LAB 2A: Basic Static Techniques

Course Name: Malware Analysis and Reverse Engineering (IAM302)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 11/1/2023

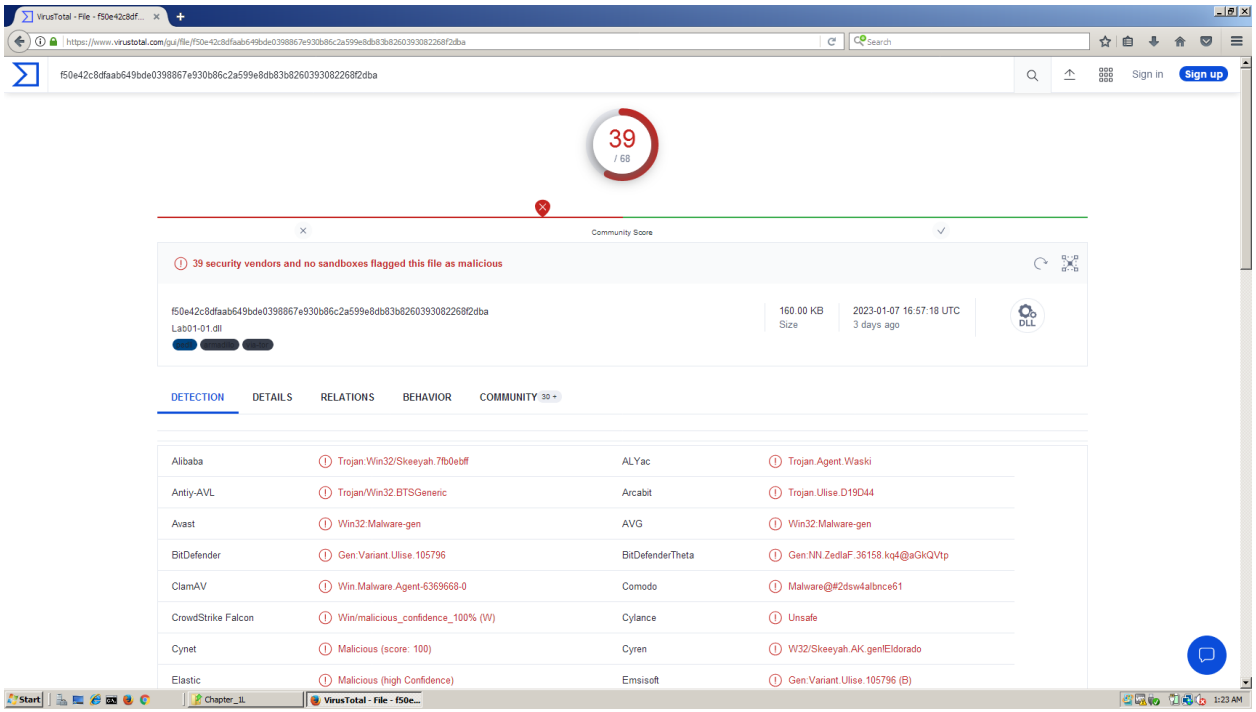
Purpose

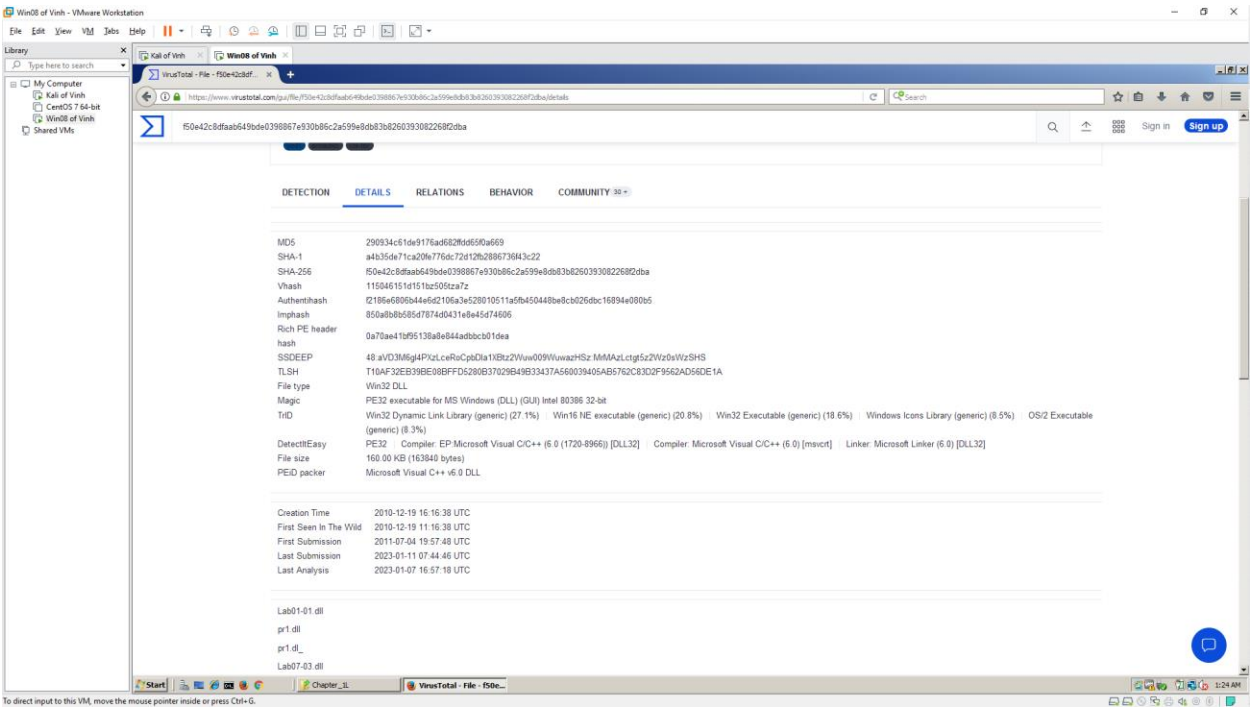
You will practice the techniques in chapter 1.
What you need:

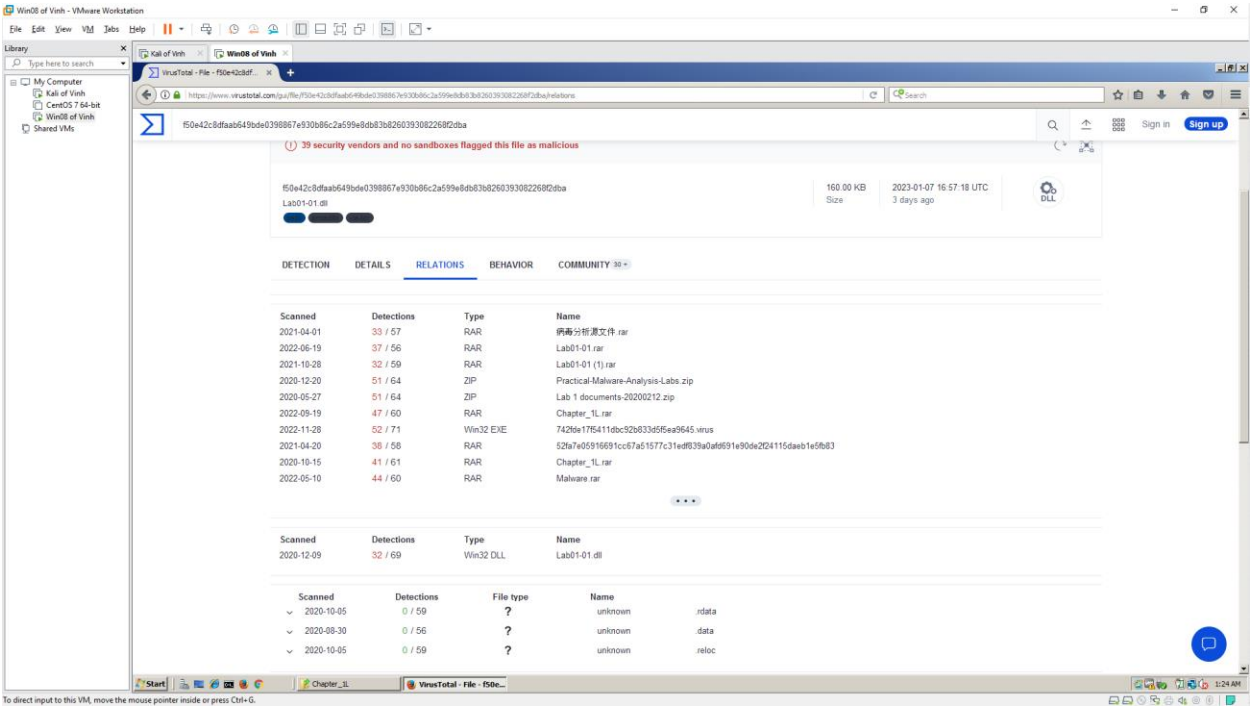
- A Windows computer (real or virtual) with an Internet connection
- Recommended: the textbook: "Practical Malware Analysis"

VirusTotal

- Lab01-01.dll

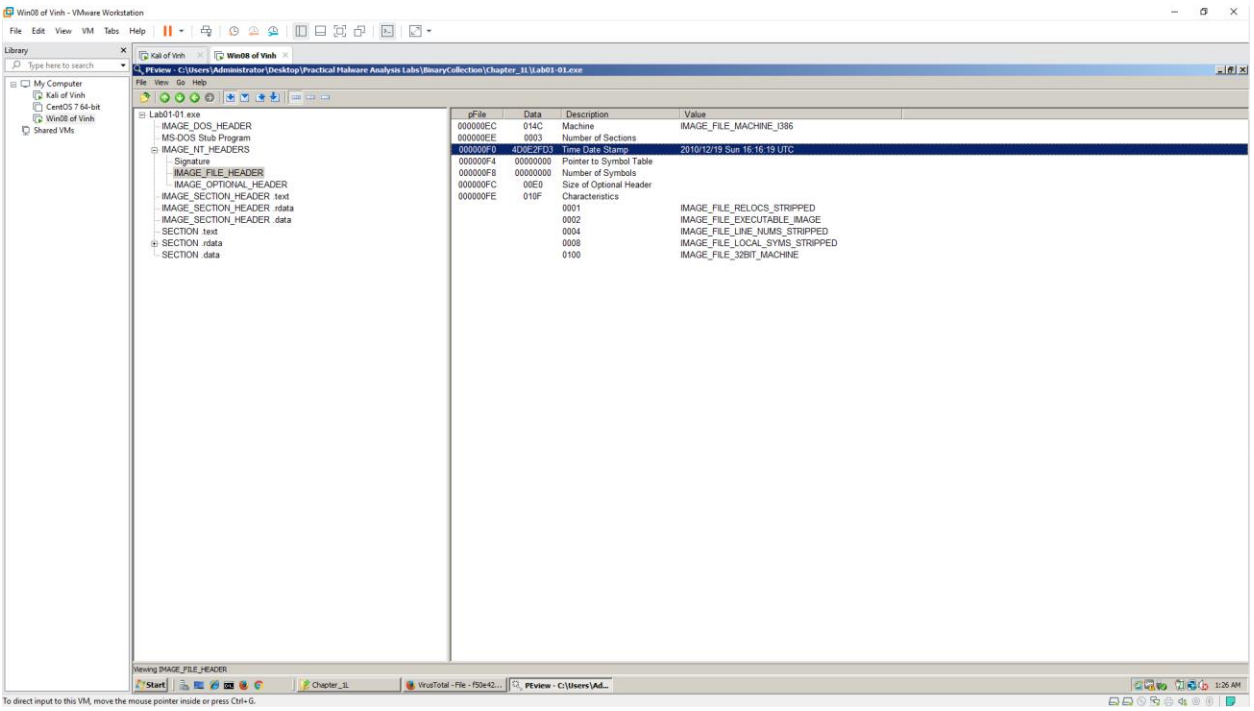






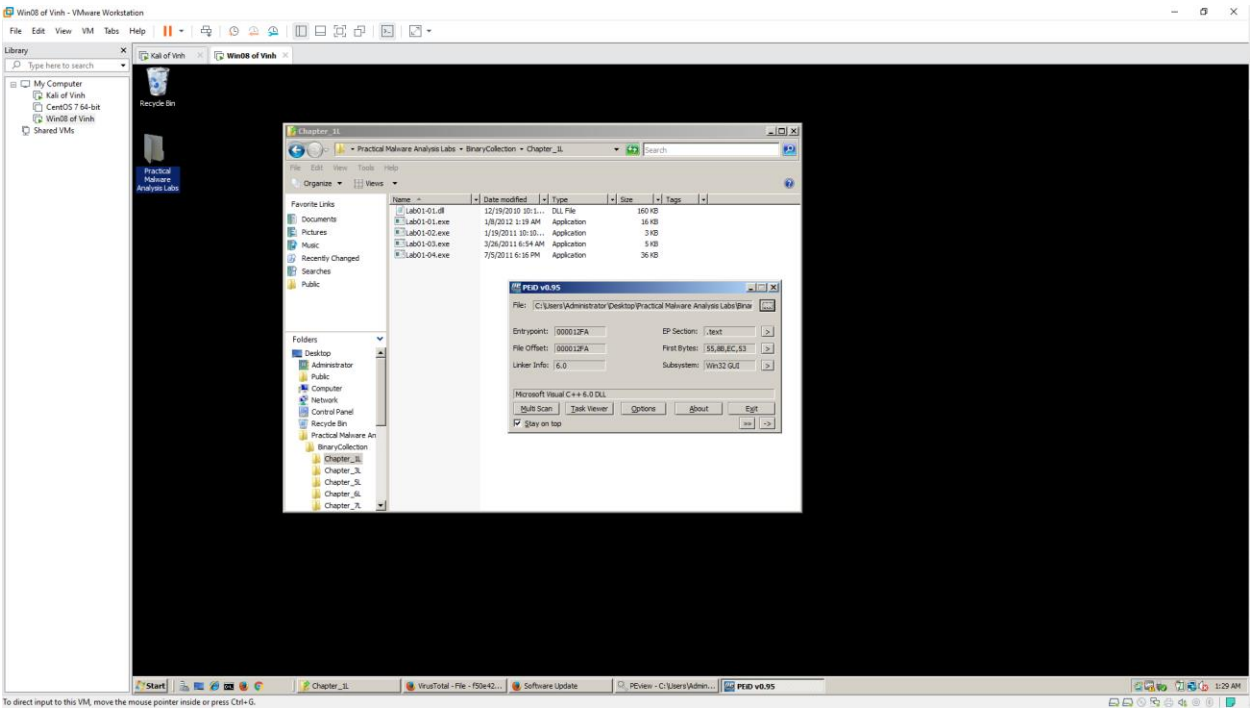
PEview

- **Lab01-01.exe**



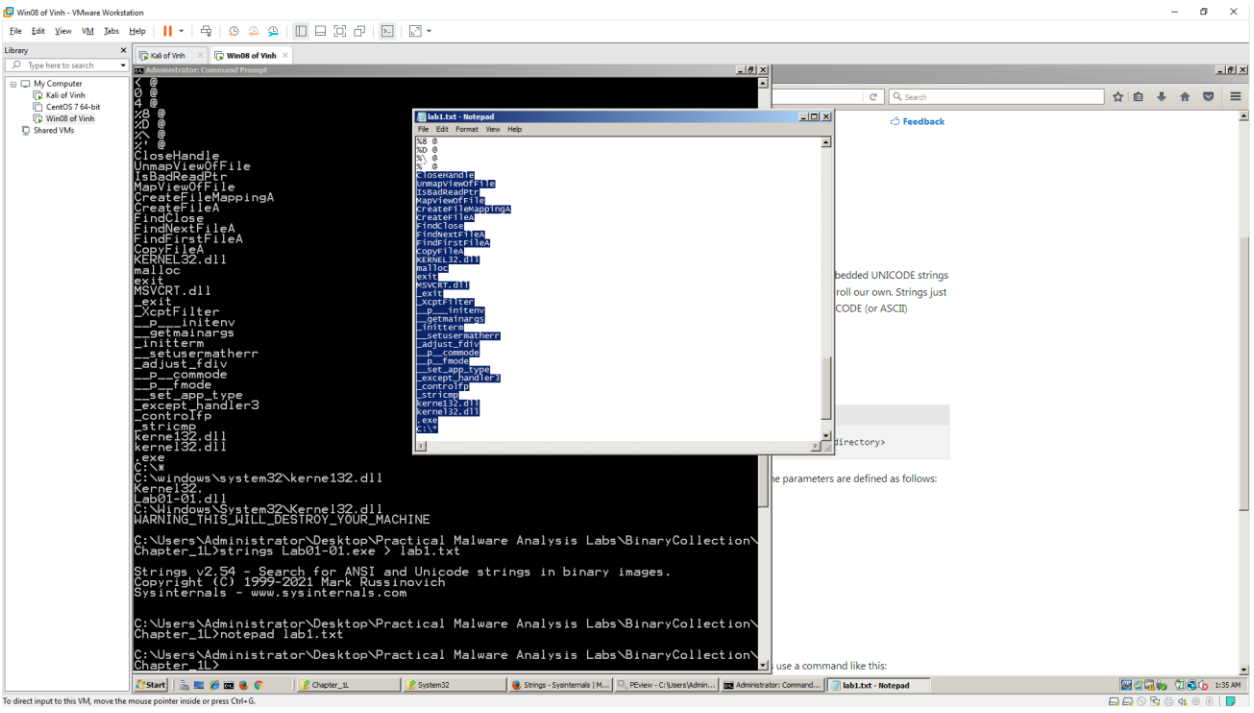
PEiD

- Lab01-01.dll

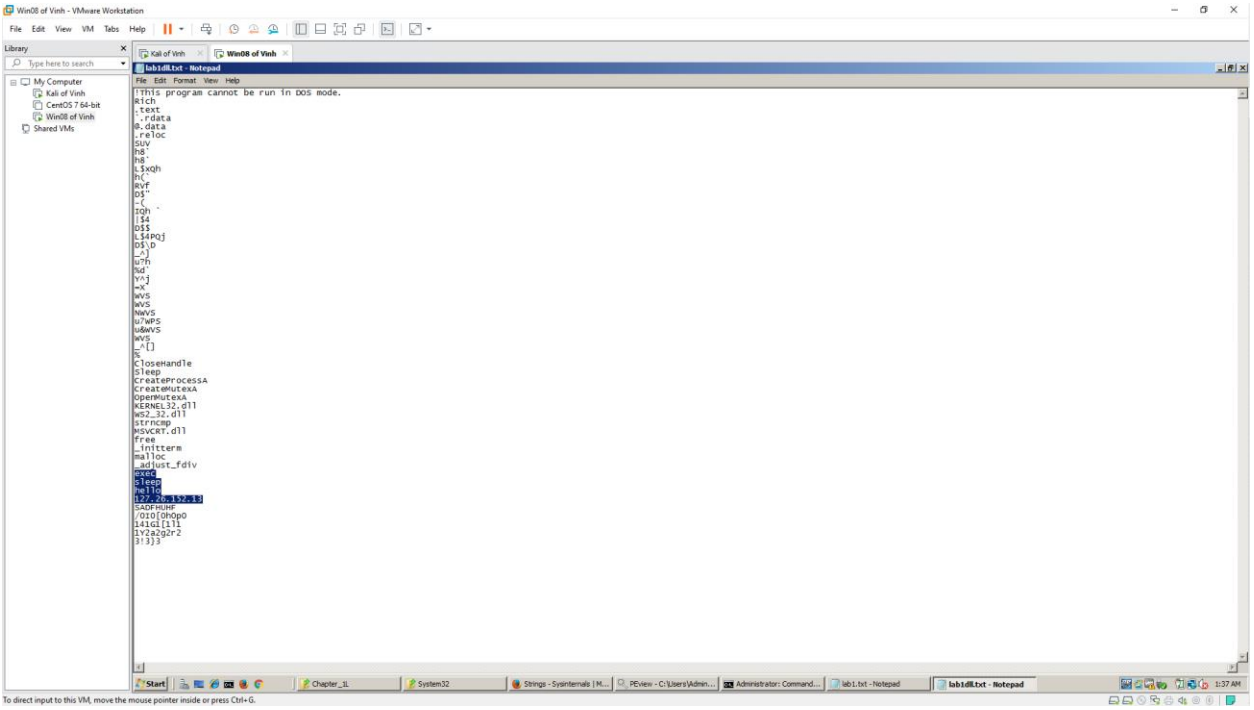


Strings

- **Lab01-01.exe**

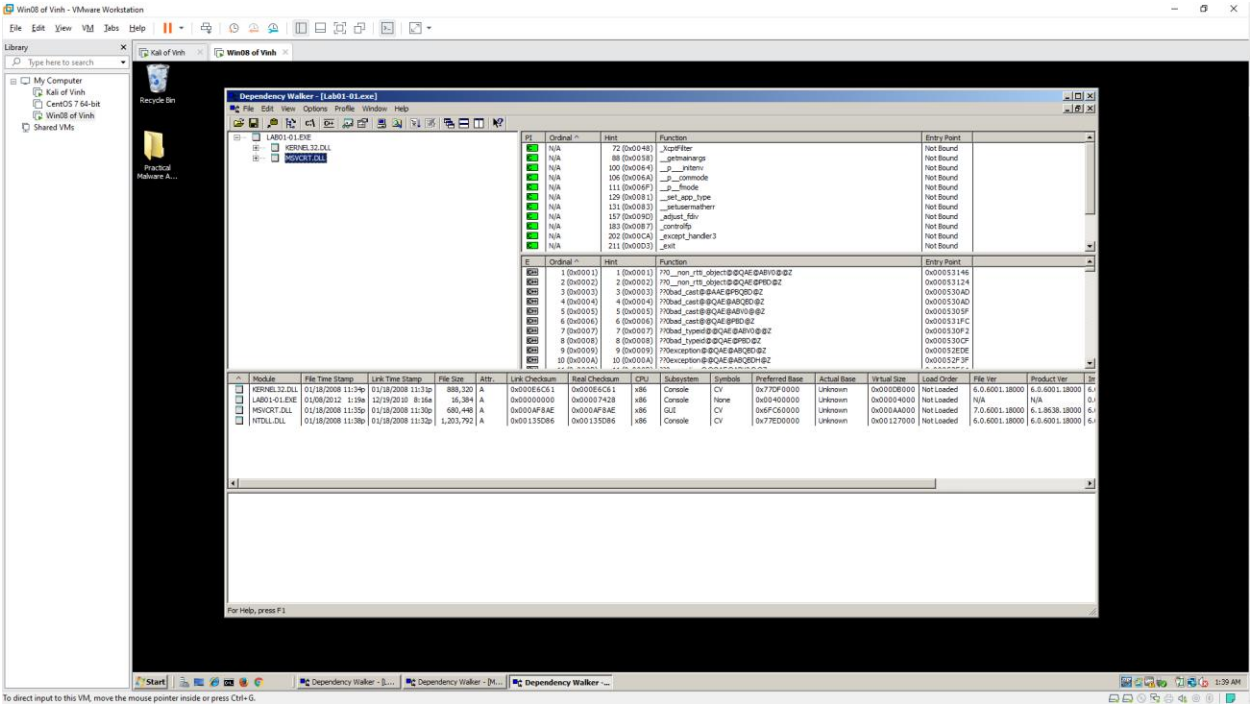


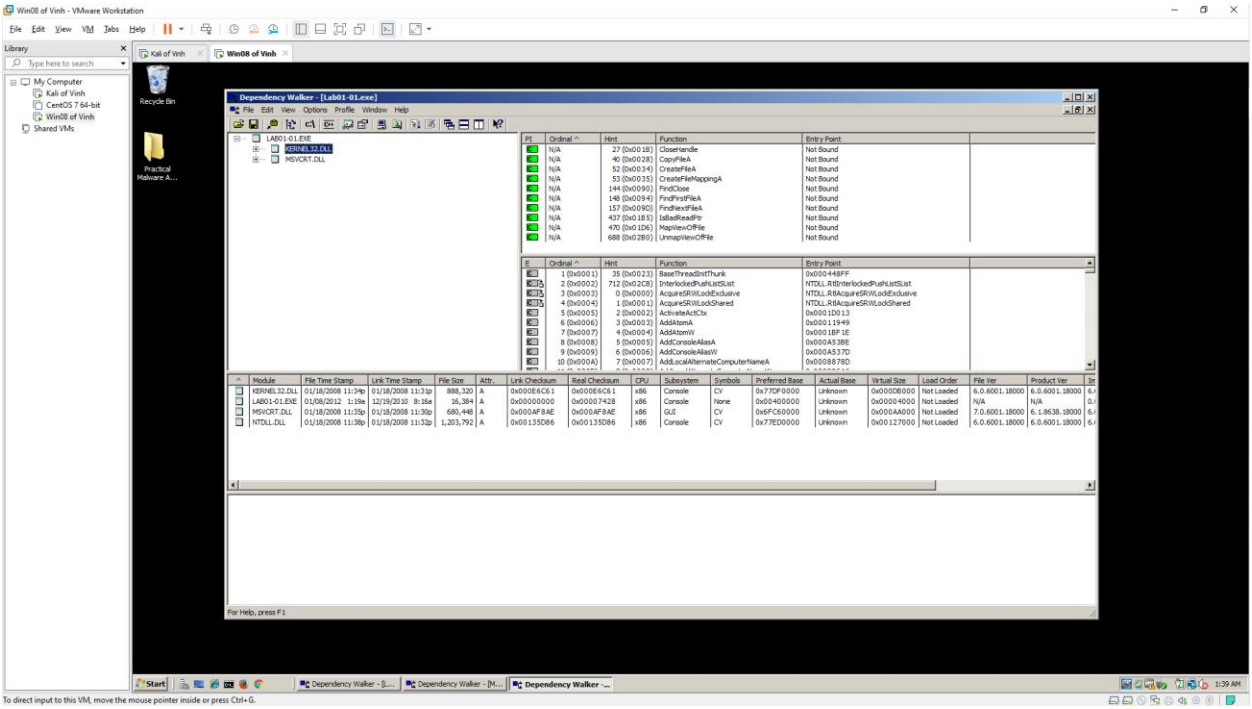
- **Lab01-01.dll**



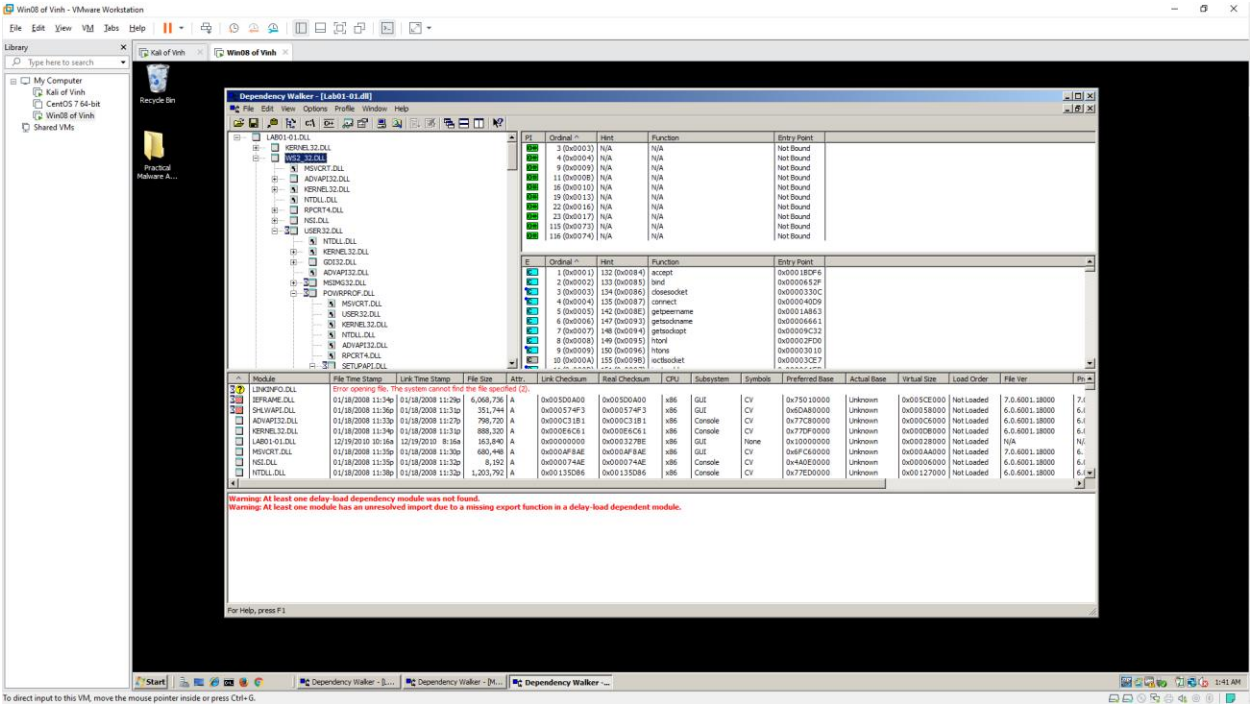
Dependency Walker

- **Lab01-01.exe**


Win08 of Vinh - VMware Workstation
Dependency Walker - [Lab01-01.exe]
LAB01-01.EXE
KERNEL32.DLL
MSVCRT.DLL
For Help, press F1


Win08 of Vinh - VMware Workstation
Dependency Walker - [Lab01-01.exe]
LAB01-01.EXE
KERNEL32.DLL
MSVCRT.DLL
For Help, press F1

- **Lab01-01.dll**


Win08 of Vinh - VMware Workstation
Dependency Walker - [Lab01-01.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.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

LAB 2B: Basic Static Techniques

Course Name: Malware Analysis and Reverse Engineering (IAM302)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 11/1/2023

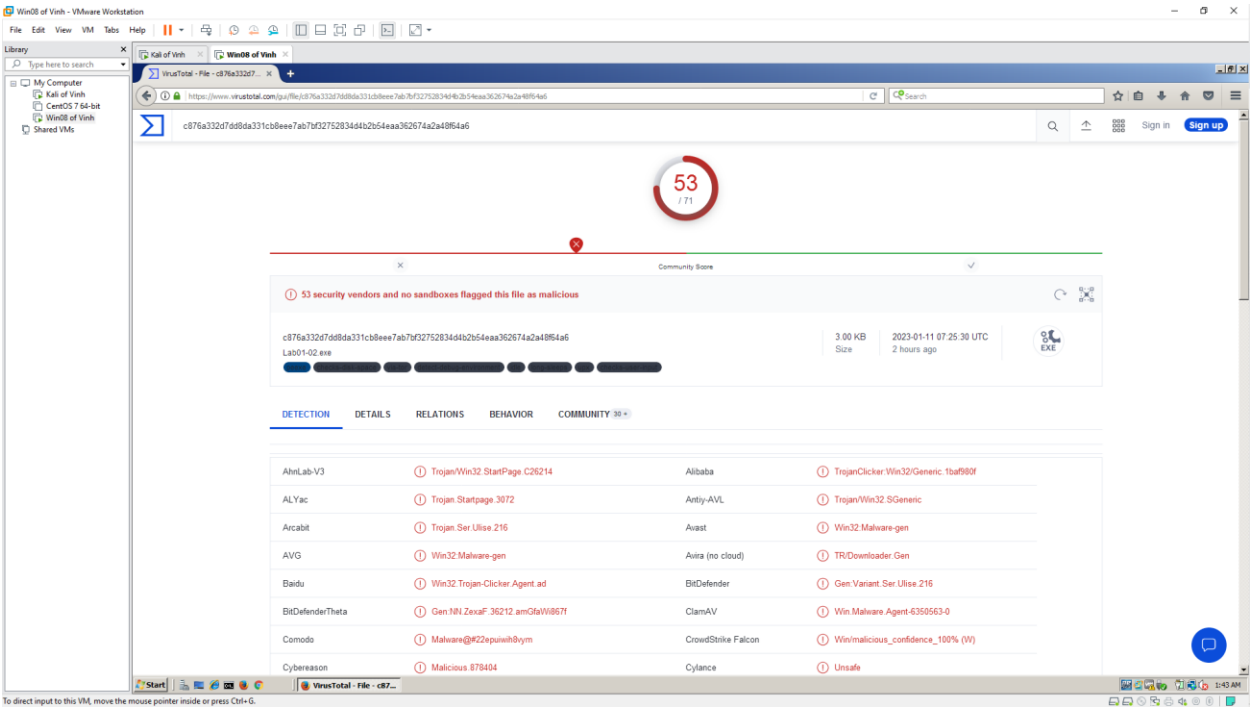
Purpose

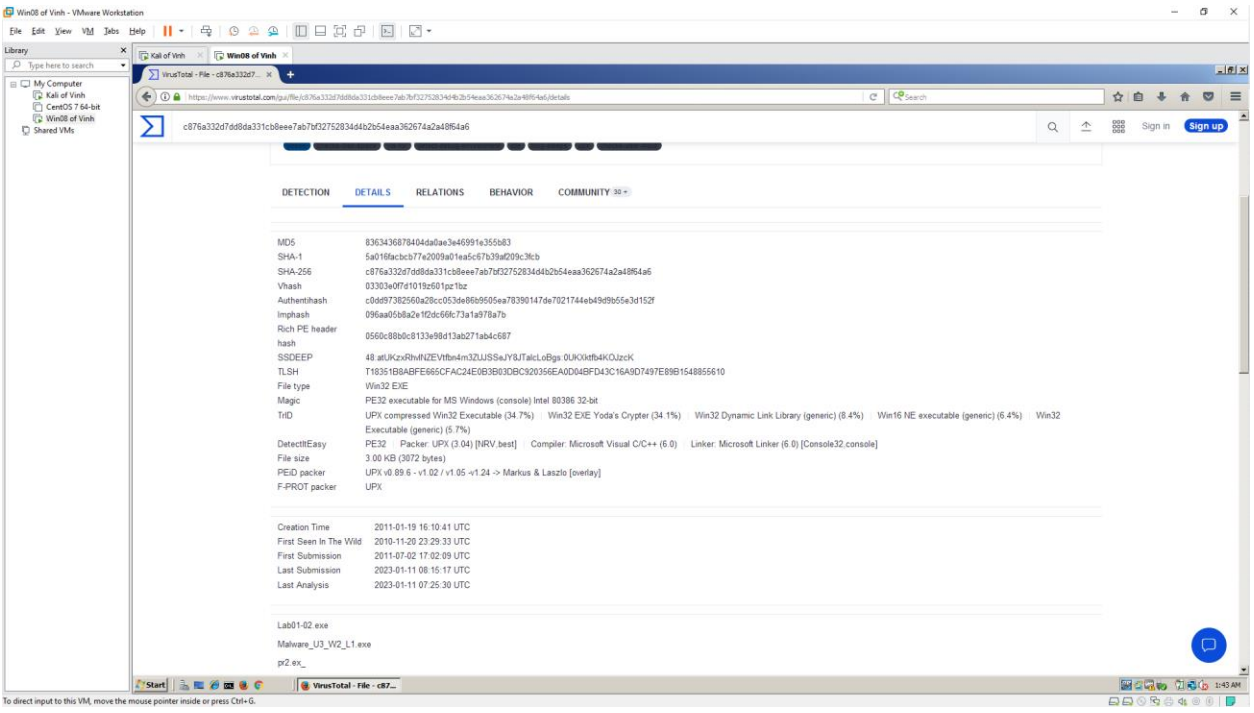
You will practice the techniques in chapter 1. This project follows Lab 1-2 in the textbook. There are more detailed solutions in the back of the book.

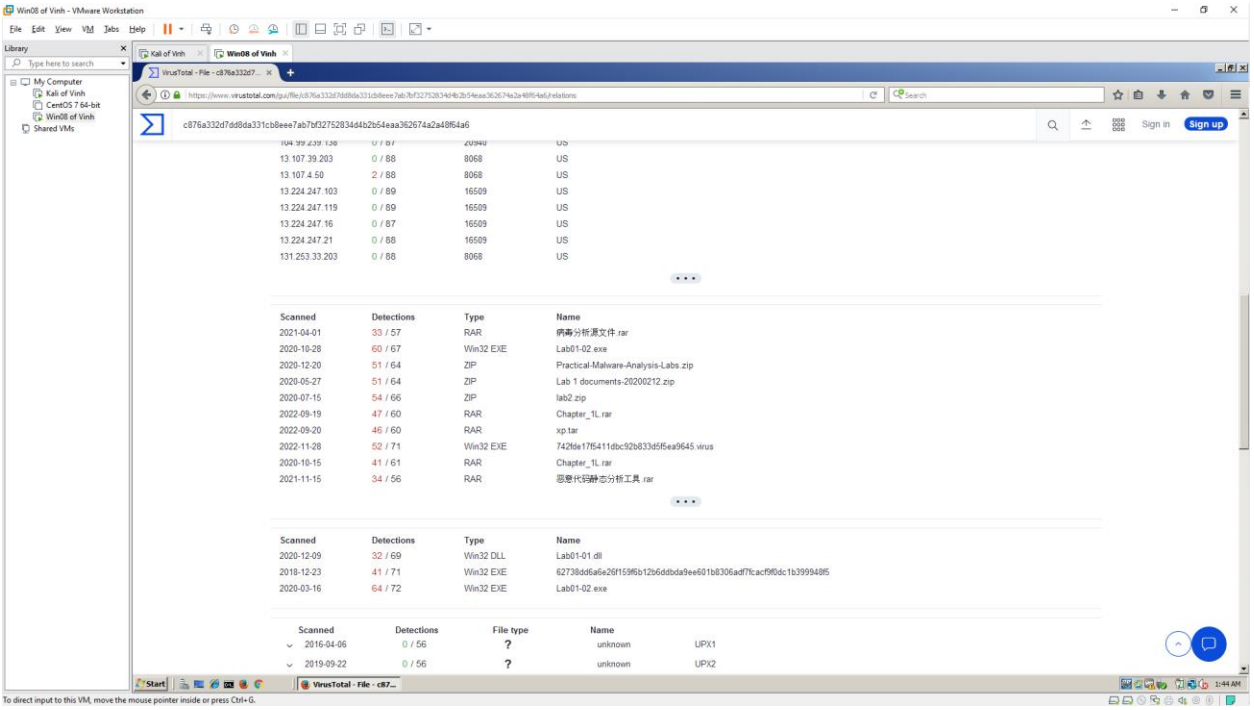
What you need:

- A Windows computer (real or virtual) with an Internet connection
- Recommended: the textbook: "Practical Malware Analysis"

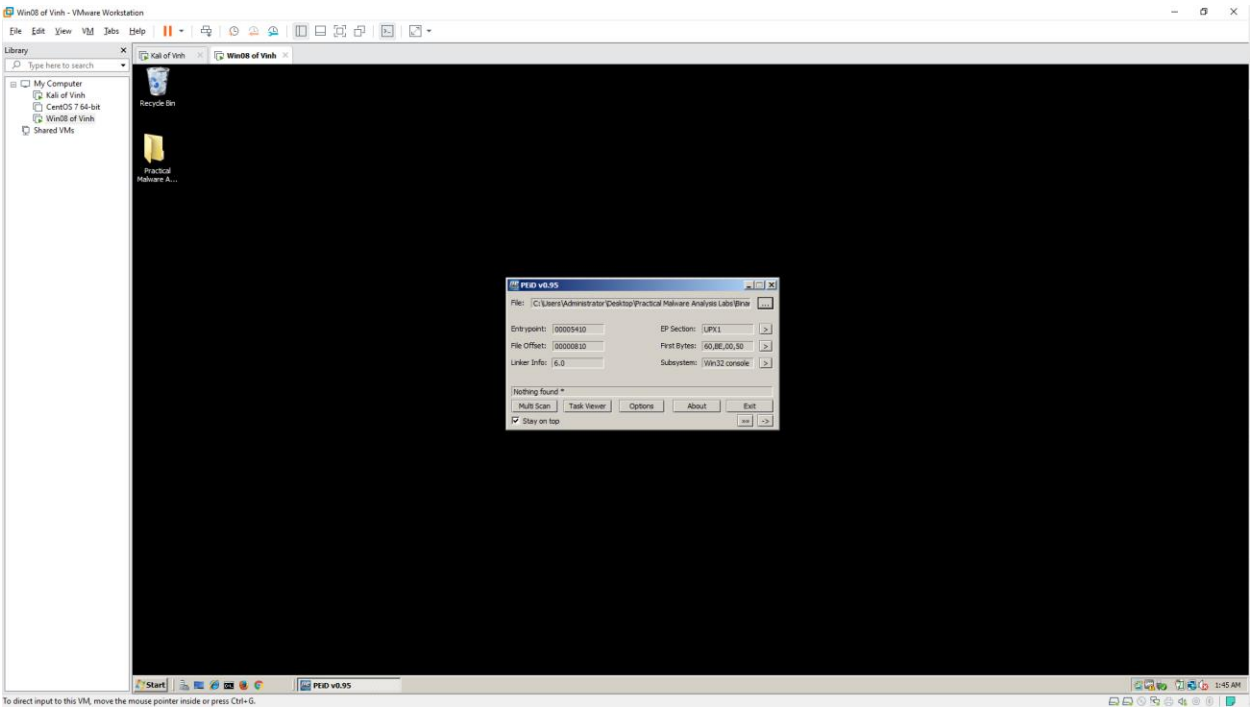
VirusTotal

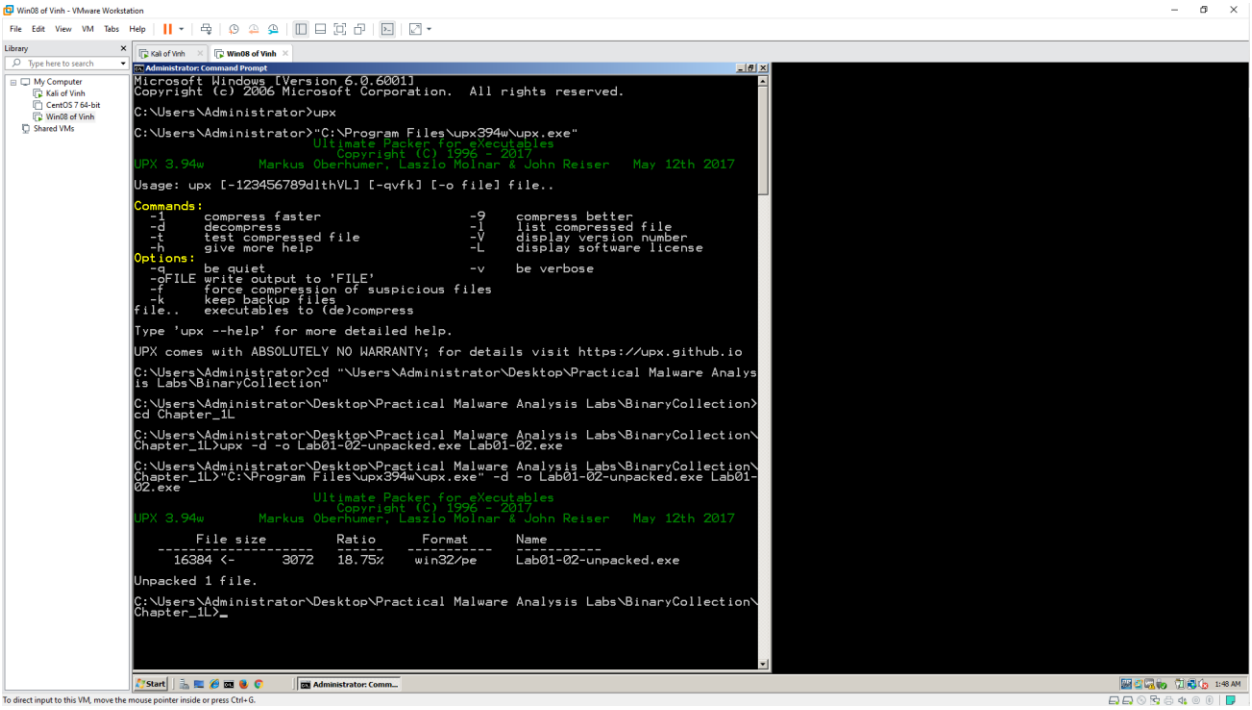


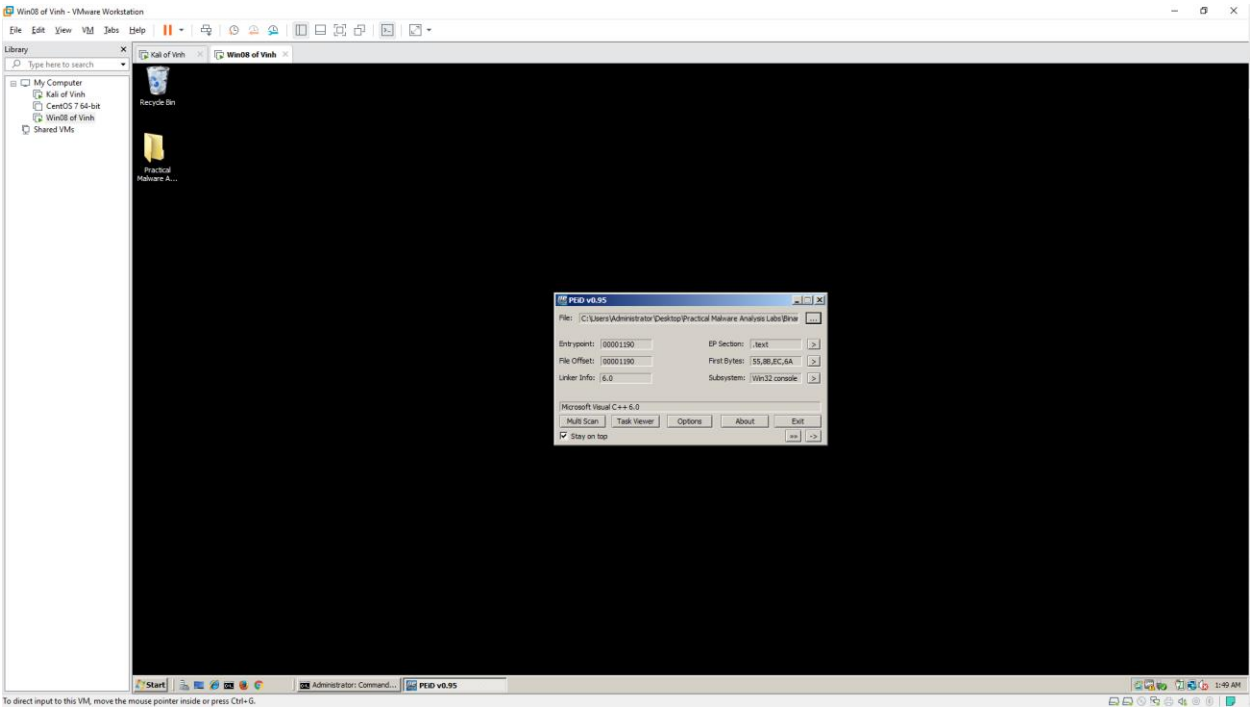




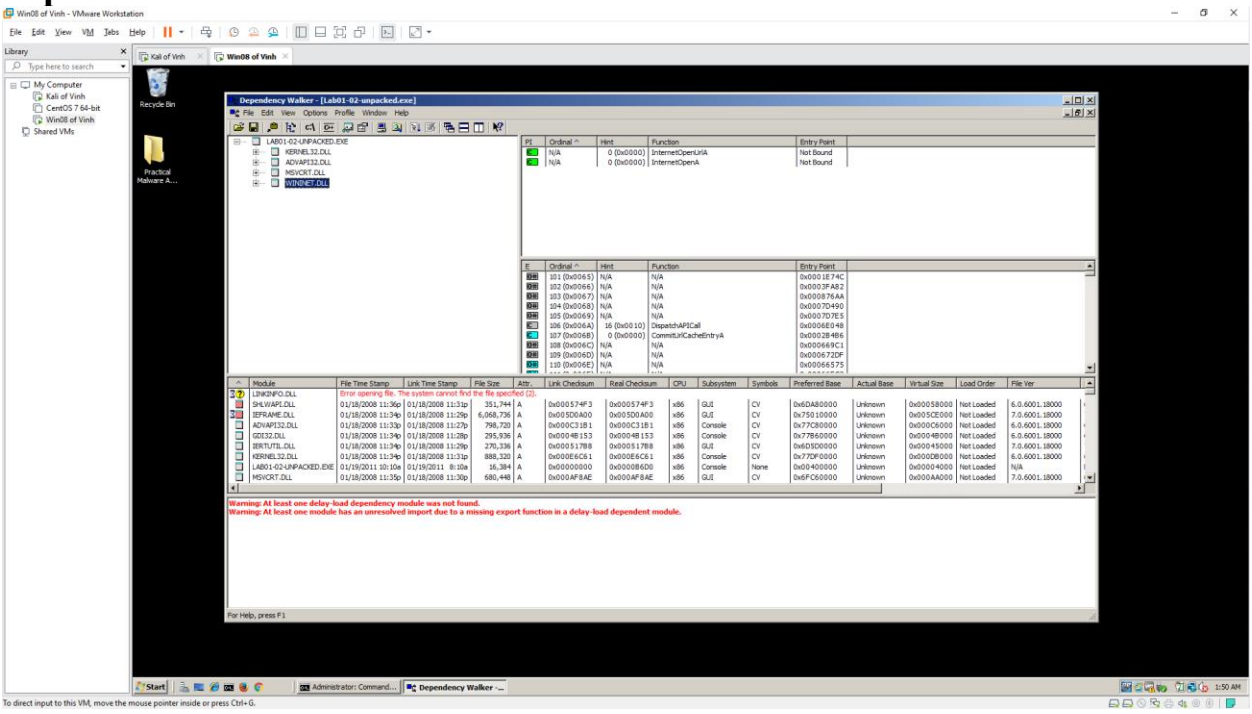
Unpacking the File


Win08 of Vinh - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali of Vinh
CentOS 7 64-bit
Win08 of Vinh
Shared VMs
Kali of Vinh
Win08 of Vinh
Recycle Bin
Practical Malware A...
PEiD v0.95
File: C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\Binar
Entrypoint: 00005410
File Offset: 00000810
Linker Info: 6.0
EP Section: UPX1
First Bytes: 60,BE,00,50
Subsystem: Win32 console
Nothing found *
Multi Scan
Task Viewer
Options
About
Exit
Stay on top
Start
PEiD v0.95
11:45 AM
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

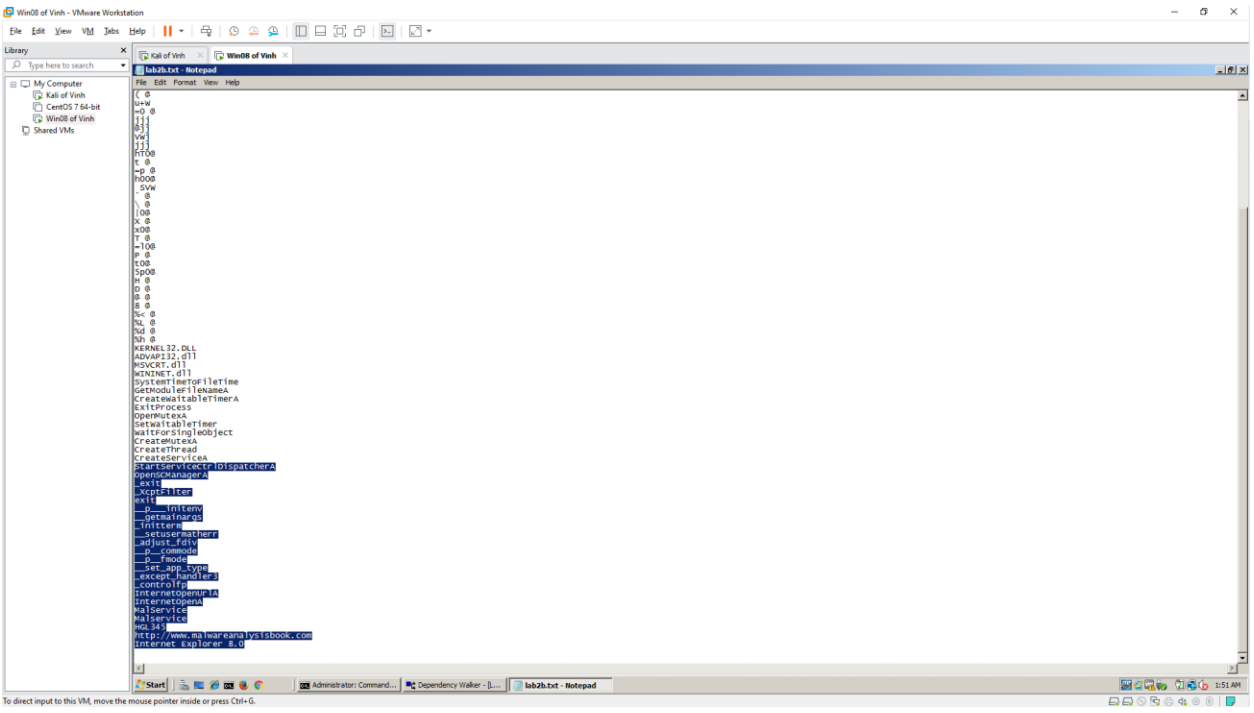

Win08 of Vinh - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali of Vinh
CentOS 7 64-bit
Win08 of Vinh
Shared VMs
Kali of Vinh
Win08 of Vinh
Administrator: Command Prompt
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights 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>cd "\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection"
C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection>cd Chapter_1L
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>
Start
Administrator: Comm...
1:48 AM
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



Imports



Strings


Win08 of Vinh - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali of Vinh
CentOS 7 64-bit
Win08 of Vinh
Shared VMs
Kali of Vinh
Win08 of Vinh
lab2b.txt - Notepad
File Edit Format View Help
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
Internet Explorer 8.0
Start
Administrator: Command...
Dependency Walker - [L...
lab2b.txt - Notepad
11:51 AM
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.