

Lab 8

Configuring a Malware Lab

Course Name: IAM302

Student Name: Phạm Thành Long

Instructor Name: Mai Hoàng Đinh

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.

The screenshot shows a VMware Workstation window titled "Win2008_Longcyber - VMware Workstation". Inside, there's a browser tab for "Ubuntu_IAM_Longcyber" and another for "Kali_Longcyber". The main content is the Hybrid Analysis web interface. On the left, a "File Upload" dialog box is open, showing a list of files including "Lab01-01.dll" and several ".exe" files. The main area displays the Hybrid Analysis logo and a brief description: "This is a free malware analysis service for the community that detects and analyzes unknown threats using a unique Hybrid Analysis technology." Below this is a "Drag & Drop For Instant Analysis" field and an "or" link followed by a URL input field "http://www.example.com/suspicious.zip" and an "Analyze" button. To the right, there are sections for "Releases & Updates" (YARA Hunting Available on Hybrid Analysis!, June 14, 2018) and "Latest News" (HijackLoader Expands Techniques to Improve Defense Evasion, Donato D'Onofrio - Emerging Cyber - February 7, 2024; IMPERIAL KITTEN Deploys Novel Malware Families in Middle East-Focused Operations, Counter Adversary Operations - November 9, 2023). At the bottom, a note says "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

Sandbox Quick Scans File Collections Resources Request Info

Analysis Environments

Name Lab01-01.dll
Size 160.0KB
Type **PE32 executable**
MIME application/x-dosexec
SHA256 f50e42cd8faeb6_93058260@2dus

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.

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!
June 19, 2024

Refreshed and Optimized Overview Page June 19, 2024 See More!

Latest News

HijackLoader Expands Techniques to Improve Defense Evasion
Dennis Drotin - Enterprise Geek - February 7, 2024

IMPERIAL KITTEN Deploys Novel Malware Families in Middle East-Focused Operations
Counter Adversary Operations - November 9, 2023

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

Sandbox Quick Scans File Collections Resources Request Info

HYBRID ANALYSIS

Search through 1.1B+ Indicators of Compromise (IOCs).

File/URL File Collection Report Search YARA Search

String Search

Search for: e930b86c2a599e8db83b8260393082268f2dba

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!
June 19, 2024

Refreshed and Optimized Overview Page June 19, 2024 See More!

Latest News

HijackLoader Expands Techniques to Improve Defense Evasion
Dennis Drotin - Enterprise Geek - February 7, 2024

IMPERIAL KITTEN Deploys Novel Malware Families in Middle East-Focused Operations
Counter Adversary Operations - November 9, 2023

New Container Exploit Rooting Non-Root Containers with CVE-2023-2640 and CVE-2023-32629, aka GameOver[lay]

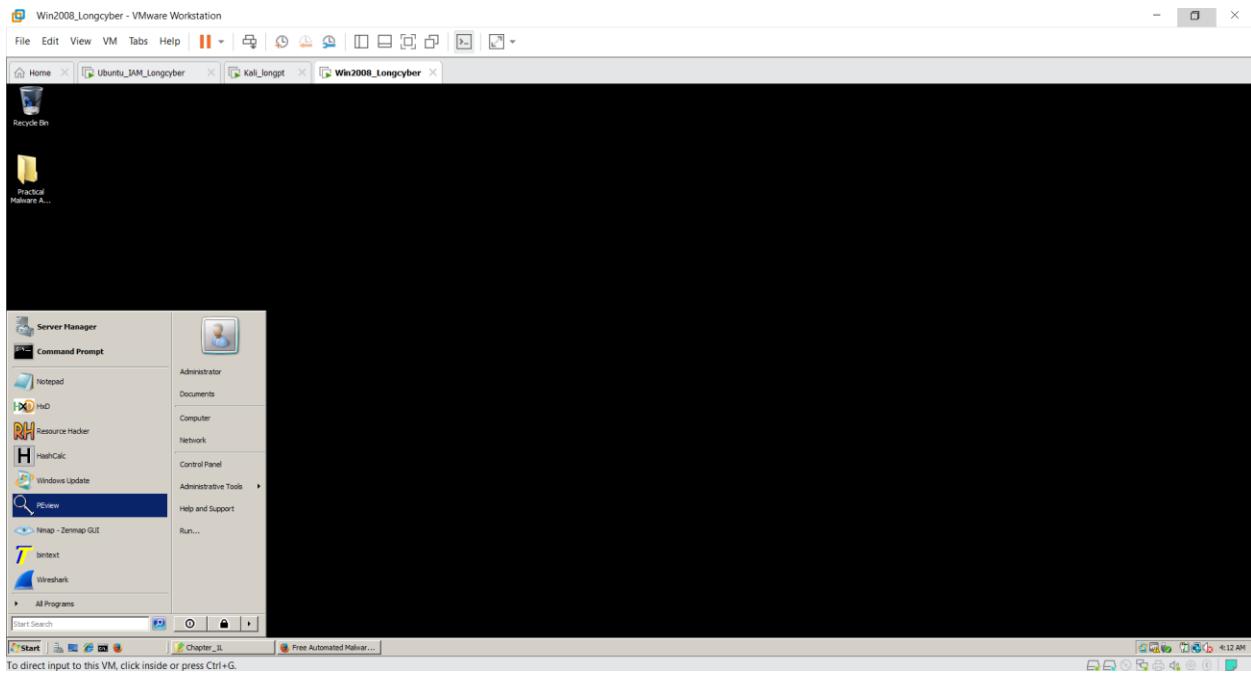
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Search results for f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2 dba							
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% Dns-Generic #tag #instructions #upx #backdoor #cmd #downloader #injector #ransomware #ransom #worm	-	Windows 10 64 bit	<input type="checkbox"/>
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% Dns-Generic Matched 17 Indicators #tag #instructions #upx #backdoor #cmd #downloader #injector #ransomware #ransom #worm	-	Windows 11 64 bit	<input type="checkbox"/>
January 18th 2023 17:44:38 (UTC)		Lab01-01.dll PE32 executable [DLL] (GUI) Intel 80386, for MS Windows f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba	suspicious	AV Detection: 83% Dns-Generic Matched 7 Indicators #tag #instructions #upx #backdoor #cmd #downloader #injector #ransomware #ransom #worm	-	Windows 7 64 bit	<input type="checkbox"/>
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% Dns-Generic Matched 6 Indicators #tag #instructions #upx #backdoor #cmd #downloader #injector #ransomware #ransom #worm	-	Windows 7 32 bit	<input type="checkbox"/>
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% Dns-Generic Matched 32 Indicators #tag #instructions #upx #backdoor #cmd #downloader #injector #ransomware #ransom #worm	-	Windows 10 64 bit	<input type="checkbox"/>

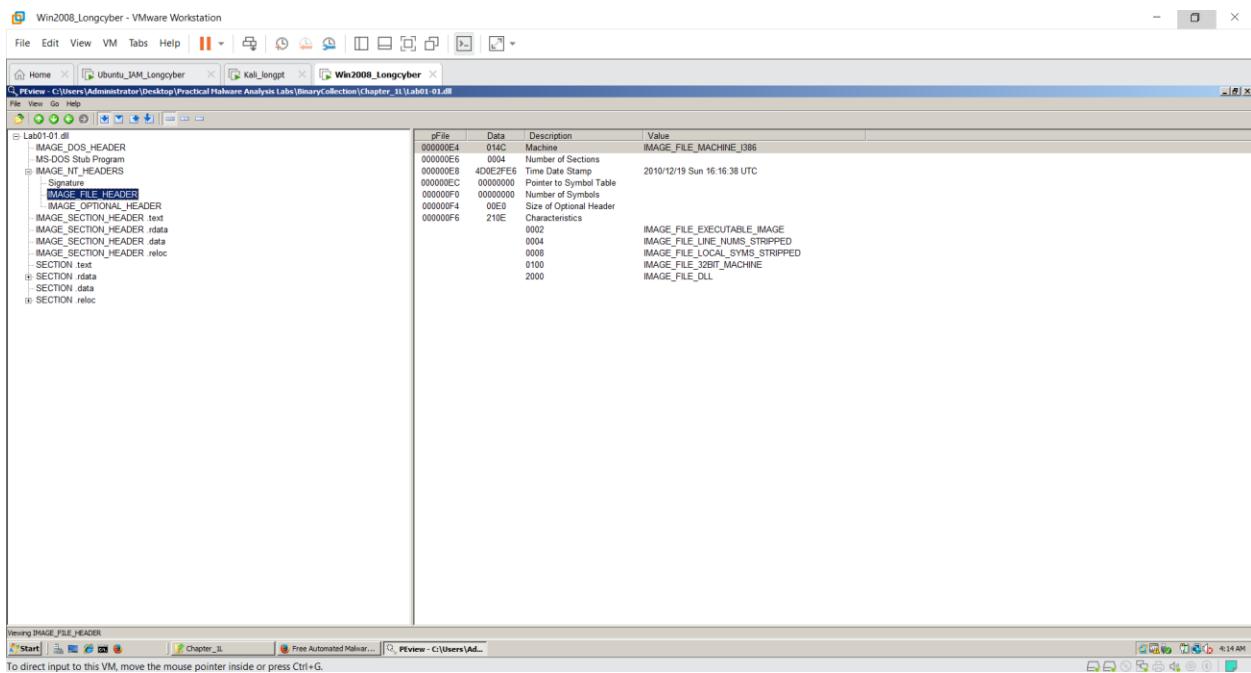
PEview

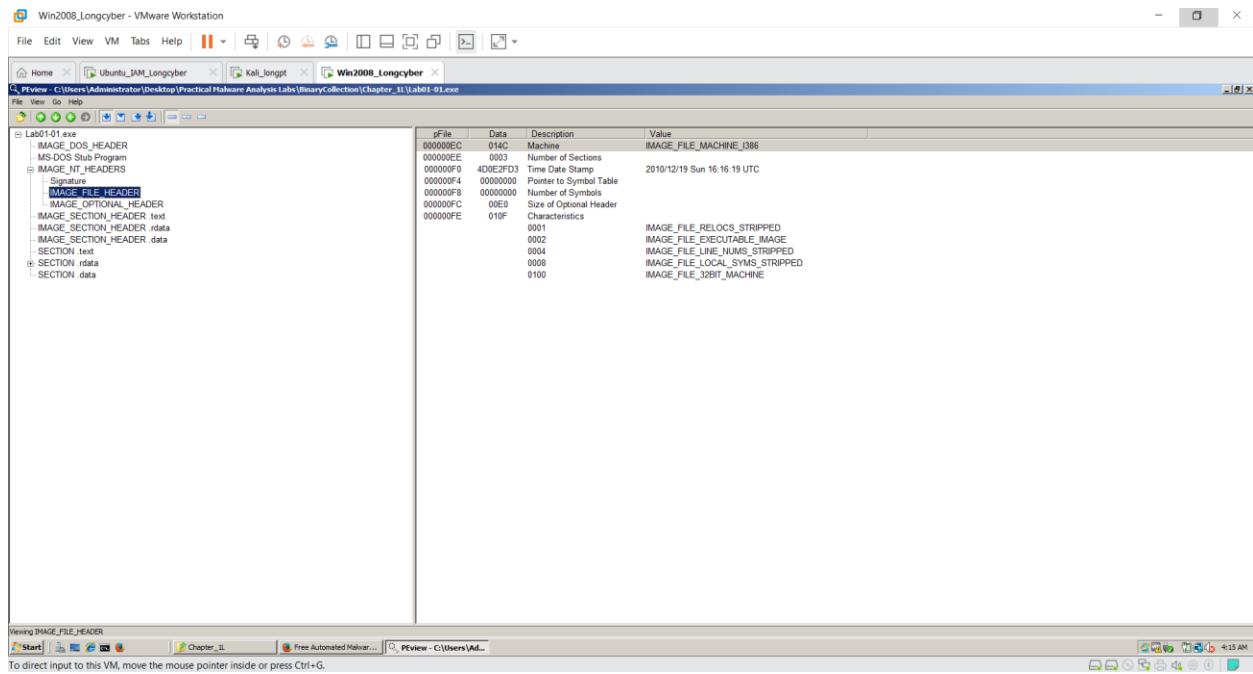
You can download PEview from here: <https://wjradburn.com/software/>

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.





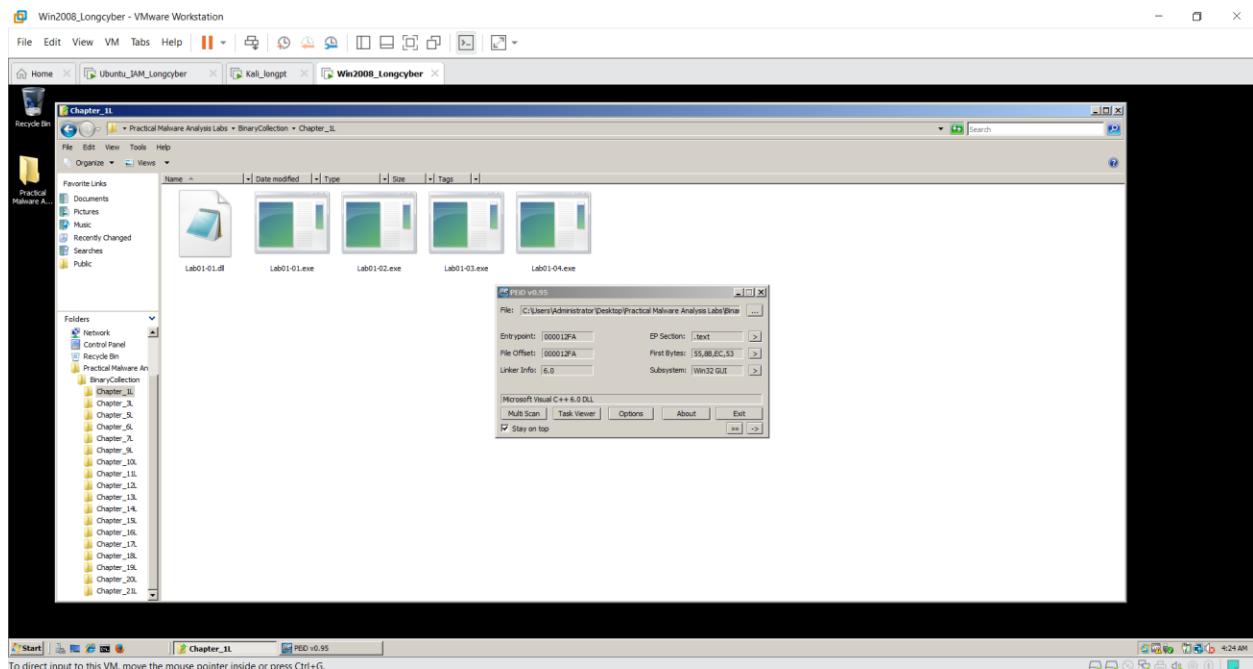
PEiD

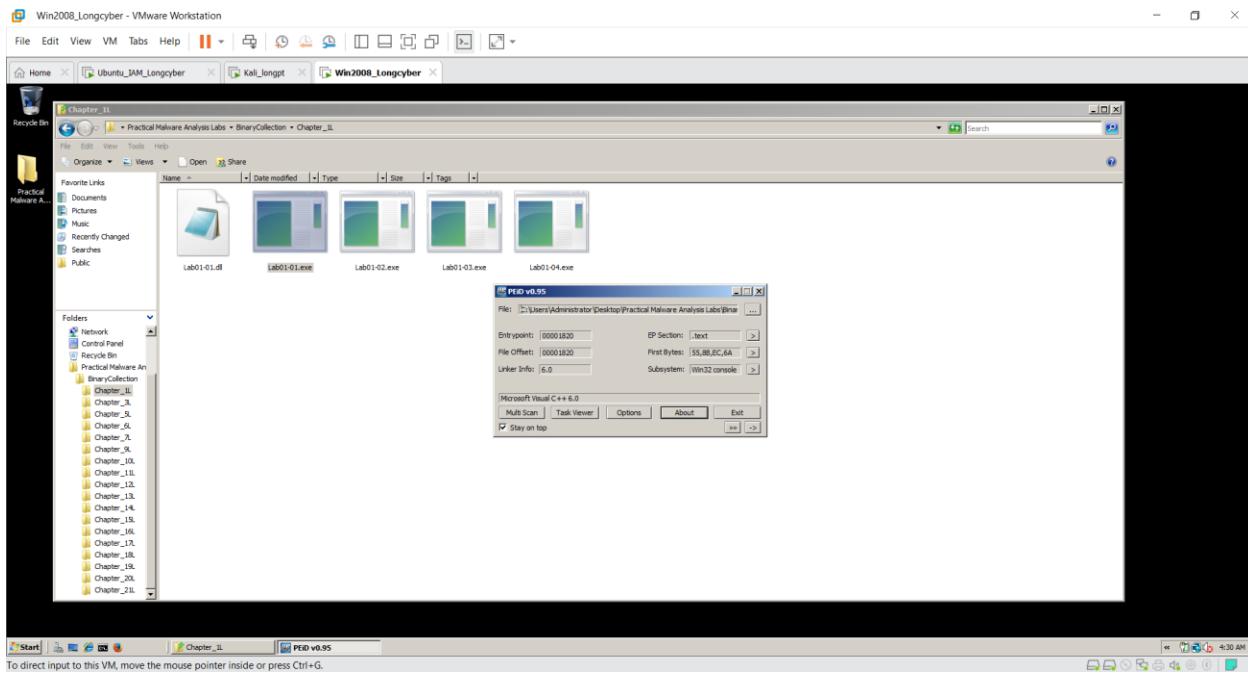
You can download PEiD here:

<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

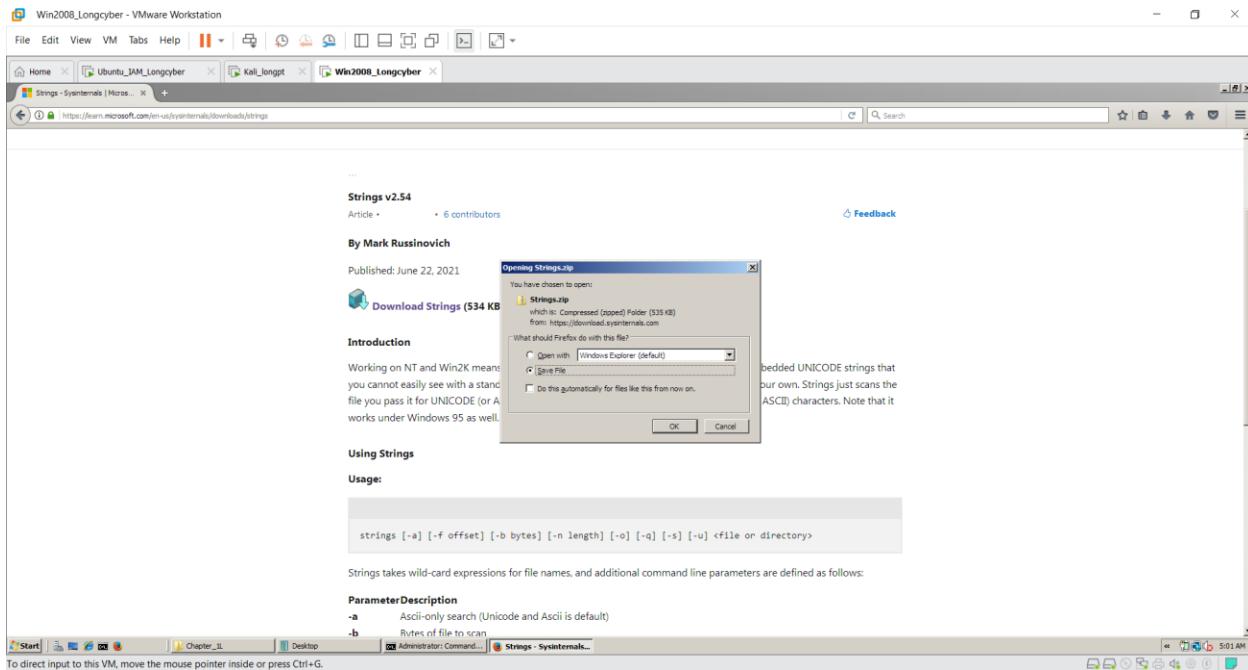
You can download Strings for Windows go here:

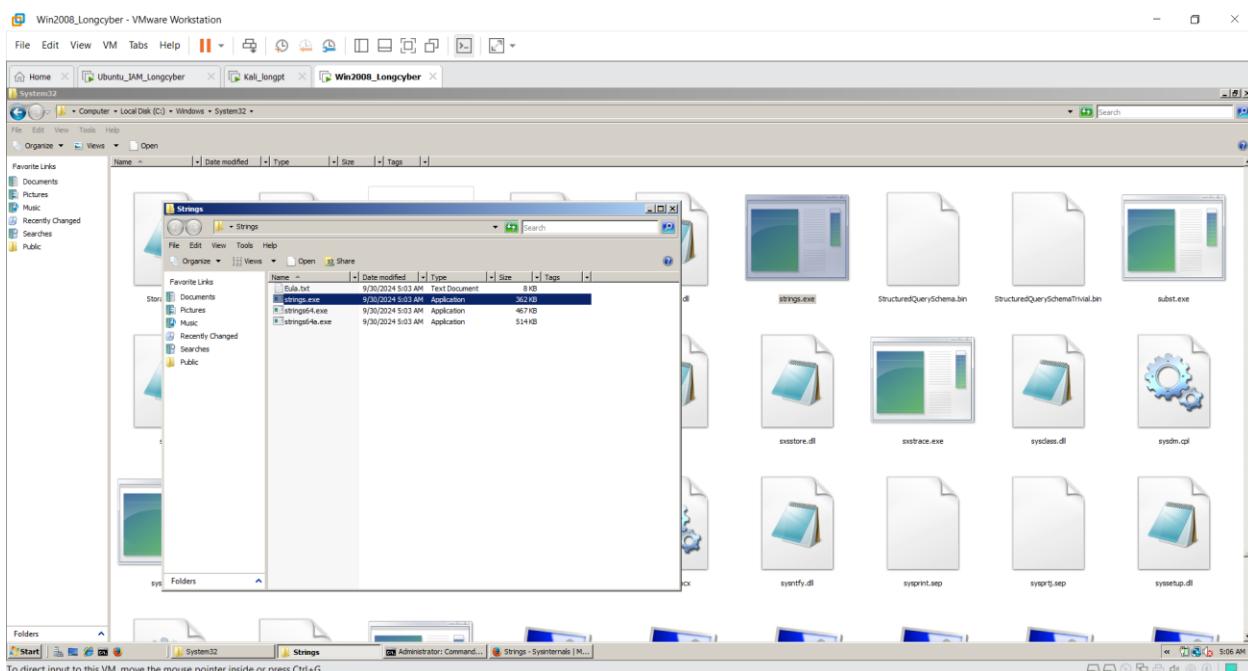
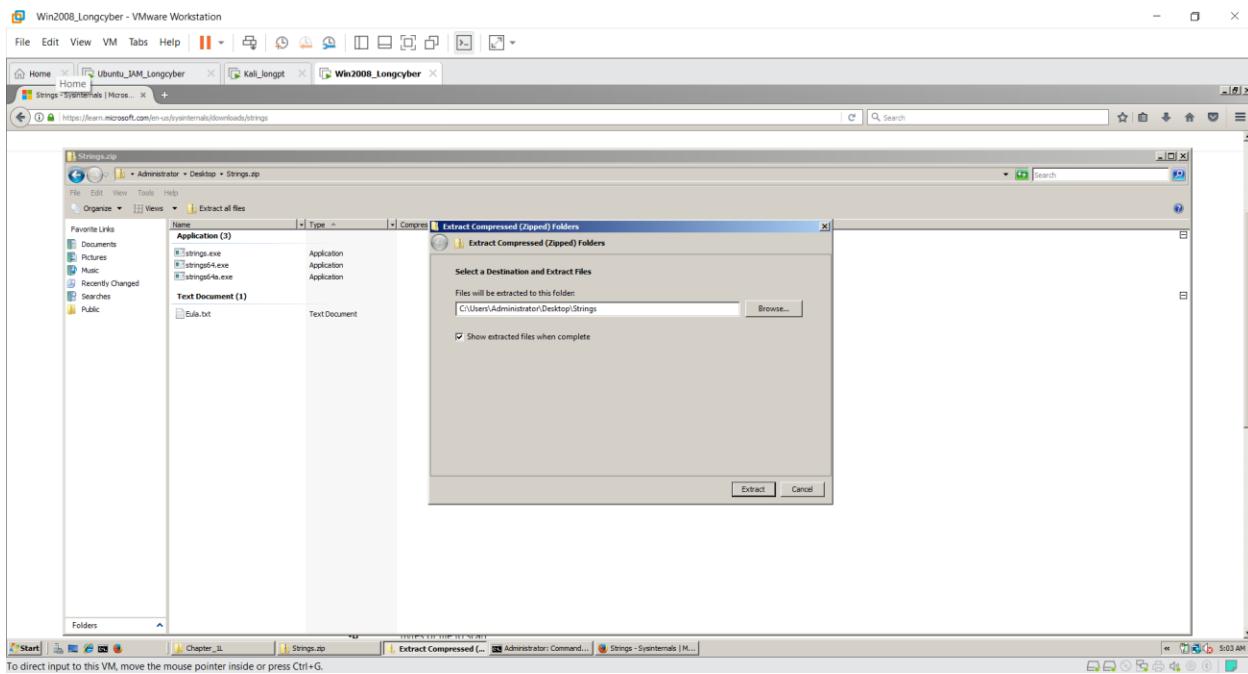
<https://technet.microsoft.com/en-us/sysinternals/bb897439>

Click the "Download Strings" link.

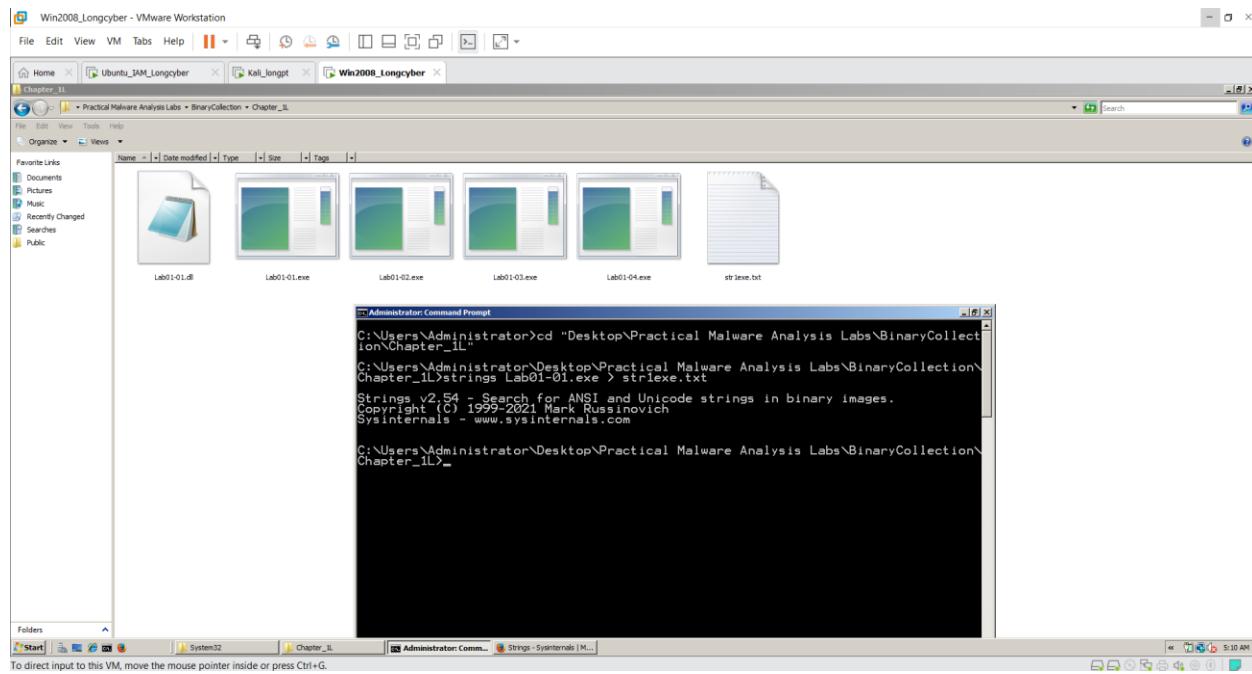
Save the Strings.zip file on your desktop.

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



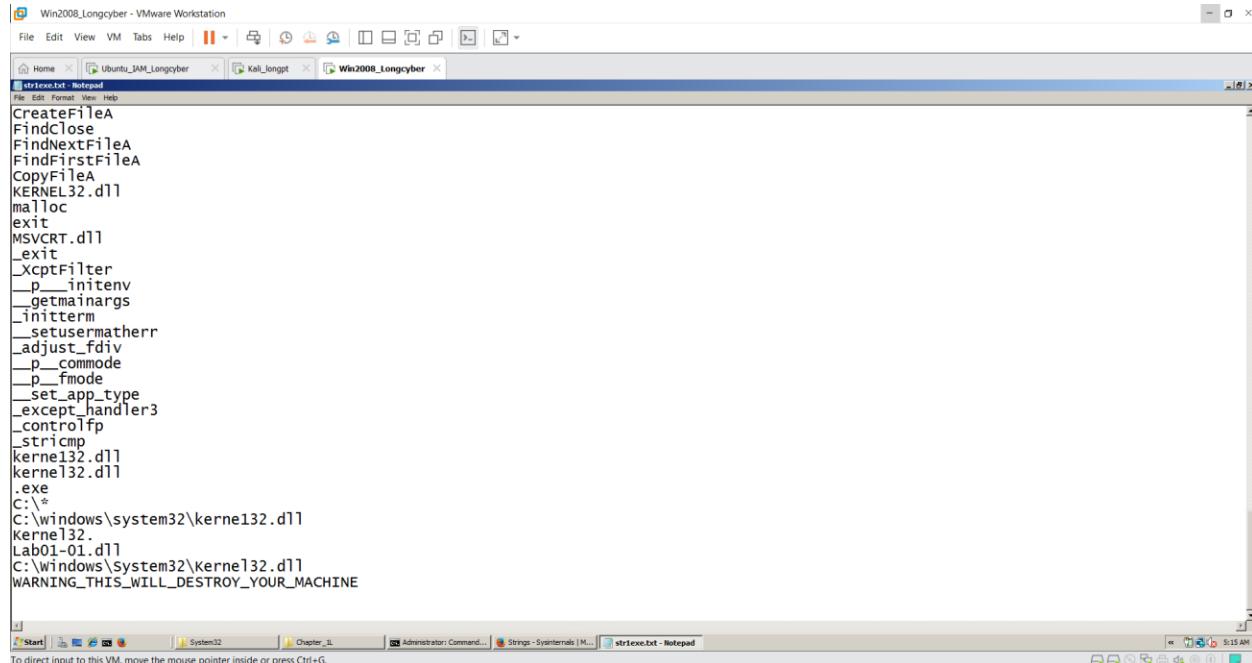


Open a Command Prompt and use the CD command to move to the directory containing your lab files. Then collect the strings from the Lab01-01.exe file. On my machine, Right-click in the **Chapter_1L** folder, and select **Open Command Window Here**.



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

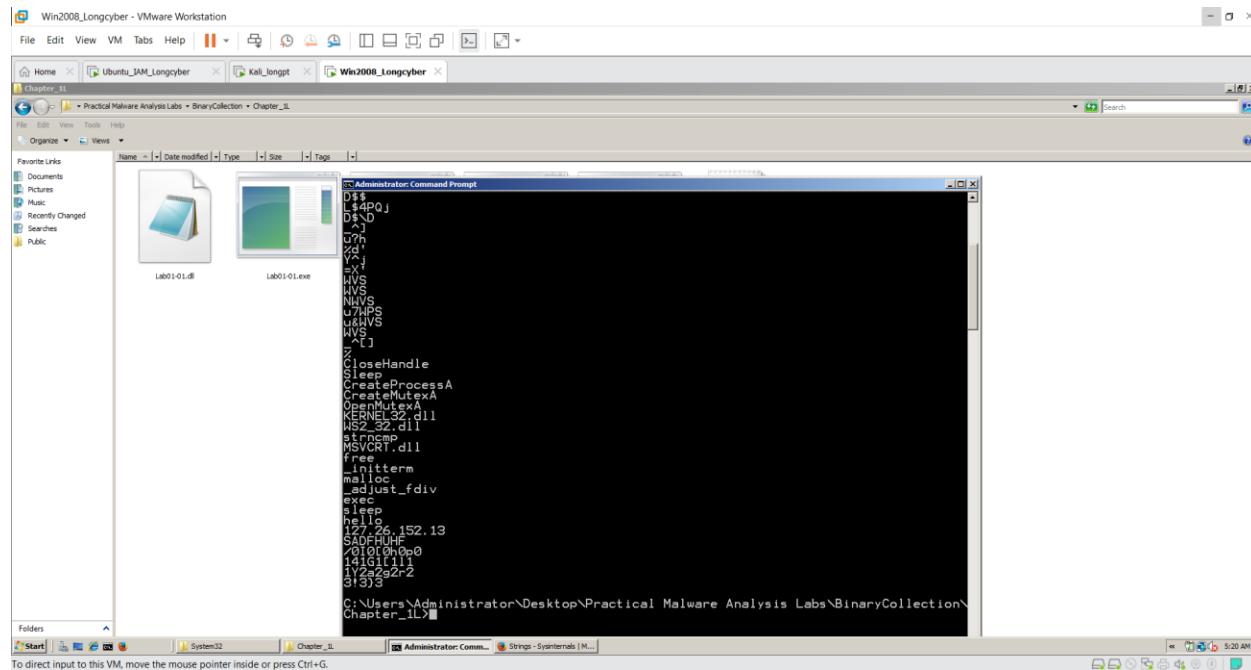


Look at the strings for Lab01-01.dll.

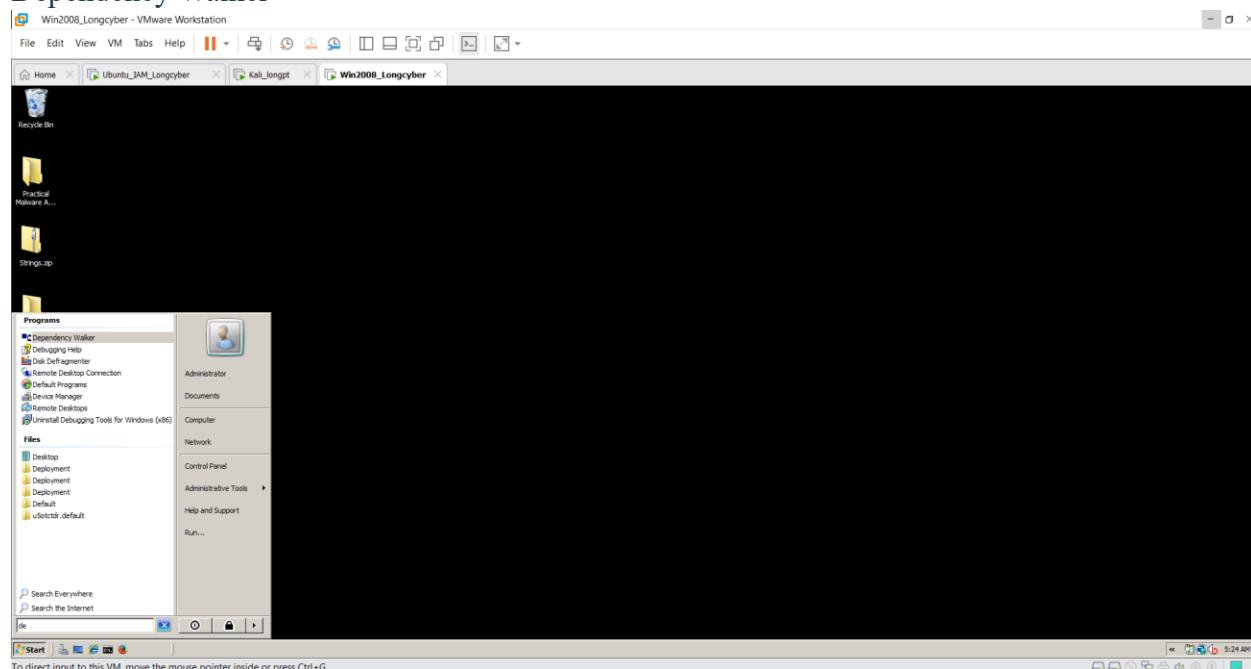
Notice these items, as shown below:

- "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

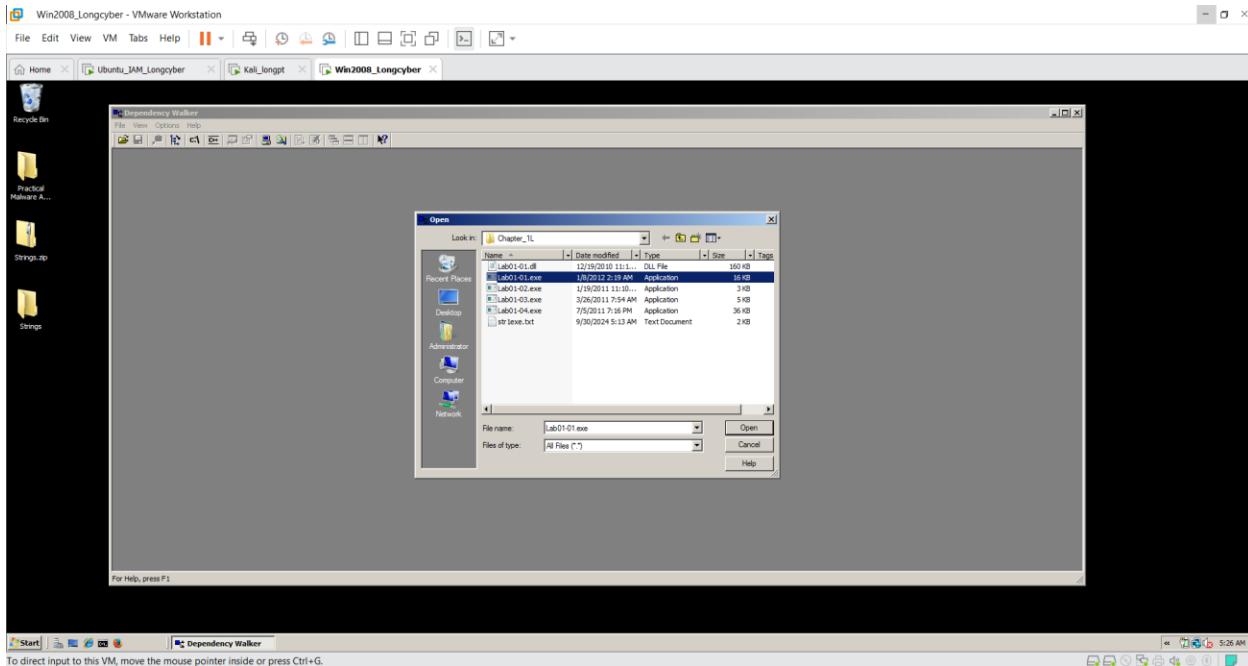
Turn in the image showing your analysis of Lab01-01.dll as shown below. Below "sleep" and "hello" there is an IP address, starting with 127. We will grade it by checking the last digits of the IP address.



Dependency Walker



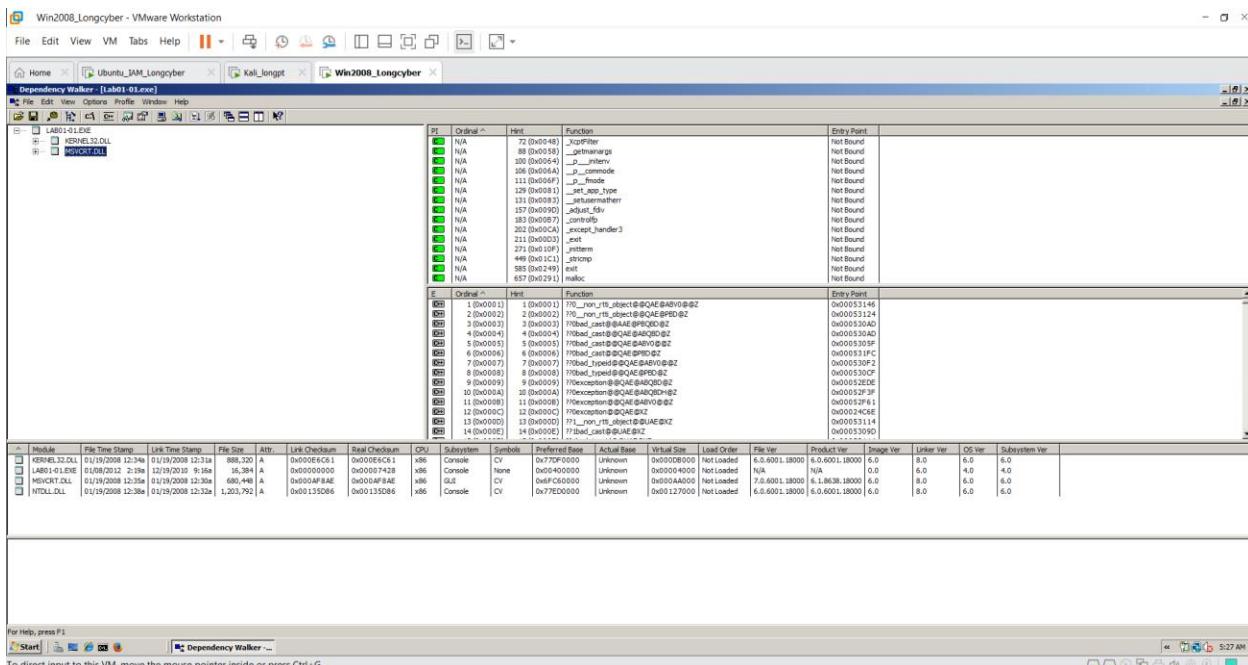
Open Lab01-01.exe in Dependency Walker.



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.

Win2008_Longcyber - VMware Workstation

File Edit View VM Tabs Help

Dependency Walker [Lab01-01.exe]

File Edit View Options Profile Window Help

Home Ubuntu_JAM_Longcyber Kali_Jongpt Win2008_Longcyber

Dependency Walker [Lab01-01.dll]

File Edit View Options Profile Window Help

LAB01-01.DLL

MSVCR7.DLL

Ordinal ^ Hint Function Entry Point

0x00000000	N/A	CloseHandle	Not Bound
0x00000000	N/A	CopyFileA	Not Bound
0x00000000	40 (0x028)	CreateFileA	Not Bound
0x00000000	52 (0x034)	CreateFileA	Not Bound
0x00000000	53 (0x035)	CreateFileMappingA	Not Bound
0x00000000	144 (0x090)	FindClose	Not Bound
0x00000000	148 (0x094)	FindFirstFileA	Not Bound
0x00000000	150 (0x096)	FindFirstFileA	Not Bound
0x00000000	437 (0x185)	SafeAllocHtr	Not Bound
0x00000000	470 (0x1D6)	MapViewOfFile	Not Bound
0x00000000	688 (0x2B0)	UnmapViewOfFile	Not Bound

Ordinal ^ Hint Function Entry Point

0x00000001	35 (0x023)	BaseThreadInitThunk	0x0004446F
0x00000002	712 (0x2C8)	InterlockedPushLockList	0x0004446F
0x00000003	1 (0x001)	InterlockedPopLockList	0x0004446F
0x00000004	1 (0x001)	AcquireSRWLockExclusive	0x0004446F
0x00000005	2 (0x002)	ActivateActCtx	0x0004446F
0x00000006	3 (0x003)	DeactivateActCtx	0x0004446F
0x00000007	4 (0x004)	AddAtomNotify	0x0004446F
0x00000008	5 (0x005)	AddConsoleArea	0x000443E8
0x00000009	6 (0x006)	AddConsoleArea	0x000443E8
0x0000000A	7 (0x007)	AddLocalAlternateComputerNameA	0x0008878D
0x0000000B	8 (0x008)	AddLocalAlternateComputerNameW	0x00088A46
0x0000000C	9 (0x009)	AddRefActCtx	0x00044AE4
0x0000000D	10 (0x00A)	AddServiceMemoryDescriptor	0x000443D9
0x0000000E	11 (0x00B)	AddSecureMemoryCacheCallback	0x000443D0

Module File Time Stamp Link Time Stamp File Size Attr Link Checksum Real Checksum CPU Subsystems Symbols Preferred Base Actual Base Virtual Size Load Order File Ver Product Ver Image Ver Linker Ver OS Ver Subsystem Ver

KERNEL32.DLL	01/19/2008 12:24a	01/19/2008 12:31a	888,320	A	0x000E6C1	0x000E6C1	x86	Console	CV	0x770F0000	Unknown	0x0000B000	Not Loaded	6.0.6001.18000	5.0.6001.18000	5.0	8.0	6.0	6.0
LAB01-01.EXE	01/09/2012 2:19a	12/19/2010 9:16a	16,384	A	0x00000009	0x00000009	x86	Console	None	0x00000000	Unknown	0x0000B400	Not Loaded	None	None	0.0	6.0	4.0	4.0
MSVCR7.DLL	01/19/2008 12:24a	01/19/2008 12:31a	1,203,792	A	0x0115066	0x0115066	x86	Console	CV	0x77E20000	Unknown	0x0000B000	Not Loaded	7.0.6001.18000	6.1.6001.18000	5.0	8.0	6.0	6.0
NTDLL.DLL	01/19/2008 12:24a	01/19/2008 12:32a	1,203,792	A	0x00115066	0x00115066	x86	Console	CV	0x77E20000	Unknown	0x000117000	Not Loaded	6.0.6001.18000	5.0.6001.18000	5.0	8.0	4.0	4.0

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

5:30 AM

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.

Win2008_Longcyber - VMware Workstation

File Edit View VM Tabs Help

Dependency Walker [Lab01-01.dll]

File Edit View Options Profile Window Help

Home Ubuntu_JAM_Longcyber Kali_Jongpt Win2008_Longcyber

Dependency Walker [Lab01-01.dll]

File Edit View Options Profile Window Help

LAB01-01.DLL

WS2_32.DLL

KERNEL32.DLL

RPCRT4.DLL

ADVAPI32.DLL

SHLWAPI.DLL

RPCOMM.DLL

NET.DLL

WS2_32.DLL

MSVCR7.DLL

Ordinal ^ Hint Function Entry Point

0x00000000	N/A	Accept	0x000444F4
0x00000001	132 (0x084)	AcceptEx	0x000444F4
0x00000002	N/A	Bind	0x000444F9
0x00000003	134 (0x086)	Closesocket	0x0000330C
0x00000004	135 (0x087)	Connect	0x00044409
0x00000005	N/A	Gethostname	0x00044483
0x00000006	147 (0x093)	Getsockoptname	0x00044661
0x00000007	148 (0x094)	Getsockopt	0x00044932
0x00000008	149 (0x095)	GetTime	0x00044400
0x00000009	150 (0x096)	Htrrc	0x00044310
0x0000000A	155 (0x098)	Octosocket	0x00043CE7
0x0000000B	151 (0x097)	Net_addr	0x000441E8

Ordinal ^ Hint Function Entry Point

0x00000001	132 (0x084)	Accept	0x000444F4
0x00000002	133 (0x085)	AcceptEx	0x000444F4
0x00000003	134 (0x086)	Closesocket	0x0000330C
0x00000004	135 (0x087)	Connect	0x00044409
0x00000005	N/A	Gethostname	0x00044483
0x00000006	147 (0x093)	Getsockoptname	0x00044661
0x00000007	148 (0x094)	Getsockopt	0x00044932
0x00000008	149 (0x095)	GetTime	0x00044400
0x00000009	150 (0x096)	Htrrc	0x00044310
0x0000000A	155 (0x098)	Octosocket	0x00043CE7
0x0000000B	151 (0x097)	Net_addr	0x000441E8

Module File Time Stamp Link Time Stamp File Size Attr Link Checksum Real Checksum CPU Subsystems Symbols Preferred Base Actual Base Virtual Size Load Order File Ver Product Ver Image Ver Linker Ver OS Ver Subsystem Ver

RPCOMM.DLL	01/19/2008 12:24a	01/19/2008 12:29a	6,068,736	A	0x0005D0A0	0x0005D0A0	x86	GUI	CV	0x75010000	Unknown	0x005C5000	Not Loaded	7.0.6001.18000	5.0.6001.18000	6.0	8.0	6.0	5.1
SHLWAPI.DLL	01/19/2008 12:36a	01/19/2008 12:31a	355,744	A	0x000574F3	0x000574F3	x86	GUI	CV	0x60400000	Unknown	0x00585000	Not Loaded	6.0.6001.18000	6.0.6001.18000	6.0	8.0	6.0	6.0
ADVAPI32.DLL	01/19/2008 12:38a	01/19/2008 12:27a	798,720	A	0x000C1181	0x000C1181	x86	Console	CV	0x77E20000	Unknown	0x0004C000	Not Loaded	6.0.6001.18000	5.0.6001.18000	6.0	8.0	6.0	6.0
RPCOMM.DLL	01/19/2008 12:38a	01/19/2008 12:29a	1,203,792	A	0x00030000	0x00030000	x86	Console	CV	0x77E20000	Unknown	0x0004C000	Not Loaded	6.0.6001.18000	5.0.6001.18000	6.0	8.0	6.0	6.0
LAB01-01.DLL	12/19/2010 11:19a	12/19/2010 9:16a	163,440	A	0x00000000	0x00001279E	x86	GUI	None	0x10000000	Unknown	0x00028000	Not Loaded	N/A	0.0	4.0	4.0		
MSVCR7.DLL	01/19/2008 12:36a	01/19/2008 12:30a	680,448	A	0x00040F8E	0x00040F8E	x86	GUI	CV	0x6FC60000	Unknown	0x000AA000	Not Loaded	7.0.6001.18000	6.1.6036.18000	6.0	8.0	6.0	6.0
NET.DLL	01/19/2008 12:38a	01/19/2008 12:29a	8,302	A	0x0000744E	0x0000744E	x86	Console	CV	0x77E20000	Unknown	0x00096000	Not Loaded	6.0.6001.18000	5.0.6001.18000	6.0	8.0	6.0	6.0
WS2_32.DLL	01/19/2008 12:38a	01/19/2008 12:31a	1,203,792	A	0x00040C92	0x00040C92	x86	Console	CV	0x77E20000	Unknown	0x0003C000	Not Loaded	6.0.6001.18000	5.0.6001.18000	6.0	8.0	6.0	6.0
RPCOMM.DLL	01/19/2008 12:38a	01/19/2008 12:29a	785,408	A	0x00040C92	0x00040C92	x86	Console	CV	0x77E20000	Unknown	0x0003C000	Not Loaded	6.0.6001.18000	6.0.6001.18000	6.0	8.0	6.0	6.0
WS2_32.DLL	01/19/2008 12:37a	01/19/2008 12:31a	170,200	A	0x0002E055	0x0002E055	x86	Console	CV	0x6B0D0000	Unknown	0x0002D000	Not Loaded	6.0.6001.18000	6.0.6001.18000	6.0	8.0	6.0	6.0

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.

5:33 AM

b. Lab01-02.exe

The screenshot shows the Hybrid Analysis interface for the file Lab01-02.exe. The file is identified as a PE32 executable (console) for MS Windows, UPX compressed. It has a size of 3KB (3072 bytes), is a process executable, and was compiled with UPX v1.25 (Delphi) Stub. The classification section shows a 34.7% chance it's UPX compressed Win32 Executable. The visualization section shows a small thumbnail of the file's binary structure. The entrypoint preview shows 44 instructions. The file details sidebar includes sections for Incident Response, Related Sandbox Artifacts, Indicators, File Metadata, File Sections, File Data Directories, and File Imports. A sidebar on the right lists screenshots, hybrid analysis, network analysis, extracted strings, extracted files, notifications, and community. A news feed at the bottom right mentions "HijackLoader Expands Techniques to Improve Defense Evasion" and "IMPERIAL KITTEN Deploys Novel Malware Families in Middle East-Focused Operations".

Unpacking the File

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

The screenshot shows the PEiD interface running on the file Lab01-02.exe. The interface displays various file headers and sections. In the main window, under the "File Details" tab, the "EP Section" dropdown is set to "UPX1". Other sections like "First bytes", "Subsystem", and "Linker Info" are also visible. The left sidebar shows the file structure with "Recycle Bin", "Practical Malware Analysis", and "Strings" entries. The taskbar at the bottom shows the PEiD application is active.

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

Download the upx391w.zip file, as shown below.

The screenshot shows a VMware Workstation window titled "Win2008_Longcyber - VMware Workstation". Inside, a browser window is displaying the UPX 4.2.4 release page from GitHub. The page header says "UPX 4.2.4 Latest". It shows a message from "markus-oberhumer" released on May 09 at 10:27, mentioning 62 commits since the previous release. The version is v4.2.4 with commit 3757579. A note states that all versions are functionally equivalent and can handle all executable formats. Security/VirusTotal links are pinned. Below is a table of assets:

Asset / File	Description / Host OS
upx-4.2.4-amd64_linux.tar.xz	UPX - Linux version, statically linked
upx-4.2.4-arm64_linuxtar.xz	UPX - Linux version, statically linked
upx-4.2.4-armeb_linuxtar.xz	UPX - Linux version, statically linked
upx-4.2.4-arm_linuxtar.xz	UPX - Linux version, statically linked
upx-4.2.4-dos.zip	UPX - DOS version
upx-4.2.4-i386_linux.tar.xz	UPX - Linux version, statically linked
upx-4.2.4-mipsel_linuxtar.xz	UPX - Linux version, statically linked
upx-4.2.4-mips_linux.tar.xz	UPX - Linux version, statically linked
upx-4.2.4-powerpc64le_linux.tar.xz	UPX - Linux version, statically linked
upx-4.2.4-powerpc_linuxtar.xz	UPX - Linux version, statically linked
upx-4.2.4-srcstar.xz	UPX - source code tarball
upx-4.2.4-win32.zip	UPX - X86 Win32 version

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.

The screenshot shows a VMware Workstation window titled "Win2008_Longcyber - VMware Workstation". Inside, a Windows desktop environment is visible. The Start menu is open, showing a list of programs. At the bottom of the list, under "User Accounts", is a file named "UPX.BAT". A tooltip for this file indicates it is a "Type: Windows Batch File" with a size of 37 bytes and was modified on 6/26/2017 at 10:25 AM. The desktop background is black, and the taskbar shows the VMware interface.

Open a Command Prompt window and execute this command: upx

You see a UPX help message, as shown below:

```

Administrator: Command Prompt
C:\Windows>cd System32
C:\Windows\System32>"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 [-123456789dthVL] [-qvfk] [-o file] file...
Commands:
-i compress faster           -g 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          -e executables to (de)compress
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:\Windows\System32>

```

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:

```

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

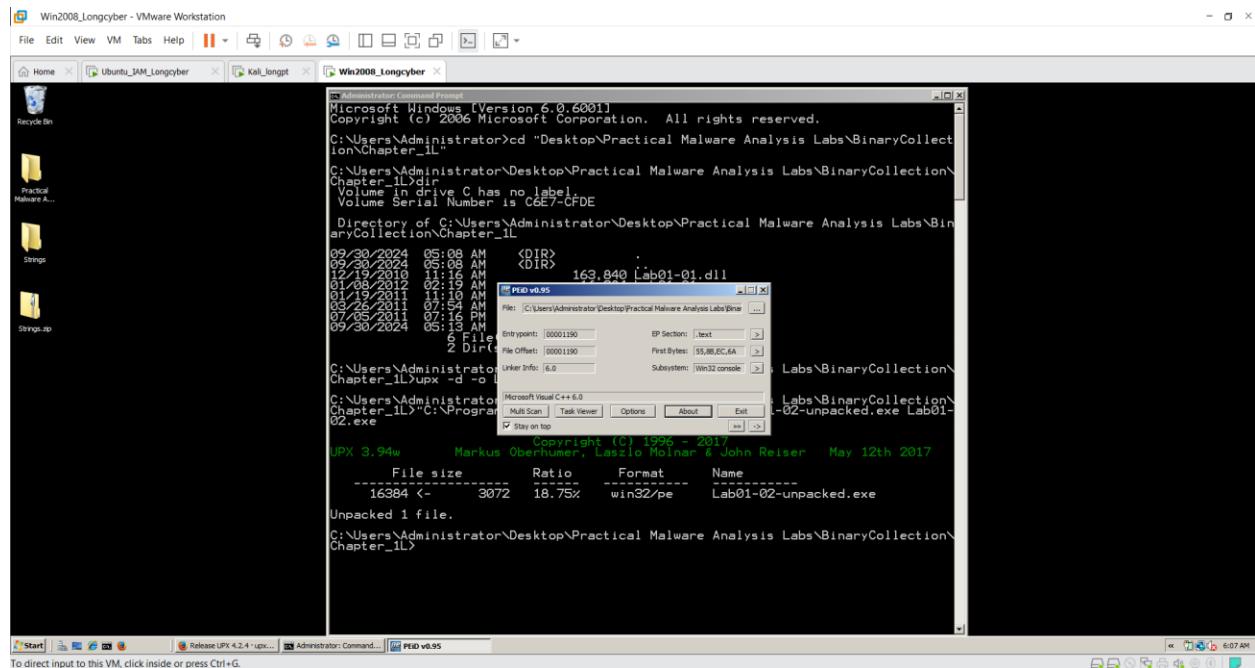
C:\Users\Administrator>cd "Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L"
C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L>dir
Volume in drive C has no label.
Volume Serial Number is CGE7-CFDE
Directory of C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L
09-30-2024 05:08 AM <DIR> .
09-30-2024 05:08 AM <DIR> ..
12-19-2010 11:16 AM 163,840 Lab01-01.dll
01-08-2012 02:19 AM 16,384 Lab01-01.exe
01-08-2012 02:19 AM 16,384 Lab01-02.exe
03-26-2011 07:54 AM 2,752 Lab01-03.exe
07-05-2011 07:16 PM 36,864 Lab01-04.exe
09-30-2024 05:13 AM 225,212 striexe.txt
               6 Dir(s)   33,677,320,192 bytes free
C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L>upx -d 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>

```

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

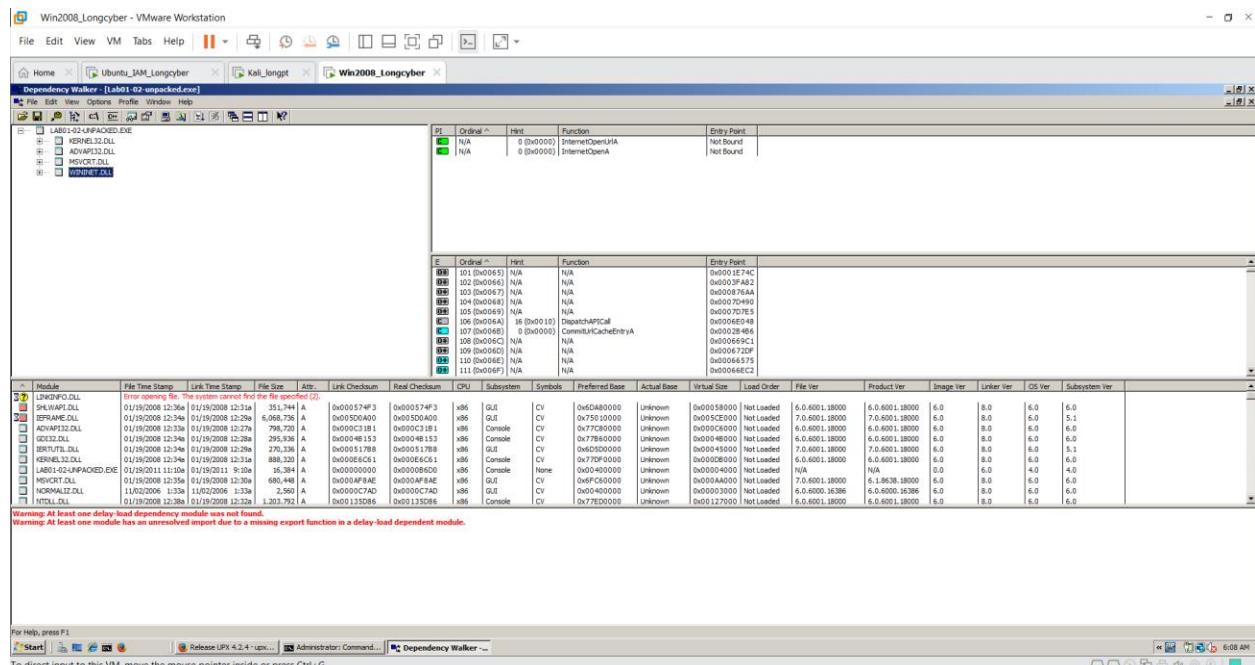
Turn in the image showing your analysis of **Lab01-02-unpacked.exe** as shown below.

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:

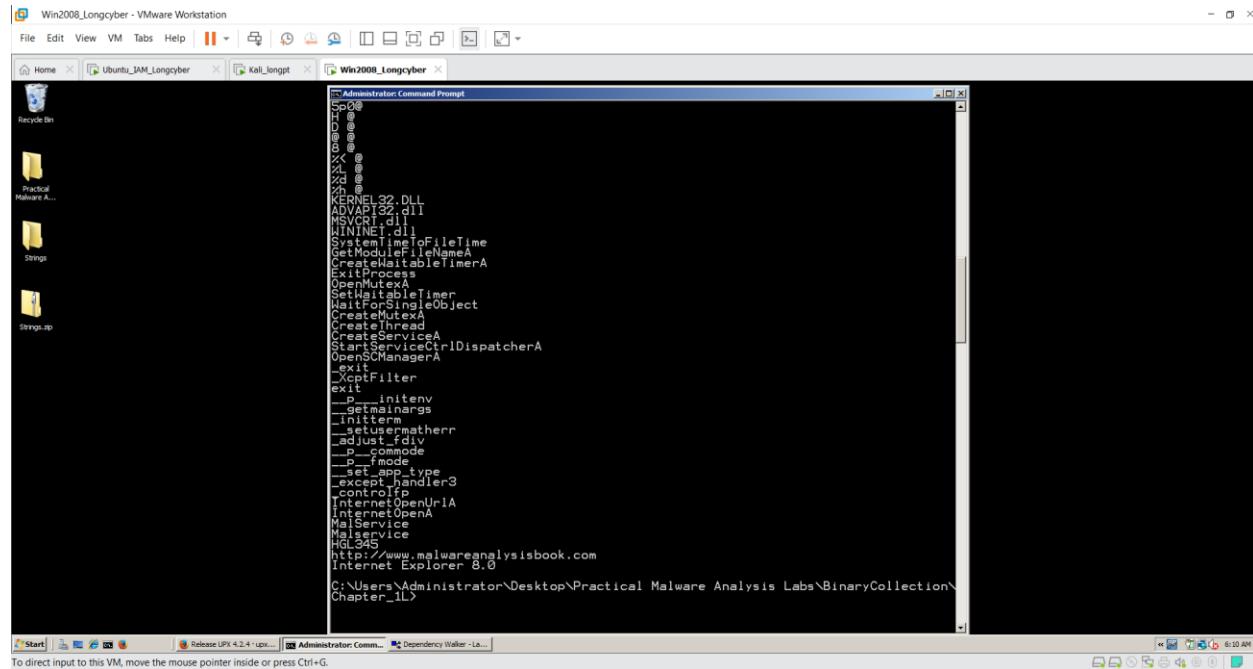


Strings

Find the strings in the unpacked file.

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

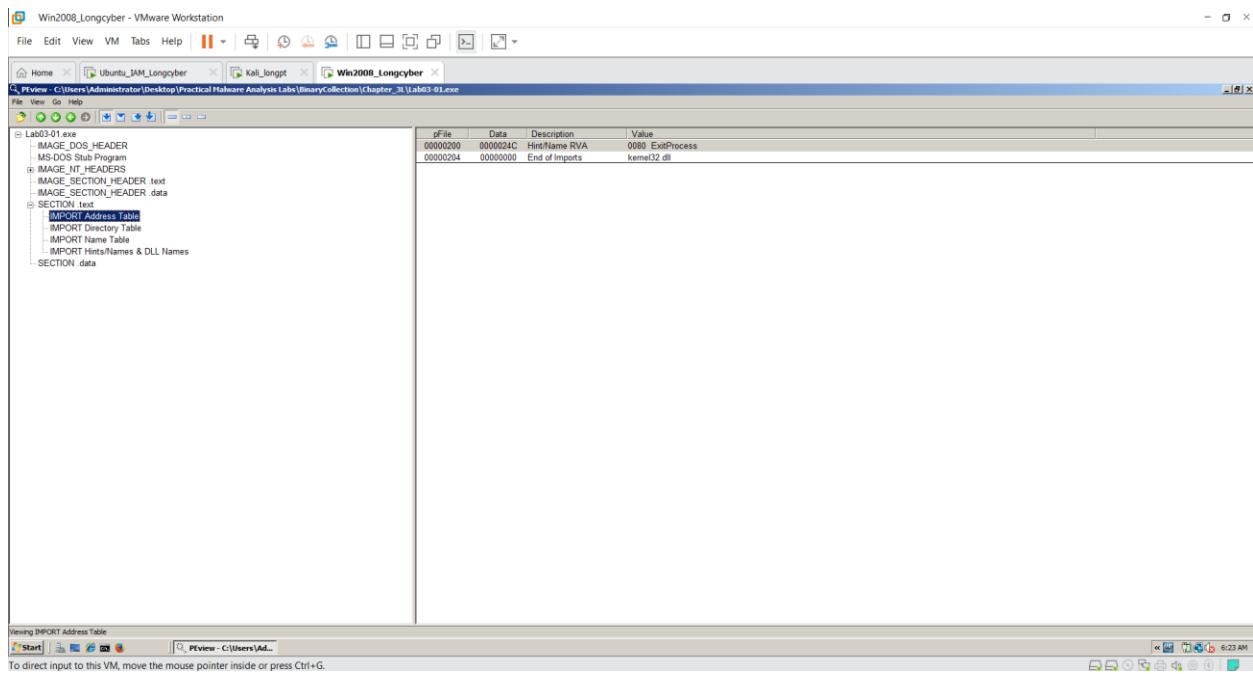
These suggest that infected machines will connect to <http://www.malwareanalysisbook.com> and will show a running service named MalService.



The screenshot shows a Windows 7 desktop environment. In the foreground, there is a Command Prompt window titled "Administrator: Command Prompt". The window displays a list of strings, many of which are function names from the Windows API, such as "KERNEL32.DLL", "APIENTRY", "GetModuleHandleA", "CreateWaitableTimerA", "ExitProcess", "OpenMutexA", "StartServiceCtrlDispatcherA", "CreateThread", "CreateService", "StartServiceCtrlDispatcherA", "OpenSCManagerA", and "exit". At the bottom of the list, it shows "C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_1\>". In the background, a file browser window titled "Win2008_Longcyber - VMware Workstation" is visible, showing files like "Practical Malware A...", "Strings", and "Strings.ap". The taskbar at the bottom has icons for Start, Release UP!, Administrator: Command Prompt, and Dependency Walker - Lab...

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

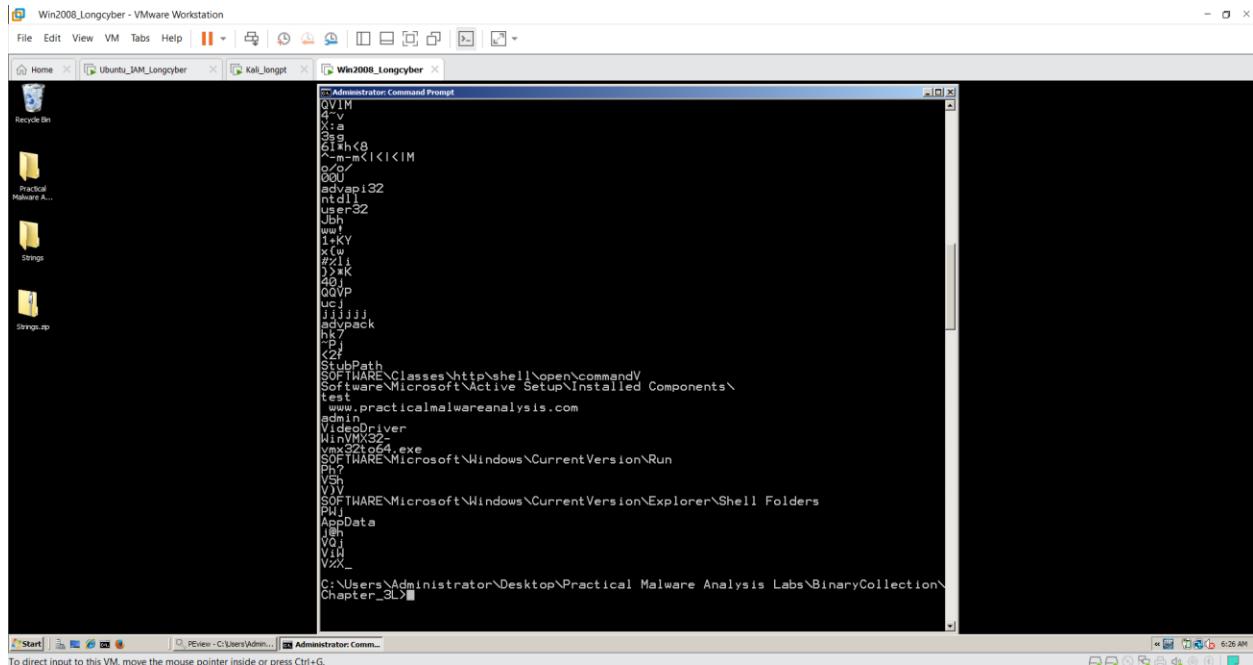
Examine the strings in **Lab03-01.exe** and find these items, as shown below.

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

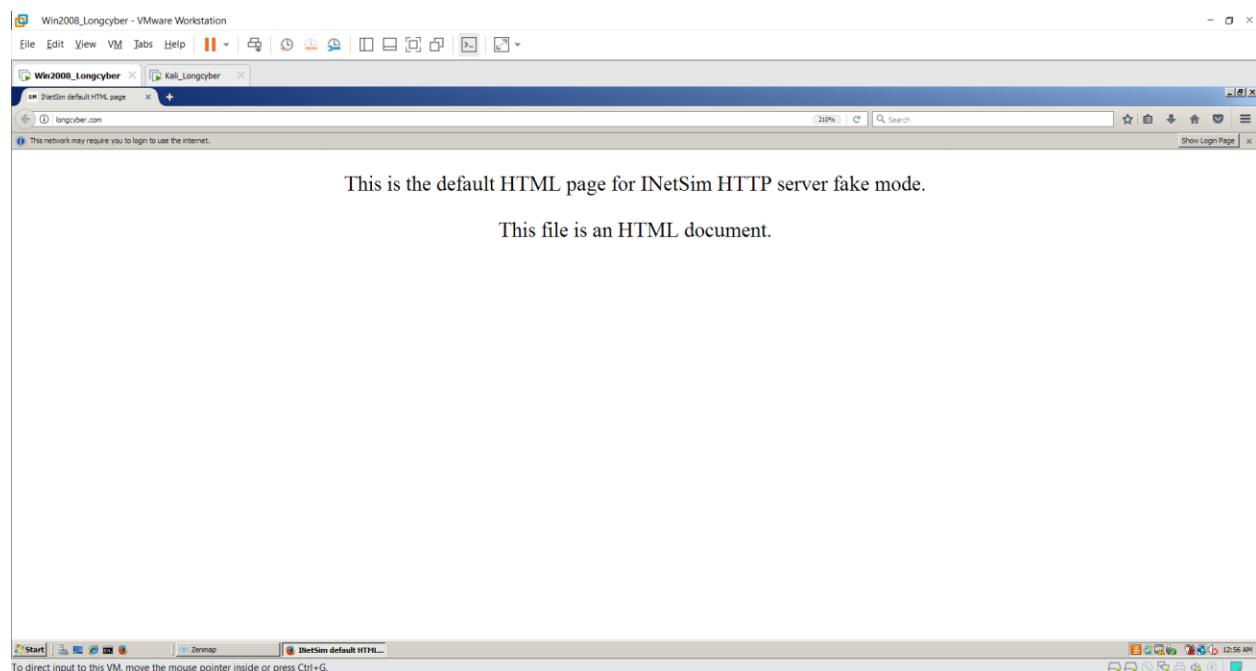
Start both the Windows and Linux VMs.

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:

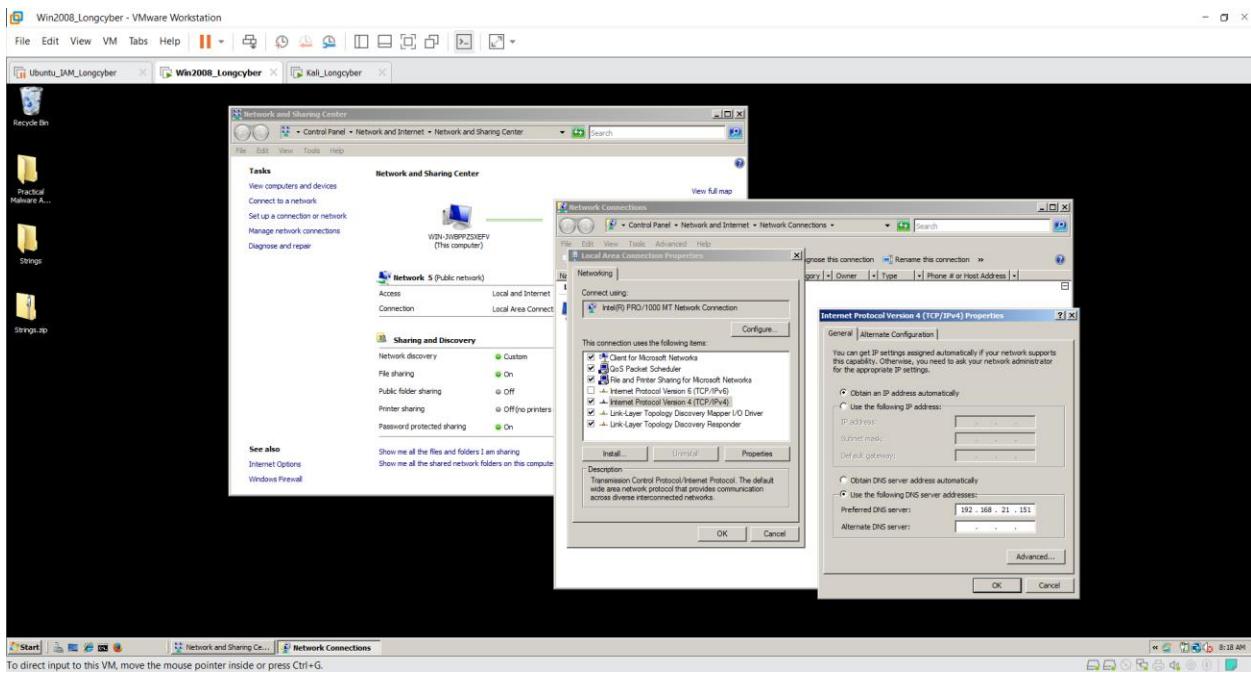


2. Setting the DNS Server

On your Windows VM, in Control Panel, open "Network Connections". Right-click "Local Area Connection" and click Properties.

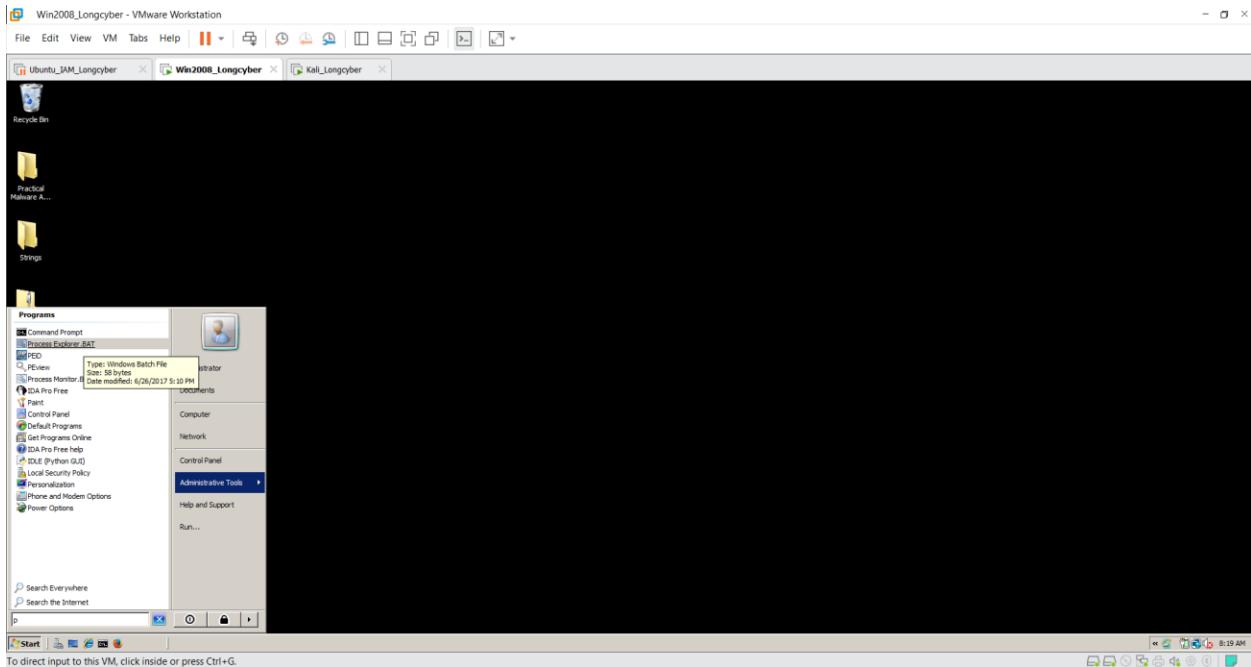
Double-click "Internet Protocol (TCP/IP)".

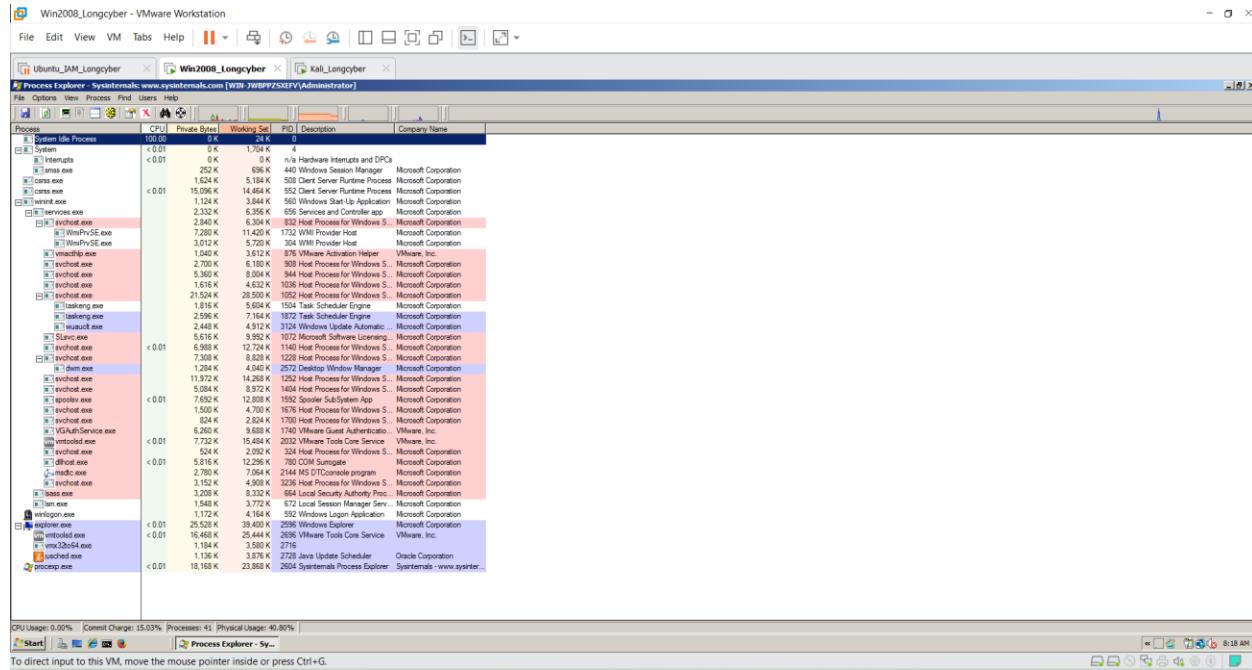
Set your DNS server to the Kali Linux machine's IP address, as show below:



3. Run Process Explorer

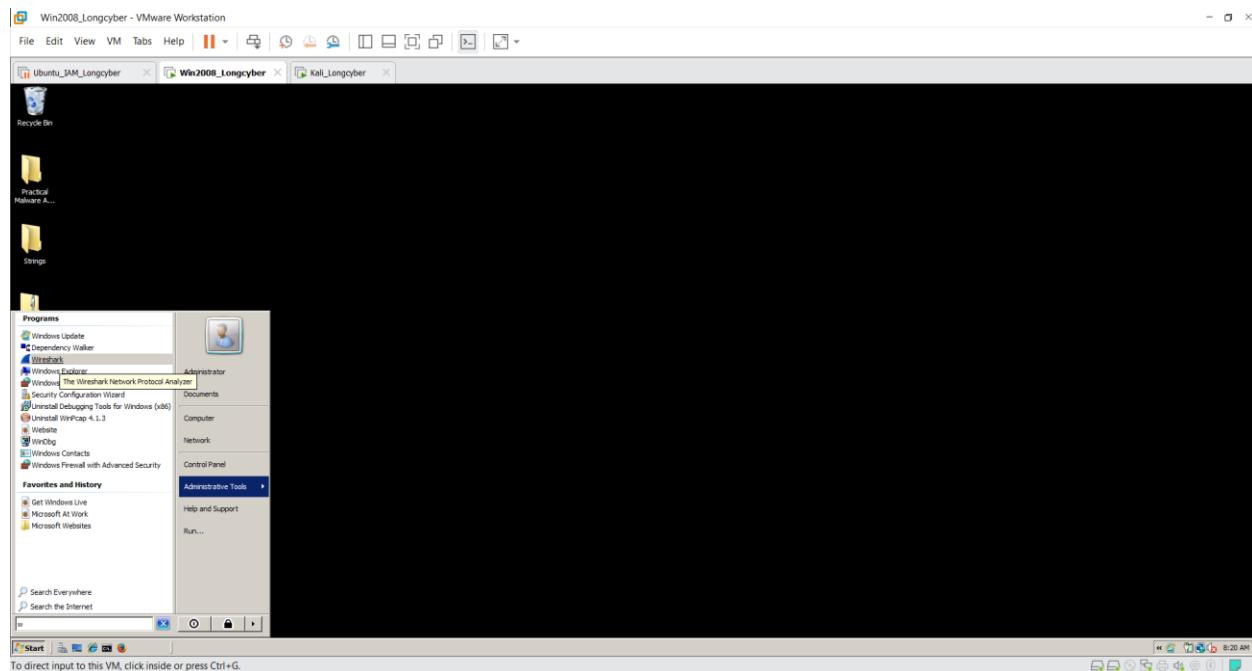
Open Process Explorer, as shown below:

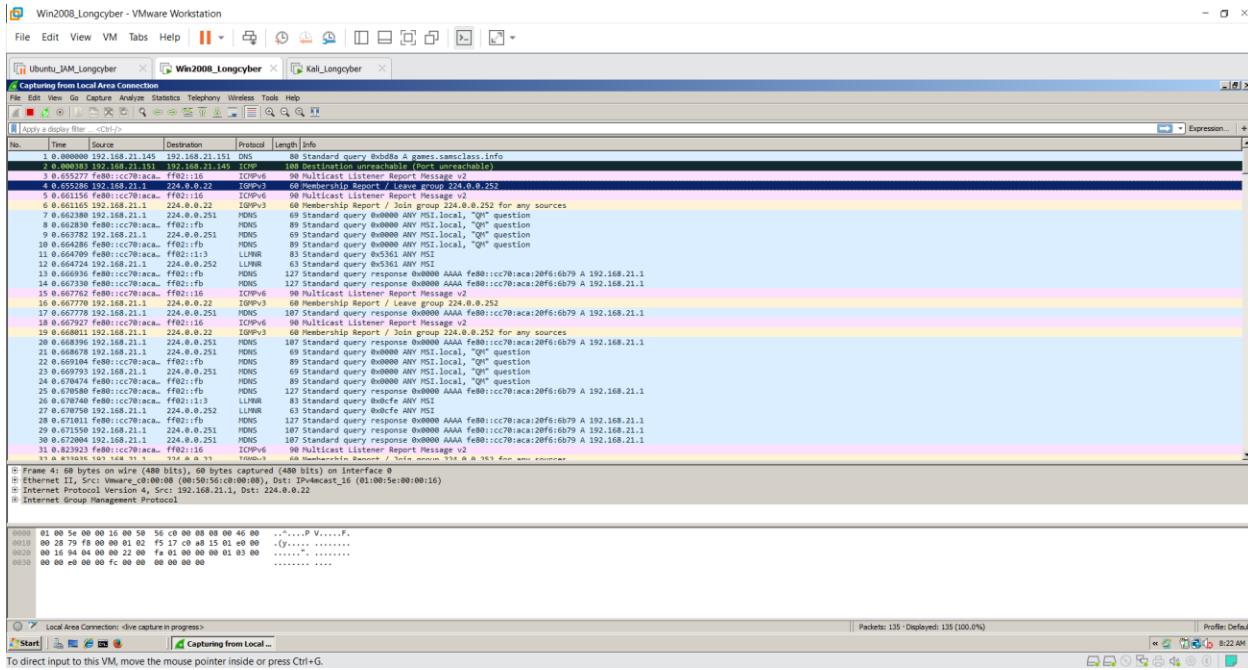




4. Run Wireshark

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

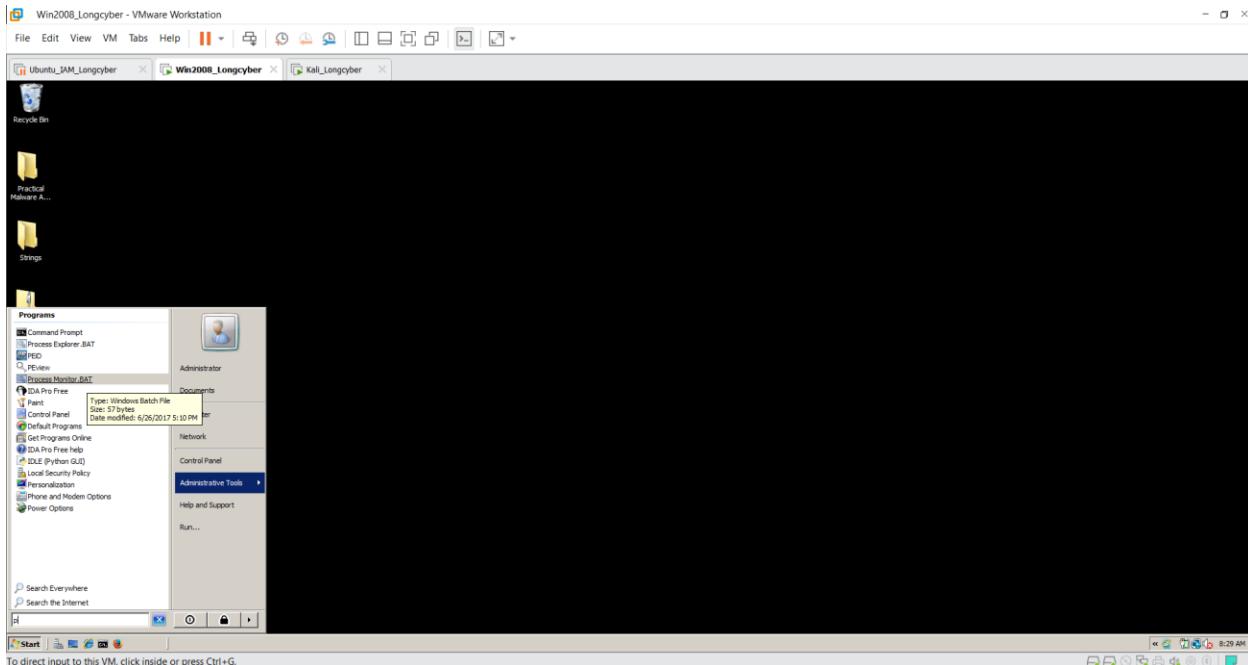
It's best to start Process Monitor last, so you can exclude all the harmless processes the other tools are using.

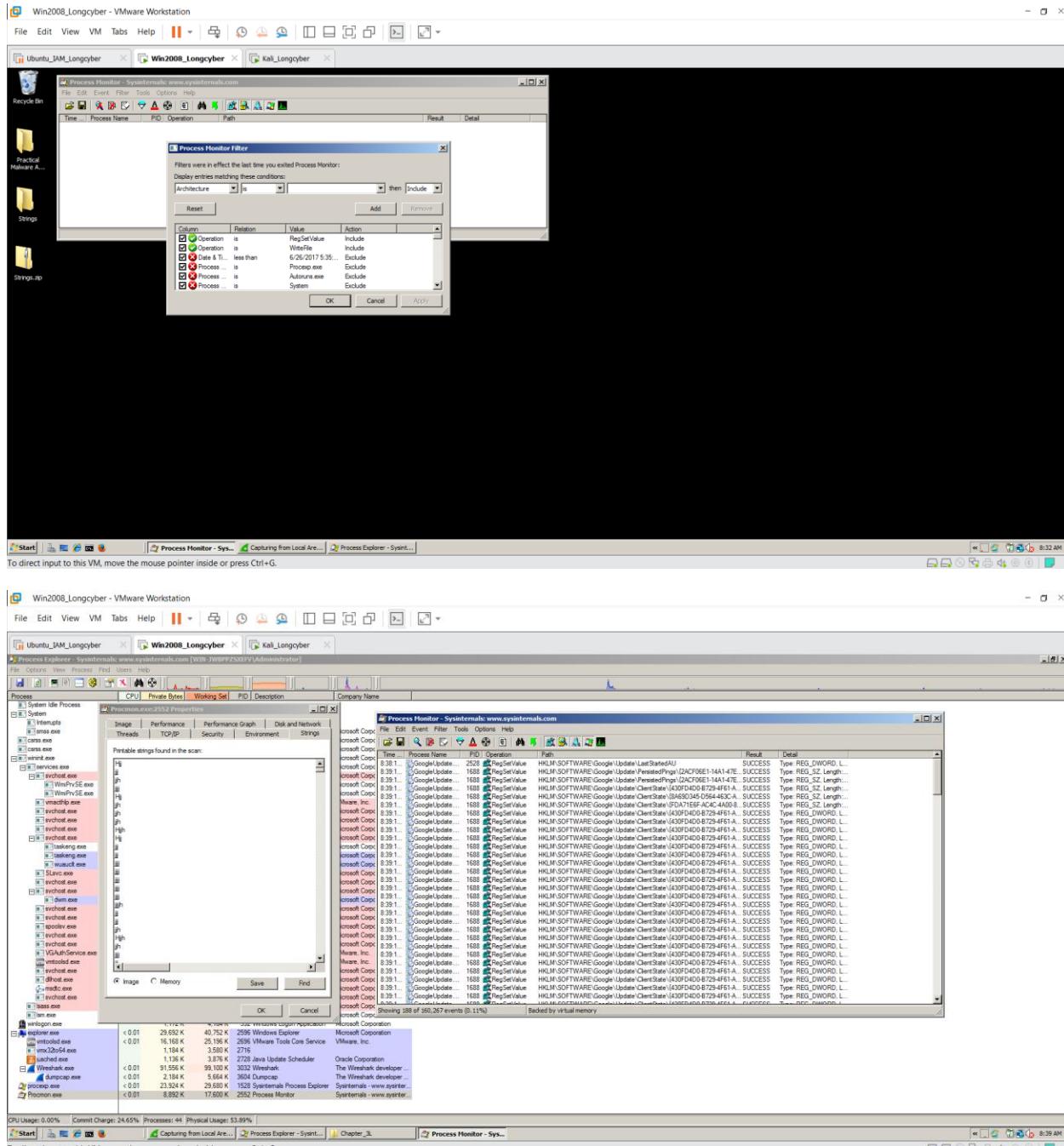
In the folder you unzipped Process Monitor into, double-click **Procmon.exe**.

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:

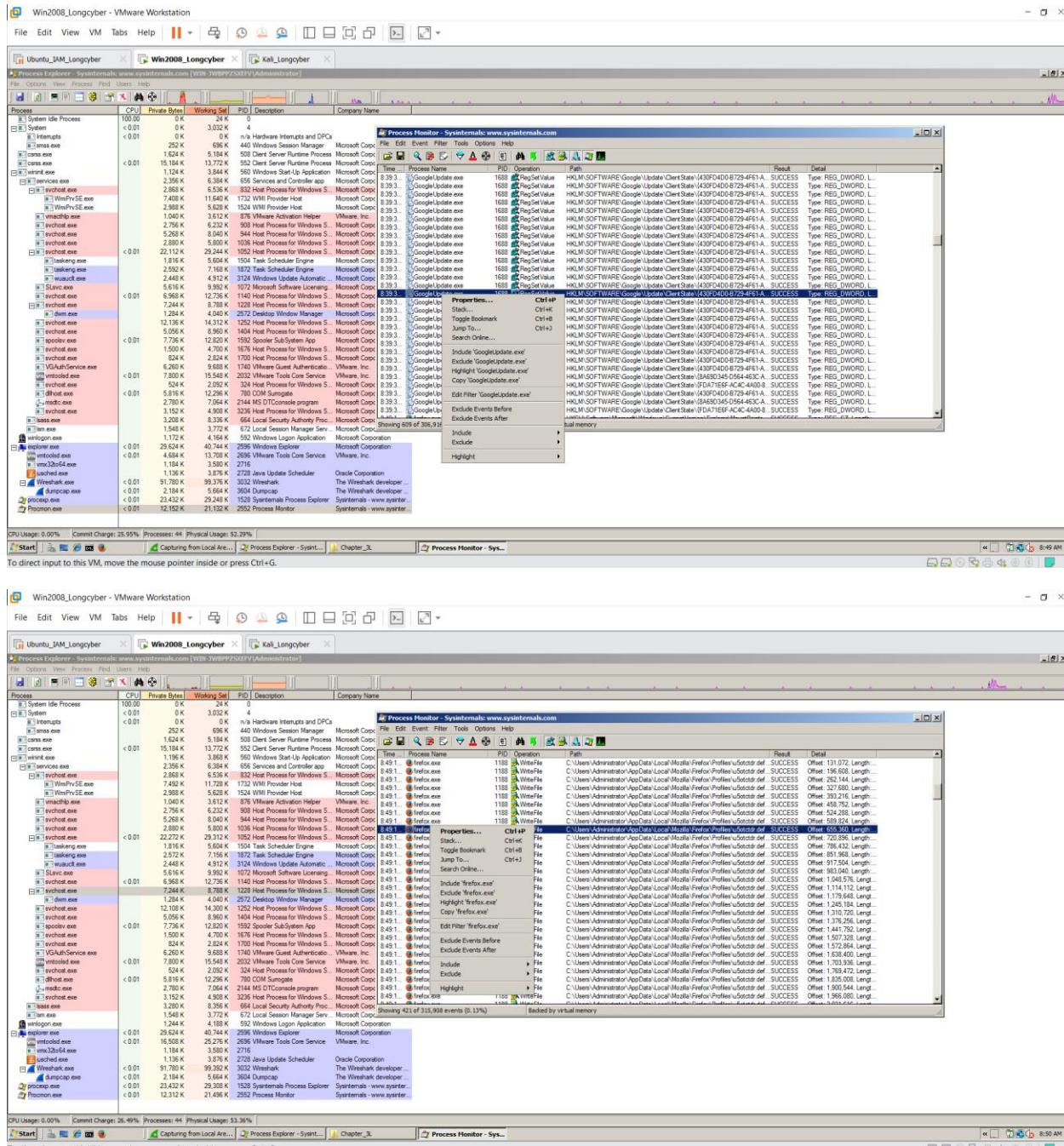




Excluding Harmless Processes

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:

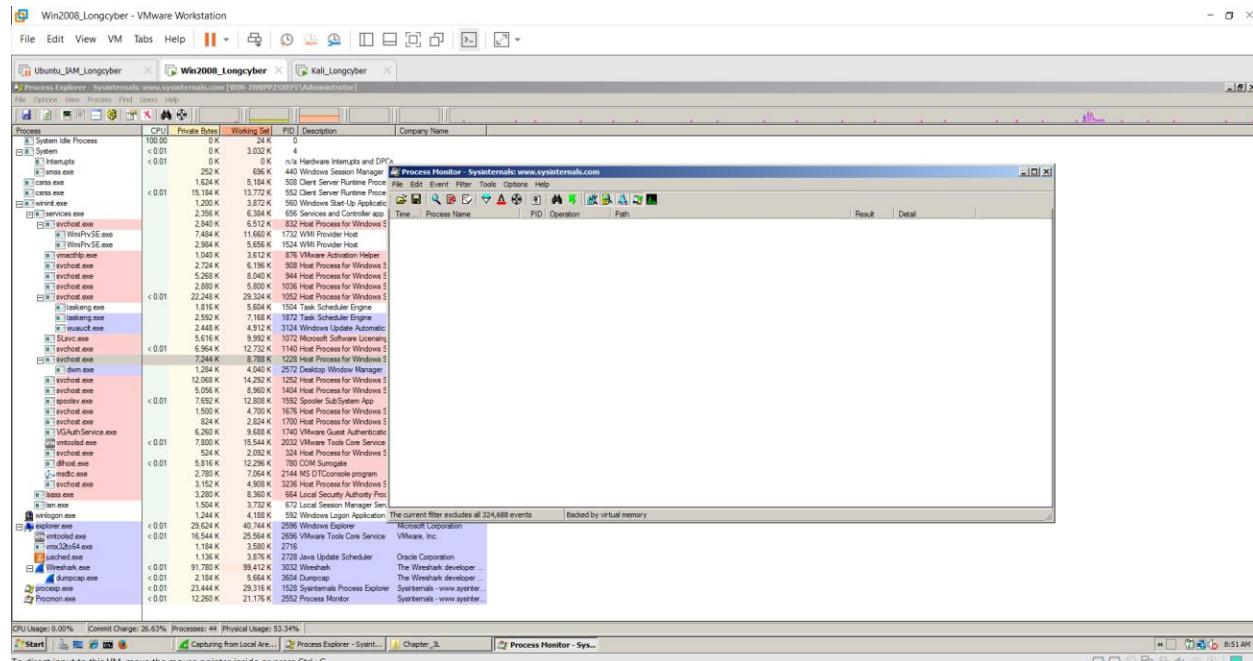


Wait while the event filter is applied.

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, wmpiprvse.exe, wuauctl.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 communication. A wonderful explantion of mutexes in terms of rubber chickens is here.