

HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA AN TOÀN THÔNG TIN

MODULE THỰC HÀNH
MÃ ĐỘC

BÀI THỰC HÀNH SỐ 02
Phân tích tĩnh cơ bản

Người thực hiện bài thực hành:

TS. Đặng Xuân Bảo

Hà Nội, 2020

Mục lục

Mục lục	2
THÔNG TIN CHUNG VỀ BÀI THỰC HÀNH	3
CHUẨN BỊ BÀI THỰC HÀNH	4
PHÂN TÍCH TÍNH CƠ BẢN	5
1.1. Mô tả	5
1.2. Chuẩn bị	5
1.3. Phân tích tính cơ bản.....	5
1.3.1. Phân tích Lab01-01	5
1.3.2. Phân tích Lab01-02.....	17

THÔNG TIN CHUNG VỀ BÀI THỰC HÀNH

Tên bài thực hành: Phân tích tĩnh cơ bản

Học phần: Mã độc

Số lượng sinh viên cùng thực hiện:

Địa điểm thực hành: Phòng máy

Yêu cầu:

- Yêu cầu phần cứng:
 - + Máy tính với cấu hình tối thiểu: CPU 2.0 GHz, RAM 4GB, HDD 500GB
- Yêu cầu phần mềm trên máy:
 - + Hệ điều hành Windows 10
 - + VMware Workstation 15.0
- Yêu cầu kết nối mạng LAN: có
- Yêu cầu kết nối mạng Internet: có

CHUẨN BỊ BÀI THỰC HÀNH

Đối với giảng viên

Trước buổi học, giảng viên (người hướng dẫn thực hành) cần kiểm tra sự phù hợp của điều kiện thực tế của phòng thực hành với các yêu cầu của bài thực hành.

Ngoài ra không đòi hỏi gì thêm.

Đối với sinh viên

Trước khi bắt đầu thực hành, cần tạo các bản sao của máy ảo để sử dụng. Đồng thời xác định vị trí lưu trữ các công cụ đã chỉ ra trong phần yêu cầu.

PHÂN TÍCH TÍNH CƠ BẢN

1.1. Mô tả

Bài thực hành hướng dẫn sinh viên sử dụng một số công cụ trong việc phân tích tính một số mẫu mã độc đơn giản.

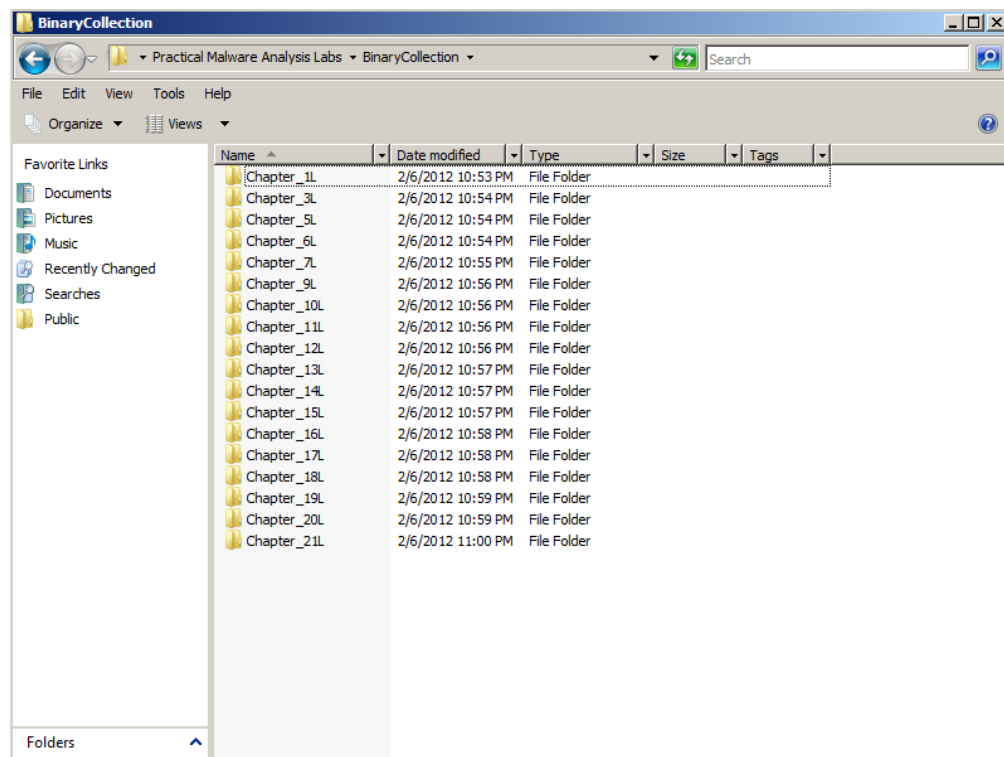
1.2. Chuẩn bị

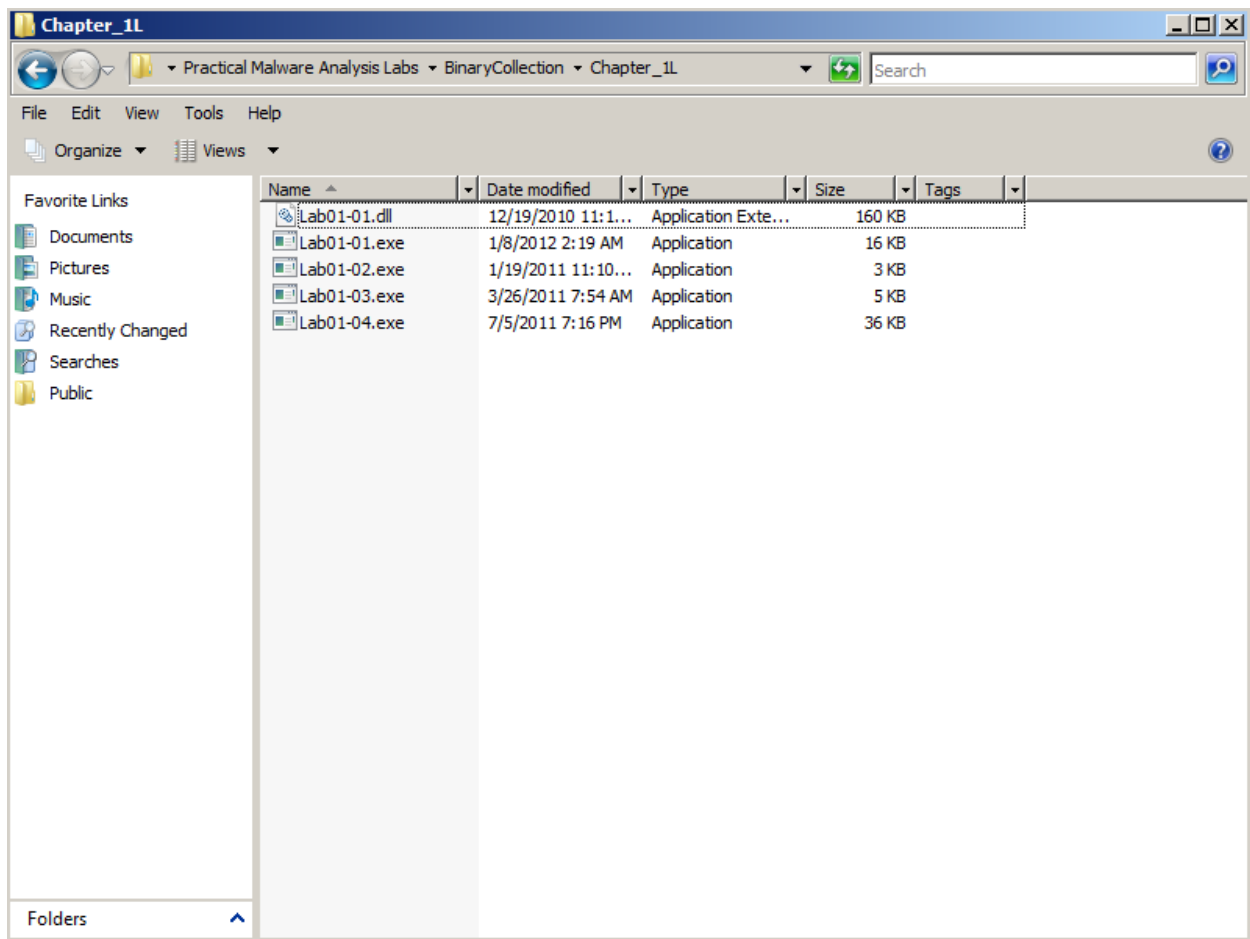
- Môi trường phân tích mã độc đã xây dựng trong bài trước.

1.3. Phân tích tính cơ bản

1.3.1. Phân tích Lab01-01

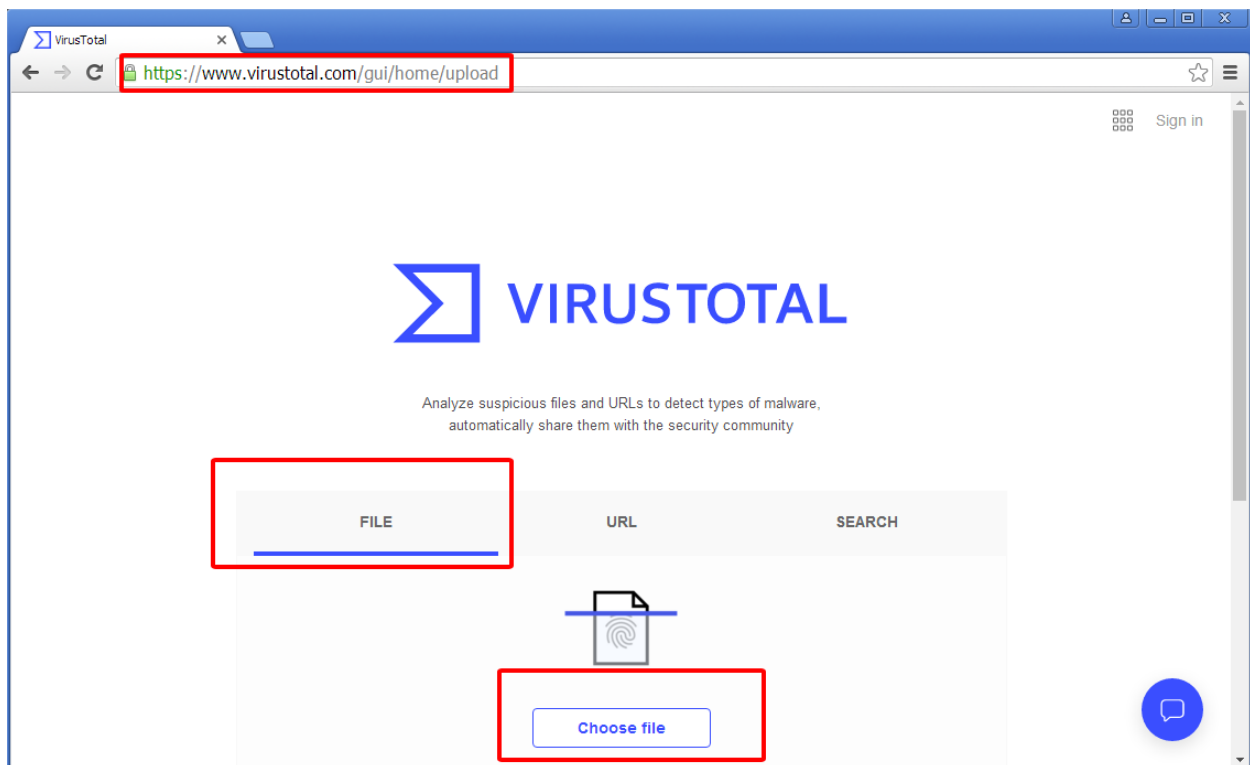
Phần này sử dụng các tệp Lab01-01.exe and Lab01-01.dll, cả trong thư mục "chapter_11". (Sinh viên tham khảo thêm tài liệu Practical Malware Analysis)



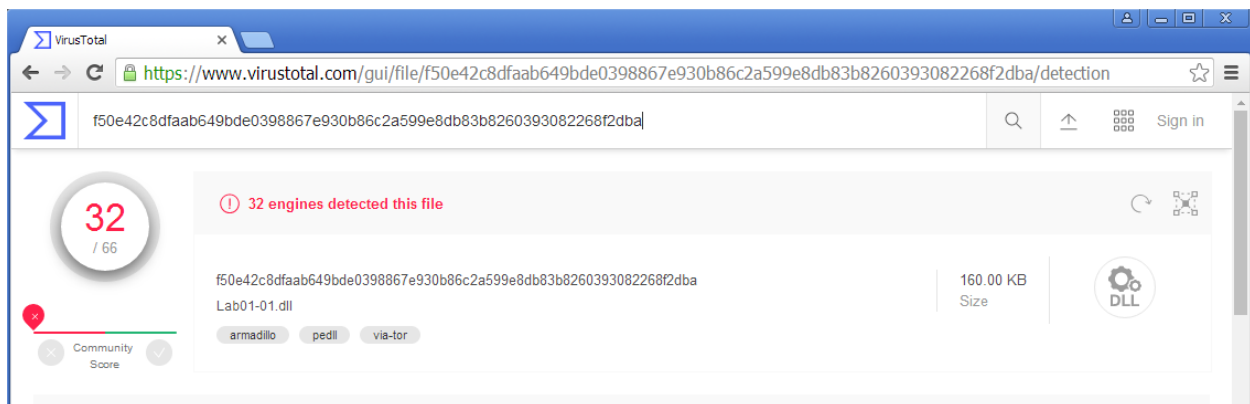


Sử dụng Virustotal để phân tích

Tải lên Lab01-01.exe và Lab01-01.dll trên www.virustotal.com



Kết quả phân tích Lab01-01.dll như hình bên dưới.



VirusTotal

WJR Software - PEview (PE) X

https://www.virustotal.com/gui/file/f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba/detection

f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba

32 / 66

32 engines detected this file

f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba

160.00 KB

Size

Lab01-01.dll

armadillo pedt via-tor

Community Score

DETECTION DETAILS RELATIONS COMMUNITY 10+

Alibaba	Trojan:Win32/Generic.1594ec0f	ALYac	Trojan.Agent.Waski
Antiy-AVL	Trojan/Win32.BTSGeneric	Avast	Win32.Malware-gen
AVG	Win32.Malware-gen	BitDefenderTheta	Gen.NN.ZedlaF.34090.kq4@aGkQVtp
CAT-QuickHeal	Trojan.IGENERIC	ClamAV	Win.Malware.Agent-6369668-0
Comodo	Malware@#2dsw4albnc6e1	Cylance	Unsafe
Endgame	Malicious (high Confidence)	ESET-NOD32	A Variant Of Generic.TGEWDD
F-Secure	Trojan.TR/Dldr.Waski.163840.1	FireEye	Generic.mg.290934c61de9176a
Fortinet	PossibleThreat	GData	Win32.Trojan.Agent.4L5OBS

VirusTotal

WJR Software - PEview (PE) X

https://www.virustotal.com/gui/file/f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba/detection

f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba

Fortinet

PossibleThreat

GData

Win32.Trojan.Agent.4L5OBS

Ikarus

Trojan.SuspectCRC

MAX

Malware (ai Score=96)

McAfee

GenericR\F\F0-RTI290934C61DE9

McAfee-GW-Edition

GenericR\F\F0-RTI290934C61DE9

Microsoft

Trojan:Win32/Occamy.C

NANO-Antivirus

Trojan.Win32.Waski.dtkvsp

Qihoo-360

Win32/Trojan.54f

Rising

Trojan.Tilkenf8.F605 (CLOUD)

Sangfor Engine Zero

Malware

Trapmine

Malicious.moderate.ml.score

TrendMicro

TROJ_GEN.R002C0DGM19

TrendMicro-HouseCall

TROJ_GEN.R002C0DGM19

VIPRE

Trojan.Win32.GenericIBT

Webroot

W32.Gen.BT

Yandex

Trojan.Agent/IH/SKjKET4

Zillya

Adware.InstallCore.Win32.1036

Acronis

Undetected

Ad-Aware

Undetected

AhnLab-V3

Undetected

SecureAge APEX

Undetected

Arcabit

Undetected

Avast-Mobile

Undetected

Baidu

Undetected

BitDefender

Undetected

Bkav

Undetected

CMC

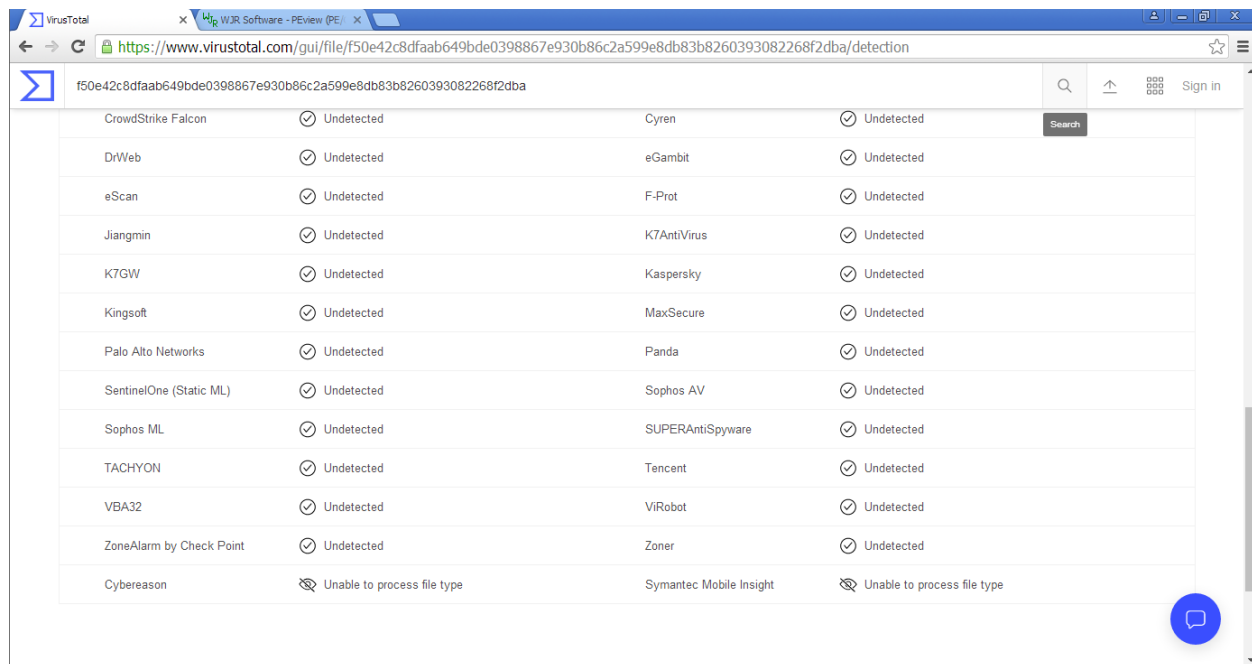
Undetected

CrowdStrike Falcon

Undetected

Cyren

Undetected

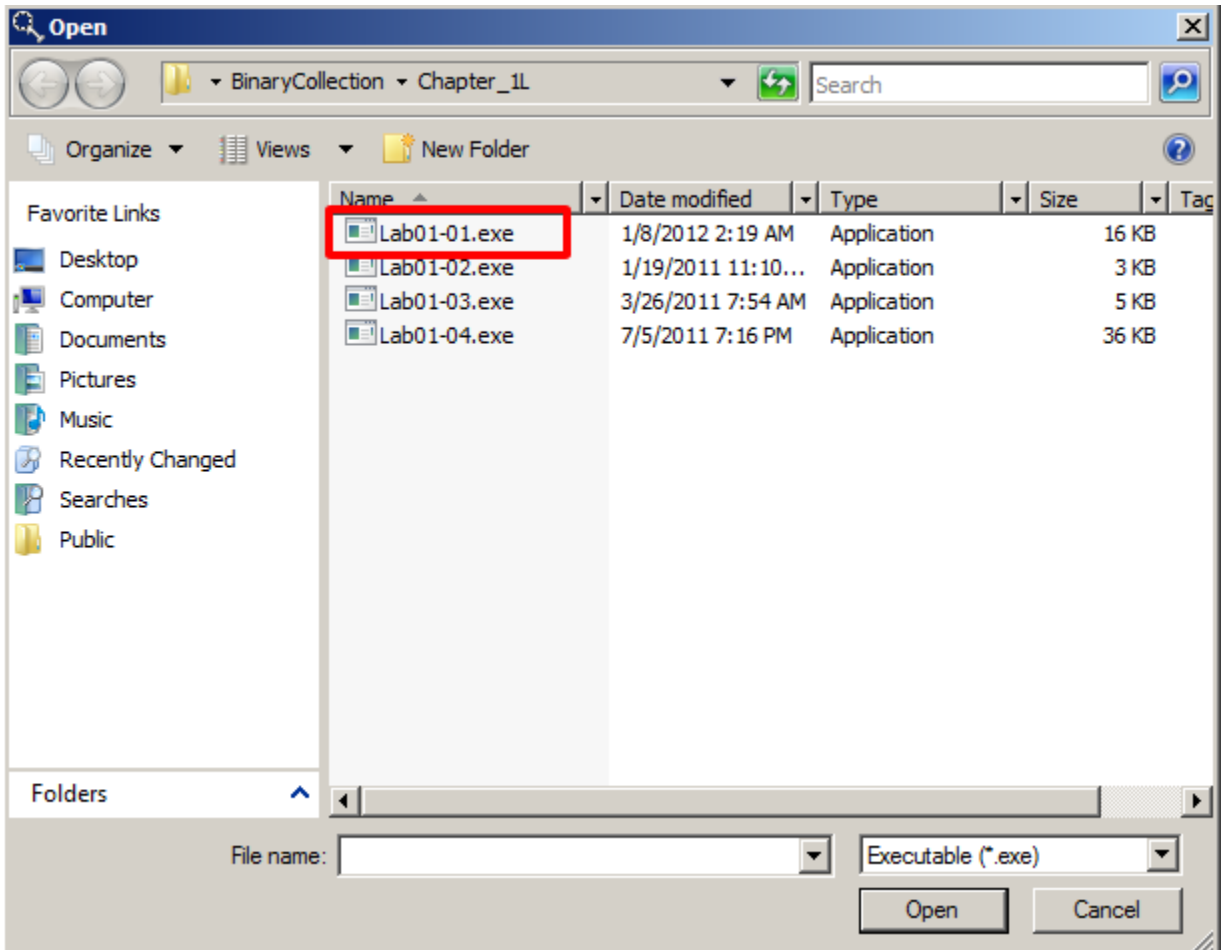


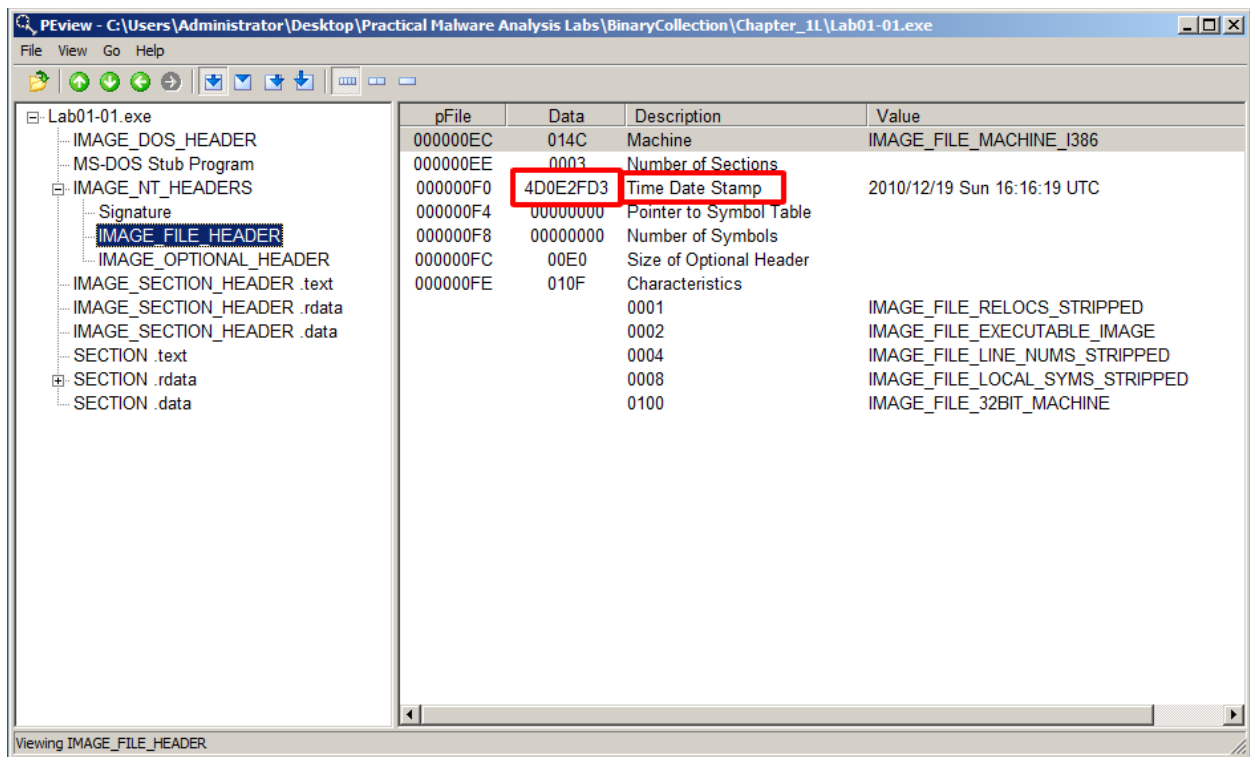
Sinh viên tìm hiểu ý nghĩa của các kết quả trên (làm tương tự với file Lab01-01.exe)

Sử dụng PView



Dùng PEview đọc thông tin về Lab01-01.exe và Lab01-01.dll. Đối với mỗi tệp, tìm "Time Date Stamp". Chúng đều được biên dịch cùng một thời gian, như vậy chúng là các phần của cùng một chương trình.

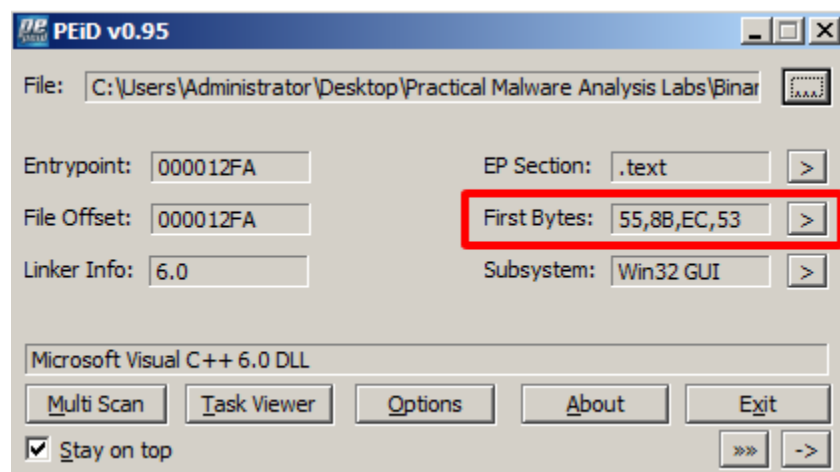




Sử dụng PeiD

Dùng PEiD đọc thông tin về Lab01-01.exe và Lab01-01.dll (tùy chọn). Ta thu được thông tin "Microsoft Visual C++ 6.0", nghĩa là chúng được viết bằng ngôn ngữ Microsoft Visual C++ 6.0.

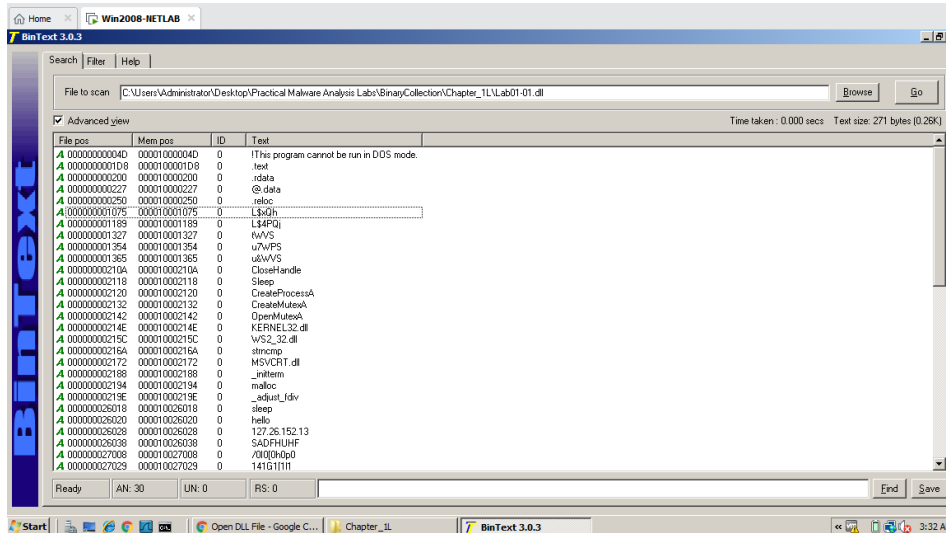
Phần EP section hiển thị .text. Sinh viên giải thích ý nghĩa.



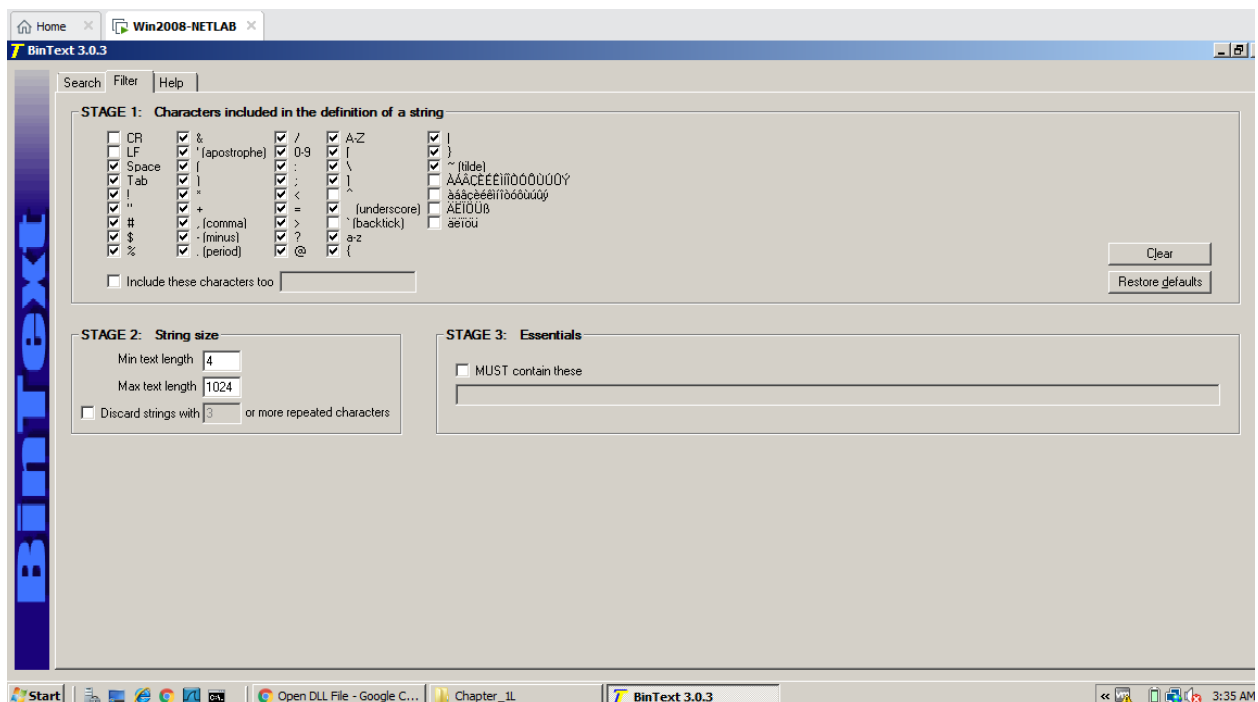
Sử dụng Bintext

Bintext là một công cụ hữu ích để xem các chuỗi. Dùng Bintext các chuỗi có trong file Lab01-01.dll, lưu ý những mục sau đây:

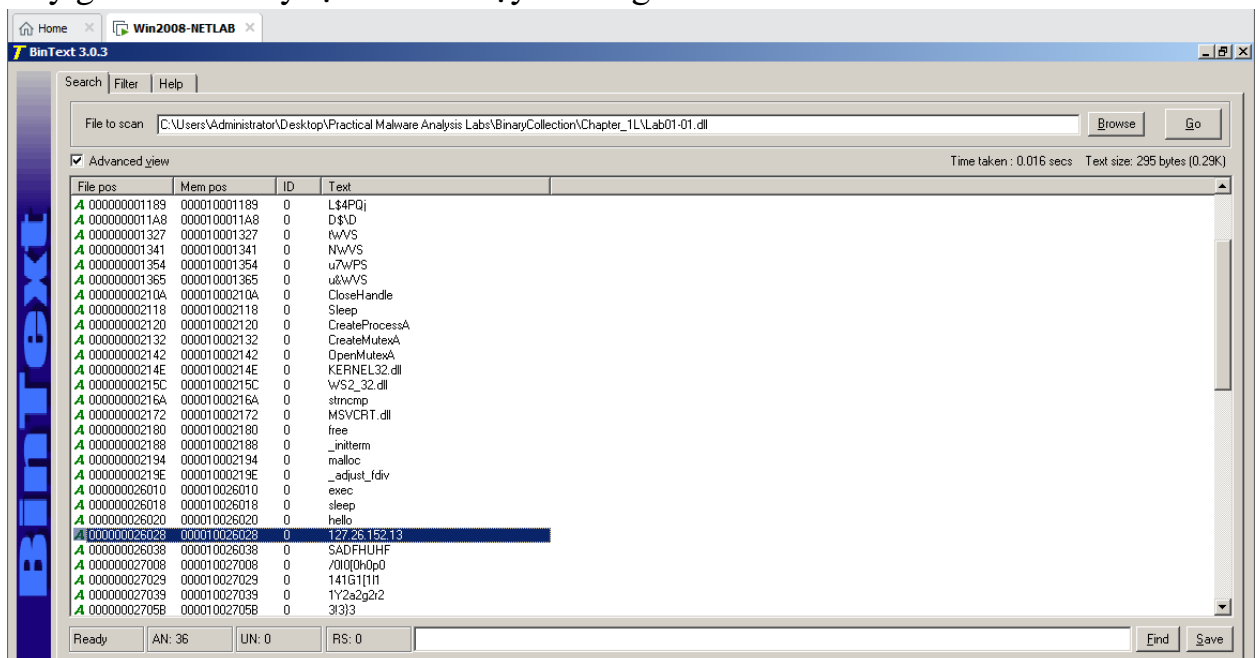
- CreateProcessA: Lệnh tạo một tiến trình
- Sleep: lệnh ngủ



Lệnh khởi động một chương trình bị thiếu. Để xem lệnh này cần vào tab **Filter** và điều chỉnh " Min. text length " thành 4.



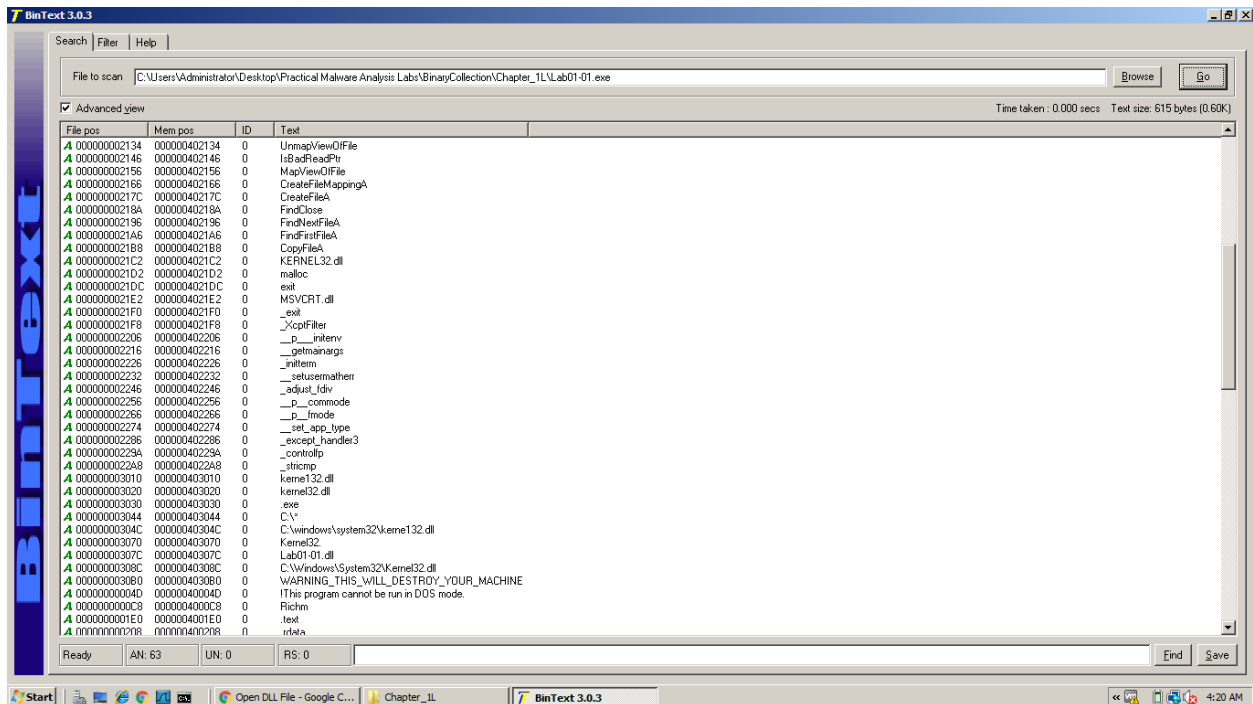
Vào tab **Search** ở trên cùng bên phải, nhấp vào **Go**.
 Bây giờ có thể thấy lệnh khởi chạy chương trình là **exec**.



Một số điểm cần lưu ý và tìm hiểu:

- Dưới "sleep" and "hello" thấy có địa chỉ IP, bắt đầu với 127. Liệu đây là địa chỉ gì?
- FindNextFileA" and "FindFirstFileA" -- Windows functions tìm các tập tin

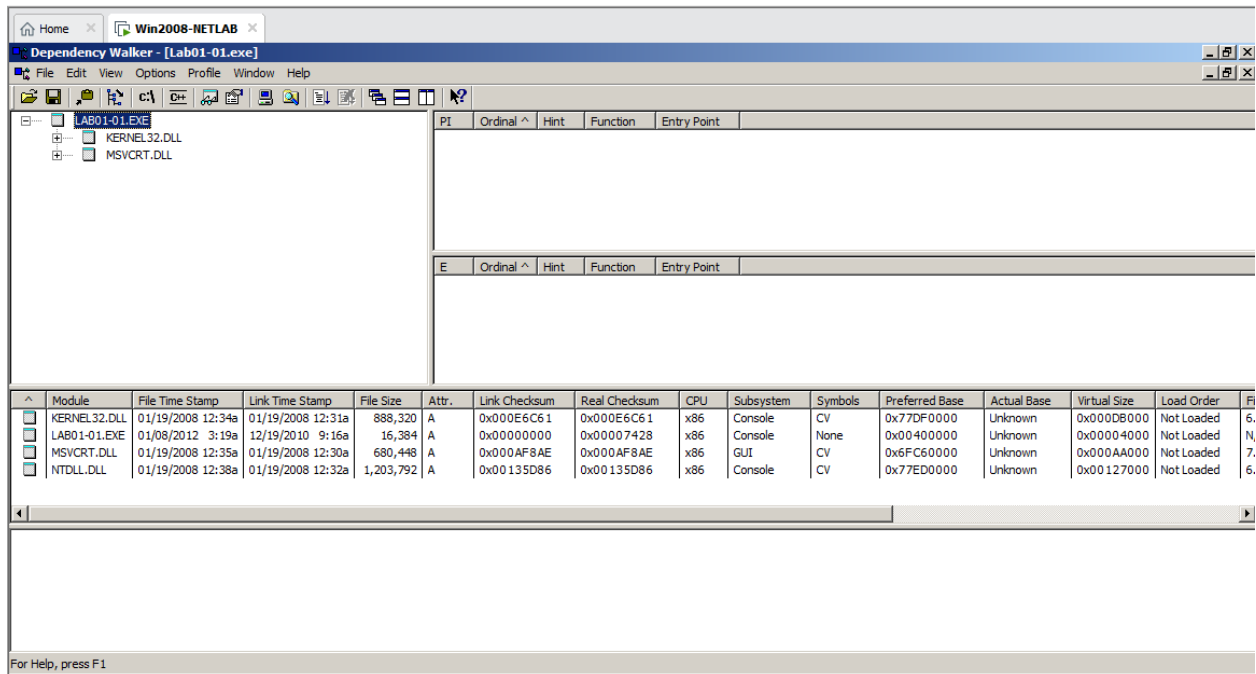
- ". exe " -- tìm kiếm tệp exe
- " C: Windows\system32\kernel32. dll " và " C: Windows\system32\kernel32. dll "
- ". Cái nào là dll của Windows ?



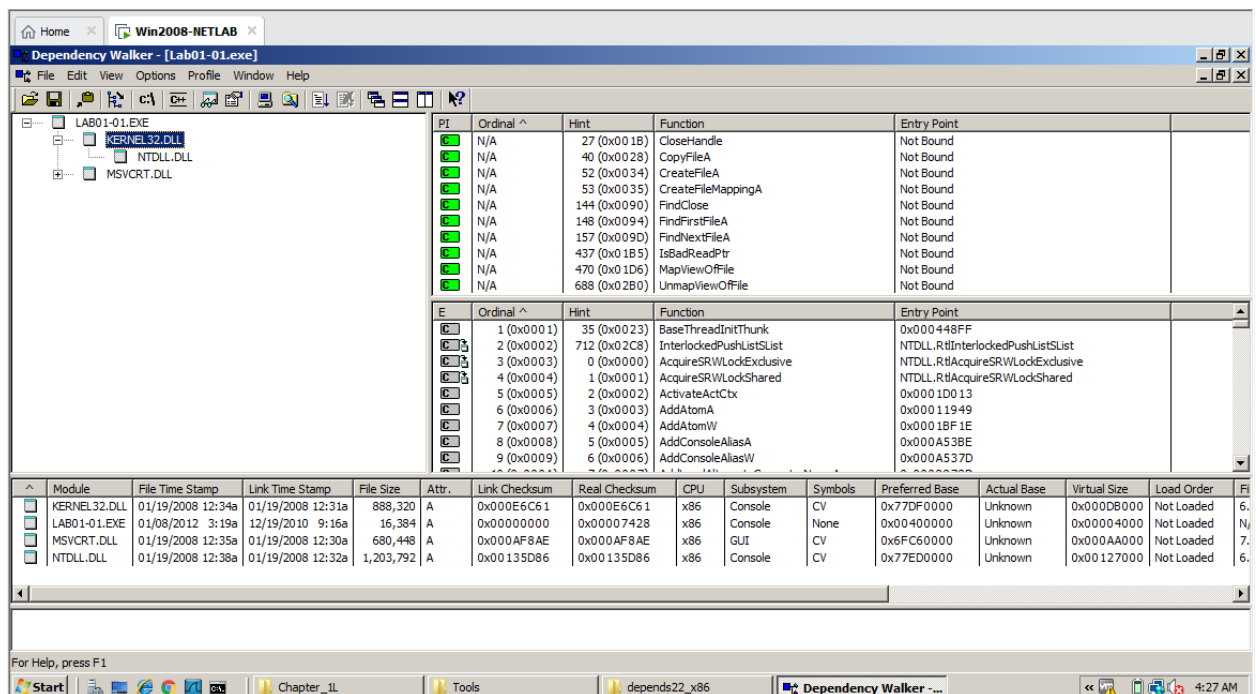
Sử dụng Dependency Walker



Dùng Dependency Walker đọc Lab01-01.exe.

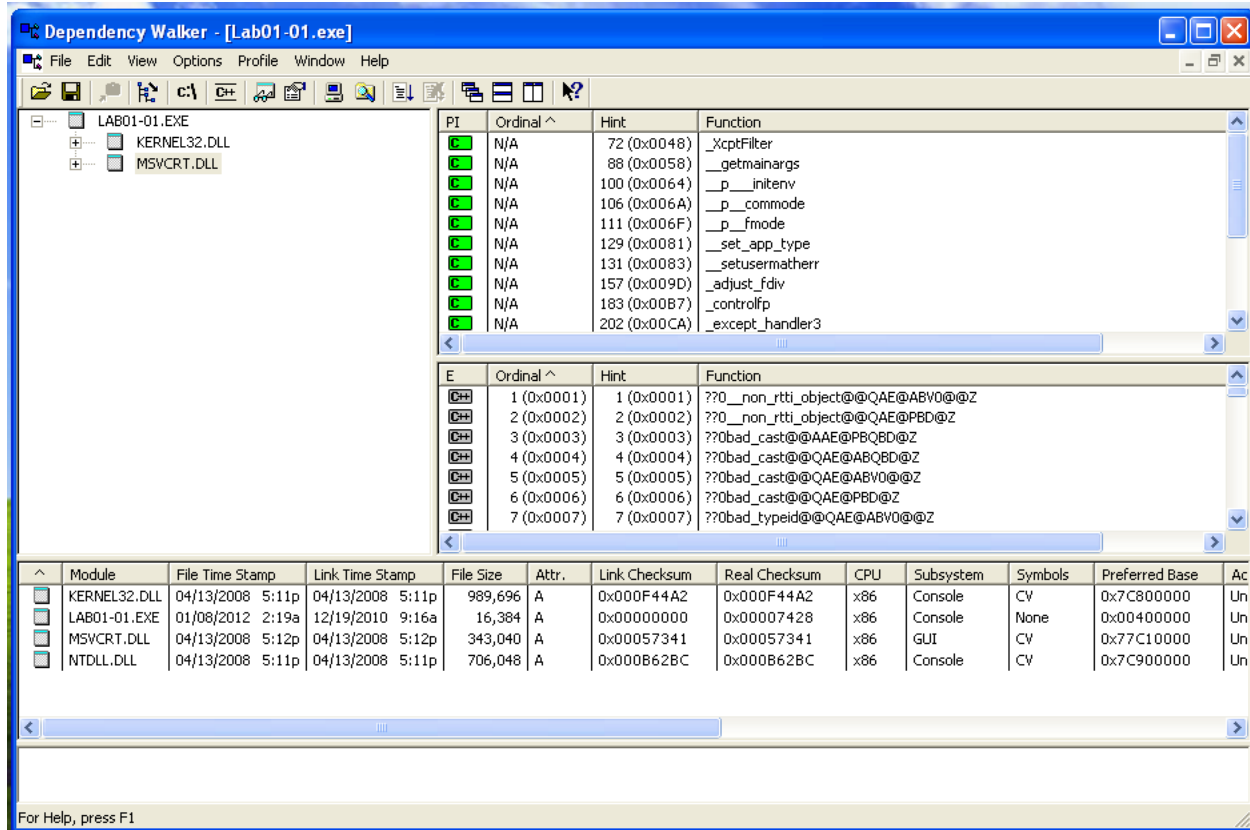


Vào phần **KERNEL32.DLL** ta thu được kết quả sau.

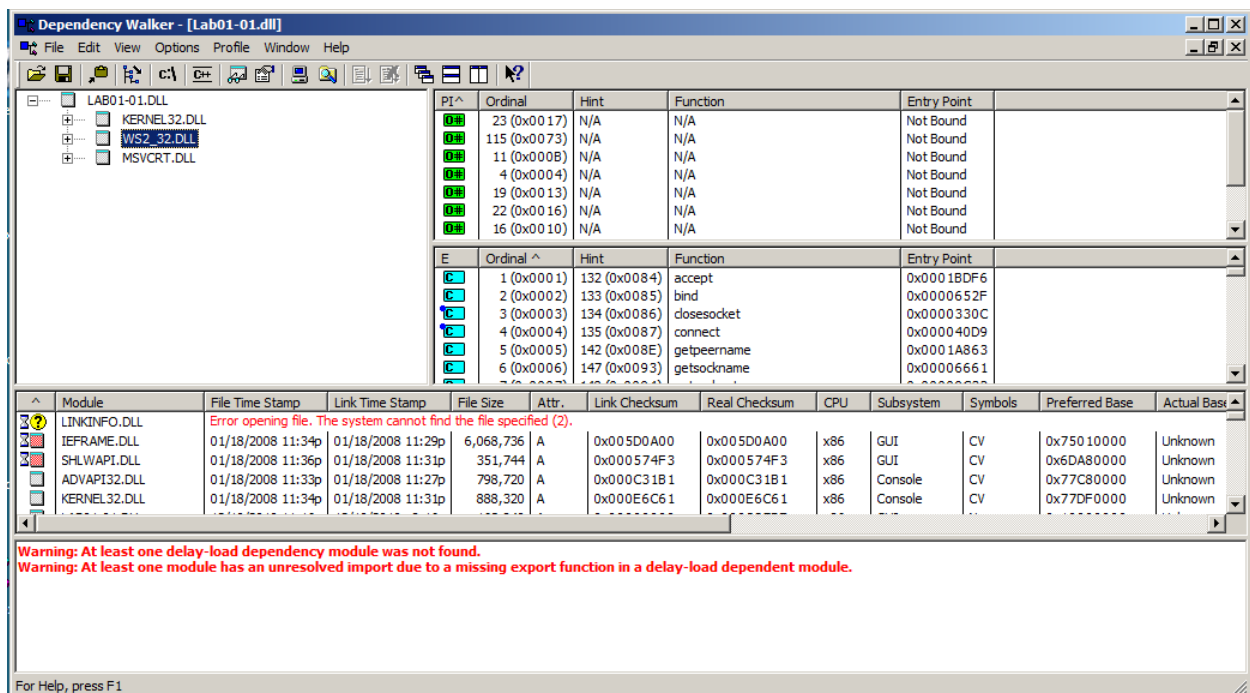


Giải thích hình trên. Lưu ý các phần "PI" (Parent Import), E (Export), các hàm **FindNextFileA**, **FindFirstFileA**...

Vào phần **MSVCRT.DLL**



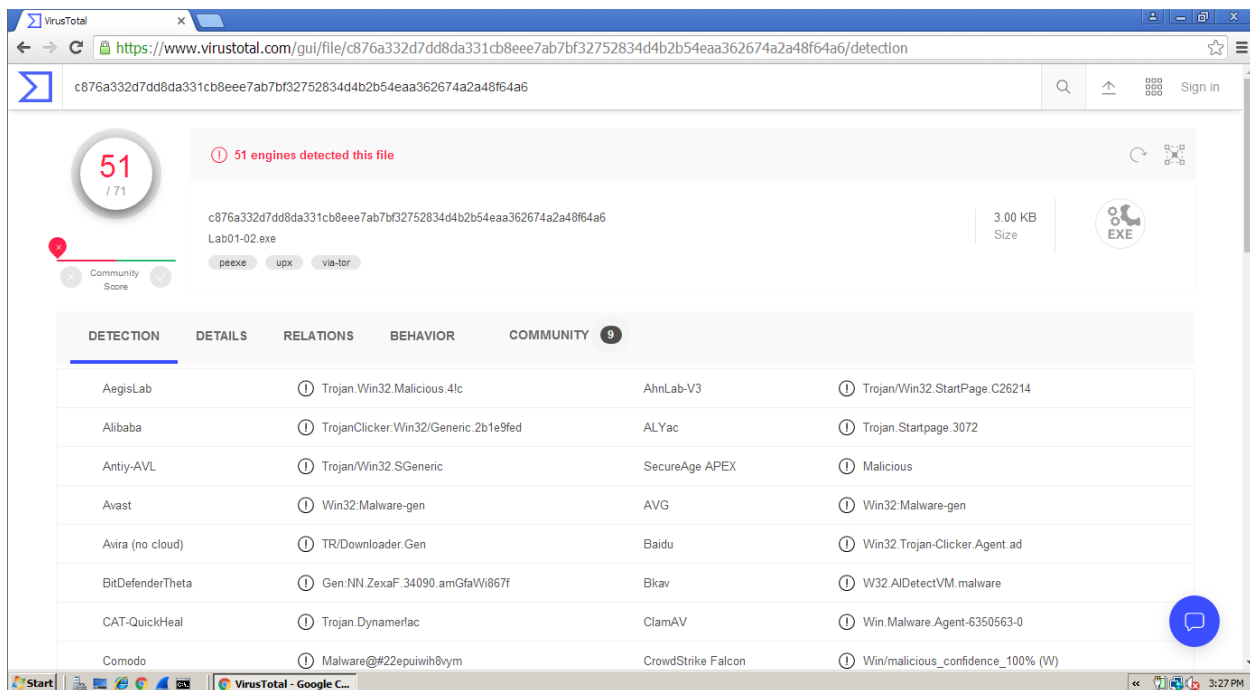
Dùng Dependency Walker đọc **Lab01-01.dll**. Lưu ý hàm "WS2_32.DLL" và "bind", "closesocket" và "connec".



1.3.2. Phân tích Lab01-02

Sử dụng Virustotal

Thực hiện các yêu cầu tương tự trong phần 1.3.1.

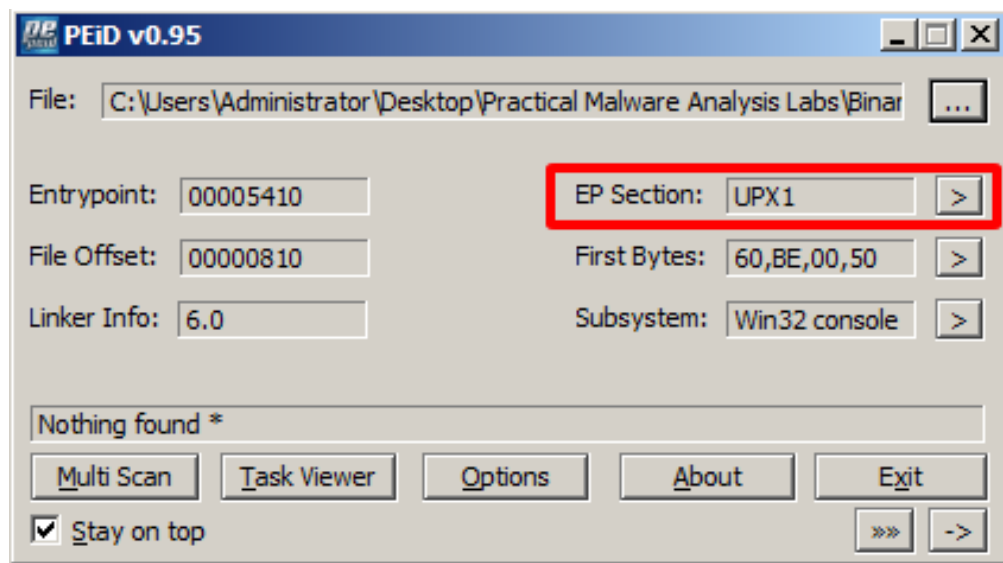


Engine	Detection	Engine	Detection
Comodo	Malware@#22epuiwih8vym	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.cbcb77	Cylance	Unsafe
DrWeb	Trojan.Click3.12740	eGambit	Generic.Downloader
Endgame	Malicious (moderate Confidence)	ESET-NOD32	Win32/TrojanClicker.Agent.NVM
F-Secure	Trojan.TR/Downloader.Gen	FireEye	Generic.mg.8363436878404da0
Fortinet	W32/Agent.NVMtr	GData	Win32.Trojan.Agent.JV4QJM
Ikarus	Trojan.Win32.TrojanClicker	Jiangmin	Trojan.Generic.bdq
MAX	Malware (ai Score=100)	MaxSecure	Trojan.Malware.2588.susgen
McAfee	Generic.ait	McAfee-GW-Edition	Generic.ait
Microsoft	Trojan.Win32/Tiggrelrln	NANO-Antivirus	Trojan.Win32.RP.cwxtpf
Palo Alto Networks	Generic.ml	Qihoo-360	HEUR/Malware.QVM11.Gen
Rising	Trojan.Clicker.Agentl8.13 (TFE:5.kDYlhM...	Sangfor Engine Zero	Malware
SentinelOne (Static ML)	DFI - Suspicious PE	Sophos AV	Mal/Generic-S
Sophos ML	Heuristic	Symantec	ML.Attribute.HighConfidence
Tencent	Win32.Trojan.Downloader.Dyzz	Trapmine	Malicious.high.ml.score

Engine	Detection	Engine	Detection
Tencent	Win32.Trojan.Downloader.Dyzz	Trapmine	Malicious.high.ml.score
TrendMicro	TROJ_GEN.R002C0DL919	TrendMicro-HouseCall	TROJ_GEN.R002C0DL919
VBA32	Trojan.Click	VIPRE	Trojan.Win32.Generic.IBT
Webroot		Yandex	Trojan.CL.AgentlSYJ1YyE/ZV4
Zillya	Trojan.Agent.Win32.1288291	Acronis	Undetected
Ad-Aware	Undetected	Arcabit	Undetected
Avast-Mobile	Undetected	BitDefender	Undetected
CMC	Undetected	Cyren	Undetected
Emsisoft	Undetected	eScan	Undetected
F-Prot	Undetected	K7AntiVirus	Undetected
K7GW	Undetected	Kaspersky	Undetected
Kingsoft	Undetected	Panda	Undetected
SUPERAntiSpyware	Undetected	TACHYON	Undetected
ViRobot	Undetected	ZoneAlarm by Check Point	Undetected
Zoner	Undetected	Symantec Mobile Insight	Unable to process file type

Sử dụng PEiD

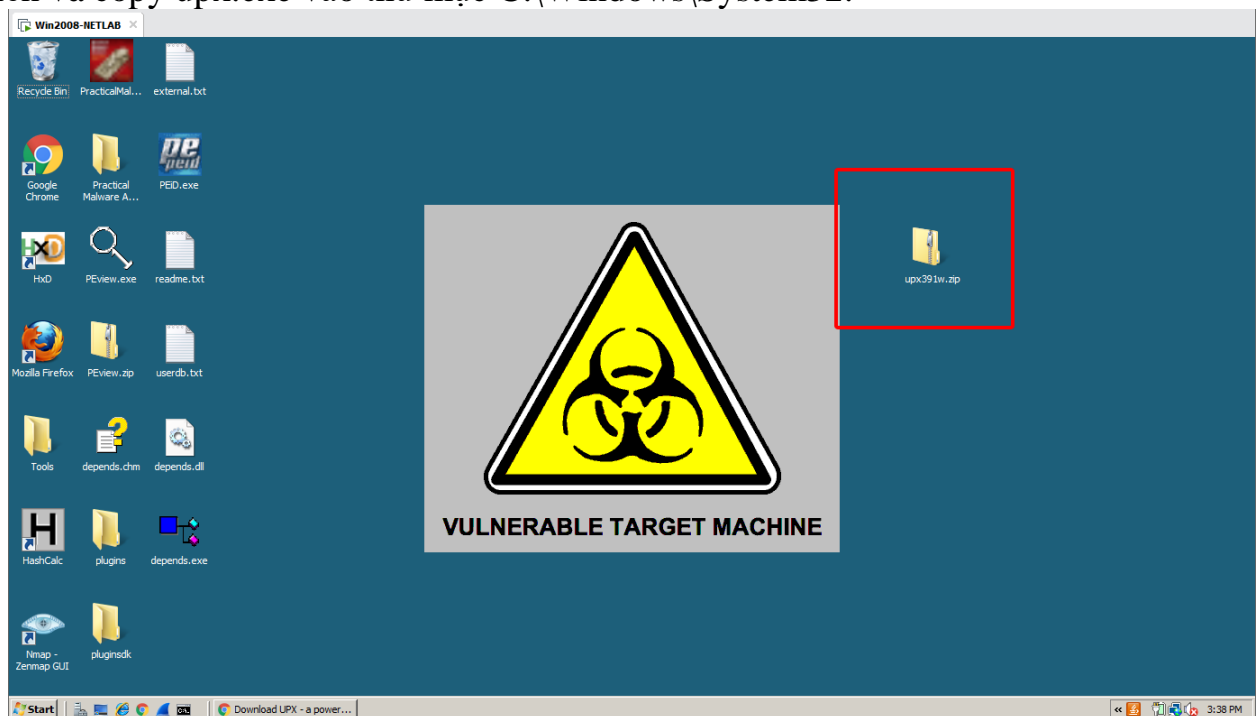
Kết quả thấy tập tin được đóng gói bằng UPX (được ghi tại phần "EP Section").

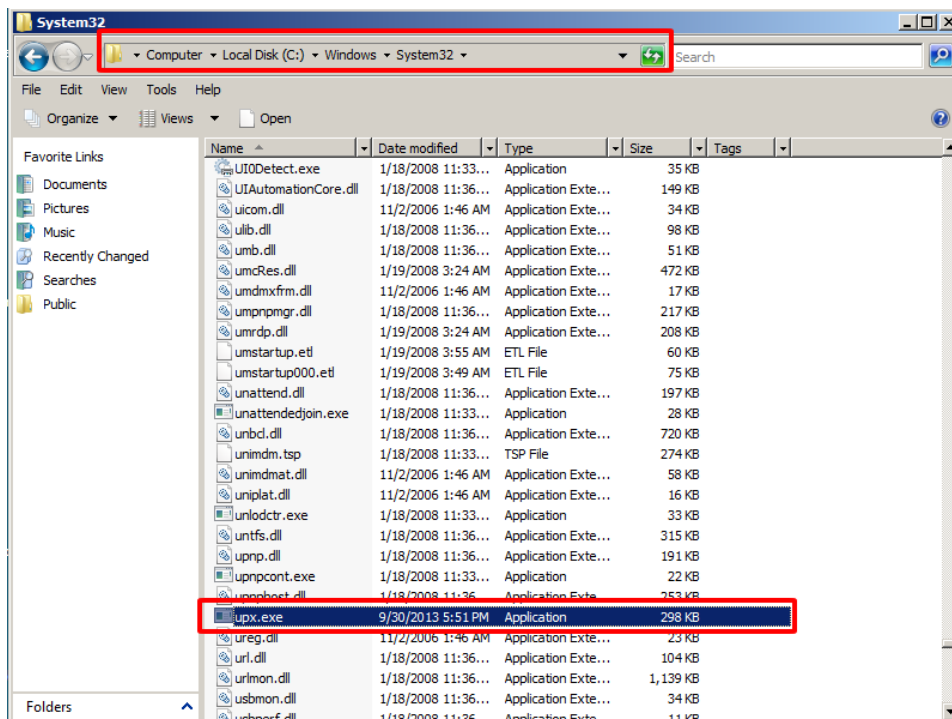


Sử dụng các kiến thức đã học, sinh viên tìm thêm dấu hiệu chứng tỏ Lab01-02.exe bị nén.

Sử dụng upx391w

Giải nén và copy upx.exe vào thư mục C:\Windows\System32.





Mở Command Prompt và thực hiện lệnh : Upx
Thông báo trợ giúp UPX hiển thị như hình dưới đây:

```

Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Windows\system32>upx.exe
      Ultimate Packer for eXecutables
      Copyright (C) 1996 - 2013
UPX 3.91w      Markus Oberhumer, Laszlo Molnar & John Reiser   Sep 30th 2013

Usage: upx [-123456789dlthUL] [-qvfk] [-o file] file..

Commands:
  -1      compress faster                      -9      compress better
  -d      decompress                          -l      list compressed file
  -t      test compressed file                 -U      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.

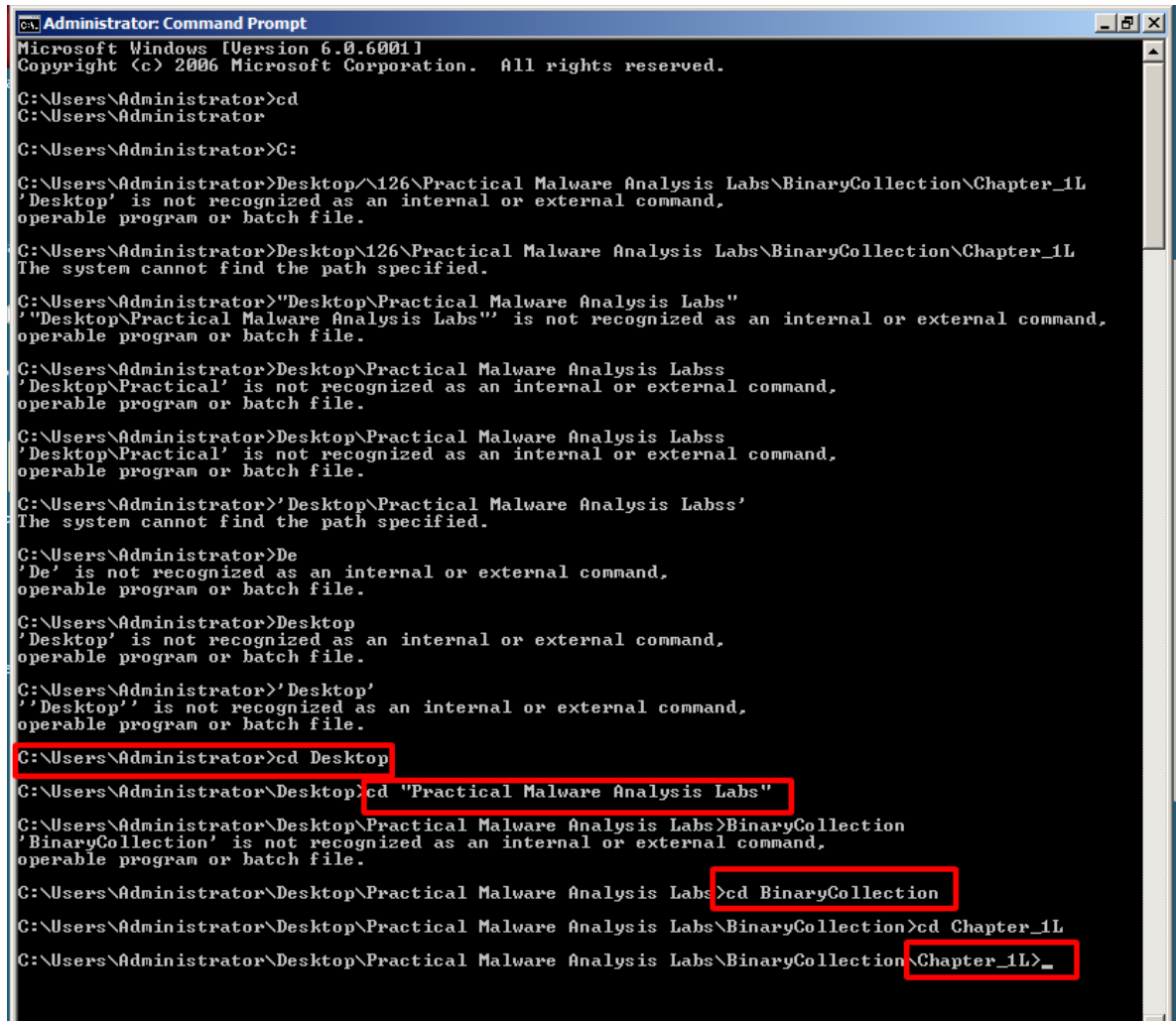
UPX comes with ABSOLUTELY NO WARRANTY; for details visit http://upx.sf.net

C:\Windows\system32>
  
```

Sử dụng lệnh `cd` để chuyển đến thư mục chứa các mẫu mã độc.

Sử dụng lệnh :

`cd "\\Users\Administrator\Desktop\126\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L`



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

C:\Users\Administrator>cd
C:\Users\Administrator

C:\Users\Administrator>C:
C:\Users\Administrator>Desktop\126\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L
'Desktop' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator>Desktop\126\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L
The system cannot find the path specified.

C:\Users\Administrator>"Desktop\Practical Malware Analysis Labs"
'"Desktop\Practical Malware Analysis Labs"' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator>Desktop\Practical Malware Analysis Labss
'Desktop\Practical' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator>Desktop\Practical Malware Analysis Labss
'Desktop\Practical' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator>'Desktop\Practical Malware Analysis Labss'
The system cannot find the path specified.

C:\Users\Administrator>De
'De' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator>Desktop
'Desktop' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator>'Desktop'
''Desktop'' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator>cd Desktop
C:\Users\Administrator\Desktop>cd "Practical Malware Analysis Labs"
C:\Users\Administrator\Desktop\Practical Malware Analysis Labs>BinaryCollection
'BinaryCollection' is not recognized as an internal or external command,
operable program or batch file.

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

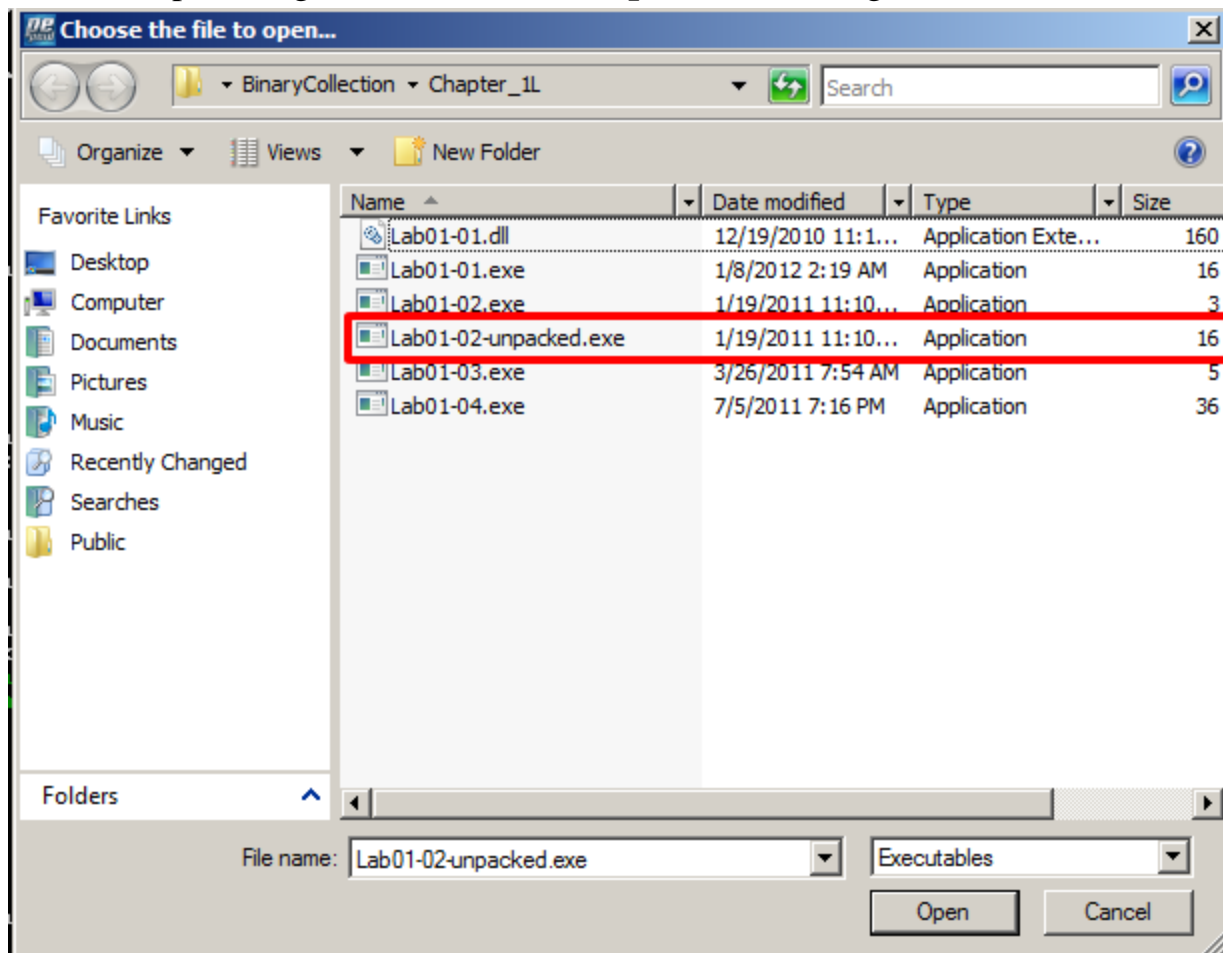
Thực hiện lệnh **`UPX -d -o Lab01-02-unpacked.exe Lab01-02.exe`** để giải nén tập tin:

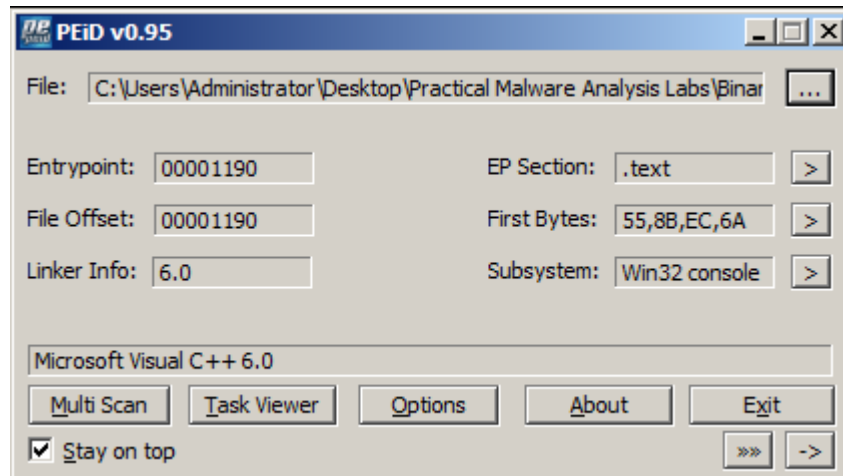
```
C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L>UPX -d -o
Lab01-02-unpacked.exe Lab01-02.exe
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2013
UPX 3.91w Markus Oberhumer, Laszlo Molnar & John Reiser Sep 30th 2013

  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>
```

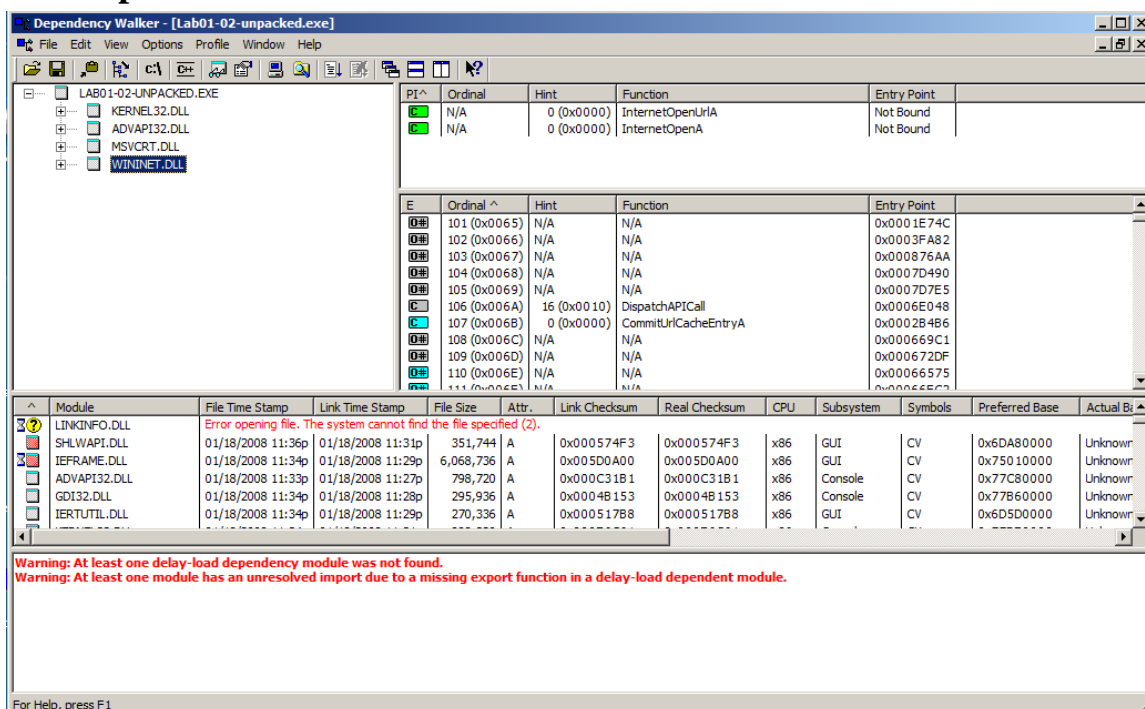
Phân tích tập tin đã giải nén **Lab01-02-unpacked.exe** bằng PEiD.





Sử dụng Dependency Walker..

Thực hiện các yêu cầu tương tự phần 1.3.1, lưu ý hai hàm **InternetOpenUrlA** và **InternetOpenA**.



Sử dụng Strings

Tìm các chuỗi trong tập tin, thấy hai chuỗi đáng ngờ là **MalService** và **http://www.malwareanalysisbook.com**.

Điều này giúp ta có thể đưa ra giả thiết rằng mã độc kết nối tới địa chỉ <http://www.malwareanalysisbook.com> và khi thực thi sẽ tạo dịch vụ với tên **MalService**.



```
Administrator: cmd - Shortcut (2)
__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
```