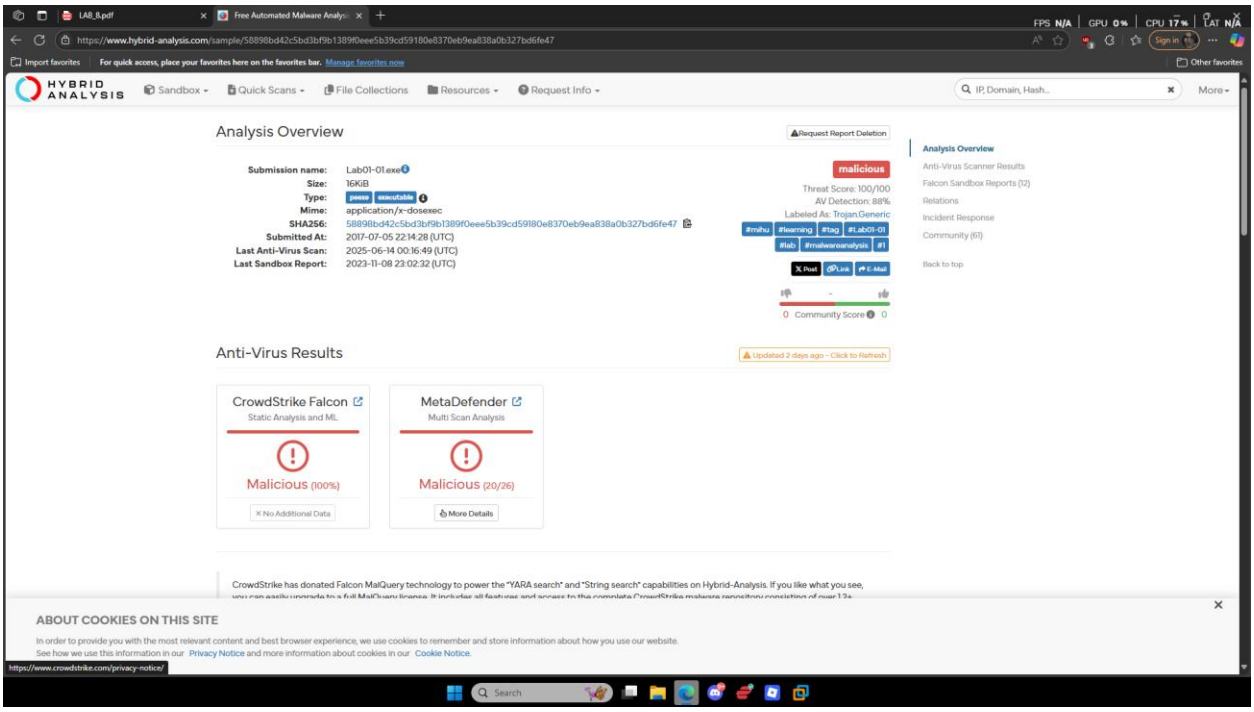
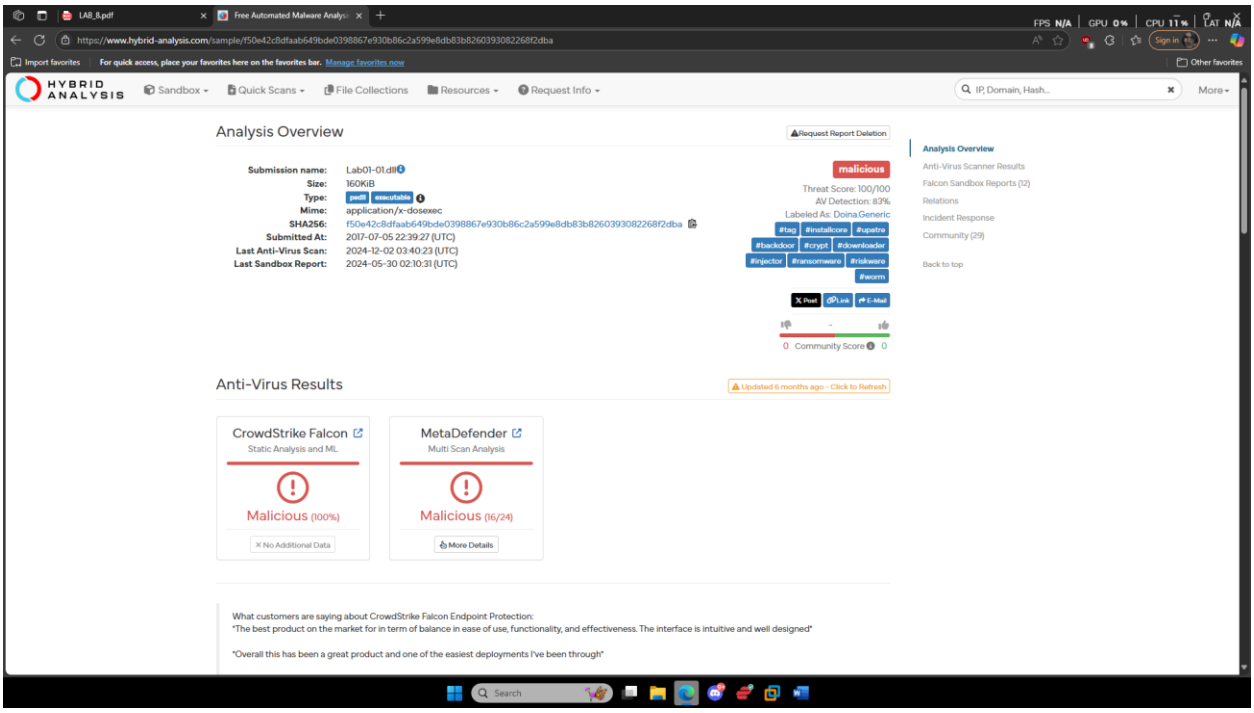
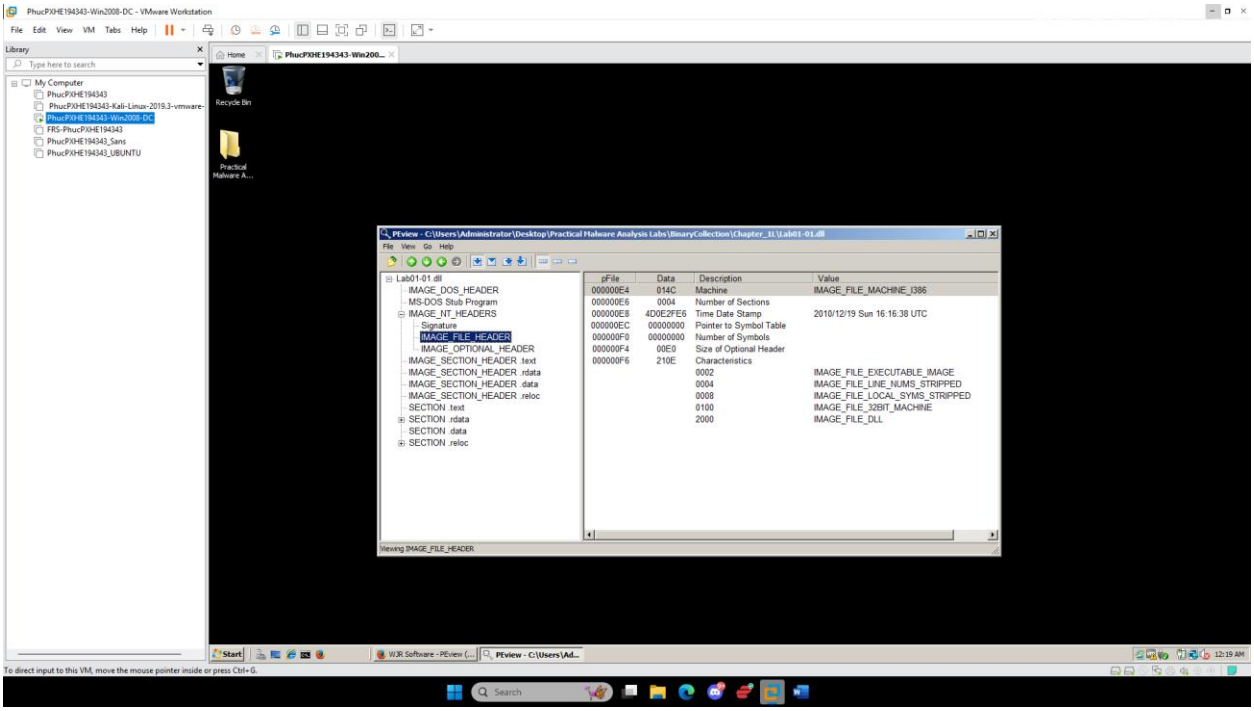
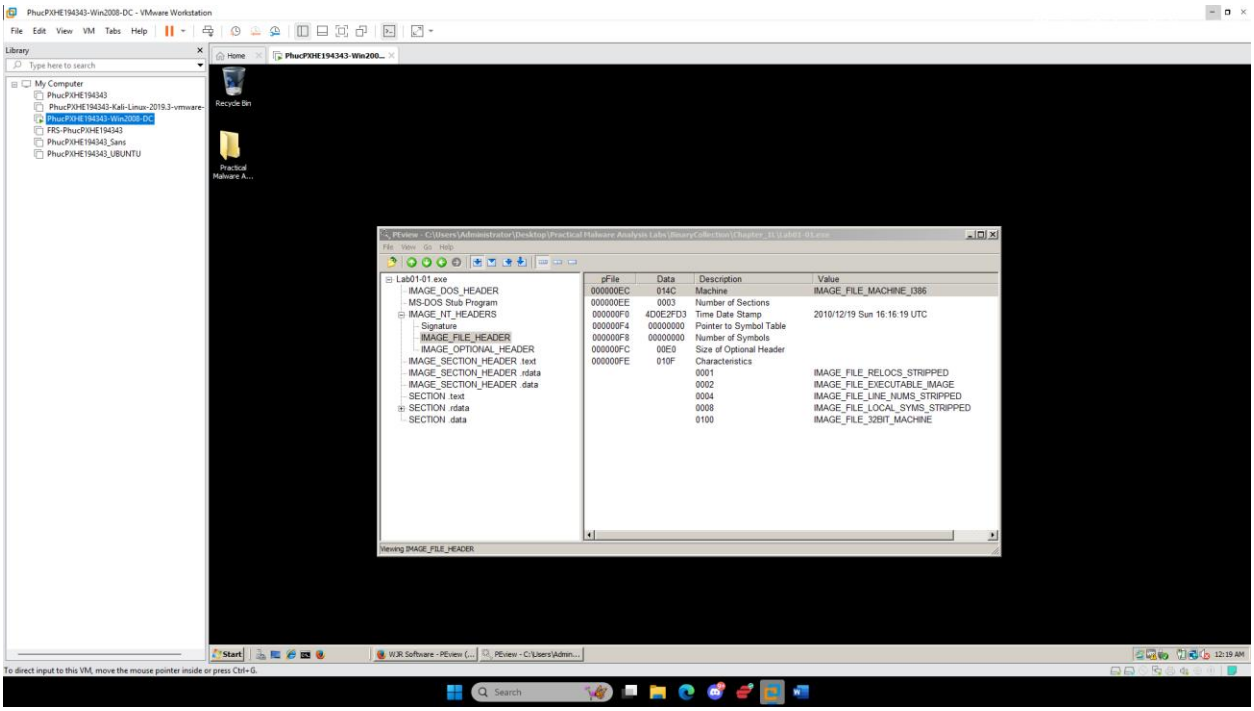
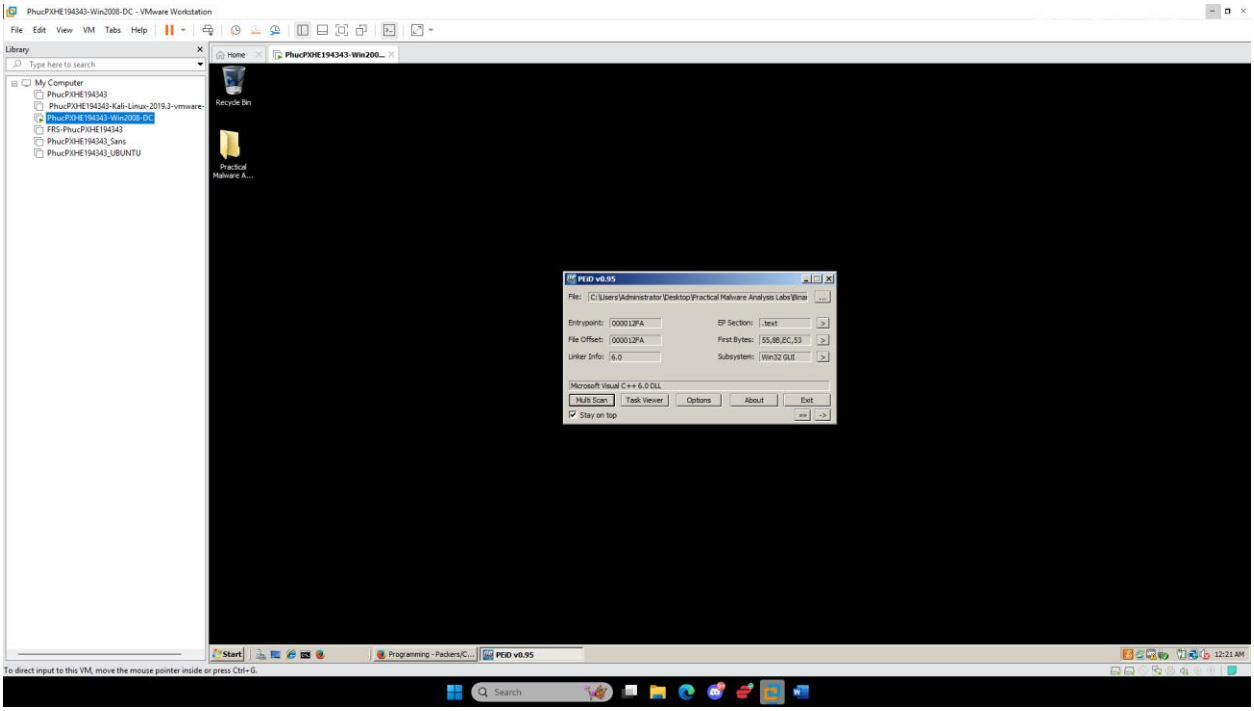
Lab8

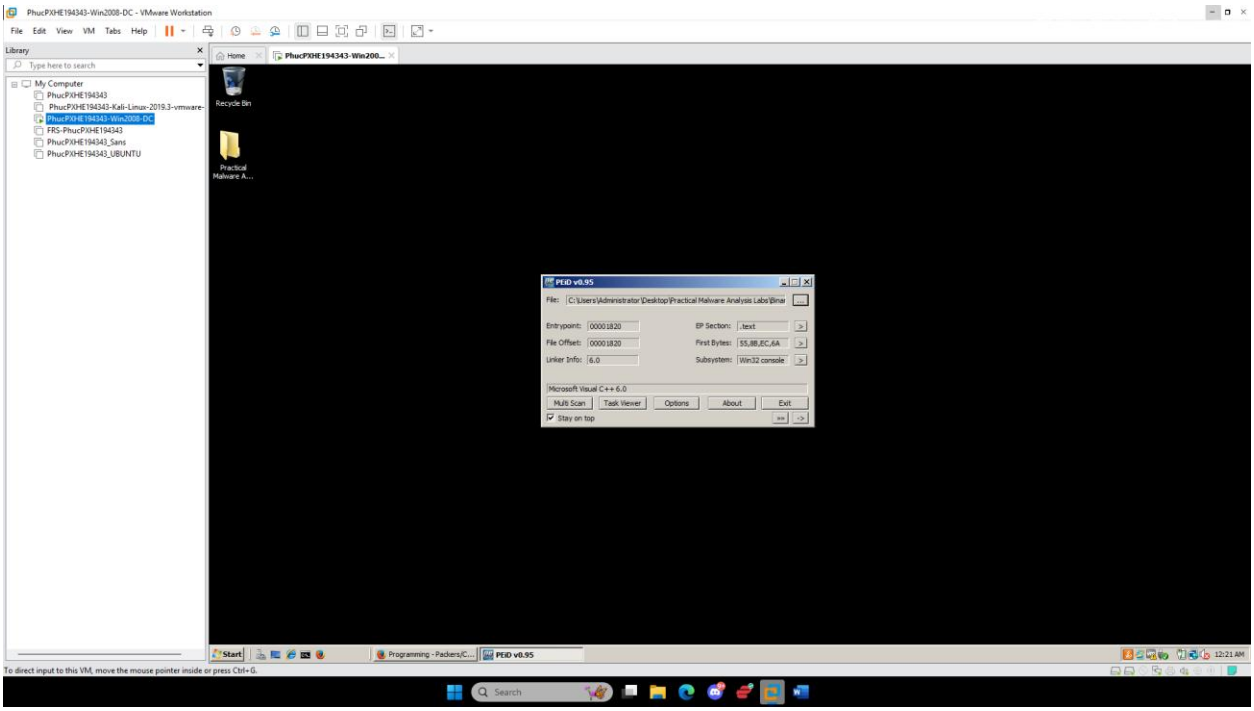

HYBRID ANALYSIS
Analysis Overview
Submission name: Lab01-01.exe
Size: 16KiB
Type: peexe executable
Mime: application/x-dosexec
SHA256: 58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47
Submitted At: 2017-07-05 22:14:28 (UTC)
Last Anti-Virus Scan: 2025-06-14 00:16:49 (UTC)
Last Sandbox Report: 2023-11-08 23:02:32 (UTC)
malicious
Threat Score: 100/100
AV Detection: 88%
Labeled As: Trojan.Generic
Anti-Virus Results
CrowdStrike Falcon
Static Analysis and ML
Malicious (100%)
MetaDefender
Multi Scan Analysis
Malicious (20/26)
ABOUT COOKIES ON THIS SITE

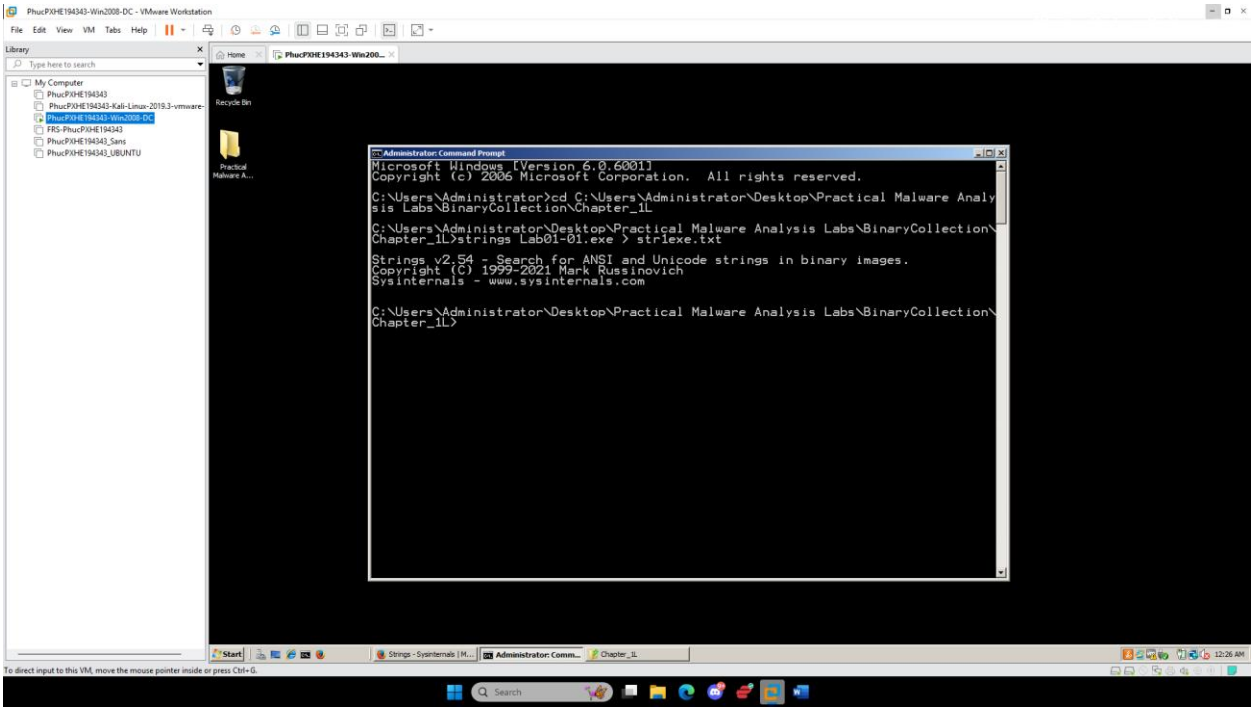

HYBRID ANALYSIS
Analysis Overview
Submission name: Lab01-01.dll
Size: 160KiB
Type: pedll executable
Mime: application/x-dosexec
SHA256: f50e42c8dfaab649bde0398867e930b86c2a599e8db83b826039308226 8f2dba
Submitted At: 2017-07-05 22:39:27 (UTC)
Last Anti-Virus Scan: 2024-12-02 03:40:23 (UTC)
Last Sandbox Report: 2024-05-30 02:10:31 (UTC)
malicious
Threat Score: 100/100
AV Detection: 83%
Labeled As: Doina.Generic
Anti-Virus Results
CrowdStrike Falcon
Static Analysis and ML
Malicious (100%)
MetaDefender
Multi Scan Analysis
Malicious (16/24)
What customers are saying about CrowdStrike Falcon Endpoint Protection:
"The best product on the market for in term of balance in ease of use, functionality, and effectiveness. The interface is intuitive and well designed"
"Overall this has been a great product and one of the easiest deployments I've been through"

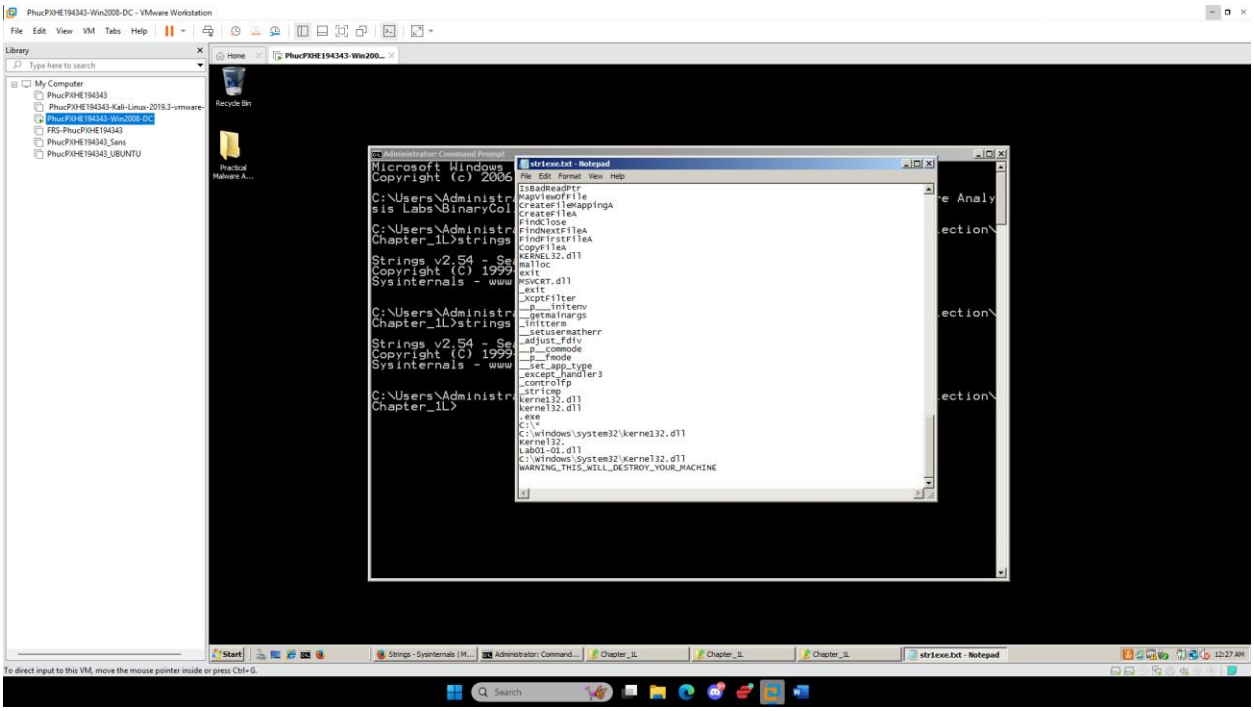

PhucPXHE194343-Win2008-DC - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
PhucPXHE194343
PhucPXHE194343-Kali-Linux-2019.3-vmware-
PhucPXHE194343-Win2008-DC
FRS-PhucPXHE194343
PhucPXHE194343_Sans
PhucPXHE194343_UBUNTU
Home
PhucPXHE194343-Win200...
Recycle Bin
Practical Malware A...
PEview - C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L\Lab01-01.dll
File View Go Help
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
Start
W3R Software - PEview (...
PEview - C:\Users\Ad...
12:19 AM
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search

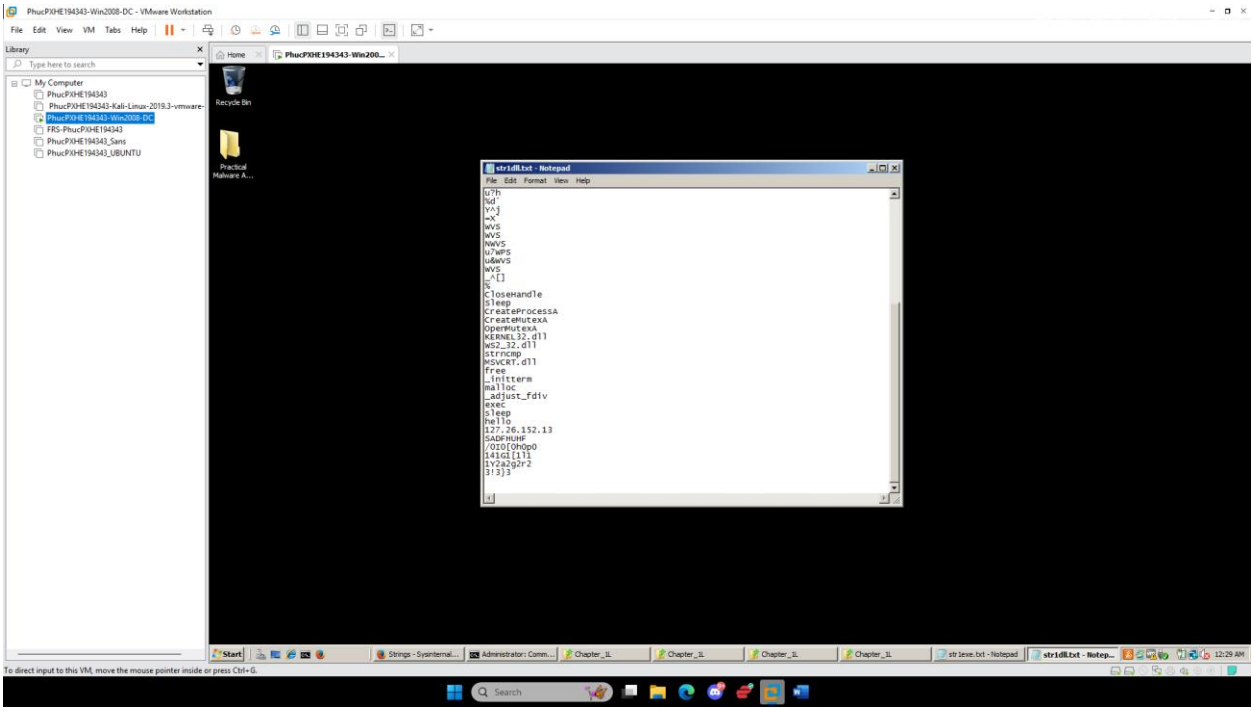

PhucPXHE194343-Win2008-DC - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
PhucPXHE194343
PhucPXHE194343-Kali-Linux-2019.3-vmware-
PhucPXHE194343-Win2008-DC
FRS-PhucPXHE194343
PhucPXHE194343_Sans
PhucPXHE194343_UBUNTU
Home
PhucPXHE194343-Win200...
Recycle Bin
Practical Malware A...
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
Start
W3R Software - PEview (...
PEview - C:\Users\Admin...
12:19 AM
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search

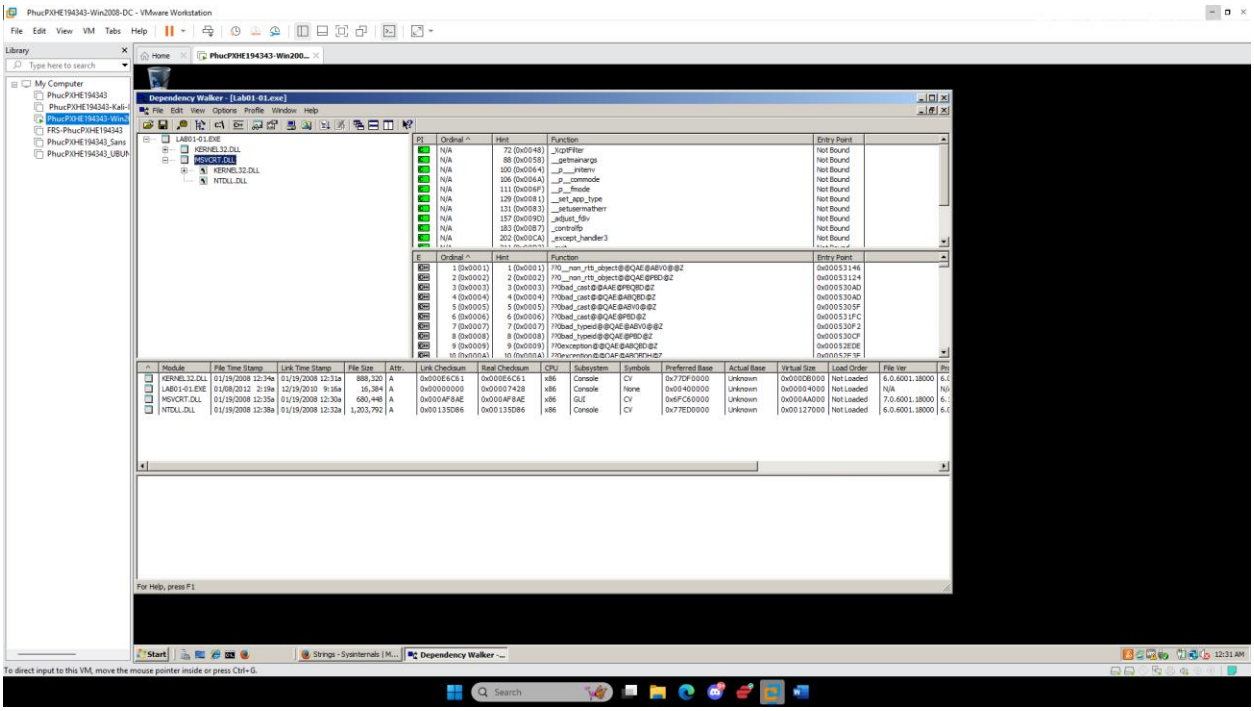

PhucPXHE194343-Win2008-DC - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
PhucPXHE194343
PhucPXHE194343-Kali-Linux-2019.3-vmware-
PhucPXHE194343-Win2008-DC
FRS-PhucPXHE194343
PhucPXHE194343_Sans
PhucPXHE194343_UBUNTU
Home
PhucPXHE194343-Win200...
Recycle Bin
Practical Malware A...
PEiD v0.95
File: C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\Binar
Entrypoint: 000012FA
EP Section: .text
File Offset: 000012FA
First Bytes: 55,8B,EC,53
Linker Info: 6.0
Subsystem: Win32 GUI
Microsoft Visual C++ 6.0 DLL
Multi Scan
Task Viewer
Options
About
Exit
Stay on top
Start
Programming - Packers/C...
PEiD v0.95
12:21 AM
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search

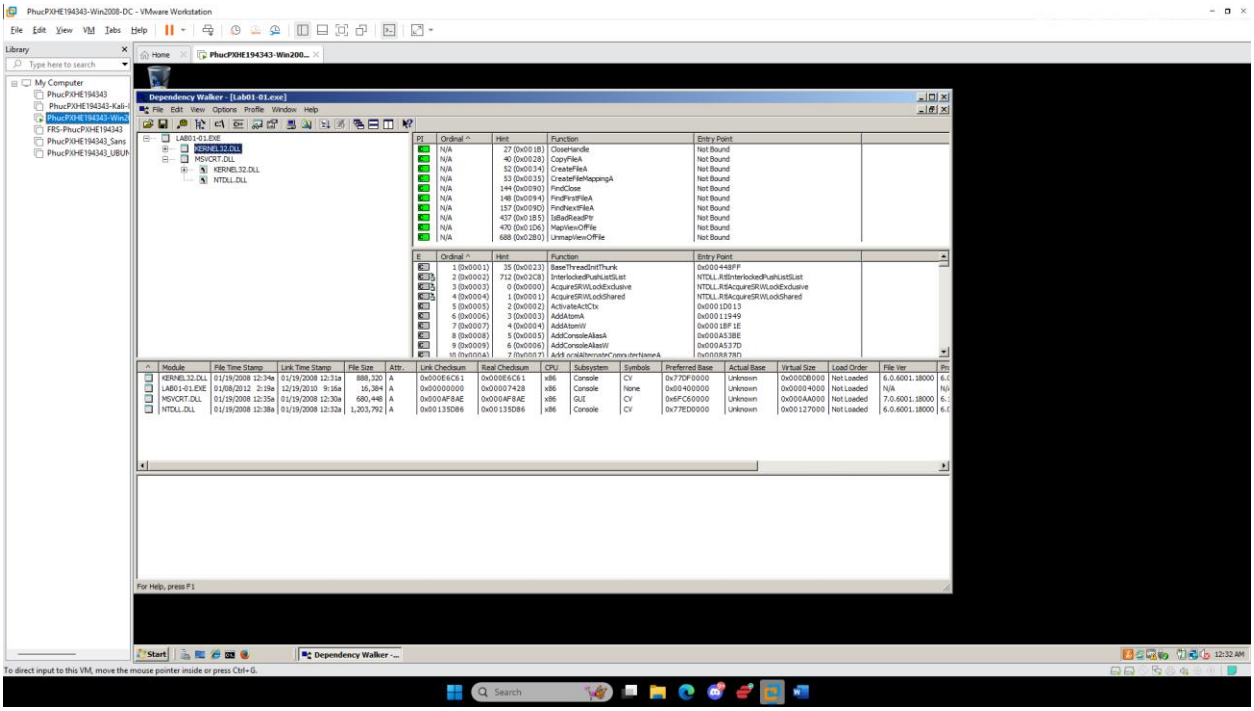

PhucPXHE194343-Win2008-DC - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
PhucPXHE194343
PhucPXHE194343-Kali-Linux-2019.3-vmware-
PhucPXHE194343-Win2008-DC
FRS-PhucPXHE194343
PhucPXHE194343_Sans
PhucPXHE194343_UBUNTU
Home
PhucPXHE194343-Win200...
Recycle Bin
Practical Malware A...
PEiD v0.95
File: C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\Binar
Entrypoint: 00001820
EP Section: .text
File Offset: 00001820
First Bytes: 55,8B,EC,6A
Linker Info: 6.0
Subsystem: Win32 console
Microsoft Visual C++ 6.0
Multi Scan
Task Viewer
Options
About
Exit
Stay on top
Start
Programming - Packers/C...
PEiD v0.95
12:21 AM
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search

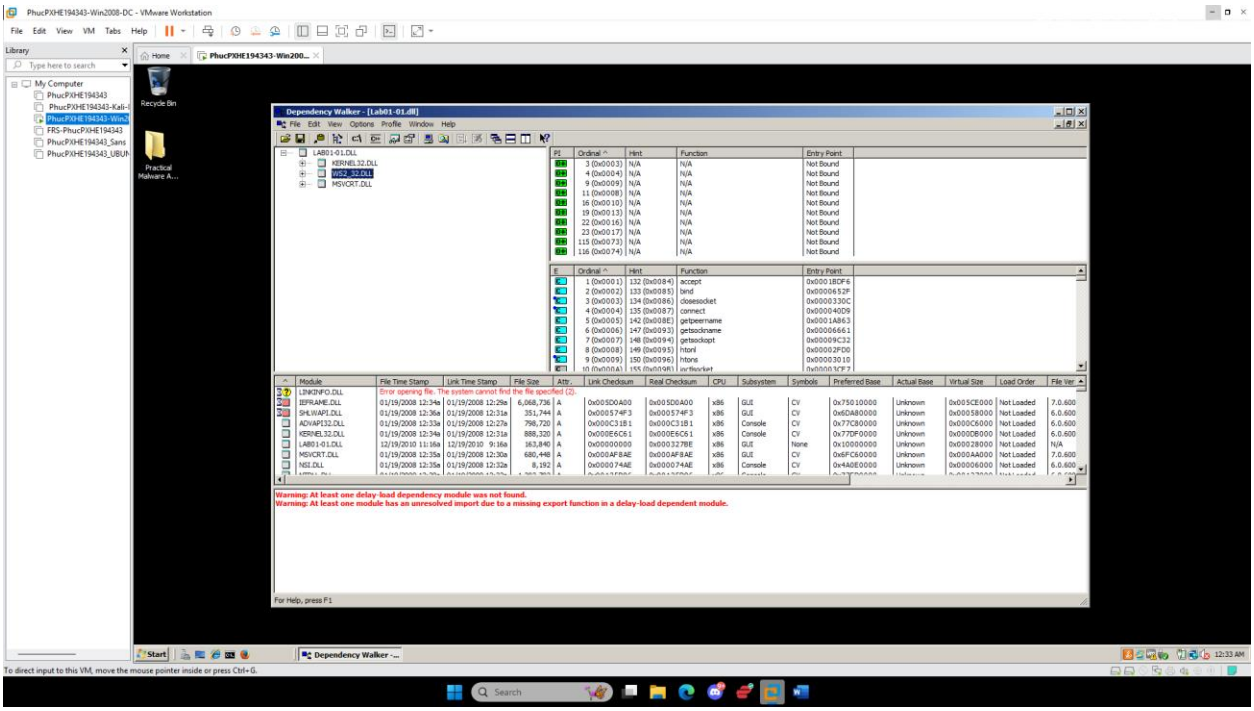

PhucPXHE194343-Win2008-DC - VMware Workstation
Administrator: Command Prompt
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>cd C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L
C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L>strings Lab01-01.exe > str1exe.txt
Strings v2.54 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2021 Mark Russinovich
Sysinternals - www.sysinternals.com
C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L>

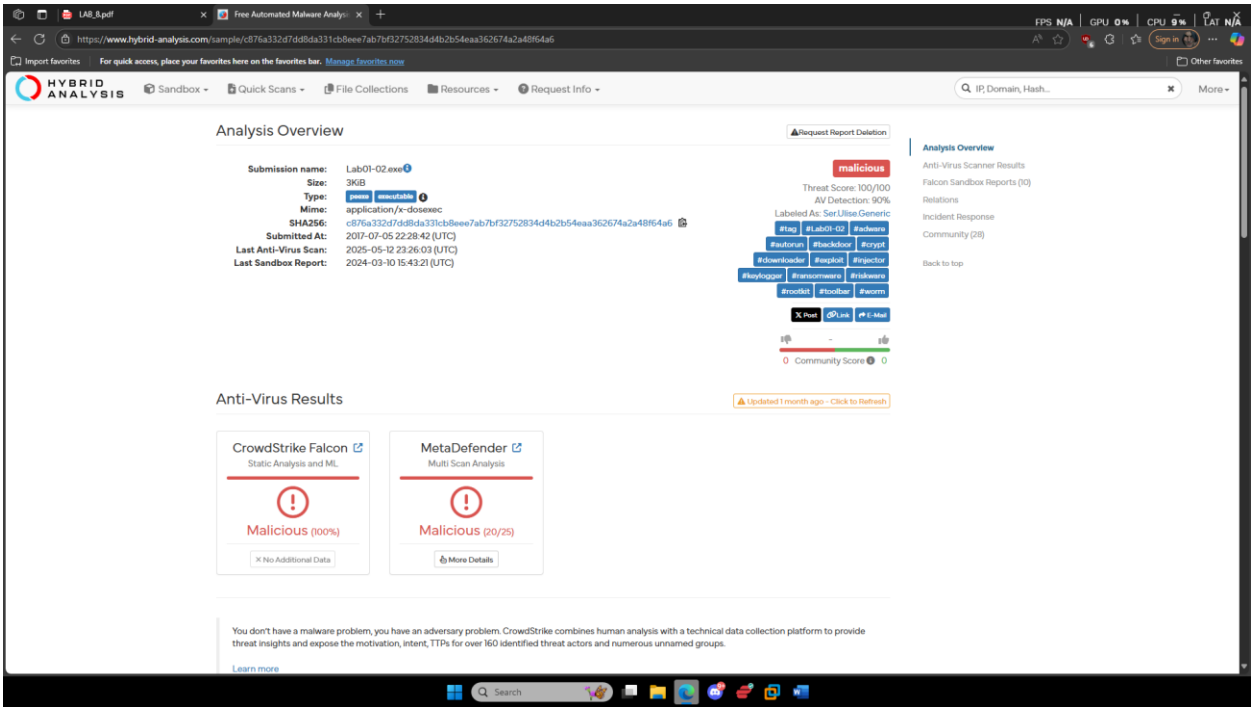

PhucPXHE194343-Win2008-DC - VMware Workstation
str1exe.txt - Notepad
IsBadReadPtr
MapViewOfFile
CreateFileMappingA
CreateFileA
FindClose
FindNextFileA
FindFirstFileA
CopyFileA
KERNEL32.dll
malloc
exit
MSVCRT.dll
_exit
_XcptFilter
__p___initenv
__getmainargs
_initterm
__setusermatherr
_adjust_fdiv
__p__commode
__p__fmode
__set_app_type
_except_handler3
_controlfp
_stricmp
kernel32.dll
kernel32.dll
.exe
C:*
C:\windows\system32\kernel32.dll
Kernel32.
Lab01-01.dll
C:\Windows\System32\kernel32.dll
WARNING_THIS_WILL_DESTROY_YOUR_MACHINE

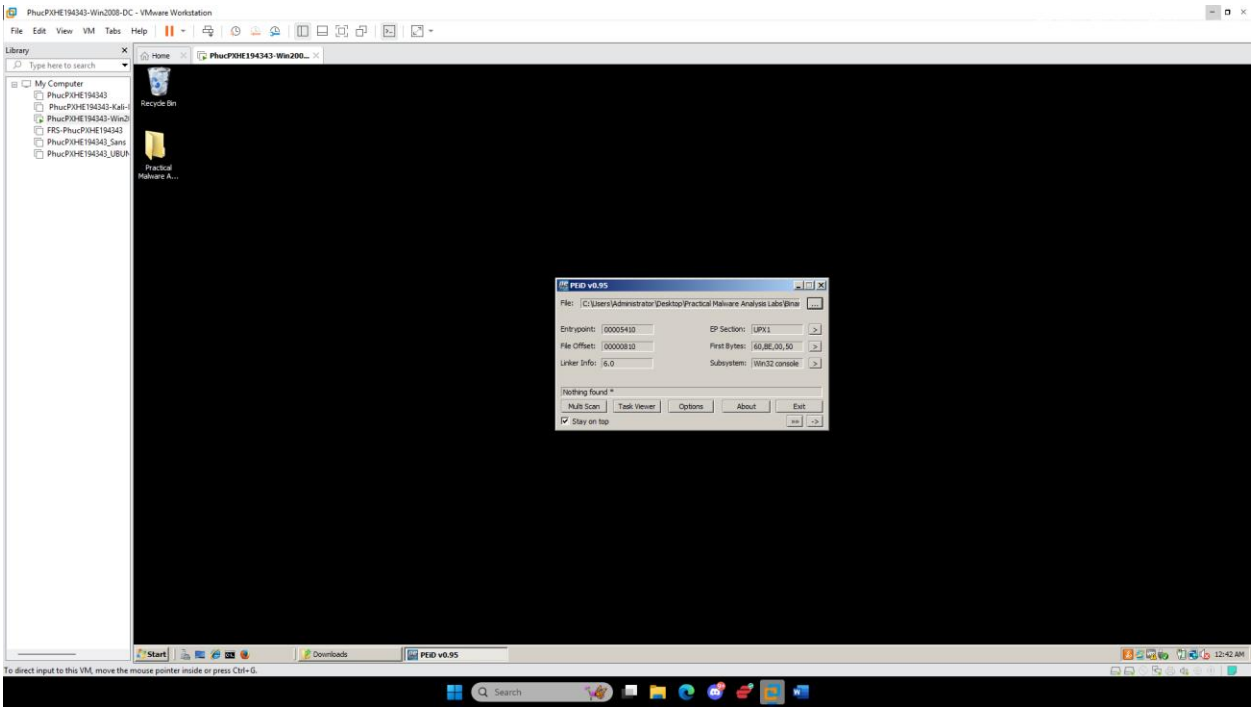

PhucPXHE194343-Win2008-DC - VMware Workstation
str1dll.txt - Notepad
u7h
%d
Y^j
=X
WVS
WVS
NWVS
u7WPS
u&WVS
WVS
_^[]
%
CloseHandle
Sleep
CreateProcessA
CreateMutexA
OpenMutexA
KERNEL32.dll
WS2_32.dll
strncmp
MSVCRT.dll
free
_initterm
malloc
_adjust_fdiv
exec
sleep
hello
127.26.152.13
SADFHUHF
/QIO[OhOpO
141G1[11
1Y2a2g2r2
3!3j3

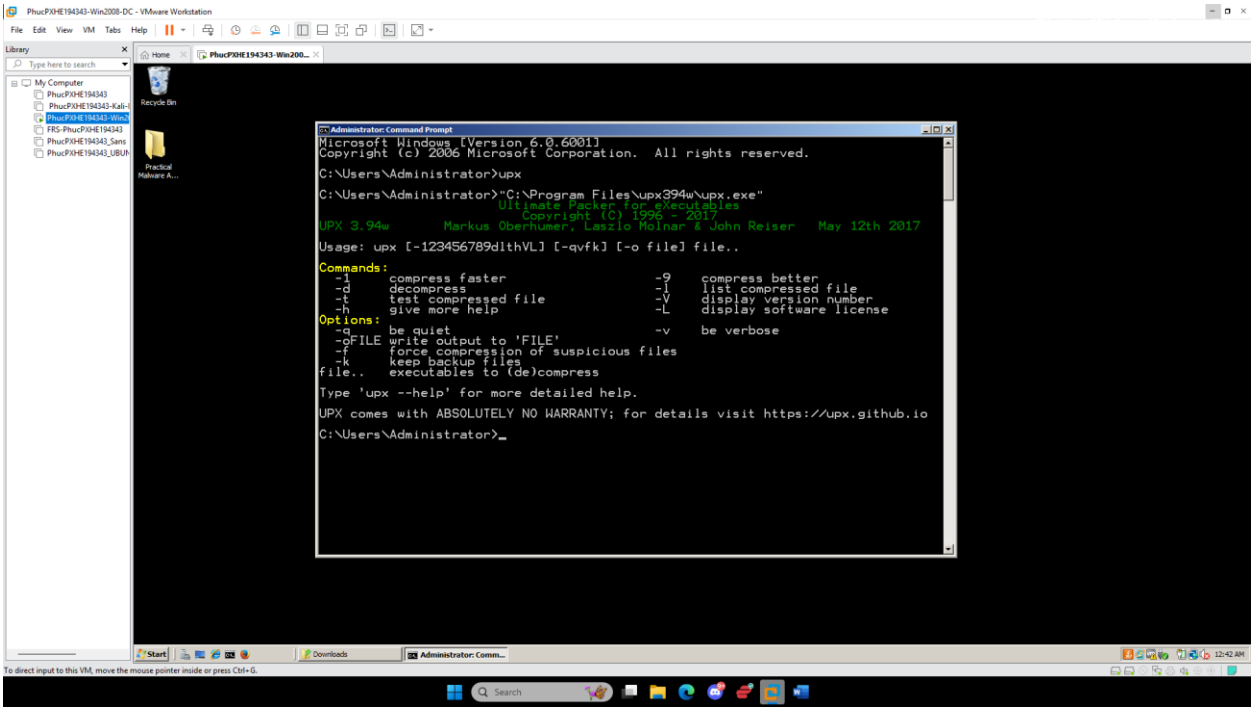

PhucPXHE194343-Win2008-DC - VMware Workstation
Dependency Walker - [Lab01-01.exe]
LAB01-01.EXE
KERNEL32.DLL
MSVCRT.DLL
NTDLL.DLL

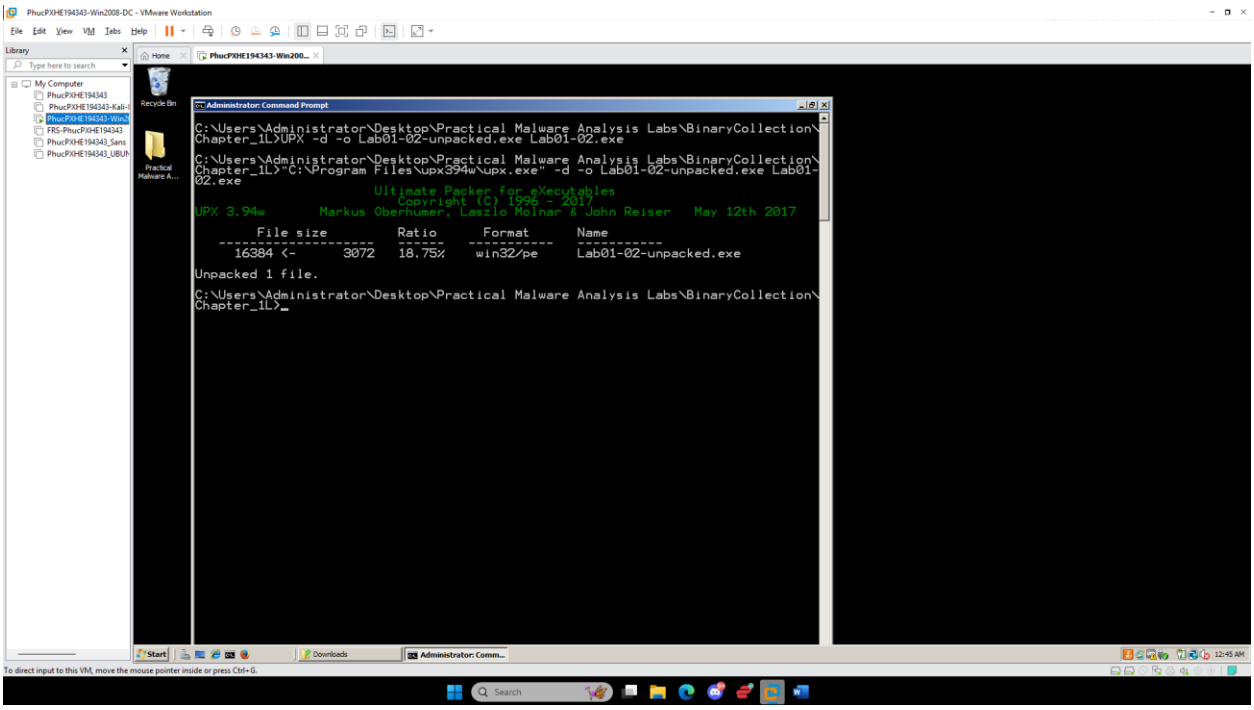

PhucPXHE194343-Win2008-DC - VMware Workstation
Dependency Walker - [Lab01-01.exe]
LAB01-01.EXE
KERNEL32.DLL
MSVCRT.DLL
NTDLL.DLL

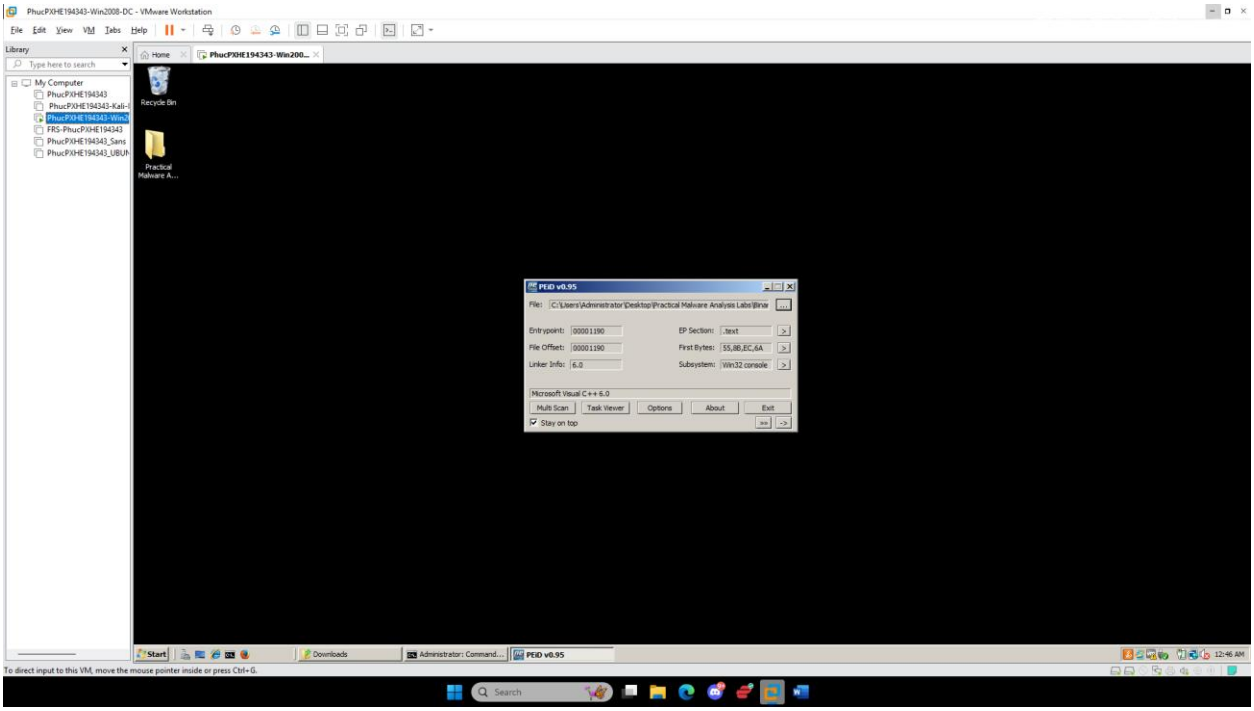

PhucPXHE194343-Win2008-DC - VMware Workstation
Dependency Walker - [Lab01-01.dll]
LAB01-01.DLL
KERNEL32.DLL
WS2_32.DLL
MSVCRT.DLL
Warning: At least one delay-load dependency module was not found.
Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.

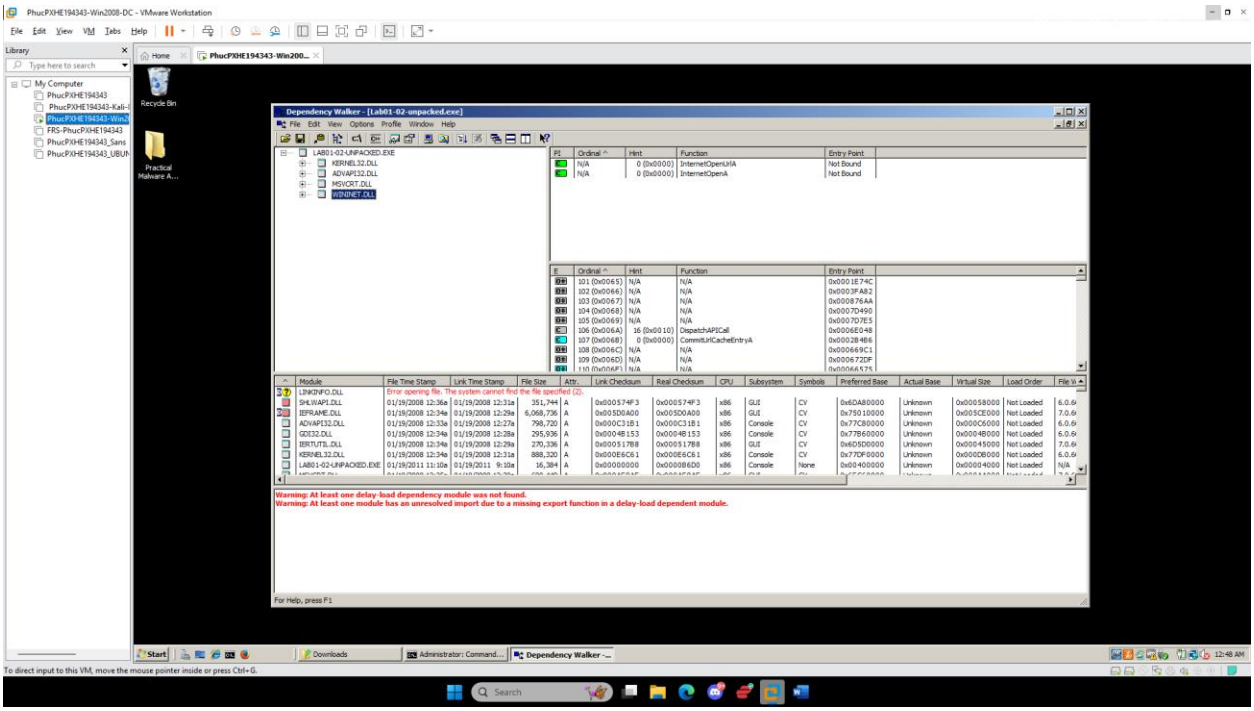

HYBRID ANALYSIS
Sandbox
Quick Scans
File Collections
Resources
Request Info
IP, Domain, Hash...
More
Analysis Overview
Request Report Deletion
Submission name: Lab01-02.exe
Size: 3KiB
Type: peexe executable
Mime: application/x-dosexec
SHA256: c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6
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
Post Link E-Mail
0 Community Score 0
Analysis Overview
Anti-Virus Scanner Results
Falcon Sandbox Reports (10)
Relations
Incident Response
Community (28)
Back to top
Anti-Virus Results
Updated 1 month ago - Click to Refresh
CrowdStrike Falcon
Static Analysis and ML
Malicious (100%)
No Additional Data
MetaDefender
Multi Scan Analysis
Malicious (20/25)
More Details
You don't have a malware problem, you have an adversary problem. CrowdStrike combines human analysis with a technical data collection platform to provide threat insights and expose the motivation, intent, TTPs for over 160 identified threat actors and numerous unnamed groups.
Learn more

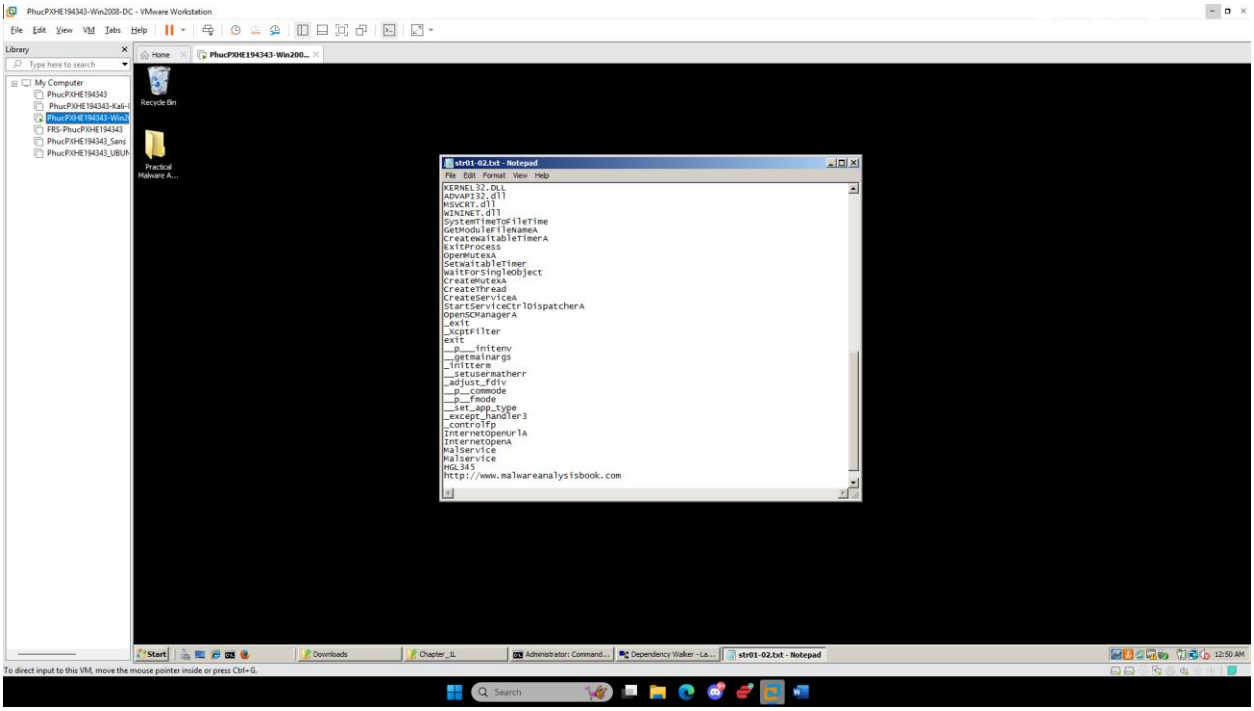

PhucPXHE194343-Win2008-DC - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
PhucPXHE194343
PhucPXHE194343-Win200...
Recycle Bin
Practical Malware A...
PEiD v0.95
File: C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\Bina
Entrypoint: 00005410
EP Section: UPX1
File Offset: 00000810
First Bytes: 60,BE,00,50
Linker Info: 6.0
Subsystem: Win32 console
Nothing found *
Multi Scan
Task Viewer
Options
About
Exit
Stay on top
Start
Downloads
PEiD v0.95
12:42 AM
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

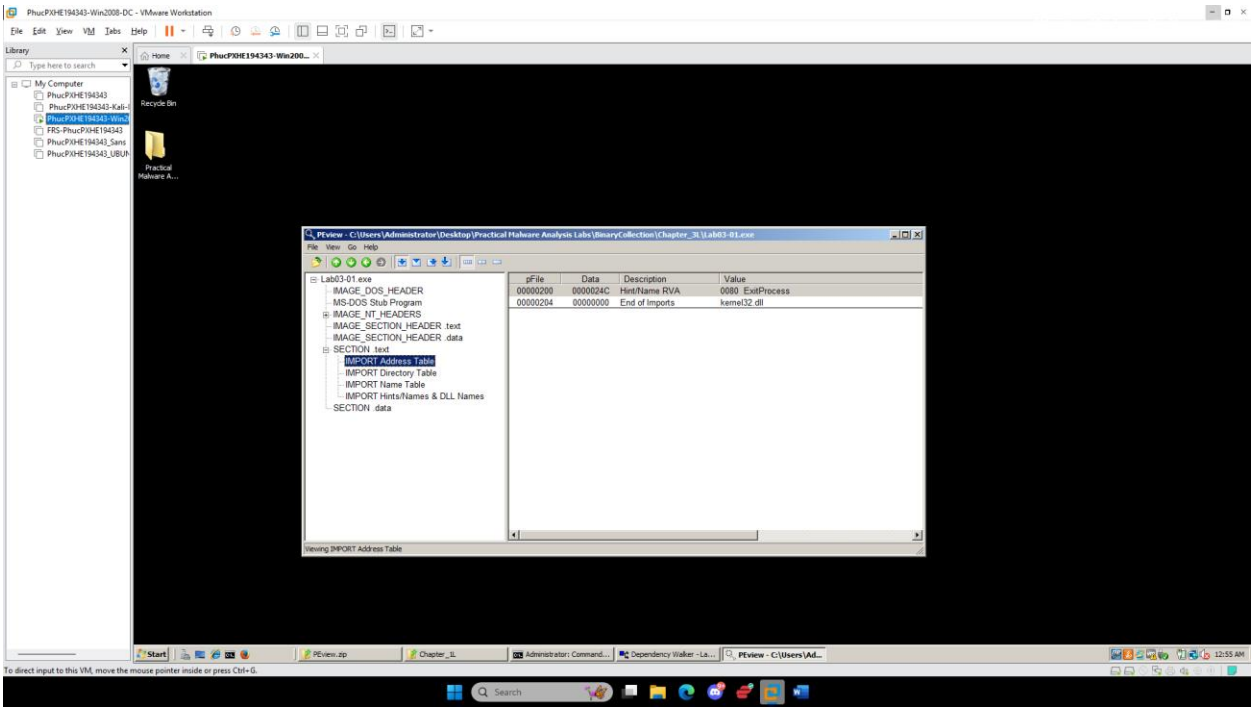

PhucPXHE194343-Win2008-DC - VMware Workstation
Administrator: Command Prompt
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>upx
C:\Users\Administrator>"C:\Program Files\upx394w\upx.exe"
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2017
UPX 3.94w Markus Oberhumer, Laszlo Molnar & John Reiser May 12th 2017
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>_

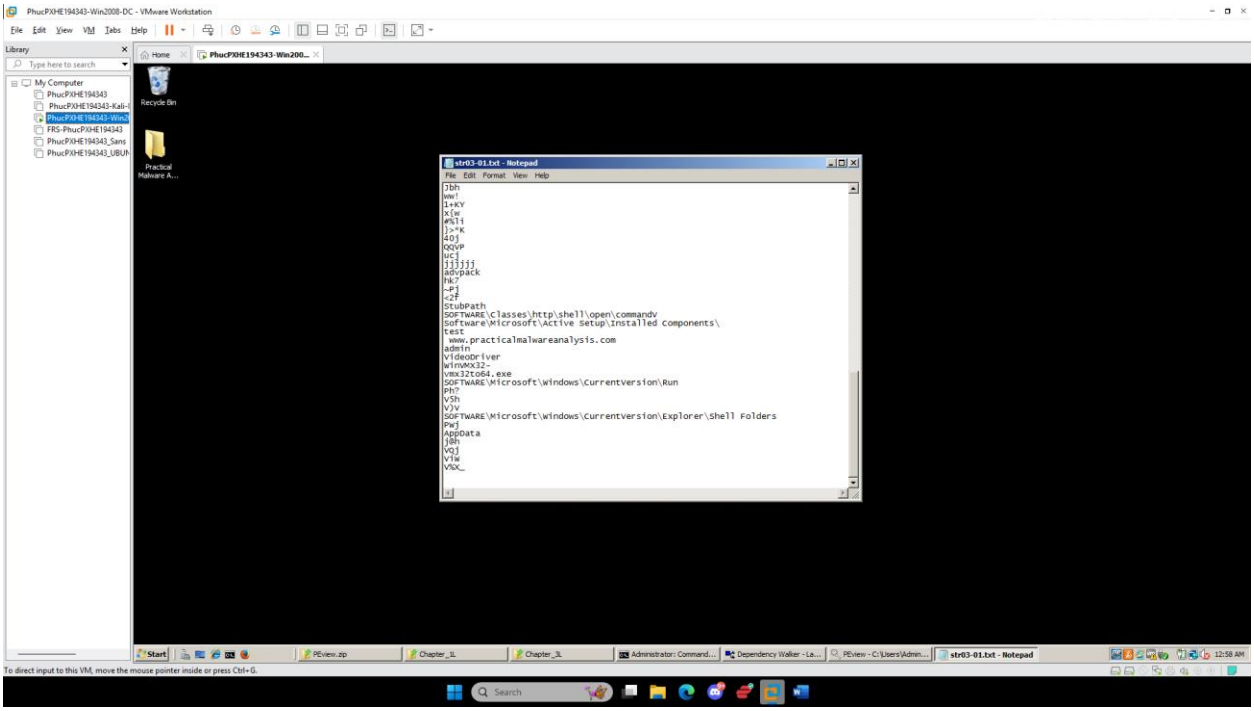

PhucPXHE194343-Win2008-DC - VMware Workstation
Administrator: Command Prompt
C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L>UPX -d -o Lab01-02-unpacked.exe Lab01-02.exe
C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L>"C:\Program Files\upx394w\upx.exe" -d -o Lab01-02-unpacked.exe Lab01-02.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\BinaryCollection\Chapter_1L>_

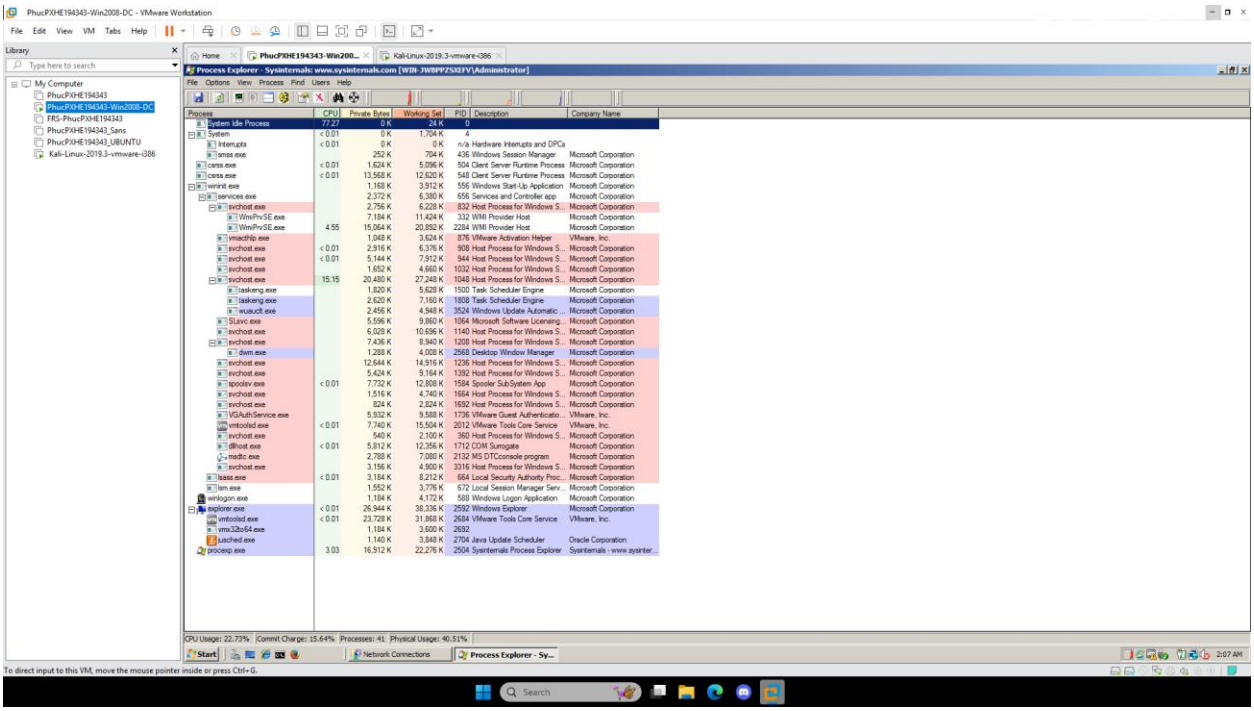

PhucPXHE194343-Win2008-DC - VMware Workstation
PEiD v0.95
Recycle Bin
Practical Malware A...

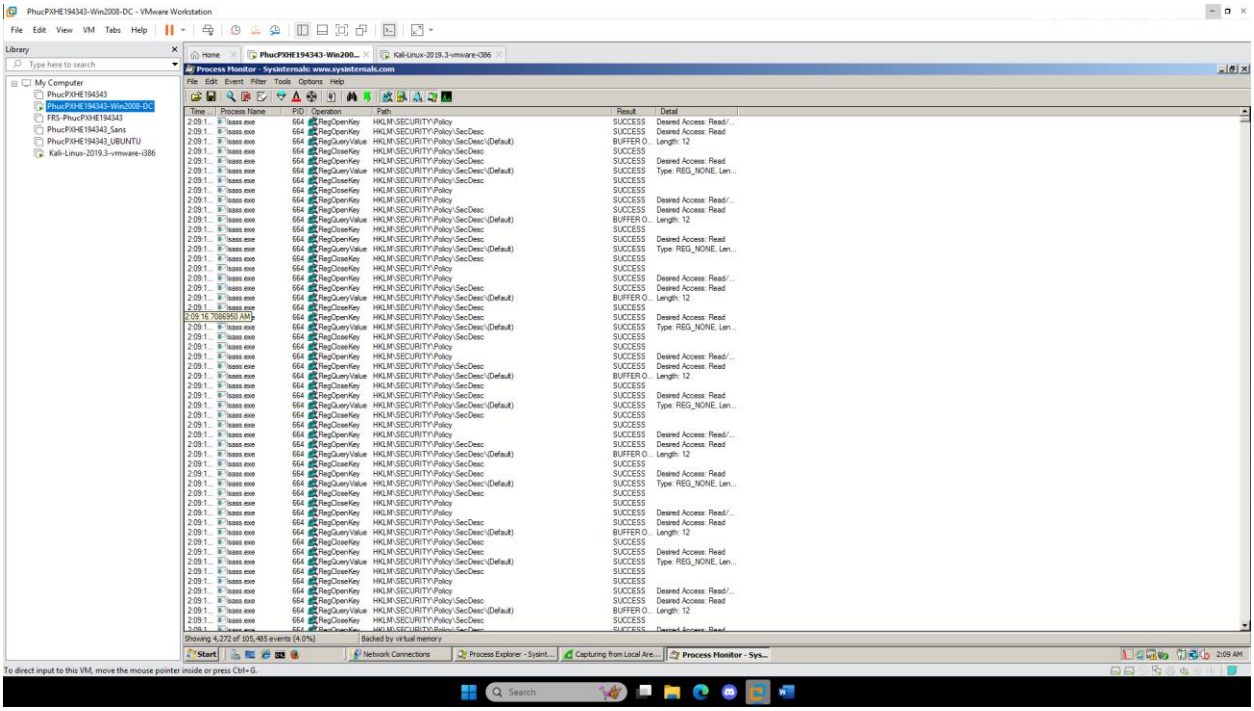

PhucPXHE194343-Win2008-DC - VMware Workstation
Dependency Walker - [Lab01-02-unpacked.exe]
Recycle Bin
Practical Malware A...

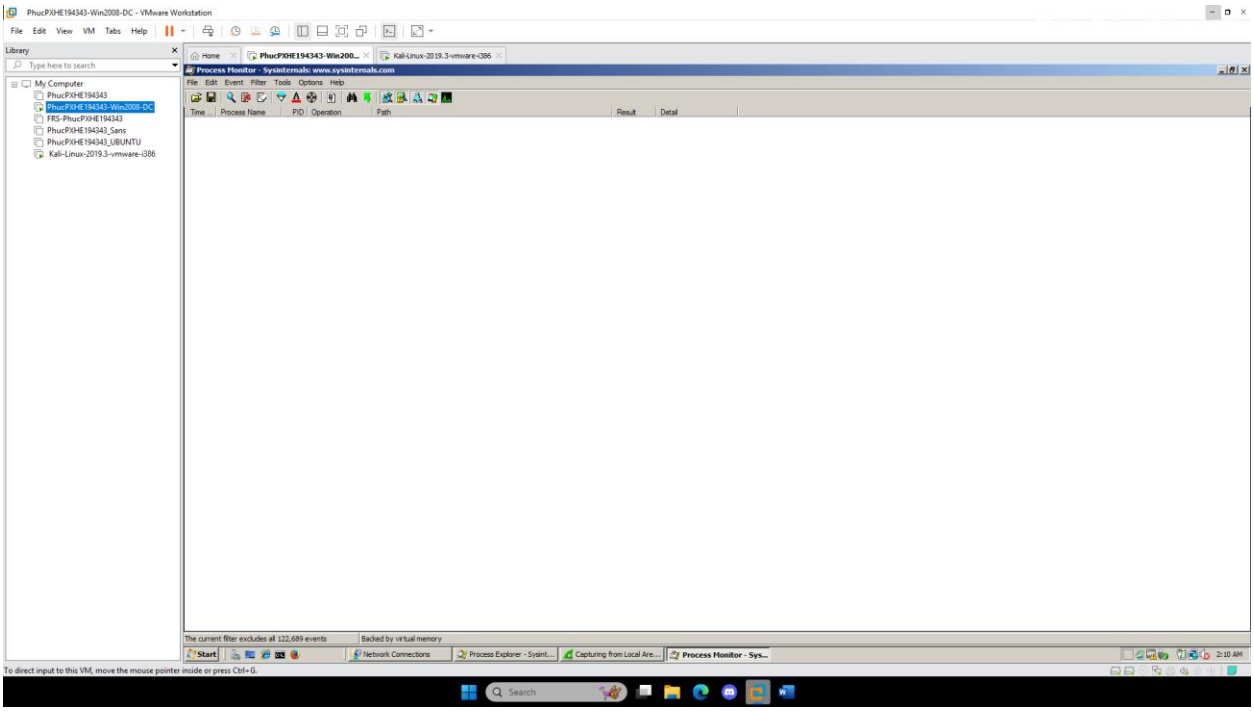

PhucPXHE194343-Win2008-DC - VMware Workstation
str01-02.txt - Notepad
KERNEL32.DLL
ADVAPI32.dll
MSVCRT.dll
WININET.dll
SystemTimeToFileTime
GetModuleFileNameA
CreatewaitableTimerA
ExitProcess
OpenMutexA
SetwaitableTimer
WaitForSingleObject
CreateMutexA
CreateThread
CreateServiceA
StartServiceCtrlDispatcherA
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

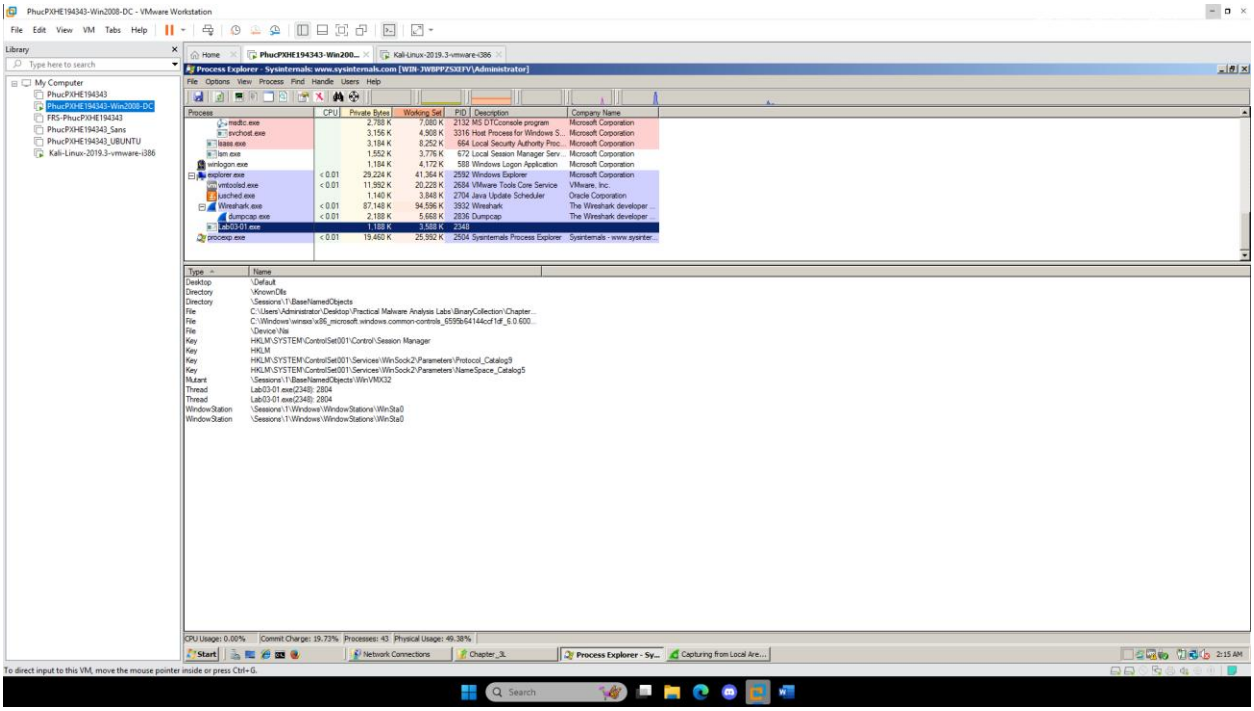

PhucPXHE194343-Win2008-DC - VMware Workstation
PEview - C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_3L\Lab03-01.exe
Lab03-01.exe
IMAGE_DOS_HEADER
MS-DOS Stub Program
IMAGE_NT_HEADERS
IMAGE_SECTION_HEADER .text
IMAGE_SECTION_HEADER .data
SECTION .text
IMPORT 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

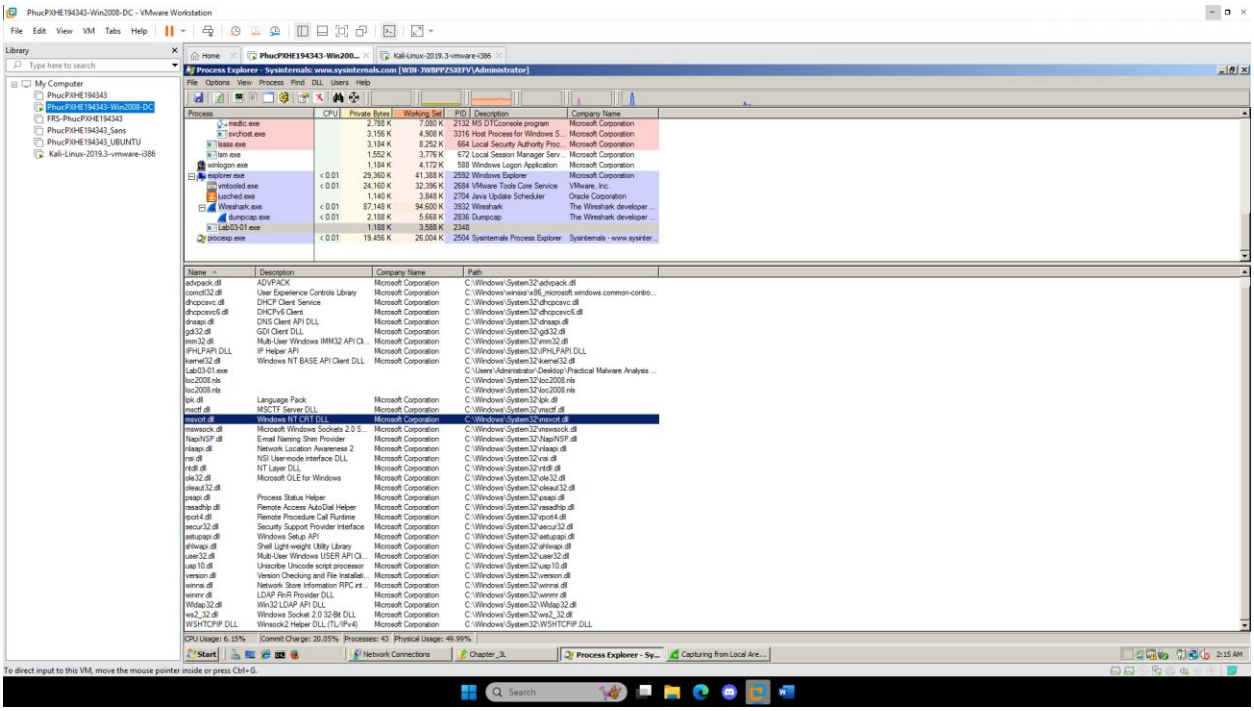

PhucPXHE194343-Win2008-DC - VMware Workstation
str03-01.txt - Notepad
Jbh
ww!
1+KY
x{w
#%1i
]>*K
4oj
QQVP
Hcj
jjjjjj
advpack
hk?
-Pj
<2f
StubPath
SOFTWARE\Classes\http\shell\open\commandv
Software\Microsoft\Active Setup\Installed Components\
test
www.practicalmalwareanalysis.com
admin
VideoDriver
WinVMX32-
vmx32to64.exe
SOFTWARE\Microsoft\Windows\Currentversion\Run
Ph?
v5h
VjV
SOFTWARE\Microsoft\Windows\Currentversion\Explorer\Shell Folders
Pwj
AppData
jBh
Vqj
V!w
V5X_

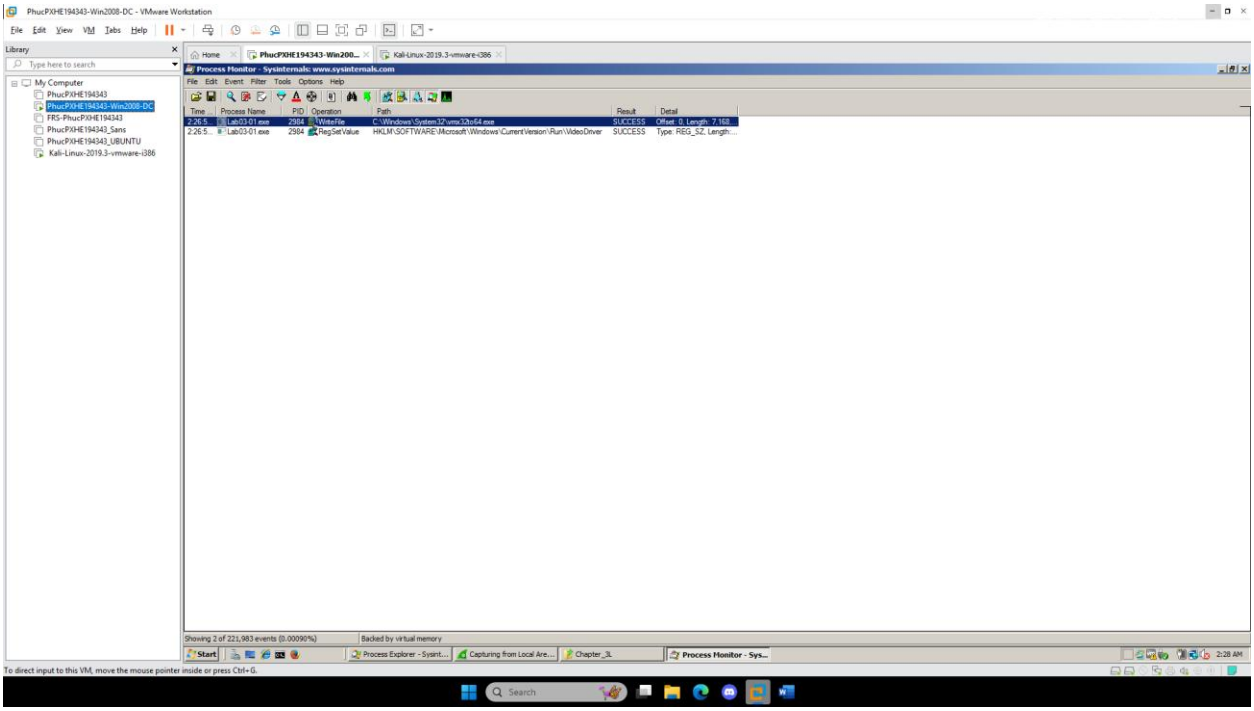

PhucPXHE194343-Win2008-DC - VMware Workstation
Process Explorer - Sysinternals: www.sysinternals.com [WIN-JW8PPZS3IFV\Administrator]

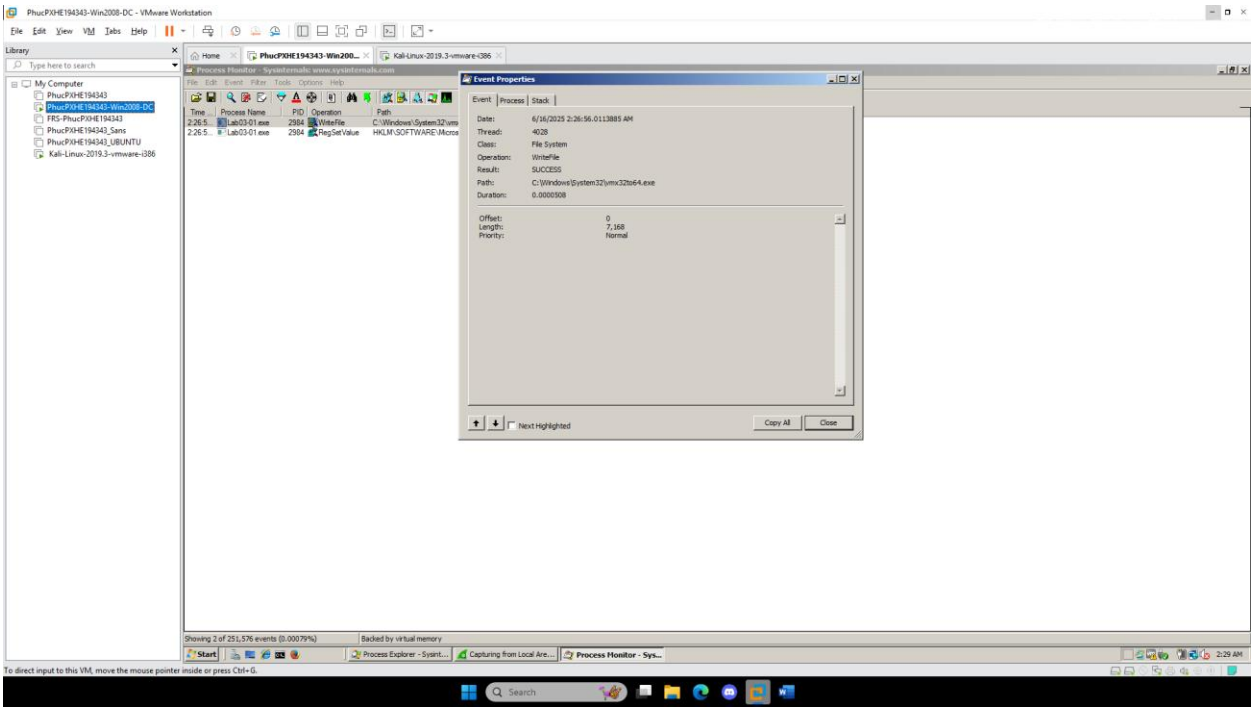

PhucPXHE194343-Win2008-DC - VMware Workstation
Process Monitor - Sysinternals: www.sysinternals.com
Showing 4,272 of 105,485 events (4.0%)
Backed by virtual memory

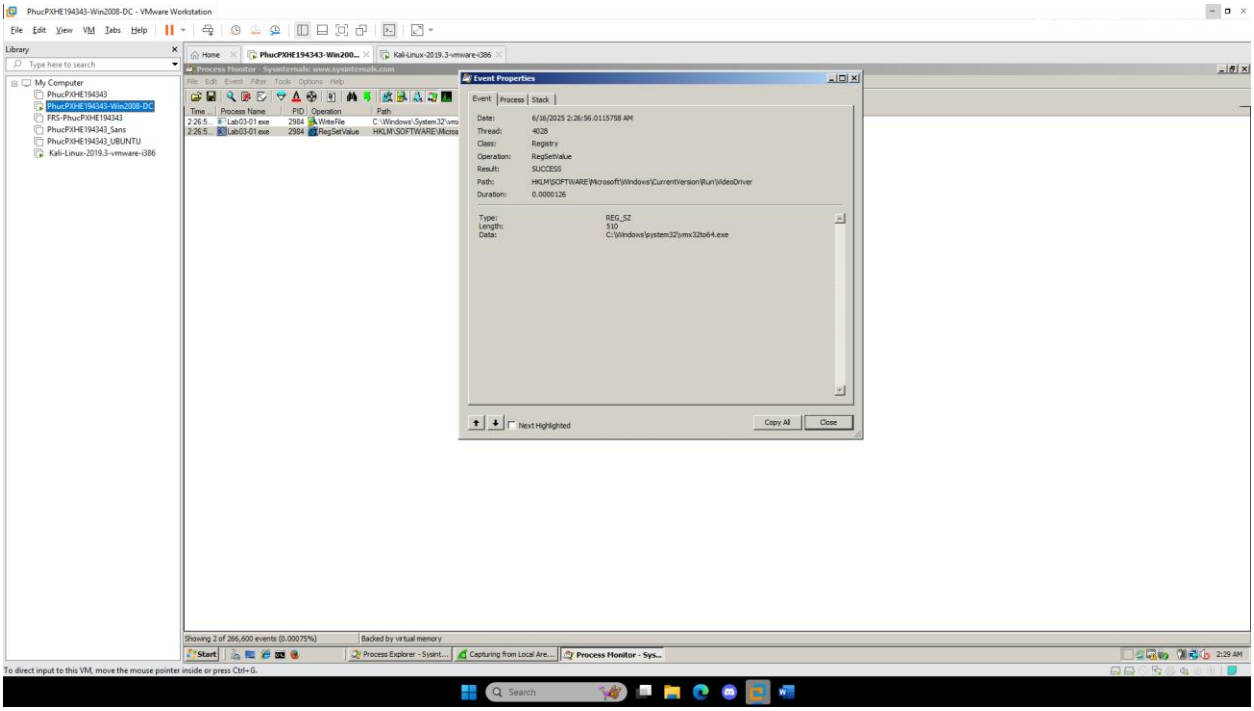

PhucPXHE194343-Win2008-DC - VMware Workstation
Process Monitor - Sysinternals: www.sysinternals.com
The current filter excludes all 122,689 events
Backed by virtual memory

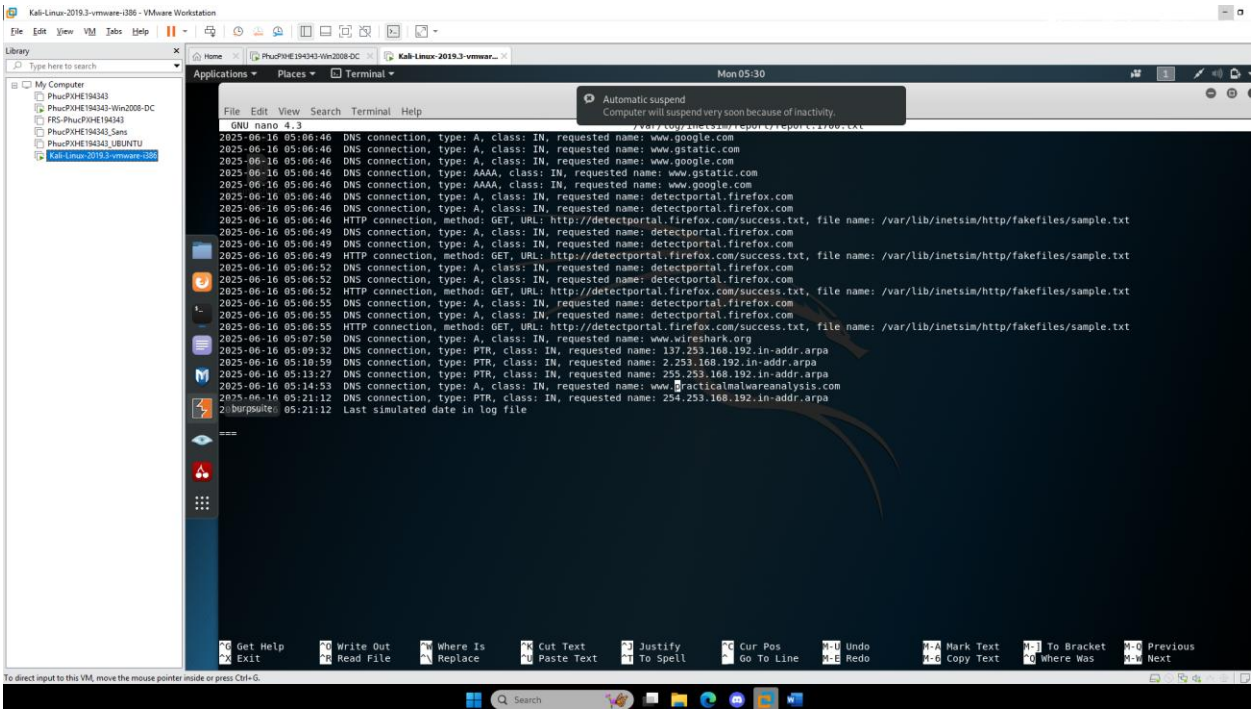

PhucPXHE194343-Win2008-DC - VMware Workstation
Process Explorer - Sysinternals: www.sysinternals.com [WIN-JW8PPZS3IFV\Administrator]


PhucPXHE194343-Win2008-DC - VMware Workstation
Process Explorer - Sysinternals: www.sysinternals.com [WIN-JW8PPZS3IFV\Administrator]


PhucPXHE194343-Win2008-DC - VMware Workstation
Process Monitor - Sysinternals: www.sysinternals.com
Lab03-01.exe
WriteFile
RegSetValue
Process Explorer - Sysint...
Capturing from Local Are...
Chapter_3L
Process Monitor - Sys...

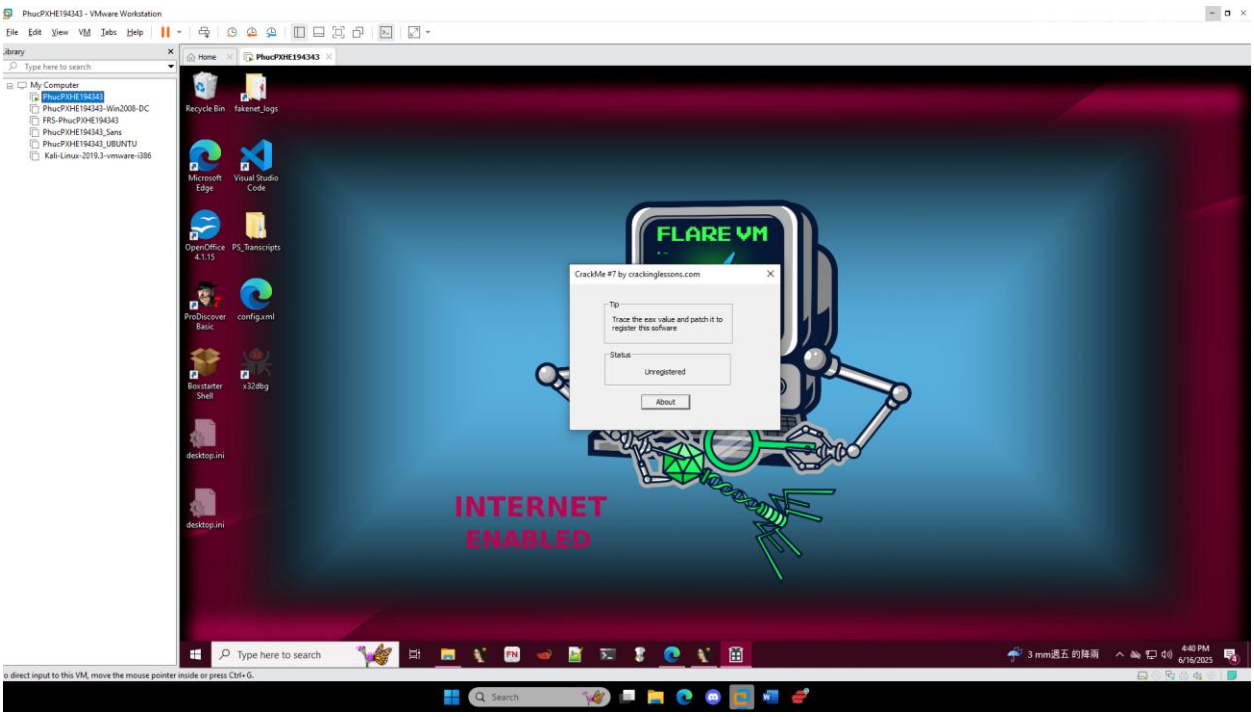

PhucPXHE194343-Win2008-DC - VMware Workstation
Event Properties
Event
Process
Stack
Date: 6/16/2025 2:26:56.0113885 AM
Thread: 4028
Class: File System
Operation: WriteFile
Result: SUCCESS
Path: C:\Windows\System32\vmx32to64.exe
Duration: 0.0000508
Offset: 0
Length: 7,168
Priority: Normal
Next Highlighted
Copy All
Close



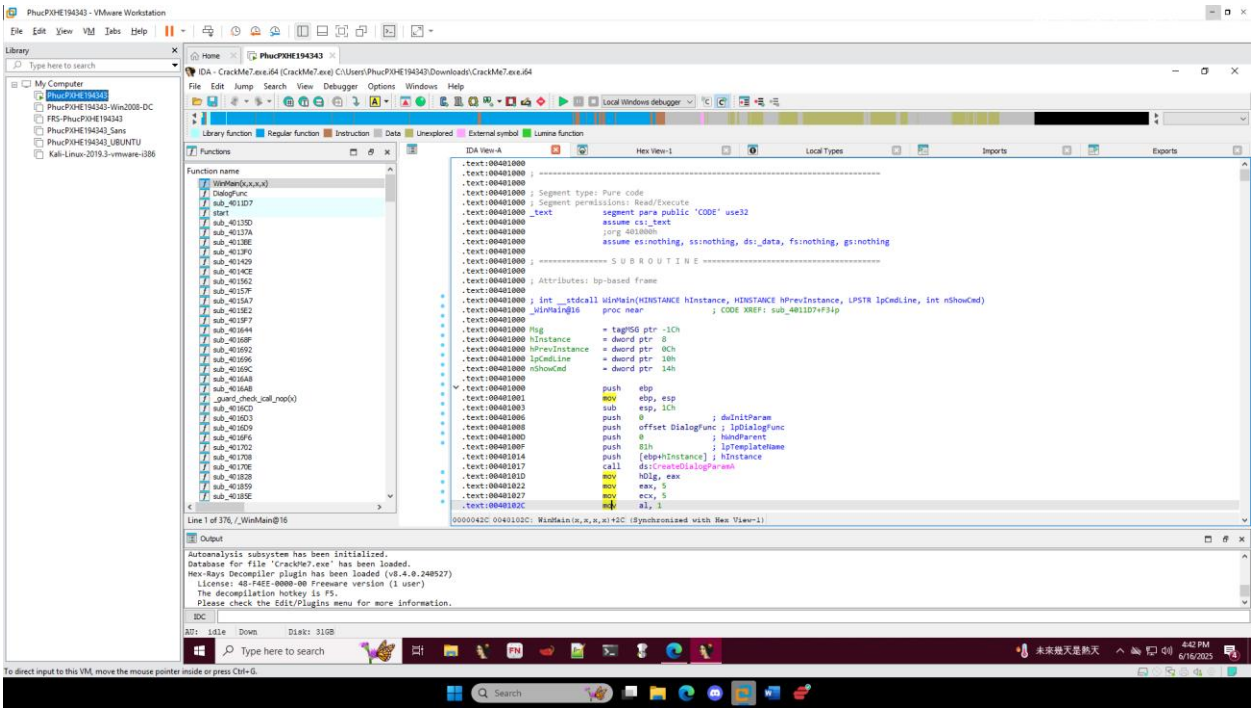


Crack Me 7

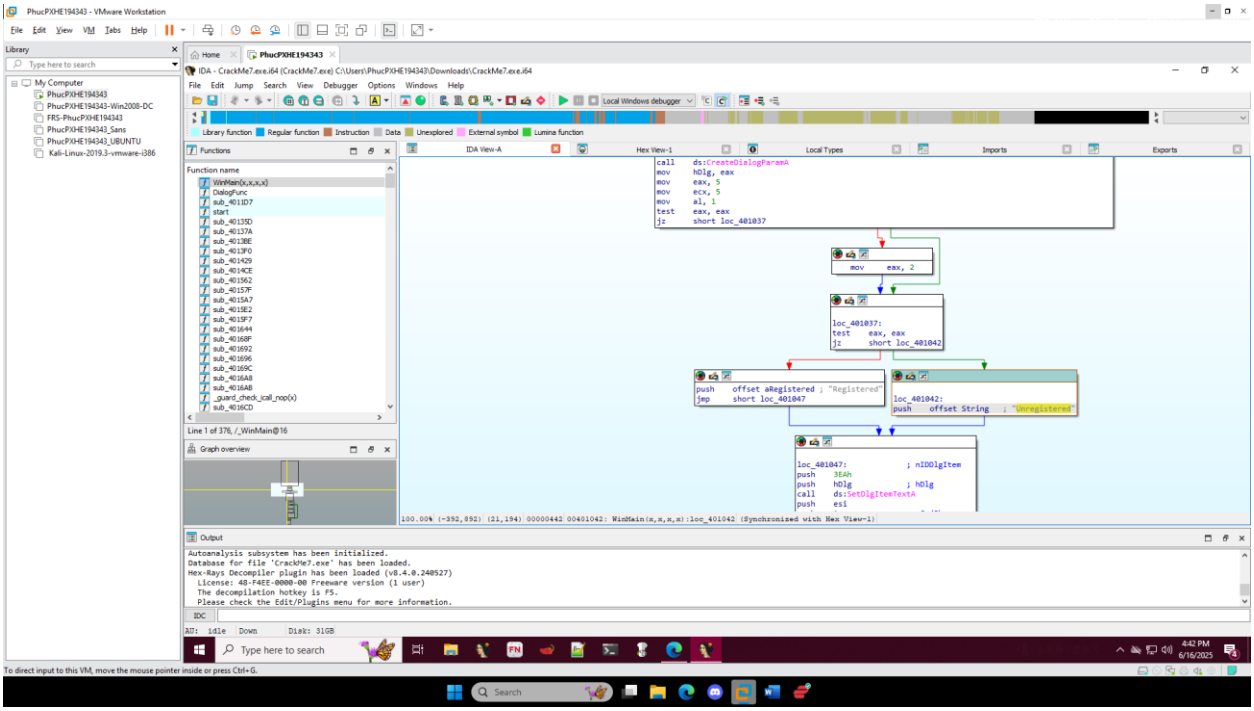
Step 1: Open the exe file to see any requirement



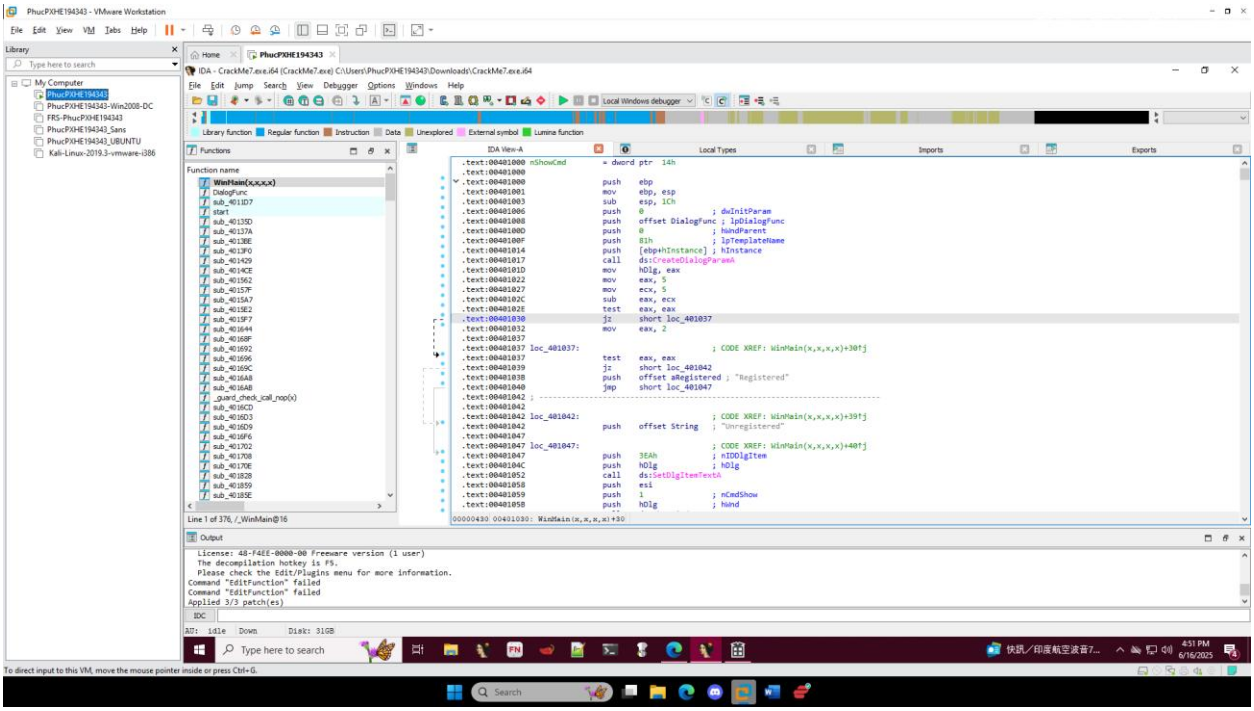
Step 2: Load the program into IDA for debugging



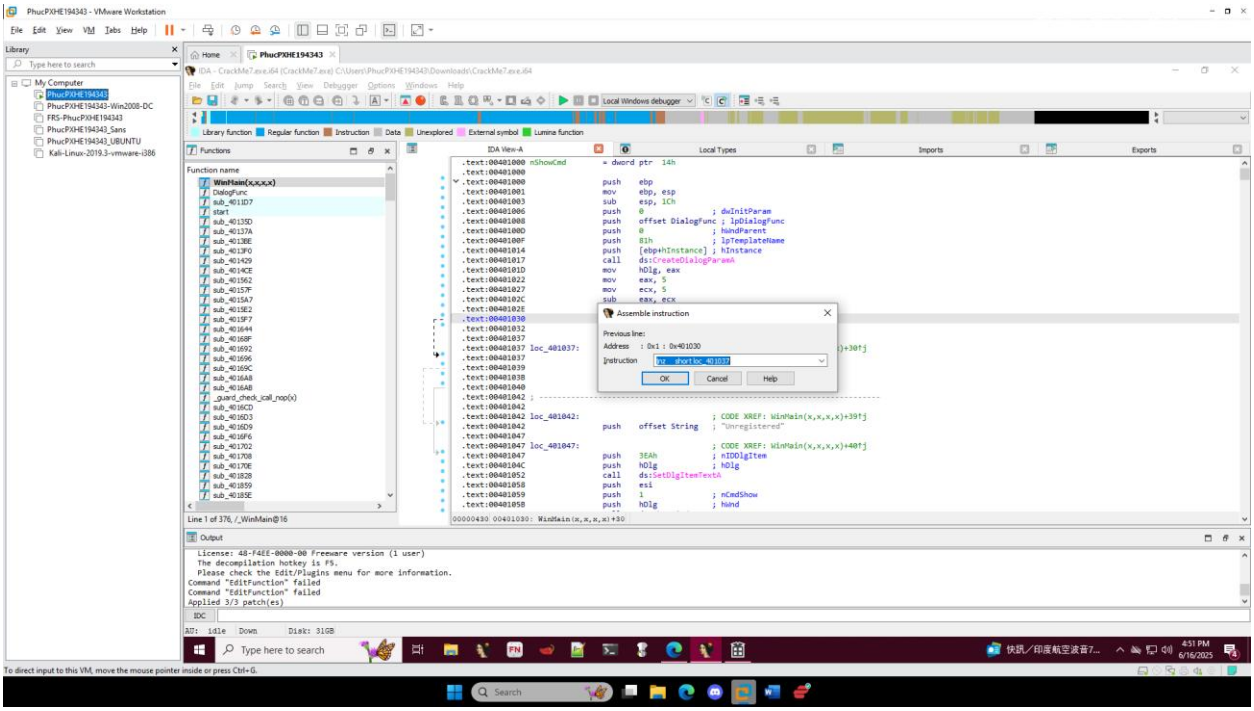
Step 3: Search for the string Unregistered and we found a diagram



Step 4: As we can see that the program show that the eax = 2, then the test eax will not equal 0, so the short loc_401042 will show unregistered. Change the command from jz to jnz to jump if not zero so the program will run the test eax, eax not equal zero



Step 5: Apply the edit and the patch



Step 6: We get the result that we desired