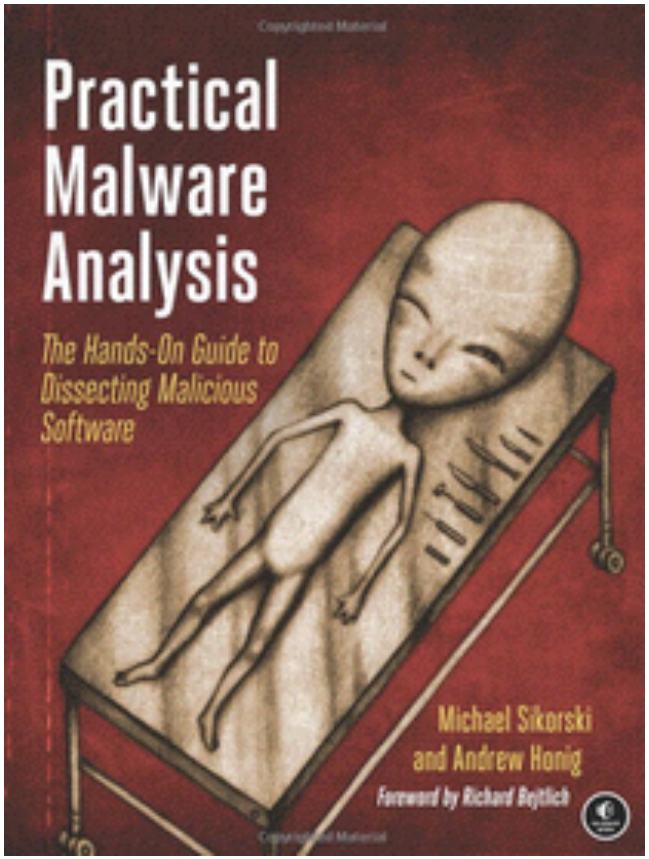
Practical Malware Analysis



Ch 2: Malware Analysis in Virtual Machines

Updated 1-16-17

Dynamic Analysis

- Running malware deliberately, while monitoring the results
- Requires a **safe environment (isolated)**
- Must prevent malware from spreading to production machines
- Real machines can be **airgapped** –no network connection to the Internet or to other machines

Real Machines

- Disadvantages
  - No Internet connection, so parts of the malware may not work
  - Can be difficult to remove malware, so re-imaging the machine will be necessary
- Advantage
  - Some malware detects virtual machines and won't run properly in one

Virtual Machines

- The most common method
- We'll do it that way
- This protects the host machine from the malware
  - Except for a few very rare cases of malware that escape the virtual machine and infect the host

VMware Player

- Free but limited
- Cannot take snapshots
- VMware Workstation or Fusion is a better choice, but they cost money
- You could also use VirtualBox, Hyper-V, Parallels, or Xen.

Creating VMware

- Determine the requirements
  -Ram (4GB), HDD (20GB)
- VMware will make a lot of choices for you and, these choices will dothe job.
- Next, you'll install your OS and applications.
- After you've installed the OS, you can install any required applications.
- Finally, you'll install VMware Tools.
  - shared folders, drag-and-drop file transfer

Windows XP

- The malware we are analyzing targets Windows XP, as most malware does
- Win XP has passed its end-of-life, so we'll use Windows Server 2008

Configuring VMware

- You can disable networking by disconnecting the virtual network adapter
- Host-only networking allows network traffic to the host but not the Internet

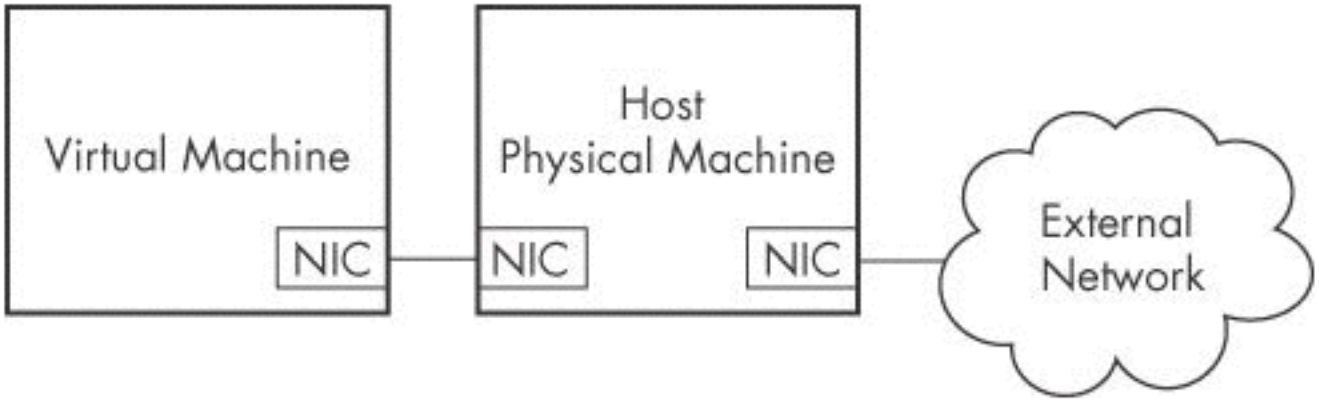


Figure 3-3. Host-only networking in VMware

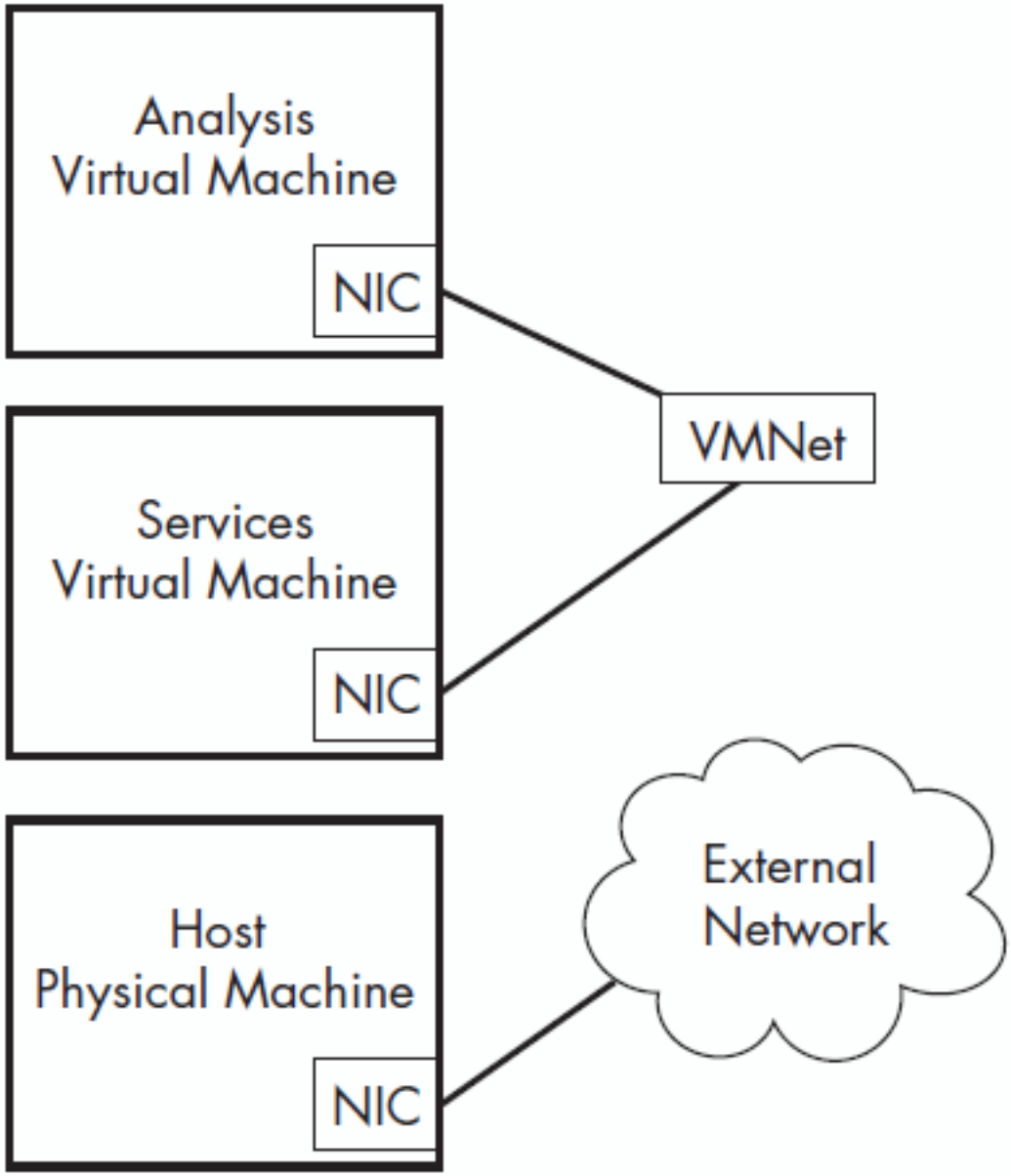


Figure 2-4: Custom networking in VMware

Connecting Malware to the Internet

- NAT mode lets VMs see each other and the Internet, but puts a virtual router between the VM and the LAN
- Bridged networking connects the VM directly to the LAN
- Can allow malware to do some harm or spread – controversial
- You could send spam or participate in a DDoS attack

Snapshots

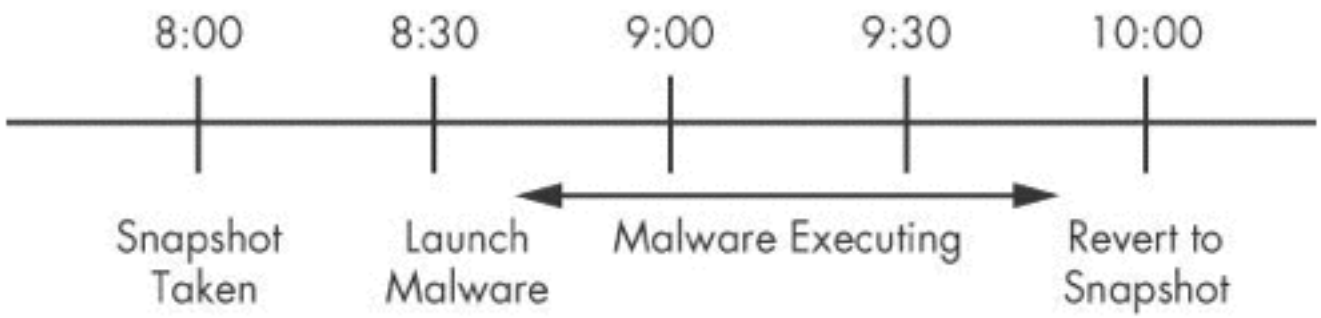


Figure 3-5. Snapshot timeline

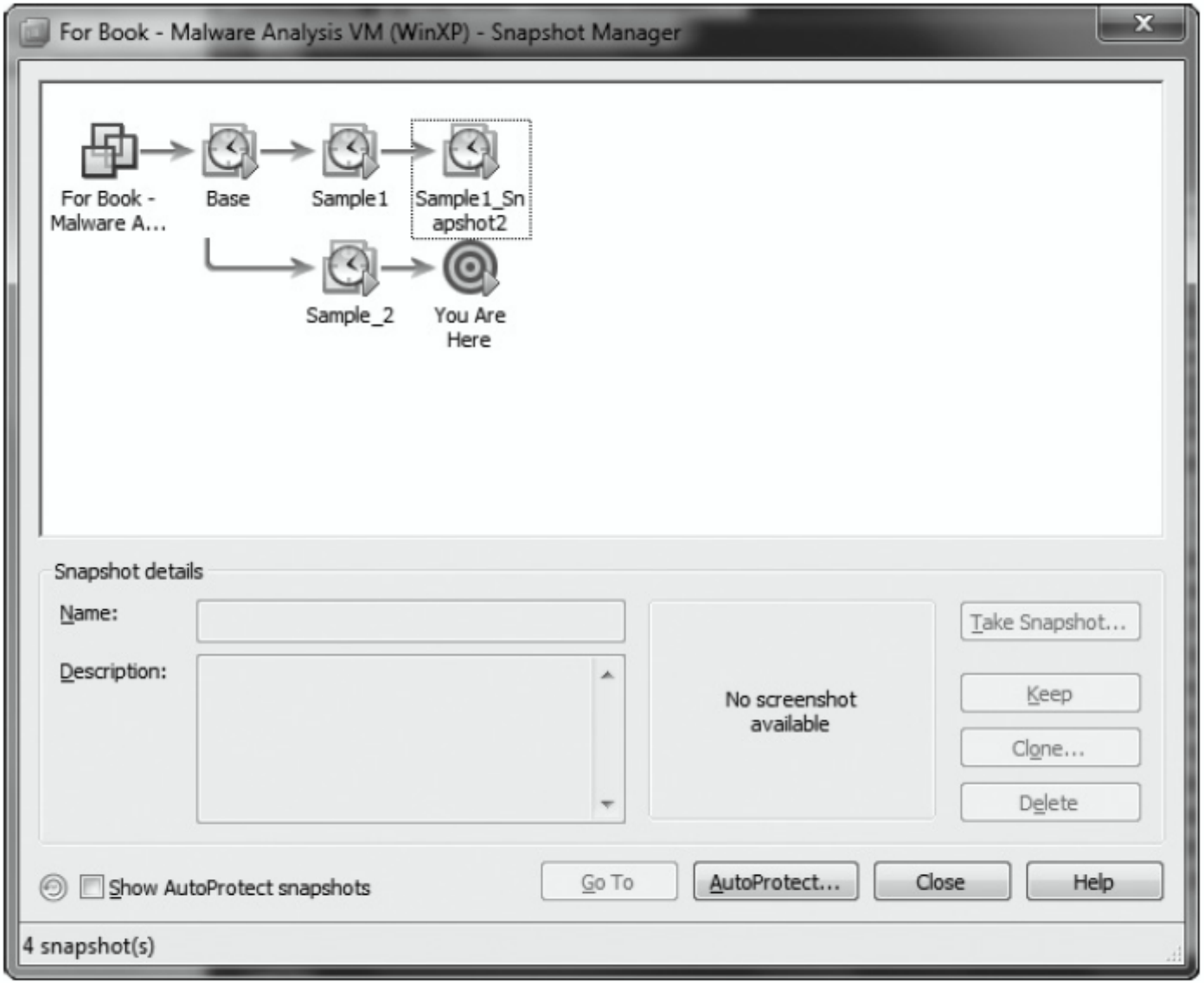


Figure 2-6: VMware Snapshot Manager

VMware Tools

- Transfering Files
  - shared folders
  - drag and drop
  - usb interface
- Record/Play
  - VMware records everything that happens so that you can replay the recording at a later time.
  - Record/replay actually executes the CPU instructions of the OS and programs

Risks of Using VMware for Malware Analysis

- Malware may detect that it is in a VM and run differently
- VMware has bugs: malware may crash or exploit it
- Malware may spread or affect the host – don't use a sensitive host machine
- **All the textbook samples are harmless**

Practical Malware Analysis

Ch 3: Basic Dynamic Analysis

Why Perform Dynamic Analysis?

- Static analysis can reach a dead-end, due to
  - Obfuscation
  - Packing
  - Examiner has exhausted the available static analysis techniques
- Dynamic analysis is efficient and will show you exactly what the malware does
- Dynamic analysis have some drawbacks
- Dynamic analysis have some limitations too

Sandboxes: The Quick-and-Dirty Approach

Sandbox

- All-in-one software for basic dynamic analysis
- Virtualized environment that simulates network services
- Examples: Norman Sandbox, GFI Sandbox, Anubis, Joe Sandbox, ThreatExpert, BitBlaze, Comodo Instant Malware Analysis
- They are expensive but easy to use
- They produce a nice PDF report of results

file

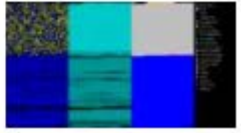
Filename	file
Size	98KiB (100651 bytes)
Type	peexe executable
Description	PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
Architecture	WINDOWS
SHA256	2c951f8c01f0c51e23f4c45f67fae20efecdb43973637f4cf0793bdad6775cff

Resources

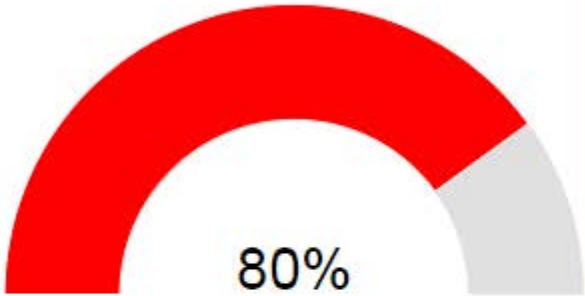
Icon

Visualization

Input File (PortEx)



CrowdStrike Falcon

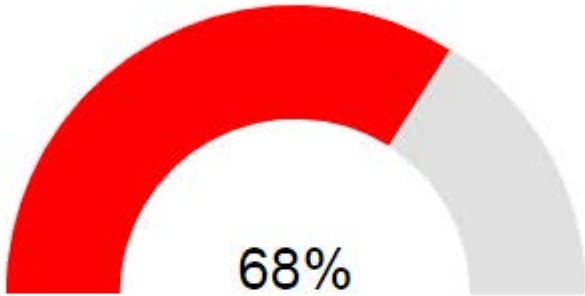


Static Analysis and ML

Last Update:	04/18/2021 17:45:02 (UTC)
View Details:	N/A
Visit Vendor:	

GET STARTED WITH A FREE TRIAL

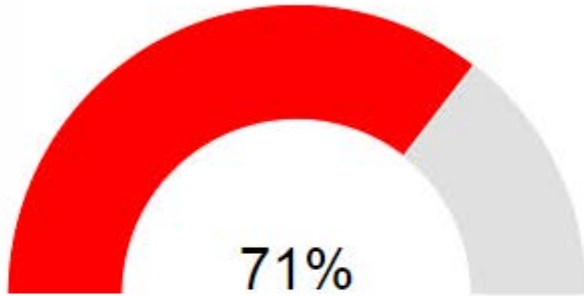
MetaDefender



Multi Scan Analysis

Last Update:	04/18/2021 17:45:02 (UTC)
View Details:	
Visit Vendor:	

VirusTotal



Multi Scan Analysis

Last Update:	04/18/2021 17:45:02 (UTC)
View Details:	
Visit Vendor:	

MALICIOUS

file

Analyzed on:	05/06/2021 06:56:24 (UTC)
Environment:	Windows 7 32 bit
Threat Score:	65/100
Indicators:	3 10 4
Network:	*(none)*

file

malicious

This report is generated from a file or URL submitted to this webservice on May 6th 2021 06:56:24 (UTC)
Guest System: Windows 7 32 bit, Professional, 6.1 (build 7601), Service Pack 1
Report generated by Falcon Sandbox v8.48.1 © Hybrid Analysis

Threat Score: 65/100
AV Detection: 90%
Labeled as: Trojan.Generic

Overview | Sample unavailable | Downloads | External Reports | Re-analyze | Hash Not Seen Before | No similar samples | Request Report Deletion

Link | Twitter | E-Mail

Incident Response

Risk Assessment

Remote Access	Reads terminal service related keys (often RDP related)
Persistence	Spawns a lot of processes Writes data to a remote process

MITRE ATT&CK™ Techniques Detection

This report has 4 indicators that were mapped to 6 attack techniques and 5 tactics. View all details

Malicious Indicators

3

Installation/Persistence

- Allocates virtual memory in a remote process
- Writes data to a remote process

Unusual Characteristics

- Spawns a lot of processes

Suspicious Indicators

10

Installation/Persistence

- Chained signature (with api-8700...). Detects file write then launch as executable
- Chained signature (with api-8701...). Detects file write then launch as executable
- Chained signature (with api-8702...). Detects file write then load as module
- Chained signature (with module-8703...). Detects file write then load as module
- Creates new processes
- Detects sample launching another instance of itself
- Drops executable files

Remote Access Related

- Reads terminal service related keys (often RDP related)

Unusual Characteristics

- Input file contains API references not part of its Import Address Table (IAT)
- Installs hooks/patches the running process

Informative

4

General

- Spawns new processes
- Spawns new processes that are not known child processes

Installation/Persistence

- Dropped files
- Touches files in the Windows directory

Network Analysis

This report was generated with enabled TOR analysis

DNS Requests

No relevant DNS requests were made.

Contacted Hosts

No relevant hosts were contacted.

HTTP Traffic

No relevant HTTP requests were made.

Extracted Strings

GFI SandBox Analysis # 2307
Sample: win32XYZ.exe (56476e02c29e5dbb9286b5f7b9e708f5)

Table of Contents

Figure 3-1: GFI Sandbox sample results for win32XYZ.exe

Running Malware

Launching DLLs

- EXE files can be run directly, but DLLs can't
- Use Rundll32.exe (included in Windows)

  rundll32.exe *DLLname*, *Export arguments*
- The *Export* value is one of the exported functions you found in Dependency Walker, PEview, or PE Explorer.

Launching DLLs

- Example
  - rip.dll has these exports: **Install** and **Uninstall**

    rundll32.exe rip.dll, Install
- Some functions use **ordinal** values instead of names, like

  rundll32.exe xyzzy.dll, #5
- It's also possible to modify the PE header and convert a DLL into an EXE

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

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

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 WI...	SyncType: SyncTypeCreateSecti...
1:17:48.6012901 PM	calc.exe	2072	CreateFileMapp...	C:\Windows\System32\WindowsCodecs.dll	SUCCESS	SyncType: SyncTypeOther
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...
1:17:48.6015591 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

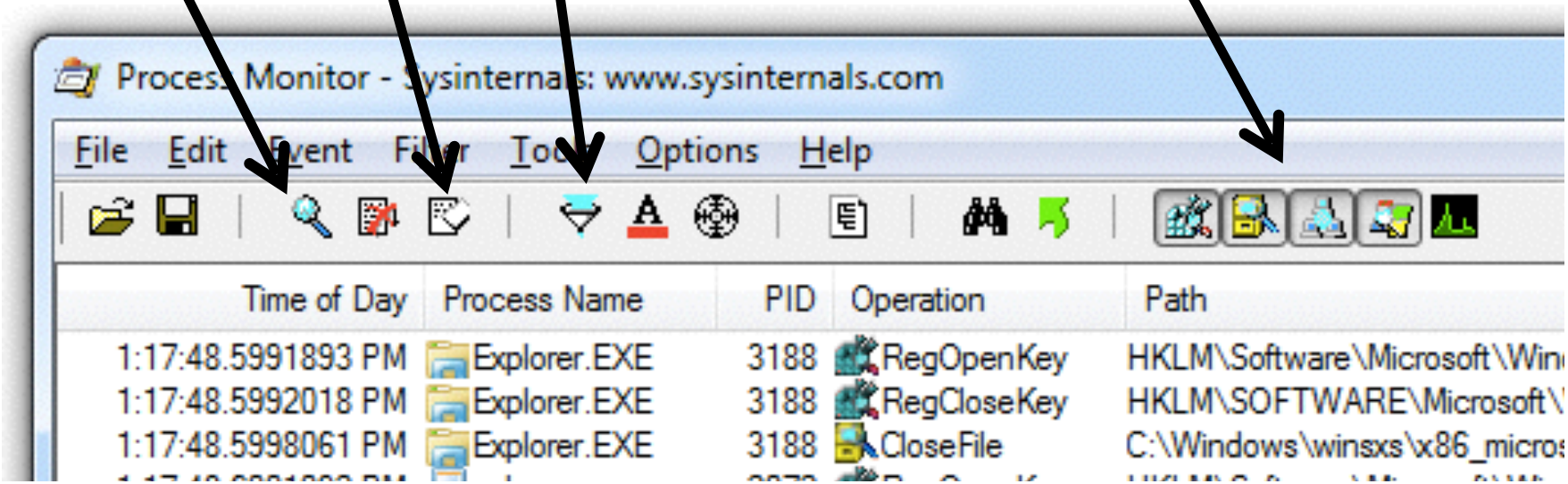
Process Monitor Toolbar

Start/Stop Capture

Erase

Filter

Default Filters
Registry, File system, Network, Processes

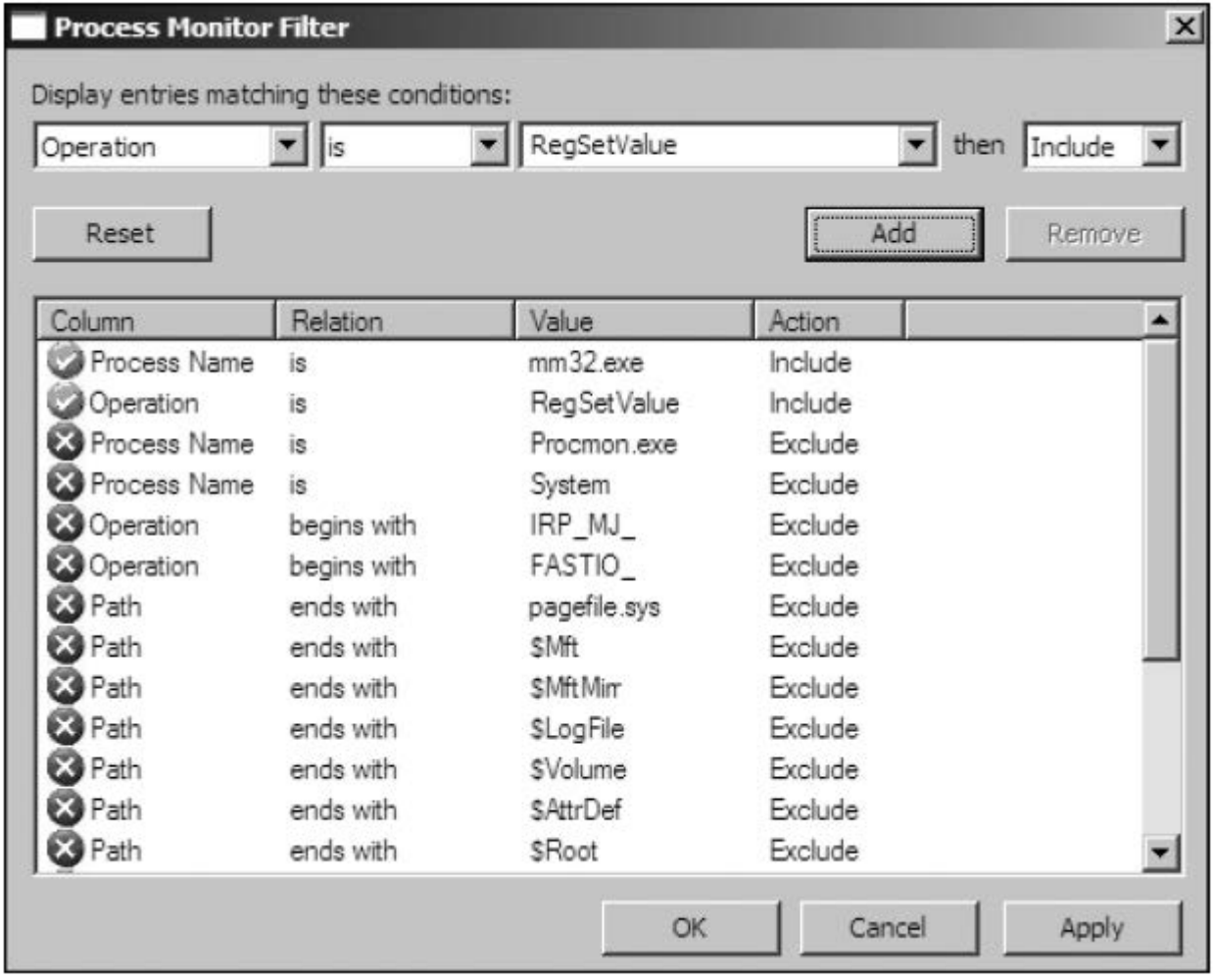


Seq.	Time ...	Process Name	Operation	Path	Result	Detail
200	1:55:31.	mm32.exe	CloseFile	Z:\Malware\mw2mmgr32.dll	SUCCESS	
201	1:55:31.	mm32.exe	ReadFile	Z:\Malware\mw2mmgr32.dll	SUCCESS	Offset: 11,776, Length: 1,024, I/O Flag
202	1:55:31.	mm32.exe	ReadFile	Z:\Malware\mw2mmgr32.dll	SUCCESS	Offset: 12,800, Length: 32,768, I/O Fla
203	1:55:31.	mm32.exe	ReadFile	Z:\Malware\mw2mmgr32.dll	SUCCESS	Offset: 1,024, Length: 9,216, I/O Flags
204	1:55:31.	mm32.exe	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Exec	NAME NOT ...	Desired Access: Read
205	1:55:31.	mm32.exe	ReadFile	Z:\Malware\mw2mmgr32.dll	SUCCESS	Offset: 45,568, Length: 25,088, I/O Fla
206	1:55:31.	mm32.exe	QueryOpen	Z:\Malware\imagehlp.dll	NAME NOT ...	
207	1:55:31.	mm32.exe	QueryOpen	C:\WINDOWS\system32\imagehlp.dll	SUCCESS	CreationTime: 2/28/2006 8:00:00 AM,
208	1:55:31.	mm32.exe	CreateFile	C:\WINDOWS\system32\imagehlp.dll	SUCCESS	Desired Access: Execute/Traverse, S
209	1:55:31.	mm32.exe	CloseFile	C:\WINDOWS\system32\imagehlp.dll	SUCCESS	
210	1:55:31.	mm32.exe	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Exec	NAME NOT ...	Desired Access: Read
211	1:55:31.	mm32.exe	ReadFile	Z:\Malware\mw2mmgr32.dll	SUCCESS	Offset: 10,240, Length: 1,536, I/O Flag
212	1:55:31.	mm32.exe	CreateFile	C:\Documents and Settings\All Users\Application Data\mw2mmgr.txt	SUCCESS	Desired Access: Generic Write, Read
213	1:55:31.	mm32.exe	ReadFile	C:\$Directory	SUCCESS	Offset: 12,288, Length: 4,096, I/O Flag
214	1:55:31.	mm32.exe	CreateFile	Z:\Malware\mm32.exe	SUCCESS	Desired Access: Generic Read, Dispo
215	1:55:31.	mm32.exe	ReadFile	Z:\Malware\mm32.exe	SUCCESS	Offset: 0, Length: 64

Figure 3-2: Procmon mm32.exe *example*

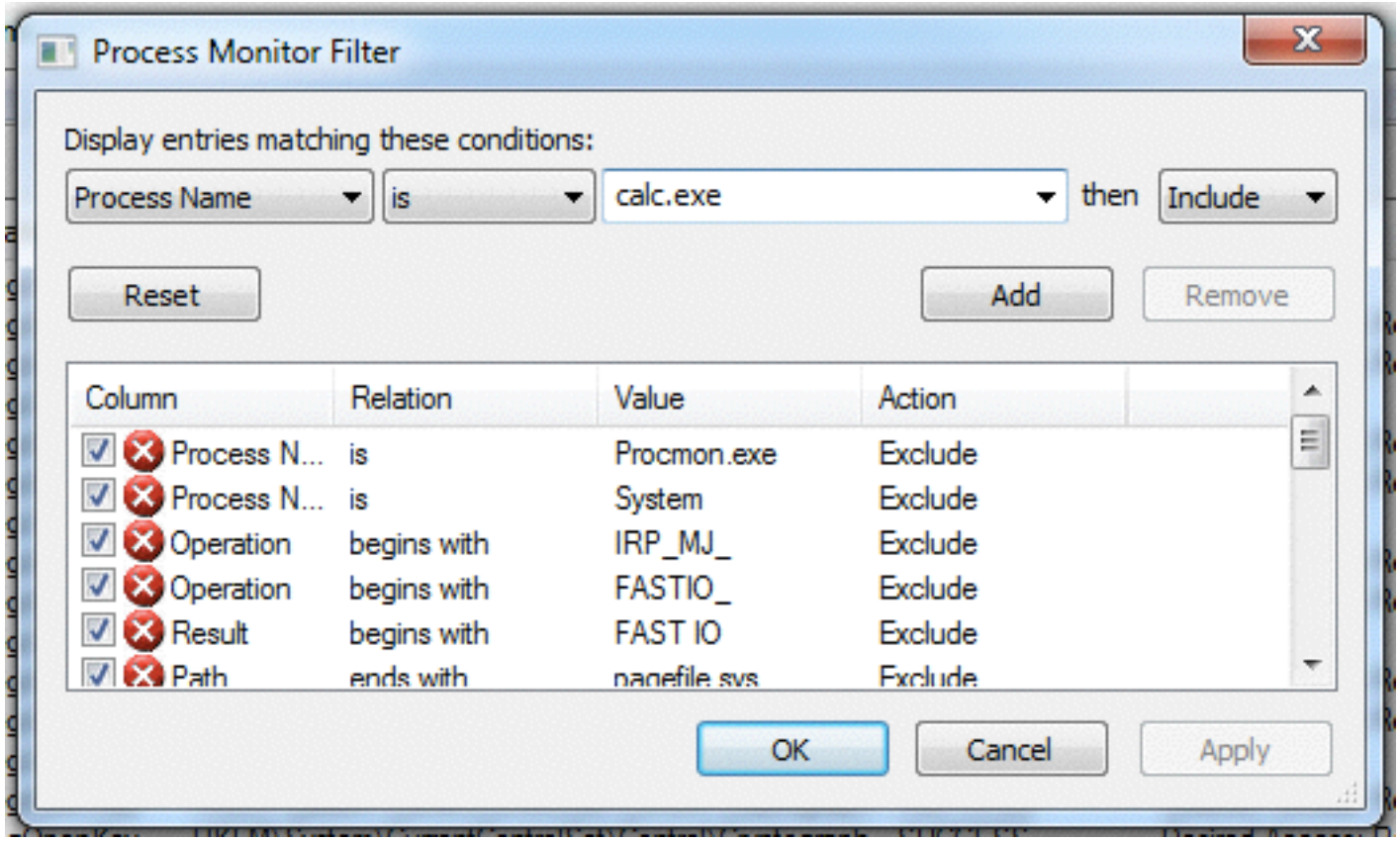
Filtering with Exclude

- 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
- If your malware runs at boot time, use procmon’s boot logging options to install procmon as a startup driver to capture startup events.


Process Monitor Filter
Display entries matching these conditions:
Operation
is
RegSetValue
then
Include
Reset
Add
Remove
Column
Relation
Value
Action
Process Name is mm32.exe Include
Operation is RegSetValue Include
Process Name is Procmon.exe Exclude
Process Name is System Exclude
Operation begins with IRP_MJ_ Exclude
Operation begins with FASTIO_ Exclude
Path ends with pagefile.sys Exclude
Path ends with $Mft Exclude
Path ends with $MftMirr Exclude
Path ends with $LogFile Exclude
Path ends with $Volume Exclude
Path ends with $AttrDef Exclude
Path ends with $Root Exclude
OK
Cancel
Apply

Filtering with Include

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



Viewing Processes with Process Explorer

Process Explorer - Sysinternals: www.sysinternals.com [W7\student]

File Options View Process Find Users Help

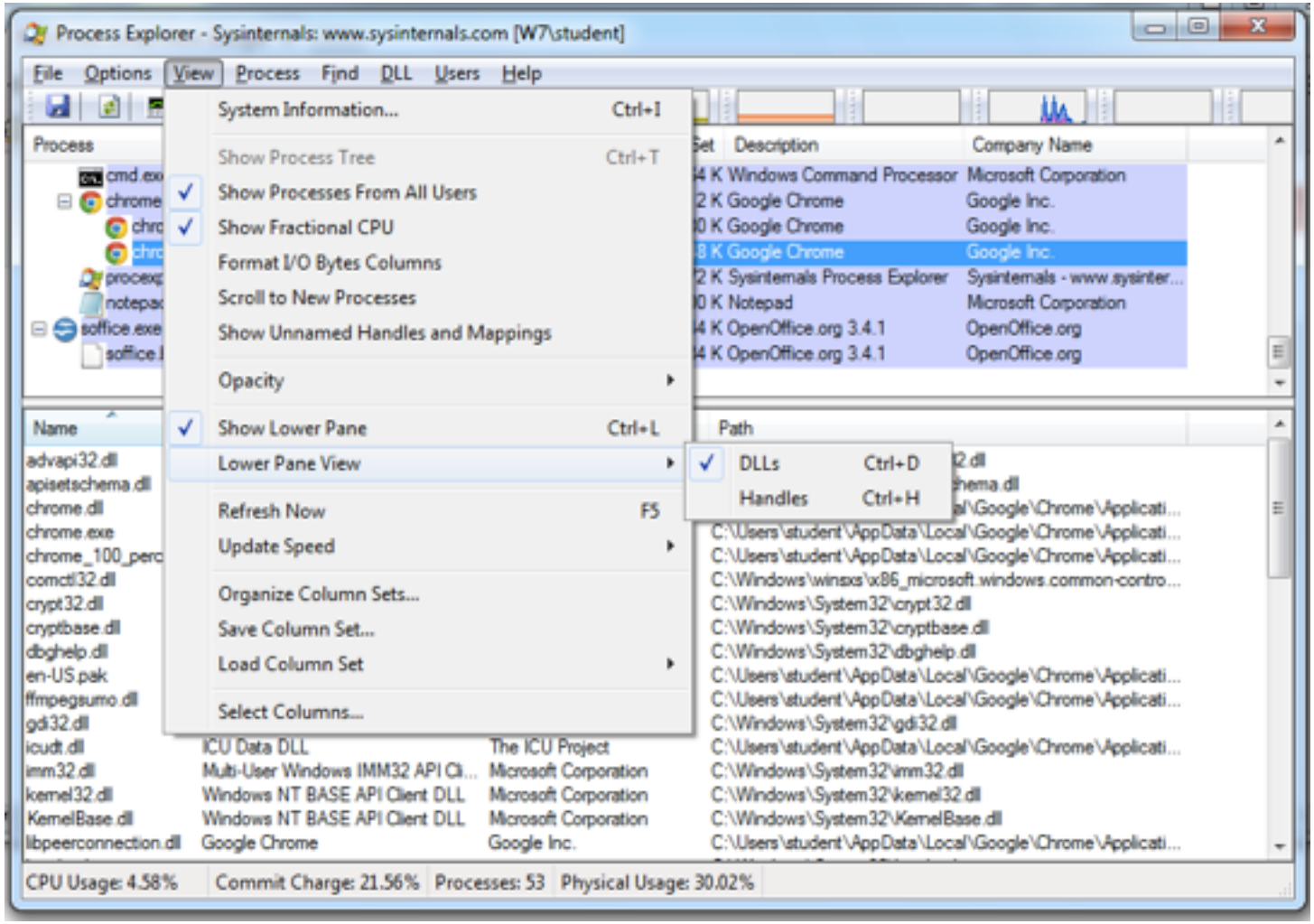
Process	PID	CPU	Private Bytes	Working Set	Description	Company Name
System Idle Process	0	96.81	0 K	24 K		
System	4	0.09	48 K	560 K		
Interrupts	n/a	0.88	0 K	0 K	Hardware Interrupts and DPCs	
smss.exe	260		224 K	748 K	Windows Session Manager	Microsoft Corporation
csrss.exe	348	< 0.01	1,252 K	3,164 K	Client Server Runtime Process	Microsoft Corporation
wininit.exe	400		892 K	3,084 K	Windows Start-Up Application	Microsoft Corporation
services.exe	504	0.01	3,972 K	6,640 K	Services and Controller app	Microsoft Corporation
svchost.exe	652		2,700 K	6,024 K	Host Process for Windows S...	Microsoft Corporation
dllhost.exe	1716		6,176 K	4,804 K	COM Surrogate	Microsoft Corporation
WmiPrvSE.exe	740		1,804 K	4,736 K	WMI Provider Host	Microsoft Corporation
svchost.exe	724	< 0.01	2,972 K	6,012 K	Host Process for Windows S...	Microsoft Corporation
svchost.exe	772		13,776 K	11,760 K	Host Process for Windows S...	Microsoft Corporation
audiodg.exe	3200		14,960 K	13,972 K	Windows Audio Device Grap...	Microsoft Corporation
svchost.exe	912		37,940 K	42,292 K	Host Process for Windows S...	Microsoft Corporation
dwm.exe	3248	0.74	61,892 K	27,976 K	Desktop Window Manager	Microsoft Corporation
svchost.exe	936	0.02	20,836 K	29,900 K	Host Process for Windows S...	Microsoft Corporation
svchost.exe	1116	0.03	5,136 K	8,340 K	Host Process for Windows S...	Microsoft Corporation
svchost.exe	1260	0.06	10,840 K	11,960 K	Host Process for Windows S...	Microsoft Corporation
spoolsv.exe	1352		5,392 K	7,436 K	Spooler SubSystem App	Microsoft Corporation
svchost.exe	1388		6,752 K	8,720 K	Host Process for Windows S...	Microsoft Corporation
svchost.exe	1500		2,472 K	4,712 K	Host Process for Windows S...	Microsoft Corporation
gogoc.exe	1592	< 0.01	1,216 K	3,920 K	gogoCLIENT	gogo6, Inc.
vmtoolsd.exe	1728	0.07	7,260 K	10,368 K	VMware Tools Core Service	VMware, Inc.
svchost.exe						

CPU Usage: 3.19% | Commit Charge: 21.92% | Processes: 57 | Physical Usage: 30.24%

Coloring

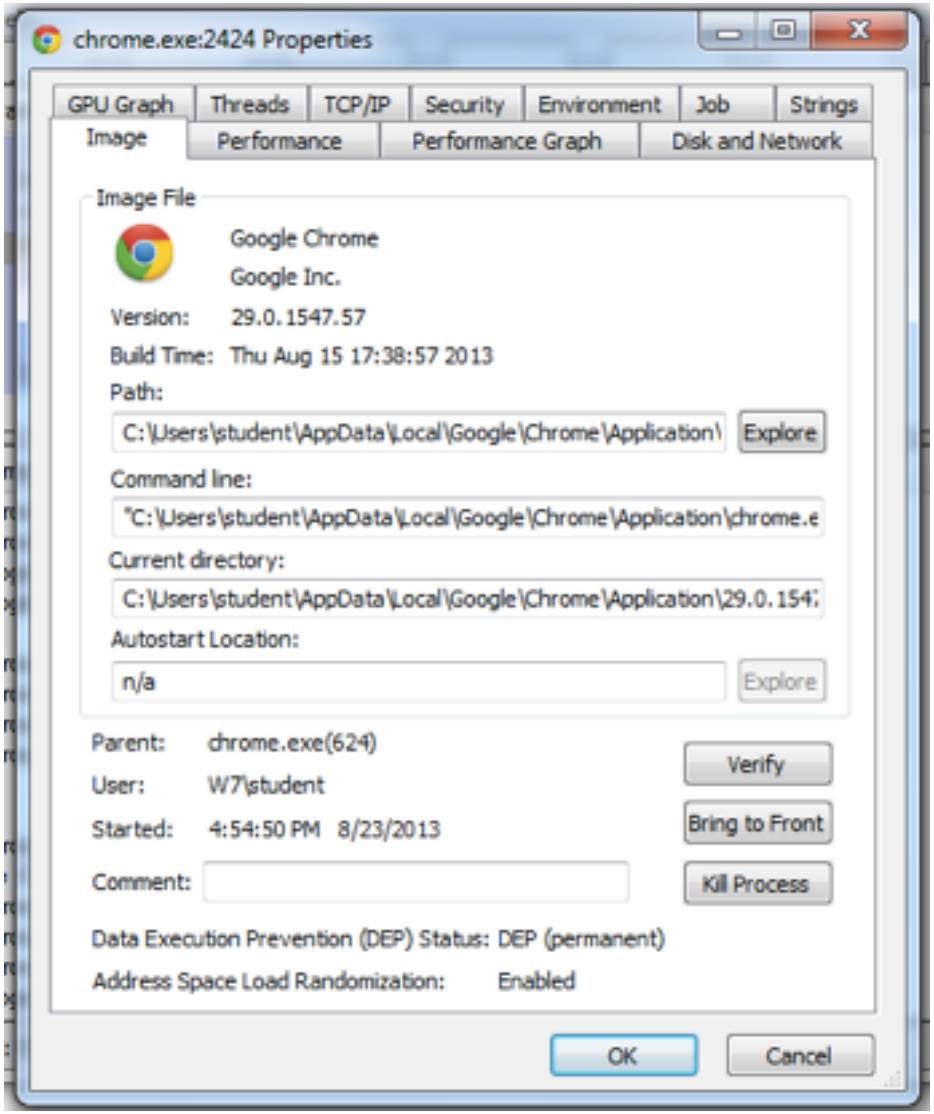
- Services are pink
- Processes are blue
- New processes are green briefly
- Terminated processes are red

DLL Mode


Process Explorer - Sysinternals: www.sysinternals.com [W7\student]
File Options View Process Find DLL Users Help
System Information... Ctrl+I
Show Process Tree Ctrl+T
Show Processes From All Users
Show Fractional CPU
Format I/O Bytes Columns
Scroll to New Processes
Show Unnamed Handles and Mappings
Opacity
Show Lower Pane Ctrl+L
Lower Pane View
DLLs Ctrl+D
Handles Ctrl+H
Refresh Now F5
Update Speed
Organize Column Sets...
Save Column Set...
Load Column Set
Select Columns...
Process
Description
Company Name
Name
Path
CPU Usage: 4.58%
Commit Charge: 21.56%
Processes: 53
Physical Usage: 30.02%

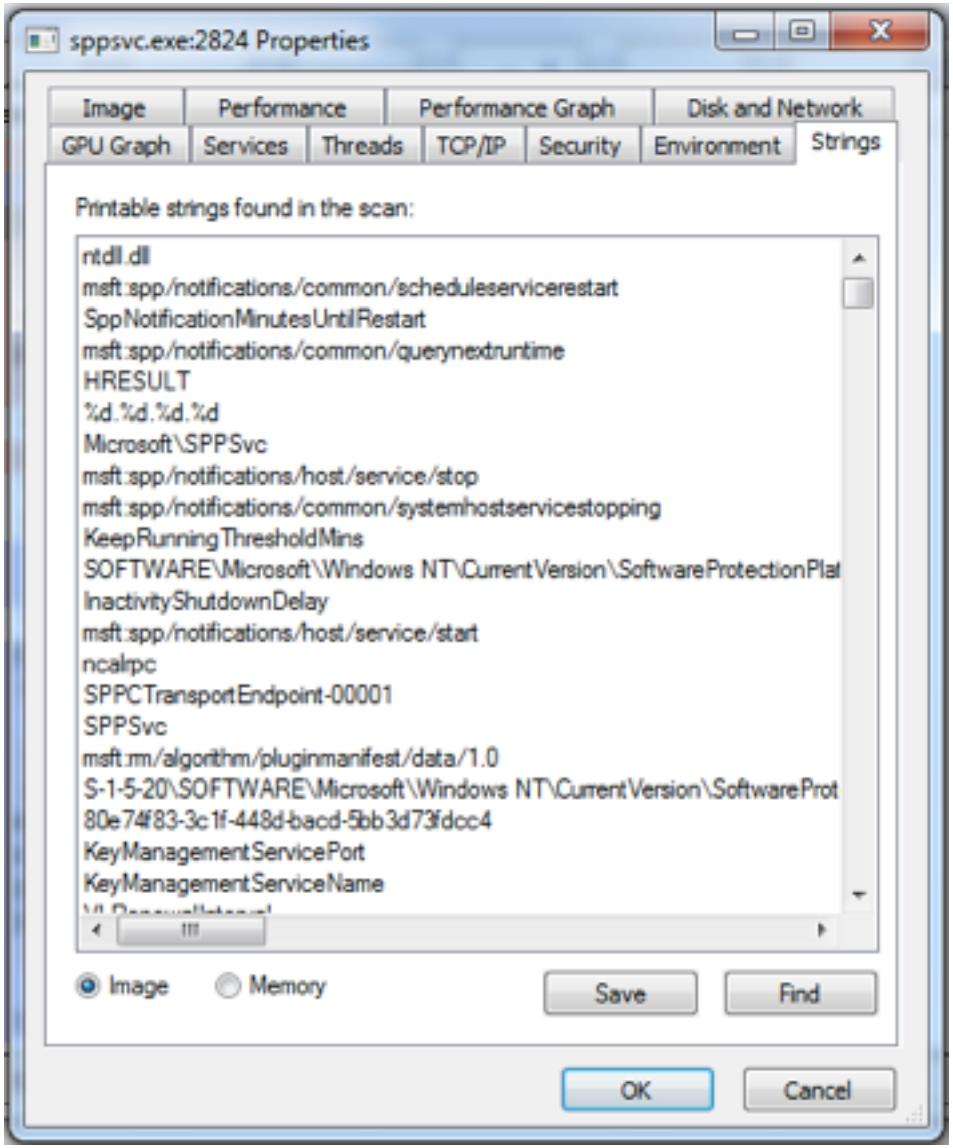
Properties

- 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



svchost.exe:1788 Properties

Image | Performance | Performance Graph | Threads
TCP/IP | Security | Environment | Strings

Printable strings found in the scan:

Parameters
System\CurrentControlSet\Services
nServiceMain
ServiceDll
ServiceDllUnloadOnStop
eventlog
ncacn_np
\PIPE\
DefaultRpcStackSize
AuthenticationCapabilities
ImpersonationLevel
AuthenticationLevel
CoInitializeSecurityParam
Software\Microsoft\Windows NT\CurrentVersion\Svchost
\Registry\Machine\System\CurrentControlSet\Control\SecurePipeServers\
VS_VERSION_INFO
StringFileInfo
CompanyName

Image | Memory | Save | Find

OK | Cancel

svchost.exe:1788 Properties

Image | Performance | Performance Graph | Threads
TCP/IP | Security | Environment | Strings

Printable strings found in the scan:

VS_VERSION_INFO
StringFileInfo
Comments
CompanyName
FileDescription
FAVORITES
FileVersion
InternalName
FAVORITES.DAT
LegalCopyright
Microsoft Corporation. All rights reserved.
LegalTrademarks
OriginalFilename
FAVORITES.DAT
PrivateBuild
ProductName
FAVORITES
ProductVersion
SpecialBuild

Image | Memory | Save | Find

OK | Cancel

Figure 3-7: The Process Explorer Strings tab shows strings on disk (left) versus strings in memory (right) for active svchost.exe.

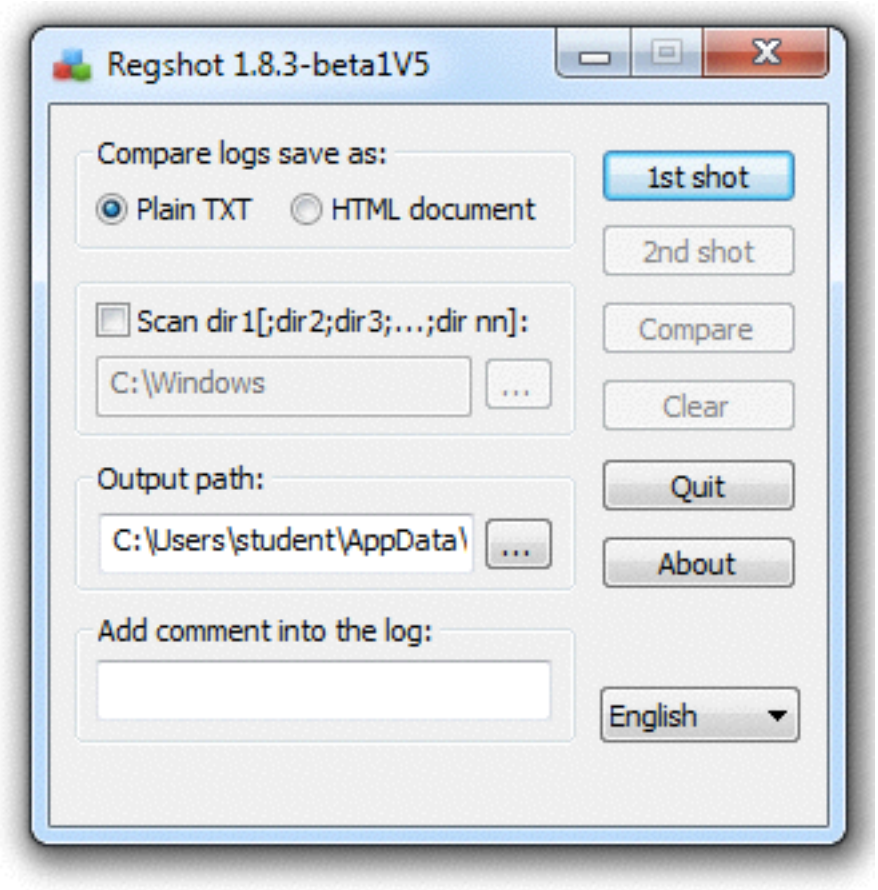
Detecting Malicious Documents

- 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

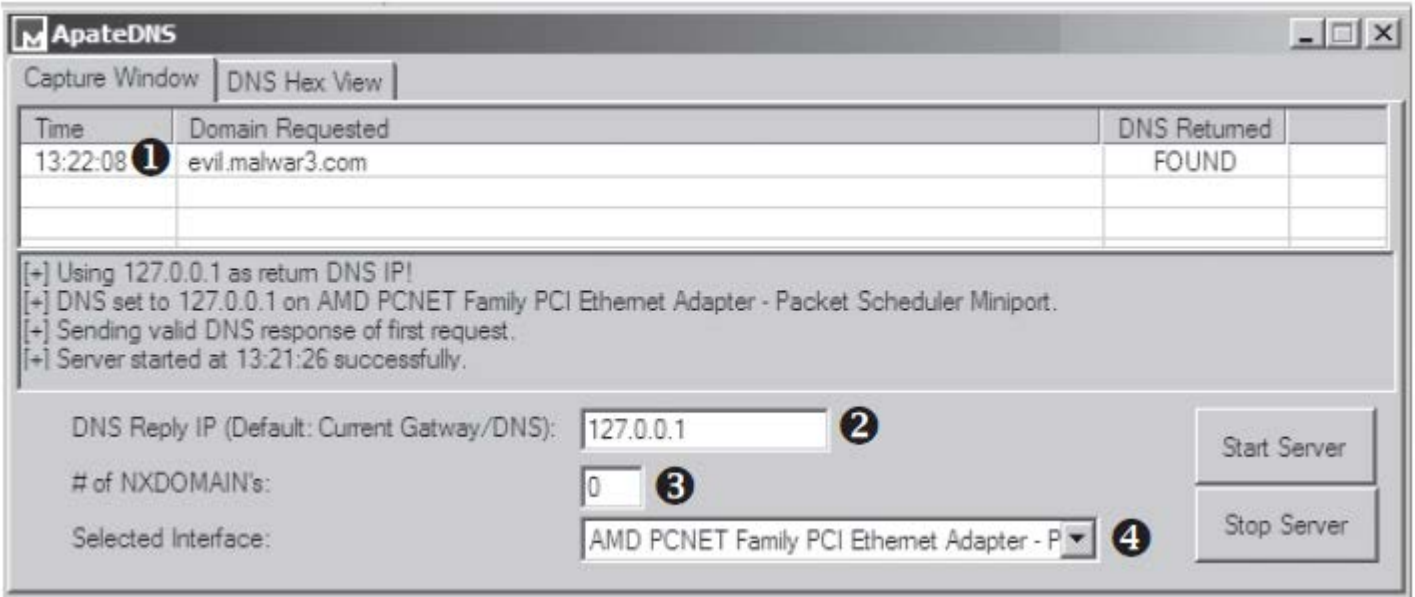
- Take 1st shot
- Run malware
- Take 2nd shot
- Compare them to see what registry keys were changed



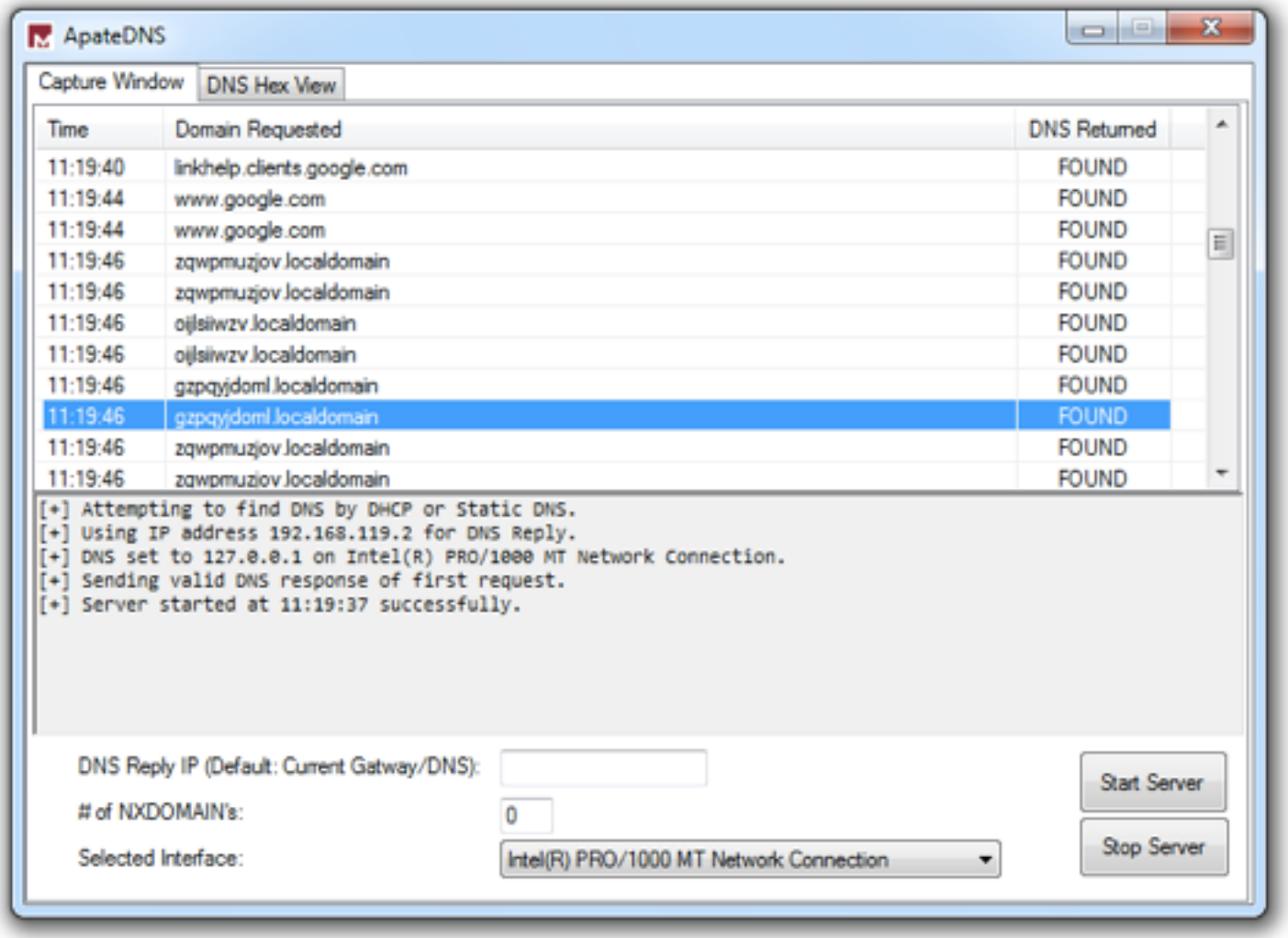
```
----------------------------------
Values added:3
----------------------------------
❶ HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ckr:C:\WINDOWS\system32\
ckr.exe
...
...

----------------------------------
Values modified:2
----------------------------------
❷ HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed: 00 43 7C 25 9C 68 DE 59 C6 C8
9D C3 1D E6 DC 87 1C 3A C4 E4 D9 0A B1 BA C1 FB 80 EB 83 25 74 C4 C5 E2 2F CE
4E E8 AC C8 49 E8 E8 10 3F 13 F6 A1 72 92 28 8A 01 3A 16 52 86 36 12 3C C7 EB
5F 99 19 1D 80 8C 8E BD 58 3A DB 18 06 3D 14 8F 22 A4
...

----------------------------------
Total changes:5
----------------------------------
```

Listing 3-1: Regshot comparison results

Faking a Network


ApateDNS
Capture Window
DNS Hex View
Time
Domain Requested
DNS Returned
13:22:08
evil.malwar3.com
FOUND
[+] Using 127.0.0.1 as return DNS IP!
[+] DNS set to 127.0.0.1 on AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport.
[+] Sending valid DNS response of first request.
[+] Server started at 13:21:26 successfully.
DNS Reply IP (Default: Current Gatway/DNS):
127.0.0.1
# of NXDOMAIN's:
0
Selected Interface:
AMD PCNET Family PCI Ethernet Adapter - P
Start Server
Stop Server

Using ApateDNS to Redirect DNS Resolutions



ApateDNS Does Not Work

- I couldn't get it to redirect any traffic in Win XP or 7
- nslookup works, but you don't see anything in a browser or with ping
- I decided to ignore it and use INetSim instead

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

nc -help – This command will print a list of all of the available commands you can use in Netcat. It will come in handy if you run into any errors while writing a script or are unsure of how to proceed.

nc -z -v site.com – This will run a basic port scan of the specified website or server. Netcat will return verbose results with lists of ports and statuses. Keep in mind that you can use an IP address in place of the site domain.

nc -l – This command will instruct the local system to begin listening for TCP connections and UDP activity on a specific port number.

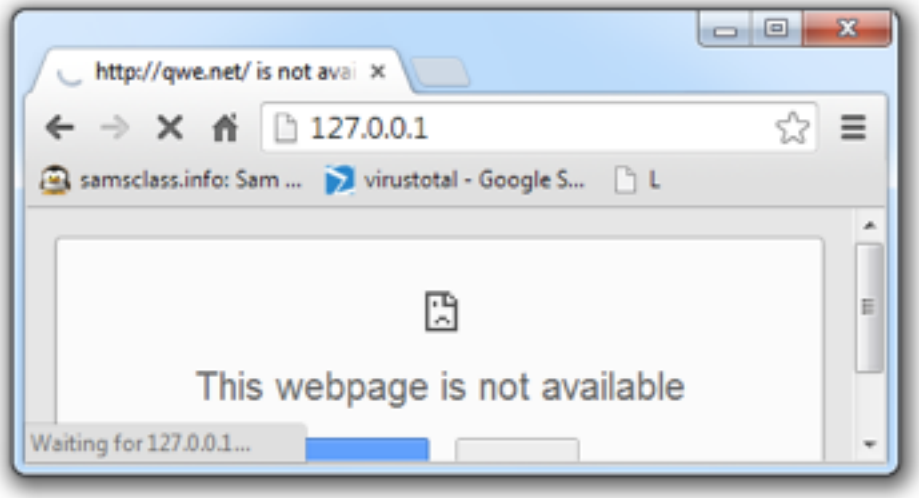
nc site.com 1234 (less than) file_name – This command will initiate the transfer of a file based on the specified port number.

Printf – Netcat can actually operate as a simplified web host. This command will let you save HTML code and publish it through your local server.

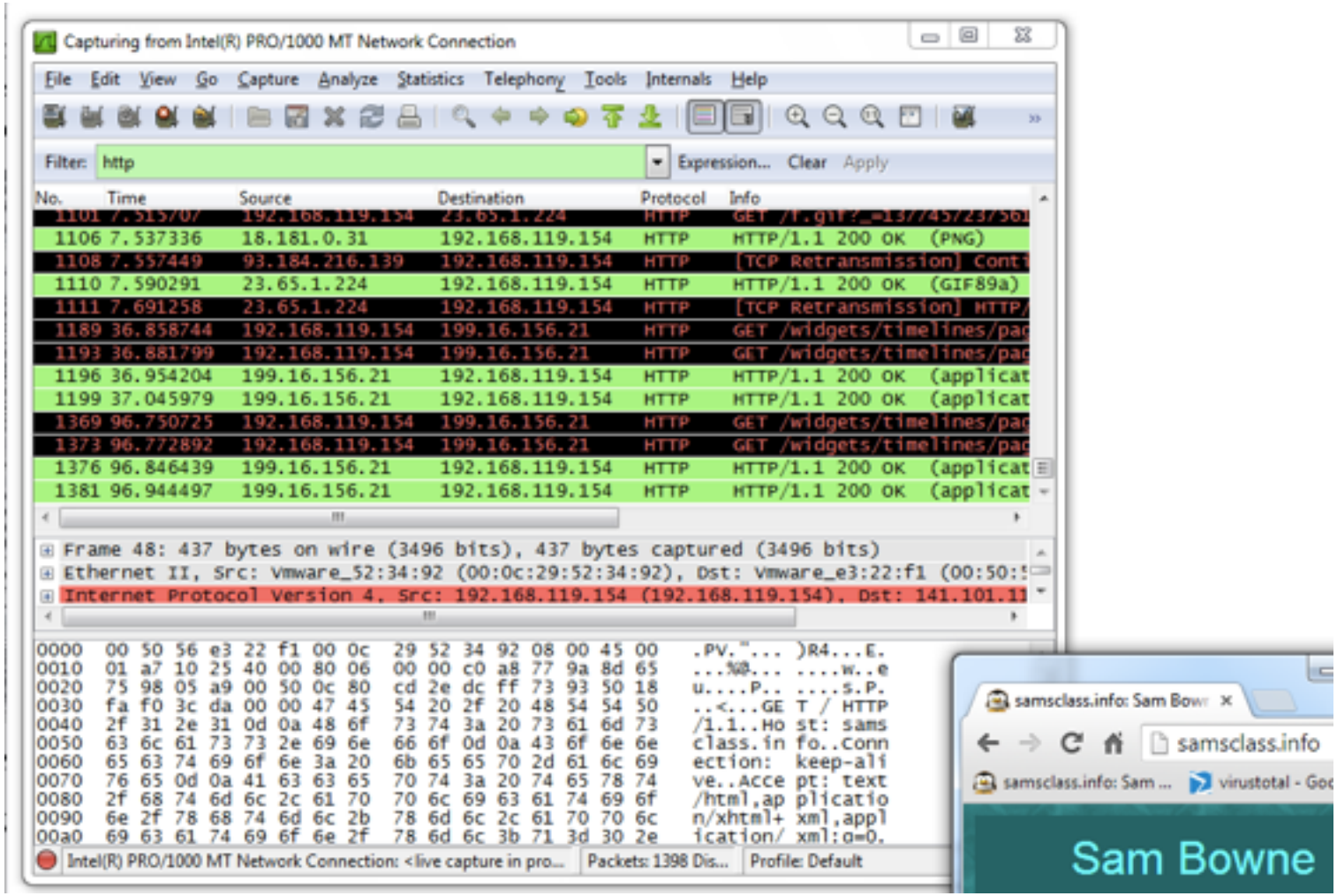
Monitoring with Ncat (included with Nmap)

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
```

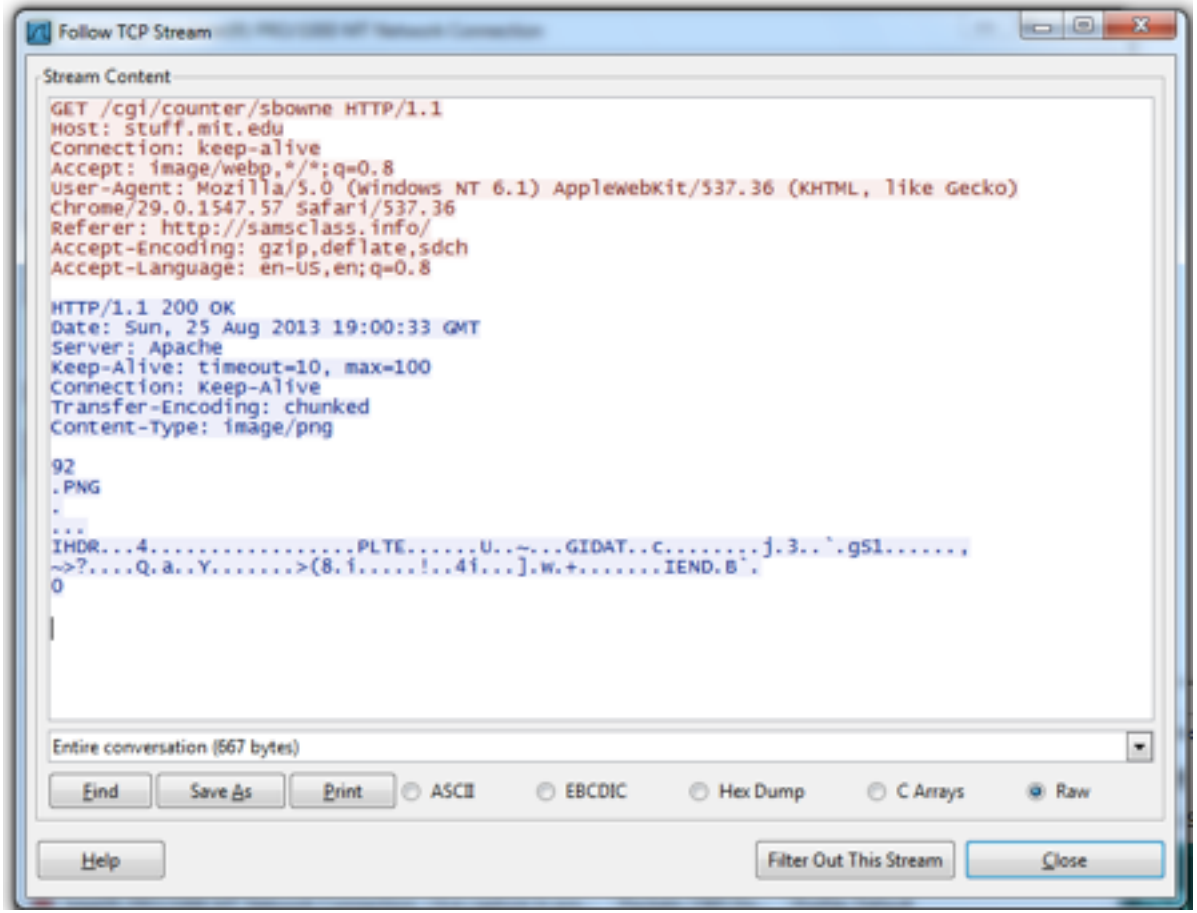


Packet Sniffing with Wireshark



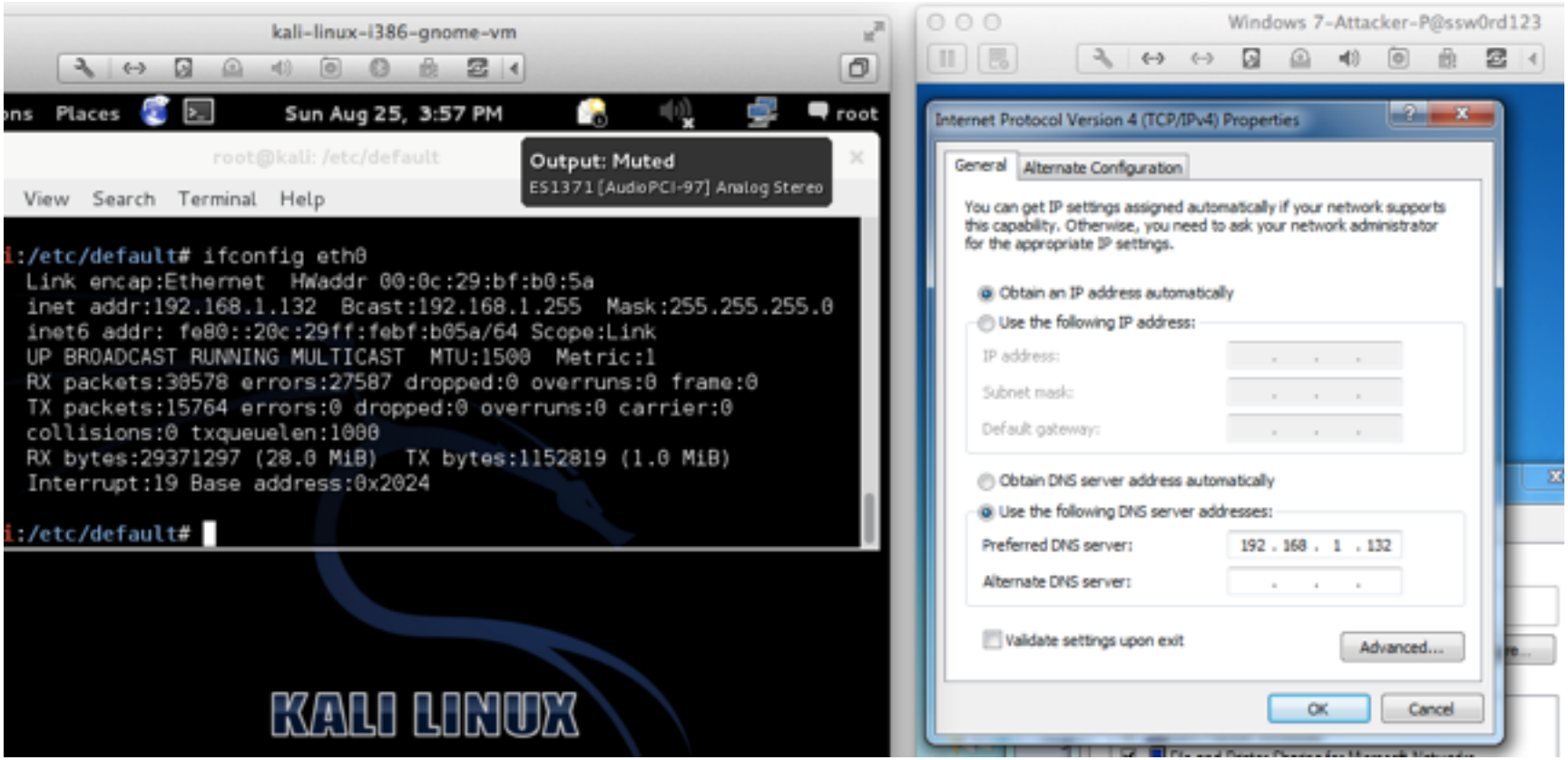
Follow TCP Stream

- Can save files from streams here too



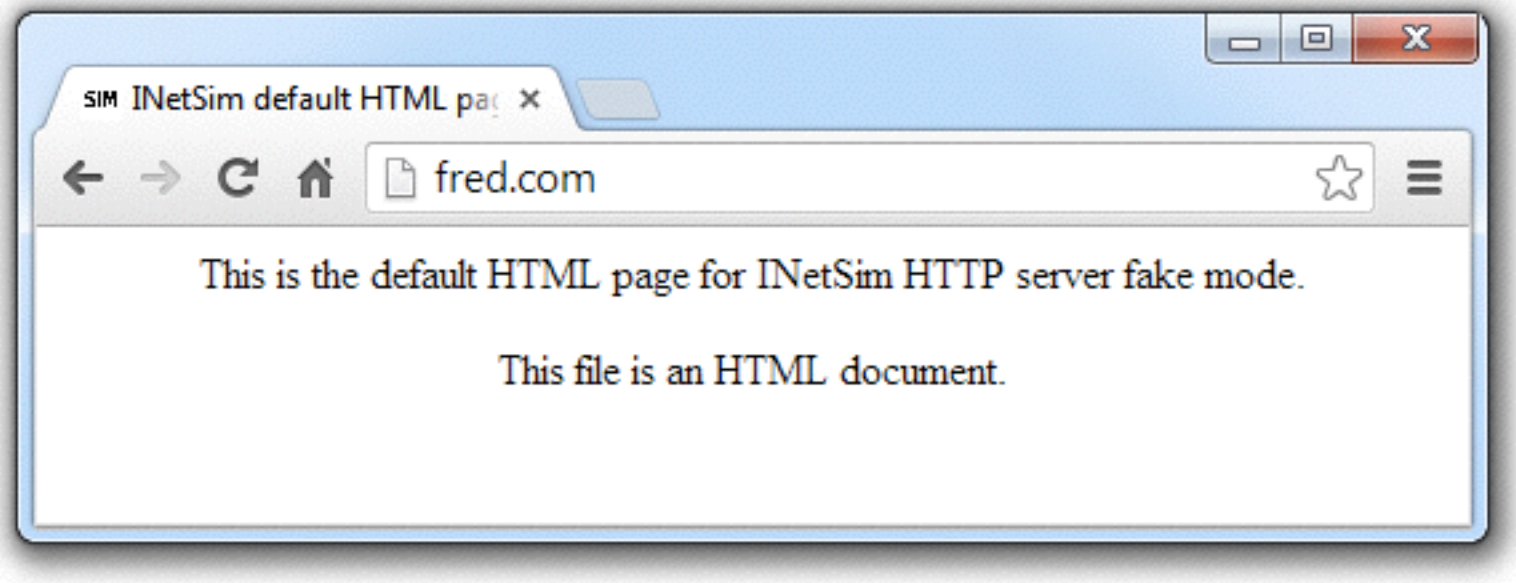
Using INetSim

inetsim


kali-linux-i386-gnome-vm
Places
Sun Aug 25, 3:57 PM
root
root@kali: /etc/default
View Search Terminal Help
Output: Muted
ES1371 [AudioPCI-97] Analog Stereo
i:/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
i:/etc/default#
KALI LINUX
Windows 7-Attacker-P@ssw0rd123
Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 1 . 132
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

```
* dns 53/udp/tcp - started (PID 9992)
* http 80/tcp - started (PID 9993)
* https 443/tcp - started (PID 9994)
* smtp 25/tcp - started (PID 9995)
* irc 6667/tcp - started (PID 10002)
* smtps 465/tcp - started (PID 9996)
* ntp 123/udp - started (PID 10003)
* pop3 110/tcp - started (PID 9997)
* finger 79/tcp - started (PID 10004)
* syslog 514/udp - started (PID 10006)
* tftp 69/udp - started (PID 10001)
* pop3s 995/tcp - started (PID 9998)
* time 37/tcp - started (PID 10007)
* ftp 21/tcp - started (PID 9999)
* ident 113/tcp - started (PID 10005)
* time 37/udp - started (PID 10008)
* ftps 990/tcp - started (PID 10000)
* daytime 13/tcp - started (PID 10009)
* daytime 13/udp - started (PID 10010)
* echo 7/tcp - started (PID 10011)
* echo 7/udp - started (PID 10012)
* discard 9/udp - started (PID 10014)
```

INetSim Fools a Browser



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

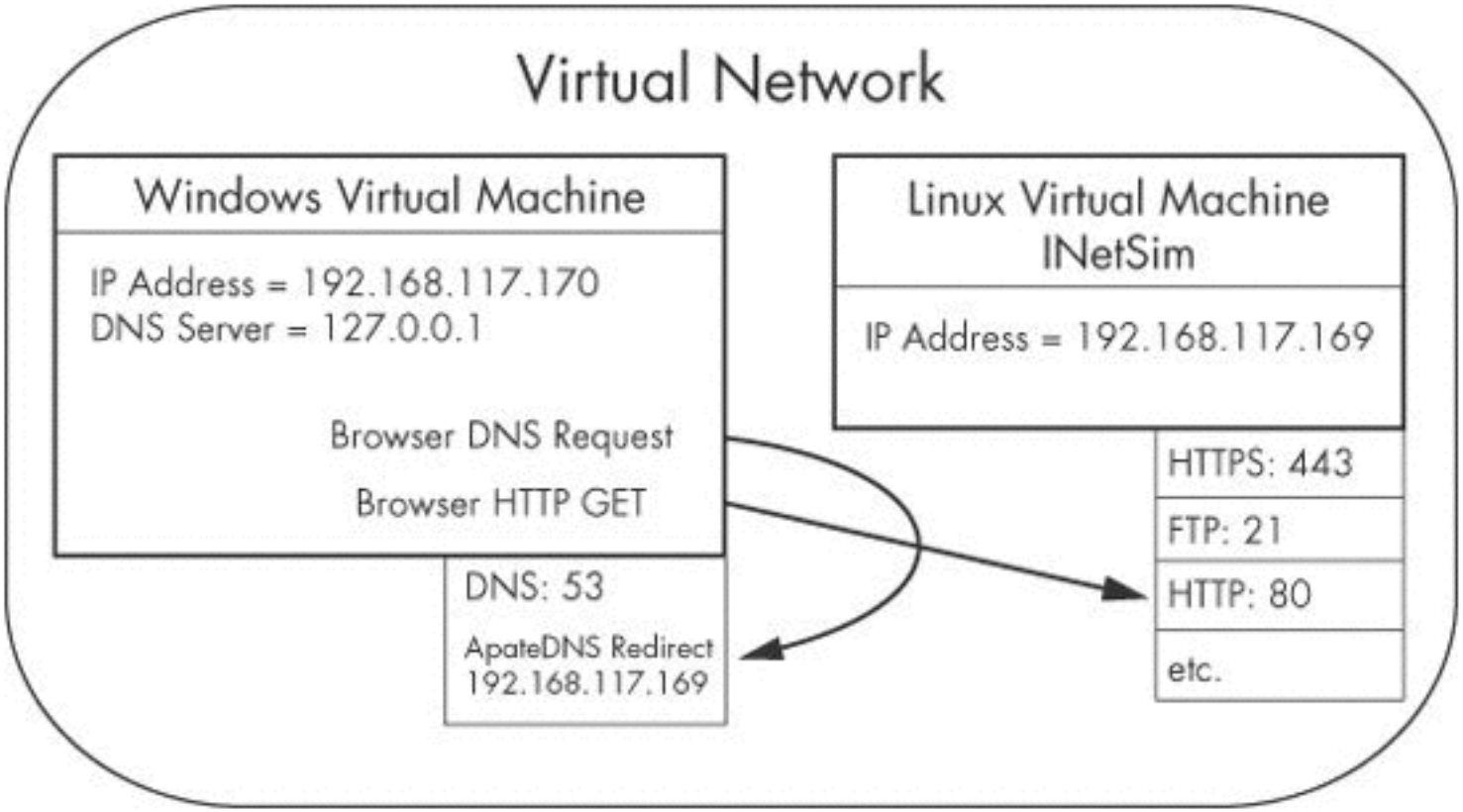


Figure 4-12. Example of a virtual network