MONTANA STATE UNIVERSITY

11/06/2025

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

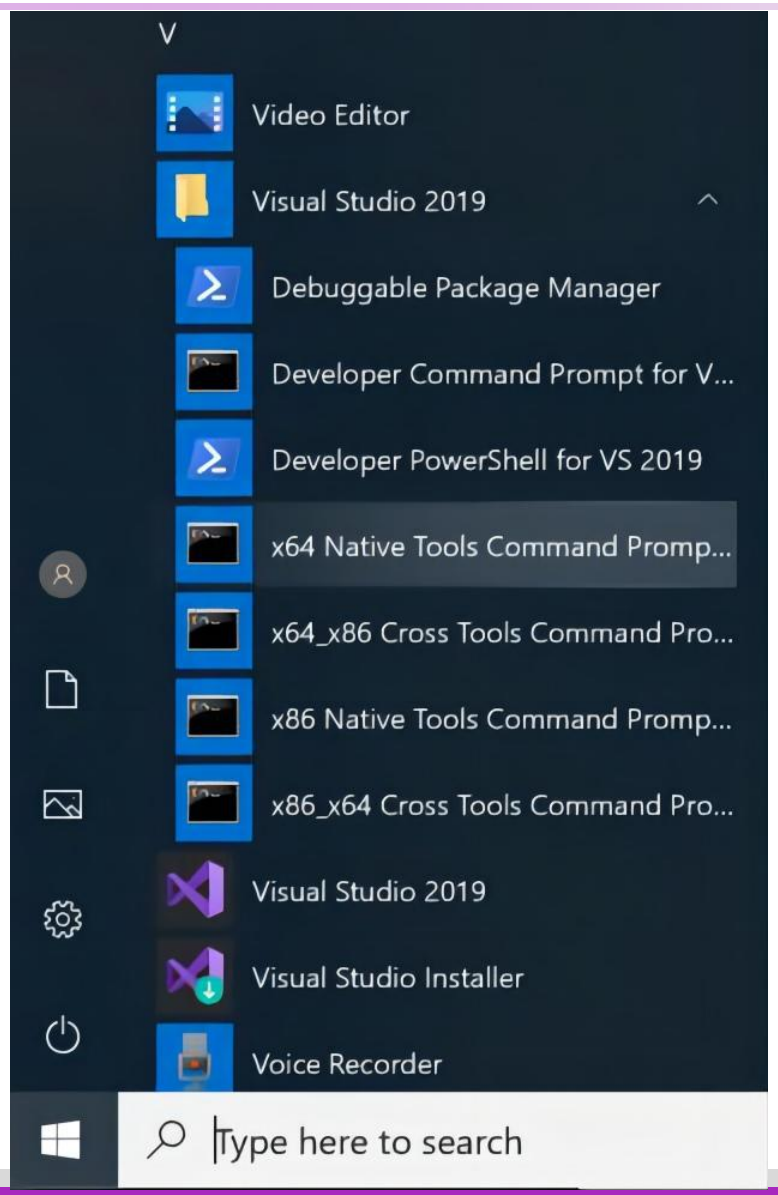
Source-Level Debugging

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:

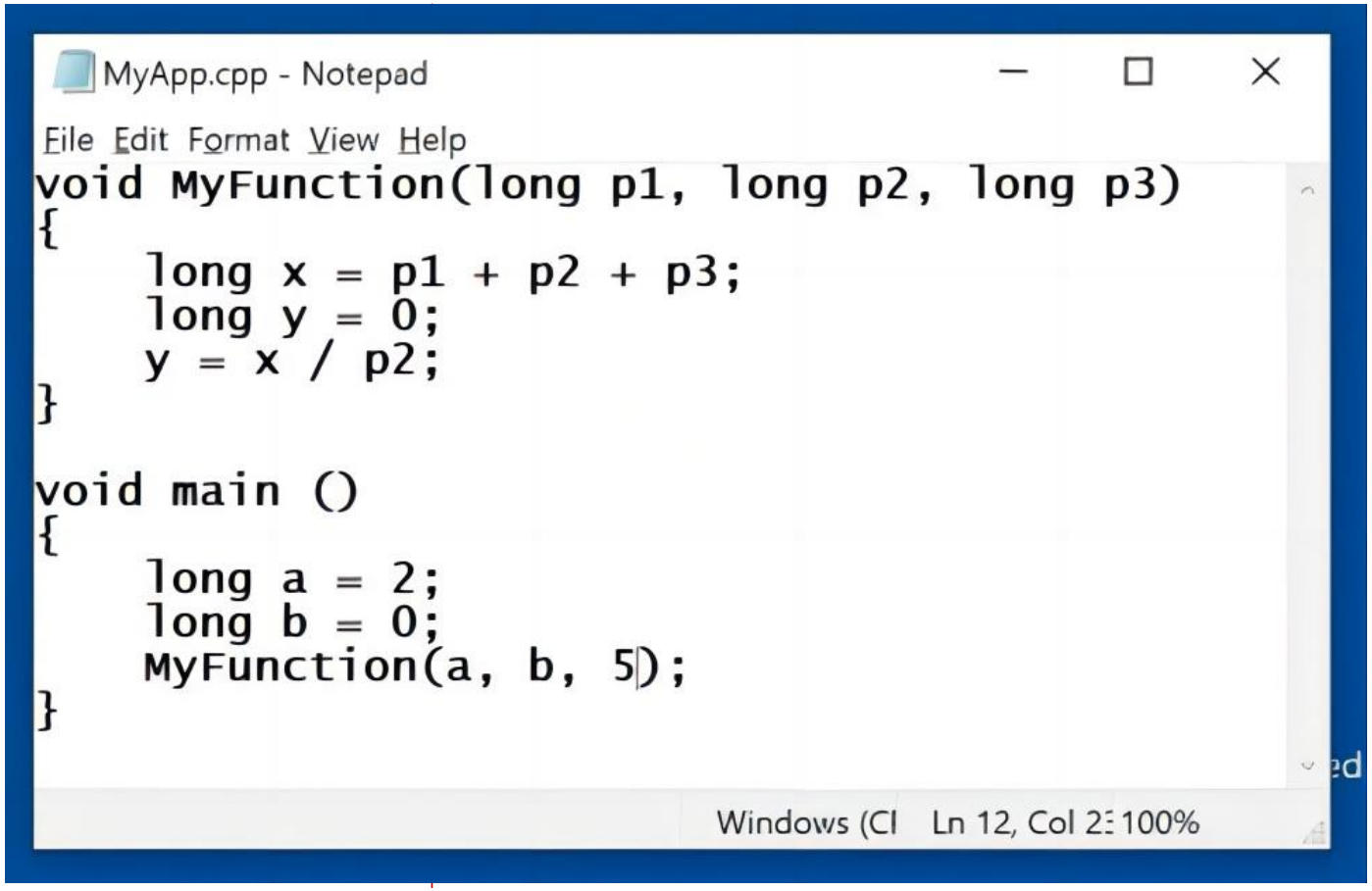
mkdir c:\MyApp
cd c:\MyApp
notepad MyApp.cpp

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.



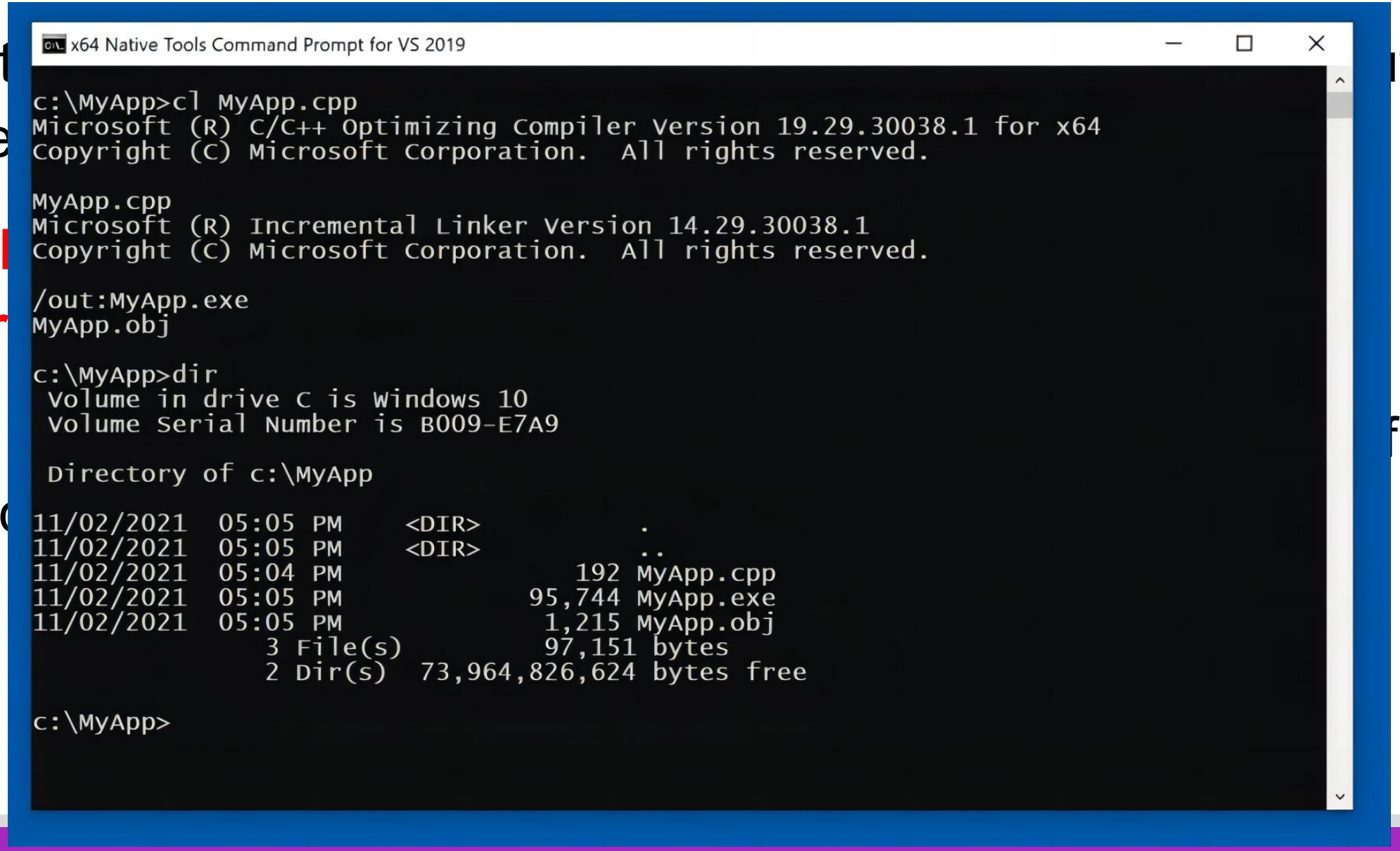
Compiling a C++ Program Without Symbols

- In t… …ite the…

  cl …

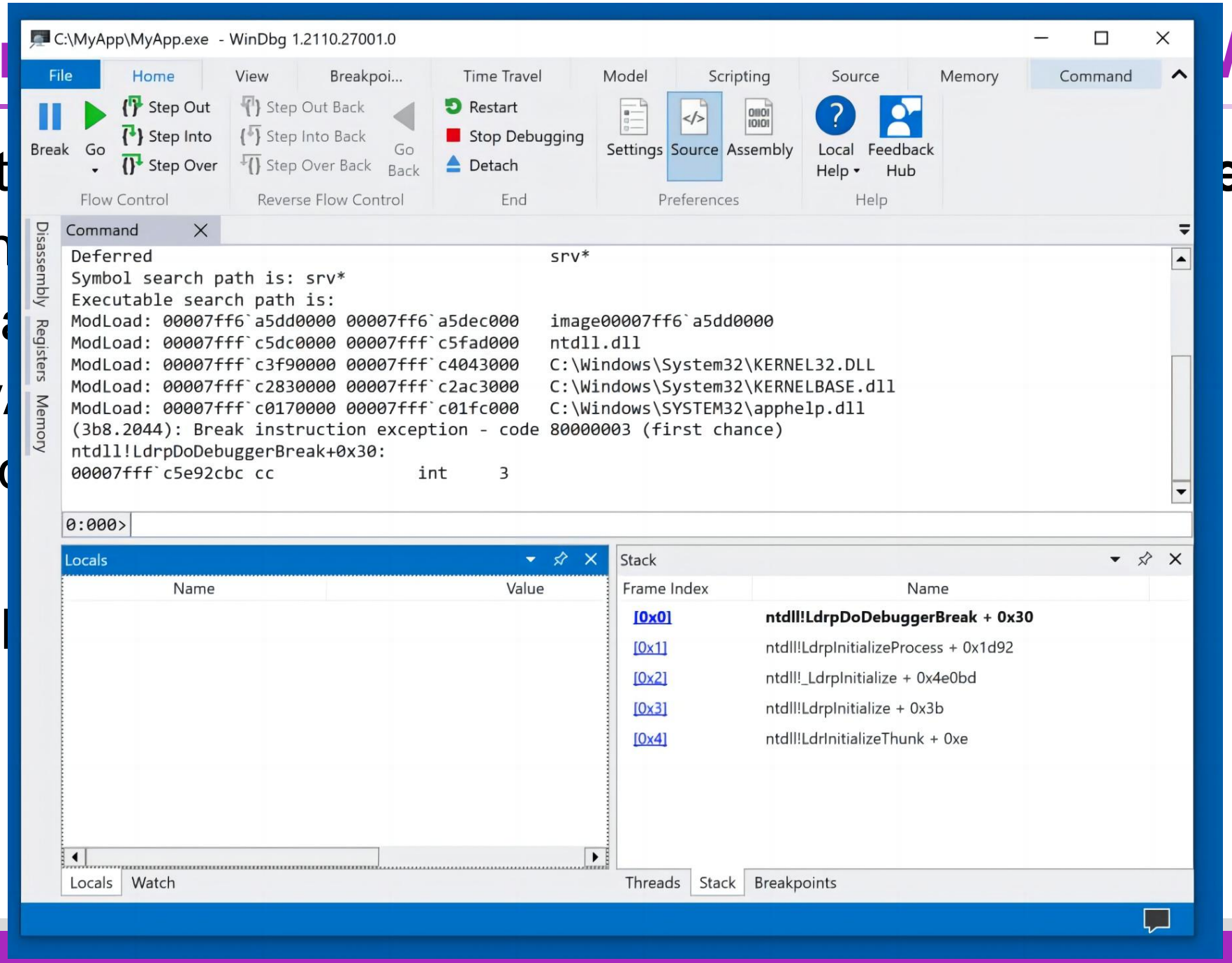
  dir

- As … …file and…



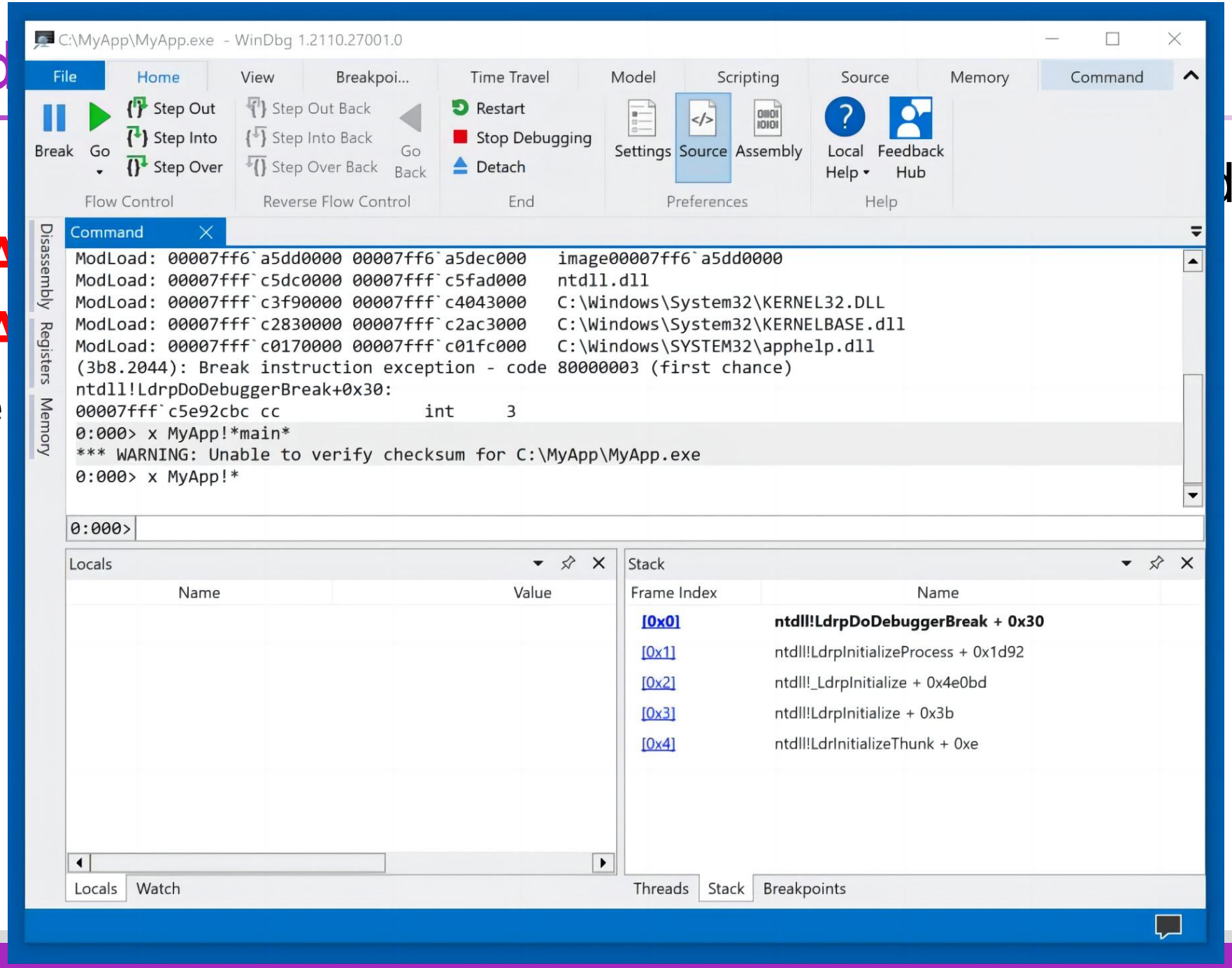
Laun MyApp

- Click t eview".
- In Win
- Naviga
  C:\My
  and d
- The a



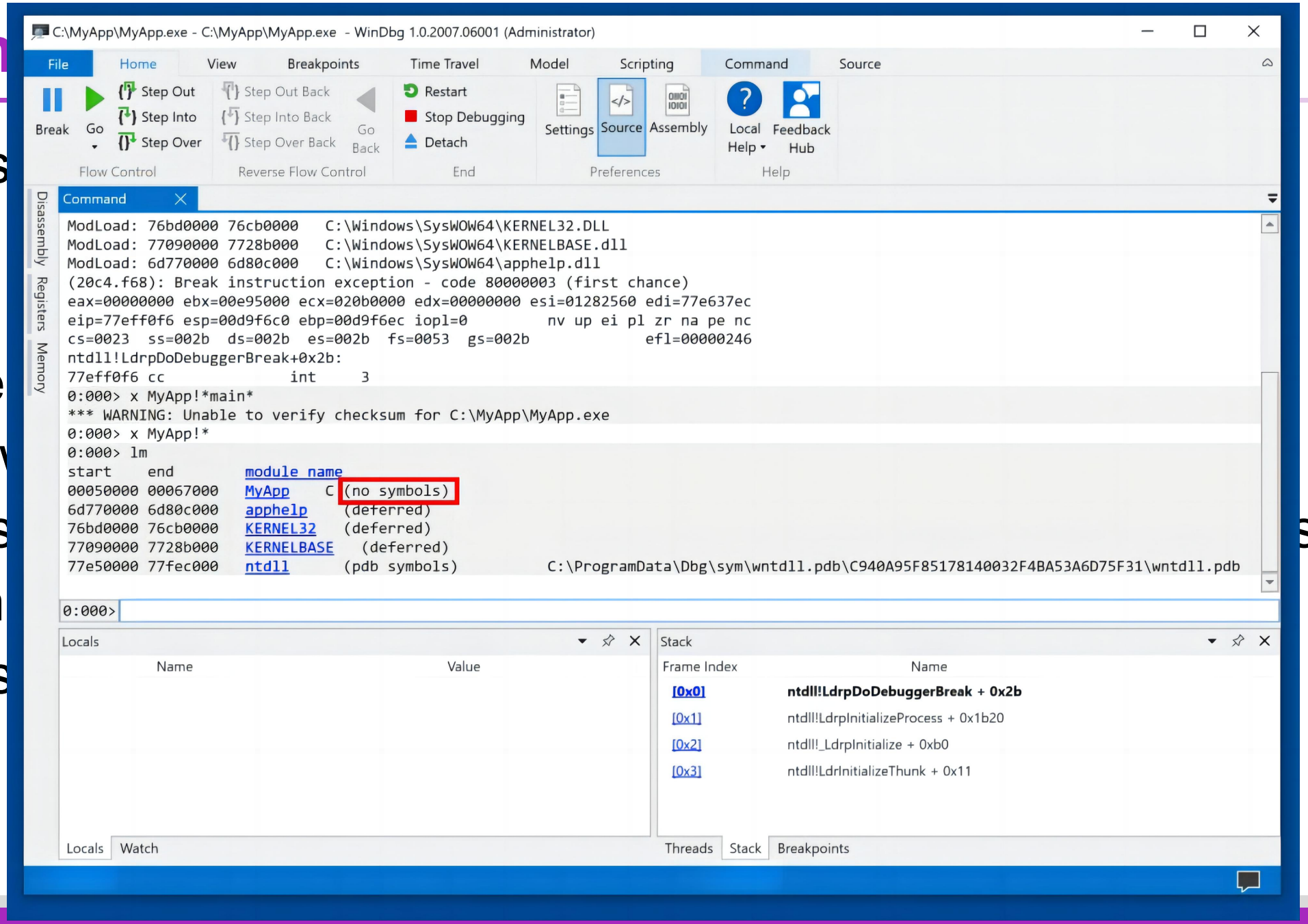
Find

- In the
  x MyA
  x MyA
- There



Sh

- To s
- lm
- The
  sho
- This
  Win
- This

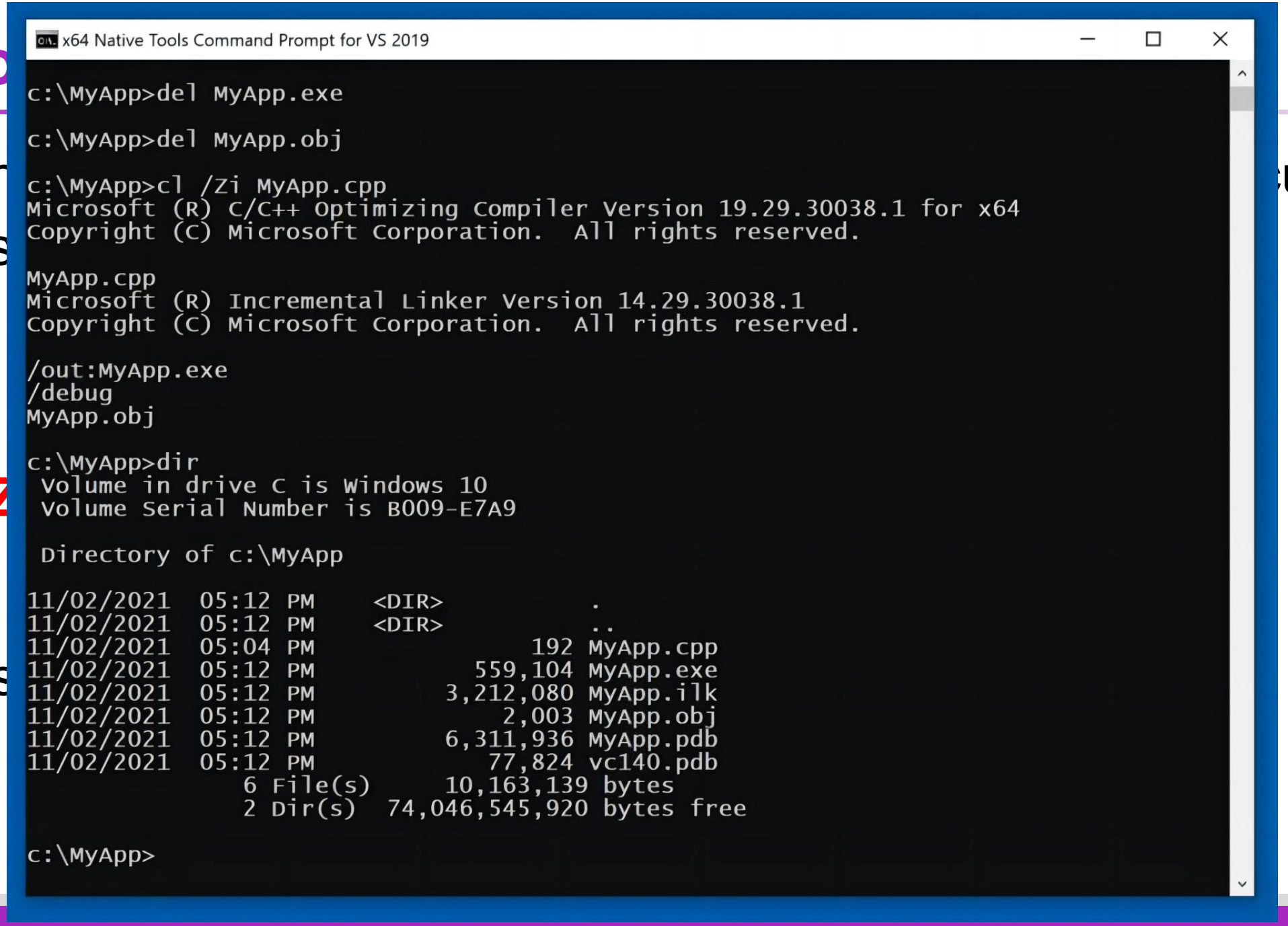


Co

- In th ute thes

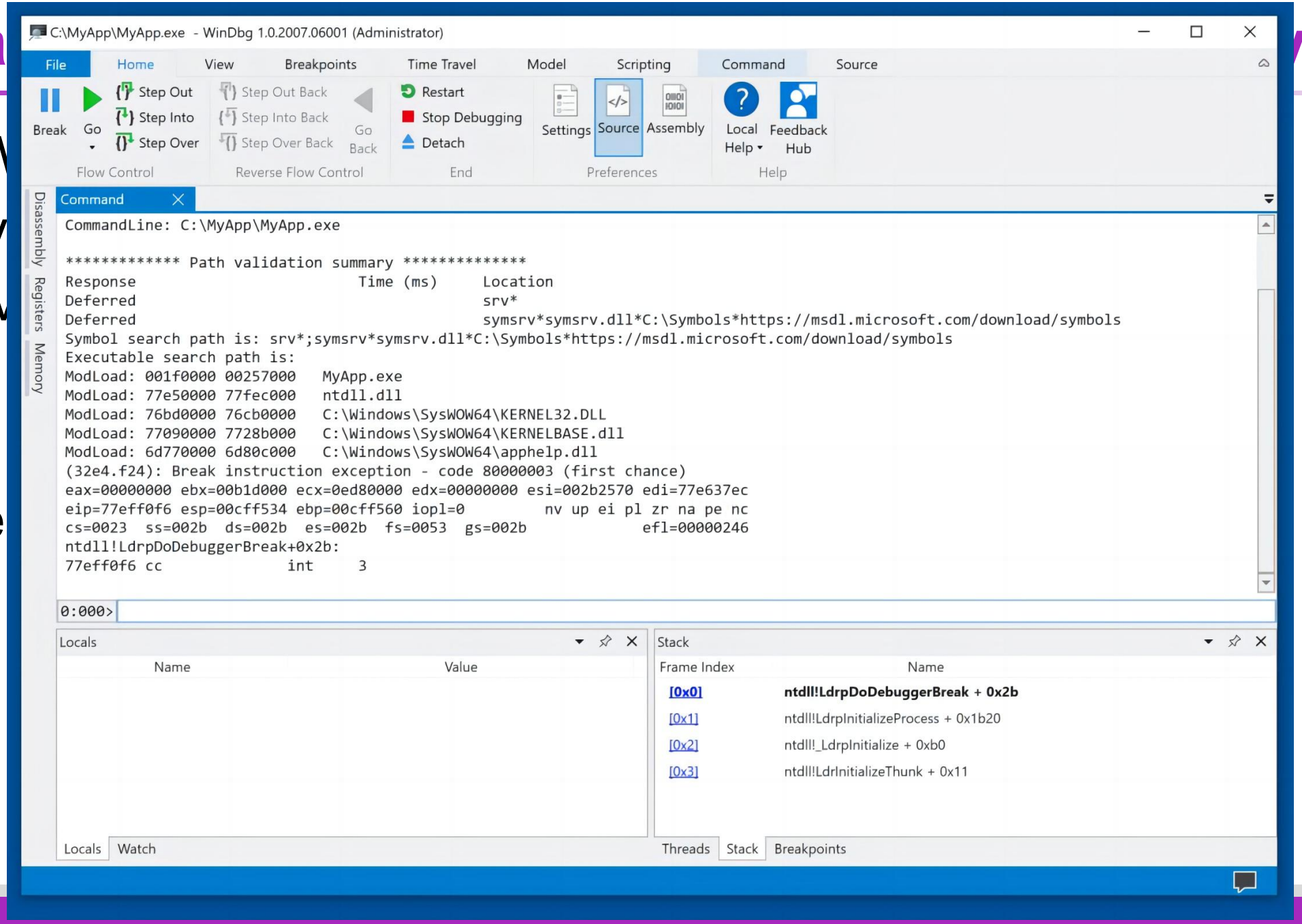
del
del
cl /Z
dir

- As s file and



La…yApp

- In W…
- Nav…
  C:\M…
  and …
- The…

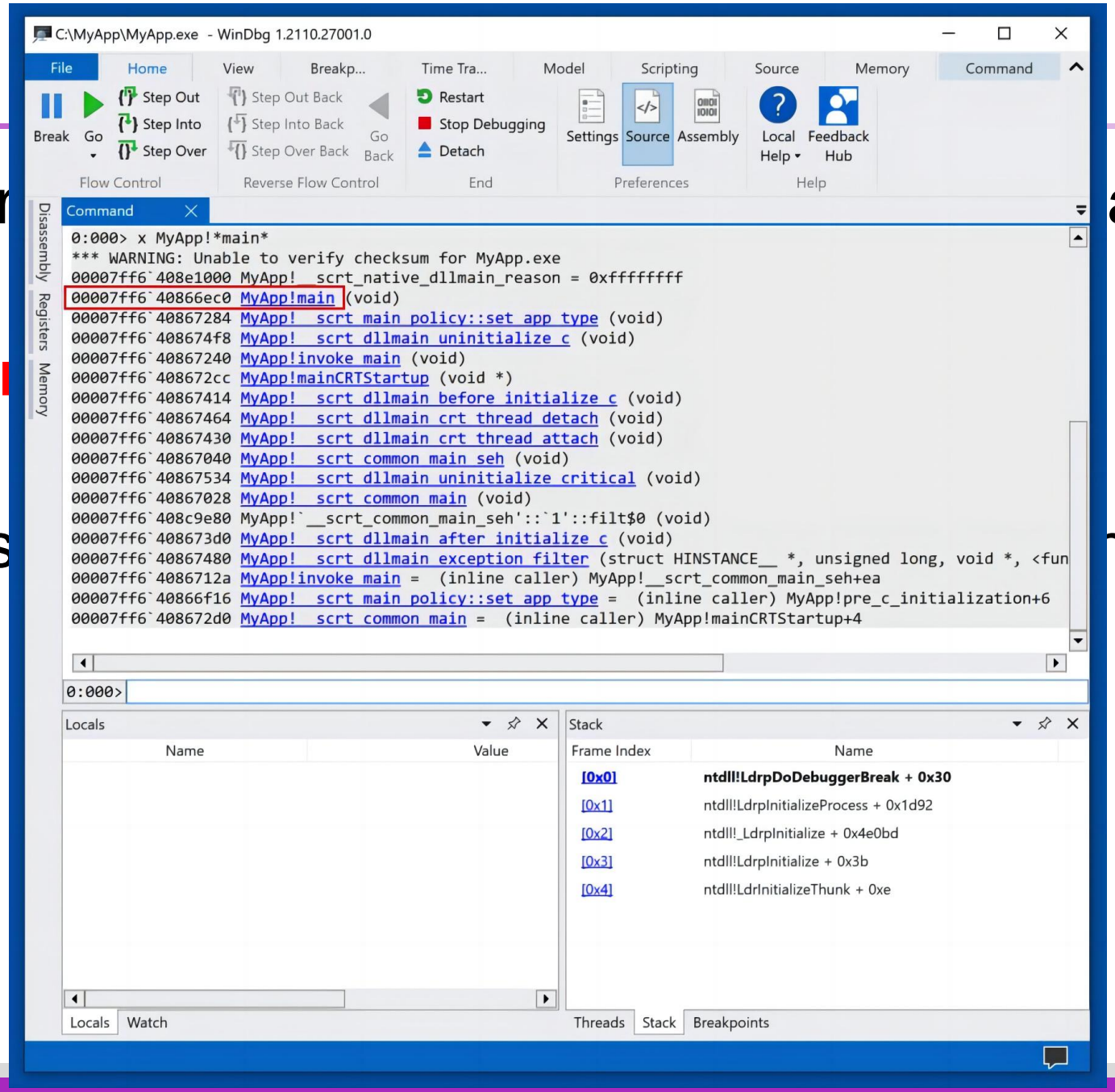


Finding

- In the lower … and:

x MyApp!*…

- Now it finds … shown below.

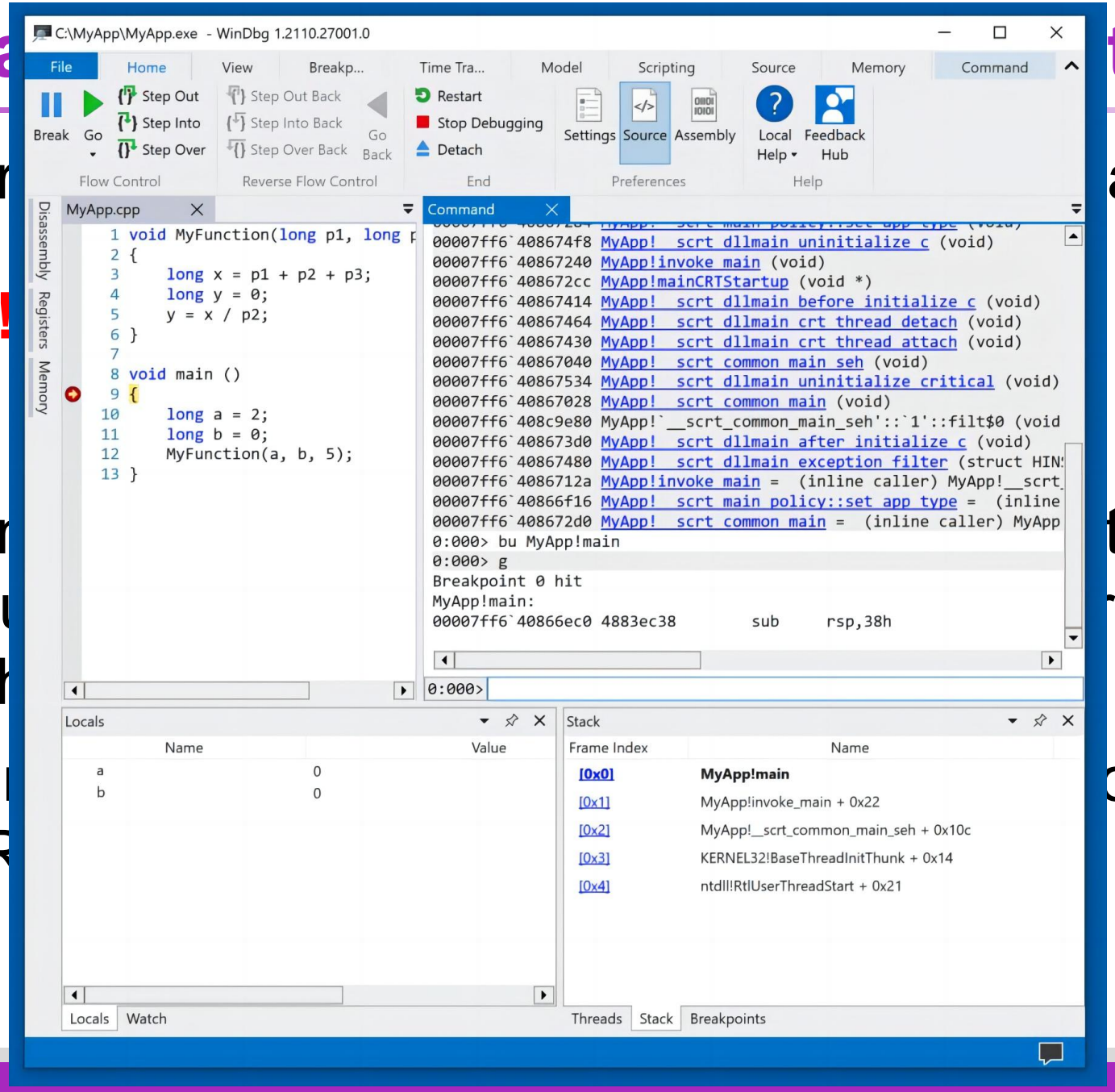


Setting a … t

- In the lower … and:

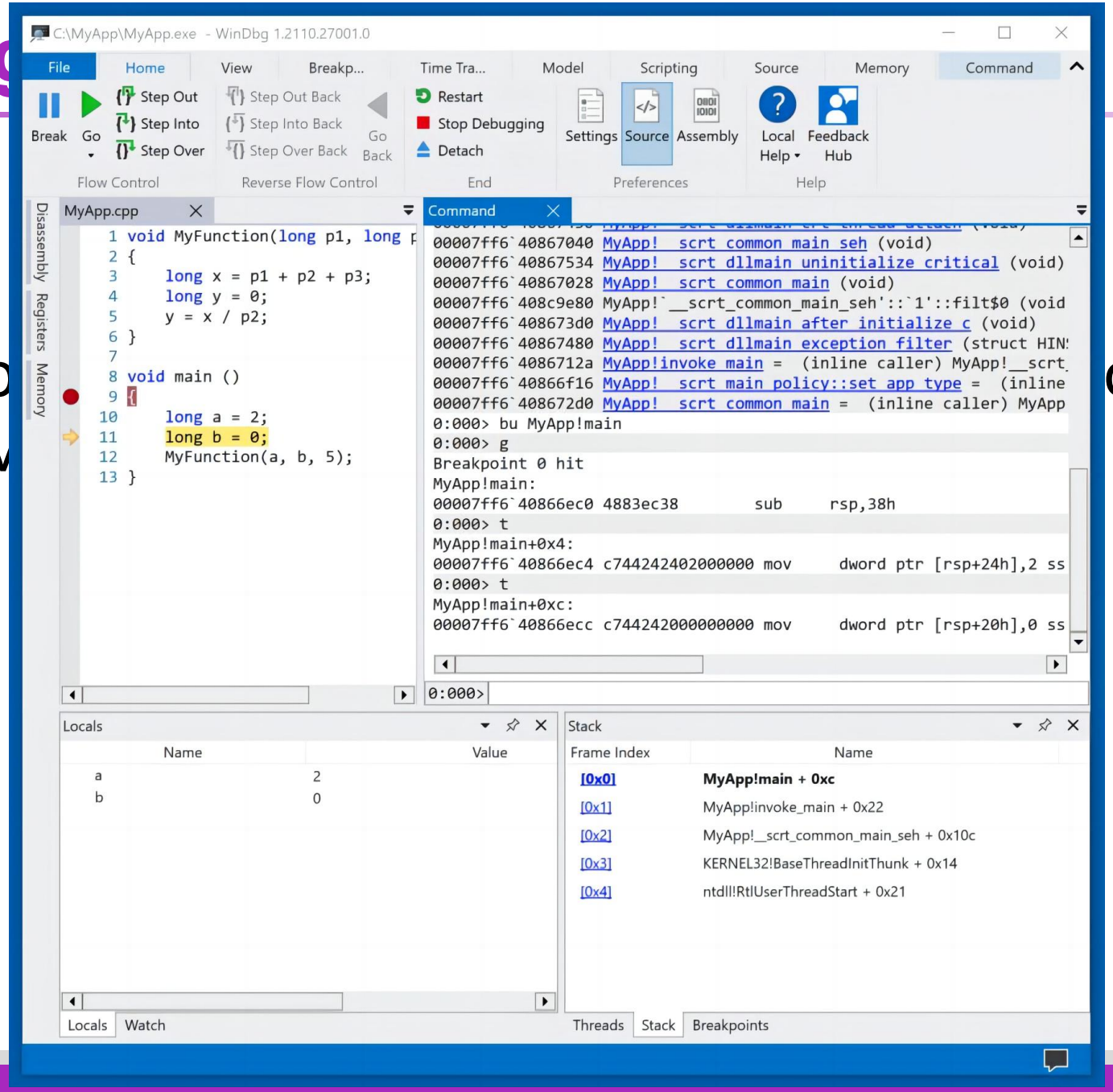
bu MyApp!

- In WinDbg, …
- The app run… t pane shows the C++ sou… rent instruction h…
- At the lower… ows the local variables. R…



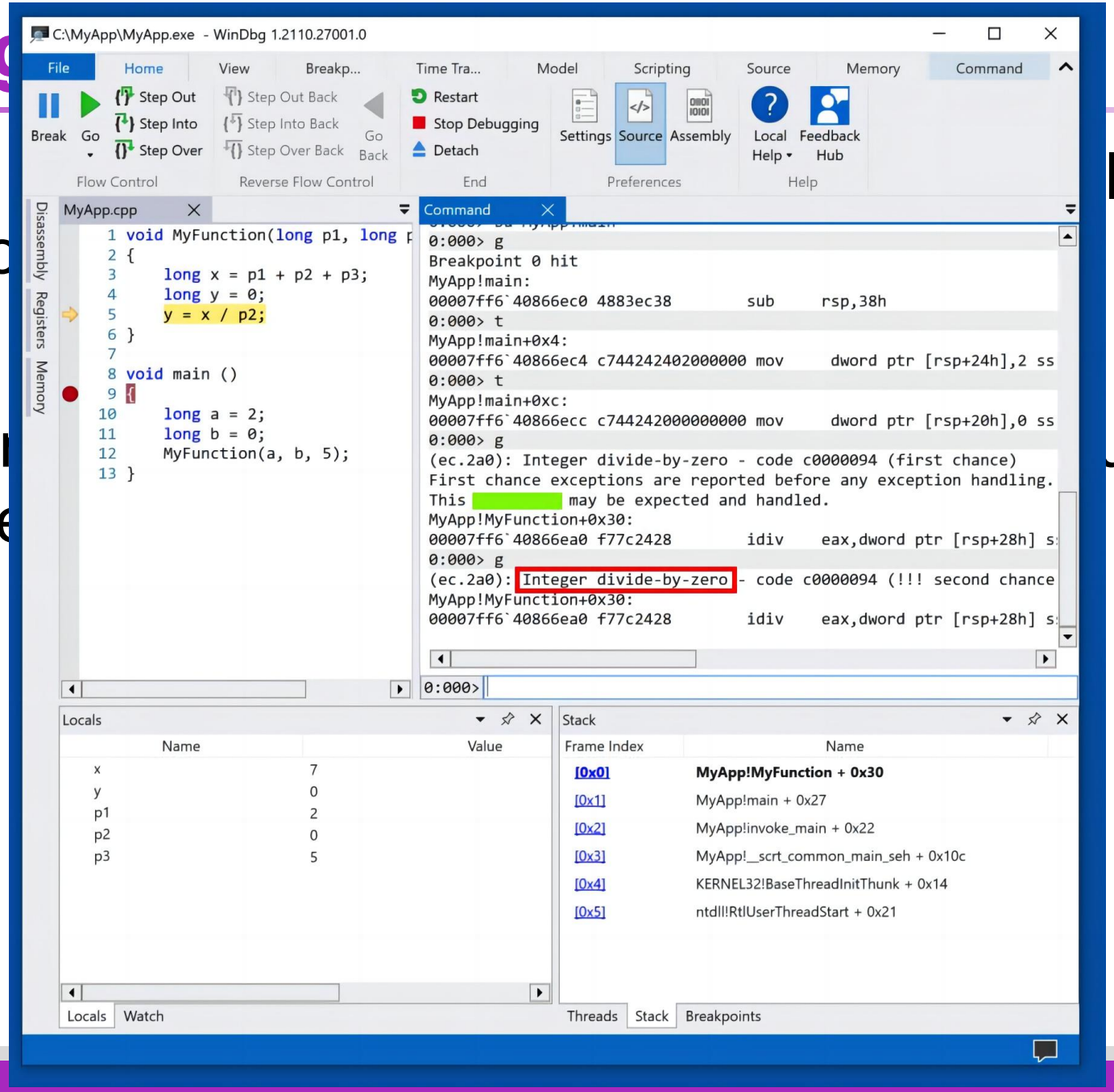
Stepping

- In WinDbg,
- As shown b of the source code. The v



Stepping

- In WinDbg, l more times, until the pro
- The progra use of a divide-by-ze



Part Four

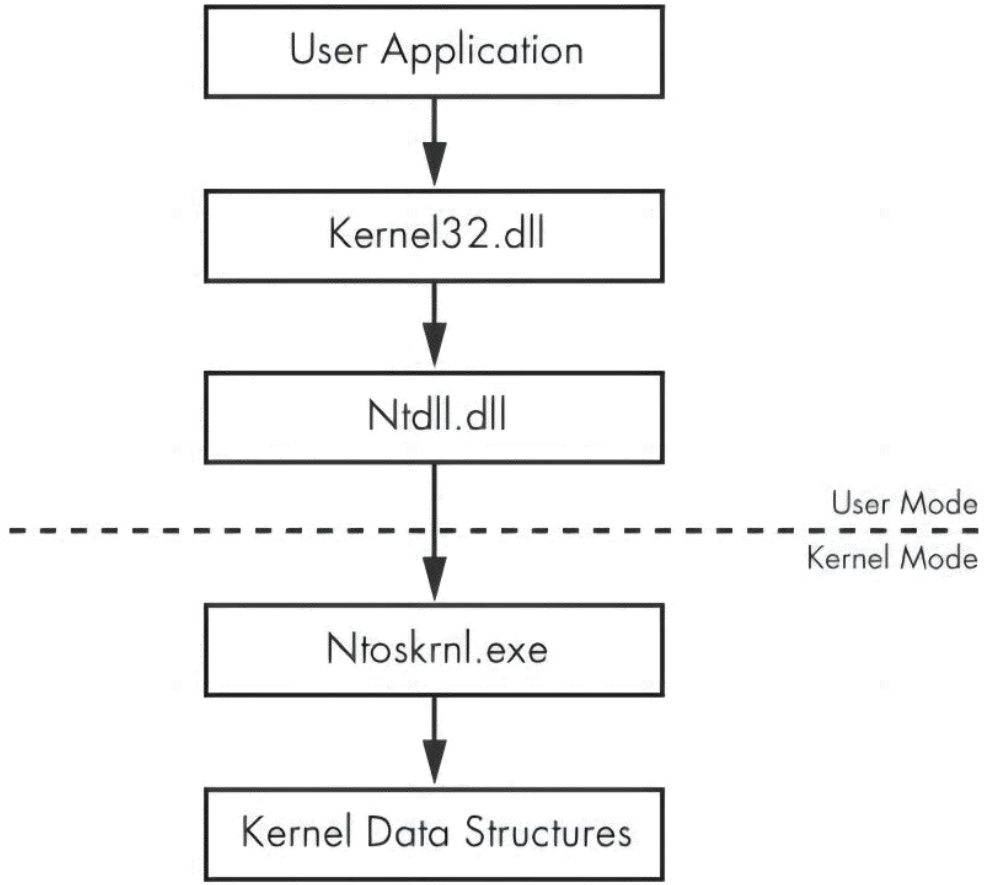
04

Kernel Debugging

2025-10-19

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

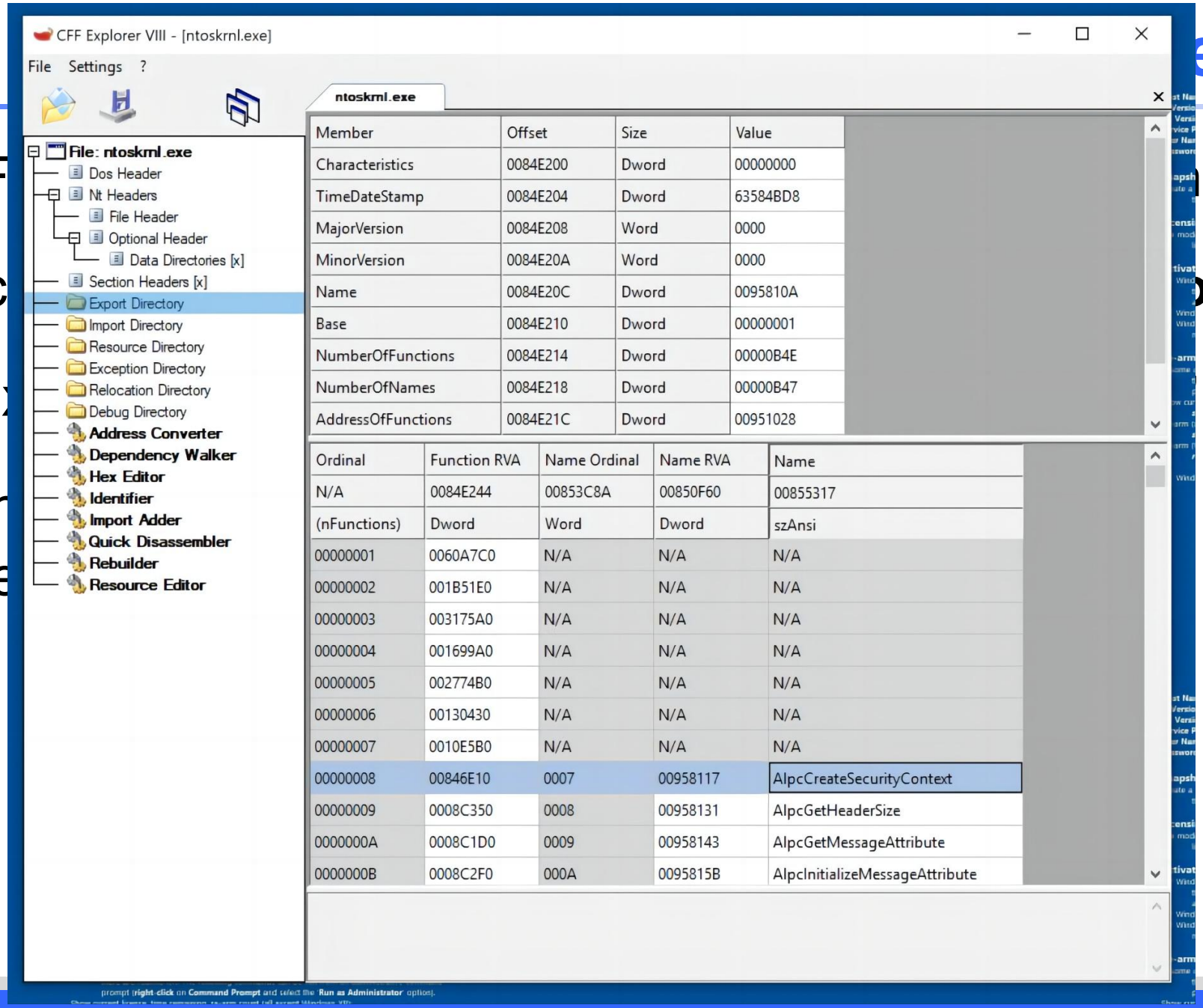
- If you are using the "Windows 10 w Tools" VM, CFF Explorer is already installed.

- If you are using some other machine, go to this URL and install "Explorer Suite":

  https://ntcore.com/?page_id=388

Exam…er

- Launch F…32.
- Right-clic…orer".
- In CFF Ex….
- As shown… ntoskrnl.e…

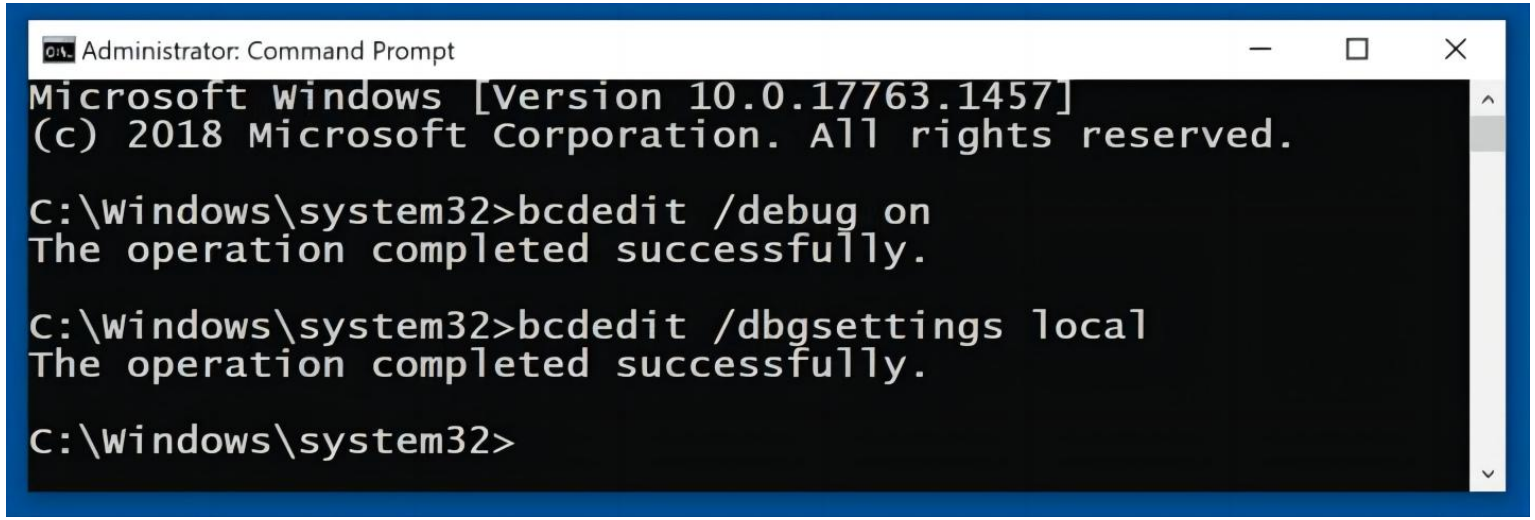


Using BCDEdit for Local Debugging

- 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

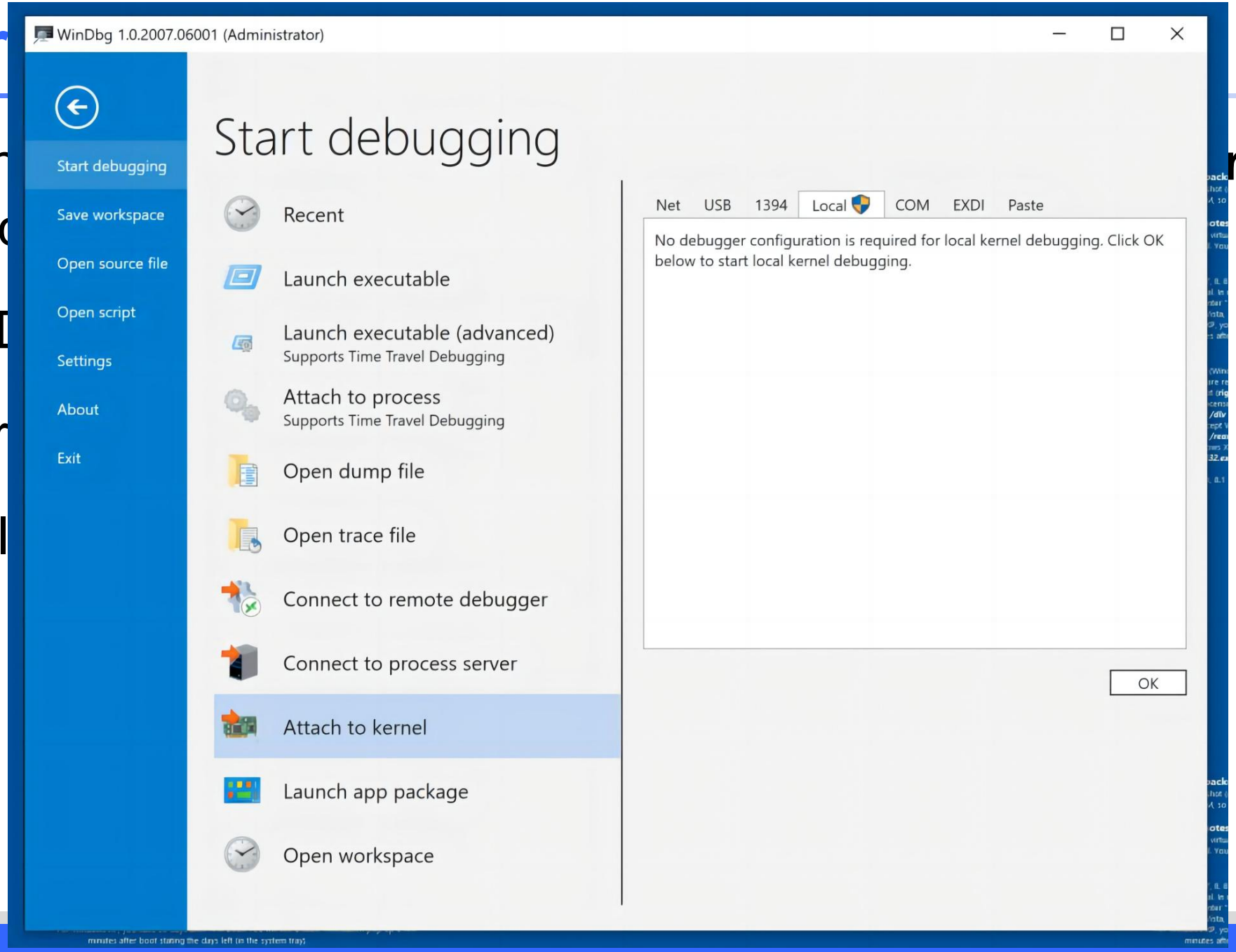
bcdedit /dbgsettings local

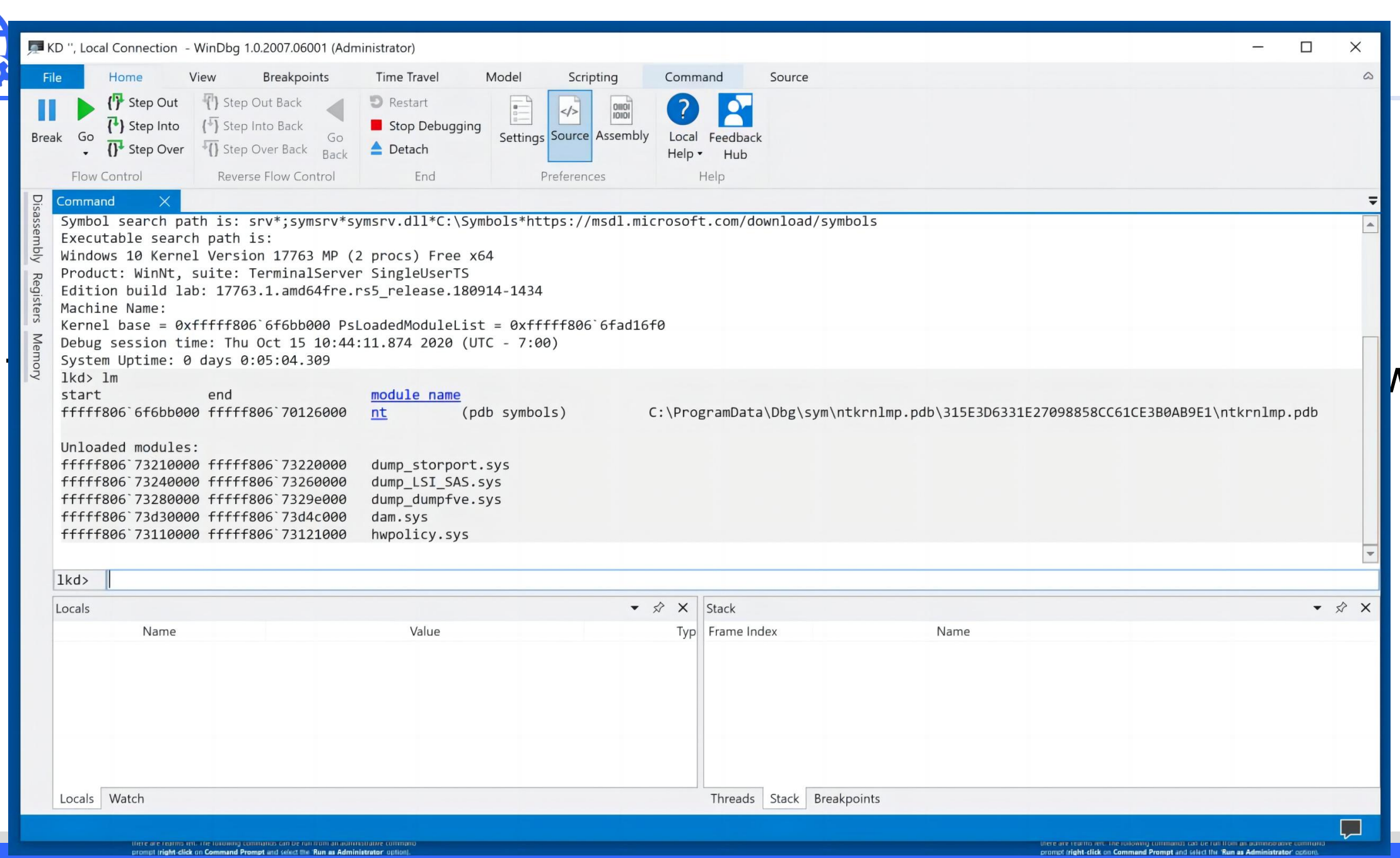


- Restart your Windows machine.

Star

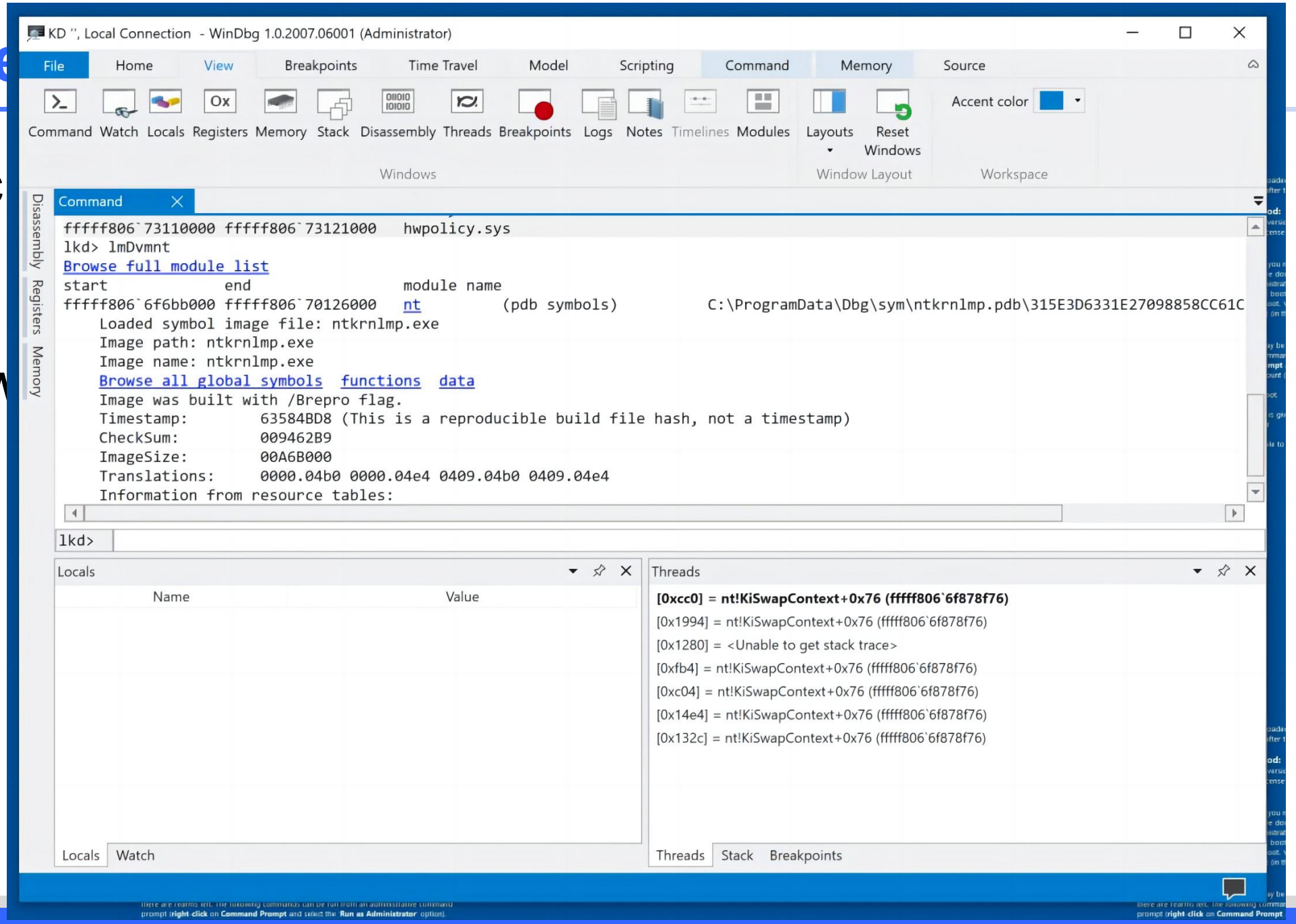
- Click th … and clic … "review"
- In WinD …
- In the r …
- At the l …




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
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
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
Typ
Stack
Frame Index
Name
Locals
Watch
Threads
Stack
Breakpoints

Vie

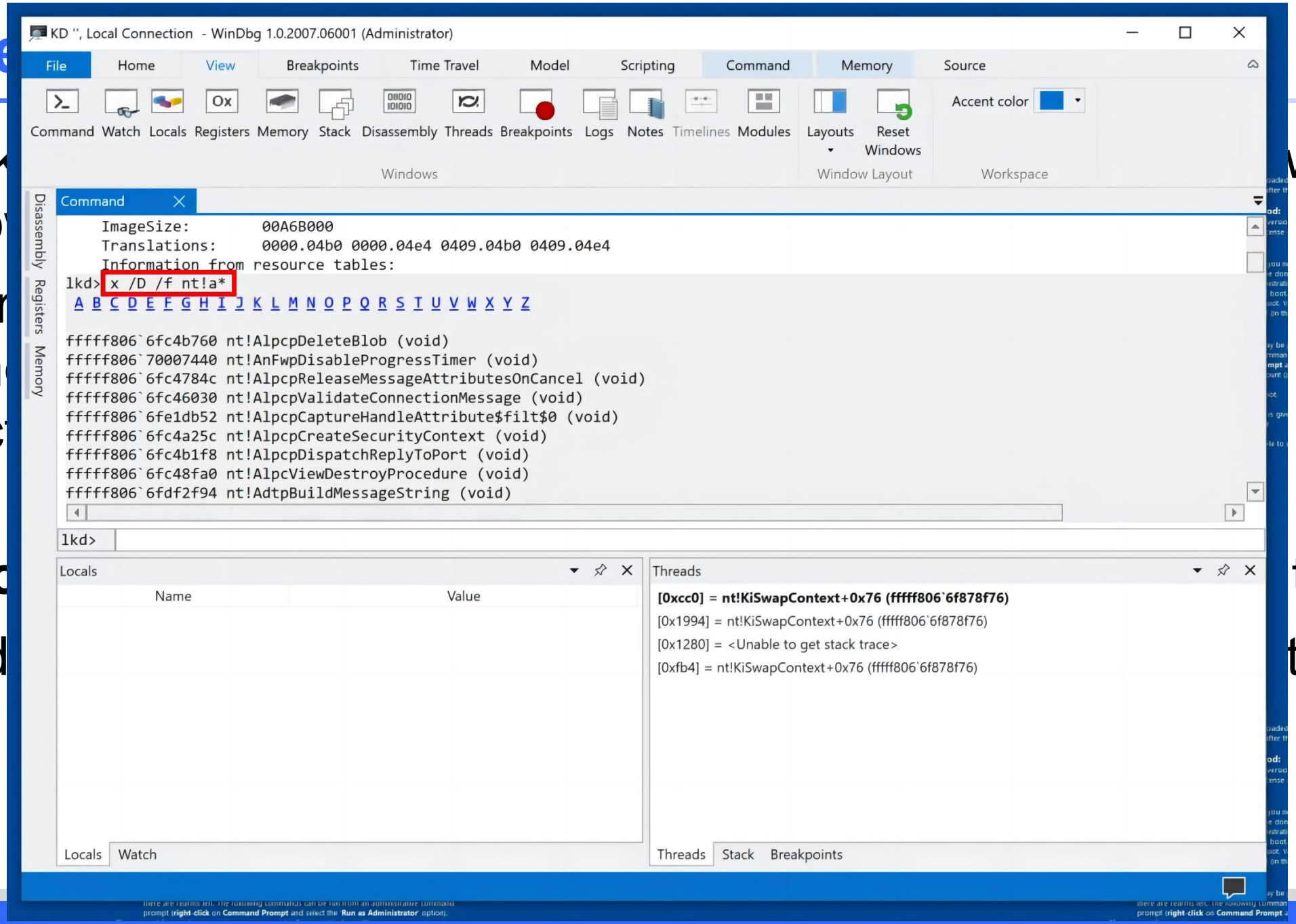
- Clic
- Now


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
Windows
Layouts Reset Windows
Window Layout
Accent color
Workspace
Disassembly Registers Memory
Command
fffff806`73110000 fffff806`73121000 hwpolicy.sys
lkd> lmDvmnt
Browse full module list
start end module name
fffff806`6f6bb000 fffff806`70126000 nt (pdb symbols) C:\ProgramData\Dbg\sym\ntkrnlmp.pdb\315E3D6331E27098858CC61C
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
Locals Watch
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)
Threads Stack Breakpoints

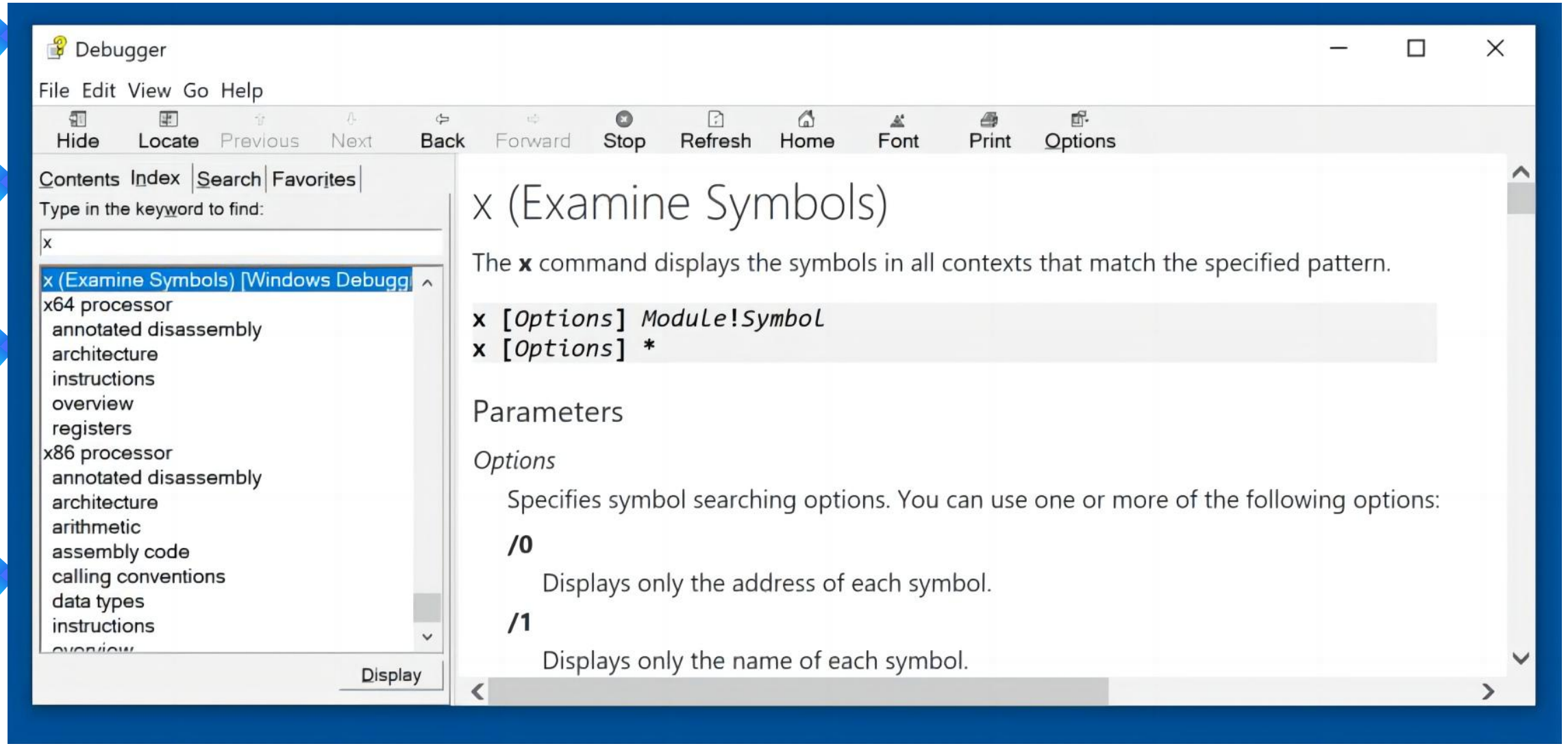
Vie

- Click
  belo
- Ther
  som
  func
- You
  Alpc
- prod
  "**A**",

  x /D



Using Help

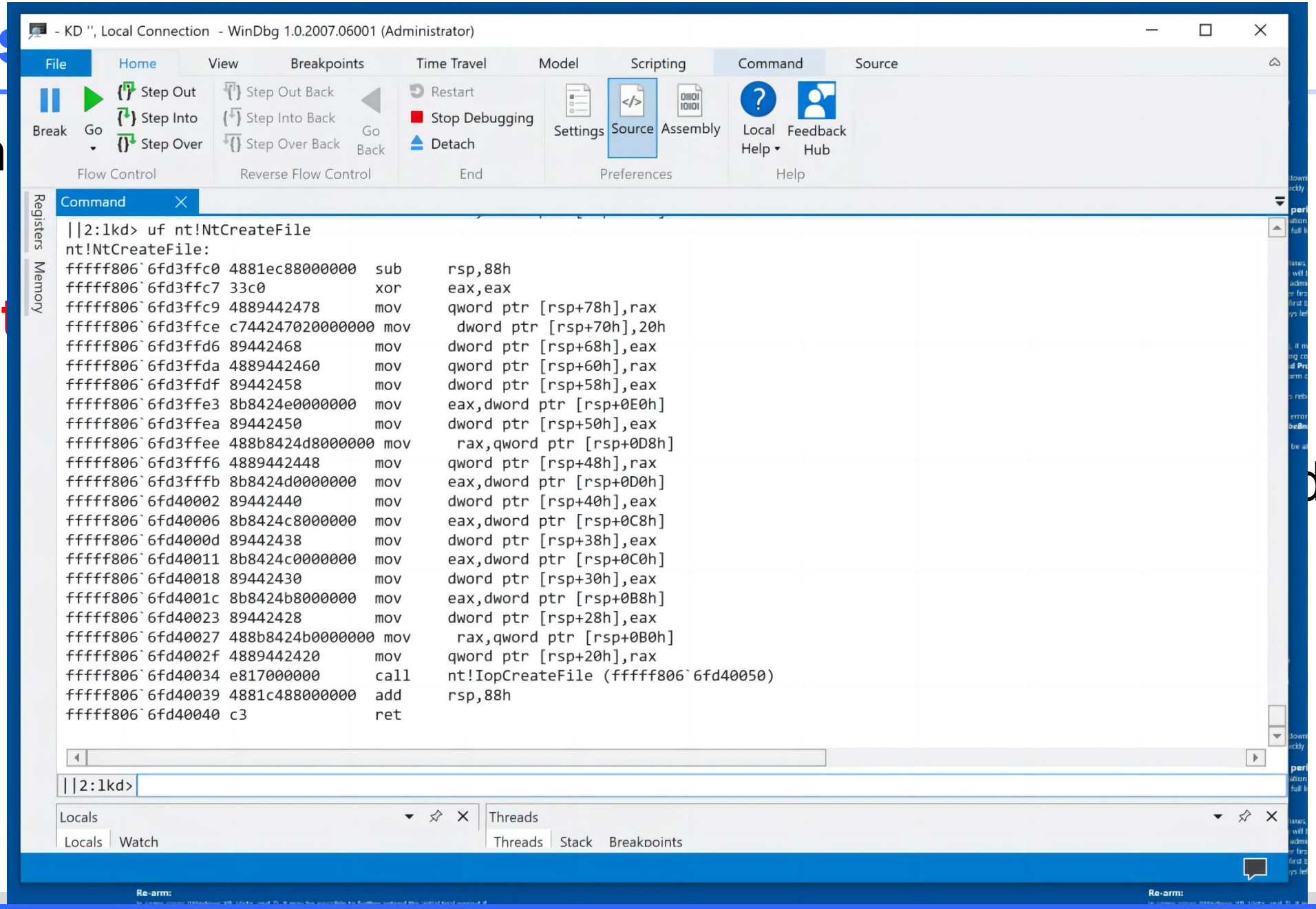

Debugger
File Edit View Go Help
Hide Locate Previous Next Back Forward Stop Refresh Home Font Print Options
Contents Index Search Favorites
Type in the keyword to find:
x
x (Examine Symbols) [Windows Debugg
x64 processor
annotated disassembly
architecture
instructions
overview
registers
x86 processor
annotated disassembly
architecture
arithmetic
assembly code
calling conventions
data types
instructions
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.

Dis

- In th

uf nt

- The



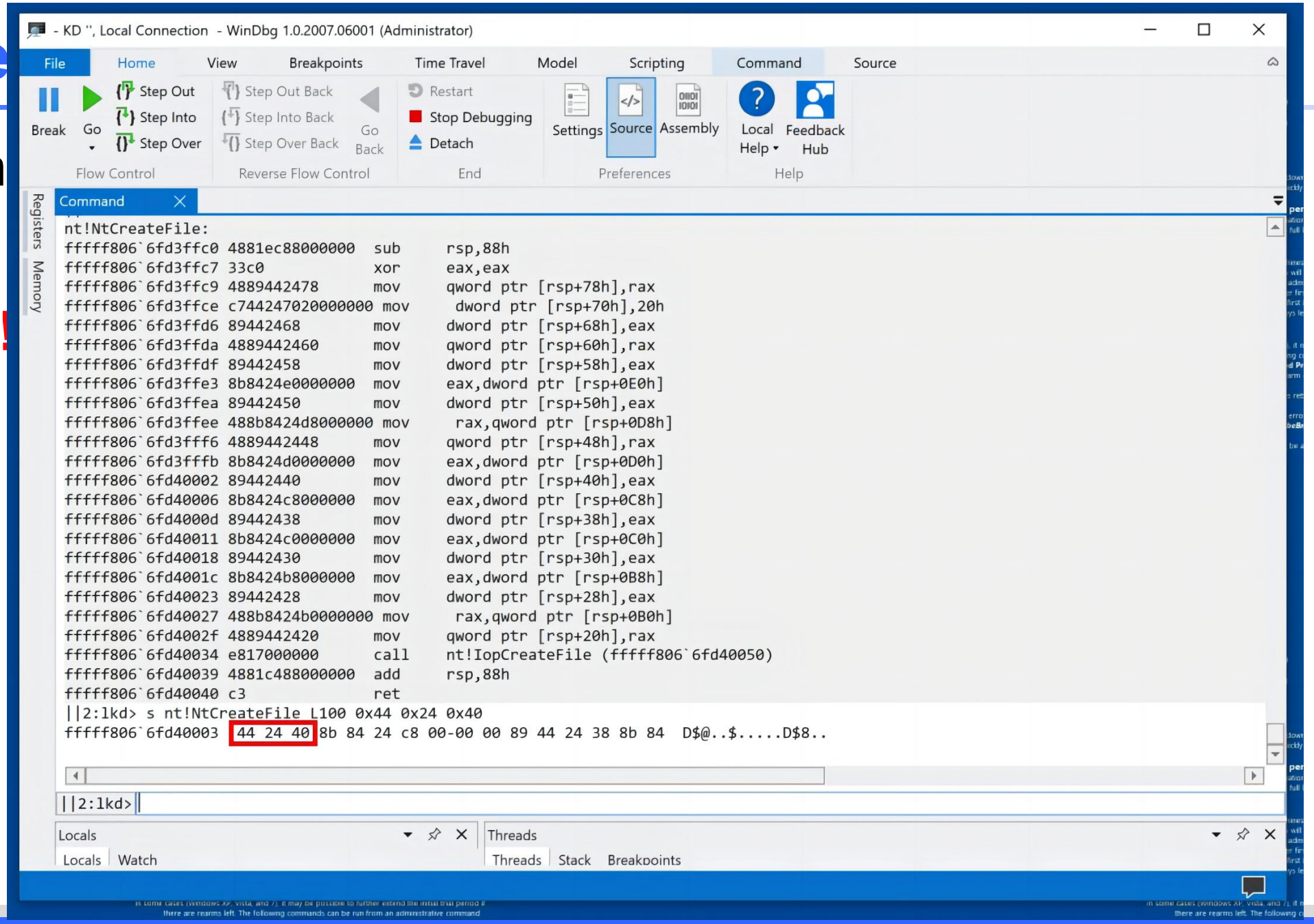
d raw hex

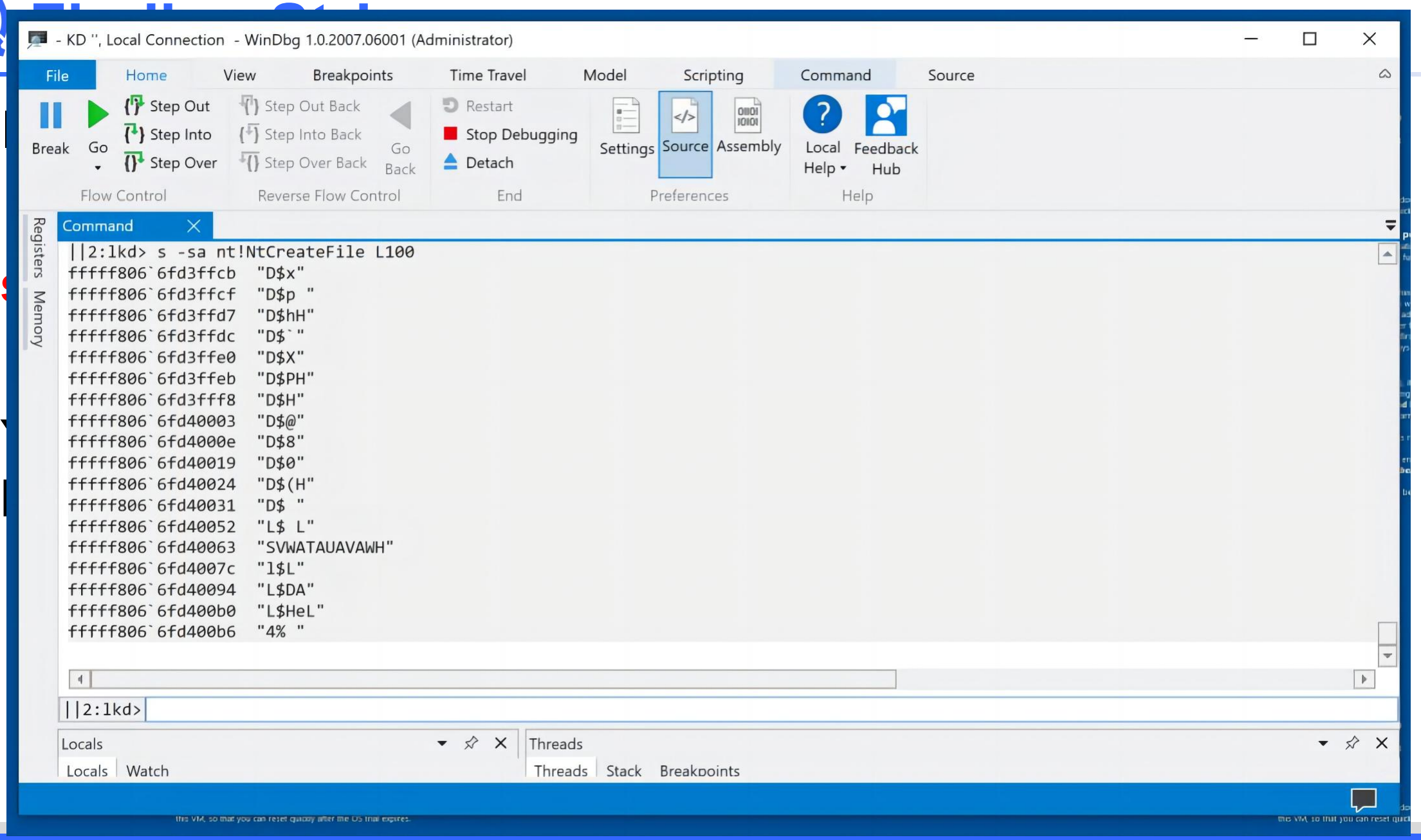
Se

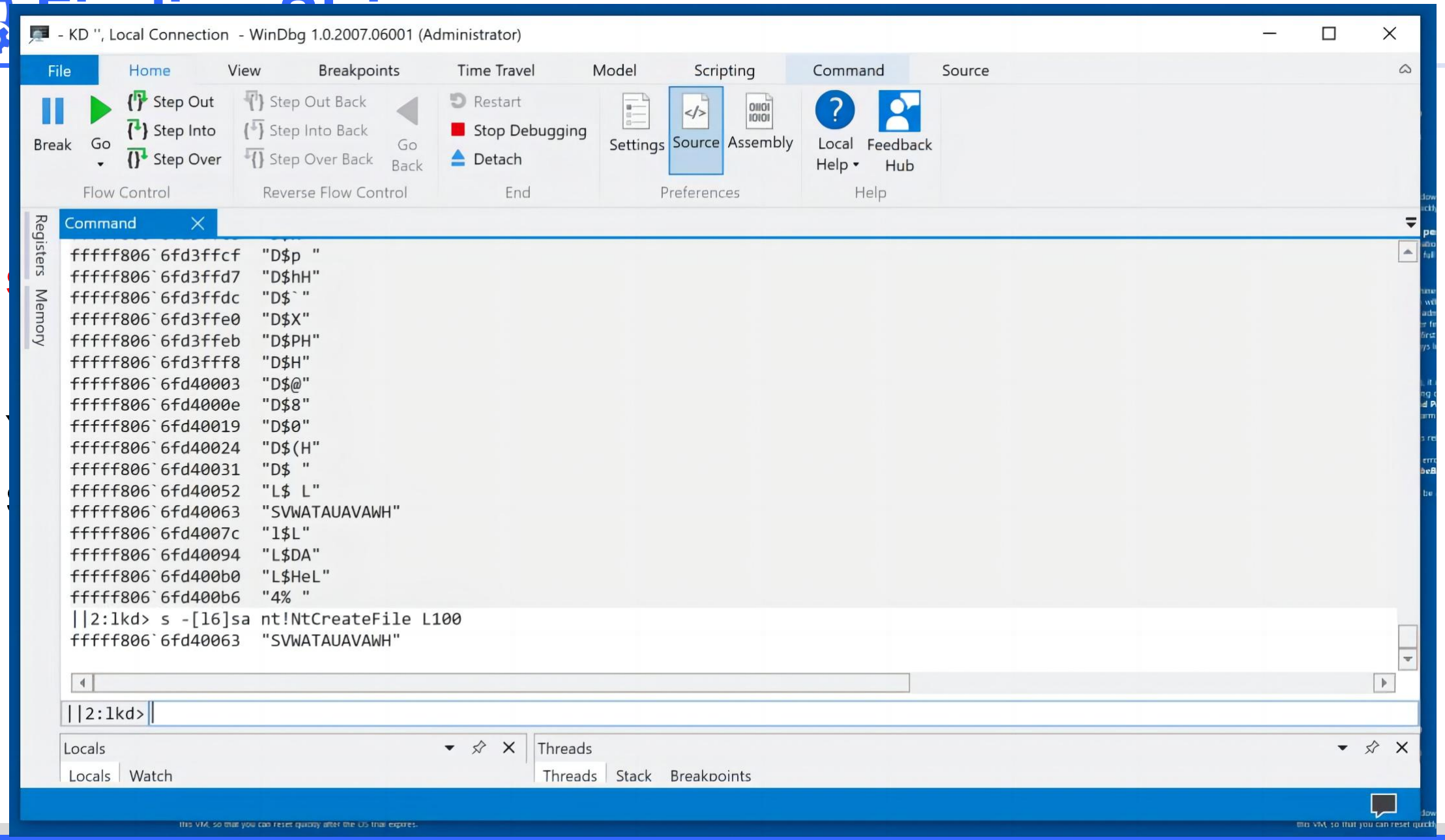
- In th

s nt!

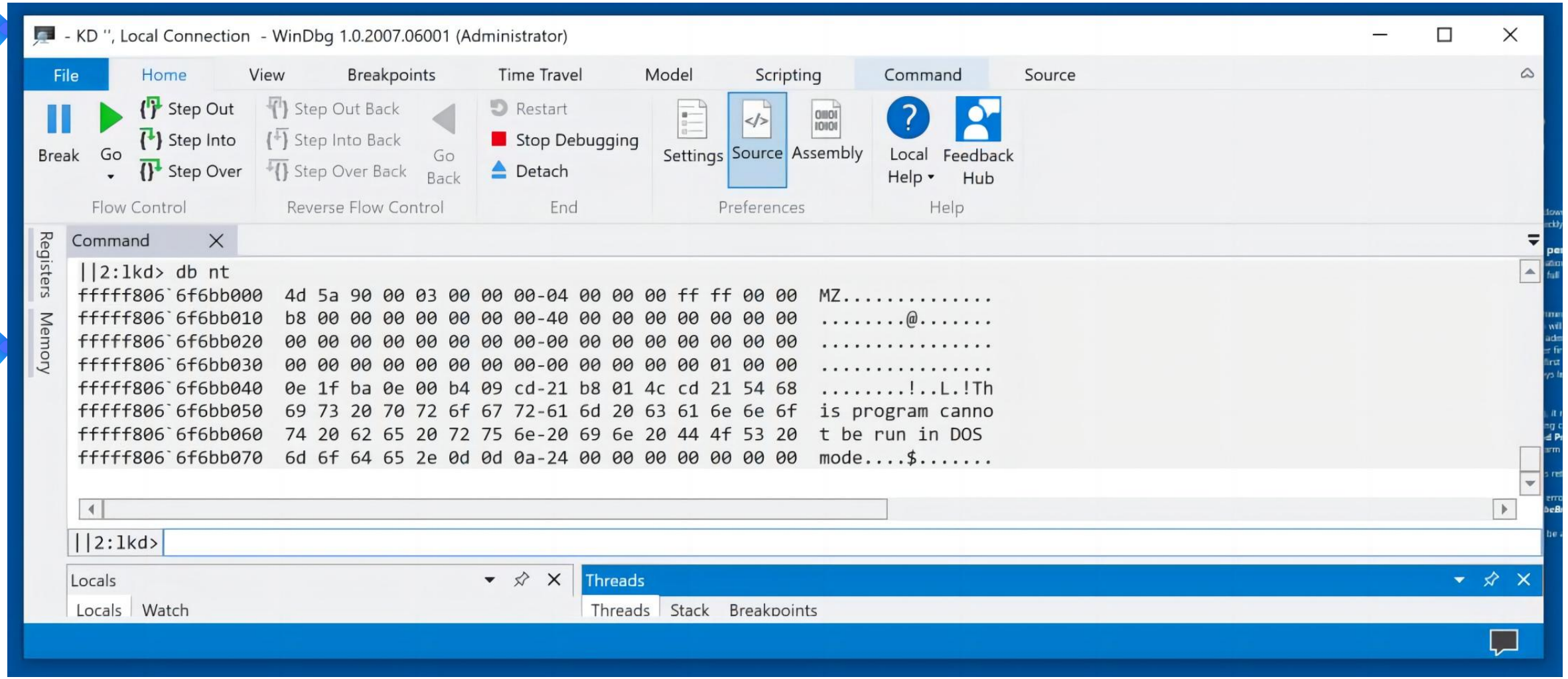
- The




- 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
Go Back
Restart
Stop Debugging
Detach
Settings
Source
Assembly
Local Help
Feedback Hub
Flow Control
Reverse Flow Control
End
Preferences
Help
Registers
Memory
Command
||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
Locals
Watch
Threads
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
Go Back
Restart
Stop Debugging
Detach
Settings
Source
Assembly
Local Help
Feedback Hub
Flow Control
Reverse Flow Control
End
Preferences
Help
Registers
Memory
Command
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> s -[16]sa nt!NtCreateFile L100
fffff806`6fd40063 "SVWATAUAVAWH"
||2:1kd>
Locals
Locals
Watch
Threads
Threads
Stack
Breakpoints

Display Memory

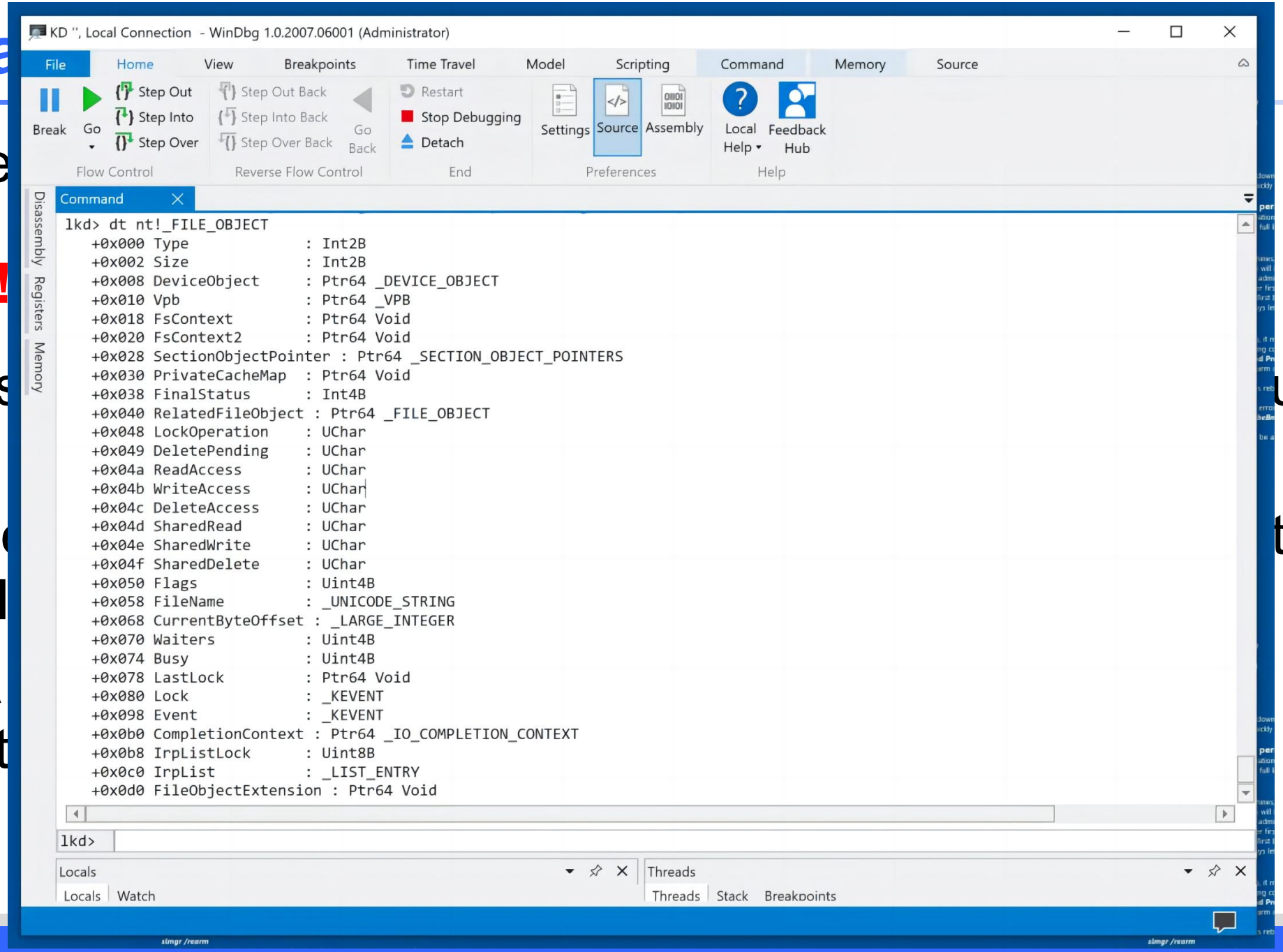


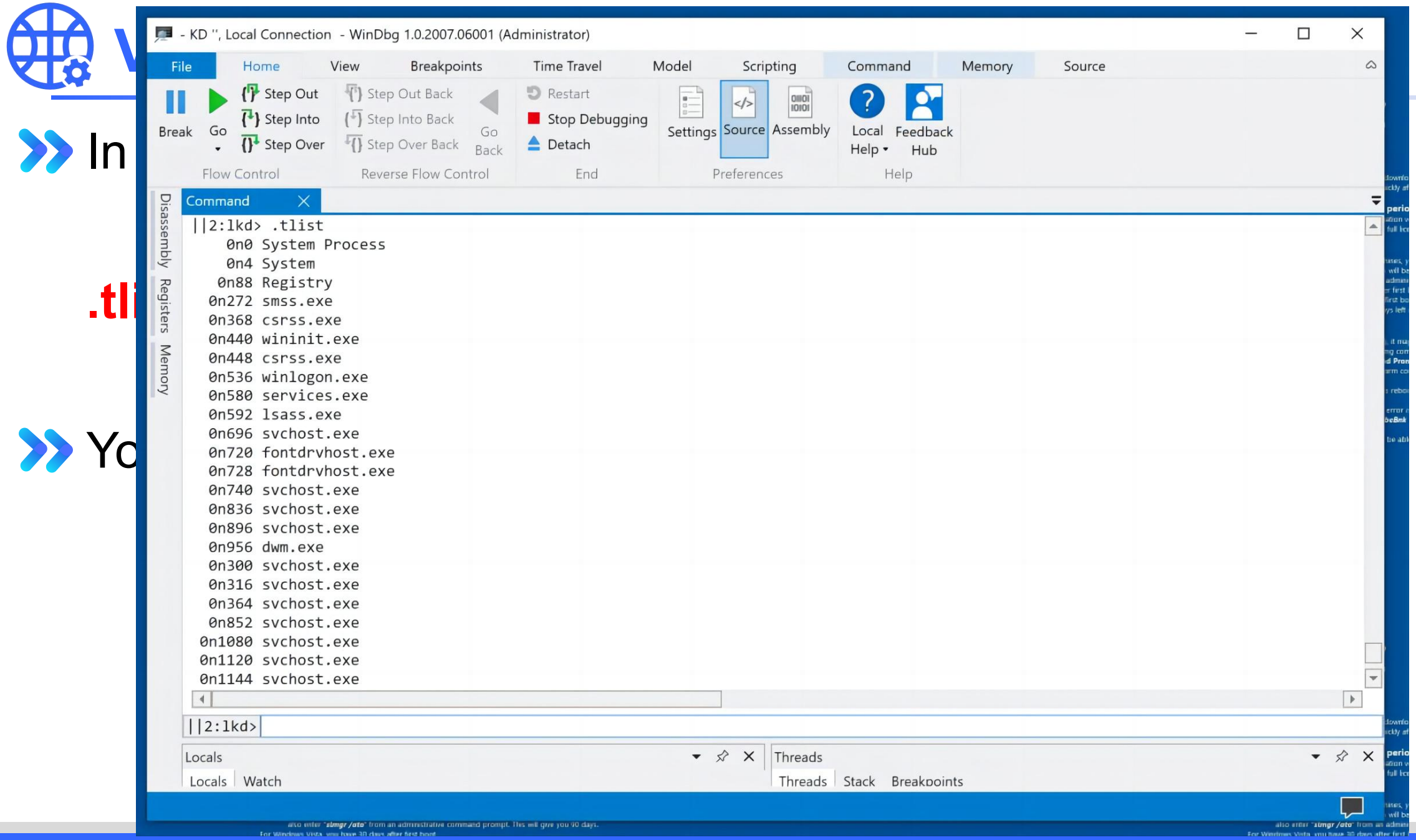
Exa

- In the

  dt nt!

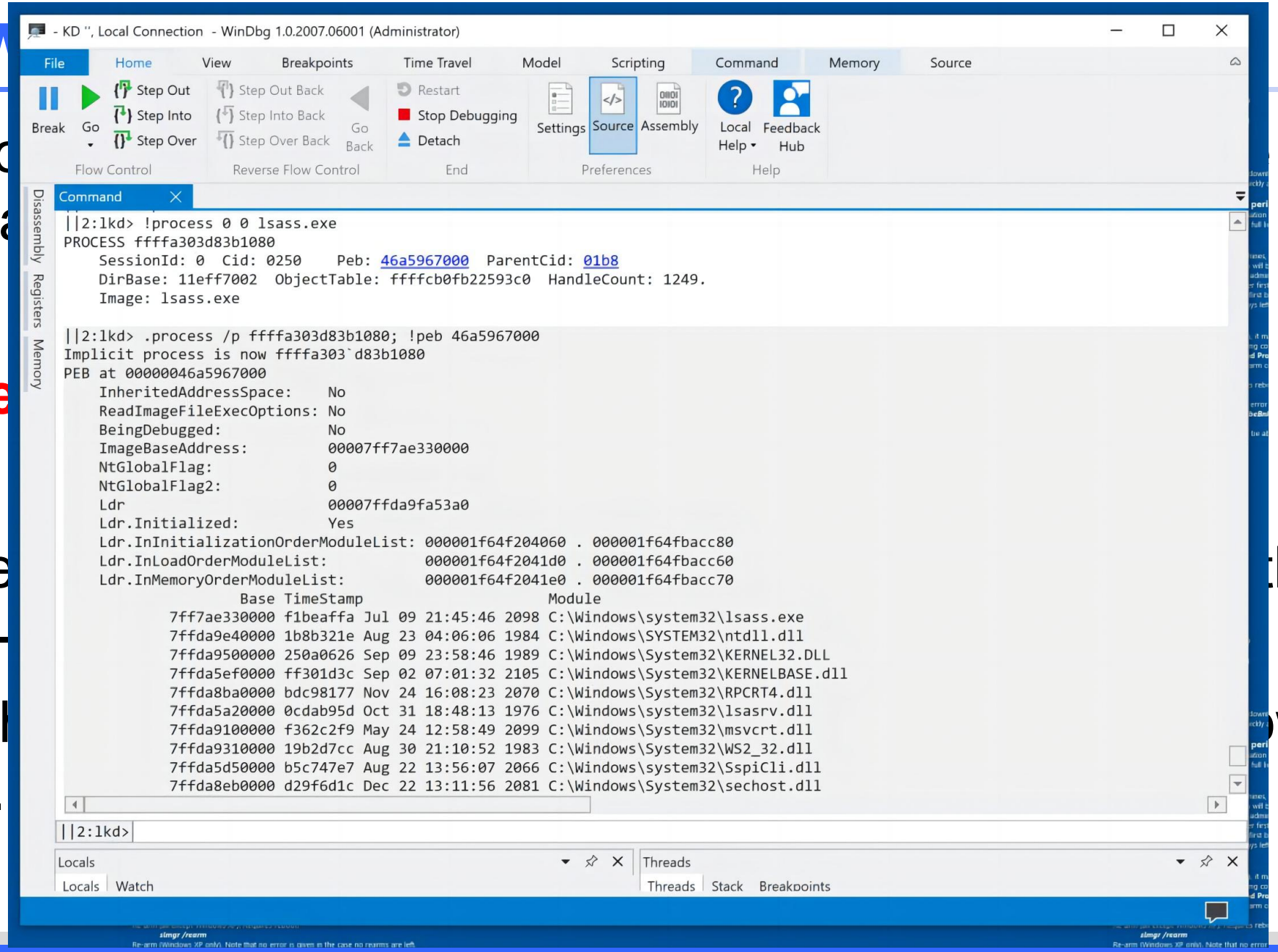
- This s ure used
- Notic the **FileN**
- For a struct



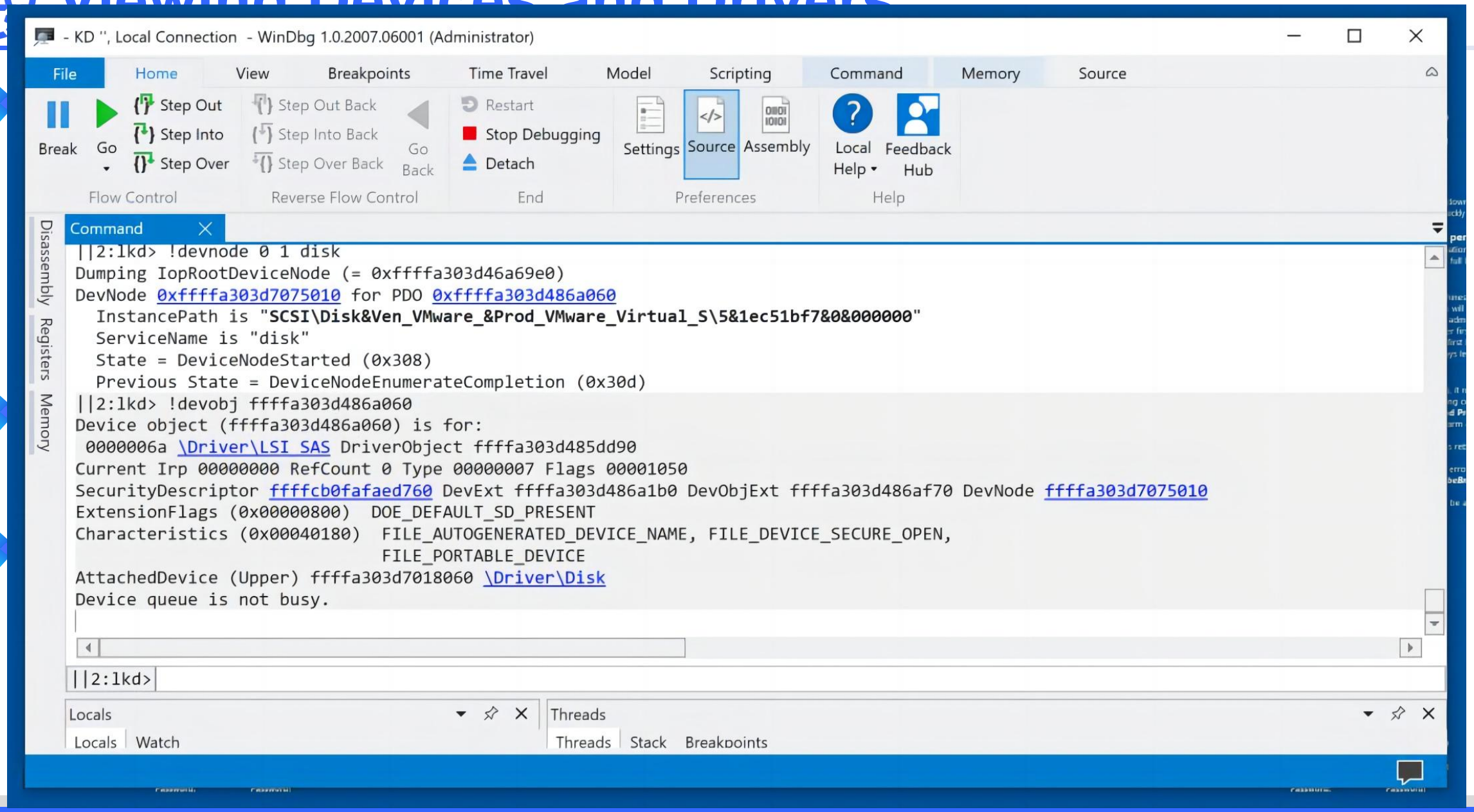

- KD '', Local Connection - WinDbg 1.0.2007.06001 (Administrator)
File
Home
View
Breakpoints
Time Travel
Model
Scripting
Command
Memory
Source
Break
Go
Step Out
Step Into
Step Over
Step Out Back
Step Into Back
Step Over Back
Go Back
Restart
Stop Debugging
Detach
Settings
Source
Assembly
Local Help
Feedback Hub
Flow Control
Reverse Flow Control
End
Preferences
Help
Disassembly
Registers
Memory
Command
||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
||2:1kd>
Locals
Locals
Watch
Threads
Threads
Stack
Breakpoints

View

- For mo… this comma…
- !proce…
- You se… the "peb"--…
- Click t… own below.



Viewing Devices and Drivers



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