Lab 8

Configuring a Malware Lab

Course Name: IAM302

Student Name: Phạm Thành Long

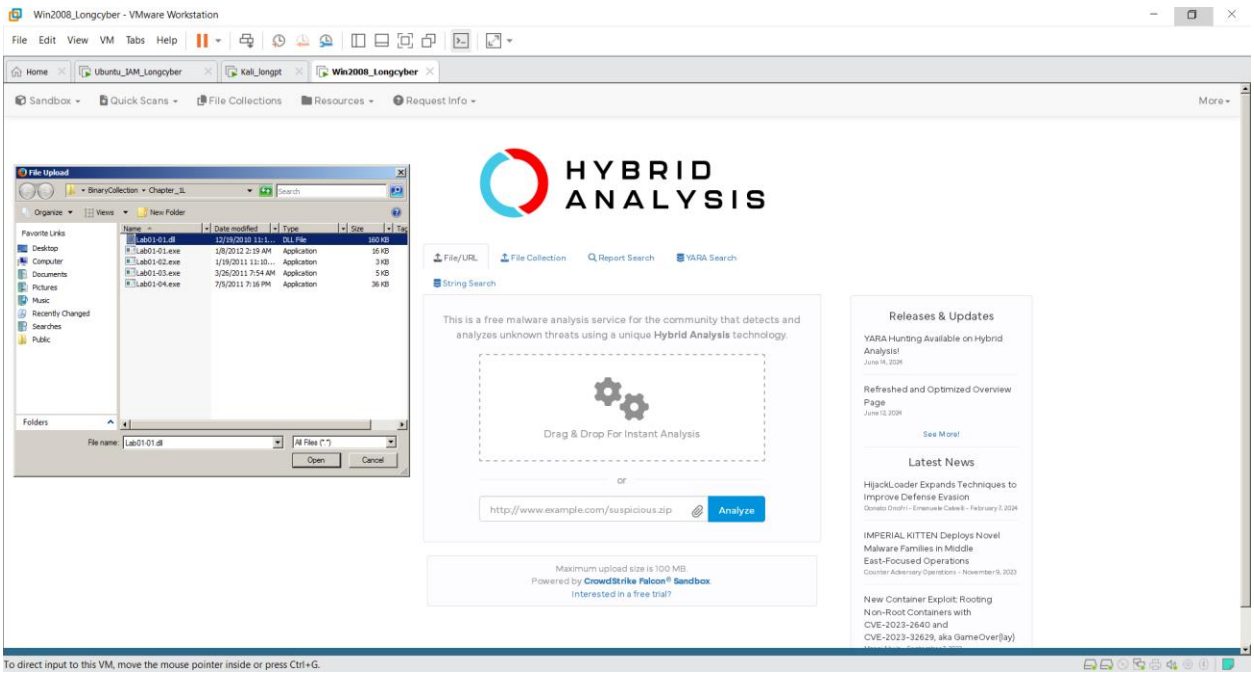
Instructor Name: Mai Hoàng Đỉnh

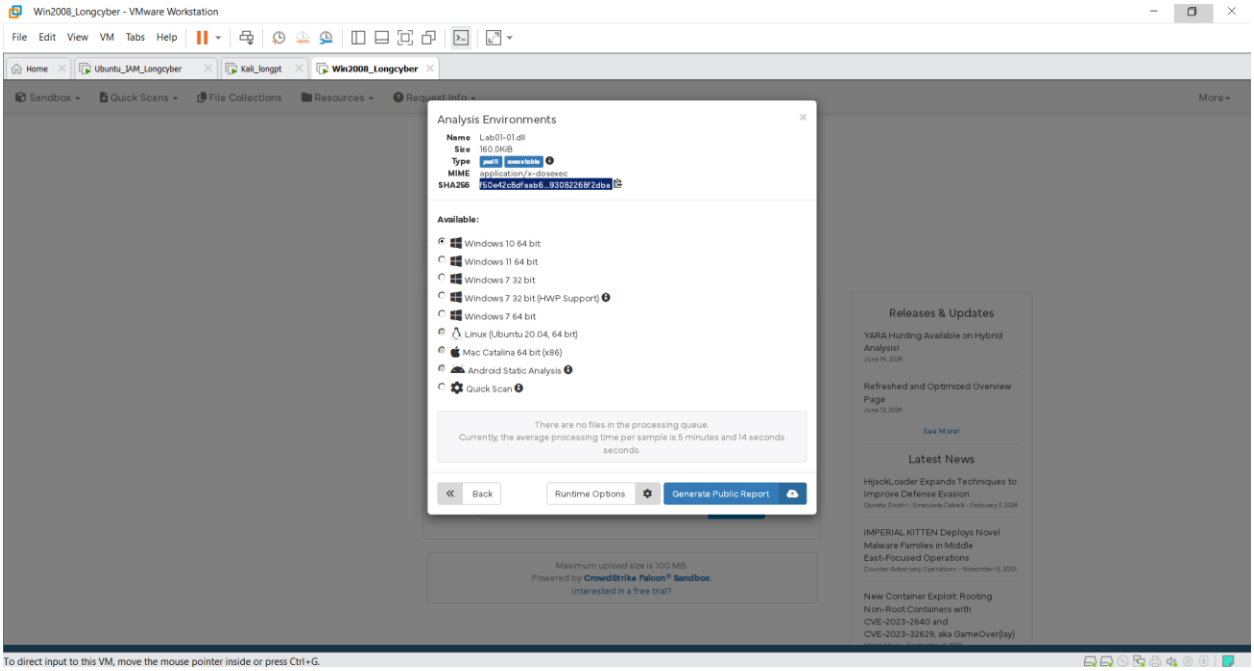
Lab Due Date: 30/09/2024

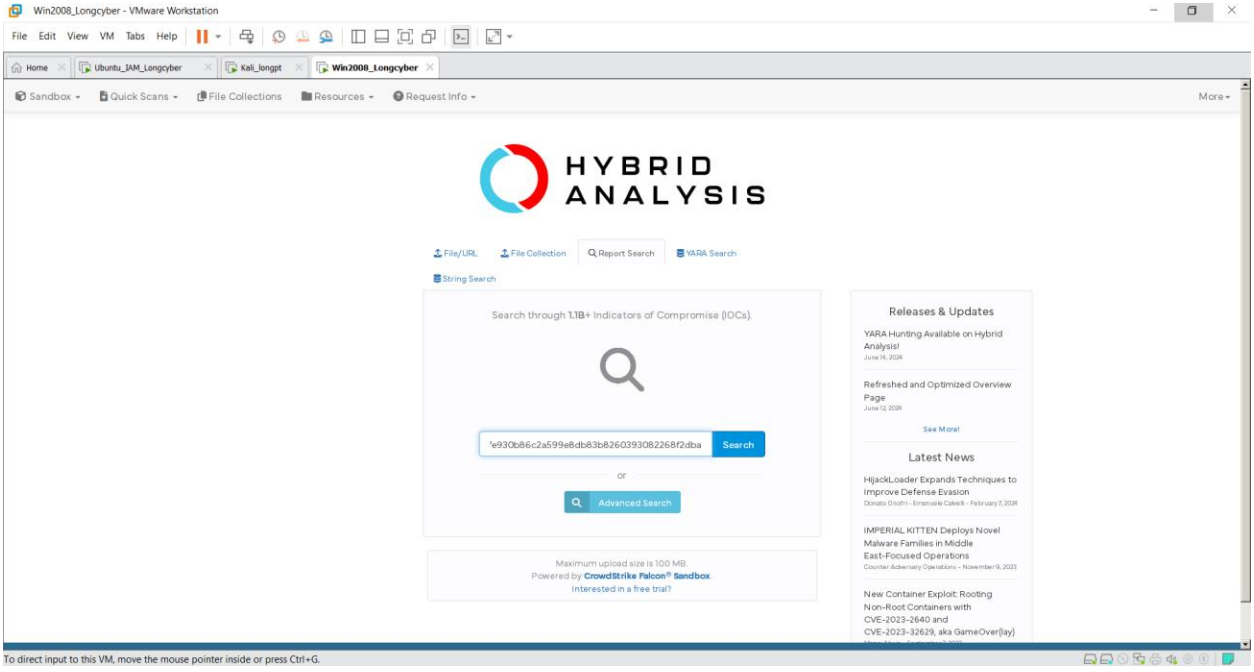
1. Basic Static Techniques

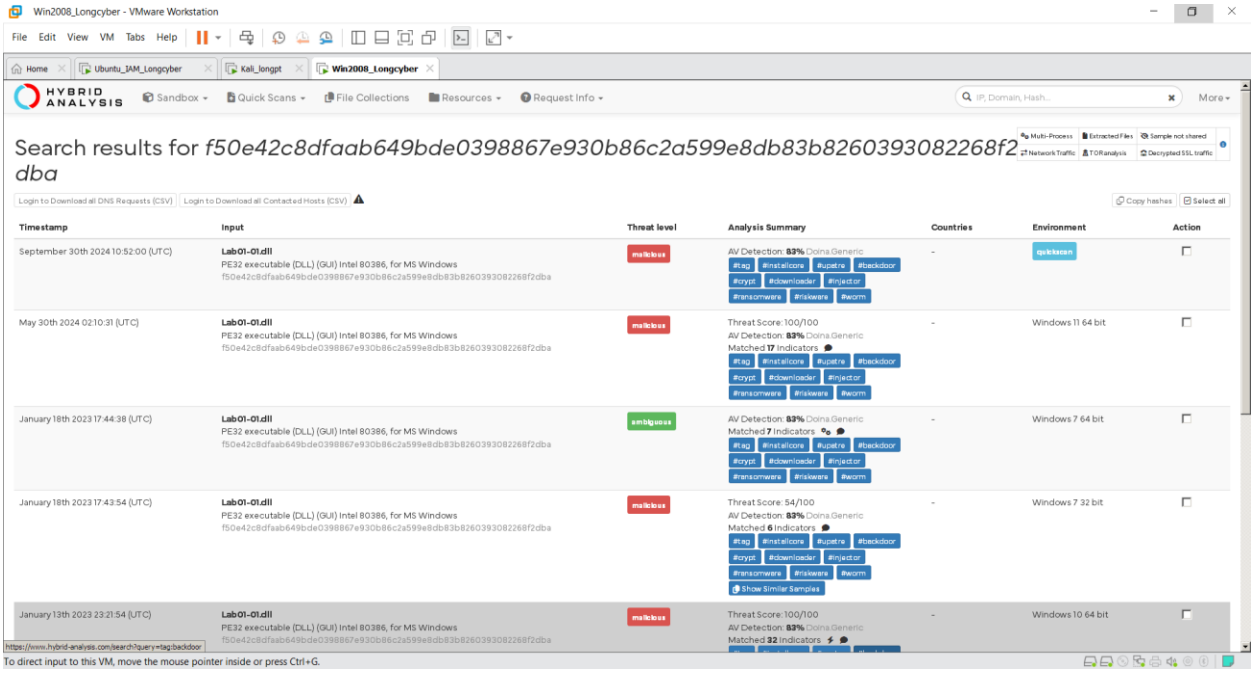
a. Lab01-01.exe

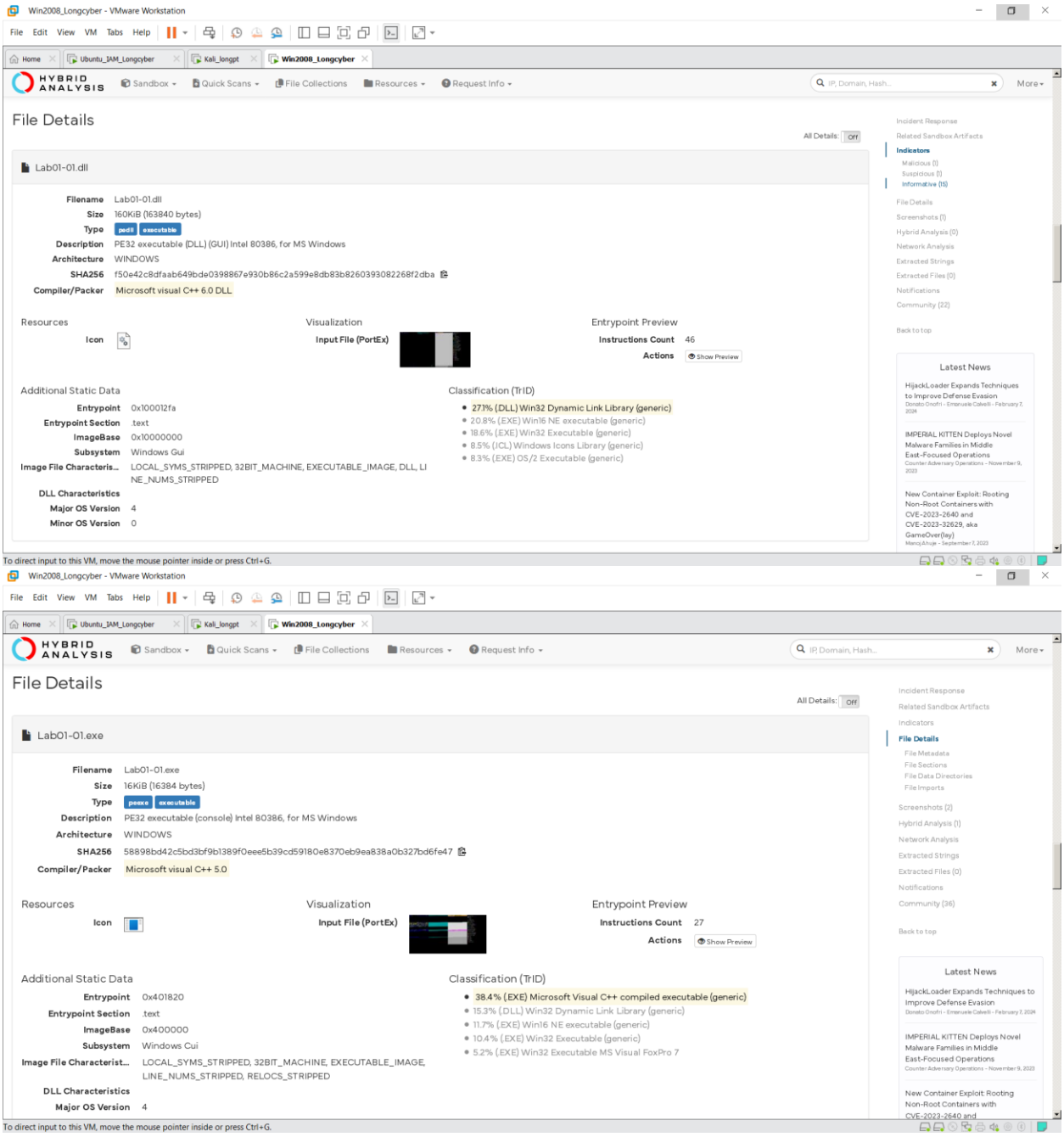
Upload the Lab01-01.exe and Lab01-01.dll files to https://www.hybrid-analysis.com
Turn in the image showing your analysis of Lab01-01.dll as shown below.




Win2008_Longcyber - VMware Workstation
File Edit View VM Tabs Help
Home
Ubuntu_IAM_Longcyber
Kali_longpt
Win2008_Longcyber
Sandbox
Quick Scans
File Collections
Resources
Request Info
More
Analysis Environments
Name Lab01-01.dll
Size 160.0KiB
Type pe32 executable
MIME application/x-dosexec
SHA256 f50e42c8dfaab6...93082268f2dba
Available:
Windows 10 64 bit
Windows 11 64 bit
Windows 7 32 bit
Windows 7 32 bit (HWP Support)
Windows 7 64 bit
Linux (Ubuntu 20.04, 64 bit)
Mac Catalina 64 bit (x86)
Android Static Analysis
Quick Scan
There are no files in the processing queue.
Currently, the average processing time per sample is 5 minutes and 14 seconds seconds.
Back
Runtime Options
Generate Public Report
Maximum upload size is 100 MB.
Powered by CrowdStrike Falcon® Sandbox
Interested in a free trial?
Releases & Updates
YARA Hunting Available on Hybrid Analysis!
Refreshed and Optimized Overview Page
See More!
Latest News
HijackLoader Expands Techniques to Improve Defense Evasion
IMPERIAL KITTEN Deploys Novel Malware Families in Middle East-Focused Operations
New Container Exploit: Rooting Non-Root Containers with CVE-2023-2640 and CVE-2023-32629, aka GameOver(lay)
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Win2008_Longcyber - VMware Workstation
File Edit View VM Tabs Help
Home
Ubuntu_IAM_Longcyber
Kali_longpt
Win2008_Longcyber
Sandbox
Quick Scans
File Collections
Resources
Request Info
More
HYBRID ANALYSIS
File/URL
File Collection
Report Search
YARA Search
String Search
Search through 1.1B+ Indicators of Compromise (IOCs).
e930b86c2a599e8db83b826039308226 8f2dba
Search
or
Advanced Search
Maximum upload size is 100 MB.
Powered by CrowdStrike Falcon® Sandbox
Interested in a free trial?
Releases & Updates
YARA Hunting Available on Hybrid Analysis!
Refreshed and Optimized Overview Page
See More!
Latest News
HijackLoader Expands Techniques to Improve Defense Evasion
IMPERIAL KITTEN Deploys Novel Malware Families in Middle East-Focused Operations
New Container Exploit: Rooting Non-Root Containers with CVE-2023-2640 and CVE-2023-32629, aka GameOver(lay)
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

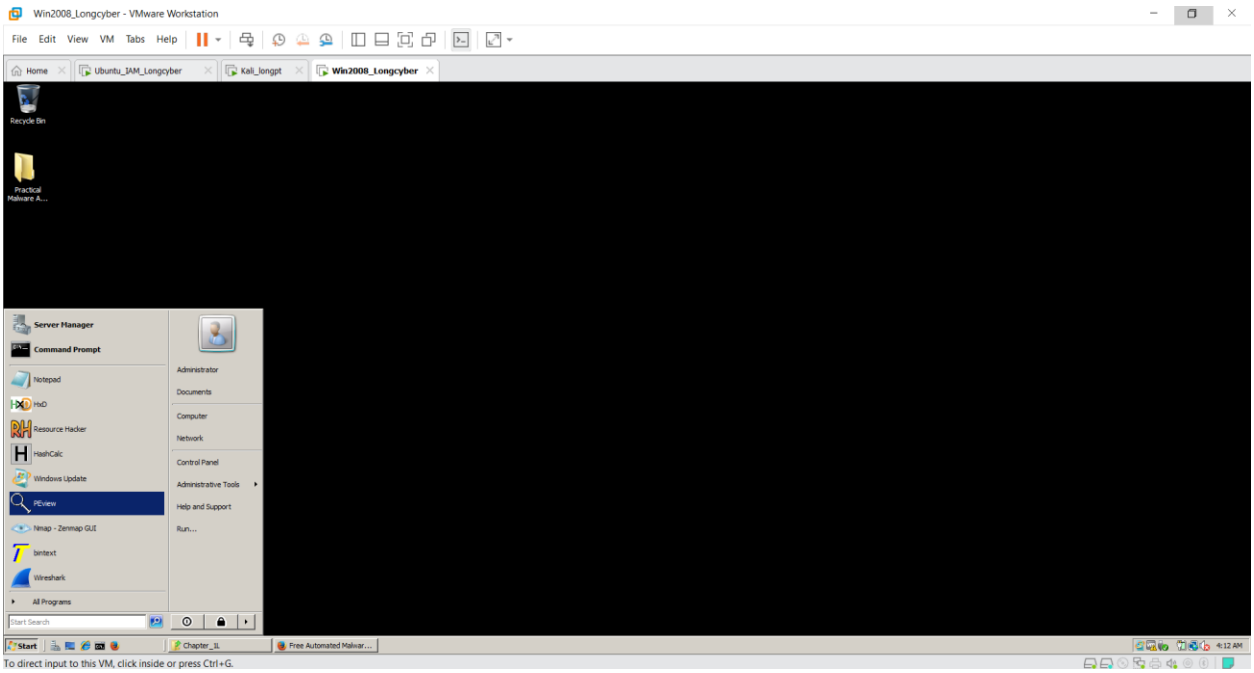

Win2008_Longcyber - VMware Workstation
File Edit View VM Tabs Help
Home
Ubuntu_IAM_Longcyber
Kali_longpt
Win2008_Longcyber
HYBRID ANALYSIS
Sandbox
Quick Scans
File Collections
Resources
Request Info
IP, Domain, Hash...
More
Search results for f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba
Multi-Process
Extracted Files
Sample not shared
Network Traffic
TOR analysis
Decrypted SSL traffic
Login to Download all DNS Requests (CSV)
Login to Download all Contacted Hosts (CSV)
Copy hashes
Select all
Timestamp
Input
Threat level
Analysis Summary
Countries
Environment
Action
September 30th 2024 10:52:00 (UTC)
Lab01-01.dll
PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba
malicious
AV Detection: 83% Doina.Generic
#tag #intelicore #upatre #backdoor
#crypt #downloader #injector
#ransomware #riskware #worm
qeleksecen
May 30th 2024 02:10:31 (UTC)
Lab01-01.dll
PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba
malicious
Threat Score: 100/100
AV Detection: 83% Doina.Generic
Matched 17 Indicators
#tag #intelicore #upatre #backdoor
#crypt #downloader #injector
#ransomware #riskware #worm
Windows 11 64 bit
January 18th 2023 17:44:38 (UTC)
Lab01-01.dll
PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba
ambiguous
AV Detection: 83% Doina.Generic
Matched 7 Indicators
#tag #intelicore #upatre #backdoor
#crypt #downloader #injector
#ransomware #riskware #worm
Windows 7 64 bit
January 18th 2023 17:43:54 (UTC)
Lab01-01.dll
PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba
malicious
Threat Score: 54/100
AV Detection: 83% Doina.Generic
Matched 6 Indicators
#tag #intelicore #upatre #backdoor
#crypt #downloader #injector
#ransomware #riskware #worm
Show Similar Samples
Windows 7 32 bit
January 13th 2023 23:21:54 (UTC)
Lab01-01.dll
PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba
malicious
Threat Score: 100/100
AV Detection: 83% Doina.Generic
Matched 32 Indicators
Windows 10 64 bit
https://www.hybrid-analysis.com/search?query=tag:backdoor
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



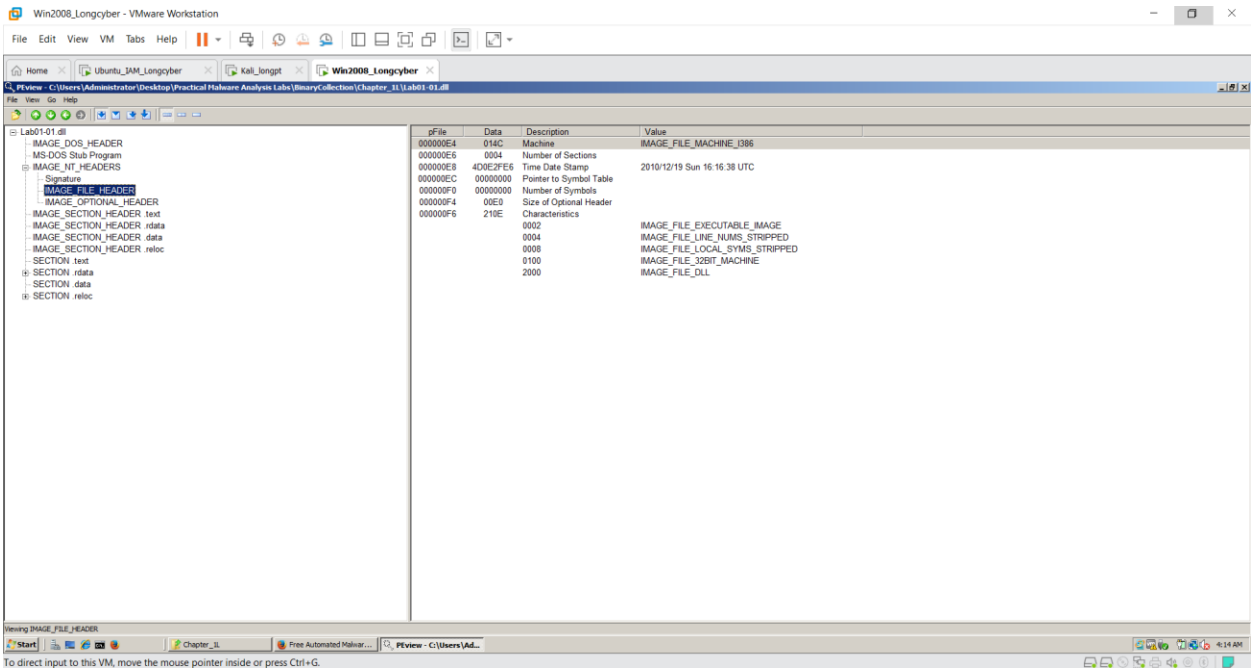
PEview

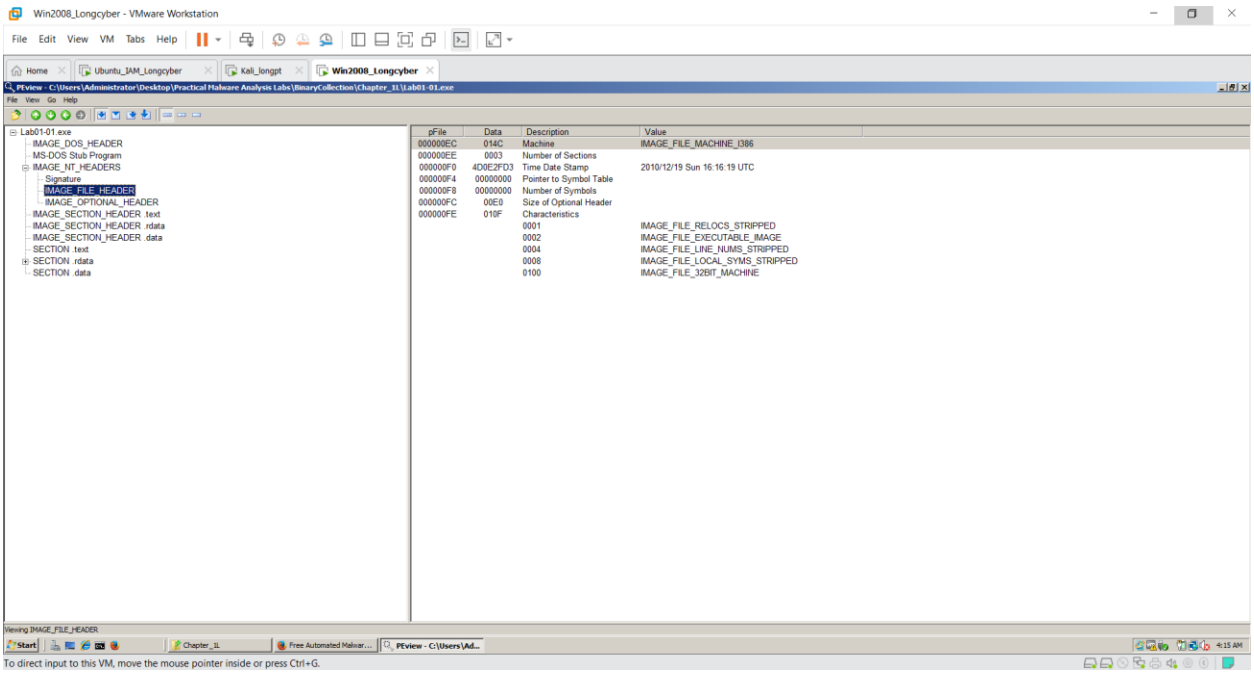
You can download PEview from here: https://wjradburn.com/software/

Open the files in PEview. For each file, find the "Time Date Stamp" as shown below. The files were both compiled on the same date within a minute of each other, indicating that they are part of the same package.



Turn in the image showing your analysis of Lab01-01.dll and Lab01-01.exe as shown below.





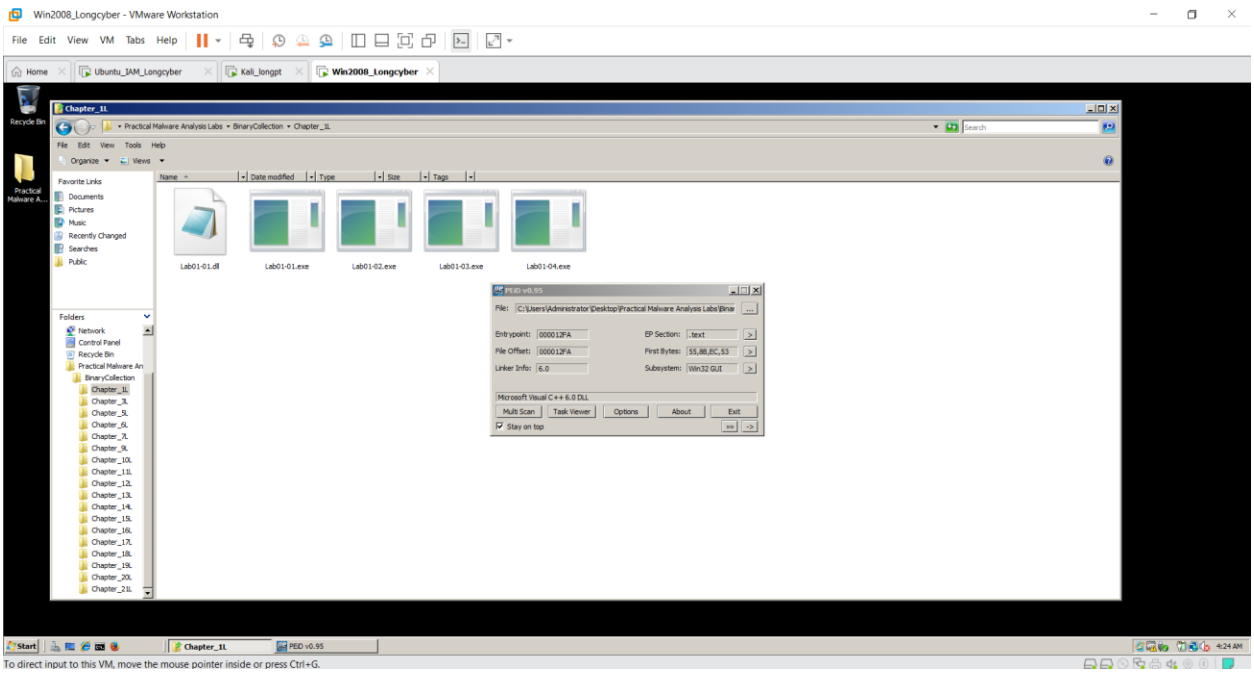
PEiD

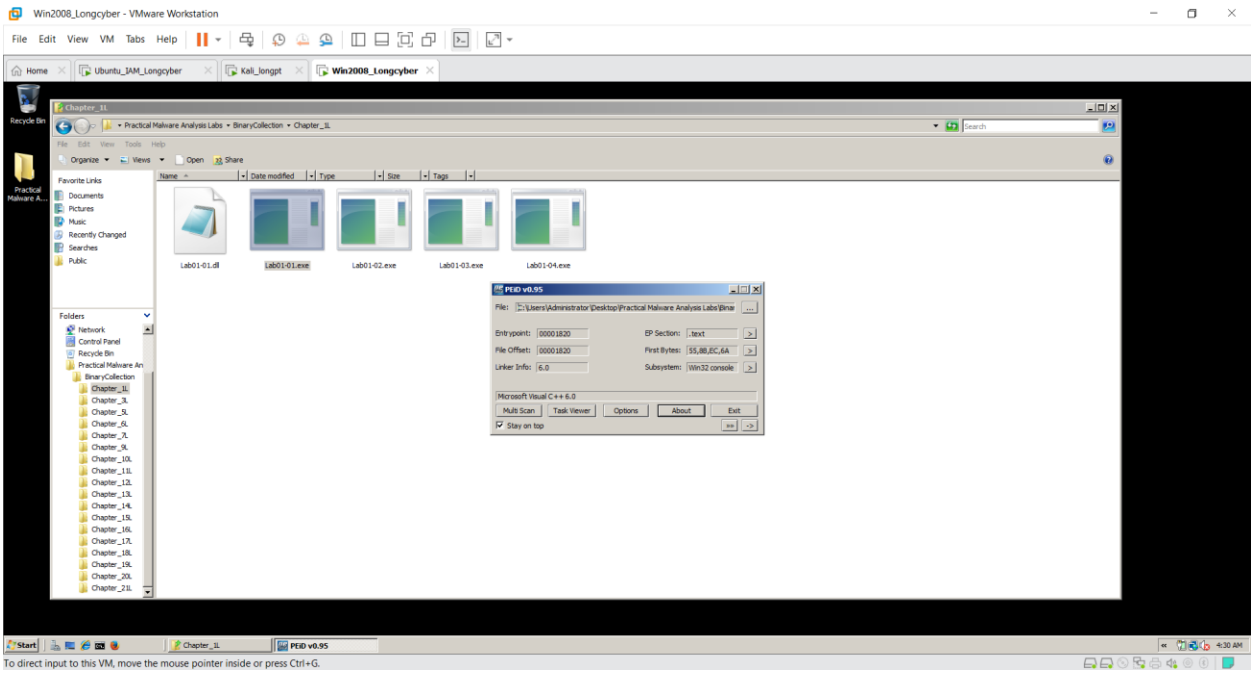
You can download PEiD here:

https://www.softpedia.com/progDownload/PEiD-updated-Download-4102.html

Open the files in PEiD. They are identified as "Microsoft Visual C++" files, which shows that they are unpacked.

Turn in the image showing your analysis of Lab01-01.dll as shown below. We will grade it based on the "First Bytes".





Strings

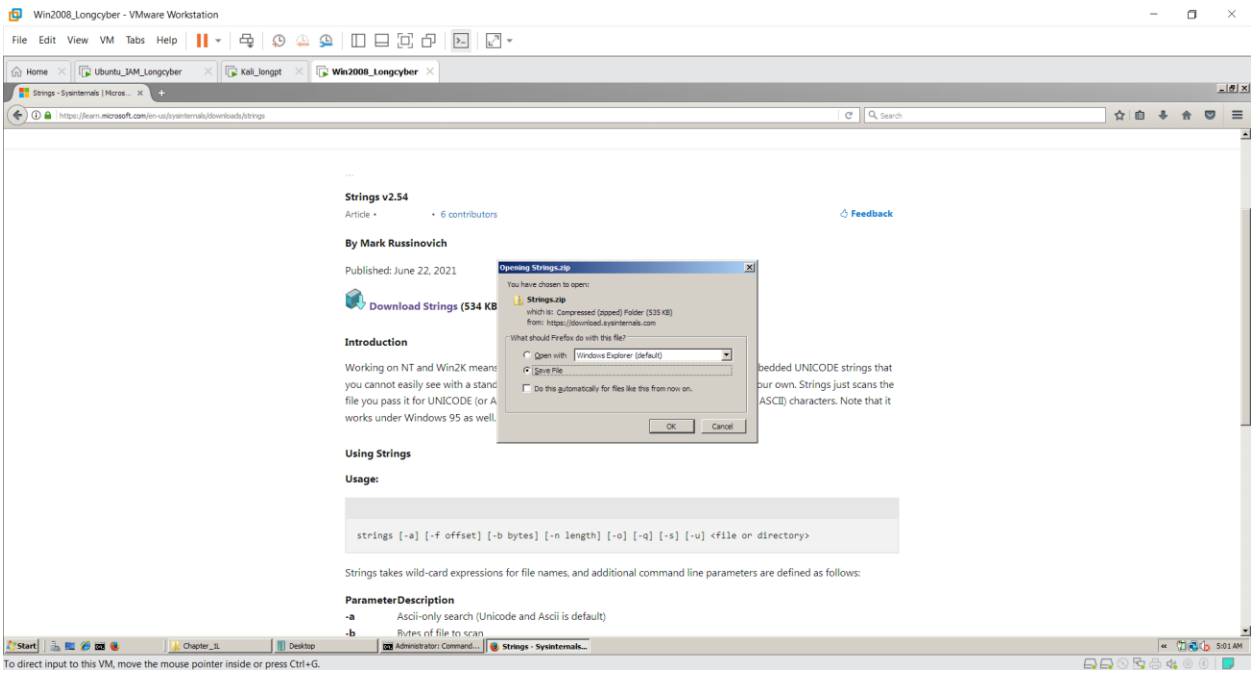
You can download Strings for Windows go here:

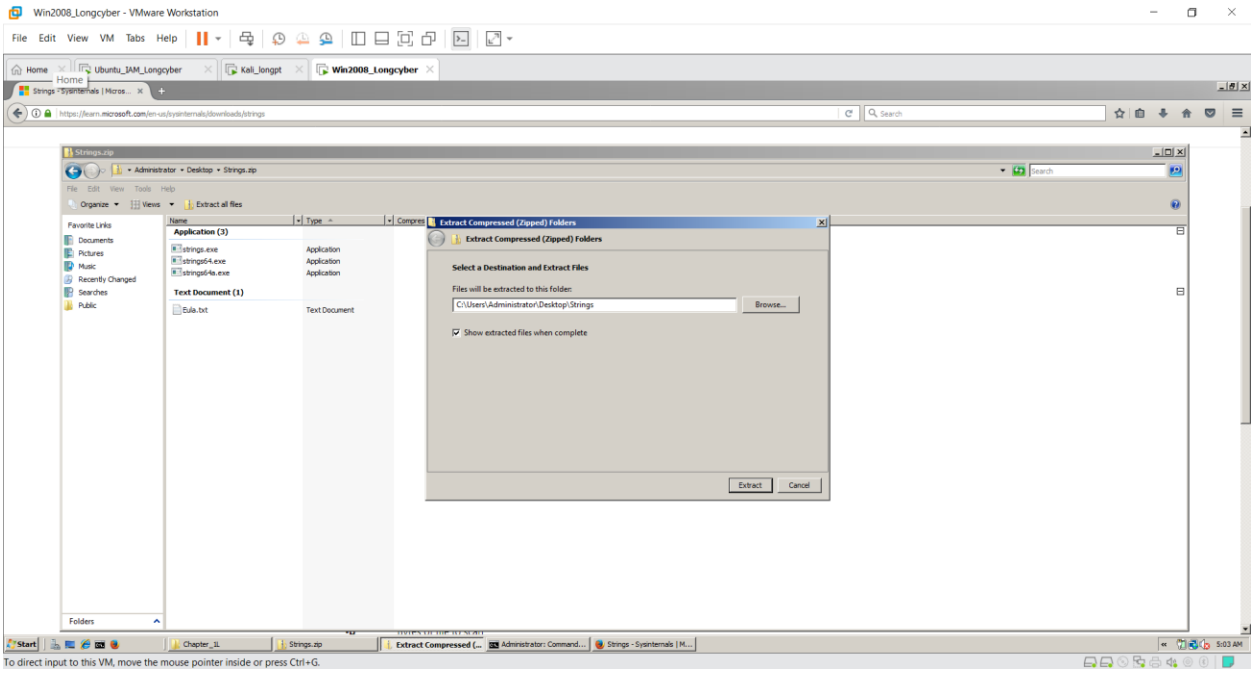
https://technet.microsoft.com/en-us/sysinternals/bb897439

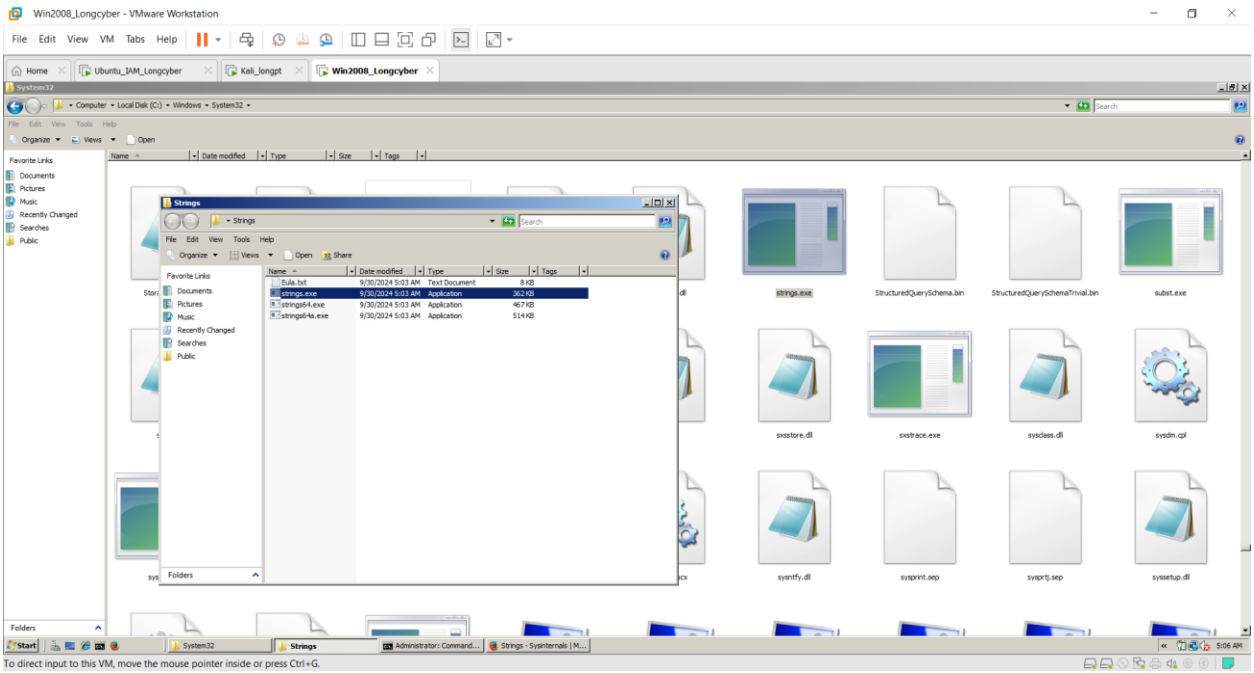
Click the "Download Strings" link.

Save the Strings.zip file on your desktop.

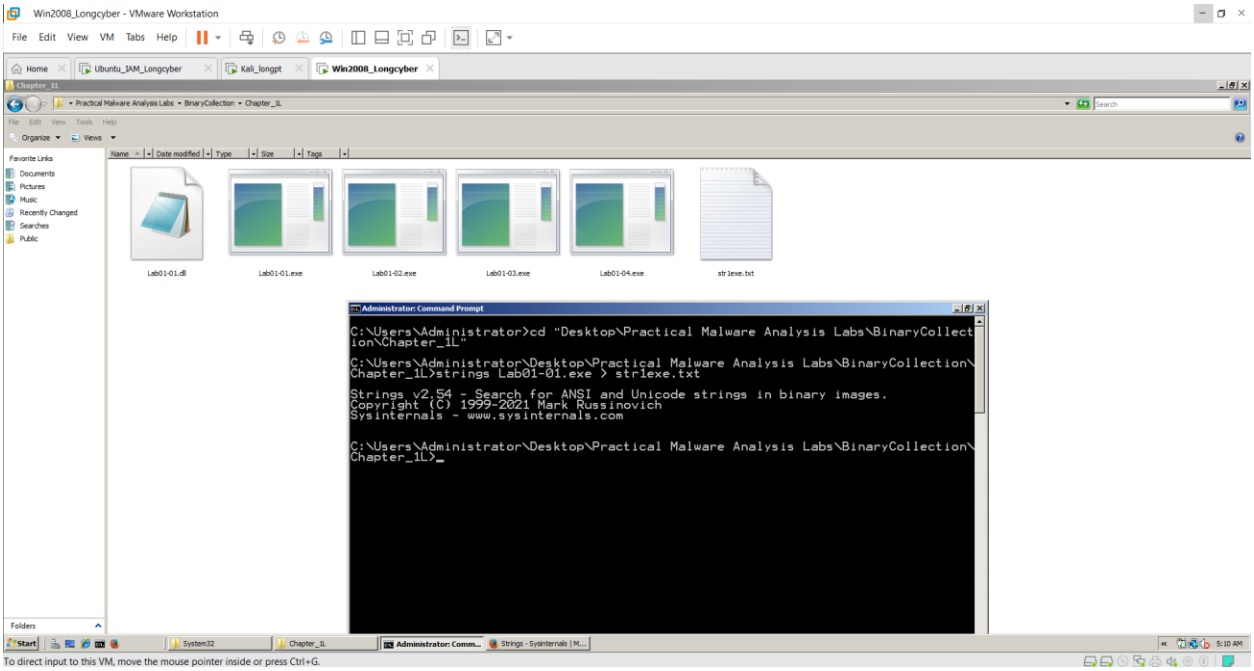
Unzip it, and copy strings.exe to the C:\Windows\System32 folder.





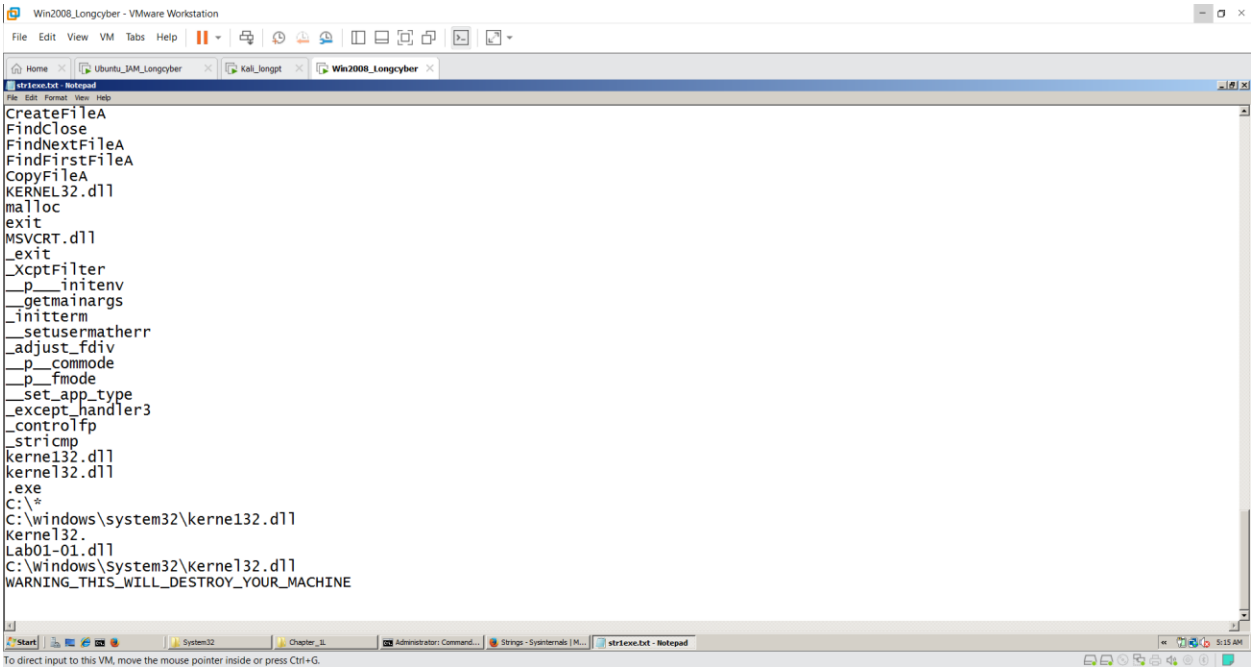


Open a Command Prompt and use the CD command to move to the directory containing your lab files. Then collect the strings from the Lab01-01.exe file. On my machine, Right-click in the **Chapter_1L folder**, and select **Open Command Window Here**.



Notice these items, as shown below:

- "FindNextFileA" and "FindFirstFileA" -- Windows functions to find files
- ".exe" -- suggesting that it will search for EXE files
- "C:\windows\system32\kerne132.dll" -- fake DLL with "kerne132" instead of "kernel32"
- "C:\Windows\System32\Kernel32.dll" -- the real Windows kernel

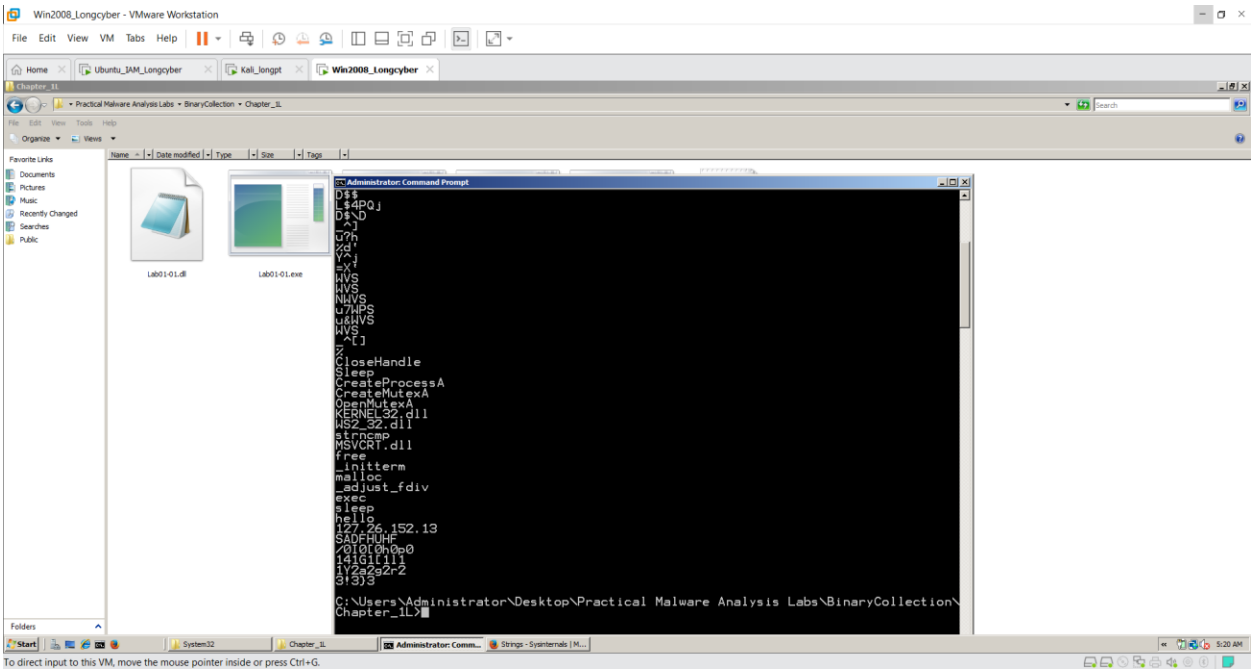


Look at the strings for Lab01-01.dll.

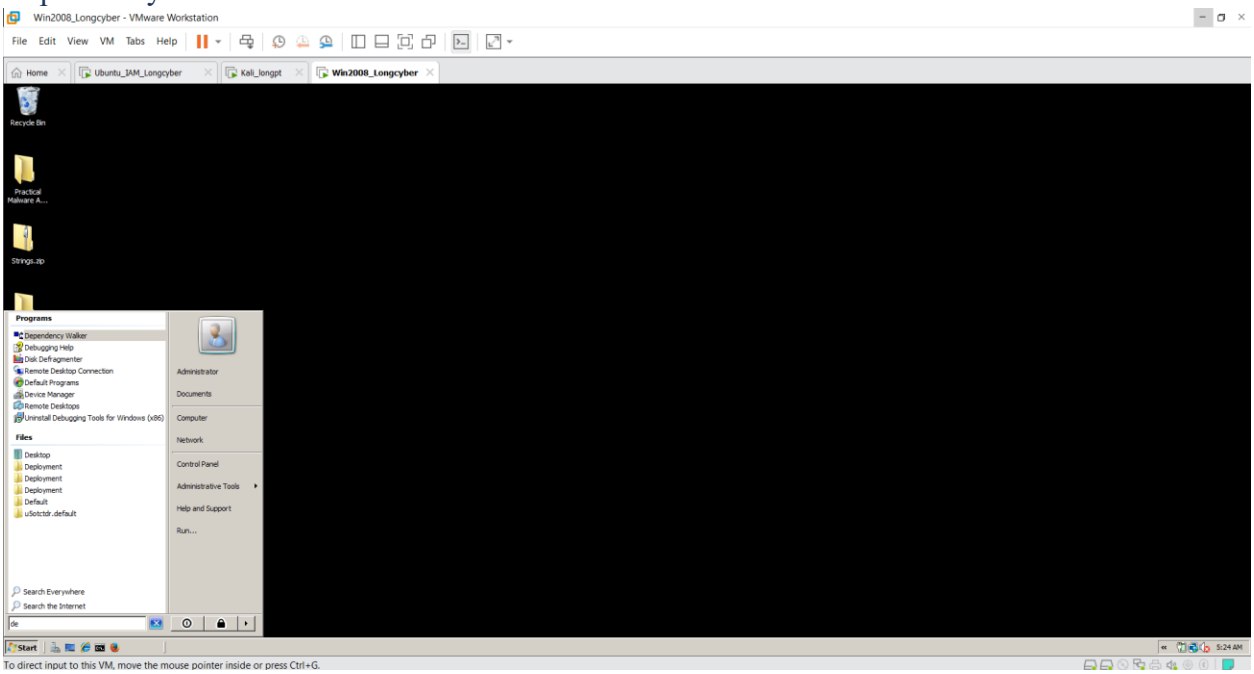
Notice these items, as shown below:

- "exec" and "sleep" -- commands that can be sent over the network to control this backdoor malware
- ".CreateProcessA" -- used to launch a program in response to the "exec" command
- "Sleep" -- used to put the backdoor to sleep in response to the "sleep" command

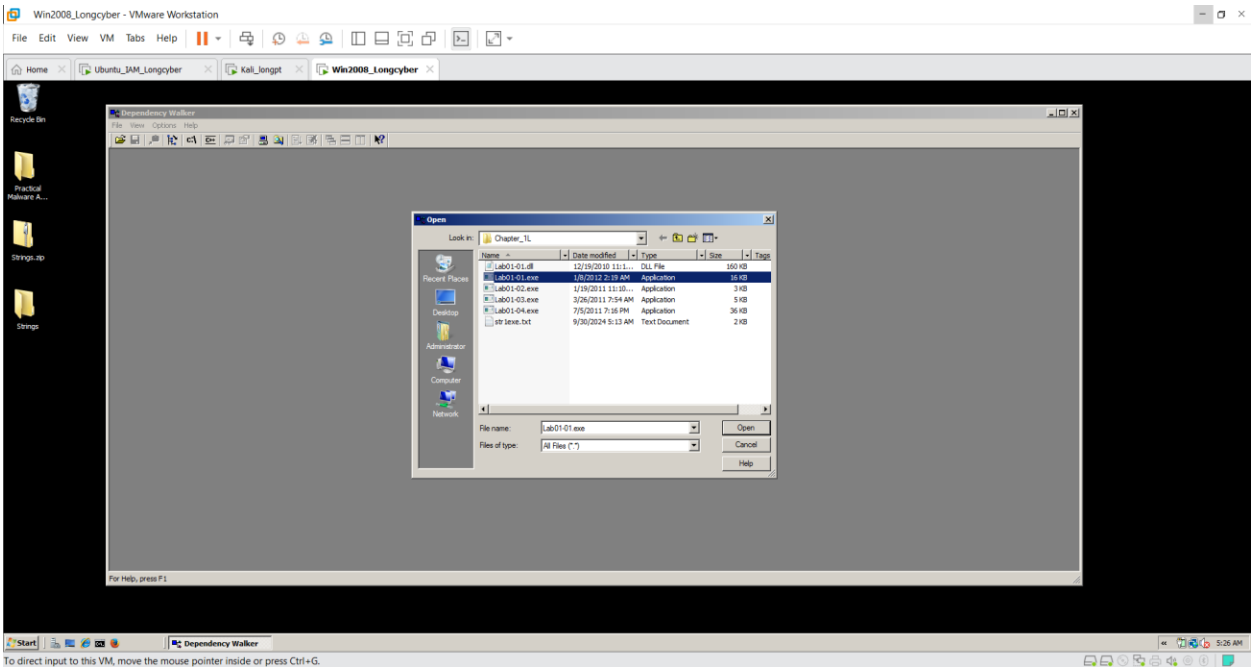
Turn in the image showing your analysis of Lab01-01.dll as shown below. Below "sleep" and "hello" there is an IP address, starting with 127. We will grade it by checking the last digits of the IP address.



Dependency Walker



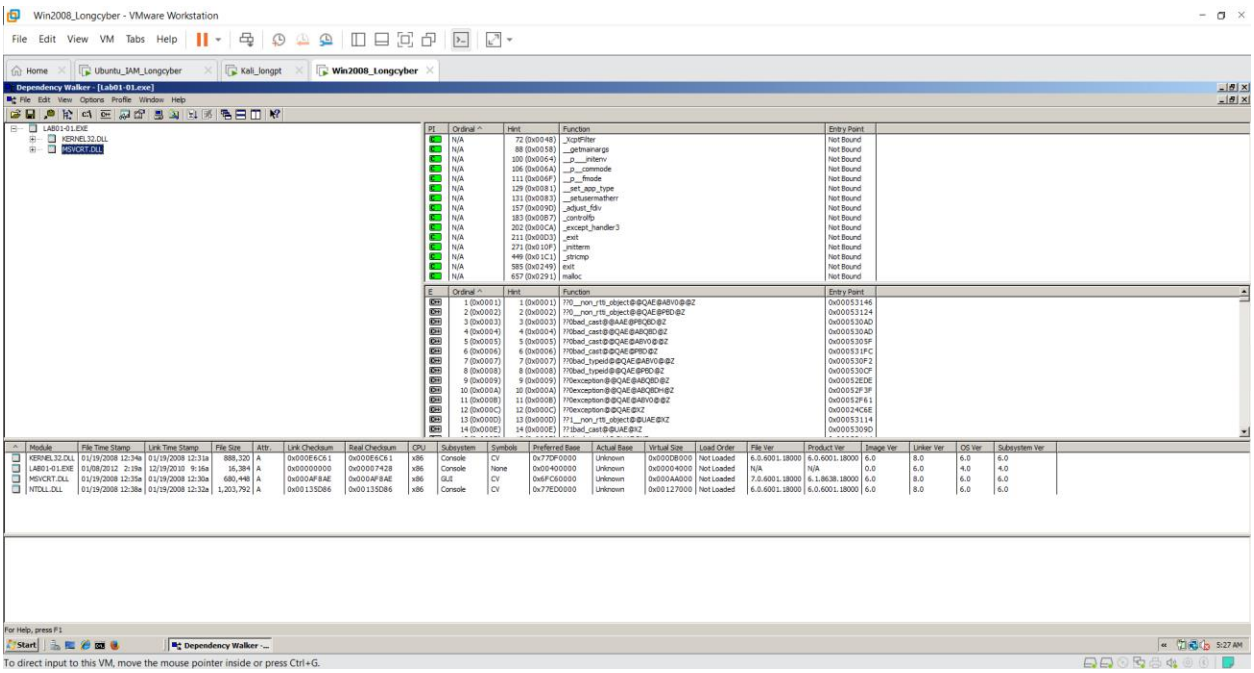
Open Lab01-01.exe in Dependency Walker.



In the left pane, click MSVCRT.DLL as shown below.

There are several imports in the upper right pane, and exports in the middle right pane.

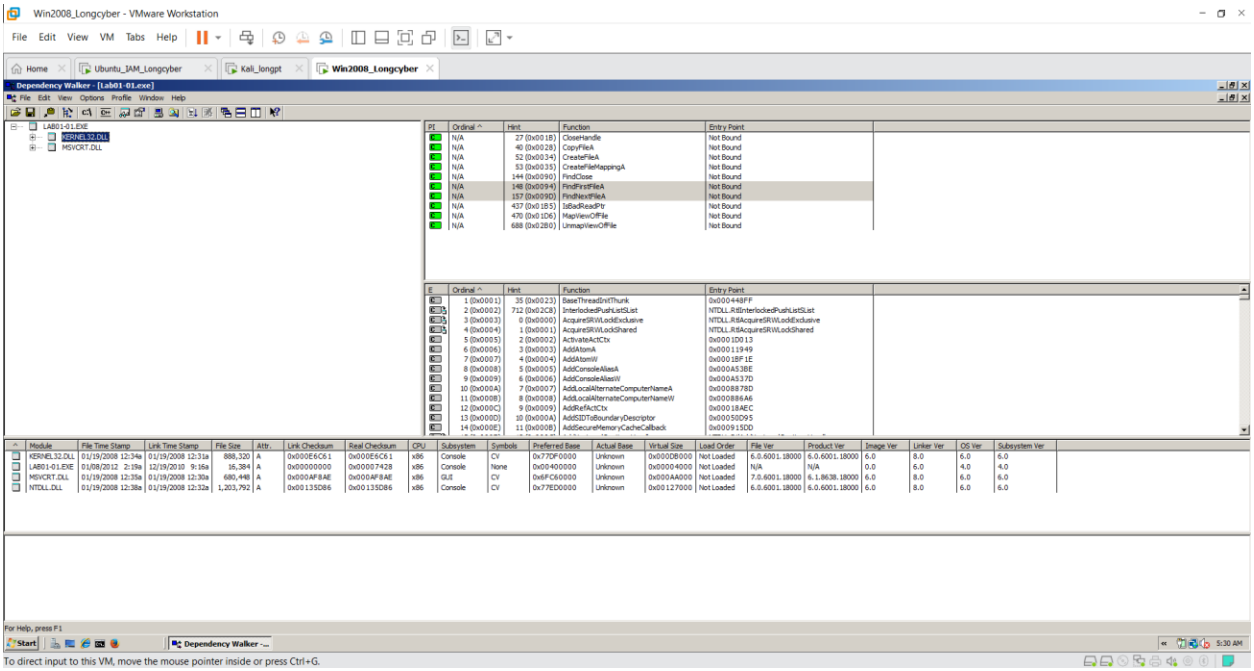
Scan through them--these are normal for any EXE



In the left pane, click KERNEL32.DLL.

Turn in the image showing your analysis of Lab01-01.exe as shown below.

In the "PI^" section (Parent Import), you should see FindNextFileA and FindFirstFileA as shown below.

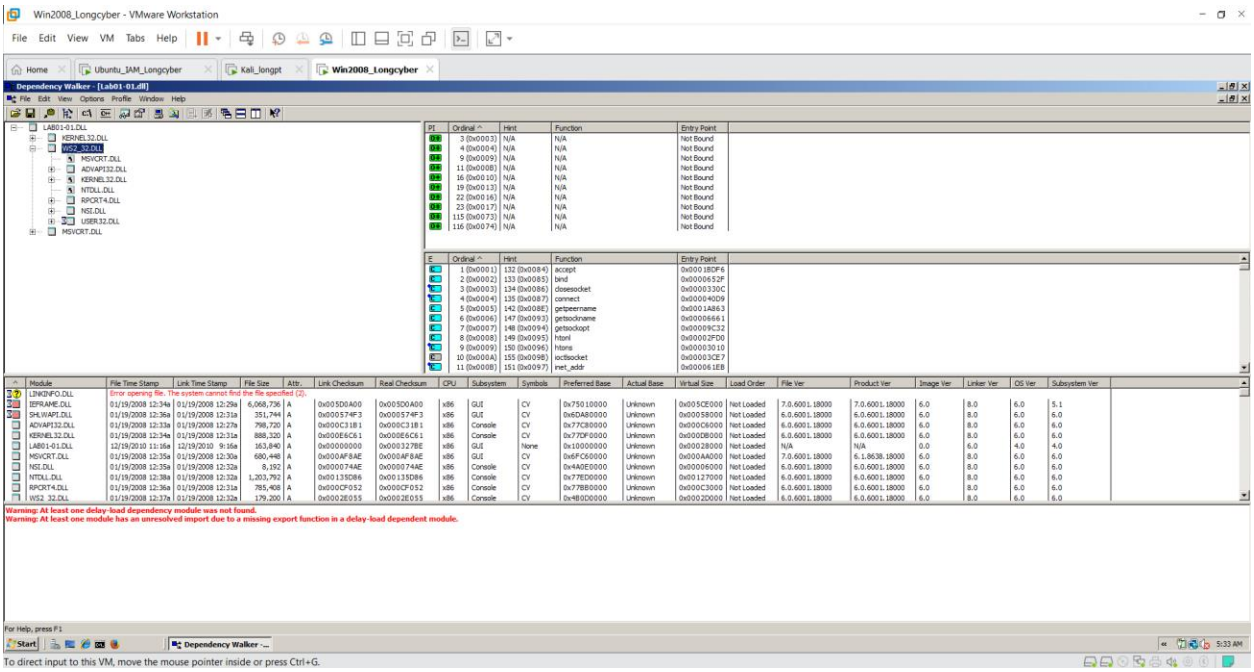


Open Lab01-01.dll in Dependency Walker.

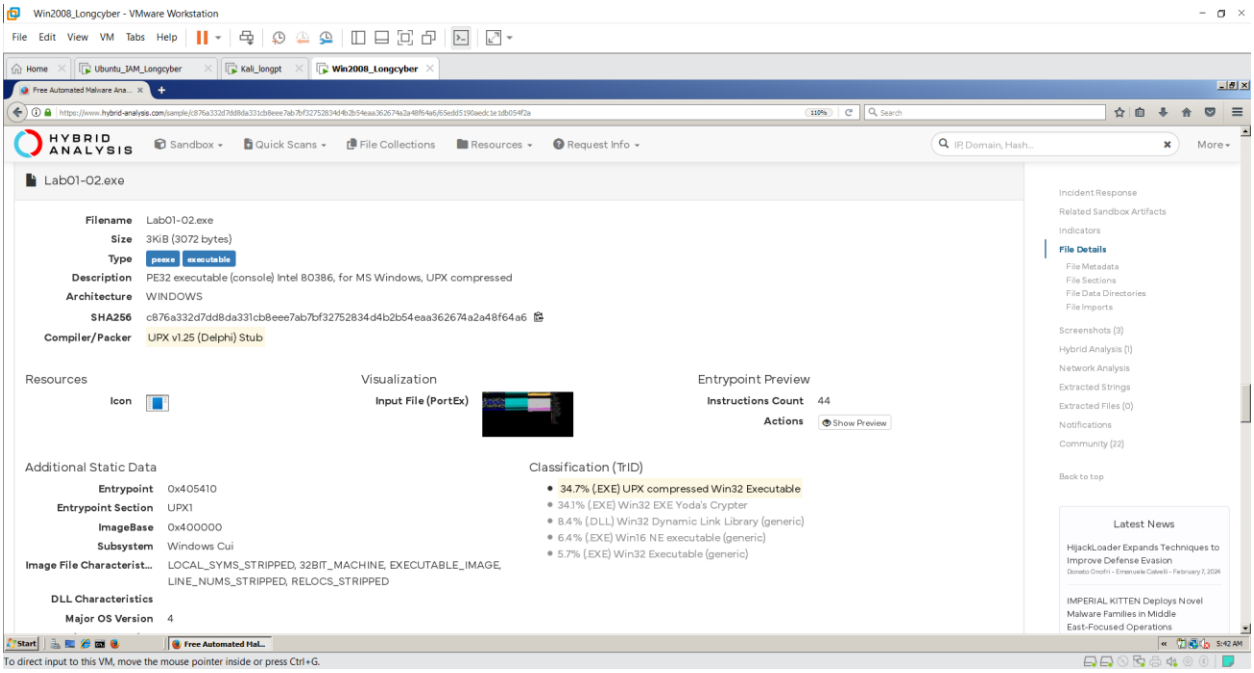
Notice that it imports functions from "WS2_32.DLL".

WS2_32.DLL has networking functions.

The right center pane shows function names that perform networking tasks, such as "bind", "closesocket", and "connect", as shown below.

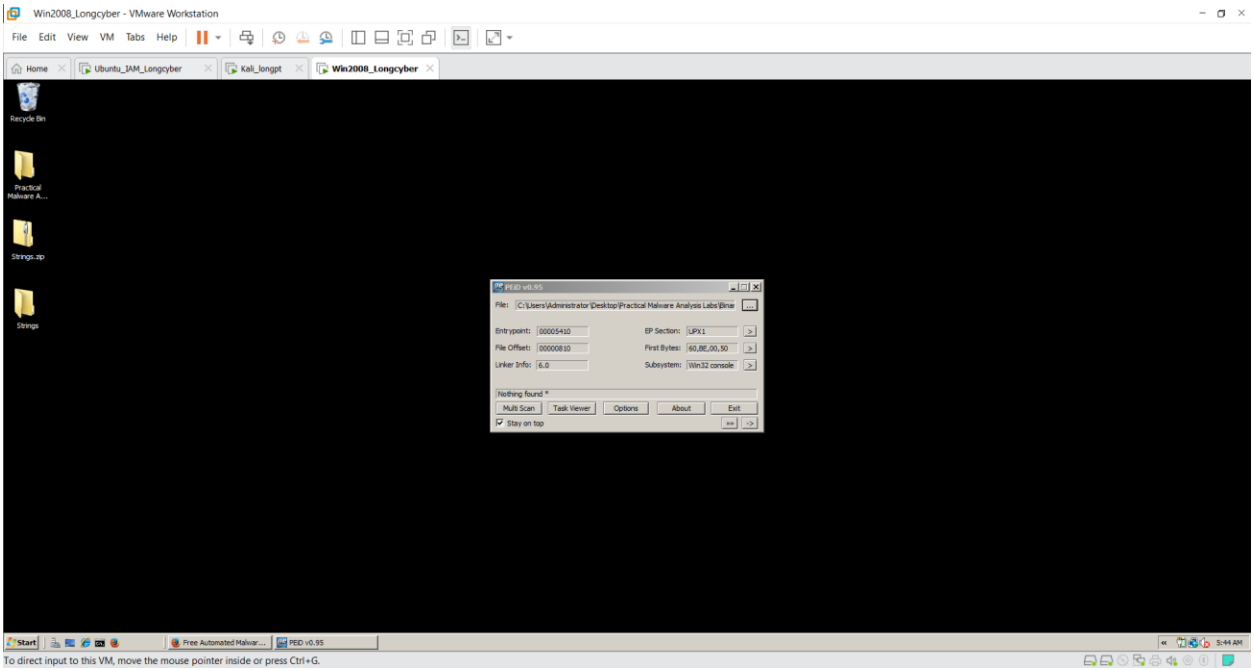


b. Lab01-02.exe



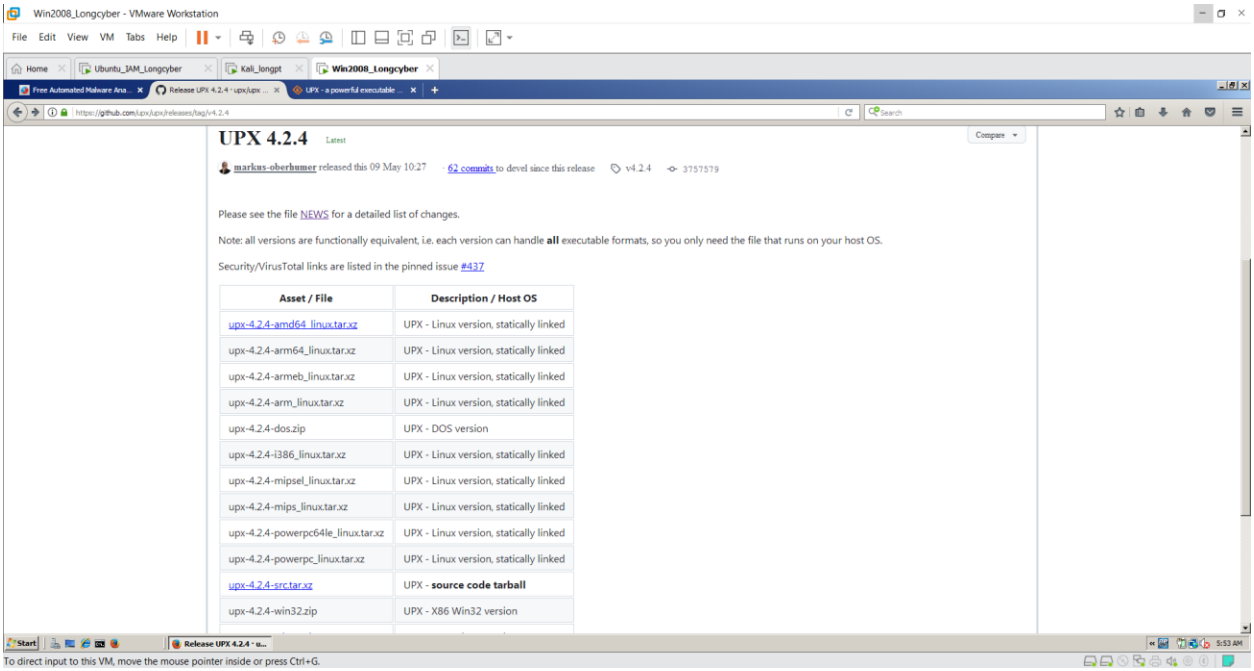
Unpacking the File

Run PEiD on the file. It shows that the file is packed with UPX, as shown in the "EP Section" below.



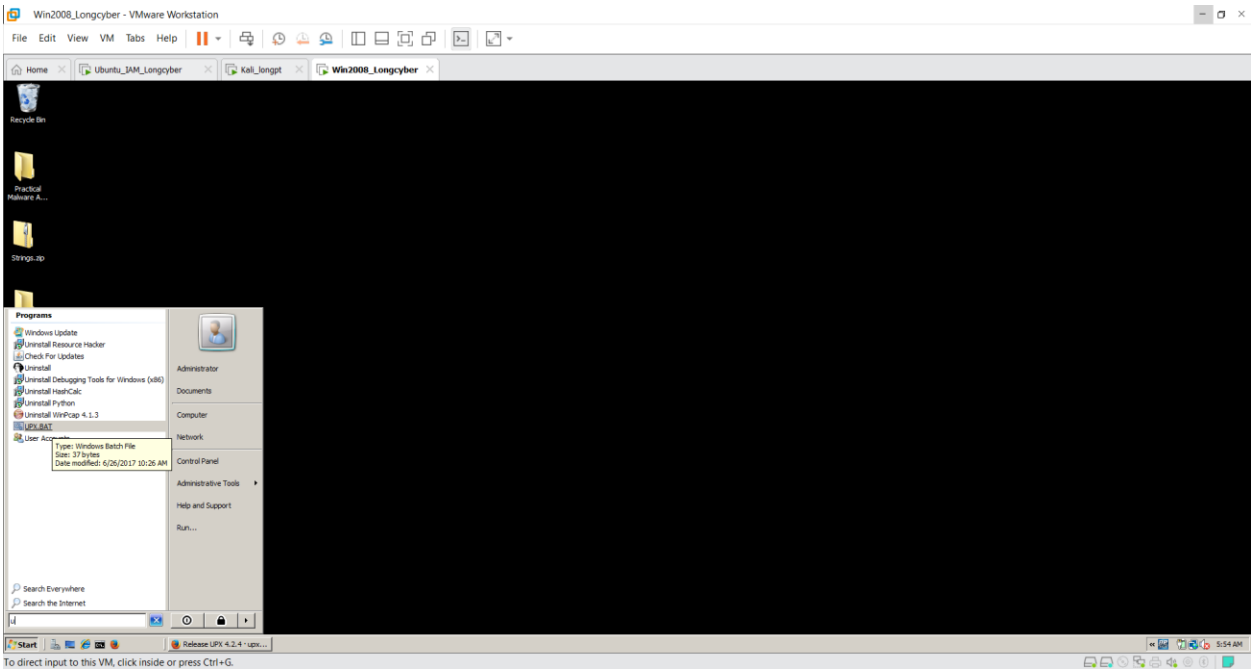
Download the UPX Zip file from here: https://upx.sourceforge.net/

Download the upx391w.zip file, as shown below.



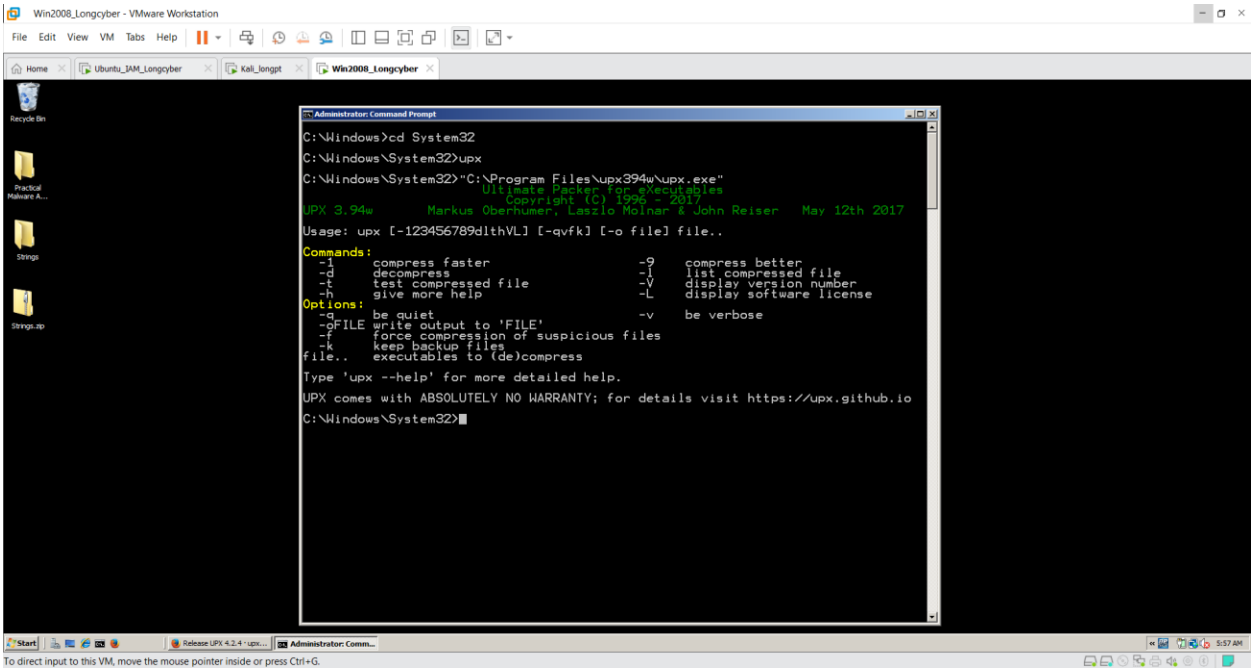
Unzip it and put upx.exe in your C:\Windows\System32 folder.

On server 2008 I have prepared it, we can open it as shown.



Open a Command Prompt window and execute this command: `upx`

You see a UPX help message, as shown below:



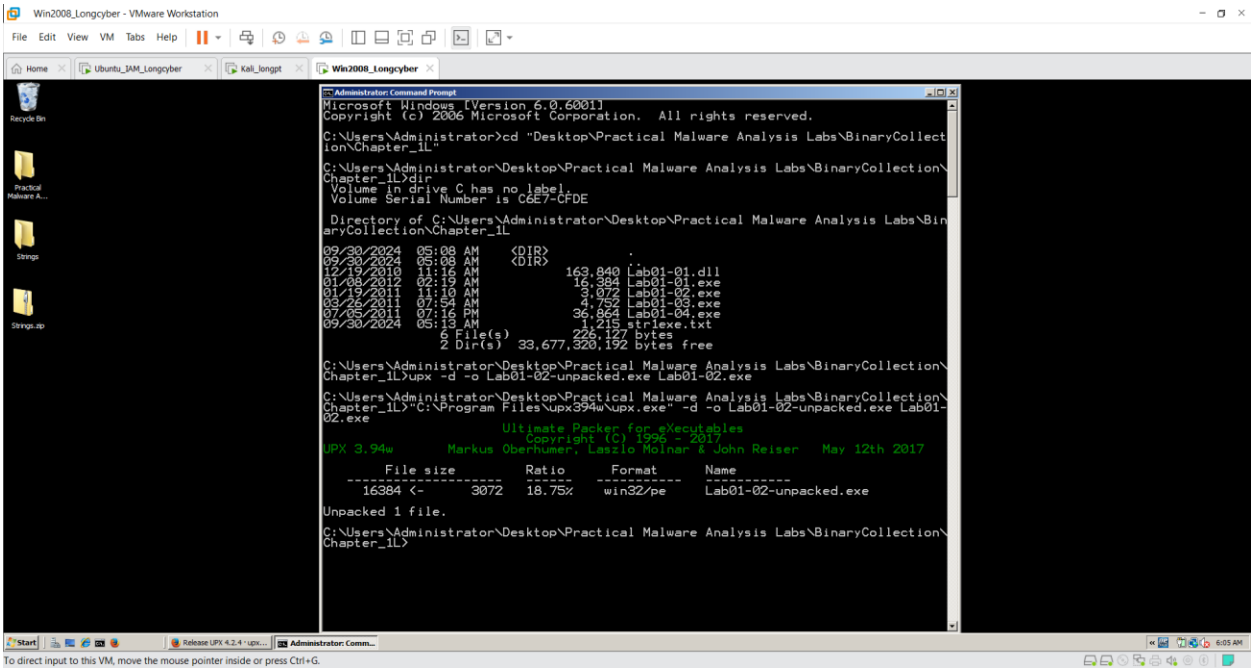
Use the CD command to move to the directory containing your malware samples. On my machine, I used this command:

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

Execute this command to unpack the file:

UPX -d -o Lab01-02-unpacked.exe Lab01-02.exe

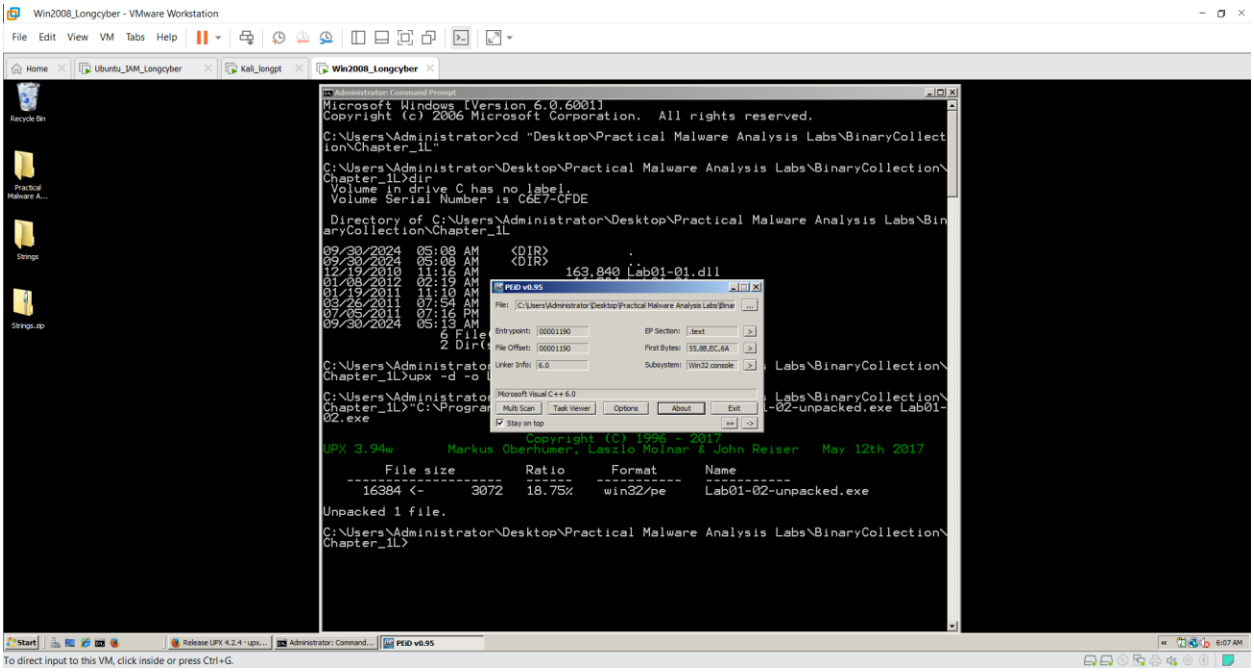
The file unpacks, as shown below:



Analyze the unpacked file with PEiD. It now is regognized as a "Microsoft Visual C++ 6.0" file, as shown below.

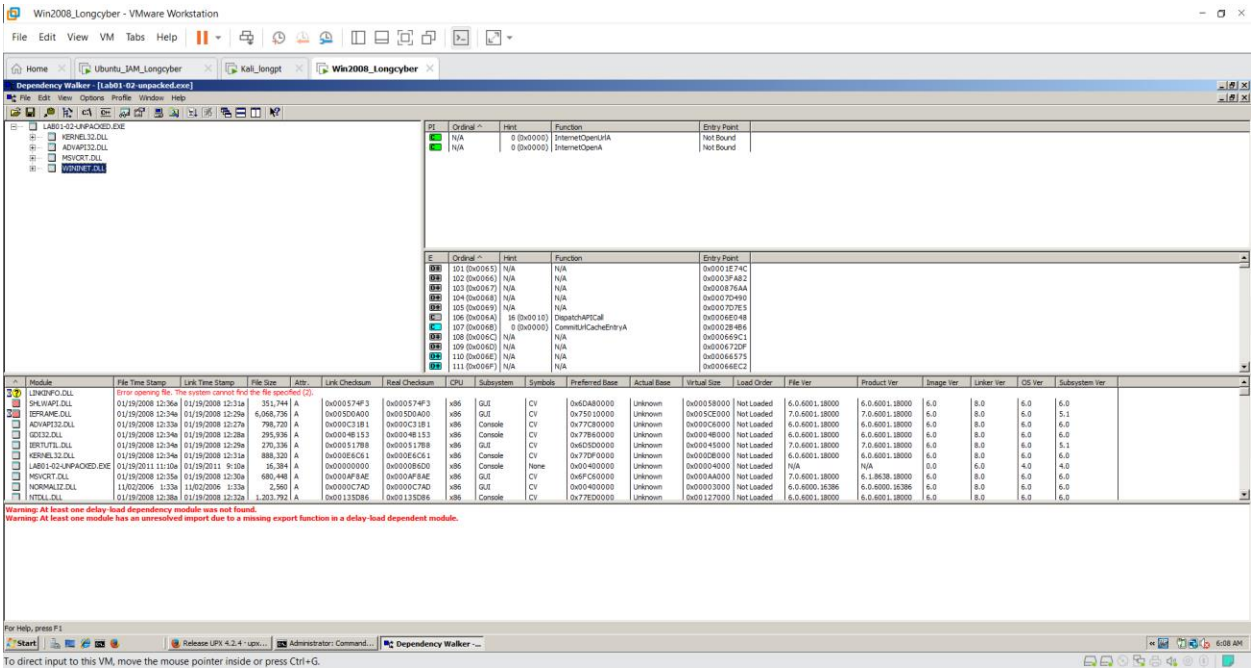
Turn in the image showing your analysis of **Lab01-02-unpacked.exe** as shown below.

We will grade it based on the "First Bytes".



Find the unpacked file's imports with Dependency Walker.

Turn in the image showing the two functions InternetOpenUrlA and InternetOpenA as shown in the upper right pane of the image below:

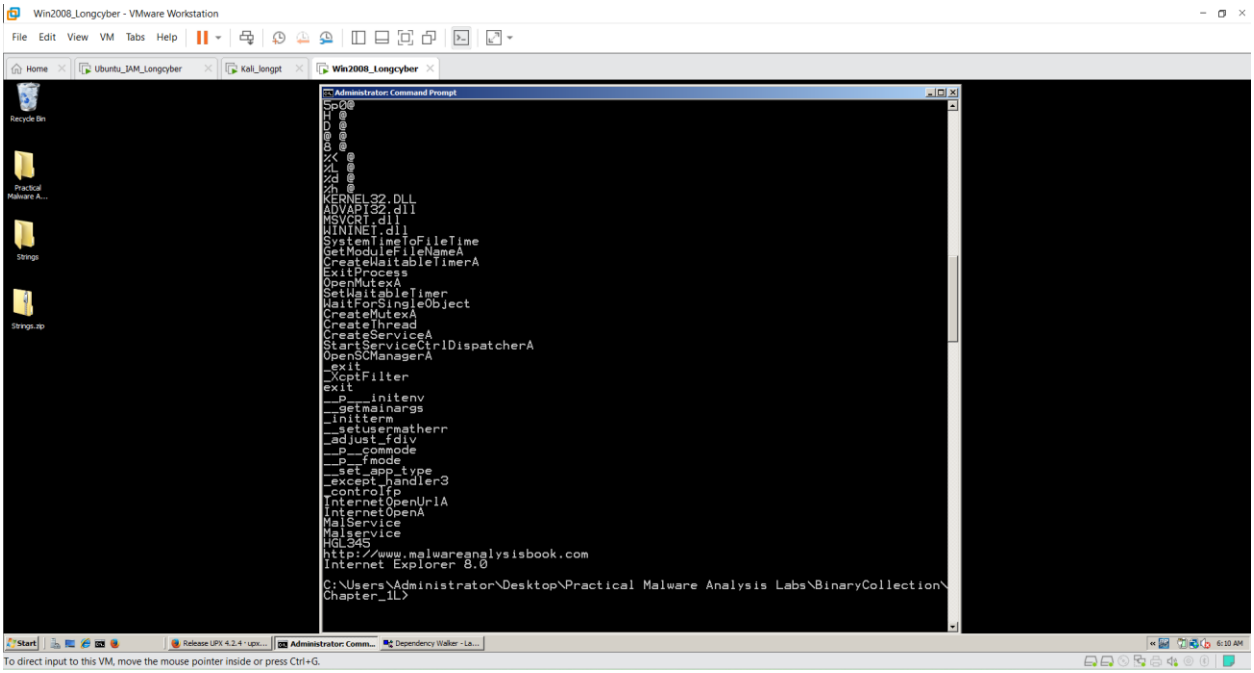


Strings

Find the strings in the unpacked file.

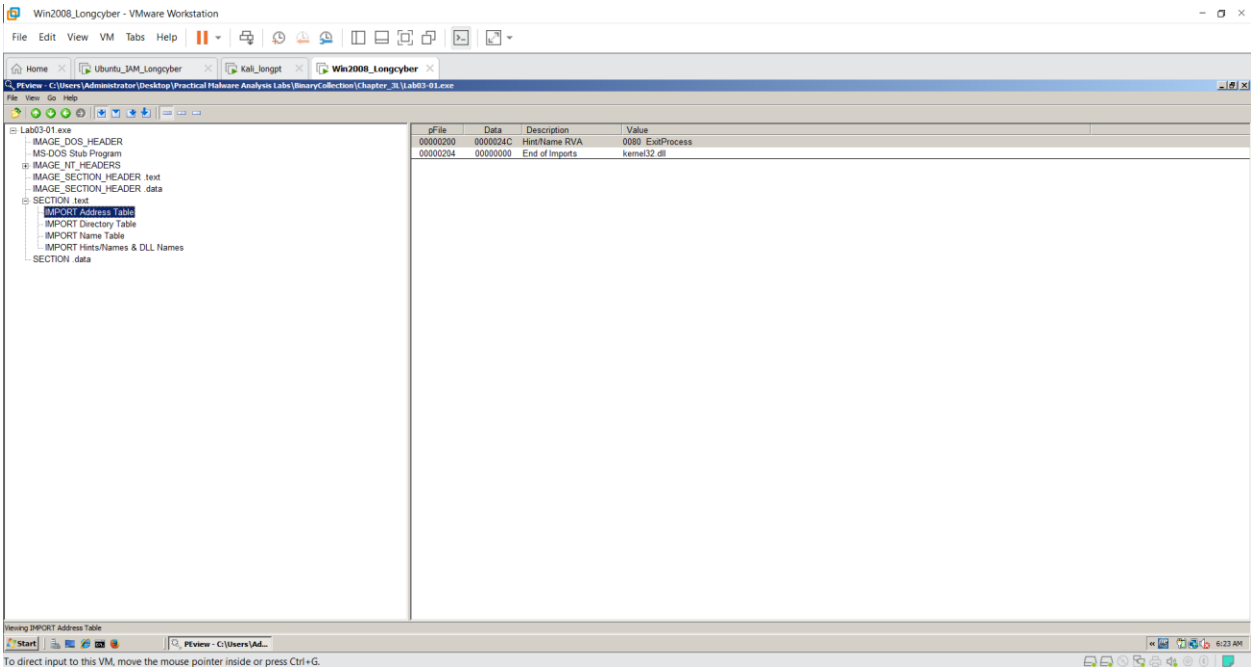
You should see **MalService** and **http://www.malwareanalysisbook.com** as shown below.

These suggest that infected machines will connect to **http://www.malwareanalysisbook.com** and will show a running service named MalService.



2. Basic Dynamic Techniques

Open Lab03-01.exe in PEview. As shown below, the only DLL imported is kernel32.dll, and the only function imported is ExitProcess. That doesn't tell us much--perhaps this malware is packed and the real imports will come at runtime. Turn in the image showing the imports of Lab03-01.exe as shown below.



Using Strings

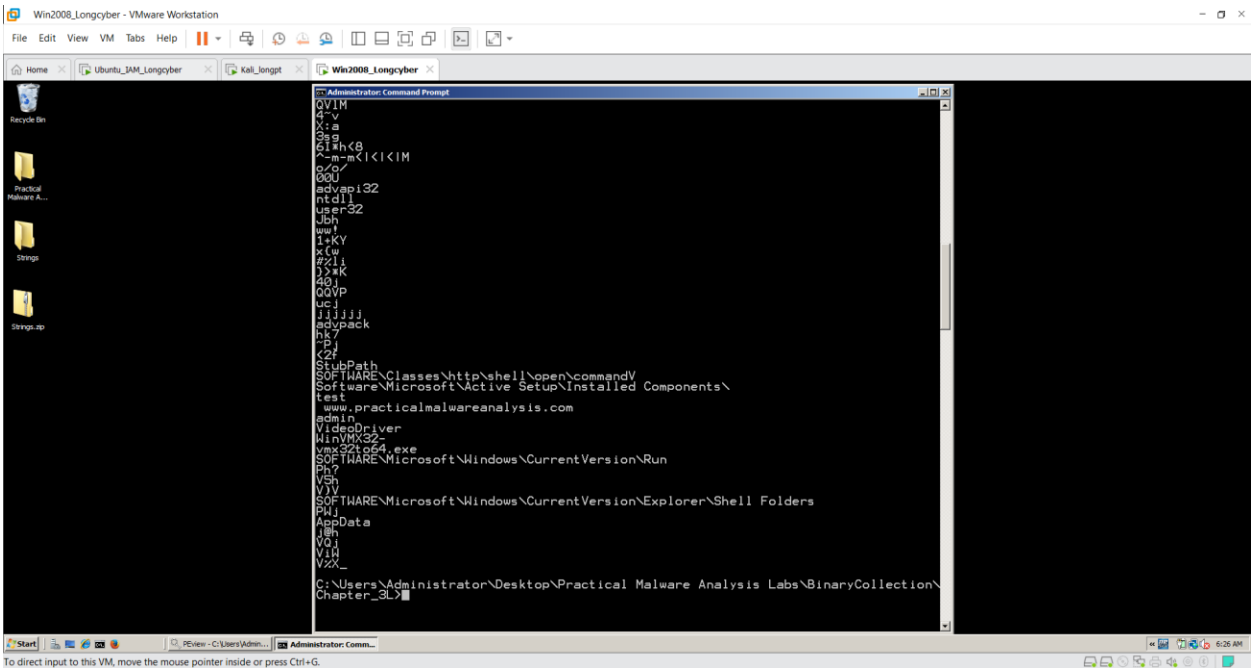
Examine the strings in **Lab03-01.exe** and find these items, as shown below.

SOFTWARE\Classes\http\shell\open\commandV -- A registry location

www.practicalmalwareanalysis.com -- a URL

VideoDriver

These readable strings are surprising--if the malware were packed, the strings would not be readable.



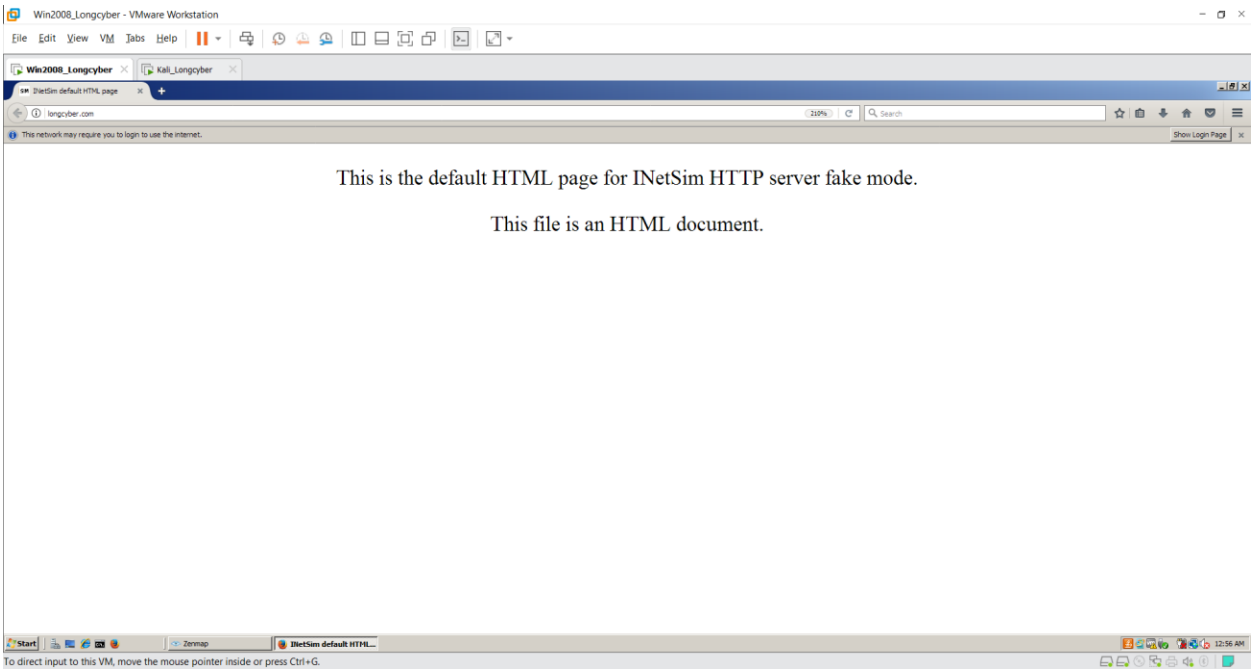
Preparing for Dynamic Analysis

Dynamic analysis will help us to understand this malware better.

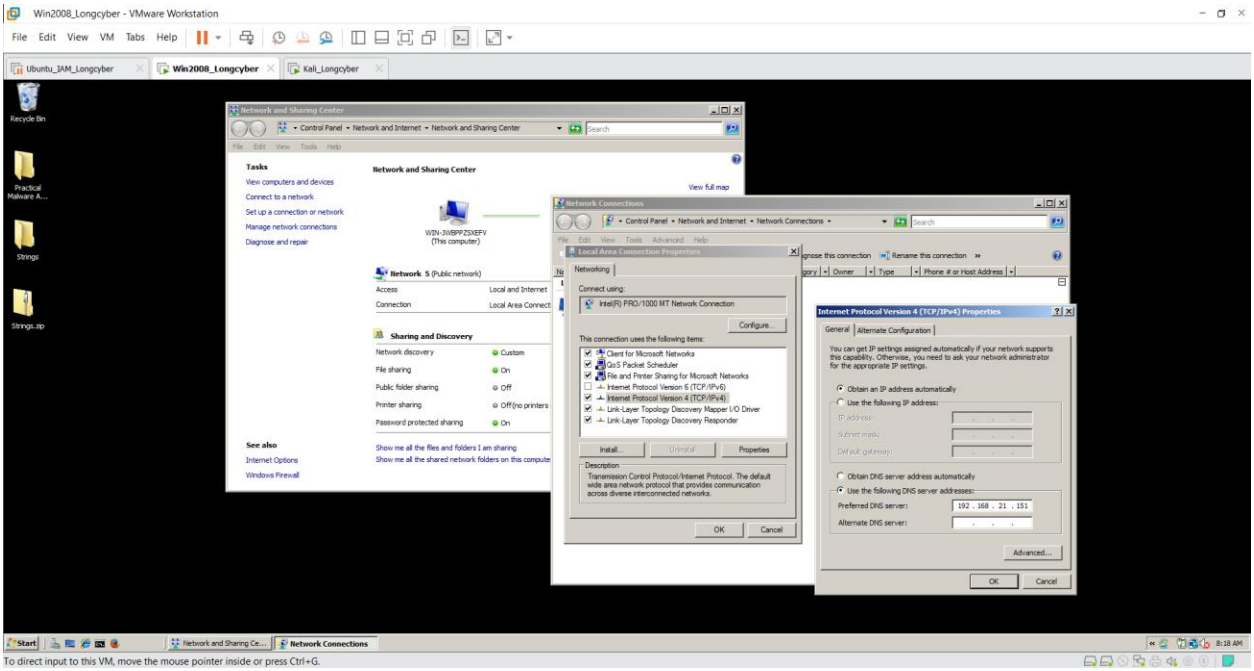
Here is the process detailed below:

1. Set up INetSim to simulate the Internet
2. Setting the DNS Server
3. Run Process Explorer
4. Run Wireshark
5. Run Process Monitor

1. **Start INetSim**
   Start both the Windows and Linux VMs.
   In Linux, start inetsim, as you did in the previous project.
   Set the Windows DNS server to the Linux machine's IP address, as you did in the previous project.
   Test it by opening a Web browser to this URL: YOURNAME.com
   You should see the "INetSIM HTTP server" page, as shown below:

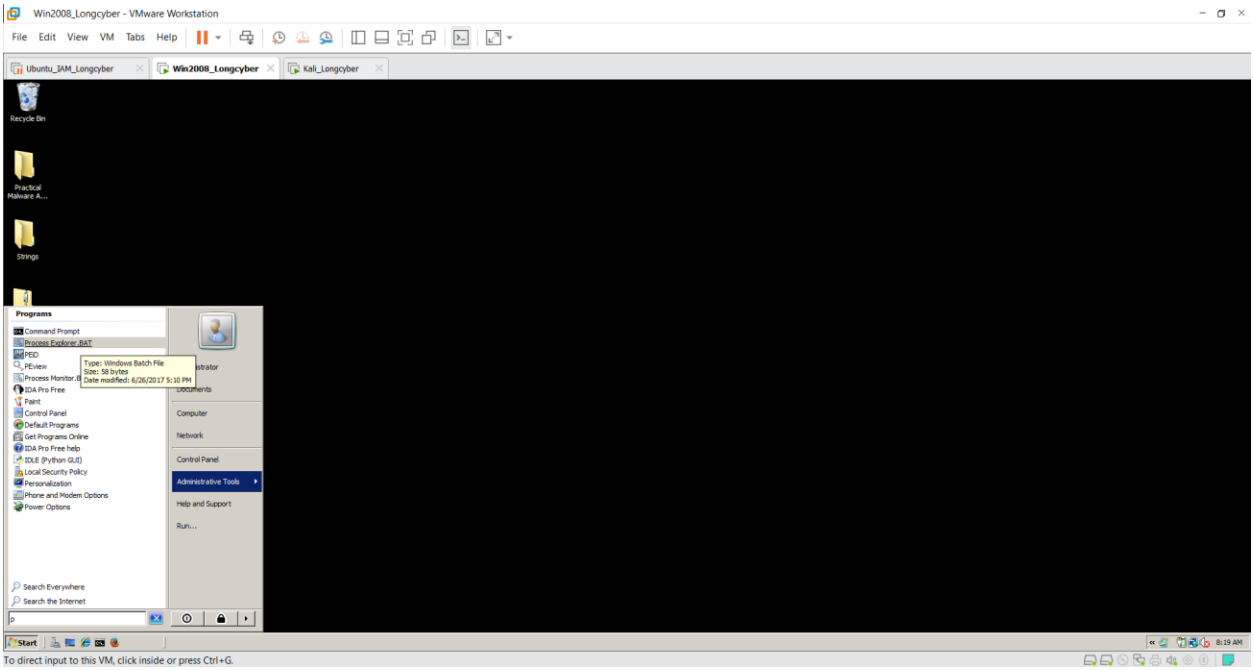


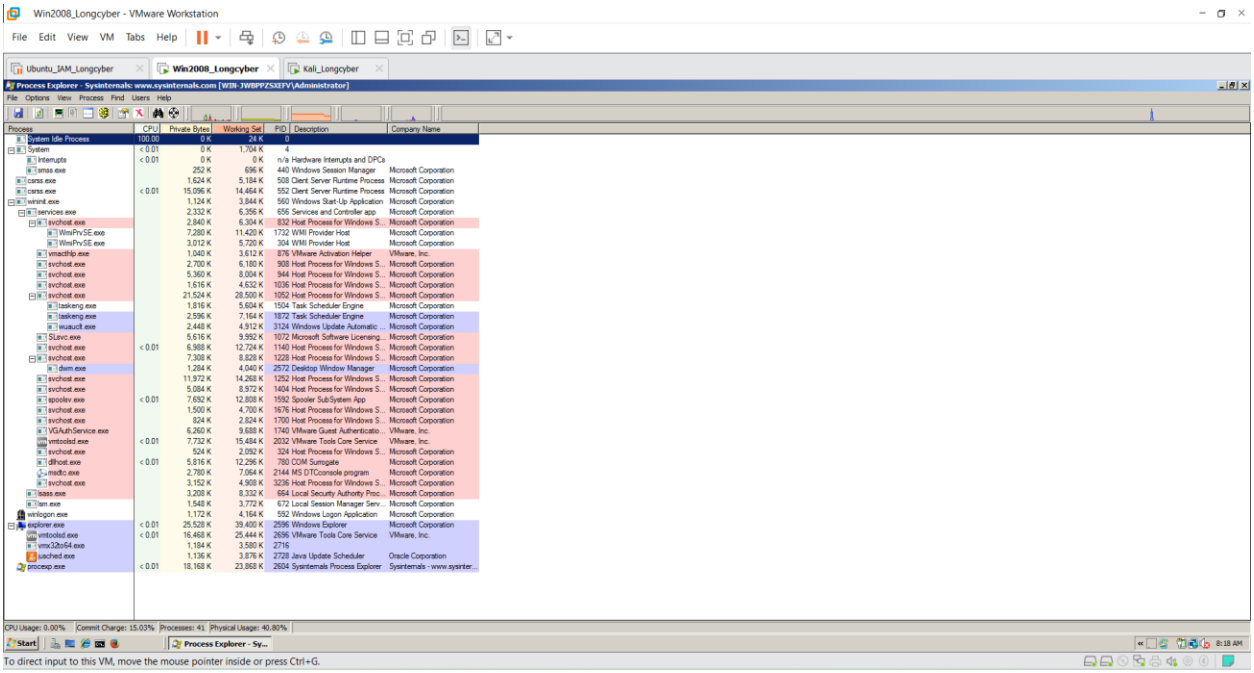
2. **Setting the DNS Server**
   On your Windows VM, in Control Panel, open "Network Connections". Right-click "Local Area Connection" and click Properties.
   Double-click "Internet Protocol (TCP/IP)".
   Set your DNS server to the Kali Linux machine's IP address, as show below:



3. Run Process Explorer

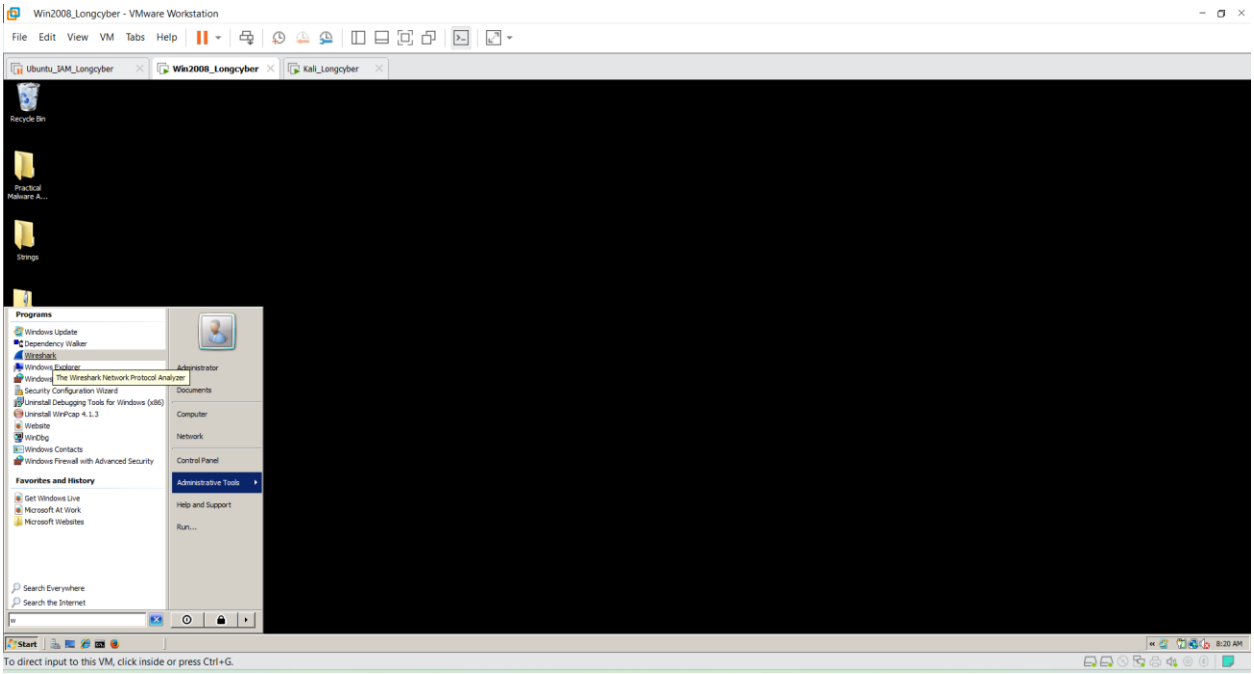
Open Process Explorer, as shown below:

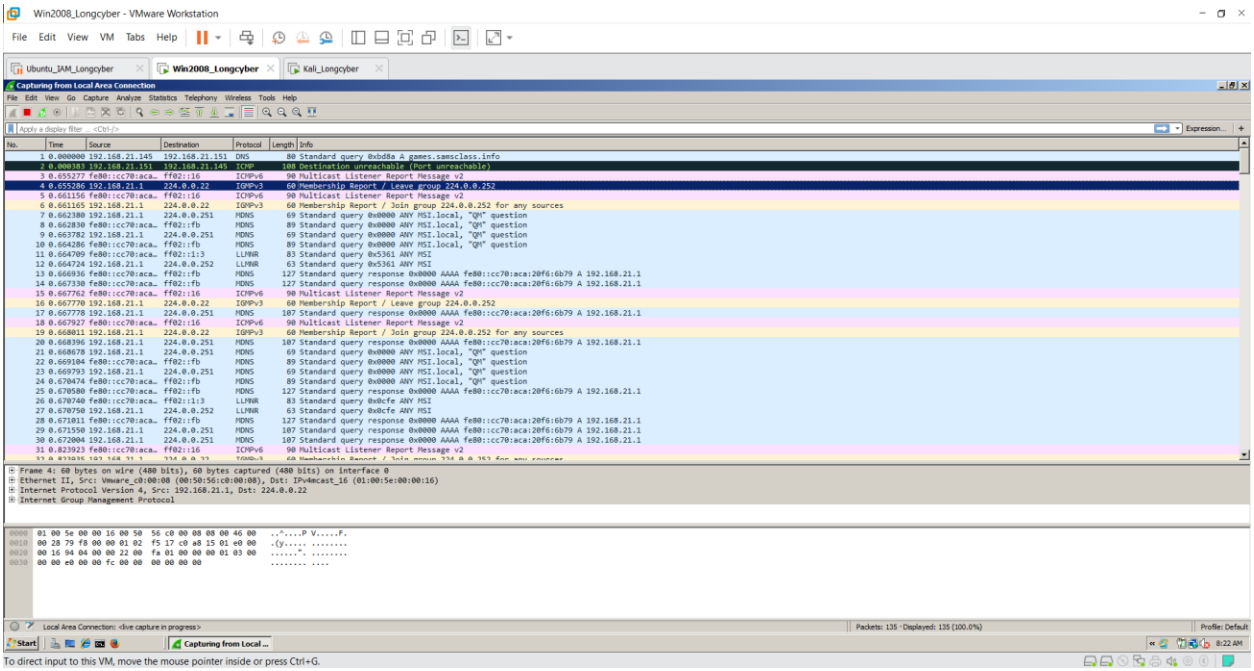




4. **Run Wireshark**

   Start Wireshark and begin capturing packets from the interface that goes to the Linux machine, which is normally "Local Area Connection".





5. **Start Process Monitor**

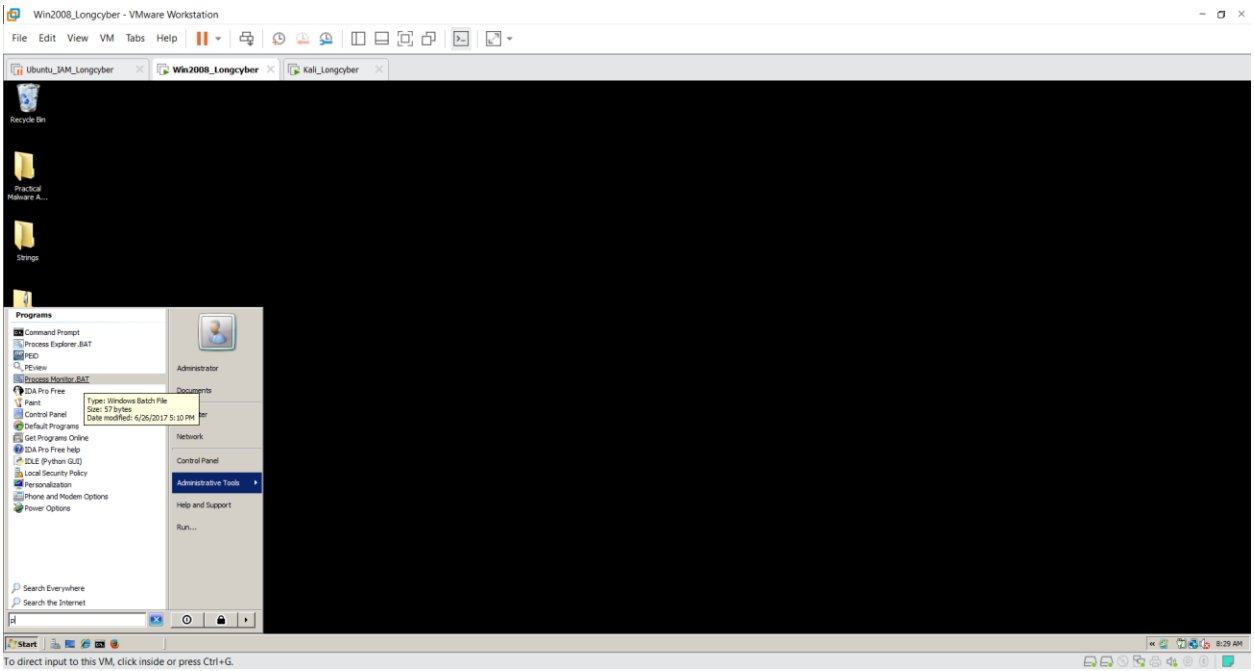
   It's best to start Process Monitor last, so you can exclude all the harmless processes the other tools are using.

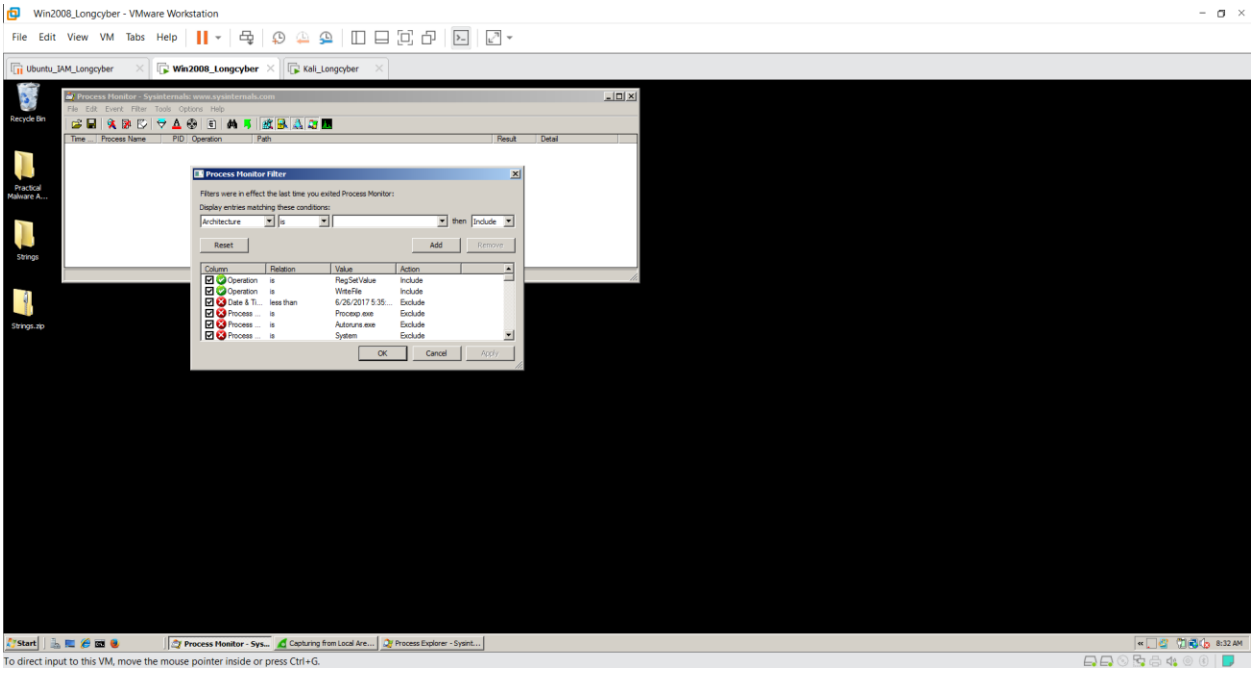
   In the folder you unzipped Process Monitor into, double-click **Procmon.exe.**

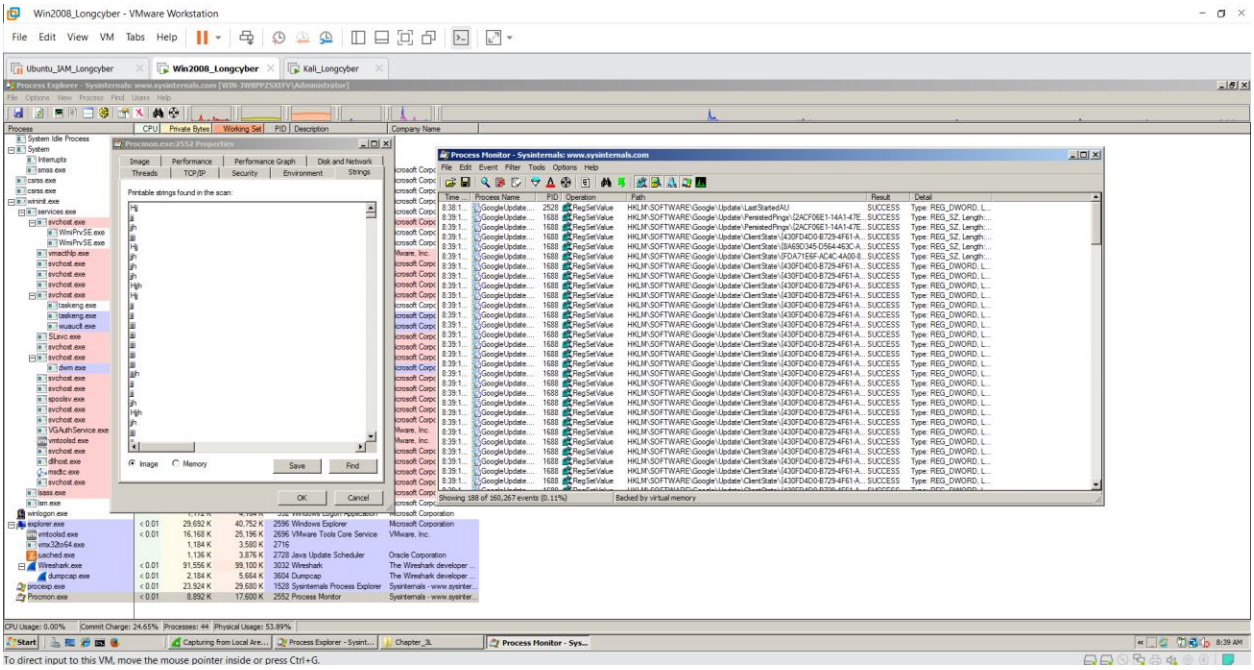
   If a Security Warning box pops up, allow the software to run.

   Agree to the license.

   You should see Process Monitor, with a lot of processes visible, as shown below:



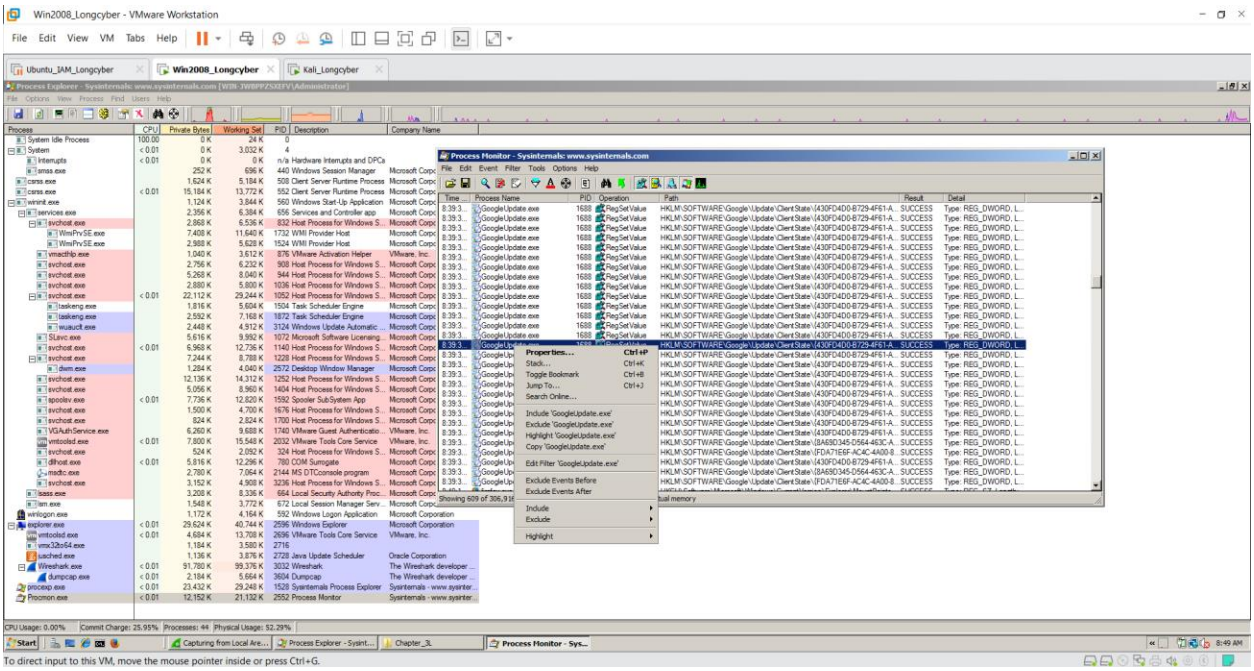


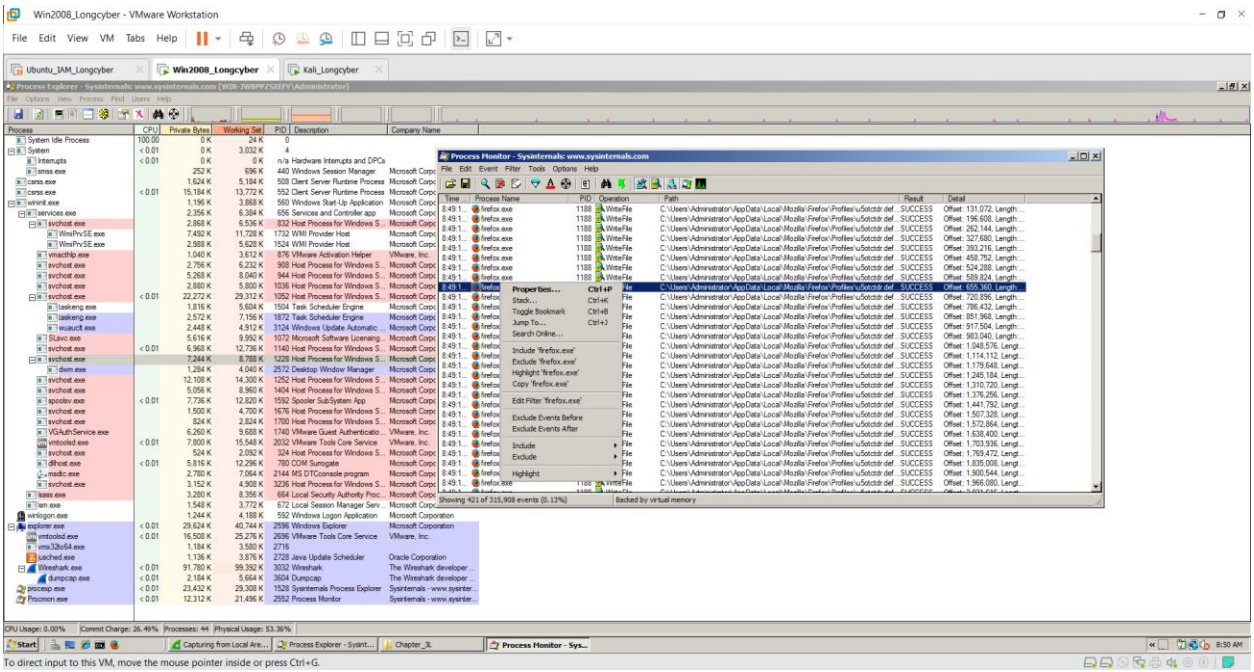


Excluding Harmless Processes

To make the analysis easier, we will ignore all the processes that are already running before the malware starts.

In Process Monitor, right-click the name of one of the visible processes, such as lsass, and click **"exclude 'lsass.exe'"**, as shown below:



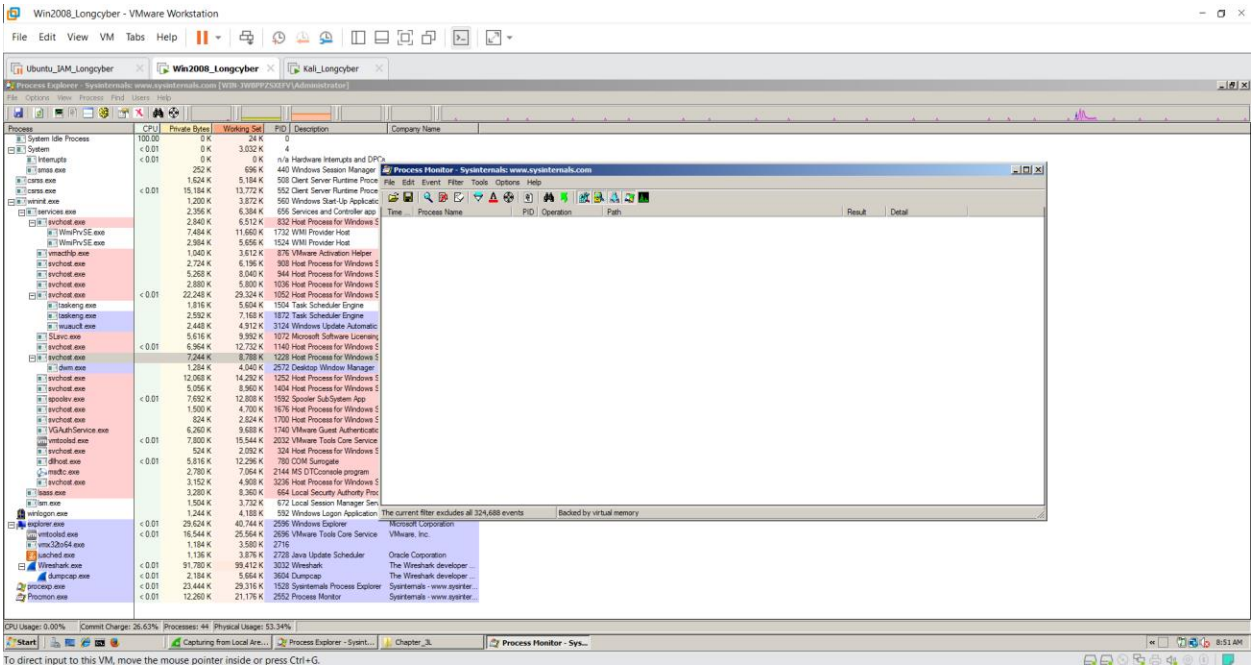


Wait while the event filter is applied.

Right-click a remaining process, such as "svchost.exe" and exclude it too.

Repeat the process until all current processes are hidden, as shown below. When I did it, the remaining processes to exclude were csrss.exe, explorer.exe, services.exe,vmtoolsd.exe, iexplore.exe, VMwareTray.exe, verclsid.exe, winlogon.exe, wmiprvse.exe, wuauclt.exe, regshot.exe, spoolsv.exe,

alg.exe, rundll.exe, WMIADAP.EXE, GoogleUpdate.exe, GoogleCrashHandler.exe, chromeinstaller.exe, and setup.exe.



Run the Lab03-01.exe File

Now double-click the Lab03-01.exe File.

Viewing the Running Malware in Process Explorer

In Process Explorer, in the top pane, find **Lab03-01.exe** and click it.

Troubleshooting

If the Lab03-01.exe process does not appear in Process Explorer, that probably means that the malware has already been run on this VM.

To make the malware run properly again, restart the VM, press F8, enter Safe Mode, and delete this file: C:\Windows\System32\vmx32to64.exe

Then restart the VM in normal mode.

In Process Explorer, click **View, "Lower Pane View", Handles.**

You see the **WinVMX32** mutant, as highlighted below. A mutant, also called a mutex, is used for interprocess connunication. A wonderful explantion of mutexes in terms of rubber chickens is here.