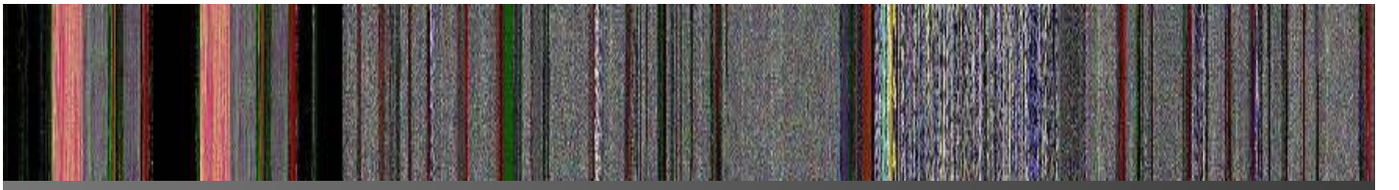


Defect
Detect

DUmps Binaries Logs INternals
School of Security

Windows Memory Dump Analysis

Advanced

with Data Structures

Version 5

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: 978-1-912636-95-2 (Paperback)

Revision 5.01 (March 2024)

Contents

Exercise C1A: Stack Trace Collection

Goal: Learn how to get stack traces related to sessions, processes, and threads; diagnose different process relationships and thread types.

Patterns: Stack Trace Collection (unmanaged space); Active Thread; Passive Thread; Coupled Processes (weak); Coupled Processes (strong); Wait Chain (ALPC); Zombie Processes; Stack Trace Collection (Predicate); Stack Trace Collection (CPUs); Input Thread; Truncated Stack Trace; Memory Data Model.

1. Launch WinDbg.

2. Open \AdvWMDA-Dumps\x64\MEMORY-Normal.DMP

3. We get the dump file loaded:

```
Microsoft (R) Windows Debugger Version 10.0.27553.1004 AMD64
Copyright (c) Microsoft Corporation. All rights reserved.


Loading Dump File [C:\AdvWMDA-Dumps\x64\MEMORY-Normal.DMP]
Kernel Bitmap Dump File: Full address space is available


************* Path validation summary **************
Response                         Time (ms)     Location
Deferred                                       srv*
Symbol search path is: srv*
Executable search path is:
Windows 10 Kernel Version 22000 MP (2 procs) Free x64
Product: WinNt, suite: TerminalServer SingleUserTS Personal
Edition build lab: 22000.1.amd64fre.co_release.210604-1628
Kernel base = 0xfffff807`62000000 PsLoadedModuleList = 0xfffff807`62c29bc0
Debug session time: Thu Feb 10 01:11:26.439 2022 (UTC + 0:00)
System Uptime: 0 days 0:07:45.422
Loading Kernel Symbols
...............................................................
...............................................................
...............................................................
..
Loading User Symbols
................................
Loading unloaded module list
........
For analysis of this file, run !analyze -v
nt!KeBugCheckEx:
fffff807`62416220 mov     qword ptr [rsp+8],rcx ss:0018:ffffa28c`9d8d8690=000000000000000a
```

4. We open a log file:

```
1: kd> .logopen C:\AdvWMDA-Dumps\x64\C1A.log
Opened log file 'C:\AdvWMDA-Dumps\x64\C1A.log'
```

5. We list running sessions:

```
1: kd> !session
unable to get nt!PspSessionIdBitmap
Sessions on machine: 2
Valid Sessions: 0 1
Current Session 1
```

Note: The error in gray color wasn't available in the previous versions of WinDbg and can be ignored.

6. We check the current process:

```
1: kd> !process
PROCESS ffffbe0c8c2cd0c0
    SessionId: 1  Cid: 243c    Peb: 34f5f83000  ParentCid: 1070
    DirBase: 12ea72002  ObjectTable: ffff800edff979c0  HandleCount: 176.
    Image: notmyfault64.exe
    VadRoot ffffbe0c8c233dc0 Vads 83 Clone 0 Private 428. Modified 15. Locked 0.
    DeviceMap ffff800eda519d60
    Token                             ffff800ee01df060
    ElapsedTime                       00:00:19.477
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         194192
    QuotaPoolUsage[NonPagedPool]      11616
    Working Set Sizes (now,min,max)  (3317, 50, 345) (13268KB, 200KB, 1380KB)
    PeakWorkingSetSize                3240
    VirtualSize                       4234 Mb
    PeakVirtualSize                   4250 Mb
    PageFaultCount                    3390
    MemoryPriority                    FOREGROUND
    BasePriority                      8
    CommitCharge                      475
    Job                               ffffbe0c8a7a36b0

        THREAD ffffbe0c8974f080  Cid 243c.1938  Teb: 00000034f5f84000 Win32Thread: ffffbe0c8cccb2a0 RUNNING on processor 1
        THREAD ffffbe0c8b5e0080  Cid 243c.24a8  Teb: 00000034f5f86000 Win32Thread: 0000000000000000 WAIT: (WrQueue) UserMode Alertable
            ffffbe0c8b617400  QueueObject

        THREAD ffffbe0c8be7c080  Cid 243c.2484  Teb: 00000034f5f88000 Win32Thread: 0000000000000000 WAIT: (WrQueue) UserMode Alertable
            ffffbe0c8b617400  QueueObject
```

Note: We used the *NotMyFault* tool to force a complete memory dump:

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

7. We set the current session to 0 and examine its implicit process:

```
1: kd> !session -s 0
Sessions on machine: 2
Implicit process is now ffffbe0c`87f2b080
Using session 0l
```

```
1: kd> !process ffffbe0c`87f2b080 3f
PROCESS ffffbe0c87f2b080
    SessionId: 0  Cid: 01fc    Peb: 3901e58000  ParentCid: 01f0
    DirBase: 01932002  ObjectTable: ffff800ed7355c00  HandleCount: 537.
    Image: csrss.exe
    VadRoot ffffbe0c897bf550 Vads 164 Clone 0 Private 277. Modified 258. Locked 0.
    DeviceMap ffff800ed4822520
    Token                             ffff800ed73f8060
    ElapsedTime                       00:07:13.525
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.468
    QuotaPoolUsage[PagedPool]         239472
    QuotaPoolUsage[NonPagedPool]      23032
    Working Set Sizes (now,min,max)  (1369, 50, 345) (5476KB, 200KB, 1380KB)
    PeakWorkingSetSize                1469
    VirtualSize                       2101339 Mb
    PeakVirtualSize                   2101340 Mb
    PageFaultCount                    2742
    MemoryPriority                    BACKGROUND
    BasePriority                      13
```

```
    CommitCharge                    485

    PEB at 0000003901e58000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00007ff6d7380000
    NtGlobalFlag:             400
    NtGlobalFlag2:            0
    Ldr                       00007ffe5b0fa120
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 0000015013a03e70 . 0000015013a2b560
    Ldr.InLoadOrderModuleList:           0000015013a04000 . 0000015013a2b540
    Ldr.InMemoryOrderModuleList:         0000015013a04010 . 0000015013a2b550
                    Base TimeStamp                     Module
            7ff6d7380000 064903e5 May 05 12:13:41 1973 C:\WINDOWS\system32\csrss.exe
            7ffe5af80000 931cda92 Mar 18 10:55:14 2048 C:\WINDOWS\SYSTEM32\ntdll.dll
            7ffe58450000 51a03181 May 25 04:35:29 2013 C:\WINDOWS\SYSTEM32\CSRSRV.dll
            7ffe58430000 d987e1f9 Aug 25 07:58:01 2085 C:\WINDOWS\system32\basesrv.DLL
            7ffe58410000 ec122896 Jul 04 11:16:54 2095 C:\WINDOWS\system32\winsrv.DLL
            7ffe58a00000 72a6f702 Dec 15 06:00:34 2030 C:\WINDOWS\System32\kernelbase.dll
            7ffe5a2c0000 7b65e245 Aug 09 13:17:09 2035 C:\WINDOWS\System32\kernel32.dll
            7ffe583e0000 864193e6 May 18 00:04:06 2041 C:\WINDOWS\SYSTEM32\winsrvext.dll
            7ffe58d80000 2eab7211 Oct 24 09:36:33 1994 C:\WINDOWS\System32\win32u.dll
            7ffe58e20000 0b2998f3 Dec 08 12:58:27 1975 C:\WINDOWS\System32\GDI32.dll
            7ffe588e0000 f03395da Sep 13 13:08:58 2097 C:\WINDOWS\System32\gdi32full.dll
            7ffe58610000 1fb7fd57 Nov 12 03:53:59 1986 C:\WINDOWS\System32\msvcp_win.dll
            7ffe584f0000 00e78ce9 Jun 25 16:14:49 1970 C:\WINDOWS\System32\ucrtbase.dll
            7ffe59000000 95c2e8f0 Aug 14 19:33:20 2049 C:\WINDOWS\System32\USER32.dll
            7ffe583d0000 203620ec Feb 15 20:11:24 1987 C:\WINDOWS\system32\sxssrv.DLL
            7ffe582e0000 a2eb73f0 Aug 12 22:00:32 2056 C:\WINDOWS\system32\sxs.dll
            7ffe5a210000 ce622c7b Sep 21 17:46:51 2079 C:\WINDOWS\System32\ADVAPI32.dll
            7ffe5a160000 90483ed2 Sep 15 20:49:38 2046 C:\WINDOWS\System32\msvcrt.dll
            7ffe5ad10000 31ec7be5 Jul 17 06:36:37 1996 C:\WINDOWS\System32\sechost.dll
            7ffe596c0000 7ff0ec4a Jan 07 16:46:02 2038 C:\WINDOWS\System32\RPCRT4.dll
            7ffe581f0000 7ac2022e Apr 07 06:01:34 2035 C:\WINDOWS\system32\ServicingCommon.dll
            7ffe58470000 a34302f0 Oct 18 07:57:52 2056 C:\WINDOWS\System32\bcryptPrimitives.dll
    SubSystemData:     0000000000000000
    ProcessHeap:       0000015013890000
    ProcessParameters: 0000015013a034f0
    CurrentDirectory:  'C:\WINDOWS\system32\'
    WindowTitle:  '< Name not readable >'
    ImageFile:    'C:\WINDOWS\system32\csrss.exe'
    CommandLine:  '%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows
ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16'
    DllPath:      '< Name not readable >'
    Environment:  0000015013a02a00
        ComSpec=C:\WINDOWS\system32\cmd.exe
        DriverData=C:\Windows\System32\Drivers\DriverData
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT

Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\WINDOWS\System32\WindowsPowerShell\v1.0\;C:\WINDOWS\System32\OpenSSH\;C:\Program
Files\dotnet\;C:\Program Files (x86)\dotnet\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 142 Stepping 10, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=8e0a
        PSModulePath=%ProgramFiles%\WindowsPowerShell\Modules;C:\WINDOWS\system32\WindowsPowerShell\v1.0\Modules
        SystemDrive=C:
        SystemRoot=C:\WINDOWS
        TEMP=C:\WINDOWS\TEMP
        TMP=C:\WINDOWS\TEMP
        USERNAME=SYSTEM
        windir=C:\WINDOWS


        THREAD ffffbe0c87d1a580  Cid 01fc.020c  Teb: 0000003901e5f000 Win32Thread: ffffbe0c87ff3c50 WAIT: (WrLpcReceive) UserMode Non-Alertable
            ffffbe0c87d1aa58  Semaphore Limit 0x1
        Not impersonating
        DeviceMap                 ffff800ed4822520
        Owning Process            ffffbe0c87f2b080       Image:         csrss.exe
        Attached Process          N/A            Image:         N/A
        Wait Start TickCount      29729          Ticks: 58 (0:00:00:00.906)
        Context Switch Count      817            IdealProcessor: 0
        UserTime                  00:00:00.000
        KernelTime                00:00:00.156
        Win32 Start Address CSRSRV!CsrApiRequestThread (0x00007ffe58451820)
        Stack Init ffffa28c9cfa1c70 Current ffffa28c9cfa13d0
        Base ffffa28c9cfa2000 Limit ffffa28c9cf9c000 Call 0000000000000000
        Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
Unable to load image \??\C:\WINDOWS\system32\drivers\myfault.sys, Win32 error 0n2
        Child-SP          RetAddr               Call Site
        ffffa28c`9cfa1410 fffff807`623327f7     nt!KiSwapContext+0x76
        ffffa28c`9cfa1550 fffff807`623346a9     nt!KiSwapThread+0x3a7
        ffffa28c`9cfa1630 fffff807`6232e5c4     nt!KiCommitThreadWait+0x159
        ffffa28c`9cfa16d0 fffff807`6222fdc6     nt!KeWaitForSingleObject+0x234
        ffffa28c`9cfa17c0 fffff807`6268caf0     nt!AlpcpWaitForSingleObject+0x3e
        ffffa28c`9cfa1800 fffff807`6274caad     nt!AlpcpCompleteDeferSignalRequestAndWait+0x3c
        ffffa28c`9cfa1840 fffff807`6274d4d3     nt!AlpcpReceiveMessagePort+0x3ad
        ffffa28c`9cfa18d0 fffff807`6274d01e     nt!AlpcpReceiveMessage+0x333
        ffffa28c`9cfa19b0 fffff807`62428775     nt!NtAlpcSendWaitReceivePort+0xfe
```

```
ffffa28c`9cfa1a70 00007ffe`5b0248c4     nt!KiSystemServiceCopyEnd+0x25 (TrapFrame @ ffffa28c`9cfa1ae0)
00000039`01d7f7f8 00007ffe`58451926     ntdll!NtAlpcSendWaitReceivePort+0x14
00000039`01d7f800 00007ffe`5af84873     CSRSRV!CsrApiRequestThread+0x106
00000039`01d7fea0 00000000`00000000     ntdll!RtlUserThreadStart+0x43

THREAD ffffbe0c887d60c0  Cid 01fc.0228  Teb: 0000003901e63000 Win32Thread: ffffbe0c8a6f1b20 WAIT: (WrLpcReply) UserMode Non-Alertable
    ffffbe0c887d6598  Semaphore Limit 0x1
Waiting for reply to ALPC Message ffff800ed83f7a50 : queued at port ffffbe0c89022b20 : owned by process ffffbe0c891020c0
Not impersonating
DeviceMap                 ffff800ed4822520
Owning Process            ffffbe0c87f2b080       Image:         csrss.exe
Attached Process          N/A            Image:         N/A
Wait Start TickCount      4008           Ticks: 25779 (0:00:06:42.796)
Context Switch Count      8              IdealProcessor: 0
UserTime                  00:00:00.000
KernelTime                00:00:00.015
Win32 Start Address winsrvext!TerminalServerRequestThread (0x00007ffe583ee680)
Stack Init ffffa28c9cfeec70 Current ffffa28c9cfee3b0
Base ffffa28c9cfef000 Limit ffffa28c9cfe9000 Call 0000000000000000
Priority 15 BasePriority 15 PriorityDecrement 0 IoPriority 2 PagePriority 5
Child-SP          RetAddr               Call Site
ffffa28c`9cfee3f0 fffff807`623327f7     nt!KiSwapContext+0x76
ffffa28c`9cfee530 fffff807`623346a9     nt!KiSwapThread+0x3a7
ffffa28c`9cfee610 fffff807`6232e5c4     nt!KiCommitThreadWait+0x159
ffffa28c`9cfee6b0 fffff807`622c45ed     nt!KeWaitForSingleObject+0x234
ffffa28c`9cfee7a0 fffff807`6274e0c6     nt!AlpcpSignalAndWait+0x13d
ffffa28c`9cfee830 fffff807`6274dc1f     nt!AlpcpReceiveSynchronousReply+0x56
ffffa28c`9cfee890 fffff807`6274d0f6     nt!AlpcpProcessSynchronousRequest+0x36f
ffffa28c`9cfee9b0 fffff807`62428775     nt!NtAlpcSendWaitReceivePort+0x1d6
ffffa28c`9cfeea70 00007ffe`5b0248c4     nt!KiSystemServiceCopyEnd+0x25 (TrapFrame @ ffffa28c`9cfeeae0)
00000039`01dff958 00007ffe`583ee984     ntdll!NtAlpcSendWaitReceivePort+0x14
00000039`01dff960 00007ffe`5af84873     winsrvext!TerminalServerRequestThread+0x304
00000039`01dffac0 00000000`00000000     ntdll!RtlUserThreadStart+0x43

THREAD ffffbe0c888020c0  Cid 01fc.0230  Teb: 0000003901e67000 Win32Thread: 0000000000000000 WAIT: (UserRequest) UserMode Alertable
    ffffbe0c87c87be0  SynchronizationEvent
    ffffbe0c87c87ae0  SynchronizationEvent
    ffffbe0c84db6ee0  SynchronizationEvent
Not impersonating
DeviceMap                 ffff800ed4822520
Owning Process            ffffbe0c87f2b080       Image:         csrss.exe
Attached Process          N/A            Image:         N/A
Wait Start TickCount      2076           Ticks: 27711 (0:00:07:12.984)
Context Switch Count      4              IdealProcessor: 0
UserTime                  00:00:00.000
KernelTime                00:00:00.000
Win32 Start Address winsrvext!NotificationThread (0x00007ffe583e3430)
Stack Init ffffa28c9cffcc70 Current ffffa28c9cffbee0
Base ffffa28c9cffd000 Limit ffffa28c9cff7000 Call 0000000000000000
Priority 3 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
Kernel stack not resident.

THREAD ffffbe0c888130c0  Cid 01fc.0234  Teb: 0000003901e69000 Win32Thread: 0000000000000000 WAIT: (UserRequest) UserMode Alertable
    ffffbe0c87c879e0  SynchronizationEvent
Not impersonating
DeviceMap                 ffff800ed4822520
Owning Process            ffffbe0c87f2b080       Image:         csrss.exe
Attached Process          N/A            Image:         N/A
Wait Start TickCount      2076           Ticks: 27711 (0:00:07:12.984)
Context Switch Count      2              IdealProcessor: 1
UserTime                  00:00:00.000
KernelTime                00:00:00.000
Win32 Start Address winsrvext!PowerNotificationThread (0x00007ffe583e3950)
Stack Init ffffa28c9ca97c70 Current ffffa28c9ca97650
Base ffffa28c9ca98000 Limit ffffa28c9ca92000 Call 0000000000000000
Priority 15 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
Kernel stack not resident.

THREAD ffffbe0c87efb080  Cid 01fc.0238  Teb: 0000003901e6b000 Win32Thread: 0000000000000000 WAIT: (WrLpcReceive) UserMode Non-Alertable
    ffffbe0c87efb558  Semaphore Limit 0x1
Not impersonating
DeviceMap                 ffff800ed4822520
Owning Process            ffffbe0c87f2b080       Image:         csrss.exe
Attached Process          N/A            Image:         N/A
Wait Start TickCount      2077           Ticks: 27710 (0:00:07:12.968)
Context Switch Count      3              IdealProcessor: 0
UserTime                  00:00:00.000
KernelTime                00:00:00.000
Win32 Start Address CSRSRV!CsrSbApiRequestThread (0x00007ffe584574b0)
Stack Init ffffa28c9cdf7c70 Current ffffa28c9cdf7410
Base ffffa28c9cdf8000 Limit ffffa28c9cdf2000 Call 0000000000000000
Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
Kernel stack not resident.

THREAD ffffbe0c88893080  Cid 01fc.0268  Teb: 0000003901e6d000 Win32Thread: ffffbe0c87ff5eb0 WAIT: (WrLpcReceive) UserMode Non-Alertable
    ffffbe0c88893558  Semaphore Limit 0x1
Not impersonating
DeviceMap                 ffff800ed4822520
Owning Process            ffffbe0c87f2b080       Image:         csrss.exe
Attached Process          N/A            Image:         N/A
Wait Start TickCount      29374          Ticks: 413 (0:00:00:06.453)
Context Switch Count      952            IdealProcessor: 1
UserTime                  00:00:00.031
```

```
    KernelTime               00:00:00.062
    Win32 Start Address CSRSRV!CsrApiRequestThread (0x00007ffe58451820)
    Stack Init ffffa28c9ce3ec70 Current ffffa28c9ce3e3d0
    Base ffffa28c9ce3f000 Limit ffffa28c9ce39000 Call 0000000000000000
    Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
    Child-SP          RetAddr               Call Site
    ffffa28c`9ce3e410 fffff807`623327f7     nt!KiSwapContext+0x76
    ffffa28c`9ce3e550 fffff807`623346a9     nt!KiSwapThread+0x3a7
    ffffa28c`9ce3e630 fffff807`6232e5c4     nt!KiCommitThreadWait+0x159
    ffffa28c`9ce3e6d0 fffff807`6222fdc6     nt!KeWaitForSingleObject+0x234
    ffffa28c`9ce3e7c0 fffff807`6268caf0     nt!AlpcpWaitForSingleObject+0x3e
    ffffa28c`9ce3e800 fffff807`6274caad     nt!AlpcpCompleteDeferSignalRequestAndWait+0x3c
    ffffa28c`9ce3e840 fffff807`6274d4d3     nt!AlpcpReceiveMessagePort+0x3ad
    ffffa28c`9ce3e8d0 fffff807`6274d01e     nt!AlpcpReceiveMessage+0x333
    ffffa28c`9ce3e9b0 fffff807`62428775     nt!NtAlpcSendWaitReceivePort+0xfe
    ffffa28c`9ce3ea70 00007ffe`5b0248c4     nt!KiSystemServiceCopyEnd+0x25 (TrapFrame @ ffffa28c`9ce3eae0)
    00000039`01cbf518 00007ffe`58451926     ntdll!NtAlpcSendWaitReceivePort+0x14
    00000039`01cbf520 00007ffe`5af84873     CSRSRV!CsrApiRequestThread+0x106
    00000039`01cbfbc0 00000000`00000000     ntdll!RtlUserThreadStart+0x43

    THREAD ffffbe0c888b4080  Cid 01fc.0278  Teb: 0000003901e6f000 Win32Thread: ffffbe0c87ff5140 WAIT: (WrUserRequest) KernelMode Non-Alertable
        ffffbe0c87447b40  QueueObject
        ffffbe0c87ff54b0  NotificationTimer
        ffffbe0c87ff5820  SynchronizationTimer
        ffffbe0c87ca65c0  SynchronizationEvent
        fffff80762c23960  NotificationEvent
        ffffbe0c886fd7e0  SynchronizationEvent
        ffffbe0c886fd8e0  Semaphore Limit 0x7fffffff
        ffffbe0c886fd0e0  SynchronizationEvent
        ffffbe0c887fd340  SynchronizationTimer
        ffffbe0c886fdce0  SynchronizationEvent
        ffffbe0c886fd960  SynchronizationEvent
        ffffbe0c886fde60  SynchronizationEvent
        ffffbe0c886fdee0  SynchronizationEvent
        ffffbe0c886fd5e0  Semaphore Limit 0x7fffffff
        ffffbe0c886fd260  SynchronizationEvent
        ffffbe0c887fe270  SynchronizationTimer
        ffffbe0c887ff350  SynchronizationTimer
        ffffbe0c887fc0b0  SynchronizationTimer
        ffffbe0c887fc260  SynchronizationTimer
        ffffbe0c887fda00  SynchronizationTimer
        ffffbe0c886fdc60  SynchronizationEvent
        ffffbe0c886fda60  SynchronizationEvent
        ffffbe0c886fd160  SynchronizationEvent
        ffffbe0c886fdfe0  SynchronizationEvent
        ffffbe0c886fd860  SynchronizationEvent
        ffffbe0c886fe060  SynchronizationEvent
    Not impersonating
    DeviceMap                 ffff800ed4822520
    Owning Process            ffffbe0c87f2b080       Image:         csrss.exe
    Attached Process          N/A            Image:         N/A
    Wait Start TickCount      29701          Ticks: 86 (0:00:00:01.343)
    Context Switch Count      126            IdealProcessor: 0
    UserTime                  00:00:00.000
    KernelTime                00:00:00.000
    Win32 Start Address winsrvext!StartCreateSystemThreads (0x00007ffe583e3fc0)
    Stack Init ffffa28c9ce5ac70 Current ffffa28c9ce5a250
    Base ffffa28c9ce5b000 Limit ffffa28c9ce55000 Call 0000000000000000
    Priority 16 BasePriority 16 PriorityDecrement 0 IoPriority 2 PagePriority 5
    Child-SP          RetAddr               Call Site
    ffffa28c`9ce5a290 fffff807`623327f7     nt!KiSwapContext+0x76
    ffffa28c`9ce5a3d0 fffff807`623346a9     nt!KiSwapThread+0x3a7
    ffffa28c`9ce5a4b0 fffff807`6228ed51     nt!KiCommitThreadWait+0x159
    ffffa28c`9ce5a550 ffffbc92`8e121ec5     nt!KeWaitForMultipleObjects+0x2b1
    ffffa28c`9ce5a650 ffffbc92`8e7a4576     win32kbase!LegacyInputDispatcher::WaitAndDispatch+0x95
    ffffa28c`9ce5a720 ffffbc92`8e192904     win32kfull!RawInputThread+0x796
    ffffa28c`9ce5a890 ffffbc92`8e192684     win32kbase!xxxCreateSystemThreads+0x214
    ffffa28c`9ce5a9b0 ffffbc92`8dc4a612     win32kbase!NtUserCreateSystemThreads+0x144
    ffffa28c`9ce5aab0 fffff807`62428775     win32k!NtUserCreateSystemThreads+0x16
    ffffa28c`9ce5aae0 00007ffe`58d88cd4     nt!KiSystemServiceCopyEnd+0x25 (TrapFrame @ ffffa28c`9ce5aae0)
    00000039`0213fdf8 00007ffe`583e3fdc     win32u!NtUserCreateSystemThreads+0x14
    00000039`0213fe00 00007ffe`5af84873     winsrvext!StartCreateSystemThreads+0x1c
    00000039`0213fe30 00000000`00000000     ntdll!RtlUserThreadStart+0x43

    THREAD ffffbe0c888b6080  Cid 01fc.027c  Teb: 0000003901e71000 Win32Thread: ffffbe0c87ff5320 WAIT: (WrUserRequest) UserMode Non-Alertable
        ffffbe0c87ca68c0  SynchronizationEvent
        ffffbe0c87ca79d0  SynchronizationEvent
        ffffbe0c87447700  QueueObject
    Not impersonating
    DeviceMap                 ffff800ed4822520
    Owning Process            ffffbe0c87f2b080       Image:         csrss.exe
    Attached Process          N/A            Image:         N/A
    Wait Start TickCount      3863           Ticks: 25924 (0:00:06:45.062)
    Context Switch Count      83             IdealProcessor: 1
    UserTime                  00:00:00.000
    KernelTime                00:00:00.015
    Win32 Start Address winsrvext!StartCreateSystemThreads (0x00007ffe583e3fc0)
    Stack Init ffffa28c9ce61c70 Current ffffa28c9ce61260
    Base ffffa28c9ce62000 Limit ffffa28c9ce5c000 Call 0000000000000000
    Priority 16 BasePriority 16 PriorityDecrement 0 IoPriority 2 PagePriority 5
    Child-SP          RetAddr               Call Site
    ffffa28c`9ce612a0 fffff807`623327f7     nt!KiSwapContext+0x76
    ffffa28c`9ce613e0 fffff807`623346a9     nt!KiSwapThread+0x3a7
```

```
ffffa28c`9ce614c0 fffff807`6228ed51     nt!KiCommitThreadWait+0x159
ffffa28c`9ce61560 ffffbc92`8e121ec5     nt!KeWaitForMultipleObjects+0x2b1
ffffa28c`9ce61660 ffffbc92`8e6f15b4     win32kbase!LegacyInputDispatcher::WaitAndDispatch+0x95
ffffa28c`9ce61730 ffffbc92`8e6f1349     win32kfull!xxxDesktopThreadWaiter+0xe0
ffffa28c`9ce617a0 ffffbc92`8e192904     win32kfull!xxxDesktopThread+0x359
ffffa28c`9ce61890 ffffbc92`8e192684     win32kbase!xxxCreateSystemThreads+0x214
ffffa28c`9ce619b0 ffffbc92`8dc4a612     win32kbase!NtUserCreateSystemThreads+0x144
ffffa28c`9ce61ab0 fffff807`62428775     win32k!NtUserCreateSystemThreads+0x16
ffffa28c`9ce61ae0 00007ffe`58d88cd4     nt!KiSystemServiceCopyEnd+0x25 (TrapFrame @ ffffa28c`9ce61ae0)
00000039`0217fe48 00007ffe`583e3fdc     win32u!NtUserCreateSystemThreads+0x14
00000039`0217fe50 00007ffe`5af84873     winsrvext!StartCreateSystemThreads+0x1c
00000039`0217fe80 00000000`00000000     ntdll!RtlUserThreadStart+0x43

THREAD ffffbe0c889c8040  Cid 01fc.03a0  Teb: 0000003901e73000 Win32Thread: ffffbe0c888fce20 WAIT: (WrQueue) UserMode Alertable
    ffffbe0c87e707c0  QueueObject
Not impersonating
DeviceMap                 ffff800ed4822520
Owning Process            ffffbe0c87f2b080       Image:         csrss.exe
Attached Process          N/A            Image:         N/A
Wait Start TickCount      2843           Ticks: 26944 (0:00:07:01.000)
Context Switch Count      16             IdealProcessor: 0
UserTime                  00:00:00.015
KernelTime                00:00:00.000
Win32 Start Address ntdll!TppWorkerThread (0x00007ffe5af96950)
Stack Init ffffa28c9d110c70 Current ffffa28c9d110360
Base ffffa28c9d111000 Limit ffffa28c9d10b000 Call 0000000000000000
Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
Kernel stack not resident.

THREAD ffffbe0c890b6080  Cid 01fc.0008  Teb: 0000003901e75000 Win32Thread: ffffbe0c89097980 WAIT: (WrUserRequest) UserMode Non-Alertable
    ffffbe0c890b0c40  QueueObject
Not impersonating
DeviceMap                 ffff800ed4822520
Owning Process            ffffbe0c87f2b080       Image:         csrss.exe
Attached Process          N/A            Image:         N/A
Wait Start TickCount      2578           Ticks: 27209 (0:00:07:05.140)
Context Switch Count      5              IdealProcessor: 1
UserTime                  00:00:00.000
KernelTime                00:00:00.000
Win32 Start Address winsrvext!StartCreateSystemThreads (0x00007ffe583e3fc0)
Stack Init ffffa28c9d1cdc70 Current ffffa28c9d1cd170
Base ffffa28c9d1ce000 Limit ffffa28c9d1c8000 Call 0000000000000000
Priority 14 BasePriority 12 PriorityDecrement 0 IoPriority 2 PagePriority 5
Kernel stack not resident.

THREAD ffffbe0c89a9a080  Cid 01fc.0cd0  Teb: 0000003901e77000 Win32Thread: ffffbe0c898d7b60 WAIT: (WrLpcReceive) UserMode Non-Alertable
    ffffbe0c89a9a558  Semaphore Limit 0x1
Not impersonating
DeviceMap                 ffff800ed4822520
Owning Process            ffffbe0c87f2b080       Image:         csrss.exe
Attached Process          N/A            Image:         N/A
Wait Start TickCount      29353          Ticks: 434 (0:00:00:06.781)
Context Switch Count      670            IdealProcessor: 0
UserTime                  00:00:00.031
KernelTime                00:00:00.015
Win32 Start Address CSRSRV!CsrApiRequestThread (0x00007ffe58451820)
Stack Init ffffa28c9e030c70 Current ffffa28c9e0303d0
Base ffffa28c9e031000 Limit ffffa28c9e02b000 Call 0000000000000000
Priority 14 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
Child-SP          RetAddr               Call Site
ffffa28c`9e030410 fffff807`623327f7     nt!KiSwapContext+0x76
ffffa28c`9e030550 fffff807`623346a9     nt!KiSwapThread+0x3a7
ffffa28c`9e030630 fffff807`6232e5c4     nt!KiCommitThreadWait+0x159
ffffa28c`9e0306d0 fffff807`6222fdc6     nt!KeWaitForSingleObject+0x234
ffffa28c`9e0307c0 fffff807`6268caf0     nt!AlpcpWaitForSingleObject+0x3e
ffffa28c`9e030800 fffff807`6274caad     nt!AlpcpCompleteDeferSignalRequestAndWait+0x3c
ffffa28c`9e030840 fffff807`6274d4d3     nt!AlpcpReceiveMessagePort+0x3ad
ffffa28c`9e0308d0 fffff807`6274d01e     nt!AlpcpReceiveMessage+0x333
ffffa28c`9e0309b0 fffff807`62428775     nt!NtAlpcSendWaitReceivePort+0xfe
ffffa28c`9e030a70 00007ffe`5b0248c4     nt!KiSystemServiceCopyEnd+0x25 (TrapFrame @ ffffa28c`9e030ae0)
00000039`0203f288 00007ffe`58451926     ntdll!NtAlpcSendWaitReceivePort+0x14
00000039`0203f290 00007ffe`5af84873     CSRSRV!CsrApiRequestThread+0x106
00000039`0203f930 00000000`00000000     ntdll!RtlUserThreadStart+0x43

THREAD ffffbe0c89fb6040  Cid 01fc.10ac  Teb: 0000003901e79000 Win32Thread: ffffbe0c8a6fa400 WAIT: (WrQueue) UserMode Alertable
    ffffbe0c87e707c0  QueueObject
Not impersonating
DeviceMap                 ffff800ed4822520
Owning Process            ffffbe0c87f2b080       Image:         csrss.exe
Attached Process          N/A            Image:         N/A
Wait Start TickCount      4270           Ticks: 25517 (0:00:06:38.703)
Context Switch Count      17             IdealProcessor: 1
UserTime                  00:00:00.000
KernelTime                00:00:00.000
Win32 Start Address ntdll!TppWorkerThread (0x00007ffe5af96950)
Stack Init ffffa28c9e60dc70 Current ffffa28c9e60d360
Base ffffa28c9e60e000 Limit ffffa28c9e608000 Call 0000000000000000
Priority 15 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
Child-SP          RetAddr               Call Site
ffffa28c`9e60d3a0 fffff807`623327f7     nt!KiSwapContext+0x76
ffffa28c`9e60d4e0 fffff807`623346a9     nt!KiSwapThread+0x3a7
ffffa28c`9e60d5c0 fffff807`62337106     nt!KiCommitThreadWait+0x159
ffffa28c`9e60d660 fffff807`62336b18     nt!KeRemoveQueueEx+0x2b6
```

```
ffffa28c`9e60d710 fffff807`6233937c     nt!IoRemoveIoCompletion+0x98
ffffa28c`9e60d830 fffff807`62428775     nt!NtWaitForWorkViaWorkerFactory+0x39c
ffffa28c`9e60da70 00007ffe`5b027304     nt!KiSystemServiceCopyEnd+0x25 (TrapFrame @ ffffa28c`9e60dae0)
00000039`0223f848 00007ffe`5af96c2f     ntdll!NtWaitForWorkViaWorkerFactory+0x14
00000039`0223f850 00007ffe`5af84873     ntdll!TppWorkerThread+0x2df
00000039`0223fb40 00000000`00000000     ntdll!RtlUserThreadStart+0x43

THREAD ffffbe0c8bfbc040  Cid 01fc.26d8  Teb: 0000003901e7d000 Win32Thread: 0000000000000000 WAIT: (WrQueue) UserMode Alertable
    ffffbe0c87e71780  QueueObject
Not impersonating
DeviceMap                 ffff800ed4822520
Owning Process            ffffbe0c87f2b080       Image:         csrss.exe
Attached Process          N/A            Image:         N/A
Wait Start TickCount      28424          Ticks: 1363 (0:00:00:21.296)
Context Switch Count      4              IdealProcessor: 1
UserTime                  00:00:00.000
KernelTime                00:00:00.000
Win32 Start Address ntdll!TppWorkerThread (0x00007ffe5af96950)
Stack Init ffffa28ca0317c70 Current ffffa28ca0317360
Base ffffa28ca0318000 Limit ffffa28ca0312000 Call 0000000000000000
Priority 13 BasePriority 13 PriorityDecrement 0 IoPriority 2 PagePriority 5
Child-SP          RetAddr               Call Site
ffffa28c`a03173a0 fffff807`623327f7     nt!KiSwapContext+0x76
ffffa28c`a03174e0 fffff807`623346a9     nt!KiSwapThread+0x3a7
ffffa28c`a03175c0 fffff807`62337106     nt!KiCommitThreadWait+0x159
ffffa28c`a0317660 fffff807`62336b18     nt!KeRemoveQueueEx+0x2b6
ffffa28c`a0317710 fffff807`6233937c     nt!IoRemoveIoCompletion+0x98
ffffa28c`a0317830 fffff807`62428775     nt!NtWaitForWorkViaWorkerFactory+0x39c
ffffa28c`a0317a70 00007ffe`5b027304     nt!KiSystemServiceCopyEnd+0x25 (TrapFrame @ ffffa28c`a0317ae0)
00000039`01cffc58 00007ffe`5af96c2f     ntdll!NtWaitForWorkViaWorkerFactory+0x14
00000039`01cffc60 00007ffe`5af84873     ntdll!TppWorkerThread+0x2df
00000039`01cfff50 00000000`00000000     ntdll!RtlUserThreadStart+0x43
```

Note: We see that the current process has changed. We specified **3f** flags to have the process context changed to that of *csrss.exe* during the execution of the **!process** command. We also notice passive threads waiting for ALPC notification, for example, **ffffbe0c87d1a580** (weakly coupled processes) and **ffffbe0c887d60c0** thread waiting for ALPC request reply from *svchost.exe* process (strongly coupled processes):

```
1: kd> !alpc /m ffff800ed83f7a50
Invalid reserved message id 0xffff800ed83f7a50
```

Note: The previous versions of WinDbg showed this (you can also use classic WinDbg), and we could check the thread:

```
1: kd> !alpc /m ffff800ed83f7a50

Message ffff800ed83f7a50
  MessageID              : 0x0008 (8)
  CallbackID             : 0x0339 (825)
  SequenceNumber         : 0x00000003 (3)
  Type                   : LPC_REQUEST
  DataLength             : 0x4048 (16456)
  TotalLength            : 0x4070 (16496)
  Canceled               : No
  Release                : No
  ReplyWaitReply         : No
  Continuation           : Yes
  OwnerPort              : ffffbe0c89115d60 [ALPC_CLIENT_COMMUNICATION_PORT]
  WaitingThread          : ffffbe0c887d60c0
  QueueType              : ALPC_MSGQUEUE_PENDING
  QueuePort              : ffffbe0c89022b20 [ALPC_CONNECTION_PORT]
  QueuePortOwnerProcess : ffffbe0c891020c0 (svchost.exe)
  ServerThread           : ffffbe0c89111080
  QuotaCharged           : Yes
  CancelQueuePort        : 0000000000000000
  CancelSequencePort     : 0000000000000000
  CancelSequenceNumber   : 0x00000000 (0)
  ClientContext          : 0000000000000000
```

```
  ServerContext          : 0000000000000000
  PortContext            : 0000029537e331f0
  CancelPortContext      : 0000000000000000
  SecurityData           : 0000000000000000
  View                   : 0000000000000000
  HandleData             : 0000000000000000
```

```
1: kd> !thread ffffbe0c89111080 3f
THREAD ffffbe0c89111080  Cid 01b4.0240  Teb: 000000e56c471000 Win32Thread: 0000000000000000 WAIT:
(WrQueue) UserMode Alertable
    ffffbe0c890b3c40  QueueObject
Not impersonating
DeviceMap                 ffff800ed4822520
Owning Process            ffffbe0c891020c0       Image:         svchost.exe
Attached Process          N/A            Image:         N/A
Wait Start TickCount      26624          Ticks: 3163 (0:00:00:49.421)
Context Switch Count      1227           IdealProcessor: 0
UserTime                  00:00:00.062
KernelTime                00:00:00.062
Win32 Start Address ntdll!TppWorkerThread (0x00007ffe5af96950)
Stack Init ffffa28c9d230c70 Current ffffa28c9d230360
Base ffffa28c9d231000 Limit ffffa28c9d22b000 Call 0000000000000000
Priority 11 BasePriority 8 PriorityDecrement 48 IoPriority 2 PagePriority 5
Child-SP          RetAddr               Call Site
ffffa28c`9d2303a0 fffff807`623327f7     nt!KiSwapContext+0x76
ffffa28c`9d2304e0 fffff807`623346a9     nt!KiSwapThread+0x3a7
ffffa28c`9d2305c0 fffff807`62337106     nt!KiCommitThreadWait+0x159
ffffa28c`9d230660 fffff807`62336b18     nt!KeRemoveQueueEx+0x2b6
ffffa28c`9d230710 fffff807`6233937c     nt!IoRemoveIoCompletion+0x98
ffffa28c`9d230830 fffff807`62428775     nt!NtWaitForWorkViaWorkerFactory+0x39c
ffffa28c`9d230a70 00007ffe`5b027304     nt!KiSystemServiceCopyEnd+0x25 (TrapFrame @ ffffa28c`9d230ae0)
000000e5`6c8ff9a8 00007ffe`5af96c2f     ntdll!NtWaitForWorkViaWorkerFactory+0x14
000000e5`6c8ff9b0 00007ffe`5a2d54e0     ntdll!TppWorkerThread+0x2df
000000e5`6c8ffca0 00007ffe`5af8485b     KERNEL32!BaseThreadInitThunk+0x10
000000e5`6c8ffcd0 00000000`00000000     ntdll!RtlUserThreadStart+0x2b
```

Note: You can also use the port option instead of the message:

```
1: kd> !alpc /p ffffbe0c89022b20
```

```
Port ffffbe0c89022b20
  Type                      : ALPC_CONNECTION_PORT
  CommunicationInfo         : ffff800ed8a33420
    ConnectionPort          : ffffbe0c89022b20 (SmSsWinStationApiPort), Connections
    ClientCommunicationPort : 0000000000000000
    ServerCommunicationPort : 0000000000000000
  OwnerProcess              : ffffbe0c891020c0 (svchost.exe), Connections
  SequenceNo                : 0x00000002 (2)
  CompletionPort            : ffffbe0c890b3c40
  CompletionList            : 0000000000000000
  ConnectionPending         : No
  ConnectionRefused         : No
  Disconnected              : No
  Closed                    : No
  FlushOnClose              : Yes
  ReturnExtendedInfo        : No
  Waitable                  : No
  Security                  : Static
  Wow64CompletionList       : No

  8 thread(s) are registered with port IO completion object:

    THREAD ffffbe0c89110040  Cid 01b4.01f0  Teb: 000000e56c46f000 Win32Thread: 0000000000000000 WAIT
    THREAD ffffbe0c89111080  Cid 01b4.0240  Teb: 000000e56c471000 Win32Thread: 0000000000000000 WAIT
    THREAD ffffbe0c8911c040  Cid 01b4.02d0  Teb: 000000e56c473000 Win32Thread: 0000000000000000 WAIT
    THREAD ffffbe0c8927e080  Cid 01b4.054c  Teb: 000000e56c475000 Win32Thread: 0000000000000000 WAIT
    THREAD ffffbe0c89def040  Cid 01b4.1b68  Teb: 000000e56c477000 Win32Thread: 0000000000000000 WAIT
    THREAD ffffbe0c8b4d9040  Cid 01b4.04cc  Teb: 000000e56c479000 Win32Thread: 0000000000000000 WAIT
    THREAD ffffbe0c8b5da040  Cid 01b4.22c8  Teb: 000000e56c47b000 Win32Thread: 0000000000000000 WAIT
```

```
    THREAD ffffbe0c8b53f040  Cid 01b4.26d4  Teb: 000000e56c47f000 Win32Thread: 0000000000000000 WAIT

  Main queue is empty.


  Direct message queue is empty.


  Large message queue is empty.


  Pending queue has 2 message(s)

    ffff800ed890a8d0 00000084 0000000000000250:000000000000029c ffffbe0c888ca080 ffffbe0c8927e080 LPC_REQUEST
    ffff800ed83f7a50 00000008 00000000000001fc:0000000000000228 ffffbe0c887d60c0 ffffbe0c89111080 LPC_REQUEST

  Canceled queue is empty.
```

Note: ALPC wait chains in *csrss.exe* are normal and expected. We can get the list of all ALPC receiver threads and threads waiting for a reply using Microsoft MEX Debugging Extension:

https://www.microsoft.com/en-us/download/details.aspx?id=53304

After downloading, extracting, and unzipping, we copy \x64*mex.dll* to our dump files folder, for example, C:\AdvWMDA-Dumps\x64. If you use the classic WinDbg from Debugging Tools for Windows, you can copy it to the WinDbg installation folder (for example, *C:\Program Files (x86)\Windows Kits\10\Debuggers\x64*). If you use the Docker environment, then it is already installed.

```
1: kd> .load C:\AdvWMDA-Dumps\x64\mex
Mex External 3.0.0.7172 Loaded!
```

```
1: kd> !mex.help
Mex currently has 255 extensions available.  Please specify a keyword to search.
Or browse by category:

All PowerShell[6] SystemCenter[3] Networking[12] Process[5] Mex[2] Kernel[27] DotNet[32] Decompile[15] Utility[40] Thread[27] Binaries[6] General[22]
```

```
1: kd> !mex.help -all
[...]
```

```
1: kd> !mex.wrlpcreceive
Process                 PID Thread              Id CSwitches User Kernel State        Time Reason       Wait Function
====================== ==== ================ ==== ========= ==== ====== ======= ========= ============ ======================================
System                    4 ffffbe0c87808040  164         60    0      0 Waiting 5m:03.562 WrLpcReceive nt!AlpcpSignalAndWait+0x13d
csrss.exe               1fc ffffbe0c87d1a580  20c        817    0  156ms Waiting     906ms WrLpcReceive CSRSRV!CsrApiRequestThread+0x106
csrss.exe               1fc ffffbe0c87efb080  238          3    0      0 Waiting 7m:12.968 WrLpcReceive Kernel stack not resident
csrss.exe               1fc ffffbe0c88893080  268        952 31ms   63ms Waiting    6s.453 WrLpcReceive CSRSRV!CsrApiRequestThread+0x106
csrss.exe               1fc ffffbe0c89a9a080  cd0        670 31ms   16ms Waiting    6s.781 WrLpcReceive CSRSRV!CsrApiRequestThread+0x106
csrss.exe               250 ffffbe0c887e5080  264        942 63ms  156ms Waiting     796ms WrLpcReceive CSRSRV!CsrApiRequestThread+0x106
csrss.exe               250 ffffbe0c888d9080  2ac          3    0      0 Waiting 7m:12.593 WrLpcReceive Kernel stack not resident
csrss.exe               250 ffffbe0c888eb080  2ec        912 78ms  125ms Waiting     796ms WrLpcReceive CSRSRV!CsrApiRequestThread+0x106
csrss.exe               250 ffffbe0c89116080  254          5    0      0 Waiting 7m:08.765 WrLpcReceive Kernel stack not resident
csrss.exe               250 ffffbe0c89122080  300        885 94ms   47ms Waiting    1s.437 WrLpcReceive CSRSRV!CsrApiRequestThread+0x106
lsass.exe               294 ffffbe0c8881b5c0  2c4          3    0      0 Waiting 7m:12.562 WrLpcReceive Kernel stack not resident
dwm.exe                 310 ffffbe0c89368080  66c        147    0      0 Waiting 7m:10.046 WrLpcReceive Kernel stack not resident
svchost.exe (Themes)    884 ffffbe0c841c9080  8d4        389    0      0 Waiting    6s.171 WrLpcReceive themeservice!CAPIConnection::Listen+0x81
svchost.exe (FontCache) 8b8 ffffbe0c895a1080  92c        814 78ms   31ms Waiting    8s.875 WrLpcReceive fntcache!AlpcServer::ProcessMessage+0xe1
ctfmon.exe              11ec ffffbe0c8978e080  878        568    0      0 Waiting    5s.453 WrLpcReceive MSCTF!CCtfServerPort::ServerLoop+0x18f
splwow64.exe            13b4 ffffbe0c8764b080 11e0         27    0      0 Waiting 1m:42.109 WrLpcReceive splwow64!LPCConnMsgsServingThread+0x5d
Count: 16
```

Note: The command takes some time to execute since it has to scan all threads. MEX command also changed the current CPU from 1 to 0.

```
0: kd> !mex.wrlpcreply
Process                 PID Thread              Id CSwitches User Kernel State        Time Reason     Waiting On                                                  Wait Function
====================== ==== ================ ==== ========= ==== ====== ======= ========= ========== ========================================================== ================================================================
csrss.exe               1fc ffffbe0c887d60c0  228         8    0   16ms Waiting 6m:42.796 WrLpcReply Thread: ffffbe0c89111080 in svchost.exe (LSM) (0n436)      winsrvext!TerminalServerRequestThread+0x304
csrss.exe               250 ffffbe0c888ca080  29c        38    0      0 Waiting 6m:42.812 WrLpcReply Thread: ffffbe0c8927e080 in svchost.exe (LSM) (0n436)      winsrvext!TerminalServerRequestThread+0x304
svchost.exe (netprofm)  694 ffffbe0c8a860080 1458         1    0      0 Waiting 6m:39.171 WrLpcReply Thread: ffffbe0c8a861080 in svchost.exe (SSDPSRV) (0n6052) ssdpapi!GetNotificationLoop+0x84
svchost.exe (SensrSvc)  720 ffffbe0c8411c080  818         1    0      0 Waiting 7m:09.359 WrLpcReply Thread: ffffbe0c89116080 in csrss.exe (0n592)              Kernel stack not resident
svchost.exe (TokenBroker) 130c ffffbe0c8a92a040 18c0      665 94ms      0 Waiting 5m:01.718 WrLpcReply Message queued to SystemSettings.exe (0n9128)             combase!CMessageCall::RpcSendRequestReceiveResponse+0xb9
svchost.exe (BITS)      1758 ffffbe0c8978f080  fa0         1    0      0 Waiting 6m:29.468 WrLpcReply Thread: ffffbe0c8a8e8040 in svchost.exe (SSDPSRV) (0n6052) SSDPAPI!GetNotificationLoop+0x84
```

```
SearchHost.exe            49c ffffbe0c8ad6f080 1b20        9    0      0 Waiting 6m:32.750 WrLpcReply Thread: ffffbe0c8acc5040 in dllhost.exe (0n6644)
SearchHost.exe            49c ffffbe0c8a3f6080 1c54       10    0      0 Waiting 6m:26.718 WrLpcReply Thread: ffffbe0c8acbe040 in dllhost.exe (0n6644)
RuntimeBroker.exe         184c ffffbe0c84ca3040 11b4      631 31ms      0 Waiting   36s.015 WrLpcReply Message queued to SearchHost.exe (0n1180)                combase!CMessageCall::RpcSendRequestReceiveResponse+0xb9
RuntimeBroker.exe         1d80 ffffbe0c8ac020c0 1d9c       60    0   16ms Waiting 6m:06.140 WrLpcReply Message queued to YourPhone.exe (0n6248)                 combase!CMessageCall::RpcSendRequestReceiveResponse+0xb9
msedge.exe                1200 ffffbe0c8760a080 25dc        1    0      0 Waiting     859ms WrLpcReply Thread: ffffbe0c89591040 in svchost.exe (-p) (0n2100)       DNSAPI!SyncResolverQueryRpc+0x1d7
SearchHost.exe            2434 ffffbe0c8b41e500  e40       10    0      0 Waiting   12s.140 WrLpcReply Thread: ffffbe0c8acb7080 in dllhost.exe (0n6644)         edgehtml!WebPlatStorageEventsManager::BackgroundThreadProc+0x15c
SearchHost.exe            2434 ffffbe0c8b419080  bf4        9    0      0 Waiting   11s.125 WrLpcReply Thread: ffffbe0c8acc0040 in dllhost.exe (0n6644)         edgehtml!WebPlatStorageEventsManager::BackgroundThreadProc+0x15c
Count: 13
```

8. Now we try to list processes and threads from session 1:

```
0: kd> !sprocess 1 3f
Dumping Session 1
```

Note: The WinDbg extension command fails in this debugger version (you may also get **Cannot read session list message** or **Cannot find nt!_MM_SESSION_SPACE type** instead), so we address this bug in Exercise C3B after learning how to navigate linked lists. However, we can still see the list of session 1 processes and also their bitness by using the MEX extension **tasklist** command:

```
0: kd> !mex.tasklist -s 1
PID            Address           Name                                Ses
============== ================= =================================== ===
0x250  0n592  ffffbe0c888840c0 csrss.exe                              1
0x2b4  0n692  ffffbe0c888dc080 winlogon.exe                           1
0x340  0n832  ffffbe0c889b11c0 fontdrvhost.exe                        1
0x310  0n784  ffffbe0c89120080 dwm.exe                                1
0x1160 0n4448 ffffbe0c8a2320c0 sihost.exe                             1
0x11f8 0n4600 ffffbe0c898c10c0 svchost.exe(CDPUserSvc)                1
0x1204 0n4612 ffffbe0c8a3340c0 svchost.exe(WpnUserService)            1
0x12d0 0n4816 ffffbe0c8a337080 taskhostw.exe                          1
0x1070 0n4208 ffffbe0c8a455080 explorer.exe                           1
0x1518 0n5400 ffffbe0c8a4f7080 svchost.exe(cbdhsvc)                   1
0x49c  0n1180 ffffbe0c8a982080 SearchHost.exe                         1
0x6d8  0n1752 ffffbe0c8aa020c0 StartMenuExperienceHost.exe            1
0x184c 0n6220 ffffbe0c8aaa00c0 RuntimeBroker.exe                      1
0x18d4 0n6356 ffffbe0c8ab52080 svchost.exe(UdkUserSvc)                1
0x18fc 0n6396 ffffbe0c8aa37080 RuntimeBroker.exe                      1
0x19f4 0n6644 ffffbe0c8acd6080 dllhost.exe                            1
0x1868 0n6248 ffffbe0c8ae6f080 YourPhone.exe                          1
0x11ec 0n4588 ffffbe0c8ae72080 ctfmon.exe                             1
0x1b70 0n7024 ffffbe0c8aeeb0c0 TabTip.exe                             1
0x1d80 0n7552 ffffbe0c8af240c0 RuntimeBroker.exe                      1
0x1df8 0n7672 ffffbe0c8ac98080 smartscreen.exe                        1
0x1e28 0n7720 ffffbe0c84120080 SecurityHealthSystray.exe              1
0x1e7c 0n7804 ffffbe0c8aedd080 vmtoolsd.exe                           1
0x1ef8 0n7928 ffffbe0c8b2080c0 ApplicationFrameHost.exe               1
0x1f04 0n7940 ffffbe0c8ad84080 TextInputHost.exe                      1
0x1fd8 0n8152 ffffbe0c8af55080 vm3dservice.exe                        1
0x1188 0n4488 ffffbe0c8b49a080 OneDrive.exe                           1
0x484  0n1156 ffffbe0c8b4020c0 Cortana.exe                            1
0x1fd4 0n8148 ffffbe0c8b417080 RuntimeBroker.exe                      1
0x1390 0n5008 ffffbe0c8b4b2080 svchost.exe(NPSMSvc)                   1
0x2040 0n8256 ffffbe0c8b092080 svchost.exe(AarSvc)                    1
0x23a8 0n9128 ffffbe0c8b5e60c0 SystemSettings.exe                     1
0x1414 0n5140 ffffbe0c8b4b60c0 UserOOBEBroker.exe                     1
0x2068 0n8296 ffffbe0c8b3d5080 svchost.exe(UnistackSvcGroup)          1
0xf0c  0n3852 ffffbe0c8b4d80c0 msedge.exe                             1
0x1e8c 0n7820 ffffbe0c8ad810c0 msedge.exe                             1
0x83c  0n2108 ffffbe0c8b0d60c0 msedge.exe                             1
0x1200 0n4608 ffffbe0c8cce90c0 msedge.exe                             1
0x20d8 0n8408 ffffbe0c8b224080 msedge.exe                             1
0x23a4 0n9124 ffffbe0c8b6960c0 msedge.exe                             1
0x7cc  0n1996 ffffbe0c8b5b30c0 msedge.exe                             1
0x12bc 0n4796 ffffbe0c8af460c0 msedge.exe                             1
```

```
0x2288 0n8840 ffffbe0c8b0e20c0 MiniSearchHost.exe                    1
0x1b24 0n6948 ffffbe0c870210c0 Notepad.exe                           1
0x22a8 0n8872 ffffbe0c876480c0 dllhost.exe                           1
0x236c 0n9068 ffffbe0c84caf080 CalculatorApp.exe                     1
0xce8  0n3304 ffffbe0c8b538080 RuntimeBroker.exe                     1
0x1d98 0n7576 ffffbe0c8be620c0 wordpad.exe*32                        1
0x13b4 0n5044 ffffbe0c8bed8080 splwow64.exe                          1
0x2384 0n9092 ffffbe0c84c990c0 svchost.exe(PrintWorkflowUserSvc)     1
0x1260 0n4704 ffffbe0c8a7a6080 LINQPad7.exe                          1
0x2478 0n9336 ffffbe0c8b318080 LINQPad7.Query.exe                    1
0x2560 0n9568 ffffbe0c8c9d3080 cmd.exe                               1
0x2568 0n9576 ffffbe0c8b317080 conhost.exe                           1
0x2678 0n9848 ffffbe0c877ec080 Taskmgr.exe                           1
0x243c 0n9276 ffffbe0c8c2cd0c0 notmyfault64.exe                      1
0x2434 0n9268 ffffbe0c8bfb10c0 SearchHost.exe                        1
============= ================ ================================ ===
PID           Address          Name                             Ses

Warning! Zombie process(es) detected (not displayed). Count: 7 [zombie report]
```

Note: For the complete list or **tasklist** command options, please use **-?** parameter. We explore *wordpad.exe* stack traces in the next Exercise C1B.

We can list zombie processes or get a shorter report about them using these commands:

```
0: kd> !mex.tasklist -z
PID           Address          Name                    Ses Thd Obj Handles Obj Pointers
============= ================ ====================== === === =========== ============
0x1234 0n4660 ffffbe0c8a0c4080 taskhostw.exe             1   0           0            1
0xbb0  0n2992 ffffbe0c8a454080 userinit.exe              1   0           1            1
0x1b78 0n7032 ffffbe0c8ae760c0 svchost.exe               0   0           0            1
0x12c8 0n4808 ffffbe0c8b4e90c0 msedge.exe                1   0           0            1
0x2328 0n9000 ffffbe0c89a020c0 Win32Bridge.Server.exe    1   0           1        32767
0x22f8 0n8952 ffffbe0c8b3960c0 identity_helper.exe       1   0           1        32768
0x25ac 0n9644 ffffbe0c8c5760c0 TabTip.exe                1   0           1        32763
============= ================ ====================== === === =========== ============
PID           Address          Name                    Ses Thd Obj Handles Obj Pointers

0: kd> !mex.tasklist -z -r
Count Name                   Ses Thd Obj Handles Obj Pointers
===== ====================== === === =========== ============
    1 identity_helper.exe      1   0           1        32768
    1 msedge.exe               1   0           0            1
    1 svchost.exe              0   0           0            1
    1 TabTip.exe               1   0           1        32763
    1 taskhostw.exe            1   0           0            1
    1 userinit.exe             1   0           1            1
    1 Win32Bridge.Server.exe   1   0           1        32767
===== ====================== === === =========== ============
Count Name                   Ses Thd Obj Handles Obj Pointers
    7
```

Sometimes, we are interested in *svchost.exe* to service name translation:

```
0: kd> !mex.tasklist -svc
PID           Address           Name
============= ================= ====================================
0x0    0n0    fffff80762d32b00 Idle
0x4    0n4    ffffbe0c840eb040 System
0x64   0n100  ffffbe0c84136080 Registry
0x168  0n360  ffffbe0c8780f040 smss.exe
0x1fc  0n508  ffffbe0c87f2b080 csrss.exe
0x244  0n580  ffffbe0c887d4080 wininit.exe
0x250  0n592  ffffbe0c888840c0 csrss.exe
0x28c  0n652  ffffbe0c888c9100 services.exe
0x294  0n660  ffffbe0c888cb0c0 lsass.exe
0x2b4  0n692  ffffbe0c888dc080 winlogon.exe
0x340  0n832  ffffbe0c889b11c0 fontdrvhost.exe
0x348  0n840  ffffbe0c889af1c0 fontdrvhost.exe
0x354  0n852  ffffbe0c889ae080 svchost.exe(-p)
0x3a8  0n936  ffffbe0c890130c0 WUDFHost.exe
0x3f0  0n1008 ffffbe0c889c7080 svchost.exe(-p)
0x1b4  0n436  ffffbe0c891020c0 svchost.exe(LSM)
0x310  0n784  ffffbe0c89120080 dwm.exe
0x44c  0n1100 ffffbe0c891a0080 svchost.exe(gpsvc)
0x454  0n1108 ffffbe0c8919e080 svchost.exe(-p)
0x460  0n1120 ffffbe0c891a80c0 svchost.exe(lmhosts)
0x474  0n1140 ffffbe0c891b90c0 svchost.exe(BTAGService)
0x494  0n1172 ffffbe0c891c6080 svchost.exe(BthAvctpSvc)
0x4b0  0n1200 ffffbe0c89209080 svchost.exe(bthserv)
0x4f0  0n1264 ffffbe0c89241080 svchost.exe(NcbService)
0x508  0n1288 ffffbe0c892550c0 svchost.exe(TimeBrokerSvc)
0x554  0n1364 ffffbe0c892b6080 svchost.exe(Schedule)
0x5bc  0n1468 ffffbe0c89348080 svchost.exe(DispBrokerDesktopSvc)
0x5d4  0n1492 ffffbe0c8934d080 svchost.exe(ProfSvc)
0x600  0n1536 ffffbe0c89362080 svchost.exe(DisplayEnhancementService)
0x63c  0n1596 ffffbe0c893bc080 svchost.exe(nsi)
0x644  0n1604 ffffbe0c893bf080 svchost.exe(UserManager)
0x664  0n1636 ffffbe0c89363080 svchost.exe(DeviceAssociationService)
0x694  0n1684 ffffbe0c89407080 svchost.exe(netprofm)
0x6a8  0n1704 ffffbe0c8940a080 svchost.exe(SensorService)
0x720  0n1824 ffffbe0c841ba080 svchost.exe(SensrSvc)
0x748  0n1864 ffffbe0c841b0080 svchost.exe(TabletInputService)
0x760  0n1888 ffffbe0c84185080 svchost.exe(camsvc)
0x82c  0n2092 ffffbe0c841ed080 svchost.exe(EventLog)
0x834  0n2100 ffffbe0c84135080 svchost.exe(-p)
0x864  0n2148 ffffbe0c89496080 svchost.exe(EventSystem)
0x870  0n2160 ffffbe0c895340c0 svchost.exe(SysMain)
0x884  0n2180 ffffbe0c89538080 svchost.exe(Themes)
0x8b8  0n2232 ffffbe0c89596080 svchost.exe(FontCache)
0x8f0  0n2288 ffffbe0c895b3040 MemCompression
0x910  0n2320 ffffbe0c895cc080 svchost.exe(SENS)
0x93c  0n2364 ffffbe0c895df080 svchost.exe(AudioEndpointBuilder)
0x97c  0n2428 ffffbe0c8963c080 svchost.exe(Dhcp)
0x9e8  0n2536 ffffbe0c896b1080 svchost.exe(WinHttpAutoProxySvc)
0xa0c  0n2572 ffffbe0c896d20c0 svchost.exe(-p)
0xa60  0n2656 ffffbe0c89730080 svchost.exe(-p)
0xa68  0n2664 ffffbe0c897450c0 svchost.exe(-p)
0xab4  0n2740 ffffbe0c89728080 svchost.exe(ShellHWDetection)
0xacc  0n2764 ffffbe0c897da080 svchost.exe(StateRepository)
0xb24  0n2852 ffffbe0c897ed0c0 spoolsv.exe
0xb48  0n2888 ffffbe0c897dc0c0 svchost.exe(-p)
```

```
0xb68  0n2920 ffffbe0c89895080 svchost.exe(LanmanWorkstation)
0xa24  0n2596 ffffbe0c89a07080 svchost.exe(-p)
0xb98  0n2968 ffffbe0c89a06080 svchost.exe(-p)
0xc04  0n3076 ffffbe0c89042080 svchost.exe(DPS)
0xc14  0n3092 ffffbe0c89a0a080 svchost.exe(iphlpsvc)
0xc54  0n3156 ffffbe0c89a8e0c0 svchost.exe(LanmanServer)
0xc6c  0n3180 ffffbe0c89a96080 svchost.exe(SstpSvc)
0xc7c  0n3196 ffffbe0c89aa6080 svchost.exe(TrkWks)
0xc84  0n3204 ffffbe0c89aa9080 VGAuthService.exe
0xc8c  0n3212 ffffbe0c89aaa080 vmtoolsd.exe
0xca0  0n3232 ffffbe0c89a42080 MsMpEng.exe
0xcac  0n3244 ffffbe0c89ac10c0 svchost.exe(Winmgmt)
0xcb8  0n3256 ffffbe0c89aae080 svchost.exe(WpnService)
0xdd8  0n3544 ffffbe0c899e80c0 svchost.exe(netsvcs)
0xf00  0n3840 ffffbe0c89c30080 dllhost.exe
0xfa8  0n4008 ffffbe0c89cf8080 AggregatorHost.exe
0x438  0n1080 ffffbe0c89e840c0 svchost.exe(RmSvc)
0xaf0  0n2800 ffffbe0c89f5e080 msdtc.exe
0x10e8 0n4328 ffffbe0c8a0540c0 svchost.exe(AppXSvc)
0x1278 0n4728 ffffbe0c8a0cb080 WmiPrvSE.exe
0x1160 0n4448 ffffbe0c8a2320c0 sihost.exe
0x11f8 0n4600 ffffbe0c898c10c0 svchost.exe(CDPUserSvc)
0x1204 0n4612 ffffbe0c8a3340c0 svchost.exe(WpnUserService)
0x12d0 0n4816 ffffbe0c8a337080 taskhostw.exe
0x130c 0n4876 ffffbe0c8a071080 svchost.exe(TokenBroker)
0x13a0 0n5024 ffffbe0c8a4020c0 MsMpEngCP.exe
0x13b8 0n5048 ffffbe0c8a43b080 svchost.exe(CDPSvc)
0x1070 0n4208 ffffbe0c8a455080 explorer.exe
0x1448 0n5192 ffffbe0c8a4f8080 svchost.exe(ClipSVC)
0x1518 0n5400 ffffbe0c8a4f7080 svchost.exe(cbdhsvc)
0x1564 0n5476 ffffbe0c8a4ef0c0 svchost.exe(Appinfo)
0x1590 0n5520 ffffbe0c8a4e9080 WmiPrvSE.exe
0x15c4 0n5572 ffffbe0c8a6c1080 NisSrv.exe
0x1650 0n5712 ffffbe0c8a729080 svchost.exe(lfsvc)
0x1744 0n5956 ffffbe0c8a8540c0 SearchIndexer.exe
0x1758 0n5976 ffffbe0c8a859080 svchost.exe(BITS)
0x17a4 0n6052 ffffbe0c8a9240c0 svchost.exe(SSDPSRV)
0x49c  0n1180 ffffbe0c8a982080 SearchHost.exe
0x6d8  0n1752 ffffbe0c8aa020c0 StartMenuExperienceHost.exe
0x181c 0n6172 ffffbe0c8a55b0c0 svchost.exe(WdiSystemHost)
0x184c 0n6220 ffffbe0c8aaa00c0 RuntimeBroker.exe
0x18d4 0n6356 ffffbe0c8ab52080 svchost.exe(UdkUserSvc)
0x18fc 0n6396 ffffbe0c8aa37080 RuntimeBroker.exe
0x196c 0n6508 ffffbe0c8ac07080 svchost.exe(PcaSvc)
0x19f4 0n6644 ffffbe0c8acd6080 dllhost.exe
0x1afc 0n6908 ffffbe0c8ad94080 svchost.exe(LicenseManager)
0x1868 0n6248 ffffbe0c8ae6f080 YourPhone.exe
0x11ec 0n4588 ffffbe0c8ae72080 ctfmon.exe
0x1b70 0n7024 ffffbe0c8aeeb0c0 TabTip.exe
0x1d38 0n7480 ffffbe0c8ac8e080 WmiApSrv.exe
0x1d80 0n7552 ffffbe0c8af240c0 RuntimeBroker.exe
0x1df8 0n7672 ffffbe0c8ac98080 smartscreen.exe
0x1e28 0n7720 ffffbe0c84120080 SecurityHealthSystray.exe
0x1e3c 0n7740 ffffbe0c8aee1080 SecurityHealthService.exe
0x1e7c 0n7804 ffffbe0c8aedd080 vmtoolsd.exe
0x1ef8 0n7928 ffffbe0c8b2080c0 ApplicationFrameHost.exe
0x1f04 0n7940 ffffbe0c8ad84080 TextInputHost.exe
0x1fd8 0n8152 ffffbe0c8af55080 vm3dservice.exe
0x1188 0n4488 ffffbe0c8b49a080 OneDrive.exe
0x484  0n1156 ffffbe0c8b4020c0 Cortana.exe
```

```
0x1fd4 0n8148 ffffbe0c8b417080 RuntimeBroker.exe
0x130  0n304  ffffbe0c8b37b080 svchost.exe(wuauserv)
0x1390 0n5008 ffffbe0c8b4b2080 svchost.exe(NPSMSvc)
0x2040 0n8256 ffffbe0c8b092080 svchost.exe(AarSvc)
0x20cc 0n8396 ffffbe0c876f2080 svchost.exe(DoSvc)
0x2124 0n8484 ffffbe0c8b4d6080 svchost.exe(StorSvc)
0x23a8 0n9128 ffffbe0c8b5e60c0 SystemSettings.exe
0x1ac0 0n6848 ffffbe0c8b8870c0 svchost.exe(UsoSvc)
0x1414 0n5140 ffffbe0c8b4b60c0 UserOOBEBroker.exe
0x1a3c 0n6716 ffffbe0c876f8080 SgrmBroker.exe
0x4e8  0n1256 ffffbe0c892bc080 svchost.exe(W32Time)
0x8d8  0n2264 ffffbe0c89a9b080 svchost.exe(wscsvc)
0x2068 0n8296 ffffbe0c8b3d5080 svchost.exe(UnistackSvcGroup)
0xf0c  0n3852 ffffbe0c8b4d80c0 msedge.exe
0x1e8c 0n7820 ffffbe0c8ad810c0 msedge.exe
0x83c  0n2108 ffffbe0c8b0d60c0 msedge.exe
0x1200 0n4608 ffffbe0c8cce90c0 msedge.exe
0x20d8 0n8408 ffffbe0c8b224080 msedge.exe
0x23a4 0n9124 ffffbe0c8b6960c0 msedge.exe
0x7cc  0n1996 ffffbe0c8b5b30c0 msedge.exe
0x12bc 0n4796 ffffbe0c8af460c0 msedge.exe
0x2288 0n8840 ffffbe0c8b0e20c0 MiniSearchHost.exe
0x1b24 0n6948 ffffbe0c870210c0 Notepad.exe
0x22a8 0n8872 ffffbe0c876480c0 dllhost.exe
0x236c 0n9068 ffffbe0c84caf080 CalculatorApp.exe
0xce8  0n3304 ffffbe0c8b538080 RuntimeBroker.exe
0x1d98 0n7576 ffffbe0c8be620c0 wordpad.exe*32
0x13b4 0n5044 ffffbe0c8bed8080 splwow64.exe
0x2384 0n9092 ffffbe0c84c990c0 svchost.exe(PrintWorkflowUserSvc)
0x328  0n808  ffffbe0c8be760c0 svchost.exe(wlidsvc)
0x1260 0n4704 ffffbe0c8a7a6080 LINQPad7.exe
0x2478 0n9336 ffffbe0c8b318080 LINQPad7.Query.exe
0x2560 0n9568 ffffbe0c8c9d3080 cmd.exe
0x2568 0n9576 ffffbe0c8b317080 conhost.exe
0x2678 0n9848 ffffbe0c877ec080 Taskmgr.exe
0x246c 0n9324 ffffbe0c8c2de0c0 audiodg.exe
0x243c 0n9276 ffffbe0c8c2cd0c0 notmyfault64.exe
0x2434 0n9268 ffffbe0c8bfb10c0 SearchHost.exe
============= ================ ======================================
PID           Address          Name

Warning! Zombie process(es) detected (not displayed). Count: 7 [zombie report]
```

Note: If you want to see command lines, use the **-cl** parameter. Nicely summarized additional information, such as whether *gflags.exe* was used, whether blocked, running, suspended, or waiting-for-ALPC threads exist (including overall thread count), can be seen with the **-a** parameter (pay attention to **!! Rn Ry Bk Lc IO Er** columns). It also shows PIDs in both hex and decimal formats. Consider this as a column-based **!process 0 3f**. Some columns may not show information for recent Windows versions.

9. Another way to list all stack traces is to use the **!for_each_thread** command, where we can customize stack trace output:

```
0: kd> !for_each_thread ".thread /r /p @#Thread; kc"
.thread /r /p @#Thread; kc
Implicit thread is now ffffbe0c`841cd080
Implicit process is now ffffbe0c`840eb040
Loading User Symbols
```

```
************* Symbol Loading Error Summary **************
Module name            Error
myfault                The system cannot find the file specified

You can troubleshoot most symbol related issues by turning on symbol loading diagnostics (!sym
noisy) and repeating the command that caused symbols to be loaded.
You should also verify that your symbol search path (.sympath) is correct.
  *** Stack trace for last set context - .thread/.cxr resets it
 # Call Site
00 nt!KiSwapContext
01 nt!KiSwapThread
02 nt!KiCommitThreadWait
03 nt!KeWaitForSingleObject
04 nt!PopIrpWorkerControl
05 nt!PspSystemThreadStartup
06 nt!KiStartSystemThread
.thread /r /p @#Thread; kc
Implicit thread is now ffffbe0c`84145080
Implicit process is now ffffbe0c`840eb040
Loading User Symbols

[...]

Implicit thread is now ffffbe0c`8c116080
Implicit process is now ffffbe0c`8bfb10c0
Loading User Symbols
...............................................................
...............................................................
.................................

************* Symbol Loading Error Summary **************
Module name            Error
vsock                  The system cannot find the file specified
vmci                   The system cannot find the file specified
WdFilter               The system cannot find the file specified
vm3dmp                 The system cannot find the file specified
vmmemctl               The system cannot find the file specified
vmhgfs                 The system cannot find the file specified
myfault                The system cannot find the file specified

You can troubleshoot most symbol related issues by turning on symbol loading diagnostics (!sym
noisy) and repeating the command that caused symbols to be loaded.
You should also verify that your symbol search path (.sympath) is correct.
  *** Stack trace for last set context - .thread/.cxr resets it
 # Call Site
00 nt!KiSwapContext
01 nt!KiSwapThread
02 nt!KiCommitThreadWait
03 nt!KeWaitForMultipleObjects
04 nt!ObWaitForMultipleObjects
05 win32kfull!xxxMsgWaitForMultipleObjectsEx
06 win32kfull!NtUserMsgWaitForMultipleObjectsEx
07 win32k!NtUserMsgWaitForMultipleObjectsEx
08 nt!KiSystemServiceCopyEnd
09 win32u!NtUserMsgWaitForMultipleObjectsEx
0a user32!RealMsgWaitForMultipleObjectsEx
0b combase!CCliModalLoop::BlockFn
0c combase!ClassicSTAThreadWaitForHandles
```

```
0d combase!CoWaitForMultipleHandles
0e edgehtml!CDwnTaskExec::ThreadExec
0f edgehtml!CExecFT::ThreadProc
10 edgehtml!CExecFT::StaticThreadProc
11 KERNEL32!BaseThreadInitThunk
12 ntdll!RtlUserThreadStart
```

Note: We can use this script to list all processes and threads, including 32-bit stack traces, when it is possible:

```
!for_each_thread "!thread @#Thread 3f;.thread /w @#Thread; .reload; kb 256; .effmach AMD64"
```

Note: Mex **!ForEachThread** (**!fet**) can also be used. Use the **-?** option to see the syntax. The advantage of it is the ability to apply commands to a particular process (we don't need to exclude other processes in the body of the **!for_each_thread** command) and also include terminated threads (we choose *wordpad.exe*32* process address from the previous output):

```
0: kd> !mex.fet -t -p ffffbe0c8be620c0 "!thread @#Thread 3f; .thread /w @#Thread; .reload; kL
256; .effmach AMD64"
Changing to thread: ffffbe0c8beda080
THREAD ffffbe0c8beda080  Cid 1d98.1bb0  Teb: 00000000008b5000 Win32Thread: ffffbe0c8ccd5ed0
WAIT: (WrUserRequest) UserMode Non-Alertable
    ffffbe0c8bd0e580  QueueObject
Not impersonating
DeviceMap                 ffff800eda518d20
Owning Process            ffffbe0c8be620c0       Image:         wordpad.exe
Attached Process          N/A            Image:         N/A
Wait Start TickCount      29755          Ticks: 32 (0:00:00:00.500)
Context Switch Count      3348           IdealProcessor: 1
UserTime                  00:00:00.187
KernelTime                00:00:00.578
Win32 Start Address wordpad!wWinMainCRTStartup (0x0000000001036e40)
Stack Init ffffa28ca02c3c70 Current ffffa28ca02c3050
Base ffffa28ca02c4000 Limit ffffa28ca02be000 Call 0000000000000000
Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
Child-SP          RetAddr               Call Site
ffffa28c`a02c3090 fffff807`623327f7     nt!KiSwapContext+0x76
ffffa28c`a02c31d0 fffff807`623346a9     nt!KiSwapThread+0x3a7
ffffa28c`a02c32b0 fffff807`6232e5c4     nt!KiCommitThreadWait+0x159
ffffa28c`a02c3350 fffff807`6228efe0     nt!KeWaitForSingleObject+0x234
ffffa28c`a02c3440 ffffbc92`8e76afd6     nt!KeWaitForMultipleObjects+0x540
ffffa28c`a02c3540 ffffbc92`8e76ac3f     win32kfull!xxxRealSleepThread+0x2c6
ffffa28c`a02c3660 ffffbc92`8e76e08a     win32kfull!xxxSleepThread2+0xb3
ffffa28c`a02c36b0 ffffbc92`8e7b26ec     win32kfull!xxxRealInternalGetMessage+0xc5a
ffffa28c`a02c3a10 ffffbc92`8dc4645a     win32kfull!NtUserGetMessage+0x8c
ffffa28c`a02c3aa0 fffff807`62428775     win32k!NtUserGetMessage+0x16
ffffa28c`a02c3ae0 00007ffe`5ac81424     nt!KiSystemServiceCopyEnd+0x25 (TrapFrame @
ffffa28c`a02c3ae0)
00000000`00a5e1d8 00007ffe`5ac7510e     wow64win!NtUserGetMessage+0x14
00000000`00a5e1e0 00007ffe`5a0f77ca     wow64win!whNtUserGetMessage+0x2e
00000000`00a5e240 00000000`775517ba     wow64!Wow64SystemServiceEx+0x15a
00000000`00a5eb00 00000000`77551d75     wow64cpu!ServiceNoTurbo+0xb
00000000`00a5ebb0 00007ffe`5a0fe06d     wow64cpu!BTCpuSimulate+0xbb5
00000000`00a5ebf0 00007ffe`5a0fd8ad     wow64!RunCpuSimulation+0xd
00000000`00a5ec20 00007ffe`5b05f87d     wow64!Wow64LdrpInitialize+0x12d
00000000`00a5eed0 00007ffe`5b04d78c     ntdll!LdrpInitializeProcess+0x16d1
00000000`00a5f290 00007ffe`5affa993     ntdll!_LdrpInitialize+0x52dc0
00000000`00a5f310 00007ffe`5affa8be     ntdll!LdrpInitializeInternal+0x6b
```

```
00000000`00a5f590 00000000`00000000     ntdll!LdrInitializeThunk+0xe

Implicit thread is now ffffbe0c`8beda080
WARNING: WOW context retrieval requires
switching to the thread's process context.
Use .process /p ffffbe0c`89120080 to switch back.
Implicit process is now ffffbe0c`8be620c0
The context is partially valid. Only x86 user-mode context is available.
x86 context set
Loading Kernel Symbols
...............................................................
...............................................................
...............................................................
..
Loading User Symbols
.......
Loading unloaded module list
........
Loading Wow64 Symbols
...............................................................
....
 # ChildEBP          RetAddr
00 00a9fd70 758e0200     win32u!NtUserGetMessage+0xc
01 00a9fdac 75238f35     USER32!GetMessageW+0x30
02 00a9fdc8 75238fe3     MFC42u!CWinThread::PumpMessage+0x15
03 00a9fde4 7520a242     MFC42u!CWinThread::Run+0x63
04 00a9fdfc 01036d0c     MFC42u!AfxWinMain+0xa2
05 00a9fe8c 75eb6739     wordpad!__wmainCRTStartup+0x153
06 00a9fe9c 775c8e7f     KERNEL32!BaseThreadInitThunk+0x19
07 00a9fef4 775c8e4d     ntdll_77560000!__RtlUserThreadStart+0x2b
08 00a9ff04 00000000     ntdll_77560000!_RtlUserThreadStart+0x1b
Effective machine: x64 (AMD64)
[...]
```

10. Yet another way is to use **!stacks** command (the default version omits paged out stacks):

```
0: kd> !stacks
Proc.Thread  .Thread  Ticks   ThreadState Blocker
                           [fffff80762d32b00 Idle]
   0.000000  fffff80762d35bc0 000230f RUNNING    nt!KiIdleLoop+0x176
   0.000000  ffffce00fb70c0c0 000745b RUNNING    nt!KiIdleLoop+0x176
   0.00002c  ffffbe0c841ab080 0003ae3 RUNNING    nt!KiSwapContext+0x76
   0.000034  ffffbe0c84178080 000745b RUNNING    nt!KiSwapContext+0x76
                           [ffffbe0c840eb040 System]
   4.000018  ffffbe0c84189080 000049a Blocked    nt!PopFxProcessWorkPool+0xf5
   4.00001c  ffffbe0c84097480 00003ba Blocked    nt!ExpWorkQueueManagerThread+0x149
   4.000020  ffffbe0c840af080 000007e Blocked    nt!KeRemovePriQueue+0x259
   4.000024  ffffbe0c8420c140 000000a Blocked    nt!ExpWorkerFactoryManagerThread+0x3b
   4.000040  ffffbe0c841ef080 00010ee Blocked    nt!MiRebuildLargePagesThread+0x5c
   4.000044  ffffbe0c84202080 0006ec8 Blocked    nt!MiZeroPageThread+0x2b
   4.00004c  ffffbe0c8412d080 0000001 READY      nt!MiReadyToZeroNextLargePage+0x179
   4.000050  ffffbe0c8412f080 00003d2 Blocked    nt!MiReadyToZeroNextLargePage+0x179
   4.000054  ffffbe0c84113080 0000029 Blocked    nt!CcQueueLazyWriteScanThread+0xdf
   4.000058  ffffbe0c84076080 0000251 Blocked    nt!CcAsyncReadWorker+0x139
   4.00005c  ffffbe0c840e5080 0007437 Blocked    nt!CcAsyncReadWorker+0x139
   4.000060  ffffbe0c84131080 0007437 Blocked    nt!CcAsyncReadWorker+0x139
   4.00006c  ffffbe0c8413a080 0000026 Blocked    nt!KeRemovePriQueue+0x259
   4.000070  ffffbe0c8413c080 0000219 Blocked    nt!KeRemovePriQueue+0x259
   4.00007c  ffffbe0c84119080 0000027 Blocked    nt!KeRemovePriQueue+0x259
   4.000080  ffffbe0c84153080 00068b3 Blocked    nt!KeRemovePriQueue+0x259
   4.000084  ffffbe0c8411f080 000014c Blocked    nt!EtwpLogger+0xc2
   4.000088  ffffbe0c8415c080 00015df Blocked    nt!EtwpLogger+0xc2
```

```
  4.00008c  ffffbe0c8415e080 0000420 Blocked    nt!EtwpLogger+0xc2
  4.000090  ffffbe0c84162080 00002f3 Blocked    nt!EtwpLogger+0xc2
  4.000094  ffffbe0c84164080 00002f3 Blocked    nt!EtwpLogger+0xc2
  4.000098  ffffbe0c8416b080 00015df Blocked    nt!EtwpLogger+0xc2
  4.00009c  ffffbe0c8416d080 0000419 Blocked    nt!EtwpLogger+0xc2
  4.0000a0  ffffbe0c84171080 0002553 Blocked    nt!EtwpLogger+0xc2
  4.0000a4  ffffbe0c84173080 0006c9e Blocked    nt!EtwpLogger+0xc2
  4.0000a8  ffffbe0c84129080 00001fc Blocked    nt!EtwpLogger+0xc2
  4.0000ac  ffffbe0c84127080 0006c9e Blocked    nt!EtwpLogger+0xc2
  4.0000b0  ffffbe0c8417c080 0006c9e Blocked    nt!EtwpLogger+0xc2
  4.0000b8  ffffbe0c84182080 0006c9e Blocked    nt!EtwpLogger+0xc2
  4.0000bc  ffffbe0c84186080 0001621 Blocked    nt!EtwpLogger+0xc2
  4.0000c0  ffffbe0c8418b080 0004f52 Blocked    nt!EtwpLogger+0xc2
  4.0000c4  ffffbe0c8418d080 0006c9e Blocked    nt!EtwpLogger+0xc2
  4.0000c8  ffffbe0c84191080 000742a Blocked    nt!IopPassiveInterruptRealtimeWorker+0x16
  4.0000cc  ffffbe0c84193080 000742a Blocked    nt!IopPassiveInterruptRealtimeWorker+0x16
  4.0000d0  ffffbe0c84195080 000742a Blocked    nt!IopPassiveInterruptRealtimeWorker+0x16
  4.0000d4  ffffbe0c84197080 000742a Blocked    nt!IopPassiveInterruptRealtimeWorker+0x16
  4.0000dc  ffffbe0c841a6080 0006fa5 Blocked    ACPI!ACPIWorkerThread+0x9a
  4.0000e0  ffffbe0c8477e080 000594e Blocked    nt!KeRemovePriQueue+0x259
  4.0000e4  ffffbe0c84b44040 000683b Blocked    nt!KeRemovePriQueue+0x259
  4.0000e8  ffffbe0c84b46080 0000019 Blocked    nt!KeRemovePriQueue+0x259
  4.0000ec  ffffbe0c84b47040 000685f Blocked    nt!KeRemovePriQueue+0x259
  4.0000f0  ffffbe0c8419e080 00073e1 Blocked    pci!RootPmeEventDispatcher+0x9b
  4.0000f4  ffffbe0c84b3f100 00073e1 Blocked    ACPI!PciRootBusBiosMethodDispatcherOnResume+0x57
  4.0000f8  ffffbe0c84a26100 00073d2 Blocked    Wdf01000!FxSystemThread::Thread+0x134
  4.0000fc  ffffbe0c84bd0480 00015f9 Blocked    tpm!Tpm20Scheduler::SchedulerThreadFunction+0x77
  4.00010c  ffffbe0c84a95040 0007383 Blocked    spaceport!SpLimiterDispatcherThreadRoutine+0x3c
  4.000110  ffffbe0c84a9c080 0007382 Blocked    vsock+0x4334
  4.000114  ffffbe0c84a9d040 0007382 Blocked    vmci+0x859f
  4.000118  ffffbe0c849cd040 000001d Blocked    WdFilter+0x1c629
  4.00011c  ffffbe0c849ce040 00001b7 Blocked    WdFilter+0x1da07
  4.000120  ffffbe0c849cf040 00000b2 Blocked    WdFilter+0x1da07
  4.000124  ffffbe0c84983040 0004830 Blocked    ndis!ndisWaitForKernelObject+0x21
  4.000128  ffffbe0c849db040 0006a3d Blocked    ndis!ndisWaitForKernelObject+0x21
  4.000134  ffffbe0c84c91040 000051d Blocked    nt!KeRemovePriQueue+0x259
  4.000144  ffffbe0c84eb4040 0000186 Blocked    nt!KeRemovePriQueue+0x259
  4.00014c  ffffbe0c84c97040 0000f26 Blocked    nt!KeRemovePriQueue+0x259
  4.000150  ffffbe0c849c8080 0001048 Blocked    nt!KeRemovePriQueue+0x259
  4.000154  ffffbe0c84df8040 00070d2 Blocked    watchdog!SMgrGdiCalloutThread+0x50
  4.000158  ffffbe0c84f440c0 00070c8 Blocked    rdbss!RxpIdleWorkerThread+0x25
  4.00015c  ffffbe0c87aec080 0000019 Blocked    bam!BampThrottlingWorker+0xc3
  4.000160  ffffbe0c87804040 00064b2 Blocked    nt!PopDirectedDripsWorkerRoutine+0x4d
  4.000164  ffffbe0c87808040 0004be4 Blocked    nt!AlpcpSignalAndWait+0x13d
  4.000170  ffffbe0c8780c540 0000000 READY      vm3dmp+0x16775
  4.000174  ffffbe0c87824040 00070ba Blocked    dxgkrnl!DpiPowerArbiterThread+0x67
  4.000180  ffffbe0c87c68040 0000564 Blocked    nt!KeRemovePriQueue+0x259
  4.00018c  ffffbe0c87d68100 00065ea Blocked    BTHport!HCI_ThreadFunction+0x172
  4.000190  ffffbe0c87d4c040 0001aec Blocked    nt!KeRemovePriQueue+0x259
  4.000194  ffffbe0c87daa080 0000186 Blocked    nt!KeRemovePriQueue+0x259
  4.0001f8  ffffbe0c87f20080 000041f Blocked    nt!MiModifiedPageWriter+0x112
  4.000214  ffffbe0c887cd5c0 0000001 Blocked    dxgmms1!VidSchiWaitForSchedulerEvents+0x211
  4.000218  ffffbe0c887ef5c0 0006713 Blocked    dxgkrnl!BLTQUEUE::BltQueueWorker+0x426
  4.00021c  ffffbe0c8880a5c0 0000155 Blocked    BasicRender!WARPKMADAPTER::RunGPU+0x4f8
  4.000220  ffffbe0c887d1100 000011d Blocked    dxgmms2!VidSchiWaitForSchedulerEvents+0x26c
  4.000224  ffffbe0c887c50c0 000015d Blocked    dxgmms2!VIDMM_WORKER_THREAD::Run+0x1bf
  4.000270  ffffbe0c888aa0c0 000018b Blocked    nt!IoRemoveIoCompletion+0x98
  4.0003e0  ffffbe0c89022080 0006bfd Blocked    nt!EtwpLogger+0xc2
  4.000788  ffffbe0c840e0040 00001b9 Blocked    luafv!SynchronousFsControl+0x19e
  4.000810  ffffbe0c84118040 0006b58 Blocked    storqosflt!SqosJobDispatcherThreadRoutine+0x63
  4.000b14  ffffbe0c8980c040 0006af1 Blocked    HTTP!UlpScavengerThread+0x148
  4.000b60  ffffbe0c89892040 0004bab Blocked    mpsdrv!MpsWorkerThread+0xe9
  4.000bb4  ffffbe0c897fc040 00004d8 Blocked    mmcss!CiSchedulerDeepSleep+0x64
  4.000be0  ffffbe0c898ca040 0001aec Blocked    nt!KeRemovePriQueue+0x259
  4.000be4  ffffbe0c898c9040 0000186 Blocked    nt!KeRemovePriQueue+0x259
  4.000970  ffffbe0c8974a040 0001aec Blocked    nt!KeRemovePriQueue+0x259
  4.000a38  ffffbe0c898e8040 0000033 Blocked    vmmemctl+0x24ff
```

```
   4.000c28  ffffbe0c89aed040 0001aed Blocked    nt!KeRemovePriQueue+0x259
   4.000c2c  ffffbe0c89aec040 00000d8 Blocked    nt!KeRemovePriQueue+0x259
   4.000c60  ffffbe0c89a11040 0006a96 Blocked    Ndu!NduTokenComputeTokensWorkerRoutine+0x85
   4.000c64  ffffbe0c89a10040 0000037 Blocked    Ndu!NduUpdateProcessEnergyWorkerRoutine+0xb1
   4.000cec  ffffbe0c89987080 0000f90 Blocked    nt!EtwpLogger+0xc2
   4.000d94  ffffbe0c899c3040 0001048 Blocked    nt!KeRemovePriQueue+0x259
   4.000de0  ffffbe0c89b50040 0006a45 Blocked    vmhgfs+0xdf6b
   4.000de4  ffffbe0c89b4f040 0006a45 Blocked    vmhgfs+0xdf6b
   4.000e58  ffffbe0c8996c040 0006a34 Blocked    srv2!RfspThreadPoolNodeManagerRun+0x81
   4.000e5c  ffffbe0c89b99040 0006a34 Blocked    srv2!RfspThreadPoolNodeWorkerProcessWorkItems+0xd3
   4.000e60  ffffbe0c89b98040 0006a34 Blocked    srv2!RfspThreadPoolNodeManagerRun+0x81
   4.000e64  ffffbe0c89b97040 0006a34 Blocked    srv2!RfspThreadPoolNodeWorkerProcessWorkItems+0xd3
   4.000e68  ffffbe0c89b96040 0006a34 Blocked    srv2!RfspThreadPoolNodeManagerRun+0x81
   4.000e6c  ffffbe0c89b95040 0006a34 Blocked    srv2!RfspThreadPoolNodeWorkerProcessWorkItems+0xd3
   4.000ea4  ffffbe0c89a74040 0006a28 Blocked    ndis!NdisWaitEvent+0x50
   4.000ea8  ffffbe0c841fe040 0006a28 Blocked    ndis!NdisWaitEvent+0x50
   4.000eac  ffffbe0c840bb040 0006a28 Blocked    ndis!NdisWaitEvent+0x50
   4.000eb0  ffffbe0c896d5040 0006a28 Blocked    ndis!NdisWaitEvent+0x50
   4.000eb4  ffffbe0c8952b040 0006a28 Blocked    ndis!NdisWaitEvent+0x50
   4.000eb8  ffffbe0c898e4040 0006a28 Blocked    ndis!NdisWaitEvent+0x50
   4.000f68  ffffbe0c89c660c0 0000c02 Blocked    nt!EtwpLogger+0xc2
   4.000ff0  ffffbe0c892ad080 00010fd Blocked    nt!KeRemovePriQueue+0x259
   4.000ff4  ffffbe0c89df4080 00000ac Blocked    nt!MiStoreEvictThread+0x109
   4.000ba0  ffffbe0c89ec3080 0006991 Blocked    nt!EtwpLogger+0xc2
   4.00105c  ffffbe0c89ce5080 0006958 Blocked    nt!EtwpLogger+0xc2
   4.000ae8  ffffbe0c89caa080 0006830 Blocked    nt!EtwpLogger+0xc2
   4.001d2c  ffffbe0c8a34a080 000001c Blocked    nt!EtwpLogger+0xc2
   4.001dec  ffffbe0c8ac5c080 0000001 READY      nt!KxDispatchInterrupt+0x151
   4.001e50  ffffbe0c8abd2080 0003ce0 Blocked    nt!EtwpLogger+0xc2
   4.001e84  ffffbe0c8aef8040 0000186 Blocked    nt!KeRemovePriQueue+0x259
   4.001e88  ffffbe0c8aef7040 0000233 Blocked    nt!KeRemovePriQueue+0x259
   4.0012c0  ffffbe0c841a7040 0005c6b Blocked    nt!KeRemovePriQueue+0x259
   4.001904  ffffbe0c8b694080 00025b6 Blocked    nt!EtwpLogger+0xc2
   4.0020e0  ffffbe0c8a197080 00055ae Blocked    nt!EtwpLogger+0xc2
   4.001338  ffffbe0c892c1080 0000137 Blocked    nt!EtwpLogger+0xc2
   4.001f10  ffffbe0c84caa300 0000d2e Blocked    nt!KeRemovePriQueue+0x259
   4.001da0  ffffbe0c8c0dd040 0001177 Blocked    nt!KeRemovePriQueue+0x259

                          [ffffbe0c84136080 Registry]
  64.000068  ffffbe0c84138080 0007437 Blocked    nt!CmpDummyThreadRoutine+0x1e
  64.0001e0  ffffbe0c87f2c080 00000d9 Blocked    nt!CmpLazyWriteWorker+0x47
  64.0001e4  ffffbe0c87f2d080 0000644 Blocked    nt!CmpLazyWriteWorker+0x47
  64.0001e8  ffffbe0c87f2e080 0001599 Blocked    nt!CmpLazyWriteWorker+0x47

                          [ffffbe0c8780f040 smss.exe]

                          [ffffbe0c87f2b080 csrss.exe]
 1fc.00020c  ffffbe0c87d1a580 000003a Blocked    nt!AlpcpWaitForSingleObject+0x3e
 1fc.000228  ffffbe0c887d60c0 00064b3 Blocked    nt!AlpcpSignalAndWait+0x13d
 1fc.000268  ffffbe0c88893080 000019d Blocked    nt!AlpcpWaitForSingleObject+0x3e
 1fc.000278  ffffbe0c888b4080 0000056 Blocked    win32kbase!LegacyInputDispatcher::WaitAndDispatch+0x95
 1fc.00027c  ffffbe0c888b6080 0006544 Blocked    win32kbase!LegacyInputDispatcher::WaitAndDispatch+0x95
 1fc.000cd0  ffffbe0c89a9a080 00001b2 Blocked    nt!AlpcpWaitForSingleObject+0x3e
 1fc.0010ac  ffffbe0c89fb6040 00063ad Blocked    nt!IoRemoveIoCompletion+0x98
 1fc.0026d8  ffffbe0c8bfbc040 0000553 Blocked    nt!IoRemoveIoCompletion+0x98

                          [ffffbe0c887d4080 wininit.exe]
 244.00026c  ffffbe0c888a8040 000212a Blocked    nt!IoRemoveIoCompletion+0x98
 244.000274  ffffbe0c888ab080 0005d0e Blocked    nt!IoRemoveIoCompletion+0x98

[...]

                          [ffffbe0c8c2cd0c0 notmyfault64.e]
243c.001938  ffffbe0c8974f080 0000001 RUNNING    nt!KeBugCheckEx
243c.0024a8  ffffbe0c8b5e0080 0000444 Blocked    nt!IoRemoveIoCompletion+0x98
243c.002484  ffffbe0c8be7c080 0000444 Blocked    nt!IoRemoveIoCompletion+0x98
```

```
                          [ffffbe0c8bfb10c0 SearchHost.exe]
2434.002440  ffffbe0c841d4080 0000333 Blocked    nt!ObWaitForMultipleObjects+0x2d5
2434.002450  ffffbe0c8c2e7080 0000126 Blocked    nt!IoRemoveIoCompletion+0x98
2434.00183c  ffffbe0c8b5eb080 00002cd Blocked    nt!IoRemoveIoCompletion+0x98
2434.00253c  ffffbe0c8b5cd080 0000309 Blocked    nt!ObWaitForSingleObject+0xbb
2434.0022b0  ffffbe0c8a2e9080 00002ff Blocked    nt!ObWaitForMultipleObjects+0x2d5
2434.000b5c  ffffbe0c8c2eb080 0000339 Blocked    nt!ObWaitForMultipleObjects+0x2d5
2434.000814  ffffbe0c8b9d8080 00001f9 Blocked    nt!ObWaitForMultipleObjects+0x2d5
2434.0017c8  ffffbe0c8c164080 0000325 Blocked    nt!ObWaitForMultipleObjects+0x2d5
2434.002438  ffffbe0c8c9cb080 0000309 Blocked    nt!ObWaitForSingleObject+0xbb
2434.000b1c  ffffbe0c89ae9080 00001f9 Blocked    nt!ObWaitForMultipleObjects+0x2d5
2434.000e88  ffffbe0c8b56d040 000023f Blocked    nt!ObWaitForMultipleObjects+0x2d5
2434.0016cc  ffffbe0c8c9a9080 0000166 Blocked    nt!ObWaitForMultipleObjects+0x2d5
2434.000390  ffffbe0c87346080 0000333 Blocked    nt!ObWaitForMultipleObjects+0x2d5
2434.000204  ffffbe0c8b120080 00000cf Blocked    nt!ObWaitForMultipleObjects+0x2d5
2434.0011f4  ffffbe0c8b6a9080 00000cd Blocked    nt!ObWaitForMultipleObjects+0x2d5
2434.000658  ffffbe0c8a346080 00001e0 Blocked    nt!KeWaitForAlertByThreadId+0xc4
2434.00225c  ffffbe0c8978a080 0000328 Blocked    nt!ObWaitForMultipleObjects+0x2d5
2434.002350  ffffbe0c8b535080 00001e0 Blocked    nt!ObWaitForSingleObject+0xbb
2434.001dc4  ffffbe0c8bfc9080 0000236 Blocked    nt!ObWaitForMultipleObjects+0x2d5
2434.001f64  ffffbe0c8b3eb080 0000236 Blocked    nt!ObWaitForMultipleObjects+0x2d5
2434.001764  ffffbe0c8a68f080 000031c Blocked    nt!IoRemoveIoCompletion+0x98
2434.000e18  ffffbe0c8b3e0080 0000216 Blocked    nt!IoRemoveIoCompletion+0x98
2434.0025b0  ffffbe0c8bfd7080 00002c5 Blocked    nt!ObWaitForMultipleObjects+0x2d5
2434.001ca0  ffffbe0c8af29080 0000187 Blocked    nt!ObWaitForMultipleObjects+0x2d5
2434.0018bc  ffffbe0c8a90b080 0000046 Blocked    nt!ObWaitForMultipleObjects+0x2d5
2434.002204  ffffbe0c8c2e8080 0000244 Blocked    nt!ObWaitForMultipleObjects+0x2d5
2434.001308  ffffbe0c8c42b080 000001a Blocked    nt!ObWaitForMultipleObjects+0x2d5
2434.0022ac  ffffbe0c8a43a300 0000314 Blocked    nt!ObWaitForMultipleObjects+0x2d5
2434.002260  ffffbe0c8c9680c0 0000313 Blocked    win32kfull!xxxRealSleepThread+0x2c6
2434.000e28  ffffbe0c8c8cd0c0 000005a Blocked    nt!ObWaitForSingleObject+0xbb
2434.0003fc  ffffbe0c8c8ef0c0 00002eb Blocked    nt!ObWaitForMultipleObjects+0x2d5
2434.0013b0  ffffbe0c8c9460c0 0000187 Blocked    nt!IoRemoveIoCompletion+0x98
2434.0024e4  ffffbe0c8bac6080 000018d Blocked    win32kfull!xxxRealSleepThread+0x2c6
2434.00228c  ffffbe0c8c2ec080 000030c Blocked    nt!ObWaitForMultipleObjects+0x2d5
2434.000e1c  ffffbe0c8b793080 000030c Blocked    nt!ObWaitForMultipleObjects+0x2d5
2434.00210c  ffffbe0c8b69a500 000030b Blocked    win32kfull!xxxRealSleepThread+0x2c6
2434.000e8c  ffffbe0c8b763080 0000187 Blocked    win32kfull!xxxRealSleepThread+0x2c6
2434.0021e8  ffffbe0c8c0de500 000028c Blocked    nt!ObWaitForMultipleObjects+0x2d5
2434.000e40  ffffbe0c8b41e500 0000309 Blocked    nt!AlpcpSignalAndWait+0x13d
2434.0023c0  ffffbe0c8c11e080 000018c Blocked    nt!IoRemoveIoCompletion+0x98
2434.001238  ffffbe0c8bcb9540 0000187 Blocked    nt!ObWaitForMultipleObjects+0x2d5
2434.001c18  ffffbe0c8bad1080 0000306 Blocked    nt!ObWaitForMultipleObjects+0x2d5
2434.000840  ffffbe0c8baea540 0000216 Blocked    nt!IoRemoveIoCompletion+0x98
2434.001804  ffffbe0c8bee0300 000014c Blocked    nt!ObWaitForMultipleObjects+0x2d5
2434.000f24  ffffbe0c8a530540 0000216 Blocked    nt!IoRemoveIoCompletion+0x98
2434.001cd0  ffffbe0c8b511080 0000165 Blocked    nt!ObWaitForMultipleObjects+0x2d5
2434.000410  ffffbe0c894952c0 00002fd Blocked    nt!IoRemoveIoCompletion+0x98
2434.0021e0  ffffbe0c8a404580 00001e0 Blocked    nt!ObWaitForMultipleObjects+0x2d5
2434.0024d0  ffffbe0c8c1110c0 00002f2 Blocked    nt!ObWaitForMultipleObjects+0x2d5
2434.0022bc  ffffbe0c89b93040 000008a Blocked    nt!IoRemoveIoCompletion+0x98
2434.000854  ffffbe0c8a79b080 0000187 Blocked    nt!IoRemoveIoCompletion+0x98
2434.000f84  ffffbe0c8ae6e0c0 00002c8 Blocked    nt!ObWaitForSingleObject+0xbb
2434.000bf4  ffffbe0c8b419080 00002c8 Blocked    nt!AlpcpSignalAndWait+0x13d
2434.001310  ffffbe0c84ca9080 0000219 Blocked    nt!IoRemoveIoCompletion+0x98
2434.000d78  ffffbe0c89d7a080 0000235 Blocked    nt!ObWaitForMultipleObjects+0x2d5
2434.0023b0  ffffbe0c8bfd1080 0000236 Blocked    nt!ObWaitForMultipleObjects+0x2d5
```

```
2434.001c0c  ffffbe0c8c11d080 000018b Blocked    nt!IoRemoveIoCompletion+0x98
2434.001d4c  ffffbe0c8752e040 0000219 Blocked    nt!IoRemoveIoCompletion+0x98
2434.0025bc  ffffbe0c8c2b7080 000023f Blocked    nt!ObWaitForMultipleObjects+0x2d5
2434.0025c0  ffffbe0c8c2b3080 0000236 Blocked    nt!IoRemoveIoCompletion+0x98
2434.000b20  ffffbe0c8c8780c0 000021a Blocked    nt!IoRemoveIoCompletion+0x98
2434.000af4  ffffbe0c8c8130c0 000018b Blocked    nt!IoRemoveIoCompletion+0x98
2434.002240  ffffbe0c8c5ed0c0 0000217 Blocked    nt!IoRemoveIoCompletion+0x98
2434.00250c  ffffbe0c8c8de0c0 000021a Blocked    nt!IoRemoveIoCompletion+0x98
2434.002224  ffffbe0c8c89a0c0 0000218 Blocked    nt!IoRemoveIoCompletion+0x98
2434.00263c  ffffbe0c8c116080 0000216 Blocked    nt!ObWaitForMultipleObjects+0x2d5


Threads Processed: 2109
```

11. Let's now check the processes that were waiting for user input:

```
0: kd> !stacks 2 NtUserGetMessage
Proc.Thread  .Thread  Ticks   ThreadState Blocker
                           [fffff80762d32b00 Idle]
                           [ffffbe0c840eb040 System]

                           [ffffbe0c84136080 Registry]

                           [ffffbe0c8780f040 smss.exe]

                           [ffffbe0c87f2b080 csrss.exe]

                           [ffffbe0c887d4080 wininit.exe]

                           [ffffbe0c888840c0 csrss.exe]

                           [ffffbe0c888c9100 services.exe]

                           [ffffbe0c888cb0c0 lsass.exe]

                           [ffffbe0c888dc080 winlogon.exe]

                           [ffffbe0c889b11c0 fontdrvhost.ex]

                           [ffffbe0c889af1c0 fontdrvhost.ex]

                           [ffffbe0c889ae080 svchost.exe]

                           [ffffbe0c890130c0 WUDFHost.exe]

                           [ffffbe0c889c7080 svchost.exe]

                           [ffffbe0c891020c0 svchost.exe]

                           [ffffbe0c89120080 dwm.exe]
 310.000288  ffffbe0c89121080 0000144 Blocked    nt!KiSwapContext+0x76
                                      nt!KiSwapThread+0x3a7
                                      nt!KiCommitThreadWait+0x159
                                      nt!KeWaitForSingleObject+0x234
                                      nt!KeWaitForMultipleObjects+0x540
                                      win32kfull!xxxRealSleepThread+0x2c6
                                      win32kfull!xxxSleepThread2+0xb3
                                      win32kfull!xxxRealInternalGetMessage+0xc5a
                                      win32kfull!NtUserGetMessage+0x8c
                                      win32k!NtUserGetMessage+0x16
                                      nt!KiSystemServiceCopyEnd+0x25
                                      win32u!NtUserGetMessage+0x14

                           [ffffbe0c891a0080 svchost.exe]

                           [ffffbe0c8919e080 svchost.exe]

                           [ffffbe0c891a80c0 svchost.exe]

                           [ffffbe0c891b90c0 svchost.exe]
```

```
[ffffbe0c891c6080 svchost.exe]
[ffffbe0c89209080 svchost.exe]
[ffffbe0c89241080 svchost.exe]
[ffffbe0c892550c0 svchost.exe]
[ffffbe0c892b6080 svchost.exe]
[ffffbe0c89348080 svchost.exe]
[ffffbe0c8934d080 svchost.exe]
[ffffbe0c89362080 svchost.exe]
[ffffbe0c893bc080 svchost.exe]
[ffffbe0c893bf080 svchost.exe]
[ffffbe0c89363080 svchost.exe]
[ffffbe0c89407080 svchost.exe]
[ffffbe0c8940a080 svchost.exe]
[ffffbe0c841ba080 svchost.exe]
[ffffbe0c841b0080 svchost.exe]
[ffffbe0c84185080 svchost.exe]
[ffffbe0c841ed080 svchost.exe]
[ffffbe0c84135080 svchost.exe]
[ffffbe0c89496080 svchost.exe]
[ffffbe0c895340c0 svchost.exe]
[ffffbe0c89538080 svchost.exe]
[ffffbe0c89596080 svchost.exe]
[ffffbe0c895b3040 MemCompression]
[ffffbe0c895cc080 svchost.exe]
[ffffbe0c895df080 svchost.exe]
[ffffbe0c8963c080 svchost.exe]
[ffffbe0c896b1080 svchost.exe]
[ffffbe0c896d20c0 svchost.exe]
[ffffbe0c89730080 svchost.exe]
[ffffbe0c897450c0 svchost.exe]
[ffffbe0c89728080 svchost.exe]
[ffffbe0c897da080 svchost.exe]
[ffffbe0c897ed0c0 spoolsv.exe]
[ffffbe0c897dc0c0 svchost.exe]
[ffffbe0c89895080 svchost.exe]
[ffffbe0c89a07080 svchost.exe]
[ffffbe0c89a06080 svchost.exe]
[ffffbe0c89042080 svchost.exe]
```

```
                          [ffffbe0c89a0a080 svchost.exe]

                          [ffffbe0c89a8e0c0 svchost.exe]

                          [ffffbe0c89a96080 svchost.exe]

                          [ffffbe0c89aa6080 svchost.exe]

                          [ffffbe0c89aa9080 VGAuthService.]

                          [ffffbe0c89aaa080 vmtoolsd.exe]

                          [ffffbe0c89a42080 MsMpEng.exe]
 ca0.001aec  ffffbe0c89ca5080 0000056 Blocked    nt!KiSwapContext+0x76
                                      nt!KiSwapThread+0x3a7
                                      nt!KiCommitThreadWait+0x159
                                      nt!KeWaitForSingleObject+0x234
                                      nt!KeWaitForMultipleObjects+0x540
                                      win32kfull!xxxRealSleepThread+0x2c6
                                      win32kfull!xxxSleepThread2+0xb3
                                      win32kfull!xxxRealInternalGetMessage+0xc5a
                                      win32kfull!NtUserGetMessage+0x8c
                                      win32k!NtUserGetMessage+0x16
                                      nt!KiSystemServiceCopyEnd+0x25
                                      win32u!NtUserGetMessage+0x14

                          [ffffbe0c89ac10c0 svchost.exe]

                          [ffffbe0c89aae080 svchost.exe]
 cb8.00023c  ffffbe0c8a446080 0001b4d Blocked    nt!KiSwapContext+0x76
                                      nt!KiSwapThread+0x3a7
                                      nt!KiCommitThreadWait+0x159
                                      nt!KeWaitForSingleObject+0x234
                                      nt!KeWaitForMultipleObjects+0x540
                                      win32kfull!xxxRealSleepThread+0x2c6
                                      win32kfull!xxxSleepThread2+0xb3
                                      win32kfull!xxxRealInternalGetMessage+0xc5a
                                      win32kfull!NtUserGetMessage+0x8c
                                      win32k!NtUserGetMessage+0x16
                                      nt!KiSystemServiceCopyEnd+0x25
                                      win32u!NtUserGetMessage+0x14

                          [ffffbe0c899e80c0 svchost.exe]

                          [ffffbe0c89c30080 dllhost.exe]
 f00.000f34  ffffbe0c89c9a080 0001f06 Blocked    nt!KiSwapContext+0x76
                                      nt!KiSwapThread+0x3a7
                                      nt!KiCommitThreadWait+0x159
                                      nt!KeWaitForSingleObject+0x234
                                      nt!KeWaitForMultipleObjects+0x540
                                      win32kfull!xxxRealSleepThread+0x2c6
                                      win32kfull!xxxSleepThread2+0xb3
                                      win32kfull!xxxRealInternalGetMessage+0xc5a
                                      win32kfull!NtUserGetMessage+0x8c
                                      win32k!NtUserGetMessage+0x16
                                      nt!KiSystemServiceCopyEnd+0x25
                                      win32u!NtUserGetMessage+0x14

                          [ffffbe0c89cf8080 AggregatorHost]

                          [ffffbe0c89e840c0 svchost.exe]

                          [ffffbe0c89f5e080 msdtc.exe]

                          [ffffbe0c8a0540c0 svchost.exe]

                          [ffffbe0c8a0cb080 WmiPrvSE.exe]
1278.00127c  ffffbe0c89be30c0 00063ad Blocked    nt!KiSwapContext+0x76
                                      nt!KiSwapThread+0x3a7
                                      nt!KiCommitThreadWait+0x159
                                      nt!KeWaitForSingleObject+0x234
                                      nt!KeWaitForMultipleObjects+0x540
                                      win32kfull!xxxRealSleepThread+0x2c6
                                      win32kfull!xxxSleepThread2+0xb3
                                      win32kfull!xxxRealInternalGetMessage+0xc5a
```

```
                                    win32kfull!NtUserGetMessage+0x8c
                                    win32k!NtUserGetMessage+0x16
                                    nt!KiSystemServiceCopyEnd+0x25
                                    win32u!NtUserGetMessage+0x14

                            [ffffbe0c8a2320c0 sihost.exe]
1160.001330  ffffbe0c8a344080 0001bdd Blocked    nt!KiSwapContext+0x76
                                    nt!KiSwapThread+0x3a7
                                    nt!KiCommitThreadWait+0x159
                                    nt!KeWaitForSingleObject+0x234
                                    nt!KeWaitForMultipleObjects+0x540
                                    win32kfull!xxxRealSleepThread+0x2c6
                                    win32kfull!xxxSleepThread2+0xb3
                                    win32kfull!xxxRealInternalGetMessage+0xc5a
                                    win32kfull!NtUserGetMessage+0x8c
                                    win32k!NtUserGetMessage+0x16
                                    nt!KiSystemServiceCopyEnd+0x25
                                    win32u!NtUserGetMessage+0x14

                            [ffffbe0c898c10c0 svchost.exe]

                            [ffffbe0c8a3340c0 svchost.exe]

                            [ffffbe0c8a0c4080 taskhostw.exe]

                            [ffffbe0c8a337080 taskhostw.exe]
12d0.001854  ffffbe0c8a92b080 000018b Blocked    nt!KiSwapContext+0x76
                                    nt!KiSwapThread+0x3a7
                                    nt!KiCommitThreadWait+0x159
                                    nt!KeWaitForSingleObject+0x234
                                    nt!KeWaitForMultipleObjects+0x540
                                    win32kfull!xxxRealSleepThread+0x2c6
                                    win32kfull!xxxSleepThread2+0xb3
                                    win32kfull!xxxRealInternalGetMessage+0xc5a
                                    win32kfull!NtUserGetMessage+0x8c
                                    win32k!NtUserGetMessage+0x16
                                    nt!KiSystemServiceCopyEnd+0x25
                                    win32u!NtUserGetMessage+0x14

                            [ffffbe0c8a071080 svchost.exe]

                            [ffffbe0c8a4020c0 MsMpEngCP.exe]

                            [ffffbe0c8a43b080 svchost.exe]

                            [ffffbe0c8a454080 userinit.exe]

                            [ffffbe0c8a455080 explorer.exe]
1070.0014e0  ffffbe0c8a5e1080 0000544 Blocked    nt!KiSwapContext+0x76
                                    nt!KiSwapThread+0x3a7
                                    nt!KiCommitThreadWait+0x159
                                    nt!KeWaitForSingleObject+0x234
                                    nt!KeWaitForMultipleObjects+0x540
                                    win32kfull!xxxRealSleepThread+0x2c6
                                    win32kfull!xxxSleepThread2+0xb3
                                    win32kfull!xxxRealInternalGetMessage+0xc5a
                                    win32kfull!NtUserGetMessage+0x8c
                                    win32k!NtUserGetMessage+0x16
                                    nt!KiSystemServiceCopyEnd+0x25
                                    win32u!NtUserGetMessage+0x14
1070.0014e8  ffffbe0c8a5df080 0000157 Blocked    nt!KiSwapContext+0x76
                                    nt!KiSwapThread+0x3a7
                                    nt!KiCommitThreadWait+0x159
                                    nt!KeWaitForSingleObject+0x234
                                    nt!KeWaitForMultipleObjects+0x540
                                    win32kfull!xxxRealSleepThread+0x2c6
                                    win32kfull!xxxSleepThread2+0xb3
                                    win32kfull!xxxRealInternalGetMessage+0xc5a
                                    win32kfull!NtUserGetMessage+0x8c
                                    win32k!NtUserGetMessage+0x16
                                    nt!KiSystemServiceCopyEnd+0x25
                                    win32u!NtUserGetMessage+0x14
1070.001ae4  ffffbe0c8ab4c080 0000544 Blocked    nt!KiSwapContext+0x76
                                    nt!KiSwapThread+0x3a7
                                    nt!KiCommitThreadWait+0x159
                                    nt!KeWaitForSingleObject+0x234
```

```
                                      nt!KeWaitForMultipleObjects+0x540
                                      win32kfull!xxxRealSleepThread+0x2c6
                                      win32kfull!xxxSleepThread2+0xb3
                                      win32kfull!xxxRealInternalGetMessage+0xc5a
                                      win32kfull!NtUserGetMessage+0x8c
                                      win32k!NtUserGetMessage+0x16
                                      nt!KiSystemServiceCopyEnd+0x25
                                      win32u!NtUserGetMessage+0x14
1070.001ae8  ffffbe0c8a74f080 00001cb Blocked    nt!KiSwapContext+0x76
                                      nt!KiSwapThread+0x3a7
                                      nt!KiCommitThreadWait+0x159
                                      nt!KeWaitForSingleObject+0x234
                                      nt!KeWaitForMultipleObjects+0x540
                                      win32kfull!xxxRealSleepThread+0x2c6
                                      win32kfull!xxxSleepThread2+0xb3
                                      win32kfull!xxxRealInternalGetMessage+0xc5a
                                      win32kfull!NtUserGetMessage+0x8c
                                      win32k!NtUserGetMessage+0x16
                                      nt!KiSystemServiceCopyEnd+0x25
                                      win32u!NtUserGetMessage+0x14
1070.001f70  ffffbe0c8b218080 00001c2 Blocked    nt!KiSwapContext+0x76
                                      nt!KiSwapThread+0x3a7
                                      nt!KiCommitThreadWait+0x159
                                      nt!KeWaitForSingleObject+0x234
                                      nt!KeWaitForMultipleObjects+0x540
                                      win32kfull!xxxRealSleepThread+0x2c6
                                      win32kfull!xxxSleepThread2+0xb3
                                      win32kfull!xxxRealInternalGetMessage+0xc5a
                                      win32kfull!NtUserGetMessage+0x8c
                                      win32k!NtUserGetMessage+0x16
                                      nt!KiSystemServiceCopyEnd+0x25
                                      win32u!NtUserGetMessage+0x14
1070.001f80  ffffbe0c8b21c080 0000544 Blocked    nt!KiSwapContext+0x76
                                      nt!KiSwapThread+0x3a7
                                      nt!KiCommitThreadWait+0x159
                                      nt!KeWaitForMultipleObjects+0x2b1
                                      win32kfull!xxxRealSleepThread+0x2c6
                                      win32kfull!xxxSleepThread2+0xb3
                                      win32kfull!xxxRealInternalGetMessage+0xc5a
                                      win32kfull!NtUserGetMessage+0x8c
                                      win32k!NtUserGetMessage+0x16
                                      nt!KiSystemServiceCopyEnd+0x25
                                      win32u!NtUserGetMessage+0x14
1070.001fec  ffffbe0c8af4a080 0000545 Blocked    nt!KiSwapContext+0x76
                                      nt!KiSwapThread+0x3a7
                                      nt!KiCommitThreadWait+0x159
                                      nt!KeWaitForMultipleObjects+0x2b1
                                      win32kfull!xxxRealSleepThread+0x2c6
                                      win32kfull!xxxSleepThread2+0xb3
                                      win32kfull!xxxRealInternalGetMessage+0xc5a
                                      win32kfull!NtUserGetMessage+0x8c
                                      win32k!NtUserGetMessage+0x16
                                      nt!KiSystemServiceCopyEnd+0x25
                                      win32u!NtUserGetMessage+0x14
1070.0017cc  ffffbe0c8942e080 0000545 Blocked    nt!KiSwapContext+0x76
                                      nt!KiSwapThread+0x3a7
                                      nt!KiCommitThreadWait+0x159
                                      nt!KeWaitForMultipleObjects+0x2b1
                                      win32kfull!xxxRealSleepThread+0x2c6
                                      win32kfull!xxxSleepThread2+0xb3
                                      win32kfull!xxxRealInternalGetMessage+0xc5a
                                      win32kfull!NtUserGetMessage+0x8c
                                      win32k!NtUserGetMessage+0x16
                                      nt!KiSystemServiceCopyEnd+0x25
                                      win32u!NtUserGetMessage+0x14
1070.0011a4  ffffbe0c8a2f1080 000050b Blocked    nt!KiSwapContext+0x76
                                      nt!KiSwapThread+0x3a7
                                      nt!KiCommitThreadWait+0x159
                                      nt!KeWaitForMultipleObjects+0x2b1
                                      win32kfull!xxxRealSleepThread+0x2c6
                                      win32kfull!xxxSleepThread2+0xb3
                                      win32kfull!xxxRealInternalGetMessage+0xc5a
                                      win32kfull!NtUserGetMessage+0x8c
                                      win32k!NtUserGetMessage+0x16
                                      nt!KiSystemServiceCopyEnd+0x25
                                      win32u!NtUserGetMessage+0x14
```

```
1070.0018f8  ffffbe0c8bad4080 000046f Blocked    nt!KiSwapContext+0x76
                                     nt!KiSwapThread+0x3a7
                                     nt!KiCommitThreadWait+0x159
                                     nt!KeWaitForSingleObject+0x234
                                     nt!KeWaitForMultipleObjects+0x540
                                     win32kfull!xxxRealSleepThread+0x2c6
                                     win32kfull!xxxSleepThread2+0xb3
                                     win32kfull!xxxRealInternalGetMessage+0xc5a
                                     win32kfull!NtUserGetMessage+0x8c
                                     win32k!NtUserGetMessage+0x16
                                     nt!KiSystemServiceCopyEnd+0x25
                                     win32u!NtUserGetMessage+0x14
1070.002778  ffffbe0c8bed7080 0000446 Blocked    nt!KiSwapContext+0x76
                                     nt!KiSwapThread+0x3a7
                                     nt!KiCommitThreadWait+0x159
                                     nt!KeWaitForSingleObject+0x234
                                     nt!KeWaitForMultipleObjects+0x540
                                     win32kfull!xxxRealSleepThread+0x2c6
                                     win32kfull!xxxSleepThread2+0xb3
                                     win32kfull!xxxRealInternalGetMessage+0xc5a
                                     win32kfull!NtUserGetMessage+0x8c
                                     win32k!NtUserGetMessage+0x16
                                     nt!KiSystemServiceCopyEnd+0x25
                                     win32u!NtUserGetMessage+0x14

                            [ffffbe0c8a4f8080 svchost.exe]

                            [ffffbe0c8a4f7080 svchost.exe]

                            [ffffbe0c8a4ef0c0 svchost.exe]

                            [ffffbe0c8a4e9080 WmiPrvSE.exe]
1590.001594  ffffbe0c8a566080 00063ad Blocked    nt!KiSwapContext+0x76
                                     nt!KiSwapThread+0x3a7
                                     nt!KiCommitThreadWait+0x159
                                     nt!KeWaitForSingleObject+0x234
                                     nt!KeWaitForMultipleObjects+0x540
                                     win32kfull!xxxRealSleepThread+0x2c6
                                     win32kfull!xxxSleepThread2+0xb3
                                     win32kfull!xxxRealInternalGetMessage+0xc5a
                                     win32kfull!NtUserGetMessage+0x8c
                                     win32k!NtUserGetMessage+0x16
                                     nt!KiSystemServiceCopyEnd+0x25
                                     win32u!NtUserGetMessage+0x14
1590.001d30  ffffbe0c8927b080 0005f8c Blocked    nt!KiSwapContext+0x76
                                     nt!KiSwapThread+0x3a7
                                     nt!KiCommitThreadWait+0x159
                                     nt!KeWaitForSingleObject+0x234
                                     nt!KeWaitForMultipleObjects+0x540
                                     win32kfull!xxxRealSleepThread+0x2c6
                                     win32kfull!xxxSleepThread2+0xb3
                                     win32kfull!xxxRealInternalGetMessage+0xc5a
                                     win32kfull!NtUserGetMessage+0x8c
                                     win32k!NtUserGetMessage+0x16
                                     nt!KiSystemServiceCopyEnd+0x25
                                     win32u!NtUserGetMessage+0x14

                            [ffffbe0c8a6c1080 NisSrv.exe]

                            [ffffbe0c8a729080 svchost.exe]

                            [ffffbe0c8a8540c0 SearchIndexer.]

                            [ffffbe0c8a859080 svchost.exe]
1758.0017a0  ffffbe0c8a9020c0 000190b Blocked    nt!KiSwapContext+0x76
                                     nt!KiSwapThread+0x3a7
                                     nt!KiCommitThreadWait+0x159
                                     nt!KeWaitForSingleObject+0x234
                                     nt!KeWaitForMultipleObjects+0x540
                                     win32kfull!xxxRealSleepThread+0x2c6
                                     win32kfull!xxxSleepThread2+0xb3
                                     win32kfull!xxxRealInternalGetMessage+0xc5a
                                     win32kfull!NtUserGetMessage+0x8c
                                     win32k!NtUserGetMessage+0x16
                                     nt!KiSystemServiceCopyEnd+0x25
                                     win32u!NtUserGetMessage+0x14
```

```
                          [ffffbe0c8a9240c0 svchost.exe]

                          [ffffbe0c8a982080 SearchHost.exe]
 49c.00193c  ffffbe0c8abfc080 00062f4 Blocked    nt!KiSwapContext+0x76
                                      nt!KiSwapThread+0x3a7
                                      nt!KiCommitThreadWait+0x159
                                      nt!KeWaitForSingleObject+0x234
                                      nt!KeWaitForMultipleObjects+0x540
                                      win32kfull!xxxRealSleepThread+0x2c6
                                      win32kfull!xxxSleepThread2+0xb3
                                      win32kfull!xxxRealInternalGetMessage+0xc5a
                                      win32kfull!NtUserGetMessage+0x8c
                                      win32k!NtUserGetMessage+0x16
                                      nt!KiSystemServiceCopyEnd+0x25
                                      win32u!NtUserGetMessage+0x14
 49c.001b08  ffffbe0c8a862080 0000c9f Blocked    nt!KiSwapContext+0x76
                                      nt!KiSwapThread+0x3a7
                                      nt!KiCommitThreadWait+0x159
                                      nt!KeWaitForSingleObject+0x234
                                      nt!KeWaitForMultipleObjects+0x540
                                      win32kfull!xxxRealSleepThread+0x2c6
                                      win32kfull!xxxSleepThread2+0xb3
                                      win32kfull!xxxRealInternalGetMessage+0xc5a
                                      win32kfull!NtUserGetMessage+0x8c
                                      win32k!NtUserGetMessage+0x16
                                      nt!KiSystemServiceCopyEnd+0x25
                                      win32u!NtUserGetMessage+0x14
 49c.001b14  ffffbe0c8ad72080 0000ca0 Blocked    nt!KiSwapContext+0x76
                                      nt!KiSwapThread+0x3a7
                                      nt!KiCommitThreadWait+0x159
                                      nt!KeWaitForSingleObject+0x234
                                      nt!KeWaitForMultipleObjects+0x540
                                      win32kfull!xxxRealSleepThread+0x2c6
                                      win32kfull!xxxSleepThread2+0xb3
                                      win32kfull!xxxRealInternalGetMessage+0xc5a
                                      win32kfull!NtUserGetMessage+0x8c
                                      win32k!NtUserGetMessage+0x16
                                      nt!KiSystemServiceCopyEnd+0x25
                                      win32u!NtUserGetMessage+0x14
 49c.001b18  ffffbe0c8ad71080 0000c9a Blocked    nt!KiSwapContext+0x76
                                      nt!KiSwapThread+0x3a7
                                      nt!KiCommitThreadWait+0x159
                                      nt!KeWaitForSingleObject+0x234
                                      nt!KeWaitForMultipleObjects+0x540
                                      win32kfull!xxxRealSleepThread+0x2c6
                                      win32kfull!xxxSleepThread2+0xb3
                                      win32kfull!xxxRealInternalGetMessage+0xc5a
                                      win32kfull!NtUserGetMessage+0x8c
                                      win32k!NtUserGetMessage+0x16
                                      nt!KiSystemServiceCopyEnd+0x25
                                      win32u!NtUserGetMessage+0x14

                          [ffffbe0c8aa020c0 StartMenuExper]

                          [ffffbe0c8a55b0c0 svchost.exe]

                          [ffffbe0c8aaa00c0 RuntimeBroker.]
184c.001c68  ffffbe0c89eb4080 0000544 Blocked    nt!KiSwapContext+0x76
                                      nt!KiSwapThread+0x3a7
                                      nt!KiCommitThreadWait+0x159
                                      nt!KeWaitForSingleObject+0x234
                                      nt!KeWaitForMultipleObjects+0x540
                                      win32kfull!xxxRealSleepThread+0x2c6
                                      win32kfull!xxxSleepThread2+0xb3
                                      win32kfull!xxxRealInternalGetMessage+0xc5a
                                      win32kfull!NtUserGetMessage+0x8c
                                      win32k!NtUserGetMessage+0x16
                                      nt!KiSystemServiceCopyEnd+0x25
                                      win32u!NtUserGetMessage+0x14
184c.000da4  ffffbe0c8b4d4080 0000ccc Blocked    nt!KiSwapContext+0x76
                                      nt!KiSwapThread+0x3a7
                                      nt!KiCommitThreadWait+0x159
                                      nt!KeWaitForSingleObject+0x234
                                      nt!KeWaitForMultipleObjects+0x540
                                      win32kfull!xxxRealSleepThread+0x2c6
```

```
                                    win32kfull!xxxSleepThread2+0xb3
                                    win32kfull!xxxRealInternalGetMessage+0xc5a
                                    win32kfull!NtUserGetMessage+0x8c
                                    win32k!NtUserGetMessage+0x16
                                    nt!KiSystemServiceCopyEnd+0x25
                                    win32u!NtUserGetMessage+0x14

                            [ffffbe0c8ab52080 svchost.exe]

                            [ffffbe0c8aa37080 RuntimeBroker.]
18fc.001b30  ffffbe0c8a055080 0001722 Blocked    nt!KiSwapContext+0x76
                                    nt!KiSwapThread+0x3a7
                                    nt!KiCommitThreadWait+0x159
                                    nt!KeWaitForSingleObject+0x234
                                    nt!KeWaitForMultipleObjects+0x540
                                    win32kfull!xxxRealSleepThread+0x2c6
                                    win32kfull!xxxSleepThread2+0xb3
                                    win32kfull!xxxRealInternalGetMessage+0xc5a
                                    win32kfull!NtUserGetMessage+0x8c
                                    win32k!NtUserGetMessage+0x16
                                    nt!KiSystemServiceCopyEnd+0x25
                                    win32u!NtUserGetMessage+0x14

                            [ffffbe0c8ac07080 svchost.exe]

                            [ffffbe0c8acd6080 dllhost.exe]
19f4.001a44  ffffbe0c8acbd080 0001783 Blocked    nt!KiSwapContext+0x76
                                    nt!KiSwapThread+0x3a7
                                    nt!KiCommitThreadWait+0x159
                                    nt!KeWaitForSingleObject+0x234
                                    nt!KeWaitForMultipleObjects+0x540
                                    win32kfull!xxxRealSleepThread+0x2c6
                                    win32kfull!xxxSleepThread2+0xb3
                                    win32kfull!xxxRealInternalGetMessage+0xc5a
                                    win32kfull!NtUserGetMessage+0x8c
                                    win32k!NtUserGetMessage+0x16
                                    nt!KiSystemServiceCopyEnd+0x25
                                    win32u!NtUserGetMessage+0x14

                            [ffffbe0c8ad94080 svchost.exe]

                            [ffffbe0c8ae6f080 YourPhone.exe]

                            [ffffbe0c8ae72080 ctfmon.exe]

                            [ffffbe0c8ae760c0 svchost.exe]

                            [ffffbe0c8aeeb0c0 TabTip.exe]
1b70.001b7c  ffffbe0c841dc080 000612d Blocked    nt!KiSwapContext+0x76
                                    nt!KiSwapThread+0x3a7
                                    nt!KiCommitThreadWait+0x159
                                    nt!KeWaitForSingleObject+0x234
                                    nt!KeWaitForMultipleObjects+0x540
                                    win32kfull!xxxRealSleepThread+0x2c6
                                    win32kfull!xxxSleepThread2+0xb3
                                    win32kfull!xxxRealInternalGetMessage+0xc5a
                                    win32kfull!NtUserGetMessage+0x8c
                                    win32k!NtUserGetMessage+0x16
                                    nt!KiSystemServiceCopyEnd+0x25
                                    win32u!NtUserGetMessage+0x14

                            [ffffbe0c8ac8e080 WmiApSrv.exe]

                            [ffffbe0c8af240c0 RuntimeBroker.]

                            [ffffbe0c8ac98080 smartscreen.ex]

                            [ffffbe0c84120080 SecurityHealth]
1e28.001e2c  ffffbe0c8abdc080 0000543 Blocked    nt!KiSwapContext+0x76
                                    nt!KiSwapThread+0x3a7
                                    nt!KiCommitThreadWait+0x159
                                    nt!KeWaitForSingleObject+0x234
                                    nt!KeWaitForMultipleObjects+0x540
                                    win32kfull!xxxRealSleepThread+0x2c6
                                    win32kfull!xxxSleepThread2+0xb3
                                    win32kfull!xxxRealInternalGetMessage+0xc5a
```

```
                                    win32kfull!NtUserGetMessage+0x8c
                                    win32k!NtUserGetMessage+0x16
                                    nt!KiSystemServiceCopyEnd+0x25
                                    win32u!NtUserGetMessage+0x14

                            [ffffbe0c8aee1080 SecurityHealth]
1e3c.001ec4  ffffbe0c8ae91080 0000cf8 Blocked    nt!KiSwapContext+0x76
                                    nt!KiSwapThread+0x3a7
                                    nt!KiCommitThreadWait+0x159
                                    nt!KeWaitForSingleObject+0x234
                                    nt!KeWaitForMultipleObjects+0x540
                                    win32kfull!xxxRealSleepThread+0x2c6
                                    win32kfull!xxxSleepThread2+0xb3
                                    win32kfull!xxxRealInternalGetMessage+0xc5a
                                    win32kfull!NtUserGetMessage+0x8c
                                    win32k!NtUserGetMessage+0x16
                                    nt!KiSystemServiceCopyEnd+0x25
                                    win32u!NtUserGetMessage+0x14

                            [ffffbe0c8aedd080 vmtoolsd.exe]

                            [ffffbe0c8b2080c0 ApplicationFra]
1ef8.001f54  ffffbe0c8aa9d080 00004c5 Blocked    nt!KiSwapContext+0x76
                                    nt!KiSwapThread+0x3a7
                                    nt!KiCommitThreadWait+0x159
                                    nt!KeWaitForMultipleObjects+0x2b1
                                    win32kfull!xxxRealSleepThread+0x2c6
                                    win32kfull!xxxSleepThread2+0xb3
                                    win32kfull!xxxRealInternalGetMessage+0xc5a
                                    win32kfull!NtUserGetMessage+0x8c
                                    win32k!NtUserGetMessage+0x16
                                    nt!KiSystemServiceCopyEnd+0x25
                                    win32u!NtUserGetMessage+0x14
1ef8.002394  ffffbe0c8a341080 00004ba Blocked    nt!KiSwapContext+0x76
                                    nt!KiSwapThread+0x3a7
                                    nt!KiCommitThreadWait+0x159
                                    nt!KeWaitForMultipleObjects+0x2b1
                                    win32kfull!xxxRealSleepThread+0x2c6
                                    win32kfull!xxxSleepThread2+0xb3
                                    win32kfull!xxxRealInternalGetMessage+0xc5a
                                    win32kfull!NtUserGetMessage+0x8c
                                    win32k!NtUserGetMessage+0x16
                                    nt!KiSystemServiceCopyEnd+0x25
                                    win32u!NtUserGetMessage+0x14
1ef8.0011c0  ffffbe0c89dea080 0000475 Blocked    nt!KiSwapContext+0x76
                                    nt!KiSwapThread+0x3a7
                                    nt!KiCommitThreadWait+0x159
                                    nt!KeWaitForMultipleObjects+0x2b1
                                    win32kfull!xxxRealSleepThread+0x2c6
                                    win32kfull!xxxSleepThread2+0xb3
                                    win32kfull!xxxRealInternalGetMessage+0xc5a
                                    win32kfull!NtUserGetMessage+0x8c
                                    win32k!NtUserGetMessage+0x16
                                    nt!KiSystemServiceCopyEnd+0x25
                                    win32u!NtUserGetMessage+0x14

                            [ffffbe0c8ad84080 TextInputHost.]

                            [ffffbe0c8af55080 vm3dservice.ex]
1fd8.001fdc  ffffbe0c8911b080 0000544 Blocked    nt!KiSwapContext+0x76
                                    nt!KiSwapThread+0x3a7
                                    nt!KiCommitThreadWait+0x159
                                    nt!KeWaitForSingleObject+0x234
                                    nt!KeWaitForMultipleObjects+0x540
                                    win32kfull!xxxRealSleepThread+0x2c6
                                    win32kfull!xxxSleepThread2+0xb3
                                    win32kfull!xxxRealInternalGetMessage+0xc5a
                                    win32kfull!NtUserGetMessage+0x8c
                                    win32k!NtUserGetMessage+0x16
                                    nt!KiSystemServiceCopyEnd+0x25
                                    win32u!NtUserGetMessage+0x14

                            [ffffbe0c8b49a080 OneDrive.exe]
1188.001a9c  ffffbe0c8b222080 0000543 Blocked    nt!KiSwapContext+0x76
                                    nt!KiSwapThread+0x3a7
                                    nt!KiCommitThreadWait+0x159
```

```
                                    nt!KeWaitForSingleObject+0x234
                                    nt!KeWaitForMultipleObjects+0x540
                                    win32kfull!xxxRealSleepThread+0x2c6
                                    win32kfull!xxxSleepThread2+0xb3
                                    win32kfull!xxxRealInternalGetMessage+0xc5a
                                    win32kfull!NtUserGetMessage+0x8c
                                    win32k!NtUserGetMessage+0x16
                                    nt!KiSystemServiceCopyEnd+0x25
                                    win32u!NtUserGetMessage+0x14
1188.001258  ffffbe0c8b48a080 0005c1a Blocked    nt!KiSwapContext+0x76
                                    nt!KiSwapThread+0x3a7
                                    nt!KiCommitThreadWait+0x159
                                    nt!KeWaitForSingleObject+0x234
                                    nt!KeWaitForMultipleObjects+0x540
                                    win32kfull!xxxRealSleepThread+0x2c6
                                    win32kfull!xxxSleepThread2+0xb3
                                    win32kfull!xxxRealInternalGetMessage+0xc5a
                                    win32kfull!NtUserGetMessage+0x8c
                                    win32k!NtUserGetMessage+0x16
                                    nt!KiSystemServiceCopyEnd+0x25
                                    win32u!NtUserGetMessage+0x14

                            [ffffbe0c8b4e90c0 msedge.exe]

                            [ffffbe0c8b4020c0 Cortana.exe]

                            [ffffbe0c8b417080 RuntimeBroker.]

                            [ffffbe0c8b37b080 svchost.exe]

                            [ffffbe0c8b4b2080 svchost.exe]

                            [ffffbe0c8b092080 svchost.exe]

                            [ffffbe0c876f2080 svchost.exe]

                            [ffffbe0c8b4d6080 svchost.exe]

                            [ffffbe0c89a020c0 Win32Bridge.Se]

                            [ffffbe0c8b5e60c0 SystemSettings]
23a8.0023f8  ffffbe0c8b2ec080 000500c Blocked    nt!KiSwapContext+0x76
                                    nt!KiSwapThread+0x3a7
                                    nt!KiCommitThreadWait+0x159
                                    nt!KeWaitForSingleObject+0x234
                                    nt!KeWaitForMultipleObjects+0x540
                                    win32kfull!xxxRealSleepThread+0x2c6
                                    win32kfull!xxxSleepThread2+0xb3
                                    win32kfull!xxxRealInternalGetMessage+0xc5a
                                    win32kfull!NtUserGetMessage+0x8c
                                    win32k!NtUserGetMessage+0x16
                                    nt!KiSystemServiceCopyEnd+0x25
                                    win32u!NtUserGetMessage+0x14
23a8.000a98  ffffbe0c8a730080 0004ff6 Blocked    nt!KiSwapContext+0x76
                                    nt!KiSwapThread+0x3a7
                                    nt!KiCommitThreadWait+0x159
                                    nt!KeWaitForSingleObject+0x234
                                    nt!KeWaitForMultipleObjects+0x540
                                    win32kfull!xxxRealSleepThread+0x2c6
                                    win32kfull!xxxSleepThread2+0xb3
                                    win32kfull!xxxRealInternalGetMessage+0xc5a
                                    win32kfull!NtUserGetMessage+0x8c
                                    win32k!NtUserGetMessage+0x16
                                    nt!KiSystemServiceCopyEnd+0x25
                                    win32u!NtUserGetMessage+0x14

                            [ffffbe0c8b8870c0 svchost.exe]

                            [ffffbe0c8b4b60c0 UserOOBEBroker]
1414.0012cc  ffffbe0c89aea080 0004faf Blocked    nt!KiSwapContext+0x76
                                    nt!KiSwapThread+0x3a7
                                    nt!KiCommitThreadWait+0x159
                                    nt!KeWaitForSingleObject+0x234
                                    nt!KeWaitForMultipleObjects+0x540
                                    win32kfull!xxxRealSleepThread+0x2c6
                                    win32kfull!xxxSleepThread2+0xb3
```

```
                                    win32kfull!xxxRealInternalGetMessage+0xc5a
                                    win32kfull!NtUserGetMessage+0x8c
                                    win32k!NtUserGetMessage+0x16
                                    nt!KiSystemServiceCopyEnd+0x25
                                    win32u!NtUserGetMessage+0x14

                            [ffffbe0c876f8080 SgrmBroker.exe]

                            [ffffbe0c892bc080 svchost.exe]

                            [ffffbe0c89a9b080 svchost.exe]

                            [ffffbe0c8b3d5080 svchost.exe]

                            [ffffbe0c8b4d80c0 msedge.exe]
 f0c.000f10  ffffbe0c87608080 0002b3f Blocked    nt!KiSwapContext+0x76
                                    nt!KiSwapThread+0x3a7
                                    nt!KiCommitThreadWait+0x159
                                    nt!KeWaitForSingleObject+0x234
                                    nt!KeWaitForMultipleObjects+0x540
                                    win32kfull!xxxRealSleepThread+0x2c6
                                    win32kfull!xxxSleepThread2+0xb3
                                    win32kfull!xxxRealInternalGetMessage+0xc5a
                                    win32kfull!NtUserGetMessage+0x8c
                                    win32k!NtUserGetMessage+0x16
                                    nt!KiSystemServiceCopyEnd+0x25
                                    win32u!NtUserGetMessage+0x14

                            [ffffbe0c8ad810c0 msedge.exe]
1e8c.000a14  ffffbe0c8a2f3080 0000544 Blocked    nt!KiSwapContext+0x76
                                    nt!KiSwapThread+0x3a7
                                    nt!KiCommitThreadWait+0x159
                                    nt!KeWaitForSingleObject+0x234
                                    nt!KeWaitForMultipleObjects+0x540
                                    win32kfull!xxxRealSleepThread+0x2c6
                                    win32kfull!xxxRealInternalGetMessage+0x14ff
                                    win32kfull!NtUserGetMessage+0x8c
                                    win32k!NtUserGetMessage+0x16
                                    nt!KiSystemServiceCopyEnd+0x25
                                    win32u!NtUserGetMessage+0x14

                            [ffffbe0c8b0d60c0 msedge.exe]

                            [ffffbe0c8cce90c0 msedge.exe]

                            [ffffbe0c8b224080 msedge.exe]

                            [ffffbe0c8b6960c0 msedge.exe]

                            [ffffbe0c8b3960c0 identity_helpe]

                            [ffffbe0c8b5b30c0 msedge.exe]

                            [ffffbe0c8af460c0 msedge.exe]

                            [ffffbe0c8b0e20c0 MiniSearchHost]

                            [ffffbe0c870210c0 Notepad.exe]
1b24.0010b4  ffffbe0c89789080 0000020 Blocked    nt!KiSwapContext+0x76
                                    nt!KiSwapThread+0x3a7
                                    nt!KiCommitThreadWait+0x159
                                    nt!KeWaitForSingleObject+0x234
                                    nt!KeWaitForMultipleObjects+0x540
                                    win32kfull!xxxRealSleepThread+0x2c6
                                    win32kfull!xxxSleepThread2+0xb3
                                    win32kfull!xxxRealInternalGetMessage+0xc5a
                                    win32kfull!NtUserGetMessage+0x8c
                                    win32k!NtUserGetMessage+0x16
                                    nt!KiSystemServiceCopyEnd+0x25
                                    win32u!NtUserGetMessage+0x14

                            [ffffbe0c876480c0 dllhost.exe]
22a8.0018e8  ffffbe0c8b6af300 00001a5 Blocked    nt!KiSwapContext+0x76
                                    nt!KiSwapThread+0x3a7
                                    nt!KiCommitThreadWait+0x159
                                    nt!KeWaitForSingleObject+0x234
```

```
                                    nt!KeWaitForMultipleObjects+0x540
                                    win32kfull!xxxRealSleepThread+0x2c6
                                    win32kfull!xxxSleepThread2+0xb3
                                    win32kfull!xxxRealInternalGetMessage+0xc5a
                                    win32kfull!NtUserGetMessage+0x8c
                                    win32k!NtUserGetMessage+0x16
                                    nt!KiSystemServiceCopyEnd+0x25
                                    win32u!NtUserGetMessage+0x14

                            [ffffbe0c84caf080 CalculatorApp.]

                            [ffffbe0c8b538080 RuntimeBroker.]
 ce8.00084c  ffffbe0c8a7b2080 0001ebb Blocked    nt!KiSwapContext+0x76
                                    nt!KiSwapThread+0x3a7
                                    nt!KiCommitThreadWait+0x159
                                    nt!KeWaitForSingleObject+0x234
                                    nt!KeWaitForMultipleObjects+0x540
                                    win32kfull!xxxRealSleepThread+0x2c6
                                    win32kfull!xxxSleepThread2+0xb3
                                    win32kfull!xxxRealInternalGetMessage+0xc5a
                                    win32kfull!NtUserGetMessage+0x8c
                                    win32k!NtUserGetMessage+0x16
                                    nt!KiSystemServiceCopyEnd+0x25
                                    win32u!NtUserGetMessage+0x14

                            [ffffbe0c8be620c0 wordpad.exe]
1d98.001bb0  ffffbe0c8beda080 0000020 Blocked    nt!KiSwapContext+0x76
                                    nt!KiSwapThread+0x3a7
                                    nt!KiCommitThreadWait+0x159
                                    nt!KeWaitForSingleObject+0x234
                                    nt!KeWaitForMultipleObjects+0x540
                                    win32kfull!xxxRealSleepThread+0x2c6
                                    win32kfull!xxxSleepThread2+0xb3
                                    win32kfull!xxxRealInternalGetMessage+0xc5a
                                    win32kfull!NtUserGetMessage+0x8c
                                    win32k!NtUserGetMessage+0x16
                                    nt!KiSystemServiceCopyEnd+0x25
                                    +0x7ffe5ac81424

                            [ffffbe0c8bed8080 splwow64.exe]

                            [ffffbe0c84c990c0 svchost.exe]

                            [ffffbe0c8be760c0 svchost.exe]

                            [ffffbe0c8a7a6080 LINQPad7.exe]

                            [ffffbe0c8b318080 LINQPad7.Query]

                            [ffffbe0c8c9d3080 cmd.exe]

                            [ffffbe0c8b317080 conhost.exe]
2568.002594  ffffbe0c8b537080 0000020 Blocked    nt!KiSwapContext+0x76
                                    nt!KiSwapThread+0x3a7
                                    nt!KiCommitThreadWait+0x159
                                    nt!KeWaitForSingleObject+0x234
                                    nt!KeWaitForMultipleObjects+0x540
                                    win32kfull!xxxRealSleepThread+0x2c6
                                    win32kfull!xxxSleepThread2+0xb3
                                    win32kfull!xxxRealInternalGetMessage+0xc5a
                                    win32kfull!NtUserGetMessage+0x8c
                                    win32k!NtUserGetMessage+0x16
                                    nt!KiSystemServiceCopyEnd+0x25
                                    win32u!NtUserGetMessage+0x14

                            [ffffbe0c877ec080 Taskmgr.exe]

                            [ffffbe0c8c2de0c0 audiodg.exe]

                            [ffffbe0c8c5760c0 TabTip.exe]

                            [ffffbe0c8c2cd0c0 notmyfault64.e]

                            [ffffbe0c8bfb10c0 SearchHost.exe]
2434.002260  ffffbe0c8c9680c0 0000313 Blocked    nt!KiSwapContext+0x76
                                    nt!KiSwapThread+0x3a7
```

```
                                       nt!KiCommitThreadWait+0x159
                                       nt!KeWaitForSingleObject+0x234
                                       nt!KeWaitForMultipleObjects+0x540
                                       win32kfull!xxxRealSleepThread+0x2c6
                                       win32kfull!xxxSleepThread2+0xb3
                                       win32kfull!xxxRealInternalGetMessage+0xc5a
                                       win32kfull!NtUserGetMessage+0x8c
                                       win32k!NtUserGetMessage+0x16
                                       nt!KiSystemServiceCopyEnd+0x25
                                       win32u!NtUserGetMessage+0x14
                                       user32!GetMessageW+0x2e
                                       edgehtml!CIndependentHitTestManager::IndependentHitTestThreadProc+0xa8
                                       KERNEL32!BaseThreadInitThunk+0x10
                                       ntdll!RtlUserThreadStart+0x2b
2434.0024e4  ffffbe0c8bac6080 000018d Blocked    nt!KiSwapContext+0x76
                                       nt!KiSwapThread+0x3a7
                                       nt!KiCommitThreadWait+0x159
                                       nt!KeWaitForSingleObject+0x234
                                       nt!KeWaitForMultipleObjects+0x540
                                       win32kfull!xxxRealSleepThread+0x2c6
                                       win32kfull!xxxSleepThread2+0xb3
                                       win32kfull!xxxRealInternalGetMessage+0xc5a
                                       win32kfull!NtUserGetMessage+0x8c
                                       win32k!NtUserGetMessage+0x16
                                       nt!KiSystemServiceCopyEnd+0x25
                                       win32u!NtUserGetMessage+0x14
                                       user32!GetMessageW+0x2e
                                       WebRuntimeManager!LCIEWWAServiceWorkerGlobalScopeHost::ThreadProc+0x7f
                                       edgeiso!_IsoThreadProc_WrapperToReleaseScope+0x20
                                       KERNEL32!BaseThreadInitThunk+0x10
                                       ntdll!RtlUserThreadStart+0x2b
2434.00210c  ffffbe0c8b69a500 000030b Blocked    nt!KiSwapContext+0x76
                                       nt!KiSwapThread+0x3a7
                                       nt!KiCommitThreadWait+0x159
                                       nt!KeWaitForSingleObject+0x234
                                       nt!KeWaitForMultipleObjects+0x540
                                       win32kfull!xxxRealSleepThread+0x2c6
                                       win32kfull!xxxSleepThread2+0xb3
                                       win32kfull!xxxRealInternalGetMessage+0xc5a
                                       win32kfull!NtUserGetMessage+0x8c
                                       win32k!NtUserGetMessage+0x16
                                       nt!KiSystemServiceCopyEnd+0x25
                                       win32u!NtUserGetMessage+0x14
                                       user32!GetMessageW+0x2e
                                       edgehtml!CRawInput::RawInputThreadProc+0x50
                                       KERNEL32!BaseThreadInitThunk+0x10
                                       ntdll!RtlUserThreadStart+0x2b
2434.000e8c  ffffbe0c8b763080 0000187 Blocked    nt!KiSwapContext+0x76
                                       nt!KiSwapThread+0x3a7
                                       nt!KiCommitThreadWait+0x159
                                       nt!KeWaitForSingleObject+0x234
                                       nt!KeWaitForMultipleObjects+0x540
                                       win32kfull!xxxRealSleepThread+0x2c6
                                       win32kfull!xxxSleepThread2+0xb3
                                       win32kfull!xxxRealInternalGetMessage+0xc5a
                                       win32kfull!NtUserGetMessage+0x8c
                                       win32k!NtUserGetMessage+0x16
                                       nt!KiSystemServiceCopyEnd+0x25
                                       win32u!NtUserGetMessage+0x14
                                       user32!GetMessageW+0x2e
                                       edgehtml!WorkerGlobalScopeThread::RunMessageLoopForSTA+0x29
                                       edgehtml!WorkerGlobalScopeThread::RunMessageLoop+0x6e
                                       edgehtml!WorkerGlobalScopeThread::RunWorkerGlobalScope+0x74
                                       edgehtml!WorkerGlobalScopeThread::RunThread+0x7f
                                       edgehtml!WorkerGlobalScopeThread::ThreadProc+0x1f
                                       KERNEL32!BaseThreadInitThunk+0x10
                                       ntdll!RtlUserThreadStart+0x2b


Threads Processed: 2109
```

Note: However, if we try to search for *ReadConsole* input threads using the **!stacks** command, we would fail since the command doesn't switch to proper process context to show correct user space thread stacks, for example, having them truncated as highlighted in red for *conhost.exe* and *wordpad.exe*. In the output for *SearchHost.exe,* we accidentally have the correct stack trace because of the previous script that set the correct context for the last process in the list. To search for *ReadConsole* threads, we can use the MEX extension command:

```
0: kd> !mex.us -a ReadConsole
Unable to load image C:\Program Files\VMware\VMware Tools\glib-2.0.dll, Win32 error 0n2
Unable to load image C:\Program Files\VMware\VMware Tools\vmtoolsd.exe, Win32 error 0n2
Unable to load image C:\Program Files\VMware\VMware Tools\plugins\vmsvc\hwUpgradeHelper.dll, Win32 error 0n2
Unable to load image C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{B3AF7FFC-0739-417C-99AE-
D5D78FD8A0CE}\mpengine.dll, Win32 error 0n2
Unable to load image c:\windows\system32\appxdeploymentserver.dll, Win32 error 0n2
Unable to load image C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{B3AF7FFC-0739-417C-99AE-
D5D78FD8A0CE}\mpengine.dll, Win32 error 0n2
Unable to load image C:\ProgramData\Microsoft\Windows Defender\Scans\MsMpEngCP.exe, Win32 error 0n2
Unable to load image C:\Program Files\VMware\VMware Tools\plugins\vmusr\unity.dll, Win32 error 0n2
Unable to load image C:\Program Files\VMware\VMware Tools\plugins\vmusr\dndcp.dll, Win32 error 0n2
Unable to load image C:\Program Files\VMware\VMware Tools\plugins\vmusr\desktopEvents.dll, Win32 error 0n2
Unable to load image C:\Program Files\VMware\VMware Tools\glib-2.0.dll, Win32 error 0n2
Unable to load image C:\Windows\System32\vm3dservice.exe, Win32 error 0n2
Unable to load image C:\Users\dumpa\AppData\Local\Microsoft\OneDrive\22.002.0103.0004\SyncEngine.DLL, Win32 error 0n2
Unable to load image C:\Users\dumpa\AppData\Local\Microsoft\OneDrive\22.002.0103.0004\FileSyncClient.dll, Win32 error
0n2
Unable to load image C:\Users\dumpa\AppData\Local\Microsoft\OneDrive\22.002.0103.0004\OneDriveTelemetryStable.dll,
Win32 error 0n2
Unable to load image C:\Users\dumpa\AppData\Local\Microsoft\OneDrive\22.002.0103.0004\LoggingPlatform.dll, Win32 error
0n2
Unable to load image C:\Program Files (x86)\Microsoft\Edge\Application\97.0.1072.76\oneds.dll, Win32 error 0n2
Unable to load image C:\Program Files (x86)\Microsoft\Edge\Application\97.0.1072.76\msedge.dll, Win32 error 0n2
Unable to load image C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe, Win32 error 0n2
Unable to load image C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe, Win32 error 0n2
Unable to load image C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe, Win32 error 0n2
Unable to load image C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe, Win32 error 0n2
Unable to load image C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe, Win32 error 0n2
*** WARNING: Unable to verify checksum for Notepad.exe
Unable to load image C:\Program
Files\WindowsApps\Microsoft.WindowsCalculator_11.2110.4.0_x64__8wekyb3d8bbwe\CalculatorApp.dll, Win32 error 0n2
*** WARNING: Unable to verify checksum for CalculatorApp.dll
Unable to load image C:\Program Files
(x86)\Microsoft\EdgeWebView\Application\97.0.1072.76\EBWebView\x64\EmbeddedBrowserWebView.dll, Win32 error 0n2
*** WARNING: Unable to verify checksum for System.Windows.Forms.Primitives.dll
*** WARNING: Unable to verify checksum for System.Windows.Forms.dll
*** WARNING: Unable to verify checksum for Microsoft.Win32.SystemEvents.dll
Process: cmd.exe @ ffffbe0c8c9d3080
============================================================
1 thread: ffffbe0c8c9aa080
    fffff8076241dce6 nt!KiSwapContext+0x76
    fffff807623327f7 nt!KiSwapThread+0x3a7
    fffff807623346a9 nt!KiCommitThreadWait+0x159
    fffff8076232e5c4 nt!KeWaitForSingleObject+0x234
    fffff8076276bd67 nt!IopSynchronousServiceTail+0x347
    fffff8076276b9d2 nt!IopXxxControlFile+0xc82
    fffff8076276ad36 nt!NtDeviceIoControlFile+0x56
    fffff80762428775 nt!KiSystemServiceCopyEnd+0x25
    00007ffe5b023834 ntdll!NtDeviceIoControlFile+0x14
    00007ffe58a25845 KERNELBASE!ConsoleCallServerGeneric+0xe9
    00007ffe58aad6bd KERNELBASE!ReadConsoleInternal+0x18d
    00007ffe58aad51a KERNELBASE!ReadConsoleW+0x1a
    00007ff66133ca6f cmd!ReadBufFromConsole+0x127
    00007ff661332202 cmd!FillBuf+0x11c82
    00007ff6613200fc cmd!Lex+0x4fc
    00007ff66131f2c6 cmd!GeToken+0x26
    00007ff66131f023 cmd!Parser+0x113
    00007ff66133384c cmd!main+0xf390
    00007ff6613298e1 cmd!__mainCRTStartup+0x161
    00007ffe5a2d54e0 KERNEL32!BaseThreadInitThunk+0x10
    00007ffe5af8485b ntdll!RtlUserThreadStart+0x2b

Threads matching filter: 1 out of 1

Unable to load image C:\Work\notmyfault64.exe, Win32 error 0n2
```

The command can also search for exception or bugcheck processing threads and also for non-waiting threads:

```
0: kd> !mex.us -a -crash
Unable to load image C:\Program Files\VMware\VMware Tools\glib-2.0.dll, Win32 error 0n2
Unable to load image C:\Program Files\VMware\VMware Tools\vmtoolsd.exe, Win32 error 0n2
Unable to load image C:\Program Files\VMware\VMware Tools\plugins\vmsvc\hwUpgradeHelper.dll, Win32 error 0n2
Unable to load image C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{B3AF7FFC-0739-417C-99AE-D5D78FD8A0CE}\mpengine.dll, Win32 error 0n2
Unable to load image c:\windows\system32\appxdeploymentserver.dll, Win32 error 0n2
Unable to load image C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{B3AF7FFC-0739-417C-99AE-D5D78FD8A0CE}\mpengine.dll, Win32 error 0n2
Unable to load image C:\ProgramData\Microsoft\Windows Defender\Scans\MsMpEngCP.exe, Win32 error 0n2
Unable to load image C:\Windows\System32\sppc.dll, Win32 error 0n2
Unable to load image C:\WINDOWS\SYSTEM32\SPPC.DLL, Win32 error 0n2
Unable to load image C:\Program Files\VMware\VMware Tools\plugins\vmusr\unity.dll, Win32 error 0n2
Unable to load image C:\Program Files\VMware\VMware Tools\plugins\vmusr\dndcp.dll, Win32 error 0n2
Unable to load image C:\Program Files\VMware\VMware Tools\plugins\vmusr\desktopEvents.dll, Win32 error 0n2
Unable to load image C:\Program Files\VMware\VMware Tools\glib-2.0.dll, Win32 error 0n2
Unable to load image C:\Windows\System32\vm3dservice.exe, Win32 error 0n2
Unable to load image C:\Users\dumpa\AppData\Local\Microsoft\OneDrive\22.002.0103.0004\SyncEngine.DLL, Win32 error 0n2
Unable to load image C:\Users\dumpa\AppData\Local\Microsoft\OneDrive\22.002.0103.0004\FileSyncClient.dll, Win32 error 0n2
Unable to load image C:\Users\dumpa\AppData\Local\Microsoft\OneDrive\22.002.0103.0004\OneDriveTelemetryStable.dll, Win32 error 0n2
Unable to load image C:\Users\dumpa\AppData\Local\Microsoft\OneDrive\22.002.0103.0004\LoggingPlatform.dll, Win32 error 0n2
Unable to load image C:\Program Files (x86)\Microsoft\Edge\Application\97.0.1072.76\oneds.dll, Win32 error 0n2
Unable to load image C:\Program Files (x86)\Microsoft\Edge\Application\97.0.1072.76\msedge.dll, Win32 error 0n2
Unable to load image C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe, Win32 error 0n2
Unable to load image C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe, Win32 error 0n2
Unable to load image C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe, Win32 error 0n2
Unable to load image C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe, Win32 error 0n2
Unable to load image C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe, Win32 error 0n2
Unable to load image C:\Program Files\WindowsApps\Microsoft.WindowsNotepad_10.2103.6.0_x64__8wekyb3d8bbwe\Notepad\Notepad.exe, Win32 error 0n2
*** WARNING: Unable to verify checksum for Notepad.exe
Unable to load image C:\Program Files\WindowsApps\Microsoft.WindowsCalculator_11.2110.4.0_x64__8wekyb3d8bbwe\CalculatorApp.dll, Win32 error 0n2
*** WARNING: Unable to verify checksum for CalculatorApp.dll
Unable to load image C:\Program Files (x86)\Microsoft\EdgeWebView\Application\97.0.1072.76\EBWebView\x64\EmbeddedBrowserWebView.dll, Win32 error 0n2
*** WARNING: Unable to verify checksum for System.Windows.Forms.Primitives.dll
*** WARNING: Unable to verify checksum for System.Windows.Forms.dll
*** WARNING: Unable to verify checksum for Microsoft.Win32.SystemEvents.dll
Unable to load image C:\Work\notmyfault64.exe, Win32 error 0n2
Process: notmyfault64.exe @ ffffbe0c8c2cd0c0
============================================================
1 thread: ffffbe0c8974f080
    fffff80762416220 nt!KeBugCheckEx
    fffff80762428da9 nt!KiBugCheckDispatch+0x69
    fffff80762424f00 nt!KiPageFault+0x440
    fffff80761781530 myfault+0x1530
    fffff80761781e2d myfault+0x1e2d
    fffff80761781f88 myfault+0x1f88
    fffff80762303115 nt!IofCallDriver+0x55
    fffff8076276bbf2 nt!IopSynchronousServiceTail+0x1d2
    fffff8076276b9d2 nt!IopXxxControlFile+0xc82
    fffff8076276ad36 nt!NtDeviceIoControlFile+0x56
    fffff80762428775 nt!KiSystemServiceCopyEnd+0x25
    00007ffe5b023834 ntdll!NtDeviceIoControlFile+0x14
    00007ffe58a33ffb KERNELBASE!DeviceIoControl+0x6b
    00007ffe5a2d5f91 KERNEL32!DeviceIoControlImplementation+0x81
    00007ff72c0426ce notmyfault64+0x26ce
    00007ffe5901484b USER32!UserCallDlgProcCheckWow+0x14b
    00007ffe5901409b USER32!DefDlgProcWorker+0xcb
    00007ffe590597c9 USER32!DefDlgProcA+0x39
    00007ffe59011c4c USER32!UserCallWinProcCheckWow+0x33c
    00007ffe5901179c USER32!DispatchClientMessage+0x9c
    00007ffe59024b4d USER32!_fnDWORD+0x3d
    00007ffe5b0276a4 ntdll!KiUserCallbackDispatcherContinue
    00007ffe58d81434 win32u!NtUserMessageCall+0x14
    00007ffe590108cf USER32!SendMessageWorker+0x12f
    00007ffe59010737 USER32!SendMessageW+0x137
    00007ffe444750bf COMCTL32!Button_ReleaseCapture+0xbb
    00007ffe444a8822 COMCTL32!Button_WndProc+0x802
    00007ffe59011c4c USER32!UserCallWinProcCheckWow+0x33c
    00007ffe59010ea6 USER32!DispatchMessageWorker+0x2a6
    00007ffe59016084 USER32!IsDialogMessageW+0x104
    00007ffe44455f9f COMCTL32!Prop_IsDialogMessage+0x4b
    00007ffe44455e48 COMCTL32!_RealPropertySheet+0x2c0
    00007ffe44455abd COMCTL32!_PropertySheet+0x49
    00007ffe44520953 COMCTL32!PropertySheetA+0x53
```

```
    00007ff72c043415 notmyfault64+0x3415
    00007ff72c045c68 notmyfault64+0x5c68
    00007ffe5a2d54e0 KERNEL32!BaseThreadInitThunk+0x10
    00007ffe5af8485b ntdll!RtlUserThreadStart+0x2b

Threads matching filter: 1 out of 3

0: kd> !mex.us -a -nw
Process: Idle @ fffff80762d32b00
============================================================
2 threads: ffffbe0c84178080 ffffbe0c841ab080
    fffff8076241dce6 nt!KiSwapContext+0x76
    fffff807623327f7 nt!KiSwapThread+0x3a7
    fffff807623be9ac nt!KiExecuteDpcDelegate+0x5c
    fffff8076241a2d4 nt!KiStartSystemThread+0x34

Threads matching filter: 2 out of 4

Process: System @ ffffbe0c840eb040
============================================================
1 thread: ffffbe0c8ac5c080
    fffff8076241df31 nt!KxDispatchInterrupt+0x151
    fffff8076241d3b6 nt!KiDpcInterrupt+0x326
    fffff807626ccc61 nt!PfTCreateTraceDump+0x1c1
    fffff807626cca66 nt!PfTGenerateTrace+0x16
    fffff8076286b763 nt!PfTLoggingWorker+0x183
    fffff807622478f5 nt!PspSystemThreadStartup+0x55
    fffff8076241a2d4 nt!KiStartSystemThread+0x34

2 threads: ffffbe0c84167080 ffffbe0c841de080
    fffff8076241dce6 nt!KiSwapContext+0x76
    fffff807623327f7 nt!KiSwapThread+0x3a7
    fffff807623346a9 nt!KiCommitThreadWait+0x159
    fffff807622548cf nt!KeWaitForGate+0xcf
    fffff807623c7222 nt!KiExecuteDpc+0x92
    fffff807622478f5 nt!PspSystemThreadStartup+0x55
    fffff8076241a2d4 nt!KiStartSystemThread+0x34

28 threads: ffffbe0c84153080 ffffbe0c84b47040 ffffbe0c84b44040 ffffbe0c841a7040 ffffbe0c8477e080 ffffbe0c89aed040
ffffbe0c8974a040 ffffbe0c87d4c040 ffffbe0c898ca040 ffffbe0c8c0dd040 ...
    fffff8076241dce6 nt!KiSwapContext+0x76
    fffff807623327f7 nt!KiSwapThread+0x3a7
    fffff807623346a9 nt!KiCommitThreadWait+0x159
    fffff8076231d989 nt!KeRemovePriQueue+0x259
    fffff8076231d2e3 nt!ExpWorkerThread+0xd3
    fffff807622478f5 nt!PspSystemThreadStartup+0x55
    fffff8076241a2d4 nt!KiStartSystemThread+0x34

Threads matching filter: 31 out of 136

Process: dwm.exe @ ffffbe0c89120080
============================================================
1 thread: ffffbe0c89190080
    00007ffe552d2700 CoreMessaging!AlpcClientConnection::PendingPortCheck
    00007ffe552d22e4 CoreMessaging!`CFlat::DelegateImpl<System::Action,0,void
__cdecl(void),void,0>::Bind<CFlat::SmartPtr<Microsoft::CoreUI::Messaging::CrossProcessReceivePort$AlpcReceiveSource>,&
Microsoft::CoreUI::Messaging::CrossProcessReceivePort$AlpcReceiveSource::ScheduleReceiveIfNeeded>'::`2'::Thunk::Invoke
+0x24
    00007ffe552aae27 CoreMessaging!CFlat::DelegateImpl<System::Action,0,void
__cdecl(void),void,0>::MulticastInvoke+0x47
    00007ffe552ca6f6 CoreMessaging!Microsoft::CoreUI::Dispatch::EventLoop::CallYieldCheckHandler+0xa2
    00007ffe552ff321 CoreMessaging!Microsoft::CoreUI::Dispatch::Dispatcher::PeekNextItem+0x26355
    00007ffe552aa4bd CoreMessaging!Microsoft::CoreUI::Dispatch::EventLoop::Callback_RunCoreLoop+0x1ed
    00007ffe552a70ba CoreMessaging!Microsoft::CoreUI::Dispatch::Win32EventLoopBridge::Callback_Run+0x41a
    00007ffe552d280e CoreMessaging!Microsoft::CoreUI::Dispatch::EventLoop::Callback_Run+0xae
    00007ffe55290dcf CoreMessaging!Microsoft::CoreUI::IExportMessageLoopExtensions::ExportAdapter$::Run+0x19f
    00007ffe54e698c9 dwmcore!CComposition::ProcessBatches+0xb1
    00007ffe54e6999b dwmcore!CComposition::PreRender+0x77
    00007ffe54e691c2 dwmcore!CComposition::ProcessComposition+0x4a
    00007ffe54e682c7 dwmcore!CPartitionVerticalBlankScheduler::Render+0x5b
    00007ffe54e67876 dwmcore!CPartitionVerticalBlankScheduler::ProcessFrame+0x102
    00007ffe54e6684f dwmcore!CPartitionVerticalBlankScheduler::ScheduleAndProcessFrame+0x8f
    00007ffe54eed3a6 dwmcore!CConnection::MainCompositionThreadLoop+0xba
    00007ffe54eed2d6 dwmcore!CConnection::RunCompositionThread+0xfa
```

```
    00007ffe5a2d54e0 KERNEL32!BaseThreadInitThunk+0x10
    00007ffe5af8485b ntdll!RtlUserThreadStart+0x2b

Threads matching filter: 1 out of 17
3 stack(s) were not displayed because we could not switch to thread context, or stack trace was empty

Process: explorer.exe @ ffffbe0c8a455080
============================================================
1 thread: ffffbe0c8a5dd080
    fffff8076241df31 nt!KxDispatchInterrupt+0x151
    fffff8076241d5d5 nt!KiDpcInterruptBypass+0x25
    fffff80762418471 nt!KiInterruptDispatchNoLockNoEtw+0xb1
    fffff807624285d5 nt!KiSystemServiceUser+0xbb
    00007ffe5b027104 ntdll!NtTraceControl+0x14
    00007ffe5afde2e7 ntdll!EtwEventActivityIdControl+0x87
    00007ffe566a1c26 windows_storage!SHILAliasTranslate+0x1c6
    00007ffe56b5655b windows_storage!SHLogILFromFSIL+0x1b
    00007ffe3223a43a windows_storage_search!CGrepQuery::_IsNotExcludedFolder+0x8a
    00007ffe3223a7c8 windows_storage_search!CGrepQuery::_ShouldCrawlItem+0xfc
    00007ffe322390fd windows_storage_search!CGrepQuery::_CheckRecurseIntoFolder+0x15
    00007ffe321feec3 windows_storage_search!CGrepQuery::CrawlForNextItemImpl+0x321e3
    00007ffe321f882d windows_storage_search!TestHook_GrepQuery_CrawlForNextItem+0x1d
    00007ffe321f863d windows_storage_search!CGrepQuery::CrawlForNextItem+0x1d
    00007ffe321ef419 windows_storage_search!CGrepRowset::GetRowsAt+0x69
    00007ffe321e30d9 windows_storage_search!CQueryResultSet::FetchResultAt+0x119
    00007ffe321d6018 windows_storage_search!CRowsetEnumeration::_EnumerateRowset+0x158
    00007ffe3224151e windows_storage_search!<lambda_1ed3756976052670480a11bef8ae9396>::operator()+0x7a
    00007ffe59fa4ead shcore!WorkThreadManager::CThread::ThreadProc+0x2dd
    00007ffe59fa2a7e shcore!WorkThreadManager::CThread::s_ExecuteThreadProc+0x22
    00007ffe59fc9289 shcore!<lambda_142c425290ac4fbd4d5aee2fc3f7d711>::<lambda_invoker_cdecl>+0x29
    00007ffe5afa1323 ntdll!TppSimplepExecuteCallback+0xa3
    00007ffe5af96fd6 ntdll!TppWorkerThread+0x686
    00007ffe5a2d54e0 KERNEL32!BaseThreadInitThunk+0x10
    00007ffe5af8485b ntdll!RtlUserThreadStart+0x2b

1 thread: ffffbe0c8c9c7080
    fffff8076241df31 nt!KxDispatchInterrupt+0x151
    fffff8076241d3b6 nt!KiDpcInterrupt+0x326
    fffff8076232d060 nt!KeLeaveCriticalRegion
    ffffbc928e134a0d win32kbase!REGION::vDeleteREGION+0x21d
    ffffbc928e14ecd5 win32kbase!DC::iCombine+0x545
    ffffbc928e14e516 win32kbase!GreIntersectClipRect+0x486
    ffffbc928e7bf933 win32kfull!NtGdiIntersectClipRect+0x13
    ffffbc928dc4d4f4 win32k!NtGdiIntersectClipRect+0x20
    fffff80762428775 nt!KiSystemServiceCopyEnd+0x25
    00007ffe58d81754 win32u!NtGdiIntersectClipRect+0x14
    00007ffe58900f02 gdi32full!IntersectClipRectImpl+0x52
    00007ffe5575562a UxTheme!DrawThemeParentBackgroundEx+0x29a
    00007ffe3bb5ac9e explorerframe!CBreadcrumbBar::_WndProc+0x1ae
    00007ffe3bb5aa51 explorerframe!CBreadcrumbBar::s_BreadcrumbWndProc+0x71
    00007ffe59011c4c user32!UserCallWinProcCheckWow+0x33c
    00007ffe5901179c user32!DispatchClientMessage+0x9c
    00007ffe59024b4d user32!_fnDWORD+0x3d
    00007ffe5b0276a4 ntdll!KiUserCallbackDispatcherContinue
    00007ffe58d81434 win32u!NtUserMessageCall+0x14
    00007ffe590108cf user32!SendMessageWorker+0x12f
    00007ffe59010737 user32!SendMessageW+0x137
    00007ffe5575553b UxTheme!DrawThemeParentBackgroundEx+0x1ab
    00007ffe3bb5af2b explorerframe!CBreadcrumbBar::_WndProc+0x43b
    00007ffe3bb5aa51 explorerframe!CBreadcrumbBar::s_BreadcrumbWndProc+0x71
    00007ffe59011c4c user32!UserCallWinProcCheckWow+0x33c
    00007ffe5901179c user32!DispatchClientMessage+0x9c
    00007ffe59024b4d user32!_fnDWORD+0x3d
    00007ffe5b0276a4 ntdll!KiUserCallbackDispatcherContinue
    00007ffe58d81434 win32u!NtUserMessageCall+0x14
    00007ffe590108cf user32!SendMessageWorker+0x12f
    00007ffe59010737 user32!SendMessageW+0x137
    00007ffe4449fa4d comctl32!CCSendNotify+0x11d
    00007ffe444a2070 comctl32!CToolbar::TB_DrawBackground+0x48
    00007ffe444a1f2f comctl32!CToolbar::TBPaintImpl+0x6f
    00007ffe444a22f8 comctl32!CToolbar::TBPaint+0x1c0
    00007ffe4449651e comctl32!CToolbar::ToolbarWndProc+0x39e
    00007ffe44496094 comctl32!CToolbar::s_ToolbarWndProc+0x54
    00007ffe59011c4c user32!UserCallWinProcCheckWow+0x33c
    00007ffe5901189e user32!CallWindowProcW+0x8e
    00007ffe444b48a8 comctl32!CallNextSubclassProc+0xa8
```

```
    00007ffe444b47d8 comctl32!DefSubclassProc+0x88
    00007ffe3bba403f explorerframe!CBreadcrumbBar::_TBWndProc+0x6f
    00007ffe444b48a8 comctl32!CallNextSubclassProc+0xa8
    00007ffe444b4697 comctl32!MasterSubclassProc+0xa7
    00007ffe59011c4c user32!UserCallWinProcCheckWow+0x33c
    00007ffe5901179c user32!DispatchClientMessage+0x9c
    00007ffe59024b4d user32!_fnDWORD+0x3d
    00007ffe5b0276a4 ntdll!KiUserCallbackDispatcherContinue
    00007ffe58d819b4 win32u!NtUserDispatchMessage+0x14
    00007ffe59010edd user32!DispatchMessageWorker+0x2dd
    00007ffe3bba4671 explorerframe!CExplorerFrame::FrameMessagePump+0x101
    00007ffe3bb78bac explorerframe!BrowserThreadProc+0x90
    00007ffe3bb78c78 explorerframe!BrowserNewThreadProc+0x4c
    00007ffe3bb78ce2 explorerframe!CExplorerTask::InternalResumeRT+0x12
    00007ffe3bbb453e explorerframe!CRunnableTask::Run+0xce
    00007ffe5678515e windows_storage!CShellTask::TT_Run+0x46
    00007ffe56784d95 windows_storage!CShellTaskThread::ThreadProc+0xdd
    00007ffe56784a34 windows_storage!CShellTaskThread::s_ThreadProc+0x44
    00007ffe59fc4e9f shcore!_WrapperThreadProc+0x10f
    00007ffe5a2d54e0 KERNEL32!BaseThreadInitThunk+0x10
    00007ffe5af8485b ntdll!RtlUserThreadStart+0x2b

Threads matching filter: 2 out of 116

Process: SearchHost.exe @ ffffbe0c8a982080
============================================================
2 threads: ffffbe0c8ab3a080 ffffbe0c89cfc080
    fffff8076241dce6 nt!KiSwapContext+0x76
    fffff807623327f7 nt!KiSwapThread+0x3a7
    fffff807623346a9 nt!KiCommitThreadWait+0x159
    fffff80762254fa4 nt!KeWaitForAlertByThreadId+0xc4
    fffff807626c72a0 nt!NtWaitForAlertByThreadId+0x30
    fffff80762428775 nt!KiSystemServiceCopyEnd+0x25
    00007ffe5b0272a4 0x7ffe5b0272a4

Threads matching filter: 2 out of 60

Unable to load image C:\Work\notmyfault64.exe, Win32 error 0n2
Process: notmyfault64.exe @ ffffbe0c8c2cd0c0
============================================================
1 thread: ffffbe0c8974f080
    fffff80762416220 nt!KeBugCheckEx
    fffff80762428da9 nt!KiBugCheckDispatch+0x69
    fffff80762424f00 nt!KiPageFault+0x440
    fffff80761781530 myfault+0x1530
    fffff80761781e2d myfault+0x1e2d
    fffff80761781f88 myfault+0x1f88
    fffff80762303115 nt!IofCallDriver+0x55
    fffff8076276bbf2 nt!IopSynchronousServiceTail+0x1d2
    fffff8076276b9d2 nt!IopXxxControlFile+0xc82
    fffff8076276ad36 nt!NtDeviceIoControlFile+0x56
    fffff80762428775 nt!KiSystemServiceCopyEnd+0x25
    00007ffe5b023834 ntdll!NtDeviceIoControlFile+0x14
    00007ffe58a33ffb KERNELBASE!DeviceIoControl+0x6b
    00007ffe5a2d5f91 KERNEL32!DeviceIoControlImplementation+0x81
    00007ff72c0426ce notmyfault64+0x26ce
    00007ffe5901484b USER32!UserCallDlgProcCheckWow+0x14b
    00007ffe5901409b USER32!DefDlgProcWorker+0xcb
    00007ffe590597c9 USER32!DefDlgProcA+0x39
    00007ffe59011c4c USER32!UserCallWinProcCheckWow+0x33c
    00007ffe5901179c USER32!DispatchClientMessage+0x9c
    00007ffe59024b4d USER32!_fnDWORD+0x3d
    00007ffe5b0276a4 ntdll!KiUserCallbackDispatcherContinue
    00007ffe58d81434 win32u!NtUserMessageCall+0x14
    00007ffe590108cf USER32!SendMessageWorker+0x12f
    00007ffe59010737 USER32!SendMessageW+0x137
    00007ffe444750bf COMCTL32!Button_ReleaseCapture+0xbb
    00007ffe444a8822 COMCTL32!Button_WndProc+0x802
    00007ffe59011c4c USER32!UserCallWinProcCheckWow+0x33c
    00007ffe59010ea6 USER32!DispatchMessageWorker+0x2a6
    00007ffe59016084 USER32!IsDialogMessageW+0x104
    00007ffe44455f9f COMCTL32!Prop_IsDialogMessage+0x4b
    00007ffe44455e48 COMCTL32!_RealPropertySheet+0x2c0
    00007ffe44455abd COMCTL32!_PropertySheet+0x49
    00007ffe44520953 COMCTL32!PropertySheetA+0x53
    00007ff72c043415 notmyfault64+0x3415
```

```
    00007ff72c045c68 notmyfault64+0x5c68
    00007ffe5a2d54e0 KERNEL32!BaseThreadInitThunk+0x10
    00007ffe5af8485b ntdll!RtlUserThreadStart+0x2b

Threads matching filter: 1 out of 3
```

Note: The option **-a** searches all processes. For illustration, we sometimes omit it to search the current process of interest only if it takes too long otherwise.

12. To see stack traces from threads running on CPUs, you can use these MEX extension commands:

```
0: kd> !mex.running
Process           PID Thread             Id Pri Base Pri Next CPU CSwitches   User Kernel State   Time Reason
=============== ==== ================ ==== === ======== ======== ========= ====== ====== ======= ==== ===========
dwm.exe           310 ffffbe0c89190080  428  15       15        0     19997 5s.266 3s.625 Running 15ms UserRequest
notmyfault64.exe 243c ffffbe0c8974f080 1938  12        8        1      1701   16ms  125ms Running 15ms WrResource

Count: 2 | Show Unique Stacks
```

```
0: kd> !mex.us -cpu
1 thread: ffffbe0c89190080
    00007ffe552d2700 CoreMessaging!AlpcClientConnection::PendingPortCheck
    00007ffe552d22e4 CoreMessaging!`CFlat::DelegateImpl<System::Action,0,void
__cdecl(void),void,0>::Bind<CFlat::SmartPtr<Microsoft::CoreUI::Messaging::CrossProcessReceivePort$AlpcReceiveSource>,&
Microsoft::CoreUI::Messaging::CrossProcessReceivePort$AlpcReceiveSource::ScheduleReceiveIfNeeded>'::`2'::Thunk::Invoke
+0x24
    00007ffe552aae27 CoreMessaging!CFlat::DelegateImpl<System::Action,0,void
__cdecl(void),void,0>::MulticastInvoke+0x47
    00007ffe552ca6f6 CoreMessaging!Microsoft::CoreUI::Dispatch::EventLoop::CallYieldCheckHandler+0xa2
    00007ffe552ff321 CoreMessaging!Microsoft::CoreUI::Dispatch::Dispatcher::PeekNextItem+0x26355
    00007ffe552aa4bd CoreMessaging!Microsoft::CoreUI::Dispatch::EventLoop::Callback_RunCoreLoop+0x1ed
    00007ffe552a70ba CoreMessaging!Microsoft::CoreUI::Dispatch::Win32EventLoopBridge::Callback_Run+0x41a
    00007ffe552d280e CoreMessaging!Microsoft::CoreUI::Dispatch::EventLoop::Callback_Run+0xae
    00007ffe55290dcf CoreMessaging!Microsoft::CoreUI::IExportMessageLoopExtensions::ExportAdapter$::Run+0x19f
    00007ffe54e698c9 dwmcore!CComposition::ProcessBatches+0xb1
    00007ffe54e6999b dwmcore!CComposition::PreRender+0x77
    00007ffe54e691c2 dwmcore!CComposition::ProcessComposition+0x4a
    00007ffe54e682c7 dwmcore!CPartitionVerticalBlankScheduler::Render+0x5b
    00007ffe54e67876 dwmcore!CPartitionVerticalBlankScheduler::ProcessFrame+0x102
    00007ffe54e6684f dwmcore!CPartitionVerticalBlankScheduler::ScheduleAndProcessFrame+0x8f
    00007ffe54eed3a6 dwmcore!CConnection::MainCompositionThreadLoop+0xba
    00007ffe54eed2d6 dwmcore!CConnection::RunCompositionThread+0xfa
    00007ffe5a2d54e0 KERNEL32!BaseThreadInitThunk+0x10
    00007ffe5af8485b ntdll!RtlUserThreadStart+0x2b

1 thread: ffffbe0c8974f080
Unable to load image C:\Work\notmyfault64.exe, Win32 error 0n2
    fffff80762416220 nt!KeBugCheckEx
    fffff80762428da9 nt!KiBugCheckDispatch+0x69
    fffff80762424f00 nt!KiPageFault+0x440
    fffff80761781530 myfault+0x1530
    fffff80761781e2d myfault+0x1e2d
    fffff80761781f88 myfault+0x1f88
    fffff80762303115 nt!IofCallDriver+0x55
    fffff8076276bbf2 nt!IopSynchronousServiceTail+0x1d2
    fffff8076276b9d2 nt!IopXxxControlFile+0xc82
    fffff8076276ad36 nt!NtDeviceIoControlFile+0x56
    fffff80762428775 nt!KiSystemServiceCopyEnd+0x25
    00007ffe5b023834 ntdll!NtDeviceIoControlFile+0x14
    00007ffe58a33ffb KERNELBASE!DeviceIoControl+0x6b
    00007ffe5a2d5f91 KERNEL32!DeviceIoControlImplementation+0x81
    00007ff72c0426ce notmyfault64+0x26ce
    00007ffe5901484b USER32!UserCallDlgProcCheckWow+0x14b
    00007ffe5901409b USER32!DefDlgProcWorker+0xcb
    00007ffe590597c9 USER32!DefDlgProcA+0x39
    00007ffe59011c4c USER32!UserCallWinProcCheckWow+0x33c
    00007ffe5901179c USER32!DispatchClientMessage+0x9c
    00007ffe59024b4d USER32!_fnDWORD+0x3d
    00007ffe5b0276a4 ntdll!KiUserCallbackDispatcherContinue
    00007ffe58d81434 win32u!NtUserMessageCall+0x14
    00007ffe590108cf USER32!SendMessageWorker+0x12f
```

```
    00007ffe59010737 USER32!SendMessageW+0x137
    00007ffe444750bf COMCTL32!Button_ReleaseCapture+0xbb
    00007ffe444a8822 COMCTL32!Button_WndProc+0x802
    00007ffe59011c4c USER32!UserCallWinProcCheckWow+0x33c
    00007ffe59010ea6 USER32!DispatchMessageWorker+0x2a6
    00007ffe59016084 USER32!IsDialogMessageW+0x104
    00007ffe44455f9f COMCTL32!Prop_IsDialogMessage+0x4b
    00007ffe44455e48 COMCTL32!_RealPropertySheet+0x2c0
    00007ffe44455abd COMCTL32!_PropertySheet+0x49
    00007ffe44520953 COMCTL32!PropertySheetA+0x53
    00007ff72c043415 notmyfault64+0x3415
    00007ff72c045c68 notmyfault64+0x5c68
    00007ffe5a2d54e0 KERNEL32!BaseThreadInitThunk+0x10
    00007ffe5af8485b ntdll!RtlUserThreadStart+0x2b

2 stack(s) with 2 threads displayed (2 Total threads)
```

Note: We use the **!mex.running** command to differentiate it from the preloaded **!kdexts.running** command:

```
0: kd> ~1s

1: kd> .thread /r /p

1: kd> !kdexts.running

System Processors:  (0000000000000003)
  Idle Processors:  (0000000000000000)

       Prcbs             Current         (pri) Next            (pri) Idle
  0    fffff807604e6180  ffffbe0c89190080 (15)                       fffff80762d35bc0  .................
  1    ffffce00fb700180  ffffbe0c8974f080 (12)                       ffffce00fb70c0c0  .................
```

Note: However, the default running command has problems loading the correct user space context for non-current processes (the **-i** option is included to list idle threads as well, if any):

```
1: kd> !kdexts.running -t -i

System Processors:  (0000000000000003)
  Idle Processors:  (0000000000000000)

       Prcbs             Current         (pri) Next            (pri) Idle
  0    fffff807604e6180  ffffbe0c89190080 (15)                       fffff80762d35bc0  .................

 # Child-SP          RetAddr               Call Site
00 0000005b`47eff318 00007ffe`552d22e4     CoreMessaging!AlpcClientConnection::PendingPortCheck
01 0000005b`47eff320 00007ffe`552aae27     CoreMessaging!`CFlat::DelegateImpl<System::Action,0,void
__cdecl(void),void,0>::Bind<CFlat::SmartPtr<Microsoft::CoreUI::Messaging::CrossProcessReceivePort$AlpcReceiveSource>,&Microsoft::CoreUI
::Messaging::CrossProcessReceivePort$AlpcReceiveSource::ScheduleReceiveIfNeeded>'::`2'::Thunk::Invoke+0x24
02 0000005b`47eff350 00007ffe`552ca6f6     CoreMessaging!CFlat::DelegateImpl<System::Action,0,void
__cdecl(void),void,0>::MulticastInvoke+0x47
03 0000005b`47eff380 00007ffe`552ff321     CoreMessaging!Microsoft::CoreUI::Dispatch::EventLoop::CallYieldCheckHandler+0xa2
04 0000005b`47eff3b0 00007ffe`552aa4bd     CoreMessaging!Microsoft::CoreUI::Dispatch::Dispatcher::PeekNextItem+0x26355
05 0000005b`47eff3e0 00007ffe`552a70ba     CoreMessaging!Microsoft::CoreUI::Dispatch::EventLoop::Callback_RunCoreLoop+0x1ed
06 0000005b`47eff4a0 00007ffe`552d280e     CoreMessaging!Microsoft::CoreUI::Dispatch::Win32EventLoopBridge::Callback_Run+0x41a
07 0000005b`47eff550 00007ffe`55290dcf     CoreMessaging!Microsoft::CoreUI::Dispatch::EventLoop::Callback_Run+0xae
08 0000005b`47eff590 00007ffe`54e698c9     CoreMessaging!Microsoft::CoreUI::IExportMessageLoopExtensions::ExportAdapter$::Run+0x19f
09 0000005b`47eff600 00000000`00000001     0x00007ffe`54e698c9
0a 0000005b`47eff608 00000000`00000003     0x1
0b 0000005b`47eff610 00007ffe`54e698c9     0x3
0c 0000005b`47eff618 0000018f`4003e340     0x00007ffe`54e698c9
0d 0000005b`47eff620 0000a68b`a6149684     0x0000018f`4003e340
0e 0000005b`47eff628 0000018f`4003ea10     0x0000a68b`a6149684
0f 0000005b`47eff630 0000018f`4003ea10     0x0000018f`4003ea10
10 0000005b`47eff638 00007ffe`54e6999b     0x0000018f`4003ea10
11 0000005b`47eff640 0000018f`40038e00     0x00007ffe`54e6999b
12 0000005b`47eff648 00000000`00000040     0x0000018f`40038e00
13 0000005b`47eff650 00000000`00000000     0x40

  1    ffffce00fb700180  ffffbe0c8974f080 (12)                       ffffce00fb70c0c0  .................

 # Child-SP          RetAddr               Call Site
00 ffffa28c`9d8d8688 fffff807`62428da9     nt!KeBugCheckEx
01 ffffa28c`9d8d8690 fffff807`62424f00     nt!KiBugCheckDispatch+0x69
02 ffffa28c`9d8d87d0 fffff807`61781530     nt!KiPageFault+0x440
03 ffffa28c`9d8d8960 fffff807`61781e2d     myfault+0x1530
```

```
04 ffffa28c`9d8d8990 fffff807`61781f88     myfault+0x1e2d
05 ffffa28c`9d8d8ae0 fffff807`62303115     myfault+0x1f88
06 ffffa28c`9d8d8b20 fffff807`6276bbf2     nt!IofCallDriver+0x55
07 ffffa28c`9d8d8b60 fffff807`6276b9d2     nt!IopSynchronousServiceTail+0x1d2
08 ffffa28c`9d8d8c10 fffff807`6276ad36     nt!IopXxxControlFile+0xc82
09 ffffa28c`9d8d8d40 fffff807`62428775     nt!NtDeviceIoControlFile+0x56
0a ffffa28c`9d8d8db0 00007ffe`5b023834     nt!KiSystemServiceCopyEnd+0x25
0b 00000034`f5d2eb88 00007ffe`58a33ffb     ntdll!NtDeviceIoControlFile+0x14
0c 00000034`f5d2eb90 00007ffe`5a2d5f91     KERNELBASE!DeviceIoControl+0x6b
0d 00000034`f5d2ec00 00007ff7`2c0426ce     KERNEL32!DeviceIoControlImplementation+0x81
0e 00000034`f5d2ec50 00007ffe`5901484b     notmyfault64+0x26ce
0f 00000034`f5d2ed50 00007ffe`5901409b     USER32!UserCallDlgProcCheckWow+0x14b
10 00000034`f5d2ee30 00007ffe`590597c9     USER32!DefDlgProcWorker+0xcb
11 00000034`f5d2eef0 00007ffe`59011c4c     USER32!DefDlgProcA+0x39
12 00000034`f5d2ef30 00007ffe`5901179c     USER32!UserCallWinProcCheckWow+0x33c
13 00000034`f5d2f0a0 00007ffe`59024b4d     USER32!DispatchClientMessage+0x9c
14 00000034`f5d2f100 00007ffe`5b0276a4     USER32!_fnDWORD+0x3d
15 00000034`f5d2f160 00007ffe`58d81434     ntdll!KiUserCallbackDispatcherContinue
16 00000034`f5d2f1e8 00007ffe`590108cf     win32u!NtUserMessageCall+0x14
17 00000034`f5d2f1f0 00007ffe`59010737     USER32!SendMessageWorker+0x12f
18 00000034`f5d2f290 00007ffe`444750bf     USER32!SendMessageW+0x137
19 00000034`f5d2f2f0 00007ffe`444a8822     COMCTL32!Button_ReleaseCapture+0xbb
1a 00000034`f5d2f320 00007ffe`59011c4c     COMCTL32!Button_WndProc+0x802
1b 00000034`f5d2f430 00007ffe`59010ea6     USER32!UserCallWinProcCheckWow+0x33c
1c 00000034`f5d2f5a0 00007ffe`59016084     USER32!DispatchMessageWorker+0x2a6
1d 00000034`f5d2f620 00007ffe`44455f9f     USER32!IsDialogMessageW+0x104
1e 00000034`f5d2f680 00007ffe`44455e48     COMCTL32!Prop_IsDialogMessage+0x4b
1f 00000034`f5d2f6c0 00007ffe`44455abd     COMCTL32!_RealPropertySheet+0x2c0
20 00000034`f5d2f790 00007ffe`44520953     COMCTL32!_PropertySheet+0x49
21 00000034`f5d2f7c0 00007ff7`2c043415     COMCTL32!PropertySheetA+0x53
22 00000034`f5d2f860 00007ff7`2c045c68     notmyfault64+0x3415
23 00000034`f5d2fa90 00007ffe`5a2d54e0     notmyfault64+0x5c68
24 00000034`f5d2fad0 00007ffe`5af8485b     KERNEL32!BaseThreadInitThunk+0x10
25 00000034`f5d2fb00 00000000`00000000     ntdll!RtlUserThreadStart+0x2b
```

```
1: kd> ~0s
```

```
0: kd> .reload /user
Loading User Symbols
...............................................................
.....................

************* Symbol Loading Error Summary **************
Module name            Error
myfault                The system cannot find the file specified

You can troubleshoot most symbol related issues by turning on symbol loading diagnostics (!sym noisy) and
repeating the command that caused symbols to be loaded.
You should also verify that your symbol search path (.sympath) is correct.
```

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

System Processors:  (0000000000000003)
  Idle Processors:  (0000000000000000)

       Prcbs             Current         (pri) Next            (pri) Idle
  0    fffff807604e6180  ffffbe0c89190080 (15)                       fffff80762d35bc0  ................

 # Child-SP          RetAddr               Call Site
00 0000005b`47eff318 00007ffe`552d22e4     CoreMessaging!AlpcClientConnection::PendingPortCheck
01 0000005b`47eff320 00007ffe`552aae27     CoreMessaging!`CFlat::DelegateImpl<System::Action,0,void
__cdecl(void),void,0>::Bind<CFlat::SmartPtr<Microsoft::CoreUI::Messaging::CrossProcessReceivePort$AlpcReceiveSource>,&Microsoft::CoreUI
::Messaging::CrossProcessReceivePort$AlpcReceiveSource::ScheduleReceiveIfNeeded>'::`2'::Thunk::Invoke+0x24
02 0000005b`47eff350 00007ffe`552ca6f6     CoreMessaging!CFlat::DelegateImpl<System::Action,0,void
__cdecl(void),void,0>::MulticastInvoke+0x47
03 0000005b`47eff380 00007ffe`552ff321     CoreMessaging!Microsoft::CoreUI::Dispatch::EventLoop::CallYieldCheckHandler+0xa2
04 0000005b`47eff3b0 00007ffe`552aa4bd     CoreMessaging!Microsoft::CoreUI::Dispatch::Dispatcher::PeekNextItem+0x26355
05 0000005b`47eff3e0 00007ffe`552a70ba     CoreMessaging!Microsoft::CoreUI::Dispatch::EventLoop::Callback_RunCoreLoop+0x1ed
06 0000005b`47eff4a0 00007ffe`552d280e     CoreMessaging!Microsoft::CoreUI::Dispatch::Win32EventLoopBridge::Callback_Run+0x41a
07 0000005b`47eff550 00007ffe`55290dcf     CoreMessaging!Microsoft::CoreUI::Dispatch::EventLoop::Callback_Run+0xae
08 0000005b`47eff590 00007ffe`54e698c9     CoreMessaging!Microsoft::CoreUI::IExportMessageLoopExtensions::ExportAdapter$::Run+0x19f
09 0000005b`47eff600 00007ffe`54e6999b     dwmcore!CComposition::ProcessBatches+0xb1
0a 0000005b`47eff640 00007ffe`54e691c2     dwmcore!CComposition::PreRender+0x77
0b 0000005b`47eff6d0 00007ffe`54e682c7     dwmcore!CComposition::ProcessComposition+0x4a
0c 0000005b`47eff770 00007ffe`54e67876     dwmcore!CPartitionVerticalBlankScheduler::Render+0x5b
0d 0000005b`47eff7d0 00007ffe`54e6684f     dwmcore!CPartitionVerticalBlankScheduler::ProcessFrame+0x102
0e 0000005b`47eff870 00007ffe`54eed3a6     dwmcore!CPartitionVerticalBlankScheduler::ScheduleAndProcessFrame+0x8f
0f 0000005b`47eff990 00007ffe`54eed2d6     dwmcore!CConnection::MainCompositionThreadLoop+0xba
10 0000005b`47effa00 00007ffe`5a2d54e0     dwmcore!CConnection::RunCompositionThread+0xfa
11 0000005b`47effa30 00007ffe`5af8485b     KERNEL32!BaseThreadInitThunk+0x10
12 0000005b`47effa60 00000000`00000000     ntdll!RtlUserThreadStart+0x2b
```

```
  1    ffffce00fb700180  ffffbe0c8974f080 (12)                     ffffce00fb70c0c0  ................

 # Child-SP          RetAddr               Call Site
00 ffffa28c`9d8d8688 fffff807`62428da9     nt!KeBugCheckEx
01 ffffa28c`9d8d8690 fffff807`62424f00     nt!KiBugCheckDispatch+0x69
02 ffffa28c`9d8d87d0 fffff807`61781530     nt!KiPageFault+0x440
03 ffffa28c`9d8d8960 fffff807`61781e2d     myfault+0x1530
04 ffffa28c`9d8d8990 fffff807`61781f88     myfault+0x1e2d
05 ffffa28c`9d8d8ae0 fffff807`62303115     myfault+0x1f88
06 ffffa28c`9d8d8b20 fffff807`6276bbf2     nt!IofCallDriver+0x55
07 ffffa28c`9d8d8b60 fffff807`6276b9d2     nt!IopSynchronousServiceTail+0x1d2
08 ffffa28c`9d8d8c10 fffff807`6276ad36     nt!IopXxxControlFile+0xc82
09 ffffa28c`9d8d8d40 fffff807`62428775     nt!NtDeviceIoControlFile+0x56
0a ffffa28c`9d8d8db0 00007ffe`5b023834     nt!KiSystemServiceCopyEnd+0x25
0b 00000034`f5d2eb88 00007ffe`58a33ffb     ntdll!NtDeviceIoControlFile+0x14
0c 00000034`f5d2eb90 00007ffe`5a2d5f91     KERNELBASE!DeviceIoControl+0x6b
0d 00000034`f5d2ec00 00007ff7`2c0426ce     KERNEL32!DeviceIoControlImplementation+0x81
0e 00000034`f5d2ec50 00000000`0004086e     0x00007ff7`2c0426ce
0f 00000034`f5d2ec58 00000034`f5d2ece9     0x4086e
10 00000034`f5d2ec60 00000034`f5d2ece9     0x00000034`f5d2ece9
11 00000034`f5d2ec68 00000000`00000000     0x00000034`f5d2ece9
```

Note: Mex **!UniqueStacks** (**!us**) and **!ForEachMatchingStack** (**!fems**) commands have many options to list and filter stack traces. Use the **-?** option to see their description.

13. We can also use regular expressions for stack traces, treating them as a multiline string (**-m**):

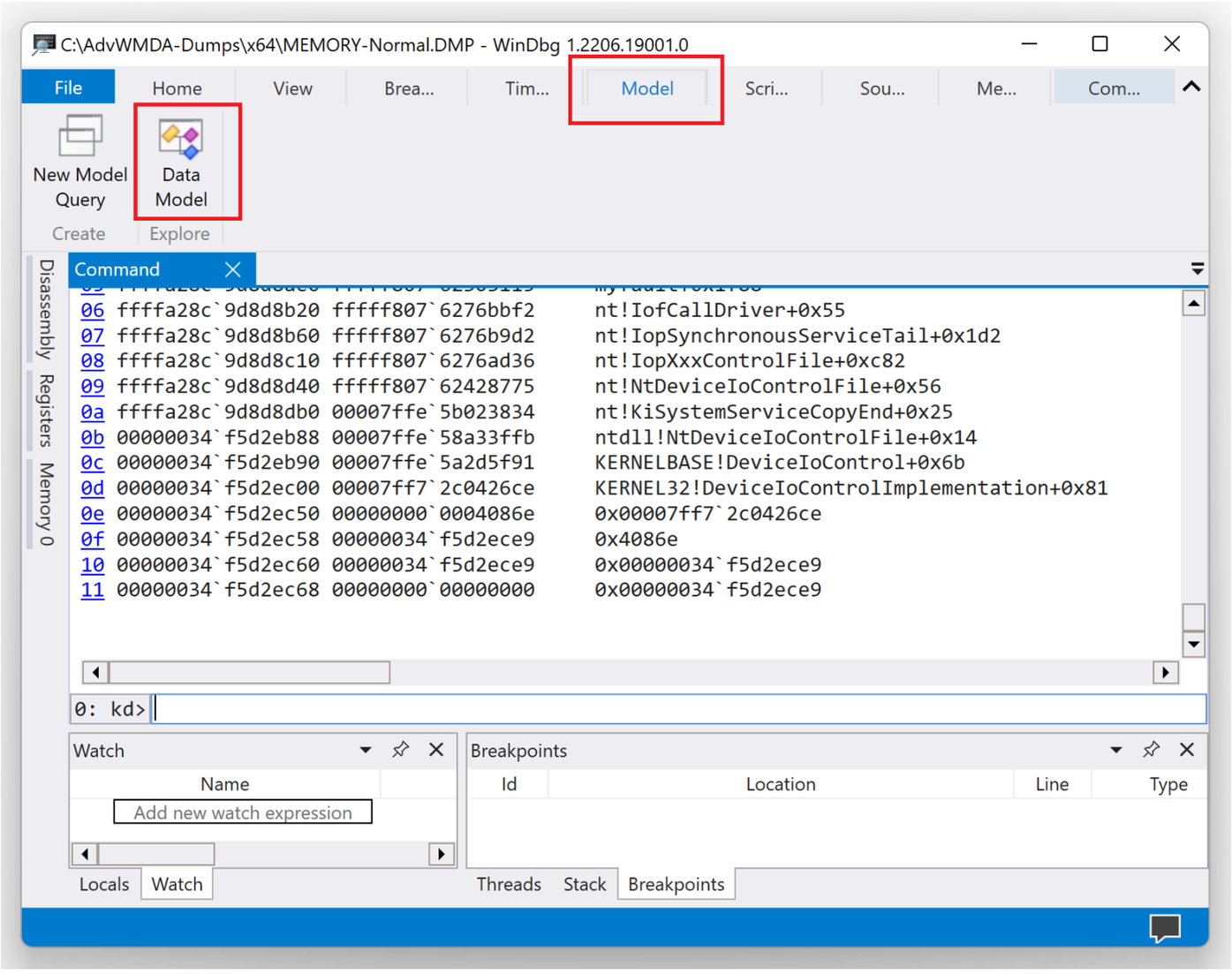
```
0: kd> ~1s

1: kd> .thread /r /p
Implicit thread is now ffffbe0c`8974f080
Implicit process is now ffffbe0c`8c2cd0c0
Loading User Symbols
.................................

************* Symbol Loading Error Summary **************
Module name            Error
vsock                  The system cannot find the file specified
vmci                   The system cannot find the file specified
WdFilter               The system cannot find the file specified
vm3dmp                 The system cannot find the file specified
vmmemctl               The system cannot find the file specified
vmhgfs                 The system cannot find the file specified
myfault                The system cannot find the file specified

You can troubleshoot most symbol related issues by turning on symbol loading diagnostics (!sym
noisy) and repeating the command that caused symbols to be loaded.
You should also verify that your symbol search path (.sympath) is correct.

1: kd> !mex.us -m (.*)BugCheck(.*)PageFault(.*)
Threads matching filter: 0 out of 3

0: kd> !mex.us -m (.*)BugCheck(.*)PageFault(.*)
1 thread [stats]: ffffc38c33ac3080
    fffff80662215590 nt!KeBugCheckEx
    fffff806622281a9 nt!KiBugCheckDispatch+0x69
    fffff80662224300 nt!KiPageFault+0x440
    fffff80660571981 myfault+0x1981
    fffff80660571d3d myfault+0x1d3d
    fffff80660571ea1 myfault+0x1ea1
    fffff80662102f65 nt!IofCallDriver+0x55
    fffff8066256b532 nt!IopSynchronousServiceTail+0x1d2
    fffff8066256acbf nt!IopXxxControlFile+0x5df
    fffff8066256a6c6 nt!NtDeviceIoControlFile+0x56
```

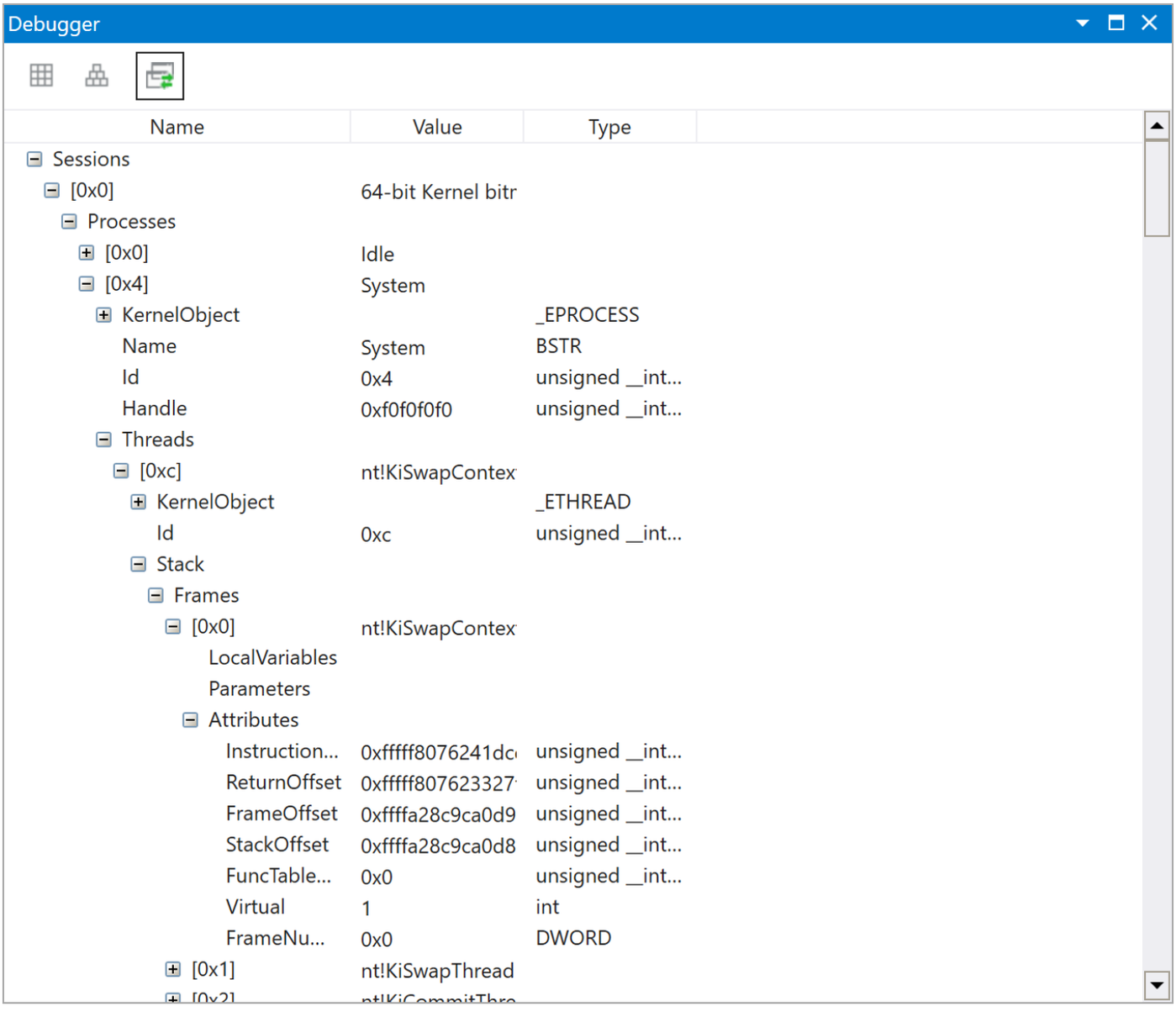
```
    fffff80662227b75 nt!KiSystemServiceCopyEnd+0x25
    00007ffc88543444 ntdll!NtDeviceIoControlFile+0x14
    00007ffc85c23edb KERNELBASE!DeviceIoControl+0x6b
    00007ffc876b5f91 KERNEL32!DeviceIoControlImplementation+0x81
    00007ff7be36342f notmyfault64+0x342f
    00007ffc87fd484b USER32!UserCallDlgProcCheckWow+0x14b
    00007ffc87fd409b USER32!DefDlgProcWorker+0xcb
    00007ffc880197c9 USER32!DefDlgProcA+0x39
    00007ffc87fd1c4c USER32!UserCallWinProcCheckWow+0x33c
    00007ffc87fd179c USER32!DispatchClientMessage+0x9c
    00007ffc87fe4b4d USER32!_fnDWORD+0x3d
    00007ffc885472b4 ntdll!KiUserCallbackDispatcherContinue
    00007ffc85b21434 win32u!NtUserMessageCall+0x14
    00007ffc87fd08cf USER32!SendMessageWorker+0x12f
    00007ffc87fd0737 USER32!SendMessageW+0x137
    00007ffc73c550bf COMCTL32!Button_ReleaseCapture+0xbb
    00007ffc73c88822 COMCTL32!Button_WndProc+0x802
    00007ffc87fd1c4c USER32!UserCallWinProcCheckWow+0x33c
    00007ffc87fd0ea6 USER32!DispatchMessageWorker+0x2a6
    00007ffc87fd6084 USER32!IsDialogMessageW+0x104
    00007ffc73c35f9f COMCTL32!Prop_IsDialogMessage+0x4b
    00007ffc73c35e48 COMCTL32!_RealPropertySheet+0x2c0
    00007ffc73c35abd COMCTL32!_PropertySheet+0x49
    00007ffc73d00953 COMCTL32!PropertySheetA+0x53
    00007ff7be364cd0 notmyfault64+0x4cd0
    00007ff7be365292 notmyfault64+0x5292
    00007ffc876b54e0 KERNEL32!BaseThreadInitThunk+0x10
    00007ffc884a485b ntdll!RtlUserThreadStart+0x2b

Threads matching filter: 1 out of 3
```

Note: As we see above, sometimes the behavior of this old extension is unpredictable: it didn't find the stack trace pattern for CPU #1 and its current thread and process context and switched to CPU #0 but didn't change current the thread and its process context there so the next command run found the pattern. If you get this output, try to change the CPU context a few times:

```
1: kd> !kdexts.running -t -i

System Processors:  (0000000000000003)
  Idle Processors:  (0000000000000000)

       Prcbs             Current         (pri) Next            (pri) Idle
  0    fffff807604e6180  ffffbe0c89190080 (15)                       fffff80762d35bc0  ................

        ^ Current scope machine type mismatch error in '0k'

  1    ffffce00fb700180  ffffbe0c8974f080 (12)                       ffffce00fb70c0c0  ................

        ^ Current scope machine type mismatch error in '1k'

1: kd> ~0s; ~1s
```

14. Another way to explore sessions, processes, and threads is to use the *Model* tab in WinDbg:





15. We close logging before exiting WinDbg:

```
0: kd> .logclose
Closing open log file C:\AdvWMDA-Dumps\x64\C1A.log
```

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