

Malicious Code Analysis

Fangtian Zhong
CSCI 591

Gianforte School of Computing
Norm Asbjornson College of Engineering
E-mail: fangtian.zhong@montana.edu





Overview

03

**Source Level
Debugging**

04

**Kernel
Debugging**

05

**Packer and
Shellcode**



Part Three

03

Source-Level Debugging





Installing Visual Studio 2022

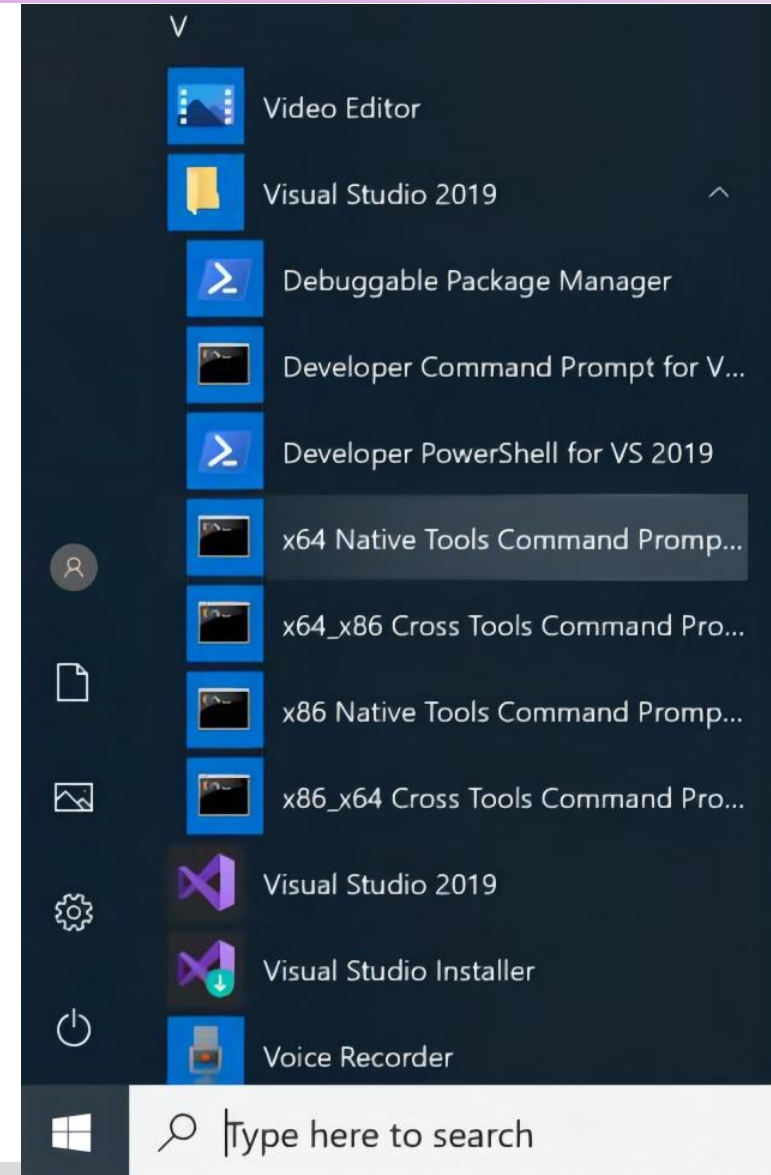
- ★ Download it from <https://visualstudio.microsoft.com/vs/older-downloads/>





Preparing to Compile C++ Code

- ★ Click **Start**. Scroll down to the programs starting with V. Expand the "Visual Studio 2022" section.
- ★ Click "**x64 Native Tools Command Prompt**", as shown below.





Creating a C++ Program

In the "x64 Native Tools Command Prompt" window, execute these commands:

```
mkdir c:\MyApp  
cd c:\MyApp  
notepad MyApp.cpp
```

Click **Yes** to create a new file.

Paste in this code, as shown below.

```
void MyFunction(long p1, long p2, long p3)  
{  
    long x = p1 + p2 + p3;  
    long y = 0;  
    y = x / p2;  
}  
  
void main ()  
{  
    long a = 2;  
    long b = 0;  
    MyFunction(a, b, 5);  
}
```

In Notepad, save the file.

```
MyApp.cpp - Notepad  
File Edit Format View Help  
void MyFunction(long p1, long p2, long p3)  
{  
    long x = p1 + p2 + p3;  
    long y = 0;  
    y = x / p2;  
}  
  
void main ()  
{  
    long a = 2;  
    long b = 0;  
    MyFunction(a, b, 5);  
}  
  
Windows (CI Ln 12, Col 2: 100%
```



Compiling a C++ Program Without Symbols



In t

the

cl

dir



As

and

```
x64 Native Tools Command Prompt for VS 2019

c:\MyApp>cl MyApp.cpp
Microsoft (R) C/C++ Optimizing Compiler Version 19.29.30038.1 for x64
Copyright (C) Microsoft Corporation. All rights reserved.

MyApp.cpp
Microsoft (R) Incremental Linker Version 14.29.30038.1
Copyright (C) Microsoft Corporation. All rights reserved.

/out:MyApp.exe
MyApp.obj

c:\MyApp>dir
Volume in drive C is windows 10
Volume Serial Number is B009-E7A9

Directory of c:\MyApp

11/02/2021  05:05 PM    <DIR>          .
11/02/2021  05:05 PM    <DIR>          ..
11/02/2021  05:04 PM                192  MyApp.cpp
11/02/2021  05:05 PM            95,744  MyApp.exe
11/02/2021  05:05 PM             1,215  MyApp.obj
               3 File(s)            97,151 bytes
               2 Dir(s)  73,964,826,624 bytes free

c:\MyApp>
```

ite

file



Laurel



Click to



In Win



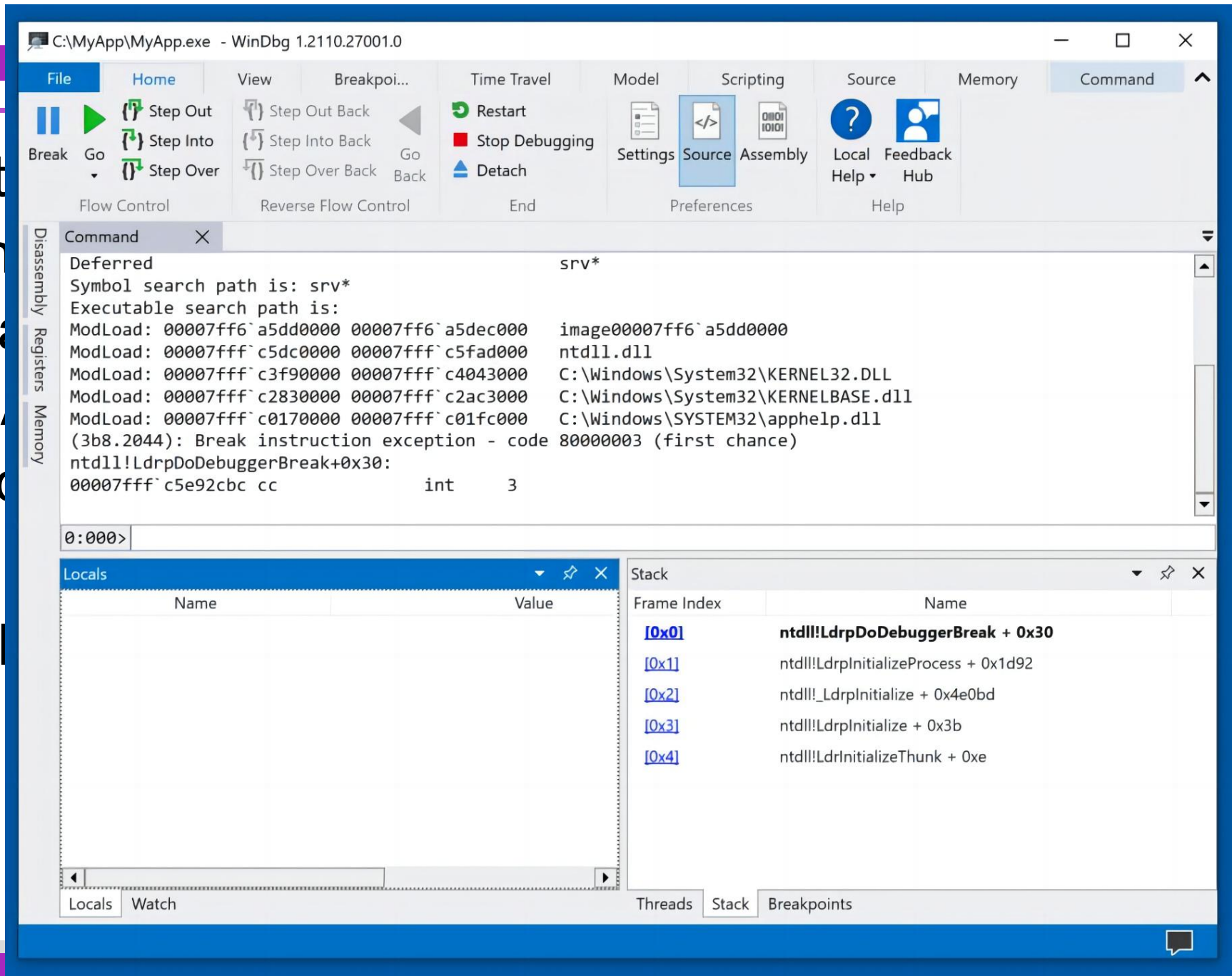
Naviga

C:\My

and do



The ap



MyApp

review".



Find



In the

x MyApp

x MyApp



There

C:\MyApp\MyApp.exe - WinDbg 1.2110.27001.0

File Home View Breakpoi... Time Travel Model Scripting Source Memory Command

Break Go Step Out Step Into Step Over Step Out Back Step Into Back Step Over Back Go Back Restart Stop Debugging Detach Settings Source Assembly Local Help Feedback Hub

Flow Control Reverse Flow Control End Preferences Help

Disassembly Registers Memory

Command

```
ModLoad: 00007ff6`a5dd0000 00007ff6`a5dec000 image00007ff6`a5dd0000
ModLoad: 00007fff`c5dc0000 00007fff`c5fad000 ntdll.dll
ModLoad: 00007fff`c3f90000 00007fff`c4043000 C:\Windows\System32\KERNEL32.DLL
ModLoad: 00007fff`c2830000 00007fff`c2ac3000 C:\Windows\System32\KERNELBASE.dll
ModLoad: 00007fff`c0170000 00007fff`c01fc000 C:\Windows\SYSTEM32\apphelp.dll
(3b8.2044): Break instruction exception - code 80000003 (first chance)
ntdll!LdrpDoDebuggerBreak+0x30:
00007fff`c5e92cbc cc int 3
0:000> x MyApp!*main*
*** WARNING: Unable to verify checksum for C:\MyApp\MyApp.exe
0:000> x MyApp!*
```

0:000>

Locals

Name	Value
------	-------

Stack

Frame Index	Name
[0x0]	ntdll!LdrpDoDebuggerBreak + 0x30
[0x1]	ntdll!LdrpInitializeProcess + 0x1d92
[0x2]	ntdll!_LdrpInitialize + 0x4e0bd
[0x3]	ntdll!LdrpInitialize + 0x3b
[0x4]	ntdll!LdrInitializeThunk + 0xe

Locals Watch Threads Stack Breakpoints

ds:



Sh



To s

Im



The

show



This

Win



This

C:\MyApp\MyApp.exe - C:\MyApp\MyApp.exe - WinDbg 1.0.2007.06001 (Administrator)

File Home View Breakpoints Time Travel Model Scripting Command Source

Break Go Step Out Step Into Step Over Step Out Back Step Into Back Step Over Back Restart Stop Debugging Detach Settings Source Assembly Local Help Feedback Hub

Flow Control Reverse Flow Control End Preferences Help

Disassembly Registers Memory

Command

```
ModLoad: 76bd0000 76cb0000 C:\Windows\SysWOW64\KERNEL32.DLL
ModLoad: 77090000 7728b000 C:\Windows\SysWOW64\KERNELBASE.dll
ModLoad: 6d770000 6d80c000 C:\Windows\SysWOW64\apphelp.dll
(20c4.f68): Break instruction exception - code 80000003 (first chance)
eax=00000000 ebx=00e95000 ecx=020b0000 edx=00000000 esi=01282560 edi=77e637ec
eip=77eff0f6 esp=00d9f6c0 ebp=00d9f6ec iopl=0         nv up ei pl zr na pe nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00000246
ntdll!LdrpDoDebuggerBreak+0x2b:
77eff0f6 cc                int     3
0:000> x MyApp!*main*
*** WARNING: Unable to verify checksum for C:\MyApp\MyApp.exe
0:000> x MyApp!*
0:000> lm
start      end          module_name
00050000 00067000    MyApp        C:(no symbols)
6d770000 6d80c000    apphelp     (deferred)
76bd0000 76cb0000    KERNEL32    (deferred)
77090000 7728b000    KERNELBASE  (deferred)
77e50000 77fec000    ntdll       (pdb symbols) C:\ProgramData\Dbg\sym\wntd11.pdb\C940A95F85178140032F4BA53A6D75F31\wntd11.pdb
0:000>
```

Locals

Name	Value
------	-------

Stack

Frame Index	Name
[0x0]	ntdll!LdrpDoDebuggerBreak + 0x2b
[0x1]	ntdll!LdrpInitializeProcess + 0x1b20
[0x2]	ntdll!_LdrpInitialize + 0xb0
[0x3]	ntdll!LdrInitializeThunk + 0x11

Locals Watch Threads Stack Breakpoints

se



Co



In the
thes

del

del

cl /Z

dir



As s
and

x64 Native Tools Command Prompt for VS 2019

```
c:\MyApp>del MyApp.exe
```

```
c:\MyApp>del MyApp.obj
```

```
c:\MyApp>cl /Zi MyApp.cpp
```

```
Microsoft (R) C/C++ Optimizing Compiler Version 19.29.30038.1 for x64  
Copyright (C) Microsoft Corporation. All rights reserved.
```

```
MyApp.cpp
```

```
Microsoft (R) Incremental Linker Version 14.29.30038.1  
Copyright (C) Microsoft Corporation. All rights reserved.
```

```
/out:MyApp.exe
```

```
/debug
```

```
MyApp.obj
```

```
c:\MyApp>dir
```

```
Volume in drive C is windows 10  
Volume Serial Number is B009-E7A9
```

```
Directory of c:\MyApp
```

11/02/2021	05:12 PM	<DIR>	.
11/02/2021	05:12 PM	<DIR>	..
11/02/2021	05:04 PM		192 MyApp.cpp
11/02/2021	05:12 PM		559,104 MyApp.exe
11/02/2021	05:12 PM		3,212,080 MyApp.ilc
11/02/2021	05:12 PM		2,003 MyApp.obj
11/02/2021	05:12 PM		6,311,936 MyApp.pdb
11/02/2021	05:12 PM		77,824 vc140.pdb
		6 File(s)	10,163,139 bytes
		2 Dir(s)	74,046,545,920 bytes free

```
c:\MyApp>
```

ute

file



La

App



In W



Nav

C:\M

and



The

Command Window Output:

```
CommandLine: C:\MyApp\MyApp.exe

***** Path validation summary *****
Response          Time (ms)      Location
Deferred          0              srv*
Deferred          0              symsrv*symsrv.dll*C:\Symbols*https://msdl.microsoft.com/download/symbols
Symbol search path is: srv*;symsrv*symsrv.dll*C:\Symbols*https://msdl.microsoft.com/download/symbols
Executable search path is:
ModLoad: 001f0000 00257000 MyApp.exe
ModLoad: 77e50000 77fec000 ntdll.dll
ModLoad: 76bd0000 76cb0000 C:\Windows\SysWOW64\KERNEL32.DLL
ModLoad: 77090000 7728b000 C:\Windows\SysWOW64\KERNELBASE.dll
ModLoad: 6d770000 6d80c000 C:\Windows\SysWOW64\apphelp.dll
(32e4.f24): Break instruction exception - code 80000003 (first chance)
eax=00000000 ebx=00b1d000 ecx=0ed80000 edx=00000000 esi=002b2570 edi=77e637ec
eip=77eff0f6 esp=00cff534 ebp=00cff560 iopl=0         nv up ei pl zr na pe nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00000246
ntdll!LdrpDoDebuggerBreak+0x2b:
77eff0f6 cc                int     3
```

Stack Window:

Frame Index	Name
[0x0]	ntdll!LdrpDoDebuggerBreak + 0x2b
[0x1]	ntdll!LdrpInitializeProcess + 0x1b20
[0x2]	ntdll!_LdrpInitialize + 0xb0
[0x3]	ntdll!LdrInitializeThunk + 0x11



Finding

> In the lower

x MyApp!*r

> Now it finds

The screenshot shows the WinDbg interface with the disassembly of the `MyApp!main` function. The command window shows the disassembly starting at `0:000> x MyApp!*main*`. The disassembly list shows the function `MyApp!main` at address `00007ff6`40866ec0`. The stack window shows the current frame at `ntdll!LdrpDoDebuggerBreak + 0x30`.

```
0:000> x MyApp!*main*
*** WARNING: Unable to verify checksum for MyApp.exe
00007ff6`408e1000 MyApp!  scr_t_native_dllmain_reason = 0xffffffff
00007ff6`40866ec0 MyApp!main (void)
00007ff6`40867284 MyApp!  scr_t_main_policy::set_app_type (void)
00007ff6`408674f8 MyApp!  scr_t_dllmain_uninitialize_c (void)
00007ff6`40867240 MyApp!invoke_main (void)
00007ff6`408672cc MyApp!mainCRTStartup (void *)
00007ff6`40867414 MyApp!  scr_t_dllmain_before_initialize_c (void)
00007ff6`40867464 MyApp!  scr_t_dllmain crt thread detach (void)
00007ff6`40867430 MyApp!  scr_t_dllmain crt thread attach (void)
00007ff6`40867040 MyApp!  scr_t_common_main_seh (void)
00007ff6`40867534 MyApp!  scr_t_dllmain_uninitialize_critical (void)
00007ff6`40867028 MyApp!  scr_t_common_main (void)
00007ff6`408c9e80 MyApp!`__scr_t_common_main_seh'::`1'::filt$0 (void)
00007ff6`408673d0 MyApp!  scr_t_dllmain_after_initialize_c (void)
00007ff6`40867480 MyApp!  scr_t_dllmain_exception_filter (struct HINSTANCE__ *, unsigned long, void *, <fun
00007ff6`4086712a MyApp!invoke_main = (inline caller) MyApp!__scr_t_common_main_seh+ea
00007ff6`40866f16 MyApp!  scr_t_main_policy::set_app_type = (inline caller) MyApp!pre_c_initialization+6
00007ff6`408672d0 MyApp!  scr_t_common_main = (inline caller) MyApp!mainCRTStartup+4
```

Frame Index	Name
[0x0]	ntdll!LdrpDoDebuggerBreak + 0x30
[0x1]	ntdll!LdrpInitializeProcess + 0x1d92
[0x2]	ntdll!LdrpInitialize + 0x4e0bd
[0x3]	ntdll!LdrpInitialize + 0x3b
[0x4]	ntdll!LdrpInitializeThunk + 0xe

and:

shown below.



Setting a

> In the lower

bu MyApp!

> In WinDbg,

> The app runs
the C++ source
instruction h

> At the lower
variables. R

C:\MyApp\MyApp.exe - WinDbg 1.2110.27001.0

File Home View Breakp... Time Tra... Model Scripting Source Memory Command

Break Go Step Out Step Out Back Step Into Step Into Back Step Over Step Over Back Go Back

Flow Control Reverse Flow Control End Preferences Help

MyApp.cpp X Command X

```
1 void MyFunction(long p1, long p2, long p3)
2 {
3     long x = p1 + p2 + p3;
4     long y = 0;
5     y = x / p2;
6 }
7
8 void main ()
9 {
10     long a = 2;
11     long b = 0;
12     MyFunction(a, b, 5);
13 }
```

0:000> bu MyApp!main
0:000> g
Breakpoint 0 hit
MyApp!main:
00007ff6`40866ec0 4883ec38 sub rsp,38h

Locals

Name	Value
a	0
b	0

Stack

Frame Index	Name
[0x0]	MyApp!main
[0x1]	MyApp!invoke_main + 0x22
[0x2]	MyApp!__scrt_common_main_seh + 0x10c
[0x3]	KERNEL32!BaseThreadInitThunk + 0x14
[0x4]	ntdll!RtlUserThreadStart + 0x21

Locals Watch Threads Stack Breakpoints

and:

t pane shows
rent

ows the local



Stepping

> In WinDbg,

> As shown by the code. The v

The screenshot shows the WinDbg interface with the source code of `MyApp.cpp` loaded. The code is as follows:

```
1 void MyFunction(long p1, long p2, long p3)
2 {
3     long x = p1 + p2 + p3;
4     long y = 0;
5     y = x / p2;
6 }
7
8 void main ()
9 {
10    long a = 2;
11    long b = 0;
12    MyFunction(a, b, 5);
13 }
```

The command window shows the following commands and output:

```
0:000> bu MyApp!main
0:000> g
Breakpoint 0 hit
MyApp!main:
00007ff6`40866ec0 4883ec38      sub     rsp,38h
0:000> t
MyApp!main+0x4:
00007ff6`40866ec4 c744242402000000 mov     dword ptr [rsp+24h],2 ss
0:000> t
MyApp!main+0xc:
00007ff6`40866ecc c744242000000000 mov     dword ptr [rsp+20h],0 ss
```

The Locals window shows the following variables:

Name	Value
a	2
b	0

The Stack window shows the following stack frames:

Frame Index	Name
[0x0]	MyApp!main + 0xc
[0x1]	MyApp!invoke_main + 0x22
[0x2]	MyApp!_scrt_common_main_seh + 0x10c
[0x3]	KERNEL32!BaseThreadInitThunk + 0x14
[0x4]	ntdll!RtlUserThreadStart + 0x21

of the source



Stepping



In WinDbg,
until the pro



The program
divide-by-zero

0:000> g
Breakpoint 0 hit
MyApp!main:
00007ff6`40866ec0 4883ec38 sub rsp,38h
0:000> t
MyApp!main+0x4:
00007ff6`40866ec4 c744242402000000 mov dword ptr [rsp+24h],2 ss
0:000> t
MyApp!main+0xc:
00007ff6`40866ecc c744242400000000 mov dword ptr [rsp+20h],0 ss
0:000> g
(ec.2a0): Integer divide-by-zero - code c0000094 (first chance)
First chance exceptions are reported before any exception handling.
This may be expected and handled.
MyApp!MyFunction+0x30:
00007ff6`40866ea0 f77c2428 idiv eax,dword ptr [rsp+28h] s
0:000> g
(ec.2a0): Integer divide-by-zero - code c0000094 (!!! second chance)
MyApp!MyFunction+0x30:
00007ff6`40866ea0 f77c2428 idiv eax,dword ptr [rsp+28h] s
0:000>

Locals

Name	Value
x	7
y	0
p1	2
p2	0
p3	5

Stack

Frame Index	Name
[0x0]	MyApp!MyFunction + 0x30
[0x1]	MyApp!main + 0x27
[0x2]	MyApp!invoke_main + 0x22
[0x3]	MyApp!_scrt_common_main_seh + 0x10c
[0x4]	KERNEL32!BaseThreadInitThunk + 0x14
[0x5]	ntdll!RtlUserThreadStart + 0x21

more times,

use of a



Part Four

04

2025-10-19

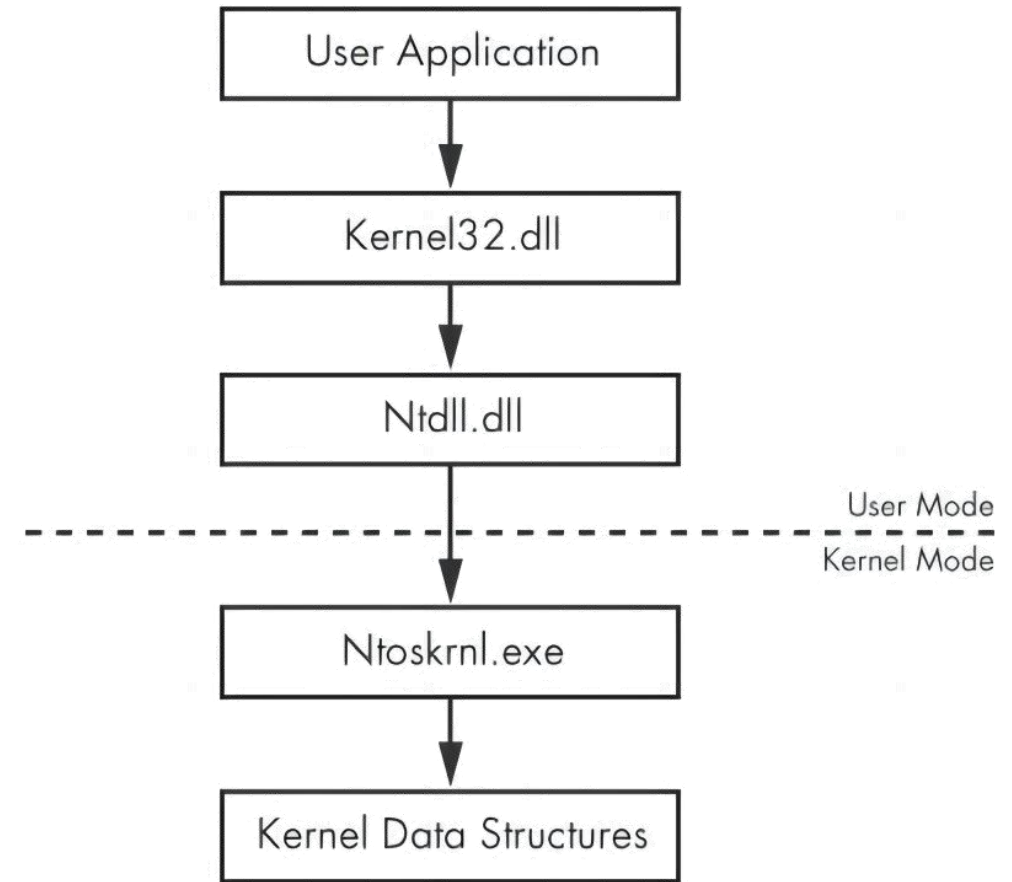
Kernel Debugging





User Mode and Kernel Mode

- » To use WinDbg Preview for kernel debugging.
- » The kernel is the heart of the operating system, and it resides in the file `ntoskrnl.exe`, as shown in the figure below, from the "Practical Malware Analysis" book.



User mode and kernel mode



Installing CFF Explorer

- If you are using the "Windows 10 w Tools" VM, CFF Explorer is already installed.
- If you are using some other machine, go to this URL and install "Explorer Suite":
https://ntcore.com/?page_id=388



Exam

» Launch F

» Right-click

» In CFF Ex

» As shown
ntoskrnl.e

CFF Explorer VIII - [ntoskrnl.exe]

File Settings ?

ntoskrnl.exe

- File: ntoskrnl.exe
 - Dos Header
 - Nt Headers
 - File Header
 - Optional Header
 - Data Directories [x]
 - Section Headers [x]
 - Export Directory
 - Import Directory
 - Resource Directory
 - Exception Directory
 - Relocation Directory
 - Debug Directory
 - Address Converter
 - Dependency Walker
 - Hex Editor
 - Identifier
 - Import Adder
 - Quick Disassembler
 - Rebuilder
 - Resource Editor

Member	Offset	Size	Value
Characteristics	0084E200	Dword	00000000
TimeDateStamp	0084E204	Dword	63584BD8
MajorVersion	0084E208	Word	0000
MinorVersion	0084E20A	Word	0000
Name	0084E20C	Dword	0095810A
Base	0084E210	Dword	00000001
NumberOfFunctions	0084E214	Dword	00000B4E
NumberOfNames	0084E218	Dword	00000B47
AddressOfFunctions	0084E21C	Dword	00951028

Ordinal	Function RVA	Name Ordinal	Name RVA	Name
N/A	0084E244	00853C8A	00850F60	00855317
(nFunctions)	Dword	Word	Dword	szAnsi
00000001	0060A7C0	N/A	N/A	N/A
00000002	001B51E0	N/A	N/A	N/A
00000003	003175A0	N/A	N/A	N/A
00000004	001699A0	N/A	N/A	N/A
00000005	002774B0	N/A	N/A	N/A
00000006	00130430	N/A	N/A	N/A
00000007	0010E5B0	N/A	N/A	N/A
00000008	00846E10	0007	00958117	AlpcCreateSecurityContext
00000009	0008C350	0008	00958131	AlpcGetHeaderSize
0000000A	0008C1D0	0009	00958143	AlpcGetMessageAttribute
0000000B	0008C2F0	000A	0095815B	AlpcInitializeMessageAttribute

er

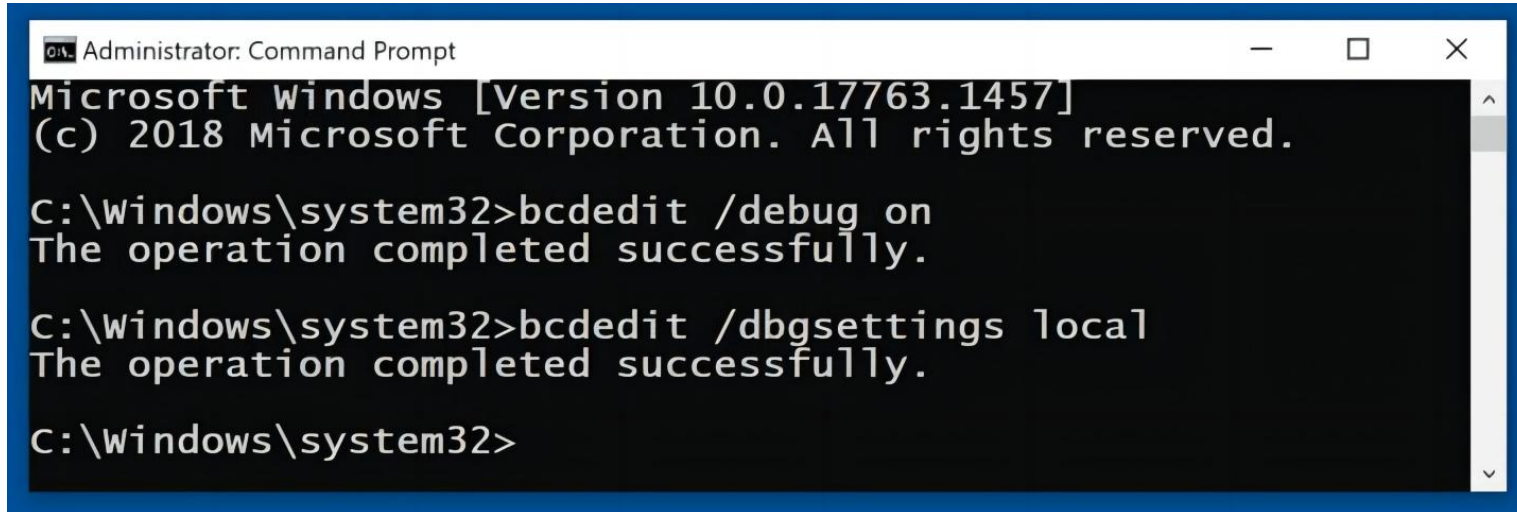
32.

orer".

Using BCDEdit for Local Debugging

- This process enables "local" kernel-mode debugging, so you can observe kernel routines and data but you cannot use breakpoints.
- Click the **Start** button and type **CMD**. Right-click "**Command Prompt**" and click "**Run as administrator**". Click **Yes**.
- Execute these commands:

bcdedit /debug on
bcdedit /dbgsettings local



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1457]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>bcdedit /debug on
The operation completed successfully.

C:\Windows\system32>bcdedit /dbgsettings local
The operation completed successfully.

C:\Windows\system32>
```

- Restart your Windows machine.

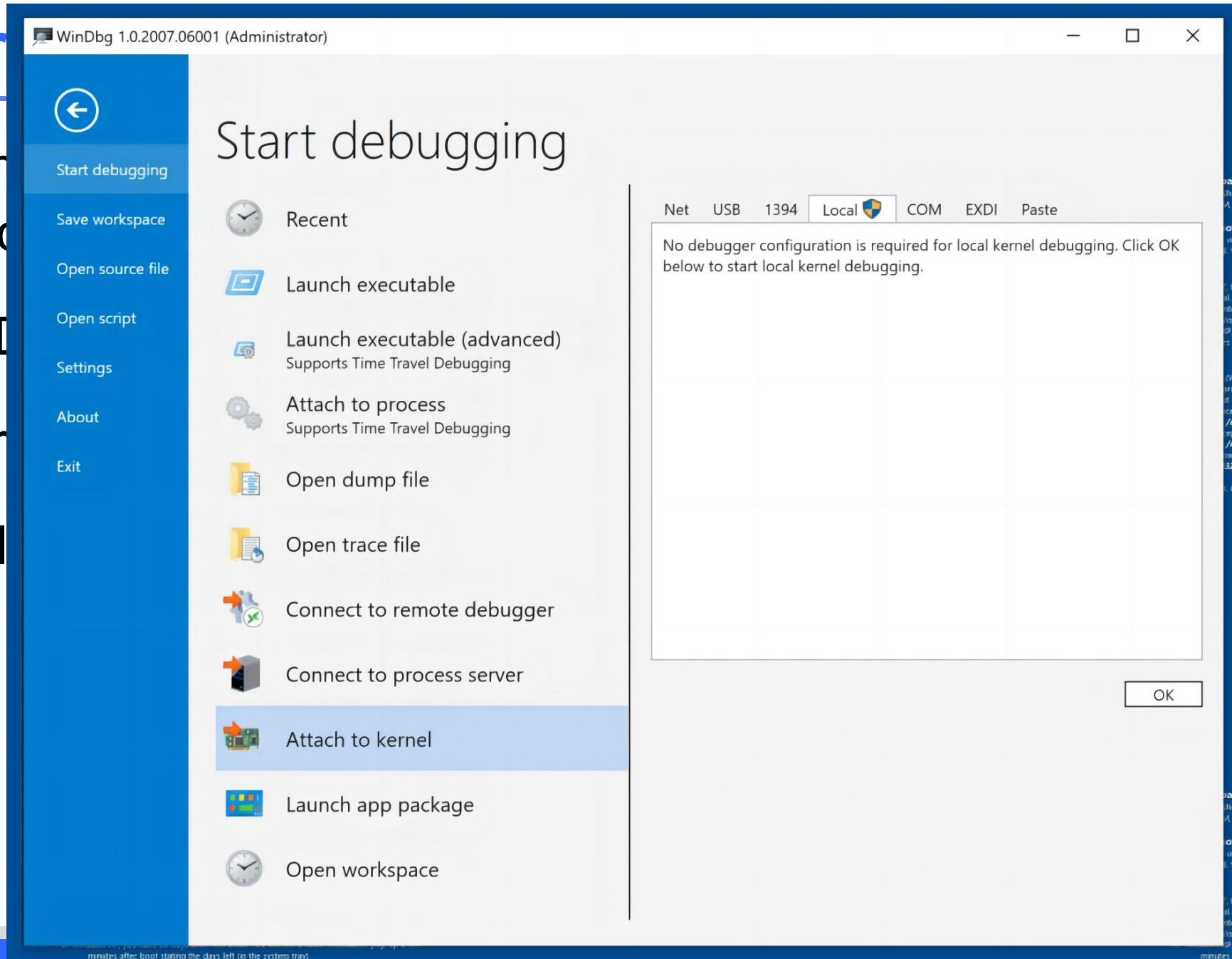


>> Click the
and click

>> In WinDbg

>> In the menu

>> At the bottom



review"



KD "", Local Connection - WinDbg 1.0.2007.06001 (Administrator)

File Home View Breakpoints Time Travel Model Scripting Command Source

Break Go Step Out Step Into Step Over Step Out Back Step Into Back Step Over Back Restart Stop Debugging Detach Settings Source Assembly Local Help Feedback Hub

Flow Control Reverse Flow Control End Preferences Help

Command

Symbol search path is: srv*;symsrv*symsrv.dll*C:\Symbols*https://msdl.microsoft.com/download/symbols
Executable search path is:
Windows 10 Kernel Version 17763 MP (2 procs) Free x64
Product: WinNt, suite: TerminalServer SingleUserTS
Edition build lab: 17763.1.amd64fre.rs5_release.180914-1434
Machine Name:
Kernel base = 0xfffff806`6f6bb000 PsLoadedModuleList = 0xfffff806`6fad16f0
Debug session time: Thu Oct 15 10:44:11.874 2020 (UTC - 7:00)
System Uptime: 0 days 0:05:04.309
lkd> lm
start end module_name
fffff806`6f6bb000 fffff806`70126000 nt (pdb symbols) C:\ProgramData\Dbg\sym\ntkrnlmp.pdb\315E3D6331E27098858CC61CE3B0AB9E1\ntkrnlmp.pdb

Unloaded modules:
fffff806`73210000 fffff806`73220000 dump_storport.sys
fffff806`73240000 fffff806`73260000 dump_LSI_SAS.sys
fffff806`73280000 fffff806`7329e000 dump_dumpfve.sys
fffff806`73d30000 fffff806`73d4c000 dam.sys
fffff806`73110000 fffff806`73121000 hwpolicy.sys

lkd>

Locals

Name	Value	Type
------	-------	------

Stack

Frame Index	Name
-------------	------

Locals Watch Threads Stack Breakpoints

N.



>> Click

>> Now

KD "", Local Connection - WinDbg 1.0.2007.06001 (Administrator)

File Home View Breakpoints Time Travel Model Scripting Command Memory Source

Command Watch Locals Registers Memory Stack Disassembly Threads Breakpoints Logs Notes Timelines Modules Layouts Reset Windows Window Layout Workspace

Command

```
fffff806`73110000 fffff806`73121000 hwpolicy.sys
lkd> lmDvmnt
Browse full module list
start          end          module name
fffff806`6f6bb000 fffff806`70126000 nt          (pdb symbols)
Loaded symbol image file: ntkrnlmp.exe
Image path: ntkrnlmp.exe
Image name: ntkrnlmp.exe
Browse all global symbols functions data
Image was built with /Brepro flag.
Timestamp:      63584BD8 (This is a reproducible build file hash, not a timestamp)
Checksum:       009462B9
ImageSize:      00A6B000
Translations:   0000.04b0 0000.04e4 0409.04b0 0409.04e4
Information from resource tables:
```

lkd>

Locals

Name	Value
------	-------

Threads

```
[0xcc0] = nt!KiSwapContext+0x76 (fffff806`6f878f76)
[0x1994] = nt!KiSwapContext+0x76 (fffff806`6f878f76)
[0x1280] = <Unable to get stack trace>
[0xfb4] = nt!KiSwapContext+0x76 (fffff806`6f878f76)
[0xc04] = nt!KiSwapContext+0x76 (fffff806`6f878f76)
[0x14e4] = nt!KiSwapContext+0x76 (fffff806`6f878f76)
[0x132c] = nt!KiSwapContext+0x76 (fffff806`6f878f76)
```

Locals Watch Threads Stack Breakpoints



Click
below



There
some
func



You
Alpc



prod
"A",

x /D

KD ", Local Connection - WinDbg 1.0.2007.06001 (Administrator)

File Home View Breakpoints Time Travel Model Scripting Command Memory Source

Command Watch Locals Registers Memory Stack Disassembly Threads Breakpoints Logs Notes Timelines Modules Layouts Reset Windows Window Layout Workspace

Command

```
ImageSize: 00A6B000
Translations: 0000.04b0 0000.04e4 0409.04b0 0409.04e4
Information from resource tables:
lkd> x /D /f nt!a*
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

fffff806`6fc4b760 nt!AlpcpDeleteBlob (void)
fffff806`70007440 nt!AnFwpDisableProgressTimer (void)
fffff806`6fc4784c nt!AlpcpReleaseMessageAttributesOnCancel (void)
fffff806`6fc46030 nt!AlpcpValidateConnectionMessage (void)
fffff806`6fe1db52 nt!AlpcpCaptureHandleAttribute$filt$0 (void)
fffff806`6fc4a25c nt!AlpcpCreateSecurityContext (void)
fffff806`6fc4b1f8 nt!AlpcpDispatchReplyToPort (void)
fffff806`6fc48fa0 nt!AlpcViewDestroyProcedure (void)
fffff806`6fdf2f94 nt!AdtpBuildMessageString (void)
```

lkd>

Locals

Name	Value
------	-------

Threads

```
[0xcc0] = nt!KiSwapContext+0x76 (fffff806`6f878f76)
[0x1994] = nt!KiSwapContext+0x76 (fffff806`6f878f76)
[0x1280] = <Unable to get stack trace>
[0xfb4] = nt!KiSwapContext+0x76 (fffff806`6f878f76)
```

Locals Watch Threads Stack Breakpoints

There are tooltips here. The following commands can be run from an administrative command prompt (right click on Command Prompt and select the Run as Administrator option).

vn

ted to
th



Using Help

The screenshot shows the Windows Debugger application window. The title bar reads "Debugger". The menu bar includes "File", "Edit", "View", "Go", and "Help". The toolbar contains icons for "Hide", "Locate", "Previous", "Next", "Back", "Forward", "Stop", "Refresh", "Home", "Font", "Print", and "Options". The "Search" tab is active in the left sidebar, with sub-tabs for "Contents", "Index", "Search", and "Favorites". Below the tabs is a search input field with the text "Type in the keyword to find:" and the letter "x" entered. A list of search results is displayed below the input field, with "x (Examine Symbols) [Windows Debugg" selected. The main pane displays the help content for the "x" command, including a description, syntax, parameters, and options.

Debugger

File Edit View Go Help

Hide Locate Previous Next Back Forward Stop Refresh Home Font Print Options

Contents Index Search Favorites

Type in the keyword to find:

x

x (Examine Symbols) [Windows Debugg

x64 processor

annotated disassembly

architecture

instructions

overview

registers

x86 processor

annotated disassembly

architecture

arithmetic

assembly code

calling conventions

data types

instructions

overview

Display

x (Examine Symbols)

The **x** command displays the symbols in all contexts that match the specified pattern.

x [*Options*] *Module!Symbol*

x [*Options*] *

Parameters

Options

Specifies symbol searching options. You can use one or more of the following options:

/0

Displays only the address of each symbol.

/1

Displays only the name of each symbol.



>> In the

uf nt

>> The
hex

WinDbg 1.0.2007.06001 (Administrator)

File Home View Breakpoints Time Travel Model Scripting Command Source

Break Go Step Out Step Into Step Over Step Out Back Step Into Back Step Over Back Restart Stop Debugging Detach Settings Source Assembly Local Help Feedback Hub

Command

```
||2:1kd> uf nt!NtCreateFile
nt!NtCreateFile:
fffff806`6fd3ffc0 4881ec88000000 sub     rsp,88h
fffff806`6fd3ffc7 33c0     xor     eax,eax
fffff806`6fd3ffc9 4889442478 mov     qword ptr [rsp+78h],rax
fffff806`6fd3ffce c744247020000000 mov     dword ptr [rsp+70h],20h
fffff806`6fd3ffd6 89442468  mov     dword ptr [rsp+68h],eax
fffff806`6fd3ffda 4889442460 mov     qword ptr [rsp+60h],rax
fffff806`6fd3ffdf 89442458  mov     dword ptr [rsp+58h],eax
fffff806`6fd3ffe3 8b8424e0000000 mov     eax,dword ptr [rsp+0E0h]
fffff806`6fd3ffea 89442450  mov     dword ptr [rsp+50h],eax
fffff806`6fd3ffee 488b8424d8000000 mov     rax,qword ptr [rsp+0D8h]
fffff806`6fd3fff6 4889442448 mov     qword ptr [rsp+48h],rax
fffff806`6fd3fffb 8b8424d0000000 mov     eax,dword ptr [rsp+0D0h]
fffff806`6fd40002 89442440  mov     dword ptr [rsp+40h],eax
fffff806`6fd40006 8b8424c8000000 mov     eax,dword ptr [rsp+0C8h]
fffff806`6fd4000d 89442438  mov     dword ptr [rsp+38h],eax
fffff806`6fd40011 8b8424c0000000 mov     eax,dword ptr [rsp+0C0h]
fffff806`6fd40018 89442430  mov     dword ptr [rsp+30h],eax
fffff806`6fd4001c 8b8424b8000000 mov     eax,dword ptr [rsp+0B8h]
fffff806`6fd40023 89442428  mov     dword ptr [rsp+28h],eax
fffff806`6fd40027 488b8424b0000000 mov     rax,qword ptr [rsp+0B0h]
fffff806`6fd4002f 4889442420  mov     qword ptr [rsp+20h],rax
fffff806`6fd40034 e817000000  call   nt!IopCreateFile (fffff806`6fd40050)
fffff806`6fd40039 4881c488000000 add     rsp,88h
fffff806`6fd40040 c3       ret
```

||2:1kd>

Locals Watch Threads Stack Breakpoints

raw



>> In the

s nt!

>> The

WinDbg 1.0.2007.06001 (Administrator)

File Home View Breakpoints Time Travel Model Scripting Command Source

Break Go Step Out Step Into Step Over Step Out Back Step Into Back Step Over Back Reverse Flow Control End Settings Source Assembly Local Help Feedback Hub

Command

```
nt!NtCreateFile:
fffff806`6fd3ffc0 4881ec88000000 sub     rsp,88h
fffff806`6fd3ffc7 33c0     xor     eax,eax
fffff806`6fd3ffc9 4889442478 mov     qword ptr [rsp+78h],rax
fffff806`6fd3ffce c744247020000000 mov     dword ptr [rsp+70h],20h
fffff806`6fd3ffd6 89442468  mov     dword ptr [rsp+68h],eax
fffff806`6fd3ffda 4889442460  mov     qword ptr [rsp+60h],rax
fffff806`6fd3ffdf 89442458  mov     dword ptr [rsp+58h],eax
fffff806`6fd3ffe3 8b8424e0000000 mov     eax,dword ptr [rsp+0E0h]
fffff806`6fd3ffea 89442450  mov     dword ptr [rsp+50h],eax
fffff806`6fd3ffee 488b8424d8000000 mov     rax,qword ptr [rsp+0D8h]
fffff806`6fd3fff6 4889442448  mov     qword ptr [rsp+48h],rax
fffff806`6fd3fffb 8b8424d0000000 mov     eax,dword ptr [rsp+0D0h]
fffff806`6fd40002 89442440  mov     dword ptr [rsp+40h],eax
fffff806`6fd40006 8b8424c8000000 mov     eax,dword ptr [rsp+0C8h]
fffff806`6fd4000d 89442438  mov     dword ptr [rsp+38h],eax
fffff806`6fd40011 8b8424c0000000 mov     eax,dword ptr [rsp+0C0h]
fffff806`6fd40018 89442430  mov     dword ptr [rsp+30h],eax
fffff806`6fd4001c 8b8424b8000000 mov     eax,dword ptr [rsp+0B8h]
fffff806`6fd40023 89442428  mov     dword ptr [rsp+28h],eax
fffff806`6fd40027 488b8424b0000000 mov     rax,qword ptr [rsp+0B0h]
fffff806`6fd4002f 4889442420  mov     qword ptr [rsp+20h],rax
fffff806`6fd40034 e817000000  call   nt!IopCreateFile (fffff806`6fd40050)
fffff806`6fd40039 4881c488000000 add     rsp,88h
fffff806`6fd40040 c3       ret

||2:1kd> s nt!NtCreateFile L100 0x44 0x24 0x40
fffff806`6fd40003 44 24 40 8b 84 24 c8 00-00 00 89 44 24 38 8b 84 D$@..$. ....D$8..
```

Locals Watch Threads Stack Breakpoints



- KD ", Local Connection - WinDbg 1.0.2007.06001 (Administrator)

File Home View Breakpoints Time Travel Model Scripting Command Source

Break Go Step Out Step Into Step Over Step Out Back Step Into Back Step Over Back Restart Stop Debugging Detach Settings Source Assembly Local Help Feedback Hub

Flow Control Reverse Flow Control End Preferences Help

Command X

```
||2:1kd> s -sa nt!NtCreateFile L100
fffff806`6fd3ffcb "D$x"
fffff806`6fd3ffcf "D$p "
fffff806`6fd3ffd7 "D$hH"
fffff806`6fd3ffdc "D$` "
fffff806`6fd3ffe0 "D$X"
fffff806`6fd3ffeb "D$PH"
fffff806`6fd3fff8 "D$H"
fffff806`6fd40003 "D$@"
fffff806`6fd4000e "D$8"
fffff806`6fd40019 "D$0"
fffff806`6fd40024 "D$(H"
fffff806`6fd40031 "D$ "
fffff806`6fd40052 "L$ L"
fffff806`6fd40063 "SVWATAUAVAWH"
fffff806`6fd4007c "l$L"
fffff806`6fd40094 "L$DA"
fffff806`6fd400b0 "L$HeL"
fffff806`6fd400b6 "4% "
```

||2:1kd>

Locals Watch Threads Stack Breakpoints



- KD ", Local Connection - WinDbg 1.0.2007.06001 (Administrator)

File Home View Breakpoints Time Travel Model Scripting Command Source

Break Go Step Out Step Into Step Over Step Out Back Step Into Back Step Over Back Restart Stop Debugging Detach Settings Source Assembly Local Help Feedback Hub

Flow Control Reverse Flow Control End Preferences Help

Registers Memory

Command

```
ffffff806`6fd3ffcf "D$p "
ffffff806`6fd3ffd7 "D$hH"
ffffff806`6fd3ffdc "D$` "
ffffff806`6fd3ffe0 "D$X"
ffffff806`6fd3ffeb "D$PH"
ffffff806`6fd3fff8 "D$H"
ffffff806`6fd40003 "D$@"
ffffff806`6fd4000e "D$8"
ffffff806`6fd40019 "D$0"
ffffff806`6fd40024 "D$(H"
ffffff806`6fd40031 "D$ "
ffffff806`6fd40052 "L$ L"
ffffff806`6fd40063 "SVWATAUAVAWH"
ffffff806`6fd4007c "l$L"
ffffff806`6fd40094 "L$DA"
ffffff806`6fd400b0 "L$HeL"
ffffff806`6fd400b6 "4% "
||2:1kd> s -[16]sa nt!NtCreateFile L100
ffffff806`6fd40063 "SVWATAUAVAWH"
```

||2:1kd>|

Locals Threads

Locals Watch Threads Stack Breakpoints



Display Memory

WinDbg 1.0.2007.06001 (Administrator)

File Home View Breakpoints Time Travel Model Scripting Command Source

Break Go Step Out Step Into Step Over Step Out Back Step Into Back Step Over Back Restart Stop Debugging Detach Settings Source Assembly Local Help Feedback Hub

Flow Control Reverse Flow Control End Preferences Help

Command X

Registers Memory

```
||2:1kd> db nt
fffff806`6f6bb000 4d 5a 90 00 03 00 00 00-04 00 00 00 ff ff 00 00 MZ.....
fffff806`6f6bb010 b8 00 00 00 00 00 00 00-40 00 00 00 00 00 00 .....@.....
fffff806`6f6bb020 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
fffff806`6f6bb030 00 00 00 00 00 00 00 00-00 00 00 00 01 00 00 .....
fffff806`6f6bb040 0e 1f ba 0e 00 b4 09 cd-21 b8 01 4c cd 21 54 68 .....!..L.!Th
fffff806`6f6bb050 69 73 20 70 72 6f 67 72-61 6d 20 63 61 6e 6f is program canno
fffff806`6f6bb060 74 20 62 65 20 72 75 6e-20 69 6e 20 44 4f 53 20 t be run in DOS
fffff806`6f6bb070 6d 6f 64 65 2e 0d 0d 0a-24 00 00 00 00 00 00 mode....$......
```

Locals Watch Threads Stack Breakpoints



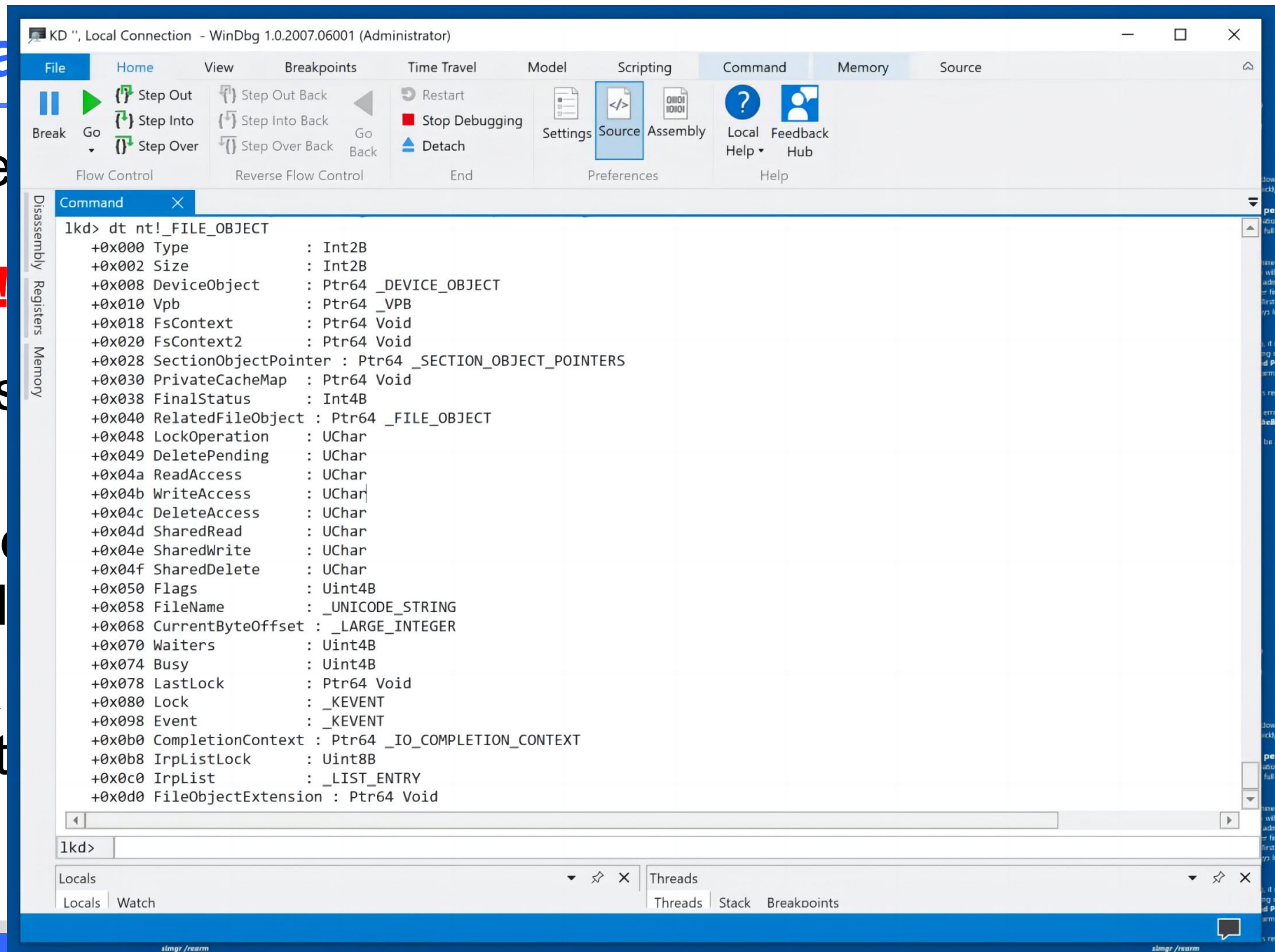
>> In the

dt nt!

>> This s
used

>> Notice
FileN

>> For a
struct



ure

the



>> In

.tl

>> Yo

WinDbg 1.0.2007.06001 (Administrator)

File Home View Breakpoints Time Travel Model Scripting Command Memory Source

Break Go Step Out Step Into Step Over Step Out Back Step Into Back Step Over Back Restart Stop Debugging Detach Settings Source Assembly Local Help Feedback Hub

Flow Control Reverse Flow Control End Preferences Help

Command

```
||2:1kd> .tlist
0n0 System Process
0n4 System
0n88 Registry
0n272 smss.exe
0n368 csrss.exe
0n440 wininit.exe
0n448 csrss.exe
0n536 winlogon.exe
0n580 services.exe
0n592 lsass.exe
0n696 svchost.exe
0n720 fontdrvhost.exe
0n728 fontdrvhost.exe
0n740 svchost.exe
0n836 svchost.exe
0n896 svchost.exe
0n956 dwm.exe
0n300 svchost.exe
0n316 svchost.exe
0n364 svchost.exe
0n852 svchost.exe
0n1080 svchost.exe
0n1120 svchost.exe
0n1144 svchost.exe
```

Locals Watch Threads Stack Breakpoints

also enter "slmgr /ato" from an administrative command prompt. This will give you 90 days.
For Windows Vista, you have 30 days after first boot.

also enter "slmgr /ato" from an administrative command prompt. This will give you 90 days.
For Windows Vista, you have 30 days after first boot.



View



For more
command

!process



You see
"peb"--



Click the
below.

WinDbg 1.0.2007.06001 (Administrator)

File Home View Breakpoints Time Travel Model Scripting Command Memory Source

Break Go Step Out Step Into Step Over Step Out Back Step Into Back Step Over Back Restart Stop Debugging Detach Settings Source Assembly Local Feedback Help Hub

Flow Control Reverse Flow Control End Preferences Help

Command

```
||2:1kd> !process 0 0 lsass.exe
PROCESS ffffffa303d83b1080
  SessionId: 0 Cid: 0250 Peb: 46a5967000 ParentCid: 01b8
  DirBase: 11eff7002 ObjectTable: fffffcb0fb22593c0 HandleCount: 1249.
  Image: lsass.exe

||2:1kd> .process /p ffffffa303d83b1080; !peb 46a5967000
Implicit process is now ffffffa303`d83b1080
PEB at 00000046a5967000
  InheritedAddressSpace: No
  ReadImageFileExecOptions: No
  BeingDebugged: No
  ImageBaseAddress: 00007ff7ae330000
  NtGlobalFlag: 0
  NtGlobalFlag2: 0
  Ldr: 00007ffda9fa53a0
  Ldr.Initialized: Yes
  Ldr.InInitializationOrderModuleList: 000001f64f204060 . 000001f64fbacc80
  Ldr.InLoadOrderModuleList: 000001f64f2041d0 . 000001f64fbacc60
  Ldr.InMemoryOrderModuleList: 000001f64f2041e0 . 000001f64fbacc70

      Base TimeStamp Module
7ff7ae330000 f1beaffa Jul 09 21:45:46 2098 C:\Windows\system32\lsass.exe
7ffda9e40000 1b8b321e Aug 23 04:06:06 1984 C:\Windows\SYSTEM32\ntdll.dll
7ffda9500000 250a0626 Sep 09 23:58:46 1989 C:\Windows\System32\KERNEL32.DLL
7ffda5ef0000 ff301d3c Sep 02 07:01:32 2105 C:\Windows\System32\KERNELBASE.dll
7ffda8ba0000 bdc98177 Nov 24 16:08:23 2070 C:\Windows\System32\RPCRT4.dll
7ffda5a20000 0cdab95d Oct 31 18:48:13 1976 C:\Windows\system32\lsasrv.dll
7ffda9100000 f362c2f9 May 24 12:58:49 2099 C:\Windows\System32\msvcrt.dll
7ffda9310000 19b2d7cc Aug 30 21:10:52 1983 C:\Windows\System32\WS2_32.dll
7ffda5d50000 b5c747e7 Aug 22 13:56:07 2066 C:\Windows\system32\SspiCli.dll
7ffda8eb0000 d29f6d1c Dec 22 13:11:56 2081 C:\Windows\System32\sechost.dll
```

Locals Watch Threads Stack Breakpoints

this

the

own



Viewing Devices and Drivers

WinDbg 1.0.2007.06001 (Administrator)

File Home View Breakpoints Time Travel Model Scripting Command Memory Source

Break Go Step Out Step Into Step Over Step Out Back Step Into Back Step Over Back Restart Stop Debugging Detach Settings Source Assembly Local Help Feedback Hub

Flow Control Reverse Flow Control End Preferences Help

Command X

```
||2:1kd> !devnode 0 1 disk
Dumping IopRootDeviceNode (= 0xfffffa303d46a69e0)
DevNode 0xfffffa303d7075010 for PDO 0xfffffa303d486a060
InstancePath is "SCSI\Disk&Ven_VMware_&Prod_VMware_Virtual_S\5&1ec51bf7&0&000000"
ServiceName is "disk"
State = DeviceNodeStarted (0x308)
Previous State = DeviceNodeEnumerateCompletion (0x30d)
||2:1kd> !devobj fffffa303d486a060
Device object (fffffa303d486a060) is for:
0000006a \Driver\LSI SAS DriverObject fffffa303d485dd90
Current Irp 00000000 RefCount 0 Type 00000007 Flags 00001050
SecurityDescriptor fffffb0fafaed760 DevExt fffffa303d486a1b0 DevObjExt fffffa303d486af70 DevNode fffffa303d7075010
ExtensionFlags (0x00000800) DOE_DEFAULT_SD_PRESENT
Characteristics (0x00040180) FILE_AUTOGENERATED_DEVICE_NAME, FILE_DEVICE_SECURE_OPEN,
FILE_PORTABLE_DEVICE
AttachedDevice (Upper) fffffa303d7018060 \Driver\Disk
Device queue is not busy.
```

Locals Watch Threads Stack Breakpoints

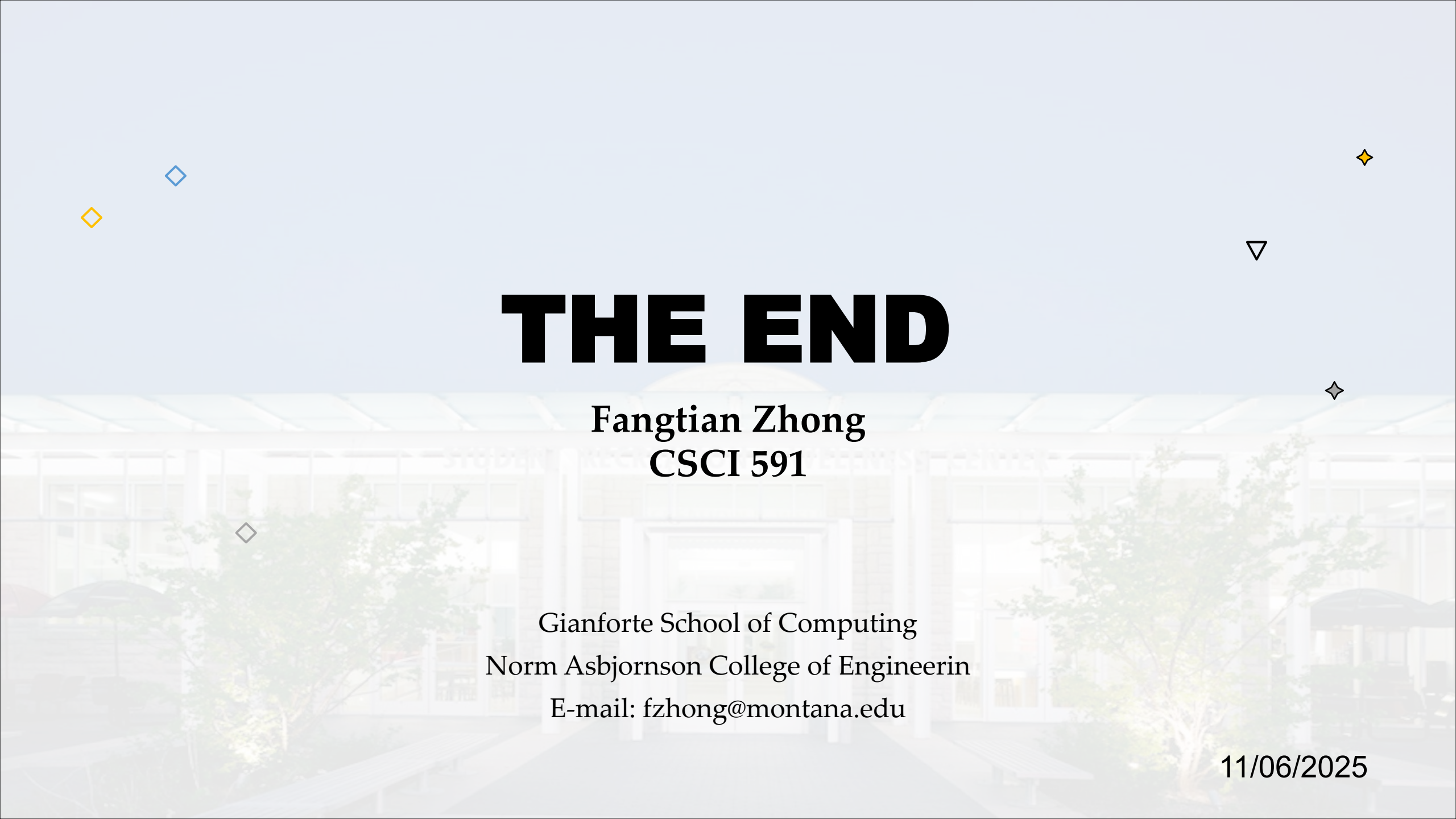


Disabling Debugging

- Click the Start button and type **CMD**. Right-click "**Command Prompt**" and click "**Run as administrator**". Click **Yes**.
- Execute this command:

bcdedit /debug off

- Restart your Windows machine.



THE END

Fangtian Zhong
CSCI 591

Gianforte School of Computing
Norm Asbjornson College of Engineerin
E-mail: fzhong@montana.edu

11/06/2025