

# Malicious Code Analysis

Fangtian Zhong  
CSCI 591

Gianforte School of Computing  
Norm Asbjornson College of Engineering  
E-mail: [fangtian.zhong@montana.edu](mailto:fangtian.zhong@montana.edu)





# Overview

---

**01**

**Debugger Overview**

**02**

**WinDbg Preview**



*Part One*

# 01

2025-10-19

# Debugger Overview

An isometric illustration of a modern office environment. It features several people working at computers, interacting with each other, and using various office equipment like printers and monitors. The scene is rendered in a light blue and white color scheme with soft shadows, giving it a clean, professional look.



# Documentation

---

- 🏆 Read the documentation
  - Installed in the debugger root directory
- 🏆 Reading the docs is key to using the debugger efficiently
  - Ever-increasing number of commands and command parameters
  - Very large number of debugging topics
  - No presentation or class can cover all the debugger features you care about
- 🏆 Use the index for any topic you need more information on
  - Use search if the index does not list the topic
- 🏆 New features are also listed on their website



# Types of Debuggers

---



## Command line debuggers

- kd.exe: kernel debugger
- cdb.exe, ntsd.exe: user mode debugger



## WinDbg

- GUI on top of kd.exe and cdb.exe
- Identical extensions and command interface
- Much more efficient for source debugging
- Can be slower because of extra data displayed



## Dbgrrsv.exe, kdsrv.exe, dbengprx.exe

- Debugger protocol remoting tools
- Discussed later as part of debugger remoting



# What Do the Debuggers Support?

---



## Processor architectures:

- x86, Itanium, x64



## OS versions:

- Windows NT 4 and later
  - No Win9x kernel debugging
- Debugging the newest OS requires using the latest debugger



## Protocols

- COM, 1394, EXDI, USB 2.0 in beta



Can debug a Windows OS running inside the Virtual PC or VMware virtual machines



# Common Issues

---

- 🏆 Local variable issues
  - Turn off compiler optimizations
    - `razzle no_opt`
- 🏆 Breakpoint issues
  - Use the “bu” command to deal with unloading modules
- 🏆 1394 debugging won't connect (firewall)
  - Disable 1394 host controller on the target
- 🏆 COM port debugging won't connect
  - Disable legacy USB support in the BIOS
- 🏆 If all else fails, you may have hit a debugger bug
  - Report it! We don't release until all known bugs are fixed.



*Part Two*

02

# WinDbg Preview

2025-10-19



# Installing

---

## Installing WinDbg Preview

 If you are using the Windows 10 or above, WinDbg Preview is already installed.

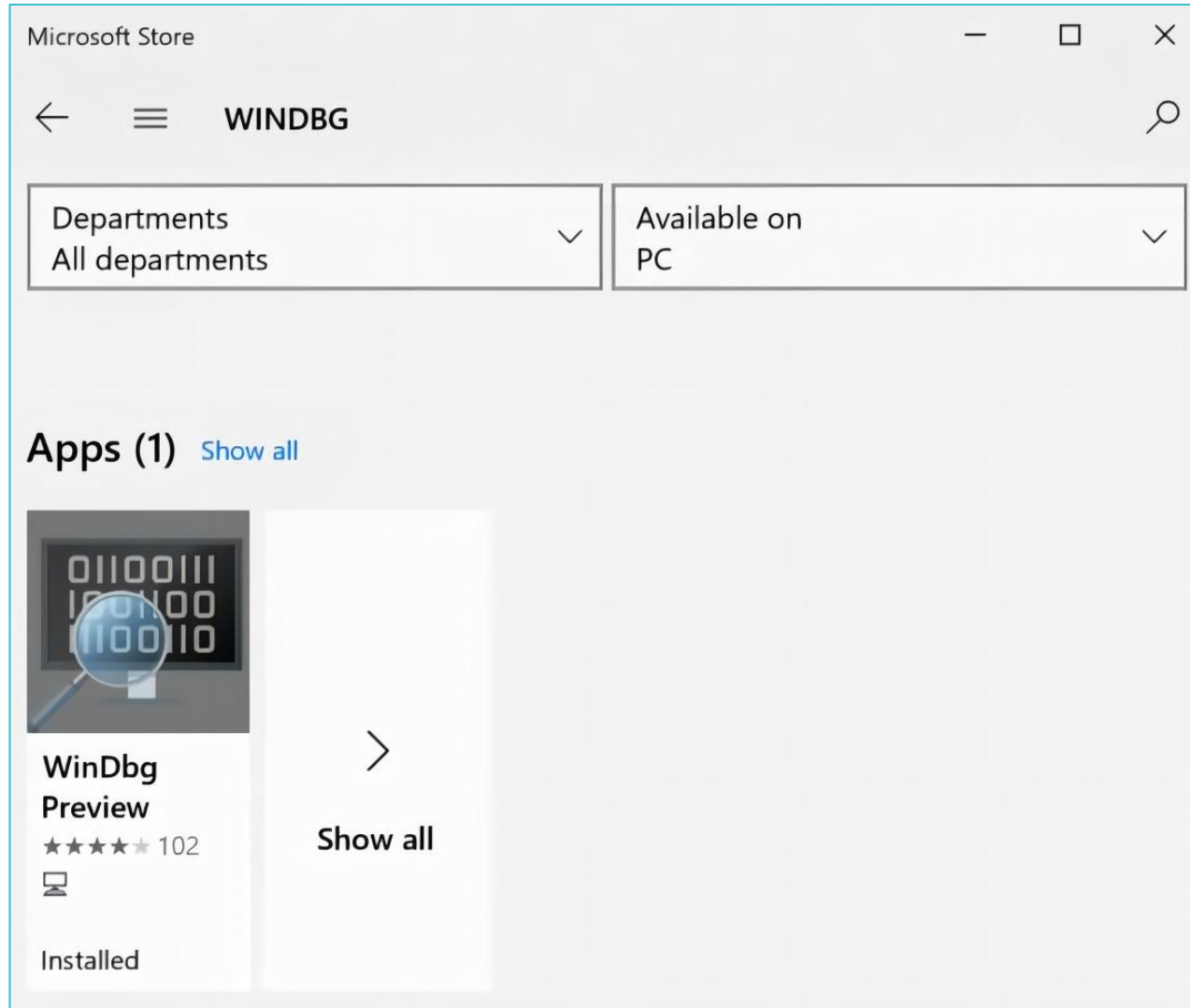
 If you are using some other machine, follow the steps below to install it.

 On Windows 10, at the lower left of the desktop, click the magnifying glass. Type STORE

 Open Microsoft Store.

 In Microsoft Store, search for WinDbg, as shown below.

# Installing



- When it finds "WinDbg Preview", click the **blue Get** button.
- A "Use across your devices" box pops up. Click **"No, thanks"**.
- Click **Launch**.



# Launching

---



Close WinDbg.



Click the **Start** button and type **WINDBG**. Right-click "**WinDbg Preview**" and click "**Run as Administrator**".



Approve the privilege escalation.





# Debugging Notepad

---

🛡️ In WinDbg, click **File**, "**Launch executable**".

🛡️ Navigate to:

C:\Windows\System32\notepad.exe

and open it.





# Loading DLLs

C:\Windows\System32\notepad.exe - WinDbg 1.0.2007.06001

File Home View Breakpoints Time Travel Model Scripting Command Source

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

Restart Stop Debugging Detach

Settings Source Assembly Preferences

Local Help Feedback Hub

Command

Microsoft (R) Windows Debugger Version 10.0.20153.1000 AMD64  
Copyright (c) Microsoft Corporation. All rights reserved.

CommandLine: C:\Windows\System32\notepad.exe

\*\*\*\*\* Path validation summary \*\*\*\*\*

Response	Time (ms)	Location
Deferred		symsrv*symsrv.dll*C:\Symbols*https://msdl.microsoft.com/download/symbols
Symbol search path is: symsrv*symsrv.dll*C:\Symbols*https://msdl.microsoft.com/download/symbols		
Executable search path is:		
ModLoad: 00007ff7`e2030000	00007ff7`e2073000	notepad.exe
ModLoad: 00007ff8`56970000	00007ff8`56b5d000	ntdll.dll
ModLoad: 00007ff8`55140000	00007ff8`551f3000	C:\Windows\System32\KERNEL32.DLL
ModLoad: 00007ff8`52f40000	00007ff8`531d4000	C:\Windows\System32\KERNELBASE.dll
ModLoad: 00007ff8`55390000	00007ff8`55433000	C:\Windows\System32\ADVAPI32.dll
ModLoad: 00007ff8`54a40000	00007ff8`54ade000	C:\Windows\System32\msvcrt.dll
ModLoad: 00007ff8`54d10000	00007ff8`54dae000	C:\Windows\System32\sechost.dll
ModLoad: 00007ff8`55260000	00007ff8`55382000	C:\Windows\System32\RPCRT4.dll
ModLoad: 00007ff8`54a10000	00007ff8`54a39000	C:\Windows\System32\GDI32.dll
ModLoad: 00007ff8`52c00000	00007ff8`52d9c000	C:\Windows\System32\gdi32full.dll

0:000>

# Loading DLLs



La



n



C



C



In



A

fi

Host Name: MSEDGEWIN10

Process Explorer - Sysinternals: www.sysinternals.com [MSEDGEWIN10\IEUser] (Admin)

File Options View Process Find DLL Users Help

Process

- notepad.exe
- procexp64.exe
- OneDrive.exe
- notepad.exe
- LocalBridge.exe

Name	Description
kernel.appcore.dll	AppModel API Host
kernel32.dll	Windows NT BASE API Client DLL
KernelBase.dll	Windows NT BASE API Client DLL
locale.nls	
msvc_p_win.dll	Microsoft® C Runtime Library
msvcrt.dll	Windows NT CRT DLL
notepad.exe	Notepad
ntdll.dll	NT Layer DLL
oleaut32.dll	OLEAUT32.DLL
powerprof.dll	Power Profile Helper DLL
profapi.dll	User Profile Basic API
propsys.dll	Microsoft Property System
rpcrt4.dll	Remote Procedure Call Runtime
schannel.dll	Host for SSL/TLS/HTTP Authentication

CPU Usage: 3.41% Commit Charge: 57.40% Processes: 142

ntdll.dll Properties

Image Strings

Image

Description: NT Layer DLL

Company:

Version: 10.0.17763.1432

Build Time:

Path: C:\Windows\System32\ntdll.dll Explore

Autostart Location: n/a Explore

Load Address: 0x00007FF856970000 Verify

Mapped Size: 0x1ED000 bytes

Mapping Type: Image

VirusTotal: Submit

Image: 64-bit

OK Cancel

PID Des

7200	Not
9652	Sys
4888	Mic
10944	Not
12140	Loc

kernel.appcore.dll

kernel32.dll

KernelBase.dll

locale.nls

msvc\_p\_win.dll

msvcrt.dll

notepad.exe

ntdll.dll

oleaut32.dll

powerprof.dll

profapi.dll

propsys.dll

rpcrt4.dll

schannel.dll

In some cases (Windows XP, Vista,  
following commands can be used to  
the 'Run as Administrator'  
Show current license, time remaining, etc. (all except Windows 7):  
slmgr /dlv

are rearms left. The  
nd Prompt and select





In WinDbg  
bottom.



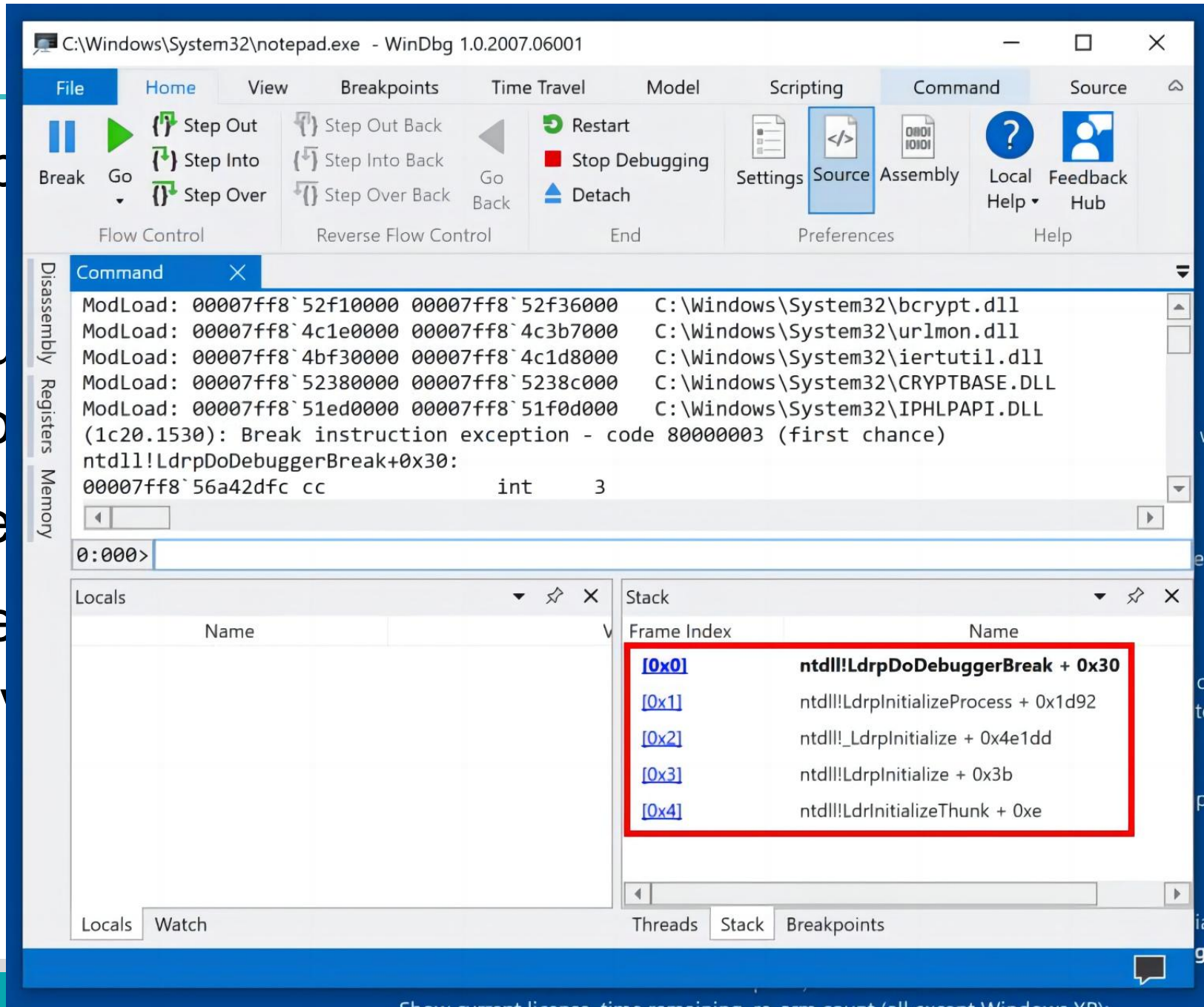
Here you  
instruction



From the



The lower  
we are fi



C:\Windows\System32\notepad.exe - WinDbg 1.0.2007.06001

File Home View Breakpoints Time Travel Model Scripting Command Source

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

Flow Control Reverse Flow Control End Preferences Help

Command

```
ModLoad: 00007ff8`52f10000 00007ff8`52f36000 C:\Windows\System32\bcrypt.dll
ModLoad: 00007ff8`4c1e0000 00007ff8`4c3b7000 C:\Windows\System32\urlmon.dll
ModLoad: 00007ff8`4bf30000 00007ff8`4c1d8000 C:\Windows\System32\iertutil.dll
ModLoad: 00007ff8`52380000 00007ff8`5238c000 C:\Windows\System32\CRYPTBASE.DLL
ModLoad: 00007ff8`51ed0000 00007ff8`51f0d000 C:\Windows\System32\IPHLPAPI.DLL
(1c20.1530): Break instruction exception - code 80000003 (first chance)
ntdll!LdrpDoDebuggerBreak+0x30:
00007ff8`56a42dfc cc int 3
```

0:000>

Locals

Name
------

Stack

Frame Index	Name
[0x0]	ntdll!LdrpDoDebuggerBreak + 0x30
[0x1]	ntdll!LdrpInitializeProcess + 0x1d92
[0x2]	ntdll!_LdrpInitialize + 0x4e1dd
[0x3]	ntdll!LdrpInitialize + 0x3b
[0x4]	ntdll!LdrpInitializeThunk + 0xe

Locals Watch Threads Stack Breakpoints

he

reak

g that

# Viewing



In the lower  
execute this  
**x notepad!**



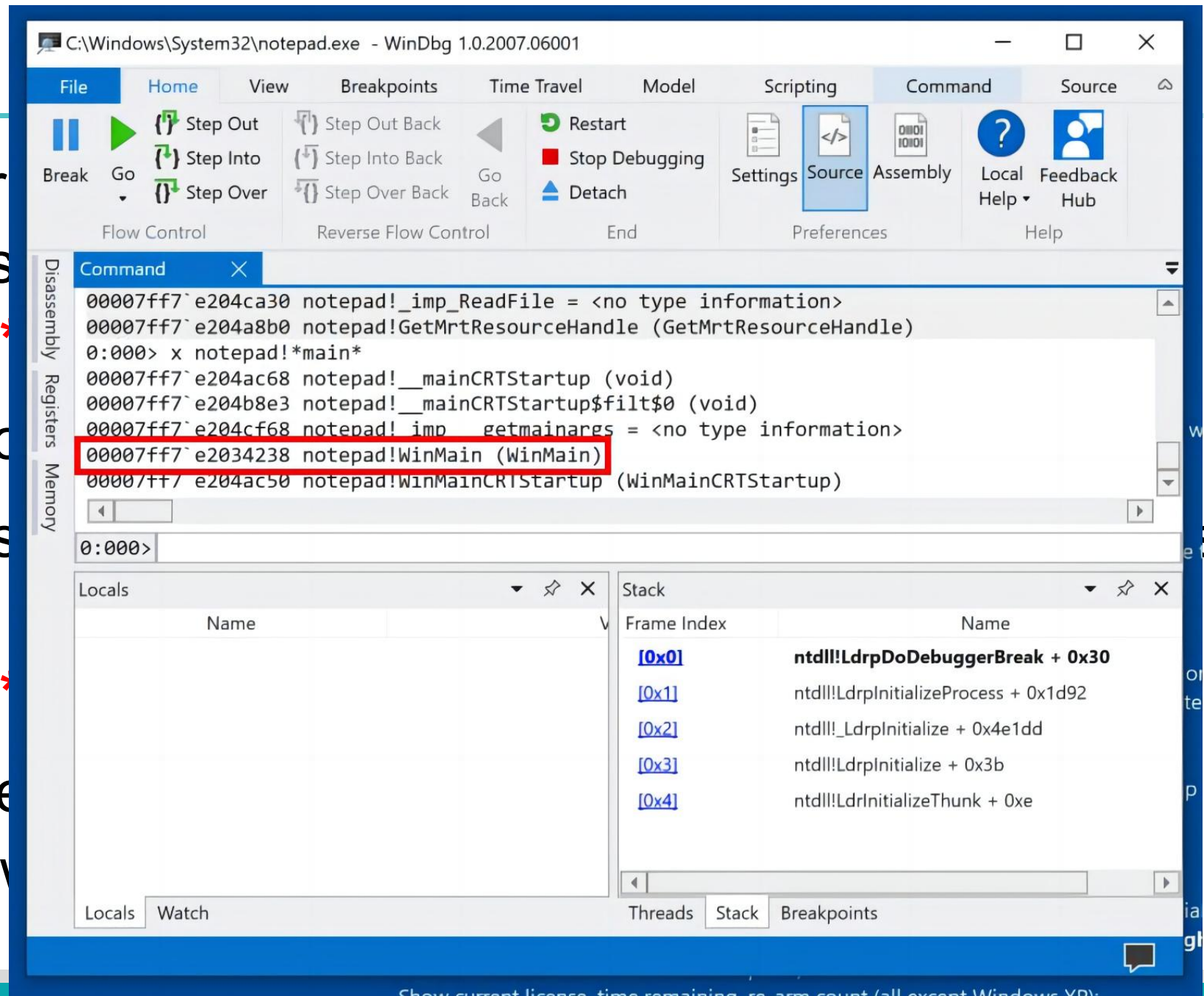
You see a lo



To see the s  
command:  
**x notepad!**



You see a fe  
shown below





# Setting

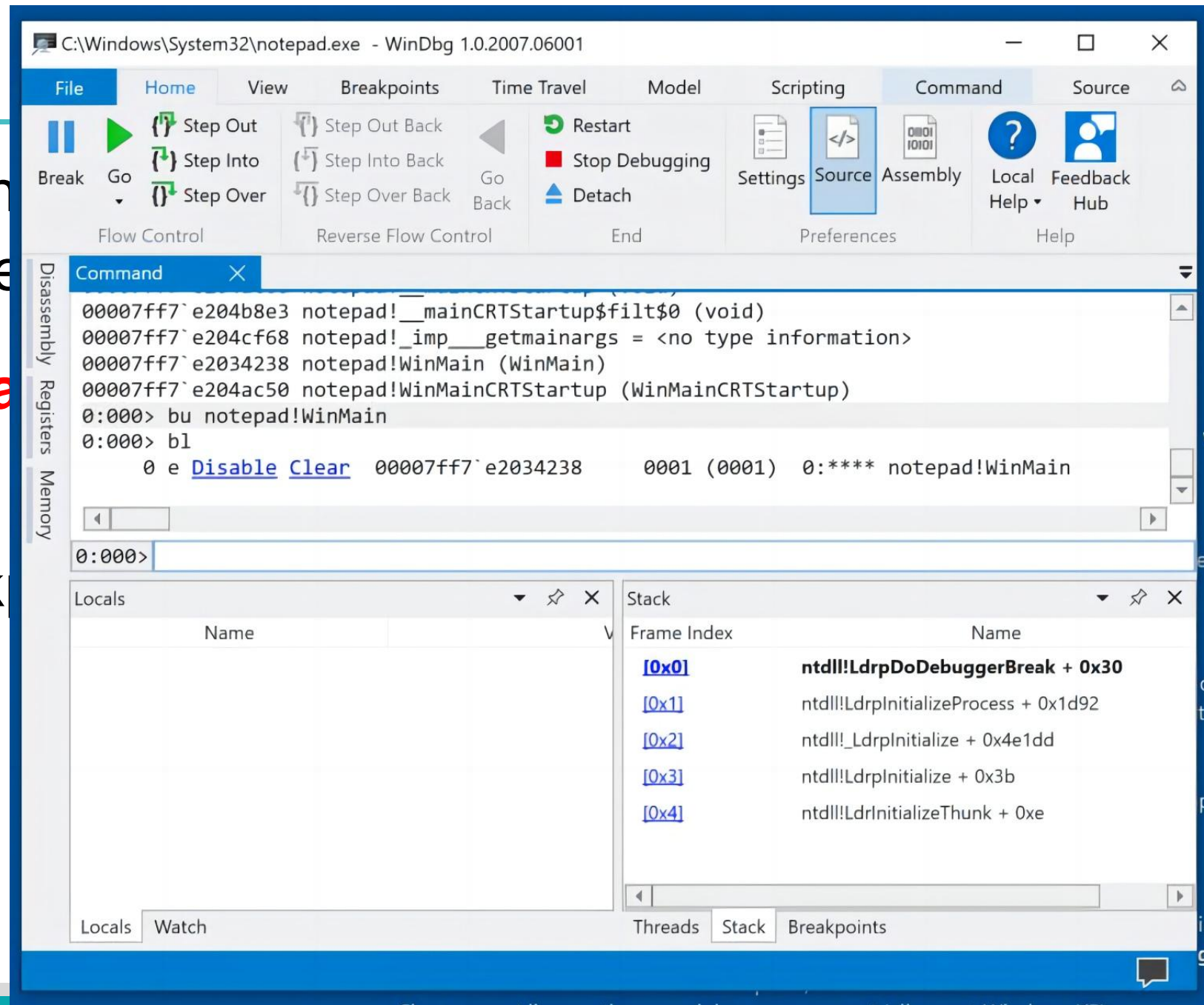


Execute the  
display break

bu notepad  
bl



The break





# Set



## Run

g



## The below

C:\Windows\System32\notepad.exe - WinDbg 1.0.2007.06001

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 Go Back Restart Stop Debugging Detach Settings Source Assembly Local Help Feedback Hub

Flow Control Reverse Flow Control End Preferences Help

Command

```
0:000> bl
0 e Disable Clear 00007ff7`e2034238 0001 (0001) 0:**** notepad!WinMain
0:000> g
ModLoad: 00007ff8`53b90000 00007ff8`53bbe000 C:\Windows\System32\IMM32.DLL
Breakpoint 0 hit
notepad!WinMain:
00007ff7`e2034238 48895c2410 mov qword ptr [rsp+10h],rbx ss:00000016`bb67f898=0000000000000000
```

Locals

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

Stack

Frame Index	Name
[0x0]	notepad!WinMain
[0x1]	notepad!_mainCRTStartup + 0x19f
[0x2]	KERNEL32!BaseThreadInitThunk + 0x14
[0x3]	ntdll!RtlUserThreadStart + 0x21

Locals Watch Threads Stack Breakpoints



C:\Windows\System32\notepad.exe - WinDbg 1.0.2007.06001

File Home View Breakpoints Time Travel Model Scripting Command Source

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

Settings Source Assembly Local Help Feedback Hub

Command

00007ff8`54960000	00007ff8`54a09000	<a href="#">shcore</a>	(deferred)	
00007ff8`54a10000	00007ff8`54a39000	<a href="#">GDI32</a>	(deferred)	
00007ff8`54a40000	00007ff8`54ade000	<a href="#">msvcrt</a>	(deferred)	
00007ff8`54be0000	00007ff8`54d07000	<a href="#">COMDLG32</a>	(deferred)	
00007ff8`54d10000	00007ff8`54dae000	<a href="#">sechost</a>	(deferred)	
00007ff8`54db0000	00007ff8`550dd000	<a href="#">combase</a>	(deferred)	
00007ff8`55140000	00007ff8`551f3000	<a href="#">KERNEL32</a>	(pdb symbols)	c:\symbols\kernel32.pdb\07EFA0465AFB4214CBD5328B0B5ED0841\kernel32.pdb
00007ff8`55260000	00007ff8`55382000	<a href="#">RPCRT4</a>	(deferred)	
00007ff8`55390000	00007ff8`55433000	<a href="#">ADVAPI32</a>	(deferred)	
00007ff8`55440000	00007ff8`56939000	<a href="#">SHELL32</a>	(deferred)	
00007ff8`56970000	00007ff8`56b5d000	<a href="#">ntdll</a>	(pdb symbols)	c:\symbols\ntdll.pdb\62C02F6EEF0AF78DFB36E22C396B9BBA1\ntdll.pdb

0:000>

Locals

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

Stack

Frame Index	Name
<a href="#">[0x0]</a>	<b>notepad!WinMain</b>
<a href="#">[0x1]</a>	notepad!_mainCRTStartup + 0x19f
<a href="#">[0x2]</a>	KERNEL32!BaseThreadInitThunk + 0x14
<a href="#">[0x3]</a>	ntdll!RtlUserThreadStart + 0x21

Locals Watch Threads Stack Breakpoints





To see a

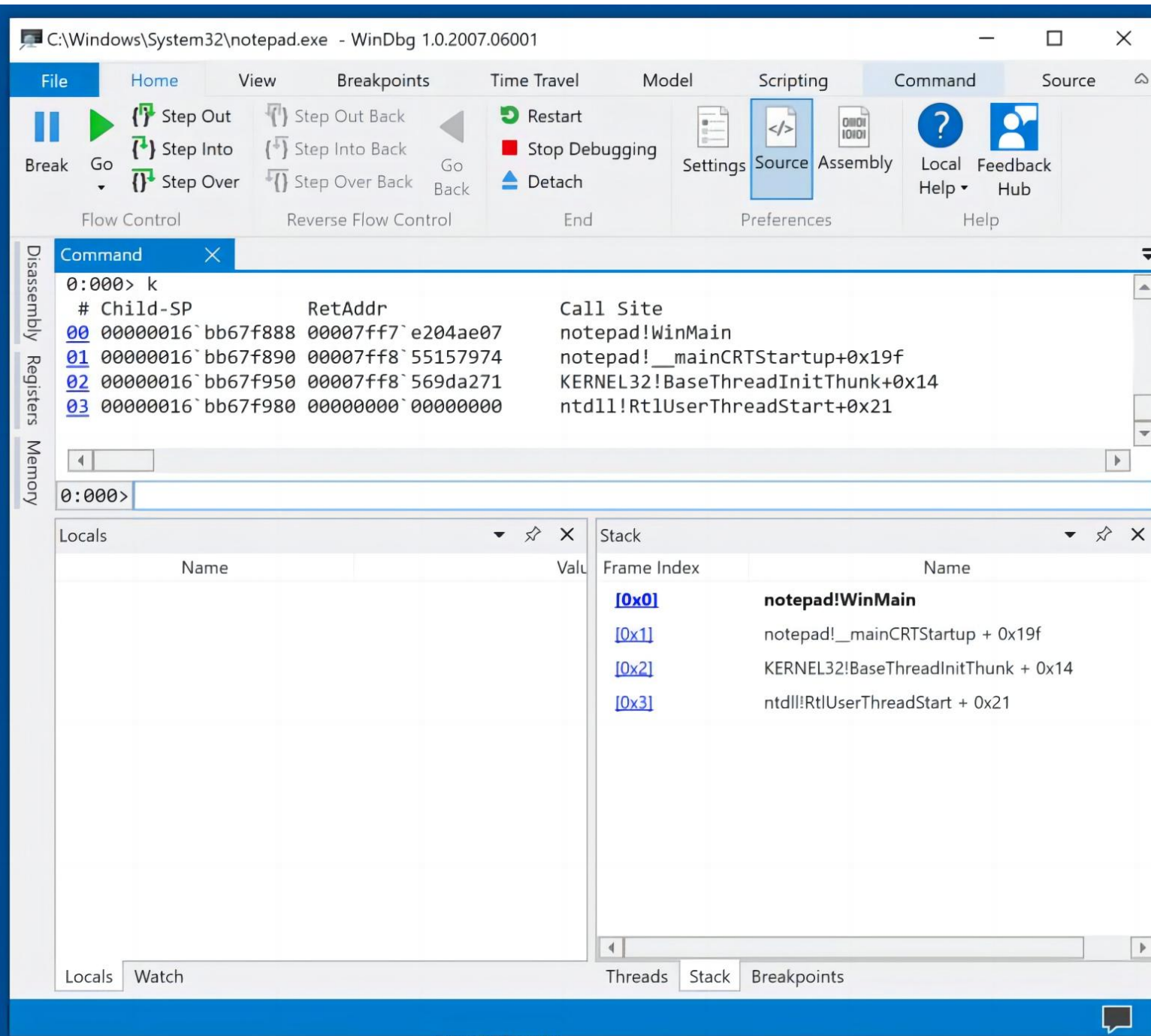
k



You see  
as shown



This is the  
pane, with



At this point,

over right



# Find



Let's find  
module

x ntdll



You see  
below.

C:\Windows\System32\notepad.exe - WinDbg 1.0.2007.06001

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: 00007ff8`48b60000 00007ff8`48be9000 C:\Windows\System32\WINSPOOL.DRV
ModLoad: 00007ff8`52f10000 00007ff8`52f36000 C:\Windows\System32\bcrypt.dll
ModLoad: 00007ff8`4c1e0000 00007ff8`4c3b7000 C:\Windows\System32\urlmon.dll
ModLoad: 00007ff8`51ed0000 00007ff8`51f0d000 C:\Windows\System32\IPHLPAPI.DLL
ModLoad: 00007ff8`4bf30000 00007ff8`4c1d8000 C:\Windows\System32\iertutil.dll
ModLoad: 00007ff8`52380000 00007ff8`5238c000 C:\Windows\System32\CRYPTBASE.DLL
(1514.398): Break instruction exception - code 80000003 (first chance)
ntdll!LdrpDoDebuggerBreak+0x30:
00007ff8`56a42dfc cc int 3
0:000> x ntdll!*CreateFile*
00007ff8`569dccbc ntdll!EtwpCreateFile (void)
00007ff8`56a101f0 ntdll!NtCreateFile (NtCreateFile)
00007ff8`56a101f0 ntdll!ZwCreateFile (ZwCreateFile)
00007ff8`56a90958 ntdll!_imp_NtCreateFile = <no type information>
```

0:000>

Locals

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

Stack

Frame Index	Name
[0x0]	ntdll!LdrpDoDebuggerBreak + 0x30
[0x1]	ntdll!LdrpInitializeProcess + 0x1d92
[0x2]	ntdll!LdrpInitialize + 0x4e1dd
[0x3]	ntdll!LdrpInitialize + 0x3b
[0x4]	ntdll!LdrpInitializeThunk + 0xe

Locals Watch Threads Stack Breakpoints

||

s shown



Untitled - Notepad

File Edit Format View Help

C:\Windows\System32\notepad.exe - C:\Windows\System32\notepad.exe - WinDbg 1.0.2007.06001 (Administrator)

FileHomeViewBreakpointsTime TravelModelScriptingCommandSource

BreakGo

Step OutStep IntoStep Over

Step Out BackStep Into BackStep Over Back

RestartStop DebuggingDetach

SettingsSourceAssembly

Local HelpFeedback Hub

Flow ControlReverse Flow ControlEndPreferencesHelp

DisassemblyRegistersMemory

Command

0 e [Disable](#) [Clear](#) 00007ff7`e2034238 0001 (0001) 2:\*\*\*\* notepad!WinMain

1 e [Disable](#) [Clear](#) 00007ff8`56a101f0 0001 (0001) 2:\*\*\*\* ntdll!NtCreateFile

2:008> g

ModLoad: 00007ff8`53b90000 00007ff8`53bbe000 C:\Windows\System32\IMM32.DLL

Breakpoint 1 hit

ntdll!NtCreateFile:

00007ff8`56a101f0 4c8bd1 mov r10,rcx

2:008>

Locals

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

Locals Watch

Stack

Frame Index	Name
<a href="#">[0x0]</a>	ntdll!NtCreateFile
<a href="#">[0x1]</a>	ntdll!LdrpMapResourceFile + 0x12b
<a href="#">[0x2]</a>	ntdll!LdrMapAndVerifyResourceFile + 0x9a
<a href="#">[0x3]</a>	ntdll!LdrLoadAlternateResourceModuleEx + 0x47c
<a href="#">[0x4]</a>	ntdll!LdrpLoadResourceFromAlternativeModule + 0x...
<a href="#">[0x5]</a>	ntdll!LdrpSearchResourceSection_U + 0x589

ThreadsStackBreakpoints

Re-arm (all except windows XP). Requires reboot.

slmar /rearm





Untitled - Notepad

File Edit Format View Help

C:\Windows\System32\notepad.exe - C:\Windows\System32\notepad.exe - WinDbg 1.0.2007.06001 (Administrator)

File Home View Breakpoints Time Travel Model Scripting Command Source

Break Go Step Out Step Out Back Restart Settings Source Assembly Local Help Feedback Hub

Flow Control Reverse Flow Control End Preferences Help

Command

2:008> k

#	Child-SP	RetAddr	Call Site
00	00000049`d97ad088	00007ff8`569b0d0b	ntdll!NtCreateFile
01	00000049`d97ad090	00007ff8`569ade36	ntdll!LdrpMapResourceFile+0x12b
02	00000049`d97ad1b0	00007ff8`569a2a5c	ntdll!LdrMapAndVerifyResourceFile+0x9a
03	00000049`d97ad230	00007ff8`569a22c9	ntdll!LdrLoadAlternateResourceModuleEx+0x47c
04	00000019`d97ad1d0	00007ff8`569a3329	ntdll!LdrpLoadResourceFromAlternativeModule+0x1f1

Locals

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

Stack

Frame Index	Name
[0x0]	ntdll!NtCreateFile
[0x1]	ntdll!LdrpMapResourceFile + 0x12b
[0x2]	ntdll!LdrMapAndVerifyResourceFile + 0x9a
[0x3]	ntdll!LdrLoadAlternateResourceModuleEx + 0x47c
[0x4]	ntdll!LdrpLoadResourceFromAlternativeModule + 0x...
[0x5]	ntdll!LdrpSearchResourceSection_U + 0x589

Locals Watch Threads Stack Breakpoints

Re-arm (all except Windows XP). Requires reboot.



Untitled - Notepad

File Edit Format View Help

C:\Windows\System32\notepad.exe - C:\Windows\System32\notepad.exe - WinDbg 1.0.2007.06001 (Administrator)

File Home View Breakpoints Time Travel Model Scripting Command Source

Break Go Step Out Step Out Back Restart Settings Source Assembly Local Help Feedback Hub

Flow Control Reverse Flow Control End Preferences Help

Command

```
15 00000049`d97aee0 00007ff8`56a338b9 ntdll!LdrpInitializeProcess+0x1e16
16 00000049`d97af310 00007ff8`569e56c3 ntdll!_LdrpInitialize+0x4e1dd
17 00000049`d97af3b0 00007ff8`569e566e ntdll!LdrpInitialize+0x3b
18 00000049`d97af3e0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
2:008> ~
. 8 Id: 1f6c.14b4 Suspend: 1 Teb: 00000049`d9858000 Unfrozen
```

Locals

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

Stack

Frame Index	Name
[0x0]	ntdll!NtCreateFile
[0x1]	ntdll!LdrpMapResourceFile + 0x12b
[0x2]	ntdll!LdrMapAndVerifyResourceFile + 0x9a
[0x3]	ntdll!LdrLoadAlternateResourceModuleEx + 0x47c
[0x4]	ntdll!LdrpLoadResourceFromAlternativeModule + 0x...
[0x5]	ntdll!LdrpSearchResourceSection_U + 0x589

Locals Watch Threads Stack Breakpoints





Untitled - Notepad

File Edit Format View Help

C:\Windows\System32\notepad.exe - C:\Windows\System32\notepad.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 Go Back Restart Stop Debugging Detach Settings Source Assembly Local Help Feedback Hub

Flow Control Reverse Flow Control End Preferences Help

Command

```
18 00000049`d97af3e0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
2:008> ~
. 8 Id: 1f6c.14b4 Suspend: 1 Teb: 00000049`d9858000 Unfrozen
2:008> bl
0 e Disable Clear 00007ff7`e2034238 0001 (0001) 2:**** notepad!WinMain
1 e Disable Clear 00007ff8`56a101f0 0001 (0001) 2:**** ntdll!NtCreateFile
```

Disassembly Registers Memory

Locals

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

Stack

Frame Index	Name
[0x0]	ntdll!NtCreateFile
[0x1]	ntdll!LdrpMapResourceFile + 0x12b
[0x2]	ntdll!LdrMapAndVerifyResourceFile + 0x9a
[0x3]	ntdll!LdrLoadAlternateResourceModuleEx + 0x47c
[0x4]	ntdll!LdrpLoadResourceFromAlternativeModule + 0x...
[0x5]	ntdll!LdrpSearchResourceSection_U + 0x589

Locals Watch Threads Stack Breakpoints

Re-arm (all except Windows XP). Requires reboot.



Untitled - Notepad

File Edit Format View Help

C:\Windows\System32\notepad.exe - C:\Windows\System32\notepad.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 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

```
18 00000049`d97af3e0 00000000`00000000 ntdll!LdrInitializeThunk+0xe
2:008> ~
. 8 Id: 1f6c.14b4 Suspend: 1 Teb: 00000049`d9858000 Unfrozen
2:008> bl
0 e Disable Clear 00007ff7`e2034238 0001 (0001) 2:**** notepad!WinMain
1 e Disable Clear 00007ff8`56a101f0 0001 (0001) 2:**** ntdll!NtCreateFile
```

Locals

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

Stack

Frame Index	Name
[0x0]	ntdll!NtCreateFile
[0x1]	ntdll!LdrpMapResourceFile + 0x12b
[0x2]	ntdll!LdrMapAndVerifyResourceFile + 0x9a
[0x3]	ntdll!LdrLoadAlternateResourceModuleEx + 0x47c
[0x4]	ntdll!LdrpLoadResourceFromAlternativeModule + 0x...
[0x5]	ntdll!LdrpSearchResourceSection_U + 0x589

Locals Watch Threads Stack Breakpoints

Re-arm (all except Windows XP). Requires reboot.

# THE END

Fangtian Zhong

CSCI 591

Gianforte School of Computing  
Norm Asbjornson College of Engineering  
E-mail: [fangtian.zhong@montana.edu](mailto:fangtian.zhong@montana.edu)

11/04/2025