Họ và tên: Trần Trí Dũng

Mã số sinh viên: HE190680

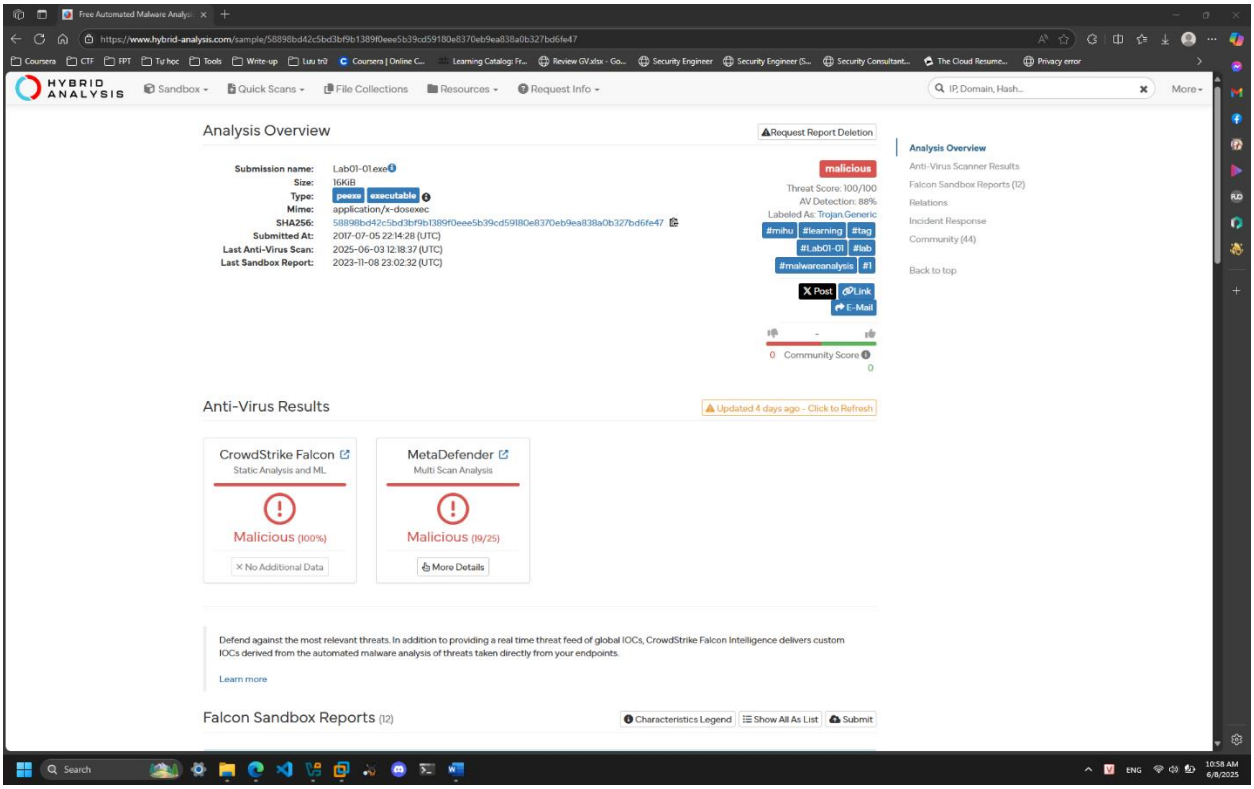
Lớp: IA1901

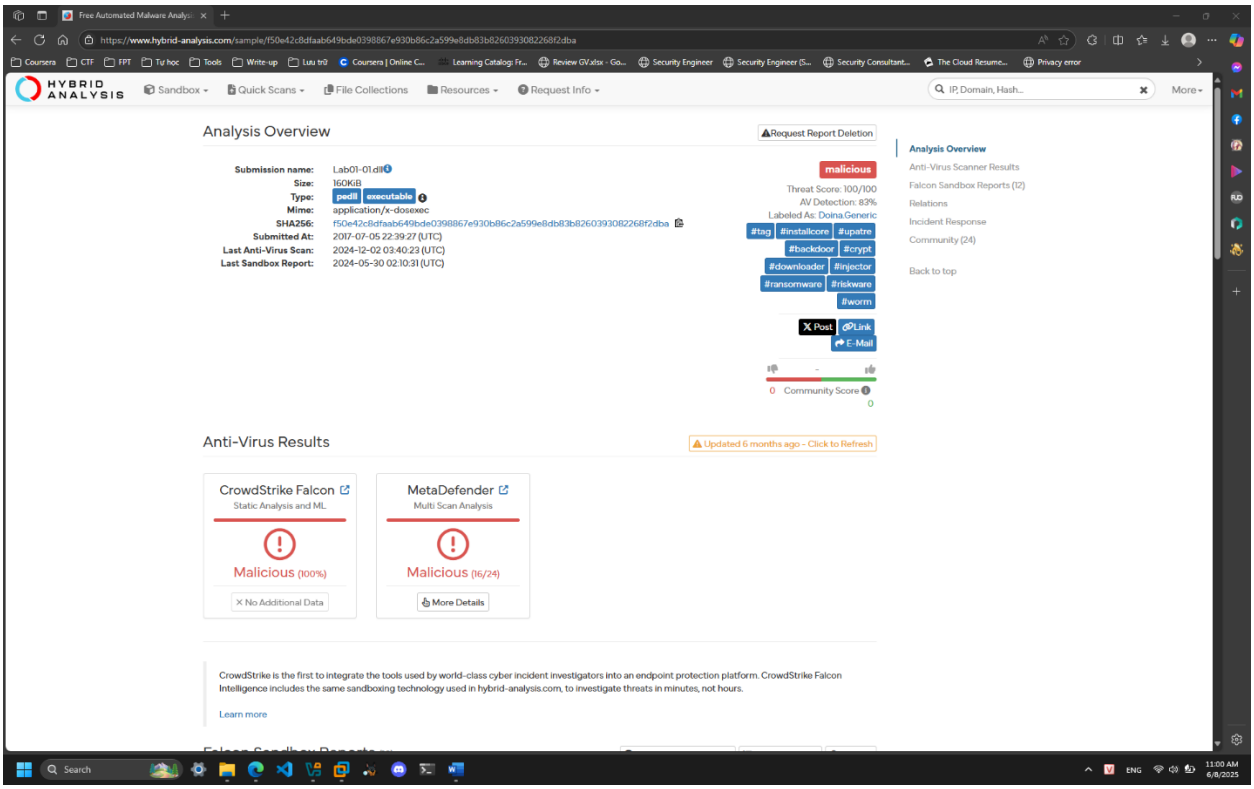
Lab 8:

1. Basic Static Techniques

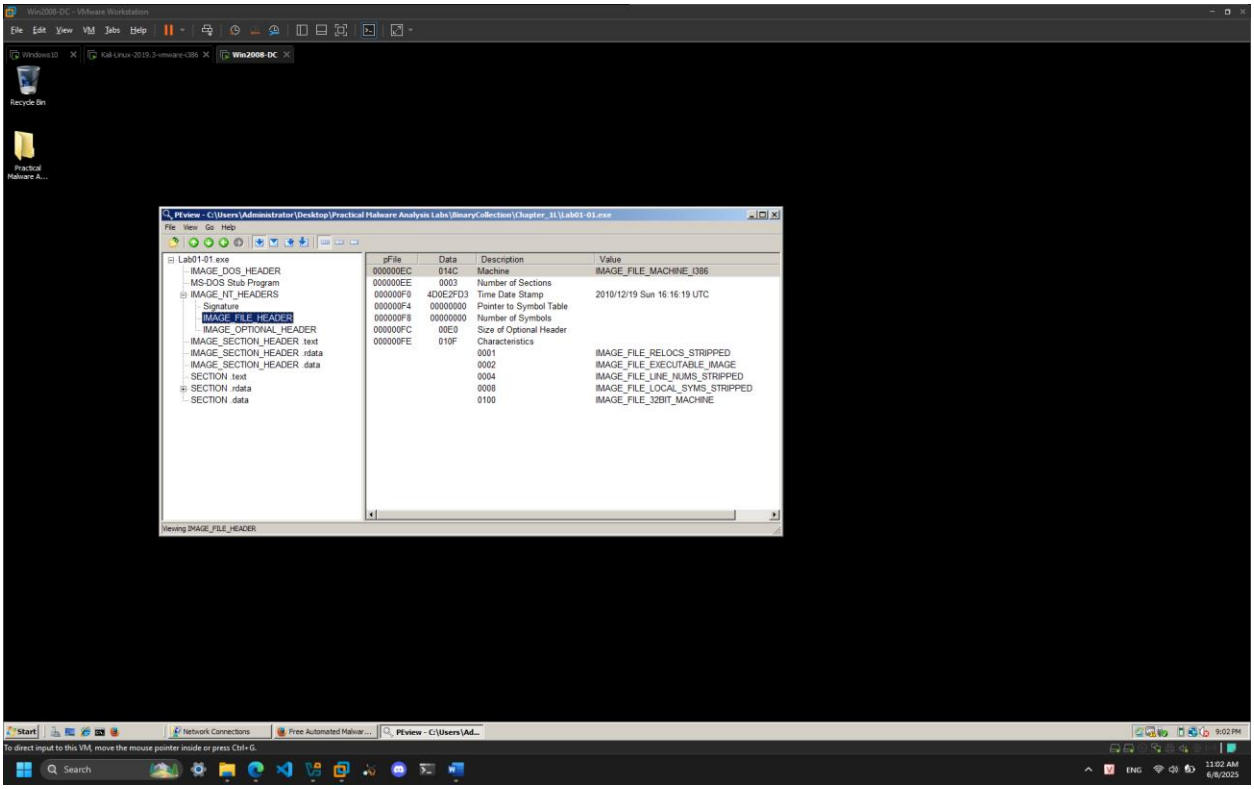
a. Lab01-01.exe

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

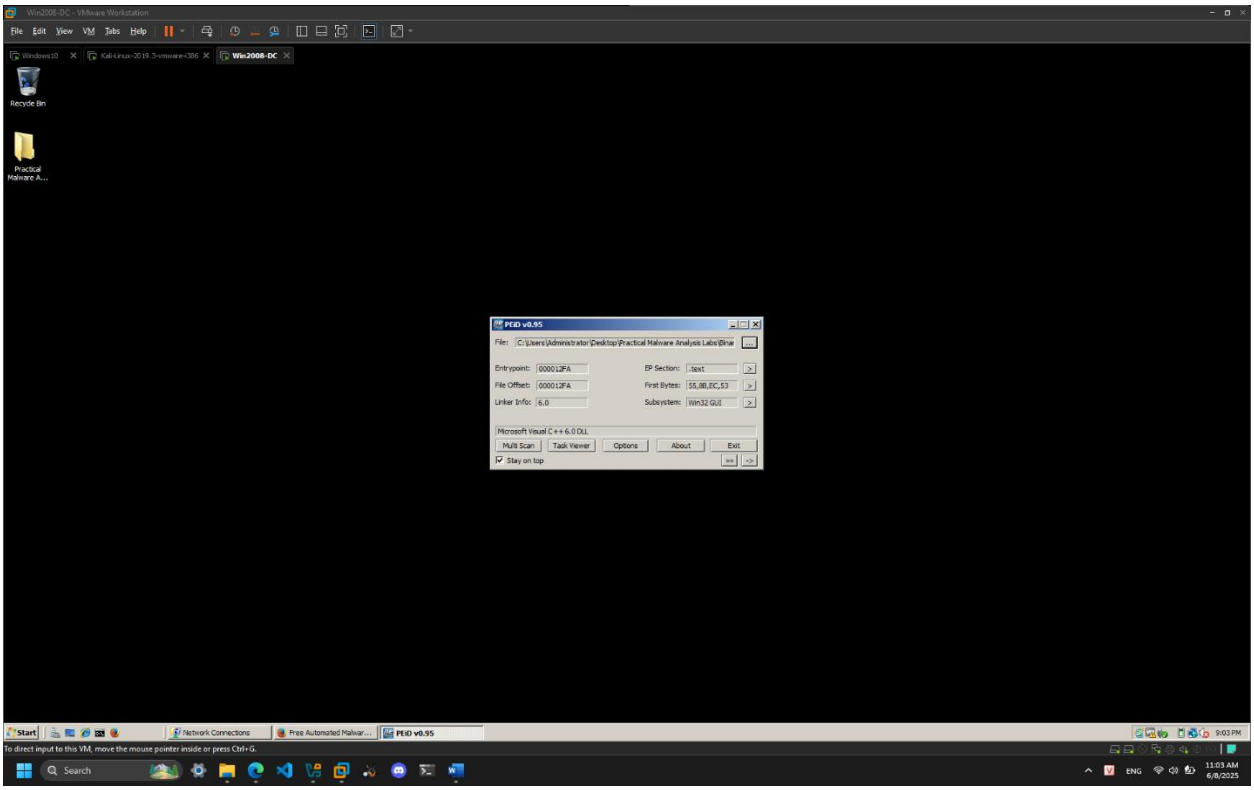




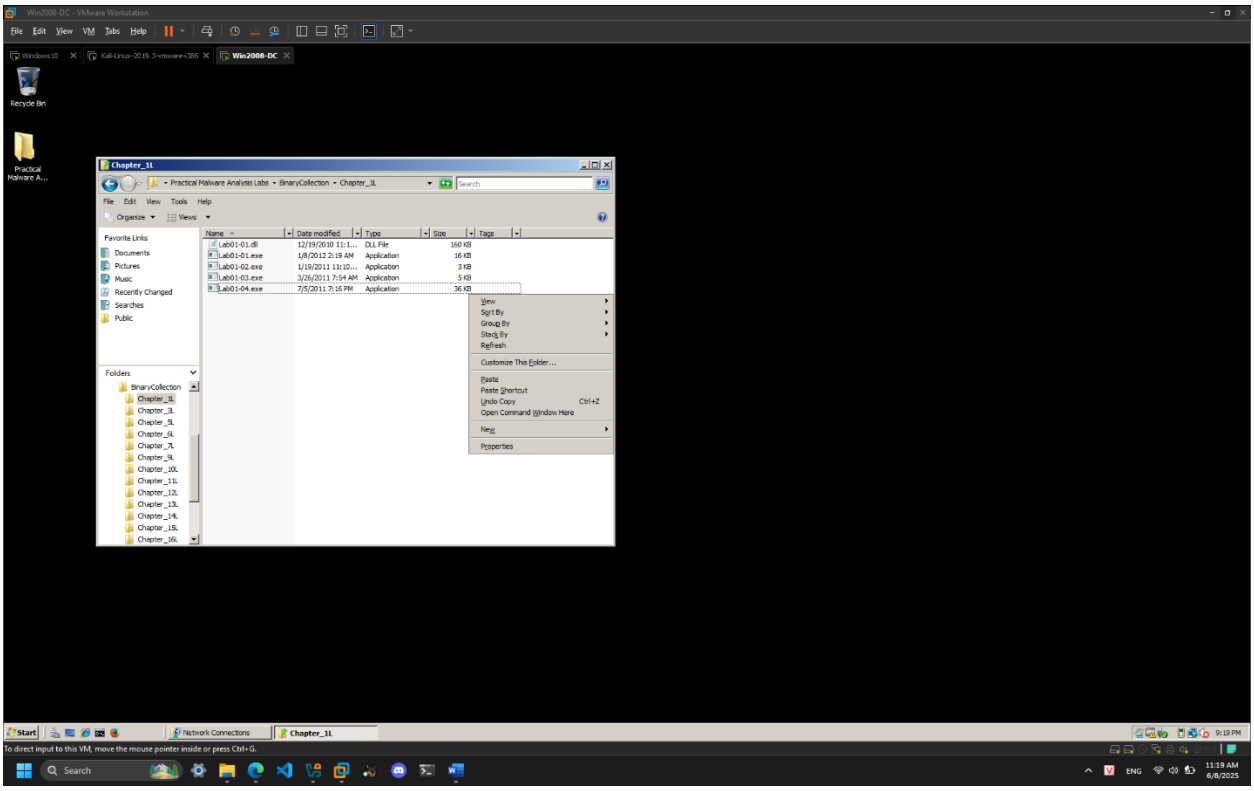
Open the files in PEview:



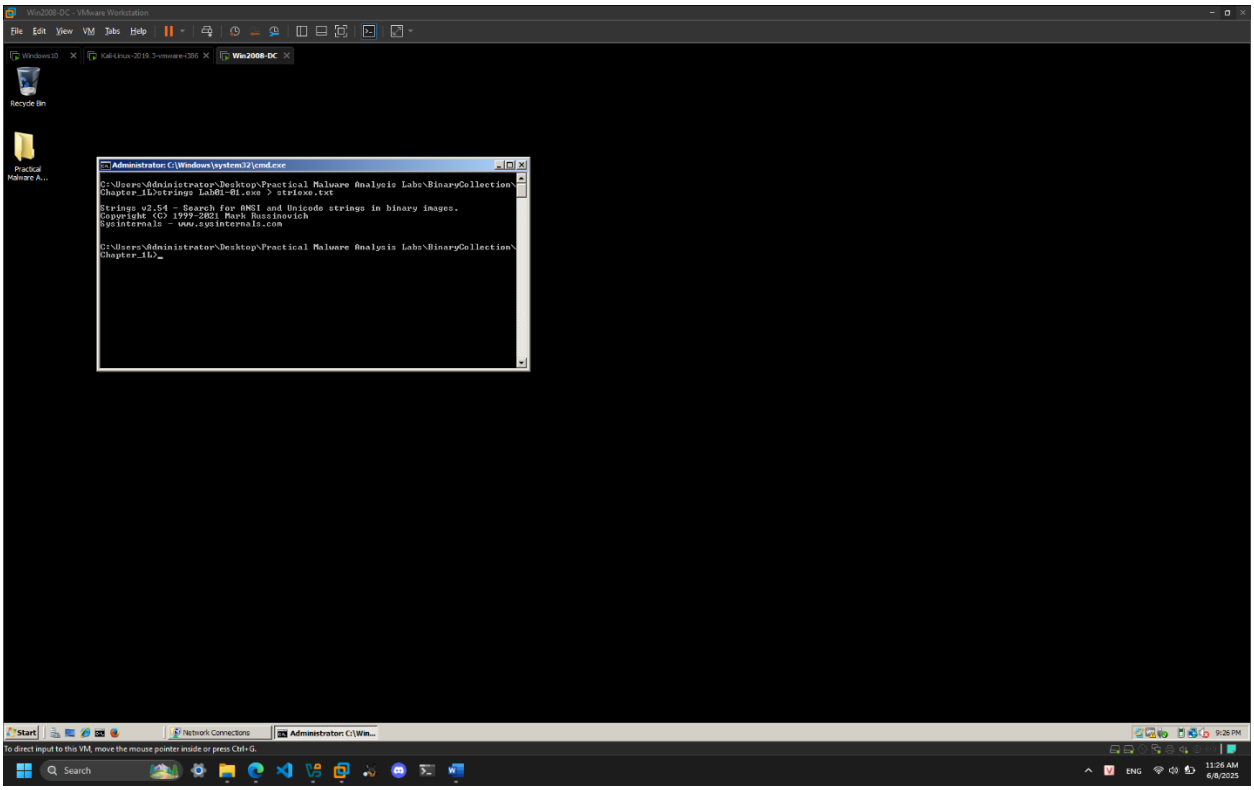
Open the files in PEiD:

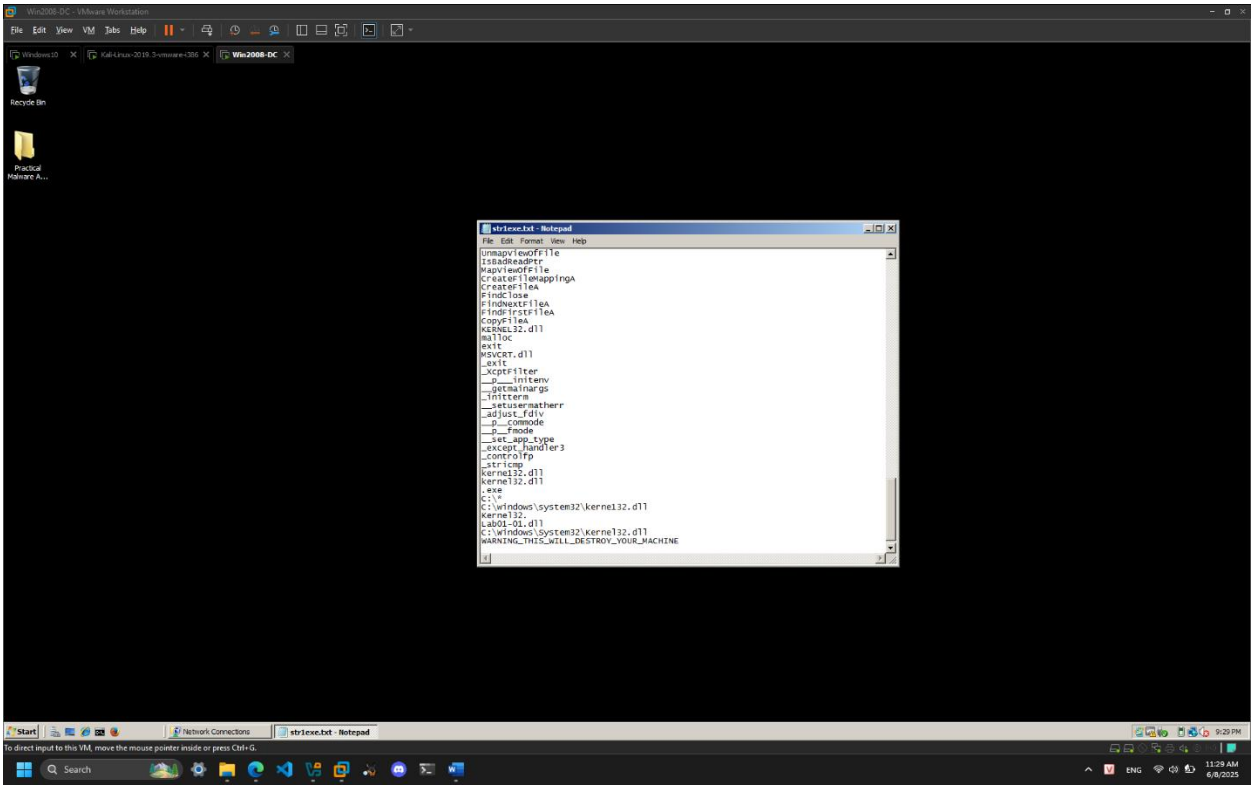


Right-click in the Chapter_1L folder, and select Open Command Window Here:

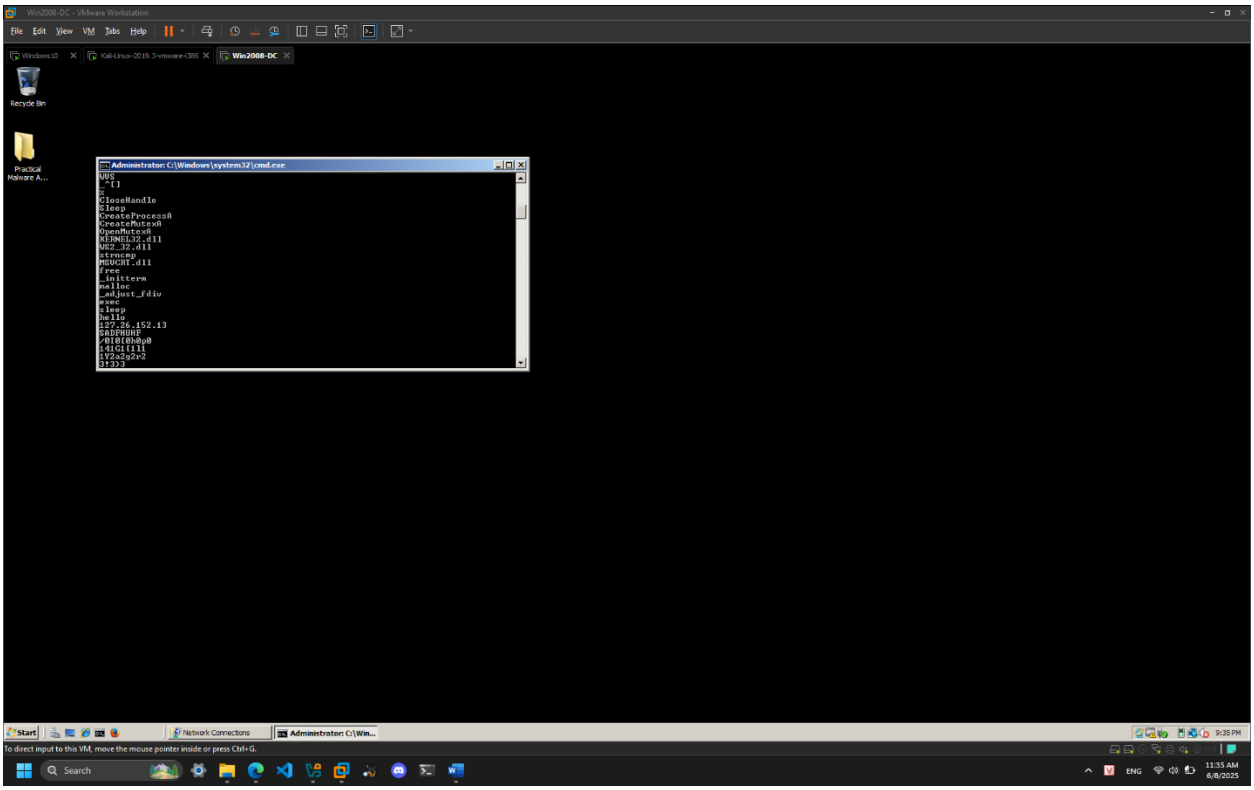


Collect the strings from the Lab01-01.exe file:

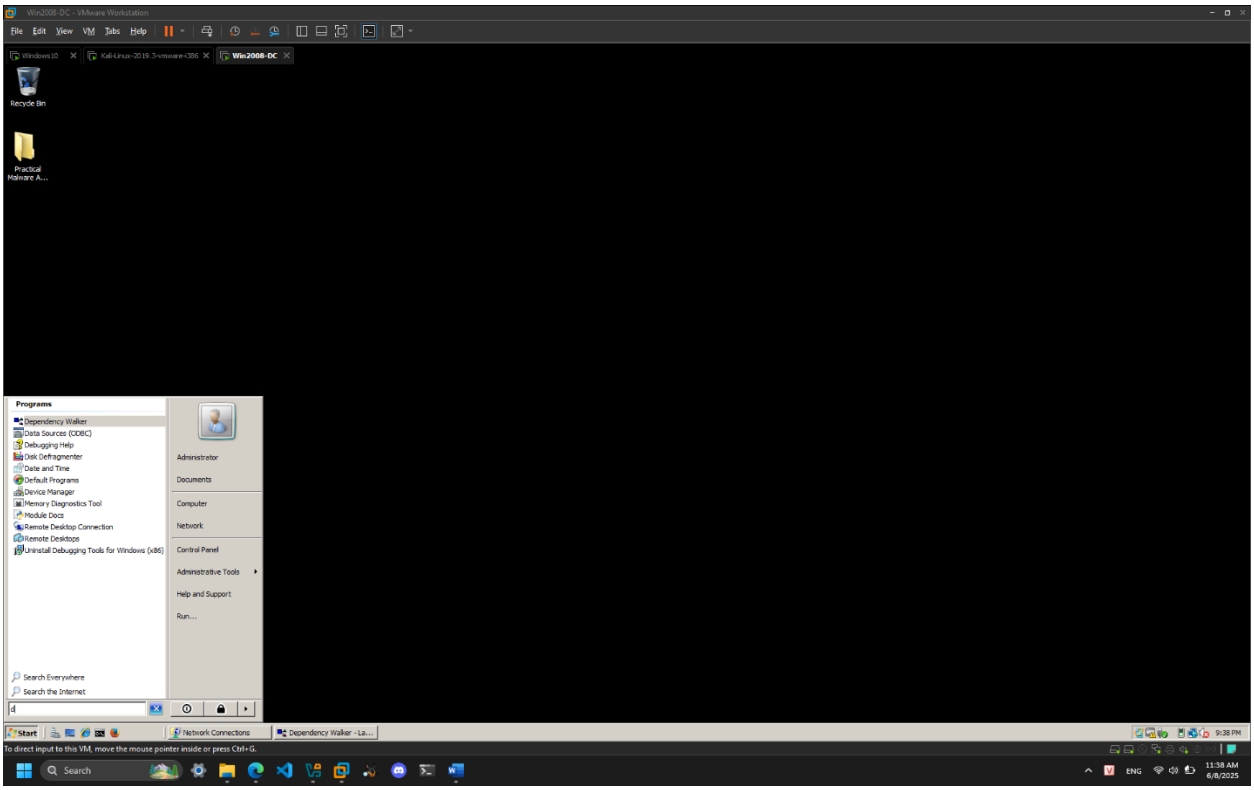




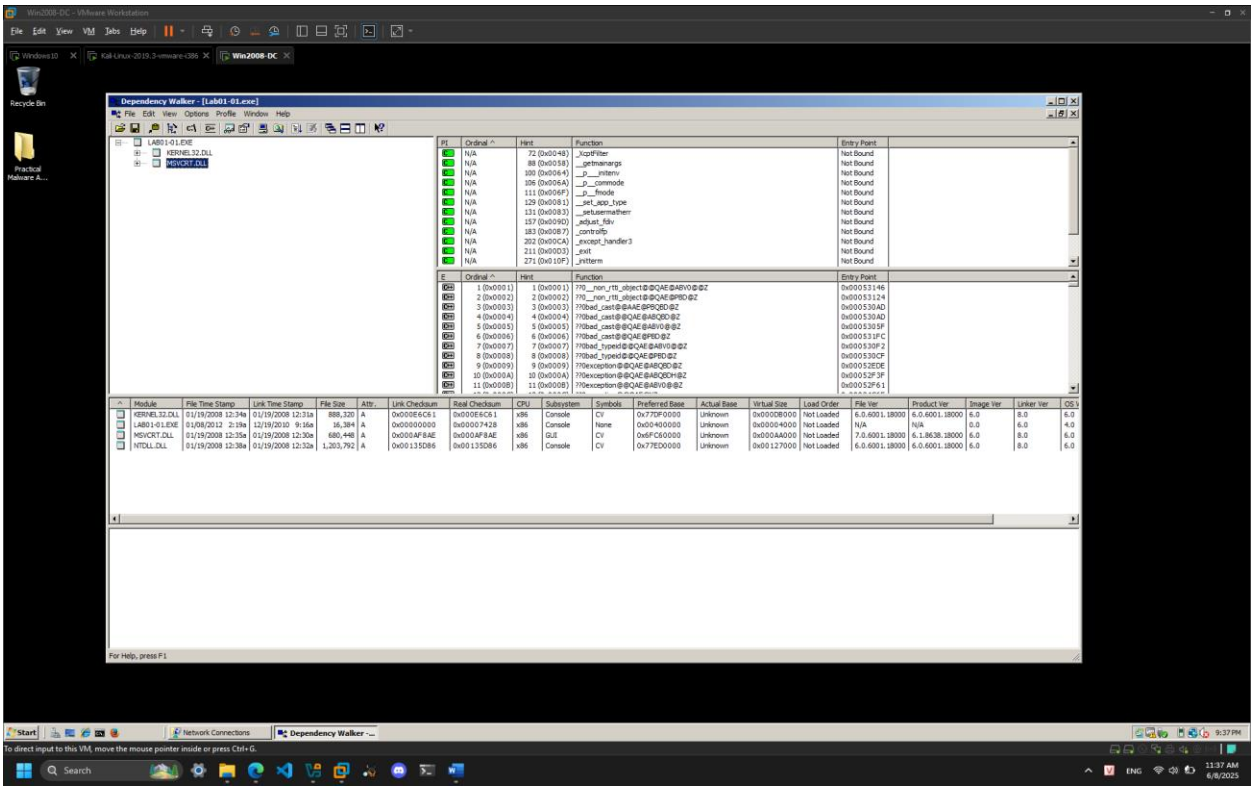
Look at the strings for Lab01-01.dll:

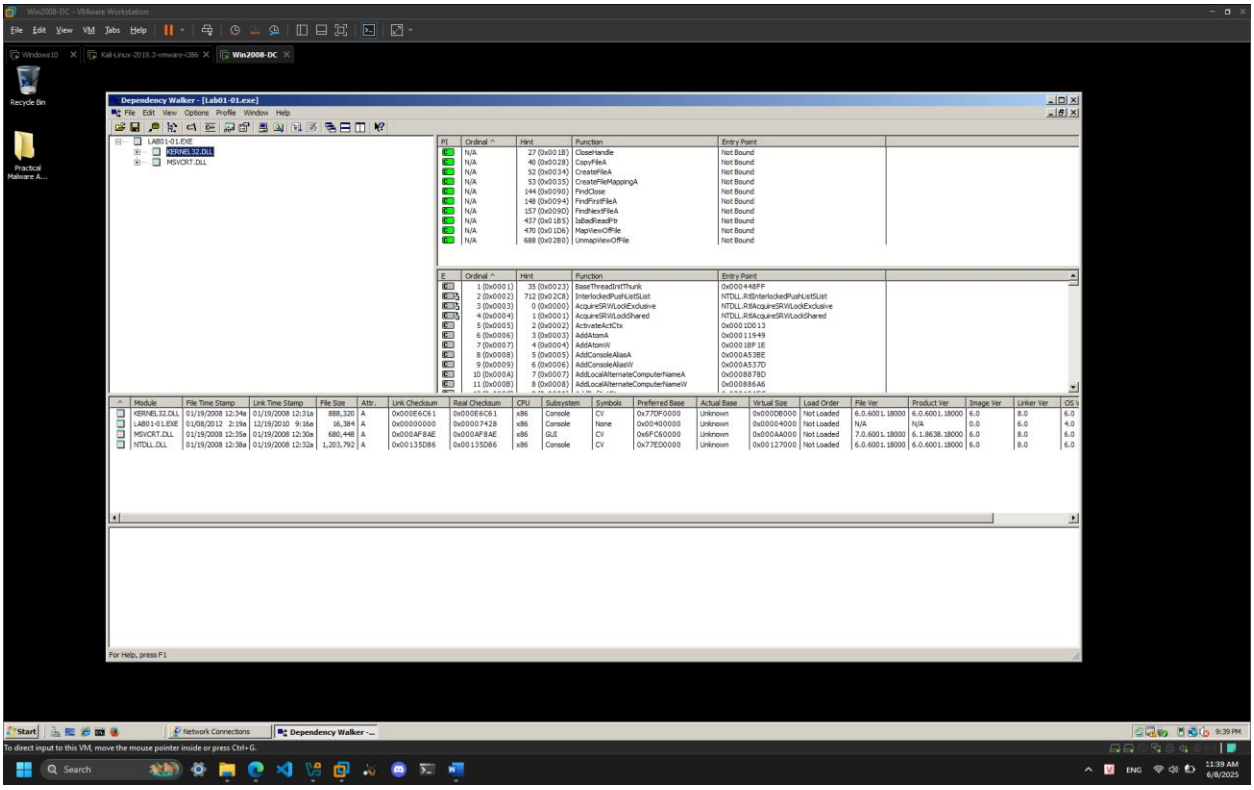


Open Dependency Walker:

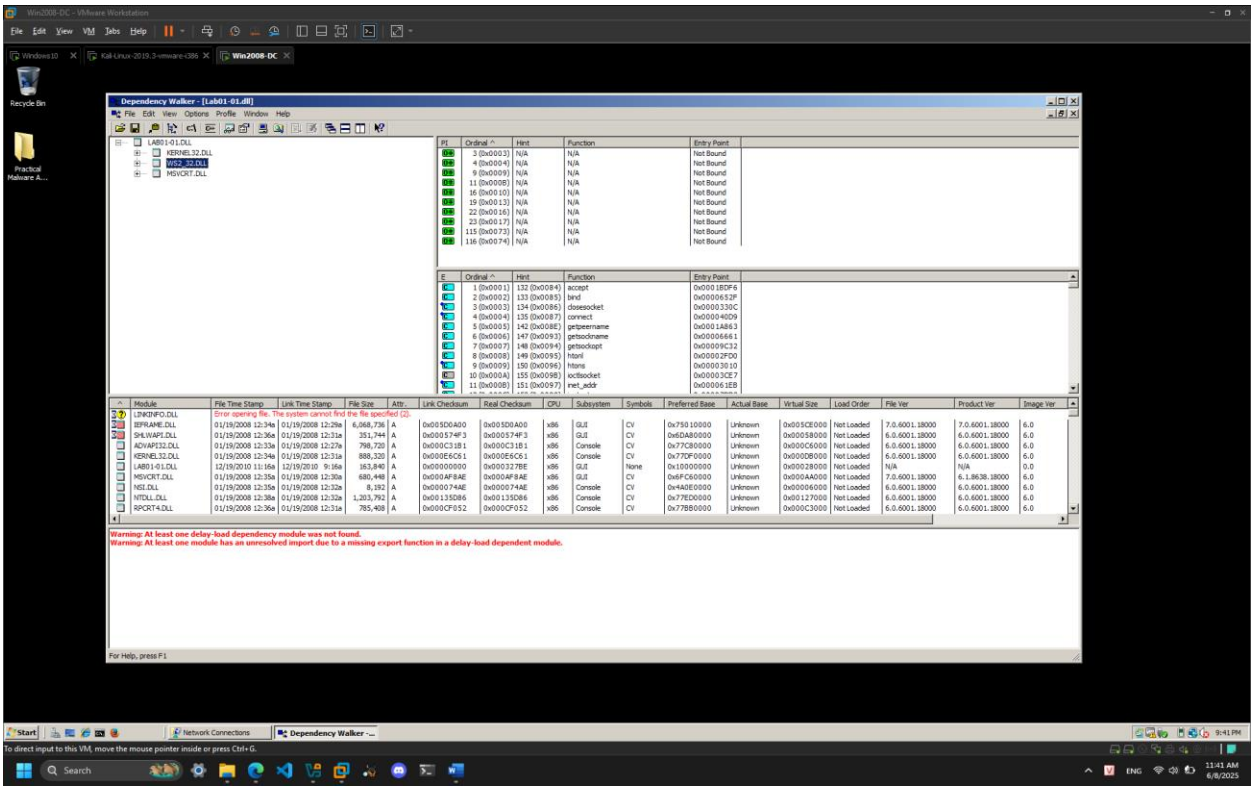


Open Lab01-01.exe in Dependency Walker:



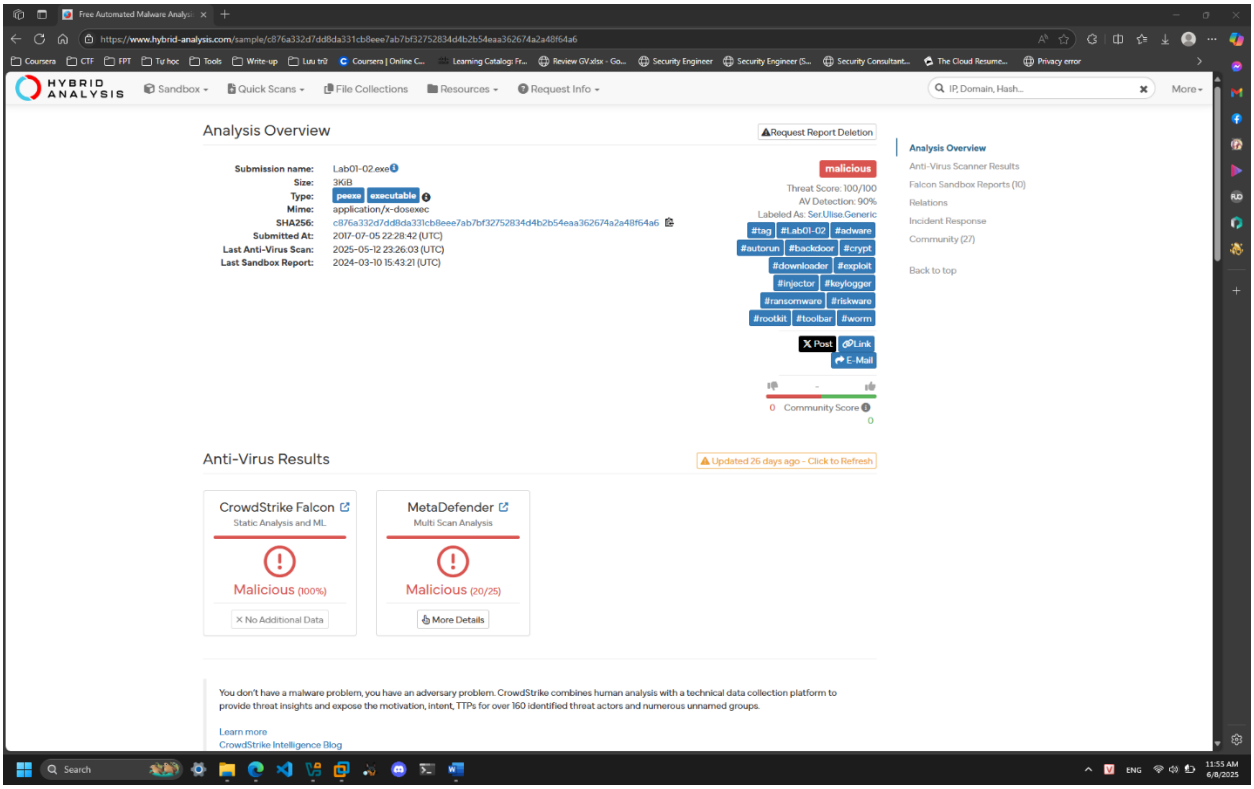


Open Lab01-01.dll in Dependency Walker:

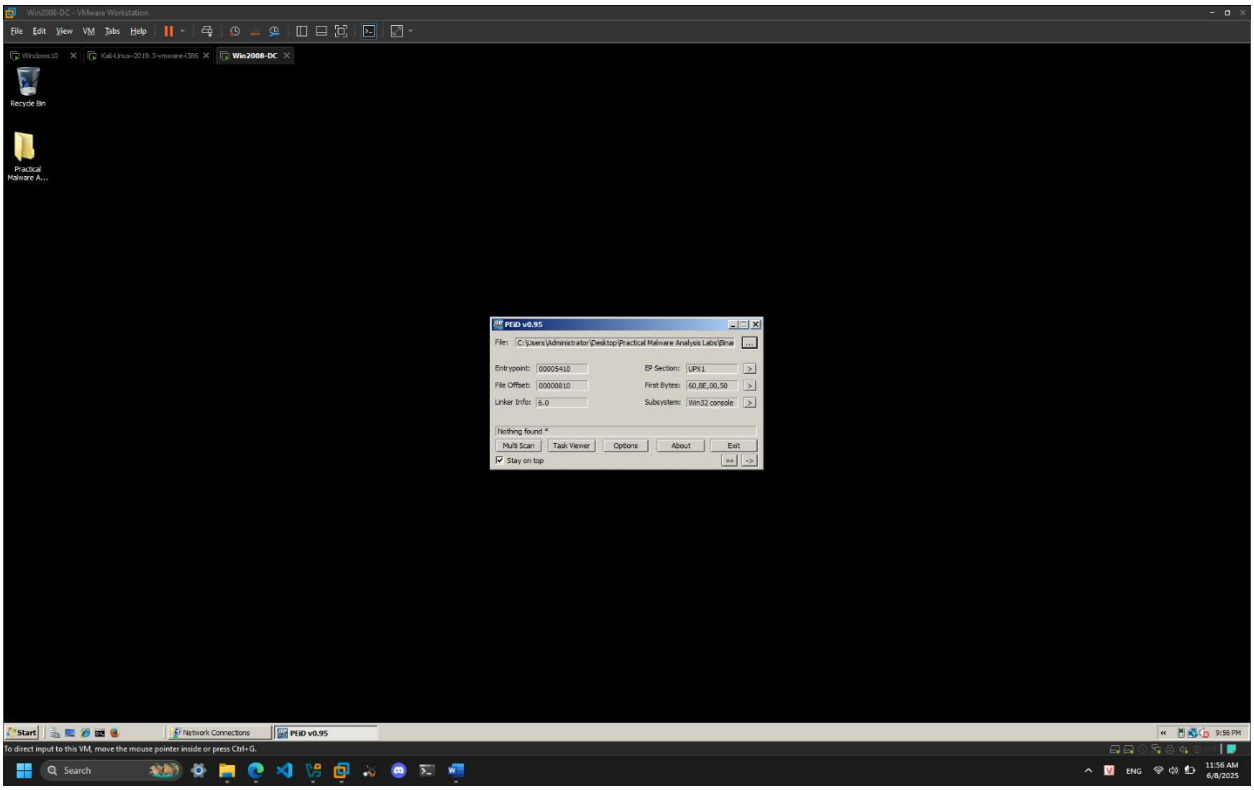


b. Lab01-02.exe

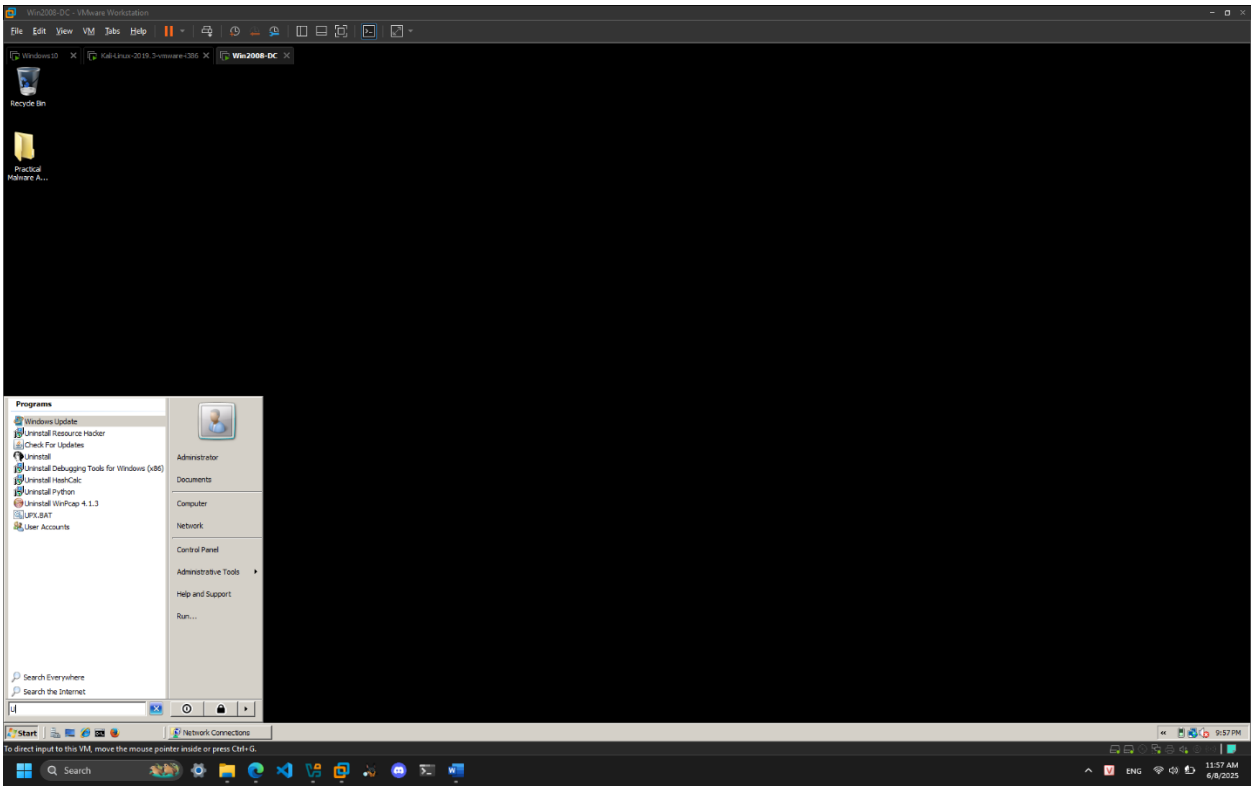
Upload the Lab01-02.exe file to https://www.hybrid analysis.com:



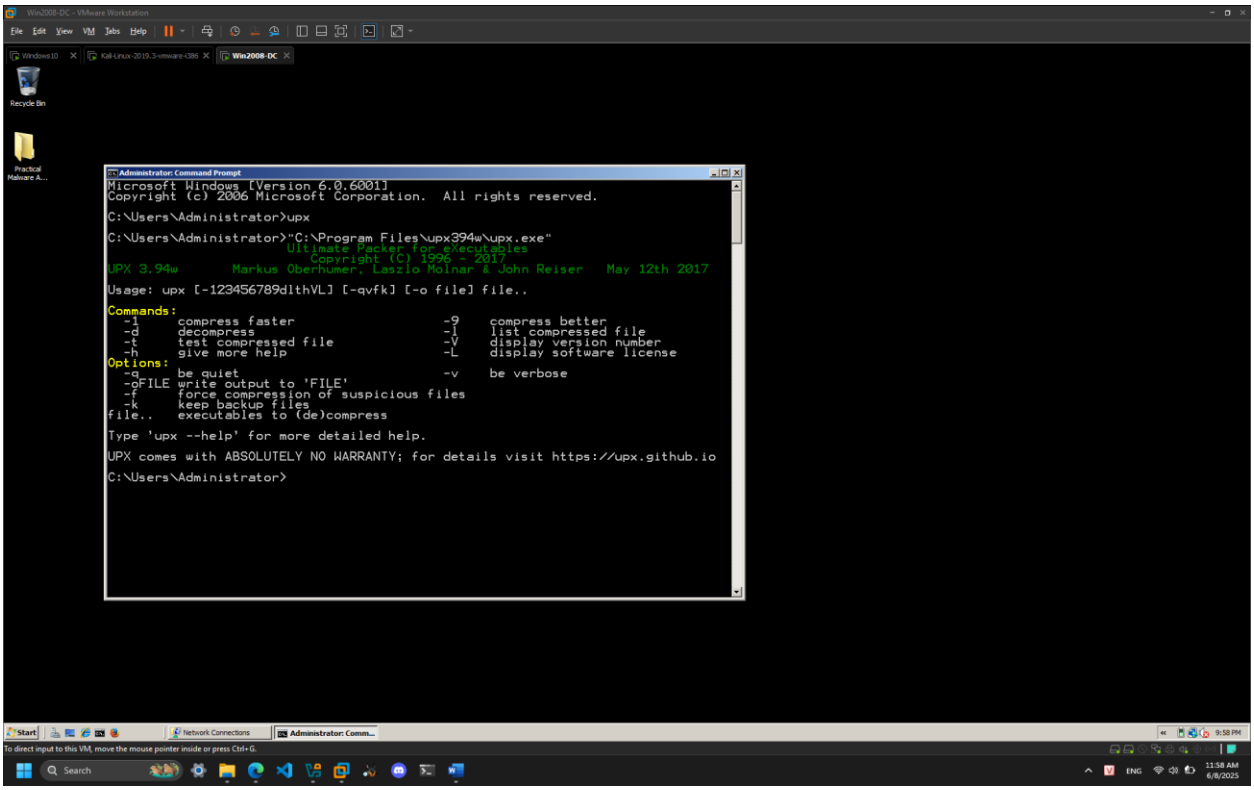
Run PEiD on the file:



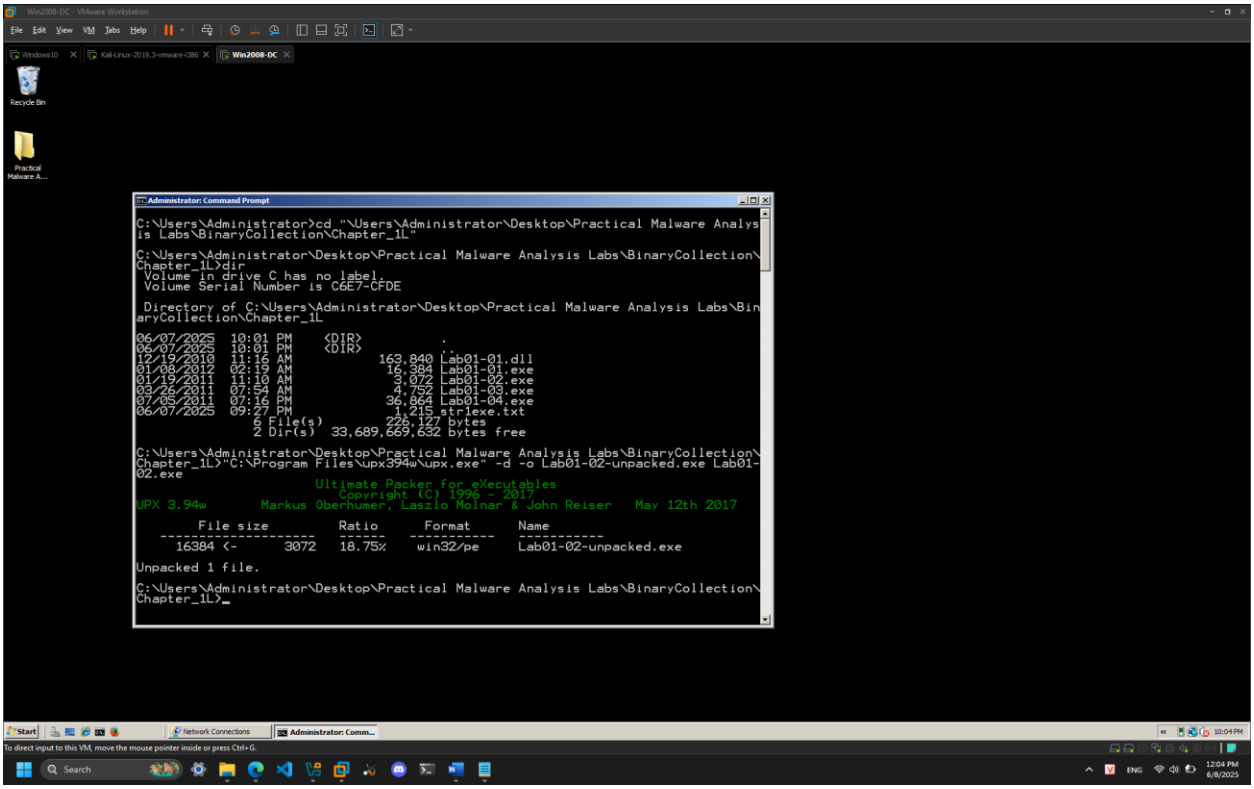
Open UPX:



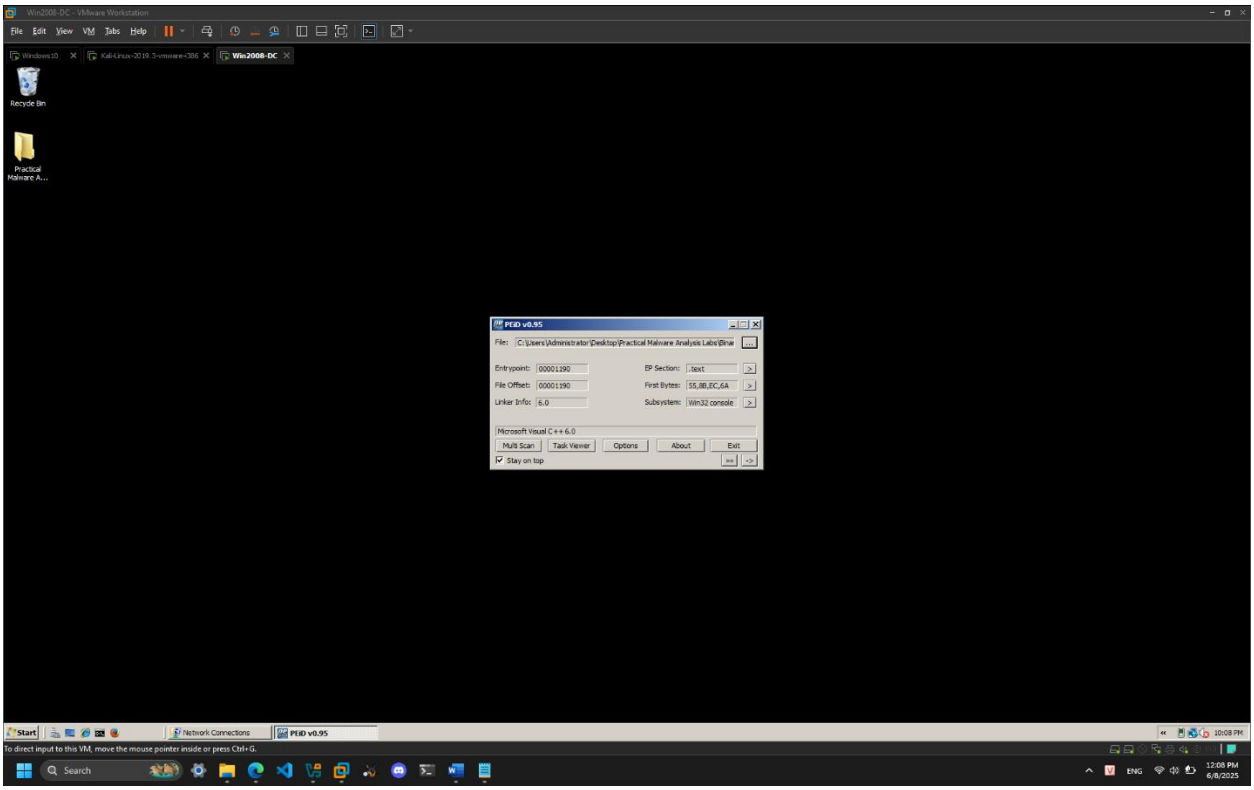
Open a Command Prompt window and execute UPX command:



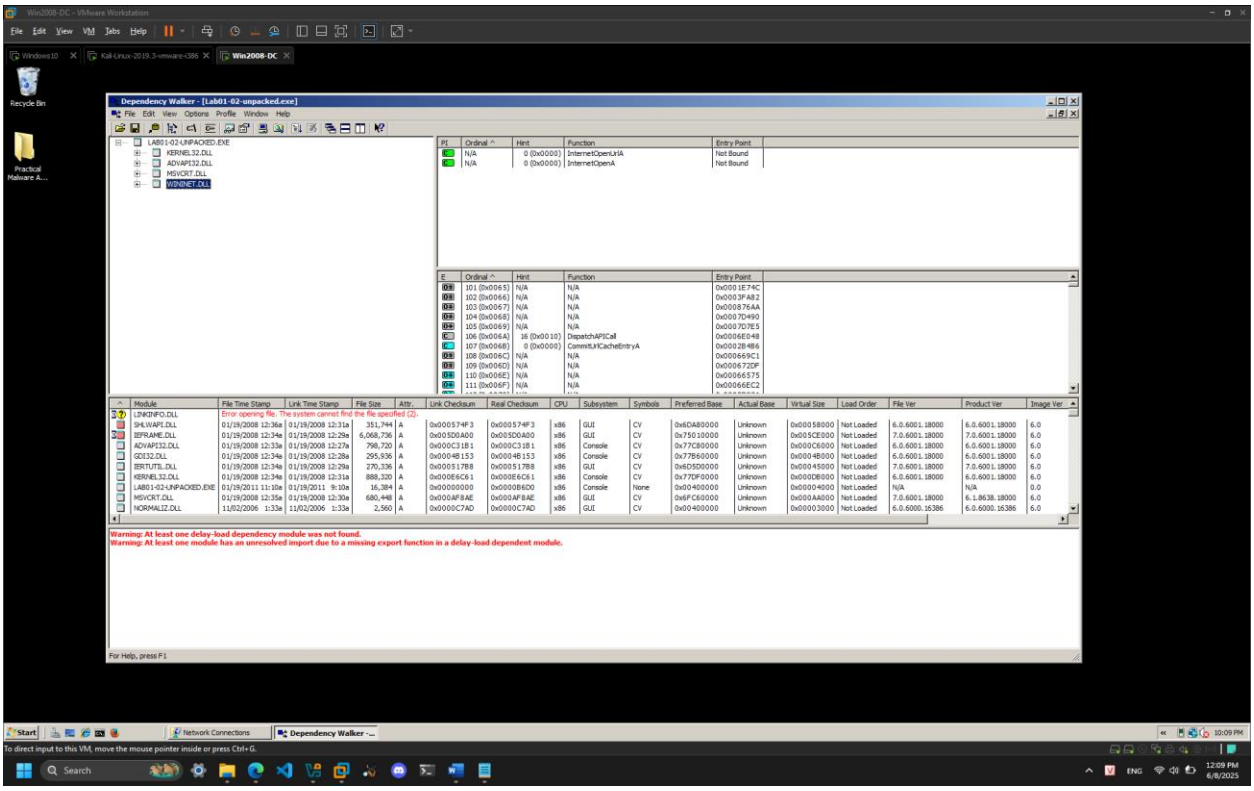
Use the CD command to move to the directory containing your malware samples and unpack the file:



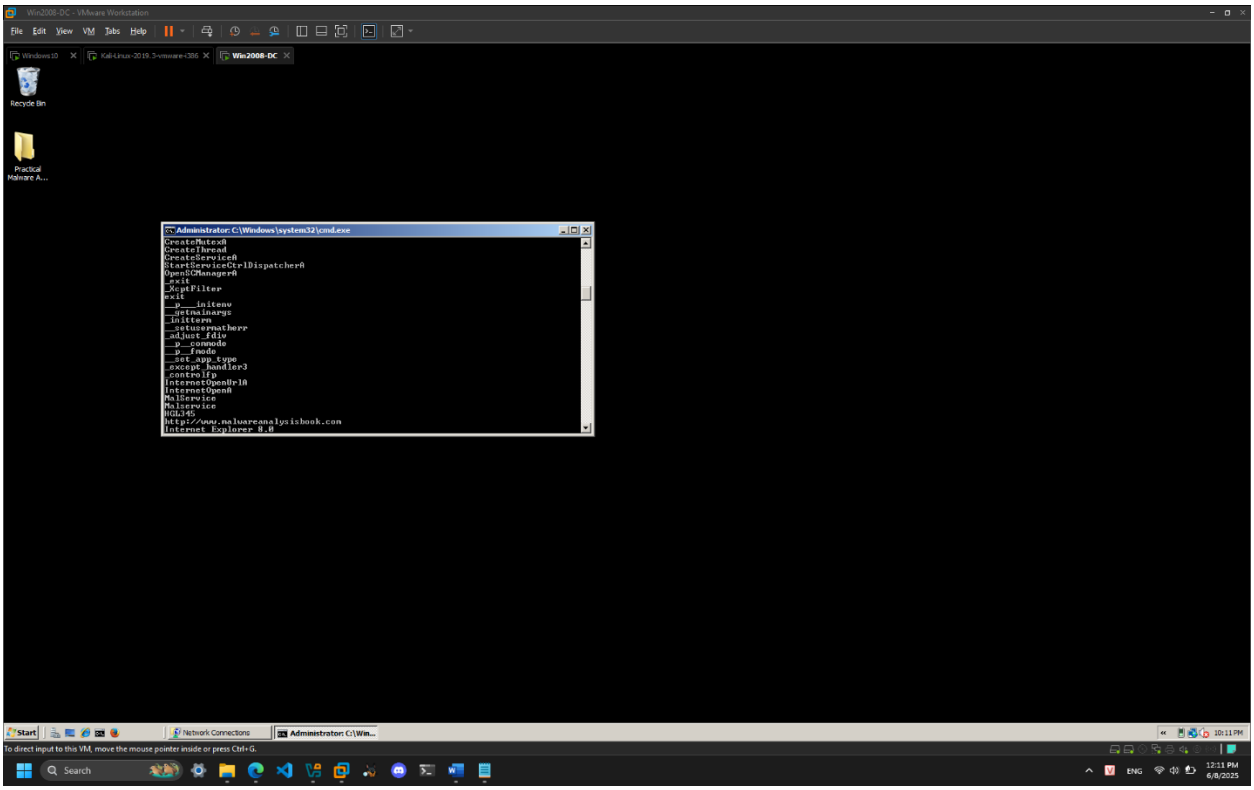
Analyze the unpacked file with PEiD:



Find the unpacked file's imports with Dependency Walker:

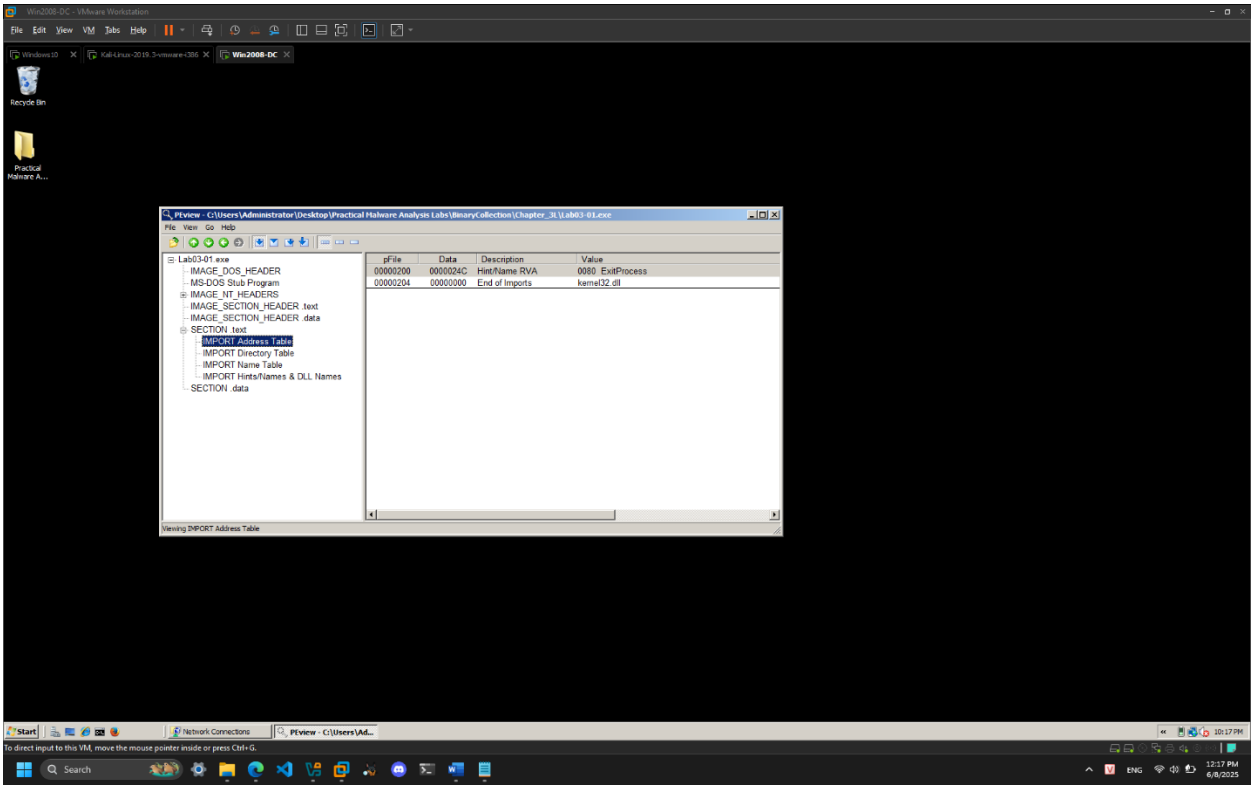


Find the strings in the unpacked file:

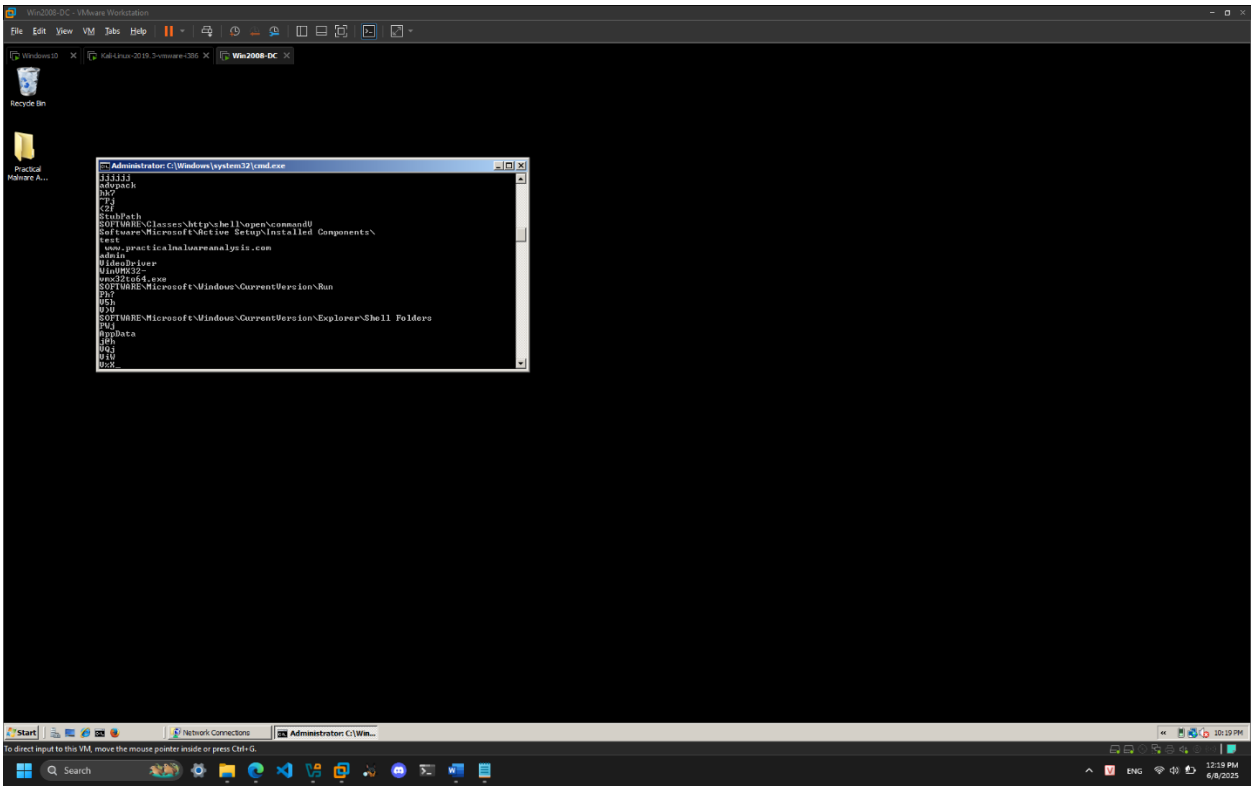


2. Basic Dynamic Techniques

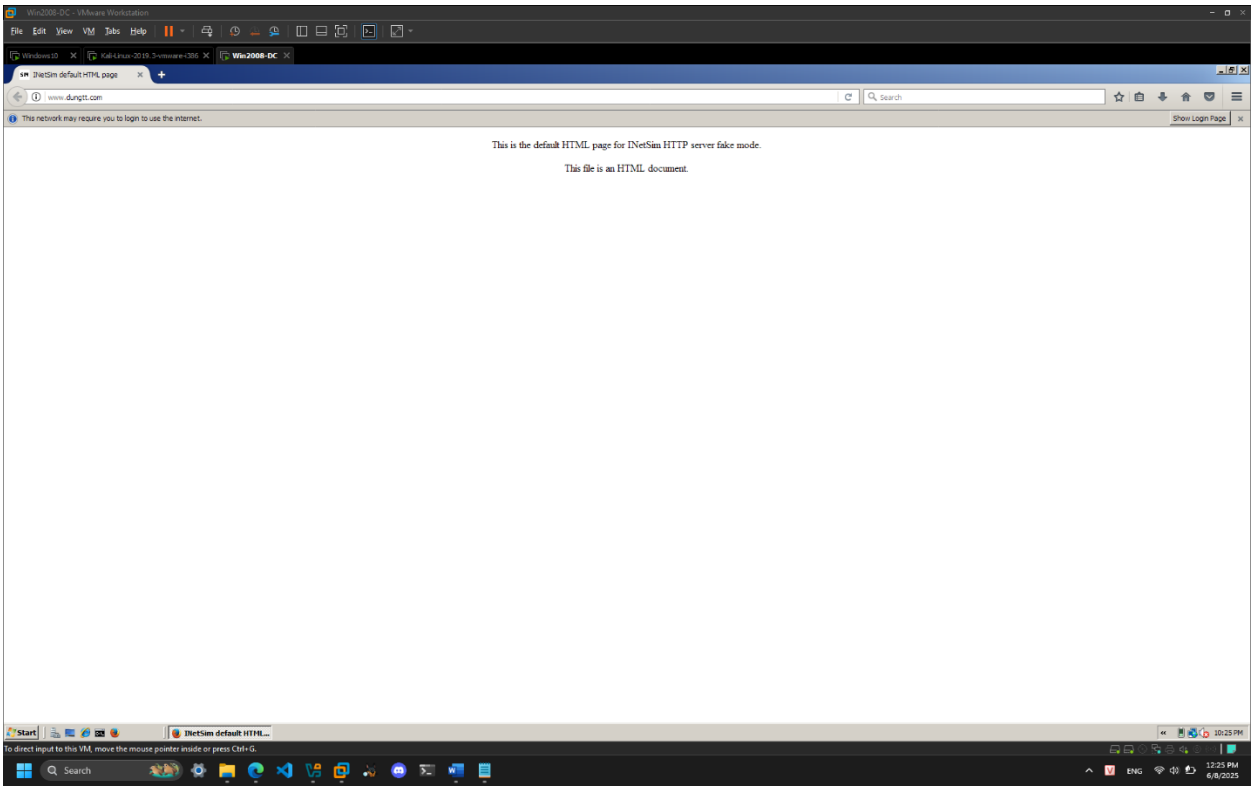
Open Lab03-01.exe in PEview:



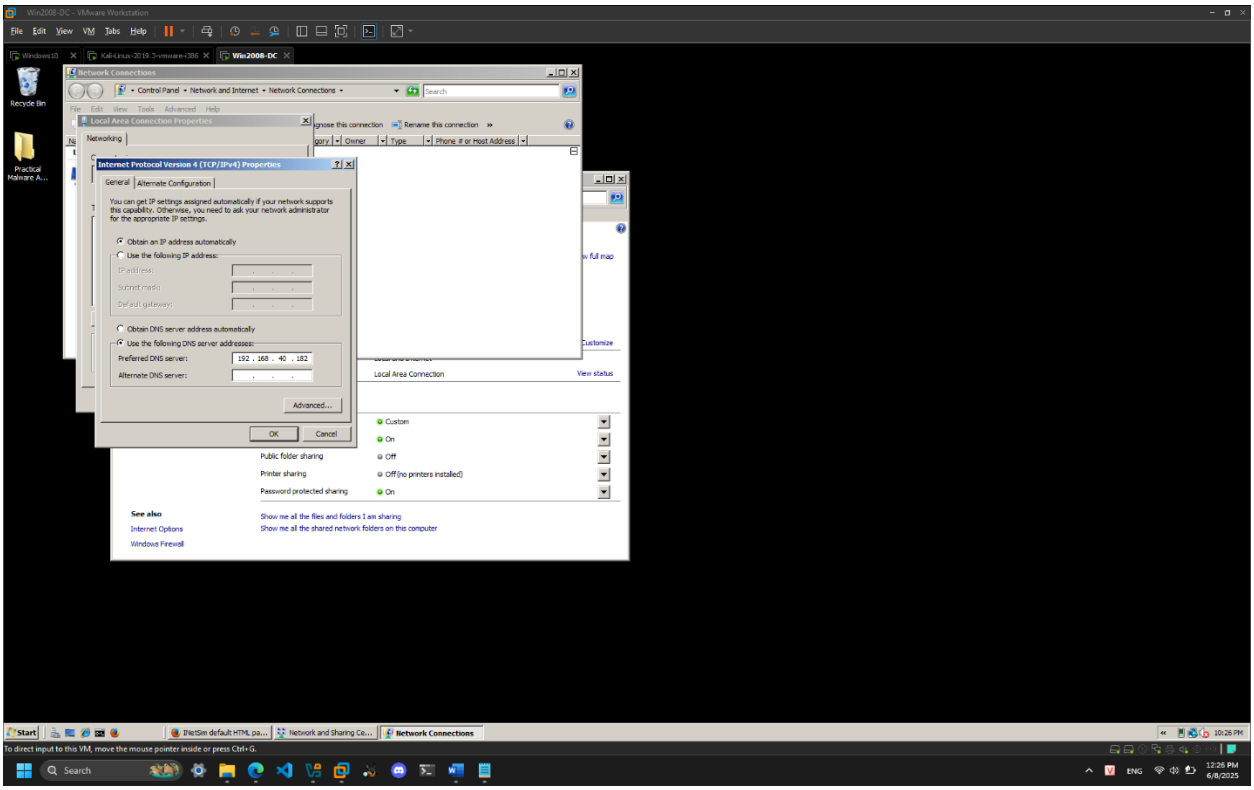
Examine the strings in Lab03-01.exe:



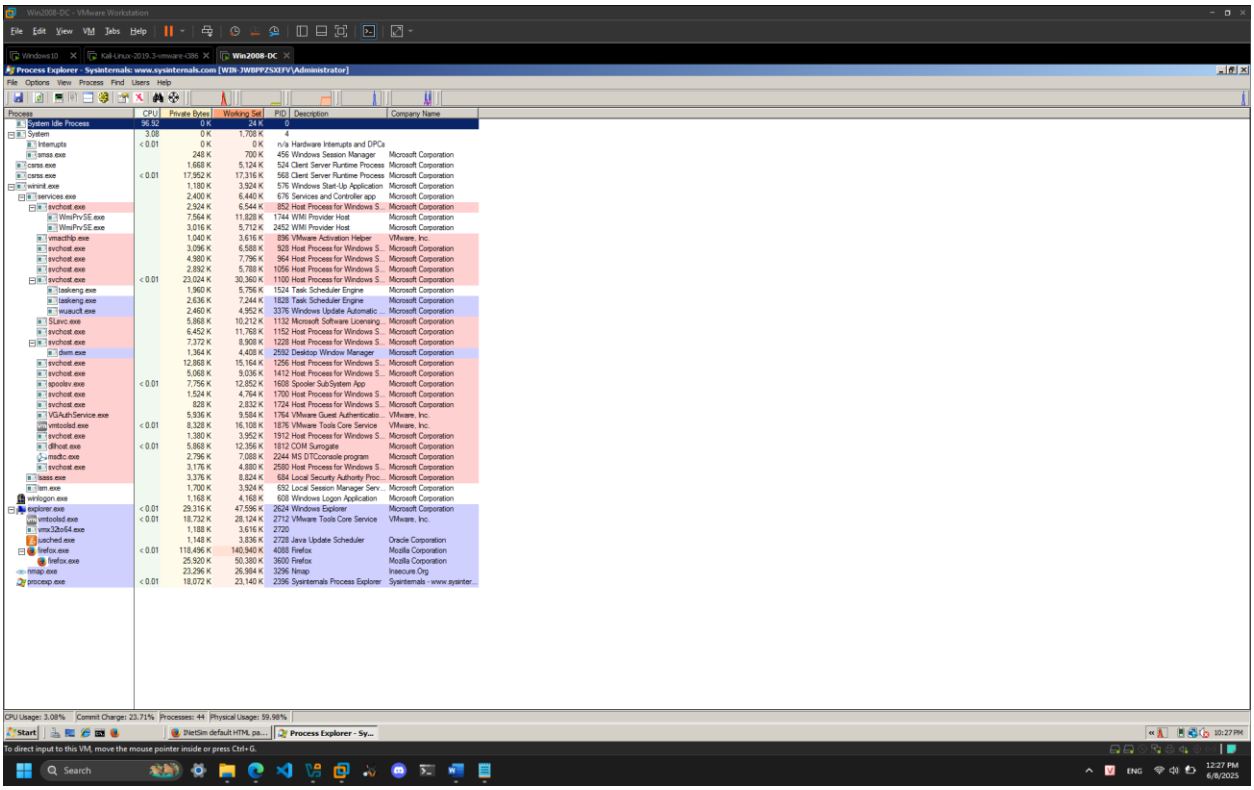
Start INetSim:



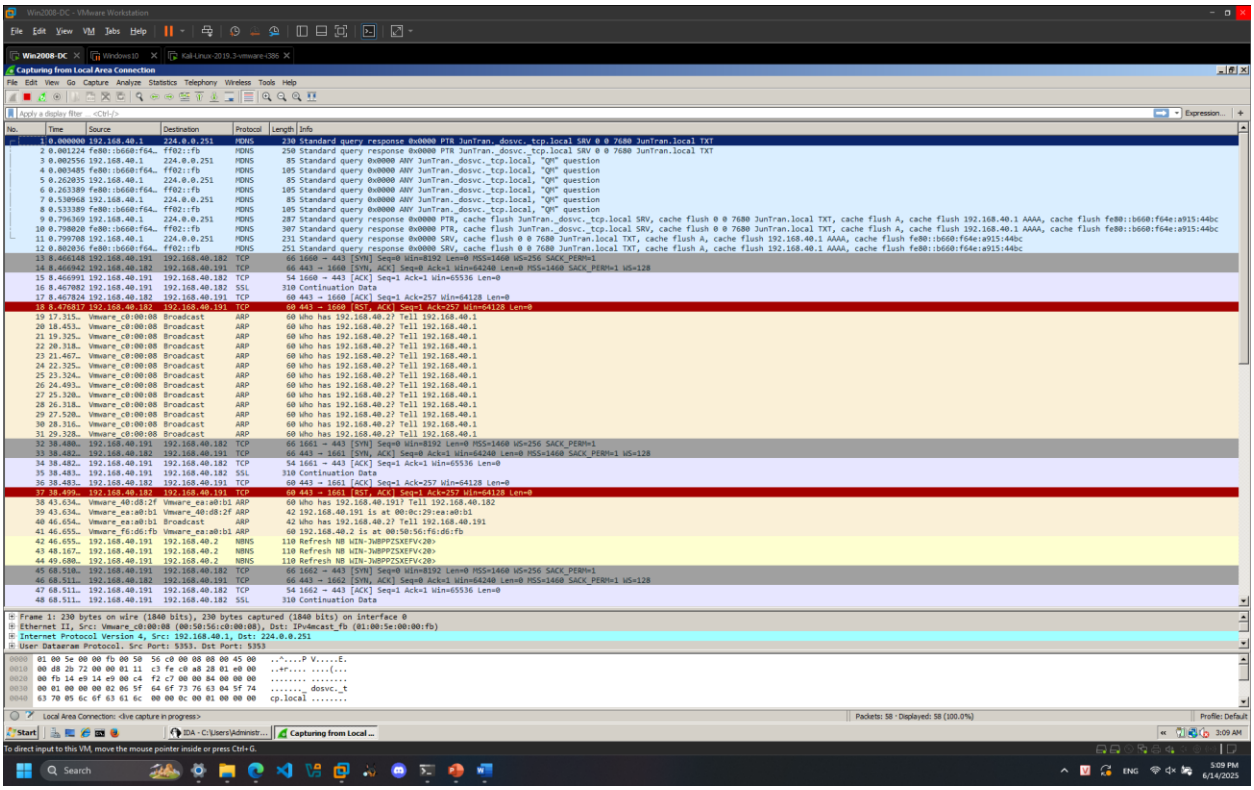
Setting the DNS Server:



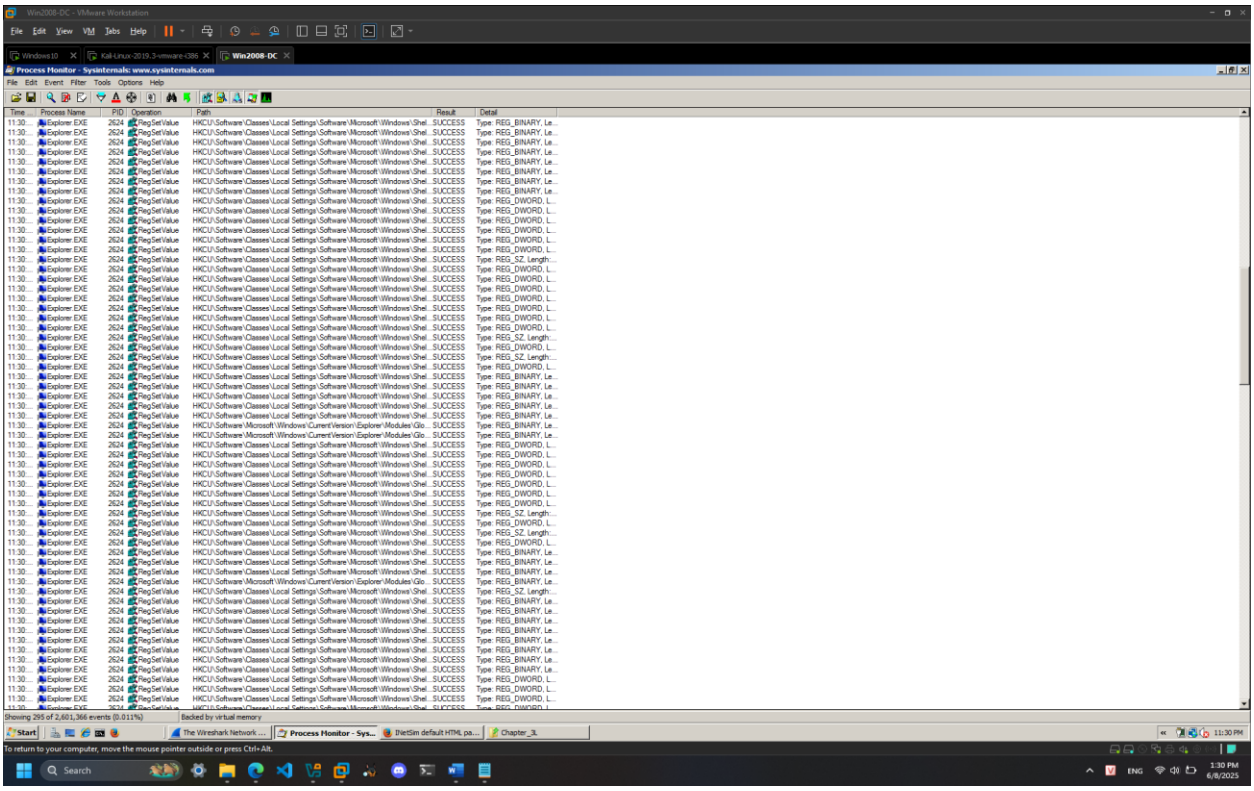
Run Process Explorer:



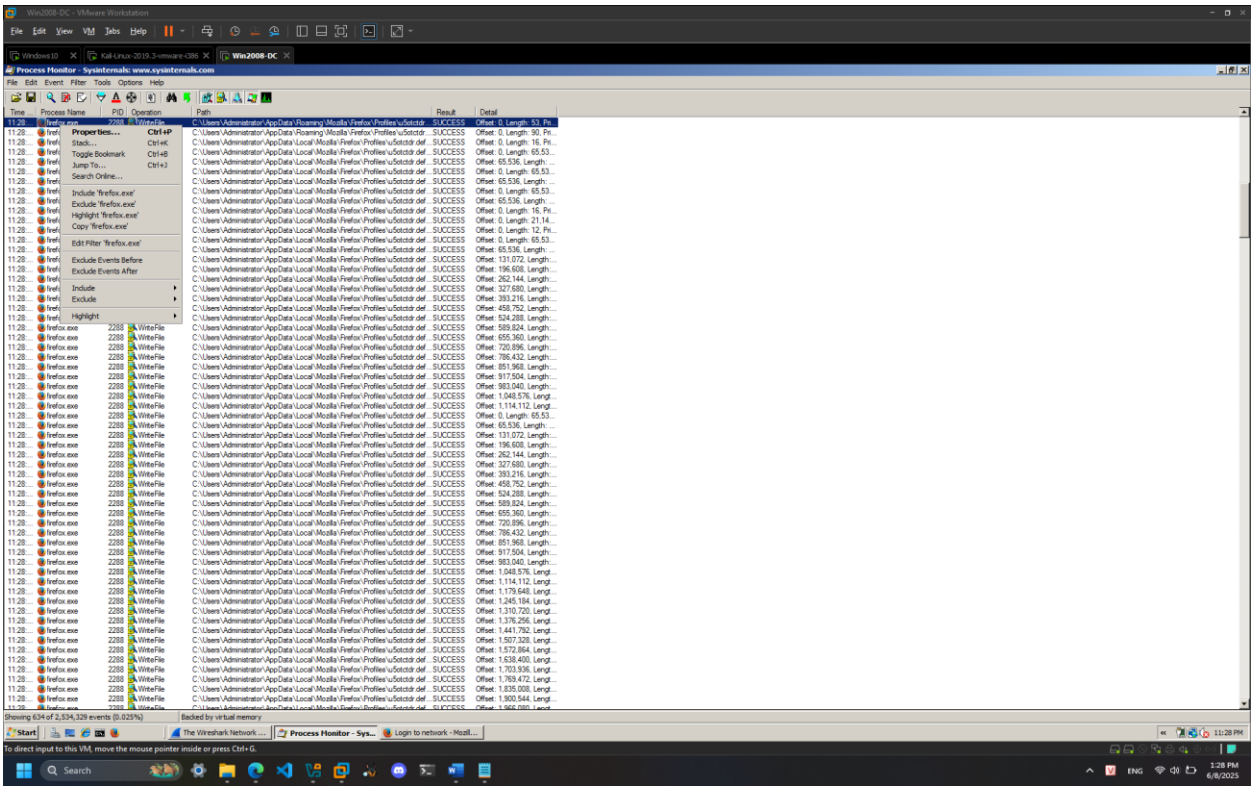
Run Wireshark:

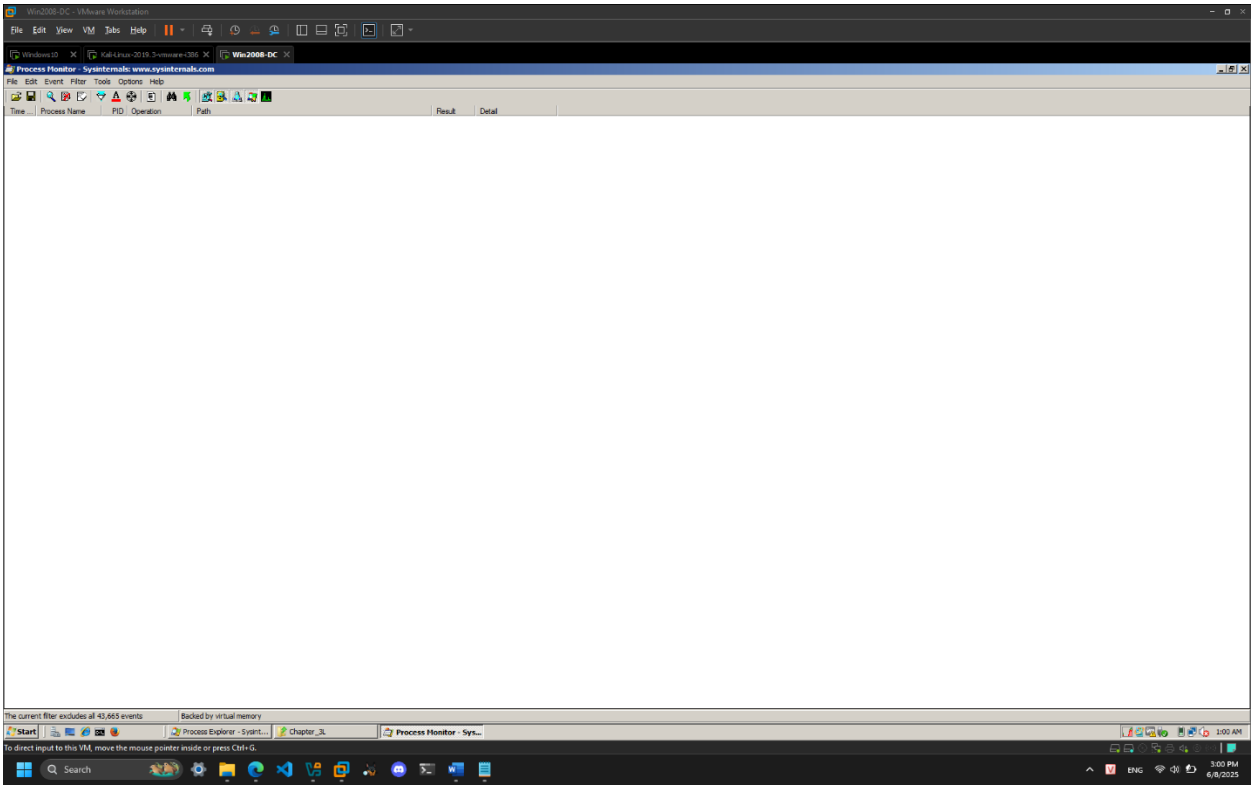


Start Process Monitor:

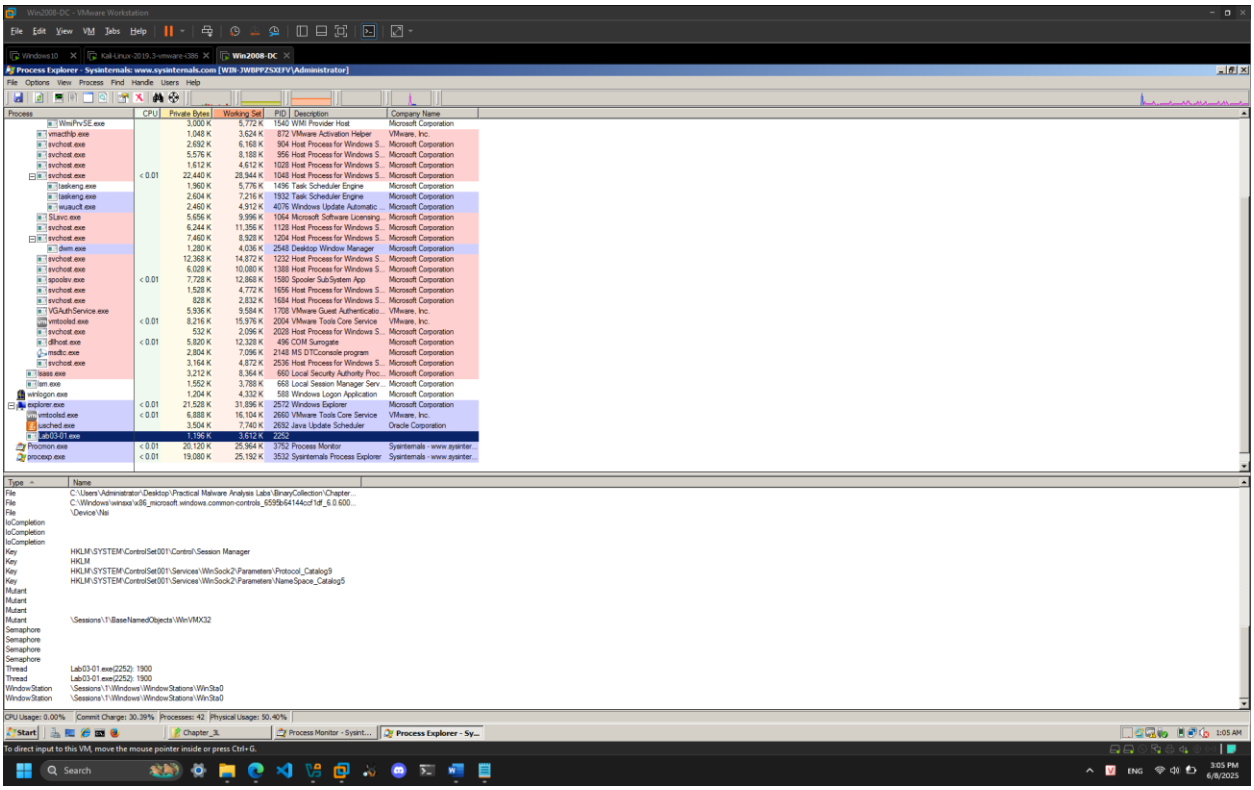


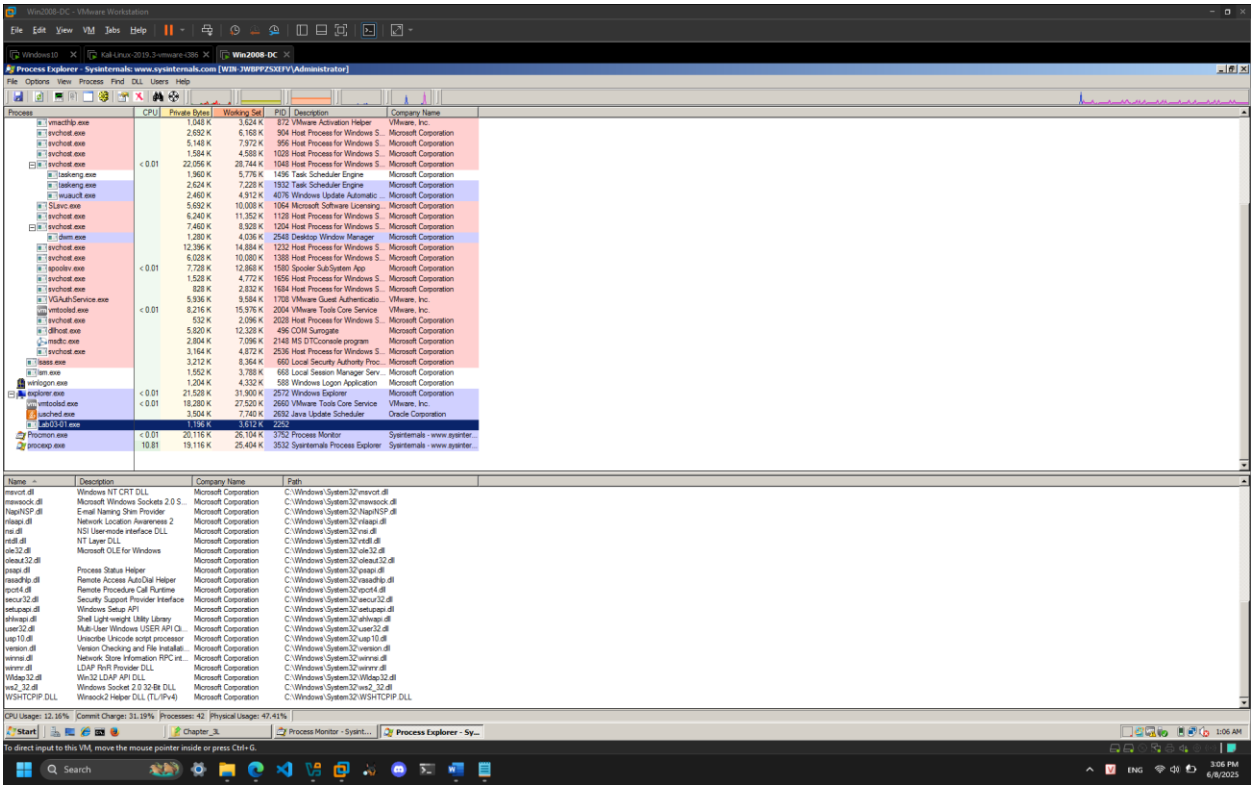
Excluding Harmless Processes:



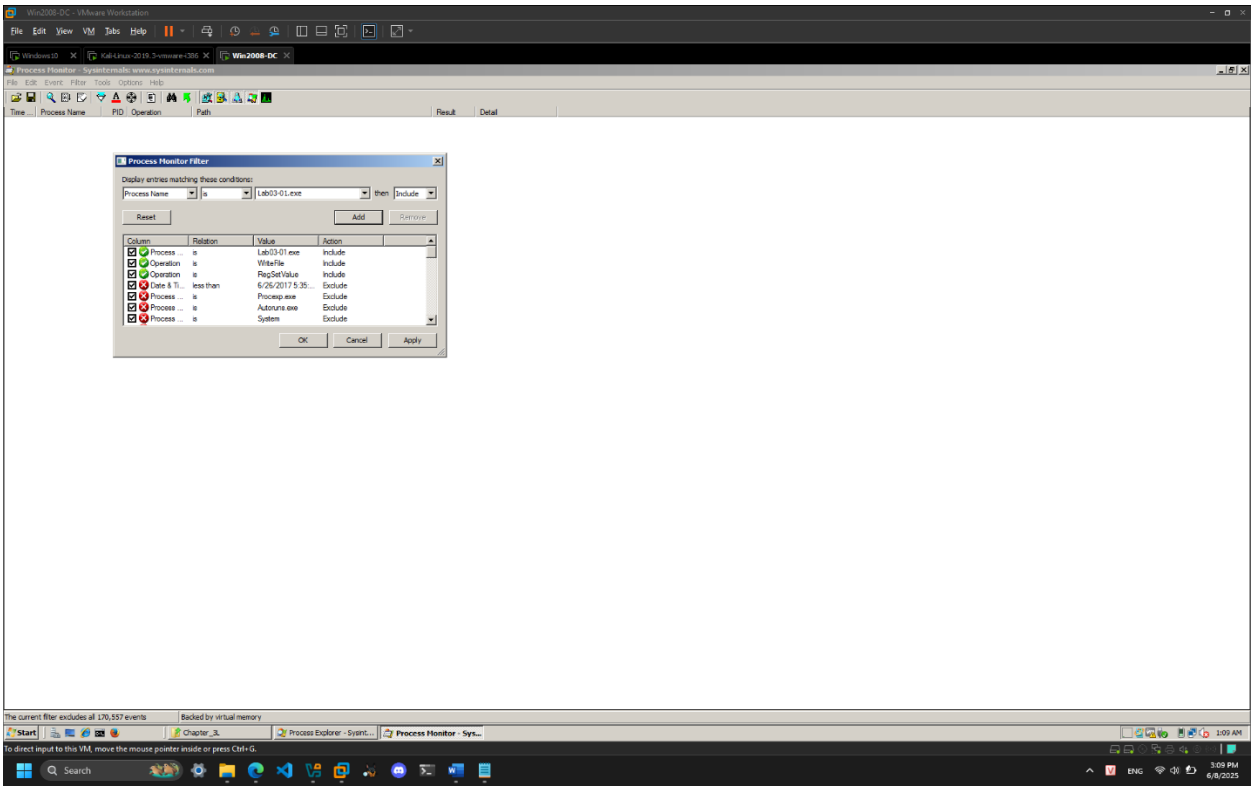


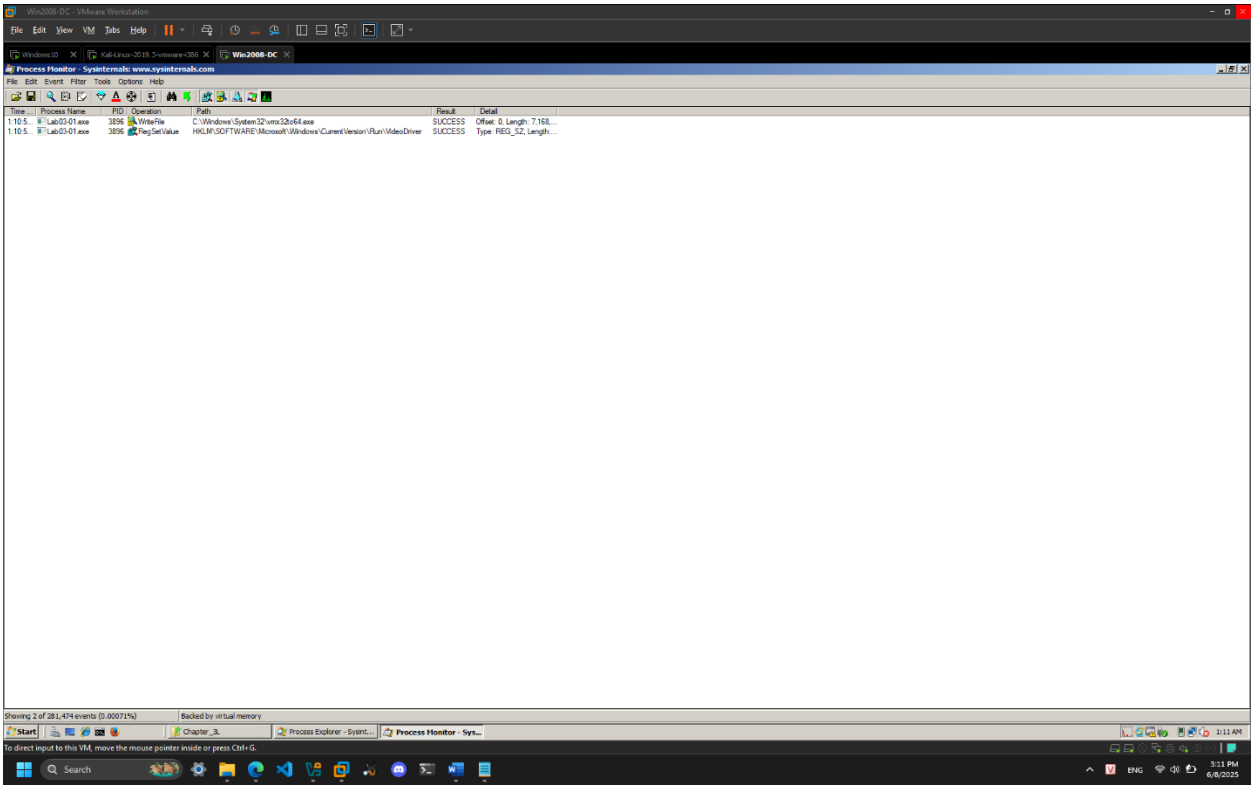
Run the Lab03-01.exe File and Viewing the Running Malware in Process Explorer:

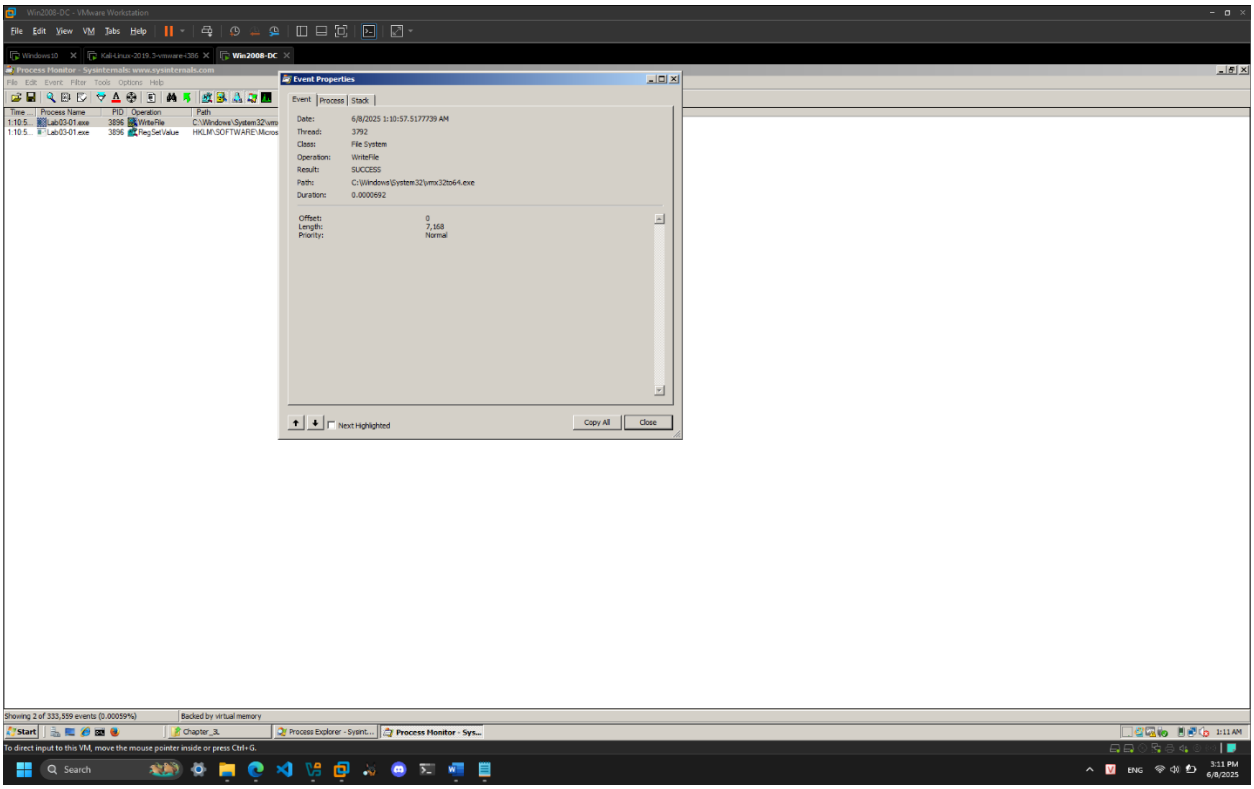


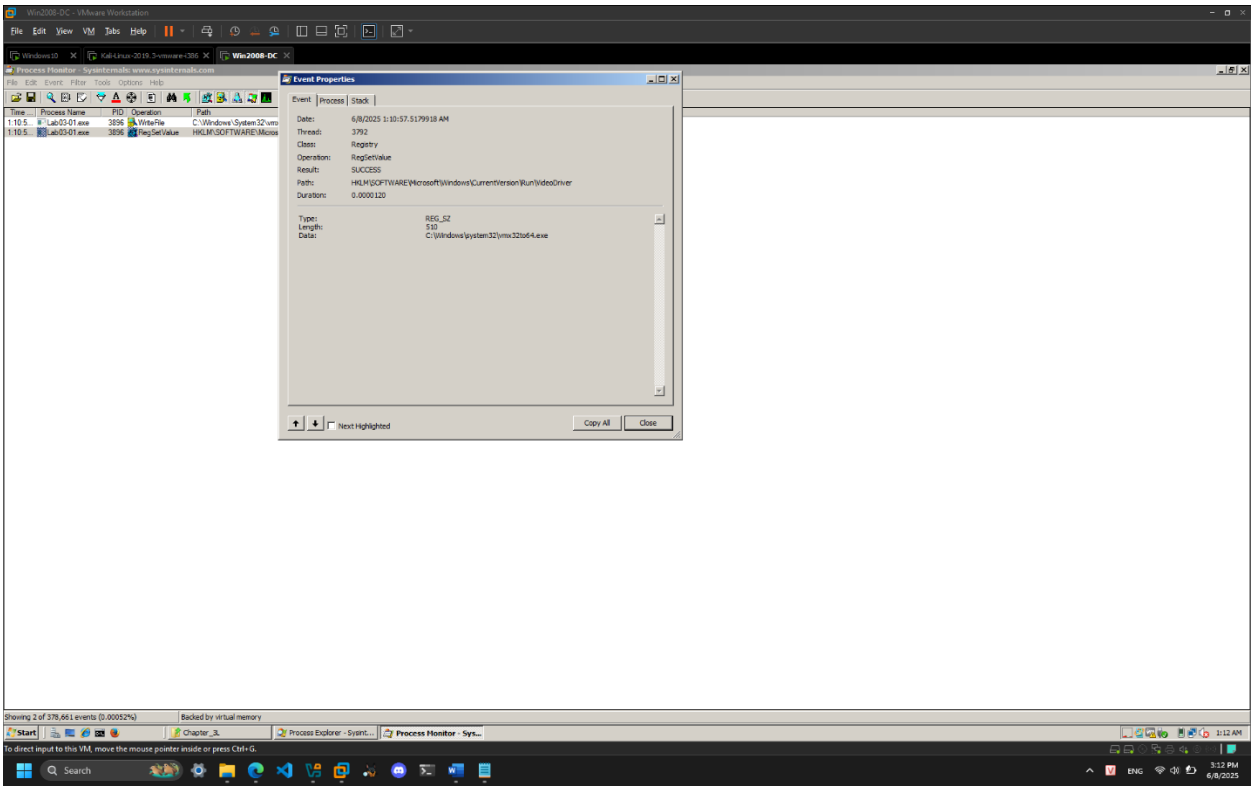


Viewing the Malicious Process's Events in Process Monitor:

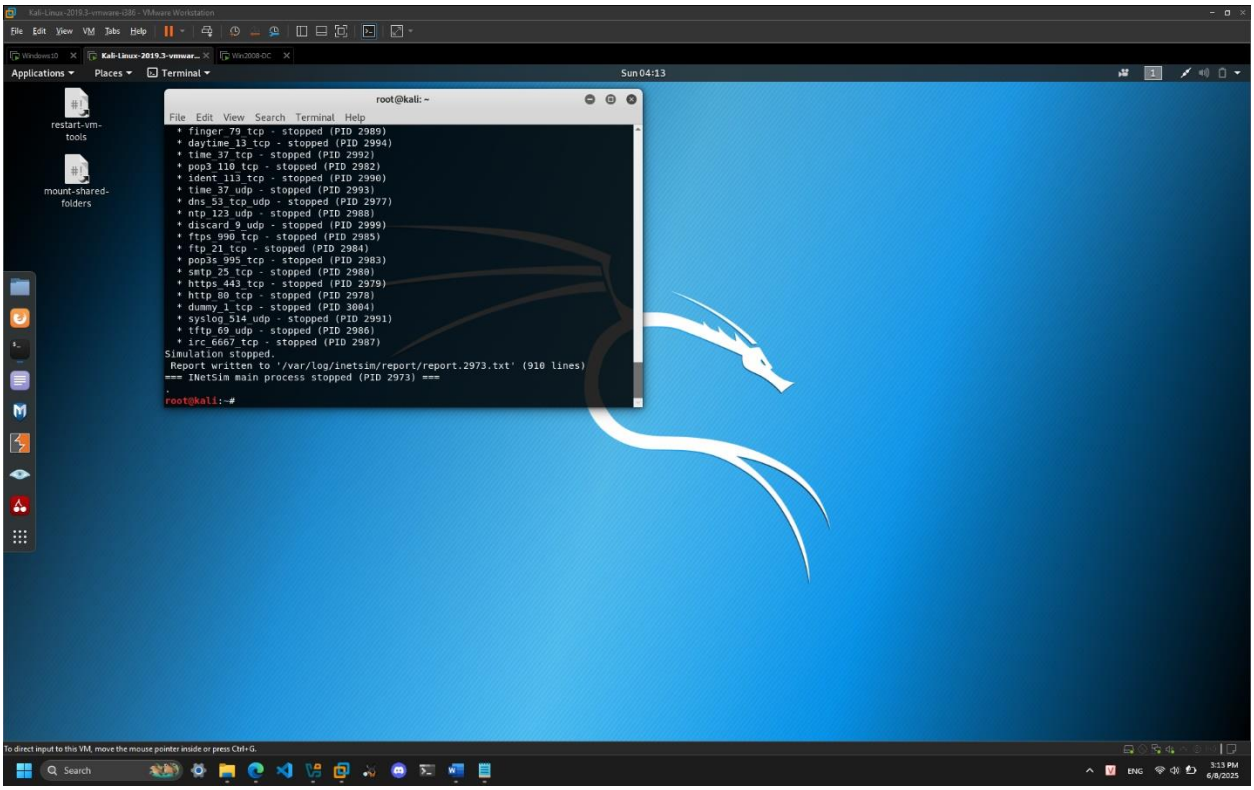


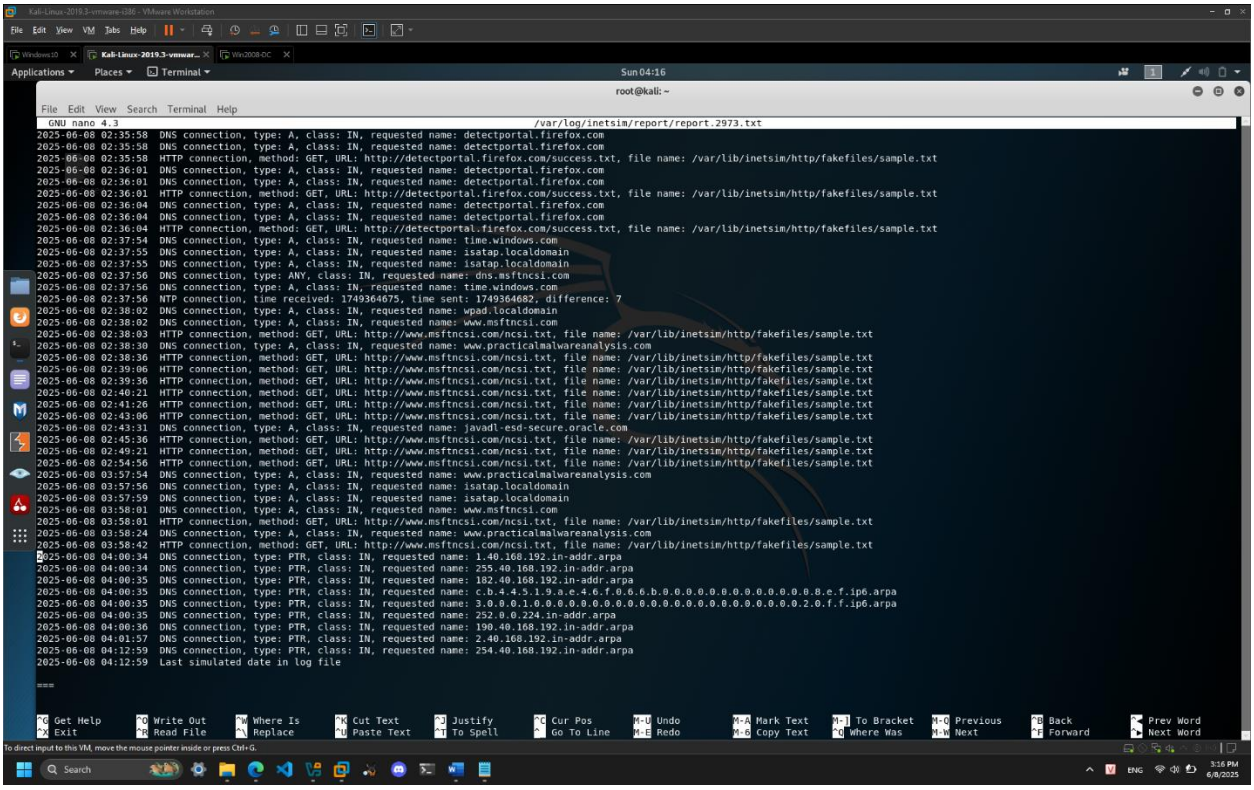



Win2008-DC - VMware Workstation
Process Monitor - Sysinternals: www.sysinternals.com
Event Properties
Event
Process
Stack
Date: 6/8/2025 1:10:57.5177739 AM
Thread: 3792
Class: File System
Operation: WriteFile
Result: SUCCESS
Path: C:\Windows\System32\vmx32to64.exe
Duration: 0.0000692
Offset: 0
Length: 7,168
Priority: Normal
Next Highlighted
Copy All
Close
Showing 2 of 333,559 events (0.00059%)
Backed by virtual memory


Win2008-DC - VMware Workstation
Process Monitor - Sysinternals: www.sysinternals.com
Event Properties
Event
Process
Stack
Date: 6/8/2025 1:10:57.5179918 AM
Thread: 3792
Class: Registry
Operation: RegSetValue
Result: SUCCESS
Path: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\VideoDriver
Duration: 0.0000120
Type: REG_SZ
Length: 510
Data: C:\Windows\system32\vmx32to64.exe
Next Highlighted
Copy All
Close
Showing 2 of 378,661 events (0.00052%)
Backed by virtual memory

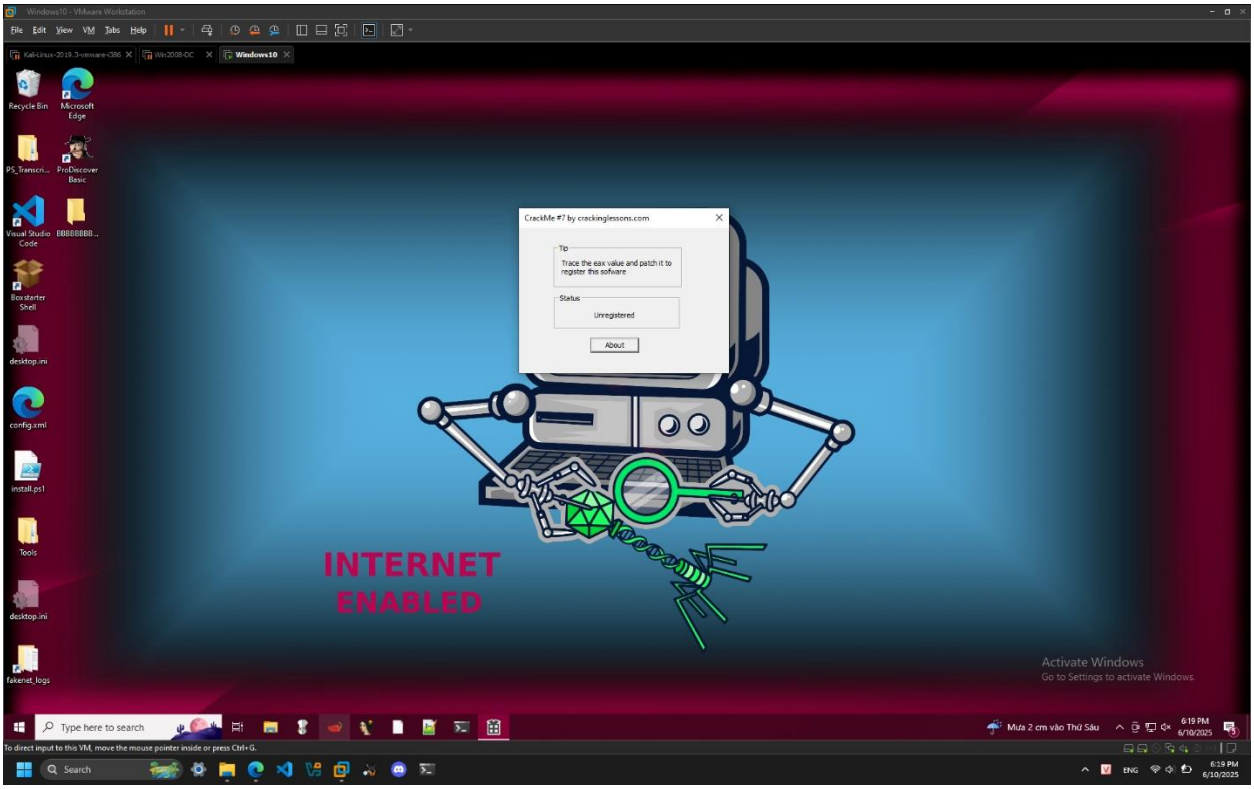
Viewing INetSim Logs:



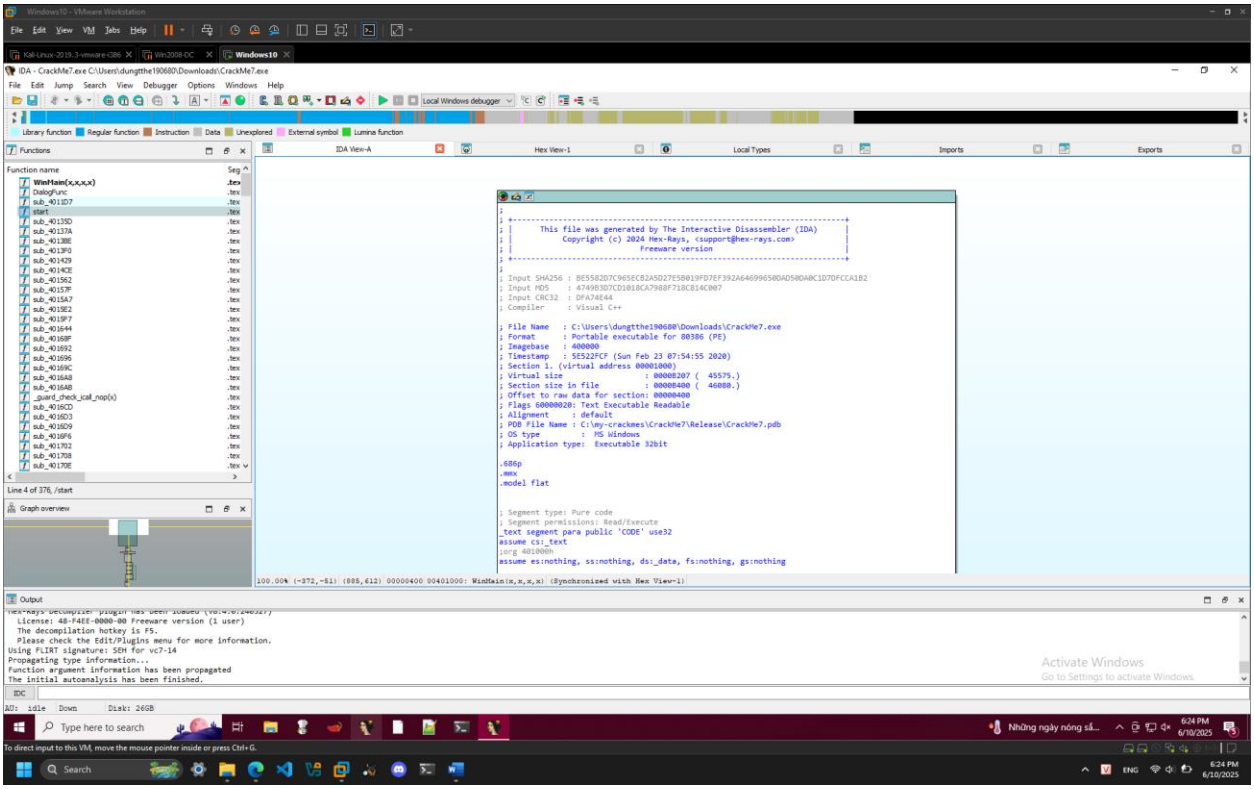


CrackMe #7

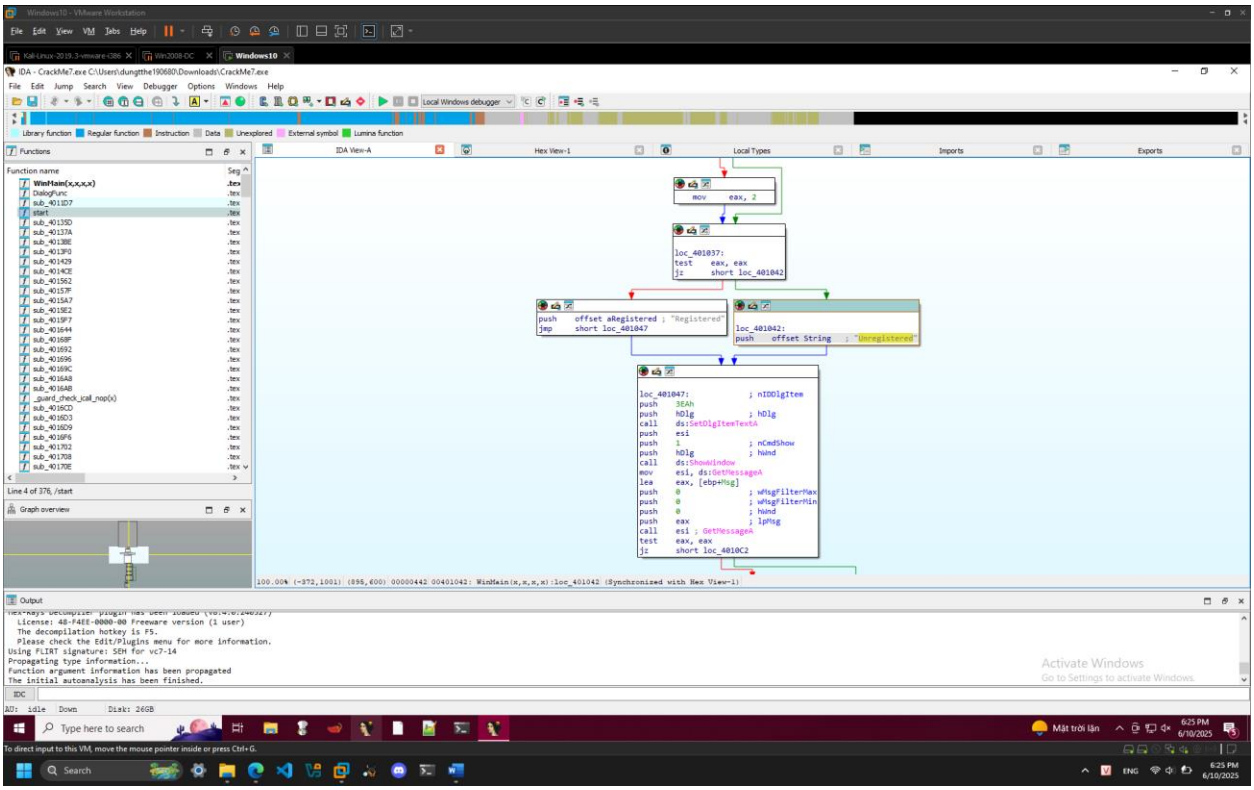
Đầu tiên em thử chạy chương trình và nhận được thông báo có từ khóa “Unregistered”:



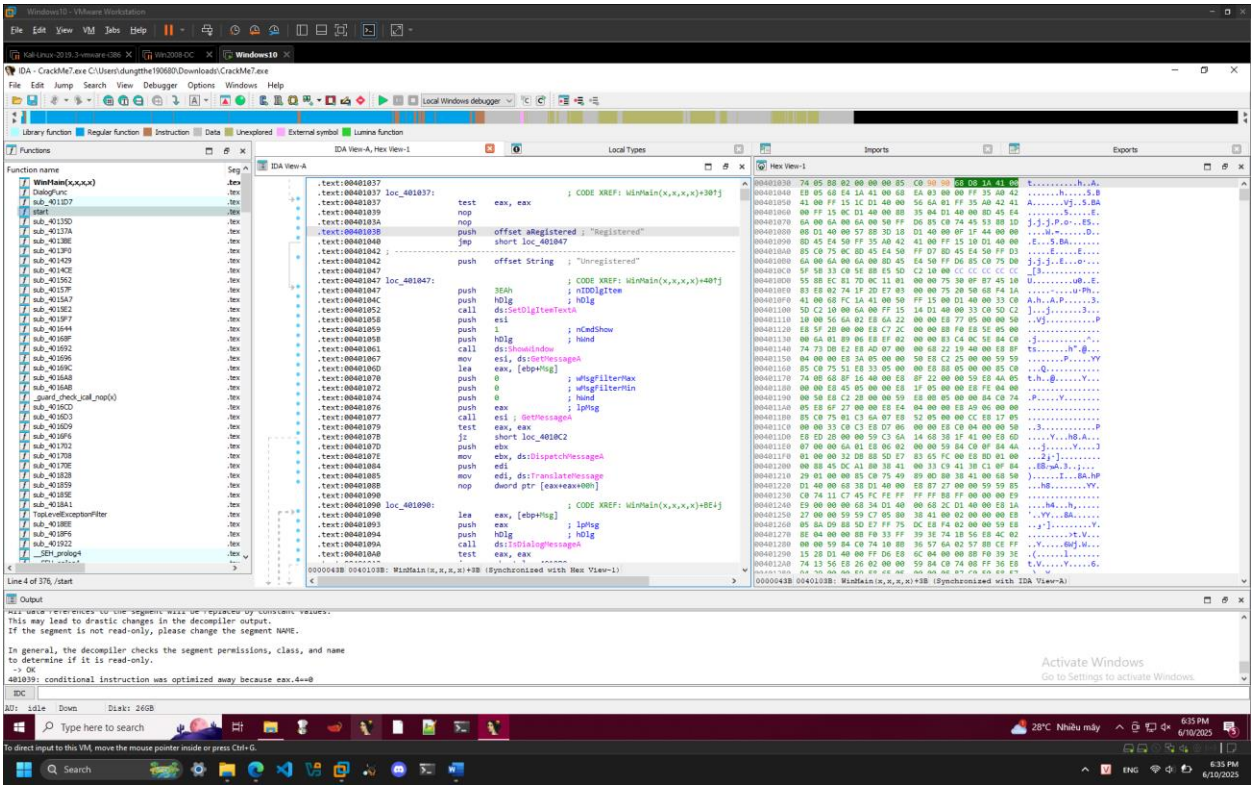
Sau đó em mở phần mềm IDA và tiến hành dịch ngược file:



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: