

Họ và tên: Trần Trí Dũng

Mã số sinh viên: HE190680

Lớp: IA1901

## Lab 8:

### 1. Basic Static Techniques

#### a. Lab01-01.exe

Upload the Lab01-01.exe and Lab01-01.dll files to <https://www.hybrid-analysis.com>:

The screenshot shows the Hybrid Analysis platform's analysis overview for the file Lab01-01.exe. Key details include:

- Submission name:** Lab01-01.exe
- Type:** PE32 executable
- SHA256:** 508908c917c5bd3fb9b1389f0eee5b39cd5910ae8370eb9ea838a0b327bd6fe47
- 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)

The analysis results section shows:

- CrowdStrike Falcon:** Malicious (100%)
- MetaDefender:** Malicious (19/25)

On the right side, there is a sidebar with various links and a social sharing section.

Free Automated Malware Analysis

<https://www.hybrid-analysis.com/samples/152e42c0dfad649bde399867e930b86c2a599e0d5d31b260393082268f2dbs>

Courses CTF FTP Tu hoc Tools Write up Lưu trú Courses Online Catalog Learning Catalog Review GVATracker Go... Security Engineer Security Engineer (S... Security Consultant... The Cloud Resum... Privacy error

**HYBRID ANALYSIS**

Sandbox Quick Scans File Collections Resources Request Info

Analysis Overview

Submission name: Lab01-01.dll  
Size: 160KB  
Type: pedfi executable  
Miner: spdrbot-2023-09-01-00-00-00  
SHA256: f52e42c0dfad649bde399867e930b86c2a599e0d5d31b260393082268f2dbs  
Submitted At: 2024-07-05 20:39:27 UTC  
Last Anti-Virus Scan: 2024-12-02 03:40:23 (UTC)  
Last Sandbox Report: 2024-05-30 02:10:31 (UTC)

Request Report Deletion

malicious

Threat Score: 100/100  
AV Detection: 83%  
Labeled As: Doina Generic

#tag #installone #upatre #backdoor #crypt #downloader #injector #ransomware #riskware #worm

X Post ⌂ Link E-Mail

Community Score: 0

Analysis Overview

Anti-Virus Scanner Results

Falcon Sandbox Reports (12)  
Relations  
Incident Response  
Community (24)  
Back to top

Anti-Virus Results

CrowdStrike Falcon Static Analysis and ML  
Malicious (100%)  
X No Additional Data

MetaDefender Multi Scan Analysis  
Malicious (16/24)  
More Details

Updated 6 months ago - Click to Refresh

CrowdStrike is the first to integrate the tools used by world-class cyber incident investigators into an endpoint protection platform. CrowdStrike Falcon Intelligence includes the same sandboxing technology used in hybrid-analysis.com, to investigate threats in minutes, not hours.

Learn more

File View Go Help

Windows 10 Kali Linux 2019.3-vmware-1386 Win2008-DC

11:00 AM 6/8/2025

Open the files in PEview:

PEview - C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter\_11\Lab01-01.exe

File View Go Help

Lab01-01.exe

pFile	Data	Description	Value
000000EC	014C	Machine	IMAGE_FILE_MACHINE_I386
000000EE	0003	Number of Sections	
000000F0	4000003	Time Date Stamp	2010/12/19 Sun 16:16:19 UTC
000000F2	00000000	Pointers to Symbol Table	
000000F8	00000000	Number of Symbols	
000000FC	00E3	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

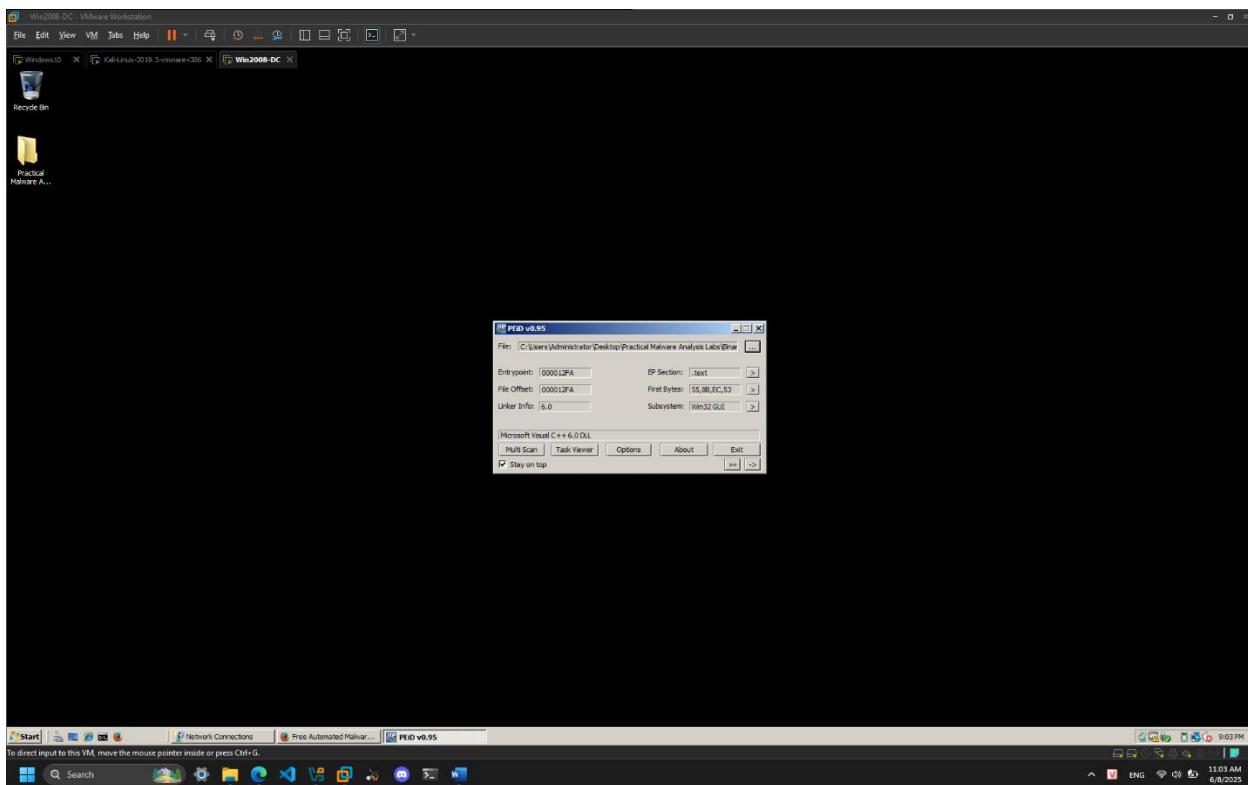
Start Network Connections Free Automated Malware Analysis PEview - C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter\_11\Lab01-01.exe

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

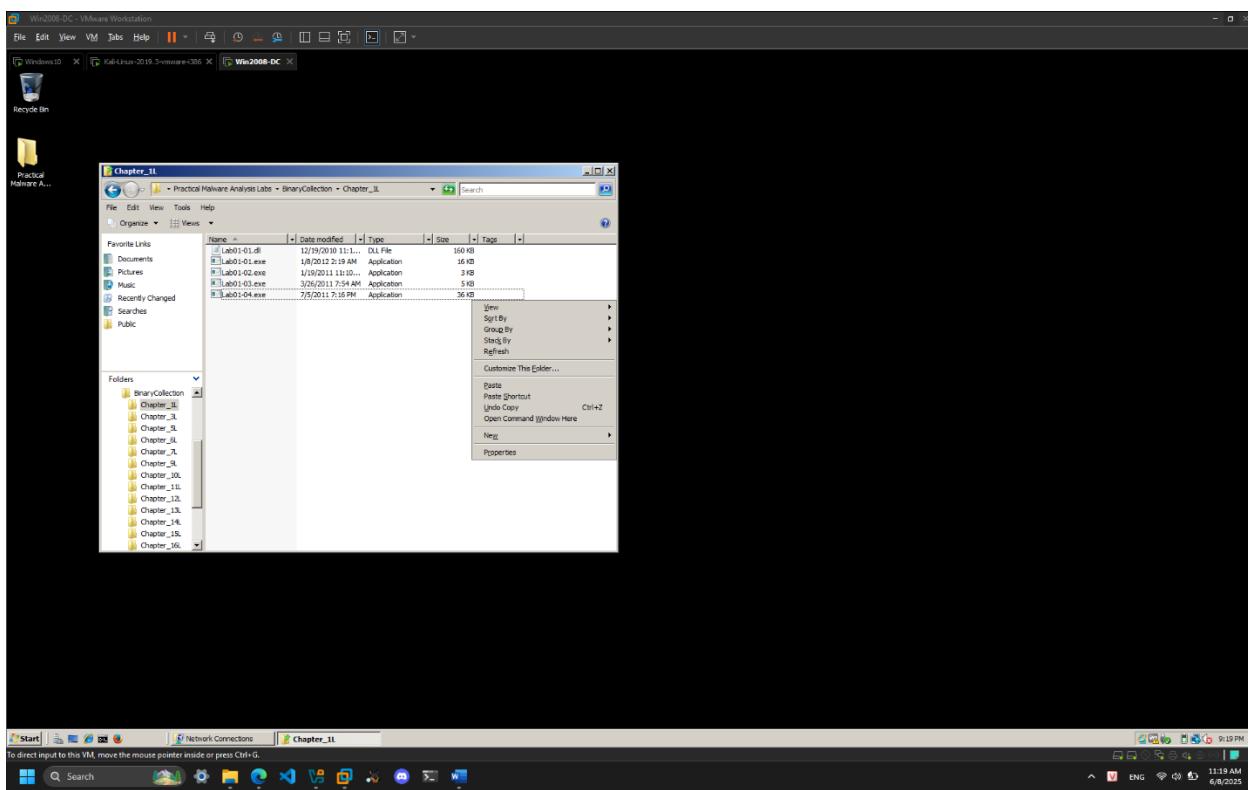
File View Go Help

11:02 AM 6/8/2025

Open the files in PEiD:



Right-click in the Chapter\_1L folder, and select Open Command Window Here:

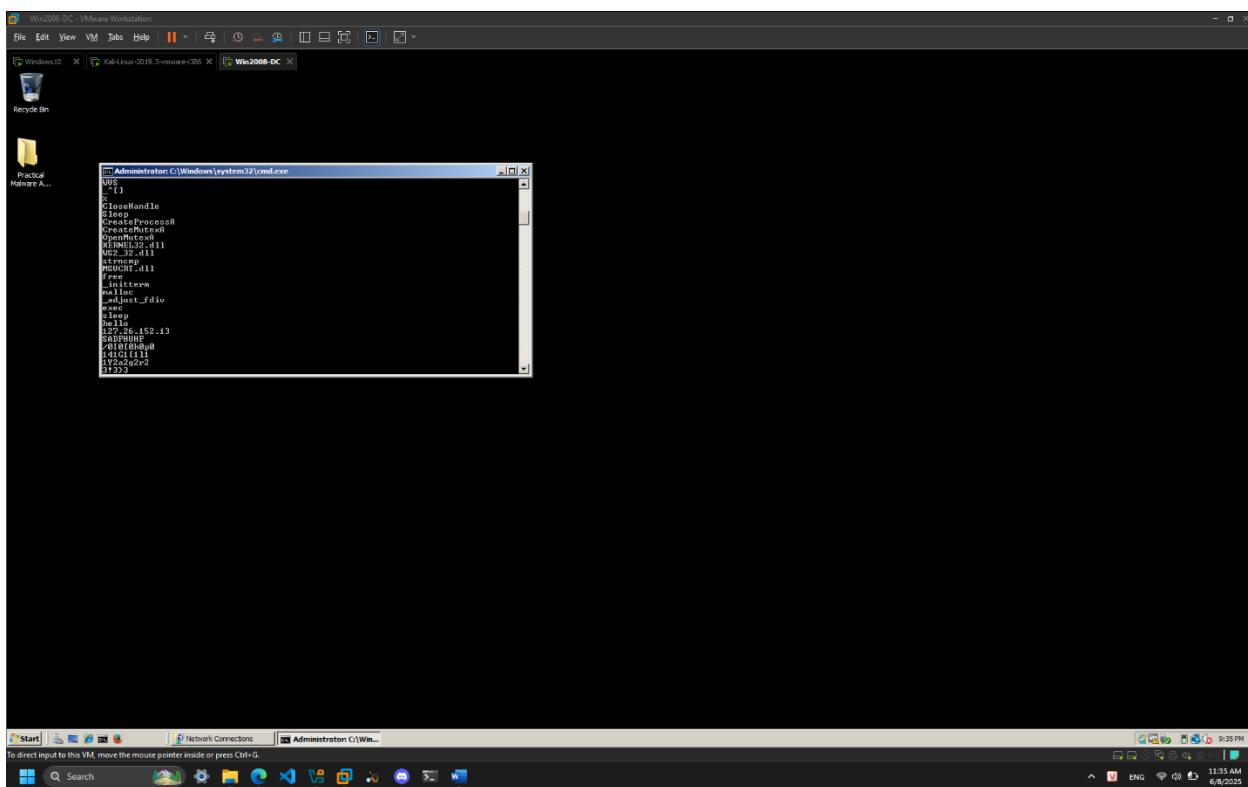


Collect the strings from the Lab01-01.exe file:

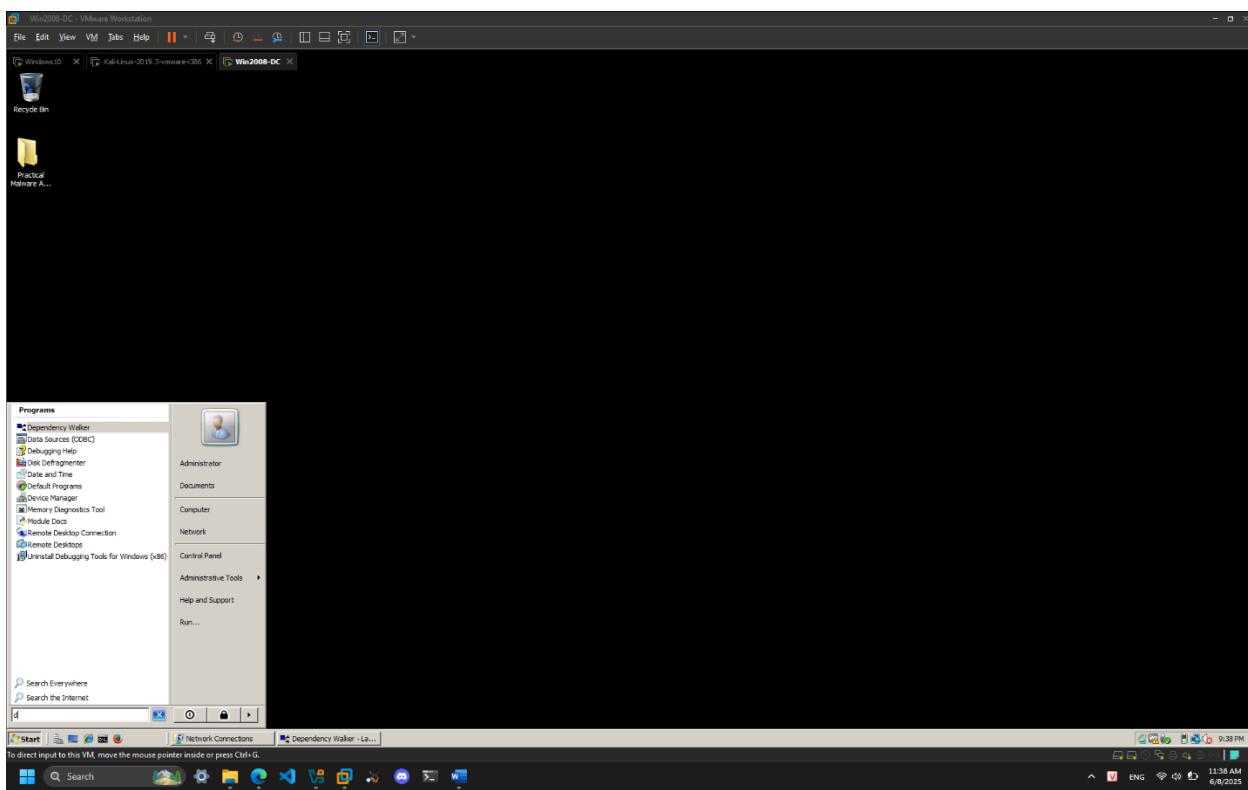
The image shows a Windows 2008 DC VMware Workstation desktop. The desktop has three windows open:

- A terminal window titled "Administrator: C:\Windows\system32\cmd.exe" showing the command "C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter\_1\Strings Lab01-01.exe > str1exe.txt". The output of the command is displayed below, listing various system DLLs and their functions.
- A desktop window showing the taskbar with icons for Start, Search, Network Connections, and other applications.
- A Notepad window titled "str1exe.txt - Notepad" displaying the collected strings from the command. The strings include file operations like UnmapViewOfFile, MapViewOfFile, CreateFileMappingA, OpenFile, FindClose, FindFirstFile, FindFirstFileA, CopyFileA, kernel32.dll, msal10c.dll, MSVCR7.dll, ext32.dll, \_setfilter, \_p\_linterv, \_setlargs, \_lnterm, \_setapphandler, \_setlastfd, \_p\_commode, \_setmode, \_set\_app\_type, \_except\_handler3, \_setobjtype, \_strictrt, kernel32.dll, kernel32.dll, .exe, C:\Windows\System32\kernel32.dll, Lab01-01.dll, C:\Windows\System32\kernel32.dll, and a warning message: "WARNING! THIS WILL DESTROY YOUR MACHINE".

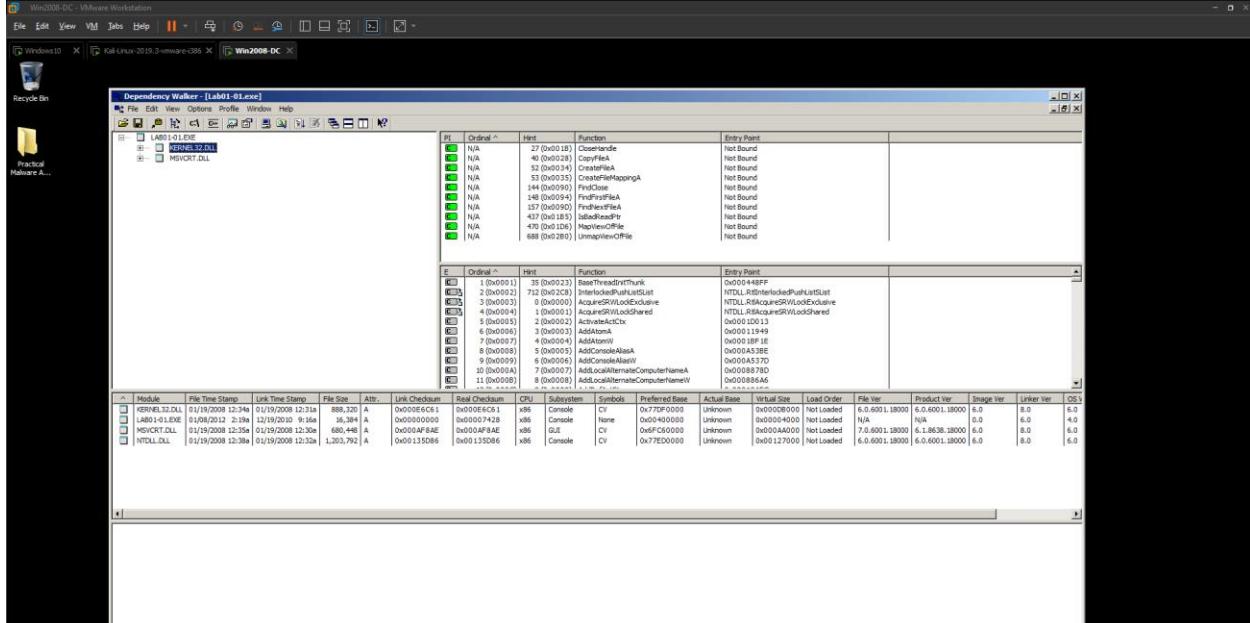
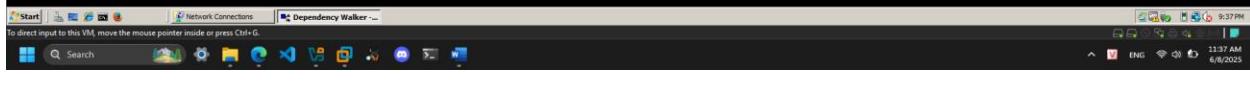
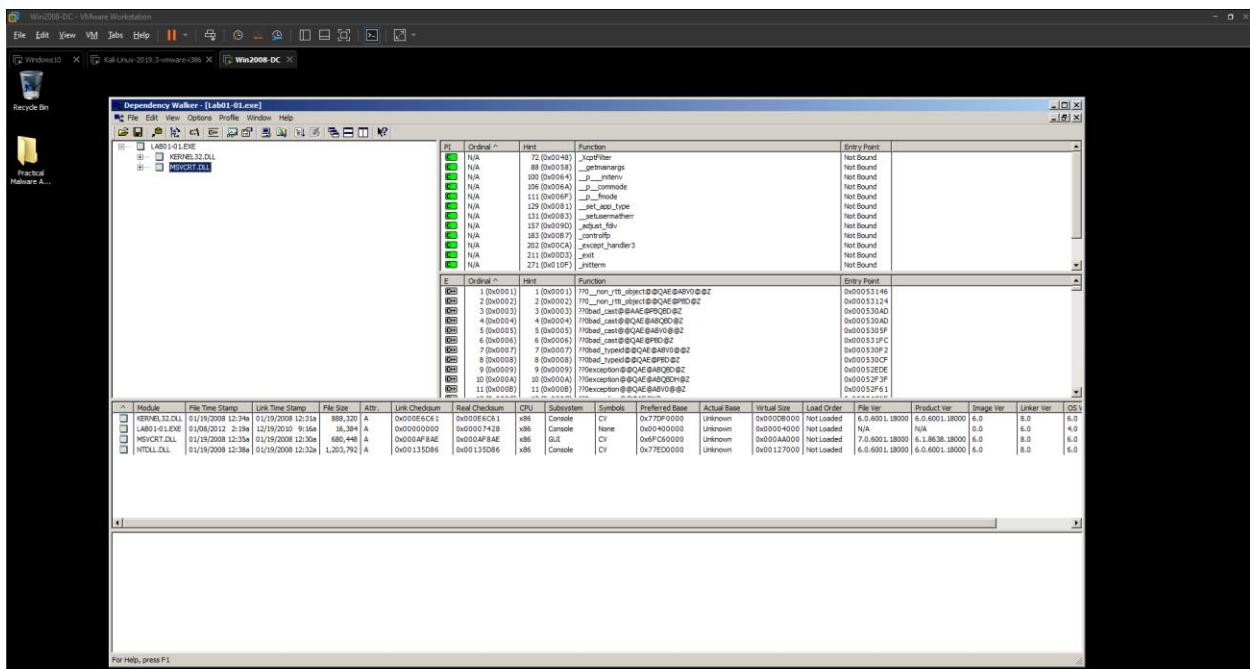
Look at the strings for Lab01-01.dll:



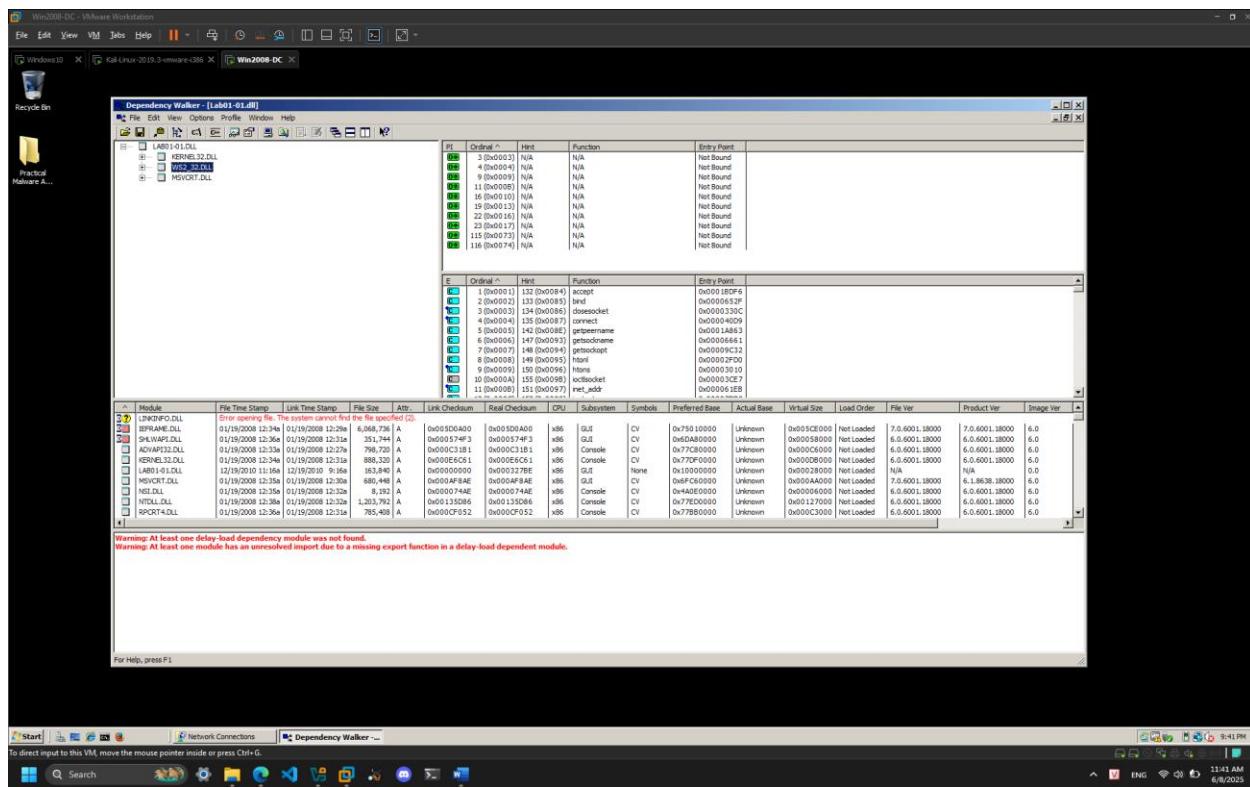
Open Dependency Walker:



## Open Lab01-01.exe in Dependency Walker:



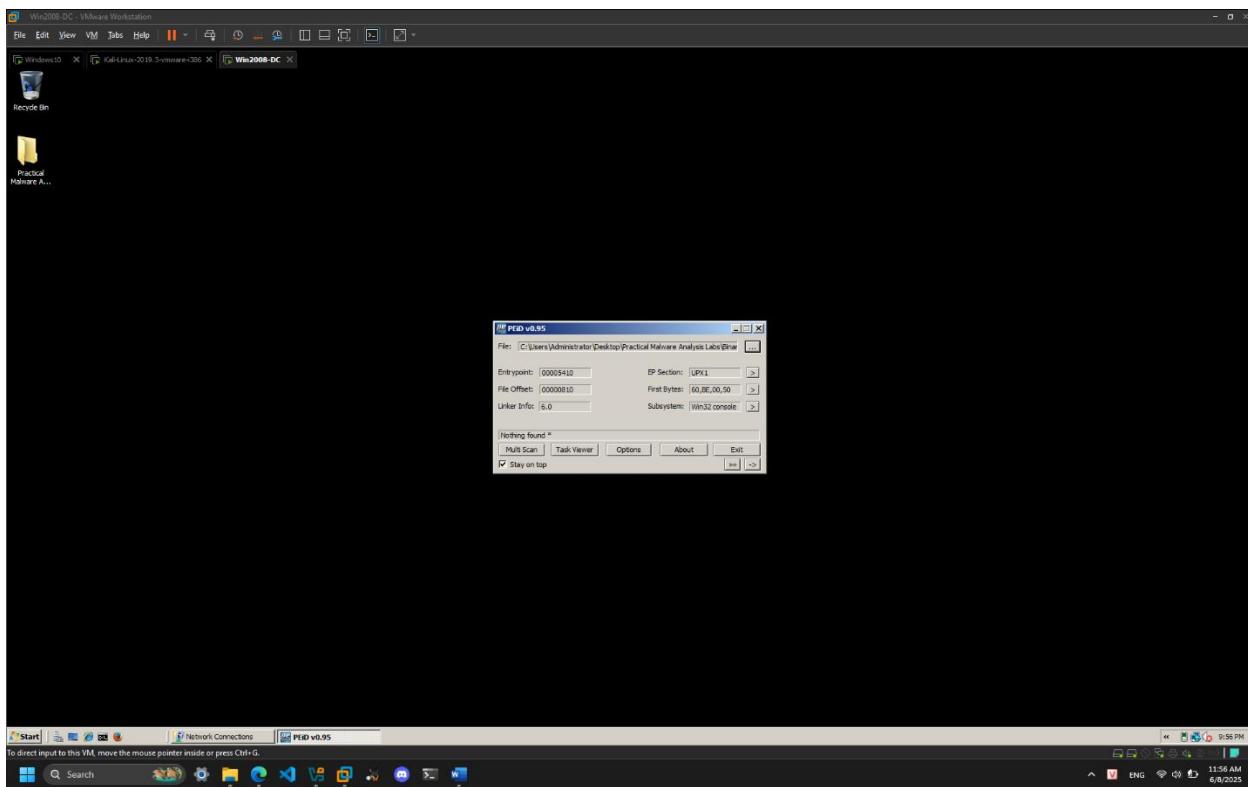
## Open Lab01-01.dll in Dependency Walker:



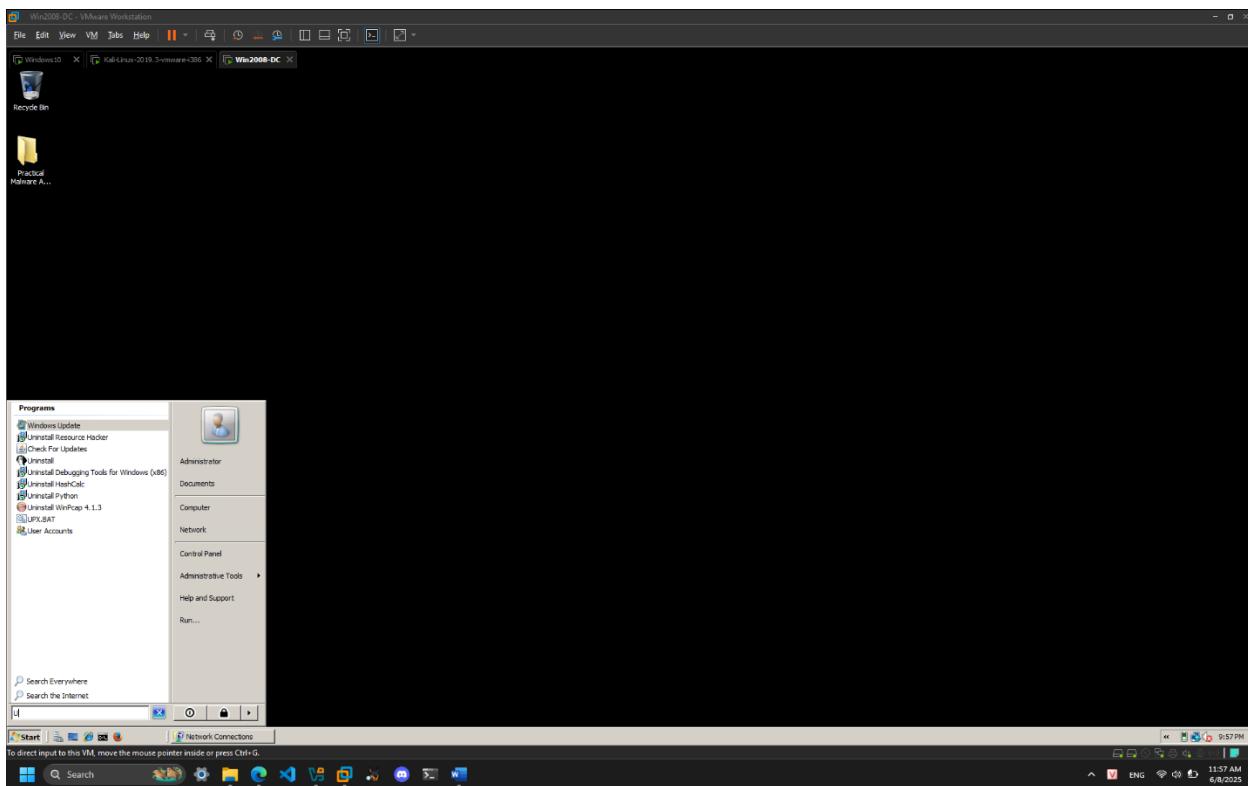
## b. Lab01-02.exe

Upload the Lab01-02.exe file to <https://www.hybrid-analysis.com>:

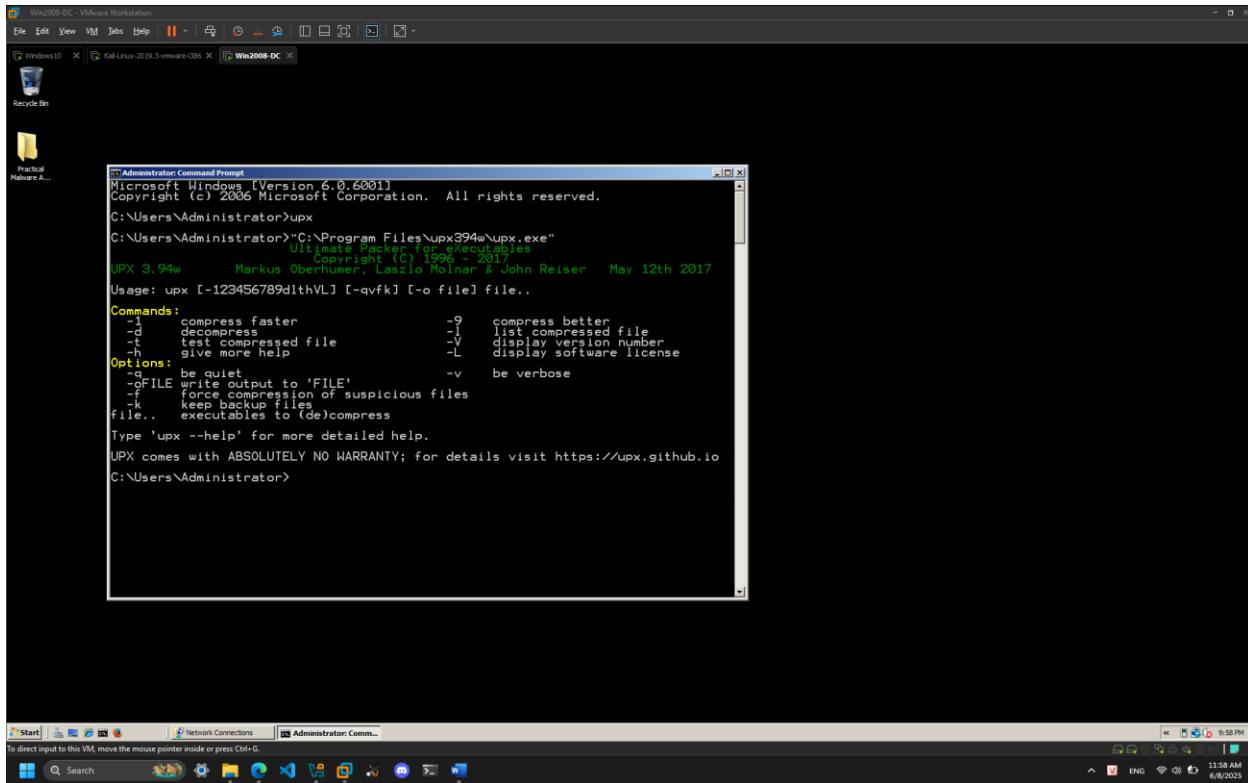
Run PEiD on the file:



Open UPX:



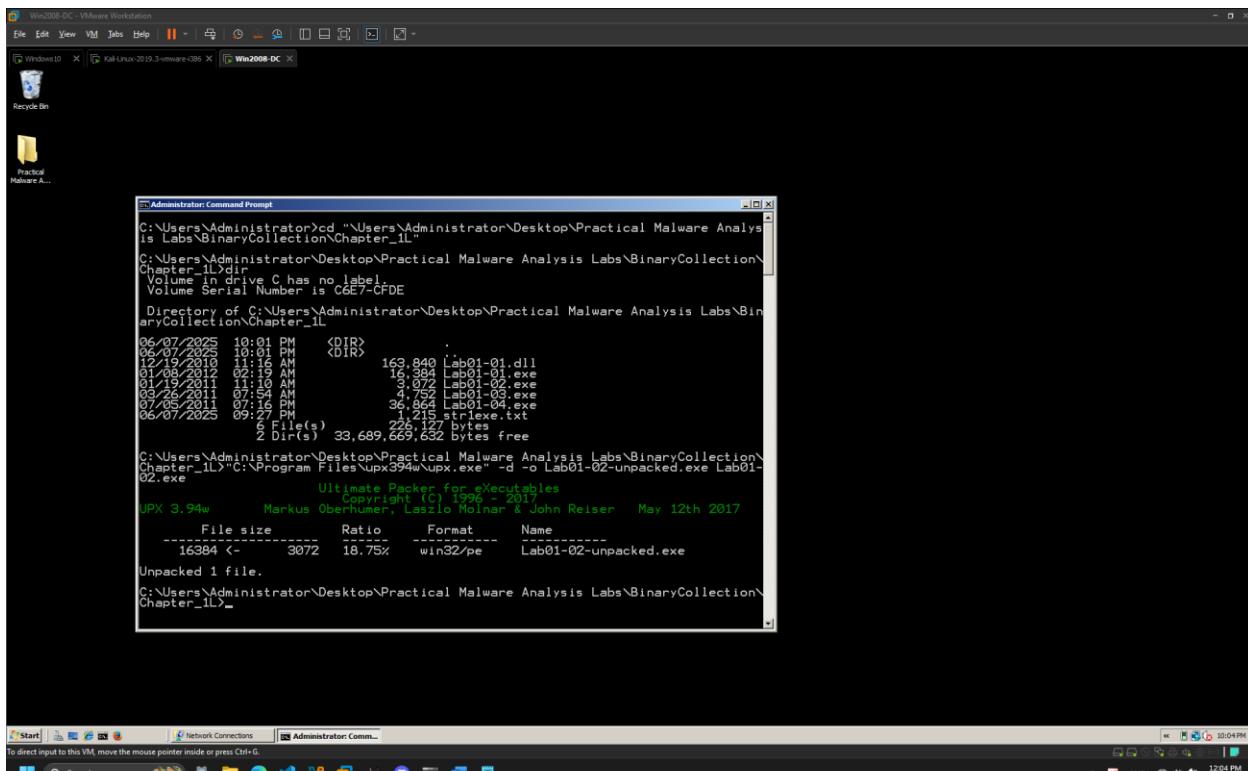
Open a Command Prompt window and execute UPX command:



```
Administrator: Command Prompt
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

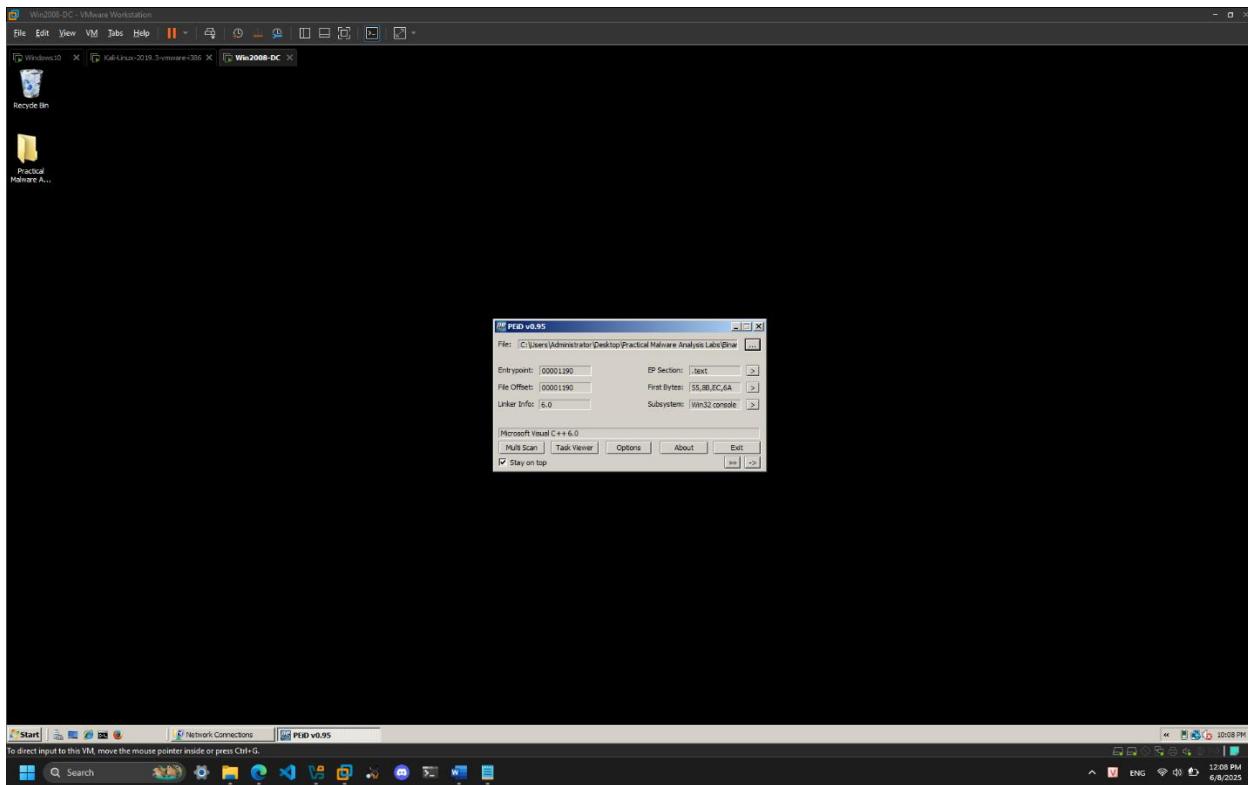
C:\Users\Administrator>upx
C:\Users\Administrator>"C:\Program Files\upx394w\upx.exe"
    Ultimate Packer for eXecutables
    Copyright (c) 1996 - 2017
UPX 3.94u      Markus Oberhumer, Laszlo Molnar & John Reiser   May 12th 2017
Usage: upx [-123456789dltv] [-qvfk] [-o file] file..
Commands:
  -d      compress faster           -g      compress better
  -t      decompress               -l      list compressed file
  -h      test compressed file     -v      display version number
  -g      give more help          -L      display software license
Options:
  -q      be quiet                  -v      be verbose
  -FILE 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>
```

Use the CD command to move to the directory containing your malware samples and unpack the file:

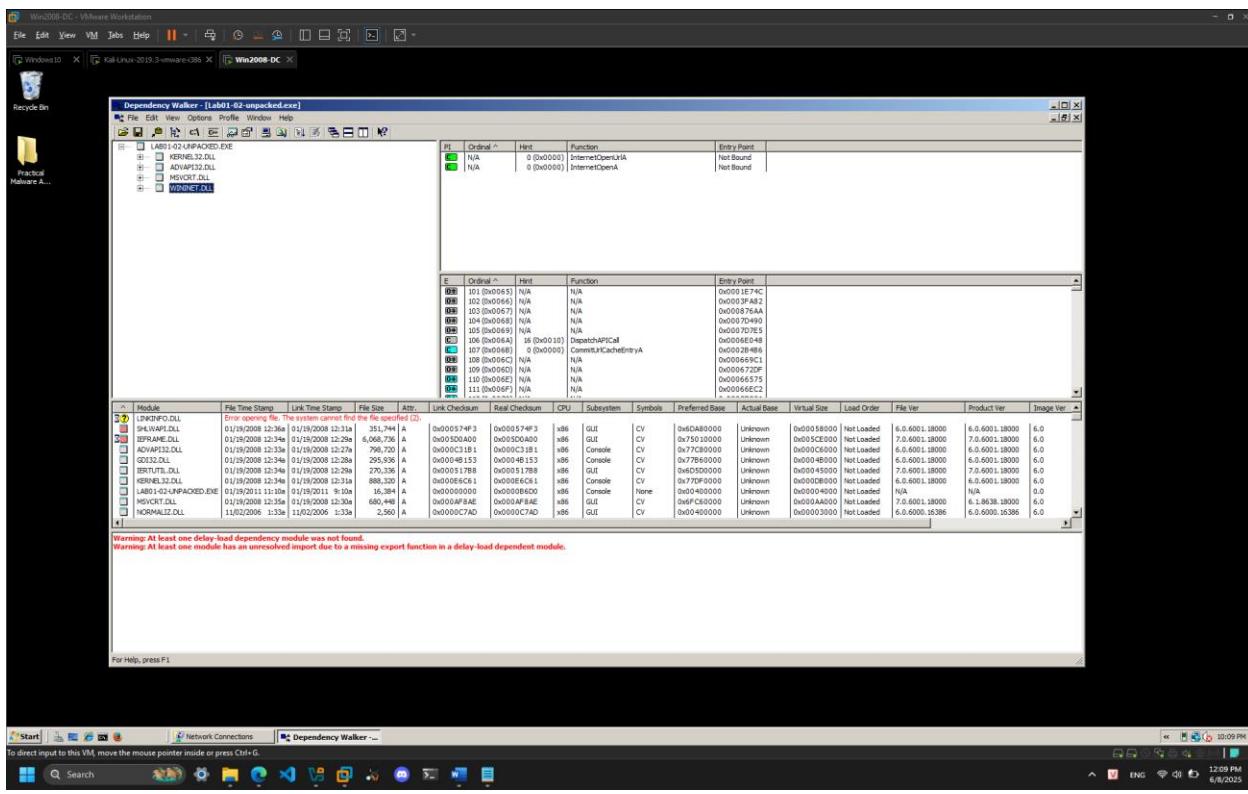


```
Administrator: Command Prompt
C:\Users\Administrator>cd "C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L"
C:\Users\Administrator>cd "C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L\dir"
Volume in drive C has no label.
Volume Serial Number is C6E7-CFDE
Directory of C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L
06/07/2025  10:01 PM  <DIR> .
06/07/2025  10:01 PM  <DIR> ..
12/19/2010  11:06 AM    163,840 Lab01-01.dll
01/08/2012  02:19 AM    16,384 Lab01-01.exe
01/19/2011  11:50 AM    3,072 Lab01-02.exe
03/19/2012  11:50 AM    4,062 Lab01-03.exe
07/05/2011  07:16 PM    36,664 Lab01-04.exe
06/07/2025  09:27 PM    1,215 str1.exe.txt
               6 File(s)    226,127 bytes
               2 Dir(s)  33,689,665,632 bytes free
C:\Users\Administrator>"C:\Program Files\upx394w\upx.exe" -d -o Lab01-02-unpacked.exe Lab01-02.exe
    Ultimate Packer for eXecutables
    Copyright (c) 1996 - 2017
UPX 3.94u      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>
```

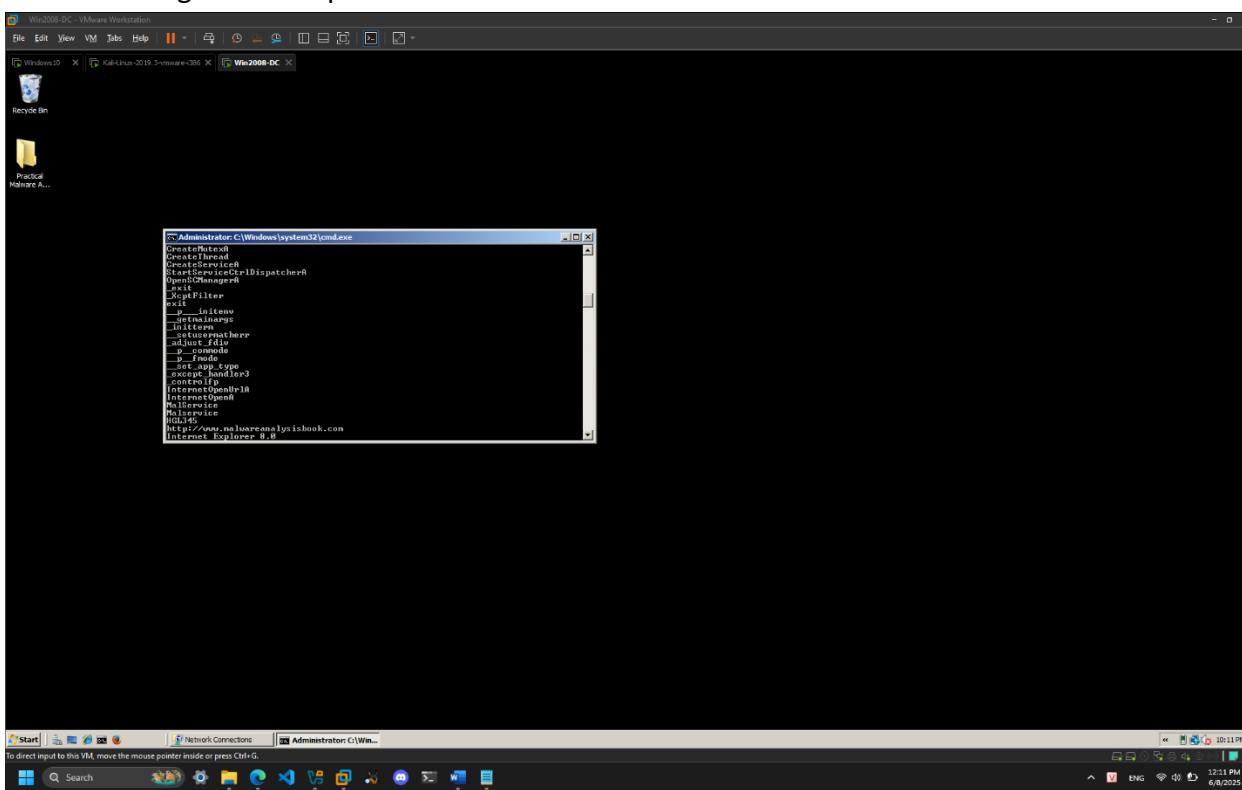
Analyze the unpacked file with PEiD:



Find the unpacked file's imports with Dependency Walker:

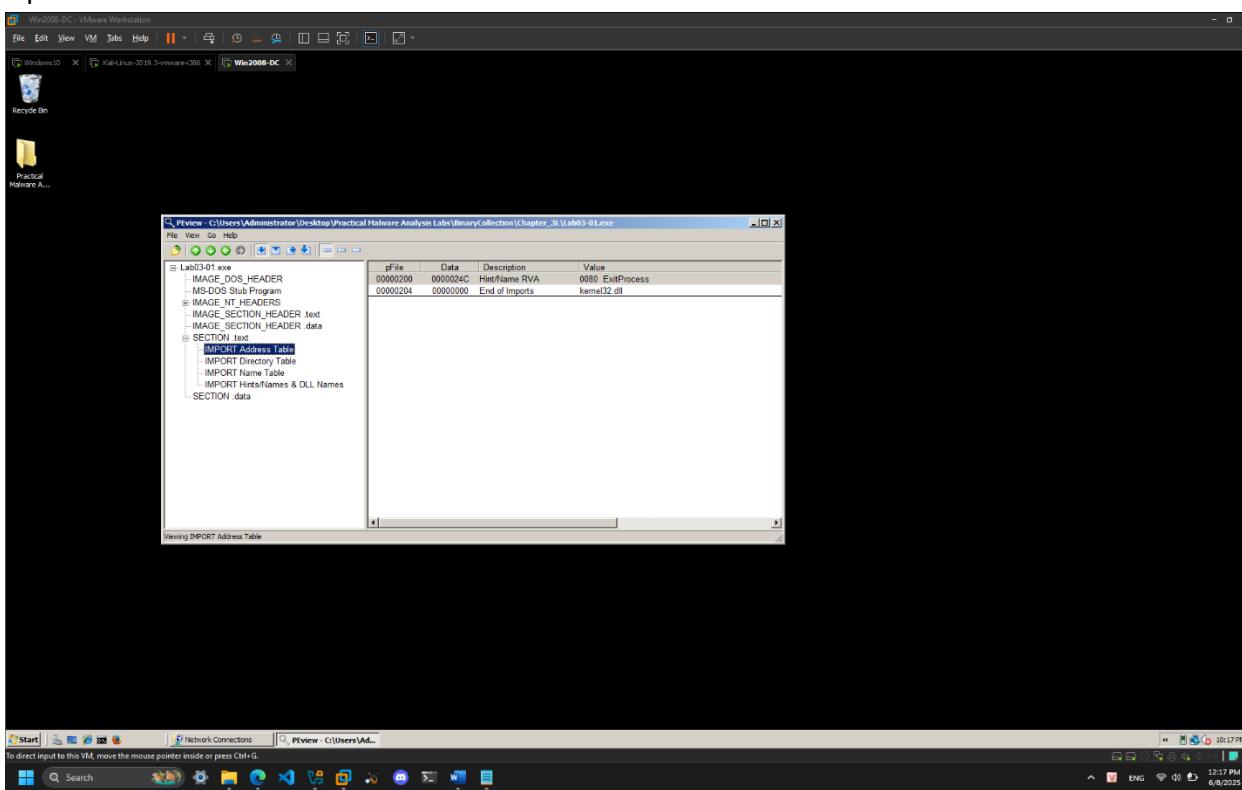


Find the strings in the unpacked file:

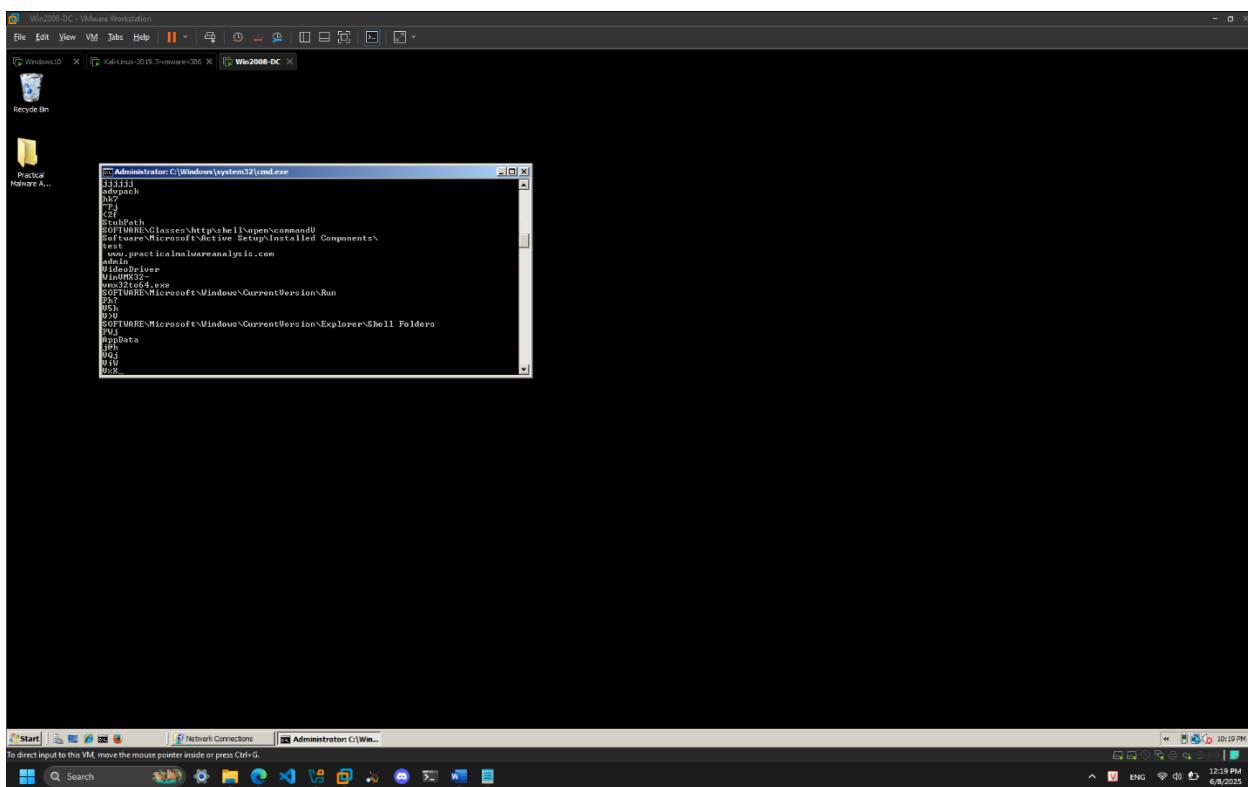


## 2. Basic Dynamic Techniques

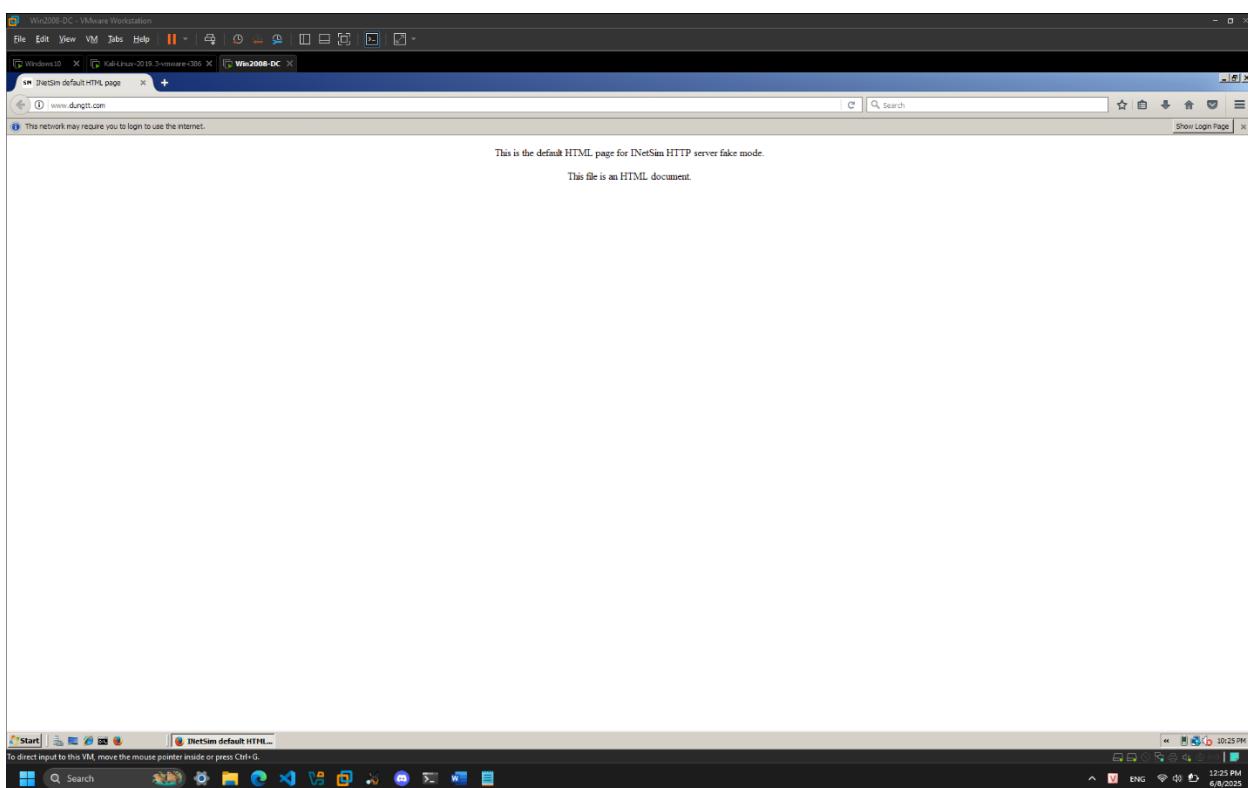
Open Lab03-01.exe in PEview:



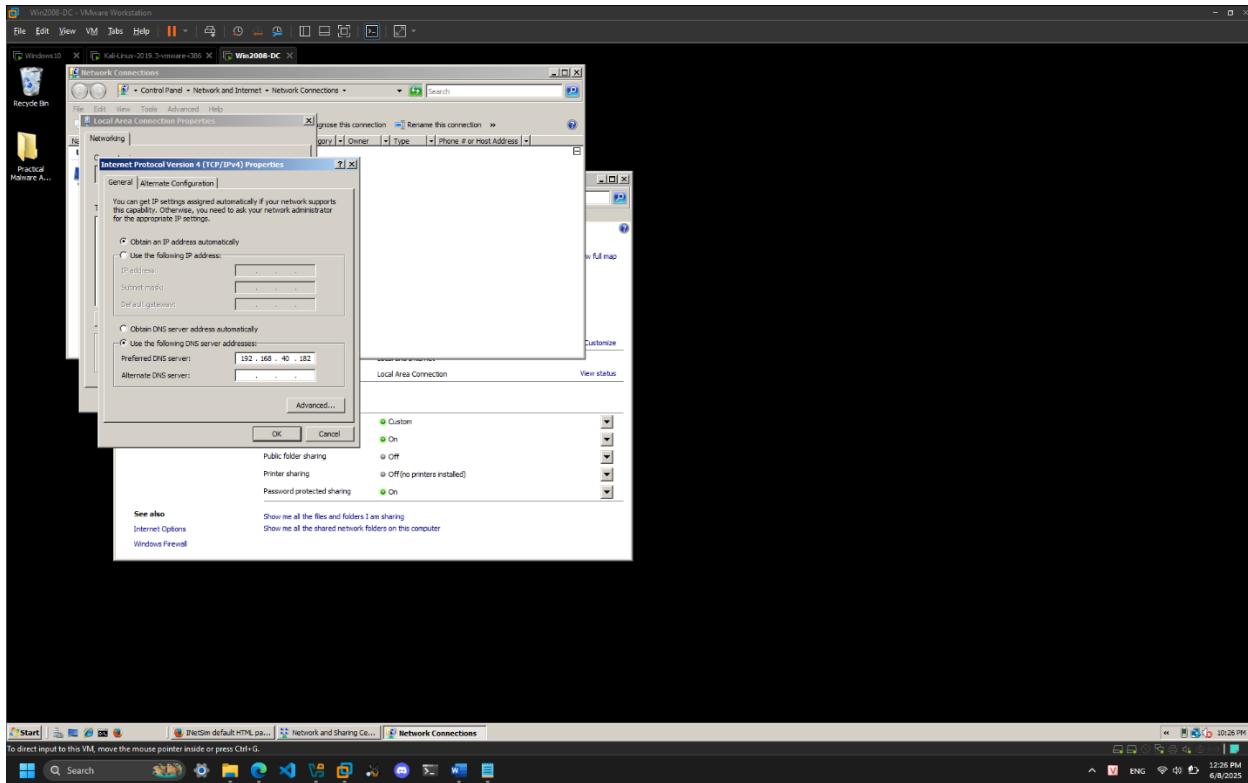
Examine the strings in Lab03-01.exe:



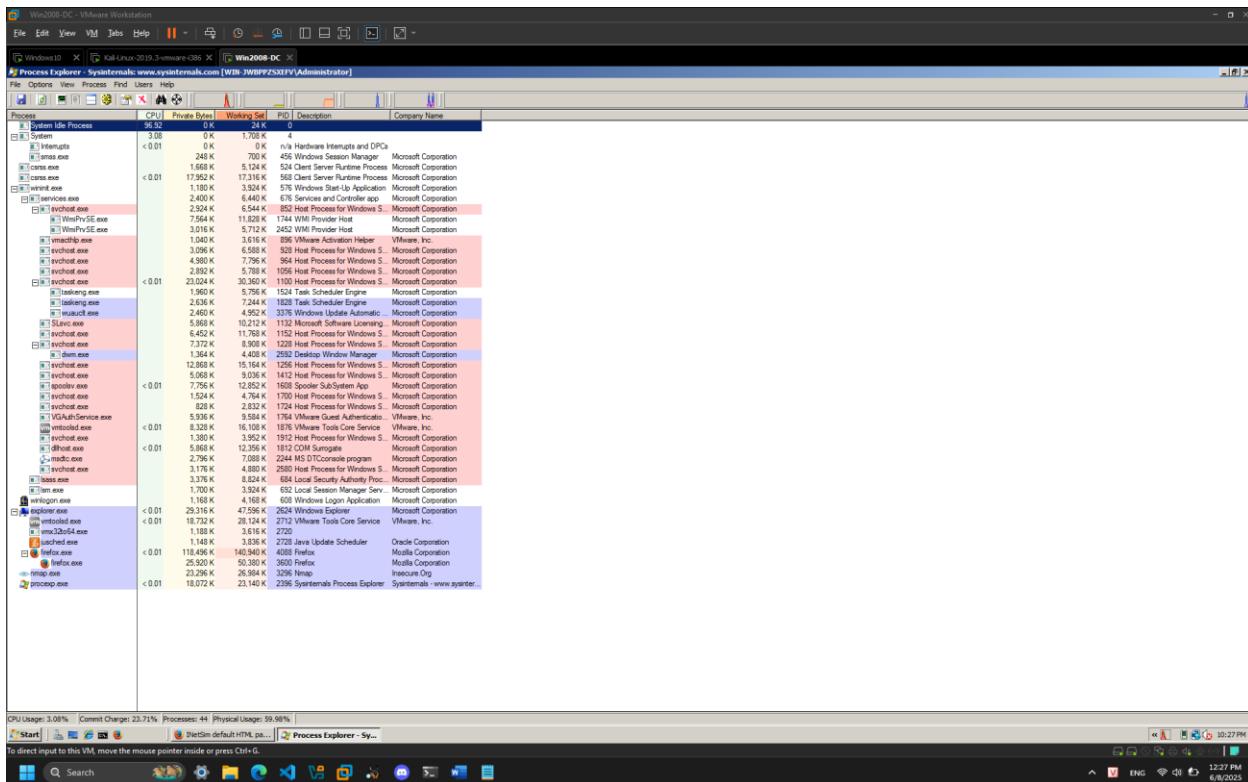
Start INetSim:



## Setting the DNS Server:



## Run Process Explorer:



## Run Wireshark:

Wireshark Screenshot Description: This screenshot shows a Wireshark capture session titled "Capturing from Local Area Connection". The packet list pane shows over 2000 captured packets, with several highlighted in red. A selected packet is shown in the details and bytes panes. The status bar at the bottom right shows "Packets: 58 - Displayed: 58 (100.0%)" and "Profile: Default".

## Start Process Monitor:

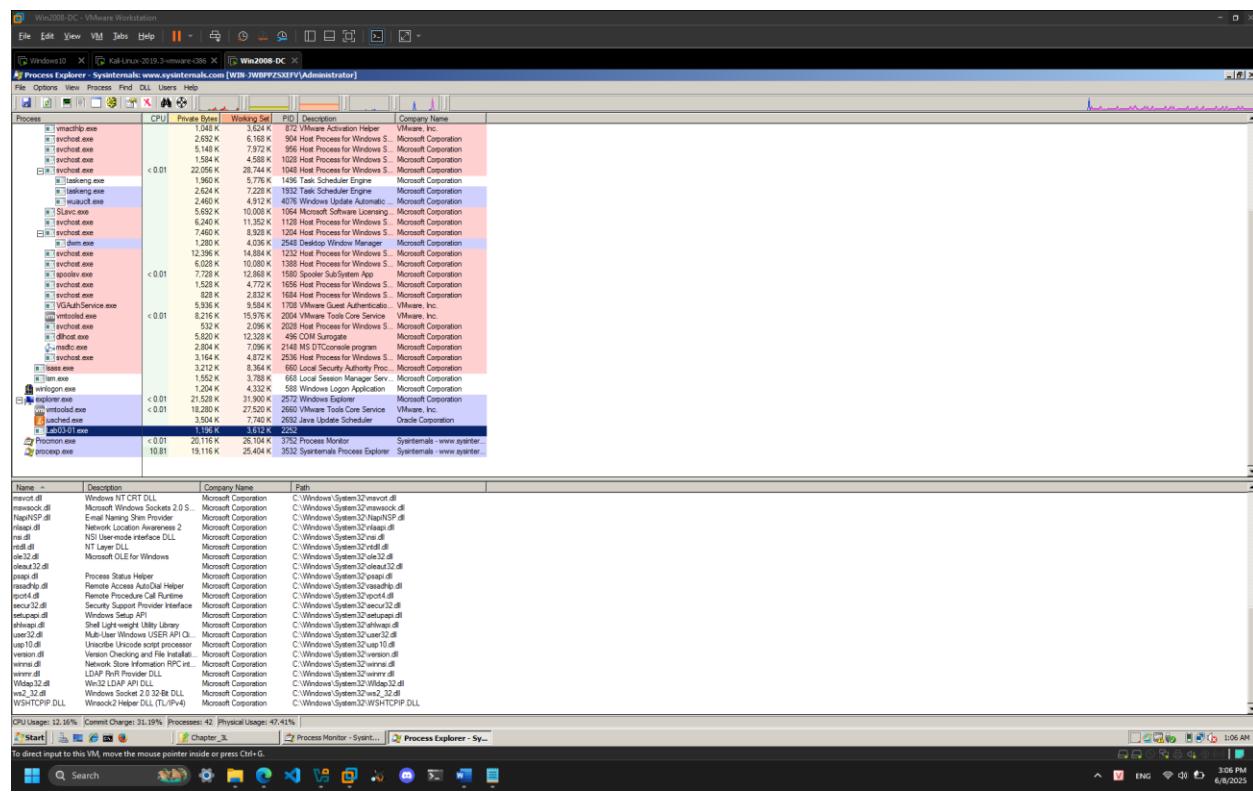
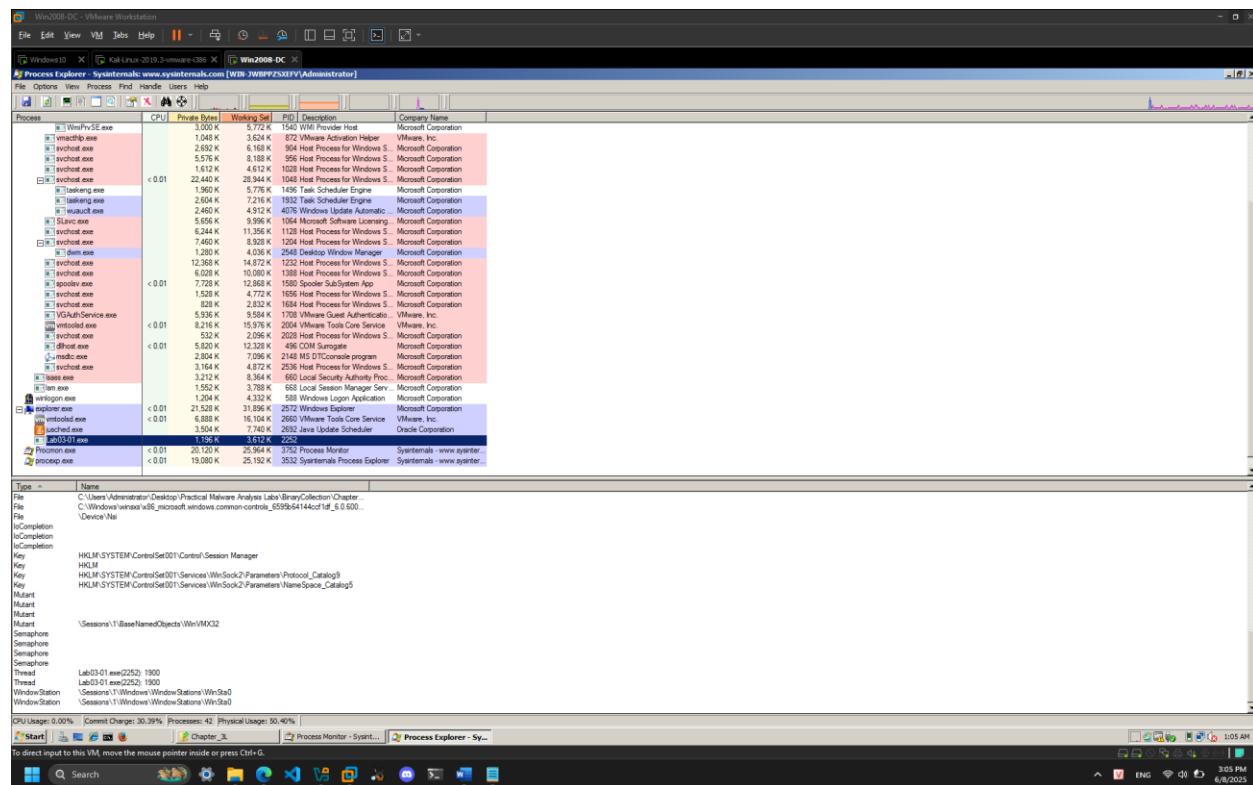
Process Monitor Screenshot Description: This screenshot shows the Windows Task Manager with "Process Monitor" selected. The main window displays a list of system calls made by "Explorer.exe". The log shows various registry operations like SetValue and SetValueEx, as well as file operations like CreateFile and ReadFile. The status bar at the bottom right shows "Packets: 58 - Displayed: 58 (100.0%)".

## Excluding Harmless Processes:

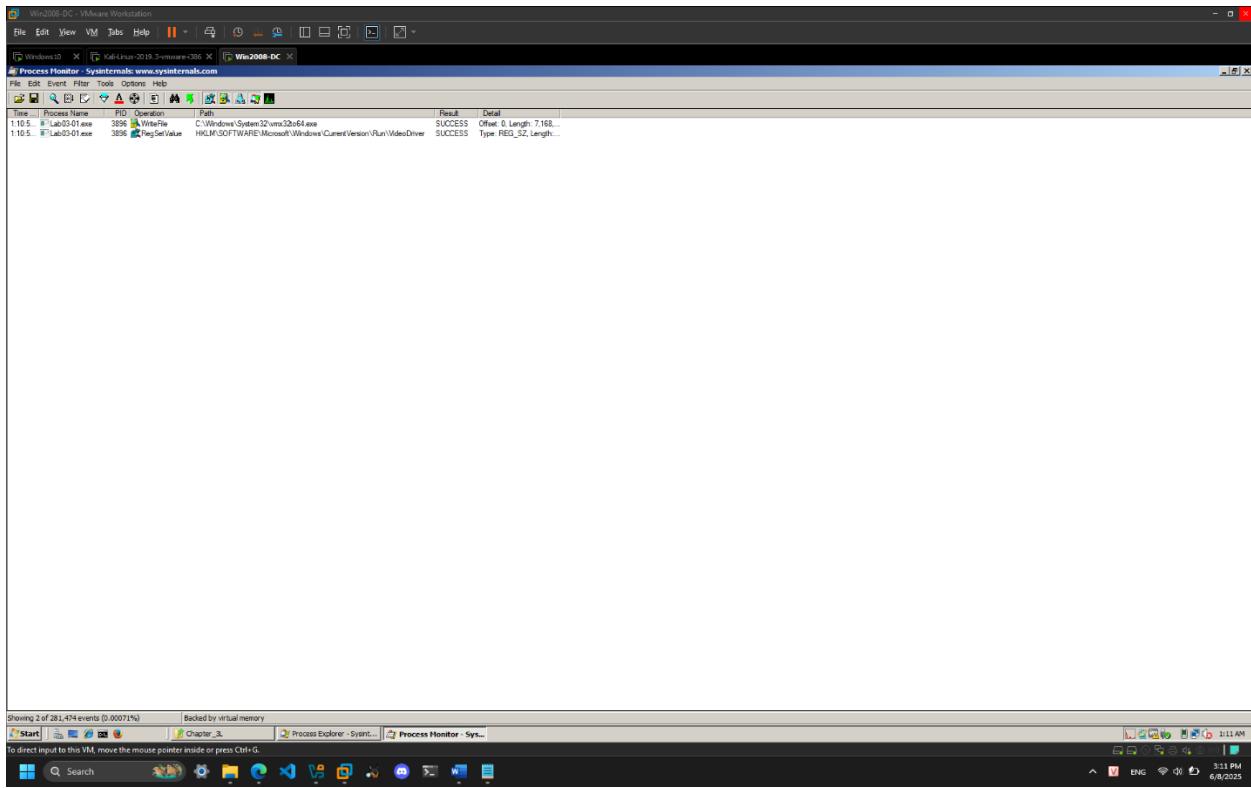
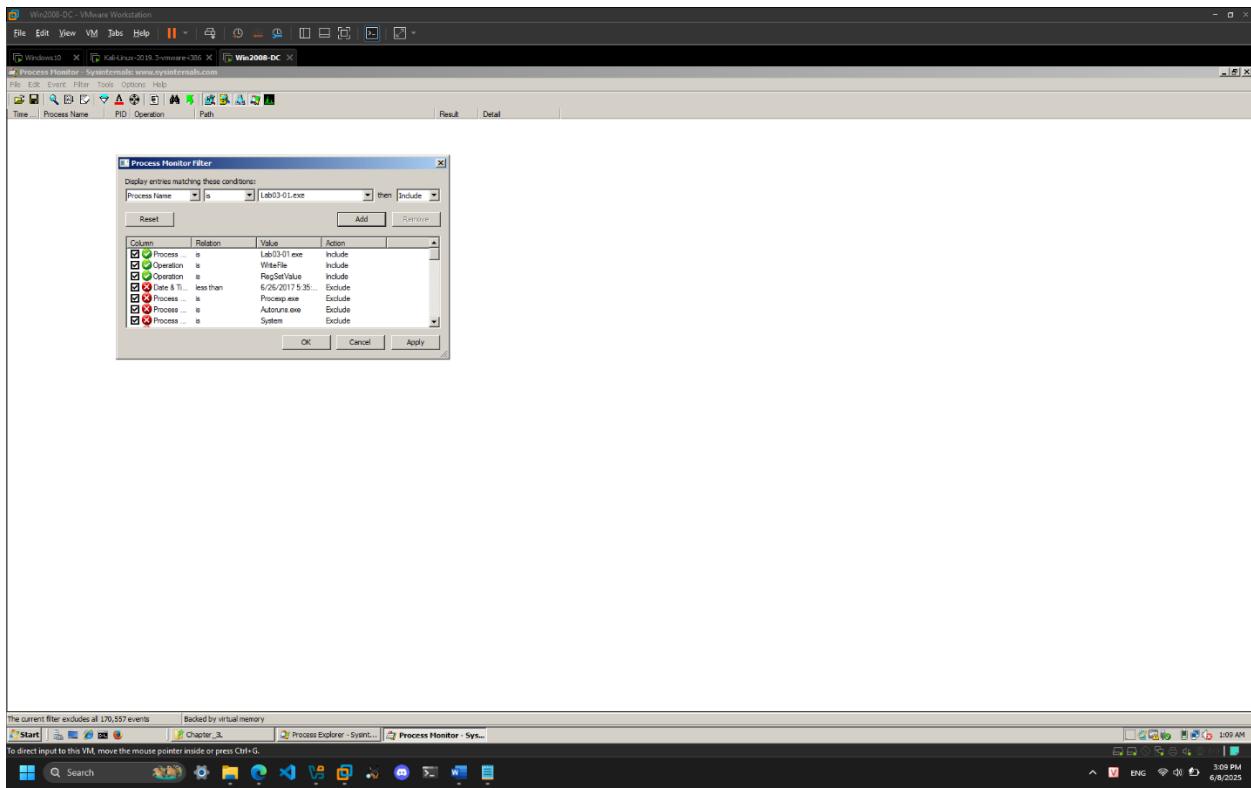
The screenshot shows Process Monitor running on a Windows 2008 DC host. The taskbar at the bottom indicates the system is connected to a Kali Linux 2019.3-vmware-136 guest. The Process Monitor window displays a list of file operations for the Firefox executable (firefox.exe) on the C:\Users\Administrator\AppData\Local\Temp\Profile\ubscddr folder. The log entries show various file operations such as WriteFile, ReadFile, and DeleteFile, all resulting in SUCCESS. A filter has been applied to exclude these processes, which is why they are not visible in the list.

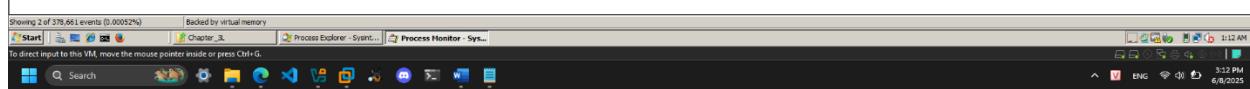
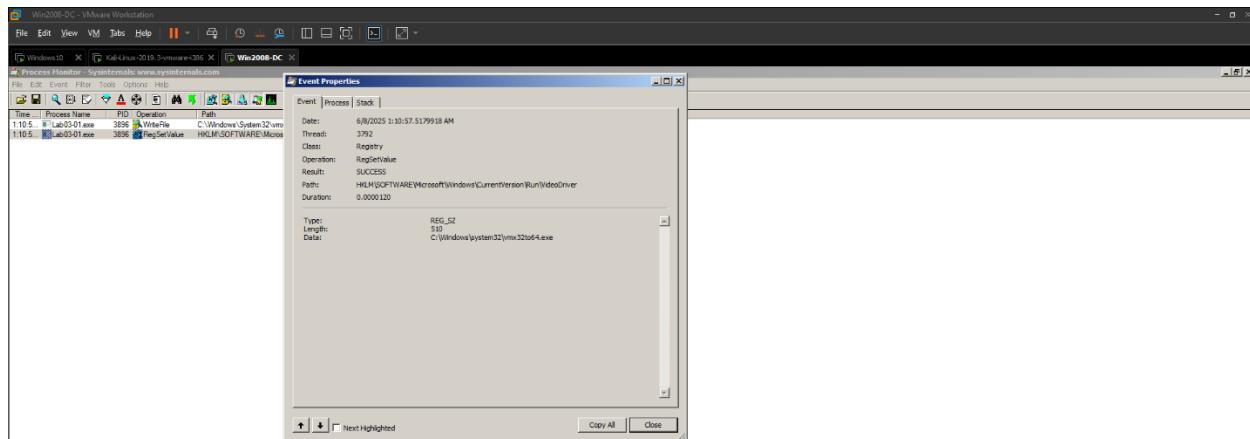
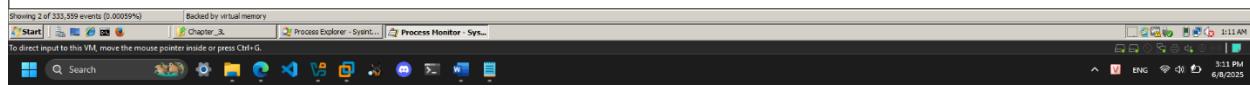
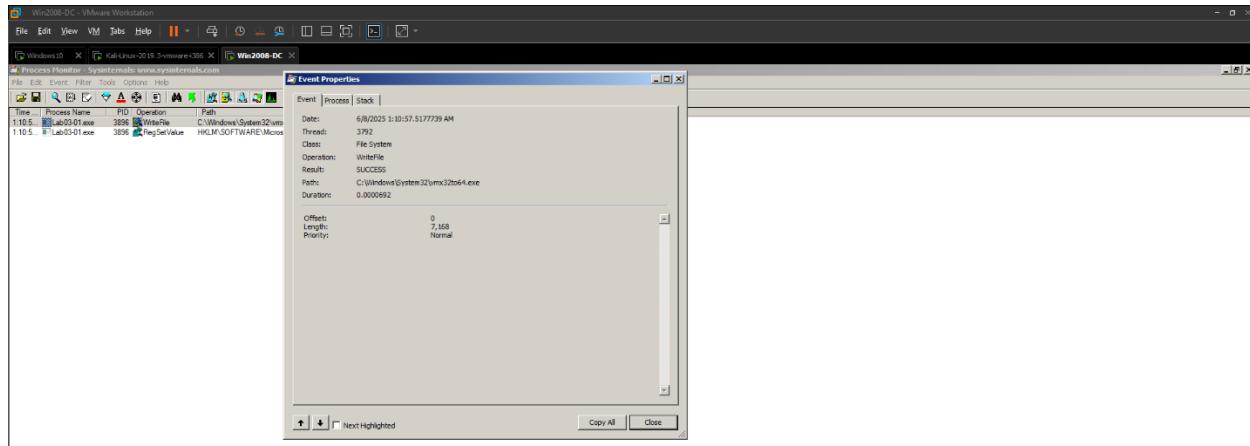
The screenshot shows Process Monitor running on a Windows 2008 DC host. The taskbar at the bottom indicates the system is connected to a Kali Linux 2019.3-vmware-136 guest. The Process Monitor window displays a list of file operations for the Firefox executable (firefox.exe) on the C:\Users\Administrator\AppData\Local\Temp\Profile\ubscddr folder. The log entries show various file operations such as WriteFile, ReadFile, and DeleteFile, all resulting in SUCCESS. A filter has been applied to exclude these processes, which is why they are not visible in the list.

## Run the Lab03-01.exe File and Viewing the Running Malware in Process Explorer:



## Viewing the Malicious Process's Events in Process Monitor:

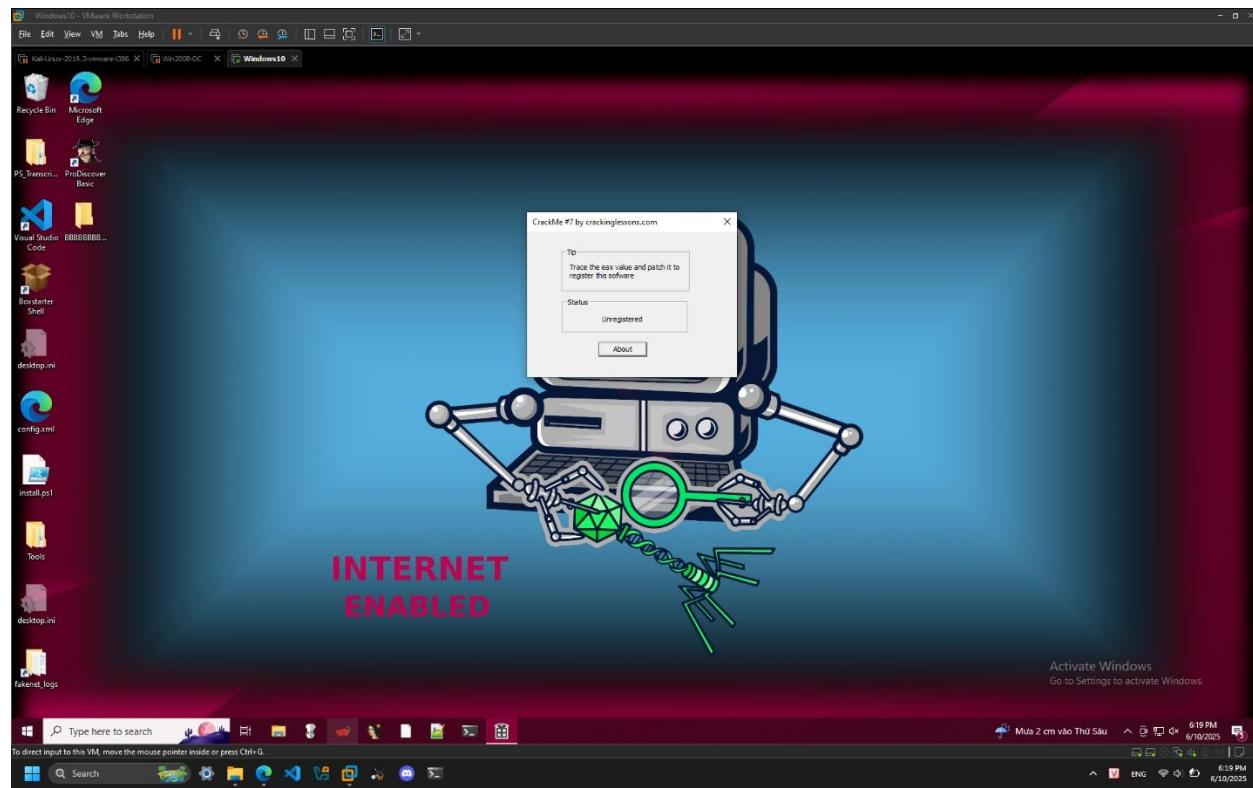




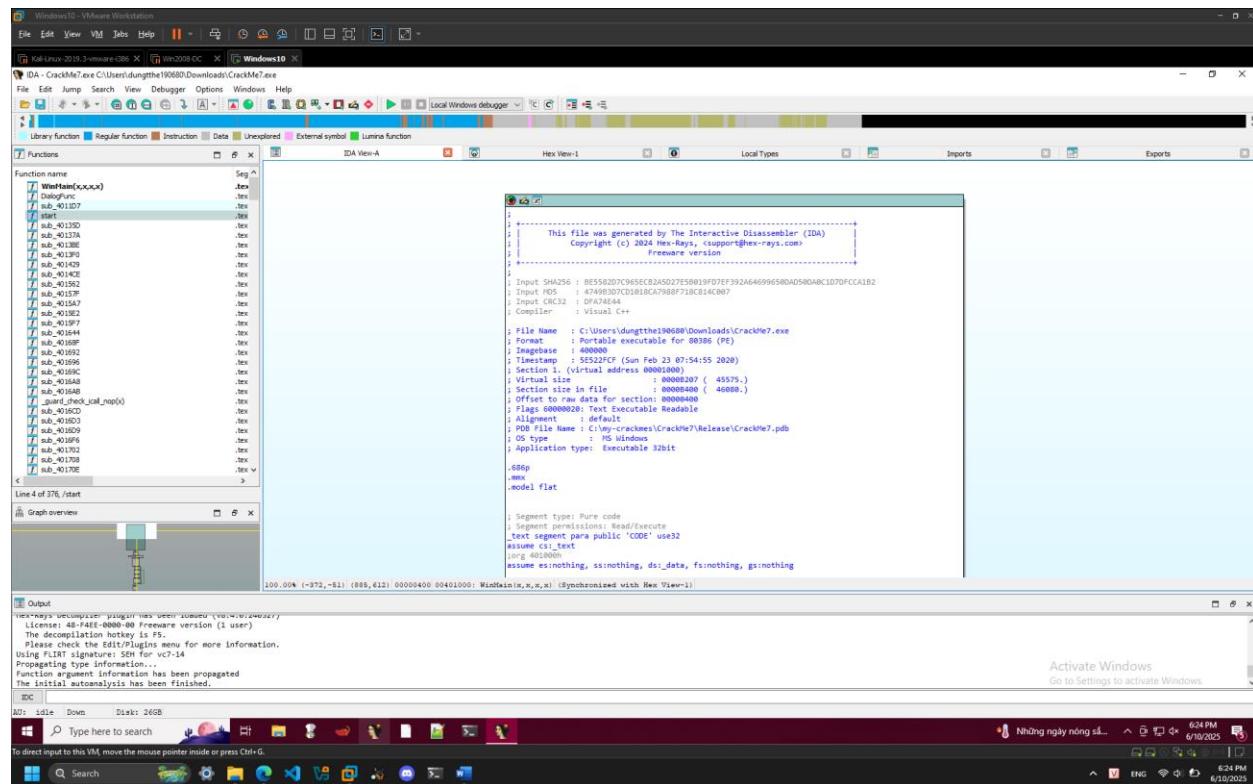


## CrackMe #7

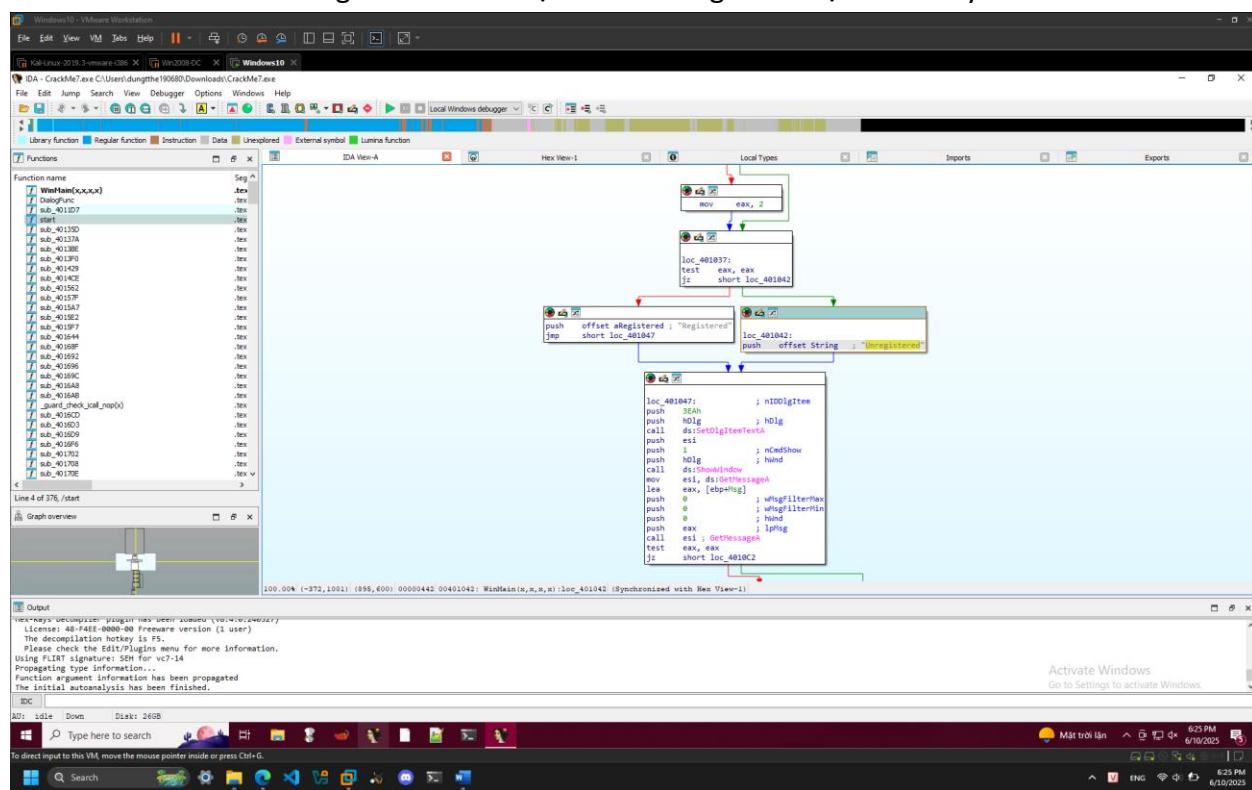
Đầu tiên em thử chạy chương trình và nhận được thông báo có từ khóa “Unregistered”:



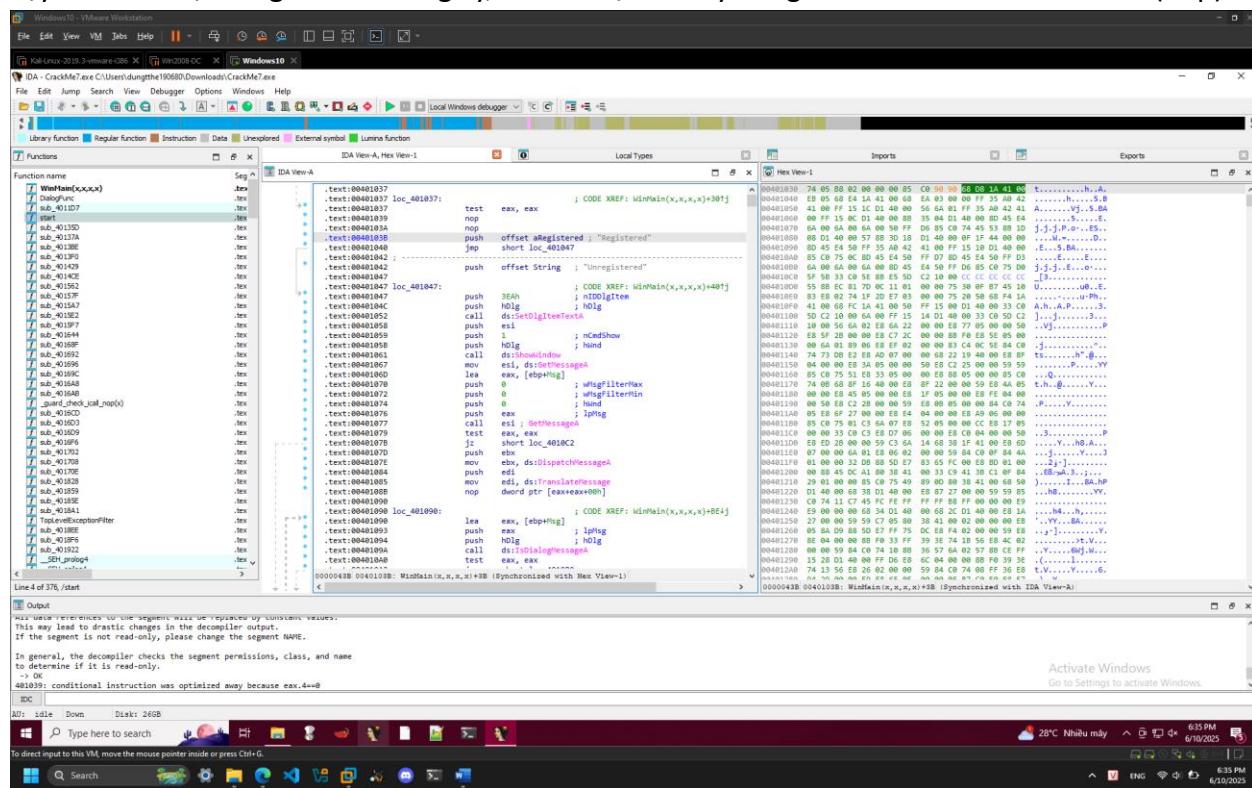
Sau đó em mở phần mềm IDA và tiến hành dịch ngược file:



Em search từ khóa “Unregistered” và được điều hướng đến đoạn code này:



Có thể thấy thông báo đã đăng ký không được hiển thị do lệnh nhảy trong đoạn loc\_401037, vì vậy để hiển thị thông báo đã đăng ký, em xóa lệnh nhảy bằng cách sửa mã hex thành 90 (nop):



Lưu lại và chạy chương trình thì em nhận được thông báo đã đăng ký:

