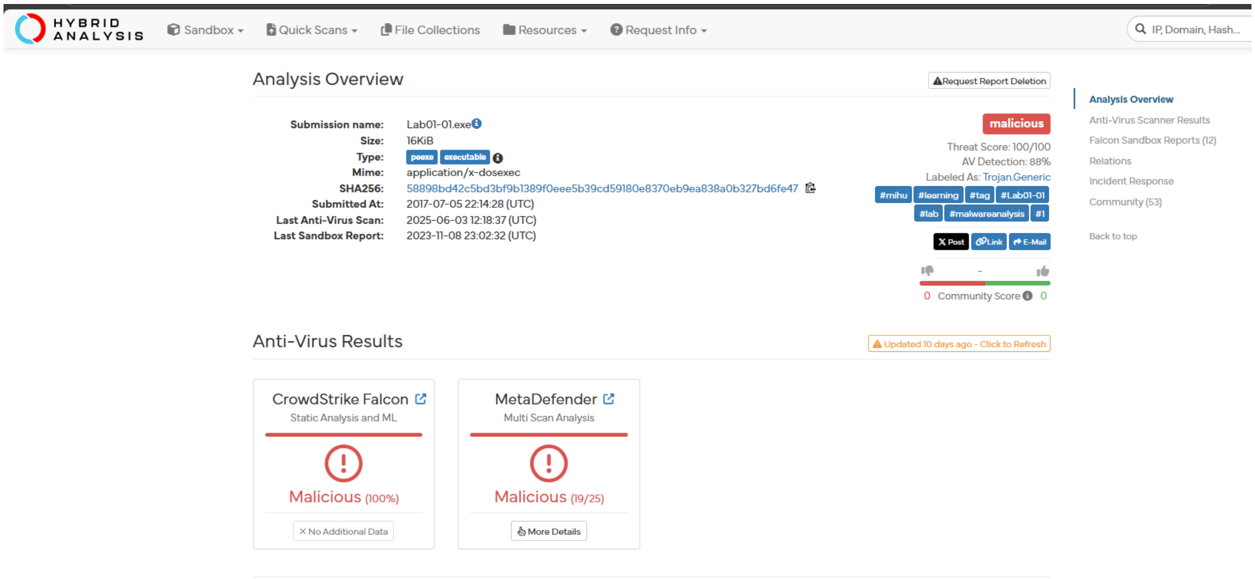
NGUYEN NAM KHANH – HE191159 – IA1902 – IAM302

LAB 8 Configuring a Malware Lab

Part 1: Basic Static Techniques

a. Analyzing Lab01-01.exe and Lab01-01.dll

Using Hybrid Analysis for Lab01-01.exe



Analysis Overview

Submission name: Lab01-01.exe
Size: 16KiB
Type: peexe executable
Mime: application/x-dosexec
SHA256: 58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47
Submitted At: 2017-07-05 22:14:28 (UTC)
Last Anti-Virus Scan: 2025-06-03 12:18:37 (UTC)
Last Sandbox Report: 2023-11-08 23:02:32 (UTC)

malicious
Threat Score: 100/100
AV Detection: 88%
Labeled As: Trojan.Generic
#mihu #learning #tag #Lab01-01 #lab #malwareanalysis #1

0 Community Score 0

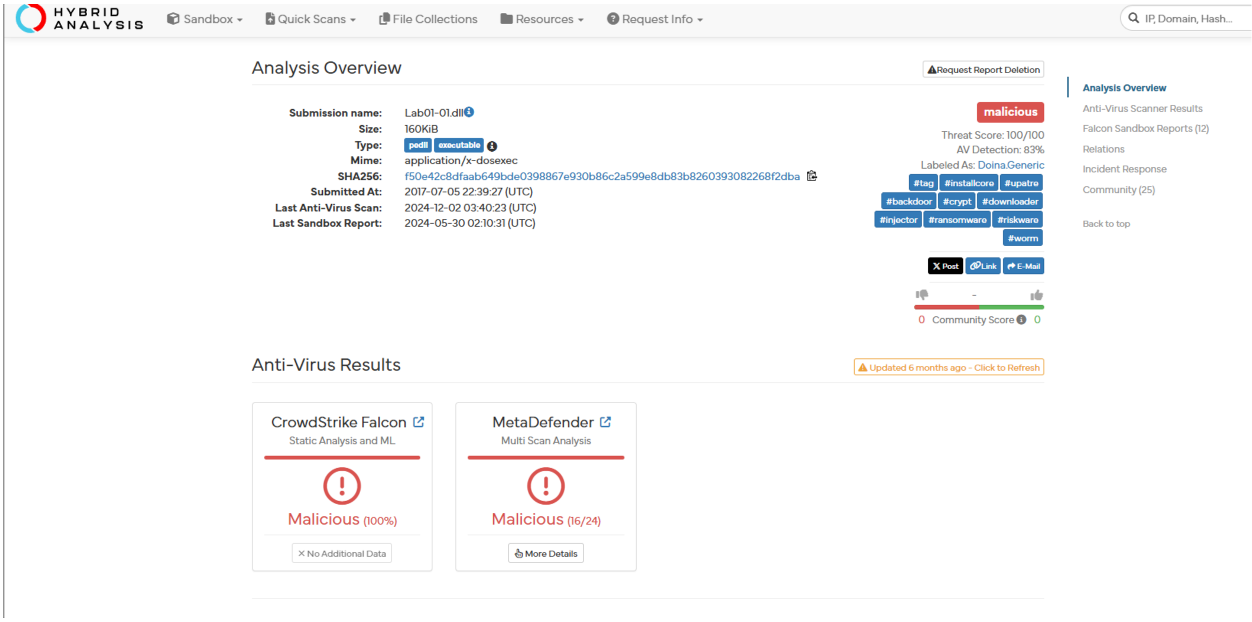
Anti-Virus Results

Updated 10 days ago - Click to Refresh

CrowdStrike Falcon
Static Analysis and ML
Malicious (100%)

MetaDefender
Multi Scan Analysis
Malicious (19/25)

Lab01-01.dll



Analysis Overview

Submission name: Lab01-01.dll
Size: 160KiB
Type: pedll executable
Mime: application/x-dosexec
SHA256: f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba
Submitted At: 2017-07-05 22:39:27 (UTC)
Last Anti-Virus Scan: 2024-12-02 03:40:23 (UTC)
Last Sandbox Report: 2024-05-30 02:10:31 (UTC)

malicious
Threat Score: 100/100
AV Detection: 83%
Labeled As: Doina.Generic
#tag #installcore #upatre #backdoor #crypt #downloader #injector #ransomware #riskware #worm

0 Community Score 0

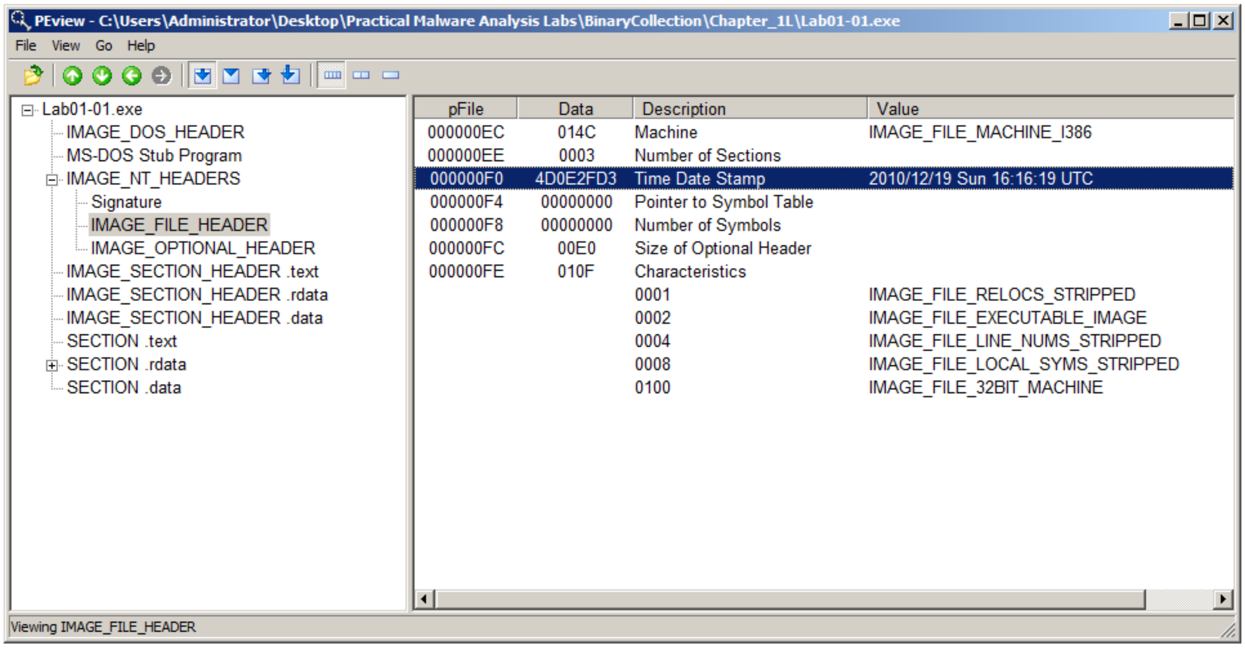
Anti-Virus Results

Updated 6 months ago - Click to Refresh

CrowdStrike Falcon
Static Analysis and ML
Malicious (100%)

MetaDefender
Multi Scan Analysis
Malicious (16/24)

Using PEView for Lab01-01.exe

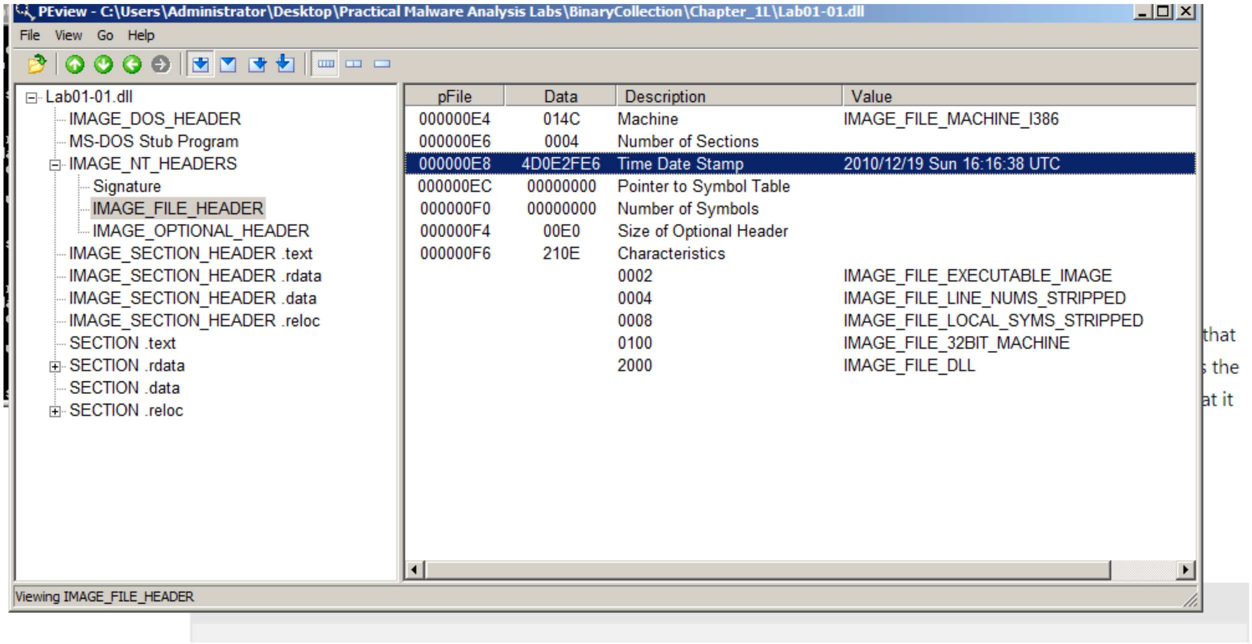

PEview - C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L\Lab01-01.exe
File View Go Help

```
⊟ Lab01-01.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
    SECTION .text
  ⊞ SECTION .rdata
    SECTION .data
```

pFile	Data	Description	Value
000000EC	014C	Machine	IMAGE_FILE_MACHINE_I386
000000EE	0003	Number of Sections	
000000F0	4D0E2FD3	Time Date Stamp	2010/12/19 Sun 16:16:19 UTC
000000F4	00000000	Pointer to Symbol Table	
000000F8	00000000	Number of Symbols	
000000FC	00E0	Size of Optional Header	
000000FE	010F	Characteristics	
		0001	IMAGE_FILE_RELOCS_STRIPPED
		0002	IMAGE_FILE_EXECUTABLE_IMAGE
		0004	IMAGE_FILE_LINE_NUMS_STRIPPED
		0008	IMAGE_FILE_LOCAL_SYMS_STRIPPED
		0100	IMAGE_FILE_32BIT_MACHINE

Viewing IMAGE_FILE_HEADER

Lab01-01.dll

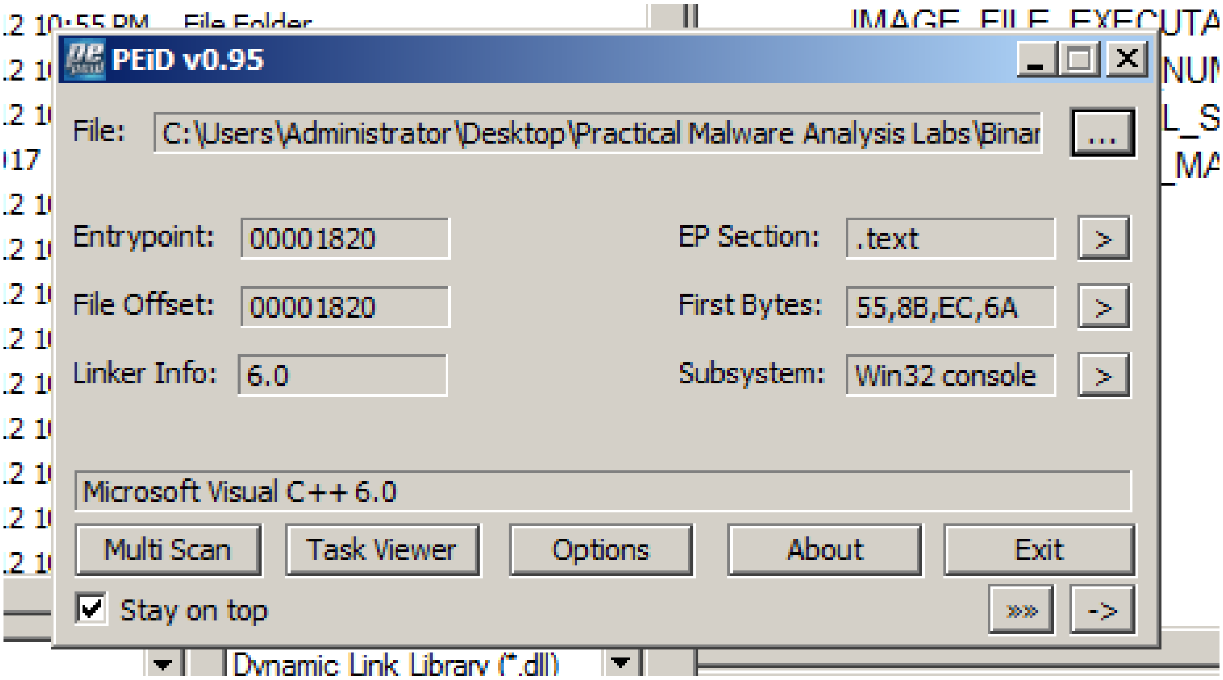

PEview - C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L\Lab01-01.dll
File View Go Help
that
the
at it

```
⊟ Lab01-01.dll
    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 .reloc
    SECTION .text
  ⊞ SECTION .rdata
    SECTION .data
  ⊞ SECTION .reloc
```

pFile	Data	Description	Value
000000E4	014C	Machine	IMAGE_FILE_MACHINE_I386
000000E6	0004	Number of Sections	
000000E8	4D0E2FE6	Time Date Stamp	2010/12/19 Sun 16:16:38 UTC
000000EC	00000000	Pointer to Symbol Table	
000000F0	00000000	Number of Symbols	
000000F4	00E0	Size of Optional Header	
000000F6	210E	Characteristics	
		0002	IMAGE_FILE_EXECUTABLE_IMAGE
		0004	IMAGE_FILE_LINE_NUMS_STRIPPED
		0008	IMAGE_FILE_LOCAL_SYMS_STRIPPED
		0100	IMAGE_FILE_32BIT_MACHINE
		2000	IMAGE_FILE_DLL

Viewing IMAGE_FILE_HEADER

Using PEiD for Lab01-01.exe



PEiD v0.95

File: C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\Binar

Entrypoint: 00001820

File Offset: 00001820

Linker Info: 6.0

EP Section: .text

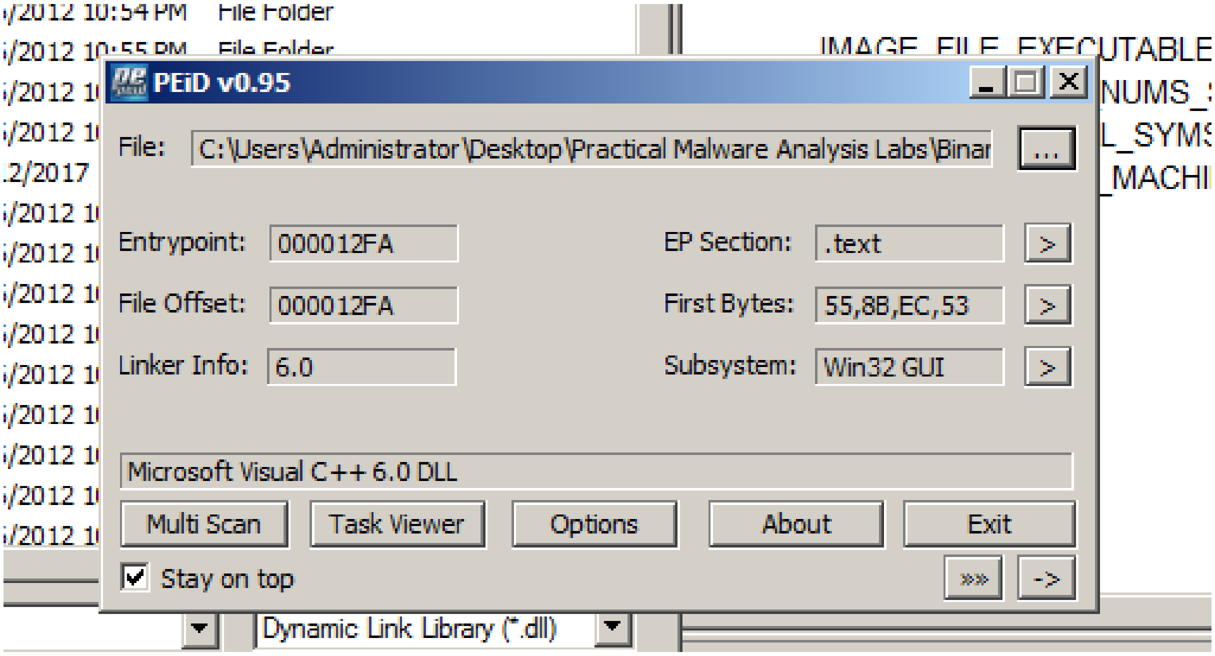
First Bytes: 55,8B,EC,6A

Subsystem: Win32 console

Microsoft Visual C++ 6.0

☑ Stay on top

Lab01-01.dll



PEiD v0.95

File: C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\Binar

Entrypoint: 000012FA

File Offset: 000012FA

Linker Info: 6.0

EP Section: .text

First Bytes: 55,8B,EC,53

Subsystem: Win32 GUI

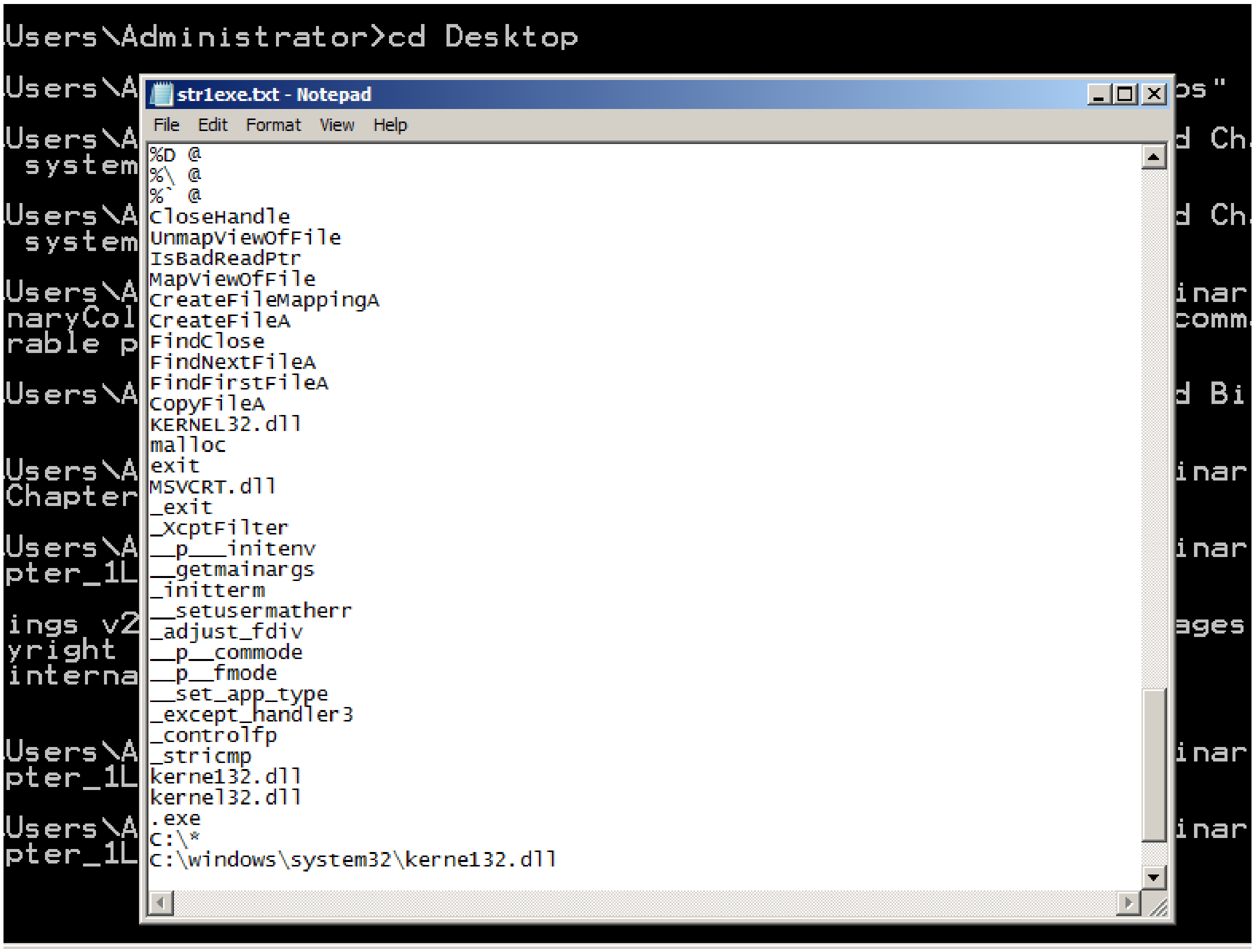
Microsoft Visual C++ 6.0 DLL

☑ Stay on top

Using Strings

strings Lab01-01.exe > str1exe.txt

notepad str1exe.txt

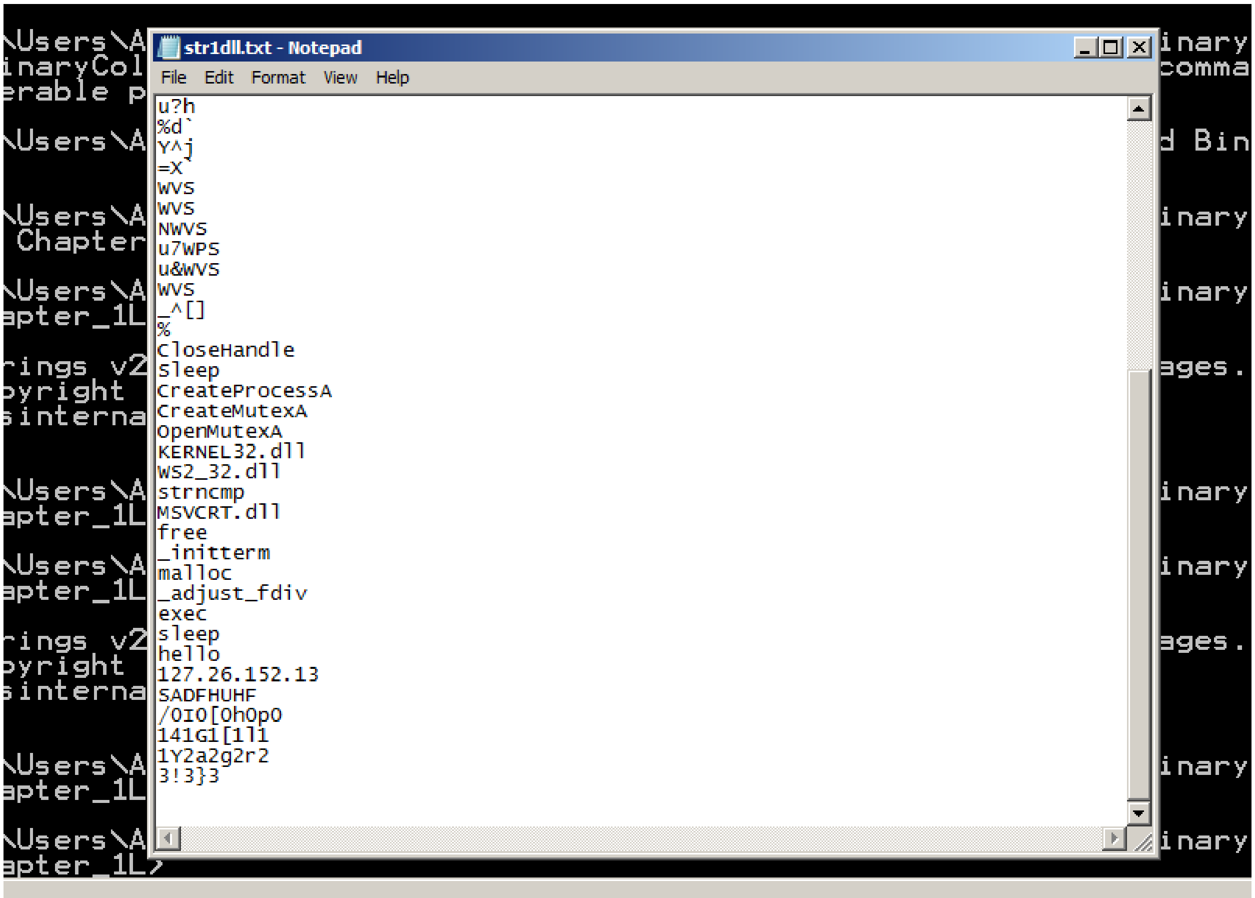


```
Users\Administrator>cd Desktop
```

```
%D @
%\ @
%` @
CloseHandle
UnmapViewOfFile
IsBadReadPtr
MapViewOfFile
CreateFileMappingA
CreateFileA
FindClose
FindNextFileA
FindFirstFileA
CopyFileA
KERNEL32.dll
malloc
exit
MSVCRT.dll
_exit
_XcptFilter
__p___initenv
__getmainargs
_initterm
__setusermatherr
_adjust_fdiv
__p__commode
__p__fmode
__set_app_type
_except_handler3
_controlfp
_stricmp
kerne132.dll
kernel32.dll
.exe
C:\*
C:\windows\system32\kerne132.dll
```

strings Lab01-01.dll > str1dll.txt

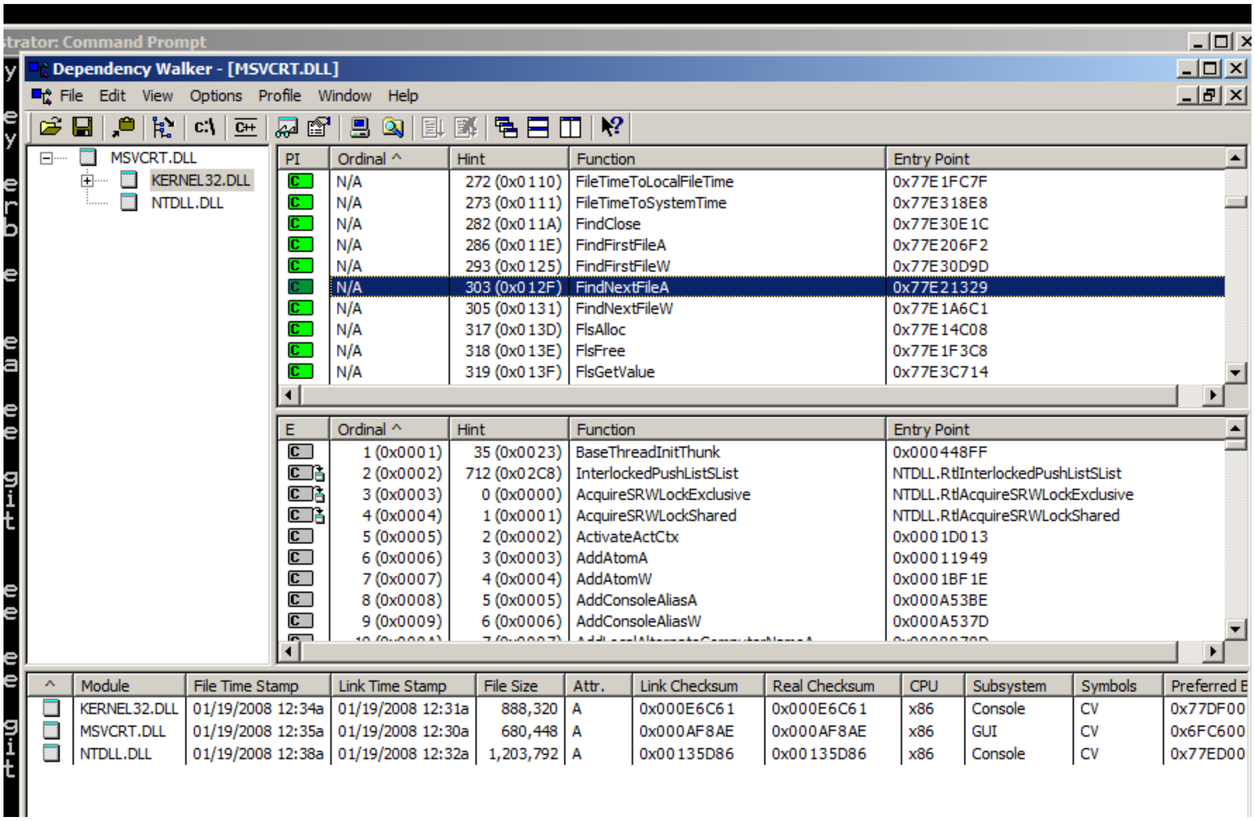
notepad str1dll.txt



```
u?h
%d`
Y^j
=X`
WVS
WVS
NWVS
u7WPS
u&WVS
WVS
_^[]
%
CloseHandle
Sleep
CreateProcessA
CreateMutexA
OpenMutexA
KERNEL32.dll
WS2_32.dll
strncmp
MSVCRT.dll
free
_initterm
malloc
_adjust_fdiv
exec
sleep
hello
127.26.152.13
SADFHUHF
/0I0[0h0p0
141G1[1l1
1Y2a2g2r2
3!3}3
```

Using Dependency Walker

Turn in the image showing your analysis of Lab01-01.exe as shown below. In the "PI^" section (Parent Import), you should see FindNextFileA and FindFirstFileA as shown below.



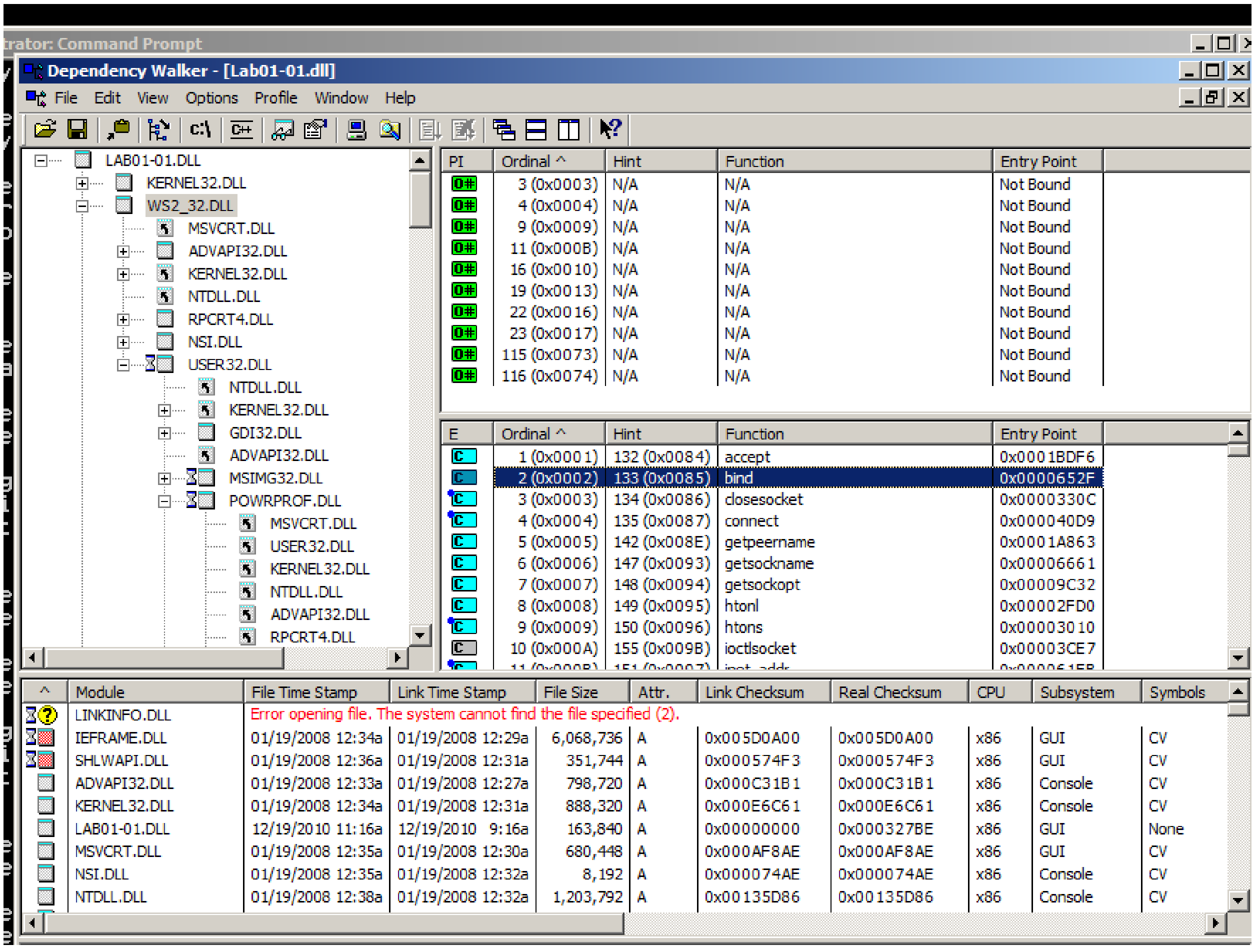
trator: Command Prompt
Dependency Walker - [MSVCRT.DLL]
File Edit View Options Profile Window Help
MSVCRT.DLL
KERNEL32.DLL
NTDLL.DLL

PI	Ordinal ^	Hint	Function	Entry Point
C	N/A	272 (0x0110)	FileTimeToLocalFileTime	0x77E1FC7F
C	N/A	273 (0x0111)	FileTimeToSystemTime	0x77E318E8
C	N/A	282 (0x011A)	FindClose	0x77E30E1C
C	N/A	286 (0x011E)	FindFirstFileA	0x77E206F2
C	N/A	293 (0x0125)	FindFirstFileW	0x77E30D9D
C	N/A	303 (0x012F)	FindNextFileA	0x77E21329
C	N/A	305 (0x0131)	FindNextFileW	0x77E1A6C1
C	N/A	317 (0x013D)	FlsAlloc	0x77E14C08
C	N/A	318 (0x013E)	FlsFree	0x77E1F3C8
C	N/A	319 (0x013F)	FlsGetValue	0x77E3C714

E	Ordinal ^	Hint	Function	Entry Point
C	1 (0x0001)	35 (0x0023)	BaseThreadInitThunk	0x000448FF
C	2 (0x0002)	712 (0x02C8)	InterlockedPushListSList	NTDLL.RtlInterlockedPushListSList
C	3 (0x0003)	0 (0x0000)	AcquireSRWLockExclusive	NTDLL.RtlAcquireSRWLockExclusive
C	4 (0x0004)	1 (0x0001)	AcquireSRWLockShared	NTDLL.RtlAcquireSRWLockShared
C	5 (0x0005)	2 (0x0002)	ActivateActCtx	0x0001D013
C	6 (0x0006)	3 (0x0003)	AddAtomA	0x00011949
C	7 (0x0007)	4 (0x0004)	AddAtomW	0x0001BF1E
C	8 (0x0008)	5 (0x0005)	AddConsoleAliasA	0x000A53BE
C	9 (0x0009)	6 (0x0006)	AddConsoleAliasW	0x000A537D

^	Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred E
	KERNEL32.DLL	01/19/2008 12:34a	01/19/2008 12:31a	888,320	A	0x000E6C61	0x000E6C61	x86	Console	CV	0x77DF00
	MSVCRT.DLL	01/19/2008 12:35a	01/19/2008 12:30a	680,448	A	0x000AF8AE	0x000AF8AE	x86	GUI	CV	0x6FC600
	NTDLL.DLL	01/19/2008 12:38a	01/19/2008 12:32a	1,203,792	A	0x00135D86	0x00135D86	x86	Console	CV	0x77ED00

Open Lab01-01.dll in Dependency Walker. Notice that it imports functions from "WS2_32.DLL". WS2_32.DLL has networking functions. The right center pane shows function names that perform networking tasks, such as "bind", "closesocket", and "connect", as shown below.



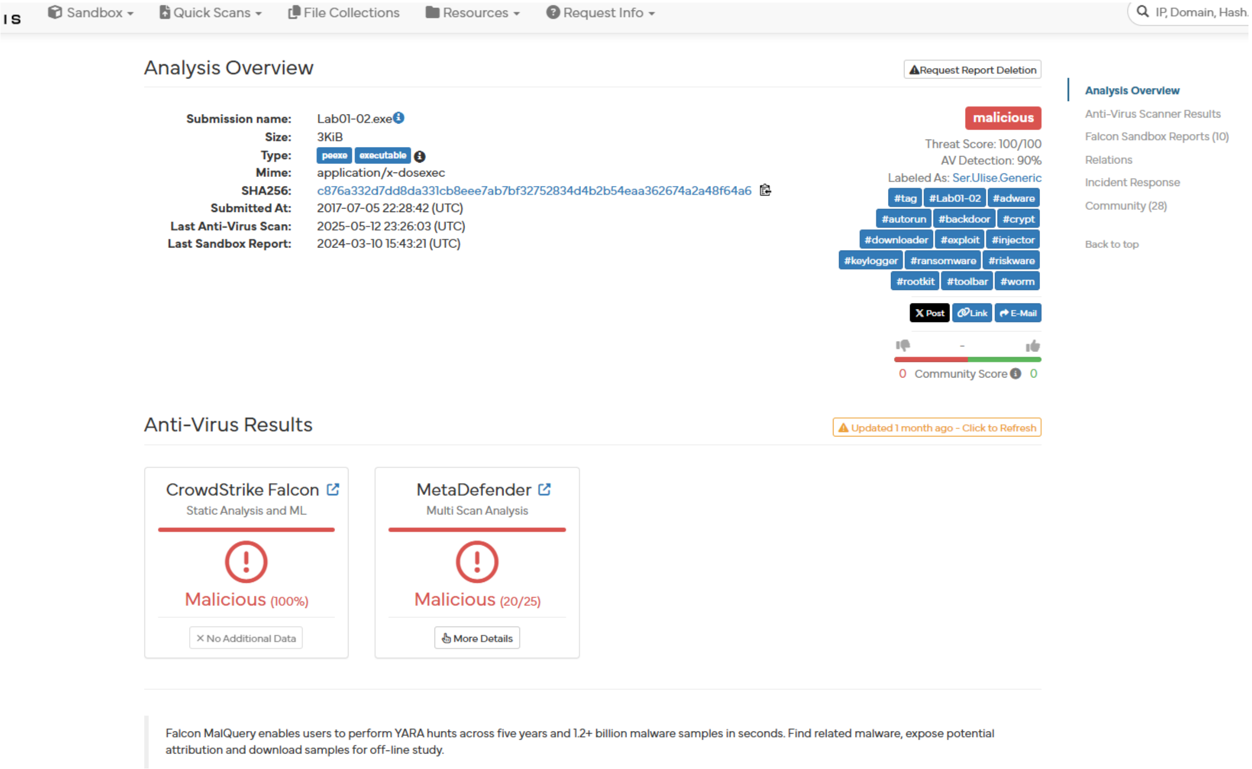
```
LAB01-01.DLL
    KERNEL32.DLL
    WS2_32.DLL
        MSVCRT.DLL
        ADVAPI32.DLL
        KERNEL32.DLL
        NTDLL.DLL
        RPCRT4.DLL
        NSI.DLL
        USER32.DLL
            NTDLL.DLL
            KERNEL32.DLL
            GDI32.DLL
            ADVAPI32.DLL
            MSIMG32.DLL
            POWRPROF.DLL
                MSVCRT.DLL
                USER32.DLL
                KERNEL32.DLL
                NTDLL.DLL
                ADVAPI32.DLL
                RPCRT4.DLL
```

PI	Ordinal ^	Hint	Function	Entry Point
0#	3 (0x0003)	N/A	N/A	Not Bound
0#	4 (0x0004)	N/A	N/A	Not Bound
0#	9 (0x0009)	N/A	N/A	Not Bound
0#	11 (0x000B)	N/A	N/A	Not Bound
0#	16 (0x0010)	N/A	N/A	Not Bound
0#	19 (0x0013)	N/A	N/A	Not Bound
0#	22 (0x0016)	N/A	N/A	Not Bound
0#	23 (0x0017)	N/A	N/A	Not Bound
0#	115 (0x0073)	N/A	N/A	Not Bound
0#	116 (0x0074)	N/A	N/A	Not Bound

E	Ordinal ^	Hint	Function	Entry Point
C	1 (0x0001)	132 (0x0084)	accept	0x0001BDF6
C	2 (0x0002)	133 (0x0085)	bind	0x0000652F
C	3 (0x0003)	134 (0x0086)	closesocket	0x0000330C
C	4 (0x0004)	135 (0x0087)	connect	0x000040D9
C	5 (0x0005)	142 (0x008E)	getpeername	0x0001A863
C	6 (0x0006)	147 (0x0093)	getsockname	0x00006661
C	7 (0x0007)	148 (0x0094)	getsockopt	0x00009C32
C	8 (0x0008)	149 (0x0095)	htonl	0x00002FD0
C	9 (0x0009)	150 (0x0096)	htons	0x00003010
C	10 (0x000A)	155 (0x009B)	ioctlsocket	0x00003CE7

^	Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols
?	LINKINFO.DLL	Error opening file. The system cannot find the file specified (2).								
	IEFRAME.DLL	01/19/2008 12:34a	01/19/2008 12:29a	6,068,736	A	0x005D0A00	0x005D0A00	x86	GUI	CV
	SHLWAPI.DLL	01/19/2008 12:36a	01/19/2008 12:31a	351,744	A	0x000574F3	0x000574F3	x86	GUI	CV
	ADVAPI32.DLL	01/19/2008 12:33a	01/19/2008 12:27a	798,720	A	0x000C31B1	0x000C31B1	x86	Console	CV
	KERNEL32.DLL	01/19/2008 12:34a	01/19/2008 12:31a	888,320	A	0x000E6C61	0x000E6C61	x86	Console	CV
	LAB01-01.DLL	12/19/2010 11:16a	12/19/2010 9:16a	163,840	A	0x00000000	0x000327BE	x86	GUI	None
	MSVCRT.DLL	01/19/2008 12:35a	01/19/2008 12:30a	680,448	A	0x000AF8AE	0x000AF8AE	x86	GUI	CV
	NSI.DLL	01/19/2008 12:35a	01/19/2008 12:32a	8,192	A	0x000074AE	0x000074AE	x86	Console	CV
	NTDLL.DLL	01/19/2008 12:38a	01/19/2008 12:32a	1,203,792	A	0x00135D86	0x00135D86	x86	Console	CV

b. Analyzing Lab01-02.exe



Analysis Overview

Submission name:	Lab01-02.exe
Size:	3KiB
Type:	peexe executable
Mime:	application/x-dosexec
SHA256:	c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6
Submitted At:	2017-07-05 22:28:42 (UTC)
Last Anti-Virus Scan:	2025-05-12 23:26:03 (UTC)
Last Sandbox Report:	2024-03-10 15:43:21 (UTC)

malicious

Threat Score: 100/100
AV Detection: 90%
Labeled As: Ser.Ulise.Generic

#tag #Lab01-02 #adware #autorun #backdoor #crypt #downloader #exploit #injector #keylogger #ransomware #riskware #rootkit #toolbar #worm

Anti-Virus Results

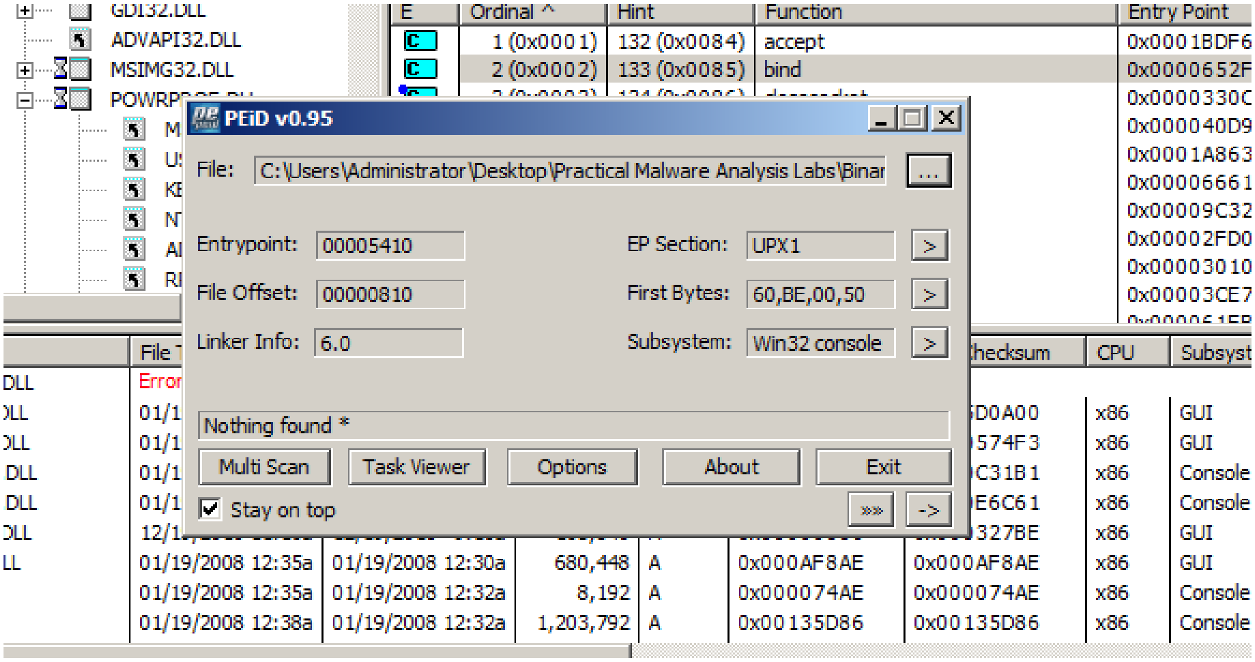
CrowdStrike Falcon
Static Analysis and ML
Malicious (100%)

MetaDefender
Multi Scan Analysis
Malicious (20/25)

Falcon MalQuery enables users to perform YARA hunts across five years and 1.2+ billion malware samples in seconds. Find related malware, expose potential attribution and download samples for off-line study.

Unpacking the File

Run PEiD on the file. It shows that the file is packed with UPX, as shown in the "EP Section" below.



E	Ordinal ^	Hint	Function	Entry Point
C	1 (0x0001)	132 (0x0084)	accept	0x0001BDF6
C	2 (0x0002)	133 (0x0085)	bind	0x0000652F
				0x0000330C
				0x000040D9
				0x0001A863
				0x00006661
				0x00009C32
				0x00002FD0
				0x00003010
				0x00003CE7

File: C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\Binar

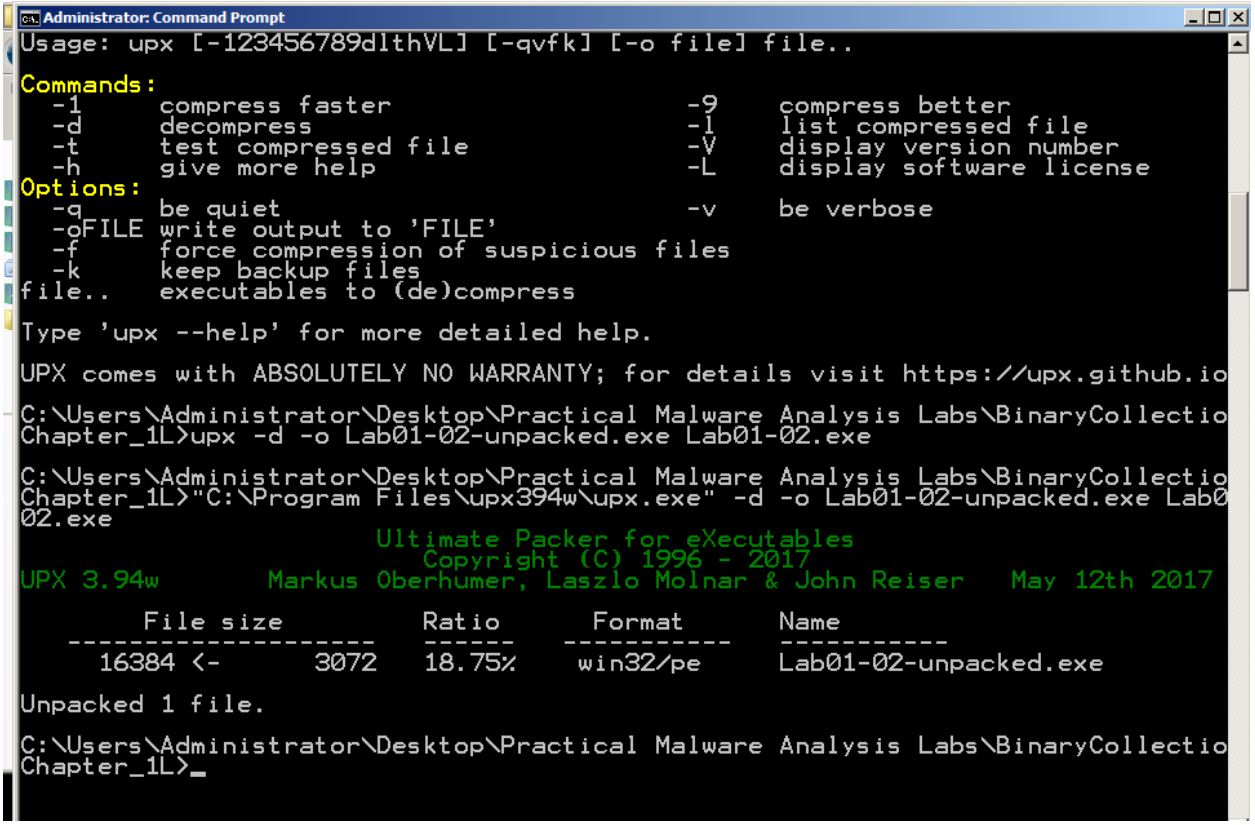
Entrypoint: 00005410
EP Section: UPX1
File Offset: 00000810
First Bytes: 60,BE,00,50
Linker Info: 6.0
Subsystem: Win32 console

Nothing found *

☑ Stay on top

	File T					hecksum	CPU	Subsyst
DLL	Error							
DLL	01/1					D0A00	x86	GUI
DLL	01/1					574F3	x86	GUI
DLL	01/1					C31B1	x86	Console
DLL	01/1					E6C61	x86	Console
DLL	12/1					327BE	x86	GUI
LL	01/19/2008 12:35a	01/19/2008 12:30a	680,448	A	0x000AF8AE	0x000AF8AE	x86	GUI
	01/19/2008 12:35a	01/19/2008 12:32a	8,192	A	0x000074AE	0x000074AE	x86	Console
	01/19/2008 12:38a	01/19/2008 12:32a	1,203,792	A	0x00135D86	0x00135D86	x86	Console

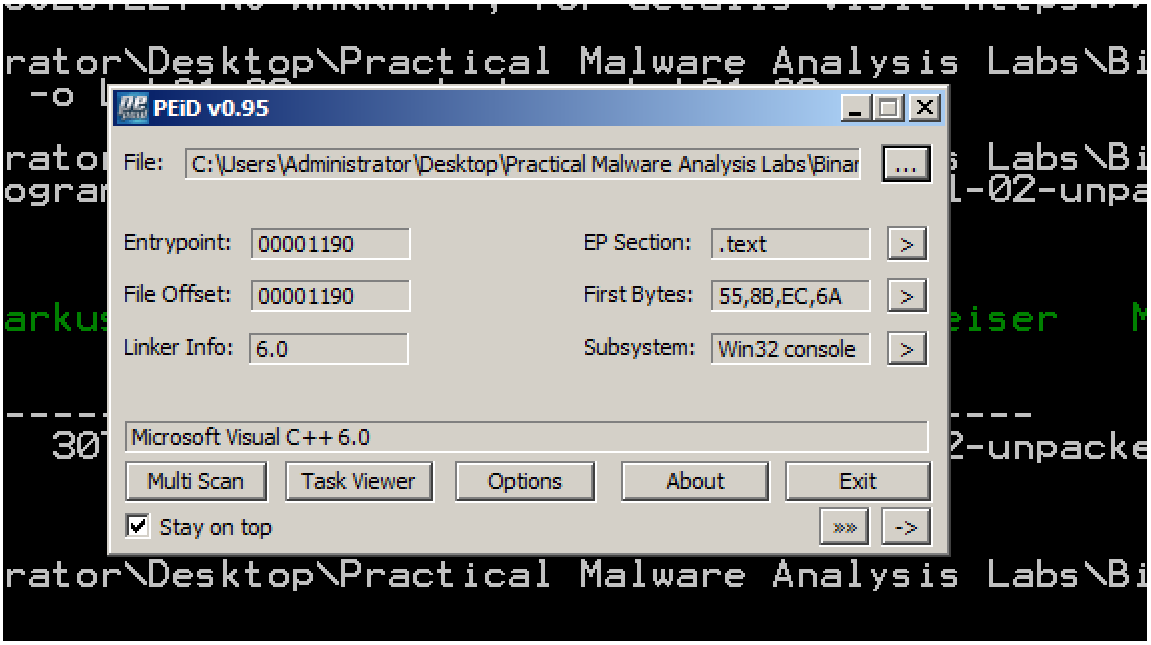
Execute this command to unpack the file: UPX -d -o Lab01-02-unpacked.exe Lab01-02.exe



Administrator: Command Prompt

```
Usage: upx [-123456789dlthVL] [-qvfk] [-o file] file..

Commands:
  -1     compress faster                   -9    compress better
  -d     decompress                        -l    list compressed file
  -t     test compressed file              -V    display version number
  -h     give more help                    -L    display software license
Options:
  -q     be quiet                          -v    be verbose
  -oFILE write output to 'FILE'
  -f     force compression of suspicious files
  -k     keep backup files
file..   executables to (de)compress

Type 'upx --help' for more detailed help.

UPX comes with ABSOLUTELY NO WARRANTY; for details visit https://upx.github.io

C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollectio
Chapter_1L>upx -d -o Lab01-02-unpacked.exe Lab01-02.exe

C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollectio
Chapter_1L>"C:\Program Files\upx394w\upx.exe" -d -o Lab01-02-unpacked.exe Lab0
02.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2017
UPX 3.94w       Markus Oberhumer, Laszlo Molnar & John Reiser   May 12th 2017

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
     16384 <-      3072   18.75%    win32/pe     Lab01-02-unpacked.exe

Unpacked 1 file.

C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollectio
Chapter_1L>_
```

Analyze the unpacked file with PEiD. It now is regognized as a "Microsoft Visual C++ 6.0" file, as shown below.



PEiD v0.95

File: C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\Binar

Entrypoint: 00001190

File Offset: 00001190

Linker Info: 6.0

EP Section: .text

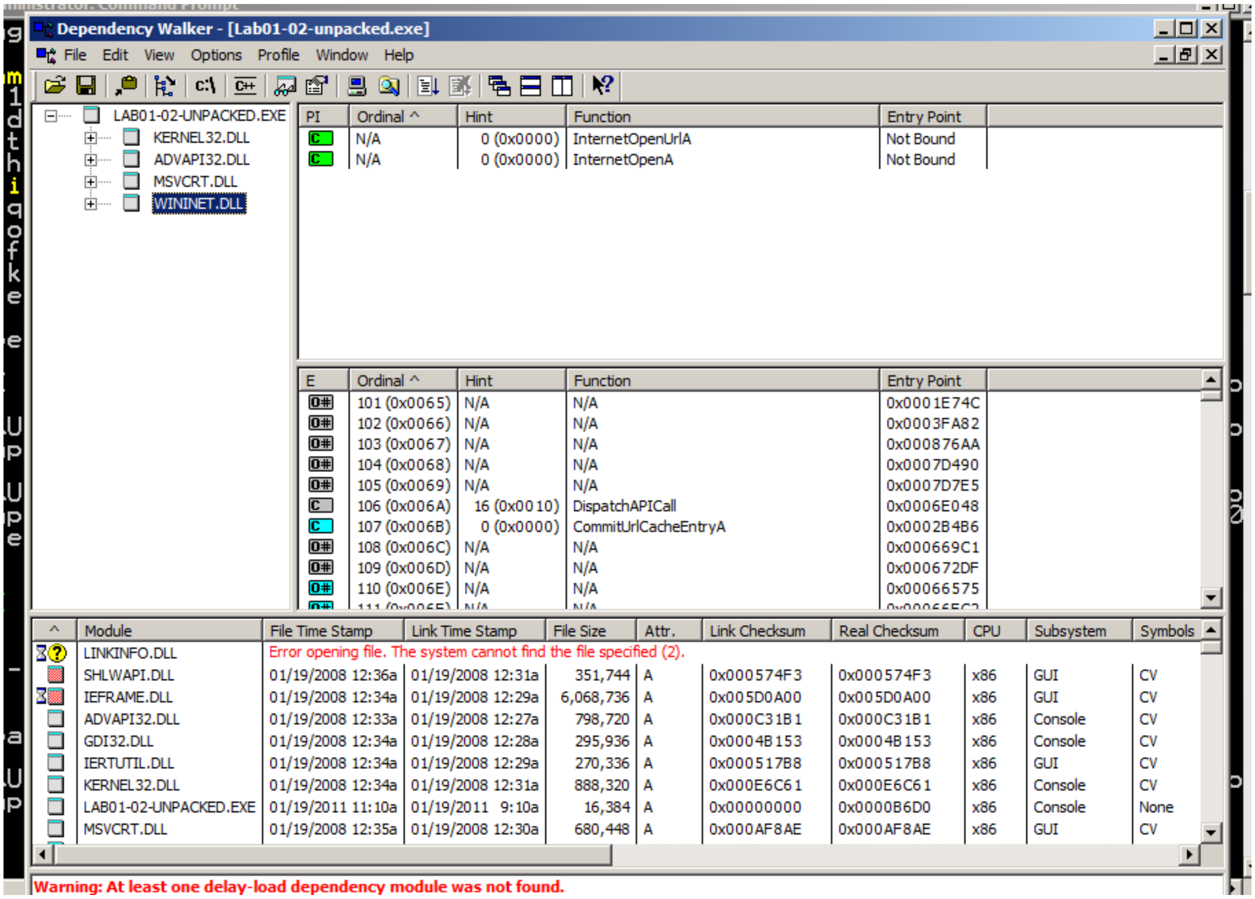
First Bytes: 55,8B,EC,6A

Subsystem: Win32 console

Microsoft Visual C++ 6.0

☑ Stay on top

Turn in the image showing the two functions InternetOpenUrlA and InternetOpenA as shown in the upper right pane of the image below



LAB01-02-UNPACKED.EXE
- KERNEL32.DLL
- ADVAPI32.DLL
- MSVCRT.DLL
- WININET.DLL

PI	Ordinal ^	Hint	Function	Entry Point
C	N/A	0 (0x0000)	InternetOpenUrlA	Not Bound
C	N/A	0 (0x0000)	InternetOpenA	Not Bound

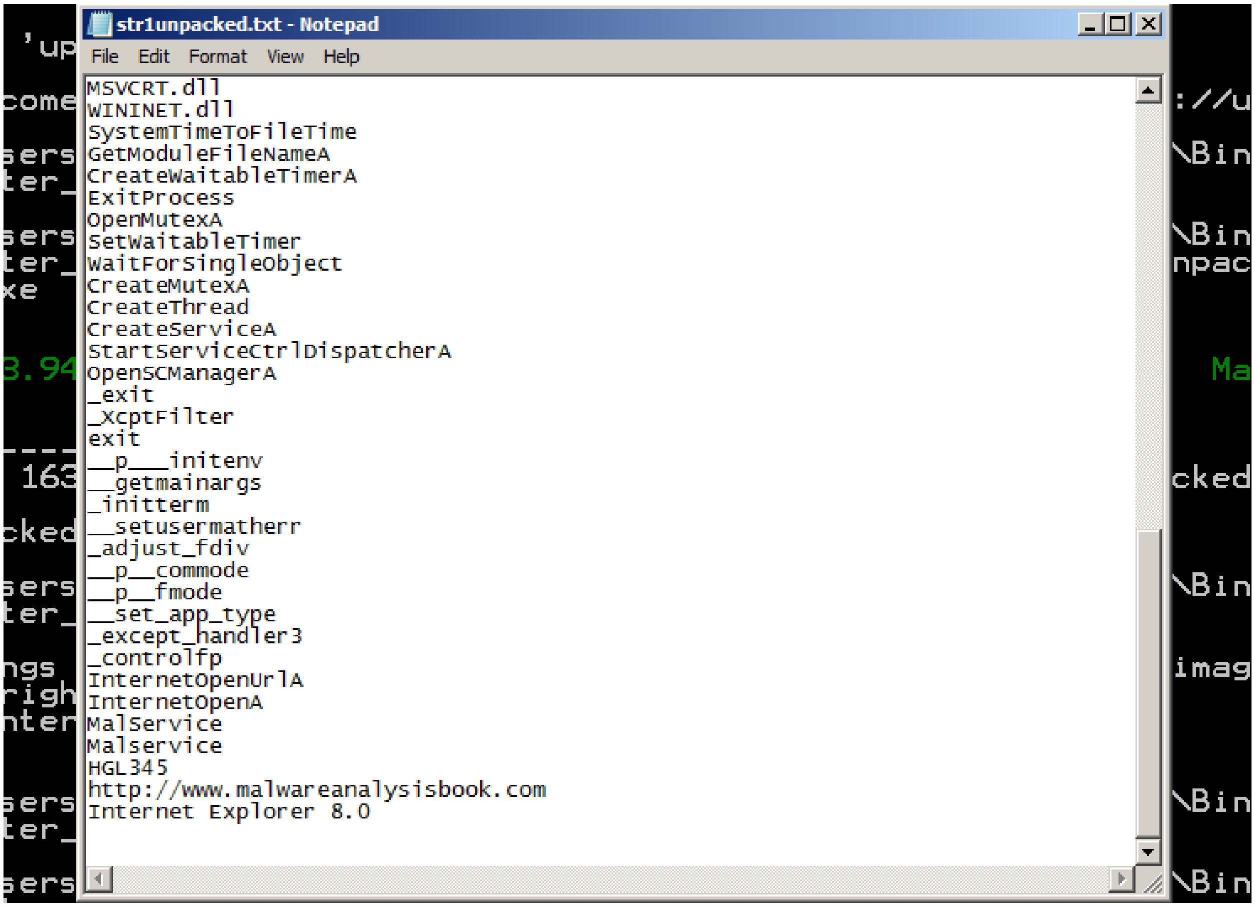
E	Ordinal ^	Hint	Function	Entry Point
O#	101 (0x0065)	N/A	N/A	0x0001E74C
O#	102 (0x0066)	N/A	N/A	0x0003FA82
O#	103 (0x0067)	N/A	N/A	0x000876AA
O#	104 (0x0068)	N/A	N/A	0x0007D490
O#	105 (0x0069)	N/A	N/A	0x0007D7E5
C	106 (0x006A)	16 (0x0010)	DispatchAPICall	0x0006E048
C	107 (0x006B)	0 (0x0000)	CommitUrlCacheEntryA	0x0002B4B6
O#	108 (0x006C)	N/A	N/A	0x000669C1
O#	109 (0x006D)	N/A	N/A	0x000672DF
O#	110 (0x006E)	N/A	N/A	0x00066575

^	Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols
?	LINKINFO.DLL	Error opening file. The system cannot find the file specified (2).								
	SHLWAPI.DLL	01/19/2008 12:36a	01/19/2008 12:31a	351,744	A	0x000574F3	0x000574F3	x86	GUI	CV
	IEFRAME.DLL	01/19/2008 12:34a	01/19/2008 12:29a	6,068,736	A	0x005D0A00	0x005D0A00	x86	GUI	CV
	ADVAPI32.DLL	01/19/2008 12:33a	01/19/2008 12:27a	798,720	A	0x000C31B1	0x000C31B1	x86	Console	CV
	GDI32.DLL	01/19/2008 12:34a	01/19/2008 12:28a	295,936	A	0x0004B153	0x0004B153	x86	Console	CV
	IERTUTIL.DLL	01/19/2008 12:34a	01/19/2008 12:29a	270,336	A	0x000517B8	0x000517B8	x86	GUI	CV
	KERNEL32.DLL	01/19/2008 12:34a	01/19/2008 12:31a	888,320	A	0x000E6C61	0x000E6C61	x86	Console	CV
	LAB01-02-UNPACKED.EXE	01/19/2011 11:10a	01/19/2011 9:10a	16,384	A	0x00000000	0x0000B6D0	x86	Console	None
	MSVCRT.DLL	01/19/2008 12:35a	01/19/2008 12:30a	680,448	A	0x000AF8AE	0x000AF8AE	x86	GUI	CV

Warning: At least one delay-load dependency module was not found.

Using Strings

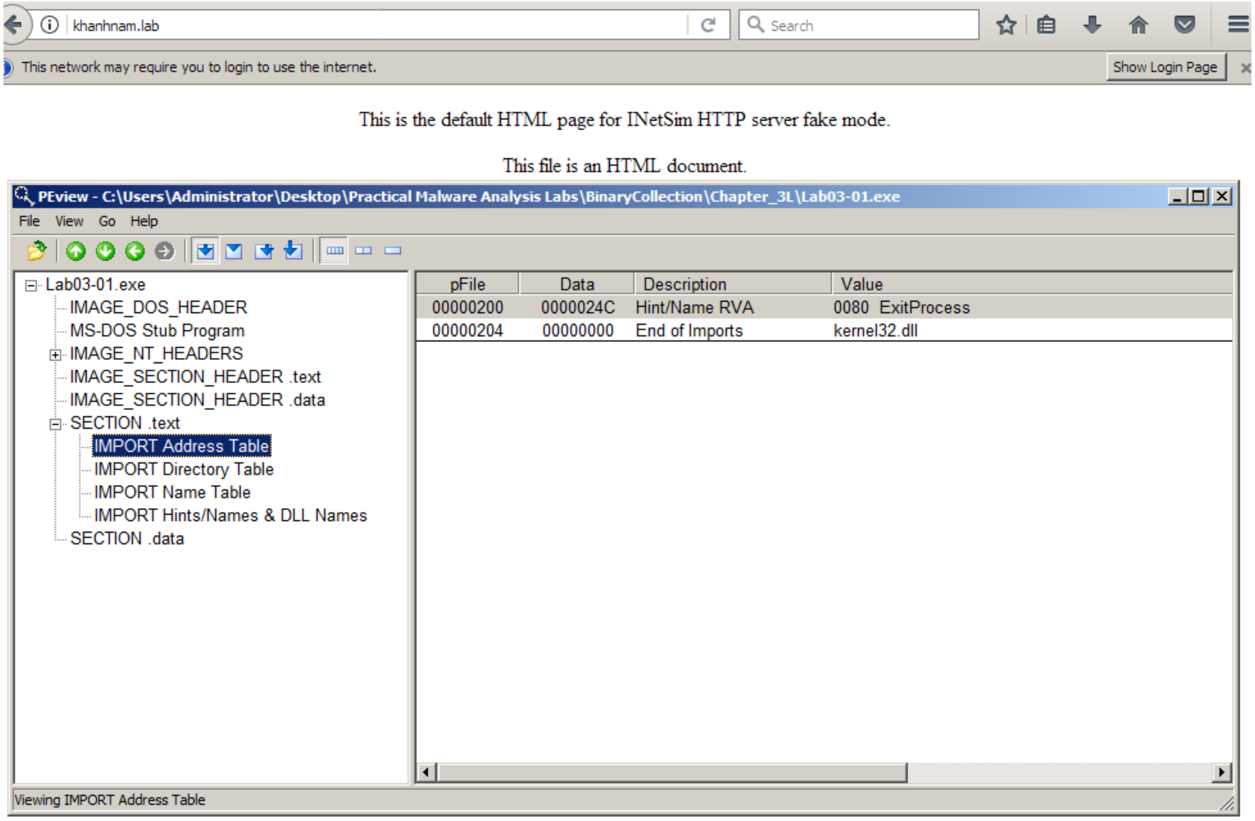
Strings Find the strings in the unpacked file. You should see MalService and http://www.malwareanalysisbook.com as shown below. These suggest that infected machines will connect to http://www.malwareanalysisbook.com and will show a running service named MalService.



```
MSVCRT.dll
WININET.dll
SystemTimeToFileTime
GetModuleFileNameA
CreateWaitableTimerA
ExitProcess
OpenMutexA
SetWaitableTimer
WaitForSingleObject
CreateMutexA
CreateThread
CreateServiceA
StartServiceCtrlDispatcherA
OpenSCManagerA
_exit
_XcptFilter
exit
__p___initenv
__getmainargs
_initterm
__setusermatherr
_adjust_fdiv
__p__commode
__p__fmode
__set_app_type
_except_handler3
_controlfp
InternetOpenUrlA
InternetOpenA
MalService
Malservice
HGL345
http://www.malwareanalysisbook.com
Internet Explorer 8.0
```

Part 2: Basic Dynamic Techniques

Using PEview Open Lab03-01.exe in PEview. As shown below, the only DLL imported is kernel32.dll, and the only function imported is ExitProcess. That doesn't tell us much--perhaps this malware is packed and the real imports will come at runtime. Turn in the image showing the imports of Lab03-01.exe as shown below. We will grade it by checking the Data value.


khanhnam.lab
Search
This network may require you to login to use the internet.
Show Login Page
PEview - C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_3L\Lab03-01.exe
File
View
Go
Help

This is the default HTML page for INetSim HTTP server fake mode.

This file is an HTML document.

- Lab03-01.exe
  - IMAGE_DOS_HEADER
  - MS-DOS Stub Program
  - IMAGE_NT_HEADERS
  - IMAGE_SECTION_HEADER .text
  - IMAGE_SECTION_HEADER .data
  - SECTION .text
    - IMPORT Address Table
    - IMPORT Directory Table
    - IMPORT Name Table
    - IMPORT Hints/Names & DLL Names
  - SECTION .data

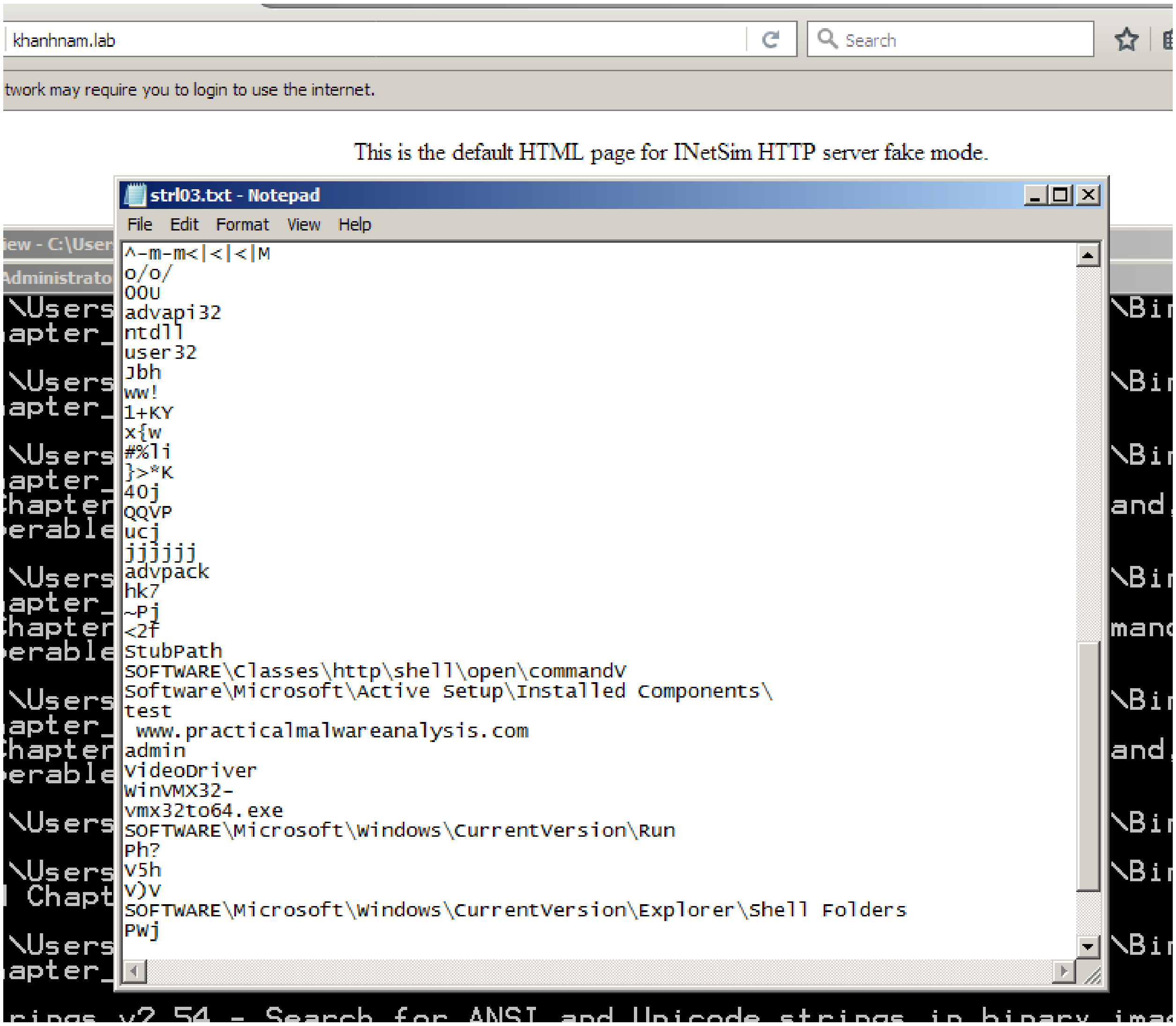
pFile	Data	Description	Value
00000200	0000024C	Hint/Name RVA	0080 ExitProcess
00000204	00000000	End of Imports	kernel32.dll

Viewing IMPORT Address Table

Using Strings

Examine the strings in Lab03-01.exe and find these items, as shown below.
SOFTWARE\Classes\http\shell\open\commandV -- A registry location
www.practicalmalwareanalysis.com -- a URL VideoDriver

These readable strings are surprising--if the malware were packed, the strings would not be readable.

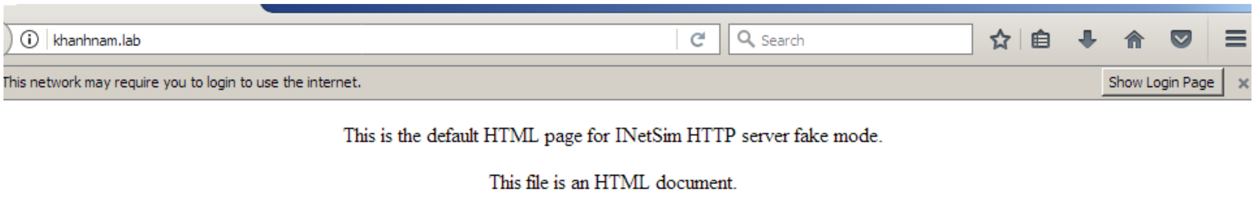

khanhnam.lab
Search
twork may require you to login to use the internet.
This is the default HTML page for INetSim HTTP server fake mode.
strl03.txt - Notepad
File
Edit
Format
View
Help

```
^-m-m<|<|<|M
o/o/
OOU
advapi32
ntdll
user32
Jbh
ww!
1+KY
x{w
#%li
}>*K
40j
QQVP
ucj
jjjjjj
advpack
hk7
~Pj
<2f
StubPath
SOFTWARE\Classes\http\shell\open\commandV
Software\Microsoft\Active Setup\Installed Components\
test
 www.practicalmalwareanalysis.com
admin
VideoDriver
WinVMX32-
vmx32to64.exe
SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Ph?
V5h
V)V
SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
PWj
```

```
rings v2.54 - Search for ANSI and Unicode strings in binary imag
```

Preparing for Dynamic Analysis

Configuring for Inetsim environment

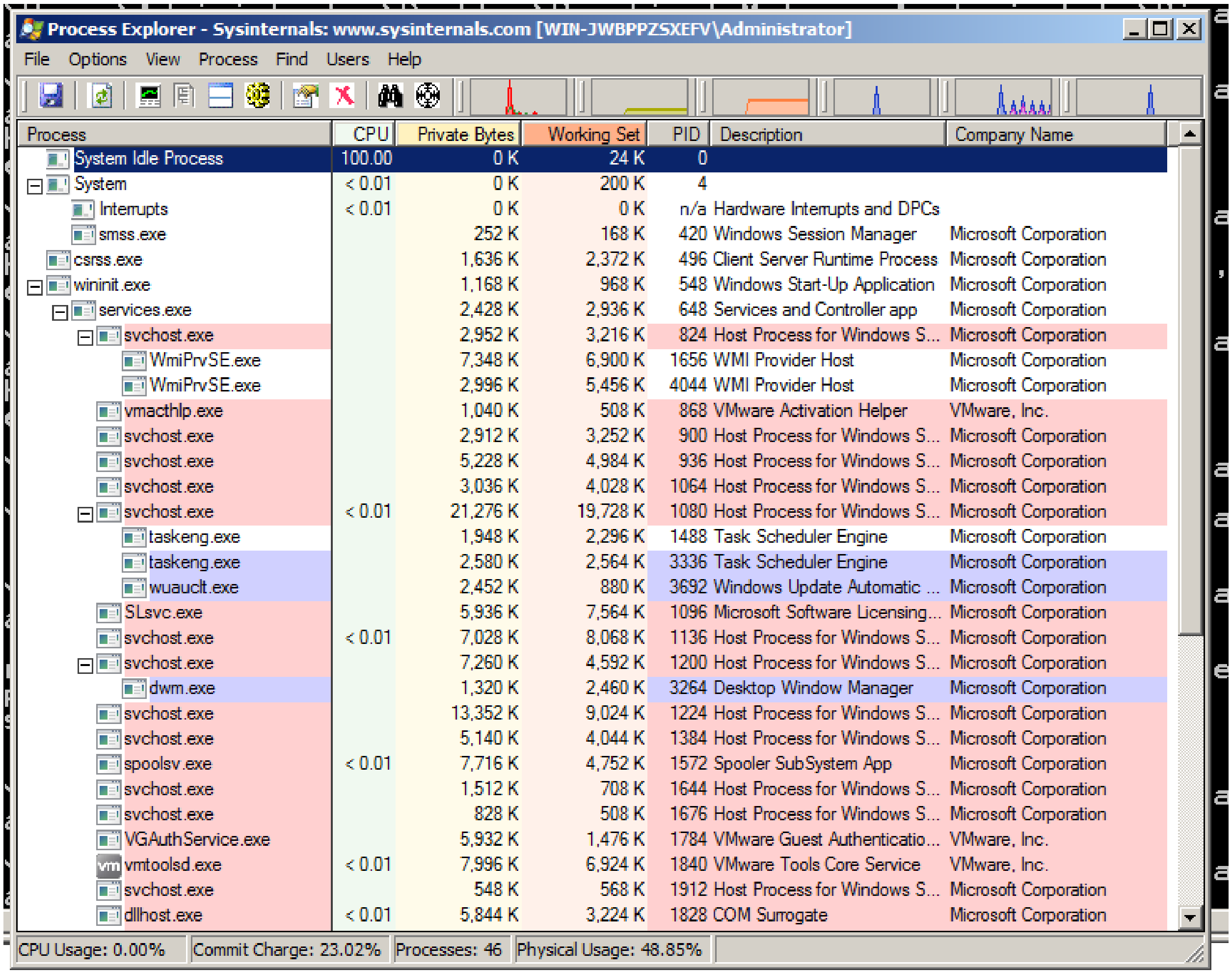


This network may require you to login to use the internet.

This is the default HTML page for INetSim HTTP server fake mode.

This file is an HTML document.

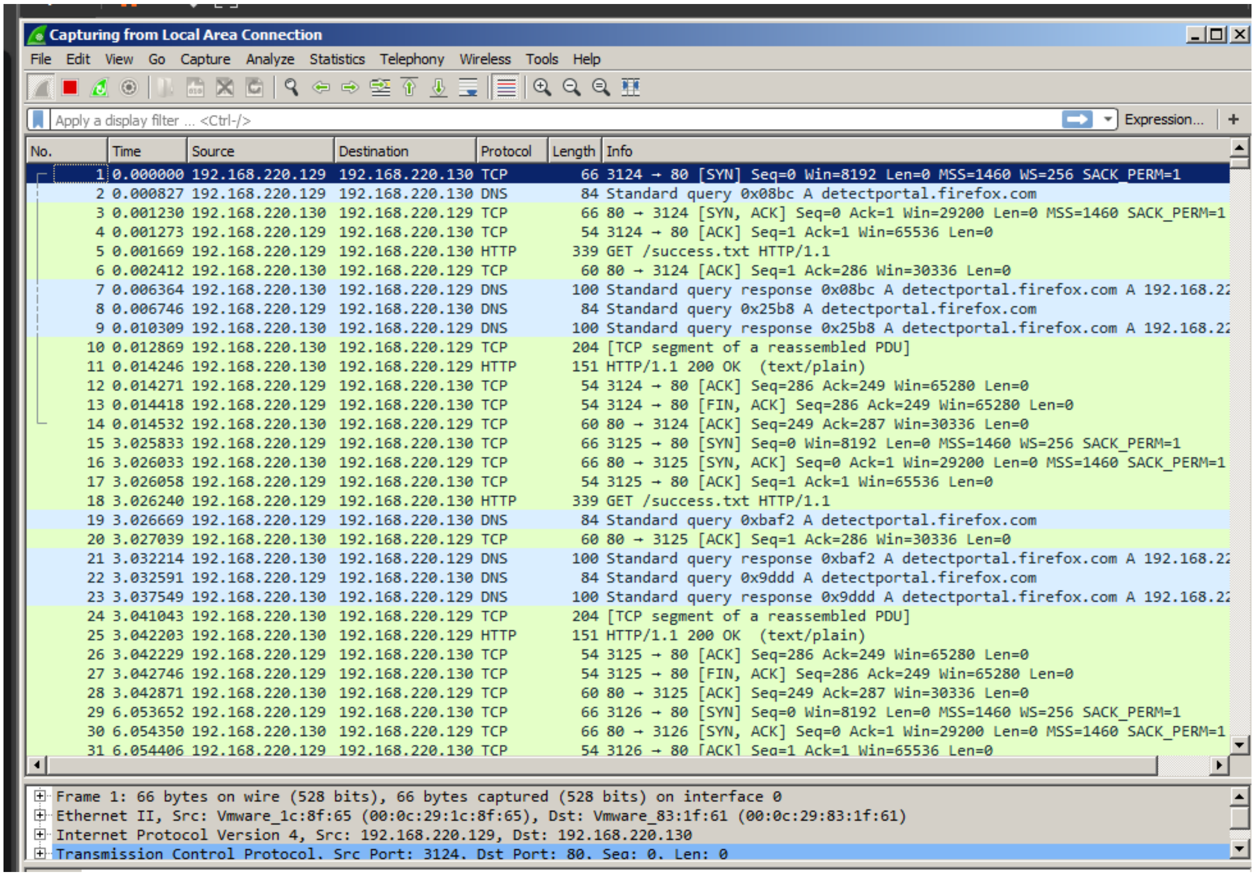
Run Process Explorer


Process Explorer - Sysinternals: www.sysinternals.com [WIN-JWBPPZSXEFV\Administrator]
File
Options
View
Process
Find
Users
Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	100.00	0 K	24 K	0		
System	< 0.01	0 K	200 K	4		
Interrupts	< 0.01	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		252 K	168 K	420	Windows Session Manager	Microsoft Corporation
csrss.exe		1,636 K	2,372 K	496	Client Server Runtime Process	Microsoft Corporation
wininit.exe		1,168 K	968 K	548	Windows Start-Up Application	Microsoft Corporation
services.exe		2,428 K	2,936 K	648	Services and Controller app	Microsoft Corporation
svchost.exe		2,952 K	3,216 K	824	Host Process for Windows S...	Microsoft Corporation
WmiPrvSE.exe		7,348 K	6,900 K	1656	WMI Provider Host	Microsoft Corporation
WmiPrvSE.exe		2,996 K	5,456 K	4044	WMI Provider Host	Microsoft Corporation
vmacthlp.exe		1,040 K	508 K	868	VMware Activation Helper	VMware, Inc.
svchost.exe		2,912 K	3,252 K	900	Host Process for Windows S...	Microsoft Corporation
svchost.exe		5,228 K	4,984 K	936	Host Process for Windows S...	Microsoft Corporation
svchost.exe		3,036 K	4,028 K	1064	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	21,276 K	19,728 K	1080	Host Process for Windows S...	Microsoft Corporation
taskeng.exe		1,948 K	2,296 K	1488	Task Scheduler Engine	Microsoft Corporation
taskeng.exe		2,580 K	2,564 K	3336	Task Scheduler Engine	Microsoft Corporation
wuauclt.exe		2,452 K	880 K	3692	Windows Update Automatic ...	Microsoft Corporation
SLsvc.exe		5,936 K	7,564 K	1096	Microsoft Software Licensing...	Microsoft Corporation
svchost.exe	< 0.01	7,028 K	8,068 K	1136	Host Process for Windows S...	Microsoft Corporation
svchost.exe		7,260 K	4,592 K	1200	Host Process for Windows S...	Microsoft Corporation
dwm.exe		1,320 K	2,460 K	3264	Desktop Window Manager	Microsoft Corporation
svchost.exe		13,352 K	9,024 K	1224	Host Process for Windows S...	Microsoft Corporation
svchost.exe		5,140 K	4,044 K	1384	Host Process for Windows S...	Microsoft Corporation
spoolsv.exe	< 0.01	7,716 K	4,752 K	1572	Spooler SubSystem App	Microsoft Corporation
svchost.exe		1,512 K	708 K	1644	Host Process for Windows S...	Microsoft Corporation
svchost.exe		828 K	508 K	1676	Host Process for Windows S...	Microsoft Corporation
VGAuthService.exe		5,932 K	1,476 K	1784	VMware Guest Authenticatio...	VMware, Inc.
vmtoolsd.exe	< 0.01	7,996 K	6,924 K	1840	VMware Tools Core Service	VMware, Inc.
svchost.exe		548 K	568 K	1912	Host Process for Windows S...	Microsoft Corporation
dllhost.exe	< 0.01	5,844 K	3,224 K	1828	COM Surrogate	Microsoft Corporation

CPU Usage: 0.00% | Commit Charge: 23.02% | Processes: 46 | Physical Usage: 48.85%

Run Wireshark

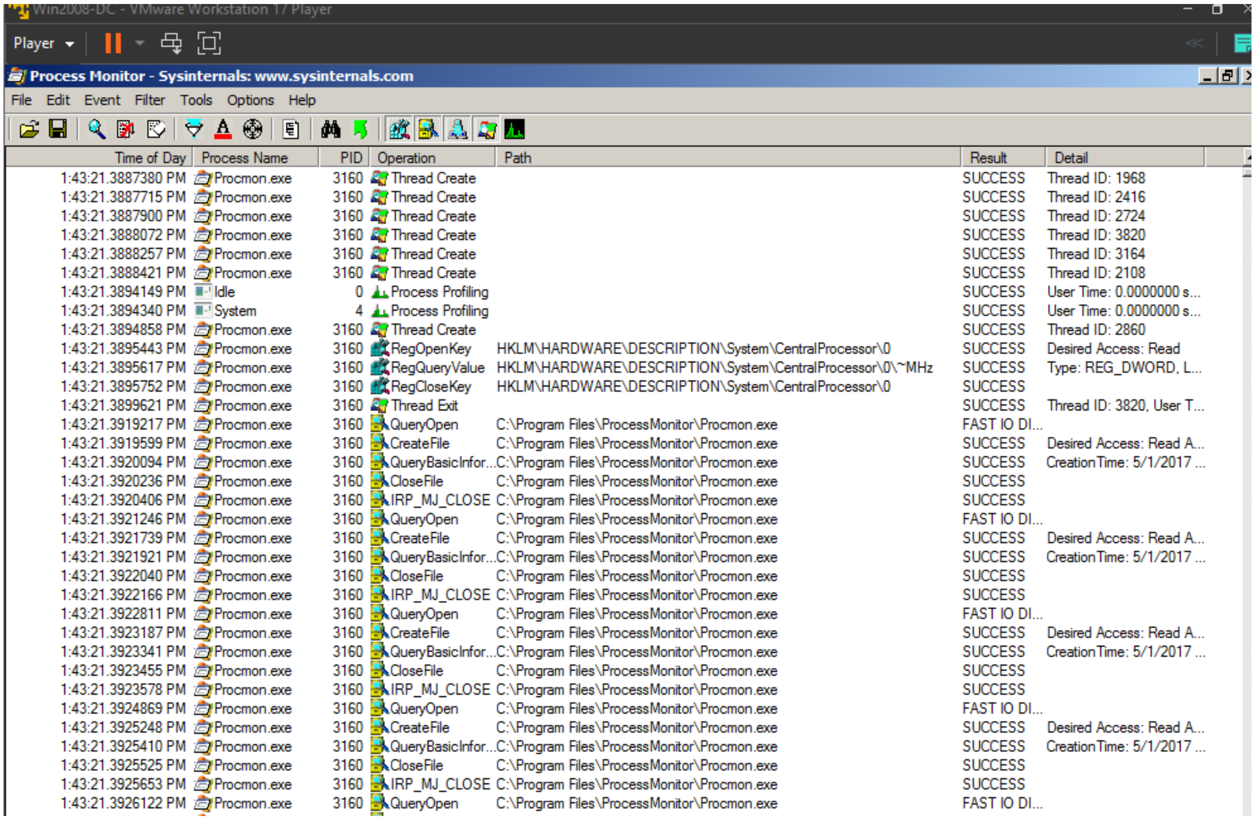


Capturing from Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.   Time     Source          Destination     Protocol Length Info
    1 0.000000 192.168.220.129 192.168.220.130 TCP        66 3124 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
    2 0.000827 192.168.220.129 192.168.220.130 DNS        84 Standard query 0x08bc A detectportal.firefox.com
    3 0.001230 192.168.220.130 192.168.220.129 TCP        66 80 → 3124 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1
    4 0.001273 192.168.220.129 192.168.220.130 TCP        54 3124 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
    5 0.001669 192.168.220.129 192.168.220.130 HTTP      339 GET /success.txt HTTP/1.1
    6 0.002412 192.168.220.130 192.168.220.129 TCP        60 80 → 3124 [ACK] Seq=1 Ack=286 Win=30336 Len=0
    7 0.006364 192.168.220.130 192.168.220.129 DNS       100 Standard query response 0x08bc A detectportal.firefox.com A 192.168.22
    8 0.006746 192.168.220.129 192.168.220.130 DNS        84 Standard query 0x25b8 A detectportal.firefox.com
    9 0.010309 192.168.220.130 192.168.220.129 DNS       100 Standard query response 0x25b8 A detectportal.firefox.com A 192.168.22
   10 0.012869 192.168.220.130 192.168.220.129 TCP       204 [TCP segment of a reassembled PDU]
   11 0.014246 192.168.220.130 192.168.220.129 HTTP      151 HTTP/1.1 200 OK  (text/plain)
   12 0.014271 192.168.220.129 192.168.220.130 TCP        54 3124 → 80 [ACK] Seq=286 Ack=249 Win=65280 Len=0
   13 0.014418 192.168.220.129 192.168.220.130 TCP        54 3124 → 80 [FIN, ACK] Seq=286 Ack=249 Win=65280 Len=0
   14 0.014532 192.168.220.130 192.168.220.129 TCP        60 80 → 3124 [ACK] Seq=249 Ack=287 Win=30336 Len=0
   15 3.025833 192.168.220.129 192.168.220.130 TCP        66 3125 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
   16 3.026033 192.168.220.130 192.168.220.129 TCP        66 80 → 3125 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1
   17 3.026058 192.168.220.129 192.168.220.130 TCP        54 3125 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
   18 3.026240 192.168.220.129 192.168.220.130 HTTP      339 GET /success.txt HTTP/1.1
   19 3.026669 192.168.220.129 192.168.220.130 DNS        84 Standard query 0xbaf2 A detectportal.firefox.com
   20 3.027039 192.168.220.130 192.168.220.129 TCP        60 80 → 3125 [ACK] Seq=1 Ack=286 Win=30336 Len=0
   21 3.032214 192.168.220.130 192.168.220.129 DNS       100 Standard query response 0xbaf2 A detectportal.firefox.com A 192.168.22
   22 3.032591 192.168.220.129 192.168.220.130 DNS        84 Standard query 0x9ddd A detectportal.firefox.com
   23 3.037549 192.168.220.130 192.168.220.129 DNS       100 Standard query response 0x9ddd A detectportal.firefox.com A 192.168.22
   24 3.041043 192.168.220.130 192.168.220.129 TCP       204 [TCP segment of a reassembled PDU]
   25 3.042203 192.168.220.130 192.168.220.129 HTTP      151 HTTP/1.1 200 OK  (text/plain)
   26 3.042229 192.168.220.129 192.168.220.130 TCP        54 3125 → 80 [ACK] Seq=286 Ack=249 Win=65280 Len=0
   27 3.042746 192.168.220.129 192.168.220.130 TCP        54 3125 → 80 [FIN, ACK] Seq=286 Ack=249 Win=65280 Len=0
   28 3.042871 192.168.220.130 192.168.220.129 TCP        60 80 → 3125 [ACK] Seq=249 Ack=287 Win=30336 Len=0
   29 6.053652 192.168.220.129 192.168.220.130 TCP        66 3126 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
   30 6.054350 192.168.220.130 192.168.220.129 TCP        66 80 → 3126 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1
   31 6.054406 192.168.220.129 192.168.220.130 TCP        54 3126 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
```

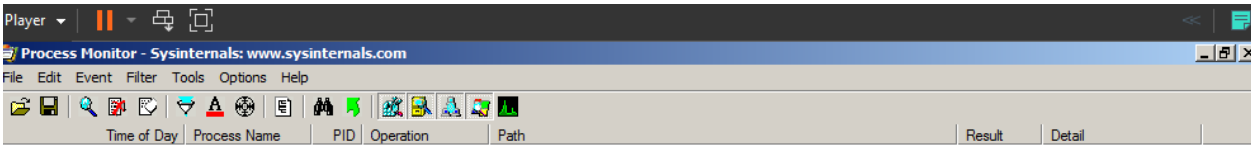
```
⊞ Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
⊞ Ethernet II, Src: Vmware_1c:8f:65 (00:0c:29:1c:8f:65), Dst: Vmware_83:1f:61 (00:0c:29:83:1f:61)
⊞ Internet Protocol Version 4, Src: 192.168.220.129, Dst: 192.168.220.130
⊞ Transmission Control Protocol, Src Port: 3124, Dst Port: 80, Seq: 0, Len: 0
```

Start Process Monitor


Win2008-DC - VMware Workstation 17 Player
Player
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

```
     Time of Day   Process Name    PID  Operation         Path                                                     Result        Detail
1:43:21.3887380 PM Procmon.exe    3160  Thread Create                                                              SUCCESS       Thread ID: 1968
1:43:21.3887715 PM Procmon.exe    3160  Thread Create                                                              SUCCESS       Thread ID: 2416
1:43:21.3887900 PM Procmon.exe    3160  Thread Create                                                              SUCCESS       Thread ID: 2724
1:43:21.3888072 PM Procmon.exe    3160  Thread Create                                                              SUCCESS       Thread ID: 3820
1:43:21.3888257 PM Procmon.exe    3160  Thread Create                                                              SUCCESS       Thread ID: 3164
1:43:21.3888421 PM Procmon.exe    3160  Thread Create                                                              SUCCESS       Thread ID: 2108
1:43:21.3894149 PM Idle              0  Process Profiling                                                          SUCCESS       User Time: 0.0000000 s...
1:43:21.3894340 PM System            4  Process Profiling                                                          SUCCESS       User Time: 0.0000000 s...
1:43:21.3894858 PM Procmon.exe    3160  Thread Create                                                              SUCCESS       Thread ID: 2860
1:43:21.3895443 PM Procmon.exe    3160  RegOpenKey        HKLM\HARDWARE\DESCRIPTION\System\CentralProcessor\0      SUCCESS       Desired Access: Read
1:43:21.3895617 PM Procmon.exe    3160  RegQueryValue     HKLM\HARDWARE\DESCRIPTION\System\CentralProcessor\0\~MHz SUCCESS       Type: REG_DWORD, L...
1:43:21.3895752 PM Procmon.exe    3160  RegCloseKey       HKLM\HARDWARE\DESCRIPTION\System\CentralProcessor\0      SUCCESS
1:43:21.3899621 PM Procmon.exe    3160  Thread Exit                                                                SUCCESS       Thread ID: 3820, User T...
1:43:21.3919217 PM Procmon.exe    3160  QueryOpen         C:\Program Files\ProcessMonitor\Procmon.exe              FAST IO DI...
1:43:21.3919599 PM Procmon.exe    3160  CreateFile        C:\Program Files\ProcessMonitor\Procmon.exe              SUCCESS       Desired Access: Read A...
1:43:21.3920094 PM Procmon.exe    3160  QueryBasicInfor...C:\Program Files\ProcessMonitor\Procmon.exe              SUCCESS       CreationTime: 5/1/2017 ...
1:43:21.3920236 PM Procmon.exe    3160  CloseFile         C:\Program Files\ProcessMonitor\Procmon.exe              SUCCESS
1:43:21.3920406 PM Procmon.exe    3160  IRP_MJ_CLOSE      C:\Program Files\ProcessMonitor\Procmon.exe              SUCCESS
1:43:21.3921246 PM Procmon.exe    3160  QueryOpen         C:\Program Files\ProcessMonitor\Procmon.exe              FAST IO DI...
1:43:21.3921739 PM Procmon.exe    3160  CreateFile        C:\Program Files\ProcessMonitor\Procmon.exe              SUCCESS       Desired Access: Read A...
1:43:21.3921921 PM Procmon.exe    3160  QueryBasicInfor...C:\Program Files\ProcessMonitor\Procmon.exe              SUCCESS       CreationTime: 5/1/2017 ...
1:43:21.3922040 PM Procmon.exe    3160  CloseFile         C:\Program Files\ProcessMonitor\Procmon.exe              SUCCESS
1:43:21.3922166 PM Procmon.exe    3160  IRP_MJ_CLOSE      C:\Program Files\ProcessMonitor\Procmon.exe              SUCCESS
1:43:21.3922811 PM Procmon.exe    3160  QueryOpen         C:\Program Files\ProcessMonitor\Procmon.exe              FAST IO DI...
1:43:21.3923187 PM Procmon.exe    3160  CreateFile        C:\Program Files\ProcessMonitor\Procmon.exe              SUCCESS       Desired Access: Read A...
1:43:21.3923341 PM Procmon.exe    3160  QueryBasicInfor...C:\Program Files\ProcessMonitor\Procmon.exe              SUCCESS       CreationTime: 5/1/2017 ...
1:43:21.3923455 PM Procmon.exe    3160  CloseFile         C:\Program Files\ProcessMonitor\Procmon.exe              SUCCESS
1:43:21.3923578 PM Procmon.exe    3160  IRP_MJ_CLOSE      C:\Program Files\ProcessMonitor\Procmon.exe              SUCCESS
1:43:21.3924869 PM Procmon.exe    3160  QueryOpen         C:\Program Files\ProcessMonitor\Procmon.exe              FAST IO DI...
1:43:21.3925248 PM Procmon.exe    3160  CreateFile        C:\Program Files\ProcessMonitor\Procmon.exe              SUCCESS       Desired Access: Read A...
1:43:21.3925410 PM Procmon.exe    3160  QueryBasicInfor...C:\Program Files\ProcessMonitor\Procmon.exe              SUCCESS       CreationTime: 5/1/2017 ...
1:43:21.3925525 PM Procmon.exe    3160  CloseFile         C:\Program Files\ProcessMonitor\Procmon.exe              SUCCESS
1:43:21.3925653 PM Procmon.exe    3160  IRP_MJ_CLOSE      C:\Program Files\ProcessMonitor\Procmon.exe              SUCCESS
1:43:21.3926122 PM Procmon.exe    3160  QueryOpen         C:\Program Files\ProcessMonitor\Procmon.exe              FAST IO DI...
```

Excluding Harmless Processes

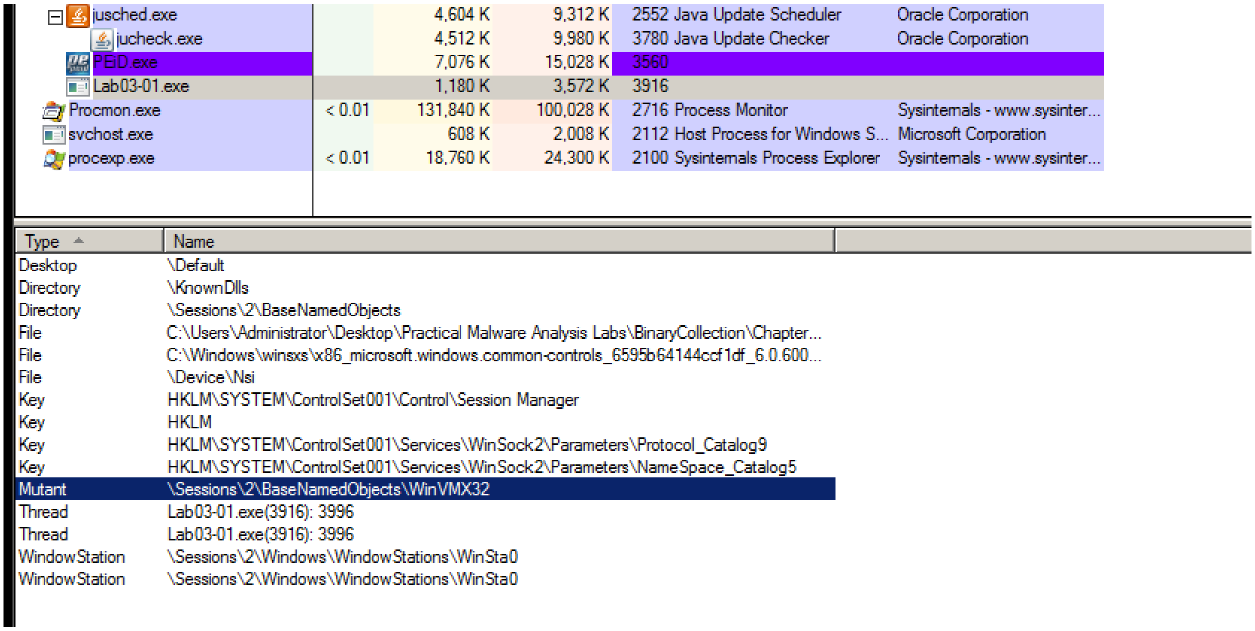

Player
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

```
     Time of Day   Process Name    PID  Operation         Path                                                     Result        Detail
```

Run the Lab03-01.exe File

Viewing the Running Malware in Process Explorer

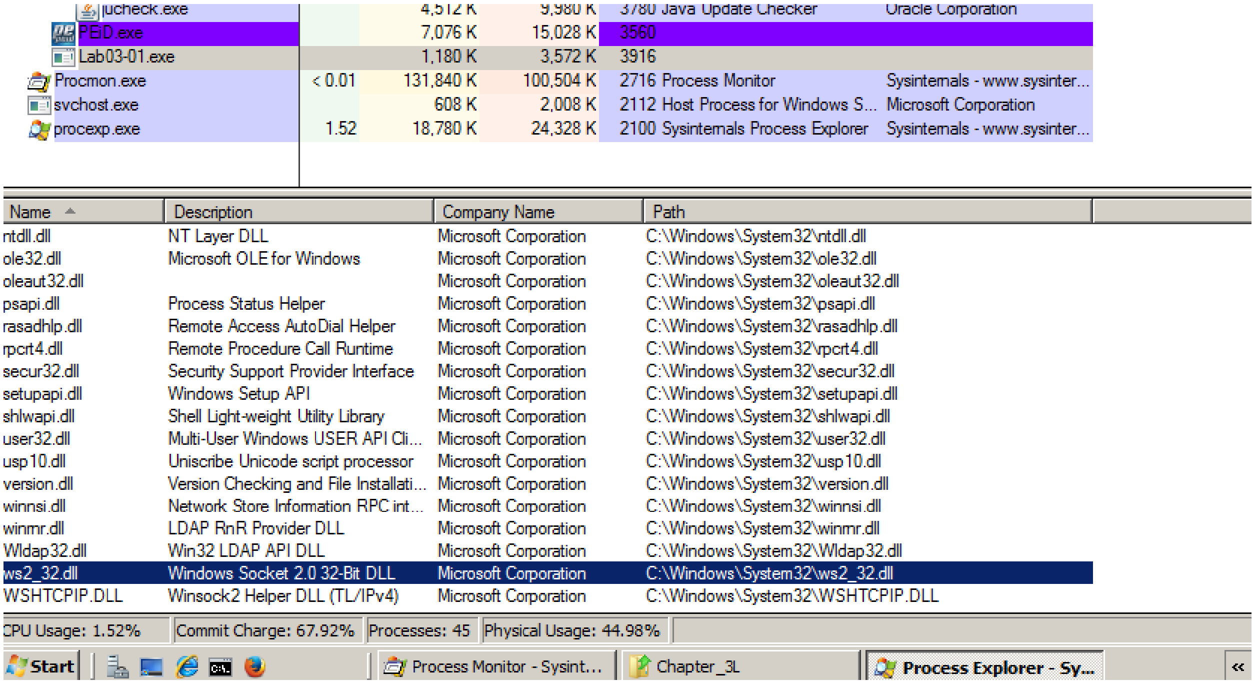
In Process Explorer, click View, "Lower Pane View", Handles. You see the WinVMX32 mutant, as highlighted below. A mutant, also called a mutex, is used for interprocess connunication.



jusched.exe		4,604 K	9,312 K	2552 Java Update Scheduler	Oracle Corporation
jucheck.exe		4,512 K	9,980 K	3780 Java Update Checker	Oracle Corporation
PEiD.exe		7,076 K	15,028 K	3560	
Lab03-01.exe		1,180 K	3,572 K	3916	
Procmon.exe	< 0.01	131,840 K	100,028 K	2716 Process Monitor	Sysinternals - www.sysinter...
svchost.exe		608 K	2,008 K	2112 Host Process for Windows S...	Microsoft Corporation
procexp.exe	< 0.01	18,760 K	24,300 K	2100 Sysinternals Process Explorer	Sysinternals - www.sysinter...

Type	Name
Desktop	\Default
Directory	\KnownDlls
Directory	\Sessions\2\BaseNamedObjects
File	C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter...
File	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.600...
File	\Device\Nsi
Key	HKLM\SYSTEM\ControlSet001\Control\Session Manager
Key	HKLM
Key	HKLM\SYSTEM\ControlSet001\Services\WinSock2\Parameters\Protocol_Catalog9
Key	HKLM\SYSTEM\ControlSet001\Services\WinSock2\Parameters\NameSpace_Catalog5
Mutant	\Sessions\2\BaseNamedObjects\WinVMX32
Thread	Lab03-01.exe(3916): 3996
Thread	Lab03-01.exe(3916): 3996
WindowStation	\Sessions\2\Windows\WindowStations\WinSta0
WindowStation	\Sessions\2\Windows\WindowStations\WinSta0

In Process Explorer, click View, "Lower Pane View", DLLs. Scroll to the bottom to find ws2_32.dll and WSHTCPIP.DLL, as shown below. This shows that the malware has networking functionality.



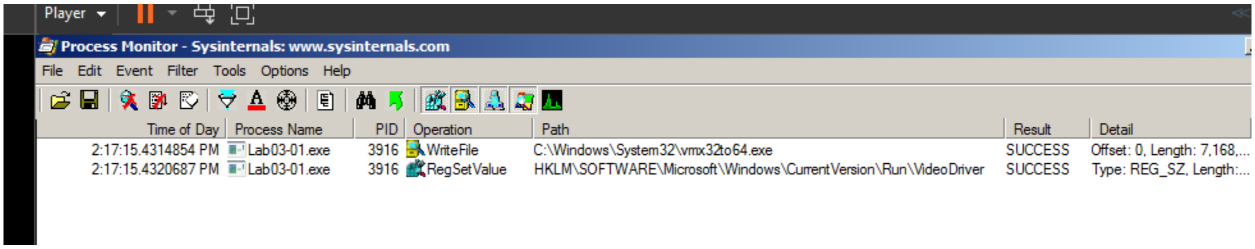
jucheck.exe		4,512 K	9,980 K	3780 Java Update Checker	Oracle Corporation
PEiD.exe		7,076 K	15,028 K	3560	
Lab03-01.exe		1,180 K	3,572 K	3916	
Procmon.exe	< 0.01	131,840 K	100,504 K	2716 Process Monitor	Sysinternals - www.sysinter...
svchost.exe		608 K	2,008 K	2112 Host Process for Windows S...	Microsoft Corporation
procexp.exe	1.52	18,780 K	24,328 K	2100 Sysinternals Process Explorer	Sysinternals - www.sysinter...

Name	Description	Company Name	Path
ntdll.dll	NT Layer DLL	Microsoft Corporation	C:\Windows\System32\ntdll.dll
ole32.dll	Microsoft OLE for Windows	Microsoft Corporation	C:\Windows\System32\ole32.dll
oleaut32.dll		Microsoft Corporation	C:\Windows\System32\oleaut32.dll
psapi.dll	Process Status Helper	Microsoft Corporation	C:\Windows\System32\psapi.dll
rasadhlp.dll	Remote Access AutoDial Helper	Microsoft Corporation	C:\Windows\System32\rasadhlp.dll
rpcrt4.dll	Remote Procedure Call Runtime	Microsoft Corporation	C:\Windows\System32\rpcrt4.dll
secur32.dll	Security Support Provider Interface	Microsoft Corporation	C:\Windows\System32\secur32.dll
setupapi.dll	Windows Setup API	Microsoft Corporation	C:\Windows\System32\setupapi.dll
shlwapi.dll	Shell Light-weight Utility Library	Microsoft Corporation	C:\Windows\System32\shlwapi.dll
user32.dll	Multi-User Windows USER API Cli...	Microsoft Corporation	C:\Windows\System32\user32.dll
usp10.dll	Uniscribe Unicode script processor	Microsoft Corporation	C:\Windows\System32\usp10.dll
version.dll	Version Checking and File Installati...	Microsoft Corporation	C:\Windows\System32\version.dll
winnsi.dll	Network Store Information RPC int...	Microsoft Corporation	C:\Windows\System32\winnsi.dll
winrnr.dll	LDAP RnR Provider DLL	Microsoft Corporation	C:\Windows\System32\winrnr.dll
Wldap32.dll	Win32 LDAP API DLL	Microsoft Corporation	C:\Windows\System32\Wldap32.dll
ws2_32.dll	Windows Socket 2.0 32-Bit DLL	Microsoft Corporation	C:\Windows\System32\ws2_32.dll
WSHTCPIP.DLL	Winsock2 Helper DLL (TL/IPv4)	Microsoft Corporation	C:\Windows\System32\WSHTCPIP.DLL

CPU Usage: 1.52% | Commit Charge: 67.92% | Processes: 45 | Physical Usage: 44.98%

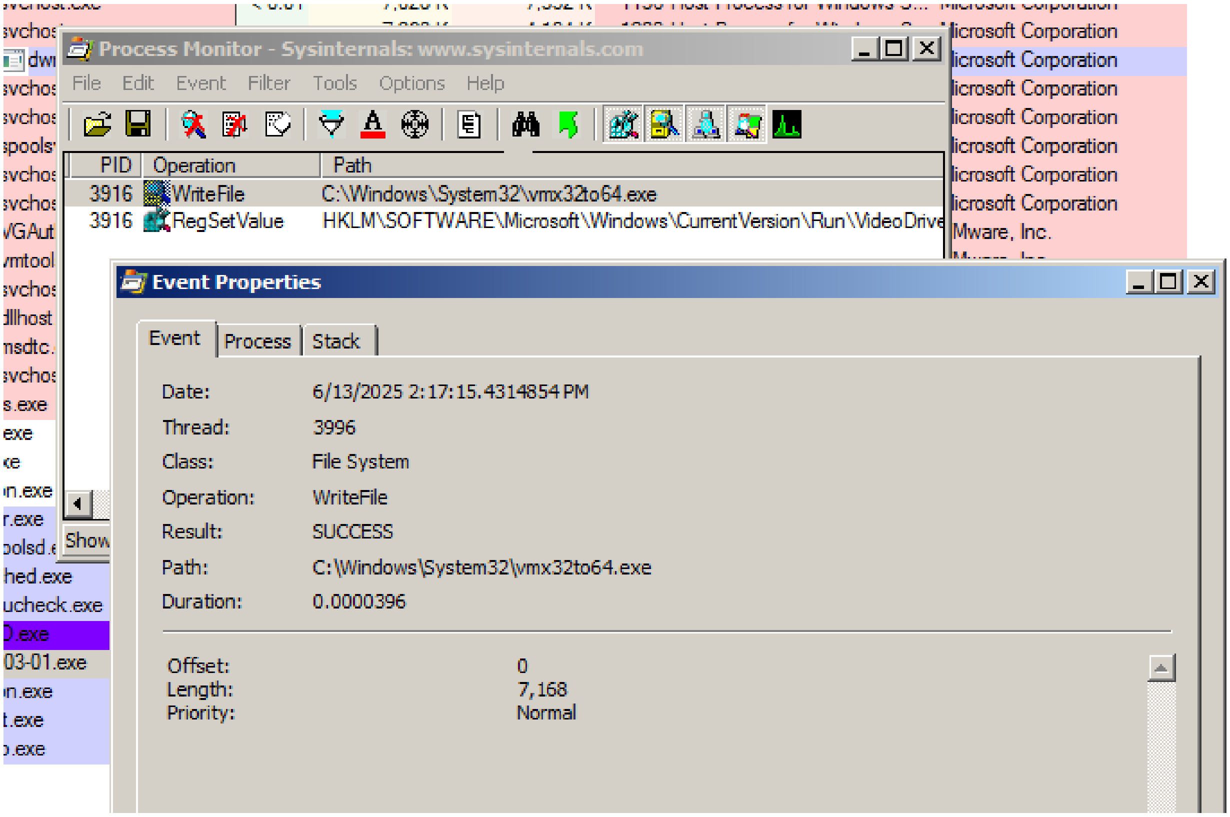
Viewing the Malicious Process's Events in Process Monitor

You end up the two events shown below.


Player
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

Time of Day	Process Name	PID	Operation	Path	Result	Detail
2:17:15.4314854 PM	Lab03-01.exe	3916	WriteFile	C:\Windows\System32\vmx32to64.exe	SUCCESS	Offset: 0, Length: 7,168,...
2:17:15.4320687 PM	Lab03-01.exe	3916	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\VideoDriver	SUCCESS	Type: REG_SZ, Length:...

Double-click the event with a Path ending in vmx32to64.exe. The Properties sheet shows that this event creates a file named vmx32to64.exe, as shown below. As explained in more detail in the book, this event has copied the malware itself to a file named vmx32to64.exe, so that filename is a useful indicator of infection.

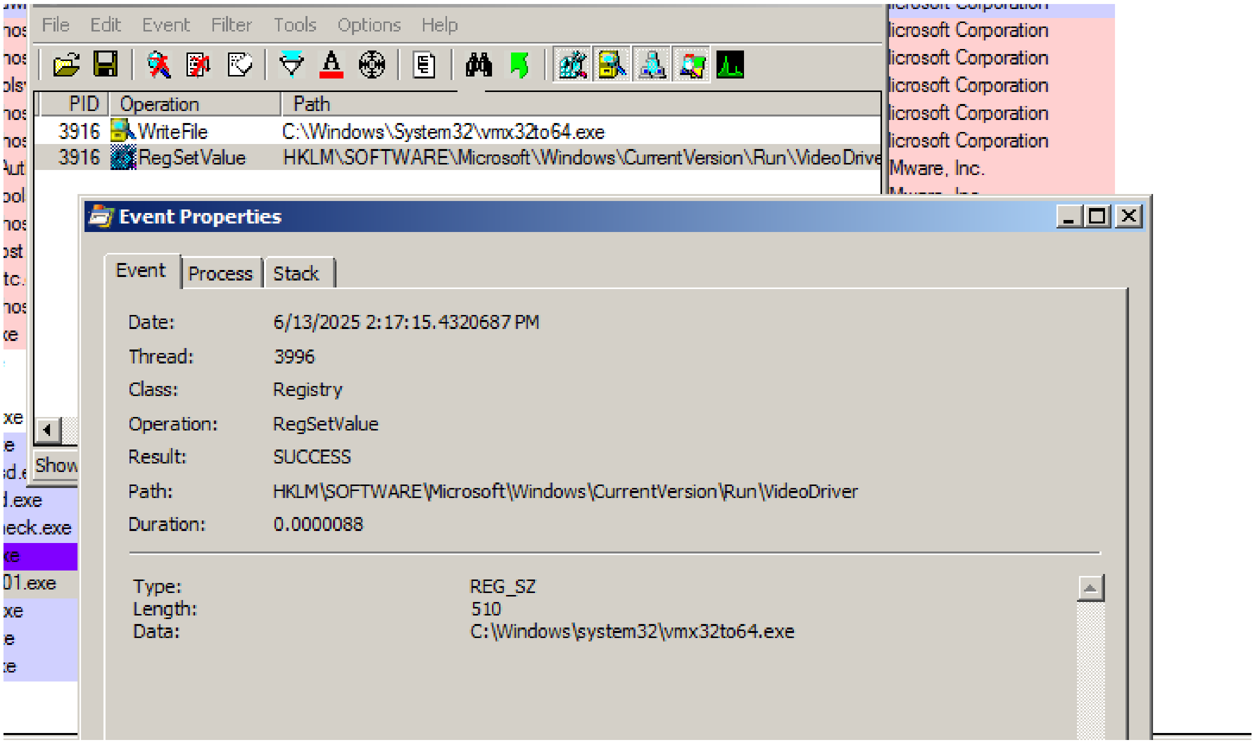

Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Event Properties
Event
Process
Stack

PID	Operation	Path
3916	WriteFile	C:\Windows\System32\vmx32to64.exe
3916	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\VideoDrive

Date: 6/13/2025 2:17:15.4314854 PM
Thread: 3996
Class: File System
Operation: WriteFile
Result: SUCCESS
Path: C:\Windows\System32\vmx32to64.exe
Duration: 0.0000396

Offset: 0
Length: 7,168
Priority: Normal

Double-click the with a Path ending in VideoDriver. This creates a new a Run key in the registry named "VideoDriver" with a value of "C:\WINDOWS\system32\vmx32to64.exe" -- this is a persistence mechanism, to relaunch the malware when the machine restarts.

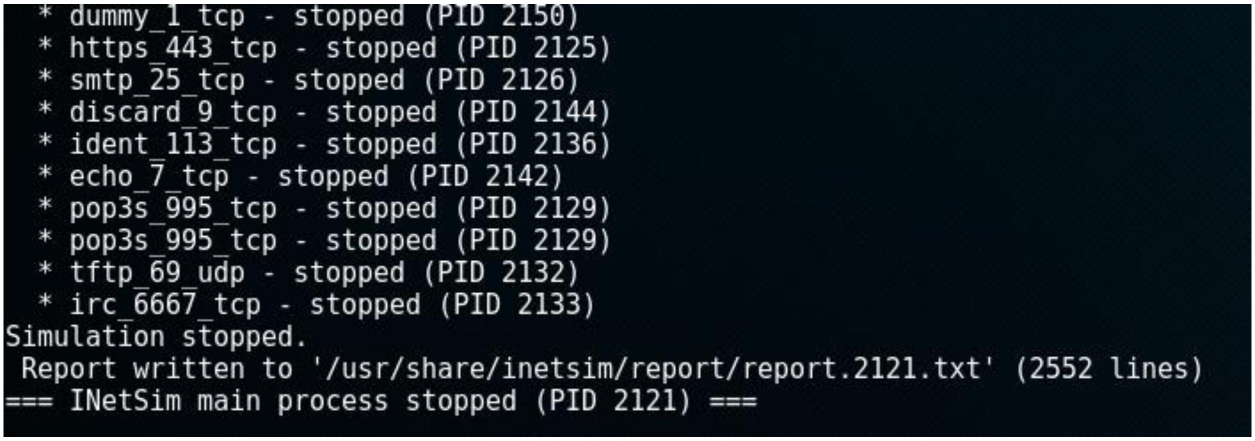


PID	Operation	Path
3916	WriteFile	C:\Windows\System32\vmx32to64.exe
3916	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\VideoDrive

Date:	6/13/2025 2:17:15.4320687 PM
Thread:	3996
Class:	Registry
Operation:	RegSetValue
Result:	SUCCESS
Path:	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\VideoDriver
Duration:	0.0000088

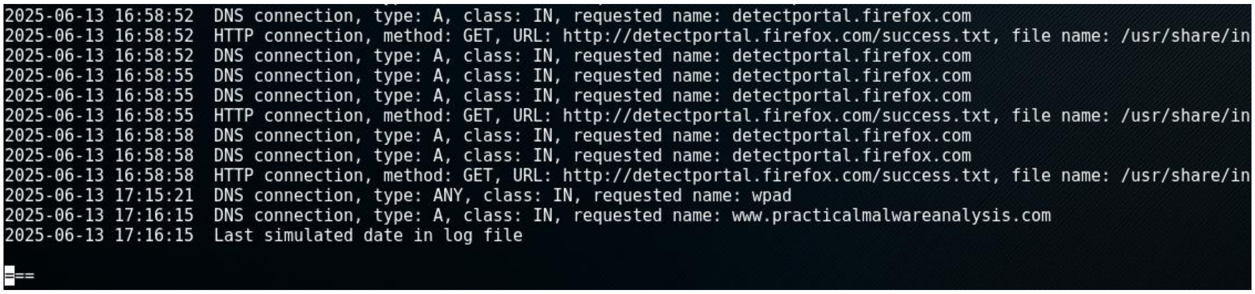
Type:	REG_SZ
Length:	510
Data:	C:\Windows\system32\vmx32to64.exe

Viewing INetSim Logs



```
  * dummy_1_tcp - stopped (PID 2150)
  * https_443_tcp - stopped (PID 2125)
  * smtp_25_tcp - stopped (PID 2126)
  * discard_9_tcp - stopped (PID 2144)
  * ident_113_tcp - stopped (PID 2136)
  * echo_7_tcp - stopped (PID 2142)
  * pop3s_995_tcp - stopped (PID 2129)
  * pop3s_995_tcp - stopped (PID 2129)
  * tftp_69_udp - stopped (PID 2132)
  * irc_6667_tcp - stopped (PID 2133)
Simulation stopped.
 Report written to '/usr/share/inetsim/report/report.2121.txt' (2552 lines)
=== INetSim main process stopped (PID 2121) ===
```

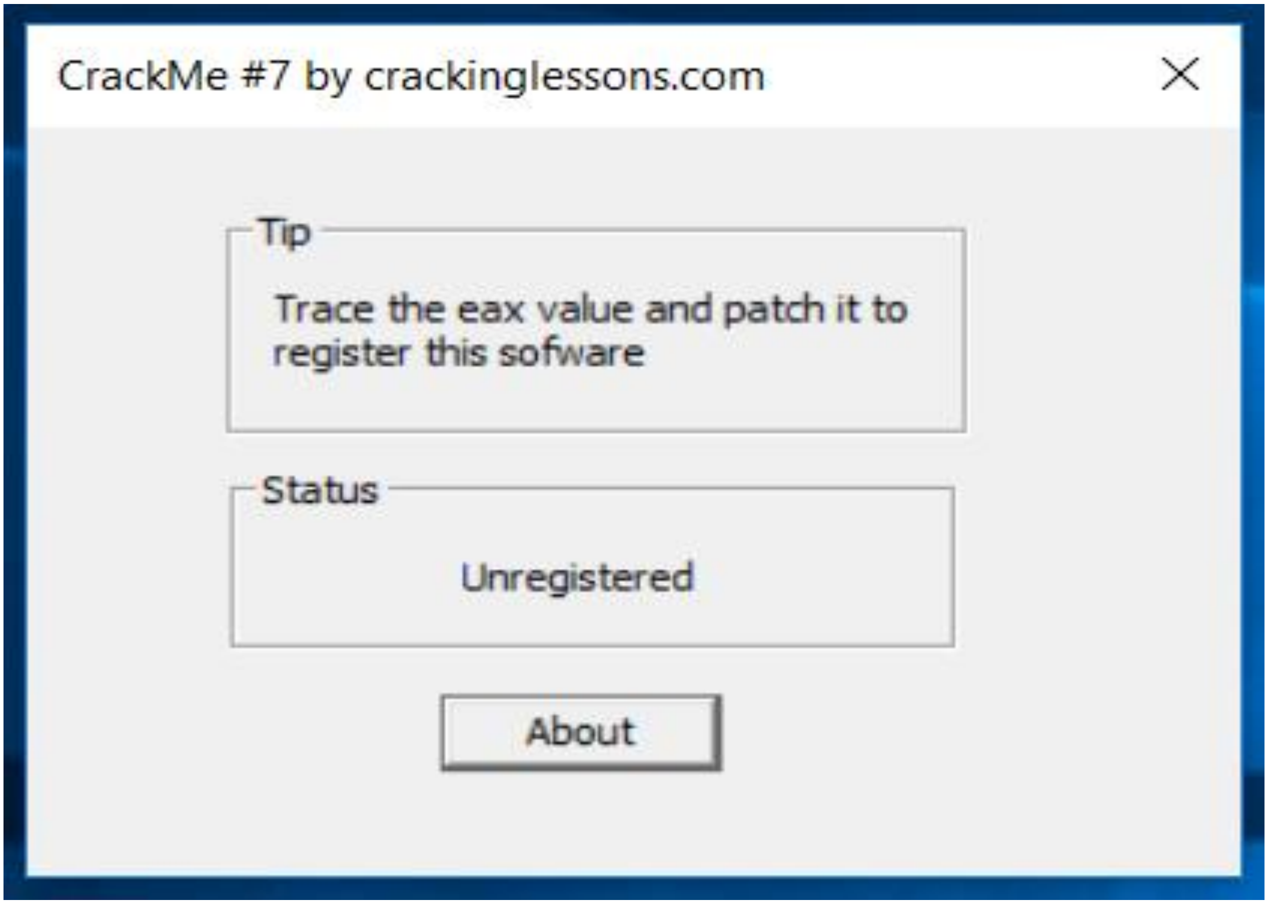
You should see DNS connections to www.practicalmalwareanalysis.com, as shown below:



```
2025-06-13 16:58:52  DNS connection, type: A, class: IN, requested name: detectportal.firefox.com
2025-06-13 16:58:52  HTTP connection, method: GET, URL: http://detectportal.firefox.com/success.txt, file name: /usr/share/in
2025-06-13 16:58:52  DNS connection, type: A, class: IN, requested name: detectportal.firefox.com
2025-06-13 16:58:55  DNS connection, type: A, class: IN, requested name: detectportal.firefox.com
2025-06-13 16:58:55  DNS connection, type: A, class: IN, requested name: detectportal.firefox.com
2025-06-13 16:58:55  HTTP connection, method: GET, URL: http://detectportal.firefox.com/success.txt, file name: /usr/share/in
2025-06-13 16:58:58  DNS connection, type: A, class: IN, requested name: detectportal.firefox.com
2025-06-13 16:58:58  DNS connection, type: A, class: IN, requested name: detectportal.firefox.com
2025-06-13 16:58:58  HTTP connection, method: GET, URL: http://detectportal.firefox.com/success.txt, file name: /usr/share/in
2025-06-13 17:15:21  DNS connection, type: ANY, class: IN, requested name: wpad
2025-06-13 17:16:15  DNS connection, type: A, class: IN, requested name: www.practicalmalwareanalysis.com
2025-06-13 17:16:15  Last simulated date in log file

===
```

CRACK ME 7

This CrackMe teaches a specific method of cracking which is to trace the eax value and patch it.



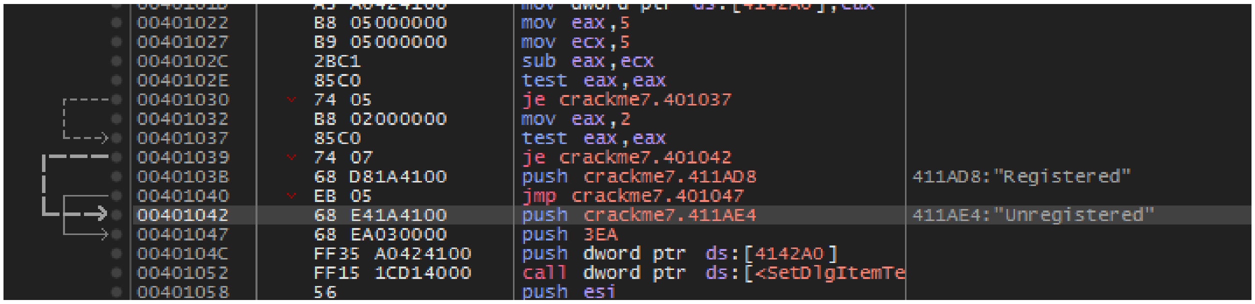
CrackMe #7 by crackinglessons.com

Trace the eax value and patch it to register this sofware

Unregistered

Follow the hint, we will notice any EAX value in the scope. But first let trace into the code of string “Unregistered” displaying in Status box.

After string referencing and trace above the code, we notice this code partition below:



```
0040101D   A3 A0424100   mov dword ptr ds:[4142A0],eax
00401022   B8 05000000   mov eax,5
00401027   B9 05000000   mov ecx,5
0040102C   2BC1          sub eax,ecx
0040102E   85C0          test eax,eax
00401030   74 05         je crackme7.401037
00401032   B8 02000000   mov eax,2
00401037   85C0          test eax,eax
00401039   74 07         je crackme7.401042
0040103B   68 D81A4100   push crackme7.411AD8                  411AD8:"Registered"
00401040   EB 05         jmp crackme7.401047
00401042   68 E41A4100   push crackme7.411AE4                  411AE4:"Unregistered"
00401047   68 EA030000   push 3EA
0040104C   FF35 A0424100 push dword ptr ds:[4142A0]
00401052   FF15 1CD14000 call dword ptr ds:[<SetDlgItemTe
00401058   56            push esi
```

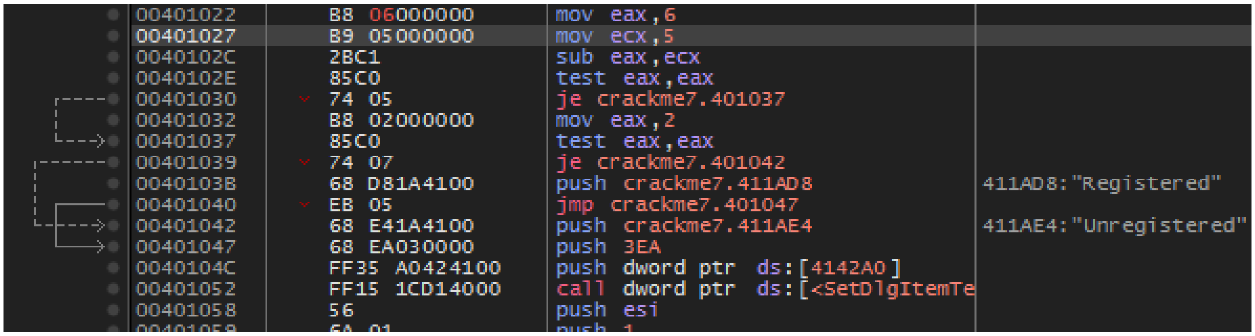
From “mov EAX, 5”, EAX is assigned value 5, happening too with ECX.

“Sub eax, ecx” created value 0 and assigned to EAX. After subtracting, “test eax, eax” executes “AND bit-wise” operation and put the flag if it’s 0 value – in this condition, EAX is 0 meaning the JE command below is executed. Jumping to another Test command, and another JE command jump to the address of status Unregistered (00401042).

If the first Test command is not operated, ignoring JE command and we have new value of EAX is 2, leading to failure of the second Test and second JE. This make status having “Registed” flag in adress 0040103B.

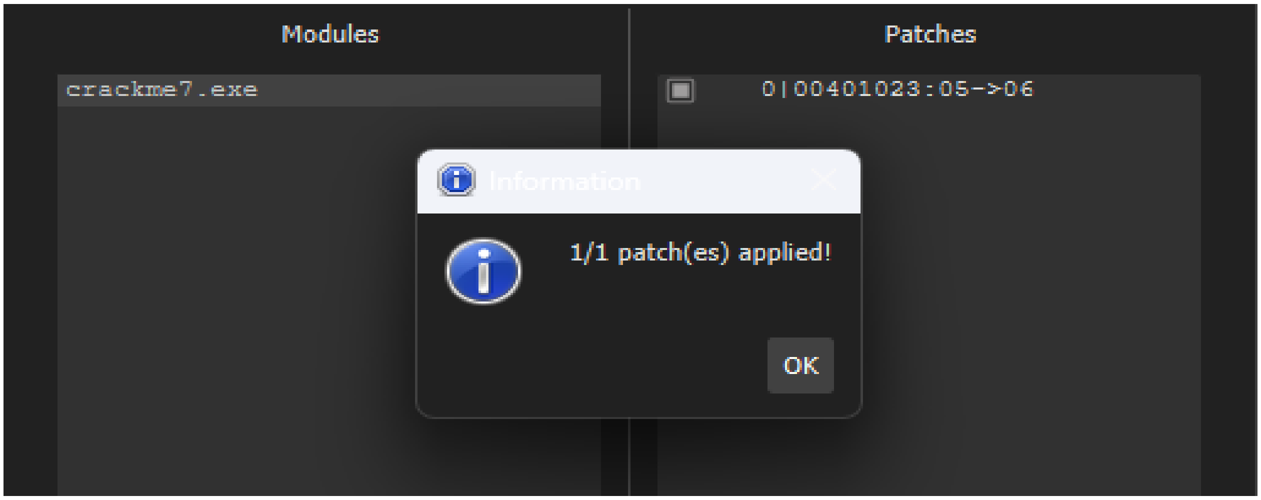
Hence, I try to change the first value of EAX in address 00401022, leading to value not equals 0 of EAX after subtraction. The idea is prevent the execution of the first Test command.

Mov eax, 5 → Mov eax, 6



```
00401022   B8 06000000   mov eax,6
00401027   B9 05000000   mov ecx,5
0040102C   2BC1          sub eax,ecx
0040102E   85C0          test eax,eax
00401030   74 05         je crackme7.401037
00401032   B8 02000000   mov eax,2
00401037   85C0          test eax,eax
00401039   74 07         je crackme7.401042
0040103B   68 D81A4100   push crackme7.411AD8                  411AD8:"Registered"
00401040   EB 05         jmp crackme7.401047
00401042   68 E41A4100   push crackme7.411AE4                  411AE4:"Unregistered"
00401047   68 EA030000   push 3EA
0040104C   FF35 A0424100 push dword ptr ds:[4142A0]
00401052   FF15 1CD14000 call dword ptr ds:[<SetDlgItemTe
00401058   56            push esi
0040105A   6A 01         push 1
```

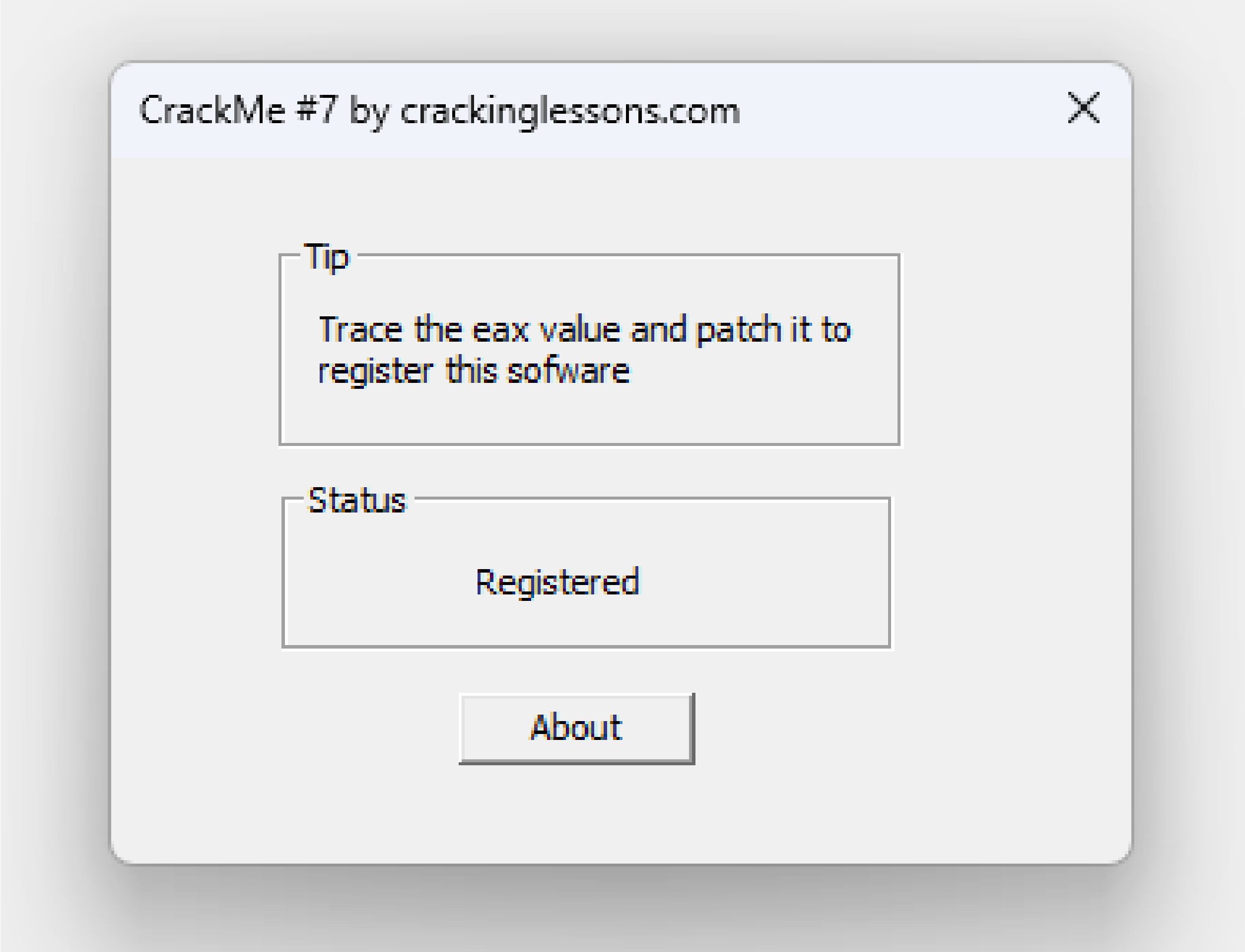
Patch file and run again.



crackme7.exe

```
0|00401023:05->06
```

1/1 patch(es) applied!



CrackMe #7 by crackinglessons.com

Trace the eax value and patch it to register this sofware

Registered

DONE!