Defect
Detect

Windows Memory Dump Analysis Accelerated

Version 6

Part 2: Kernel and Complete Spaces

Dmitry Vostokov
Software Diagnostics Services

Published by OpenTask, Republic of Ireland

OpenTask books and magazines are available through booksellers and distributors worldwide. For further information or comments, send requests to press@opentask.com.

A CIP catalog record for this book is available from the British Library.

ISBN-l3: 978-1-912636-93-8 (Paperback)

Revision 6.00 (July 2023)

Contents

About the Author 5

Presentation Slides and Transcript 7

Review of x64 Disassembly 37

Practice Exercises 49

Exercise 0: Download, setup, and verify your WinDbg or Debugging Tools for Windows installation, or Docker Debugging Tools for Windows image 54

Exercise K1: Analysis of a normal kernel dump (64-bit) 68

Exercise K2: Analysis of a kernel dump with pool leak (64-bit) 122

Exercise K3: Analysis of a kernel dump with pool corruption (64-bit) 137

Exercise K4: Analysis of a kernel dump with code corruption (64-bit) 144

Exercise K5: Analysis of a kernel dump with hang I/O (64-bit) 163

Exercise K6: Analysis of a kernel dump with stack overflow (64-bit) 183

Exercise K7: Analysis of a kernel dump with stack overwrite (64-bit) 198

Exercise K8: Analysis of a kernel dump with blocked service process (64-bit) 204

Exercise C1: Analysis of a normal complete dump (64-bit) 221

Exercise C2: Analysis of a problem complete dump (64-bit) 240

Exercise C3: Analysis of a problem complete dump (64-bit) 274

Exercise C4: Analysis of a problem complete dump (64-bit) 287

Exercise C5: Analysis of a problem complete dump (64-bit) 312

Application Source Code 325

AppA 327

AppB 329

AppC 331

AppE 333

AppK 335

ServiceA 336

Selected Q&A 339

Minidump Analysis 365

Scripts and WinDbg Commands 365

Component Identification 368

Raw Stack Data Analysis 373

Symbols and Images 382

Wait Chain (Executive Resources) 385

Exercise K1: Analysis of a normal kernel dump (64-bit)

Goal: Learn how to get various information related to hardware, system, sessions, processes, threads, and modules.

Patterns: NULL Pointer (Data); False Effective Address; Invalid Pointer (General); Virtualized System (WOW64); Stack Trace Collection (Unmanaged Space); Unloaded Module.

1. Launch WinDbg.

2. Open \AWMDA-Dumps\Kernel\x64\MEMORY-PageFault.DMP.

3. We get the dump file loaded:

```
Microsoft (R) Windows Debugger Version 10.0.25877.1004 AMD64
Copyright (c) Microsoft Corporation. All rights reserved.


Loading Dump File [C:\AWMDA-Dumps\Kernel\x64\MEMORY-PageFault.DMP]
Kernel Bitmap Dump File: Kernel address space is available, User address space may not be
available.


************* Path validation summary **************
Response                         Time (ms)     Location
Deferred                                       srv*
Symbol search path is: srv*
Executable search path is:
Windows 10 Kernel Version 19041 MP (2 procs) Free x64
Product: WinNt, suite: TerminalServer SingleUserTS Personal
Edition build lab: 19041.1.amd64fre.vb_release.191206-1406
Machine Name:
Kernel base = 0xfffff803`18200000 PsLoadedModuleList = 0xfffff803`18e2a230
Debug session time: Sun Sep 26 13:27:34.008 2021 (UTC + 1:00)
System Uptime: 0 days 0:25:13.988
Loading Kernel Symbols
................................................................
.................................................................
.................................................................
.......
Loading User Symbols
PEB is paged out (Peb.Ldr = 0000005b`e4328018).  Type ".hh dbgerr001" for details
Loading unloaded module list
..........
For analysis of this file, run !analyze -v
nt!KeBugCheckEx:
fffff803`185f71c0 48894c2408      mov     qword ptr [rsp+8],rcx
ss:0018:fffff406`ca7d46a0=000000000000000a
```

Note: We see that the debugger suggests **!analyze -v** command. But we start with low-level command exploration instead to learn more WinDbg commands for better diagnostic analysis accuracy.

4. We open a log file:

```
0: kd> .logopen C:\AWMDA-Dumps\Kernel\x64\MEMORY-PageFault.log
Opened log file 'C:\AWMDA-Dumps\Kernel\x64\MEMORY-PageFault.log'
```

5. We check the stack trace of the current thread running on the current processor (**k** command):

```
0: kd> k
 # Child-SP          RetAddr               Call Site
00 fffff406`ca7d4698 fffff803`18609169     nt!KeBugCheckEx
01 fffff406`ca7d46a0 fffff803`18605469     nt!KiBugCheckDispatch+0x69
02 fffff406`ca7d47e0 fffff803`15431981     nt!KiPageFault+0x469
Unable to load image \??\C:\WINDOWS\system32\drivers\myfault.sys, Win32 error 0n2
03 fffff406`ca7d4970 fffff803`15431d3d     myfault+0x1981
04 fffff406`ca7d49a0 fffff803`15431ea1     myfault+0x1d3d
05 fffff406`ca7d4ae0 fffff803`1848f865     myfault+0x1ea1
06 fffff406`ca7d4b40 fffff803`18875328     nt!IofCallDriver+0x55
07 fffff406`ca7d4b80 fffff803`18874bf5     nt!IopSynchronousServiceTail+0x1a8
08 fffff406`ca7d4c20 fffff803`188745f6     nt!IopXxxControlFile+0x5e5
09 fffff406`ca7d4d60 fffff803`18608bb5     nt!NtDeviceIoControlFile+0x56
0a fffff406`ca7d4dd0 00007ffe`4bf2ce54     nt!KiSystemServiceCopyEnd+0x25
0b 0000005b`e44fedb8 00000000`00000000     0x00007ffe`4bf2ce54
```

Note: We see the `myfault` module. We used the NotMyFault tool from Sysinternals to trigger a kernel dump:

https://docs.microsoft.com/en-us/sysinternals/downloads/notmyfault

Note: We see that almost all addresses have **FFFFF** as the first digits. Welcome to the kernel space. The only address **00007ffe`4bf2ce54** is included because this is a return address to the process user space. We notice that the **myfault** module caused a page fault (a memory access exception). We also see that the thread was running on the processor/CPU/core No. 0 (0-based counting) because of the prompt **0: kd>**.

6. We can get more detailed information about the current thread by using the **!thread** command:

```
0: kd> !thread
THREAD ffffdb0de16bd080  Cid 0dec.1e28  Teb: 0000005be4329000 Win32Thread: ffffdb0dddc561a0 RUNNING on processor 0
IRP List:
    ffffdb0de17fcea0: (0006,0118) Flags: 00060000  Mdl: 00000000
Not impersonating
DeviceMap                 ffffae0391bb2810
Owning Process            ffffdb0ddbb27080       Image:         notmyfault64.exe
Attached Process          N/A            Image:         N/A
Wait Start TickCount      96894          Ticks: 1 (0:00:00:00.015)
Context Switch Count      3157           IdealProcessor: 1
UserTime                  00:00:00.062
KernelTime                00:00:00.390
Win32 Start Address 0x00007ff6a93f5384
Stack Init fffff406ca7d4fd0 Current fffff406ca7d4010
Base fffff406ca7d5000 Limit fffff406ca7cf000 Call 0000000000000000
Priority 12 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
Child-SP          RetAddr               : Args to Child                                                           : Call Site
fffff406`ca7d4698 fffff803`18609169     : 00000000`0000000a ffffae03`917c7760 00000000`00000002 00000000`00000000 : nt!KeBugCheckEx
fffff406`ca7d46a0 fffff803`18605469     : 00007ffe`4bf2cc00 00000000`00000000 00000000`00000f4d 00000000`00000000 : nt!KiBugCheckDispatch+0x69
fffff406`ca7d47e0 fffff803`15431981     : 00000000`00000000 fffff406`ca7d49c8 00000000`00000000 00000000`00000000 : nt!KiPageFault+0x469 (TrapFrame @
fffff406`ca7d47e0)
fffff406`ca7d4970 fffff803`15431d3d     : 00000000`917c6760 00000237`89f794e0 00000000`000000f0 00000000`00000000 : myfault+0x1981
fffff406`ca7d49a0 fffff803`15431ea1     : ffffdb0d`e17fcea0 00000000`00000000 00000000`00000000 fffff803`187f5e51 : myfault+0x1d3d
fffff406`ca7d4ae0 fffff803`1848f865     : ffffdb0d`e17fcea0 00000000`00000001 fffff406`ca7d4ec0 00000000`00000001 : myfault+0x1ea1
fffff406`ca7d4b40 fffff803`18875328     : fffff406`ca7d4ec0 ffffdb0d`e17fcea0 00000000`00000001 fffff803`00000000 : nt!IofCallDriver+0x55
fffff406`ca7d4b80 fffff803`18874bf5     : 00000000`00000000 fffff406`ca7d4ec0 00000000`00000000 fffff406`ca7d4ec0 : nt!IopSynchronousServiceTail+0x1a8
fffff406`ca7d4c20 fffff803`188745f6     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : nt!IopXxxControlFile+0x5e5
fffff406`ca7d4d60 fffff803`18608bb5     : 00000000`fffffffc ffff47e9`00000000 00000000`00000001 00000237`89af8a50 : nt!NtDeviceIoControlFile+0x56
fffff406`ca7d4dd0 00007ffe`4bf2ce54     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : nt!KiSystemServiceCopyEnd+0x25 (TrapFrame
@ fffff406`ca7d4e40)
0000005b`e44fedb8 00000000`00000000     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : 0x00007ffe`4bf2ce54
```

Note: **ffffdb0de16bd080** is the address of the kernel thread structure and given any such one, we can examine any thread using the **!thread** *<address>* command (we explore this in later exercises). We see the process image **notmyfault64.exe** and CPU time spent in kernel and user mode, respectively. We also see PID.TID pair (**Cid**). **TrapFrame** is equivalent to thread CONTEXT we encountered and used when analyzing process memory dumps (**.cxr** command) in Part 1. Here we can use the **.trap** command to see the exact processor instruction and module that caused the trap (exception):

```
0: kd> .trap fffff406`ca7d47e0
NOTE: The trap frame does not contain all registers.
Some register values may be zeroed or incorrect.
rax=00000000917c6760 rbx=0000000000000000 rcx=ffffae038d200340
rdx=0000000000000890 rsi=0000000000000000 rdi=0000000000000000
rip=fffff80315431981 rsp=fffff406ca7d4970 rbp=0000000000000002
 r8=ffffae0393bb9db0  r9=0000000000000000 r10=ffffae038d2002c0
r11=ffffae03917c0750 r12=0000000000000000 r13=0000000000000000
r14=0000000000000000 r15=0000000000000000
iopl=0         nv up ei ng nz na pe nc
myfault+0x1981:
fffff803`15431981 8b03            mov     eax,dword ptr [rbx] ds:00000000`00000000=????????

0: kd> k
  *** Stack trace for last set context - .thread/.cxr resets it
 # Child-SP          RetAddr               Call Site
00 fffff406`ca7d4970 fffff803`15431d3d     myfault+0x1981
01 fffff406`ca7d49a0 fffff803`15431ea1     myfault+0x1d3d
02 fffff406`ca7d4ae0 fffff803`1848f865     myfault+0x1ea1
03 fffff406`ca7d4b40 fffff803`18875328     nt!IofCallDriver+0x55
04 fffff406`ca7d4b80 fffff803`18874bf5     nt!IopSynchronousServiceTail+0x1a8
05 fffff406`ca7d4c20 fffff803`188745f6     nt!IopXxxControlFile+0x5e5
06 fffff406`ca7d4d60 fffff803`18608bb5     nt!NtDeviceIoControlFile+0x56
07 fffff406`ca7d4dd0 00007ffe`4bf2ce54     nt!KiSystemServiceCopyEnd+0x25
08 0000005b`e44fedb8 00000000`00000000     0x00007ffe`4bf2ce54
```

Note: The warning that some register values may be zeroed or incorrect means that the access violation may not have happened because of NULL pointer access (**False Effective Address** pattern).

7. As we would see from **!analyze -v** output, later on, the real address was probably **ffffae03917c7760**. Checking the address value (**!pte** command):

```
0: kd> .bugcheck
Bugcheck code 000000D1
Arguments ffffae03`917c7760 00000000`00000002 00000000`00000000 fffff803`15431981

0: kd> !pte ffffae03`917c7760
                                           VA ffffae03917c7760
PXE at FFFFF8FC7E3F1AE0    PPE at FFFFF8FC7E35C070    PDE at FFFFF8FC6B80E458    PTE at FFFFF8D701C8BE38
contains 0A0000013CCCE863  contains 0A0000013CCCF863  contains 0A00000115E34863  contains
000068EA00000000
pfn 13ccce    ---DA--KWEV  pfn 13cccf    ---DA--KWEV  pfn 115e34    ---DA--KWEV  not valid
                                                                                  Page has been freed
```

Note: This shows us that the thread tried accessing memory at the invalid **ffffae03`917c7760** address. This command also shows if the contents of accessed memory reside in a page file.

8.	Now we check the current process by using the short version of **!process** command:

```
0: kd> !process
PROCESS ffffdb0ddbb27080
    SessionId: 1  Cid: 0dec    Peb: 5be4328000  ParentCid: 0494
    DirBase: adf09002  ObjectTable: ffffae0398090580  HandleCount: 188.
    Image: notmyfault64.exe
    VadRoot ffffdb0de21ad4a0 Vads 83 Clone 0 Private 452. Modified 8. Locked 0.
    DeviceMap ffffae0391bb2810
    Token                             ffffae03931d9830
    ElapsedTime                       00:05:01.661
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         192256
    QuotaPoolUsage[NonPagedPool]      11616
    Working Set Sizes (now,min,max)  (3336, 50, 345) (13344KB, 200KB, 1380KB)
    PeakWorkingSetSize                3258
    VirtualSize                       4236 Mb
    PeakVirtualSize                   4249 Mb
    PageFaultCount                    3415
    MemoryPriority                    FOREGROUND
    BasePriority                      8
    CommitCharge                      506
    Job                               ffffdb0de27a4060

        THREAD ffffdb0de16bd080  Cid 0dec.1e28  Teb: 0000005be4329000 Win32Thread: ffffdb0dddc561a0 RUNNING on processor 0
        THREAD ffffdb0de19b4040  Cid 0dec.1c8c  Teb: 0000005be432f000 Win32Thread: 0000000000000000 WAIT: (WrQueue) UserMode Alertable
            ffffdb0de0b1e500  QueueObject

        THREAD ffffdb0de13b0080  Cid 0dec.2234  Teb: 0000005be4331000 Win32Thread: 0000000000000000 WAIT: (WrQueue) UserMode Alertable
            ffffdb0de0b1e500  QueueObject

        THREAD ffffdb0de2416040  Cid 0dec.0fbc  Teb: 0000005be4333000 Win32Thread: 0000000000000000 WAIT: (WrQueue) UserMode Alertable
            ffffdb0de269c0c0  QueueObject

        THREAD ffffdb0de19cb080  Cid 0dec.0ae0  Teb: 0000005be4335000 Win32Thread: 0000000000000000 WAIT: (WrQueue) UserMode Alertable
            ffffdb0de269c0c0  QueueObject
```

Note: ffffdb0ddbb27080 is an address of a process structure in the kernel. The **!process** *<address>* command can be used if you have any such an address, and we explore this later. We also note session Id 1 (console session), Cid (PID), and parent Cid (PID). We also see that the process has one running thread and 4 waiting threads.

9.	Now we check loaded modules using **lm** command:

```
0: kd> lm
start             end                 module name
fffff803`14b10000 fffff803`14d9f000   mcupdate_GenuineIntel   (deferred)
fffff803`14da0000 fffff803`14da6000   hal        (deferred)
fffff803`14db0000 fffff803`14dbb000   kd         (deferred)
fffff803`14dc0000 fffff803`14de7000   tm         (deferred)
fffff803`14df0000 fffff803`14e59000   CLFS       (deferred)
fffff803`14e60000 fffff803`14e7a000   PSHED      (deferred)
fffff803`14e80000 fffff803`14e8b000   BOOTVID    (deferred)
fffff803`14e90000 fffff803`14eff000   FLTMGR     (deferred)
fffff803`14f00000 fffff803`14f0e000   cmimcext   (deferred)
fffff803`15000000 fffff803`15014000   mmcss      (deferred)
fffff803`15020000 fffff803`150e7000   srv2       (deferred)
fffff803`150f0000 fffff803`15142000   mrxsmb10   (deferred)
fffff803`15150000 fffff803`15177000   Ndu        (deferred)
fffff803`15180000 fffff803`15256000   peauth     (deferred)
fffff803`15260000 fffff803`15275000   tcpipreg   (deferred)
fffff803`15280000 fffff803`1529c000   rassstp    (deferred)
fffff803`152a0000 fffff803`152bd000   NDProxy    (deferred)
fffff803`152c0000 fffff803`152eb000   vmhgfs     (deferred)
fffff803`152f0000 fffff803`15302000   condrv     (deferred)
fffff803`15310000 fffff803`15337000   AgileVpn   (deferred)
fffff803`15340000 fffff803`15361000   rasl2tp    (deferred)
fffff803`15370000 fffff803`15391000   raspptp    (deferred)
fffff803`153a0000 fffff803`153bc000   raspppoe   (deferred)
```

```
fffff803`153c0000 fffff803`153cf000   ndistapi   (deferred)
fffff803`153d0000 fffff803`1540b000   ndiswan    (deferred)
fffff803`15410000 fffff803`1542a000   WdNisDrv   (deferred)
fffff803`15430000 fffff803`15438000   myfault    (no symbols)
fffff803`15450000 fffff803`1545e000   dump_diskdump   (deferred)
fffff803`15480000 fffff803`1549f000   dump_lsi_sas   (deferred)
fffff803`154c0000 fffff803`154dd000   dump_dumpfve   (deferred)
fffff803`15ca0000 fffff803`15d34000   mrxsmb     (deferred)
fffff803`15d40000 fffff803`15d86000   mrxsmb20   (deferred)
fffff803`15d90000 fffff803`15d9a000   vmmemctl   (deferred)
fffff803`15da0000 fffff803`15df3000   srvnet     (deferred)
fffff803`18200000 fffff803`19246000   nt         (pdb symbols)
C:\ProgramData\dbg\sym\ntkrnlmp.pdb\1B4A6F5E0766C552C90710C8ACC0295C1\ntkrnlmp.pdb
fffff803`1a400000 fffff803`1a514000   clipsp     (deferred)
fffff803`1a520000 fffff803`1a549000   ksecdd     (deferred)
fffff803`1a550000 fffff803`1a5b3000   msrpc      (deferred)
fffff803`1a5c0000 fffff803`1a5d1000   werkernel   (deferred)
fffff803`1a5e0000 fffff803`1a5ec000   ntosext    (deferred)
fffff803`1a5f0000 fffff803`1a6d3000   CI         (deferred)
fffff803`1a6e0000 fffff803`1a79b000   cng        (deferred)
fffff803`1a7a0000 fffff803`1a871000   Wdf01000   (deferred)
fffff803`1a880000 fffff803`1a893000   WDFLDR     (deferred)
fffff803`1a8a0000 fffff803`1a8af000   SleepStudyHelper   (deferred)
fffff803`1a8b0000 fffff803`1a8c1000   WppRecorder   (deferred)
fffff803`1a8d0000 fffff803`1a8f6000   acpiex     (deferred)
fffff803`1a900000 fffff803`1a91a000   SgrmAgent   (deferred)
fffff803`1a920000 fffff803`1a9ec000   ACPI       (deferred)
fffff803`1a9f0000 fffff803`1a9fc000   WMILIB     (deferred)
fffff803`1aa20000 fffff803`1aa8b000   intelpep   (deferred)
fffff803`1aa90000 fffff803`1aaa7000   WindowsTrustedRT   (deferred)
fffff803`1aab0000 fffff803`1aabb000   IntelTA    (deferred)
fffff803`1aac0000 fffff803`1aacb000   WindowsTrustedRTProxy   (deferred)
fffff803`1aad0000 fffff803`1aae4000   pcw        (deferred)
fffff803`1aaf0000 fffff803`1aafb000   msisadrv   (deferred)
fffff803`1ab00000 fffff803`1ab77000   pci        (deferred)
fffff803`1ab80000 fffff803`1ab95000   vdrvroot   (deferred)
fffff803`1aba0000 fffff803`1abe4000   ucx01000   (deferred)
fffff803`1abf0000 fffff803`1ac1f000   pdc        (deferred)
fffff803`1ac20000 fffff803`1ac3a000   CEA        (deferred)
fffff803`1ac40000 fffff803`1ac71000   partmgr    (deferred)
fffff803`1ac80000 fffff803`1ad2a000   spaceport   (deferred)
fffff803`1ad30000 fffff803`1ad3b000   intelide   (deferred)
fffff803`1ad40000 fffff803`1ad53000   PCIIDEX    (deferred)
fffff803`1ad60000 fffff803`1ad79000   volmgr     (deferred)
fffff803`1ad80000 fffff803`1adcf000   sdbus      (deferred)
fffff803`1add0000 fffff803`1ae33000   volmgrx    (deferred)
fffff803`1ae40000 fffff803`1ae58000   vsock      (deferred)
fffff803`1ae60000 fffff803`1ae7c000   vmci       (deferred)
fffff803`1ae80000 fffff803`1ae98000   urscx01000   (deferred)
fffff803`1aea0000 fffff803`1aebe000   mountmgr   (deferred)
fffff803`1aec0000 fffff803`1aedf000   lsi_sas    (deferred)
fffff803`1aee0000 fffff803`1af93000   storport   (deferred)
fffff803`1afa0000 fffff803`1afad000   atapi      (deferred)
fffff803`1afb0000 fffff803`1afec000   ataport    (deferred)
fffff803`1aff0000 fffff803`1b022000   storahci   (deferred)
fffff803`1b030000 fffff803`1b04c000   EhStorClass   (deferred)
fffff803`1b050000 fffff803`1b06a000   fileinfo   (deferred)
fffff803`1b070000 fffff803`1b0b0000   Wof        (deferred)
fffff803`1b0c0000 fffff803`1b12c000   WdFilter   (deferred)
fffff803`1b130000 fffff803`1b409000   Ntfs       (deferred)
```

```
fffff803`1b410000 fffff803`1b443000   usbccgp    (deferred)
fffff803`1b450000 fffff803`1b45e000   USBD       (deferred)
fffff803`1b460000 fffff803`1b46d000   urschipidea   (deferred)
fffff803`1b470000 fffff803`1b48a000   usbehci    (deferred)
fffff803`1b490000 fffff803`1b509000   USBPORT    (deferred)
fffff803`1b510000 fffff803`1b595000   usbhub     (deferred)
fffff803`1b5a0000 fffff803`1b643000   UsbHub3    (deferred)
fffff803`1b650000 fffff803`1b65d000   Fs_Rec     (deferred)
fffff803`1b660000 fffff803`1b7d0000   ndis       (deferred)
fffff803`1b7e0000 fffff803`1b878000   NETIO      (deferred)
fffff803`1b880000 fffff803`1b8b2000   ksecpkg    (deferred)
fffff803`1b8c0000 fffff803`1bbac000   tcpip      (deferred)
fffff803`1bbb0000 fffff803`1bc2f000   fwpkclnt   (deferred)
fffff803`1bc30000 fffff803`1bc60000   wfplwfs    (deferred)
fffff803`1bc70000 fffff803`1bd38000   fvevol     (deferred)
fffff803`1bd40000 fffff803`1bd4b000   volume     (deferred)
fffff803`1bd50000 fffff803`1bdbd000   volsnap    (deferred)
fffff803`1bdc0000 fffff803`1be5a000   USBXHCI    (deferred)
fffff803`1be60000 fffff803`1be85000   USBSTOR    (deferred)
fffff803`1be90000 fffff803`1bea8000   uaspstor   (deferred)
fffff803`1beb0000 fffff803`1bece000   sdstor     (deferred)
fffff803`1bed0000 fffff803`1bf20000   rdyboost   (deferred)
fffff803`1bf30000 fffff803`1bf56000   mup        (deferred)
fffff803`1bf60000 fffff803`1bf72000   iorate     (deferred)
fffff803`1bfa0000 fffff803`1bfbc000   disk       (deferred)
fffff803`1bfc0000 fffff803`1c02d000   CLASSPNP   (deferred)
fffff803`1c620000 fffff803`1c65f000   HIDCLASS   (deferred)
fffff803`1c660000 fffff803`1c673000   HIDPARSE   (deferred)
fffff803`1c6a0000 fffff803`1c6b0000   mouhid     (deferred)
fffff803`1c6c0000 fffff803`1c6c9000   vmusbmouse   (deferred)
fffff803`1c6d0000 fffff803`1c702000   cdrom      (deferred)
fffff803`1c710000 fffff803`1c723000   mouclass   (deferred)
fffff803`1c730000 fffff803`1c745000   filecrypt   (deferred)
fffff803`1c750000 fffff803`1c75e000   tbs        (deferred)
fffff803`1c760000 fffff803`1c776000   BasicDisplay   (deferred)
fffff803`1c780000 fffff803`1c798000   watchdog   (deferred)
fffff803`1c7a0000 fffff803`1c7aa000   Null       (deferred)
fffff803`1c7b0000 fffff803`1cb5a000   dxgkrnl    (deferred)
fffff803`1cb60000 fffff803`1cb6a000   Beep       (deferred)
fffff803`1cb70000 fffff803`1cb80000   vmrawdsk   (deferred)
fffff803`1cb90000 fffff803`1cc32000   Vid        (deferred)
fffff803`1cc40000 fffff803`1cc61000   winhvr     (deferred)
fffff803`1cc70000 fffff803`1cc81000   BasicRender   (deferred)
fffff803`1cc90000 fffff803`1cca2000   CompositeBus   (deferred)
fffff803`1ccb0000 fffff803`1ccbd000   kdnic      (deferred)
fffff803`1ccc0000 fffff803`1ccd5000   umbus      (deferred)
fffff803`1cce0000 fffff803`1cd01000   i8042prt   (deferred)
fffff803`1cd10000 fffff803`1cd24000   kbdclass   (deferred)
fffff803`1cd30000 fffff803`1cd39000   vmmouse    (deferred)
fffff803`1cd40000 fffff803`1cd5c000   serial     (deferred)
fffff803`1cd60000 fffff803`1cd6f000   serenum    (deferred)
fffff803`1cd70000 fffff803`1cd7a000   vm3dmp_loader   (deferred)
fffff803`1cd80000 fffff803`1cdcb000   vm3dmp     (deferred)
fffff803`1cdd0000 fffff803`1cde0000   usbuhci    (deferred)
fffff803`1cdf0000 fffff803`1ce19000   HDAudBus   (deferred)
fffff803`1ce20000 fffff803`1ce86000   portcls    (deferred)
fffff803`1ce90000 fffff803`1ceb1000   drmk       (deferred)
fffff803`1cec0000 fffff803`1cf36000   ks         (deferred)
fffff803`1cf40000 fffff803`1cfce000   e1i65x64   (deferred)
fffff803`1cfd0000 fffff803`1cfdb000   vmgencounter   (deferred)
```

```
fffff803`1cfe0000 fffff803`1cfef000   CmBatt     (deferred)
fffff803`1cff0000 fffff803`1d000000   BATTC      (deferred)
fffff803`1d010000 fffff803`1d050000   intelppm   (deferred)
fffff803`1d060000 fffff803`1d06d000   NdisVirtualBus   (deferred)
fffff803`1d070000 fffff803`1d080000   mssmbios   (deferred)
fffff803`1d090000 fffff803`1d09c000   swenum     (deferred)
fffff803`1d0a0000 fffff803`1d0ae000   rdpbus     (deferred)
fffff803`1d0b0000 fffff803`1d11f000   HdAudio    (deferred)
fffff803`1d120000 fffff803`1d12f000   ksthunk    (deferred)
fffff803`1d150000 fffff803`1d16e000   crashdmp   (deferred)
fffff803`1d1d0000 fffff803`1d1e2000   hidusb     (deferred)
fffff803`1d200000 fffff803`1d222000   tdx        (deferred)
fffff803`1d230000 fffff803`1d240000   TDI        (deferred)
fffff803`1d250000 fffff803`1d2ac000   netbt      (deferred)
fffff803`1d2b0000 fffff803`1d2c3000   afunix     (deferred)
fffff803`1d2d0000 fffff803`1d376000   afd        (deferred)
fffff803`1d380000 fffff803`1d39a000   vwififlt   (deferred)
fffff803`1d3a0000 fffff803`1d3cb000   pacer      (deferred)
fffff803`1d3d0000 fffff803`1d3e4000   ndiscap    (deferred)
fffff803`1d3f0000 fffff803`1d404000   netbios    (deferred)
fffff803`1d410000 fffff803`1d48b000   rdbss      (deferred)
fffff803`1d490000 fffff803`1d4a2000   nsiproxy   (deferred)
fffff803`1d4b0000 fffff803`1d4be000   npsvctrig   (deferred)
fffff803`1d4c0000 fffff803`1d4ca000   gpuenergydrv   (deferred)
fffff803`1d4d0000 fffff803`1d4fc000   dfsc       (deferred)
fffff803`1d520000 fffff803`1d58c000   fastfat    (deferred)
fffff803`1d590000 fffff803`1d5a7000   bam        (deferred)
fffff803`1d5b0000 fffff803`1d5fe000   ahcache    (deferred)
fffff803`1d600000 fffff803`1d621000   BTHUSB     (deferred)
fffff803`1d630000 fffff803`1d7b5000   BTHport    (deferred)
fffff803`1d7c0000 fffff803`1d7fd000   rfcomm     (deferred)
fffff803`1d800000 fffff803`1d822000   BthEnum    (deferred)
fffff803`1d830000 fffff803`1d856000   bthpan     (deferred)
fffff803`1d900000 fffff803`1d973000   dxgmms1    (deferred)
fffff803`1d980000 fffff803`1d99b000   monitor    (deferred)
fffff803`1d9a0000 fffff803`1da81000   dxgmms2    (deferred)
fffff803`1da90000 fffff803`1dae4000   WUDFRd     (deferred)
fffff803`1daf0000 fffff803`1db19000   luafv      (deferred)
fffff803`1db20000 fffff803`1db56000   wcifs      (deferred)
fffff803`1db60000 fffff803`1dbe2000   cldflt     (deferred)
fffff803`1dbf0000 fffff803`1dc0a000   storqosflt   (deferred)
fffff803`1dc10000 fffff803`1dc38000   bindflt    (deferred)
fffff803`1dc40000 fffff803`1dc58000   lltdio     (deferred)
fffff803`1dc60000 fffff803`1dc78000   mslldp     (deferred)
fffff803`1dc80000 fffff803`1dc9b000   rspndr     (deferred)
fffff803`1dca0000 fffff803`1dcbd000   wanarp     (deferred)
fffff803`1dcc0000 fffff803`1dd16000   msquic     (deferred)
fffff803`1dd20000 fffff803`1dea8000   HTTP       (deferred)
fffff803`1deb0000 fffff803`1ded5000   bowser     (deferred)
fffff803`1dee0000 fffff803`1defa000   mpsdrv     (deferred)
fffff803`1df90000 fffff803`1dfac000   Npfs       (deferred)
fffff803`1dfb0000 fffff803`1dfc1000   Msfs       (deferred)
fffff803`1dfd0000 fffff803`1dfee000   CimFS      (deferred)
fffffcbd`42a00000 fffffcbd`42cd3000   win32kbase   (deferred)
fffffcbd`42ce0000 fffffcbd`43096000   win32kfull   (deferred)
fffffcbd`430a0000 fffffcbd`430e9000   cdd        (deferred)
fffffcbd`432d0000 fffffcbd`4336a000   win32k     (deferred)

Unloaded modules:
fffff803`1d870000 fffff803`1d87f000   dump_storport.sys
```

```
fffff803`1d8a0000 fffff803`1d8c0000   dump_lsi_sas.sys
fffff803`1d8e0000 fffff803`1d8fe000   dump_dumpfve.sys
fffff803`1d180000 fffff803`1d18f000   dump_storport.sys
fffff803`1d1b0000 fffff803`1d1d0000   dump_lsi_sas.sys
fffff803`1c680000 fffff803`1c69e000   dump_dumpfve.sys
fffff803`1d500000 fffff803`1d51c000   dam.sys
fffff803`1de00000 fffff803`1de55000   WUDFRd.sys
fffff803`1aa00000 fffff803`1aa11000   WdBoot.sys
fffff803`1bf80000 fffff803`1bf91000   hwpolicy.sys
```

10. **lmt** command can be used to check timestamps for 3rd-party modules:

```
0: kd> lmt
start             end                 module name
fffff803`14b10000 fffff803`14d9f000   mcupdate_GenuineIntel  9FB1DE46 (This is a reproducible build file hash, not a timestamp)
fffff803`14da0000 fffff803`14da6000   hal      1A7BE8E9 (This is a reproducible build file hash, not a timestamp)
fffff803`14db0000 fffff803`14dbb000   kd       FE185FA8 (This is a reproducible build file hash, not a timestamp)
fffff803`14dc0000 fffff803`14de7000   tm       D8EFCDE6 (This is a reproducible build file hash, not a timestamp)
fffff803`14df0000 fffff803`14e59000   CLFS     B6B72B14 (This is a reproducible build file hash, not a timestamp)
fffff803`14e60000 fffff803`14e7a000   PSHED    4C55DC99 (This is a reproducible build file hash, not a timestamp)
fffff803`14e80000 fffff803`14e8b000   BOOTVID  D13EE5B6 (This is a reproducible build file hash, not a timestamp)
fffff803`14e90000 fffff803`14eff000   FLTMGR   5AFF36CB (This is a reproducible build file hash, not a timestamp)
fffff803`14f00000 fffff803`14f0e000   cmimcext 633C2FE0 (This is a reproducible build file hash, not a timestamp)
fffff803`15000000 fffff803`15014000   mmcss    07117A5A (This is a reproducible build file hash, not a timestamp)
fffff803`15020000 fffff803`150e7000   srv2     E647F001 (This is a reproducible build file hash, not a timestamp)
fffff803`150f0000 fffff803`15142000   mrxsmb10 ABA1F2CF (This is a reproducible build file hash, not a timestamp)
fffff803`15150000 fffff803`15177000   Ndu      ABC6C894 (This is a reproducible build file hash, not a timestamp)
fffff803`15180000 fffff803`15256000   peauth   B0E514F1 (This is a reproducible build file hash, not a timestamp)
fffff803`15260000 fffff803`15275000   tcpipreg 0651E2F3 (This is a reproducible build file hash, not a timestamp)
fffff803`15280000 fffff803`1529c000   rassstp  3C5B7B7A (This is a reproducible build file hash, not a timestamp)
fffff803`152a0000 fffff803`152bd000   NDProxy  77FE1198 (This is a reproducible build file hash, not a timestamp)
fffff803`152c0000 fffff803`152eb000   vmhgfs   Fri Jul 26 05:02:51 2019 (5D3A7B6B)
fffff803`152f0000 fffff803`15302000   condrv   2E6C186F (This is a reproducible build file hash, not a timestamp)
fffff803`15310000 fffff803`15337000   AgileVpn 58BD83C1 (This is a reproducible build file hash, not a timestamp)
fffff803`15340000 fffff803`15361000   rasl2tp  10E99A75 (This is a reproducible build file hash, not a timestamp)
fffff803`15370000 fffff803`15391000   raspptp  DBF07670 (This is a reproducible build file hash, not a timestamp)
fffff803`153a0000 fffff803`153bc000   raspppoe 22793BEF (This is a reproducible build file hash, not a timestamp)
fffff803`153c0000 fffff803`153cf000   ndistapi E2027389 (This is a reproducible build file hash, not a timestamp)
fffff803`153d0000 fffff803`1540b000   ndiswan  67EDCBD1 (This is a reproducible build file hash, not a timestamp)
fffff803`15410000 fffff803`1542a000   WdNisDrv 5FD0376A (This is a reproducible build file hash, not a timestamp)
fffff803`15430000 fffff803`15438000   myfault  Wed Jun 12 19:36:53 2019 (5D014645)
fffff803`15450000 fffff803`1545e000   dump_diskdump  95F39C8A (This is a reproducible build file hash, not a timestamp)
fffff803`15480000 fffff803`1549f000   dump_lsi_sas  Wed Mar 25 19:36:48 2015 (55130E50)
fffff803`154c0000 fffff803`154dd000   dump_dumpfve  0DC8CA44 (This is a reproducible build file hash, not a timestamp)
fffff803`15ca0000 fffff803`15d34000   mrxsmb   CB6AAED6 (This is a reproducible build file hash, not a timestamp)
fffff803`15d40000 fffff803`15d86000   mrxsmb20 97B69CF8 (This is a reproducible build file hash, not a timestamp)
fffff803`15d90000 fffff803`15d9a000   vmmemctl  Sat Oct 19 10:37:52 2019 (5DAAD970)
fffff803`15da0000 fffff803`15df3000   srvnet   0FB644CD (This is a reproducible build file hash, not a timestamp)
fffff803`18200000 fffff803`19246000   nt       7A04BFB2 (This is a reproducible build file hash, not a timestamp)
fffff803`1a400000 fffff803`1a514000   clipsp   Thu Aug 26 05:05:48 2021 (6127131C)
fffff803`1a520000 fffff803`1a549000   ksecdd   5F6E7114 (This is a reproducible build file hash, not a timestamp)
fffff803`1a550000 fffff803`1a5b3000   msrpc    CACA2825 (This is a reproducible build file hash, not a timestamp)
fffff803`1a5c0000 fffff803`1a5d1000   werkernel  1BD4610F (This is a reproducible build file hash, not a timestamp)
fffff803`1a5e0000 fffff803`1a5ec000   ntosext  71DD3C9F (This is a reproducible build file hash, not a timestamp)
fffff803`1a5f0000 fffff803`1a6d3000   CI       104F974B (This is a reproducible build file hash, not a timestamp)
fffff803`1a6e0000 fffff803`1a79b000   cng      2546750A (This is a reproducible build file hash, not a timestamp)
fffff803`1a7a0000 fffff803`1a871000   Wdf01000 0CA8C8E4 (This is a reproducible build file hash, not a timestamp)
fffff803`1a880000 fffff803`1a893000   WDFLDR   565B60B2 (This is a reproducible build file hash, not a timestamp)
fffff803`1a8a0000 fffff803`1a8af000   SleepStudyHelper  664F6ECB (This is a reproducible build file hash, not a timestamp)
fffff803`1a8b0000 fffff803`1a8c1000   WppRecorder  15060D00 (This is a reproducible build file hash, not a timestamp)
fffff803`1a8d0000 fffff803`1a8f6000   acpiex   C8D60B44 (This is a reproducible build file hash, not a timestamp)
fffff803`1a900000 fffff803`1a91a000   SgrmAgent  A6474774 (This is a reproducible build file hash, not a timestamp)
fffff803`1a920000 fffff803`1a9ec000   ACPI     98F9EEE3 (This is a reproducible build file hash, not a timestamp)
fffff803`1a9f0000 fffff803`1a9fc000   WMILIB   CD518505 (This is a reproducible build file hash, not a timestamp)
fffff803`1aa20000 fffff803`1aa8b000   intelpep 4F6AD80A (This is a reproducible build file hash, not a timestamp)
fffff803`1aa90000 fffff803`1aaa7000   WindowsTrustedRT  7AF9978A (This is a reproducible build file hash, not a timestamp)
fffff803`1aab0000 fffff803`1aabb000   IntelTA  9D7941CE (This is a reproducible build file hash, not a timestamp)
fffff803`1aac0000 fffff803`1aacb000   WindowsTrustedRTProxy  AA5F5790 (This is a reproducible build file hash, not a timestamp)
fffff803`1aad0000 fffff803`1aae4000   pcw      D212A83E (This is a reproducible build file hash, not a timestamp)
fffff803`1aaf0000 fffff803`1aafb000   msisadrv 1AAAEF93 (This is a reproducible build file hash, not a timestamp)
fffff803`1ab00000 fffff803`1ab77000   pci      233F1106 (This is a reproducible build file hash, not a timestamp)
fffff803`1ab80000 fffff803`1ab95000   vdrvroot E613EBA7 (This is a reproducible build file hash, not a timestamp)
fffff803`1aba0000 fffff803`1abe4000   ucx01000 11447CC9 (This is a reproducible build file hash, not a timestamp)
fffff803`1abf0000 fffff803`1ac1f000   pdc      5A01FAEC (This is a reproducible build file hash, not a timestamp)
fffff803`1ac20000 fffff803`1ac3a000   CEA      00042D11 (This is a reproducible build file hash, not a timestamp)
fffff803`1ac40000 fffff803`1ac71000   partmgr  46C9AA09 (This is a reproducible build file hash, not a timestamp)
fffff803`1ac80000 fffff803`1ad2a000   spaceport  6510AA3A (This is a reproducible build file hash, not a timestamp)
fffff803`1ad30000 fffff803`1ad3b000   intelide 360A0288 (This is a reproducible build file hash, not a timestamp)
fffff803`1ad40000 fffff803`1ad53000   PCIIDEX  FAE17D6F (This is a reproducible build file hash, not a timestamp)
fffff803`1ad60000 fffff803`1ad79000   volmgr   51E4251D (This is a reproducible build file hash, not a timestamp)
```

```
fffff803`1ad80000 fffff803`1adcf000   sdbus     7950EC83 (This is a reproducible build file hash, not a timestamp)
fffff803`1add0000 fffff803`1ae33000   volmgrx   Fri Nov 29 18:04:07 2013 (5298D717)
fffff803`1ae40000 fffff803`1ae58000   vsock     Tue Jul 16 06:04:39 2019 (5D2D5AE7)
fffff803`1ae60000 fffff803`1ae7c000   vmci      Tue Jul 16 06:03:34 2019 (5D2D5AA6)
fffff803`1ae80000 fffff803`1ae98000   urscx01000  9B8E4DD0 (This is a reproducible build file hash, not a timestamp)
fffff803`1aea0000 fffff803`1aebe000   mountmgr  6FA7424A (This is a reproducible build file hash, not a timestamp)
fffff803`1aec0000 fffff803`1aedf000   lsi_sas   Wed Mar 25 19:36:48 2015 (55130E50)
fffff803`1aee0000 fffff803`1af93000   storport  4F71E812 (This is a reproducible build file hash, not a timestamp)
fffff803`1afa0000 fffff803`1afad000   atapi     424B07CC (This is a reproducible build file hash, not a timestamp)
fffff803`1afb0000 fffff803`1afec000   ataport   E634C2E3 (This is a reproducible build file hash, not a timestamp)
fffff803`1aff0000 fffff803`1b022000   storahci  6A1B92AB (This is a reproducible build file hash, not a timestamp)
fffff803`1b030000 fffff803`1b04c000   EhStorClass  DA9273CC (This is a reproducible build file hash, not a timestamp)
fffff803`1b050000 fffff803`1b06a000   fileinfo  AEE275C2 (This is a reproducible build file hash, not a timestamp)
fffff803`1b070000 fffff803`1b0b0000   Wof       66C89E3D (This is a reproducible build file hash, not a timestamp)
fffff803`1b0c0000 fffff803`1b12c000   WdFilter  EC5BA60F (This is a reproducible build file hash, not a timestamp)
fffff803`1b130000 fffff803`1b409000   Ntfs      D55BBFB4 (This is a reproducible build file hash, not a timestamp)
fffff803`1b410000 fffff803`1b443000   usbccgp   6ADA60BC (This is a reproducible build file hash, not a timestamp)
fffff803`1b450000 fffff803`1b45e000   USBD      76AC3507 (This is a reproducible build file hash, not a timestamp)
fffff803`1b460000 fffff803`1b46d000   urschipidea  DF2A818E (This is a reproducible build file hash, not a timestamp)
fffff803`1b470000 fffff803`1b48a000   usbehci   10F7905D (This is a reproducible build file hash, not a timestamp)
fffff803`1b490000 fffff803`1b509000   USBPORT   708EDB60 (This is a reproducible build file hash, not a timestamp)
fffff803`1b510000 fffff803`1b595000   usbhub    58FDCC74 (This is a reproducible build file hash, not a timestamp)
fffff803`1b5a0000 fffff803`1b643000   UsbHub3   8D1085E2 (This is a reproducible build file hash, not a timestamp)
fffff803`1b650000 fffff803`1b65d000   Fs_Rec    B9E5C55C (This is a reproducible build file hash, not a timestamp)
fffff803`1b660000 fffff803`1b7d0000   ndis      F389339C (This is a reproducible build file hash, not a timestamp)
fffff803`1b7e0000 fffff803`1b878000   NETIO     CF7CAF79 (This is a reproducible build file hash, not a timestamp)
fffff803`1b880000 fffff803`1b8b2000   ksecpkg   2E049C7F (This is a reproducible build file hash, not a timestamp)
fffff803`1b8c0000 fffff803`1bbac000   tcpip     9200AFD7 (This is a reproducible build file hash, not a timestamp)
fffff803`1bbb0000 fffff803`1bc2f000   fwpkclnt  951BC5AB (This is a reproducible build file hash, not a timestamp)
fffff803`1bc30000 fffff803`1bc60000   wfplwfs   3340819A (This is a reproducible build file hash, not a timestamp)
fffff803`1bc70000 fffff803`1bd38000   fvevol    FA0DD3CA (This is a reproducible build file hash, not a timestamp)
fffff803`1bd40000 fffff803`1bd4b000   volume    83CF10C9 (This is a reproducible build file hash, not a timestamp)
fffff803`1bd50000 fffff803`1bdbd000   volsnap   8AFD80F6 (This is a reproducible build file hash, not a timestamp)
fffff803`1bdc0000 fffff803`1be5a000   USBXHCI   8F70849A (This is a reproducible build file hash, not a timestamp)
fffff803`1be60000 fffff803`1be85000   USBSTOR   0AC69120 (This is a reproducible build file hash, not a timestamp)
fffff803`1be90000 fffff803`1bea8000   uaspstor  A9EA6129 (This is a reproducible build file hash, not a timestamp)
fffff803`1beb0000 fffff803`1bece000   sdstor    6057F024 (This is a reproducible build file hash, not a timestamp)
fffff803`1bed0000 fffff803`1bf20000   rdyboost  76CA3270 (This is a reproducible build file hash, not a timestamp)
fffff803`1bf30000 fffff803`1bf56000   mup       71933DBD (This is a reproducible build file hash, not a timestamp)
fffff803`1bf60000 fffff803`1bf72000   iorate    E3086CCD (This is a reproducible build file hash, not a timestamp)
fffff803`1bfa0000 fffff803`1bfbc000   disk      3457FE4D (This is a reproducible build file hash, not a timestamp)
fffff803`1bfc0000 fffff803`1c02d000   CLASSPNP  D469298F (This is a reproducible build file hash, not a timestamp)
fffff803`1c620000 fffff803`1c65f000   HIDCLASS  021FDD4D (This is a reproducible build file hash, not a timestamp)
fffff803`1c660000 fffff803`1c673000   HIDPARSE  3404D246 (This is a reproducible build file hash, not a timestamp)
fffff803`1c6a0000 fffff803`1c6b0000   mouhid    E502FBD9 (This is a reproducible build file hash, not a timestamp)
fffff803`1c6c0000 fffff803`1c6c9000   vmusbmouse  Tue Jul 16 07:56:07 2019 (5D2D7507)
fffff803`1c6d0000 fffff803`1c702000   cdrom     B69B2563 (This is a reproducible build file hash, not a timestamp)
fffff803`1c710000 fffff803`1c723000   mouclass  3E1AA9CC (This is a reproducible build file hash, not a timestamp)
fffff803`1c730000 fffff803`1c745000   filecrypt  3C7F622A (This is a reproducible build file hash, not a timestamp)
fffff803`1c750000 fffff803`1c75e000   tbs       CDEA9CC8 (This is a reproducible build file hash, not a timestamp)
fffff803`1c760000 fffff803`1c776000   BasicDisplay  A816CE22 (This is a reproducible build file hash, not a timestamp)
fffff803`1c780000 fffff803`1c798000   watchdog  F13839AB (This is a reproducible build file hash, not a timestamp)
fffff803`1c7a0000 fffff803`1c7aa000   Null      01FE6381 (This is a reproducible build file hash, not a timestamp)
fffff803`1c7b0000 fffff803`1cb5a000   dxgkrnl   5B01032B (This is a reproducible build file hash, not a timestamp)
fffff803`1cb60000 fffff803`1cb6a000   Beep      E4AC8238 (This is a reproducible build file hash, not a timestamp)
fffff803`1cb70000 fffff803`1cb80000   vmrawdsk  Tue Jul 16 08:03:33 2019 (5D2D76C5)
fffff803`1cb90000 fffff803`1cc32000   Vid       20AD7F88 (This is a reproducible build file hash, not a timestamp)
fffff803`1cc40000 fffff803`1cc61000   winhvr    C1F13DBD (This is a reproducible build file hash, not a timestamp)
fffff803`1cc70000 fffff803`1cc81000   BasicRender  4A52C9B4 (This is a reproducible build file hash, not a timestamp)
fffff803`1cc90000 fffff803`1cca2000   CompositeBus  6AE1B302 (This is a reproducible build file hash, not a timestamp)
fffff803`1ccb0000 fffff803`1ccbd000   kdnic     9401D3B8 (This is a reproducible build file hash, not a timestamp)
fffff803`1ccc0000 fffff803`1ccd5000   umbus     E7B4847E (This is a reproducible build file hash, not a timestamp)
fffff803`1cce0000 fffff803`1cd01000   i8042prt  515D28B1 (This is a reproducible build file hash, not a timestamp)
fffff803`1cd10000 fffff803`1cd24000   kbdclass  3156654A (This is a reproducible build file hash, not a timestamp)
fffff803`1cd30000 fffff803`1cd39000   vmmouse   Tue Jul 16 07:56:27 2019 (5D2D751B)
fffff803`1cd40000 fffff803`1cd5c000   serial    58F73A85 (This is a reproducible build file hash, not a timestamp)
fffff803`1cd60000 fffff803`1cd6f000   serenum   A5178D42 (This is a reproducible build file hash, not a timestamp)
fffff803`1cd70000 fffff803`1cd7a000   vm3dmp_loader  Fri Oct 25 11:28:23 2019 (5DB2CE47)
fffff803`1cd80000 fffff803`1cdcb000   vm3dmp    Fri Oct 25 11:28:24 2019 (5DB2CE48)
fffff803`1cdd0000 fffff803`1cde0000   usbuhci   1D25AB52 (This is a reproducible build file hash, not a timestamp)
fffff803`1cdf0000 fffff803`1ce19000   HDAudBus  8472BE9E (This is a reproducible build file hash, not a timestamp)
fffff803`1ce20000 fffff803`1ce86000   portcls   5373C5A4 (This is a reproducible build file hash, not a timestamp)
fffff803`1ce90000 fffff803`1ceb1000   drmk      38043810 (This is a reproducible build file hash, not a timestamp)
fffff803`1cec0000 fffff803`1cf36000   ks        365F95B9 (This is a reproducible build file hash, not a timestamp)
fffff803`1cf40000 fffff803`1cfce000   e1i65x64  Mon Jun 11 19:01:06 2018 (5B1EB8E2)
fffff803`1cfd0000 fffff803`1cfdb000   vmgencounter  ECEBB696 (This is a reproducible build file hash, not a timestamp)
fffff803`1cfe0000 fffff803`1cfef000   CmBatt    770987AD (This is a reproducible build file hash, not a timestamp)
fffff803`1cff0000 fffff803`1d000000   BATTC     FF322591 (This is a reproducible build file hash, not a timestamp)
fffff803`1d010000 fffff803`1d050000   intelppm  7EBD22FD (This is a reproducible build file hash, not a timestamp)
fffff803`1d060000 fffff803`1d06d000   NdisVirtualBus  A7AE93D1 (This is a reproducible build file hash, not a timestamp)
fffff803`1d070000 fffff803`1d080000   mssmbios  6233611A (This is a reproducible build file hash, not a timestamp)
fffff803`1d090000 fffff803`1d09c000   swenum    E117266B (This is a reproducible build file hash, not a timestamp)
fffff803`1d0a0000 fffff803`1d0ae000   rdpbus    84DFD52A (This is a reproducible build file hash, not a timestamp)
fffff803`1d0b0000 fffff803`1d11f000   HdAudio   6321FCBF (This is a reproducible build file hash, not a timestamp)
fffff803`1d120000 fffff803`1d12f000   ksthunk   2816E646 (This is a reproducible build file hash, not a timestamp)
fffff803`1d150000 fffff803`1d16e000   crashdmp  9A19AF81 (This is a reproducible build file hash, not a timestamp)
```

```
fffff803`1d1d0000 fffff803`1d1e2000   hidusb    1B0E634F (This is a reproducible build file hash, not a timestamp)
fffff803`1d200000 fffff803`1d222000   tdx       5FEFAB86 (This is a reproducible build file hash, not a timestamp)
fffff803`1d230000 fffff803`1d240000   TDI       D1AD2BD4 (This is a reproducible build file hash, not a timestamp)
fffff803`1d250000 fffff803`1d2ac000   netbt     45CF76EF (This is a reproducible build file hash, not a timestamp)
fffff803`1d2b0000 fffff803`1d2c3000   afunix    1FE42D67 (This is a reproducible build file hash, not a timestamp)
fffff803`1d2d0000 fffff803`1d376000   afd       93D14ADE (This is a reproducible build file hash, not a timestamp)
fffff803`1d380000 fffff803`1d39a000   vwififlt  03489583 (This is a reproducible build file hash, not a timestamp)
fffff803`1d3a0000 fffff803`1d3cb000   pacer     26BE44D4 (This is a reproducible build file hash, not a timestamp)
fffff803`1d3d0000 fffff803`1d3e4000   ndiscap   DCEEC70E (This is a reproducible build file hash, not a timestamp)
fffff803`1d3f0000 fffff803`1d404000   netbios   618ED82E (This is a reproducible build file hash, not a timestamp)
fffff803`1d410000 fffff803`1d48b000   rdbss     F124E9A6 (This is a reproducible build file hash, not a timestamp)
fffff803`1d490000 fffff803`1d4a2000   nsiproxy  F6E31779 (This is a reproducible build file hash, not a timestamp)
fffff803`1d4b0000 fffff803`1d4be000   npsvctrig  677B42C8 (This is a reproducible build file hash, not a timestamp)
fffff803`1d4c0000 fffff803`1d4ca000   gpuenergydrv  F10C03D8 (This is a reproducible build file hash, not a timestamp)
fffff803`1d4d0000 fffff803`1d4fc000   dfsc      5EDE3E45 (This is a reproducible build file hash, not a timestamp)
fffff803`1d520000 fffff803`1d58c000   fastfat   ED0854E5 (This is a reproducible build file hash, not a timestamp)
fffff803`1d590000 fffff803`1d5a7000   bam       4BADB6B8 (This is a reproducible build file hash, not a timestamp)
fffff803`1d5b0000 fffff803`1d5fe000   ahcache   20345F4C (This is a reproducible build file hash, not a timestamp)
fffff803`1d600000 fffff803`1d621000   BTHUSB    0305F304 (This is a reproducible build file hash, not a timestamp)
fffff803`1d630000 fffff803`1d7b5000   BTHport   31CE81D7 (This is a reproducible build file hash, not a timestamp)
fffff803`1d7c0000 fffff803`1d7fd000   rfcomm    F3616FE9 (This is a reproducible build file hash, not a timestamp)
fffff803`1d800000 fffff803`1d822000   BthEnum   3F5A14AF (This is a reproducible build file hash, not a timestamp)
fffff803`1d830000 fffff803`1d856000   bthpan    DC7BFA34 (This is a reproducible build file hash, not a timestamp)
fffff803`1d900000 fffff803`1d973000   dxgmms1   2B700581 (This is a reproducible build file hash, not a timestamp)
fffff803`1d980000 fffff803`1d99b000   monitor   54752B1B (This is a reproducible build file hash, not a timestamp)
fffff803`1d9a0000 fffff803`1da81000   dxgmms2   AF897EC9 (This is a reproducible build file hash, not a timestamp)
fffff803`1da90000 fffff803`1dae4000   WUDFRd    8B909C0C (This is a reproducible build file hash, not a timestamp)
fffff803`1daf0000 fffff803`1db19000   luafv     86E5647D (This is a reproducible build file hash, not a timestamp)
fffff803`1db20000 fffff803`1db56000   wcifs     CF4B5050 (This is a reproducible build file hash, not a timestamp)
fffff803`1db60000 fffff803`1dbe2000   cldflt    F28FA84B (This is a reproducible build file hash, not a timestamp)
fffff803`1dbf0000 fffff803`1dc0a000   storqosflt  461A811E (This is a reproducible build file hash, not a timestamp)
fffff803`1dc10000 fffff803`1dc38000   bindflt   3B53A127 (This is a reproducible build file hash, not a timestamp)
fffff803`1dc40000 fffff803`1dc58000   lltdio    D4D91B57 (This is a reproducible build file hash, not a timestamp)
fffff803`1dc60000 fffff803`1dc78000   mslldp    71FCC6F4 (This is a reproducible build file hash, not a timestamp)
fffff803`1dc80000 fffff803`1dc9b000   rspndr    9E43BCCD (This is a reproducible build file hash, not a timestamp)
fffff803`1dca0000 fffff803`1dcbd000   wanarp    2A517681 (This is a reproducible build file hash, not a timestamp)
fffff803`1dcc0000 fffff803`1dd16000   msquic    DE688303 (This is a reproducible build file hash, not a timestamp)
fffff803`1dd20000 fffff803`1dea8000   HTTP      8D578BD8 (This is a reproducible build file hash, not a timestamp)
fffff803`1deb0000 fffff803`1ded5000   bowser    D8EF76F6 (This is a reproducible build file hash, not a timestamp)
fffff803`1dee0000 fffff803`1defa000   mpsdrv    0EBF3D28 (This is a reproducible build file hash, not a timestamp)
fffff803`1df90000 fffff803`1dfac000   Npfs      9E3E4C73 (This is a reproducible build file hash, not a timestamp)
fffff803`1dfb0000 fffff803`1dfc1000   Msfs      95155DF1 (This is a reproducible build file hash, not a timestamp)
fffff803`1dfd0000 fffff803`1dfee000   CimFS     A2B46170 (This is a reproducible build file hash, not a timestamp)
fffffcbd`42a00000 fffffcbd`42cd3000   win32kbase  28C61D16 (This is a reproducible build file hash, not a timestamp)
fffffcbd`42ce0000 fffffcbd`43096000   win32kfull  E78A5DA6 (This is a reproducible build file hash, not a timestamp)
fffffcbd`430a0000 fffffcbd`430e9000   cdd       4FB5AE34 (This is a reproducible build file hash, not a timestamp)
fffffcbd`432d0000 fffffcbd`4336a000   win32k    3DBFF176 (This is a reproducible build file hash, not a timestamp)

Unloaded modules:
fffff803`1d870000 fffff803`1d87f000   dump_storport.sys
    Timestamp: unavailable (00000000)
    Checksum:  00000000
    ImageSize:  0000F000
fffff803`1d8a0000 fffff803`1d8c0000   dump_lsi_sas.sys
    Timestamp: unavailable (00000000)
    Checksum:  00000000
    ImageSize:  00020000
fffff803`1d8e0000 fffff803`1d8fe000   dump_dumpfve.sys
    Timestamp: unavailable (00000000)
    Checksum:  00000000
    ImageSize:  0001E000
fffff803`1d180000 fffff803`1d18f000   dump_storport.sys
    Timestamp: unavailable (00000000)
    Checksum:  00000000
    ImageSize:  0000F000
fffff803`1d1b0000 fffff803`1d1d0000   dump_lsi_sas.sys
    Timestamp: unavailable (00000000)
    Checksum:  00000000
    ImageSize:  00020000
fffff803`1c680000 fffff803`1c69e000   dump_dumpfve.sys
    Timestamp: unavailable (00000000)
    Checksum:  00000000
    ImageSize:  0001E000
fffff803`1d500000 fffff803`1d51c000   dam.sys
    Timestamp: unavailable (00000000)
    Checksum:  00000000
    ImageSize:  0001C000
fffff803`1de00000 fffff803`1de55000   WUDFRd.sys
    Timestamp: unavailable (00000000)
    Checksum:  00000000
    ImageSize:  00055000
fffff803`1aa00000 fffff803`1aa11000   WdBoot.sys
    Timestamp: unavailable (00000000)
    Checksum:  00000000
    ImageSize:  00011000
fffff803`1bf80000 fffff803`1bf91000   hwpolicy.sys
```

```
    Timestamp: unavailable (00000000)
    Checksum:  00000000
    ImageSize:  00011000
```

Note: Because this is a kernel memory dump, only kernel space modules (drivers) are shown (we see their load addresses have higher than the FFFF8000`00000000 address). To see loaded process modules, we need a complete memory dump. Also, modules that do not have this output “**This is a reproducible build file hash, not a timestamp**“ are most likely not from the original Windows distribution. **Unloaded modules** may give hints at past system behavior.

11. Use **lmv m** *<module>* or **!lmi** command to check module information:

```
0: kd> lmv m win32k
Browse full module list
start             end                 module name
fffffcbd`432d0000 fffffcbd`4336a000   win32k     (deferred)
    Image path: \SystemRoot\System32\win32k.sys
    Image name: win32k.sys
    Browse all global symbols  functions  data
    Image was built with /Brepro flag.
    Timestamp:        3DBFF176 (This is a reproducible build file hash, not a timestamp)
    CheckSum:         0009E5BE
    ImageSize:        0009A000
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
    Translations:     0000.04b0 0000.04e4 0409.04b0 0409.04e4
    Information from resource tables:
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details
Page 11cfc7 not present in the dump file. Type ".hh dbgerr004" for details

0: kd> !lmi win32k
Loaded Module Info: [win32k]
         Module: win32k
   Base Address: fffffcbd432d0000
     Image Name: win32k.sys
   Machine Type: 34404 (X64)
     Time Stamp: 3dbff176 (This is a reproducible build file hash, not a true timestamp)
           Size: 9a000
       CheckSum: 9e5be
Characteristics: 22
Debug Data Dirs: Type  Size     VA  Pointer
             CODEVIEW    23, 53900,   52d00 RSDS - GUID: {AD6D3E11-D496-C883-7D01-42839435EE07}
               Age: 1, Pdb: win32k.pdb
                 POGO   1c0, 53924,   52d24 [Data not mapped]
                REPRO    24, 53ae4,   52ee4 Reproducible build[Data not mapped]
    Symbol Type: DEFERRED - No error - symbol load deferred
    Load Report: no symbols loaded
```

Note: “Page not present in the dump file” messages mean that WinDbg tried to access a page to get additional information, but the page was not included in the kernel dump and may have been paged out. If you don’t see any vendor information in the output, you can use **s-sa** and **s-su** commands to view driver data strings, and if nothing is found, you can search the Internet for driver vendors:

```
0: kd> lmv m e1i65x64
Browse full module list
start             end                 module name
fffff803`1cf40000 fffff803`1cfce000   e1i65x64   (deferred)
    Image path: \SystemRoot\System32\drivers\e1i65x64.sys
    Image name: e1i65x64.sys
    Browse all global symbols  functions  data
    Timestamp:        Mon Jun 11 19:01:06 2018 (5B1EB8E2)
    CheckSum:         0008A03D
    ImageSize:        0008E000
    Translations:     0000.04b0 0000.04e4 0409.04b0 0409.04e4
    Information from resource tables:


0: kd> s-su fffff803`1cf40000 fffff803`1cfce000
[...]
fffff803`1cfae67a  "쳭쳭쳭INTELPRO_"
[...]
```

Note: We could not find a good description in the output, but the Internet search indicated that the module is "Intel(R) Gigabit Adapter NDIS 6.x driver for Windows".

12. Now we check if the system was running under VMware. Most such virtualization systems load additional drivers we search for their typical names, for example, vmmemctl or using wildcards (*vm**) :

```
0: kd> lmv m vmmemctl
Browse full module list
start             end                 module name
fffff803`15d90000 fffff803`15d9a000   vmmemctl   (deferred)
    Image path: \SystemRoot\system32\DRIVERS\vmmemctl.sys
    Image name: vmmemctl.sys
    Browse all global symbols  functions  data
    Timestamp:        Sat Oct 19 10:37:52 2019 (5DAAD970)
    CheckSum:         00018ACF
    ImageSize:        0000A000
    Translations:     0000.04b0 0000.04e4 0409.04b0 0409.04e4
    Information from resource tables:
```

13. The **version** command can show you the dump type, system version, uptime, and when the dump was generated:

```
0: kd> version
Windows 10 Kernel Version 19041 MP (2 procs) Free x64
Product: WinNt, suite: TerminalServer SingleUserTS Personal
Edition build lab: 19041.1.amd64fre.vb_release.191206-1406
Machine Name:
Kernel base = 0xfffff803`18200000 PsLoadedModuleList = 0xfffff803`18e2a230
Debug session time: Sun Sep 26 13:27:34.008 2021 (UTC + 1:00)
System Uptime: 0 days 0:25:13.988
64-bit Kernel bitmap dump: C:\AWMDA-Dumps\Kernel\x64\MEMORY-PageFault.DMP

Microsoft (R) Windows Debugger Version 10.0.25111.1000 AMD64
Copyright (c) Microsoft Corporation. All rights reserved.

command line: '"C:\Program Files\WindowsApps\Microsoft.WinDbg_1.2205.18001.0_x64__8wekyb3d8bbwe\amd64\EngHost.exe"
npipe:pipe=DbgX_f3dcc4c16f1342d791c6d418138a9c15,password=6ae7cdd5be1e "C:\Program
Files\WindowsApps\Microsoft.WinDbg_1.2205.18001.0_x64__8wekyb3d8bbwe\amd64" "C:\ProgramData\Dbg"'  Debugger Process
0x6CD0
dbgeng:  image 10.0.25111.1000,
        [path: C:\Program Files\WindowsApps\Microsoft.WinDbg_1.2205.18001.0_x64__8wekyb3d8bbwe\amd64\dbgeng.dll]
dbghelp: image 10.0.25111.1000,
        [path: C:\Program Files\WindowsApps\Microsoft.WinDbg_1.2205.18001.0_x64__8wekyb3d8bbwe\amd64\dbghelp.dll]
        DIA version: 30795
Extension DLL search Path:
[...]
Extension DLL chain:
    wdfkd: image 10.0.25111.1000, API 1.0.0,
        [path: C:\Program Files\WindowsApps\Microsoft.WinDbg_1.2205.18001.0_x64__8wekyb3d8bbwe\amd64\winext\wdfkd.dll]
    MachOBinComposition: image 10.0.25111.1000, API 0.0.0,
        [path: C:\Program
Files\WindowsApps\Microsoft.WinDbg_1.2205.18001.0_x64__8wekyb3d8bbwe\amd64\winext\MachOBinComposition.dll]
    ELFBinComposition: image 10.0.25111.1000, API 0.0.0,
        [path: C:\Program
Files\WindowsApps\Microsoft.WinDbg_1.2205.18001.0_x64__8wekyb3d8bbwe\amd64\winext\ELFBinComposition.dll]
    dbghelp: image 10.0.25111.1000, API 10.0.6,
        [path: C:\Program Files\WindowsApps\Microsoft.WinDbg_1.2205.18001.0_x64__8wekyb3d8bbwe\amd64\dbghelp.dll]
    exts: image 10.0.25111.1000, API 1.0.0,
        [path: C:\Program Files\WindowsApps\Microsoft.WinDbg_1.2205.18001.0_x64__8wekyb3d8bbwe\amd64\WINXP\exts.dll]
    kext: image 10.0.25111.1000, API 1.0.0,
        [path: C:\Program Files\WindowsApps\Microsoft.WinDbg_1.2205.18001.0_x64__8wekyb3d8bbwe\amd64\winext\kext.dll]
    kdexts: image 10.0.25111.1000, API 1.0.0,
        [path: C:\Program Files\WindowsApps\Microsoft.WinDbg_1.2205.18001.0_x64__8wekyb3d8bbwe\amd64\winxp\kdexts.dll]
```

14. We check now virtual memory statistics using **!vm** command (it also shows the processes):

```
0: kd> !vm
Page File: \??\C:\pagefile.sys
  Current:   4456448 Kb  Free Space:    4447416 Kb
  Minimum:   4456448 Kb  Maximum:       7785468 Kb
Page File: \??\C:\swapfile.sys
  Current:     16384 Kb  Free Space:      16376 Kb
  Minimum:     16384 Kb  Maximum:       6228376 Kb
No Name for Paging File
  Current:  11978728 Kb  Free Space:  11484620 Kb
  Minimum:  11978728 Kb  Maximum:     11978728 Kb

Physical Memory:          1048315 (    4193260 Kb)
Available Pages:           424719 (    1698876 Kb)
ResAvail Pages:            886911 (    3547644 Kb)
Locked IO Pages:                0 (          0 Kb)
Free System PTEs:      4294991671 (17179966684 Kb)

******* 201600 kernel stack PTE allocations have failed ******


******* 417654976 kernel stack growth attempts have failed ******

Modified Pages:              8530 (      34120 Kb)
Modified PF Pages:           8184 (      32736 Kb)
Modified No Write Pages:        0 (          0 Kb)
NonPagedPool Usage:           229 (        916 Kb)
NonPagedPoolNx Usage:       21033 (      84132 Kb)
NonPagedPool Max:      4294967296 (17179869184 Kb)
PagedPool Usage:            34452 (     137808 Kb)
PagedPool Maximum:     4294967296 (17179869184 Kb)
Processor Commit:             468 (       1872 Kb)
Session Commit:              4457 (      17828 Kb)
Shared Commit:              72552 (     290208 Kb)
Special Pool:                   0 (          0 Kb)
Kernel Stacks:              10230 (      40920 Kb)
Pages For MDLs:              1961 (       7844 Kb)
ContigMem Pages:                0 (          0 Kb)
Pages For AWE:                  0 (          0 Kb)
NonPagedPool Commit:        22027 (      88108 Kb)
PagedPool Commit:           34452 (     137808 Kb)
Driver Commit:              12741 (      50964 Kb)
Boot Commit:                 4731 (      18924 Kb)
PFN Array Commit:           12833 (      51332 Kb)
SmallNonPagedPtesCommit:      133 (        532 Kb)
SlabAllocatorPages:          4608 (      18432 Kb)
System PageTables:            823 (       3292 Kb)
ProcessLockedFilePages:        12 (         48 Kb)
Pagefile Hash Pages:            4 (         16 Kb)
Sum System Commit:         182032 (     728128 Kb)
Total Private:             465388 (    1861552 Kb)

********** Sum of individual system commit + Process commit exceeds overall commit by 7096 Kb ?
********
Committed pages:           645646 (    2582584 Kb)
Commit limit:             2162427 (    8649708 Kb)

  Pid ImageName                       Commit   SharedCommit        Debt
```

```
 21c dwm.exe                       260604 Kb      128516 Kb        0 Kb
 dc0 MsMpEng.exe                   229356 Kb        2360 Kb        0 Kb
22e0 SearchApp.exe                 173164 Kb       12328 Kb        0 Kb
176c SearchApp.exe                 137176 Kb       31660 Kb        0 Kb
14c4 msedge.exe                     73872 Kb        3884 Kb        0 Kb
237c msedge.exe                     68816 Kb       39948 Kb        0 Kb
 494 explorer.exe                   62004 Kb       51072 Kb        0 Kb
2288 msedge.exe                     44712 Kb        8236 Kb        0 Kb
1d30 msedge.exe                     42096 Kb       36008 Kb        0 Kb
136c svchost.exe                    37296 Kb        3244 Kb        0 Kb
16c4 StartMenuExperienceHost.       27316 Kb       18112 Kb        0 Kb
165c YourPhone.exe                  24452 Kb        2936 Kb        0 Kb
1aa0 msedge.exe                     23668 Kb        3052 Kb        0 Kb
2028 SystemSettings.exe             23636 Kb       38776 Kb        0 Kb
1518 SearchIndexer.exe              21552 Kb        2816 Kb        0 Kb
 df8 Calculator.exe                 20092 Kb       15216 Kb        0 Kb
 5dc svchost.exe                    17364 Kb        1952 Kb        0 Kb
 d14 svchost.exe                    16776 Kb        2276 Kb        0 Kb
1dbc vmtoolsd.exe                   15452 Kb        4072 Kb        0 Kb
17f8 RuntimeBroker.exe              13772 Kb        4044 Kb        0 Kb
19d4 LockApp.exe                    13652 Kb        4424 Kb        0 Kb
 d24 svchost.exe                    12864 Kb        1964 Kb        0 Kb
1978 explorer.exe                   12428 Kb       12084 Kb        0 Kb
1a00 ShellExperienceHost.exe        12232 Kb        7200 Kb        0 Kb
 e04 ApplicationFrameHost.exe       11788 Kb       10800 Kb        0 Kb
19ec msedge.exe                     11540 Kb        2732 Kb        0 Kb
 ab8 TextInputHost.exe              11352 Kb        3056 Kb        0 Kb
2380 msedge.exe                     11128 Kb        2852 Kb        0 Kb
1148 WmiPrvSE.exe                   10484 Kb        2224 Kb        0 Kb
 304 svchost.exe                    10368 Kb        2364 Kb        0 Kb
1a94 svchost.exe                    10080 Kb        1980 Kb        0 Kb
 b98 svchost.exe                     9984 Kb        1956 Kb        0 Kb
 aac svchost.exe                     9832 Kb        2744 Kb        0 Kb
1f20 OneDrive.exe                    9808 Kb        3884 Kb        0 Kb
1138 svchost.exe                     9608 Kb        2964 Kb        0 Kb
1510 svchost.exe                     9012 Kb        1992 Kb        0 Kb
1aac RuntimeBroker.exe               8944 Kb        3936 Kb        0 Kb
 d30 svchost.exe                     8920 Kb        1984 Kb        0 Kb
 9f8 svchost.exe                     7960 Kb        1980 Kb        0 Kb
 3ac svchost.exe                     7720 Kb         636 Kb        0 Kb
 2a0 lsass.exe                       7360 Kb        2312 Kb        0 Kb
 a40 sihost.exe                      7056 Kb        2732 Kb        0 Kb
1704 RuntimeBroker.exe               6756 Kb        2768 Kb        0 Kb
 ba0 taskhostw.exe                   6676 Kb        3880 Kb        0 Kb
1b80 RuntimeBroker.exe               6668 Kb        2964 Kb        0 Kb
1d98 msedge.exe                      6560 Kb        2436 Kb        0 Kb
 534 svchost.exe                     6236 Kb        2044 Kb        0 Kb
1efc svchost.exe                     5752 Kb        2864 Kb        0 Kb
 b30 spoolsv.exe                     5728 Kb        1988 Kb        0 Kb
 a64 svchost.exe                     5664 Kb        2736 Kb        0 Kb
  5c Registry                        5540 Kb           0 Kb        0 Kb
 db8 vmtoolsd.exe                    5504 Kb        2016 Kb        0 Kb
 d9c svchost.exe                     5380 Kb        2244 Kb        0 Kb
 598 dllhost.exe                     5176 Kb        2576 Kb        0 Kb
 290 services.exe                    5076 Kb         372 Kb        0 Kb
1b94 svchost.exe                     4884 Kb        2276 Kb        0 Kb
 dd4 svchost.exe                     4520 Kb        2264 Kb        0 Kb
1cd8 svchost.exe                     4492 Kb        1980 Kb        0 Kb
1d60 SecurityHealthService.ex        4468 Kb        2276 Kb        0 Kb
1514 svchost.exe                     4288 Kb        2252 Kb        0 Kb
```

```
 894 svchost.exe                     4268 Kb        1968 Kb        0 Kb
1f6c svchost.exe                     4264 Kb        1960 Kb        0 Kb
182c ctfmon.exe                      4232 Kb        3612 Kb        0 Kb
 710 svchost.exe                     4112 Kb        1952 Kb        0 Kb
1064 dllhost.exe                     3964 Kb        1976 Kb        0 Kb
 bd4 svchost.exe                     3848 Kb        2264 Kb        0 Kb
1428 svchost.exe                     3804 Kb        2736 Kb        0 Kb
1898 TabTip.exe                      3800 Kb        2480 Kb        0 Kb
1838 NisSrv.exe                      3776 Kb        1956 Kb        0 Kb
 834 SgrmBroker.exe                  3768 Kb         352 Kb        0 Kb
 634 svchost.exe                     3680 Kb        2280 Kb        0 Kb
 cf8 svchost.exe                     3656 Kb        2088 Kb        0 Kb
 f18 svchost.exe                     3408 Kb        1980 Kb        0 Kb
21a4 MoUsoCoreWorker.exe             3332 Kb        1984 Kb        0 Kb
 92c svchost.exe                     3320 Kb        1960 Kb        0 Kb
 580 svchost.exe                     3284 Kb        2280 Kb        0 Kb
  d8 svchost.exe                     3144 Kb        1976 Kb        0 Kb
 de4 VGAuthService.exe               3136 Kb        1992 Kb        0 Kb
 9cc svchost.exe                     3096 Kb        1952 Kb        0 Kb
 7e0 svchost.exe                     3092 Kb        1956 Kb        0 Kb
 93c svchost.exe                     2936 Kb        1956 Kb        0 Kb
1100 msdtc.exe                       2916 Kb        1960 Kb        0 Kb
16f8 RuntimeBroker.exe               2892 Kb        2748 Kb        0 Kb
1594 svchost.exe                     2804 Kb        1984 Kb        0 Kb
 184 svchost.exe                     2784 Kb        2268 Kb        0 Kb
1ec8 RuntimeBroker.exe               2748 Kb        2748 Kb        0 Kb
 7e8 svchost.exe                     2744 Kb        1984 Kb        0 Kb
1338 svchost.exe                     2732 Kb        1956 Kb        0 Kb
 3f8 notepad.exe                     2732 Kb       11220 Kb        0 Kb
1b34 RuntimeBroker.exe               2720 Kb        2748 Kb        0 Kb
 268 winlogon.exe                    2704 Kb        6944 Kb        0 Kb
 e48 svchost.exe                     2668 Kb        1980 Kb        0 Kb
 574 svchost.exe                     2648 Kb        2264 Kb        0 Kb
12fc svchost.exe                     2576 Kb        1988 Kb        0 Kb
 9d8 svchost.exe                     2516 Kb        1956 Kb        0 Kb
 d74 svchost.exe                     2424 Kb        1980 Kb        0 Kb
 3f0 svchost.exe                     2384 Kb        1980 Kb        0 Kb
 470 svchost.exe                     2368 Kb        1960 Kb        0 Kb
 aa4 svchost.exe                     2260 Kb        1980 Kb        0 Kb
 7d4 svchost.exe                     2252 Kb        1952 Kb        0 Kb
 36c WUDFHost.exe                    2228 Kb        1952 Kb        0 Kb
 4b0 svchost.exe                     2180 Kb        1984 Kb        0 Kb
 464 svchost.exe                     2180 Kb        1960 Kb        0 Kb
1444 svchost.exe                     2176 Kb        1980 Kb        0 Kb
1144 svchost.exe                     2112 Kb        1956 Kb        0 Kb
 1d4 UserOOBEBroker.exe              2112 Kb        2464 Kb        0 Kb
12d4 SettingSyncHost.exe             2088 Kb        3832 Kb        0 Kb
 688 svchost.exe                     2072 Kb        1960 Kb        0 Kb
1d4c msedge.exe                      2032 Kb        3544 Kb        0 Kb
1bf0 svchost.exe                     2028 Kb        1952 Kb        0 Kb
 dec notmyfault64.exe                2024 Kb        4176 Kb        0 Kb
 8dc svchost.exe                     1996 Kb        1956 Kb        0 Kb
 b58 svchost.exe                     1956 Kb        1956 Kb        0 Kb
 fa4 VSSVC.exe                       1944 Kb        1980 Kb        0 Kb
 604 svchost.exe                     1940 Kb        1980 Kb        0 Kb
1d3c SecurityHealthSystray.ex        1924 Kb        2452 Kb        0 Kb
1dec MpCopyAccelerator.exe           1916 Kb        1976 Kb        0 Kb
 218 csrss.exe                       1880 Kb        6212 Kb        0 Kb
 418 svchost.exe                     1876 Kb        1956 Kb        0 Kb
 864 svchost.exe                     1868 Kb        1984 Kb        0 Kb
```

```
  8bc svchost.exe                     1860 Kb         2016 Kb         0 Kb
  69c svchost.exe                     1828 Kb         1980 Kb         0 Kb
  1bc csrss.exe                       1812 Kb         8400 Kb         0 Kb
  ea8 svchost.exe                     1808 Kb         1976 Kb         0 Kb
  8b0 svchost.exe                     1796 Kb         1980 Kb         0 Kb
 1454 svchost.exe                     1788 Kb         1976 Kb         0 Kb
 159c svchost.exe                     1740 Kb         1980 Kb         0 Kb
  31c fontdrvhost.exe                 1732 Kb          360 Kb         0 Kb
 1e30 svchost.exe                     1696 Kb         1952 Kb         0 Kb
  420 svchost.exe                     1676 Kb         1956 Kb         0 Kb
  9c4 svchost.exe                     1660 Kb         1952 Kb         0 Kb
  d88 svchost.exe                     1604 Kb         1952 Kb         0 Kb
  5f0 svchost.exe                     1568 Kb         1980 Kb         0 Kb
  4b8 svchost.exe                     1528 Kb         1952 Kb         0 Kb
  188 svchost.exe                     1516 Kb         1976 Kb         0 Kb
  62c svchost.exe                     1484 Kb         1956 Kb         0 Kb
  208 wininit.exe                     1408 Kb         1932 Kb         0 Kb
 1f10 vm3dservice.exe                 1376 Kb         3532 Kb         0 Kb
  4a4 svchost.exe                     1344 Kb         1976 Kb         0 Kb
  410 svchost.exe                     1324 Kb         1952 Kb         0 Kb
  324 fontdrvhost.exe                 1316 Kb          360 Kb         0 Kb
  e78 svchost.exe                     1300 Kb         1960 Kb         0 Kb
  da4 svchost.exe                     1256 Kb         1976 Kb         0 Kb
  160 smss.exe                        1100 Kb          264 Kb         0 Kb
  854 MemCompression                   352 Kb            0 Kb         0 Kb
    4 System                           192 Kb          292 Kb         0 Kb
 1d00 msedge.exe                       100 Kb            0 Kb         0 Kb
 22b4 svchost.exe                       80 Kb            0 Kb         0 Kb
 1e74 TabTip.exe                        80 Kb            0 Kb         0 Kb
 1474 svchost.exe                       80 Kb            0 Kb         0 Kb
 13e8 userinit.exe                      80 Kb            0 Kb         0 Kb
  1c0 LogonUI.exe                       80 Kb            0 Kb         0 Kb
```

Note: We see some failures (in grey), but we need to be skeptical about whether they are real or false positives. In our case, these can be ignored. If you see a questionable output, it is good to compare it with the normal system output.

Note: When the page file size + 10Mb is less than the amount of physical memory, we most likely get a truncated complete memory dump with the most vital information missing necessary for WinDbg commands. However, for kernel memory dumps, the page file size is not that so stringent.

15. We can check how many processors we have and their running threads using the **!running** command. The simple form gives only the really running threads:

```
0: kd> !running

System Processors:  (0000000000000003)
  Idle Processors:  (0000000000000002)

       Prcbs             Current         (pri) Next            (pri) Idle
  0    fffff80313caf180  ffffdb0de16bd080 (12)                       fffff80318f26a00  ................
```

```
0: kd> !thread ffffdb0de16bd080 3f
THREAD ffffdb0de16bd080  Cid 0dec.1e28  Teb: 0000005be4329000 Win32Thread: ffffdb0dddc561a0 RUNNING on
processor 0
IRP List:
    ffffdb0de17fcea0: (0006,0118) Flags: 00060000  Mdl: 00000000
Not impersonating
DeviceMap                 ffffae0391bb2810
Owning Process            ffffdb0ddbb27080       Image:         notmyfault64.exe
Attached Process          N/A            Image:         N/A
Wait Start TickCount      96894          Ticks: 1 (0:00:00:00.015)
Context Switch Count      3157           IdealProcessor: 1
UserTime                  00:00:00.062
KernelTime                00:00:00.390
Win32 Start Address 0x00007ff6a93f5384
Stack Init fffff406ca7d4fd0 Current fffff406ca7d4010
Base fffff406ca7d5000 Limit fffff406ca7cf000 Call 0000000000000000
Priority 12 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
Child-SP          RetAddr               Call Site
fffff406`ca7d4698 fffff803`18609169     nt!KeBugCheckEx
fffff406`ca7d46a0 fffff803`18605469     nt!KiBugCheckDispatch+0x69
fffff406`ca7d47e0 fffff803`15431981     nt!KiPageFault+0x469 (TrapFrame @ fffff406`ca7d47e0)
fffff406`ca7d4970 fffff803`15431d3d     myfault+0x1981
fffff406`ca7d49a0 fffff803`15431ea1     myfault+0x1d3d
fffff406`ca7d4ae0 fffff803`1848f865     myfault+0x1ea1
fffff406`ca7d4b40 fffff803`18875328     nt!IofCallDriver+0x55
fffff406`ca7d4b80 fffff803`18874bf5     nt!IopSynchronousServiceTail+0x1a8
fffff406`ca7d4c20 fffff803`188745f6     nt!IopXxxControlFile+0x5e5
fffff406`ca7d4d60 fffff803`18608bb5     nt!NtDeviceIoControlFile+0x56
fffff406`ca7d4dd0 00007ffe`4bf2ce54     nt!KiSystemServiceCopyEnd+0x25 (TrapFrame @ fffff406`ca7d4e40)
0000005b`e44fedb8 00000000`00000000     0x00007ffe`4bf2ce54
```

Note: The **3f** flag for the **!thread** command reduces the output clutter by omitting stack frame arguments which are, most of the time, do not reflect actual function arguments (call parameters) due to x64 calling convention optimization (the first 4 parameters are passed by registers, not by stack locations).

Note: Another command variant also includes idle threads (there has to be a thread for every processor even if it does nothing; it also accumulates processor time and is not considered as a CPU spike):

```
0: kd> !running -i

System Processors:  (0000000000000003)
  Idle Processors:  (0000000000000002)

       Prcbs             Current         (pri) Next            (pri) Idle
  0    fffff80313caf180  ffffdb0de16bd080 (12)                       fffff80318f26a00  ................
  1    ffffcb0034fc3180  ffffcb0034fce0c0 ( 0)                       ffffcb0034fce0c0  ................

0: kd> !thread ffffcb0034fce0c0 3f
THREAD ffffcb0034fce0c0  Cid 0000.0000  Teb: 0000000000000000 Win32Thread: 0000000000000000
RUNNING on processor 1
Not impersonating
DeviceMap                 ffffae038da371e0
Owning Process            fffff80318f23a00       Image:         Idle
Attached Process          ffffdb0ddbaa1040       Image:         System
Wait Start TickCount      0              Ticks: 96895 (0:00:25:13.984)
Context Switch Count      252152         IdealProcessor: 1
UserTime                  00:00:00.000
KernelTime                00:16:44.000
Win32 Start Address nt!KiIdleLoop (0xfffff803185fac90)
Stack Init fffff406c9829c90 Current fffff406c9829c20
Base fffff406c982a000 Limit fffff406c9824000 Call 0000000000000000
Priority 0 BasePriority 0 PriorityDecrement 0 IoPriority 0 PagePriority 0
Child-SP          RetAddr               Call Site
```

```
fffff406`c98296b8 fffff803`185b9eb4     nt!HalProcessorIdle+0xf
fffff406`c98296c0 fffff803`184184b6     nt!PpmIdleDefaultExecute+0x14
fffff406`c98296f0 fffff803`18417274     nt!PpmIdleExecuteTransition+0x10c6
fffff406`c9829af0 fffff803`185face4     nt!PoIdle+0x374
fffff406`c9829c60 00000000`00000000     nt!KiIdleLoop+0x54
```

Note: Another flag **-t** includes stack traces in the output of **!running** command:

```
0: kd> !running -i -t

System Processors:  (0000000000000003)
  Idle Processors:  (0000000000000002)

       Prcbs             Current         (pri) Next            (pri) Idle
  0    fffff80313caf180  ffffdb0de16bd080 (12)                       fffff80318f26a00  ................

 # Child-SP          RetAddr               Call Site
00 fffff406`ca7d4698 fffff803`18609169     nt!KeBugCheckEx
01 fffff406`ca7d46a0 fffff803`18605469     nt!KiBugCheckDispatch+0x69
02 fffff406`ca7d47e0 fffff803`15431981     nt!KiPageFault+0x469
03 fffff406`ca7d4970 fffff803`15431d3d     myfault+0x1981
04 fffff406`ca7d49a0 fffff803`15431ea1     myfault+0x1d3d
05 fffff406`ca7d4ae0 fffff803`1848f865     myfault+0x1ea1
06 fffff406`ca7d4b40 fffff803`18875328     nt!IofCallDriver+0x55
07 fffff406`ca7d4b80 fffff803`18874bf5     nt!IopSynchronousServiceTail+0x1a8
08 fffff406`ca7d4c20 fffff803`188745f6     nt!IopXxxControlFile+0x5e5
09 fffff406`ca7d4d60 fffff803`18608bb5     nt!NtDeviceIoControlFile+0x56
0a fffff406`ca7d4dd0 00007ffe`4bf2ce54     nt!KiSystemServiceCopyEnd+0x25
0b 0000005b`e44fedb8 00000000`00000000     0x00007ffe`4bf2ce54

  1    ffffcb0034fc3180  ffffcb0034fce0c0 ( 0)                       ffffcb0034fce0c0  ................

 # Child-SP          RetAddr               Call Site
00 fffff406`c98296b8 fffff803`185b9eb4     nt!HalProcessorIdle+0xf
01 fffff406`c98296c0 fffff803`184184b6     nt!PpmIdleDefaultExecute+0x14
02 fffff406`c98296f0 fffff803`18417274     nt!PpmIdleExecuteTransition+0x10c6
03 fffff406`c9829af0 fffff803`185face4     nt!PoIdle+0x374
04 fffff406`c9829c60 00000000`00000000     nt!KiIdleLoop+0x54
```

16. We can use the **~***<processor >***s** command to switch to other processors and set their thread/process as current:

```
0: kd> ~1s

1: kd> k
 # Child-SP          RetAddr               Call Site
00 fffff406`c98296b8 fffff803`185b9eb4     nt!HalProcessorIdle+0xf
01 fffff406`c98296c0 fffff803`184184b6     nt!PpmIdleDefaultExecute+0x14
02 fffff406`c98296f0 fffff803`18417274     nt!PpmIdleExecuteTransition+0x10c6
03 fffff406`c9829af0 fffff803`185face4     nt!PoIdle+0x374
04 fffff406`c9829c60 00000000`00000000     nt!KiIdleLoop+0x54
```

Note: In the kernel and complete memory dumps, the **~**<number>**s** command is different from process memory dumps, where it is used to switch between threads. We see how to switch between threads in kernel dumps later.

17. We can check user sessions by using the **!session** command:

```
1: kd> !session
Sessions on machine: 2
Valid Sessions: 0 1
Error in reading current session
```

18. We can see what processes belong to any session by using the **!sprocess** *<number>* command:

```
1: kd> !sprocess 1
Dumping Session 1

_MM_SESSION_SPACE ffffcb00361f6000
_MMSESSION        ffffcb00361f60c0
PROCESS ffffdb0ddf7c9140
    SessionId: 1  Cid: 0218    Peb: eec7286000  ParentCid: 0200
    DirBase: 11cf0c002  ObjectTable: ffffae03915f5180  HandleCount: 454.
    Image: csrss.exe

PROCESS ffffdb0ddf876080
    SessionId: 1  Cid: 0268    Peb: 508399000  ParentCid: 0200
    DirBase: 117690002  ObjectTable: ffffae03915f67c0  HandleCount: 294.
    Image: winlogon.exe

PROCESS ffffdb0ddf911080
    SessionId: 1  Cid: 031c    Peb: 826a9a6000  ParentCid: 0268
    DirBase: 11059d002  ObjectTable: ffffae03917767c0  HandleCount:  32.
    Image: fontdrvhost.exe

PROCESS ffffdb0de009c100
    SessionId: 1  Cid: 01c0    Peb: c37a97f000  ParentCid: 0268
    DirBase: 114d58002  ObjectTable: 00000000  HandleCount:   0.
    Image: LogonUI.exe

PROCESS ffffdb0de009d080
    SessionId: 1  Cid: 021c    Peb: b16c62000  ParentCid: 0268
    DirBase: 114cc2002  ObjectTable: ffffae0391908480  HandleCount: 1204.
    Image: dwm.exe

PROCESS ffffdb0de069b340
    SessionId: 1  Cid: 0a40    Peb: 9f526a5000  ParentCid: 0634
    DirBase: 122719002  ObjectTable: ffffae03922f8240  HandleCount: 662.
    Image: sihost.exe

PROCESS ffffdb0de069f080
    SessionId: 1  Cid: 0a64    Peb: 39beec5000  ParentCid: 0290
    DirBase: 1226b7002  ObjectTable: ffffae03922fb540  HandleCount: 353.
    Image: svchost.exe

PROCESS ffffdb0de0725080
    SessionId: 1  Cid: 0aac    Peb: a76efc6000  ParentCid: 0290
    DirBase: 10a431002  ObjectTable: ffffae03922fcec0  HandleCount: 550.
    Image: svchost.exe

PROCESS ffffdb0de0794080
    SessionId: 1  Cid: 0ba0    Peb: 1e43ce6000  ParentCid: 0534
    DirBase: 106352002  ObjectTable: ffffae039250c5c0  HandleCount: 283.
    Image: taskhostw.exe

PROCESS ffffdb0de10d60c0
    SessionId: 1  Cid: 13e8    Peb: fdbab30000  ParentCid: 0268
    DirBase: 120866002  ObjectTable: 00000000  HandleCount:   0.
    Image: userinit.exe

PROCESS ffffdb0de11c4080
    SessionId: 1  Cid: 0494    Peb: 00627000  ParentCid: 13e8
    DirBase: 1300ab002  ObjectTable: ffffae03932869c0  HandleCount: 2425.
    Image: explorer.exe

PROCESS ffffdb0de11dd080
    SessionId: 1  Cid: 12d4    Peb: ee9e47d000  ParentCid: 0304
    DirBase: 137788002  ObjectTable: ffffae039251e6c0  HandleCount: 187.
    Image: SettingSyncHost.exe

PROCESS ffffdb0de13ca080
    SessionId: 1  Cid: 1428    Peb: 8332d29000  ParentCid: 0290
    DirBase: 13a995002  ObjectTable: ffffae039328ab80  HandleCount: 315.
    Image: svchost.exe

PROCESS ffffdb0de15ef080
    SessionId: 1  Cid: 16c4    Peb: 7f820a1000  ParentCid: 0304
    DirBase: 12f9a4002  ObjectTable: ffffae0393781180  HandleCount: 725.
    Image: StartMenuExperienceHost.exe

PROCESS ffffdb0de169c080
    SessionId: 1  Cid: 1704    Peb: 51e4f06000  ParentCid: 0304
    DirBase: 90c2d002  ObjectTable: ffffae0393769dc0  HandleCount: 312.
    Image: RuntimeBroker.exe

PROCESS ffffdb0de0ecb080
    SessionId: 1  Cid: 176c    Peb: b5f4d2c000  ParentCid: 0304
DeepFreeze
    DirBase: 924a5002  ObjectTable: ffffae0393768340  HandleCount: 1677.
    Image: SearchApp.exe

PROCESS ffffdb0de1795080
    SessionId: 1  Cid: 17f8    Peb: ae15909000  ParentCid: 0304
    DirBase: 91777002  ObjectTable: ffffae0393787580  HandleCount: 689.
    Image: RuntimeBroker.exe

PROCESS ffffdb0de19452c0
    SessionId: 1  Cid: 165c    Peb: 7ac8c02000  ParentCid: 0304
DeepFreeze
    DirBase: 137d71002  ObjectTable: ffffae0393783280  HandleCount: 534.
    Image: YourPhone.exe

PROCESS ffffdb0de19ae300
    SessionId: 1  Cid: 182c    Peb: b2059db000  ParentCid: 069c
    DirBase: 9778a002  ObjectTable: ffffae03937958c0  HandleCount: 468.
    Image: ctfmon.exe

PROCESS ffffdb0de1a2c080
    SessionId: 1  Cid: 1898    Peb: bf248b000  ParentCid: 069c
    DirBase: 9a4c8002  ObjectTable: ffffae0394402500  HandleCount: 326.
    Image: TabTip.exe

PROCESS ffffdb0de127e080
    SessionId: 1  Cid: 19d4    Peb: 6ab557d000  ParentCid: 0304
DeepFreeze
    DirBase: a216e002  ObjectTable: ffffae03941c2e00  HandleCount: 539.
    Image: LockApp.exe

PROCESS ffffdb0de1c0e080
    SessionId: 1  Cid: 1a00    Peb: 26c59c0000  ParentCid: 0304
    DirBase: a13c9002  ObjectTable: ffffae03941c2580  HandleCount: 577.
    Image: ShellExperienceHost.exe
```

```
PROCESS ffffdb0de1d7d0c0
    SessionId: 1  Cid: 1aac    Peb: c68d3d5000  ParentCid: 0304
    DirBase: a6996002  ObjectTable: ffffae03941ca400  HandleCount: 443.
    Image: RuntimeBroker.exe

PROCESS ffffdb0de1d8c080
    SessionId: 1  Cid: 1b34    Peb: 35f0964000  ParentCid: 0304
    DirBase: a5fb0002  ObjectTable: ffffae03941d27c0  HandleCount: 224.
    Image: RuntimeBroker.exe

PROCESS ffffdb0de1ec4080
    SessionId: 1  Cid: 1b80    Peb: 9662206000  ParentCid: 0304
    DirBase: 133e1b002  ObjectTable: ffffae03941d4240  HandleCount: 359.
    Image: RuntimeBroker.exe

PROCESS ffffdb0de1630080
    SessionId: 1  Cid: 1d3c    Peb: 5068bd6000  ParentCid: 0494
    DirBase: b1f53002  ObjectTable: ffffae0393762d40  HandleCount: 186.
    Image: SecurityHealthSystray.exe

PROCESS ffffdb0de076b080
    SessionId: 1  Cid: 1dbc    Peb: 55d648c000  ParentCid: 0494
    DirBase: a3ea8002  ObjectTable: ffffae03941ee940  HandleCount: 410.
    Image: vmtoolsd.exe

PROCESS ffffdb0de0e47080
    SessionId: 1  Cid: 1ec8    Peb: 34bb373000  ParentCid: 0304
    DirBase: bb33c002  ObjectTable: ffffae03929c5800  HandleCount: 223.
    Image: RuntimeBroker.exe

PROCESS ffffdb0de0791080
    SessionId: 1  Cid: 1f10    Peb: a9a4314000  ParentCid: 0494
    DirBase: 3e377002  ObjectTable: ffffae03941f6480  HandleCount:  92.
    Image: vm3dservice.exe

PROCESS ffffdb0de1995080
    SessionId: 1  Cid: 1f20    Peb: ce1d85e000  ParentCid: 0494
    DirBase: a8aa4002  ObjectTable: ffffae03941f7880  HandleCount: 407.
    Image: OneDrive.exe

PROCESS ffffdb0de06a0080
    SessionId: 1  Cid: 1d00    Peb: 4b664ee000  ParentCid: 0a40
    DirBase: 126f04002  ObjectTable: 00000000  HandleCount:   0.
    Image: msedge.exe

PROCESS ffffdb0de126d080
    SessionId: 1  Cid: 0ab8    Peb: ced1d40000  ParentCid: 0304
    DirBase: 16bd4002  ObjectTable: ffffae0394422840  HandleCount: 551.
    Image: TextInputHost.exe

PROCESS ffffdb0de1ee02c0
    SessionId: 1  Cid: 0598    Peb: 1003ef000  ParentCid: 0304
    DirBase: 264dc002  ObjectTable: ffffae0394426a40  HandleCount: 260.
    Image: dllhost.exe

PROCESS ffffdb0de0ecf2c0
    SessionId: 1  Cid: 03f8    Peb: 633f372000  ParentCid: 0494
    DirBase: 10b80002  ObjectTable: ffffae0391908580  HandleCount: 242.
    Image: notepad.exe
```

```
PROCESS ffffdb0de1ee12c0
    SessionId: 1  Cid: 0df8    Peb: 6d275a6000  ParentCid: 0304
    DirBase: 2c2b2002  ObjectTable: ffffae0394439d40  HandleCount: 533.
    Image: Calculator.exe

PROCESS ffffdb0de220c2c0
    SessionId: 1  Cid: 0e04    Peb: 14571db000  ParentCid: 0304
    DirBase: 24b5a002  ObjectTable: ffffae039443cd00  HandleCount: 503.
    Image: ApplicationFrameHost.exe

PROCESS ffffdb0de2307080
    SessionId: 1  Cid: 16f8    Peb: eef11f7000  ParentCid: 0304
    DirBase: 2f6d6002  ObjectTable: ffffae0394440240  HandleCount: 251.
    Image: RuntimeBroker.exe

PROCESS ffffdb0de22a8080
    SessionId: 1  Cid: 1efc    Peb: 72d0db6000  ParentCid: 0290
    DirBase: 3dabd002  ObjectTable: ffffae0396207180  HandleCount: 461.
    Image: svchost.exe

PROCESS ffffdb0de27c4080
    SessionId: 1  Cid: 1d30    Peb: c96bfa6000  ParentCid: 0360
    DirBase: a2754002  ObjectTable: ffffae0396203b40  HandleCount: 1545.
    Image: msedge.exe

PROCESS ffffdb0de2d59080
    SessionId: 1  Cid: 1d4c    Peb: 7598a4c000  ParentCid: 1d30
    DirBase: 2436f002  ObjectTable: ffffae0394416a40  HandleCount: 165.
    Image: msedge.exe

PROCESS ffffdb0de23c5080
    SessionId: 1  Cid: 237c    Peb: 32fd5bb000  ParentCid: 1d30
    DirBase: a8d39002  ObjectTable: ffffae039620ad00  HandleCount: 511.
    Image: msedge.exe

PROCESS ffffdb0de23c7080
    SessionId: 1  Cid: 2380    Peb: 3dd5153000  ParentCid: 1d30
    DirBase: 11cfff002  ObjectTable: ffffae039620c040  HandleCount: 315.
    Image: msedge.exe

PROCESS ffffdb0de2058080
    SessionId: 1  Cid: 1d98    Peb: c6b0c10000  ParentCid: 1d30
    DirBase: 33b4e002  ObjectTable: ffffae0396211540  HandleCount: 205.
    Image: msedge.exe

PROCESS ffffdb0de2d60080
    SessionId: 1  Cid: 01d4    Peb: b2fa7af000  ParentCid: 0304
    DirBase: afb78002  ObjectTable: ffffae0396232100  HandleCount: 153.
    Image: UserOOBEBroker.exe

PROCESS ffffdb0de3077340
    SessionId: 1  Cid: 14c4    Peb: 19fba9e000  ParentCid: 1d30
    DirBase: 50fdd002  ObjectTable: ffffae039441cd00  HandleCount: 366.
    Image: msedge.exe

PROCESS ffffdb0de1c020c0
    SessionId: 1  Cid: 22e0    Peb: 5061264000  ParentCid: 0304
DeepFreeze
    DirBase: 1127f7002  ObjectTable: ffffae0396218b00  HandleCount: 1129.
    Image: SearchApp.exe
```

```
PROCESS ffffdb0de27b0080
    SessionId: 1  Cid: 2288    Peb: fbb9624000  ParentCid: 1d30
    DirBase: 52b13002  ObjectTable: ffffae0396240e00  HandleCount: 348.
    Image: msedge.exe

PROCESS ffffdb0de240f080
    SessionId: 1  Cid: 1aa0    Peb: bd57386000  ParentCid: 1d30
    DirBase: bbb94002  ObjectTable: ffffae03941b9940  HandleCount: 265.
    Image: msedge.exe

PROCESS ffffdb0de2d5e080
    SessionId: 1  Cid: 19ec    Peb: d5030e0000  ParentCid: 1d30
    DirBase: 50b54002  ObjectTable: ffffae03941d9640  HandleCount: 220.
    Image: msedge.exe

PROCESS ffffdb0ddbb27080
    SessionId: 1  Cid: 0dec    Peb: 5be4328000  ParentCid: 0494
    DirBase: adf09002  ObjectTable: ffffae0398090580  HandleCount: 188.
    Image: notmyfault64.exe

PROCESS ffffdb0de0f5f080
    SessionId: 1  Cid: 1978    Peb: 005b1000  ParentCid: 0304
    DirBase: 9f58d002  ObjectTable: ffffae0398093340  HandleCount: 519.
    Image: explorer.exe

PROCESS ffffdb0de23f5080
    SessionId: 1  Cid: 2028    Peb: 4bf3961000  ParentCid: 0304
DeepFreeze
    DirBase: 9e745002  ObjectTable: ffffae0396212c80  HandleCount: 947.
    Image: SystemSettings.exe

PROCESS ffffdb0de2ec4080
    SessionId: 1  Cid: 1e74    Peb: e4c20f9000  ParentCid: 069c
    DirBase: 4bf1a002  ObjectTable: 00000000  HandleCount:   0.
    Image: TabTip.exe
```

Note: Some commands accept numbers in decimal and some in hexadecimal. This command accepts decimal session numbers, so if you want to specify session number 12 in hex, type 0x12; otherwise, this would be session number C in hex. Use the **.formats** command to convert various numbers:

```
1: kd> .formats 0x12
Evaluate expression:
  Hex:     00000000`00000012
  Decimal: 18
  Decimal (unsigned) : 18
  Octal:   0000000000000000000022
  Binary:  00000000 00000000 00000000 00000000 00000000 00000000 00000000 00010010
  Chars:   ........
  Time:    Thu Jan  1 00:00:18 1970
  Float:   low 2.52234e-044 high 0
  Double:  8.89318e-323
```

Note: You can also use WinDbg as a calculator:

```
1: kd> ? 0n20*2+5
Evaluate expression: 45 = 00000000`0000002d
```

19. Now we come to the **!process 0 0** command to list all processes from all sessions:

```
1: kd> !process 0 0
**** NT ACTIVE PROCESS DUMP ****
PROCESS ffffdb0ddbaa1040
    SessionId: none  Cid: 0004    Peb: 00000000  ParentCid: 0000
    DirBase: 001ad002  ObjectTable: ffffae038da99e00  HandleCount: 3338.
    Image: System

PROCESS ffffdb0ddbadf080
    SessionId: none  Cid: 005c    Peb: 00000000  ParentCid: 0004
    DirBase: 0037a002  ObjectTable: ffffae038da3a1c0  HandleCount:   0.
    Image: Registry

PROCESS ffffdb0dddc98040
    SessionId: none  Cid: 0160    Peb: dd2ea56000  ParentCid: 0004
    DirBase: 132f42002  ObjectTable: ffffae038f353a00  HandleCount:  53.
    Image: smss.exe

PROCESS ffffdb0ddde36080
    SessionId: 0  Cid: 01bc    Peb: c024afd000  ParentCid: 01b0
    DirBase: 115e78002  ObjectTable: ffffae038dec7040  HandleCount: 563.
    Image: csrss.exe

PROCESS ffffdb0ddf7c5080
    SessionId: 0  Cid: 0208    Peb: 4189872000  ParentCid: 01b0
    DirBase: 03c0c002  ObjectTable: ffffae03915f32c0  HandleCount: 166.
    Image: wininit.exe

PROCESS ffffdb0ddf7c9140
    SessionId: 1  Cid: 0218    Peb: eec7286000  ParentCid: 0200
    DirBase: 11cf0c002  ObjectTable: ffffae03915f5180  HandleCount: 454.
    Image: csrss.exe

PROCESS ffffdb0ddf876080
    SessionId: 1  Cid: 0268    Peb: 508399000  ParentCid: 0200
    DirBase: 117690002  ObjectTable: ffffae03915f67c0  HandleCount: 294.
    Image: winlogon.exe

PROCESS ffffdb0ddf8cb100
    SessionId: 0  Cid: 0290    Peb: ddd37c1000  ParentCid: 0208
    DirBase: 115826002  ObjectTable: ffffae03915f6e40  HandleCount: 694.
    Image: services.exe

PROCESS ffffdb0ddf8cc080
    SessionId: 0  Cid: 02a0    Peb: 744c158000  ParentCid: 0208
    DirBase: 117799002  ObjectTable: ffffae03915f9580  HandleCount: 1342.
    Image: lsass.exe

PROCESS ffffdb0ddf90e080
    SessionId: 0  Cid: 0304    Peb: eeb47b0000  ParentCid: 0290
    DirBase: 113306002  ObjectTable: ffffae0391773900  HandleCount: 1500.
    Image: svchost.exe

PROCESS ffffdb0ddf911080
    SessionId: 1  Cid: 031c    Peb: 826a9a6000  ParentCid: 0268
    DirBase: 11059d002  ObjectTable: ffffae03917767c0  HandleCount:  32.
    Image: fontdrvhost.exe

PROCESS ffffdb0ddf9101c0
```

```
    SessionId: 0  Cid: 0324    Peb: d2bfe1b000  ParentCid: 0208
    DirBase: 1104fd002  ObjectTable: ffffae0391776c00  HandleCount:  32.
    Image: fontdrvhost.exe

PROCESS ffffdb0ddf978240
    SessionId: 0  Cid: 036c    Peb: ca82cf2000  ParentCid: 0290
    DirBase: 112b44002  ObjectTable: ffffae0391778e00  HandleCount: 416.
    Image: WUDFHost.exe

PROCESS ffffdb0de001b340
    SessionId: 0  Cid: 03ac    Peb: 47bf3cf000  ParentCid: 0290
    DirBase: 112f59002  ObjectTable: ffffae0391904080  HandleCount: 1224.
    Image: svchost.exe

PROCESS ffffdb0de006e2c0
    SessionId: 0  Cid: 03f0    Peb: 9288fc4000  ParentCid: 0290
    DirBase: 10b05b002  ObjectTable: ffffae0391904c00  HandleCount: 273.
    Image: svchost.exe

PROCESS ffffdb0de009c100
    SessionId: 1  Cid: 01c0    Peb: c37a97f000  ParentCid: 0268
    DirBase: 114d58002  ObjectTable: 00000000  HandleCount:   0.
    Image: LogonUI.exe

PROCESS ffffdb0de009d080
    SessionId: 1  Cid: 021c    Peb: b16c62000  ParentCid: 0268
    DirBase: 114cc2002  ObjectTable: ffffae0391908480  HandleCount: 1204.
    Image: dwm.exe

PROCESS ffffdb0de0133380
    SessionId: 0  Cid: 0410    Peb: e77cd8d000  ParentCid: 0290
    DirBase: 1127f5002  ObjectTable: ffffae0391a91180  HandleCount: 109.
    Image: svchost.exe

PROCESS ffffdb0de0130080
    SessionId: 0  Cid: 0418    Peb: cf46d8d000  ParentCid: 0290
    DirBase: 10ef55002  ObjectTable: ffffae0391a95040  HandleCount: 175.
    Image: svchost.exe

PROCESS ffffdb0de01390c0
    SessionId: 0  Cid: 0420    Peb: 36a6f9f000  ParentCid: 0290
    DirBase: 10d215002  ObjectTable: ffffae0391a937c0  HandleCount: 152.
    Image: svchost.exe

PROCESS ffffdb0de0154080
    SessionId: 0  Cid: 0464    Peb: 9ccba00000  ParentCid: 0290
    DirBase: 10932b002  ObjectTable: ffffae0391a97340  HandleCount: 285.
    Image: svchost.exe

PROCESS ffffdb0de0179080
    SessionId: 0  Cid: 0470    Peb: 1692c1a000  ParentCid: 0290
    DirBase: 1103e4002  ObjectTable: ffffae0391a96c00  HandleCount: 257.
    Image: svchost.exe

PROCESS ffffdb0de017e300
    SessionId: 0  Cid: 04b0    Peb: 531d22d000  ParentCid: 0290
    DirBase: 109759002  ObjectTable: ffffae0391a97040  HandleCount: 224.
    Image: svchost.exe

PROCESS ffffdb0de01a9340
```

```
    SessionId: 0  Cid: 04b8    Peb: 6843260000  ParentCid: 0290
    DirBase: 10b7e2002  ObjectTable: ffffae0391a979c0  HandleCount: 164.
    Image: svchost.exe

PROCESS ffffdb0de01cd2c0
    SessionId: 0  Cid: 0534    Peb: 69bdf9e000  ParentCid: 0290
    DirBase: 10e9a9002  ObjectTable: ffffae0391b3d080  HandleCount: 416.
    Image: svchost.exe

PROCESS ffffdb0de0249300
    SessionId: 0  Cid: 0574    Peb: db74ed6000  ParentCid: 0290
    DirBase: 110fc6002  ObjectTable: ffffae0391b3ea00  HandleCount: 330.
    Image: svchost.exe

PROCESS ffffdb0de024a080
    SessionId: 0  Cid: 0580    Peb: db883dd000  ParentCid: 0290
    DirBase: 116810002  ObjectTable: ffffae0391b3ec40  HandleCount: 262.
    Image: svchost.exe

PROCESS ffffdb0de0299380
    SessionId: 0  Cid: 05dc    Peb: 885bb85000  ParentCid: 0290
    DirBase: 10b751002  ObjectTable: ffffae0391b42e00  HandleCount: 401.
    Image: svchost.exe

PROCESS ffffdb0de02bd0c0
    SessionId: 0  Cid: 05f0    Peb: fdeae21000  ParentCid: 0290
    DirBase: 10931c002  ObjectTable: ffffae0391b45bc0  HandleCount: 157.
    Image: svchost.exe

PROCESS ffffdb0de02c0300
    SessionId: 0  Cid: 0604    Peb: 8f7be06000  ParentCid: 0290
    DirBase: 1072c1002  ObjectTable: ffffae0391b45540  HandleCount: 208.
    Image: svchost.exe

PROCESS ffffdb0de02dd080
    SessionId: 0  Cid: 062c    Peb: 27bed2000  ParentCid: 0290
    DirBase: 12125f002  ObjectTable: ffffae0391b46980  HandleCount: 127.
    Image: svchost.exe

PROCESS ffffdb0de02e02c0
    SessionId: 0  Cid: 0634    Peb: 991c197000  ParentCid: 0290
    DirBase: 1215d7002  ObjectTable: ffffae0391a98ac0  HandleCount: 351.
    Image: svchost.exe

PROCESS ffffdb0de033d080
    SessionId: 0  Cid: 0688    Peb: a79e10000  ParentCid: 0290
    DirBase: 10eaf7002  ObjectTable: ffffae0391b49740  HandleCount: 197.
    Image: svchost.exe

PROCESS ffffdb0de033e080
    SessionId: 0  Cid: 069c    Peb: ce59128000  ParentCid: 0290
    DirBase: 10ea84002  ObjectTable: ffffae0391d14800  HandleCount: 178.
    Image: svchost.exe

PROCESS ffffdb0de038a340
    SessionId: 0  Cid: 0710    Peb: 69e7251000  ParentCid: 0290
    DirBase: 110747002  ObjectTable: ffffae0391d19040  HandleCount: 136.
    Image: svchost.exe

PROCESS ffffdb0ddf7ab0c0
```

```
    SessionId: 0  Cid: 07d4    Peb: 203ec54000  ParentCid: 0290
    DirBase: 11689b002  ObjectTable: ffffae0391d1c9c0  HandleCount: 223.
    Image: svchost.exe

PROCESS ffffdb0de0477340
    SessionId: 0  Cid: 07e0    Peb: 70b84d1000  ParentCid: 0290
    DirBase: 1053a8002  ObjectTable: ffffae0391d1cac0  HandleCount: 454.
    Image: svchost.exe

PROCESS ffffdb0de04750c0
    SessionId: 0  Cid: 07e8    Peb: 96816d8000  ParentCid: 0290
    DirBase: 10baab002  ObjectTable: ffffae0391d1c8c0  HandleCount: 241.
    Image: svchost.exe

PROCESS ffffdb0de04b62c0
    SessionId: 0  Cid: 04a4    Peb: a14bb03000  ParentCid: 0290
    DirBase: 116c5c002  ObjectTable: ffffae0391d1de00  HandleCount: 190.
    Image: svchost.exe

PROCESS ffffdb0ddbbb3040
    SessionId: none  Cid: 0854    Peb: 00000000  ParentCid: 0004
    DirBase: 110816002  ObjectTable: ffffae0391d21200  HandleCount:   0.
    Image: MemCompression

PROCESS ffffdb0ddbae8080
    SessionId: 0  Cid: 0864    Peb: 16738b9000  ParentCid: 0290
    DirBase: 11da78002  ObjectTable: ffffae0391eee0c0  HandleCount: 179.
    Image: svchost.exe

PROCESS ffffdb0ddbb82080
    SessionId: 0  Cid: 0894    Peb: 13fc929000  ParentCid: 0290
    DirBase: 117418002  ObjectTable: ffffae0391ef1e40  HandleCount: 410.
    Image: svchost.exe

PROCESS ffffdb0ddbb7e080
    SessionId: 0  Cid: 08b0    Peb: f2528ad000  ParentCid: 0290
    DirBase: 10aa53002  ObjectTable: ffffae0391ef1d40  HandleCount: 178.
    Image: svchost.exe

PROCESS ffffdb0ddbb6b080
    SessionId: 0  Cid: 08bc    Peb: 288c2fd000  ParentCid: 0290
    DirBase: 10fc2a002  ObjectTable: ffffae0391ef4180  HandleCount: 151.
    Image: svchost.exe

PROCESS ffffdb0de04c2240
    SessionId: 0  Cid: 092c    Peb: 724c5e1000  ParentCid: 0290
    DirBase: 1119db002  ObjectTable: ffffae03922ee840  HandleCount: 351.
    Image: svchost.exe

PROCESS ffffdb0de051c340
    SessionId: 0  Cid: 093c    Peb: 1e9474000  ParentCid: 0290
    DirBase: 10c14f002  ObjectTable: ffffae03922f0c40  HandleCount: 438.
    Image: svchost.exe

PROCESS ffffdb0dddfea0c0
    SessionId: 0  Cid: 09c4    Peb: 56552af000  ParentCid: 0290
    DirBase: 1206c9002  ObjectTable: ffffae03922f3180  HandleCount: 130.
    Image: svchost.exe

PROCESS ffffdb0de061f080
```

```
    SessionId: 0  Cid: 09cc    Peb: 4e06bb6000  ParentCid: 0290
    DirBase: 1207e1002  ObjectTable: ffffae03922f4c00  HandleCount: 278.
    Image: svchost.exe

PROCESS ffffdb0de0673080
    SessionId: 0  Cid: 09d8    Peb: e6817da000  ParentCid: 0290
    DirBase: 120622002  ObjectTable: ffffae03922f6380  HandleCount: 363.
    Image: svchost.exe

PROCESS ffffdb0de067b2c0
    SessionId: 0  Cid: 09f8    Peb: bde1a63000  ParentCid: 0290
    DirBase: 123102002  ObjectTable: ffffae03922f8880  HandleCount: 209.
    Image: svchost.exe

PROCESS ffffdb0de069b340
    SessionId: 1  Cid: 0a40    Peb: 9f526a5000  ParentCid: 0634
    DirBase: 122719002  ObjectTable: ffffae03922f8240  HandleCount: 662.
    Image: sihost.exe

PROCESS ffffdb0de069f080
    SessionId: 1  Cid: 0a64    Peb: 39beec5000  ParentCid: 0290
    DirBase: 1226b7002  ObjectTable: ffffae03922fb540  HandleCount: 353.
    Image: svchost.exe

PROCESS ffffdb0de07262c0
    SessionId: 0  Cid: 0aa4    Peb: 540b9e3000  ParentCid: 0290
    DirBase: 1226dc002  ObjectTable: ffffae03922fbcc0  HandleCount: 208.
    Image: svchost.exe

PROCESS ffffdb0de0725080
    SessionId: 1  Cid: 0aac    Peb: a76efc6000  ParentCid: 0290
    DirBase: 10a431002  ObjectTable: ffffae03922fcec0  HandleCount: 550.
    Image: svchost.exe

PROCESS ffffdb0de0779280
    SessionId: 0  Cid: 0b30    Peb: 00b8c000  ParentCid: 0290
    DirBase: 124988002  ObjectTable: ffffae0392506840  HandleCount: 458.
    Image: spoolsv.exe

PROCESS ffffdb0de0793080
    SessionId: 0  Cid: 0b58    Peb: 5fde8d4000  ParentCid: 0290
    DirBase: 109e07002  ObjectTable: ffffae03925091c0  HandleCount: 175.
    Image: svchost.exe

PROCESS ffffdb0de0792080
    SessionId: 0  Cid: 0b98    Peb: 2a93c35000  ParentCid: 0290
    DirBase: 12024f002  ObjectTable: ffffae039250ac40  HandleCount: 408.
    Image: svchost.exe

PROCESS ffffdb0de0794080
    SessionId: 1  Cid: 0ba0    Peb: 1e43ce6000  ParentCid: 0534
    DirBase: 106352002  ObjectTable: ffffae039250c5c0  HandleCount: 283.
    Image: taskhostw.exe

PROCESS ffffdb0de07d42c0
    SessionId: 0  Cid: 0bd4    Peb: b7d175a000  ParentCid: 0290
    DirBase: 122098002  ObjectTable: ffffae039250e8c0  HandleCount: 316.
    Image: svchost.exe

PROCESS ffffdb0de080c080
```

```
    SessionId: 0  Cid: 08dc    Peb: 5b3a4a9000  ParentCid: 0290
    DirBase: 115645002  ObjectTable: ffffae0391b406c0  HandleCount: 185.
    Image: svchost.exe

PROCESS ffffdb0de097a080
    SessionId: 0  Cid: 0cf8    Peb: 324635f000  ParentCid: 0290
    DirBase: 128144002  ObjectTable: ffffae0392513240  HandleCount: 269.
    Image: svchost.exe

PROCESS ffffdb0de097d2c0
    SessionId: 0  Cid: 0d14    Peb: 203ed4e000  ParentCid: 0290
    DirBase: 12c0b0002  ObjectTable: ffffae0392515980  HandleCount: 537.
    Image: svchost.exe

PROCESS ffffdb0de097c080
    SessionId: 0  Cid: 0d24    Peb: 6cc6bfe000  ParentCid: 0290
    DirBase: 121021002  ObjectTable: ffffae0392515a80  HandleCount: 324.
    Image: svchost.exe

PROCESS ffffdb0de097f2c0
    SessionId: 0  Cid: 0d30    Peb: bab3759000  ParentCid: 0290
    DirBase: 1261c3002  ObjectTable: ffffae0392516740  HandleCount: 401.
    Image: svchost.exe

PROCESS ffffdb0de09c22c0
    SessionId: 0  Cid: 0d74    Peb: 448af91000  ParentCid: 0290
    DirBase: 1278fa002  ObjectTable: ffffae0392517640  HandleCount: 216.
    Image: svchost.exe

PROCESS ffffdb0de09c4340
    SessionId: 0  Cid: 0d88    Peb: d51f6f6000  ParentCid: 0290
    DirBase: 1161d7002  ObjectTable: ffffae039251a0c0  HandleCount: 132.
    Image: svchost.exe

PROCESS ffffdb0de09ba0c0
    SessionId: 0  Cid: 0d9c    Peb: 9437346000  ParentCid: 0290
    DirBase: 11c570002  ObjectTable: ffffae039251ab40  HandleCount: 370.
    Image: svchost.exe

PROCESS ffffdb0de09be080
    SessionId: 0  Cid: 0da4    Peb: ba3c0ea000  ParentCid: 0290
    DirBase: 11c5b2002  ObjectTable: ffffae039251a500  HandleCount: 125.
    Image: svchost.exe

PROCESS ffffdb0de09bc080
    SessionId: 0  Cid: 0db8    Peb: 621c518000  ParentCid: 0290
    DirBase: 1274fb002  ObjectTable: ffffae039251c2c0  HandleCount: 297.
    Image: vmtoolsd.exe

PROCESS ffffdb0de0a6f0c0
    SessionId: 0  Cid: 0dc0    Peb: df448ae000  ParentCid: 0290
    DirBase: 1233ac002  ObjectTable: ffffae039251da00  HandleCount: 839.
    Image: MsMpEng.exe

PROCESS ffffdb0de09c3340
    SessionId: 0  Cid: 0dd4    Peb: 198338c000  ParentCid: 0290
    DirBase: 12bedc002  ObjectTable: ffffae039251c180  HandleCount: 388.
    Image: svchost.exe

PROCESS ffffdb0de0a75080
```

```
    SessionId: 0  Cid: 0de4    Peb: 2b2b40e000  ParentCid: 0290
    DirBase: 12bf05002  ObjectTable: ffffae039251eb00  HandleCount: 174.
    Image: VGAuthService.exe

PROCESS ffffdb0de0aa82c0
    SessionId: 0  Cid: 0e48    Peb: 65b9661000  ParentCid: 0290
    DirBase: 130ced002  ObjectTable: ffffae03929ac680  HandleCount: 363.
    Image: svchost.exe

PROCESS ffffdb0de0a22080
    SessionId: 0  Cid: 0e78    Peb: b2ea219000  ParentCid: 0290
    DirBase: 11c515002  ObjectTable: ffffae03929b00c0  HandleCount: 103.
    Image: svchost.exe

PROCESS ffffdb0de0bc22c0
    SessionId: 0  Cid: 0f18    Peb: 9a6ee77000  ParentCid: 0290
    DirBase: 129da3002  ObjectTable: ffffae03929b4900  HandleCount: 382.
    Image: svchost.exe

PROCESS ffffdb0de0db3080
    SessionId: 0  Cid: 1064    Peb: a3ee134000  ParentCid: 0290
    DirBase: 1394fa002  ObjectTable: ffffae03929c3600  HandleCount: 266.
    Image: dllhost.exe

PROCESS ffffdb0de0ed2300
    SessionId: 0  Cid: 1148    Peb: 10818e3000  ParentCid: 0304
    DirBase: 116b09002  ObjectTable: ffffae03929c95c0  HandleCount: 365.
    Image: WmiPrvSE.exe

PROCESS ffffdb0de108c080
    SessionId: 0  Cid: 12fc    Peb: c9e494a000  ParentCid: 0290
    DirBase: 1124e9002  ObjectTable: ffffae039327e500  HandleCount: 288.
    Image: svchost.exe

PROCESS ffffdb0de10d60c0
    SessionId: 1  Cid: 13e8    Peb: fdbab30000  ParentCid: 0268
    DirBase: 120866002  ObjectTable: 00000000  HandleCount:   0.
    Image: userinit.exe

PROCESS ffffdb0de11c4080
    SessionId: 1  Cid: 0494    Peb: 00627000  ParentCid: 13e8
    DirBase: 1300ab002  ObjectTable: ffffae03932869c0  HandleCount: 2425.
    Image: explorer.exe

PROCESS ffffdb0de12430c0
    SessionId: 0  Cid: 1144    Peb: 9b6bd02000  ParentCid: 0290
    DirBase: 13216e002  ObjectTable: ffffae039328c640  HandleCount: 222.
    Image: svchost.exe

PROCESS ffffdb0de12980c0
    SessionId: 0  Cid: 1100    Peb: f078d8d000  ParentCid: 0290
    DirBase: 132176002  ObjectTable: ffffae039328d600  HandleCount: 228.
    Image: msdtc.exe

PROCESS ffffdb0de11dd080
    SessionId: 1  Cid: 12d4    Peb: ee9e47d000  ParentCid: 0304
    DirBase: 137788002  ObjectTable: ffffae039251e6c0  HandleCount: 187.
    Image: SettingSyncHost.exe

PROCESS ffffdb0de13ca080
```

```
    SessionId: 1  Cid: 1428    Peb: 8332d29000  ParentCid: 0290
    DirBase: 13a995002  ObjectTable: ffffae039328ab80  HandleCount: 315.
    Image: svchost.exe

PROCESS ffffdb0de15ef080
    SessionId: 1  Cid: 16c4    Peb: 7f820a1000  ParentCid: 0304
    DirBase: 12f9a4002  ObjectTable: ffffae0393781180  HandleCount: 725.
    Image: StartMenuExperienceHost.exe

PROCESS ffffdb0de169c080
    SessionId: 1  Cid: 1704    Peb: 51e4f06000  ParentCid: 0304
    DirBase: 90c2d002  ObjectTable: ffffae0393769dc0  HandleCount: 312.
    Image: RuntimeBroker.exe

PROCESS ffffdb0de0ecb080
    SessionId: 1  Cid: 176c    Peb: b5f4d2c000  ParentCid: 0304
DeepFreeze
    DirBase: 924a5002  ObjectTable: ffffae0393768340  HandleCount: 1677.
    Image: SearchApp.exe

PROCESS ffffdb0de1795080
    SessionId: 1  Cid: 17f8    Peb: ae15909000  ParentCid: 0304
    DirBase: 91777002  ObjectTable: ffffae0393787580  HandleCount: 689.
    Image: RuntimeBroker.exe

PROCESS ffffdb0de1793080
    SessionId: 0  Cid: 1518    Peb: 6cd5ed7000  ParentCid: 0290
    DirBase: 8093c002  ObjectTable: ffffae039376da40  HandleCount: 711.
    Image: SearchIndexer.exe

PROCESS ffffdb0de16a6300
    SessionId: 0  Cid: 1514    Peb: 5af211f000  ParentCid: 0290
    DirBase: 885e1002  ObjectTable: ffffae0393788cc0  HandleCount: 329.
    Image: svchost.exe

PROCESS ffffdb0de19452c0
    SessionId: 1  Cid: 165c    Peb: 7ac8c02000  ParentCid: 0304
DeepFreeze
    DirBase: 137d71002  ObjectTable: ffffae0393783280  HandleCount: 534.
    Image: YourPhone.exe

PROCESS ffffdb0de198f2c0
    SessionId: 0  Cid: 1474    Peb: a833abd000  ParentCid: 0290
    DirBase: 9b2fd002  ObjectTable: 00000000  HandleCount:   0.
    Image: svchost.exe

PROCESS ffffdb0de19ae300
    SessionId: 1  Cid: 182c    Peb: b2059db000  ParentCid: 069c
    DirBase: 9778a002  ObjectTable: ffffae03937958c0  HandleCount: 468.
    Image: ctfmon.exe

PROCESS ffffdb0de1a240c0
    SessionId: 0  Cid: 1838    Peb: 32eb95d000  ParentCid: 0290
    DirBase: 962d1002  ObjectTable: ffffae03937946c0  HandleCount: 203.
    Image: NisSrv.exe

PROCESS ffffdb0de1a2c080
    SessionId: 1  Cid: 1898    Peb: bf248b000  ParentCid: 069c
    DirBase: 9a4c8002  ObjectTable: ffffae0394402500  HandleCount: 326.
    Image: TabTip.exe
```

```
PROCESS ffffdb0de127e080
    SessionId: 1  Cid: 19d4    Peb: 6ab557d000  ParentCid: 0304
DeepFreeze
    DirBase: a216e002  ObjectTable: ffffae03941c2e00  HandleCount: 539.
    Image: LockApp.exe

PROCESS ffffdb0de1c0e080
    SessionId: 1  Cid: 1a00    Peb: 26c59c0000  ParentCid: 0304
    DirBase: a13c9002  ObjectTable: ffffae03941c2580  HandleCount: 577.
    Image: ShellExperienceHost.exe

PROCESS ffffdb0de1d7d0c0
    SessionId: 1  Cid: 1aac    Peb: c68d3d5000  ParentCid: 0304
    DirBase: a6996002  ObjectTable: ffffae03941ca400  HandleCount: 443.
    Image: RuntimeBroker.exe

PROCESS ffffdb0de1d8c080
    SessionId: 1  Cid: 1b34    Peb: 35f0964000  ParentCid: 0304
    DirBase: a5fb0002  ObjectTable: ffffae03941d27c0  HandleCount: 224.
    Image: RuntimeBroker.exe

PROCESS ffffdb0de1ec4080
    SessionId: 1  Cid: 1b80    Peb: 9662206000  ParentCid: 0304
    DirBase: 133e1b002  ObjectTable: ffffae03941d4240  HandleCount: 359.
    Image: RuntimeBroker.exe

PROCESS ffffdb0de1ee9080
    SessionId: 0  Cid: 1bf0    Peb: e861c2c000  ParentCid: 0290
    DirBase: a9486002  ObjectTable: ffffae03941dc840  HandleCount: 227.
    Image: svchost.exe

PROCESS ffffdb0de1630080
    SessionId: 1  Cid: 1d3c    Peb: 5068bd6000  ParentCid: 0494
    DirBase: b1f53002  ObjectTable: ffffae0393762d40  HandleCount: 186.
    Image: SecurityHealthSystray.exe

PROCESS ffffdb0de162f300
    SessionId: 0  Cid: 1d60    Peb: 176cbae000  ParentCid: 0290
    DirBase: b1f95002  ObjectTable: ffffae0393789980  HandleCount: 448.
    Image: SecurityHealthService.exe

PROCESS ffffdb0de076b080
    SessionId: 1  Cid: 1dbc    Peb: 55d648c000  ParentCid: 0494
    DirBase: a3ea8002  ObjectTable: ffffae03941ee940  HandleCount: 410.
    Image: vmtoolsd.exe

PROCESS ffffdb0de0e47080
    SessionId: 1  Cid: 1ec8    Peb: 34bb373000  ParentCid: 0304
    DirBase: bb33c002  ObjectTable: ffffae03929c5800  HandleCount: 223.
    Image: RuntimeBroker.exe

PROCESS ffffdb0de0791080
    SessionId: 1  Cid: 1f10    Peb: a9a4314000  ParentCid: 0494
    DirBase: 3e377002  ObjectTable: ffffae03941f6480  HandleCount:  92.
    Image: vm3dservice.exe

PROCESS ffffdb0de1995080
    SessionId: 1  Cid: 1f20    Peb: ce1d85e000  ParentCid: 0494
    DirBase: a8aa4002  ObjectTable: ffffae03941f7880  HandleCount: 407.
    Image: OneDrive.exe

PROCESS ffffdb0de06a0080
    SessionId: 1  Cid: 1d00    Peb: 4b664ee000  ParentCid: 0a40
    DirBase: 126f04002  ObjectTable: 00000000  HandleCount:   0.
    Image: msedge.exe

PROCESS ffffdb0de1d86080
    SessionId: 0  Cid: 1cd8    Peb: a308fcd000  ParentCid: 0290
    DirBase: 08fd1002  ObjectTable: ffffae03944152c0  HandleCount: 272.
    Image: svchost.exe

PROCESS ffffdb0de23c8080
    SessionId: 0  Cid: 0ea8    Peb: 4590410000  ParentCid: 0290
    DirBase: 1c0ef002  ObjectTable: ffffae039442ef00  HandleCount: 163.
    Image: svchost.exe

PROCESS ffffdb0de126d080
    SessionId: 1  Cid: 0ab8    Peb: ced1d40000  ParentCid: 0304
    DirBase: 16bd4002  ObjectTable: ffffae0394422840  HandleCount: 551.
    Image: TextInputHost.exe

PROCESS ffffdb0de1ee02c0
    SessionId: 1  Cid: 0598    Peb: 1003ef000  ParentCid: 0304
    DirBase: 264dc002  ObjectTable: ffffae0394426a40  HandleCount: 260.
    Image: dllhost.exe

PROCESS ffffdb0de0ecf2c0
    SessionId: 1  Cid: 03f8    Peb: 633f372000  ParentCid: 0494
    DirBase: 10b80002  ObjectTable: ffffae0391908580  HandleCount: 242.
    Image: notepad.exe

PROCESS ffffdb0de1ee12c0
    SessionId: 1  Cid: 0df8    Peb: 6d275a6000  ParentCid: 0304
    DirBase: 2c2b2002  ObjectTable: ffffae0394439d40  HandleCount: 533.
    Image: Calculator.exe

PROCESS ffffdb0de220c2c0
    SessionId: 1  Cid: 0e04    Peb: 14571db000  ParentCid: 0304
    DirBase: 24b5a002  ObjectTable: ffffae039443cd00  HandleCount: 503.
    Image: ApplicationFrameHost.exe

PROCESS ffffdb0de2307080
    SessionId: 1  Cid: 16f8    Peb: eef11f7000  ParentCid: 0304
    DirBase: 2f6d6002  ObjectTable: ffffae0394440240  HandleCount: 251.
    Image: RuntimeBroker.exe

PROCESS ffffdb0de22a8080
    SessionId: 1  Cid: 1efc    Peb: 72d0db6000  ParentCid: 0290
    DirBase: 3dabd002  ObjectTable: ffffae0396207180  HandleCount: 461.
    Image: svchost.exe

PROCESS ffffdb0de2d50080
    SessionId: 0  Cid: 1f6c    Peb: 50c2b3000  ParentCid: 0290
    DirBase: 3ddc4002  ObjectTable: ffffae039621e140  HandleCount: 345.
    Image: svchost.exe

PROCESS ffffdb0de257b300
    SessionId: 0  Cid: 0184    Peb: a93c5f3000  ParentCid: 0290
    DirBase: bbf5b002  ObjectTable: ffffae039442f240  HandleCount: 230.
    Image: svchost.exe

PROCESS ffffdb0de26d6080
    SessionId: 0  Cid: 0834    Peb: 8eaabdf000  ParentCid: 0290
    DirBase: beea4002  ObjectTable: ffffae0396220dc0  HandleCount: 105.
    Image: SgrmBroker.exe

PROCESS ffffdb0de2d5a080
    SessionId: 0  Cid: 1b94    Peb: f8bf31f000  ParentCid: 0290
    DirBase: b81ad002  ObjectTable: ffffae0394431640  HandleCount: 320.
    Image: svchost.exe

PROCESS ffffdb0de277c340
    SessionId: 0  Cid: 1e30    Peb: b8ce083000  ParentCid: 0290
    DirBase: 41b5e002  ObjectTable: ffffae0396221640  HandleCount: 193.
    Image: svchost.exe

PROCESS ffffdb0de2792080
    SessionId: 0  Cid: 1338    Peb: 74c9754000  ParentCid: 0290
    DirBase: 41a94002  ObjectTable: ffffae0396225600  HandleCount: 232.
    Image: svchost.exe

PROCESS ffffdb0de1796080
    SessionId: 0  Cid: 22b4    Peb: 41bd8a3000  ParentCid: 0290
    DirBase: 37abc002  ObjectTable: 00000000  HandleCount:   0.
    Image: svchost.exe

PROCESS ffffdb0de259d340
    SessionId: 0  Cid: 1dec    Peb: ab2d84000  ParentCid: 0dc0
    DirBase: 365d1002  ObjectTable: ffffae03941d0b00  HandleCount: 103.
    Image: MpCopyAccelerator.exe

PROCESS ffffdb0de27c4080
    SessionId: 1  Cid: 1d30    Peb: c96bfa6000  ParentCid: 0360
    DirBase: a2754002  ObjectTable: ffffae0396203b40  HandleCount: 1545.
    Image: msedge.exe

PROCESS ffffdb0de2d59080
    SessionId: 1  Cid: 1d4c    Peb: 7598a4c000  ParentCid: 1d30
    DirBase: 2436f002  ObjectTable: ffffae0394416a40  HandleCount: 165.
    Image: msedge.exe

PROCESS ffffdb0de23c5080
    SessionId: 1  Cid: 237c    Peb: 32fd5bb000  ParentCid: 1d30
    DirBase: a8d39002  ObjectTable: ffffae039620ad00  HandleCount: 511.
    Image: msedge.exe

PROCESS ffffdb0de23c7080
    SessionId: 1  Cid: 2380    Peb: 3dd5153000  ParentCid: 1d30
    DirBase: 11cfff002  ObjectTable: ffffae039620c040  HandleCount: 315.
    Image: msedge.exe

PROCESS ffffdb0de2058080
    SessionId: 1  Cid: 1d98    Peb: c6b0c10000  ParentCid: 1d30
    DirBase: 33b4e002  ObjectTable: ffffae0396211540  HandleCount: 205.
    Image: msedge.exe

PROCESS ffffdb0de2d60080
    SessionId: 1  Cid: 01d4    Peb: b2fa7af000  ParentCid: 0304
    DirBase: afb78002  ObjectTable: ffffae0396232100  HandleCount: 153.
    Image: UserOOBEBroker.exe

PROCESS ffffdb0de3077340
    SessionId: 1  Cid: 14c4    Peb: 19fba9e000  ParentCid: 1d30
    DirBase: 50fdd002  ObjectTable: ffffae039441cd00  HandleCount: 366.
    Image: msedge.exe

PROCESS ffffdb0de1c020c0
    SessionId: 1  Cid: 22e0    Peb: 5061264000  ParentCid: 0304
DeepFreeze
    DirBase: 1127f7002  ObjectTable: ffffae0396218b00  HandleCount: 1129.
    Image: SearchApp.exe

PROCESS ffffdb0de3075300
    SessionId: 0  Cid: 0188    Peb: ad81383000  ParentCid: 0290
    DirBase: 65bf7002  ObjectTable: ffffae0393796d00  HandleCount: 125.
    Image: svchost.exe

PROCESS ffffdb0de27b0080
    SessionId: 1  Cid: 2288    Peb: fbb9624000  ParentCid: 1d30
    DirBase: 52b13002  ObjectTable: ffffae0396240e00  HandleCount: 348.
    Image: msedge.exe

PROCESS ffffdb0de240f080
    SessionId: 1  Cid: 1aa0    Peb: bd57386000  ParentCid: 1d30
    DirBase: bbb94002  ObjectTable: ffffae03941b9940  HandleCount: 265.
    Image: msedge.exe

PROCESS ffffdb0de2d5e080
    SessionId: 1  Cid: 19ec    Peb: d5030e0000  ParentCid: 1d30
    DirBase: 50b54002  ObjectTable: ffffae03941d9640  HandleCount: 220.
    Image: msedge.exe

PROCESS ffffdb0ddbb27080
    SessionId: 1  Cid: 0dec    Peb: 5be4328000  ParentCid: 0494
    DirBase: adf09002  ObjectTable: ffffae0398090580  HandleCount: 188.
    Image: notmyfault64.exe

PROCESS ffffdb0de2dea0c0
    SessionId: 0  Cid: 21a4    Peb: dde3e78000  ParentCid: 0304
    DirBase: 113401002  ObjectTable: ffffae0398094100  HandleCount: 192.
    Image: MoUsoCoreWorker.exe

PROCESS ffffdb0de23c4080
    SessionId: 0  Cid: 136c    Peb: 8843cbd000  ParentCid: 0290
    DirBase: 2f26d002  ObjectTable: ffffae039327dc80  HandleCount: 670.
    Image: svchost.exe

PROCESS ffffdb0de242f080
    SessionId: 0  Cid: 1444    Peb: bb11116000  ParentCid: 0290
    DirBase: 130f42002  ObjectTable: ffffae039809a1c0  HandleCount: 176.
    Image: svchost.exe

PROCESS ffffdb0de30650c0
    SessionId: 0  Cid: 1138    Peb: f24660b000  ParentCid: 0290
    DirBase: 2cdcf002  ObjectTable: ffffae039809cb40  HandleCount: 518.
    Image: svchost.exe

PROCESS ffffdb0de3080340
    SessionId: 0  Cid: 1a94    Peb: 6334537000  ParentCid: 0290
    DirBase: 1289ad002  ObjectTable: ffffae03932814c0  HandleCount: 227.
    Image: svchost.exe

PROCESS ffffdb0de306f080
    SessionId: 0  Cid: 1594    Peb: d82cf74000  ParentCid: 0290
    DirBase: 97331002  ObjectTable: ffffae03980a8200  HandleCount: 226.
    Image: svchost.exe

PROCESS ffffdb0de17e4080
    SessionId: 0  Cid: 00d8    Peb: 8bb602b000  ParentCid: 0290
    DirBase: aff46002  ObjectTable: ffffae03980ae280  HandleCount: 137.
    Image: svchost.exe

PROCESS ffffdb0de2ed1340
    SessionId: 0  Cid: 1510    Peb: 2c9d7d7000  ParentCid: 0290
    DirBase: 63441002  ObjectTable: ffffae03980b7640  HandleCount: 1722.
    Image: svchost.exe

PROCESS ffffdb0de0f5f080
    SessionId: 1  Cid: 1978    Peb: 005b1000  ParentCid: 0304
    DirBase: 9f58d002  ObjectTable: ffffae0398093340  HandleCount: 519.
    Image: explorer.exe

PROCESS ffffdb0de24ea080
    SessionId: 0  Cid: 1454    Peb: ad711a000  ParentCid: 0290
    DirBase: 8864d002  ObjectTable: ffffae0393778f00  HandleCount: 175.
    Image: svchost.exe

PROCESS ffffdb0de23f5080
    SessionId: 1  Cid: 2028    Peb: 4bf3961000  ParentCid: 0304
DeepFreeze
    DirBase: 9e745002  ObjectTable: ffffae0396212c80  HandleCount: 947.
    Image: SystemSettings.exe

PROCESS ffffdb0de2ec4080
    SessionId: 1  Cid: 1e74    Peb: e4c20f9000  ParentCid: 069c
    DirBase: 4bf1a002  ObjectTable: 00000000  HandleCount:   0.
    Image: TabTip.exe

PROCESS ffffdb0de22f4080
    SessionId: 0  Cid: 0fa4    Peb: 2f5a955000  ParentCid: 0290
    DirBase: 58f05002  ObjectTable: ffffae0396231540  HandleCount: 172.
    Image: VSSVC.exe

PROCESS ffffdb0de2ea9080
    SessionId: 0  Cid: 159c    Peb: 5977a8f000  ParentCid: 0290
    DirBase: 47f5e002  ObjectTable: ffffae03941ebb80  HandleCount: 136.
    Image: svchost.exe
```

20. Let’s now check one of the **msedge.exe** processes and its threads by using **!process** *<address>* **3f** command:

```
1: kd> !process ffffdb0de2d5e080 3f
PROCESS ffffdb0de2d5e080
    SessionId: 1  Cid: 19ec    Peb: d5030e0000  ParentCid: 1d30
    DirBase: 50b54002  ObjectTable: ffffae03941d9640  HandleCount: 220.
    Image: msedge.exe
    VadRoot ffffdb0de21981e0 Vads 98 Clone 0 Private 1718. Modified 98. Locked 0.
    DeviceMap ffffae0391bb2750
    Token                             ffffae0397af0060
    ElapsedTime                       00:07:49.357
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         545592
    QuotaPoolUsage[NonPagedPool]      13656
    Working Set Sizes (now,min,max)  (6635, 50, 345) (26540KB, 200KB, 1380KB)
    PeakWorkingSetSize                6440
    VirtualSize                       2158978 Mb
    PeakVirtualSize                   2163048 Mb
    PageFaultCount                    7152
    MemoryPriority                    BACKGROUND
    BasePriority                      4
    CommitCharge                      2885
    Job                               ffffdb0de2d9b060

    PEB NULL...


        THREAD ffffdb0de1eeb0c0  Cid 19ec.1cd4  Teb: 000000d5030e1000 Win32Thread: 0000000000000000 WAIT:
(UserRequest) UserMode Non-Alertable
            ffffdb0de18e3ee0  SynchronizationEvent
        Not impersonating
        DeviceMap                 ffffae0391bb2750
        Owning Process            ffffdb0de2d5e080       Image:         msedge.exe
        Attached Process          N/A            Image:         N/A
        Wait Start TickCount      94160          Ticks: 2735 (0:00:00:42.734)
        Context Switch Count      332            IdealProcessor: 1
        UserTime                  00:00:00.093
        KernelTime                00:00:00.046
        Win32 Start Address 0x00007ff6530913a0
        Stack Init fffff406cc892c90 Current fffff406cc8926a0
        Base fffff406cc893000 Limit fffff406cc88d000 Call 0000000000000000
        Priority 4 BasePriority 4 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr               Call Site
        fffff406`cc8926e0 fffff803`1840c970     nt!KiSwapContext+0x76
        fffff406`cc892820 fffff803`1840be9f     nt!KiSwapThread+0x500
        fffff406`cc8928d0 fffff803`1840b743     nt!KiCommitThreadWait+0x14f
        fffff406`cc892970 fffff803`187f7571     nt!KeWaitForSingleObject+0x233
        fffff406`cc892a60 fffff803`187f761a     nt!ObWaitForSingleObject+0x91
        fffff406`cc892ac0 fffff803`18608bb5     nt!NtWaitForSingleObject+0x6a
        fffff406`cc892b00 00007ffe`4bf2cdf4     nt!KiSystemServiceCopyEnd+0x25 (TrapFrame @ fffff406`cc892b00)
        000000d5`039fed78 00000000`00000000     0x00007ffe`4bf2cdf4

        THREAD ffffdb0de2da1500  Cid 19ec.20a0  Teb: 000000d5030e3000 Win32Thread: 0000000000000000 WAIT:
(UserRequest) UserMode Non-Alertable
            ffffdb0de18e39e0  SynchronizationEvent
        Not impersonating
        DeviceMap                 ffffae0391bb2750
        Owning Process            ffffdb0de2d5e080       Image:         msedge.exe
        Attached Process          N/A            Image:         N/A
        Wait Start TickCount      67063          Ticks: 29832 (0:00:07:46.125)
        Context Switch Count      1              IdealProcessor: 0
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x00007ffe1186c3d0
        Stack Init fffff406cca3dc90 Current fffff406cca3d6a0
        Base fffff406cca3e000 Limit fffff406cca38000 Call 0000000000000000
        Priority 4 BasePriority 4 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr               Call Site
        fffff406`cca3d6e0 fffff803`1840c970     nt!KiSwapContext+0x76
        fffff406`cca3d820 fffff803`1840be9f     nt!KiSwapThread+0x500
        fffff406`cca3d8d0 fffff803`1840b743     nt!KiCommitThreadWait+0x14f
        fffff406`cca3d970 fffff803`187f7571     nt!KeWaitForSingleObject+0x233
        fffff406`cca3da60 fffff803`187f761a     nt!ObWaitForSingleObject+0x91
        fffff406`cca3dac0 fffff803`18608bb5     nt!NtWaitForSingleObject+0x6a
        fffff406`cca3db00 00007ffe`4bf2cdf4     nt!KiSystemServiceCopyEnd+0x25 (TrapFrame @ fffff406`cca3db00)
        000000d5`041ff638 00000000`00000000     0x00007ffe`4bf2cdf4

        THREAD ffffdb0de2e8b0c0  Cid 19ec.1954  Teb: 000000d5030e5000 Win32Thread: 0000000000000000 WAIT:
(UserRequest) UserMode Non-Alertable
            ffffdb0de18e5960  SynchronizationEvent
        Not impersonating
        DeviceMap                 ffffae0391bb2750
        Owning Process            ffffdb0de2d5e080       Image:         msedge.exe
        Attached Process          N/A            Image:         N/A
        Wait Start TickCount      67064          Ticks: 29831 (0:00:07:46.109)
        Context Switch Count      1              IdealProcessor: 1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x00007ffe1186c3d0
        Stack Init fffff406cca1ac90 Current fffff406cca1a6a0
        Base fffff406cca1b000 Limit fffff406cca15000 Call 0000000000000000
        Priority 4 BasePriority 4 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr               Call Site
        fffff406`cca1a6e0 fffff803`1840c970     nt!KiSwapContext+0x76
        fffff406`cca1a820 fffff803`1840be9f     nt!KiSwapThread+0x500
        fffff406`cca1a8d0 fffff803`1840b743     nt!KiCommitThreadWait+0x14f
        fffff406`cca1a970 fffff803`187f7571     nt!KeWaitForSingleObject+0x233
        fffff406`cca1aa60 fffff803`187f761a     nt!ObWaitForSingleObject+0x91
        fffff406`cca1aac0 fffff803`18608bb5     nt!NtWaitForSingleObject+0x6a
        fffff406`cca1ab00 00007ffe`4bf2cdf4     nt!KiSystemServiceCopyEnd+0x25 (TrapFrame @ fffff406`cca1ab00)
        000000d5`049ff678 00000000`00000000     0x00007ffe`4bf2cdf4

        THREAD ffffdb0de26020c0  Cid 19ec.1b44  Teb: 000000d5030e7000 Win32Thread: 0000000000000000 WAIT:
(UserRequest) UserMode Non-Alertable
            ffffdb0de18e5760  SynchronizationEvent
        Not impersonating
        DeviceMap                 ffffae0391bb2750
        Owning Process            ffffdb0de2d5e080       Image:         msedge.exe
        Attached Process          N/A            Image:         N/A
        Wait Start TickCount      96725          Ticks: 170 (0:00:00:02.656)
        Context Switch Count      35             IdealProcessor: 0
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x00007ffe1186c3d0
        Stack Init fffff406cca36c90 Current fffff406cca366a0
        Base fffff406cca37000 Limit fffff406cca31000 Call 0000000000000000
        Priority 4 BasePriority 4 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr               Call Site
        fffff406`cca366e0 fffff803`1840c970     nt!KiSwapContext+0x76
        fffff406`cca36820 fffff803`1840be9f     nt!KiSwapThread+0x500
        fffff406`cca368d0 fffff803`1840b743     nt!KiCommitThreadWait+0x14f
        fffff406`cca36970 fffff803`187f7571     nt!KeWaitForSingleObject+0x233
        fffff406`cca36a60 fffff803`187f761a     nt!ObWaitForSingleObject+0x91
        fffff406`cca36ac0 fffff803`18608bb5     nt!NtWaitForSingleObject+0x6a
        fffff406`cca36b00 00007ffe`4bf2cdf4     nt!KiSystemServiceCopyEnd+0x25 (TrapFrame @ fffff406`cca36b00)
        000000d5`051ff9f8 00000000`00000000     0x00007ffe`4bf2cdf4

        THREAD ffffdb0de196b080  Cid 19ec.10fc  Teb: 000000d5030e9000 Win32Thread: 0000000000000000 WAIT:
(UserRequest) UserMode Non-Alertable
            ffffdb0de18e5ce0  SynchronizationEvent
        Not impersonating
        DeviceMap                 ffffae0391bb2750
        Owning Process            ffffdb0de2d5e080       Image:         msedge.exe
        Attached Process          N/A            Image:         N/A
        Wait Start TickCount      96725          Ticks: 170 (0:00:00:02.656)
        Context Switch Count      76             IdealProcessor: 1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x00007ffe1186c3d0
        Stack Init fffff406cca21c90 Current fffff406cca216a0
        Base fffff406cca22000 Limit fffff406cca1c000 Call 0000000000000000
        Priority 2 BasePriority 2 PriorityDecrement 0 IoPriority 0 PagePriority 1
        Child-SP          RetAddr               Call Site
        fffff406`cca216e0 fffff803`1840c970     nt!KiSwapContext+0x76
        fffff406`cca21820 fffff803`1840be9f     nt!KiSwapThread+0x500
        fffff406`cca218d0 fffff803`1840b743     nt!KiCommitThreadWait+0x14f
        fffff406`cca21970 fffff803`187f7571     nt!KeWaitForSingleObject+0x233
        fffff406`cca21a60 fffff803`187f761a     nt!ObWaitForSingleObject+0x91
        fffff406`cca21ac0 fffff803`18608bb5     nt!NtWaitForSingleObject+0x6a
        fffff406`cca21b00 00007ffe`4bf2cdf4     nt!KiSystemServiceCopyEnd+0x25 (TrapFrame @ fffff406`cca21b00)
        000000d5`059ff8f8 00000000`00000000     0x00007ffe`4bf2cdf4

        THREAD ffffdb0de2557080  Cid 19ec.0840  Teb: 000000d5030eb000 Win32Thread: 0000000000000000 WAIT: (WrQueue)
UserMode Non-Alertable
            ffffdb0de23486c0  QueueObject
        Not impersonating
        DeviceMap                 ffffae0391bb2750
        Owning Process            ffffdb0de2d5e080       Image:         msedge.exe
        Attached Process          N/A            Image:         N/A
        Wait Start TickCount      67387          Ticks: 29508 (0:00:07:41.062)
        Context Switch Count      97             IdealProcessor: 0
        UserTime                  00:00:00.015
        KernelTime                00:00:00.015
        Win32 Start Address 0x00007ffe1186c3d0
        Stack Init fffff406cca4bc90 Current fffff406cca4b540
        Base fffff406cca4c000 Limit fffff406cca46000 Call 0000000000000000
        Priority 5 BasePriority 5 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr               Call Site
        fffff406`cca4b580 fffff803`1840c970     nt!KiSwapContext+0x76
        fffff406`cca4b6c0 fffff803`1840be9f     nt!KiSwapThread+0x500
        fffff406`cca4b770 fffff803`1840f7d3     nt!KiCommitThreadWait+0x14f
        fffff406`cca4b810 fffff803`1840f208     nt!KeRemoveQueueEx+0x263
        fffff406`cca4b8b0 fffff803`188d68ed     nt!IoRemoveIoCompletion+0x98
        fffff406`cca4b9e0 fffff803`18608bb5     nt!NtRemoveIoCompletion+0x13d
        fffff406`cca4ba90 00007ffe`4bf2ce94     nt!KiSystemServiceCopyEnd+0x25 (TrapFrame @ fffff406`cca4bb00)
        000000d5`061fef98 00000000`00000000     0x00007ffe`4bf2ce94

        THREAD ffffdb0de278d500  Cid 19ec.1a18  Teb: 000000d5030ef000 Win32Thread: 0000000000000000 WAIT: (WrQueue)
UserMode Alertable
            ffffdb0de2348180  QueueObject
        Not impersonating
        DeviceMap                 ffffae0391bb2750
        Owning Process            ffffdb0de2d5e080       Image:         msedge.exe
        Attached Process          N/A            Image:         N/A
        Wait Start TickCount      67065          Ticks: 29830 (0:00:07:46.093)
        Context Switch Count      1              IdealProcessor: 0
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x00007ffe4bee2ad0
        Stack Init fffff406cca6ec90 Current fffff406cca6e3c0
        Base fffff406cca6f000 Limit fffff406cca69000 Call 0000000000000000
        Priority 4 BasePriority 4 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr               Call Site
        fffff406`cca6e400 fffff803`1840c970     nt!KiSwapContext+0x76
        fffff406`cca6e540 fffff803`1840be9f     nt!KiSwapThread+0x500
        fffff406`cca6e5f0 fffff803`1840f7d3     nt!KiCommitThreadWait+0x14f
        fffff406`cca6e690 fffff803`1840f208     nt!KeRemoveQueueEx+0x263
        fffff406`cca6e730 fffff803`1841029e     nt!IoRemoveIoCompletion+0x98
        fffff406`cca6e860 fffff803`18608bb5     nt!NtWaitForWorkViaWorkerFactory+0x38e
        fffff406`cca6ea90 00007ffe`4bf307c4     nt!KiSystemServiceCopyEnd+0x25 (TrapFrame @ fffff406`cca6eb00)
        000000d5`071ff4a8 00000000`00000000     0x00007ffe`4bf307c4

        THREAD ffffdb0de204d2c0  Cid 19ec.1e78  Teb: 000000d5030f1000 Win32Thread: 0000000000000000 WAIT:
(UserRequest) UserMode Non-Alertable
            ffffdb0de18e84e0  SynchronizationEvent
        Not impersonating
        DeviceMap                 ffffae0391bb2750
        Owning Process            ffffdb0de2d5e080       Image:         msedge.exe
        Attached Process          N/A            Image:         N/A
        Wait Start TickCount      67065          Ticks: 29830 (0:00:07:46.093)
        Context Switch Count      1              IdealProcessor: 1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x00007ffe1186c3d0
        Stack Init fffff406cca75c90 Current fffff406cca756a0
        Base fffff406cca76000 Limit fffff406cca70000 Call 0000000000000000
        Priority 4 BasePriority 4 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr               Call Site
        fffff406`cca756e0 fffff803`1840c970     nt!KiSwapContext+0x76
        fffff406`cca75820 fffff803`1840be9f     nt!KiSwapThread+0x500
        fffff406`cca758d0 fffff803`1840b743     nt!KiCommitThreadWait+0x14f
        fffff406`cca75970 fffff803`187f7571     nt!KeWaitForSingleObject+0x233
        fffff406`cca75a60 fffff803`187f761a     nt!ObWaitForSingleObject+0x91
        fffff406`cca75ac0 fffff803`18608bb5     nt!NtWaitForSingleObject+0x6a
        fffff406`cca75b00 00007ffe`4bf2cdf4     nt!KiSystemServiceCopyEnd+0x25 (TrapFrame @ fffff406`cca75b00)
        000000d5`079ff798 00000000`00000000     0x00007ffe`4bf2cdf4

        THREAD ffffdb0de259f080  Cid 19ec.0e34  Teb: 000000d5030f3000 Win32Thread: 0000000000000000 WAIT:
(UserRequest) UserMode Non-Alertable
            ffffdb0de18e8ce0  SynchronizationEvent
        Not impersonating
        DeviceMap                 ffffae0391bb2750
        Owning Process            ffffdb0de2d5e080       Image:         msedge.exe
        Attached Process          N/A            Image:         N/A
        Wait Start TickCount      67065          Ticks: 29830 (0:00:07:46.093)
        Context Switch Count      3              IdealProcessor: 0
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x00007ffe1186c3d0
        Stack Init fffff406cca67c90 Current fffff406cca676a0
        Base fffff406cca68000 Limit fffff406cca62000 Call 0000000000000000
        Priority 5 BasePriority 5 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr               Call Site
        fffff406`cca676e0 fffff803`1840c970     nt!KiSwapContext+0x76
        fffff406`cca67820 fffff803`1840be9f     nt!KiSwapThread+0x500
        fffff406`cca678d0 fffff803`1840b743     nt!KiCommitThreadWait+0x14f
        fffff406`cca67970 fffff803`187f7571     nt!KeWaitForSingleObject+0x233
        fffff406`cca67a60 fffff803`187f761a     nt!ObWaitForSingleObject+0x91
        fffff406`cca67ac0 fffff803`18608bb5     nt!NtWaitForSingleObject+0x6a
        fffff406`cca67b00 00007ffe`4bf2cdf4     nt!KiSystemServiceCopyEnd+0x25 (TrapFrame @ fffff406`cca67b00)
        000000d5`081ff878 00000000`00000000     0x00007ffe`4bf2cdf4

        THREAD ffffdb0de11f9080  Cid 19ec.0c50  Teb: 000000d5030f7000 Win32Thread: 0000000000000000 WAIT:
(UserRequest) UserMode Non-Alertable
            ffffdb0de18e85e0  SynchronizationEvent
        Not impersonating
        DeviceMap                 ffffae0391bb2750
        Owning Process            ffffdb0de2d5e080       Image:         msedge.exe
        Attached Process          N/A            Image:         N/A
        Wait Start TickCount      67130          Ticks: 29765 (0:00:07:45.078)
        Context Switch Count      3              IdealProcessor: 0
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x00007ffe1186c3d0
        Stack Init fffff406cca28c90 Current fffff406cca286a0
        Base fffff406cca29000 Limit fffff406cca23000 Call 0000000000000000
        Priority 4 BasePriority 4 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr               Call Site
        fffff406`cca286e0 fffff803`1840c970     nt!KiSwapContext+0x76
        fffff406`cca28820 fffff803`1840be9f     nt!KiSwapThread+0x500
        fffff406`cca288d0 fffff803`1840b743     nt!KiCommitThreadWait+0x14f
        fffff406`cca28970 fffff803`187f7571     nt!KeWaitForSingleObject+0x233
        fffff406`cca28a60 fffff803`187f761a     nt!ObWaitForSingleObject+0x91
        fffff406`cca28ac0 fffff803`18608bb5     nt!NtWaitForSingleObject+0x6a
        fffff406`cca28b00 00007ffe`4bf2cdf4     nt!KiSystemServiceCopyEnd+0x25 (TrapFrame @ fffff406`cca28b00)
        000000d5`091ff648 00000000`00000000     0x00007ffe`4bf2cdf4

        THREAD ffffdb0de2ad8080  Cid 19ec.2140  Teb: 000000d5030f9000 Win32Thread: 0000000000000000 WAIT:
(WrAlertByThreadId) UserMode Non-Alertable
            00006444000882b0  NotificationEvent
        Not impersonating
        DeviceMap                 ffffae0391bb2750
        Owning Process            ffffdb0de2d5e080       Image:         msedge.exe
        Attached Process          N/A            Image:         N/A
        Wait Start TickCount      67066          Ticks: 29829 (0:00:07:46.078)
        Context Switch Count      1              IdealProcessor: 1
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x00007ffe1186c3d0
        Stack Init fffff406cca2fc90 Current fffff406cca2f7a0
        Base fffff406cca30000 Limit fffff406cca2a000 Call 0000000000000000
        Priority 4 BasePriority 4 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Child-SP          RetAddr               Call Site
        fffff406`cca2f7e0 fffff803`1840c970     nt!KiSwapContext+0x76
        fffff406`cca2f920 fffff803`1840be9f     nt!KiSwapThread+0x500
        fffff406`cca2f9d0 fffff803`1853973c     nt!KiCommitThreadWait+0x14f
        fffff406`cca2fa70 fffff803`188df210     nt!KeWaitForAlertByThreadId+0xc4
        fffff406`cca2fad0 fffff803`18608bb5     nt!NtWaitForAlertByThreadId+0x30
        fffff406`cca2fb00 00007ffe`4bf30764     nt!KiSystemServiceCopyEnd+0x25 (TrapFrame @ fffff406`cca2fb00)
        000000d5`099ff878 00000000`00000000     0x00007ffe`4bf30764

        THREAD ffffdb0de2429080  Cid 19ec.0f38  Teb: 000000d5030fb000 Win32Thread: 0000000000000000 WAIT:
(WrAlertByThreadId) UserMode Non-Alertable
            00006444000882b0  NotificationEvent
        Not impersonating
        DeviceMap                 ffffae0391bb2750
        Owning Process            ffffdb0de2d5e080       Image:         msedge.exe
        Attached Process          N/A            Image:         N/A
        Wait Start TickCount      67066          Ticks: 29829 (0:00:07:46.078)
        Context Switch Count      6              IdealProcessor: 0
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address 0x00007ffe1186c3d0
        Stack Init fffff406cca44c90 Current fffff406cca447a0
        Base fffff406cca45000 Limit fffff406cca3f000 Call 0000000000000000
        Priority 2 BasePriority 2 PriorityDecrement 0 IoPriority 0 PagePriority 1
        Child-SP          RetAddr               Call Site
        fffff406`cca447e0 fffff803`1840c970     nt!KiSwapContext+0x76
        fffff406`cca44920 fffff803`1840be9f     nt!KiSwapThread+0x500
        fffff406`cca449d0 fffff803`1853973c     nt!KiCommitThreadWait+0x14f
        fffff406`cca44a70 fffff803`188df210     nt!KeWaitForAlertByThreadId+0xc4
        fffff406`cca44ad0 fffff803`18608bb5     nt!NtWaitForAlertByThreadId+0x30
        fffff406`cca44b00 00007ffe`4bf30764     nt!KiSystemServiceCopyEnd+0x25 (TrapFrame @ fffff406`cca44b00)
        000000d5`0a1ffa38 00000000`00000000     0x00007ffe`4bf30764
```

Note: The command outputs every thread stack trace. We also note that every thread is not running and has a "swapped" context (saved to be restored when a thread is scheduled for running).

21. Let's make the last explorer thread current (**.thread** *<address>* command) so we can use **kv** command, for example:

```
1: kd> .thread ffffdb0de2429080
Implicit thread is now ffffdb0d`e2429080

1: kd> kv
  *** Stack trace for last set context - .thread/.cxr resets it
 # Child-SP          RetAddr               : Args to Child                                                           : Call Site
00 fffff406`cca447e0 fffff803`1840c970     : fffff803`13caf180 00000000`ffffffff 00000000`00000000 00000000`00000000 : nt!KiSwapContext+0x76
01 fffff406`cca44920 fffff803`1840be9f     : ffffdb0d`00000000 00000000`00000001 00000000`00000000 00000000`00000000 : nt!KiSwapThread+0x500
02 fffff406`cca449d0 fffff803`1853973c     : ffffdb0d`00000000 ffffdb0d`00000000 fffff406`00000000 00006444`00088378 : nt!KiCommitThreadWait+0x14f
03 fffff406`cca44a70 fffff803`188df210     : ffffdb0d`e2429080 fffff406`cca44b80 00000000`00000000 00000000`00000000 : nt!KeWaitForAlertByThreadId+0xc4
04 fffff406`cca44ad0 fffff803`18608bb5     : ffffdb0d`e2429080 00000000`00000000 00000000`00000000 ffffdb0d`00000000 : nt!NtWaitForAlertByThreadId+0x30
05 fffff406`cca44b00 00007ffe`4bf30764     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : nt!KiSystemServiceCopyEnd+0x25
(TrapFrame @ fffff406`cca44b00)
06 000000d5`0a1ffa38 00000000`00000000     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : 0x00007ffe`4bf30764
```

Note: Trap frame for **nt!KiSystemServiceCopyEnd** is not a fault: the transition from user to kernel mode uses a similar mechanism to save process and thread context in user mode. We see that when we look at a complete memory dump later. If we want to revert to the original thread, we can use the **.thread** command again (without parameters).

Note: We can come back to the original running thread by omitting the thread address:

```
1: kd> .thread
Implicit thread is now ffffcb00`34fce0c0

1: kd> kv
 # Child-SP          RetAddr               : Args to Child                                                           : Call Site
00 fffff406`c98296b8 fffff803`185b9eb4     : 00000000`00000000 000002ed`4b3eb6af 00000000`00000000 00000000`00000024 : nt!HalProcessorIdle+0xf
01 fffff406`c98296c0 fffff803`184184b6     : ffffffff`ffffffff 00000000`00000000 00000000`00000000 00000000`00000000 : nt!PpmIdleDefaultExecute+0x14
02 fffff406`c98296f0 fffff803`18417274     : 00000000`00000000 00001f80`00000200 00000000`00000000 00000000`00000000 : nt!PpmIdleExecuteTransition+0x10c6
03 fffff406`c9829af0 fffff803`185face4     : 00000000`00000000 ffffcb00`34fce0c0 ffffdb0d`e1bf0080 00000000`00001004 : nt!PoIdle+0x374
04 fffff406`c9829c60 00000000`00000000     : fffff406`c982a000 fffff406`c9824000 00000000`00000000 00000000`00000000 : nt!KiIdleLoop+0x54
```

22. What if we want to list every process and thread? This action is useful to check for anomalies, especially in complete memory dumps. We can use the **!process 0 3f** command. **The command can be time-consuming**.

23. Another way to list all threads or list threads based on some stack trace pattern is to use the **!stacks** command:

```
1: kd> !stacks 2
Proc.Thread  .Thread  Ticks   ThreadState Blocker
                            [fffff80318f23a00 Idle]
   0.000000  fffff80318f26a00 0000aaa RUNNING    nt!KiIdleLoop+0x176
   0.000000  ffffcb0034fce0c0 0017a7f RUNNING    nt!HalProcessorIdle+0xf
                                        nt!PpmIdleDefaultExecute+0x14
                                        nt!PpmIdleExecuteTransition+0x10c6
                                        nt!PoIdle+0x374
                                        nt!KiIdleLoop+0x54
                            [ffffdb0ddbaa1040 System]
   4.00000c  ffffdb0ddbaa2040 00177a6 Blocked    nt!KiSwapContext+0x76
                                        nt!KiSwapThread+0x500
                                        nt!KiCommitThreadWait+0x14f
                                        nt!KeWaitForSingleObject+0x233
                                        nt!PopIrpWorkerControl+0x22
                                        nt!PspSystemThreadStartup+0x55
                                        nt!KiStartSystemThread+0x28
   4.000010  ffffdb0ddbb57080 00177a6 Blocked    nt!KiSwapContext+0x76
                                        nt!KiSwapThread+0x500
                                        nt!KiCommitThreadWait+0x14f
                                        nt!KeWaitForSingleObject+0x233
                                        nt!PopIrpWorker+0xf9
                                        nt!PspSystemThreadStartup+0x55
                                        nt!KiStartSystemThread+0x28
   4.000014  ffffdb0ddbb02080 00177a6 Blocked    nt!KiSwapContext+0x76
                                        nt!KiSwapThread+0x500
                                        nt!KiCommitThreadWait+0x14f
                                        nt!KeWaitForSingleObject+0x233
                                        nt!PopIrpWorker+0xf9
                                        nt!PspSystemThreadStartup+0x55
                                        nt!KiStartSystemThread+0x28
   4.000018  ffffdb0ddbacc080 0004b2a Blocked    nt!KiSwapContext+0x76
                                        nt!KiSwapThread+0x500
                                        nt!KiCommitThreadWait+0x14f
                                        nt!KeWaitForMultipleObjects+0x2be
                                        nt!PopFxProcessWorkPool+0xed
                                        nt!PopFxEmergencyWorker+0x27
                                        nt!PspSystemThreadStartup+0x55
                                        nt!KiStartSystemThread+0x28

[...]

                            [ffffdb0dddc98040 smss.exe]
 160.000164  ffffdb0dddcd7040 00177eb Blocked    Stack paged out
 160.00016c  ffffdb0dddcdb080 001778d Blocked    Stack paged out
 160.0013e4  ffffdb0de10d8040 0007506 Blocked    nt!KiSwapContext+0x76
                                        nt!KiSwapThread+0x500
                                        nt!KiCommitThreadWait+0x14f
                                        nt!KeRemoveQueueEx+0x263
                                        nt!IoRemoveIoCompletion+0x98
                                        nt!NtWaitForWorkViaWorkerFactory+0x38e
                                        nt!KiSystemServiceCopyEnd+0x25
                                        +0x7ffe4bf307c4

                            [ffffdb0ddde36080 csrss.exe]
 1bc.0001cc  ffffdb0ddde42080 0000034 Blocked    nt!KiSwapContext+0x76
                                        nt!KiSwapThread+0x500
                                        nt!KiCommitThreadWait+0x14f
                                        nt!KeWaitForSingleObject+0x233
                                        nt!AlpcpWaitForSingleObject+0x3e
                                        nt!AlpcpCompleteDeferSignalRequestAndWait+0x3c
                                        nt!AlpcpReceiveMessagePort+0x3ad
                                        nt!AlpcpReceiveMessage+0x33d
                                        nt!NtAlpcSendWaitReceivePort+0xfe
                                        nt!KiSystemServiceCopyEnd+0x25
                                        +0x7ffe4bf2dee4

[...]
```

```
0: kd> !stacks 2 fault
Proc.Thread  .Thread  Ticks   ThreadState Blocker
                            [fffff80318f23a00 Idle]
   0.000000  ffffcb0034fce0c0 0017a7f RUNNING    nt!HalProcessorIdle+0xf
                                        nt!PpmIdleDefaultExecute+0x14
                                        nt!PpmIdleExecuteTransition+0x10c6
                                        nt!PoIdle+0x374
                                        nt!KiIdleLoop+0x54
                            [ffffdb0ddbaa1040 System]

                            [ffffdb0ddbadf080 Registry]

                            [ffffdb0dddc98040 smss.exe]

                            [ffffdb0ddde36080 csrss.exe]

                            [ffffdb0ddf7c5080 wininit.exe]

                            [ffffdb0ddf7c9140 csrss.exe]

                            [ffffdb0ddf876080 winlogon.exe]

                            [ffffdb0ddf8cb100 services.exe]

                            [ffffdb0ddf8cc080 lsass.exe]

                            [ffffdb0ddf90e080 svchost.exe]

                            [ffffdb0ddf911080 fontdrvhost.ex]

                            [ffffdb0ddf9101c0 fontdrvhost.ex]

                            [ffffdb0ddf978240 WUDFHost.exe]

                            [ffffdb0de001b340 svchost.exe]

                            [ffffdb0de006e2c0 svchost.exe]

                            [ffffdb0de009c100 LogonUI.exe]

                            [ffffdb0de009d080 dwm.exe]

                            [ffffdb0de0133380 svchost.exe]

                            [ffffdb0de0130080 svchost.exe]

                            [ffffdb0de01390c0 svchost.exe]

                            [ffffdb0de0154080 svchost.exe]

                            [ffffdb0de0179080 svchost.exe]

                            [ffffdb0de017e300 svchost.exe]

                            [ffffdb0de01a9340 svchost.exe]

                            [ffffdb0de01cd2c0 svchost.exe]

                            [ffffdb0de0249300 svchost.exe]
```

```
[ffffdb0de024a080 svchost.exe]
[ffffdb0de0299380 svchost.exe]
[ffffdb0de02bd0c0 svchost.exe]
[ffffdb0de02c0300 svchost.exe]
[ffffdb0de02dd080 svchost.exe]
[ffffdb0de02e02c0 svchost.exe]
[ffffdb0de033d080 svchost.exe]
[ffffdb0de033e080 svchost.exe]
[ffffdb0de038a340 svchost.exe]
[ffffdb0ddf7ab0c0 svchost.exe]
[ffffdb0de0477340 svchost.exe]
[ffffdb0de04750c0 svchost.exe]
[ffffdb0de04b62c0 svchost.exe]
[ffffdb0ddbbb3040 MemCompression]
[ffffdb0ddbae8080 svchost.exe]
[ffffdb0ddbb82080 svchost.exe]
[ffffdb0ddbb7e080 svchost.exe]
[ffffdb0ddbb6b080 svchost.exe]
[ffffdb0de04c2240 svchost.exe]
[ffffdb0de051c340 svchost.exe]
[ffffdb0dddfea0c0 svchost.exe]
[ffffdb0de061f080 svchost.exe]
[ffffdb0de0673080 svchost.exe]
[ffffdb0de067b2c0 svchost.exe]
[ffffdb0de069b340 sihost.exe]
[ffffdb0de069f080 svchost.exe]
[ffffdb0de07262c0 svchost.exe]
[ffffdb0de0725080 svchost.exe]
[ffffdb0de0779280 spoolsv.exe]
[ffffdb0de0793080 svchost.exe]
```

```
[ffffdb0de0792080 svchost.exe]

[ffffdb0de0794080 taskhostw.exe]

[ffffdb0de07d42c0 svchost.exe]

[ffffdb0de080c080 svchost.exe]

[ffffdb0de097a080 svchost.exe]

[ffffdb0de097d2c0 svchost.exe]

[ffffdb0de097c080 svchost.exe]

[ffffdb0de097f2c0 svchost.exe]

[ffffdb0de09c22c0 svchost.exe]

[ffffdb0de09c4340 svchost.exe]

[ffffdb0de09ba0c0 svchost.exe]

[ffffdb0de09be080 svchost.exe]

[ffffdb0de09bc080 vmtoolsd.exe]

[ffffdb0de0a6f0c0 MsMpEng.exe]

[ffffdb0de09c3340 svchost.exe]

[ffffdb0de0a75080 VGAuthService.]

[ffffdb0de0aa82c0 svchost.exe]

[ffffdb0de0a22080 svchost.exe]

[ffffdb0de0bc22c0 svchost.exe]

[ffffdb0de0db3080 dllhost.exe]

[ffffdb0de0ed2300 WmiPrvSE.exe]

[ffffdb0de108c080 svchost.exe]

[ffffdb0de10d60c0 userinit.exe]

[ffffdb0de11c4080 explorer.exe]

[ffffdb0de12430c0 svchost.exe]

[ffffdb0de12980c0 msdtc.exe]

[ffffdb0de11dd080 SettingSyncHos]

[ffffdb0de13ca080 svchost.exe]

[ffffdb0de15ef080 StartMenuExper]

[ffffdb0de169c080 RuntimeBroker.]
```

```
[ffffdb0de0ecb080 SearchApp.exe]

[ffffdb0de1795080 RuntimeBroker.]

[ffffdb0de1793080 SearchIndexer.]

[ffffdb0de16a6300 svchost.exe]

[ffffdb0de19452c0 YourPhone.exe]

[ffffdb0de198f2c0 svchost.exe]

[ffffdb0de19ae300 ctfmon.exe]

[ffffdb0de1a240c0 NisSrv.exe]

[ffffdb0de1a2c080 TabTip.exe]

[ffffdb0de127e080 LockApp.exe]

[ffffdb0de1c0e080 ShellExperienc]

[ffffdb0de1d7d0c0 RuntimeBroker.]

[ffffdb0de1d8c080 RuntimeBroker.]

[ffffdb0de1ec4080 RuntimeBroker.]

[ffffdb0de1ee9080 svchost.exe]

[ffffdb0de1630080 SecurityHealth]

[ffffdb0de162f300 SecurityHealth]

[ffffdb0de076b080 vmtoolsd.exe]

[ffffdb0de0e47080 RuntimeBroker.]

[ffffdb0de0791080 vm3dservice.ex]

[ffffdb0de1995080 OneDrive.exe]

[ffffdb0de06a0080 msedge.exe]

[ffffdb0de1d86080 svchost.exe]

[ffffdb0de23c8080 svchost.exe]

[ffffdb0de126d080 TextInputHost.]

[ffffdb0de1ee02c0 dllhost.exe]

[ffffdb0de0ecf2c0 notepad.exe]

[ffffdb0de1ee12c0 Calculator.exe]

[ffffdb0de220c2c0 ApplicationFra]

[ffffdb0de2307080 RuntimeBroker.]
```

```
                           [ffffdb0de22a8080 svchost.exe]

                           [ffffdb0de2d50080 svchost.exe]

                           [ffffdb0de257b300 svchost.exe]

                           [ffffdb0de26d6080 SgrmBroker.exe]

                           [ffffdb0de2d5a080 svchost.exe]

                           [ffffdb0de277c340 svchost.exe]

                           [ffffdb0de2792080 svchost.exe]

                           [ffffdb0de1796080 svchost.exe]

                           [ffffdb0de259d340 MpCopyAccelera]

                           [ffffdb0de27c4080 msedge.exe]

                           [ffffdb0de2d59080 msedge.exe]

                           [ffffdb0de23c5080 msedge.exe]

                           [ffffdb0de23c7080 msedge.exe]

                           [ffffdb0de2058080 msedge.exe]

                           [ffffdb0de2d60080 UserOOBEBroker]

                           [ffffdb0de3077340 msedge.exe]

                           [ffffdb0de1c020c0 SearchApp.exe]

                           [ffffdb0de3075300 svchost.exe]

                           [ffffdb0de27b0080 msedge.exe]

                           [ffffdb0de240f080 msedge.exe]

                           [ffffdb0de2d5e080 msedge.exe]

                           [ffffdb0ddbb27080 notmyfault64.e]
dec.001e28  ffffdb0de16bd080 0000001 RUNNING    nt!KeBugCheckEx
                                       nt!KiBugCheckDispatch+0x69
                                       nt!KiPageFault+0x469
                                       myfault+0x1981
                                       myfault+0x1d3d
                                       myfault+0x1ea1
                                       nt!IofCallDriver+0x55
                                       nt!IopSynchronousServiceTail+0x1a8
                                       nt!IopXxxControlFile+0x5e5
                                       nt!NtDeviceIoControlFile+0x56
                                       nt!KiSystemServiceCopyEnd+0x25
                                       +0x7ffe4bf2ce54

                           [ffffdb0de2dea0c0 MoUsoCoreWorke]

                           [ffffdb0de23c4080 svchost.exe]
```

```
                            [ffffdb0de242f080 svchost.exe]

                            [ffffdb0de30650c0 svchost.exe]

                            [ffffdb0de3080340 svchost.exe]

                            [ffffdb0de306f080 svchost.exe]

                            [ffffdb0de17e4080 svchost.exe]

                            [ffffdb0de2ed1340 svchost.exe]

                            [ffffdb0de0f5f080 explorer.exe]

                            [ffffdb0de24ea080 svchost.exe]

                            [ffffdb0de23f5080 SystemSettings]

                            [ffffdb0de2ec4080 TabTip.exe]

                            [ffffdb0de22f4080 VSSVC.exe]

                            [ffffdb0de2ea9080 svchost.exe]


Threads Processed: 1620
```

24. The kernel uses its own dynamic memory called a pool (like a heap for processes). There are 2 kinds of a pool: paged (can be swapped to a page file) and nonpaged (resident in memory). Nx nonpaged pool is for noexecute data. We can see pool stats in the output of the **!vm** command:

```
1: kd> !vm

[...]

Modified Pages:               8530 (      34120 Kb)
Modified PF Pages:            8184 (      32736 Kb)
Modified No Write Pages:         0 (          0 Kb)
NonPagedPool Usage:            229 (        916 Kb)
NonPagedPoolNx Usage:        21033 (      84132 Kb)
NonPagedPool Max:       4294967296 (17179869184 Kb)
PagedPool Usage:             34452 (     137808 Kb)
PagedPool Maximum:      4294967296 (17179869184 Kb)
Processor Commit:              468 (       1872 Kb)
Session Commit:               4457 (      17828 Kb)
Shared Commit:               72552 (     290208 Kb)
Special Pool:                    0 (          0 Kb)
Kernel Stacks:               10230 (      40920 Kb)
Pages For MDLs:               1961 (       7844 Kb)
ContigMem Pages:                 0 (          0 Kb)
Partition Pages:                 0 (          0 Kb)
Pages For AWE:                   0 (          0 Kb)
NonPagedPool Commit:         22027 (      88108 Kb)
PagedPool Commit:            34452 (     137808 Kb)
Driver Commit:               12741 (      50964 Kb)
Boot Commit:                  4731 (      18924 Kb)
PFN Array Commit:            12833 (      51332 Kb)
SmallNonPagedPtesCommit:       133 (        532 Kb)
SlabAllocatorPages:           4608 (      18432 Kb)
```

```
SkPagesInUnchargedSlabs:        0 (         0 Kb)
System PageTables:            823 (      3292 Kb)
ProcessLockedFilePages:        12 (        48 Kb)
Pagefile Hash Pages:            4 (        16 Kb)
Sum System Commit:         182032 (    728128 Kb)
Total Private:             465388 (   1861552 Kb)

[...]
```

25. Usually, when a driver or an OS subsystem uses a pool, it associates a so-called pool tag with each allocation. We can use **!poolused 4** or **!poolused 5** commands to see how many bytes were allocated per each pool tag in the paged pool and **!poolused 2** or **!poolused 3** for nonpaged pool tags (the command output was truncated for clarity here):

```
1: kd> !poolused 4
..
 Sorting by Paged Pool Consumed

               NonPaged                  Paged
 Tag     Allocs         Used     Allocs         Used

 MmSt         0            0       7906     18895584     Mm section object prototype ptes , Binary: nt!mm
 CM25         0            0       3223     14635008     Internal Configuration manager allocations , Binary: nt!cm
 FMfn         4         1216      22978     10849280     NAME_CACHE_NODE structure , Binary: fltmgr.sys
 MmRe         0            0       1720      8779056     ASLR relocation blocks , Binary: nt!mm
 Ntff        11         4048       5295      7455360     FCB_DATA , Binary: ntfs.sys
 Toke         0            0       3117      5552704     Token objects , Binary: nt!se
 RvaL         0            0       1683      4178816     UNKNOWN pooltag 'RvaL', please update pooltag.txt
 CM16         0            0        555      2584576     Internal Configuration manager allocations , Binary: nt!cm
 MPsc         0            0       4870      2571360     UNKNOWN pooltag 'MPsc', please update pooltag.txt
 Obtb         0            0        631      1950432     object tables via EX handle.c , Binary: nt!ob
 ClfI         0            0         19      1782880     CLFS Log marshal buffer lookaside list , Binary: clfs.sys
 NtfF         0            0       1068      1708800     FCB_INDEX , Binary: ntfs.sys
 SeAt         0            0      15467      1646048     Security Attributes , Binary: nt!se
[...]
 Nhfs         2         4672          0            0     NetIO Hash Function State Data , Binary: tcpip.sys
 Alep       160        23200          0            0     ALE process info , Binary: tcpip.sys
 HGTG         1           96          0            0     UNKNOWN pooltag 'HGTG', please update pooltag.txt
 NLcp         2         3584          0            0     Network Layer Compartments , Binary: tcpip.sys
 TDIk         4         6912          0            0     TDI resource
 TcRF         1         1600          0            0     TCP Recent Connection Failure , Binary: tcpip.sys
 NSIk       704       270720          0            0     NSI RPC Tansactions , Binary: nsi.dll
 LS2e         3         1280          0            0     SMB2 endpoint , Binary: srv2.sys
 PoEi         1           48          0            0     MTAG_HANDLETABLE , Binary: raspppoe.sys
 Wnln         4          256          0            0     UNKNOWN pooltag 'Wnln', please update pooltag.txt
 InCo         2          128          0            0     Inet Compartment , Binary: tcpip.sys
 UMDs         1          128          0            0     UMDF pool allocation , Binary: WUDFRd.sys
 TcST         5          880          0            0     TCP Syn TCBs , Binary: tcpip.sys
 HidP        13        38400          0            0     HID Parser , Binary: hidparse.sys
 BTMO         1          128          0            0     Bluetooth modem , Binary: bthmodem.sys
 ClfB         9        77760          0            0     CLFS Log base file lookaside list , Binary: clfs.sys
 SWfd         1          800          0            0     POOLTAG_DEVICE_FDOEXTENSION
 Ipcr        58         7104          0            0     IP Cache-aware Reference Counters , Binary: tcpip.sys
 WfpS         4        14832          0            0     WFP startup , Binary: netio.sys
 Ipur         4        16384          0            0     IP Unicast Routes , Binary: tcpip.sys
 ObCI         2          288          0            0     object creation lookaside list , Binary: nt!ob
 Nph2         2         8192          0            0     NetIO Protocol Header2 Data , Binary: netio.sys
 RaDr         5         8368          0            0     DPC_REDIRECTION_TAG , Binary: storport.sys
 aFDT         5          480          0            0     Afd TL provider context , Binary: afd.sys
 NDoc         1           80          0            0     NDIS_TAG_OPEN_CONTEXT , Binary: ndis.sys
 MPic         5         2880          0            0     UNKNOWN pooltag 'MPic', please update pooltag.txt
 Wfra         3         1072          0            0     UNKNOWN pooltag 'Wfra', please update pooltag.txt
 smBA        36         9520          0            0     ReadyBoost allocations , Binary: nt!store or rdyboost.sys
 I6nb         3        12288          0            0     IPv6 Neighbors , Binary: tcpip.sys
 ScAD         1           48          0            0     Mass storage driver tags
 MmCx        19          608          0            0     info for dynamic section extension , Binary: nt!mm
 ScCD         3          512          0            0     Adaptor & Device descriptor buffer , Binary: cdrom.sys
 NDel        11         1872          0            0     NDIS debugging event log , Binary: ndis.sys
 UMDu         1           32          0            0     UMDF pool allocation , Binary: WUDFRd.sys
 SePa         1          32          0           0     Process audit image names and captured policy structures ,
Binary: nt!se

TOTAL     191889      86738928      236363     121475920
```

Note: We see, for example, *MmSt* pool tag belongs to *nt!mm* subsystem (memory management) and *ntfs.sys* allocated 7455360 bytes and tagged these allocations with *Ntff* pool tag.

26. The **!locks** command is frequently used to see if there are any blockages or deadlocks in file and remote file systems and SMB redirectors (this command is a bit similar to the critical section command in user space, **!cs**):

```
1: kd> !locks
**** DUMP OF ALL RESOURCE OBJECTS ****
KD: Scanning for held
locks.............................................................................................
................................................................................................
................................................................................................
................................................................................................
................................................................................................
.......................................................................................
17731 total locks
```

Note: For a practical example of using **!locks,** please refer to the **Wait Chain (Executive Resources)** case study at the end of the course reprinted from Memory Dump Analysis Anthology, Revised Edition, Volume 2. There is also a list of associated patterns and case studies (also available in Memory Dump Analysis Anthology, Volume 7):

https://www.dumpanalysis.org/blog/index.php/2011/11/07/eresource-patterns-and-case-studies/

27. We can use the following command to check the computer name from a kernel memory dump (this is useful for support when a customer just sends *memory.dmp*, and you want to tell them they forgot to apply a fix on just one bluescreening computer):

```
1: kd> dS mrxsmb!SmbCeContext+10
ffffdb0d`dd910860  "DESKTOP-OGPC0LO"
```

28. And finally (almost), its time for **!analyze –v** command:

```
1: kd> !analyze -v
*******************************************************************************
*                                                                             *
*                        Bugcheck Analysis                                    *
*                                                                             *
*******************************************************************************

DRIVER_IRQL_NOT_LESS_OR_EQUAL (d1)
An attempt was made to access a pageable (or completely invalid) address at an
interrupt request level (IRQL) that is too high.  This is usually
caused by drivers using improper addresses.
If kernel debugger is available get stack backtrace.
Arguments:
Arg1: ffffae03917c7760, memory referenced
Arg2: 0000000000000002, IRQL
Arg3: 0000000000000000, value 0 = read operation, 1 = write operation
Arg4: fffff80315431981, address which referenced memory

Debugging Details:
------------------

Page 1229a4 not present in the dump file. Type ".hh dbgerr004" for details
Page 1229a4 not present in the dump file. Type ".hh dbgerr004" for details

KEY_VALUES_STRING: 1

    Key  : Analysis.CPU.mSec
    Value: 2249

    Key  : Analysis.DebugAnalysisProvider.CPP
    Value: Create: 8007007e on DESKTOP-IS6V2L0
    Key  : Analysis.DebugData
    Value: CreateObject

    Key  : Analysis.DebugModel
    Value: CreateObject

    Key  : Analysis.Elapsed.mSec
    Value: 3215

    Key  : Analysis.Init.CPU.mSec
    Value: 879312

    Key  : Analysis.Init.Elapsed.mSec
    Value: 29219880

    Key  : Analysis.Memory.CommitPeak.Mb
    Value: 677

    Key  : Analysis.System
    Value: CreateObject

    Key  : WER.OS.Branch
    Value: vb_release

    Key  : WER.OS.Timestamp
    Value: 2019-12-06T14:06:00Z

    Key  : WER.OS.Version
    Value: 10.0.19041.1


ADDITIONAL_XML: 1

OS_BUILD_LAYERS: 1

VIRTUAL_MACHINE:  VMware

BUGCHECK_CODE:  d1

BUGCHECK_P1: ffffae03917c7760

BUGCHECK_P2: 2

BUGCHECK_P3: 0

BUGCHECK_P4: fffff80315431981

READ_ADDRESS:  ffffae03917c7760 Paged pool

BLACKBOXBSD: 1 (!blackboxbsd)


BLACKBOXNTFS: 1 (!blackboxntfs)


BLACKBOXWINLOGON: 1

PROCESS_NAME:  notmyfault64.exe

TRAP_FRAME:  fffff406ca7d47e0 -- (.trap 0xfffff406ca7d47e0)
NOTE: The trap frame does not contain all registers.
Some register values may be zeroed or incorrect.
rax=00000000917c6760 rbx=0000000000000000 rcx=ffffae038d200340
rdx=0000000000000890 rsi=0000000000000000 rdi=0000000000000000
rip=fffff80315431981 rsp=fffff406ca7d4970 rbp=0000000000000002
 r8=ffffae0393bb9db0  r9=0000000000000000 r10=ffffae038d2002c0
r11=ffffae03917c0750 r12=0000000000000000 r13=0000000000000000
r14=0000000000000000 r15=0000000000000000
iopl=0         nv up ei ng nz na pe nc
myfault+0x1981:
fffff803`15431981 8b03            mov     eax,dword ptr [rbx] ds:00000000`00000000=????????
Resetting default scope

STACK_TEXT:
fffff406`ca7d4698 fffff803`18609169     : 00000000`0000000a ffffae03`917c7760 00000000`00000002 00000000`00000000 : nt!KeBugCheckEx
fffff406`ca7d46a0 fffff803`18605469     : 00007ffe`4bf2cc00 00000000`00000000 00000000`00000f4d 00000000`00000000 : nt!KiBugCheckDispatch+0x69
fffff406`ca7d47e0 fffff803`15431981     : 00000000`00000000 fffff406`ca7d49c8 00000000`00000000 00000000`00000000 : nt!KiPageFault+0x469
fffff406`ca7d4970 fffff803`15431d3d     : 00000000`917c6760 00000237`89f794e0 00000000`000000f0 00000000`00000000 : myfault+0x1981
fffff406`ca7d49a0 fffff803`15431ea1     : ffffdb0d`e17fcea0 00000000`00000000 00000000`00000000 fffff803`187f5e51 : myfault+0x1d3d
fffff406`ca7d4ae0 fffff803`1848f865     : ffffdb0d`e17fcea0 00000000`00000001 fffff406`ca7d4ec0 00000000`00000001 : myfault+0x1ea1
fffff406`ca7d4b40 fffff803`18875328     : fffff406`ca7d4ec0 ffffdb0d`e17fcea0 00000000`00000001 fffff803`00000000 : nt!IofCallDriver+0x55
fffff406`ca7d4b80 fffff803`18874bf5     : 00000000`00000000 fffff406`ca7d4ec0 00000000`00000000 fffff406`ca7d4ec0 : nt!IopSynchronousServiceTail+0x1a8
fffff406`ca7d4c20 fffff803`188745f6     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : nt!IopXxxControlFile+0x5e5
fffff406`ca7d4d60 fffff803`18608bb5     : 00000000`fffffffc ffff47e9`00000000 00000000`00000001 00000237`89af8a50 : nt!NtDeviceIoControlFile+0x56
fffff406`ca7d4dd0 00007ffe`4bf2ce54     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : nt!KiSystemServiceCopyEnd+0x25
0000005b`e44fedb8 00000000`00000000     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : 0x00007ffe`4bf2ce54


SYMBOL_NAME:  myfault+1981

MODULE_NAME: myfault

IMAGE_NAME:  myfault.sys

STACK_COMMAND:  .thread ; .cxr ; kb

BUCKET_ID_FUNC_OFFSET:  1981

FAILURE_BUCKET_ID:  AV_myfault!unknown_function
```

```
OS_VERSION:  10.0.19041.1

BUILDLAB_STR:  vb_release

OSPLATFORM_TYPE:  x64

OSNAME:  Windows 10

FAILURE_ID_HASH:  {9745090a-9bce-ccba-c096-ca6e9ca04c64}

Followup:     MachineOwner
---------
```

Note: Sometimes, the output of the **!analyze -v** command depends on the current CPU.

29. If you play with hardware you can use various parameters for **!sysinfo** command:

```
1: kd> !sysinfo
!sysinfo [ cpuinfo | cpumicrocode | cpuspeed | gbl | machineid | registers | smbios ] [-csv | -
noheaders]
Latest SMBIOs support: v3.4

1: kd> !sysinfo cpuinfo
[CPU Information]
~MHz = REG_DWORD 2112
Component Information = REG_BINARY 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
Configuration Data = REG_FULL_RESOURCE_DESCRIPTOR ff,ff,ff,ff,ff,ff,ff,ff,0,0,0,0,0,0,0,0
Identifier = REG_SZ Intel64 Family 6 Model 142 Stepping 10
ProcessorNameString = REG_SZ Intel(R) Core(TM) i7-8650U CPU @ 1.90GHz
Update Status = REG_DWORD 2
VendorIdentifier = REG_SZ GenuineIntel
MSR8B = REG_QWORD ffffffff00000000

1: kd> !sysinfo machineid
Machine ID Information [From Smbios 2.7, DMIVersion 0, Size=10028]
BiosVendor = VMware, Inc.
BiosVersion = VMW71.00V.16221537.B64.2005150253
BiosReleaseDate = 05/15/2020
SystemManufacturer = VMware, Inc.
SystemProductName = VMware7,1
SystemVersion = None
BaseBoardManufacturer = Intel Corporation
BaseBoardProduct = 440BX Desktop Reference Platform
BaseBoardVersion = None
```

30. We close logging before exiting WinDbg:

```
1: kd> .logclose
Closing open log file C:\AWMDA-Dumps\Kernel\x64\MEMORY-PageFault.log
```

Note: We recommend exiting WinDbg after each exercise to avoid possible confusion and glitches.