Chapter 5
Basic Dynamic Analysis

Mohd Zaki Mas’ud

Topic

- Malware Analysis in Virtual Machines
- Introduction to Dynamic Analysis
- Sandbox
- Running Malware
- ProcMon (Process Monitor)
- Process Explorer
- Faking a Network
- Using Inetsim
- Basic Dynamics Tool

MALWARE ANALYSIS IN VIRTUAL MACHINE

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 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.

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

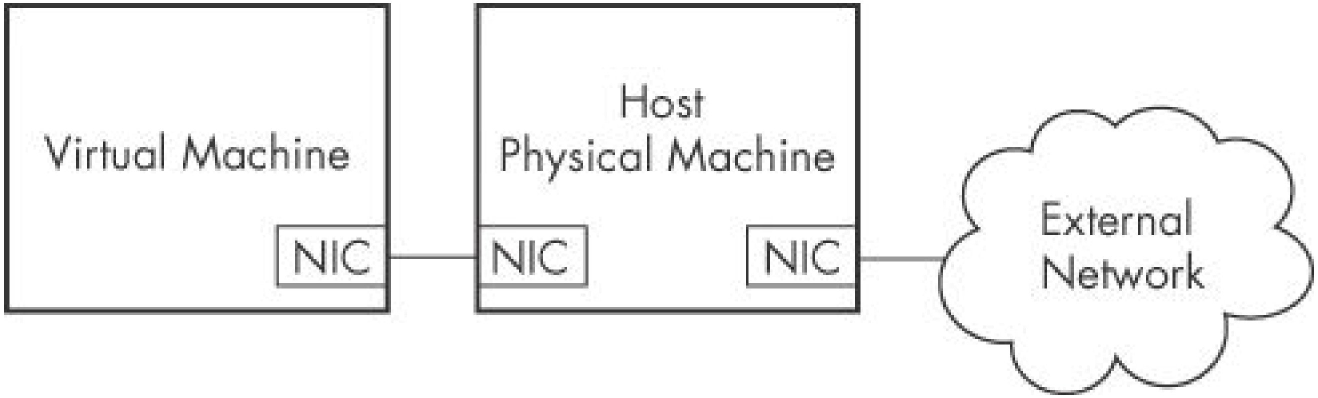


Figure 3-3. Host-only networking in VMware

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

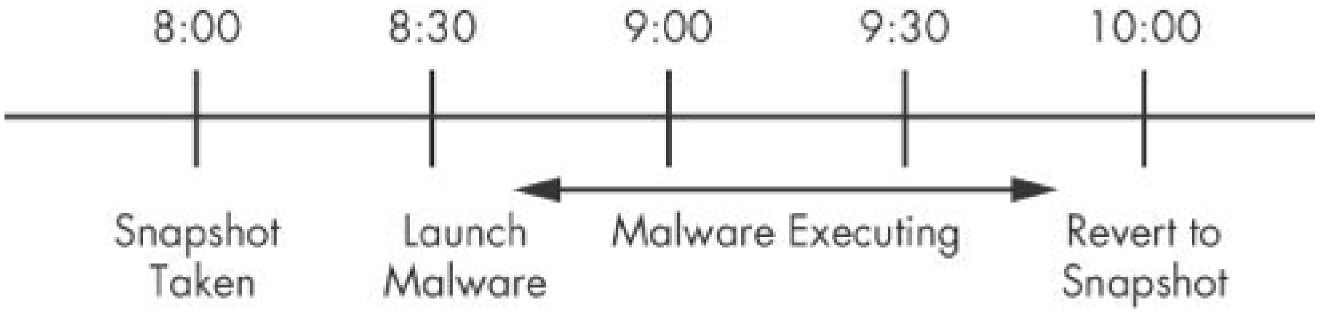


Figure 3-5. Snapshot timeline

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

PRACTICAL MALWARE ANALYSIS

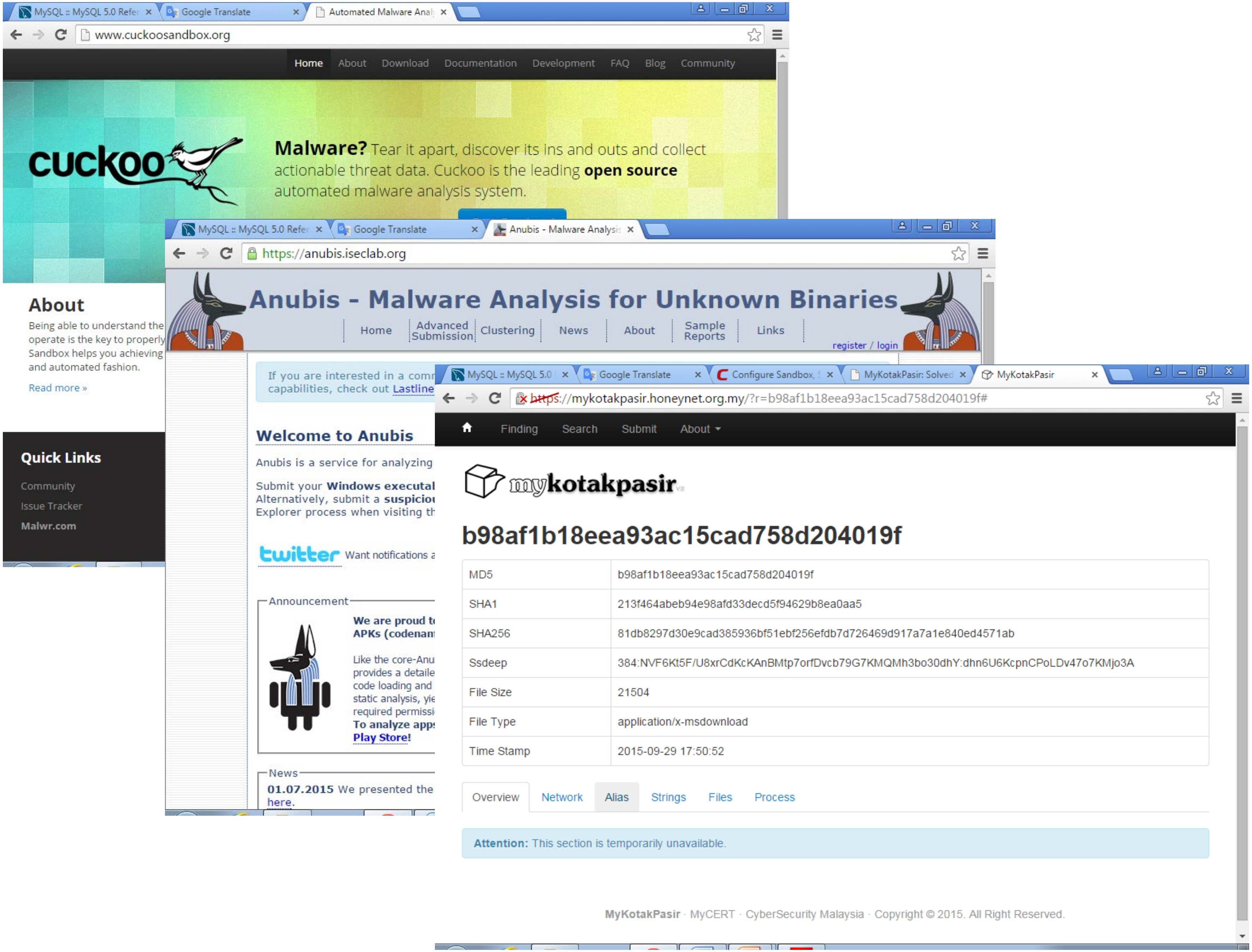
Why Perform Dynamic Analysis?

- 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



Malware? Tear it apart, discover its ins and outs and collect actionable threat data. Cuckoo is the leading **open source** automated malware analysis system.

About

Being able to understand the
operate is the key to properly
Sandbox helps you achieving
and automated fashion.

Read more »

Quick Links

Community
Issue Tracker
Malwr.com

Anubis - Malware Analysis for Unknown Binaries

If you are interested in a comm
capabilities, check out Lastline

Welcome to Anubis

Anubis is a service for analyzing

Submit your **Windows executal**
Alternatively, submit a **suspiciou**
Explorer process when visiting th

twitter Want notifications a

Announcement

We are proud t
APKs (codenam

Like the core-Anu
provides a detaile
code loading and
static analysis, yie
required permissi
To analyze app
Play Store!

News

01.07.2015 We presented the
here.

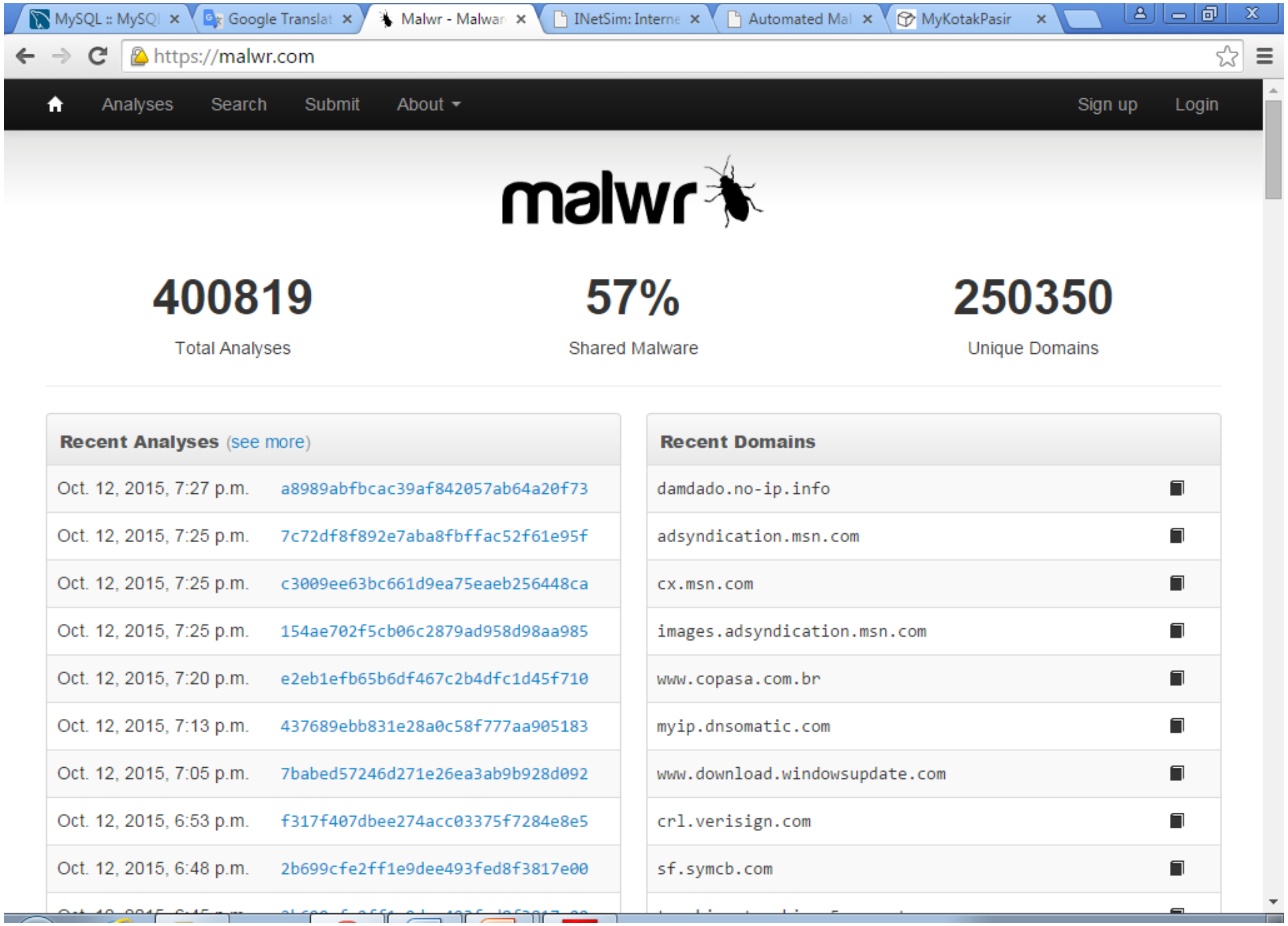
b98af1b18eea93ac15cad758d204019f

MD5	b98af1b18eea93ac15cad758d204019f
SHA1	213f464abeb94e98afd33decd5f94629b8ea0aa5
SHA256	81db8297d30e9cad385936bf51ebf256efdb7d726469d917a7a1e840ed4571ab
Ssdeep	384:NVF6Kt5F/U8xrCdKcKAnBMtp7orfDvcb79G7KMQMh3bo30dhY:dhn6U6KcpnCPoLDv47o7KMjo3A
File Size	21504
File Type	application/x-msdownload
Time Stamp	2015-09-29 17:50:52

Attention: This section is temporarily unavailable.

MyKotakPasir · MyCERT · CyberSecurity Malaysia · Copyright © 2015. All Right Reserved.

Malwr.com



400819	57%	250350
Total Analyses	Shared Malware	Unique Domains

Recent Analyses (see more)

Oct. 12, 2015, 7:27 p.m.	a8989abfbcac39af842057ab64a20f73
Oct. 12, 2015, 7:25 p.m.	7c72df8f892e7aba8fbffac52f61e95f
Oct. 12, 2015, 7:25 p.m.	c3009ee63bc661d9ea75eaeb256448ca
Oct. 12, 2015, 7:25 p.m.	154ae702f5cb06c2879ad958d98aa985
Oct. 12, 2015, 7:20 p.m.	e2eb1efb65b6df467c2b4dfc1d45f710
Oct. 12, 2015, 7:13 p.m.	437689ebb831e28a0c58f777aa905183
Oct. 12, 2015, 7:05 p.m.	7babed57246d271e26ea3ab9b928d092
Oct. 12, 2015, 6:53 p.m.	f317f407dbee274acc03375f7284e8e5
Oct. 12, 2015, 6:48 p.m.	2b699cfe2ff1e9dee493fed8f3817e00

Recent Domains

damdado.no-ip.info
adsyndication.msn.com
cx.msn.com
images.adsyndication.msn.com
www.copasa.com.br
myip.dnsomatic.com
www.download.windowsupdate.com
crl.verisign.com
sf.symcb.com

Potential Drawbacks

- Malware often detects when it is running in a virtual machine, and if a virtual machine is detected, the malware might stop running or behave differently. Not all sandboxes take this issue into account.
- Some malware requires the presence of certain registry keys or files on the system that might not be found in the sandbox. These might be required to contain legitimate data, such as commands or encryption keys.
- If the malware is a DLL, certain exported functions will not be invoked properly, because a DLL will not run as easily as an executable.
- The sandbox environment OS may not be correct for the malware. For example, the malware might crash on Windows XP but run correctly in Windows 7.
- A sandbox cannot tell you what the malware does. It may report basic functionality, but it cannot tell you that the malware is a custom Security Accounts Manager (SAM) hash dump utility or an encrypted keylogging backdoor, for example. Those are conclusions that you must draw on your own.

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
```

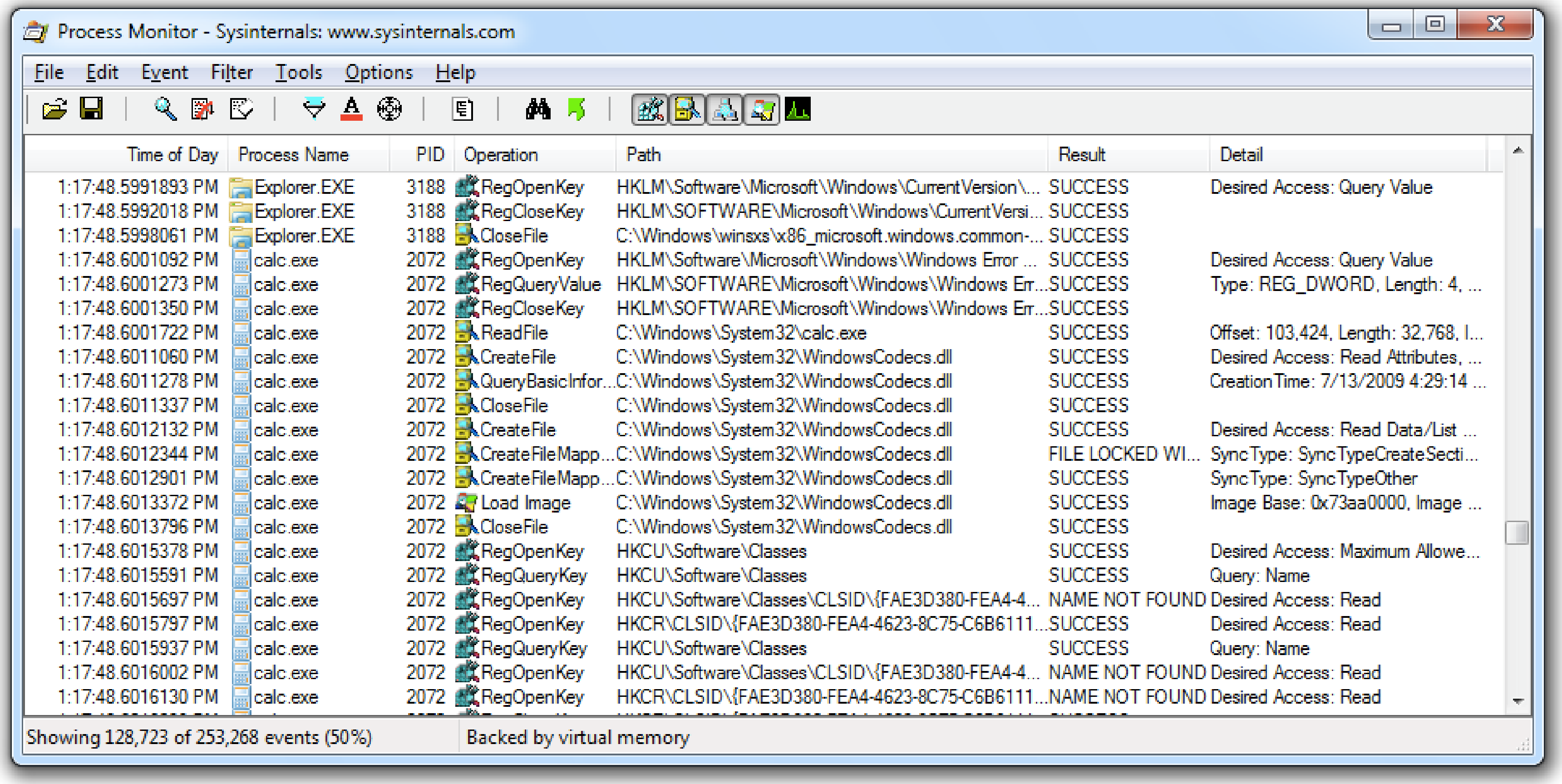
- It's also possible to modify the PE header and convert a DLL into an EXE

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



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

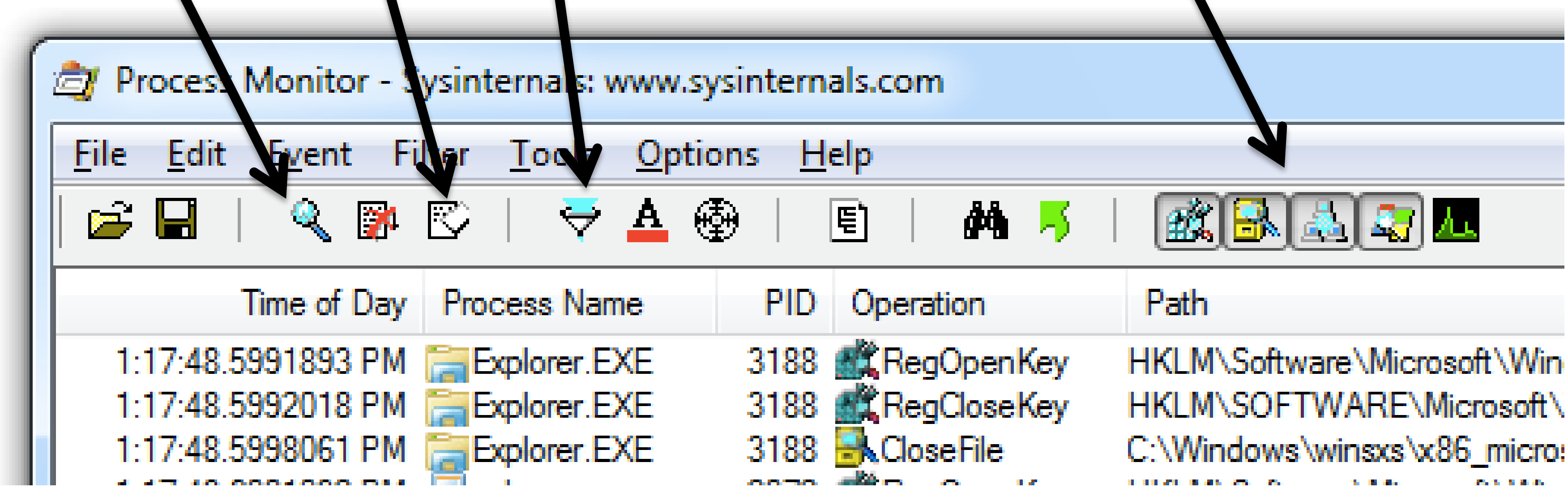
Process Monitor Toolbar

Start/Stop Capture

Erase

Filter

Default Filters
Registry, File system, Network, Processes



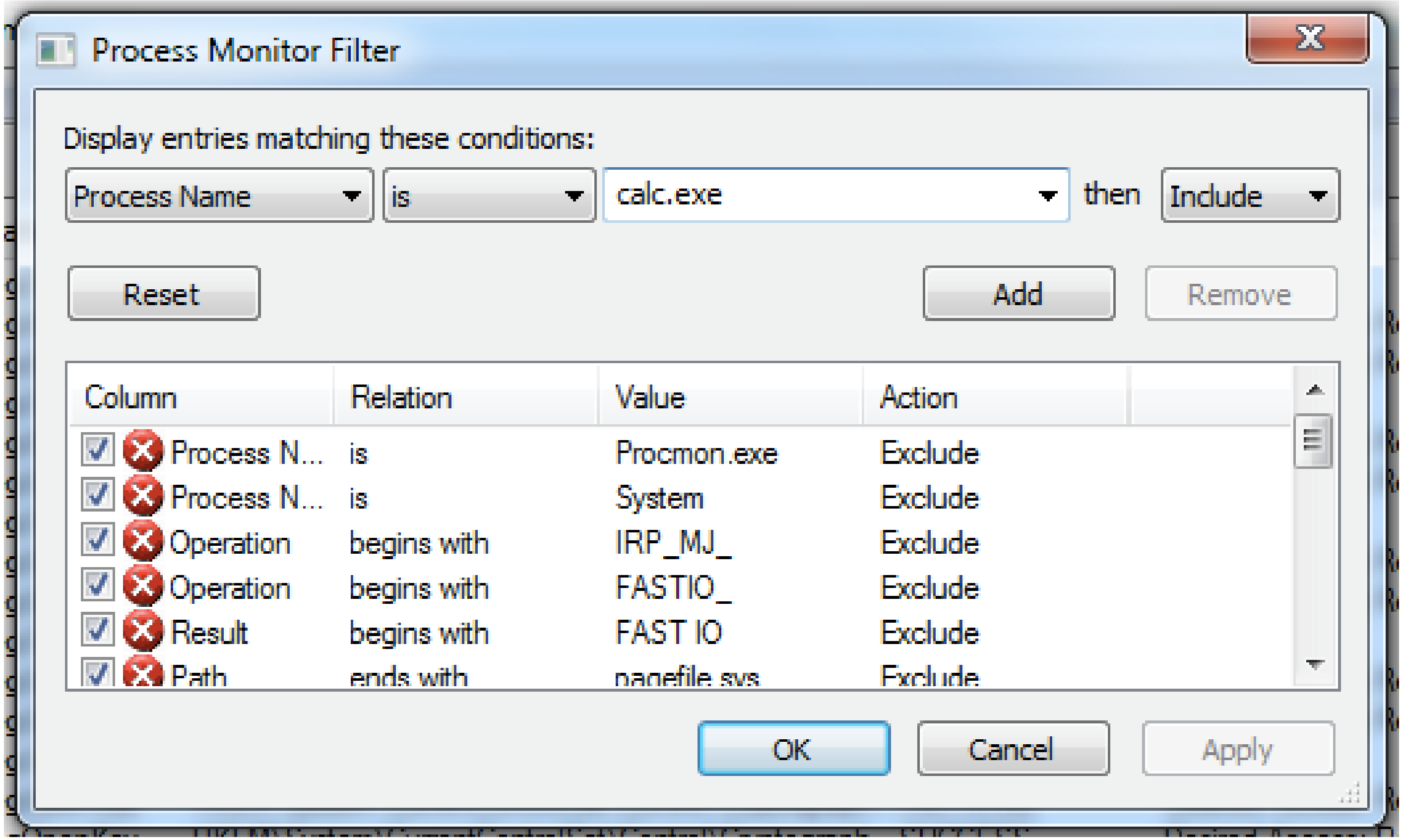
Time of Day	Process Name	PID	Operation	Path
1:17:48.5991893 PM	Explorer.EXE	3188	RegOpenKey	HKLM\Software\Microsoft\Win
1:17:48.5992018 PM	Explorer.EXE	3188	RegCloseKey	HKLM\SOFTWARE\Microsoft\
1:17:48.5998061 PM	Explorer.EXE	3188	CloseFile	C:\Windows\winsxs\x86_micro

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



Display entries matching these conditions:

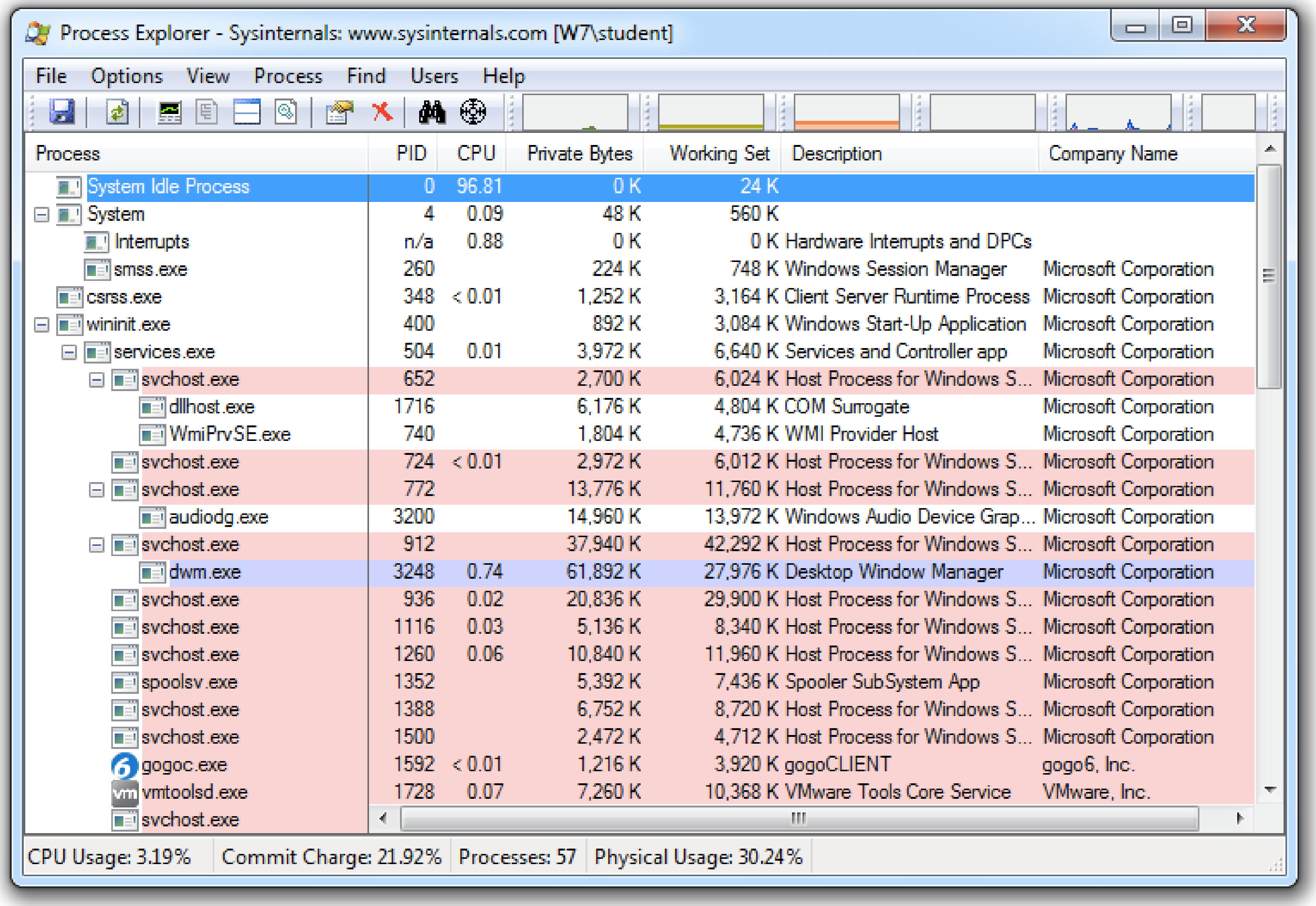
Process Name ▾ | is ▾ | calc.exe ▾ | then | Include ▾

	Column	Relation	Value	Action
☑	Process N...	is	Procmon.exe	Exclude
☑	Process N...	is	System	Exclude
☑	Operation	begins with	IRP_MJ_	Exclude
☑	Operation	begins with	FASTIO_	Exclude
☑	Result	begins with	FAST IO	Exclude
☑	Path	ends with	pagefile.sys	Exclude

Procmon provides helpful automatic filters on its toolbar

- **Registry** By examining registry operations, you can tell how a piece of malware installs itself in the registry.
- **File system** Exploring file system interaction can show all files that the malware creates or configuration files it uses.
- **Process activity** Investigating process activity can tell you whether the malware spawned additional processes.
- **Network** Identifying network connections can show you any ports on which the malware is listening.

VIEWING PROCESSES WITH PROCESS EXPLORER



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

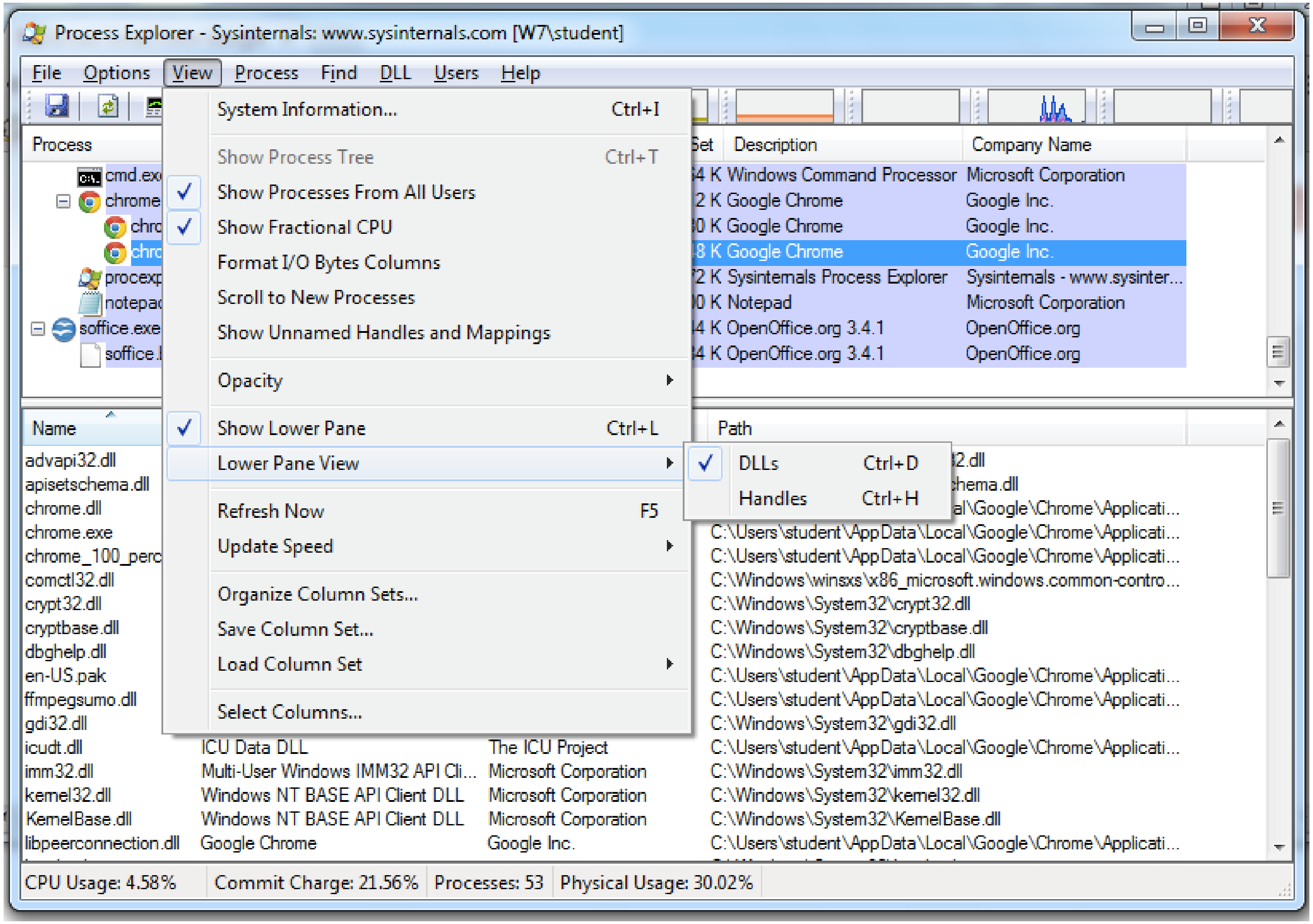
Process	PID	CPU	Private Bytes	Working Set	Description	Company Name
System Idle Process	0	96.81	0 K	24 K		
System	4	0.09	48 K	560 K		
Interrupts	n/a	0.88	0 K	0 K	Hardware Interrupts and DPCs	
smss.exe	260		224 K	748 K	Windows Session Manager	Microsoft Corporation
csrss.exe	348	< 0.01	1,252 K	3,164 K	Client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

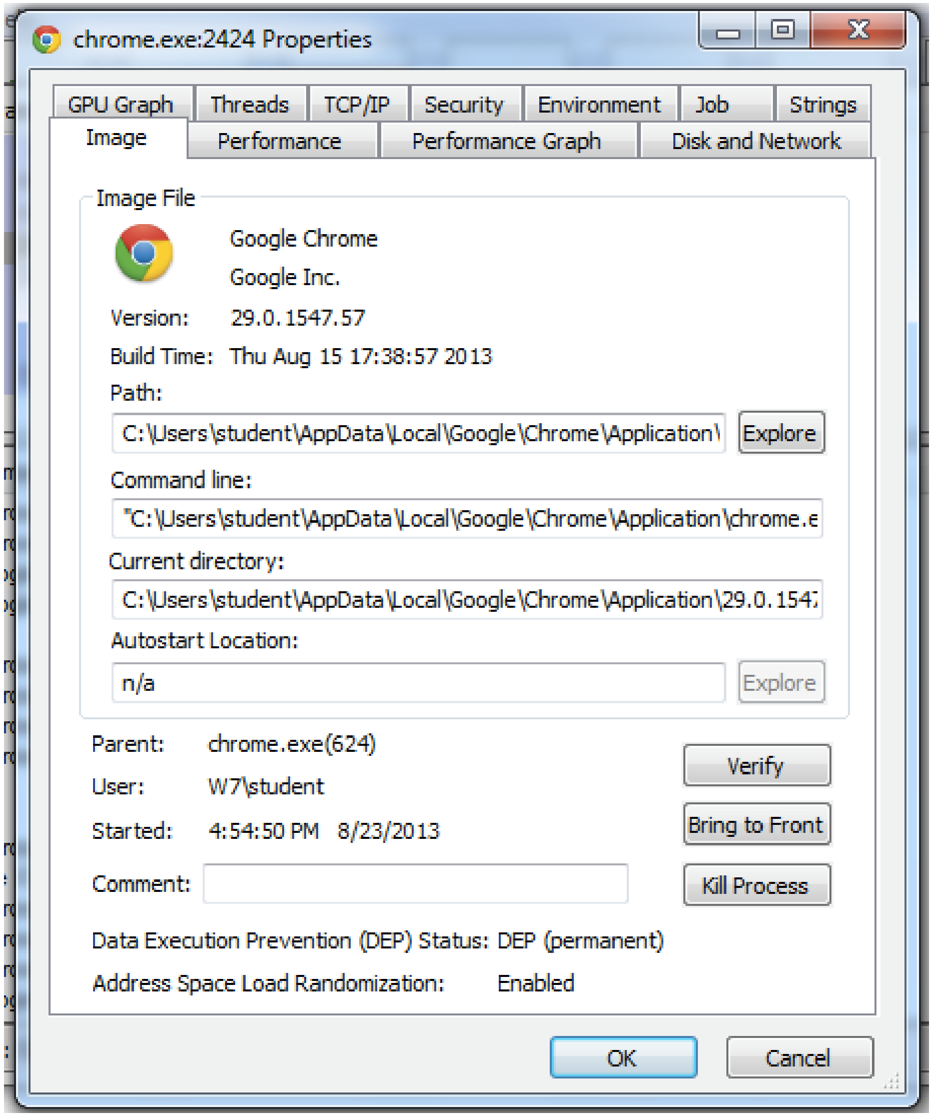
Process	Set	Description	Company Name
cmd.ex	4 K	Windows Command Processor	Microsoft Corporation
chrome	2 K	Google Chrome	Google Inc.
chro	0 K	Google Chrome	Google Inc.
chro	8 K	Google Chrome	Google Inc.
procexp	2 K	Sysinternals Process Explorer	Sysinternals - www.sysinter...
notepad	0 K	Notepad	Microsoft Corporation
soffice.exe	4 K	OpenOffice.org 3.4.1	OpenOffice.org
soffice.l	4 K	OpenOffice.org 3.4.1	OpenOffice.org

Name			Path
advapi32.dll			2.dll
apisetschema.dll			hema.dll
chrome.dll			al\Google\Chrome\Applicati...
chrome.exe			C:\Users\student\AppData\Local\Google\Chrome\Applicati...
chrome_100_perc			C:\Users\student\AppData\Local\Google\Chrome\Applicati...
comctl32.dll			C:\Windows\winsxs\x86_microsoft.windows.common-contro...
crypt32.dll			C:\Windows\System32\crypt32.dll
cryptbase.dll			C:\Windows\System32\cryptbase.dll
dbghelp.dll			C:\Windows\System32\dbghelp.dll
en-US.pak			C:\Users\student\AppData\Local\Google\Chrome\Applicati...
ffmpegsumo.dll			C:\Users\student\AppData\Local\Google\Chrome\Applicati...
gdi32.dll			C:\Windows\System32\gdi32.dll
icudt.dll	ICU Data DLL	The ICU Project	C:\Users\student\AppData\Local\Google\Chrome\Applicati...
imm32.dll	Multi-User Windows IMM32 API Cli...	Microsoft Corporation	C:\Windows\System32\imm32.dll
kernel32.dll	Windows NT BASE API Client DLL	Microsoft Corporation	C:\Windows\System32\kernel32.dll
KernelBase.dll	Windows NT BASE API Client DLL	Microsoft Corporation	C:\Windows\System32\KernelBase.dll
libpeerconnection.dll	Google Chrome	Google Inc.	C:\Users\student\AppData\Local\Google\Chrome\Applicati...

CPU Usage: 4.58% | Commit Charge: 21.56% | Processes: 53 | Physical Usage: 30.02%

Properties

- Verify button checks the disk file's Windows signature
  - But not the RAM image, so it won't detect **process replacement**



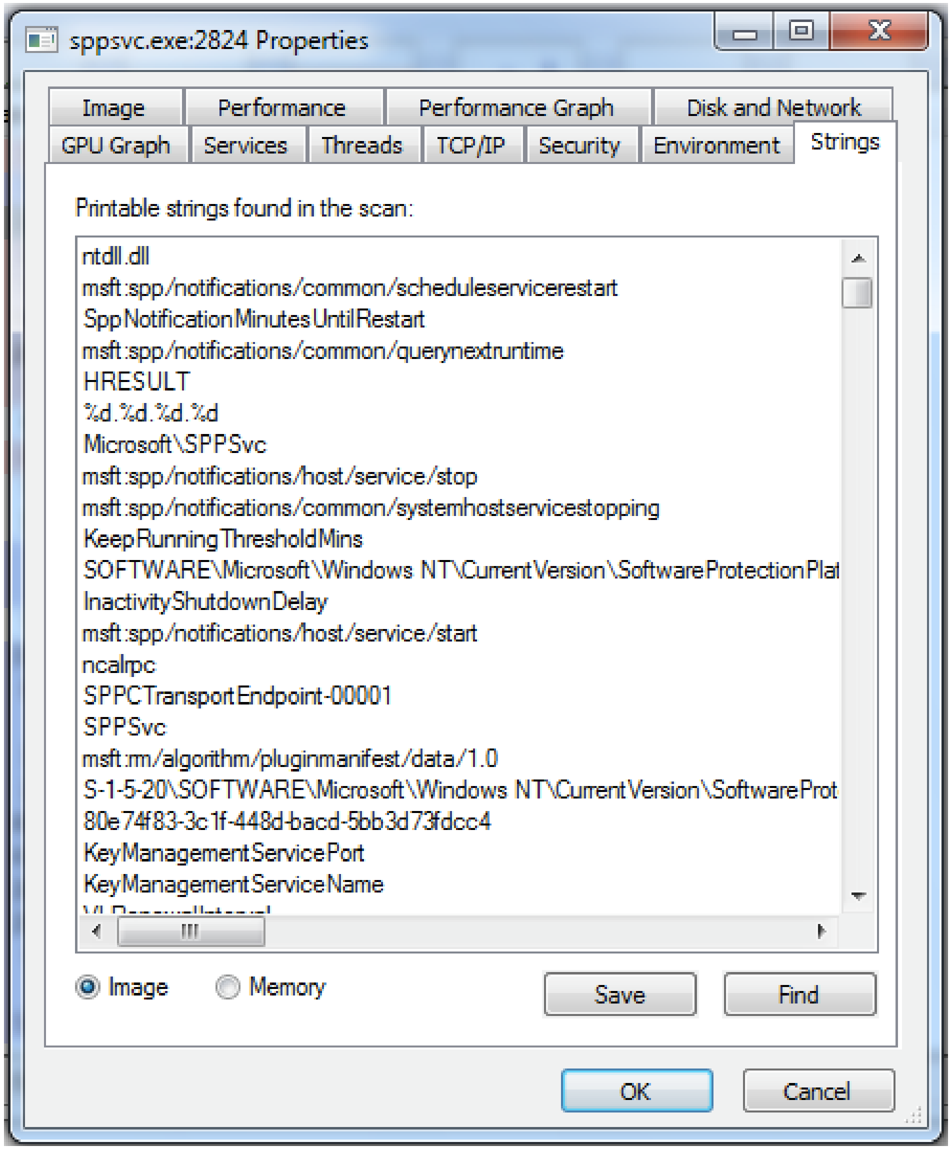
Google Chrome
Google Inc.
Version: 29.0.1547.57
Build Time: Thu Aug 15 17:38:57 2013
Path:
C:\Users\student\AppData\Local\Google\Chrome\Application\
Command line:
"C:\Users\student\AppData\Local\Google\Chrome\Application\chrome.e
Current directory:
C:\Users\student\AppData\Local\Google\Chrome\Application\29.0.154
Autostart Location:
n/a

Parent: chrome.exe(624)
User: W7\student
Started: 4:54:50 PM 8/23/2013
Comment:

Data Execution Prevention (DEP) Status: DEP (permanent)
Address Space Load Randomization: Enabled

Strings

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



Printable strings found in the scan:

```
ntdll.dll
msft:spp/notifications/common/scheduleservicerestart
SppNotificationMinutesUntilRestart
msft:spp/notifications/common/querynextruntime
HRESULT
%d.%d.%d.%d
Microsoft\SPPSvc
msft:spp/notifications/host/service/stop
msft:spp/notifications/common/systemhostservicestopping
KeepRunningThresholdMins
SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlat
InactivityShutdownDelay
msft:spp/notifications/host/service/start
ncalrpc
SPPCTransportEndpoint-00001
SPPSvc
msft:rm/algorithm/pluginmanifest/data/1.0
S-1-5-20\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProt
80e74f83-3c1f-448d-bacd-5bb3d73fdcc4
KeyManagementServicePort
KeyManagementServiceName
```

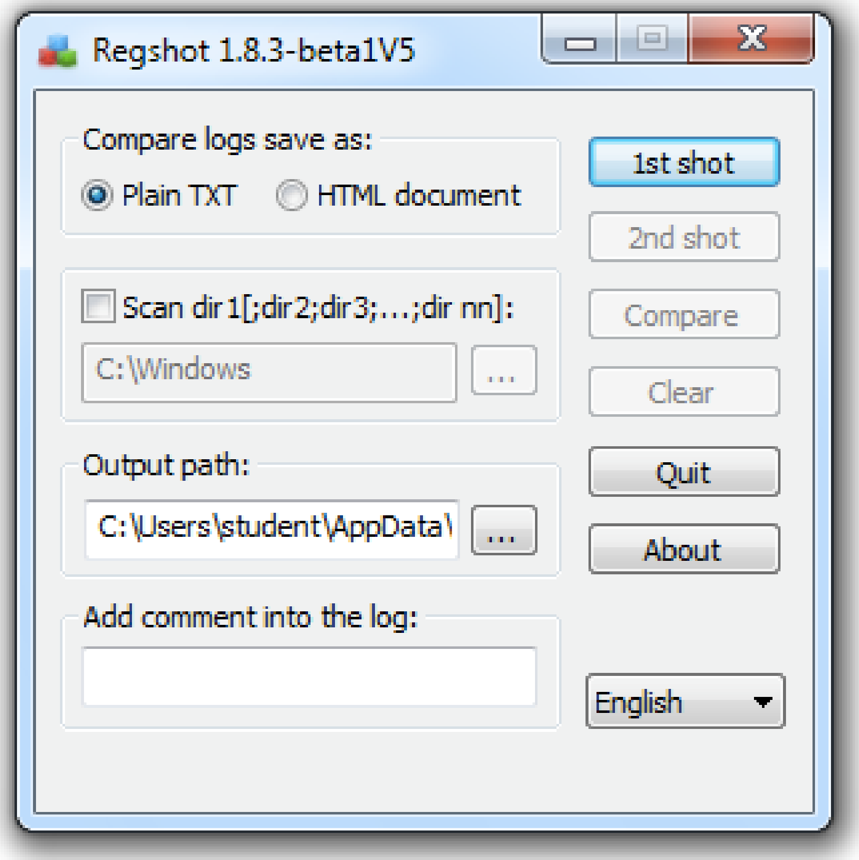
● Image ○ Memory

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 is an open source registry comparison tool that allows you to take and compare two registry snapshots.
- To use Regshot for malware analysis, simply take the first shot by clicking the **1st Shot** button, and then run the malware and wait for it to finish making any system changes.
- Next, take the second shot by clicking the **2nd Shot** button. Finally, click the **Compare** button to compare the two snapshots.



Regshot 1.8.3-beta1V5

Compare logs save as:

● Plain TXT ○ HTML document

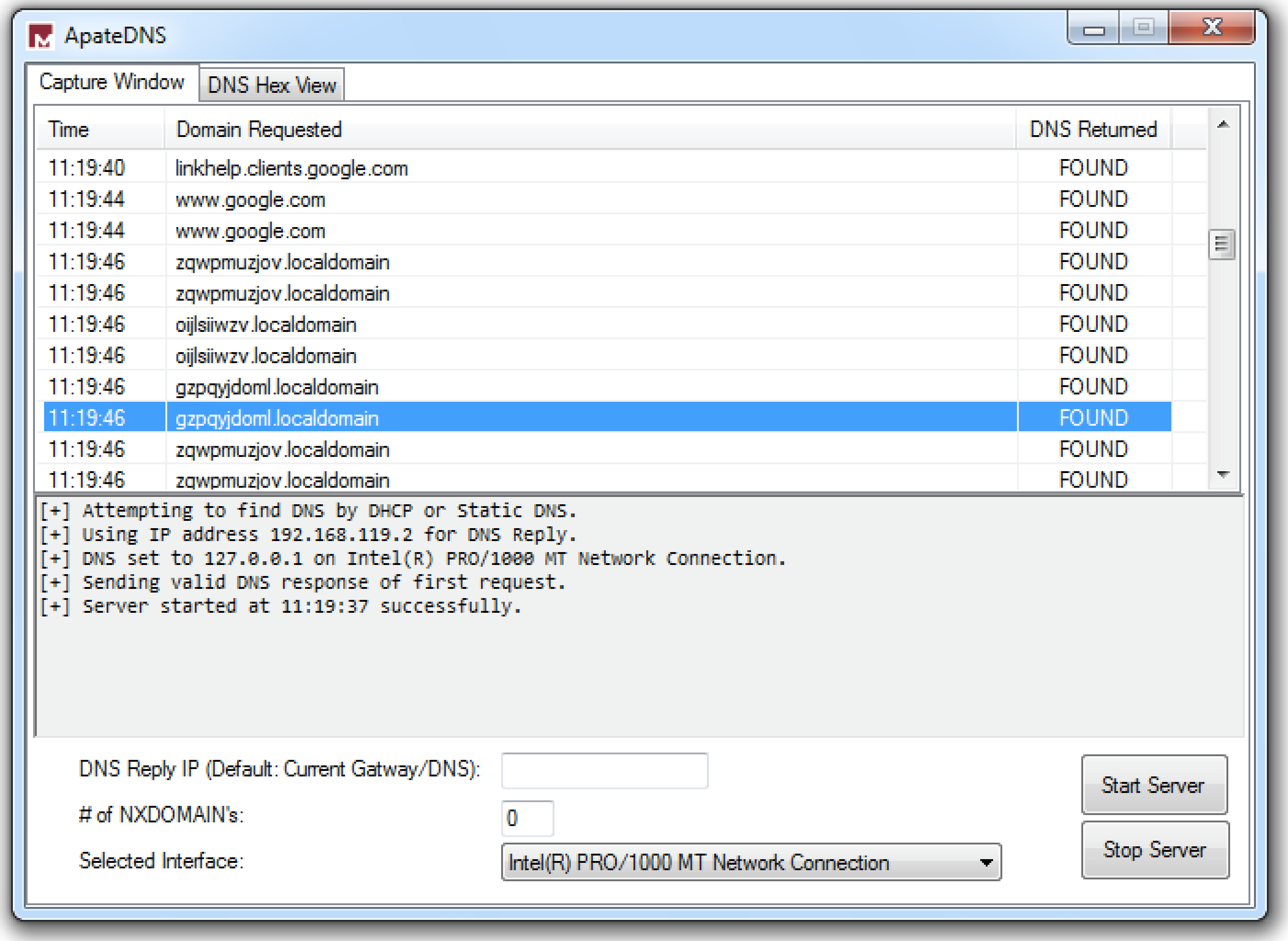
□ Scan dir1[;dir2;dir3;...;dir nn]: C:\Windows

Output path: C:\Users\student\AppData\

Add comment into the log:

FAKING A NETWORK

Using ApateDNS to Redirect DNS Resolutions



Time	Domain Requested	DNS Returned
11:19:40	linkhelp.clients.google.com	FOUND
11:19:44	www.google.com	FOUND
11:19:44	www.google.com	FOUND
11:19:46	zqwpmuzjov.localdomain	FOUND
11:19:46	zqwpmuzjov.localdomain	FOUND
11:19:46	oijlsiiwzv.localdomain	FOUND
11:19:46	oijlsiiwzv.localdomain	FOUND
11:19:46	gzpqyjdoml.localdomain	FOUND
11:19:46	gzpqyjdoml.localdomain	FOUND
11:19:46	zqwpmuzjov.localdomain	FOUND
11:19:46	zqwpmuzjov.localdomain	FOUND

```
[+] Attempting to find DNS by DHCP or Static DNS.
[+] Using IP address 192.168.119.2 for DNS Reply.
[+] DNS set to 127.0.0.1 on Intel(R) PRO/1000 MT Network Connection.
[+] Sending valid DNS response of first request.
[+] Server started at 11:19:37 successfully.
```

DNS Reply IP (Default: Current Gatway/DNS):

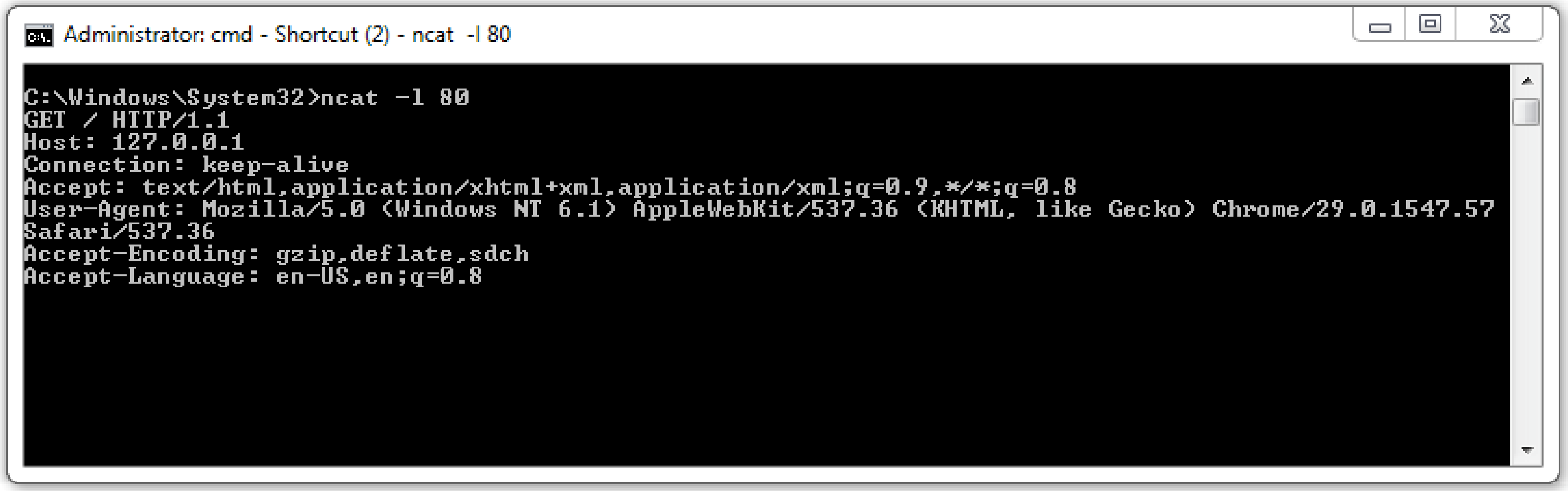
# of NXDOMAIN's: 0

Selected Interface: Intel(R) PRO/1000 MT Network Connection

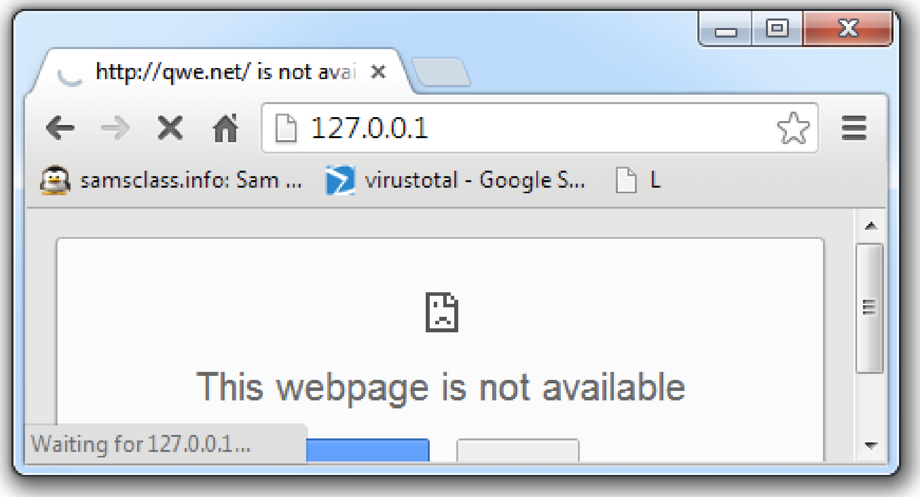
Problem with ApateDNS

- 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

Monitoring with Ncat (included with Nmap)



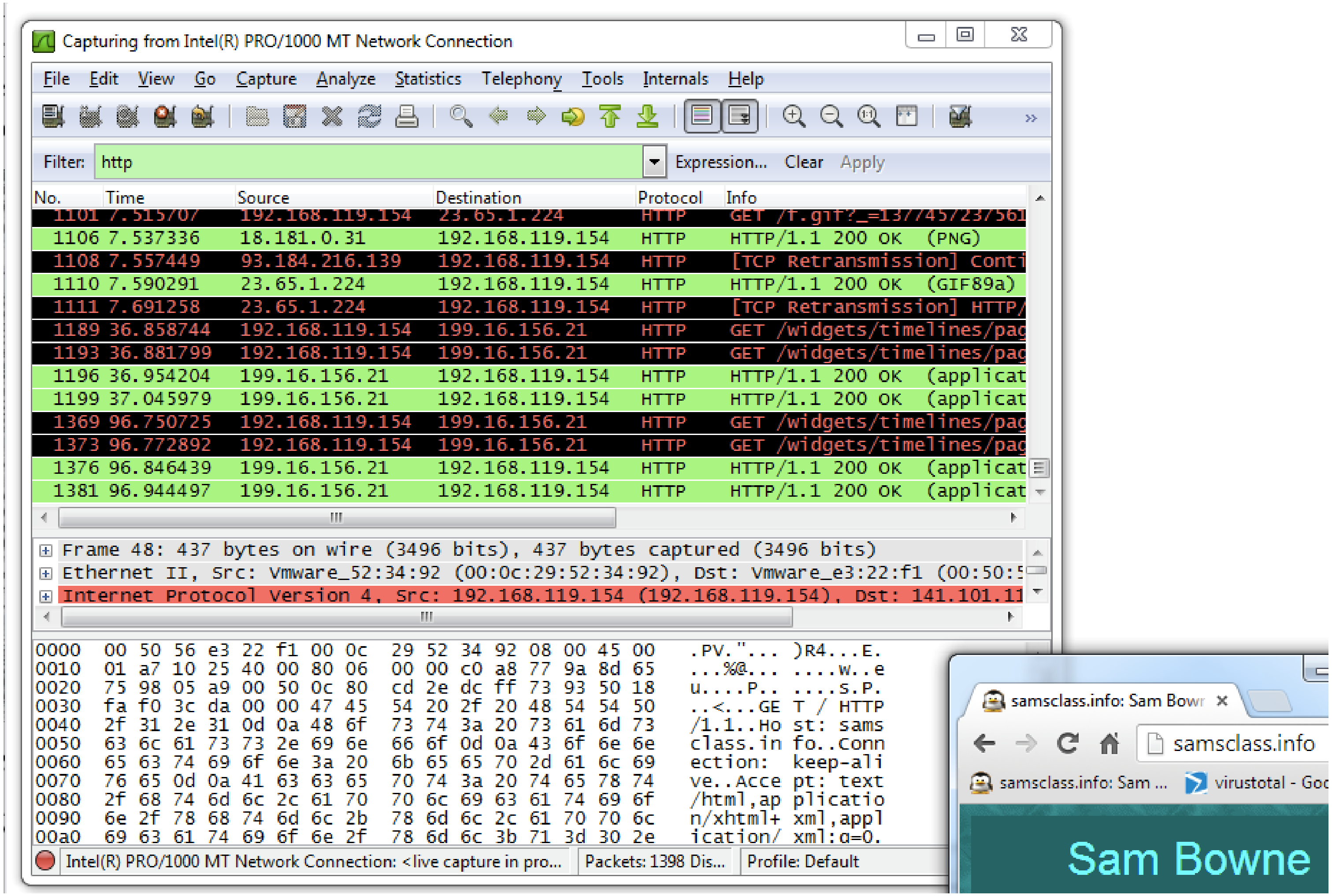
```
C:\Windows\System32>ncat -l 80
GET / HTTP/1.1
Host: 127.0.0.1
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/29.0.1547.57
Safari/537.36
Accept-Encoding: gzip,deflate,sdch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



This webpage is not available

Waiting for 127.0.0.1...

Packet Sniffing with Wireshark



Capturing from Intel(R) PRO/1000 MT Network Connection
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply
samsclass.info: Sam Bowr
samsclass.info
samsclass.info: Sam ...
virustotal - Goo
Sam Bowne

Filter: http

```
No.  Time       Source           Destination      Protocol  Info
1101 7.515707   192.168.119.154  23.65.1.224      HTTP      GET /f.gif?_=1377457237561
1106 7.537336   18.181.0.31      192.168.119.154  HTTP      HTTP/1.1 200 OK  (PNG)
1108 7.557449   93.184.216.139   192.168.119.154  HTTP      [TCP Retransmission] Conti
1110 7.590291   23.65.1.224      192.168.119.154  HTTP      HTTP/1.1 200 OK  (GIF89a)
1111 7.691258   23.65.1.224      192.168.119.154  HTTP      [TCP Retransmission] HTTP/
1189 36.858744  192.168.119.154  199.16.156.21    HTTP      GET /widgets/timelines/pag
1193 36.881799  192.168.119.154  199.16.156.21    HTTP      GET /widgets/timelines/pag
1196 36.954204  199.16.156.21    192.168.119.154  HTTP      HTTP/1.1 200 OK  (applicat
1199 37.045979  199.16.156.21    192.168.119.154  HTTP      HTTP/1.1 200 OK  (applicat
1369 96.750725  192.168.119.154  199.16.156.21    HTTP      GET /widgets/timelines/pag
1373 96.772892  192.168.119.154  199.16.156.21    HTTP      GET /widgets/timelines/pag
1376 96.846439  199.16.156.21    192.168.119.154  HTTP      HTTP/1.1 200 OK  (applicat
1381 96.944497  199.16.156.21    192.168.119.154  HTTP      HTTP/1.1 200 OK  (applicat
```

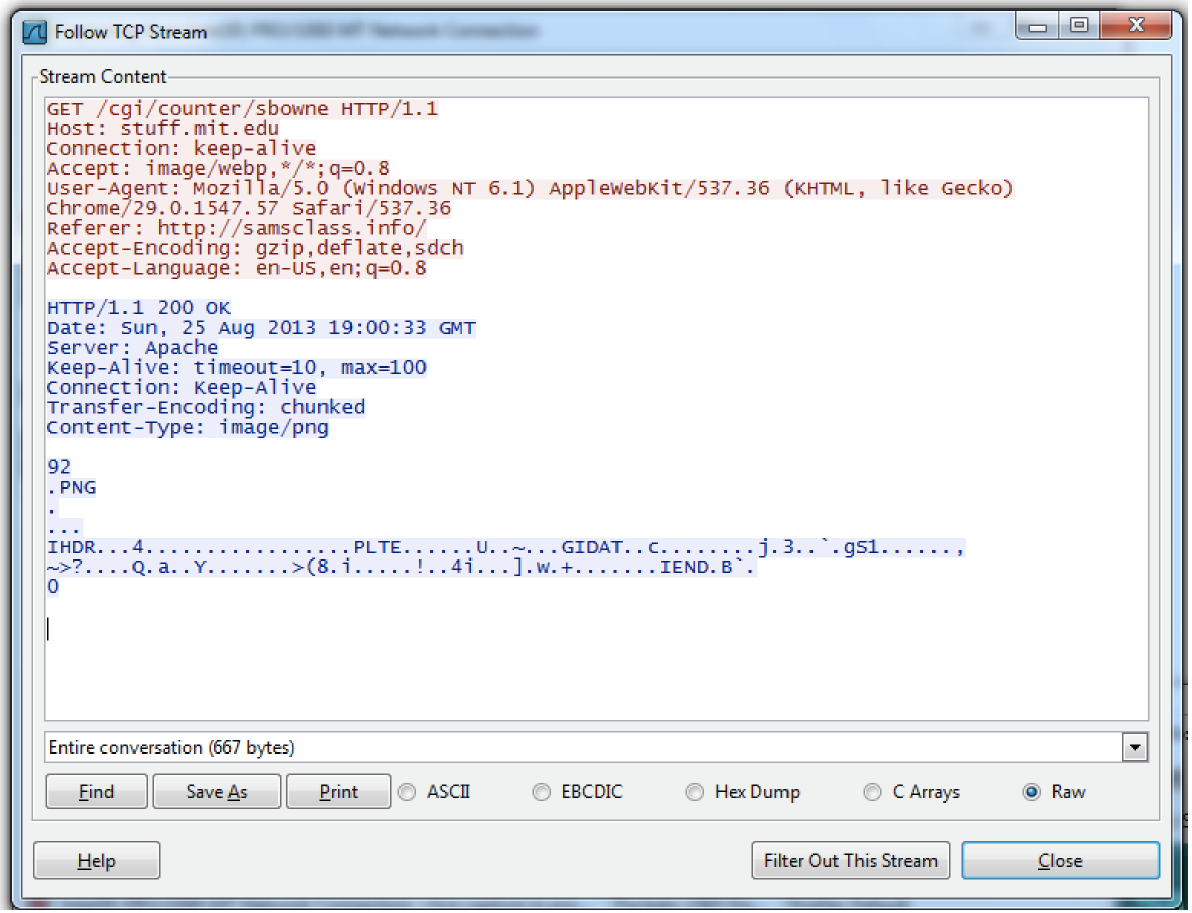
```
⊞ Frame 48: 437 bytes on wire (3496 bits), 437 bytes captured (3496 bits)
⊞ Ethernet II, Src: Vmware_52:34:92 (00:0c:29:52:34:92), Dst: Vmware_e3:22:f1 (00:50:5
⊞ Internet Protocol Version 4, Src: 192.168.119.154 (192.168.119.154), Dst: 141.101.11
```

```
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;q=0.
```

Intel(R) PRO/1000 MT Network Connection: <live capture in pro... Packets: 1398 Dis... Profile: Default

Follow TCP Stream

- Can safe files from streams here too

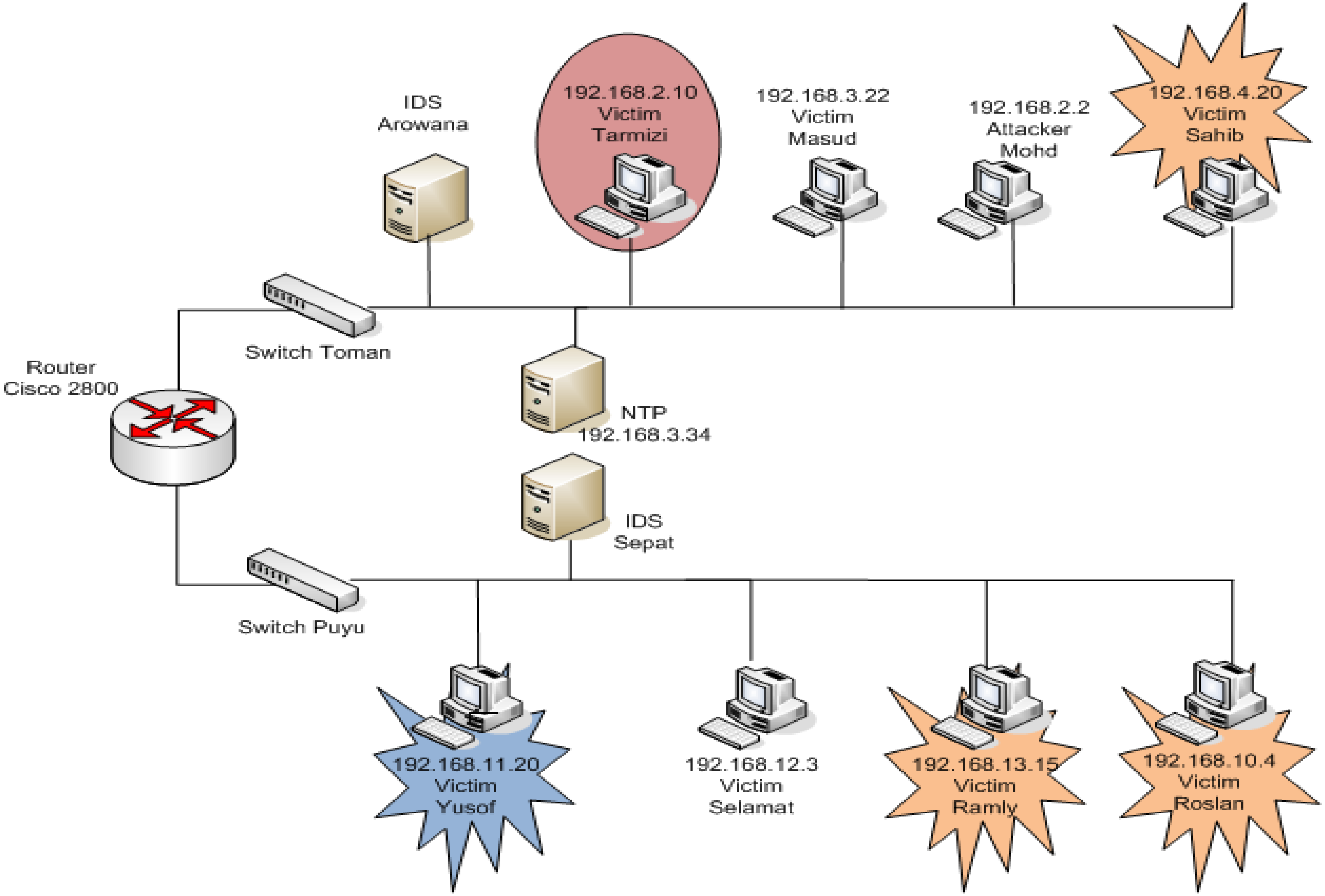


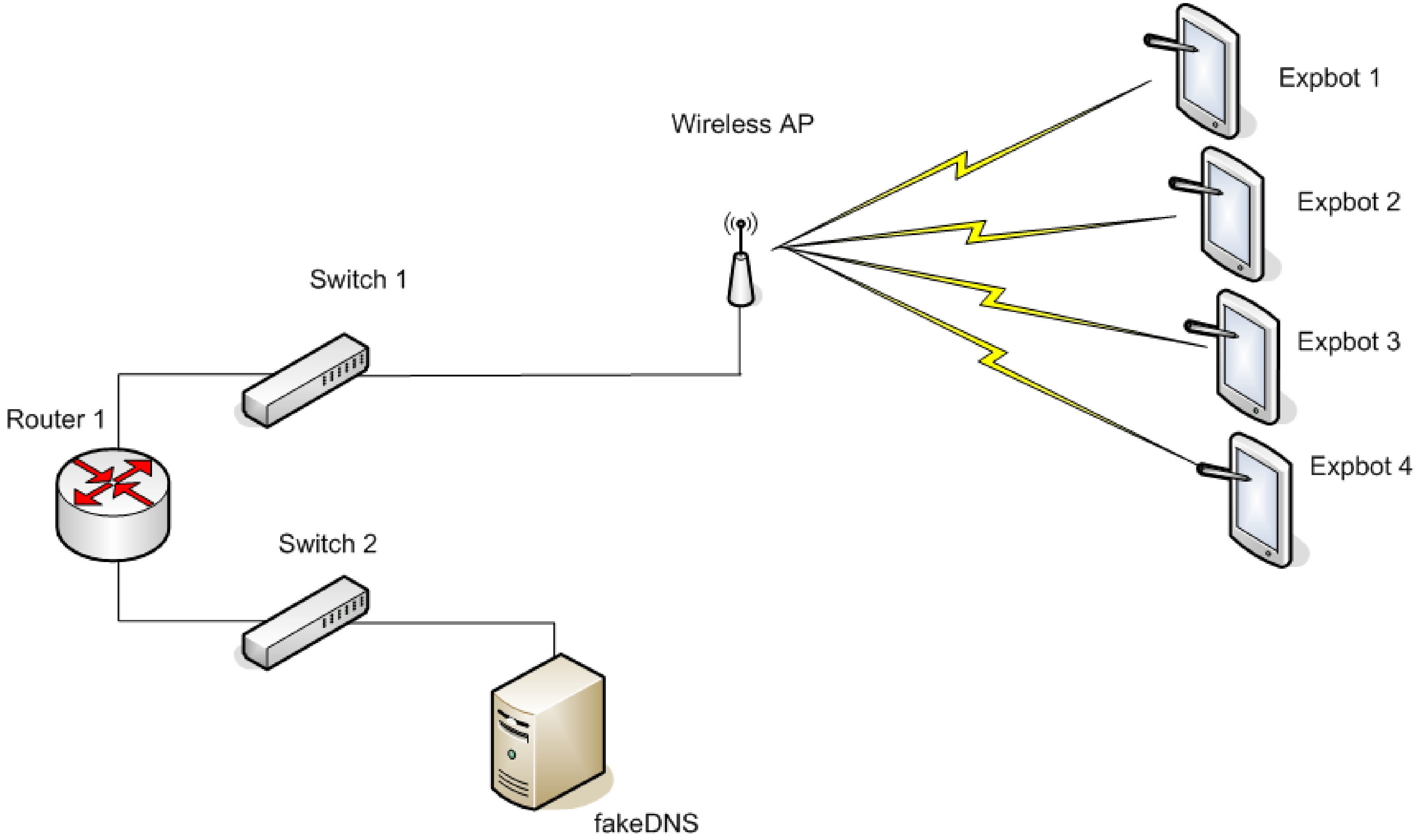
```
GET /cgi/counter/sbowne HTTP/1.1
Host: stuff.mit.edu
Connection: keep-alive
Accept: image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/29.0.1547.57 Safari/537.36
Referer: http://samsclass.info/
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8

HTTP/1.1 200 OK
Date: Sun, 25 Aug 2013 19:00:33 GMT
Server: Apache
Keep-Alive: timeout=10, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: image/png

92
.PNG
.
...
IHDR...4................PLTE......U..~...GIDAT..c........j.3..`.gS1......,
~>?....Q.a..Y........>(8.i.....!..4i...].w.+.......IEND.B`.
0
```

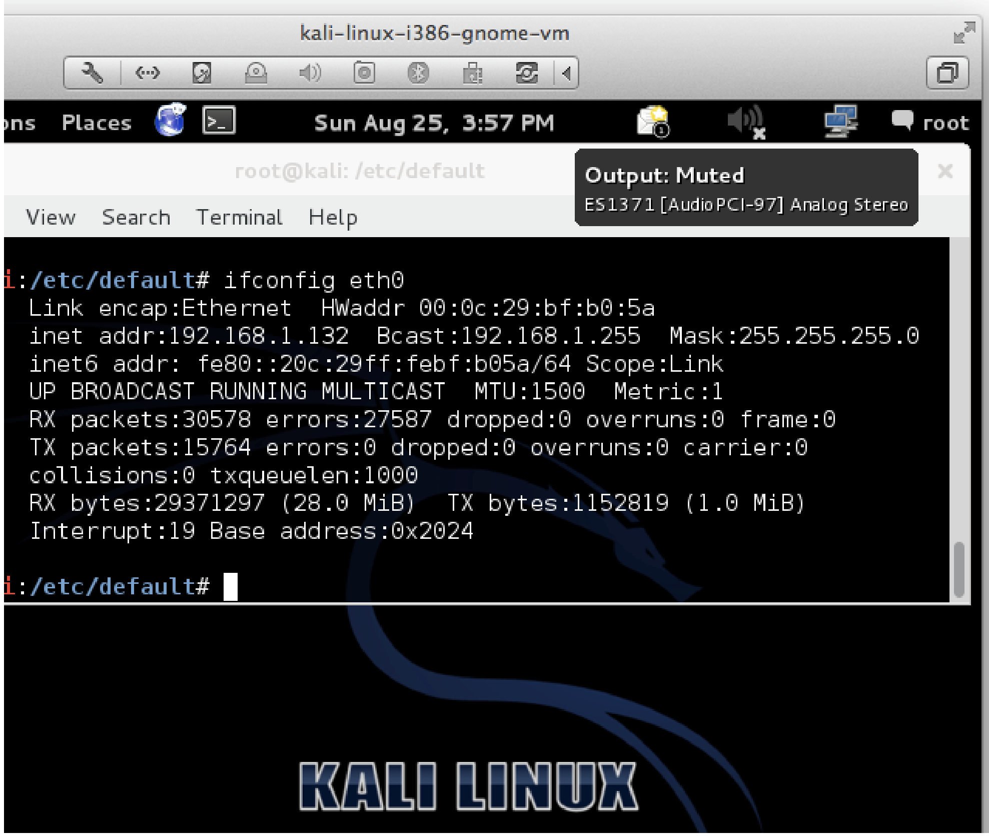
Entire conversation (667 bytes)


IDS
Arowana
192.168.2.10
Victim
Tarmizi
192.168.3.22
Victim
Masud
192.168.2.2
Attacker
Mohd
192.168.4.20
Victim
Sahib
Router
Cisco 2800
Switch Toman
NTP
192.168.3.34
IDS
Sepat
Switch Puyu
192.168.11.20
Victim
Yusof
192.168.12.3
Victim
Selamat
192.168.13.15
Victim
Ramly
192.168.10.4
Victim
Roslan


Expbot 1
Wireless AP
Expbot 2
Switch 1
Expbot 3
Router 1
Expbot 4
Switch 2
fakeDNS

USING INETSIM

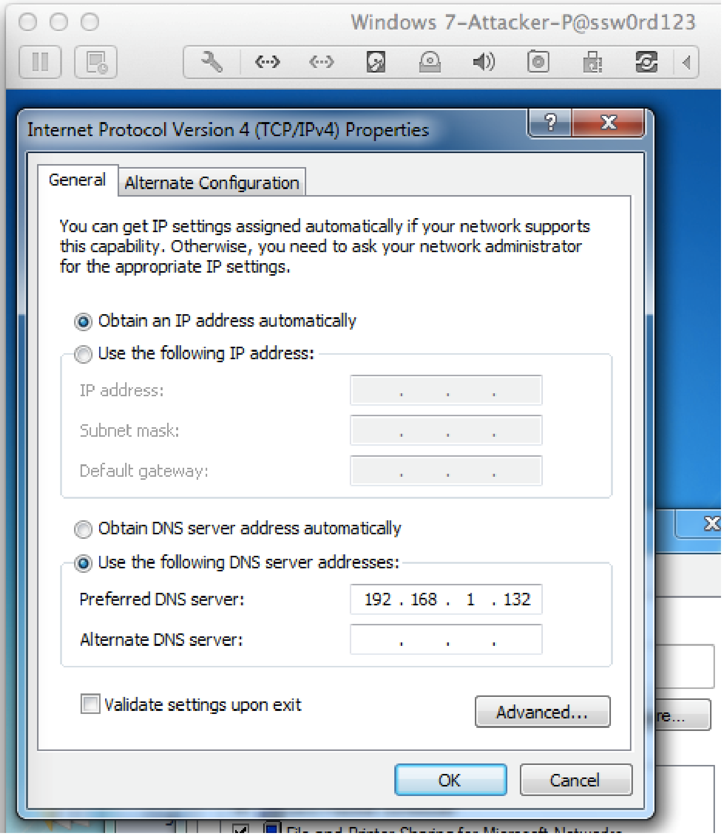
inetsim



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# 
```


Windows 7-Attacker-P@ssw0rd123
Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
Advanced...
OK
Cancel

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

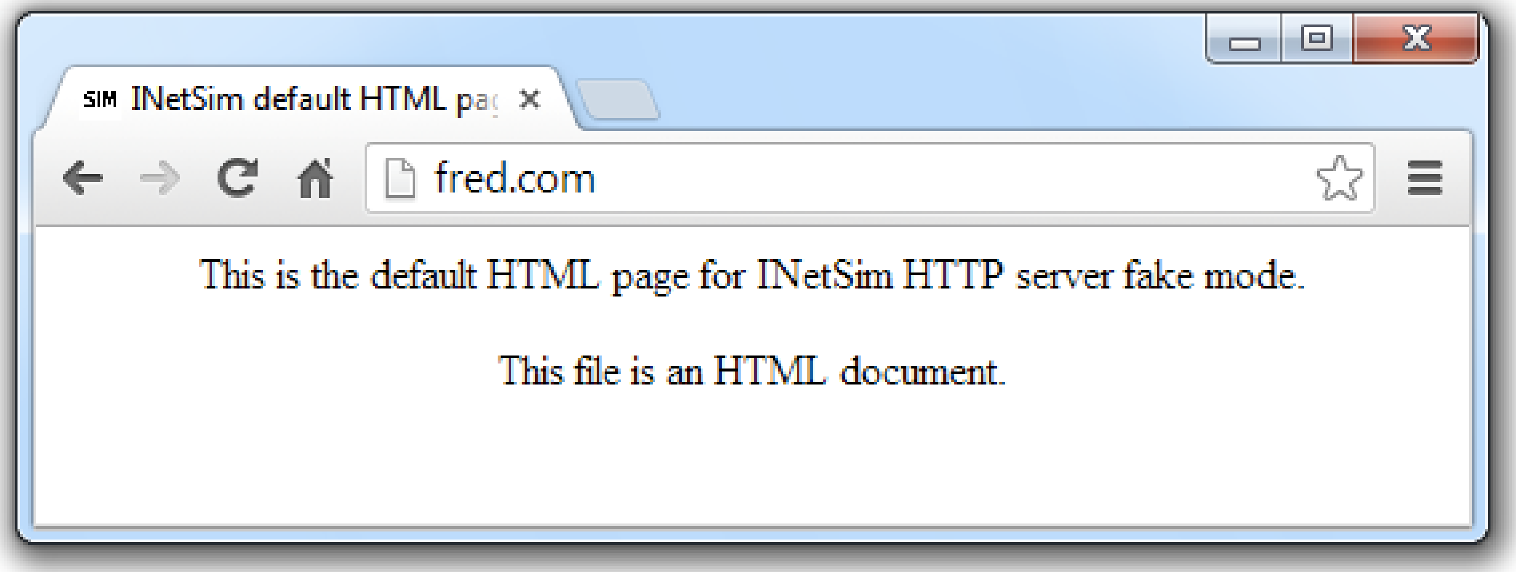
● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 1 . 132

Alternate DNS server: . . .

□ Validate settings upon exit

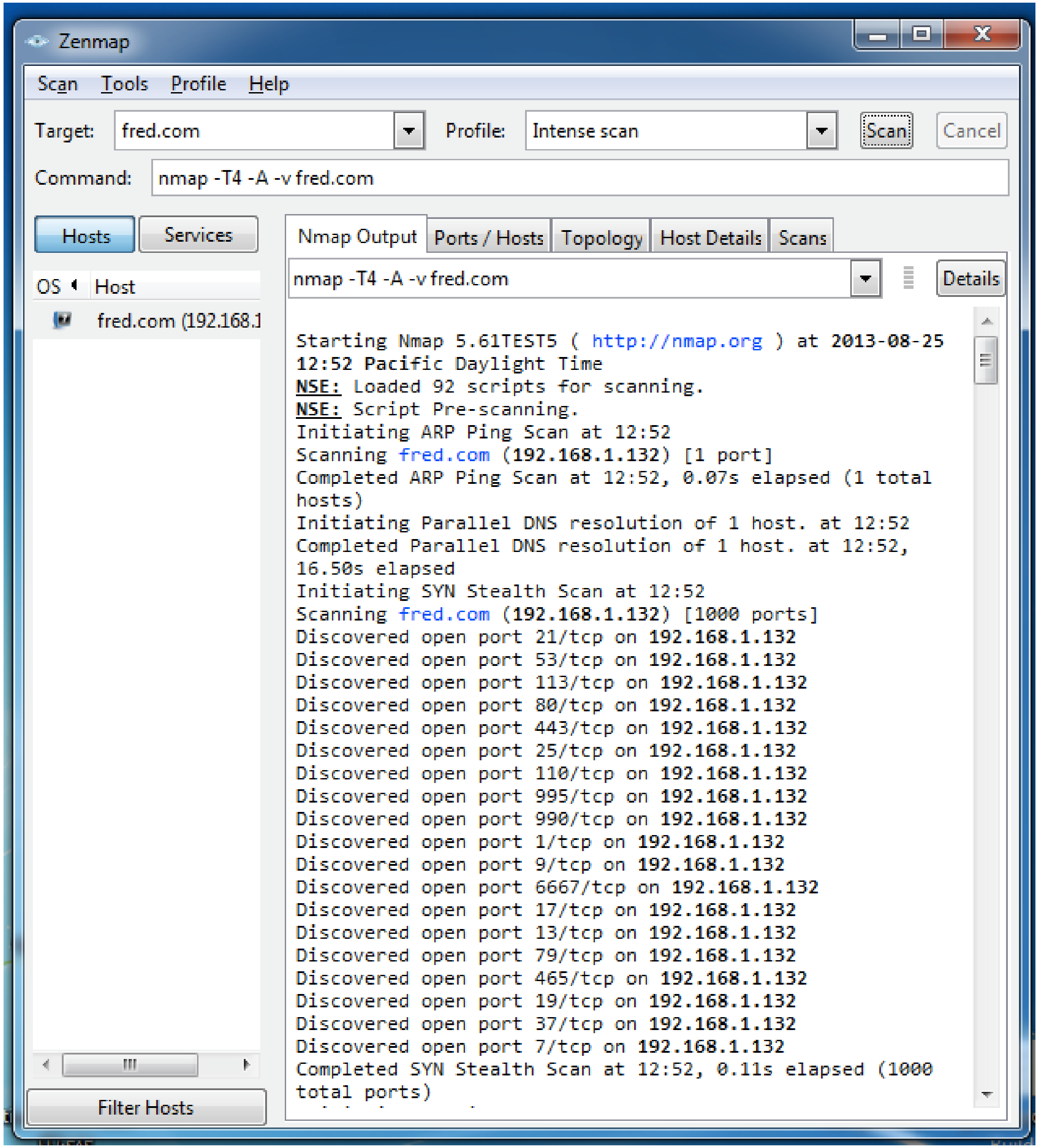
INetSim Fools a Browser



This is the default HTML page for INetSim HTTP server fake mode.

This file is an HTML document.

INetSim Fools Nmap



Target: fred.com

Profile: Intense scan

Command: nmap -T4 -A -v fred.com

```
nmap -T4 -A -v fred.com

Starting Nmap 5.61TEST5 ( http://nmap.org ) at 2013-08-25
12:52 Pacific Daylight Time
NSE: Loaded 92 scripts for scanning.
NSE: Script Pre-scanning.
Initiating ARP Ping Scan at 12:52
Scanning fred.com (192.168.1.132) [1 port]
Completed ARP Ping Scan at 12:52, 0.07s elapsed (1 total
hosts)
Initiating Parallel DNS resolution of 1 host. at 12:52
Completed Parallel DNS resolution of 1 host. at 12:52,
16.50s elapsed
Initiating SYN Stealth Scan at 12:52
Scanning fred.com (192.168.1.132) [1000 ports]
Discovered open port 21/tcp on 192.168.1.132
Discovered open port 53/tcp on 192.168.1.132
Discovered open port 113/tcp on 192.168.1.132
Discovered open port 80/tcp on 192.168.1.132
Discovered open port 443/tcp on 192.168.1.132
Discovered open port 25/tcp on 192.168.1.132
Discovered open port 110/tcp on 192.168.1.132
Discovered open port 995/tcp on 192.168.1.132
Discovered open port 990/tcp on 192.168.1.132
Discovered open port 1/tcp on 192.168.1.132
Discovered open port 9/tcp on 192.168.1.132
Discovered open port 6667/tcp on 192.168.1.132
Discovered open port 17/tcp on 192.168.1.132
Discovered open port 13/tcp on 192.168.1.132
Discovered open port 79/tcp on 192.168.1.132
Discovered open port 465/tcp on 192.168.1.132
Discovered open port 19/tcp on 192.168.1.132
Discovered open port 37/tcp on 192.168.1.132
Discovered open port 7/tcp on 192.168.1.132
Completed SYN Stealth Scan at 12:52, 0.11s elapsed (1000
total ports)
```

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
- Remnux (Distro for all Reverse Engineering Tool)

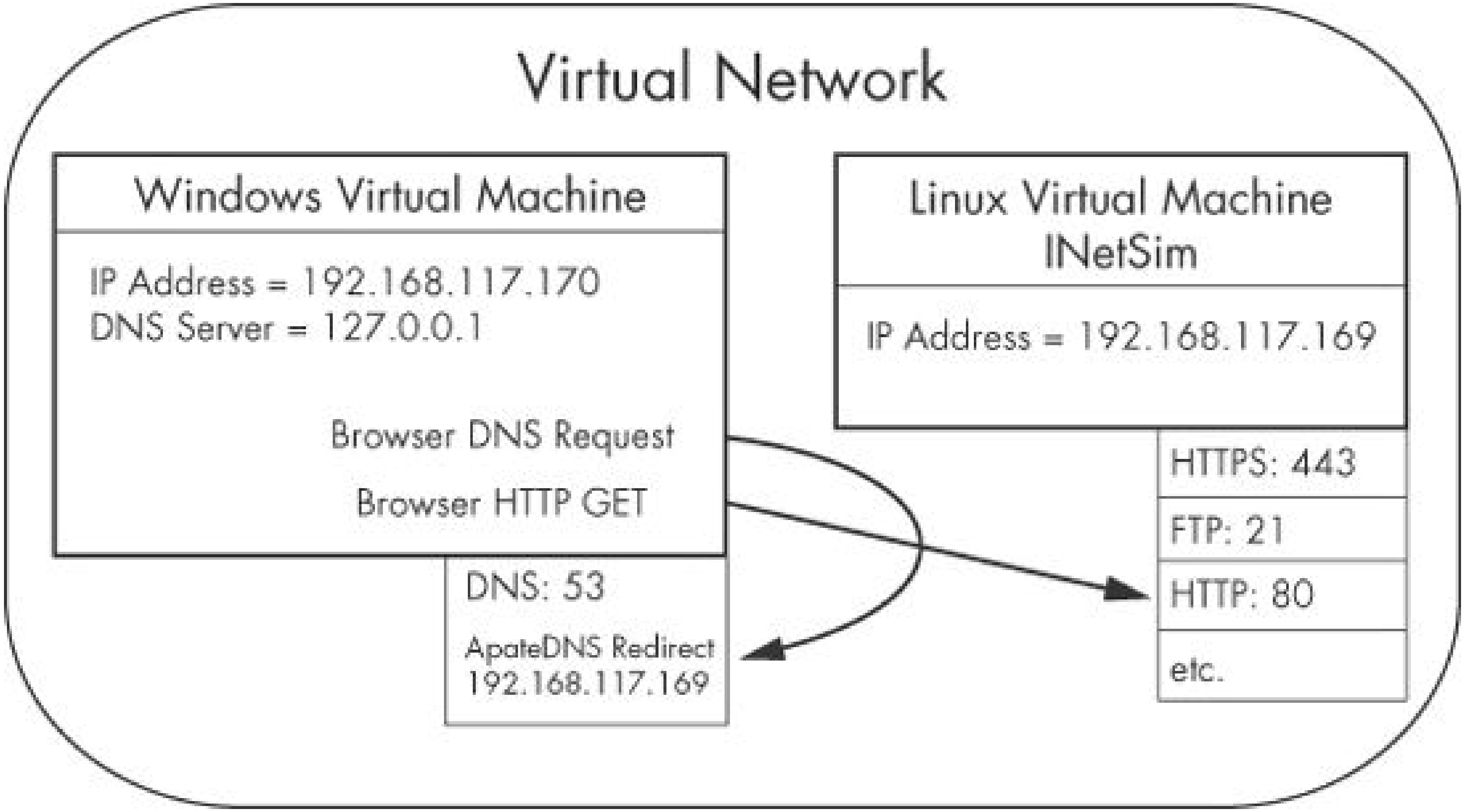


Figure 4-12. Example of a virtual network

SUMMARY

In Conclusion

- Setting up the isolated environment using VM is important in analysing malware sample
- In dynamic analysis we can observed the behaviour of malware during the execution, thus showing the real behaviour and traces.
- Sandbox is an automated tool for dynamic analysis, but the output report of the analysis might be to general
- There are several tool that a malware analyst can use to monitor the processes and activity of malware during execution.
- Linux distro like Kali and Remnux might help malware analyst in creating a simulated network complete with DNS, web server, ftp or other internet services.