BASIC DYNAMIC ANALYSIS

MALWARE ANALYSIS AND INCIDENT FORENSICS
M.Sc. in Cyber Security

MALWARE ANALYSIS
M.Sc. in Engineering in Computer Science

A.Y. 2025/2026

SAPIENZA
UNIVERSITÀ DI ROMA

CIS SAPIENZA
CYBER INTELLIGENCE AND INFORMATION SECURITY

DYNAMIC ANALYSIS

- Running malware deliberately, while monitoring the results
- Requires a **controlled, safe environment**
- Must prevent malware from spreading to production machines
- Real machines can be **air-gapped** (i.e., no network connection to the Internet or to other machines)

DYNAMIC ANALYSIS

Static analysis can reach a dead-end, due to

- Obfuscation
- Packing
- Examiner has exhausted the available static analysis techniques

Dynamic analysis will show you exactly what the malware does

- Not really…

Main goal: understand the malware behavior

Approaches: diffing, monitoring, tracing, debugging

DIFFING

- Take a snapshot of a clean system state and a snapshot of a compromised system state
- Compare before and after
- Pros:
  - Artifacts can be observed easily
- Cons:
  - Can miss evidence that is created during malware activities and erased purposely by malware
- Tools: regshot, autoruns

SYSTEM MONITORING

From a clean system state, record every individual change in system and network traffic that appears after executing the suspicious file

Pros:

- Can collect all manifested changes

Cons:

- Often too much information and need to weed out irrelevant data

Tools: procmon, Wireshark

API TRACING

Hook and record important API calls made by the suspicious process

Pro:

- Provides visibility into activity beyond the typical file/process/registry/network shown by other tools. Gets you a little closer to the type of interpretation that is required when doing static analysis.

Cons:

- Often too much of information and need to weed out irrelevant data. API-specific interpretation can take a lot of time (but still less than static analysis ;))

Tools: Rohitab API Monitor, WinApiOverride

DEBUGGING

Set breakpoints inside the suspicious file to stop its execution at a given location and inspect its state.

Pro:

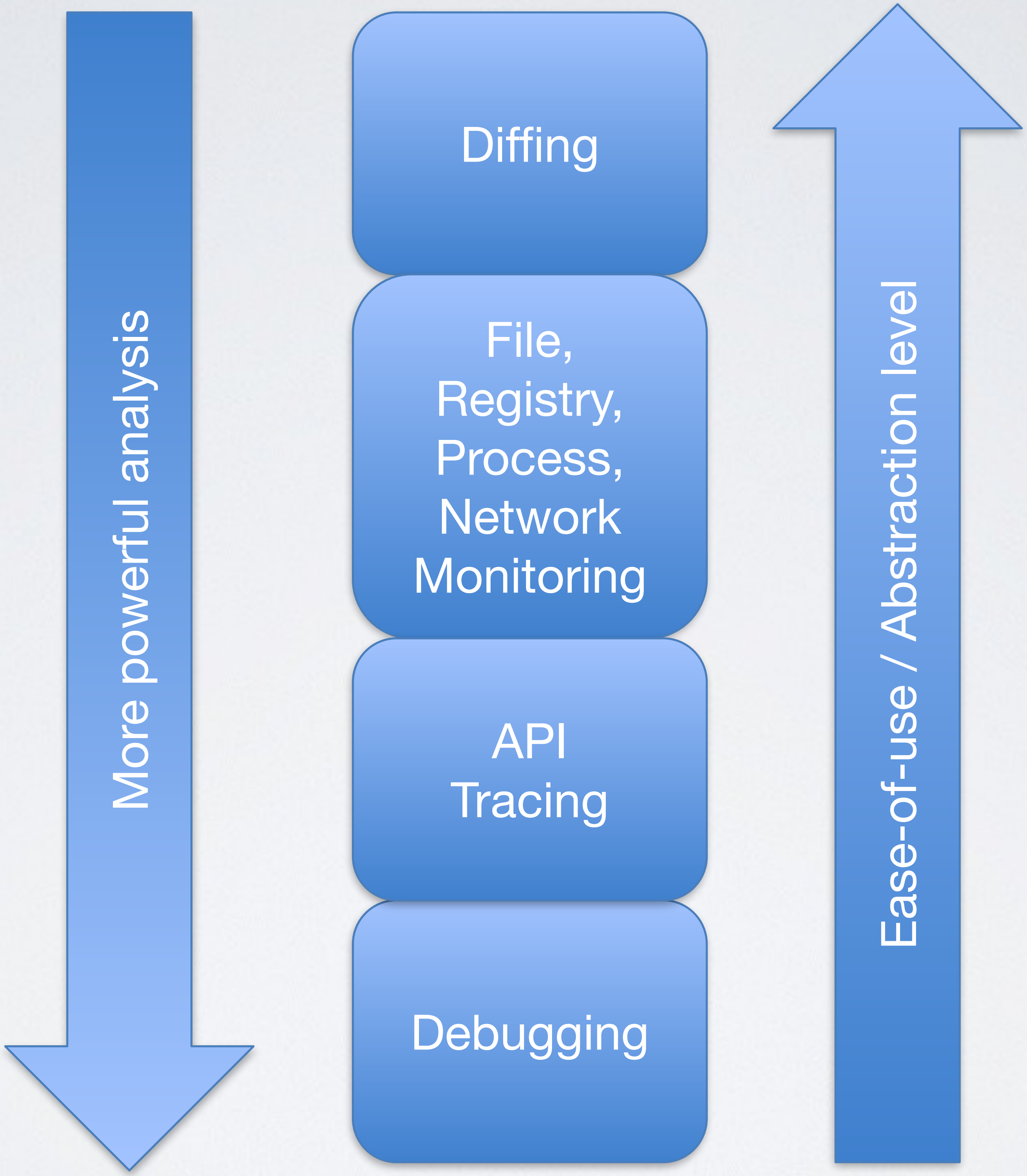
- Provides a superset of the functionality of an API monitor

Cons:

- Typically must be be done in conjunction with some basic static analysis and assembly reading. Malware will often change its behavior or refuse to run when being debugged, which may require workarounds

Tools: IDA, OllyDbg, Immunity Debugger, WinDbg

BEHAVIORAL ANALYSIS TECHNIQUES



More powerful analysis

Diffing

File, Registry, Process, Network Monitoring

API Tracing

Debugging

Ease-of-use / Abstraction level

DYNAMIC ANALYSIS

Limits you need to be aware of:

- in general, single path (execution trace) is examined
- analysis environment possibly not invisible
- analysis environment possibly not comprehensive
- scalability issues

How do you technically perform it?

- **instrument** the program, operating system or hardware

DYNAMIC ANALYSIS

PROGRAM INSTRUMENTATION

- analysis operates in same address space as sample
- manual analysis with debugger
- Detours (Windows API hooking mechanism)
- Binary under analysis is modified
  - breakpoints are inserted
  - functions are rewritten
  - debug registers are used
- Not invisible, malware can detect analysis artifacts
- May require significant manual effort

DYNAMIC ANALYSIS

OS INSTRUMENTATION

- analysis operates in OS where sample is run
- Windows system call hooks
- somewhat invisible to (user-mode) malware
- can cause problems when malware runs in OS kernel
- limited visibility of activity inside program
  - for example, cannot set function breakpoints

DYNAMIC ANALYSIS

HW INSTRUMENTATION

- provide virtual hardware (processor) where sample can execute (sometimes including OS)
- for example: software emulation of executed instructions
- analysis observes activity “from the outside”
- transparent to sample (and guest OS)
- OS environment needs to be provided
- limited environment could be detected, but faster
- complete environment is more comprehensive, but slower
- >>> Sandboxes

DYNAMIC ANALYSIS

What do we want to observe?

Process interacts with operating system via system calls

- needs OS for every interaction with environment
  - file system, network, registry, ...
- monitor system calls
  - many Windows system calls (“Native APIs”) are undocumented and can change without notice
  - developers are expected to use **Windows APIs**, a collection of stable user-mode shared libraries
  - of course, Windows APIs can be bypassed

DYNAMIC ANALYSIS

Report from the analysis:

- File activity
  - read, write, create, open, ...
- Registry activity
- Service activity
  - Start/Stop of Windows services (via Service Manager)
- Process activity
  - start, terminate process, inter-process communication
- Network activity
  - API calls and packet logs

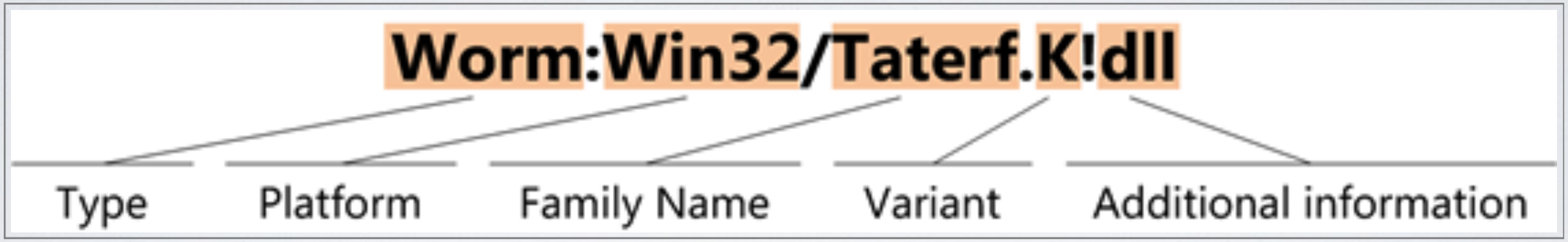
SANDBOX

- 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
  - Some of them offer a free tier
- They can automate dynamic analysis
- They produce a nice PDF report of results
  - Example from Joe Sandbox Cloud: https://www.joesecurity.org/joe-sandbox-reports

MALWARE CLASSIFICATION

A nice byproduct of sandboxes is (tentative) family classification

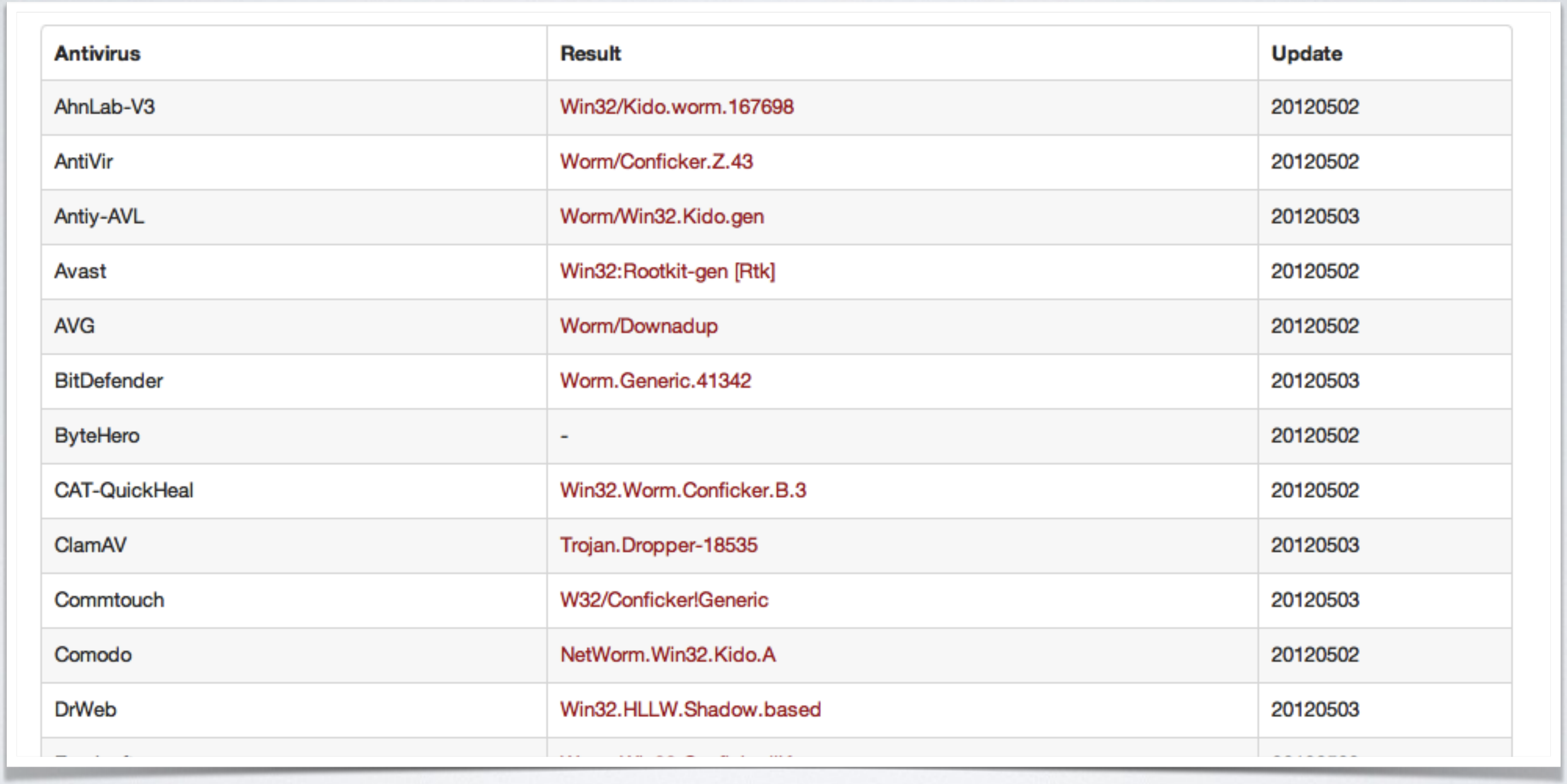
- Naming conventions derived from *Computer Antivirus Research Organization* (CARO) Malware Naming Scheme



Vendor	Name Convention	Example
Symantec	Prefix.Name.Suffix	Infostealer.Banker.C
Avira	Prefix:Name [Type]	Win32:Zbot-BS [Trj]
Kaspersky	[Prefix:]Behaviour.Platform.Name[.Variant]	Trojan.Win32.Genome.taql

MALWARE CLASSIFICATION

Classification schemes are hardly coherent



Antivirus	Result	Update
AhnLab-V3	Win32/Kido.worm.167698	20120502
AntiVir	Worm/Conficker.Z.43	20120502
Antiy-AVL	Worm/Win32.Kido.gen	20120503
Avast	Win32:Rootkit-gen [Rtk]	20120502
AVG	Worm/Downadup	20120502
BitDefender	Worm.Generic.41342	20120503
ByteHero	-	20120502
CAT-QuickHeal	Win32.Worm.Conficker.B.3	20120502
ClamAV	Trojan.Dropper-18535	20120503
Commtouch	W32/Conficker!Generic	20120503
Comodo	NetWorm.Win32.Kido.A	20120502
DrWeb	Win32.HLLW.Shadow.based	20120503

REAL MACHINES

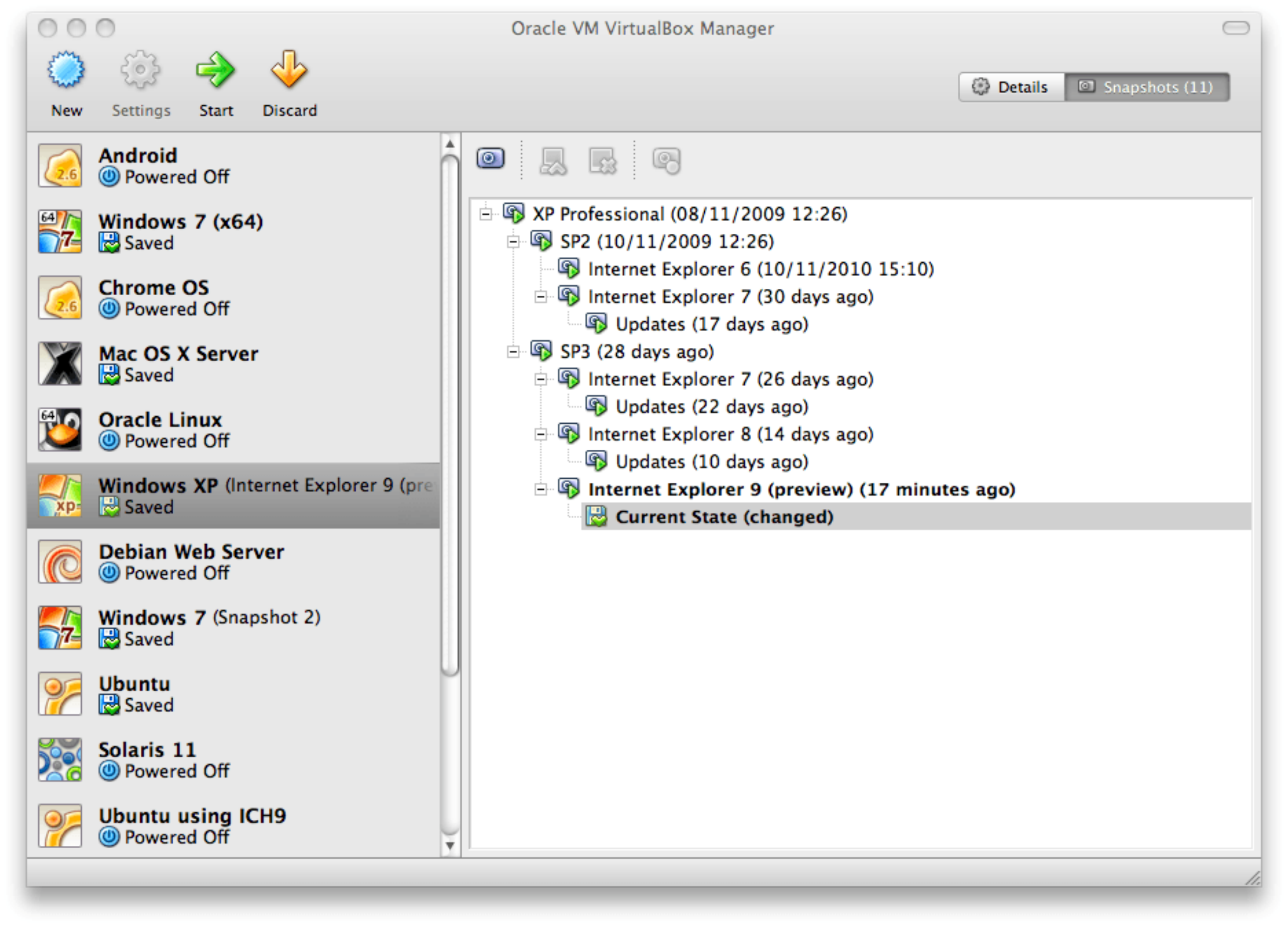
- Disadvantages
  - No Internet connection, so parts of the malware may not work
  - Can be difficult to remove malware: re-imaging the machine will be necessary
- Advantage
  - Some malware detects virtual machines and will not run properly in one

VIRTUAL MACHINES

- The most common method
- This protects the host machine from the malware
  - VM-escape attacks remain possible (but currently unlikely)
  - naive VM usage is way more dangerous
- You can easily “snapshot” the VM and revert it to a clean state at the end of each analysis job

ORACLE VIRTUAL BOX

- Free!
- Can read/write VMware disks
- Reasonable performance for the goals of this course
- You can take several snapshots and revert back to them if needed



Oracle VM VirtualBox Manager

Android
Powered Off

Windows 7 (x64)
Saved

Chrome OS
Powered Off

Mac OS X Server
Saved

Oracle Linux
Powered Off

Windows XP (Internet Explorer 9 (pre
Saved

Debian Web Server
Powered Off

Windows 7 (Snapshot 2)
Saved

Ubuntu
Saved

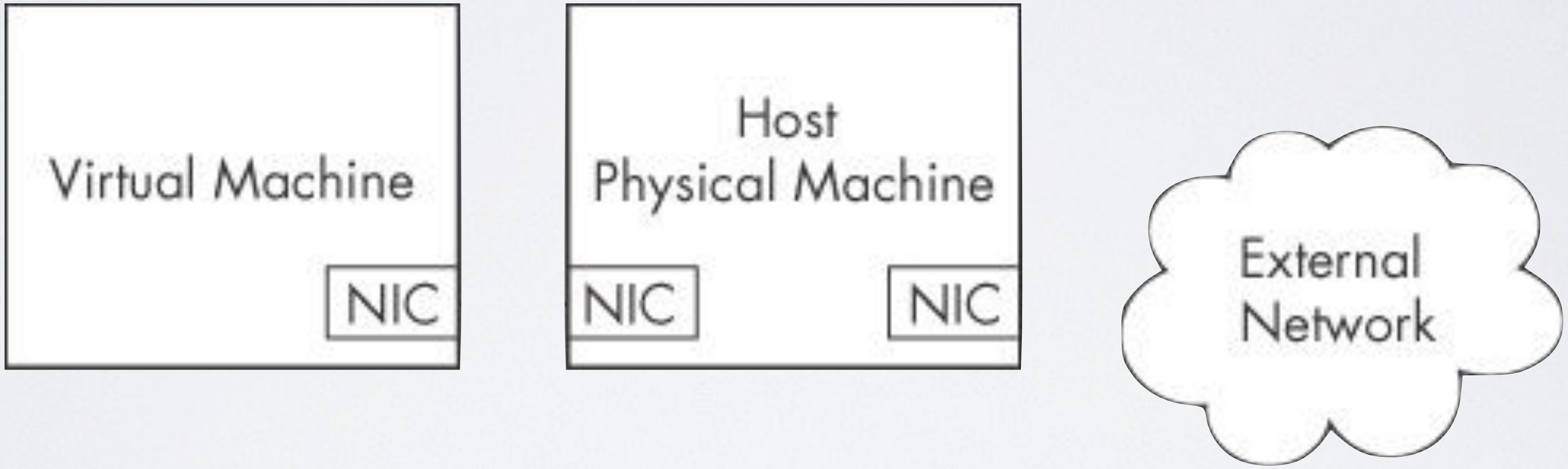
Solaris 11
Powered Off

Ubuntu using ICH9
Powered Off

```
XP Professional (08/11/2009 12:26)
  SP2 (10/11/2009 12:26)
    Internet Explorer 6 (10/11/2010 15:10)
    Internet Explorer 7 (30 days ago)
      Updates (17 days ago)
  SP3 (28 days ago)
    Internet Explorer 7 (26 days ago)
      Updates (22 days ago)
    Internet Explorer 8 (14 days ago)
      Updates (10 days ago)
    Internet Explorer 9 (preview) (17 minutes ago)
      Current State (changed)
```

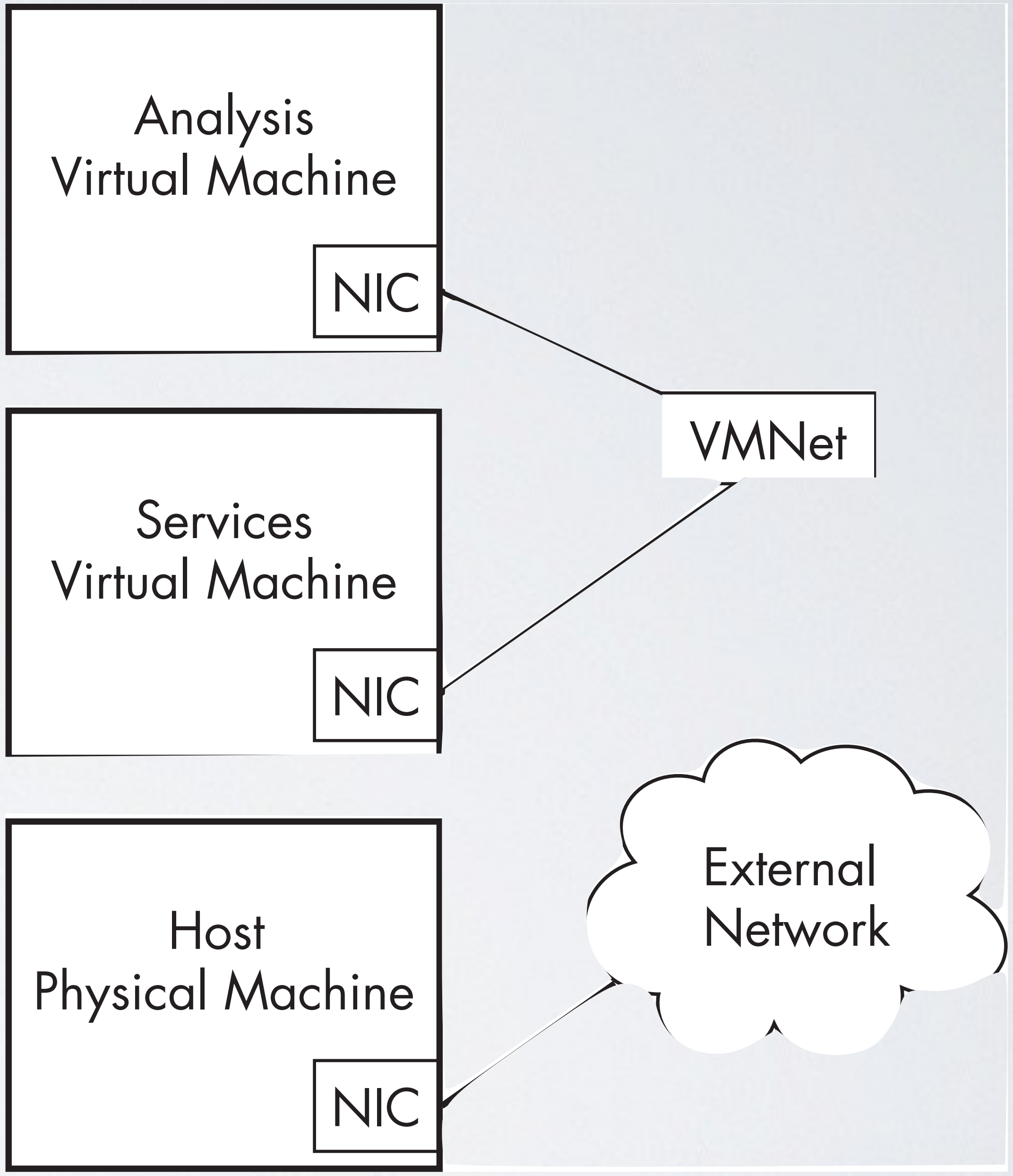
CONFIGURING VIRTUAL BOX

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



CONFIGURING VIRTUAL BOX

- More complex setups are possible
- Use ad-hoc networking to fake external services
  - host-only networking



SNAPSHOTS

- Use snapshots to:
  - Protect a clean installation of the analysis environment
  - Keep track of ongoing progress during analysis
  - Hop instantly from job to job if you need to analyze several samples at the same time

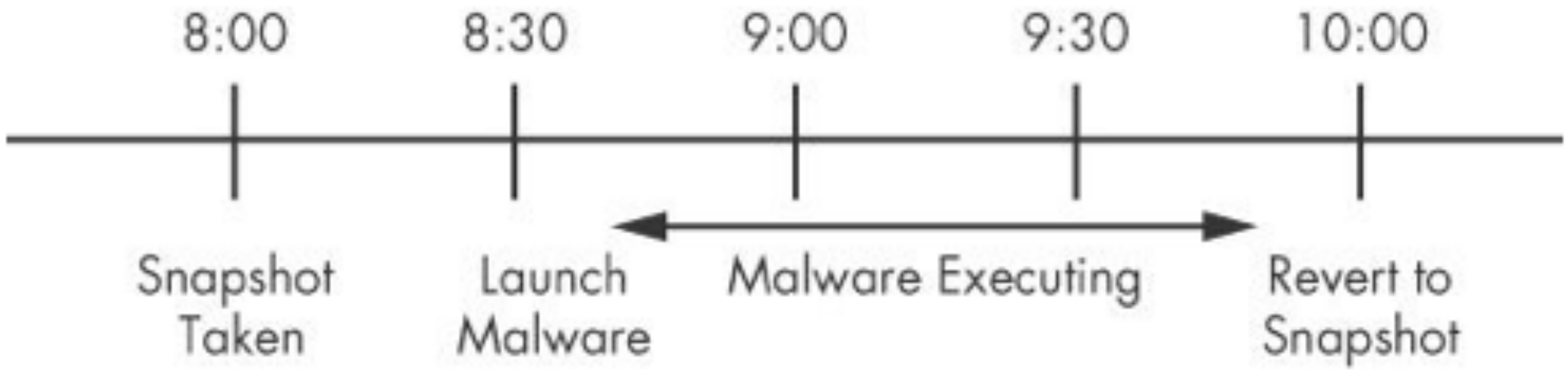


Figure 3-5. Snapshot timeline

RISKS OF USING A VM FOR MALWARE ANALYSIS

- Malware may detect that it is in a VM and run differently
- Virtualization environments may have bugs: in some cases, malware may exploit it to spread and/or affect the host
- All the samples we analyze in this course are harmless

WINDOWS

- Most malware you will typically encounter is Windows based
- We will use a Windows 10 VM for analysis
  - Some old malware may not run without admin privileges
  - Internal safety protections (e.g., Windows Defender) need to be disabled to avoid malware samples to be automatically quarantined/deleted
    - gpedit.msc

LAUNCHING DLLS

- EXE files can be run directly, but DLLs can't
- Use the Windows tool *Rundll32.exe* as follows:

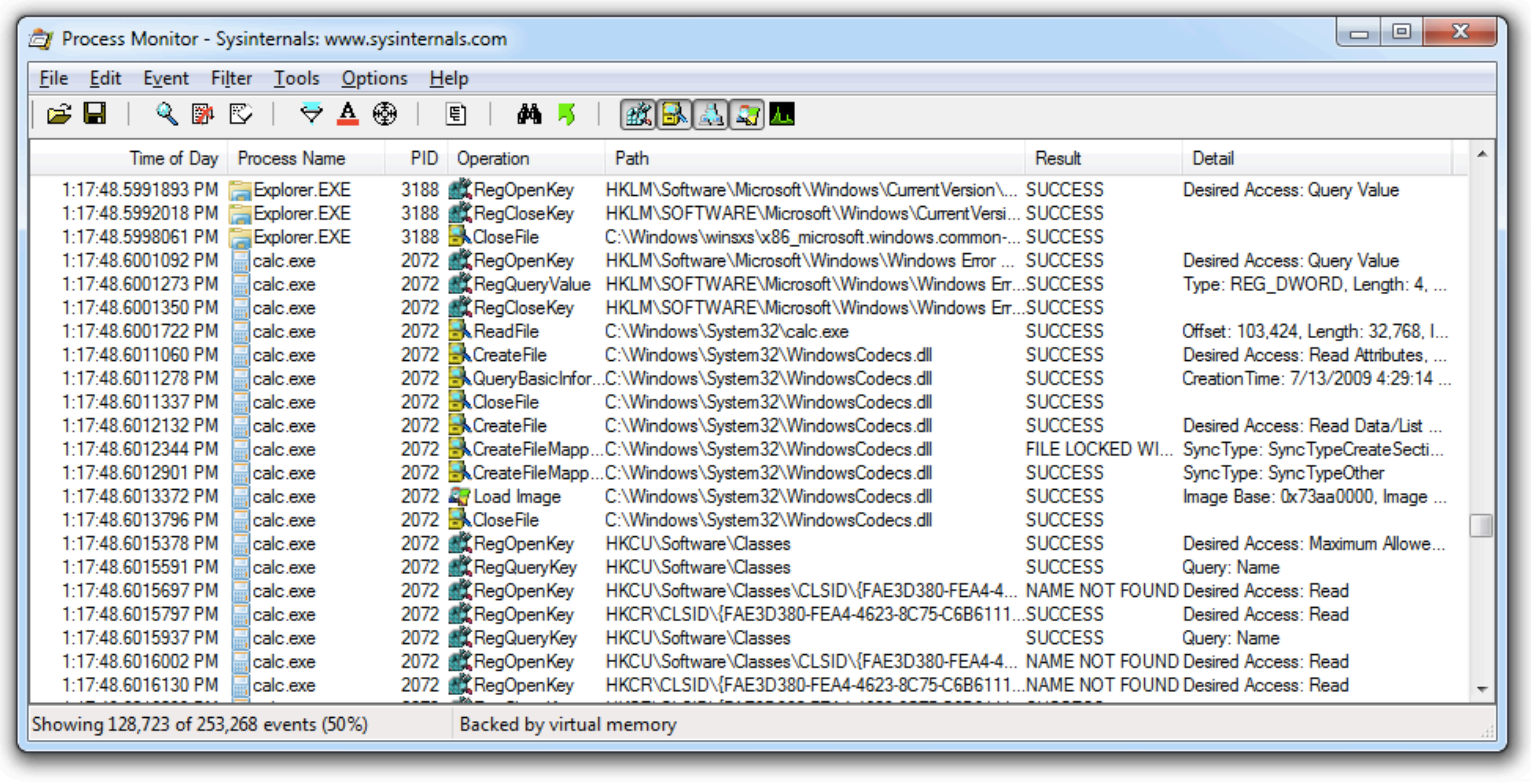
  rundll32.exe DLLname, Export arguments

- The Export value is one of the exported functions you found in Dependency Walker, PEview, or PE Explorer
- But many malicious DLLs do not have an export. We will cover DLL launching in a hands-on session later in the course

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
- Do not 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

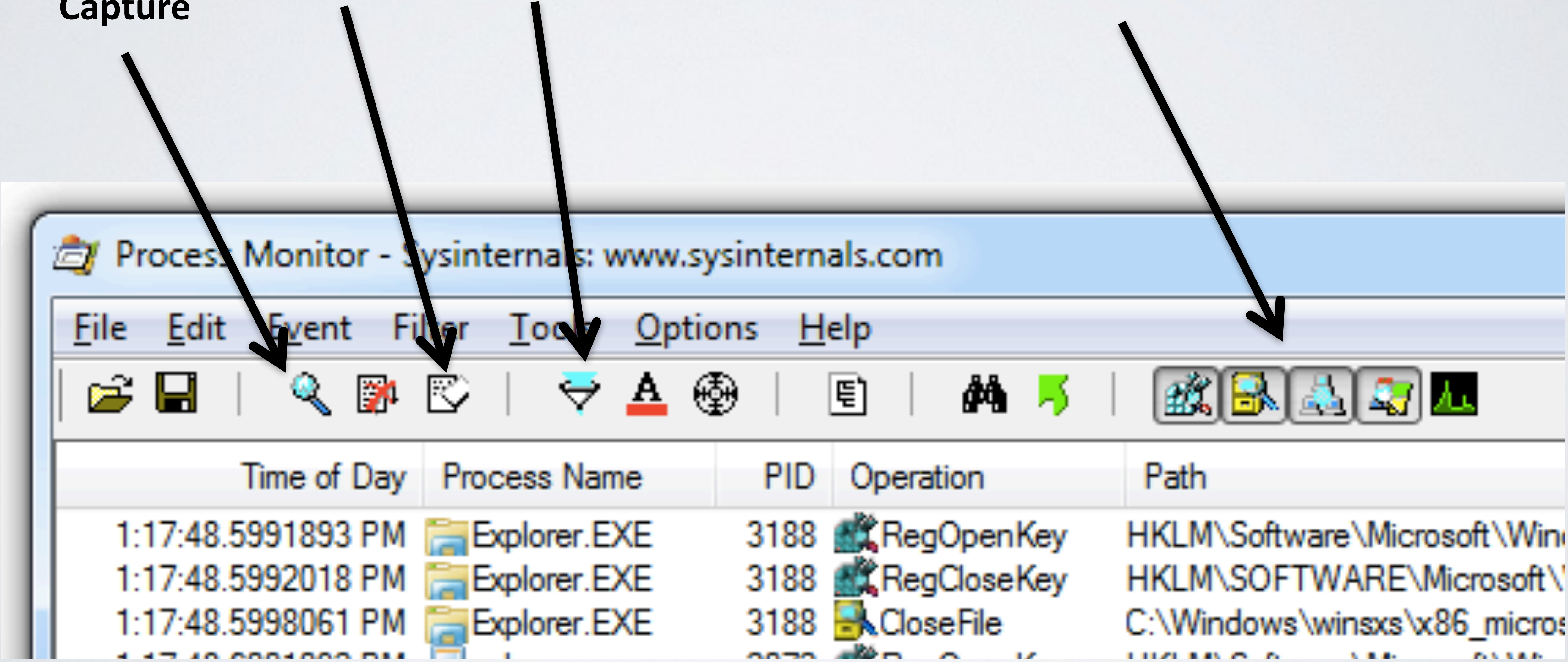
PROCESS MONITOR TOOLBAR

Start/Stop Capture

Erase

Filter

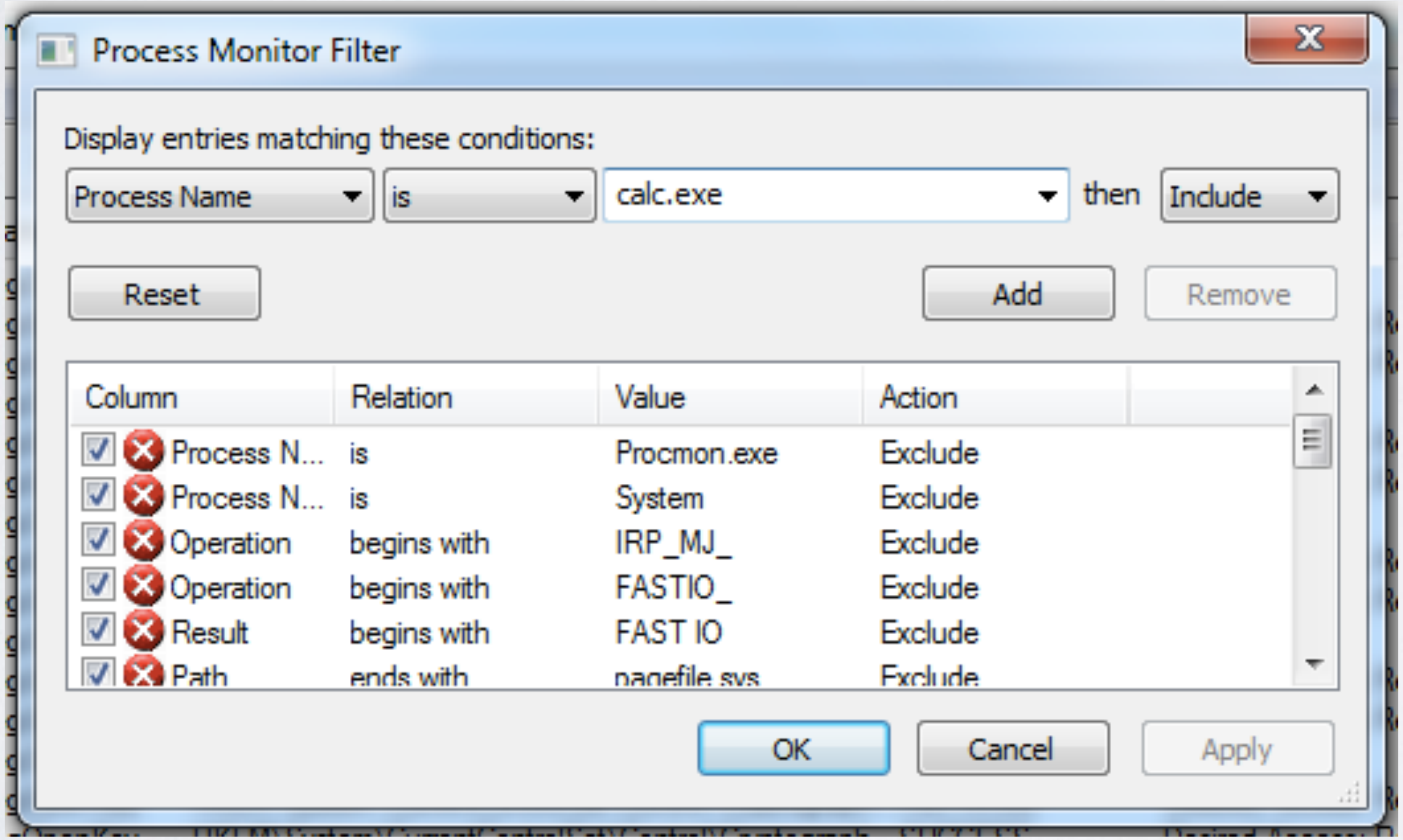
Default Filters
Registry, File system, Network, Processes



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_micros

FILTERING WITH EXCLUDE

- One technique: hide normal activity before launching malware
- Right-click each Process Name and click **Exclude**
- Most useful filters: Process Name, Operation, and Detail

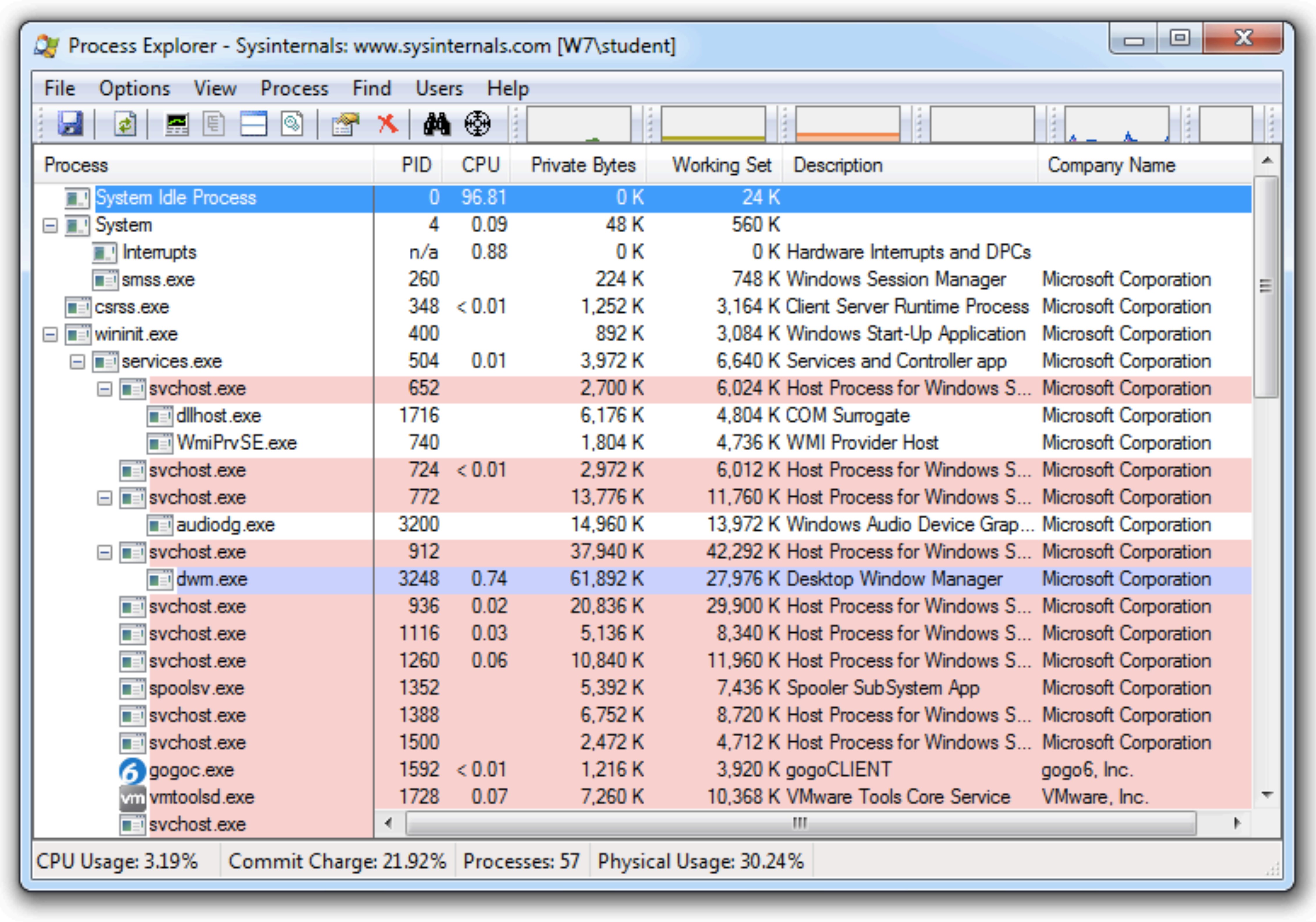


Display entries matching these conditions:

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

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						

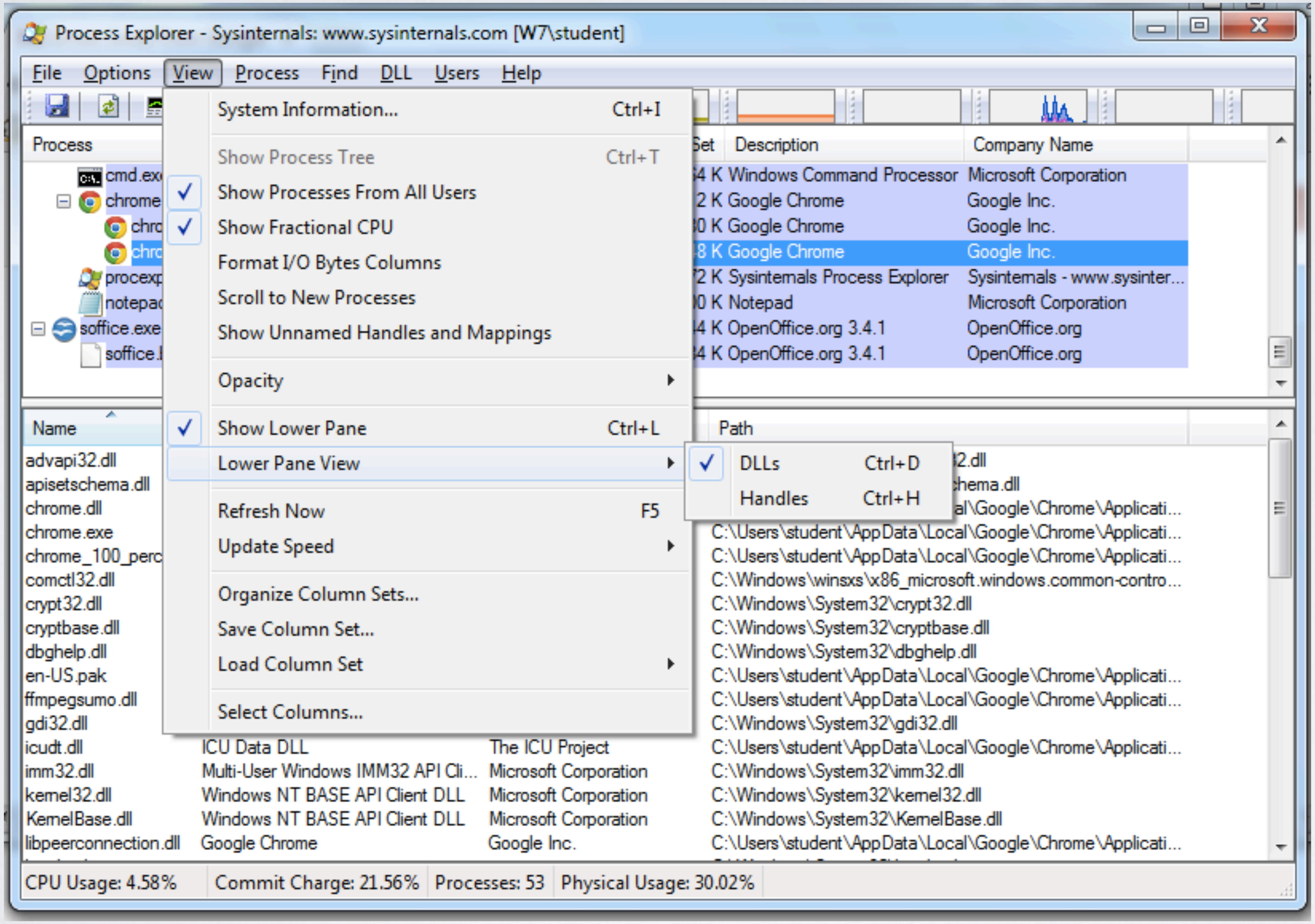
CPU Usage: 3.19% | Commit Charge: 21.92% | Processes: 57 | Physical Usage: 30.24%

PROCESS EXPLORER

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

PROCESS EXPLORER

Info on loaded DLLs is available



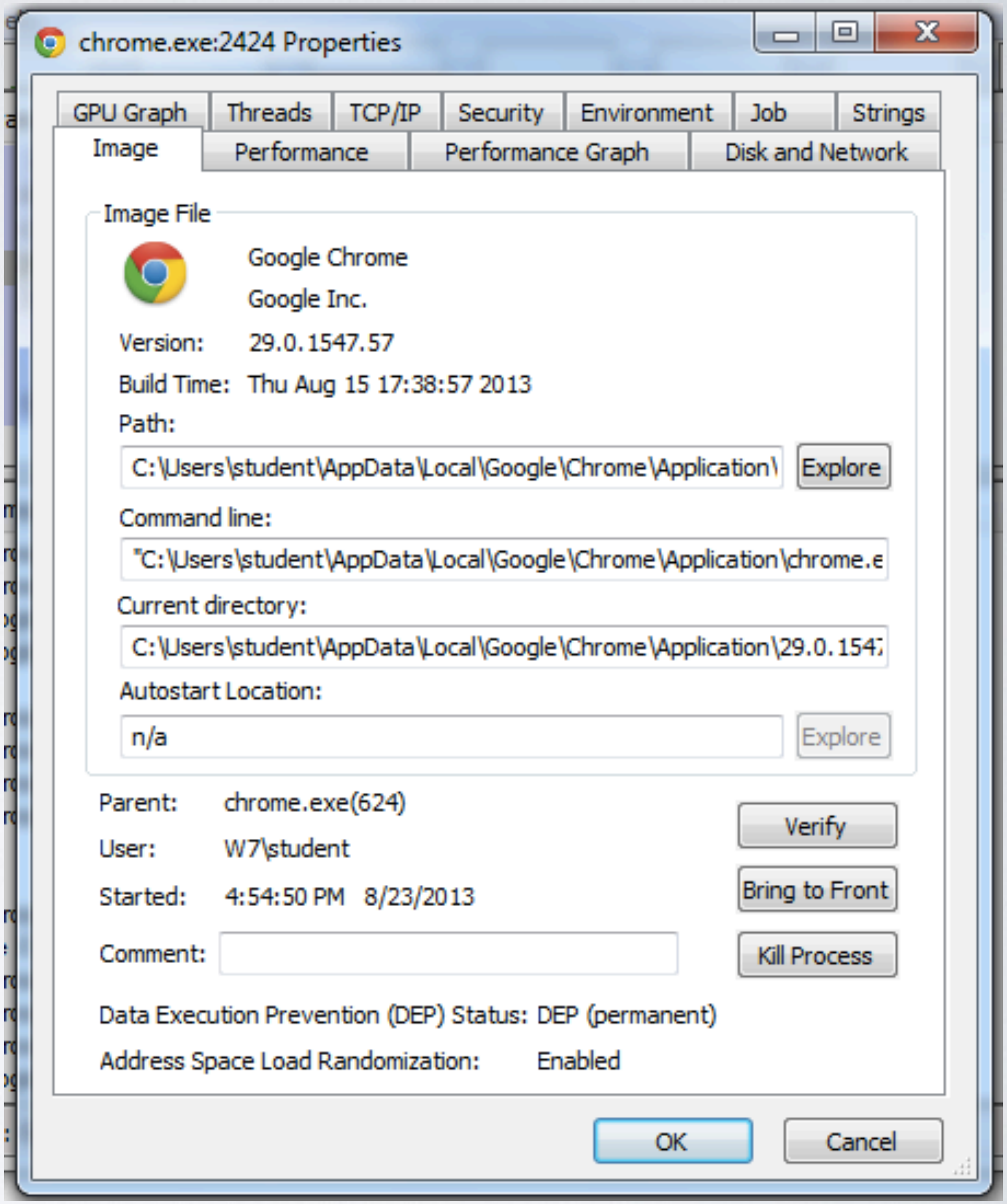
Process	Set	Description	Company Name
cmd.ex	4 K	Windows Command Processor	Microsoft Corporation
chrome	2 K	Google Chrome	Google Inc.
chro	0 K	Google Chrome	Google Inc.
chro	8 K	Google Chrome	Google Inc.
procexp	2 K	Sysinternals Process Explorer	Sysinternals - www.sysinter...
notepad	0 K	Notepad	Microsoft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

- Shows DEP and ASLR status
- Verify button checks the disk file's Windows signature
- But not the memory image, so it will not detect **process replacement**



chrome.exe:2424 Properties

Image File

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

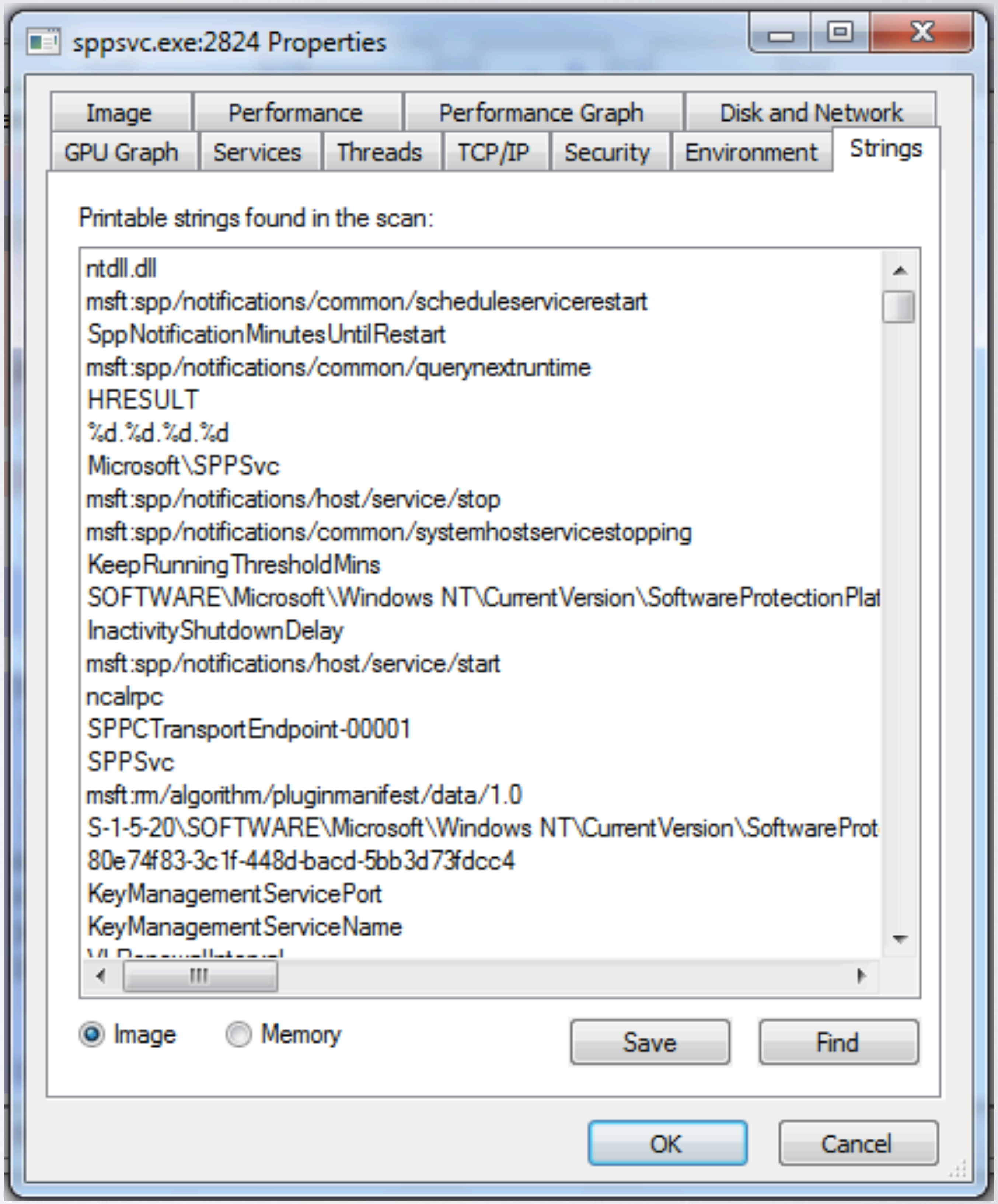
Comment:

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 (e.g., an old version of Adobe Reader)
- Watch Process Explorer to see if it launches a process
- The Image tab of the Properties sheet for that process will show where the malware is

THE REGISTRY

Repository for configuration and control of Windows systems

System-wide

- Which device drivers to load, how to configure memory manager, process manager, etc.
- Applications read system-wide settings

Per-user settings

- Per-user preferences
- Most-recently accessed documents

THE REGISTRY

Registry key is a container consisting of other keys (subkeys) or values

Registry value stores data whose type can be REG_SZ, REG_DWORD, REG_BINARY, etc.

Root Key	**Stored Information**	**Link**
HKEY_CLASSES_ROOT (HKCR)	File association and Component Object Model (COM) object registration (e.g ProgID and CLSID)	Merged
HKEY_CURRENT_USER (HKCU)	Data associated with the currently logged-on user	Yes
HKEY_LOCAL_MACHINE (HKLM)	Global settings for the machine	No
HKEY_USERS (HKU)	All the accounts on the machine	No
HKEY_CURRENT_CONFIG (HKCC)	Current hardware profile	Yes

THE REGISTRY

REG_LINK

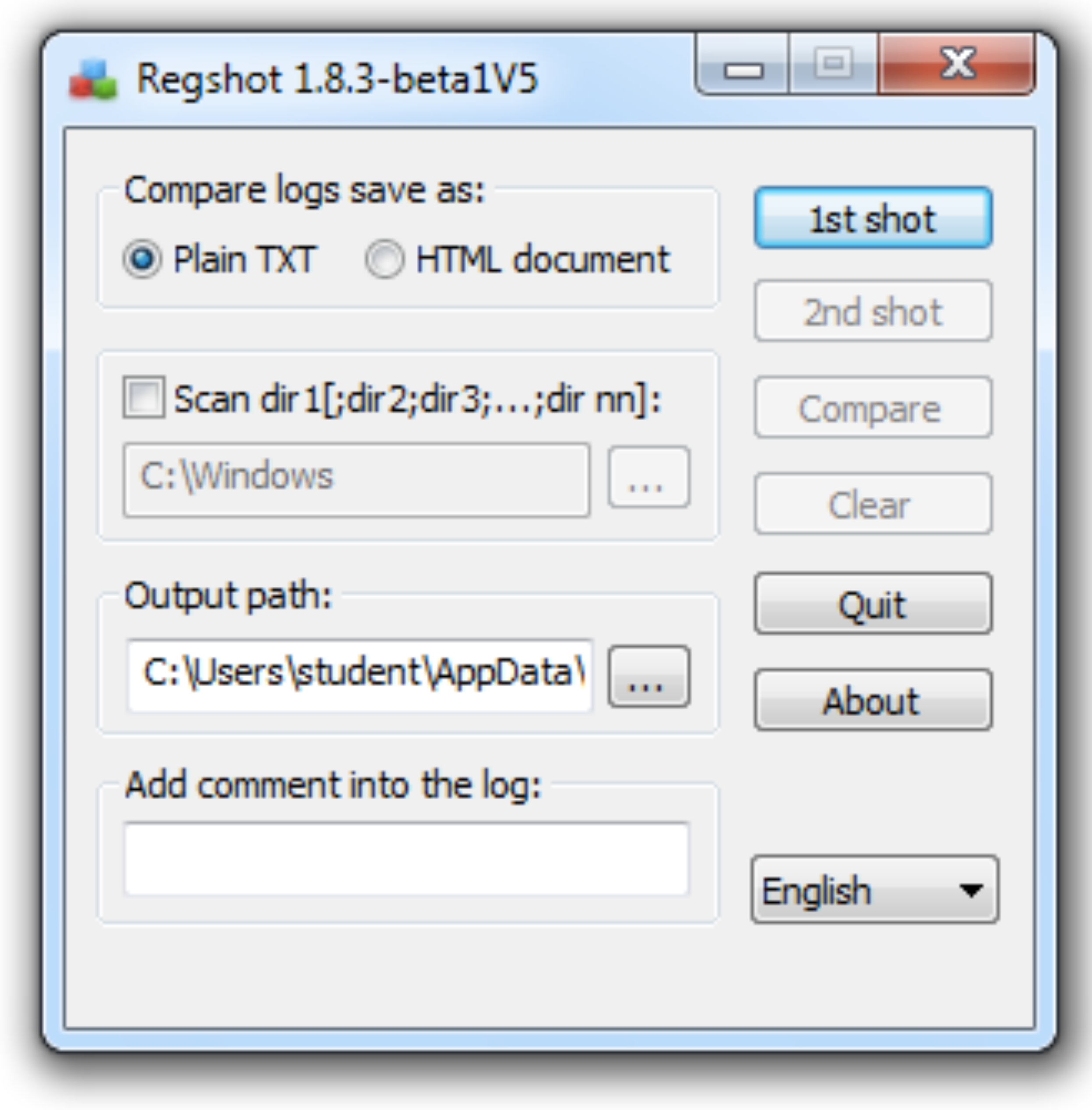
- HKEY_CURRENT_USER is a link to HKEY_USERS\Security ID (SID) of current user
- HKEY_CURRENT_CONFIG is a link to HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\Current
- HKLM\SYSTEM\CurrentControlSet is a link to HKLM\SYSTEM\ControlSet00X, where X is a number

Registry Hive

- “Logical group of keys, subkeys and values in the registry that has a set of supporting files containing backups of its data”
  - HKLM\SAM is stored in c:\windows\system32\config\SAM
- Or constructed dynamically in memory

REGSHOT

Useful to check how a process modified the registry



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:

```
Regshot
Comments:
Datetime: <date>
Computer: MALWAREANALYSIS
Username: username
----------------------------------
Keys added: 0
----------------------------------

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

----------------------------------
Values modified:2
----------------------------------
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
----------------------------------
```

PERSISTENCE

Techniques to survive after reboot

- Registry Key
- File System
  - Startup locations
  - DLL search order hijacking
  - Trojanizing system files
- Master Boot Record (MBR)
- Basic Input/Output System (BIOS)

FREQUENTLY USED REGISTRY KEY

Administrator privilege is required to update HKLM (The list is not comprehensive nor more important than others, which are not listed here)
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\”Shell” and “UserInit”
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\”Appinit_Dlls”
HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
HKLM\System\CurrentControlSet\Services
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects

Without administrator privileges, malware can persist with the following registry keys (The list is not comprehensive nor more important than others, which are not listed here)
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
HKCU\Software\Policies\Microsoft\Windows\System\Scripts\Logon
HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell

PERSISTENCE USING FILE SYSTEM

Startup locations

- For the logged-in user: %USERPROFILE%\Start Menu\Programs\Startup
- For all users: %ALLUSERSPROFILE%\Start Menu\Programs\Startup

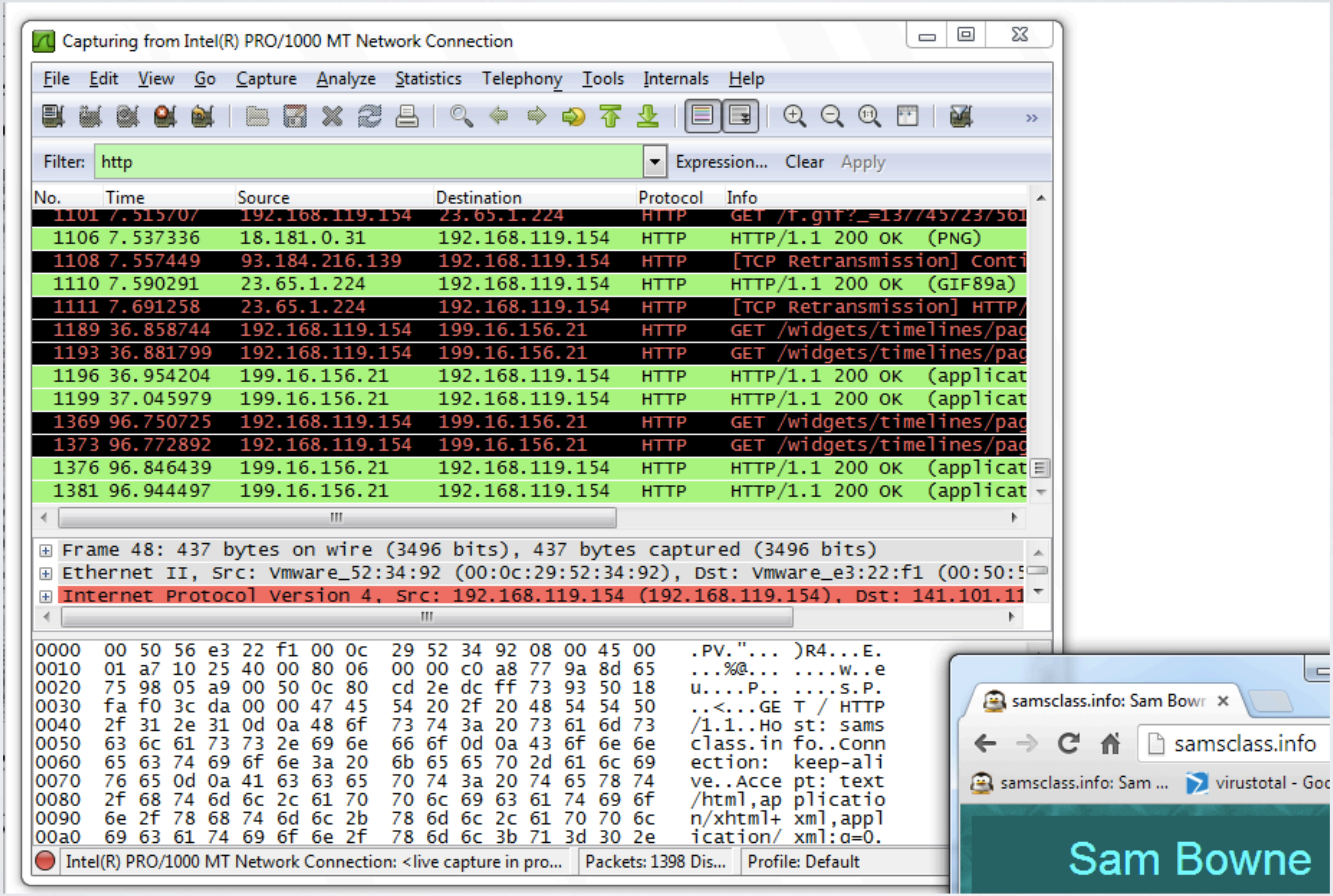
MICROSOFT WINDOWS SERVICES

- Long-running executables without user interaction (like a *nix daemon)
- Can be automatically started when the computer boots
- CreateService() Windows API to register a service
- Registered services can be found under the registry key HKLM\System\CurrentControlSet\Services

SVCHOST

- C:\Windows\System32\svchost.exe is a generic host process for services that run from DLLs
- Multiple instances are often running
  - One instance contains a group of services
- Groups are listed in the registry key HKLM\Software\Microsoft\Windows NT\CurrentVersion\Svchost
- It is common to have malware name itself svchost.exe but run from somewhere other than C:\Windows\System32 (e.g., C:\Windows)
- Or alternatively they will just add a new DLL for the real svchost to run as a service

PACKET SNIFFING WITH WIRESHARK



Capturing from Intel(R) PRO/1000 MT Network Connection
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: http
Expression... Clear Apply

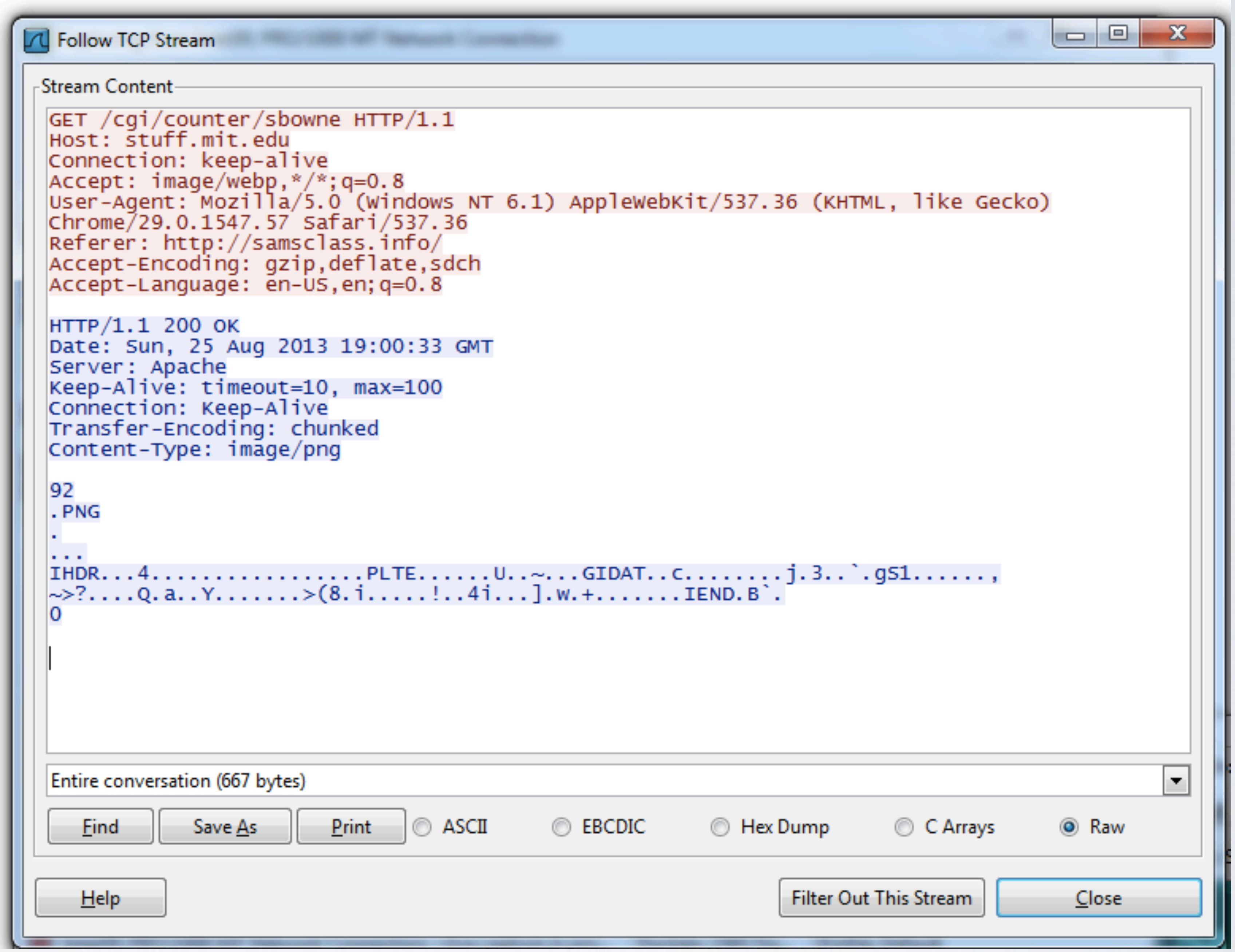
```
No.  Time       Source           Destination      Protocol  Info
1101 7.515707   192.168.119.154  23.65.1.224      HTTP      GET /f.gif?_=1377457237561
1106 7.537336   18.181.0.31      192.168.119.154  HTTP      HTTP/1.1 200 OK  (PNG)
1108 7.557449   93.184.216.139   192.168.119.154  HTTP      [TCP 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.
```

FOLLOW TCP STREAM

- Can save files from streams here too



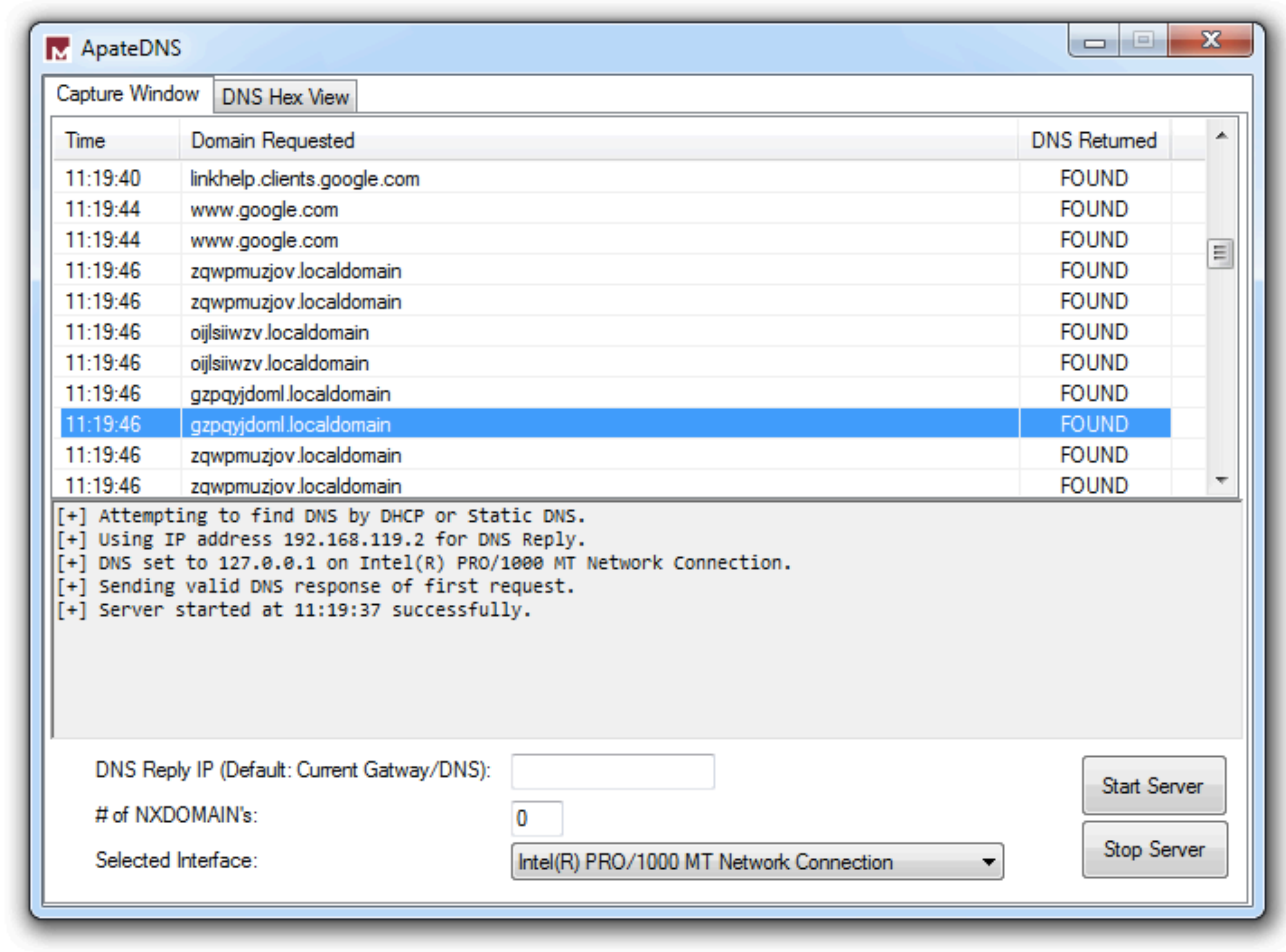
```
GET /cgi/counter/sbowne HTTP/1.1
Host: stuff.mit.edu
Connection: keep-alive
Accept: image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/29.0.1547.57 Safari/537.36
Referer: http://samsclass.info/
Accept-Encoding: gzip,deflate,sdch
Accept-Language: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

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

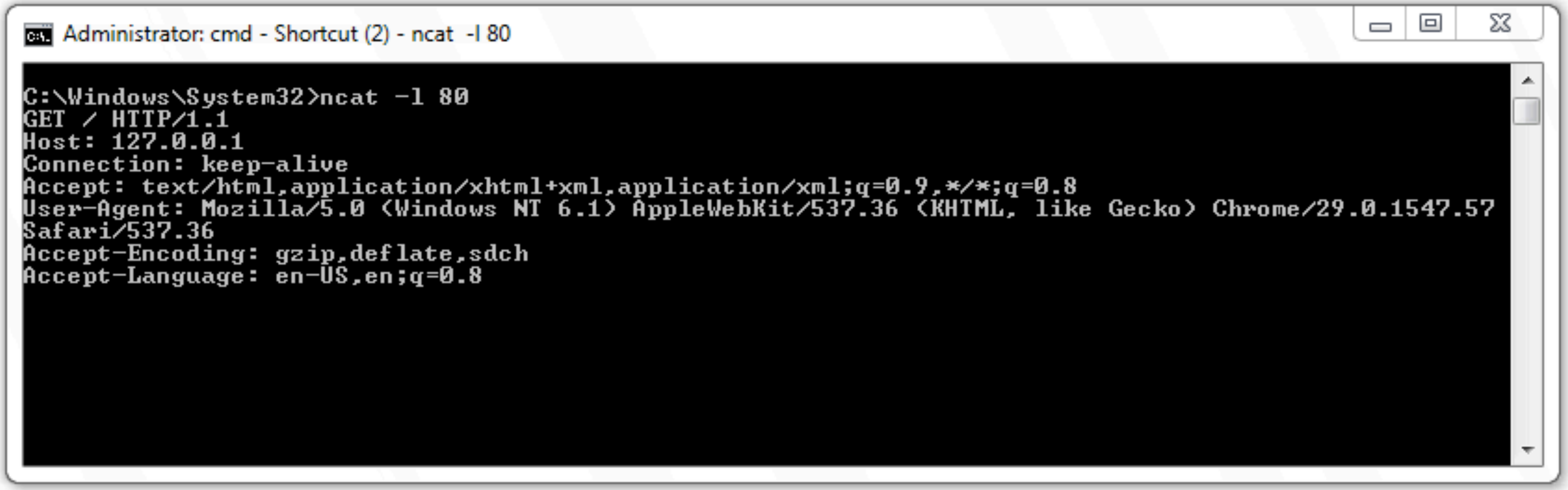
```
[+] Attempting to find DNS by DHCP or Static DNS.
[+] Using IP address 192.168.119.2 for DNS Reply.
[+] DNS set to 127.0.0.1 on Intel(R) PRO/1000 MT Network Connection.
[+] Sending valid DNS response of first request.
[+] Server started at 11:19:37 successfully.
```

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

# of NXDOMAIN's: 0

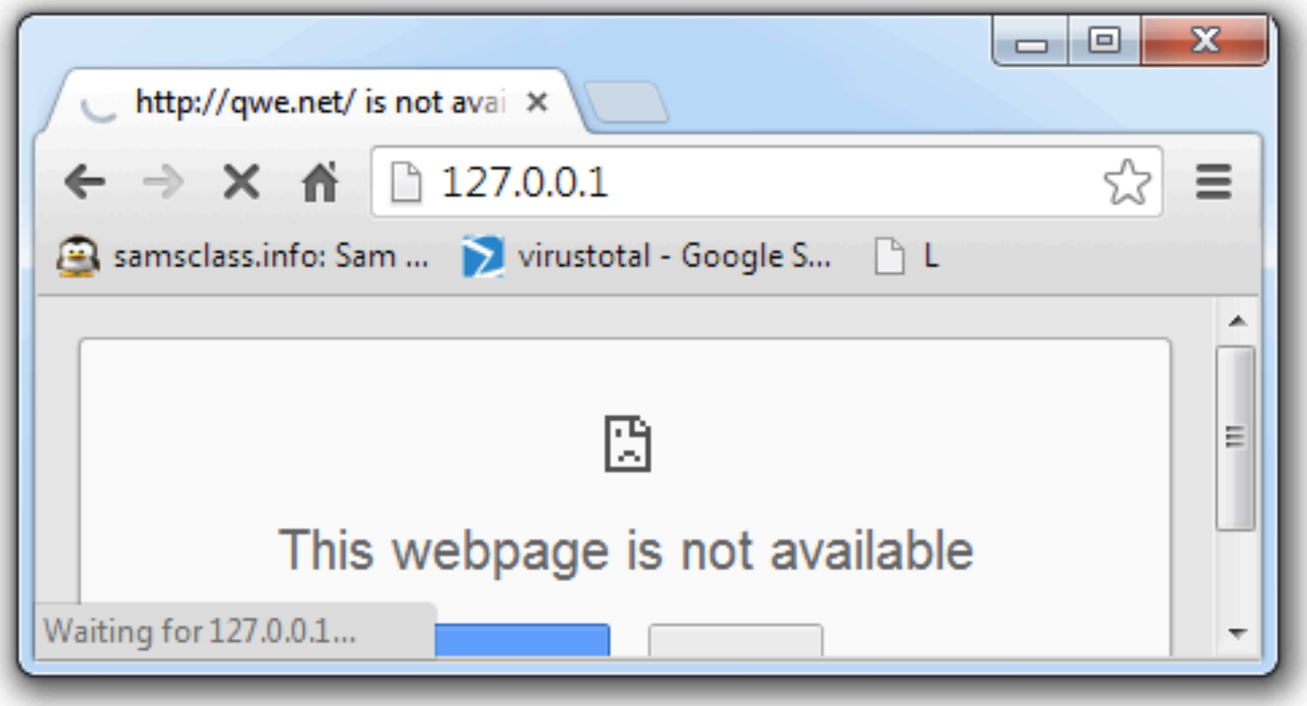
Selected Interface: Intel(R) PRO/1000 MT Network Connection

MONITORING WITH NCAT (INCLUDED WITH NMAP)



Administrator: cmd - Shortcut (2) - ncat -l 80

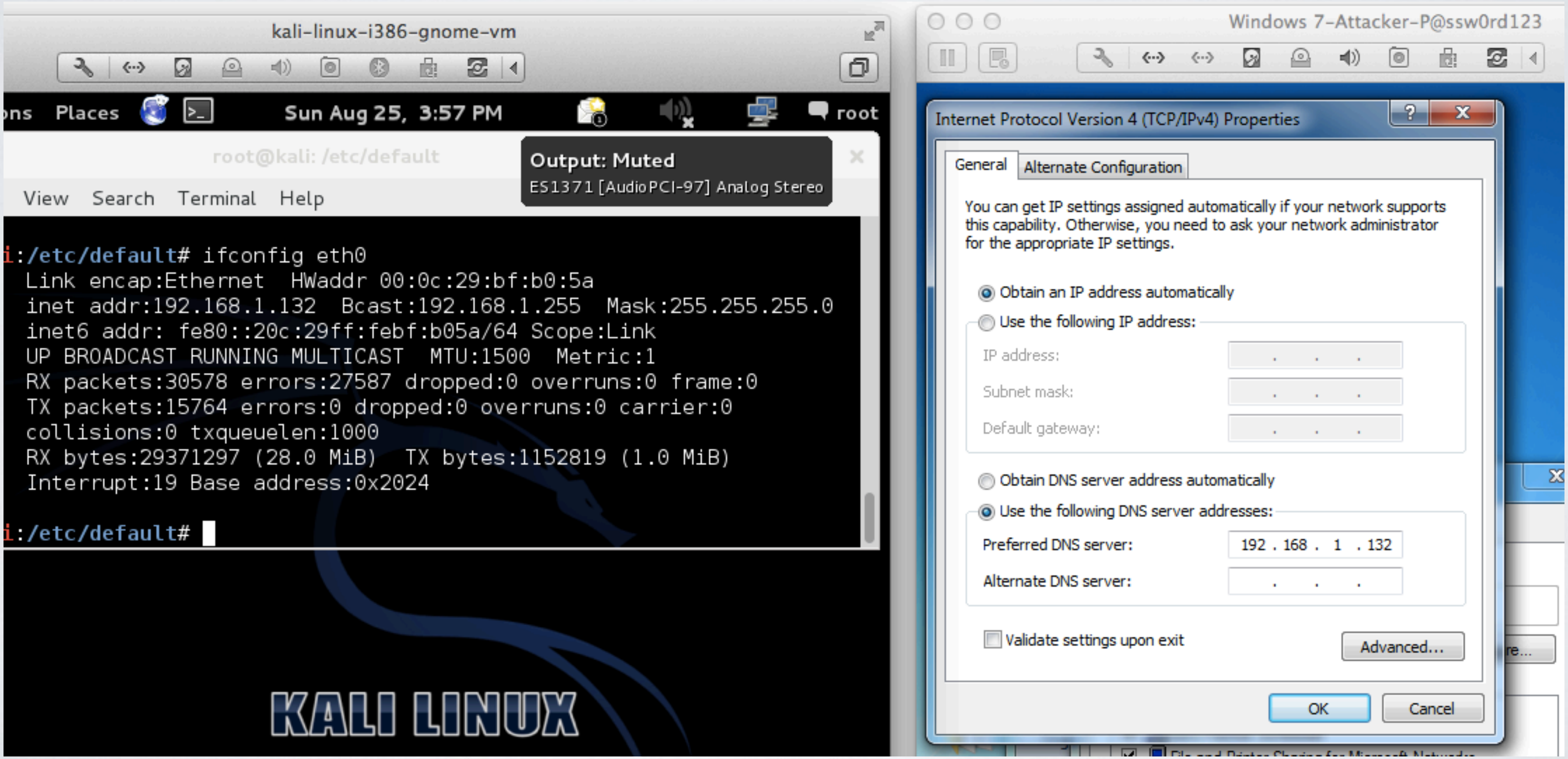
```
C:\Windows\System32>ncat -l 80
GET / HTTP/1.1
Host: 127.0.0.1
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/29.0.1547.57
Safari/537.36
Accept-Encoding: gzip,deflate,sdch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



This webpage is not available

Waiting for 127.0.0.1...

INETSIM



```
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# 
```

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

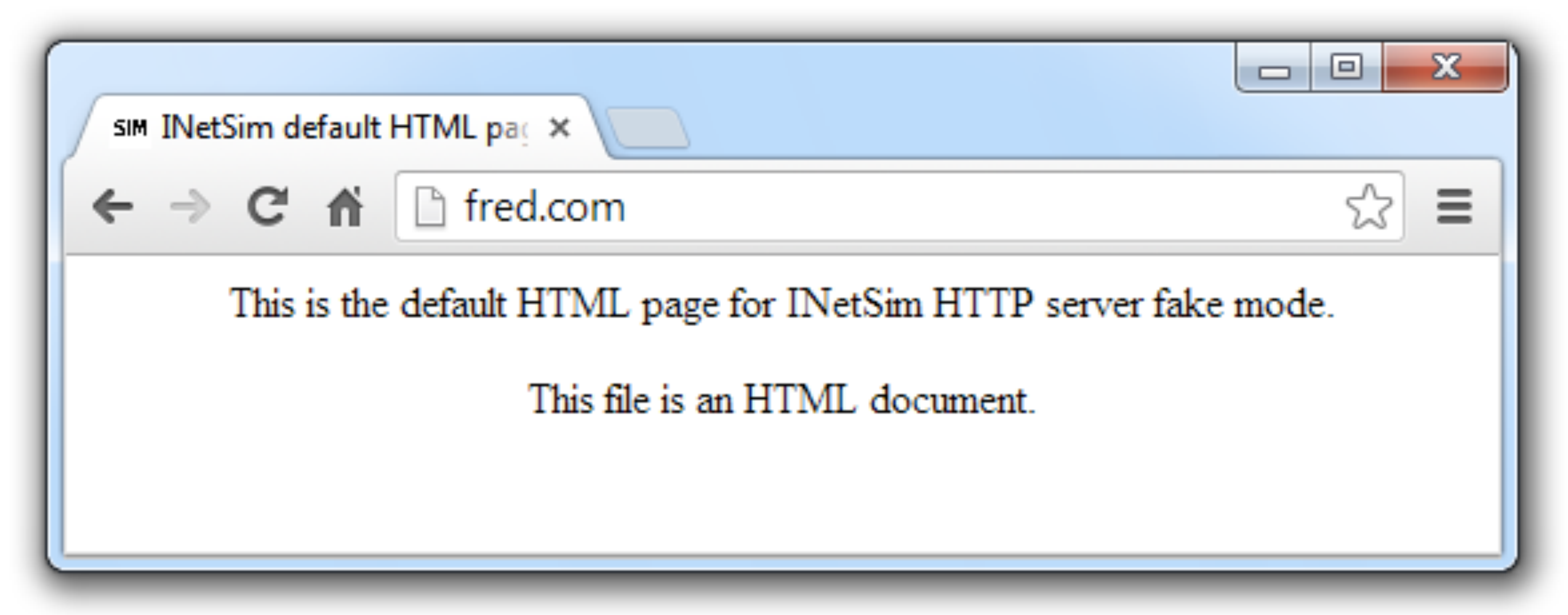
● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 1 . 132

Alternate DNS server: . . .

□ Validate settings upon exit

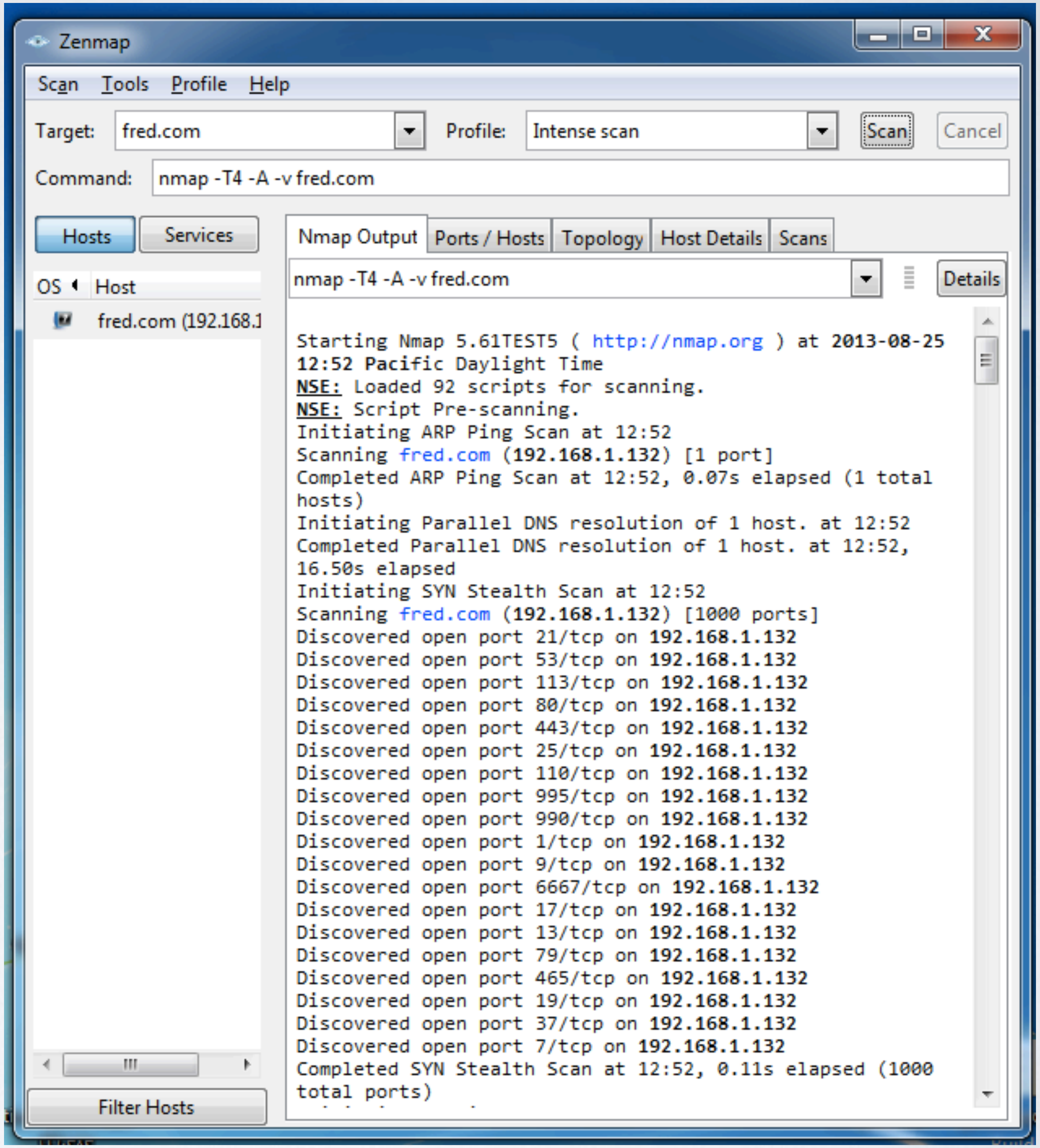
INETSIM FOOLS A BROWSER



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

```
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)
```

USING THE TOOLS

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

CREDITS

- Some of these slides come from:
  - http://opensecuritytraining.info/MalwareDynamicAnalysis.htm