Malware Analysis

Chapter 3: Basic Dynamic Analysis

王志
zwang@nankai.edu.cn

updated on Mar. 8th 2021

College of Cyber Science
Nankai University
2021/2022

Outline

- Basic Dynamic Analysis
- Sandbox
- Launch DLLs
- Monitor process
- Regshot
- Faking a Network
- Basic Dynamic

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

GFI SandBox™ Analysis # 2307

Sample: win32XYZ.exe (56476e02c29e5dbb9286b5f7b9e708f5)

Table of Contents

Sandboxes

- Without command-line options
  - Botnet C&C packets
- Not record all events
  - Stalling behaviors
- Anti-VM techniques
- Certain Environment

Launching DLLs

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

Launching DLL

- Installed as a service
  - rpr32x.dll has the export: InstallService
  - rundll32 ipr32x.dll, InstallService ServiceName
  - net start ServiceName

Process Monitor

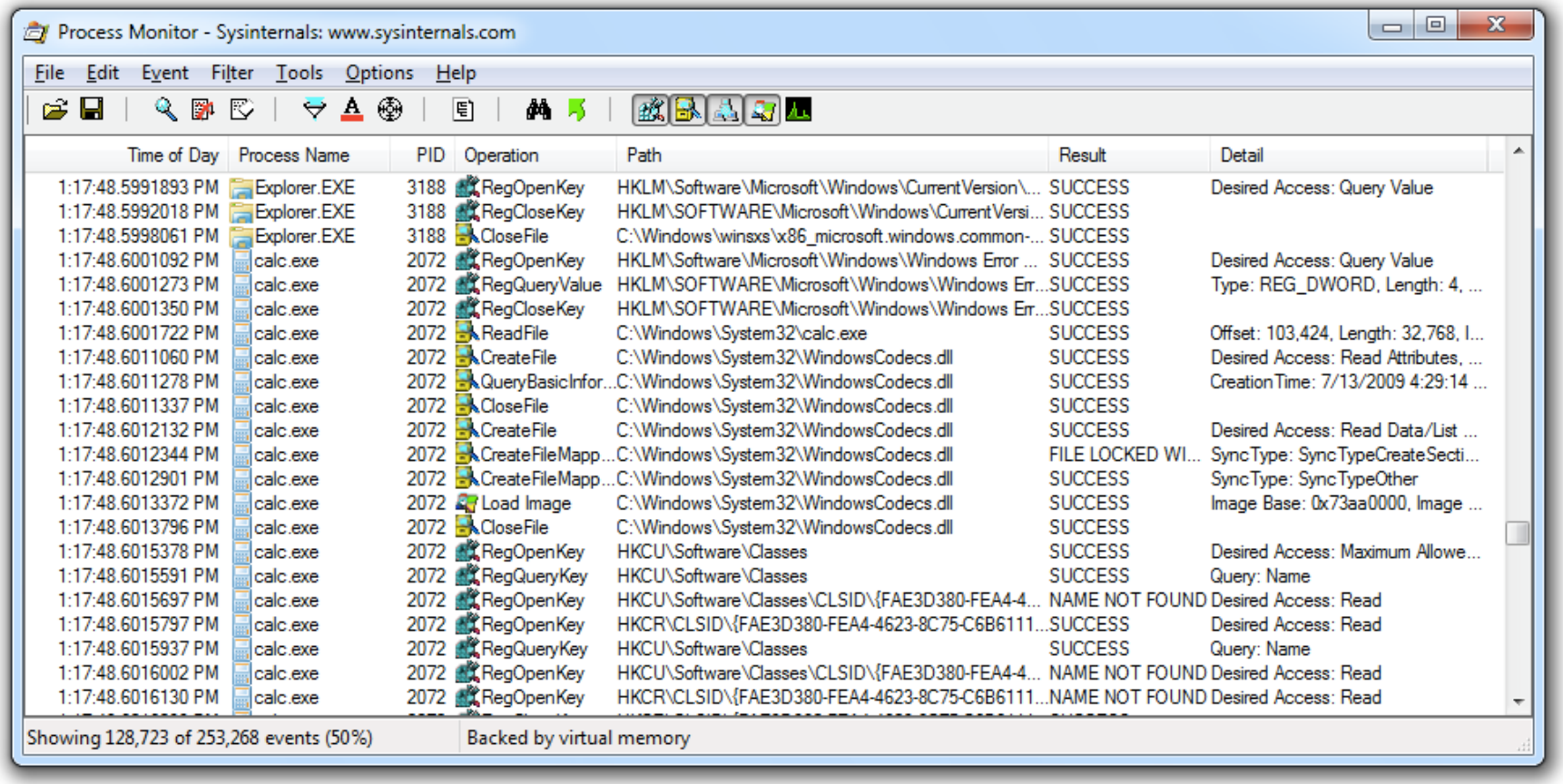
Process Monitor

- 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

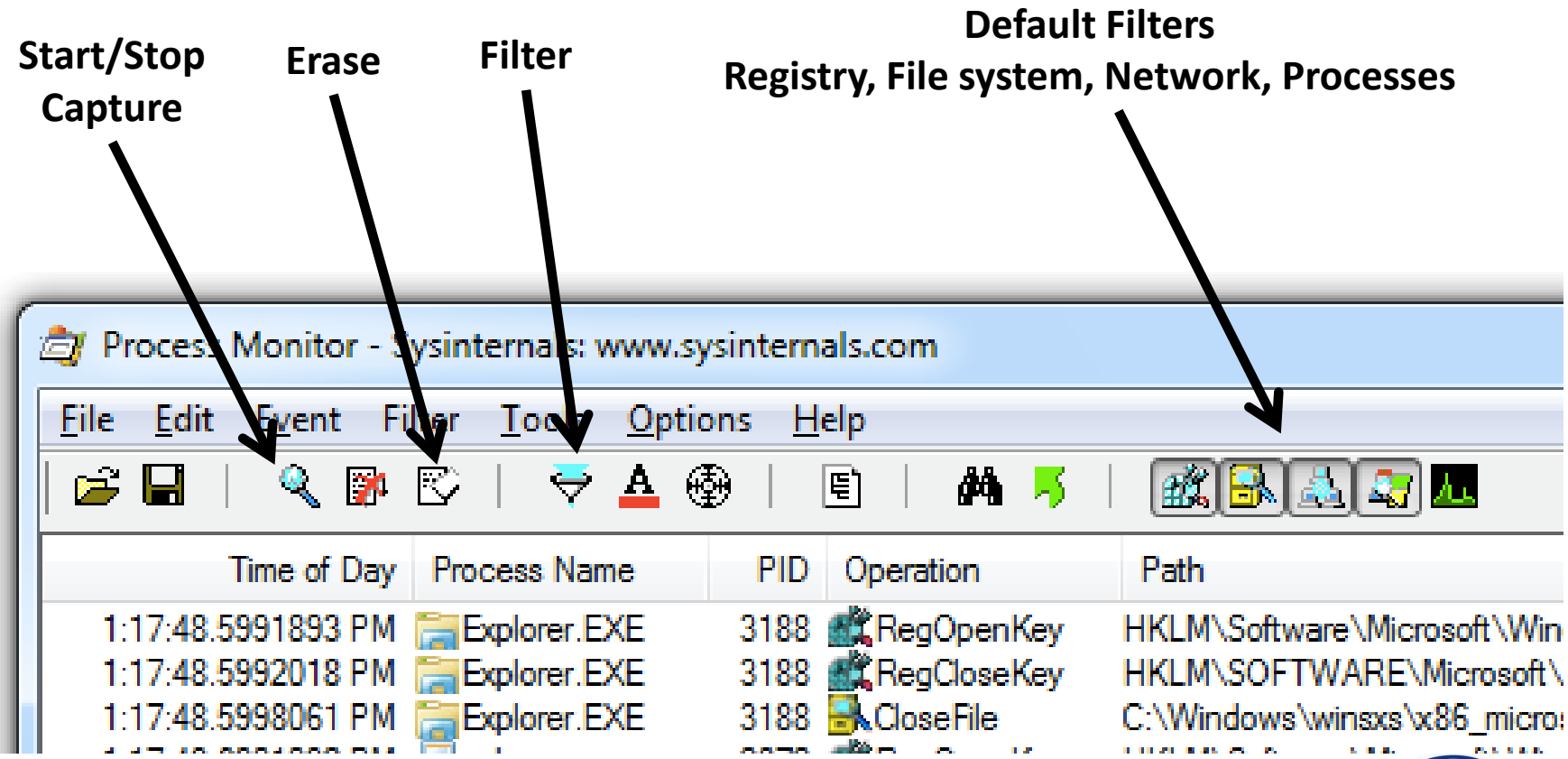
Process Monitor

- Don't run it too long or it will fill up all RAM and crash the machine
  - Use RAM to log events until it is told to stop capturing
  - run out memory to crash the system
  - limited periods of time
  - File->Capture Events
  - File->Clear Display

Launching Calc.exe



Process Monitor Toolbar

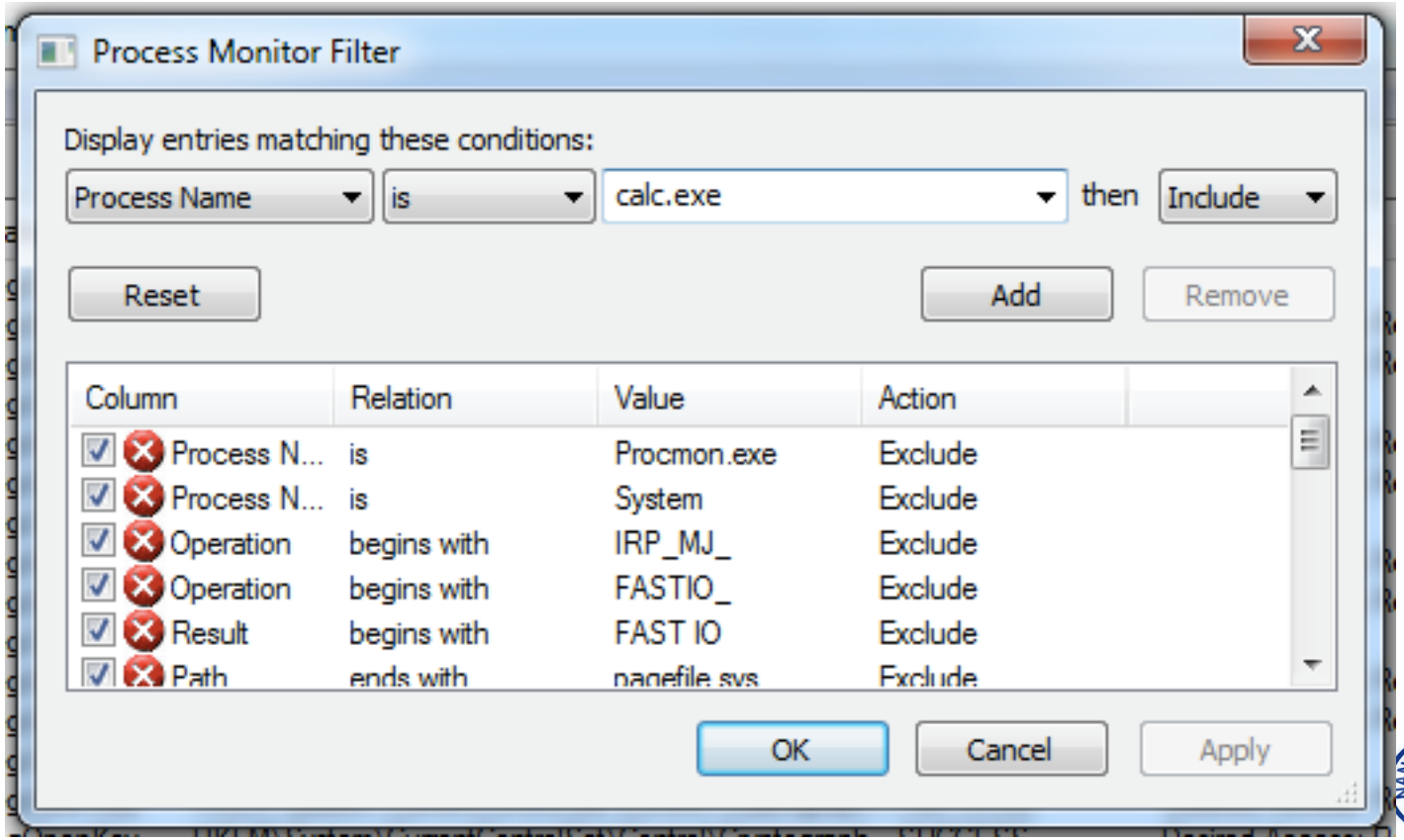


Filtering with Exclude

- One technique: hide normal activity before launching malware
- Filter on process name
- Filter on system calls
- Right-click each Process Name and click **Exclude**

Filtering with Include

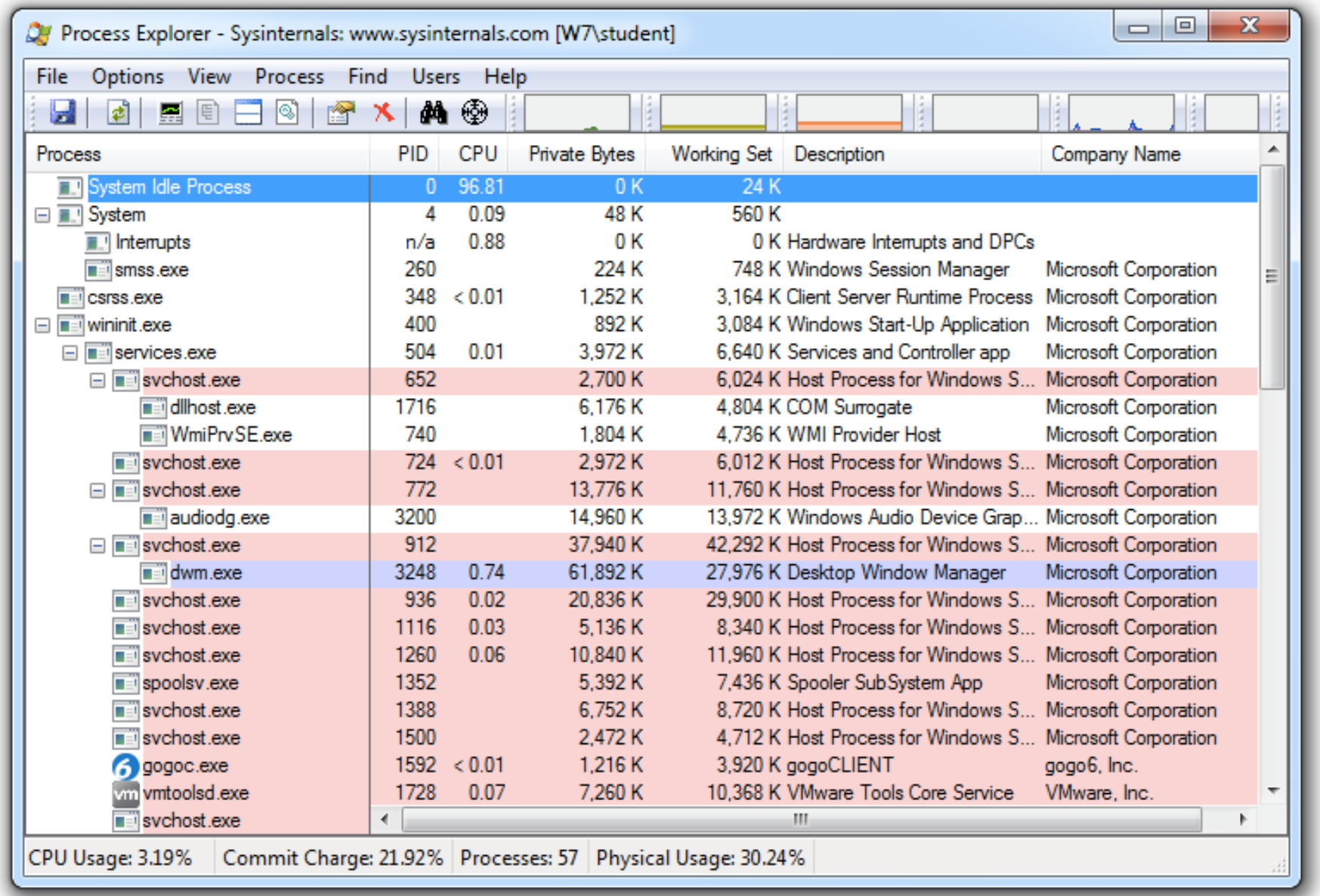
- Most useful filters: Process Name, Operation, and Detail



Process Explorer

Process Explorer

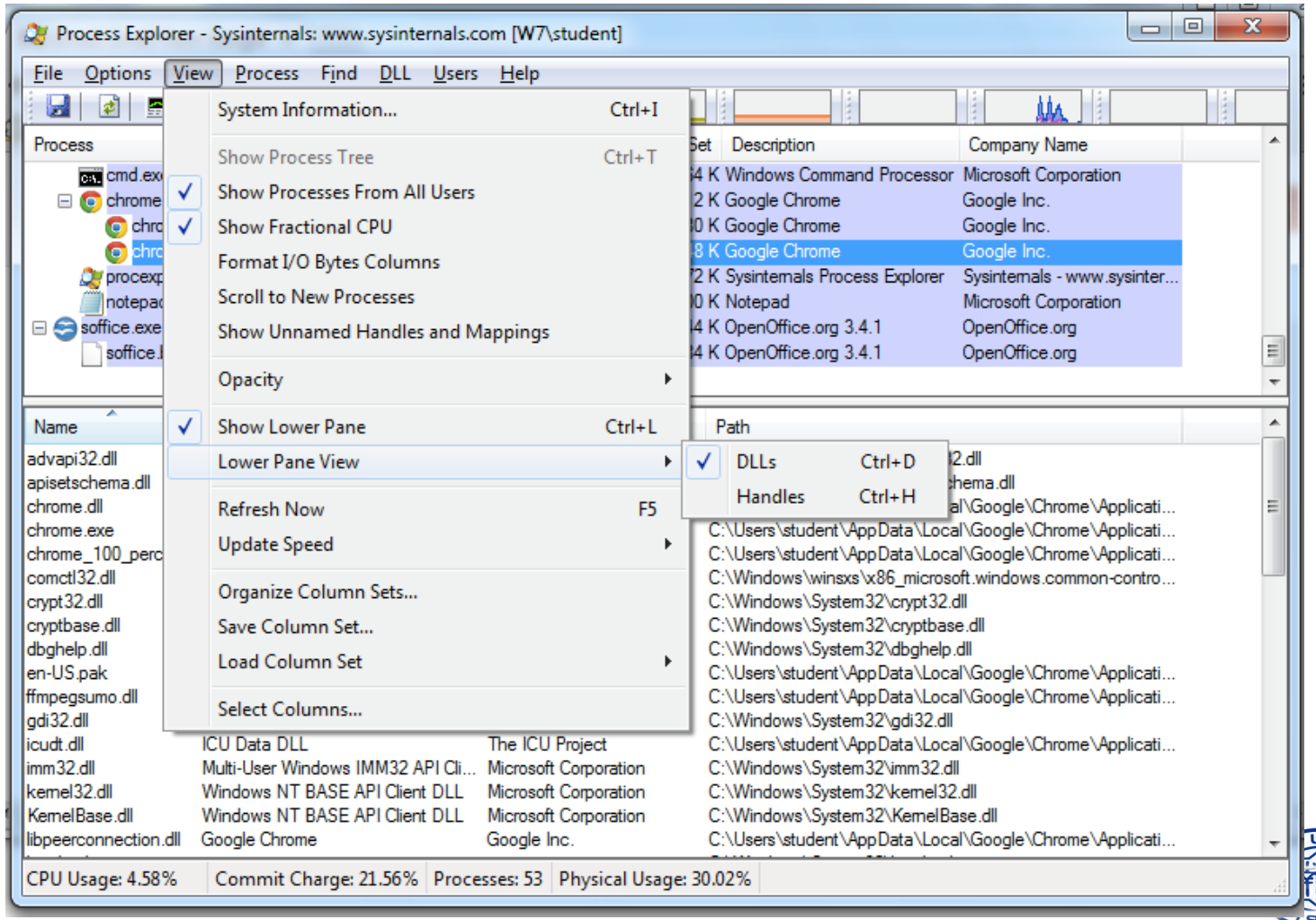
- List all processes currently running on the system
  - Dlls loaded
  - Various process properties
  - Overall system information



Coloring

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

DLL Mode

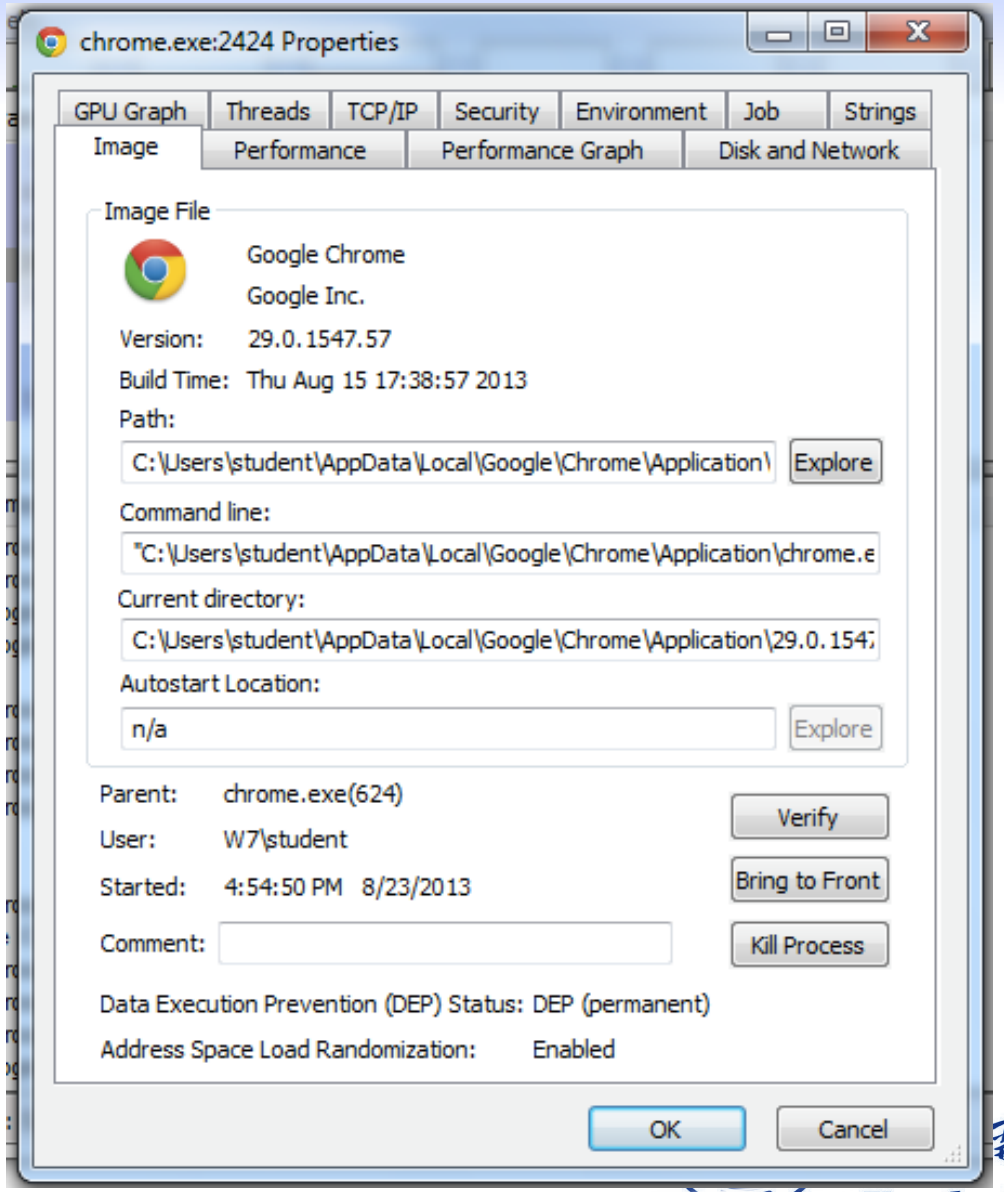

Process Explorer - Sysinternals: www.sysinternals.com [W7\student]
File Options View Process Find DLL Users Help
System Information... Ctrl+I
Show Process Tree Ctrl+T
Show Processes From All Users
Show Fractional CPU
Format I/O Bytes Columns
Scroll to New Processes
Show Unnamed Handles and Mappings
Opacity
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%

Handle Mode

Type	Name
Directory	\Windows
Directory	\BaseNamedObjects
Event	\BaseNamedObjects\crypt32LogoffEvent
Event	\BaseNamedObjects\userenv: User Profile setup event
Event	\BaseNamedObjects\userenv: Machine Group Policy has been applied
Event	\BaseNamedObjects\userenv: User Group Policy has been applied
File	C:\Tools\ProcessExplorer
File	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1d...
File	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1d...
File	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1d...
File	\Device\KsecDD
File	C:\Documents and Settings\xpbot\Local Settings\Temp\Perflib_Perfdata_25...
File	\Device\PROCEXP152
File	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1d...
File	\Device\Tcp
File	\Device\Tcp
File	\Device\Ip
File	\Device\Ip
File	\Device\Ip

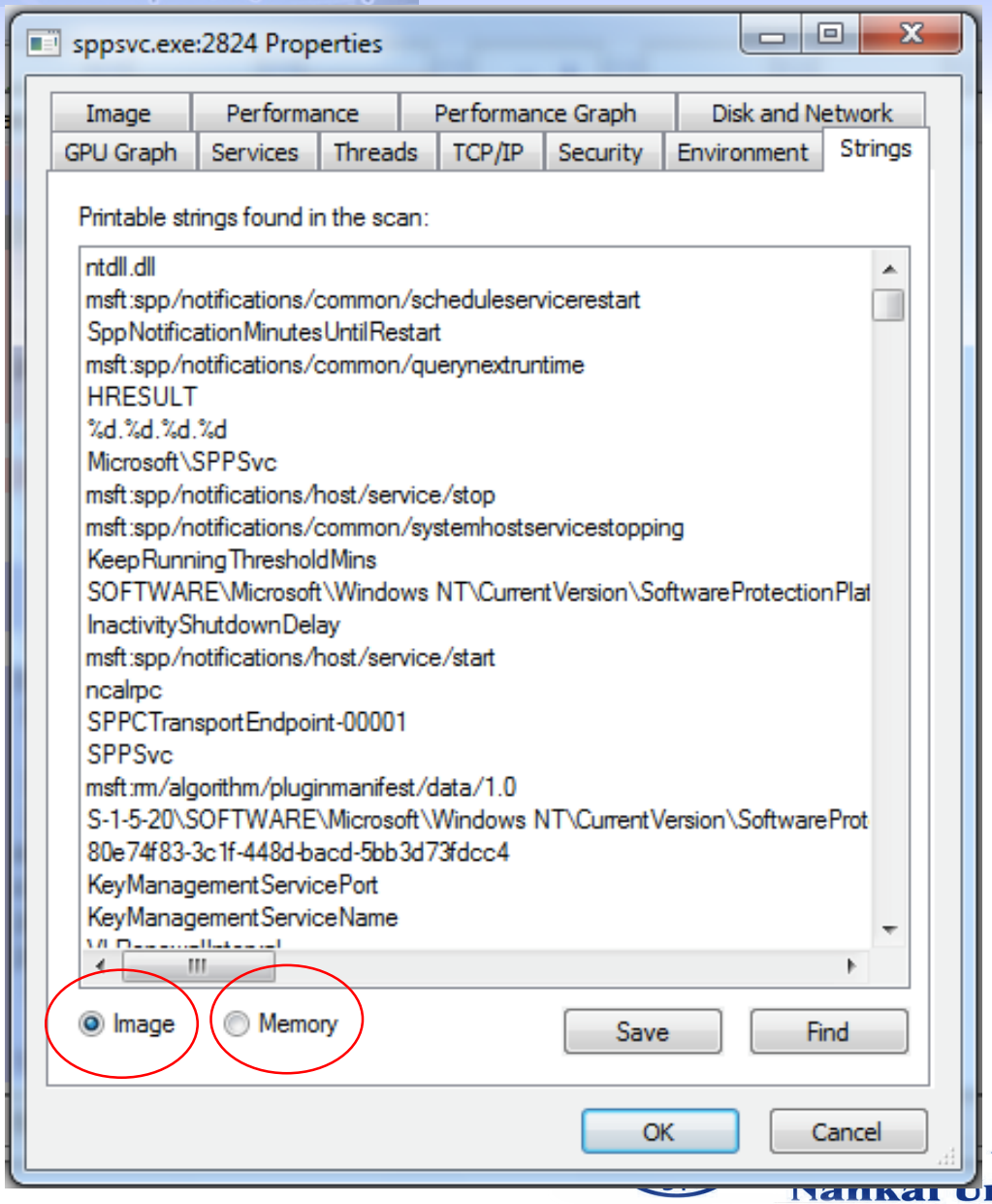
Properties

- Shows DEP and ASLR 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



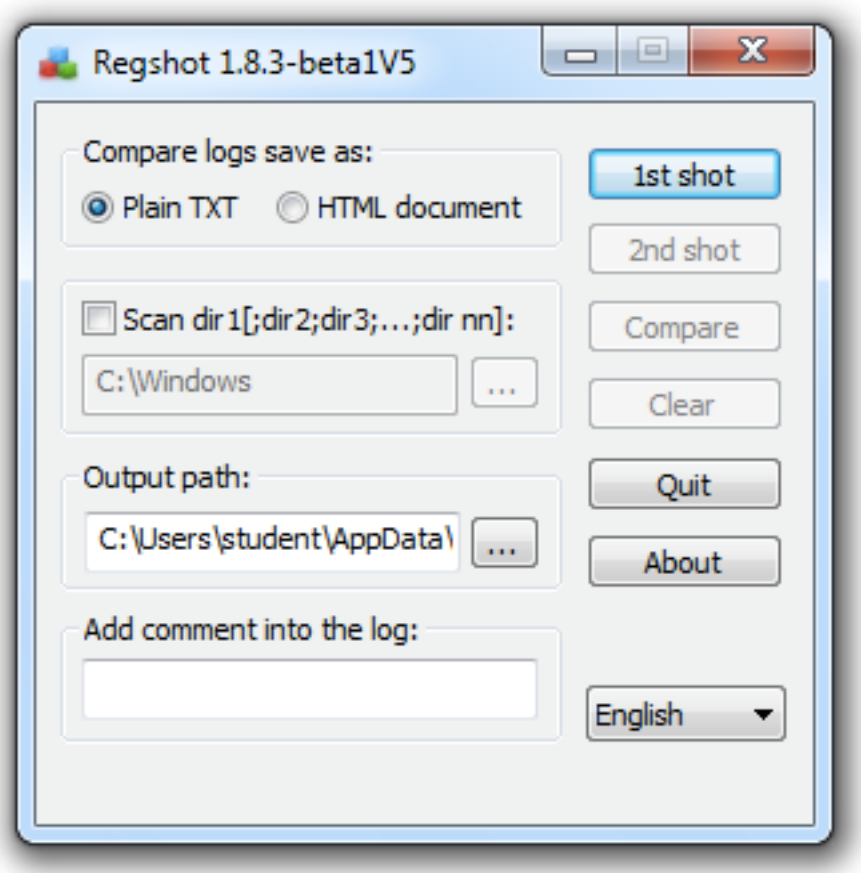
Detecting Malicious Documents

- 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

Regshot

Regshot

- An open source registry comparison tool
  - Take registry snapshots
  - Compare two registry 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:
1st shot
2nd shot
Compare
Clear
Quit
About
English

主观题 10分

设置

Windows注册表有哪些功能?

正常使用主观题需2.0以上版本雨课堂

作答

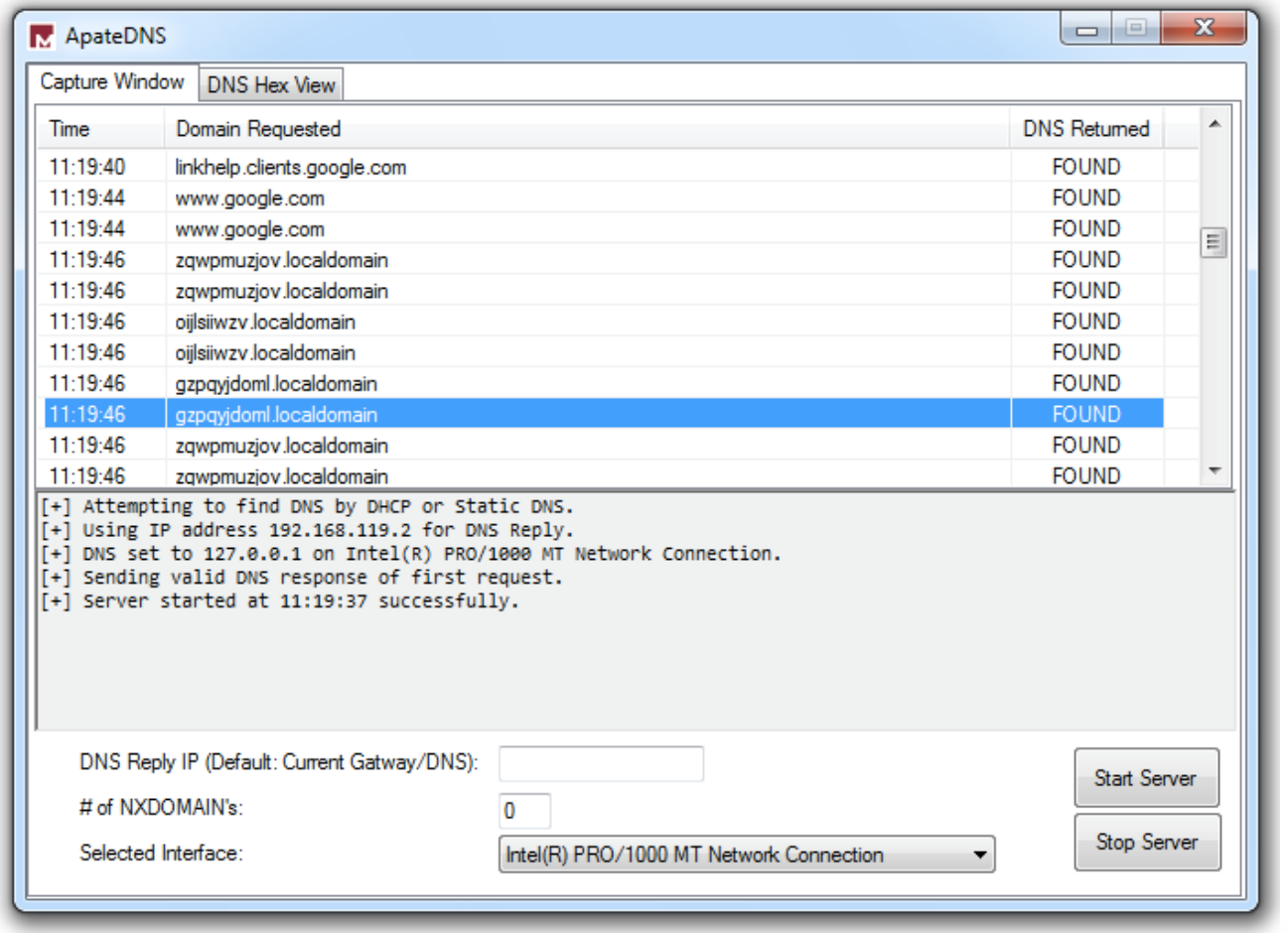
南開大學 Nankai University

Faking a Network

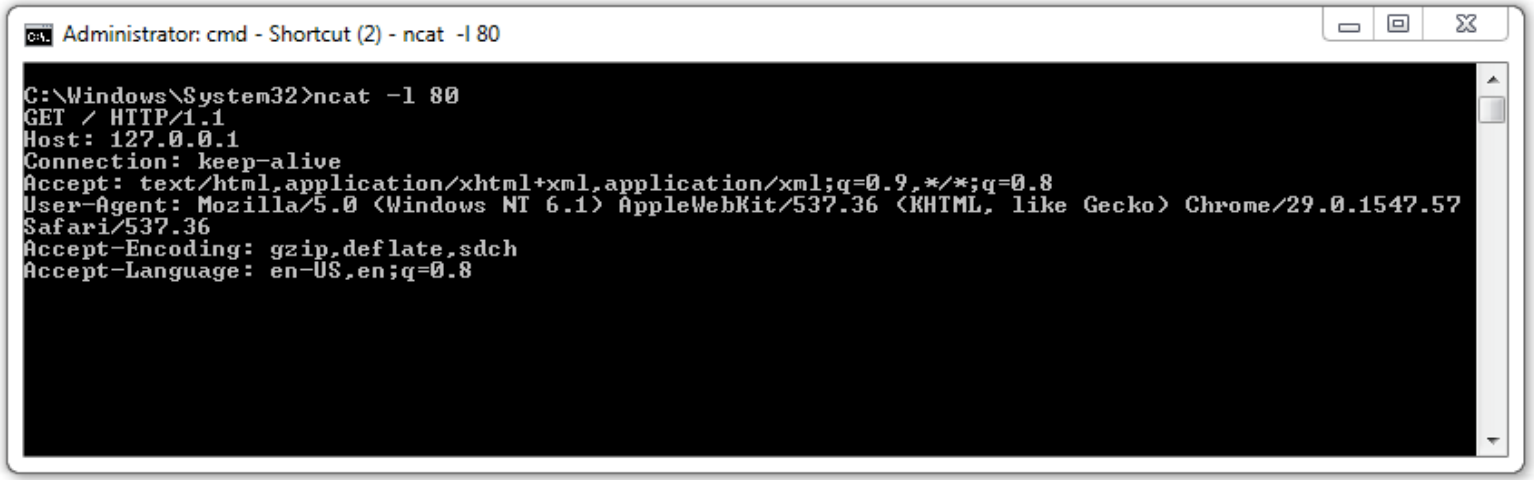
Faking a Network

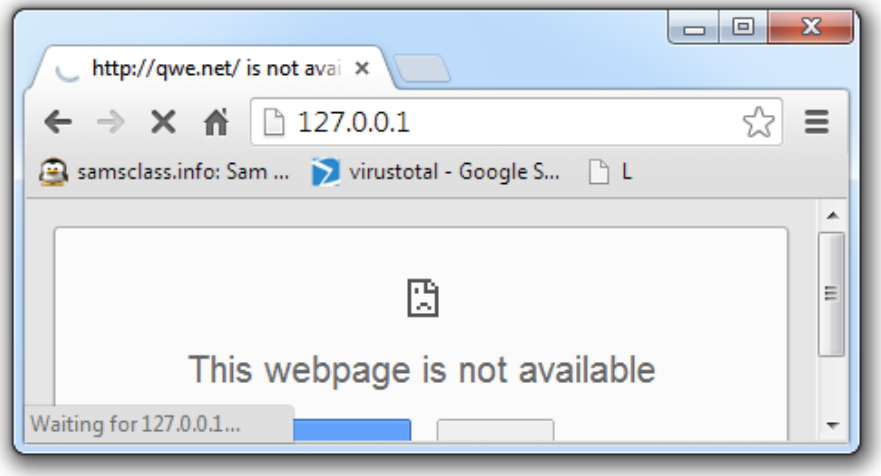
- Malware:
  - beacons out
  - communicate with a C&C server
- Fake Network
  - obtain network indicators
  - airgap between VM and Internet

Using ApateDNS to Redirect DNS Resolutions



Monitoring with Ncat (included with Nmap)

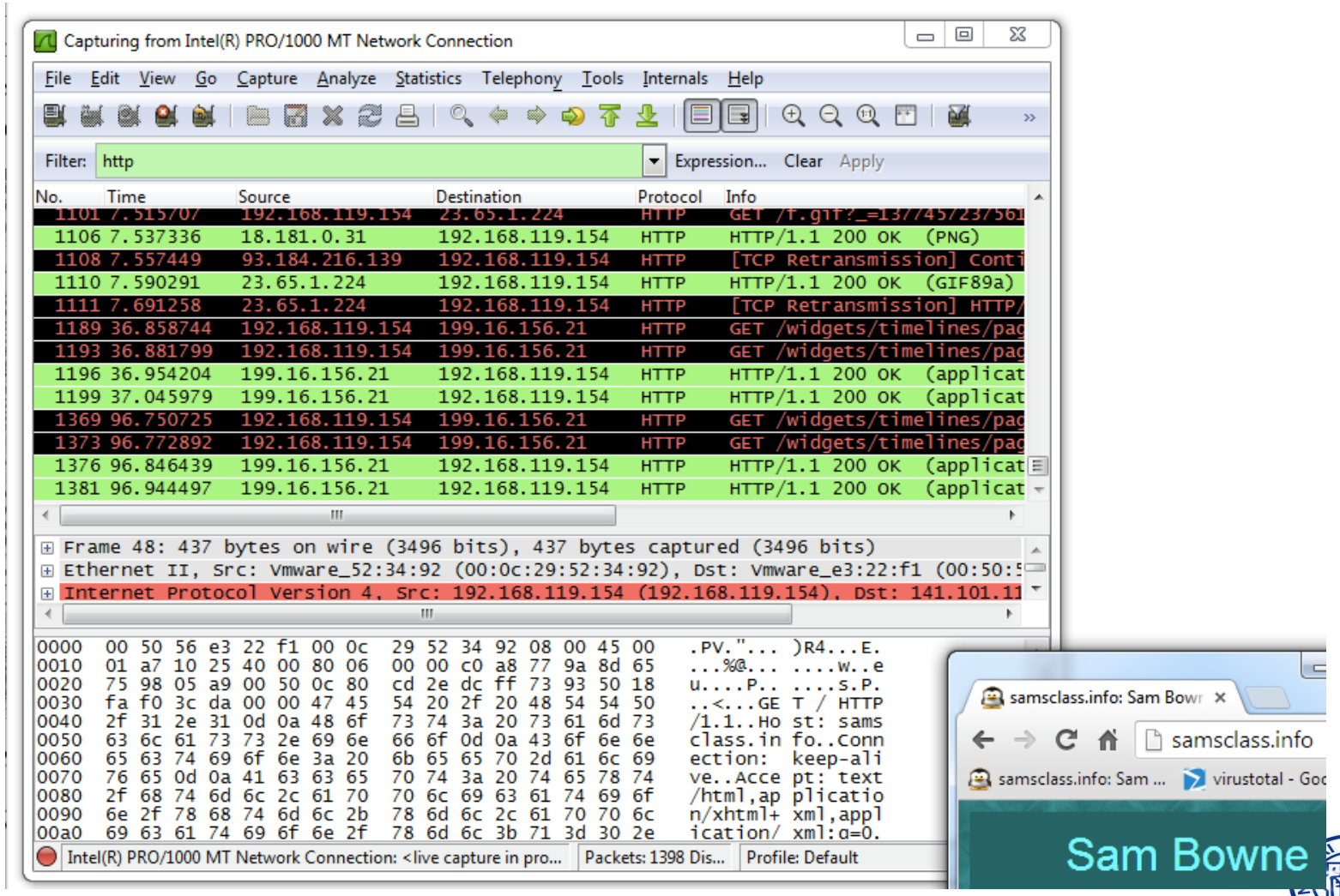




Wireshark

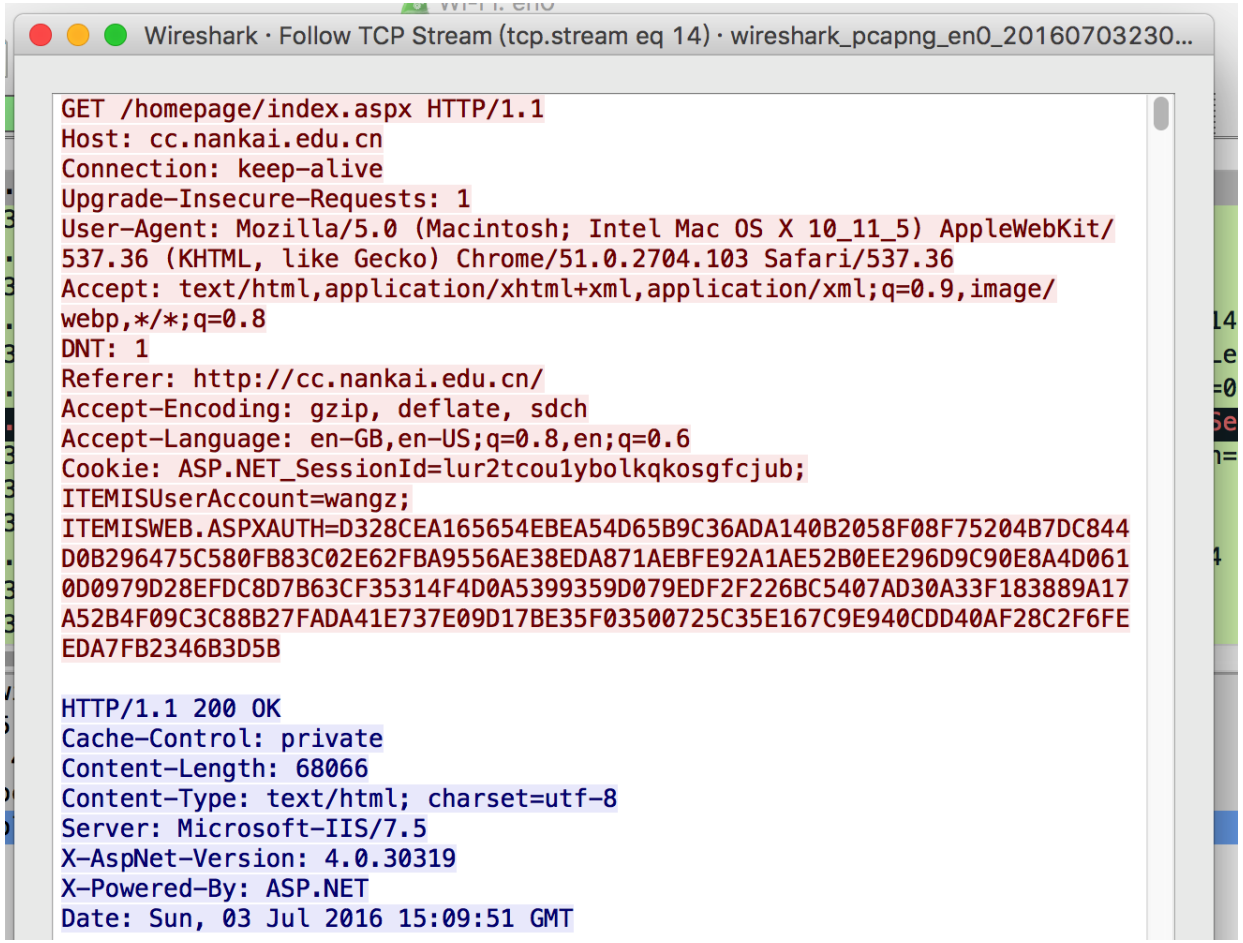
- Open source sniffer
  - capture packets
  - intercepts and logs network traffic
- Understand malware network communication
- Chapter 14 discusses protocol analysis and additional uses of Wireshark.

Packet Sniffing with Wireshark

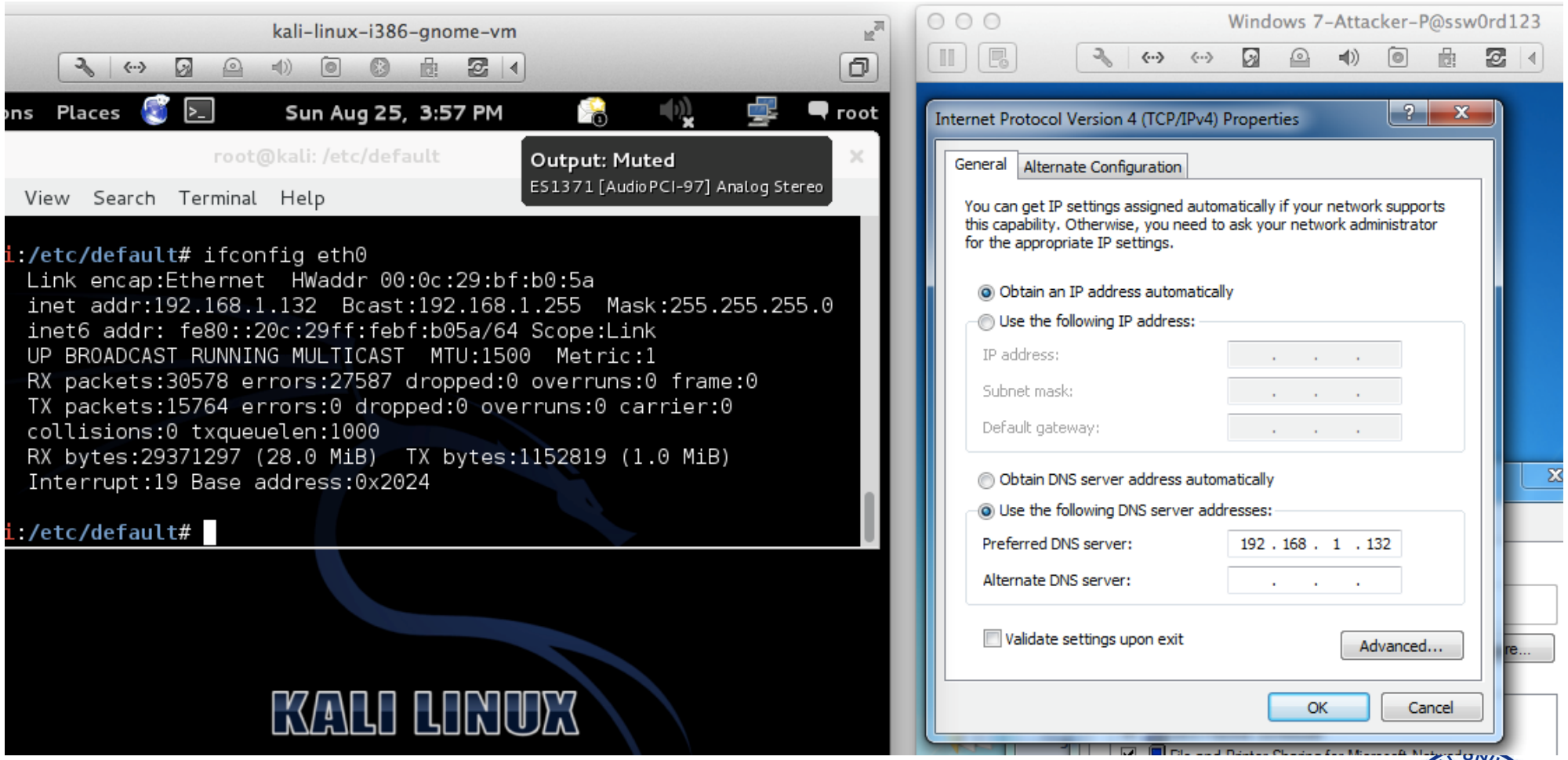


Follow TCP Stream

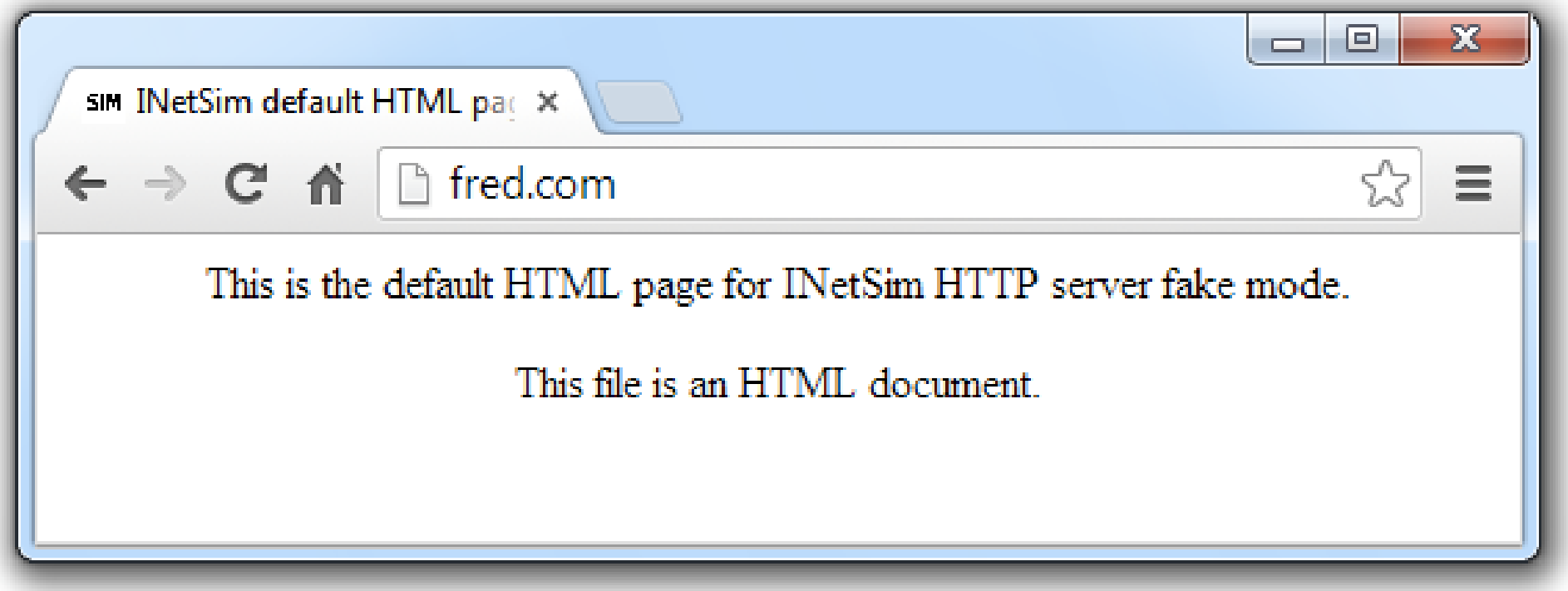
- Can save files from streams here too



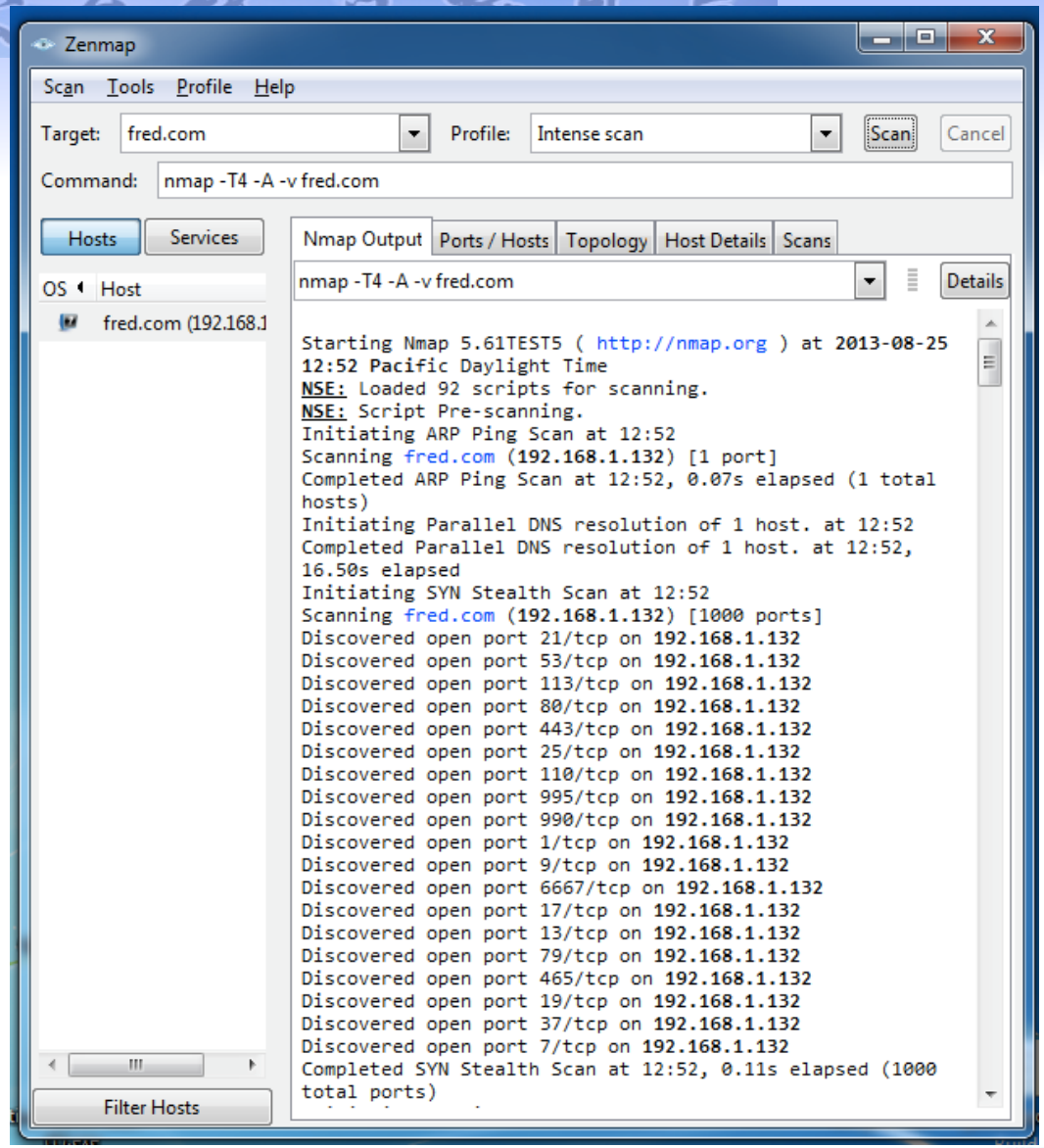
inetsim


kali-linux-i386-gnome-vm
Places
Sun Aug 25, 3:57 PM
root
root@kali: /etc/default
Output: Muted
ES1371 [AudioPCI-97] Analog Stereo
View Search Terminal Help
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

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

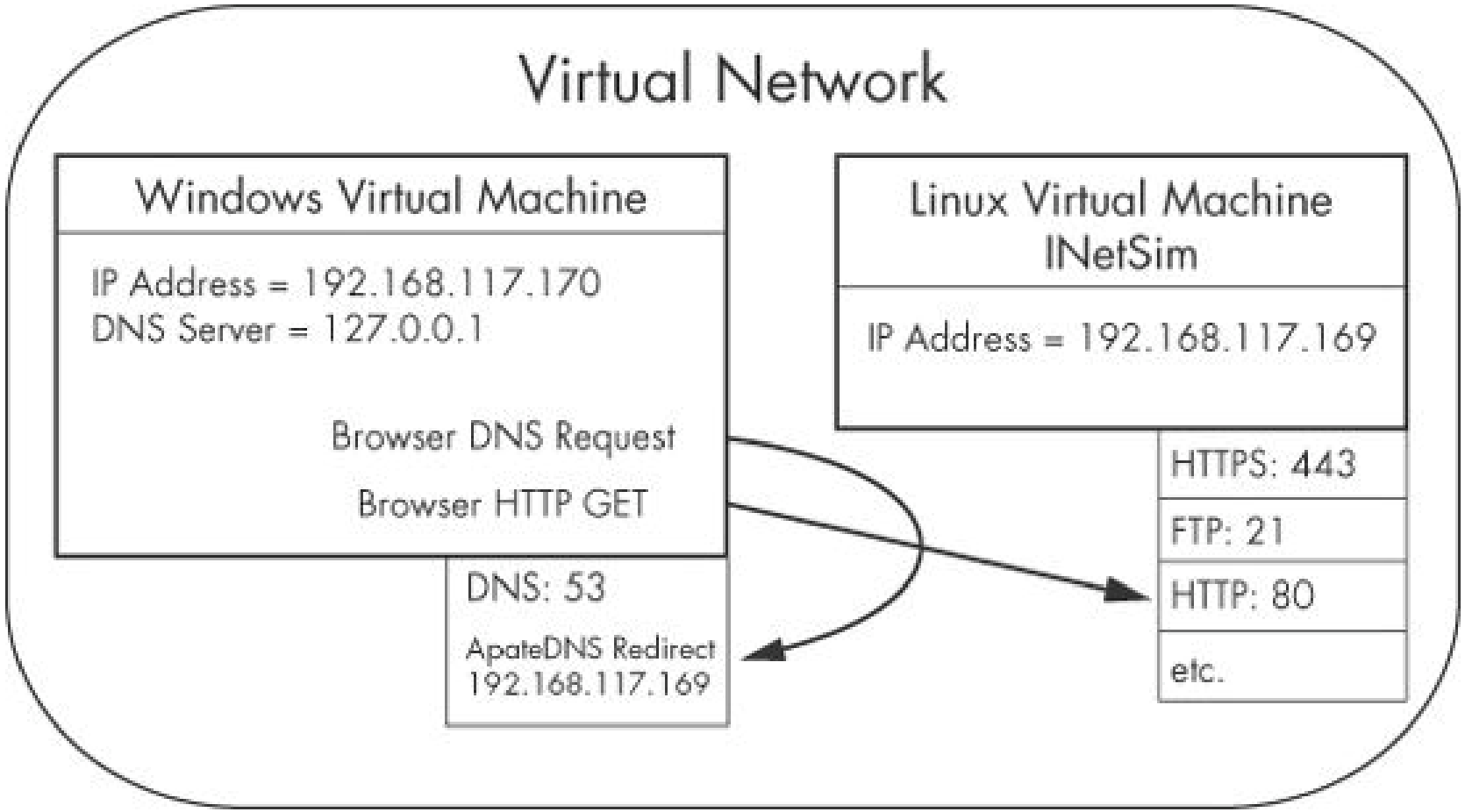


Figure 4-12. Example of a virtual network

Conclusion

- Assist and conform basic static analysis findings
- Most of tools are free and easy to use
- Next chapter is **Advanced Static Analysis** using reverse engineering.

Labs

Lab 3-1

Analyze the malware found in the file *Lab03-01.exe* using basic dynamic analysis tools.

Questions

1. What are this malware's imports and strings?
2. What are the malware's host-based indicators?
3. Are there any useful network-based signatures for this malware? If so, what are they?

Labs

Lab 3-2

Analyze the malware found in the file *Lab03-02.dll* using basic dynamic analysis tools.

Questions

1. How can you get this malware to install itself?
2. How would you get this malware to run after installation?
3. How can you find the process under which this malware is running?
4. Which filters could you set in order to use procmon to glean information?
5. What are the malware's host-based indicators?
6. Are there any useful network-based signatures for this malware?

Labs

Lab 3-3

Execute the malware found in the file *Lab03-03.exe* while monitoring it using basic dynamic analysis tools in a safe environment.

Questions

1. What do you notice when monitoring this malware with Process Explorer?
2. Can you identify any live memory modifications?
3. What are the malware's host-based indicators?
4. What is the purpose of this program?

Labs

Lab 3-4

Analyze the malware found in the file *Lab03-04.exe* using basic dynamic analysis tools. (This program is analyzed further in the Chapter 9 labs.)

Questions

1. What happens when you run this file?
2. What is causing the roadblock in dynamic analysis?
3. Are there other ways to run this program?

Malware Analysis

Chapter 3: Basic Dynamic Analysis

王志
zwang@nankai.edu.cn

updated on Mar. 8th 2021

College of Cyber Science
Nankai University
2021/2022