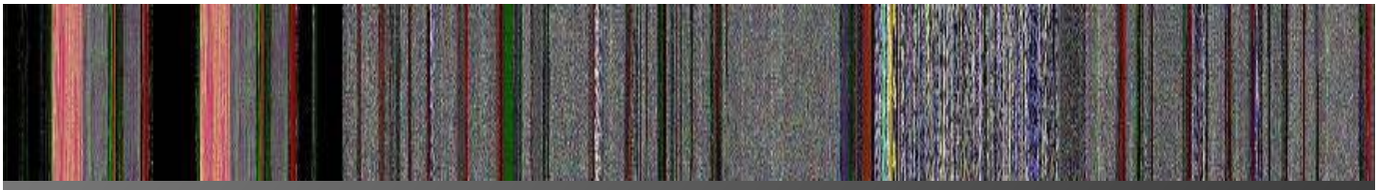


Defect
Detect

DUmps Binaries Logs INternals
School of Security

.NET
Memory Dump Analysis
Accelerated

Seventh Edition

Dmitry Vostokov
Software Diagnostics Services

Accelerated .NET Memory Dump Analysis: Training Course Transcript with WinDbg and LLDB Practice Exercises, Seventh Edition

Published by OpenTask, Republic of Ireland

OpenTask books 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: 978-1-912636-87-7 (Paperback)

Revision 7.02 (May 2025)

Contents

Exercise PN1 (Windows)

Goal: Learn how to use the SOS WinDbg extension to analyze managed space for the presence of exceptions.

Patterns: Manual Dump (Process); Stack Trace Collection (Unmanaged Space); CLR Thread; Technology-Specific Subtrace (JIT .NET Code); Technology-Specific Subtrace (JIT .NET Code); Software Exception; Exception Stack Trace; Managed Code Exception; Managed Stack Trace; Stack Trace Collection (Managed Space); Mixed Exception; Invalid Pointer; NULL Pointer (Data).

Commands: .logopen, version, !peb, ~*k, ~*kL, .load, !pe, ~*e, lmv, .chain, .unload, !analyze -v, kL, u, .cxr, !CLRStack, .sympath+, .srcpath+, .frame, !help, .logclose

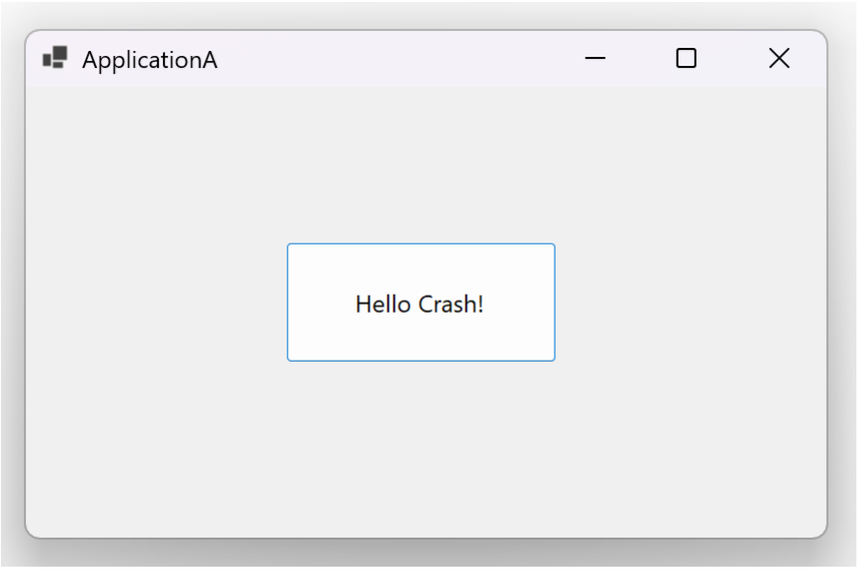
1. Launch WinDbg.

2. Open \ANETMDA-Dumps\Windows\x64\ApplicationA.DMP

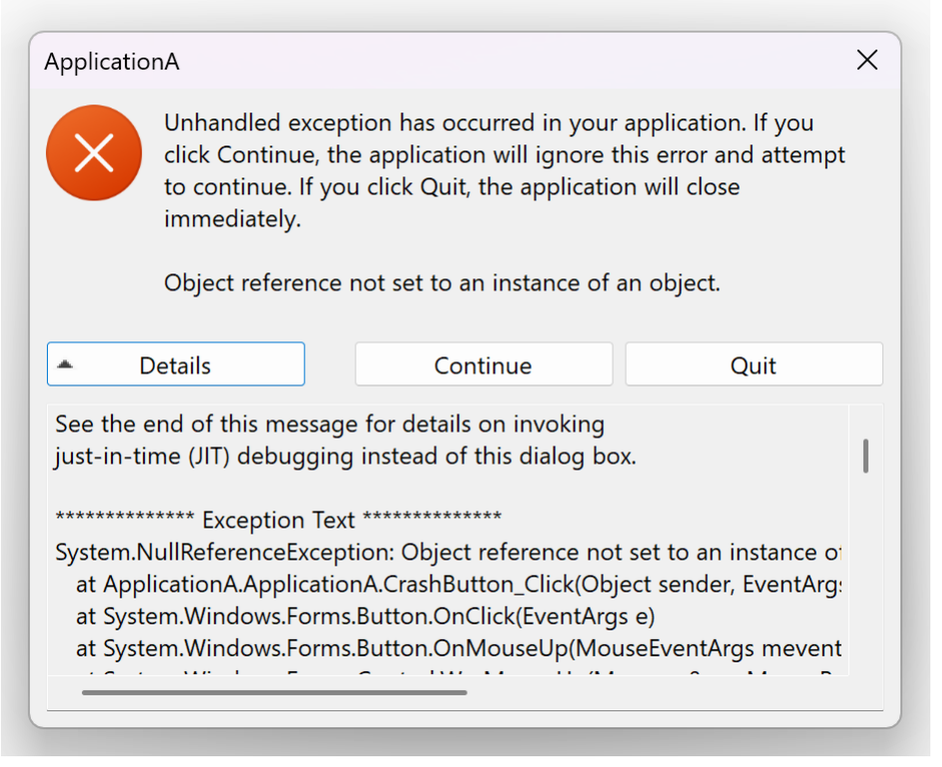
3. We get the dump file loaded:

```
Microsoft (R) Windows Debugger Version 10.0.27829.1001 AMD64
Copyright (c) Microsoft Corporation. All rights reserved.


Loading Dump File [C:\ANETMDA-Dumps\Windows\x64\ApplicationA.DMP]
User Mini Dump File with Full Memory: Only application data is available


************* Path validation summary **************
Response                         Time (ms)     Location
Deferred                                       srv*
Symbol search path is: srv*
Executable search path is:
Windows 10 Version 22000 MP (4 procs) Free x64
Product: WinNt, suite: SingleUserTS
Edition build lab: 22000.1.amd64fre.co_release.210604-1628
Debug session time: Sat Apr 26 13:45:10.000 2025 (UTC + 1:00)
System Uptime: 0 days 0:15:37.058
Process Uptime: 0 days 0:00:42.000
................................................................
.....................................
For analysis of this file, run !analyze -v
win32u!NtUserWaitMessage+0x14:
00007ffb`e61814d4 ret
```

Note: *ApplicationA* shows this window when launched:



When we click on a button, it shows an exception dialog:



At this time, we use Task Manager to save a memory dump.

4. Open a log file using the **.logopen** command:

```
0:000> .logopen C:\ANETMDA-Dumps\Windows\x64\ApplicationA.log
Opened log file 'C:\ANETMDA-Dumps\Windows\x64\ApplicationA.log'
```

Note: The WinDbg output may be slightly different on your system if you have a different WinDbg version, a different SOS extension version, you don't have .NET 9 installed, or you have a .NET version different from version 9.0.4 that was on a virtual machine where all the dumps were saved.

5. WinDbg **version** command shows information about the operating system and when the dump was taken:

```
0:000> version
Windows 10 Version 19042 MP (2 procs) Free x64
Product: WinNt, suite: SingleUserTS Personal
Edition build lab: 19041.1.amd64fre.vb_release.191206-1406
Machine Name:
Debug session time: Thu Apr  1 23:15:28.000 2021 (UTC + 0:00)
System Uptime: 0 days 0:12:42.262
Process Uptime: 0 days 0:01:43.000
  Kernel time: 0 days 0:00:00.000
  User time: 0 days 0:00:01.000
Full memory user mini dump: C:\ANETCMDA-Dumps\Windows\x64\ApplicationA.exe.9152.dmp
[...]
```

6. We can get the computer name from where the dump was taken using **!peb** command:

```
0:000> !peb
PEB at 000000d076d70000
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00007ff609cd0000
    NtGlobalFlag:             400
    NtGlobalFlag2:            0
    Ldr                       00007ffbe8e9a140
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 0000020ece432000 . 0000020ecff5c5c0
    Ldr.InLoadOrderModuleList:           0000020ece432180 . 0000020ecff5c5a0
    Ldr.InMemoryOrderModuleList:         0000020ece432190 . 0000020ecff5c5b0
[...]
    SubSystemData:     0000000000000000
    ProcessHeap:       0000020ece430000
    ProcessParameters: 0000020ece436500
    CurrentDirectory:  'C:\Work\'
    WindowTitle:  'C:\Work\ApplicationA.exe'
    ImageFile:    'C:\Work\ApplicationA.exe'
    CommandLine:  '"C:\Work\ApplicationA.exe" '
    DllPath:      '< Name not readable >'
    Environment:  0000020ece4311f0
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\User\AppData\Roaming
        CLIENTNAME=DESKTOP-IS6V2L0
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        CommonProgramW6432=C:\Program Files\Common Files
        COMPUTERNAME=WINDEV2204EVAL
        ComSpec=C:\WINDOWS\system32\cmd.exe
        DriverData=C:\Windows\System32\Drivers\DriverData
        HOMEDRIVE=C:
        HOMEPATH=\Users\User
        LOCALAPPDATA=C:\Users\User\AppData\Local
        LOGONSERVER=\\WINDEV2204EVAL
        NUMBER_OF_PROCESSORS=4
        OneDrive=C:\Users\User\OneDrive
        OS=Windows_NT

Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerSh
ell\v1.0\;C:\Windows\System32\OpenSSH\;C:\Program Files\Microsoft SQL
Server\150\Tools\Binn\;C:\Program Files\Microsoft SQL Server\Client
```

```
SDK\ODBC\170\Tools\Binn\;C:\Program
Files\dotnet\;C:\Users\User\AppData\Local\Microsoft\WindowsApps;C:\Users\User\.dotnet\tools
        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
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        ProgramW6432=C:\Program Files
        PSModulePath=C:\Program
Files\WindowsPowerShell\Modules;C:\WINDOWS\system32\WindowsPowerShell\v1.0\Modules
        PUBLIC=C:\Users\Public
        SESSIONNAME=31C5CE94259D4006A9E4#0
        SystemDrive=C:
        SystemRoot=C:\WINDOWS
        TEMP=C:\Users\User\AppData\Local\Temp
        TMP=C:\Users\User\AppData\Local\Temp
        USERDOMAIN=WINDEV2204EVAL
        USERDOMAIN_ROAMINGPROFILE=WINDEV2204EVAL
        USERNAME=User
        USERPROFILE=C:\Users\User
        windir=C:\WINDOWS
```

7. Type ~***kL** command to verify the correctness of all stack traces (the command execution time may be longer for the first time because symbol files need to be downloaded from the Microsoft symbol server). The **~*k** command output includes references to the .NET CLR source code, and we use the **~*kL** command variant to reduce output clutter.

```
0:000> ~*kL

.  0  Id: 1bcc.19fc Suspend: 0 Teb: 000000d0`76d71000 Unfrozen
 # Child-SP          RetAddr               Call Site
00 000000d0`76b9b218 00007ffb`55d9c454     win32u!NtUserWaitMessage+0x14
01 000000d0`76b9b220 00007ffb`b5237d33     System_Windows_Forms_Primitives!Windows.Win32.PInvoke.WaitMessage+0x74
02 000000d0`76b9b2d0 00007ffb`b5237c1a     System_Windows_Forms!System.Windows.Forms.Application.LightThreadContext.FPushMessageLoop+0x43
03 000000d0`76b9b360 00007ffb`b5239597     System_Windows_Forms!System.Windows.Forms.Application.LightThreadContext.RunMessageLoop+0xa
04 000000d0`76b9b390 00007ffb`b52392d2     System_Windows_Forms!System.Windows.Forms.Application.ThreadContext.RunMessageLoopInner+0x287
05 000000d0`76b9b410 00007ffb`b517feae     System_Windows_Forms!System.Windows.Forms.Application.ThreadContext.RunMessageLoop+0x42
06 000000d0`76b9b470 00007ffb`b52390d9     System_Windows_Forms!System.Windows.Forms.Form.ShowDialog+0x27e
07 000000d0`76b9b520 00007ffb`55d83d0e     System_Windows_Forms!System.Windows.Forms.Application.ThreadContext.OnThreadException+0x99
08 000000d0`76b9b590 00007ffb`b58cc4ef     System_Windows_Forms!System.Windows.Forms.NativeWindow.Callback+0x26e
09 000000d0`76b9b5f0 00007ffb`b09e7a56     coreclr!CallCatchFunclet+0x17f
0a 000000d0`76b9b700 00007ffb`b09e717a     System_Private_CoreLib!System.Runtime.EH.DispatchEx+0x536
0b 000000d0`76b9b860 00007ffb`b5942eb3     System_Private_CoreLib!System.Runtime.EH.RhThrowHwEx+0xaa
0c 000000d0`76b9b8a0 00007ffb`b58c1568     coreclr!CallDescrWorkerInternal+0x83
0d 000000d0`76b9b8e0 00007ffb`b59f5cde     coreclr!DispatchCallSimple+0x60
0e 000000d0`76b9b970 00007ffb`b59cf58a     coreclr!HandleManagedFaultNew+0x192
0f 000000d0`76b9d480 00007ffb`e8d9ca2a     coreclr!CLRVectoredExceptionHandlerShim+0xa84ca
10 000000d0`76b9d4d0 00007ffb`e8d559f2     ntdll!RtlpCallVectoredHandlers+0x112
11 000000d0`76b9d570 00007ffb`e8dc805e     ntdll!RtlDispatchException+0x62
12 000000d0`76b9d7c0 00007ffb`55d8cb36     ntdll!KiUserExceptionDispatch+0x2e
13 000000d0`76b9def0 00007ffb`b4f78dd5     ApplicationA!ApplicationA.ApplicationA.CrashButton_Click+0x26
14 000000d0`76b9df10 00007ffb`b4f78f69     System_Windows_Forms!System.Windows.Forms.Button.OnClick+0x195
15 000000d0`76b9dfc0 00007ffb`b4f63d6d     System_Windows_Forms!System.Windows.Forms.Button.OnMouseUp+0xe9
16 000000d0`76b9e020 00007ffb`55d84d09     System_Windows_Forms!System.Windows.Forms.Control.WmMouseUp+0x2bd
17 000000d0`76b9e0b0 00007ffb`55d8b5d7     System_Windows_Forms!System.Windows.Forms.Control.WndProc+0x8d9
18 000000d0`76b9e140 00007ffb`55d83b69     System_Windows_Forms!System.Windows.Forms.ButtonBase.WndProc+0x97
19 000000d0`76b9e1a0 00007ffb`55d7347c     System_Windows_Forms!System.Windows.Forms.NativeWindow.Callback+0xc9
1a 000000d0`76b9e220 00007ffb`e7701cac     System_Windows_Forms_Primitives!ILStubClass.IL_STUB_ReversePInvoke(Windows.Win32.Foundation.HWND,
Windows.Win32.MessageId, Windows.Win32.Foundation.WPARAM, Windows.Win32.Foundation.LPARAM)+0x5c
1b 000000d0`76b9e2a0 00007ffb`e7700f06     user32!UserCallWinProcCheckWow+0x33c
1c 000000d0`76b9e410 00007ffb`b2d2291f     user32!DispatchMessageWorker+0x2a6
1d 000000d0`76b9e490 00007ffb`b5237e7e     System_Windows_Forms_Primitives!
1e 000000d0`76b9e560 00007ffb`b5237c1a     System_Windows_Forms!System.Windows.Forms.Application.LightThreadContext.FPushMessageLoop+0x18e
1f 000000d0`76b9e5f0 00007ffb`b5239597     System_Windows_Forms!System.Windows.Forms.Application.LightThreadContext.RunMessageLoop+0xa
20 000000d0`76b9e620 00007ffb`b52392d2     System_Windows_Forms!System.Windows.Forms.Application.ThreadContext.RunMessageLoopInner+0x287
21 000000d0`76b9e6a0 00007ffb`55d7189d     System_Windows_Forms!System.Windows.Forms.Application.ThreadContext.RunMessageLoop+0x42
22 000000d0`76b9e700 00007ffb`b5942eb3     ApplicationA!ApplicationA.Program.Main+0x3d
23 000000d0`76b9e740 00007ffb`b58c180c     coreclr!CallDescrWorkerInternal+0x83
24 000000d0`76b9e780 00007ffb`b58abab8     coreclr!MethodDescCallSite::CallTargetWorker+0x208
25 (Inline Function) --------`--------     coreclr!MethodDescCallSite::Call+0xb
26 000000d0`76b9e8c0 00007ffb`b58acc19     coreclr!RunMainInternal+0x11c
```

```
27 000000d0`76b9e9e0 00007ffb`b58acf2d     coreclr!RunMain+0xd1
28 000000d0`76b9ea70 00007ffb`b58ac1bb     coreclr!Assembly::ExecuteMainMethod+0x199
29 000000d0`76b9ed40 00007ffb`b58a704c     coreclr!CorHost2::ExecuteAssembly+0x1cb
2a 000000d0`76b9ee50 00007ffb`bec8e8ec     coreclr!coreclr_execute_assembly+0xcc
2b (Inline Function) --------`--------     hostpolicy!coreclr_t::execute_assembly+0x2d
2c 000000d0`76b9eef0 00007ffb`bec8ebbc     hostpolicy!run_app_for_context+0x58c
2d 000000d0`76b9f020 00007ffb`bec8f4ca     hostpolicy!run_app+0x3c
2e 000000d0`76b9f060 00007ffb`c83bd986     hostpolicy!corehost_main+0x15a
2f 000000d0`76b9f160 00007ffb`c83bff66     hostfxr!execute_app+0x2e6
30 000000d0`76b9f1f0 00007ffb`c83c204c     hostfxr!`anonymous namespace'::read_config_and_execute+0xa6
31 000000d0`76b9f2e0 00007ffb`c83c0533     hostfxr!fx_muxer_t::handle_exec_host_command+0x16c
32 000000d0`76b9f390 00007ffb`c83b8460     hostfxr!fx_muxer_t::execute+0x483
33 000000d0`76b9f4d0 00007ff6`09cdaae3     hostfxr!hostfxr_main_startupinfo+0xa0
34 000000d0`76b9f5d0 00007ff6`09cdaef6     ApplicationA_exe!exe_start+0x793
35 000000d0`76b9f780 00007ff6`09ce2818     ApplicationA_exe!wmain+0x146
36 (Inline Function) --------`--------     ApplicationA_exe!invoke_main+0x22
37 000000d0`76b9f7f0 00007ffb`e86253e0     ApplicationA_exe!__scrt_common_main_seh+0x10c
38 000000d0`76b9f830 00007ffb`e8d2485b     kernel32!BaseThreadInitThunk+0x10
39 000000d0`76b9f860 00000000`00000000     ntdll!RtlUserThreadStart+0x2b

   1  Id: 1bcc.e34 Suspend: 0 Teb: 000000d0`76d73000 Unfrozen
 # Child-SP          RetAddr               Call Site
00 000000d0`76f7f4d8 00007ffb`e8d36cdf     ntdll!NtWaitForWorkViaWorkerFactory+0x14
01 000000d0`76f7f4e0 00007ffb`e86253e0     ntdll!TppWorkerThread+0x2df
02 000000d0`76f7f7d0 00007ffb`e8d2485b     kernel32!BaseThreadInitThunk+0x10
03 000000d0`76f7f800 00000000`00000000     ntdll!RtlUserThreadStart+0x2b

   2  Id: 1bcc.1e10 Suspend: 0 Teb: 000000d0`76d75000 Unfrozen
 # Child-SP          RetAddr               Call Site
00 000000d0`770ff738 00007ffb`e8d36cdf     ntdll!NtWaitForWorkViaWorkerFactory+0x14
01 000000d0`770ff740 00007ffb`e86253e0     ntdll!TppWorkerThread+0x2df
02 000000d0`770ffa30 00007ffb`e8d2485b     kernel32!BaseThreadInitThunk+0x10
03 000000d0`770ffa60 00000000`00000000     ntdll!RtlUserThreadStart+0x2b

   3  Id: 1bcc.1d58 Suspend: 0 Teb: 000000d0`76d77000 Unfrozen
 # Child-SP          RetAddr               Call Site
00 000000d0`7727f788 00007ffb`e8d36cdf     ntdll!NtWaitForWorkViaWorkerFactory+0x14
01 000000d0`7727f790 00007ffb`e86253e0     ntdll!TppWorkerThread+0x2df
02 000000d0`7727fa80 00007ffb`e8d2485b     kernel32!BaseThreadInitThunk+0x10
03 000000d0`7727fab0 00000000`00000000     ntdll!RtlUserThreadStart+0x2b

   4  Id: 1bcc.1a9c Suspend: 0 Teb: 000000d0`76d79000 Unfrozen ".NET EventPipe"
 # Child-SP          RetAddr               Call Site
00 000000d0`773ff398 00007ffb`e644dcb0     ntdll!NtWaitForMultipleObjects+0x14
01 000000d0`773ff3a0 00007ffb`e644dbae     KERNELBASE!WaitForMultipleObjectsEx+0xf0
02 000000d0`773ff690 00007ffb`b591693f     KERNELBASE!WaitForMultipleObjects+0xe
03 000000d0`773ff6d0 00007ffb`b59168a0     coreclr!ds_ipc_poll+0x7f
04 000000d0`773ff950 00007ffb`b5916784     coreclr!ds_ipc_stream_factory_get_next_available_stream+0x108
05 000000d0`773ffa20 00007ffb`e86253e0     coreclr!server_thread+0x54
06 000000d0`773ffa90 00007ffb`e8d2485b     kernel32!BaseThreadInitThunk+0x10
07 000000d0`773ffac0 00000000`00000000     ntdll!RtlUserThreadStart+0x2b

   5  Id: 1bcc.17ec Suspend: 0 Teb: 000000d0`76d7b000 Unfrozen ".NET Debugger"
 # Child-SP          RetAddr               Call Site
00 000000d0`7757f888 00007ffb`e644dcb0     ntdll!NtWaitForMultipleObjects+0x14
01 000000d0`7757f890 00007ffb`b5907a9e     KERNELBASE!WaitForMultipleObjectsEx+0xf0
02 000000d0`7757fb80 00007ffb`b5907e26     coreclr!DebuggerRCThread::MainLoop+0xee
03 000000d0`7757fc40 00007ffb`b590785b     coreclr!DebuggerRCThread::ThreadProc+0x12e
04 000000d0`7757fca0 00007ffb`e86253e0     coreclr!DebuggerRCThread::ThreadProcStatic+0x5b
05 000000d0`7757fcd0 00007ffb`e8d2485b     kernel32!BaseThreadInitThunk+0x10
06 000000d0`7757fd00 00000000`00000000     ntdll!RtlUserThreadStart+0x2b

   6  Id: 1bcc.470 Suspend: 0 Teb: 000000d0`76d7d000 Unfrozen ".NET Finalizer"
 # Child-SP          RetAddr               Call Site
00 000000d0`776ff308 00007ffb`e644dcb0     ntdll!NtWaitForMultipleObjects+0x14
01 000000d0`776ff310 00007ffb`b5908a90     KERNELBASE!WaitForMultipleObjectsEx+0xf0
02 000000d0`776ff600 00007ffb`b590889f     coreclr!FinalizerThread::WaitForFinalizerEvent+0x78
03 000000d0`776ff640 00007ffb`b58aef05     coreclr!FinalizerThread::FinalizerThreadWorker+0x4f
04 (Inline Function) --------`--------     coreclr!ManagedThreadBase_DispatchInner+0xd
05 000000d0`776ff890 00007ffb`b58aee2d     coreclr!ManagedThreadBase_DispatchMiddle+0x79
06 000000d0`776ff940 00007ffb`b58fe921     coreclr!ManagedThreadBase_DispatchOuter+0x8d
07 (Inline Function) --------`--------     coreclr!ManagedThreadBase_NoADTransition+0x28
08 (Inline Function) --------`--------     coreclr!ManagedThreadBase::FinalizerBase+0x28
09 000000d0`776ff9b0 00007ffb`e86253e0     coreclr!FinalizerThread::FinalizerThreadStart+0x91
0a 000000d0`776ffac0 00007ffb`e8d2485b     kernel32!BaseThreadInitThunk+0x10
0b 000000d0`776ffaf0 00000000`00000000     ntdll!RtlUserThreadStart+0x2b

   7  Id: 1bcc.1a4 Suspend: 0 Teb: 000000d0`76d83000 Unfrozen
 # Child-SP          RetAddr               Call Site
00 000000d0`779ffc88 00007ffb`e770d2de     win32u!NtUserMsgWaitForMultipleObjectsEx+0x14
01 000000d0`779ffc90 00007ffb`e770d1d5     user32!RealMsgWaitForMultipleObjectsEx+0x1e
02 000000d0`779ffcd0 00007ffb`c2509970     user32!MsgWaitForMultipleObjects+0x55
03 000000d0`779ffd10 00007ffb`c25098c9     GdiPlus!BackgroundThreadProc+0x70
04 000000d0`779ffd80 00007ffb`e86253e0     GdiPlus!DllRefCountSafeThreadThunk+0x29
05 000000d0`779ffdb0 00007ffb`e8d2485b     kernel32!BaseThreadInitThunk+0x10
06 000000d0`779ffde0 00000000`00000000     ntdll!RtlUserThreadStart+0x2b

   8  Id: 1bcc.c6c Suspend: 0 Teb: 000000d0`76d85000 Unfrozen
 # Child-SP          RetAddr               Call Site
00 000000d0`77b7f208 00007ffb`e644dcb0     ntdll!NtWaitForMultipleObjects+0x14
01 000000d0`77b7f210 00007ffb`e7b2f598     KERNELBASE!WaitForMultipleObjectsEx+0xf0
02 000000d0`77b7f500 00007ffb`e7b2f40a     combase!WaitCoalesced+0xa4
03 000000d0`77b7f790 00007ffb`e7b2f20c     combase!CROIDTable::WorkerThreadLoop+0x5a
```

```
04 000000d0`77b7f7e0 00007ffb`e7b2f189     combase!CRpcThread::WorkerLoop+0x58
05 000000d0`77b7f850 00007ffb`e86253e0     combase!CRpcThreadCache::RpcWorkerThreadEntry+0x29
06 000000d0`77b7f880 00007ffb`e8d2485b     kernel32!BaseThreadInitThunk+0x10
07 000000d0`77b7f8b0 00000000`00000000     ntdll!RtlUserThreadStart+0x2b

   9  Id: 1bcc.1044 Suspend: 0 Teb: 000000d0`76d87000 Unfrozen
 # Child-SP          RetAddr               Call Site
00 000000d0`77cff6c8 00007ffb`e8d36cdf     ntdll!NtWaitForWorkViaWorkerFactory+0x14
01 000000d0`77cff6d0 00007ffb`e86253e0     ntdll!TppWorkerThread+0x2df
02 000000d0`77cff9c0 00007ffb`e8d2485b     kernel32!BaseThreadInitThunk+0x10
03 000000d0`77cff9f0 00000000`00000000     ntdll!RtlUserThreadStart+0x2b

  10  Id: 1bcc.1d40 Suspend: 0 Teb: 000000d0`76d89000 Unfrozen
 # Child-SP          RetAddr               Call Site
00 000000d0`77e7f448 00007ffb`e8d36cdf     ntdll!NtWaitForWorkViaWorkerFactory+0x14
01 000000d0`77e7f450 00007ffb`e86253e0     ntdll!TppWorkerThread+0x2df
02 000000d0`77e7f740 00007ffb`e8d2485b     kernel32!BaseThreadInitThunk+0x10
03 000000d0`77e7f770 00000000`00000000     ntdll!RtlUserThreadStart+0x2b

  11  Id: 1bcc.1cf8 Suspend: 0 Teb: 000000d0`76d8b000 Unfrozen ".NET System Events"
 # Child-SP          RetAddr               Call Site
00 000000d0`77fff338 00007ffb`e771472e     win32u!NtUserGetMessage+0x14
01 000000d0`77fff340 00007ffb`c0bb6979     user32!GetMessageW+0x2e
02 000000d0`77fff3a0 00007ffb`c0bb63f2     Microsoft_Win32_SystemEvents!
03 000000d0`77fff480 00007ffb`b5942eb3     Microsoft_Win32_SystemEvents!Microsoft.Win32.SystemEvents.WindowThreadProc+0x92
04 000000d0`77fff4f0 00007ffb`b58c1568     coreclr!CallDescrWorkerInternal+0x83
05 000000d0`77fff530 00007ffb`b59315a3     coreclr!DispatchCallSimple+0x60
06 000000d0`77fff5c0 00007ffb`b58aef05     coreclr!ThreadNative::KickOffThread_Worker+0x63
07 (Inline Function) --------`--------     coreclr!ManagedThreadBase_DispatchInner+0xd
08 000000d0`77fff620 00007ffb`b58aee2d     coreclr!ManagedThreadBase_DispatchMiddle+0x79
09 000000d0`77fff6d0 00007ffb`b58aefbb     coreclr!ManagedThreadBase_DispatchOuter+0x8d
0a (Inline Function) --------`--------     coreclr!ManagedThreadBase_FullTransition+0x28
0b (Inline Function) --------`--------     coreclr!ManagedThreadBase::KickOff+0x28
0c 000000d0`77fff740 00007ffb`e86253e0     coreclr!ThreadNative::KickOffThread+0x7b
0d 000000d0`77fff7a0 00007ffb`e8d2485b     kernel32!BaseThreadInitThunk+0x10
0e 000000d0`77fff7d0 00000000`00000000     ntdll!RtlUserThreadStart+0x2b
```

Note: We see that threads #0, #4 - #6, #11 have **coreclr** module on their stack traces (the previous versions of .NET Framework used the **clr** module and **mscorwks** module). We also see signs of software exception (in red) and exception stack trace #0, which has signs of managed code exception processing (in yellow). Finally, the stack trace fragment from our *ApplicationA* module is shown in green.

8. We now check the version of .NET used when *ApplicationA* was running:

```
0:000> lmv m coreclr
Browse full module list
start             end                 module name
00007ffb`b57f0000 00007ffb`b5c9a000   coreclr    (private pdb symbols)
C:\ProgramData\Dbg\sym\coreclr.pdb\80E26C0B98AE42B2AAB3114358114E551\coreclr.pdb
    Loaded symbol image file: coreclr.dll
    Image path: C:\Program Files\dotnet\shared\Microsoft.NETCore.App\9.0.4\coreclr.dll
    Image name: coreclr.dll
    Browse all global symbols  functions  data  Symbol Reload
    Timestamp:        Thu Mar 13 22:01:10 2025 (67D355A6)
    CheckSum:         0049FD9A
    ImageSize:        004AA000
    File version:     9.0.425.16305
    Product version:  9.0.425.16305
    File flags:       0 (Mask 3F)
    File OS:          4 Unknown Win32
    File type:        0.0 Unknown
    File date:        00000000.00000000
    Translations:     0409.04b0
    Information from resource tables:
        CompanyName:      Microsoft Corporation
        ProductName:      Microsoft® .NET
        InternalName:     CoreCLR.dll
        OriginalFilename: CoreCLR.dll
        ProductVersion:   9,0,425,16305 @Commit: f57e6dc747158ab7ade4e62a75a6750d16b771e8
        FileVersion:      9,0,425,16305 @Commit: f57e6dc747158ab7ade4e62a75a6750d16b771e8
        FileDescription:  .NET Runtime
```

```
        LegalCopyright:   © Microsoft Corporation. All rights reserved.
        Comments:         Flavor=Retail
```

9. WinDbg may load the SOS extension automatically and its version may not be exactly the same as the SOS extension from the process memory dump .NET version.

```
0:000> .chain
Extension DLL search Path:
[...]
Extension DLL chain:
    C:\Program Files\WindowsApps\Microsoft.WinDbg_1.2504.15001.0_x64__8wekyb3d8bbwe\amd64\winext\sos\sos: image 9,0,12,7501 @Commit:
a651406e39038aef1dbc7c8097b52953284dba27, API 2.0.0, built Sat Jan 25 08:30:17 2025
        [path: C:\Program Files\WindowsApps\Microsoft.WinDbg_1.2504.15001.0_x64__8wekyb3d8bbwe\amd64\winext\sos\sos.dll]
    DbgEngCoreDMExt: image 10.0.27829.1001, API 0.0.0,
        [path: C:\Program Files\WindowsApps\Microsoft.WinDbg_1.2504.15001.0_x64__8wekyb3d8bbwe\amd64\winext\DbgEngCoreDMExt.dll]
    CLRComposition: image 10.0.27829.1001, API 0.0.0,
        [path: C:\Program Files\WindowsApps\Microsoft.WinDbg_1.2504.15001.0_x64__8wekyb3d8bbwe\amd64\winext\CLRComposition.dll]
    MachOBinComposition: image 10.0.27829.1001, API 0.0.0,
        [path: C:\Program Files\WindowsApps\Microsoft.WinDbg_1.2504.15001.0_x64__8wekyb3d8bbwe\amd64\winext\MachOBinComposition.dll]
    ELFBinComposition: image 10.0.27829.1001, API 0.0.0,
        [path: C:\Program Files\WindowsApps\Microsoft.WinDbg_1.2504.15001.0_x64__8wekyb3d8bbwe\amd64\winext\ELFBinComposition.dll]
    dbghelp: image 10.0.27829.1001, API 10.0.6,
        [path: C:\Program Files\WindowsApps\Microsoft.WinDbg_1.2504.15001.0_x64__8wekyb3d8bbwe\amd64\dbghelp.dll]
    exts: image 10.0.27829.1001, API 1.0.0,
        [path: C:\Program Files\WindowsApps\Microsoft.WinDbg_1.2504.15001.0_x64__8wekyb3d8bbwe\amd64\WINXP\exts.dll]
    uext: image 10.0.27829.1001, API 1.0.0,
        [path: C:\Program Files\WindowsApps\Microsoft.WinDbg_1.2504.15001.0_x64__8wekyb3d8bbwe\amd64\winext\uext.dll]
    ntsdexts: image 10.0.27829.1001, API 1.0.0,
        [path: C:\Program Files\WindowsApps\Microsoft.WinDbg_1.2504.15001.0_x64__8wekyb3d8bbwe\amd64\WINXP\ntsdexts.dll]
```

Note: if this extension is not loaded, all commands related to .NET will not be available:

```
0:000> .unload C:\Program
Files\WindowsApps\Microsoft.WinDbg_1.2504.15001.0_x64__8wekyb3d8bbwe\amd64\winext\sos\sos
Unloading C:\Program
Files\WindowsApps\Microsoft.WinDbg_1.2504.15001.0_x64__8wekyb3d8bbwe\amd64\winext\sos\sos
extension DLL

0:000> .chain
Extension DLL search Path:
[...]
Extension DLL chain:
    DbgEngCoreDMExt: image 10.0.27829.1001, API 0.0.0,
        [path: C:\Program Files\WindowsApps\Microsoft.WinDbg_1.2504.15001.0_x64__8wekyb3d8bbwe\amd64\winext\DbgEngCoreDMExt.dll]
    CLRComposition: image 10.0.27829.1001, API 0.0.0,
        [path: C:\Program Files\WindowsApps\Microsoft.WinDbg_1.2504.15001.0_x64__8wekyb3d8bbwe\amd64\winext\CLRComposition.dll]
    MachOBinComposition: image 10.0.27829.1001, API 0.0.0,
        [path: C:\Program Files\WindowsApps\Microsoft.WinDbg_1.2504.15001.0_x64__8wekyb3d8bbwe\amd64\winext\MachOBinComposition.dll]
    ELFBinComposition: image 10.0.27829.1001, API 0.0.0,
        [path: C:\Program Files\WindowsApps\Microsoft.WinDbg_1.2504.15001.0_x64__8wekyb3d8bbwe\amd64\winext\ELFBinComposition.dll]
    dbghelp: image 10.0.27829.1001, API 10.0.6,
        [path: C:\Program Files\WindowsApps\Microsoft.WinDbg_1.2504.15001.0_x64__8wekyb3d8bbwe\amd64\dbghelp.dll]
    exts: image 10.0.27829.1001, API 1.0.0,
        [path: C:\Program Files\WindowsApps\Microsoft.WinDbg_1.2504.15001.0_x64__8wekyb3d8bbwe\amd64\WINXP\exts.dll]
    uext: image 10.0.27829.1001, API 1.0.0,
        [path: C:\Program Files\WindowsApps\Microsoft.WinDbg_1.2504.15001.0_x64__8wekyb3d8bbwe\amd64\winext\uext.dll]
    ntsdexts: image 10.0.27829.1001, API 1.0.0,
        [path: C:\Program Files\WindowsApps\Microsoft.WinDbg_1.2504.15001.0_x64__8wekyb3d8bbwe\amd64\WINXP\ntsdexts.dll]

0:000> !pe
pe is not extension gallery command
No export pe found
```

Note: The SOS version can also be checked by listing all loaded WinDbg extensions (**sos.dll** is used for .NET analysis):

10. We load the SOS extension we previosly installed with the *dotnet-sos* tool. See the **SOS Setup (Specific .NET)** slide.

```
0:000> .load C:\Users\dmitr\.dotnet\sos\sos.dll
```

```
0:000> .chain
Extension DLL search Path:
[...]
Extension DLL chain:
    C:\Users\dmitr\.dotnet\sos\sos.dll: image 9,0,12,21003 @Commit: ebd1db46a2395bd7de706694ff54f1c9526951d7, API 2.0.0, built Fri Apr
11 05:48:49 2025
        [path: C:\Users\dmitr\.dotnet\sos\sos.dll]
    DbgEngCoreDMExt: image 10.0.27829.1001, API 0.0.0,
        [path: C:\Program Files\WindowsApps\Microsoft.WinDbg_1.2504.15001.0_x64__8wekyb3d8bbwe\amd64\winext\DbgEngCoreDMExt.dll]
    CLRComposition: image 10.0.27829.1001, API 0.0.0,
        [path: C:\Program Files\WindowsApps\Microsoft.WinDbg_1.2504.15001.0_x64__8wekyb3d8bbwe\amd64\winext\CLRComposition.dll]
    MachOBinComposition: image 10.0.27829.1001, API 0.0.0,
        [path: C:\Program Files\WindowsApps\Microsoft.WinDbg_1.2504.15001.0_x64__8wekyb3d8bbwe\amd64\winext\MachOBinComposition.dll]
    ELFBinComposition: image 10.0.27829.1001, API 0.0.0,
        [path: C:\Program Files\WindowsApps\Microsoft.WinDbg_1.2504.15001.0_x64__8wekyb3d8bbwe\amd64\winext\ELFBinComposition.dll]
    dbghelp: image 10.0.27829.1001, API 10.0.6,
        [path: C:\Program Files\WindowsApps\Microsoft.WinDbg_1.2504.15001.0_x64__8wekyb3d8bbwe\amd64\dbghelp.dll]
    exts: image 10.0.27829.1001, API 1.0.0,
        [path: C:\Program Files\WindowsApps\Microsoft.WinDbg_1.2504.15001.0_x64__8wekyb3d8bbwe\amd64\WINXP\exts.dll]
    uext: image 10.0.27829.1001, API 1.0.0,
        [path: C:\Program Files\WindowsApps\Microsoft.WinDbg_1.2504.15001.0_x64__8wekyb3d8bbwe\amd64\winext\uext.dll]
    ntsdexts: image 10.0.27829.1001, API 1.0.0,
        [path: C:\Program Files\WindowsApps\Microsoft.WinDbg_1.2504.15001.0_x64__8wekyb3d8bbwe\amd64\WINXP\ntsdexts.dll]
```

11. Now, we check if there is a .NET exception on the current thread 0 (W):

```
0:000> !pe
Exception object: 0000020ed20130f8
Exception type:   System.NullReferenceException
Message:          Object reference not set to an instance of an object.
InnerException:   <none>
StackTrace (generated):
    SP               IP               Function
    000000D076B9DEF0 00007FFB55D8CB37 ApplicationA!ApplicationA.ApplicationA.CrashButton_Click(System.Object, System.EventArgs)+0x27
    000000D076B9DF10 00007FFBB4F78DD5 System_Windows_Forms!System.Windows.Forms.Button.OnClick(System.EventArgs)+0x195
    000000D076B9DFC0 00007FFBB4F78F69 System_Windows_Forms!System.Windows.Forms.Button.OnMouseUp(System.Windows.Forms.MouseEventArgs)+0xe9
    000000D076B9E020 00007FFBB4F63D6D System_Windows_Forms!System.Windows.Forms.Control.WmMouseUp(System.Windows.Forms.Message ByRef,
System.Windows.Forms.MouseButtons, Int32)+0x2bd
    000000D076B9E0B0 00007FFB55D84D09 System_Windows_Forms!System.Windows.Forms.Control.WndProc(System.Windows.Forms.Message ByRef)+0x8d9
    000000D076B9E140 00007FFB55D8B5D7 System_Windows_Forms!System.Windows.Forms.ButtonBase.WndProc(System.Windows.Forms.Message ByRef)+0x97
    000000D076B9E1A0 00007FFB55D83B69 System_Windows_Forms!System.Windows.Forms.NativeWindow.Callback(Windows.Win32.Foundation.HWND, Windows.Win32.MessageId,
Windows.Win32.Foundation.WPARAM, Windows.Win32.Foundation.LPARAM)+0xc9

StackTraceString: <none>
HResult: 80004003
```

Note: We also double-check that no other threads have exceptions by executing **!pe** command for each thread using **~*e** command:

```
0:000> ~*e !pe
Exception object: 0000020ed20130f8
Exception type:   System.NullReferenceException
Message:          Object reference not set to an instance of an object.
InnerException:   <none>
StackTrace (generated):
    SP               IP               Function
    000000D076B9DEF0 00007FFB55D8CB37 ApplicationA!ApplicationA.ApplicationA.CrashButton_Click(System.Object, System.EventArgs)+0x27
    000000D076B9DF10 00007FFBB4F78DD5 System_Windows_Forms!System.Windows.Forms.Button.OnClick(System.EventArgs)+0x195
    000000D076B9DFC0 00007FFBB4F78F69 System_Windows_Forms!System.Windows.Forms.Button.OnMouseUp(System.Windows.Forms.MouseEventArgs)+0xe9
    000000D076B9E020 00007FFBB4F63D6D System_Windows_Forms!System.Windows.Forms.Control.WmMouseUp(System.Windows.Forms.Message ByRef,
System.Windows.Forms.MouseButtons, Int32)+0x2bd
    000000D076B9E0B0 00007FFB55D84D09 System_Windows_Forms!System.Windows.Forms.Control.WndProc(System.Windows.Forms.Message ByRef)+0x8d9
    000000D076B9E140 00007FFB55D8B5D7 System_Windows_Forms!System.Windows.Forms.ButtonBase.WndProc(System.Windows.Forms.Message ByRef)+0x97
    000000D076B9E1A0 00007FFB55D83B69 System_Windows_Forms!System.Windows.Forms.NativeWindow.Callback(Windows.Win32.Foundation.HWND, Windows.Win32.MessageId,
Windows.Win32.Foundation.WPARAM, Windows.Win32.Foundation.LPARAM)+0xc9

StackTraceString: <none>
HResult: 80004003
The current thread is unmanaged
The current thread is unmanaged
The current thread is unmanaged
The current thread is unmanaged
The current thread is unmanaged
There is no current managed exception on this thread
The current thread is unmanaged
The current thread is unmanaged
The current thread is unmanaged
```

```
The current thread is unmanaged
There is no current managed exception on this thread
```

12. Let's see what **!analyze -v** command says:

```
0:000> !analyze -v
.....................................................................
.....................................................
ClrmaManagedAnalysis::AssociateClient
AssociateClient trying managed CLRMA
AssociateClient trying DAC CLRMA
*******************************************************************************
*                                                                             *
*                        Exception Analysis                                   *
*                                                                             *
*******************************************************************************

*** WARNING: Unable to verify checksum for ApplicationA.dll
*** WARNING: Unable to verify checksum for ApplicationA.exe
ClrmaManagedAnalysis::GetThread 19fc
ClrmaThread::Initialize 19fc
~ClrmaThread
ClrmaManagedAnalysis::GetThread 0e34
ClrmaThread::Initialize 0e34
ClrmaThread::Initialize FAILED managed thread not found
~ClrmaThread
ClrmaManagedAnalysis::GetThread 1e10
ClrmaThread::Initialize 1e10
ClrmaThread::Initialize FAILED managed thread not found
~ClrmaThread
ClrmaManagedAnalysis::GetThread 1d58
ClrmaThread::Initialize 1d58
ClrmaThread::Initialize FAILED managed thread not found
~ClrmaThread
ClrmaManagedAnalysis::GetThread 1a9c
ClrmaThread::Initialize 1a9c
ClrmaThread::Initialize FAILED managed thread not found
~ClrmaThread
ClrmaManagedAnalysis::GetThread 17ec
ClrmaThread::Initialize 17ec
ClrmaThread::Initialize FAILED managed thread not found
~ClrmaThread
ClrmaManagedAnalysis::GetThread 0470
ClrmaThread::Initialize 0470
~ClrmaThread
ClrmaManagedAnalysis::GetThread 01a4
ClrmaThread::Initialize 01a4
ClrmaThread::Initialize FAILED managed thread not found
~ClrmaThread
ClrmaManagedAnalysis::GetThread 0c6c
ClrmaThread::Initialize 0c6c
ClrmaThread::Initialize FAILED managed thread not found
~ClrmaThread
ClrmaManagedAnalysis::GetThread 1044
ClrmaThread::Initialize 1044
ClrmaThread::Initialize FAILED managed thread not found
~ClrmaThread
ClrmaManagedAnalysis::GetThread 1d40
ClrmaThread::Initialize 1d40
ClrmaThread::Initialize FAILED managed thread not found
~ClrmaThread
ClrmaManagedAnalysis::GetThread 1cf8
ClrmaThread::Initialize 1cf8
~ClrmaThread
ClrmaManagedAnalysis::get_ProviderName
ClrmaManagedAnalysis::GetThread ffffffff
ClrmaThread::Initialize 19fc
ClrmaThread::get_CurrentException
~ClrmaException
ClrmaThread::get_NestedExceptionCount
~ClrmaThread
Failed to request MethodData, not in JIT code range

KEY_VALUES_STRING: 1

    Key  : Analysis.CPU.mSec
    Value: 4531

    Key  : Analysis.Elapsed.mSec
    Value: 6221

    Key  : Analysis.IO.Other.Mb
    Value: 4

    Key  : Analysis.IO.Read.Mb
    Value: 4

    Key  : Analysis.IO.Write.Mb
    Value: 13

    Key  : Analysis.Init.CPU.mSec
    Value: 13140

    Key  : Analysis.Init.Elapsed.mSec
    Value: 3614105

    Key  : Analysis.Memory.CommitPeak.Mb
    Value: 407

    Key  : Analysis.Version.DbgEng
    Value: 10.0.27829.1001

    Key  : Analysis.Version.Description
    Value: 10.2503.24.01 amd64fre

    Key  : Analysis.Version.Ext
    Value: 1.2503.24.1

    Key  : CLR.Engine
    Value: CORECLR

    Key  : CLR.Version
    Value: 9.0.425.16305

    Key  : Failure.Bucket
    Value: BREAKPOINT_80000003_win32u.dll!NtUserWaitMessage
```

```
    Key  : Failure.Exception.Code
    Value: 0x80000003

    Key  : Failure.Exception.Record
    Value: 0x7ffbb57856e8

    Key  : Failure.Hash
    Value: {a106cd41-a8b1-c51d-6d94-a75661270841}

    Key  : Failure.ProblemClass.Primary
    Value: BREAKPOINT

    Key  : Faulting.IP.Type
    Value: Null

    Key  : Timeline.OS.Boot.DeltaSec
    Value: 937

    Key  : Timeline.Process.Start.DeltaSec
    Value: 42

    Key  : WER.OS.Branch
    Value: co_release

    Key  : WER.OS.Version
    Value: 10.0.22000.1

    Key  : WER.Process.Version
    Value: 1.0.0.0


FILE_IN_CAB:  ApplicationA.DMP

NTGLOBALFLAG:  400

APPLICATION_VERIFIER_FLAGS:  0

EXCEPTION_RECORD:  00007ffbb57856e8 -- (.exr 0x7ffbb57856e8)
ExceptionAddress: 00007ffbb52de4f8 (System_Windows_Forms+0x000000000080e4f8)
   ExceptionCode: 560bb828
  ExceptionFlags: 00007ffb
NumberParameters: -1255283464
   Parameter[0]: 00007ffb56039788
   Parameter[1]: 00007ffb560b07b0
   Parameter[2]: 00007ffb560b07f8
   Parameter[3]: 00007ffbb52de4f8
   Parameter[4]: 00007ffbb52de4f8
   Parameter[5]: 00007ffbb52de4f8
   Parameter[6]: 00007ffbb52de4f8
   Parameter[7]: 00007ffbb52de4f8
   Parameter[8]: 00007ffbb52de4f8
   Parameter[9]: 00007ffbb52de4f8
   Parameter[10]: 00007ffbb52de4f8
   Parameter[11]: 00007ffbb52de4f8
   Parameter[12]: 00007ffbb52de4f8
   Parameter[13]: 00007ffb560b8078
   Parameter[14]: 00007ffbb52de4f8

FAULTING_THREAD:  19fc

PROCESS_NAME:  ApplicationA.dll

ERROR_CODE: (NTSTATUS) 0x80000003 - {EXCEPTION}  Breakpoint  A breakpoint has been reached.

EXCEPTION_CODE_STR:  80000003

CONTEXT:  00007ffbe8d496fd -- (.cxr 0x7ffbe8d496fd)
rax=4080ce8040000001 rbx=c35b5d5e5f5c415d rcx=4810438d480f7388
rdx=415e415f4178c483 rsi=17b08fb60f000000 rdi=618d4448708b0000
rip=001786e8e5b4894a rsp=0030253c8b4865cc rbp=3025048b48650000
 r8=0000c824a48944ff  r9=39480e78e4854500 r10=840f001786e0cdb4
r11=ef0d1d8bfffffdbd r12=440007f644e80014 r13=a48944e32344e08b
r14=4c8d41000000c824 r15=000017b08f880124
iopl=0         nv dn di pl nz na po cy
cs=0f3f  ss=0030  ds=7485  es=0944  fs=8300  gs=247c             efl=02a1850f
001786e8`e5b4894a ???
Resetting default scope

IP_ON_HEAP:  001786e8e5b4894a
The fault address in not in any loaded module, please check your build's rebase
log at <releasedir>\bin\build_logs\timebuild\ntrebase.log for module which may
contain the address if it were loaded.

FRAME_ONE_INVALID: 1

STACK_TEXT:
000000d0`76b9b218 00007ffb`55d9c454     : 000000d0`00000000 00000000`00000000 000037c7`aacf9f22 00007ffb`b5bc1d60 : win32u!NtUserWaitMessage+0x14
000000d0`76b9b220 00007ffb`b5237d33     : 0000020e`d200d860 000000d0`76b9b2f8 000000d0`76b9b108 00000000`00000000 : System_Windows_Forms_Primitives!Windows.Win32.PInvoke.WaitMessage+0x74
000000d0`76b9b2d0 00007ffb`b5237c1a     : 0000020e`d2812da8 00000000`00000004 00000000`00000001 00000000`0000000d :
System_Windows_Forms!System.Windows.Forms.Application.LightThreadContext.FPushMessageLoop+0x43
000000d0`76b9b360 00007ffb`b5239597     : 0000020e`d2825fa8 00000000`00000001 00000000`0000051a 00000000`00000030 :
System_Windows_Forms!System.Windows.Forms.Application.LightThreadContext.RunMessageLoop+0xa
000000d0`76b9b390 00007ffb`b52392d2     : 0000020e`d200d860 00000000`00000004 0000020e`d20201d8 00007ffb`5602f3b0 :
System_Windows_Forms!System.Windows.Forms.Application.ThreadContext.RunMessageLoopInner+0x287
000000d0`76b9b410 00007ffb`b517feae     : 0000020e`d2812da8 00000000`00000004 0000020e`d2846d88 00007ffb`5602f3b0 :
System_Windows_Forms!System.Windows.Forms.Application.ThreadContext.RunMessageLoop+0x42
000000d0`76b9b470 00007ffb`b52390d9     : 0000020e`d2013b18 00000000`00000000 00000000`00000200 000000d0`76b9b2d0 : System_Windows_Forms!System.Windows.Forms.Form.ShowDialog+0x27e
000000d0`76b9b520 00007ffb`55d83d0e     : 0000020e`d200d860 0000020e`d28249b0 0000020e`ce458c50 00007ffb`55f93ff0 :
System_Windows_Forms!System.Windows.Forms.Application.ThreadContext.OnThreadException+0x99
000000d0`76b9b590 00007ffb`b58cc4ef     : 000000d0`76b9b810 000000d0`76b9b850 000000d0`76b9c308 000000d0`76b9e1a0 : System_Windows_Forms!System.Windows.Forms.NativeWindow.Callback+0x26e
000000d0`76b9b5f0 00007ffb`b09e7a56     : 000000d0`76b9bf90 00007ffb`55d83cdb 000000d0`76b9bed0 000000d0`76b9bed0 : coreclr!CallCatchFunclet+0x17f
000000d0`76b9b700 00007ffb`b09e717a     : 000000d0`76b9bf90 000000d0`76b9bed0 00000000`00000001 0000020e`ce50d000 : System_Private_CoreLib!System.Runtime.EH.DispatchEx+0x536
000000d0`76b9b860 00007ffb`b5942eb3     : 00000000`00000000 000000d0`76b9bed0 00000000`00000000 00007ffb`55d62874 : System_Private_CoreLib!System.Runtime.EH.RhThrowHwEx+0xaa
000000d0`76b9b8a0 00007ffb`b58c1568     : 000000d0`76d70000 0000020e`cfd50890 00007ffb`b5b95230 00007ffb`55d50af0 : coreclr!CallDescrWorkerInternal+0x83
000000d0`76b9b8e0 00007ffb`b59f5cde     : 00000000`00000000 000000d0`76b9dcb0 000000d0`76b9dcb0 0000020e`ce458c50 : coreclr!DispatchCallSimple+0x60
000000d0`76b9b970 00007ffb`b59cf58a     : 00000000`00000000 000000d0`76ba0000 000000d0`76ba0000 000000d0`76b9d510 : coreclr!HandleManagedFaultNew+0x192
000000d0`76b9d480 00007ffb`e8d9ca2a     : 00007ffb`b59270c0 00000000`00000000 0000020e`cfd50880 00000000`00000000 : coreclr!CLRVectoredExceptionHandlerShim+0xa84ca
000000d0`76b9d4d0 00007ffb`e8d559f2     : 000000d0`76b9dcb0 000000d0`76b9d7c0 00000000`00000000 00000000`00000000 : ntdll!RtlpCallVectoredHandlers+0x112
000000d0`76b9d570 00007ffb`e8dc805e     : 00007ffb`b57856e8 00007ffb`e8d496fd 0000020e`d28179c0 00007ffb`00000000 : ntdll!RtlDispatchException+0x62
000000d0`76b9d7c0 00007ffb`55d8cb36     : 00000000`000002af 00000000`00000000 000000d0`76b9dfb0 00007ffb`b4f78dd5 : ntdll!KiUserExceptionDispatch+0x2e
000000d0`76b9def0 00007ffb`b4f78dd5     : 0000020e`d2811050 0000020e`d28179c0 0000020e`d2824168 00000000`00000006 : ApplicationA!ApplicationA.ApplicationA.CrashButton_Click+0x26
000000d0`76b9df10 00007ffb`b4f78f69     : 0000020e`d28179c0 0000020e`d2824168 000000d0`76b9dee8 000000d0`76b9dfb0 : System_Windows_Forms!System.Windows.Forms.Button.OnClick+0x195
000000d0`76b9dfc0 00007ffb`b4f63d6d     : 0000020e`d28179c0 0000020e`d2824168 00000000`00000001 00000033`000000b5 : System_Windows_Forms!System.Windows.Forms.Button.OnMouseUp+0xe9
000000d0`76b9e020 00007ffb`55d84d09     : 0000020e`d28179c0 000000d0`76b9e1d0 00000000`00100000 00000000`00000001 : System_Windows_Forms!System.Windows.Forms.Control.WmMouseUp+0x2bd
000000d0`76b9e0b0 00007ffb`55d8b5d7     : 0000020e`ce517d90 000000d0`76b9e550 00000000`00000202 0000020e`ce517d90 : System_Windows_Forms!System.Windows.Forms.Control.WndProc+0x8d9
000000d0`76b9e140 00007ffb`55d83b69     : 0000020e`d28179c0 00000000`00000000 00000000`00000000 00007ffb`e8d5ff83 : System_Windows_Forms!System.Windows.Forms.ButtonBase.WndProc+0x97
000000d0`76b9e1a0 00007ffb`55d7347c     : 0000020e`d200eef0 000000d0`76b9e290 00000000`00000202 00000000`00000001 : System_Windows_Forms!System.Windows.Forms.NativeWindow.Callback+0xc9
000000d0`76b9e220 00007ffb`e7701cac     : 00000000`00000000 00000000`00000000 00000000`00000001 00000000`00000000 :
System_Windows_Forms_Primitives!ILStubClass.IL_STUB_ReversePInvoke(Windows.Win32.Foundation.HWND, Windows.Win32.MessageId, Windows.Win32.Foundation.WPARAM,
Windows.Win32.Foundation.LPARAM)+0x5c
```

```
000000d0`76b9e2a0 00007ffb`e7700f06     : 00007ffb`e8dc4060 00007ffb`55c33124 00000000`002b0572 00000000`00000202 : user32!UserCallWinProcCheckWow+0x33c
000000d0`76b9e410 00007ffb`b2d2291f     : 00007ffb`55c33124 00000000`ffffffff 0000020e`d2812da8 00007ffb`55d8bd30 : user32!DispatchMessageWorker+0x2a6
000000d0`76b9e490 00007ffb`b5237e7e     : 0000020e`d2812da8 000000d0`76b9e588 00000000`00000001 00000000`0000000d : System_Windows_Forms_Primitives!
000000d0`76b9e560 00007ffb`b5237c1a     : 0000020e`d2812da8 00000000`ffffffff 00000000`00000000 00007ffb`55f92a10 :
System_Windows_Forms!System.Windows.Forms.Application.LightThreadContext.FPushMessageLoop+0x18e
000000d0`76b9e5f0 00007ffb`b5239597     : 0000020e`d2812da8 00000000`ffffffff 00000000`00000000 00007ffb`55f92a10 :
System_Windows_Forms!System.Windows.Forms.Application.LightThreadContext.RunMessageLoop+0xa
000000d0`76b9e620 00007ffb`b52392d2     : 0000020e`d200d860 00000000`ffffffff 0000020e`d200f3c8 0000020e`cff15fd0 :
System_Windows_Forms!System.Windows.Forms.Application.ThreadContext.RunMessageLoopInner+0x287
000000d0`76b9e6a0 00007ffb`55d7189d     : 0000020e`d2812da8 00000000`ffffffff 0000020e`d2818838 00007ffb`5602f3b0 :
System_Windows_Forms!System.Windows.Forms.Application.ThreadContext.RunMessageLoop+0x42
000000d0`76b9e700 00007ffb`b5942eb3     : 00007ffb`b58c168b 000000d0`76b9ed68 000000d0`76b9ed68 000000d0`76b9e979 : ApplicationA!ApplicationA.Program.Main+0x3d
000000d0`76b9e740 00007ffb`b58c180c     : 000000d0`00000000 00000000`00000008 000000d0`76b9e7b0 00007ffb`00000001 : coreclr!CallDescrWorkerInternal+0x83
000000d0`76b9e780 00007ffb`b58abab8     : 000000d0`76b9ea30 00000000`00000001 00000000`00000000 00007ffb`b58db606 : coreclr!MethodDescCallSite::CallTargetWorker+0x208
(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : coreclr!MethodDescCallSite::Call+0xb
000000d0`76b9e8c0 00007ffb`b58acc19     : 00000000`00000000 00000000`00000000 00000000`00000001 000000d0`76b9ed68 : coreclr!RunMainInternal+0x11c
000000d0`76b9e9e0 00007ffb`b58acf2d     : 0000020e`ce50d000 00007ffb`00000001 00007ffb`55e25778 00000000`00000001 : coreclr!RunMain+0xd1
000000d0`76b9ea70 00007ffb`b58ac1bb     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : coreclr!Assembly::ExecuteMainMethod+0x199
000000d0`76b9ed40 00007ffb`b58a704c     : 00000000`00000001 000000d0`76b9ee01 00000000`00000000 00007ffb`bec72350 : coreclr!CorHost2::ExecuteAssembly+0x1cb
000000d0`76b9ee50 00007ffb`bec8e8ec     : 0000020e`ce47a6d0 0000020e`ce47a6e0 0000020e`ce44b440 0000020e`ce447040 : coreclr!coreclr_execute_assembly+0xcc
(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : hostpolicy!coreclr_t::execute_assembly+0x2d
000000d0`76b9eef0 00007ffb`bec8ebbc     : 0000020e`ce447048 000000d0`76b9f0f9 00007ffb`becc61e0 0000020e`ce447048 : hostpolicy!run_app_for_context+0x58c
000000d0`76b9f020 00007ffb`bec8f4ca     : 00000000`00000000 0000020e`ce447040 000000d0`76b9f0f9 0000020e`ce447040 : hostpolicy!run_app+0x3c
000000d0`76b9f060 00007ffb`c83bd986     : 0000020e`ce43da38 0000020e`ce43d920 00000000`00000000 000000d0`76b9f299 : hostpolicy!corehost_main+0x15a
000000d0`76b9f160 00007ffb`c83bff66     : 0000020e`ce44b040 000000d0`76b9f510 00000000`00000000 00000000`00000000 : hostfxr!execute_app+0x2e6
000000d0`76b9f1f0 00007ffb`c83c204c     : 00007ffb`c83f2898 0000020e`ce447630 000000d0`76b9f450 000000d0`76b9f400 : hostfxr!`anonymous namespace'::read_config_and_execute+0xa6
000000d0`76b9f2e0 00007ffb`c83c0533     : 000000d0`76b9f510 000000d0`76b9f530 000000d0`76b9f481 000000d0`76b9f510 : hostfxr!fx_muxer_t::handle_exec_host_command+0x16c
000000d0`76b9f390 00007ffb`c83b8460     : 000000d0`76b9f530 0000020e`ce447d10 00000000`00000001 00007ff6`09cd9b5e : hostfxr!fx_muxer_t::execute+0x483
000000d0`76b9f4d0 00007ff6`09cdaae3     : 00007ffb`e693f4f8 00007ffb`c83b99c0 000000d0`76b9f6d0 0000020e`ce447f90 : hostfxr!hostfxr_main_startupinfo+0xa0
000000d0`76b9f5d0 00007ff6`09cdaef6     : 00007ff6`09ced040 00000000`00000007 0000020e`ce447040 00000000`0000005d : ApplicationA_exe!exe_start+0x793
000000d0`76b9f780 00007ff6`09ce2818     : 00000000`00000000 00007ff6`09ce2899 0000020e`ce447040 00000000`00000000 : ApplicationA_exe!wmain+0x146
(Inline Function) --------`--------     : --------`-------- --------`-------- --------`-------- --------`-------- : ApplicationA_exe!invoke_main+0x22
000000d0`76b9f7f0 00007ffb`e86253e0     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : ApplicationA_exe!__scrt_common_main_seh+0x10c
000000d0`76b9f830 00007ffb`e8d2485b     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : kernel32!BaseThreadInitThunk+0x10
000000d0`76b9f860 00000000`00000000     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : ntdll!RtlUserThreadStart+0x2b


STACK_COMMAND: ~0s; .ecxr ; kb

SYMBOL_NAME:  win32u!NtUserWaitMessage+14

MODULE_NAME: win32u

IMAGE_NAME:  win32u.dll

FAILURE_BUCKET_ID:  BREAKPOINT_80000003_win32u.dll!NtUserWaitMessage

OS_VERSION:  10.0.22000.1

BUILDLAB_STR:  co_release

OSPLATFORM_TYPE:  x64

OSNAME:  Windows 10

IMAGE_VERSION:  10.0.22000.3260

FAILURE_ID_HASH:  {a106cd41-a8b1-c51d-6d94-a75661270841}

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

CLRMAReleaseInstance
~ClrmaManagedAnalysis
```

Note: We see that this version of WinDbg was not able to provide the unmanaged NULL pointer exception diagnostics. Rather, it points to the manual dump creation.

13. What we saw from the exception thread stack trace is that the unmanaged exception was enveloped into the managed exception. We now try to get the unmanaged exception context.

```
0:000> kL 16
 # Child-SP          RetAddr               Call Site
00 000000d0`76b9b218 00007ffb`55d9c454     win32u!NtUserWaitMessage+0x14
01 000000d0`76b9b220 00007ffb`b5237d33     System_Windows_Forms_Primitives!Windows.Win32.PInvoke.WaitMessage+0x74
02 000000d0`76b9b2d0 00007ffb`b5237c1a     System_Windows_Forms!System.Windows.Forms.Application.LightThreadContext.FPushMessageLoop+0x43
03 000000d0`76b9b360 00007ffb`b5239597     System_Windows_Forms!System.Windows.Forms.Application.LightThreadContext.RunMessageLoop+0xa
04 000000d0`76b9b390 00007ffb`b52392d2     System_Windows_Forms!System.Windows.Forms.Application.ThreadContext.RunMessageLoopInner+0x287
05 000000d0`76b9b410 00007ffb`b517feae     System_Windows_Forms!System.Windows.Forms.Application.ThreadContext.RunMessageLoop+0x42
06 000000d0`76b9b470 00007ffb`b52390d9     System_Windows_Forms!System.Windows.Forms.Form.ShowDialog+0x27e
07 000000d0`76b9b520 00007ffb`55d83d0e     System_Windows_Forms!System.Windows.Forms.Application.ThreadContext.OnThreadException+0x99
08 000000d0`76b9b590 00007ffb`b58cc4ef     System_Windows_Forms!System.Windows.Forms.NativeWindow.Callback+0x26e
09 000000d0`76b9b5f0 00007ffb`b09e7a56     coreclr!CallCatchFunclet+0x17f
0a 000000d0`76b9b700 00007ffb`b09e717a     System_Private_CoreLib!System.Runtime.EH.DispatchEx+0x536
0b 000000d0`76b9b860 00007ffb`b5942eb3     System_Private_CoreLib!System.Runtime.EH.RhThrowHwEx+0xaa
0c 000000d0`76b9b8a0 00007ffb`b58c1568     coreclr!CallDescrWorkerInternal+0x83
0d 000000d0`76b9b8e0 00007ffb`b59f5cde     coreclr!DispatchCallSimple+0x60
0e 000000d0`76b9b970 00007ffb`b59cf58a     coreclr!HandleManagedFaultNew+0x192
0f 000000d0`76b9d480 00007ffb`e8d9ca2a     coreclr!CLRVectoredExceptionHandlerShim+0xa84ca
10 000000d0`76b9d4d0 00007ffb`e8d559f2     ntdll!RtlpCallVectoredHandlers+0x112
11 000000d0`76b9d570 00007ffb`e8dc805e     ntdll!RtlDispatchException+0x62
12 000000d0`76b9d7c0 00007ffb`55d8cb36     ntdll!KiUserExceptionDispatch+0x2e
13 000000d0`76b9def0 00007ffb`b4f78dd5     ApplicationA!ApplicationA.ApplicationA.CrashButton_Click+0x26
14 000000d0`76b9df10 00007ffb`b4f78f69     System_Windows_Forms!System.Windows.Forms.Button.OnClick+0x195
15 000000d0`76b9dfc0 00007ffb`b4f63d6d     System_Windows_Forms!System.Windows.Forms.Button.OnMouseUp+0xe9
```

```
0:000> u 00007ffb`55d8cb36
ApplicationA!ApplicationA.ApplicationA.CrashButton_Click+0x26:
00007ffb`55d8cb36 mov     dword ptr [rax],1
00007ffb`55d8cb3c add     rsp,10h
00007ffb`55d8cb40 pop     rbp
00007ffb`55d8cb41 ret
00007ffb`55d8cb42 add     byte ptr [rax],al
00007ffb`55d8cb44 sbb     dword ptr [00007ffb`67ddcb4c],eax
00007ffb`55d8cb4a add     dword ptr [rax],edx
00007ffb`55d8cb4d add     byte ptr [rax],al
```

```
0:000> .cxr 000000d0`76b9d7c0
rax=0000000000000000 rbx=0000020ed28179c0 rcx=0000020ed2811050
rdx=0000020ed28179c0 rsi=0000020ed2824168 rdi=0000000000000018
rip=00007ffb55d8cb36 rsp=000000d076b9def0 rbp=000000d076b9df00
 r8=0000020ed2824168  r9=0000000000000006 r10=0000020ece300000
r11=000000d076b9d8c0 r12=0000000000000000 r13=00000000000002af
r14=0000000000000048 r15=00000000000005fd
iopl=0         nv up ei pl zr na po nc
cs=0033  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00010246
ApplicationA!ApplicationA.ApplicationA.CrashButton_Click+0x26:
00007ffb`55d8cb36 mov     dword ptr [rax],1       ds:00000000`00000000=????????
```

14. If we dump the stack trace, we see it starts from the exception frame. To reset it to the original stack trace, just use the .cxr command:

```
0:000> kL 5
 # Child-SP          RetAddr               Call Site
00 000000d0`76b9def0 00007ffb`b4f78dd5     ApplicationA!ApplicationA.ApplicationA.CrashButton_Click+0x26
01 000000d0`76b9df10 00007ffb`b4f78f69     System_Windows_Forms!System.Windows.Forms.Button.OnClick+0x195
02 000000d0`76b9dfc0 00007ffb`b4f63d6d     System_Windows_Forms!System.Windows.Forms.Button.OnMouseUp+0xe9
03 000000d0`76b9e020 00007ffb`55d84d09     System_Windows_Forms!System.Windows.Forms.Control.WmMouseUp+0x2bd
04 000000d0`76b9e0b0 00007ffb`55d8b5d7     System_Windows_Forms!System.Windows.Forms.Control.WndProc+0x8d9
```

```
0:000> .cxr
Resetting default scope
```

```
0:000> kL 5
 # Child-SP          RetAddr               Call Site
00 000000d0`76b9b218 00007ffb`55d9c454     win32u!NtUserWaitMessage+0x14
01 000000d0`76b9b220 00007ffb`b5237d33     System_Windows_Forms_Primitives!Windows.Win32.PInvoke.WaitMessage+0x74
02 000000d0`76b9b2d0 00007ffb`b5237c1a     System_Windows_Forms!System.Windows.Forms.Application.LightThreadContext.FPushMessageLoop+0x43
03 000000d0`76b9b360 00007ffb`b5239597     System_Windows_Forms!System.Windows.Forms.Application.LightThreadContext.RunMessageLoop+0xa
04 000000d0`76b9b390 00007ffb`b52392d2     System_Windows_Forms!System.Windows.Forms.Application.ThreadContext.RunMessageLoopInner+0x287
```

15. Finally, we get the managed stack trace of the current thread:

```
0:000> !CLRStack
OS Thread Id: 0x19fc (0)
        Child SP               IP Call Site
000000D076B9B250 00007ffbe61814d4 [InlinedCallFrame: 000000d076b9b250] Windows.Win32.PInvoke.g__LocalExternFunction|3644_0()
000000D076B9B250 00007ffb55d9c454 [InlinedCallFrame: 000000d076b9b250] Windows.Win32.PInvoke.g__LocalExternFunction|3644_0()
000000D076B9B220 00007ffb55d9c454 Windows.Win32.PInvoke.WaitMessage()
000000D076B9B2D0 00007ffbb5237d33 System.Windows.Forms.Application+LightThreadContext.FPushMessageLoop(Microsoft.Office.msoloop)
000000D076B9B360 00007ffbb5237c1a System.Windows.Forms.Application+LightThreadContext.RunMessageLoop(Microsoft.Office.msoloop, Boolean)
000000D076B9B390 00007ffbb5239597 System.Windows.Forms.Application+ThreadContext.RunMessageLoopInner(Microsoft.Office.msoloop,
System.Windows.Forms.ApplicationContext)
000000D076B9B410 00007ffbb52392d2 System.Windows.Forms.Application+ThreadContext.RunMessageLoop(Microsoft.Office.msoloop,
System.Windows.Forms.ApplicationContext)
000000D076B9B470 00007ffbb517feae System.Windows.Forms.Form.ShowDialog(System.Windows.Forms.IWin32Window)
000000D076B9B520 00007ffbb52390d9 System.Windows.Forms.Application+ThreadContext.OnThreadException(System.Exception)
000000D076B9B590 00007ffb55d83d0e System.Windows.Forms.NativeWindow.Callback(Windows.Win32.Foundation.HWND, Windows.Win32.MessageId,
Windows.Win32.Foundation.WPARAM, Windows.Win32.Foundation.LPARAM)
000000D076B9B760 00007ffbb58cc4ef [InlinedCallFrame: 000000d076b9b760]
000000D076B9B760 00007ffbb09e7a31 [InlinedCallFrame: 000000d076b9b760]
000000D076B9B700 00007ffbb09e7a31 System.Runtime.EH.DispatchEx(System.Runtime.StackFrameIterator ByRef, ExInfo ByRef)
000000D076B9B860 00007ffbb09e717a System.Runtime.EH.RhThrowHwEx(UInt32, ExInfo ByRef)
000000D076B9B9D0 00007ffbb5942eb3 [FaultingExceptionFrame: 000000d076b9b9d0]
000000D076B9DEF0 00007ffb55d8cb36 ApplicationA.ApplicationA.CrashButton_Click(System.Object, System.EventArgs)
000000D076B9DF10 00007ffbb4f78dd5 System.Windows.Forms.Button.OnClick(System.EventArgs)
000000D076B9DFC0 00007ffbb4f78f69 System.Windows.Forms.Button.OnMouseUp(System.Windows.Forms.MouseEventArgs)
000000D076B9E020 00007ffbb4f63d6d System.Windows.Forms.Control.WmMouseUp(System.Windows.Forms.Message ByRef, System.Windows.Forms.MouseButtons, Int32)
000000D076B9E0B0 00007ffb55d84d09 System.Windows.Forms.Control.WndProc(System.Windows.Forms.Message ByRef)
```

```
000000D076B9E140 00007ffb55d8b5d7 System.Windows.Forms.ButtonBase.WndProc(System.Windows.Forms.Message ByRef)
000000D076B9E1A0 00007ffb55d83b69 System.Windows.Forms.NativeWindow.Callback(Windows.Win32.Foundation.HWND, Windows.Win32.MessageId,
Windows.Win32.Foundation.WPARAM, Windows.Win32.Foundation.LPARAM)
000000D076B9E220 00007ffb55d7347c ILStubClass.IL_STUB_ReversePInvoke(Windows.Win32.Foundation.HWND, Windows.Win32.MessageId, Windows.Win32.Foundation.WPARAM,
Windows.Win32.Foundation.LPARAM)
000000D076B9E4C8 00007ffbe7701cac [InlinedCallFrame: 000000d076b9e4c8]
000000D076B9E4C8 00007ffbb2d2290f [InlinedCallFrame: 000000d076b9e4c8]
000000D076B9E490 00007ffbb2d2290f Windows.Win32.PInvoke.DispatchMessage(Windows.Win32.UI.WindowsAndMessaging.MSG*)
000000D076B9E560 00007ffbb5237e7e System.Windows.Forms.Application+LightThreadContext.FPushMessageLoop(Microsoft.Office.msoloop)
000000D076B9E5F0 00007ffbb5237c1a System.Windows.Forms.Application+LightThreadContext.RunMessageLoop(Microsoft.Office.msoloop, Boolean)
000000D076B9E620 00007ffbb5239597 System.Windows.Forms.Application+ThreadContext.RunMessageLoopInner(Microsoft.Office.msoloop,
System.Windows.Forms.ApplicationContext)
000000D076B9E6A0 00007ffbb52392d2 System.Windows.Forms.Application+ThreadContext.RunMessageLoop(Microsoft.Office.msoloop,
System.Windows.Forms.ApplicationContext)
000000D076B9E700 00007ffb55d7189d ApplicationA.Program.Main()
```

16. If we want to see *ApplicationA* source code lines in stack traces, we need to specify the symbol files. It is also possible to see the problem source code if we specify the path to the source code.

```
0:000> .sympath+ C:\ANETMDA-Dumps\Windows\x64\Symbols
Symbol search path is: srv*;C:\ANETMDA-Dumps\Windows\x64\Symbols
Expanded Symbol search path is:
cache*;SRV*https://msdl.microsoft.com/download/symbols;c:\anetmda-dumps\windows\x64\symbols

************* Path validation summary **************
Response                         Time (ms)     Location
Deferred                                       srv*
OK                                             C:\ANETMDA-Dumps\Windows\x64\Symbols
```

```
0:000> k 16
 # Child-SP          RetAddr               Call Site
00 000000d0`76b9b218 00007ffb`55d9c454     win32u!NtUserWaitMessage+0x14
01 000000d0`76b9b220 00007ffb`b5237d33     System_Windows_Forms_Primitives!Windows.Win32.PInvoke.WaitMessage+0x74
[/_/artifacts/obj/System.Windows.Forms.Primitives/Release/net9.0/Microsoft.Windows.CsWin32/Microsoft.Windows.CsWin32.SourceGenerator/Windows.Win32.PInvoke.USER32.dll.g.cs @ 4487]
02 000000d0`76b9b2d0 00007ffb`b5237c1a     System_Windows_Forms!System.Windows.Forms.Application.LightThreadContext.FPushMessageLoop+0x43 [/_/src/System.Windows.Forms/src/System/Windows/Forms/Application.LightThreadContext.cs @ 83]
03 000000d0`76b9b360 00007ffb`b5239597     System_Windows_Forms!System.Windows.Forms.Application.LightThreadContext.RunMessageLoop+0xa [/_/src/System.Windows.Forms/src/System/Windows/Forms/Application.LightThreadContext.cs @ 26]
04 000000d0`76b9b390 00007ffb`b52392d2     System_Windows_Forms!System.Windows.Forms.Application.ThreadContext.RunMessageLoopInner+0x287 [/_/src/System.Windows.Forms/src/System/Windows/Forms/Application.ThreadContext.cs @ 809]
05 000000d0`76b9b410 00007ffb`b517feae     System_Windows_Forms!System.Windows.Forms.Application.ThreadContext.RunMessageLoop+0x42 [/_/src/System.Windows.Forms/src/System/Windows/Forms/Application.ThreadContext.cs @ 696]
06 000000d0`76b9b470 00007ffb`b52390d9     System_Windows_Forms!System.Windows.Forms.Form.ShowDialog+0x27e [/_/src/System.Windows.Forms/src/System/Windows/Forms/Form.cs @ 5892]
07 000000d0`76b9b520 00007ffb`55d83d0e     System_Windows_Forms!System.Windows.Forms.Application.ThreadContext.OnThreadException+0x99 [/_/src/System.Windows.Forms/src/System/Windows/Forms/Application.ThreadContext.cs @ 624]
08 000000d0`76b9b590 00007ffb`b58cc4ef     System_Windows_Forms!System.Windows.Forms.NativeWindow.Callback+0x26e [/_/src/System.Windows.Forms/src/System/Windows/Forms/NativeWindow.cs @ 363]
09 000000d0`76b9b5f0 00007ffb`b09e7a56     coreclr!CallCatchFunclet+0x17f [D:\a\_work\1\s\src\coreclr\vm\exceptionhandling.cpp @ 7751]
0a 000000d0`76b9b700 00007ffb`b09e717a     System_Private_CoreLib!System.Runtime.EH.DispatchEx+0x536 [/_/src/coreclr/nativeaot/Runtime.Base/src/System/Runtime/ExceptionHandling.cs @ 928]
0b 000000d0`76b9b860 00007ffb`b5942eb3     System_Private_CoreLib!System.Runtime.EH.RhThrowHwEx+0xaa [/_/src/coreclr/nativeaot/Runtime.Base/src/System/Runtime/ExceptionHandling.cs @ 620]
0c 000000d0`76b9b8a0 00007ffb`b58c1568     coreclr!CallDescrWorkerInternal+0x83 [D:\a\_work\1\s\src\coreclr\vm\amd64\CallDescrWorkerAMD64.asm @ 74]
0d 000000d0`76b9b8e0 00007ffb`b59f5cde     coreclr!DispatchCallSimple+0x60 [D:\a\_work\1\s\src\coreclr\vm\callhelpers.cpp @ 248]
0e 000000d0`76b9b970 00007ffb`b59cf58a     coreclr!HandleManagedFaultNew+0x192 [D:\a\_work\1\s\src\coreclr\vm\excep.cpp @ 6304]
0f 000000d0`76b9d480 00007ffb`e8d9ca2a     coreclr!CLRVectoredExceptionHandlerShim+0xa84ca [D:\a\_work\1\s\src\coreclr\vm\excep.cpp @ 7276]
10 000000d0`76b9d4d0 00007ffb`e8d559f2     ntdll!RtlpCallVectoredHandlers+0x112
11 000000d0`76b9d570 00007ffb`e8dc805e     ntdll!RtlDispatchException+0x62
12 000000d0`76b9d7c0 00007ffb`55d8cb36     ntdll!KiUserExceptionDispatch+0x2e
13 000000d0`76b9def0 00007ffb`b4f78dd5     ApplicationA!ApplicationA.ApplicationA.CrashButton_Click+0x26 [C:\ANETMDA-Examples\ApplicationA\ApplicationA.cs @ 15]
14 000000d0`76b9df10 00007ffb`b4f78f69     System_Windows_Forms!System.Windows.Forms.Button.OnClick+0x195 [/_/src/System.Windows.Forms/src/System/Windows/Forms/Controls/Buttons/Button.cs @ 209]
15 000000d0`76b9dfc0 00007ffb`b4f63d6d     System_Windows_Forms!System.Windows.Forms.Button.OnMouseUp+0xe9 [/_/src/System.Windows.Forms/src/System/Windows/Forms/Controls/Buttons/Button.cs @ 239]
```

```
0:000> .srcpath+ C:\ANETMDA-Dumps\Windows\Source\ApplicationA
Source search path is: SRV*;C:\ANETMDA-Dumps\Windows\Source\ApplicationA

************* Path validation summary **************
Response                         Time (ms)     Location
Deferred                                       SRV*
OK                                             C:\ANETMDA-Dumps\Windows\Source\ApplicationA
```

```
0:000> .frame 13
13 000000d0`76b9def0 00007ffb`b4f78dd5
ApplicationA!ApplicationA.ApplicationA.CrashButton_Click+0x26 [C:\ANETMDA-
Examples\ApplicationA\ApplicationA.cs @ 15]
```

ApplicationA.cs

```
1  namespace ApplicationA
2  {
3      public partial class ApplicationA :
4      {
5          public ApplicationA()
6          {
7              InitializeComponent();
8          }
9
10         private void CrashButton_Click(
11         {
12             unsafe
13             {
14                 int* p = (int*)0;
15                 *p = 1;
16             }
17         }
18     }
19 }
20
```

17. The help command shows all available SOS extension commands:

```
0:000> !sos.help
analyzeoom, AnalyzeOOM                                  Displays the info of the last OOM that occurred on an
allocation request to the GC heap.
assemblies, clrmodules                                  Lists the managed assemblies in the process.
clrstack <arguments>                                    Provides a stack trace of managed code only.
clrthreads <arguments>                                  Lists the managed threads running.
comstate <arguments>                                    Lists the COM apartment model for each thread.
crashinfo                                               Displays the crash details that created the dump.
d, readmemory <address>                                 Dumps memory contents.
da <address>                                            Dumps memory as zero-terminated byte strings.
db <address>                                            Dumps memory as bytes.
dbgout <arguments>                                      Enables/disables (-off) internal SOS logging.
dc <address>                                            Dumps memory as chars.
dd <address>                                            Dumps memory as dwords (uint).
dp <address>                                            Dumps memory as pointers.
dq <address>                                            Dumps memory as qwords (ulong).
du <address>                                            Dumps memory as zero-terminated char strings.
dumpalc <arguments>                                     Displays details about a collectible AssemblyLoadContext into
which the specified object is loaded.
dumparray <arguments>                                   Displays details about a managed array.
dumpassembly <arguments>                                Displays details about an assembly.
dumpasync, DumpAsync                                    Displays information about async "stacks" on the garbage-
collected heap.
dumpccw <arguments>                                     Displays information about a COM Callable Wrapper.
dumpclass <arguments>                                   Displays information about a EE class structure at the
specified address.
dumpconcurrentdictionary, dcd <address>                 Displays concurrent dictionary content.
dumpconcurrentqueue, dcq <address>                      Displays concurrent queue content.
dumpdelegate <arguments>                                Displays information about a delegate.
dumpdomain <arguments>                                  Displays the Microsoft intermediate language (MSIL) that's
associated with a managed method.
dumpexceptions                                          Displays a list of all managed exceptions.
```

```
dumpgcdata <arguments>                                  Displays information about the GC data.
dumpgen, dg <generation>                                Displays heap content for the specified generation.
dumpheap, DumpHeap <memoryrange>                        Displays a list of all managed objects.
dumphttp, DumpHttp                                      Displays information about HTTP requests.
dumpil <arguments>                                      Displays the Microsoft intermediate language (MSIL) that is
associated with a managed method.
dumplog <arguments>                                     Writes the contents of an in-memory stress log to the
specified file.
dumpmd <arguments>                                      Displays information about a MethodDesc structure at the
specified address.
dumpmodule <arguments>                                  Displays information about a EE module structure at the
specified address.
dumpmt <arguments>                                      Displays information about a method table at the specified
address.
dumpobj, do <arguments>                                 Displays info about an object at the specified address.
dumpobjgcrefs <object>                                  A helper command to implement !dumpobj -refs
dumppermissionset <arguments>                           Displays a PermissionSet object (debug build only).
dumprcw <arguments>                                     Displays information about a Runtime Callable Wrapper.
dumprequests, DumpRequests                              Displays all currently active incoming HTTP requests.
dumpruntimetypes, DumpRuntimeTypes                      Finds all System.RuntimeType objects in the GC heap and
prints the type name and MethodTable they refer too.
dumpsig <arguments>                                     Dumps the signature of a method or field specified by
<sigaddr> <moduleaddr>.
dumpsigelem <arguments>                                 Dumps a single element of a signature object.
dumpstackobjects, dso, DumpStackObjects <stackbounds>   Displays all managed objects found within the bounds of the
current stack.
dumpvc <arguments>                                      Displays info about the fields of a value class.
dw <address>                                            Dumps memory as words (ushort).
eeheap, EEHeap <memoryrange>                            Displays information about native memory that CLR has
allocated.
eeversion <arguments>                                   Displays information about the runtime version.
ehinfo <arguments>                                      Displays the exception handling blocks in a JIT-ed method.
enummem <arguments>                                     ICLRDataEnumMemoryRegions.EnumMemoryRegions test command.
ephrefs                                                 Finds older generation objects which reference objects in the
ephemeral segment.
ephtoloh                                                Finds ephemeral objects which reference the large object
heap.
finalizequeue, fq, FinalizeQueue                        Displays all objects registered for finalization.
findappdomain <arguments>                               Attempts to resolve the AppDomain of a GC object.
findpointersin <regions>                                Finds pointers to the GC heap within the given memory
regions.
gchandleleaks <arguments>                               Helps in tracking down GCHandle leaks.
gchandles <arguments>                                   Provides statistics about GCHandles in the process.
gcheapstat, GCHeapStat                                  Displays various GC heap stats.
gcinfo <arguments>                                      Displays JIT GC encoding for a method.
gcroot, GCRoot <target>                                 Displays info about references (or roots) to an object at the
specified address.
gctonative <memorytypes>                                Finds GC objects which point to the given native memory
ranges.
gcwhere, GCWhere <address>                              Displays the location in the GC heap of the specified
address.
help, soshelp <command>                                 Displays help for a command.
histclear <arguments>                                   Releases any resources used by the family of Hist commands.
histinit <arguments>                                    Initializes the SOS structures from the stress log saved in
the debuggee.
histobj <arguments>                                     Examines all stress log relocation records and displays the
chain of garbage collection relocations that may have led to  the address passed in as an argument.
histobjfind <arguments>                                 Displays all the log entries that reference an object at the
specified address.
histroot <arguments>                                    Displays information related to both promotions and
relocations of the specified root.
histstats <arguments>                                   Displays stress log stats.
ip2md <arguments>                                       Displays the MethodDesc structure at the specified address in
code that has been JIT-compiled.
listnearobj, lno, ListNearObj <address>                 Displays the object preceding and succeeding the specified
address.
loadsymbols <url>                                       Loads symbols for all modules.
logclose <path>                                         Disables console file logging.
logging <path>                                          Enables/disables internal diagnostic logging.
logopen <path>                                          Enables console file logging.
maddress                                                Displays a breakdown of the virtual address space.
modules, lm                                             Displays the native modules in the process.
name2ee <arguments>                                     Displays the MethodTable structure and EEClass structure for
the specified type or method in the specified module.
notreachableinrange <start> <end>                       A helper command for !finalizerqueue
```

```
objsize, ObjSize <objectaddress>                    Lists the sizes of the all the objects found on managed
threads.
parallelstacks, pstacks                             Displays the merged threads stack similarly to the Visual
Studio 'Parallel Stacks' panel.
pathto, PathTo <source> <target>                    Displays the GC path from <root> to <target>.
printexception, pe <arguments>                      Displays and formats fields of any object derived from the
Exception class at the specified address.
registers, r                                        Displays the thread's registers.
runtimes, setruntime <id>                           Lists the runtimes in the target or changes the default
runtime.
setclrpath <path>                                   Sets the path to load coreclr DAC/DBI files.
setsymbolserver, SetSymbolServer <url>              Enables and sets symbol server support for symbols and module
download.
sizestats                                           Size statistics for the GC heap.
sosflush                                            Resets the internal cached state.
sosstatus                                           Displays internal status.
syncblk <arguments>                                 Displays the SyncBlock holder info.
taskstate, tks <address>                            Displays a Task state in a human readable format.
threadpool, ThreadPool                              Displays info about the runtime thread pool.
threadpoolqueue, tpq                                Displays queued ThreadPool work items.
threads, setthread <thread>                         Lists the threads in the target or sets the current thread.
threadstate <arguments>                             Pretty prints the meaning of a threads state.
timerinfo, ti                                       Displays information about running timers.
traverseheap, TraverseHeap <filename>               Writes out heap information to a file in a format understood
by the CLR Profiler.
verifyheap, VerifyHeap <memoryrange>                Searches the managed heap for memory corruption..
verifyobj, VerifyObj <objectaddress>                Checks the given object for signs of corruption.
watsonbuckets <arguments>                           Displays the Watson buckets.
```

18. Another way to see the list of the SOS extension commands is to filter all available extension commands:

```
0:000> .extmatch /e sos *
!sos.AnalyzeOOM
!sos.BPMD
!sos.CLRMACreateInstance
!sos.CLRMAReleaseInstance
!sos.CLRStack
!sos.COMState
!sos.ClrStack
!sos.DumpALC
!sos.DumpArray
!sos.DumpAssembly
!sos.DumpAsync
!sos.DumpCCW
!sos.DumpClass
!sos.DumpDelegate
!sos.DumpDomain
!sos.DumpGCConfigLog
!sos.DumpGCData
!sos.DumpHeap
!sos.DumpHttp
!sos.DumpIL
!sos.DumpLocks
!sos.DumpLog
!sos.DumpMD
!sos.DumpMT
!sos.DumpModule
!sos.DumpObj
!sos.DumpRCW
!sos.DumpRequests
!sos.DumpRuntimeTypes
!sos.DumpSig
!sos.DumpSigElem
!sos.DumpStack
!sos.DumpStackObjects
```

```
!sos.DumpVC
!sos.Dumpccw
!sos.Dumplog
!sos.Dumprcw
!sos.Dumpruntimetypes
!sos.EEHeap
!sos.EEStack
!sos.EEVersion
!sos.EHInfo
!sos.Ehinfo
!sos.ExposeDML
!sos.FinalizeQueue
!sos.FindAppDomain
!sos.FindRoots
!sos.Findappdomain
!sos.GCHandleLeaks
!sos.GCHandleleaks
!sos.GCHandles
!sos.GCHeapStat
!sos.GCInfo
!sos.GCRoot
!sos.GCWhere
!sos.GcHeapStat
!sos.GcWhere
!sos.Gchandleleaks
!sos.GetCodeTypeFlags
!sos.HeapStat
!sos.Help
!sos.HistClear
!sos.HistInit
!sos.HistObj
!sos.HistObjFind
!sos.HistRoot
!sos.HistStats
!sos.IP2MD
!sos.InitializeHostServices
!sos.ListNearObj
!sos.MinidumpMode
!sos.Minidumpmode
!sos.Name2EE
!sos.ObjSize
!sos.PathTo
!sos.PrintException
!sos.Printexception
!sos.ProcInfo
!sos.RCWCleanupList
!sos.Rcwcleanuplist
!sos.SOSFlush
!sos.SOSHandleCLRN
!sos.SOSInitializeByHost
!sos.SOSStatus
!sos.SOSUninitializeByHost
!sos.SaveAllModules
!sos.SaveModule
!sos.SaveState
!sos.SetClrPath
!sos.SetHostRuntime
!sos.SetSymbolServer
!sos.StopOnCatch
!sos.StopOnException
```

```
!sos.Stoponexception
!sos.SuppressJitOptimization
!sos.SyncBlk
!sos.ThreadPool
!sos.ThreadState
!sos.Threads
!sos.Token2EE
!sos.TraceToCode
!sos.TraverseHeap
!sos.Traverseheap
!sos.U
!sos.VMMap
!sos.VMStat
!sos.VerifyGMT
!sos.VerifyHeap
!sos.VerifyObj
!sos.VerifyStackTrace
!sos.Verifyheap
!sos.Watch
!sos.WatsonBuckets
!sos.analyzeoom
!sos.ao
!sos.assemblies
!sos.bpmd
!sos.clrmaconfig
!sos.clrmodules
!sos.clrstack
!sos.clrthreads
!sos.clru
!sos.comstate
!sos.crashinfo
!sos.da
!sos.dbgout
!sos.dclog
!sos.dg
!sos.dgc
!sos.do
!sos.dso
!sos.dumpalc
!sos.dumparray
!sos.dumpassembly
!sos.dumpasync
!sos.dumpccw
!sos.dumpclass
!sos.dumpdelegate
!sos.dumpdomain
!sos.dumpexceptions
!sos.dumpgcconfiglog
!sos.dumpgcdata
!sos.dumpgen
!sos.dumpheap
!sos.dumphttp
!sos.dumpil
!sos.dumplocks
!sos.dumplog
!sos.dumpmd
!sos.dumpmodule
!sos.dumpmt
!sos.dumpobj
!sos.dumprcw
```

```
!sos.dumprequests
!sos.dumpruntimetypes
!sos.dumpsig
!sos.dumpsigelem
!sos.dumpstack
!sos.dumpstackobjects
!sos.dumpvc
!sos.eeheap
!sos.eestack
!sos.eeversion
!sos.ehinfo
!sos.enummem
!sos.exposeDML
!sos.ext
!sos.finalizequeue
!sos.findappdomain
!sos.findroots
!sos.fq
!sos.gchandleleaks
!sos.gchandles
!sos.gcheapstat
!sos.gcinfo
!sos.gcroot
!sos.gcwhere
!sos.getCodeTypeFlags
!sos.heapstat
!sos.help
!sos.histclear
!sos.histinit
!sos.histobj
!sos.histobjfind
!sos.histroot
!sos.histstats
!sos.hof
!sos.ip2md
!sos.listnearobj
!sos.lno
!sos.logging
!sos.maddress
!sos.minidumpmode
!sos.name2ee
!sos.objsize
!sos.pathto
!sos.pe
!sos.printexception
!sos.processor
!sos.procinfo
!sos.rcwcleanuplist
!sos.runtimes
!sos.saveallmodules
!sos.savemodule
!sos.savestate
!sos.setclrpath
!sos.sethostruntime
!sos.setsymbolserver
!sos.sizestats
!sos.sjo
!sos.soe
!sos.sos
!sos.sosflush
```

```
!sos.soshelp
!sos.sosstatus
!sos.stoponcatch
!sos.stoponexception
!sos.suppressjitoptimization
!sos.syncblk
!sos.t
!sos.threadpool
!sos.threads
!sos.threadstate
!sos.token2ee
!sos.tp
!sos.tracetocode
!sos.traverseheap
!sos.u
!sos.verifyheap
!sos.verifyobj
!sos.vh
!sos.vmmap
!sos.vmstat
!sos.vo
!sos.watch
```

Note: Command help https://learn.microsoft.com/en-us/dotnet/core/diagnostics/sos-debugging-extension

19. We close logging before exiting WinDbg:

```
0:000> .logclose
Closing open log file C:\ANETMDA-Dumps\Windows\x64\ApplicationA.log
```

Note: To avoid possible confusion and glitches, we recommend exiting WinDbg after each exercise.