.NET Memory Dump Analysis Accelerated

Version 2.0

Dmitry Vostokov
Software Diagnostics Services

Published by OpenTask, Republic of Ireland

Copyright © 2013 by OpenTask

Copyright © 2013 by Software Diagnostics Services

Copyright © 2013 by Dmitry Vostokov

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, without the prior written permission of the publisher.

You must not circulate this book in any other binding or cover, and you must impose the same condition on any acquirer.

Product and company names mentioned in this book may be trademarks of their owners.

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: 978-1-908043-59-7 (Paperback)

Second edition, 1st revision, 2013

Revision 2.01 (March 2017)

Contents

Presentation Slides and Transcript 5

Practice Exercises 21

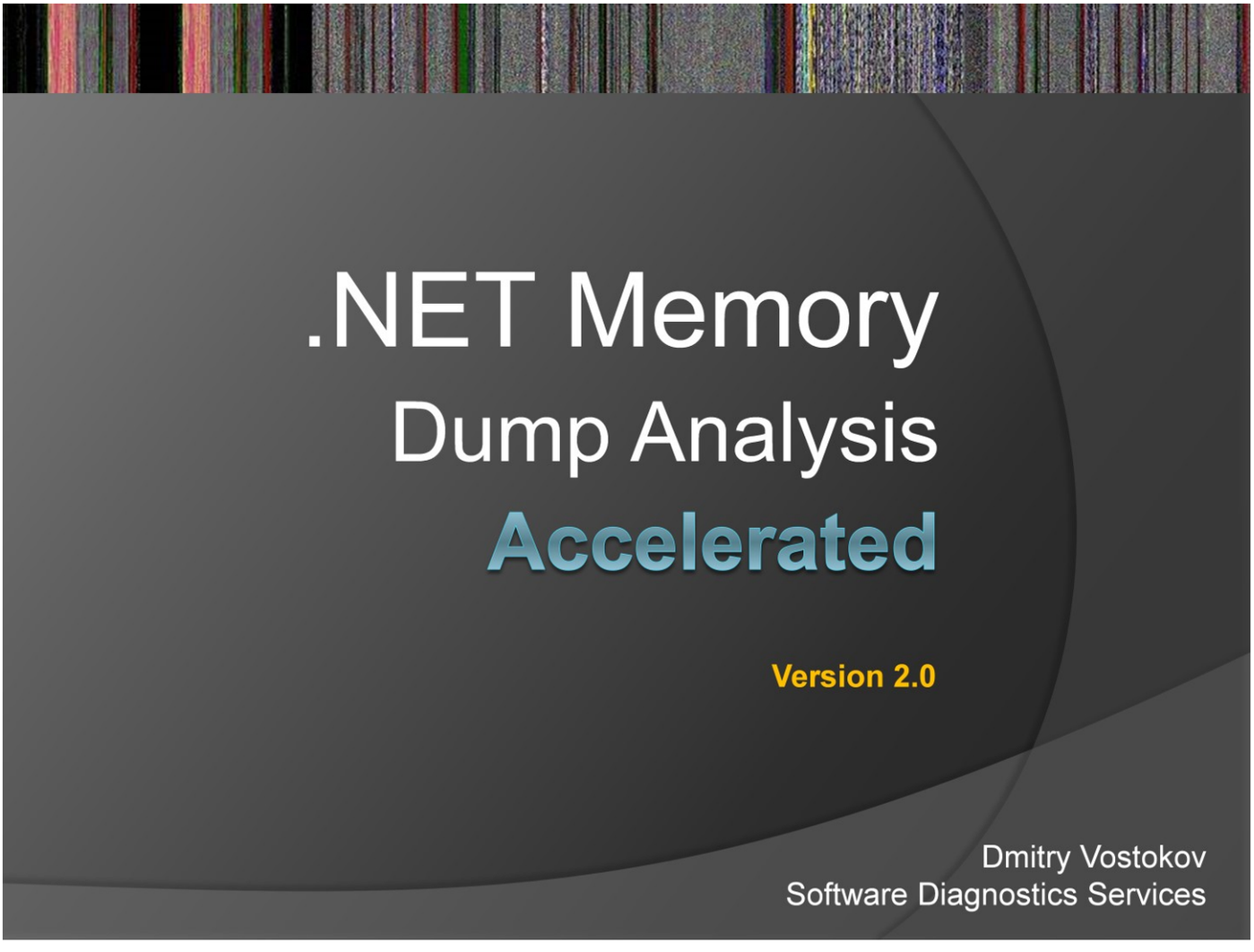
- Exercise 0: Download, setup and verify your WinDbg installation 26
- Exercise PN1: Analysis of an application process dump (ApplicationA, 32-bit, CLR 2) 34
- Exercise PN2: Analysis of an application process dump (ApplicationA, 32-bit, CLR 4) 45
- Exercise PN3: Analysis of an application process dump (LINQPadB, 32-bit, CLR 2) 62
- Exercise PN4: Analysis of an application process dump (LINQPadC, 32-bit, CLR 4) 82
- Exercise PN5: Analysis of an application process dump (LINQPadD, 32-bit, CLR 4) 107
- Exercise PN6: Analysis of an application process dump (LINQPadE, 32-bit, CLR 4) 150
- Exercise PN7: Analysis of an application process dump (LINQPadB, 64-bit, CLR 4) 163
- Exercise PN8: Analysis of an application process dump (LINQPadC, 64-bit, CLR 4) 187
- Optional exercise: Complete memory dump analysis 206

Application Source Code 235

- ApplicationA 237
- LinqB 238
- LinqC 239
- LinqD 241
- LinqE 243

Selected Q&A 247

Presentation Slides and Transcript



Hello Everyone, my name is Dmitry Vostokov, and I teach this training course.

Prerequisites

WinDbg Commands

We use these boxes to introduce some WinDbg commands used in practice exercises

Basic .NET programming and debugging

© 2013 Software Diagnostics Services

Definitely, you need to have software development and debugging experience in .NET. I suppose you know C# although this is not strictly necessary. The ability to read unmanaged assembly language has some advantages but is not necessary for this training. I also assume that you already know what is .NET, its basic architecture and vocabulary such as assemblies, CLR, managed code, classes, and objects. The familiarity with stack traces is essential too.

Training Goals

- Review fundamentals
- Learn how to analyze process dumps
- Learn necessary commands in context
- Cover CLR 2 / CLR 4 (x86 and x64)

© 2013 Software Diagnostics Services

Our primary goal is to learn .NET memory dump analysis in an accelerated fashion. So, first, we review absolutely essential fundamentals necessary for memory dump analysis. Then we go through 8 process memory dumps with the goal to learn most useful WinDbg and its debugging extension commands in the context of real-life like examples where multiple threads are modeling different patterns of abnormal software behavior. We also cover both Common Language Runtime 2.0 (3.5) and 4.0. If time permits we also do a complete memory dump analysis corresponding to one process memory dump analysis exercise. I'd like to note that this training is about memory dump analysis and not about memory dump collection methods.

Training Principles

- Talk only about what I can show
- Lots of pictures
- Lots of examples
- Original content and examples

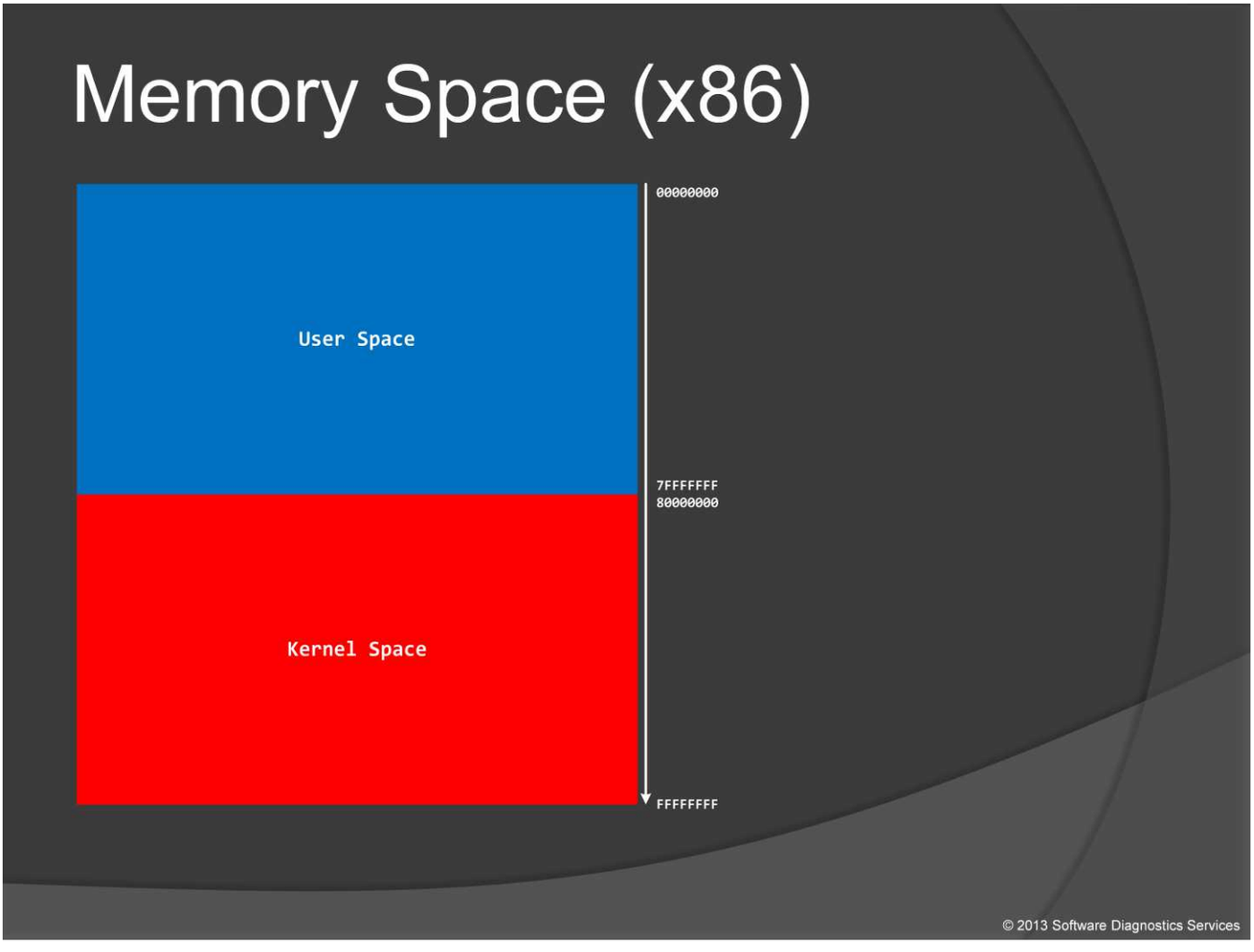
© 2013 Software Diagnostics Services

For me, there were many training formats to consider, and I decided that the best way is to concentrate on exercises. Specifically for this training, I developed 8 of them. I also left many concepts traditionally included in such training courses because I felt that they were not really necessary for accelerated training.

Part 1: Fundamentals

© 2013 Software Diagnostics Services

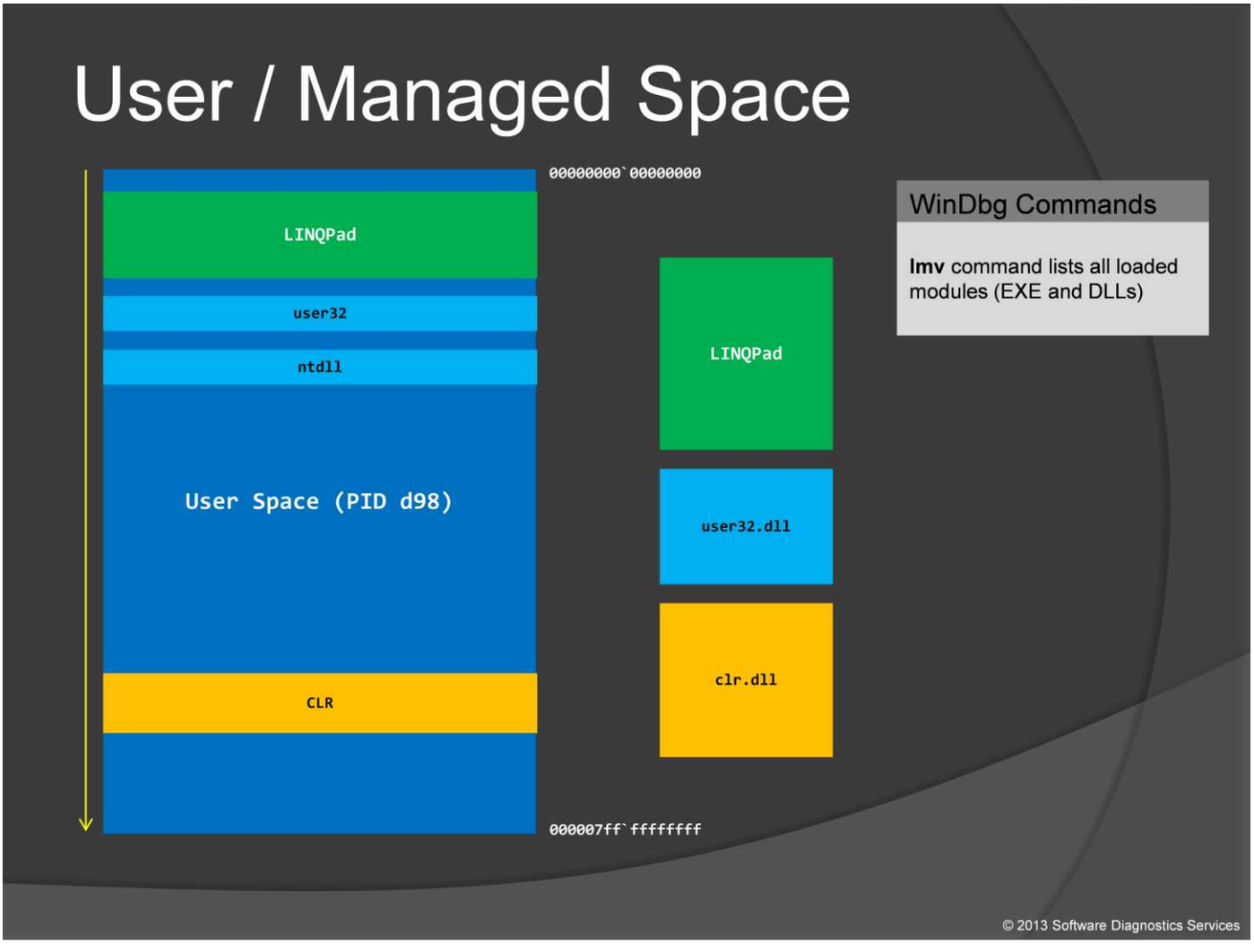
So now I present you some pictures. We use both 32-bit and 64-bit examples. Most of the time fundamentals do not change when we move to x64 Windows platform, and the analysis process (including WinDbg commands) is the same.



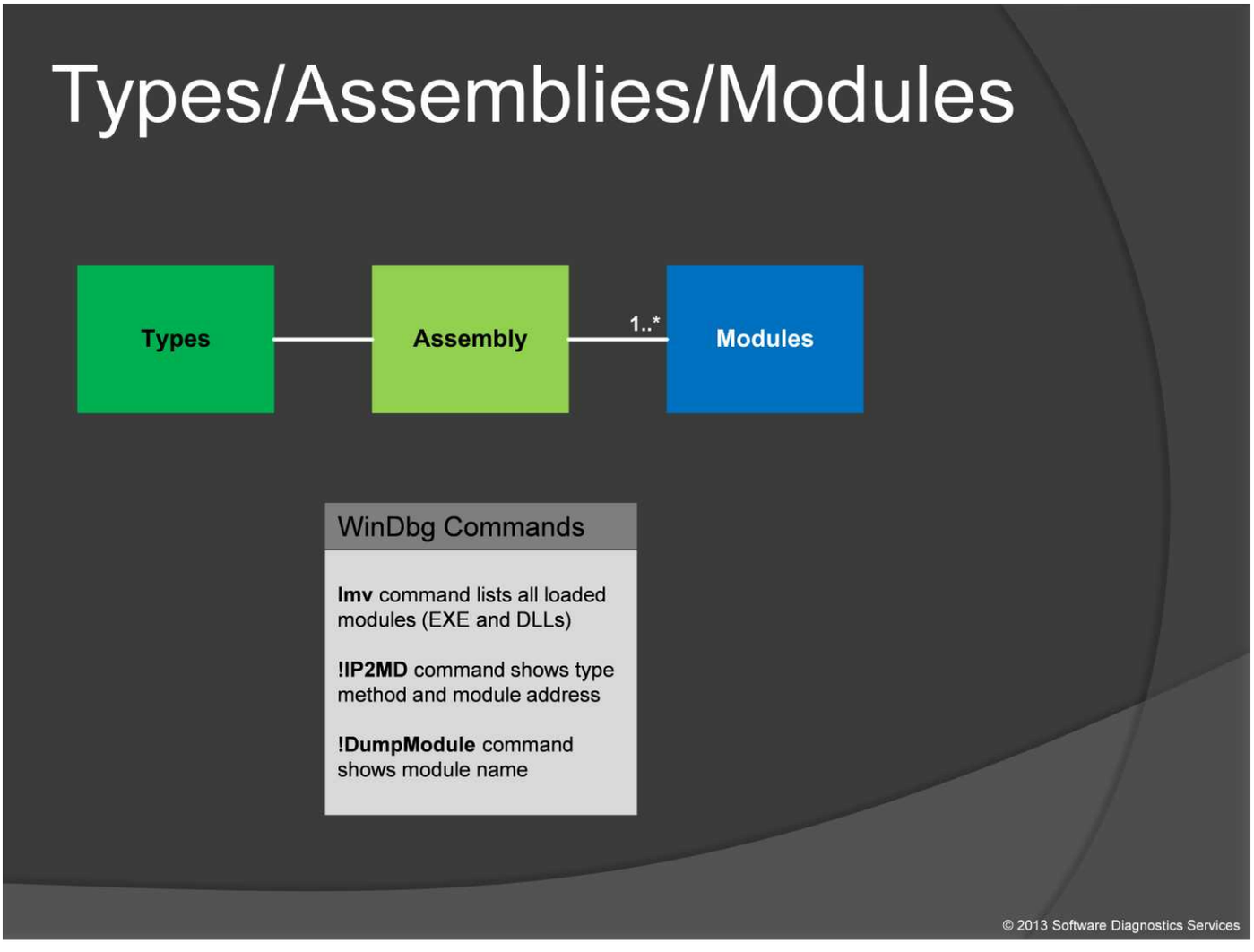
Every Windows process memory range is divided into kernel space part and user space part. I follow the long tradition to use red color for kernel and blue color for user part. This uniform memory space is called process virtual space because it is an abstraction that allows us to analyze memory dumps without thinking about how it is all organized in physical memory. In this training, we are concerned with the user space only except one exercise where we also look at kernel space.

Memory Space (x64)

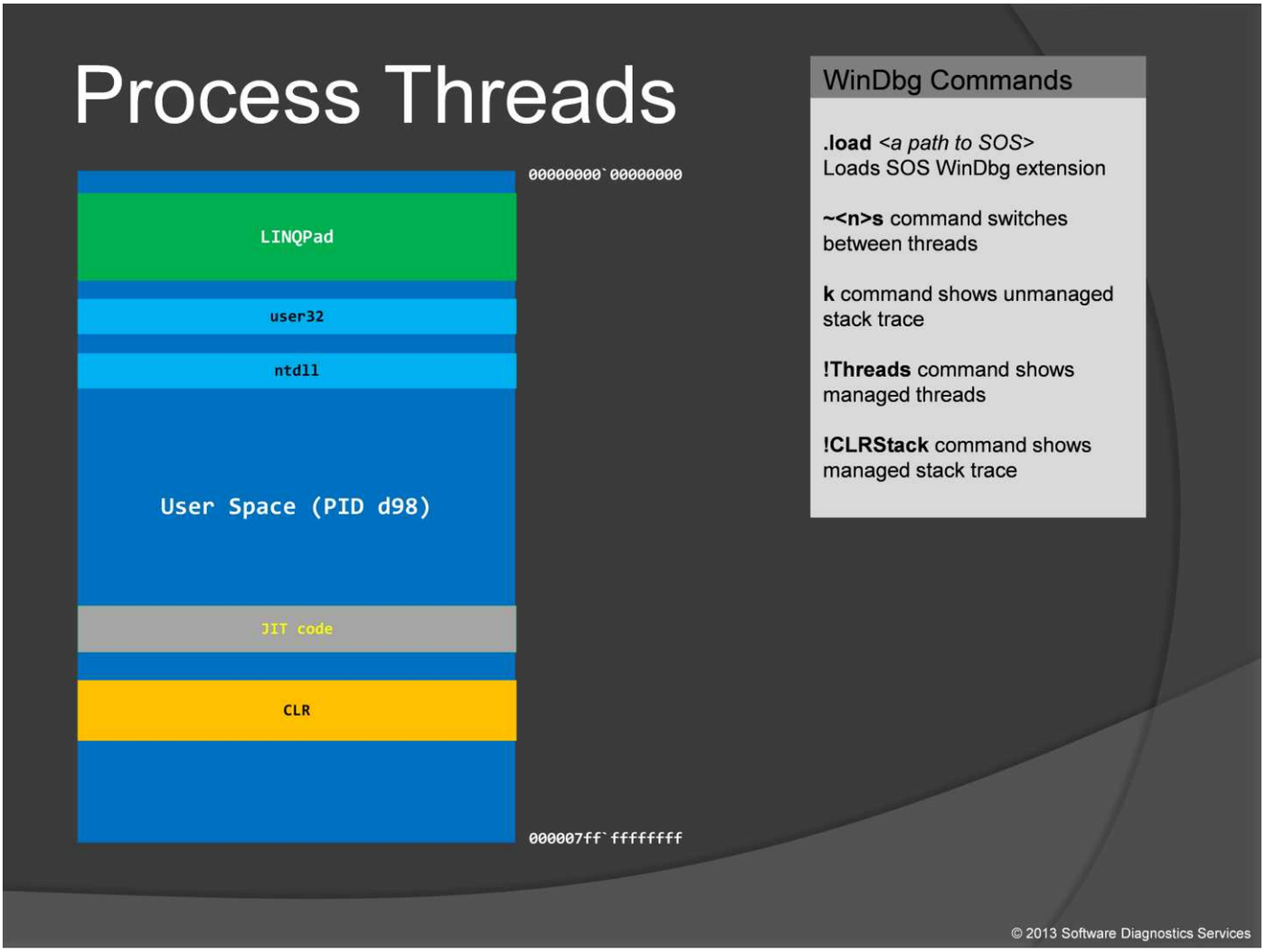
© 2013 Software Diagnostics Services



When an application is loaded all modules (an executable image on a disk and associated DLLs) are organized sequentially in memory space. Some modules can also be loaded twice at different memory locations. A process then is setup for running, and a process ID is assigned to it. If you run another such process it will have the different memory space (could be exactly the same in layout but most recent Windows versions put modules in a different order). Note that CLR is just another module in a process address space and so are all supporting modules from .NET Framework.



Just to remind you that all assembly types (classes) can be spread through several modules like DLLs. 3 commands listed in a box allow you to see which module corresponds to a code address from a stack trace. I show you an example in a few minutes.



Now we come to another important fundamental concept in Windows memory dump analysis: a thread. It is basically a unit of execution, and there can be many threads in a given process. When a thread executes managed code, it is compiled into memory: the so-called JIT code. We need to load a WinDbg SOS extension to analyze it. It is named sos.dll and is located in the same .NET Framework folder as clr.dll or mscorwks.dll. We see this in our example.

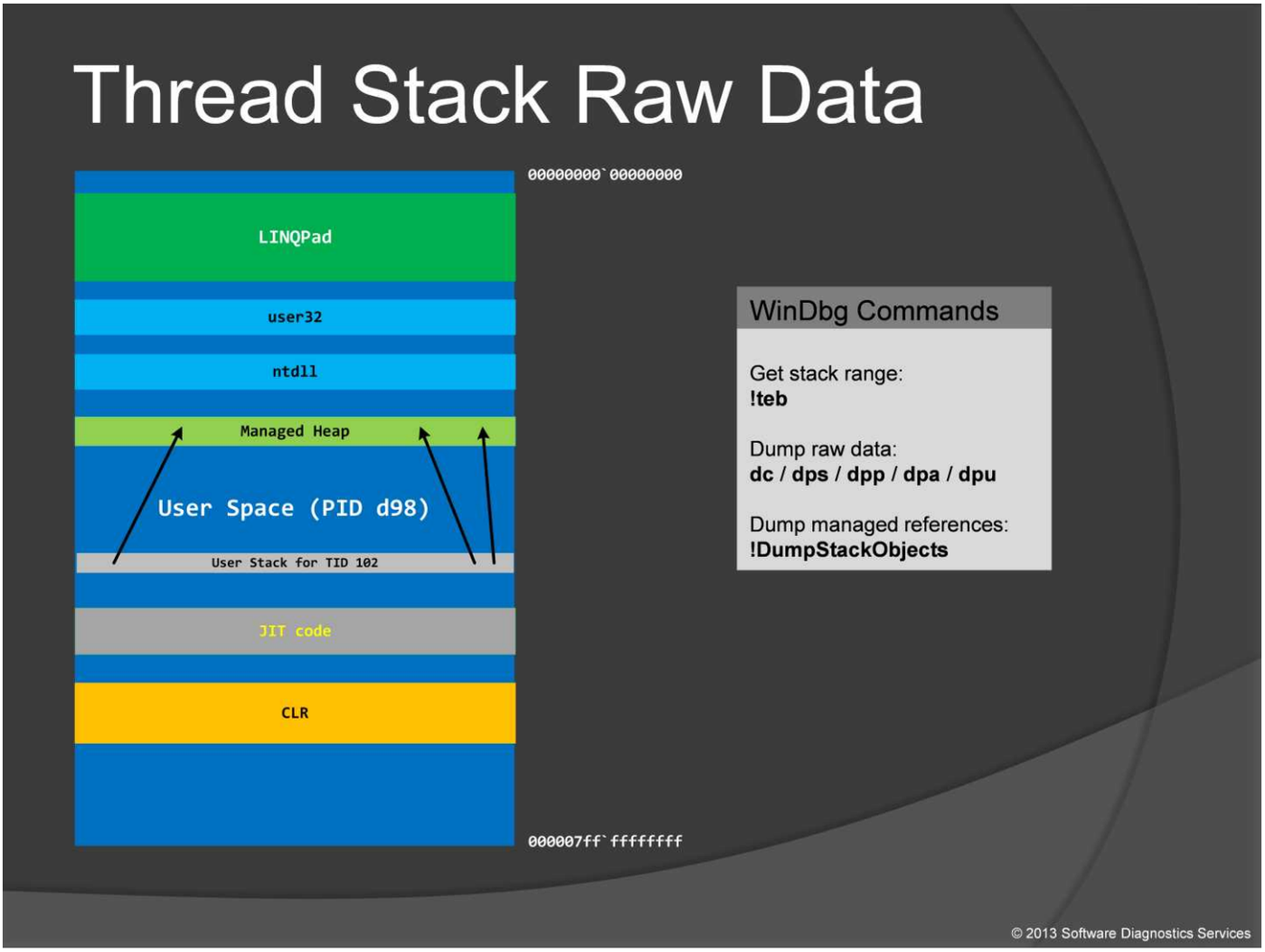
Example

```
0:000> kL
ChildEBP RetAddr
0020e95c 7720b5b4 ntdll!KiFastSystemCallRet
0020e960 68e6737a user32!NtUserWaitMessage+0xc
0020e9f4 68e66e2c System_Windows_Forms_ni+0x22737a
0020ea50 68e66c81 System_Windows_Forms_ni+0x226e2c
0020ea80 68df366d System_Windows_Forms_ni+0x226c81
0020ea98 002b31fd System_Windows_Forms_ni+0x1b366d
0020eb7c 002b1515 0x2b31fd
0020ee24 6ce421db 0x2b1515
0020ee34 6ce64a2a clr!CallDescrWorker+0x33
0020eeb0 6ce64bcc clr!CallDescrWorkerWithHandler+0x8e
0020efe8 6ce64c01 clr!MethodDesc::CallDescr+0x194
0020f004 6ce64c21 clr!MethodDesc::CallTargetWorker+0x21
0020f01c 6cf2ce82 clr!MethodDescCallSite::Call+0x1c
0020f180 6cf2cf90 clr!ClassLoader::RunMain+0x24c
0020f3e8 6cf2cda4 clr!Assembly::ExecuteMainMethod+0xc1
0020f8cc 6cf2d199 clr!SystemDomain::ExecuteMain...
0020f920 6cf2d09a clr!ExecuteEXE+0x58
0020f96c 6cfaaf00 clr!_CorExeMainInternal+0x19f
0020f9a4 6e1e55ab clr!_CorExeMain+0x4e
0020f9b0 6e187f16 mscoreei!_CorExeMain+0x38
0020f9c0 6e184de3 mscoree!ShellShim__CorExeMain+0x99
0020f9c8 77563833 mscoree!_CorExeMain_Exported+0x8
0020f9d4 77b7a9bd kernel32!BaseThreadInitThunk+0xe
0020fa14 00000000 ntdll!_RtlUserThreadStart+0x23
```

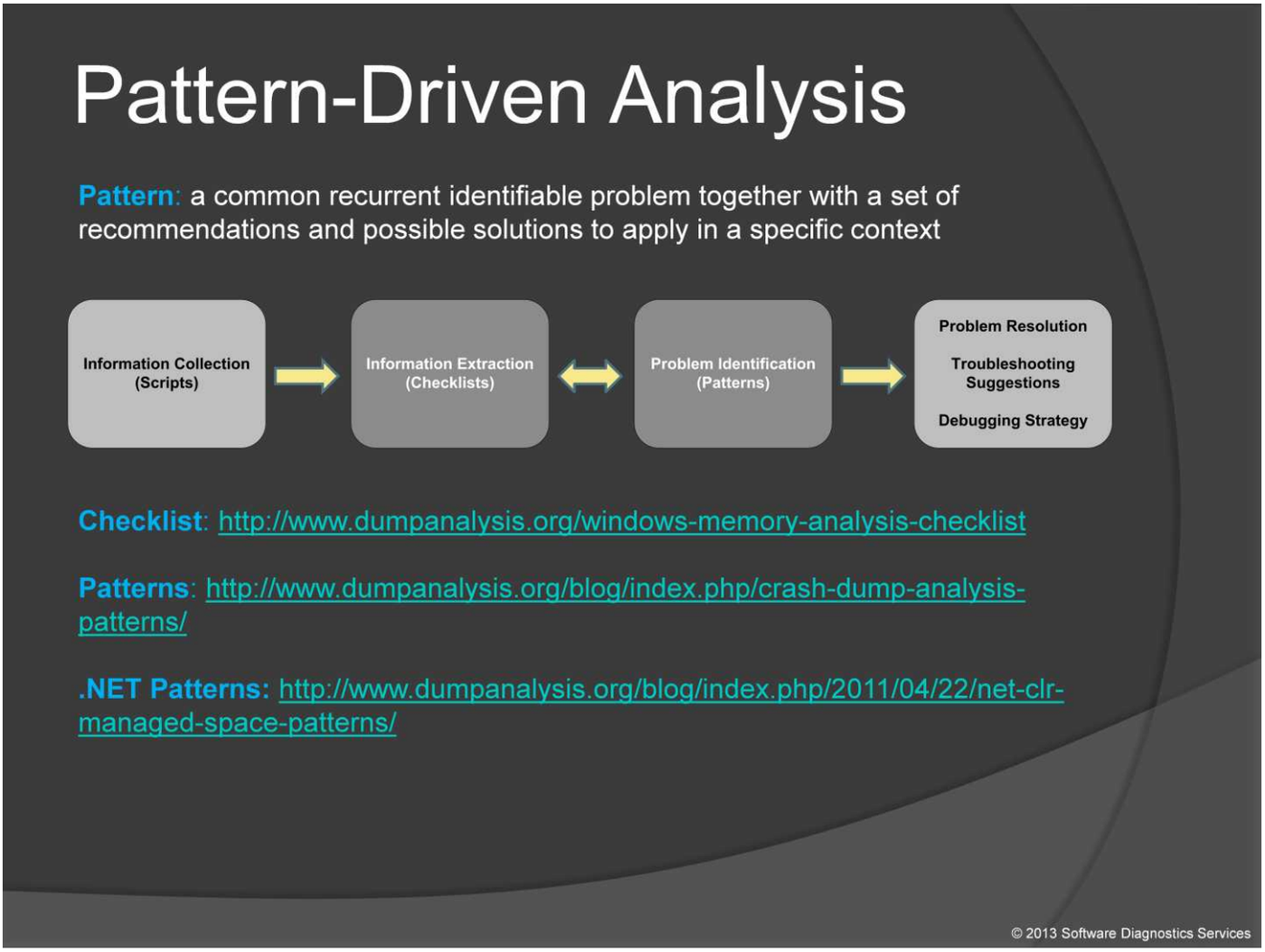
```
0:000> !IP2MD 0x2b1515
MethodDesc:   000e934c
Method Name:  LINQPad.Program.Go(...)
Class:        002c05dc
MethodTable:  000e954c
mdToken:      06000272
Module:       000e2e9c
IsJitted:     yes
CodeAddr:     002b05c0
Transparency: Critical

0:000> !DumpModule 000e2e9c
Name:       C:\LINQPad4\LINQPad.exe
Attributes: PEFile
Assembly:   00317418
[...]
```

© 2013 Software Diagnostics Services

I suppose that you know that all .NET managed code is translated to machine code (the so-called JIT). Then CLR calls it. You see this continuity when you look at a stack trace. This JIT code is shown in yellow. There is also precompiled managed code you see in blue. These are usually .NET Framework modules. So to reiterate: IL and managed space is an abstraction that is translated to unmanaged process space. The debugger output shows you how to manually get module name, class and method of a JIT-compiled address from an unmanaged stack trace.



Every thread also needs a temporary memory region to store its execution history and temporary data. This region is called thread stack. Please note that stack region is just any other memory region and you can use any WinDbg data dumping commands there. We will also learn how to get the thread stack region address range. Examining raw stack data can give some hints to the past system behavior: the so-called Execution Residue pattern. Because managed code (an abstraction) is JIT-translated to unmanaged machine code, raw stack data also contains object references, and you can dump them using **!DumpStackObjects** (**!dso**) command.



Checklist: http://www.dumpanalysis.org/windows-memory-analysis-checklist
Patterns: http://www.dumpanalysis.org/blog/index.php/crash-dump-analysis-patterns/ (also available in Memory Dump Analysis Anthology volumes or Encyclopedia of Crash Dump Analysis Patterns)
.NET Patterns: http://www.dumpanalysis.org/blog/index.php/2011/04/22/net-clr-managed-space-patterns/ (also available in Memory Dump Analysis Anthology volumes or Encyclopedia of Crash Dump Analysis Patterns)

A few words about logs, checklists, and patterns. Memory dump analysis is usually an analysis of a text for the presence of patterns. We run commands, they output text, and then we look at that textual output and when we find something suspicious we execute more commands. Here checklists can be very useful. One such checklist is provided as a link. I recently expanded it to include .NET process memory dumps. In some cases (such as complete memory dumps) it is beneficial to collect information into one log file by running several commands at once (like a script) and then do the first-order analysis.

Practice Exercises

Part 2: Practice Exercises

© 2011 Memory Dump Analysis Services

Now we come to practice. The goal is to show you important commands and how their output helps in recognizing patterns of abnormal software behavior.

Links

- Memory Dumps:

Links are below on this page

- Exercise Transcripts:

Included in this book

© 2013 Software Diagnostics Services

http://www.patterndiagnostics.com/Training/ANETMDA/ANETMDA-Dumps-Part1.zip
http://www.patterndiagnostics.com/Training/ANETMDA/ANETMDA-Dumps-Part2.zip

Exercise 0

- **Goal:** Install Debugging Tools for Windows and learn how to set up symbols correctly
- **Patterns:** Incorrect Stack Trace
- **Commands:** .symfix, .reload, k
- \ANETMDA-Dumps\Exercise-0-Download-Setup-WinDbg.pdf

© 2013 Software Diagnostics Services

Exercise 0: Download, setup and verify your WinDbg installation

Goal: Install Debugging Tools for Windows and learn how to set up symbols correctly.

Patterns: Incorrect Stack Trace

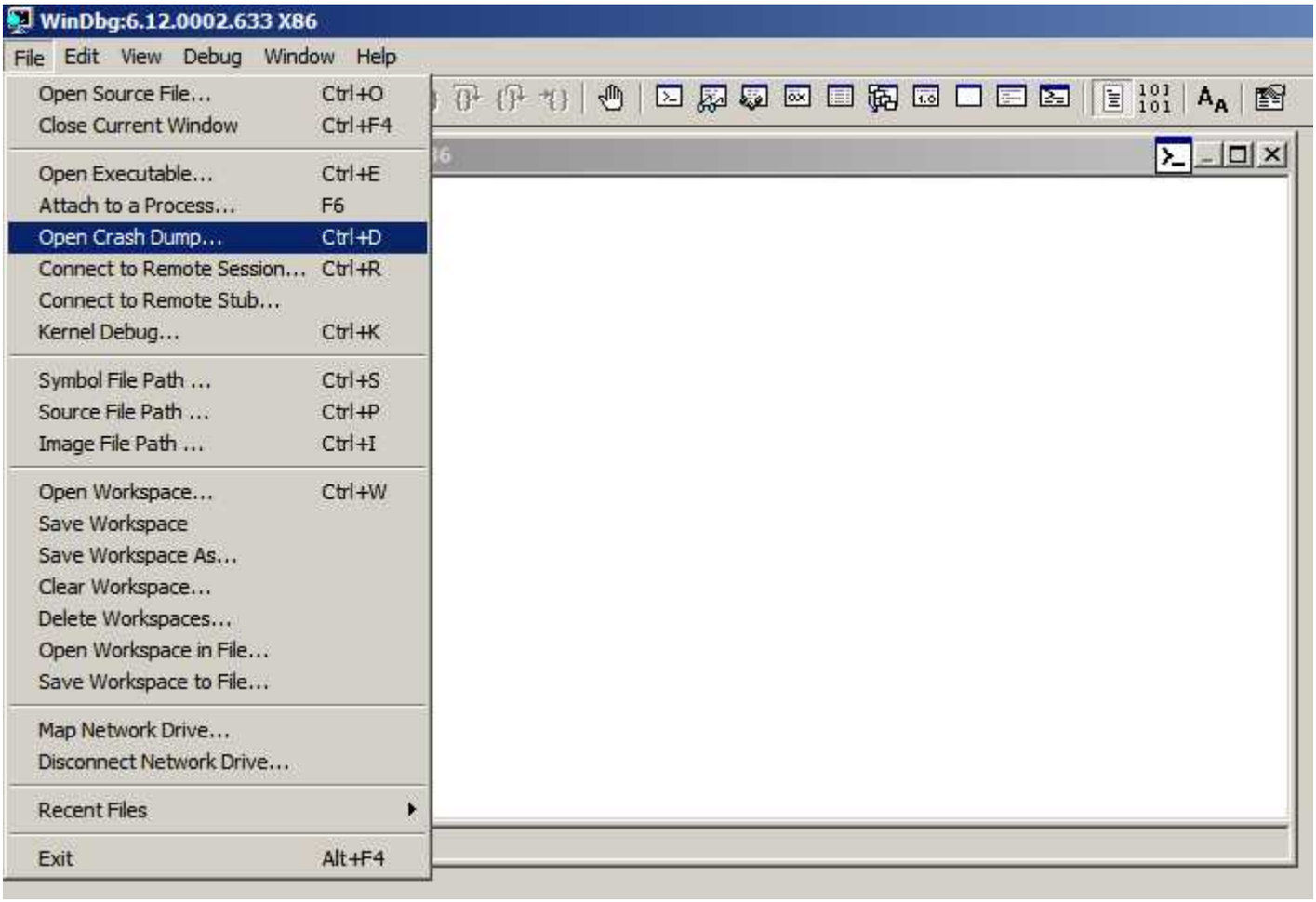
Commands: .symfix, .reload, k

1. Download and install the latest version of 32-bit Debugging Tools for Windows: \ANETMDA-Dumps\dbg_x86.msi (windbg.org for quick links)

2. Choose Complete option during installation

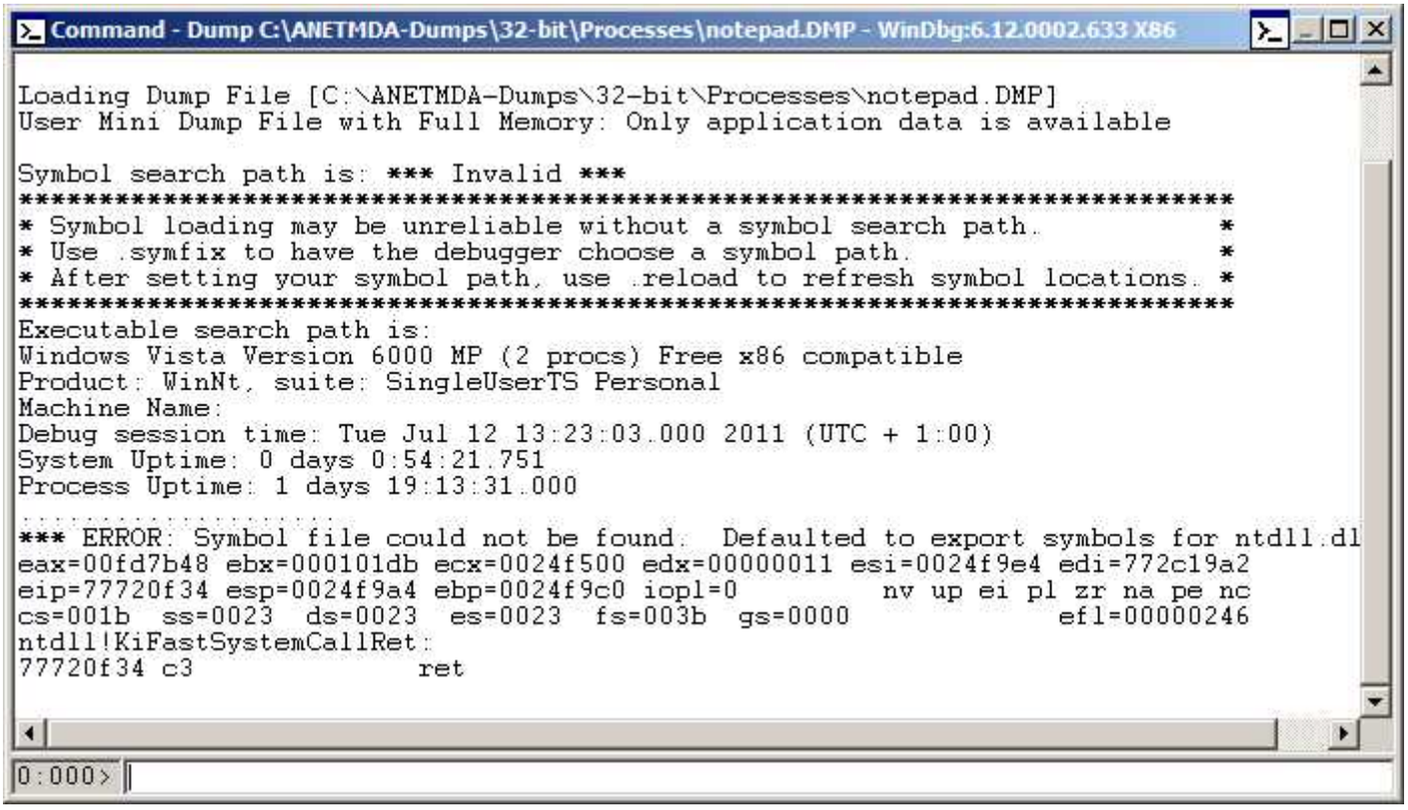
3. Launch WinDbg from Debugging Tools for Windows or Debugging Tools for Windows (x86)

4. Open \ANETMDA-Dumps\32-bit\Processes\notepad.DMP



5. If you are presented with this dialog say No:

6. You get the dump file loaded:



7. Type the command **.symfix c:\mss** to set a path to download symbol files from Microsoft symbol file server (use ENTER to execute commands after typing):

```
Command - Dump C:\ANETMDA-Dumps\32-bit\Processes\notepad.DMP - WinDbg:6.12.0002.633 X86

Loading Dump File [C:\ANETMDA-Dumps\32-bit\Processes\notepad.DMP]
User Mini Dump File with Full Memory: Only application data is available

Symbol search path is: *** Invalid ***
************************************************************************
* Symbol loading may be unreliable without a symbol search path.       *
* Use .symfix to have the debugger choose a symbol path.               *
* After setting your symbol path, use .reload to refresh symbol locations. *
************************************************************************
Executable search path is:
Windows Vista Version 6000 MP (2 procs) Free x86 compatible
Product: WinNt, suite: SingleUserTS Personal
Machine Name:
Debug session time: Tue Jul 12 13:23:03.000 2011 (UTC + 1:00)
System Uptime: 0 days 0:54:21.751
Process Uptime: 1 days 19:13:31.000
.....................
*** ERROR: Symbol file could not be found.  Defaulted to export symbols for ntdll.dl
eax=00fd7b48 ebx=000101db ecx=0024f500 edx=00000011 esi=0024f9e4 edi=772c19a2
eip=77720f34 esp=0024f9a4 ebp=0024f9c0 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
ntdll!KiFastSystemCallRet:
77720f34 c3              ret

0:000> .symfix c:\mss
```

8. Type **.reload** command to download them if necessary:

```
Command - Dump C:\ANETMDA-Dumps\32-bit\Processes\notepad.DMP - WinDbg:6.12.0002.633 X86
Loading Dump File [C:\ANETMDA-Dumps\32-bit\Processes\notepad.DMP]
User Mini Dump File with Full Memory: Only application data is available

Symbol search path is: *** Invalid ***
************************************************************************
* Symbol loading may be unreliable without a symbol search path.       *
* Use .symfix to have the debugger choose a symbol path.               *
* After setting your symbol path, use .reload to refresh symbol locations. *
************************************************************************
Executable search path is:
Windows Vista Version 6000 MP (2 procs) Free x86 compatible
Product: WinNt, suite: SingleUserTS Personal
Machine Name:
Debug session time: Tue Jul 12 13:23:03.000 2011 (UTC + 1:00)
System Uptime: 0 days 0:54:21.751
Process Uptime: 1 days 19:13:31.000
.....................
*** ERROR: Symbol file could not be found.  Defaulted to export symbols for ntdll.dl
eax=00fd7b48 ebx=000101db ecx=0024f500 edx=00000011 esi=0024f9e4 edi=772c19a2
eip=77720f34 esp=0024f9a4 ebp=0024f9c0 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
ntdll!KiFastSystemCallRet:
77720f34 c3              ret
0:000> .symfix c:\mss

0:000> .reload
```

9. Type **k** command to verify the correctness of the stack trace:

```
Command - Dump C:\ANETMDA-Dumps\32-bit\Processes\notepad.DMP - WinDbg:6.12.0002.633 X86

Symbol search path is: *** Invalid ***
************************************************************************
* Symbol loading may be unreliable without a symbol search path.       *
* Use .symfix to have the debugger choose a symbol path.               *
* After setting your symbol path, use .reload to refresh symbol locations. *
************************************************************************
Executable search path is:
Windows Vista Version 6000 MP (2 procs) Free x86 compatible
Product: WinNt, suite: SingleUserTS Personal
Machine Name:
Debug session time: Tue Jul 12 13:23:03.000 2011 (UTC + 1:00)
System Uptime: 0 days 0:54:21.751
Process Uptime: 1 days 19:13:31.000
.....................
*** ERROR: Symbol file could not be found.  Defaulted to export symbols for ntdll.dl
eax=00fd7b48 ebx=000101db ecx=0024f500 edx=00000011 esi=0024f9e4 edi=772c19a2
eip=77720f34 esp=0024f9a4 ebp=0024f9c0 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
ntdll!KiFastSystemCallRet:
77720f34 c3              ret
0:000> .symfix c:\mss
0:000> .reload
.....................

0:000> k
```

```
Command - Dump C:\ANETMDA-Dumps\32-bit\Processes\notepad.DMP - WinDbg:6.12.0002.633 X86
Product: WinNt, suite: SingleUserTS Personal
Machine Name:
Debug session time: Tue Jul 12 13:23:03.000 2011 (UTC + 1:00)
System Uptime: 0 days 0:54:21.751
Process Uptime: 1 days 19:13:31.000
.....................
*** ERROR: Symbol file could not be found.  Defaulted to export symbols for ntdll.dl
eax=00fd7b48 ebx=000101db ecx=0024f500 edx=00000011 esi=0024f9e4 edi=772c19a2
eip=77720f34 esp=0024f9a4 ebp=0024f9c0 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
ntdll!KiFastSystemCallRet:
77720f34 c3              ret
0:000> .symfix c:\mss
0:000> .reload
.....................
0:000> k
ChildEBP RetAddr
0024f9a0 772c199a ntdll!KiFastSystemCallRet
0024f9a4 772c19cd user32!NtUserGetMessage+0xc
0024f9c0 00b9149c user32!GetMessageW+0x33
0024fa00 00b91971 notepad!WinMain+0xec
0024fa90 76193833 notepad!_initterm_e+0x1a1
0024fa9c 776fa9bd kernel32!BaseThreadInitThunk+0xe
0024fadc 00000000 ntdll!_RtlUserThreadStart+0x23

0:000>
```

10. The output of the command shoud be this:

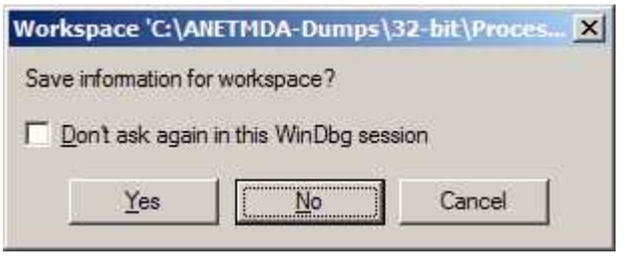
```
0:000> k
ChildEBP RetAddr
0024f9a0 772c199a ntdll!KiFastSystemCallRet
0024f9a4 772c19cd user32!NtUserGetMessage+0xc
0024f9c0 00b9149c user32!GetMessageW+0x33
0024fa00 00b91971 notepad!WinMain+0xec
0024fa90 76193833 notepad!_initterm_e+0x1a1
0024fa9c 776fa9bd kernel32!BaseThreadInitThunk+0xe
0024fadc 00000000 ntdll!_RtlUserThreadStart+0x23
```

If it has this form below then your symbol files were not set up correctly (*coloring is mine*) - **Incorrect Stack Trace** pattern:

```
0:000> k
ChildEBP RetAddr
WARNING: Stack unwind information not available. Following frames may be wrong.
0024f9c0 00b9149c ntdll!KiFastSystemCallRet
0024fa00 00b91971 notepad+0x149c
0024fa90 76193833 notepad+0x1971
0024fa9c 776fa9bd kernel32!BaseThreadInitThunk+0x12
0024fadc 00000000 ntdll!LdrInitializeThunk+0x4d
```

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

If presented with this dialog choose No:



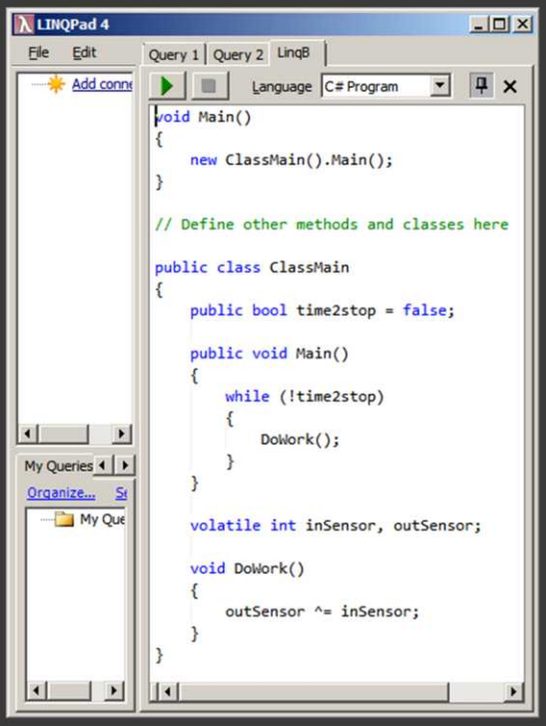
Process Memory Dumps

Exercises PN1 - PN8

© 2013 Software Diagnostics Services

All exercises were modeled on real-life examples using specially constructed applications. Process memory dumps from exercises PN1 – PN6 were saved from an isolated Windows Vista system, and process memory dumps from exercises PN7 – PN8 were saved from Windows 7 x64 system. We will learn how to recognize 20 .NET patterns and a few general unmanaged ones.

Modeling with LINQPad



http://www.linqpad.net/

© 2013 Software Diagnostics Services

Exercises 3, 4, 5, 6, 7 and 8 were modeled using LINQPad application (www.linqpad.net) where you can write code and instantly execute it. When it hangs, for example, I used Task Manager to save a memory dump.

Exercise PN1

- **Goal:** Learn how to load the correct .NET SOS WinDbg extension and analyze managed space
- **Patterns:** Stack Trace Collection; CLR Thread; Version-Specific Extension; Managed Code Exception; Managed Stack Trace
- **Commands:** .logopen, ~*k, !analyze -v, !pe, ~*e, lmv, .chain, .unload, .load, .logclose
- \ANETMDA-Dumps\Exercise-PN1-Analysis-process-dump-ApplicationA-32-CLR2.pdf

© 2013 Software Diagnostics Services

Exercise PN1: Analysis of an application process dump (ApplicationA, 32-bit, CLR 2)

Goal: Learn how to load the correct .NET SOS WinDbg extension and analyze managed space.

Patterns: Stack Trace Collection; CLR Thread; Version-Specific Extension; Managed Code Exception; Managed Stack Trace

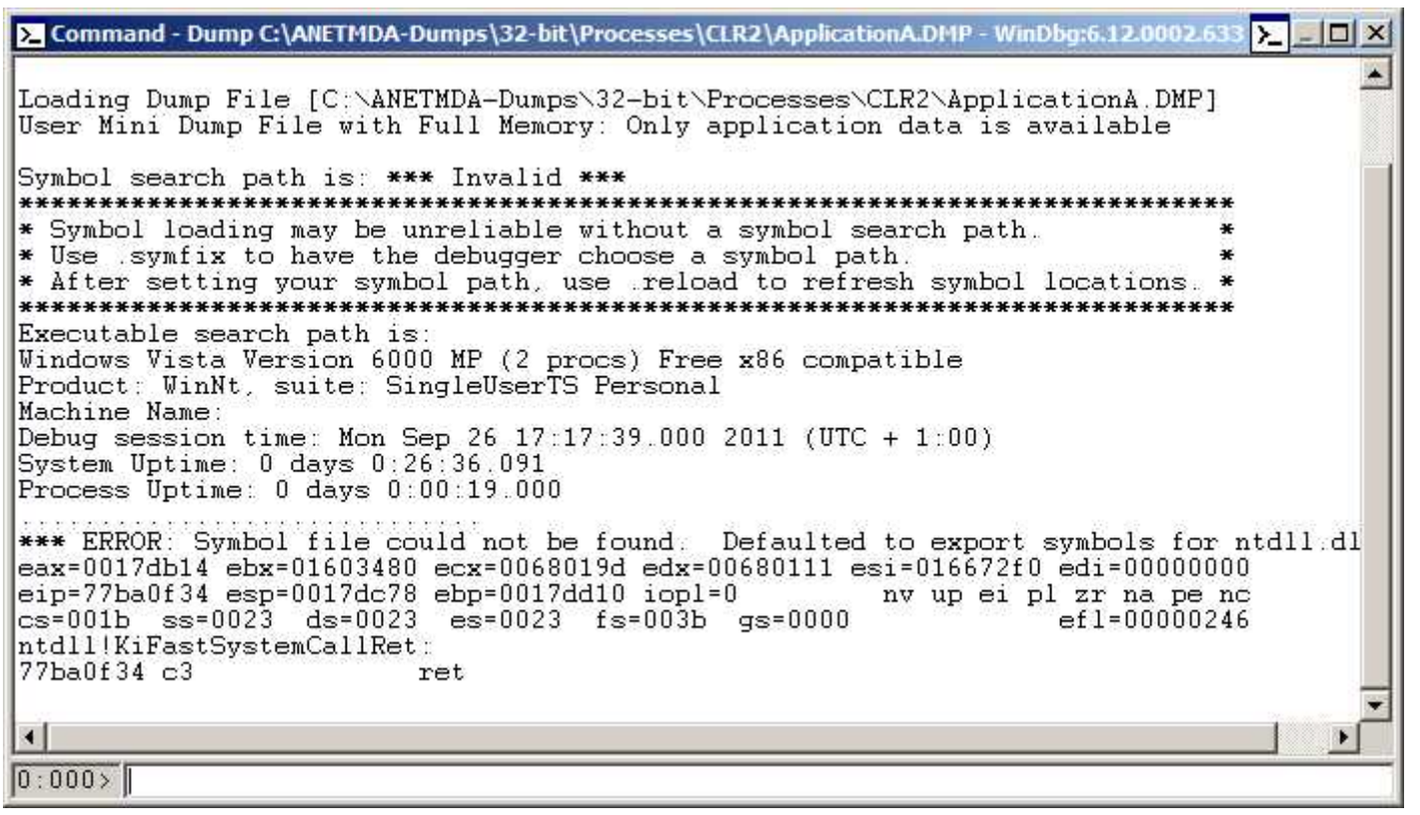
Commands: .logopen, ~*k, !analyze –v, !pe, ~*e, lmv, .chain, .unload, .load, .logclose

1. Launch WinDbg from Debugging Tools for Windows or Debugging Tools for Windows (x86)

2. Open \ANETMDA-Dumps\32-bit\Processes\CLR2\ApplicationA.DMP

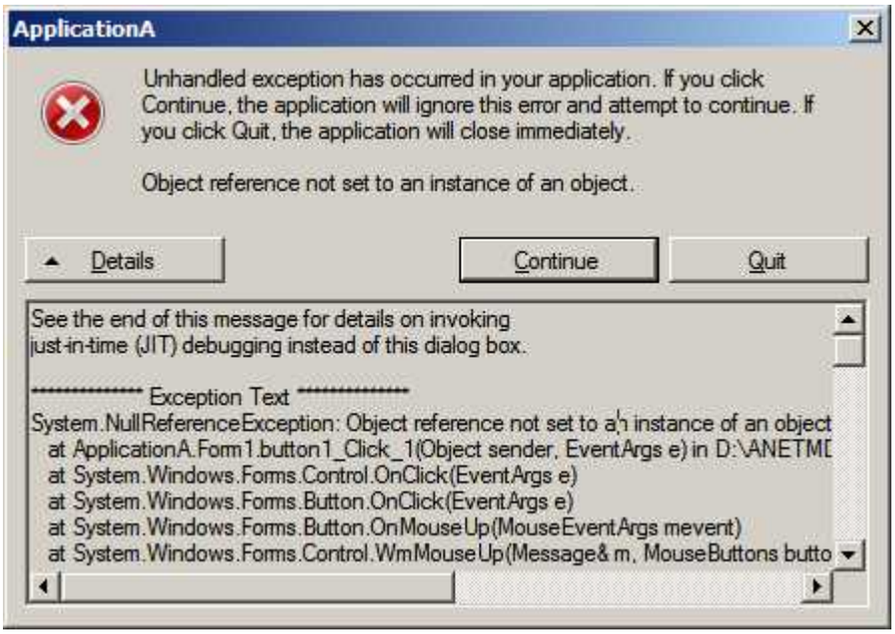
3. If you are presented with this dialog say No:

4. We get the dump file loaded:



Note: ApplicationA shows this dialog when launched:

When we click on a button it shows the following exception dialog:



At this point, we saved a process memory dump on a Vista system using Task Manager.

5. Open a log file using **.logopen** command and load symbols (**.symfix** and **.reload** commands):

```
0:000> .logopen C:\ANETMDA-Dumps\32-bit\Processes\CLR2\ApplicationA.log
Opened log file 'C:\ANETMDA-Dumps\32-bit\Processes\CLR2\ApplicationA.log'

0:000> .symfix c:\mss

0:000> .reload
.............................
```

Note: The results may be slightly different on your system if you have 32-bit .NET Framework 2.0.50727.**312** already installed or you don't have any .NET Framework 2.0.50727 installed.

6. Type ~***k** command to verify the correctness of all stack traces:

```
0:000> ~*k

.  0  Id: dec.dac Suspend: 0 Teb: 7ffdf000 Unfrozen
ChildEBP RetAddr
0017dc74 7720b5b4 ntdll!KiFastSystemCallRet
*** WARNING: Unable to verify checksum for System.Windows.Forms.ni.dll
0017dc78 7b061e04 user32!NtUserWaitMessage+0xc
0017dd10 7b0620f1 System_Windows_Forms_ni+0x91e04
0017dd80 7b062293 System_Windows_Forms_ni+0x920f1
0017ddb0 7b2256ae System_Windows_Forms_ni+0x92293
0017de94 7b2251af System_Windows_Forms_ni+0x2556ae
0017ded4 7b0d1b87 System_Windows_Forms_ni+0x2551af
0017ed38 77211a10 System_Windows_Forms_ni+0x101b87
0017ed64 77211ae8 user32!InternalCallWinProc+0x23
0017eddc 77212a47 user32!UserCallWinProcCheckWow+0x14b
0017ee40 77212a98 user32!DispatchMessageWorker+0x322
0017ee50 00911046 user32!DispatchMessageW+0xf
WARNING: Frame IP not in any known module. Following frames may be wrong.
0017ee6c 7b061c9a 0x911046
0017ef24 7b0620f1 System_Windows_Forms_ni+0x91c9a
0017ef94 7b062293 System_Windows_Forms_ni+0x920f1
0017efc4 7b0c7a3a System_Windows_Forms_ni+0x92293
0017eff0 79e826bd System_Windows_Forms_ni+0xf7a3a
0017f070 79e8451b mscorwks!CallDescrWorkerWithHandler+0xa3
0017f1b4 79e84403 mscorwks!MethodDesc::CallDescr+0x19c
0017f1cc 79e843e0 mscorwks!MethodDesc::CallTargetWorker+0x20
0017f1e0 79ef3e20 mscorwks!MethodDescCallSite::CallWithValueTypes+0x18
0017f344 79ef3c19 mscorwks!ClassLoader::RunMain+0x220
0017f5ac 79ef3aee mscorwks!Assembly::ExecuteMainMethod+0xa6
0017fa7c 79ef3737 mscorwks!SystemDomain::ExecuteMainMethod+0x398
0017facc 79ef18d1 mscorwks!ExecuteEXE+0x59
0017fb14 6e1e55ab mscorwks!_CorExeMain+0x11b
0017fb20 6e187f16 mscoreei!_CorExeMain+0x38
0017fb30 6e184de3 mscoree!ShellShim__CorExeMain+0x99
0017fb38 77563833 mscoree!_CorExeMain_Exported+0x8
0017fb44 77b7a9bd kernel32!BaseThreadInitThunk+0xe
0017fb84 00000000 ntdll!_RtlUserThreadStart+0x23

   1  Id: dec.d14 Suspend: 0 Teb: 7ffde000 Unfrozen
ChildEBP RetAddr
015ff9d0 77ba0690 ntdll!KiFastSystemCallRet
015ff9d4 77567e09 ntdll!ZwWaitForMultipleObjects+0xc
015ffa70 77568150 kernel32!WaitForMultipleObjectsEx+0x11d
015ffa8c 79eec20e kernel32!WaitForMultipleObjects+0x18
015ffaec 79eec16b mscorwks!DebuggerRCThread::MainLoop+0xcf
015ffb1c 79eec0ae mscorwks!DebuggerRCThread::ThreadProc+0xca
015ffb4c 77563833 mscorwks!DebuggerRCThread::ThreadProcStatic+0x82
015ffb58 77b7a9bd kernel32!BaseThreadInitThunk+0xe
015ffb98 00000000 ntdll!_RtlUserThreadStart+0x23
```

```
   2  Id: dec.1b0 Suspend: 0 Teb: 7ffdd000 Unfrozen
ChildEBP RetAddr
00f7f698 77ba0690 ntdll!KiFastSystemCallRet
00f7f69c 77567e09 ntdll!ZwWaitForMultipleObjects+0xc
00f7f738 77568150 kernel32!WaitForMultipleObjectsEx+0x11d
00f7f754 79f8c8ec kernel32!WaitForMultipleObjects+0x18
00f7f774 79ec547e mscorwks!WKS::WaitForFinalizerEvent+0x7a
00f7f788 79ee171c mscorwks!WKS::GCHeap::FinalizerThreadWorker+0x75
00f7f798 79ee16ba mscorwks!Thread::UserResumeThread+0xfb
00f7f82c 79ee15df mscorwks!Thread::DoADCallBack+0x355
00f7f868 79eed73a mscorwks!Thread::DoADCallBack+0x541
00f7f890 79eed705 mscorwks!ManagedThreadBase_NoADTransition+0x32
00f7f89c 79eeecdb mscorwks!ManagedThreadBase::FinalizerBase+0xb
00f7f8d4 79ee118b mscorwks!WKS::GCHeap::FinalizerThreadStart+0xbb
00f7f96c 77563833 mscorwks!Thread::intermediateThreadProc+0x49
00f7f978 77b7a9bd kernel32!BaseThreadInitThunk+0xe
00f7f9b8 00000000 ntdll!_RtlUserThreadStart+0x23

   3  Id: dec.8ac Suspend: 0 Teb: 7ffdc000 Unfrozen
ChildEBP RetAddr
03a0f8a8 77ba0690 ntdll!KiFastSystemCallRet
03a0f8ac 77567e09 ntdll!ZwWaitForMultipleObjects+0xc
03a0f948 7720c4af kernel32!WaitForMultipleObjectsEx+0x11d
03a0f99c 77208b7b user32!RealMsgWaitForMultipleObjectsEx+0x13c
03a0f9b8 74c71965 user32!MsgWaitForMultipleObjects+0x1f
03a0fa04 77563833 GdiPlus!BackgroundThreadProc+0x59
03a0fa10 77b7a9bd kernel32!BaseThreadInitThunk+0xe
03a0fa50 00000000 ntdll!_RtlUserThreadStart+0x23
```

Note: We see that all threads except the last one have **mscorwks** module on their stack traces (newer version of .NET 4.x uses **clr** module).

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

/* start of WinDbg output */

```
0:000> !analyze -v
*******************************************************************************
*                                                                             *
*                        Exception Analysis                                   *
*                                                                             *
*******************************************************************************

*** WARNING: Unable to verify checksum for ApplicationA.exe
*** ERROR: Module load completed but symbols could not be loaded for ApplicationA.exe
*** WARNING: Unable to verify checksum for mscorlib.ni.dll
GetPageUrlData failed, server returned HTTP status 404
URL requested:
http://watson.microsoft.com/StageOne/ApplicationA_exe/1_0_0_0/4e80a47e/unknown/0_0_0_0/bbbbbbb4
/80000003/00000000.htm?Retriage=1

FAULTING_IP:
+680b2faf0087de2c
00000000 ??              ???
```

```
EXCEPTION_RECORD:  ffffffff -- (.exr 0xffffffffffffffff)
ExceptionAddress: 00000000
   ExceptionCode: 80000003 (Break instruction exception)
  ExceptionFlags: 00000000
NumberParameters: 0

FAULTING_THREAD:  00000dac

PROCESS_NAME:  ApplicationA.exe

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

EXCEPTION_CODE: (HRESULT) 0x80000003 (2147483651) - One or more arguments are invalid

MOD_LIST: <ANALYSIS/>

NTGLOBALFLAG:  0

APPLICATION_VERIFIER_FLAGS:  0

MANAGED_STACK: !dumpstack -EE
OS Thread Id: 0xdac (0)
Current frame:
ChildEBP RetAddr  Caller,Callee

EXCEPTION_OBJECT: !pe 161fe3c
Exception object: 0161fe3c
Exception type: System.NullReferenceException
Message: Object reference not set to an instance of an object.
InnerException: <none>
StackTrace (generated):
    SP       IP       Function

StackTraceString: <none>
HResult: 80004003

MANAGED_OBJECT: !dumpobj 1631624
Name: System.String
MethodTable: 790fc6cc
EEClass: 790fc62c
Size: 124(0x7c) bytes
 (C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll)
String: Object reference not set to an instance of an object.
Fields:
      MT    Field   Offset                 Type VT     Attr    Value Name
790ff7f0  4000096        4         System.Int32  1 instance       54 m_arrayLength
790ff7f0  4000097        8         System.Int32  1 instance       53 m_stringLength
790fe2dc  4000098        c          System.Char  1 instance       4f m_firstChar
790fc6cc  4000099       10        System.String  0   shared   static Empty
    >> Domain:Value  002056d0:790d7eb4 <<
7913cb00  400009a       14        System.Char[]  0   shared   static WhitespaceChars
    >> Domain:Value  002056d0:016016dc <<

EXCEPTION_MESSAGE:  Object reference not set to an instance of an object.

MANAGED_OBJECT_NAME:  System.NullReferenceException

DEFAULT_BUCKET_ID:  WRONG_SYMBOLS

PRIMARY_PROBLEM_CLASS:  WRONG_SYMBOLS
```

```
BUGCHECK_STR:  APPLICATION_FAULT_WRONG_SYMBOLS__SYSTEM.NULLREFERENCEEXCEPTION

LAST_CONTROL_TRANSFER:  from 7720b5b4 to 77ba0f34

STACK_TEXT:
0017dc74 7720b5b4 7b061e04 8edbe630 79e719d0 ntdll!KiFastSystemCallRet
0017dc78 7b061e04 8edbe630 79e719d0 0017ddc0 user32!NtUserWaitMessage+0xc
0017dd10 7b0620f1 00000000 00000004 0017dd6c System_Windows_Forms_ni+0x91e04
0017dd80 7b062293 0165789c 00000000 01654d5c System_Windows_Forms_ni+0x920f1
0017ddb0 7b2256ae 0165789c 8edbe630 79e719d0 System_Windows_Forms_ni+0x92293
0017de94 7b2251af 7b0c916b 016318ac 0161fe3c System_Windows_Forms_ni+0x2556ae
0017ded4 7b0d1b87 016051c0 7b0d2a70 7b05e61d System_Windows_Forms_ni+0x2551af
0017ed38 77211a10 001202da 00000202 00000000 System_Windows_Forms_ni+0x101b87
0017ed64 77211ae8 00b20caa 001202da 00000202 user32!InternalCallWinProc+0x23
0017eddc 77212a47 00232e4c 00b20caa 001202da user32!UserCallWinProcCheckWow+0x14b
0017ee40 77212a98 00b20caa 00000000 0017ee6c user32!DispatchMessageWorker+0x322
0017ee50 00911046 0017eee0 8edbe630 00000000 user32!DispatchMessageW+0xf
WARNING: Frame IP not in any known module. Following frames may be wrong.
0017ee6c 7b061c9a 0160c07c 00000001 01603480 0x911046
0017ef24 7b0620f1 00000000 ffffffff 7754736a System_Windows_Forms_ni+0x91c9a
0017ef94 7b062293 01606eac 1e2f0005 016061ec System_Windows_Forms_ni+0x920f1
0017efc4 7b0c7a3a 01606eac 0017f00c 01602bc0 System_Windows_Forms_ni+0x92293
0017eff0 79e826bd 0017f0c0 00000000 0017f090 System_Windows_Forms_ni+0xf7a3a
0017f070 79e8451b 0017f0c0 00000000 0017f090 mscorwks!CallDescrWorkerWithHandler+0xa3
0017f1b4 79e84403 00733068 0017f290 0017f244 mscorwks!MethodDesc::CallDescr+0x19c
0017f1cc 79e843e0 00733068 0017f290 0017f244 mscorwks!MethodDesc::CallTargetWorker+0x20
0017f1e0 79ef3e20 0017f244 8edbaaf6 00000000
mscorwks!MethodDescCallSite::CallWithValueTypes+0x18
0017f344 79ef3c19 00733008 00000001 0017f380 mscorwks!ClassLoader::RunMain+0x220
0017f5ac 79ef3aee 00000000 8edbae26 00000000 mscorwks!Assembly::ExecuteMainMethod+0xa6
0017fa7c 79ef3737 00fc0000 00000000 8edba2b2 mscorwks!SystemDomain::ExecuteMainMethod+0x398
0017facc 79ef18d1 00fc0000 8edba36a 00000000 mscorwks!ExecuteEXE+0x59
0017fb14 6e1e55ab 79ef183a 0017fb30 6e187f16 mscorwks!_CorExeMain+0x11b
0017fb20 6e187f16 00000000 6e1e0000 0017fb44 mscoreei!_CorExeMain+0x38
0017fb30 6e184de3 00000000 77563833 7ffd9000 mscoree!ShellShim__CorExeMain+0x99
0017fb38 77563833 7ffd9000 0017fb84 77b7a9bd mscoree!_CorExeMain_Exported+0x8
0017fb44 77b7a9bd 7ffd9000 001785fa 00000000 kernel32!BaseThreadInitThunk+0xe
0017fb84 00000000 00fc35ee 7ffd9000 00000000 ntdll!_RtlUserThreadStart+0x23


FOLLOWUP_IP:
System_Windows_Forms_ni+91e04
7b061e04 8b4dac          mov     ecx,dword ptr [ebp-54h]

SYMBOL_STACK_INDEX:  2

SYMBOL_NAME:  System_Windows_Forms_ni+91e04

FOLLOWUP_NAME:  MachineOwner

MODULE_NAME: System_Windows_Forms_ni

IMAGE_NAME:  System.Windows.Forms.ni.dll

DEBUG_FLR_IMAGE_TIMESTAMP:  4536f34f

STACK_COMMAND:  dt ntdll!LdrpLastDllInitializer BaseDllName ; dt ntdll!LdrpFailureData ; ~0s;
.ecxr ; kb
```

```
FAILURE_BUCKET_ID:  WRONG_SYMBOLS_80000003_System.Windows.Forms.ni.dll!Unknown

BUCKET_ID:
APPLICATION_FAULT_WRONG_SYMBOLS__SYSTEM.NULLREFERENCEEXCEPTION_System_Windows_Forms_ni+91e04

WATSON_STAGEONE_URL:
http://watson.microsoft.com/StageOne/ApplicationA_exe/1_0_0_0/4e80a47e/unknown/0_0_0_0/bbbbbbb4
/80000003/00000000.htm?Retriage=1

Followup: MachineOwner
---------
                                    /* end of WinDbg output */
```

Note: In addition to normal manual dump breakpoint error (in blue) we have .NET diagnostics (in red) pointing to a NULL object reference (similar to a NULL pointer dereference). However, we don't see any managed stack trace we see on a dialog above. Now we try to get it.

8. We check if there is a .NET exception on the current thread 0:

```
0:000> !pe
Exception object: 0161fe3c
Exception type: System.NullReferenceException
Message: Object reference not set to an instance of an object.
InnerException: <none>
StackTrace (generated):
    SP       IP       Function

StackTraceString: <none>
HResult: 80004003
```

Note: We see the exception but no stack trace. We also double check that no other threads have exceptions by executing **!pe** command for each thread using **~*e** command:

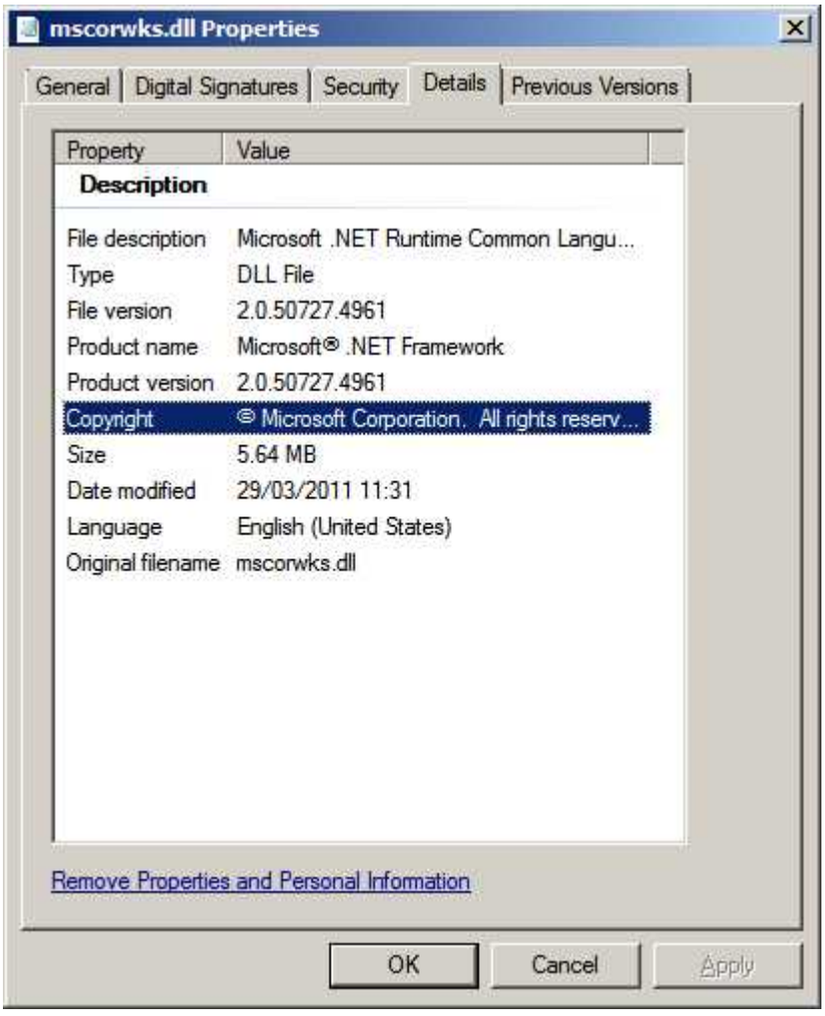
```
0:000> ~*e !pe
Exception object: 0161fe3c
Exception type: System.NullReferenceException
Message: Object reference not set to an instance of an object.
InnerException: <none>
StackTrace (generated):
    SP       IP       Function

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

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

```
0:000> lmv m mscorwks
start    end        module name
79e70000 7a3d6000   mscorwks   (pdb symbols)
c:\mss\mscorwks.pdb\777BB0057A2341BA8F3A03546FA9EB542\mscorwks.pdb
    Loaded symbol image file: mscorwks.dll
    Image path: C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
    Image name: mscorwks.dll
```

```
Timestamp:        Thu Oct 19 08:08:07 2006 (45372457)
CheckSum:         00562079
ImageSize:        00566000
File version:     2.0.50727.312
Product version:  2.0.50727.312
File flags:       0 (Mask 3F)
File OS:          4 Unknown Win32
File type:        2.0 Dll
File date:        00000000.00000000
Translations:     0409.04b0
CompanyName:      Microsoft Corporation
ProductName:      Microsoft® .NET Framework
InternalName:     mscorwks.dll
OriginalFilename: mscorwks.dll
ProductVersion:   2.0.50727.312
FileVersion:      2.0.50727.312 (rtmLHS.050727-3100)
FileDescription:  Microsoft .NET Runtime Common Language Runtime - WorkStation
LegalCopyright:   © Microsoft Corporation.  All rights reserved.
Comments:         Flavor=Retail
```

Note: On my analysis system the version is slightly different (C:\Windows\Microsoft.NET\Framework\v2.0.50727):



It has a different .4961 version suffix. The version can also be checked by listing all loaded WinDbg extensions (sos.dll is used for .NET analysis):

```
0:000> .chain
Extension DLL search Path:
[...]
Extension DLL chain:
    C:\Windows\Microsoft.NET\Framework\v2.0.50727\sos: image 2.0.50727.4961, API 1.0.0, built
Fri Mar 25 04:23:32 2011
        [path: C:\Windows\Microsoft.NET\Framework\v2.0.50727\sos.dll]
    dbghelp: image 6.12.0002.633, API 6.1.6, built Mon Feb 01 20:08:26 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\dbghelp.dll]
    ext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:31 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\winext\ext.dll]
    exts: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:24 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\WINXP\exts.dll]
    uext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:23 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\winext\uext.dll]
    ntsdexts: image 6.1.7650.0, API 1.0.0, built Mon Feb 01 20:08:08 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\WINXP\ntsdexts.dll]
```

10. In the folder C:\ANETMDA-Dumps\32-bit\Microsoft.NET\Framework\v2.0.50727 we have the correct version .312 of .NET Framework copied from the machine the memory dump came from. So we unload the current SOS extension (**.unload** command) and load the new one (**.load** command):

```
0:000> .unload C:\Windows\Microsoft.NET\Framework\v2.0.50727\sos
Unloading C:\Windows\Microsoft.NET\Framework\v2.0.50727\sos extension DLL

0:000> .chain
Extension DLL search Path:
[...]
Extension DLL chain:
    dbghelp: image 6.12.0002.633, API 6.1.6, built Mon Feb 01 20:08:26 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\dbghelp.dll]
    ext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:31 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\winext\ext.dll]
    exts: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:24 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\WINXP\exts.dll]
    uext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:23 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\winext\uext.dll]
    ntsdexts: image 6.1.7650.0, API 1.0.0, built Mon Feb 01 20:08:08 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\WINXP\ntsdexts.dll]

0:000> .load C:\ANETMDA-Dumps\32-bit\Microsoft.NET\Framework\v2.0.50727\sos

0:000> .chain
Extension DLL search Path:
[...]
Extension DLL chain:
    C:\ANETMDA-Dumps\32-bit\Microsoft.NET\Framework\v2.0.50727\sos: image 2.0.50727.312, API
1.0.0, built Thu Oct 19 04:37:43 2006
        [path: C:\ANETMDA-Dumps\32-bit\Microsoft.NET\Framework\v2.0.50727\sos.dll]
    dbghelp: image 6.12.0002.633, API 6.1.6, built Mon Feb 01 20:08:26 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\dbghelp.dll]
    ext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:31 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\winext\ext.dll]
    exts: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:24 2010
```

```
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\WINXP\exts.dll]
    uext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:23 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\winext\uext.dll]
    ntsdexts: image 6.1.7650.0, API 1.0.0, built Mon Feb 01 20:08:08 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\WINXP\ntsdexts.dll]
```

11. We now retry **!pe** command:

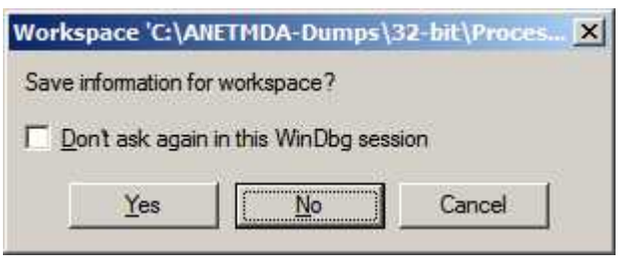
```
0:000> !pe
Exception object: 0161fe3c
Exception type: System.NullReferenceException
Message: Object reference not set to an instance of an object.
InnerException: <none>
StackTrace (generated):
    SP       IP       Function
    0017EB78 00800299 ApplicationA.Form1.button1_Click_1(System.Object, System.EventArgs)
    0017EB80 7B0693EB System.Windows.Forms.Control.OnClick(System.EventArgs)
    0017EB90 7B1065E9 System.Windows.Forms.Button.OnClick(System.EventArgs)
    0017EB9C 7B1066EF
System.Windows.Forms.Button.OnMouseUp(System.Windows.Forms.MouseEventArgs)
    0017EBC0 7B0D16EF System.Windows.Forms.Control.WmMouseUp(System.Windows.Forms.Message
ByRef, System.Windows.Forms.MouseButtons, Int32)
    0017EC1C 7B062A8F System.Windows.Forms.Control.WndProc(System.Windows.Forms.Message ByRef)
    0017EC80 7B08512B System.Windows.Forms.ButtonBase.WndProc(System.Windows.Forms.Message
ByRef)
    0017ECBC 7B08504B System.Windows.Forms.Button.WndProc(System.Windows.Forms.Message ByRef)
    0017ECC4 7B06237D
System.Windows.Forms.Control+ControlNativeWindow.OnMessage(System.Windows.Forms.Message ByRef)
    0017ECC8 7B062466
System.Windows.Forms.Control+ControlNativeWindow.WndProc(System.Windows.Forms.Message ByRef)
    0017ECDC 7B05E605 System.Windows.Forms.NativeWindow.Callback(IntPtr, Int32, IntPtr, IntPtr)

StackTraceString: <none>
HResult: 80004003
```

Note: We see now the correct managed stack trace.

12. We close logging before exiting WinDbg:

```
0:000> .logclose
Closing open log file C:\ANETMDA-Dumps\32-bit\Processes\CLR2\ApplicationA.log
```

If presented with this dialog choose No:



Note: To avoid possible confusion and glitches we recommend to exit WinDbg after each exercise.

Exercise PN2

- **Goal:** Compare CLR 2 with CLR 4. Manual stack reconstruction (*Advanced*).
- **Patterns:** Stack Trace Collection; CLR Thread; Version-Specific Extension; Managed Code Exception; Managed Stack Trace; Truncated Stack Trace; Incorrect Stack Trace (*Advanced*)
- **Commands:** .kframes, kc, dps, k L=<>
- \ANETMDA-Dumps\Exercise-PN2-Analysis-process-dump-ApplicationA-32-CLR4.pdf

© 2013 Software Diagnostics Services

Exercise PN2: Analysis of an application process dump (ApplicationA, 32-bit, CLR 4)

Goal: Compare CLR 2 with CLR 4. Manual stack reconstruction (*Advanced*).

Patterns: Stack Trace Collection; CLR Thread; Version-Specific Extension; Managed Code Exception; Managed Stack Trace; Truncated Stack Trace; Incorrect Stack Trace (*Advanced*)

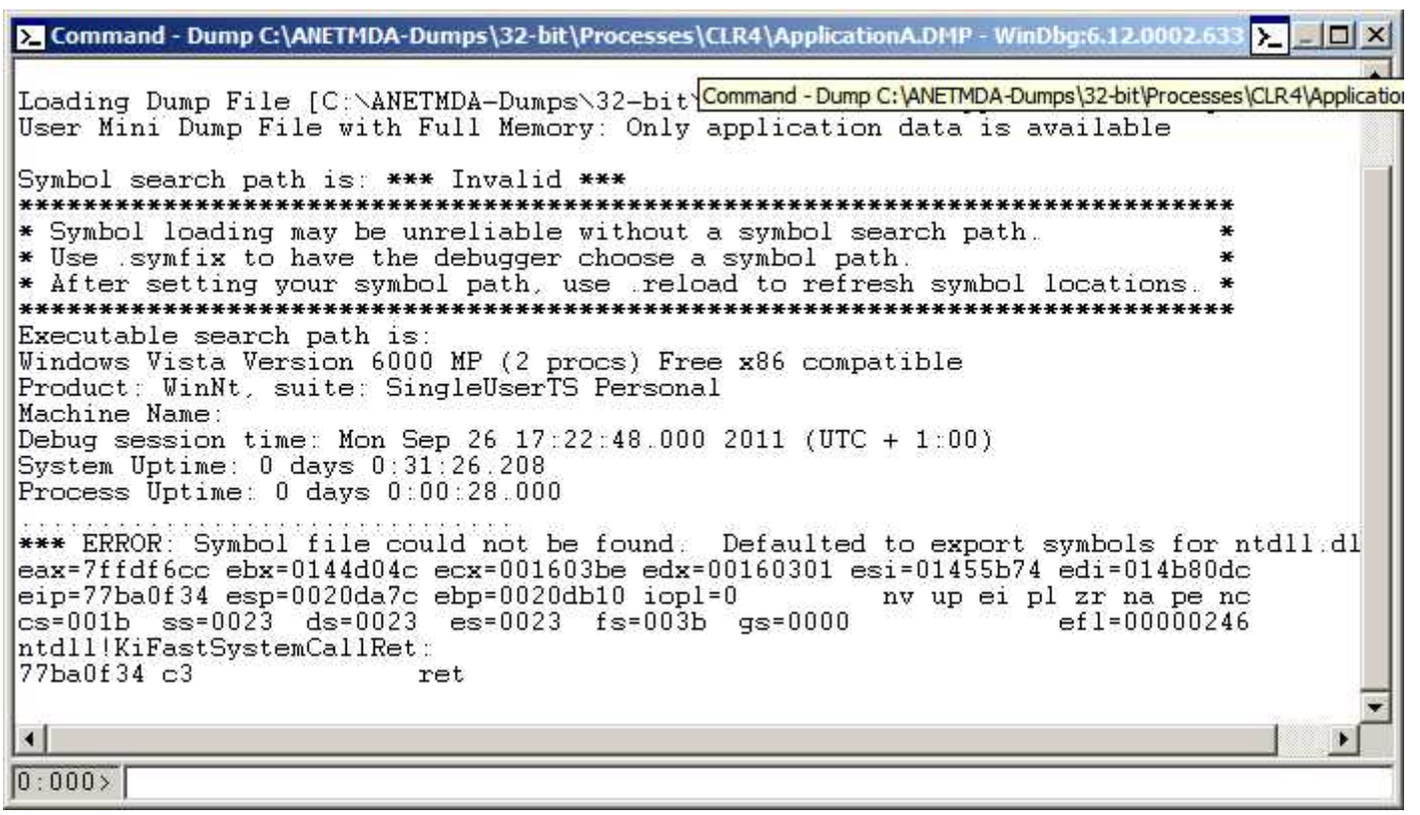
Commands: .kframes, kc, dps, k L=<>

1. Launch WinDbg from Debugging Tools for Windows or Debugging Tools for Windows (x86)

2. Open \ANETMDA-Dumps\32-bit\Processes\CLR4\ApplicationA.DMP

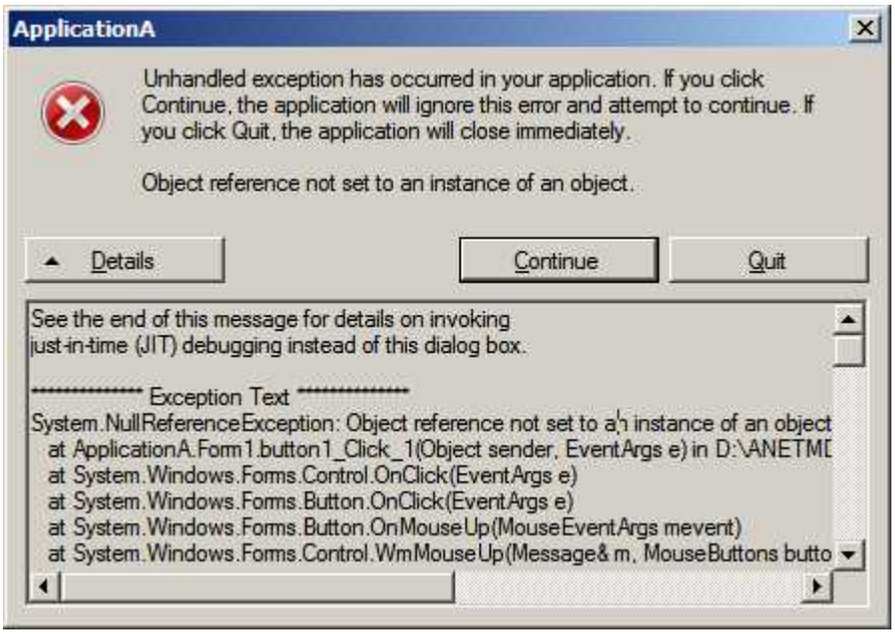
3. If you are presented with this dialog say No:

4. We get the dump file loaded:



Note: ApplicationA shows this dialog when launched:

When we click on a button it shows the following exception dialog:



At this point, we saved a process memory dump on a Vista system using Task Manager.

5. Open a log file using **.logopen** command and load symbols (**.symfix** and **.reload** commands):

```
0:000> .logopen C:\ANETMDA-Dumps\32-bit\Processes\CLR4\ApplicationA.log
Opened log file 'C:\ANETMDA-Dumps\32-bit\Processes\CLR4\ApplicationA.log'

0:000> .symfix c:\mss

0:000> .reload
.............................
```

Note: The results may be slightly different on your system if you have 32-bit .NET Framework 4.0.30319.**1** already installed or you don't have any .NET Framework 4.0.30319 installed.

6. Type ~*k command to verify the correctness of all stack traces:

```
0:000> ~*k

.  0  Id: 864.a70 Suspend: 0 Teb: 7ffdf000 Unfrozen
ChildEBP RetAddr
0020da78 7720b5b4 ntdll!KiFastSystemCallRet
*** WARNING: Unable to verify checksum for System.Windows.Forms.ni.dll
0020da7c 68e6737a user32!NtUserWaitMessage+0xc
0020db10 68e66e2c System_Windows_Forms_ni+0x22737a
0020db6c 68e66c81 System_Windows_Forms_ni+0x226e2c
0020db9c 6935fefb System_Windows_Forms_ni+0x226c81
0020dbb4 69389f83 System_Windows_Forms_ni+0x71fefb
0020dc50 6938a1b7 System_Windows_Forms_ni+0x749f83
0020dc90 69369866 System_Windows_Forms_ni+0x74a1b7
0020dc9c 6936ff9c System_Windows_Forms_ni+0x729866
0020ecb0 764a2459 System_Windows_Forms_ni+0x72ff9c
0020ecbc 77211a10 msctf!TF_Notify+0x239
0020ece8 77211ae8 user32!InternalCallWinProc+0x23
0020ed60 77212a47 user32!UserCallWinProcCheckWow+0x14b
0020edc4 77212a98 user32!DispatchMessageWorker+0x322
0020edd4 68e72eec user32!DispatchMessageW+0xf
0020ee20 68e671ff System_Windows_Forms_ni+0x232eec
0020eeb4 68e66e2c System_Windows_Forms_ni+0x2271ff
0020ef10 68e66c81 System_Windows_Forms_ni+0x226e2c
0020ef40 68df366d System_Windows_Forms_ni+0x226c81
0020ef64 6ce421db System_Windows_Forms_ni+0x1b366d
0020ef6c 6ce4e021 clr!CallDescrWorker+0x33
0020ef84 00000000 clr!SigParser::GetElemType+0x28

   1  Id: 864.c64 Suspend: 0 Teb: 7ffde000 Unfrozen
ChildEBP RetAddr
0130faa8 77ba0690 ntdll!KiFastSystemCallRet
0130faac 77567e09 ntdll!ZwWaitForMultipleObjects+0xc
0130fb48 77568150 kernel32!WaitForMultipleObjectsEx+0x11d
0130fb64 6cfa75e8 kernel32!WaitForMultipleObjects+0x18
0130fbc8 6cfa7526 clr!DebuggerRCThread::MainLoop+0xd9
0130fbf8 6cfa7461 clr!DebuggerRCThread::ThreadProc+0xca
0130fc24 77563833 clr!DebuggerRCThread::ThreadProcStatic+0x83
0130fc30 77b7a9bd kernel32!BaseThreadInitThunk+0xe
0130fc70 00000000 ntdll!_RtlUserThreadStart+0x23

   2  Id: 864.d84 Suspend: 0 Teb: 7ffdd000 Unfrozen
ChildEBP RetAddr
0369f910 77ba0690 ntdll!KiFastSystemCallRet
0369f914 77567e09 ntdll!ZwWaitForMultipleObjects+0xc
0369f9b0 77568150 kernel32!WaitForMultipleObjectsEx+0x11d
0369f9cc 6cfb833d kernel32!WaitForMultipleObjects+0x18
0369f9ec 6cfb83a1 clr!WKS::WaitForFinalizerEvent+0xa6
0369fa04 6cef5c05 clr!WKS::GCHeap::FinalizerThreadWorker+0x4a
0369fa18 6cef5c87 clr!Thread::DoExtraWorkForFinalizer+0x114
0369fac8 6cef5d42 clr!Thread::ShouldChangeAbortToUnload+0x101
0369fb28 6cee78be clr!Thread::ShouldChangeAbortToUnload+0x399
0369fb4c 6cee78d1 clr!ManagedThreadBase_NoADTransition+0x35
0369fb5c 6cf2d313 clr!ManagedThreadBase::FinalizerBase+0xf
0369fb94 6cef5a08 clr!WKS::GCHeap::FinalizerThreadStart+0x10c
0369fc34 77563833 clr!Thread::intermediateThreadProc+0x4b
0369fc40 77b7a9bd kernel32!BaseThreadInitThunk+0xe
0369fc80 00000000 ntdll!_RtlUserThreadStart+0x23
```

```
   3  Id: 864.b7c Suspend: 0 Teb: 7ffdc000 Unfrozen
ChildEBP RetAddr
03abfb70 77ba0690 ntdll!KiFastSystemCallRet
03abfb74 77567e09 ntdll!ZwWaitForMultipleObjects+0xc
03abfc10 7720c4af kernel32!WaitForMultipleObjectsEx+0x11d
03abfc64 77208b7b user32!RealMsgWaitForMultipleObjectsEx+0x13c
03abfc80 74c71965 user32!MsgWaitForMultipleObjects+0x1f
03abfccc 77563833 GdiPlus!BackgroundThreadProc+0x59
03abfcd8 77b7a9bd kernel32!BaseThreadInitThunk+0xe
03abfd18 00000000 ntdll!_RtlUserThreadStart+0x23
```

Note: We see that all threads except the last one have **clr** module on their stack traces (older versions like .NET 2.x-3.x use **mscorwks** module).

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

/* start of WinDbg output */

```
0:000> !analyze -v
*******************************************************************************
*                                                                             *
*                        Exception Analysis                                   *
*                                                                             *
*******************************************************************************

*** WARNING: Unable to verify checksum for ApplicationA.exe
*** ERROR: Module load completed but symbols could not be loaded for ApplicationA.exe
*** WARNING: Unable to verify checksum for mscorlib.ni.dll
The version of SOS does not match the version of CLR you are debugging.  Please
load the matching version of SOS for the version of CLR you are debugging.
CLR Version: 4.0.30319.1
SOS Version: 4.0.30319.235
The version of SOS does not match the version of CLR you are debugging.  Please
load the matching version of SOS for the version of CLR you are debugging.
CLR Version: 4.0.30319.1
SOS Version: 4.0.30319.235
The version of SOS does not match the version of CLR you are debugging.  Please
load the matching version of SOS for the version of CLR you are debugging.
CLR Version: 4.0.30319.1
SOS Version: 4.0.30319.235
The version of SOS does not match the version of CLR you are debugging.  Please
load the matching version of SOS for the version of CLR you are debugging.
CLR Version: 4.0.30319.1
SOS Version: 4.0.30319.235
The version of SOS does not match the version of CLR you are debugging.  Please
load the matching version of SOS for the version of CLR you are debugging.
CLR Version: 4.0.30319.1
SOS Version: 4.0.30319.235
The version of SOS does not match the version of CLR you are debugging.  Please
load the matching version of SOS for the version of CLR you are debugging.
CLR Version: 4.0.30319.1
SOS Version: 4.0.30319.235
The version of SOS does not match the version of CLR you are debugging.  Please
load the matching version of SOS for the version of CLR you are debugging.
CLR Version: 4.0.30319.1
SOS Version: 4.0.30319.235
The version of SOS does not match the version of CLR you are debugging.  Please
load the matching version of SOS for the version of CLR you are debugging.
CLR Version: 4.0.30319.1
SOS Version: 4.0.30319.235
The version of SOS does not match the version of CLR you are debugging.  Please
load the matching version of SOS for the version of CLR you are debugging.
CLR Version: 4.0.30319.1
SOS Version: 4.0.30319.235
The version of SOS does not match the version of CLR you are debugging.  Please
load the matching version of SOS for the version of CLR you are debugging.
CLR Version: 4.0.30319.1
SOS Version: 4.0.30319.235
The version of SOS does not match the version of CLR you are debugging.  Please
```

```
load the matching version of SOS for the version of CLR you are debugging.
CLR Version: 4.0.30319.1
SOS Version: 4.0.30319.235
The version of SOS does not match the version of CLR you are debugging.  Please
load the matching version of SOS for the version of CLR you are debugging.
CLR Version: 4.0.30319.1
SOS Version: 4.0.30319.235
GetPageUrlData failed, server returned HTTP status 404
URL requested:
http://watson.microsoft.com/StageOne/ApplicationA_exe/1_0_0_0/4e80a65a/unknown/0_0_0_0/bbbbbbb4/80000003/00000000.htm?
Retriage=1

FAULTING_IP:
+6c482faf020eded8
00000000 ??              ???

EXCEPTION_RECORD:  ffffffff -- (.exr 0xffffffffffffffff)
ExceptionAddress: 00000000
   ExceptionCode: 80000003 (Break instruction exception)
  ExceptionFlags: 00000000
NumberParameters: 0

FAULTING_THREAD:  00000a70

PROCESS_NAME:  ApplicationA.exe

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

EXCEPTION_CODE: (HRESULT) 0x80000003 (2147483651) - One or more arguments are invalid

MOD_LIST: <ANALYSIS/>

NTGLOBALFLAG:  0

APPLICATION_VERIFIER_FLAGS:  0

MANAGED_STACK:
SP       IP       Function
    0020EA90 002D0250 ApplicationA!ApplicationA.Form1.button1_Click_1(System.Object, System.EventArgs)
    0020EA98 68E04AE8 System_Windows_Forms_ni!System.Windows.Forms.Control.OnClick(System.EventArgs)+0x70
    0020EAB0 68E070A2 System_Windows_Forms_ni!System.Windows.Forms.Button.OnClick(System.EventArgs)+0xa2
    0020EAC8 69396174
System_Windows_Forms_ni!System.Windows.Forms.Button.OnMouseUp(System.Windows.Forms.MouseEventArgs)+0xac
    0020EAE4 693695B5 System_Windows_Forms_ni!System.Windows.Forms.Control.WmMouseUp(System.Windows.Forms.Message
ByRef, System.Windows.Forms.MouseButtons, Int32)+0x2d1
    0020EB78 6972A1BF System_Windows_Forms_ni!System.Windows.Forms.Control.WndProc(System.Windows.Forms.Message
ByRef)+0x8d30bf
    0020EBD0 697318DD System_Windows_Forms_ni!System.Windows.Forms.ButtonBase.WndProc(System.Windows.Forms.Message
ByRef)+0x8c3ac1
    0020EC14 68E6DE00 System_Windows_Forms_ni!System.Windows.Forms.Button.WndProc(System.Windows.Forms.Message
ByRef)+0x20
    0020EC20 68E570F3
System_Windows_Forms_ni!System.Windows.Forms.Control+ControlNativeWindow.OnMessage(System.Windows.Forms.Message
ByRef)+0x13
    0020EC28 68E57071
System_Windows_Forms_ni!System.Windows.Forms.Control+ControlNativeWindow.WndProc(System.Windows.Forms.Message
ByRef)+0x31
    0020EC3C 68E56FB6 System_Windows_Forms_ni!System.Windows.Forms.NativeWindow.Callback(IntPtr, Int32, IntPtr,
IntPtr)+0x96

StackTraceString: <none>
HResult: 80004003
```

```
EXCEPTION_OBJECT: !pe 1467f44
The version of SOS does not match the version of CLR you are debugging.  Please
load the matching version of SOS for the version of CLR you are debugging.
CLR Version: 4.0.30319.1
SOS Version: 4.0.30319.235
Exception object: 01467f44
Exception type:   System.NullReferenceException
Message:          Object reference not set to an instance of an object.
InnerException:   <none>
StackTrace (generated):
    SP       IP       Function
    0020EA90 002D0250 ApplicationA!ApplicationA.Form1.button1_Click_1(System.Object, System.EventArgs)
    0020EA98 68E04AE8 System_Windows_Forms_ni!System.Windows.Forms.Control.OnClick(System.EventArgs)+0x70
    0020EAB0 68E070A2 System_Windows_Forms_ni!System.Windows.Forms.Button.OnClick(System.EventArgs)+0xa2
    0020EAC8 69396174
System_Windows_Forms_ni!System.Windows.Forms.Button.OnMouseUp(System.Windows.Forms.MouseEventArgs)+0xac
    0020EAE4 693695B5 System_Windows_Forms_ni!System.Windows.Forms.Control.WmMouseUp(System.Windows.Forms.Message
ByRef, System.Windows.Forms.MouseButtons, Int32)+0x2d1
    0020EB78 6972A1BF System_Windows_Forms_ni!System.Windows.Forms.Control.WndProc(System.Windows.Forms.Message
ByRef)+0x8d30bf
    0020EBD0 697318DD System_Windows_Forms_ni!System.Windows.Forms.ButtonBase.WndProc(System.Windows.Forms.Message
ByRef)+0x8c3ac1
    0020EC14 68E6DE00 System_Windows_Forms_ni!System.Windows.Forms.Button.WndProc(System.Windows.Forms.Message
ByRef)+0x20
    0020EC20 68E570F3
System_Windows_Forms_ni!System.Windows.Forms.Control+ControlNativeWindow.OnMessage(System.Windows.Forms.Message
ByRef)+0x13
    0020EC28 68E57071
System_Windows_Forms_ni!System.Windows.Forms.Control+ControlNativeWindow.WndProc(System.Windows.Forms.Message
ByRef)+0x31
    0020EC3C 68E56FB6 System_Windows_Forms_ni!System.Windows.Forms.NativeWindow.Callback(IntPtr, Int32, IntPtr,
IntPtr)+0x96

StackTraceString: <none>
HResult: 80004003

MANAGED_OBJECT: !dumpobj 147eee4
The version of SOS does not match the version of CLR you are debugging.  Please
load the matching version of SOS for the version of CLR you are debugging.
CLR Version: 4.0.30319.1
SOS Version: 4.0.30319.235
Name:        System.String
MethodTable: 6a46f9ac
EEClass:     6a1a8bb0
Size:        120(0x78) bytes
File:        C:\Windows\Microsoft.Net\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll
String:      Object reference not set to an instance of an object.
Fields:
      MT    Field   Offset                 Type VT     Attr    Value Name
6a472978  40000ed        4         System.Int32  1 instance       53 m_stringLength
6a471dc8  40000ee        8          System.Char  1 instance       4f m_firstChar
6a46f9ac  40000ef        8        System.String  0   shared   static Empty
    >> Domain:Value  003e1130:01441228 <<

EXCEPTION_MESSAGE:  Object reference not set to an instance of an object.

MANAGED_OBJECT_NAME:  System.NullReferenceException

MANAGED_STACK_COMMAND:  !pe 1467f44


LAST_CONTROL_TRANSFER:  from 7720b5b4 to 77ba0f34

ADDITIONAL_DEBUG_TEXT:  Followup set based on attribute [Is_ChosenCrashFollowupThread] from Frame:[0] on
thread:[PSEUDO_THREAD]

DEFAULT_BUCKET_ID:  WRONG_SYMBOLS

PRIMARY_PROBLEM_CLASS:  WRONG_SYMBOLS

BUGCHECK_STR:  APPLICATION_FAULT_WRONG_SYMBOLS__SYSTEM.NULLREFERENCEEXCEPTION
```

```
STACK_TEXT:
0020ea90 002d0250 applicationa!ApplicationA.Form1.button1_Click_1+0x0
0020ea98 68e04ae8 system_windows_forms_ni!System.Windows.Forms.Control.OnClick+0x70
0020eab0 68e070a2 system_windows_forms_ni!System.Windows.Forms.Button.OnClick+0xa2
0020eac8 69396174 system_windows_forms_ni!System.Windows.Forms.Button.OnMouseUp+0xac
0020eae4 693695b5 system_windows_forms_ni!System.Windows.Forms.Control.WmMouseUp+0x2d1
0020eb78 6972a1bf system_windows_forms_ni!System.Windows.Forms.Control.WndProc+0x8d30bf
0020ebd0 697318dd system_windows_forms_ni!System.Windows.Forms.ButtonBase.WndProc+0x8c3ac1
0020ec14 68e6de00 system_windows_forms_ni!System.Windows.Forms.Button.WndProc+0x20
0020ec20 68e570f3 system_windows_forms_ni!System.Windows.Forms.Control_ControlNativeWindow.OnMessage+0x13
0020ec28 68e57071 system_windows_forms_ni!System.Windows.Forms.Control_ControlNativeWindow.WndProc+0x31
0020ec3c 68e56fb6 system_windows_forms_ni!System.Windows.Forms.NativeWindow.Callback+0x96


FOLLOWUP_IP:
System_Windows_Forms_ni+1c4ae8
68e04ae8 59              pop     ecx

SYMBOL_STACK_INDEX:  1

SYMBOL_NAME:  system_windows_forms_ni!System.Windows.Forms.Control.OnClick+1c4ae8

FOLLOWUP_NAME:  MachineOwner

MODULE_NAME: System_Windows_Forms_ni

IMAGE_NAME:  System.Windows.Forms.ni.dll

DEBUG_FLR_IMAGE_TIMESTAMP:  4ba1e14e

STACK_COMMAND:  !pe 1467f44
 ; dt ntdll!LdrpLastDllInitializer BaseDllName ; dt ntdll!LdrpFailureData ; ** Pseudo Context ** ; kb

FAILURE_BUCKET_ID:  WRONG_SYMBOLS_80000003_System.Windows.Forms.ni.dll!System.Windows.Forms.Control.OnClick

BUCKET_ID:
APPLICATION_FAULT_WRONG_SYMBOLS__SYSTEM.NULLREFERENCEEXCEPTION_system_windows_forms_ni!System.Windows.Forms.Control.On
Click+1c4ae8

WATSON_STAGEONE_URL:
http://watson.microsoft.com/StageOne/ApplicationA_exe/1_0_0_0/4e80a65a/unknown/0_0_0_0/bbbbbbb4/80000003/00000000.htm?
Retriage=1

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

/* end of WinDbg output */

Note: We see .NET diagnostics (in blue) pointing to a NULL object reference (similar to a NULL pointer dereference). However, we see lots of warnings (in red) that CLR version on a system where the dump file came from (CLR Version: 4.0.30319.**1**) is not the save as on an analysis machine (SOS Version: 4.0.30319.**235**).

8. We check if there is a .NET exception on the current thread 0:

```
0:000> !pe
The version of SOS does not match the version of CLR you are debugging.  Please
load the matching version of SOS for the version of CLR you are debugging.
CLR Version: 4.0.30319.1
SOS Version: 4.0.30319.235
Exception object: 01467f44
Exception type:   System.NullReferenceException
Message:          Object reference not set to an instance of an object.
InnerException:   <none>
StackTrace (generated):
    SP       IP       Function
    0020EA90 002D0250 ApplicationA!ApplicationA.Form1.button1_Click_1(System.Object, System.EventArgs)
    0020EA98 68E04AE8 System_Windows_Forms_ni!System.Windows.Forms.Control.OnClick(System.EventArgs)+0x70
    0020EAB0 68E070A2 System_Windows_Forms_ni!System.Windows.Forms.Button.OnClick(System.EventArgs)+0xa2
    0020EAC8 69396174
System_Windows_Forms_ni!System.Windows.Forms.Button.OnMouseUp(System.Windows.Forms.MouseEventArgs)+0xac
    0020EAE4 693695B5 System_Windows_Forms_ni!System.Windows.Forms.Control.WmMouseUp(System.Windows.Forms.Message
ByRef, System.Windows.Forms.MouseButtons, Int32)+0x2d1
    0020EB78 6972A1BF System_Windows_Forms_ni!System.Windows.Forms.Control.WndProc(System.Windows.Forms.Message
ByRef)+0x8d30bf
    0020EBD0 697318DD System_Windows_Forms_ni!System.Windows.Forms.ButtonBase.WndProc(System.Windows.Forms.Message
ByRef)+0x8c3ac1
    0020EC14 68E6DE00 System_Windows_Forms_ni!System.Windows.Forms.Button.WndProc(System.Windows.Forms.Message
ByRef)+0x20
    0020EC20 68E570F3
System_Windows_Forms_ni!System.Windows.Forms.Control+ControlNativeWindow.OnMessage(System.Windows.Forms.Message
ByRef)+0x13
    0020EC28 68E57071
System_Windows_Forms_ni!System.Windows.Forms.Control+ControlNativeWindow.WndProc(System.Windows.Forms.Message
ByRef)+0x31
    0020EC3C 68E56FB6 System_Windows_Forms_ni!System.Windows.Forms.NativeWindow.Callback(IntPtr, Int32, IntPtr,
IntPtr)+0x96

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
The version of SOS does not match the version of CLR you are debugging.  Please
load the matching version of SOS for the version of CLR you are debugging.
CLR Version: 4.0.30319.1
SOS Version: 4.0.30319.235
Exception object: 01467f44
Exception type:   System.NullReferenceException
Message:          Object reference not set to an instance of an object.
InnerException:   <none>
StackTrace (generated):
    SP       IP       Function
    0020EA90 002D0250 ApplicationA!ApplicationA.Form1.button1_Click_1(System.Object, System.EventArgs)
    0020EA98 68E04AE8 System_Windows_Forms_ni!System.Windows.Forms.Control.OnClick(System.EventArgs)+0x70
    0020EAB0 68E070A2 System_Windows_Forms_ni!System.Windows.Forms.Button.OnClick(System.EventArgs)+0xa2
    0020EAC8 69396174
System_Windows_Forms_ni!System.Windows.Forms.Button.OnMouseUp(System.Windows.Forms.MouseEventArgs)+0xac
    0020EAE4 693695B5 System_Windows_Forms_ni!System.Windows.Forms.Control.WmMouseUp(System.Windows.Forms.Message
ByRef, System.Windows.Forms.MouseButtons, Int32)+0x2d1
    0020EB78 6972A1BF System_Windows_Forms_ni!System.Windows.Forms.Control.WndProc(System.Windows.Forms.Message
ByRef)+0x8d30bf
    0020EBD0 697318DD System_Windows_Forms_ni!System.Windows.Forms.ButtonBase.WndProc(System.Windows.Forms.Message
ByRef)+0x8c3ac1
    0020EC14 68E6DE00 System_Windows_Forms_ni!System.Windows.Forms.Button.WndProc(System.Windows.Forms.Message
ByRef)+0x20
    0020EC20 68E570F3
System_Windows_Forms_ni!System.Windows.Forms.Control+ControlNativeWindow.OnMessage(System.Windows.Forms.Message
ByRef)+0x13
    0020EC28 68E57071
System_Windows_Forms_ni!System.Windows.Forms.Control+ControlNativeWindow.WndProc(System.Windows.Forms.Message
ByRef)+0x31
    0020EC3C 68E56FB6 System_Windows_Forms_ni!System.Windows.Forms.NativeWindow.Callback(IntPtr, Int32, IntPtr,
IntPtr)+0x96
```

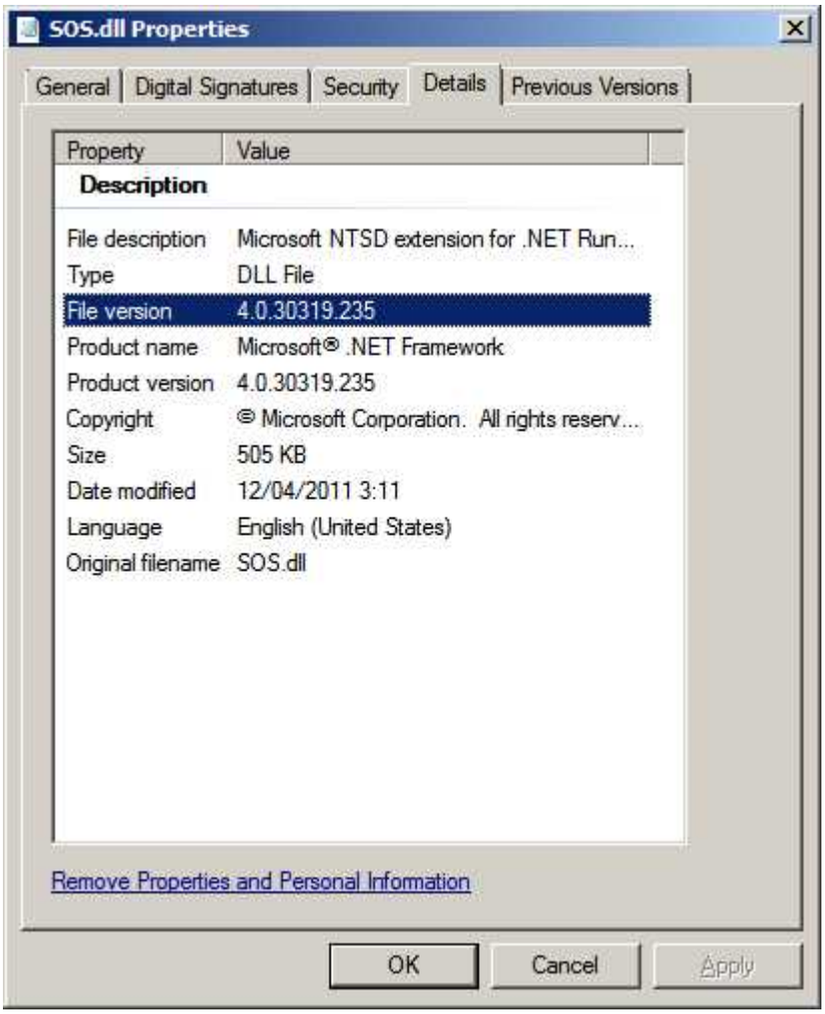
```
StackTraceString: <none>
HResult: 80004003
The version of SOS does not match the version of CLR you are debugging.  Please
load the matching version of SOS for the version of CLR you are debugging.
CLR Version: 4.0.30319.1
SOS Version: 4.0.30319.235
The current thread is unmanaged
The version of SOS does not match the version of CLR you are debugging.  Please
load the matching version of SOS for the version of CLR you are debugging.
CLR Version: 4.0.30319.1
SOS Version: 4.0.30319.235
There is no current managed exception on this thread
The version of SOS does not match the version of CLR you are debugging.  Please
load the matching version of SOS for the version of CLR you are debugging.
CLR Version: 4.0.30319.1
SOS Version: 4.0.30319.235
The current thread is unmanaged
```

Note: We see that the other managed thread (#2) doesn't have managed exceptions (threads #1 and #3 are unmanaged). We also see lots of warnings about SOS mismatch. So we try to load and use the correct SOS extension like we did in the previous exercise (PN1).

9. We check the version of .NET used when ApplicationA was running:

```
0:000> lmv m clr
start    end        module name
6ce40000 6d4af000   clr        (pdb symbols)
c:\mss\clr.pdb\C58C9AF63E5D49A8BE0DBA9C5E0093BE2\clr.pdb
    Loaded symbol image file: clr.dll
    Image path: C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.dll
    Image name: clr.dll
    Timestamp:        Thu Mar 18 07:44:47 2010 (4BA1D9EF)
    CheckSum:         00671FC0
    ImageSize:        0066F000
    File version:     4.0.30319.1
    Product version:  4.0.30319.1
    File flags:       8 (Mask 3F) Private
    File OS:          4 Unknown Win32
    File type:        2.0 Dll
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      Microsoft Corporation
    ProductName:      Microsoft® .NET Framework
    InternalName:     clr.dll
    OriginalFilename: clr.dll
    ProductVersion:   4.0.30319.1
    FileVersion:      4.0.30319.1 (RTMRel.030319-0100)
    PrivateBuild:     DDBLD766
    FileDescription:  Microsoft .NET Runtime Common Language Runtime - WorkStation
    LegalCopyright:   © Microsoft Corporation.  All rights reserved.
    Comments:         Flavor=Retail
```

Note: On my analysis system the version is slightly different (C:\Windows\Microsoft.NET\Framework\4.0.30319.235):



It has a different **.235** version suffix. The version can also be checked by listing all loaded WinDbg extensions (sos.dll is used for .NET analysis):

```
0:000> .chain
Extension DLL search Path:
[...]
Extension DLL chain:
    C:\Windows\Microsoft.NET\Framework\v4.0.30319\sos: image 4.0.30319.235, API 1.0.0, built
Tue Apr 12 08:47:32 2011
        [path: C:\Windows\Microsoft.NET\Framework\v4.0.30319\sos.dll]
    dbghelp: image 6.12.0002.633, API 6.1.6, built Mon Feb 01 20:08:26 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\dbghelp.dll]
    ext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:31 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\winext\ext.dll]
    exts: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:24 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\WINXP\exts.dll]
    uext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:23 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\winext\uext.dll]
    ntsdexts: image 6.1.7650.0, API 1.0.0, built Mon Feb 01 20:08:08 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\WINXP\ntsdexts.dll]
```

10. In the folder C:\ANETMDA-Dumps\32-bit\Microsoft.NET\Framework\v4.0.30319 we have the correct version **.1** of .NET Framework copied from the machine the memory dump came from. So we unload the current SOS extension (**.unload** command) and load the new one (**.load** command):

```
0:000> .unload C:\Windows\Microsoft.NET\Framework\v4.0.30319\sos
Unloading C:\Windows\Microsoft.NET\Framework\v4.0.30319\sos extension DLL

0:000> .chain
Extension DLL search Path:
[...]
Extension DLL chain:
    dbghelp: image 6.12.0002.633, API 6.1.6, built Mon Feb 01 20:08:26 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\dbghelp.dll]
    ext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:31 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\winext\ext.dll]
    exts: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:24 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\WINXP\exts.dll]
    uext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:23 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\winext\uext.dll]
    ntsdexts: image 6.1.7650.0, API 1.0.0, built Mon Feb 01 20:08:08 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\WINXP\ntsdexts.dll]

0:000> .load C:\ANETMDA-Dumps\32-bit\Microsoft.NET\Framework\v4.0.30319\sos

0:000> .chain
Extension DLL search Path:
[...]
Extension DLL chain:
    C:\ANETMDA-Dumps\32-bit\Microsoft.NET\Framework\v4.0.30319\sos: image 4.0.30319.1, API
1.0.0, built Thu Mar 18 08:09:41 2010
        [path: C:\ANETMDA-Dumps\32-bit\Microsoft.NET\Framework\v4.0.30319\sos.dll]
    dbghelp: image 6.12.0002.633, API 6.1.6, built Mon Feb 01 20:08:26 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\dbghelp.dll]
    ext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:31 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\winext\ext.dll]
    exts: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:24 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\WINXP\exts.dll]
    uext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:23 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\winext\uext.dll]
    ntsdexts: image 6.1.7650.0, API 1.0.0, built Mon Feb 01 20:08:08 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\WINXP\ntsdexts.dll]
```

11. We now retry **!pe** command to make sure the extension works:

```
0:000> !pe
Exception object: 01467f44
Exception type:   System.NullReferenceException
Message:          Object reference not set to an instance of an object.
InnerException:   <none>
StackTrace (generated):
    SP       IP       Function
    0020EA90 002D0250 ApplicationA!ApplicationA.Form1.button1_Click_1(System.Object, System.EventArgs)
    0020EA98 68E04AE8 System_Windows_Forms_ni!System.Windows.Forms.Control.OnClick(System.EventArgs)+0x70
    0020EAB0 68E070A2 System_Windows_Forms_ni!System.Windows.Forms.Button.OnClick(System.EventArgs)+0xa2
    0020EAC8 69396174
System_Windows_Forms_ni!System.Windows.Forms.Button.OnMouseUp(System.Windows.Forms.MouseEventArgs)+0xac
    0020EAE4 693695B5 System_Windows_Forms_ni!System.Windows.Forms.Control.WmMouseUp(System.Windows.Forms.Message
ByRef, System.Windows.Forms.MouseButtons, Int32)+0x2d1
    0020EB78 6972A1BF System_Windows_Forms_ni!System.Windows.Forms.Control.WndProc(System.Windows.Forms.Message
ByRef)+0x8d30bf
    0020EBD0 697318DD System_Windows_Forms_ni!System.Windows.Forms.ButtonBase.WndProc(System.Windows.Forms.Message
ByRef)+0x8c3ac1
    0020EC14 68E6DE00 System_Windows_Forms_ni!System.Windows.Forms.Button.WndProc(System.Windows.Forms.Message
ByRef)+0x20
```

```
    0020EC20 68E570F3
System_Windows_Forms_ni!System.Windows.Forms.Control+ControlNativeWindow.OnMessage(System.Windows.Forms.Message
ByRef)+0x13
    0020EC28 68E57071
System_Windows_Forms_ni!System.Windows.Forms.Control+ControlNativeWindow.WndProc(System.Windows.Forms.Message
ByRef)+0x31
    0020EC3C 68E56FB6 System_Windows_Forms_ni!System.Windows.Forms.NativeWindow.Callback(IntPtr, Int32, IntPtr,
IntPtr)+0x96

StackTraceString: <none>
HResult: 80004003
```

Note: We see now that mismatch warnings have disappeared.

12. Now we examine the first thread unmanaged stack trace:

```
0:000> k
ChildEBP RetAddr
0020da78 7720b5b4 ntdll!KiFastSystemCallRet
0020da7c 68e6737a user32!NtUserWaitMessage+0xc
0020db10 68e66e2c System_Windows_Forms_ni+0x22737a
0020db6c 68e66c81 System_Windows_Forms_ni+0x226e2c
0020db9c 6935fefb System_Windows_Forms_ni+0x226c81
0020dbb4 69389f83 System_Windows_Forms_ni+0x71fefb
0020dc50 6938a1b7 System_Windows_Forms_ni+0x749f83
0020dc90 69369866 System_Windows_Forms_ni+0x74a1b7
0020dc9c 6936ff9c System_Windows_Forms_ni+0x729866
0020ecb0 764a2459 System_Windows_Forms_ni+0x72ff9c
0020ecbc 77211a10 msctf!TF_Notify+0x239
0020ece8 77211ae8 user32!InternalCallWinProc+0x23
0020ed60 77212a47 user32!UserCallWinProcCheckWow+0x14b
0020edc4 77212a98 user32!DispatchMessageWorker+0x322
0020edd4 68e72eec user32!DispatchMessageW+0xf
0020ee20 68e671ff System_Windows_Forms_ni+0x232eec
0020eeb4 68e66e2c System_Windows_Forms_ni+0x2271ff
0020ef10 68e66c81 System_Windows_Forms_ni+0x226e2c
0020ef40 68df366d System_Windows_Forms_ni+0x226c81
0020ef64 6ce421db System_Windows_Forms_ni+0x1b366d
0020ef6c 6ce4e021 clr!CallDescrWorker+0x33
0020ef84 00000000 clr!SigParser::GetElemType+0x28
```

Note: The stack trace appears truncated. Using **.kframes** command doesn't help, and we still have incorrect stack trace (we don't see expected *kernel32!BaseThreadInitThunk* and *ntdll!_RtlUserThreadStart* at the bottom):

```
0:000> .kframes 100
Default stack trace depth is 0n256 frames
```

```
0:000> kc

ntdll!KiFastSystemCallRet
user32!NtUserWaitMessage
System_Windows_Forms_ni
System_Windows_Forms_ni
System_Windows_Forms_ni
System_Windows_Forms_ni
System_Windows_Forms_ni
System_Windows_Forms_ni
System_Windows_Forms_ni
System_Windows_Forms_ni
msctf!TF_Notify
user32!InternalCallWinProc
user32!UserCallWinProcCheckWow
user32!DispatchMessageWorker
user32!DispatchMessageW
System_Windows_Forms_ni
System_Windows_Forms_ni
System_Windows_Forms_ni
System_Windows_Forms_ni
System_Windows_Forms_ni
clr!CallDescrWorker
clr!SigParser::GetElemType
```

13. We now try to manually reconstruct the bottom of the stack trace by using **k L=**<*address*> command variant and try it with different EBP values saved on the stack. First, we dump raw stack area with symbols using **dps** command and specify the last ChildEBP value from the stack trace above.

```
0:000> dps 0020ef84
0020ef84  0020f010
0020ef88  00000000
0020ef8c  0029c020
0020ef90  0020efe0
0020ef94  6ceccc44 clr!COMPlusFrameHandler
0020ef98  0020f19c
0020ef9c  fc557a96
0020efa0  0020f1c0
0020efa4  0020f030
0020efa8  00000000
0020efac  00000001
0020efb0  0020f19c
0020efb4  003ebde8
0020efb8  00000000
0020efbc  00000000
0020efc0  00000000
0020efc4  00000000
0020efc8  00000000
0020efcc  6ce5c58d clr!ArgIterator::Init+0x6b
0020efd0  0020ef90
0020efd4  fc557a96
0020efd8  0020ef90
```

```
0020efdc  0020effc
0020efe0  0020f2bc
0020efe4  6cf11498 clr!_except_handler4
0020efe8  9093df0e
0020efec  00000000
0020eff0  0020f134
0020eff4  6ce64bcc clr!MethodDesc::CallDescr+0x194
0020eff8  0020f040
0020effc  00000000
0020f000  0020f010
```

Next, we try every address of supposedly saved EBP (non-zero):

```
Address   Saved EBP
Address+4 Saved Return Address Module!Function+Offset

0:000> dps 0020ef84
0020ef84  0020f010
0020ef88  00000000
0020ef8c  0029c020
0020ef90  0020efe0
0020ef94  6ceccc44 clr!COMPlusFrameHandler
0020ef98  0020f19c
0020ef9c  fc557a96
0020efa0  0020f1c0
0020efa4  0020f030
0020efa8  00000000
0020efac  00000001
0020efb0  0020f19c
0020efb4  003ebde8
0020efb8  00000000
0020efbc  00000000
0020efc0  00000000
0020efc4  00000000
0020efc8  00000000
0020efcc  6ce5c58d clr!ArgIterator::Init+0x6b
0020efd0  0020ef90
0020efd4  fc557a96
0020efd8  0020ef90
0020efdc  0020effc
0020efe0  0020f2bc
0020efe4  6cf11498 clr!_except_handler4
0020efe8  9093df0e
0020efec  00000000
0020eff0  0020f134
0020eff4  6ce64bcc clr!MethodDesc::CallDescr+0x194
0020eff8  0020f040
0020effc  00000000
0020f000  0020f010
```

```
0:000> k L=0020ef90
ChildEBP RetAddr
0020da78 7720b5b4 ntdll!KiFastSystemCallRet
0020da7c 68e6737a user32!NtUserWaitMessage+0xc
0020efc8 6ce5c58d System_Windows_Forms_ni+0x22737a
0020efe0 6cf11497 clr!ArgIterator::Init+0x6b
0020f2cc 6cf2cf90 clr!__safe_se_handler_table+0x4407
0020f528 6d341ab4 clr!Assembly::ExecuteMainMethod+0xc1
0020fa18 6cf2d199 clr! ?? ::FNODOBFM::`string'+0xd400
0020fa5c 6cf11497 clr!ExecuteEXE+0x58
0020fab8 6cfaaf00 clr!__safe_se_handler_table+0x4407
0020fae0 6cf11497 clr!_CorExeMain+0x4e
0020fb50 77b48bf1 clr!__safe_se_handler_table+0x4407
0020fb60 00000000 ntdll!RtlLockMemoryZone+0x99

0:000> k L=0020efe0
ChildEBP RetAddr
0020da78 7720b5b4 ntdll!KiFastSystemCallRet
0020da7c 68e6737a user32!NtUserWaitMessage+0xc
0020eff0 6ce64bcc System_Windows_Forms_ni+0x22737a
0020f2bc 6cf11497 clr!MethodDesc::CallDescr+0x194
0020f534 6cf2cda4 clr!__safe_se_handler_table+0x4407
0020fa0c 6d33f632 clr!SystemDomain::ExecuteMainMethod+0x4ec
0020fa6c 6cf2d09a clr! ?? ::FNODOBFM::`string'+0xb930
0020faac 6d330354 clr!_CorExeMainInternal+0x19f
0020faf0 6e1e55ab clr! ?? ::FNODOBFM::`string'+0xa64
0020fb50 77b48bf1 mscoreei!_CorExeMain+0x38
0020fb60 00000000 ntdll!RtlLockMemoryZone+0x99

0:000> k L=0020eff0
ChildEBP RetAddr
0020da78 7720b5b4 ntdll!KiFastSystemCallRet
0020da7c 68e6737a user32!NtUserWaitMessage+0xc
0020eff0 6ce64bcc System_Windows_Forms_ni+0x22737a
0020f134 6ce64c01 clr!MethodDesc::CallDescr+0x194
0020f150 6ce64c21 clr!MethodDesc::CallTargetWorker+0x21
0020f168 6cf2ce82 clr!MethodDescCallSite::Call+0x1c
0020f2cc 6cf2cf90 clr!ClassLoader::RunMain+0x24c
0020f534 6cf2cda4 clr!Assembly::ExecuteMainMethod+0xc1
0020fa18 6cf2d199 clr!SystemDomain::ExecuteMainMethod+0x4ec
0020fa6c 6cf2d09a clr!ExecuteEXE+0x58
0020fab8 6cfaaf00 clr!_CorExeMainInternal+0x19f
0020faf0 6e1e55ab clr!_CorExeMain+0x4e
0020fafc 6e187f16 mscoreei!_CorExeMain+0x38
0020fb0c 6e184de3 mscoree!ShellShim__CorExeMain+0x99
0020fb14 77563833 mscoree!_CorExeMain_Exported+0x8
0020fb20 77b7a9bd kernel32!BaseThreadInitThunk+0xe
0020fb60 00000000 ntdll!_RtlUserThreadStart+0x23
```

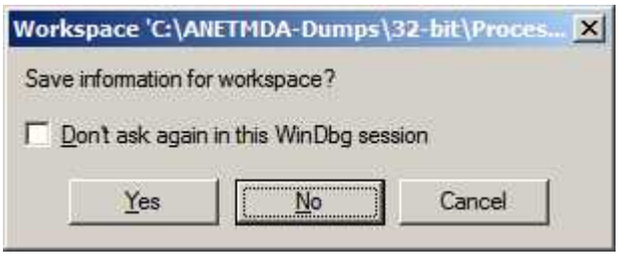
Note: Only the 3rd address appears to be good. The following article explains stack trace reconstruction on x86 systems:

http://www.dumpanalysis.org/blog/index.php/2007/07/25/reconstructing-stack-trace-manually/

14. We close logging before exiting WinDbg:

```
0:000> .logclose
Closing open log file C:\ANETMDA-Dumps\32-bit\Processes\CLR4\ApplicationA.log
```

If presented with this dialog choose No:



Note: To avoid possible confusion and glitches we recommend to exit WinDbg after each exercise.

Exercise PN3

- **Goal:** Learn how to find problem assemblies, modules, classes and methods, disassemble code, analyze CPU spikes
- **Patterns:** Stack Trace Collection; CLR Thread; Version-Specific Extension; Duplicate Extension; JIT Code; Spiking Thread; Annotated Disassembly
- **Commands:** !analyze -v -hang, !CLRStack, !IP2MD, !runaway, ~<>s, ~<>k, !U, !DumpMD, !DumpClass, !DumpMT, !DumpModule, !DumpAssembly, !DumpDomain
- \ANETMDA-Dumps\Exercise-PN3-Analysis-process-dump-LINQPadB-32-CLR2.pdf

© 2013 Software Diagnostics Services

Exercise PN3: Analysis of an application process dump (LINQPadB, 32-bit, CLR 2)

Goal: Learn how to find problem assemblies, modules, classes and methods, disassemble code, analyze CPU spikes.

Patterns: Stack Trace Collection; CLR Thread; Version-Specific Extension; Duplicate Extension; JIT Code; Spiking Thread; Annotated Disassembly.

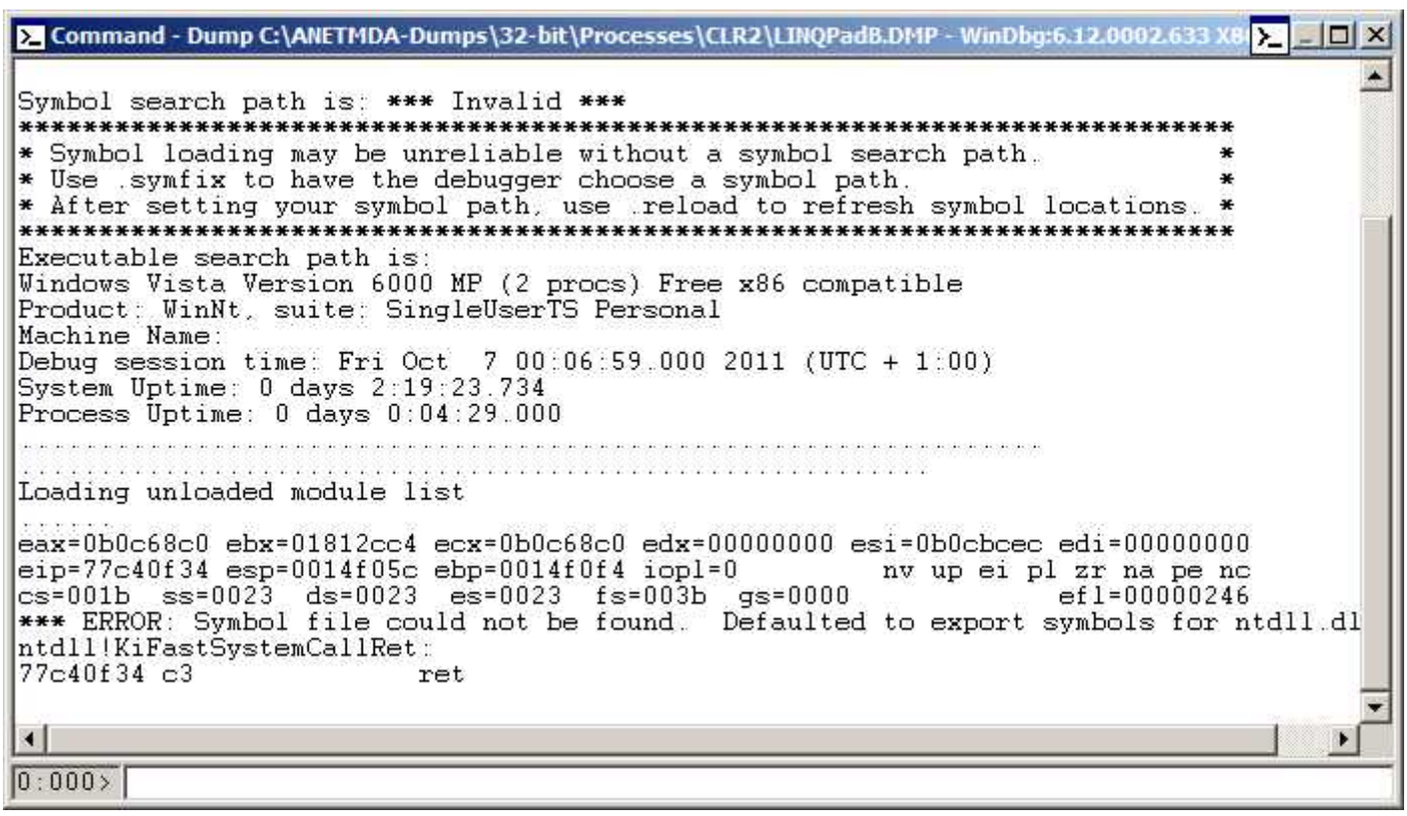
Commands: !anayze -v -hang, !CLRStack, !IP2MD, !runaway, ~<>s, ~<>k, !U, !DumpMD, !DumpClass, !DumpMT, !DumpModule, !DumpAssembly, !DumpDomain

1. Launch WinDbg from Debugging Tools for Windows or Debugging Tools for Windows (x86)

2. Open \ANETMDA-Dumps\32-bit\Processes\CLR2\LINQPadB.DMP

3. If you are presented with this dialog say No:

4. We get the dump file loaded:



5. Open a log file using **.logopen** command and load symbols (**.symfix** and **.reload** commands):

```
0:000> .logopen C:\ANETMDA-Dumps\32-bit\Processes\CLR2\LINQPadB.log
Opened log file 'C:\ANETMDA-Dumps\32-bit\Processes\CLR2\LINQPadB.log'

0:000> .symfix c:\mss

0:000> .reload
.........................
```

Note: The results may be slightly different on your system if you have 32-bit .NET Framework 2.0.50727.**1433** already installed or you don't have any .NET Framework 2.0.50727 installed.

6. Type ~***k** command to verify the correctness of all stack traces:

```
0:000> ~*k

.  0  Id: f60.ea0 Suspend: 0 Teb: 7ffdf000 Unfrozen
ChildEBP RetAddr
0014f058 7674b5b4 ntdll!KiFastSystemCallRet
*** WARNING: Unable to verify checksum for System.Windows.Forms.ni.dll
0014f05c 7b08374f user32!NtUserWaitMessage+0xc
0014f0f4 7b0831a5 System_Windows_Forms_ni+0xb374f
0014f170 7b082fe3 System_Windows_Forms_ni+0xb31a5
0014f1a0 7b0692c2 System_Windows_Forms_ni+0xb2fe3
0014f1f8 007c11dc System_Windows_Forms_ni+0x992c2
WARNING: Frame IP not in any known module. Following frames may be wrong.
0014f3b0 79e7c74b 0x7c11dc
0014f3c0 79e7c6cc mscorwks!CallDescrWorker+0x33
0014f440 79e7c8e1 mscorwks!CallDescrWorkerWithHandler+0xa3
0014f584 79e7c783 mscorwks!MethodDesc::CallDescr+0x19c
0014f5a0 79e7c90d mscorwks!MethodDesc::CallTargetWorker+0x1f
0014f5b4 79eefb9e mscorwks!MethodDescCallSite::Call_RetArgSlot+0x18
0014f718 79eef830 mscorwks!ClassLoader::RunMain+0x263
0014f980 79ef01da mscorwks!Assembly::ExecuteMainMethod+0xa6
0014fe50 79fb9793 mscorwks!SystemDomain::ExecuteMainMethod+0x43f
0014fea0 79fb96df mscorwks!ExecuteEXE+0x59
0014fee8 736455ab mscorwks!_CorExeMain+0x15c
0014fef4 73747f16 mscoreei!_CorExeMain+0x38
0014ff04 73744de3 mscoree!ShellShim__CorExeMain+0x99
0014ff0c 76573833 mscoree!_CorExeMain_Exported+0x8
0014ff18 77c1a9bd kernel32!BaseThreadInitThunk+0xe
0014ff58 00000000 ntdll!_RtlUserThreadStart+0x23

   1  Id: f60.e84 Suspend: 0 Teb: 7ffdd000 Unfrozen
ChildEBP RetAddr
0180f648 77c40690 ntdll!KiFastSystemCallRet
0180f64c 76577e09 ntdll!ZwWaitForMultipleObjects+0xc
0180f6e8 76578150 kernel32!WaitForMultipleObjectsEx+0x11d
0180f704 79f4e8d8 kernel32!WaitForMultipleObjects+0x18
0180f764 79f4e831 mscorwks!DebuggerRCThread::MainLoop+0xe9
0180f794 79f4e765 mscorwks!DebuggerRCThread::ThreadProc+0xe5
0180f7c4 76573833 mscorwks!DebuggerRCThread::ThreadProcStatic+0x9c
0180f7d0 77c1a9bd kernel32!BaseThreadInitThunk+0xe
0180f810 00000000 ntdll!_RtlUserThreadStart+0x23
```

```
   2  Id: f60.1bc Suspend: 0 Teb: 7ffdc000 Unfrozen
ChildEBP RetAddr
0393f5c0 77c40690 ntdll!KiFastSystemCallRet
0393f5c4 76577e09 ntdll!ZwWaitForMultipleObjects+0xc
0393f660 76578150 kernel32!WaitForMultipleObjectsEx+0x11d
0393f67c 79ef224b kernel32!WaitForMultipleObjects+0x18
0393f69c 79fb997b mscorwks!WKS::WaitForFinalizerEvent+0x77
0393f6b0 79ef3207 mscorwks!WKS::GCHeap::FinalizerThreadWorker+0x79
0393f6c4 79ef31a3 mscorwks!Thread::DoADCallBack+0x32a
0393f758 79ef30c3 mscorwks!Thread::ShouldChangeAbortToUnload+0xe3
0393f794 79fb9643 mscorwks!Thread::ShouldChangeAbortToUnload+0x30a
0393f7bc 79fb960d mscorwks!ManagedThreadBase_NoADTransition+0x32
0393f7cc 79fba09b mscorwks!ManagedThreadBase::FinalizerBase+0xd
0393f804 79f95a2e mscorwks!WKS::GCHeap::FinalizerThreadStart+0xbb
0393f8a4 76573833 mscorwks!Thread::intermediateThreadProc+0x49
0393f8b0 77c1a9bd kernel32!BaseThreadInitThunk+0xe
0393f8f0 00000000 ntdll!_RtlUserThreadStart+0x23

   3  Id: f60.cc8 Suspend: 0 Teb: 7ffdb000 Unfrozen
ChildEBP RetAddr
044af458 77c3f9c0 ntdll!KiFastSystemCallRet
044af45c 7653f00d ntdll!NtFsControlFile+0xc
044af4a0 0025b432 kernel32!ConnectNamedPipe+0x52
*** WARNING: Unable to verify checksum for System.Core.ni.dll
WARNING: Frame IP not in any known module. Following frames may be wrong.
044af4cc 6c2033d0 0x25b432
*** WARNING: Unable to verify checksum for mscorlib.ni.dll
044af53c 793b0d1f System_Core_ni+0x733d0
044af544 79373ecd mscorlib_ni+0x2f0d1f
044af558 793b0c68 mscorlib_ni+0x2b3ecd
044af570 79e7c74b mscorlib_ni+0x2f0c68
044af580 79e7c6cc mscorwks!CallDescrWorker+0x33
044af600 79e7c8e1 mscorwks!CallDescrWorkerWithHandler+0xa3
044af73c 79e7c783 mscorwks!MethodDesc::CallDescr+0x19c
044af758 79e7c90d mscorwks!MethodDesc::CallTargetWorker+0x1f
044af76c 79fc58cd mscorwks!MethodDescCallSite::Call_RetArgSlot+0x18
044af954 79ef3207 mscorwks!ThreadNative::KickOffThread_Worker+0x190
044af968 79ef31a3 mscorwks!Thread::DoADCallBack+0x32a
044af9fc 79ef30c3 mscorwks!Thread::ShouldChangeAbortToUnload+0xe3
044afa38 79ef4826 mscorwks!Thread::ShouldChangeAbortToUnload+0x30a
044afa60 79fc57b1 mscorwks!Thread::ShouldChangeAbortToUnload+0x33e
044afa78 79fc56ac mscorwks!ManagedThreadBase::KickOff+0x13
044afb14 79f95a2e mscorwks!ThreadNative::KickOffThread+0x269
044afc2c 76573833 mscorwks!Thread::intermediateThreadProc+0x49
044afc38 77c1a9bd kernel32!BaseThreadInitThunk+0xe
044afc78 00000000 ntdll!_RtlUserThreadStart+0x23

   4  Id: f60.a14 Suspend: 0 Teb: 7ffda000 Unfrozen
ChildEBP RetAddr
046bf73c 77c40690 ntdll!KiFastSystemCallRet
046bf740 76577e09 ntdll!ZwWaitForMultipleObjects+0xc
046bf7dc 7674c4af kernel32!WaitForMultipleObjectsEx+0x11d
046bf830 76748b7b user32!RealMsgWaitForMultipleObjectsEx+0x13c
046bf84c 74d01965 user32!MsgWaitForMultipleObjects+0x1f
046bf898 76573833 GdiPlus!BackgroundThreadProc+0x59
046bf8a4 77c1a9bd kernel32!BaseThreadInitThunk+0xe
046bf8e4 00000000 ntdll!_RtlUserThreadStart+0x23
```

```
   5  Id: f60.8d4 Suspend: 0 Teb: 7ffd6000 Unfrozen
ChildEBP RetAddr
058ef940 77c406a0 ntdll!KiFastSystemCallRet
058ef944 765777d4 ntdll!NtWaitForSingleObject+0xc
058ef9b4 776dfc38 kernel32!WaitForSingleObjectEx+0xbe
058ef9d8 776dfc73 ole32!CRpcThread::WorkerLoop+0xc0
058ef9e4 76573833 ole32!CRpcThreadCache::RpcWorkerThreadEntry+0x20
058ef9f0 77c1a9bd kernel32!BaseThreadInitThunk+0xe
058efa30 00000000 ntdll!_RtlUserThreadStart+0x23

   6  Id: f60.bb8 Suspend: 0 Teb: 7ffd5000 Unfrozen
ChildEBP RetAddr
056cec80 77c40690 ntdll!KiFastSystemCallRet
056cec84 76577e09 ntdll!ZwWaitForMultipleObjects+0xc
056ced20 79ed98fd kernel32!WaitForMultipleObjectsEx+0x11d
056ced88 79ed9889 mscorwks!WaitForMultipleObjectsEx_SO_TOLERANT+0x6f
056ceda8 79ed9808 mscorwks!Thread::DoAppropriateAptStateWait+0x3c
056cee2c 79ed96c4 mscorwks!Thread::DoAppropriateWaitWorker+0x13c
056cee7c 79ed9a62 mscorwks!Thread::DoAppropriateWait+0x40
056ceed8 79e78944 mscorwks!CLREvent::WaitEx+0xf7
056ceeec 79fc6aa9 mscorwks!CLREvent::Wait+0x17
056cef00 79fc6a84 mscorwks!Thread::Wait+0x1b
056cef14 79fc6a33 mscorwks!Thread::Block+0x18
056cefa0 79fc6947 mscorwks!SyncBlock::Wait+0x12e
056cefb4 79fc68d4 mscorwks!ObjHeader::Wait+0x2a
056cf064 794050e2 mscorwks!ObjectNative::WaitTimeout+0xe6
056cf0fc 793b0d1f mscorlib_ni+0x3450e2
056cf104 79373ecd mscorlib_ni+0x2f0d1f
056cf118 793b0c68 mscorlib_ni+0x2b3ecd
056cf130 79e7c74b mscorlib_ni+0x2f0c68
056cf140 79e7c6cc mscorwks!CallDescrWorker+0x33
056cf1c0 79e7c8e1 mscorwks!CallDescrWorkerWithHandler+0xa3
056cf2fc 79e7c783 mscorwks!MethodDesc::CallDescr+0x19c
056cf318 79e7c90d mscorwks!MethodDesc::CallTargetWorker+0x1f
056cf32c 79fc58cd mscorwks!MethodDescCallSite::Call_RetArgSlot+0x18
056cf514 79ef3207 mscorwks!ThreadNative::KickOffThread_Worker+0x190
056cf528 79ef31a3 mscorwks!Thread::DoADCallBack+0x32a
056cf5bc 79ef30c3 mscorwks!Thread::ShouldChangeAbortToUnload+0xe3
056cf5f8 79ef4826 mscorwks!Thread::ShouldChangeAbortToUnload+0x30a
056cf620 79fc57b1 mscorwks!Thread::ShouldChangeAbortToUnload+0x33e
056cf638 79fc56ac mscorwks!ManagedThreadBase::KickOff+0x13
056cf6d4 79f95a2e mscorwks!ThreadNative::KickOffThread+0x269
056cf9f0 76573833 mscorwks!Thread::intermediateThreadProc+0x49
056cf9fc 77c1a9bd kernel32!BaseThreadInitThunk+0xe
056cfa3c 00000000 ntdll!_RtlUserThreadStart+0x23

   7  Id: f60.c38 Suspend: 0 Teb: 7ffd9000 Unfrozen
ChildEBP RetAddr
0639ead4 77c40690 ntdll!KiFastSystemCallRet
0639ead8 76577e09 ntdll!ZwWaitForMultipleObjects+0xc
0639eb74 79ed98fd kernel32!WaitForMultipleObjectsEx+0x11d
0639ebdc 79ed9889 mscorwks!WaitForMultipleObjectsEx_SO_TOLERANT+0x6f
0639ebfc 79ed9808 mscorwks!Thread::DoAppropriateAptStateWait+0x3c
0639ec80 79ed96c4 mscorwks!Thread::DoAppropriateWaitWorker+0x13c
0639ecd0 79fcfc58 mscorwks!Thread::DoAppropriateWait+0x40
0639edd4 793b03fe mscorwks!WaitHandleNative::CorWaitOneNative+0x156
0639ee3c 793b0d1f mscorlib_ni+0x2f03fe
0639ee44 79373ecd mscorlib_ni+0x2f0d1f
0639ee58 793b0c68 mscorlib_ni+0x2b3ecd
0639ee70 79e7c74b mscorlib_ni+0x2f0c68
```

```
0639ee80 79e7c6cc mscorwks!CallDescrWorker+0x33
0639ef00 79e7c8e1 mscorwks!CallDescrWorkerWithHandler+0xa3
0639f03c 79e7c783 mscorwks!MethodDesc::CallDescr+0x19c
0639f058 79e7c90d mscorwks!MethodDesc::CallTargetWorker+0x1f
0639f06c 79fc58cd mscorwks!MethodDescCallSite::Call_RetArgSlot+0x18
0639f254 79ef3207 mscorwks!ThreadNative::KickOffThread_Worker+0x190
0639f268 79ef31a3 mscorwks!Thread::DoADCallBack+0x32a
0639f2fc 79ef30c3 mscorwks!Thread::ShouldChangeAbortToUnload+0xe3
0639f338 79ef4826 mscorwks!Thread::ShouldChangeAbortToUnload+0x30a
0639f360 79fc57b1 mscorwks!Thread::ShouldChangeAbortToUnload+0x33e
0639f378 79fc56ac mscorwks!ManagedThreadBase::KickOff+0x13
0639f414 79f95a2e mscorwks!ThreadNative::KickOffThread+0x269
0639f7b0 76573833 mscorwks!Thread::intermediateThreadProc+0x49
0639f7bc 77c1a9bd kernel32!BaseThreadInitThunk+0xe
0639f7fc 00000000 ntdll!_RtlUserThreadStart+0x23

   8  Id: f60.9e8 Suspend: 0 Teb: 7ffd7000 Unfrozen
ChildEBP RetAddr
064af31c 77c406a0 ntdll!KiFastSystemCallRet
064af320 765777d4 ntdll!NtWaitForSingleObject+0xc
064af390 79e789c6 kernel32!WaitForSingleObjectEx+0xbe
064af3d4 79e7898f mscorwks!PEImage::LoadImage+0x1af
064af424 79e78944 mscorwks!CLREvent::WaitEx+0x117
064af438 79f0b1e7 mscorwks!CLREvent::Wait+0x17
064af504 79f95a2e mscorwks!AppDomain::ADUnloadThreadStart+0x308
064af920 76573833 mscorwks!Thread::intermediateThreadProc+0x49
064af92c 77c1a9bd kernel32!BaseThreadInitThunk+0xe
064af96c 00000000 ntdll!_RtlUserThreadStart+0x23

   9  Id: f60.134 Suspend: 0 Teb: 7ffd3000 Unfrozen
ChildEBP RetAddr
0783f864 77c400f0 ntdll!KiFastSystemCallRet
0783f868 76557948 ntdll!NtRemoveIoCompletion+0xc
0783f894 79f02f04 kernel32!GetQueuedCompletionStatus+0x29
0783f904 79f95a2e mscorwks!ThreadpoolMgr::CompletionPortThreadStart+0x141
0783fd9c 76573833 mscorwks!Thread::intermediateThreadProc+0x49
0783fda8 77c1a9bd kernel32!BaseThreadInitThunk+0xe
0783fde8 00000000 ntdll!_RtlUserThreadStart+0x23

  10  Id: f60.8f4 Suspend: 0 Teb: 7ff4d000 Unfrozen
ChildEBP RetAddr
0794f6d8 77c400f0 ntdll!KiFastSystemCallRet
0794f6dc 76557948 ntdll!NtRemoveIoCompletion+0xc
0794f708 7665af2e kernel32!GetQueuedCompletionStatus+0x29
0794f744 7665b067 rpcrt4!COMMON_ProcessCalls+0xb5
0794f7b0 7665ac4f rpcrt4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
0794f7bc 7665acb9 rpcrt4!ProcessIOEventsWrapper+0xe
0794f7e0 7665ad03 rpcrt4!BaseCachedThreadRoutine+0x5c
0794f7ec 76573833 rpcrt4!ThreadStartRoutine+0x1e
0794f7f8 77c1a9bd kernel32!BaseThreadInitThunk+0xe
0794f838 00000000 ntdll!_RtlUserThreadStart+0x23

  11  Id: f60.334 Suspend: 0 Teb: 7ff4c000 Unfrozen
ChildEBP RetAddr
097df8dc 77c406a0 ntdll!KiFastSystemCallRet
097df8e0 765777d4 ntdll!NtWaitForSingleObject+0xc
097df950 76577742 kernel32!WaitForSingleObjectEx+0xbe
097df964 6d01f57d kernel32!WaitForSingleObject+0x12
097df97c 6d016c92 mshtml!CDwnTaskExec::ThreadExec+0x127
097df988 6cf9dadc mshtml!CExecFT::ThreadProc+0x3c
```

```
097df990 76573833 mshtml!CExecFT::StaticThreadProc+0xd
097df99c 77c1a9bd kernel32!BaseThreadInitThunk+0xe
097df9dc 00000000 ntdll!_RtlUserThreadStart+0x23

  12  Id: f60.cf8 Suspend: 0 Teb: 7ff4a000 Unfrozen
ChildEBP RetAddr
WARNING: Frame IP not in any known module. Following frames may be wrong.
0a0ae5d0 79e7c6cc 0x7562074
0a0ae650 79e7c8e1 mscorwks!CallDescrWorkerWithHandler+0xa3
0a0ae78c 79e7c783 mscorwks!MethodDesc::CallDescr+0x19c
0a0ae7a8 79e7c90d mscorwks!MethodDesc::CallTargetWorker+0x1f
0a0ae7bc 79f321b6 mscorwks!MethodDescCallSite::Call_RetArgSlot+0x18
0a0ae9a8 79f31eaf mscorwks!InvokeImpl+0x559
0a0aea68 793a44bd mscorwks!RuntimeMethodHandle::InvokeMethodFast+0xbd
0a0aeab4 793a41e5 mscorlib_ni+0x2e44bd
00000000 00000000 mscorlib_ni+0x2e41e5

  13  Id: f60.1cc Suspend: 0 Teb: 7ff4b000 Unfrozen
ChildEBP RetAddr
09adf1f4 77c406a0 ntdll!KiFastSystemCallRet
09adf1f8 765777d4 ntdll!NtWaitForSingleObject+0xc
09adf268 79e789c6 kernel32!WaitForSingleObjectEx+0xbe
09adf2ac 79e7898f mscorwks!PEImage::LoadImage+0x1af
09adf2fc 79e78944 mscorwks!CLREvent::WaitEx+0x117
09adf310 79f014ef mscorwks!CLREvent::Wait+0x17
09adf390 79f02143 mscorwks!ThreadpoolMgr::SafeWait+0x73
09adf3f4 79f95a2e mscorwks!ThreadpoolMgr::WorkerThreadStart+0x11c
09adfa8c 76573833 mscorwks!Thread::intermediateThreadProc+0x49
09adfa98 77c1a9bd kernel32!BaseThreadInitThunk+0xe
09adfad8 00000000 ntdll!_RtlUserThreadStart+0x23
```

Note: We see that almost all threads have **mscorwks** module on their stack traces.

7. Now we load the appropriate SOS extension after checking that it is not loaded and verifying mscorwks module version:

```
0:000> .chain
Extension DLL search Path:
[...]
Extension DLL chain:
    dbghelp: image 6.12.0002.633, API 6.1.6, built Mon Feb 01 20:08:26 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\dbghelp.dll]
    ext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:31 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\winext\ext.dll]
    exts: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:24 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\WINXP\exts.dll]
    uext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:23 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\winext\uext.dll]
    ntsdexts: image 6.1.7650.0, API 1.0.0, built Mon Feb 01 20:08:08 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\WINXP\ntsdexts.dll]
```

```
0:000> lmv m mscorwks
start    end        module name
79e70000 7a3ff000   mscorwks   (pdb symbols)
c:\mss\mscorwks.pdb\62286AFFFC674D5198883B98518936FF2\mscorwks.pdb
    Loaded symbol image file: mscorwks.dll
    Image path: C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
    Image name: mscorwks.dll
    Timestamp:        Wed Oct 24 08:41:29 2007 (471EF729)
    CheckSum:         00597AA8
    ImageSize:        0058F000
    File version:     2.0.50727.1433
    Product version:  2.0.50727.1433
    File flags:       0 (Mask 3F)
    File OS:          4 Unknown Win32
    File type:        2.0 Dll
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      Microsoft Corporation
    ProductName:      Microsoft® .NET Framework
    InternalName:     mscorwks.dll
    OriginalFilename: mscorwks.dll
    ProductVersion:   2.0.50727.1433
    FileVersion:      2.0.50727.1433 (REDBITS.050727-1400)
    FileDescription:  Microsoft .NET Runtime Common Language Runtime - WorkStation
    LegalCopyright:   © Microsoft Corporation.  All rights reserved.
    Comments:         Flavor=Retail
```

Note: We see version 1433 and recall that in the previous exercise it was 312. This is because Framework 3.5 was installed in the mean time that upgraded SOS.dll in the same folder.

We load the extension from \ANETMDA-Dumps\32-bit\Framework.Updates\Microsoft.NET\Framework\v2.0.50727 folder:

```
0:000> .load C:\ANETMDA-Dumps\32-bit\Framework.Updates\Microsoft.NET\Framework\v2.0.50727\sos

0:000> .chain
[...]
    C:\ANETMDA-Dumps\32-bit\Framework.Updates\Microsoft.NET\Framework\v2.0.50727\sos: image
2.0.50727.1433, API 1.0.0, built Wed Oct 24 04:41:30 2007
        [path: C:\ANETMDA-Dumps\32-
bit\Framework.Updates\Microsoft.NET\Framework\v2.0.50727\sos.dll]
    dbghelp: image 6.12.0002.633, API 6.1.6, built Mon Feb 01 20:08:26 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\dbghelp.dll]
    ext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:31 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\winext\ext.dll]
    exts: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:24 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\WINXP\exts.dll]
    uext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:23 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\winext\uext.dll]
    ntsdexts: image 6.1.7650.0, API 1.0.0, built Mon Feb 01 20:08:08 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\WINXP\ntsdexts.dll]
```

8. We check if there are .NET exceptions on each thread:

```
0:000> ~*e !pe
There is no current managed exception on this thread
The current thread is unmanaged
There is no current managed exception on this thread
There is no current managed exception on this thread
The current thread is unmanaged
The current thread is unmanaged
There is no current managed exception on this thread
There is no current managed exception on this thread
There is no current managed exception on this thread
There is no current managed exception on this thread
The current thread is unmanaged
The current thread is unmanaged
There is no current managed exception on this thread
There is no current managed exception on this thread
```

9. "The customer" reported one of application windows was unresponsive. We now try the default WinDbg analysis command with **-hang** switch:

/* start of WinDbg output */

```
0:000> !analyze -v -hang
*******************************************************************************
*                                                                             *
*                        Exception Analysis                                   *
*                                                                             *
*******************************************************************************

*** ERROR: Module load completed but symbols could not be loaded for LINQPad.exe
GetPageUrlData failed, server returned HTTP status 404
URL requested: http://watson.microsoft.com/00000000.htm?Retriage=1

FAULTING_IP:
+6c532faf0439dadc
00000000 ??              ???

EXCEPTION_RECORD:  ffffffff -- (.exr 0xffffffffffffffff)
ExceptionAddress: 00000000
   ExceptionCode: 80000003 (Break instruction exception)
  ExceptionFlags: 00000000
NumberParameters: 0

FAULTING_THREAD:  00000000

BUGCHECK_STR:  HANG

PROCESS_NAME:  LINQPad.exe

ERROR_CODE: (NTSTATUS) 0xcfffffff - <Unable to get error code text>

EXCEPTION_CODE: (NTSTATUS) 0xcfffffff - <Unable to get error code text>

MOD_LIST: <ANALYSIS/>

NTGLOBALFLAG:  0

APPLICATION_VERIFIER_FLAGS:  0
```

```
MANAGED_STACK: !dumpstack -EE
OS Thread Id: 0xea0 (0)
Current frame:
ChildEBP RetAddr  Caller,Callee

DERIVED_WAIT_CHAIN:

Dl Eid Cid     WaitType
-- --- ------- -------------------------
   0   f60.ea0 Unknown

WAIT_CHAIN_COMMAND:  ~0s;k;;

BLOCKING_THREAD:  00000ea0

DEFAULT_BUCKET_ID:  APPLICATION_HANG_WRONG_SYMBOLS

PRIMARY_PROBLEM_CLASS:  APPLICATION_HANG_WRONG_SYMBOLS

LAST_CONTROL_TRANSFER:  from 7674b5b4 to 77c40f34

STACK_TEXT:
0014f058 7674b5b4 7b08374f bc6c3701 79e73940 ntdll!KiFastSystemCallRet
0014f05c 7b08374f bc6c3701 79e73940 0014f5d4 user32!NtUserWaitMessage+0xc
0014f0f4 7b0831a5 00000000 ffffffff 0031288c System_Windows_Forms_ni+0xb374f
0014f170 7b082fe3 064dcd50 16c6001d 01827064 System_Windows_Forms_ni+0xb31a5
0014f1a0 7b0692c2 06ea72cc 00000000 01826b30 System_Windows_Forms_ni+0xb2fe3
0014f1f8 007c11dc 00000000 00000000 00000000 System_Windows_Forms_ni+0x992c2
WARNING: Frame IP not in any known module. Following frames may be wrong.
0014f3b0 79e7c74b 00000003 0014f3c4 0014f440 0x7c11dc
0014f3c0 79e7c6cc 0014f490 00000000 0014f460 mscorwks!CallDescrWorker+0x33
0014f440 79e7c8e1 0014f490 00000000 0014f460 mscorwks!CallDescrWorkerWithHandler+0xa3
0014f584 79e7c783 0026c030 0014f64c 0014f618 mscorwks!MethodDesc::CallDescr+0x19c
0014f5a0 79e7c90d 0026c030 0014f64c 0014f618 mscorwks!MethodDesc::CallTargetWorker+0x1f
0014f5b4 79eefb9e 0014f618 bc0386cf 00000000 mscorwks!MethodDescCallSite::Call_RetArgSlot+0x18
0014f718 79eef830 00264410 00000001 0014f754 mscorwks!ClassLoader::RunMain+0x263
0014f980 79ef01da 00000000 bc038f87 00000001 mscorwks!Assembly::ExecuteMainMethod+0xa6
0014fe50 79fb9793 00a30000 00000000 bc038f77 mscorwks!SystemDomain::ExecuteMainMethod+0x43f
0014fea0 79fb96df 00a30000 bc038f3f 00000000 mscorwks!ExecuteEXE+0x59
0014fee8 736455ab 79fb9647 0014ff04 73747f16 mscorwks!_CorExeMain+0x15c
0014fef4 73747f16 00000000 73640000 0014ff18 mscoreei!_CorExeMain+0x38
0014ff04 73744de3 00000000 76573833 7ffde000 mscoree!ShellShim__CorExeMain+0x99
0014ff0c 76573833 7ffde000 0014ff58 77c1a9bd mscoree!_CorExeMain_Exported+0x8
0014ff18 77c1a9bd 7ffde000 001473cf 00000000 kernel32!BaseThreadInitThunk+0xe
0014ff58 00000000 00de552e 7ffde000 00000000 ntdll!_RtlUserThreadStart+0x23


FOLLOWUP_IP:
ntdll!KiFastSystemCallRet+0
77c40f34 c3              ret

SYMBOL_STACK_INDEX:  0

SYMBOL_NAME:  ntdll!KiFastSystemCallRet+0

FOLLOWUP_NAME:  MachineOwner

MODULE_NAME: ntdll
```

```
IMAGE_NAME:  ntdll.dll

DEBUG_FLR_IMAGE_TIMESTAMP:  4549bdc9

STACK_COMMAND:  ~0s ; kb

BUCKET_ID:  HANG_ntdll!KiFastSystemCallRet+0

FAILURE_BUCKET_ID:  APPLICATION_HANG_WRONG_SYMBOLS_cffffffff_ntdll.dll!KiFastSystemCallRet

WATSON_STAGEONE_URL:  http://watson.microsoft.com/00000000.htm?Retriage=1

Followup: MachineOwner
---------
                                    /* end of WinDbg output */
```

Note: We see the command wasn't found anything useful. It shows only the main (#0) assembly thread that is waiting for a user message (normal GUI Win32 API message loop).

10. Let's now check the managed stack trace for this thread (**!CLRStack** command):

```
0:000> !CLRStack
OS Thread Id: 0xea0 (0)
ESP       EIP
0014f068 77c40f34 [InlinedCallFrame: 0014f068]
0014f064 7b08374f
0014f104 7b0831a5
0014f17c 7b082fe3
0014f1ac 7b0692c2
0014f1bc 007c3264
0014f210 007c11dc
0014f36c 007c0545
0014f3a0 007c0362
0014f3a8 007c00e3
0014f5d4 79e7c74b [GCFrame: 0014f5d4]
```

Note: Something has got wrong. We don't see symbols on the managed stack trace. Let's check loaded extensions chain:

```
0:000> .chain
Extension DLL search Path:
[...]
Extension DLL chain:
    C:\Windows\Microsoft.NET\Framework\v2.0.50727\sos: image 2.0.50727.4963, API 1.0.0, built Thu Jul 07 03:08:08 2011
        [path: C:\Windows\Microsoft.NET\Framework\v2.0.50727\sos.dll]
    C:\ANETMDA-Dumps\32-bit\Framework.Updates\Microsoft.NET\Framework\v2.0.50727\sos: image 2.0.50727.1433, API 1.0.0,
built Wed Oct 24 04:41:30 2007
        [path: C:\ANETMDA-Dumps\32-bit\Framework.Updates\Microsoft.NET\Framework\v2.0.50727\sos.dll]
    dbghelp: image 6.12.0002.633, API 6.1.6, built Mon Feb 01 20:08:26 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\dbghelp.dll]
    ext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:31 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\winext\ext.dll]
    exts: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:24 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\WINXP\exts.dll]
    uext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:23 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\winext\uext.dll]
```

```
    ntsdexts: image 6.1.7650.0, API 1.0.0, built Mon Feb 01 20:08:08 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\WINXP\ntsdexts.dll]
```

Note: We see that the default analysis command loaded another version of sos.dll (.4963) and it is on top of the search list and used instead of the correct sos.dll (.1433). We, therefore, remove the first sos.dll from the chain and see the correct managed stack trace:

```
0:000> .unload C:\Windows\Microsoft.NET\Framework\v2.0.50727\sos
Unloading C:\Windows\Microsoft.NET\Framework\v2.0.50727\sos extension DLL

0:000> !CLRStack
OS Thread Id: 0xea0 (0)
ESP       EIP
0014f068 77c40f34 [InlinedCallFrame: 0014f068] System.Windows.Forms.UnsafeNativeMethods.WaitMessage()
0014f064 7b08374f
System.Windows.Forms.Application+ComponentManager.System.Windows.Forms.UnsafeNativeMethods.IMsoComponentManager.FPushM
essageLoop(Int32, Int32, Int32)
0014f104 7b0831a5 System.Windows.Forms.Application+ThreadContext.RunMessageLoopInner(Int32,
System.Windows.Forms.ApplicationContext)
0014f17c 7b082fe3 System.Windows.Forms.Application+ThreadContext.RunMessageLoop(Int32,
System.Windows.Forms.ApplicationContext)
0014f1ac 7b0692c2 System.Windows.Forms.Application.Run(System.Windows.Forms.Form)
0014f1bc 007c3264 LINQPad.Program.Run(System.String, Boolean, System.String, Boolean, Boolean, System.String)
0014f210 007c11dc LINQPad.Program.Go(System.String[])
0014f36c 007c0545 LINQPad.Program.Start(System.String[])
0014f3a0 007c0362 LINQPad.ProgramStarter.Run(System.String[])
0014f3a8 007c00e3 LINQPad.Loader.Main(System.String[])
0014f5d4 79e7c74b [GCFrame: 0014f5d4]
```

11. We also see a possible JIT call on the stack trace and double check that using **!IP2MD** command:

```
0:000> k
ChildEBP RetAddr
0014f058 7674b5b4 ntdll!KiFastSystemCallRet
0014f05c 7b08374f user32!NtUserWaitMessage+0xc
0014f0f4 7b0831a5 System_Windows_Forms_ni+0xb374f
0014f170 7b082fe3 System_Windows_Forms_ni+0xb31a5
0014f1a0 7b0692c2 System_Windows_Forms_ni+0xb2fe3
0014f1f8 007c11dc System_Windows_Forms_ni+0x992c2
WARNING: Frame IP not in any known module. Following frames may be wrong.
0014f3b0 79e7c74b 0x7c11dc
0014f3c0 79e7c6cc mscorwks!CallDescrWorker+0x33
0014f440 79e7c8e1 mscorwks!CallDescrWorkerWithHandler+0xa3
0014f584 79e7c783 mscorwks!MethodDesc::CallDescr+0x19c
0014f5a0 79e7c90d mscorwks!MethodDesc::CallTargetWorker+0x1f
0014f5b4 79eefb9e mscorwks!MethodDescCallSite::Call_RetArgSlot+0x18
0014f718 79eef830 mscorwks!ClassLoader::RunMain+0x263
0014f980 79ef01da mscorwks!Assembly::ExecuteMainMethod+0xa6
0014fe50 79fb9793 mscorwks!SystemDomain::ExecuteMainMethod+0x43f
0014fea0 79fb96df mscorwks!ExecuteEXE+0x59
0014fee8 736455ab mscorwks!_CorExeMain+0x15c
0014fef4 73747f16 mscoreei!_CorExeMain+0x38
0014ff04 73744de3 mscoree!ShellShim__CorExeMain+0x99
0014ff0c 76573833 mscoree!_CorExeMain_Exported+0x8
0014ff18 77c1a9bd kernel32!BaseThreadInitThunk+0xe
0014ff58 00000000 ntdll!_RtlUserThreadStart+0x23
```

```
0:000> !IP2MD 0x7c11dc
MethodDesc: 00267ac0
Method Name: LINQPad.Program.Go(System.String[])
Class: 00750e28
MethodTable: 00267c30
mdToken: 0600022a
Module: 00262c3c
IsJitted: yes
m_CodeOrIL: 007c0580
```

12. We now check thread CPU consumption (**!runaway** command):

```
0:000> !runaway f
 User Mode Time
  Thread       Time
  12:cf8       0 days 0:03:43.921
   0:ea0       0 days 0:00:05.000
   7:c38       0 days 0:00:00.625
   6:bb8       0 days 0:00:00.125
   8:9e8       0 days 0:00:00.015
  13:1cc       0 days 0:00:00.000
  11:334       0 days 0:00:00.000
  10:8f4       0 days 0:00:00.000
   9:134       0 days 0:00:00.000
   5:8d4       0 days 0:00:00.000
   4:a14       0 days 0:00:00.000
   3:cc8       0 days 0:00:00.000
   2:1bc       0 days 0:00:00.000
   1:e84       0 days 0:00:00.000
 Kernel Mode Time
  Thread       Time
  12:cf8       0 days 0:00:04.218
   0:ea0       0 days 0:00:02.546
   7:c38       0 days 0:00:00.281
   6:bb8       0 days 0:00:00.078
  13:1cc       0 days 0:00:00.000
  11:334       0 days 0:00:00.000
  10:8f4       0 days 0:00:00.000
   9:134       0 days 0:00:00.000
   8:9e8       0 days 0:00:00.000
   5:8d4       0 days 0:00:00.000
   4:a14       0 days 0:00:00.000
   3:cc8       0 days 0:00:00.000
   2:1bc       0 days 0:00:00.000
   1:e84       0 days 0:00:00.000
 Elapsed Time
  Thread       Time
   0:ea0       0 days 0:04:28.788
   2:1bc       0 days 0:04:28.225
   1:e84       0 days 0:04:28.225
   3:cc8       0 days 0:04:28.084
```

```
   4:a14       0 days 0:04:28.006
   6:bb8       0 days 0:04:27.788
   5:8d4       0 days 0:04:27.788
   7:c38       0 days 0:04:23.256
   8:9e8       0 days 0:04:23.225
   9:134       0 days 0:04:22.709
  10:8f4       0 days 0:03:57.803
  11:334       0 days 0:03:49.272
  12:cf8       0 days 0:03:48.178
  13:1cc       0 days 0:03:48.006
```

Note: We see that the thread #12 spent most of the time (03:43) spiking CPU in user mode since its creation 03:48 minutes ago (we can add 4 seconds for kernel mode and see that it was consuming CPU almost all time).

13. We now switch to this thread:

```
0:000> ~12s
eax=00000000 ebx=0a0ae5ec ecx=08299850 edx=052f7f80 esi=052f7f80 edi=00000000
eip=07562074 esp=0a0ae5c0 ebp=0a0ae5d0 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
07562074 80790c00        cmp     byte ptr [ecx+0Ch],0       ds:0023:0829985c=00

0:012> k
ChildEBP RetAddr
WARNING: Frame IP not in any known module. Following frames may be wrong.
0a0ae5d0 79e7c6cc 0x7562074
0a0ae650 79e7c8e1 mscorwks!CallDescrWorkerWithHandler+0xa3
0a0ae78c 79e7c783 mscorwks!MethodDesc::CallDescr+0x19c
0a0ae7a8 79e7c90d mscorwks!MethodDesc::CallTargetWorker+0x1f
0a0ae7bc 79f321b6 mscorwks!MethodDescCallSite::Call_RetArgSlot+0x18
0a0ae9a8 79f31eaf mscorwks!InvokeImpl+0x559
0a0aea68 793a44bd mscorwks!RuntimeMethodHandle::InvokeMethodFast+0xbd
0a0aeab4 793a41e5 mscorlib_ni+0x2e44bd
00000000 00000000 mscorlib_ni+0x2e41e5
```

Note: We see that it is executing some code instead of waiting like other threads:

```
0:012> ~11k
ChildEBP RetAddr
097df8dc 77c406a0 ntdll!KiFastSystemCallRet
097df8e0 765777d4 ntdll!NtWaitForSingleObject+0xc
097df950 76577742 kernel32!WaitForSingleObjectEx+0xbe
097df964 6d01f57d kernel32!WaitForSingleObject+0x12
097df97c 6d016c92 mshtml!CDwnTaskExec::ThreadExec+0x127
097df988 6cf9dadc mshtml!CExecFT::ThreadProc+0x3c
097df990 76573833 mshtml!CExecFT::StaticThreadProc+0xd
097df99c 77c1a9bd kernel32!BaseThreadInitThunk+0xe
097df9dc 00000000 ntdll!_RtlUserThreadStart+0x23

0:012> ~10k
ChildEBP RetAddr
0794f6d8 77c400f0 ntdll!KiFastSystemCallRet
0794f6dc 76557948 ntdll!NtRemoveIoCompletion+0xc
0794f708 7665af2e kernel32!GetQueuedCompletionStatus+0x29
0794f744 7665b067 rpcrt4!COMMON_ProcessCalls+0xb5
0794f7b0 7665ac4f rpcrt4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
0794f7bc 7665acb9 rpcrt4!ProcessIOEventsWrapper+0xe
```

```
0794f7e0 7665ad03 rpcrt4!BaseCachedThreadRoutine+0x5c
0794f7ec 76573833 rpcrt4!ThreadStartRoutine+0x1e
0794f7f8 77c1a9bd kernel32!BaseThreadInitThunk+0xe
0794f838 00000000 ntdll!_RtlUserThreadStart+0x23

0:012> ~9k
ChildEBP RetAddr
0783f864 77c400f0 ntdll!KiFastSystemCallRet
0783f868 76557948 ntdll!NtRemoveIoCompletion+0xc
0783f894 79f02f04 kernel32!GetQueuedCompletionStatus+0x29
0783f904 79f95a2e mscorwks!ThreadpoolMgr::CompletionPortThreadStart+0x141
0783fd9c 76573833 mscorwks!Thread::intermediateThreadProc+0x49
0783fda8 77c1a9bd kernel32!BaseThreadInitThunk+0xe
0783fde8 00000000 ntdll!_RtlUserThreadStart+0x23

0:012> ~8k
ChildEBP RetAddr
064af31c 77c406a0 ntdll!KiFastSystemCallRet
064af320 765777d4 ntdll!NtWaitForSingleObject+0xc
064af390 79e789c6 kernel32!WaitForSingleObjectEx+0xbe
064af3d4 79e7898f mscorwks!PEImage::LoadImage+0x1af
064af424 79e78944 mscorwks!CLREvent::WaitEx+0x117
064af438 79f0b1e7 mscorwks!CLREvent::Wait+0x17
064af504 79f95a2e mscorwks!AppDomain::ADUnloadThreadStart+0x308
064af920 76573833 mscorwks!Thread::intermediateThreadProc+0x49
064af92c 77c1a9bd kernel32!BaseThreadInitThunk+0xe
064af96c 00000000 ntdll!_RtlUserThreadStart+0x23
```

14. We check if the address instruction pointer address belongs to JIT-compiled code:

```
0:012> !IP2MD 0x7562074
MethodDesc: 05f80be8
Method Name: UserQuery+ClassMain.Main()
Class: 07554130
MethodTable: 05f80c00
mdToken: 06000004
Module: 05f8064c
IsJitted: yes
m_CodeOrIL: 07562068

0:012> !U 07562068
Normal JIT generated code
UserQuery+ClassMain.Main()
Begin 07562068, size 13
>>> 07562068 80790c00        cmp     byte ptr [ecx+0Ch],0
0756206c 750c            jne     0756207a
0756206e 8b4104          mov     eax,dword ptr [ecx+4]
07562071 314108          xor     dword ptr [ecx+8],eax
07562074 80790c00        cmp     byte ptr [ecx+0Ch],0
07562078 74f4            je      0756206e
0756207a c3              ret
```

15. We double check our findings with **!CLRStack** command:

```
0:012> !CLRStack
OS Thread Id: 0xcf8 (12)
ESP       EIP
0a0ae5c0 07562074 UserQuery+ClassMain.Main()
0a0ae5c4 07562052 UserQuery.RunUserAuthoredQuery()
0a0ae840 79e7c74b [CustomGCFrame: 0a0ae840]
0a0ae824 79e7c74b [GCFrame: 0a0ae824]
0a0ae808 79e7c74b [GCFrame: 0a0ae808]
0a0aea10 79e7c74b [HelperMethodFrame_1OBJ: 0a0aea10] System.RuntimeMethodHandle._InvokeMethodFast(System.Object,
System.Object[], System.SignatureStruct ByRef, System.Reflection.MethodAttributes, System.RuntimeTypeHandle)
0a0aea80 793a44bd System.RuntimeMethodHandle.InvokeMethodFast(System.Object, System.Object[], System.Signature,
System.Reflection.MethodAttributes, System.RuntimeTypeHandle)
0a0aeacc 793a41e5 System.Reflection.RuntimeMethodInfo.Invoke(System.Object, System.Reflection.BindingFlags,
System.Reflection.Binder, System.Object[], System.Globalization.CultureInfo, Boolean)
0a0aeb18 793a40a2 System.Reflection.RuntimeMethodInfo.Invoke(System.Object, System.Reflection.BindingFlags,
System.Reflection.Binder, System.Object[], System.Globalization.CultureInfo)
0a0aeb38 7942c542 System.Reflection.MethodBase.Invoke(System.Object, System.Object[])
0a0aeb40 07561337 LINQPad.ExecutionModel.Server.RunClrQuery()
0a0aec80 07560b53 LINQPad.ExecutionModel.Server.StartClrQuery()
0a0aecc4 793b0d1f System.Threading.ThreadHelper.ThreadStart_Context(System.Object)
0a0aeccc 79373ecd System.Threading.ExecutionContext.Run(System.Threading.ExecutionContext,
System.Threading.ContextCallback, System.Object)
0a0aece4 793b0c68 System.Threading.ThreadHelper.ThreadStart()
0a0aef10 79e7c74b [GCFrame: 0a0aef10]
0a0af200 79e7c74b [ContextTransitionFrame: 0a0af200]
```

16. We now dump the method descriptor, class, method table (with or without method descriptors), module and assembly information using **!DumpMD**, **!DumpClass**, **!DumpMT**, **!DumpModule**, **!DumpAssembly** and **!DumpDomain** SOS extension commands respectively:

```
0:012> !IP2MD 0x7562074
MethodDesc: 05f80be8
Method Name: UserQuery+ClassMain.Main()
Class: 07554130
MethodTable: 05f80c00
mdToken: 06000004
Module: 05f8064c
IsJitted: yes
m_CodeOrIL: 07562068

0:012> !DumpMD 05f80be8
Method Name: UserQuery+ClassMain.Main()
Class: 07554130
MethodTable: 05f80c00
mdToken: 06000004
Module: 05f8064c
IsJitted: yes
m_CodeOrIL: 07562068
```

```
0:012> !DumpClass 07554130
Class Name: UserQuery+ClassMain
mdToken: 02000003 (C:\Users\Training\AppData\Local\Temp\LINQPad\kxaiqwhz\query_toeaqn.dll)
Parent Class: 790fd08c
Module: 05f8064c
Method Table: 05f80c00
Vtable Slots: 4
Total Method Slots: 7
Class Attributes: 100002
NumInstanceFields: 3
NumStaticFields: 0
      MT    Field   Offset                 Type VT     Attr    Value Name
7910be50  4000001        c       System.Boolean  1 instance           time2stop
79102290  4000002        4         System.Int32  1 instance           inSensor
79102290  4000003        8         System.Int32  1 instance           outSensor

0:012> !DumpMT 05f80c00
EEClass: 07554130
Module: 05f8064c
Name: UserQuery+ClassMain
mdToken: 02000003  (C:\Users\Training\AppData\Local\Temp\LINQPad\kxaiqwhz\query_toeaqn.dll)
BaseSize: 0x14
ComponentSize: 0x0
Number of IFaces in IFaceMap: 0
Slots in VTable: 7

0:012> !DumpMT -md 05f80c00
EEClass: 07554130
Module: 05f8064c
Name: UserQuery+ClassMain
mdToken: 02000003  (C:\Users\Training\AppData\Local\Temp\LINQPad\kxaiqwhz\query_toeaqn.dll)
BaseSize: 0x14
ComponentSize: 0x0
Number of IFaces in IFaceMap: 0
Slots in VTable: 7
--------------------------------------
MethodDesc Table
   Entry MethodDesc      JIT Name
79371278   7914b928   PreJIT System.Object.ToString()
7936b3b0   7914b930   PreJIT System.Object.Equals(System.Object)
7936b3d0   7914b948   PreJIT System.Object.GetHashCode()
793624d0   7914b950   PreJIT System.Object.Finalize()
07562068   05f80be8      JIT UserQuery+ClassMain.Main()
0751cea9   05f80bf0     NONE UserQuery+ClassMain.DoWork()
0751cead   05f80bf8     NONE UserQuery+ClassMain..ctor()
```

```
0:012> !DumpModule 05f8064c
Name: C:\Users\Training\AppData\Local\Temp\LINQPad\kxaiqwhz\query_toeaqn.dll
Attributes: PEFile
Assembly: 094a07f8
LoaderHeap: 00000000
TypeDefToMethodTableMap: 0755271c
TypeRefToMethodTableMap: 07552728
MethodDefToDescMap: 07552758
FieldDefToDescMap: 07552774
MemberRefToDescMap: 07552784
FileReferencesMap: 075527a4
AssemblyReferencesMap: 075527a8
MetaData start address: 739020a4 (1328 bytes)

0:012> !DumpAssembly 094a07f8
Parent Domain: 095a5520
Name: C:\Users\Training\AppData\Local\Temp\LINQPad\kxaiqwhz\query_toeaqn.dll
ClassLoader: 0525e310
SecurityDescriptor: 003f2610
  Module Name
05f8064c C:\Users\Training\AppData\Local\Temp\LINQPad\kxaiqwhz\query_toeaqn.dll

0:012> !DumpDomain 095a5520
--------------------------------------
Domain 3: 095a5520
LowFrequencyHeap: 095a5544
HighFrequencyHeap: 095a559c
StubHeap: 095a55f4
Stage: OPEN
SecurityDescriptor: 0951fe78
Name: LINQPad Query Server [LinqB]
Assembly: 002cb0d0 [C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll]
ClassLoader: 002aba10
SecurityDescriptor: 094a05d8
  Module Name
790c2000 C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll
0028479c C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\sortkey.nlp
00284410 C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\sorttbls.nlp

Assembly: 094a0000 [C:\LINQPad\LINQPad.exe]
ClassLoader: 0525e070
SecurityDescriptor: 094a0198
  Module Name
07512cf0 C:\LINQPad\LINQPad.exe

Assembly: 094a02a8
[C:\Windows\assembly\GAC_32\System.Data\2.0.0.0__b77a5c561934e089\System.Data.dll]
ClassLoader: 0525e0e0
SecurityDescriptor: 094a0908
  Module Name
653f2000 C:\Windows\assembly\GAC_32\System.Data\2.0.0.0__b77a5c561934e089\System.Data.dll
```

```
Assembly: 002eb458 [C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll]
ClassLoader: 002abe70
SecurityDescriptor: 094a0110
  Module Name
7a726000 C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll

Assembly: 002ebea8
[C:\Windows\assembly\GAC_MSIL\System.Core\3.5.0.0__b77a5c561934e089\System.Core.dll]
ClassLoader: 002ac340
SecurityDescriptor: 094a0330
  Module Name
6c25c000 C:\Windows\assembly\GAC_MSIL\System.Core\3.5.0.0__b77a5c561934e089\System.Core.dll

Assembly: 00380cf0
[C:\Windows\assembly\GAC_MSIL\System.Configuration\2.0.0.0__b03f5f7f11d50a3a\System.Configurati
on.dll]
ClassLoader: 00302770
SecurityDescriptor: 0949ff78
  Module Name
648ea000
C:\Windows\assembly\GAC_MSIL\System.Configuration\2.0.0.0__b03f5f7f11d50a3a\System.Configuratio
n.dll

Assembly: 002ec260
[C:\Windows\assembly\GAC_MSIL\System.Xml\2.0.0.0__b77a5c561934e089\System.Xml.dll]
ClassLoader: 002ac500
SecurityDescriptor: 094a0660
  Module Name
639f8000 C:\Windows\assembly\GAC_MSIL\System.Xml\2.0.0.0__b77a5c561934e089\System.Xml.dll

Assembly: 002ebd10
[C:\Windows\assembly\GAC_MSIL\System.Data.Linq\3.5.0.0__b77a5c561934e089\System.Data.Linq.dll]
ClassLoader: 002abf50
SecurityDescriptor: 094a03b8
  Module Name
00282010
C:\Windows\assembly\GAC_MSIL\System.Data.Linq\3.5.0.0__b77a5c561934e089\System.Data.Linq.dll

Assembly: 094a07f8 [C:\Users\Training\AppData\Local\Temp\LINQPad\kxaiqwhz\query_toeaqn.dll]
ClassLoader: 0525e310
SecurityDescriptor: 094a0440
  Module Name
05f8064c C:\Users\Training\AppData\Local\Temp\LINQPad\kxaiqwhz\query_toeaqn.dll
```

17. At the end of this exercise we revisit out CLR stack trace again and disassemble the previous method:

```
0:012> !CLRStack
OS Thread Id: 0xcf8 (12)
ESP       EIP
0a0ae5c0 07562074 UserQuery+ClassMain.Main()
0a0ae5c4 07562052 UserQuery.RunUserAuthoredQuery()
0a0ae840 79e7c74b [CustomGCFrame: 0a0ae840]
[...]
```

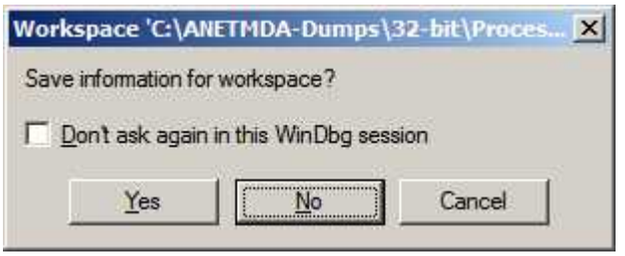
```
0:012> !U 07562052
Normal JIT generated code
UserQuery.RunUserAuthoredQuery()
Begin 07562040, size 13
07562040 b9000cf805      mov     ecx,5F80C00h (MT: UserQuery+ClassMain)
07562045 e8d2ffcef8      call    0025201c (JitHelp: CORINFO_HELP_NEWSFAST)
0756204a 8bc8            mov     ecx,eax
0756204c ff15380cf805    call    dword ptr ds:[5F80C38h] (UserQuery+ClassMain.Main(), mdToken: 06000004)
>>> 07562052 c3              ret
```

Note: We see JIT code annotated with method names and this can be helpful with reverse engineering of an unknown method.

18. We close logging before exiting WinDbg:

```
0:012> .logclose
Closing open log file C:\ANETMDA-Dumps\32-bit\Processes\CLR2\LINQPadB.log
```

If presented with this dialog choose No:



Note: To avoid possible confusion and glitches we recommend to exit WinDbg after each exercise.

Exercise PN4

- **Goal:** Learn how to recognize and analyze deadlocks using SOS(EX), execution residue, handled exceptions, dump object references
- **Patterns:** CLR Thread; Special Thread; Blocked Thread; Annotated Disassembly; Deadlock; Caller-n-Callee; Execution Residue; Handled Exception
- **Commands:** !Threads -special, kL, !syncblk, !DumpObject, ub, !U, dp, !dlk, !DumpStack, !DumpStackObjects, !teb, dps
- \ANETMDA-Dumps\Exercise-PN4-Analysis-process-dump-LINQPadC-32-CLR4.pdf

© 2013 Software Diagnostics Services

Exercise PN4: Analysis of an application process dump (LINQPadC, 32-bit, CLR 4)

Goal: Learn how to recognize and analyze deadlocks using SOS(EX), execution residue, handled exceptions, dump object references.

Patterns: CLR Thread; Special Thread; Blocked Thread; Annotated Disassembly; Deadlock; Caller-n-Callee; Execution Residue; Handled Exception

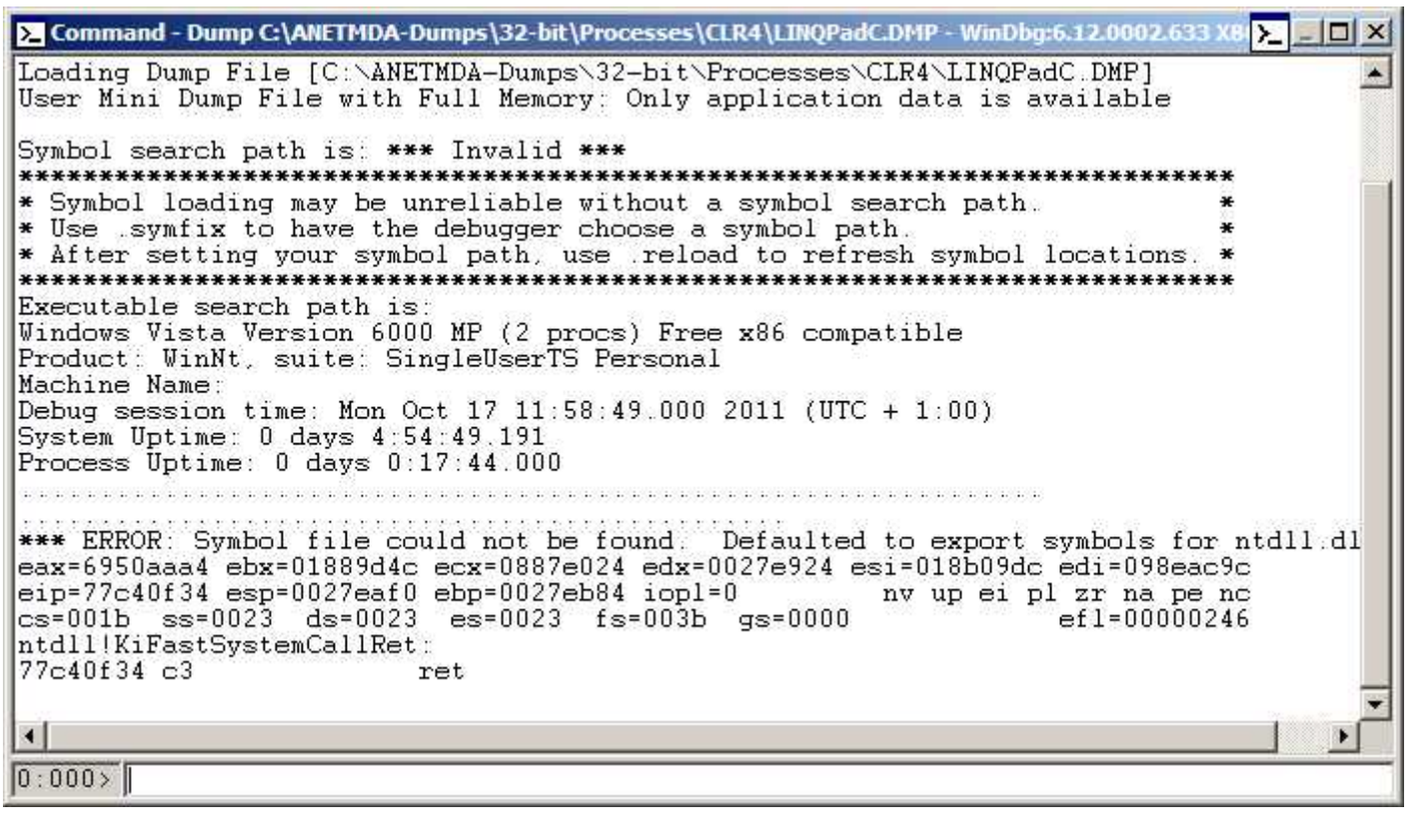
Commands: !Threads -special, kL, !syncblk, !DumpObject, ub, dp, !dlk, !DumpStack, !DumpStackObjects, !teb

1. Launch WinDbg from Debugging Tools for Windows or Debugging Tools for Windows (x86)

2. Open \ANETMDA-Dumps\32-bit\Processes\CLR4\LINQPadC.DMP

3. If you are presented with this dialog say No:

4. We get the dump file loaded:



5. Open a log file using **.logopen** command and load symbols (**.symfix** and **.reload** commands):

```
0:000> .logopen C:\ANETMDA-Dumps\32-bit\Processes\CLR4\LINQPadC.log
Opened log file 'C:\ANETMDA-Dumps\32-bit\Processes\CLR4\LINQPadC.log'

0:000> .symfix c:\mss

0:000> .reload
.........................
```

Note: The results may be slightly different on your system if you have 32-bit .NET Framework 4.0.30319.**1** already installed or you don't have any .NET Framework 4.0.30319 installed.

6. Type ~***k** command to verify the correctness of all stack traces:

```
0:000> ~*k

.  0  Id: 74c.844 Suspend: 0 Teb: 7ffdf000 Unfrozen
ChildEBP RetAddr
0027eaec 7674b5b4 ntdll!KiFastSystemCallRet
*** WARNING: Unable to verify checksum for System.Windows.Forms.ni.dll
0027eaf0 694d737a user32!NtUserWaitMessage+0xc
0027eb84 694d6e2c System_Windows_Forms_ni+0x22737a
0027ebe0 694d6c81 System_Windows_Forms_ni+0x226e2c
0027ec10 6946366d System_Windows_Forms_ni+0x226c81
0027ec28 00173f0d System_Windows_Forms_ni+0x1b366d
WARNING: Frame IP not in any known module. Following frames may be wrong.
0027ed0c 00171515 0x173f0d
0027efb4 6b9f21db 0x171515
0027efb8 6b9fe021 clr!CallDescrWorker+0x33
0027f06c 6ba128bb clr!SigParser::GetElemType+0x28
0027f084 0027f16c clr!MetaSig::MetaSig+0x3c
0027f0f8 6b9fe30a 0x27f16c
0027f160 00000000 clr!MethodDesc::GetSigFromMetadata+0x21

   1  Id: 74c.b30 Suspend: 0 Teb: 7ffde000 Unfrozen
ChildEBP RetAddr
0183fde8 77c40690 ntdll!KiFastSystemCallRet
0183fdec 76577e09 ntdll!ZwWaitForMultipleObjects+0xc
0183fe88 76578150 kernel32!WaitForMultipleObjectsEx+0x11d
0183fea4 6bb575e8 kernel32!WaitForMultipleObjects+0x18
0183ff08 6bb57526 clr!DebuggerRCThread::MainLoop+0xd9
0183ff38 6bb57461 clr!DebuggerRCThread::ThreadProc+0xca
0183ff64 76573833 clr!DebuggerRCThread::ThreadProcStatic+0x83
0183ff70 77c1a9bd kernel32!BaseThreadInitThunk+0xe
0183ffb0 00000000 ntdll!_RtlUserThreadStart+0x23
```

```
   2  Id: 74c.aa4 Suspend: 0 Teb: 7ffdd000 Unfrozen
ChildEBP RetAddr
039dfab0 77c40690 ntdll!KiFastSystemCallRet
039dfab4 76577e09 ntdll!ZwWaitForMultipleObjects+0xc
039dfb50 76578150 kernel32!WaitForMultipleObjectsEx+0x11d
039dfb6c 6bb6833d kernel32!WaitForMultipleObjects+0x18
039dfb8c 6bb683a1 clr!WKS::WaitForFinalizerEvent+0xa6
039dfba4 6baa5c05 clr!WKS::GCHeap::FinalizerThreadWorker+0x4a
039dfbb8 6baa5c87 clr!Thread::DoExtraWorkForFinalizer+0x114
039dfc68 6baa5d42 clr!Thread::ShouldChangeAbortToUnload+0x101
039dfcc8 6ba978be clr!Thread::ShouldChangeAbortToUnload+0x399
039dfcec 6ba978d1 clr!ManagedThreadBase_NoADTransition+0x35
039dfcfc 6badd313 clr!ManagedThreadBase::FinalizerBase+0xf
039dfd34 6baa5a08 clr!WKS::GCHeap::FinalizerThreadStart+0x10c
039dfdcc 76573833 clr!Thread::intermediateThreadProc+0x4b
039dfdd8 77c1a9bd kernel32!BaseThreadInitThunk+0xe
039dfe18 00000000 ntdll!_RtlUserThreadStart+0x23

   3  Id: 74c.30c Suspend: 0 Teb: 7ffdc000 Unfrozen
ChildEBP RetAddr
046af440 77c3f9c0 ntdll!KiFastSystemCallRet
046af444 7653f00d ntdll!NtFsControlFile+0xc
*** WARNING: Unable to verify checksum for System.Core.ni.dll
046af488 68ef80b7 kernel32!ConnectNamedPipe+0x52
046af4f8 68f8c07c System_Core_ni+0x3080b7
*** WARNING: Unable to verify checksum for mscorlib.ni.dll
046af5a0 6aa6ae5b System_Core_ni+0x39c07c
046af5b0 6a9f7ff4 mscorlib_ni+0x2aae5b
046af5cc 6a9f7f34 mscorlib_ni+0x237ff4
046af5ec 6aa6ade8 mscorlib_ni+0x237f34
046af604 6b9f21db mscorlib_ni+0x2aade8
046af614 6ba14a2a clr!CallDescrWorker+0x33
046af690 6ba14bcc clr!CallDescrWorkerWithHandler+0x8e
046af7d4 6ba14c01 clr!MethodDesc::CallDescr+0x194
046af7f0 6bb8b512 clr!MethodDesc::CallTargetWorker+0x21
046af9fc 6baa5c05 clr!ThreadNative::KickOffThread_Worker+0x1e1
046afa10 6baa5c87 clr!Thread::DoExtraWorkForFinalizer+0x114
046afac0 6baa5d42 clr!Thread::ShouldChangeAbortToUnload+0x101
046afb20 6baa5dd9 clr!Thread::ShouldChangeAbortToUnload+0x399
046afb44 6bb8b3e5 clr!Thread::ShouldChangeAbortToUnload+0x43a
046afb5c 6bb8b2e0 clr!ManagedThreadBase::KickOff+0x15
046afbf4 6baa5a08 clr!ThreadNative::KickOffThread+0x23e
046afd14 76573833 clr!Thread::intermediateThreadProc+0x4b
046afd20 77c1a9bd kernel32!BaseThreadInitThunk+0xe
046afd60 00000000 ntdll!_RtlUserThreadStart+0x23

   4  Id: 74c.d20 Suspend: 0 Teb: 7ffdb000 Unfrozen
ChildEBP RetAddr
048efbe4 77c40690 ntdll!KiFastSystemCallRet
048efbe8 76577e09 ntdll!ZwWaitForMultipleObjects+0xc
048efc84 7674c4af kernel32!WaitForMultipleObjectsEx+0x11d
048efcd8 76748b7b user32!RealMsgWaitForMultipleObjectsEx+0x13c
048efcf4 74d01965 user32!MsgWaitForMultipleObjects+0x1f
048efd40 76573833 GdiPlus!BackgroundThreadProc+0x59
048efd4c 77c1a9bd kernel32!BaseThreadInitThunk+0xe
048efd8c 00000000 ntdll!_RtlUserThreadStart+0x23
```

```
   5  Id: 74c.e9c Suspend: 0 Teb: 7ffd6000 Unfrozen
ChildEBP RetAddr
05c4ead8 77c40690 ntdll!KiFastSystemCallRet
05c4eadc 76577e09 ntdll!ZwWaitForMultipleObjects+0xc
05c4eb78 6baa516a kernel32!WaitForMultipleObjectsEx+0x11d
05c4ebdc 6baa4f98 clr!WaitForMultipleObjectsEx_SO_TOLERANT+0x56
05c4ebfc 6baa4dd8 clr!Thread::DoAppropriateAptStateWait+0x4d
05c4ec90 6baa4e99 clr!Thread::DoAppropriateWaitWorker+0x17d
05c4ecfc 6baa4f17 clr!Thread::DoAppropriateWait+0x60
05c4ed50 6ba4d409 clr!CLREvent::WaitEx+0x106
05c4ed64 6bb8c71c clr!CLREvent::Wait+0x19
05c4ed78 6bb8c73a clr!Thread::Wait+0x1d
05c4ed8c 6bb8c545 clr!Thread::Block+0x1a
05c4ee38 6bb8c5b2 clr!SyncBlock::Wait+0x169
05c4ee4c 6bb8c6a4 clr!ObjHeader::Wait+0x2c
05c4eef4 6a9f9140 clr!ObjectNative::WaitTimeout+0x147
05c4ef04 6afb428a mscorlib_ni+0x239140
05c4efd0 6aa6ae5b mscorlib_ni+0x7f428a
05c4efe0 6a9f7ff4 mscorlib_ni+0x2aae5b
05c4effc 6a9f7f34 mscorlib_ni+0x237ff4
05c4f01c 6aa6ade8 mscorlib_ni+0x237f34
05c4f034 6b9f21db mscorlib_ni+0x2aade8
05c4f044 6ba14a2a clr!CallDescrWorker+0x33
05c4f0c0 6ba14bcc clr!CallDescrWorkerWithHandler+0x8e
05c4f204 6ba14c01 clr!MethodDesc::CallDescr+0x194
05c4f220 6bb8b512 clr!MethodDesc::CallTargetWorker+0x21
05c4f42c 6baa5c05 clr!ThreadNative::KickOffThread_Worker+0x1e1
05c4f440 6baa5c87 clr!Thread::DoExtraWorkForFinalizer+0x114
05c4f4f0 6baa5d42 clr!Thread::ShouldChangeAbortToUnload+0x101
05c4f550 6baa5dd9 clr!Thread::ShouldChangeAbortToUnload+0x399
05c4f574 6bb8b3e5 clr!Thread::ShouldChangeAbortToUnload+0x43a
05c4f58c 6bb8b2e0 clr!ManagedThreadBase::KickOff+0x15
05c4f624 6baa5a08 clr!ThreadNative::KickOffThread+0x23e
05c4f8c8 76573833 clr!Thread::intermediateThreadProc+0x4b
05c4f8d4 77c1a9bd kernel32!BaseThreadInitThunk+0xe
05c4f914 00000000 ntdll!_RtlUserThreadStart+0x23

   6  Id: 74c.9e4 Suspend: 0 Teb: 7ffda000 Unfrozen
ChildEBP RetAddr
0639ef4c 77c40690 ntdll!KiFastSystemCallRet
0639ef50 76577e09 ntdll!ZwWaitForMultipleObjects+0xc
0639efec 6baa516a kernel32!WaitForMultipleObjectsEx+0x11d
0639f050 6baa4f98 clr!WaitForMultipleObjectsEx_SO_TOLERANT+0x56
0639f070 6baa4dd8 clr!Thread::DoAppropriateAptStateWait+0x4d
0639f104 6baa4e99 clr!Thread::DoAppropriateWaitWorker+0x17d
0639f170 6ba81329 clr!Thread::DoAppropriateWait+0x60
0639f270 6aa6b5ef clr!WaitHandleNative::CorWaitOneNative+0x196
0639f288 6aa6b5ad mscorlib_ni+0x2ab5ef
0639f2a8 6aa6b570 mscorlib_ni+0x2ab5ad
0639f2f0 6aa6ae5b mscorlib_ni+0x2ab570
0639f300 6a9f7ff4 mscorlib_ni+0x2aae5b
0639f31c 6a9f7f34 mscorlib_ni+0x237ff4
0639f33c 6aa6ade8 mscorlib_ni+0x237f34
0639f354 6b9f21db mscorlib_ni+0x2aade8
0639f364 6ba14a2a clr!CallDescrWorker+0x33
0639f3e0 6ba14bcc clr!CallDescrWorkerWithHandler+0x8e
0639f524 6ba14c01 clr!MethodDesc::CallDescr+0x194
0639f540 6bb8b512 clr!MethodDesc::CallTargetWorker+0x21
0639f74c 6baa5c05 clr!ThreadNative::KickOffThread_Worker+0x1e1
0639f760 6baa5c87 clr!Thread::DoExtraWorkForFinalizer+0x114
```

```
0639f810 6baa5d42 clr!Thread::ShouldChangeAbortToUnload+0x101
0639f870 6baa5dd9 clr!Thread::ShouldChangeAbortToUnload+0x399
0639f894 6bb8b3e5 clr!Thread::ShouldChangeAbortToUnload+0x43a
0639f8ac 6bb8b2e0 clr!ManagedThreadBase::KickOff+0x15
0639f944 6baa5a08 clr!ThreadNative::KickOffThread+0x23e
0639fce4 76573833 clr!Thread::intermediateThreadProc+0x4b
0639fcf0 77c1a9bd kernel32!BaseThreadInitThunk+0xe
0639fd30 00000000 ntdll!_RtlUserThreadStart+0x23

   7  Id: 74c.508 Suspend: 0 Teb: 7ffd4000 Unfrozen
ChildEBP RetAddr
0776fcec 77c3f7c0 ntdll!KiFastSystemCallRet
0776fcf0 765778e0 ntdll!NtDelayExecution+0xc
0776fd58 6ba4cc0a kernel32!SleepEx+0x62
0776fd6c 6ba4cbdb clr!__DangerousSwitchToThread+0x48
0776fd80 6bac878b clr!__SwitchToThread+0x12
0776fe68 76573833 clr!ThreadpoolMgr::GateThreadStart+0x83
0776fe74 77c1a9bd kernel32!BaseThreadInitThunk+0xe
0776feb4 00000000 ntdll!_RtlUserThreadStart+0x23

   8  Id: 74c.f34 Suspend: 0 Teb: 7ff4f000 Unfrozen
ChildEBP RetAddr
0788f370 77c400f0 ntdll!KiFastSystemCallRet
0788f374 76557948 ntdll!NtRemoveIoCompletion+0xc
0788f3a0 6babaeab kernel32!GetQueuedCompletionStatus+0x29
0788f404 6baa5a08 clr!ThreadpoolMgr::CompletionPortThreadStart+0x155
0788f828 76573833 clr!Thread::intermediateThreadProc+0x4b
0788f834 77c1a9bd kernel32!BaseThreadInitThunk+0xe
0788f874 00000000 ntdll!_RtlUserThreadStart+0x23

   9  Id: 74c.e3c Suspend: 0 Teb: 7ff4c000 Unfrozen
ChildEBP RetAddr
0a26f134 77c406a0 ntdll!KiFastSystemCallRet
0a26f138 765777d4 ntdll!NtWaitForSingleObject+0xc
0a26f1a8 6ba51030 kernel32!WaitForSingleObjectEx+0xbe
0a26f1dc 6ba51071 clr!CLREvent::CreateManualEvent+0xf6
0a26f22c 6ba4d3e8 clr!CLREvent::CreateManualEvent+0x137
0a26f26c 6ba4d409 clr!CLREvent::WaitEx+0x126
0a26f280 6bb7ce05 clr!CLREvent::Wait+0x19
0a26f354 6baa5a08 clr!AppDomain::ADUnloadThreadStart+0x2f5
0a26f8f4 76573833 clr!Thread::intermediateThreadProc+0x4b
0a26f900 77c1a9bd kernel32!BaseThreadInitThunk+0xe
0a26f940 00000000 ntdll!_RtlUserThreadStart+0x23
```

```
  10  Id: 74c.b74 Suspend: 0 Teb: 7ff4b000 Unfrozen
ChildEBP RetAddr
0a3ee0b0 77c40690 ntdll!KiFastSystemCallRet
0a3ee0b4 76577e09 ntdll!ZwWaitForMultipleObjects+0xc
0a3ee150 7674c4af kernel32!WaitForMultipleObjectsEx+0x11d
0a3ee1a4 776dcec8 user32!RealMsgWaitForMultipleObjectsEx+0x13c
0a3ee1cc 776c03ef ole32!CCliModalLoop::BlockFn+0x97
0a3ee248 6bab74f3 ole32!CoWaitForMultipleHandles+0xcd
0a3ee2b0 6bab747f clr!MsgWaitHelper+0x80
0a3ee2d0 6baa4dd8 clr!Thread::DoAppropriateAptStateWait+0x39
0a3ee364 6baa4e99 clr!Thread::DoAppropriateWaitWorker+0x17d
0a3ee3d0 6bb8cfed clr!Thread::DoAppropriateWait+0x60
0a3ee420 6bb8d0db clr!Thread::JoinEx+0xd5
0a3ee488 6bb8d1db clr!ThreadNative::DoJoin+0xaf
0a3ee52c 059523c5 clr!ThreadNative::Join+0xf2
WARNING: Frame IP not in any known module. Following frames may be wrong.
0a3ee544 6b9f21db 0x59523c5
0a3ee554 6ba14a2a clr!CallDescrWorker+0x33
0a3ee5d0 6ba14bcc clr!CallDescrWorkerWithHandler+0x8e
0a3ee710 6ba14c01 clr!MethodDesc::CallDescr+0x194
0a3ee72c 6ba14c21 clr!MethodDesc::CallTargetWorker+0x21
0a3ee744 6ba87856 clr!MethodDescCallSite::Call+0x1c
0a3ee908 6ba87ba3 clr!CallWithValueTypes_RetArgSlotWrapper+0x5c
0a3eebd4 6ba87d65 clr!InvokeImpl+0x621
0a3eeca0 6aa7d689 clr!RuntimeMethodHandle::InvokeMethodFast+0x180
0a3eecf4 6aa7d3d0 mscorlib_ni+0x2bd689
0a3eed2c 6aa7bfed mscorlib_ni+0x2bd3d0
0a3eed54 6aa83284 mscorlib_ni+0x2bbfed
0a3eed78 6ba0de7e mscorlib_ni+0x2c3284
0a3eef84 05950988 clr!ListLockEntry::Release+0x68
0a3eefe0 6aa6ae5b 0x5950988
0a3eeff0 6a9f7ff4 mscorlib_ni+0x2aae5b
0a3ef00c 6a9f7f34 mscorlib_ni+0x237ff4
0a3ef02c 6aa6ade8 mscorlib_ni+0x237f34
0a3ef044 6b9f21db mscorlib_ni+0x2aade8
0a3ef054 6ba14a2a clr!CallDescrWorker+0x33
0a3ef0d0 6ba14bcc clr!CallDescrWorkerWithHandler+0x8e
0a3ef208 6ba14c01 clr!MethodDesc::CallDescr+0x194
0a3ef224 6bb8b512 clr!MethodDesc::CallTargetWorker+0x21
0a3ef430 6baa5c05 clr!ThreadNative::KickOffThread_Worker+0x1e1
0a3ef444 6baa5c87 clr!Thread::DoExtraWorkForFinalizer+0x114
0a3ef4f4 6baa5d42 clr!Thread::ShouldChangeAbortToUnload+0x101
0a3ef554 6ba937a2 clr!Thread::ShouldChangeAbortToUnload+0x399
0a3ef560 6bb76465 clr!Thread::RaiseCrossContextException+0x3f8
0a3ef640 6ba937cf clr!Thread::DoADCallBack+0xf0
0a3ef660 6baa5c87 clr!Thread::DoExtraWorkForFinalizer+0xfa
0a3ef710 6baa5d42 clr!Thread::ShouldChangeAbortToUnload+0x101
0a3ef770 6baa5dd9 clr!Thread::ShouldChangeAbortToUnload+0x399
0a3ef794 6bb8b3e5 clr!Thread::ShouldChangeAbortToUnload+0x43a
0a3ef7ac 6bb8b2e0 clr!ManagedThreadBase::KickOff+0x15
0a3ef844 6baa5a08 clr!ThreadNative::KickOffThread+0x23e
0a3efe5c 76573833 clr!Thread::intermediateThreadProc+0x4b
0a3efe68 77c1a9bd kernel32!BaseThreadInitThunk+0xe
0a3efea8 00000000 ntdll!_RtlUserThreadStart+0x23
```

```
  11  Id: 74c.3cc Suspend: 0 Teb: 7ff4d000 Unfrozen
ChildEBP RetAddr
09d2e690 77c40690 ntdll!KiFastSystemCallRet
09d2e694 76577e09 ntdll!ZwWaitForMultipleObjects+0xc
09d2e730 6baa516a kernel32!WaitForMultipleObjectsEx+0x11d
09d2e794 6baa4f98 clr!WaitForMultipleObjectsEx_SO_TOLERANT+0x56
09d2e7b4 6baa4dd8 clr!Thread::DoAppropriateAptStateWait+0x4d
09d2e848 6baa4e99 clr!Thread::DoAppropriateWaitWorker+0x17d
09d2e8b4 6baa4f17 clr!Thread::DoAppropriateWait+0x60
09d2e908 6ba4d409 clr!CLREvent::WaitEx+0x106
09d2e91c 6bb90160 clr!CLREvent::Wait+0x19
09d2e9ac 6bb90256 clr!AwareLock::EnterEpilogHelper+0xa8
09d2e9ec 6bb9029b clr!AwareLock::EnterEpilog+0x42
09d2ea0c 6ba90f78 clr!AwareLock::Enter+0x5f
09d2eaa8 05952499 clr!JIT_MonEnterWorker_Portable+0xf8
WARNING: Frame IP not in any known module. Following frames may be wrong.
09d2ead0 6aa6ae5b 0x5952499
09d2eae0 6a9f7ff4 mscorlib_ni+0x2aae5b
09d2eafc 6a9f7f34 mscorlib_ni+0x237ff4
09d2eb1c 6aa6ade8 mscorlib_ni+0x237f34
09d2eb34 6b9f21db mscorlib_ni+0x2aade8
09d2eb44 6ba14a2a clr!CallDescrWorker+0x33
09d2ebc0 6ba14bcc clr!CallDescrWorkerWithHandler+0x8e
09d2ecf8 6ba14c01 clr!MethodDesc::CallDescr+0x194
09d2ed14 6bb8b512 clr!MethodDesc::CallTargetWorker+0x21
09d2ef20 6baa5c05 clr!ThreadNative::KickOffThread_Worker+0x1e1
09d2ef34 6baa5c87 clr!Thread::DoExtraWorkForFinalizer+0x114
09d2efe4 6baa5d42 clr!Thread::ShouldChangeAbortToUnload+0x101
09d2f044 6ba937a2 clr!Thread::ShouldChangeAbortToUnload+0x399
09d2f050 6bb76465 clr!Thread::RaiseCrossContextException+0x3f8
09d2f130 6ba937cf clr!Thread::DoADCallBack+0xf0
09d2f150 6baa5c87 clr!Thread::DoExtraWorkForFinalizer+0xfa
09d2f200 6baa5d42 clr!Thread::ShouldChangeAbortToUnload+0x101
09d2f260 6baa5dd9 clr!Thread::ShouldChangeAbortToUnload+0x399
09d2f284 6bb8b3e5 clr!Thread::ShouldChangeAbortToUnload+0x43a
09d2f29c 6bb8b2e0 clr!ManagedThreadBase::KickOff+0x15
09d2f334 6baa5a08 clr!ThreadNative::KickOffThread+0x23e
09d2f9d0 76573833 clr!Thread::intermediateThreadProc+0x4b
09d2f9dc 77c1a9bd kernel32!BaseThreadInitThunk+0xe
09d2fa1c 00000000 ntdll!_RtlUserThreadStart+0x23
```

```
  12  Id: 74c.ae4 Suspend: 0 Teb: 7ff48000 Unfrozen
ChildEBP RetAddr
0ac2e910 77c40690 ntdll!KiFastSystemCallRet
0ac2e914 76577e09 ntdll!ZwWaitForMultipleObjects+0xc
0ac2e9b0 6baa516a kernel32!WaitForMultipleObjectsEx+0x11d
0ac2ea14 6baa4f98 clr!WaitForMultipleObjectsEx_SO_TOLERANT+0x56
0ac2ea34 6baa4dd8 clr!Thread::DoAppropriateAptStateWait+0x4d
0ac2eac8 6baa4e99 clr!Thread::DoAppropriateWaitWorker+0x17d
0ac2eb34 6baa4f17 clr!Thread::DoAppropriateWait+0x60
0ac2eb88 6ba4d409 clr!CLREvent::WaitEx+0x106
0ac2eb9c 6bb90160 clr!CLREvent::Wait+0x19
0ac2ec2c 6bb90256 clr!AwareLock::EnterEpilogHelper+0xa8
0ac2ec6c 6bb9029b clr!AwareLock::EnterEpilog+0x42
0ac2ec8c 6ba90f78 clr!AwareLock::Enter+0x5f
0ac2ed28 05956ace clr!JIT_MonEnterWorker_Portable+0xf8
WARNING: Frame IP not in any known module. Following frames may be wrong.
0ac2ed30 6aa6ae5b 0x5956ace
0ac2ed40 6a9f7ff4 mscorlib_ni+0x2aae5b
0ac2ed5c 6a9f7f34 mscorlib_ni+0x237ff4
0ac2ed7c 6aa6ade8 mscorlib_ni+0x237f34
0ac2ed94 6b9f21db mscorlib_ni+0x2aade8
0ac2eda4 6ba14a2a clr!CallDescrWorker+0x33
0ac2ee20 6ba14bcc clr!CallDescrWorkerWithHandler+0x8e
0ac2ef58 6ba14c01 clr!MethodDesc::CallDescr+0x194
0ac2ef74 6bb8b512 clr!MethodDesc::CallTargetWorker+0x21
0ac2f180 6baa5c05 clr!ThreadNative::KickOffThread_Worker+0x1e1
0ac2f194 6baa5c87 clr!Thread::DoExtraWorkForFinalizer+0x114
0ac2f244 6baa5d42 clr!Thread::ShouldChangeAbortToUnload+0x101
0ac2f2a4 6ba937a2 clr!Thread::ShouldChangeAbortToUnload+0x399
0ac2f2b0 6bb76465 clr!Thread::RaiseCrossContextException+0x3f8
0ac2f390 6ba937cf clr!Thread::DoADCallBack+0xf0
0ac2f3b0 6baa5c87 clr!Thread::DoExtraWorkForFinalizer+0xfa
0ac2f460 6baa5d42 clr!Thread::ShouldChangeAbortToUnload+0x101
0ac2f4c0 6baa5dd9 clr!Thread::ShouldChangeAbortToUnload+0x399
0ac2f4e4 6bb8b3e5 clr!Thread::ShouldChangeAbortToUnload+0x43a
0ac2f4fc 6bb8b2e0 clr!ManagedThreadBase::KickOff+0x15
0ac2f594 6baa5a08 clr!ThreadNative::KickOffThread+0x23e
0ac2fdac 76573833 clr!Thread::intermediateThreadProc+0x4b
0ac2fdb8 77c1a9bd kernel32!BaseThreadInitThunk+0xe
0ac2fdf8 00000000 ntdll!_RtlUserThreadStart+0x23

  13  Id: 74c.8fc Suspend: 0 Teb: 7ffd8000 Unfrozen
ChildEBP RetAddr
0a8bfbd8 77c400f0 ntdll!KiFastSystemCallRet
0a8bfbdc 76557948 ntdll!NtRemoveIoCompletion+0xc
0a8bfc08 7665af2e kernel32!GetQueuedCompletionStatus+0x29
0a8bfc44 7665b067 rpcrt4!COMMON_ProcessCalls+0xb5
0a8bfcb0 7665ac4f rpcrt4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
0a8bfcbc 7665acb9 rpcrt4!ProcessIOEventsWrapper+0xe
0a8bfce0 7665ad03 rpcrt4!BaseCachedThreadRoutine+0x5c
0a8bfcec 76573833 rpcrt4!ThreadStartRoutine+0x1e
0a8bfcf8 77c1a9bd kernel32!BaseThreadInitThunk+0xe
0a8bfd38 00000000 ntdll!_RtlUserThreadStart+0x23
```

Note: We see that almost all threads have **clr** module on their stack traces.

7. Now we load the appropriate SOS extension after checking that it is not loaded and verifying **clr** module version:

```
0:000> .chain
Extension DLL search Path:
[...]
Extension DLL chain:
    dbghelp: image 6.12.0002.633, API 6.1.6, built Mon Feb 01 20:08:26 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\dbghelp.dll]
    ext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:31 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\winext\ext.dll]
    exts: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:24 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\WINXP\exts.dll]
    uext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:23 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\winext\uext.dll]
    ntsdexts: image 6.1.7650.0, API 1.0.0, built Mon Feb 01 20:08:08 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\WINXP\ntsdexts.dll]

0:000> lmv m clr
start    end        module name
6b9f0000 6c05f000   clr        (pdb symbols)
c:\mss\clr.pdb\C58C9AF63E5D49A8BE0DBA9C5E0093BE2\clr.pdb
    Loaded symbol image file: clr.dll
    Image path: C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.dll
    Image name: clr.dll
    Timestamp:        Thu Mar 18 07:44:47 2010 (4BA1D9EF)
    CheckSum:         00671FC0
    ImageSize:        0066F000
    File version:     4.0.30319.1
    Product version:  4.0.30319.1
    File flags:       8 (Mask 3F) Private
    File OS:          4 Unknown Win32
    File type:        2.0 Dll
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      Microsoft Corporation
    ProductName:      Microsoft® .NET Framework
    InternalName:     clr.dll
    OriginalFilename: clr.dll
    ProductVersion:   4.0.30319.1
    FileVersion:      4.0.30319.1 (RTMRel.030319-0100)
    PrivateBuild:     DDBLD766
    FileDescription:  Microsoft .NET Runtime Common Language Runtime - WorkStation
    LegalCopyright:   © Microsoft Corporation.  All rights reserved.
    Comments:         Flavor=Retail

0:000> .load C:\ANETMDA-Dumps\32-bit\Microsoft.NET\Framework\v4.0.30319\sos

0:000> .chain
Extension DLL search Path:
[...]
Extension DLL chain:
    C:\ANETMDA-Dumps\32-bit\Microsoft.NET\Framework\v4.0.30319\sos: image 4.0.30319.1, API
1.0.0, built Thu Mar 18 08:09:41 2010
        [path: C:\ANETMDA-Dumps\32-bit\Microsoft.NET\Framework\v4.0.30319\sos.dll]
    dbghelp: image 6.12.0002.633, API 6.1.6, built Mon Feb 01 20:08:26 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\dbghelp.dll]
    ext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:31 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\winext\ext.dll]
    exts: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:24 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\WINXP\exts.dll]
```

```
    uext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:23 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\winext\uext.dll]
    ntsdexts: image 6.1.7650.0, API 1.0.0, built Mon Feb 01 20:08:08 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\WINXP\ntsdexts.dll]
```

8. Now we check managed threads and list special CLR threads (**!Threads -special** command):

```
0:000> !Threads -special
ThreadCount:      13
UnstartedThread:  0
BackgroundThread: 7
PendingThread:    0
DeadThread:       3
Hosted Runtime:   no
                                     PreEmptive   GC Alloc                 Lock
       ID  OSID ThreadOBJ    State GC           Context       Domain   Count APT Exception
   0    1   844 002fbe88      6020 Enabled  098eacc0:098eb774 002f17d0     0 STA
   2    2   aa4 00306b18      b220 Enabled  00000000:00000000 002f17d0     0 MTA (Finalizer)
   3    3   30c 00358430      b220 Enabled  00000000:00000000 002f17d0     0 MTA
XXXX    5       003ba928     19820 Enabled  00000000:00000000 002f17d0     0 Ukn
   5    6   e9c 003b2290   200b220 Enabled  00000000:00000000 002f17d0     0 MTA
XXXX    7       05042838     19820 Enabled  00000000:00000000 002f17d0     0 Ukn
   6    4   9e4 0509b610   200b220 Enabled  00000000:00000000 002f17d0     0 MTA
   8    8   f34 050b8ee0   8009220 Enabled  00000000:00000000 002f17d0     0 MTA (Threadpool Completion
Port)
   9    b   e3c 050d1b48      1220 Enabled  00000000:00000000 002f17d0     0 Ukn
  10    c   b74 05109fe0   2007220 Enabled  00000000:00000000 09f1d868     0 STA
  11    d   3cc 05118530   200b020 Enabled  00000000:00000000 09f1d868     1 MTA
XXXX    e       0511a920   1019820 Enabled  00000000:00000000 002f17d0     0 Ukn (Threadpool Worker)
  12    a   ae4 050eb8a8   200b020 Enabled  00000000:00000000 09f1d868     1 MTA
```

	OSID	Special thread type
1	b30	DbgHelper
2	aa4	Finalizer
7	508	Gate
8	f34	IOCompletion
9	e3c	ADUnloadHelper

Note: The application was reported hanging, so we check **Lock Count** ID threads. Thread No 3 is blocked on a named pipe.

```
0:000> ~3s

0:003> kL
ChildEBP RetAddr
046af440 77c3f9c0 ntdll!KiFastSystemCallRet
046af444 7653f00d ntdll!NtFsControlFile+0xc
046af488 68ef80b7 kernel32!ConnectNamedPipe+0x52
046af4f8 68f8c07c System_Core_ni+0x3080b7
046af5a0 6aa6ae5b System_Core_ni+0x39c07c
046af5b0 6a9f7ff4 mscorlib_ni+0x2aae5b
046af5cc 6a9f7f34 mscorlib_ni+0x237ff4
046af5ec 6aa6ade8 mscorlib_ni+0x237f34
046af604 6b9f21db mscorlib_ni+0x2aade8
046af614 6ba14a2a clr!CallDescrWorker+0x33
046af690 6ba14bcc clr!CallDescrWorkerWithHandler+0x8e
046af7d4 6ba14c01 clr!MethodDesc::CallDescr+0x194
046af7f0 6bb8b512 clr!MethodDesc::CallTargetWorker+0x21
046af9fc 6baa5c05 clr!ThreadNative::KickOffThread_Worker+0x1e1
```

```
046afa10 6baa5c87 clr!Thread::DoExtraWorkForFinalizer+0x114
046afac0 6baa5d42 clr!Thread::ShouldChangeAbortToUnload+0x101
046afb20 6baa5dd9 clr!Thread::ShouldChangeAbortToUnload+0x399
046afb44 6bb8b3e5 clr!Thread::ShouldChangeAbortToUnload+0x43a
046afb5c 6bb8b2e0 clr!ManagedThreadBase::KickOff+0x15
046afbf4 6baa5a08 clr!ThreadNative::KickOffThread+0x23e
046afd14 76573833 clr!Thread::intermediateThreadProc+0x4b
046afd20 77c1a9bd kernel32!BaseThreadInitThunk+0xe
046afd60 00000000 ntdll!_RtlUserThreadStart+0x23
```

9. We suspect a deadlock between threads 11 (**d**) and 12 (**a**) and check that using **!syncblk** command:

```
0:003> !syncblk
Index SyncBlock MonitorHeld Recursion Owning Thread Info  SyncBlock Owner
  386 050e86cc            3         1 050eb8a8 ae4  12   097b0dac System.String
  390 050e8664            3         1 05118530 3cc  11   097b0d78 System.String
-----------------------------
Total           392
CCW             108
RCW             28
ComClassFactory 0
Free            53
```

Note: What we see here is that thread 12 (**a**) holds a lock on **050e86cc** synchronization block that is owned by **097b0dac** String object with "**critical section 2**" value:

```
0:003> !DumpObj 097b0dac
Name:        System.String
MethodTable: 6aadf9ac
EEClass:     6a818bb0
Size:        50(0x32) bytes
File:
C:\Windows\Microsoft.Net\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll
String:      critical section 2
Fields:
      MT    Field   Offset                 Type VT     Attr    Value Name
6aae2978  40000ed        4         System.Int32  1 instance       18 m_stringLength
6aae1dc8  40000ee        8          System.Char  1 instance       63 m_firstChar
6aadf9ac  40000ef        8        System.String  0   shared   static Empty
    >> Domain:Value  002f17d0:01881228 09f1d868:01881228 <<
```

and that thread 11 (**d**) holds a lock on **050e8664** block that is owned by **097b0d78** String object with "**critical section 1**" value:

```
0:003> !DumpObj 097b0d78
Name:        System.String
MethodTable: 6aadf9ac
EEClass:     6a818bb0
Size:        50(0x32) bytes
File:
C:\Windows\Microsoft.Net\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll
String:      critical section 1
Fields:
      MT    Field   Offset                 Type VT     Attr    Value Name
6aae2978  40000ed        4         System.Int32  1 instance       18 m_stringLength
6aae1dc8  40000ee        8          System.Char  1 instance       63 m_firstChar
6aadf9ac  40000ef        8        System.String  0   shared   static Empty
    >> Domain:Value  002f17d0:01881228 09f1d868:01881228 <<
```

10. However, to see what blocks they are waiting for we need to inspect their stack traces:

```
0:003> ~11k 10
ChildEBP RetAddr
09d2e690 77c40690 ntdll!KiFastSystemCallRet
09d2e694 76577e09 ntdll!ZwWaitForMultipleObjects+0xc
09d2e730 6baa516a kernel32!WaitForMultipleObjectsEx+0x11d
09d2e794 6baa4f98 clr!WaitForMultipleObjectsEx_SO_TOLERANT+0x56
09d2e7b4 6baa4dd8 clr!Thread::DoAppropriateAptStateWait+0x4d
09d2e848 6baa4e99 clr!Thread::DoAppropriateWaitWorker+0x17d
09d2e8b4 6baa4f17 clr!Thread::DoAppropriateWait+0x60
09d2e908 6ba4d409 clr!CLREvent::WaitEx+0x106
09d2e91c 6bb90160 clr!CLREvent::Wait+0x19
09d2e9ac 6bb90256 clr!AwareLock::EnterEpilogHelper+0xa8
09d2e9ec 6bb9029b clr!AwareLock::EnterEpilog+0x42
09d2ea0c 6ba90f78 clr!AwareLock::Enter+0x5f
09d2eaa8 05952499 clr!JIT_MonEnterWorker_Portable+0xf8
WARNING: Frame IP not in any known module. Following frames may be wrong.
09d2ead0 6aa6ae5b 0x5952499
09d2eae0 6a9f7ff4 mscorlib_ni+0x2aae5b
09d2eafc 6a9f7f34 mscorlib_ni+0x237ff4

0:003> !IP2MD 0x5952499
MethodDesc:   05982108
Method Name:  UserQuery+ClassMain.thread_proc_1()
Class:        05974170
MethodTable:  0598213c
mdToken:      06000005
Module:       05981048
IsJitted:     yes
CodeAddr:     05952430
Transparency: Critical
```

```
0:003> ub 05952499
05952472 eb10            jmp     05952484
05952474 8b0d28a09902    mov     ecx,dword ptr ds:[299A028h]
0595247a e82d4c0c65      call    mscorlib_ni+0x2570ac (6aa170ac)
0595247f e854fe0966      call    clr!JIT_EndCatch (6b9f22d8)
05952484 b9d0070000      mov     ecx,7D0h
05952489 e894f21466      call    clr!ThreadNative::Sleep (6baa1722)
0595248e 8b0d0cc58802    mov     ecx,dword ptr ds:[288C50Ch]
05952494 e851060a66      call    clr!JIT_MonEnterWorker (6b9f2aea)

0:003> dp 288C50Ch l1
0288c50c  097b0dac
```

Note: We see the thread 11 (**d**) is waiting for the sync block owner (String) from the thread 12 (**a**). We can double check that in the annotated disassembly:

```
0:003> !U 0x5952499
Normal JIT generated code
UserQuery+ClassMain.thread_proc_1()
Begin 05952430, size 97
05952430 55              push    ebp
05952431 8bec            mov     ebp,esp
05952433 57              push    edi
05952434 56              push    esi
05952435 53              push    ebx
05952436 83ec14          sub     esp,14h
05952439 33c0            xor     eax,eax
0595243b 8945e0          mov     dword ptr [ebp-20h],eax
0595243e 8945e4          mov     dword ptr [ebp-1Ch],eax
05952441 8945e8          mov     dword ptr [ebp-18h],eax
05952444 8945ec          mov     dword ptr [ebp-14h],eax
05952447 33c0            xor     eax,eax
05952449 8945e8          mov     dword ptr [ebp-18h],eax
0595244c 8b0d08c58802    mov     ecx,dword ptr ds:[288C508h] ("critical section 1")
05952452 e893060a66      call    clr!JIT_MonEnterWorker (6b9f2aea)
05952457 ff1504219805    call    dword ptr ds:[5982104h] (UserQuery+ClassMain.DoWork(), mdToken: 06000004)
0595245d c7050000000001000000 mov dword ptr ds:[0],1
05952467 8b0d08c58802    mov     ecx,dword ptr ds:[288C508h] ("critical section 1")
0595246d e8460a0a66      call    clr!JIT_MonExitWorker (6b9f2eb8)
05952472 eb10            jmp     05952484
05952474 8b0d28a09902    mov     ecx,dword ptr ds:[299A028h] ("We caught an exception.")
0595247a e82d4c0c65      call    mscorlib_ni+0x2570ac (6aa170ac) (System.Console.WriteLine(System.String), mdToken:
06000919)
0595247f e854fe0966      call    clr!JIT_EndCatch (6b9f22d8)
05952484 b9d0070000      mov     ecx,7D0h
05952489 e894f21466      call    clr!ThreadNative::Sleep (6baa1722)
0595248e 8b0d0cc58802    mov     ecx,dword ptr ds:[288C50Ch] ("critical section 2")
05952494 e851060a66      call    clr!JIT_MonEnterWorker (6b9f2aea)
>>> 05952499 ff1504219805    call    dword ptr ds:[5982104h] (UserQuery+ClassMain.DoWork(), mdToken: 06000004)
0595249f 8b0d0cc58802    mov     ecx,dword ptr ds:[288C50Ch] ("critical section 2")
059524a5 e80e0a0a66      call    clr!JIT_MonExitWorker (6b9f2eb8)
059524aa e8214c0c65      call    mscorlib_ni+0x2570d0 (6aa170d0) (System.Console.get_Out(), mdToken: 060008cd)
059524af 8bc8            mov     ecx,eax
059524b1 8b152ca09902    mov     edx,dword ptr ds:[299A02Ch] ("Thread 1 has finished.")
059524b7 8b01            mov     eax,dword ptr [ecx]
059524b9 8b403c          mov     eax,dword ptr [eax+3Ch]
059524bc ff5010          call    dword ptr [eax+10h]
059524bf 8d65f4          lea     esp,[ebp-0Ch]
059524c2 5b              pop     ebx
059524c3 5e              pop     esi
059524c4 5f              pop     edi
059524c5 5d              pop     ebp
```

```
059524c6 c3              ret
```

11. We repeat the same exercise for the thread 12 (**a**):

```
0:003> ~12kL 10
ChildEBP RetAddr
0ac2e910 77c40690 ntdll!KiFastSystemCallRet
0ac2e914 76577e09 ntdll!ZwWaitForMultipleObjects+0xc
0ac2e9b0 6baa516a kernel32!WaitForMultipleObjectsEx+0x11d
0ac2ea14 6baa4f98 clr!WaitForMultipleObjectsEx_SO_TOLERANT+0x56
0ac2ea34 6baa4dd8 clr!Thread::DoAppropriateAptStateWait+0x4d
0ac2eac8 6baa4e99 clr!Thread::DoAppropriateWaitWorker+0x17d
0ac2eb34 6baa4f17 clr!Thread::DoAppropriateWait+0x60
0ac2eb88 6ba4d409 clr!CLREvent::WaitEx+0x106
0ac2eb9c 6bb90160 clr!CLREvent::Wait+0x19
0ac2ec2c 6bb90256 clr!AwareLock::EnterEpilogHelper+0xa8
0ac2ec6c 6bb9029b clr!AwareLock::EnterEpilog+0x42
0ac2ec8c 6ba90f78 clr!AwareLock::Enter+0x5f
0ac2ed28 05956ace clr!JIT_MonEnterWorker_Portable+0xf8
WARNING: Frame IP not in any known module. Following frames may be wrong.
0ac2ed30 6aa6ae5b 0x5956ace
0ac2ed40 6a9f7ff4 mscorlib_ni+0x2aae5b
0ac2ed5c 6a9f7f34 mscorlib_ni+0x237ff4

0:003> !IP2MD 05956ace
MethodDesc:   05982114
Method Name:  UserQuery+ClassMain.thread_proc_2()
Class:        05974170
MethodTable:  0598213c
mdToken:      06000006
Module:       05981048
IsJitted:     yes
CodeAddr:     05956ab0
Transparency: Critical

0:003> ub 05956ace
05956aab 0514219805      add     eax,5982114h
05956ab0 55              push    ebp
05956ab1 8bec            mov     ebp,esp
05956ab3 8b0d0cc58802    mov     ecx,dword ptr ds:[288C50Ch]
05956ab9 e82cc00966      call    clr!JIT_MonEnterWorker (6b9f2aea)
05956abe e81dbaffff      call    059524e0
05956ac3 8b0d08c58802    mov     ecx,dword ptr ds:[288C508h]
05956ac9 e81cc00966      call    clr!JIT_MonEnterWorker (6b9f2aea)

0:003> dp 288C508h l1
0288c508  097b0d78
```

```
0:003> !U 0x5956ace
Normal JIT generated code
UserQuery+ClassMain.thread_proc_2()
Begin 05956ab0, size 64
05956ab0 55              push    ebp
05956ab1 8bec            mov     ebp,esp
05956ab3 8b0d0cc58802    mov     ecx,dword ptr ds:[288C50Ch] ("critical section 2")
05956ab9 e82cc00966      call    clr!JIT_MonEnterWorker (6b9f2aea)
05956abe e81dbaffff      call    059524e0 (UserQuery+ClassMain.DoWork(), mdToken: 06000004)
05956ac3 8b0d08c58802    mov     ecx,dword ptr ds:[288C508h] ("critical section 1")
05956ac9 e81cc00966      call    clr!JIT_MonEnterWorker (6b9f2aea)
>>> 05956ace e80dbaffff      call    059524e0 (UserQuery+ClassMain.DoWork(), mdToken: 06000004)
05956ad3 b9b80b0000      mov     ecx,0BB8h
05956ad8 e845ac1466      call    clr!ThreadNative::Sleep (6baa1722)
05956add e8feb9ffff      call    059524e0 (UserQuery+ClassMain.DoWork(), mdToken: 06000004)
05956ae2 8b0d08c58802    mov     ecx,dword ptr ds:[288C508h] ("critical section 1")
05956ae8 e8cbc30966      call    clr!JIT_MonExitWorker (6b9f2eb8)
05956aed e8eeb9ffff      call    059524e0 (UserQuery+ClassMain.DoWork(), mdToken: 06000004)
05956af2 8b0d0cc58802    mov     ecx,dword ptr ds:[288C50Ch] ("critical section 2")
05956af8 e8bbc30966      call    clr!JIT_MonExitWorker (6b9f2eb8)
05956afd e8ce050c65      call    mscorlib_ni+0x2570d0 (6aa170d0) (System.Console.get_Out(), mdToken: 060008cd)
05956b02 8bc8            mov     ecx,eax
05956b04 8b15b4a09902    mov     edx,dword ptr ds:[299A0B4h] ("Thread 2 has finished.")
05956b0a 8b01            mov     eax,dword ptr [ecx]
05956b0c 8b403c          mov     eax,dword ptr [eax+3Ch]
05956b0f ff5010          call    dword ptr [eax+10h]
05956b12 5d              pop     ebp
05956b13 c3              ret
```

Note: We see the thread 12 (**a**) is waiting for the sync block owner (String) from the thread 11 (**d**). Since both threads are mutually waiting for each other, we consider them as deadlocked.

12. This was a very lengthy manual exercise which can be automated by SOSEX extension **!dlk** command:

```
0:003> .load C:\ANETMDA-Dumps\32-bit\SOSEX\sosex

0:003> !dlk
Examining SyncBlocks...
Scanning for ReaderWriterLock instances...
Scanning for holders of ReaderWriterLock locks...
Scanning for ReaderWriterLockSlim instances...
Scanning for holders of ReaderWriterLockSlim locks...
Examining CriticalSections...
Scanning for threads waiting on SyncBlocks...
```

```
[...]
Scanning for threads waiting on ReaderWriterLock locks...
Scanning for threads waiting on ReaderWriterLocksSlim locks...
Scanning for threads waiting on CriticalSections...
*DEADLOCK DETECTED*
CLR thread 0xd holds the lock on SyncBlock 050e8664 OBJ:097b0d78[System.String] STRVAL=critical section 1
...and is waiting for the lock on SyncBlock 050e86cc OBJ:097b0dac[System.String] STRVAL=critical section 2
CLR thread 0xa holds the lock on SyncBlock 050e86cc OBJ:097b0dac[System.String] STRVAL=critical section 2
...and is waiting for the lock on SyncBlock 050e8664 OBJ:097b0d78[System.String] STRVAL=critical section 1
CLR Thread 0xd is waiting at UserQuery+ClassMain.thread_proc_1()(+0x42 IL)(+0x69 Native)
CLR Thread 0xa is waiting at UserQuery+ClassMain.thread_proc_2()(+0x19 IL)(+0x1e Native)


1 deadlock detected.
```

13. How did this deadlock happen? If we look at both threads execution residue we would see that in the case of the thread No. 11 exception was thrown and handled but there was no a finally block to release the lock:

```
0:003> ~11s
eax=09d2d968 ebx=00000001 ecx=098de550 edx=098df350 esi=00000000 edi=00000000
eip=77c40f34 esp=09d2e694 ebp=09d2e730 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
ntdll!KiFastSystemCallRet:
77c40f34 c3              ret

0:011> !DumpStack
OS Thread Id: 0x3cc (11)
Current frame: ntdll!KiFastSystemCallRet
ChildEBP RetAddr  Caller, Callee
09d2e690 77c40690 ntdll!ZwWaitForMultipleObjects+0xc
09d2e694 76577e09 kernel32!WaitForMultipleObjectsEx+0x11d, calling ntdll!NtWaitForMultipleObjects
09d2e6d8 76578101 kernel32!WaitForMultipleObjectsEx+0x33, calling ntdll!RtlActivateActivationContextUnsafeFast
09d2e6e4 77c41039 ntdll!ExecuteHandler2+0x26
09d2e708 77c4100b ntdll!ExecuteHandler+0x24, calling ntdll!ExecuteHandler2
09d2e730 6baa516a clr!WaitForMultipleObjectsEx_SO_TOLERANT+0x56, calling kernel32!WaitForMultipleObjectsEx
09d2e794 6baa4f98 clr!Thread::DoAppropriateAptStateWait+0x4d, calling clr!WaitForMultipleObjectsEx_SO_TOLERANT
09d2e7b4 6baa4dd8 clr!Thread::DoAppropriateWaitWorker+0x17d, calling clr!Thread::DoAppropriateAptStateWait
09d2e848 6baa4e99 clr!Thread::DoAppropriateWait+0x60, calling clr!Thread::DoAppropriateWaitWorker
09d2e8b4 6baa4f17 clr!CLREvent::WaitEx+0x106, calling clr!Thread::DoAppropriateWait
09d2e8e0 6baa484b clr!CLRGetTickCount64+0x6b, calling clr!_allmul
09d2e908 6ba4d409 clr!CLREvent::Wait+0x19, calling clr!CLREvent::WaitEx
09d2e91c 6bb90160 clr!AwareLock::EnterEpilogHelper+0xa8, calling clr!CLREvent::Wait
09d2e984 6b9f1c5c clr!UnsafeEELeaveCriticalSection+0x21, calling  (JitHelp: CORINFO_HELP_GET_THREAD)
09d2e98c 6b9f1c8f clr!CrstBase::Leave+0x2b, calling clr!UnsafeEELeaveCriticalSection
09d2e9ac 6bb90256 clr!AwareLock::EnterEpilog+0x42, calling clr!AwareLock::EnterEpilogHelper
09d2e9ec 6bb9029b clr!AwareLock::Enter+0x5f, calling clr!AwareLock::EnterEpilog
09d2ea0c 6ba90f78 clr!JIT_MonEnterWorker_Portable+0xf8, calling clr!ObjHeader::EnterObjMonitor
09d2ea50 6ba90ed7 clr!JIT_MonEnterWorker_Portable+0x21, calling clr!LazyMachStateCaptureState
09d2eaa8 05952499 (MethodDesc 05982108 +0x69 UserQuery+ClassMain.thread_proc_1()), calling clr!JIT_MonEnterWorker
09d2ead0 6aa6ae5b (MethodDesc 6a8ae4d4 +0x63 System.Threading.ThreadHelper.ThreadStart_Context(System.Object))
09d2eae0 6a9f7ff4 (MethodDesc 6a8375e8 +0xb0 System.Threading.ExecutionContext.Run(System.Threading.ExecutionContext,
System.Threading.ContextCallback, System.Object, Boolean))
09d2eafc 6a9f7f34 (MethodDesc 6a8375dc +0x2c System.Threading.ExecutionContext.Run(System.Threading.ExecutionContext,
System.Threading.ContextCallback, System.Object)), calling (MethodDesc 6a8375e8 +0
```

```
System.Threading.ExecutionContext.Run(System.Threading.ExecutionContext, System.Threading.ContextCallback,
System.Object, Boolean))
09d2eb1c 6aa6ade8 (MethodDesc 6a8286c0 +0x44 System.Threading.ThreadHelper.ThreadStart()), calling (MethodDesc
6a8375dc +0 System.Threading.ExecutionContext.Run(System.Threading.ExecutionContext, System.Threading.ContextCallback,
System.Object))
09d2eb34 6b9f21db clr!CallDescrWorker+0x33
09d2eb44 6ba14a2a clr!CallDescrWorkerWithHandler+0x8e, calling clr!CallDescrWorker
09d2eb98 6ba0c58d clr!ArgIterator::Init+0x6b, calling clr!MetaSig::HasRetBuffArg
09d2ebc0 6ba14bcc clr!MethodDesc::CallDescr+0x194, calling clr!CallDescrWorkerWithHandler
09d2ebec 6ba128bb clr!MetaSig::MetaSig+0x3c, calling MSVCR100_CLR0400!memcpy
09d2ebfc 6ba14b0a clr!MethodDesc::CallDescr+0xa8, calling clr!ClrSafeInt<unsigned long>::addition
09d2ec08 6ba14b1a clr!MethodDesc::CallDescr+0xb4, calling clr!_alloca_probe_16
09d2ec6c 77c418c3 ntdll!RtlFreeHeap+0x101, calling ntdll!RtlpLowFragHeapFree
09d2ec80 76577a7e kernel32!HeapFree+0x14, calling ntdll!RtlFreeHeap
09d2ec94 6ba4c036 clr!EEHeapFree+0x36, calling kernel32!HeapFree
09d2eca8 6ba4c09d clr!EEHeapFreeInProcessHeap+0x24, calling clr!EEHeapFree
09d2ecf8 6ba14c01 clr!MethodDesc::CallTargetWorker+0x21, calling clr!MethodDesc::CallDescr
09d2ed14 6bb8b512 clr!ThreadNative::KickOffThread_Worker+0x1e1, calling clr!MethodDesc::CallTargetWorker
09d2ed6c 77c1c257 ntdll!RtlFindNextActivationContextSection+0x46, calling ntdll!RtlpFindNextActivationContextSection
09d2ede0 77c1b913 ntdll!WinSqmAddToStream+0x7d0, calling ntdll!RtlFindActivationContextSectionString
09d2edfc 77c1b973 ntdll!WinSqmAddToStream+0x8e5, calling ntdll!__security_check_cookie
09d2eebc 77c418c3 ntdll!RtlFreeHeap+0x101, calling ntdll!RtlpLowFragHeapFree
09d2eed0 76577a7e kernel32!HeapFree+0x14, calling ntdll!RtlFreeHeap
09d2eee4 6ba4c036 clr!EEHeapFree+0x36, calling kernel32!HeapFree
09d2eef8 6ba4c09d clr!EEHeapFreeInProcessHeap+0x24, calling clr!EEHeapFree
09d2ef20 6baa5c05 clr!Thread::DoExtraWorkForFinalizer+0x114
09d2ef34 6baa5c87 clr!Thread::ShouldChangeAbortToUnload+0x101, calling clr!Thread::DoExtraWorkForFinalizer+0xb7
09d2ef58 6b9f19c1 clr!StressLog::LogOn+0x1e, calling clr!StressLog::ETWLogOn
09d2ef74 6bab8fca clr!Thread::SetLastThrownObject+0x100, calling clr!_EH_epilog3
09d2efa8 6bab9038 clr!Thread::SafeSetLastThrownObject+0x161, calling clr!_EH_epilog3_catch_GS
09d2efe4 6baa5d42 clr!Thread::ShouldChangeAbortToUnload+0x399, calling clr!Thread::ShouldChangeAbortToUnload+0x34
09d2f044 6ba937a2 clr!Thread::RaiseCrossContextException+0x3f8, calling clr!Thread::ShouldChangeAbortToUnload+0x33c
09d2f050 6bb76465 clr!Thread::DoADCallBack+0xf0
09d2f0b4 77c41843 ntdll!RtlpLowFragHeapAllocFromContext+0xa6f, calling ntdll!_SEH_epilog4
09d2f0b8 77c416dc ntdll!RtlAllocateHeap+0x17c, calling ntdll!RtlpLowFragHeapAllocFromContext
09d2f0e8 77c41843 ntdll!RtlpLowFragHeapAllocFromContext+0xa6f, calling ntdll!_SEH_epilog4
09d2f100 7655a863 kernel32!GetSystemInfoInternal+0xb4, calling kernel32!GetProcessVersion
09d2f130 6ba937cf clr!Thread::DoExtraWorkForFinalizer+0xfa, calling clr!Thread::DoADCallBack
09d2f150 6baa5c87 clr!Thread::ShouldChangeAbortToUnload+0x101, calling clr!Thread::DoExtraWorkForFinalizer+0xb7
09d2f168 6b9f1d85 clr!UnsafeEETryEnterCriticalSection+0xf, calling ntdll!RtlTryEnterCriticalSection
09d2f16c 6b9f1d9e clr!UnsafeEETryEnterCriticalSection+0x28, calling  (JitHelp: CORINFO_HELP_GET_THREAD)
09d2f178 6b9f1d55 clr!CrstBase::Enter+0xb4, calling clr!UnsafeEETryEnterCriticalSection
09d2f190 6b9f191f clr!ClrFlsGetValue+0xb, calling 018407e8
09d2f198 6b9f191f clr!ClrFlsGetValue+0xb, calling 018407e8
09d2f1a0 6b9f1e36 clr!DecCantStopCount+0xa, calling clr!ClrFlsGetValue
09d2f1ac 6ba4dea7 clr!ThreadStore::UnlockThreadStore+0x4b, calling clr!DecCantStopCount
09d2f200 6baa5d42 clr!Thread::ShouldChangeAbortToUnload+0x399, calling clr!Thread::ShouldChangeAbortToUnload+0x34
09d2f260 6baa5dd9 clr!Thread::ShouldChangeAbortToUnload+0x43a, calling clr!Thread::ShouldChangeAbortToUnload+0x33c
09d2f284 6bb8b3e5 clr!ManagedThreadBase::KickOff+0x15, calling clr!Thread::ShouldChangeAbortToUnload+0x403
09d2f29c 6bb8b2e0 clr!ThreadNative::KickOffThread+0x23e, calling clr!ManagedThreadBase::KickOff
09d2f2c4 76577a7e kernel32!HeapFree+0x14, calling ntdll!RtlFreeHeap
09d2f2d8 6ba4c036 clr!EEHeapFree+0x36, calling kernel32!HeapFree
09d2f300 6ba4c06d clr!operator delete[]+0x30, calling clr!EEHeapFreeInProcessHeap
09d2f334 6baa5a08 clr!Thread::intermediateThreadProc+0x4b
09d2f340 77a018a4 urlmon!EnsureFeatureCache+0x36f, calling urlmon!__security_check_cookie
09d2f354 77c42447 ntdll!RtlpAllocateHeap+0xe2f, calling ntdll!_SEH_epilog4
09d2f370 77c42ebb ntdll!RtlInitializeCriticalSectionEx+0x119, calling ntdll!RtlLeaveCriticalSection
09d2f394 77c13600 ntdll!RtlpCreateLowFragHeap+0x28, calling ntdll!RtlpInitializeLowFragHeap
09d2f3b0 77c42f2f ntdll!RtlInitializeCriticalSection+0x12, calling ntdll!RtlInitializeCriticalSectionEx
09d2f3c4 77c13632 ntdll!RtlpInitializeLowFragHeap+0x28, calling ntdll!RtlInitializeCriticalSection
09d2f3d8 77c13600 ntdll!RtlpCreateLowFragHeap+0x28, calling ntdll!RtlpInitializeLowFragHeap
09d2f3e4 77c134e8 ntdll!RtlpActivateLowFragmentationHeap+0x11e, calling ntdll!RtlLeaveCriticalSection
09d2f3e8 77c134fc ntdll!RtlpActivateLowFragmentationHeap+0x132, calling ntdll!_SEH_epilog4
09d2f41c 77c134fc ntdll!RtlpActivateLowFragmentationHeap+0x132, calling ntdll!_SEH_epilog4
09d2f428 77c4648c ntdll!RtlpAllocateHeap+0xc76, calling ntdll!memset
09d2f434 77c42447 ntdll!RtlpAllocateHeap+0xe2f, calling ntdll!_SEH_epilog4
```

```
09d2f448 77c1afe1 ntdll!RtlpAllocateAffinityIndex+0xf5, calling ntdll!_allshl
09d2f470 77c41843 ntdll!RtlpLowFragHeapAllocFromContext+0xa6f, calling ntdll!_SEH_epilog4
09d2f494 77c45ba9 ntdll!RtlpLowFragHeapAllocFromContext+0x805, calling ntdll!RtlpSubSegmentInitialize
09d2f4e4 77c41843 ntdll!RtlpLowFragHeapAllocFromContext+0xa6f, calling ntdll!_SEH_epilog4
09d2f4e8 77c416dc ntdll!RtlAllocateHeap+0x17c, calling ntdll!RtlpLowFragHeapAllocFromContext
09d2f510 77c42447 ntdll!RtlpAllocateHeap+0xe2f, calling ntdll!_SEH_epilog4
09d2f514 77c4214c ntdll!RtlAllocateHeap+0x1e3, calling ntdll!RtlpAllocateHeap
09d2f544 73644358 mscoreei!_CRT_INIT+0x1d0, calling mscoreei!DllMain
09d2f558 77a01c48 urlmon!CUrlMkTls::TLSAllocData+0x3f, calling kernel32!TlsSetValue
09d2f568 77a0198d urlmon!CUrlMkTls::CUrlMkTls+0x29, calling urlmon!CUrlMkTls::TLSAllocData
09d2f574 77a01be5 urlmon!TlsDllMain+0x100, calling urlmon!EnsureFeatureCache
09d2f580 6d016a21 mshtml!DllMain+0x10, calling kernel32!GetCurrentThreadId
09d2f590 6d016b6c mshtml!_CRT_INIT+0x281, calling mshtml!DllMain
09d2f5a8 7239133e msimtf!_CRT_INIT+0x281, calling msimtf!DllMain
09d2f5b4 72391375 msimtf!_CRT_INIT+0x3e7, calling msimtf!_SEH_epilog4
09d2f5f0 6d016ad0 mshtml!_DllMainStartup+0x56, calling mshtml!_DllMainCRTStartup
09d2f604 72391375 msimtf!_CRT_INIT+0x3e7, calling msimtf!_SEH_epilog4
09d2f608 77c4a604 ntdll!LdrpCallInitRoutine+0x14
09d2f630 77c1ab6c ntdll!LdrpInitializeThread+0x1e9, calling ntdll!RtlLeaveCriticalSection
09d2f638 77c1a9ea ntdll!LdrpInitializeThread+0x1cd, calling ntdll!_SEH_epilog4
09d2f68c 77c1ab15 ntdll!LdrpInitializeThread+0x11f, calling ntdll!RtlActivateActivationContextUnsafeFast
09d2f690 77c1ab53 ntdll!LdrpInitializeThread+0x167, calling ntdll!RtlDeactivateActivationContextUnsafeFast
09d2f6c4 77c1a9ea ntdll!LdrpInitializeThread+0x1cd, calling ntdll!_SEH_epilog4
09d2f6c8 77c405a0 ntdll!NtTestAlert+0xc
09d2f6cc 77c1a968 ntdll!_LdrpInitialize+0x29c, calling ntdll!_SEH_epilog4
09d2f72c 77c3f3d0 ntdll!NtContinue+0xc
09d2f730 77c1a98a ntdll!LdrInitializeThunk+0x1a, calling ntdll!NtContinue
09d2f9bc 6baa59f6 clr!Thread::intermediateThreadProc+0x39, calling clr!_alloca_probe_16
09d2f9d0 76573833 kernel32!BaseThreadInitThunk+0xe
09d2f9dc 77c1a9bd ntdll!_RtlUserThreadStart+0x23

0:011> ~12s
eax=0ac2d338 ebx=00000001 ecx=6a7c4f4c edx=00000000 esi=00000000 edi=00000000
eip=77c40f34 esp=0ac2e914 ebp=0ac2e9b0 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
ntdll!KiFastSystemCallRet:
77c40f34 c3              ret

0:012> !DumpStack
OS Thread Id: 0xae4 (12)
Current frame: ntdll!KiFastSystemCallRet
ChildEBP RetAddr  Caller, Callee
0ac2e910 77c40690 ntdll!ZwWaitForMultipleObjects+0xc
0ac2e914 76577e09 kernel32!WaitForMultipleObjectsEx+0x11d, calling ntdll!NtWaitForMultipleObjects
0ac2e958 76578101 kernel32!WaitForMultipleObjectsEx+0x33, calling ntdll!RtlActivateActivationContextUnsafeFast
0ac2e9b0 6baa516a clr!WaitForMultipleObjectsEx_SO_TOLERANT+0x56, calling kernel32!WaitForMultipleObjectsEx
0ac2ea14 6baa4f98 clr!Thread::DoAppropriateAptStateWait+0x4d, calling clr!WaitForMultipleObjectsEx_SO_TOLERANT
0ac2ea34 6baa4dd8 clr!Thread::DoAppropriateWaitWorker+0x17d, calling clr!Thread::DoAppropriateAptStateWait
0ac2eac8 6baa4e99 clr!Thread::DoAppropriateWait+0x60, calling clr!Thread::DoAppropriateWaitWorker
0ac2eb34 6baa4f17 clr!CLREvent::WaitEx+0x106, calling clr!Thread::DoAppropriateWait
0ac2eb60 6baa484b clr!CLRGetTickCount64+0x6b, calling clr!_allmul
0ac2eb88 6ba4d409 clr!CLREvent::Wait+0x19, calling clr!CLREvent::WaitEx
0ac2eb9c 6bb90160 clr!AwareLock::EnterEpilogHelper+0xa8, calling clr!CLREvent::Wait
0ac2ec04 6b9f1c5c clr!UnsafeEELeaveCriticalSection+0x21, calling  (JitHelp: CORINFO_HELP_GET_THREAD)
0ac2ec0c 6b9f1c8f clr!CrstBase::Leave+0x2b, calling clr!UnsafeEELeaveCriticalSection
0ac2ec2c 6bb90256 clr!AwareLock::EnterEpilog+0x42, calling clr!AwareLock::EnterEpilogHelper
0ac2ec6c 6bb9029b clr!AwareLock::Enter+0x5f, calling clr!AwareLock::EnterEpilog
0ac2ec8c 6ba90f78 clr!JIT_MonEnterWorker_Portable+0xf8, calling clr!ObjHeader::EnterObjMonitor
0ac2ecd0 6ba90ed7 clr!JIT_MonEnterWorker_Portable+0x21, calling clr!LazyMachStateCaptureState
0ac2ed28 05956ace (MethodDesc 05982114 +0x1e UserQuery+ClassMain.thread_proc_2()), calling clr!JIT_MonEnterWorker
0ac2ed30 6aa6ae5b (MethodDesc 6a8ae4d4 +0x63 System.Threading.ThreadHelper.ThreadStart_Context(System.Object))
0ac2ed40 6a9f7ff4 (MethodDesc 6a8375e8 +0xb0 System.Threading.ExecutionContext.Run(System.Threading.ExecutionContext,
System.Threading.ContextCallback, System.Object, Boolean))
```

```
0ac2ed5c 6a9f7f34 (MethodDesc 6a8375dc +0x2c System.Threading.ExecutionContext.Run(System.Threading.ExecutionContext,
System.Threading.ContextCallback, System.Object)), calling (MethodDesc 6a8375e8 +0
System.Threading.ExecutionContext.Run(System.Threading.ExecutionContext, System.Threading.ContextCallback,
System.Object, Boolean))
0ac2ed7c 6aa6ade8 (MethodDesc 6a8286c0 +0x44 System.Threading.ThreadHelper.ThreadStart()), calling (MethodDesc
6a8375dc +0 System.Threading.ExecutionContext.Run(System.Threading.ExecutionContext, System.Threading.ContextCallback,
System.Object))
0ac2ed94 6b9f21db clr!CallDescrWorker+0x33
0ac2eda4 6ba14a2a clr!CallDescrWorkerWithHandler+0x8e, calling clr!CallDescrWorker
0ac2edf8 6ba0c58d clr!ArgIterator::Init+0x6b, calling clr!MetaSig::HasRetBuffArg
0ac2ee20 6ba14bcc clr!MethodDesc::CallDescr+0x194, calling clr!CallDescrWorkerWithHandler
0ac2ee4c 6ba128bb clr!MetaSig::MetaSig+0x3c, calling MSVCR100_CLR0400!memcpy
0ac2ee5c 6ba14b0a clr!MethodDesc::CallDescr+0xa8, calling clr!ClrSafeInt<unsigned long>::addition
0ac2ee68 6ba14b1a clr!MethodDesc::CallDescr+0xb4, calling clr!_alloca_probe_16
0ac2eecc 77c418c3 ntdll!RtlFreeHeap+0x101, calling ntdll!RtlpLowFragHeapFree
0ac2eee0 76577a7e kernel32!HeapFree+0x14, calling ntdll!RtlFreeHeap
0ac2eef4 6ba4c036 clr!EEHeapFree+0x36, calling kernel32!HeapFree
0ac2ef08 6ba4c09d clr!EEHeapFreeInProcessHeap+0x24, calling clr!EEHeapFree
0ac2ef58 6ba14c01 clr!MethodDesc::CallTargetWorker+0x21, calling clr!MethodDesc::CallDescr
0ac2ef74 6bb8b512 clr!ThreadNative::KickOffThread_Worker+0x1e1, calling clr!MethodDesc::CallTargetWorker
0ac2f010 77c435c6 ntdll!bsearch+0x70
0ac2f01c 77c43516 ntdll!ARRAY_FITS+0x2d, calling ntdll!ULongAdd
0ac2f030 77c434c8 ntdll!RtlpLocateActivationContextSection+0x1d9, calling ntdll!ARRAY_FITS
0ac2f054 77c1c16a ntdll!RtlpFindUnicodeStringInSection+0x71, calling ntdll!RtlHashUnicodeString
0ac2f094 77c1c257 ntdll!RtlFindNextActivationContextSection+0x46, calling ntdll!RtlpFindNextActivationContextSection
0ac2f11c 77c418c3 ntdll!RtlFreeHeap+0x101, calling ntdll!RtlpLowFragHeapFree
0ac2f130 76577a7e kernel32!HeapFree+0x14, calling ntdll!RtlFreeHeap
0ac2f144 6ba4c036 clr!EEHeapFree+0x36, calling kernel32!HeapFree
0ac2f158 6ba4c09d clr!EEHeapFreeInProcessHeap+0x24, calling clr!EEHeapFree
0ac2f180 6baa5c05 clr!Thread::DoExtraWorkForFinalizer+0x114
0ac2f194 6baa5c87 clr!Thread::ShouldChangeAbortToUnload+0x101, calling clr!Thread::DoExtraWorkForFinalizer+0xb7
0ac2f1b8 6b9f19c1 clr!StressLog::LogOn+0x1e, calling clr!StressLog::ETWLogOn
0ac2f1d4 6bab8fca clr!Thread::SetLastThrownObject+0x100, calling clr!_EH_epilog3
0ac2f208 6bab9038 clr!Thread::SafeSetLastThrownObject+0x161, calling clr!_EH_epilog3_catch_GS
0ac2f244 6baa5d42 clr!Thread::ShouldChangeAbortToUnload+0x399, calling clr!Thread::ShouldChangeAbortToUnload+0x34
0ac2f2a4 6ba937a2 clr!Thread::RaiseCrossContextException+0x3f8, calling clr!Thread::ShouldChangeAbortToUnload+0x33c
0ac2f2b0 6bb76465 clr!Thread::DoADCallBack+0xf0
0ac2f314 77c41843 ntdll!RtlpLowFragHeapAllocFromContext+0xa6f, calling ntdll!_SEH_epilog4
0ac2f318 77c416dc ntdll!RtlAllocateHeap+0x17c, calling ntdll!RtlpLowFragHeapAllocFromContext
0ac2f348 77c41843 ntdll!RtlpLowFragHeapAllocFromContext+0xa6f, calling ntdll!_SEH_epilog4
0ac2f360 7655a863 kernel32!GetSystemInfoInternal+0xb4, calling kernel32!GetProcessVersion
0ac2f390 6ba937cf clr!Thread::DoExtraWorkForFinalizer+0xfa, calling clr!Thread::DoADCallBack
0ac2f3b0 6baa5c87 clr!Thread::ShouldChangeAbortToUnload+0x101, calling clr!Thread::DoExtraWorkForFinalizer+0xb7
0ac2f3c8 6b9f1d85 clr!UnsafeEETryEnterCriticalSection+0xf, calling ntdll!RtlTryEnterCriticalSection
0ac2f3cc 6b9f1d9e clr!UnsafeEETryEnterCriticalSection+0x28, calling  (JitHelp: CORINFO_HELP_GET_THREAD)
0ac2f3d8 6b9f1d55 clr!CrstBase::Enter+0xb4, calling clr!UnsafeEETryEnterCriticalSection
0ac2f3f0 6b9f191f clr!ClrFlsGetValue+0xb, calling 018407e8
0ac2f3f8 6b9f191f clr!ClrFlsGetValue+0xb, calling 018407e8
0ac2f400 6b9f1e36 clr!DecCantStopCount+0xa, calling clr!ClrFlsGetValue
0ac2f40c 6ba4dea7 clr!ThreadStore::UnlockThreadStore+0x4b, calling clr!DecCantStopCount
0ac2f460 6baa5d42 clr!Thread::ShouldChangeAbortToUnload+0x399, calling clr!Thread::ShouldChangeAbortToUnload+0x34
0ac2f4c0 6baa5dd9 clr!Thread::ShouldChangeAbortToUnload+0x43a, calling clr!Thread::ShouldChangeAbortToUnload+0x33c
0ac2f4e4 6bb8b3e5 clr!ManagedThreadBase::KickOff+0x15, calling clr!Thread::ShouldChangeAbortToUnload+0x403
0ac2f4fc 6bb8b2e0 clr!ThreadNative::KickOffThread+0x23e, calling clr!ManagedThreadBase::KickOff
0ac2f524 76577a7e kernel32!HeapFree+0x14, calling ntdll!RtlFreeHeap
0ac2f538 6ba4c036 clr!EEHeapFree+0x36, calling kernel32!HeapFree
0ac2f560 6ba4c06d clr!operator delete[]+0x30, calling clr!EEHeapFreeInProcessHeap
0ac2f594 6baa5a08 clr!Thread::intermediateThreadProc+0x4b
0ac2f59c 7657b6ce kernel32!_BaseDllInitialize+0x92, calling kernel32!ConDllInitialize
0ac2f5b0 7657b6e3 kernel32!_BaseDllInitialize+0x594, calling kernel32!__security_check_cookie
0ac2f630 77c1c485 ntdll!LdrpSnapThunk+0xc9, calling ntdll!LdrpNameToOrdinal
0ac2f644 77c1c4d1 ntdll!LdrpSnapThunk+0x40d, calling ntdll!_SEH_epilog4
0ac2f668 77c1c4d1 ntdll!LdrpSnapThunk+0x40d, calling ntdll!_SEH_epilog4
0ac2f670 77c488d8 ntdll!RtlImageNtHeaderEx+0xf6, calling ntdll!_SEH_epilog4
0ac2f6a4 77c489fd ntdll!RtlpImageDirectoryEntryToDataEx+0x78, calling ntdll!RtlpImageDirectoryEntryToData32
0ac2f6d4 77c1c4d1 ntdll!LdrpSnapThunk+0x40d, calling ntdll!_SEH_epilog4
```

```
0ac2f6d8 77c1c5f7 ntdll!LdrGetProcedureAddressEx+0x1a4, calling ntdll!LdrpSnapThunk
0ac2f6f4 77c1c652 ntdll!LdrGetProcedureAddressEx+0x2b0, calling ntdll!RtlLeaveCriticalSection
0ac2f6f8 77c42d96 ntdll!_SEH_epilog4_GS+0xa, calling ntdll!__security_check_cookie
0ac2f6fc 77c1c628 ntdll!LdrGetProcedureAddressEx+0xb8, calling ntdll!_SEH_epilog4_GS
0ac2f710 77a01c82 urlmon!EnsureFeatureCache+0x58, calling kernel32!TlsSetValue
0ac2f71c 77a018a4 urlmon!EnsureFeatureCache+0x36f, calling urlmon!__security_check_cookie
0ac2f794 77c1c628 ntdll!LdrGetProcedureAddressEx+0xb8, calling ntdll!_SEH_epilog4_GS
0ac2f798 77c0c46f ntdll!LdrpSnapThunk+0x3d7, calling ntdll!LdrGetProcedureAddressEx
0ac2f7ac 77c1c4d1 ntdll!LdrpSnapThunk+0x40d, calling ntdll!_SEH_epilog4
0ac2f7d0 77c41843 ntdll!RtlpLowFragHeapAllocFromContext+0xa6f, calling ntdll!_SEH_epilog4
0ac2f80c 77c489fd ntdll!RtlpImageDirectoryEntryToDataEx+0x78, calling ntdll!RtlpImageDirectoryEntryToData32
0ac2f83c 77c486cd ntdll!RtlAllocateHeap+0x193, calling ntdll!memset
0ac2f84c 77c41843 ntdll!RtlpLowFragHeapAllocFromContext+0xa6f, calling ntdll!_SEH_epilog4
0ac2f860 77c42d96 ntdll!_SEH_epilog4_GS+0xa, calling ntdll!__security_check_cookie
0ac2f864 77c1c628 ntdll!LdrGetProcedureAddressEx+0xb8, calling ntdll!_SEH_epilog4_GS
0ac2f8c0 77c41843 ntdll!RtlpLowFragHeapAllocFromContext+0xa6f, calling ntdll!_SEH_epilog4
0ac2f8c4 77c416dc ntdll!RtlAllocateHeap+0x17c, calling ntdll!RtlpLowFragHeapAllocFromContext
0ac2f8f0 77c486cd ntdll!RtlAllocateHeap+0x193, calling ntdll!memset
0ac2f920 73644358 mscoreei!_CRT_INIT+0x1d0, calling mscoreei!DllMain
0ac2f934 77a01c48 urlmon!CUrlMkTls::TLSAllocData+0x3f, calling kernel32!TlsSetValue
0ac2f944 77a0198d urlmon!CUrlMkTls::CUrlMkTls+0x29, calling urlmon!CUrlMkTls::TLSAllocData
0ac2f950 77a01be5 urlmon!TlsDllMain+0x100, calling urlmon!EnsureFeatureCache
0ac2f95c 6d016a21 mshtml!DllMain+0x10, calling kernel32!GetCurrentThreadId
0ac2f96c 6d016b6c mshtml!_CRT_INIT+0x281, calling mshtml!DllMain
0ac2f984 6dd622ff jscript!_CRT_INIT+0x281, calling jscript!DllMain
0ac2f990 6dd62336 jscript!_CRT_INIT+0x3e7, calling jscript!_SEH_epilog4
0ac2f9cc 6d016ad0 mshtml!_DllMainStartup+0x56, calling mshtml!_DllMainCRTStartup
0ac2f9e0 6dd62336 jscript!_CRT_INIT+0x3e7, calling jscript!_SEH_epilog4
0ac2f9e4 77c4a604 ntdll!LdrpCallInitRoutine+0x14
0ac2fa0c 77c1ab6c ntdll!LdrpInitializeThread+0x1e9, calling ntdll!RtlLeaveCriticalSection
0ac2fa14 77c1a9ea ntdll!LdrpInitializeThread+0x1cd, calling ntdll!_SEH_epilog4
0ac2fa68 77c1ab15 ntdll!LdrpInitializeThread+0x11f, calling ntdll!RtlActivateActivationContextUnsafeFast
0ac2fa6c 77c1ab53 ntdll!LdrpInitializeThread+0x167, calling ntdll!RtlDeactivateActivationContextUnsafeFast
0ac2faa0 77c1a9ea ntdll!LdrpInitializeThread+0x1cd, calling ntdll!_SEH_epilog4
0ac2faa4 77c405a0 ntdll!NtTestAlert+0xc
0ac2faa8 77c1a968 ntdll!_LdrpInitialize+0x29c, calling ntdll!_SEH_epilog4
0ac2fb08 77c3f3d0 ntdll!NtContinue+0xc
0ac2fb0c 77c1a98a ntdll!LdrInitializeThunk+0x1a, calling ntdll!NtContinue
0ac2fd98 6baa59f6 clr!Thread::intermediateThreadProc+0x39, calling clr!_alloca_probe_16
0ac2fdac 76573833 kernel32!BaseThreadInitThunk+0xe
0ac2fdb8 77c1a9bd ntdll!_RtlUserThreadStart+0x23
```

Note: We also double check our hypothesis by looking at the thread unmanaged raw stack (**!DumpStackObjects** command doesn't show anything suspicios in managed residue):

```
0:012> !DumpStackObjects
OS Thread Id: 0xae4 (12)
ESP/REG  Object   Name
0AC2EC00 097b0d78 System.String    critical section 1
0AC2EC9C 097e2fec System.Windows.Forms.ClientUtils+WeakRefCollection+WeakRefObject
0AC2ECB0 097e2fec System.Windows.Forms.ClientUtils+WeakRefCollection+WeakRefObject
0AC2ED08 097e2fec System.Windows.Forms.ClientUtils+WeakRefCollection+WeakRefObject
0AC2ED14 097b0d78 System.String    critical section 1
0AC2ED68 097b5624 System.Threading.ThreadHelper
0AC2EFF4 097b5638 System.Threading.ThreadStart
```

```
0:012> ~11s
eax=09d2d968 ebx=00000001 ecx=098de550 edx=098df350 esi=00000000 edi=00000000
eip=77c40f34 esp=09d2e694 ebp=09d2e730 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
ntdll!KiFastSystemCallRet:
77c40f34 c3              ret

0:011> !DumpStackObjects
OS Thread Id: 0x3cc (11)
ESP/REG  Object   Name
ecx      098de550 System.Object[]    (System.Windows.Forms.Layout.TableLayout+LayoutInfo[])
09D2E980 097b0dac System.String    critical section 2
09D2EA94 097b0dac System.String    critical section 2
09D2EB08 097b0cd8 System.Threading.ThreadHelper
09D2ED94 097b0cec System.Threading.ThreadStart
09D2EFBC 098dc090 System.Version

0:011> !teb
TEB at 7ff4d000
    ExceptionList:        09d2e720
    StackBase:            09d30000
    StackLimit:           09d2b000
    SubSystemTib:         00000000
    FiberData:            00001e00
    ArbitraryUserPointer: 00000000
    Self:                 7ff4d000
    EnvironmentPointer:   00000000
    ClientId:             0000074c . 000003cc
    RpcHandle:            00000000
    Tls Storage:          7ff4d02c
    PEB Address:          7ffd3000
    LastErrorValue:       0
    LastStatusValue:      c000007c
    Count Owned Locks:    0
    HardErrorMode:        0

0:011> dps 09d2b000 09d30000
[...]
09d2dc68  09d2dc98
09d2dc6c  6bab85bd clr!ExInfo::Init+0x3d
09d2dc70  05118530
09d2dc74  6bab85e5 clr!ExInfo::Init+0x7a
09d2dc78  00004000
09d2dc7c  00000000
09d2dc80  00000000
09d2dc84  6ba7d382 clr!ExInfo::UnwindExInfo+0x102
09d2dc88  9be5e18c
09d2dc8c  09d2dc3c
09d2dc90  09d2e448
09d2dc94  6bac14ce clr!SetCurrentSEHRecord+0xb
09d2dc98  05118530
09d2dc9c  6ba7d834 clr!COMPlusCheckForAbort+0x14d
09d2dca0  098dc068
```

```
09d2dca4  09d2dcb0
09d2dca8  09d2eab0
09d2dcac  05952484
09d2dcb0  00000000
09d2dcb4  09d2ead0
09d2dcb8  6b9f22ee clr!JIT_EndCatch+0x16
09d2dcbc  09d2ead0
09d2dcc0  09d2eab0
09d2dcc4  05952484
09d2dcc8  09d2dcec
[...]
```

Note: We double check symbolic references we found to see if they are valid return addresses:

```
0:003> ub 6b9f22ee
clr!JIT_EndCatch+0x3:
6b9f22db 50              push    eax
6b9f22dc 50              push    eax
6b9f22dd e88bb50800      call    clr!COMPlusEndCatch (6ba7d86d)
6b9f22e2 8b0c24          mov     ecx,dword ptr [esp]
6b9f22e5 8bd0            mov     edx,eax
6b9f22e7 50              push    eax
6b9f22e8 55              push    ebp
6b9f22e9 e80bb50800      call    clr!COMPlusCheckForAbort (6ba7d7f9)
```

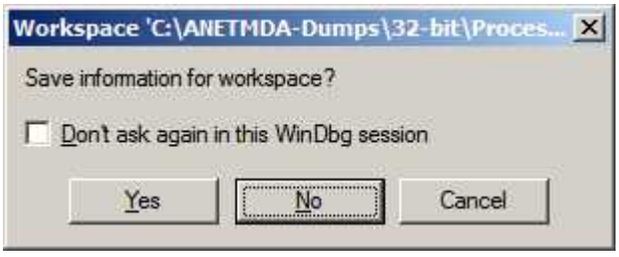
Note: Here the source code fragment explaining why the lock was never released and why we got "catch residue":

```
            try
            {
                  Monitor.Enter(cs1);
                  {
                        DoWork();
                        unsafe
                        {
                              int* p = (int *)0;
                              *p = 1;
                        }
                  }
                  Monitor.Exit(cs1);
            }
            catch (Exception e)
            {
                  Console.WriteLine("We caught an exception.");
            }
```

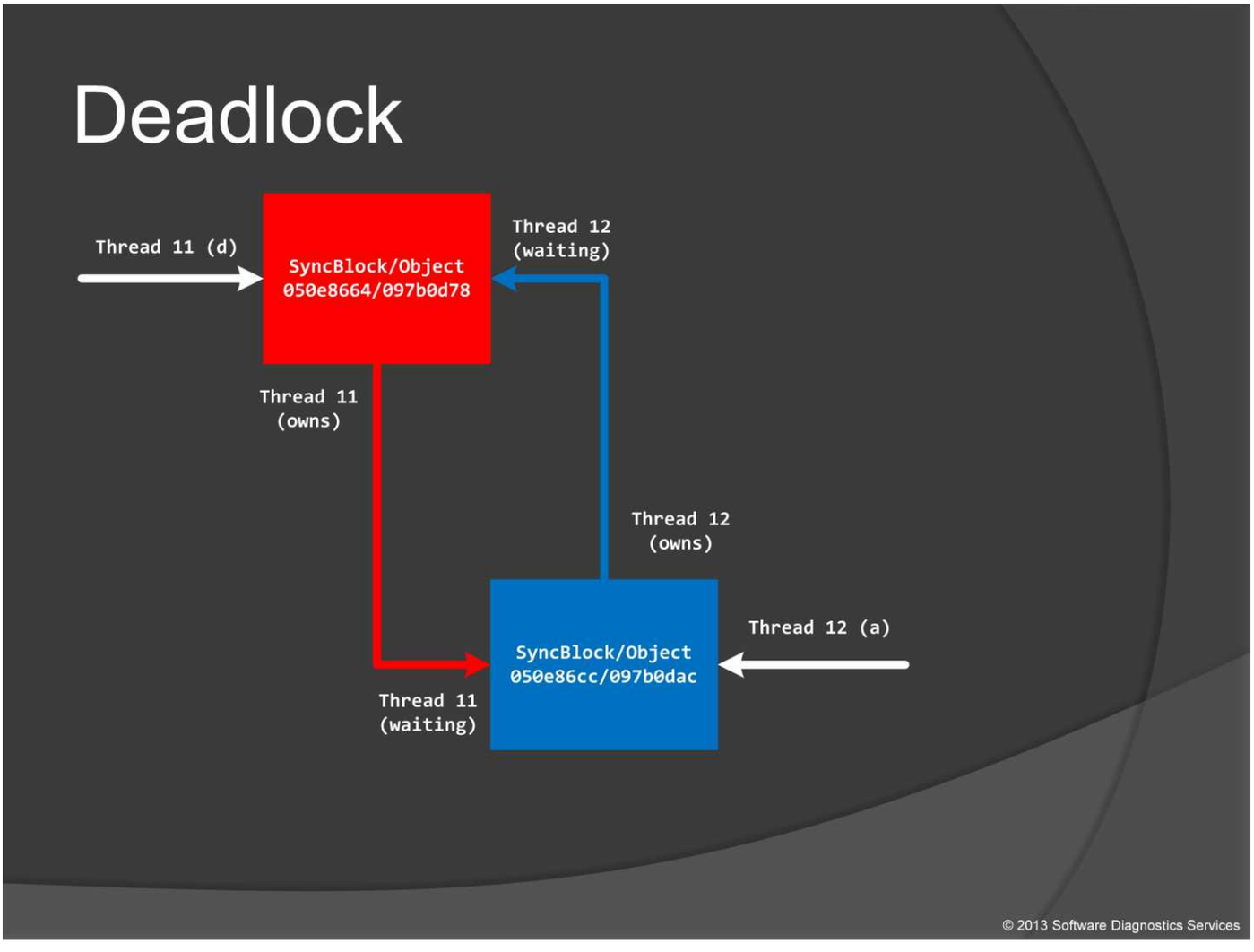
14. We close logging before exiting WinDbg:

```
0:003> .logclose
Closing open log file C:\ANETMDA-Dumps\32-bit\Processes\CLR4\LINQPadC.log
```

If presented with this dialog choose No:



Note: To avoid possible confusion and glitches we recommend to exit WinDbg after each exercise.



Here we depict the deadlock from the exercise PN4.

Exercise PN5

- **Goal:** Learn how to analyze multiple managed exceptions, diagnose heap and handle leaks
- **Patterns:** CLR Thread; Managed Stack Trace Collection; Managed Code Exception; Handle Leak; Multiple Exceptions; Nested Exceptions; Annotated Disassembly; Execution Residue; Exception Thread; Hidden Exception; NULL Pointer
- **Commands:** kv, .cxr, !DumpHeap, ?, !eeheap, !GCHandles, !FinalizeQueue
- \ANETMDA-Dumps\Exercise-PN5-Analysis-process-dump-LINQPadD-32-CLR4.pdf

© 2013 Software Diagnostics Services

Exercise PN5: Analysis of an application process dump (LINQPadD, 32-bit, CLR 4)

Goal: Learn how to analyze multiple managed exceptions, diagnose heap and handle leaks.

Patterns: CLR Thread; Managed Stack Trace Collection; Managed Code Exception; Handle Leak; Multiple Exceptions; Nested Exceptions; Annotated Disassembly; Execution Residue; Exception Thread; Hidden Exception; NULL Pointer

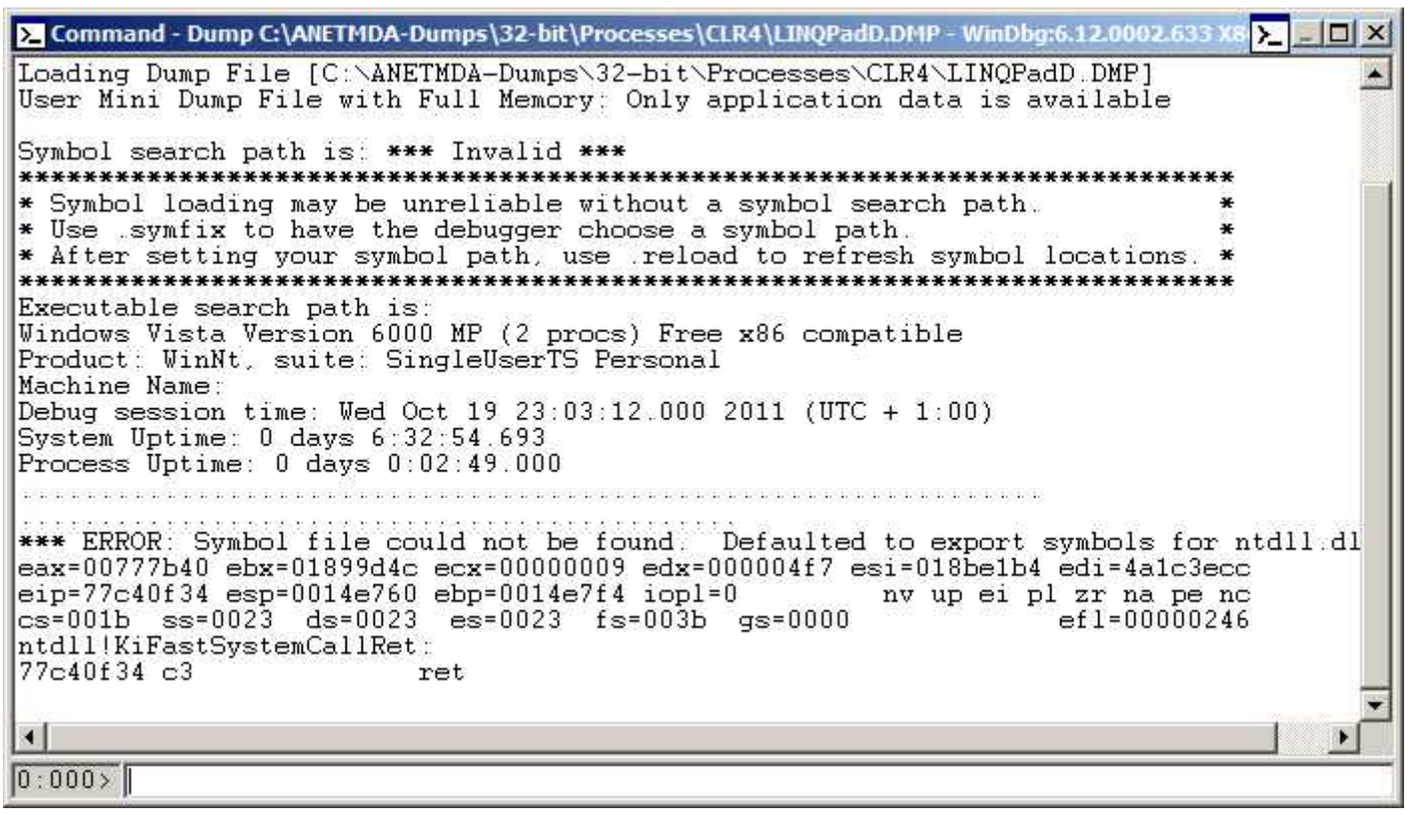
Commands: kv, .cxr, !DumpHeap, ?, !eeheap, !GCHandles, !FinalizeQueue

1. Launch WinDbg from Debugging Tools for Windows or Debugging Tools for Windows (x86)

2. Open \ANETMDA-Dumps\32-bit\Processes\CLR4\LINQPadD.DMP

3. If you are presented with this dialog say No:

4. We get the dump file loaded:



5. Open a log file using **.logopen** command and load symbols (**.symfix** and **.reload** commands):

```
0:000> .logopen C:\ANETMDA-Dumps\32-bit\Processes\CLR4\LINQPadD.log
Opened log file 'C:\ANETMDA-Dumps\32-bit\Processes\CLR4\LINQPadD.log'

0:000> .symfix c:\mss

0:000> .reload
.........................
```

Note: The results may be slightly different on your system if you have 32-bit .NET Framework 4.0.30319.**1** already installed or you don't have any .NET Framework 4.0.30319 installed.

6. Type ~***k** command to verify the correctness of all stack traces:

```
0:000> ~*k

.  0  Id: 6245c.62460 Suspend: 0 Teb: 7ffdf000 Unfrozen
ChildEBP RetAddr
0014e75c 7674b5b4 ntdll!KiFastSystemCallRet
*** WARNING: Unable to verify checksum for System.Windows.Forms.ni.dll
0014e760 67b3737a user32!NtUserWaitMessage+0xc
0014e7f4 67b36e2c System_Windows_Forms_ni+0x22737a
0014e850 67b36c81 System_Windows_Forms_ni+0x226e2c
0014e880 67ac366d System_Windows_Forms_ni+0x226c81
0014e898 00d73f0d System_Windows_Forms_ni+0x1b366d
WARNING: Frame IP not in any known module. Following frames may be wrong.
0014e97c 00d71515 0xd73f0d
0014ec24 6af221db 0xd71515
0014ec34 6af44a2a clr!CallDescrWorker+0x33
0014ecb0 6af44bcc clr!CallDescrWorkerWithHandler+0x8e
0014ede8 6af44c01 clr!MethodDesc::CallDescr+0x194
0014ee04 6af44c21 clr!MethodDesc::CallTargetWorker+0x21
0014ee1c 6b00ce82 clr!MethodDescCallSite::Call+0x1c
0014ef80 6b00cf90 clr!ClassLoader::RunMain+0x24c
0014f1e8 6b00cda4 clr!Assembly::ExecuteMainMethod+0xc1
0014f6cc 6b00d199 clr!SystemDomain::ExecuteMainMethod+0x4ec
0014f720 6b00d09a clr!ExecuteEXE+0x58
0014f76c 6b08af00 clr!_CorExeMainInternal+0x19f
0014f7a4 736455ab clr!_CorExeMain+0x4e
0014f7b0 73747f16 mscoreei!_CorExeMain+0x38
0014f7c0 73744de3 mscoree!ShellShim__CorExeMain+0x99
0014f7c8 76573833 mscoree!_CorExeMain_Exported+0x8
0014f7d4 77c1a9bd kernel32!BaseThreadInitThunk+0xe
0014f814 00000000 ntdll!_RtlUserThreadStart+0x23

   1  Id: 6245c.62474 Suspend: 0 Teb: 7ffde000 Unfrozen
ChildEBP RetAddr
0184f760 77c40690 ntdll!KiFastSystemCallRet
0184f764 76577e09 ntdll!ZwWaitForMultipleObjects+0xc
0184f800 76578150 kernel32!WaitForMultipleObjectsEx+0x11d
0184f81c 6b0875e8 kernel32!WaitForMultipleObjects+0x18
0184f880 6b087526 clr!DebuggerRCThread::MainLoop+0xd9
0184f8b0 6b087461 clr!DebuggerRCThread::ThreadProc+0xca
0184f8dc 76573833 clr!DebuggerRCThread::ThreadProcStatic+0x83
0184f8e8 77c1a9bd kernel32!BaseThreadInitThunk+0xe
0184f928 00000000 ntdll!_RtlUserThreadStart+0x23
```

```
   2  Id: 6245c.62478 Suspend: 0 Teb: 7ffdc000 Unfrozen
ChildEBP RetAddr
039be32c 7674b5b4 ntdll!KiFastSystemCallRet
039be330 67b3737a user32!NtUserWaitMessage+0xc
039be3c4 67b36e2c System_Windows_Forms_ni+0x22737a
039be420 67b36c81 System_Windows_Forms_ni+0x226e2c
039be450 6802fefb System_Windows_Forms_ni+0x226c81
039be468 68059f83 System_Windows_Forms_ni+0x71fefb
039be504 6805a1b7 System_Windows_Forms_ni+0x749f83
039be544 6af221db System_Windows_Forms_ni+0x74a1b7
039be554 6af44a2a clr!CallDescrWorker+0x33
039be5d0 6af44bcc clr!CallDescrWorkerWithHandler+0x8e
039be720 6af44c01 clr!MethodDesc::CallDescr+0x194
039be73c 6b192379 clr!MethodDesc::CallTargetWorker+0x21
039be834 6b134ad1 clr!ExceptionNotifications::DeliverExceptionNotification+0x98
039be8a8 6b134e86 clr!COMDelegate::BindToMethodInfo+0x504
039be94c 6b11c19b clr!DistributeUnhandledExceptionReliably+0xeb
039be9a4 6b11bfd3 clr!AppDomain::RaiseUnhandledExceptionEvent+0xba
039bea3c 6b0a8688 clr!AppDomain::RaiseUnhandledExceptionEvent_Wrapper+0x1cd
039beb14 6b11c13e clr!Thread::DoADCallBack+0xe0
039beb70 6b11de38 clr!AppDomain::RaiseUnhandledExceptionEvent+0xc2
039bebe4 6b11e807 clr!AppDomain::RaiseUnhandledExceptionEventNoThrow+0x7a
039bec40 6b19518a clr!AppDomain::OnUnhandledException+0x81
039bed58 6b1969c1 clr!NotifyAppDomainsOfUnhandledException+0x141
039bef48 6b196f8f clr!DefaultCatchHandler+0xdb
039bef74 6b01c411 clr!DefaultCatchHandler+0x623
039bef84 6b01c45b clr!ThreadBaseExceptionAppDomainFilter+0x13
039befbc 6b01c4df clr!ManagedThreadCallState::IsAppDomainEqual+0x9c
039befc4 71262b04 clr!Thread::ShouldChangeAbortToUnload+0x3af
039befd8 71284ae4 MSVCR100_CLR0400!_EH4_CallFilterFunc+0x12
039bf004 6aff14b8 MSVCR100_CLR0400!_except_handler4_common+0x8e
039bf024 77c41039 clr!_except_handler4+0x20
039bf048 77c4100b ntdll!ExecuteHandler2+0x26
039bf0f0 77c40e97 ntdll!ExecuteHandler+0x24
039bf0f0 05602dfc ntdll!KiUserExceptionDispatcher+0xf
WARNING: Frame IP not in any known module. Following frames may be wrong.
039bf410 6afd4b01 0x5602dfc
039bf46c 6afd49c7 clr!MethodTable::SetObjCreateDelegate+0xbd
039bf498 6afd4a56 clr!MethodTable::CallFinalizer+0xca
039bf4b0 6afd4c9f clr!WKS::CallFinalizer+0xa7
039bf500 6afd4bdb clr!WKS::GCHeap::TraceGCSegments+0x239
039bf530 6b0d88ac clr!WKS::GCHeap::TraceGCSegments+0x415
039bf544 6afd5c05 clr!WKS::ProfScanRootsHelper+0x6b
039bf558 6afd5c87 clr!Thread::DoExtraWorkForFinalizer+0x114
039bf608 6afd5d42 clr!Thread::ShouldChangeAbortToUnload+0x101
039bf668 6afc37a2 clr!Thread::ShouldChangeAbortToUnload+0x399
039bf674 6b0a8688 clr!Thread::RaiseCrossContextException+0x3f8
039bf74c 6b0acca8 clr!Thread::DoADCallBack+0xe0
039bf770 6b0acbda clr!Thread::DoExtraWorkForFinalizer+0x10c
039bf77c 6b0d8921 clr!ManagedThreadBase::FinalizerAppDomain+0x27
039bf7d8 6afd4bdb clr!WKS::GCHeap::TraceGCSegments+0x2e3
039bf808 6b098405 clr!WKS::GCHeap::TraceGCSegments+0x415
039bf824 6afd5c05 clr!WKS::GCHeap::FinalizerThreadWorker+0xcd
039bf838 6afd5c87 clr!Thread::DoExtraWorkForFinalizer+0x114
039bf8e8 6afd5d42 clr!Thread::ShouldChangeAbortToUnload+0x101
039bf948 6afc78be clr!Thread::ShouldChangeAbortToUnload+0x399
039bf96c 6afc78d1 clr!ManagedThreadBase_NoADTransition+0x35
039bf97c 6b00d313 clr!ManagedThreadBase::FinalizerBase+0xf
039bf9b4 6afd5a08 clr!WKS::GCHeap::FinalizerThreadStart+0x10c
039bfa4c 76573833 clr!Thread::intermediateThreadProc+0x4b
```

```
039bfa58 77c1a9bd kernel32!BaseThreadInitThunk+0xe
039bfa98 00000000 ntdll!_RtlUserThreadStart+0x23

   3  Id: 6245c.6247c Suspend: 0 Teb: 7ffdb000 Unfrozen
ChildEBP RetAddr
0483f560 77c3f9c0 ntdll!KiFastSystemCallRet
0483f564 7653f00d ntdll!NtFsControlFile+0xc
*** WARNING: Unable to verify checksum for System.Core.ni.dll
0483f5a8 68fc80b7 kernel32!ConnectNamedPipe+0x52
0483f618 6905c07c System_Core_ni+0x3080b7
*** WARNING: Unable to verify checksum for mscorlib.ni.dll
0483f6c0 6962ae5b System_Core_ni+0x39c07c
0483f6d0 695b7ff4 mscorlib_ni+0x2aae5b
0483f6ec 695b7f34 mscorlib_ni+0x237ff4
0483f70c 6962ade8 mscorlib_ni+0x237f34
0483f724 6af221db mscorlib_ni+0x2aade8
0483f734 6af44a2a clr!CallDescrWorker+0x33
0483f7b0 6af44bcc clr!CallDescrWorkerWithHandler+0x8e
0483f8f4 6af44c01 clr!MethodDesc::CallDescr+0x194
0483f910 6b0bb512 clr!MethodDesc::CallTargetWorker+0x21
0483fb1c 6afd5c05 clr!ThreadNative::KickOffThread_Worker+0x1e1
0483fb30 6afd5c87 clr!Thread::DoExtraWorkForFinalizer+0x114
0483fbe0 6afd5d42 clr!Thread::ShouldChangeAbortToUnload+0x101
0483fc40 6afd5dd9 clr!Thread::ShouldChangeAbortToUnload+0x399
0483fc64 6b0bb3e5 clr!Thread::ShouldChangeAbortToUnload+0x43a
0483fc7c 6b0bb2e0 clr!ManagedThreadBase::KickOff+0x15
0483fd14 6afd5a08 clr!ThreadNative::KickOffThread+0x23e
0483fe2c 76573833 clr!Thread::intermediateThreadProc+0x4b
0483fe38 77c1a9bd kernel32!BaseThreadInitThunk+0xe
0483fe78 00000000 ntdll!_RtlUserThreadStart+0x23

   4  Id: 6245c.62480 Suspend: 0 Teb: 7ffda000 Unfrozen
ChildEBP RetAddr
04a4f954 77c40690 ntdll!KiFastSystemCallRet
04a4f958 76577e09 ntdll!ZwWaitForMultipleObjects+0xc
04a4f9f4 7674c4af kernel32!WaitForMultipleObjectsEx+0x11d
04a4fa48 76748b7b user32!RealMsgWaitForMultipleObjectsEx+0x13c
04a4fa64 74d01965 user32!MsgWaitForMultipleObjects+0x1f
04a4fab0 76573833 GdiPlus!BackgroundThreadProc+0x59
04a4fabc 77c1a9bd kernel32!BaseThreadInitThunk+0xe
04a4fafc 00000000 ntdll!_RtlUserThreadStart+0x23

   5  Id: 6245c.62490 Suspend: 0 Teb: 7ffd6000 Unfrozen
ChildEBP RetAddr
059cfb74 77c3f7c0 ntdll!KiFastSystemCallRet
059cfb78 765778e0 ntdll!NtDelayExecution+0xc
059cfbe0 76531da0 kernel32!SleepEx+0x62
059cfbf0 776f40f4 kernel32!Sleep+0xf
059cfbfc 776dfc0d ole32!CROIDTable::WorkerThreadLoop+0x14
059cfc18 776dfc73 ole32!CRpcThread::WorkerLoop+0x26
059cfc24 76573833 ole32!CRpcThreadCache::RpcWorkerThreadEntry+0x20
059cfc30 77c1a9bd kernel32!BaseThreadInitThunk+0xe
059cfc70 00000000 ntdll!_RtlUserThreadStart+0x23
```

```
   6  Id: 6245c.624a0 Suspend: 0 Teb: 7ffd5000 Unfrozen
ChildEBP RetAddr
05e1f1a8 77c40690 ntdll!KiFastSystemCallRet
05e1f1ac 76577e09 ntdll!ZwWaitForMultipleObjects+0xc
05e1f248 6afd516a kernel32!WaitForMultipleObjectsEx+0x11d
05e1f2ac 6afd4f98 clr!WaitForMultipleObjectsEx_SO_TOLERANT+0x56
05e1f2cc 6afd4dd8 clr!Thread::DoAppropriateAptStateWait+0x4d
05e1f360 6afd4e99 clr!Thread::DoAppropriateWaitWorker+0x17d
05e1f3cc 6afd4f17 clr!Thread::DoAppropriateWait+0x60
05e1f420 6af7d409 clr!CLREvent::WaitEx+0x106
05e1f434 6b0bc71c clr!CLREvent::Wait+0x19
05e1f448 6b0bc73a clr!Thread::Wait+0x1d
05e1f45c 6b0bc545 clr!Thread::Block+0x1a
05e1f508 6b0bc5b2 clr!SyncBlock::Wait+0x169
05e1f51c 6b0bc6a4 clr!ObjHeader::Wait+0x2c
05e1f5c4 695b9140 clr!ObjectNative::WaitTimeout+0x147
05e1f5d4 69b7428a mscorlib_ni+0x239140
05e1f6a0 6962ae5b mscorlib_ni+0x7f428a
05e1f6b0 695b7ff4 mscorlib_ni+0x2aae5b
05e1f6cc 695b7f34 mscorlib_ni+0x237ff4
05e1f6ec 6962ade8 mscorlib_ni+0x237f34
05e1f704 6af221db mscorlib_ni+0x2aade8
05e1f714 6af44a2a clr!CallDescrWorker+0x33
05e1f790 6af44bcc clr!CallDescrWorkerWithHandler+0x8e
05e1f8d4 6af44c01 clr!MethodDesc::CallDescr+0x194
05e1f8f0 6b0bb512 clr!MethodDesc::CallTargetWorker+0x21
05e1fafc 6afd5c05 clr!ThreadNative::KickOffThread_Worker+0x1e1
05e1fb10 6afd5c87 clr!Thread::DoExtraWorkForFinalizer+0x114
05e1fbc0 6afd5d42 clr!Thread::ShouldChangeAbortToUnload+0x101
05e1fc20 6afd5dd9 clr!Thread::ShouldChangeAbortToUnload+0x399
05e1fc44 6b0bb3e5 clr!Thread::ShouldChangeAbortToUnload+0x43a
05e1fc5c 6b0bb2e0 clr!ManagedThreadBase::KickOff+0x15
05e1fcf4 6afd5a08 clr!ThreadNative::KickOffThread+0x23e
05e1ff94 76573833 clr!Thread::intermediateThreadProc+0x4b
05e1ffa0 77c1a9bd kernel32!BaseThreadInitThunk+0xe
05e1ffe0 00000000 ntdll!_RtlUserThreadStart+0x23
```

```
   7  Id: 6245c.624c8 Suspend: 0 Teb: 7ffd4000 Unfrozen
ChildEBP RetAddr
05caf1c0 7657811f ntdll!RtlDeactivateActivationContextUnsafeFast+0x8
05caf24c 6afd516a kernel32!WaitForMultipleObjectsEx+0x195
05caf2b0 6afd4f98 clr!WaitForMultipleObjectsEx_SO_TOLERANT+0x56
05caf2d0 6afd4dd8 clr!Thread::DoAppropriateAptStateWait+0x4d
05caf364 6afd4e99 clr!Thread::DoAppropriateWaitWorker+0x17d
05caf3d0 6b1bed54 clr!Thread::DoAppropriateWait+0x60
05caf50c 695f573b clr!WaitHandleNative::CorWaitMultipleNative+0x230
*** WARNING: Unable to verify checksum for System.ni.dll
05caf530 6a7b6e1e mscorlib_ni+0x27573b
05caf590 6962ae5b System_ni+0x136e1e
05caf5a0 695b7ff4 mscorlib_ni+0x2aae5b
05caf5bc 695b7f34 mscorlib_ni+0x237ff4
05caf5dc 6962ade8 mscorlib_ni+0x237f34
05caf5f4 6af221db mscorlib_ni+0x2aade8
05caf604 6af44a2a clr!CallDescrWorker+0x33
05caf680 6af44bcc clr!CallDescrWorkerWithHandler+0x8e
05caf7c4 6af44c01 clr!MethodDesc::CallDescr+0x194
05caf7e0 6b0bb512 clr!MethodDesc::CallTargetWorker+0x21
05caf9ec 6afd5c05 clr!ThreadNative::KickOffThread_Worker+0x1e1
05cafa00 6afd5c87 clr!Thread::DoExtraWorkForFinalizer+0x114
05cafab0 6afd5d42 clr!Thread::ShouldChangeAbortToUnload+0x101
05cafb10 6afd5dd9 clr!Thread::ShouldChangeAbortToUnload+0x399
05cafb34 6b0bb3e5 clr!Thread::ShouldChangeAbortToUnload+0x43a
05cafb4c 6b0bb2e0 clr!ManagedThreadBase::KickOff+0x15
05cafbe4 6afd5a08 clr!ThreadNative::KickOffThread+0x23e
05caff08 76573833 clr!Thread::intermediateThreadProc+0x4b
05caff14 77c1a9bd kernel32!BaseThreadInitThunk+0xe
05caff54 00000000 ntdll!_RtlUserThreadStart+0x23

   8  Id: 6245c.62518 Suspend: 0 Teb: 7ffd9000 Unfrozen
ChildEBP RetAddr
065bea6c 77c40690 ntdll!KiFastSystemCallRet
065bea70 76577e09 ntdll!ZwWaitForMultipleObjects+0xc
065beb0c 6afd516a kernel32!WaitForMultipleObjectsEx+0x11d
065beb70 6afd4f98 clr!WaitForMultipleObjectsEx_SO_TOLERANT+0x56
065beb90 6afd4dd8 clr!Thread::DoAppropriateAptStateWait+0x4d
065bec24 6afd4e99 clr!Thread::DoAppropriateWaitWorker+0x17d
065bec90 6afb1329 clr!Thread::DoAppropriateWait+0x60
065bed90 6962b5ef clr!WaitHandleNative::CorWaitOneNative+0x196
065beda8 6962b5ad mscorlib_ni+0x2ab5ef
065bedc8 6962b570 mscorlib_ni+0x2ab5ad
065bee10 6962ae5b mscorlib_ni+0x2ab570
065bee20 695b7ff4 mscorlib_ni+0x2aae5b
065bee3c 695b7f34 mscorlib_ni+0x237ff4
065bee5c 6962ade8 mscorlib_ni+0x237f34
065bee74 6af221db mscorlib_ni+0x2aade8
065bee84 6af44a2a clr!CallDescrWorker+0x33
065bef00 6af44bcc clr!CallDescrWorkerWithHandler+0x8e
065bf044 6af44c01 clr!MethodDesc::CallDescr+0x194
065bf060 6b0bb512 clr!MethodDesc::CallTargetWorker+0x21
065bf26c 6afd5c05 clr!ThreadNative::KickOffThread_Worker+0x1e1
065bf280 6afd5c87 clr!Thread::DoExtraWorkForFinalizer+0x114
065bf330 6afd5d42 clr!Thread::ShouldChangeAbortToUnload+0x101
065bf390 6afd5dd9 clr!Thread::ShouldChangeAbortToUnload+0x399
065bf3b4 6b0bb3e5 clr!Thread::ShouldChangeAbortToUnload+0x43a
065bf3cc 6b0bb2e0 clr!ManagedThreadBase::KickOff+0x15
065bf464 6afd5a08 clr!ThreadNative::KickOffThread+0x23e
065bf804 76573833 clr!Thread::intermediateThreadProc+0x4b
```

```
065bf810 77c1a9bd kernel32!BaseThreadInitThunk+0xe
065bf850 00000000 ntdll!_RtlUserThreadStart+0x23

   9  Id: 6245c.62520 Suspend: 0 Teb: 7ffd3000 Unfrozen
ChildEBP RetAddr
08b9fadc 77c3f7c0 ntdll!KiFastSystemCallRet
08b9fae0 765778e0 ntdll!NtDelayExecution+0xc
08b9fb48 6af7cc0a kernel32!SleepEx+0x62
08b9fb5c 6af7cbdb clr!__DangerousSwitchToThread+0x48
08b9fb70 6aff878b clr!__SwitchToThread+0x12
08b9fc60 76573833 clr!ThreadpoolMgr::GateThreadStart+0x83
08b9fc6c 77c1a9bd kernel32!BaseThreadInitThunk+0xe
08b9fcac 00000000 ntdll!_RtlUserThreadStart+0x23

  10  Id: 6245c.62524 Suspend: 0 Teb: 7ff4f000 Unfrozen
ChildEBP RetAddr
08cff3a0 77c400f0 ntdll!KiFastSystemCallRet
08cff3a4 76557948 ntdll!NtRemoveIoCompletion+0xc
08cff3d0 6afeaeab kernel32!GetQueuedCompletionStatus+0x29
08cff434 6afd5a08 clr!ThreadpoolMgr::CompletionPortThreadStart+0x155
08cff850 76573833 clr!Thread::intermediateThreadProc+0x4b
08cff85c 77c1a9bd kernel32!BaseThreadInitThunk+0xe
08cff89c 00000000 ntdll!_RtlUserThreadStart+0x23

  11  Id: 6245c.62538 Suspend: 0 Teb: 7ff4e000 Unfrozen
ChildEBP RetAddr
09fcf870 77c406a0 ntdll!KiFastSystemCallRet
09fcf874 765777d4 ntdll!NtWaitForSingleObject+0xc
09fcf8e4 76577742 kernel32!WaitForSingleObjectEx+0xbe
09fcf8f8 6d01f57d kernel32!WaitForSingleObject+0x12
09fcf910 6d016c92 mshtml!CDwnTaskExec::ThreadExec+0x127
09fcf91c 6cf9dadc mshtml!CExecFT::ThreadProc+0x3c
09fcf924 76573833 mshtml!CExecFT::StaticThreadProc+0xd
09fcf930 77c1a9bd kernel32!BaseThreadInitThunk+0xe
09fcf970 00000000 ntdll!_RtlUserThreadStart+0x23

  12  Id: 6245c.62544 Suspend: 0 Teb: 7ff4c000 Unfrozen
ChildEBP RetAddr
0a78f194 77c406a0 ntdll!KiFastSystemCallRet
0a78f198 765777d4 ntdll!NtWaitForSingleObject+0xc
0a78f208 6af81030 kernel32!WaitForSingleObjectEx+0xbe
0a78f23c 6af81071 clr!CLREvent::CreateManualEvent+0xf6
0a78f28c 6af7d3e8 clr!CLREvent::CreateManualEvent+0x137
0a78f2cc 6af7d409 clr!CLREvent::WaitEx+0x126
0a78f2e0 6b0ace05 clr!CLREvent::Wait+0x19
0a78f3b4 6afd5a08 clr!AppDomain::ADUnloadThreadStart+0x2f5
0a78f94c 76573833 clr!Thread::intermediateThreadProc+0x4b
0a78f958 77c1a9bd kernel32!BaseThreadInitThunk+0xe
0a78f998 00000000 ntdll!_RtlUserThreadStart+0x23
```

```
  13  Id: 6245c.62548 Suspend: 0 Teb: 7ff4b000 Unfrozen
ChildEBP RetAddr
0a8adb98 77c40690 ntdll!KiFastSystemCallRet
0a8adb9c 76577e09 ntdll!ZwWaitForMultipleObjects+0xc
0a8adc38 7674c4af kernel32!WaitForMultipleObjectsEx+0x11d
0a8adc8c 776dcec8 user32!RealMsgWaitForMultipleObjectsEx+0x13c
0a8adcb4 776c03ef ole32!CCliModalLoop::BlockFn+0x97
0a8add30 6afe74f3 ole32!CoWaitForMultipleHandles+0xcd
0a8add98 6afe747f clr!MsgWaitHelper+0x80
0a8addb8 6afd4dd8 clr!Thread::DoAppropriateAptStateWait+0x39
0a8ade4c 6afd4e99 clr!Thread::DoAppropriateWaitWorker+0x17d
0a8adeb8 6b0bcfed clr!Thread::DoAppropriateWait+0x60
0a8adf08 6b0bd0db clr!Thread::JoinEx+0xd5
0a8adf70 6b0bd1db clr!ThreadNative::DoJoin+0xaf
0a8ae014 0560271d clr!ThreadNative::Join+0xf2
WARNING: Frame IP not in any known module. Following frames may be wrong.
0a8ae034 6af221db 0x560271d
0a8ae044 6af44a2a clr!CallDescrWorker+0x33
0a8ae0c0 6af44bcc clr!CallDescrWorkerWithHandler+0x8e
0a8ae200 6af44c01 clr!MethodDesc::CallDescr+0x194
0a8ae21c 6af44c21 clr!MethodDesc::CallTargetWorker+0x21
0a8ae234 6afb7856 clr!MethodDescCallSite::Call+0x1c
0a8ae3f8 6afb7ba3 clr!CallWithValueTypes_RetArgSlotWrapper+0x5c
0a8ae6c4 6afb7d65 clr!InvokeImpl+0x621
0a8ae790 6963d689 clr!RuntimeMethodHandle::InvokeMethodFast+0x180
0a8ae7e4 6963d3d0 mscorlib_ni+0x2bd689
0a8ae81c 6963bfed mscorlib_ni+0x2bd3d0
0a8ae844 69643284 mscorlib_ni+0x2bbfed
0a8ae868 6af3de7e mscorlib_ni+0x2c3284
0a8aea74 05600988 clr!ListLockEntry::Release+0x68
0a8aead0 6962ae5b 0x5600988
0a8aeae0 695b7ff4 mscorlib_ni+0x2aae5b
0a8aeafc 695b7f34 mscorlib_ni+0x237ff4
0a8aeb1c 6962ade8 mscorlib_ni+0x237f34
0a8aeb34 6af221db mscorlib_ni+0x2aade8
0a8aeb44 6af44a2a clr!CallDescrWorker+0x33
0a8aebc0 6af44bcc clr!CallDescrWorkerWithHandler+0x8e
0a8aecf8 6af44c01 clr!MethodDesc::CallDescr+0x194
0a8aed14 6b0bb512 clr!MethodDesc::CallTargetWorker+0x21
0a8aef20 6afd5c05 clr!ThreadNative::KickOffThread_Worker+0x1e1
0a8aef34 6afd5c87 clr!Thread::DoExtraWorkForFinalizer+0x114
0a8aefe4 6afd5d42 clr!Thread::ShouldChangeAbortToUnload+0x101
0a8af044 6afc37a2 clr!Thread::ShouldChangeAbortToUnload+0x399
0a8af050 6b0a6465 clr!Thread::RaiseCrossContextException+0x3f8
0a8af130 6afc37cf clr!Thread::DoADCallBack+0xf0
0a8af150 6afd5c87 clr!Thread::DoExtraWorkForFinalizer+0xfa
0a8af200 6afd5d42 clr!Thread::ShouldChangeAbortToUnload+0x101
0a8af260 6afd5dd9 clr!Thread::ShouldChangeAbortToUnload+0x399
0a8af284 6b0bb3e5 clr!Thread::ShouldChangeAbortToUnload+0x43a
0a8af29c 6b0bb2e0 clr!ManagedThreadBase::KickOff+0x15
0a8af334 6afd5a08 clr!ThreadNative::KickOffThread+0x23e
0a8af950 76573833 clr!Thread::intermediateThreadProc+0x4b
0a8af95c 77c1a9bd kernel32!BaseThreadInitThunk+0xe
0a8af99c 00000000 ntdll!_RtlUserThreadStart+0x23
```

```
  14  Id: 6245c.6254c Suspend: 0 Teb: 7ff4d000 Unfrozen
ChildEBP RetAddr
0a62dd4c 7674b5b4 ntdll!KiFastSystemCallRet
0a62dd50 67b3737a user32!NtUserWaitMessage+0xc
0a62dde4 67b36e2c System_Windows_Forms_ni+0x22737a
0a62de40 67b36c81 System_Windows_Forms_ni+0x226e2c
0a62de70 6802fefb System_Windows_Forms_ni+0x226c81
0a62de88 68059f83 System_Windows_Forms_ni+0x71fefb
0a62df24 6805a1b7 System_Windows_Forms_ni+0x749f83
0a62df64 6af221db System_Windows_Forms_ni+0x74a1b7
0a62df74 6af44a2a clr!CallDescrWorker+0x33
0a62dff0 6af44bcc clr!CallDescrWorkerWithHandler+0x8e
0a62e140 6af44c01 clr!MethodDesc::CallDescr+0x194
0a62e15c 6b192379 clr!MethodDesc::CallTargetWorker+0x21
0a62e254 6b134ad1 clr!ExceptionNotifications::DeliverExceptionNotification+0x98
0a62e2c8 6b134e86 clr!COMDelegate::BindToMethodInfo+0x504
0a62e36c 6b11c19b clr!DistributeUnhandledExceptionReliably+0xeb
0a62e3c4 6b11bfd3 clr!AppDomain::RaiseUnhandledExceptionEvent+0xba
0a62e45c 6b0a8688 clr!AppDomain::RaiseUnhandledExceptionEvent_Wrapper+0x1cd
0a62e534 6b11c13e clr!Thread::DoADCallBack+0xe0
0a62e590 6b11de38 clr!AppDomain::RaiseUnhandledExceptionEvent+0xc2
0a62e604 6b11e807 clr!AppDomain::RaiseUnhandledExceptionEventNoThrow+0x7a
0a62e660 6b19518a clr!AppDomain::OnUnhandledException+0x81
0a62e774 6b1969c1 clr!NotifyAppDomainsOfUnhandledException+0x141
0a62e964 6b196f8f clr!DefaultCatchHandler+0xdb
0a62e990 6b01c411 clr!DefaultCatchHandler+0x623
0a62e9a0 6b01c45b clr!ThreadBaseExceptionAppDomainFilter+0x13
0a62e9d8 6b01c4df clr!ManagedThreadCallState::IsAppDomainEqual+0x9c
0a62e9e0 71262b04 clr!Thread::ShouldChangeAbortToUnload+0x3af
0a62e9f4 71284ae4 MSVCR100_CLR0400!_EH4_CallFilterFunc+0x12
0a62ea20 6aff14b8 MSVCR100_CLR0400!_except_handler4_common+0x8e
0a62ea40 77c41039 clr!_except_handler4+0x20
0a62ea64 77c4100b ntdll!ExecuteHandler2+0x26
0a62eb0c 77c40e97 ntdll!ExecuteHandler+0x24
0a62eb0c 7654b09e ntdll!KiUserExceptionDispatcher+0xf
0a62ee68 6afaac08 kernel32!RaiseException+0x58
0a62eef8 6afaae41 clr!RaiseTheExceptionInternalOnly+0x276
0a62efb8 05602765 clr!IL_Throw+0x14c
WARNING: Frame IP not in any known module. Following frames may be wrong.
0a62efd0 695b7ff4 0x5602765
0a62efec 695b7f34 mscorlib_ni+0x237ff4
0a62f00c 6962ade8 mscorlib_ni+0x237f34
0a62f024 6af221db mscorlib_ni+0x2aade8
0a62f034 6af44a2a clr!CallDescrWorker+0x33
0a62f0b0 6af44bcc clr!CallDescrWorkerWithHandler+0x8e
0a62f1e8 6af44c01 clr!MethodDesc::CallDescr+0x194
0a62f204 6b0bb512 clr!MethodDesc::CallTargetWorker+0x21
0a62f410 6afd5c05 clr!ThreadNative::KickOffThread_Worker+0x1e1
0a62f424 6afd5c87 clr!Thread::DoExtraWorkForFinalizer+0x114
0a62f4d4 6afd5d42 clr!Thread::ShouldChangeAbortToUnload+0x101
0a62f534 6afc37a2 clr!Thread::ShouldChangeAbortToUnload+0x399
0a62f540 6b0a6465 clr!Thread::RaiseCrossContextException+0x3f8
0a62f620 6afc37cf clr!Thread::DoADCallBack+0xf0
0a62f640 6afd5c87 clr!Thread::DoExtraWorkForFinalizer+0xfa
0a62f6f0 6afd5d42 clr!Thread::ShouldChangeAbortToUnload+0x101
0a62f750 6afd5dd9 clr!Thread::ShouldChangeAbortToUnload+0x399
0a62f774 6b0bb3e5 clr!Thread::ShouldChangeAbortToUnload+0x43a
0a62f78c 6b0bb2e0 clr!ManagedThreadBase::KickOff+0x15
0a62f824 6afd5a08 clr!ThreadNative::KickOffThread+0x23e
0a62fec4 76573833 clr!Thread::intermediateThreadProc+0x4b
```

```
0a62fed0 77c1a9bd kernel32!BaseThreadInitThunk+0xe
0a62ff10 00000000 ntdll!_RtlUserThreadStart+0x23

  15  Id: 6245c.62558 Suspend: 0 Teb: 7ff48000 Unfrozen
ChildEBP RetAddr
0b13da8c 7674b5b4 ntdll!KiFastSystemCallRet
0b13da90 67b3737a user32!NtUserWaitMessage+0xc
0b13db24 67b36e2c System_Windows_Forms_ni+0x22737a
0b13db80 67b36c81 System_Windows_Forms_ni+0x226e2c
0b13dbb0 6802fefb System_Windows_Forms_ni+0x226c81
0b13dbc8 68059f83 System_Windows_Forms_ni+0x71fefb
0b13dc64 6805a1b7 System_Windows_Forms_ni+0x749f83
0b13dca4 6af221db System_Windows_Forms_ni+0x74a1b7
0b13dcb4 6af44a2a clr!CallDescrWorker+0x33
0b13dd30 6af44bcc clr!CallDescrWorkerWithHandler+0x8e
0b13de80 6af44c01 clr!MethodDesc::CallDescr+0x194
0b13de9c 6b192379 clr!MethodDesc::CallTargetWorker+0x21
0b13df94 6b134ad1 clr!ExceptionNotifications::DeliverExceptionNotification+0x98
0b13e008 6b134e86 clr!COMDelegate::BindToMethodInfo+0x504
0b13e0ac 6b11c19b clr!DistributeUnhandledExceptionReliably+0xeb
0b13e104 6b11bfd3 clr!AppDomain::RaiseUnhandledExceptionEvent+0xba
0b13e19c 6b0a8688 clr!AppDomain::RaiseUnhandledExceptionEvent_Wrapper+0x1cd
0b13e274 6b11c13e clr!Thread::DoADCallBack+0xe0
0b13e2d0 6b11de38 clr!AppDomain::RaiseUnhandledExceptionEvent+0xc2
0b13e344 6b11e807 clr!AppDomain::RaiseUnhandledExceptionEventNoThrow+0x7a
0b13e3a0 6b19518a clr!AppDomain::OnUnhandledException+0x81
0b13e4bc 6b1969c1 clr!NotifyAppDomainsOfUnhandledException+0x141
0b13e6ac 6b196f8f clr!DefaultCatchHandler+0xdb
0b13e6d8 6b01c411 clr!DefaultCatchHandler+0x623
0b13e6e8 6b01c45b clr!ThreadBaseExceptionAppDomainFilter+0x13
0b13e720 6b01c4df clr!ManagedThreadCallState::IsAppDomainEqual+0x9c
0b13e728 71262b04 clr!Thread::ShouldChangeAbortToUnload+0x3af
0b13e73c 71284ae4 MSVCR100_CLR0400!_EH4_CallFilterFunc+0x12
0b13e768 6aff14b8 MSVCR100_CLR0400!_except_handler4_common+0x8e
0b13e788 77c41039 clr!_except_handler4+0x20
0b13e7ac 77c4100b ntdll!ExecuteHandler2+0x26
0b13e854 77c40e97 ntdll!ExecuteHandler+0x24
0b13e854 7654b09e ntdll!KiUserExceptionDispatcher+0xf
0b13ebb0 6afaac08 kernel32!RaiseException+0x58
0b13ec40 6afaae41 clr!RaiseTheExceptionInternalOnly+0x276
0b13ed00 056028bb clr!IL_Throw+0x14c
WARNING: Frame IP not in any known module. Following frames may be wrong.
0b13edd0 6962ae5b 0x56028bb
0b13ede0 695b7ff4 mscorlib_ni+0x2aae5b
0b13edfc 695b7f34 mscorlib_ni+0x237ff4
0b13ee1c 6962ade8 mscorlib_ni+0x237f34
0b13ee34 6af221db mscorlib_ni+0x2aade8
0b13ee44 6af44a2a clr!CallDescrWorker+0x33
0b13eec0 6af44bcc clr!CallDescrWorkerWithHandler+0x8e
0b13eff8 6af44c01 clr!MethodDesc::CallDescr+0x194
0b13f014 6b0bb512 clr!MethodDesc::CallTargetWorker+0x21
0b13f220 6afd5c05 clr!ThreadNative::KickOffThread_Worker+0x1e1
0b13f234 6afd5c87 clr!Thread::DoExtraWorkForFinalizer+0x114
0b13f2e4 6afd5d42 clr!Thread::ShouldChangeAbortToUnload+0x101
0b13f344 6afc37a2 clr!Thread::ShouldChangeAbortToUnload+0x399
0b13f350 6b0a6465 clr!Thread::RaiseCrossContextException+0x3f8
0b13f430 6afc37cf clr!Thread::DoADCallBack+0xf0
0b13f450 6afd5c87 clr!Thread::DoExtraWorkForFinalizer+0xfa
0b13f500 6afd5d42 clr!Thread::ShouldChangeAbortToUnload+0x101
0b13f560 6afd5dd9 clr!Thread::ShouldChangeAbortToUnload+0x399
```

```
0b13f584 6b0bb3e5 clr!Thread::ShouldChangeAbortToUnload+0x43a
0b13f59c 6b0bb2e0 clr!ManagedThreadBase::KickOff+0x15
0b13f634 6afd5a08 clr!ThreadNative::KickOffThread+0x23e
0b13fed4 76573833 clr!Thread::intermediateThreadProc+0x4b
0b13fee0 77c1a9bd kernel32!BaseThreadInitThunk+0xe
0b13ff20 00000000 ntdll!_RtlUserThreadStart+0x23

  16  Id: 6245c.1ffe0 Suspend: 0 Teb: 7ff45000 Unfrozen
ChildEBP RetAddr
0adffac0 77c400f0 ntdll!KiFastSystemCallRet
0adffac4 76557948 ntdll!NtRemoveIoCompletion+0xc
0adffaf0 7665af2e kernel32!GetQueuedCompletionStatus+0x29
0adffb2c 7665b067 rpcrt4!COMMON_ProcessCalls+0xb5
0adffb98 7665ac4f rpcrt4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
0adffba4 7665acb9 rpcrt4!ProcessIOEventsWrapper+0xe
0adffbc8 7665ad03 rpcrt4!BaseCachedThreadRoutine+0x5c
0adffbd4 76573833 rpcrt4!ThreadStartRoutine+0x1e
0adffbe0 77c1a9bd kernel32!BaseThreadInitThunk+0xe
0adffc20 00000000 ntdll!_RtlUserThreadStart+0x23
```

Note: We see that almost all threads have **clr** module on their stack traces. We also notice that there is an exception on the finalizer thread no. 2 and there are two threads 14 and 15 which have a thrown exception.

7. Now we load the appropriate SOS extension after checking that it is not loaded and verifying **clr** module version:

```
0:000> .chain
Extension DLL search Path:
[...]
Extension DLL chain:
    dbghelp: image 6.12.0002.633, API 6.1.6, built Mon Feb 01 20:08:26 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\dbghelp.dll]
    ext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:31 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\winext\ext.dll]
    exts: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:24 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\WINXP\exts.dll]
    uext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:23 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\winext\uext.dll]
    ntsdexts: image 6.1.7650.0, API 1.0.0, built Mon Feb 01 20:08:08 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\WINXP\ntsdexts.dll]
```

```
0:000> lmv m clr
start    end        module name
6af20000 6b58f000   clr        (pdb symbols)
c:\mss\clr.pdb\C58C9AF63E5D49A8BE0DBA9C5E0093BE2\clr.pdb
    Loaded symbol image file: clr.dll
    Image path: C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.dll
    Image name: clr.dll
    Timestamp:        Thu Mar 18 07:44:47 2010 (4BA1D9EF)
    CheckSum:         00671FC0
    ImageSize:        0066F000
    File version:     4.0.30319.1
    Product version:  4.0.30319.1
    File flags:       8 (Mask 3F) Private
    File OS:          4 Unknown Win32
    File type:        2.0 Dll
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      Microsoft Corporation
    ProductName:      Microsoft® .NET Framework
    InternalName:     clr.dll
    OriginalFilename: clr.dll
    ProductVersion:   4.0.30319.1
    FileVersion:      4.0.30319.1 (RTMRel.030319-0100)
    PrivateBuild:     DDBLD766
    FileDescription:  Microsoft .NET Runtime Common Language Runtime - WorkStation
    LegalCopyright:   © Microsoft Corporation.  All rights reserved.
    Comments:         Flavor=Retail

0:000> .load C:\ANETMDA-Dumps\32-bit\Microsoft.NET\Framework\v4.0.30319\sos

0:000> .chain
Extension DLL search Path:
[...]
Extension DLL chain:
    C:\ANETMDA-Dumps\32-bit\Microsoft.NET\Framework\v4.0.30319\sos: image 4.0.30319.1, API
1.0.0, built Thu Mar 18 08:09:41 2010
        [path: C:\ANETMDA-Dumps\32-bit\Microsoft.NET\Framework\v4.0.30319\sos.dll]
    dbghelp: image 6.12.0002.633, API 6.1.6, built Mon Feb 01 20:08:26 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\dbghelp.dll]
    ext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:31 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\winext\ext.dll]
    exts: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:24 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\WINXP\exts.dll]
    uext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:23 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\winext\uext.dll]
    ntsdexts: image 6.1.7650.0, API 1.0.0, built Mon Feb 01 20:08:08 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\WINXP\ntsdexts.dll]
```

8. We now list managed stack traces:

```
0:000> ~*e !ClrStack
OS Thread Id: 0x62460 (0)
Child SP IP       Call Site
0014e76c 77c40f34 [InlinedCallFrame: 0014e76c] System.Windows.Forms.UnsafeNativeMethods.WaitMessage()
0014e768 67b3737a
System.Windows.Forms.Application+ComponentManager.System.Windows.Forms.UnsafeNativeMethods.IMsoComponentManager.FPushM
essageLoop(IntPtr, Int32, Int32)
0014e804 67b36e2c System.Windows.Forms.Application+ThreadContext.RunMessageLoopInner(Int32,
System.Windows.Forms.ApplicationContext)
0014e85c 67b36c81 System.Windows.Forms.Application+ThreadContext.RunMessageLoop(Int32,
System.Windows.Forms.ApplicationContext)
0014e88c 67ac366d System.Windows.Forms.Application.Run(System.Windows.Forms.Form)
0014e8a0 00d73f0d LINQPad.Program.Run(System.String, Boolean, System.String, Boolean, Boolean, System.String)
0014e994 00d71515 LINQPad.Program.Go(System.String[])
0014ebc4 00d70584 LINQPad.Program.Start(System.String[])
0014ec04 00d7034f LINQPad.ProgramStarter.Run(System.String[])
0014ec10 00d700f5 LINQPad.Loader.Main(System.String[])
0014ee50 6af221db [GCFrame: 0014ee50]
OS Thread Id: 0x62474 (1)
Unable to walk the managed stack. The current thread is likely not a
managed thread. You can run !threads to get a list of managed threads in
the process
OS Thread Id: 0x62478 (2)
Child SP IP       Call Site
039be33c 77c40f34 [InlinedCallFrame: 039be33c] System.Windows.Forms.UnsafeNativeMethods.WaitMessage()
039be338 67b3737a
System.Windows.Forms.Application+ComponentManager.System.Windows.Forms.UnsafeNativeMethods.IMsoComponentManager.FPushM
essageLoop(IntPtr, Int32, Int32)
039be3d4 67b36e2c System.Windows.Forms.Application+ThreadContext.RunMessageLoopInner(Int32,
System.Windows.Forms.ApplicationContext)
039be42c 67b36c81 System.Windows.Forms.Application+ThreadContext.RunMessageLoop(Int32,
System.Windows.Forms.ApplicationContext)
039be45c 6802fefb System.Windows.Forms.Application.RunDialog(System.Windows.Forms.Form)
039be470 68059f83 System.Windows.Forms.Form.ShowDialog(System.Windows.Forms.IWin32Window)
039be474 6805a1b7 [InlinedCallFrame: 039be474]
039be50c 6805a1b7 System.Windows.Forms.Form.ShowDialog()
039be510 0543a204 LINQPad.Program.CurrentDomain_UnhandledException(System.Object, System.UnhandledExceptionEventArgs)
039be8d0 6af221db [GCFrame: 039be8d0]
039be96c 6af221db [GCFrame: 039be96c]
039be9cc 6af221db [GCFrame: 039be9cc]
039bea88 6af221db [ContextTransitionFrame: 039bea88]
039bec0c 6af221db [GCFrame: 039bec0c]
039bed0c 6af221db [GCFrame: 039bed0c]
039bed9c 6af221db [GCFrame: 039bed9c]
039bf628 6af221db [DebuggerU2MCatchHandlerFrame: 039bf628]
039bf3f0 05602dfc UserQuery+SmallObject.Finalize()
039bf628 6afd4b01 [DebuggerU2MCatchHandlerFrame: 039bf628]
039bf6c0 6afd4b01 [ContextTransitionFrame: 039bf6c0]
039bf7a4 6afd4b01 [GCFrame: 039bf7a4]
039bf908 6afd4b01 [DebuggerU2MCatchHandlerFrame: 039bf908]
OS Thread Id: 0x6247c (3)
Child SP IP       Call Site
0483f5bc 77c40f34 [InlinedCallFrame: 0483f5bc]
0483f5b8 68fc80b7 DomainNeutralILStubClass.IL_STUB_PInvoke(Microsoft.Win32.SafeHandles.SafePipeHandle, IntPtr)
0483f5bc 6905c07c [InlinedCallFrame: 0483f5bc]
Microsoft.Win32.UnsafeNativeMethods.ConnectNamedPipe(Microsoft.Win32.SafeHandles.SafePipeHandle, IntPtr)
0483f620 6905c07c System.IO.Pipes.NamedPipeServerStream.WaitForConnection()
0483f630 00d731ed LINQPad.Program.Listen()
0483f6c8 6962ae5b System.Threading.ThreadHelper.ThreadStart_Context(System.Object)
0483f6d8 695b7ff4 System.Threading.ExecutionContext.Run(System.Threading.ExecutionContext,
System.Threading.ContextCallback, System.Object, Boolean)
0483f6fc 695b7f34 System.Threading.ExecutionContext.Run(System.Threading.ExecutionContext,
System.Threading.ContextCallback, System.Object)
0483f718 6962ade8 System.Threading.ThreadHelper.ThreadStart()
0483f93c 6af221db [GCFrame: 0483f93c]
0483fc00 6af221db [DebuggerU2MCatchHandlerFrame: 0483fc00]
OS Thread Id: 0x62480 (4)
Unable to walk the managed stack. The current thread is likely not a
managed thread. You can run !threads to get a list of managed threads in
the process
OS Thread Id: 0x62490 (5)
Unable to walk the managed stack. The current thread is likely not a
managed thread. You can run !threads to get a list of managed threads in
```

```
the process
OS Thread Id: 0x624a0 (6)
Child SP IP       Call Site
05e1f480 77c40f34 [GCFrame: 05e1f480]
05e1f574 77c40f34 [HelperMethodFrame_1OBJ: 05e1f574] System.Threading.Monitor.ObjWait(Boolean, Int32, System.Object)
05e1f5d0 695b9140 System.Threading.Monitor.Wait(System.Object, Int32, Boolean)
05e1f5e0 69b7428a System.Threading.Monitor.Wait(System.Object)
05e1f5e4 00d7d13a ActiproSoftware.SyntaxEditor.SemanticParserService.c()
05e1f6a8 6962ae5b System.Threading.ThreadHelper.ThreadStart_Context(System.Object)
05e1f6b8 695b7ff4 System.Threading.ExecutionContext.Run(System.Threading.ExecutionContext,
System.Threading.ContextCallback, System.Object, Boolean)
05e1f6dc 695b7f34 System.Threading.ExecutionContext.Run(System.Threading.ExecutionContext,
System.Threading.ContextCallback, System.Object)
05e1f6f8 6962ade8 System.Threading.ThreadHelper.ThreadStart()
05e1f91c 6af221db [GCFrame: 05e1f91c]
05e1fbe0 6af221db [DebuggerU2MCatchHandlerFrame: 05e1fbe0]
OS Thread Id: 0x624c8 (7)
Child SP IP       Call Site
05caf454 77c415a9 [HelperMethodFrame_1OBJ: 05caf454]
System.Threading.WaitHandle.WaitMultiple(System.Threading.WaitHandle[], Int32, Boolean, Boolean)
05caf51c 695f573b System.Threading.WaitHandle.WaitAny(System.Threading.WaitHandle[], Int32, Boolean)
05caf53c 6a7b6e1e System.Net.TimerThread.ThreadProc()
05caf598 6962ae5b System.Threading.ThreadHelper.ThreadStart_Context(System.Object)
05caf5a8 695b7ff4 System.Threading.ExecutionContext.Run(System.Threading.ExecutionContext,
System.Threading.ContextCallback, System.Object, Boolean)
05caf5cc 695b7f34 System.Threading.ExecutionContext.Run(System.Threading.ExecutionContext,
System.Threading.ContextCallback, System.Object)
05caf5e8 6962ade8 System.Threading.ThreadHelper.ThreadStart()
05caf80c 6af221db [GCFrame: 05caf80c]
05cafad0 6af221db [DebuggerU2MCatchHandlerFrame: 05cafad0]
OS Thread Id: 0x62518 (8)
Child SP IP       Call Site
065becf8 77c40f34 [HelperMethodFrame_1OBJ: 065becf8]
System.Threading.WaitHandle.WaitOneNative(System.Runtime.InteropServices.SafeHandle, UInt32, Boolean, Boolean)
065beda0 6962b5ef System.Threading.WaitHandle.InternalWaitOne(System.Runtime.InteropServices.SafeHandle, Int64,
Boolean, Boolean)
065bedbc 6962b5ad System.Threading.WaitHandle.WaitOne(Int32, Boolean)
065bedd4 6962b570 System.Threading.WaitHandle.WaitOne()
065beddc 052507d4 ActiproBridge.ReferenceManager+?15?.<StartAdvanceFeeder>b__4()
065bee18 6962ae5b System.Threading.ThreadHelper.ThreadStart_Context(System.Object)
065bee28 695b7ff4 System.Threading.ExecutionContext.Run(System.Threading.ExecutionContext,
System.Threading.ContextCallback, System.Object, Boolean)
065bee4c 695b7f34 System.Threading.ExecutionContext.Run(System.Threading.ExecutionContext,
System.Threading.ContextCallback, System.Object)
065bee68 6962ade8 System.Threading.ThreadHelper.ThreadStart()
065bf08c 6af221db [GCFrame: 065bf08c]
065bf350 6af221db [DebuggerU2MCatchHandlerFrame: 065bf350]
OS Thread Id: 0x62520 (9)
Unable to walk the managed stack. The current thread is likely not a
managed thread. You can run !threads to get a list of managed threads in
the process
OS Thread Id: 0x62524 (10)
Child SP IP       Call Site
GetFrameContext failed: 1
OS Thread Id: 0x62538 (11)
Unable to walk the managed stack. The current thread is likely not a
managed thread. You can run !threads to get a list of managed threads in
the process
OS Thread Id: 0x62544 (12)
Child SP IP       Call Site
GetFrameContext failed: 1
OS Thread Id: 0x62548 (13)
Child SP IP       Call Site
0a8adfc8 77c40f34 [HelperMethodFrame_1OBJ: 0a8adfc8] System.Threading.Thread.JoinInternal()
0a8ae01c 0560271d UserQuery+ClassMain.Main()
0a8ae038 05602612 UserQuery.RunUserAuthoredQuery()
0a8ae584 6af221db [DebuggerU2MCatchHandlerFrame: 0a8ae584]
0a8ae550 6af221db [CustomGCFrame: 0a8ae550]
0a8ae524 6af221db [GCFrame: 0a8ae524]
0a8ae508 6af221db [GCFrame: 0a8ae508]
0a8ae72c 6af221db [HelperMethodFrame_PROTECTOBJ: 0a8ae72c]
System.RuntimeMethodHandle._InvokeMethodFast(System.IRuntimeMethodInfo, System.Object, System.Object[],
System.SignatureStruct ByRef, System.Reflection.MethodAttributes, System.RuntimeType)
0a8ae7a8 6963d689 System.RuntimeMethodHandle.InvokeMethodFast(System.IRuntimeMethodInfo, System.Object,
System.Object[], System.Signature, System.Reflection.MethodAttributes, System.RuntimeType)
```

```
0a8ae7fc 6963d3d0 System.Reflection.RuntimeMethodInfo.Invoke(System.Object, System.Reflection.BindingFlags,
System.Reflection.Binder, System.Object[], System.Globalization.CultureInfo, Boolean)
0a8ae838 6963bfed System.Reflection.RuntimeMethodInfo.Invoke(System.Object, System.Reflection.BindingFlags,
System.Reflection.Binder, System.Object[], System.Globalization.CultureInfo)
0a8ae85c 69643284 System.Reflection.MethodBase.Invoke(System.Object, System.Object[])
0a8ae868 0560168c LINQPad.ExecutionModel.Server.RunClrQuery()
0a8aea7c 05600988 LINQPad.ExecutionModel.Server.StartClrQuery()
0a8aead8 6962ae5b System.Threading.ThreadHelper.ThreadStart_Context(System.Object)
0a8aeae8 695b7ff4 System.Threading.ExecutionContext.Run(System.Threading.ExecutionContext,
System.Threading.ContextCallback, System.Object, Boolean)
0a8aeb0c 695b7f34 System.Threading.ExecutionContext.Run(System.Threading.ExecutionContext,
System.Threading.ContextCallback, System.Object)
0a8aeb28 6962ade8 System.Threading.ThreadHelper.ThreadStart()
0a8aed40 6af221db [GCFrame: 0a8aed40]
0a8af004 6af221db [DebuggerU2MCatchHandlerFrame: 0a8af004]
0a8af09c 6af221db [ContextTransitionFrame: 0a8af09c]
0a8af220 6af221db [DebuggerU2MCatchHandlerFrame: 0a8af220]
OS Thread Id: 0x6254c (14)
Child SP IP       Call Site
0a62dd5c 77c40f34 [InlinedCallFrame: 0a62dd5c] System.Windows.Forms.UnsafeNativeMethods.WaitMessage()
0a62dd58 67b3737a
System.Windows.Forms.Application+ComponentManager.System.Windows.Forms.UnsafeNativeMethods.IMsoComponentManager.FPushM
essageLoop(IntPtr, Int32, Int32)
0a62ddf4 67b36e2c System.Windows.Forms.Application+ThreadContext.RunMessageLoopInner(Int32,
System.Windows.Forms.ApplicationContext)
0a62de4c 67b36c81 System.Windows.Forms.Application+ThreadContext.RunMessageLoop(Int32,
System.Windows.Forms.ApplicationContext)
0a62de7c 6802fefb System.Windows.Forms.Application.RunDialog(System.Windows.Forms.Form)
0a62de90 68059f83 System.Windows.Forms.Form.ShowDialog(System.Windows.Forms.IWin32Window)
0a62de94 6805a1b7 [InlinedCallFrame: 0a62de94]
0a62df2c 6805a1b7 System.Windows.Forms.Form.ShowDialog()
0a62df30 0543a204 LINQPad.Program.CurrentDomain_UnhandledException(System.Object, System.UnhandledExceptionEventArgs)
0a62e2f0 6af221db [GCFrame: 0a62e2f0]
0a62e38c 6af221db [GCFrame: 0a62e38c]
0a62e3ec 6af221db [GCFrame: 0a62e3ec]
0a62e4a8 6af221db [ContextTransitionFrame: 0a62e4a8]
0a62e62c 6af221db [GCFrame: 0a62e62c]
0a62e728 6af221db [GCFrame: 0a62e728]
0a62e7b8 6af221db [GCFrame: 0a62e7b8]
0a62ef70 6af221db [HelperMethodFrame: 0a62ef70]
0a62efc0 05602765 UserQuery+ClassMain.thread_proc_1()
0a62efc8 6962ae5b System.Threading.ThreadHelper.ThreadStart_Context(System.Object)
0a62efd8 695b7ff4 System.Threading.ExecutionContext.Run(System.Threading.ExecutionContext,
System.Threading.ContextCallback, System.Object, Boolean)
0a62effc 695b7f34 System.Threading.ExecutionContext.Run(System.Threading.ExecutionContext,
System.Threading.ContextCallback, System.Object)
0a62f018 6962ade8 System.Threading.ThreadHelper.ThreadStart()
0a62f230 6af221db [GCFrame: 0a62f230]
0a62f4f4 6af221db [DebuggerU2MCatchHandlerFrame: 0a62f4f4]
0a62f58c 6af221db [ContextTransitionFrame: 0a62f58c]
0a62f710 6af221db [DebuggerU2MCatchHandlerFrame: 0a62f710]
OS Thread Id: 0x62558 (15)
Child SP IP       Call Site
0b13da9c 77c40f34 [InlinedCallFrame: 0b13da9c] System.Windows.Forms.UnsafeNativeMethods.WaitMessage()
0b13da98 67b3737a
System.Windows.Forms.Application+ComponentManager.System.Windows.Forms.UnsafeNativeMethods.IMsoComponentManager.FPushM
essageLoop(IntPtr, Int32, Int32)
0b13db34 67b36e2c System.Windows.Forms.Application+ThreadContext.RunMessageLoopInner(Int32,
System.Windows.Forms.ApplicationContext)
0b13db8c 67b36c81 System.Windows.Forms.Application+ThreadContext.RunMessageLoop(Int32,
System.Windows.Forms.ApplicationContext)
0b13dbbc 6802fefb System.Windows.Forms.Application.RunDialog(System.Windows.Forms.Form)
0b13dbd0 68059f83 System.Windows.Forms.Form.ShowDialog(System.Windows.Forms.IWin32Window)
0b13dbd4 6805a1b7 [InlinedCallFrame: 0b13dbd4]
0b13dc6c 6805a1b7 System.Windows.Forms.Form.ShowDialog()
0b13dc70 0543a204 LINQPad.Program.CurrentDomain_UnhandledException(System.Object, System.UnhandledExceptionEventArgs)
0b13e030 6af221db [GCFrame: 0b13e030]
0b13e0cc 6af221db [GCFrame: 0b13e0cc]
0b13e12c 6af221db [GCFrame: 0b13e12c]
0b13e1e8 6af221db [ContextTransitionFrame: 0b13e1e8]
0b13e36c 6af221db [GCFrame: 0b13e36c]
0b13e470 6af221db [GCFrame: 0b13e470]
0b13e500 6af221db [GCFrame: 0b13e500]
0b13ecb8 6af221db [HelperMethodFrame: 0b13ecb8]
0b13ed08 056028bb UserQuery+ClassMain.thread_proc_3()
0b13edd8 6962ae5b System.Threading.ThreadHelper.ThreadStart_Context(System.Object)
```

```
0b13ede8 695b7ff4 System.Threading.ExecutionContext.Run(System.Threading.ExecutionContext,
System.Threading.ContextCallback, System.Object, Boolean)
0b13ee0c 695b7f34 System.Threading.ExecutionContext.Run(System.Threading.ExecutionContext,
System.Threading.ContextCallback, System.Object)
0b13ee28 6962ade8 System.Threading.ThreadHelper.ThreadStart()
0b13f040 6af221db [GCFrame: 0b13f040]
0b13f304 6af221db [DebuggerU2MCatchHandlerFrame: 0b13f304]
0b13f39c 6af221db [ContextTransitionFrame: 0b13f39c]
0b13f520 6af221db [DebuggerU2MCatchHandlerFrame: 0b13f520]
OS Thread Id: 0x1ffe0 (16)
Unable to walk the managed stack. The current thread is likely not a
managed thread. You can run !threads to get a list of managed threads in
the process
```

9. Then we list managed threads:

```
0:000> !Threads
ThreadCount:      50014
UnstartedThread:  0
BackgroundThread: 8
PendingThread:    0
DeadThread:       50003
Hosted Runtime:   no
                                    PreEmptive   GC Alloc                 Lock
       ID  OSID ThreadOBJ    State GC           Context       Domain   Count APT Exception
   0    1 62460 0020bc78      6020 Enabled  4a1c3ef0:4a1c4bb8 002017d0     0 STA
   2    2 62478 00216b18      b220 Enabled  00000000:00000000 002017d0     0 MTA (Finalizer)
   3    3 6247c 00277490      b220 Enabled  00000000:00000000 002017d0     0 MTA
XXXX    5       050a0048     19820 Enabled  00000000:00000000 002017d0     0 Ukn
   6    6 624a0 002bc318   200b220 Enabled  00000000:00000000 002017d0     0 MTA
   7    7 624c8 050c7e18   200b220 Enabled  00000000:00000000 002017d0     1 MTA
   8    4 62518 05100a90   200b220 Enabled  00000000:00000000 002017d0     0 MTA
  10    8 62524 0511d890   8009220 Enabled  00000000:00000000 002017d0     0 MTA (Threadpool Completion
Port)
  12    b 62544 0517bc68      1220 Enabled  00000000:00000000 002017d0     0 Ukn
  13    c 62548 0515a108   2007220 Enabled  00000000:00000000 05179888     0 STA
  14    a 6254c 0513e8f8      b020 Enabled  00000000:00000000 002017d0     0 MTA
XXXX    9       051617a0     19820 Enabled  00000000:00000000 002017d0     0 Ukn
XXXX    d       051622b8     19820 Enabled  00000000:00000000 002017d0     0 Ukn
  15    e 62558 05162dd0      b020 Enabled  00000000:00000000 002017d0     0 MTA
System.Runtime.Serialization.SerializationException (098be808) (nested exceptions)
XXXX    f       051627b0     19820 Enabled  00000000:00000000 002017d0     0 Ukn
XXXX   10       0a1b1380     19820 Enabled  00000000:00000000 002017d0     0 Ukn
XXXX   11       0a1b45c0     19820 Enabled  00000000:00000000 002017d0     0 Ukn
XXXX   12       0a1c43a8     19820 Enabled  00000000:00000000 002017d0     0 Ukn
XXXX   13       0a1c48b0     19820 Enabled  00000000:00000000 002017d0     0 Ukn
XXXX   14       0a1c4db8     19820 Enabled  00000000:00000000 002017d0     0 Ukn
XXXX   15       0a1c52c0     19820 Enabled  00000000:00000000 002017d0     0 Ukn
XXXX   16       0a1c57c8     19820 Enabled  00000000:00000000 002017d0     0 Ukn
XXXX   17       0a1c5cd0     19820 Enabled  00000000:00000000 002017d0     0 Ukn
XXXX   18       0a1c61d8     19820 Enabled  00000000:00000000 002017d0     0 Ukn
XXXX   19       0a1c66e0     19820 Enabled  00000000:00000000 002017d0     0 Ukn
XXXX   1a       0a1c6be8     19820 Enabled  00000000:00000000 002017d0     0 Ukn
XXXX   1b       0a1c70f0     19820 Enabled  00000000:00000000 002017d0     0 Ukn
XXXX   1c       0a1c75f8     19820 Enabled  00000000:00000000 002017d0     0 Ukn
XXXX   1d       0a1c7b00     19820 Enabled  00000000:00000000 002017d0     0 Ukn
XXXX   1e       0a1bc3a8     19820 Enabled  00000000:00000000 002017d0     0 Ukn
XXXX   1f       0a1bc8b0     19820 Enabled  00000000:00000000 002017d0     0 Ukn
XXXX   20       0a1bcdb8     19820 Enabled  00000000:00000000 002017d0     0 Ukn
XXXX   21       0a1bd2c0     19820 Enabled  00000000:00000000 002017d0     0 Ukn
XXXX   22       0a1bd7c8     19820 Enabled  00000000:00000000 002017d0     0 Ukn
[...]
```

Note: We see the endless list of threads and use Ctrl-Break to stop the output. Thread count is more than 50,000 and all of them are dead but not released, and this means we have a thread handle leak. We also see that the thread 15 has an exception which also has nested exceptions.

10. We double check managed exceptions by running **!PrintException** (**!pe**) for every thread:

```
0:000> ~*e !pe
There is no current managed exception on this thread
The current thread is unmanaged
There is no current managed exception on this thread
There is no current managed exception on this thread
The current thread is unmanaged
The current thread is unmanaged
There is no current managed exception on this thread
There is no current managed exception on this thread
There is no current managed exception on this thread
The current thread is unmanaged
There is no current managed exception on this thread
The current thread is unmanaged
There is no current managed exception on this thread
There is no current managed exception on this thread
There is no current managed exception on this thread
Exception object: 098be808
Exception type:   System.Runtime.Serialization.SerializationException
Message:          Type 'UserQuery+CustomException' in Assembly 'query_uobgah, Version=0.0.0.0,
Culture=neutral, PublicKeyToken=null' is not marked as serializable.
InnerException:   <none>
StackTrace (generated):
<none>
StackTraceString: <none>
HResult: 8013150c
There are nested exceptions on this thread. Run with -nested for details
The current thread is unmanaged
```

Note: We switch to the thread 15 and try to get the nested exception as well:

```
0:000> ~15s
eax=00000000 ebx=098c4d04 ecx=0000025c edx=0b490000 esi=098cd5e0 edi=0be93974
eip=77c40f34 esp=0b13da90 ebp=0b13db24 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
ntdll!KiFastSystemCallRet:
77c40f34 c3              ret

0:015> !pe -nested
Exception object: 098be808
Exception type:   System.Runtime.Serialization.SerializationException
Message:          Type 'UserQuery+CustomException' in Assembly 'query_uobgah, Version=0.0.0.0,
Culture=neutral, PublicKeyToken=null' is not marked as serializable.
InnerException:   <none>
StackTrace (generated):
<none>
StackTraceString: <none>
HResult: 8013150c

Nested exception -------------------------------------------------------------
Exception object: 098b924c
Exception type:   System.IO.FileNotFoundException
Message:          Unable to find the specified file.
InnerException:   <none>
StackTrace (generated):
    SP       IP       Function
    0B13EDA8 0560288A UNKNOWN!UserQuery+ClassMain.thread_proc_3()+0x2a
```

```
StackTraceString: <none>
HResult: 80070002
```

Note: We see it was thrown from **thread_proc_3** method. We see that **FileNotFoundException** was initially thrown (inner) but then rethrown (translated). Let's check the stack trace with all parameters and local variables if any:

```
0:015> !CLRStack -a
OS Thread Id: 0x62558 (15)
Child SP IP       Call Site
0b13da9c 77c40f34 [InlinedCallFrame: 0b13da9c] System.Windows.Forms.UnsafeNativeMethods.WaitMessage()
0b13da98 67b3737a
System.Windows.Forms.Application+ComponentManager.System.Windows.Forms.UnsafeNativeMethods.IMsoComponentManager.FPushM
essageLoop(IntPtr, Int32, Int32)
    PARAMETERS:
        this (0x0b13dad0) = 0x098cd5ac
        dwComponentID = <no data>
        reason (0x0b13db30) = 0x00000004
        pvLoopData (0x0b13db2c) = 0x00000000
    LOCALS:
        <no data>
        0x0b13db00 = 0x00000001
        0x0b13dafc = 0x00000001
        0x0b13dacc = 0x00000000
        <no data>
        <no data>
        <no data>
        0x0b13dac8 = 0x098c4d04
        <no data>
        <no data>
        <no data>
        <no data>
        <no data>
        <no data>
        0x0b13dad8 = 0x00000000
        0x0b13dac4 = 0x0991006c

0b13db34 67b36e2c System.Windows.Forms.Application+ThreadContext.RunMessageLoopInner(Int32,
System.Windows.Forms.ApplicationContext)
    PARAMETERS:
        this (0x0b13db48) = 0x098c4d04
        reason (0x0b13db5c) = 0x00000004
        context (0x0b13db88) = 0x098cd560
    LOCALS:
        0x0b13db44 = 0x00000000
        0x0b13db58 = 0x00000001
        <no data>
        <no data>
        <no data>

0b13db8c 67b36c81 System.Windows.Forms.Application+ThreadContext.RunMessageLoop(Int32,
System.Windows.Forms.ApplicationContext)
    PARAMETERS:
        this = <no data>
        reason = <no data>
        context = <no data>
    LOCALS:
        0x0b13db8c = 0x00000000

0b13dbbc 6802fefb System.Windows.Forms.Application.RunDialog(System.Windows.Forms.Form)
    PARAMETERS:
        form = <no data>

0b13dbd0 68059f83 System.Windows.Forms.Form.ShowDialog(System.Windows.Forms.IWin32Window)
    PARAMETERS:
        this (0x0b13dc04) = 0x098c302c
        owner = <no data>
    LOCALS:
        <no data>
        0x0b13dc40 = 0x00000000
        0x0b13dc3c = 0x00000000
        0x0b13dbfc = 0x00000000
        <no data>
```

```
        <no data>
        <no data>
        <no data>
        <no data>
        <no data>

0b13dbd4 6805a1b7 [InlinedCallFrame: 0b13dbd4]
0b13dc6c 6805a1b7 System.Windows.Forms.Form.ShowDialog()
    PARAMETERS:
        this = <no data>

0b13dc70 0543a204 LINQPad.Program.CurrentDomain_UnhandledException(System.Object, System.UnhandledExceptionEventArgs)
    PARAMETERS:
        sender (0x0b13dca0) = 0x018912c8
        e (0x0b13dc8c) = 0x098c1458
    LOCALS:
        0x0b13dc9c = 0x00000000

0b13e030 6af221db [GCFrame: 0b13e030]
0b13e0cc 6af221db [GCFrame: 0b13e0cc]
0b13e12c 6af221db [GCFrame: 0b13e12c]
0b13e1e8 6af221db [ContextTransitionFrame: 0b13e1e8]
0b13e36c 6af221db [GCFrame: 0b13e36c]
0b13e470 6af221db [GCFrame: 0b13e470]
0b13e500 6af221db [GCFrame: 0b13e500]
0b13ecb8 6af221db [HelperMethodFrame: 0b13ecb8]
0b13ed08 056028bb UserQuery+ClassMain.thread_proc_3()
    PARAMETERS:
        this = <no data>

0b13edd8 6962ae5b System.Threading.ThreadHelper.ThreadStart_Context(System.Object)
    PARAMETERS:
        state = <no data>
    LOCALS:
        <no data>

0b13ede8 695b7ff4 System.Threading.ExecutionContext.Run(System.Threading.ExecutionContext,
System.Threading.ContextCallback, System.Object, Boolean)
    PARAMETERS:
        executionContext = <no data>
        callback = <no data>
        state = <no data>
        ignoreSyncCtx = <no data>
    LOCALS:
        <no data>

0b13ee0c 695b7f34 System.Threading.ExecutionContext.Run(System.Threading.ExecutionContext,
System.Threading.ContextCallback, System.Object)
    PARAMETERS:
        executionContext = <no data>
        callback = <no data>
        state = <no data>

0b13ee28 6962ade8 System.Threading.ThreadHelper.ThreadStart()
    PARAMETERS:
        this = <no data>

0b13f040 6af221db [GCFrame: 0b13f040]
0b13f304 6af221db [DebuggerU2MCatchHandlerFrame: 0b13f304]
0b13f39c 6af221db [ContextTransitionFrame: 0b13f39c]
0b13f520 6af221db [DebuggerU2MCatchHandlerFrame: 0b13f520]
```

Note: We examine the second parameter to **_UnhandledException** method (e) as it might point us to an exception:

```
0:015> !DumpObj 0x098c1458
Name:        System.UnhandledExceptionEventArgs
MethodTable: 69680f24
EEClass:     693c357c
Size:        16(0x10) bytes
File:        C:\Windows\Microsoft.Net\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll
Fields:
      MT    Field   Offset                 Type VT     Attr    Value Name
69693fc0  40001c7       40     System.EventArgs  0   shared   static Empty
    >> Domain:Value  002017d0:018b6770 05179888:NotInit  <<
6969f5e8  400064f        4        System.Object  0 instance 098be808 _Exception
696a662c  4000650        8       System.Boolean  1 instance        0 _IsTerminating

0:000> !DumpObj 098be808
Name:        System.Runtime.Serialization.SerializationException
MethodTable: 69693814
EEClass:     693d1334
Size:        84(0x54) bytes
File:        C:\Windows\Microsoft.Net\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll
Fields:
      MT    Field   Offset                 Type VT     Attr    Value Name
6969f9ac  400004a        4        System.String  0 instance 098be8ac _className
696a01f4  400004b        8 ...ection.MethodBase  0 instance 00000000 _exceptionMethod
6969f9ac  400004c        c        System.String  0 instance 098bf0b4 _exceptionMethodString
6969f9ac  400004d       10        System.String  0 instance 098be920 _message
69694004  400004e       14 ...tions.IDictionary  0 instance 00000000 _data
6969fc0c  400004f       18     System.Exception  0 instance 00000000 _innerException
6969f9ac  4000050       1c        System.String  0 instance 00000000 _helpURL
6969f5e8  4000051       20        System.Object  0 instance 00000000 _stackTrace
6969f5e8  4000052       24        System.Object  0 instance 098bf4e0 _watsonBuckets
6969f9ac  4000053       28        System.String  0 instance 00000000 _stackTraceString
6969f9ac  4000054       2c        System.String  0 instance 098c0be4 _remoteStackTraceString
696a2978  4000055       3c         System.Int32  1 instance        0 _remoteStackIndex
6969f5e8  4000056       30        System.Object  0 instance 00000000 _dynamicMethods
696a2978  4000057       40         System.Int32  1 instance -2146233076 _HResult
6969f9ac  4000058       34        System.String  0 instance 098bf4c0 _source
6969aa2c  4000059       44        System.IntPtr  1 instance        0 _xptrs
696a2978  400005a       48         System.Int32  1 instance        0 _xcode
6965a29c  400005b       4c       System.UIntPtr  1 instance        0 _ipForWatsonBuckets
69659888  400005c       38 ...ializationManager  0 instance 098c0bc8 _safeSerializationManager
6969f9ac  40010e7      338        System.String  0   shared   static _nullMessage
    >> Domain:Value  002017d0:NotInit  05179888:NotInit  <<
```

11. We now check unmanaged stack trace:

```
0:015> kL
ChildEBP RetAddr
0b13da8c 7674b5b4 ntdll!KiFastSystemCallRet
0b13da90 67b3737a user32!NtUserWaitMessage+0xc
0b13db24 67b36e2c System_Windows_Forms_ni+0x22737a
0b13db80 67b36c81 System_Windows_Forms_ni+0x226e2c
0b13dbb0 6802fefb System_Windows_Forms_ni+0x226c81
0b13dbc8 68059f83 System_Windows_Forms_ni+0x71fefb
0b13dc64 6805a1b7 System_Windows_Forms_ni+0x749f83
0b13dca4 6af221db System_Windows_Forms_ni+0x74a1b7
0b13dcb4 6af44a2a clr!CallDescrWorker+0x33
0b13dd30 6af44bcc clr!CallDescrWorkerWithHandler+0x8e
0b13de80 6af44c01 clr!MethodDesc::CallDescr+0x194
0b13de9c 6b192379 clr!MethodDesc::CallTargetWorker+0x21
0b13df94 6b134ad1 clr!ExceptionNotifications::DeliverExceptionNotification+0x98
0b13e008 6b134e86 clr!COMDelegate::BindToMethodInfo+0x504
0b13e0ac 6b11c19b clr!DistributeUnhandledExceptionReliably+0xeb
0b13e104 6b11bfd3 clr!AppDomain::RaiseUnhandledExceptionEvent+0xba
0b13e19c 6b0a8688 clr!AppDomain::RaiseUnhandledExceptionEvent_Wrapper+0x1cd
0b13e274 6b11c13e clr!Thread::DoADCallBack+0xe0
0b13e2d0 6b11de38 clr!AppDomain::RaiseUnhandledExceptionEvent+0xc2
```

```
0b13e344 6b11e807 clr!AppDomain::RaiseUnhandledExceptionEventNoThrow+0x7a
0b13e3a0 6b19518a clr!AppDomain::OnUnhandledException+0x81
0b13e4bc 6b1969c1 clr!NotifyAppDomainsOfUnhandledException+0x141
0b13e6ac 6b196f8f clr!DefaultCatchHandler+0xdb
0b13e6d8 6b01c411 clr!DefaultCatchHandler+0x623
0b13e6e8 6b01c45b clr!ThreadBaseExceptionAppDomainFilter+0x13
0b13e720 6b01c4df clr!ManagedThreadCallState::IsAppDomainEqual+0x9c
0b13e728 71262b04 clr!Thread::ShouldChangeAbortToUnload+0x3af
0b13e73c 71284ae4 MSVCR100_CLR0400!_EH4_CallFilterFunc+0x12
0b13e768 6aff14b8 MSVCR100_CLR0400!_except_handler4_common+0x8e
0b13e788 77c41039 clr!_except_handler4+0x20
0b13e7ac 77c4100b ntdll!ExecuteHandler2+0x26
0b13e854 77c40e97 ntdll!ExecuteHandler+0x24
0b13e854 7654b09e ntdll!KiUserExceptionDispatcher+0xf
0b13ebb0 6afaac08 kernel32!RaiseException+0x58
0b13ec40 6afaae41 clr!RaiseTheExceptionInternalOnly+0x276
0b13ed00 056028bb clr!IL_Throw+0x14c
WARNING: Frame IP not in any known module. Following frames may be wrong.
0b13edd0 6962ae5b 0x56028bb
0b13ede0 695b7ff4 mscorlib_ni+0x2aae5b
0b13edfc 695b7f34 mscorlib_ni+0x237ff4
0b13ee1c 6962ade8 mscorlib_ni+0x237f34
0b13ee34 6af221db mscorlib_ni+0x2aade8
0b13ee44 6af44a2a clr!CallDescrWorker+0x33
0b13eec0 6af44bcc clr!CallDescrWorkerWithHandler+0x8e
0b13eff8 6af44c01 clr!MethodDesc::CallDescr+0x194
0b13f014 6b0bb512 clr!MethodDesc::CallTargetWorker+0x21
0b13f220 6afd5c05 clr!ThreadNative::KickOffThread_Worker+0x1e1
0b13f234 6afd5c87 clr!Thread::DoExtraWorkForFinalizer+0x114
0b13f2e4 6afd5d42 clr!Thread::ShouldChangeAbortToUnload+0x101
0b13f344 6afc37a2 clr!Thread::ShouldChangeAbortToUnload+0x399
0b13f350 6b0a6465 clr!Thread::RaiseCrossContextException+0x3f8
0b13f430 6afc37cf clr!Thread::DoADCallBack+0xf0
0b13f450 6afd5c87 clr!Thread::DoExtraWorkForFinalizer+0xfa
0b13f500 6afd5d42 clr!Thread::ShouldChangeAbortToUnload+0x101
0b13f560 6afd5dd9 clr!Thread::ShouldChangeAbortToUnload+0x399
0b13f584 6b0bb3e5 clr!Thread::ShouldChangeAbortToUnload+0x43a
0b13f59c 6b0bb2e0 clr!ManagedThreadBase::KickOff+0x15
0b13f634 6afd5a08 clr!ThreadNative::KickOffThread+0x23e
0b13fed4 76573833 clr!Thread::intermediateThreadProc+0x4b
0b13fee0 77c1a9bd kernel32!BaseThreadInitThunk+0xe
0b13ff20 00000000 ntdll!_RtlUserThreadStart+0x23
```

Note: We notice **RaiseException** call and want to check what exception was raised. Here **KiUserExceptionDispatcher** frame might point us to the right exception context that was saved at the time of the exception. Here we need to dump verbose stack trace:

```
0:015> kv
ChildEBP RetAddr  Args to Child
0b13da8c 7674b5b4 67b3737a bb1f3dee 6af25d80 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
0b13da90 67b3737a bb1f3dee 6af25d80 0b13dbd4 user32!NtUserWaitMessage+0xc (FPO: [0,0,0])
0b13db24 67b36e2c 00000000 00000004 00000000 System_Windows_Forms_ni+0x22737a
0b13db80 67b36c81 098cd560 00000000 00000000 System_Windows_Forms_ni+0x226e2c
0b13dbb0 6802fefb 0994c0b8 00000000 00772010 System_Windows_Forms_ni+0x226c81
0b13dbc8 68059f83 bb1f3dee 6af25d80 0b13e030 System_Windows_Forms_ni+0x71fefb
0b13dc64 6805a1b7 0543a204 09907aa0 09907aa0 System_Windows_Forms_ni+0x749f83
0b13dca4 6af221db ffffffff 6af30bcc 0b13dd30 System_Windows_Forms_ni+0x74a1b7
0b13dcb4 6af44a2a 0b13dd84 00000001 0b13dd50 clr!CallDescrWorker+0x33
0b13dd30 6af44bcc 0b13dd84 00000001 0b13dd50 clr!CallDescrWorkerWithHandler+0x8e (FPO: [Non-Fpo])
0b13de80 6af44c01 6957ced8 0b13dec8 0b13df78 clr!MethodDesc::CallDescr+0x194 (FPO: [Non-Fpo])
0b13de9c 6b192379 6957ced8 0b13dec8 0b13df78 clr!MethodDesc::CallTargetWorker+0x21 (FPO: [Non-Fpo])
0b13df94 6b134ad1 00000001 0b13e0fc 0b13e184 clr!ExceptionNotifications::DeliverExceptionNotification+0x98 (FPO: [Non-
Fpo])
0b13e008 6b134e86 0b13e0fc 0b13e184 0b13e088 clr!COMDelegate::BindToMethodInfo+0x504 (FPO: [Non-Fpo])
0b13e0ac 6b11c19b 0b13e0fc 0b13e184 0b13e180 clr!DistributeUnhandledExceptionReliably+0xeb (FPO: [Non-Fpo])
0b13e104 6b11bfd3 0b13e184 0b13e180 00000000 clr!AppDomain::RaiseUnhandledExceptionEvent+0xba (FPO: [Non-Fpo])
0b13e19c 6b0a8688 0b13e2b0 b16ccf52 00000000 clr!AppDomain::RaiseUnhandledExceptionEvent_Wrapper+0x1cd (FPO: [Non-
Fpo])
0b13e274 6b11c13e 002017d0 6b11befb 0b13e2b0 clr!Thread::DoADCallBack+0xe0 (FPO: [Non-Fpo])
0b13e2d0 6b11de38 0b13e390 0b13e4a8 00000000 clr!AppDomain::RaiseUnhandledExceptionEvent+0xc2 (FPO: [Non-Fpo])
0b13e344 6b11e807 0b13e390 0b13e4a8 00000000 clr!AppDomain::RaiseUnhandledExceptionEventNoThrow+0x7a (FPO: [Non-Fpo])
0b13e3a0 6b19518a 0b13e4a8 00000000 0b13e4b0 clr!AppDomain::OnUnhandledException+0x81 (FPO: [Non-Fpo])
0b13e4bc 6b1969c1 0b13e750 0b13e594 00000000 clr!NotifyAppDomainsOfUnhandledException+0x141 (FPO: [Non-Fpo])
0b13e6ac 6b196f8f 0b13e750 00000000 00000000 clr!DefaultCatchHandler+0xdb (FPO: [Non-Fpo])
0b13e6d8 6b01c411 00000001 00000001 0b13e720 clr!DefaultCatchHandler+0x623 (FPO: [Non-Fpo])
0b13e6e8 6b01c45b 0b13e750 0b13f568 b16cca06 clr!ThreadBaseExceptionAppDomainFilter+0x13 (FPO: [Non-Fpo])
0b13e720 6b01c4df 0b13e750 71262b04 00000001 clr!ManagedThreadCallState::IsAppDomainEqual+0x9c (FPO: [Non-Fpo])
0b13e728 71262b04 00000001 0b13f344 6afd5d58 clr!Thread::ShouldChangeAbortToUnload+0x3af (FPO: [SEH])
0b13e73c 71284ae4 00000000 00000000 00000000 MSVCR100_CLR0400!_EH4_CallFilterFunc+0x12 (FPO: [Uses EBP] [0,0,4])
0b13e768 6aff14b8 6b509240 6af217d7 0b13e86c MSVCR100_CLR0400!_except_handler4_common+0x8e (FPO: [Non-Fpo])
0b13e788 77c41039 0b13e86c 0b13f334 0b13e894 clr!_except_handler4+0x20 (FPO: [Non-Fpo])
0b13e7ac 77c4100b 0b13e86c 0b13f334 0b13e894 ntdll!ExecuteHandler2+0x26
0b13e854 77c40e97 0b13c000 0b13e894 0b13e86c ntdll!ExecuteHandler+0x24
0b13e854 7654b09e 0b13c000 0b13e894 0b13e86c ntdll!KiUserExceptionDispatcher+0xf (FPO: [2,0,0]) (CONTEXT @ 0b13e894)
0b13ebb0 6afaac08 e0434352 00000001 00000005 kernel32!RaiseException+0x58 (FPO: [Non-Fpo])
0b13ec40 6afaae41 098e5728 00000000 00000000 clr!RaiseTheExceptionInternalOnly+0x276 (FPO: [Non-Fpo])
0b13ed00 056028bb 0b13ee60 6afaddc2 0b13f040 clr!IL_Throw+0x14c (FPO: [Non-Fpo])
WARNING: Frame IP not in any known module. Following frames may be wrong.
0b13edd0 6962ae5b 098d5948 0289922c 0b13edfc 0x56028bb
0b13ede0 695b7ff4 098aa838 00000000 098d5914 mscorlib_ni+0x2aae5b
0b13edfc 695b7f34 00000000 098b3eec 00000000 mscorlib_ni+0x237ff4
0b13ee1c 6962ade8 098d5914 00000000 05162dd0 mscorlib_ni+0x237f34
0b13ee34 6af221db 00000000 00000000 0b13eec0 mscorlib_ni+0x2aade8
0b13ee44 6af44a2a 0b13ef10 00000000 0b13eee0 clr!CallDescrWorker+0x33
0b13eec0 6af44bcc 0b13ef10 00000000 0b13eee0 clr!CallDescrWorkerWithHandler+0x8e (FPO: [Non-Fpo])
0b13eff8 6af44c01 69557c90 0b13f160 0b13f07c clr!MethodDesc::CallDescr+0x194 (FPO: [Non-Fpo])
0b13f014 6b0bb512 69557c90 0b13f160 0b13f07c clr!MethodDesc::CallTargetWorker+0x21 (FPO: [Non-Fpo])
0b13f220 6afd5c05 0b13f5f4 0b13f304 05162dd0 clr!ThreadNative::KickOffThread_Worker+0x1e1 (FPO: [Non-Fpo])
0b13f234 6afd5c87 0b13f568 b16cdfc2 0b13f568 clr!Thread::DoExtraWorkForFinalizer+0x114 (FPO: [Non-Fpo])
0b13f2e4 6afd5d42 0b13f568 b16cde62 05162dd0 clr!Thread::ShouldChangeAbortToUnload+0x101 (FPO: [Non-Fpo])
0b13f344 6afc37a2 05162dd0 0b13f430 6b0a6465 clr!Thread::ShouldChangeAbortToUnload+0x399 (FPO: [Non-Fpo])
0b13f350 6b0a6465 0b13f568 b16cd916 05162dd0 clr!Thread::RaiseCrossContextException+0x3f8 (FPO: [Non-Fpo])
0b13f430 6afc37cf 00000002 6afc378b 0b13f568 clr!Thread::DoADCallBack+0xf0 (FPO: [Non-Fpo])
0b13f450 6afd5c87 0b13f568 b16cd826 0b13f568 clr!Thread::DoExtraWorkForFinalizer+0xfa (FPO: [Non-Fpo])
0b13f500 6afd5d42 0b13f568 b16cd846 00000000 clr!Thread::ShouldChangeAbortToUnload+0x101 (FPO: [Non-Fpo])
0b13f560 6afd5dd9 00000002 00000000 00000001 clr!Thread::ShouldChangeAbortToUnload+0x399 (FPO: [Non-Fpo])
0b13f584 6b0bb3e5 00000002 6b0bb3e9 0b13f5f4 clr!Thread::ShouldChangeAbortToUnload+0x43a (FPO: [Non-Fpo])
0b13f59c 6b0bb2e0 00000002 6b0bb3e9 0b13f5f4 clr!ManagedThreadBase::KickOff+0x15 (FPO: [Non-Fpo])
0b13f634 6afd5a08 05168138 0b13f64c 00000000 clr!ThreadNative::KickOffThread+0x23e (FPO: [Non-Fpo])
0b13fed4 76573833 0514eb28 0b13ff20 77c1a9bd clr!Thread::intermediateThreadProc+0x4b (FPO: [Non-Fpo])
0b13fee0 77c1a9bd 0514eb28 0b13250b 00000000 kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
0b13ff20 00000000 6afd59c0 0514eb28 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

12. We now set the exception context and get the stack trace again:

```
0:015> .cxr 0b13e894
eax=0b13eb60 ebx=00000005 ecx=00000005 edx=00000000 esi=0b13ec0c edi=05162dd0
eip=7654b09e esp=0b13eb60 ebp=0b13ebb0 iopl=0         nv up ei pl nz ac pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000216
kernel32!RaiseException+0x58:
7654b09e c9              leave

0:015> k
  *** Stack trace for last set context - .thread/.cxr resets it
ChildEBP RetAddr
0b13ebb0 6afaac08 kernel32!RaiseException+0x58
0b13ec40 6afaae41 clr!RaiseTheExceptionInternalOnly+0x276
0b13ed00 056028bb clr!IL_Throw+0x14c
WARNING: Frame IP not in any known module. Following frames may be wrong.
0b13edd0 6962ae5b 0x56028bb
0b13ede0 695b7ff4 mscorlib_ni+0x2aae5b
0b13edfc 695b7f34 mscorlib_ni+0x237ff4
0b13ee1c 6962ade8 mscorlib_ni+0x237f34
0b13ee34 6af221db mscorlib_ni+0x2aade8
0b13ee44 6af44a2a clr!CallDescrWorker+0x33
0b13eec0 6af44bcc clr!CallDescrWorkerWithHandler+0x8e
0b13eff8 6af44c01 clr!MethodDesc::CallDescr+0x194
0b13f014 6b0bb512 clr!MethodDesc::CallTargetWorker+0x21
0b13f220 6afd5c05 clr!ThreadNative::KickOffThread_Worker+0x1e1
0b13f234 6afd5c87 clr!Thread::DoExtraWorkForFinalizer+0x114
0b13f2e4 6afd5d42 clr!Thread::ShouldChangeAbortToUnload+0x101
0b13f344 6afc37a2 clr!Thread::ShouldChangeAbortToUnload+0x399
0b13f350 6b0a6465 clr!Thread::RaiseCrossContextException+0x3f8
0b13f430 6afc37cf clr!Thread::DoADCallBack+0xf0
0b13f450 6afd5c87 clr!Thread::DoExtraWorkForFinalizer+0xfa
0b13f500 6afd5d42 clr!Thread::ShouldChangeAbortToUnload+0x101
0b13f560 6afd5dd9 clr!Thread::ShouldChangeAbortToUnload+0x399
0b13f584 6b0bb3e5 clr!Thread::ShouldChangeAbortToUnload+0x43a
0b13f59c 6b0bb2e0 clr!ManagedThreadBase::KickOff+0x15
0b13f634 6afd5a08 clr!ThreadNative::KickOffThread+0x23e
0b13fed4 76573833 clr!Thread::intermediateThreadProc+0x4b
0b13fee0 77c1a9bd kernel32!BaseThreadInitThunk+0xe
0b13ff20 00000000 ntdll!_RtlUserThreadStart+0x23
```

Note: We then check the managed code that threw the exception:

```
0:015> !IP2MD 056028bb
MethodDesc:   05622104
Method Name:  UserQuery+ClassMain.thread_proc_3()
Class:        056143e0
MethodTable:  05622124
mdToken:      0600000a
Module:       05621050
IsJitted:     yes
CodeAddr:     05602860
Transparency: Critical
```

```
0:015> !U 056028bb
Normal JIT generated code
UserQuery+ClassMain.thread_proc_3()
Begin 05602860, size 5c
05602860 55              push    ebp
05602861 8bec            mov     ebp,esp
05602863 57              push    edi
05602864 56              push    esi
05602865 53              push    ebx
05602866 83ec1c          sub     esp,1Ch
05602869 33c0            xor     eax,eax
0560286b 8945e8          mov     dword ptr [ebp-18h],eax
0560286e b9ec486969      mov     ecx,offset mscorlib_ni+0x3148ec (696948ec) (MT:
System.IO.FileNotFoundException)
05602873 e8a8f7bcfa      call    001d2020 (JitHelp: CORINFO_HELP_NEWSFAST)
05602878 8945dc          mov     dword ptr [ebp-24h],eax
0560287b 8bc8            mov     ecx,eax
0560287d e8ce1c6b64      call    mscorlib_ni+0x934550 (69cb4550)
(System.IO.FileNotFoundException..ctor(), mdToken: 06003f17)
05602882 8b4ddc          mov     ecx,dword ptr [ebp-24h]
05602885 e8d4849a65      call    clr!IL_Throw (6afaad5e)
0560288a b954226205      mov     ecx,5622254h (MT: UserQuery+CustomException)
0560288f e88cf7bcfa      call    001d2020 (JitHelp: CORINFO_HELP_NEWSFAST)
05602894 8945d8          mov     dword ptr [ebp-28h],eax
05602897 ba50106205      mov     edx,5621050h
0560289c b901000070      mov     ecx,70000001h
056028a1 e873bb9a65      call    clr!JIT_StrCns (6afae419)
056028a6 6a05            push    5
056028a8 8bd0            mov     edx,eax
056028aa 8b4dd8          mov     ecx,dword ptr [ebp-28h]
056028ad ff153c226205    call    dword ptr ds:[562223Ch]
(UserQuery+CustomException..ctor(System.String, Int32), mdToken: 06000004)
056028b3 8b4dd8          mov     ecx,dword ptr [ebp-28h]
056028b6 e8a3849a65      call    clr!IL_Throw (6afaad5e)
>>> 056028bb cc              int     3
```

Note: We notice CustomException constructor was been called before throw and check execution residue on the stack (references to UserQuery+CustomException object):

```
0:015> !DumpStackObjects
OS Thread Id: 0x62558 (15)
ESP/REG  Object   Name
0B13DAC4 0991006c System.Windows.Forms.NativeMethods+MSG[]
0B13DAC8 098c4d04 System.Windows.Forms.Application+ThreadContext
0B13DAD0 098cd5ac System.Windows.Forms.Application+ComponentManager
0B13DB48 098c4d04 System.Windows.Forms.Application+ThreadContext
0B13DB88 098cd560 System.Windows.Forms.Application+ModalApplicationContext
0B13DC04 098c302c LINQPad.UI.ThreadExceptionForm
0B13DC8C 098c1458 System.UnhandledExceptionEventArgs
0B13DCA0 018912c8 System.AppDomain
0B13DD50 018912c8 System.AppDomain
0B13DD54 018c10c4 System.UnhandledExceptionEventHandler
0B13DF78 018c10c4 System.UnhandledExceptionEventHandler
0B13DF80 018912c8 System.AppDomain
0B13E088 098c1458 System.UnhandledExceptionEventArgs
0B13E0FC 018c10c4 System.UnhandledExceptionEventHandler
0B13E180 098be808 System.Runtime.Serialization.SerializationException
0B13E184 018912c8 System.AppDomain
0B13E1F8 098b92e8 UserQuery+CustomException
0B13E390 09890200 System.AppDomain
0B13E4A8 098b92e8 UserQuery+CustomException
0B13E594 098b92e8 UserQuery+CustomException
0B13EE08 098b3eec System.Threading.ThreadHelper
0B13F094 098b3f00 System.Threading.ThreadStart
```

13. We now look at that object fields:

```
0:015> !DumpObj 098b92e8
Name:        UserQuery+CustomException
MethodTable: 05622254
EEClass:     05614604
Size:        92(0x5c) bytes
File:        C:\Users\Training\AppData\Local\Temp\LINQPad\zbqvhjml\query_uobgah.dll
Fields:
      MT    Field   Offset                 Type VT     Attr    Value Name
6969f9ac  400004a        4        System.String  0 instance 00000000 _className
696a01f4  400004b        8 ...ection.MethodBase  0 instance 00000000 _exceptionMethod
6969f9ac  400004c        c        System.String  0 instance 00000000 _exceptionMethodString
6969f9ac  400004d       10        System.String  0 instance 00000000 _message
69694004  400004e       14 ...tions.IDictionary  0 instance 00000000 _data
6969fc0c  400004f       18     System.Exception  0 instance 00000000 _innerException
6969f9ac  4000050       1c        System.String  0 instance 00000000 _helpURL
6969f5e8  4000051       20        System.Object  0 instance 098b938c _stackTrace
6969f5e8  4000052       24        System.Object  0 instance 00000000 _watsonBuckets
6969f9ac  4000053       28        System.String  0 instance 00000000 _stackTraceString
6969f9ac  4000054       2c        System.String  0 instance 00000000 _remoteStackTraceString
696a2978  4000055       3c         System.Int32  1 instance        0 _remoteStackIndex
6969f5e8  4000056       30        System.Object  0 instance 00000000 _dynamicMethods
696a2978  4000057       40         System.Int32  1 instance -2146233088 _HResult
6969f9ac  4000058       34        System.String  0 instance 00000000 _source
6969aa2c  4000059       44        System.IntPtr  1 instance        0 _xptrs
696a2978  400005a       48         System.Int32  1 instance -532462766 _xcode
6965a29c  400005b       4c       System.UIntPtr  1 instance  56028ba _ipForWatsonBuckets
69659888  400005c       38 ...ializationManager  0 instance 098b9370 _safeSerializationManager
6969f9ac  4000001       50        System.String  0 instance 098b9344 description
696a2978  4000002       54         System.Int32  1 instance        5 code
```

Note: We see it has a value type field code with the value 5 and a String desription field with the value "File Not Found":

```
0:015> !DumpObj 098b9344
Name:        System.String
MethodTable: 6969f9ac
EEClass:     693d8bb0
Size:        42(0x2a) bytes
File:
C:\Windows\Microsoft.Net\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll
String:      File Not Found
Fields:
      MT    Field   Offset                 Type VT     Attr    Value Name
696a2978  40000ed        4         System.Int32  1 instance       14 m_stringLength
696a1dc8  40000ee        8          System.Char  1 instance       46 m_firstChar
6969f9ac  40000ef        8        System.String  0   shared   static Empty
    >> Domain:Value  002017d0:01891228 05179888:01891228 <<
```

Note: All this makes sense when we look at C# code for thread_proc_3 where we see the inner exception rethrown:

```
void thread_proc_3()
{
      try
      {
            throw new FileNotFoundException();
      }
      catch (Exception e)
      {
            throw new CustomException ("File Not Found", 5);
      }
}
```

14. We remember we have seen another exception processing code on the thread 14 stack trace:

```
0:015> ~14s
eax=03a80968 ebx=098c6b00 ecx=0a62d694 edx=0000001a esi=098cc7cc edi=0b960acc
eip=77c40f34 esp=0a62dd50 ebp=0a62dde4 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
ntdll!KiFastSystemCallRet:
77c40f34 c3              ret
```

```
0:014> k
ChildEBP RetAddr
0a62dd4c 7674b5b4 ntdll!KiFastSystemCallRet
0a62dd50 67b3737a user32!NtUserWaitMessage+0xc
0a62dde4 67b36e2c System_Windows_Forms_ni+0x22737a
0a62de40 67b36c81 System_Windows_Forms_ni+0x226e2c
0a62de70 6802fefb System_Windows_Forms_ni+0x226c81
0a62de88 68059f83 System_Windows_Forms_ni+0x71fefb
0a62df24 6805a1b7 System_Windows_Forms_ni+0x749f83
0a62df64 6af221db System_Windows_Forms_ni+0x74a1b7
0a62df74 6af44a2a clr!CallDescrWorker+0x33
0a62dff0 6af44bcc clr!CallDescrWorkerWithHandler+0x8e
0a62e140 6af44c01 clr!MethodDesc::CallDescr+0x194
0a62e15c 6b192379 clr!MethodDesc::CallTargetWorker+0x21
0a62e254 6b134ad1 clr!ExceptionNotifications::DeliverExceptionNotification+0x98
0a62e2c8 6b134e86 clr!COMDelegate::BindToMethodInfo+0x504
0a62e36c 6b11c19b clr!DistributeUnhandledExceptionReliably+0xeb
0a62e3c4 6b11bfd3 clr!AppDomain::RaiseUnhandledExceptionEvent+0xba
0a62e45c 6b0a8688 clr!AppDomain::RaiseUnhandledExceptionEvent_Wrapper+0x1cd
0a62e534 6b11c13e clr!Thread::DoADCallBack+0xe0
0a62e590 6b11de38 clr!AppDomain::RaiseUnhandledExceptionEvent+0xc2
0a62e604 6b11e807 clr!AppDomain::RaiseUnhandledExceptionEventNoThrow+0x7a
0a62e660 6b19518a clr!AppDomain::OnUnhandledException+0x81
0a62e774 6b1969c1 clr!NotifyAppDomainsOfUnhandledException+0x141
0a62e964 6b196f8f clr!DefaultCatchHandler+0xdb
0a62e990 6b01c411 clr!DefaultCatchHandler+0x623
0a62e9a0 6b01c45b clr!ThreadBaseExceptionAppDomainFilter+0x13
0a62e9d8 6b01c4df clr!ManagedThreadCallState::IsAppDomainEqual+0x9c
0a62e9e0 71262b04 clr!Thread::ShouldChangeAbortToUnload+0x3af
0a62e9f4 71284ae4 MSVCR100_CLR0400!_EH4_CallFilterFunc+0x12
0a62ea20 6aff14b8 MSVCR100_CLR0400!_except_handler4_common+0x8e
0a62ea40 77c41039 clr!_except_handler4+0x20
0a62ea64 77c4100b ntdll!ExecuteHandler2+0x26
0a62eb0c 77c40e97 ntdll!ExecuteHandler+0x24
0a62eb0c 7654b09e ntdll!KiUserExceptionDispatcher+0xf
0a62ee68 6afaac08 kernel32!RaiseException+0x58
0a62eef8 6afaae41 clr!RaiseTheExceptionInternalOnly+0x276
0a62efb8 05602765 clr!IL_Throw+0x14c
WARNING: Frame IP not in any known module. Following frames may be wrong.
0a62efd0 695b7ff4 0x5602765
0a62efec 695b7f34 mscorlib_ni+0x237ff4
0a62f00c 6962ade8 mscorlib_ni+0x237f34
0a62f024 6af221db mscorlib_ni+0x2aade8
0a62f034 6af44a2a clr!CallDescrWorker+0x33
0a62f0b0 6af44bcc clr!CallDescrWorkerWithHandler+0x8e
0a62f1e8 6af44c01 clr!MethodDesc::CallDescr+0x194
0a62f204 6b0bb512 clr!MethodDesc::CallTargetWorker+0x21
0a62f410 6afd5c05 clr!ThreadNative::KickOffThread_Worker+0x1e1
0a62f424 6afd5c87 clr!Thread::DoExtraWorkForFinalizer+0x114
0a62f4d4 6afd5d42 clr!Thread::ShouldChangeAbortToUnload+0x101
0a62f534 6afc37a2 clr!Thread::ShouldChangeAbortToUnload+0x399
0a62f540 6b0a6465 clr!Thread::RaiseCrossContextException+0x3f8
0a62f620 6afc37cf clr!Thread::DoADCallBack+0xf0
0a62f640 6afd5c87 clr!Thread::DoExtraWorkForFinalizer+0xfa
0a62f6f0 6afd5d42 clr!Thread::ShouldChangeAbortToUnload+0x101
0a62f750 6afd5dd9 clr!Thread::ShouldChangeAbortToUnload+0x399
0a62f774 6b0bb3e5 clr!Thread::ShouldChangeAbortToUnload+0x43a
0a62f78c 6b0bb2e0 clr!ManagedThreadBase::KickOff+0x15
0a62f824 6afd5a08 clr!ThreadNative::KickOffThread+0x23e
0a62fec4 76573833 clr!Thread::intermediateThreadProc+0x4b
```

```
0a62fed0 77c1a9bd kernel32!BaseThreadInitThunk+0xe
0a62ff10 00000000 ntdll!_RtlUserThreadStart+0x23

0:014> !IP2MD 0x5602765
MethodDesc:   056220ec
Method Name:  UserQuery+ClassMain.thread_proc_1()
Class:        056143e0
MethodTable:  05622124
mdToken:      06000008
Module:       05621050
IsJitted:     yes
CodeAddr:     05602748
Transparency: Critical

0:014> !U 0x5602765
Normal JIT generated code
UserQuery+ClassMain.thread_proc_1()
Begin 05602748, size 1e
05602748 50              push    eax
05602749 b9ec486969      mov     ecx,offset mscorlib_ni+0x3148ec (696948ec) (MT:
System.IO.FileNotFoundException)
0560274e e8cdf8bcfa      call    001d2020 (JitHelp: CORINFO_HELP_NEWSFAST)
05602753 890424          mov     dword ptr [esp],eax
05602756 8bc8            mov     ecx,eax
05602758 e89baaf763      call    mscorlib_ni+0x1fd1f8 (6957d1f8)
(System.IO.FileNotFoundException..ctor(), mdToken: 06003f17)
0560275d 8b0c24          mov     ecx,dword ptr [esp]
05602760 e8f9859a65      call    clr!IL_Throw (6afaad5e)
>>> 05602765 cc              int     3
```

Note: We see that another thread threw **FileNotFoundException**. **!pe** command couldn't help us here (in some sense the exception was "hidden"):

```
0:014> !pe
There is no current managed exception on this thread

0:014> !pe -nested
There is no current managed exception on this thread
```

15. We also recall that the finalizer thread had exception processing code on its unmanaged thread stack trace:

```
0:014> ~2s
eax=00000000 ebx=09bd2c6c ecx=0000013e edx=1c530000 esi=09bd417c edi=1c8444fc
eip=77c40f34 esp=039be330 ebp=039be3c4 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
ntdll!KiFastSystemCallRet:
77c40f34 c3              ret
```

```
0:002> k
ChildEBP RetAddr
039be32c 7674b5b4 ntdll!KiFastSystemCallRet
039be330 67b3737a user32!NtUserWaitMessage+0xc
039be3c4 67b36e2c System_Windows_Forms_ni+0x22737a
039be420 67b36c81 System_Windows_Forms_ni+0x226e2c
039be450 6802fefb System_Windows_Forms_ni+0x226c81
039be468 68059f83 System_Windows_Forms_ni+0x71fefb
039be504 6805a1b7 System_Windows_Forms_ni+0x749f83
039be544 6af221db System_Windows_Forms_ni+0x74a1b7
039be554 6af44a2a clr!CallDescrWorker+0x33
039be5d0 6af44bcc clr!CallDescrWorkerWithHandler+0x8e
039be720 6af44c01 clr!MethodDesc::CallDescr+0x194
039be73c 6b192379 clr!MethodDesc::CallTargetWorker+0x21
039be834 6b134ad1 clr!ExceptionNotifications::DeliverExceptionNotification+0x98
039be8a8 6b134e86 clr!COMDelegate::BindToMethodInfo+0x504
039be94c 6b11c19b clr!DistributeUnhandledExceptionReliably+0xeb
039be9a4 6b11bfd3 clr!AppDomain::RaiseUnhandledExceptionEvent+0xba
039bea3c 6b0a8688 clr!AppDomain::RaiseUnhandledExceptionEvent_Wrapper+0x1cd
039beb14 6b11c13e clr!Thread::DoADCallBack+0xe0
039beb70 6b11de38 clr!AppDomain::RaiseUnhandledExceptionEvent+0xc2
039bebe4 6b11e807 clr!AppDomain::RaiseUnhandledExceptionEventNoThrow+0x7a
039bec40 6b19518a clr!AppDomain::OnUnhandledException+0x81
039bed58 6b1969c1 clr!NotifyAppDomainsOfUnhandledException+0x141
039bef48 6b196f8f clr!DefaultCatchHandler+0xdb
039bef74 6b01c411 clr!DefaultCatchHandler+0x623
039bef84 6b01c45b clr!ThreadBaseExceptionAppDomainFilter+0x13
039befbc 6b01c4df clr!ManagedThreadCallState::IsAppDomainEqual+0x9c
039befc4 71262b04 clr!Thread::ShouldChangeAbortToUnload+0x3af
039befd8 71284ae4 MSVCR100_CLR0400!_EH4_CallFilterFunc+0x12
039bf004 6aff14b8 MSVCR100_CLR0400!_except_handler4_common+0x8e
039bf024 77c41039 clr!_except_handler4+0x20
039bf048 77c4100b ntdll!ExecuteHandler2+0x26
039bf0f0 77c40e97 ntdll!ExecuteHandler+0x24
039bf0f0 05602dfc ntdll!KiUserExceptionDispatcher+0xf
WARNING: Frame IP not in any known module. Following frames may be wrong.
039bf410 6afd4b01 0x5602dfc
039bf46c 6afd49c7 clr!MethodTable::SetObjCreateDelegate+0xbd
039bf498 6afd4a56 clr!MethodTable::CallFinalizer+0xca
039bf4b0 6afd4c9f clr!WKS::CallFinalizer+0xa7
039bf500 6afd4bdb clr!WKS::GCHeap::TraceGCSegments+0x239
039bf530 6b0d88ac clr!WKS::GCHeap::TraceGCSegments+0x415
039bf544 6afd5c05 clr!WKS::ProfScanRootsHelper+0x6b
039bf558 6afd5c87 clr!Thread::DoExtraWorkForFinalizer+0x114
039bf608 6afd5d42 clr!Thread::ShouldChangeAbortToUnload+0x101
039bf668 6afc37a2 clr!Thread::ShouldChangeAbortToUnload+0x399
039bf674 6b0a8688 clr!Thread::RaiseCrossContextException+0x3f8
039bf74c 6b0acca8 clr!Thread::DoADCallBack+0xe0
039bf770 6b0acbda clr!Thread::DoExtraWorkForFinalizer+0x10c
039bf77c 6b0d8921 clr!ManagedThreadBase::FinalizerAppDomain+0x27
039bf7d8 6afd4bdb clr!WKS::GCHeap::TraceGCSegments+0x2e3
039bf808 6b098405 clr!WKS::GCHeap::TraceGCSegments+0x415
039bf824 6afd5c05 clr!WKS::GCHeap::FinalizerThreadWorker+0xcd
039bf838 6afd5c87 clr!Thread::DoExtraWorkForFinalizer+0x114
039bf8e8 6afd5d42 clr!Thread::ShouldChangeAbortToUnload+0x101
039bf948 6afc78be clr!Thread::ShouldChangeAbortToUnload+0x399
039bf96c 6afc78d1 clr!ManagedThreadBase_NoADTransition+0x35
039bf97c 6b00d313 clr!ManagedThreadBase::FinalizerBase+0xf
039bf9b4 6afd5a08 clr!WKS::GCHeap::FinalizerThreadStart+0x10c
039bfa4c 76573833 clr!Thread::intermediateThreadProc+0x4b
```

```
039bfa58 77c1a9bd kernel32!BaseThreadInitThunk+0xe
039bfa98 00000000 ntdll!_RtlUserThreadStart+0x23
```

Note: when we disassemble the code we see it's SmallObject finalize method which generated a possible NULL pointer access violation exception:

```
0:002> !IP2MD 0x5602dfc
MethodDesc:   056221a8
Method Name:  UserQuery+SmallObject.Finalize()
Class:        0561450c
MethodTable:  056221bc
mdToken:      06000007
Module:       05621050
IsJitted:     yes
CodeAddr:     05602de0
Transparency: Safe critical

0:002> !U 0x5602dfc
Normal JIT generated code
UserQuery+SmallObject.Finalize()
Begin 05602de0, size 4f
05602de0 55              push    ebp
05602de1 8bec            mov     ebp,esp
05602de3 57              push    edi
05602de4 56              push    esi
05602de5 53              push    ebx
05602de6 83ec14          sub     esp,14h
05602de9 33c0            xor     eax,eax
05602deb 8945e0          mov     dword ptr [ebp-20h],eax
05602dee 8945e4          mov     dword ptr [ebp-1Ch],eax
05602df1 8945e8          mov     dword ptr [ebp-18h],eax
05602df4 8945ec          mov     dword ptr [ebp-14h],eax
05602df7 33c0            xor     eax,eax
05602df9 8945e8          mov     dword ptr [ebp-18h],eax
>>> 05602dfc c7050000000001000000 mov dword ptr ds:[0],1
05602e06 c745e400000000  mov     dword ptr [ebp-1Ch],0
05602e0d c745e8fc000000  mov     dword ptr [ebp-18h],0FCh
05602e14 68262e6005      push    5602E26h
05602e19 eb00            jmp     05602e1b
05602e1b 58              pop     eax
05602e1c ffe0            jmp     eax
05602e1e 8d65f4          lea     esp,[ebp-0Ch]
05602e21 5b              pop     ebx
05602e22 5e              pop     esi
05602e23 5f              pop     edi
05602e24 5d              pop     ebp
05602e25 c3              ret
05602e26 c745e800000000  mov     dword ptr [ebp-18h],0
05602e2d ebef            jmp     05602e1e
```

Note: We can double check that by setting exception context:

```
0:002> kv
ChildEBP RetAddr  Args to Child
039be32c 7674b5b4 67b3737a bb1f3dee 6af25d80 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
039be330 67b3737a bb1f3dee 6af25d80 039be474 user32!NtUserWaitMessage+0xc (FPO: [0,0,0])
039be3c4 67b36e2c 00000000 00000004 00000000 System_Windows_Forms_ni+0x22737a
039be420 67b36c81 09bd40fc 10d80002 00000000 System_Windows_Forms_ni+0x226e2c
039be450 6802fefb 0b7ded4c 00000000 00772010 System_Windows_Forms_ni+0x226c81
039be468 68059f83 bb1f3dee 6af25d80 039be8d0 System_Windows_Forms_ni+0x71fefb
039be504 6805a1b7 0543a204 0b7d15b8 0b7d15b8 System_Windows_Forms_ni+0x749f83
039be544 6af221db 0b7d5d80 09895194 039be5d0 System_Windows_Forms_ni+0x74a1b7
039be554 6af44a2a 039be624 00000001 039be5f0 clr!CallDescrWorker+0x33
039be5d0 6af44bcc 039be624 00000001 039be5f0 clr!CallDescrWorkerWithHandler+0x8e (FPO: [Non-Fpo])
039be720 6af44c01 6957ced8 039be768 039be818 clr!MethodDesc::CallDescr+0x194 (FPO: [Non-Fpo])
039be73c 6b192379 6957ced8 039be768 039be818 clr!MethodDesc::CallTargetWorker+0x21 (FPO: [Non-Fpo])
039be834 6b134ad1 00000001 039be99c 039bea24 clr!ExceptionNotifications::DeliverExceptionNotification+0x98 (FPO: [Non-
Fpo])
039be8a8 6b134e86 039be99c 039bea24 039be928 clr!COMDelegate::BindToMethodInfo+0x504 (FPO: [Non-Fpo])
039be94c 6b11c19b 039be99c 039bea24 039bea20 clr!DistributeUnhandledExceptionReliably+0xeb (FPO: [Non-Fpo])
039be9a4 6b11bfd3 039bea24 039bea20 00000000 clr!AppDomain::RaiseUnhandledExceptionEvent+0xba (FPO: [Non-Fpo])
039bea3c 6b0a8688 039beb50 b9e4c632 00000000 clr!AppDomain::RaiseUnhandledExceptionEvent_Wrapper+0x1cd (FPO: [Non-
Fpo])
039beb14 6b11c13e 002017d0 6b11befb 039beb50 clr!Thread::DoADCallBack+0xe0 (FPO: [Non-Fpo])
039beb70 6b11de38 039bec30 039bed44 00000000 clr!AppDomain::RaiseUnhandledExceptionEvent+0xc2 (FPO: [Non-Fpo])
039bebe4 6b11e807 039bec30 039bed44 00000000 clr!AppDomain::RaiseUnhandledExceptionEventNoThrow+0x7a (FPO: [Non-Fpo])
039bec40 6b19518a 039bed44 00000000 039bed4c clr!AppDomain::OnUnhandledException+0x81 (FPO: [Non-Fpo])
039bed58 6b1969c1 039befec 039bee30 00000000 clr!NotifyAppDomainsOfUnhandledException+0x141 (FPO: [Non-Fpo])
039bef48 6b196f8f 039befec 00000000 00000000 clr!DefaultCatchHandler+0xdb (FPO: [Non-Fpo])
039bef74 6b01c411 00000001 00000001 039befbc clr!DefaultCatchHandler+0x623 (FPO: [Non-Fpo])
039bef84 6b01c45b 039befec 039bf950 b9e4c29a clr!ThreadBaseExceptionAppDomainFilter+0x13 (FPO: [Non-Fpo])
039befbc 6b01c4df 039befec 71262b04 00000001 clr!ManagedThreadCallState::IsAppDomainEqual+0x9c (FPO: [Non-Fpo])
039befc4 71262b04 00000001 039bf668 6afd5d58 clr!Thread::ShouldChangeAbortToUnload+0x3af (FPO: [SEH])
039befd8 71284ae4 00000000 00000000 00000000 MSVCR100_CLR0400!_EH4_CallFilterFunc+0x12 (FPO: [Uses EBP] [0,0,4])
039bf004 6aff14b8 6b509240 6af217d7 039bf108 MSVCR100_CLR0400!_except_handler4_common+0x8e (FPO: [Non-Fpo])
039bf024 77c41039 039bf108 039bf658 039bf124 clr!_except_handler4+0x20 (FPO: [Non-Fpo])
039bf048 77c4100b 039bf108 039bf658 039bf124 ntdll!ExecuteHandler2+0x26
039bf0f0 77c40e97 039bd000 039bf124 039bf108 ntdll!ExecuteHandler+0x24
039bf0f0 05602dfc 039bd000 039bf124 039bf108 ntdll!KiUserExceptionDispatcher+0xf (FPO: [2,0,0]) (CONTEXT @ 039bf124)
WARNING: Frame IP not in any known module. Following frames may be wrong.
039bf410 6afd4b01 039bf45c 6afacc44 039bf628 0x5602dfc
039bf46c 6afd49c7 0b56f038 0547d2f5 00000000 clr!MethodTable::SetObjCreateDelegate+0xbd (FPO: [Non-Fpo])
039bf498 6afd4a56 0b56f038 0b56f038 00000000 clr!MethodTable::CallFinalizer+0xca (FPO: [Non-Fpo])
039bf4b0 6afd4c9f 0b56f038 b9e4d826 039bf520 clr!WKS::CallFinalizer+0xa7 (FPO: [Non-Fpo])
039bf500 6afd4bdb 00216b18 00000409 039bf52f clr!WKS::GCHeap::TraceGCSegments+0x239 (FPO: [Non-Fpo])
039bf530 6b0d88ac 00216b18 00000000 039bf950 clr!WKS::GCHeap::TraceGCSegments+0x415 (FPO: [Non-Fpo])
039bf544 6afd5c05 039bf7bc 039bf628 00216b18 clr!WKS::ProfScanRootsHelper+0x6b (FPO: [Non-Fpo])
039bf558 6afd5c87 039bf950 b9e4db2e 039bf950 clr!Thread::DoExtraWorkForFinalizer+0x114 (FPO: [Non-Fpo])
039bf608 6afd5d42 039bf950 b9e4db4e 00216b18 clr!Thread::ShouldChangeAbortToUnload+0x101 (FPO: [Non-Fpo])
039bf668 6afc37a2 00000000 039bf74c 6b0a8688 clr!Thread::ShouldChangeAbortToUnload+0x399 (FPO: [Non-Fpo])
039bf674 6b0a8688 039bf950 b9e4da6a 00216b18 clr!Thread::RaiseCrossContextException+0x3f8 (FPO: [Non-Fpo])
039bf74c 6b0acca8 05179888 6afc378b 039bf950 clr!Thread::DoADCallBack+0xe0 (FPO: [Non-Fpo])
039bf770 6b0acbda 039bf950 039bf7d8 6b0d8921 clr!Thread::DoExtraWorkForFinalizer+0x10c (FPO: [Non-Fpo])
039bf77c 6b0d8921 05179888 6b0d8891 039bf7bc clr!ManagedThreadBase::FinalizerAppDomain+0x27 (FPO: [Non-Fpo])
039bf7d8 6afd4bdb 00216b18 00000000 039bf807 clr!WKS::GCHeap::TraceGCSegments+0x2e3 (FPO: [Non-Fpo])
039bf808 6b098405 00216b18 00000000 00216b18 clr!WKS::GCHeap::TraceGCSegments+0x415 (FPO: [Non-Fpo])
039bf824 6afd5c05 00000001 039bf908 00216b18 clr!WKS::GCHeap::FinalizerThreadWorker+0xcd (FPO: [Non-Fpo])
039bf838 6afd5c87 039bf950 b9e4d5ce 039bf950 clr!Thread::DoExtraWorkForFinalizer+0x114 (FPO: [Non-Fpo])
039bf8e8 6afd5d42 039bf950 b9e4d46e 00000000 clr!Thread::ShouldChangeAbortToUnload+0x101 (FPO: [Non-Fpo])
039bf948 6afc78be 00000000 05179888 00000000 clr!Thread::ShouldChangeAbortToUnload+0x399 (FPO: [Non-Fpo])
039bf96c 6afc78d1 6b098354 00000008 039bf9b4 clr!ManagedThreadBase_NoADTransition+0x35 (FPO: [Non-Fpo])
039bf97c 6b00d313 6b098354 b9e4d492 00000000 clr!ManagedThreadBase::FinalizerBase+0xf (FPO: [Non-Fpo])
039bf9b4 6afd5a08 00000000 00000000 00000000 clr!WKS::GCHeap::FinalizerThreadStart+0x10c (FPO: [Non-Fpo])
039bfa4c 76573833 001ff2d8 039bfa98 77c1a9bd clr!Thread::intermediateThreadProc+0x4b (FPO: [Non-Fpo])
039bfa58 77c1a9bd 001ff2d8 039b20b3 00000000 kernel32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
039bfa98 00000000 6afd59c0 001ff2d8 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

```
0:002> .cxr 039bf124
eax=00000000 ebx=00000000 ecx=0b56f038 edx=039bf418 esi=00216b18 edi=039bf418
eip=05602dfc esp=039bf3f0 ebp=039bf410 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010246
05602dfc c7050000000001000000 mov dword ptr ds:[0],1  ds:0023:00000000=????????

0:002> k
  *** Stack trace for last set context - .thread/.cxr resets it
ChildEBP RetAddr
WARNING: Frame IP not in any known module. Following frames may be wrong.
039bf410 6afd4b01 0x5602dfc
039bf46c 6afd49c7 clr!MethodTable::SetObjCreateDelegate+0xbd
039bf498 6afd4a56 clr!MethodTable::CallFinalizer+0xca
039bf4b0 6afd4c9f clr!WKS::CallFinalizer+0xa7
039bf500 6afd4bdb clr!WKS::GCHeap::TraceGCSegments+0x239
039bf530 6b0d88ac clr!WKS::GCHeap::TraceGCSegments+0x415
039bf544 6afd5c05 clr!WKS::ProfScanRootsHelper+0x6b
039bf558 6afd5c87 clr!Thread::DoExtraWorkForFinalizer+0x114
039bf608 6afd5d42 clr!Thread::ShouldChangeAbortToUnload+0x101
039bf668 6afc37a2 clr!Thread::ShouldChangeAbortToUnload+0x399
039bf674 6b0a8688 clr!Thread::RaiseCrossContextException+0x3f8
039bf74c 6b0acca8 clr!Thread::DoADCallBack+0xe0
039bf770 6b0acbda clr!Thread::DoExtraWorkForFinalizer+0x10c
039bf77c 6b0d8921 clr!ManagedThreadBase::FinalizerAppDomain+0x27
039bf7d8 6afd4bdb clr!WKS::GCHeap::TraceGCSegments+0x2e3
039bf808 6b098405 clr!WKS::GCHeap::TraceGCSegments+0x415
039bf824 6afd5c05 clr!WKS::GCHeap::FinalizerThreadWorker+0xcd
039bf838 6afd5c87 clr!Thread::DoExtraWorkForFinalizer+0x114
039bf8e8 6afd5d42 clr!Thread::ShouldChangeAbortToUnload+0x101
039bf948 6afc78be clr!Thread::ShouldChangeAbortToUnload+0x399
039bf96c 6afc78d1 clr!ManagedThreadBase_NoADTransition+0x35
039bf97c 6b00d313 clr!ManagedThreadBase::FinalizerBase+0xf
039bf9b4 6afd5a08 clr!WKS::GCHeap::FinalizerThreadStart+0x10c
039bfa4c 76573833 clr!Thread::intermediateThreadProc+0x4b
039bfa58 77c1a9bd kernel32!BaseThreadInitThunk+0xe
039bfa98 00000000 ntdll!_RtlUserThreadStart+0x23
```

Note: Indeed, we also have NullReferenceException objects on the raw stack:

```
0:002> !DumpStackObjects
OS Thread Id: 0x62478 (2)
ESP/REG  Object   Name
039BE364 09be4ea0 System.Windows.Forms.NativeMethods+MSG[]
039BE368 09bd2c6c System.Windows.Forms.Application+ThreadContext
039BE370 09bd4148 System.Windows.Forms.Application+ComponentManager
039BE3E8 09bd2c6c System.Windows.Forms.Application+ThreadContext
039BE428 09bd40fc System.Windows.Forms.Application+ModalApplicationContext
039BE4A4 09bd28f4 LINQPad.UI.ThreadExceptionForm
039BE52C 09bd281c System.UnhandledExceptionEventArgs
039BE540 09895194 System.Runtime.Remoting.Proxies.__TransparentProxy
039BE550 09895194 System.Runtime.Remoting.Proxies.__TransparentProxy
039BE5F0 09895194 System.Runtime.Remoting.Proxies.__TransparentProxy
039BE5F4 018c10c4 System.UnhandledExceptionEventHandler
039BE818 018c10c4 System.UnhandledExceptionEventHandler
039BE820 09895194 System.Runtime.Remoting.Proxies.__TransparentProxy
039BE928 09bd281c System.UnhandledExceptionEventArgs
039BE99C 018c10c4 System.UnhandledExceptionEventHandler
039BEA20 09bd1ff0 System.NullReferenceException
039BEA24 09895194 System.Runtime.Remoting.Proxies.__TransparentProxy
039BEA98 09bcd21c System.NullReferenceException
039BEC30 09890200 System.AppDomain
039BED44 09bcd21c System.NullReferenceException
039BEE30 09bcd21c System.NullReferenceException
```

16. If a finalizer thread is hanging we might have the problem with GC and have a possible heap leak as all objects on a finalizer queue are rooted. We check managed heap statistics:

```
0:002> !DumpHeap -stat
total 0 objects
Statistics:
      MT    Count    TotalSize Class Name
[...]
056221bc    49999       799984 UserQuery+SmallObject
6968b6bc    41102       986448 System.Collections.Generic.List`1[[System.Object, mscorlib]]
051ffa40    84856      1357696
System.Collections.ObjectModel.ReadOnlyCollection`1[[ICSharpCode.SharpDevelop.Dom.IParameter,
ICSharpCode.SharpDevelop.Dom]]
6969ffcc    50012      2400576 System.Threading.Thread
051fbbec    18790      2405120 ICSharpCode.SharpDevelop.Dom.DefaultClass
6a86f97c    64965      2598600 System.Collections.Generic.SortedList`2[[System.String, mscorlib],[System.Object,
mscorlib]]
051febfc    31785      2924220 ICSharpCode.SharpDevelop.Dom.DefaultField
051fc718    64965      3118320 ICSharpCode.SharpDevelop.Dom.DefaultAttribute
0524392c    41680      5835200 ICSharpCode.SharpDevelop.Dom.DefaultProperty
051ff810   163570      7197080 ICSharpCode.SharpDevelop.Dom.DefaultParameter
69656c28   256714      7220260 System.Object[]
6969f9ac   160003      8840480 System.String
051ff090   107240     12010880 ICSharpCode.SharpDevelop.Dom.DefaultMethod
0020d6c8    69335     14477560      Free
696a2938    50303    819928316 System.Int32[]
Total 1644434 objects
```

Note: We see about 50,000 UserQuery+SmallObject objects and almost the same amount of int32 arrays. We check the object class:

```
0:002> !DumpMT 056221bc
EEClass:      0561450c
Module:       05621050
Name:         UserQuery+SmallObject
mdToken:      02000004
File:         C:\Users\Training\AppData\Local\Temp\LINQPad\zbqvhjml\query_uobgah.dll
BaseSize:        0x10
ComponentSize:   0x0
Slots in VTable: 6
Number of IFaces in IFaceMap: 0

0:002> !DumpClass 0561450c
Class Name:      UserQuery+SmallObject
mdToken:         02000004
File:            C:\Users\Training\AppData\Local\Temp\LINQPad\zbqvhjml\query_uobgah.dll
Parent Class:    69383ef8
Module:          05621050
Method Table:    056221bc
Vtable Slots:    4
Total Method Slots:  5
Class Attributes:    100002
Transparency:        Critical
NumInstanceFields:   2
NumStaticFields:     0
      MT    Field   Offset                 Type VT     Attr    Value Name
696a2938  4000003        4       System.Int32[]  0 instance           buffer
6969ffcc  4000004        8 ....Threading.Thread  0 instance           thread
```

17. We can calulate the average array size and dump all heap objects that satisfy the minimum size:

```
0:002> ? 0n819928316/0n50000
Evaluate expression: 16398 = 0000400e

0:002> !DumpHeap -min 16000
 Address       MT     Size
01913368 696a4944    82668
01cd7eb4 05242c00    30908
0203c450 05242c00    30908
0285dfcc 05242c00    30908
068f9d98 05242c00    30908
0712097c 05242c00    30908
0748c998 05242c00    30908
07a74810 696a2938    16396
07dcfa0c 05242c00    30908
082637ac 05242c00    30908
09067948 05242c00    30908
093ce87c 05242c00    30908
098b5200 696a2938    16396
098b9620 696a2938    16396
098c827c 696a2938    16396
098cd880 696a2938    16396
098d18cc 696a2938    16396
098d5918 696a2938    16396
098d9964 696a2938    16396
098dd9b0 696a2938    16396
098e19fc 696a2938    16396
098e5a48 696a2938    16396
098e9a94 696a2938    16396
098edae0 696a2938    16396
098f1b2c 696a2938    16396
```

```
098f5b78 696a2938    16396
098f9bc4 696a2938    16396
098fdc10 696a2938    16396
099023bc 696a2938    16396
09906408 696a2938    16396
0990ba9c 696a2938    16396
09910144 696a2938    16396
09914190 696a2938    16396
09918334 696a2938    16396
0991c380 696a2938    16396
099203cc 696a2938    16396
09924418 696a2938    16396
09928464 696a2938    16396
0992c4b0 696a2938    16396
099304fc 696a2938    16396
09934548 696a2938    16396
099387f4 696a2938    16396
0993cd30 696a2938    16396
09940d7c 696a2938    16396
09944dc8 696a2938    16396
09948e14 696a2938    16396
0994ce60 696a2938    16396
09950eac 696a2938    16396
09954ef8 696a2938    16396
0995933c 696a2938    16396
0995d388 696a2938    16396
099613d4 696a2938    16396
09965420 696a2938    16396
0996946c 696a2938    16396
0996d4b8 696a2938    16396
09971504 696a2938    16396
09975550 696a2938    16396
0997959c 696a2938    16396
0997d618 696a2938    16396
09981664 696a2938    16396
099856b0 696a2938    16396
099896fc 696a2938    16396
0998d748 696a2938    16396
09991794 696a2938    16396
099957e0 696a2938    16396
0999982c 696a2938    16396
0999d878 696a2938    16396
099a18c4 696a2938    16396
099a5910 696a2938    16396
099a995c 696a2938    16396
099ad9a8 696a2938    16396
099b19f4 696a2938    16396
[...]

0:002> !DumpObj 099b19f4
Name:        System.Int32[]
MethodTable: 696a2938
EEClass:     693d9d48
Size:        16396(0x400c) bytes
Array:       Rank 1, Number of elements 4096, Type Int32
Element Type:System.Int32
Fields:
None
```

18. We can also dump all UserQuery+SmallObject objects from the managed heap:

```
0:002> !DumpHeap -type UserQuery+SmallObject
 Address       MT     Size
07a7881c 056221bc       16
098b4d54 056221bc       16
098b920c 056221bc       16
098bd62c 056221bc       16
098cc288 056221bc       16
098d188c 056221bc       16
098d58d8 056221bc       16
098d9924 056221bc       16
098dd970 056221bc       16
098e19bc 056221bc       16
098e5a08 056221bc       16
098e9a54 056221bc       16
098edaa0 056221bc       16
098f1aec 056221bc       16
098f5b38 056221bc       16
098f9b84 056221bc       16
098fdbd0 056221bc       16
09901c1c 056221bc       16
099063c8 056221bc       16
0990a414 056221bc       16
0990faa8 056221bc       16
[...]

0:002> !DumpObj 0990faa8
Name:        UserQuery+SmallObject
MethodTable: 056221bc
EEClass:     0561450c
Size:        16(0x10) bytes
File:        C:\Users\Training\AppData\Local\Temp\LINQPad\zbqvhjml\query_uobgah.dll
Fields:
      MT    Field   Offset                 Type VT     Attr    Value Name
696a2938  4000003        4       System.Int32[]  0 instance 09910144 buffer
6969ffcc  4000004        8 ....Threading.Thread  0 instance 0990fab8 thread

0:002> !DumpObj 09910144
Name:        System.Int32[]
MethodTable: 696a2938
EEClass:     693d9d48
Size:        16396(0x400c) bytes
Array:       Rank 1, Number of elements 4096, Type Int32
Element Type:System.Int32
Fields:
None
```

Note: We see that every object has a thread object reference and we have almost the same amount of Thread objects on the managed heap so this could have contributed to our thread handle leak.

19. We also check GC heap, GC handles and the finalizer queue:

```
0:002> !eeheap -gc
Number of GC Heaps: 1
generation 0 starts at 0x4a17ebb8
generation 1 starts at 0x49e81000
generation 2 starts at 0x01891000
ephemeral segment allocation context: none
 segment     begin allocated  size
01890000  01891000  0288ffd0  0xffefd0(16773072)
065c0000  065c1000  075bffe4  0xffefe4(16773092)
07750000  07751000  0874f088  0xffe088(16769160)
08d00000  08d01000  09cff5d0  0xffe5d0(16770512)
0b490000  0b491000  0c48daf0  0xffcaf0(16763632)
0c9e0000  0c9e1000  0d9de290  0xffd290(16765584)
0e070000  0e071000  0f06d970  0xffc970(16763248)
0f870000  0f871000  1086ce1c  0xffbe1c(16760348)
10870000  10871000  1186bff4  0xffaff4(16756724)
11870000  11871000  1286fdd0  0xffedd0(16772560)
13840000  13841000  1483e018  0xffd018(16764952)
14840000  14841000  1583f334  0xffe334(16769844)
15840000  15841000  1683eed0  0xffded0(16768720)
16840000  16841000  1783c6b8  0xffb6b8(16758456)
17840000  17841000  187d855c  0xf9755c(16348508)
18840000  18841000  19725e4c  0xee4e4c(15617612)
1a560000  1a561000  1b44a2bc  0xee92bc(15635132)
1c530000  1c531000  1d419528  0xee8528(15631656)
1d530000  1d531000  1e414898  0xee3898(15612056)
1e530000  1e531000  1f41ae60  0xee9e60(15638112)
1f530000  1f531000  2041ed48  0xeedd48(15654216)
20530000  20531000  21404af4  0xed3af4(15547124)
21530000  21531000  22447418  0xf16418(15819800)
22530000  22531000  23473488  0xf42488(16000136)
24500000  24501000  253eeed8  0xeeded8(15654616)
25500000  25501000  263e41dc  0xee31dc(15610332)
26500000  26501000  273e5738  0xee4738(15615800)
27500000  27501000  283f1a1c  0xef0a1c(15665692)
28500000  28501000  293e6b30  0xee5b30(15620912)
29500000  29501000  2a3e9174  0xee8174(15630708)
2a500000  2a501000  2b3e6df4  0xee5df4(15621620)
2c4d0000  2c4d1000  2d3a8e3c  0xed7e3c(15564348)
2d4d0000  2d4d1000  2e3ac408  0xedb408(15578120)
2e4d0000  2e4d1000  2f3bd83c  0xeec83c(15648828)
2f4d0000  2f4d1000  303b379c  0xee279c(15607708)
31f10000  31f11000  32deba58  0xedaa58(15575640)
32f10000  32f11000  33df0c20  0xedfc20(15596576)
33f10000  33f11000  34df7f84  0xee6f84(15626116)
35ee0000  35ee1000  36dcc0e8  0xeeb0e8(15642856)
36ee0000  36ee1000  37dc22dc  0xee12dc(15602396)
37ee0000  37ee1000  38cbeb88  0xdddb88(14539656)
38ee0000  38ee1000  39edf5a8  0xffe5a8(16770472)
39ee0000  39ee1000  3ae90688  0xfaf688(16447112)
3aee0000  3aee1000  3bdbee9c  0xedde9c(15589020)
3bee0000  3bee1000  3cdc8544  0xee7544(15627588)
3deb0000  3deb1000  3ed9b364  0xeea364(15639396)
3eeb0000  3eeb1000  3fd900ec  0xedf0ec(15593708)
3feb0000  3feb1000  40d8d44c  0xedc44c(15582284)
40eb0000  40eb1000  41d94edc  0xee3edc(15613660)
41eb0000  41eb1000  42d98fa4  0xee7fa4(15630244)
42eb0000  42eb1000  43d8a520  0xed9520(15570208)
```

```
43eb0000  43eb1000  44d80040  0xecf040(15528000)
44eb0000  44eb1000  45e9f25c  0xfee25c(16704092)
46e80000  46e81000  47dbad68  0xf39d68(15965544)
47e80000  47e81000  48d8ca1c  0xf0ba1c(15776284)
48e80000  48e81000  49a13fc8  0xb92fc8(12136392)
49e80000  49e81000  4a1c4bc4  0x343bc4(3423172)
Large object heap starts at 0x02891000
 segment     begin allocated  size
02890000  02891000  02ef8050  0x667050(6713424)
Total Size:              Size: 0x35b35b5c (900946780) bytes.
------------------------------
GC Heap Size:            Size: 0x35b35b5c (900946780) bytes.

0:002> !GCHandles
GC Handle Statistics:
Strong Handles:       90
Pinned Handles:       15
Async Pinned Handles: 1
Ref Count Handles:    108
Weak Long Handles:    0
Weak Short Handles:   0
Other Handles:        0
Statistics:
      MT    Count    TotalSize Class Name
6d5f7208        1           12 System.Management.MarshalWbemObject
696aa71c        1           12 System.OleAutBinder
696a4c1c        1           12 System.Security.Permissions.SecurityPermission
6969f5e8        1           12 System.Object
6a862d34        1           20 System.Net.TimerThread+TimerQueue
696a1b18        1           28 System.SharedStatics
67b62fec        3           60 System.Windows.Forms.DropTarget
6938736c        1           68 System.Threading.OverlappedData
6969fde8        1           84 System.ExecutionEngineException
6969fd9c        1           84 System.StackOverflowException
6969fd50        1           84 System.OutOfMemoryException
6969fc0c        1           84 System.Exception
6969470c        1           84 System.NullReferenceException
69693814        1           84 System.Runtime.Serialization.SerializationException
05622254        1           92 UserQuery+CustomException
696a3670        3          108 System.Security.PermissionSet
67b70f14        9          144 System.Windows.Forms.WebBrowser+WebBrowserSite
6969fe34        2          168 System.Threading.ThreadAbortException
67b712c8        9          180 System.Windows.Forms.WebBrowser+WebBrowserEvent
696948ec        2          192 System.IO.FileNotFoundException
696a0ec8        2          224 System.AppDomain
69688df4        3          240 System.Runtime.Remoting.ServerIdentity
67b716b8        9          324 System.Windows.Forms.WebBrowserContainer
67b6deb4        8          384 System.Windows.Forms.Timer
6969ffcc        9          432 System.Threading.Thread
012050f0        1          792 LINQPad.UI.MainForm
0130838c        3         1044 LINQPad.UI.ThreadExceptionForm
6d726880       78         1560 System.Drawing.Internal.GPStream
696a0070       32         1920 System.Reflection.RuntimeMethodInfo
696a4944        1         8204 System.Byte[]
69656c28       26       111140 System.Object[]
Total 214 objects
```

```
0:002> !FinalizeQueue
SyncBlocks to be cleaned up: 9
MTA Interfaces to be released: 0
STA Interfaces to be released: 0
----------------------------------
generation 0 has 2841 finalizable objects (056837e8->0568644c)
generation 1 has 13 finalizable objects (056837b4->056837e8)
generation 2 has 3557 finalizable objects (05680020->056837b4)
Ready for finalization 107495 objects (0568644c->056ef3e8)
Statistics for all finalizable objects (including all objects ready for finalization):
      MT    Count    TotalSize Class Name
6d727f98        1           12 System.Drawing.Imaging.ImageAttributes
6968e2d8        1           12 System.LocalDataStoreHolder
6d7270e8        1           16 System.Drawing.StringFormat
6965e334        1           16 System.Threading.OverlappedDataCache
6a853aac        1           20 System.Net.SafeInternetHandle
6a852d78        1           20 System.Net.SafeLocalFree
696a73c4        1           20 Microsoft.Win32.SafeHandles.SafeFileMappingHandle
696a736c        1           20 Microsoft.Win32.SafeHandles.SafeViewOfFileHandle
6969f4d0        1           20 Microsoft.Win32.SafeHandles.SafePEFileHandle
6965e388        1           20 System.Threading.OverlappedDataCacheLine
691d428c        1           20 Microsoft.Win32.SafeHandles.SafePipeHandle
67b680f0        1           20 System.Windows.Forms.ApplicationContext
6968e258        1           24 System.LocalDataStoreSlot
67b6555c        3           36 System.Windows.Forms.ImageList+NativeImageList
6a857f7c        2           40 System.Net.SafeCloseSocket+InnerSafeCloseSocket
696a6034        2           40 Microsoft.Win32.SafeHandles.SafeFileHandle
696a5740        2           40 System.Security.Cryptography.SafeProvHandle
6965f56c        1           40 System.Reflection.Emit.DynamicResolver
6965a46c        2           40 System.Threading.ThreadPoolWorkQueueThreadLocals
012055d8        2           40 LINQPad.TempFileRef
67b6aaf4        1           44 System.Windows.Forms.NativeWindow
0524c8d0        1           44 ActiproSoftware.SyntaxEditor.FindReplaceOptions
6a8538bc        2           56 System.Net.SafeCloseSocketAndEvent
03dc4748        1           56 LINQPad.UI.EditManager
691d5c28        1           60 System.IO.Pipes.NamedPipeServerStream
67b55850        3           60 System.Windows.Forms.HtmlShimManager
696987e0        1           72 System.Diagnostics.Eventing.FrameworkEventSource
683606f0        3           72 System.Windows.Forms.Application+ModalApplicationContext
6969224c        1           80 System.IO.FileStream
69698834        1           84
System.Diagnostics.Eventing.EventProviderBase+OverideEventProvider
6a865604        1           92 System.IO.FileSystemWatcher
6a853968        4           96 System.Net.SafeRegistryHandle
67b5d1a4        3           96 System.Windows.Forms.CachedItemHdcInfo
67b59850        9          108
System.Windows.Forms.VisualStyles.VisualStyleRenderer+ThemeHandle
67b6f1e4        4          112 System.Windows.Forms.Cursor
69688a28        2          120 System.Runtime.Remoting.Contexts.Context
051f1024        3          132
ActiproSoftware.SyntaxEditor.Addons.Dynamic.LexicalMacroCollection
69697a30        7          140 Microsoft.Win32.SafeHandles.SafeRegistryHandle
67b6d278       10          160 System.Windows.Forms.Control+FontHandleWrapper
0524ce48        4          160 ActiproSoftware.SyntaxEditor.IntelliPromptSmartTag
04e69818        3          192 ActiproSoftware.SyntaxEditor.IntelliPromptParameterInfo
008233bc        3          192 ActiproSoftware.SyntaxEditor.IntelliPromptMemberList
67b6d3d8        4          208 System.Windows.Forms.Control+ThreadMethodEntry
67b65074        1          208 System.Windows.Forms.TabControl
6d726edc        6          216 System.Drawing.Pen
051f1784        6          216 ActiproSoftware.SyntaxEditor.SyntaxLanguageProperty
```

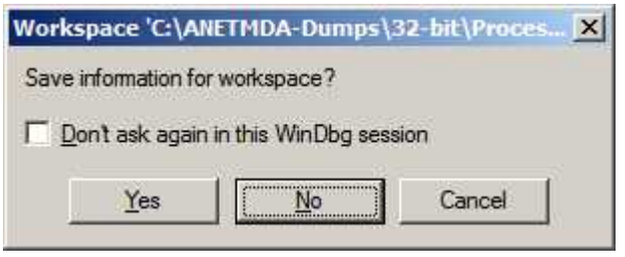
```
044caab8        6          216 ActiproSoftware.SyntaxEditor.MacroRecording
6965a65c       11          220 Microsoft.Win32.SafeHandles.SafeTokenHandle
67b5c85c        1          220 System.Windows.Forms.Application+ParkingWindow
67b60b60        3          228 System.Windows.Forms.ImageList
03dc35e8        1          236 LINQPad.UI.QueryTabControl
6d72778c        6          240 System.Drawing.Icon
67b6dd84       12          240 System.Windows.Forms.Internal.WindowsRegion
6a867074        8          256 System.ComponentModel.Container
696a5efc        6          264 System.Threading.ReaderWriterLock
044cb67c        6          264 ActiproSoftware.SyntaxEditor.EditorViewCollection
044ca884        6          264 ActiproSoftware.SyntaxEditor.IntelliPrompt
044c7138        6          264 ActiproSoftware.SyntaxEditor.TriggerCollection
044c6e64        6          264 ActiproSoftware.SyntaxEditor.SyntaxLanguageCollection
044c6014        6          264 ActiproSoftware.SyntaxEditor.HighlightingStyleCollection
6d725ffc        4          272 System.Drawing.BufferedGraphicsContext
03dc14f0        1          296 LINQPad.UI.SampleQueries
03dc0044        1          308 LINQPad.UI.SchemaTree
052491a0        6          312 ActiproSoftware.SyntaxEditor.ProgrammaticLexicalScope
04e6a2c4        6          312 ActiproSoftware.SyntaxEditor.IntelliPromptQuickInfo
03dc0c0c        1          312 LINQPad.UI.MyQueries
6969b298       16          320 Microsoft.Win32.SafeHandles.SafeWaitHandle
0120f218        1          332 LINQPad.UI.ResultsDockForm
6d81b9a8        6          336 System.Drawing.Printing.PrintDocument
044c4830        6          336 ActiproSoftware.SyntaxEditor.UndoRedo
67b570b0        1          340 System.Windows.Forms.MenuStrip
67b71918       18          360 System.Windows.Forms.AxHost+ConnectionPointCookie
044cada4        6          384 ActiproSoftware.SyntaxEditor.PrintSettings
051f0db4        3          396 LINQPad.Lexers.SqlDynamicSyntaxLanguage
044ca1e0        6          408 bl
67b6b4e4        4          416 System.Windows.Forms.Application+MarshalingControl
67b71ae4        9          432 System.Windows.Forms.WebBrowserBase+WebBrowserBaseNativeWindow
67b615ac        3          432 System.Windows.Forms.ToolStripProgressBar
044c80c0       12          432 ActiproSoftware.SyntaxEditor.UndoableModificationStack
052488cc        3          444 ActiproBridge.CustomCSharpSyntaxLanguage
67b61134        3          456 System.Windows.Forms.ProgressBar
044c3cd0        3          468 LINQPad.UI.FixedLinkLabel
67b6b16c        4          528 System.Windows.Forms.Application+ThreadContext
044c5ea4        9          576 ActiproSoftware.SyntaxEditor.DefaultLexicalState
67b59370        7          644 System.Windows.Forms.ToolStripPanelCell
04e65714        6          672 bm
67b619d8        3          696 System.Windows.Forms.LinkLabel
67b69948        7          728 System.Windows.Forms.Control
67b63534       16          768 System.Windows.Forms.ToolTip+ToolTipNativeWindow
051f1340       18          792
ActiproSoftware.SyntaxEditor.Addons.Dynamic.LexicalPatternGroupCollection
044cb528       18          792 ActiproSoftware.WinUICore.UIElementCollection
012050f0        1          792 LINQPad.UI.MainForm
03dc3e70        7          812 LINQPad.UI.ClearButton
67b59a9c        6          840 System.Windows.Forms.ToolStripDropDownButton
6d7265bc       43          860 System.Drawing.FontFamily
00820818        3          876 LINQPad.UI.DataResultsWebBrowser
67b560f8       18          936 System.Windows.Forms.Timer+TimerNativeWindow
683576c8        5          940 System.Windows.Forms.TabPage
67b6e83c        3         1008 System.Windows.Forms.ToolStrip
67b694b4        6         1008 System.Windows.Forms.TextBox
67b59908        7         1008 System.Windows.Forms.ToolStripOverflowButton
03dc8ee4        6         1032 LINQPad.UI.ImageButton
01300660        6         1032 LINQPad.UI.MainForm+MruToolStripMenuItem
67b57bfc        3         1044 System.Windows.Forms.StatusStrip
0130838c        3         1044 LINQPad.UI.ThreadExceptionForm
```

```
6938736c       16         1088 System.Threading.OverlappedData
67b66b6c        7         1176 System.Windows.Forms.Button
051f1a24       21         1176 ActiproSoftware.SyntaxEditor.Addons.Dynamic.DynamicLexicalScope
044c7b4c       27         1188 ActiproSoftware.SyntaxEditor.LexicalScopeCollection
03dcf6c0        6         1248 ActiproSoftware.SyntaxEditor.Document
67b5d3d8        7         1260 System.Windows.Forms.TableLayoutPanel
67b66e64        6         1392 System.Windows.Forms.ComboBox
04e654d4       12         1392 b1
051f1210       18         1512 ActiproSoftware.SyntaxEditor.Addons.Dynamic.DynamicLexicalState
03dc2834        3         1584 LINQPad.UI.QueryControl
00820af8        9         1584 LINQPad.UI.QueryControl+BrowserBorder
04e66fa0       12         1680 ActiproSoftware.WinUICore.ScrollBarThumb
6d727048       47         1692 System.Drawing.SolidBrush
0082003c        6         1704 LINQPad.UI.ResultsWebBrowser
044c59d0       33         1716 ActiproSoftware.SyntaxEditor.LexicalStateCollection
67b6deb4       37         1776 System.Windows.Forms.Timer
67b5cbb8      111         1776 System.Windows.Forms.WindowsGraphicsWrapper
67b69678       14         1792 System.Windows.Forms.Label
67b70af4       10         1840 System.Windows.Forms.SplitterPanel
67b60e08       16         1856 System.Windows.Forms.ToolTip
67b6fcdc        5         1860 System.Windows.Forms.SplitContainer
67b57f2c        9         1872 System.Windows.Forms.ToolStripStatusLabel
6d727528       43         1892 System.Drawing.Font
67b6fb50        4         1984 System.Windows.Forms.ContextMenuStrip
67b580e4       15         2040 System.Windows.Forms.ToolStripButton
04e60d04        6         2256 ActiproSoftware.SyntaxEditor.EditorView
03dcda9c        3         2532 ActiproSoftware.SyntaxEditor.SyntaxEditor
6d7271fc      107         2568 System.Drawing.Bitmap
67b5d6ac       43         2580 System.Windows.Forms.Control+PrintPaintEventArgs
044c30a4        3         2688 LINQPad.UI.QueryEditor
04e66da4       24         2784 ActiproSoftware.WinUICore.ScrollBarButton
044c22e0        6         2952
ActiproSoftware.SyntaxEditor.VisualStudio2005SyntaxEditorRenderer
6d726084       70         3080 System.Drawing.BufferedGraphics
67b59678       24         3840 System.Windows.Forms.ToolStripGrip
67b5b150       24         4224 System.Windows.Forms.Panel
67b5bd38       34         4488 System.Windows.Forms.ToolStripScrollButton+StickyLabel
04e66474       12         4608 ActiproSoftware.WinUICore.ScrollBar
67b5597c       39         4992 System.Windows.Forms.ToolStripSeparator
67b5bbf4       34         5032 System.Windows.Forms.ToolStripScrollButton
67b5ad24       13         6448 System.Windows.Forms.ToolStripDropDownMenu
6d7279c4      210         6720 System.Drawing.Graphics
6d7278c8      440         7040 System.Drawing.Drawing2D.Matrix
6d7273c8      447         7152 System.Drawing.Region
67b6d6e8      208         8320 System.Windows.Forms.PaintEventArgs
67b6c430      298         8344 System.Windows.Forms.Internal.WindowsGraphics
051f2000      102        10608 ActiproSoftware.SyntaxEditor.Addons.Dynamic.LexicalPatternGroup
67b6aa5c      225        12600 System.Windows.Forms.Control+ControlNativeWindow
044c68f4       75        13500 ActiproSoftware.SyntaxEditor.HighlightingStyle
69699e60     1225        19600 System.WeakReference
67b57890      127        21844 System.Windows.Forms.ToolStripMenuItem
67b6c224     1058        38088 System.Windows.Forms.Internal.WindowsFont
051f2300     1212        53328 ActiproSoftware.SyntaxEditor.Addons.Dynamic.LexicalPattern
67b6c574     6812       490464 System.Windows.Forms.Internal.DeviceContext
056221bc    49999       799984 UserQuery+SmallObject
6969ffcc    50012      2400576 System.Threading.Thread
Total 113906 objects
```

20. We close logging before exiting WinDbg:

```
0:002> .logclose
Closing open log file C:\ANETMDA-Dumps\32-bit\Processes\CLR4\LINQPadD.log
```

If presented with this dialog choose No:



Note: To avoid possible confusion and glitches we recommend to exit WinDbg after each exercise.

Exercise PN6

- **Goal:** Learn how to recognize and analyze heap corruption
- **Patterns:** CLR Thread; Exception Thread; Invalid Pointer; Managed Heap Corruption; Execution Residue
- **Commands:** !VerifyHeap, dc
- \ANETMDA-Dumps\Exercise-PN6-Analysis-process-dump-LINQPadE-32-CLR4.pdf

© 2013 Software Diagnostics Services

Exercise PN6: Analysis of an application process dump (LINQPadE, 32-bit, CLR 4)

Goal: Learn how to recognize and analyze heap corruption.

Patterns: CLR Thread; Exception Thread; Invalid Pointer; Managed Heap Corruption; Execution Residue

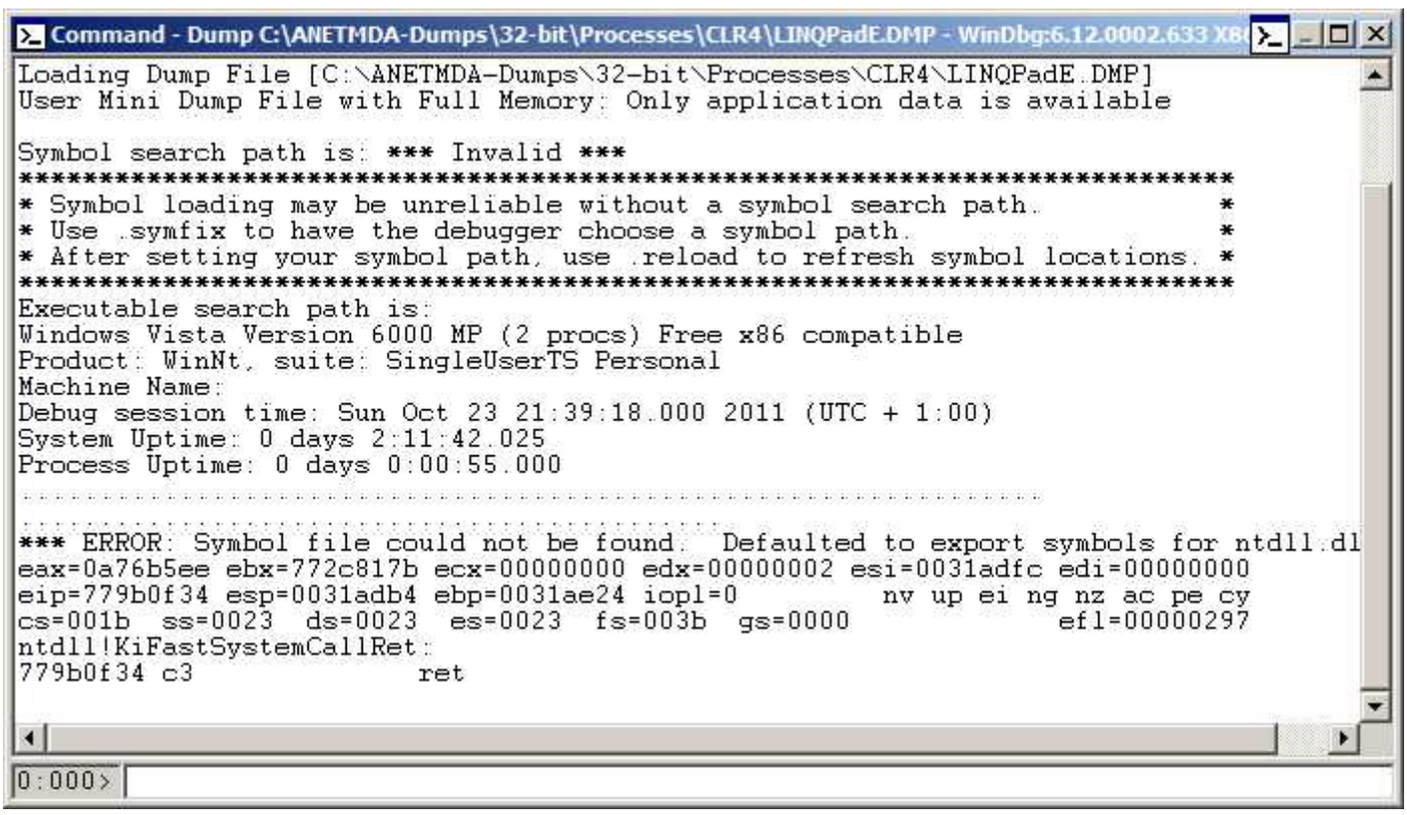
Commands: !VerifyHeap, dc

1. Launch WinDbg from Debugging Tools for Windows or Debugging Tools for Windows (x86)

2. Open \ANETMDA-Dumps\32-bit\Processes\CLR4\LINQPadE.DMP

3. If you are presented with this dialog say No:

4. We get the dump file loaded:



5. Open a log file using **.logopen** command and load symbols (**.symfix** and **.reload** commands):

```
0:000> .logopen C:\ANETMDA-Dumps\32-bit\Processes\CLR4\LINQPadE.log
Opened log file 'C:\ANETMDA-Dumps\32-bit\Processes\CLR4\LINQPadE.log'

0:000> .symfix c:\mss

0:000> .reload
.........................
```

Note: The results may be slightly different on your system if you have 32-bit .NET Framework 4.0.30319.**1** already installed or you don't have any .NET Framework 4.0.30319 installed.

6. Type ~***k** command to verify the correctness of all stack traces:

```
0:000> ~*k

.  0  Id: 36ec.36f0 Suspend: 0 Teb: 7ffdf000 Unfrozen
ChildEBP RetAddr
0031adb0 779b06a0 ntdll!KiFastSystemCallRet
0031adb4 772c77d4 ntdll!NtWaitForSingleObject+0xc
0031ae24 772c7742 kernel32!WaitForSingleObjectEx+0xbe
0031ae38 6c395816 kernel32!WaitForSingleObject+0x12
0031ae68 6c395eb1 clr!ClrWaitForSingleObject+0x24
0031b324 6c398c9a clr!RunWatson+0x1e3
0031ba50 6c3994c6 clr!DoFaultReportWorker+0xbd4
0031ba94 6c3e6769 clr!DoFaultReport+0x146
0031bae8 6c3e075c clr!WatsonLastChance+0x191
0031c4d0 6c3e0c36 clr!EEPolicy::LogFatalError+0x523
0031c81c 6c3e20a6 clr!EEPolicy::HandleFatalError+0x105
0031c840 6c23cad6 clr!CLRVectoredExceptionHandlerPhase3+0xaf
0031c874 6c23cd5f clr!CLRVectoredExceptionHandlerPhase2+0x20
0031c8a4 6c225b1f clr!CLRVectoredExceptionHandler+0xba
0031c8d0 7795c41b clr!CLRVectoredExceptionHandlerShim+0xa8
0031c8f8 77972b3a ntdll!RtlpCallVectoredHandlers+0x57
0031c90c 77972960 ntdll!RtlCallVectoredExceptionHandlers+0x15
0031c97c 779b0e97 ntdll!RtlDispatchException+0x19
0031c97c 6c421562 ntdll!KiUserExceptionDispatcher+0xf
0031cc7c 6c22bf56 clr!MethodTable::GetLoaderAllocatorObjectForGC+0x15
0031ccbc 6c22be41 clr!WKS::gc_heap::mark_object_simple1+0x3c0
0031cce8 6c22b9db clr!WKS::gc_heap::mark_object_simple+0x209
0031cd64 6c2282c6 clr!WKS::gc_heap::mark_through_cards_for_large_objects+0x36c
0031cda4 6c2273c5 clr!WKS::gc_heap::mark_phase+0x299
0031cdcc 6c227972 clr!WKS::gc_heap::gc1+0x134
0031ce50 6c22771f clr!WKS::gc_heap::garbage_collect+0x3ae
0031ce7c 6c22878a clr!WKS::GCHeap::GarbageCollectGeneration+0x17b
0031cea0 6c226b82 clr!WKS::gc_heap::try_allocate_more_space+0x162
0031ceb4 6c226e65 clr!WKS::gc_heap::allocate_more_space+0x13
0031ced4 6c1cc953 clr!WKS::GCHeap::Alloc+0x3d
0031cef0 6c18ecd8 clr!Alloc+0x8d
0031cf30 6c18edb6 clr!FastAllocateObject+0x38
*** WARNING: Unable to verify checksum for mscorlib.ni.dll
0031cfd0 6b65665e clr!JIT_NewFast+0xc8
0031e124 05a01798 mscorlib_ni+0x2b665e
WARNING: Frame IP not in any known module. Following frames may be wrong.
0031e834 6c20ff88 0x5a01798
0031e840 097fab1c clr!LayoutDestroyNative+0x3d
0031e84c 099bc590 0x97fab1c
00000000 00000000 0x99bc590
```

```
   1  Id: 36ec.36f8 Suspend: 0 Teb: 7ffdd000 Unfrozen
ChildEBP RetAddr
0113f7c0 779b0690 ntdll!KiFastSystemCallRet
0113f7c4 772c7e09 ntdll!ZwWaitForMultipleObjects+0xc
0113f860 772c8150 kernel32!WaitForMultipleObjectsEx+0x11d
0113f87c 6c2d75e8 kernel32!WaitForMultipleObjects+0x18
0113f8e0 6c2d7526 clr!DebuggerRCThread::MainLoop+0xd9
0113f910 6c2d7461 clr!DebuggerRCThread::ThreadProc+0xca
0113f93c 772c3833 clr!DebuggerRCThread::ThreadProcStatic+0x83
0113f948 7798a9bd kernel32!BaseThreadInitThunk+0xe
0113f988 00000000 ntdll!_RtlUserThreadStart+0x23

   2  Id: 36ec.36fc Suspend: 0 Teb: 7ffdc000 Unfrozen
ChildEBP RetAddr
03c2f9a0 779b0690 ntdll!KiFastSystemCallRet
03c2f9a4 772c7e09 ntdll!ZwWaitForMultipleObjects+0xc
03c2fa40 772c8150 kernel32!WaitForMultipleObjectsEx+0x11d
03c2fa5c 6c2e833d kernel32!WaitForMultipleObjects+0x18
03c2fa7c 6c2e83a1 clr!WKS::WaitForFinalizerEvent+0xa6
03c2fa94 6c225c05 clr!WKS::GCHeap::FinalizerThreadWorker+0x4a
03c2faa8 6c225c87 clr!Thread::DoExtraWorkForFinalizer+0x114
03c2fb58 6c225d42 clr!Thread::ShouldChangeAbortToUnload+0x101
03c2fbb8 6c2178be clr!Thread::ShouldChangeAbortToUnload+0x399
03c2fbdc 6c2178d1 clr!ManagedThreadBase_NoADTransition+0x35
03c2fbec 6c25d313 clr!ManagedThreadBase::FinalizerBase+0xf
03c2fc24 6c225a08 clr!WKS::GCHeap::FinalizerThreadStart+0x10c
03c2fcc0 772c3833 clr!Thread::intermediateThreadProc+0x4b
03c2fccc 7798a9bd kernel32!BaseThreadInitThunk+0xe
03c2fd0c 00000000 ntdll!_RtlUserThreadStart+0x23

   3  Id: 36ec.3700 Suspend: 0 Teb: 7ffdb000 Unfrozen
ChildEBP RetAddr
0470f070 779af9c0 ntdll!KiFastSystemCallRet
0470f074 7728f00d ntdll!NtFsControlFile+0xc
*** WARNING: Unable to verify checksum for System.Core.ni.dll
0470f0b8 699380b7 kernel32!ConnectNamedPipe+0x52
0470f128 699cc07c System_Core_ni+0x3080b7
0470f1d0 6b64ae5b System_Core_ni+0x39c07c
0470f1e0 6b5d7ff4 mscorlib_ni+0x2aae5b
0470f1fc 6b5d7f34 mscorlib_ni+0x237ff4
0470f21c 6b64ade8 mscorlib_ni+0x237f34
0470f234 6c1721db mscorlib_ni+0x2aade8
0470f244 6c194a2a clr!CallDescrWorker+0x33
0470f2c0 6c194bcc clr!CallDescrWorkerWithHandler+0x8e
0470f404 6c194c01 clr!MethodDesc::CallDescr+0x194
0470f420 6c30b512 clr!MethodDesc::CallTargetWorker+0x21
0470f62c 6c225c05 clr!ThreadNative::KickOffThread_Worker+0x1e1
0470f640 6c225c87 clr!Thread::DoExtraWorkForFinalizer+0x114
0470f6f0 6c225d42 clr!Thread::ShouldChangeAbortToUnload+0x101
0470f750 6c225dd9 clr!Thread::ShouldChangeAbortToUnload+0x399
0470f774 6c30b3e5 clr!Thread::ShouldChangeAbortToUnload+0x43a
0470f78c 6c30b2e0 clr!ManagedThreadBase::KickOff+0x15
0470f824 6c225a08 clr!ThreadNative::KickOffThread+0x23e
0470f948 772c3833 clr!Thread::intermediateThreadProc+0x4b
0470f954 7798a9bd kernel32!BaseThreadInitThunk+0xe
0470f994 00000000 ntdll!_RtlUserThreadStart+0x23
```

```
   4  Id: 36ec.3704 Suspend: 0 Teb: 7ffda000 Unfrozen
ChildEBP RetAddr
04a2f778 779b0690 ntdll!KiFastSystemCallRet
04a2f77c 772c7e09 ntdll!ZwWaitForMultipleObjects+0xc
04a2f818 7622c4af kernel32!WaitForMultipleObjectsEx+0x11d
04a2f86c 76228b7b user32!RealMsgWaitForMultipleObjectsEx+0x13c
04a2f888 74a41965 user32!MsgWaitForMultipleObjects+0x1f
04a2f8d4 772c3833 GdiPlus!BackgroundThreadProc+0x59
04a2f8e0 7798a9bd kernel32!BaseThreadInitThunk+0xe
04a2f920 00000000 ntdll!_RtlUserThreadStart+0x23

   5  Id: 36ec.3710 Suspend: 0 Teb: 7ffd7000 Unfrozen
ChildEBP RetAddr
0586fce0 779b00f0 ntdll!KiFastSystemCallRet
0586fce4 772a7948 ntdll!NtRemoveIoCompletion+0xc
0586fd10 774baf2e kernel32!GetQueuedCompletionStatus+0x29
0586fd4c 774bb067 rpcrt4!COMMON_ProcessCalls+0xb5
0586fdb8 774bac4f rpcrt4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
0586fdc4 774bacb9 rpcrt4!ProcessIOEventsWrapper+0xe
0586fde8 774bad03 rpcrt4!BaseCachedThreadRoutine+0x5c
0586fdf4 772c3833 rpcrt4!ThreadStartRoutine+0x1e
0586fe00 7798a9bd kernel32!BaseThreadInitThunk+0xe
0586fe40 00000000 ntdll!_RtlUserThreadStart+0x23

   6  Id: 36ec.3714 Suspend: 0 Teb: 7ffd6000 Unfrozen
ChildEBP RetAddr
05b0fe74 779af7c0 ntdll!KiFastSystemCallRet
05b0fe78 772c78e0 ntdll!NtDelayExecution+0xc
05b0fee0 77281da0 kernel32!SleepEx+0x62
05b0fef0 777d40f4 kernel32!Sleep+0xf
05b0fefc 777bfc0d ole32!CROIDTable::WorkerThreadLoop+0x14
05b0ff18 777bfc73 ole32!CRpcThread::WorkerLoop+0x26
05b0ff24 772c3833 ole32!CRpcThreadCache::RpcWorkerThreadEntry+0x20
05b0ff30 7798a9bd kernel32!BaseThreadInitThunk+0xe
05b0ff70 00000000 ntdll!_RtlUserThreadStart+0x23
```

```
   7  Id: 36ec.3718 Suspend: 0 Teb: 7ffd5000 Unfrozen
ChildEBP RetAddr
0596eb68 779b0690 ntdll!KiFastSystemCallRet
0596eb6c 772c7e09 ntdll!ZwWaitForMultipleObjects+0xc
0596ec08 6c22516a kernel32!WaitForMultipleObjectsEx+0x11d
0596ec6c 6c224f98 clr!WaitForMultipleObjectsEx_SO_TOLERANT+0x56
0596ec8c 6c224dd8 clr!Thread::DoAppropriateAptStateWait+0x4d
0596ed20 6c224e99 clr!Thread::DoAppropriateWaitWorker+0x17d
0596ed8c 6c224f17 clr!Thread::DoAppropriateWait+0x60
0596ede0 6c1cd409 clr!CLREvent::WaitEx+0x106
0596edf4 6c30c71c clr!CLREvent::Wait+0x19
0596ee08 6c30c73a clr!Thread::Wait+0x1d
0596ee1c 6c30c545 clr!Thread::Block+0x1a
0596eec8 6c30c5b2 clr!SyncBlock::Wait+0x169
0596eedc 6c30c6a4 clr!ObjHeader::Wait+0x2c
0596ef84 6b5d9140 clr!ObjectNative::WaitTimeout+0x147
0596ef94 6bb9428a mscorlib_ni+0x239140
0596f060 6b64ae5b mscorlib_ni+0x7f428a
0596f070 6b5d7ff4 mscorlib_ni+0x2aae5b
0596f08c 6b5d7f34 mscorlib_ni+0x237ff4
0596f0ac 6b64ade8 mscorlib_ni+0x237f34
0596f0c4 6c1721db mscorlib_ni+0x2aade8
0596f0d4 6c194a2a clr!CallDescrWorker+0x33
0596f150 6c194bcc clr!CallDescrWorkerWithHandler+0x8e
0596f294 6c194c01 clr!MethodDesc::CallDescr+0x194
0596f2b0 6c30b512 clr!MethodDesc::CallTargetWorker+0x21
0596f4bc 6c225c05 clr!ThreadNative::KickOffThread_Worker+0x1e1
0596f4d0 6c225c87 clr!Thread::DoExtraWorkForFinalizer+0x114
0596f580 6c225d42 clr!Thread::ShouldChangeAbortToUnload+0x101
0596f5e0 6c225dd9 clr!Thread::ShouldChangeAbortToUnload+0x399
0596f604 6c30b3e5 clr!Thread::ShouldChangeAbortToUnload+0x43a
0596f61c 6c30b2e0 clr!ManagedThreadBase::KickOff+0x15
0596f6b4 6c225a08 clr!ThreadNative::KickOffThread+0x23e
0596f94c 772c3833 clr!Thread::intermediateThreadProc+0x4b
0596f958 7798a9bd kernel32!BaseThreadInitThunk+0xe
0596f998 00000000 ntdll!_RtlUserThreadStart+0x23
```

```
   8  Id: 36ec.3764 Suspend: 0 Teb: 7ffd9000 Unfrozen
ChildEBP RetAddr
0564eebc 779b0690 ntdll!KiFastSystemCallRet
0564eec0 772c7e09 ntdll!ZwWaitForMultipleObjects+0xc
0564ef5c 6c22516a kernel32!WaitForMultipleObjectsEx+0x11d
0564efc0 6c224f98 clr!WaitForMultipleObjectsEx_SO_TOLERANT+0x56
0564efe0 6c224dd8 clr!Thread::DoAppropriateAptStateWait+0x4d
0564f074 6c224e99 clr!Thread::DoAppropriateWaitWorker+0x17d
0564f0e0 6c201329 clr!Thread::DoAppropriateWait+0x60
0564f1e0 6b64b5ef clr!WaitHandleNative::CorWaitOneNative+0x196
0564f1f8 6b64b5ad mscorlib_ni+0x2ab5ef
0564f218 6b64b570 mscorlib_ni+0x2ab5ad
0564f260 6b64ae5b mscorlib_ni+0x2ab570
0564f270 6b5d7ff4 mscorlib_ni+0x2aae5b
0564f28c 6b5d7f34 mscorlib_ni+0x237ff4
0564f2ac 6b64ade8 mscorlib_ni+0x237f34
0564f2c4 6c1721db mscorlib_ni+0x2aade8
0564f2d4 6c194a2a clr!CallDescrWorker+0x33
0564f350 6c194bcc clr!CallDescrWorkerWithHandler+0x8e
0564f494 6c194c01 clr!MethodDesc::CallDescr+0x194
0564f4b0 6c30b512 clr!MethodDesc::CallTargetWorker+0x21
0564f6bc 6c225c05 clr!ThreadNative::KickOffThread_Worker+0x1e1
0564f6d0 6c225c87 clr!Thread::DoExtraWorkForFinalizer+0x114
0564f780 6c225d42 clr!Thread::ShouldChangeAbortToUnload+0x101
0564f7e0 6c225dd9 clr!Thread::ShouldChangeAbortToUnload+0x399
0564f804 6c30b3e5 clr!Thread::ShouldChangeAbortToUnload+0x43a
0564f81c 6c30b2e0 clr!ManagedThreadBase::KickOff+0x15
0564f8b4 6c225a08 clr!ThreadNative::KickOffThread+0x23e
0564fc4c 772c3833 clr!Thread::intermediateThreadProc+0x4b
0564fc58 7798a9bd kernel32!BaseThreadInitThunk+0xe
0564fc98 00000000 ntdll!_RtlUserThreadStart+0x23

   9  Id: 36ec.3768 Suspend: 0 Teb: 7ffd8000 Unfrozen
ChildEBP RetAddr
0769f7bc 779af7c0 ntdll!KiFastSystemCallRet
0769f7c0 772c78e0 ntdll!NtDelayExecution+0xc
0769f828 6c1ccc0a kernel32!SleepEx+0x62
0769f83c 6c1ccbdb clr!__DangerousSwitchToThread+0x48
0769f850 6c24878b clr!__SwitchToThread+0x12
0769f938 772c3833 clr!ThreadpoolMgr::GateThreadStart+0x83
0769f944 7798a9bd kernel32!BaseThreadInitThunk+0xe
0769f984 00000000 ntdll!_RtlUserThreadStart+0x23

  10  Id: 36ec.376c Suspend: 0 Teb: 7ffd4000 Unfrozen
ChildEBP RetAddr
0797fa10 779b00f0 ntdll!KiFastSystemCallRet
0797fa14 772a7948 ntdll!NtRemoveIoCompletion+0xc
0797fa40 6c23aeab kernel32!GetQueuedCompletionStatus+0x29
0797faa4 6c225a08 clr!ThreadpoolMgr::CompletionPortThreadStart+0x155
0797febc 772c3833 clr!Thread::intermediateThreadProc+0x4b
0797fec8 7798a9bd kernel32!BaseThreadInitThunk+0xe
0797ff08 00000000 ntdll!_RtlUserThreadStart+0x23
```

```
  11  Id: 36ec.3798 Suspend: 0 Teb: 7ff4c000 Unfrozen
ChildEBP RetAddr
0a54f354 779b06a0 ntdll!KiFastSystemCallRet
0a54f358 772c77d4 ntdll!NtWaitForSingleObject+0xc
0a54f3c8 6c1d1030 kernel32!WaitForSingleObjectEx+0xbe
0a54f3fc 6c1d1071 clr!CLREvent::CreateManualEvent+0xf6
0a54f44c 6c1cd3e8 clr!CLREvent::CreateManualEvent+0x137
0a54f48c 6c1cd409 clr!CLREvent::WaitEx+0x126
0a54f4a0 6c2fce05 clr!CLREvent::Wait+0x19
0a54f574 6c225a08 clr!AppDomain::ADUnloadThreadStart+0x2f5
0a54fb0c 772c3833 clr!Thread::intermediateThreadProc+0x4b
0a54fb18 7798a9bd kernel32!BaseThreadInitThunk+0xe
0a54fb58 00000000 ntdll!_RtlUserThreadStart+0x23

  12  Id: 36ec.37e0 Suspend: 0 Teb: 7ff4e000 Unfrozen
ChildEBP RetAddr
0a09fb6c 779b06a0 ntdll!KiFastSystemCallRet
0a09fb70 772c77d4 ntdll!NtWaitForSingleObject+0xc
0a09fbe0 772c7742 kernel32!WaitForSingleObjectEx+0xbe
0a09fbf4 6d58f57d kernel32!WaitForSingleObject+0x12
0a09fc0c 6d586c92 mshtml!CDwnTaskExec::ThreadExec+0x127
0a09fc18 6d50dadc mshtml!CExecFT::ThreadProc+0x3c
0a09fc20 772c3833 mshtml!CExecFT::StaticThreadProc+0xd
0a09fc2c 7798a9bd kernel32!BaseThreadInitThunk+0xe
0a09fc6c 00000000 ntdll!_RtlUserThreadStart+0x23

  13  Id: 36ec.37f8 Suspend: 0 Teb: 7ff4b000 Unfrozen
ChildEBP RetAddr
0ad2fd80 779b00f0 ntdll!KiFastSystemCallRet
0ad2fd84 772a7948 ntdll!NtRemoveIoCompletion+0xc
0ad2fdb0 774baf2e kernel32!GetQueuedCompletionStatus+0x29
0ad2fdec 774bb067 rpcrt4!COMMON_ProcessCalls+0xb5
0ad2fe58 774bac4f rpcrt4!LOADABLE_TRANSPORT::ProcessIOEvents+0xef
0ad2fe64 774bacb9 rpcrt4!ProcessIOEventsWrapper+0xe
0ad2fe88 774bad03 rpcrt4!BaseCachedThreadRoutine+0x5c
0ad2fe94 772c3833 rpcrt4!ThreadStartRoutine+0x1e
0ad2fea0 7798a9bd kernel32!BaseThreadInitThunk+0xe
0ad2fee0 00000000 ntdll!_RtlUserThreadStart+0x23
```

Note: We see that many threads have **clr** module on their stack traces. We also notice that there is an exception on the the main thread no. 0. We set exception context and see the invalid pointer access violation during garbage collection process:

```
0:000> kv
ChildEBP RetAddr  Args to Child
0031adb0 779b06a0 772c77d4 000006b0 00000000 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
0031adb4 772c77d4 000006b0 00000000 0031adfc ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
0031ae24 772c7742 000006b0 00004e20 00000000 kernel32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
0031ae38 6c395816 000006b0 00004e20 3cd5e26d kernel32!WaitForSingleObject+0x12 (FPO: [Non-Fpo])
0031ae68 6c395eb1 000006b0 00004e20 3cd5ff21 clr!ClrWaitForSingleObject+0x24 (FPO: [Non-Fpo])
0031b324 6c398c9a 000005cc 000006b0 00000780 clr!RunWatson+0x1e3 (FPO: [Non-Fpo])
0031ba50 6c3994c6 0031c8e8 00000002 0053bc78 clr!DoFaultReportWorker+0xbd4 (FPO: [Non-Fpo])
0031ba94 6c3e6769 0031c8e8 00000002 3cd5f6ed clr!DoFaultReport+0x146 (FPO: [Non-Fpo])
0031bae8 6c3e075c 0053bc78 00000002 00000002 clr!WatsonLastChance+0x191 (FPO: [Non-Fpo])
0031c4d0 6c3e0c36 80131506 6c3e209b 00000000 clr!EEPolicy::LogFatalError+0x523 (FPO: [Non-Fpo])
0031c81c 6c3e20a6 80131506 6c3e209b 00000000 clr!EEPolicy::HandleFatalError+0x105 (FPO: [Non-Fpo])
0031c840 6c23cad6 0053bc78 3cd58471 00004000 clr!CLRVectoredExceptionHandlerPhase3+0xaf (FPO: [Non-Fpo])
0031c874 6c23cd5f 0031c8e8 3cd584a1 00000000 clr!CLRVectoredExceptionHandlerPhase2+0x20 (FPO: [Non-Fpo])
0031c8a4 6c225b1f 0031c8e8 3cd584d5 00538be8 clr!CLRVectoredExceptionHandler+0xba (FPO: [Non-Fpo])
0031c8d0 7795c41b 0031c8e8 0031c994 0031c994 clr!CLRVectoredExceptionHandlerShim+0xa8 (FPO: [Non-Fpo])
0031c8f8 77972b3a 00000000 00538be0 77a154b8 ntdll!RtlpCallVectoredHandlers+0x57 (FPO: [Non-Fpo])
0031c90c 77972960 0031c994 0031c9b0 0064006c ntdll!RtlCallVectoredExceptionHandlers+0x15 (FPO: [Non-Fpo])
0031c97c 779b0e97 0031c994 0031c9b0 0031c994 ntdll!RtlDispatchException+0x19 (FPO: [Non-Fpo])
0031c97c 6c421562 0031c994 0031c9b0 0031c994 ntdll!KiUserExceptionDispatcher+0xf (FPO: [2,0,0]) (CONTEXT @ 0031c9b0)
0031cc7c 6c22bf56 09823e1c 09823e24 09823e28 clr!MethodTable::GetLoaderAllocatorObjectForGC+0x15 (FPO: [0,0,4])
0031ccbc 6c22be41 0981f024 0296c50c 6b676c1c clr!WKS::gc_heap::mark_object_simple1+0x3c0 (FPO: [Non-Fpo])
0031cce8 6c22b9db 059921f8 6c228410 6c228115 clr!WKS::gc_heap::mark_object_simple+0x209 (FPO: [Non-Fpo])
0031cd64 6c2282c6 6c228410 00000000 00000004 clr!WKS::gc_heap::mark_through_cards_for_large_objects+0x36c (FPO: [Non-
Fpo])
0031cda4 6c2273c5 00000001 00000000 00000004 clr!WKS::gc_heap::mark_phase+0x299 (FPO: [Non-Fpo])
0031cdcc 6c227972 3cd58255 00000000 6c76c3a8 clr!WKS::gc_heap::gc1+0x134 (FPO: [Non-Fpo])
0031ce50 6c22771f 00000000 00000000 0000001c clr!WKS::gc_heap::garbage_collect+0x3ae (FPO: [Non-Fpo])
0031ce7c 6c22878a 00000000 00000001 0000001c clr!WKS::GCHeap::GarbageCollectGeneration+0x17b (FPO: [Non-Fpo])
0031cea0 6c226b82 0053bcc0 0000001c 00000000 clr!WKS::gc_heap::try_allocate_more_space+0x162 (FPO: [Non-Fpo])
0031ceb4 6c226e65 0053bcc0 0000001c 00000000 clr!WKS::gc_heap::allocate_more_space+0x13 (FPO: [Non-Fpo])
0031ced4 6c1cc953 0053bcc0 0000001c 00000002 clr!WKS::GCHeap::Alloc+0x3d (FPO: [Non-Fpo])
0031cef0 6c18ecd8 0000001c 00000000 00080000 clr!Alloc+0x8d (FPO: [Non-Fpo])
0031cf30 6c18edb6 6b6c4cd8 3cd583d5 099bd20c clr!FastAllocateObject+0x38 (FPO: [Non-Fpo])
0031cfd0 6b65665e 0031d774 0031dfa4 059f4c92 clr!JIT_NewFast+0xc8 (FPO: [Non-Fpo])
0031e124 05a01798 0031e6bc 00000000 00000042 mscorlib_ni+0x2b665e
WARNING: Frame IP not in any known module. Following frames may be wrong.
0031e834 6c20ff88 099bc5ac 097fab1c 097fab1c 0x5a01798
0031e840 097fab1c 099bc4f0 00000000 099bc590 clr!LayoutDestroyNative+0x3d (FPO: [Non-Fpo])
0031e84c 099bc590 00000000 099bac00 099bc580 0x97fab1c
00000000 00000000 00000000 00000000 00000000 0x99bc590

0:000> .cxr 0031c9b0
eax=0008f36f ebx=80000000 ecx=68006300 edx=2db1a755 esi=0064006c edi=0064006d
eip=6c421562 esp=0031cc7c ebp=0031ccbc iopl=0         nv up ei pl nz na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010206
clr!MethodTable::GetLoaderAllocatorObjectForGC+0x15:
6c421562 83b82c06000009  cmp     dword ptr [eax+62Ch],9 ds:0023:0008f99b=????????
```

```
0:000> kL
  *** Stack trace for last set context - .thread/.cxr resets it
ChildEBP RetAddr
0031cc7c 6c22bf56 clr!MethodTable::GetLoaderAllocatorObjectForGC+0x15
0031ccbc 6c22be41 clr!WKS::gc_heap::mark_object_simple1+0x3c0
0031cce8 6c22b9db clr!WKS::gc_heap::mark_object_simple+0x209
0031cd64 6c2282c6 clr!WKS::gc_heap::mark_through_cards_for_large_objects+0x36c
0031cda4 6c2273c5 clr!WKS::gc_heap::mark_phase+0x299
0031cdcc 6c227972 clr!WKS::gc_heap::gc1+0x134
0031ce50 6c22771f clr!WKS::gc_heap::garbage_collect+0x3ae
0031ce7c 6c22878a clr!WKS::GCHeap::GarbageCollectGeneration+0x17b
0031cea0 6c226b82 clr!WKS::gc_heap::try_allocate_more_space+0x162
0031ceb4 6c226e65 clr!WKS::gc_heap::allocate_more_space+0x13
0031ced4 6c1cc953 clr!WKS::GCHeap::Alloc+0x3d
0031cef0 6c18ecd8 clr!Alloc+0x8d
0031cf30 6c18edb6 clr!FastAllocateObject+0x38
0031cfd0 6b65665e clr!JIT_NewFast+0xc8
0031e124 05a01798 mscorlib_ni+0x2b665e
WARNING: Frame IP not in any known module. Following frames may be wrong.
0031e834 6c20ff88 0x5a01798
0031e840 097fab1c clr!LayoutDestroyNative+0x3d
0031e84c 099bc590 0x97fab1c
00000000 00000000 0x99bc590
```

7. To verify the managed heap (**!VerifyHeap** SOS extension command) we load the appropriate SOS extension after checking that it is not loaded and verifying **clr** module version:

```
0:000> .chain
Extension DLL search Path:
[...]
Extension DLL chain:
    dbghelp: image 6.12.0002.633, API 6.1.6, built Mon Feb 01 20:08:26 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\dbghelp.dll]
    ext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:31 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\winext\ext.dll]
    exts: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:24 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\WINXP\exts.dll]
    uext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:23 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\winext\uext.dll]
    ntsdexts: image 6.1.7650.0, API 1.0.0, built Mon Feb 01 20:08:08 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\WINXP\ntsdexts.dll]
```

```
0:000> lmv m clr
start    end        module name
6af20000 6b58f000   clr        (pdb symbols)
c:\mss\clr.pdb\C58C9AF63E5D49A8BE0DBA9C5E0093BE2\clr.pdb
    Loaded symbol image file: clr.dll
    Image path: C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.dll
    Image name: clr.dll
    Timestamp:        Thu Mar 18 07:44:47 2010 (4BA1D9EF)
    CheckSum:         00671FC0
    ImageSize:        0066F000
    File version:     4.0.30319.1
    Product version:  4.0.30319.1
    File flags:       8 (Mask 3F) Private
    File OS:          4 Unknown Win32
    File type:        2.0 Dll
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      Microsoft Corporation
    ProductName:      Microsoft® .NET Framework
    InternalName:     clr.dll
    OriginalFilename: clr.dll
    ProductVersion:   4.0.30319.1
    FileVersion:      4.0.30319.1 (RTMRel.030319-0100)
    PrivateBuild:     DDBLD766
    FileDescription:  Microsoft .NET Runtime Common Language Runtime - WorkStation
    LegalCopyright:   © Microsoft Corporation.  All rights reserved.
    Comments:         Flavor=Retail

0:000> .load C:\ANETMDA-Dumps\32-bit\Microsoft.NET\Framework\v4.0.30319\sos

0:000> .chain
Extension DLL search Path:
[...]
Extension DLL chain:
    C:\ANETMDA-Dumps\32-bit\Microsoft.NET\Framework\v4.0.30319\sos: image 4.0.30319.1, API
1.0.0, built Thu Mar 18 08:09:41 2010
        [path: C:\ANETMDA-Dumps\32-bit\Microsoft.NET\Framework\v4.0.30319\sos.dll]
    dbghelp: image 6.12.0002.633, API 6.1.6, built Mon Feb 01 20:08:26 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\dbghelp.dll]
    ext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:31 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\winext\ext.dll]
    exts: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:24 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\WINXP\exts.dll]
    uext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:08:23 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\winext\uext.dll]
    ntsdexts: image 6.1.7650.0, API 1.0.0, built Mon Feb 01 20:08:08 2010
        [path: C:\Program Files (x86)\Debugging Tools for Windows (x86)\WINXP\ntsdexts.dll]

0:000> !VerifyHeap
-verify will only produce output if there are errors in the heap
object 0981f024: does not have valid MT
curr_object:      0981f024
Last good object: 0981f010
----------------
```

8. We now check consecutive last good and invalid objects that according to source code should have values 499 and 500:

```
0:000> !DumpObj 0981f010
Name:        System.String
MethodTable: 6b6bf9ac
EEClass:     6b3f8bb0
Size:        20(0x14) bytes
File:
C:\Windows\Microsoft.Net\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll
String:      499
Fields:
      MT    Field   Offset                 Type VT     Attr    Value Name
6b6c2978  40000ed        4          System.Int32  1 instance        3 m_stringLength
6b6c1dc8  40000ee        8           System.Char  1 instance       34 m_firstChar
6b6bf9ac  40000ef        8         System.String  0   shared   static Empty
    >> Domain:Value  005317d0:01961228 05bf9120:01961228 <<

0:000> !DumpObj 0981f024
<Note: this object has an invalid CLASS field>
Invalid object
```

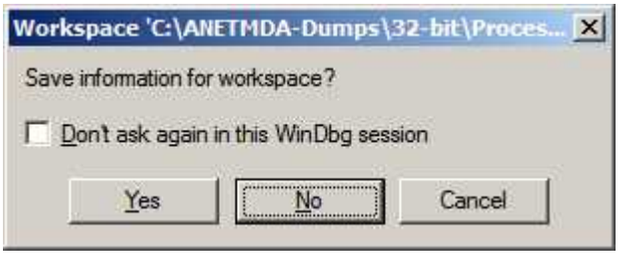
Note: If we check raw memory we would see the values but we also see that the beginning of the invalid object contains UNICODE string “bugs.dml” in reverse:

```
0:000> dc 0981f024
0981f024  0064006d 0073002e 00750067 00000062  m.d...s.g.u.b...
0981f034  00000000 6b6bf9ac 00000003 00300035  ......kk....5.0.
0981f044  00000030 00000000 05992205 0981f060  0........"..`...
0981f054  0981f024 000001f5 00000000 6b6bf9ad  $............kk
0981f064  00000003 00300035 00000031 00000000  ....5.0.1.......
0981f074  05992205 0981f088 0981f04c 000001f6  ."......L.......
0981f084  00000000 6b6bf9ad 00000003 00300035  ......kk....5.0.
0981f094  00000032 00000000 05992205 0981f0b0  2........"......
0:000> dc 0981f010
0981f010  6b6bf9ac 00000003 00390034 00000039  ..kk....4.9.9...
0981f020  006c0000 0064006d 0073002e 00750067  ..l.m.d...s.g.u.
0981f030  00000062 00000000 6b6bf9ac 00000003  b........kk....
0981f040  00300035 00000030 00000000 05992205  5.0.0........"..
0981f050  0981f060 0981f024 000001f5 00000000  `...$...........
0981f060  6b6bf9ad 00000003 00300035 00000031  ..kk....5.0.1...
0981f070  00000000 05992205 0981f088 0981f04c  ....."......L...
0981f080  000001f6 00000000 6b6bf9ad 00000003  ..........kk....
```

9. We close logging before exiting WinDbg:

```
0:000> .logclose
Closing open log file C:\ANETMDA-Dumps\32-bit\Processes\CLR4\LINQPadE.log
```

If presented with this dialog choose No:



Note: To avoid possible confusion and glitches we recommend to exit WinDbg after each exercise.

Exercise PN7 (x64)

- **Goal:** Learn how to find problem assemblies, modules, classes and methods, disassemble code, analyze CPU spikes
- **Patterns:** Stack Trace Collection; CLR Thread; Version-Specific Extension; Duplicate Extension; JIT Code; Spiking Thread; Annotated Disassembly
- **Commands:** !analyze -v -hang, !CLRStack, !IP2MD, !runaway, ~<>s, ~<>k, !U, !DumpMD, !DumpClass, !DumpMT, !DumpModule, !DumpAssembly, !DumpDomain
- \ANETMDA-Dumps\Exercise-PN7-Analysis-process-dump-LINQPadB-64-CLR4.pdf

© 2013 Software Diagnostics Services

Exercises PN7 and PN8 were modeled on Windows 7 x64 machine.

Exercise PN7: Analysis of an application process dump (LINQPadB, 64-bit, CLR 4)

Goal: Learn how to find problem assemblies, modules, classes and methods, disassemble code, analyze CPU spikes.

Patterns: Stack Trace Collection; CLR Thread; Version-Specific Extension; Duplicate Extension; JIT Code; Spiking Thread; Annotated Disassembly.

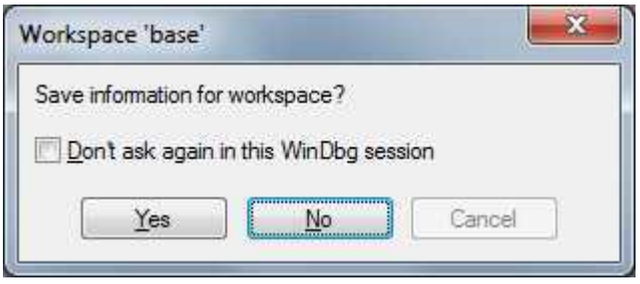
Commands: !analyze -v -hang, !CLRStack, !IP2MD, !runaway, ~<>s, ~<>k, !U, !DumpMD, !DumpClass, !DumpMT, !DumpModule, !DumpAssembly, !DumpDomain

1. Download and install the latest version of 64-bit Debugging Tools for Windows. You can get download links from www.windbg.org or download the package at www.patterndiagnostics.com/Training/ANETMDA/dbg_amd64.msi. In this and the next exercises, we use the latter version.

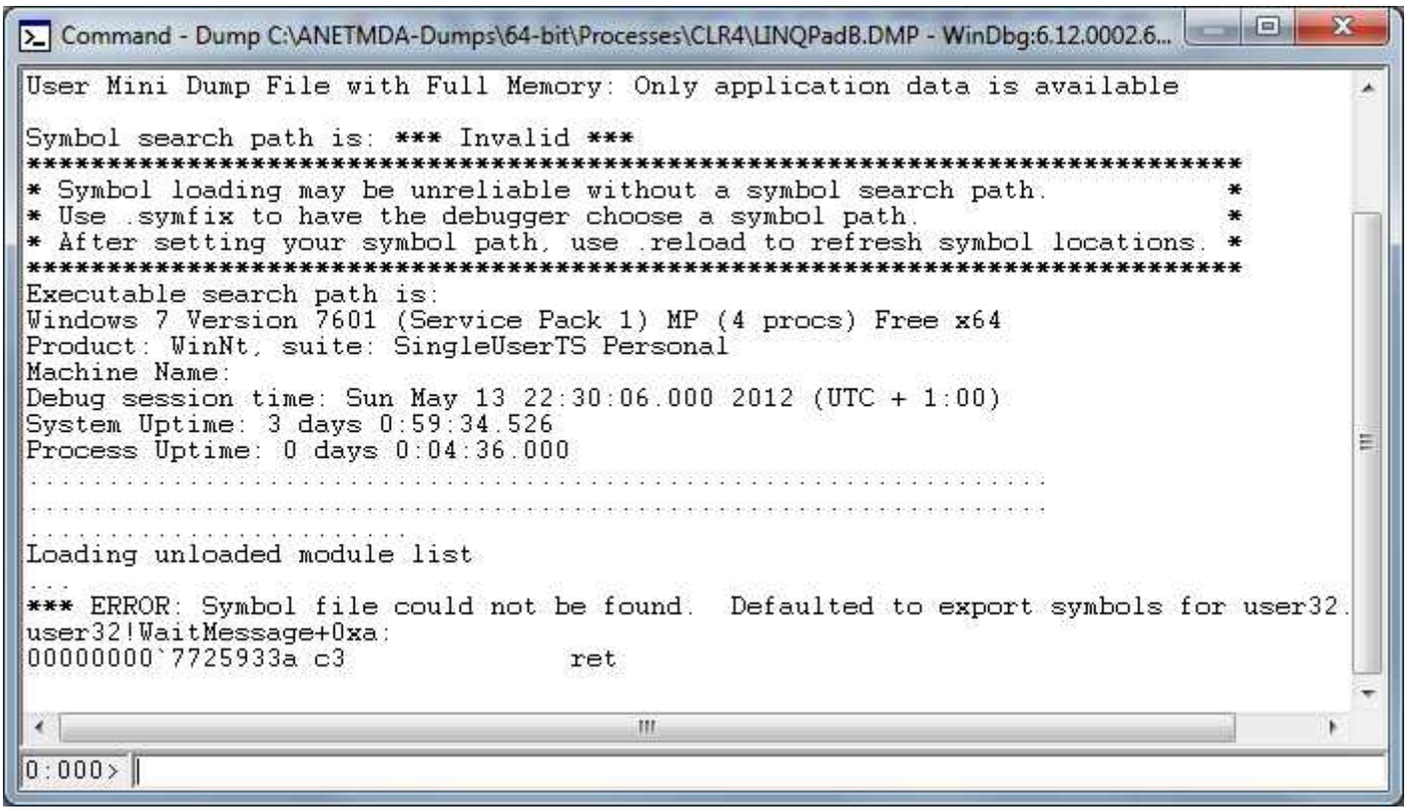
2. Launch WinDbg from Debugging Tools for Windows (x64 version).

3. Open \ANETMDA-Dumps\64-bit\Processes\CLR4\LINQPadB.DMP

4. If you are presented with this dialog say No:



5. We get the dump file loaded:



6. Open a log file using **.logopen** command and load symbols (**.symfix** and **.reload** commands):

```
0:000> .logopen C:\ANETMDA-Dumps\64-bit\Processes\CLR4\LINQPadBx64.log
Opened log file 'C:\ANETMDA-Dumps\64-bit\Processes\CLR4\LINQPadBx64.log'

0:000> .symfix c:\mss

0:000> .reload
.............................
```

Note: The results may be slightly different on your system if you have a different version of 64-bit .NET Framework 4 installed or you don't have any .NET Framework 4 installed.

7. Type ~***k** command to verify the correctness of all stack traces:

```
0:000> ~*k

.  0  Id: 1624.efc Suspend: 0 Teb: 000007ff`fffde000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`0014e0d8 000007fe`ed9119c2 user32!ZwUserWaitMessage+0xa
*** WARNING: Unable to verify checksum for System.Windows.Forms.ni.dll
00000000`0014e0e0 000007fe`ea179379 clr!DoNDirectCallWorker+0x62
00000000`0014e170 000007fe`ea178993 System_Windows_Forms_ni+0x349379
00000000`0014e3b0 000007fe`ea178321 System_Windows_Forms_ni+0x348993
00000000`0014e510 000007ff`00174a1a System_Windows_Forms_ni+0x348321
00000000`0014e5a0 000007ff`00171cb6 0x7ff`00174a1a
00000000`0014e830 000007ff`0017092c 0x7ff`00171cb6
00000000`0014ecc0 000007ff`00170509 0x7ff`0017092c
00000000`0014ed30 000007ff`001701bd 0x7ff`00170509
00000000`0014ed60 000007fe`ed9c90b4 0x7ff`001701bd
```

```
00000000`0014eda0 000007fe`ed9c91c9 clr!CallDescrWorker+0x84
00000000`0014edf0 000007fe`ed9c9245 clr!CallDescrWorkerWithHandler+0xa9
00000000`0014ee70 000007fe`eda331d1 clr!MethodDesc::CallDescr+0x2a1
00000000`0014f0a0 000007fe`eda3330c clr!ClassLoader::RunMain+0x228
00000000`0014f2f0 000007fe`eda330be clr!Assembly::ExecuteMainMethod+0xac
00000000`0014f5a0 000007fe`eda7f5c2 clr!SystemDomain::ExecuteMainMethod+0x452
00000000`0014fb50 000007fe`eda7f4df clr!ExecuteEXE+0x43
00000000`0014fbb0 000007fe`eda43835 clr!CorExeMainInternal+0xc4
00000000`0014fc20 000007fe`f7013309 clr!CorExeMain+0x15
00000000`0014fc60 000007fe`f7475b21 mscoreei!CorExeMain+0x41
00000000`0014fc90 00000000`7735652d mscoree!CorExeMain_Exported+0x57
00000000`0014fcc0 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`0014fcf0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

   1  Id: 1624.edc Suspend: 0 Teb: 000007ff`fffdc000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`028dfa58 000007fe`fdcd1420 ntdll!ZwWaitForMultipleObjects+0xa
00000000`028dfa60 00000000`77351220 KERNELBASE!WaitForMultipleObjectsEx+0xe8
00000000`028dfb60 000007fe`eda3d516 kernel32!WaitForMultipleObjects+0xb0
00000000`028dfbf0 000007fe`eda3d44b clr!DebuggerRCThread::MainLoop+0xba
00000000`028dfca0 000007fe`eda3d351 clr!DebuggerRCThread::ThreadProc+0xe4
00000000`028dfd00 00000000`7735652d clr!DebuggerRCThread::ThreadProcStatic+0x4d
00000000`028dfd60 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`028dfd90 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

   2  Id: 1624.ab4 Suspend: 0 Teb: 000007ff`fffda000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`1b0ef908 000007fe`fdcd1420 ntdll!ZwWaitForMultipleObjects+0xa
00000000`1b0ef910 00000000`77351220 KERNELBASE!WaitForMultipleObjectsEx+0xe8
00000000`1b0efa10 000007fe`edb390df kernel32!WaitForMultipleObjects+0xb0
00000000`1b0efaa0 000007fe`edb393f3 clr!WKS::WaitForFinalizerEvent+0xcb
00000000`1b0efad0 000007fe`ed9d8fd2 clr!WKS::GCHeap::FinalizerThreadWorker+0x33
00000000`1b0efb00 000007fe`ed9d8f67 clr!QueueUserWorkItemManagedCallback+0x92
00000000`1b0efb40 000007fe`ed9d8ed4 clr!EEUtf8HashTableHelper::Hash+0xe8
00000000`1b0efc40 000007fe`eda7f36e clr!IncCantStopCount+0xbd
00000000`1b0efce0 000007fe`eda7f7ff clr!ManagedThreadBase_NoADTransition+0x3f
00000000`1b0efd40 000007fe`eda88906 clr!WKS::GCHeap::FinalizerThreadStart+0x93
00000000`1b0efd80 00000000`7735652d clr!Thread::intermediateThreadProc+0x7d
00000000`1b0efe40 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`1b0efe70 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

   3  Id: 1624.630 Suspend: 0 Teb: 000007ff`fffd8000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`1b60f7b8 00000000`777db007 ntdll!ZwWaitForMultipleObjects+0xa
00000000`1b60f7c0 00000000`7735652d ntdll!TppWaiterpThread+0x14d
00000000`1b60fa60 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`1b60fa90 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

   4  Id: 1624.1664 Suspend: 0 Teb: 000007ff`fffd6000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`1bb3eb98 000007fe`fdcdc3ff ntdll!NtFsControlFile+0xa
00000000`1bb3eba0 000007fe`ed9117c7 KERNELBASE!ConnectNamedPipe+0x6f
*** WARNING: Unable to verify checksum for System.Core.ni.dll
00000000`1bb3ec10 000007fe`eb597790 clr!DoNDirectCall__PatchGetThreadCall+0x7b
00000000`1bb3ecb0 000007fe`eb6a1dc3 System_Core_ni+0x467790
00000000`1bb3ed90 000007ff`00173494 System_Core_ni+0x571dc3
*** WARNING: Unable to verify checksum for mscorlib.ni.dll
00000000`1bb3edd0 000007fe`eca017fc 0x7ff`00173494
00000000`1bb3ef00 000007fe`eca0170b mscorlib_ni+0x3717fc
00000000`1bb3ef60 000007fe`eca96fed mscorlib_ni+0x37170b
```

```
00000000`1bb3efb0 000007fe`ed9c90b4 mscorlib_ni+0x406fed
00000000`1bb3f000 000007fe`ed9c91c9 clr!CallDescrWorker+0x84
00000000`1bb3f050 000007fe`ed9c9245 clr!CallDescrWorkerWithHandler+0xa9
00000000`1bb3f0d0 000007fe`ed9c9718 clr!MethodDesc::CallDescr+0x2a1
00000000`1bb3f300 000007fe`eda20618 clr!MethodDesc::CallTargetWorker+0x44
00000000`1bb3f340 000007fe`ed9d8fd2 clr!ThreadNative::KickOffThread_Worker+0x148
00000000`1bb3f660 000007fe`ed9d8f67 clr!QueueUserWorkItemManagedCallback+0x92
00000000`1bb3f6a0 000007fe`ed9d8ed4 clr!EEUtf8HashTableHelper::Hash+0xe8
00000000`1bb3f7a0 000007fe`ed9d902b clr!IncCantStopCount+0xbd
00000000`1bb3f840 000007fe`eda20468 clr!ThreadpoolMgr::TimerThreadStart+0x9f
00000000`1bb3f8a0 000007fe`eda88906 clr!ThreadNative::KickOffThread+0xc0
00000000`1bb3f980 00000000`7735652d clr!Thread::intermediateThreadProc+0x7d
00000000`1bb3fac0 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`1bb3faf0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

   5  Id: 1624.13e4 Suspend: 0 Teb: 000007ff`fffd4000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`1c05f768 000007fe`fdcd1420 ntdll!ZwWaitForMultipleObjects+0xa
00000000`1c05f770 00000000`77362cf3 KERNELBASE!WaitForMultipleObjectsEx+0xe8
00000000`1c05f870 00000000`77258f7d kernel32!WaitForMultipleObjectsExImplementation+0xb3
00000000`1c05f900 00000000`772562b2 user32!RealMsgWaitForMultipleObjectsEx+0x12a
00000000`1c05f9a0 00000000`772562e0 user32!MsgWaitForMultipleObjectsEx+0x46
00000000`1c05f9e0 000007fe`fb302c6c user32!MsgWaitForMultipleObjects+0x20
00000000`1c05fa20 000007fe`fb302ad0 GdiPlus!BackgroundThreadProc+0x68
00000000`1c05fa90 00000000`7735652d GdiPlus!DllRefCountSafeThreadThunk+0x18
00000000`1c05fac0 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`1c05faf0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

   6  Id: 1624.da0 Suspend: 0 Teb: 000007ff`ffefa000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`1d50fa58 000007fe`fdcd10dc ntdll!ZwWaitForSingleObject+0xa
00000000`1d50fa60 000007fe`fa951fae KERNELBASE!WaitForSingleObjectEx+0x79
00000000`1d50fb00 00000000`7735652d rasman!RasmanServiceMonitorThread+0x171
00000000`1d50fb90 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`1d50fbc0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

   7  Id: 1624.4e4 Suspend: 0 Teb: 000007ff`ffef6000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`1de6f4f8 00000000`777dfe0b ntdll!NtWaitForWorkViaWorkerFactory+0xa
00000000`1de6f500 00000000`7735652d ntdll!TppWorkerThread+0x2c9
00000000`1de6f800 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`1de6f830 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

   8  Id: 1624.162c Suspend: 0 Teb: 000007ff`ffef2000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`1e06f7b8 00000000`777dfe0b ntdll!NtWaitForWorkViaWorkerFactory+0xa
00000000`1e06f7c0 00000000`7735652d ntdll!TppWorkerThread+0x2c9
00000000`1e06fac0 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`1e06faf0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

   9  Id: 1624.3d4 Suspend: 0 Teb: 000007ff`ffeee000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`1e95e748 000007fe`fdcd1420 ntdll!ZwWaitForMultipleObjects+0xa
00000000`1e95e750 00000000`77362cf3 KERNELBASE!WaitForMultipleObjectsEx+0xe8
00000000`1e95e850 000007fe`eda907a5 kernel32!WaitForMultipleObjectsExImplementation+0xb3
00000000`1e95e8e0 000007fe`eda90582 clr!WaitForMultipleObjectsEx_SO_TOLERANT+0x91
00000000`1e95e970 000007fe`eda9040d clr!Thread::DoAppropriateAptStateWait+0x56
00000000`1e95e9b0 000007fe`eda90503 clr!Thread::DoAppropriateWaitWorker+0x1b1
00000000`1e95eab0 000007fe`eda906fa clr!Thread::DoAppropriateWait+0x73
00000000`1e95eb30 000007fe`eda23f4f clr!CLREvent::WaitEx+0xc1
```

```
00000000`1e95ebd0 000007fe`eda23ebc clr!Thread::Block+0x2f
00000000`1e95ec00 000007fe`eda23c94 clr!SyncBlock::Wait+0x15c
00000000`1e95ed40 000007fe`ed0bcfee clr!ObjectNative::WaitTimeout+0x124
00000000`1e95eef0 000007ff`0017c821 mscorlib_ni+0xa2cfee
00000000`1e95ef30 000007fe`eca017fc 0x7ff`0017c821
00000000`1e95f0a0 000007fe`eca0170b mscorlib_ni+0x3717fc
00000000`1e95f100 000007fe`eca96fed mscorlib_ni+0x37170b
00000000`1e95f150 000007fe`ed9c90b4 mscorlib_ni+0x406fed
00000000`1e95f1a0 000007fe`ed9c91c9 clr!CallDescrWorker+0x84
00000000`1e95f1f0 000007fe`ed9c9245 clr!CallDescrWorkerWithHandler+0xa9
00000000`1e95f270 000007fe`ed9c9718 clr!MethodDesc::CallDescr+0x2a1
00000000`1e95f4a0 000007fe`eda20618 clr!MethodDesc::CallTargetWorker+0x44
00000000`1e95f4e0 000007fe`ed9d8fd2 clr!ThreadNative::KickOffThread_Worker+0x148
00000000`1e95f800 000007fe`ed9d8f67 clr!QueueUserWorkItemManagedCallback+0x92
00000000`1e95f840 000007fe`ed9d8ed4 clr!EEUtf8HashTableHelper::Hash+0xe8
00000000`1e95f940 000007fe`ed9d902b clr!IncCantStopCount+0xbd
00000000`1e95f9e0 000007fe`eda20468 clr!ThreadpoolMgr::TimerThreadStart+0x9f
00000000`1e95fa40 000007fe`eda88906 clr!ThreadNative::KickOffThread+0xc0
00000000`1e95fb20 00000000`7735652d clr!Thread::intermediateThreadProc+0x7d
00000000`1e95fe60 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`1e95fe90 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

  10  Id: 1624.15f8 Suspend: 0 Teb: 000007ff`ffefc000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`1e72f4d8 000007fe`fdcd10dc ntdll!ZwWaitForSingleObject+0xa
00000000`1e72f4e0 000007fe`ed9c77e7 KERNELBASE!WaitForSingleObjectEx+0x79
00000000`1e72f580 000007fe`ed9c7790 clr!CLREvent::WaitEx+0x170
00000000`1e72f5c0 000007fe`ed9c764b clr!CLREvent::WaitEx+0xf8
00000000`1e72f620 000007fe`eda1bbd8 clr!CLREvent::WaitEx+0x5e
00000000`1e72f6c0 000007fe`eda88906 clr!AppDomain::ADUnloadThreadStart+0x144
00000000`1e72f800 00000000`7735652d clr!Thread::intermediateThreadProc+0x7d
00000000`1e72fc40 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`1e72fc70 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

  11  Id: 1624.124c Suspend: 0 Teb: 000007ff`ffeea000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`1ebefa48 000007fe`fdcd1203 ntdll!NtDelayExecution+0xa
00000000`1ebefa50 000007fe`ed9a8ed0 KERNELBASE!SleepEx+0xab
00000000`1ebefaf0 000007fe`ed9a8e8a clr!ThreadpoolMgr::TimerThreadFire+0x44
00000000`1ebefb90 00000000`7735652d clr!ThreadpoolMgr::TimerThreadStart+0x6e
00000000`1ebefbc0 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`1ebefbf0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

  12  Id: 1624.1428 Suspend: 0 Teb: 000007ff`ffeec000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`1f17f998 000007fe`fdcd1203 ntdll!NtDelayExecution+0xa
00000000`1f17f9a0 000007fe`ff5201d0 KERNELBASE!SleepEx+0xab
00000000`1f17fa40 000007fe`ff520106 ole32!CROIDTable::WorkerThreadLoop+0x10
[d:\w7rtm\com\ole32\com\dcomrem\refcache.cxx @ 1345]
00000000`1f17fa70 000007fe`ff520182 ole32!CRpcThread::WorkerLoop+0x1e
[d:\w7rtm\com\ole32\com\dcomrem\threads.cxx @ 257]
00000000`1f17fab0 00000000`7735652d ole32!CRpcThreadCache::RpcWorkerThreadEntry+0x1a
[d:\w7rtm\com\ole32\com\dcomrem\threads.cxx @ 63]
00000000`1f17fae0 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`1f17fb10 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
  13  Id: 1624.c50 Suspend: 0 Teb: 000007ff`ffee6000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`2027f468 000007fe`fdcd169d ntdll!NtRemoveIoCompletion+0xa
00000000`2027f470 00000000`7734a4e1 KERNELBASE!GetQueuedCompletionStatus+0x39
00000000`2027f4d0 000007fe`ed9bda57 kernel32!GetQueuedCompletionStatusStub+0x11
00000000`2027f510 000007fe`eda88906 clr!ThreadpoolMgr::CompletionPortThreadStart+0x113
00000000`2027f5c0 00000000`7735652d clr!Thread::intermediateThreadProc+0x7d
00000000`2027fa80 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`2027fab0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

  14  Id: 1624.12c0 Suspend: 0 Teb: 000007ff`ffee0000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`20a9f4e8 00000000`777dfe0b ntdll!NtWaitForWorkViaWorkerFactory+0xa
00000000`20a9f4f0 00000000`7735652d ntdll!TppWorkerThread+0x2c9
00000000`20a9f7f0 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`20a9f820 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

  15  Id: 1624.16ec Suspend: 0 Teb: 000007ff`ffeda000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`2230fd88 00000000`77259e9e user32!NtUserGetMessage+0xa
00000000`2230fd90 000007fe`fe4c6ad8 user32!GetMessageW+0x34
00000000`2230fdc0 000007fe`ff1bc71e shell32!MessagePumpThreadProc+0x3e
00000000`2230fe30 00000000`7735652d shlwapi!WrapperThreadProc+0x19b
00000000`2230ff30 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`2230ff60 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

  16  Id: 1624.e5c Suspend: 0 Teb: 000007ff`ffefe000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`2070f358 000007fe`fdcd10dc ntdll!ZwWaitForSingleObject+0xa
00000000`2070f360 000007fe`ed9b870e KERNELBASE!WaitForSingleObjectEx+0x79
00000000`2070f400 000007fe`ed9b8ad7 clr!CLRSemaphore::Wait+0xaa
00000000`2070f4c0 000007fe`ed9b8c60 clr!ThreadpoolMgr::UnfairSemaphore::Wait+0x140
00000000`2070f500 000007fe`eda8a5a3 clr!ThreadpoolMgr::NewWorkerThreadStart+0x2a7
00000000`2070f5a0 000007fe`eda88906 clr!ThreadpoolMgr::WorkerThreadStart+0x3b
00000000`2070f640 00000000`7735652d clr!Thread::intermediateThreadProc+0x7d
00000000`2070fb80 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`2070fbb0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

  17  Id: 1624.115c Suspend: 0 Teb: 000007ff`ffed2000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`2274f858 000007fe`fdcd10dc ntdll!ZwWaitForSingleObject+0xa
00000000`2274f860 00000000`665519a0 KERNELBASE!WaitForSingleObjectEx+0x79
00000000`2274f900 00000000`6654fe45 mshtml!CDwnTaskExec::ThreadExec+0x387
00000000`2274f990 00000000`7735652d mshtml!CExecFT::ThreadProc+0x57
00000000`2274f9c0 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`2274f9f0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

  18  Id: 1624.156c Suspend: 0 Teb: 000007ff`ffecc000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`22c8fb18 000007fe`fdcd10dc ntdll!ZwWaitForSingleObject+0xa
00000000`22c8fb20 00000000`6655938c KERNELBASE!WaitForSingleObjectEx+0x79
00000000`22c8fbc0 00000000`6654fe45 mshtml!CTimerMan::ThreadExec+0x17c
00000000`22c8fc10 00000000`7735652d mshtml!CExecFT::ThreadProc+0x57
00000000`22c8fc40 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`22c8fc70 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
  19  Id: 1624.c74 Suspend: 0 Teb: 000007ff`ffeca000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`2060ce70 000007ff`008f48fe 0x7ff`008f49dc
00000000`2060ceb0 000007fe`ed9c90b4 0x7ff`008f48fe
00000000`2060cef0 000007fe`ed9c91c9 clr!CallDescrWorker+0x84
00000000`2060cf40 000007fe`ed9c9245 clr!CallDescrWorkerWithHandler+0xa9
00000000`2060cfc0 000007fe`eda93ab9 clr!MethodDesc::CallDescr+0x2a1
00000000`2060d1f0 000007fe`eda9397f clr!CallWithValueTypes_RetArgSlotWrapper+0x91
00000000`2060d480 000007fe`eda93638 clr!InvokeImpl+0x2e6
00000000`2060d910 000007fe`eca05c98 clr!RuntimeMethodHandle::InvokeMethodFast+0x1d8
00000000`2060db00 000007fe`eca0576c mscorlib_ni+0x375c98
00000000`2060dbf0 000007fe`eca502e6 mscorlib_ni+0x37576c
00000000`2060dd30 000007fe`eca50313 mscorlib_ni+0x3c02e6
00000000`2060dd80 000007ff`008f4308 mscorlib_ni+0x3c0313
00000000`2060ddc0 000007ff`008f24c0 0x7ff`008f4308
00000000`2060dff0 000007ff`008f1e15 0x7ff`008f24c0
00000000`2060e270 000007ff`008f18ea 0x7ff`008f1e15
00000000`2060e3a0 000007fe`eca017fc 0x7ff`008f18ea
00000000`2060e400 000007fe`eca0170b mscorlib_ni+0x3717fc
00000000`2060e460 000007fe`eca96fed mscorlib_ni+0x37170b
00000000`2060e4b0 000007fe`ed9c90b4 mscorlib_ni+0x406fed
00000000`2060e500 000007fe`ed9c91c9 clr!CallDescrWorker+0x84
00000000`2060e550 000007fe`ed9c9245 clr!CallDescrWorkerWithHandler+0xa9
00000000`2060e5d0 000007fe`ed9c9718 clr!MethodDesc::CallDescr+0x2a1
00000000`2060e800 000007fe`eda20618 clr!MethodDesc::CallTargetWorker+0x44
00000000`2060e840 000007fe`ed9d8fd2 clr!ThreadNative::KickOffThread_Worker+0x148
00000000`2060eb60 000007fe`ed9d8f67 clr!QueueUserWorkItemManagedCallback+0x92
00000000`2060eba0 000007fe`ed9d8ed4 clr!EEUtf8HashTableHelper::Hash+0xe8
00000000`2060eca0 000007fe`ed9d91c4 clr!IncCantStopCount+0xbd
00000000`2060ed40 000007fe`edd1356a clr!CExecutionEngine::TLS_GetMasterSlotIndex+0x2d
00000000`2060ed70 000007fe`ed9d91f8 clr! ?? ::FNODOBFM::`string'+0xad77a
00000000`2060ef20 000007fe`ed9d8f67 clr!QueueUserWorkItemManagedCallback+0xc7
00000000`2060ef60 000007fe`ed9d8ed4 clr!EEUtf8HashTableHelper::Hash+0xe8
00000000`2060f060 000007fe`ed9d902b clr!IncCantStopCount+0xbd
00000000`2060f100 000007fe`eda20468 clr!ThreadpoolMgr::TimerThreadStart+0x9f
00000000`2060f160 000007fe`eda88906 clr!ThreadNative::KickOffThread+0xc0
00000000`2060f240 00000000`7735652d clr!Thread::intermediateThreadProc+0x7d
00000000`2060f980 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`2060f9b0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

  20  Id: 1624.165c Suspend: 0 Teb: 000007ff`ffece000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`21eedad8 000007fe`fdcd1420 ntdll!ZwWaitForMultipleObjects+0xa
00000000`21eedae0 00000000`77362cf3 KERNELBASE!WaitForMultipleObjectsEx+0xe8
00000000`21eedbe0 000007fe`eda907a5 kernel32!WaitForMultipleObjectsExImplementation+0xb3
00000000`21eedc70 000007fe`eda90582 clr!WaitForMultipleObjectsEx_SO_TOLERANT+0x91
00000000`21eedd00 000007fe`eda9040d clr!Thread::DoAppropriateAptStateWait+0x56
00000000`21eedd40 000007fe`eda90503 clr!Thread::DoAppropriateWaitWorker+0x1b1
00000000`21eede40 000007fe`edb0fb65 clr!Thread::DoAppropriateWait+0x73
00000000`21eedec0 000007fe`eca8c2f4 clr!WaitHandleNative::CorWaitOneNative+0x195
00000000`21eee110 000007ff`008f61a4 mscorlib_ni+0x3fc2f4
00000000`21eee150 000007fe`eca017fc 0x7ff`008f61a4
00000000`21eee1f0 000007fe`eca0170b mscorlib_ni+0x3717fc
00000000`21eee250 000007fe`eca96fed mscorlib_ni+0x37170b
00000000`21eee2a0 000007fe`ed9c90b4 mscorlib_ni+0x406fed
00000000`21eee2f0 000007fe`ed9c91c9 clr!CallDescrWorker+0x84
00000000`21eee340 000007fe`ed9c9245 clr!CallDescrWorkerWithHandler+0xa9
00000000`21eee3c0 000007fe`ed9c9718 clr!MethodDesc::CallDescr+0x2a1
00000000`21eee5f0 000007fe`eda20618 clr!MethodDesc::CallTargetWorker+0x44
00000000`21eee630 000007fe`ed9d8fd2 clr!ThreadNative::KickOffThread_Worker+0x148
```

```
00000000`21eee950 000007fe`ed9d8f67 clr!QueueUserWorkItemManagedCallback+0x92
00000000`21eee990 000007fe`ed9d8ed4 clr!EEUtf8HashTableHelper::Hash+0xe8
00000000`21eeea90 000007fe`ed9d91c4 clr!IncCantStopCount+0xbd
00000000`21eeeb30 000007fe`edd1356a clr!CExecutionEngine::TLS_GetMasterSlotIndex+0x2d
00000000`21eeeb60 000007fe`ed9d91f8 clr! ?? ::FNODOBFM::`string'+0xad77a
00000000`21eeed10 000007fe`ed9d8f67 clr!QueueUserWorkItemManagedCallback+0xc7
00000000`21eeed50 000007fe`ed9d8ed4 clr!EEUtf8HashTableHelper::Hash+0xe8
00000000`21eeee50 000007fe`ed9d902b clr!IncCantStopCount+0xbd
00000000`21eeeef0 000007fe`eda20468 clr!ThreadpoolMgr::TimerThreadStart+0x9f
00000000`21eeef50 000007fe`eda88906 clr!ThreadNative::KickOffThread+0xc0
00000000`21eef030 00000000`7735652d clr!Thread::intermediateThreadProc+0x7d
00000000`21eef7f0 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`21eef820 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

  21  Id: 1624.c0c Suspend: 0 Teb: 000007ff`ffef8000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`2011f988 00000000`777dfe0b ntdll!NtWaitForWorkViaWorkerFactory+0xa
00000000`2011f990 00000000`7735652d ntdll!TppWorkerThread+0x2c9
00000000`2011fc90 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`2011fcc0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

  22  Id: 1624.4c8 Suspend: 0 Teb: 000007ff`ffef0000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`2082f8d8 00000000`777dfe0b ntdll!NtWaitForWorkViaWorkerFactory+0xa
00000000`2082f8e0 00000000`7735652d ntdll!TppWorkerThread+0x2c9
00000000`2082fbe0 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`2082fc10 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

Note: We see that half of all threads have **clr** module on their stack traces.

8. Now we load the appropriate SOS extension after checking that it is not loaded and verifying mscorwks module version:

```
0:000> .chain
Extension DLL search Path:
[...]
Extension DLL chain:
    dbghelp: image 6.12.0002.633, API 6.1.6, built Mon Feb 01 20:15:44 2010
        [path: C:\Program Files\Debugging Tools for Windows (x64)\dbghelp.dll]
    ext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:15:46 2010
        [path: C:\Program Files\Debugging Tools for Windows (x64)\winext\ext.dll]
    exts: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:15:38 2010
        [path: C:\Program Files\Debugging Tools for Windows (x64)\WINXP\exts.dll]
    uext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:15:36 2010
        [path: C:\Program Files\Debugging Tools for Windows (x64)\winext\uext.dll]
    ntsdexts: image 6.1.7650.0, API 1.0.0, built Mon Feb 01 20:15:18 2010
        [path: C:\Program Files\Debugging Tools for Windows (x64)\WINXP\ntsdexts.dll]
```

```
0:000> lmv m clr
start             end                 module name
000007fe`ed910000 000007fe`ee274000   clr        (pdb symbols)
c:\mss\clr.pdb\9AE088FF3C1D4CDC92FD4155F258998F2\clr.pdb
    Loaded symbol image file: clr.dll
    Image path: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll
    Image name: clr.dll
    Timestamp:        Mon Nov 21 06:57:42 2011 (4EC9F666)
    CheckSum:         00965983
    ImageSize:        00964000
    File version:     4.0.30319.261
    Product version:  4.0.30319.261
    File flags:       8 (Mask 3F) Private
    File OS:          4 Unknown Win32
    File type:        2.0 Dll
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      Microsoft Corporation
    ProductName:      Microsoft® .NET Framework
    InternalName:     clr.dll
    OriginalFilename: clr.dll
    ProductVersion:   4.0.30319.261
    FileVersion:      4.0.30319.261 (RTMGDR.030319-2600)
    PrivateBuild:     DDBLD208
    FileDescription:  Microsoft .NET Runtime Common Language Runtime - WorkStation
    LegalCopyright:   © Microsoft Corporation.  All rights reserved.
    Comments:         Flavor=Retail
```

Note: We see version **261**.

We load the SOS extension from \ANETMDA-Dumps\64-bit\Framework64\v4.0.30319 folder:

```
0:000> .load C:\ANETMDA-Dumps\64-bit\Framework64\v4.0.30319\sos

0:000> .chain
Extension DLL search Path:
[...]
Extension DLL chain:
    C:\ANETMDA-Dumps\64-bit\Framework64\v4.0.30319\sos: image 4.0.30319.261, API 1.0.0, built
Mon Nov 21 07:14:03 2011
        [path: C:\ANETMDA-Dumps\64-bit\Framework64\v4.0.30319\sos.dll]
    dbghelp: image 6.12.0002.633, API 6.1.6, built Mon Feb 01 20:15:44 2010
        [path: C:\Program Files\Debugging Tools for Windows (x64)\dbghelp.dll]
    ext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:15:46 2010
        [path: C:\Program Files\Debugging Tools for Windows (x64)\winext\ext.dll]
    exts: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:15:38 2010
        [path: C:\Program Files\Debugging Tools for Windows (x64)\WINXP\exts.dll]
    uext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:15:36 2010
        [path: C:\Program Files\Debugging Tools for Windows (x64)\winext\uext.dll]
    ntsdexts: image 6.1.7650.0, API 1.0.0, built Mon Feb 01 20:15:18 2010
        [path: C:\Program Files\Debugging Tools for Windows (x64)\WINXP\ntsdexts.dll]
```

9. We check if there are .NET exceptions on each thread:

```
0:000> ~*e !pe
There is no current managed exception on this thread
The current thread is unmanaged
There is no current managed exception on this thread
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
There is no current managed exception on this thread
There is no current managed exception on this thread
The current thread is unmanaged
There is no current managed exception on this thread
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
There is no current managed exception on this thread
There is no current managed exception on this thread
The current thread is unmanaged
The current thread is unmanaged
```

10. "The customer" reported one of application windows was unresponsive. We now try the default WinDbg analysis command with **-hang** switch:

/* start of WinDbg output */

```
0:000> !analyze -v -hang
*******************************************************************************
*                                                                             *
*                        Exception Analysis                                   *
*                                                                             *
*******************************************************************************

*** ERROR: Module load completed but symbols could not be loaded for LINQPad.exe
*** WARNING: Unable to verify checksum for System.ni.dll
The version of SOS does not match the version of CLR you are debugging.  Please
load the matching version of SOS for the version of CLR you are debugging.
CLR Version: 4.0.30319.261
SOS Version: 4.0.30319.18052
Failed to load data access DLL, 0x80004005
Verify that 1) you have a recent build of the debugger (6.2.14 or newer)
            2) the file mscordacwks.dll that matches your version of clr.dll is
               in the version directory or on the symbol path
            3) or, if you are debugging a dump file, verify that the file
               mscordacwks_<arch>_<arch>_<version>.dll is on your symbol path.
            4) you are debugging on supported cross platform architecture as
               the dump file. For example, an ARM dump file must be debugged
               on an X86 or an ARM machine; an AMD64 dump file must be
               debugged on an AMD64 machine.

You can also run the debugger command .cordll to control the debugger's
load of mscordacwks.dll.  .cordll -ve -u -l will do a verbose reload.
If that succeeds, the SOS command should work on retry.

If you are debugging a minidump, you need to make sure that your executable
path is pointing to clr.dll as well.
The version of SOS does not match the version of CLR you are debugging.  Please
load the matching version of SOS for the version of CLR you are debugging.
CLR Version: 4.0.30319.261
SOS Version: 4.0.30319.18052
```

```
Failed to load data access DLL, 0x80004005
Verify that 1) you have a recent build of the debugger (6.2.14 or newer)
            2) the file mscordacwks.dll that matches your version of clr.dll is
                in the version directory or on the symbol path
            3) or, if you are debugging a dump file, verify that the file
                mscordacwks_<arch>_<arch>_<version>.dll is on your symbol path.
            4) you are debugging on supported cross platform architecture as
                the dump file. For example, an ARM dump file must be debugged
                on an X86 or an ARM machine; an AMD64 dump file must be
                debugged on an AMD64 machine.

You can also run the debugger command .cordll to control the debugger's
load of mscordacwks.dll.  .cordll -ve -u -l will do a verbose reload.
If that succeeds, the SOS command should work on retry.

If you are debugging a minidump, you need to make sure that your executable
path is pointing to clr.dll as well.
GetPageUrlData failed, server returned HTTP status 404
URL requested: http://watson.microsoft.com/00000000.htm?Retriage=1

FAULTING_IP:
+a2baa20
00000000`00000000 ??              ???

EXCEPTION_RECORD:  ffffffffffffffff -- (.exr 0xffffffffffffffff)
ExceptionAddress: 0000000000000000
   ExceptionCode: 80000003 (Break instruction exception)
  ExceptionFlags: 00000000
NumberParameters: 0

FAULTING_THREAD:  0000000000000000

BUGCHECK_STR:  HANG

PROCESS_NAME:  LINQPad.exe

ERROR_CODE: (NTSTATUS) 0xcfffffff - <Unable to get error code text>

EXCEPTION_CODE: (NTSTATUS) 0xcfffffff - <Unable to get error code text>

MOD_LIST: <ANALYSIS/>

NTGLOBALFLAG:  0

APPLICATION_VERIFIER_FLAGS:  0

MANAGED_STACK: !dumpstack -EE
The version of SOS does not match the version of CLR you are debugging.  Please
load the matching version of SOS for the version of CLR you are debugging.
CLR Version: 4.0.30319.261
SOS Version: 4.0.30319.18052
Failed to load data access DLL, 0x80004005
Some functionality may be impaired
OS Thread Id: 0xefc (0)
Current frame:
Child-SP         RetAddr          Caller, Callee

DERIVED_WAIT_CHAIN:

Dl Eid Cid     WaitType
-- --- ------- -------------------------
   0   1624.efc Unknown

WAIT_CHAIN_COMMAND:  ~0s;k;;

BLOCKING_THREAD:  0000000000000efc

DEFAULT_BUCKET_ID:  APPLICATION_HANG_WRONG_SYMBOLS

PRIMARY_PROBLEM_CLASS:  APPLICATION_HANG_WRONG_SYMBOLS

LAST_CONTROL_TRANSFER:  from 000007feed9119c2 to 000000007725933a
```

```
STACK_TEXT:
00000000`0014e0d8 000007fe`ed9119c2 : 00000000`00000000 00000000`00000000 00000000`00967890 00000000`0014e308 :
user32!ZwUserWaitMessage+0xa
00000000`0014e0e0 000007fe`ea179379 : 00000000`028efc58 00000000`0014e308 00000000`00000113 000031c0`0f2c3c95 :
clr!DoNDirectCallWorker+0x62
00000000`0014e170 000007fe`ea178993 : 00000000`0291a408 00000000`00000001 00000000`ffffffff 00000000`00000000 :
System_Windows_Forms_ni+0x349379
00000000`0014e3b0 000007fe`ea178321 : 00000000`028efc58 00000000`ffffffff 00000000`0460c1e8 00000000`00000000 :
System_Windows_Forms_ni+0x348993
00000000`0014e510 000007ff`00174a1a : 00000000`028efc58 00000000`ffffffff 00000000`05f8d748 00000000`00000010 :
System_Windows_Forms_ni+0x348321
00000000`0014e5a0 000007ff`00171cb6 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 :
0x7ff`00174a1a
00000000`0014e830 000007ff`0017092c : 00000000`028ed470 00000000`00010000 00000000`028f68a4 00000000`00000efc :
0x7ff`00171cb6
00000000`0014ecc0 000007ff`00170509 : 00000000`028ed470 00000000`028f2b78 00000000`00000000 00000000`0000766f :
0x7ff`0017092c
00000000`0014ed30 000007ff`001701bd : 00000000`028ed470 00000000`028f2b78 00000000`00000000 00000000`0000766f :
0x7ff`00170509
00000000`0014ed60 000007fe`ed9c90b4 : 00000000`028ed470 00000000`0014efa0 00000000`0014ee00 000007fe`ed914db5 :
0x7ff`001701bd
00000000`0014eda0 000007fe`ed9c91c9 : 000007ff`000273e8 00000000`00000001 00000000`00000000 00000000`00000000 :
clr!CallDescrWorker+0x84
00000000`0014edf0 000007fe`ed9c9245 : 00000000`0014ef08 00000000`00000001 00000000`0014ef10 00000000`0014f0f0 :
clr!CallDescrWorkerWithHandler+0xa9
00000000`0014ee70 000007fe`eda331d1 : 00000000`00000000 00000000`0014f0f8 00000000`00000001 000007fe`ec691a32 :
clr!MethodDesc::CallDescr+0x2a1
00000000`0014f0a0 000007fe`eda3330c : 00000000`00967890 00000000`00967890 00000000`00000000 00000000`00000000 :
clr!ClassLoader::RunMain+0x228
00000000`0014f2f0 000007fe`eda330be : 00000000`0014f8f0 00000000`00000200 00000000`00974830 00000000`00000200 :
clr!Assembly::ExecuteMainMethod+0xac
00000000`0014f5a0 000007fe`eda7f5c2 : 00000000`00000000 00000000`00310000 00000000`00000000 00000000`00000000 :
clr!SystemDomain::ExecuteMainMethod+0x452
00000000`0014fb50 000007fe`eda7f4df : 00000000`00310000 00000000`00000000 00000000`00000000 00000000`00000000 :
clr!ExecuteEXE+0x43
00000000`0014fbb0 000007fe`eda43835 : 00000000`00967890 ffffffff`ffffffff 00000000`00000000 00000000`00000000 :
clr!CorExeMainInternal+0xc4
00000000`0014fc20 000007fe`f7013309 : 00000000`00000000 00000000`00000000 00000000`00000001 00000000`0014fc08 :
clr!CorExeMain+0x15
00000000`0014fc60 000007fe`f7475b21 : 000007fe`eda43820 000007fe`f70132c0 00000000`00000000 00000000`00000000 :
mscoreei!CorExeMain+0x41
00000000`0014fc90 00000000`7735652d : 000007fe`f7010000 00000000`00000000 00000000`00000000 00000000`00000000 :
mscoree!CorExeMain_Exported+0x57
00000000`0014fcc0 00000000`777ec521 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 :
kernel32!BaseThreadInitThunk+0xd
00000000`0014fcf0 00000000`00000000 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 :
ntdll!RtlUserThreadStart+0x1d


FOLLOWUP_IP:
user32!ZwUserWaitMessage+a
00000000`7725933a c3              ret

SYMBOL_STACK_INDEX:  0

SYMBOL_NAME:  user32!ZwUserWaitMessage+a

FOLLOWUP_NAME:  MachineOwner

MODULE_NAME: user32

IMAGE_NAME:  user32.dll

DEBUG_FLR_IMAGE_TIMESTAMP:  4ce7c9f1

STACK_COMMAND:  ~0s ; kb

BUCKET_ID:  X64_HANG_user32!ZwUserWaitMessage+a

FAILURE_BUCKET_ID:  APPLICATION_HANG_WRONG_SYMBOLS_cfffffff_user32.dll!ZwUserWaitMessage

WATSON_STAGEONE_URL:  http://watson.microsoft.com/00000000.htm?Retriage=1

Followup: MachineOwner
```

/* end of WinDbg output */

Note: We see the command wasn't found anything useful. It shows only the main (#0) assembly thread that is waiting for a user message (normal GUI Win32 API message loop). We also see SOS / CLR version mismatch (shown in red), and this means a second SOS DLL was loaded. We unload it:

```
0:000> .chain
Extension DLL search Path:
[...]
Extension DLL chain:
    C:\Windows\Microsoft.NET\Framework64\v4.0.30319\sos: image 4.0.30319.18052, API 1.0.0,
built Sun Apr 21 11:25:18 2013
        [path: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\sos.dll]
    C:\ANETMDA-Dumps\64-bit\Framework64\v4.0.30319\sos: image 4.0.30319.261, API 1.0.0, built
Mon Nov 21 07:14:03 2011
        [path: C:\ANETMDA-Dumps\64-bit\Framework64\v4.0.30319\sos.dll]
    dbghelp: image 6.12.0002.633, API 6.1.6, built Mon Feb 01 20:15:44 2010
        [path: C:\Program Files\Debugging Tools for Windows (x64)\dbghelp.dll]
    ext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:15:46 2010
        [path: C:\Program Files\Debugging Tools for Windows (x64)\winext\ext.dll]
    exts: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:15:38 2010
        [path: C:\Program Files\Debugging Tools for Windows (x64)\WINXP\exts.dll]
    uext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:15:36 2010
        [path: C:\Program Files\Debugging Tools for Windows (x64)\winext\uext.dll]
    ntsdexts: image 6.1.7650.0, API 1.0.0, built Mon Feb 01 20:15:18 2010
        [path: C:\Program Files\Debugging Tools for Windows (x64)\WINXP\ntsdexts.dll]

0:000> .unload C:\Windows\Microsoft.NET\Framework64\v4.0.30319\sos
Unloading C:\Windows\Microsoft.NET\Framework64\v4.0.30319\sos extension DLL
```

11. Let's now check the managed stack trace for thread #0 to see that SOS extension is working correctly now (**!CLRStack** command):

```
0:000> !CLRStack
OS Thread Id: 0xefc (0)
Child SP         IP               Call Site
000000000014e1f0 000000007725933a [NDirectMethodFrameStandalone: 000000000014e1f0]
System.Windows.Forms.UnsafeNativeMethods.WaitMessage()
000000000014e170 000007feea179379
System.Windows.Forms.Application+ComponentManager.System.Windows.Forms.UnsafeNativeMethods.IMsoComponentManager.FPushM
essageLoop(IntPtr, Int32, Int32)
000000000014e3b0 000007feea178993 System.Windows.Forms.Application+ThreadContext.RunMessageLoopInner(Int32,
System.Windows.Forms.ApplicationContext)
000000000014e510 000007feea178321 System.Windows.Forms.Application+ThreadContext.RunMessageLoop(Int32,
System.Windows.Forms.ApplicationContext)
000000000014e5a0 000007ff00174a1a LINQPad.Program.Run(System.String, Boolean, System.String, Boolean, Boolean,
Boolean, System.String)
000000000014e830 000007ff00171cb6 LINQPad.Program.Go(System.String[])
000000000014ecc0 000007ff0017092c LINQPad.Program.Start(System.String[])
000000000014ed30 000007ff00170509 LINQPad.ProgramStarter.Run(System.String[])
000000000014ed60 000007ff001701bd LINQPad.Loader.Main(System.String[])
000000000014f170 000007feed9c90b4 [GCFrame: 000000000014f170]
```

12. On the unmanaged stack trace we also see possible JIT calls and double check on of them using **!IP2MD** command:

```
0:000> k
Child-SP          RetAddr           Call Site
00000000`0014e0d8 000007fe`ed9119c2 user32!ZwUserWaitMessage+0xa
00000000`0014e0e0 000007fe`ea179379 clr!DoNDirectCallWorker+0x62
00000000`0014e170 000007fe`ea178993 System_Windows_Forms_ni+0x349379
00000000`0014e3b0 000007fe`ea178321 System_Windows_Forms_ni+0x348993
00000000`0014e510 000007ff`00174a1a System_Windows_Forms_ni+0x348321
00000000`0014e5a0 000007ff`00171cb6 0x7ff`00174a1a
00000000`0014e830 000007ff`0017092c 0x7ff`00171cb6
00000000`0014ecc0 000007ff`00170509 0x7ff`0017092c
00000000`0014ed30 000007ff`001701bd 0x7ff`00170509
00000000`0014ed60 000007fe`ed9c90b4 0x7ff`001701bd
00000000`0014eda0 000007fe`ed9c91c9 clr!CallDescrWorker+0x84
00000000`0014edf0 000007fe`ed9c9245 clr!CallDescrWorkerWithHandler+0xa9
00000000`0014ee70 000007fe`eda331d1 clr!MethodDesc::CallDescr+0x2a1
00000000`0014f0a0 000007fe`eda3330c clr!ClassLoader::RunMain+0x228
00000000`0014f2f0 000007fe`eda330be clr!Assembly::ExecuteMainMethod+0xac
00000000`0014f5a0 000007fe`eda7f5c2 clr!SystemDomain::ExecuteMainMethod+0x452
00000000`0014fb50 000007fe`eda7f4df clr!ExecuteEXE+0x43
00000000`0014fbb0 000007fe`eda43835 clr!CorExeMainInternal+0xc4
00000000`0014fc20 000007fe`f7013309 clr!CorExeMain+0x15
00000000`0014fc60 000007fe`f7475b21 mscoreei!CorExeMain+0x41
00000000`0014fc90 00000000`7735652d mscoree!CorExeMain_Exported+0x57
00000000`0014fcc0 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`0014fcf0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

0:000> !IP2MD 0x7ff`00174a1a
MethodDesc:   000007ff00162340
Method Name:  LINQPad.Program.Run(System.String, Boolean, System.String, Boolean, Boolean,
Boolean, System.String)
Class:        000007ff0015a688
MethodTable:  000007ff00162578
mdToken:      0000000006000805
Module:       000007ff000230e0
IsJitted:     yes
CodeAddr:     000007ff00173f60
Transparency: Critical
```

13. We now check thread CPU consumption (**!runaway** command):

```
0:000> !runaway f
 User Mode Time
  Thread       Time
  19:c74       0 days 0:03:20.227
   0:efc       0 days 0:00:10.748
   9:3d4       0 days 0:00:00.452
  14:12c0      0 days 0:00:00.015
   7:4e4       0 days 0:00:00.015
   4:1664      0 days 0:00:00.015
  22:4c8       0 days 0:00:00.000
  21:c0c       0 days 0:00:00.000
  20:165c      0 days 0:00:00.000
  18:156c      0 days 0:00:00.000
  17:115c      0 days 0:00:00.000
  16:e5c       0 days 0:00:00.000
```

```
 15:16ec      0 days 0:00:00.000
 13:c50       0 days 0:00:00.000
 12:1428      0 days 0:00:00.000
 11:124c      0 days 0:00:00.000
 10:15f8      0 days 0:00:00.000
  8:162c      0 days 0:00:00.000
  6:da0       0 days 0:00:00.000
  5:13e4      0 days 0:00:00.000
  3:630       0 days 0:00:00.000
  2:ab4       0 days 0:00:00.000
  1:edc       0 days 0:00:00.000
Kernel Mode Time
 Thread       Time
  0:efc       0 days 0:00:03.634
 14:12c0      0 days 0:00:00.031
 19:c74       0 days 0:00:00.015
  8:162c      0 days 0:00:00.015
  7:4e4       0 days 0:00:00.015
 22:4c8       0 days 0:00:00.000
 21:c0c       0 days 0:00:00.000
 20:165c      0 days 0:00:00.000
 18:156c      0 days 0:00:00.000
 17:115c      0 days 0:00:00.000
 16:e5c       0 days 0:00:00.000
 15:16ec      0 days 0:00:00.000
 13:c50       0 days 0:00:00.000
 12:1428      0 days 0:00:00.000
 11:124c      0 days 0:00:00.000
 10:15f8      0 days 0:00:00.000
  9:3d4       0 days 0:00:00.000
  6:da0       0 days 0:00:00.000
  5:13e4      0 days 0:00:00.000
  4:1664      0 days 0:00:00.000
  3:630       0 days 0:00:00.000
  2:ab4       0 days 0:00:00.000
  1:edc       0 days 0:00:00.000
Elapsed Time
 Thread       Time
  0:efc       0 days 0:04:35.613
  1:edc       0 days 0:04:35.573
  2:ab4       0 days 0:04:35.572
  3:630       0 days 0:04:35.571
  4:1664      0 days 0:04:33.968
  5:13e4      0 days 0:04:32.410
  6:da0       0 days 0:04:31.234
  7:4e4       0 days 0:04:31.233
  8:162c      0 days 0:04:31.210
  9:3d4       0 days 0:04:30.383
 10:15f8      0 days 0:04:29.317
 11:124c      0 days 0:04:29.156
 12:1428      0 days 0:04:28.800
 13:c50       0 days 0:04:14.989
 14:12c0      0 days 0:03:45.051
 15:16ec      0 days 0:03:45.005
 16:e5c       0 days 0:03:28.248
 17:115c      0 days 0:03:26.110
 18:156c      0 days 0:03:24.510
 19:c74       0 days 0:03:23.079
 20:165c      0 days 0:03:21.812
 21:c0c       0 days 0:00:58.798
```

```
  22:4c8       0 days 0:00:31.221
```

Note: We see that the thread #19 spent most of the time (03:20) spiking CPU in user mode since its creation 03:23 minutes ago.

14. We now switch to this thread:

```
0:000> ~19s
000007ff`008f49dc 88442420        mov     byte ptr [rsp+20h],al ss:00000000`2060ce90=01
```

Note: we don't see register state as in the previous exercises. We need to allow them for prompts if you don't see them too:

```
0:019> .prompt_allow
Allow the following information to be displayed at the prompt:
(Other settings can affect whether the information is actually displayed)
   sym - Symbol for current instruction
   dis - Disassembly of current instruction
    ea - Effective address for current instruction
   src - Source info for current instruction
Do not allow the following information to be displayed at the prompt:
   reg - Register state

0:019> .prompt_allow +reg
Allow the following information to be displayed at the prompt:
(Other settings can affect whether the information is actually displayed)
   sym - Symbol for current instruction
   dis - Disassembly of current instruction
    ea - Effective address for current instruction
   reg - Register state
   src - Source info for current instruction
Do not allow the following information to be displayed at the prompt:
  None

0:019> ~19s
rax=0000000000000001 rbx=0000000000000000 rcx=0000000000000000
rdx=0000000000000006 rsi=000000002060d060 rdi=000000002060cef8
rip=000007ff008f49dc rsp=000000002060ce70 rbp=000000002060cf20
 r8=0000000000000000  r9=0000000000000000 r10=0000000000000000
r11=0000000000007220 r12=0000000000000000 r13=0000000000000000
r14=0000000000000000 r15=0000000000000000
iopl=0         nv up ei pl zr na po nc
cs=0033  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00000246
000007ff`008f49dc 88442420        mov     byte ptr [rsp+20h],al ss:00000000`2060ce90=01

0:019> k
Child-SP          RetAddr           Call Site
00000000`2060ce70 000007ff`008f48fe 0x7ff`008f49dc
00000000`2060ceb0 000007fe`ed9c90b4 0x7ff`008f48fe
00000000`2060cef0 000007fe`ed9c91c9 clr!CallDescrWorker+0x84
00000000`2060cf40 000007fe`ed9c9245 clr!CallDescrWorkerWithHandler+0xa9
00000000`2060cfc0 000007fe`eda93ab9 clr!MethodDesc::CallDescr+0x2a1
00000000`2060d1f0 000007fe`eda9397f clr!CallWithValueTypes_RetArgSlotWrapper+0x91
00000000`2060d480 000007fe`eda93638 clr!InvokeImpl+0x2e6
00000000`2060d910 000007fe`eca05c98 clr!RuntimeMethodHandle::InvokeMethodFast+0x1d8
00000000`2060db00 000007fe`eca0576c mscorlib_ni+0x375c98
00000000`2060dbf0 000007fe`eca502e6 mscorlib_ni+0x37576c
00000000`2060dd30 000007fe`eca50313 mscorlib_ni+0x3c02e6
00000000`2060dd80 000007ff`008f4308 mscorlib_ni+0x3c0313
```

```
00000000`2060ddc0 000007ff`008f24c0 0x7ff`008f4308
00000000`2060dff0 000007ff`008f1e15 0x7ff`008f24c0
00000000`2060e270 000007ff`008f18ea 0x7ff`008f1e15
00000000`2060e3a0 000007fe`eca017fc 0x7ff`008f18ea
00000000`2060e400 000007fe`eca0170b mscorlib_ni+0x3717fc
00000000`2060e460 000007fe`eca96fed mscorlib_ni+0x37170b
00000000`2060e4b0 000007fe`ed9c90b4 mscorlib_ni+0x406fed
00000000`2060e500 000007fe`ed9c91c9 clr!CallDescrWorker+0x84
00000000`2060e550 000007fe`ed9c9245 clr!CallDescrWorkerWithHandler+0xa9
00000000`2060e5d0 000007fe`ed9c9718 clr!MethodDesc::CallDescr+0x2a1
00000000`2060e800 000007fe`eda20618 clr!MethodDesc::CallTargetWorker+0x44
00000000`2060e840 000007fe`ed9d8fd2 clr!ThreadNative::KickOffThread_Worker+0x148
00000000`2060eb60 000007fe`ed9d8f67 clr!QueueUserWorkItemManagedCallback+0x92
00000000`2060eba0 000007fe`ed9d8ed4 clr!EEUtf8HashTableHelper::Hash+0xe8
00000000`2060eca0 000007fe`ed9d91c4 clr!IncCantStopCount+0xbd
00000000`2060ed40 000007fe`edd1356a clr!CExecutionEngine::TLS_GetMasterSlotIndex+0x2d
00000000`2060ed70 000007fe`ed9d91f8 clr! ?? ::FNODOBFM::`string'+0xad77a
00000000`2060ef20 000007fe`ed9d8f67 clr!QueueUserWorkItemManagedCallback+0xc7
00000000`2060ef60 000007fe`ed9d8ed4 clr!EEUtf8HashTableHelper::Hash+0xe8
00000000`2060f060 000007fe`ed9d902b clr!IncCantStopCount+0xbd
00000000`2060f100 000007fe`eda20468 clr!ThreadpoolMgr::TimerThreadStart+0x9f
00000000`2060f160 000007fe`eda88906 clr!ThreadNative::KickOffThread+0xc0
00000000`2060f240 00000000`7735652d clr!Thread::intermediateThreadProc+0x7d
00000000`2060f980 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`2060f9b0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

Note: We see that it is executing some code instead of waiting like other threads:

```
0:019> ~20k
Child-SP          RetAddr           Call Site
00000000`21eedad8 000007fe`fdcd1420 ntdll!ZwWaitForMultipleObjects+0xa
00000000`21eedae0 00000000`77362cf3 KERNELBASE!WaitForMultipleObjectsEx+0xe8
00000000`21eedbe0 000007fe`eda907a5 kernel32!WaitForMultipleObjectsExImplementation+0xb3
00000000`21eedc70 000007fe`eda90582 clr!WaitForMultipleObjectsEx_SO_TOLERANT+0x91
00000000`21eedd00 000007fe`eda9040d clr!Thread::DoAppropriateAptStateWait+0x56
00000000`21eedd40 000007fe`eda90503 clr!Thread::DoAppropriateWaitWorker+0x1b1
00000000`21eede40 000007fe`edb0fb65 clr!Thread::DoAppropriateWait+0x73
00000000`21eedec0 000007fe`eca8c2f4 clr!WaitHandleNative::CorWaitOneNative+0x195
00000000`21eee110 000007ff`008f61a4 mscorlib_ni+0x3fc2f4
00000000`21eee150 000007fe`eca017fc 0x7ff`008f61a4
00000000`21eee1f0 000007fe`eca0170b mscorlib_ni+0x3717fc
00000000`21eee250 000007fe`eca96fed mscorlib_ni+0x37170b
00000000`21eee2a0 000007fe`ed9c90b4 mscorlib_ni+0x406fed
00000000`21eee2f0 000007fe`ed9c91c9 clr!CallDescrWorker+0x84
00000000`21eee340 000007fe`ed9c9245 clr!CallDescrWorkerWithHandler+0xa9
00000000`21eee3c0 000007fe`ed9c9718 clr!MethodDesc::CallDescr+0x2a1
00000000`21eee5f0 000007fe`eda20618 clr!MethodDesc::CallTargetWorker+0x44
00000000`21eee630 000007fe`ed9d8fd2 clr!ThreadNative::KickOffThread_Worker+0x148
00000000`21eee950 000007fe`ed9d8f67 clr!QueueUserWorkItemManagedCallback+0x92
00000000`21eee990 000007fe`ed9d8ed4 clr!EEUtf8HashTableHelper::Hash+0xe8
00000000`21eeea90 000007fe`ed9d91c4 clr!IncCantStopCount+0xbd
00000000`21eeeb30 000007fe`edd1356a clr!CExecutionEngine::TLS_GetMasterSlotIndex+0x2d
00000000`21eeeb60 000007fe`ed9d91f8 clr! ?? ::FNODOBFM::`string'+0xad77a
00000000`21eeed10 000007fe`ed9d8f67 clr!QueueUserWorkItemManagedCallback+0xc7
00000000`21eeed50 000007fe`ed9d8ed4 clr!EEUtf8HashTableHelper::Hash+0xe8
00000000`21eeee50 000007fe`ed9d902b clr!IncCantStopCount+0xbd
00000000`21eeeef0 000007fe`eda20468 clr!ThreadpoolMgr::TimerThreadStart+0x9f
00000000`21eeef50 000007fe`eda88906 clr!ThreadNative::KickOffThread+0xc0
00000000`21eef030 00000000`7735652d clr!Thread::intermediateThreadProc+0x7d
00000000`21eef7f0 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
```

```
00000000`21eef820 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

15. We check if the address instruction pointer address belongs to JIT-compiled code:

```
0:019> !IP2MD 0x7ff`008f49dc
MethodDesc:   000007ff0093dbc0
Method Name:  UserQuery+ClassMain.Main()
Class:        000007ff009446c8
MethodTable:  000007ff0093dbe8
mdToken:      0000000006000004
Module:       000007ff0093cbd0
IsJitted:     yes
CodeAddr:     000007ff008f4990
Transparency: Critical
*** WARNING: Unable to verify checksum for query_elvfgs.dll
*** ERROR: Module load completed but symbols could not be loaded for query_elvfgs.dll
```

16. We double check our findings with !CLRStack command:

```
0:019> !CLRStack
OS Thread Id: 0xc74 (19)
Child SP         IP               Call Site
000000002060ce70 000007ff008f49dc UserQuery+ClassMain.Main()
000000002060ceb0 000007ff008f48fe UserQuery.Main()
000000002060d5a8 000007feed9c90b4 [DebuggerU2MCatchHandlerFrame: 000000002060d5a8]
000000002060d690 000007feed9c90b4 [CustomGCFrame: 000000002060d690]
000000002060d658 000007feed9c90b4 [GCFrame: 000000002060d658]
000000002060d5e8 000007feed9c90b4 [GCFrame: 000000002060d5e8]
000000002060d9b8 000007feed9c90b4 [HelperMethodFrame_PROTECTOBJ: 000000002060d9b8]
System.RuntimeMethodHandle._InvokeMethodFast(System.IRuntimeMethodInfo, System.Object, System.Object[],
System.SignatureStruct ByRef, System.Reflection.MethodAttributes, System.RuntimeType)
000000002060db00 000007feeca05c98 System.RuntimeMethodHandle.InvokeMethodFast(System.IRuntimeMethodInfo,
System.Object, System.Object[], System.Signature, System.Reflection.MethodAttributes, System.RuntimeType)
000000002060dbf0 000007feeca0576c System.Reflection.RuntimeMethodInfo.Invoke(System.Object,
System.Reflection.BindingFlags, System.Reflection.Binder, System.Object[], System.Globalization.CultureInfo, Boolean)
000000002060dd30 000007feeca502e6 System.Reflection.RuntimeMethodInfo.Invoke(System.Object,
System.Reflection.BindingFlags, System.Reflection.Binder, System.Object[], System.Globalization.CultureInfo)
000000002060dd80 000007feeca50313 System.Reflection.MethodBase.Invoke(System.Object, System.Object[])
000000002060ddc0 000007ff008f4308 LINQPad.ExecutionModel.ClrQueryRunner.Run()
000000002060dff0 000007ff008f24c0 LINQPad.ExecutionModel.Server.RunQuery(LINQPad.ExecutionModel.QueryRunner)
000000002060e270 000007ff008f1e15 LINQPad.ExecutionModel.Server.StartQuery(LINQPad.ExecutionModel.QueryRunner)
000000002060e3a0 000007ff008f18ea LINQPad.ExecutionModel.Server+<>c__DisplayClass1c.<ExecuteClrQuery>b__1b()
000000002060e400 000007feeca017fc System.Threading.ExecutionContext.Run(System.Threading.ExecutionContext,
System.Threading.ContextCallback, System.Object, Boolean)
000000002060e460 000007feeca0170b System.Threading.ExecutionContext.Run(System.Threading.ExecutionContext,
System.Threading.ContextCallback, System.Object)
000000002060e4b0 000007feeca96fed System.Threading.ThreadHelper.ThreadStart()
000000002060e908 000007feed9c90b4 [GCFrame: 000000002060e908]
000000002060ecf0 000007feed9c90b4 [DebuggerU2MCatchHandlerFrame: 000000002060ecf0]
000000002060eec8 000007feed9c90b4 [ContextTransitionFrame: 000000002060eec8]
000000002060f0b0 000007feed9c90b4 [DebuggerU2MCatchHandlerFrame: 000000002060f0b0]
```

17. We now dump the method descriptor, class, method table (with or without method descriptors), module and assembly information using **!DumpMD**, **!DumpClass**, **!DumpMT**, **!DumpModule**, **!DumpAssembly** and **!DumpDomain** SOS extension commands respectively:

```
0:019> !IP2MD 0x7ff`008f49dc
MethodDesc:   000007ff0093dbc0
Method Name:  UserQuery+ClassMain.Main()
Class:        000007ff009446c8
MethodTable:  000007ff0093dbe8
mdToken:      0000000006000004
Module:       000007ff0093cbd0
IsJitted:     yes
CodeAddr:     000007ff008f4990
Transparency: Critical

0:019> !DumpMD 000007ff0093dbc0
Method Name:  UserQuery+ClassMain.Main()
Class:        000007ff009446c8
MethodTable:  000007ff0093dbe8
mdToken:      0000000006000004
Module:       000007ff0093cbd0
IsJitted:     yes
CodeAddr:     000007ff008f4990
Transparency: Critical

0:019> !DumpClass 000007ff009446c8
Class Name:      UserQuery+ClassMain
mdToken:         0000000002000003
File:            C:\Users\Training\AppData\Local\Temp\LINQPad\zjqxgmos\query_elvfgs.dll
Parent Class:    000007feec6916c0
Module:          000007ff0093cbd0
Method Table:    000007ff0093dbe8
Vtable Slots:    4
Total Method Slots:  5
Class Attributes:    100002
Transparency:        Critical
NumInstanceFields:   3
NumStaticFields:     0
              MT    Field   Offset                 Type VT     Attr            Value Name
000007feecb5d800  4000001       10       System.Boolean  1 instance           time2stop
000007feecb5c9d0  4000002        8         System.Int32  1 instance           inSensor
000007feecb5c9d0  4000003        c         System.Int32  1 instance           outSensor

0:019> !DumpMT 000007ff0093dbe8
EEClass:      000007ff009446c8
Module:       000007ff0093cbd0
Name:         UserQuery+ClassMain
mdToken:      0000000002000003
File:         C:\Users\Training\AppData\Local\Temp\LINQPad\zjqxgmos\query_elvfgs.dll
BaseSize:        0x20
ComponentSize:   0x0
Slots in VTable: 7
Number of IFaces in IFaceMap: 0
```

```
0:019> !DumpMT 0md 000007ff0093dbe8
Incorrect argument: 000007ff0093dbe8
0:019> !DumpMT -md 000007ff0093dbe8
EEClass:      000007ff009446c8
Module:       000007ff0093cbd0
Name:         UserQuery+ClassMain
mdToken:      0000000002000003
File:         C:\Users\Training\AppData\Local\Temp\LINQPad\zjqxgmos\query_elvfgs.dll
BaseSize:        0x20
ComponentSize:   0x0
Slots in VTable: 7
Number of IFaces in IFaceMap: 0
--------------------------------------
MethodDesc Table
           Entry       MethodDesc      JIT Name
000007feec9fa430 000007feec70a928   PreJIT System.Object.ToString()
000007feeca48b60 000007feec70a930   PreJIT System.Object.Equals(System.Object)
000007feeca48a30 000007feec70a958   PreJIT System.Object.GetHashCode()
000007feeca335b0 000007feec70a970   PreJIT System.Object.Finalize()
000007ff008f4930 000007ff0093dbe0      JIT UserQuery+ClassMain..ctor()
000007ff008f4990 000007ff0093dbc0      JIT UserQuery+ClassMain.Main()
000007ff008f4a10 000007ff0093dbd0      JIT UserQuery+ClassMain.DoWork()

0:019> !DumpModule 000007ff0093cbd0
Name:       C:\Users\Training\AppData\Local\Temp\LINQPad\zjqxgmos\query_elvfgs.dll
Attributes: PEFile
Assembly:   000000001f6d91f0
LoaderHeap:              0000000000000000
TypeDefToMethodTableMap: 000007ff008eedd0
TypeRefToMethodTableMap: 000007ff008eedf0
MethodDefToDescMap:      000007ff008eee50
FieldDefToDescMap:       000007ff008eee88
MemberRefToDescMap:      000007ff008eeea8
FileReferencesMap:       000007ff008eeef0
AssemblyReferencesMap:   000007ff008eeef8
MetaData start address:  00000000713e20c4 (1336 bytes)

0:019> !DumpAssembly 000000001f6d91f0
Parent Domain:      000000001fd2cfd0
Name:               C:\Users\Training\AppData\Local\Temp\LINQPad\zjqxgmos\query_elvfgs.dll
ClassLoader:        000000001f81e390
  Module Name
000007ff0093cbd0    C:\Users\Training\AppData\Local\Temp\LINQPad\zjqxgmos\query_elvfgs.dll

0:019> !DumpDomain 000000001fd2cfd0
--------------------------------------
Domain 3:           000000001fd2cfd0
LowFrequencyHeap:   000000001fd2d590
HighFrequencyHeap:  000000001fd2d620
StubHeap:           000000001fd2d6b0
Stage:              OPEN
SecurityDescriptor: 000000001fb9ead0
Name:               LINQPad Query Server [LinqB]
Assembly:           0000000000971260
[C:\windows\Microsoft.Net\assembly\GAC_64\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll]
ClassLoader:        000000000094ac70
SecurityDescriptor: 000000001f6d1040
  Module Name
000007feec691000
C:\windows\Microsoft.Net\assembly\GAC_64\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll
```

```
Assembly:           000000001fb62a70 [C:\Users\Training\Downloads\LINQPad4-AnyCPU\LINQPad.exe]
ClassLoader:        000000001f994b30
SecurityDescriptor: 000000001f6d1220
  Module Name
000007ff008a3228    C:\Users\Training\Downloads\LINQPad4-AnyCPU\LINQPad.exe

Assembly:           00000000026fc0e0
[C:\windows\Microsoft.Net\assembly\GAC_MSIL\System.Drawing\v4.0_4.0.0.0__b03f5f7f11d50a3a\Syste
m.Drawing.dll]
ClassLoader:        000000000094b0f0
SecurityDescriptor: 000000001f6cfe70
  Module Name
000007feef361000
C:\windows\Microsoft.Net\assembly\GAC_MSIL\System.Drawing\v4.0_4.0.0.0__b03f5f7f11d50a3a\System
.Drawing.dll

Assembly:           00000000026fc1c0
[C:\windows\Microsoft.Net\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll]
ClassLoader:        000000000094b1b0
SecurityDescriptor: 000000001f8e0b50
  Module Name
000007feebb31000
C:\windows\Microsoft.Net\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll

Assembly:           000000000272e260
[C:\windows\Microsoft.Net\assembly\GAC_MSIL\System.Configuration\v4.0_4.0.0.0__b03f5f7f11d50a3a
\System.Configuration.dll]
ClassLoader:        000000000094bc30
SecurityDescriptor: 000000001f8e0f10
  Module Name
000007feeaff1000
C:\windows\Microsoft.Net\assembly\GAC_MSIL\System.Configuration\v4.0_4.0.0.0__b03f5f7f11d50a3a\
System.Configuration.dll

Assembly:           00000000026fc620
[C:\windows\Microsoft.Net\assembly\GAC_MSIL\System.Xml\v4.0_4.0.0.0__b77a5c561934e089\System.Xm
l.dll]
ClassLoader:        000000000094b6f0
SecurityDescriptor: 000000001f8e0a60
  Module Name
000007feeeca1000
C:\windows\Microsoft.Net\assembly\GAC_MSIL\System.Xml\v4.0_4.0.0.0__b77a5c561934e089\System.Xml
.dll

Assembly:           00000000026fc000
[C:\windows\Microsoft.Net\assembly\GAC_MSIL\System.Windows.Forms\v4.0_4.0.0.0__b77a5c561934e089
\System.Windows.Forms.dll]
ClassLoader:        000000000094b030
SecurityDescriptor: 0000000023076d40
  Module Name
000007fee9e31000
C:\windows\Microsoft.Net\assembly\GAC_MSIL\System.Windows.Forms\v4.0_4.0.0.0__b77a5c561934e089\
System.Windows.Forms.dll

Assembly:           000000001ec705b0
[C:\windows\Microsoft.Net\assembly\GAC_MSIL\System.Data.Linq\v4.0_4.0.0.0__b77a5c561934e089\Sys
tem.Data.Linq.dll]
ClassLoader:        000000000094c3b0
SecurityDescriptor: 00000000230775b0
```

```
  Module Name
000007fee96f1000
C:\windows\Microsoft.Net\assembly\GAC_MSIL\System.Data.Linq\v4.0_4.0.0.0__b77a5c561934e089\Syst
em.Data.Linq.dll

Assembly:           00000000026fc540
[C:\windows\Microsoft.Net\assembly\GAC_MSIL\System.Core\v4.0_4.0.0.0__b77a5c561934e089\System.C
ore.dll]
ClassLoader:        000000000094b4b0
SecurityDescriptor: 00000000230776a0
  Module Name
000007feeb131000
C:\windows\Microsoft.Net\assembly\GAC_MSIL\System.Core\v4.0_4.0.0.0__b77a5c561934e089\System.Co
re.dll

Assembly:           000000001f6d91f0
[C:\Users\Training\AppData\Local\Temp\LINQPad\zjqxgmos\query_elvfgs.dll]
ClassLoader:        000000001f81e390
SecurityDescriptor: 0000000023077a60
  Module Name
000007ff0093cbd0    C:\Users\Training\AppData\Local\Temp\LINQPad\zjqxgmos\query_elvfgs.dll
```

18. At the end of this exercise we revisit out CLR stack trace again and disassemble the previous method:

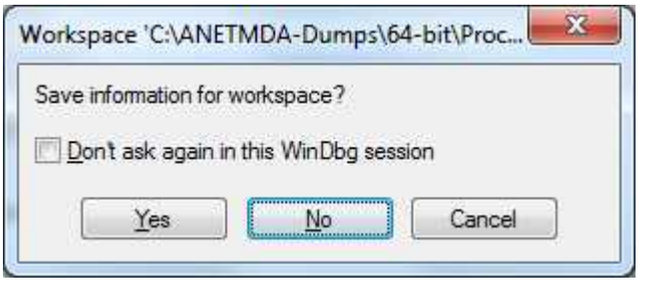
```
0:019> k
Child-SP          RetAddr           Call Site
00000000`2060ce70 000007ff`008f48fe 0x7ff`008f49dc
00000000`2060ceb0 000007fe`ed9c90b4 0x7ff`008f48fe
[...]

0:019> !U 0x7ff`008f48fe
Normal JIT generated code
UserQuery.Main()
Begin 000007ff008f48b0, size 56
000007ff`008f48b0 48894c2408      mov     qword ptr [rsp+8],rcx
000007ff`008f48b5 4883ec38        sub     rsp,38h
000007ff`008f48b9 48b8d0cf9300ff070000 mov rax,7FF0093CFD0h
000007ff`008f48c3 8b00            mov     eax,dword ptr [rax]
000007ff`008f48c5 85c0            test    eax,eax
000007ff`008f48c7 7405            je      000007ff`008f48ce
000007ff`008f48c9 e8c25e48ed      call    clr!JIT_DbgIsJustMyCode (000007fe`edd7a790)
000007ff`008f48ce 90              nop
000007ff`008f48cf 488d0d12930400  lea     rcx,[000007ff`0093dbe8]
000007ff`008f48d6 e885e501ed      call    clr!JIT_TrialAllocSFastMP_InlineGetThread (000007fe`ed912e60)
000007ff`008f48db 4889442420      mov     qword ptr [rsp+20h],rax
000007ff`008f48e0 488b442420      mov     rax,qword ptr [rsp+20h]
000007ff`008f48e5 4889442428      mov     qword ptr [rsp+28h],rax
000007ff`008f48ea 488b4c2428      mov     rcx,qword ptr [rsp+28h]
000007ff`008f48ef e82cb0fbff      call    000007ff`008af920 (UserQuery+ClassMain..ctor(), mdToken:
0000000006000006)
000007ff`008f48f4 488b4c2428      mov     rcx,qword ptr [rsp+28h]
000007ff`008f48f9 e812b0fbff      call    000007ff`008af910 (UserQuery+ClassMain.Main(), mdToken:
0000000006000004)
>>> 000007ff`008f48fe 90              nop
000007ff`008f48ff eb00            jmp     000007ff`008f4901
000007ff`008f4901 4883c438        add     rsp,38h
000007ff`008f4905 c3              ret
```

Note: We see JIT code annotated with method names and this can be helpful with reverse engineering of an unknown method.

19. We close logging before exiting WinDbg:

```
0:019> .logclose
Closing open log file C:\ANETMDA-Dumps\64-bit\Processes\CLR4\LINQPadBx64.log
```

If presented with this dialog choose No:



Note: To avoid possible confusion and glitches we recommend to exit WinDbg after each exercise.

Exercise PN8 (x64)

- **Goal:** Learn how to recognize and analyze deadlocks using SOS(EX), execution residue, handled exceptions, dump object references
- **Patterns:** CLR Thread; Special Thread; Blocked Thread; Deadlock; Execution Residue; Handled Exception
- **Commands:** !Threads -special, kL, !syncblk, !DumpObject, ub, dp, !dlk, !DumpStack, !DumpStackObjects, !teb, dps
- \ANETMDA-Dumps\Exercise-PN8-Analysis-process-dump-LINQPadC-64-CLR4.pdf

© 2013 Software Diagnostics Services

Exercise PN8: Analysis of an application process dump (LINQPadC, 64-bit, CLR 4)

Goal: Learn how to recognize and analyze deadlocks using SOS(EX), execution residue, handled exceptions, dump object references.

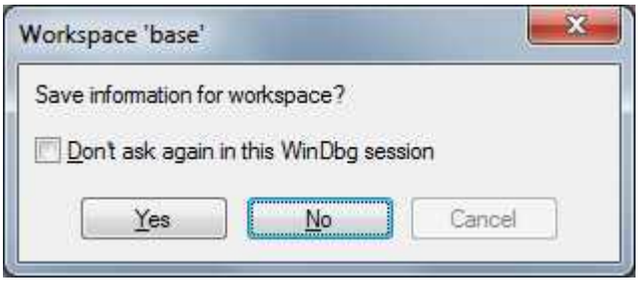
Patterns: CLR Thread; Special Thread; Blocked Thread; Deadlock; Execution Residue; Handled Exception

Commands: !Threads -special, kL, !syncblk, !DumpObject, ub, dp, !dlk, !DumpStackObjects, !teb

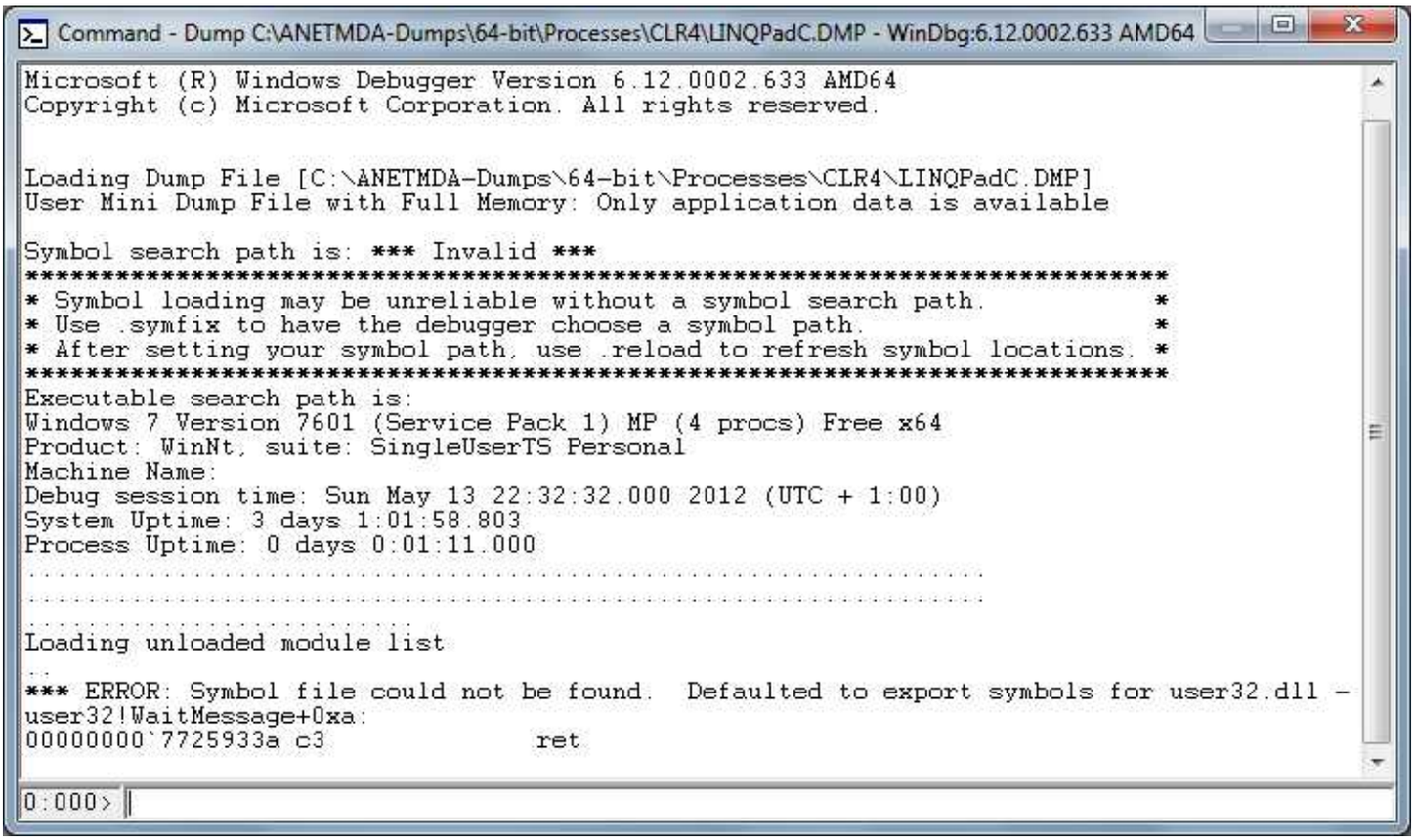
1. Launch WinDbg from Debugging Tools for Windows or Debugging Tools for Windows (x64)

2. Open \ANETMDA-Dumps\64-bit\Processes\CLR4\LINQPadC.DMP

3. If you are presented with this dialog say No:



4. We get the dump file loaded:



5. Open a log file using **.logopen** command and load symbols (**.symfix** and **.reload** commands):

```
0:000> .logopen C:\ANETMDA-Dumps\64-bit\Processes\CLR4\LINQPadCx64.log
Opened log file 'C:\ANETMDA-Dumps\64-bit\Processes\CLR4\LINQPadCx64.log'

0:000> .symfix c:\mss

0:000> .reload
.............................
```

Note: The results may be slightly different on your system if you have a different version of 64-bit .NET Framework 4 installed or you don't have any .NET Framework 4 installed.

6. Type **~*k** command to verify the correctness of all stack traces:

```
0:000> ~*k

.  0  Id: 1084.1140 Suspend: 0 Teb: 000007ff`fffdd000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`0018e098 000007fe`eec319c2 user32!ZwUserWaitMessage+0xa
*** WARNING: Unable to verify checksum for System.Windows.Forms.ni.dll
00000000`0018e0a0 000007fe`eb769379 clr!DoNDirectCallWorker+0x62
00000000`0018e130 000007fe`eb768993 System_Windows_Forms_ni+0x349379
00000000`0018e370 000007fe`eb768321 System_Windows_Forms_ni+0x348993
00000000`0018e4d0 000007ff`0019583a System_Windows_Forms_ni+0x348321
00000000`0018e560 000007ff`00191cb6 0x7ff`0019583a
00000000`0018e7f0 000007ff`0019092c 0x7ff`00191cb6
00000000`0018ec80 000007ff`00190509 0x7ff`0019092c
00000000`0018ecf0 000007ff`001901bd 0x7ff`00190509
00000000`0018ed20 000007fe`eece90b4 0x7ff`001901bd
00000000`0018ed60 000007fe`eece91c9 clr!CallDescrWorker+0x84
00000000`0018edb0 000007fe`eece9245 clr!CallDescrWorkerWithHandler+0xa9
00000000`0018ee30 000007fe`eed531d1 clr!MethodDesc::CallDescr+0x2a1
00000000`0018f060 000007fe`eed5330c clr!ClassLoader::RunMain+0x228
00000000`0018f2b0 000007fe`eed530be clr!Assembly::ExecuteMainMethod+0xac
00000000`0018f560 000007fe`eed9f5c2 clr!SystemDomain::ExecuteMainMethod+0x452
00000000`0018fb10 000007fe`eed9f4df clr!ExecuteEXE+0x43
00000000`0018fb70 000007fe`eed63835 clr!CorExeMainInternal+0xc4
00000000`0018fbe0 000007fe`f7103309 clr!CorExeMain+0x15
00000000`0018fc20 000007fe`f74b5b21 mscoreei!CorExeMain+0x41
00000000`0018fc50 00000000`7735652d mscoree!CorExeMain_Exported+0x57
00000000`0018fc80 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`0018fcb0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

   1  Id: 1084.16fc Suspend: 0 Teb: 000007ff`fffdb000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`00f4f908 000007fe`fdcd1420 ntdll!ZwWaitForMultipleObjects+0xa
00000000`00f4f910 00000000`77351220 KERNELBASE!WaitForMultipleObjectsEx+0xe8
00000000`00f4fa10 000007fe`eed5d516 kernel32!WaitForMultipleObjects+0xb0
00000000`00f4faa0 000007fe`eed5d44b clr!DebuggerRCThread::MainLoop+0xba
00000000`00f4fb50 000007fe`eed5d351 clr!DebuggerRCThread::ThreadProc+0xe4
00000000`00f4fbb0 00000000`7735652d clr!DebuggerRCThread::ThreadProcStatic+0x4d
00000000`00f4fc10 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`00f4fc40 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

   2  Id: 1084.11cc Suspend: 0 Teb: 000007ff`fffd9000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`0116f5e8 000007fe`fdcd1420 ntdll!ZwWaitForMultipleObjects+0xa
00000000`0116f5f0 00000000`77351220 KERNELBASE!WaitForMultipleObjectsEx+0xe8
00000000`0116f6f0 000007fe`eee590df kernel32!WaitForMultipleObjects+0xb0
00000000`0116f780 000007fe`eee593f3 clr!WKS::WaitForFinalizerEvent+0xcb
00000000`0116f7b0 000007fe`eecf8fd2 clr!WKS::GCHeap::FinalizerThreadWorker+0x33
00000000`0116f7e0 000007fe`eecf8f67 clr!QueueUserWorkItemManagedCallback+0x92
00000000`0116f820 000007fe`eecf8ed4 clr!EEUtf8HashTableHelper::Hash+0xe8
00000000`0116f920 000007fe`eed9f36e clr!IncCantStopCount+0xbd
00000000`0116f9c0 000007fe`eed9f7ff clr!ManagedThreadBase_NoADTransition+0x3f
00000000`0116fa20 000007fe`eeda8906 clr!WKS::GCHeap::FinalizerThreadStart+0x93
00000000`0116fa60 00000000`7735652d clr!Thread::intermediateThreadProc+0x7d
00000000`0116fb20 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`0116fb50 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
   3  Id: 1084.12fc Suspend: 0 Teb: 000007ff`fffd7000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`1b58fb58 00000000`777db007 ntdll!ZwWaitForMultipleObjects+0xa
00000000`1b58fb60 00000000`7735652d ntdll!TppWaiterpThread+0x14d
00000000`1b58fe00 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`1b58fe30 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

   4  Id: 1084.b34 Suspend: 0 Teb: 000007ff`fffd5000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`1bbfeb98 000007fe`fdcdc3ff ntdll!NtFsControlFile+0xa
00000000`1bbfeba0 000007fe`eec317c7 KERNELBASE!ConnectNamedPipe+0x6f
*** WARNING: Unable to verify checksum for System.Core.ni.dll
00000000`1bbfec10 000007fe`ea917790 clr!DoNDirectCall__PatchGetThreadCall+0x7b
00000000`1bbfecb0 000007fe`eaa21dc3 System_Core_ni+0x467790
00000000`1bbfed90 000007ff`001942b4 System_Core_ni+0x571dc3
*** WARNING: Unable to verify checksum for mscorlib.ni.dll
00000000`1bbfedd0 000007fe`ed3717fc 0x7ff`001942b4
00000000`1bbfef00 000007fe`ed37170b mscorlib_ni+0x3717fc
00000000`1bbfef60 000007fe`ed406fed mscorlib_ni+0x37170b
00000000`1bbfefb0 000007fe`eece90b4 mscorlib_ni+0x406fed
00000000`1bbff000 000007fe`eece91c9 clr!CallDescrWorker+0x84
00000000`1bbff050 000007fe`eece9245 clr!CallDescrWorkerWithHandler+0xa9
00000000`1bbff0d0 000007fe`eece9718 clr!MethodDesc::CallDescr+0x2a1
00000000`1bbff300 000007fe`eed40618 clr!MethodDesc::CallTargetWorker+0x44
00000000`1bbff340 000007fe`eecf8fd2 clr!ThreadNative::KickOffThread_Worker+0x148
00000000`1bbff660 000007fe`eecf8f67 clr!QueueUserWorkItemManagedCallback+0x92
00000000`1bbff6a0 000007fe`eecf8ed4 clr!EEUtf8HashTableHelper::Hash+0xe8
00000000`1bbff7a0 000007fe`eecf902b clr!IncCantStopCount+0xbd
00000000`1bbff840 000007fe`eed40468 clr!ThreadpoolMgr::TimerThreadStart+0x9f
00000000`1bbff8a0 000007fe`eeda8906 clr!ThreadNative::KickOffThread+0xc0
00000000`1bbff980 00000000`7735652d clr!Thread::intermediateThreadProc+0x7d
00000000`1bbffac0 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`1bbffaf0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

   5  Id: 1084.1698 Suspend: 0 Teb: 000007ff`fffd3000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`1bf2f5e8 000007fe`fdcd1420 ntdll!ZwWaitForMultipleObjects+0xa
00000000`1bf2f5f0 00000000`77362cf3 KERNELBASE!WaitForMultipleObjectsEx+0xe8
00000000`1bf2f6f0 00000000`77258f7d kernel32!WaitForMultipleObjectsExImplementation+0xb3
00000000`1bf2f780 00000000`772562b2 user32!RealMsgWaitForMultipleObjectsEx+0x12a
00000000`1bf2f820 00000000`772562e0 user32!MsgWaitForMultipleObjectsEx+0x46
00000000`1bf2f860 000007fe`fb302c6c user32!MsgWaitForMultipleObjects+0x20
00000000`1bf2f8a0 000007fe`fb302ad0 GdiPlus!BackgroundThreadProc+0x68
00000000`1bf2f910 00000000`7735652d GdiPlus!DllRefCountSafeThreadThunk+0x18
00000000`1bf2f940 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`1bf2f970 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

   6  Id: 1084.14e0 Suspend: 0 Teb: 000007ff`ffefa000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`1d84e568 000007fe`fdcd1420 ntdll!ZwWaitForMultipleObjects+0xa
00000000`1d84e570 00000000`77362cf3 KERNELBASE!WaitForMultipleObjectsEx+0xe8
00000000`1d84e670 000007fe`eedb07a5 kernel32!WaitForMultipleObjectsExImplementation+0xb3
00000000`1d84e700 000007fe`eedb0582 clr!WaitForMultipleObjectsEx_SO_TOLERANT+0x91
00000000`1d84e790 000007fe`eedb040d clr!Thread::DoAppropriateAptStateWait+0x56
00000000`1d84e7d0 000007fe`eedb0503 clr!Thread::DoAppropriateWaitWorker+0x1b1
00000000`1d84e8d0 000007fe`eedb06fa clr!Thread::DoAppropriateWait+0x73
00000000`1d84e950 000007fe`eed43f4f clr!CLREvent::WaitEx+0xc1
00000000`1d84e9f0 000007fe`eed43ebc clr!Thread::Block+0x2f
00000000`1d84ea20 000007fe`eed43c94 clr!SyncBlock::Wait+0x15c
00000000`1d84eb60 000007fe`eda2cfee clr!ObjectNative::WaitTimeout+0x124
00000000`1d84ed10 000007ff`0019c491 mscorlib_ni+0xa2cfee
00000000`1d84ed50 000007fe`ed3717fc 0x7ff`0019c491
00000000`1d84eec0 000007fe`ed37170b mscorlib_ni+0x3717fc
00000000`1d84ef20 000007fe`ed406fed mscorlib_ni+0x37170b
00000000`1d84ef70 000007fe`eece90b4 mscorlib_ni+0x406fed
00000000`1d84efc0 000007fe`eece91c9 clr!CallDescrWorker+0x84
00000000`1d84f010 000007fe`eece9245 clr!CallDescrWorkerWithHandler+0xa9
00000000`1d84f090 000007fe`eece9718 clr!MethodDesc::CallDescr+0x2a1
00000000`1d84f2c0 000007fe`eed40618 clr!MethodDesc::CallTargetWorker+0x44
00000000`1d84f300 000007fe`eecf8fd2 clr!ThreadNative::KickOffThread_Worker+0x148
00000000`1d84f620 000007fe`eecf8f67 clr!QueueUserWorkItemManagedCallback+0x92
00000000`1d84f660 000007fe`eecf8ed4 clr!EEUtf8HashTableHelper::Hash+0xe8
00000000`1d84f760 000007fe`eecf902b clr!IncCantStopCount+0xbd
00000000`1d84f800 000007fe`eed40468 clr!ThreadpoolMgr::TimerThreadStart+0x9f
00000000`1d84f860 000007fe`eeda8906 clr!ThreadNative::KickOffThread+0xc0
00000000`1d84f940 00000000`7735652d clr!Thread::intermediateThreadProc+0x7d
```

```
00000000`1d84fc00 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`1d84fc30 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

   7  Id: 1084.418 Suspend: 0 Teb: 000007ff`ffef6000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`1de4fc88 000007fe`fdcd10dc ntdll!ZwWaitForSingleObject+0xa
00000000`1de4fc90 000007fe`fa951fae KERNELBASE!WaitForSingleObjectEx+0x79
00000000`1de4fd30 00000000`7735652d rasman!RasmanServiceMonitorThread+0x171
00000000`1de4fdc0 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`1de4fdf0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

   8  Id: 1084.dcc Suspend: 0 Teb: 000007ff`ffef2000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`1dd3f478 00000000`777dfe0b ntdll!NtWaitForWorkViaWorkerFactory+0xa
00000000`1dd3f480 00000000`7735652d ntdll!TppWorkerThread+0x2c9
00000000`1dd3f780 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`1dd3f7b0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

   9  Id: 1084.11f0 Suspend: 0 Teb: 000007ff`ffef0000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`1df6f478 000007fe`fdcd1420 ntdll!ZwWaitForMultipleObjects+0xa
00000000`1df6f480 00000000`77362cf3 KERNELBASE!WaitForMultipleObjectsEx+0xe8
00000000`1df6f580 00000000`77258f7d kernel32!WaitForMultipleObjectsExImplementation+0xb3
00000000`1df6f610 00000000`772562b2 user32!RealMsgWaitForMultipleObjectsEx+0x12a
00000000`1df6f6b0 00000000`772562e0 user32!MsgWaitForMultipleObjectsEx+0x46
00000000`1df6f6f0 000007fe`fe4c2bc1 user32!MsgWaitForMultipleObjects+0x20
00000000`1df6f730 000007fe`fe4c2e54 shell32!CShellTaskScheduler::_TT_MsgWaitForMultipleObjects+0x51
00000000`1df6f7b0 000007fe`fe4c2db8 shell32!CShellTaskScheduler::TT_TransitionThreadToRunningOrTerminating+0xac
00000000`1df6f830 000007fe`fe4c2ebe shell32!CShellTaskThread::ThreadProc+0x257
00000000`1df6f8d0 000007fe`ff1c3843 shell32!CShellTaskThread::s_ThreadProc+0x22
00000000`1df6f900 00000000`777e15ab shlwapi!ExecuteWorkItemThreadProc+0xf
00000000`1df6f930 00000000`777e0c26 ntdll!RtlpTpWorkCallback+0x16b
00000000`1df6fa10 00000000`7735652d ntdll!TppWorkerThread+0x5ff
00000000`1df6fd10 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`1df6fd40 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

  10  Id: 1084.dc4 Suspend: 0 Teb: 000007ff`ffeee000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`1e31f3e8 000007fe`fdcd1420 ntdll!ZwWaitForMultipleObjects+0xa
00000000`1e31f3f0 00000000`77362cf3 KERNELBASE!WaitForMultipleObjectsEx+0xe8
00000000`1e31f4f0 00000000`77258f7d kernel32!WaitForMultipleObjectsExImplementation+0xb3
00000000`1e31f580 00000000`772562b2 user32!RealMsgWaitForMultipleObjectsEx+0x12a
00000000`1e31f620 00000000`772562e0 user32!MsgWaitForMultipleObjectsEx+0x46
00000000`1e31f660 000007fe`fe4c2bc1 user32!MsgWaitForMultipleObjects+0x20
00000000`1e31f6a0 000007fe`fe4c2e54 shell32!CShellTaskScheduler::_TT_MsgWaitForMultipleObjects+0x51
00000000`1e31f720 000007fe`fe4c2db8 shell32!CShellTaskScheduler::TT_TransitionThreadToRunningOrTerminating+0xac
00000000`1e31f7a0 000007fe`fe4c2ebe shell32!CShellTaskThread::ThreadProc+0x257
00000000`1e31f840 000007fe`ff1c3843 shell32!CShellTaskThread::s_ThreadProc+0x22
00000000`1e31f870 00000000`777e15ab shlwapi!ExecuteWorkItemThreadProc+0xf
00000000`1e31f8a0 00000000`777e0c26 ntdll!RtlpTpWorkCallback+0x16b
00000000`1e31f980 00000000`7735652d ntdll!TppWorkerThread+0x5ff
00000000`1e31fc80 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`1e31fcb0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

  11  Id: 1084.57c Suspend: 0 Teb: 000007ff`ffeec000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`1e1efad8 000007fe`fdcd1203 ntdll!NtDelayExecution+0xa
00000000`1e1efae0 000007fe`ff5201d0 KERNELBASE!SleepEx+0xab
00000000`1e1efb80 000007fe`ff520106 ole32!CROIDTable::WorkerThreadLoop+0x10
[d:\w7rtm\com\ole32\com\dcomrem\refcache.cxx @ 1345]
00000000`1e1efbb0 000007fe`ff520182 ole32!CRpcThread::WorkerLoop+0x1e [d:\w7rtm\com\ole32\com\dcomrem\threads.cxx @
257]
00000000`1e1efbf0 00000000`7735652d ole32!CRpcThreadCache::RpcWorkerThreadEntry+0x1a
[d:\w7rtm\com\ole32\com\dcomrem\threads.cxx @ 63]
00000000`1e1efc20 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`1e1efc50 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
  12  Id: 1084.1754 Suspend: 0 Teb: 000007ff`ffeea000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`1e83e338 000007fe`fdcd1420 ntdll!ZwWaitForMultipleObjects+0xa
00000000`1e83e340 00000000`77362cf3 KERNELBASE!WaitForMultipleObjectsEx+0xe8
00000000`1e83e440 000007fe`eedb07a5 kernel32!WaitForMultipleObjectsExImplementation+0xb3
00000000`1e83e4d0 000007fe`eedb0582 clr!WaitForMultipleObjectsEx_SO_TOLERANT+0x91
00000000`1e83e560 000007fe`eedb040d clr!Thread::DoAppropriateAptStateWait+0x56
00000000`1e83e5a0 000007fe`eedb0503 clr!Thread::DoAppropriateWaitWorker+0x1b1
00000000`1e83e6a0 000007fe`ef29946d clr!Thread::DoAppropriateWait+0x73
00000000`1e83e720 000007fe`eda5f6f6 clr!WaitHandleNative::CorWaitMultipleNative+0x2ad
*** WARNING: Unable to verify checksum for System.ni.dll
00000000`1e83e9a0 000007fe`ec6a57e6 mscorlib_ni+0xa5f6f6
00000000`1e83ea00 000007fe`ed3717fc System_ni+0x2057e6
00000000`1e83ead0 000007fe`ed37170b mscorlib_ni+0x3717fc
00000000`1e83eb30 000007fe`ed406fed mscorlib_ni+0x37170b
00000000`1e83eb80 000007fe`eece90b4 mscorlib_ni+0x406fed
00000000`1e83ebd0 000007fe`eece91c9 clr!CallDescrWorker+0x84
00000000`1e83ec20 000007fe`eece9245 clr!CallDescrWorkerWithHandler+0xa9
00000000`1e83eca0 000007fe`eece9718 clr!MethodDesc::CallDescr+0x2a1
00000000`1e83eed0 000007fe`eed40618 clr!MethodDesc::CallTargetWorker+0x44
00000000`1e83ef10 000007fe`eecf8fd2 clr!ThreadNative::KickOffThread_Worker+0x148
00000000`1e83f230 000007fe`eecf8f67 clr!QueueUserWorkItemManagedCallback+0x92
00000000`1e83f270 000007fe`eecf8ed4 clr!EEUtf8HashTableHelper::Hash+0xe8
00000000`1e83f370 000007fe`eecf902b clr!IncCantStopCount+0xbd
00000000`1e83f410 000007fe`eed40468 clr!ThreadpoolMgr::TimerThreadStart+0x9f
00000000`1e83f470 000007fe`eeda8906 clr!ThreadNative::KickOffThread+0xc0
00000000`1e83f550 00000000`7735652d clr!Thread::intermediateThreadProc+0x7d
00000000`1e83f910 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`1e83f940 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

  13  Id: 1084.1560 Suspend: 0 Teb: 000007ff`ffee8000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`1f42f8a8 000007fe`fdcd1203 ntdll!NtDelayExecution+0xa
00000000`1f42f8b0 000007fe`eecc8ed0 KERNELBASE!SleepEx+0xab
00000000`1f42f950 000007fe`eecc8e8a clr!ThreadpoolMgr::TimerThreadFire+0x44
00000000`1f42f9f0 00000000`7735652d clr!ThreadpoolMgr::TimerThreadStart+0x6e
00000000`1f42fa20 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`1f42fa50 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

  14  Id: 1084.850 Suspend: 0 Teb: 000007ff`ffefc000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`1f80f768 000007fe`fdcd10dc ntdll!ZwWaitForSingleObject+0xa
00000000`1f80f770 000007fe`eece77e7 KERNELBASE!WaitForSingleObjectEx+0x79
00000000`1f80f810 000007fe`eece7790 clr!CLREvent::WaitEx+0x170
00000000`1f80f850 000007fe`eece764b clr!CLREvent::WaitEx+0xf8
00000000`1f80f8b0 000007fe`eed3bbd8 clr!CLREvent::WaitEx+0x5e
00000000`1f80f950 000007fe`eeda8906 clr!AppDomain::ADUnloadThreadStart+0x144
00000000`1f80fa90 00000000`7735652d clr!Thread::intermediateThreadProc+0x7d
00000000`1f80fed0 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`1f80ff00 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

  15  Id: 1084.14dc Suspend: 0 Teb: 000007ff`ffefe000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`1f70fb58 000007fe`fdcd1203 ntdll!NtDelayExecution+0xa
00000000`1f70fb60 000007fe`eec4d33d KERNELBASE!SleepEx+0xab
00000000`1f70fc00 000007fe`eec4d358 clr!EESleepEx+0x22
00000000`1f70fc30 000007fe`eecc40e5 clr!__DangerousSwitchToThread+0x6a
00000000`1f70fc60 00000000`7735652d clr!ThreadpoolMgr::GateThreadStart+0xdc
00000000`1f70fdf0 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`1f70fe20 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

  16  Id: 1084.1720 Suspend: 0 Teb: 000007ff`ffef8000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`201bf1c8 000007fe`fdcd169d ntdll!NtRemoveIoCompletion+0xa
00000000`201bf1d0 00000000`7734a4e1 KERNELBASE!GetQueuedCompletionStatus+0x39
00000000`201bf230 000007fe`eecdda57 kernel32!GetQueuedCompletionStatusStub+0x11
00000000`201bf270 000007fe`eeda8906 clr!ThreadpoolMgr::CompletionPortThreadStart+0x113
00000000`201bf320 00000000`7735652d clr!Thread::intermediateThreadProc+0x7d
00000000`201bf7e0 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`201bf810 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
  17  Id: 1084.21c Suspend: 0 Teb: 000007ff`ffee6000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`2042f5e8 000007fe`fdcd1420 ntdll!ZwWaitForMultipleObjects+0xa
00000000`2042f5f0 00000000`77362cf3 KERNELBASE!WaitForMultipleObjectsEx+0xe8
00000000`2042f6f0 00000000`77258f7d kernel32!WaitForMultipleObjectsExImplementation+0xb3
00000000`2042f780 00000000`772562b2 user32!RealMsgWaitForMultipleObjectsEx+0x12a
00000000`2042f820 00000000`772562e0 user32!MsgWaitForMultipleObjectsEx+0x46
00000000`2042f860 000007fe`fe4c2bc1 user32!MsgWaitForMultipleObjects+0x20
00000000`2042f8a0 000007fe`fe4c2e54 shell32!CShellTaskScheduler::_TT_MsgWaitForMultipleObjects+0x51
00000000`2042f920 000007fe`fe4c2db8 shell32!CShellTaskScheduler::TT_TransitionThreadToRunningOrTerminating+0xac
00000000`2042f9a0 000007fe`fe4c2ebe shell32!CShellTaskThread::ThreadProc+0x257
00000000`2042fa40 000007fe`ff1c3843 shell32!CShellTaskThread::s_ThreadProc+0x22
00000000`2042fa70 00000000`777e15ab shlwapi!ExecuteWorkItemThreadProc+0xf
00000000`2042faa0 00000000`777e0c26 ntdll!RtlpTpWorkCallback+0x16b
00000000`2042fb80 00000000`7735652d ntdll!TppWorkerThread+0x5ff
00000000`2042fe80 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`2042feb0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

  18  Id: 1084.1598 Suspend: 0 Teb: 000007ff`ffee2000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`20aaf368 000007fe`fdcd1420 ntdll!ZwWaitForMultipleObjects+0xa
00000000`20aaf370 00000000`77362cf3 KERNELBASE!WaitForMultipleObjectsEx+0xe8
00000000`20aaf470 00000000`77258f7d kernel32!WaitForMultipleObjectsExImplementation+0xb3
00000000`20aaf500 00000000`772562b2 user32!RealMsgWaitForMultipleObjectsEx+0x12a
00000000`20aaf5a0 00000000`772562e0 user32!MsgWaitForMultipleObjectsEx+0x46
00000000`20aaf5e0 000007fe`fe4c2bc1 user32!MsgWaitForMultipleObjects+0x20
00000000`20aaf620 000007fe`fe4c2e54 shell32!CShellTaskScheduler::_TT_MsgWaitForMultipleObjects+0x51
00000000`20aaf6a0 000007fe`fe4c2db8 shell32!CShellTaskScheduler::TT_TransitionThreadToRunningOrTerminating+0xac
00000000`20aaf720 000007fe`fe4c2ebe shell32!CShellTaskThread::ThreadProc+0x257
00000000`20aaf7c0 000007fe`ff1c3843 shell32!CShellTaskThread::s_ThreadProc+0x22
00000000`20aaf7f0 00000000`777e15ab shlwapi!ExecuteWorkItemThreadProc+0xf
00000000`20aaf820 00000000`777e0c26 ntdll!RtlpTpWorkCallback+0x16b
00000000`20aaf900 00000000`7735652d ntdll!TppWorkerThread+0x5ff
00000000`20aafc00 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`20aafc30 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

  19  Id: 1084.ecc Suspend: 0 Teb: 000007ff`ffee0000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`20d8f468 000007fe`fdcd1420 ntdll!ZwWaitForMultipleObjects+0xa
00000000`20d8f470 00000000`77362cf3 KERNELBASE!WaitForMultipleObjectsEx+0xe8
00000000`20d8f570 00000000`77258f7d kernel32!WaitForMultipleObjectsExImplementation+0xb3
00000000`20d8f600 00000000`772562b2 user32!RealMsgWaitForMultipleObjectsEx+0x12a
00000000`20d8f6a0 00000000`772562e0 user32!MsgWaitForMultipleObjectsEx+0x46
00000000`20d8f6e0 000007fe`fe4c2bc1 user32!MsgWaitForMultipleObjects+0x20
00000000`20d8f720 000007fe`fe4c2e54 shell32!CShellTaskScheduler::_TT_MsgWaitForMultipleObjects+0x51
00000000`20d8f7a0 000007fe`fe4c2db8 shell32!CShellTaskScheduler::TT_TransitionThreadToRunningOrTerminating+0xac
00000000`20d8f820 000007fe`fe4c2ebe shell32!CShellTaskThread::ThreadProc+0x257
00000000`20d8f8c0 000007fe`ff1c3843 shell32!CShellTaskThread::s_ThreadProc+0x22
00000000`20d8f8f0 00000000`777e15ab shlwapi!ExecuteWorkItemThreadProc+0xf
00000000`20d8f920 00000000`777e0c26 ntdll!RtlpTpWorkCallback+0x16b
00000000`20d8fa00 00000000`7735652d ntdll!TppWorkerThread+0x5ff
00000000`20d8fd00 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`20d8fd30 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

  20  Id: 1084.eec Suspend: 0 Teb: 000007ff`ffede000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`20f1f6f8 00000000`777dfe0b ntdll!NtWaitForWorkViaWorkerFactory+0xa
00000000`20f1f700 00000000`7735652d ntdll!TppWorkerThread+0x2c9
00000000`20f1fa00 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`20f1fa30 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

  21  Id: 1084.1284 Suspend: 0 Teb: 000007ff`ffedc000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`2107f4b8 00000000`777dfe0b ntdll!NtWaitForWorkViaWorkerFactory+0xa
00000000`2107f4c0 00000000`7735652d ntdll!TppWorkerThread+0x2c9
00000000`2107f7c0 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`2107f7f0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

  22  Id: 1084.1530 Suspend: 0 Teb: 000007ff`ffeda000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`2126f818 00000000`77259e9e user32!NtUserGetMessage+0xa
00000000`2126f820 000007fe`fe4c6ad8 user32!GetMessageW+0x34
00000000`2126f850 000007fe`ff1bc71e shell32!MessagePumpThreadProc+0x3e
00000000`2126f8c0 00000000`7735652d shlwapi!WrapperThreadProc+0x19b
00000000`2126f9c0 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`2126f9f0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
  23  Id: 1084.1088 Suspend: 0 Teb: 000007ff`ffed8000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`2170f8f8 00000000`777dfe0b ntdll!NtWaitForWorkViaWorkerFactory+0xa
00000000`2170f900 00000000`7735652d ntdll!TppWorkerThread+0x2c9
00000000`2170fc00 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`2170fc30 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

  24  Id: 1084.e0c Suspend: 0 Teb: 000007ff`ffed4000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`220df598 000007fe`fdcd10dc ntdll!ZwWaitForSingleObject+0xa
00000000`220df5a0 000007fe`eecd870e KERNELBASE!WaitForSingleObjectEx+0x79
00000000`220df640 000007fe`eecd8ad7 clr!CLRSemaphore::Wait+0xaa
00000000`220df700 000007fe`eecd8c60 clr!ThreadpoolMgr::UnfairSemaphore::Wait+0x140
00000000`220df740 000007fe`eedaa5a3 clr!ThreadpoolMgr::NewWorkerThreadStart+0x2a7
00000000`220df7e0 000007fe`eeda8906 clr!ThreadpoolMgr::WorkerThreadStart+0x3b
00000000`220df880 00000000`7735652d clr!Thread::intermediateThreadProc+0x7d
00000000`220dfec0 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`220dfef0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

  25  Id: 1084.72c Suspend: 0 Teb: 000007ff`ffed6000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`2249f858 000007fe`fdcd10dc ntdll!ZwWaitForSingleObject+0xa
00000000`2249f860 00000000`654519a0 KERNELBASE!WaitForSingleObjectEx+0x79
00000000`2249f900 00000000`6544fe45 mshtml!CDwnTaskExec::ThreadExec+0x387
00000000`2249f990 00000000`7735652d mshtml!CExecFT::ThreadProc+0x57
00000000`2249f9c0 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`2249f9f0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

  26  Id: 1084.1704 Suspend: 0 Teb: 000007ff`ffed0000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`1c44fb98 000007fe`fdcd10dc ntdll!ZwWaitForSingleObject+0xa
00000000`1c44fba0 00000000`6545938c KERNELBASE!WaitForSingleObjectEx+0x79
00000000`1c44fc40 00000000`6544fe45 mshtml!CTimerMan::ThreadExec+0x17c
00000000`1c44fc90 00000000`7735652d mshtml!CExecFT::ThreadProc+0x57
00000000`1c44fcc0 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`1c44fcf0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

  27  Id: 1084.15cc Suspend: 0 Teb: 000007ff`ffece000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`23bfc648 000007fe`fdcd1420 ntdll!ZwWaitForMultipleObjects+0xa
00000000`23bfc650 00000000`77362cf3 KERNELBASE!WaitForMultipleObjectsEx+0xe8
00000000`23bfc750 00000000`77258f7d kernel32!WaitForMultipleObjectsExImplementation+0xb3
00000000`23bfc7e0 00000000`772562b2 user32!RealMsgWaitForMultipleObjectsEx+0x12a
00000000`23bfc880 000007fe`ff51acd6 user32!MsgWaitForMultipleObjectsEx+0x46
00000000`23bfc8c0 000007fe`ff63a2a2 ole32!CCliModalLoop::BlockFn+0xc2 [d:\w7rtm\com\ole32\com\dcomrem\callctrl.cxx @
1222]
00000000`23bfc910 000007fe`eee5296c ole32!CoWaitForMultipleHandles+0x102 [d:\w7rtm\com\ole32\com\dcomrem\sync.cxx @
109]
00000000`23bfca20 000007fe`eee52893 clr!MsgWaitHelper+0xd0
00000000`23bfcac0 000007fe`eedb040d clr!Thread::DoAppropriateAptStateWait+0x85
00000000`23bfcb00 000007fe`eedb0503 clr!Thread::DoAppropriateWaitWorker+0x1b1
00000000`23bfcc00 000007fe`eeda1206 clr!Thread::DoAppropriateWait+0x73
00000000`23bfcc80 000007fe`eeda163a clr!Thread::JoinEx+0xa6
00000000`23bfcd20 000007fe`eeda14ed clr!ThreadNative::DoJoin+0xd8
00000000`23bfcdc0 000007ff`007f4b5a clr!ThreadNative::Join+0xfd
00000000`23bfcf60 000007ff`007f48fe 0x7ff`007f4b5a
00000000`23bfcff0 000007fe`eece90b4 0x7ff`007f48fe
00000000`23bfd030 000007fe`eece91c9 clr!CallDescrWorker+0x84
00000000`23bfd080 000007fe`eece9245 clr!CallDescrWorkerWithHandler+0xa9
00000000`23bfd100 000007fe`eedb3ab9 clr!MethodDesc::CallDescr+0x2a1
00000000`23bfd330 000007fe`eedb397f clr!CallWithValueTypes_RetArgSlotWrapper+0x91
00000000`23bfd5c0 000007fe`eedb3638 clr!InvokeImpl+0x2e6
00000000`23bfda50 000007fe`ed375c98 clr!RuntimeMethodHandle::InvokeMethodFast+0x1d8
00000000`23bfdc40 000007fe`ed37576c mscorlib_ni+0x375c98
00000000`23bfdd30 000007fe`ed3c02e6 mscorlib_ni+0x37576c
00000000`23bfde70 000007fe`ed3c0313 mscorlib_ni+0x3c02e6
00000000`23bfdec0 000007ff`007f4308 mscorlib_ni+0x3c0313
00000000`23bfdf00 000007ff`007f24c0 0x7ff`007f4308
00000000`23bfe130 000007ff`007f1e15 0x7ff`007f24c0
00000000`23bfe3b0 000007ff`007f18ea 0x7ff`007f1e15
00000000`23bfe4e0 000007fe`ed3717fc 0x7ff`007f18ea
00000000`23bfe540 000007fe`ed37170b mscorlib_ni+0x3717fc
00000000`23bfe5a0 000007fe`ed406fed mscorlib_ni+0x37170b
00000000`23bfe5f0 000007fe`eece90b4 mscorlib_ni+0x406fed
00000000`23bfe640 000007fe`eece91c9 clr!CallDescrWorker+0x84
```

```
00000000`23bfe690 000007fe`eece9245 clr!CallDescrWorkerWithHandler+0xa9
00000000`23bfe710 000007fe`eece9718 clr!MethodDesc::CallDescr+0x2a1
00000000`23bfe940 000007fe`eed40618 clr!MethodDesc::CallTargetWorker+0x44
00000000`23bfe980 000007fe`eecf8fd2 clr!ThreadNative::KickOffThread_Worker+0x148
00000000`23bfeca0 000007fe`eecf8f67 clr!QueueUserWorkItemManagedCallback+0x92
00000000`23bfece0 000007fe`eecf8ed4 clr!EEUtf8HashTableHelper::Hash+0xe8
00000000`23bfede0 000007fe`eecf91c4 clr!IncCantStopCount+0xbd
00000000`23bfee80 000007fe`ef03356a clr!CExecutionEngine::TLS_GetMasterSlotIndex+0x2d
00000000`23bfeeb0 000007fe`eecf91f8 clr! ?? ::FNODOBFM::`string'+0xad77a
00000000`23bff060 000007fe`eecf8f67 clr!QueueUserWorkItemManagedCallback+0xc7
00000000`23bff0a0 000007fe`eecf8ed4 clr!EEUtf8HashTableHelper::Hash+0xe8
00000000`23bff1a0 000007fe`eecf902b clr!IncCantStopCount+0xbd
00000000`23bff240 000007fe`eed40468 clr!ThreadpoolMgr::TimerThreadStart+0x9f
00000000`23bff2a0 000007fe`eeda8906 clr!ThreadNative::KickOffThread+0xc0
00000000`23bff380 00000000`7735652d clr!Thread::intermediateThreadProc+0x7d
00000000`23bffac0 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`23bffaf0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

  28  Id: 1084.d14 Suspend: 0 Teb: 000007ff`ffed2000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`2094de48 000007fe`fdcd1420 ntdll!ZwWaitForMultipleObjects+0xa
00000000`2094de50 00000000`77362cf3 KERNELBASE!WaitForMultipleObjectsEx+0xe8
00000000`2094df50 000007fe`eedb07a5 kernel32!WaitForMultipleObjectsExImplementation+0xb3
00000000`2094dfe0 000007fe`eedb0582 clr!WaitForMultipleObjectsEx_SO_TOLERANT+0x91
00000000`2094e070 000007fe`eedb040d clr!Thread::DoAppropriateAptStateWait+0x56
00000000`2094e0b0 000007fe`eedb0503 clr!Thread::DoAppropriateWaitWorker+0x1b1
00000000`2094e1b0 000007fe`eedb06fa clr!Thread::DoAppropriateWait+0x73
00000000`2094e230 000007fe`eedc3e3a clr!CLREvent::WaitEx+0xc1
00000000`2094e2d0 000007fe`eedc3d43 clr!AwareLock::EnterEpilogHelper+0xca
00000000`2094e3a0 000007fe`eee3e613 clr!AwareLock::EnterEpilog+0x63
00000000`2094e400 000007ff`007f4c38 clr!JIT_MonEnterWorker_Portable+0x14f
00000000`2094e5d0 000007fe`ed3717fc 0x7ff`007f4c38
00000000`2094e620 000007fe`ed37170b mscorlib_ni+0x3717fc
00000000`2094e680 000007fe`ed406fed mscorlib_ni+0x37170b
00000000`2094e6d0 000007fe`eece90b4 mscorlib_ni+0x406fed
00000000`2094e720 000007fe`eece91c9 clr!CallDescrWorker+0x84
00000000`2094e770 000007fe`eece9245 clr!CallDescrWorkerWithHandler+0xa9
00000000`2094e7f0 000007fe`eece9718 clr!MethodDesc::CallDescr+0x2a1
00000000`2094ea20 000007fe`eed40618 clr!MethodDesc::CallTargetWorker+0x44
00000000`2094ea60 000007fe`eecf8fd2 clr!ThreadNative::KickOffThread_Worker+0x148
00000000`2094ed80 000007fe`eecf8f67 clr!QueueUserWorkItemManagedCallback+0x92
00000000`2094edc0 000007fe`eecf8ed4 clr!EEUtf8HashTableHelper::Hash+0xe8
00000000`2094eec0 000007fe`eecf91c4 clr!IncCantStopCount+0xbd
00000000`2094ef60 000007fe`ef03356a clr!CExecutionEngine::TLS_GetMasterSlotIndex+0x2d
00000000`2094ef90 000007fe`eecf91f8 clr! ?? ::FNODOBFM::`string'+0xad77a
00000000`2094f140 000007fe`eecf8f67 clr!QueueUserWorkItemManagedCallback+0xc7
00000000`2094f180 000007fe`eecf8ed4 clr!EEUtf8HashTableHelper::Hash+0xe8
00000000`2094f280 000007fe`eecf902b clr!IncCantStopCount+0xbd
00000000`2094f320 000007fe`eed40468 clr!ThreadpoolMgr::TimerThreadStart+0x9f
00000000`2094f380 000007fe`eeda8906 clr!ThreadNative::KickOffThread+0xc0
00000000`2094f460 00000000`7735652d clr!Thread::intermediateThreadProc+0x7d
00000000`2094fc20 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`2094fc50 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

  29  Id: 1084.17f0 Suspend: 0 Teb: 000007ff`ffecc000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`1c57f768 00000000`7725615e user32!NtUserGetMessage+0xa
00000000`1c57f770 000007fe`fb1510d5 user32!GetMessageA+0xc4
00000000`1c57f7a0 00000000`7735652d winmm!mciwindow+0x174
00000000`1c57f840 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`1c57f870 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

  30  Id: 1084.15bc Suspend: 0 Teb: 000007ff`ffeca000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`23e1f668 000007fe`fdcd1420 ntdll!ZwWaitForMultipleObjects+0xa
00000000`23e1f670 00000000`77351220 KERNELBASE!WaitForMultipleObjectsEx+0xe8
00000000`23e1f770 000007fe`e81f1119 kernel32!WaitForMultipleObjects+0xb0
00000000`23e1f800 000007fe`e825ae4b jscript9!Recycler::ThreadProc+0xbb
00000000`23e1f850 000007fe`ff23415f jscript9!Recycler::StaticThreadProc+0x1b
00000000`23e1f8a0 000007fe`ff236ebd msvcrt!endthreadex+0x47
00000000`23e1f8d0 00000000`7735652d msvcrt!endthreadex+0xe0
00000000`23e1f900 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`23e1f930 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

```
  31  Id: 1084.17ac Suspend: 0 Teb: 000007ff`ffec8000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`2065fb08 000007fe`fdcd10dc ntdll!ZwWaitForSingleObject+0xa
00000000`2065fb10 000007fe`e8229936 KERNELBASE!WaitForSingleObjectEx+0x79
00000000`2065fbb0 000007fe`e825af20 jscript9!BackgroundCodeGenThread::GetNextCodeGenWorkItem+0x28a
00000000`2065fc00 000007fe`e825aebb jscript9!BackgroundCodeGenThread::MainProc+0x7c
00000000`2065fc50 000007fe`ff23415f jscript9!BackgroundCodeGenThread::StaticThreadProc+0x1b
00000000`2065fca0 000007fe`ff236ebd msvcrt!endthreadex+0x47
00000000`2065fcd0 00000000`7735652d msvcrt!endthreadex+0xe0
00000000`2065fd00 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`2065fd30 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

  32  Id: 1084.1194 Suspend: 0 Teb: 000007ff`ffec6000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`2497dd08 000007fe`fdcd1420 ntdll!ZwWaitForMultipleObjects+0xa
00000000`2497dd10 00000000`77362cf3 KERNELBASE!WaitForMultipleObjectsEx+0xe8
00000000`2497de10 000007fe`eedb07a5 kernel32!WaitForMultipleObjectsExImplementation+0xb3
00000000`2497dea0 000007fe`eedb0582 clr!WaitForMultipleObjectsEx_SO_TOLERANT+0x91
00000000`2497df30 000007fe`eedb040d clr!Thread::DoAppropriateAptStateWait+0x56
00000000`2497df70 000007fe`eedb0503 clr!Thread::DoAppropriateWaitWorker+0x1b1
00000000`2497e070 000007fe`eee2fb65 clr!Thread::DoAppropriateWait+0x73
00000000`2497e0f0 000007fe`ed3fc2f4 clr!WaitHandleNative::CorWaitOneNative+0x195
00000000`2497e340 000007ff`007fba34 mscorlib_ni+0x3fc2f4
00000000`2497e380 000007fe`ed3717fc 0x7ff`007fba34
00000000`2497e420 000007fe`ed37170b mscorlib_ni+0x3717fc
00000000`2497e480 000007fe`ed406fed mscorlib_ni+0x37170b
00000000`2497e4d0 000007fe`eece90b4 mscorlib_ni+0x406fed
00000000`2497e520 000007fe`eece91c9 clr!CallDescrWorker+0x84
00000000`2497e570 000007fe`eece9245 clr!CallDescrWorkerWithHandler+0xa9
00000000`2497e5f0 000007fe`eece9718 clr!MethodDesc::CallDescr+0x2a1
00000000`2497e820 000007fe`eed40618 clr!MethodDesc::CallTargetWorker+0x44
00000000`2497e860 000007fe`eecf8fd2 clr!ThreadNative::KickOffThread_Worker+0x148
00000000`2497eb80 000007fe`eecf8f67 clr!QueueUserWorkItemManagedCallback+0x92
00000000`2497ebc0 000007fe`eecf8ed4 clr!EEUtf8HashTableHelper::Hash+0xe8
00000000`2497ecc0 000007fe`eecf91c4 clr!IncCantStopCount+0xbd
00000000`2497ed60 000007fe`ef03356a clr!CExecutionEngine::TLS_GetMasterSlotIndex+0x2d
00000000`2497ed90 000007fe`eecf91f8 clr! ?? ::FNODOBFM::`string'+0xad77a
00000000`2497ef40 000007fe`eecf8f67 clr!QueueUserWorkItemManagedCallback+0xc7
00000000`2497ef80 000007fe`eecf8ed4 clr!EEUtf8HashTableHelper::Hash+0xe8
00000000`2497f080 000007fe`eecf902b clr!IncCantStopCount+0xbd
00000000`2497f120 000007fe`eed40468 clr!ThreadpoolMgr::TimerThreadStart+0x9f
00000000`2497f180 000007fe`eeda8906 clr!ThreadNative::KickOffThread+0xc0
00000000`2497f260 00000000`7735652d clr!Thread::intermediateThreadProc+0x7d
00000000`2497faa0 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`2497fad0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

  33  Id: 1084.1070 Suspend: 0 Teb: 000007ff`ffec4000 Unfrozen
Child-SP          RetAddr           Call Site
00000000`24a7dc08 000007fe`fdcd1420 ntdll!ZwWaitForMultipleObjects+0xa
00000000`24a7dc10 00000000`77362cf3 KERNELBASE!WaitForMultipleObjectsEx+0xe8
00000000`24a7dd10 000007fe`eedb07a5 kernel32!WaitForMultipleObjectsExImplementation+0xb3
00000000`24a7dda0 000007fe`eedb0582 clr!WaitForMultipleObjectsEx_SO_TOLERANT+0x91
00000000`24a7de30 000007fe`eedb040d clr!Thread::DoAppropriateAptStateWait+0x56
00000000`24a7de70 000007fe`eedb0503 clr!Thread::DoAppropriateWaitWorker+0x1b1
00000000`24a7df70 000007fe`eedb06fa clr!Thread::DoAppropriateWait+0x73
00000000`24a7dff0 000007fe`eedc3e3a clr!CLREvent::WaitEx+0xc1
00000000`24a7e090 000007fe`eedc3d43 clr!AwareLock::EnterEpilogHelper+0xca
00000000`24a7e160 000007fe`eee3e613 clr!AwareLock::EnterEpilog+0x63
00000000`24a7e1c0 000007ff`007fc126 clr!JIT_MonEnterWorker_Portable+0x14f
00000000`24a7e390 000007fe`ed3717fc 0x7ff`007fc126
00000000`24a7e3c0 000007fe`ed37170b mscorlib_ni+0x3717fc
00000000`24a7e420 000007fe`ed406fed mscorlib_ni+0x37170b
00000000`24a7e470 000007fe`eece90b4 mscorlib_ni+0x406fed
00000000`24a7e4c0 000007fe`eece91c9 clr!CallDescrWorker+0x84
00000000`24a7e510 000007fe`eece9245 clr!CallDescrWorkerWithHandler+0xa9
00000000`24a7e590 000007fe`eece9718 clr!MethodDesc::CallDescr+0x2a1
00000000`24a7e7c0 000007fe`eed40618 clr!MethodDesc::CallTargetWorker+0x44
00000000`24a7e800 000007fe`eecf8fd2 clr!ThreadNative::KickOffThread_Worker+0x148
00000000`24a7eb20 000007fe`eecf8f67 clr!QueueUserWorkItemManagedCallback+0x92
00000000`24a7eb60 000007fe`eecf8ed4 clr!EEUtf8HashTableHelper::Hash+0xe8
00000000`24a7ec60 000007fe`eecf91c4 clr!IncCantStopCount+0xbd
00000000`24a7ed00 000007fe`ef03356a clr!CExecutionEngine::TLS_GetMasterSlotIndex+0x2d
00000000`24a7ed30 000007fe`eecf91f8 clr! ?? ::FNODOBFM::`string'+0xad77a
00000000`24a7eee0 000007fe`eecf8f67 clr!QueueUserWorkItemManagedCallback+0xc7
00000000`24a7ef20 000007fe`eecf8ed4 clr!EEUtf8HashTableHelper::Hash+0xe8
00000000`24a7f020 000007fe`eecf902b clr!IncCantStopCount+0xbd
```

```
00000000`24a7f0c0 000007fe`eed40468 clr!ThreadpoolMgr::TimerThreadStart+0x9f
00000000`24a7f120 000007fe`eeda8906 clr!ThreadNative::KickOffThread+0xc0
00000000`24a7f200 00000000`7735652d clr!Thread::intermediateThreadProc+0x7d
00000000`24a7fac0 00000000`777ec521 kernel32!BaseThreadInitThunk+0xd
00000000`24a7faf0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

Note: We see that almost half of threads have **clr** module on their stack traces.

7. Now we load the appropriate SOS extension:

```
0:000> .chain
Extension DLL search Path:
[...]
Extension DLL chain:
    dbghelp: image 6.12.0002.633, API 6.1.6, built Mon Feb 01 20:15:44 2010
        [path: C:\Program Files\Debugging Tools for Windows (x64)\dbghelp.dll]
    ext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:15:46 2010
        [path: C:\Program Files\Debugging Tools for Windows (x64)\winext\ext.dll]
    exts: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:15:38 2010
        [path: C:\Program Files\Debugging Tools for Windows (x64)\WINXP\exts.dll]
    uext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:15:36 2010
        [path: C:\Program Files\Debugging Tools for Windows (x64)\winext\uext.dll]
    ntsdexts: image 6.1.7650.0, API 1.0.0, built Mon Feb 01 20:15:18 2010
        [path: C:\Program Files\Debugging Tools for Windows (x64)\WINXP\ntsdexts.dll]

0:000> lmv m clr
start             end                 module name
000007fe`eec30000 000007fe`ef594000   clr        (pdb symbols)
c:\mss\clr.pdb\9AE088FF3C1D4CDC92FD4155F258998F2\clr.pdb
    Loaded symbol image file: clr.dll
    Image path: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll
    Image name: clr.dll
    Timestamp:        Mon Nov 21 06:57:42 2011 (4EC9F666)
    CheckSum:         00965983
    ImageSize:        00964000
    File version:     4.0.30319.261
    Product version:  4.0.30319.261
    File flags:       8 (Mask 3F) Private
    File OS:          4 Unknown Win32
    File type:        2.0 Dll
    File date:        00000000.00000000
    Translations:     0409.04b0
    CompanyName:      Microsoft Corporation
    ProductName:      Microsoft® .NET Framework
    InternalName:     clr.dll
    OriginalFilename: clr.dll
    ProductVersion:   4.0.30319.261
    FileVersion:      4.0.30319.261 (RTMGDR.030319-2600)
    PrivateBuild:     DDBLD208
    FileDescription:  Microsoft .NET Runtime Common Language Runtime - WorkStation
    LegalCopyright:   © Microsoft Corporation.  All rights reserved.
    Comments:         Flavor=Retail

0:000> .load C:\ANETMDA-Dumps\64-bit\Framework64\v4.0.30319\sos
```

```
0:000> .chain
Extension DLL search Path:
[...]
Extension DLL chain:
    C:\ANETMDA-Dumps\64-bit\Framework64\v4.0.30319\sos: image 4.0.30319.261, API 1.0.0, built
Mon Nov 21 07:14:03 2011
        [path: C:\ANETMDA-Dumps\64-bit\Framework64\v4.0.30319\sos.dll]
    dbghelp: image 6.12.0002.633, API 6.1.6, built Mon Feb 01 20:15:44 2010
        [path: C:\Program Files\Debugging Tools for Windows (x64)\dbghelp.dll]
    ext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:15:46 2010
        [path: C:\Program Files\Debugging Tools for Windows (x64)\winext\ext.dll]
    exts: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:15:38 2010
        [path: C:\Program Files\Debugging Tools for Windows (x64)\WINXP\exts.dll]
    uext: image 6.12.0002.633, API 1.0.0, built Mon Feb 01 20:15:36 2010
        [path: C:\Program Files\Debugging Tools for Windows (x64)\winext\uext.dll]
    ntsdexts: image 6.1.7650.0, API 1.0.0, built Mon Feb 01 20:15:18 2010
        [path: C:\Program Files\Debugging Tools for Windows (x64)\WINXP\ntsdexts.dll]
```

8. Now we check managed threads and list special CLR threads (**!Threads -special** command):

```
0:000> !Threads -special
ThreadCount:      16
UnstartedThread:  0
BackgroundThread: 10
PendingThread:    0
DeadThread:       3
Hosted Runtime:   no
                                          PreEmptive                                                  Lock
       ID  OSID        ThreadOBJ     State GC       GC Alloc Context                  Domain           Count APT
Exception
   0    1  1140 0000000000257890      6020 Enabled  0000000004312cd8:0000000004314140 0000000000240b50     0 STA
   2    2  11cc 000000000025db70      b220 Enabled  0000000000000000:0000000000000000 0000000000240b50     0 MTA
(Finalizer)
   4    3   b34 0000000000f70010      b220 Enabled  0000000000000000:0000000000000000 0000000000240b50     0 MTA
XXXX    5       000000000104b780     19820 Enabled  0000000000000000:0000000000000000 0000000000240b50     0 Ukn
   6    6  14e0 0000000001045950   200b220 Enabled  0000000000000000:0000000000000000 0000000000240b50     0 MTA
XXXX    7       000000000104eab0     19820 Enabled  0000000000000000:0000000000000000 0000000000240b50     0 MTA
  12    8  1754 000000001bd448f0   200b220 Enabled  0000000000000000:0000000000000000 0000000000240b50     1 MTA
  13    9  1560 000000001bd45000   100a220 Enabled  0000000000000000:0000000000000000 0000000000240b50     0 MTA
(Threadpool Worker)
  14    a   850 000000001bd45710      1220 Enabled  0000000000000000:0000000000000000 0000000000240b50     0 Ukn
  16    4  1720 000000001bd45e20   8009220 Enabled  0000000000000000:0000000000000000 0000000000240b50     0 MTA
(Threadpool Completion Port)
XXXX    b       000000001bd46530   1019820 Enabled  0000000000000000:0000000000000000 0000000000240b50     0 Ukn
(Threadpool Worker)
  24    d   e0c 000000001bd47350   1009220 Enabled  0000000000000000:0000000000000000 0000000000240b50     0 MTA
(Threadpool Worker)
  27    f  15cc 000000001ed9ce90   2007220 Enabled  0000000000000000:0000000000000000 000000001feed370     0 STA
  28   10   d14 000000001ed9d5a0   200b020 Enabled  0000000000000000:0000000000000000 000000001feed370     1 MTA
  32    e  1194 000000001bd47a60   200b220 Enabled  0000000000000000:0000000000000000 000000001feed370     0 MTA
  33    c  1070 000000001bd46c40   200b020 Enabled  0000000000000000:0000000000000000 000000001feed370     1 MTA

       OSID     Special thread type
    1   16fc    DbgHelper
    2   11cc    Finalizer
   13   1560    Timer
   14    850    ADUnloadHelper
   15   14dc    Gate
   16   1720    IOCompletion
   24    e0c    ThreadpoolWorker
```

Note: The application was reported hanging, so we check **Lock Count** ID threads.

9. We suspect a deadlock between threads #28 (**10**) and #33 (**c**) and check that using **!syncblk** command:

```
0:000> !syncblk
Index         SyncBlock MonitorHeld Recursion Owning Thread Info          SyncBlock Owner
  600 000000001edd0488            3         1 000000001bd46c40 1070  33   0000000004213eb8 System.String
  601 000000001edd0438            3         1 000000001ed9d5a0 d14  28   0000000004213e78 System.String
-----------------------------
Total           673
CCW             244
RCW             67
ComClassFactory 0
Free            2
```

Note: What we see here is that thread 33 holds a lock on **000000001edd0488** synchronization block that is owned by **0000000004213eb8** String object with "**critical section 2**" value:

```
0:000> !DumpObj 0000000004213eb8
Name:        System.String
MethodTable: 000007feed4c6ae8
EEClass:     000007feed04ed68
Size:        62(0x3e) bytes
File:
C:\windows\Microsoft.Net\assembly\GAC_64\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll
String:      critical section 2
Fields:
              MT    Field   Offset                 Type VT     Attr            Value Name
000007feed4cc9d0  4000103        8         System.Int32  1 instance               18 m_stringLength
000007feed4cb510  4000104        c          System.Char  1 instance               63 m_firstChar
000007feed4c6ae8  4000105       10        System.String  0   shared           static Empty
                                 >> Domain:Value  0000000000240b50:0000000002a21420
000000001feed370:0000000002a21420 <<
```

and that thread 28 holds a lock on **000000001edd0438** block that is owned by **0000000004213e78** String object with "**critical section 1**" value:

```
0:000> !DumpObj 0000000004213e78
Name:        System.String
MethodTable: 000007feed4c6ae8
EEClass:     000007feed04ed68
Size:        62(0x3e) bytes
File:
C:\windows\Microsoft.Net\assembly\GAC_64\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll
String:      critical section 1
Fields:
              MT    Field   Offset                 Type VT     Attr            Value Name
000007feed4cc9d0  4000103        8         System.Int32  1 instance               18 m_stringLength
000007feed4cb510  4000104        c          System.Char  1 instance               63 m_firstChar
000007feed4c6ae8  4000105       10        System.String  0   shared           static Empty
                                 >> Domain:Value  0000000000240b50:0000000002a21420
000000001feed370:0000000002a21420 <<
```

10. However, to see what blocks they are waiting for we need to inspect their stack traces:

```
0:000> ~28k 10
Child-SP          RetAddr           Call Site
00000000`2094de48 000007fe`fdcd1420 ntdll!ZwWaitForMultipleObjects+0xa
00000000`2094de50 00000000`77362cf3 KERNELBASE!WaitForMultipleObjectsEx+0xe8
00000000`2094df50 000007fe`eedb07a5 kernel32!WaitForMultipleObjectsExImplementation+0xb3
00000000`2094dfe0 000007fe`eedb0582 clr!WaitForMultipleObjectsEx_SO_TOLERANT+0x91
00000000`2094e070 000007fe`eedb040d clr!Thread::DoAppropriateAptStateWait+0x56
00000000`2094e0b0 000007fe`eedb0503 clr!Thread::DoAppropriateWaitWorker+0x1b1
00000000`2094e1b0 000007fe`eedb06fa clr!Thread::DoAppropriateWait+0x73
00000000`2094e230 000007fe`eedc3e3a clr!CLREvent::WaitEx+0xc1
00000000`2094e2d0 000007fe`eedc3d43 clr!AwareLock::EnterEpilogHelper+0xca
00000000`2094e3a0 000007fe`eee3e613 clr!AwareLock::EnterEpilog+0x63
00000000`2094e400 000007ff`007f4c38 clr!JIT_MonEnterWorker_Portable+0x14f
00000000`2094e5d0 000007fe`ed3717fc 0x7ff`007f4c38
00000000`2094e620 000007fe`ed37170b mscorlib_ni+0x3717fc
00000000`2094e680 000007fe`ed406fed mscorlib_ni+0x37170b
00000000`2094e6d0 000007fe`eece90b4 mscorlib_ni+0x406fed
00000000`2094e720 000007fe`eece91c9 clr!CallDescrWorker+0x84

0:000> !IP2MD 0x7ff`007f4c38
MethodDesc:   000007ff0083dce8
Method Name:  UserQuery+ClassMain.thread_proc_1()
Class:        000007ff008446c8
MethodTable:  000007ff0083dd28
mdToken:      0000000006000005
Module:       000007ff0083ccd0
IsJitted:     yes
CodeAddr:     000007ff007f4ba0
Transparency: Critical
*** WARNING: Unable to verify checksum for query_johhme.dll
*** ERROR: Module load completed but symbols could not be loaded for query_johhme.dll

0:000> ub 0x7ff`007f4c38
000007ff`007f4c18 eb00            jmp     000007ff`007f4c1a
000007ff`007f4c1a 90              nop
000007ff`007f4c1b b9d0070000      mov     ecx,7D0h
000007ff`007f4c20 e8cb211ded      call    mscorlib_ni+0x9c6df0 (000007fe`ed9c6df0)
000007ff`007f4c25 90              nop
000007ff`007f4c26 48b9d8f4a31200000000 mov rcx,12A3F4D8h
000007ff`007f4c30 488b09          mov     rcx,qword ptr [rcx]
000007ff`007f4c33 e818e443ee      call    clr!JIT_MonEnter (000007fe`eec33050)

0:000> dp 12A3F4D8h L1
00000000`12a3f4d8  00000000`04213eb8
```

Note: We see the thread 28 is waiting for the sync block owner (String) from the thread 33.

11. We repeat the same exercise for the thread 33:

```
0:000> ~33k L10
Child-SP          RetAddr           Call Site
00000000`24a7dc08 000007fe`fdcd1420 ntdll!ZwWaitForMultipleObjects+0xa
00000000`24a7dc10 00000000`77362cf3 KERNELBASE!WaitForMultipleObjectsEx+0xe8
00000000`24a7dd10 000007fe`eedb07a5 kernel32!WaitForMultipleObjectsExImplementation+0xb3
00000000`24a7dda0 000007fe`eedb0582 clr!WaitForMultipleObjectsEx_SO_TOLERANT+0x91
00000000`24a7de30 000007fe`eedb040d clr!Thread::DoAppropriateAptStateWait+0x56
00000000`24a7de70 000007fe`eedb0503 clr!Thread::DoAppropriateWaitWorker+0x1b1
00000000`24a7df70 000007fe`eedb06fa clr!Thread::DoAppropriateWait+0x73
00000000`24a7dff0 000007fe`eedc3e3a clr!CLREvent::WaitEx+0xc1
00000000`24a7e090 000007fe`eedc3d43 clr!AwareLock::EnterEpilogHelper+0xca
00000000`24a7e160 000007fe`eee3e613 clr!AwareLock::EnterEpilog+0x63
00000000`24a7e1c0 000007ff`007fc126 clr!JIT_MonEnterWorker_Portable+0x14f
00000000`24a7e390 000007fe`ed3717fc 0x7ff`007fc126
00000000`24a7e3c0 000007fe`ed37170b mscorlib_ni+0x3717fc
00000000`24a7e420 000007fe`ed406fed mscorlib_ni+0x37170b
00000000`24a7e470 000007fe`eece90b4 mscorlib_ni+0x406fed
00000000`24a7e4c0 000007fe`eece91c9 clr!CallDescrWorker+0x84

0:000> !IP2MD 0x7ff`007fc126
MethodDesc:   000007ff0083dcf8
Method Name:  UserQuery+ClassMain.thread_proc_2()
Class:        000007ff008446c8
MethodTable:  000007ff0083dd28
mdToken:      0000000006000006
Module:       000007ff0083ccd0
IsJitted:     yes
CodeAddr:     000007ff007fc0e0
Transparency: Critical

0:000> ub 0x7ff`007fc126
000007ff`007fc107 e8446f43ee      call    clr!JIT_MonEnter (000007fe`eec33050)
000007ff`007fc10c 90              nop
000007ff`007fc10d 90              nop
000007ff`007fc10e e8cd8bffff      call    000007ff`007f4ce0
000007ff`007fc113 90              nop
000007ff`007fc114 48b9d0f4a31200000000 mov rcx,12A3F4D0h
000007ff`007fc11e 488b09          mov     rcx,qword ptr [rcx]
000007ff`007fc121 e82a6f43ee      call    clr!JIT_MonEnter (000007fe`eec33050)

0:000> dp 12A3F4D0h L1
00000000`12a3f4d0  00000000`04213e78
```

Note: We see the thread 33 is waiting for the sync block owner (String) from the thread 28. Since both threads are mutually waiting for each other, we consider them as deadlocked.

12. This was a very lengthy manual exercise which can be automated by SOSEX extension **!dlk** command:

```
0:000> .load C:\ANETMDA-Dumps\64-bit\sosex_64\sosex
This dump has no SOSEX heap index.
The heap index makes searching for references and roots much faster.
To create a heap index, run !bhi
```

```
0:000> !dlk
Examining SyncBlocks...
Scanning for ReaderWriterLock instances...
Scanning for holders of ReaderWriterLock locks...
Scanning for ReaderWriterLockSlim instances...
Scanning for holders of ReaderWriterLockSlim locks...
Examining CriticalSections...
Scanning for threads waiting on SyncBlocks...
*** WARNING: Unable to verify checksum for query_johhme.dll
*** ERROR: Module load completed but symbols could not be loaded for query_johhme.dll
Scanning for threads waiting on ReaderWriterLock locks...
Scanning for threads waiting on ReaderWriterLocksSlim locks...
Scanning for threads waiting on CriticalSections...
*DEADLOCK DETECTED*
CLR thread 0x10 holds the lock on SyncBlock 000000001edd0438
OBJ:0000000004213e78[System.String] STRVAL="critical section 1"
...and is waiting for the lock on SyncBlock 000000001edd0488
OBJ:0000000004213eb8[System.String] STRVAL="critical section 2"
CLR thread 0xc holds the lock on SyncBlock 000000001edd0488 OBJ:0000000004213eb8[System.String]
STRVAL="critical section 2"
...and is waiting for the lock on SyncBlock 000000001edd0438
OBJ:0000000004213e78[System.String] STRVAL="critical section 1"
CLR Thread 0x10 is waiting at UserQuery+ClassMain.thread_proc_1()(+0x51 IL,+0x98 Native)
CLR Thread 0xc is waiting at UserQuery+ClassMain.thread_proc_2()(+0x1d IL,+0x46 Native)


1 deadlock detected.
```

13. How did this deadlock happen? If we look at both threads execution residue we would see that in the case of the thread No. 28 there was an exception:

```
0:000> ~28s
ntdll!ZwWaitForMultipleObjects+0xa:
00000000`778118ca c3              ret

0:028> !DumpStackObjects
OS Thread Id: 0xd14 (28)
RSP/REG          Object           Name
rcx              0000000004213eb8 System.String    critical section 2
000000002094DF68 0000000004213f90 System.Threading.ThreadHelper
000000002094E320 0000000004213eb8 System.String    critical section 2
000000002094E428 0000000004213eb8 System.String    critical section 2
000000002094E528 0000000004213f90 System.Threading.ThreadHelper
000000002094E530 0000000004213ff8 System.Threading.ExecutionContext
000000002094E5D0 0000000004213ff8 System.Threading.ExecutionContext
000000002094E5E0 0000000004213f90 System.Threading.ThreadHelper
000000002094E5E8 0000000003fd7280 System.Threading.ContextCallback
000000002094E600 0000000003fff150 System.NullReferenceException
000000002094E608 0000000004214260 System.Windows.Forms.Internal.DeviceContext+GraphicsState
000000002094E620 0000000004213ef8 System.Threading.ThreadStart
000000002094E628 0000000004213f90 System.Threading.ThreadHelper
000000002094E630 0000000004213f90 System.Threading.ThreadHelper
000000002094E660 0000000004213ff8 System.Threading.ExecutionContext
000000002094E670 0000000004213f90 System.Threading.ThreadHelper
000000002094E680 0000000004213f90 System.Threading.ThreadHelper
000000002094E6B0 0000000004213ff8 System.Threading.ExecutionContext
000000002094E6C0 0000000004213f90 System.Threading.ThreadHelper
000000002094E6D0 0000000004213f90 System.Threading.ThreadHelper
000000002094E720 0000000004213fb8 System.Threading.ThreadStart
```

```
000000002094E888 0000000004213fb8 System.Threading.ThreadStart
000000002094EAC0 0000000004213fb8 System.Threading.ThreadStart
000000002094EAD8 0000000004213fb8 System.Threading.ThreadStart

0:028> ~33s
ntdll!ZwWaitForMultipleObjects+0xa:
00000000`778118ca c3              ret

0:033> !dso
OS Thread Id: 0x1070 (33)
RSP/REG          Object           Name
rcx              0000000004213e78 System.String    critical section 1
0000000024A7E0E0 0000000004213e78 System.String    critical section 1
0000000024A7E1E8 0000000004213e78 System.String    critical section 1
0000000024A7E3A8 0000000003fd7280 System.Threading.ContextCallback
0000000024A7E860 000000000400a718 System.Threading.ThreadStart
```

Note: We also double check our hypothesis by looking at the thread unmanaged raw stack (also in the case if **!DumpStackObjects** command (**!dso**) doesn't show anything suspicious in managed residue). We would see lots of exception processing references on thread 28 raw stack and nothing on thread 33:

```
0:033> ~28s
ntdll!ZwWaitForMultipleObjects+0xa:
00000000`778118ca c3              ret

0:028> !teb
TEB at 000007ffffed2000
    ExceptionList:        0000000000000000
    StackBase:            0000000020950000
    StackLimit:           0000000020948000
    SubSystemTib:         0000000000000000
    FiberData:            0000000000001e00
    ArbitraryUserPointer: 0000000000000000
    Self:                 000007ffffed2000
    EnvironmentPointer:   0000000000000000
    ClientId:             0000000000001084 . 0000000000000d14
    RpcHandle:            0000000000000000
    Tls Storage:          000000001ed87140
    PEB Address:          000007fffffdf000
    LastErrorValue:       0
    LastStatusValue:      c000007c
    Count Owned Locks:    0
    HardErrorMode:        0
```

```
0:028> dps 0000000020948000 0000000020950000
00000000`20948000  00000000`00000000
00000000`20948008  00000000`00000000
[...]
00000000`2094c0f0  00000000`2094e5d0
00000000`2094c0f8  000007fe`eedc083f clr!ProcessCLRException+0x304
00000000`2094c100  000007ff`007f4c1a
00000000`2094c108  00000000`2094c290
00000000`2094c110  00000000`00255410
00000000`2094c118  000007ff`007f4c1a
00000000`2094c120  00000000`1ed9d5a0
00000000`2094c128  00000000`00000000
00000000`2094c130  000007fe`eedbe1fa clr!NakedThrowHelper_RspAligned+0x3d
00000000`2094c138  00000000`777e9b3e ntdll!RtlLookupFunctionTable+0xaa
00000000`2094c140  00000000`2094c8d0
00000000`2094c148  000007fe`00000000
00000000`2094c150  00000000`00000000
00000000`2094c158  ffffffff`fffffffe
00000000`2094c160  000031c0`81a4a98c
00000000`2094c168  000007fe`eedbe1fa clr!NakedThrowHelper_RspAligned+0x3d
00000000`2094c170  000007fe`eedbe1fa clr!NakedThrowHelper_RspAligned+0x3d
00000000`2094c178  00000000`2094df70
00000000`2094c180  00000000`2094c8d0
00000000`2094c188  000007ff`00844a0c
00000000`2094c190  000007ff`007f4bfc
00000000`2094c198  00000000`2094e5d0
00000000`2094c1a0  00000000`2094e5d0
00000000`2094c1a8  00000000`2094b000
00000000`2094c1b0  00000000`2094c8d0
00000000`2094c1b8  00000000`2094c380
00000000`2094c1c0  00000000`00000000
00000000`2094c1c8  00000000`777e9d8d ntdll!RtlpExecuteHandlerForUnwind+0xd
00000000`2094c1d0  000007ff`007f4b00
00000000`2094c1d8  00000000`2094e5d0
00000000`2094c1e0  00000000`2094c8d0
00000000`2094c1e8  00000000`2094c290
00000000`2094c1f0  00000000`2094c290
00000000`2094c1f8  00000000`777d8a2c ntdll!RtlUnwindEx+0x539
00000000`2094c200  00000000`00000000
00000000`2094c208  00000000`2094c800
00000000`2094c210  00010202`00000000
00000000`2094c218  00000000`2094e5d0
00000000`2094c220  00000000`2094c380
00000000`2094c228  00000000`2094c270
00000000`2094c230  00000000`2094c260
00000000`2094c238  00000000`00000000
[...]
00000000`2094c890  00000000`2094cf50
00000000`2094c898  000007fe`eedc2e58 clr!ClrUnwindEx+0x40
00000000`2094c8a0  00000000`2094e5d0
[...]
```

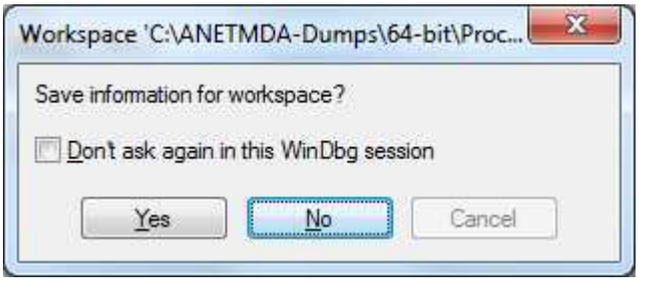
```
0:033> ub 000007fe`eedc083f
clr!ProcessCLRException+0x2e2:
000007fe`eedc081d 4d8bc5          mov     r8,r13
000007fe`eedc0820 498bd4          mov     rdx,r12
000007fe`eedc0823 488bcf          mov     rcx,rdi
000007fe`eedc0826 e8b52b0000      call    clr!FixNonvolatileRegisters (000007fe`eedc33e0)
000007fe`eedc082b 4989742410      mov     qword ptr [r12+10h],rsi
000007fe`eedc0830 49899df8000000  mov     qword ptr [r13+0F8h],rbx
000007fe`eedc0837 498bcd          mov     rcx,r13
000007fe`eedc083a e8112d0000      call    clr!ExceptionTracker::ResumeExecution
(000007fe`eedc3550)

0:033> ub 00000000`777d8a2c
ntdll!RtlUnwindEx+0x520:
00000000`777d8a13 24b8            and     al,0B8h
00000000`777d8a15 0000            add     byte ptr [rax],al
00000000`777d8a17 004c8994        add     byte ptr [rcx+rcx*4-6Ch],cl
00000000`777d8a1b 24c0            and     al,0C0h
00000000`777d8a1d 0000            add     byte ptr [rax],al
00000000`777d8a1f 00899c24d800    add     byte ptr [rcx+0D8249Ch],cl
00000000`777d8a25 0000            add     byte ptr [rax],al
00000000`777d8a27 e854130100      call    ntdll!RtlpExecuteHandlerForUnwind (00000000`777e9d80)

0:033> ub 000007fe`eedc2e58
clr!ClrUnwindEx+0x1f:
000007fe`eedc2e37 498bc0          mov     rax,r8
000007fe`eedc2e3a 4c8d442430      lea     r8,[rsp+30h]
000007fe`eedc2e3f 4c89442420      mov     qword ptr [rsp+20h],r8
000007fe`eedc2e44 4c8bca          mov     r9,rdx
000007fe`eedc2e47 4c8bc1          mov     r8,rcx
000007fe`eedc2e4a 488bc8          mov     rcx,rax
000007fe`eedc2e4d bad0ba0000      mov     edx,0BAD0h
000007fe`eedc2e52 ff1580b54e00    call    qword ptr [clr!_imp_RtlUnwindEx (000007fe`ef2ae3d8)]
```

Note: We also double checked symbolic references we found to see if they were valid return addresses.

14. We close logging before exiting WinDbg:

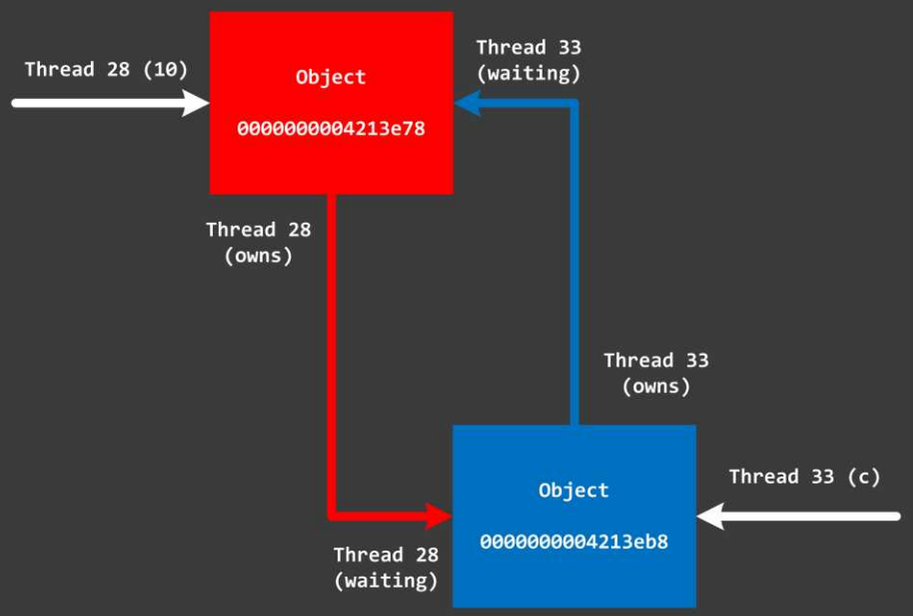
```
0:033> .logclose
Closing open log file C:\ANETMDA-Dumps\64-bit\Processes\CLR4\LINQPadCx64.log
```

If presented with this dialog choose No:



Note: To avoid possible confusion and glitches we recommend to exit WinDbg after each exercise.

Deadlock (x64)



© 2013 Software Diagnostics Services

Optional exercise: Complete memory dump analysis

Goal: Learn how to extract and recognize .NET CLR threads in the context of a physical memory dump.

Patterns: Special Process; Handle Leak; Paged Out Data; CLR Thread; Exception Thread

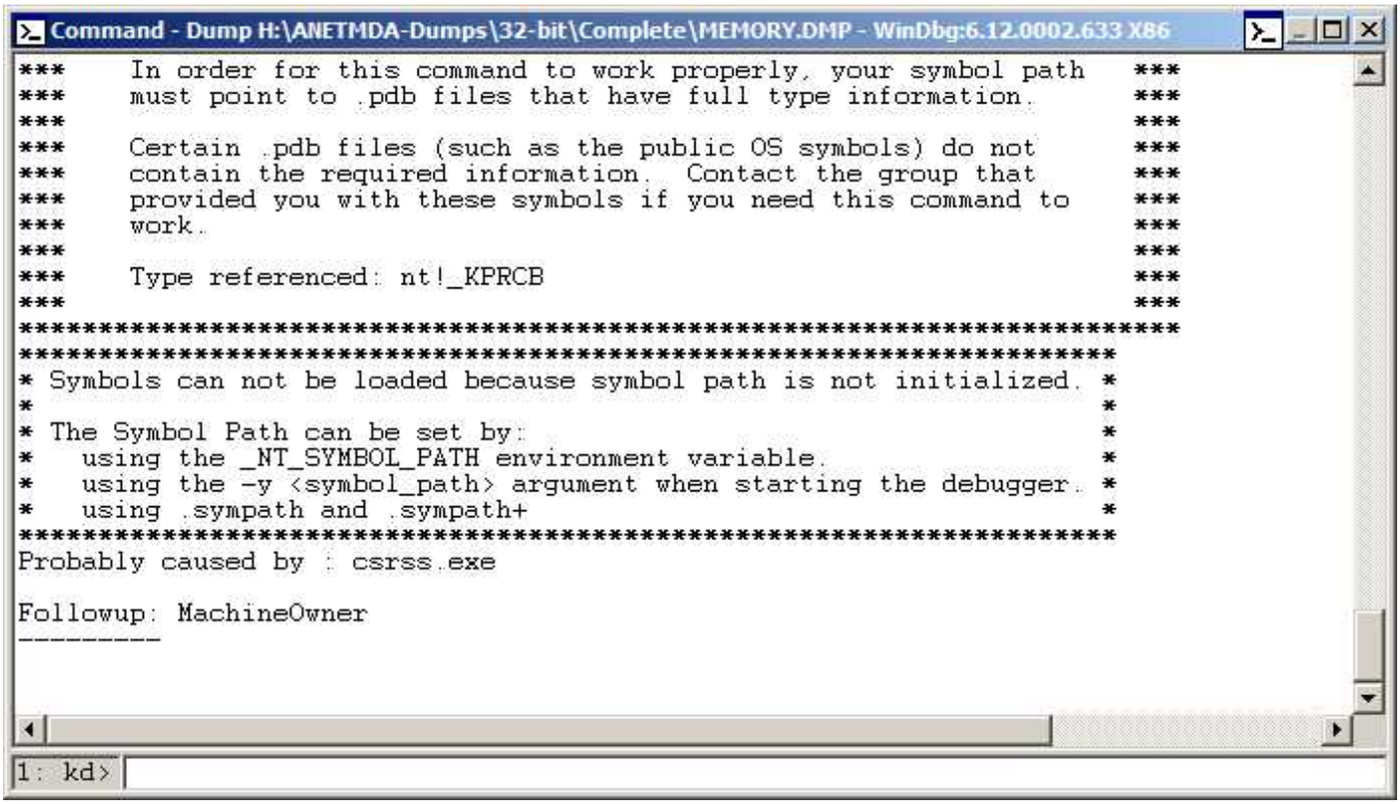
Commands: !process 0 0; !poolused 3; .process /r /p <>; !vm; !handle; !thread <> ff; !process <> ff; .thread /r /p <>; .trap

1. Launch WinDbg from Debugging Tools for Windows or Debugging Tools for Windows (x86)

2. Open \ANETMDA-Dumps\32-bit\Complete\MEMORY.DMP

3. If you are presented with this dialog say No:

4. We get the dump file loaded:



5. We load symbols (**.symfix** and **.reload** commands):

```
0:000> .symfix c:\mss

0:000> .reload
.............................
```

6. We dump the list of all processes:

```
1: kd> !process 0 0
**** NT ACTIVE PROCESS DUMP ****
PROCESS 82b34d90  SessionId: none  Cid: 0004    Peb: 00000000  ParentCid: 0000
    DirBase: 00122000  ObjectTable: 85a00180  HandleCount: 360.
    Image: System

PROCESS 84bd9598  SessionId: none  Cid: 017c    Peb: 7ffdf000  ParentCid: 0004
    DirBase: 2f01e020  ObjectTable: 87306110  HandleCount:  28.
    Image: smss.exe

PROCESS 84ac51d8  SessionId: 0  Cid: 01fc    Peb: 7ffd4000  ParentCid: 01f0
    DirBase: 2f01e060  ObjectTable: 8c426c00  HandleCount: 481.
    Image: csrss.exe

PROCESS 83cafd90  SessionId: 0  Cid: 0228    Peb: 7ffdf000  ParentCid: 01f0
    DirBase: 2f01e0a0  ObjectTable: 8c53f400  HandleCount:  98.
    Image: wininit.exe

PROCESS 84bfdd90  SessionId: 1  Cid: 0234    Peb: 7ffdf000  ParentCid: 0220
    DirBase: 2f01e040  ObjectTable: 8c4987f8  HandleCount: 332.
    Image: csrss.exe

PROCESS 89639158  SessionId: 0  Cid: 0258    Peb: 7ffd3000  ParentCid: 0228
    DirBase: 2f01e0c0  ObjectTable: 8c57f450  HandleCount: 226.
    Image: services.exe

PROCESS 89612d90  SessionId: 0  Cid: 0274    Peb: 7ffdd000  ParentCid: 0228
    DirBase: 2f01e0e0  ObjectTable: 8c57c868  HandleCount: 577.
    Image: lsass.exe

PROCESS 89646348  SessionId: 0  Cid: 027c    Peb: 7ffdb000  ParentCid: 0228
    DirBase: 2f01e100  ObjectTable: 8c569780  HandleCount: 155.
    Image: lsm.exe

PROCESS 89679c80  SessionId: 1  Cid: 029c    Peb: 7ffde000  ParentCid: 0220
    DirBase: 2f01e120  ObjectTable: 8c4bf830  HandleCount: 128.
    Image: winlogon.exe

PROCESS 89700d90  SessionId: 0  Cid: 032c    Peb: 7ffd9000  ParentCid: 0258
    DirBase: 2f01e080  ObjectTable: 966c1630  HandleCount: 303.
    Image: svchost.exe
```

```
PROCESS 896fb9f8  SessionId: 0  Cid: 0364    Peb: 7ffdd000  ParentCid: 0258
    DirBase: 2f01e140  ObjectTable: 962c9870  HandleCount: 281.
    Image: svchost.exe

PROCESS 8971a310  SessionId: 0  Cid: 0384    Peb: 7ffd9000  ParentCid: 0258
    DirBase: 2f01e160  ObjectTable: 8c5d3e18  HandleCount: 317.
    Image: svchost.exe

PROCESS 897501f0  SessionId: 0  Cid: 03e0    Peb: 7ffdb000  ParentCid: 0258
    DirBase: 2f01e1a0  ObjectTable: 96311260  HandleCount: 390.
    Image: svchost.exe

PROCESS 89759550  SessionId: 0  Cid: 0428    Peb: 7ffd4000  ParentCid: 0258
    DirBase: 2f01e1c0  ObjectTable: 963487a8  HandleCount: 416.
    Image: svchost.exe

PROCESS 89747d90  SessionId: 0  Cid: 0434    Peb: 7ffde000  ParentCid: 0258
    DirBase: 2f01e1e0  ObjectTable: 96387a28  HandleCount: 1076.
    Image: svchost.exe

PROCESS 89798020  SessionId: 0  Cid: 04a8    Peb: 7ffd3000  ParentCid: 03e0
    DirBase: 2f01e200  ObjectTable: 963bcf28  HandleCount: 107.
    Image: audiodg.exe

PROCESS 897799a0  SessionId: 0  Cid: 04c4    Peb: 7ffd5000  ParentCid: 0258
    DirBase: 2f01e220  ObjectTable: 967dac48  HandleCount:  74.
    Image: SLsvc.exe

PROCESS 8978e460  SessionId: 0  Cid: 0510    Peb: 7ffde000  ParentCid: 0258
    DirBase: 2f01e240  ObjectTable: 963bf240  HandleCount: 600.
    Image: svchost.exe

PROCESS 8aeb8198  SessionId: 0  Cid: 0560    Peb: 7ffd9000  ParentCid: 0258
    DirBase: 2f01e260  ObjectTable: 9704f8f8  HandleCount: 462.
    Image: svchost.exe

PROCESS 897a0d90  SessionId: 0  Cid: 0604    Peb: 7ffdd000  ParentCid: 0258
    DirBase: 2f01e280  ObjectTable: 9704c800  HandleCount: 327.
    Image: spoolsv.exe

PROCESS 897c9680  SessionId: 0  Cid: 061c    Peb: 7ffd9000  ParentCid: 0258
    DirBase: 2f01e2a0  ObjectTable: 9704e460  HandleCount: 285.
    Image: svchost.exe

PROCESS 8ae6e5a0  SessionId: 0  Cid: 0700    Peb: 7ffd9000  ParentCid: 0258
    DirBase: 2f01e2c0  ObjectTable: 96626ac8  HandleCount: 107.
    Image: svchost.exe

PROCESS 8ae94b30  SessionId: 0  Cid: 0774    Peb: 7ffde000  ParentCid: 0258
    DirBase: 2f01e300  ObjectTable: 96246380  HandleCount: 277.
    Image: vmtoolsd.exe
```

```
PROCESS 8aeb3d90  SessionId: 0  Cid: 07cc    Peb: 7ffd7000  ParentCid: 0258
    DirBase: 2f01e320  ObjectTable: 98406fc8  HandleCount:  79.
    Image: svchost.exe

PROCESS 8aec6ad0  SessionId: 0  Cid: 07e4    Peb: 7ffd6000  ParentCid: 0258
    DirBase: 2f01e340  ObjectTable: 97169f38  HandleCount: 658.
    Image: SearchIndexer.exe

PROCESS 8aecbc78  SessionId: 0  Cid: 011c    Peb: 7ffde000  ParentCid: 0258
    DirBase: 2f01e360  ObjectTable: 9843f770  HandleCount:  90.
    Image: VMUpgradeHelper.exe

PROCESS 8af353d0  SessionId: 0  Cid: 0328    Peb: 7ffd6000  ParentCid: 0258
    DirBase: 2f01e3c0  ObjectTable: 98598f60  HandleCount: 242.
    Image: dllhost.exe

PROCESS 8af4e720  SessionId: 0  Cid: 0854    Peb: 7ffd4000  ParentCid: 0258
    DirBase: 2f01e3e0  ObjectTable: 9717cbd8  HandleCount: 151.
    Image: msdtc.exe

PROCESS 8315bc10  SessionId: 1  Cid: 0d4c    Peb: 7ffd5000  ParentCid: 0434
    DirBase: 2f01e480  ObjectTable: 9dea7e30  HandleCount: 298.
    Image: taskeng.exe

PROCESS 831684f0  SessionId: 1  Cid: 0d6c    Peb: 7ffd5000  ParentCid: 0428
    DirBase: 2f01e4c0  ObjectTable: 9deb1e48  HandleCount:  92.
    Image: dwm.exe

PROCESS 831f3020  SessionId: 1  Cid: 0d8c    Peb: 7ffdf000  ParentCid: 0d5c
    DirBase: 2f01e4e0  ObjectTable: 9b3ad6d8  HandleCount: 826.
    Image: explorer.exe

PROCESS 83102aa8  SessionId: 1  Cid: 0e48    Peb: 7ffde000  ParentCid: 0d8c
    DirBase: 2f01e440  ObjectTable: 97065528  HandleCount: 314.
    Image: MSASCui.exe

PROCESS 830f23a8  SessionId: 1  Cid: 0e50    Peb: 7ffdc000  ParentCid: 0d8c
    DirBase: 2f01e520  ObjectTable: 9df87050  HandleCount:  70.
    Image: VMwareTray.exe

PROCESS 8318f878  SessionId: 1  Cid: 0e64    Peb: 7ffdb000  ParentCid: 0d8c
    DirBase: 2f01e540  ObjectTable: 962949a0  HandleCount: 221.
    Image: VMwareUser.exe

PROCESS 8af09968  SessionId: 1  Cid: 04ec    Peb: 7ffd6000  ParentCid: 0d8c
    DirBase: 2f01e380  ObjectTable: 9d756c10  HandleCount: 411.
    Image: sidebar.exe

PROCESS 831e20f0  SessionId: 1  Cid: 0f98    Peb: 7ffd7000  ParentCid: 0434
    DirBase: 2f01e560  ObjectTable: 9de95ef8  HandleCount: 135.
    Image: taskeng.exe
```

```
PROCESS 830ca020  SessionId: 1  Cid: 305ac    Peb: 7ffd8000  ParentCid: 07cc
    DirBase: 2f01e500  ObjectTable: 00000000  HandleCount:   0.
    Image: WerFault.exe

PROCESS 8312f800  SessionId: 1  Cid: 6245c    Peb: 7ffdd000  ParentCid: 0d8c
    DirBase: 2f01e400  ObjectTable: 9dec11d8  HandleCount: 252146.
    Image: LINQPad.exe

PROCESS a13f6020  SessionId: 1  Cid: 31420    Peb: 7ffd9000  ParentCid: 032c
    DirBase: 2f01e4a0  ObjectTable: 97057968  HandleCount: 117.
    Image: mobsync.exe

PROCESS a201cd90  SessionId: 1  Cid: 31540    Peb: 7ffdd000  ParentCid: 09c4
    DirBase: 2f01e2e0  ObjectTable: 8c561100  HandleCount: 103.
    Image: taskmgr.exe
```

Note: We notice the presence of WerFault.exe, and this signifies the possible past exceptions in one of the processes (not necessarily on the current list). We also see LINQPad.exe process with more than 250K handles (definitely a handle leak). Actually, this complete physical memory dump was forced after saving a process memory for exercise PN5.

7. We switch to our process:

```
1: kd> .process /r /p 8312f800
Implicit process is now 8312f800
Loading User Symbols
..................Unable to read NT module Base Name string at 00220f82 - NTSTATUS 0xC0000147
Missing image name, possible paged-out or corrupt data.
.............................Unable to read NT module Base Name string at 00266eaa - NTSTATUS
0xC0000147
Missing image name, possible paged-out or corrupt data.
................
......Unable to read NT module Base Name string at 002dea60 - NTSTATUS 0xC0000147
..Unable to read NT module Base Name string at 002deaa8 - NTSTATUS 0xC0000147
...Unable to read NT module Base Name string at 002deaf0 - NTSTATUS 0xC0000147
...Unable to read NT module Base Name string at 002dee50 - NTSTATUS 0xC0000147
Missing image name, possible paged-out or corrupt data.
..Unable to read NT module Base Name string at 002deee0 - NTSTATUS 0xC0000147
.Unable to read NT module Base Name string at 002def28 - NTSTATUS 0xC0000147
.....Unable to read NT module Base Name string at 050ccf48 - NTSTATUS 0xC0000147
Missing image name, possible paged-out or corrupt data.
........Unable to read LDR_DATA_TABLE_ENTRY at 050cbfd8 - HRESULT 0x80004005

WARNING: .reload failed, module list may be incomplete
```

Note: We see lots of warnings because some process data was paged out as the committed size of the process is larger than the amount of physical memory:

```
1: kd> !vm

*** Virtual Memory Usage ***
      Physical Memory:      261872 (   1047488 Kb)
      Page File: \??\C:\pagefile.sys
        Current:   1354688 Kb  Free Space:     53120 Kb
        Minimum:   1354688 Kb  Maximum:      4194304 Kb
      Available Pages:      180984 (    723936 Kb)
      ResAvail Pages:       216475 (    865900 Kb)
      Locked IO Pages:           0 (         0 Kb)
      Free System PTEs:     352925 (   1411700 Kb)
      Modified Pages:          129 (       516 Kb)
      Modified PF Pages:        94 (       376 Kb)
      NonPagedPool Usage:        0 (         0 Kb)
      NonPagedPoolNx Usage:  16894 (     67576 Kb)
      NonPagedPool Max:     192350 (    769400 Kb)
      PagedPool 0 Usage:      5957 (     23828 Kb)
      PagedPool 1 Usage:      3218 (     12872 Kb)
      PagedPool 2 Usage:       965 (      3860 Kb)
      PagedPool 3 Usage:      1311 (      5244 Kb)
      PagedPool 4 Usage:      1064 (      4256 Kb)
      PagedPool Usage:       12515 (     50060 Kb)
      PagedPool Maximum:    523264 (   2093056 Kb)
      Session Commit:         5021 (     20084 Kb)
      Shared Commit:         15023 (     60092 Kb)
      Special Pool:              0 (         0 Kb)
      Shared Process:         1938 (      7752 Kb)
      PagedPool Commit:      12523 (     50092 Kb)
      Driver Commit:          2592 (     10368 Kb)
      Committed pages:      402494 (   1609976 Kb)
      Commit limit:         589254 (   2357016 Kb)

      Total Private:        350654 (   1402616 Kb)
        6245c LINQPad.exe     268837 (   1075348 Kb)
        0d8c explorer.exe      13584 (     54336 Kb)
        0428 svchost.exe       11448 (     45792 Kb)
        07e4 SearchIndexer.e    8142 (     32568 Kb)
        04ec sidebar.exe        5933 (     23732 Kb)
        0434 svchost.exe        4803 (     19212 Kb)
        03e0 svchost.exe        3359 (     13436 Kb)
        061c svchost.exe        2973 (     11892 Kb)
        0560 svchost.exe        2842 (     11368 Kb)
        04a8 audiodg.exe        2777 (     11108 Kb)
        0234 csrss.exe          2563 (     10252 Kb)
        0d4c taskeng.exe        2208 (      8832 Kb)
        0604 spoolsv.exe        1528 (      6112 Kb)
        0328 dllhost.exe        1452 (      5808 Kb)
        0384 svchost.exe        1445 (      5780 Kb)
        0774 vmtoolsd.exe       1327 (      5308 Kb)
        0e48 MSASCui.exe        1230 (      4920 Kb)
        0e64 VMwareUser.exe     1207 (      4828 Kb)
        04c4 SLsvc.exe          1176 (      4704 Kb)
        0f98 taskeng.exe        1160 (      4640 Kb)
        0510 svchost.exe        1117 (      4468 Kb)
        0364 svchost.exe         875 (      3500 Kb)
        0274 lsass.exe           768 (      3072 Kb)
        032c svchost.exe         721 (      2884 Kb)
        31420 mobsync.exe         707 (      2828 Kb)
        0e50 VMwareTray.exe      686 (      2744 Kb)
        0258 services.exe        645 (      2580 Kb)
```

```
         0854 msdtc.exe          625 (      2500 Kb)
         31540 taskmgr.exe        600 (      2400 Kb)
         011c VMUpgradeHelper    555 (      2220 Kb)
         029c winlogon.exe       504 (      2016 Kb)
         027c lsm.exe            488 (      1952 Kb)
         0700 svchost.exe        446 (      1784 Kb)
         01fc csrss.exe          417 (      1668 Kb)
         0d6c dwm.exe            415 (      1660 Kb)
         0004 System             372 (      1488 Kb)
         0228 wininit.exe        333 (      1332 Kb)
         07cc svchost.exe        314 (      1256 Kb)
         017c smss.exe            72 (       288 Kb)
         305ac WerFault.exe         0 (         0 Kb)
```

8. Now we get the list of all process handles:

```
1: kd> !handle

PROCESS 8312f800  SessionId: 1  Cid: 6245c    Peb: 7ffdd000  ParentCid: 0d8c
    DirBase: 2f01e400  ObjectTable: 9dec11d8  HandleCount: 252146.
    Image: LINQPad.exe

Handle table at 9d632000 with 252146 entries in use

0004: Object: 8b7d6b88  GrantedAccess: 00000003 Entry: 9d4ac008
Object: 8b7d6b88  Type: (82b38ed0) Directory
    ObjectHeader: 8b7d6b70 (old version)
        HandleCount: 36  PointerCount: 65
        Directory Object: 85a074c0  Name: KnownDlls

0008: Object: 8aed9548  GrantedAccess: 00100020 Entry: 9d4ac010
Object: 8aed9548  Type: (82b76350) File
    ObjectHeader: 8aed9530 (old version)
        HandleCount: 1  PointerCount: 1
        Directory Object: 00000000  Name: \LINQPad4 {HarddiskVolume1}

000c: Object: 83225e08  GrantedAccess: 001f0001 Entry: 9d4ac018
Object: 83225e08  Type: (82b75bf0) Mutant
    ObjectHeader: 83225df0 (old version)
        HandleCount: 1  PointerCount: 1

0010: Object: 997cca60  GrantedAccess: 00000001 Entry: 9d4ac020
Object: 997cca60  Type: (82b7a3c8) Key
    ObjectHeader: 997cca48 (old version)
        HandleCount: 1  PointerCount: 1
        Directory Object: 00000000  Name:
\REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\SESSION MANAGER

0014: Object: 8ae79f08  GrantedAccess: 001f0001 Entry: 9d4ac028
Object: 8ae79f08  Type: (82b6ebf0) ALPC Port
    ObjectHeader: 8ae79ef0 (old version)
        HandleCount: 1  PointerCount: 3

[...]
```

```
f6b74: Object: a32bdd78  GrantedAccess: 001fffff Entry: 95d326e8
Object: a32bdd78  Type: (82b386f8) Thread
    ObjectHeader: a32bdd60 (old version)
        HandleCount: 1  PointerCount: 1

f6b78: Object: a32bc078  GrantedAccess: 001f0003 Entry: 95d326f0
Object: a32bc078  Type: (82b75ed0) Event
    ObjectHeader: a32bc060 (old version)
        HandleCount: 1  PointerCount: 1

f6b7c: Object: a32bdd38  GrantedAccess: 001f0003 Entry: 95d326f8
Object: a32bdd38  Type: (82b75ed0) Event
    ObjectHeader: a32bdd20 (old version)
        HandleCount: 1  PointerCount: 1

f6b80: Object: a32bdd08  GrantedAccess: 001f0003 Entry: 95d32700
Object: a32bdd08  Type: (82b75ed0) Event
    ObjectHeader: a32bdcf0 (old version)
        HandleCount: 1  PointerCount: 1

f6b84: Object: a32bdcd8  GrantedAccess: 001f0003 Entry: 95d32708
Object: a32bdcd8  Type: (82b75ed0) Event
    ObjectHeader: a32bdcc0 (old version)
        HandleCount: 1  PointerCount: 1

f6b88: Object: a32bda30  GrantedAccess: 001fffff Entry: 95d32710
Object: a32bda30  Type: (82b386f8) Thread
    ObjectHeader: a32bda18 (old version)
        HandleCount: 1  PointerCount: 1

f6b8c: Object: 89723420  GrantedAccess: 001f0003 Entry: 95d32718
Object: 89723420  Type: (82b75ed0) Event
    ObjectHeader: 89723408 (old version)
        HandleCount: 1  PointerCount: 1

f6b90: Object: 83343c60  GrantedAccess: 001fffff Entry: 95d32720
Object: 83343c60  Type: (82b386f8) Thread
    ObjectHeader: 83343c48 (old version)
        HandleCount: 2  PointerCount: 3

f6ba4: Object: 9f84b510  GrantedAccess: 00100003 Entry: 95d32748
Object: 9f84b510  Type: (82b75ed0) Event
    ObjectHeader: 9f84b4f8 (old version)
        HandleCount: 1  PointerCount: 1

f6bac: Object: a217cd78  GrantedAccess: 001fffff Entry: 95d32758
Object: a217cd78  Type: (82b386f8) Thread
    ObjectHeader: a217cd60 (old version)
        HandleCount: 2  PointerCount: 3
```

Note: We check a few thread objects to see that they were terminated but not completely released:

```
1: kd> !thread a32bdd78 ff
THREAD a32bdd78  Cid 6245c.30cf0  Teb: 00000000 Win32Thread: 00000000 TERMINATED
Not impersonating
DeviceMap                 9b2d5900
Owning Process            8312f800       Image:         LINQPad.exe
Attached Process          N/A            Image:         N/A
Wait Start TickCount      1481345        Ticks: 62188 (0:00:16:11.687)
Context Switch Count      4
UserTime                  00:00:00.000
KernelTime                00:00:00.000
Win32 Start Address clr!Thread::intermediateThreadProc (0x6afd59c0)
Stack Init 0 Current 987afc18 Base 987b0000 Limit 987ad000 Call 0
Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
ChildEBP RetAddr
WARNING: Frame IP not in any known module. Following frames may be wrong.
987afc74 8c2db6d4 0xa32f5078
987afc90 8c2d9926 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
987afce8 8c2dd933 win32k!xxxRealInternalGetMessage+0x4a4 (FPO: [Non-Fpo])
987afd4c 8188c96a win32k!NtUserGetMessage+0x3f (FPO: [Non-Fpo])
987afd4c 77c40f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 987afd64)
016bf1dc 00000000 ntdll!KiFastSystemCallRet (FPO: [0,0,0])

1: kd> !thread a32bda30 ff
THREAD a32bda30  Cid 6245c.30cf4  Teb: 00000000 Win32Thread: 00000000 TERMINATED
Not impersonating
DeviceMap                 9b2d5900
Owning Process            8312f800       Image:         LINQPad.exe
Attached Process          N/A            Image:         N/A
Wait Start TickCount      1481345        Ticks: 62188 (0:00:16:11.687)
Context Switch Count      2
UserTime                  00:00:00.000
KernelTime                00:00:00.000
Win32 Start Address clr!Thread::intermediateThreadProc (0x6afd59c0)
Stack Init 0 Current 9c922c18 Base 9c923000 Limit 9c920000 Call 0
Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
```

9. Now we list process thread stack traces:

```
1: kd> !process 8312f800 3f
PROCESS 8312f800  SessionId: 1  Cid: 6245c    Peb: 7ffdd000  ParentCid: 0d8c
    DirBase: 2f01e400  ObjectTable: 9dec11d8  HandleCount: 252146.
    Image: LINQPad.exe
    VadRoot 830f6540 Vads 380 Clone 0 Private 263452. Modified 326850. Locked 0.
    DeviceMap 9b2d5900
    Token                             9ac50ca0
    ElapsedTime                       00:17:25.399
    UserTime                          00:00:11.953
    KernelTime                        00:00:23.859
    QuotaPoolUsage[PagedPool]         2411728
    QuotaPoolUsage[NonPagedPool]      50424
    Working Set Sizes (now,min,max)  (23683, 50, 345) (94732KB, 200KB, 1380KB)
    PeakWorkingSetSize                224984
    VirtualSize                       1296 Mb
    PeakVirtualSize                   1304 Mb
    PageFaultCount                    816085
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      268837

    PEB at 7ffdd000
```

```
    InheritedAddressSpace:    No
    ReadImageFileExecOptions: No
    BeingDebugged:            No
    ImageBaseAddress:         00dc0000
    Ldr                       77ca5d00
    Ldr.Initialized:          Yes
    Ldr.InInitializationOrderModuleList: 001e1618 . 0513a090
    Ldr.InLoadOrderModuleList:           001e1598 . 0513a080
    Ldr.InMemoryOrderModuleList:         001e15a0 . 0513a088
            Base TimeStamp                     Module
          dc0000 4cfb29be Dec 05 05:57:18 2010 C:\LINQPad4\LINQPad.exe
        77be0000 4549bdc9 Nov 02 09:43:37 2006 C:\Windows\system32\ntdll.dll
        73740000 4af3af84 Nov 06 05:09:24 2009 C:\Windows\system32\mscoree.dll
        76530000 4549bd80 Nov 02 09:42:24 2006 C:\Windows\system32\KERNEL32.dll
        77500000 4549bcd2 Nov 02 09:39:30 2006 C:\Windows\system32\ADVAPI32.dll
        76610000 4549bdab Nov 02 09:43:07 2006 C:\Windows\system32\RPCRT4.dll
        73640000 4ba1d8a9 Mar 18 07:39:21 2010 C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll
        775c0000 4549bdb9 Nov 02 09:43:21 2006 C:\Windows\system32\SHLWAPI.dll
        77650000 4549bcd3 Nov 02 09:39:31 2006 C:\Windows\system32\GDI32.dll
        76730000 4549bde0 Nov 02 09:44:00 2006 C:\Windows\system32\USER32.dll
        77b30000 4549bd61 Nov 02 09:41:53 2006 C:\Windows\system32\msvcrt.dll
        77e00000 4549bd29 Nov 02 09:40:57 2006 C:\Windows\system32\IMM32.DLL
        77430000 4549bd4a Nov 02 09:41:30 2006 C:\Windows\system32\MSCTF.dll
        77d00000 4549bcff Nov 02 09:40:15 2006 C:\Windows\system32\LPK.DLL
        777f0000 4549bde3 Nov 02 09:44:03 2006 C:\Windows\system32\USP10.dll
        75240000 4549bd09 Nov 02 09:40:25 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.6000.16386_none_5d07289e07e1d100\comctl32.dll
        6af20000 4ba1d9ef Mar 18 07:44:47 2010 C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.dll
        71260000 4ba1dbf2 Mar 18 07:53:22 2010 C:\Windows\system32\MSVCR100_CLR0400.dll
        69380000 4ba1da6f Mar 18 07:46:55 2010 < Name not readable >
        776a0000 4549bd92 Nov 02 09:42:42 2006 C:\Windows\system32\ole32.dll
        75540000 4549bde7 Nov 02 09:44:07 2006 C:\Windows\system32\uxtheme.dll
        73900000 4ba1d8aa Mar 18 07:39:22 2010 C:\Windows\Microsoft.NET\Framework\v4.0.30319\culture.dll
        738d0000 4ba1d8ae Mar 18 07:39:26 2010 C:\Windows\Microsoft.NET\Framework\v4.0.30319\nlssorting.dll
        75890000 4549bdae Nov 02 09:43:10 2006 C:\Windows\system32\rsaenh.dll
        714d0000 4ba1da36 Mar 18 07:45:58 2010 C:\Windows\Microsoft.NET\Framework\v4.0.30319\clrjit.dll
        6a680000 4ba1dff4 Mar 18 08:10:28 2010
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\964da027ebca3b263a05cadb8eaa20a3\System.ni.dll
        6d6d0000 4ba1e086 Mar 18 08:12:54 2010
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\dd57bc19f5807c6dbe8f88d4a23277f6\System.Drawing.ni.dll
        67910000 4ba1e14e Mar 18 08:16:14 2010
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\17e020ae92d7fab33bcc1c98b25019d0\System.Windows.Fo
rms.ni.dll
        738f0000 4549bdb5 Nov 02 09:43:17 2006 C:\Windows\system32\shfolder.dll
        768d0000 4549bdb4 Nov 02 09:43:16 2006 C:\Windows\system32\SHELL32.dll
        76350000 4549bde2 Nov 02 09:44:02 2006 C:\Windows\system32\USERENV.dll
        76330000 4549bdd2 Nov 02 09:43:46 2006 C:\Windows\system32\Secur32.dll
        68cc0000 4ba1dfee Mar 18 08:10:22 2010
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\713647b987b140a17e3c4ffe4c721f85\System.Core.ni.dll
        71180000 4ba1e39e Mar 18 08:26:06 2010
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml.Linq\8eca92a64c232f34b5b559625b022369\System.Xml.Linq.ni.dll
        68760000 4ba1dfec Mar 18 08:10:20 2010
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\e997d0200c25f7db6bd32313d50b729d\System.Xml.ni.dll
        6bdd0000 4ba1f437 Mar 18 09:36:55 2010
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runtime.Seri#\e9f8a45b1063d6c6a62718c88a5623d1\System.Runtime.Se
rialization.ni.dll
        75810000 4549bddb Nov 02 09:43:55 2006 C:\Windows\system32\NTMARTA.DLL
        766e0000 4549be44 Nov 02 09:45:40 2006 C:\Windows\system32\WLDAP32.dll
        76820000 4549be0e Nov 02 09:44:46 2006 C:\Windows\system32\WS2_32.dll
        77df0000 4549bdc7 Nov 02 09:43:35 2006 C:\Windows\system32\NSI.dll
        76490000 4549bd99 Nov 02 09:42:49 2006 C:\Windows\system32\PSAPI.DLL
        75fa0000 4549bda8 Nov 02 09:43:04 2006 C:\Windows\system32\SAMLIB.dll
        742b0000 4549bcb0 Nov 02 09:38:56 2006 C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.6000.16386_none_87e0cb09378714f1\comctl32.dll
        6a2e0000 4ba1f805 Mar 18 09:53:09 2010
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\d17606e813f01376bd0def23726ecc62\WindowsBase.ni.dll
```

```
        663f0000 4ba1f865 Mar 18 09:54:45 2010
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\3963e9ce8d44f50e8367e92a8e3e42e6\PresentationCore.ni.d
ll
        74cf0000 4549bcaf Nov 02 09:38:55 2006
C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.0.6000.16386_none_9ea0ac9ec96e7127\gdiplus.dll
        71230000 4549bccc Nov 02 09:39:24 2006 C:\Windows\system32\dciman32.dll
        6d510000 4ba1e140 Mar 18 08:16:00 2010
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\6a6f4be744ed5bc5273cbcf0fcf303e3\System.Management.ni
.dll
        6d410000 4ba1e04b Mar 18 08:11:55 2010 < Name not readable >
        738c0000 4ba1db9f Mar 18 07:51:59 2010 C:\Windows\Microsoft.NET\Framework\v4.0.30319\wminet_utils.dll
        764a0000 4549bd95 Nov 02 09:42:45 2006 C:\Windows\system32\OLEAUT32.dll
        773a0000 4549bce9 Nov 02 09:39:53 2006 C:\Windows\system32\CLBCatQ.DLL
        72730000 4549be6b Nov 02 09:46:19 2006 C:\Windows\system32\wbem\wmiutils.dll
        732c0000 4549bdea Nov 02 09:44:10 2006 C:\Windows\system32\wbem\wbemcomn.dll
        73240000 4549bdef Nov 02 09:44:15 2006 C:\Windows\system32\wbem\wbemprox.dll
        72da0000 4549bdf0 Nov 02 09:44:16 2006 C:\Windows\system32\wbem\wbemsvc.dll
        75400000 4549bda3 Nov 02 09:42:59 2006 C:\Windows\system32\rasapi32.dll
        75700000 4549bdab Nov 02 09:43:07 2006 C:\Windows\system32\rasman.dll
        75fc0000 4549bd53 Nov 02 09:41:39 2006 C:\Windows\system32\NETAPI32.dll
        75010000 4549bdd1 Nov 02 09:43:45 2006 C:\Windows\system32\TAPI32.dll
        75630000 4549bdba Nov 02 09:43:22 2006 C:\Windows\system32\rtutils.dll
        74fd0000 4549be1d Nov 02 09:45:01 2006 C:\Windows\system32\WINMM.dll
        74ec0000 4549bd93 Nov 02 09:42:43 2006 C:\Windows\system32\OLEACC.dll
        72750000 4549bcd4 Nov 02 09:39:32 2006 C:\Windows\system32\wbem\fastprox.dll
        75f60000 4549bdcc Nov 02 09:43:40 2006 C:\Windows\system32\NTDSAPI.dll
        76030000 4549bcf1 Nov 02 09:40:01 2006 C:\Windows\system32\DNSAPI.dll
        75c30000 4549bd20 Nov 02 09:40:48 2006 C:\Windows\system32\credssp.dll
        75e40000 4549bd24 Nov 02 09:40:52 2006 C:\Windows\system32\CRYPT32.dll
        75f80000 4549bd41 Nov 02 09:41:21 2006 C:\Windows\system32\MSASN1.dll
        758d0000 4549bdb4 Nov 02 09:43:16 2006 C:\Windows\system32\schannel.dll
        75b80000 4549bd69 Nov 02 09:42:01 2006 < Name not readable >
        757d0000 4549be27 Nov 02 09:45:11 2006 C:\Windows\System32\wshtcpip.dll
        75be0000 4549be21 Nov 02 09:45:05 2006 < Name not readable >
        735b0000 4ba1f41f Mar 18 09:36:31 2010
C:\Windows\assembly\NativeImages_v4.0.30319_32\SMDiagnostics\4d2a51c03b27e615ff9f1c430f2014ba\SMDiagnostics.ni.dll
        6d310000 4ba1f421 Mar 18 09:36:33 2010
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runtime.Dura#\f3989d3e9cb8904e4edf23ede5adb6c1\System.Runtime.Du
rableInstancing.ni.dll
        73fc0000 4549be18 Nov 02 09:44:56 2006 < Name not readable >
        75d90000 4549bd3f Nov 02 09:41:19 2006 C:\Windows\system32\iphlpapi.dll
        75d50000 4549bcc6 Nov 02 09:39:18 2006 C:\Windows\system32\dhcpcsvc.DLL
        75d40000 4549be1e Nov 02 09:45:02 2006 < Name not readable >
        75d20000 4549bcc7 Nov 02 09:39:19 2006 C:\Windows\system32\dhcpcsvc6.DLL
        753e0000 4549bd6b Nov 02 09:42:03 2006 < Name not readable >
        738b0000 4549be1f Nov 02 09:45:03 2006 < Name not readable >
        738e0000 4549bd3b Nov 02 09:41:15 2006 C:\Windows\system32\napinsp.dll
        73560000 4549bdc0 Nov 02 09:43:28 2006 C:\Windows\system32\pnrpnsp.dll
        75bf0000 4549bde4 Nov 02 09:44:04 2006 C:\Windows\system32\VERSION.dll
        6b8f0000 4ba1e3c9 Mar 18 08:26:49 2010
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Data.Linq\87a713cee613d08ee04ae9483a9d4716\System.Data.Linq.ni.d
ll
        738a0000 4549bda2 Nov 02 09:42:58 2006 < Name not readable >
        676a0000 4ba1dfe7 Mar 18 08:10:15 2010
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Data.SqlXml\1fdd0961d8d07ef4d1fcaf30f0050c0a\System.Data.SqlXml.
ni.dll
        71340000 4ba1e09d Mar 18 08:13:17 2010
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Transactions\dd9dbf82e44454689976a49a9e4ddb6d\System.Transaction
s.ni.dll
        6fbc0000 4ba1e09d Mar 18 08:13:17 2010
C:\Windows\Microsoft.Net\assembly\GAC_32\System.Transactions\v4.0_4.0.0.0__b77a5c561934e089\System.Transactions.dll
        71900000 4ba1dfda Mar 18 08:10:02 2010
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Numerics\b07f0d26a34ad53fc369248f289d1126\System.Numerics.ni.dll
        6bd00000 4ba1df90 Mar 18 08:08:48 2010
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.EnterpriseSe#\8b6e9d6171aad3561263ce2cd05c57df\System.Enterprise
Services.ni.dll
```

```
        6e320000 4ba1df78 Mar 18 08:08:24 2010
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Security\09a97525ae5583cc2685e2c39a3078bd\System.Security.ni.dll
        67320000 4ba1f6f8 Mar 18 09:48:40 2010
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\035910922f160d304fb834aae41f45a6\System.Xaml.ni.dll
        64d30000 00000000 Jan 01 00:00:00 1970
    SubSystemData:     00000000
    ProcessHeap:       001e0000
    ProcessParameters: 001e0f48
    CurrentDirectory:  'C:\LINQPad4\'
    WindowTitle:  'C:\LINQPad4\LINQPad.exe'
    ImageFile:    'C:\LINQPad4\LINQPad.exe'
    CommandLine:  '"C:\LINQPad4\LINQPad.exe" '
    DllPath:
'C:\LINQPad4;C:\Windows\system32;C:\Windows\system;C:\Windows;.;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbe
m'
    Environment:  001e07e8
        =::=::\
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\Training\AppData\Roaming
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=LH-KTCYRPBZYQHY
        ComSpec=C:\Windows\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        HOMEDRIVE=C:
        HOMEPATH=\Users\Training
        LOCALAPPDATA=C:\Users\Training\AppData\Local
        LOGONSERVER=\\LH-KTCYRPBZYQHY
        NUMBER_OF_PROCESSORS=2
        OS=Windows_NT
        Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 42 Stepping 7, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=2a07
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        PUBLIC=C:\Users\Public
        SESSIONNAME=Console
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Users\Training\AppData\Local\Temp
        TMP=C:\Users\Training\AppData\Local\Temp
        USERDOMAIN=LH-KTCYRPBZYQHY
        USERNAME=Training
        USERPROFILE=C:\Users\Training
        windir=C:\Windows


        THREAD 83127030  Cid 6245c.62460  Teb: 7ffdf000 Win32Thread: fe6f90c0 WAIT: (WrUserRequest) UserMode Non-
Alertable
            a3248188  SynchronizationEvent
        Not impersonating
        DeviceMap                 9b2d5900
        Owning Process            8312f800       Image:         LINQPad.exe
        Attached Process          N/A            Image:         N/A
        Wait Start TickCount      1543531        Ticks: 2 (0:00:00:00.031)
        Context Switch Count      33406
        UserTime                  00:00:03.218
        KernelTime                00:00:07.031
*** ERROR: Module load completed but symbols could not be loaded for LINQPad.exe
        Win32 Start Address LINQPad (0x0114e4ae)
        Stack Init 99dcc000 Current 99dcbc10 Base 99dcc000 Limit 99dc9000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
*** WARNING: Unable to verify timestamp for System.Windows.Forms.ni.dll
*** ERROR: Module load completed but symbols could not be loaded for System.Windows.Forms.ni.dll
```

```
        ChildEBP RetAddr
        99dcbc28 818ac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        99dcbc64 81829308 nt!KiSwapThread+0x389
        99dcbcc0 8c2db89d nt!KeWaitForSingleObject+0x414
        99dcbd1c 8c2db6d4 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        99dcbd38 8c2d571c win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        99dcbd4c 8c2d5739 win32k!xxxRealWaitMessageEx+0x12 (FPO: [Non-Fpo])
        99dcbd5c 8188c96a win32k!NtUserWaitMessage+0x14 (FPO: [0,0,4])
        99dcbd5c 77c40f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 99dcbd64)
        0014e75c 7674b5b4 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0014e760 67b3737a USER32!NtUserWaitMessage+0xc (FPO: [0,0,0])
WARNING: Stack unwind information not available. Following frames may be wrong.
        0014e7f4 67b36e2c System_Windows_Forms_ni+0x22737a
        0014e850 67b36c81 System_Windows_Forms_ni+0x226e2c
        0014e880 67ac366d System_Windows_Forms_ni+0x226c81
        0014e898 00d73f0d System_Windows_Forms_ni+0x1b366d
        0014e97c 00d71515 0xd73f0d
        0014ec24 6af221db 0xd71515
        0014ec34 6af44a2a clr!CallDescrWorker+0x33
        0014ecb0 6af44bcc clr!CallDescrWorkerWithHandler+0x8e (FPO: [Non-Fpo])
        0014ede8 6af44c01 clr!MethodDesc::CallDescr+0x194 (FPO: [Non-Fpo])
        0014ee04 6af44c21 clr!MethodDesc::CallTargetWorker+0x21 (FPO: [Non-Fpo])
        0014ee1c 6b00ce82 clr!MethodDescCallSite::Call+0x1c (FPO: [Non-Fpo])
        0014ef80 6b00cf90 clr!ClassLoader::RunMain+0x24c (FPO: [Non-Fpo])
        0014f1e8 00000000 clr!Assembly::ExecuteMainMethod+0xc1 (FPO: [Non-Fpo])

        THREAD 8380c030  Cid 6245c.62474  Teb: 7ffde000 Win32Thread: 00000000 WAIT: (UserRequest) UserMode Non-
Alertable
            8ae8c3e0  SynchronizationEvent
            83298f88  SynchronizationEvent
            8af598f8  SynchronizationEvent
        Not impersonating
        DeviceMap                 9b2d5900
        Owning Process            8312f800       Image:         LINQPad.exe
        Attached Process          N/A            Image:         N/A
        Wait Start TickCount      1508811        Ticks: 34722 (0:00:09:02.531)
        Context Switch Count      5
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address clr!DebuggerRCThread::ThreadProcStatic (0x6b08741c)
        Stack Init 9cb2c000 Current 9cb2b8d0 Base 9cb2c000 Limit 9cb29000 Call 0
        Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.

        THREAD 8412bd78  Cid 6245c.62478  Teb: 7ffdc000 Win32Thread: fe9ffe98 WAIT: (WrUserRequest) UserMode Non-
Alertable
            830a87a0  SynchronizationEvent
        Not impersonating
        DeviceMap                 9b2d5900
        Owning Process            8312f800       Image:         LINQPad.exe
        Attached Process          N/A            Image:         N/A
        Wait Start TickCount      1539998        Ticks: 3535 (0:00:00:55.234)
        Context Switch Count      694
        UserTime                  00:00:00.031
        KernelTime                00:00:00.062
        Win32 Start Address clr!Thread::intermediateThreadProc (0x6afd59c0)
        Stack Init 97ca6000 Current 97ca5c10 Base 97ca6000 Limit 97ca3000 Call 0
        Priority 12 BasePriority 10 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        97ca5c28 818ac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        97ca5c64 81829308 nt!KiSwapThread+0x389
        97ca5cc0 8c2db89d nt!KeWaitForSingleObject+0x414
        97ca5d1c 8c2db6d4 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        97ca5d38 8c2d571c win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        97ca5d4c 8c2d5739 win32k!xxxRealWaitMessageEx+0x12 (FPO: [Non-Fpo])
```

```
        97ca5d5c 8188c96a win32k!NtUserWaitMessage+0x14 (FPO: [0,0,4])
        97ca5d5c 77c40f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 97ca5d64)
        039be32c 7674b5b4 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        039be330 67b3737a USER32!NtUserWaitMessage+0xc (FPO: [0,0,0])
WARNING: Stack unwind information not available. Following frames may be wrong.
        039be3c4 67b36e2c System_Windows_Forms_ni+0x22737a
        039be420 67b36c81 System_Windows_Forms_ni+0x226e2c
        039be450 6802fefb System_Windows_Forms_ni+0x226c81
        039be468 68059f83 System_Windows_Forms_ni+0x71fefb
        039be504 6805a1b7 System_Windows_Forms_ni+0x749f83
        039be544 6af221db System_Windows_Forms_ni+0x74a1b7
        039be554 6af44a2a clr!CallDescrWorker+0x33
        039be5d0 6af44bcc clr!CallDescrWorkerWithHandler+0x8e (FPO: [Non-Fpo])
        039be720 6af44c01 clr!MethodDesc::CallDescr+0x194 (FPO: [Non-Fpo])
        039be73c 6b192379 clr!MethodDesc::CallTargetWorker+0x21 (FPO: [Non-Fpo])
        039be834 6b134ad1 clr!ExceptionNotifications::DeliverExceptionNotification+0x98 (FPO: [Non-Fpo])
        039be8a8 6b134e86 clr!COMDelegate::BindToMethodInfo+0x504 (FPO: [Non-Fpo])
        039be94c 6b11c19b clr!DistributeUnhandledExceptionReliably+0xeb (FPO: [Non-Fpo])
        039be9a4 6b11bfd3 clr!AppDomain::RaiseUnhandledExceptionEvent+0xba (FPO: [Non-Fpo])
        039bea3c 6b0a8688 clr!AppDomain::RaiseUnhandledExceptionEvent_Wrapper+0x1cd (FPO: [Non-Fpo])
        039beb14 6b11c13e clr!Thread::DoADCallBack+0xe0 (FPO: [Non-Fpo])
        039beb70 6b11de38 clr!AppDomain::RaiseUnhandledExceptionEvent+0xc2 (FPO: [Non-Fpo])
        039bebe4 6b11e807 clr!AppDomain::RaiseUnhandledExceptionEventNoThrow+0x7a (FPO: [Non-Fpo])
        039bec40 6b19518a clr!AppDomain::OnUnhandledException+0x81 (FPO: [Non-Fpo])
        039bed58 6b1969c1 clr!NotifyAppDomainsOfUnhandledException+0x141 (FPO: [Non-Fpo])
        039bef48 6b196f8f clr!DefaultCatchHandler+0xdb (FPO: [Non-Fpo])
        039bef74 6b01c411 clr!DefaultCatchHandler+0x623 (FPO: [Non-Fpo])
        039bef84 6b01c45b clr!ThreadBaseExceptionAppDomainFilter+0x13 (FPO: [Non-Fpo])
        039befbc 6b01c4df clr!ManagedThreadCallState::IsAppDomainEqual+0x9c (FPO: [Non-Fpo])
        039befc4 71262b04 clr!Thread::ShouldChangeAbortToUnload+0x3af (FPO: [SEH])
        039befd8 71284ae4 MSVCR100_CLR0400!_EH4_CallFilterFunc+0x12 (FPO: [Uses EBP] [0,0,4])
        039bf004 6aff14b8 MSVCR100_CLR0400!_except_handler4_common+0x8e (FPO: [Non-Fpo])
        039bf024 77c41039 clr!_except_handler4+0x20 (FPO: [Non-Fpo])
        039bf048 77c4100b ntdll!ExecuteHandler2+0x26
        039bf0f0 77c40e97 ntdll!ExecuteHandler+0x24

        THREAD 83cb5920  Cid 6245c.6247c  Teb: 7ffdb000 Win32Thread: 00000000 WAIT: (Executive) UserMode Non-Alertable
            84b2faac  NotificationEvent
        IRP List:
            896f84d8: (0006,0094) Flags: 00060800  Mdl: 00000000
        Not impersonating
        DeviceMap                 9b2d5900
        Owning Process            8312f800       Image:         LINQPad.exe
        Attached Process          N/A            Image:         N/A
        Wait Start TickCount      1508811        Ticks: 34722 (0:00:09:02.531)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address clr!Thread::intermediateThreadProc (0x6afd59c0)
        Stack Init 98614000 Current 98613b80 Base 98614000 Limit 98611000 Call 0
        Priority 8 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
        Kernel stack not resident.

        THREAD 8979ed78  Cid 6245c.62480  Teb: 7ffda000 Win32Thread: fee5a3b8 WAIT: (UserRequest) UserMode Non-
Alertable
            830c6d48  NotificationEvent
            8affdc20  SynchronizationEvent
        Not impersonating
        DeviceMap                 9b2d5900
        Owning Process            8312f800       Image:         LINQPad.exe
        Attached Process          N/A            Image:         N/A
        Wait Start TickCount      1536557        Ticks: 6976 (0:00:01:49.000)
        Context Switch Count      38
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address gdiplus!BackgroundThreadProc (0x74d01909)
```

```
Stack Init 88818000 Current 888178d0 Base 88818000 Limit 88815000 Call 0
Priority 10 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
ChildEBP RetAddr
888178e8 818ac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
88817924 81828bc5 nt!KiSwapThread+0x389
88817970 819f55b1 nt!KeWaitForMultipleObjects+0x47d
88817bfc 819f5219 nt!ObpWaitForMultipleObjects+0x256
88817d48 8188c96a nt!NtWaitForMultipleObjects+0xcc
88817d48 77c40f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 88817d64)
04a4f954 77c40690 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
04a4f958 76577e09 ntdll!ZwWaitForMultipleObjects+0xc (FPO: [5,0,0])
04a4f9f4 7674c4af KERNEL32!WaitForMultipleObjectsEx+0x11d (FPO: [Non-Fpo])
04a4fa48 76748b7b USER32!RealMsgWaitForMultipleObjectsEx+0x13c (FPO: [Non-Fpo])
04a4fa64 74d01965 USER32!MsgWaitForMultipleObjects+0x1f (FPO: [Non-Fpo])
04a4fab0 76573833 gdiplus!BackgroundThreadProc+0x59 (FPO: [Non-Fpo])
04a4fabc 77c1a9bd KERNEL32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
04a4fafc 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])

THREAD 897c0630  Cid 6245c.624a0  Teb: 7ffd5000 Win32Thread: fd3b44b0 WAIT: (UserRequest) UserMode Alertable
    8351db88  NotificationEvent
Not impersonating
DeviceMap                 9b2d5900
Owning Process            8312f800       Image:         LINQPad.exe
Attached Process          N/A            Image:         N/A
Wait Start TickCount      1508811        Ticks: 34722 (0:00:09:02.531)
Context Switch Count      215
UserTime                  00:00:00.312
KernelTime                00:00:00.046
Win32 Start Address clr!Thread::intermediateThreadProc (0x6afd59c0)
Stack Init 99d9c000 Current 99d9b8d0 Base 99d9c000 Limit 99d99000 Call 0
Priority 10 BasePriority 7 PriorityDecrement 2 IoPriority 2 PagePriority 5
Kernel stack not resident.

THREAD a32b2c60  Cid 6245c.62518  Teb: 7ffd9000 Win32Thread: fd3ad548 WAIT: (UserRequest) UserMode Alertable
    847f9148  SynchronizationEvent
Not impersonating
DeviceMap                 9b2d5900
Owning Process            8312f800       Image:         LINQPad.exe
Attached Process          N/A            Image:         N/A
Wait Start TickCount      1508811        Ticks: 34722 (0:00:09:02.531)
Context Switch Count      377
UserTime                  00:00:01.109
KernelTime                00:00:00.281
Win32 Start Address clr!Thread::intermediateThreadProc (0x6afd59c0)
Stack Init 8881c000 Current 8881b8d0 Base 8881c000 Limit 88819000 Call 0
Priority 6 BasePriority 6 PriorityDecrement 0 IoPriority 2 PagePriority 5
Kernel stack not resident.

THREAD a3276030  Cid 6245c.62524  Teb: 7ff4f000 Win32Thread: 00000000 WAIT: (WrQueue) UserMode Non-Alertable
    896b2768  QueueObject
Not impersonating
DeviceMap                 9b2d5900
Owning Process            8312f800       Image:         LINQPad.exe
Attached Process          N/A            Image:         N/A
Wait Start TickCount      1508811        Ticks: 34722 (0:00:09:02.531)
Context Switch Count      15
UserTime                  00:00:00.000
KernelTime                00:00:00.000
Win32 Start Address clr!Thread::intermediateThreadProc (0x6afd59c0)
Stack Init 99dac000 Current 99dabbc8 Base 99dac000 Limit 99da9000 Call 0
Priority 10 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
Kernel stack not resident.
```

```
        THREAD 830b79d8  Cid 6245c.62544  Teb: 7ff4c000 Win32Thread: 00000000 WAIT: (UserRequest) UserMode Non-
Alertable
            84891d28  SynchronizationEvent
        Not impersonating
        DeviceMap                 9b2d5900
        Owning Process            8312f800       Image:         LINQPad.exe
        Attached Process          N/A            Image:         N/A
        Wait Start TickCount      1508811        Ticks: 34722 (0:00:09:02.531)
        Context Switch Count      4
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address clr!Thread::intermediateThreadProc (0x6afd59c0)
        Stack Init 99d64000 Current 99d63c38 Base 99d64000 Limit 99d61000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        Kernel stack not resident.

        THREAD 832abd78  Cid 6245c.62548  Teb: 7ff4b000 Win32Thread: ff435e98 WAIT: (UserRequest) UserMode Alertable
            830b9a40  Thread
            8967b5f8  SynchronizationEvent
        Not impersonating
        DeviceMap                 9b2d5900
        Owning Process            8312f800       Image:         LINQPad.exe
        Attached Process          N/A            Image:         N/A
        Wait Start TickCount      1509126        Ticks: 34407 (0:00:08:57.609)
        Context Switch Count      31
        UserTime                  00:00:00.046
        KernelTime                00:00:00.015
        Win32 Start Address clr!Thread::intermediateThreadProc (0x6afd59c0)
        Stack Init 98724000 Current 987238d0 Base 98724000 Limit 98721000 Call 0
        Priority 13 BasePriority 8 PriorityDecrement 3 IoPriority 2 PagePriority 5
        Kernel stack not resident.

        THREAD 830b9a40  Cid 6245c.6254c  Teb: 7ff4d000 Win32Thread: ffbcc398 WAIT: (WrUserRequest) UserMode Non-
Alertable
            84b48ce8  SynchronizationEvent
        Not impersonating
        DeviceMap                 9b2d5900
        Owning Process            8312f800       Image:         LINQPad.exe
        Attached Process          N/A            Image:         N/A
        Wait Start TickCount      1539999        Ticks: 3534 (0:00:00:55.218)
        Context Switch Count      596
        UserTime                  00:00:00.031
        KernelTime                00:00:00.031
        Win32 Start Address clr!Thread::intermediateThreadProc (0x6afd59c0)
        Stack Init 9c9a3000 Current 9c9a2c10 Base 9c9a3000 Limit 9c9a0000 Call 0
        Priority 12 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        9c9a2c28 818ac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        9c9a2c64 81829308 nt!KiSwapThread+0x389
        9c9a2cc0 8c2db89d nt!KeWaitForSingleObject+0x414
        9c9a2d1c 8c2db6d4 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        9c9a2d38 8c2d571c win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        9c9a2d4c 8c2d5739 win32k!xxxRealWaitMessageEx+0x12 (FPO: [Non-Fpo])
        9c9a2d5c 8188c96a win32k!NtUserWaitMessage+0x14 (FPO: [0,0,4])
        9c9a2d5c 77c40f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 9c9a2d64)
        0a62dd4c 7674b5b4 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0a62dd50 67b3737a USER32!NtUserWaitMessage+0xc (FPO: [0,0,0])
WARNING: Stack unwind information not available. Following frames may be wrong.
        0a62dde4 67b36e2c System_Windows_Forms_ni+0x22737a
        0a62de40 67b36c81 System_Windows_Forms_ni+0x226e2c
        0a62de70 6802fefb System_Windows_Forms_ni+0x226c81
        0a62de88 68059f83 System_Windows_Forms_ni+0x71fefb
        0a62df24 6805a1b7 System_Windows_Forms_ni+0x749f83
        0a62df64 6af221db System_Windows_Forms_ni+0x74a1b7
        0a62df74 6af44a2a clr!CallDescrWorker+0x33
        0a62dff0 6af44bcc clr!CallDescrWorkerWithHandler+0x8e (FPO: [Non-Fpo])
```

```
        0a62e140 6af44c01 clr!MethodDesc::CallDescr+0x194 (FPO: [Non-Fpo])
        0a62e15c 6b192379 clr!MethodDesc::CallTargetWorker+0x21 (FPO: [Non-Fpo])
        0a62e254 6b134ad1 clr!ExceptionNotifications::DeliverExceptionNotification+0x98 (FPO: [Non-Fpo])
        0a62e2c8 6b134e86 clr!COMDelegate::BindToMethodInfo+0x504 (FPO: [Non-Fpo])
        0a62e36c 6b11c19b clr!DistributeUnhandledExceptionReliably+0xeb (FPO: [Non-Fpo])
        0a62e3c4 6b11bfd3 clr!AppDomain::RaiseUnhandledExceptionEvent+0xba (FPO: [Non-Fpo])
        0a62e45c 6b0a8688 clr!AppDomain::RaiseUnhandledExceptionEvent_Wrapper+0x1cd (FPO: [Non-Fpo])
        0a62e534 6b11c13e clr!Thread::DoADCallBack+0xe0 (FPO: [Non-Fpo])
        0a62e590 6b11de38 clr!AppDomain::RaiseUnhandledExceptionEvent+0xc2 (FPO: [Non-Fpo])
        0a62e604 6b11e807 clr!AppDomain::RaiseUnhandledExceptionEventNoThrow+0x7a (FPO: [Non-Fpo])
        0a62e660 6b19518a clr!AppDomain::OnUnhandledException+0x81 (FPO: [Non-Fpo])
        0a62e774 6b1969c1 clr!NotifyAppDomainsOfUnhandledException+0x141 (FPO: [Non-Fpo])
        0a62e964 6b196f8f clr!DefaultCatchHandler+0xdb (FPO: [Non-Fpo])
        0a62e990 6b01c411 clr!DefaultCatchHandler+0x623 (FPO: [Non-Fpo])
        0a62e9a0 6b01c45b clr!ThreadBaseExceptionAppDomainFilter+0x13 (FPO: [Non-Fpo])
        0a62e9d8 6b01c4df clr!ManagedThreadCallState::IsAppDomainEqual+0x9c (FPO: [Non-Fpo])
        0a62e9e0 71262b04 clr!Thread::ShouldChangeAbortToUnload+0x3af (FPO: [SEH])
        0a62e9f4 71284ae4 MSVCR100_CLR0400!_EH4_CallFilterFunc+0x12 (FPO: [Uses EBP] [0,0,4])
        0a62ea20 6aff14b8 MSVCR100_CLR0400!_except_handler4_common+0x8e (FPO: [Non-Fpo])
        0a62ea40 77c41039 clr!_except_handler4+0x20 (FPO: [Non-Fpo])
        0a62ea64 77c4100b ntdll!ExecuteHandler2+0x26
        0a62eb0c 77c40e97 ntdll!ExecuteHandler+0x24

        THREAD 831a2d78  Cid 6245c.62558  Teb: 7ff48000 Win32Thread: fe7d20c0 WAIT: (WrUserRequest) UserMode Non-
Alertable
            83107f18  SynchronizationEvent
        Not impersonating
        DeviceMap                 9b2d5900
        Owning Process            8312f800       Image:         LINQPad.exe
        Attached Process          N/A            Image:         N/A
        Wait Start TickCount      1539999        Ticks: 3534 (0:00:00:55.218)
        Context Switch Count      792
        UserTime                  00:00:00.031
        KernelTime                00:00:00.046
        Win32 Start Address clr!Thread::intermediateThreadProc (0x6afd59c0)
        Stack Init 99d8c000 Current 99d8bc10 Base 99d8c000 Limit 99d89000 Call 0
        Priority 11 BasePriority 8 PriorityDecrement 1 IoPriority 2 PagePriority 5
        Kernel stack not resident.
        ChildEBP RetAddr
        99d8bc28 818ac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        99d8bc64 81829308 nt!KiSwapThread+0x389
        99d8bcc0 8c2db89d nt!KeWaitForSingleObject+0x414
        99d8bd1c 8c2db6d4 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
        99d8bd38 8c2d571c win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
        99d8bd4c 8c2d5739 win32k!xxxRealWaitMessageEx+0x12 (FPO: [Non-Fpo])
        99d8bd5c 8188c96a win32k!NtUserWaitMessage+0x14 (FPO: [0,0,4])
        99d8bd5c 77c40f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 99d8bd64)
        0b13da8c 7674b5b4 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        0b13da90 67b3737a USER32!NtUserWaitMessage+0xc (FPO: [0,0,0])
WARNING: Stack unwind information not available. Following frames may be wrong.
        0b13db24 67b36e2c System_Windows_Forms_ni+0x22737a
        0b13db80 67b36c81 System_Windows_Forms_ni+0x226e2c
        0b13dbb0 6802fefb System_Windows_Forms_ni+0x226c81
        0b13dbc8 68059f83 System_Windows_Forms_ni+0x71fefb
        0b13dc64 6805a1b7 System_Windows_Forms_ni+0x749f83
        0b13dca4 6af221db System_Windows_Forms_ni+0x74a1b7
        0b13dcb4 6af44a2a clr!CallDescrWorker+0x33
        0b13dd30 6af44bcc clr!CallDescrWorkerWithHandler+0x8e (FPO: [Non-Fpo])
        0b13de80 6af44c01 clr!MethodDesc::CallDescr+0x194 (FPO: [Non-Fpo])
        0b13de9c 6b192379 clr!MethodDesc::CallTargetWorker+0x21 (FPO: [Non-Fpo])
        0b13df94 6b134ad1 clr!ExceptionNotifications::DeliverExceptionNotification+0x98 (FPO: [Non-Fpo])
        0b13e008 6b134e86 clr!COMDelegate::BindToMethodInfo+0x504 (FPO: [Non-Fpo])
        0b13e0ac 6b11c19b clr!DistributeUnhandledExceptionReliably+0xeb (FPO: [Non-Fpo])
        0b13e104 6b11bfd3 clr!AppDomain::RaiseUnhandledExceptionEvent+0xba (FPO: [Non-Fpo])
        0b13e19c 6b0a8688 clr!AppDomain::RaiseUnhandledExceptionEvent_Wrapper+0x1cd (FPO: [Non-Fpo])
        0b13e274 6b11c13e clr!Thread::DoADCallBack+0xe0 (FPO: [Non-Fpo])
```

```
0b13e2d0 6b11de38 clr!AppDomain::RaiseUnhandledExceptionEvent+0xc2 (FPO: [Non-Fpo])
0b13e344 6b11e807 clr!AppDomain::RaiseUnhandledExceptionEventNoThrow+0x7a (FPO: [Non-Fpo])
0b13e3a0 6b19518a clr!AppDomain::OnUnhandledException+0x81 (FPO: [Non-Fpo])
0b13e4bc 6b1969c1 clr!NotifyAppDomainsOfUnhandledException+0x141 (FPO: [Non-Fpo])
0b13e6ac 6b196f8f clr!DefaultCatchHandler+0xdb (FPO: [Non-Fpo])
0b13e6d8 6b01c411 clr!DefaultCatchHandler+0x623 (FPO: [Non-Fpo])
0b13e6e8 6b01c45b clr!ThreadBaseExceptionAppDomainFilter+0x13 (FPO: [Non-Fpo])
0b13e720 6b01c4df clr!ManagedThreadCallState::IsAppDomainEqual+0x9c (FPO: [Non-Fpo])
0b13e728 71262b04 clr!Thread::ShouldChangeAbortToUnload+0x3af (FPO: [SEH])
0b13e73c 71284ae4 MSVCR100_CLR0400!_EH4_CallFilterFunc+0x12 (FPO: [Uses EBP] [0,0,4])
0b13e768 6aff14b8 MSVCR100_CLR0400!_except_handler4_common+0x8e (FPO: [Non-Fpo])
0b13e788 77c41039 clr!_except_handler4+0x20 (FPO: [Non-Fpo])
0b13e7ac 77c4100b ntdll!ExecuteHandler2+0x26
0b13e854 77c40e97 ntdll!ExecuteHandler+0x24

THREAD 83343c60  Cid 6245c.30f74  Teb: 7ffd8000 Win32Thread: 00000000 WAIT: (WrQueue) UserMode Non-Alertable
    8334b820  QueueObject
Not impersonating
DeviceMap                 9b2d5900
Owning Process            8312f800       Image:         LINQPad.exe
Attached Process          N/A            Image:         N/A
Wait Start TickCount      1511025        Ticks: 32508 (0:00:08:27.937)
Context Switch Count      42
UserTime                  00:00:00.000
KernelTime                00:00:00.015
Win32 Start Address RPCRT4!ThreadStartRoutine (0x7665ace5)
Stack Init 98644000 Current 98643bc8 Base 98644000 Limit 98641000 Call 0
Priority 9 BasePriority 8 PriorityDecrement 0 IoPriority 2 PagePriority 5
Kernel stack not resident.

THREAD a217cd78  Cid 6245c.30ff8  Teb: 7ffd7000 Win32Thread: 00000000 WAIT: (UserRequest) UserMode Non-
Alertable
    83325548  SynchronizationEvent
    a217ce00  NotificationTimer
Not impersonating
DeviceMap                 9b2d5900
Owning Process            8312f800       Image:         LINQPad.exe
Attached Process          N/A            Image:         N/A
Wait Start TickCount      1543033        Ticks: 500 (0:00:00:07.812)
Context Switch Count      27
UserTime                  00:00:00.000
KernelTime                00:00:00.000
Win32 Start Address clr!WKS::gc_heap::gc_thread_stub (0x6afd5751)
Stack Init 88db1000 Current 88db0c38 Base 88db1000 Limit 88dae000 Call 0
Priority 10 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
ChildEBP RetAddr
88db0c50 818ac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
88db0c8c 81829308 nt!KiSwapThread+0x389
88db0ce8 819f50ef nt!KeWaitForSingleObject+0x414
88db0d50 8188c96a nt!NtWaitForSingleObject+0xbe
88db0d50 77c40f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 88db0d64)
076df6bc 77c406a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
076df6c0 765777d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
076df730 6af81030 KERNEL32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
076df764 6af81071 clr!CLREvent::CreateManualEvent+0xf6 (FPO: [Non-Fpo])
076df7b4 6af7d3e8 clr!CLREvent::CreateManualEvent+0x137 (FPO: [Non-Fpo])
076df7f4 6af7d409 clr!CLREvent::WaitEx+0x126 (FPO: [Non-Fpo])
076df808 6afd5704 clr!CLREvent::Wait+0x19 (FPO: [Non-Fpo])
076df82c 6afd577a clr!WKS::gc_heap::gc_thread_function+0x3a (FPO: [Non-Fpo])
076df830 76573833 clr!WKS::gc_heap::gc_thread_stub+0x29 (FPO: [1,0,0])
076df83c 77c1a9bd KERNEL32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
076df87c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Note: We can see some CLR threads. Some thread stacks are paged out, for example, for the thread 897c0630. We switch to the thread 831a2d78 to get a better stack trace:

```
1: kd> .thread /r /p 831a2d78
Implicit thread is now 831a2d78
Implicit process is now 8312f800
Loading User Symbols
..................Unable to read NT module Base Name string at 00220f82 - NTSTATUS 0xC0000147
Missing image name, possible paged-out or corrupt data.
...............................Unable to read NT module Base Name string at 00266eaa - NTSTATUS 0xC0000147
Missing image name, possible paged-out or corrupt data.
................
......Unable to read NT module Base Name string at 002dea60 - NTSTATUS 0xC0000147
..Unable to read NT module Base Name string at 002deaa8 - NTSTATUS 0xC0000147
...Unable to read NT module Base Name string at 002deaf0 - NTSTATUS 0xC0000147
...Unable to read NT module Base Name string at 002dee50 - NTSTATUS 0xC0000147
Missing image name, possible paged-out or corrupt data.
..Unable to read NT module Base Name string at 002deee0 - NTSTATUS 0xC0000147
.Unable to read NT module Base Name string at 002def28 - NTSTATUS 0xC0000147
.....Unable to read NT module Base Name string at 050ccf48 - NTSTATUS 0xC0000147
Missing image name, possible paged-out or corrupt data.
........Unable to read LDR_DATA_TABLE_ENTRY at 050cbfd8 - HRESULT 0x80004005

WARNING: .reload failed, module list may be incomplete

1: kd> kv
  *** Stack trace for last set context - .thread/.cxr resets it
ChildEBP RetAddr  Args to Child
99d8bc28 818ac9cf 831a2e00 831a2d78 831a2e30 nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
99d8bc64 81829308 831a2d78 00000000 fe7d20c0 nt!KiSwapThread+0x389
99d8bcc0 8c2db89d 83107f18 0000000d 00000001 nt!KeWaitForSingleObject+0x414
99d8bd1c 8c2db6d4 000024ff 00000000 00000001 win32k!xxxRealSleepThread+0x1ad (FPO: [Non-Fpo])
99d8bd38 8c2d571c 000024ff 00000000 00000001 win32k!xxxSleepThread+0x2d (FPO: [Non-Fpo])
99d8bd4c 8c2d5739 000024ff 00000000 0b13da98 win32k!xxxRealWaitMessageEx+0x12 (FPO: [Non-Fpo])
99d8bd5c 8188c96a 0b13db24 77c40f34 badb0d00 win32k!NtUserWaitMessage+0x14 (FPO: [0,0,4])
99d8bd5c 77c40f34 0b13db24 77c40f34 badb0d00 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 99d8bd64)
0b13da8c 7674b5b4 67b3737a bb1f3dee 6af25d80 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
*** WARNING: Unable to verify timestamp for System.Windows.Forms.ni.dll
*** ERROR: Module load completed but symbols could not be loaded for System.Windows.Forms.ni.dll
0b13da90 67b3737a bb1f3dee 6af25d80 0b13dbd4 USER32!NtUserWaitMessage+0xc (FPO: [0,0,0])
WARNING: Stack unwind information not available. Following frames may be wrong.
0b13db24 67b36e2c 00000000 00000004 00000000 System_Windows_Forms_ni+0x22737a
0b13db80 67b36c81 098cd560 00000000 00000000 System_Windows_Forms_ni+0x226e2c
0b13dbb0 6802fefb 0994c0b8 00000000 00772010 System_Windows_Forms_ni+0x226c81
0b13dbc8 68059f83 bb1f3dee 6af25d80 0b13e030 System_Windows_Forms_ni+0x71fefb
0b13dc64 6805a1b7 0543a204 09907aa0 09907aa0 System_Windows_Forms_ni+0x749f83
0b13dca4 6af221db ffffffff 6af30bcc 0b13dd30 System_Windows_Forms_ni+0x74a1b7
0b13dcb4 6af44a2a 0b13dd84 00000001 0b13dd50 clr!CallDescrWorker+0x33
0b13dd30 6af44bcc 0b13dd84 00000001 0b13dd50 clr!CallDescrWorkerWithHandler+0x8e (FPO: [Non-Fpo])
0b13de80 6af44c01 6957ced8 0b13dec8 0b13df78 clr!MethodDesc::CallDescr+0x194 (FPO: [Non-Fpo])
0b13de9c 6b192379 6957ced8 0b13dec8 0b13df78 clr!MethodDesc::CallTargetWorker+0x21 (FPO: [Non-Fpo])
0b13df94 6b134ad1 00000001 0b13e0fc 0b13e184 clr!ExceptionNotifications::DeliverExceptionNotification+0x98 (FPO: [Non-
Fpo])
0b13e008 6b134e86 0b13e0fc 0b13e184 0b13e088 clr!COMDelegate::BindToMethodInfo+0x504 (FPO: [Non-Fpo])
0b13e0ac 6b11c19b 0b13e0fc 0b13e184 0b13e180 clr!DistributeUnhandledExceptionReliably+0xeb (FPO: [Non-Fpo])
0b13e104 6b11bfd3 0b13e184 0b13e180 00000000 clr!AppDomain::RaiseUnhandledExceptionEvent+0xba (FPO: [Non-Fpo])
0b13e19c 6b0a8688 0b13e2b0 b16ccf52 00000000 clr!AppDomain::RaiseUnhandledExceptionEvent_Wrapper+0x1cd (FPO: [Non-
Fpo])
0b13e274 6b11c13e 002017d0 6b11befb 0b13e2b0 clr!Thread::DoADCallBack+0xe0 (FPO: [Non-Fpo])
0b13e2d0 6b11de38 0b13e390 0b13e4a8 00000000 clr!AppDomain::RaiseUnhandledExceptionEvent+0xc2 (FPO: [Non-Fpo])
0b13e344 6b11e807 0b13e390 0b13e4a8 00000000 clr!AppDomain::RaiseUnhandledExceptionEventNoThrow+0x7a (FPO: [Non-Fpo])
0b13e3a0 6b19518a 0b13e4a8 00000000 0b13e4b0 clr!AppDomain::OnUnhandledException+0x81 (FPO: [Non-Fpo])
0b13e4bc 6b1969c1 0b13e750 0b13e594 00000000 clr!NotifyAppDomainsOfUnhandledException+0x141 (FPO: [Non-Fpo])
0b13e6ac 6b196f8f 0b13e750 00000000 00000000 clr!DefaultCatchHandler+0xdb (FPO: [Non-Fpo])
```

```
0b13e6d8 6b01c411 00000001 00000001 0b13e720 clr!DefaultCatchHandler+0x623 (FPO: [Non-Fpo])
0b13e6e8 6b01c45b 0b13e750 0b13f568 b16cca06 clr!ThreadBaseExceptionAppDomainFilter+0x13 (FPO: [Non-Fpo])
0b13e720 6b01c4df 0b13e750 71262b04 00000001 clr!ManagedThreadCallState::IsAppDomainEqual+0x9c (FPO: [Non-Fpo])
0b13e728 71262b04 00000001 0b13f344 6afd5d58 clr!Thread::ShouldChangeAbortToUnload+0x3af (FPO: [SEH])
0b13e73c 71284ae4 00000000 00000000 00000000 MSVCR100_CLR0400!_EH4_CallFilterFunc+0x12 (FPO: [Uses EBP] [0,0,4])
0b13e768 6aff14b8 6b509240 6af217d7 0b13e86c MSVCR100_CLR0400!_except_handler4_common+0x8e (FPO: [Non-Fpo])
0b13e788 77c41039 0b13e86c 0b13f334 0b13e894 clr!_except_handler4+0x20 (FPO: [Non-Fpo])
0b13e7ac 77c4100b 0b13e86c 0b13f334 0b13e894 ntdll!ExecuteHandler2+0x26
0b13e854 77c40e97 0b13c000 0b13e894 0b13e86c ntdll!ExecuteHandler+0x24
0b13e854 7654b09e 0b13c000 0b13e894 0b13e86c ntdll!KiUserExceptionDispatcher+0xf (FPO: [2,0,0]) (CONTEXT @ 0b13e894)
0b13ebb0 6afaac08 e0434352 00000001 00000005 KERNEL32!RaiseException+0x58 (FPO: [Non-Fpo])
0b13ec40 6afaae41 098e5728 00000000 00000000 clr!RaiseTheExceptionInternalOnly+0x276 (FPO: [Non-Fpo])
0b13ed00 056028bb 0b13ee60 6afaddc2 0b13f040 clr!IL_Throw+0x14c (FPO: [Non-Fpo])
*** WARNING: Unable to verify timestamp for Unknown_Module_69380000
*** ERROR: Module load completed but symbols could not be loaded for Unknown_Module_69380000
0b13edd0 6962ae5b 098d5948 0289922c 0b13edfc 0x56028bb
0b13ede0 695b7ff4 098aa838 00000000 098d5914 Unknown_Module_69380000+0x2aae5b
0b13edfc 695b7f34 00000000 098b3eec 00000000 Unknown_Module_69380000+0x237ff4
0b13ee1c 6962ade8 098d5914 00000000 05162dd0 Unknown_Module_69380000+0x237f34
0b13ee34 6af221db 00000000 00000000 0b13eec0 Unknown_Module_69380000+0x2aade8
0b13ee44 6af44a2a 0b13ef10 00000000 0b13eee0 clr!CallDescrWorker+0x33
0b13eec0 6af44bcc 0b13ef10 00000000 0b13eee0 clr!CallDescrWorkerWithHandler+0x8e (FPO: [Non-Fpo])
0b13eff8 6af44c01 69557c90 0b13f160 0b13f07c clr!MethodDesc::CallDescr+0x194 (FPO: [Non-Fpo])
0b13f014 6b0bb512 69557c90 0b13f160 0b13f07c clr!MethodDesc::CallTargetWorker+0x21 (FPO: [Non-Fpo])
0b13f220 6afd5c05 0b13f5f4 0b13f304 05162dd0 clr!ThreadNative::KickOffThread_Worker+0x1e1 (FPO: [Non-Fpo])
0b13f234 6afd5c87 0b13f568 b16cdfc2 0b13f568 clr!Thread::DoExtraWorkForFinalizer+0x114 (FPO: [Non-Fpo])
0b13f2e4 6afd5d42 0b13f568 b16cde62 05162dd0 clr!Thread::ShouldChangeAbortToUnload+0x101 (FPO: [Non-Fpo])
0b13f344 6afc37a2 05162dd0 0b13f430 6b0a6465 clr!Thread::ShouldChangeAbortToUnload+0x399 (FPO: [Non-Fpo])
0b13f350 6b0a6465 0b13f568 b16cd916 05162dd0 clr!Thread::RaiseCrossContextException+0x3f8 (FPO: [Non-Fpo])
0b13f430 6afc37cf 00000002 6afc378b 0b13f568 clr!Thread::DoADCallBack+0xf0 (FPO: [Non-Fpo])
0b13f450 6afd5c87 0b13f568 b16cd826 0b13f568 clr!Thread::DoExtraWorkForFinalizer+0xfa (FPO: [Non-Fpo])
0b13f500 6afd5d42 0b13f568 b16cd846 00000000 clr!Thread::ShouldChangeAbortToUnload+0x101 (FPO: [Non-Fpo])
0b13f560 6afd5dd9 00000002 00000000 00000001 clr!Thread::ShouldChangeAbortToUnload+0x399 (FPO: [Non-Fpo])
0b13f584 6b0bb3e5 00000002 6b0bb3e9 0b13f5f4 clr!Thread::ShouldChangeAbortToUnload+0x43a (FPO: [Non-Fpo])
0b13f59c 6b0bb2e0 00000002 6b0bb3e9 0b13f5f4 clr!ManagedThreadBase::KickOff+0x15 (FPO: [Non-Fpo])
0b13f634 6afd5a08 05168138 0b13f64c 00000000 clr!ThreadNative::KickOffThread+0x23e (FPO: [Non-Fpo])
0b13fed4 76573833 0514eb28 0b13ff20 77c1a9bd clr!Thread::intermediateThreadProc+0x4b (FPO: [Non-Fpo])
0b13fee0 77c1a9bd 0514eb28 0b13250b 00000000 KERNEL32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
0b13ff20 00000000 6afd59c0 0514eb28 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Note: First we use **.trap** command to get user space portion of the stack trace (as seen from process memory dump).

```
1: kd> kv
  *** Stack trace for last set context - .thread/.cxr resets it
ChildEBP RetAddr  Args to Child
0b13da8c 7674b5b4 67b3737a bb1f3dee 6af25d80 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
0b13da90 67b3737a bb1f3dee 6af25d80 0b13dbd4 USER32!NtUserWaitMessage+0xc (FPO: [0,0,0])
WARNING: Stack unwind information not available. Following frames may be wrong.
0b13db24 67b36e2c 00000000 00000004 00000000 System_Windows_Forms_ni+0x22737a
0b13db80 67b36c81 098cd560 00000000 00000000 System_Windows_Forms_ni+0x226e2c
0b13dbb0 6802fefb 0994c0b8 00000000 00772010 System_Windows_Forms_ni+0x226c81
0b13dbc8 68059f83 bb1f3dee 6af25d80 0b13e030 System_Windows_Forms_ni+0x71fefb
0b13dc64 6805a1b7 0543a204 09907aa0 09907aa0 System_Windows_Forms_ni+0x749f83
0b13dca4 6af221db ffffffff 6af30bcc 0b13dd30 System_Windows_Forms_ni+0x74a1b7
0b13dcb4 6af44a2a 0b13dd84 00000001 0b13dd50 clr!CallDescrWorker+0x33
0b13dd30 6af44bcc 0b13dd84 00000001 0b13dd50 clr!CallDescrWorkerWithHandler+0x8e (FPO: [Non-Fpo])
0b13de80 6af44c01 6957ced8 0b13dec8 0b13df78 clr!MethodDesc::CallDescr+0x194 (FPO: [Non-Fpo])
0b13de9c 6b192379 6957ced8 0b13dec8 0b13df78 clr!MethodDesc::CallTargetWorker+0x21 (FPO: [Non-Fpo])
0b13df94 6b134ad1 00000001 0b13e0fc 0b13e184 clr!ExceptionNotifications::DeliverExceptionNotification+0x98 (FPO: [Non-
Fpo])
0b13e008 6b134e86 0b13e0fc 0b13e184 0b13e088 clr!COMDelegate::BindToMethodInfo+0x504 (FPO: [Non-Fpo])
0b13e0ac 6b11c19b 0b13e0fc 0b13e184 0b13e180 clr!DistributeUnhandledExceptionReliably+0xeb (FPO: [Non-Fpo])
0b13e104 6b11bfd3 0b13e184 0b13e180 00000000 clr!AppDomain::RaiseUnhandledExceptionEvent+0xba (FPO: [Non-Fpo])
```

```
0b13e19c 6b0a8688 0b13e2b0 b16ccf52 00000000 clr!AppDomain::RaiseUnhandledExceptionEvent_Wrapper+0x1cd (FPO: [Non-
Fpo])
0b13e274 6b11c13e 002017d0 6b11befb 0b13e2b0 clr!Thread::DoADCallBack+0xe0 (FPO: [Non-Fpo])
0b13e2d0 6b11de38 0b13e390 0b13e4a8 00000000 clr!AppDomain::RaiseUnhandledExceptionEvent+0xc2 (FPO: [Non-Fpo])
0b13e344 6b11e807 0b13e390 0b13e4a8 00000000 clr!AppDomain::RaiseUnhandledExceptionEventNoThrow+0x7a (FPO: [Non-Fpo])
0b13e3a0 6b19518a 0b13e4a8 00000000 0b13e4b0 clr!AppDomain::OnUnhandledException+0x81 (FPO: [Non-Fpo])
0b13e4bc 6b1969c1 0b13e750 0b13e594 00000000 clr!NotifyAppDomainsOfUnhandledException+0x141 (FPO: [Non-Fpo])
0b13e6ac 6b196f8f 0b13e750 00000000 00000000 clr!DefaultCatchHandler+0xdb (FPO: [Non-Fpo])
0b13e6d8 6b01c411 00000001 00000001 0b13e720 clr!DefaultCatchHandler+0x623 (FPO: [Non-Fpo])
0b13e6e8 6b01c45b 0b13e750 0b13f568 b16cca06 clr!ThreadBaseExceptionAppDomainFilter+0x13 (FPO: [Non-Fpo])
0b13e720 6b01c4df 0b13e750 71262b04 00000001 clr!ManagedThreadCallState::IsAppDomainEqual+0x9c (FPO: [Non-Fpo])
0b13e728 71262b04 00000001 0b13f344 6afd5d58 clr!Thread::ShouldChangeAbortToUnload+0x3af (FPO: [SEH])
0b13e73c 71284ae4 00000000 00000000 00000000 MSVCR100_CLR0400!_EH4_CallFilterFunc+0x12 (FPO: [Uses EBP] [0,0,4])
0b13e768 6aff14b8 6b509240 6af217d7 0b13e86c MSVCR100_CLR0400!_except_handler4_common+0x8e (FPO: [Non-Fpo])
0b13e788 77c41039 0b13e86c 0b13f334 0b13e894 clr!_except_handler4+0x20 (FPO: [Non-Fpo])
0b13e7ac 77c4100b 0b13e86c 0b13f334 0b13e894 ntdll!ExecuteHandler2+0x26
0b13e854 77c40e97 0b13c000 0b13e894 0b13e86c ntdll!ExecuteHandler+0x24
0b13e854 7654b09e 0b13c000 0b13e894 0b13e86c ntdll!KiUserExceptionDispatcher+0xf (FPO: [2,0,0]) (CONTEXT @ 0b13e894)
0b13ebb0 6afaac08 e0434352 00000001 00000005 KERNEL32!RaiseException+0x58 (FPO: [Non-Fpo])
0b13ec40 6afaae41 098e5728 00000000 00000000 clr!RaiseTheExceptionInternalOnly+0x276 (FPO: [Non-Fpo])
0b13ed00 056028bb 0b13ee60 6afaddc2 0b13f040 clr!IL_Throw+0x14c (FPO: [Non-Fpo])
0b13edd0 6962ae5b 098d5948 0289922c 0b13edfc 0x56028bb
0b13ede0 695b7ff4 098aa838 00000000 098d5914 Unknown_Module_69380000+0x2aae5b
0b13edfc 695b7f34 00000000 098b3eec 00000000 Unknown_Module_69380000+0x237ff4
0b13ee1c 6962ade8 098d5914 00000000 05162dd0 Unknown_Module_69380000+0x237f34
0b13ee34 6af221db 00000000 00000000 0b13eec0 Unknown_Module_69380000+0x2aade8
0b13ee44 6af44a2a 0b13ef10 00000000 0b13eee0 clr!CallDescrWorker+0x33
0b13eec0 6af44bcc 0b13ef10 00000000 0b13eee0 clr!CallDescrWorkerWithHandler+0x8e (FPO: [Non-Fpo])
0b13eff8 6af44c01 69557c90 0b13f160 0b13f07c clr!MethodDesc::CallDescr+0x194 (FPO: [Non-Fpo])
0b13f014 6b0bb512 69557c90 0b13f160 0b13f07c clr!MethodDesc::CallTargetWorker+0x21 (FPO: [Non-Fpo])
0b13f220 6afd5c05 0b13f5f4 0b13f304 05162dd0 clr!ThreadNative::KickOffThread_Worker+0x1e1 (FPO: [Non-Fpo])
0b13f234 6afd5c87 0b13f568 b16cdfc2 0b13f568 clr!Thread::DoExtraWorkForFinalizer+0x114 (FPO: [Non-Fpo])
0b13f2e4 6afd5d42 0b13f568 b16cde62 05162dd0 clr!Thread::ShouldChangeAbortToUnload+0x101 (FPO: [Non-Fpo])
0b13f344 6afc37a2 05162dd0 0b13f430 6b0a6465 clr!Thread::ShouldChangeAbortToUnload+0x399 (FPO: [Non-Fpo])
0b13f350 6b0a6465 0b13f568 b16cd916 05162dd0 clr!Thread::RaiseCrossContextException+0x3f8 (FPO: [Non-Fpo])
0b13f430 6afc37cf 00000002 6afc378b 0b13f568 clr!Thread::DoADCallBack+0xf0 (FPO: [Non-Fpo])
0b13f450 6afd5c87 0b13f568 b16cd826 0b13f568 clr!Thread::DoExtraWorkForFinalizer+0xfa (FPO: [Non-Fpo])
0b13f500 6afd5d42 0b13f568 b16cd846 00000000 clr!Thread::ShouldChangeAbortToUnload+0x101 (FPO: [Non-Fpo])
0b13f560 6afd5dd9 00000002 00000000 00000001 clr!Thread::ShouldChangeAbortToUnload+0x399 (FPO: [Non-Fpo])
0b13f584 6b0bb3e5 00000002 6b0bb3e9 0b13f5f4 clr!Thread::ShouldChangeAbortToUnload+0x43a (FPO: [Non-Fpo])
0b13f59c 6b0bb2e0 00000002 6b0bb3e9 0b13f5f4 clr!ManagedThreadBase::KickOff+0x15 (FPO: [Non-Fpo])
0b13f634 6afd5a08 05168138 0b13f64c 00000000 clr!ThreadNative::KickOffThread+0x23e (FPO: [Non-Fpo])
0b13fed4 76573833 0514eb28 0b13ff20 77c1a9bd clr!Thread::intermediateThreadProc+0x4b (FPO: [Non-Fpo])
0b13fee0 77c1a9bd 0514eb28 0b13250b 00000000 KERNEL32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
0b13ff20 00000000 6afd59c0 0514eb28 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

Note: We also see exception processing code and can set its context:

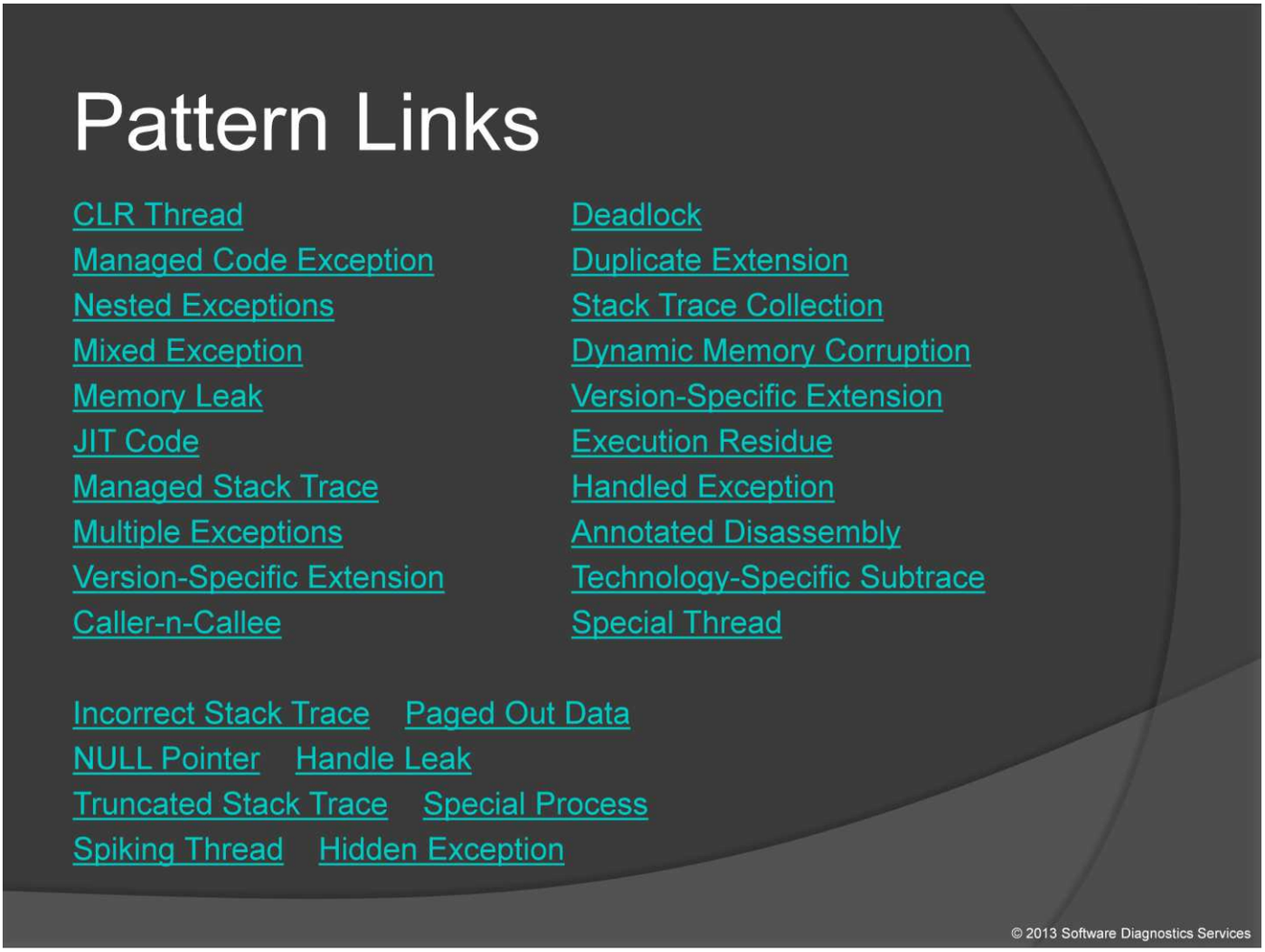
```
1: kd> .cxr 0b13e894
eax=0b13eb60 ebx=00000005 ecx=00000005 edx=00000000 esi=0b13ec0c edi=05162dd0
eip=7654b09e esp=0b13eb60 ebp=0b13ebb0 iopl=0         nv up ei pl nz ac pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000216
KERNEL32!RaiseException+0x58:
001b:7654b09e c9              leave

1: kd> kL
  *** Stack trace for last set context - .thread/.cxr resets it
ChildEBP RetAddr
0b13ebb0 6afaac08 KERNEL32!RaiseException+0x58
0b13ec40 6afaae41 clr!RaiseTheExceptionInternalOnly+0x276
0b13ed00 056028bb clr!IL_Throw+0x14c
WARNING: Frame IP not in any known module. Following frames may be wrong.
0b13edd0 6962ae5b 0x56028bb
0b13ede0 695b7ff4 Unknown_Module_69380000+0x2aae5b
```

```
0b13edfc 695b7f34 Unknown_Module_69380000+0x237ff4
0b13ee1c 6962ade8 Unknown_Module_69380000+0x237f34
0b13ee34 6af221db Unknown_Module_69380000+0x2aade8
0b13ee44 6af44a2a clr!CallDescrWorker+0x33
0b13eec0 6af44bcc clr!CallDescrWorkerWithHandler+0x8e
0b13eff8 6af44c01 clr!MethodDesc::CallDescr+0x194
0b13f014 6b0bb512 clr!MethodDesc::CallTargetWorker+0x21
0b13f220 6afd5c05 clr!ThreadNative::KickOffThread_Worker+0x1e1
0b13f234 6afd5c87 clr!Thread::DoExtraWorkForFinalizer+0x114
0b13f2e4 6afd5d42 clr!Thread::ShouldChangeAbortToUnload+0x101
0b13f344 6afc37a2 clr!Thread::ShouldChangeAbortToUnload+0x399
0b13f350 6b0a6465 clr!Thread::RaiseCrossContextException+0x3f8
0b13f430 6afc37cf clr!Thread::DoADCallBack+0xf0
0b13f450 6afd5c87 clr!Thread::DoExtraWorkForFinalizer+0xfa
0b13f500 6afd5d42 clr!Thread::ShouldChangeAbortToUnload+0x101
0b13f560 6afd5dd9 clr!Thread::ShouldChangeAbortToUnload+0x399
0b13f584 6b0bb3e5 clr!Thread::ShouldChangeAbortToUnload+0x43a
0b13f59c 6b0bb2e0 clr!ManagedThreadBase::KickOff+0x15
0b13f634 6afd5a08 clr!ThreadNative::KickOffThread+0x23e
0b13fed4 76573833 clr!Thread::intermediateThreadProc+0x4b
0b13fee0 77c1a9bd KERNEL32!BaseThreadInitThunk+0xe
0b13ff20 00000000 ntdll!_RtlUserThreadStart+0x23
```

10. Because thread objects are allocated from the non-paged pool, we check its consumption. We see that **Thre** pool tag is the topmost consumer:

```
1: kd> !poolused 3
   Sorting by  NonPaged Pool Consumed

  Pool Used:
            NonPaged                    Paged
 Tag    Allocs    Frees     Diff     Used   Allocs    Frees     Diff     Used
 Thre   471852   421242    50610 35223056        0        0        0        0     Thread objects , Binary: nt!ps
 Even  2097702  1892195   205507  9866064        0        0        0        0     Event objects
 EtwB      287      155      132  6221824       14        0       14   475136     Etw Buffer , Binary: nt!etw
 Cont     1282      256     1026  4754680        0        0        0        0     Contiguous physical memory
allocations for device drivers
 vmmp       20       15        5  2120080        0        0        0        0     UNKNOWN pooltag 'vmmp', please
update pooltag.txt
 Pool       15       10        5  1204648        0        0        0        0     Pool tables, etc.
 RaRS     1000        0     1000   680000        0        0        0        0     RaidUnitAllocateResources , Binary:
storport.sys
 AmlH        6        0        6   393216        0        0        0        0     ACPI AMLI Pooltags
 File  1084342  1082307     2035   344024        0        0        0        0     File objects
 Devi      753      384      369   284160        0        0        0        0     Device objects
 HTab      610      508      102   273144        0        0        0        0     Hash Table pool
 EcBp        2        0        2   246016        0        0        0        0     UNKNOWN pooltag 'EcBp', please
update pooltag.txt
 PciB      582      237      345   217976     3736     3699       37     2856     PnP pci bus enumerator , Binary:
pci.sys
 ALPC    25056    24301      755   212824        0        0        0        0     ALPC port objects , Binary: nt!alpc
 NtfJ        4        0        4   200704        5        4        1      128     NTFS Specific allocation tags ,
Binary: ntfs.sys
 Ntfr    33280    30319     2961   189960        0        0        0        0     ERESOURCE , Binary: ntfs.sys
 MmCi     6067     5343      724   176320        0        0        0        0     Mm control areas for images ,
Binary: nt!mm
 FMsl    27189    25499     1690   175760        0        0        0        0     STREAM_LIST_CTRL structure , Binary:
fltmgr.sys
 Mm      22252    22245        7   167744       87       82        5      848     general Mm Allocations , Binary:
nt!mm
 Vad    199559   196589     2970   166320        0        0        0        0     Mm virtual address descriptors ,
Binary: nt!mm
 VoSm       14        9        5   163896        0        0        0        0     Bitmap allocations , Binary:
volsnap.sys
```

```
 ViMm     2553     2408      145   160800     1566     1424      142   118648     Video memory manager , Binary:
dxgkrnl.sys
 Icp      9088     5742     3346   160544        0        0        0        0     I/O completion packets queue on a
completion ports
 MmAc   236172   236137       35   143360        0        0        0        0     Mm access log buffers , Binary:
nt!mm
```



Here are links to pattern descriptions and additional examples:

CLR Thread:
http://www.dumpanalysis.org/blog/index.php/2009/12/07/crash-dump-analysis-patterns-part-95/

Deadlock (managed space):
http://www.dumpanalysis.org/blog/index.php/2011/10/17/crash-dump-analysis-patterns-part-9g/

Managed Code Exception:
http://www.dumpanalysis.org/blog/index.php/2007/07/20/crash-dump-analysis-patterns-part-17/

Duplicate Extension:
http://www.dumpanalysis.org/blog/index.php/2011/10/21/crash-dump-analysis-patterns-part-153/

Nested Exceptions (managed code):
http://www.dumpanalysis.org/blog/index.php/2008/06/25/crash-dump-analysis-patterns-part-67b/

Stack Trace Collection (managed space):
http://www.dumpanalysis.org/blog/index.php/2011/10/24/crash-dump-analysis-patterns-part-27b/

Mixed Exception:
http://www.dumpanalysis.org/blog/index.php/2009/10/28/crash-dump-analysis-patterns-part-90/

Dynamic Memory Corruption (managed heap):
http://www.dumpanalysis.org/blog/index.php/2011/10/24/crash-dump-analysis-patterns-part-2c/

Memory Leak (managed heap):
http://www.dumpanalysis.org/blog/index.php/2007/08/19/crash-dump-analysis-patterns-part-20b/

Version-Specific Extension:
http://www.dumpanalysis.org/blog/index.php/2011/06/01/crash-dump-analysis-patterns-part-136/

JIT Code:
http://www.dumpanalysis.org/blog/index.php/2009/05/15/crash-dump-analysis-patterns-part-84/

Execution Residue (managed space):
http://www.dumpanalysis.org/blog/index.php/2011/10/17/crash-dump-analysis-patterns-part-60b/

Managed Stack Trace:
http://www.dumpanalysis.org/blog/index.php/2011/06/17/crash-dump-analysis-patterns-part-139/

Handled Exception (.NET CLR):
http://www.dumpanalysis.org/blog/index.php/2011/10/17/crash-dump-analysis-patterns-part-152b/

Multiple Exceptions (managed space):
http://www.dumpanalysis.org/blog/index.php/2011/06/28/crash-dump-analysis-patterns-part-1c/

Annotated Disassembly (JIT .NET code):
http://www.dumpanalysis.org/blog/index.php/2011/10/13/crash-dump-analysis-patterns-part-151/

Technology-Specific Subtrace (JIT .NET code):
http://www.dumpanalysis.org/blog/index.php/2011/10/10/crash-dump-analysis-patterns-part-127c/

Caller-n-Callee:
http://www.dumpanalysis.org/blog/index.php/2011/10/10/crash-dump-analysis-patterns-part-150/

Special Thread (.NET CLR):
http://www.dumpanalysis.org/blog/index.php/2011/10/27/crash-dump-analysis-patterns-part-154a/

Incorrect Stack Trace:
http://www.dumpanalysis.org/blog/index.php/2007/04/03/crash-dump-analysis-patterns-part-11/

Paged Out Data:
http://www.dumpanalysis.org/blog/index.php/2009/02/19/crash-dump-analysis-patterns-part-81/

NULL Pointer (data):
http://www.dumpanalysis.org/blog/index.php/2009/04/14/crash-dump-analysis-patterns-part-6b/

Handle Leak (kernel pool):
http://www.dumpanalysis.org/blog/index.php/2007/07/15/crash-dump-analysis-patterns-part-13b/

Truncated Stack Trace:
http://www.dumpanalysis.org/blog/index.php/2011/03/20/crash-dump-analysis-patterns-part-133/

Special Process:
http://www.dumpanalysis.org/blog/index.php/2008/02/12/crash-dump-analysis-patterns-part-48/

Spiking Thread:
http://www.dumpanalysis.org/blog/index.php/2007/05/11/crash-dump-analysis-patterns-part-14/

Hidden Exception (user space):
http://www.dumpanalysis.org/blog/index.php/2007/02/02/crash-dump-analysis-patterns-part-8/

Note: all these patterns are also available in Memory Dump Analysis Anthology volumes or Encyclopedia of Crash Dump Analysis Patterns.

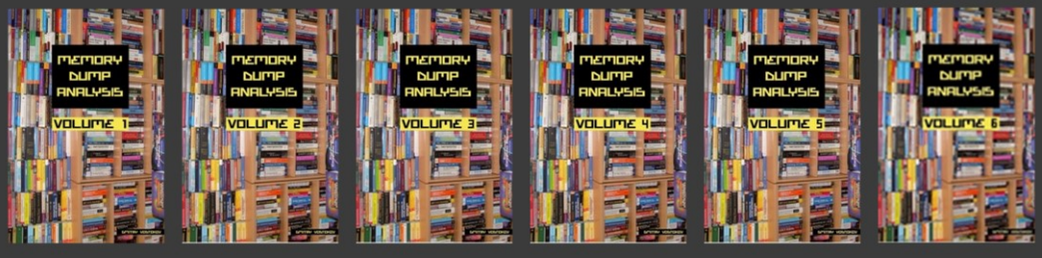
SOS Checklist

- CLR module and SOS extension versions (lmv and .chain)
- Managed exceptions (~*e !pe -nested)
- Managed threads (!Threads -special)
- Managed stack traces (~*e !CLRStack)
- Managed execution residue (~*e !DumpStackObjects)
- Managed heap (!VerifyHeap, !DumpHeap -stat and !eeheap -gc)
- GC handles (!GCHandles)
- Finalizer queue (!FinalizeQueue)
- Sync blocks (!syncblk)

© 2013 Software Diagnostics Services

Resources

- WinDbg Help / WinDbg.org (quick links)
- DumpAnalysis.org
- C# 4.0 in a Nutshell
- Advanced .NET Debugging
- Debugging Microsoft .NET 2.0 Applications
- Shared Source CLI 2.0 Internals
- Accelerated Windows Memory Dump Analysis, 2nd edition
- Memory Dump Analysis Anthology, volumes 1 - 6



© 2013 Software Diagnostics Services

Application Source Code

ApplicationA

```
// ApplicationA
// Copyright (c) 2011 Memory Dump Analysis Services
// GNU GENERAL PUBLIC LICENSE
// http://www.gnu.org/licenses/gpl-3.0.txt

using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Text;
using System.Windows.Forms;

namespace ApplicationR
{
    public partial class Form1 : Form
    {
        public Form1()
        {
            InitializeComponent();
        }

        private void Form1_Load(object sender, EventArgs e)
        {

        }

        private void button1_Click(object sender, EventArgs e)
        {
        }

        private void button1_Click_1(object sender, EventArgs e)
        {
            unsafe
            {
                int* p = (int*)0;
                *p = 1;
            }
        }
    }
}
```

LinqB

```
// LinqB.linq
// Copyright (c) 2011 Memory Dump Analysis Services
// GNU GENERAL PUBLIC LICENSE
// http://www.gnu.org/licenses/gpl-3.0.txt

<Query Kind="Program" />

void Main()
{
	new ClassMain().Main();
}

// Define other methods and classes here

public class ClassMain
{
	public bool time2stop = false;

	public void Main()
	{
		while (!time2stop)
		{
		DoWork();
		}
	}

	volatile int inSensor, outSensor;

	void DoWork()
	{
		outSensor ^= inSensor;
	}
}
```

LinqC

```
// LinqC.linq
// Copyright (c) 2011 Memory Dump Analysis Services
// GNU GENERAL PUBLIC LICENSE
// http://www.gnu.org/licenses/gpl-3.0.txt

<Query Kind="Program" />

void Main()
{
	new ClassMain().Main();
}

public class ClassMain
{
	static string cs1 = "critical section 1";
	static string cs2 = "critical section 2";

	static volatile int inSensor, outSensor;

	static void DoWork()
	{
		outSensor ^= inSensor;
	}

	static void thread_proc_1()
	{
		try
		{
			Monitor.Enter(cs1);
			{
				DoWork();
				unsafe
				{
					int* p = (int *)0;
					*p = 1;
				}
			}
			Monitor.Exit(cs1);
		}
		catch (Exception e)
		{
			Console.WriteLine("We caught an exception.");
		}

		Thread.Sleep(2000);

		Monitor.Enter(cs2);
		{
			DoWork();
		}
		Monitor.Exit(cs2);

		Console.WriteLine("Thread 1 has finished.");
	}
```

```
        static void thread_proc_2()
        {
                Monitor.Enter(cs2);
                {
                        DoWork();
                        Monitor.Enter(cs1);
                        {
                                DoWork();
                                Thread.Sleep(3000);
                                DoWork();
                        }
                        Monitor.Exit(cs1);
                        DoWork();
                }
                Monitor.Exit(cs2);

                Console.WriteLine("Thread 2 has finished.");
        }

        public void Main()
        {
                Thread t1 = new Thread(thread_proc_1);
                t1.Start();
                Thread.Sleep(1000);
                Thread t2 = new Thread(thread_proc_2);
                t2.Start();
                t1.Join();
                t2.Join();
        }
}
```

LinqD

```
// LinqD.linq
// Copyright (c) 2011 Memory Dump Analysis Services
// GNU GENERAL PUBLIC LICENSE
// http://www.gnu.org/licenses/gpl-3.0.txt

<Query Kind="Program" />

void Main()
{
	new ClassMain().Main();
}

public class CustomException : Exception
{
	public string description;
	public int code;

	public CustomException (string _description, int _code)
	{
		description = _description;
		code = _code;
	}
}

public class SmallObject
{
	static void thread_proc() {}
	public int[] buffer;
	public Thread thread;

	public SmallObject ()
	{
		thread = new Thread(thread_proc);
		thread.Start();
		buffer = new int[4096];
	}

	~SmallObject ()
	{
		unsafe
		{
			int *p = (int *)0;
			*p = 1;
		};
	}
}

public class ClassMain
{
	void thread_proc_1()
	{
		throw new FileNotFoundException();
	}
```

```
        void thread_proc_2()
        {
                int max = 50000;
                for (int i = 0; i < max; ++i)
                        new SmallObject();
        }

        void thread_proc_3()
        {
                try
                {
                        throw new FileNotFoundException();
                }
                catch (Exception e)
                {
                        throw new CustomException ("File Not Found", 5);
                }
        }

        public void Main()
        {
                Thread t1 = new Thread(thread_proc_1);
                t1.Start();
                Thread t2 = new Thread(thread_proc_2);
                t2.Start();
                Thread t3 = new Thread(thread_proc_3);
                t3.Start();
                t1.Join();
                t2.Join();
                t3.Join();
        }
}
```

LinqE

```
// LinqE.linq
// Copyright (c) 2011 Memory Dump Analysis Services
// GNU GENERAL PUBLIC LICENSE
// http://www.gnu.org/licenses/gpl-3.0.txt

<Query Kind="Program" />

void Main()
{
	new ClassMain().Main();
}

public class SomeObject
{
	int id;
	String data;
	SomeObject prev;

	public SomeObject (int _id, SomeObject _prev)
	{
		id = _id;
		data = id.ToString();
		prev = _prev;
	}

	public SomeObject Prev
	{
	   get { return prev; }
	}

	unsafe public int * idptr ()
	{
		fixed ( int *p = &id ) { return p; }
	}
}

public class ClassMain
{
	static int id;
	static SomeObject sobjRoot = new SomeObject (0, null);
	static SomeObject sobjLast;

	void thread_proc_1()
	{
		SomeObject sobj = sobjRoot;
		for (id = 1; id < 1000; ++id)
		{
			sobj = new SomeObject (id, sobj);
		}
		sobjLast = sobj;
	}
```

```
        void thread_proc_2()
        {
                SomeObject sobj = sobjLast;
                for (id = 1; id < 500; ++id)
                {
                        sobj = sobj.Prev;
                }
                unsafe
                {
                    char[] b = {'b', 'u', 'g', 's', '.', 'd', 'l', 'l' };
                      char *pc = (char *) sobj.idptr();
                      for (int i = 0; i < b.Length; i++)
                      {
                              *(pc - i)  = b[i];
                      }
                }
        }

        public void Main()
        {
                Thread t1 = new Thread(thread_proc_1);
                t1.Start();
                t1.Join();
                Thread.Sleep(5000);
                Thread t2 = new Thread(thread_proc_2);
                t2.Start();
                t2.Join();
        }
}
```

Selected Q&A

Q. Could you share some insights about ds:[]?

A. Let's look at the typical output of an invalid pointer access violation context:

```
0:000> r
Last set context:
eax=00000000 ebx=00000001 ecx=00000000 edx=0018fe40 esi=00426310 edi=00000111
eip=0041ff21 esp=0018f81c ebp=0018f850 iopl=0         nv up ei pl zr na pe nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00010246
Module!Function+0xb1:
0041ff21 mov dword ptr ds:[812c2bef],0  ds:002b:812c2bef=????????
```

We can ignore ds (data segment register) as segmentation is no longer used and is in fact abandoned in x64 model. The same is for ss (stack segment), es (extra data segment), cs (code segment). You can treat what's in square brackets [] as a memory address so the whole [] expression is a value of a memory cell at that address. The code above tries to write 0 to that memory address replacing the the original value at that address. And it is outside user space process memory space (> 0x7fffffff) so is invalid:

```
0:000> dp 812c2bef
812c2bef  ???????? ???????? ???????? ????????
812c2bff  ???????? ???????? ???????? ????????
812c2c0f  ???????? ???????? ???????? ????????
812c2c1f  ???????? ???????? ???????? ????????
812c2c2f  ???????? ???????? ???????? ????????
812c2c3f  ???????? ???????? ???????? ????????
812c2c4f  ???????? ???????? ???????? ????????
812c2c5f  ???????? ???????? ???????? ????????
```

The following books teach assembly language fundamentals necessary for Windows debugging:

Windows Debugging: Practical Foundations

http://www.dumpanalysis.org/Forthcoming+Windows+Debugging%3A+Practical+Foundations

x64 Windows Debugging: Practical Foundations

http://www.dumpanalysis.org/x64+Windows+Debugging%3A+Practical+Foundations

Q. ***!clrstack -a*** command sometimes shows *<no data>* for parameters or locals. What can we do here?

A. The only way I can see is to use **!U** command to disassemble IP and do reverse engineering of assembly language output but this could be very difficult task. **!mk -p -l -a** SOSEX command might give you additional local names:

```
0:000> !CLRStack -a
OS Thread Id: 0xa70 (0)
Child SP IP       Call Site
[...]
0020dc5c 69360f2a
System.Windows.Forms.Application+ThreadContext.OnThreadException(System.Exception)
    PARAMETERS:
        this (0x0020dc64) = 0x0144d04c
        t (0x0020dc60) = 0x01467f44
    LOCALS:
        0x0020dc5c = 0x0147f160
        0x0020dc68 = 0x00000001
        <no data>
        <no data>
[...]

0:000> !mk -p -l -a
Thread 0:
     ESP      EIP
[...]
08:M 0020dc5c 69360f2a
System.Windows.Forms.Application+ThreadContext.OnThreadException(System.Exception)(+0x4c
IL)(+0xda Native)
     [A0]:this:0x0144d04c (ThreadContext)
     [A1]:t:0x01467f44 (System.Exception)
     [L0]:0x0147f160 (System.Windows.Forms.ThreadExceptionDialog)
     [L1]:0x1 (OK) (System.Windows.Forms.DialogResult)
     [L2]:<?>
     [L3]:<?>
[...]
```

Q. Context Record seems useful but is it only available when an exception is thrown? Do all calls on a stack trace have the context record?

A. Saving context record is a time consuming operation so for ordinary calls only some registers may be saved on the stack and this is entirely compiler and calling convention dependent. Similar to the context record is a trap frame structure that is also saved when a thread transitions to kernel space (in addition to faults in kernel space). Please see an additional complete memory dump analysis exercise in this book.

A. Is it possible to get parameters from a managed exception?

Q. Yes, we can use **!DumpObject** (**!do**) command:

```
0:000> !pe
Exception object: 01467f44
Exception type:   System.NullReferenceException
Message:          Object reference not set to an instance of an object.
InnerException:   <none>
StackTrace (generated):
    SP       IP       Function
    0020EA90 002D0250 ApplicationA!ApplicationA.Form1.button1_Click_1(System.Object, System.EventArgs)
    0020EA98 68E04AE8 System_Windows_Forms_ni!System.Windows.Forms.Control.OnClick(System.EventArgs)+0x70
    0020EAB0 68E070A2 System_Windows_Forms_ni!System.Windows.Forms.Button.OnClick(System.EventArgs)+0xa2
    0020EAC8 69396174
System_Windows_Forms_ni!System.Windows.Forms.Button.OnMouseUp(System.Windows.Forms.MouseEventArgs)+0xac
    0020EAE4 693695B5 System_Windows_Forms_ni!System.Windows.Forms.Control.WmMouseUp(System.Windows.Forms.Message
ByRef, System.Windows.Forms.MouseButtons, Int32)+0x2d1
    0020EB78 6972A1BF System_Windows_Forms_ni!System.Windows.Forms.Control.WndProc(System.Windows.Forms.Message
ByRef)+0x8d30bf
```

```
    0020EBD0 697318DD System_Windows_Forms_ni!System.Windows.Forms.ButtonBase.WndProc(System.Windows.Forms.Message
ByRef)+0x8c3ac1
    0020EC14 68E6DE00 System_Windows_Forms_ni!System.Windows.Forms.Button.WndProc(System.Windows.Forms.Message
ByRef)+0x20
    0020EC20 68E570F3
System_Windows_Forms_ni!System.Windows.Forms.Control+ControlNativeWindow.OnMessage(System.Windows.Forms.Message
ByRef)+0x13
    0020EC28 68E57071
System_Windows_Forms_ni!System.Windows.Forms.Control+ControlNativeWindow.WndProc(System.Windows.Forms.Message
ByRef)+0x31
    0020EC3C 68E56FB6 System_Windows_Forms_ni!System.Windows.Forms.NativeWindow.Callback(IntPtr, Int32, IntPtr,
IntPtr)+0x96

StackTraceString: <none>
HResult: 80004003

0:000> !DumpObj 0x01467f44
Name:        System.NullReferenceException
MethodTable: 6a46470c
EEClass:     6a1a1cb4
Size:        84(0x54) bytes
File:
C:\Windows\Microsoft.Net\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll
Fields:
      MT    Field   Offset                 Type VT     Attr    Value Name
6a46f9ac  400004a        4        System.String  0 instance 01489400 _className
6a4701f4  400004b        8 ...ection.MethodBase  0 instance 00000000 _exceptionMethod
6a46f9ac  400004c        c        System.String  0 instance 00000000 _exceptionMethodString
6a46f9ac  400004d       10        System.String  0 instance 0147eee4 _message
6a464004  400004e       14 ...tions.IDictionary  0 instance 00000000 _data
6a46fc0c  400004f       18     System.Exception  0 instance 00000000 _innerException
6a46f9ac  4000050       1c        System.String  0 instance 00000000 _helpURL
6a46f5e8  4000051       20        System.Object  0 instance 0147f088 _stackTrace
6a46f5e8  4000052       24        System.Object  0 instance 00000000 _watsonBuckets
6a46f9ac  4000053       28        System.String  0 instance 00000000 _stackTraceString
6a46f9ac  4000054       2c        System.String  0 instance 00000000 _remoteStackTraceString
6a472978  4000055       3c         System.Int32  1 instance        0 _remoteStackIndex
6a46f5e8  4000056       30        System.Object  0 instance 00000000 _dynamicMethods
6a472978  4000057       40         System.Int32  1 instance -2147467261 _HResult
6a46f9ac  4000058       34        System.String  0 instance 00000000 _source
6a46aa2c  4000059       44        System.IntPtr  1 instance   20e618 _xptrs
6a472978  400005a       48         System.Int32  1 instance -1073741819 _xcode
6a42a29c  400005b       4c       System.UIntPtr  1 instance   2d0250 _ipForWatsonBuckets
6a429888  400005c       38 ...ializationManager  0 instance 0147efbc _safeSerializationManager
```

We can even try to analyze saved raw stack trace using **!IP2MD** command:

```
0:000> dps 0147f088
0147f088  6a426024 mscorlib_ni+0x2d6024
0147f08c  000000a0
0147f090  0000000b
0147f094  003ebde8
0147f098  002d0250
0147f09c  0020ea90
0147f0a0  0029631c
0147f0a4  68e04ae7 System_Windows_Forms_ni+0x1c4ae7
0147f0a8  0020ea98
0147f0ac  68c5c1e8 System_Windows_Forms_ni+0x1c1e8
0147f0b0  68e070a1 System_Windows_Forms_ni+0x1c70a1
0147f0b4  0020eab0
0147f0b8  68cf1900 System_Windows_Forms_ni+0xb1900
0147f0bc  69396173 System_Windows_Forms_ni+0x756173
0147f0c0  0020eac8
```

```
0147f0c4  68cf1918 System_Windows_Forms_ni+0xb1918
0147f0c8  693695b4 System_Windows_Forms_ni+0x7295b4
0147f0cc  0020eae4
0147f0d0  68c5d764 System_Windows_Forms_ni+0x1d764
0147f0d4  6972a1be System_Windows_Forms_ni+0xaea1be
0147f0d8  0020eb78
0147f0dc  68c5c940 System_Windows_Forms_ni+0x1c940
0147f0e0  697318dc System_Windows_Forms_ni+0xaf18dc
0147f0e4  0020ebd0
0147f0e8  68cf2274 System_Windows_Forms_ni+0xb2274
0147f0ec  68e6ddff System_Windows_Forms_ni+0x22ddff
0147f0f0  0020ec14
0147f0f4  68cf1948 System_Windows_Forms_ni+0xb1948
0147f0f8  68e570f2 System_Windows_Forms_ni+0x2170f2
0147f0fc  0020ec20
0147f100  68cf73c4 System_Windows_Forms_ni+0xb73c4
0147f104  68e57070 System_Windows_Forms_ni+0x217070

0:000> !IP2MD 002d0250
MethodDesc:   0029631c
Method Name:  ApplicationA.Form1.button1_Click_1(System.Object, System.EventArgs)
Class:        002916c0
MethodTable:  00296378
mdToken:      0600000c
Module:       00292e9c
IsJitted:     yes
CodeAddr:     002d0250
Transparency: Critical

0:000> !IP2MD 68e04ae8
MethodDesc:   68c5c1e8
Method Name:  System.Windows.Forms.Control.OnClick(System.EventArgs)
Class:        68c4df38
MethodTable:  68e99948
mdToken:      060007ee
Module:       68c41000
IsJitted:     yes
CodeAddr:     68e04a78
Transparency: Safe critical

0:000> !IP2MD 69396173
MethodDesc:   68cf1918
Method Name:  System.Windows.Forms.Button.OnMouseUp(System.Windows.Forms.MouseEventArgs)
Class:        68c7bc28
MethodTable:  68e96b6c
mdToken:      060011a0
Module:       68c41000
IsJitted:     yes
CodeAddr:     693960c8
Transparency: Safe critical
```

Q. When multiple exceptions are seen how do we know which exception was responsible for the crash? Some exceptions may be in process of handling so might not be responsible for the crash.

A. Usually you would see that from the stack trace. Here I show you a managed code example:

```
0:000> !CLRStack
OS Thread Id: 0xa70 (0)
Child SP IP       Call Site
0020da88 77ba0f34 [InlinedCallFrame: 0020da88] System.Windows.Forms.UnsafeNativeMethods.WaitMessage()
0020da84 68e6737a
System.Windows.Forms.Application+ComponentManager.System.Windows.Forms.UnsafeNativeMethods.IMsoComponentManager.FPushM
essageLoop(IntPtr, Int32, Int32)
0020db20 68e66e2c System.Windows.Forms.Application+ThreadContext.RunMessageLoopInner(Int32,
System.Windows.Forms.ApplicationContext)
0020db78 68e66c81 System.Windows.Forms.Application+ThreadContext.RunMessageLoop(Int32,
System.Windows.Forms.ApplicationContext)
0020dba8 6935fefb System.Windows.Forms.Application.RunDialog(System.Windows.Forms.Form)
0020dbbc 69389f83 System.Windows.Forms.Form.ShowDialog(System.Windows.Forms.IWin32Window)
0020dbc0 6938a1b7 [InlinedCallFrame: 0020dbc0]
0020dc58 6938a1b7 System.Windows.Forms.Form.ShowDialog()
0020dc5c 69360f2a System.Windows.Forms.Application+ThreadContext.OnThreadException(System.Exception)
0020dc98 69369866 System.Windows.Forms.Control.WndProcException(System.Exception)
0020dca4 6936ff9c System.Windows.Forms.Control+ControlNativeWindow.OnThreadException(System.Exception)
0020dca8 68e56fd1 System.Windows.Forms.NativeWindow.Callback(IntPtr, Int32, IntPtr, IntPtr)
0020ede4 014009dd [InlinedCallFrame: 0020ede4]
0020ede0 68e72eec DomainBoundILStubClass.IL_STUB_PInvoke(MSG ByRef)
0020ede4 68e671ff [InlinedCallFrame: 0020ede4] System.Windows.Forms.UnsafeNativeMethods.DispatchMessageW(MSG ByRef)
0020ee28 68e671ff
System.Windows.Forms.Application+ComponentManager.System.Windows.Forms.UnsafeNativeMethods.IMsoComponentManager.FPushM
essageLoop(IntPtr, Int32, Int32)
0020ee2c 68e66e2c [InlinedCallFrame: 0020ee2c]
0020eec4 68e66e2c System.Windows.Forms.Application+ThreadContext.RunMessageLoopInner(Int32,
System.Windows.Forms.ApplicationContext)
0020ef1c 68e66c81 System.Windows.Forms.Application+ThreadContext.RunMessageLoop(Int32,
System.Windows.Forms.ApplicationContext)
0020ef4c 68df366d System.Windows.Forms.Application.Run(System.Windows.Forms.Form)
0020ef60 002d009a ApplicationA.Program.Main()
```

We try get exception parameters for exception processing functions:

```
0:000> !CLRStack -a
OS Thread Id: 0xa70 (0)
Child SP IP       Call Site
[...]
0020dc5c 69360f2a
System.Windows.Forms.Application+ThreadContext.OnThreadException(System.Exception)
    PARAMETERS:
        this (0x0020dc64) = 0x0144d04c
        t (0x0020dc60) = 0x01467f44
    LOCALS:
        0x0020dc5c = 0x0147f160
        0x0020dc68 = 0x00000001
        <no data>
        <no data>
[...]

0:000> !pe 0x01467f44
Exception object: 01467f44
Exception type:   System.NullReferenceException
Message:          Object reference not set to an instance of an object.
InnerException:   <none>
StackTrace (generated):
    SP       IP       Function
    0020EA90 002D0250 ApplicationA!ApplicationA.Form1.button1_Click_1(System.Object,
System.EventArgs)
```

```
    0020EA98 68E04AE8
System_Windows_Forms_ni!System.Windows.Forms.Control.OnClick(System.EventArgs)+0x70
    0020EAB0 68E070A2
System_Windows_Forms_ni!System.Windows.Forms.Button.OnClick(System.EventArgs)+0xa2
    0020EAC8 69396174
System_Windows_Forms_ni!System.Windows.Forms.Button.OnMouseUp(System.Windows.Forms.MouseEventAr
gs)+0xac
    0020EAE4 693695B5
System_Windows_Forms_ni!System.Windows.Forms.Control.WmMouseUp(System.Windows.Forms.Message
ByRef, System.Windows.Forms.MouseButtons, Int32)+0x2d1
    0020EB78 6972A1BF
System_Windows_Forms_ni!System.Windows.Forms.Control.WndProc(System.Windows.Forms.Message
ByRef)+0x8d30bf
    0020EBD0 697318DD
System_Windows_Forms_ni!System.Windows.Forms.ButtonBase.WndProc(System.Windows.Forms.Message
ByRef)+0x8c3ac1
    0020EC14 68E6DE00
System_Windows_Forms_ni!System.Windows.Forms.Button.WndProc(System.Windows.Forms.Message
ByRef)+0x20
    0020EC20 68E570F3
System_Windows_Forms_ni!System.Windows.Forms.Control+ControlNativeWindow.OnMessage(System.Windo
ws.Forms.Message ByRef)+0x13
    0020EC28 68E57071
System_Windows_Forms_ni!System.Windows.Forms.Control+ControlNativeWindow.WndProc(System.Windows
.Forms.Message ByRef)+0x31
    0020EC3C 68E56FB6
System_Windows_Forms_ni!System.Windows.Forms.NativeWindow.Callback(IntPtr, Int32, IntPtr,
IntPtr)+0x96

StackTraceString: <none>
HResult: 80004003
```

Handled exceptions might appear as execution residue on raw stack when we use **!DumpStackObjects** (**!dso**) command.

Q. How do we find code in a case it was not jitted?

A. In such cases we can use **!DumpIL** SOS extension command or **!muf** SOSEX extension command. Let's open C:\ANETMDA-Dumps\32-bit\Processes\CLR4\LINQPadA.dmp and find a suitable non-jitted method:

```
0:000> .symfix c:\mss

0:000> .reload

0:000> .load C:\ANETMDA-Dumps\32-bit\Microsoft.NET\Framework\v4.0.30319\sos

0:000> k
ChildEBP RetAddr
0020e95c 7720b5b4 ntdll!KiFastSystemCallRet
0020e960 68e6737a user32!NtUserWaitMessage+0xc
0020e9f4 68e66e2c System_Windows_Forms_ni+0x22737a
0020ea50 68e66c81 System_Windows_Forms_ni+0x226e2c
0020ea80 68df366d System_Windows_Forms_ni+0x226c81
0020ea98 002b31fd System_Windows_Forms_ni+0x1b366d
WARNING: Frame IP not in any known module. Following frames may be wrong.
0020eb7c 002b1515 0x2b31fd
0020ee24 6ce421db 0x2b1515
```

```
0020ee34 6ce64a2a clr!CallDescrWorker+0x33
0020eeb0 6ce64bcc clr!CallDescrWorkerWithHandler+0x8e
0020efe8 6ce64c01 clr!MethodDesc::CallDescr+0x194
0020f004 6ce64c21 clr!MethodDesc::CallTargetWorker+0x21
0020f01c 6cf2ce82 clr!MethodDescCallSite::Call+0x1c
0020f180 6cf2cf90 clr!ClassLoader::RunMain+0x24c
0020f3e8 6cf2cda4 clr!Assembly::ExecuteMainMethod+0xc1
0020f8cc 6cf2d199 clr!SystemDomain::ExecuteMainMethod+0x4ec
0020f920 6cf2d09a clr!ExecuteEXE+0x58
0020f96c 6cfaaf00 clr!_CorExeMainInternal+0x19f
0020f9a4 6e1e55ab clr!_CorExeMain+0x4e
0020f9b0 6e187f16 mscoreei!_CorExeMain+0x38
0020f9c0 6e184de3 mscoree!ShellShim__CorExeMain+0x99
0020f9c8 77563833 mscoree!_CorExeMain_Exported+0x8
0020f9d4 77b7a9bd kernel32!BaseThreadInitThunk+0xe
0020fa14 00000000 ntdll!_RtlUserThreadStart+0x23

0:000> !IP2MD 0x2b1515
MethodDesc:   000e934c
Method Name:  LINQPad.Program.Go(System.String[])
Class:        002c05dc
MethodTable:  000e954c
mdToken:      06000272
Module:       000e2e9c
IsJitted:     yes
CodeAddr:     002b05c0
Transparency: Critical

0:000> !name2ee * LINQPad.Program
Module:      67061000
Assembly:    PresentationCore.dll
--------------------------------------
Module:      000c5f20
Assembly:    SMDiagnostics.dll
--------------------------------------
Module:      6af31000
Assembly:    System.Data.SqlXml.dll
--------------------------------------
Module:      6b411000
Assembly:    WindowsBase.dll
--------------------------------------
Module:      6a151000
Assembly:    mscorlib.dll
--------------------------------------
Module:      6bda1000
Assembly:    System.Security.dll
--------------------------------------
Module:      6ba51000
Assembly:    System.Configuration.dll
--------------------------------------
Module:      055e16c0
Assembly:    System.Web.dll
--------------------------------------
Module:      6d4b1000
Assembly:    System.Numerics.dll
--------------------------------------
Module:      68c41000
Assembly:    System.Windows.Forms.dll
--------------------------------------
Module:      03e3f74c
```

```
Assembly:    System.Xaml.dll
--------------------------------------
Module:      000c37cc
Assembly:    System.Runtime.Serialization.dll
--------------------------------------
Module:      055e9f28
Assembly:    System.Data.Services.Client.dll
--------------------------------------
Module:      698b1000
Assembly:    System.dll
--------------------------------------
Module:      03e39f6c
Assembly:    System.Xml.Linq.dll
--------------------------------------
Module:      65e01000
Assembly:    System.Data.dll
--------------------------------------
Module:      03e3d23c
Assembly:    System.Transactions.dll
--------------------------------------
Module:      6b1a1000
Assembly:    System.Data.Linq.dll
--------------------------------------
Module:      000c672c
Assembly:    System.Management.dll
--------------------------------------
Module:      019368f0
Assembly:    System.Runtime.DurableInstancing.dll
--------------------------------------
Module:      6bb51000
Assembly:    System.Drawing.dll
--------------------------------------
Module:      03e3e374
Assembly:    System.EnterpriseServices.dll
--------------------------------------
Module:      68581000
Assembly:    System.Core.dll
--------------------------------------
Module:      66b01000
Assembly:    System.Xml.dll
--------------------------------------
Module:      055eb030
Assembly:    System.Data.Services.Design.dll
--------------------------------------
Module:      000e2e9c
Assembly:    LINQPad.exe
Token:       0200003c
MethodTable: 000e954c
EEClass:     002c05dc
Name:        LINQPad.Program
--------------------------------------
Module:      008610a0
Assembly:    Resources, Version=1.0.0.0, Culture=neutral
--------------------------------------
Module:      0086438c
Assembly:    ICSharpCode.SharpDevelop.Dom, Version=3.0.0.3630, Culture=neutral
--------------------------------------
Module:      008685d0
Assembly:    ICSharpCode.NRefactory, Version=3.0.0.3630, Culture=neutral
--------------------------------------
```

```
Module:      0086bf88
Assembly:    ActiproSoftware.SyntaxEditor.Net20, Version=4.0.277.0, Culture=neutral
--------------------------------------
Module:      04b2a44c
Assembly:    ActiproSoftware.Shared.Net20, Version=1.0.96.0, Culture=neutral
--------------------------------------
Module:      04b2b6a0
Assembly:    ActiproSoftware.WinUICore.Net20, Version=1.0.96.0, Culture=neutral
--------------------------------------
Module:      0557a9a4
Assembly:    DotNetLanguage, Version=4.9.0.0, Culture=neutral
--------------------------------------
Module:      055a7e60
Assembly:    Mono.Cecil, Version=0.6.0.0, Culture=neutral
--------------------------------------
Module:      05d62f54
Assembly:    LINQPad.exe
Token:       0200003c
MethodTable: 05d666a8
EEClass:     075df8bc
Name:        LINQPad.Program
--------------------------------------
Module:      08131050
Assembly:    query_dnzqvd.dll

0:000> !DumpClass 075df8bc
Class Name:      LINQPad.Program
mdToken:         0200003c
File:            C:\LINQPad4\LINQPad.exe
Parent Class:    6a153ef8
Module:          05d62f54
Method Table:    05d666a8
Vtable Slots:    4
Total Method Slots:  5
Class Attributes:    100180  Abstract,
Transparency:        Critical
NumInstanceFields:   0
NumStaticFields:     28
      MT    Field   Offset                 Type VT     Attr    Value Name
6a472978  40001b8      278         System.Int32  1   static      431 CurrentVersion
6a472978  40001b9      27c         System.Int32  1   static        0 Subversion
6a46f9ac  40001ba      200        System.String  0   static 07111fd4 AppDataFolder
6a46f9ac  40001bb      204        System.String  0   static 07112010 UserDataFolder
6a46f9ac  40001bc      208        System.String  0   static 07112070 LocalUserDataFolder
6a46f9ac  40001bd      20c        System.String  0   static 071120cc TempFolderBase
6a46f9ac  40001be      210        System.String  0   static 00000000 _appInstanceID
6a46f9ac  40001bf      214        System.String  0   static 00000000 _tempFolder
6a46f9ac  40001c0      218        System.String  0   static 07112134 OneToOneAckFile
6a46f9ac  40001c1      21c        System.String  0   static 00000000 QueryConfigFile
6a46ffcc  40001c2      220 ....Threading.Thread  0   static 00000000 _updateThread
00000000  40001c3      224    LINQPad.UI.Splash  0   static 00000000 Splash
6a472978  40001c4      280         System.Int32  1   static   227396 _sessionID
6a46b21c  40001c5      1fc ...em.DateTimeOffset  1   static 02a61424 _lastError
6a435230  40001c6      228 ...embly, mscorlib]]  0   static 07112198 _libs
6a47662c  40001c7      284       System.Boolean  1   static        1 _linqPadAssemblyResolverAdded
6a47662c  40001c8      288       System.Boolean  1   static        0 <BetaMode>k__BackingField
6a47662c  40001c9      28c       System.Boolean  1   static        0 <MTAMode>k__BackingField
6a47662c  40001ca      290       System.Boolean  1   static        0 <PresentationMode>k__BackingField
6a46f9ac  40001cb      22c        System.String  0   static 00000000 <Caller>k__BackingField
6a47662c  40001cc      294       System.Boolean  1   static        0 <AllowOneToOne>k__BackingField
6a47662c  40001cd      298       System.Boolean  1   static        0 <PreserveAppDomains>k__BackingField
6a47662c  40001ce      29c       System.Boolean  1   static        0 <FreshAppDomains>k__BackingField
6a47662c  40001cf      2a0       System.Boolean  1   static        0 <EnableMARS>k__BackingField
6a47662c  40001d0      2a4       System.Boolean  1   static        0 <DiagnosticMode>k__BackingField
00000000  40001d1      230                       0   static 00000000 CS$<>9__CachedAnonymousMethodDelegatee
00000000  40001d2      234                       0   static 00000000 CS$<>9__CachedAnonymousMethodDelegatef
00000000  40001d3      238                       0   static 00000000 CS$<>9__CachedAnonymousMethodDelegate10
00000000  40001d4      23c                       0   static 00000000 CS$<>9__CachedAnonymousMethodDelegate11
00000000  40001d5      240                       0   static 00000000 CS$<>9__CachedAnonymousMethodDelegate12
```

```
00000000  40001d6      244                      0   static 00000000 CS$<>9__CachedAnonymousMethodDelegate13
00000000  40001d7      248                      0   static 00000000 CS$<>9__CachedAnonymousMethodDelegate14
00000000  40001d8      24c                      0   static 00000000 CS$<>9__CachedAnonymousMethodDelegate15
00000000  40001d9      250                      0   static 00000000 CS$<>9__CachedAnonymousMethodDelegate16
00000000  40001da      254                      0   static 00000000 CS$<>9__CachedAnonymousMethodDelegate17
00000000  40001db      258                      0   static 00000000 CS$<>9__CachedAnonymousMethodDelegate18
00000000  40001dc      25c                      0   static 00000000 CS$<>9__CachedAnonymousMethodDelegate19
00000000  40001dd      260                      0   static 00000000 CS$<>9__CachedAnonymousMethodDelegate1a
00000000  40001de      264                      0   static 00000000 CS$<>9__CachedAnonymousMethodDelegate1d
6a45b0a8  40001df      268 ...solveEventHandler  0   static 071121cc CS$<>9__CachedAnonymousMethodDelegate33

0:000> !DumpMT -md 05d666a8
EEClass:      075df8bc
Module:       05d62f54
Name:         LINQPad.Program
mdToken:      0200003c
File:         C:\LINQPad4\LINQPad.exe
BaseSize:        0xc
ComponentSize:   0x0
Slots in VTable: 67
Number of IFaces in IFaceMap: 0
--------------------------------------
MethodDesc Table
   Entry MethodDesc      JIT Name
6a37a7e0   6a154934   PreJIT System.Object.ToString()
6a37e2e0   6a15493c   PreJIT System.Object.Equals(System.Object)
6a37e1f0   6a15495c   PreJIT System.Object.GetHashCode()
6a401600   6a154970   PreJIT System.Object.Finalize()
07ee0110   05d66698      JIT LINQPad.Program..cctor()
05d6c0c1   05d66394     NONE LINQPad.Program.get_BetaMode()
05d6c0c5   05d663a0     NONE LINQPad.Program.set_BetaMode(Boolean)
05d6c0c9   05d663ac     NONE LINQPad.Program.get_MTAMode()
05d6c0cd   05d663b8     NONE LINQPad.Program.set_MTAMode(Boolean)
05d6c0d1   05d663c4     NONE LINQPad.Program.get_PresentationMode()
05d6c0d5   05d663d0     NONE LINQPad.Program.set_PresentationMode(Boolean)
05d6c0d9   05d663dc     NONE LINQPad.Program.get_Caller()
05d6c0dd   05d663e8     NONE LINQPad.Program.set_Caller(System.String)
05d6c0e1   05d663f4     NONE LINQPad.Program.get_AllowOneToOne()
05d6c0e5   05d66400     NONE LINQPad.Program.set_AllowOneToOne(Boolean)
05d6c0e9   05d6640c     NONE LINQPad.Program.get_PreserveAppDomains()
05d6c0ed   05d66418     NONE LINQPad.Program.set_PreserveAppDomains(Boolean)
05d6c0f1   05d66424     NONE LINQPad.Program.get_FreshAppDomains()
05d6c0f5   05d66430     NONE LINQPad.Program.set_FreshAppDomains(Boolean)
05d6c0f9   05d6643c     NONE LINQPad.Program.get_EnableMARS()
05d6c0fd   05d66448     NONE LINQPad.Program.set_EnableMARS(Boolean)
05d6c101   05d66454     NONE LINQPad.Program.get_DiagnosticMode()
05d6c105   05d66460     NONE LINQPad.Program.set_DiagnosticMode(Boolean)
05d6c109   05d6646c     NONE LINQPad.Program.get_CurrentVersionString()
05d6c10d   05d66478     NONE LINQPad.Program.get_AppInstanceID()
05d6c111   05d66484     NONE LINQPad.Program.get_TempFolder()
05d6c115   05d66490     NONE LINQPad.Program.Start(System.String[])
05d6c119   05d6649c     NONE LINQPad.Program.Application_ThreadException(System.Object,
System.Threading.ThreadExceptionEventArgs)
05d6c11d   05d664a8     NONE LINQPad.Program.Go(System.String[])
05d6c121   05d664b4     NONE LINQPad.Program.CheckForExistingProcess(System.String)
05d6c125   05d664c0     NONE LINQPad.Program.Listen()
05d6c129   05d664cc     NONE LINQPad.Program.OpenFile(System.String)
05d6c12d   05d664d8     NONE LINQPad.Program.ReadMessage(System.IO.Pipes.PipeStream)
05d6c131   05d664e4     NONE LINQPad.Program.PropagateConfig(System.String)
05d6c135   05d664f0     NONE LINQPad.Program.CreateAppDataFolder()
05d6c139   05d664fc     NONE LINQPad.Program.SetProcessDPIAware()
```

```
05d6c13d   05d66524     NONE LINQPad.Program.Run(System.String, Boolean, System.String,
Boolean, Boolean, System.String)
05d6c151   05d66530     NONE LINQPad.Program.StartSemanticParsingService()
05d6c155   05d6653c     NONE LINQPad.Program.CurrentDomain_UnhandledException(System.Object,
System.UnhandledExceptionEventArgs)
05d6c159   05d66548     NONE LINQPad.Program.QueryOneToOne()
05d6c15d   05d66554     NONE LINQPad.Program.QueryStudioKeys(Boolean)
05d6c161   05d66560     NONE LINQPad.Program.ProcessException(System.Exception)
05d6c165   05d6656c     NONE LINQPad.Program.GetExceptionInfo(System.Exception, Int32)
05d6c169   05d66578     NONE LINQPad.Program.GetStackInfo(System.Exception)
05d6c16d   05d66584     NONE LINQPad.Program.SubmitFeedback(System.String, System.String,
System.String, System.String)
05d6c171   05d66590     NONE LINQPad.Program.SubmitFeedback(System.String, System.String,
System.String, System.String, Boolean)
05d6c175   05d6659c     NONE LINQPad.Program.UnpackDb()
05d6c179   05d665a8     NONE LINQPad.Program.Uncompress(System.String, System.String)
05d6c17d   05d665b4     NONE LINQPad.Program.FindAssem(System.Object, System.ResolveEventArgs)
07ee02a0   05d665c0      JIT LINQPad.Program.AddLINQPadAssemblyResolver()
05d6c185   05d665cc     NONE LINQPad.Program.RunOnWinFormsTimer(System.Action)
05d6c189   05d665d8     NONE LINQPad.Program.RunOnWinFormsTimer(System.Action, Int32)
05d6c18d   05d665e4     NONE LINQPad.Program.<Go>b__1(System.String)
05d6c191   05d665f0     NONE LINQPad.Program.<Go>b__2(System.String)
05d6c195   05d665fc     NONE LINQPad.Program.<Go>b__3(System.String)
05d6c199   05d66608     NONE LINQPad.Program.<Go>b__4(System.String)
05d6c19d   05d66614     NONE LINQPad.Program.<Go>b__5(System.String)
05d6c1a1   05d66620     NONE LINQPad.Program.<Go>b__6(System.String)
05d6c1a5   05d6662c     NONE LINQPad.Program.<Go>b__7(System.String)
05d6c1a9   05d66638     NONE LINQPad.Program.<Go>b__8(System.String)
05d6c1ad   05d66644     NONE LINQPad.Program.<Go>b__9(System.String)
05d6c1b1   05d66650     NONE LINQPad.Program.<Go>b__a(System.String)
05d6c1b5   05d6665c     NONE LINQPad.Program.<Go>b__b(System.String)
05d6c1b9   05d66668     NONE LINQPad.Program.<Go>b__c(System.String)
05d6c1bd   05d66674     NONE LINQPad.Program.<Go>b__d(System.String)
05d6c1c1   05d66680     NONE
LINQPad.Program.<CheckForExistingProcess>b__1c(System.Diagnostics.Process)
05d6c1c5   05d6668c     NONE LINQPad.Program.<AddLINQPadAssemblyResolver>b__32(System.Object,
System.ResolveEventArgs)

0:000> !name2ee * LINQPad.Program.Uncompress
Module:      67061000
Assembly:    PresentationCore.dll
--------------------------------------
Module:      000c5f20
Assembly:    SMDiagnostics.dll
--------------------------------------
Module:      6af31000
Assembly:    System.Data.SqlXml.dll
--------------------------------------
Module:      6b411000
Assembly:    WindowsBase.dll
--------------------------------------
Module:      6a151000
Assembly:    mscorlib.dll
--------------------------------------
Module:      6bda1000
Assembly:    System.Security.dll
--------------------------------------
Module:      6ba51000
Assembly:    System.Configuration.dll
--------------------------------------
```

```
Module:      055e16c0
Assembly:    System.Web.dll
--------------------------------------
Module:      6d4b1000
Assembly:    System.Numerics.dll
--------------------------------------
Module:      68c41000
Assembly:    System.Windows.Forms.dll
--------------------------------------
Module:      03e3f74c
Assembly:    System.Xaml.dll
--------------------------------------
Module:      000c37cc
Assembly:    System.Runtime.Serialization.dll
--------------------------------------
Module:      055e9f28
Assembly:    System.Data.Services.Client.dll
--------------------------------------
Module:      698b1000
Assembly:    System.dll
--------------------------------------
Module:      03e39f6c
Assembly:    System.Xml.Linq.dll
--------------------------------------
Module:      65e01000
Assembly:    System.Data.dll
--------------------------------------
Module:      03e3d23c
Assembly:    System.Transactions.dll
--------------------------------------
Module:      6b1a1000
Assembly:    System.Data.Linq.dll
--------------------------------------
Module:      000c672c
Assembly:    System.Management.dll
--------------------------------------
Module:      019368f0
Assembly:    System.Runtime.DurableInstancing.dll
--------------------------------------
Module:      6bb51000
Assembly:    System.Drawing.dll
--------------------------------------
Module:      03e3e374
Assembly:    System.EnterpriseServices.dll
--------------------------------------
Module:      68581000
Assembly:    System.Core.dll
--------------------------------------
Module:      66b01000
Assembly:    System.Xml.dll
--------------------------------------
Module:      055eb030
Assembly:    System.Data.Services.Design.dll
--------------------------------------
Module:      000e2e9c
Assembly:    LINQPad.exe
Token:       06000285
MethodDesc:  000e944c
Name:        LINQPad.Program.Uncompress(System.String, System.String)
JITTED Code Address: 002b5ba0
```

```
--------------------------------------
Module:      008610a0
Assembly:    Resources, Version=1.0.0.0, Culture=neutral
--------------------------------------
Module:      0086438c
Assembly:    ICSharpCode.SharpDevelop.Dom, Version=3.0.0.3630, Culture=neutral
--------------------------------------
Module:      008685d0
Assembly:    ICSharpCode.NRefactory, Version=3.0.0.3630, Culture=neutral
--------------------------------------
Module:      0086bf88
Assembly:    ActiproSoftware.SyntaxEditor.Net20, Version=4.0.277.0, Culture=neutral
--------------------------------------
Module:      04b2a44c
Assembly:    ActiproSoftware.Shared.Net20, Version=1.0.96.0, Culture=neutral
--------------------------------------
Module:      04b2b6a0
Assembly:    ActiproSoftware.WinUICore.Net20, Version=1.0.96.0, Culture=neutral
--------------------------------------
Module:      0557a9a4
Assembly:    DotNetLanguage, Version=4.9.0.0, Culture=neutral
--------------------------------------
Module:      055a7e60
Assembly:    Mono.Cecil, Version=0.6.0.0, Culture=neutral
--------------------------------------
Module:      05d62f54
Assembly:    LINQPad.exe
Token:       06000285
MethodDesc:  05d665a8
Name:        LINQPad.Program.Uncompress(System.String, System.String)
Not JITTED yet. Use !bpmd -md 05d665a8 to break on run.
--------------------------------------
Module:      08131050
Assembly:    query_dnzqvd.dll

0:000> !DumpIL 05d665a8
ilAddr = 0092aa68
IL_0000: nop
.try
{
  IL_0001: nop
  IL_0002: ldarg.1
  IL_0003: call System.IO.File::Exists
  IL_0008: ldc.i4.0
  IL_0009: ceq
  IL_000b: stloc.s VAR OR ARG 7
  IL_000d: ldloc.s VAR OR ARG 7
  IL_000f: brtrue.s IL_0016
  IL_0011: leave IL_00d5
  IL_0016: ldarg.1
  IL_0017: call System.IO.Path::GetDirectoryName
  IL_001c: stloc.0
  IL_001d: ldloc.0
  IL_001e: call System.IO.Directory::Exists
  IL_0023: stloc.s VAR OR ARG 7
  IL_0025: ldloc.s VAR OR ARG 7
  IL_0027: brtrue.s IL_0030
  IL_0029: ldloc.0
  IL_002a: call System.IO.Directory::CreateDirectory
  IL_002f: pop
```

```
IL_0030: ldc.i4 4096
IL_0035: newarr System.Byte
IL_003a: stloc.1
IL_003b: call System.Reflection.Assembly::GetExecutingAssembly
IL_0040: ldarg.0
IL_0041: callvirt System.Reflection.Assembly::GetManifestResourceStream
IL_0046: stloc.2
.try
{
  IL_0047: ldloc.2
  IL_0048: ldc.i4.0
  IL_0049: newobj System.IO.Compression.DeflateStream::.ctor
  IL_004e: stloc.3
  .try
  {
    IL_004f: ldarg.1
    IL_0050: call System.IO.File::Create
    IL_0055: stloc.s VAR OR ARG 4
    .try
    {
      IL_0057: br.s IL_0084
      IL_0059: nop
      IL_005a: ldloc.3
      IL_005b: ldloc.1
      IL_005c: ldc.i4.0
      IL_005d: ldloc.1
      IL_005e: ldlen
      IL_005f: conv.i4
      IL_0060: callvirt System.IO.Stream::Read
      IL_0065: stloc.s VAR OR ARG 5
      IL_0067: ldloc.s VAR OR ARG 5
      IL_0069: ldc.i4.0
      IL_006a: ceq
      IL_006c: ldc.i4.0
      IL_006d: ceq
      IL_006f: stloc.s VAR OR ARG 7
      IL_0071: ldloc.s VAR OR ARG 7
      IL_0073: brtrue.s IL_0077
      IL_0075: leave.s IL_00d5
      IL_0077: ldloc.s VAR OR ARG 4
      IL_0079: ldloc.1
      IL_007a: ldc.i4.0
      IL_007b: ldloc.s VAR OR ARG 5
      IL_007d: callvirt System.IO.Stream::Write
      IL_0082: nop
      IL_0083: nop
      IL_0084: ldc.i4.1
      IL_0085: stloc.s VAR OR ARG 7
      IL_0087: br.s IL_0159
    } // end .try
    .finally
    {
      IL_0089: ldloc.s VAR OR ARG 4
      IL_008b: ldnull
      IL_008c: ceq
      IL_008e: stloc.s VAR OR ARG 7
      IL_0090: ldloc.s VAR OR ARG 7
      IL_0092: brtrue.s IL_009c
      IL_0094: ldloc.s VAR OR ARG 4
      IL_0096: callvirt System.IDisposable::Dispose
```

```
        IL_009b: nop
        IL_009c: endfinally
      } // end .finally
    } // end .try
    .finally
    {
      IL_009d: ldloc.3
      IL_009e: ldnull
      IL_009f: ceq
      IL_00a1: stloc.s VAR OR ARG 7
      IL_00a3: ldloc.s VAR OR ARG 7
      IL_00a5: brtrue.s IL_00ae
      IL_00a7: ldloc.3
      IL_00a8: callvirt System.IDisposable::Dispose
      IL_00ad: nop
      IL_00ae: endfinally
    } // end .finally
  } // end .try
  .finally
  {
    IL_00af: ldloc.2
    IL_00b0: ldnull
    IL_00b1: ceq
    IL_00b3: stloc.s VAR OR ARG 7
    IL_00b5: ldloc.s VAR OR ARG 7
    IL_00b7: brtrue.s IL_00c0
    IL_00b9: ldloc.2
    IL_00ba: callvirt System.IDisposable::Dispose
    IL_00bf: nop
    IL_00c0: endfinally
  } // end .finally
} // end .try
.catch
{
  IL_00c1: stloc.s VAR OR ARG 6
  IL_00c3: nop
  IL_00c4: ldloc.s VAR OR ARG 6
  IL_00c6: ldstr "Uncompress"
  IL_00cb: call LINQPad.Log::Write
  IL_00d0: nop
  IL_00d1: nop
  IL_00d2: leave.s IL_00d4
} // end .catch
IL_00d4: nop
IL_00d5: nop
IL_00d6: ret

0:000> .load C:\ANETMDA-Dumps\32-bit\SOSEX\sosex

0:000> !muf 05d665a8 -il
LINQPad.Program.Uncompress(string, string): void
    loc 0:string
    loc 1:byte[]
    loc 2:System.IO.Stream
    loc 3:System.IO.Compression.DeflateStream
    loc 4:System.IO.Stream
    loc 5:int
    loc 6:System.Exception
    loc 7:bool
```

```
IL_0000: nop
.try {
IL_0001: nop
IL_0002: ldarg.1  (outPath)
IL_0003: call System.IO.File::Exists
IL_0008: ldc.i4.0
IL_0009: ceq
IL_000b: stloc.s 7
IL_000d: ldloc.s 7
IL_000f: brtrue.s IL_0016
IL_0011: leave IL_00d5
IL_0016: ldarg.1  (outPath)
IL_0017: call System.IO.Path::GetDirectoryName
IL_001c: stloc.0
IL_001d: ldloc.0
IL_001e: call System.IO.Directory::Exists
IL_0023: stloc.s 7
IL_0025: ldloc.s 7
IL_0027: brtrue.s IL_0030
IL_0029: ldloc.0
IL_002a: call System.IO.Directory::CreateDirectory
IL_002f: pop
IL_0030: ldc.i4 4096(0x1000)
IL_0035: newarr System.Byte
IL_003a: stloc.1
IL_003b: call System.Reflection.Assembly::GetExecutingAssembly
IL_0040: ldarg.0  (resourceName)
IL_0041: callvirt System.Reflection.Assembly::GetManifestResourceStream
IL_0046: stloc.2
.try {
IL_0047: ldloc.2
IL_0048: ldc.i4.0
IL_0049: newobj System.IO.Compression.DeflateStream::.ctor
IL_004e: stloc.3
.try {
IL_004f: ldarg.1  (outPath)
IL_0050: call System.IO.File::Create
IL_0055: stloc.s 4
.try {
IL_0057: br.s IL_0084
IL_0059: nop
IL_005a: ldloc.3
IL_005b: ldloc.1
IL_005c: ldc.i4.0
IL_005d: ldloc.1
IL_005e: ldlen
IL_005f: conv.i4
IL_0060: callvirt System.IO.Stream::Read
IL_0065: stloc.s 5
IL_0067: ldloc.s 5
IL_0069: ldc.i4.0
IL_006a: ceq
IL_006c: ldc.i4.0
IL_006d: ceq
IL_006f: stloc.s 7
IL_0071: ldloc.s 7
IL_0073: brtrue.s IL_0077
IL_0075: leave.s IL_00d5
IL_0077: ldloc.s 4
IL_0079: ldloc.1
```

```
IL_007a: ldc.i4.0
IL_007b: ldloc.s 5
IL_007d: callvirt System.IO.Stream::Write
IL_0082: nop
IL_0083: nop
IL_0084: ldc.i4.1
IL_0085: stloc.s 7
IL_0087: br.s IL_0059
} // END TRY (IL_0057)
.finally {
IL_0089: ldloc.s 4
IL_008b: ldnull
IL_008c: ceq
IL_008e: stloc.s 7
IL_0090: ldloc.s 7
IL_0092: brtrue.s IL_009c
IL_0094: ldloc.s 4
IL_0096: callvirt System.IDisposable::Dispose
IL_009b: nop
IL_009c: endfinally
} // END FINALLY (IL_0089)
} // END TRY (IL_004f)
.finally {
IL_009d: ldloc.3
IL_009e: ldnull
IL_009f: ceq
IL_00a1: stloc.s 7
IL_00a3: ldloc.s 7
IL_00a5: brtrue.s IL_00ae
IL_00a7: ldloc.3
IL_00a8: callvirt System.IDisposable::Dispose
IL_00ad: nop
IL_00ae: endfinally
} // END FINALLY (IL_009d)
} // END TRY (IL_0047)
.finally {
IL_00af: ldloc.2
IL_00b0: ldnull
IL_00b1: ceq
IL_00b3: stloc.s 7
IL_00b5: ldloc.s 7
IL_00b7: brtrue.s IL_00c0
IL_00b9: ldloc.2
IL_00ba: callvirt System.IDisposable::Dispose
IL_00bf: nop
IL_00c0: endfinally
} // END FINALLY (IL_00af)
} // END TRY (IL_0001)
.catch {
IL_00c1: stloc.s 6
IL_00c3: nop
IL_00c4: ldloc.s 6
IL_00c6: ldstr "Uncompress"
IL_00cb: call LINQPad.Log::Write(System.Exception, string)
IL_00d0: nop
IL_00d1: nop
IL_00d2: leave.s IL_00d4
} // END CATCH (IL_00c1)
IL_00d4: nop
IL_00d5: nop
```

```
IL_00d6: ret
```

Q. What is the default value for showing stack trace size to make sure we get the whole unmanaged stack trace?

A. .kframes command without parameters shows the default value:

```
0:000> .kframes
Default stack trace depth is 0n256 frames
```

Q. Is the pdb file of a .ni and a regular dll the same or not?

A. A regular DLL may have IL to source code mapping, for example:

```
0:000> * Without PDB

0:000> !U 0029631c
Normal JIT generated code
ApplicationA.Form1.button1_Click_1(System.Object, System.EventArgs)
Begin 002d0250, size d
002d0250 c7050000000001000000 mov dword ptr ds:[0],1
002d025a c20400          ret     4

0:000> * With PDB

0:000> .sympath+ C:\ANETMDA-Examples\ApplicationA\ApplicationA\bin\Release
Symbol search path is: srv*;C:\ANETMDA-Examples\ApplicationA\ApplicationA\bin\Release
Expanded Symbol search path is:
SRV*c:\mss*http://msdl.microsoft.com/download/symbols;c:\anetmda-
examples\applicationa\applicationa\bin\release

0:000> .reload
...............................

0:000> !U 0029631c
Normal JIT generated code
ApplicationA.Form1.button1_Click_1(System.Object, System.EventArgs)
Begin 002d0250, size d

D:\ANETMDA-Examples\ApplicationA\ApplicationA\Form1.cs @ 28:
002d0250 c7050000000001000000 mov dword ptr ds:[0],1

D:\ANETMDA-Examples\ApplicationA\ApplicationA\Form1.cs @ 34:
002d025a c20400          ret     4
```

Q. You seem to have skipped the step ".loadby sos clr" and ".loadby sos mscorwks"

A. There is no need to use .loadby command. Most of the time it doesn't work for dumps from other computers other than the development machine. If there is no correct SOS then this command will not work and you need to specify a path to a customer's SOS manually via **.load**. All this was specifically modeled because of our experience of getting .NET dumps from all over the world from diverse customer computer environments.

Q. What WinDbg we should use: 32-bit or 64-bit?

A. Because we need to load platform specific SOS DLL we need to use 32-bit WinDbg for 32-bit .NET memory dumps saved from 32-bit processes and 64-bit WinDbg for .NET memory dumps saved from

64-bit processes. We can only load a 32-bit DLL into a 32-bit process address space and a 64-bit DLL into 64-bit process (x64) address space.

Q. Do all objects go through the finalizer queue or only objects that have Finalize() go through the finalizer queue?

A. Based on some finalization internals hints (from http://msdn.microsoft.com/en-us/magazine/bb985010.aspx) it looks like only objects with Finalize() got to the finalizer queue. We randomly picked up objects from such a queue and all of them had that method and we have never seen very simple objects on such a queue.

Q. What does ntdll!KiFastSystemCallRet indicate?

A. This is better illustrated by a stack trace from a complete memory dump:

```
        THREAD a217cd78  Cid 6245c.30ff8  Teb: 7ffd7000 Win32Thread: 00000000 WAIT:
(UserRequest) UserMode Non-Alertable
            83325548  SynchronizationEvent
            a217ce00  NotificationTimer
        Not impersonating
        DeviceMap                 9b2d5900
        Owning Process            8312f800       Image:         LINQPad.exe
        Attached Process          N/A            Image:         N/A
        Wait Start TickCount      1543033        Ticks: 500 (0:00:00:07.812)
        Context Switch Count      27
        UserTime                  00:00:00.000
        KernelTime                00:00:00.000
        Win32 Start Address clr!WKS::gc_heap::gc_thread_stub (0x6afd5751)
        Stack Init 88db1000 Current 88db0c38 Base 88db1000 Limit 88dae000 Call 0
        Priority 10 BasePriority 8 PriorityDecrement 2 IoPriority 2 PagePriority 5
        ChildEBP RetAddr
        88db0c50 818ac9cf nt!KiSwapContext+0x26 (FPO: [Uses EBP] [0,0,4])
        88db0c8c 81829308 nt!KiSwapThread+0x389
        88db0ce8 819f50ef nt!KeWaitForSingleObject+0x414
        88db0d50 8188c96a nt!NtWaitForSingleObject+0xbe
        88db0d50 77c40f34 nt!KiFastCallEntry+0x12a (FPO: [0,3] TrapFrame @ 88db0d64)
        076df6bc 77c406a0 ntdll!KiFastSystemCallRet (FPO: [0,0,0])
        076df6c0 765777d4 ntdll!NtWaitForSingleObject+0xc (FPO: [3,0,0])
        076df730 6af81030 KERNEL32!WaitForSingleObjectEx+0xbe (FPO: [Non-Fpo])
        076df764 6af81071 clr!CLREvent::CreateManualEvent+0xf6 (FPO: [Non-Fpo])
        076df7b4 6af7d3e8 clr!CLREvent::CreateManualEvent+0x137 (FPO: [Non-Fpo])
        076df7f4 6af7d409 clr!CLREvent::WaitEx+0x126 (FPO: [Non-Fpo])
        076df808 6afd5704 clr!CLREvent::Wait+0x19 (FPO: [Non-Fpo])
        076df82c 6afd577a clr!WKS::gc_heap::gc_thread_function+0x3a (FPO: [Non-Fpo])
        076df830 76573833 clr!WKS::gc_heap::gc_thread_stub+0x29 (FPO: [1,0,0])
        076df83c 77c1a9bd KERNEL32!BaseThreadInitThunk+0xe (FPO: [Non-Fpo])
        076df87c 00000000 ntdll!_RtlUserThreadStart+0x23 (FPO: [Non-Fpo])
```

We see that it can be considered as a return address from kernel space.