Public Preview Version

.NET Memory Dump Analysis Accelerated

Version 4.0

.NET Core and Framework

Dmitry Vostokov
Software Diagnostics Services

Prerequisites

WinDbg Commands

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

Basic .NET programming and debugging

Training Goals

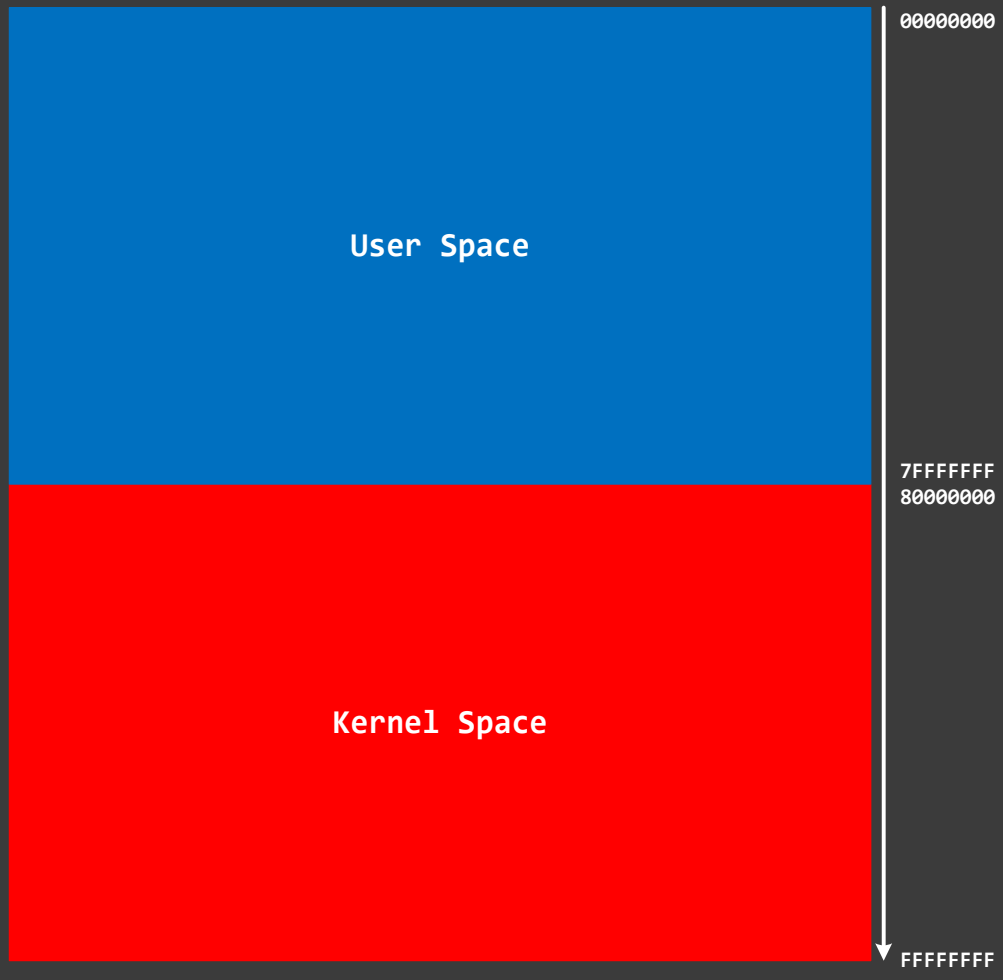
- Review fundamentals
- Learn how to analyze process dumps
- Learn necessary commands in context
- Cover CoreCLR and CLR 4 (x86 and x64)

Training Principles

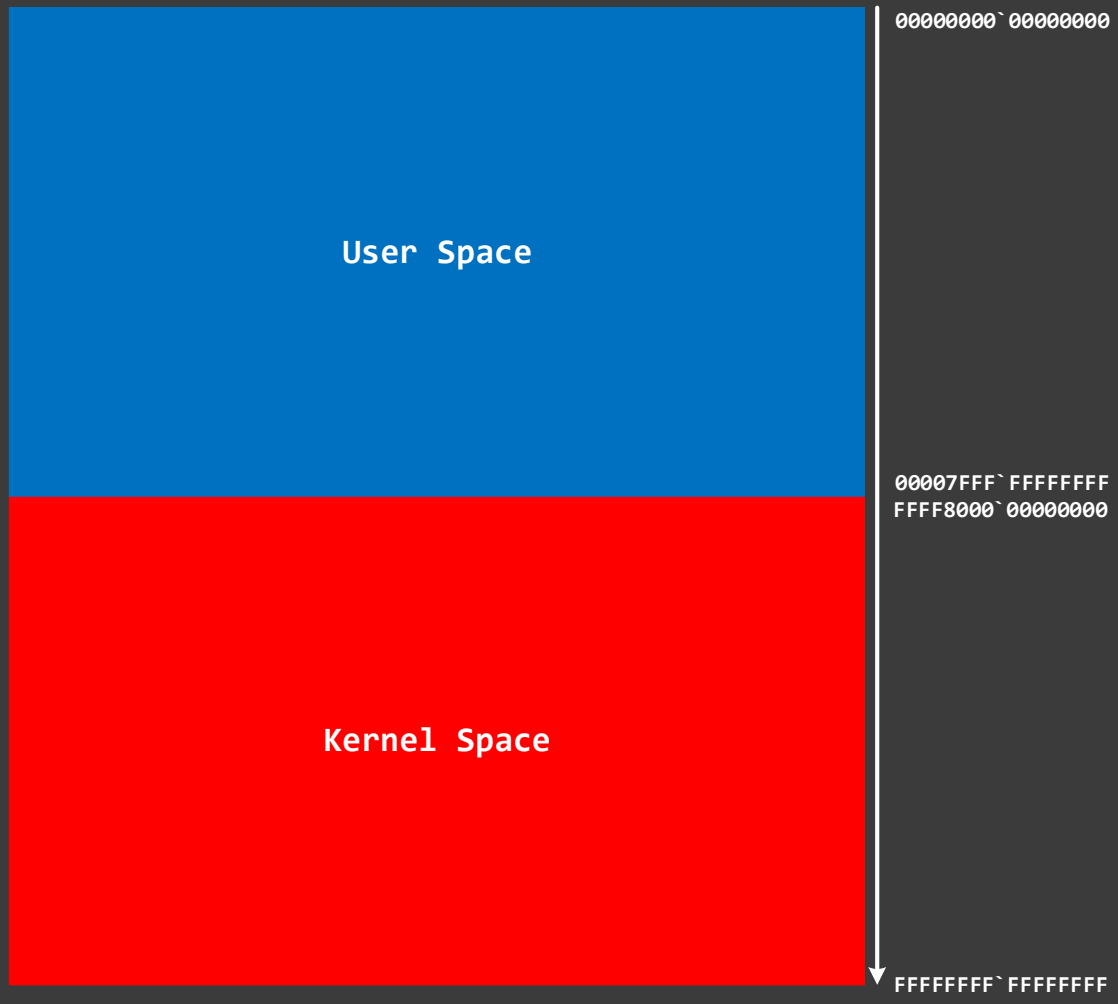
- Talk only about what I can show
- Lots of pictures
- Lots of examples
- Original content and examples

Part 1: Fundamentals

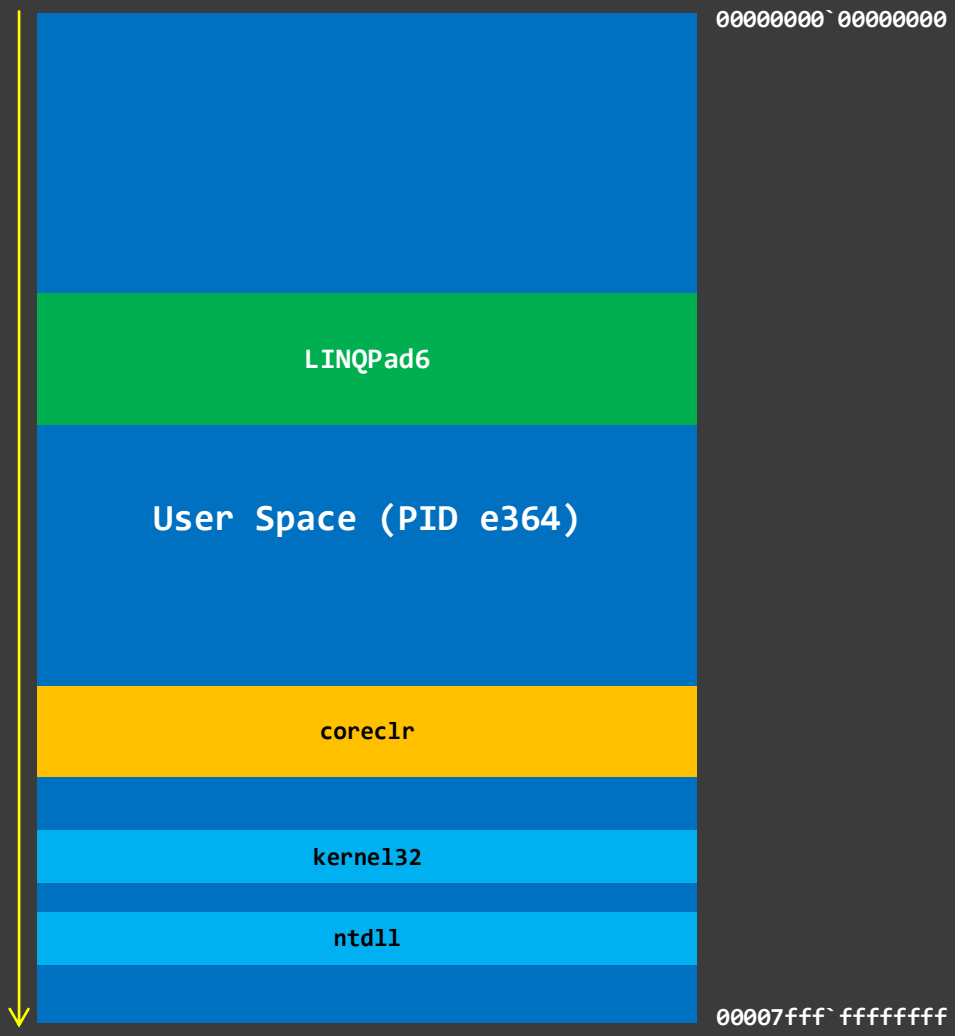
Memory Space (x86)



Memory Space (x64)



User / Managed Space



WinDbg Commands

lmv command lists all loaded modules (EXE and DLLs)

Types/Assemblies/Modules

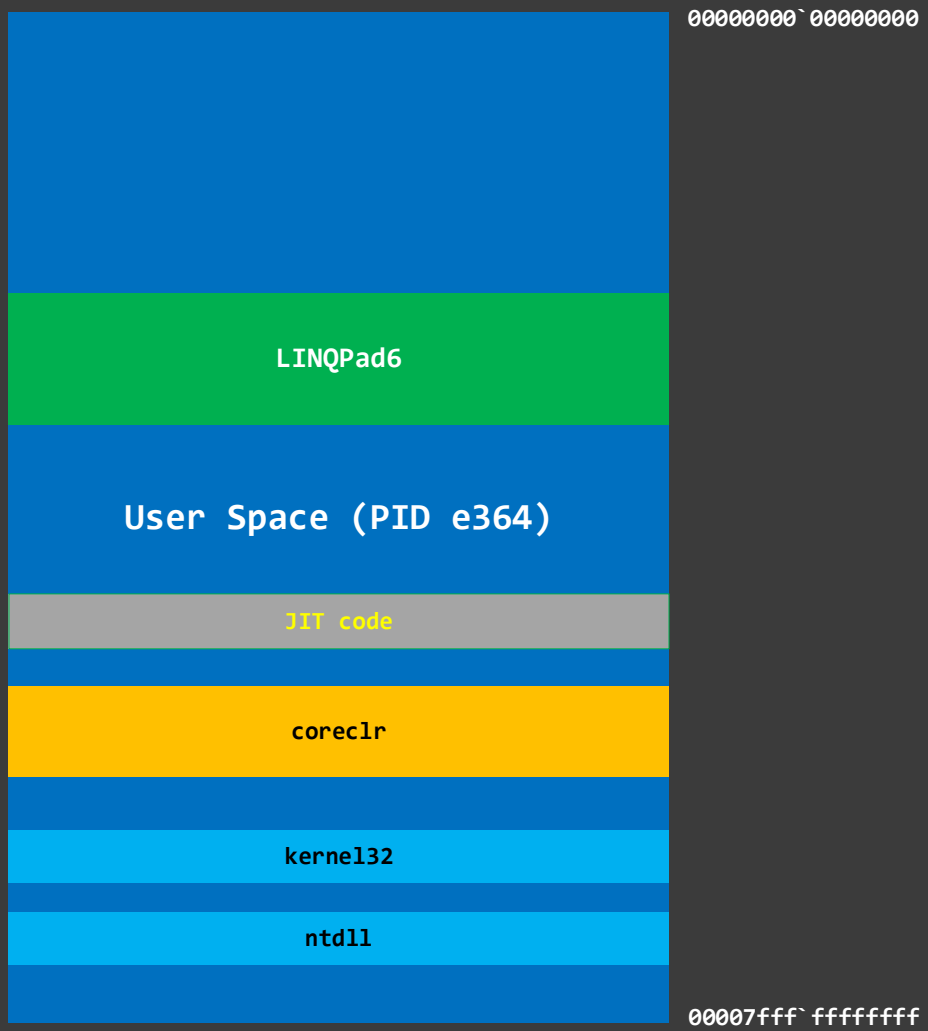
WinDbg Commands

lmv command lists all loaded modules (EXE and DLLs)

!IP2MD command shows type method and module address

!DumpModule command shows module name

Process Threads



WinDbg Commands

.load *<a path to SOS>*
Loads SOS WinDbg extension

~<n>s command switches between threads

k command shows unmanaged stack trace

!Threads command shows managed threads

!CLRStack command shows managed stack trace

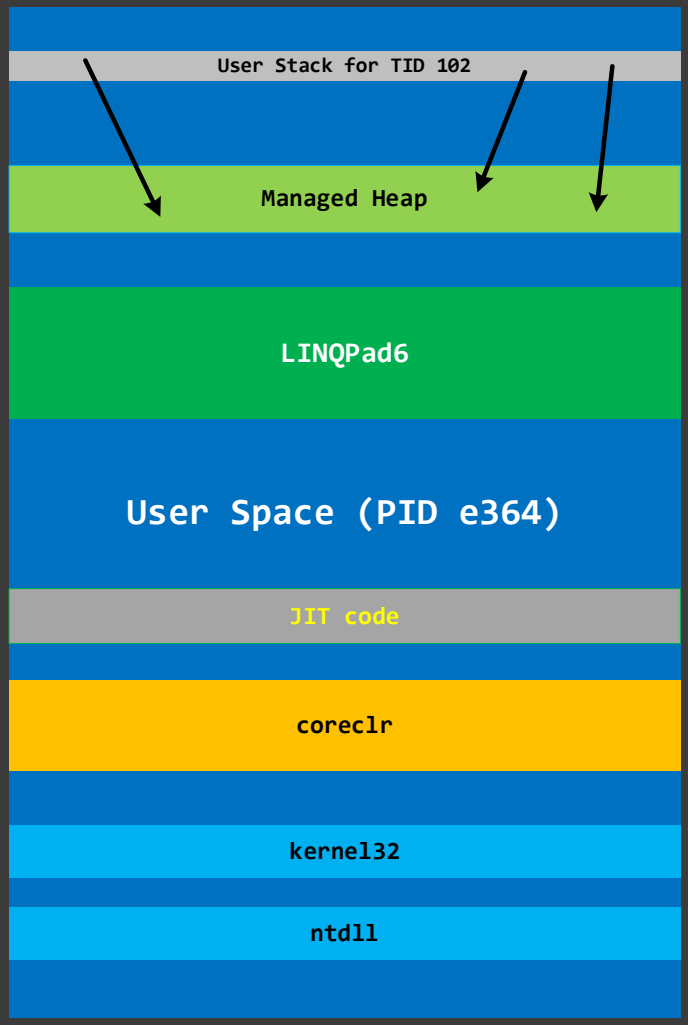
Example

```
0:000> kL
 # Child-SP          RetAddr           Call Site
00 00000029`6e3add78 00007ffa`7eb90458 win32u!NtUserWaitMessage+0x14
01 00000029`6e3add80 00007ffa`d7244d61 0x00007ffa`7eb90458
02 00000029`6e3ade40 00007ffa`d7247486 System_Windows_Forms!...+0x581
03 00000029`6e3adf50 00007ffa`d7247026 System_Windows_Forms!...+0x416
04 00000029`6e3ae000 00007ffa`d6ef212b System_Windows_Forms!...+0x46
05 00000029`6e3ae060 00007ffa`7cb021e4 System_Windows_Forms!...+0x3b
06 00000029`6e3ae0a0 00007ffa`7cae2534 0x00007ffa`7cb021e4
07 00000029`6e3ae350 00007ffa`7c70a16d 0x00007ffa`7cae2534
08 00000029`6e3ae680 00007ffa`7c7015c2 0x00007ffa`7c70a16d
09 00000029`6e3ae6e0 00007ffa`dc226ce3 0x00007ffa`7c7015c2
0a 00000029`6e3ae7b0 00007ffa`dc1bcc42 coreclr!CallDescrWorkerInternal+0x83
0b (Inline Function) --------`-------- coreclr!CallDescrWorkerWithHandler+0x57
0c 00000029`6e3ae7f0 00007ffa`dc1c3c09 coreclr!MethodDescCallSite::...+0x196
0d (Inline Function) --------`-------- coreclr!MethodDescCallSite::Call+0xb
0e 00000029`6e3ae930 00007ffa`dc1c4097 coreclr!RunMain+0x1f5
0f 00000029`6e3aeb10 00007ffa`dc1c4841 coreclr!Assembly::ExecuteMainMethod+0x1cb
10 00000029`6e3aeea0 00007ffa`dc0e21c1 coreclr!CorHost2::ExecuteAssembly+0x221
11 00000029`6e3af030 00007ffb`2ef54e2d coreclr!coreclr_execute_assembly+0x101
12 00000029`6e3af0d0 00007ffb`2ef62e27 hostpolicy!coreclr_t::execute_assembly+0x2d
13 00000029`6e3af120 00007ffb`2ef62a36 hostpolicy!run_app_for_context+0x387
14 00000029`6e3af280 00007ffb`2ef64262 hostpolicy!run_app+0x46
15 00000029`6e3af2d0 00007ffb`36ff3a7e hostpolicy!corehost_main+0x132
16 00000029`6e3af480 00007ffb`36ff72d8 hostfxr!execute_app+0x1de
17 (Inline Function) --------`-------- hostfxr!?A0xd51c85dd::read_config...+0x10a
18 00000029`6e3af570 00007ffb`36ff5b5b hostfxr!fx_muxer_t::handle_exec_...+0x214
19 00000029`6e3af660 00007ffb`36ff2109 hostfxr!fx_muxer_t::execute+0x39b
1a 00000029`6e3af7a0 00007ff6`ea712361 hostfxr!hostfxr_main_startupinfo+0x89
1b 00000029`6e3af8a0 00007ff6`ea712758 LINQPad6!exe_start+0x651
1c 00000029`6e3afad0 00007ff6`ea714608 LINQPad6!wmain+0x88
1d (Inline Function) --------`-------- LINQPad6!invoke_main+0x22
1e 00000029`6e3afb00 00007ffb`58387034 LINQPad6!__scrt_common_main_seh+0x10c
1f 00000029`6e3afb40 00007ffb`5a002651 kernel32!BaseThreadInitThunk+0x14
20 00000029`6e3afb70 00000000`00000000 ntdll!RtlUserThreadStart+0x21
```

```
0:000> !IP2MD 0x00007ffa`7cae2534
MethodDesc:   00007ffa7c7f5aa0
Method Name:  LINQPad.UIProgram.Go(System.String[])
Class:        00007ffa7c803a28
MethodTable:  00007ffa7c7f7078
mdToken:      00000000060001A4
Module:       00007ffa7c79f798
IsJitted:     yes
Current CodeAddr:     00007ffa7cae1b90
Version History:
  ILCodeVersion:      0000000000000000
  ReJIT ID:           0
  IL Addr:            0000000000000000
     CodeAddr:           00007ffa7cae1b90
(MinOptJitted)
     NativeCodeVersion:  0000000000000000

0:000> !DumpModule 00007ffa7c79f798
Name: C:\Program Files\LINQPad6\LINQPad.GUI.dll
Attributes:              PEFile
SupportsUpdateableMethods
Assembly:                00000177c5cdece0
BaseAddress:             00000177DFDE0000
PEFile:                  00000177C5CDE0E0
ModuleId:                00007FFA7C7D1860
ModuleIndex:             0000000000000001
LoaderHeap:              0000000000000000
TypeDefToMethodTableMap: 00007FFA7C7A0020
TypeRefToMethodTableMap: 00007FFA7C7A1860
MethodDefToDescMap:      00007FFA7C7A4138
FieldDefToDescMap:       00007FFA7C7AF300
MemberRefToDescMap:      0000000000000000
FileReferencesMap:       00007FFA7C7B7F78
AssemblyReferencesMap:   00007FFA7C7B7F80
MetaData start address:  00000177DFE887DC (719936
bytes)
```

Thread Stack Raw Data



WinDbg Commands

Get stack range:
!teb

Dump raw data:
dc / **dps** / **dpp** / **dpa** / **dpu**

Dump managed references:
!DumpStackObjects

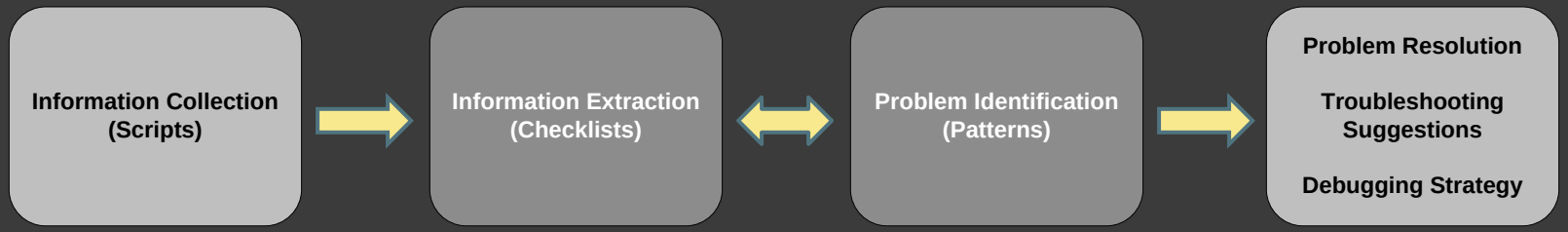
Pattern-Oriented Diagnostic Analysis

Diagnostic Pattern: a common recurrent identifiable problem together with a set of recommendations and possible solutions to apply in a specific context.

Diagnostic Problem: a set of indicators (symptoms, signs) describing a problem.

Diagnostic Analysis Pattern: a common recurrent analysis technique and method of diagnostic pattern identification in a specific context.

Diagnostics Pattern Language: common names of diagnostic and diagnostic analysis patterns. The same language for any operating system: Windows, Mac OS X, Linux, ...



Checklist: http://www.dumpanalysis.org/windows-memory-analysis-checklist

Part 2: Practice Exercises

Links

- Memory Dumps:

Not available in preview version

- Exercise Transcripts:

Not available in preview version

Exercise 0

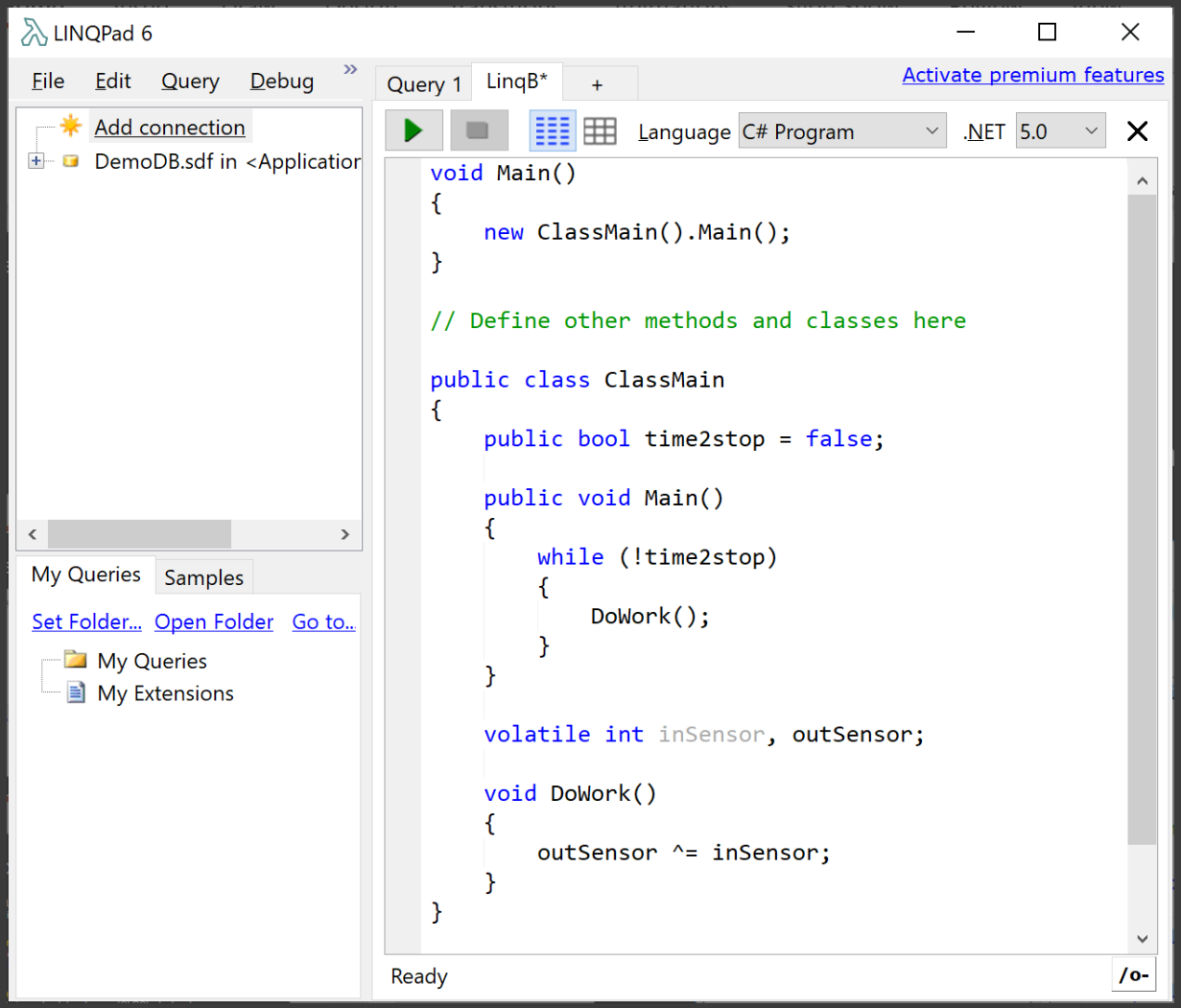
- **Goal:** Install Debugging Tools for Windows or WinDbg Preview or pull Docker WinDbg image and check that symbols are set up correctly
- **Patterns:** Incorrect Stack Trace; Truncated Stack Trace
- **Commands:** k
- \ANETMDA-Core-Dumps\Exercise-0-Download-Setup-WinDbg.pdf

Process Memory Dumps

Practice Exercises Core.PNx

.NET Core

Modeling with LINQPad 6



http://www.linqpad.net/

Exercise Core.PN1

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

Exercise Core.PN2

- **Goal:** Compare 64-bit process memory dump from exercise Core.PN1 with 32-bit process memory dump
- **Patterns:** Platform-Specific Debugger
- \ANETMDA-Core-Dumps\Exercise-Core-PN2-Analysis-process-dump-ApplicationA-32.pdf

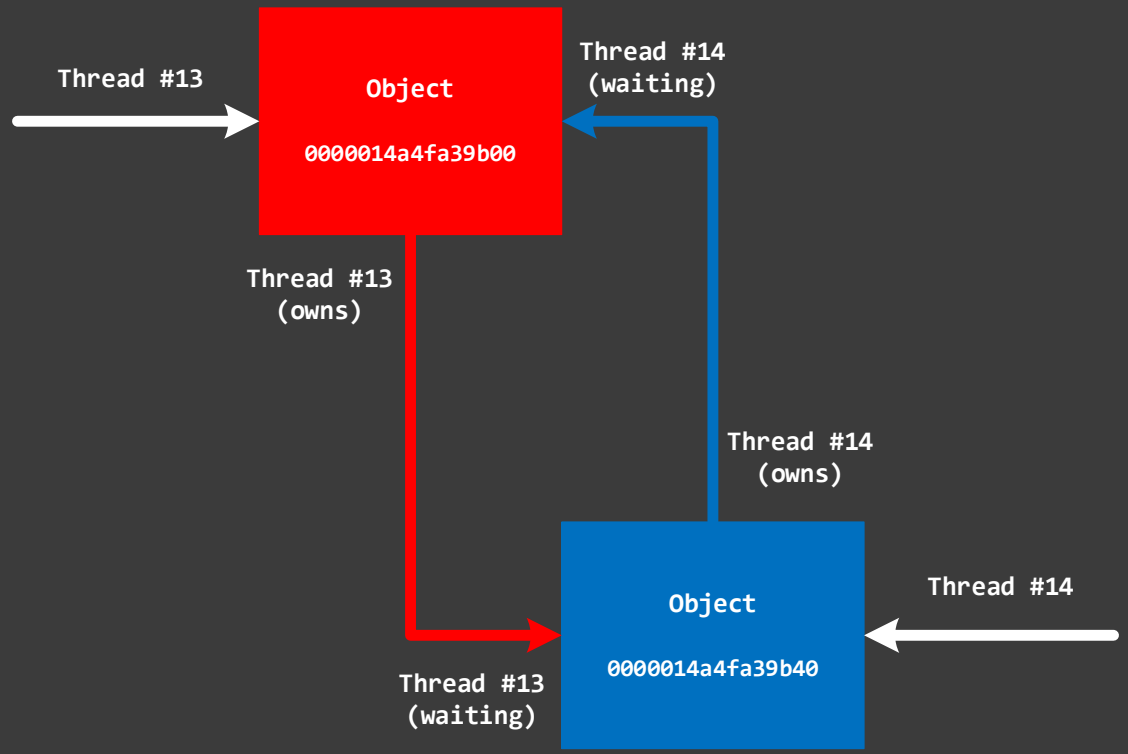
Exercise Core.PN3

- **Goal:** Learn how to find problem assemblies, modules, classes and methods, disassemble code, analyze CPU spikes
- **Patterns:** Active Thread; Manual Dump; Technology-Specific Subtrace; JIT Code; Spiking Thread; Annotated Disassembly
- **Commands:** !analyze -v -hang, !IP2MD, !runaway, ~<>k, !U, !DumpMD, !DumpClass, !DumpMT, !DumpModule, !DumpAssembly, !DumpDomain
- \ANETMDA-Core-Dumps\Exercise-Core-PN3-Analysis-process-dump-LINQPadB.pdf

Exercise Core.PN5

- **Goal:** Learn how to recognize and analyze deadlocks using SOS, execution residue, handled exceptions, dump object references
- **Patterns:** Special Thread; Wait Chain; Deadlock; Execution Residue (user space); Value References; Hidden Exception (user space); Coincidental Symbolic Information; Caller-n-Callee
- **Commands:** ~<>s, !Threads, !syncblk, !DumpObj, ub, dps, !DumpStack, !teb, dpS, !DumpStackObjects
- \ANETMDA-Core-Dumps\Exercise-Core-PN5-Analysis-process-dump-LINQPadC.pdf

Deadlock (x64, Core.PN5)



Exercise Core.PN7

- **Goal:** Learn how to analyze multiple managed exceptions
- **Patterns:** Managed Stack Trace Collection; Multiple Exceptions
- **Commands:** .sympath
- \ANETMDA-Core-Dumps\Exercise-Core-PN7-Analysis-process-dump-ApplicationD.pdf

Exercise Core.PN9

- **Goal:** Learn how to diagnose heap and handle leaks
- **Patterns:** Handle Leak; Memory Leak
- **Commands:** !heap, !address, !DumpHeap, ?, !eeheap, !GCHandles, !FinalizeQueue, !handle, .cxr
- \ANETMDA-Core-Dumps\Exercise-Core-PN9-Analysis-process-dump-LINQPadD.pdf

Exercise Core.PN11

- **Goal:** Learn how to recognize and analyze heap corruption
- **Patterns:** Regular Data; Managed Heap Corruption
- **Commands:** .formats, !VerifyHeap
- \ANETMDA-Core-Dumps\Exercise-Core-PN11-Analysis-process-dump-LINQPadE.pdf

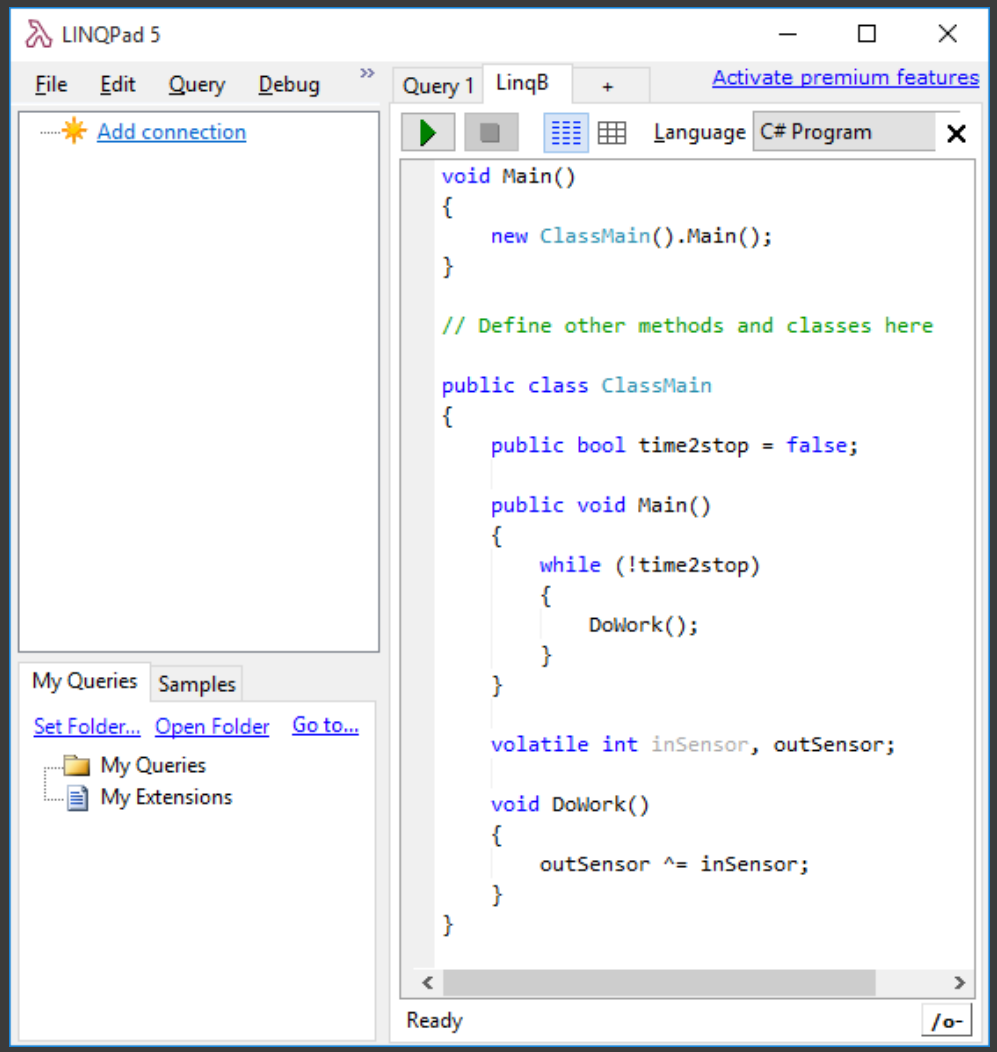
Process Memory Dumps

Practice Exercises

Framework.PN1 – Framework.PN12

.NET Framework

Modeling with LINQPad 5



http://www.linqpad.net/

Exercise Framework.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; Software Exception; Exception Stack Trace; Managed Code Exception; Managed Stack Trace
- **Commands:** .logopen, .symfix, .reload, ~*k, .load, !pe, ~*e, lmv, .chain, .unload, !analyze -v, !CLRStack, .logclose
- \ANETMDA-Dumps\Exercise-Framework-PN1-Analysis-process-dump-ApplicationA.pdf

Exercise Framework.PN2

- **Goal:** Compare 64-bit process memory dump from exercise Framework.PN1 with 32-bit process memory dump
- **Patterns:** Platform-Specific Debugger
- \ANETMDA-Dumps\Exercise-Framework-PN2-Analysis-process-dump-ApplicationA-32.pdf

Exercise Framework.PN3

- **Goal:** Learn how to find problem assemblies, modules, classes and methods, disassemble code, analyze CPU spikes
- **Patterns:** Active Thread; Technology-Specific Subtrace; JIT Code; Spiking Thread; Annotated Disassembly
- **Commands:** !analyze -v -hang, !IP2MD, !runaway, .prompt_allow, ~<>s, ~<>k, !U, !DumpMD, !DumpClass, !DumpMT, !DumpModule, !DumpAssembly, !DumpDomain
- \ANETMDA-Dumps\Exercise-Framework-PN3-Analysis-process-dump-LINQPadB.pdf

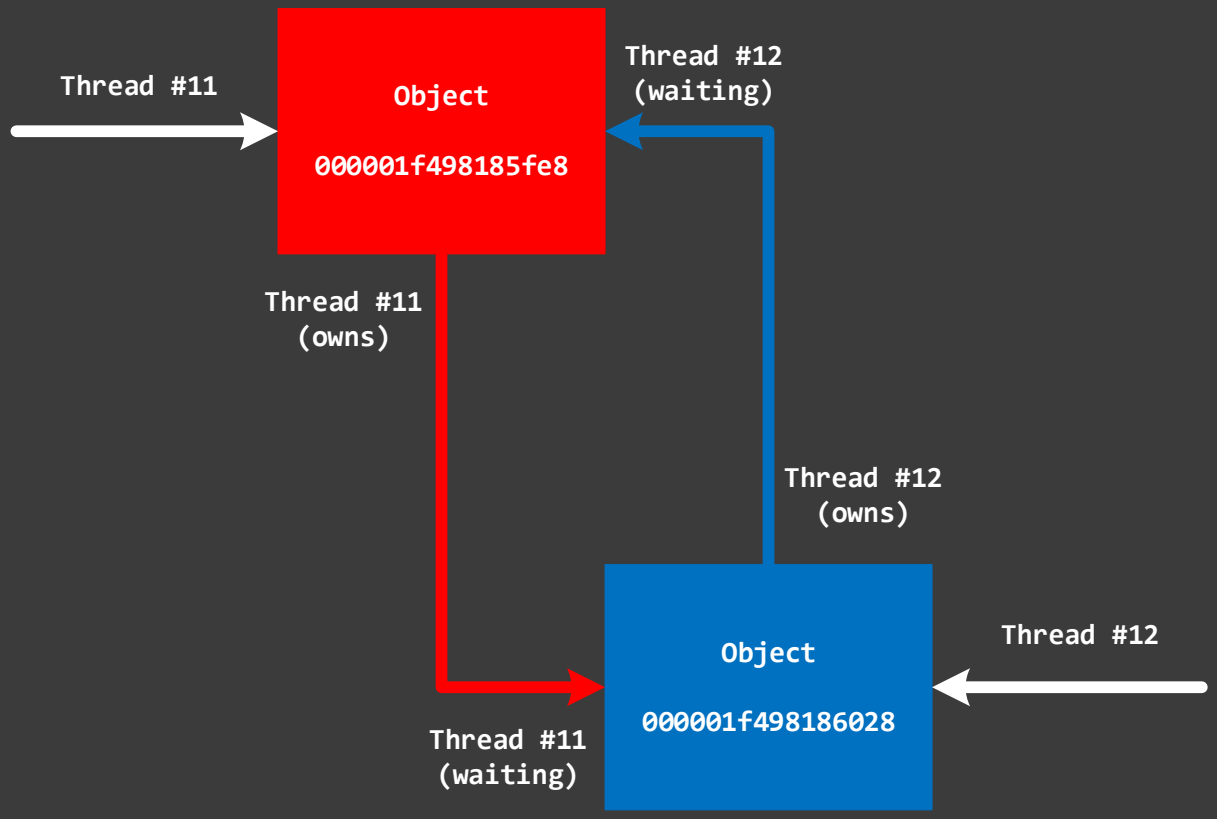
Exercise Framework.PN4

- **Goal:** Compare 64-bit process memory dump from exercise Framework.PN3 with 32-bit process memory dump
- \ANETMDA-Dumps\Exercise-Framework-PN4-Analysis-process-dump-LINQPadB-32.pdf

Exercise Framework.PN5

- **Goal:** Learn how to recognize and analyze deadlocks using SOS(EX), execution residue, handled exceptions, dump object references
- **Patterns:** Special Thread; Wait Chain; Deadlock; Execution Residue (user space); Hidden Exception (user space); Coincidental Symbolic Information; Caller-n-Callee
- **Commands:** ~*kL, !Threads, !syncblk, !DumpObj, ub, dp, !dlk, !DumpStack, !teb, dpS
- \ANETMDA-Dumps\Exercise-Framework-PN5-Analysis-process-dump-LINQPadC.pdf

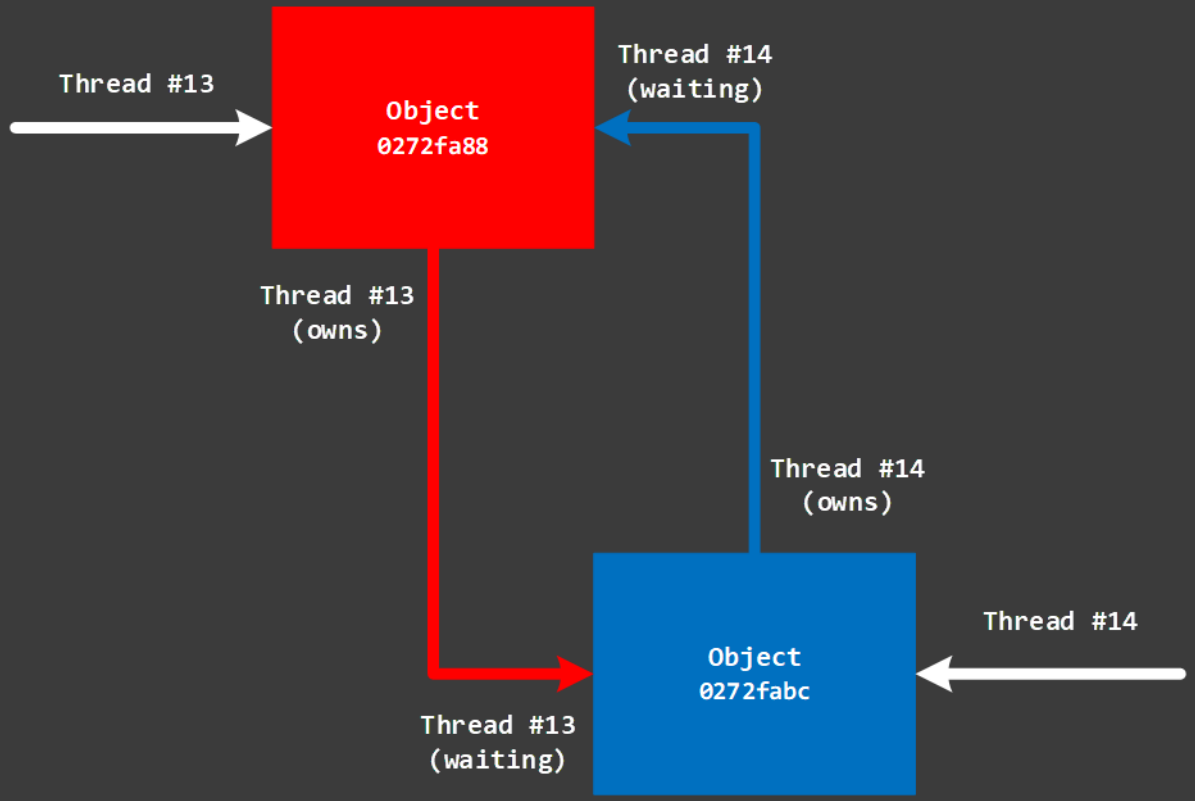
Deadlock (x64, Framework.PN5)



Exercise Framework.PN6

- **Goal:** Compare 64-bit process memory dump from exercise Framework.PN5 with 32-bit process memory dump
- **Patterns:** Execution Residue (managed space); Hidden Exception (managed space), Handled Exception
- **Commands:** !DumpStackObjects
- \ANETMDA-Dumps\Exercise-Framework-PN6-Analysis-process-dump-LINQPadC-32.pdf

Deadlock (x86, Framework.PN6)



Exercise Framework.PN7

- **Goal:** Learn how to analyze multiple managed exceptions
- **Patterns:** Managed Stack Trace Collection; Multiple Exceptions; Nested Exceptions; NULL Pointer
- \ANETMDA-Dumps\Exercise-Framework-PN7-Analysis-process-dump-ApplicationD.pdf

Exercise Framework.PN8

- **Goal:** Compare 64-bit process memory dump from exercise Framework.PN7 with 32-bit process memory dump
- \ANETMDA-Dumps\Exercise-Framework-PN8-Analysis-process-dump-ApplicationD-32.pdf

Exercise Framework.PN9

- **Goal:** Learn how to diagnose heap and handle leaks
- **Patterns:** Handle Leak; Memory Leak
- **Commands:** !heap, !address, !DumpHeap, ?, !eeheap, !GCHandles, !FinalizeQueue, !handle, .cxr
- \ANETMDA-Dumps\Exercise-Framework-PN9-Analysis-process-dump-LINQPadD.pdf

Exercise Framework.PN10

- **Goal:** Compare 64-bit process memory dump from exercise Framework.PN9 with 32-bit process memory dump
- \ANETMDA-Dumps\Exercise-Framework-PN10-Analysis-process-dump-LINQPadD-32.pdf

Exercise Framework.PN11

- **Goal:** Learn how to recognize and analyze heap corruption
- **Patterns:** Invalid Pointer; Regular Data; Managed Heap Corruption
- **Commands:** .formats, !VerifyHeap
- \ANETMDA-Dumps\Exercise-Framework-PN11-Analysis-process-dump-LINQPadE.pdf

Exercise Framework.PN12

- **Goal:** Compare 64-bit process memory dump from exercise Framework.PN11 with 32-bit process memory dump
- \ANETMDA-Dumps\Exercise-Framework-PN12-Analysis-process-dump-LINQPadE-32.pdf

Pattern Links

CLR Thread
Managed Code Exception
Nested Exceptions
Mixed Exception
Memory Leak
JIT Code
Managed Stack Trace
Multiple Exceptions
Version-Specific Extension
Caller-n-Callee
Hidden Exception
Deadlock
Duplicate Extension
Stack Trace Collection
Dynamic Memory Corruption
Special Thread
Execution Residue
Handled Exception
Annotated Disassembly
Technology-Specific Subtrace
Wait Chain
Object Distribution Anomaly

CLR-related and managed

Incorrect Stack Trace
Execution Residue
NULL Pointer
Handle Leak
Exception Stack Trace
Software Exception
Platform-Specific Debugger
Spiking Thread
Hidden Exception
Regular Data
Coincidental Symbolic Information
Active Thread
Truncated Stack Trace
Value References
Manual Dump

Unmanaged user space

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)

Resources

- WinDbg Help / WinDbg.org (quick links) / DumpAnalysis.org
- WinDbg images https://hub.docker.com/r/patterndiagnostics/windbg
- .NET Runtime https://github.com/dotnet/runtime
- Accelerated Windows Memory Dump Analysis, 5th Edition
- Encyclopedia of Crash Dump Analysis Patterns, 3rd Edition
- Memory Dump Analysis Anthology (Volumes 1 – 13)

Q&A

Please send your feedback using the contact form on PatternDiagnostics.com

Thank you for attendance!