

## LAB 02

Thầy Mai Hoàng Đình  
Trường đại học FPT

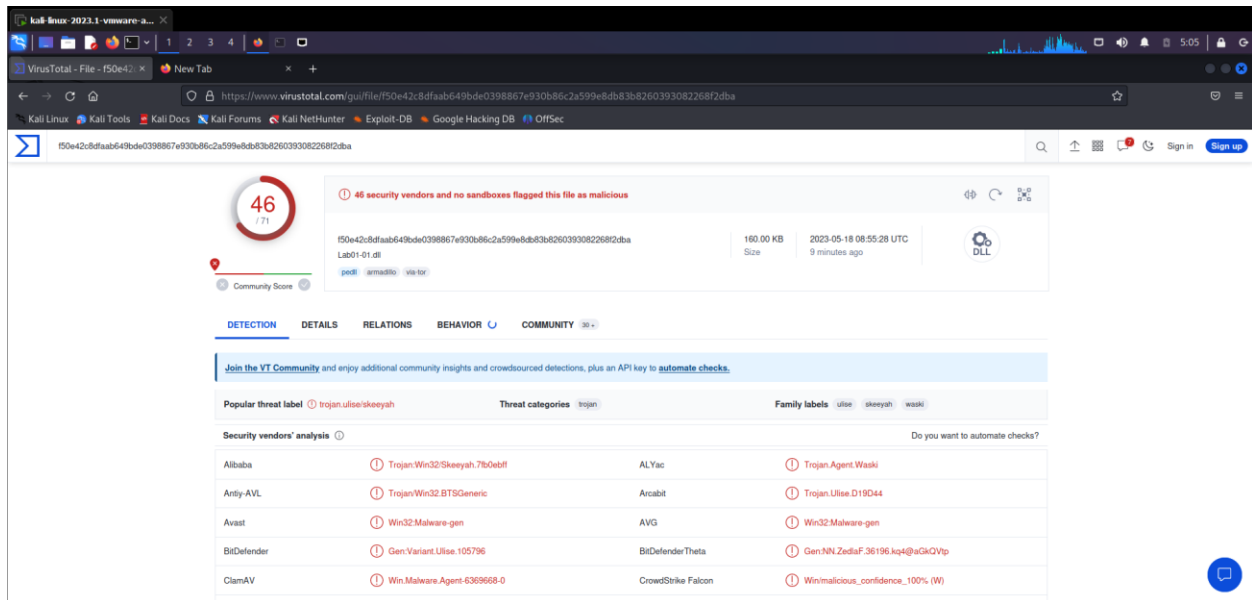
Người thực hiện

Đặng Hoàng Nguyên

## VirusTotal

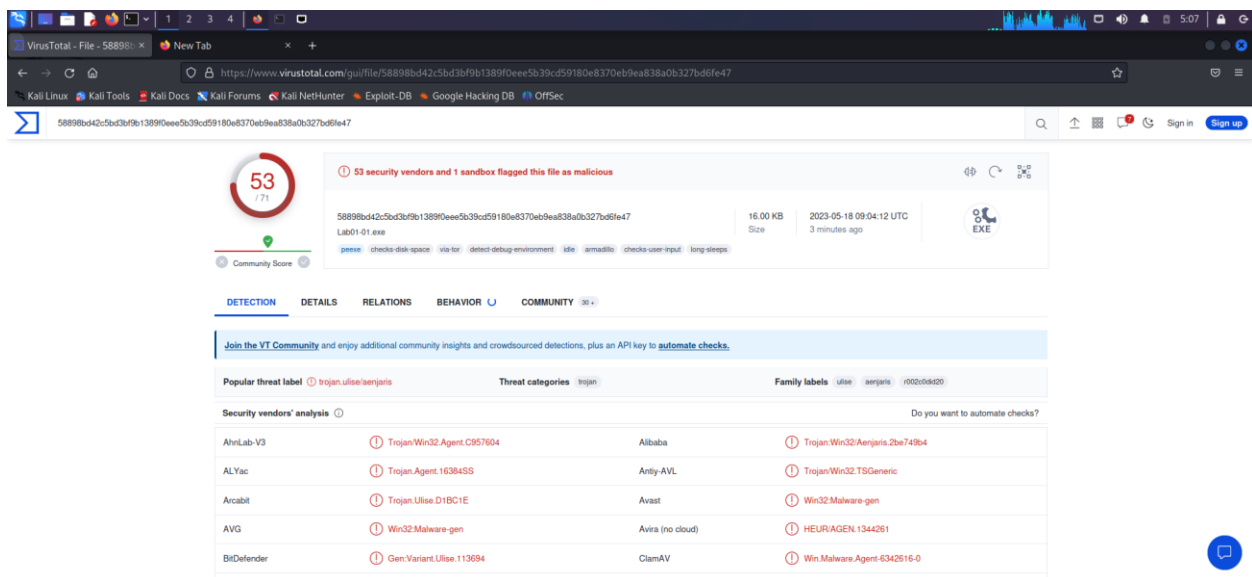
Ta sẽ up hai file là **Lab01-01.exe** và **Lab01-01.dll** vào trong virustotal.

Dưới đây là hình kiểm tra security của Virustotal với hai file là **Lab01-01.dll** và **Lab01-01.exe**



The screenshot shows the VirusTotal report for the file **Lab01-01.dll** (file ID: f50e42c8dfa649bde0398867e930b86c2a599e8db83b6260393082268f2dba). The file is 160.00 KB and was uploaded 9 minutes ago. It has a Community Score of 46/71, with 46 security vendors and no sandboxes flagging it as malicious. The file is identified as a Trojan (Trojan:Win32/Skeeyah.7b0ebff). The security vendors' analysis table shows the following results:

Vendor	Detection
Alibaba	Trojan:Win32/Skeeyah.7b0ebff
Antiy-AVL	Trojan:Win32/BT9Generic
Avast	Win32/Malware-gen
BitDefender	Gen:Variant.Ulisse.105796
ClamAV	Win.Malware.Agent-6369668-0
ALYac	Trojan.Agent.Waski
Arcabit	Trojan.Ulisse.D19D44
AVG	Win32/Malware-gen
BitDefender Theta	Gen:NN.ZedfAF.36196.kq4@vGkGVtp
CrowdStrike Falcon	Win/malicious_confidence_100% (W)



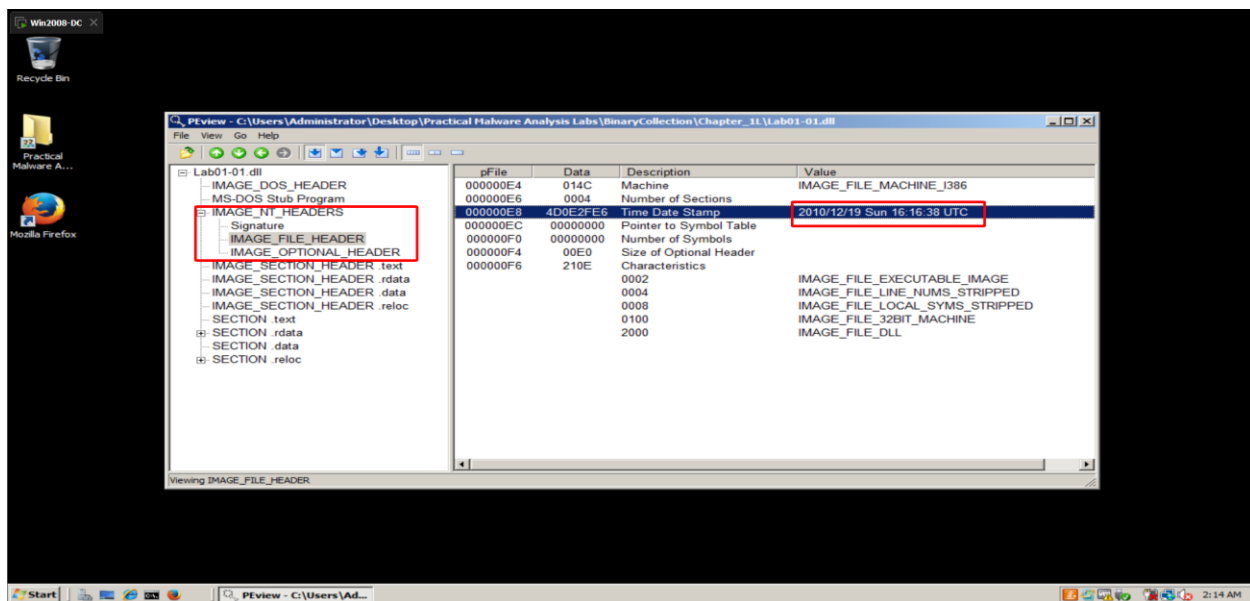
The screenshot shows the VirusTotal report for the file **Lab01-01.exe** (file ID: 58898bd42c5bd3bf9b13890deee5b39cd59180e8370eb9ea838a0b327bd6fe47). The file is 16.00 KB and was uploaded 3 minutes ago. It has a Community Score of 53/71, with 53 security vendors and 1 sandbox flagging it as malicious. The file is identified as a Trojan (Trojan:Win32/Aenjaris.2ba743b4). The security vendors' analysis table shows the following results:

Vendor	Detection
AhnLab-V3	Trojan:Win32/Agent.C957604
ALYac	Trojan.Agent.1638455
Arcabit	Trojan.Ulisse.D1BC1E
AVG	Win32/Malware-gen
BitDefender	Gen:Variant.Ulisse.113694
Alibaba	Trojan:Win32/Aenjaris.2ba743b4
Antiy-AVL	Trojan:Win32/TS_Generic
Avast	Win32/Malware-gen
Avira (no cloud)	HEUR/AGEN.1344261
ClamAV	Win.Malware.Agent-6342616-0

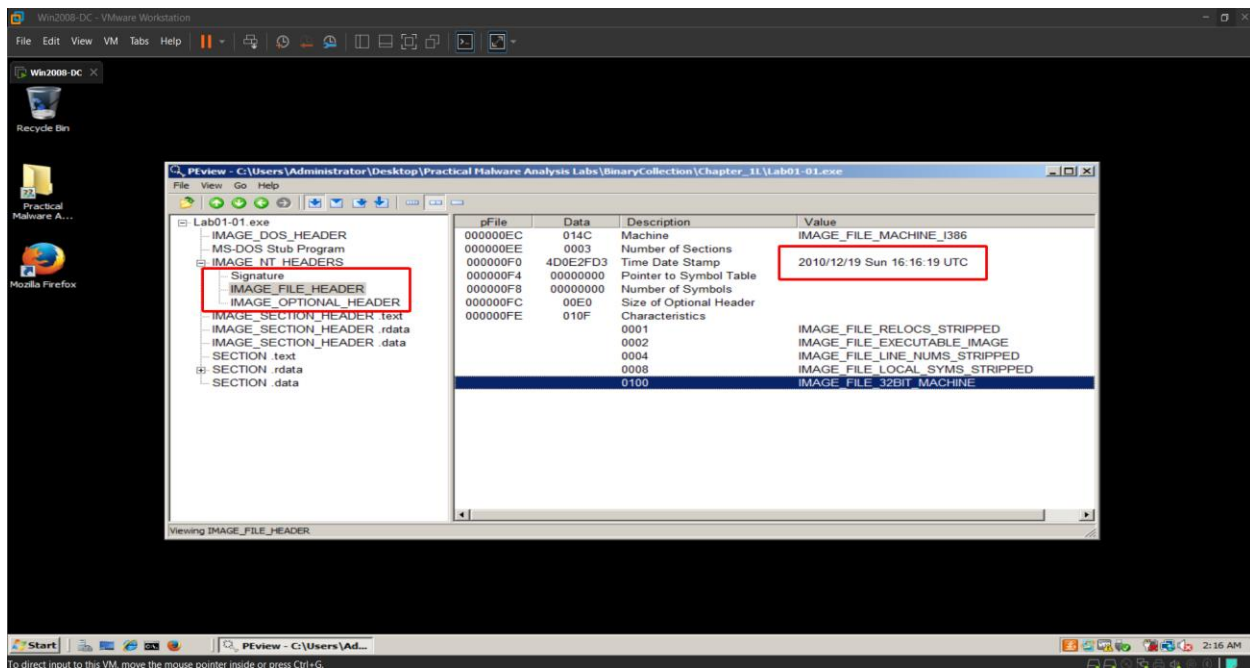
Nhận thấy rằng hai file này có độ nguy hiểm rất cao do có dính Trojan

## PEVIEW

Dùng công cụ PEVIEW để phân tích DLL và file EXE ta, vào timestamp để xem thời gian hoạt động của chúng



Đây là file timestamp của file dll, hoạt động lúc 16:15:38 ngày 19/12/2010 theo giờ UTC. Vì đó chỉ là một file dynamic library link nên chúng ta sẽ phân tích thêm file EXE có gì.



File EXE được khởi động lúc 16:16:19 ngày 19/12/2010 theo giờ UTC.. Nhận thấy rằng hai file có timestamp trong khoảng thời gian không lâu sau khi thành dll, ta có thể một phần kết luận rằng hai file này có thể chạy chung với nhau trong cùng một package.

PEiD

Win2008-DC - VMware Workstation

File Edit View VM Tabs Help

Win2008-DC

Recycle Bin

Practical Malware Analysis Labs

Mozilla Firefox

PEED v0.5.5

File: C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\bin\...

Entrypoint: 000012FA EP Section: .text

File Offset: 000012FA First Bytes: 55,8B,EC,53

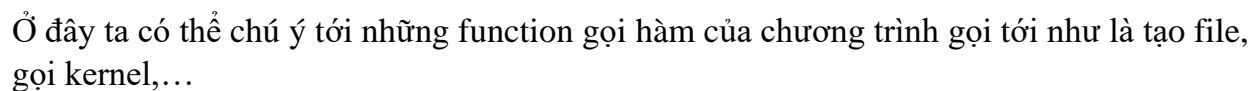
Linker Info: 6.0 Subsystem: Win32 GUI

Microsoft Visual C++ 6.0 DLL

Multi Scan Task Viewer Options About Exit

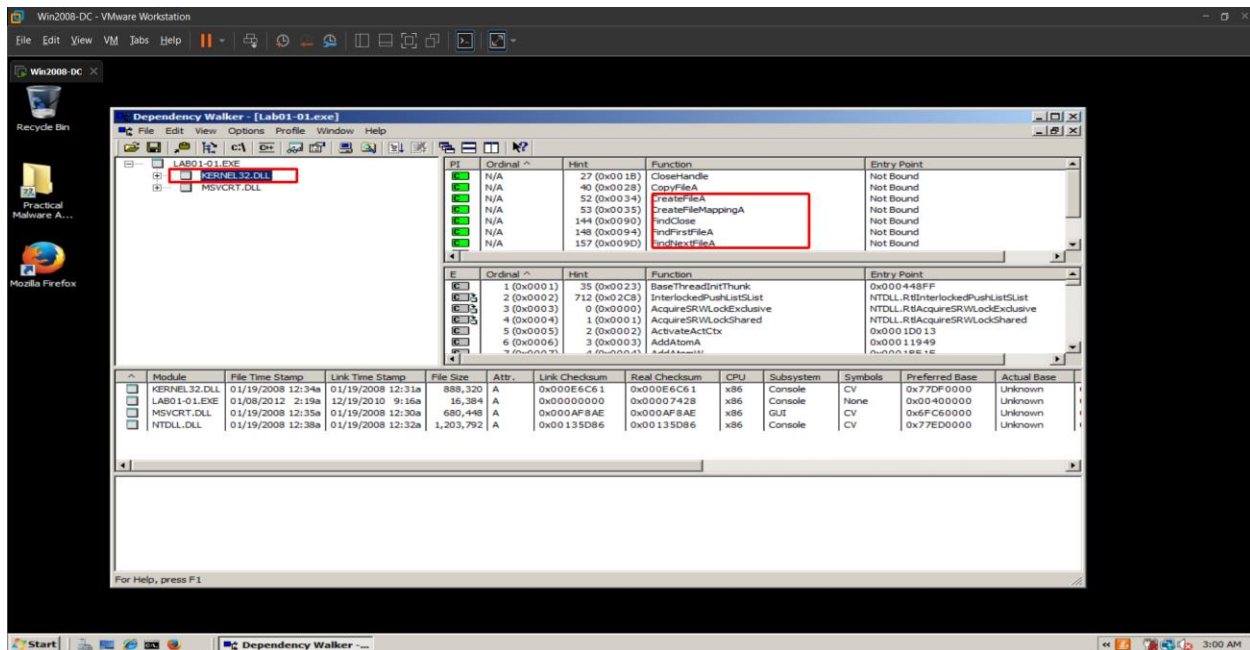
☒ Stay on top

Sử dụng command **String** để có thể xem được các ascii và UNICODE để có thể xem function của chương trình





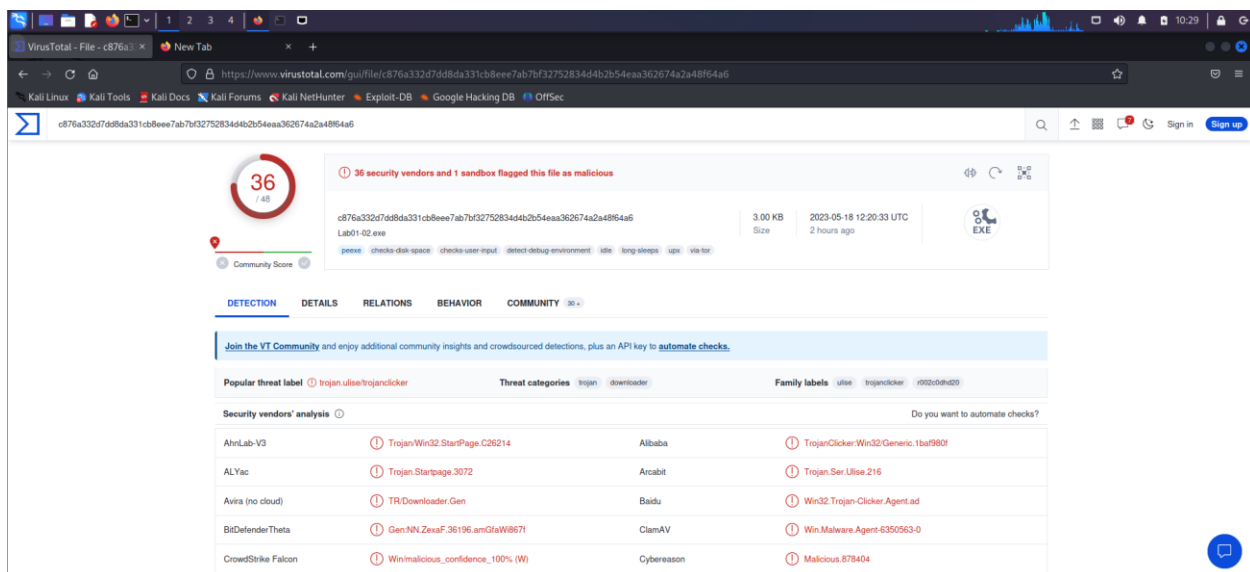
Vào bên KERNEL32.DLL ta sẽ thấy có mootj số function được sử dụng bởi con exe. Giống như là tạo file đóng file



## Proj 2: Basic Static Techniques (Lab 1-2) (20 pts.)

### VirusTotal

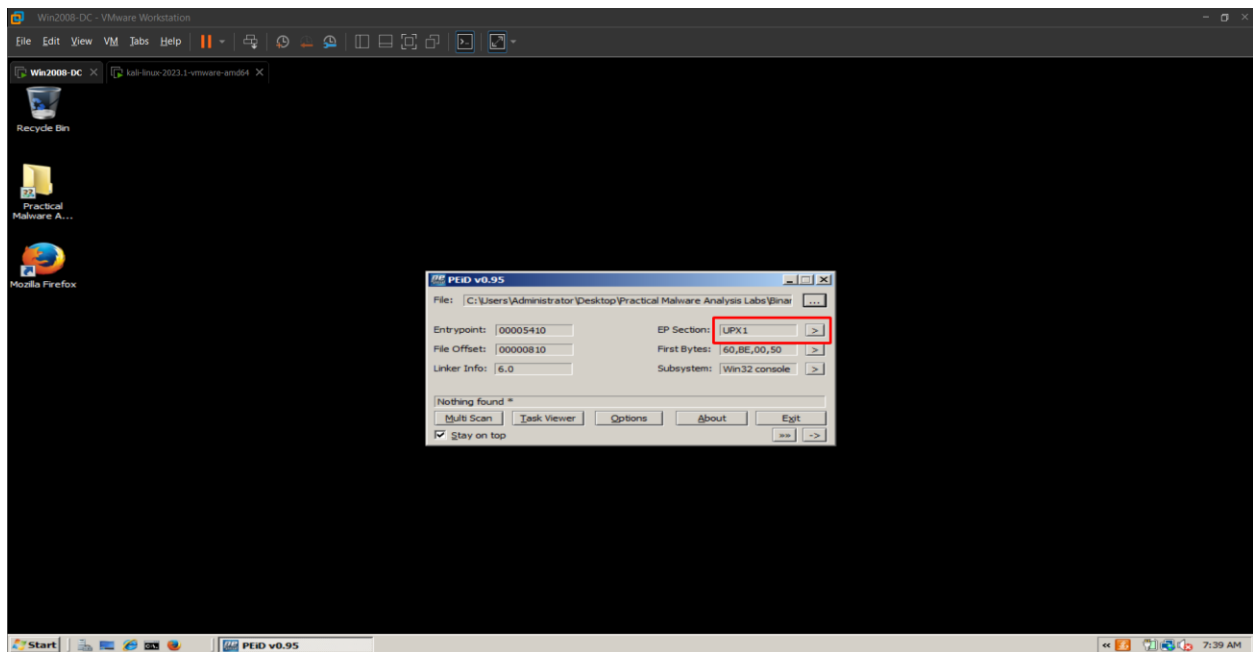
Như mọi thường, chúng ta sẽ phân tích **Lab01-02.exe** để xem file có bị dính malware không bằng virustotal bằng cách kiểm tra mã hash của nó



Nhận thấy rằng đây là một con malware, chúng ta sẽ tiến hành phân tích chuyên sâu thêm

### Unpacking the File

Nhìn thấy đây là file chứa malware, chúng ta sẽ tiến hành xem nó bằng PeID

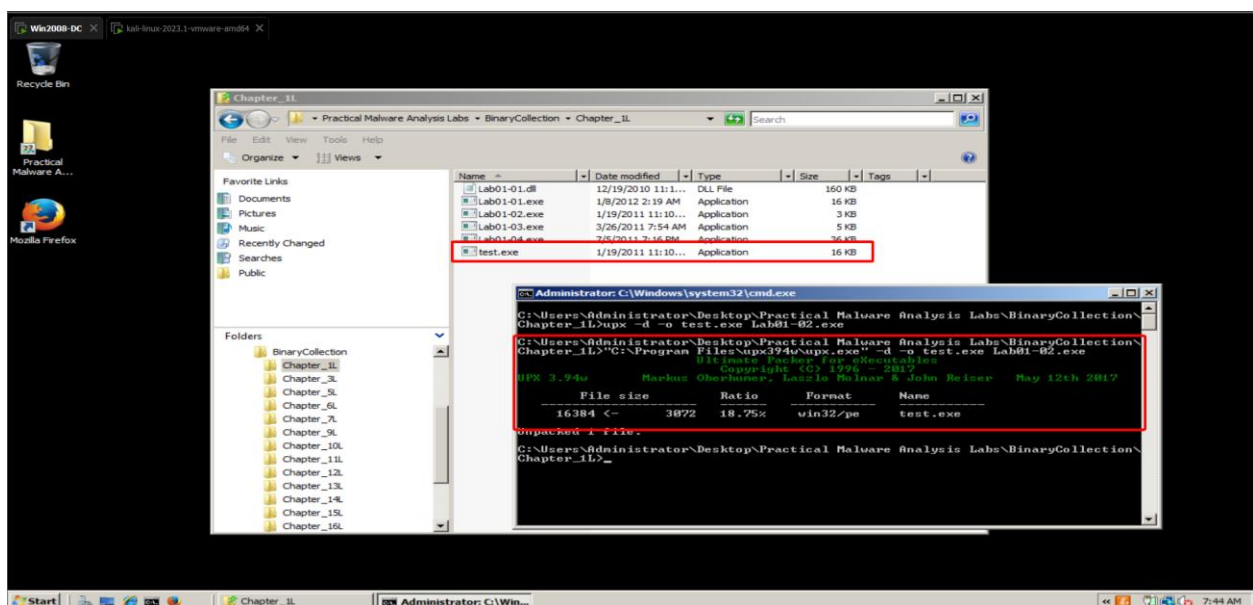


Chúng ta dễ dàng nhận thấy rằng, file này đã bị pack lại, theo em hiểu thì nó giống như là một dạng mã hóa code, khi thực thi, nó sẽ có hàm giải mã, và sau khi giải mã xong thì nó sẽ bắt đầu compile ứng dụng.

Dễ dàng nhận biết một file bị pack thông qua UPX.

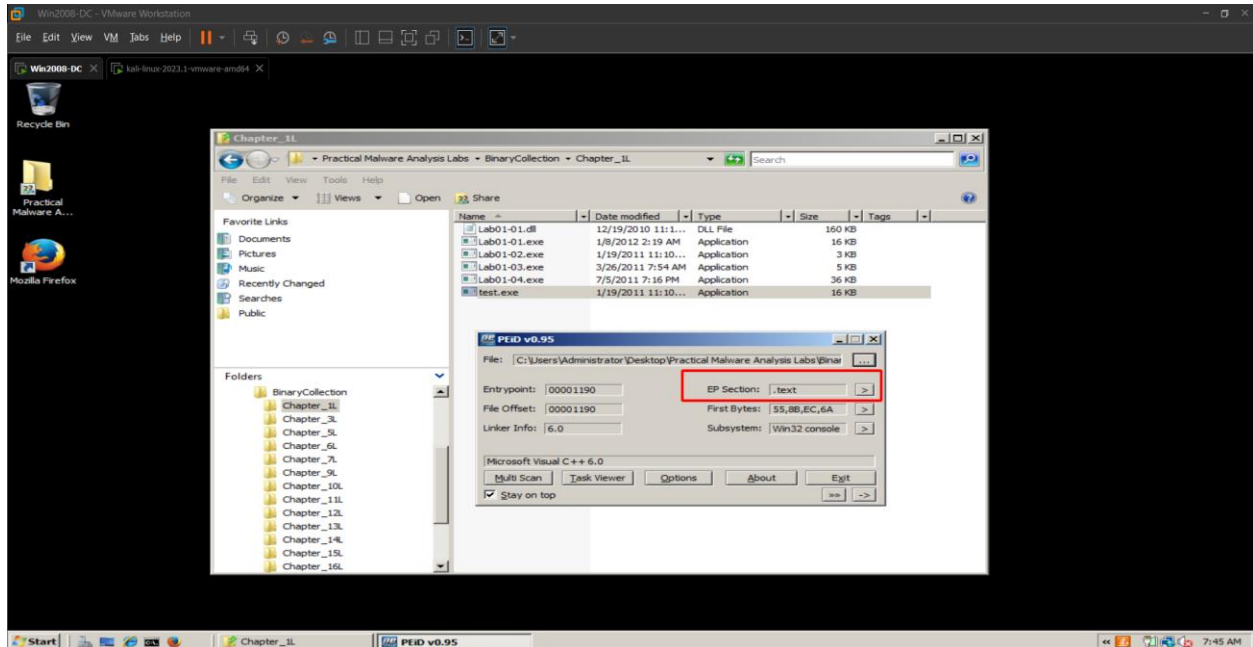
Muốn unpack, chúng ta sẽ sử dụng **upx** trong command line. Truy cập vào thư mục chứa file exe, ta sẽ bắt đầu unpack với câu lệnh **UPX -d -o test.exe Lab01-02.exe**

Sau khi unpack xong, ta có thể thấy được có một file mới được gọi là test.exe được tạo



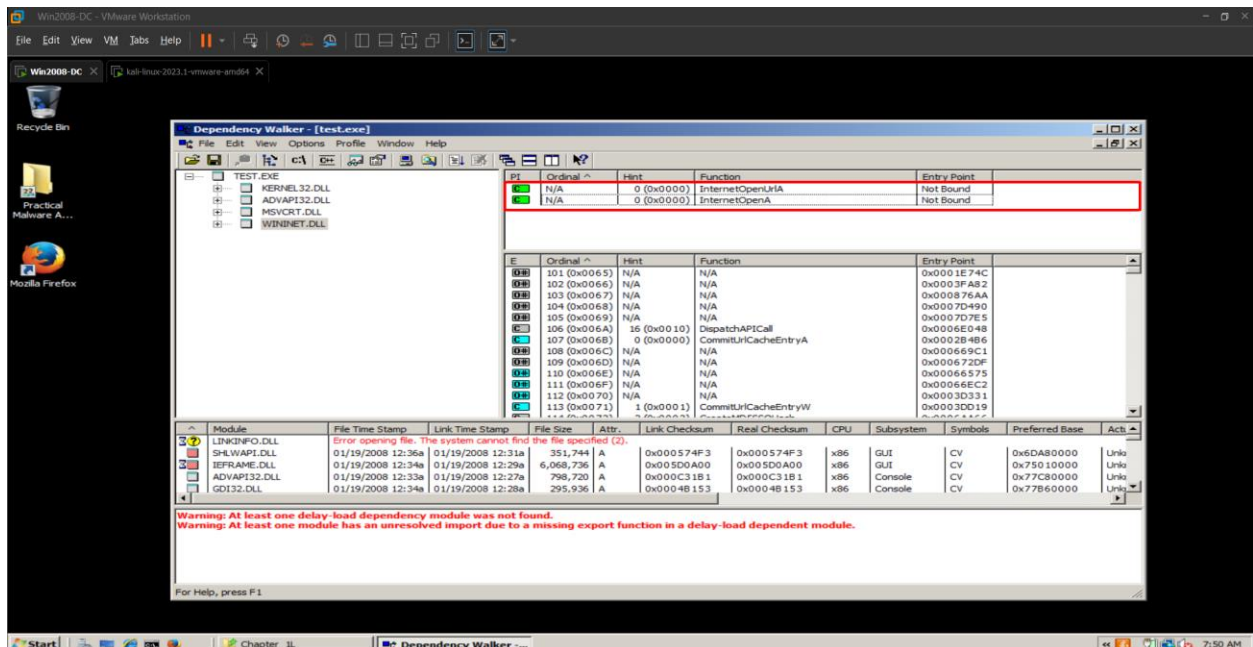


Bỏ file test.exe vào trong PeID để check lại xem file còn bị pack nữa không. Ta có kết quả là unpacked rồi



## Imports

Sau khi unpack xong, chúng ta sẽ bỏ vào bên trong dependency walker để phân tích tiếp



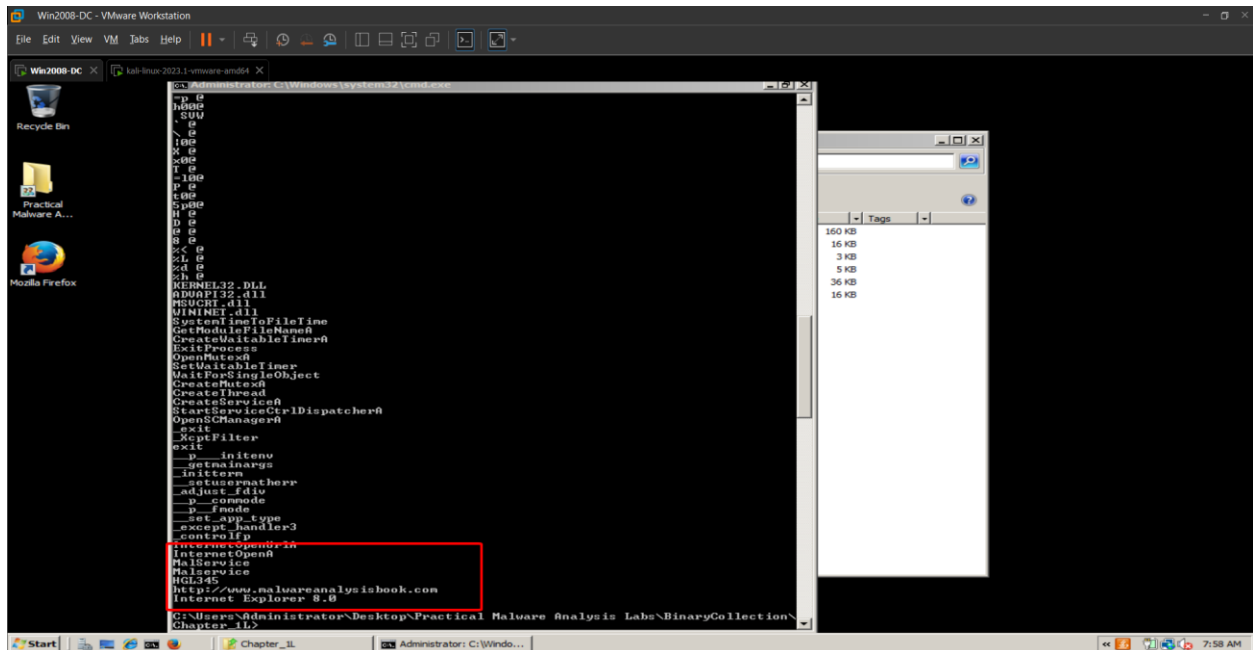
Ở trong thư viện wininet, ta có thể thấy rằng test.exe sẽ gọi hai hàm InternetOpenUrlA và InternetOpenA bên trong thư viện wininte.dll. Các hàm này được sử dụng để tạo kết nối tới một máy chủ qua giao thức HTTP, HTTPS hoặc FTP. InternetOpenA được sử



dùng để khởi tạo một phiên làm việc với WinINet, còn InternetOpenUrlA được sử dụng để mở một URL trên mạng.

## Strings

Sau khi mở bằng Dependency walker, ta sẽ sử dụng strings để xem malware này sẽ làm gì.



Có vẻ như ta thấy được Malware này sẽ giả dạng dưới tên Malservice, nó sẽ kết nối tới trang **malwareanalysisbook.com** bằng Internet Explorer 8.0