Non-Alertable
            85d6b0f8  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85d6ed88       Image:         mdm.exe
        Wait Start TickCount      115843         Ticks: 125 (0:00:00:01.953)
        Context Switch Count      883                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.109
        Win32 Start Address mdm (0x0040851f)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f661d000 Current f661cbc4 Base f661d000 Limit f6619000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f661cbdc 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f661cbf4 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f661cc38 bf89b1c3 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f661cc94 bf89b986 win32k!xxxSleepThread+0x1be (FPO: [Non-Fpo])
        f661ccec bf89da22 win32k!xxxRealInternalGetMessage+0x46a (FPO: [Non-Fpo])
        f661cd4c 80883908 win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        f661cd4c 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f661cd64)
        00d2ff14 7739c811 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00d2ff3c 004084ce USER32!NtUserGetMessage+0xc
        00d2ffb4 00408528 mdm+0x84ce
        00d2ffec 00000000 mdm+0x8528
```

```
        THREAD 85d675e8  Cid 056c.05a0  Teb: 7ffdb000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d72a20  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85d6ed88       Image:         mdm.exe
        Wait Start TickCount      59668          Ticks: 56300 (0:00:14:39.687)
        Context Switch Count      12
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address 0x00001da3
        LPC Server thread working on message Id 1da3
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f65e1000 Current f65e0c24 Base f65e1000 Limit f65de000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f65e0c3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f65e0c54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f65e0c98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f65e0d48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f65e0d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f65e0d64)
        010ffe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        010ffe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        010fff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        010fff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        010fffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        010fffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        010fffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

Svchost process (regsvc)

```
PROCESS 85d6b5f0  SessionId: 0  Cid: 0584    Peb: 7ffd4000  ParentCid: 0198
    DirBase: 3af1a260  ObjectTable: e16e4840  HandleCount:  39.
    Image: svchost.exe
    VadRoot 85d6e370 Vads 27 Clone 0 Private 50. Modified 0. Locked 0.
    DeviceMap e159ad18
    Token                             e154ede8
    ElapsedTime                       00:38:43.984
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.156
    QuotaPoolUsage[PagedPool]         15796
    QuotaPoolUsage[NonPagedPool]      1312
    Working Set Sizes (now,min,max)  (324, 50, 345) (1296KB, 200KB, 1380KB)
    PeakWorkingSetSize                325
    VirtualSize                       7 Mb
    PeakVirtualSize                   7 Mb
    PageFaultCount                    326
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      67

    Setting context for this process...
.process /p /r ffffffff85d6b5f0

    !peb
PEB at 7ffd4000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         01000000
    Ldr                       7c8877e0
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00081f18 . 00086650
    Ldr.InLoadOrderModuleList:           00081eb0 . 000866e0
    Ldr.InMemoryOrderModuleList:         00081eb8 . 000866e8
            Base TimeStamp                     Module
         1000000 45d6a03c Feb 17 06:27:08 2007 C:\WINDOWS\system32\svchost.exe
        7c800000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\ntdll.dll
        77e40000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\kernel32.dll
        77f50000 45d70a26 Feb 17 13:59:02 2007 C:\WINDOWS\system32\ADVAPI32.dll
        77c50000 45d70aaa Feb 17 14:01:14 2007 C:\WINDOWS\system32\RPCRT4.dll
        76f50000 45d70ac3 Feb 17 14:01:39 2007 C:\WINDOWS\system32\Secur32.dll
        74a20000 45d70ab2 Feb 17 14:01:22 2007 c:\windows\system32\regsvc.dll
        77ba0000 45d70b06 Feb 17 14:02:46 2007 C:\WINDOWS\system32\msvcrt.dll
    SubSystemData:     00000000
    ProcessHeap:       00080000
    ProcessParameters: 00020000
    WindowTitle:  'C:\WINDOWS\system32\svchost.exe'
    ImageFile:    'C:\WINDOWS\system32\svchost.exe'
    CommandLine:  'C:\WINDOWS\system32\svchost.exe -k regsvc'
    DllPath:
'C:\WINDOWS\system32;C:\WINDOWS\system32;C:\WINDOWS\system;C:\WINDOWS;.;C:\WINDOWS\system32;C:\WIND
OWS;C:\WINDOWS\System32\Wbem'
    Environment:  00010000
        ALLUSERSPROFILE=C:\Documents and Settings\All Users
        ClusterLog=C:\WINDOWS\Cluster\cluster.log
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\WINDOWS\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        NUMBER_OF_PROCESSORS=1
        OS=Windows_NT
        Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 15 Model 5 Stepping 10, AuthenticAMD
```

```
        PROCESSOR_LEVEL=15
        PROCESSOR_REVISION=050a
        ProgramFiles=C:\Program Files
        SystemDrive=C:
        SystemRoot=C:\WINDOWS
        TEMP=C:\DOCUME~1\LOCALS~1\LOCALS~1\Temp
        TMP=C:\DOCUME~1\LOCALS~1\LOCALS~1\Temp
        USERDOMAIN=NT AUTHORITY
        USERNAME=LOCAL SERVICE
        USERPROFILE=C:\Documents and Settings\LocalService
        windir=C:\WINDOWS


        THREAD 85d69db0  Cid 0584.0588  Teb: 7ffdf000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d6afac  NotificationEvent
        Not impersonating
        DeviceMap                 e159ad18
        Owning Process            85d6b5f0       Image:         svchost.exe
        Wait Start TickCount      5341           Ticks: 110627 (0:00:28:48.546)
        Context Switch Count      23
        UserTime                  00:00:00.000
        KernelTime                00:00:00.109
        Win32 Start Address svchost!wmainCRTStartup (0x010020b9)
        Start Address kernel32!BaseProcessStartThunk (0x77e617f8)
        Stack Init f65c9000 Current f65c8c04 Base f65c9000 Limit f65c6000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f65c8c1c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f65c8c34 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f65c8c78 808ed456 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f65c8ca0 808ea5ad nt!IopSynchronousServiceTail+0x180 (FPO: [Non-Fpo])
        f65c8d38 80883908 nt!NtReadFile+0x5d5 (FPO: [Non-Fpo])
        f65c8d38 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f65c8d64)
        0006fc40 7c82776b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0006fc44 77e418b2 ntdll!NtReadFile+0xc (FPO: [9,0,0])
        0006fcac 77f65edb kernel32!ReadFile+0x16c (FPO: [Non-Fpo])
        0006fcd8 77f65f82 ADVAPI32!ScGetPipeInput+0x2a (FPO: [Non-Fpo])
        0006fd4c 77f51ed9 ADVAPI32!ScDispatcherLoop+0x51 (FPO: [Non-Fpo])
        0006ffb0 0100213d ADVAPI32!StartServiceCtrlDispatcherW+0xe3 (FPO: [Non-Fpo])
        0006ffc0 77e6f23b svchost!_wmainCRTStartup+0x7f (FPO: [0,0,2])
        0006fff0 00000000 kernel32!BaseProcessStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 85d62b58  Cid 0584.05c4  Teb: 7ffdd000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d76418  QueueObject
        IRP List:
            85d659b8: (0006,0094) Flags: 00000800  Mdl: 00000000
        Not impersonating
        DeviceMap                 e159ad18
        Owning Process            85d6b5f0       Image:         svchost.exe
        Wait Start TickCount      11167          Ticks: 104801 (0:00:27:17.515)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x77c7b0f5)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6555000 Current f6554c4c Base f6555000 Limit f6552000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6554c64 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6554c7c 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6554cc4 808e55e2 nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f6554d48 80883908 nt!NtRemoveIoCompletion+0xdc (FPO: [Non-Fpo])
        f6554d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6554d64)
        0030feac 7c8277db ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0030feb0 77e5bea2 ntdll!ZwRemoveIoCompletion+0xc (FPO: [5,0,0])
        0030fedc 77c7b900 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        0030ff18 77c7b703 RPCRT4!COMMON_ProcessCalls+0xa1 (FPO: [Non-Fpo])
        0030ff84 77c7b9b5 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x117 (FPO: [Non-Fpo])
        0030ff8c 77c8872d RPCRT4!ProcessIOEventsWrapper+0xd (FPO: [Non-Fpo])
        0030ffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        0030ffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        0030ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

VMwareService process

```
PROCESS 85d56d88  SessionId: 0  Cid: 05ec    Peb: 7ffda000  ParentCid: 0198
    DirBase: 3af1a2a0  ObjectTable: e198a7d0  HandleCount:  56.
    Image: VMwareService.exe
    VadRoot 85d63958 Vads 43 Clone 0 Private 102. Modified 0. Locked 2.
    DeviceMap e1000170
    Token                             e251b030
    ElapsedTime                       00:38:41.577
    UserTime                          00:00:00.062
    KernelTime                        00:00:00.890
    QuotaPoolUsage[PagedPool]         28900
    QuotaPoolUsage[NonPagedPool]      1760
    Working Set Sizes (now,min,max)  (532, 50, 345) (2128KB, 200KB, 1380KB)
    PeakWorkingSetSize                532
    VirtualSize                       17 Mb
    PeakVirtualSize                   17 Mb
    PageFaultCount                    530
    MemoryPriority                    BACKGROUND
    BasePriority                      13
    CommitCharge                      142

    Setting context for this process...
.process /p /r ffffffff85d56d88

    !peb
PEB at 7ffda000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00400000
    Ldr                       7c8877e0
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00141f18 . 00144d80
    Ldr.InLoadOrderModuleList:           00141eb0 . 00145000
    Ldr.InMemoryOrderModuleList:         00141eb8 . 00145008
            Base TimeStamp                     Module
          400000 40c8fdf2 Jun 11 01:33:54 2004 C:\Program Files\VMware\VMware
Tools\VMwareService.exe
        7c800000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\ntdll.dll
        77e40000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\kernel32.dll
        77ba0000 45d70b06 Feb 17 14:02:46 2007 C:\WINDOWS\system32\MSVCRT.dll
        77f50000 45d70a26 Feb 17 13:59:02 2007 C:\WINDOWS\system32\ADVAPI32.dll
        77c50000 45d70aaa Feb 17 14:01:14 2007 C:\WINDOWS\system32\RPCRT4.dll
        76f50000 45d70ac3 Feb 17 14:01:39 2007 C:\WINDOWS\system32\Secur32.dll
        77380000 45d70ac7 Feb 17 14:01:43 2007 C:\WINDOWS\system32\USER32.dll
        77c00000 45d70a3e Feb 17 13:59:26 2007 C:\WINDOWS\system32\GDI32.dll
        77b90000 45d70ac8 Feb 17 14:01:44 2007 C:\WINDOWS\system32\VERSION.dll
        76cf0000 45d70a6c Feb 17 14:00:12 2007 C:\WINDOWS\system32\IpHlpApi.dll
        76b70000 45d70ab5 Feb 17 14:01:25 2007 C:\WINDOWS\system32\PSAPI.DLL
        71c00000 45d70ae9 Feb 17 14:02:17 2007 C:\WINDOWS\system32\WS2_32.dll
        71bf0000 45d70aea Feb 17 14:02:18 2007 C:\WINDOWS\system32\WS2HELP.dll
    SubSystemData:     00000000
    ProcessHeap:       00140000
    ProcessParameters: 00020000
    WindowTitle:  'C:\Program Files\VMware\VMware Tools\VMwareService.exe'
    ImageFile:    'C:\Program Files\VMware\VMware Tools\VMwareService.exe'
    CommandLine:  '"C:\Program Files\VMware\VMware Tools\VMwareService.exe"'
    DllPath:      'C:\Program Files\VMware\VMware
Tools;C:\WINDOWS\system32;C:\WINDOWS\system;C:\WINDOWS;.;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\
System32\Wbem'
    Environment:  00010000
        ALLUSERSPROFILE=C:\Documents and Settings\All Users
        ClusterLog=C:\WINDOWS\Cluster\cluster.log
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\WINDOWS\system32\cmd.exe
```

```
        FP_NO_HOST_CHECK=NO
        NUMBER_OF_PROCESSORS=1
        OS=Windows_NT
        Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 15 Model 5 Stepping 10, AuthenticAMD
        PROCESSOR_LEVEL=15
        PROCESSOR_REVISION=050a
        ProgramFiles=C:\Program Files
        SystemDrive=C:
        SystemRoot=C:\WINDOWS
        TEMP=C:\WINDOWS\TEMP
        TMP=C:\WINDOWS\TEMP
        USERPROFILE=C:\Documents and Settings\Default User
        windir=C:\WINDOWS


        THREAD 85d5b608  Cid 05ec.05f0  Teb: 7ffdf000 Win32Thread: e251dcb0 WAIT: (Unknown)
UserMode Non-Alertable
            85d5c28c  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85d56d88       Image:         VMwareService.exe
        Wait Start TickCount      5488           Ticks: 110480 (0:00:28:46.250)
        Context Switch Count      31                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.093
        Win32 Start Address VMwareService (0x00405f08)
        Start Address kernel32!BaseProcessStartThunk (0x77e617f8)
        Stack Init f67de000 Current f67ddc04 Base f67de000 Limit f67da000 Call 0
        Priority 13 BasePriority 13 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f67ddc1c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f67ddc34 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f67ddc78 808ed456 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f67ddca0 808ea5ad nt!IopSynchronousServiceTail+0x180 (FPO: [Non-Fpo])
        f67ddd38 80883908 nt!NtReadFile+0x5d5 (FPO: [Non-Fpo])
        f67ddd38 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f67ddd64)
        0012fbc0 7c82776b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0012fbc4 77e418b2 ntdll!NtReadFile+0xc (FPO: [9,0,0])
        0012fc2c 77f65edb kernel32!ReadFile+0x16c (FPO: [Non-Fpo])
        0012fc58 77f65f82 ADVAPI32!ScGetPipeInput+0x2a (FPO: [Non-Fpo])
        0012fccc 77fb75af ADVAPI32!ScDispatcherLoop+0x51 (FPO: [Non-Fpo])
        0012ff10 00402a2f ADVAPI32!StartServiceCtrlDispatcherA+0x93 (FPO: [Non-Fpo])
        0012ff30 00401242 VMwareService+0x2a2f
        0012ff4c 00405feb VMwareService+0x1242
        0012ffc0 77e6f23b VMwareService+0x5feb
        0012fff0 00000000 kernel32!BaseProcessStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 85d56b18  Cid 05ec.05f4  Teb: 7ffde000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d59d00  SynchronizationEvent
        IRP List:
            85d60280: (0006,0094) Flags: 00000000  Mdl: 86350208
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85d56d88       Image:         VMwareService.exe
        Wait Start TickCount      5490           Ticks: 110478 (0:00:28:46.218)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address MSVCRT!_endthread (0x77bcb35a)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6575000 Current f6574c78 Base f6575000 Limit f6572000 Call 0
        Priority 13 BasePriority 13 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6574c90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6574ca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6574cec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6574d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f6574d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6574d64)
        00a1e6b8 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00a1e6bc 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        00a1e72c 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        00a1e740 77e43a2c kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        00a1e754 004034ba kernel32!GetOverlappedResult+0x29 (FPO: [Non-Fpo])
        00a1ff84 77bcb3ca VMwareService+0x34ba
        00a1ffb8 77e64829 MSVCRT!_endthread+0xab (FPO: [Non-Fpo])
        00a1ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85d76b40  Cid 05ec.05f8  Teb: 7ffdd000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d76bb8  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85d56d88       Image:         VMwareService.exe
        Wait Start TickCount      114982         Ticks: 986 (0:00:00:15.406)
        Context Switch Count      304
        UserTime                  00:00:00.000
        KernelTime                00:00:00.046
        Win32 Start Address MSVCRT!_endthread (0x77bcb35a)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6551000 Current f6550c98 Base f6551000 Limit f654e000 Call 0
        Priority 13 BasePriority 13 PriorityDecrement 0
        ChildEBP RetAddr
        f6550cb0 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6550cc8 80827e1e nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6550d0c 8098c418 nt!KeDelayExecutionThread+0x254 (FPO: [Non-Fpo])
        f6550d54 80883908 nt!NtDelayExecution+0x84 (FPO: [Non-Fpo])
        f6550d54 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6550d64)
        00b1feec 7c826f4b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00b1fef0 77e41ed1 ntdll!NtDelayExecution+0xc (FPO: [2,0,0])
        00b1ff58 77e424ed kernel32!SleepEx+0x68 (FPO: [Non-Fpo])
        00b1ff68 00402e0d kernel32!Sleep+0xf (FPO: [Non-Fpo])
        00b1ff80 00402d33 VMwareService+0x2e0d
        00b1ffb8 77e64829 VMwareService+0x2d33
        00b1ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d5b398  Cid 05ec.05fc  Teb: 7ffdc000 Win32Thread: e2511ac0 WAIT: (Unknown)
UserMode Alertable
            85d5fa30  SynchronizationEvent
            85d5b410  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85d56d88       Image:         VMwareService.exe
        Wait Start TickCount      115962         Ticks: 6 (0:00:00:00.093)
        Context Switch Count      16148                 LargeStack
        UserTime                  00:00:00.062
        KernelTime                00:00:00.718
        Win32 Start Address ADVAPI32!ScSvcctrlThreadA (0x77f65e70)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6d58000 Current f6d57914 Base f6d58000 Limit f6d54000 Call 0
        Priority 15 BasePriority 15 PriorityDecrement 0
        ChildEBP RetAddr
        f6d5792c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6d57944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6d57978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6d57bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6d57d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6d57d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6d57d64)
        00c1fe74 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00c1fe78 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00c1ff20 00401745 kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        00c1ff44 0040162d VMwareService+0x1745
        00c1ff9c 00402ad3 VMwareService+0x162d
        00c1ffb8 77e64829 VMwareService+0x2ad3
        00c1ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

Svchost process (termsvcs)

```
PROCESS 85dc8d88  SessionId: 0  Cid: 065c    Peb: 7ffd4000  ParentCid: 0198
    DirBase: 3af1a1a0  ObjectTable: e1559c30  HandleCount: 138.
    Image: svchost.exe
    VadRoot 85d726e0 Vads 97 Clone 0 Private 214. Modified 2. Locked 0.
    DeviceMap e1000170
    Token                             e1815d08
    ElapsedTime                       00:38:30.234
    UserTime                          00:00:00.109
    KernelTime                        00:00:00.609
    QuotaPoolUsage[PagedPool]         59372
    QuotaPoolUsage[NonPagedPool]      4536
    Working Set Sizes (now,min,max)  (952, 50, 345) (3808KB, 200KB, 1380KB)
    PeakWorkingSetSize                956
    VirtualSize                       52 Mb
    PeakVirtualSize                   52 Mb
    PageFaultCount                    1097
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      341

    Setting context for this process...
.process /p /r ffffffff85dc8d88

    !peb
PEB at 7ffd4000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         01000000
    Ldr                       7c8877e0
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00091f18 . 0009e5a8
    Ldr.InLoadOrderModuleList:           00091eb0 . 0009e598
    Ldr.InMemoryOrderModuleList:         00091eb8 . 0009e5a0
            Base TimeStamp                     Module
         1000000 45d6a03c Feb 17 06:27:08 2007 C:\WINDOWS\System32\svchost.exe
        7c800000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\ntdll.dll
        77e40000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\kernel32.dll
        77f50000 45d70a26 Feb 17 13:59:02 2007 C:\WINDOWS\system32\ADVAPI32.dll
        77c50000 45d70aaa Feb 17 14:01:14 2007 C:\WINDOWS\system32\RPCRT4.dll
        76f50000 45d70ac3 Feb 17 14:01:39 2007 C:\WINDOWS\system32\Secur32.dll
        77e00000 45d70aab Feb 17 14:01:15 2007 C:\WINDOWS\System32\NTMARTA.DLL
        77ba0000 45d70b06 Feb 17 14:02:46 2007 C:\WINDOWS\system32\msvcrt.dll
        77380000 45d70ac7 Feb 17 14:01:43 2007 C:\WINDOWS\system32\USER32.dll
        77c00000 45d70a3e Feb 17 13:59:26 2007 C:\WINDOWS\system32\GDI32.dll
        76f10000 45d70ad5 Feb 17 14:01:57 2007 C:\WINDOWS\system32\WLDAP32.dll
        7e020000 45d70aa8 Feb 17 14:01:12 2007 C:\WINDOWS\System32\SAMLIB.dll
        77670000 45d70aa5 Feb 17 14:01:09 2007 C:\WINDOWS\system32\ole32.dll
          660000 45d69418 Feb 17 05:35:20 2007 C:\WINDOWS\System32\xpsp2res.dll
        76540000 45d70ac3 Feb 17 14:01:39 2007 c:\windows\system32\termsrv.dll
        74d90000 45d70a4d Feb 17 13:59:41 2007 c:\windows\system32\ICAAPI.dll
        71c00000 45d70ae9 Feb 17 14:02:17 2007 c:\windows\system32\WS2_32.dll
        71bf0000 45d70aea Feb 17 14:02:18 2007 c:\windows\system32\WS2HELP.dll
        77d00000 45d70aa6 Feb 17 14:01:10 2007 C:\WINDOWS\system32\OLEAUT32.dll
        76c40000 45d70a49 Feb 17 13:59:37 2007 c:\windows\system32\AUTHZ.dll
        74f60000 45d70b01 Feb 17 14:02:41 2007 c:\windows\system32\mstlsapi.dll
        76df0000 45d70a11 Feb 17 13:58:41 2007 c:\windows\system32\ACTIVEDS.dll
        76dc0000 45d70a22 Feb 17 13:58:58 2007 c:\windows\system32\adsldpc.dll
        71c40000 45d70a82 Feb 17 14:00:34 2007 C:\WINDOWS\system32\NETAPI32.dll
        76b80000 45d70a7f Feb 17 14:00:31 2007 c:\windows\system32\credui.dll
        7c8d0000 45d70abb Feb 17 14:01:31 2007 C:\WINDOWS\system32\SHELL32.dll
        77da0000 45d70ac0 Feb 17 14:01:36 2007 C:\WINDOWS\system32\SHLWAPI.dll
        76a80000 3e80249c Mar 25 09:42:52 2003 c:\windows\system32\ATL.DLL
        761b0000 45d70a80 Feb 17 14:00:32 2007 C:\WINDOWS\system32\CRYPT32.dll
        76190000 45d70aac Feb 17 14:01:16 2007 C:\WINDOWS\system32\MSASN1.dll
```

```
        77910000 45d70ab1 Feb 17 14:01:21 2007 c:\windows\system32\REGAPI.dll
        77420000 45d70a05 Feb 17 13:58:29 2007 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.3790.3959_x-ww_D8713E55\comctl32.dll
        68000000 45d69786 Feb 17 05:49:58 2007 C:\WINDOWS\System32\rsaenh.dll
        76b70000 45d70ab5 Feb 17 14:01:25 2007 C:\WINDOWS\System32\PSAPI.DLL
        77b90000 45d70ac8 Feb 17 14:01:44 2007 C:\WINDOWS\system32\VERSION.dll
        76920000 45d70ac8 Feb 17 14:01:44 2007 C:\WINDOWS\System32\USERENV.dll
    SubSystemData:     00000000
    ProcessHeap:       00090000
    ProcessParameters: 00020000
    WindowTitle:  'C:\WINDOWS\System32\svchost.exe'
    ImageFile:    'C:\WINDOWS\System32\svchost.exe'
    CommandLine:  'C:\WINDOWS\System32\svchost.exe -k termsvcs'
    DllPath:
'C:\WINDOWS\System32;C:\WINDOWS\system32;C:\WINDOWS\system;C:\WINDOWS;.;C:\WINDOWS\system32;C:\WIND
OWS;C:\WINDOWS\System32\Wbem'
    Environment:  00010000
        ALLUSERSPROFILE=C:\Documents and Settings\All Users
        ClusterLog=C:\WINDOWS\Cluster\cluster.log
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\WINDOWS\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        NUMBER_OF_PROCESSORS=1
        OS=Windows_NT
        Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 15 Model 5 Stepping 10, AuthenticAMD
        PROCESSOR_LEVEL=15
        PROCESSOR_REVISION=050a
        ProgramFiles=C:\Program Files
        SystemDrive=C:
        SystemRoot=C:\WINDOWS
        TEMP=C:\WINDOWS\TEMP
        TMP=C:\WINDOWS\TEMP
        USERPROFILE=C:\Documents and Settings\Default User
        windir=C:\WINDOWS


        THREAD 863b6360  Cid 065c.0660  Teb: 7ffdf000 Win32Thread: e253d868 WAIT: (Unknown)
UserMode Non-Alertable
            8633aaac  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85dc8d88       Image:         svchost.exe
        Wait Start TickCount      6267           Ticks: 109701 (0:00:28:34.078)
        Context Switch Count      46                LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.140
        Win32 Start Address svchost!wmainCRTStartup (0x010020b9)
        Start Address kernel32!BaseProcessStartThunk (0x77e617f8)
        Stack Init f65fd000 Current f65fcc04 Base f65fd000 Limit f65f9000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f65fcc1c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f65fcc34 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f65fcc78 808ed456 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f65fcca0 808ea5ad nt!IopSynchronousServiceTail+0x180 (FPO: [Non-Fpo])
        f65fcd38 80883908 nt!NtReadFile+0x5d5 (FPO: [Non-Fpo])
        f65fcd38 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f65fcd64)
        0007fc40 7c82776b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0007fc44 77e418b2 ntdll!NtReadFile+0xc (FPO: [9,0,0])
        0007fcac 77f65edb kernel32!ReadFile+0x16c (FPO: [Non-Fpo])
        0007fcd8 77f65f82 ADVAPI32!ScGetPipeInput+0x2a (FPO: [Non-Fpo])
        0007fd4c 77f51ed9 ADVAPI32!ScDispatcherLoop+0x51 (FPO: [Non-Fpo])
        0007ffb0 0100213d ADVAPI32!StartServiceCtrlDispatcherW+0xe3 (FPO: [Non-Fpo])
        0007ffc0 77e6f23b svchost!_wmainCRTStartup+0x7f (FPO: [0,0,2])
        0007fff0 00000000 kernel32!BaseProcessStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 85e07db0  Cid 065c.0670  Teb: 7ffdc000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d64c80  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85dc8d88       Image:         svchost.exe
        Wait Start TickCount      19074          Ticks: 96894 (0:00:25:13.968)
        Context Switch Count      9
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address termsrv!NotificationQueueWorker (0x76561eaf)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f653d000 Current f653cc78 Base f653d000 Limit f653a000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f653cc90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f653cca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f653ccec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f653cd50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f653cd50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f653cd64)
        00a2ff1c 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00a2ff20 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        00a2ff90 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        00a2ffa4 76561e79 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        00a2ffb4 76561eb4 termsrv!NotificationQueueWorkerEx+0x11 (FPO: [0,0,1])
        00a2ffb8 77e64829 termsrv!NotificationQueueWorker+0x5 (FPO: [1,0,0])
        00a2ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85df0d68  Cid 065c.0674  Teb: 7ffdb000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            862c56a0  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85dc8d88       Image:         svchost.exe
        Wait Start TickCount      37014          Ticks: 78954 (0:00:20:33.656)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x77c7b0f5)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f679e000 Current f679dc24 Base f679e000 Limit f679b000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f679dc3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f679dc54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f679dc98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f679dd48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f679dd48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f679dd64)
        00a7fe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00a7fe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        00a7ff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        00a7ff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        00a7ffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        00a7ffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        00a7ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d65688  Cid 065c.0678  Teb: 7ffda000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d82290  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85dc8d88       Image:         svchost.exe
        Wait Start TickCount      19019          Ticks: 96949 (0:00:25:14.828)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x000014be
        LPC Server thread working on message Id 14be
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f68ce000 Current f68cdc0c Base f68ce000 Limit f68cb000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f68cdc24 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f68cdc3c 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f68cdc80 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f68cdd30 8091a8d8 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f68cdd4c 80883908 nt!NtReplyWaitReceivePort+0x18 (FPO: [Non-Fpo])
        f68cdd4c 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f68cdd64)
        00abfe74 7c82782b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00abfe78 76557eee ntdll!ZwReplyWaitReceivePort+0xc (FPO: [4,0,0])
        00abffb8 77e64829 termsrv!WinStationLpcThread+0x5a (FPO: [Non-Fpo])
        00abffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85d67db0  Cid 065c.067c  Teb: 7ffd9000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d82290  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85dc8d88       Image:         svchost.exe
        Wait Start TickCount      6301           Ticks: 109667 (0:00:28:33.546)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x00000a8b
        LPC Server thread working on message Id a8b
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f65cd000 Current f65ccc0c Base f65cd000 Limit f65ca000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f65ccc24 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f65ccc3c 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f65ccc80 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f65ccd30 8091a8d8 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f65ccd4c 80883908 nt!NtReplyWaitReceivePort+0x18 (FPO: [Non-Fpo])
        f65ccd4c 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f65ccd64)
        00affe74 7c82782b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00affe78 76557eee ntdll!ZwReplyWaitReceivePort+0xc (FPO: [4,0,0])
        00afffb8 77e64829 termsrv!WinStationLpcThread+0x5a (FPO: [Non-Fpo])
        00afffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 86331980  Cid 065c.0680  Teb: 7ffd8000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d82290  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85dc8d88       Image:         svchost.exe
        Wait Start TickCount      6301           Ticks: 109667 (0:00:28:33.546)
        Context Switch Count      2
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x00000a8c
        LPC Server thread working on message Id a8c
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f66a1000 Current f66a0c0c Base f66a1000 Limit f669e000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f66a0c24 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f66a0c3c 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f66a0c80 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f66a0d30 8091a8d8 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f66a0d4c 80883908 nt!NtReplyWaitReceivePort+0x18 (FPO: [Non-Fpo])
        f66a0d4c 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f66a0d64)
        00b3fe74 7c82782b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00b3fe78 76557eee ntdll!ZwReplyWaitReceivePort+0xc (FPO: [4,0,0])
        00b3ffb8 77e64829 termsrv!WinStationLpcThread+0x5a (FPO: [Non-Fpo])
        00b3ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85d474e0  Cid 065c.0684  Teb: 7ffd7000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d63178  SynchronizationEvent
            85d67b48  SynchronizationEvent
            85d5f480  SynchronizationEvent
            85d4dee0  SynchronizationEvent
            85d713a8  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85dc8d88       Image:         svchost.exe
        Wait Start TickCount      6304           Ticks: 109664 (0:00:28:33.500)
        Context Switch Count      6
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address termsrv!GroupPolicyNotifyThread (0x7654ee1e)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6455000 Current f6454914 Base f6455000 Limit f6452000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f645492c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6454944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6454978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6454bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6454d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6454d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6454d64)
        00b9fe74 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00b9fe78 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00b9ff20 77e62fbe kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        00b9ff3c 779121f5 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        00b9ff84 7654ee79 REGAPI!WaitForTSConnectionsPolicyChanges+0x1fe (FPO: [Non-Fpo])
        00b9ffb8 77e64829 termsrv!GroupPolicyNotifyThread+0x5b (FPO: [Non-Fpo])
        00b9ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 86346730  Cid 065c.0688  Teb: 7ffd6000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d6a1c8  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85dc8d88       Image:         svchost.exe
        Wait Start TickCount      6303           Ticks: 109665 (0:00:28:33.515)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address termsrv!WinStationIdleControlThread (0x7654ed14)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6451000 Current f6450c78 Base f6451000 Limit f644e000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6450c90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6450ca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6450cec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6450d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f6450d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6450d64)
        00bdff8c 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00bdff90 7654ed83 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        00bdffb8 77e64829 termsrv!WinStationIdleControlThread+0x6f (FPO: [Non-Fpo])
        00bdffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 8633adb0  Cid 065c.068c  Teb: 7ffd5000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d6a198  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85dc8d88       Image:         svchost.exe
        Wait Start TickCount      6303           Ticks: 109665 (0:00:28:33.515)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address termsrv!WinStationTerminateThread (0x7654a5e5)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f644d000 Current f644c914 Base f644d000 Limit f644a000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f644c92c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f644c944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f644c978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f644cbf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f644cd48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f644cd48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f644cd64)
        00c1ff5c 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00c1ff60 7654a7cc ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00c1ffb8 77e64829 termsrv!WinStationTerminateThread+0x1e7 (FPO: [Non-Fpo])
        00c1ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d48020  Cid 065c.0694  Teb: 7ffae000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85da8d98  QueueObject
        IRP List:
            85d5feb8: (0006,0094) Flags: 00000800  Mdl: 00000000
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85dc8d88       Image:         svchost.exe
        Wait Start TickCount      12065          Ticks: 103903 (0:00:27:03.484)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address RPCRT4!ThreadStartRoutine (0x77c7b0f5)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6445000 Current f6444c4c Base f6445000 Limit f6442000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6444c64 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6444c7c 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6444cc4 808e55e2 nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f6444d48 80883908 nt!NtRemoveIoCompletion+0xdc (FPO: [Non-Fpo])
        f6444d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6444d64)
        00c9feac 7c8277db ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00c9feb0 77e5bea2 ntdll!ZwRemoveIoCompletion+0xc (FPO: [5,0,0])
        00c9fedc 77c7b900 kernel32!GetQueuedCompletionStatus+0x29 (FPO: [Non-Fpo])
        00c9ff18 77c7b703 RPCRT4!COMMON_ProcessCalls+0xa1 (FPO: [Non-Fpo])
        00c9ff84 77c7b9b5 RPCRT4!LOADABLE_TRANSPORT::ProcessIOEvents+0x117 (FPO: [Non-Fpo])
        00c9ff8c 77c8872d RPCRT4!ProcessIOEventsWrapper+0xd (FPO: [Non-Fpo])
        00c9ffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        00c9ffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        00c9ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85d8a440  Cid 065c.069c  Teb: 7ffdd000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d636a8  NotificationEvent
            862fdeb0  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85dc8d88       Image:         svchost.exe
        Wait Start TickCount      6304           Ticks: 109664 (0:00:28:33.500)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address USERENV!NotificationThread (0x76929dd9)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f643d000 Current f643c914 Base f643d000 Limit f643a000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f643c92c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f643c944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f643c978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f643cbf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f643cd48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f643cd48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f643cd64)
        0096fec0 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0096fec4 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0096ff6c 77e62fbe kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        0096ff88 76929e35 kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        0096ffb8 77e64829 USERENV!NotificationThread+0x5f (FPO: [Non-Fpo])
        0096ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d5bdb0  Cid 065c.06a0  Teb: 7ffac000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            85d5be28  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85dc8d88       Image:         svchost.exe
        Wait Start TickCount      6305           Ticks: 109663 (0:00:28:33.484)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address ntdll!RtlpTimerThread (0x7c83d3dd)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6439000 Current f6438c98 Base f6439000 Limit f6436000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6438cb0 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6438cc8 80827e1e nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6438d0c 8098c418 nt!KeDelayExecutionThread+0x254 (FPO: [Non-Fpo])
        f6438d54 80883908 nt!NtDelayExecution+0x84 (FPO: [Non-Fpo])
        f6438d54 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6438d64)
        00d3ff9c 7c826f4b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00d3ffa0 7c83d424 ntdll!NtDelayExecution+0xc (FPO: [2,0,0])
        00d3ffb8 77e64829 ntdll!RtlpTimerThread+0x47 (FPO: [Non-Fpo])
        00d3ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85d53db0  Cid 065c.06a4  Teb: 7ffad000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d8b3d0  Semaphore Limit 0x7fffffff
            85d53e28  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85dc8d88       Image:         svchost.exe
        Wait Start TickCount      102602         Ticks: 13366 (0:00:03:28.843)
        Context Switch Count      58
        UserTime                  00:00:00.000
        KernelTime                00:00:00.125
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6e35000 Current f6e34c24 Base f6e35000 Limit f6e32000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6e34c3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6e34c54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6e34c98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6e34d48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f6e34d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6e34d64)
        00cffe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00cffe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        00cfff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        00cfff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        00cfffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        00cfffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        00cfffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d45ae0  Cid 065c.079c  Teb: 7ffaf000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d8b3d0  Semaphore Limit 0x7fffffff
            85d45b58  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85dc8d88       Image:         svchost.exe
        Wait Start TickCount      102442         Ticks: 13526 (0:00:03:31.343)
        Context Switch Count      8
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f66ad000 Current f66acc24 Base f66ad000 Limit f66aa000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f66acc3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f66acc54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f66acc98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f66acd48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f66acd48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f66acd64)
        00c5fe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00c5fe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        00c5ff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        00c5ff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        00c5ffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        00c5ffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        00c5ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

Wmiprvse process

```
PROCESS 85d41958  SessionId: 0  Cid: 06ec    Peb: 7ffd8000  ParentCid: 0280
    DirBase: 3af1a280  ObjectTable: 00000000  HandleCount:   0.
    Image: wmiprvse.exe
    VadRoot 00000000 Vads 0 Clone 0 Private 0. Modified 13. Locked 0.
    DeviceMap e16b5d18
    Token                             e2500900
    ElapsedTime                       00:35:43.546
    UserTime                          00:00:00.062
    KernelTime                        406 Days 01:05:42.984
    QuotaPoolUsage[PagedPool]         0
    QuotaPoolUsage[NonPagedPool]      0
    Working Set Sizes (now,min,max)  (7, 50, 345) (28KB, 200KB, 1380KB)
    PeakWorkingSetSize                1505
    VirtualSize                       25 Mb
    PeakVirtualSize                   32 Mb
    PageFaultCount                    1839
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      0
    Job                               8637c780

    Setting context for this process...
.process /p /r ffffffff85d41958

    !peb
PEB at 7ffd8000
error 1 InitTypeRead( nt!_PEB at 7ffd8000)...


No active threads
```

Wmiprvse process

```
PROCESS 85d46b18  SessionId: 0  Cid: 0730    Peb: 7ffde000  ParentCid: 0280
    DirBase: 3af1a2c0  ObjectTable: e2549198  HandleCount: 155.
    Image: wmiprvse.exe
    VadRoot 85d51048 Vads 79 Clone 0 Private 308. Modified 1. Locked 0.
    DeviceMap e1000170
    Token                             e2546b08
    ElapsedTime                       00:35:41.906
    UserTime                          00:00:00.062
    KernelTime                        00:00:01.625
    QuotaPoolUsage[PagedPool]         46252
    QuotaPoolUsage[NonPagedPool]      3448
    Working Set Sizes (now,min,max)  (1241, 50, 345) (4964KB, 200KB, 1380KB)
    PeakWorkingSetSize                1310
    VirtualSize                       26 Mb
    PeakVirtualSize                   27 Mb
    PageFaultCount                    1692
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      399
    Job                               8637c780

    Setting context for this process...
.process /p /r ffffffff85d46b18

    !peb
PEB at 7ffde000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         01000000
    Ldr                       7c8877e0
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00091f18 . 000e3300
    Ldr.InLoadOrderModuleList:           00091eb0 . 000e32f0
    Ldr.InMemoryOrderModuleList:         00091eb8 . 000e32f8
            Base TimeStamp                     Module
         1000000 45d698b6 Feb 17 05:55:02 2007 C:\WINDOWS\system32\wbem\wmiprvse.exe
        7c800000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\ntdll.dll
        77e40000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\kernel32.dll
        77ba0000 45d70b06 Feb 17 14:02:46 2007 C:\WINDOWS\system32\msvcrt.dll
        77f50000 45d70a26 Feb 17 13:59:02 2007 C:\WINDOWS\system32\ADVAPI32.dll
        77c50000 45d70aaa Feb 17 14:01:14 2007 C:\WINDOWS\system32\RPCRT4.dll
        76f50000 45d70ac3 Feb 17 14:01:39 2007 C:\WINDOWS\system32\Secur32.dll
        77380000 45d70ac7 Feb 17 14:01:43 2007 C:\WINDOWS\system32\USER32.dll
        77c00000 45d70a3e Feb 17 13:59:26 2007 C:\WINDOWS\system32\GDI32.dll
        750f0000 45d70ad3 Feb 17 14:01:55 2007 C:\WINDOWS\system32\wbem\wbemcomn.dll
        77d00000 45d70aa6 Feb 17 14:01:10 2007 C:\WINDOWS\system32\OLEAUT32.dll
        77670000 45d70aa5 Feb 17 14:01:09 2007 C:\WINDOWS\system32\ole32.dll
        75550000 45d70a3a Feb 17 13:59:22 2007 C:\WINDOWS\system32\wbem\FastProx.dll
          400000 45d6a071 Feb 17 06:28:01 2007 C:\WINDOWS\system32\msvcp60.dll
        766f0000 45d70a9f Feb 17 14:01:03 2007 C:\WINDOWS\system32\NTDSAPI.dll
        76ed0000 45d70a64 Feb 17 14:00:04 2007 C:\WINDOWS\system32\DNSAPI.dll
        71c00000 45d70ae9 Feb 17 14:02:17 2007 C:\WINDOWS\system32\WS2_32.dll
        71bf0000 45d70aea Feb 17 14:02:18 2007 C:\WINDOWS\system32\WS2HELP.dll
        76f10000 45d70ad5 Feb 17 14:01:57 2007 C:\WINDOWS\system32\WLDAP32.dll
        71c40000 45d70a82 Feb 17 14:00:34 2007 C:\WINDOWS\system32\NETAPI32.dll
        5fb10000 45d70a7a Feb 17 14:00:26 2007 C:\WINDOWS\system32\NCObjAPI.DLL
        69500000 45d70a3a Feb 17 13:59:22 2007 C:\WINDOWS\system32\faultrep.DLL
        77b90000 45d70ac8 Feb 17 14:01:44 2007 C:\WINDOWS\system32\VERSION.dll
        76920000 45d70ac8 Feb 17 14:01:44 2007 C:\WINDOWS\system32\USERENV.dll
        771f0000 45d70ace Feb 17 14:01:50 2007 C:\WINDOWS\system32\WINSTA.dll
        770e0000 45d70ab3 Feb 17 14:01:23 2007 C:\WINDOWS\system32\SETUPAPI.dll
        77da0000 45d70ac0 Feb 17 14:01:36 2007 C:\WINDOWS\system32\SHLWAPI.dll
          880000 45d69418 Feb 17 05:35:20 2007 C:\WINDOWS\system32\xpsp2res.dll
        777b0000 45d70a3b Feb 17 13:59:23 2007 C:\WINDOWS\system32\CLBCatQ.DLL
```

```
        77010000 45d70a76 Feb 17 14:00:22 2007 C:\WINDOWS\system32\COMRes.dll
        74ce0000 3e8024a8 Mar 25 09:43:04 2003 C:\WINDOWS\system32\wbem\wbemsvc.dll
        74e60000 45d70aef Feb 17 14:02:23 2007 C:\WINDOWS\system32\wbem\wmiutils.dll
        72fa0000 45d70aea Feb 17 14:02:18 2007 C:\WINDOWS\system32\wbem\wmiprov.dll
        76cc0000 3e80249b Mar 25 09:42:51 2003 C:\WINDOWS\system32\WMI.dll
        77e00000 45d70aab Feb 17 14:01:15 2007 C:\WINDOWS\system32\NTMARTA.DLL
        7e020000 45d70aa8 Feb 17 14:01:12 2007 C:\WINDOWS\system32\SAMLIB.dll
        76c40000 45d70a49 Feb 17 13:59:37 2007 C:\WINDOWS\system32\authz.dll
        769f0000 45d70a3f Feb 17 13:59:27 2007 C:\WINDOWS\system32\wbem\esscli.dll
    SubSystemData:     00000000
    ProcessHeap:       00090000
    ProcessParameters: 00020000
    WindowTitle:  'C:\WINDOWS\system32\wbem\wmiprvse.exe'
    ImageFile:    'C:\WINDOWS\system32\wbem\wmiprvse.exe'
    CommandLine:  'C:\WINDOWS\system32\wbem\wmiprvse.exe'
    DllPath:
'C:\WINDOWS\system32\wbem;C:\WINDOWS\system32;C:\WINDOWS\system;C:\WINDOWS;.;C:\WINDOWS\system32;C:
\WINDOWS;C:\WINDOWS\System32\Wbem'
    Environment:  00010000
        ALLUSERSPROFILE=C:\Documents and Settings\All Users
        ClusterLog=C:\WINDOWS\Cluster\cluster.log
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\WINDOWS\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        NUMBER_OF_PROCESSORS=1
        OS=Windows_NT
        Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 15 Model 5 Stepping 10, AuthenticAMD
        PROCESSOR_LEVEL=15
        PROCESSOR_REVISION=050a
        ProgramFiles=C:\Program Files
        SystemDrive=C:
        SystemRoot=C:\WINDOWS
        TEMP=C:\WINDOWS\TEMP
        TMP=C:\WINDOWS\TEMP
        USERPROFILE=C:\Documents and Settings\Default User
        windir=C:\WINDOWS


        THREAD 85d468a8  Cid 0730.0734  Teb: 7ffdd000 Win32Thread: e25395d0 WAIT: (Unknown)
UserMode Non-Alertable
            863b6808  SynchronizationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85d46b18       Image:         wmiprvse.exe
        Wait Start TickCount      24720          Ticks: 91248 (0:00:23:45.750)
        Context Switch Count      93                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.390
        Win32 Start Address wmiprvse!WinMainCRTStartup (0x0102328c)
        Start Address kernel32!BaseProcessStartThunk (0x77e617f8)
        Stack Init f6b03000 Current f6b02bc4 Base f6b03000 Limit f6aff000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6b02bdc 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6b02bf4 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6b02c38 bf89b1c3 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6b02c94 bf89b986 win32k!xxxSleepThread+0x1be (FPO: [Non-Fpo])
        f6b02cec bf89da22 win32k!xxxRealInternalGetMessage+0x46a (FPO: [Non-Fpo])
        f6b02d4c 80883908 win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        f6b02d4c 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6b02d64)
        0007fe40 7739c811 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0007fe60 0100a6eb USER32!NtUserGetMessage+0xc
        0007fe9c 0100c025 wmiprvse!WindowsDispatch+0x31 (FPO: [Non-Fpo])
        0007ff14 0100c115 wmiprvse!Process+0x20b (FPO: [Non-Fpo])
        0007ff1c 0102340e wmiprvse!WinMain+0x59 (FPO: [Non-Fpo])
```

```
        0007ffc0 77e6f23b wmiprvse!WinMainCRTStartup+0x182 (FPO: [Non-Fpo])
        0007fff0 00000000 kernel32!BaseProcessStart+0x23 (FPO: [Non-Fpo])

        THREAD 860e6020  Cid 0730.074c  Teb: 7ffd8000 Win32Thread: e17cfab0 WAIT: (Unknown)
UserMode Alertable
            862dae30  SynchronizationEvent
            86415558  SynchronizationEvent
            86415528  SynchronizationEvent
            8645a1e8  SynchronizationEvent
            863bfb40  SynchronizationEvent
            860e6098  NotificationTimer
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85d46b18       Image:         wmiprvse.exe
        Wait Start TickCount      112854         Ticks: 3114 (0:00:00:48.656)
        Context Switch Count      29                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.078
        Win32 Start Address wmiprvse!WmiThread<unsigned long>::ThreadProc (0x0100cb14)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6ae3000 Current f6ae2914 Base f6ae3000 Limit f6ae0000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6ae292c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6ae2944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6ae2978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6ae2bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6ae2d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6ae2d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6ae2d64)
        00d7fd28 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00d7fd2c 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00d7fdd4 7739bbd1 kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        00d7fe30 0100cc9b USER32!RealMsgWaitForMultipleObjectsEx+0x141 (FPO: [Non-Fpo])
        00d7ff78 0100cbfe wmiprvse!WmiThread<unsigned long>::ThreadWait+0x65 (FPO: [Non-Fpo])
        00d7ffa8 0100cb3f wmiprvse!WmiThread<unsigned long>::ThreadDispatch+0xa3 (FPO: [Non-Fpo])
        00d7ffb8 77e64829 wmiprvse!WmiThread<unsigned long>::ThreadProc+0x2b (FPO: [Non-Fpo])
        00d7ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 860e6db0  Cid 0730.0750  Teb: 7ffd7000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            8630f320  Semaphore Limit 0x7fffffff
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85d46b18       Image:         wmiprvse.exe
        Wait Start TickCount      110351         Ticks: 5617 (0:00:01:27.765)
        Context Switch Count      127
        UserTime                  00:00:00.000
        KernelTime                00:00:00.062
        Win32 Start Address 0x00002345
        LPC Server thread working on message Id 2345
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f63f5000 Current f63f4c24 Base f63f5000 Limit f63f2000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f63f4c3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f63f4c54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f63f4c98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f63f4d48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f63f4d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f63f4d64)
        00dbfe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00dbfe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        00dbff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        00dbff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        00dbffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        00dbffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        00dbffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 860b6db0  Cid 0730.0770  Teb: 7ffd5000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            8636c2f0  NotificationEvent
            86312240  NotificationEvent
        Not impersonating
        DeviceMap                 e1000170
        Owning Process            85d46b18       Image:         wmiprvse.exe
        Wait Start TickCount      11265          Ticks: 104703 (0:00:27:15.984)
        Context Switch Count      1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address NCObjAPI!CNamedPipeClient::ProviderReadyThreadProc (0x5fb1168d)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f63d9000 Current f63d8914 Base f63d9000 Limit f63d6000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f63d892c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f63d8944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f63d8978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f63d8bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f63d8d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f63d8d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f63d8d64)
        00f3fe9c 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00f3fea0 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        00f3ff48 77e62fbe kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        00f3ff64 5fb116db kernel32!WaitForMultipleObjects+0x18 (FPO: [Non-Fpo])
        00f3ffb8 77e64829 NCObjAPI!CNamedPipeClient::ProviderReadyThreadProc+0xb3 (FPO: [Non-Fpo])
        00f3ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

Userinit process

```
PROCESS 85d446e8  SessionId: 0  Cid: 0300    Peb: 7ffdc000  ParentCid: 0168
    DirBase: 3af1a2e0  ObjectTable: 00000000  HandleCount:   0.
    Image: userinit.exe
    VadRoot 00000000 Vads 0 Clone 0 Private 0. Modified 3. Locked 0.
    DeviceMap e249e270
    Token                             e102f9e0
    ElapsedTime                       00:28:08.000
    UserTime                          00:00:00.000
    KernelTime                        406 Days 01:08:44.937
    QuotaPoolUsage[PagedPool]         0
    QuotaPoolUsage[NonPagedPool]      0
    Working Set Sizes (now,min,max)  (7, 50, 345) (28KB, 200KB, 1380KB)
    PeakWorkingSetSize                477
    VirtualSize                       10 Mb
    PeakVirtualSize                   14 Mb
    PageFaultCount                    554
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      0

    Setting context for this process...
.process /p /r ffffffff85d446e8

    !peb
PEB at 7ffdc000
error 1 InitTypeRead( nt!_PEB at 7ffdc000)...


No active threads
```

Explorer process

```
PROCESS 85d5ed88  SessionId: 0  Cid: 035c    Peb: 7ffda000  ParentCid: 0300
    DirBase: 3af1a300  ObjectTable: e104d0f8  HandleCount: 352.
    Image: explorer.exe
    VadRoot 86346b78 Vads 180 Clone 0 Private 1772. Modified 17761. Locked 0.
    DeviceMap e249e270
    Token                             e1060c40
    ElapsedTime                       00:28:03.703
    UserTime                          00:00:00.796
    KernelTime                        00:00:16.671
    QuotaPoolUsage[PagedPool]         103588
    QuotaPoolUsage[NonPagedPool]      10560
    Working Set Sizes (now,min,max)  (3778, 50, 345) (15112KB, 200KB, 1380KB)
    PeakWorkingSetSize                3866
    VirtualSize                       59 Mb
    PeakVirtualSize                   67 Mb
    PageFaultCount                    17488
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      2262

    Setting context for this process...
.process /p /r ffffffff85d5ed88

    !peb
PEB at 7ffda000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         01000000
    Ldr                       7c8877e0
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00091f18 . 001328b8
    Ldr.InLoadOrderModuleList:           00091eb0 . 001328a8
    Ldr.InMemoryOrderModuleList:         00091eb8 . 001328b0
            Base TimeStamp                     Module
         1000000 45d6a1b7 Feb 17 06:33:27 2007 C:\WINDOWS\Explorer.EXE
        7c800000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\ntdll.dll
        77e40000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\kernel32.dll
        77ba0000 45d70b06 Feb 17 14:02:46 2007 C:\WINDOWS\system32\msvcrt.dll
        77f50000 45d70a26 Feb 17 13:59:02 2007 C:\WINDOWS\system32\ADVAPI32.dll
        77c50000 45d70aaa Feb 17 14:01:14 2007 C:\WINDOWS\system32\RPCRT4.dll
        76f50000 45d70ac3 Feb 17 14:01:39 2007 C:\WINDOWS\system32\Secur32.dll
        77c00000 45d70a3e Feb 17 13:59:26 2007 C:\WINDOWS\system32\GDI32.dll
        77380000 45d70ac7 Feb 17 14:01:43 2007 C:\WINDOWS\system32\USER32.dll
        77da0000 45d70ac0 Feb 17 14:01:36 2007 C:\WINDOWS\system32\SHLWAPI.dll
        7c8d0000 45d70abb Feb 17 14:01:31 2007 C:\WINDOWS\system32\SHELL32.dll
        77670000 45d70aa5 Feb 17 14:01:09 2007 C:\WINDOWS\system32\ole32.dll
        77d00000 45d70aa6 Feb 17 14:01:10 2007 C:\WINDOWS\system32\OLEAUT32.dll
        75eb0000 45d70a19 Feb 17 13:58:49 2007 C:\WINDOWS\system32\BROWSEUI.dll
        77980000 45d70aba Feb 17 14:01:30 2007 C:\WINDOWS\system32\SHDOCVW.dll
        761b0000 45d70a80 Feb 17 14:00:32 2007 C:\WINDOWS\system32\CRYPT32.dll
        76190000 45d70aac Feb 17 14:01:16 2007 C:\WINDOWS\system32\MSASN1.dll
        75360000 45d70a85 Feb 17 14:00:37 2007 C:\WINDOWS\system32\CRYPTUI.dll
        76bb0000 45d70acf Feb 17 14:01:51 2007 C:\WINDOWS\system32\WINTRUST.dll
        76c10000 45d70a5d Feb 17 13:59:57 2007 C:\WINDOWS\system32\imagehlp.dll
        71c40000 45d70a82 Feb 17 14:00:34 2007 C:\WINDOWS\system32\NETAPI32.dll
        76f10000 45d70ad5 Feb 17 14:01:57 2007 C:\WINDOWS\system32\WLDAP32.dll
        77b90000 45d70ac8 Feb 17 14:01:44 2007 C:\WINDOWS\system32\VERSION.dll
        71b70000 45d70acb Feb 17 14:01:47 2007 C:\WINDOWS\system32\UxTheme.dll
        77420000 45d70a05 Feb 17 13:58:29 2007 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.3790.3959_x-ww_D8713E55\comctl32.dll
        75e60000 45d70a36 Feb 17 13:59:18 2007 C:\WINDOWS\system32\apphelp.dll
        777b0000 45d70a3b Feb 17 13:59:23 2007 C:\WINDOWS\system32\CLBCatQ.DLL
        77010000 45d70a76 Feb 17 14:00:22 2007 C:\WINDOWS\system32\COMRes.dll
        77b00000 45d70a88 Feb 17 14:00:40 2007 C:\WINDOWS\System32\cscui.dll
```

```
        76520000 45d70a87 Feb 17 14:00:39 2007 C:\WINDOWS\System32\CSCDLL.dll
        5efa0000 45d70ac4 Feb 17 14:01:40 2007 C:\WINDOWS\system32\themeui.dll
        76280000 3e80249f Mar 25 09:42:55 2003 C:\WINDOWS\system32\MSIMG32.dll
         1110000 45d69418 Feb 17 05:35:20 2007 C:\WINDOWS\system32\xpsp2res.dll
        76920000 45d70ac8 Feb 17 14:01:44 2007 C:\WINDOWS\system32\USERENV.dll
        7e020000 45d70aa8 Feb 17 14:01:12 2007 C:\WINDOWS\system32\SAMLIB.dll
        768e0000 45d70a54 Feb 17 13:59:48 2007 C:\WINDOWS\system32\LINKINFO.dll
        768f0000 45d70ab3 Feb 17 14:01:23 2007 C:\WINDOWS\system32\ntshrui.dll
        770e0000 45d70ab3 Feb 17 14:01:23 2007 C:\WINDOWS\system32\SETUPAPI.dll
        772c0000 45d70ac4 Feb 17 14:01:40 2007 C:\WINDOWS\system32\urlmon.dll
        771f0000 45d70ace Feb 17 14:01:50 2007 C:\WINDOWS\system32\WINSTA.dll
        76300000 45d70a8a Feb 17 14:00:42 2007 C:\WINDOWS\system32\NETSHELL.dll
        76e30000 45d70abb Feb 17 14:01:31 2007 C:\WINDOWS\system32\rtutils.dll
        76b80000 45d70a7f Feb 17 14:00:31 2007 C:\WINDOWS\system32\credui.dll
        71c00000 45d70ae9 Feb 17 14:02:17 2007 C:\WINDOWS\system32\WS2_32.dll
        71bf0000 45d70aea Feb 17 14:02:18 2007 C:\WINDOWS\system32\WS2HELP.dll
        76a80000 3e80249c Mar 25 09:42:52 2003 C:\WINDOWS\system32\ATL.DLL
        76cf0000 45d70a6c Feb 17 14:00:12 2007 C:\WINDOWS\system32\iphlpapi.dll
        76b70000 45d70ab5 Feb 17 14:01:25 2007 C:\WINDOWS\system32\PSAPI.DLL
        74de0000 45d70a43 Feb 17 13:59:31 2007 C:\WINDOWS\system32\CLUSAPI.dll
        74920000 45d70ade Feb 17 14:02:06 2007 C:\WINDOWS\system32\webcheck.dll
        71bb0000 3e8024be Mar 25 09:43:26 2003 C:\WINDOWS\system32\WSOCK32.dll
        748f0000 45d70af6 Feb 17 14:02:30 2007 C:\WINDOWS\system32\stobject.dll
        748e0000 45d70a15 Feb 17 13:58:45 2007 C:\WINDOWS\system32\BatMeter.dll
        748c0000 45d70aaf Feb 17 14:01:19 2007 C:\WINDOWS\system32\POWRPROF.dll
        76f00000 45d70af7 Feb 17 14:02:31 2007 C:\WINDOWS\system32\WTSAPI32.dll
        10000000 40c8fe08 Jun 11 01:34:16 2004 C:\Program Files\VMware\VMware Tools\hook.dll
        745e0000 45d70ad6 Feb 17 14:01:58 2007 C:\WINDOWS\system32\msi.dll
        71bd0000 45d70a84 Feb 17 14:00:36 2007 C:\WINDOWS\system32\MPR.dll
        75e90000 45d70a7c Feb 17 14:00:28 2007 C:\WINDOWS\System32\drprov.dll
        5f120000 45d70aaa Feb 17 14:01:14 2007 C:\WINDOWS\System32\ntlanman.dll
        5f8a0000 3e80253d Mar 25 09:45:33 2003 C:\WINDOWS\System32\NETUI0.dll
        5f860000 3e80253e Mar 25 09:45:34 2003 C:\WINDOWS\System32\NETUI1.dll
        75ea0000 45d70a2c Feb 17 13:59:08 2007 C:\WINDOWS\System32\davclnt.dll
         13e0000 40c8fe33 Jun 11 01:34:59 2004 C:\WINDOWS\System32\hgfs1.dll
        72490000 3e8024b9 Mar 25 09:43:21 2003 C:\WINDOWS\system32\browselc.dll
        77530000 45d70a06 Feb 17 13:58:30 2007 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_5.82.3790.3959_x-ww_78FCF8D0\COMCTL32.dll
          910000 3a9fc7f3 Mar 02 16:18:59 2001 C:\Program Files\Adobe\Acrobat
5.0\Reader\ActiveX\AcroIEHelper.ocx
        75da0000 45d70afe Feb 17 14:02:38 2007 C:\WINDOWS\system32\SXS.DLL
        77210000 45d70aee Feb 17 14:02:22 2007 C:\WINDOWS\system32\WININET.dll
        74540000 45d70a6f Feb 17 14:00:15 2007 C:\WINDOWS\system32\MLANG.dll
        76050000 3e8024a0 Mar 25 09:42:56 2003 C:\WINDOWS\system32\shdoclc.dll
        72470000 45d70b1a Feb 17 14:03:06 2007 C:\WINDOWS\system32\mydocs.dll
    SubSystemData:     00000000
    ProcessHeap:       00090000
    ProcessParameters: 00020000
    WindowTitle:  'C:\WINDOWS\Explorer.EXE'
    ImageFile:    'C:\WINDOWS\Explorer.EXE'
    CommandLine:  'C:\WINDOWS\Explorer.EXE'
    DllPath:
'C:\WINDOWS;C:\WINDOWS\system32;C:\WINDOWS\system;C:\WINDOWS;.;C:\WINDOWS\system32;C:\WINDOWS;C:\WI
NDOWS\System32\Wbem'
    Environment:  00010000
        ALLUSERSPROFILE=C:\Documents and Settings\All Users
        APPDATA=C:\Documents and Settings\Administrator\Application Data
        ClusterLog=C:\WINDOWS\Cluster\cluster.log
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\WINDOWS\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        HOMEDRIVE=C:
        HOMEPATH=\Documents and Settings\Administrator
        LOGONSERVER=\\COMPUTERNAME
        NUMBER_OF_PROCESSORS=1
        OS=Windows_NT
        Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
        PROCESSOR_ARCHITECTURE=x86
```

```
        PROCESSOR_IDENTIFIER=x86 Family 15 Model 5 Stepping 10, AuthenticAMD
        PROCESSOR_LEVEL=15
        PROCESSOR_REVISION=050a
        ProgramFiles=C:\Program Files
        SESSIONNAME=Console
        SystemDrive=C:
        SystemRoot=C:\WINDOWS
        TEMP=C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp
        TMP=C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp
        USERDOMAIN=COMPUTERNAME
        USERNAME=Administrator
        USERPROFILE=C:\Documents and Settings\Administrator
        windir=C:\WINDOWS


        THREAD 86080380  Cid 035c.0234  Teb: 7ffdf000 Win32Thread: e17f7648 WAIT: (Unknown)
UserMode Non-Alertable
            85d46330  SynchronizationEvent
        Not impersonating
        DeviceMap                 e249e270
        Owning Process            85d5ed88       Image:         explorer.exe
        Wait Start TickCount      97170          Ticks: 18798 (0:00:04:53.718)
        Context Switch Count      838                 LargeStack
        UserTime                  00:00:00.093
        KernelTime                00:00:02.531
        Win32 Start Address Explorer!ModuleEntry (0x010148a4)
        Start Address kernel32!BaseProcessStartThunk (0x77e617f8)
        Stack Init f64ed000 Current f64ecc68 Base f64ed000 Limit f64e7000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f64ecc80 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f64ecc98 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f64eccdc bf89b1c3 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f64ecd38 bf89e033 win32k!xxxSleepThread+0x1be (FPO: [Non-Fpo])
        f64ecd4c bf89e9f1 win32k!xxxRealWaitMessageEx+0x12 (FPO: [Non-Fpo])
        f64ecd5c 80883908 win32k!NtUserWaitMessage+0x14 (FPO: [0,0,0])
        f64ecd5c 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f64ecd64)
        0007feec 7739bf53 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0007ff08 7c8fadbd USER32!NtUserWaitMessage+0xc
        0007ff14 0100fff1 SHELL32!SHDesktopMessageLoop+0x24 (FPO: [Non-Fpo])
        0007ff5c 0101490c Explorer!ExplorerWinMain+0x2c4 (FPO: [Non-Fpo])
        0007ffc0 77e6f23b Explorer!ModuleEntry+0x6d (FPO: [Non-Fpo])
        0007fff0 00000000 kernel32!BaseProcessStart+0x23 (FPO: [Non-Fpo])

        THREAD 85d6f368  Cid 035c.03b0  Teb: 7ffdb000 Win32Thread: e1081ea8 WAIT: (Unknown)
UserMode Non-Alertable
            85d5ed58  SynchronizationEvent
        Not impersonating
        DeviceMap                 e249e270
        Owning Process            85d5ed88       Image:         explorer.exe
        Wait Start TickCount      115811         Ticks: 157 (0:00:00:02.453)
        Context Switch Count      2464                LargeStack
        UserTime                  00:00:00.046
        KernelTime                00:00:02.343
        Win32 Start Address SHLWAPI!WrapperThreadProc (0x77da3ea5)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f683e000 Current f683dc68 Base f683e000 Limit f6838000 Call 0
        Priority 11 BasePriority 9 PriorityDecrement 0
        ChildEBP RetAddr
        f683dc80 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f683dc98 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f683dcdc bf89b1c3 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f683dd38 bf89e033 win32k!xxxSleepThread+0x1be (FPO: [Non-Fpo])
        f683dd4c bf89e9f1 win32k!xxxRealWaitMessageEx+0x12 (FPO: [Non-Fpo])
        f683dd5c 80883908 win32k!NtUserWaitMessage+0x14 (FPO: [0,0,0])
        f683dd5c 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f683dd64)
        00faff14 7739bf53 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00faff48 010122b6 USER32!NtUserWaitMessage+0xc
        00faff54 77da3f12 Explorer!CTray::MainThreadProc+0x29 (FPO: [Non-Fpo])
```

```
        00faffb8 77e64829 SHLWAPI!WrapperThreadProc+0x94 (FPO: [Non-Fpo])
        00faffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85d6fdb0  Cid 035c.03d8  Teb: 7ffd9000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            85d6fe28  NotificationTimer
        Not impersonating
        DeviceMap                 e249e270
        Owning Process            85d5ed88       Image:         explorer.exe
        Wait Start TickCount      91738          Ticks: 24230 (0:00:06:18.593)
        Context Switch Count      10
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!RtlpTimerThread (0x7c83d3dd)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6459000 Current f6458c98 Base f6459000 Limit f6456000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6458cb0 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6458cc8 80827e1e nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6458d0c 8098c418 nt!KeDelayExecutionThread+0x254 (FPO: [Non-Fpo])
        f6458d54 80883908 nt!NtDelayExecution+0x84 (FPO: [Non-Fpo])
        f6458d54 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6458d64)
        00feff9c 7c826f4b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00feffa0 7c83d424 ntdll!NtDelayExecution+0xc (FPO: [2,0,0])
        00feffb8 77e64829 ntdll!RtlpTimerThread+0x47 (FPO: [Non-Fpo])
        00feffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85d6f8d0  Cid 035c.040c  Teb: 7ffd7000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            862bb8b0  NotificationTimer
            862d1fc0  SynchronizationEvent
            863c4020  NotificationEvent
        Not impersonating
        DeviceMap                 e249e270
        Owning Process            85d5ed88       Image:         explorer.exe
        Wait Start TickCount      20602          Ticks: 95366 (0:00:24:50.093)
        Context Switch Count      3
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address ntdll!RtlpWaitThread (0x7c83c643)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f63d5000 Current f63d4914 Base f63d5000 Limit f63d2000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f63d492c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f63d4944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f63d4978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f63d4bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f63d4d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f63d4d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f63d4d64)
        0145fcec 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0145fcf0 7c83c78e ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0145ffb8 77e64829 ntdll!RtlpWaitThread+0x161 (FPO: [Non-Fpo])
        0145ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d6f660  Cid 035c.0414  Teb: 7ffd6000 Win32Thread: e1101ea8 WAIT: (Unknown)
UserMode Alertable
            862e9c14  NotificationEvent
            860c717c  NotificationEvent
            85d8b914  NotificationEvent
            85d87fec  NotificationEvent
            862c6884  NotificationEvent
            862f0d84  NotificationEvent
            85d42994  NotificationEvent
            8630240c  NotificationEvent
            862d1c1c  NotificationEvent
            862edae8  SynchronizationEvent
        IRP List:
            860b20d8: (0006,01b4) Flags: 00000000  Mdl: 00000000
            863e7c88: (0006,01b4) Flags: 00000000  Mdl: 00000000
            85d57970: (0006,01b4) Flags: 00000000  Mdl: 00000000
            864a0e48: (0006,01b4) Flags: 00000000  Mdl: 00000000
            85d57d38: (0006,01b4) Flags: 00000000  Mdl: 00000000
            862bf5f0: (0006,01b4) Flags: 00000000  Mdl: 00000000
            85d45008: (0006,01b4) Flags: 00000000  Mdl: 00000000
            85d452d8: (0006,01b4) Flags: 00000000  Mdl: 00000000
            860bebd8: (0006,01b4) Flags: 00000000  Mdl: 00000000
        Not impersonating
        DeviceMap                 e249e270
        Owning Process            85d5ed88       Image:         explorer.exe
        Wait Start TickCount      95879          Ticks: 20089 (0:00:05:13.890)
        Context Switch Count      453                 LargeStack
        UserTime                  00:00:00.015
        KernelTime                00:00:00.140
        Win32 Start Address SHLWAPI!WrapperThreadProc (0x77da3ea5)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6355000 Current f6354914 Base f6355000 Limit f6351000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f635492c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6354944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6354978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6354bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6354d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6354d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6354d64)
        014afd24 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        014afd28 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        014afdd0 7739bbd1 kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        014afe2c 7c919b2e USER32!RealMsgWaitForMultipleObjectsEx+0x141 (FPO: [Non-Fpo])
        014aff50 7c8f7ada SHELL32!CChangeNotify::_MessagePump+0x3b (FPO: [Non-Fpo])
        014aff54 77da3f12 SHELL32!CChangeNotify::ThreadProc+0x1e (FPO: [1,0,0])
        014affb8 77e64829 SHLWAPI!WrapperThreadProc+0x94 (FPO: [Non-Fpo])
        014affec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 865aca40  Cid 035c.0540  Teb: 7ffad000 Win32Thread: e1142b88 WAIT: (Unknown)
UserMode Non-Alertable
            865ac6d0  SynchronizationEvent
        Not impersonating
        DeviceMap                 e249e270
        Owning Process            85d5ed88       Image:         explorer.exe
        Wait Start TickCount      94484          Ticks: 21484 (0:00:05:35.687)
        Context Switch Count      467                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.406
        Win32 Start Address stobject!CSysTray::SysTrayThreadProc (0x748f26e4)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f62c5000 Current f62c4bc4 Base f62c5000 Limit f62c1000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f62c4bdc 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f62c4bf4 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f62c4c38 bf89b1c3 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f62c4c94 bf89b986 win32k!xxxSleepThread+0x1be (FPO: [Non-Fpo])
        f62c4cec bf89da22 win32k!xxxRealInternalGetMessage+0x46a (FPO: [Non-Fpo])
        f62c4d4c 80883908 win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        f62c4d4c 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f62c4d64)
        0177fcf8 7739c811 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0177fd18 748f15ae USER32!NtUserGetMessage+0xc
        0177fd90 748f2733 stobject!SysTrayMain+0x180 (FPO: [Non-Fpo])
        0177ffb8 77e64829 stobject!CSysTray::SysTrayThreadProc+0x4f (FPO: [Non-Fpo])
        0177ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 864a1a30  Cid 035c.05d0  Teb: 7ffab000 Win32Thread: e13024f0 WAIT: (Unknown)
UserMode Non-Alertable
            85d8bd10  Semaphore Limit 0x7fffffff
            864a1aa8  NotificationTimer
        Not impersonating
        DeviceMap                 e249e270
        Owning Process            85d5ed88       Image:         explorer.exe
        Wait Start TickCount      114447         Ticks: 1521 (0:00:00:23.765)
        Context Switch Count      69                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6395000 Current f6394c24 Base f6395000 Limit f6392000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f6394c3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6394c54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6394c98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6394d48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f6394d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6394d64)
        017bfe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        017bfe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        017bff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        017bff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        017bffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        017bffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        017bffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d84db0  Cid 035c.06e0  Teb: 7ffde000 Win32Thread: e251acb0 WAIT: (Unknown)
UserMode Non-Alertable
            85dbcd00  SynchronizationEvent
        Not impersonating
        DeviceMap                 e249e270
        Owning Process            85d5ed88       Image:         explorer.exe
        Wait Start TickCount      108687         Ticks: 7281 (0:00:01:53.765)
        Context Switch Count      11293                 LargeStack
        UserTime                  00:00:00.484
        KernelTime                00:00:03.671
        Win32 Start Address BROWSEUI!BrowserProtectedThreadProc (0x75ec1c3f)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f619d000 Current f619cc68 Base f619d000 Limit f619a000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f619cc80 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f619cc98 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f619ccdc bf89b1c3 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f619cd38 bf89e033 win32k!xxxSleepThread+0x1be (FPO: [Non-Fpo])
        f619cd4c bf89e9f1 win32k!xxxRealWaitMessageEx+0x12 (FPO: [Non-Fpo])
        f619cd5c 80883908 win32k!NtUserWaitMessage+0x14 (FPO: [0,0,0])
        f619cd5c 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f619cd64)
        00effccc 7739bf53 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00efff2c 75ec1c83 USER32!NtUserWaitMessage+0xc
        00efffb8 77e64829 BROWSEUI!BrowserProtectedThreadProc+0x44 (FPO: [Non-Fpo])
        00efffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85d87698  Cid 035c.07c0  Teb: 7ffdc000 Win32Thread: e117e7e0 WAIT: (Unknown)
UserMode Non-Alertable
            862cd8c0  QueueObject
            85d87710  NotificationTimer
        Not impersonating
        DeviceMap                 e249e270
        Owning Process            85d5ed88       Image:         explorer.exe
        Wait Start TickCount      113768         Ticks: 2200 (0:00:00:34.375)
        Context Switch Count      341                 LargeStack
        UserTime                  00:00:00.015
        KernelTime                00:00:00.109
        Win32 Start Address ntdll!RtlpWorkerThread (0x7c839efb)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6db8000 Current f6db7c4c Base f6db8000 Limit f6db4000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f6db7c64 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6db7c7c 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6db7cc4 808e55e2 nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
        f6db7d48 80883908 nt!NtRemoveIoCompletion+0xdc (FPO: [Non-Fpo])
        f6db7d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6db7d64)
        01b0ff70 7c8277db ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01b0ff74 7c839f38 ntdll!ZwRemoveIoCompletion+0xc (FPO: [5,0,0])
        01b0ffb8 77e64829 ntdll!RtlpWorkerThread+0x3d (FPO: [Non-Fpo])
        01b0ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 85d3d020  Cid 035c.0860  Teb: 7ffdd000 Win32Thread: e13423b0 WAIT: (Unknown)
UserMode Non-Alertable
            85d8bd10  Semaphore Limit 0x7fffffff
            85d3d098  NotificationTimer
        Not impersonating
        DeviceMap                 e249e270
        Owning Process            85d5ed88       Image:         explorer.exe
        Wait Start TickCount      114447         Ticks: 1521 (0:00:00:23.765)
        Context Switch Count      9                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6da8000 Current f6da7c24 Base f6da8000 Limit f6da5000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f6da7c3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6da7c54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6da7c98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6da7d48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f6da7d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6da7d64)
        015ffe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        015ffe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        015fff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        015fff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        015fffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        015fffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        015fffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

VMwareTray process

```
PROCESS 865add88  SessionId: 0  Cid: 05dc    Peb: 7ffd7000  ParentCid: 035c
    DirBase: 3af1a320  ObjectTable: e114a908  HandleCount:  46.
    Image: VMwareTray.exe
    VadRoot 865accd8 Vads 59 Clone 0 Private 141. Modified 0. Locked 0.
    DeviceMap e249e270
    Token                             e1142d10
    ElapsedTime                       00:27:51.672
    UserTime                          00:00:00.031
    KernelTime                        00:00:00.515
    QuotaPoolUsage[PagedPool]         58052
    QuotaPoolUsage[NonPagedPool]      2360
    Working Set Sizes (now,min,max)  (780, 50, 345) (3120KB, 200KB, 1380KB)
    PeakWorkingSetSize                780
    VirtualSize                       31 Mb
    PeakVirtualSize                   38 Mb
    PageFaultCount                    814
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      204

    Setting context for this process...
.process /p /r ffffffff865add88

    !peb
PEB at 7ffd7000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00400000
    Ldr                       7c8877e0
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00141f18 . 0014cd38
    Ldr.InLoadOrderModuleList:           00141eb0 . 0014cd28
    Ldr.InMemoryOrderModuleList:         00141eb8 . 0014cd30
            Base TimeStamp                     Module
          400000 40c8fe11 Jun 11 01:34:25 2004 C:\Program Files\VMware\VMware Tools\VMwareTray.exe
        7c800000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\ntdll.dll
        77e40000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\kernel32.dll
        77ba0000 45d70b06 Feb 17 14:02:46 2007 C:\WINDOWS\system32\MSVCRT.dll
        10000000 40c8fe05 Jun 11 01:34:13 2004 C:\Program Files\VMware\VMware
Tools\VMControlPanel.cpl
        73eb0000 45d70a63 Feb 17 14:00:03 2007 C:\WINDOWS\system32\MFC42.DLL
        77380000 45d70ac7 Feb 17 14:01:43 2007 C:\WINDOWS\system32\USER32.dll
        77c00000 45d70a3e Feb 17 13:59:26 2007 C:\WINDOWS\system32\GDI32.dll
        77f50000 45d70a26 Feb 17 13:59:02 2007 C:\WINDOWS\system32\ADVAPI32.dll
        77c50000 45d70aaa Feb 17 14:01:14 2007 C:\WINDOWS\system32\RPCRT4.dll
        76f50000 45d70ac3 Feb 17 14:01:39 2007 C:\WINDOWS\system32\Secur32.dll
        77670000 45d70aa5 Feb 17 14:01:09 2007 C:\WINDOWS\system32\ole32.dll
        77d00000 45d70aa6 Feb 17 14:01:10 2007 C:\WINDOWS\system32\OLEAUT32.dll
        77210000 45d70aee Feb 17 14:02:22 2007 C:\WINDOWS\system32\WININET.dll
        77da0000 45d70ac0 Feb 17 14:01:36 2007 C:\WINDOWS\system32\SHLWAPI.dll
        761b0000 45d70a80 Feb 17 14:00:32 2007 C:\WINDOWS\system32\CRYPT32.dll
        76190000 45d70aac Feb 17 14:01:16 2007 C:\WINDOWS\system32\MSASN1.dll
        71bb0000 3e8024be Mar 25 09:43:26 2003 C:\WINDOWS\system32\WSOCK32.dll
        71c00000 45d70ae9 Feb 17 14:02:17 2007 C:\WINDOWS\system32\WS2_32.dll
        71bf0000 45d70aea Feb 17 14:02:18 2007 C:\WINDOWS\system32\WS2HELP.dll
        48890000 45d70ae1 Feb 17 14:02:09 2007 C:\WINDOWS\system32\ODBC32.dll
        77530000 45d70a06 Feb 17 13:58:30 2007 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_5.82.3790.3959_x-ww_78FCF8D0\COMCTL32.dll
        7c8d0000 45d70abb Feb 17 14:01:31 2007 C:\WINDOWS\system32\SHELL32.dll
        762b0000 45d70a72 Feb 17 14:00:18 2007 C:\WINDOWS\system32\comdlg32.dll
        77420000 45d70a05 Feb 17 13:58:29 2007 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.3790.3959_x-ww_D8713E55\comctl32.dll
           3e0000 45d684b8 Feb 17 04:29:44 2007 C:\WINDOWS\system32\odbcint.dll
    SubSystemData:     00000000
```

```
    ProcessHeap:       00140000
    ProcessParameters: 00020000
    WindowTitle:  'C:\Program Files\VMware\VMware Tools\VMwareTray.exe'
    ImageFile:    'C:\Program Files\VMware\VMware Tools\VMwareTray.exe'
    CommandLine:  '"C:\Program Files\VMware\VMware Tools\VMwareTray.exe" '
    DllPath:      'C:\Program Files\VMware\VMware
Tools;C:\WINDOWS\system32;C:\WINDOWS\system;C:\WINDOWS;.;C:\Program Files\VMware\VMware
Tools\;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem'
    Environment:  00010000
        ALLUSERSPROFILE=C:\Documents and Settings\All Users
        APPDATA=C:\Documents and Settings\Administrator\Application Data
        ClusterLog=C:\WINDOWS\Cluster\cluster.log
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\WINDOWS\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        HOMEDRIVE=C:
        HOMEPATH=\Documents and Settings\Administrator
        LOGONSERVER=\\COMPUTERNAME
        NUMBER_OF_PROCESSORS=1
        OS=Windows_NT
        Path=C:\Program Files\VMware\VMware
Tools\;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 15 Model 5 Stepping 10, AuthenticAMD
        PROCESSOR_LEVEL=15
        PROCESSOR_REVISION=050a
        ProgramFiles=C:\Program Files
        SESSIONNAME=Console
        SystemDrive=C:
        SystemRoot=C:\WINDOWS
        TEMP=C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp
        TMP=C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp
        USERDOMAIN=COMPUTERNAME
        USERNAME=Administrator
        USERPROFILE=C:\Documents and Settings\Administrator
        windir=C:\WINDOWS


        THREAD 860b3bf0  Cid 05dc.0600  Teb: 7ffdf000 Win32Thread: e1251868 WAIT: (Unknown)
UserMode Non-Alertable
            860c9db0  SynchronizationEvent
        Not impersonating
        DeviceMap                 e249e270
        Owning Process            865add88       Image:         VMwareTray.exe
        Wait Start TickCount      94484          Ticks: 21484 (0:00:05:35.687)
        Context Switch Count      75                 LargeStack
        UserTime                  00:00:00.031
        KernelTime                00:00:00.484
        Win32 Start Address VMwareTray (0x00401876)
        Start Address kernel32!BaseProcessStartThunk (0x77e617f8)
        Stack Init f6285000 Current f6284bc4 Base f6285000 Limit f6282000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6284bdc 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6284bf4 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6284c38 bf89b1c3 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6284c94 bf89b986 win32k!xxxSleepThread+0x1be (FPO: [Non-Fpo])
        f6284cec bf89da22 win32k!xxxRealInternalGetMessage+0x46a (FPO: [Non-Fpo])
        f6284d4c 80883908 win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        f6284d4c 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6284d64)
        0012fe84 7739c811 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0012feac 00401277 USER32!NtUserGetMessage+0xc
        0012feec 00401148 VMwareTray+0x1277
        0012ff24 004019aa VMwareTray+0x1148
        0012ffc0 77e6f23b VMwareTray+0x19aa
        0012fff0 00000000 kernel32!BaseProcessStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 864a0980  Cid 05dc.0598  Teb: 7ffdd000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            864a09f8  NotificationTimer
        Not impersonating
        DeviceMap                 e249e270
        Owning Process            865add88       Image:         VMwareTray.exe
        Wait Start TickCount      115949         Ticks: 19 (0:00:00:00.296)
        Context Switch Count      2700
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address VMwareTray (0x00401640)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f63c5000 Current f63c4c98 Base f63c5000 Limit f63c2000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f63c4cb0 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f63c4cc8 80827e1e nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f63c4d0c 8098c418 nt!KeDelayExecutionThread+0x254 (FPO: [Non-Fpo])
        f63c4d54 80883908 nt!NtDelayExecution+0x84 (FPO: [Non-Fpo])
        f63c4d54 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f63c4d64)
        00d2ff24 7c826f4b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        00d2ff28 77e41ed1 ntdll!NtDelayExecution+0xc (FPO: [2,0,0])
        00d2ff90 77e424ed kernel32!SleepEx+0x68 (FPO: [Non-Fpo])
        00d2ffa0 00401687 kernel32!Sleep+0xf (FPO: [Non-Fpo])
        00d2ffb8 77e64829 VMwareTray+0x1687
        00d2ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

VMwareUser process

```
PROCESS 85d847e8  SessionId: 0  Cid: 0610    Peb: 7ffd5000  ParentCid: 035c
    DirBase: 3af1a340  ObjectTable: e1056180  HandleCount:  44.
    Image: VMwareUser.exe
    VadRoot 860b3878 Vads 59 Clone 0 Private 150. Modified 0. Locked 0.
    DeviceMap e249e270
    Token                             e116b670
    ElapsedTime                       00:27:50.906
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.468
    QuotaPoolUsage[PagedPool]         58100
    QuotaPoolUsage[NonPagedPool]      2360
    Working Set Sizes (now,min,max)  (779, 50, 345) (3116KB, 200KB, 1380KB)
    PeakWorkingSetSize                781
    VirtualSize                       30 Mb
    PeakVirtualSize                   38 Mb
    PageFaultCount                    814
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      214

    Setting context for this process...
.process /p /r ffffffff85d847e8

    !peb
PEB at 7ffd5000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00400000
    Ldr                       7c8877e0
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00141f18 . 0014cdc8
    Ldr.InLoadOrderModuleList:           00141eb0 . 0014cdb8
    Ldr.InMemoryOrderModuleList:         00141eb8 . 0014cdc0
            Base TimeStamp                     Module
          400000 40c8fe10 Jun 11 01:34:24 2004 C:\Program Files\VMware\VMware Tools\VMwareUser.exe
        7c800000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\ntdll.dll
        77e40000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\kernel32.dll
        73eb0000 45d70a63 Feb 17 14:00:03 2007 C:\WINDOWS\system32\MFC42.DLL
        77ba0000 45d70b06 Feb 17 14:02:46 2007 C:\WINDOWS\system32\msvcrt.dll
        77380000 45d70ac7 Feb 17 14:01:43 2007 C:\WINDOWS\system32\USER32.dll
        77c00000 45d70a3e Feb 17 13:59:26 2007 C:\WINDOWS\system32\GDI32.dll
        77f50000 45d70a26 Feb 17 13:59:02 2007 C:\WINDOWS\system32\ADVAPI32.dll
        77c50000 45d70aaa Feb 17 14:01:14 2007 C:\WINDOWS\system32\RPCRT4.dll
        76f50000 45d70ac3 Feb 17 14:01:39 2007 C:\WINDOWS\system32\Secur32.dll
        77670000 45d70aa5 Feb 17 14:01:09 2007 C:\WINDOWS\system32\ole32.dll
        77d00000 45d70aa6 Feb 17 14:01:10 2007 C:\WINDOWS\system32\OLEAUT32.dll
        77210000 45d70aee Feb 17 14:02:22 2007 C:\WINDOWS\system32\WININET.dll
        77da0000 45d70ac0 Feb 17 14:01:36 2007 C:\WINDOWS\system32\SHLWAPI.dll
        761b0000 45d70a80 Feb 17 14:00:32 2007 C:\WINDOWS\system32\CRYPT32.dll
        76190000 45d70aac Feb 17 14:01:16 2007 C:\WINDOWS\system32\MSASN1.dll
        71bb0000 3e8024be Mar 25 09:43:26 2003 C:\WINDOWS\system32\WSOCK32.dll
        71c00000 45d70ae9 Feb 17 14:02:17 2007 C:\WINDOWS\system32\WS2_32.dll
        71bf0000 45d70aea Feb 17 14:02:18 2007 C:\WINDOWS\system32\WS2HELP.dll
        48890000 45d70ae1 Feb 17 14:02:09 2007 C:\WINDOWS\system32\ODBC32.dll
        77530000 45d70a06 Feb 17 13:58:30 2007 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_5.82.3790.3959_x-ww_78FCF8D0\COMCTL32.dll
        7c8d0000 45d70abb Feb 17 14:01:31 2007 C:\WINDOWS\system32\SHELL32.dll
        762b0000 45d70a72 Feb 17 14:00:18 2007 C:\WINDOWS\system32\comdlg32.dll
        76aa0000 45d70af0 Feb 17 14:02:24 2007 C:\WINDOWS\system32\WINMM.dll
        10000000 40c8fe08 Jun 11 01:34:16 2004 C:\Program Files\VMware\VMware Tools\hook.dll
        77420000 45d70a05 Feb 17 13:58:29 2007 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.3790.3959_x-ww_D8713E55\comctl32.dll
          3e0000 45d684b8 Feb 17 04:29:44 2007 C:\WINDOWS\system32\odbcint.dll
    SubSystemData:     00000000
```

```
    ProcessHeap:       00140000
    ProcessParameters: 00020000
    WindowTitle:  'C:\Program Files\VMware\VMware Tools\VMwareUser.exe'
    ImageFile:    'C:\Program Files\VMware\VMware Tools\VMwareUser.exe'
    CommandLine:  '"C:\Program Files\VMware\VMware Tools\VMwareUser.exe" '
    DllPath:      'C:\Program Files\VMware\VMware
Tools;C:\WINDOWS\system32;C:\WINDOWS\system;C:\WINDOWS;.;C:\Program Files\VMware\VMware
Tools\;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem'
    Environment:  00010000
        ALLUSERSPROFILE=C:\Documents and Settings\All Users
        APPDATA=C:\Documents and Settings\Administrator\Application Data
        ClusterLog=C:\WINDOWS\Cluster\cluster.log
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\WINDOWS\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        HOMEDRIVE=C:
        HOMEPATH=\Documents and Settings\Administrator
        LOGONSERVER=\\COMPUTERNAME
        NUMBER_OF_PROCESSORS=1
        OS=Windows_NT
        Path=C:\Program Files\VMware\VMware
Tools\;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 15 Model 5 Stepping 10, AuthenticAMD
        PROCESSOR_LEVEL=15
        PROCESSOR_REVISION=050a
        ProgramFiles=C:\Program Files
        SESSIONNAME=Console
        SystemDrive=C:
        SystemRoot=C:\WINDOWS
        TEMP=C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp
        TMP=C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp
        USERDOMAIN=COMPUTERNAME
        USERNAME=Administrator
        USERPROFILE=C:\Documents and Settings\Administrator
        windir=C:\WINDOWS


        THREAD 85d857d0  Cid 0610.045c  Teb: 7ffdf000 Win32Thread: e124f8f8 WAIT: (Unknown)
UserMode Non-Alertable
            864a1d58  SynchronizationEvent
            85d855b0  SynchronizationEvent
            85d85848  NotificationTimer
        Not impersonating
        DeviceMap                 e249e270
        Owning Process            85d847e8       Image:         VMwareUser.exe
        Wait Start TickCount      115962         Ticks: 6 (0:00:00:00.093)
        Context Switch Count      13962                LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.468
        Win32 Start Address VMwareUser (0x004056b8)
        Start Address kernel32!BaseProcessStartThunk (0x77e617f8)
        Stack Init f6295000 Current f6294914 Base f6295000 Limit f6291000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        ChildEBP RetAddr
        f629492c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6294944 808282b0 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6294978 80930d34 nt!KeWaitForMultipleObjects+0x320 (FPO: [Non-Fpo])
        f6294bf4 80930e96 nt!ObpWaitForMultipleObjects+0x202 (FPO: [Non-Fpo])
        f6294d48 80883908 nt!NtWaitForMultipleObjects+0xc8 (FPO: [Non-Fpo])
        f6294d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6294d64)
        0012fd60 7c827cfb ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0012fd64 77e6202c ntdll!NtWaitForMultipleObjects+0xc (FPO: [5,0,0])
        0012fe0c 7739bbd1 kernel32!WaitForMultipleObjectsEx+0x11a (FPO: [Non-Fpo])
        0012fe68 7739ce36 USER32!RealMsgWaitForMultipleObjectsEx+0x141 (FPO: [Non-Fpo])
        0012fe84 00401660 USER32!MsgWaitForMultipleObjects+0x1f (FPO: [Non-Fpo])
        0012fed8 004011e8 VMwareUser+0x1660
        0012ff24 004057ec VMwareUser+0x11e8
```

```
        0012ffc0 77e6f23b VMwareUser+0x57ec
        0012fff0 00000000 kernel32!BaseProcessStart+0x23 (FPO: [Non-Fpo])
```

Iexplore process

```
PROCESS 860af368  SessionId: 0  Cid: 0840    Peb: 7ffdf000  ParentCid: 035c
    DirBase: 3af1a380  ObjectTable: e127eca0  HandleCount: 299.
    Image: iexplore.exe
    VadRoot 85d45fd8 Vads 183 Clone 0 Private 1051. Modified 1116. Locked 0.
    DeviceMap e249e270
    Token                             e1314d10
    ElapsedTime                       00:05:37.031
    UserTime                          00:00:00.187
    KernelTime                        00:00:02.140
    QuotaPoolUsage[PagedPool]         108772
    QuotaPoolUsage[NonPagedPool]      9944
    Working Set Sizes (now,min,max)  (594, 50, 345) (2376KB, 200KB, 1380KB)
    PeakWorkingSetSize                3552
    VirtualSize                       69 Mb
    PeakVirtualSize                   78 Mb
    PageFaultCount                    5293
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      1510

    Setting context for this process...
.process /p /r ffffffff860af368

    !peb
PEB at 7ffdf000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00400000
    Ldr                       7c8877e0
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 00151f18 . 00241488
    Ldr.InLoadOrderModuleList:           00151eb0 . 00241478
    Ldr.InMemoryOrderModuleList:         00151eb8 . 00241480
            Base TimeStamp                     Module
          400000 45d69af1 Feb 17 06:04:33 2007 C:\Program Files\Internet Explorer\iexplore.exe
        7c800000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\ntdll.dll
        77e40000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\kernel32.dll
        77ba0000 45d70b06 Feb 17 14:02:46 2007 C:\WINDOWS\system32\msvcrt.dll
        77380000 45d70ac7 Feb 17 14:01:43 2007 C:\WINDOWS\system32\USER32.dll
        77c00000 45d70a3e Feb 17 13:59:26 2007 C:\WINDOWS\system32\GDI32.dll
        77f50000 45d70a26 Feb 17 13:59:02 2007 C:\WINDOWS\system32\ADVAPI32.dll
        77c50000 45d70aaa Feb 17 14:01:14 2007 C:\WINDOWS\system32\RPCRT4.dll
        76f50000 45d70ac3 Feb 17 14:01:39 2007 C:\WINDOWS\system32\Secur32.dll
        77da0000 45d70ac0 Feb 17 14:01:36 2007 C:\WINDOWS\system32\SHLWAPI.dll
        77980000 45d70aba Feb 17 14:01:30 2007 C:\WINDOWS\system32\SHDOCVW.dll
        761b0000 45d70a80 Feb 17 14:00:32 2007 C:\WINDOWS\system32\CRYPT32.dll
        76190000 45d70aac Feb 17 14:01:16 2007 C:\WINDOWS\system32\MSASN1.dll
        75360000 45d70a85 Feb 17 14:00:37 2007 C:\WINDOWS\system32\CRYPTUI.dll
        76bb0000 45d70acf Feb 17 14:01:51 2007 C:\WINDOWS\system32\WINTRUST.dll
        76c10000 45d70a5d Feb 17 13:59:57 2007 C:\WINDOWS\system32\imagehlp.dll
        77d00000 45d70aa6 Feb 17 14:01:10 2007 C:\WINDOWS\system32\OLEAUT32.dll
        77670000 45d70aa5 Feb 17 14:01:09 2007 C:\WINDOWS\system32\ole32.dll
        71c40000 45d70a82 Feb 17 14:00:34 2007 C:\WINDOWS\system32\NETAPI32.dll
        76f10000 45d70ad5 Feb 17 14:01:57 2007 C:\WINDOWS\system32\WLDAP32.dll
        77b90000 45d70ac8 Feb 17 14:01:44 2007 C:\WINDOWS\system32\VERSION.dll
        77420000 45d70a05 Feb 17 13:58:29 2007 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.3790.3959_x-ww_D8713E55\Comctl32.dll
        7c8d0000 45d70abb Feb 17 14:01:31 2007 C:\WINDOWS\system32\SHELL32.dll
        75eb0000 45d70a19 Feb 17 13:58:49 2007 C:\WINDOWS\system32\BROWSEUI.dll
```

```
        72490000 3e8024b9 Mar 25 09:43:21 2003 C:\WINDOWS\system32\browselc.dll
        77530000 45d70a06 Feb 17 13:58:30 2007 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_5.82.3790.3959_x-ww_78FCF8D0\COMCTL32.dll
        75e60000 45d70a36 Feb 17 13:59:18 2007 C:\WINDOWS\system32\apphelp.dll
        777b0000 45d70a3b Feb 17 13:59:23 2007 C:\WINDOWS\system32\CLBCatQ.DLL
        77010000 45d70a76 Feb 17 14:00:22 2007 C:\WINDOWS\system32\COMRes.dll
        76920000 45d70ac8 Feb 17 14:01:44 2007 C:\WINDOWS\system32\USERENV.dll
        71b70000 45d70acb Feb 17 14:01:47 2007 C:\WINDOWS\system32\UxTheme.dll
        77b00000 45d70a88 Feb 17 14:00:40 2007 C:\WINDOWS\System32\cscui.dll
        76520000 45d70a87 Feb 17 14:00:39 2007 C:\WINDOWS\System32\CSCDLL.dll
        770e0000 45d70ab3 Feb 17 14:01:23 2007 C:\WINDOWS\system32\SETUPAPI.dll
        772c0000 45d70ac4 Feb 17 14:01:40 2007 C:\WINDOWS\system32\urlmon.dll
        10000000 3a9fc7f3 Mar 02 16:18:59 2001 C:\Program Files\Adobe\Acrobat
5.0\Reader\ActiveX\AcroIEHelper.ocx
        75da0000 45d70afe Feb 17 14:02:38 2007 C:\WINDOWS\system32\SXS.DLL
          f10000 45d69418 Feb 17 05:35:20 2007 C:\WINDOWS\system32\xpsp2res.dll
        77210000 45d70aee Feb 17 14:02:22 2007 C:\WINDOWS\system32\WININET.dll
        76050000 3e8024a0 Mar 25 09:42:56 2003 C:\WINDOWS\system32\shdoclc.dll
        74540000 45d70a6f Feb 17 14:00:15 2007 C:\WINDOWS\system32\mlang.dll
        71bb0000 3e8024be Mar 25 09:43:26 2003 C:\WINDOWS\system32\wsock32.dll
        71c00000 45d70ae9 Feb 17 14:02:17 2007 C:\WINDOWS\system32\WS2_32.dll
        71bf0000 45d70aea Feb 17 14:02:18 2007 C:\WINDOWS\system32\WS2HELP.dll
        71b20000 45d70b0d Feb 17 14:02:53 2007 C:\WINDOWS\system32\mswsock.dll
        5f270000 45d70a4a Feb 17 13:59:38 2007 C:\WINDOWS\system32\hnetcfg.dll
        71ae0000 45d70af3 Feb 17 14:02:27 2007 C:\WINDOWS\System32\wshtcpip.dll
        745e0000 45d70ad6 Feb 17 14:01:58 2007 C:\WINDOWS\system32\msi.dll
        76e90000 45d70a9e Feb 17 14:01:02 2007 C:\WINDOWS\system32\RASAPI32.DLL
        76e40000 45d70aa3 Feb 17 14:01:07 2007 C:\WINDOWS\system32\rasman.dll
        76e60000 45d70abc Feb 17 14:01:32 2007 C:\WINDOWS\system32\TAPI32.dll
        76e30000 45d70abb Feb 17 14:01:31 2007 C:\WINDOWS\system32\rtutils.dll
        76aa0000 45d70af0 Feb 17 14:02:24 2007 C:\WINDOWS\system32\WINMM.dll
         13f0000 40c8fe08 Jun 11 01:34:16 2004 C:\Program Files\VMware\VMware Tools\hook.dll
        722f0000 45d70aae Feb 17 14:01:18 2007 C:\WINDOWS\system32\sensapi.dll
        76ed0000 45d70a64 Feb 17 14:00:04 2007 C:\WINDOWS\system32\DNSAPI.dll
        76f70000 45d70ac7 Feb 17 14:01:43 2007 C:\WINDOWS\System32\winrnr.dll
        76f80000 45d70a9d Feb 17 14:01:01 2007 C:\WINDOWS\system32\rasadhlp.dll
        7f9e0000 45d70ad4 Feb 17 14:01:56 2007 C:\WINDOWS\system32\mshtml.dll
        74490000 45d70ae1 Feb 17 14:02:09 2007 C:\WINDOWS\system32\msls31.dll
        76b70000 45d70ab5 Feb 17 14:01:25 2007 C:\WINDOWS\system32\PSAPI.DLL
        744c0000 45d70adb Feb 17 14:02:03 2007 C:\WINDOWS\system32\msimtf.dll
        4b3c0000 45d70ab2 Feb 17 14:01:22 2007 C:\WINDOWS\system32\MSCTF.dll
        76290000 45d70a5f Feb 17 13:59:59 2007 C:\WINDOWS\system32\IMM32.DLL
        71bd0000 45d70a84 Feb 17 14:00:36 2007 C:\WINDOWS\system32\MPR.dll
        75e90000 45d70a7c Feb 17 14:00:28 2007 C:\WINDOWS\System32\drprov.dll
        5f120000 45d70aaa Feb 17 14:01:14 2007 C:\WINDOWS\System32\ntlanman.dll
        5f8a0000 3e80253d Mar 25 09:45:33 2003 C:\WINDOWS\System32\NETUI0.dll
        5f860000 3e80253e Mar 25 09:45:34 2003 C:\WINDOWS\System32\NETUI1.dll
        7e020000 45d70aa8 Feb 17 14:01:12 2007 C:\WINDOWS\System32\SAMLIB.dll
        75ea0000 45d70a2c Feb 17 13:59:08 2007 C:\WINDOWS\System32\davclnt.dll
         20d0000 40c8fe33 Jun 11 01:34:59 2004 C:\WINDOWS\System32\hgfs1.dll
        76f90000 45d70a50 Feb 17 13:59:44 2007 C:\WINDOWS\system32\jscript.dll
        64610000 45d70a5e Feb 17 13:59:58 2007 C:\WINDOWS\system32\ImgUtil.dll
        5e120000 45d70aa7 Feb 17 14:01:11 2007 C:\WINDOWS\system32\pngfilt.dll
    SubSystemData:     00000000
    ProcessHeap:       00150000
    ProcessParameters: 00020000
    WindowTitle:  'C:\Documents and Settings\Administrator\Start Menu\Programs\Internet
Explorer.lnk'
    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'
    Environment:  00010000
        ALLUSERSPROFILE=C:\Documents and Settings\All Users
        APPDATA=C:\Documents and Settings\Administrator\Application Data
        ClusterLog=C:\WINDOWS\Cluster\cluster.log
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\WINDOWS\system32\cmd.exe
```

```
        FP_NO_HOST_CHECK=NO
        HOMEDRIVE=C:
        HOMEPATH=\Documents and Settings\Administrator
        LOGONSERVER=\\COMPUTERNAME
        NUMBER_OF_PROCESSORS=1
        OS=Windows_NT
        Path=C:\Program Files\Internet
Explorer;;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 15 Model 5 Stepping 10, AuthenticAMD
        PROCESSOR_LEVEL=15
        PROCESSOR_REVISION=050a
        ProgramFiles=C:\Program Files
        SESSIONNAME=Console
        SystemDrive=C:
        SystemRoot=C:\WINDOWS
        TEMP=C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp
        TMP=C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp
        USERDOMAIN=COMPUTERNAME
        USERNAME=Administrator
        USERPROFILE=C:\Documents and Settings\Administrator
        windir=C:\WINDOWS


        THREAD 862bcdb0  Cid 0840.0844  Teb: 7ffde000 Win32Thread: e118e930 WAIT: (Unknown)
UserMode Non-Alertable
            860affc0  SynchronizationEvent
        Not impersonating
        DeviceMap                 e249e270
        Owning Process            860af368       Image:         iexplore.exe
        Wait Start TickCount      95846          Ticks: 20122 (0:00:05:14.406)
        Context Switch Count      1232                LargeStack
        UserTime                  00:00:00.140
        KernelTime                00:00:01.562
        Win32 Start Address iexplore!WinMainCRTStartup (0x004025c2)
        Start Address kernel32!BaseProcessStartThunk (0x77e617f8)
        Stack Init f7577000 Current f7576c68 Base f7577000 Limit f7571000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f7576c80 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f7576c98 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f7576cdc bf89b1c3 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f7576d38 bf89e033 win32k!xxxSleepThread+0x1be (FPO: [Non-Fpo])
        f7576d4c bf89e9f1 win32k!xxxRealWaitMessageEx+0x12 (FPO: [Non-Fpo])
        f7576d5c 80883908 win32k!NtUserWaitMessage+0x14 (FPO: [0,0,0])
        f7576d5c 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f7576d64)
        0013eb38 7739bf53 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0013ed98 75ec1c83 USER32!NtUserWaitMessage+0xc
        0013ee24 75ec61ef BROWSEUI!BrowserProtectedThreadProc+0x44 (FPO: [Non-Fpo])
        0013fea8 779ba36e BROWSEUI!SHOpenFolderWindow+0x22c (FPO: [Non-Fpo])
        0013fec8 0040243d SHDOCVW!IEWinMain+0x129 (FPO: [Non-Fpo])
        0013ff1c 00402744 iexplore!WinMain+0x316 (FPO: [Non-Fpo])
        0013ffc0 77e6f23b iexplore!WinMainCRTStartup+0x182 (FPO: [Non-Fpo])
        0013fff0 00000000 kernel32!BaseProcessStart+0x23 (FPO: [Non-Fpo])
```

```
        THREAD 85d70db0  Cid 0840.084c  Teb: 7ffdc000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d8f5b8  Semaphore Limit 0x7fffffff
            85d70e28  NotificationTimer
        Not impersonating
        DeviceMap                 e249e270
        Owning Process            860af368       Image:         iexplore.exe
        Wait Start TickCount      106153         Ticks: 9815 (0:00:02:33.359)
        Context Switch Count      16
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x00002540
        LPC Server thread working on message Id 2540
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6401000 Current f6400c24 Base f6401000 Limit f63fe000 Call 0
        Priority 12 BasePriority 8 PriorityDecrement 3
        Kernel stack not resident.
        ChildEBP RetAddr
        f6400c3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6400c54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6400c98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6400d48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f6400d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6400d64)
        012dfe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        012dfe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        012dff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        012dff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        012dffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        012dffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        012dffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 85d68a80  Cid 0840.0854  Teb: 7ffda000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            86082ee0  NotificationEvent
            85d68af8  NotificationTimer
        IRP List:
            860b13e0: (0006,01b4) Flags: 00000070  Mdl: 00000000
        Not impersonating
        DeviceMap                 e249e270
        Owning Process            860af368       Image:         iexplore.exe
        Wait Start TickCount      95686          Ticks: 20282 (0:00:05:16.906)
        Context Switch Count      182
        UserTime                  00:00:00.015
        KernelTime                00:00:00.031
        Win32 Start Address WININET!ICAsyncThread::SelectThreadWrapper (0x77238da7)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6585000 Current f6584c78 Base f6585000 Limit f6582000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6584c90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6584ca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6584cec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6584d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f6584d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6584d64)
        0158fad4 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0158fad8 71b21af5 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        0158fb14 71b21a03 mswsock!SockWaitForSingleObject+0x19d (FPO: [Non-Fpo])
        0158fc04 71c0283c mswsock!WSPSelect+0x380 (FPO: [Non-Fpo])
        0158fc54 77226314 WS2_32!select+0xb9 (FPO: [Non-Fpo])
        0158ffb0 77238db4 WININET!ICAsyncThread::SelectThread+0x22a (FPO: [Non-Fpo])
        0158ffb8 77e64829 WININET!ICAsyncThread::SelectThreadWrapper+0xd (FPO: [Non-Fpo])
        0158ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 860827d8  Cid 0840.0858  Teb: 7ffd9000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Alertable
            86082850  NotificationTimer
        Not impersonating
        DeviceMap                 e249e270
        Owning Process            860af368       Image:         iexplore.exe
        Wait Start TickCount      95309          Ticks: 20659 (0:00:05:22.796)
        Context Switch Count      20
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address ntdll!RtlpTimerThread (0x7c83d3dd)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6a7b000 Current f6a7ac98 Base f6a7b000 Limit f6a78000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6a7acb0 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6a7acc8 80827e1e nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6a7ad0c 8098c418 nt!KeDelayExecutionThread+0x254 (FPO: [Non-Fpo])
        f6a7ad54 80883908 nt!NtDelayExecution+0x84 (FPO: [Non-Fpo])
        f6a7ad54 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6a7ad64)
        0168ff9c 7c826f4b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0168ffa0 7c83d424 ntdll!NtDelayExecution+0xc (FPO: [2,0,0])
        0168ffb8 77e64829 ntdll!RtlpTimerThread+0x47 (FPO: [Non-Fpo])
        0168ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 863957f8  Cid 0840.0864  Teb: 7ffd7000 Win32Thread: 00000000 WAIT: (Unknown)
UserMode Non-Alertable
            85d8f5b8  Semaphore Limit 0x7fffffff
            86395870  NotificationTimer
        Not impersonating
        DeviceMap                 e249e270
        Owning Process            860af368       Image:         iexplore.exe
        Wait Start TickCount      106675         Ticks: 9293 (0:00:02:25.203)
        Context Switch Count      6
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x00002565
        LPC Server thread working on message Id 2565
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6539000 Current f6538c24 Base f6539000 Limit f6536000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 1
        Kernel stack not resident.
        ChildEBP RetAddr
        f6538c3c 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6538c54 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6538c98 8091a5f1 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6538d48 80883908 nt!NtReplyWaitReceivePortEx+0x521 (FPO: [Non-Fpo])
        f6538d48 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6538d64)
        0188fe18 7c82783b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0188fe1c 77c885ac ntdll!NtReplyWaitReceivePortEx+0xc (FPO: [5,0,0])
        0188ff84 77c88792 RPCRT4!LRPC_ADDRESS::ReceiveLotsaCalls+0x198 (FPO: [Non-Fpo])
        0188ff8c 77c8872d RPCRT4!RecvLotsaCallsWrapper+0xd (FPO: [Non-Fpo])
        0188ffac 77c7b110 RPCRT4!BaseCachedThreadRoutine+0x9d (FPO: [Non-Fpo])
        0188ffb8 77e64829 RPCRT4!ThreadStartRoutine+0x1b (FPO: [Non-Fpo])
        0188ffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

```
        THREAD 8649b4a8  Cid 0840.0870  Teb: 7ffd5000 Win32Thread: e1856b48 WAIT: (Unknown)
UserMode Non-Alertable
            85d706a0  SynchronizationEvent
            8649b520  NotificationTimer
        Not impersonating
        DeviceMap                 e249e270
        Owning Process            860af368       Image:         iexplore.exe
        Wait Start TickCount      95322          Ticks: 20646 (0:00:05:22.593)
        Context Switch Count      26                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.015
        Win32 Start Address mshtml!CExecFT::StaticThreadProc (0x7fab0fc1)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6305000 Current f6304c78 Base f6305000 Limit f6301000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6304c90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6304ca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6304cec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6304d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f6304d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6304d64)
        01eaff08 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01eaff0c 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        01eaff7c 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        01eaff90 7fab0803 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        01eaffa8 7fab0ffc mshtml!CDwnTaskExec::ThreadExec+0xae (FPO: [0,0,0])
        01eaffb0 7fab0fce mshtml!CExecFT::ThreadProc+0x28 (FPO: [0,0,0])
        01eaffb8 77e64829 mshtml!CExecFT::StaticThreadProc+0xd (FPO: [Non-Fpo])
        01eaffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])

        THREAD 860ae608  Cid 0840.0874  Teb: 7ffd4000 Win32Thread: e12cb1f8 WAIT: (Unknown)
UserMode Non-Alertable
            863b3080  SynchronizationEvent
            860ae680  NotificationTimer
        Not impersonating
        DeviceMap                 e249e270
        Owning Process            860af368       Image:         iexplore.exe
        Wait Start TickCount      95334          Ticks: 20634 (0:00:05:22.406)
        Context Switch Count      129                LargeStack
        UserTime                  00:00:00.015
        KernelTime                00:00:00.062
        Win32 Start Address mshtml!CExecFT::StaticThreadProc (0x7fab0fc1)
        Start Address kernel32!BaseThreadStartThunk (0x77e617ec)
        Stack Init f6375000 Current f6374c78 Base f6375000 Limit f6371000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f6374c90 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f6374ca8 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f6374cec 80930ad8 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f6374d50 80883908 nt!NtWaitForSingleObject+0x9a (FPO: [Non-Fpo])
        f6374d50 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f6374d64)
        01faff08 7c827d0b ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        01faff0c 77e61d1e ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        01faff7c 77e61c8d kernel32!WaitForSingleObjectEx+0xac (FPO: [Non-Fpo])
        01faff90 7fab0803 kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
        01faffa8 7fab0ffc mshtml!CDwnTaskExec::ThreadExec+0xae (FPO: [0,0,0])
        01faffb0 7fab0fce mshtml!CExecFT::ThreadProc+0x28 (FPO: [0,0,0])
        01faffb8 77e64829 mshtml!CExecFT::StaticThreadProc+0xd (FPO: [Non-Fpo])
        01faffec 00000000 kernel32!BaseThreadStart+0x34 (FPO: [Non-Fpo])
```

Notepad process

```
PROCESS 85d4ad88  SessionId: 0  Cid: 0884    Peb: 7ffdd000  ParentCid: 035c
    DirBase: 3af1a3a0  ObjectTable: e139f3d0  HandleCount:  25.
    Image: notepad.exe
    VadRoot 863495e8 Vads 44 Clone 0 Private 92. Modified 2632. Locked 0.
    DeviceMap e249e270
    Token                             e13aa508
    ElapsedTime                       00:05:14.937
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.031
    QuotaPoolUsage[PagedPool]         48020
    QuotaPoolUsage[NonPagedPool]      1760
    Working Set Sizes (now,min,max)  (59, 50, 345) (236KB, 200KB, 1380KB)
    PeakWorkingSetSize                547
    VirtualSize                       23 Mb
    PeakVirtualSize                   30 Mb
    PageFaultCount                    652
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      155

    Setting context for this process...
.process /p /r ffffffff85d4ad88

    !peb
PEB at 7ffdd000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         01000000
    Ldr                       7c8877e0
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 000a1f18 . 000a9238
    Ldr.InLoadOrderModuleList:           000a1eb0 . 000a9228
    Ldr.InMemoryOrderModuleList:         000a1eb8 . 000a9230
            Base TimeStamp                     Module
         1000000 45d69be5 Feb 17 06:08:37 2007 C:\WINDOWS\system32\notepad.exe
        7c800000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\ntdll.dll
        77e40000 45d70ad8 Feb 17 14:02:00 2007 C:\WINDOWS\system32\kernel32.dll
        762b0000 45d70a72 Feb 17 14:00:18 2007 C:\WINDOWS\system32\comdlg32.dll
        77ba0000 45d70b06 Feb 17 14:02:46 2007 C:\WINDOWS\system32\msvcrt.dll
        77da0000 45d70ac0 Feb 17 14:01:36 2007 C:\WINDOWS\system32\SHLWAPI.dll
        77c00000 45d70a3e Feb 17 13:59:26 2007 C:\WINDOWS\system32\GDI32.dll
        77380000 45d70ac7 Feb 17 14:01:43 2007 C:\WINDOWS\system32\USER32.dll
        77f50000 45d70a26 Feb 17 13:59:02 2007 C:\WINDOWS\system32\ADVAPI32.dll
        77c50000 45d70aaa Feb 17 14:01:14 2007 C:\WINDOWS\system32\RPCRT4.dll
        76f50000 45d70ac3 Feb 17 14:01:39 2007 C:\WINDOWS\system32\Secur32.dll
        77420000 45d70a05 Feb 17 13:58:29 2007 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.3790.3959_x-ww_D8713E55\COMCTL32.dll
        7c8d0000 45d70abb Feb 17 14:01:31 2007 C:\WINDOWS\system32\SHELL32.dll
        73070000 45d70acb Feb 17 14:01:47 2007 C:\WINDOWS\system32\WINSPOOL.DRV
        71b70000 45d70acb Feb 17 14:01:47 2007 C:\WINDOWS\system32\UxTheme.dll
        10000000 40c8fe08 Jun 11 01:34:16 2004 C:\Program Files\VMware\VMware Tools\hook.dll
    SubSystemData:     00000000
    ProcessHeap:       000a0000
    ProcessParameters: 00020000
    WindowTitle:  'C:\Documents and Settings\Administrator\Start
Menu\Programs\Accessories\Notepad.lnk'
    ImageFile:    'C:\WINDOWS\system32\notepad.exe'
    CommandLine:  '"C:\WINDOWS\system32\notepad.exe" '
    DllPath:
'C:\WINDOWS\system32;C:\WINDOWS\system32;C:\WINDOWS\system;C:\WINDOWS;.;C:\WINDOWS\system32;C:\WIND
OWS;C:\WINDOWS\System32\Wbem'
    Environment:  00010000
        ALLUSERSPROFILE=C:\Documents and Settings\All Users
        APPDATA=C:\Documents and Settings\Administrator\Application Data
```

```
        ClusterLog=C:\WINDOWS\Cluster\cluster.log
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=COMPUTERNAME
        ComSpec=C:\WINDOWS\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        HOMEDRIVE=C:
        HOMEPATH=\Documents and Settings\Administrator
        LOGONSERVER=\\COMPUTERNAME
        NUMBER_OF_PROCESSORS=1
        OS=Windows_NT
        Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 15 Model 5 Stepping 10, AuthenticAMD
        PROCESSOR_LEVEL=15
        PROCESSOR_REVISION=050a
        ProgramFiles=C:\Program Files
        SESSIONNAME=Console
        SystemDrive=C:
        SystemRoot=C:\WINDOWS
        TEMP=C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp
        TMP=C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp
        USERDOMAIN=COMPUTERNAME
        USERNAME=Administrator
        USERPROFILE=C:\Documents and Settings\Administrator
        windir=C:\WINDOWS


        THREAD 860af9f0  Cid 0884.0888  Teb: 7ffdf000 Win32Thread: e1815008 WAIT: (Unknown)
UserMode Non-Alertable
            8649e440  SynchronizationEvent
        Not impersonating
        DeviceMap                 e249e270
        Owning Process            85d4ad88       Image:         notepad.exe
        Wait Start TickCount      95969          Ticks: 19999 (0:00:05:12.484)
        Context Switch Count      157                 LargeStack
        UserTime                  00:00:00.000
        KernelTime                00:00:00.031
        Win32 Start Address notepad!WinMainCRTStartup (0x010073a5)
        Start Address kernel32!BaseProcessStartThunk (0x77e617f8)
        Stack Init f67ce000 Current f67cdbc4 Base f67ce000 Limit f67c9000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 0
        Kernel stack not resident.
        ChildEBP RetAddr
        f67cdbdc 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
        f67cdbf4 808287b4 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
        f67cdc38 bf89b1c3 nt!KeWaitForSingleObject+0x2e0 (FPO: [Non-Fpo])
        f67cdc94 bf89b986 win32k!xxxSleepThread+0x1be (FPO: [Non-Fpo])
        f67cdcec bf89da22 win32k!xxxRealInternalGetMessage+0x46a (FPO: [Non-Fpo])
        f67cdd4c 80883908 win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
        f67cdd4c 7c8285ec nt!KiFastCallEntry+0xf8 (FPO: [0,0] TrapFrame @ f67cdd64)
        0007feb8 7739c811 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0007fed8 01002a3b USER32!NtUserGetMessage+0xc
        0007ff1c 01007527 notepad!WinMain+0xe5 (FPO: [Non-Fpo])
        0007ffc0 77e6f23b notepad!WinMainCRTStartup+0x182 (FPO: [Non-Fpo])
        0007fff0 00000000 kernel32!BaseProcessStart+0x23 (FPO: [Non-Fpo])
```

Stacks Summary

```
kd> !stacks
Proc.Thread  .Thread  Ticks   ThreadState Blocker
                           [865a1818 System]
   4.000264  862eadb0 001b5d2 Blocked    VsapiNT!IsVsapiWT+0x153
   4.000268  8644e740 001b5d2 Blocked    VsapiNT!IsVsapiWT+0x153
   4.00026c  8641fb18 001b5d2 Blocked    VsapiNT!IsVsapiWT+0x153
   4.000270  8636adb0 00005e2 Blocked    TmXPFlt+0x704b
   4.000274  862ff6b0 00032e2 Blocked    TmXPFlt+0x704b
   4.000278  862b4218 0001c62 Blocked    TmXPFlt+0x704b
   4.00027c  864469f0 0000022 Blocked    TmXPFlt+0x7873
   4.000470  85da9db0 00050c6 Blocked    TmXPFlt+0x98a3
   4.000474  862cf7b0 00050bf Blocked    TmXPFlt+0x98a3
   4.000478  86304bf0 00050be Blocked    TmXPFlt+0x98a3
   4.00047c  863e88f8 00050b8 Blocked    TmXPFlt+0x98a3
   4.000480  86304980 00050b4 Blocked    TmXPFlt+0x98a3
   4.000484  863d0db0 00050b4 Blocked    TmXPFlt+0x98a3
   4.000488  8634b938 00050b2 Blocked    TmXPFlt+0x98a3
   4.00048c  86331db0 00050b2 Blocked    TmXPFlt+0x98a3
   4.000490  86331600 00050b0 Blocked    TmXPFlt+0x98a3
   4.000494  863d0b40 0004ec0 Blocked    TmXPFlt+0x98a3
   4.00088c  85da11e8 0004b00 RUNNING    nt!KeBugCheckEx+0x1b

                           [8631ad88 smss.exe]

                           [862d0248 csrss.exe]
 150.000170  862d2db0 00005b3 Blocked    nt!KiFastCallEntry+0xf8
 150.0001d8  86387b18 00005cc Blocked    nt!KiFastCallEntry+0xf8

                           [862dd218 winlogon.exe]
 168.000084  85d44020 00003e0 Blocked    nt!KiFastCallEntry+0xf8

                           [8638ed88 services.exe]
 198.0001b4  862ecdb0 000029b Blocked    nt!KiFastCallEntry+0xf8
 198.0001b8  862ea730 0000215 Blocked    nt!KiFastCallEntry+0xf8
 198.0001bc  862b2020 000029b Blocked    nt!ObpWaitForMultipleObjects+0x202
 198.000240  86443288 000029b Blocked    nt!KiFastCallEntry+0xf8
 198.000258  863b52d8 0000013 Blocked    nt!KiFastCallEntry+0xf8
 198.00064c  85d51650 0000013 Blocked    nt!KiFastCallEntry+0xf8
 198.000154  85d44db0 0000013 Blocked    nt!KiFastCallEntry+0xf8

                           [86342988 lsass.exe]
 1a4.0001c0  86456380 000048a Blocked    nt!KiFastCallEntry+0xf8
 1a4.0001c4  862dbdb0 000048a Blocked    nt!KiFastCallEntry+0xf8
 1a4.0001d4  863b1c20 000078b Blocked    nt!KiFastCallEntry+0xf8
 1a4.0005b0  85d698d0 000003f Blocked    nt!ObpWaitForMultipleObjects+0x202

                           [8633a298 svchost.exe]
 280.0002b4  86454a70 000078c Blocked    nt!KiFastCallEntry+0xf8

                           [862c1c08 svchost.exe]
 2d4.0002e8  8631b4f0 000068a Blocked    nt!KiFastCallEntry+0xf8
 2d4.0002f8  8641e820 00005f1 Blocked    nt!KiFastCallEntry+0xf8
 2d4.0002fc  86374db0 00005e4 Blocked    nt!KiFastCallEntry+0xf8
 2d4.0004a8  8635cdb0 00005e4 Blocked    nt!KiFastCallEntry+0xf8
 2d4.0005a4  85d49690 00005e4 Blocked    nt!KiFastCallEntry+0xf8

                           [862d6b30 svchost.exe]
 314.000338  86323b70 000025d Blocked    nt!KiFastCallEntry+0xf8
 314.0004c8  863396b0 000039d Blocked    nt!KiFastCallEntry+0xf8
 314.0004d0  85d8a6b0 00002fd Blocked    nt!KiFastCallEntry+0xf8

                           [862fdbf0 svchost.exe]
 328.00034c  862cab28 000025d Blocked    nt!ObpWaitForMultipleObjects+0x202
 328.000364  8637b9b0 00001ea Blocked    nt!KiFastCallEntry+0xf8
 328.000368  86350db0 00001ea Blocked    nt!KiFastCallEntry+0xf8
```

```
328.000618  85d546b0 00003ec Blocked    nt!KiFastCallEntry+0xf8
328.00061c  85d54440 00003eb Blocked    nt!KiFastCallEntry+0xf8
328.000634  85d558a0 0000024 Blocked    nt!KiFastCallEntry+0xf8
328.000638  85d51a80 0000024 Blocked    nt!ObpWaitForMultipleObjects+0x202
328.0007f0  86380b70 00003e9 Blocked    nt!KiFastCallEntry+0xf8
328.0007f4  85d41478 00003eb Blocked    nt!KiFastCallEntry+0xf8

                          [86433518 svchost.exe]
350.000370  8632ad08 00008eb Blocked    nt!KiFastCallEntry+0xf8
350.000374  863fc020 000021c Blocked    nt!KiFastCallEntry+0xf8
350.000378  862fa740 00003da Blocked    nt!KiFastCallEntry+0xf8
350.00039c  864258d8 000049c Blocked    nt!KiFastCallEntry+0xf8
350.0003d4  862d2730 00008c1 Blocked    nt!KiFastCallEntry+0xf8
350.000604  85d5adb0 00003ec Blocked    nt!ObpWaitForMultipleObjects+0x202

                          [86444d88 spoolsv.exe]
3dc.0007a8  85d532e8 00000e1 Blocked    nt!KiFastCallEntry+0xf8
3dc.0007ac  85d7aa58 0000022 Blocked    nt!KiFastCallEntry+0xf8

                          [85de8d88 SpntSvc.exe]
434.000440  85dafdb0 0000107 Blocked    nt!KiFastCallEntry+0xf8
434.00044c  862c5a70 00000e1 Blocked    nt!KiFastCallEntry+0xf8
434.000450  85daedb0 000002d Blocked    nt!KiFastCallEntry+0xf8
434.00049c  863a0718 000002d Blocked    nt!KiFastCallEntry+0xf8
434.0004a0  86304710 0000046 Blocked    nt!KiFastCallEntry+0xf8
434.0004ac  863d1af0 000075a Blocked    nt!KiFastCallEntry+0xf8
434.0004b0  863d1880 00005f6 Blocked    nt!KiFastCallEntry+0xf8
434.0004b4  862b2c48 000025d Blocked    nt!KiFastCallEntry+0xf8
434.0006c0  85d48300 0000759 Blocked    nt!KiFastCallEntry+0xf8
434.0006cc  863383a0 00005f6 Blocked    nt!KiFastCallEntry+0xf8

                          [8635fb50 StWatchDog.exe]

                          [85d7fa08 StOPP.exe]

                          [85d7f770 msdtc.exe]

                          [85d71020 svchost.exe]

                          [85d6ed88 mdm.exe]

                          [85d6b5f0 svchost.exe]

                          [85d56d88 VMwareService.e]
5ec.0005f8  85d76b40 00003da Blocked    nt!KiFastCallEntry+0xf8
5ec.0005fc  85d5b398 0000006 Blocked    nt!ObpWaitForMultipleObjects+0x202

                          [85dc8d88 svchost.exe]

                          [85d41958 wmiprvse.exe]

                          [85d46b18 wmiprvse.exe]

                          [85d446e8 userinit.exe]

                          [85d5ed88 explorer.exe]
35c.0005d0  864a1a30 00005f1 Blocked    nt!KiFastCallEntry+0xf8
35c.0007c0  85d87698 0000898 Blocked    nt!KiFastCallEntry+0xf8
35c.000860  85d3d020 00005f1 Blocked    nt!KiFastCallEntry+0xf8

                          [865add88 VMwareTray.exe]
5dc.000598  864a0980 0000013 Blocked    nt!KiFastCallEntry+0xf8

                          [85d847e8 VMwareUser.exe]
610.00045c  85d857d0 0000006 Blocked    nt!ObpWaitForMultipleObjects+0x202

                          [860af368 iexplore.exe]

                          [85d4ad88 notepad.exe]
```

Threads Processed: 339

Executive Queues

```
kd> !exqueue ff
Dumping ExWorkerQueue: 808A76C0

**** Critical WorkQueue( current = 0 maximum = 1 )
THREAD 865a0b40  Cid 0004.0010  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown) KernelMode Non-
Alertable
    808a76c0  QueueObject
Not impersonating
DeviceMap                 e1000170
Owning Process            865a1818       Image:         System
Wait Start TickCount      20             Ticks: 115948 (0:00:30:11.687)
Context Switch Count      1
UserTime                  00:00:00.000
KernelTime                00:00:00.000
Start Address nt!ExpWorkerThread (0x8087acd6)
Stack Init f78b7000 Current f78b6d00 Base f78b7000 Limit f78b4000 Call 0
Priority 13 BasePriority 13 PriorityDecrement 0
ChildEBP RetAddr
f78b6d18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
f78b6d30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
f78b6d78 8087ad9e nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
f78b6dac 809418f4 nt!ExpWorkerThread+0xc8 (FPO: [Non-Fpo])
f78b6ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
00000000 00000000 nt!KiThreadStartup+0x16

THREAD 865a08d0  Cid 0004.0014  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown) KernelMode Non-
Alertable
    808a76c0  QueueObject
Not impersonating
DeviceMap                 e1000170
Owning Process            865a1818       Image:         System
Wait Start TickCount      20             Ticks: 115948 (0:00:30:11.687)
Context Switch Count      1
UserTime                  00:00:00.000
KernelTime                00:00:00.000
Start Address nt!ExpWorkerThread (0x8087acd6)
Stack Init f78bb000 Current f78bad00 Base f78bb000 Limit f78b8000 Call 0
Priority 13 BasePriority 13 PriorityDecrement 0
ChildEBP RetAddr
f78bad18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
f78bad30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
f78bad78 8087ad9e nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
f78badac 809418f4 nt!ExpWorkerThread+0xc8 (FPO: [Non-Fpo])
f78baddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
00000000 00000000 nt!KiThreadStartup+0x16
```

```
THREAD 8659f020  Cid 0004.0018  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown) KernelMode Non-
Alertable
    808a76c0  QueueObject
Not impersonating
DeviceMap                 e1000170
Owning Process            865a1818       Image:         System
Wait Start TickCount      4800           Ticks: 111168 (0:00:28:57.000)
Context Switch Count      2
UserTime                  00:00:00.000
KernelTime                00:00:00.000
Start Address nt!ExpWorkerThread (0x8087acd6)
Stack Init f78bf000 Current f78bed00 Base f78bf000 Limit f78bc000 Call 0
Priority 13 BasePriority 13 PriorityDecrement 0
ChildEBP RetAddr
f78bed18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
f78bed30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
f78bed78 8087ad9e nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
f78bedac 809418f4 nt!ExpWorkerThread+0xc8 (FPO: [Non-Fpo])
f78beddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
00000000 00000000 nt!KiThreadStartup+0x16

THREAD 8659fdb0  Cid 0004.001c  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown) KernelMode Non-
Alertable
    808a76c0  QueueObject
Not impersonating
DeviceMap                 e1000170
Owning Process            865a1818       Image:         System
Wait Start TickCount      115952         Ticks: 16 (0:00:00:00.250)
Context Switch Count      6313
UserTime                  00:00:00.000
KernelTime                00:00:01.406
Start Address nt!ExpWorkerThread (0x8087acd6)
Stack Init f78c3000 Current f78c2d00 Base f78c3000 Limit f78c0000 Call 0
Priority 13 BasePriority 13 PriorityDecrement 0
ChildEBP RetAddr
f78c2d18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
f78c2d30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
f78c2d78 8087ad9e nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
f78c2dac 809418f4 nt!ExpWorkerThread+0xc8 (FPO: [Non-Fpo])
f78c2ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
00000000 00000000 nt!KiThreadStartup+0x16

THREAD 8659fb40  Cid 0004.0020  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown) KernelMode Non-
Alertable
    808a76c0  QueueObject
Not impersonating
DeviceMap                 e1000170
Owning Process            865a1818       Image:         System
Wait Start TickCount      97025          Ticks: 18943 (0:00:04:55.984)
Context Switch Count      4800
UserTime                  00:00:00.000
KernelTime                00:00:00.421
Start Address nt!ExpWorkerThread (0x8087acd6)
Stack Init f78c7000 Current f78c6d00 Base f78c7000 Limit f78c4000 Call 0
Priority 13 BasePriority 13 PriorityDecrement 0
ChildEBP RetAddr
f78c6d18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
f78c6d30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
f78c6d78 8087ad9e nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
f78c6dac 809418f4 nt!ExpWorkerThread+0xc8 (FPO: [Non-Fpo])
f78c6ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
00000000 00000000 nt!KiThreadStartup+0x16
```

```
THREAD 8659f8d0  Cid 0004.0024  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown) KernelMode Non-
Alertable
    808a76c0  QueueObject
Not impersonating
DeviceMap                 e1000170
Owning Process            865a1818       Image:         System
Wait Start TickCount      115941         Ticks: 27 (0:00:00:00.421)
Context Switch Count      5086
UserTime                  00:00:00.000
KernelTime                00:00:00.343
Start Address nt!ExpWorkerThread (0x8087acd6)
Stack Init f78cb000 Current f78cad00 Base f78cb000 Limit f78c8000 Call 0
Priority 13 BasePriority 13 PriorityDecrement 0
ChildEBP RetAddr
f78cad18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
f78cad30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
f78cad78 8087ad9e nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
f78cadac 809418f4 nt!ExpWorkerThread+0xc8 (FPO: [Non-Fpo])
f78caddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
00000000 00000000 nt!KiThreadStartup+0x16

THREAD 8659f660  Cid 0004.0028  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown) KernelMode Non-
Alertable
    808a76c0  QueueObject
Not impersonating
DeviceMap                 e1000170
Owning Process            865a1818       Image:         System
Wait Start TickCount      112613         Ticks: 3355 (0:00:00:52.421)
Context Switch Count      810
UserTime                  00:00:00.000
KernelTime                00:00:00.125
Start Address nt!ExpWorkerThread (0x8087acd6)
Stack Init f78cf000 Current f78ced00 Base f78cf000 Limit f78cc000 Call 0
Priority 13 BasePriority 13 PriorityDecrement 0
ChildEBP RetAddr
f78ced18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
f78ced30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
f78ced78 8087ad9e nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
f78cedac 809418f4 nt!ExpWorkerThread+0xc8 (FPO: [Non-Fpo])
f78ceddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
00000000 00000000 nt!KiThreadStartup+0x16

THREAD 8659f3f0  Cid 0004.002c  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown) KernelMode Non-
Alertable
    808a76c0  QueueObject
Not impersonating
DeviceMap                 e1000170
Owning Process            865a1818       Image:         System
Wait Start TickCount      4800           Ticks: 111168 (0:00:28:57.000)
Context Switch Count      555
UserTime                  00:00:00.000
KernelTime                00:00:00.093
Start Address nt!ExpWorkerThread (0x8087acd6)
Stack Init f78d3000 Current f78d2d00 Base f78d3000 Limit f78d0000 Call 0
Priority 13 BasePriority 13 PriorityDecrement 0
ChildEBP RetAddr
f78d2d18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
f78d2d30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
f78d2d78 8087ad9e nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
f78d2dac 809418f4 nt!ExpWorkerThread+0xc8 (FPO: [Non-Fpo])
f78d2ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
00000000 00000000 nt!KiThreadStartup+0x16
```

```
THREAD 8659e020  Cid 0004.0030  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown) KernelMode Non-
Alertable
    808a76c0  QueueObject
Not impersonating
DeviceMap                 e1000170
Owning Process            865a1818       Image:         System
Wait Start TickCount      97025          Ticks: 18943 (0:00:04:55.984)
Context Switch Count      1645
UserTime                  00:00:00.000
KernelTime                00:00:00.140
Start Address nt!ExpWorkerThread (0x8087acd6)
Stack Init f78d7000 Current f78d6d00 Base f78d7000 Limit f78d4000 Call 0
Priority 13 BasePriority 13 PriorityDecrement 0
ChildEBP RetAddr
f78d6d18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
f78d6d30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
f78d6d78 8087ad9e nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
f78d6dac 809418f4 nt!ExpWorkerThread+0xc8 (FPO: [Non-Fpo])
f78d6ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
00000000 00000000 nt!KiThreadStartup+0x16

THREAD 8659edb0  Cid 0004.0034  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown) KernelMode Non-
Alertable
    808a76c0  QueueObject
Not impersonating
DeviceMap                 e1000170
Owning Process            865a1818       Image:         System
Wait Start TickCount      95717          Ticks: 20251 (0:00:05:16.421)
Context Switch Count      121
UserTime                  00:00:00.000
KernelTime                00:00:00.171
Start Address nt!ExpWorkerThread (0x8087acd6)
Stack Init f78db000 Current f78dad00 Base f78db000 Limit f78d8000 Call 0
Priority 13 BasePriority 13 PriorityDecrement 0
ChildEBP RetAddr
f78dad18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
f78dad30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
f78dad78 8087ad9e nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
f78dadac 809418f4 nt!ExpWorkerThread+0xc8 (FPO: [Non-Fpo])
f78daddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
00000000 00000000 nt!KiThreadStartup+0x16


**** Delayed WorkQueue( current = 0 maximum = 1 )
THREAD 8659eb40  Cid 0004.0038  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown) UserMode Non-
Alertable
    808a76fc  QueueObject
Not impersonating
DeviceMap                 e1000170
Owning Process            865a1818       Image:         System
Wait Start TickCount      20             Ticks: 115948 (0:00:30:11.687)
Context Switch Count      1
UserTime                  00:00:00.000
KernelTime                00:00:00.000
Start Address nt!ExpWorkerThread (0x8087acd6)
Stack Init f78df000 Current f78ded00 Base f78df000 Limit f78dc000 Call 0
Priority 12 BasePriority 12 PriorityDecrement 0
Kernel stack not resident.
ChildEBP RetAddr
f78ded18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
f78ded30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
f78ded78 8087ad9e nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
f78dedac 809418f4 nt!ExpWorkerThread+0xc8 (FPO: [Non-Fpo])
f78deddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
00000000 00000000 nt!KiThreadStartup+0x16
```

```
THREAD 8659e8d0  Cid 0004.003c  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown) UserMode Non-
Alertable
    808a76fc  QueueObject
Not impersonating
DeviceMap                 e1000170
Owning Process            865a1818       Image:         System
Wait Start TickCount      20             Ticks: 115948 (0:00:30:11.687)
Context Switch Count      1
UserTime                  00:00:00.000
KernelTime                00:00:00.000
Start Address nt!ExpWorkerThread (0x8087acd6)
Stack Init f78e3000 Current f78e2d00 Base f78e3000 Limit f78e0000 Call 0
Priority 12 BasePriority 12 PriorityDecrement 0
Kernel stack not resident.
ChildEBP RetAddr
f78e2d18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
f78e2d30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
f78e2d78 8087ad9e nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
f78e2dac 809418f4 nt!ExpWorkerThread+0xc8 (FPO: [Non-Fpo])
f78e2ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
00000000 00000000 nt!KiThreadStartup+0x16

THREAD 8659e660  Cid 0004.0040  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown) UserMode Non-
Alertable
    808a76fc  QueueObject
Not impersonating
DeviceMap                 e1000170
Owning Process            865a1818       Image:         System
Wait Start TickCount      3081           Ticks: 112887 (0:00:29:23.859)
Context Switch Count      5
UserTime                  00:00:00.000
KernelTime                00:00:00.000
Start Address nt!ExpWorkerThread (0x8087acd6)
Stack Init f78e7000 Current f78e6d00 Base f78e7000 Limit f78e4000 Call 0
Priority 12 BasePriority 12 PriorityDecrement 0
Kernel stack not resident.
ChildEBP RetAddr
f78e6d18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
f78e6d30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
f78e6d78 8087ad9e nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
f78e6dac 809418f4 nt!ExpWorkerThread+0xc8 (FPO: [Non-Fpo])
f78e6ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
00000000 00000000 nt!KiThreadStartup+0x16

THREAD 8659e3f0  Cid 0004.0044  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown) UserMode Non-
Alertable
    808a76fc  QueueObject
Not impersonating
DeviceMap                 e1000170
Owning Process            865a1818       Image:         System
Wait Start TickCount      115952         Ticks: 16 (0:00:00:00.250)
Context Switch Count      17561
UserTime                  00:00:00.000
KernelTime                00:00:01.593
Start Address nt!ExpWorkerThread (0x8087acd6)
Stack Init f78eb000 Current f78ead00 Base f78eb000 Limit f78e8000 Call 0
Priority 12 BasePriority 12 PriorityDecrement 0
ChildEBP RetAddr
f78ead18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
f78ead30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
f78ead78 8087ad9e nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
f78eadac 809418f4 nt!ExpWorkerThread+0xc8 (FPO: [Non-Fpo])
f78eaddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
00000000 00000000 nt!KiThreadStartup+0x16
```

```
THREAD 8659d020  Cid 0004.0048  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown) UserMode Non-
Alertable
    808a76fc  QueueObject
Not impersonating
DeviceMap                 e1000170
Owning Process            865a1818       Image:         System
Wait Start TickCount      4302           Ticks: 111666 (0:00:29:04.781)
Context Switch Count      21
UserTime                  00:00:00.000
KernelTime                00:00:00.000
Start Address nt!ExpWorkerThread (0x8087acd6)
Stack Init f78ef000 Current f78eed00 Base f78ef000 Limit f78ec000 Call 0
Priority 13 BasePriority 12 PriorityDecrement 0
Kernel stack not resident.
ChildEBP RetAddr
f78eed18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
f78eed30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
f78eed78 8087ad9e nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
f78eedac 809418f4 nt!ExpWorkerThread+0xc8 (FPO: [Non-Fpo])
f78eeddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
00000000 00000000 nt!KiThreadStartup+0x16

THREAD 8659ddb0  Cid 0004.004c  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown) UserMode Non-
Alertable
    808a76fc  QueueObject
Not impersonating
DeviceMap                 e1000170
Owning Process            865a1818       Image:         System
Wait Start TickCount      111781         Ticks: 4187 (0:00:01:05.421)
Context Switch Count      442
UserTime                  00:00:00.000
KernelTime                00:00:00.625
Start Address nt!ExpWorkerThread (0x8087acd6)
Stack Init f78f3000 Current f78f2d00 Base f78f3000 Limit f78f0000 Call 0
Priority 12 BasePriority 12 PriorityDecrement 0
Kernel stack not resident.
ChildEBP RetAddr
f78f2d18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
f78f2d30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
f78f2d78 8087ad9e nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
f78f2dac 809418f4 nt!ExpWorkerThread+0xc8 (FPO: [Non-Fpo])
f78f2ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
00000000 00000000 nt!KiThreadStartup+0x16

THREAD 8659db40  Cid 0004.0050  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown) UserMode Non-
Alertable
    808a76fc  QueueObject
Not impersonating
DeviceMap                 e1000170
Owning Process            865a1818       Image:         System
Wait Start TickCount      3534           Ticks: 112434 (0:00:29:16.781)
Context Switch Count      460
UserTime                  00:00:00.000
KernelTime                00:00:00.921
Start Address nt!ExpWorkerThread (0x8087acd6)
Stack Init f78f7000 Current f78f6d00 Base f78f7000 Limit f78f4000 Call 0
Priority 12 BasePriority 12 PriorityDecrement 0
Kernel stack not resident.
ChildEBP RetAddr
f78f6d18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
f78f6d30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
f78f6d78 8087ad9e nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
f78f6dac 809418f4 nt!ExpWorkerThread+0xc8 (FPO: [Non-Fpo])
f78f6ddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
00000000 00000000 nt!KiThreadStartup+0x16
```

```
**** HyperCritical WorkQueue( current = 0 maximum = 1 )
THREAD 8659d8d0  Cid 0004.0054  Teb: 00000000 Win32Thread: 00000000 WAIT: (Unknown) KernelMode Non-
Alertable
    808a7738  QueueObject
Not impersonating
DeviceMap                 e1000170
Owning Process            865a1818       Image:         System
Wait Start TickCount      114509         Ticks: 1459 (0:00:00:22.796)
Context Switch Count      290
UserTime                  00:00:00.000
KernelTime                00:00:00.031
Start Address nt!ExpWorkerThread (0x8087acd6)
Stack Init f78fb000 Current f78fad00 Base f78fb000 Limit f78f8000 Call 0
Priority 15 BasePriority 15 PriorityDecrement 0
ChildEBP RetAddr
f78fad18 8082ffb7 nt!KiSwapContext+0x25 (FPO: [Uses EBP] [0,0,4])
f78fad30 80829fc5 nt!KiSwapThread+0x83 (FPO: [Non-Fpo])
f78fad78 8087ad9e nt!KeRemoveQueue+0x3a1 (FPO: [Non-Fpo])
f78fadac 809418f4 nt!ExpWorkerThread+0xc8 (FPO: [Non-Fpo])
f78faddc 80887f4a nt!PspSystemThreadStartup+0x2e (FPO: [Non-Fpo])
00000000 00000000 nt!KiThreadStartup+0x16
```

Root Objects

```
kd> !object \
Object: e1000710  Type: (865ca418) Directory
    ObjectHeader: e10006f8 (old version)
    HandleCount: 0  PointerCount: 38
    Directory Object: 00000000  Name: \

    Hash Address  Type          Name
    ---- -------  ----          ----
     00  e10069f0 Directory     ArcName
         86541338 Device        Ntfs
     01  e1595368 Port          SeLsaCommandPort
     03  e1007148 Key           \REGISTRY
     06  e17e2818 Port          XactSrvLpcPort
     09  e1498e50 Directory     NLS
     10  e1006fe0 SymbolicLink  DosDevices
     13  e16c5120 Port          SeRmCommandPort
     14  864f0cd0 Device        Dfs
         e184b7b8 Port          LsaAuthenticationPort
         86541d38 Event         LanmanServerAnnounceEvent
     16  e10078c0 Directory     Driver
     19  e10079a8 Directory     Device
     20  e16fef60 Directory     Windows
     21  e16f98f8 Directory     Sessions
         86316818 Event         SAM_SERVICE_STARTED
     22  e16e5498 Directory     RPC Control
         e16ec770 Port          SmApiPort
     23  e1697260 Directory     BaseNamedObjects
         e1001638 Directory     KernelObjects
     24  e13f0700 Directory     FileSystem
         e10003d0 Directory     GLOBAL??
     25  86463030 WaitablePort  NLAPublicPort
     26  e250a938 Port          SmSsWinStationApiPort
         e1001450 Directory     ObjectTypes
     27  e1006eb0 Directory     Security
         e1915030 Port          ErrorLogPort
     30  e2502608 Port          AELPort
     31  e1007870 SymbolicLink  SystemRoot
         8632c378 Device        Cdfs
     32  863cb3d8 WaitablePort  NLAPrivatePort
         e1007030 Directory     Callback
     33  862b9098 Event         SeLsaInitEvent
         865e1608 Event         UniqueSessionIdEvent
     35  e16ffa70 Directory     KnownDlls
     36  86541758 Device        DfsServer
```

Device Objects

```
kd> !object \Device
Object: e10079a8  Type: (865ca418) Directory
    ObjectHeader: e1007990 (old version)
    HandleCount: 0  PointerCount: 170
    Directory Object: e1000710  Name: Device

    Hash Address  Type          Name
    ---- -------  ----          ----
     00  86305030 Device        Beep
         86541548 Device        KsecDD
         86542900 Device        Ndis
         86576540 Device        00000025
         86577160 Device        00000019
     01  86447b80 Device        Netbios
         865752a0 Device        00000033
         865762f8 Device        00000026
     02  865e17e8 Device        Ip
         865c2030 Device        00000027
         865963e0 Device        00000034
         86546030 Device        00000040
     03  865c1e00 Device        WMIAdminDevice
         8633b030 Device        Fips
         86403508 Device        Video0
         865c2de8 Device        00000028
         863c7aa0 Device        KeyboardClass0
         86546f18 Device        00000041
         865bf0f0 Device        00000035
     04  86437790 Device        Video1
         865c2ba0 Device        00000029
         863978d8 Device        NDProxy
         864047f0 Device        KeyboardClass1
         86546e00 Device        00000042
         8656b6f8 Device        00000036
     05  862c4430 Device        {AF91AA4F-7E97-4174-8526-B6AC4551ECA9}
         86546ce8 Device        00000043
         863ff128 Device        Video2
         863d8898 Device        Serial0
         863e4a08 Device        PointerClass0
         863ea3e0 Device        RdpDrDvMgr
         8656b5e0 Device        00000037
         865783a8 Device        0000000a
     06  86546bd0 Device        00000044
         86468ca0 Device        Video3
         863d5040 Device        Serial1
         862cc480 Device        USBPDO-0
         863be030 Device        Processor
         863bdaa0 Device        PointerClass1
         865a6248 Device        CompositeBattery
         865a7be0 Device        00000038
         86578160 Device        0000000b
     07  865c1f18 Device        WMIDataDevice
         e14a4af8 Directory     DmControl
         86546ab8 Device        00000045
         865a7930 Device        00000039
         86572678 Device        RawTape
         865c4f10 Device        0000000c
     08  86442948 Device        FloppyPDO0
         865a6df0 Device        00000046
         863d85f0 Device        RdpDrPort
         86572ac8 Device        NTPNP_PCI0000
         865c3f10 Device        0000001a
         865c4cc8 Device        0000000d
     09  865a6cd8 Device        00000047
         86547030 Device        NTPNP_PCI0001
         865c3cc8 Device        0000001b
```

```
    865c4a80 Device        0000000e
10  86325bd8 Device        RasAcd
    86453518 Device        VsapiNt
    865a6bc0 Device        00000048
    86547e50 Device        NTPNP_PCI0002
    865c3a80 Device        0000001c
    865c4838 Device        0000000f
11  865e5f18 Device        Tcp
    862cede8 Device        ParallelVdm0
    863c67c8 Device        ParallelPort0
    865a6aa8 Device        00000049
    86547c70 Device        NTPNP_PCI0003
    865c3838 Device        0000001d
12  86547938 Device        NTPNP_PCI0004
    865c2958 Device        0000002a
    862b5800 Device        RdpDr
    e14a1030 Directory     HarddiskDmVolumes
    865c35f0 Device        0000001e
13  8655de00 Device        HarddiskVolume1
    85da20f8 Device        SystemDump
    8637a770 Device        {77C98F24-7B91-4E2E-A5AF-140464C70963}
    86547600 Device        NTPNP_PCI0005
    865c2710 Device        0000002b
    865c33a8 Device        0000001f
14  863ea878 Device        Termdd
    8641a2e0 Device        CdRom0
    86316c00 Device        FsWrap
    865472c8 Device        NTPNP_PCI0006
    865c24c8 Device        0000002c
15  e13d8a38 Directory     Ide
    862fe988 Device        hgfsInternal
    865c2280 Device        0000002d
    86409338 Device        Parallel0
    865a7e50 Device        NTPNP_PCI0007
    865a7818 Device        0000003a
16  86575030 Device        0000002e
    865a7700 Device        0000003b
17  86300240 Device        VprotectTMFilter0
    8631ad18 Event         VolumesSafeForWriteAccess
    86575de8 Device        0000002f
    86563528 Device        0000003c
18  86563410 Device        0000003d
19  8632fd08 Device        NetBt_Wins_Export
    865632f8 Device        0000003e
20  865631e0 Device        0000003f
21  863ca8a0 Device        NetbiosSmb
    863d5b70 Device        0000004c
22  86438c10 Device        0000004d
23  86545e58 Device        MountPointManager
    86375210 Device        0000004e
24  864f08f8 Device        Mup
    862c53b8 Device        LanmanServer
    862b72d0 Device        WANARP
25  8635abd8 Device        Udp
26  e14a2890 Directory     Harddisk0
    863b2ad8 Device        RawIp
    863a2030 Device        NdisWanIp
    86361430 Device        {4A0CCFE0-53E5-441F-8DAE-6F649F63324F}
    865c5b10 Device        00000001
27  86467628 Device        Floppy0
    862e29b0 Device        {A72C2629-36A1-463C-AA9E-D67B118888C5}
    865728a8 Device        RawDisk
    865c57a8 Device        00000002
28  862ae028 Device        USBFDO-0
    8639ee00 Device        HGFS
    86324468 Device        Null
    865c5560 Device        00000003
    865c45f0 Device        00000010
29  864194c0 Device        IPSEC
    8639d1c8 Device        ParTechInc0
```

```
    865c5318 Device        00000004
    865c43a8 Device        00000011
30  86306ab0 Device        LanmanDatagramReceiver
    e1001948 Section       PhysicalMemory
    86305d70 Device        IPMULTICAST
    864341a8 Device        NdisWan
    86370240 Device        ParTechInc1
    863c9ec8 Device        NdisTapi
    86545730 Device        DmLoader
    865c4160 Device        00000012
    86578f10 Device        00000005
31  863d9990 Device        LanmanRedirector
    86398030 Device        Gpc
    8638f218 Device        ParTechInc2
    86577f10 Device        00000013
    86578cc8 Device        00000006
32  86345030 Device        NamedPipe
    86545948 Device        FtControl
    865c3160 Device        00000020
    86577cc8 Device        00000014
    86578a80 Device        00000007
33  862f90d8 Device        Mailslot
    86576f10 Device        00000021
    86577a80 Device        00000015
    86578838 Device        00000008
34  86325558 Device        Afd
    86373830 Device        NetBT_Tcpip_{A72C2629-36A1-463C-AA9E-D67B118888C5}
    863ae788 Device        Ndisuio
    86572790 Device        RawCdRom
    86576c18 Device        00000022
    86577838 Device        00000016
    865785f0 Device        00000009
35  e14905c8 SymbolicLink  ScsiPort0
    86575ba0 Device        00000030
    865769d0 Device        00000023
    865775f0 Device        00000017
36  863e3030 Device        {3F79461B-8A75-4352-9E73-999160B0B8EB}
    e1402150 Directory     WinDfs
    e14a6f58 SymbolicLink  ScsiPort1
    86575958 Device        00000031
    86576788 Device        00000024
    865773a8 Device        00000018
```

Driver Objects

```
kd> !object \Driver
Object: e10078c0  Type: (865ca418) Directory
    ObjectHeader: e10078a8 (old version)
    HandleCount: 0  PointerCount: 75
    Directory Object: e1000710  Name: Driver

    Hash Address  Type          Name
    ---- -------  ----          ----
     00  86325f38 Driver        Beep
         86542a18 Driver        NDIS
         86541660 Driver        KSecDD
     01  864058d0 Driver        Mouclass
         863d4478 Driver        Raspti
         863a8350 Driver        es1371
     02  863fd188 Driver        vmx_svga
     03  86333720 Driver        Fips
         8646c8e0 Driver        Kbdclass
     04  8655f9c0 Driver        VgaSave
         8634bf38 Driver        NDProxy
         865a6510 Driver        Compbatt
     05  8643e7a8 Driver        Ptilink
         86545030 Driver        MountMgr
     07  86545850 Driver        dmload
         86563798 Driver        isapnp
     08  86470030 Driver        redbook
         863eb548 Driver        vmmouse
         865a52f0 Driver        atapi
     10  86306d68 Driver        RasAcd
         86545638 Driver        dmio
         863af9f8 Driver        VsapiNT
     11  8644b5b8 Driver        audstub
         863d21c8 Driver        usbuhci
         863bf518 Driver        Win32k
     12  8634d030 Driver        usbhub
         863cb5d0 Driver        swenum
         86445838 Driver        rdpdr
     13  860db5e8 Driver        SystemDump
         863d9720 Driver        RDPCDD
         863a84f0 Driver        Update
         863aa758 Driver        RasPppoe
     14  863de418 Driver        TermDD
         8646c058 Driver        AmdK8
         86545d60 Driver        Ftdisk
     15  86397668 Driver        Rasl2tp
         863aabb0 Driver        Fdc
     16  862e9250 Driver        tmpreflt
         8633c970 Driver        Parvdm
     18  864059d8 Driver        PptpMiniport
         863ac658 Driver        serenum
         864f0800 Driver        crcdisk
         865751a8 Driver        WMIxWDM
         86575738 Driver        ACPI_HAL
     20  86404f38 Driver        PCnet
     21  8630b388 Driver        NetBT
         865729d0 Driver        agp440
     22  863d4668 Driver        Cdrom
         86412690 Driver        mssmbios
     24  8637d1a8 Driver        Wanarp
         86357030 Driver        Tcpip
         863b2238 Driver        mnmdd
         8646d8e0 Driver        gameenum
     25  865a54e0 Driver        VolSnap
     27  863a99b8 Driver        imapi
     28  8635a720 Driver        Null
     29  86451030 Driver        IPSec
```

```
    865c5030 Driver        Disk
    86548710 Driver        PCI
    863b8b90 Driver        TMFilter
30  863cac60 Driver        Serial
    863631d8 Driver        NdisTapi
    86441380 Driver        NdisWan
    865a53e8 Driver        PartMgr
31  8641b030 Driver        Gpc
32  86574c08 Driver        ACPI
33  8634a030 Driver        Flpydisk
    865992d8 Driver        PnpManager
34  86387030 Driver        AFD
    86369718 Driver        Ndisuio
35  86441478 Driver        Parport
36  863c1d78 Driver        i8042prt
    863ad430 Driver        CmBatt
    86562f38 Driver        IntelIde
```

File System Objects

```
kd> !object \FileSystem
Object: e13f0700  Type: (865ca418) Directory
    ObjectHeader: e13f06e8 (old version)
    HandleCount: 0  PointerCount: 21
    Directory Object: e1000710  Name: FileSystem

    Hash Address  Type          Name
    ---- -------  ----          ----
     00  86541450 Driver        Ntfs
     01  86318ca0 Driver        NetBIOS
     05  864a6d60 Driver        Rdbss
         86541870 Driver        DfsDriver
     15  863ff5c0 Driver        Msfs
     17  86311030 Driver        MRxSmb
     18  86335a30 Device        UdfsCdRomRecognizer
     19  862c54f8 Driver        Srv
     24  864f0de8 Driver        Mup
         8659e308 Driver        RAW
     25  862e0370 Driver        Npfs
         86335f38 Driver        Fs_Rec
     26  e13d8b20 Directory     Filters
     28  863373f0 Driver        hgfs
     31  86342030 Driver        Cdfs
     32  862c2030 Device        FatCdRomRecognizer
         86335530 Device        CdfsRecognizer
         8655d528 Driver        FltMgr
     34  86379448 Device        FatDiskRecognizer
     36  86336458 Device        UdfsDiskRecognizer
```

Base Named Objects

```
kd> !object \BaseNamedObjects
Object: e1697260  Type: (865ca418) Directory
    ObjectHeader: e1697248 (old version)
    HandleCount: 26  PointerCount: 178
    Directory Object: e1000710  Name: BaseNamedObjects

    Hash Address  Type          Name
    ---- -------  ----          ----
     00  85da4b70 Mutant        ZonesCacheCounterMutex
         e1464a50 SymbolicLink  Local
         862fdeb0 Event         userenv: Machine Group Policy has been applied
         85de6ee8 Event         TMDMON_DATA_READY_SPNT
         86314380 Event         AgentToWkssvcEvent
         86322d80 Event         jjCSCSessEvent_UM_KM_0
         862d1950 Event         userenv: machine policy force refresh event
     01  862bf808 Mutant        ZonesLockedCacheCounterMutex
         86449318 Event         TermSrvReadyEvent
         85d7c548 Mutant        0CADFD67AF62496dB34264F000F5624A
         85d818b8 Mutant        MSDTC_STATS_EVENT
         863ed5e0 Mutant        WPA_RT_MUTEX
         8644d4a8 Event         ThemesStartEvent
         8638ad28 Event         WinlogonTSSynchronizeEvent
     02  8607f240 Semaphore     PowerProfileRegistrySemaphore
         862e67b0 Event         EVENT_READYROOT/CIMV2WMI SELF-INSTRUMENTATION EVENT PROVIDER
         863ed630 Mutant        WPA_PR_MUTEX
         86431fb0 Event         WFP_IDLE_TRIGGER
         e140ae50 Directory     Restricted
     03  862f7be8 Event         WkssvcToAgentStartEvent
         86421ab0 Event         Microsoft Smart Card Resource Manager Started
         862fbeb0 Event         ScNetDrvMsg
     04  e25394a0 Section       C:_Documents and Settings_Administrator_Cookies_index.dat_32768
         85d87b40 Event         VMwareDnDDataTranser
         85d6cf20 Event         IPSEC_GP_REFRESH_EVENT
         862f65c0 Event         DHCPNEWIPADDRESS
     05  86358cf8 Event         WBEM_ESS_OPEN_FOR_BUSINESS
     06  e1397548 Section       MSIMGSIZECacheMap
         e198a760 Section       HGFSMEMORY
         860bb190 Event         WlballoonLogoffNotification
         862fd0f0 Event         userenv: User Group Policy ForcedRefresh Needs Foreground
Processing
         86385f70 Mutant        userenv: machine policy mutex
         862f48f0 Event         {11C1A7F3-7DEA-4F56-85C7-327CB46A5225}ShellHWDetection
         862eeb60 Event         msgina: ReturnToWelcome
     07  85d4f3c8 Semaphore     shell.BitBucket.c.DirtyCount
         85d552b8 Event         CscCacheInitCompleteEvent
         862b6e70 Mutant        userenv: user policy mutex
     08  85da3b70 Mutant        c:!documents and settings!administrator!cookies!
         85d562a0 Mutant        WindowsUpdateTracingMutex
         862d30b8 Event         LSA_RPC_SERVER_ACTIVE
     09  862e1fb0 Event         crypt32LogoffEvent
         86343680 Event         SENS Started Event
     10  862d7148 Event         userenv:  User Profile setup event
     11  8633baf8 Mutant        c:!documents and settings!administrator!local
settings!history!history.ie5!mshist012008013020080131!
         85db7cf8 Mutant        c:!documents and settings!administrator!local settings!temporary
internet files!content.ie5!
         85d51a50 Event         WMI_SysEvent_UnLodCtr
         8635d188 Event         userenv: Machine Group Policy Processing is done
     13  85d5dc60 Mutant        HGFSMUTEX
         8644d580 Semaphore     shell.{7CB834F0-527B-11D2-9D1F-0000F805CA57}
         85d5ce28 Semaphore     shell.{6D5313C0-8C62-11D1-B2CD-006097DF8C11}
         85d582e8 Semaphore     shell.BitBucket.NumDeleters
         8639e9f0 Event         SAConEvt
         85d4fd98 Event         WMI_RevAdap_ACK
         863e6c08 Event         ShellReadyEvent
```

```
         862fd0b0 Event         userenv: User Group Policy Processing is done
         862fd030 Event         userenv: User Group Policy has been applied
         86320890 Event         SC_AutoStartComplete
         85d7c4f8 Mutant        4FCC0DEFE22C4f138FB9D5AF25FD9398
     14  e1031a38 Section       UrlZonesSM_Administrator
         85d47e58 Event         0000000000023751_WlballoonKerberosNotificationEventName
         85daad38 Semaphore     Sem_NumReaders_9035e0f0-31a1-11d2-9e4b-0080c83a5c2c_SpntLog
     15  8641e4e8 Event         ScmCreatedEvent
         860db558 Mutant        DBWinMutex
         8642d0f0 Event         userenv: Machine Group Policy ForcedRefresh Needs Foreground
Processing
         863ed540 Mutant        WPA_HWID_MUTEX
     16  e1466638 SymbolicLink  Global
         85d4e310 Event         WINMGMT_COREDLL_CANSHUTDOWN
         85d651c0 Event         Microsoft.RPC_Registry_Server
     17  85d5cf58 Event         WMI_ProcessIdleTasksStart
         863ed590 Mutant        WPA_LT_MUTEX
         8638ace8 Event         TS-WPAAE
     18  86322d40 Event         AgentExistsEvent
     19  863b90f8 Mutant        WininetProxyRegistryMutex
         862db308 Mutant        c:!documents and settings!administrator!local
settings!history!history.ie5!
         862da030 Event         WinSta0_DesktopSwitch
     20  864227f8 Mutant        _!SHMSFTHISTORY!_
         862fd070 Event         userenv: User Policy Foreground Done Event
         86372de0 Mutant        userenv: Machine Registry policy mutex
     21  862ea6c0 Event         SvcctrlStartEvent_A3752DX
         860c9430 Semaphore     shell.BitBucket.GlobalDirtyCount
         85d5fb10 Event         W32TIME_NAMED_EVENT_SYSTIME_NOT_CORRECT
         e17cafa8 Section       TMDMON_BUFFER_SPNT
         863033b8 Event         jjCSCSharedFillEvent_UM_KM
         865e97a8 Event         PrefetchParametersChanged
         86458268 Mutant        userenv: User Registry policy mutex
     22  85d8d6c0 Mutant        _!MSFTHISTORY!_
         85d87a80 Event         HPlugEjectEvent
         863ed4f0 Mutant        WPA_LICSTORE_MUTEX
         85d6cf90 Event         IPSEC_POLICY_CHANGE_NOTIFY
         85dafce8 Mutant        Mutex_NoWriter_9035e0f0-31a1-11d2-9e4b-0080c83a5c2c_SpntLog
     23  865e97e8 Event         PrefetchTracesReady
         862b70f0 Event         ReconEvent
         e198a190 Section       MSDTC_STATS_FILE
         85debfc0 Event         Event_SpntSvc_304b9ef1-5b78-4dff-8969-38f4125c8968_
         86444730 Event         PrefetchOverrideIdle
     24  e2511390 Section       SENS Information Cache
         860ca388 Mutant        WininetStartupMutex
         860b32b0 Mutant        VMwareGuestDnDDataMutex
         862bc598 Event         RDPAudioDisabledEvent
     25  863509f0 Mutant        RasPbFile
         8635d148 Event         userenv: Machine Policy Foreground Done Event
         85d5cf18 Event         WMI_ProcessIdleTasksComplete
         85d5fa30 Event         VMwareToolsServiceEvent
         85da7cf0 Event         Event_NoReaders_9035e0f0-31a1-11d2-9e4b-0080c83a5c2c_SpntLog
     26  85d43760 Semaphore     shell._ie_sessioncount
         e2542c40 Section       C:_Documents and Settings_Administrator_Local Settings_Temporary
Internet Files_Content.IE5_index.dat_98304
         85d64cc0 Event         WinMMConsoleAudioEvent
         85d63ca8 Mutant        746bbf3569adEncrypt
     27  862c1580 Semaphore     shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
         862f07f0 Event         DINPUTWINMM
         85d82428 Event         Event_TmOPP_d99dc435-515d-475e-8f3e-a1e660a1eeee_
     28  85d4d200 Event         WINMGMT_PROVIDER_CANSHUTDOWN
         85d46578 Mutant        _SHuassist.mtx
         85d78730 Event         WMI_RevAdap_Set
     29  862bccb0 Mutant        ZonesCounterMutex
         e17f7bf8 Section       RotHintTable
         85d88d10 Event         userenv: user policy refresh event
         8637c780 Job           WmiProviderSubSystemHostJob
         85d7c4a8 Mutant        238FAD3109D3473aB4764B20B3731840
     30  86424270 Mutant        WininetConnectionMutex
```

```
         e1120570 Section       C:_Documents and Settings_Administrator_Local
Settings_History_History.IE5_index.dat_32768
         862c2df0 Semaphore     shell.{090851A5-EB96-11D2-8BE4-00C04FA31A66}
         85d5d508 Semaphore     shell.BitBucket.c.NextFileNum
         8636fcf0 Event         RouterPreInitEvent
         e159adb8 Section       Wmi Provider Sub System Counters
         85dedea8 Event         ProcessDetectorSync
         85d6a778 Event         IPSEC_POLICY_CHANGE_EVENT
         86422988 Event         WkssvcToAgentStopEvent
         8645b880 Event         WiaServiceStarted
         86374ab8 Event         PnP_No_Pending_Install_Events
         8641e630 Mutant        {A3BD3259-3E4F-428a-84C8-F0463A9D3EB5}
         e1495ad8 SymbolicLink  Session
     31  8643cb70 Mutant        ExplorerIsShellMutex
         85d713a8 Event         TermSrv:  machine GP event
         86314340 Event         wkssvc:  MUP finished initializing event
         8634d2e0 Mutant        winlogon: Logon UserProfileMapping Mutex
     32  e2541928 Section       C:_Documents and Settings_Administrator_Local
Settings_History_History.IE5_MSHist012008013020080131_index.dat_32768
         85d6b3c8 Semaphore     shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}
         86312240 Event         EVENT_READYROOT/CIMV2PROVIDERSUBSYSTEM
     33  863539c0 Event         userenv: user policy force refresh event
         86353640 Event         EVENT_READYROOT/CIMV2SCM EVENT PROVIDER
         862d1990 Event         userenv: machine policy refresh event
         86350a68 Event         WIRELESS_POLICY_CHANGE_EVENT
         e1515ac0 Section       Debug.Memory.1a4
     34  862f7e30 Event         Event_NewInfection_564e61d0-6f9f-11d2-9eaa-0080c83a5c2c
     35  85d6c6f0 Event         PS_SERVICE_STARTED
     36  85d557d0 Event         WMI_SysEvent_LodCtr
         864a1d58 Event         VMwareDnDManagerEvent
         864446f0 Event         PrefetchProcessingComplete
         e1800268 Section       {A64C7F33-DA35-459b-96CA-63B51FB0CDB9}
         863560e0 Mutant        SingleSesMutex
```

Kernel Objects

```
kd> !object \KernelObjects
Object: e1001638  Type: (865ca418) Directory
    ObjectHeader: e1001620 (old version)
    HandleCount: 0  PointerCount: 8
    Directory Object: e1000710  Name: KernelObjects

    Hash Address  Type          Name
    ---- -------  ----          ----
     04  8659c340 Event         HighMemoryCondition
     10  8659c280 Event         LowNonPagedPoolCondition
     11  8659c240 Event         HighNonPagedPoolCondition
     25  8659c300 Event         LowPagedPoolCondition
     26  8659c2c0 Event         HighPagedPoolCondition
     32  e1006d58 KeyedEvent    CritSecOutOfMemoryEvent
         8659f2b8 Event         LowMemoryCondition
```

Loaded System Modules

```
kd> lmv
start    end        module name
80800000 80a4c000   nt         (pdb symbols)
c:\mss\ntkrnlpa.pdb\4121E0AD95474F849EBDDF280C7E498D1\ntkrnlpa.pdb
    Loaded symbol image file: ntkrnlpa.exe
    Image path: ntkrnlpa.exe
    Image name: ntkrnlpa.exe
    Timestamp:        Sat Feb 17 05:48:00 2007 (45D69710)
    CheckSum:         0023564E
    ImageSize:        0024C000
    File version:     5.2.3790.3959
    Product version:  5.2.3790.3959
    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:     ntkrnlpa.exe
    OriginalFilename: ntkrnlpa.exe
    ProductVersion:   5.2.3790.3959
    FileVersion:      5.2.3790.3959 (srv03_sp2_rtm.070216-1710)
    FileDescription:  NT Kernel & System
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
80a4c000 80a78000   hal        (deferred)
    Image path: halaacpi.dll
    Image name: halaacpi.dll
    Timestamp:        Sat Feb 17 05:48:25 2007 (45D69729)
    CheckSum:         0001EDD4
    ImageSize:        0002C000
    File version:     5.2.3790.3959
    Product version:  5.2.3790.3959
    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:     halaacpi.dll
    OriginalFilename: halaacpi.dll
    ProductVersion:   5.2.3790.3959
    FileVersion:      5.2.3790.3959 (srv03_sp2_rtm.070216-1710)
    FileDescription:  Hardware Abstraction Layer DLL
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
bf800000 bf9cf000   win32k     (pdb symbols)
c:\mss\win32k.pdb\698367509D2C4E13BE411D3436B653502\win32k.pdb
    Loaded symbol image file: win32k.sys
    Image path: \SystemRoot\System32\win32k.sys
    Image name: win32k.sys
    Timestamp:        Sat Feb 17 06:31:05 2007 (45D6A129)
    CheckSum:         001C50CA
    ImageSize:        001CF000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
bf9cf000 bf9e6000   dxg        (deferred)
    Image path: \SystemRoot\System32\drivers\dxg.sys
    Image name: dxg.sys
    Timestamp:        Sat Feb 17 06:14:39 2007 (45D69D4F)
    CheckSum:         00012550
    ImageSize:        00017000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
bf9e6000 bf9ec080   vmx_fb     (deferred)
    Image path: \SystemRoot\System32\vmx_fb.dll
    Image name: vmx_fb.dll
```

```
    Timestamp:        Fri Jun 11 01:34:35 2004 (40C8FE1B)
    CheckSum:         000134A8
    ImageSize:        00006080
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f66b5000 f6712000   srv        (pdb symbols)
c:\mss\srv.pdb\826BC4DC0D8C477E874DEB57B3F628372\srv.pdb
    Loaded symbol image file: srv.sys
    Image path: \SystemRoot\system32\DRIVERS\srv.sys
    Image name: srv.sys
    Timestamp:        Sat Feb 17 06:27:20 2007 (45D6A048)
    CheckSum:         0005AEFC
    ImageSize:        0005D000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f673a000 f674d520   hgfs       (deferred)
    Image path: \SystemRoot\System32\DRIVERS\hgfs.sys
    Image name: hgfs.sys
    Timestamp:        Fri Jun 11 01:34:57 2004 (40C8FE31)
    CheckSum:         00020EC9
    ImageSize:        00013520
    File version:     0.1.0.0
    Product version:  0.1.0.0
    File flags:       8 (Mask 3F) Private
    File OS:          40004 NT Win32
    File type:        3.0 Driver
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      VMware, Inc.
    ProductName:      VMware HGFS
    InternalName:     hgfs.sys
    OriginalFilename: hgfs.sys
    ProductVersion:   Build build-8848
    FileVersion:      0.1.0.0
    FileDescription:  VMware HGFS Driver
    LegalCopyright:   Copyright © 1998-2003 VMware, Inc.
f68de000 f690f500   TmXPFlt    (no symbols)
    Loaded symbol image file: TmXPFlt.sys
    Image path: \??\C:\Program Files\Trend\SProtect\TmXPFlt.sys
    Image name: TmXPFlt.sys
    Timestamp:        Tue Mar 30 10:35:10 2004 (40693F4E)
    CheckSum:         0003F2AA
    ImageSize:        00031500
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f6910000 f69f2fa0   VsapiNT    (export symbols)       VsapiNT.sys
    Loaded symbol image file: VsapiNT.sys
    Image path: \??\C:\Program Files\Trend\SProtect\VsapiNT.sys
    Image name: VsapiNT.sys
    Timestamp:        Tue Mar 30 10:12:36 2004 (40693A04)
    CheckSum:         000E667C
    ImageSize:        000E2FA0
    File version:     7.100.0.1003
    Product version:  7.1.0.0
    File flags:       8 (Mask 3F) Private
    File OS:          40000 NT Base
    File type:        2.0 Dll
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      Trend Micro Inc.
    ProductName:      vsapi
    InternalName:     VSAPINT
    OriginalFilename: VsapiNt.sys
    ProductVersion:   7.100
    FileVersion:      7.100-1003
    FileDescription:  VsapiNT
    LegalCopyright:   Copyright (C) 1998-2004 Trend Micro Incorporated. All rights reserved.
    LegalTrademarks:  Copyright (C) Trend Micro Inc.
f6b33000 f6b50000   dump_atapi   (deferred)
    Image path: \SystemRoot\System32\Drivers\dump_atapi.sys
    Image name: dump_atapi.sys
    Timestamp:        Sat Feb 17 06:07:34 2007 (45D69BA6)
    CheckSum:         0001D4C5
```

```
    ImageSize:        0001D000
    File version:     5.2.3790.3959
    Product version:  5.2.3790.3959
    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:   5.2.3790.3959
    FileVersion:      5.2.3790.3959 (srv03_sp2_rtm.070216-1710)
    FileDescription:  IDE/ATAPI Port Driver
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
f6b50000 f6b65000   Cdfs       (deferred)
    Image path: \SystemRoot\System32\Drivers\Cdfs.SYS
    Image name: Cdfs.SYS
    Timestamp:        Sat Feb 17 06:27:08 2007 (45D6A03C)
    CheckSum:         00015D3A
    ImageSize:        00015000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f6b8d000 f6b9e000   Fips       (deferred)
    Image path: \SystemRoot\System32\Drivers\Fips.SYS
    Image name: Fips.SYS
    Timestamp:        Sat Feb 17 06:26:33 2007 (45D6A019)
    CheckSum:         0000B9EB
    ImageSize:        00011000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f6b9e000 f6c14000   mrxsmb     (deferred)
    Image path: \SystemRoot\system32\DRIVERS\mrxsmb.sys
    Image name: mrxsmb.sys
    Timestamp:        Sat Feb 17 06:28:15 2007 (45D6A07F)
    CheckSum:         00074736
    ImageSize:        00076000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f6c14000 f6c44000   rdbss      (pdb symbols)
c:\mss\rdbss.pdb\FB1A2E64899146228FFC6BFECCE150742\rdbss.pdb
    Loaded symbol image file: rdbss.sys
    Image path: \SystemRoot\system32\DRIVERS\rdbss.sys
    Image name: rdbss.sys
    Timestamp:        Sat Feb 17 06:27:37 2007 (45D6A059)
    CheckSum:         000346F8
    ImageSize:        00030000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f6c44000 f6c6e000   afd        (deferred)
    Image path: \SystemRoot\System32\drivers\afd.sys
    Image name: afd.sys
    Timestamp:        Sat Feb 17 06:28:16 2007 (45D6A080)
    CheckSum:         00025770
    ImageSize:        0002A000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f6c6e000 f6c9f000   netbt      (deferred)
    Image path: \SystemRoot\system32\DRIVERS\netbt.sys
    Image name: netbt.sys
    Timestamp:        Sat Feb 17 06:28:57 2007 (45D6A0A9)
    CheckSum:         0002E9F6
    ImageSize:        00031000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f6c9f000 f6d2f000   tcpip      (deferred)
    Image path: \SystemRoot\system32\DRIVERS\tcpip.sys
    Image name: tcpip.sys
    Timestamp:        Sat Feb 17 06:28:05 2007 (45D6A075)
    CheckSum:         0006B568
    ImageSize:        00090000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f6d2f000 f6d48000   ipsec      (deferred)
    Image path: \SystemRoot\system32\DRIVERS\ipsec.sys
    Image name: ipsec.sys
```

```
    Timestamp:        Sat Feb 17 06:29:28 2007 (45D6A0C8)
    CheckSum:         0001DA9A
    ImageSize:        00019000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f6d78000 f6d82000   ndisuio    (deferred)
    Image path: \SystemRoot\system32\DRIVERS\ndisuio.sys
    Image name: ndisuio.sys
    Timestamp:        Sat Feb 17 05:58:25 2007 (45D69981)
    CheckSum:         00004C9B
    ImageSize:        0000A000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f6e08000 f6e1d000   usbhub     (deferred)
    Image path: \SystemRoot\system32\DRIVERS\usbhub.sys
    Image name: usbhub.sys
    Timestamp:        Sat Feb 17 06:13:05 2007 (45D69CF1)
    CheckSum:         0001E7B9
    ImageSize:        00015000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f6e6d000 f6eb7000   update     (deferred)
    Image path: \SystemRoot\system32\DRIVERS\update.sys
    Image name: update.sys
    Timestamp:        Sat Feb 17 06:28:59 2007 (45D6A0AB)
    CheckSum:         0004D6FA
    ImageSize:        0004A000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f6eb7000 f6eee000   rdpdr      (pdb symbols)
c:\mss\rdpdr.pdb\848BC2B36384480CA59D94CD7CDFB0AF1\rdpdr.pdb
    Loaded symbol image file: rdpdr.sys
    Image path: \SystemRoot\system32\DRIVERS\rdpdr.sys
    Image name: rdpdr.sys
    Timestamp:        Sat Feb 17 05:51:00 2007 (45D697C4)
    CheckSum:         00031FE4
    ImageSize:        00037000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f6f8e000 f6fa0000   raspptp    (pdb symbols)
c:\mss\raspptp.pdb\4A592EBA851241449D43421574548C4E2\raspptp.pdb
    Loaded symbol image file: raspptp.sys
    Image path: \SystemRoot\system32\DRIVERS\raspptp.sys
    Image name: raspptp.sys
    Timestamp:        Sat Feb 17 06:29:20 2007 (45D6A0C0)
    CheckSum:         00013B9A
    ImageSize:        00012000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f6fa0000 f6fb9000   ndiswan    (deferred)
    Image path: \SystemRoot\system32\DRIVERS\ndiswan.sys
    Image name: ndiswan.sys
    Timestamp:        Sat Feb 17 06:29:22 2007 (45D6A0C2)
    CheckSum:         00021659
    ImageSize:        00019000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f6fb9000 f6fcd000   rasl2tp    (deferred)
    Image path: \SystemRoot\system32\DRIVERS\rasl2tp.sys
    Image name: rasl2tp.sys
    Timestamp:        Sat Feb 17 06:29:02 2007 (45D6A0AE)
    CheckSum:         0001D4BD
    ImageSize:        00014000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f6ff5000 f700a000   drmk       (deferred)
    Image path: \SystemRoot\system32\drivers\drmk.sys
    Image name: drmk.sys
    Timestamp:        Sat Feb 17 06:12:29 2007 (45D69CCD)
    CheckSum:         000109BA
    ImageSize:        00015000
    File version:     5.2.3790.3959
    Product version:  5.2.3790.3959
    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:   5.2.3790.3959
    FileVersion:      5.2.3790.3959 (srv03_sp2_rtm.070216-1710)
    FileDescription:  Microsoft Kernel DRM Descrambler Filter
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
f700a000 f7033000   portcls    (deferred)
    Image path: \SystemRoot\system32\drivers\portcls.sys
    Image name: portcls.sys
    Timestamp:        Sat Feb 17 06:30:03 2007 (45D6A0EB)
    CheckSum:         00031CAE
    ImageSize:        00029000
    File version:     5.2.3790.3959
    Product version:  5.2.3790.3959
    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:   5.2.3790.3959
    FileVersion:      5.2.3790.3959 (srv03_sp2_rtm.070216-1710)
    FileDescription:  Port Class (Class Driver for Port/Miniport Devices)
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
f7033000 f704f000   VIDEOPRT   (deferred)
    Image path: \SystemRoot\system32\DRIVERS\VIDEOPRT.SYS
    Image name: VIDEOPRT.SYS
    Timestamp:        Sat Feb 17 06:10:30 2007 (45D69C56)
    CheckSum:         000223AF
    ImageSize:        0001C000
    File version:     5.2.3790.3959
    Product version:  5.2.3790.3959
    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:   5.2.3790.3959
    FileVersion:      5.2.3790.3959 (srv03_sp2_rtm.070216-1710)
    FileDescription:  Video Port Driver
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
f704f000 f7079000   USBPORT    (pdb symbols)
c:\mss\usbport.pdb\8A87CD9FE4234E4DBABFF30842FD3E761\usbport.pdb
    Loaded symbol image file: USBPORT.SYS
    Image path: \SystemRoot\system32\DRIVERS\USBPORT.SYS
    Image name: USBPORT.SYS
    Timestamp:        Sat Feb 17 06:12:59 2007 (45D69CEB)
    CheckSum:         00027A92
    ImageSize:        0002A000
    File version:     5.2.3790.3959
    Product version:  5.2.3790.3959
    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:   5.2.3790.3959
```

```
    FileVersion:      5.2.3790.3959 (srv03_sp2_rtm.070216-1710)
    FileDescription:  USB 1.1 & 2.0 Port Driver
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
f7079000 f70a0000   ks         (deferred)
    Image path: \SystemRoot\system32\DRIVERS\ks.sys
    Image name: ks.sys
    Timestamp:        Sat Feb 17 06:30:40 2007 (45D6A110)
    CheckSum:         0002DD89
    ImageSize:        00027000
    File version:     5.3.3790.3959
    Product version:  5.3.3790.3959
    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(R) Windows(R) Operating System
    InternalName:     ks.sys
    OriginalFilename: ks.sys
    ProductVersion:   5.3.3790.3959
    FileVersion:      5.3.3790.3959 (srv03_sp2_rtm.070216-1710)
    FileDescription:  Kernel CSA Library
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
f70a0000 f70b4000   redbook    (pdb symbols)
c:\mss\redbook.pdb\458F1549775540A98F797ED48965388A1\redbook.pdb
    Loaded symbol image file: redbook.sys
    Image path: \SystemRoot\system32\DRIVERS\redbook.sys
    Image name: redbook.sys
    Timestamp:        Sat Feb 17 06:07:26 2007 (45D69B9E)
    CheckSum:         00011CDD
    ImageSize:        00014000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f70b4000 f70c9000   cdrom      (deferred)
    Image path: \SystemRoot\system32\DRIVERS\cdrom.sys
    Image name: cdrom.sys
    Timestamp:        Sat Feb 17 06:07:48 2007 (45D69BB4)
    CheckSum:         0001CAE1
    ImageSize:        00015000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f70c9000 f70de000   serial     (deferred)
    Image path: \SystemRoot\system32\DRIVERS\serial.sys
    Image name: serial.sys
    Timestamp:        Sat Feb 17 06:06:46 2007 (45D69B76)
    CheckSum:         0001E1B9
    ImageSize:        00015000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f70de000 f70f6000   parport    (pdb symbols)
c:\mss\parport.pdb\DEC7D1923209457FB9A63A108E0F4D4D1\parport.pdb
    Loaded symbol image file: parport.sys
    Image path: \SystemRoot\system32\DRIVERS\parport.sys
    Image name: parport.sys
    Timestamp:        Sat Feb 17 06:06:42 2007 (45D69B72)
    CheckSum:         00021142
    ImageSize:        00018000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f70f6000 f7109000   i8042prt   (deferred)
    Image path: \SystemRoot\system32\DRIVERS\i8042prt.sys
    Image name: i8042prt.sys
    Timestamp:        Sat Feb 17 06:30:40 2007 (45D6A110)
    CheckSum:         000184DF
    ImageSize:        00013000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f7151000 f7170000   Mup        (deferred)
    Image path: Mup.sys
    Image name: Mup.sys
    Timestamp:        Sat Feb 17 06:27:41 2007 (45D6A05D)
    CheckSum:         00023FA8
    ImageSize:        0001F000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
```

```
f7170000 f71af000   NDIS       (pdb symbols)
c:\mss\ndis.pdb\A14D4209157649C29C2B53ACB7C24C122\ndis.pdb
    Loaded symbol image file: NDIS.sys
    Image path: NDIS.sys
    Image name: NDIS.sys
    Timestamp:        Sat Feb 17 06:28:49 2007 (45D6A0A1)
    CheckSum:         0003CA0F
    ImageSize:        0003F000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f71af000 f7244000   Ntfs       (deferred)
    Image path: Ntfs.sys
    Image name: Ntfs.sys
    Timestamp:        Sat Feb 17 06:27:23 2007 (45D6A04B)
    CheckSum:         00097DDD
    ImageSize:        00095000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f7244000 f726a000   KSecDD     (deferred)
    Image path: KSecDD.sys
    Image name: KSecDD.sys
    Timestamp:        Sat Feb 17 05:46:32 2007 (45D696B8)
    CheckSum:         00024591
    ImageSize:        00026000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f726a000 f728f000   fltmgr     (deferred)
    Image path: fltmgr.sys
    Image name: fltmgr.sys
    Timestamp:        Sat Feb 17 05:51:08 2007 (45D697CC)
    CheckSum:         00028DAD
    ImageSize:        00025000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f728f000 f72a2000   CLASSPNP   (deferred)
    Image path: \WINDOWS\system32\DRIVERS\CLASSPNP.SYS
    Image name: CLASSPNP.SYS
    Timestamp:        Sat Feb 17 06:28:16 2007 (45D6A080)
    CheckSum:         0000EFB8
    ImageSize:        00013000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f72a2000 f72bf000   atapi      (deferred)
    Image path: atapi.sys
    Image name: atapi.sys
    Timestamp:        Sat Feb 17 06:07:34 2007 (45D69BA6)
    CheckSum:         0001D4C5
    ImageSize:        0001D000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f72bf000 f72e9000   volsnap    (deferred)
    Image path: volsnap.sys
    Image name: volsnap.sys
    Timestamp:        Sat Feb 17 06:08:23 2007 (45D69BD7)
    CheckSum:         00029843
    ImageSize:        0002A000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f72e9000 f7315000   dmio       (pdb symbols)
c:\mss\dmio.pdb\FD474E74B14F40AEB147FB0399D67BDB1\dmio.pdb
    Loaded symbol image file: dmio.sys
    Image path: dmio.sys
    Image name: dmio.sys
    Timestamp:        Sat Feb 17 06:10:44 2007 (45D69C64)
    CheckSum:         000270C9
    ImageSize:        0002C000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f7315000 f733c000   ftdisk     (deferred)
    Image path: ftdisk.sys
    Image name: ftdisk.sys
    Timestamp:        Sat Feb 17 06:08:05 2007 (45D69BC5)
    CheckSum:         00024F7A
    ImageSize:        00027000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f733c000 f7352000   pci        (deferred)
    Image path: pci.sys
    Image name: pci.sys
```

```
    Timestamp:        Sat Feb 17 05:59:03 2007 (45D699A7)
    CheckSum:         0001E42B
    ImageSize:        00016000
    File version:     5.2.3790.3959
    Product version:  5.2.3790.3959
    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:   5.2.3790.3959
    FileVersion:      5.2.3790.3959 (srv03_sp2_rtm.070216-1710)
    FileDescription:  NT Plug and Play PCI Enumerator
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
f7352000 f7386000   ACPI       (pdb symbols)
c:\mss\acpi.pdb\FBB7E7F76E2D4337B34F0D037397A1F91\acpi.pdb
    Loaded symbol image file: ACPI.sys
    Image path: ACPI.sys
    Image name: ACPI.sys
    Timestamp:        Sat Feb 17 05:58:47 2007 (45D69997)
    CheckSum:         00032E63
    ImageSize:        00034000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f7487000 f7490000   WMILIB     (deferred)
    Image path: \WINDOWS\system32\DRIVERS\WMILIB.SYS
    Image name: WMILIB.SYS
    Timestamp:        Tue Mar 25 07:13:00 2003 (3E80017C)
    CheckSum:         00004365
    ImageSize:        00009000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f7497000 f74a6000   isapnp     (deferred)
    Image path: isapnp.sys
    Image name: isapnp.sys
    Timestamp:        Sat Feb 17 05:58:57 2007 (45D699A1)
    CheckSum:         0000DC0C
    ImageSize:        0000F000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f74a7000 f74b4000   PCIIDEX    (deferred)
    Image path: \WINDOWS\system32\DRIVERS\PCIIDEX.SYS
    Image name: PCIIDEX.SYS
    Timestamp:        Sat Feb 17 06:07:32 2007 (45D69BA4)
    CheckSum:         00010ED8
    ImageSize:        0000D000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f74b7000 f74c7000   MountMgr   (deferred)
    Image path: MountMgr.sys
    Image name: MountMgr.sys
    Timestamp:        Sat Feb 17 06:05:35 2007 (45D69B2F)
    CheckSum:         00018F39
    ImageSize:        00010000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f74c7000 f74d2000   PartMgr    (deferred)
    Image path: PartMgr.sys
    Image name: PartMgr.sys
    Timestamp:        Sat Feb 17 06:29:25 2007 (45D6A0C5)
    CheckSum:         0000EE27
    ImageSize:        0000B000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f74d7000 f74e7000   disk       (deferred)
    Image path: disk.sys
    Image name: disk.sys
    Timestamp:        Sat Feb 17 06:07:51 2007 (45D69BB7)
    CheckSum:         00017691
    ImageSize:        00010000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f74e7000 f74f3000   Dfs        (deferred)
```

```
    Image path: Dfs.sys
    Image name: Dfs.sys
    Timestamp:        Sat Feb 17 05:51:17 2007 (45D697D5)
    CheckSum:         00016C54
    ImageSize:        0000C000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f74f7000 f7507000   agp440     (deferred)
    Image path: agp440.sys
    Image name: agp440.sys
    Timestamp:        Sat Feb 17 05:58:53 2007 (45D6999D)
    CheckSum:         0001715F
    ImageSize:        00010000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f7507000 f7511000   crcdisk    (deferred)
    Image path: crcdisk.sys
    Image name: crcdisk.sys
    Timestamp:        Sat Feb 17 06:09:50 2007 (45D69C2E)
    CheckSum:         0001142A
    ImageSize:        0000A000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f7517000 f7524000   wanarp     (deferred)
    Image path: \SystemRoot\system32\DRIVERS\wanarp.sys
    Image name: wanarp.sys
    Timestamp:        Sat Feb 17 05:59:17 2007 (45D699B5)
    CheckSum:         0000969A
    ImageSize:        0000D000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f7527000 f7534000   netbios    (deferred)
    Image path: \SystemRoot\system32\DRIVERS\netbios.sys
    Image name: netbios.sys
    Timestamp:        Sat Feb 17 05:58:29 2007 (45D69985)
    CheckSum:         00011592
    ImageSize:        0000D000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f7547000 f7550000   dump_WMILIB   (deferred)
    Image path: \SystemRoot\System32\Drivers\dump_WMILIB.SYS
    Image name: dump_WMILIB.SYS
    Timestamp:        Tue Mar 25 07:13:00 2003 (3E80017C)
    CheckSum:         00004365
    ImageSize:        00009000
    File version:     5.2.3790.0
    Product version:  5.2.3790.0
    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:     WmiLib.sys
    OriginalFilename: WmiLib.sys
    ProductVersion:   5.2.3790.0
    FileVersion:      5.2.3790.0 (srv03_rtm.030324-2048)
    FileDescription:  WMILIB WMI support library Dll
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
f7557000 f7561000   Dxapi      (deferred)
    Image path: \SystemRoot\System32\drivers\Dxapi.sys
    Image name: Dxapi.sys
    Timestamp:        Tue Mar 25 07:06:01 2003 (3E7FFFD9)
    CheckSum:         0001039A
    ImageSize:        0000A000
    File version:     5.2.3790.0
    Product version:  5.2.3790.0
    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:   5.2.3790.0
    FileVersion:      5.2.3790.0 (srv03_rtm.030324-2048)
    FileDescription:  DirectX API Driver
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
f7597000 f75a6000   amdk8      (deferred)
    Image path: \SystemRoot\system32\DRIVERS\amdk8.sys
    Image name: amdk8.sys
    Timestamp:        Sat Feb 17 05:48:31 2007 (45D6972F)
    CheckSum:         0000DC70
    ImageSize:        0000F000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f75a7000 f75b2000   kbdclass   (deferred)
    Image path: \SystemRoot\system32\DRIVERS\kbdclass.sys
    Image name: kbdclass.sys
    Timestamp:        Sat Feb 17 06:05:39 2007 (45D69B33)
    CheckSum:         00007486
    ImageSize:        0000B000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f75b7000 f75c1000   mouclass   (deferred)
    Image path: \SystemRoot\system32\DRIVERS\mouclass.sys
    Image name: mouclass.sys
    Timestamp:        Tue Mar 25 07:03:09 2003 (3E7FFF2D)
    CheckSum:         000062DB
    ImageSize:        0000A000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f75c7000 f75d1000   serenum    (deferred)
    Image path: \SystemRoot\system32\DRIVERS\serenum.sys
    Image name: serenum.sys
    Timestamp:        Sat Feb 17 06:06:44 2007 (45D69B74)
    CheckSum:         00009B3C
    ImageSize:        0000A000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f75d7000 f75e2000   fdc        (deferred)
    Image path: \SystemRoot\system32\DRIVERS\fdc.sys
    Image name: fdc.sys
    Timestamp:        Sat Feb 17 06:07:16 2007 (45D69B94)
    CheckSum:         00011681
    ImageSize:        0000B000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f75e7000 f75f5000   imapi      (deferred)
    Image path: \SystemRoot\system32\DRIVERS\imapi.sys
    Image name: imapi.sys
    Timestamp:        Sat Feb 17 06:08:22 2007 (45D69BD6)
    CheckSum:         0000D14B
    ImageSize:        0000E000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f75f7000 f7600000   watchdog   (deferred)
    Image path: \SystemRoot\system32\DRIVERS\watchdog.sys
    Image name: watchdog.sys
    Timestamp:        Sat Feb 17 06:11:45 2007 (45D69CA1)
    CheckSum:         00009AB6
    ImageSize:        00009000
    File version:     5.2.3790.3959
    Product version:  5.2.3790.3959
    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:   5.2.3790.3959
    FileVersion:      5.2.3790.3959 (srv03_sp2_rtm.070216-1710)
    FileDescription:  Watchdog Driver
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
f7607000 f760fa00   pcntpci5   (deferred)
```

```
    Image path: \SystemRoot\system32\DRIVERS\pcntpci5.sys
    Image name: pcntpci5.sys
    Timestamp:        Tue Jun 05 20:54:43 2001 (3B1D3903)
    CheckSum:         0001827B
    ImageSize:        00008A00
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f7617000 f7620f80   es1371mp   (deferred)
    Image path: \SystemRoot\system32\drivers\es1371mp.sys
    Image name: es1371mp.sys
    Timestamp:        Mon Jun 03 19:18:31 2002 (3CFBB2F7)
    CheckSum:         00016042
    ImageSize:        00009F80
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f7627000 f7630000   ndistapi   (deferred)
    Image path: \SystemRoot\system32\DRIVERS\ndistapi.sys
    Image name: ndistapi.sys
    Timestamp:        Sat Feb 17 05:59:19 2007 (45D699B7)
    CheckSum:         00010072
    ImageSize:        00009000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f7637000 f7646000   raspppoe   (deferred)
    Image path: \SystemRoot\system32\DRIVERS\raspppoe.sys
    Image name: raspppoe.sys
    Timestamp:        Sat Feb 17 05:59:23 2007 (45D699BB)
    CheckSum:         0001208D
    ImageSize:        0000F000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f7647000 f7652000   TDI        (deferred)
    Image path: \SystemRoot\system32\DRIVERS\TDI.SYS
    Image name: TDI.SYS
    Timestamp:        Sat Feb 17 06:01:19 2007 (45D69A2F)
    CheckSum:         0000C620
    ImageSize:        0000B000
    File version:     5.2.3790.3959
    Product version:  5.2.3790.3959
    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:   5.2.3790.3959
    FileVersion:      5.2.3790.3959 (srv03_sp2_rtm.070216-1710)
    FileDescription:  TDI Wrapper
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
f7657000 f7662000   ptilink    (deferred)
    Image path: \SystemRoot\system32\DRIVERS\ptilink.sys
    Image name: ptilink.sys
    Timestamp:        Sat Feb 17 06:06:38 2007 (45D69B6E)
    CheckSum:         0000D201
    ImageSize:        0000B000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f7667000 f7670000   raspti     (deferred)
    Image path: \SystemRoot\system32\DRIVERS\raspti.sys
    Image name: raspti.sys
    Timestamp:        Sat Feb 17 05:59:23 2007 (45D699BB)
    CheckSum:         0001246A
    ImageSize:        00009000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f7677000 f7686000   termdd     (deferred)
    Image path: \SystemRoot\system32\DRIVERS\termdd.sys
    Image name: termdd.sys
    Timestamp:        Sat Feb 17 05:44:32 2007 (45D69640)
    CheckSum:         0000ED7D
    ImageSize:        0000F000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f7687000 f7690000   mssmbios   (deferred)
```

```
    Image path: \SystemRoot\system32\DRIVERS\mssmbios.sys
    Image name: mssmbios.sys
    Timestamp:        Sat Feb 17 05:59:12 2007 (45D699B0)
    CheckSum:         0000C632
    ImageSize:        00009000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f7697000 f76a5000   NDProxy    (deferred)
    Image path: \SystemRoot\System32\Drivers\NDProxy.SYS
    Image name: NDProxy.SYS
    Timestamp:        Sat Feb 17 05:59:21 2007 (45D699B9)
    CheckSum:         0000EC7F
    ImageSize:        0000E000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f76b7000 f76c1000   flpydisk   (deferred)
    Image path: \SystemRoot\system32\DRIVERS\flpydisk.sys
    Image name: flpydisk.sys
    Timestamp:        Tue Mar 25 07:04:32 2003 (3E7FFF80)
    CheckSum:         000132D1
    ImageSize:        0000A000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f76c7000 f76d3000   vga        (deferred)
    Image path: \SystemRoot\System32\drivers\vga.sys
    Image name: vga.sys
    Timestamp:        Sat Feb 17 06:10:30 2007 (45D69C56)
    CheckSum:         00014C94
    ImageSize:        0000C000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f76d7000 f76e2000   Msfs       (deferred)
    Image path: \SystemRoot\System32\Drivers\Msfs.SYS
    Image name: Msfs.SYS
    Timestamp:        Sat Feb 17 05:50:33 2007 (45D697A9)
    CheckSum:         000118ED
    ImageSize:        0000B000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f76e7000 f76f4000   Npfs       (deferred)
    Image path: \SystemRoot\System32\Drivers\Npfs.SYS
    Image name: Npfs.SYS
    Timestamp:        Sat Feb 17 05:50:36 2007 (45D697AC)
    CheckSum:         00015D8A
    ImageSize:        0000D000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f76f7000 f7705000   msgpc      (deferred)
    Image path: \SystemRoot\system32\DRIVERS\msgpc.sys
    Image name: msgpc.sys
    Timestamp:        Sat Feb 17 05:58:37 2007 (45D6998D)
    CheckSum:         0001679D
    ImageSize:        0000E000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f7707000 f770f000   kdcom      (deferred)
    Image path: kdcom.dll
    Image name: kdcom.dll
    Timestamp:        Tue Mar 25 07:08:00 2003 (3E800050)
    CheckSum:         0000E3AA
    ImageSize:        00008000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f770f000 f7717000   BOOTVID    (deferred)
    Image path: \WINDOWS\system32\BOOTVID.dll
    Image name: BOOTVID.dll
    Timestamp:        Tue Mar 25 07:07:58 2003 (3E80004E)
    CheckSum:         00008BE3
    ImageSize:        00008000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f7717000 f771e000   intelide   (deferred)
    Image path: intelide.sys
    Image name: intelide.sys
    Timestamp:        Sat Feb 17 06:07:32 2007 (45D69BA4)
    CheckSum:         0000B3A2
    ImageSize:        00007000
    File version:     5.2.3790.3959
    Product version:  5.2.3790.3959
```

```
    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:   5.2.3790.3959
    FileVersion:      5.2.3790.3959 (srv03_sp2_rtm.070216-1710)
    FileDescription:  Intel PCI IDE Driver
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
f771f000 f7726000   dmload     (deferred)
    Image path: dmload.sys
    Image name: dmload.sys
    Timestamp:        Tue Mar 25 07:08:08 2003 (3E800058)
    CheckSum:         00004F35
    ImageSize:        00007000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f774f000 f7754180   usbuhci    (deferred)
    Image path: \SystemRoot\system32\DRIVERS\usbuhci.sys
    Image name: usbuhci.sys
    Timestamp:        Sat Feb 17 06:13:02 2007 (45D69CEE)
    CheckSum:         0000FDE1
    ImageSize:        00005180
    File version:     5.2.3790.3959
    Product version:  5.2.3790.3959
    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:     USBUHCI.sys
    OriginalFilename: USBUHCI.sys
    ProductVersion:   5.2.3790.3959
    FileVersion:      5.2.3790.3959 (srv03_sp2_rtm.070216-1710)
    FileDescription:  UHCI USB Miniport Driver
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
f7757000 f775f000   audstub    (deferred)
    Image path: \SystemRoot\system32\DRIVERS\audstub.sys
    Image name: audstub.sys
    Timestamp:        Tue Mar 25 07:09:12 2003 (3E800098)
    CheckSum:         00005AA7
    ImageSize:        00008000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f7767000 f776f000   Fs_Rec     (deferred)
    Image path: \SystemRoot\System32\Drivers\Fs_Rec.SYS
    Image name: Fs_Rec.SYS
    Timestamp:        Tue Mar 25 07:08:36 2003 (3E800074)
    CheckSum:         0000F5E9
    ImageSize:        00008000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f776f000 f7776000   Null       (deferred)
    Image path: \SystemRoot\System32\Drivers\Null.SYS
    Image name: Null.SYS
    Timestamp:        Tue Mar 25 07:03:05 2003 (3E7FFF29)
    CheckSum:         0000C34A
    ImageSize:        00007000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f7777000 f777e000   Beep       (deferred)
    Image path: \SystemRoot\System32\Drivers\Beep.SYS
    Image name: Beep.SYS
    Timestamp:        Tue Mar 25 07:03:04 2003 (3E7FFF28)
    CheckSum:         0000B82F
    ImageSize:        00007000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f777f000 f7787000   mnmdd      (deferred)
```

```
    Image path: \SystemRoot\System32\Drivers\mnmdd.SYS
    Image name: mnmdd.SYS
    Timestamp:        Tue Mar 25 07:07:53 2003 (3E800049)
    CheckSum:         0000B73B
    ImageSize:        00008000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f7787000 f778f000   RDPCDD     (deferred)
    Image path: \SystemRoot\System32\DRIVERS\RDPCDD.sys
    Image name: RDPCDD.sys
    Timestamp:        Tue Mar 25 07:03:05 2003 (3E7FFF29)
    CheckSum:         00008EDA
    ImageSize:        00008000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f778f000 f7797000   rasacd     (pdb symbols)
c:\mss\rasacd.pdb\1B61FBD6F931427DBF2E82BA4D54E9471\rasacd.pdb
    Loaded symbol image file: rasacd.sys
    Image path: \SystemRoot\system32\DRIVERS\rasacd.sys
    Image name: rasacd.sys
    Timestamp:        Tue Mar 25 07:11:50 2003 (3E800136)
    CheckSum:         000067ED
    ImageSize:        00008000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f7797000 f779e000   dxgthk     (deferred)
    Image path: \SystemRoot\System32\drivers\dxgthk.sys
    Image name: dxgthk.sys
    Timestamp:        Tue Mar 25 07:05:52 2003 (3E7FFFD0)
    CheckSum:         000019C5
    ImageSize:        00007000
    File version:     5.2.3790.0
    Product version:  5.2.3790.0
    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:     dxgthk.sys
    OriginalFilename: dxgthk.sys
    ProductVersion:   5.2.3790.0
    FileVersion:      5.2.3790.0 (srv03_rtm.030324-2048)
    FileDescription:  DirectX Graphics Driver Thunk
    LegalCopyright:   © Microsoft Corporation. All rights reserved.
f77af000 f77b4180   tmpreflt   (deferred)
    Image path: \??\C:\Program Files\Trend\SProtect\tmpreflt.sys
    Image name: tmpreflt.sys
    Timestamp:        Tue Mar 30 10:35:08 2004 (40693F4C)
    CheckSum:         000092DC
    ImageSize:        00005180
    File version:     7.100.0.1003
    Product version:  7.100.0.1003
    File flags:       28 (Mask 3F) Private Special
    File OS:          40000 NT Base
    File type:        3.8 Driver
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      Trend Micro Inc.
    ProductName:      TMFilter for XP
    InternalName:     TMPreflt.sys
    OriginalFilename: TMPreflt.sys
    ProductVersion:   7.100
    FileVersion:      7.100.0.1003
    PrivateBuild:     Build 1003 - 3/30/2004
    SpecialBuild:     1003
    FileDescription:  Pre-Filter For XP
    LegalCopyright:   Copyright (C) 1999-2004 Trend Micro Incorporated. All rights reserved.
    LegalTrademarks:  Copyright (C) Trend Micro Inc.
f77c7000 f77ce000   parvdm     (deferred)
    Image path: \SystemRoot\system32\DRIVERS\parvdm.sys
    Image name: parvdm.sys
```

```
    Timestamp:        Tue Mar 25 07:03:49 2003 (3E7FFF55)
    CheckSum:         000023C8
    ImageSize:        00007000
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f7897000 f7899980   compbatt   (deferred)
    Image path: compbatt.sys
    Image name: compbatt.sys
    Timestamp:        Sat Feb 17 05:58:51 2007 (45D6999B)
    CheckSum:         0000741E
    ImageSize:        00002980
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f789b000 f789e900   BATTC      (deferred)
    Image path: \WINDOWS\system32\DRIVERS\BATTC.SYS
    Image name: BATTC.SYS
    Timestamp:        Sat Feb 17 05:58:46 2007 (45D69996)
    CheckSum:         0000CFF6
    ImageSize:        00003900
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f793f000 f7942360   vmx_svga   (deferred)
    Image path: \SystemRoot\system32\DRIVERS\vmx_svga.sys
    Image name: vmx_svga.sys
    Timestamp:        Fri Jun 11 01:34:27 2004 (40C8FE13)
    CheckSum:         0000B189
    ImageSize:        00003360
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f7943000 f7946700   CmBatt     (deferred)
    Image path: \SystemRoot\system32\DRIVERS\CmBatt.sys
    Image name: CmBatt.sys
    Timestamp:        Sat Feb 17 05:58:51 2007 (45D6999B)
    CheckSum:         00013110
    ImageSize:        00003700
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f796b000 f796d780   gameenum   (deferred)
    Image path: \SystemRoot\system32\DRIVERS\gameenum.sys
    Image name: gameenum.sys
    Timestamp:        Tue Mar 25 07:10:22 2003 (3E8000DE)
    CheckSum:         00012659
    ImageSize:        00002780
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f7991000 f7992180   SystemDump   (no symbols)
    Loaded symbol image file: SystemDump.sys
    Image path: \??\C:\temp\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
f7993000 f7994060   vmmouse    (deferred)
    Image path: \SystemRoot\system32\DRIVERS\vmmouse.sys
    Image name: vmmouse.sys
    Timestamp:        Fri Jun 11 01:34:47 2004 (40C8FE27)
    CheckSum:         000026E9
    ImageSize:        00001060
    File version:     5.0.2195.1620
    Product version:  5.0.2195.1620
    File flags:       8 (Mask 3F) Private
    File OS:          40004 NT Win32
    File type:        3.7 Driver
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      VMware, Inc.
    ProductName:      VMware Pointing Device
    InternalName:     VMMOUSE
    OriginalFilename: VMMOUSE.SYS
    ProductVersion:   11.0.0.0
    FileVersion:      11.0.0.0 build-8848 JUB4
    FileDescription:  VMware Pointing Device Driver
    LegalCopyright:   Copyright 1998 VMware, Inc.  All rights reserved. -- VMware Confidential
f7995000 f7996280   swenum     (deferred)
    Image path: \SystemRoot\system32\DRIVERS\swenum.sys
```

```
    Image name: swenum.sys
    Timestamp:        Sat Feb 17 06:05:56 2007 (45D69B44)
    CheckSum:         00006FC6
    ImageSize:        00001280
    Translations:     0000.04b0 0000.04e0 0409.04b0 0409.04e0
f7997000 f7998580   USBD       (deferred)
    Image path: \SystemRoot\system32\DRIVERS\USBD.SYS
    Image name: USBD.SYS
    Timestamp:        Tue Mar 25 07:10:39 2003 (3E8000EF)
    CheckSum:         0000A359
    ImageSize:        00001580
    File version:     5.2.3790.0
    Product version:  5.2.3790.0
    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:   5.2.3790.0
    FileVersion:      5.2.3790.0 (srv03_rtm.030324-2048)
    FileDescription:  Universal Serial Bus Driver
    LegalCopyright:   © Microsoft Corporation. All rights reserved.

Unloaded modules:
f7a2d000 f7a2f000   SystemDump.sys
    Timestamp: unavailable (00000000)
    Checksum:  00000000
f775f000 f7767000   Sfloppy.SYS
    Timestamp: unavailable (00000000)
    Checksum:  00000000
```

IRP Distribution

```
kd> !irpfind

  Irp    [ Thread ] irpStack: (Mj,Mn)   DevObj  [Driver]         MDL Process
85925908 [8601f288] irpStack: ( f, 3)  85eb19c8 []
859288f0 [859409f0] irpStack: ( e, 9)  85f20468 [86066e38: is not a driver object
]
8593dcf0 [859475e8] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
8593e548 [859475e8] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85945008 [859475e8] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85946928 [859475e8] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
859485d8 [859475e8] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85948b78 [859475e8] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85949518 [859475e8] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
8595d860 [85ed4718] irpStack: ( e, 0)  85f0c8c0 []
85964ad0 [85fd1350] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
8596f5a8 [85fe2470] irpStack: ( d, 0)  85f27030 [ Name paged out]
8596fc08 [85fe2470] irpStack: ( d, 0)  85f27030 [ Name paged out]
85985140 [85973cd0] irpStack: ( 3, 0)  85f27030 [ Name paged out]
8598b2e8 [85faad88] irpStack: ( 3, 0)  85f27030 [ Name paged out]
859917b0 [859475e8] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85993008 [859945f0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
8599a868 [85c88748] irpStack: ( 3, 0)  85f27030 [ Name paged out]
859b0cd0 [85f05860] irpStack: ( d, 0)  85f27030 [ Name paged out]
859d6d08 [8594c6e0] irpStack: ( d, 0)  85f27030 [ Name paged out]
859d6da8 [85f5fd70] irpStack: ( d, 0)  85f27030 [ Name paged out]
85c5f108 [85f33db0] irpStack: ( 3, 0)  85ff98c8 []
85c87e88 [859856b0] irpStack: ( d, 0)  85f27030 [ Name paged out]
85c881d0 [8596a320] irpStack: ( d, 0)  85f27030 [ Name paged out]
85caf898 [859475e8] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85cb5320 [85973cd0] irpStack: ( d, 0)  85f27030 [ Name paged out]
85cb91e8 [85c8a3d8] irpStack: ( 3, 0)  85f4df10 []
85cb9e48 [86044d08] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85cdaae8 [8597edb0] irpStack: ( e, 0)  85f552b0 [] 0x85980aa0
85d45008 [85d6f660] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
85d452d8 [85d6f660] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
85d45d50 [863234d8] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
85d4f4b8 [85d42660] irpStack: ( d, 0)  86345030 [ \FileSystem\Npfs]
85d52c88 [85d5adb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
85d54e78 [85d42660] irpStack: ( 3, 0)  86345030 [ \FileSystem\Npfs]
85d55bf0 [85d558a0] irpStack: ( e, 0)  865e17e8 [ \Driver\Tcpip]
85d57970 [85d6f660] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
85d57d38 [85d6f660] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
85d5fa48 [85d54440] irpStack: ( d, 0)  86345030 [ \FileSystem\Npfs]
85d5fb28 [862bedb0] irpStack: ( 3, 0)  86345030 [ \FileSystem\Npfs]
85d5fbc8 [85d8eca0] irpStack: ( e, 0)  865e17e8 [ \Driver\Tcpip]
85d5fc68 [85d5b608] irpStack: ( 3, 0)  86345030 [ \FileSystem\Npfs]
85d5fd08 [862d47d8] irpStack: ( d, 0)  86345030 [ \FileSystem\Npfs]
85d5fda8 [85d7b020] irpStack: ( 3, 0)  863ea878 [ \Driver\TermDD]
85d5feb8 [85d48020] irpStack: ( d, 0)  86345030 [ \FileSystem\Npfs]
85d60280 [85d56b18] irpStack: ( e, 0)  862fe988 [ \FileSystem\hgfs] 0x85d56d88
85d65918 [862d47d8] irpStack: ( d, 0)  86345030 [ \FileSystem\Npfs]
85d659b8 [85d62b58] irpStack: ( d, 0)  86345030 [ \FileSystem\Npfs]
85d66e48 [85d783f0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
```

```
85d6aa28 [863b6360] irpStack: ( 3, 0)  86345030 [ \FileSystem\Npfs]
85d727d0 [85d6e758] irpStack: ( 3, 0)  86345030 [ \FileSystem\Npfs]
85d72b68 [862d47d8] irpStack: ( d, 0)  86345030 [ \FileSystem\Npfs]
85d7d348 [85d65400] irpStack: ( e, 0)  864194c0 [ \Driver\IPSec]
85d7e480 [85d788d0] irpStack: ( d, 0)  86345030 [ \FileSystem\Npfs]
85d83bc8 [85d834b8] irpStack: ( 3, 0)  86345030 [ \FileSystem\Npfs]
85d8ba90 [85d72db0] irpStack: ( 3, 0)  86345030 [ \FileSystem\Npfs]
85d8ca70 [85d69db0] irpStack: ( 3, 0)  86345030 [ \FileSystem\Npfs]
85d8f2f0 [862b29d8] irpStack: ( d, 0)  86345030 [ \FileSystem\Npfs]
85d8fcb8 [86338db0] irpStack: ( e, 0)  865e17e8 [ \Driver\Tcpip]
85dc4cd0 [86319870] irpStack: ( d, 0)  86345030 [ \FileSystem\Npfs]
85de5cf8 [863d1880] irpStack: ( d, 0)  86345030 [ \FileSystem\Npfs]
85e9a218 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85e9a4b0 [85f5fd70] irpStack: ( e,20)  85f20468 [86066e38: is not a driver object
] 0x859d2d88
85e9a898 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85e9ab30 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85e9d630 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85e9d8f0 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85e9db30 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85e9de70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85e9e328 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85e9e658 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85ea8b28 [85fa3d20] irpStack: ( 3, 0)  85fdab78 [] 0x85ea94d8
85eac410 [860475b8] irpStack: ( e, 0)  8606a030 [8606a030: is not a device object
]
85ead218 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85eb63b8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85eb9008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85eb9608 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85eb9b08 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85ebd008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85ebd340 [85f86db0] irpStack: ( 3, 0)  85f27030 [ Name paged out]
85ebea40 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85ebee70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85ebf4b0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x316e6f43
85ebf7f0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85ec32f8 [85ea4530] irpStack: ( e, 0)  86048d08 [86048d08: is not a device object
] 0x85eb0310
85ec3e88 [861efdb0] irpStack: ( 3, 0)  85f27030 [ Name paged out]
85ec74b8 [8594c6e0] irpStack: ( d, 0)  85f27030 [ Name paged out]
85eca008 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85ecb318 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x86032380
85ecb5b0 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85ecb7f0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85ecba88 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85ecbcc8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85ecc3a8 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85edf158 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0xf78cad04
85edf658 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85edfb30 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x005ea000
85edfe70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x005ea000
85ee0230 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85ee75f8 [4e4e4e4e] irpStack: (4e,4e)  4e4e4e4e [4e4e4e4e: Could not read device object or
_DEVICE_OBJECT not found
]
85eea970 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85eeac30 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85eeae70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85eeb1c8 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
```

```
]
85eeb408 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85eeb6a0 [85fc5bf0] irpStack: (4e,4e)  860cc718 [8616b768: is not a driver object
]
85eeb838 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85eebb50 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85ef5be8 [85c8b570] irpStack: ( e, 0)  8606a030 [8606a030: is not a device object
]
85f0f008 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f0f350 [85f15020] irpStack: ( 3, 0)  85f27030 [ Name paged out]
85f0f998 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f0fe70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f10398 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f13008 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f13d70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f142a0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f14560 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f147a0 [4e4e4e4e] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f14a88 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f14cc8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f15328 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f15d70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0xf78c6d04
85f1b008 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f1b600 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f1b898 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f1bad8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f1bd70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f1c280 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f1c418 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f1c658 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f1c8f0 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f1d2d0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f1d610 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f1d928 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f1db40 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f1dcd8 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f1de70 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f22228 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f224c0 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f22700 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f22998 [85f33db0] irpStack: ( 3, 0)  85ef4030 []
85f22bd8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f23228 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f23568 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f23800 [85fc02a0] irpStack: ( 3, 0)  85ec6030 [ ]
85f23998 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f23b30 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f24008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00040001
85f25008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x85f9a5c8
85f25418 [00000000] irpStack: (16, 0)  8600e4d8 [86038600: is not a driver object
]
85f25658 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0xfffffffc
```

```
85f258f0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2)
85f25b30 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f26328 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f26568 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f2a468 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x0a09001c
85f2a700 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f2b700 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f2b998 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f2bbd8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0xf6671000
85f2be70 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f2c008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f2c228 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x85fe0e58
85f2c4c0 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f2c700 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0xf6671000
85f2c998 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f2cbd8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x85fe0fa4
85f2ce70 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f38cc8 [85fe2470] irpStack: ( d, 0)  85f27030 [ Name paged out]
85f46598 [85eed4f0] irpStack: ( e, 0)  86048d08 [86048d08: is not a device object
] 0x85eb0310
85f46850 [85ed4718] irpStack: ( 0, 0)  86142480 [86142480: is not a device object
]
85f46e70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f47170 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f47718 [85f46b70] irpStack: ( 3, 0)  85f27030 [ Name paged out]
85f47e70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f48008 [00000000] irpStack: ( f, 0)  8600e4d8 [86038600: is not a driver object
]
85f48468 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f48700 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
85f48940 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f48bd8 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f48d70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f4ee48 [85f7fdb0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f5b318 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f659a8 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f65b40 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f65cd8 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f66008 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f664e0 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f66678 [85fc5bf0] irpStack: (4e,4e)  4e4e4e4e [4e4e4e4e: Could not read device object or
_DEVICE_OBJECT not found
]
85f67868 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f68008 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f68cd8 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f68e70 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f69008 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f691b0 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
```

```
85f69348 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f694e0 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f69b40 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f69cd8 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f69e70 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f76008 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f77898 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f77d70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f785f8 [85f34bf0] irpStack: ( d, 0)  85f27030 [ Name paged out]
85f796b0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f79998 [85997db0] irpStack: ( e,2d)  85f20468 [86066e38: is not a driver object
]
85f79bd8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0xf78ced04
85f7a158 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x85980aa0
85f7ab30 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f7ae70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x85f6c208
85f7c008 [85e9fa60] irpStack: ( e, 0)  85eaa030 []
85f7c370 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f7c898 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f7cd70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f7d820 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00700005
85f7dd48 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00030007
85f7e6b0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x0a150005
85f80998 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f80e70 [8606c310] irpStack: ( e,20)  85f20468 [86066e38: is not a driver object
] 0x85f3dd88
85f81008 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f81600 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f81940 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f81c58 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f82008 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f825b8 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f827f8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f82ae0 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f83258 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f83540 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f83bd8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x000770d5
85f84008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f84418 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f848f0 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f84dc8 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f85558 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f857f0 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f86458 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00001000
85f86798 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f86c58 [859d0db0] irpStack: ( 3, 0)  85f27030 [ Name paged out]
85f86cf8 [85f5fd70] irpStack: ( d, 0)  85f27030 [ Name paged out]
85f877f0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x8607f6a8
85f87b30 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f88d70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f8ca30 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f8d200 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x81b01000
85f8d540 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x85fe61a8
```

```
85f8e008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x85fe61a8
85f8ecc8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x85fe61a8
85f91008 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f92bd8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f92e70 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f93138 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x81b01000
85f93420 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f93660 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f93948 [4e4e4e4e] irpStack: ( 0, 0)  8597f068 [8597f068: is not a device object
]
85f94288 [85f80530] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f94998 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f94e70 [85f63890] irpStack: ( e,2d)  85f20468 [86066e38: is not a driver object
]
85f958f0 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f95b30 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f96a40 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f976d8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x19051105
85f979b0 [8606c310] irpStack: ( d, 0)  85f27030 [ Name paged out]
85f97a50 [85fa59e0] irpStack: ( d, 0)  85f27030 [ Name paged out]
85f98138 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x81b01000
85f98420 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f98660 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x006f0056
85f98b88 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f98e70 [85f4f9e8] irpStack: ( e,20)  85f20468 [86066e38: is not a driver object
] 0x85ea9d88
85f991b0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x81b01000
85f99498 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f99998 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f99e70 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f9a318 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85f9b130 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85f9bb30 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x85bf2970
85f9c448 [00000000] irpStack: ( 0, 0)  85fcdb50 [86024b10: is not a driver object
] 0x00000000
85f9d600 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x86015ca0
85f9d940 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x2e6e6968
85f9f540 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0xf78c6d04
85f9fcd8 [85974840] irpStack: ( e,20)  85f20468 [86066e38: is not a driver object
] 0x85eb1d88
85fa0488 [85ed0020] irpStack: ( 3, 0)  85f27030 [ Name paged out]
85fa0668 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85fa1768 [859754c0] irpStack: ( 3, 0)  85f27030 [ Name paged out]
85fa54c0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85fa6008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85fa6418 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85fa6658 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85fa6b30 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x808be030
85fa6dc8 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85fa73d0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85fa7668 [8597aab8] irpStack: ( e,2d)  85f20468 [86066e38: is not a driver object
]
85fa7bd8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85fa9008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85fa9328 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85fa98a8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
```

```
85fa9b40 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85faa008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x85e9f8c8
85faa478 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x0003e738
85faba30 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85fabd70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x85fd5be8
85fad008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0xffffffff
85fadb30 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000013
85faddc8 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85faf320 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00001000
85faf848 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x0003eaa0
85fafd70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85fb01b0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85fb1188 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85fb1bd8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x0003e811
85fb1e70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x0003e811
85fb2308 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x81b01000
85fb3008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x85f28020
85fb3370 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85fb3898 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x0003eaa0
85fb4450 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x0003e811
85fb4768 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85fb4900 [00000000] Irp is complete (CurrentLocation 5 > StackCount 4)
85fb4e70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85fb5008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0xac0641e4
85fb53b0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85fb5a30 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x0003eaa0
85fb62f8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85fb6820 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85fb7188 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85fb76b0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85fb8008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x0003eaa0
85fb8200 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85fb8700 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x0003eaa0
85fb8bd8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85fb9008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x0003eaa0
85fb96b0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85fb9bd8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x0003c8fb
85fba4e0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85fbb2f8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0xf7066880
85fbbd48 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00002676
85fbc200 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85fbc700 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x0003c8fb
85fbd008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85fbd470 [85f99c18] irpStack: ( e,2d)  85f20468 [86066e38: is not a driver object
]
85fbd6b0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85fbe008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85fbe630 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85fbeb30 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x860793b0
85fbf008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00003a1f
85fbf8a0 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85fbfae0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x000002fd
85fc14c0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x0003c8fb
85fc1998 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00010000
85fc1e70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85fc2348 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85fc2678 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85fc2b40 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85fc2cd8 [00000000] Irp is complete (CurrentLocation 5 > StackCount 4) 0x00000000
85fc3300 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85fc3498 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85fc3e70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85fc7770 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
```

```
85fc7c88 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85fc7e70 [85e9fa60] irpStack: ( e, 0)  85eaa030 [] 0x81b01000
85fc8008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85fc8258 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85fc9678 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85fc9810 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
85fca748 [85f7e1f0] irpStack: ( e,2d)  85f20468 [86066e38: is not a driver object
]
85fca930 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
85fcb178 [85e9fa60] irpStack: ( e, 0)  85eaa030 []
85fcb730 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x85fd0200
85ff0ea0 [8598e420] irpStack: ( d, 0)  85f27030 [ Name paged out]
85ff46b0 [85ec1418] irpStack: ( e, 0)  8606a030 [8606a030: is not a device object
]
85ff4990 [85f8cdb0] irpStack: ( d, 0)  85f27030 [ Name paged out]
85ff4c18 [86093b40] irpStack: ( d, 0)  85f27030 [ Name paged out]
85ff4d80 [85f91888] irpStack: ( 3, 0)  85f27030 [ Name paged out]
85ff4e20 [85f971f0] irpStack: ( 3, 0)  85f27030 [ Name paged out]
85ff4ec0 [85fb7c18] irpStack: ( 3, 0)  85f27030 [ Name paged out]
85ff7650 [8593b2a0] irpStack: ( d, 0)  85f27030 [ Name paged out]
85ff77e0 [85f9cdb0] irpStack: ( d, 0)  85f27030 [ Name paged out]
85ff8008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000100
85ff84c8 [85fc5bf0] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
86001898 [85f9cdb0] irpStack: ( 3, 0)  85f27030 [ Name paged out]
8608dbd8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000cd2
8608de70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000002
8608e008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00140004
8608e308 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
8608e988 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
8608ecc8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0xe17ccb08
8608f710 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x0000535c
86098d38 [85fc02a0] irpStack: ( 3, 0)  85fc6740 [ ]
86099008 [85fd1350] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
8609ac60 [859475e8] irpStack: ( c, 2)  860cc718 [8616b768: is not a driver object
]
8609b640 [00000000] irpStack: ( f, 3)  85eb19c8 []
860b13e0 [85d68a80] irpStack: ( e, 9)  86325558 [ \Driver\AFD]
860b20d8 [85d6f660] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
860bebd8 [85d6f660] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
860c60b0 [862d90f8] irpStack: ( 3, 0)  863e4a08 [ \Driver\Mouclass]
860c9798 [85d49690] irpStack: ( e,20)  86325558 [ \Driver\AFD] 0x862c1c08
860ca478 [863234d8] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
860e67c0 [863234d8] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
862b3518 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
862b52f8 [85d788d0] irpStack: ( d, 0)  86345030 [ \FileSystem\Npfs]
862b5e70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862b6370 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862b6898 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862b8440 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x0a050005
862b8940 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862b8d70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862b9228 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x863fd540
862b94c0 [86374db0] irpStack: ( e,2d)  86325558 [ \Driver\AFD]
862b9700 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862b9bd8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862bb3c0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862bc5b0 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
862bf5f0 [85d6f660] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
862c0b30 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862c0e70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862c1008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x808a6280
862c2658 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862c2b30 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862c5d70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
```

```
862c6328 [85d5a548] irpStack: ( e,2d)  86325558 [ \Driver\AFD]
862c9998 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00040001
862c9c30 [85d6e478] irpStack: ( e,2d)  86325558 [ \Driver\AFD]
862c9e70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x8639c71c
862ca3b0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862ca6f0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862cb988 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862cbc88 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
862cbe48 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
862cce70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x8639ce58
862cd4c0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0xf795b000
862cd998 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x8639cfa4
862cde70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862ce3b0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000004
862d1848 [862d47d8] irpStack: ( d, 0)  86345030 [ \FileSystem\Npfs]
862d4280 [8630cdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
862d4ad8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862d6578 [86374db0] irpStack: ( d, 0)  86345030 [ \FileSystem\Npfs]
862d8530 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x863fc518
862d8a30 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x8630cdb0
862d8e48 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
862da470 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
862da630 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
862da948 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
862dab08 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
862dc1d8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862dc700 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862deb30 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862dee70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862df618 [85d76db0] irpStack: ( e, 0)  86306ab0 [ \FileSystem\MRxSmb]
862e0008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x0d000845
862e1658 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00002015
862e1b30 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862e3008 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
862e3300 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
862e4e70 [00000000] irpStack: (16, 0)  862cc480 [ \Driver\usbuhci]
862e53b0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862e56f0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x003db000
862e5a30 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x003db000
862e5d70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862e61a0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862e64b8 [862d90f8] irpStack: ( 3, 0)  863bdaa0 [ \Driver\Mouclass]
862e7d70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862e81a8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862e84e8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862e9008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862eb008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862eb700 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0xf793f000
862ebbd8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x863fed44
862ec468 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862ec7a8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x86433518
862ed7d8 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
862edbd8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862ee228 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x863ff24c
862ee700 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862eec88 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
862eee48 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
862f02f0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x8082061e
862f08a0 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
862f0a60 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
862f2008 [85d76db0] irpStack: ( e, 0)  86306ab0 [ \FileSystem\MRxSmb]
862f26b0 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
862f2870 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
862f2bd8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862f3470 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x0108070a
862f3970 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862f3e70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x863ffc88
862f4440 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862f6230 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862f7270 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
```

```
862f7430 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
862f83e8 [8645d4c8] irpStack: ( 3, 0)  86345030 [ \FileSystem\Npfs]
862f8d70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862f9800 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2)
862f9c88 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
862f9e48 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
862fa008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0xf78cad04
862fb658 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862fb998 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
862fd330 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
862fd4f0 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
862fe4d8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x008ac000
862ff230 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
862ff3f0 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86300008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86300a98 [863fc020] irpStack: ( 3, 0)  863ae788 [ \Driver\Ndisuio] 0x86433518
86300d70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
863013d0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86305800 [862d47d8] irpStack: ( d, 0)  86345030 [ \FileSystem\Npfs]
86306388 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
863066c8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0xf78cad04
86307008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x86599e70
86307b30 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x8639f910
86308498 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86308998 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86309008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86309440 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86309780 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86309be0 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86309da0 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8630a3e8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
8630c258 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8630c418 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8630e4d8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000001
8630e9b0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x86433518
8630ecf0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x862fdbf0
86310550 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86310890 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86313898 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86313bd8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x0a0e0002
86314d70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x86433518
863156f0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x85d56d88
86315a30 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86315d70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86316830 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
863169f0 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8631d7a8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
8631e008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
8631e200 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0xfffffffc
8631e700 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x0a050013
8631ebd8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
8631f008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x86418988
8631f630 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x006f0072
8631fb30 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86320008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86320530 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x86418a28
86320a30 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86320d70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86321418 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86321c88 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86321e48 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8632f008 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8632f2a8 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86333008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x863a00e0
86333b30 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
863344c0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x0a050010
8633e898 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000001
86340008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000001
863406d8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000038
86340bd8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x0a0a0013
```

```
86341008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x0a06000a
863415e0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0xf6cbc97b
86341ae0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86341dc8 [863b3258] irpStack: ( 3, 0)  864047f0 [ \Driver\Kbdclass]
86342470 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
863446b0 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86347818 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86347b58 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
863483c0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x8c35c34f
86348658 [86344db0] irpStack: ( e,20)  86325558 [ \Driver\AFD] 0x86342988
86348898 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x11d0a61a
86348d70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86349008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0xc0009296
86349228 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86349be0 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86349da0 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8634a4c0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x0a214806
8634abe8 [8633c468] irpStack: ( 3, 0)  86345030 [ \FileSystem\Npfs]
8634d5a0 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8634fad8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x0a070002
8634fd70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x85d56d88
86350688 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
863511a8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0xffffffff
86352228 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x0000faf0
86352700 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86352bd8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86353008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000002
86353228 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000001
86353700 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000002
86353bd8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x0000080d
863565b8 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86356a90 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86359a78 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86359c88 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86359e48 [863b3258] irpStack: ( 3, 0)  863c7aa0 [ \Driver\Kbdclass]
8635a158 [00000000] irpStack: ( 0, 0)  8641a2e0 [ \Driver\Cdrom] 0x00000000
8635ad70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
8635b008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x863cfc90
8635ba18 [00000000] Irp is complete (CurrentLocation 5 > StackCount 4) 0x85d6da78
8635bdc8 [00000000] irpStack: ( 0, 0)  00000000 [00000000: Could not read device object or
_DEVICE_OBJECT not found
] 0x00000000
863603b0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
863606f0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86363700 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x808a6280
86363bd8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86366240 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86366c88 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86366e48 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86367bd8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0xe1650888
86367e70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0xe1650888
86368008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0xe1650888
86368308 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0xe1650888
86368648 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0xe1650888
86368988 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0xe1650888
86368cc8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0xe1650888
863693c0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0xe1650888
86369d70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000007
8636a2c0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
8636a798 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x0a070002
8636aad8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86370558 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86370a30 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86370d70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
863713e8 [862cab28] irpStack: ( e, 0)  8632fd08 [ \Driver\NetBT] 0x862fdbf0
863717d8 [862dcdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86371a40 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86373bd8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86375008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86375cc8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
```

```
86376bb0 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86376d70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86378c88 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86378e48 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8637b2d8 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8637b498 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8637c4c0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
8637db30 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
8637de70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
8637e2d0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
8637ec88 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8637ee48 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8637f3f8 [00000000] Irp is complete (CurrentLocation 5 > StackCount 4)
8637fa18 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
8637fe70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
863804c0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
863836f0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86383a30 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86383d70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
863846f0 [864258d8] irpStack: ( d, 0)  86345030 [ \FileSystem\Npfs]
86384838 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86384ad0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86386008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
863862d8 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86386498 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86386700 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86386bd8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86386e70 [85d5a7b8] irpStack: ( e,2d)  86325558 [ \Driver\AFD]
86388c88 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86388e48 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8638a008 [8631b4f0] irpStack: ( e,2d)  86325558 [ \Driver\AFD]
8638a798 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
8638ad70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
8638b970 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
8638be70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
8638c228 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00300012
8638ca70 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8638cc30 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8638d600 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8638d7c0 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8638dcd8 [85d76db0] irpStack: ( e, 0)  86306ab0 [ \FileSystem\MRxSmb] 0x86433518
8638fc60 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86391b40 [862b29d8] irpStack: ( e,20)  86325558 [ \Driver\AFD] 0x8635fb50
86392678 [863d1880] irpStack: ( e,20)  86325558 [ \Driver\AFD] 0x85de8d88
86393318 [85d76db0] irpStack: ( e, 0)  86306ab0 [ \FileSystem\MRxSmb]
8639b4d8 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8639b698 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8639c790 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8639c950 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8639dc88 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8639de48 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
863a0c88 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
863a0e48 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
863a2ac8 [865a0020] irpStack: ( 3, 0)  86345030 [ \FileSystem\Npfs]
863a2c20 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
863a2de0 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
863ad008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x81b01000
863ad848 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x81b01000
863aeb08 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
863afcd8 [00000000] irpStack: ( f, 0)  862cc480 [ \Driver\usbuhci]
863b0888 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
863b0a48 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
863b0e70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
863b1468 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
863b1940 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
863b23b0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
863b26f0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
863b3558 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
863b3898 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x0044005c
863b76d8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
```

```
863b7bd8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
863b8138 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x85d6da78
863b91b0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
863b9d70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
863ba320 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x81b01000
863bad48 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
863bcaa0 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
863bcc60 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
863be5d8 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
863be798 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
863c0410 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
863c8630 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
863ce300 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
863d2320 [86331240] irpStack: ( 3, 0)  86345030 [ \FileSystem\Npfs]
863d24c8 [862bedb0] irpStack: ( d, 0)  86345030 [ \FileSystem\Npfs]
863d2690 [862bedb0] irpStack: ( d, 0)  86345030 [ \FileSystem\Npfs]
863d27d0 [86344db0] irpStack: ( d, 0)  86345030 [ \FileSystem\Npfs]
863d2ab0 [860cadb0] irpStack: ( d, 0)  86345030 [ \FileSystem\Npfs]
863e2e28 [862b4d10] irpStack: ( e, 0)  865e17e8 [ \Driver\Tcpip]
863e2ec8 [862e7a70] irpStack: ( 3, 0)  86345030 [ \FileSystem\Npfs]
863e7c88 [85d6f660] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
863e7e48 [862b2c48] irpStack: ( f, 3)  865e5f18 [ \Driver\Tcpip]
863fcc10 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
863fcdd0 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86403108 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
864032c8 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86405008 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
864052b0 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8640b8f0 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8640bab0 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86410008 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
864102b0 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86415610 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86416970 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86416b30 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8641c500 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8641c6c0 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8641c880 [85d48b40] irpStack: ( 3, 0)  86345030 [ \FileSystem\Npfs]
8641cbd8 [8645adb0] irpStack: ( d, 0)  86345030 [ \FileSystem\Npfs]
8641cd18 [85d85020] irpStack: ( d, 0)  86345030 [ \FileSystem\Npfs]
8641cdb8 [862e9db0] irpStack: ( 3, 0)  86345030 [ \FileSystem\Npfs]
8641ce58 [86351db0] irpStack: ( 3, 0)  86345030 [ \FileSystem\Npfs]
8641f6e8 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8641fd70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86420d70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
864215b8 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86422008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x860b13e0
86422bd8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x85d56d88
86424558 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86424898 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86424bd8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x86417000
86425bd8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x0a070002
86425e70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86426378 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86427320 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86427b28 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
864284c0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
864288e8 [862fa740] irpStack: ( d, 0)  864b0020 [ \FileSystem\Ntfs]
864294c0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86429998 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x86417000
8642a008 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8642aa28 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8642ad70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
8642b228 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
8642b700 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x81b01000
8642c228 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
8642ea80 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8642f4a8 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86430008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
864302d0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x86417000
```

```
86430888 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86431658 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86431c10 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86433798 [8637bc20] irpStack: ( e, 0)  8632fd08 [ \Driver\NetBT] 0x862fdbf0
86433940 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
864347e8 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86434cc0 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86435008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86435228 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86435700 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00610072
86435cc0 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
864371b0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
864374e0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
864392f8 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
864394b8 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8643ccd8 [00000000] Irp is complete (CurrentLocation 4 > StackCount 3)
86441008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x81b01000
86441b30 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x81b01000
86442008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86442478 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86442cc8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86443660 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86444c30 [85de5db0] irpStack: ( 3, 0)  86345030 [ \FileSystem\Npfs]
86444cd0 [86344db0] irpStack: ( d, 0)  86345030 [ \FileSystem\Npfs]
864459b0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86445ee8 [863d1880] irpStack: ( d, 0)  86345030 [ \FileSystem\Npfs]
86446cf0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
864484d8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86448818 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86448b58 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86449a30 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
8644b848 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8644ba08 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8644cd20 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x81b01000
8644d5a0 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8644d760 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8644dbb0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x85d56d88
8644ecb8 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8644f008 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
8644fbb0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86450510 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86450e48 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86451200 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86451620 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86452458 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86452798 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86452ad8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86453d70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86455e70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x81b01000
86457c88 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86457e48 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86458640 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
86458e70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86459468 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
864597a8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x860e6020
8645abf8 [862ce870] irpStack: ( 3, 0)  86345030 [ \FileSystem\Npfs]
8645d9b0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
8645e558 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
8645ea30 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
8645ed70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x81b01000
8645fbd8 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86460580 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86461328 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
8646b008 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
8646b2a8 [8630fdb0] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
864a0e48 [85d6f660] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
864a5e70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
86547200 [8640e1b0] irpStack: ( d, 0)  86345030 [ \FileSystem\Npfs]
865487e0 [00000000] irpStack: ( e, 0)  8656b5e0 [ \Driver\ACPI]
86598990 [00000000] Irp is complete (CurrentLocation 21 > StackCount 20)
```

```
865a04b0 [862fa740] irpStack: ( c, 2)  864b0020 [ \FileSystem\Ntfs]
865a7a20 [00000000] Irp is complete (CurrentLocation 6 > StackCount 5) 0x00000000
865a8760 [8659db40] irpStack: ( e, 0)  8655de00 [ \Driver\Ftdisk]
865c5100 [86359698] irpStack: ( d, 0)  86345030 [ \FileSystem\Npfs]
865c5920 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1) 0x00000000
865c5c08 [00000000] Irp is complete (CurrentLocation 2 > StackCount 1) 0x00000000
865e42a0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x863e7e48
865e4740 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x81b01000
865e4be0 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
865e5c70 [00000000] Irp is complete (CurrentLocation 3 > StackCount 2) 0x00000000
```