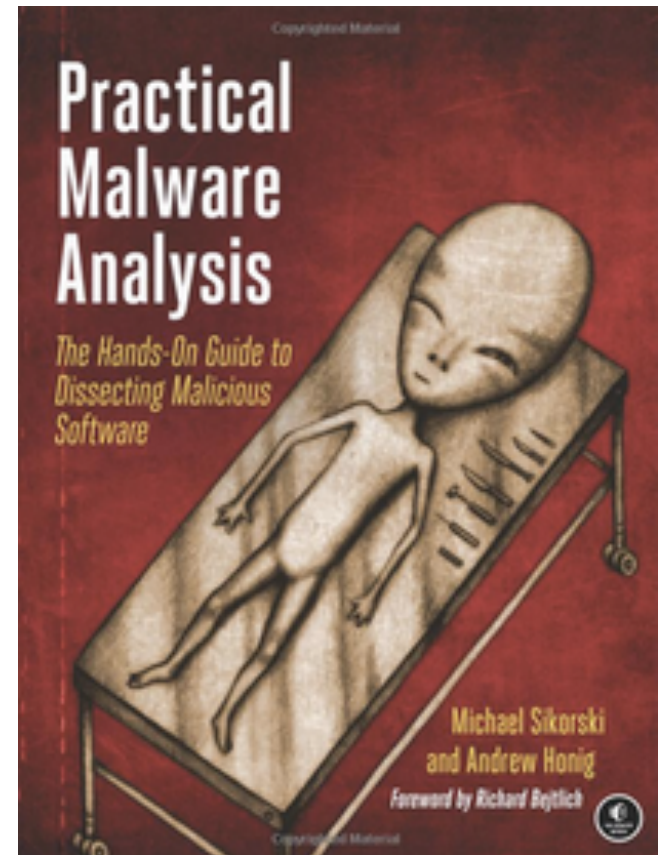


Practical Malware Analysis



Ch 2: Malware Analysis in Virtual Machines

Updated 2-2-21

Dynamic Analysis

- Running malware deliberately, while monitoring the results
- Requires a **safe environment**
- 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 Workstation Player/Fusion

- Free for education
- Cannot take snapshots
- You could also use VirtualBox, Hyper-V, Parallels, or Xen.

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

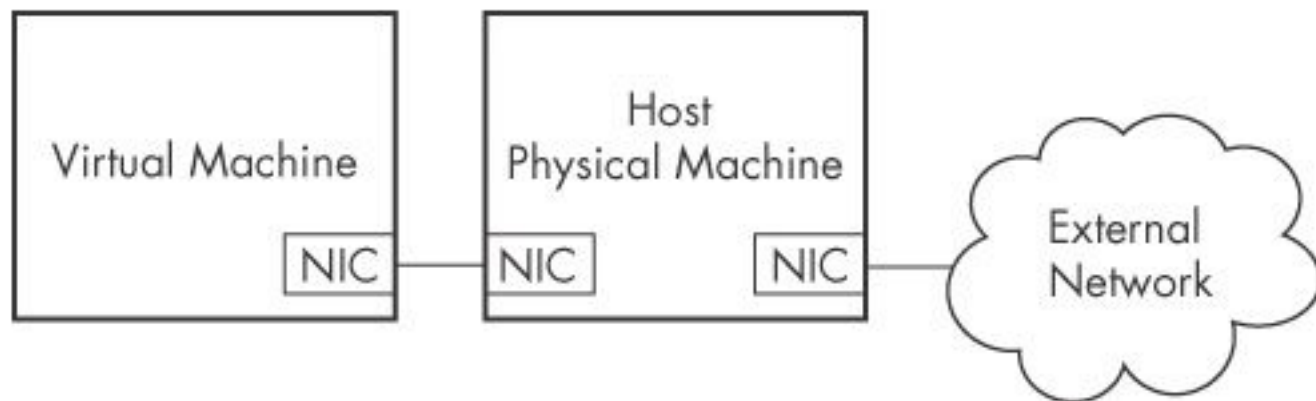
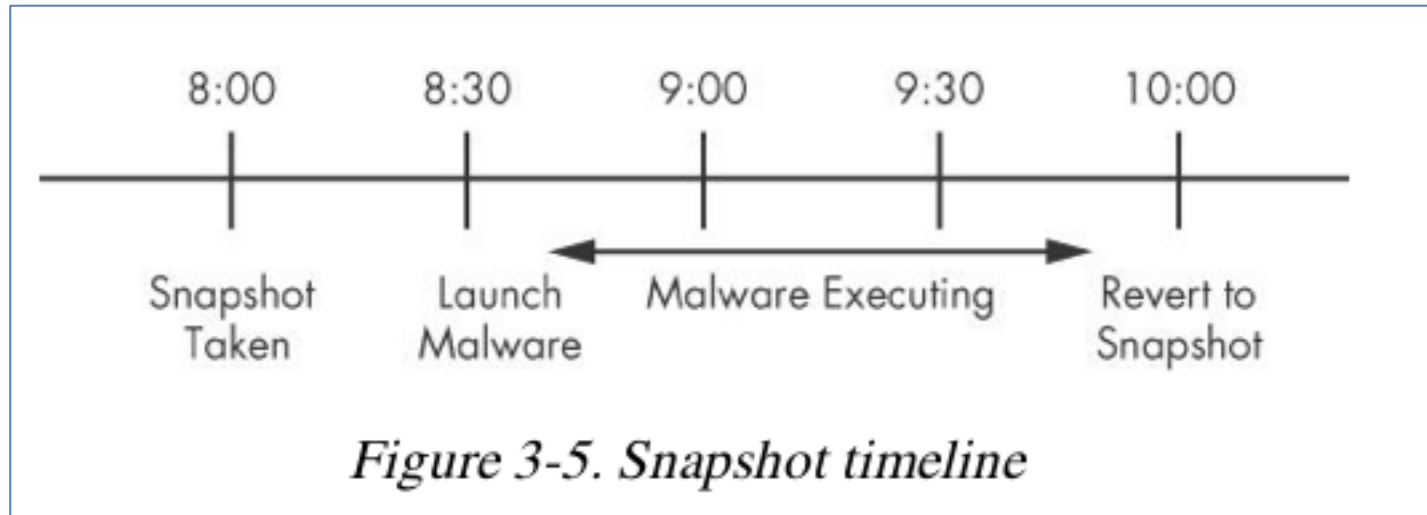


Figure 3-3. Host-only networking in VMware

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



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

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

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

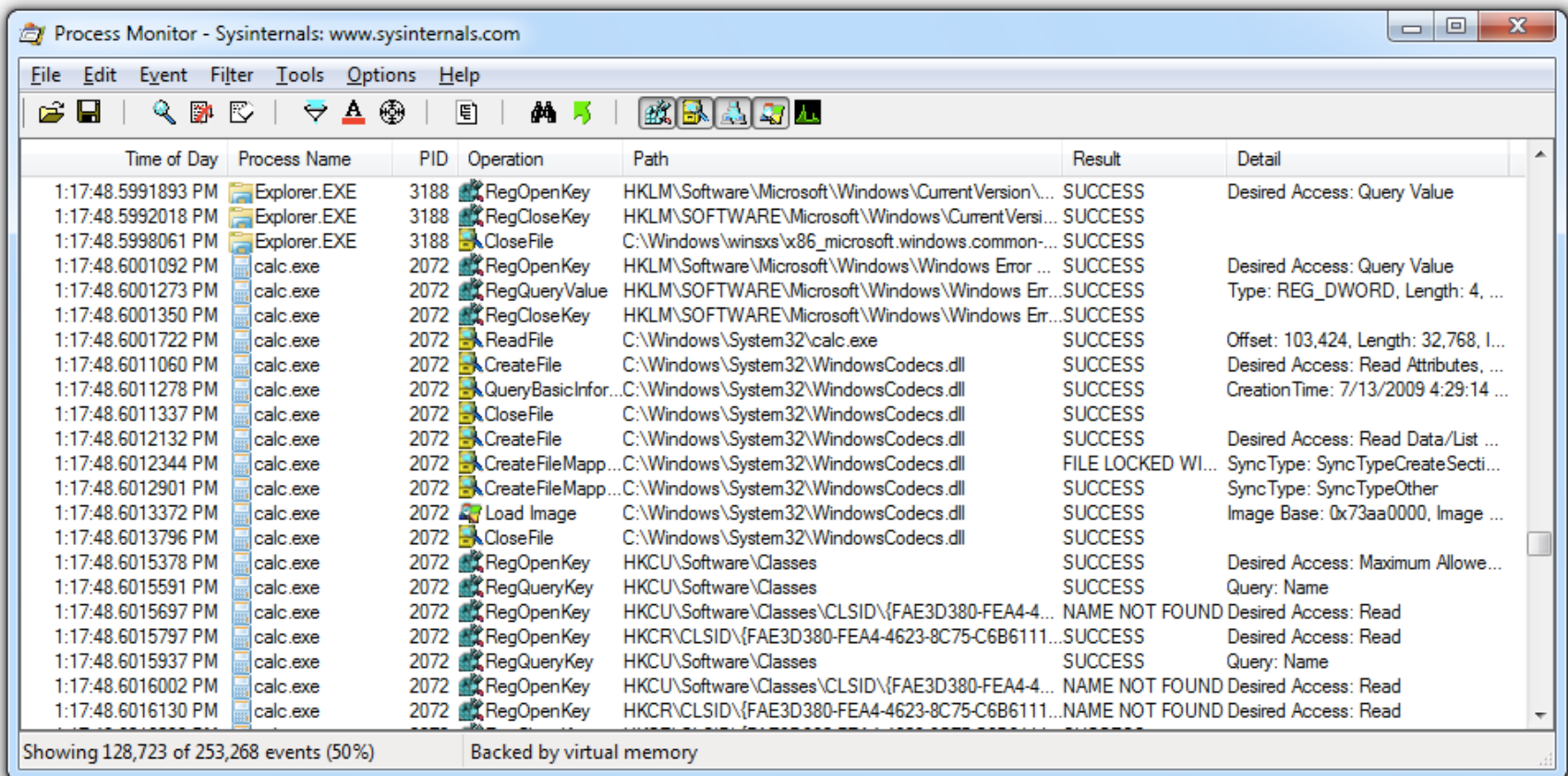
Monitoring with Process Monitor

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



The screenshot shows the Process Monitor application window with a list of events. The window title is "Process Monitor - Sysinternals: www.sysinternals.com". The menu bar includes File, Edit, Event, Filter, Tools, Options, and Help. The toolbar contains various icons for file operations, search, and process management. The main area is a table with columns for Time of Day, Process Name, PID, Operation, Path, Result, and Detail.

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\Current Versi...	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

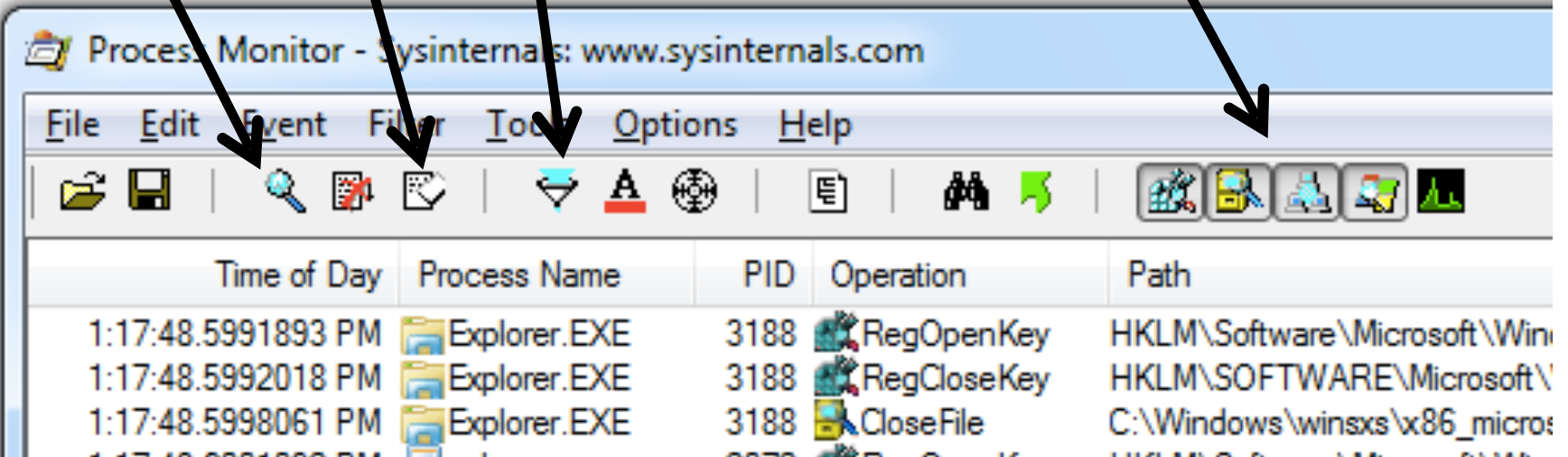
Process Monitor Toolbar

Start/Stop
Capture

Erase

Filter

Default Filters
Registry, File system, Network,
Processes



The screenshot shows the Process Monitor application window. The title bar reads "Process Monitor - Sysinternals: www.sysinternals.com". The menu bar includes "File", "Edit", "Event", "Filter", "Tools", "Options", and "Help". The toolbar contains several icons: a folder, a floppy disk, a magnifying glass (Start/Stop Capture), a red X (Erase), a funnel (Filter), a red triangle (Default Filters), a globe, a document, binoculars, a green arrow, and a group of icons including a bar chart, a magnifying glass, a blue arrow, a red arrow, and a green arrow. Arrows from the text labels point to the magnifying glass, red X, funnel, and the group of icons.

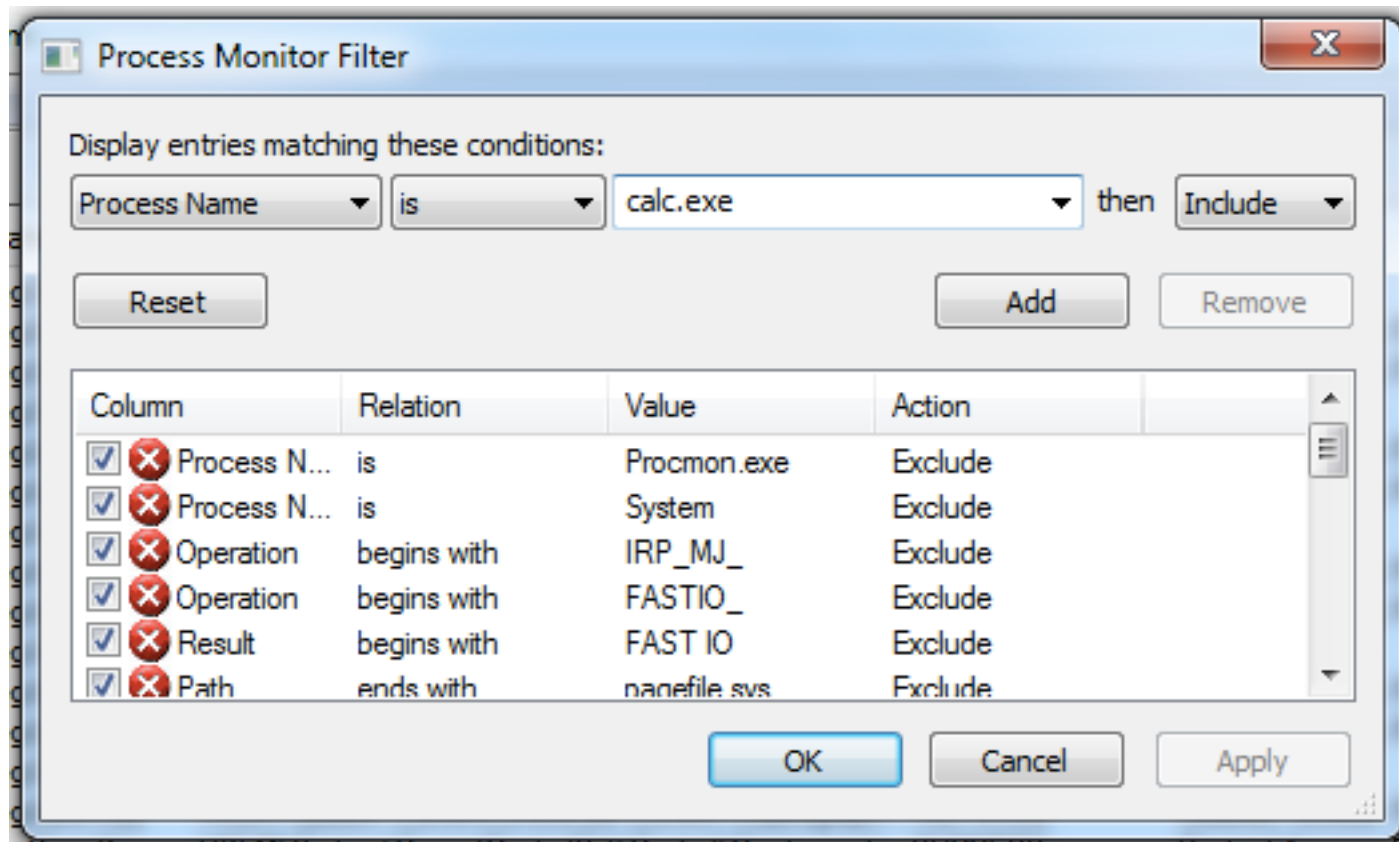
Time of Day	Process Name	PID	Operation	Path
1:17:48.5991893 PM	Explorer.EXE	3188	RegOpenKey	HKLM\Software\Microsoft\Win
1:17:48.5992018 PM	Explorer.EXE	3188	RegCloseKey	HKLM\SOFTWARE\Microsoft\
1:17:48.5998061 PM	Explorer.EXE	3188	CloseFile	C:\Windows\winsxs\x86_micros
1:17:48.6001000 PM		3070		HKLM\SOFTWARE\Microsoft\

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

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

File Options View Process Find Users Help

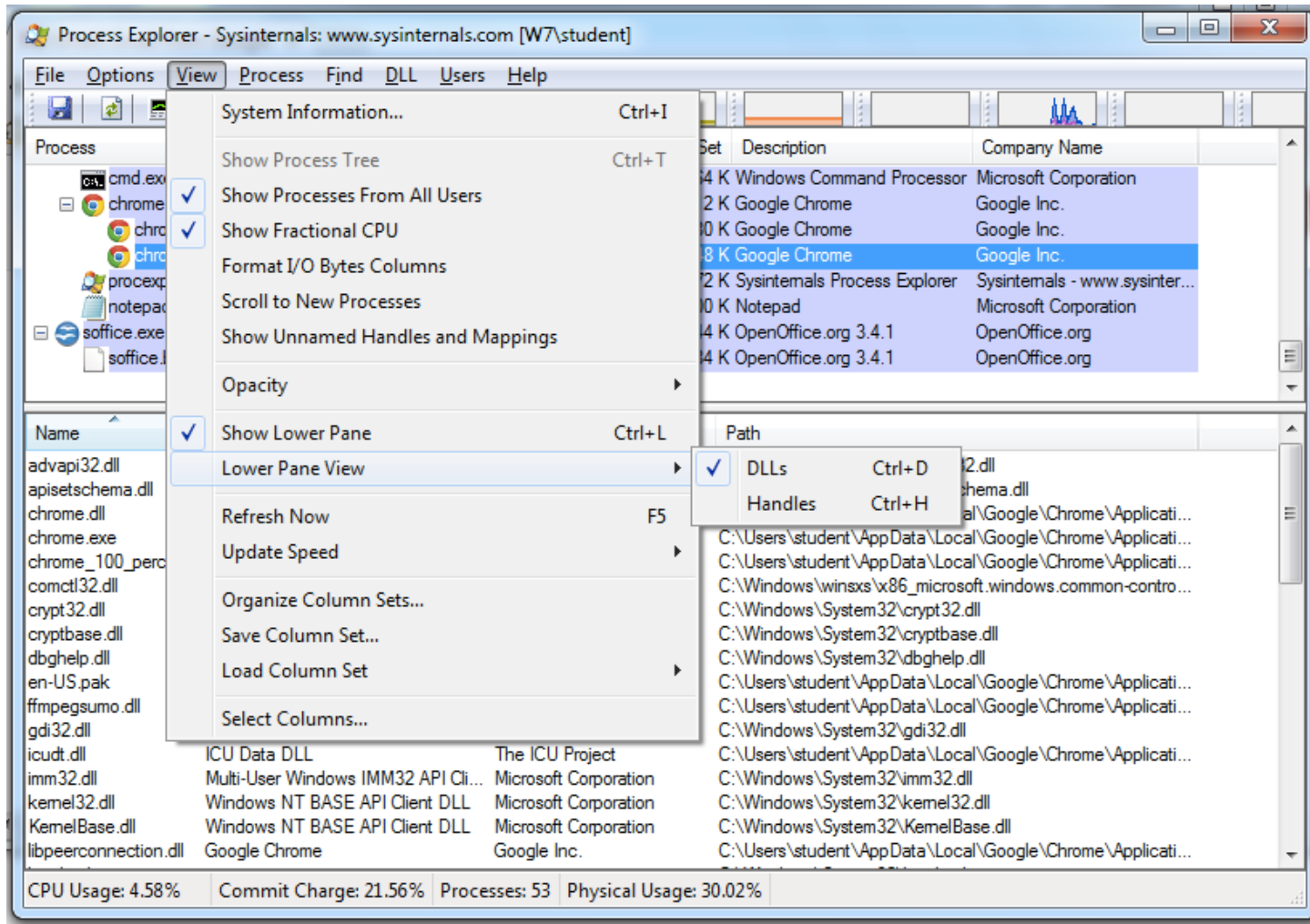
Process	PID	CPU	Private Bytes	Working Set	Description	Company Name
System Idle Process	0	96.81	0 K	24 K		
System	4	0.09	48 K	560 K		
Interrupts	n/a	0.88	0 K	0 K	Hardware Interrupts and DPCs	
smss.exe	260		224 K	748 K	Windows Session Manager	Microsoft Corporation
csrss.exe	348	< 0.01	1,252 K	3,164 K	Client 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
6 gogoc.exe	1592	< 0.01	1,216 K	3,920 K	gogoCLIENT	gogo6, Inc.
vm 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

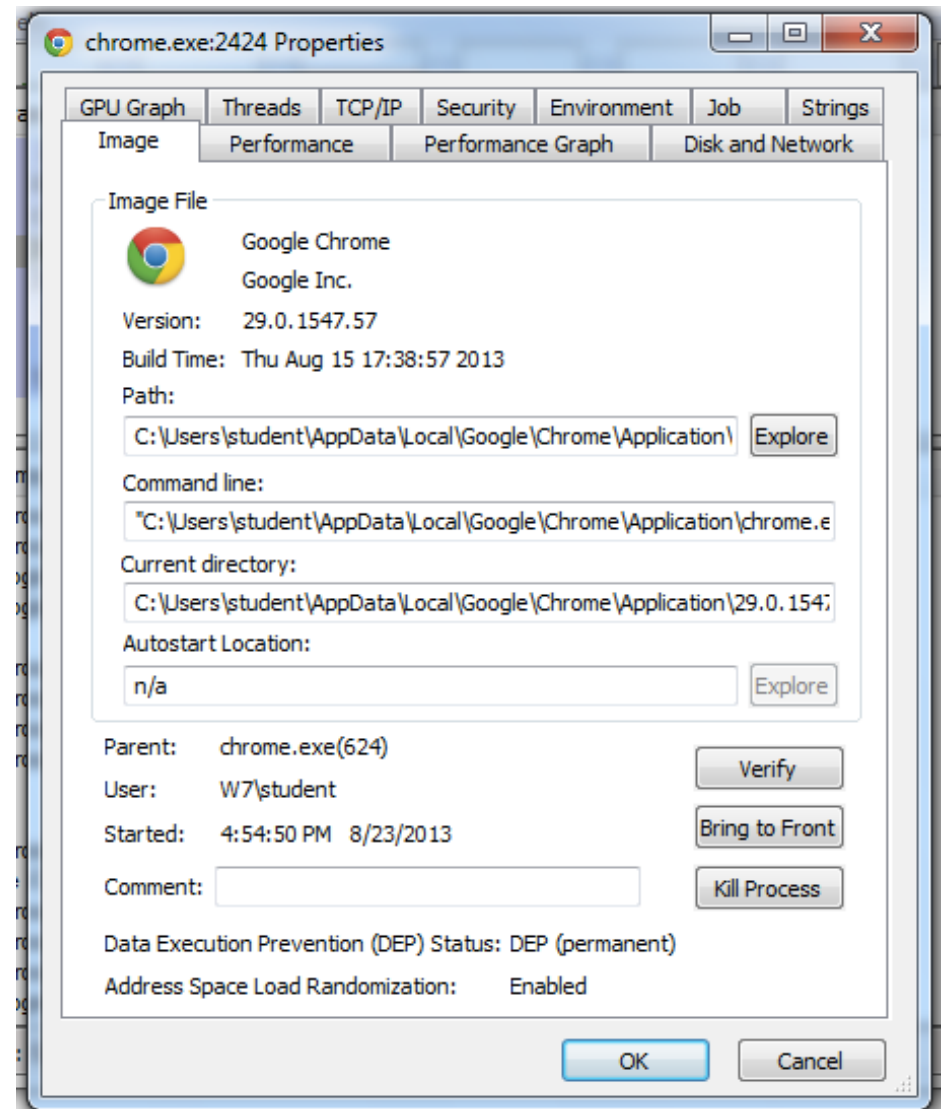
- Services are pink
- Processes are blue
- New processes are green briefly
- Terminated processes are red

DLL Mode



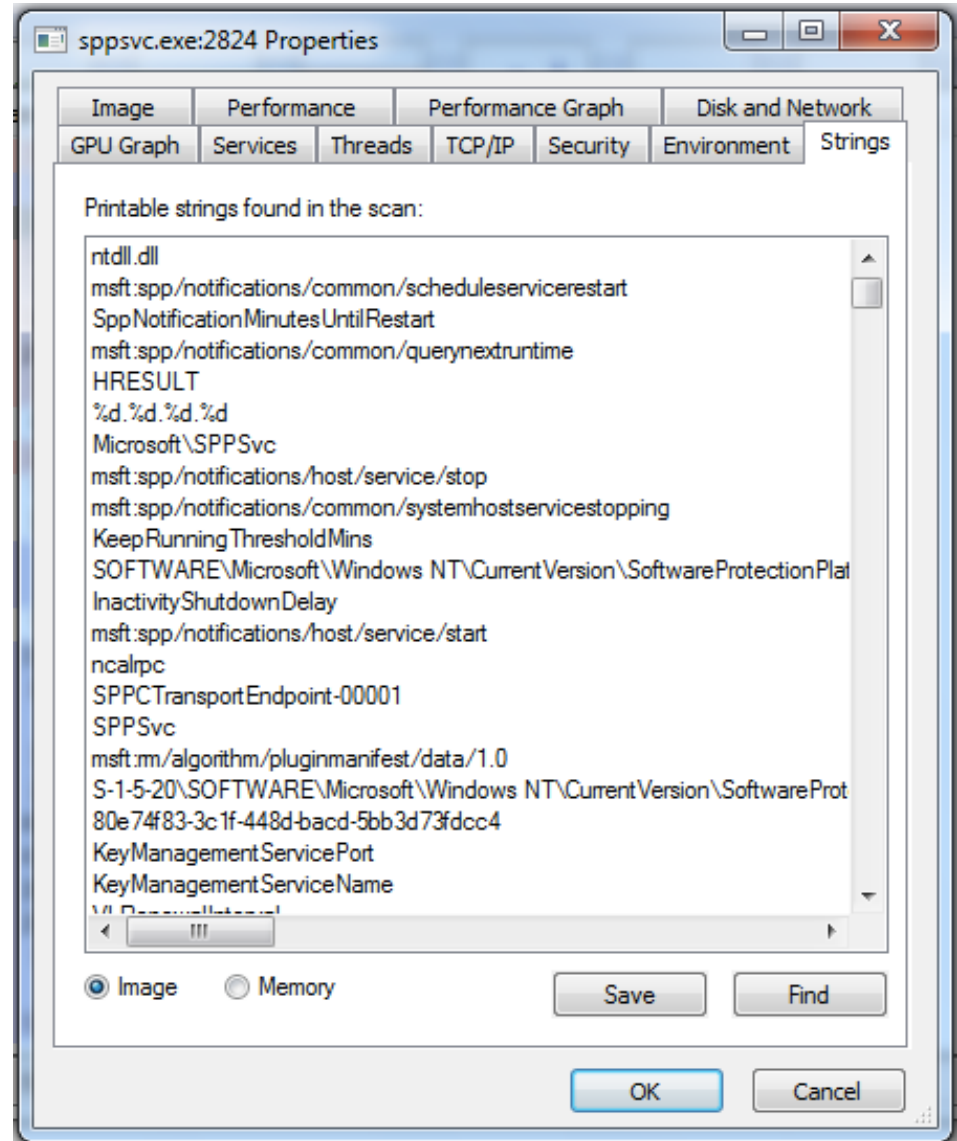
Properties

- 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



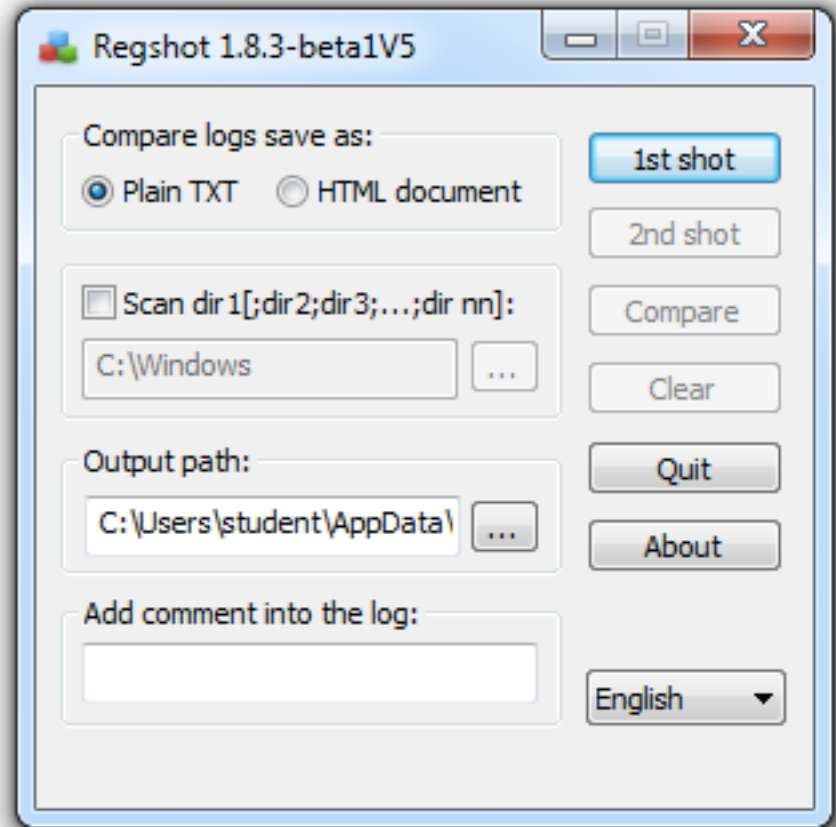
Detecting Malicious Documents

- 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

INetSim

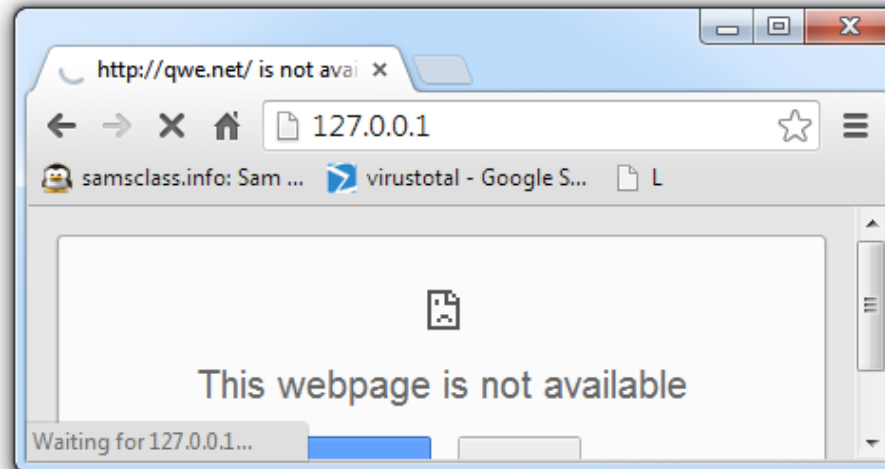
- Included in Kali Linux
- Simulates the Internet, including
 - HTTP / HTTPS
 - SMTP, POP3
 - DNS
 - FTP
 - Much more

Ncat Listener

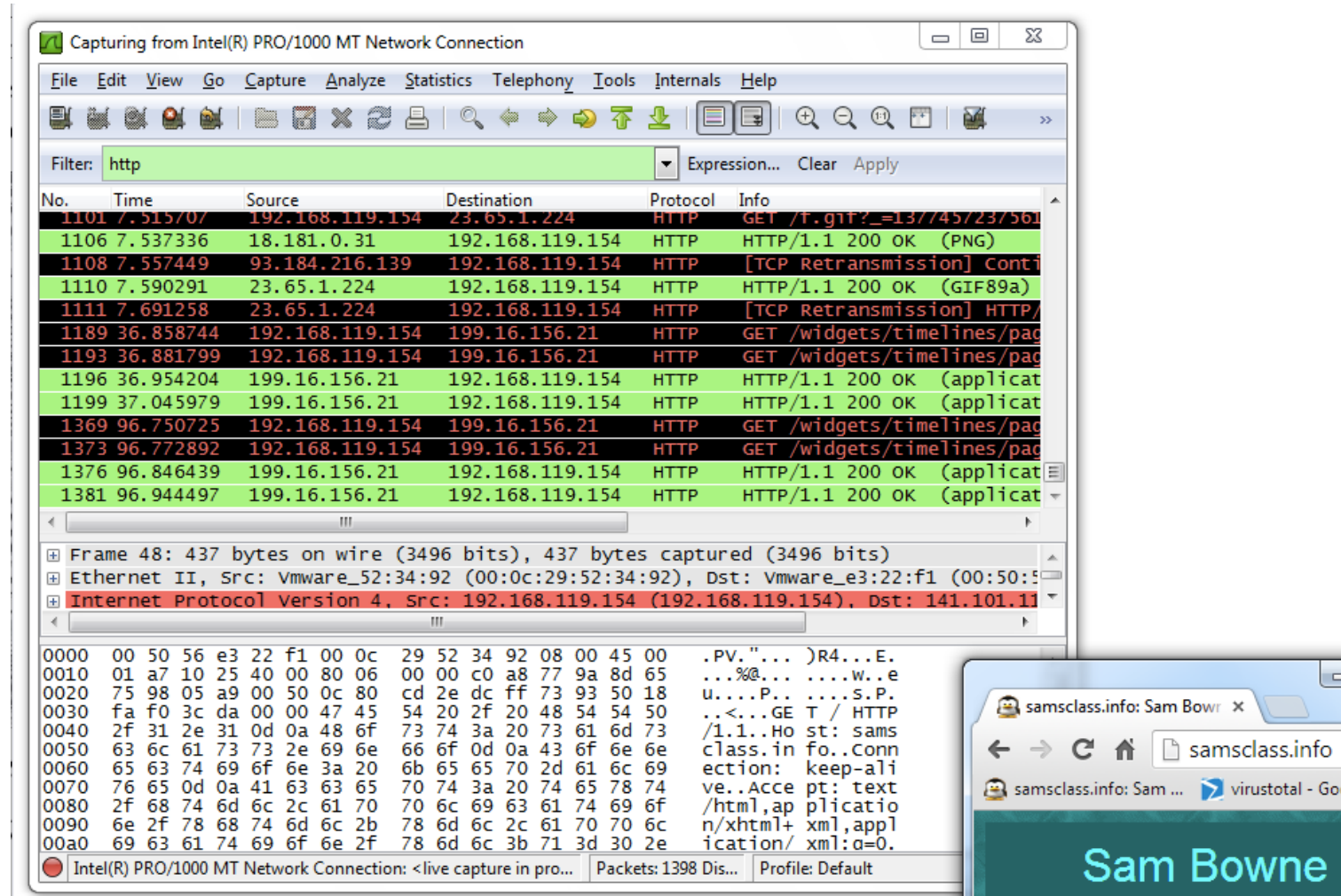
- Using Ncat.exe, you can listen on a single TCP port in Windows
 - In Linux, use nc (netcat)
- This will allow malware to complete a TCP handshake, so you get some rudimentary information about its requests
- But it's not a real server, so it won't reply to requests after the handshake

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
```

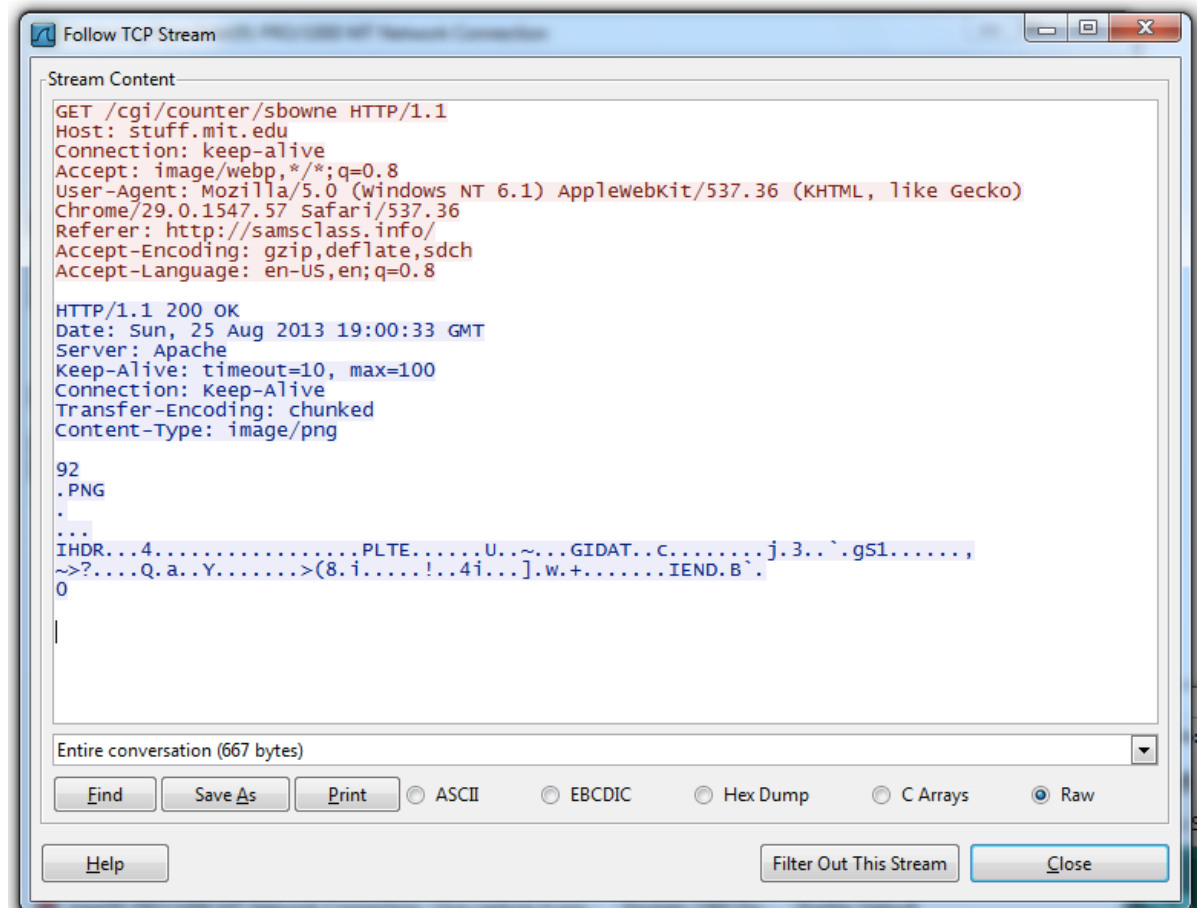


Packet Sniffing with Wireshark



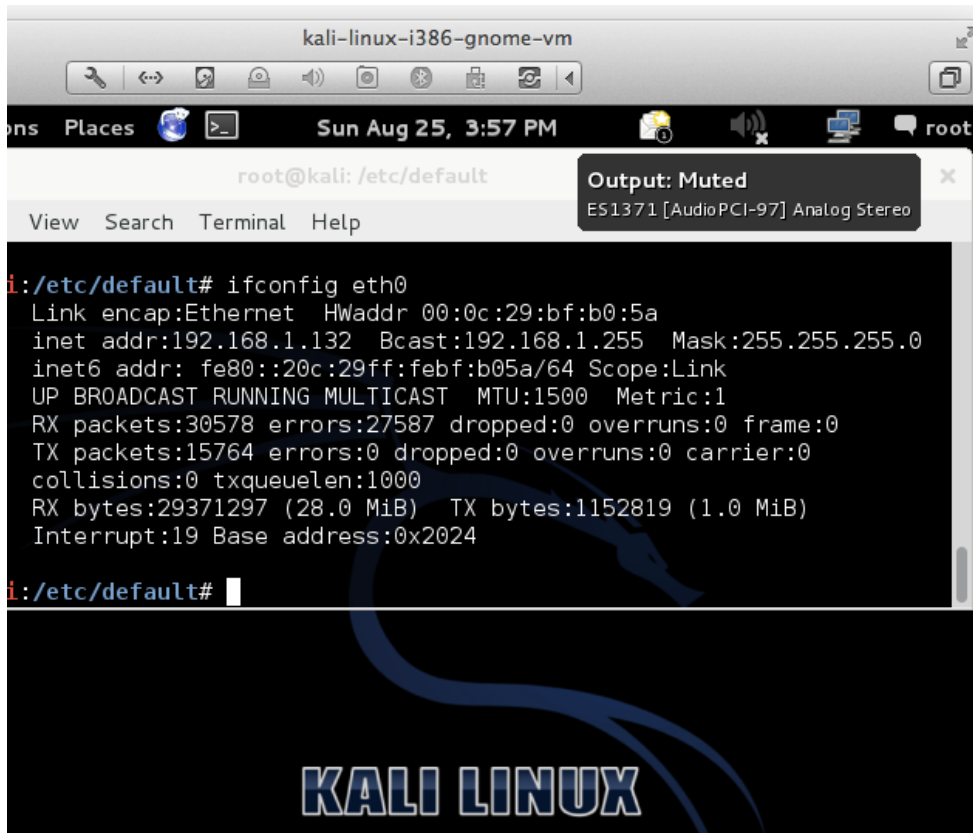
Follow TCP Stream

- Can save files from streams here too



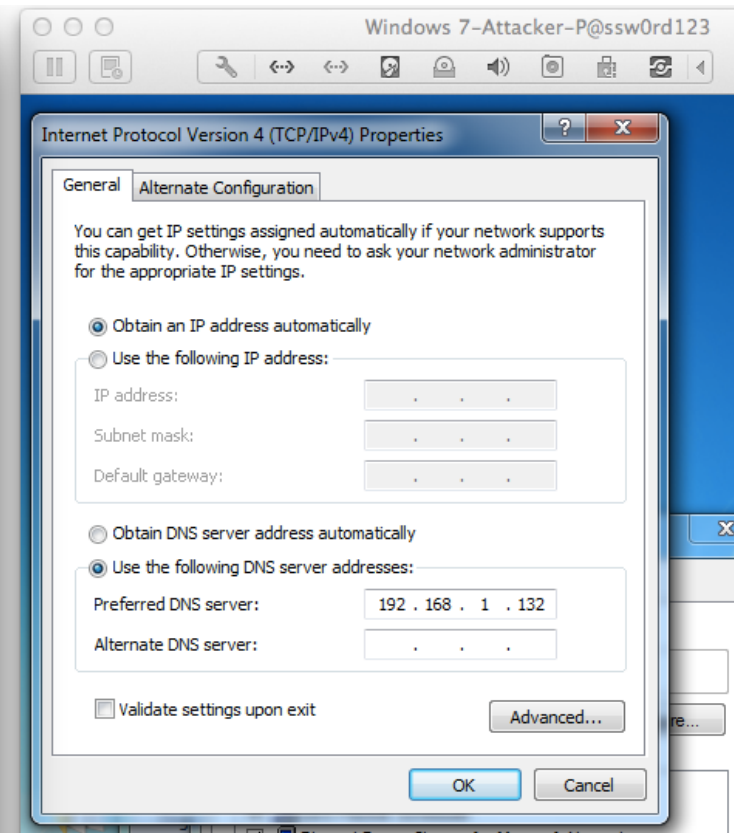
Using INetSim

inetsim

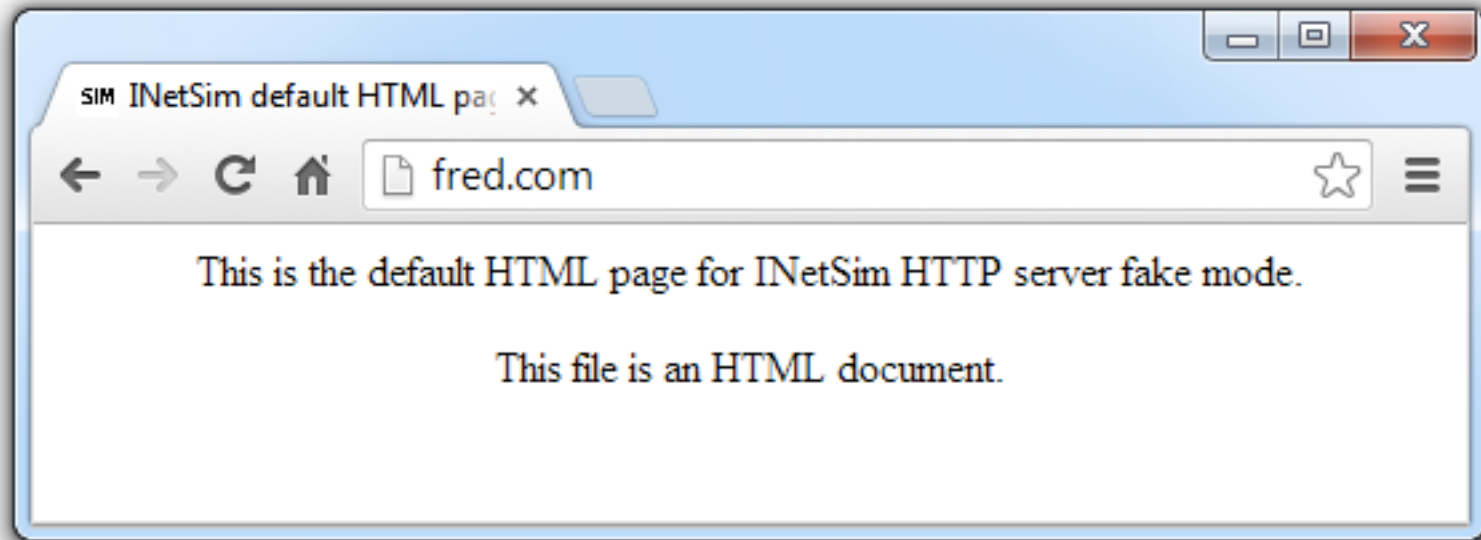


A terminal window titled 'kali-linux-i386-gnome-vm' showing the output of the 'ifconfig eth0' command. The window has a menu bar with 'View', 'Search', 'Terminal', and 'Help'. A notification bubble says 'Output: Muted ES1371 [AudioPCI-97] Analog Stereo'. The terminal output is as follows:

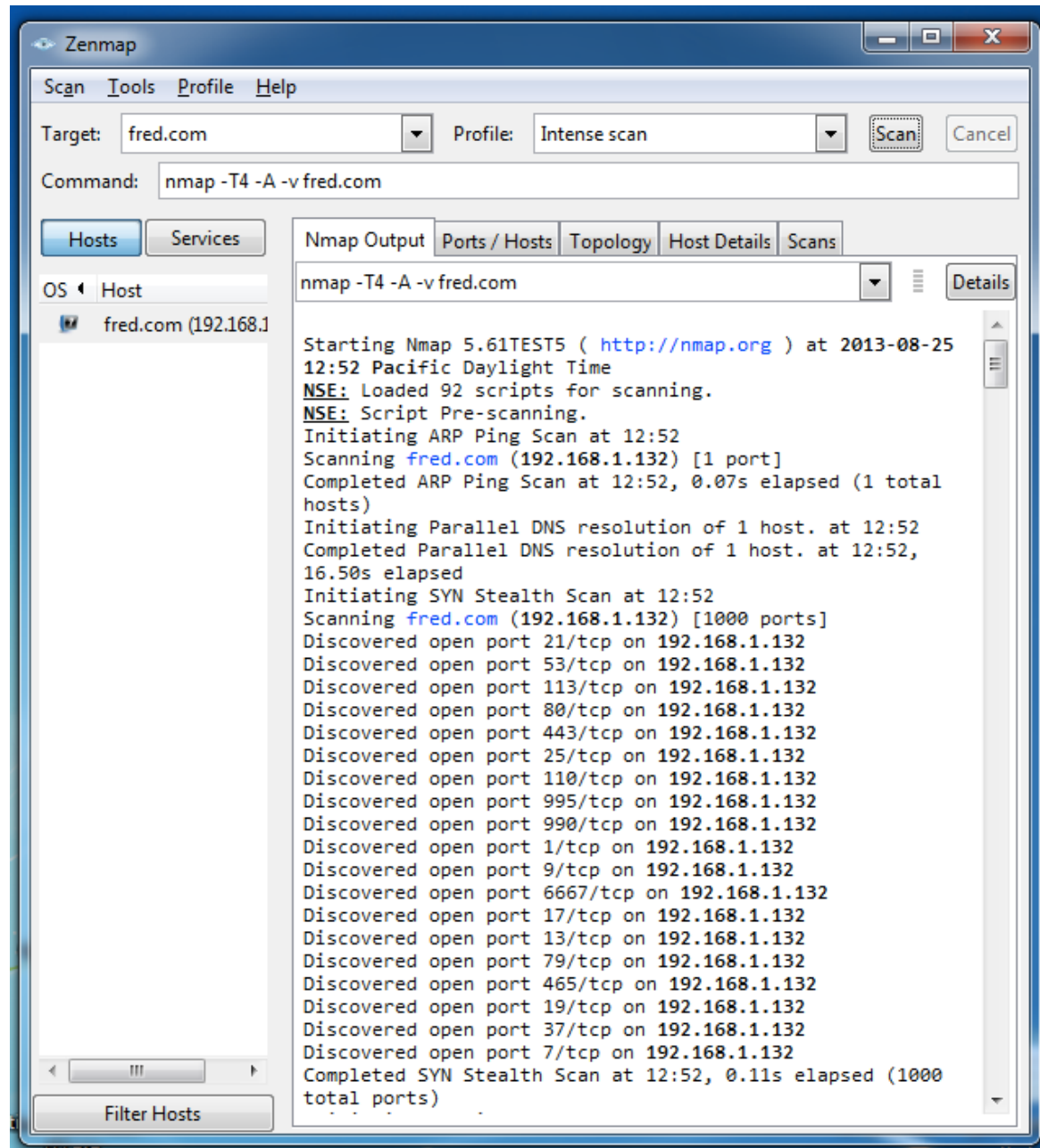
```
root@kali: /etc/default
View Search Terminal Help
Output: Muted
ES1371 [AudioPCI-97] Analog Stereo
root@kali: /etc/default# ifconfig eth0
Link encap:Ethernet HWaddr 00:0c:29:bf:b0:5a
inet addr:192.168.1.132 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:febf:b05a/64 Scope:Link
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

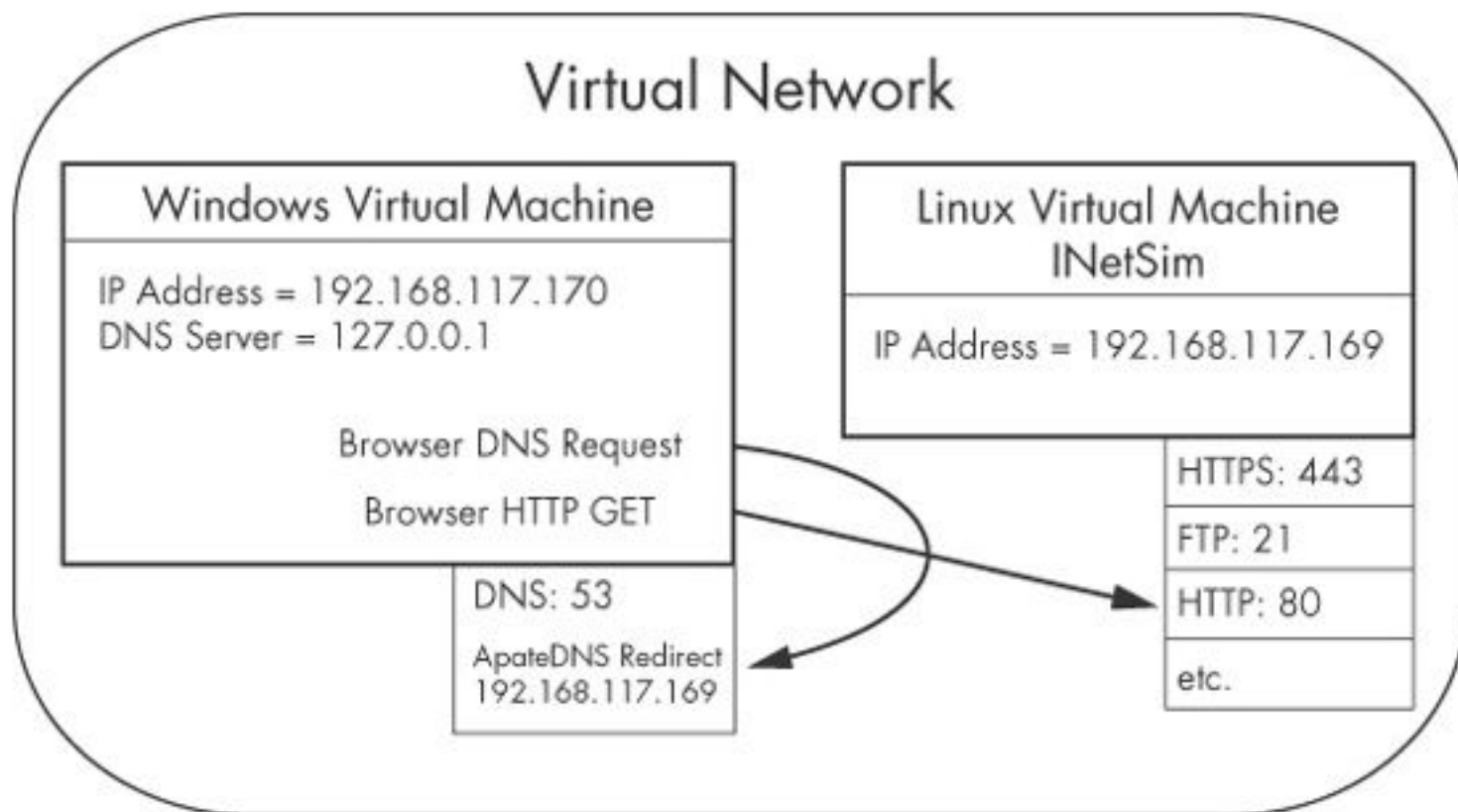


Figure 4-12. Example of a virtual network

Kahoot!