

Proj 4: Basic Dynamic Techniques (Lab 3-1) (30 pts., 6 images)

What you need:

- A Windows 2008 Server virtual machine with a Kali virtual machine running INetSim, which you prepped in the previous project.

NOTE: Windows 7 will not work for this project!

- Recommended: the textbook: "Practical Malware Analysis"

Purpose

You will practice the techniques in chapter 3.

This project follows **Lab 3-1** in the textbook. There are more detailed solutions in the back of the book.

Downloading Software

At the end of the previous project, you ended up with your Windows 2008 Server machine's DNS address set to your Kali machine's IP address, which means it cannot reach the Internet.

In order to download software, you need to configure a real DNS server, such as 8.8.8.8.

Setting the DNS Server to 8.8.8.8

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 8.8.8.8

Required Downloads

Make sure you have these items:

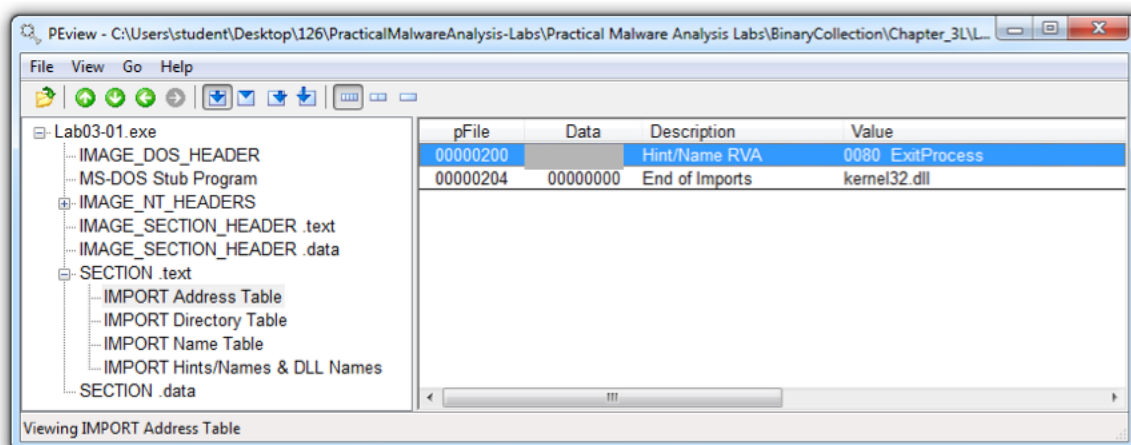
- Lab Files** from <http://practicalmalwareanalysis.com/labs/> -- download and unzip them.
- PEview** from <http://wjrdburn.com/software/> -- download and install
- Strings** from <http://technet.microsoft.com/en-us/sysinternals/bb897439> -- Click "**Download Strings**" to get **Strings.zip**; unzip it, and copy **strings.exe** to the C:\Windows\System32 folder.
- Process Monitor** from <http://technet.microsoft.com/en-us/sysinternals/bb896645> -- download and unzip
- Process Explorer** from <http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx> -- download and unzip
- Wireshark** from <http://www.wireshark.org/> -- download and install

Using PEview

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.

We will grade it by checking the Data value.



Press the **PrntScr**n key to capture an image of the whole desktop.

Open Paint and paste the image in with **Ctrl+V**.

Save this image with the filename "**Proj 4a from YOUR NAME**".

YOU MUST SUBMIT WHOLE-DESKTOP IMAGES TO GET FULL CREDIT!

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.

Above "advpack" there is a string starting with "j".

We will grade it by checking that string.



```
>>*K
40j
QQUP
ucj
j
advpack
hk?
~Pj
<2f
StubPath
SOFTWARE\Classes\http\shell\open\commandU
Software\Microsoft\Active Setup\Installed Components\
test
www.practicalmalwareanalysis.com
admin
VideoDriver
WinUMX32-
vmx32to64.exe
SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Ph?
U5h
U>U
SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
PWj
AppData
jeh
UQj
UiW
U%K_
```

Save this image with the filename "**Proj 4b from YOUR NAME**".

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

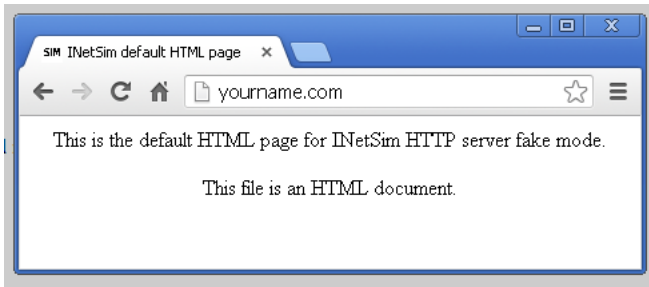
Start both the Windows and Linux VMs.

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:

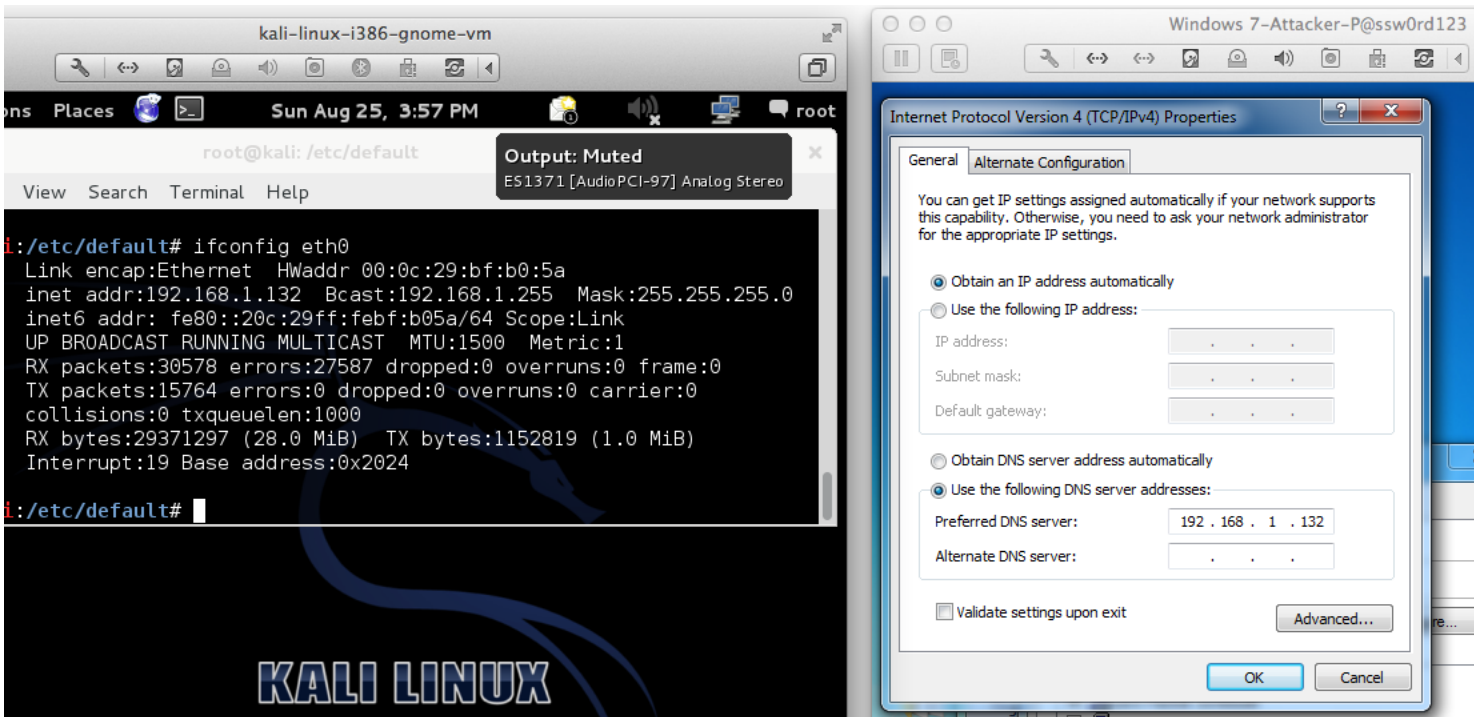


2. Setting the DNS Server

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

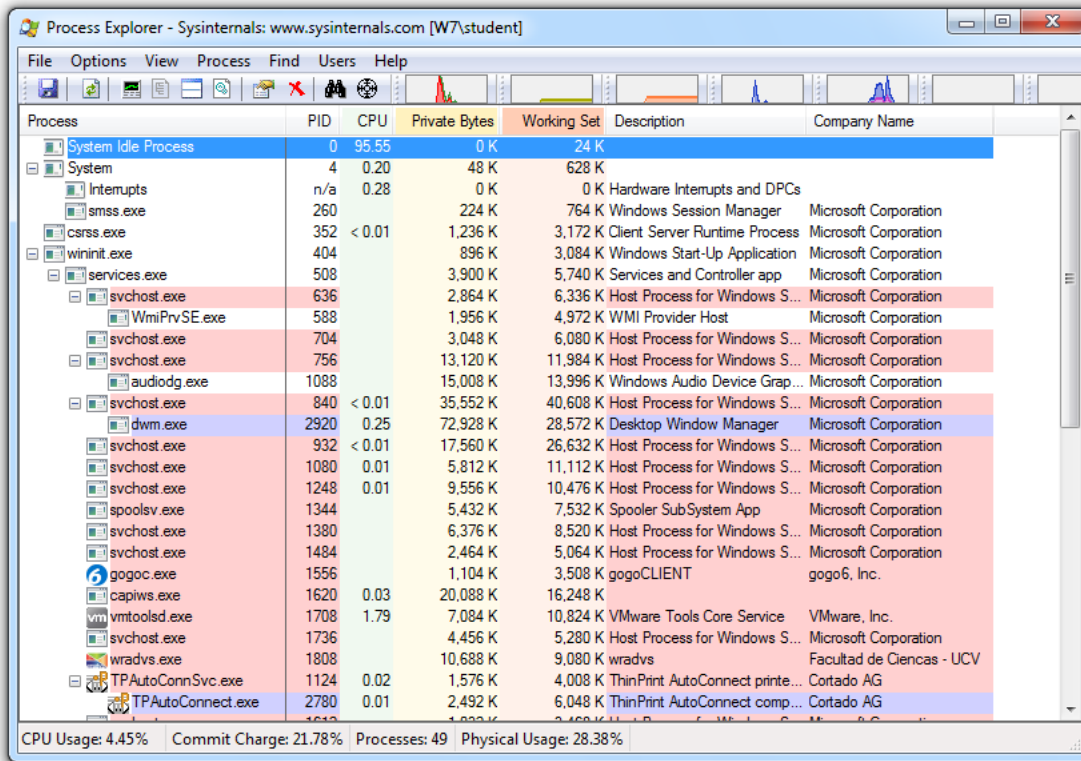
Double-click "Internet Protocol (TCP/IP)".

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

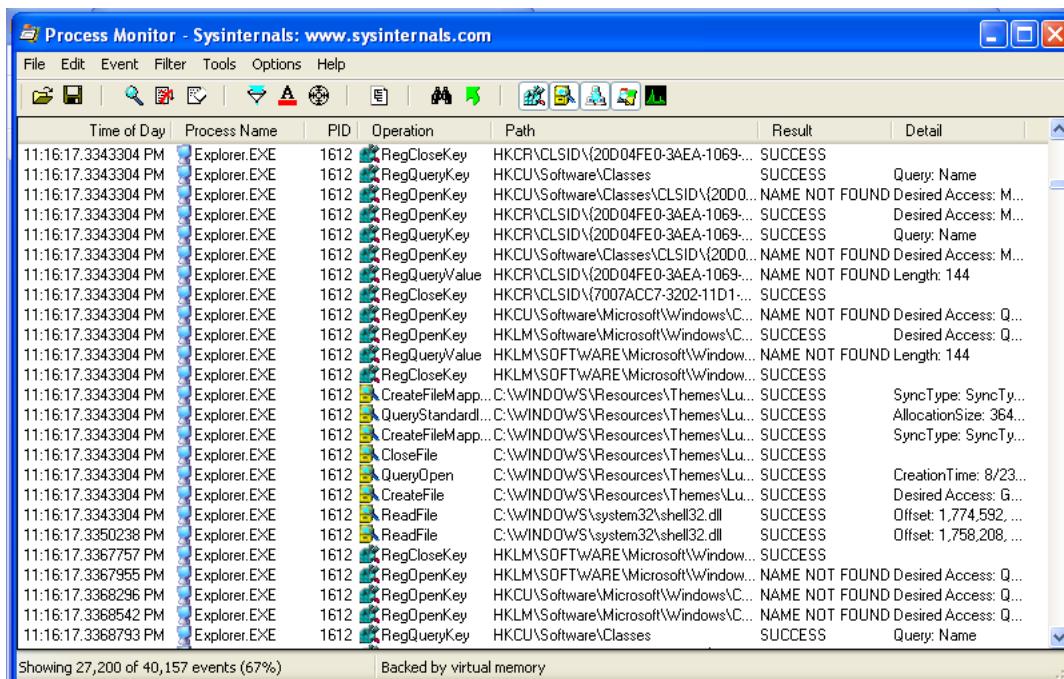
It's best to start Process Monitor last, so you can exclude all the harmless processes the other tools are using.

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.

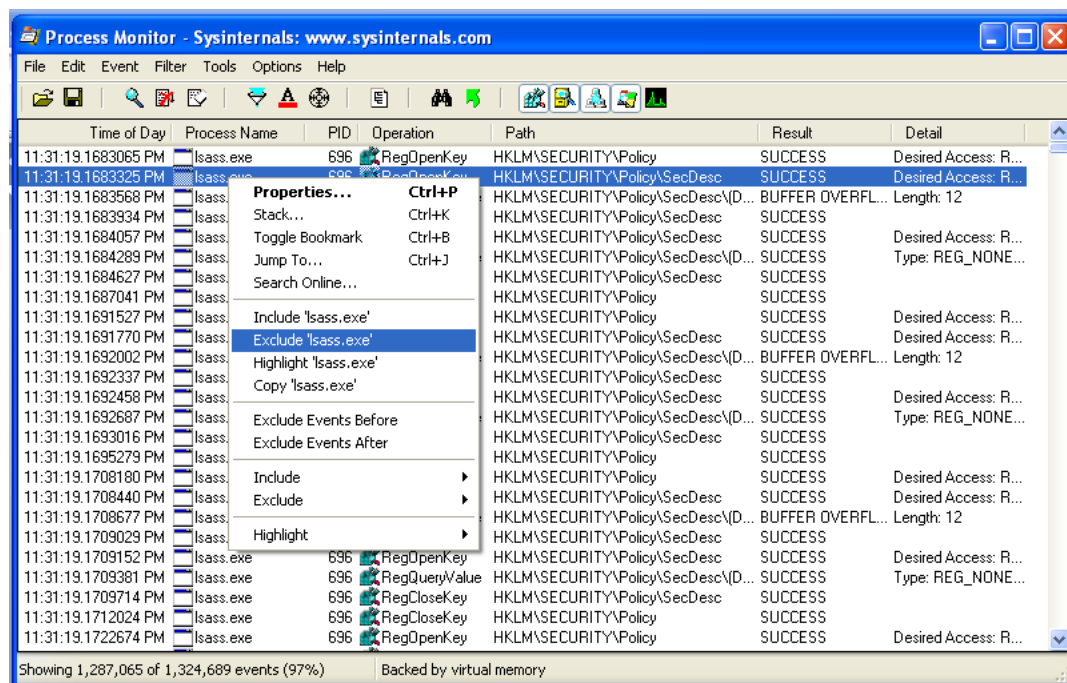
You should see Process Monitor, with a lot of processes visible, as shown below:



Excluding Harmless Processes

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

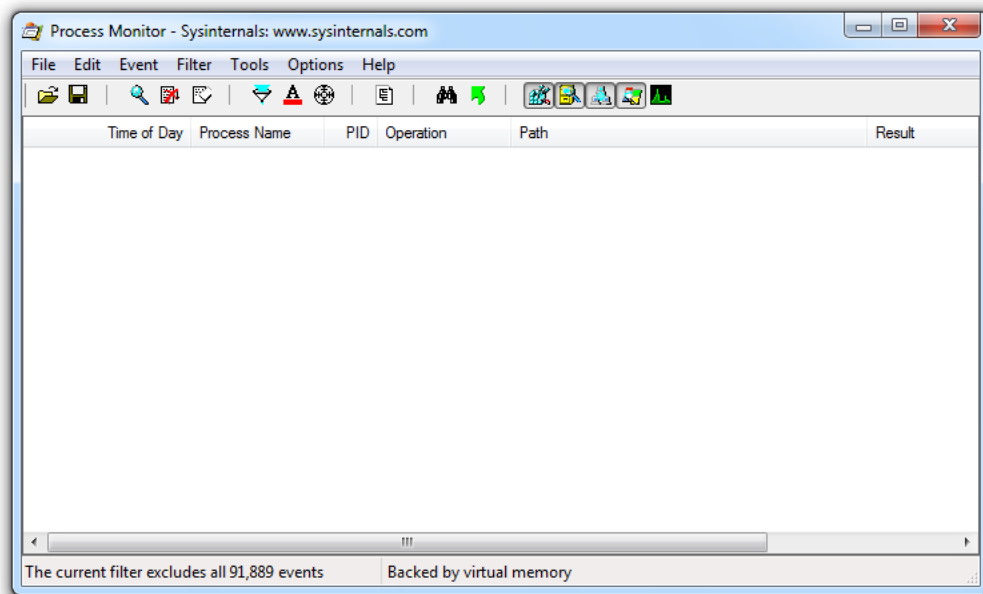
In Process Monitor, right-click the name of one of the visible processes, such as **lsass**, and click "exclude 'lsass.exe'", as shown below:



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, wuaucft.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.

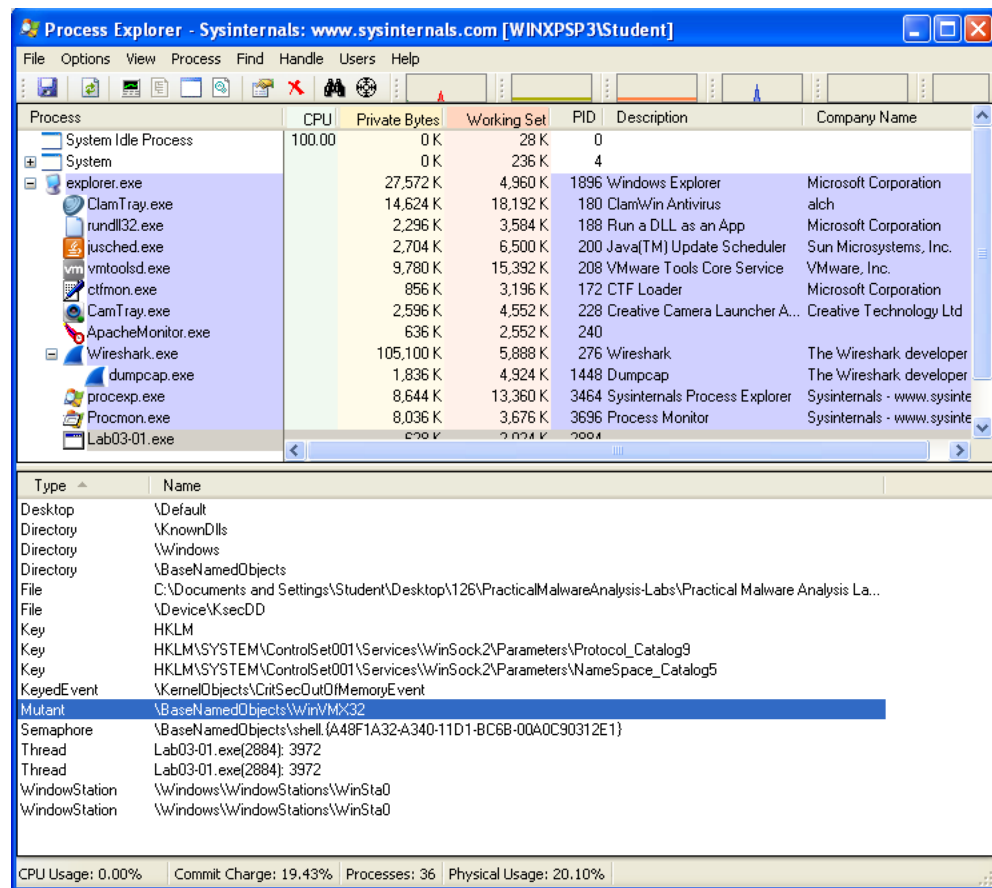
To make the malware run properly again, restart the VM, press F8, enter Safe Mode, and delete this file:

C:\Windows\System32\vmx32to64.exe

Then restart the VM in normal mode.

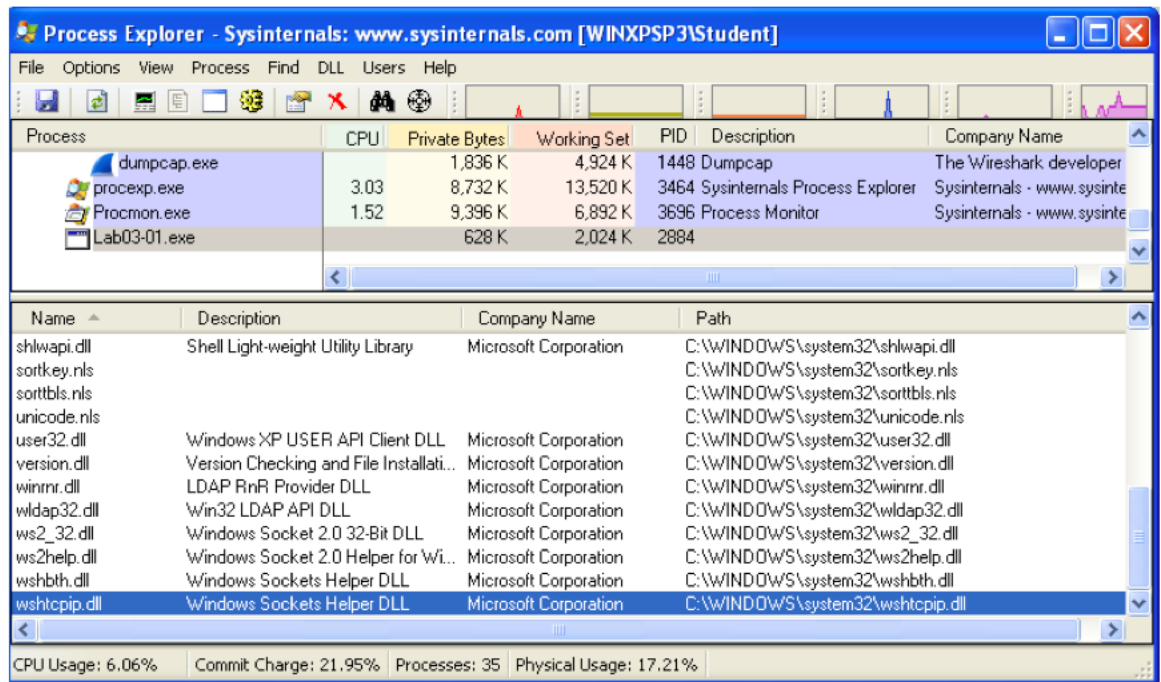
In Process Explorer, click **View**, "**Lower Pane View**", **Handles**.

You see the **WinVMX32** mutant, as highlighted below. A mutant, also called a mutex, is used for interprocess communication. A wonderful explanation of mutexes in terms of rubber chickens is [here](#).



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

Scroll to the bottom to find **ws2_32.dll** and **wshtcpip.dll**, as shown below. This shows that the malware has networking functionality.



Save this image with the filename "Proj 4c from YOUR NAME".

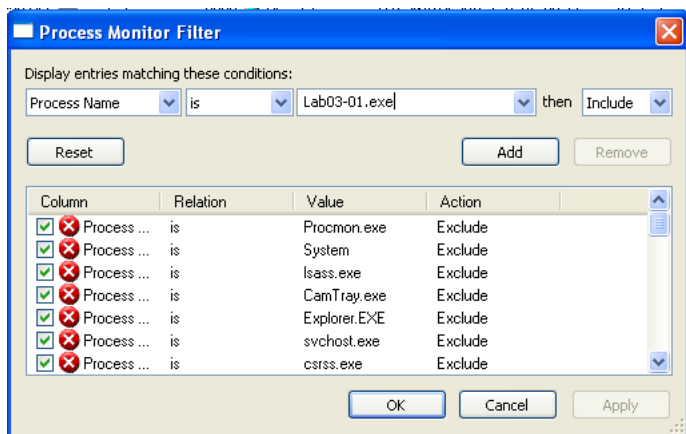
Make sure it contains the **ws2_32.dll** and **wshtcpip.dll** items. (In Server 2008, the second item appears in capital letters like this: **WSHTCPIP.DLL**)

Viewing the Malicious Process's Events in Process Monitor

In Process Monitor, click the magnifying glass icon on the toolbar to stop capturing events.

In Process Monitor, click **Filter**, **Filter**. Enter a Filter for "Process Name" is **Lab03-01.exe**, **Include**, as shown below.

Click **Add** to add the filter.

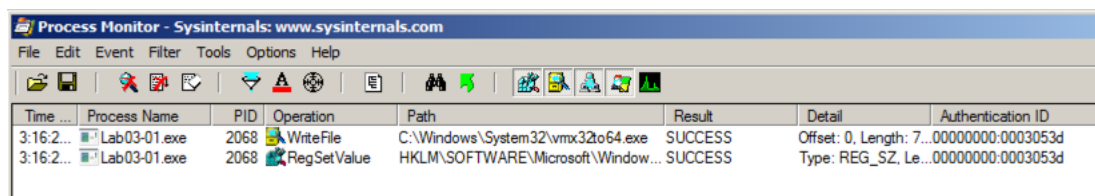


Add two more filters:

- Operation of **RegSetValue**
- Operation of **WriteFile**

Click **OK**.

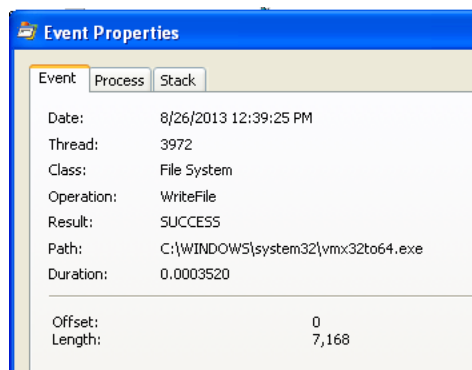
You end up the two events shown below. (Windows XP has an additional 8 events with Paths ending in "Cryptography\RNG\Seed" -- if you see those events, just ignore them.)



Eight of them are random number seed generation events and uninteresting. Only the second and third events are interesting.

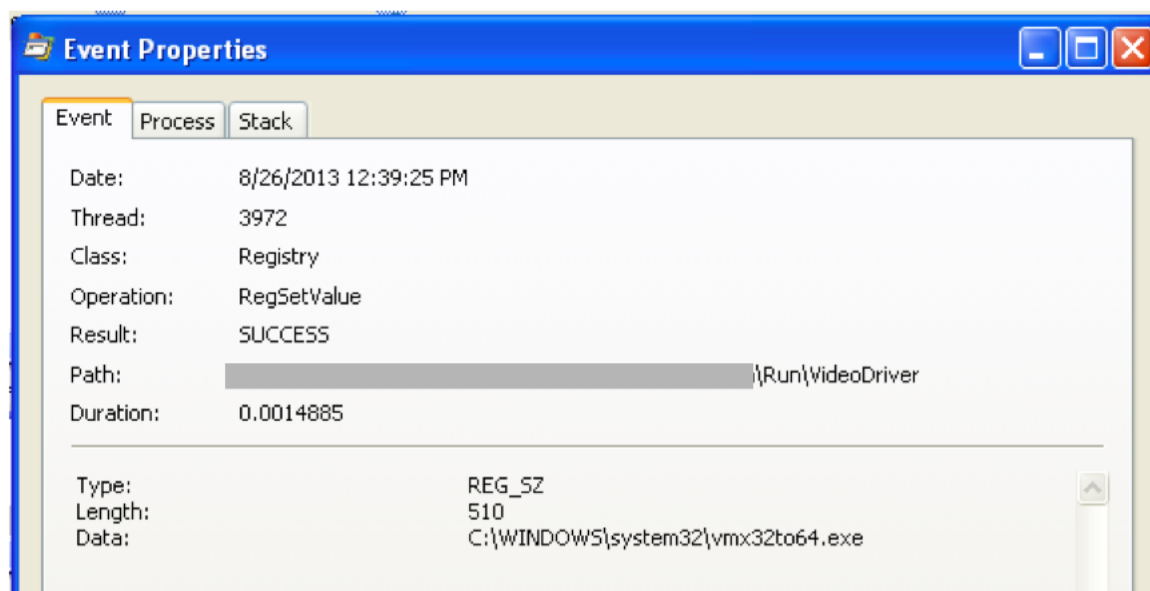
Double-click the event with a Path ending in **vmx32to64.exe**. The Properties sheet shows that this event creates a file named vmx32to64.exe, as shown below.

As explained in more detail in the book, this event has copied the malware itself to a file named vmx32to64.exe, so that filename is a useful indicator of infection.



Double-click the with a Path ending in **VideoDriver**.

This creates a new Run key in the registry named "VideoDriver" with a value of "C:\WINDOWS\system32\vmx32to64.exe" -- this is a persistence mechanism, to re-launch the malware when the machine restarts.]



Save this image with the filename "**Proj 4d from YOUR NAME**".

We will grade it based on the start of the Run registry key that is redacted above.

Viewing INetSim Logs

On the Kali Linux machine, click in the window running inetsim.

Press **Ctrl+C**. A message appears telling you where the Report file is, as shown below:


```
* daytime_13_udp - stopped (PID 3404)
* daytime_13_tcp - stopped (PID 3403)
* time_37_udp - stopped (PID 3402)
* time_37_tcp - stopped (PID 3401)
* pop3s_995_tcp - stopped (PID 3392)
* syslog_514_udp - stopped (PID 3400)
* ident_113_tcp - stopped (PID 3399)
* finger_79_tcp - stopped (PID 3398)
* ntp_123_udp - stopped (PID 3397)
* ftps_990_tcp - stopped (PID 3394)
* ftp_21_tcp - stopped (PID 3393)
* pop3_110_tcp - stopped (PID 3391)
* smtps_465_tcp - stopped (PID 3390)
* smtp_25_tcp - stopped (PID 3389)
* https_443_tcp - stopped (PID 3388)
* http_80_tcp - stopped (PID 3387)
* dns_53_tcp_udp - stopped (PID 3386)
* tftp_69_udp - stopped (PID 3395)
* irc_6667_tcp - stopped (PID 3396)
Simulation stopped.
Report written to '/var/log/inetsim/report/report.3384.txt' (45 lines)
=== INetSim main process stopped (PID 3384) ===
```

In the Linux machine, execute this command, replacing "report.3384.txt" with the correct name of your report file.

```
nano /var/log/inetsim/report/report.3384.txt
```

Scroll to the bottom and you should see DNS connections to **www.practicalmalwareanalysis.com**, as shown below:



Save this image with the filename "Proj 4e from YOUR NAME".

Make sure "www.practicalmalwareanalysis.com" is visible.

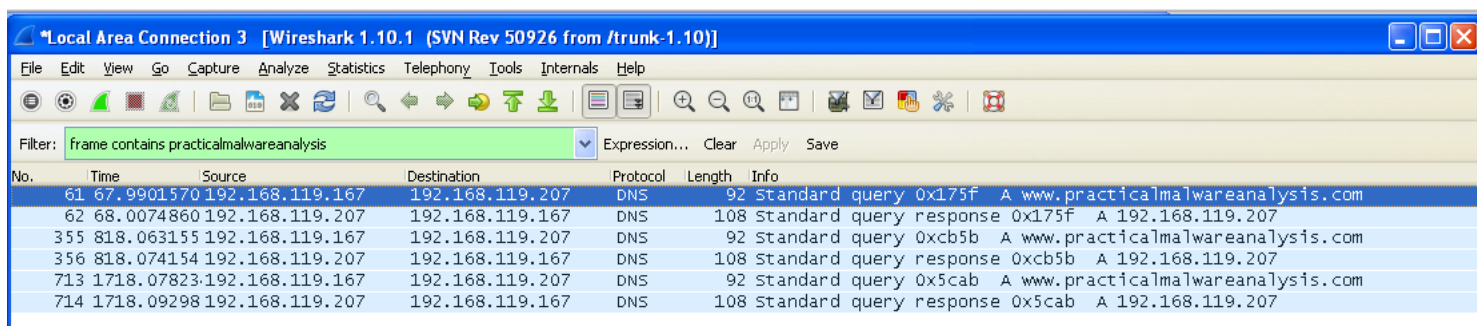
Viewing the Network Request in Wireshark

In the Windows machine, in Wireshark, click **Capture, Stop**.

At the top left of the Wireshark window, in the Filter bar, type a filter of

```
frame contains practicalmalwareanalysis
```

Press Enter to see the filtered packets, as shown below.



Click the line showing the first DNS request for www.practicalmalwareanalysis.com -- in the example above, it is packet 61.

In the top center of Wireshark, click the **Clear** button to clear the filter. The packets following the DNS request appear, as shown below.

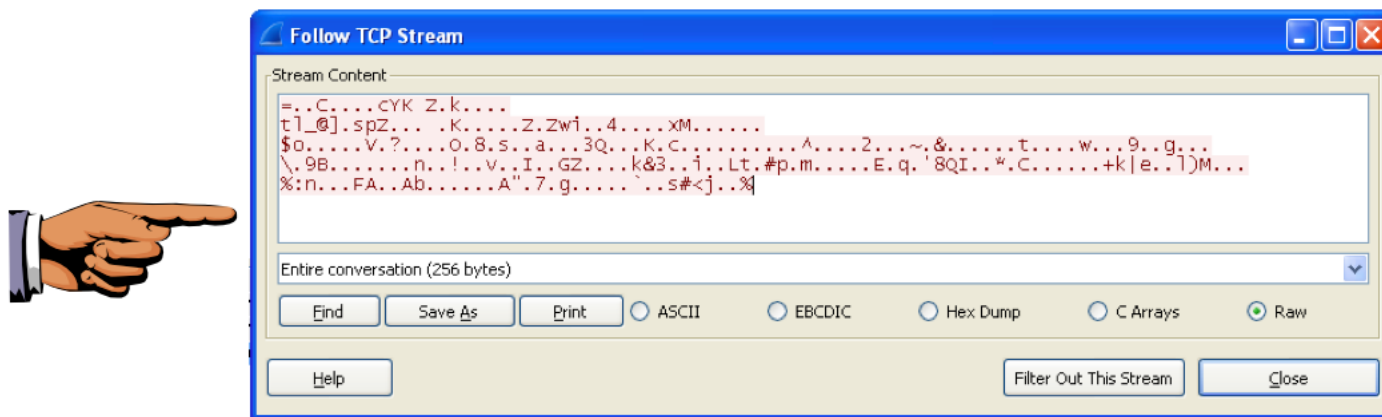
| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|------------|-----------------|-----------------|----------|--------|---|
| 61 | 67.9901570 | 192.168.119.167 | 192.168.119.207 | DNS | 92 | Standard query 0x175f A www.practicalmalwareanalysis.com |
| 62 | 68.0074860 | 192.168.119.207 | 192.168.119.167 | DNS | 108 | Standard query response 0x175f A 192.168.119.207 |
| 63 | 68.0121800 | 192.168.119.167 | 192.168.119.207 | TCP | 62 | hp-webadmin > https [SYN] Seq=0 win=64240 Len=0 MSS=1460 SACK_PERM |
| 64 | 68.0177040 | 192.168.119.207 | 192.168.119.167 | TCP | 62 | https > hp-webadmin [SYN, ACK] Seq=0 Ack=1 win=14600 Len=0 MSS=1460 |
| 65 | 68.0177350 | 192.168.119.167 | 192.168.119.207 | TCP | 54 | hp-webadmin > https [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 66 | 68.0178320 | 192.168.119.167 | 192.168.119.207 | SSL | 310 | Continuation Data |
| 67 | 68.0222380 | 192.168.119.207 | 192.168.119.167 | TCP | 60 | https > hp-webadmin [ACK] Seq=1 Ack=257 win=15544 Len=0 |
| 68 | 68.0277140 | 192.168.119.207 | 192.168.119.167 | TCP | 60 | https > hp-webadmin [RST, ACK] Seq=1 Ack=257 win=15544 Len=0 |

There is a TCP handshake here, but no actual HTTPS connection. A real HTTPS connection contains many more packets, such as "Client Hello", "Server Hello", and "Change Cipher Spec".

Find the SYN packet sent to the https port, which may be marked "443". In the example above, it is packet 63. Right-click it and click "**Follow TCP Stream**".

You see "Stream Content" containing 256 bytes of random packets, as shown below. These are **beacons** and are used by malware to notify the Command and Control server that the machine is infected and ready to use.

Since the data is random, your image will look different than the example below, but it should be 256 bytes in size.



Save this image with the filename "**Proj 4f from YOUR NAME**".

Make sure the "(256 bytes)" message is visible at the bottom.

Turning in your Project

Email the images showing to cnit.126sam@gmail.com with the subject line: **Proj 4 from YOUR NAME**

Last modified 2-1-16