



南开大学

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月异

恶意代码分析与防治技术

## 第5章 基本动态分析

王志

zwang@nankai.edu.cn

updated on 2022-10-16

南开大学 网络空间安全学院

2022-2023学年



允公允能 日新月异

# Outline

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





南開大學

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月異



# 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





南開大學

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月異



# Sandboxes: The Quick-and-Dirty Approach



# Sandbox

允公允能 日新月异

- **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





## Table of Contents

<b>Analysis Summary</b>	<b>3</b>
Analysis Summary	3
Digital Behavior Traits	3
<b>File Activity</b>	<b>4</b>
Stored Modified Files	4
<b>Created Mutexes</b>	<b>5</b>
Created Mutexes	5
<b>Registry Activity</b>	<b>6</b>
Set Values	6
<b>Network Activity</b>	<b>7</b>
Network Events	7
Network Traffic	8
DNS Requests	9
<b>VirusTotal Results</b>	<b>10</b>



允公允能 日新月异

# Sandboxes

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







南開大學

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月異

A light blue world map is centered in the background of the slide.

Launching DLLs



# Launching DLLs

允公允能 日新月异

- 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, PView, or PE Explorer.





# Launching DLLs

允公允能 日新月异

- 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





允公允能 日新月异

# Launching DLL

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





南開大學

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月異

# Process Monitor



允公允能 日新月异

# 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



南開大學  
Nankai University





# Process Monitor

允公允能 日新月异

- 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 - Sysinternals: www.sysinternals.com

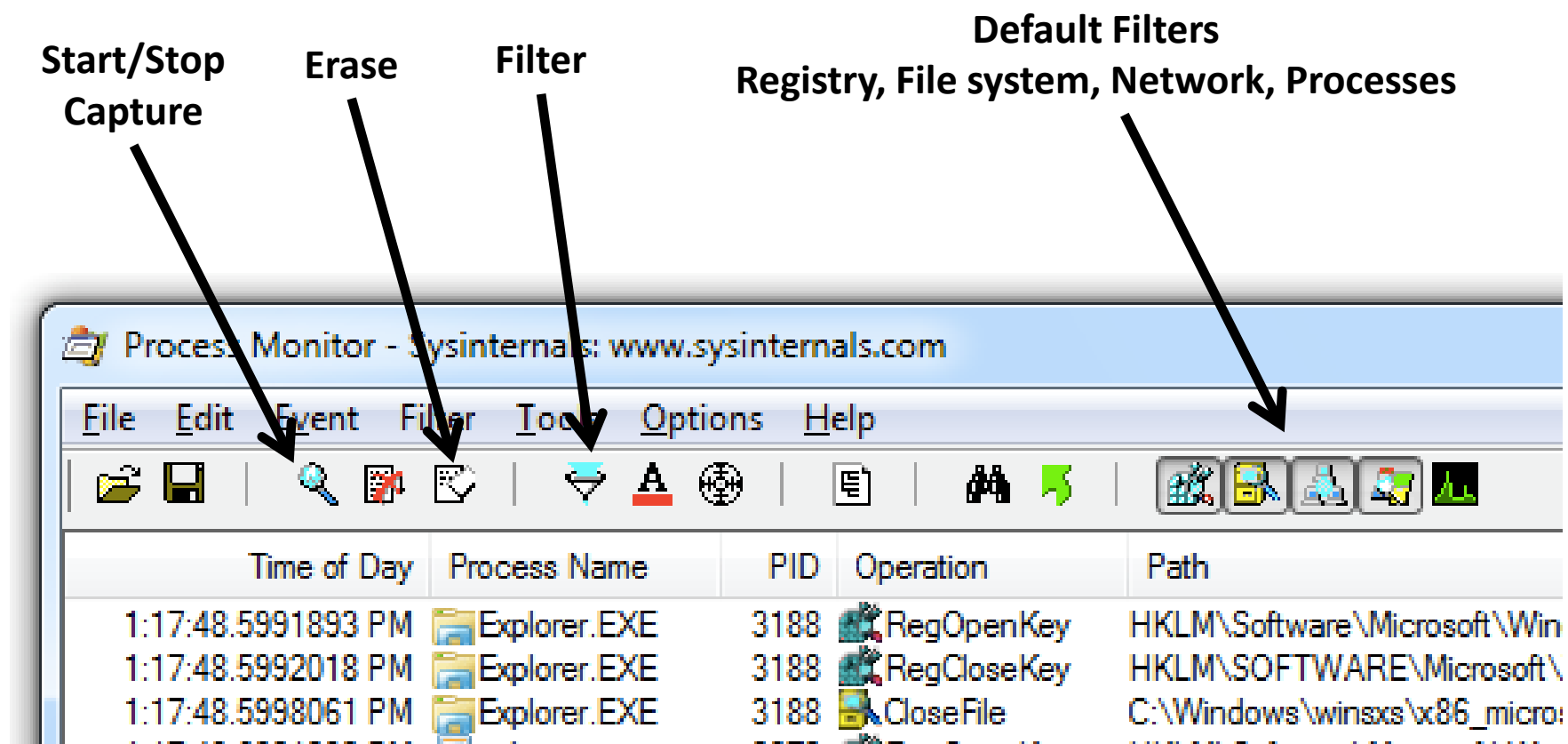
File Edit Event Filter Tools Options Help

Time of Day	Process Name	PID	Operation	Path	Result	Detail
1:17:48.5991893 PM	Explorer.EXE	3188	RegOpenKey	HKLM\Software\Microsoft\Windows\CurrentVersion\...	SUCCESS	Desired Access: Query Value
1:17:48.5992018 PM	Explorer.EXE	3188	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersi...	SUCCESS	
1:17:48.5998061 PM	Explorer.EXE	3188	CloseFile	C:\Windows\winsxs\x86_microsoft.windows.common-...	SUCCESS	
1:17:48.6001092 PM	calc.exe	2072	RegOpenKey	HKLM\Software\Microsoft\Windows\Windows Error ...	SUCCESS	Desired Access: Query Value
1:17:48.6001273 PM	calc.exe	2072	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\Windows Err...	SUCCESS	Type: REG_DWORD, Length: 4, ...
1:17:48.6001350 PM	calc.exe	2072	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows\Windows Err...	SUCCESS	
1:17:48.6001722 PM	calc.exe	2072	ReadFile	C:\Windows\System32\calc.exe	SUCCESS	Offset: 103,424, Length: 32,768, I...
1:17:48.6011060 PM	calc.exe	2072	CreateFile	C:\Windows\System32\WindowsCodecs.dll	SUCCESS	Desired Access: Read Attributes, ...
1:17:48.6011278 PM	calc.exe	2072	QueryBasicInfor...	C:\Windows\System32\WindowsCodecs.dll	SUCCESS	CreationTime: 7/13/2009 4:29:14 ...
1:17:48.6011337 PM	calc.exe	2072	CloseFile	C:\Windows\System32\WindowsCodecs.dll	SUCCESS	
1:17:48.6012132 PM	calc.exe	2072	CreateFile	C:\Windows\System32\WindowsCodecs.dll	SUCCESS	Desired Access: Read Data/List ...
1:17:48.6012344 PM	calc.exe	2072	CreateFileMapp...	C:\Windows\System32\WindowsCodecs.dll	FILE LOCKED WI...	SyncType: SyncTypeCreateSecti...
1:17:48.6012901 PM	calc.exe	2072	CreateFileMapp...	C:\Windows\System32\WindowsCodecs.dll	SUCCESS	SyncType: SyncTypeOther
1:17:48.6013372 PM	calc.exe	2072	Load Image	C:\Windows\System32\WindowsCodecs.dll	SUCCESS	Image Base: 0x73aa0000, Image ...
1:17:48.6013796 PM	calc.exe	2072	CloseFile	C:\Windows\System32\WindowsCodecs.dll	SUCCESS	
1:17:48.6015378 PM	calc.exe	2072	RegOpenKey	HKCU\Software\Classes	SUCCESS	Desired Access: Maximum Allowe...
1:17:48.6015591 PM	calc.exe	2072	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
1:17:48.6015697 PM	calc.exe	2072	RegOpenKey	HKCU\Software\Classes\CLSID\{FAE3D380-FEA4-4...	NAME NOT FOUND	Desired Access: Read
1:17:48.6015797 PM	calc.exe	2072	RegOpenKey	HKCR\CLSID\{FAE3D380-FEA4-4623-8C75-C6B6111...	SUCCESS	Desired Access: Read
1:17:48.6015937 PM	calc.exe	2072	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
1:17:48.6016002 PM	calc.exe	2072	RegOpenKey	HKCU\Software\Classes\CLSID\{FAE3D380-FEA4-4...	NAME NOT FOUND	Desired Access: Read
1:17:48.6016130 PM	calc.exe	2072	RegOpenKey	HKCR\CLSID\{FAE3D380-FEA4-4623-8C75-C6B6111...	NAME NOT FOUND	Desired Access: Read

Showing 128,723 of 253,268 events (50%)      Backed by virtual memory



# Process Monitor Toolbar





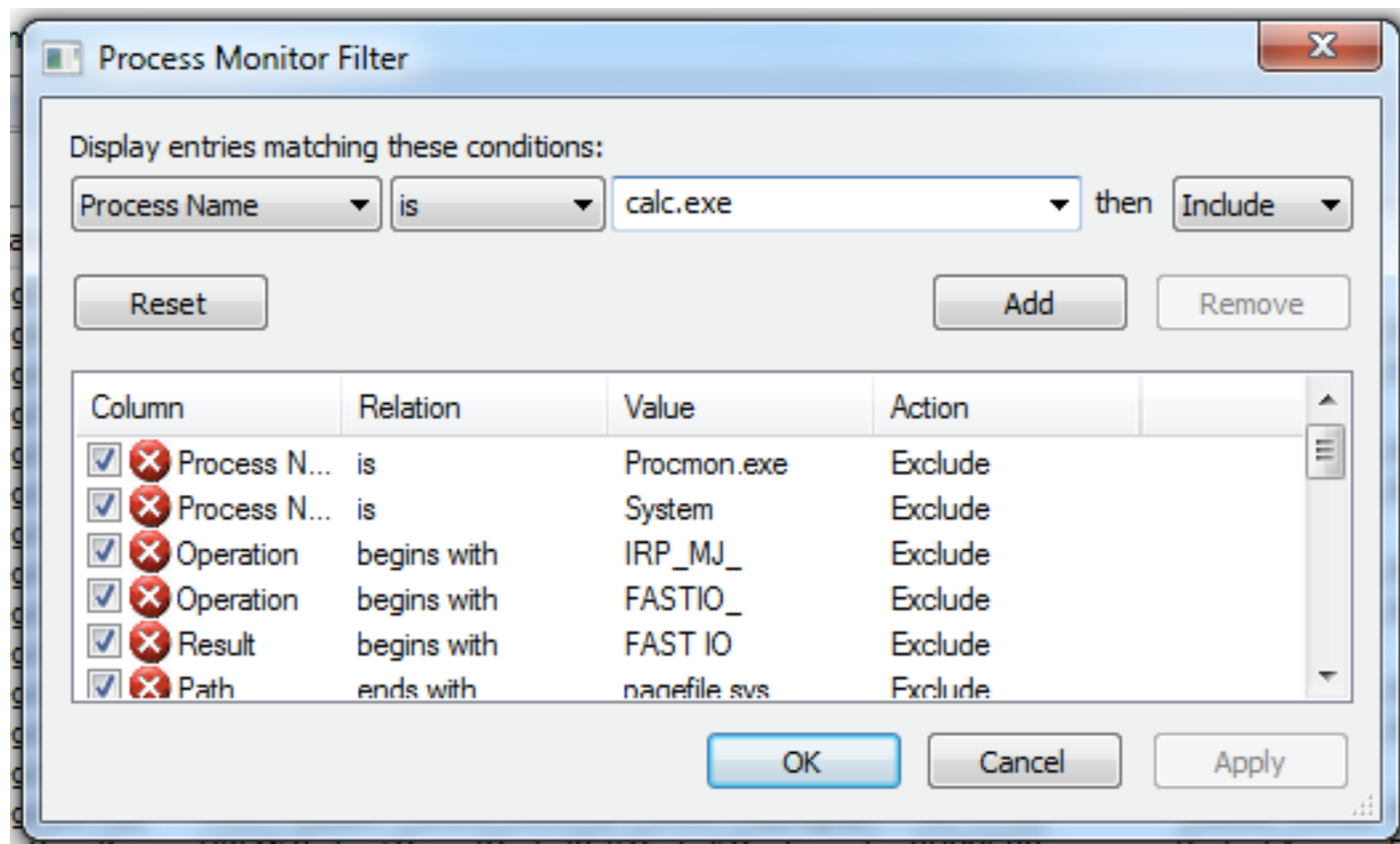
# Filtering with Exclude

- 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





南開大學

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月異

# Process Explorer





# Process Explorer

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



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%





允公允能 日新月异

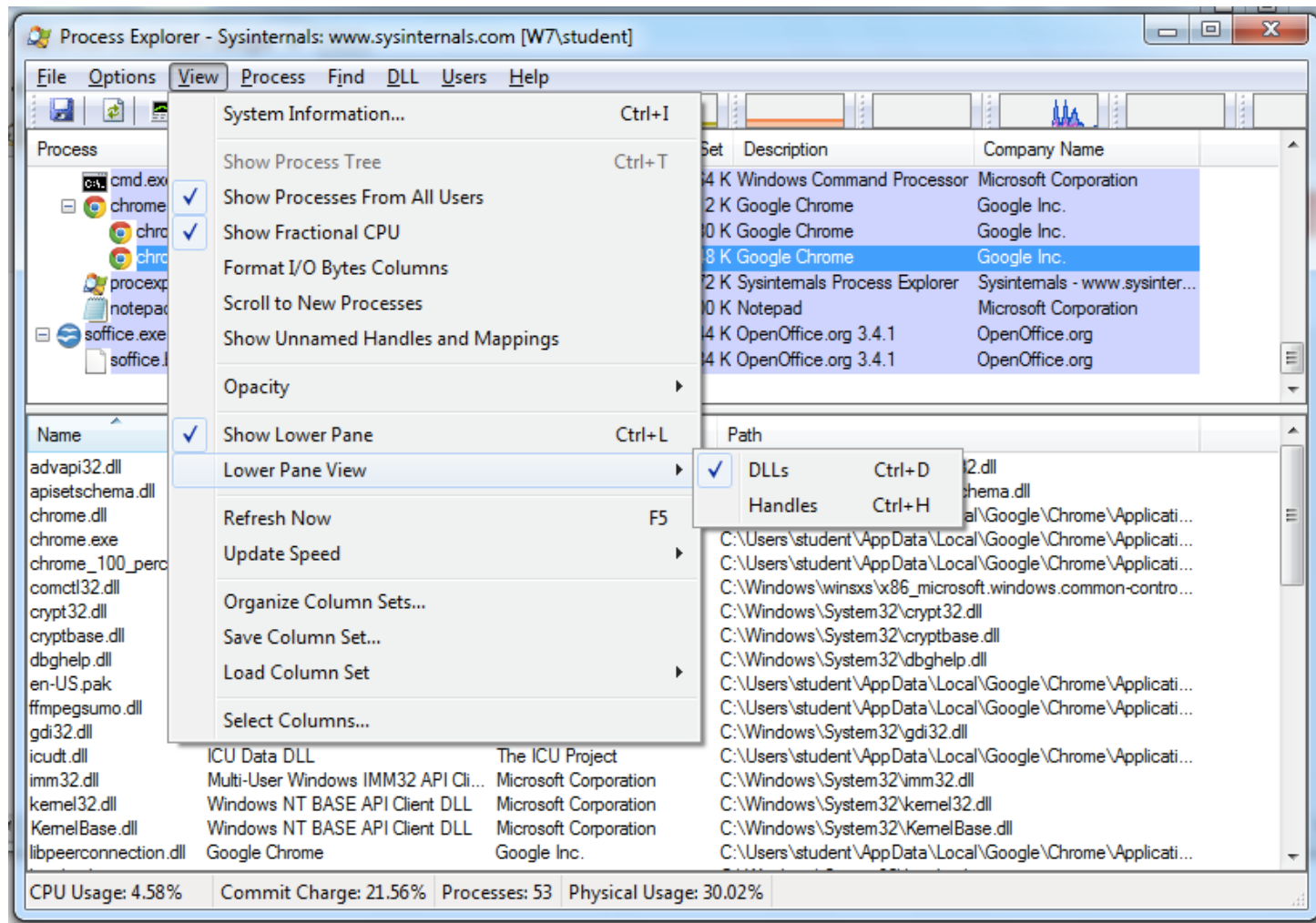
# Coloring

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



# DLL Mode

允公允能 日新月异





允公允能 日新月异

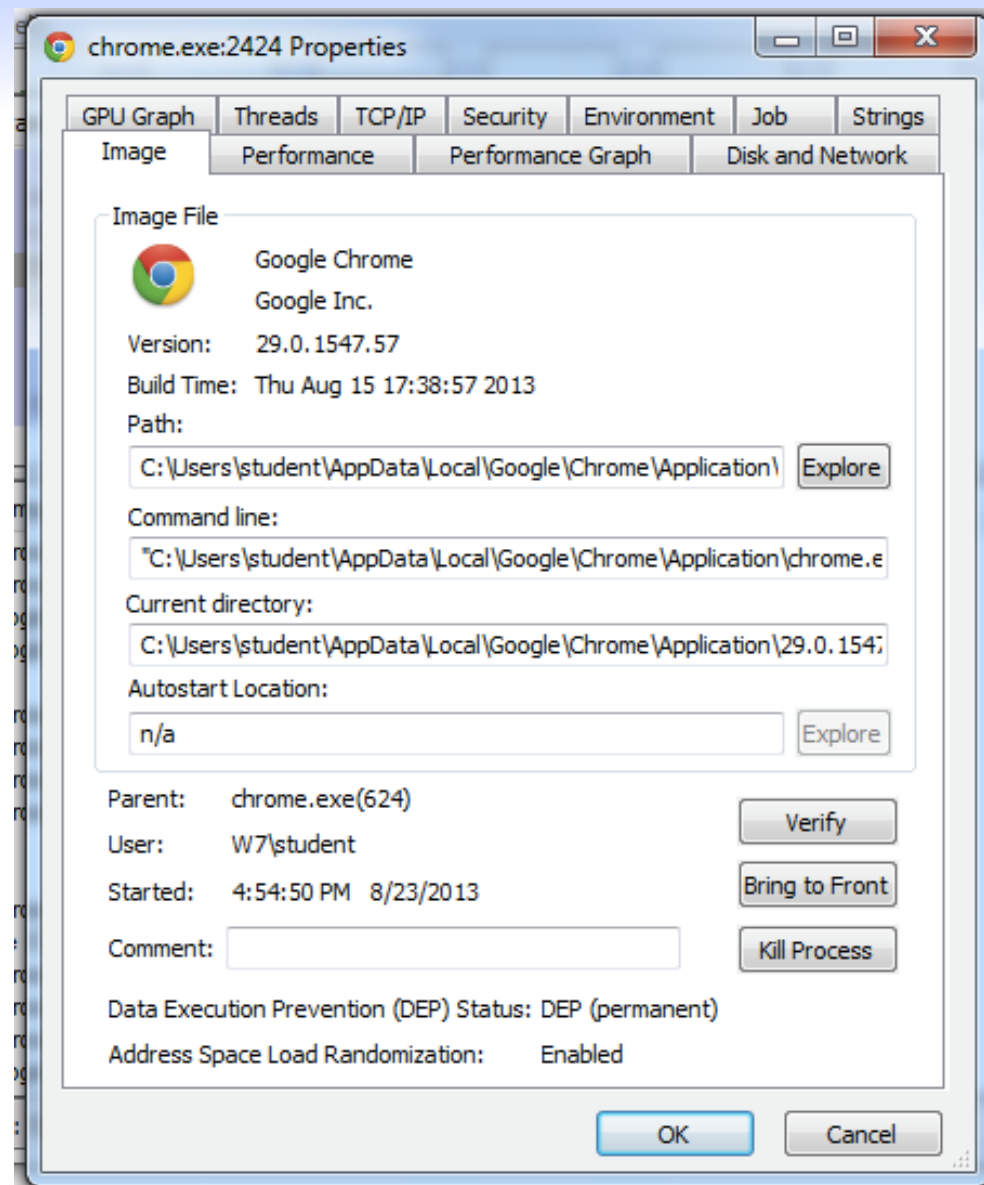
# Handle Mode

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

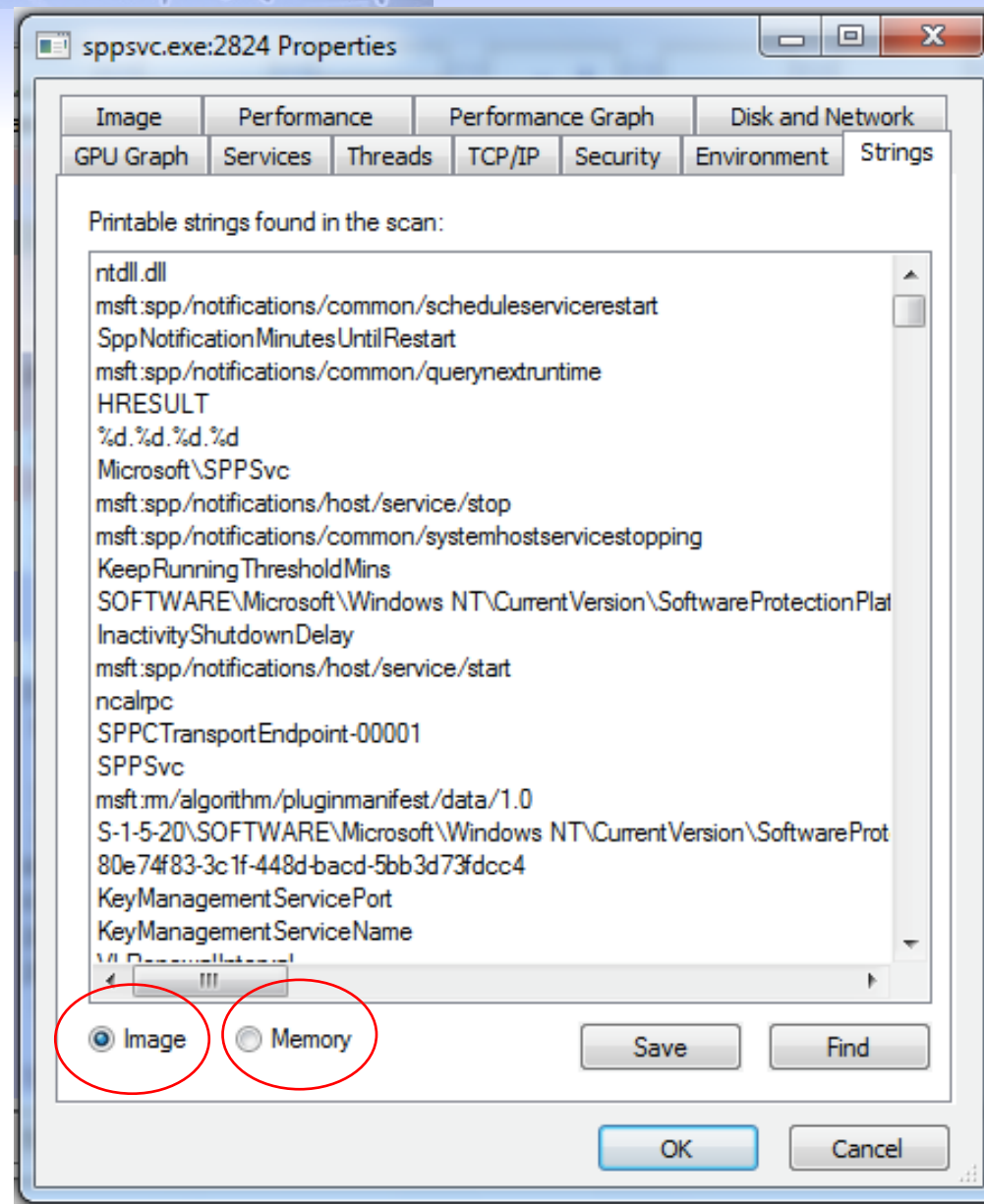
- Shows **DEP** and **ASLR** status
- Verify button checks the disk file's Windows signature
  - But not the RAM image, so it won't detect **process replacement**





# 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





南開大學

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月異

Regshot



# Regshot

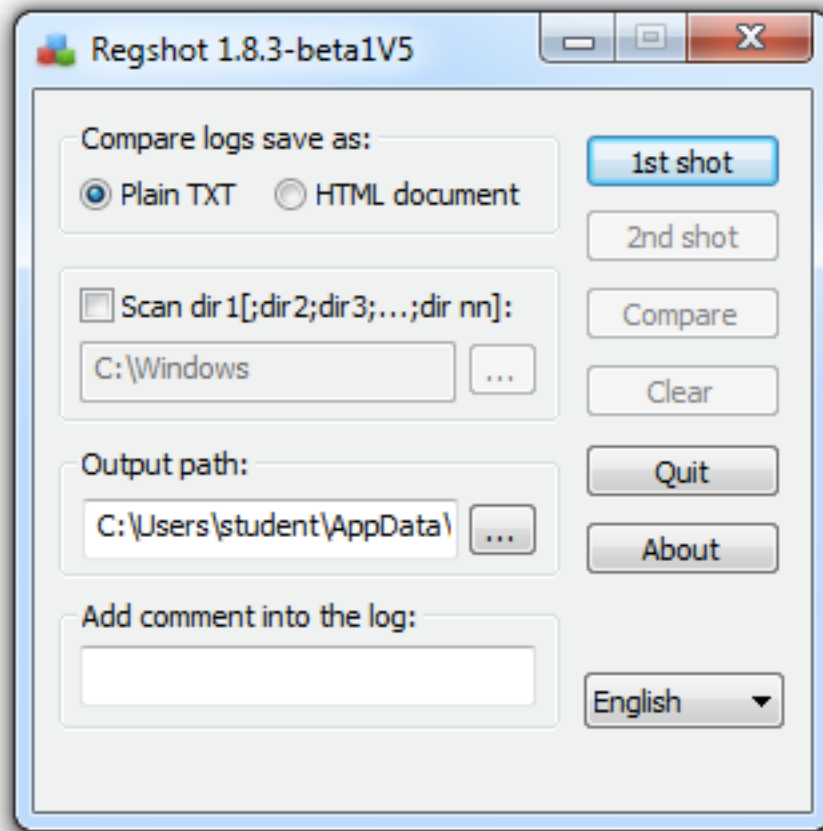
允公允能 日新月异

- An open source registry comparison tool
  - Take registry **snapshots**
  - Compare two registry snapshots





# 允公允能 日新月异





南開大學

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月異

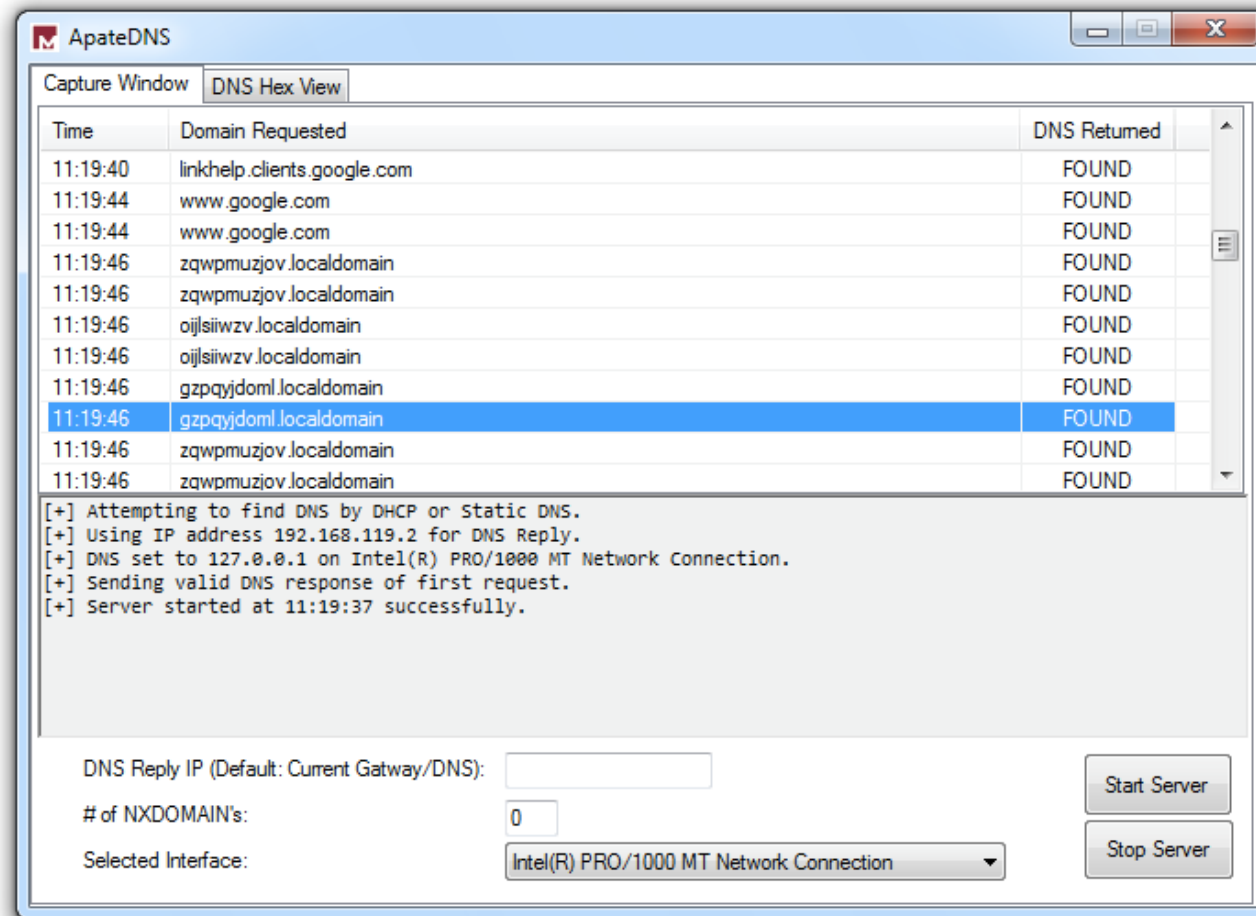
# Faking a Network



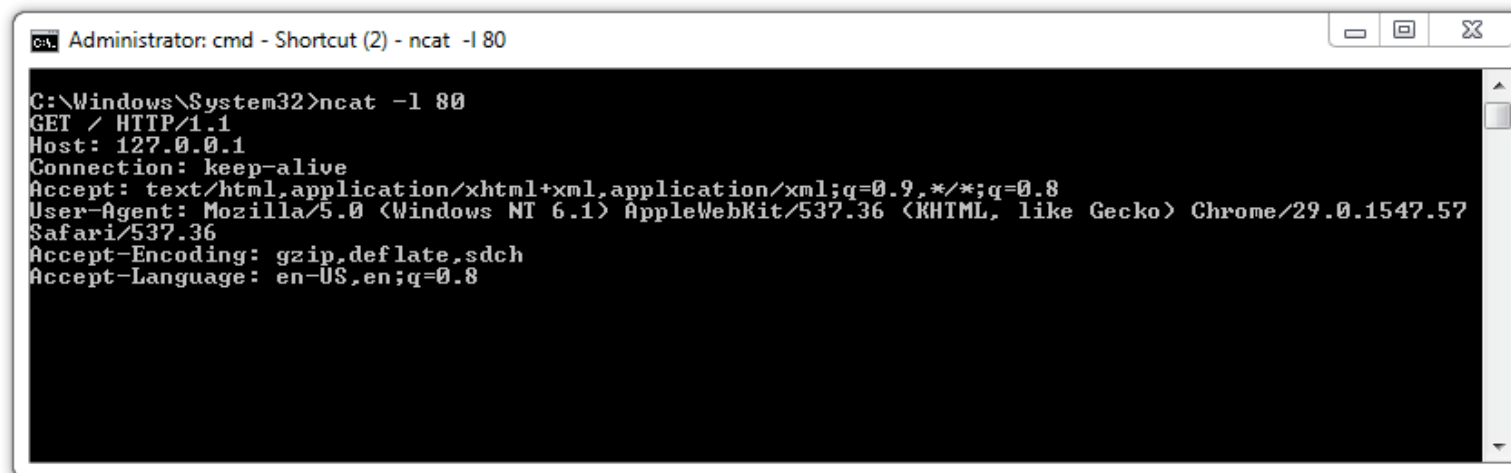
# Faking a Network

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

# Using ApatDNS to Redirect DNS Resolutions

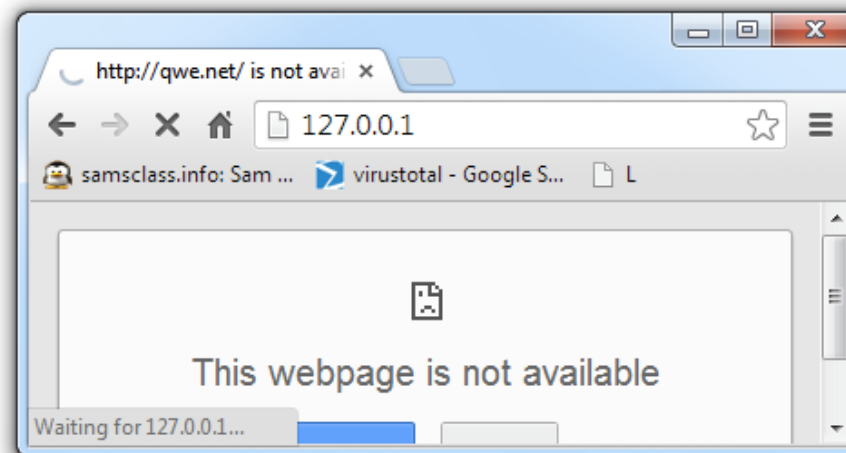


# Monitoring with Ncat (included with Nmap)



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
```





# Wireshark

允公允能 日新月异

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



允公允能 日新月异

# Packet Sniffing with Wireshark

The image displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. The main display area is divided into three panes:

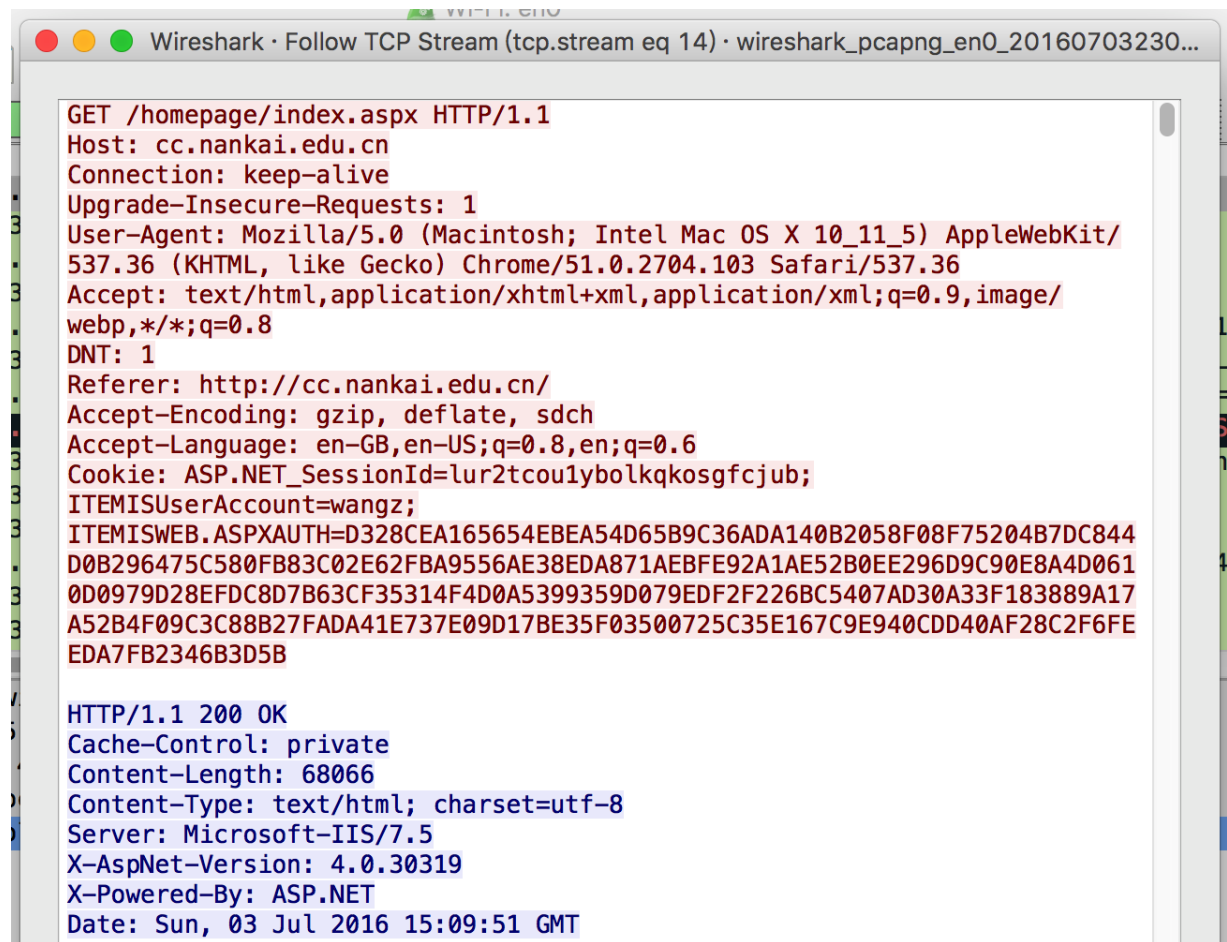
- Filter:** Set to 'http'.
- Packet List:** A table of captured packets. The first 13 packets are highlighted in green, indicating they are HTTP. The table columns are No., Time, Source, Destination, Protocol, and Info.
- Packet Details:** Shows the selected packet (No. 48) with its structure: Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol.
- Packet Bytes:** A hex dump of the selected packet's raw data.

In the background, a web browser window is visible, showing the 'samsclass.info' website. The browser's address bar displays 'samsclass.info', and the page content includes a search bar and navigation links. The browser window also shows the name 'Sam Bowne' in the title bar.



# Follow TCP Stream

- Can save files from streams here too



```
Wireshark · Follow TCP Stream (tcp.stream eq 14) · wireshark_pcapng_en0_20160703230...

GET /homepage/index.aspx HTTP/1.1
Host: cc.nankai.edu.cn
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
DNT: 1
Referer: http://cc.nankai.edu.cn/
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-GB,en-US;q=0.8,en;q=0.6
Cookie: ASP.NET_SessionId=lur2tcoulybolqkqosgfcjub;
ITEMISUserAccount=wangz;
ITEMISWEB.ASPXAUTH=D328CEA165654EBEA54D65B9C36ADA140B2058F08F75204B7DC844D0B296475C580FB83C02E62FBA9556AE38EDA871AEBFE92A1AE52B0EE296D9C90E8A4D0610D0979D28EFD8D7B63CF35314F4D0A5399359D079EDF2F226BC5407AD30A33F183889A17A52B4F09C3C88B27FADA41E737E09D17BE35F03500725C35E167C9E940CDD40AF28C2F6FEEDA7FB2346B3D5B

HTTP/1.1 200 OK
Cache-Control: private
Content-Length: 68066
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/7.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Sun, 03 Jul 2016 15:09:51 GMT
```





# inetsim

允公允能 日新月异

```
kali-linux-i386-gnome-vm
root@kali: /etc/default
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

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: . . .

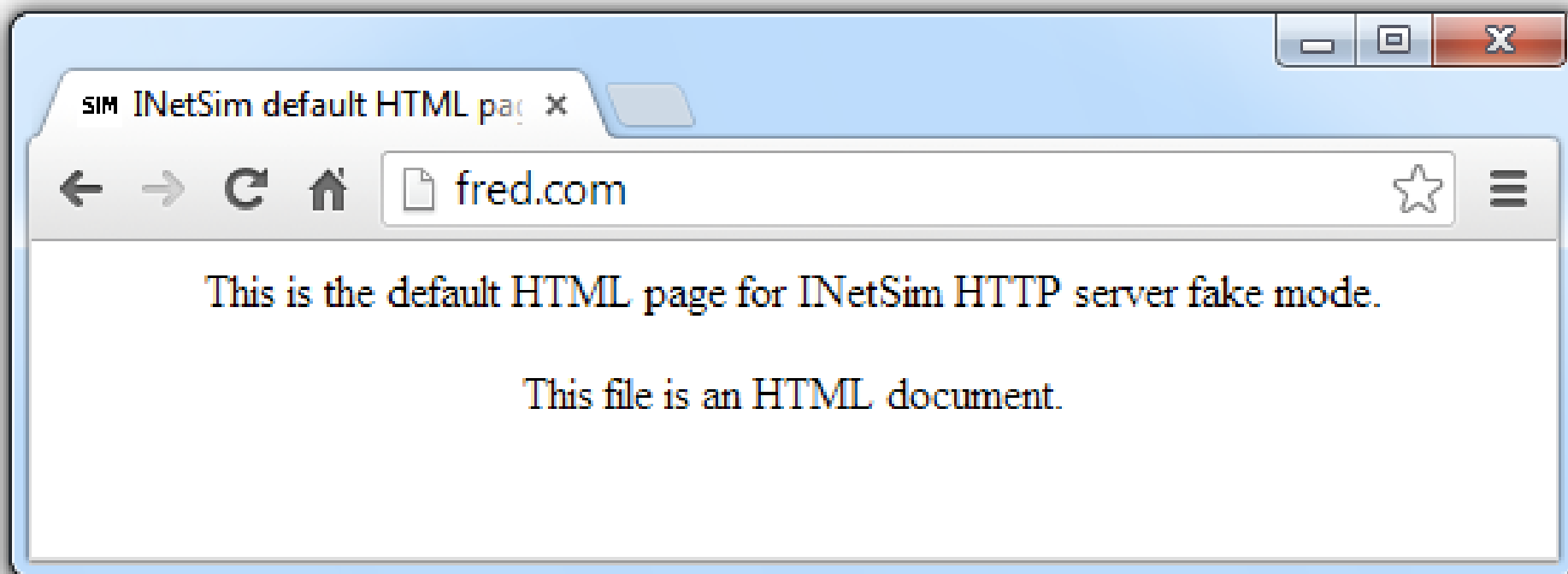
☐ Validate settings upon exit

Advanced...

OK Cancel



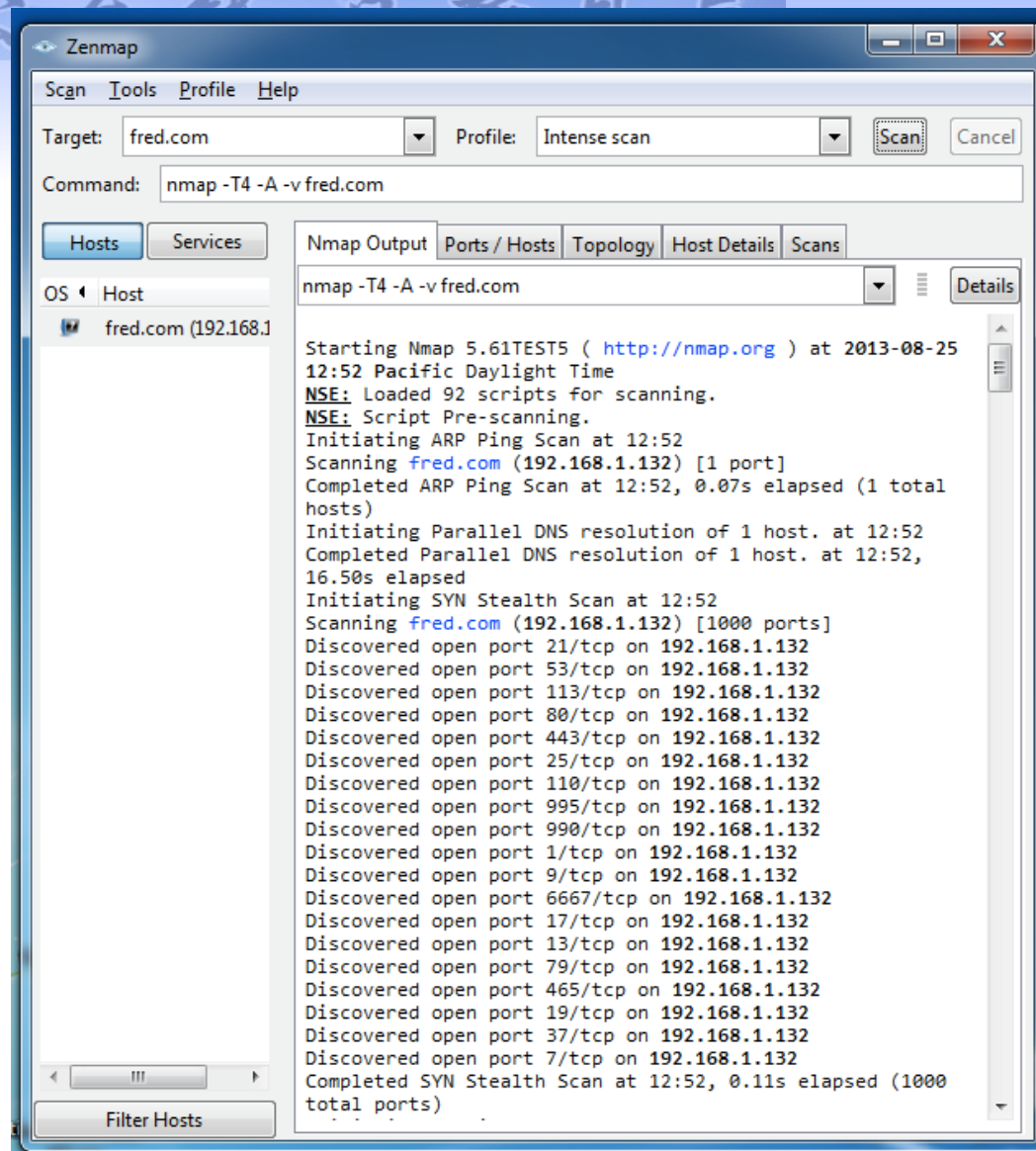
# INetSim Fools a Browser



# INetSim

## Fools

## Nmap





允公允能 日新月异

# Basic Dynamic Tools in Practice



南開大學  
Nankai University

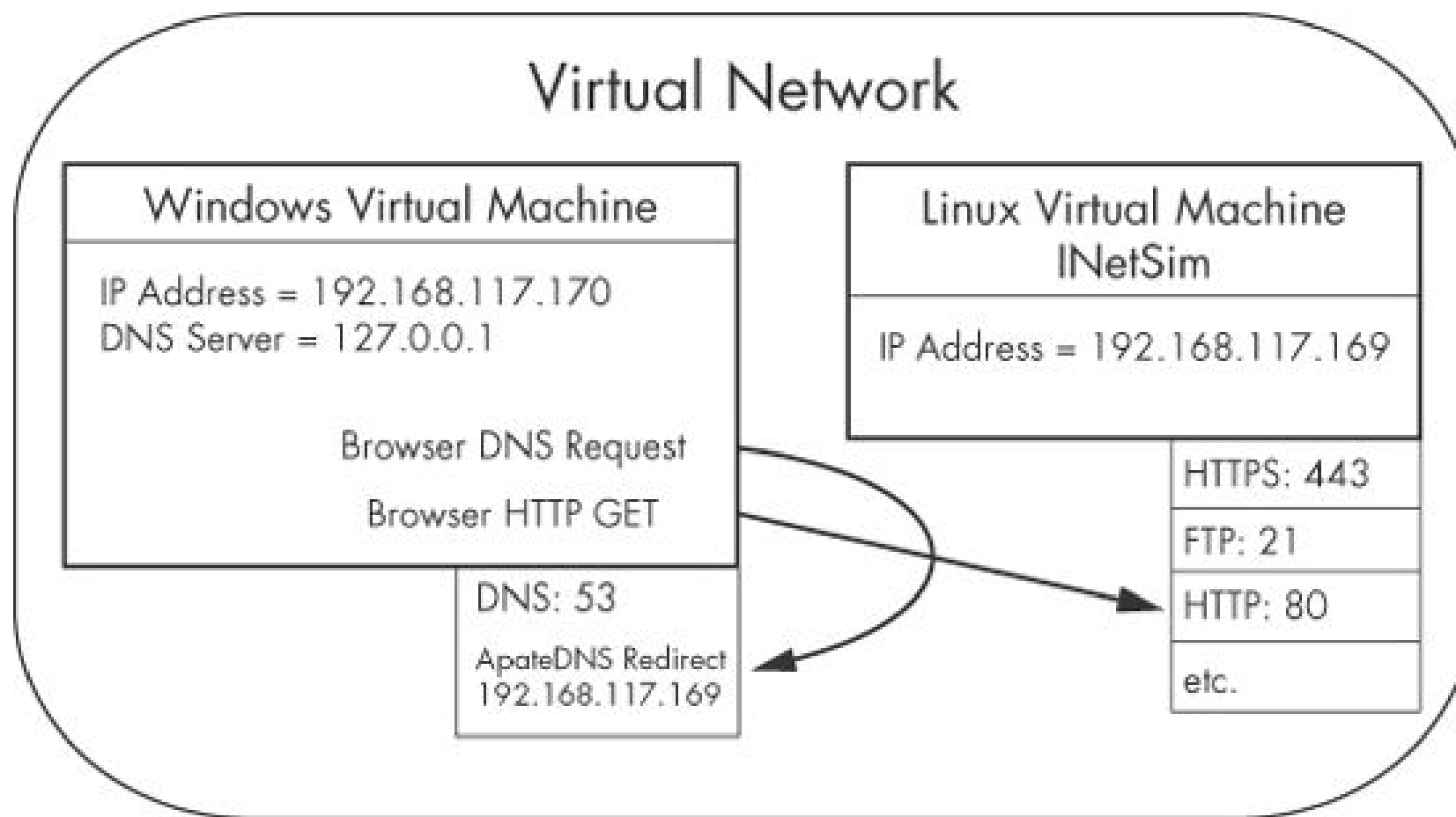


允公允能 日新月异

# 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*





允公允能 日新月异

# 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

允公允能 日新月异

## 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?



## 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

允公允能 日新月异

## 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

允公允能 日新月异

## 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?





南开大学

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月异

恶意代码分析与防治技术

## 第5章 基本动态分析

王志

zwang@nankai.edu.cn

updated on 2022-10-16

南开大学 网络空间安全学院

2022-2023学年