

School of

Engineering and Computer Science

Te Kura Mātai Pūkaha, Pūrorohiko

CYBR 473 T1 2023

Malware and Reverse Engineering

Basic Dynamic Analysis

Chapter 3: “*Practical Malware Analysis: The Hands-on Guide to Dissecting Malicious Software*”, Michael Sikorski and Andrew Honig, 2012

Tweaking an Analysis VM

- Disable Hidden Extensions
- Show Hidden Files and Folders
- Disable ASLR
- Disable Windows Firewall
- Disable Windows Defender
- Mimic an End-User System
 - Disk size
 - RAM
 - Install software used by most end users
 - Copy over dummy files
 - Populate file history

MONITORING WITH PROCESS MONITOR

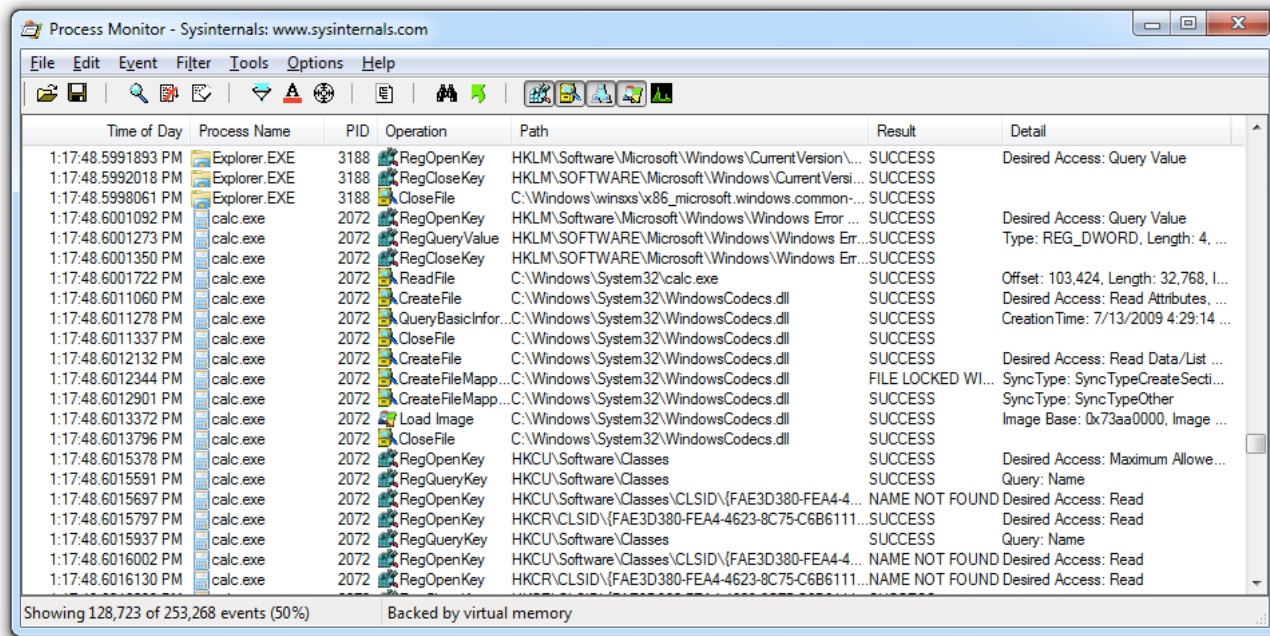


Process Monitor

- Monitors registry, file system, network, process, and thread activity
- All recorded events are kept, but you can filter the display to make it easier to find items of interest
- Don't run it too long, or it will fill up all RAM and crash the machine

Launching Calc.exe

- Many, many events recorded



The screenshot shows the Process Monitor application window with a list of events. The table below represents the data shown in the application.

Time of Day	Process Name	PID	Operation	Path	Result	Detail
1:17:48.5991893 PM	Explorer.EXE	3188	RegOpenKey	HKLM\Software\Microsoft\Windows\CurrentVersion\...	SUCCESS	Desired Access: Query Value
1:17:48.5992018 PM	Explorer.EXE	3188	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersi...	SUCCESS	
1:17:48.5998061 PM	Explorer.EXE	3188	CloseFile	C:\Windows\winsxs\x86_microsoft.windows.common...	SUCCESS	
1:17:48.6001092 PM	calc.exe	2072	RegOpenKey	HKLM\Software\Microsoft\Windows\Windows Error ...	SUCCESS	Desired Access: Query Value
1:17:48.6001273 PM	calc.exe	2072	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\Windows Err...	SUCCESS	Type: REG_DWORD, Length: 4, ...
1:17:48.6001350 PM	calc.exe	2072	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows\Windows Err...	SUCCESS	
1:17:48.6001722 PM	calc.exe	2072	ReadFile	C:\Windows\System32\calc.exe	SUCCESS	Offset: 103,424, Length: 32,768, I...
1:17:48.6011060 PM	calc.exe	2072	CreateFile	C:\Windows\System32\WindowsCodecs.dll	SUCCESS	Desired Access: Read Attributes, ...
1:17:48.6011278 PM	calc.exe	2072	QueryBasicInfor...	C:\Windows\System32\WindowsCodecs.dll	SUCCESS	CreationTime: 7/13/2009 4:29:14 ...
1:17:48.6011337 PM	calc.exe	2072	CloseFile	C:\Windows\System32\WindowsCodecs.dll	SUCCESS	
1:17:48.6012132 PM	calc.exe	2072	CreateFile	C:\Windows\System32\WindowsCodecs.dll	SUCCESS	Desired Access: Read Data/List ...
1:17:48.6012344 PM	calc.exe	2072	CreateFileMapp...	C:\Windows\System32\WindowsCodecs.dll	FILE LOCKED WL...	Sync Type: Sync TypeCreateSecti...
1:17:48.6012901 PM	calc.exe	2072	CreateFileMapp...	C:\Windows\System32\WindowsCodecs.dll	SUCCESS	Sync Type: Sync TypeOther
1:17:48.6013372 PM	calc.exe	2072	Load Image	C:\Windows\System32\WindowsCodecs.dll	SUCCESS	Image Base: 0x73aa0000, Image ...
1:17:48.6013796 PM	calc.exe	2072	CloseFile	C:\Windows\System32\WindowsCodecs.dll	SUCCESS	
1:17:48.6015378 PM	calc.exe	2072	RegOpenKey	HKCU\Software\Classes	SUCCESS	Desired Access: Maximum Allowe...
1:17:48.6015691 PM	calc.exe	2072	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
1:17:48.6015697 PM	calc.exe	2072	RegOpenKey	HKCU\Software\Classes\CLSID\{FAE3D380-FEA4-4...	NAME NOT FOUND	Desired Access: Read
1:17:48.6015797 PM	calc.exe	2072	RegOpenKey	HKCR\CLSID\{FAE3D380-FEA4-4623-8C75-C6B6111...	SUCCESS	Desired Access: Read
1:17:48.6015937 PM	calc.exe	2072	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
1:17:48.6016002 PM	calc.exe	2072	RegOpenKey	HKCU\Software\Classes\CLSID\{FAE3D380-FEA4-4...	NAME NOT FOUND	Desired Access: Read
1:17:48.6016130 PM	calc.exe	2072	RegOpenKey	HKCR\CLSID\{FAE3D380-FEA4-4623-8C75-C6B6111...	NAME NOT FOUND	Desired Access: Read

Showing 128,723 of 253,268 events (50%) Backed by virtual memory

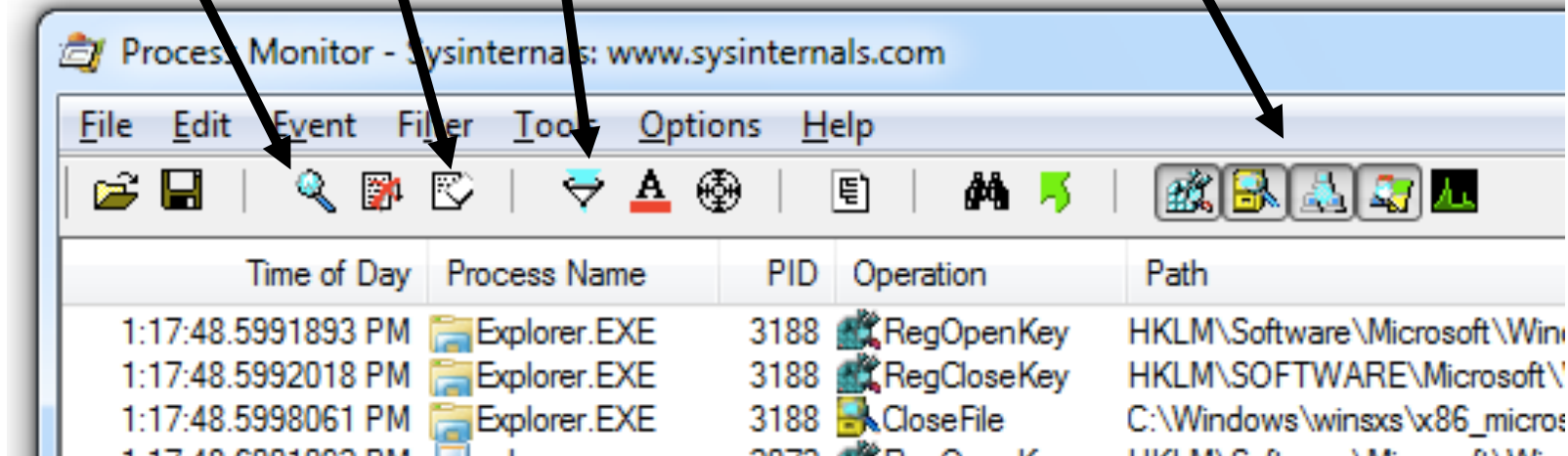
Process Monitor Toolbar

Start/Stop
Capture

Erase

Filter

Default Filters
Registry, File system, Network, Processes

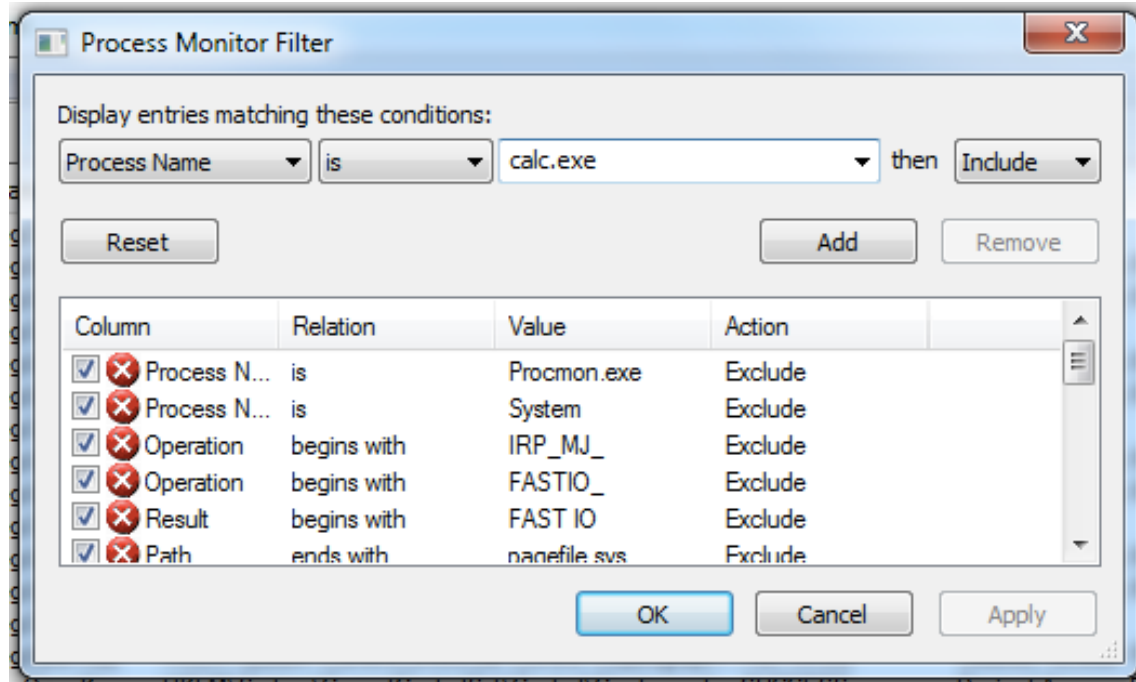


Filtering with **Exclude**

- One technique: hide normal activity before launching malware
- Right-click each Process Name and click **Exclude**
- Doesn't seem to work well with these samples

Filtering with **Include**

- Most useful filters: Process Name, Operation, and Detail

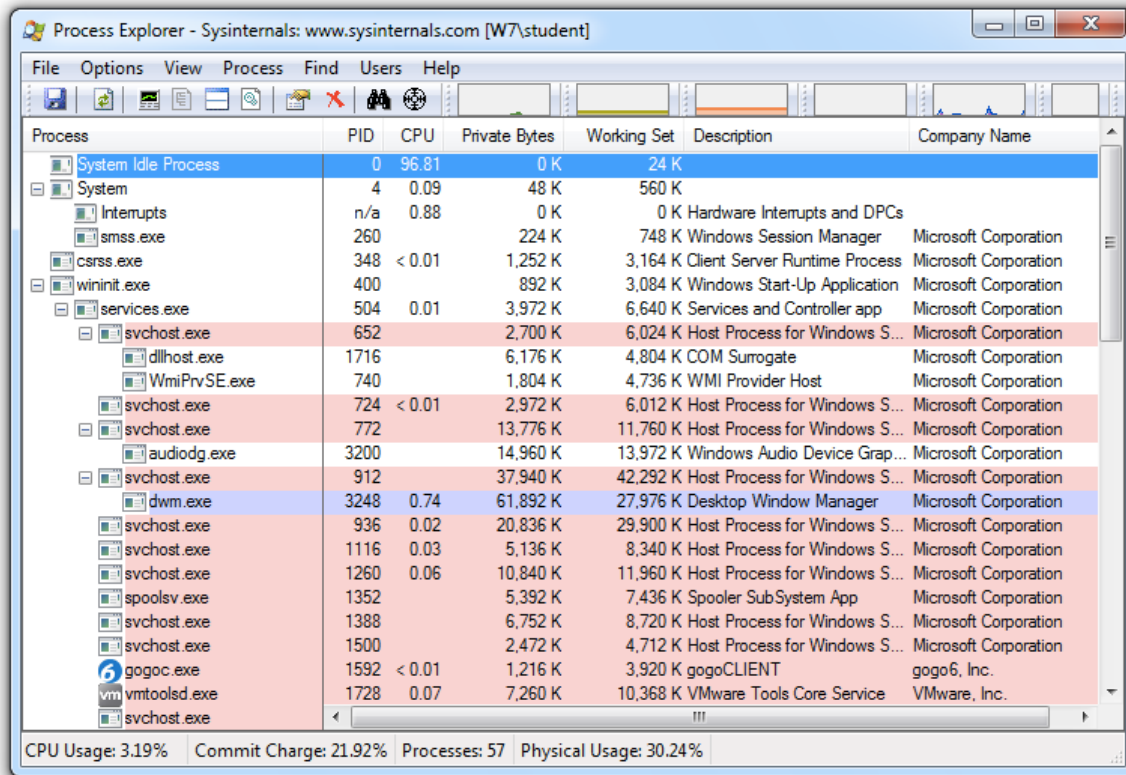


VIEWING PROCESSES WITH PROCESS EXPLORER

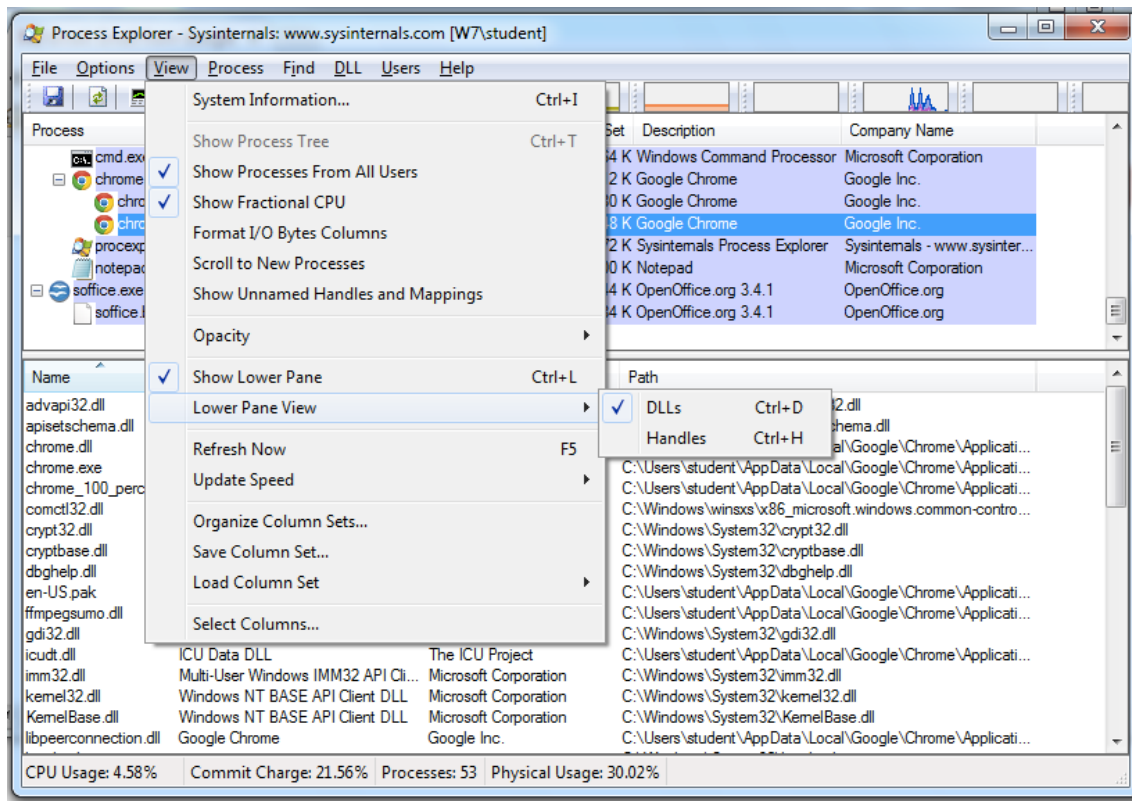


Viewing Processes with Process Explorer

- Services are pink
- Processes are blue
- New processes are green briefly
- Terminated processes are red

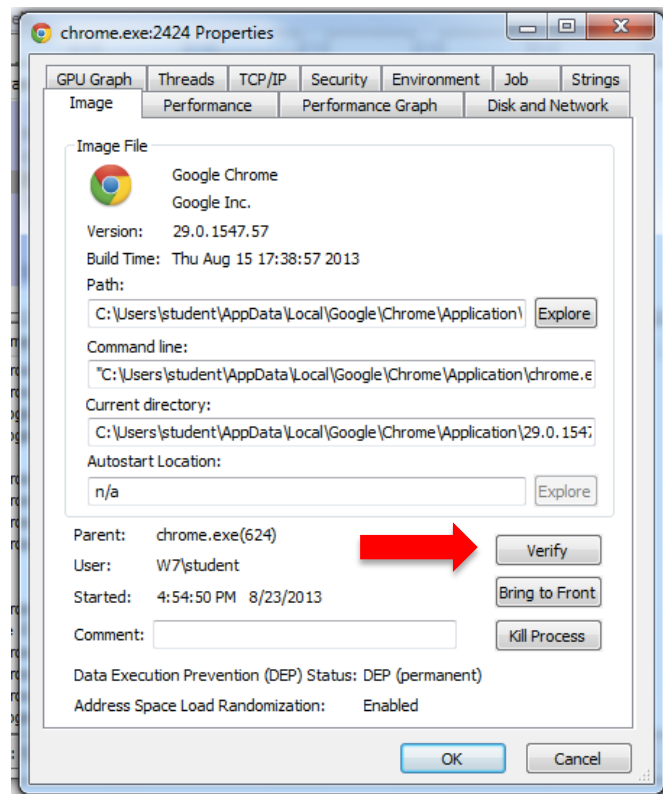


DLL Mode

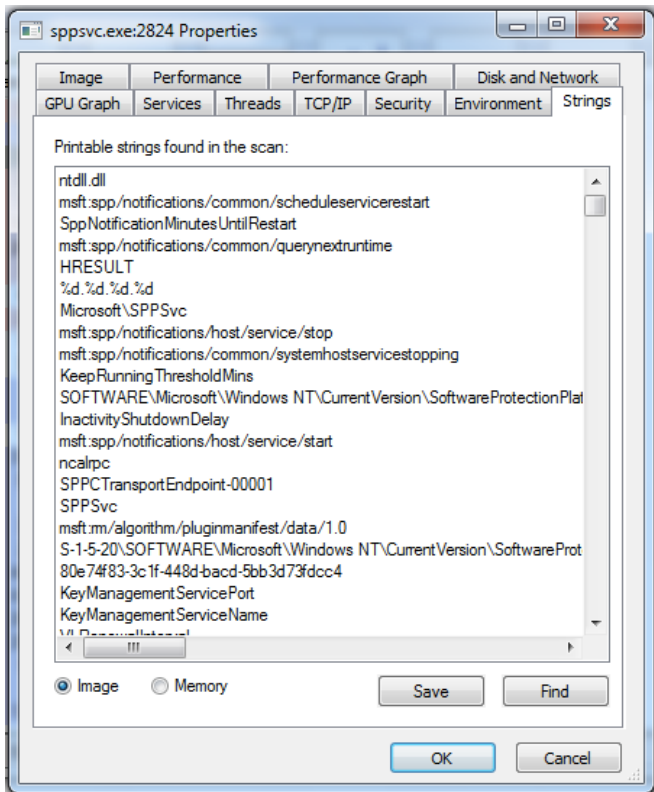


Properties

- Shows **DEP** (Data Execution Prevention) and **ASLR** (Address Space Layout Randomization) status
- Verify button checks the disk file's Windows signature
 - But not the RAM image, so it won't detect **process replacement**



Strings



Compare **Image** to **Memory** strings, if they are very different, it can indicate process replacement

Detecting Malicious Documents

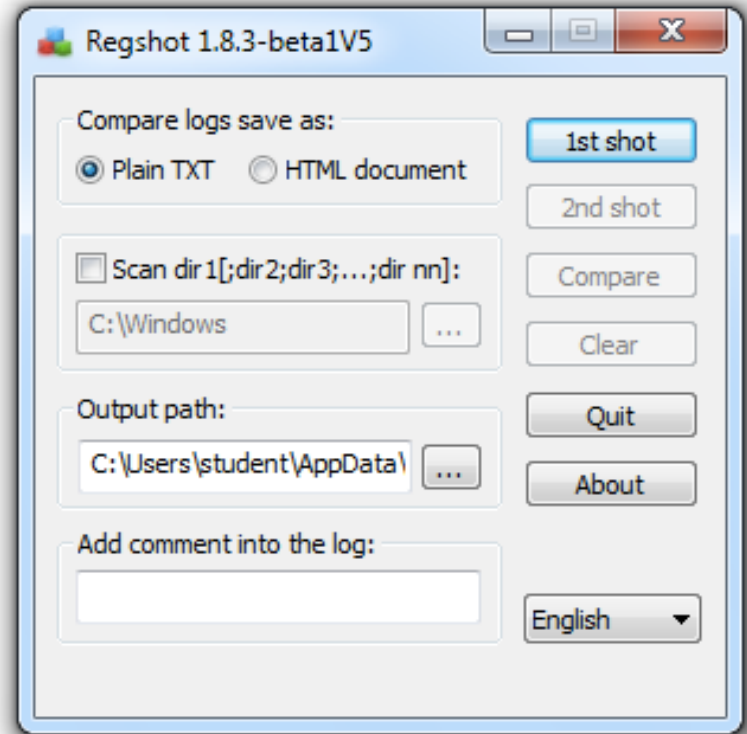
- Open the document (e.g. PDF) on a system with a **vulnerable application**
- Watch Process Explorer to see if it launches a process
- The Image tab of that process's Properties sheet will show where the malware is



COMPARING REGISTRY SNAPSHOTS WITH REGSHOT

Regshot

- Take 1st shot
- Run malware
- Take 2nd shot
- Compare them to see what registry keys were changed

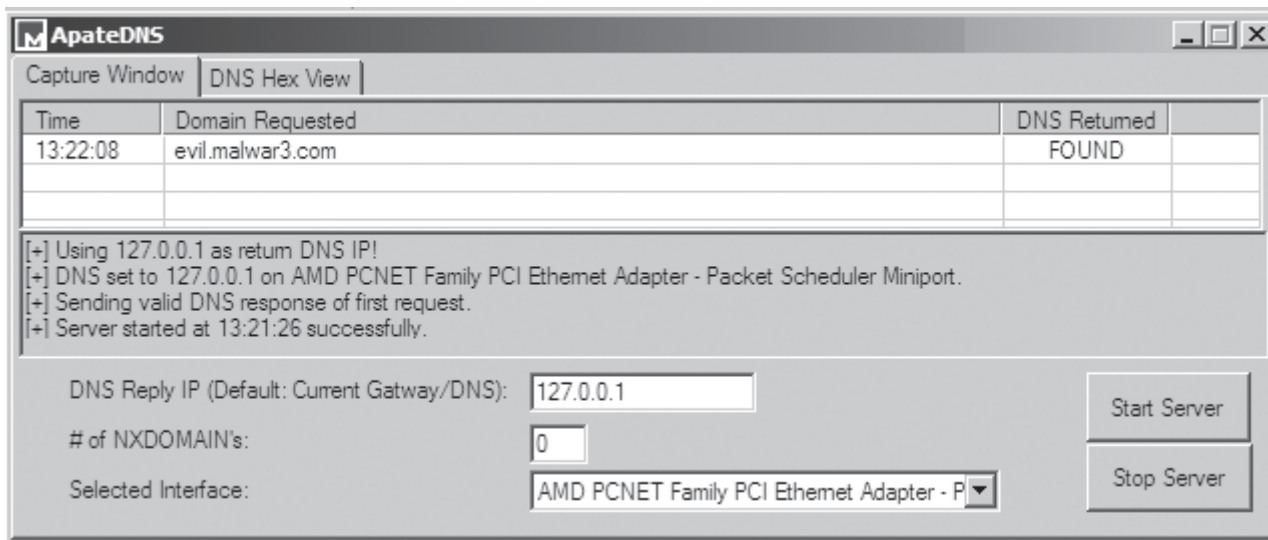


FAKING A NETWORK



ApateDNS

- Spoofing DNS responses to a user-specified IP address
- Listening on UDP port 53 on the local machine
- Responding to DNS requests using a predefined IP address

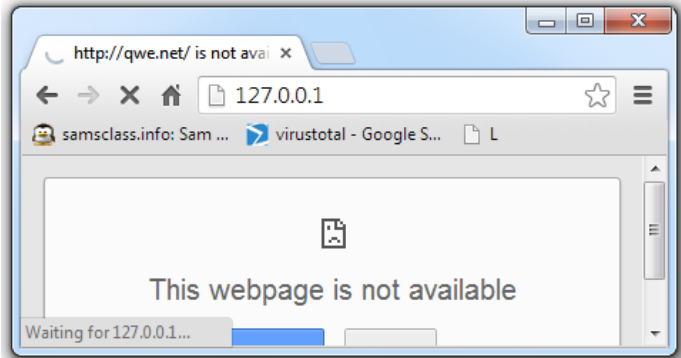


Ncat Listener

- Using Ncat.exe, you can listen on a single TCP port in Windows
 - In Linux, use nc (netcat)
- This will allow malware to complete a TCP handshake, so you get some rudimentary information about its requests
- But it's not a real server, so it won't reply to requests after the handshake

Monitoring with Ncat (included with Nmap)

```
Administrator: cmd - Shortcut (2) - ncat -l 80
C:\Windows\System32>ncat -l 80
GET / HTTP/1.1
Host: 127.0.0.1
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/29.0.1547.57 Safari/537.36
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
```



```
C:\> nc -l -p 80 ❶
POST /cq/frame.htm HTTP/1.1
Host: www.google.com ❷
User-Agent: Mozilla/5.0 (Windows; Windows NT 5.1; TWfSd2FyZUh1bnRlcm91bnQ=; rv:1.38)
Accept: text/html, application
Accept-Language: en-US, en;q=
Accept-Encoding: gzip, deflate
Keep-Alive: 300
Content-Type: application/x-form-urlencoded
Content-Length
```

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
```

```
Z:\Malware> ❸
```

Packet Sniffing with Wireshark

The screenshot displays the Wireshark interface for a network capture on an Intel(R) PRO/1000 MT Network Connection. The filter is set to 'http'. The packet list shows several HTTP requests and responses. The selected packet (No. 1381) is an HTTP 200 OK response from 199.16.156.21 to 192.168.119.154. The packet details pane shows the following structure:

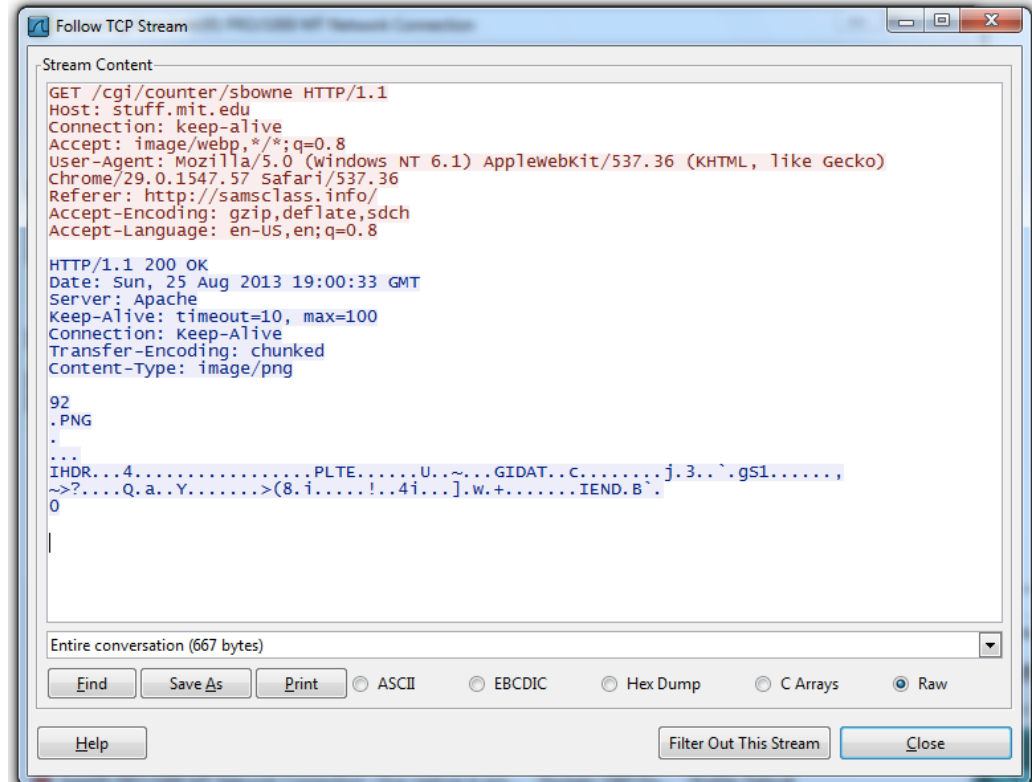
- Frame 48: 437 bytes on wire (3496 bits), 437 bytes captured (3496 bits)
- Ethernet II, Src: Vmware_52:34:92 (00:0c:29:52:34:92), Dst: Vmware_e3:22:f1 (00:50:56:e3:22:f1)
- Internet Protocol Version 4, Src: 192.168.119.154 (192.168.119.154), Dst: 141.101.1...

The raw packet data (hex and ASCII) is shown below:

```
0000 00 50 56 e3 22 f1 00 0c 29 52 34 92 08 00 45 00 .PV."... )R4...E.
0010 01 a7 10 25 40 00 80 06 00 00 c0 a8 77 9a 8d 65 ...%@... ..w.e
0020 75 98 05 a9 00 50 0c 80 cd 2e dc ff 73 93 50 18 u...P... ..s.P.
0030 fa f0 3c da 00 00 47 45 54 20 2f 20 48 54 54 50 ..<...GE T / HTTP
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 73 61 6d 73 /1.1..Ho st: sams
0050 63 6c 61 73 73 2e 69 6e 66 6f 0d 0a 43 6f 6e 6e class.in fo..Conn
0060 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 ection: keep-ali
0070 76 65 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 ve..Acce pt: text
0080 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f /html,ap plicatio
0090 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c n/xhtml+ xml,appl
00a0 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e ication/ xml:a=0.
```

Follow TCP Stream

- Can save files from streams here too

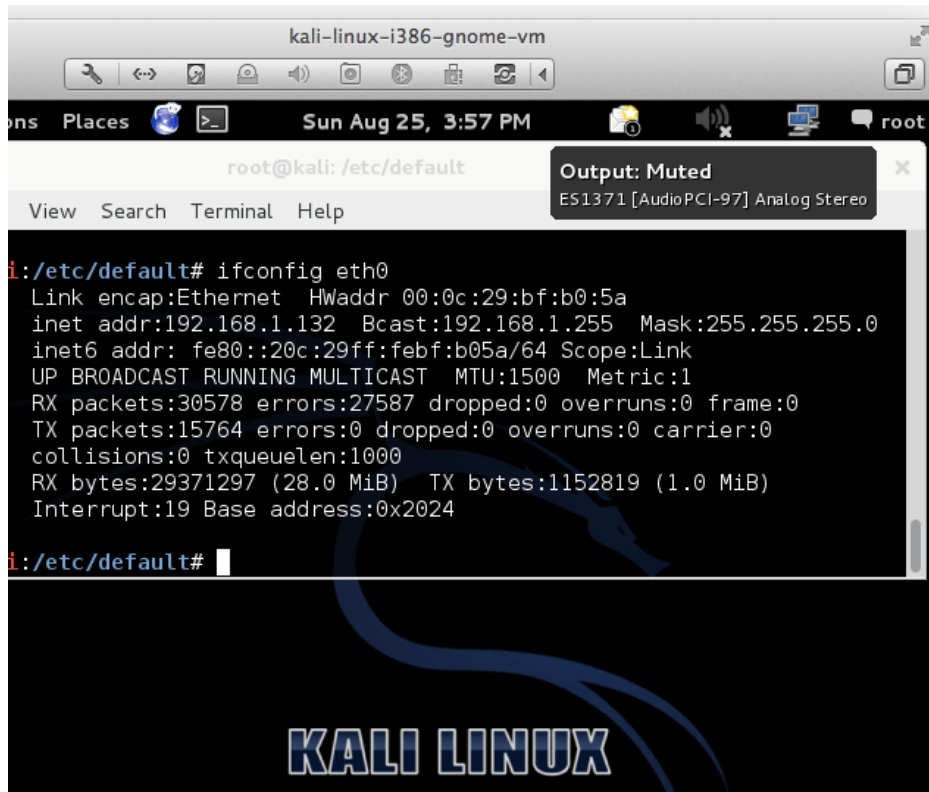


USING INETSIM

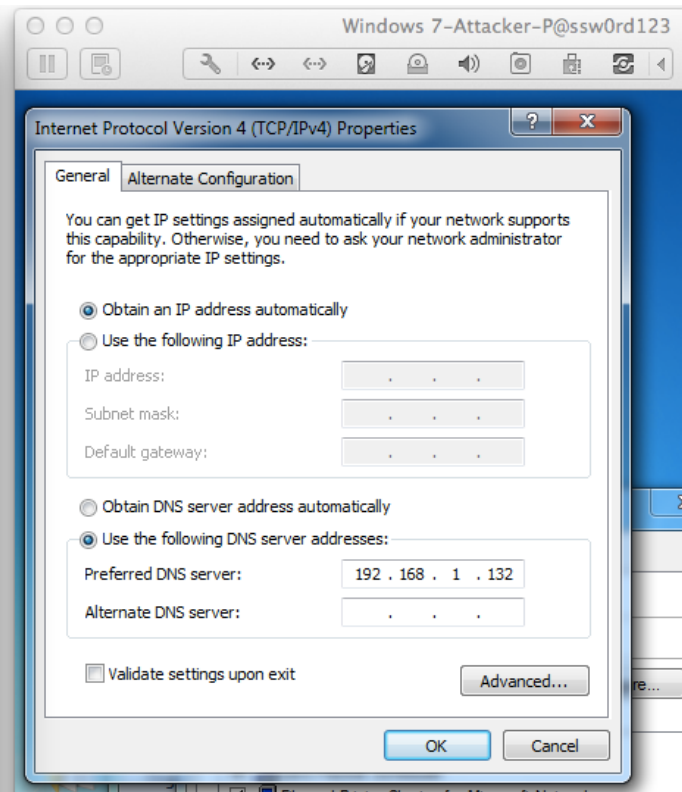
INetSim

- Included in Kali Linux
- Simulates the Internet, including
 - HTTP / HTTPS
 - SMTP, POP3
 - DNS
 - FTP
 - Much more

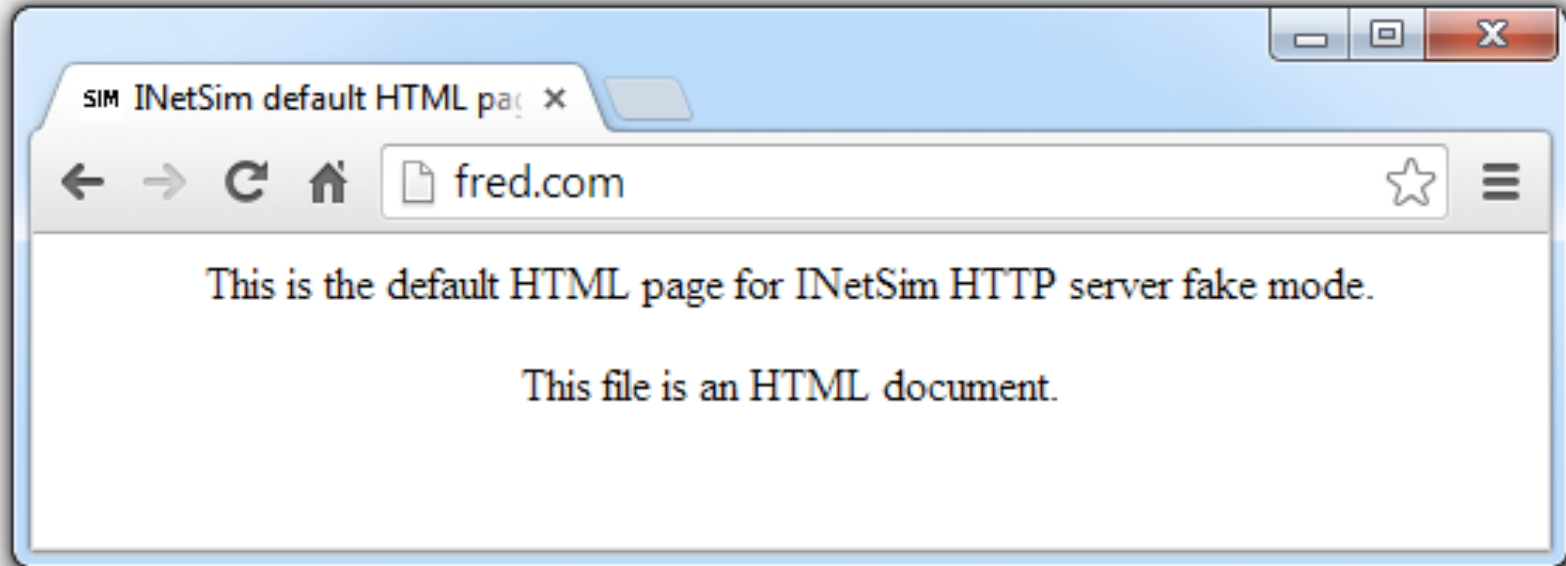
INetSim



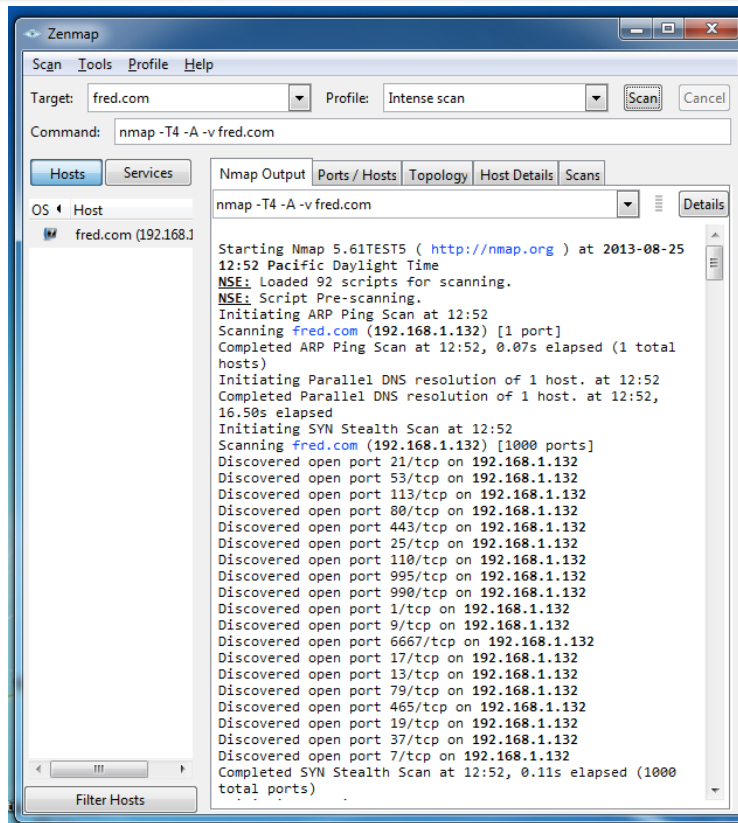
```
kali-linux-i386-gnome-vm
root@kali: /etc/default
Output: Muted
ES1371 [AudioPCI-97] Analog Stereo
View Search Terminal Help
root@kali: /etc/default# ifconfig eth0
Link encap:Ethernet HWaddr 00:0c:29:bf:b0:5a
inet addr:192.168.1.132 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:febf:b05a/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:30578 errors:27587 dropped:0 overruns:0 frame:0
TX packets:15764 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:29371297 (28.0 MiB) TX bytes:1152819 (1.0 MiB)
Interrupt:19 Base address:0x2024
root@kali: /etc/default#
```



INetSim Fools a Browser



INetSim Fools Nmap



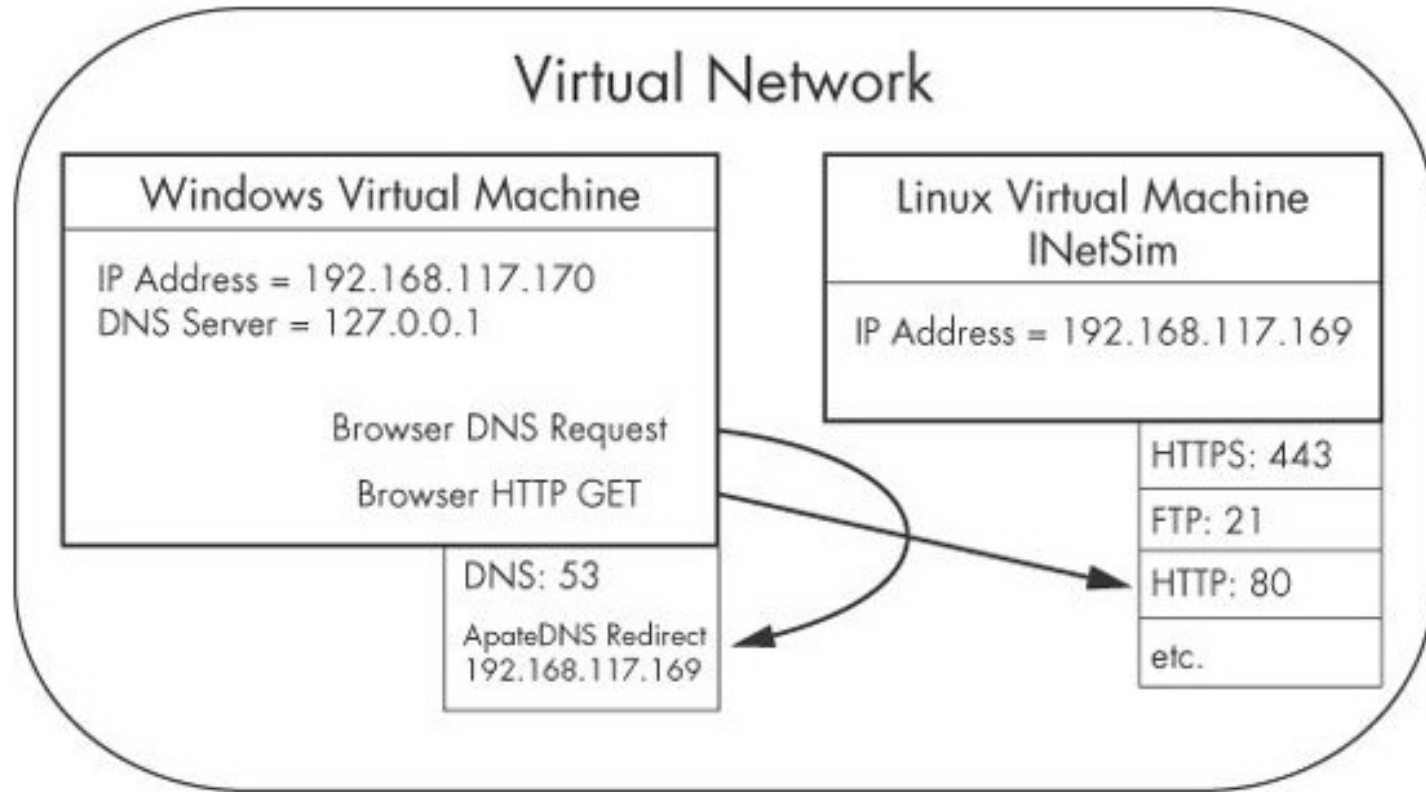
BASIC DYNAMIC TOOLS IN PRACTICE



Using the Tools

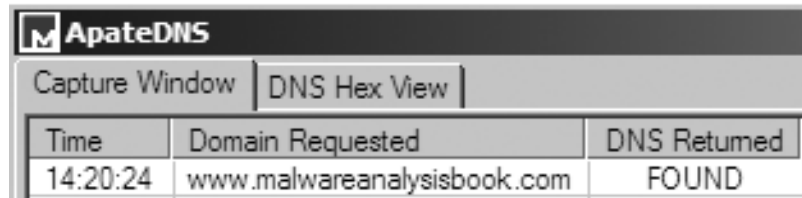
- Procmon
 - Filter on the malware executable name and clear all events just before running it
- Process Explorer
- Regshot
- Virtual Network with INetSim
- Wireshark

Example of a Virtual Network



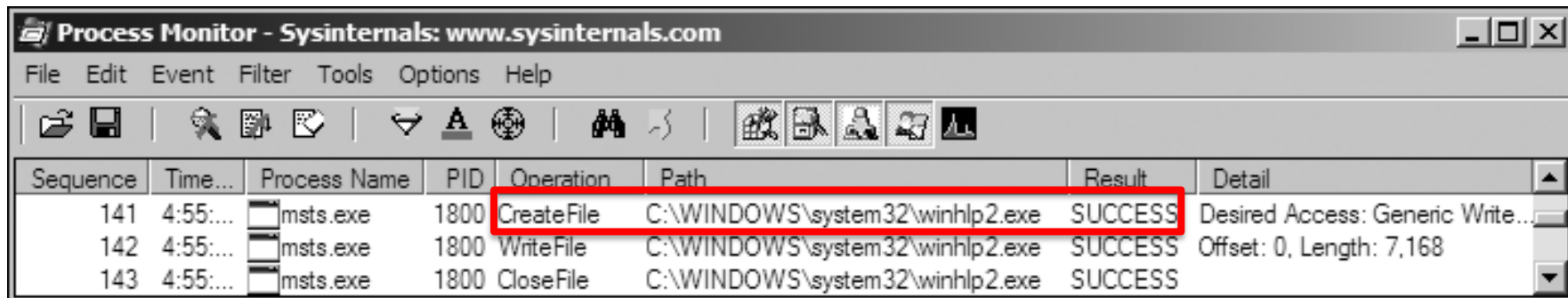
Examining the malware *msts.exe*

- Examine ApateDNS to see if DNS requests were performed



Time	Domain Requested	DNS Returned
14:20:24	www.malwareanalysisbook.com	FOUND

- Review the Procmon results for file system modifications



Sequence	Time...	Process Name	PID	Operation	Path	Result	Detail
141	4:55:...	msts.exe	1800	CreateFile	C:\WINDOWS\system32\winhlp2.exe	SUCCESS	Desired Access: Generic Write...
142	4:55:...	msts.exe	1800	WriteFile	C:\WINDOWS\system32\winhlp2.exe	SUCCESS	Offset: 0, Length: 7,168
143	4:55:...	msts.exe	1800	CloseFile	C:\WINDOWS\system32\winhlp2.exe	SUCCESS	

Examining the malware *msts.exe* (cont.)

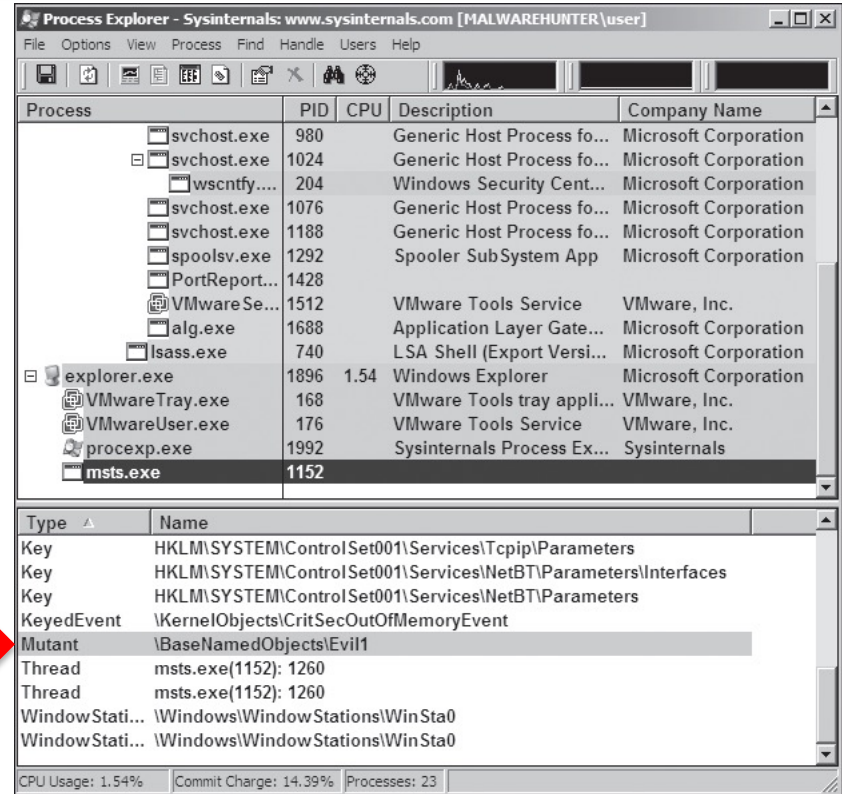
- Compare the two snapshots taken with Regshot to identify changes

Values added:3

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\winhlp: C:\WINDOWS\system32\winhlp2.exe

Examining the malware *msts.exe* (cont.)

- Use Process Explorer to examine the process to determine whether it creates **mutexes** or listens for incoming connections



The screenshot shows Process Explorer with the *msts.exe* process selected. The process list table is as follows:

Process	PID	CPU	Description	Company Name
svchost.exe	980		Generic Host Process fo...	Microsoft Corporation
svchost.exe	1024		Generic Host Process fo...	Microsoft Corporation
wsentfy...	204		Windows Security Cent...	Microsoft Corporation
svchost.exe	1076		Generic Host Process fo...	Microsoft Corporation
svchost.exe	1188		Generic Host Process fo...	Microsoft Corporation
spoolsv.exe	1292		Spooler SubSystem App	Microsoft Corporation
PortReport...	1428			
VMwareSe...	1512		VMware Tools Service	VMware, Inc.
alg.exe	1688		Application Layer Gate...	Microsoft Corporation
lsass.exe	740		LSA Shell (Export Versi...	Microsoft Corporation
explorer.exe	1896	1.54	Windows Explorer	Microsoft Corporation
VMwareTray.exe	168		VMware Tools tray appli...	VMware, Inc.
VMwareUser.exe	176		VMware Tools Service	VMware, Inc.
procexp.exe	1992		Sysinternals Process Ex...	Sysinternals
msts.exe	1152			

The system objects table for *msts.exe* is as follows:

Type	Name
Key	HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters
Key	HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters\Interfaces
Key	HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters
KeyedEvent	\KernelObjects\CritSecOutOfMemoryEvent
Mutant	\BaseNamedObjects\Evil1
Thread	msts.exe(1152): 1260
Thread	msts.exe(1152): 1260
Window Stati...	\Windows\Window Stations\WinSta0
Window Stati...	\Windows\Window Stations\WinSta0

A red arrow points to the **Mutant** entry in the system objects table.

Process Explorer status bar: CPU Usage: 1.54% | Commit Charge: 14.39% | Processes: 23

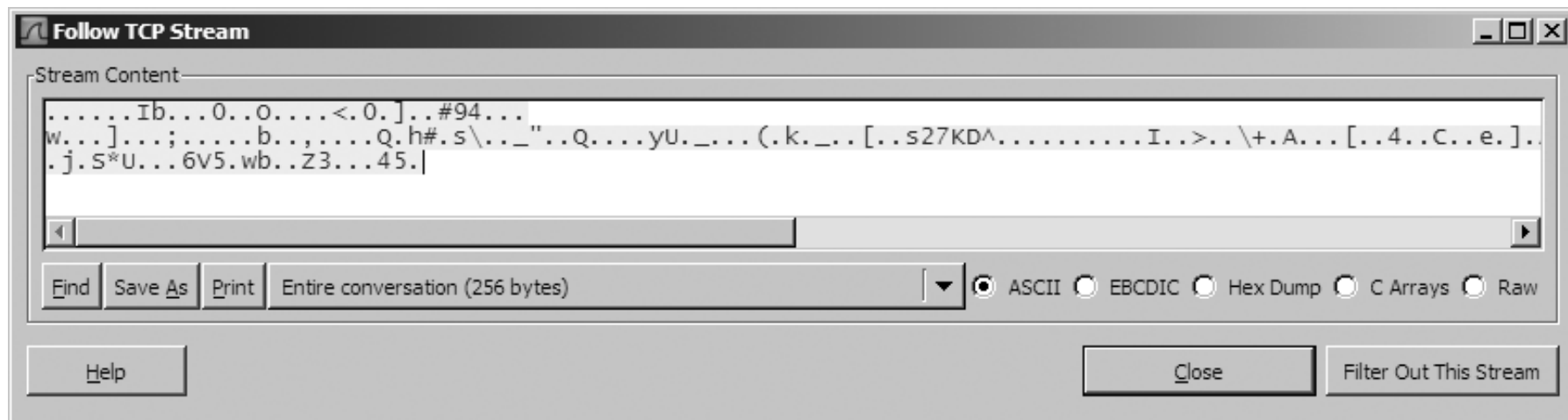
Examining the malware *msts.exe* (cont.)

- Review the **INetSim** logs for requests and attempted connections on standard services

```
[2010-X] [15013] [https 443/tcp 15199] [192.168.117.128:1043] connect
[2010-X] [15013] [https 443/tcp 15199] [192.168.117.128:1043]
Error setting up SSL: SSL accept attempt failed with unknown error
Error:140760FC:SSL routines:SSL23_GET_CLIENT_HELLO:unknown protocol
[2010-X] [15013] [https 443/tcp 15199] [192.168.117.128:1043] disconnect
```

Examining the malware *msts.exe* (cont.)

- Review the Wireshark capture for network traffic generated by the malware





END OF LECTURE. THANK YOU.