

Practical Malware Analysis

Chapter 3: Basic Dynamic Analysis

Akbar Namin

Texas Tech University

Fall 2021

Reference:

Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software 1st Edition
by [Michael Sikorski](#) (Author), [Andrew Honig](#) (Author)

Dynamic analysis

- Dynamic analysis is any examination performed after executing malware
- 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

- All-in-one software for basic dynamic analysis
- Virtualized environment that simulates network services
- Examples:
 - Norman Sandbox
 - GFI Sandbox
 - Anubis
 - Joe Sandbox
 - ThreatExpert
 - BitBlaze Comodo Instant Malware Analysis
- They are expensive but easy to use
- They produce a nice PDF report of results

Running Malware

- Launching DLLs

- EXE files can be run directly, but DLLs can't
- Use Rundll32.exe (included in Windows) rundll32.exe DLLname, Export arguments
- The Export value is one of the exported functions you found in Dependency Walker, PView, or PE Explorer.

Launching DLLs

- Example

➤ rip.dll has these exports: Install and Uninstall

```
C:\>rundll32.exe rip.dll, Install
```

- Some functions use ordinal values instead of names, like

```
C:\>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, or procmon, is an advanced monitoring tool for Windows
- 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

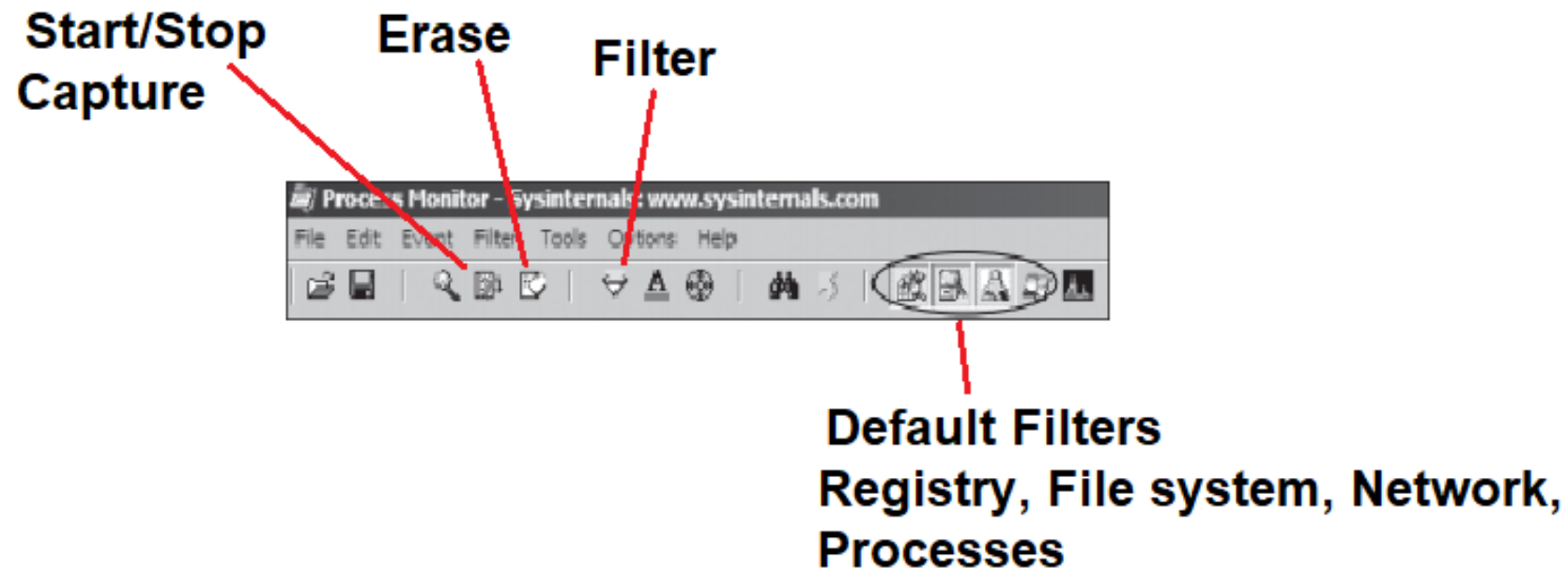
The Procmon Display

- Procmon displays configurable columns containing information about:
 - individual events, including the event's sequence number, timestamp, name of the process causing the event, event operation, path used by the event,

Seq.	Time	Process Name	Operation	Path	Result	Detail
200	1:55:31	mm32.exe	CloseFile	Z:\Malware\mw2mmqr32.dll	SUCCESS	
201	1:55:31	mm32.exe	ReadFile	Z:\Malware\mw2mmqr32.dll	SUCCESS	Offset: 11,776, Length: 1,024, I/O Flag
202	1:55:31	mm32.exe	ReadFile	Z:\Malware\mw2mmqr32.dll	SUCCESS	Offset: 12,800, Length: 32,768, I/O Flag
203	1:55:31	mm32.exe	ReadFile	Z:\Malware\mw2mmqr32.dll	SUCCESS	Offset: 1,024, Length: 9,216, I/O Flag
204	1:55:31	mm32.exe	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Exec	NAME NOT	Desired Access: Read
205	1:55:31	mm32.exe	ReadFile	Z:\Malware\mw2mmqr32.dll	SUCCESS	Offset: 45,568, Length: 25,088, I/O Flag
206	1:55:31	mm32.exe	QueryOpen	Z:\Malware\imagehlp.dll	NAME NOT	
207	1:55:31	mm32.exe	QueryOpen	C:\WINDOWS\system32\imagehlp.dll	SUCCESS	CreationTime: 2/28/2006 8:00:00 AM,
208	1:55:31	mm32.exe	CreateFile	C:\WINDOWS\system32\imagehlp.dll	SUCCESS	Desired Access: Execute/Traverse, S
209	1:55:31	mm32.exe	CloseFile	C:\WINDOWS\system32\imagehlp.dll	SUCCESS	
210	1:55:31	mm32.exe	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Exec	NAME NOT	Desired Access: Read
211	1:55:31	mm32.exe	ReadFile	Z:\Malware\mw2mmqr32.dll	SUCCESS	Offset: 10,240, Length: 1,536, I/O Flag
212	1:55:31	mm32.exe	CreateFile	C:\Documents and Settings\All Users\Application Data\mw2mmqr.txt	SUCCESS	Desired Access: Generic Write, Read
213	1:55:31	mm32.exe	ReadFile	C:\\$Directory	SUCCESS	Offset: 12,288, Length: 4,096, I/O Flag
214	1:55:31	mm32.exe	CreateFile	Z:\Malware\mm32.exe	SUCCESS	Desired Access: Generic Read, Disc
215	1:55:31	mm32.exe	ReadFile	Z:\Malware\mm32.exe	SUCCESS	Offset: 0, Length: 64

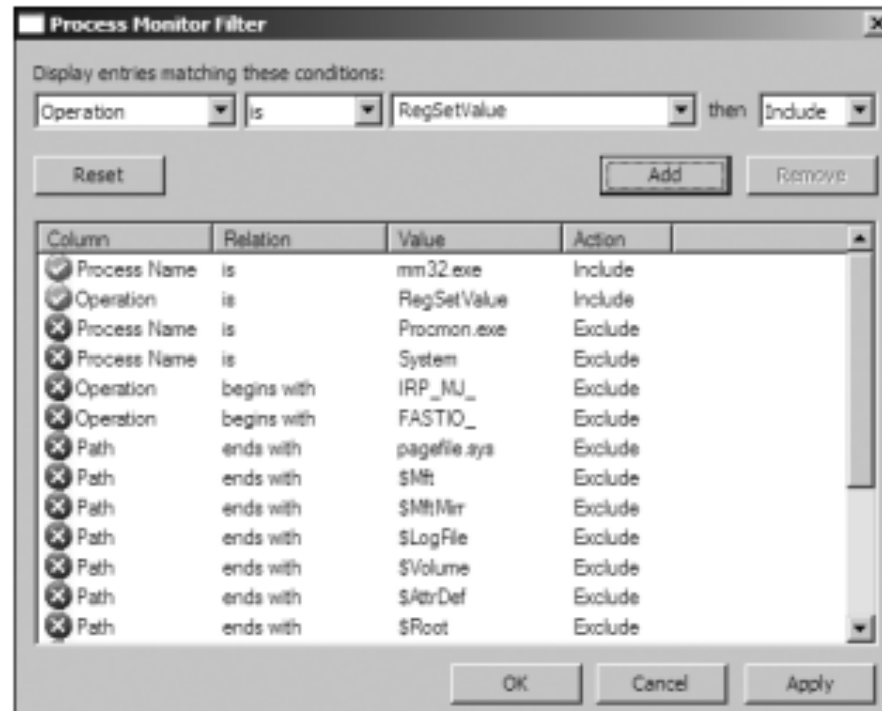
Procmon mm32.exe example

Process Monitor Toolbar



Filtering with Exclude and Include

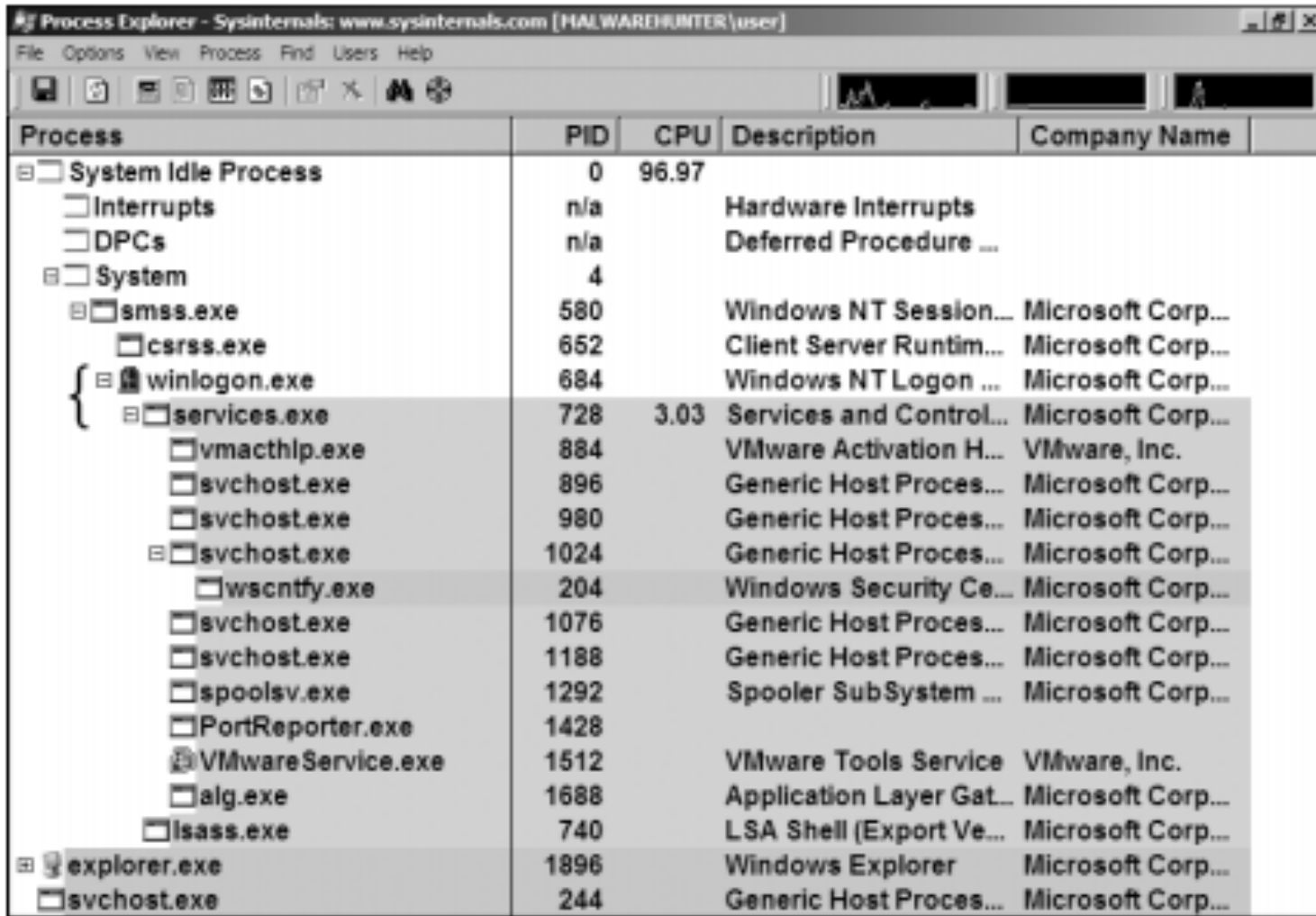
- One technique: hide normal activity before launching malware
- Right-click each Process Name and click Exclude
- Filtering with Include
 - Most useful filters: Process Name, Operation, and Detail



Seq...	Time...	Process Name	Operation	Path	Result
0	4:18:5...	mm32.exe	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RING\Seed	SUCCESS
1	4:18:5...	mm32.exe	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\C...	SUCCESS
2	4:18:5...	mm32.exe	RegSetValue	HKLM\SOFTWARE\SAXP32\F4KL\Options	SUCCESS
3	4:18:5...	mm32.exe	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Sys32\2Contoller	SUCCESS
4	4:18:5...	mm32.exe	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RING\Seed	SUCCESS
5	4:18:5...	mm32.exe	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RING\Seed	SUCCESS
6	4:18:5...	mm32.exe	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RING\Seed	SUCCESS
7	4:18:5...	mm32.exe	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RING\Seed	SUCCESS
8	4:18:5...	mm32.exe	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RING\Seed	SUCCESS
9	4:18:5...	mm32.exe	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RING\Seed	SUCCESS
10	4:18:5...	mm32.exe	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RING\Seed	SUCCESS

Setting a procmon filter

Viewing Processes with Process Explorer



Process Explorer - Sysinternals: www.sysinternals.com [HALWAREHUNTER\user]

File Options View Process Find Users Help

Process	PID	CPU	Description	Company Name
System Idle Process	0	96.97		
Interrupts	n/a		Hardware Interrupts	
DPCs	n/a		Deferred Procedure ...	
System	4			
smss.exe	580		Windows NT Session...	Microsoft Corp...
csrss.exe	652		Client Server Runtime...	Microsoft Corp...
winlogon.exe	684		Windows NT Logon ...	Microsoft Corp...
services.exe	728	3.03	Services and Control...	Microsoft Corp...
vmacthlp.exe	884		VMware Activation H...	VMware, Inc.
svchost.exe	896		Generic Host Proces...	Microsoft Corp...
svchost.exe	980		Generic Host Proces...	Microsoft Corp...
svchost.exe	1024		Generic Host Proces...	Microsoft Corp...
wscntfy.exe	204		Windows Security Ce...	Microsoft Corp...
svchost.exe	1076		Generic Host Proces...	Microsoft Corp...
svchost.exe	1188		Generic Host Proces...	Microsoft Corp...
spoolsv.exe	1292		Spooler SubSystem ...	Microsoft Corp...
PortReporter.exe	1428			
VMwareService.exe	1512		VMware Tools Service	VMware, Inc.
alg.exe	1688		Application Layer Gat...	Microsoft Corp...
lsass.exe	740		LSA Shell (Export Ve...	Microsoft Corp...
explorer.exe	1896		Windows Explorer	Microsoft Corp...
svchost.exe	244		Generic Host Proces...	Microsoft Corp...

Process Explorer examining svchost.exe malware

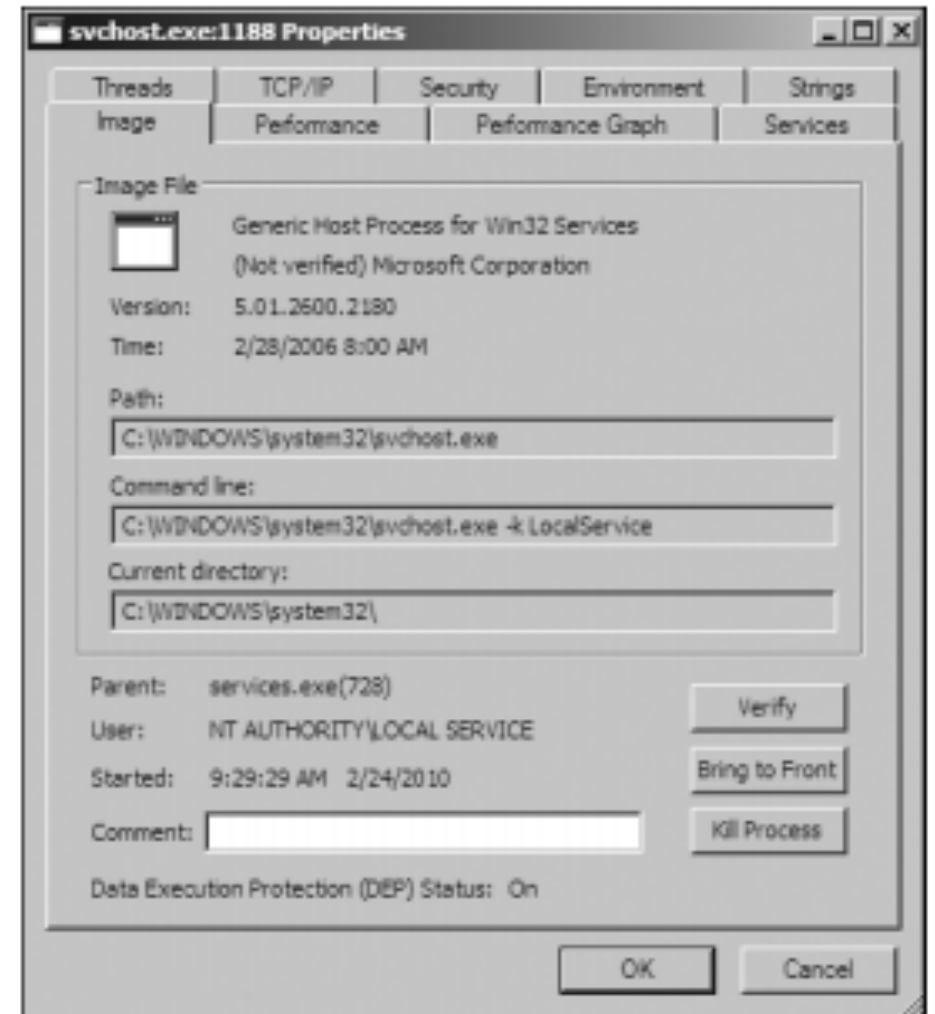
Coloring

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

DLL Mode

- Process Explorer can display quite a bit of information for each process. For example
 - click a process to see all DLLs it loaded into memory.
 - You can change the DLL display window to the Handles window, which shows all handles held by the process, including file handles, mutexes, events, and so on.

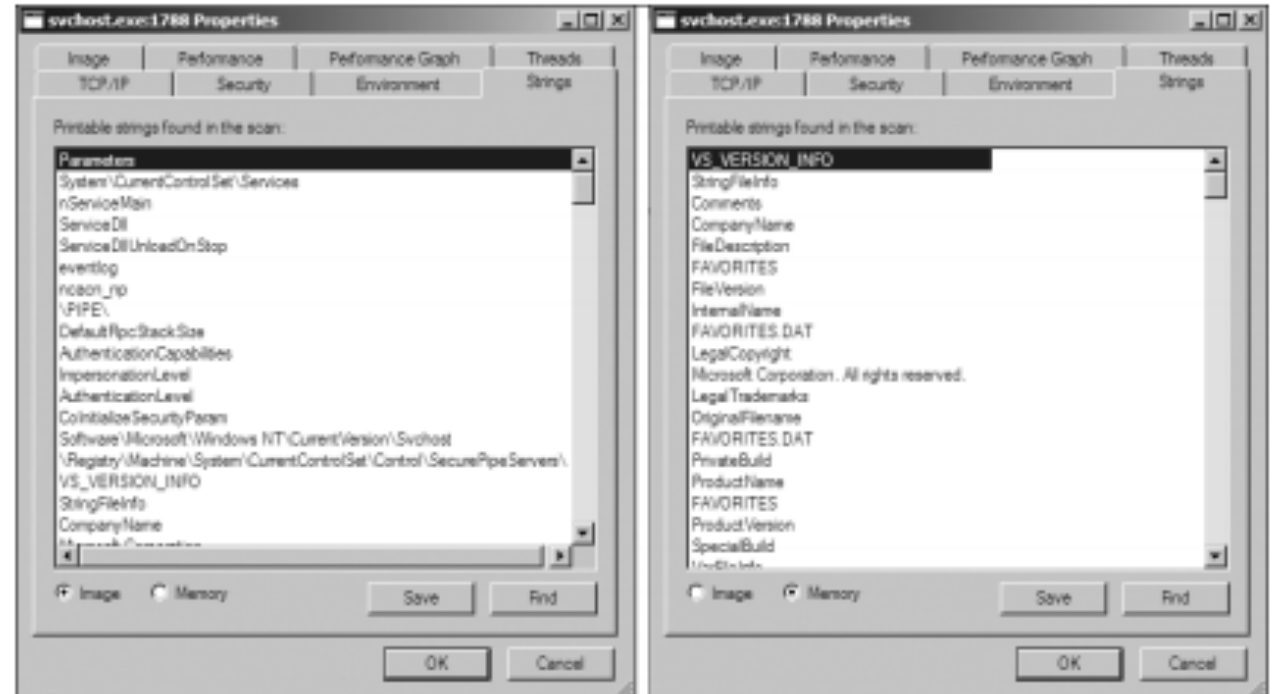
- Shows DEP (Data Execution Prevention) and ASLR (Address Space Layout Randomization) status
- Verify button checks the disk file's Windows signature
- But not the RAM image, so it won't detect process replacement



The Properties window, Image tab

Strings

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



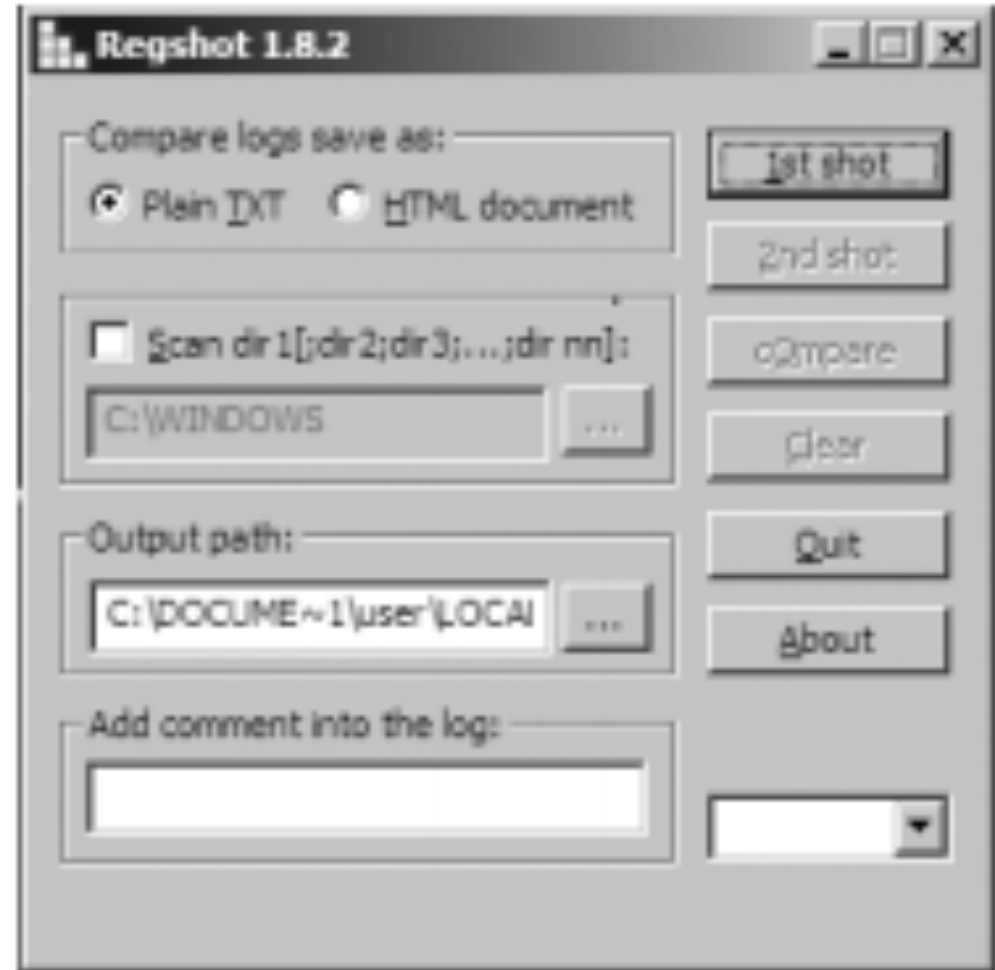
The Process Explorer Strings tab shows strings on disk (left) versus strings in memory (right) for active svchost.exe.

Analyzing Malicious Documents

- Open the document (e.g. PDF) on a system with a vulnerable application
- Watch Process Explorer to see if it launches a process
- The Image tab of that process's Properties sheet will show where the malware is

Comparing Registry Snapshots with Regshot

- Regshot
- Take 1st shot
- Run malware
- Take 2nd shot
- Compare them to see what registry keys were changed



Regshot window

Regshot comparison results

Regshot

Comments:

Datetime: <date>

Computer: MALWAREANALYSIS

Username: username

Keys added: 0

Values added:3

-
- ① HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ckr:C:\WINDOWS\system32\ckr.exe
...
...

Values modified:2

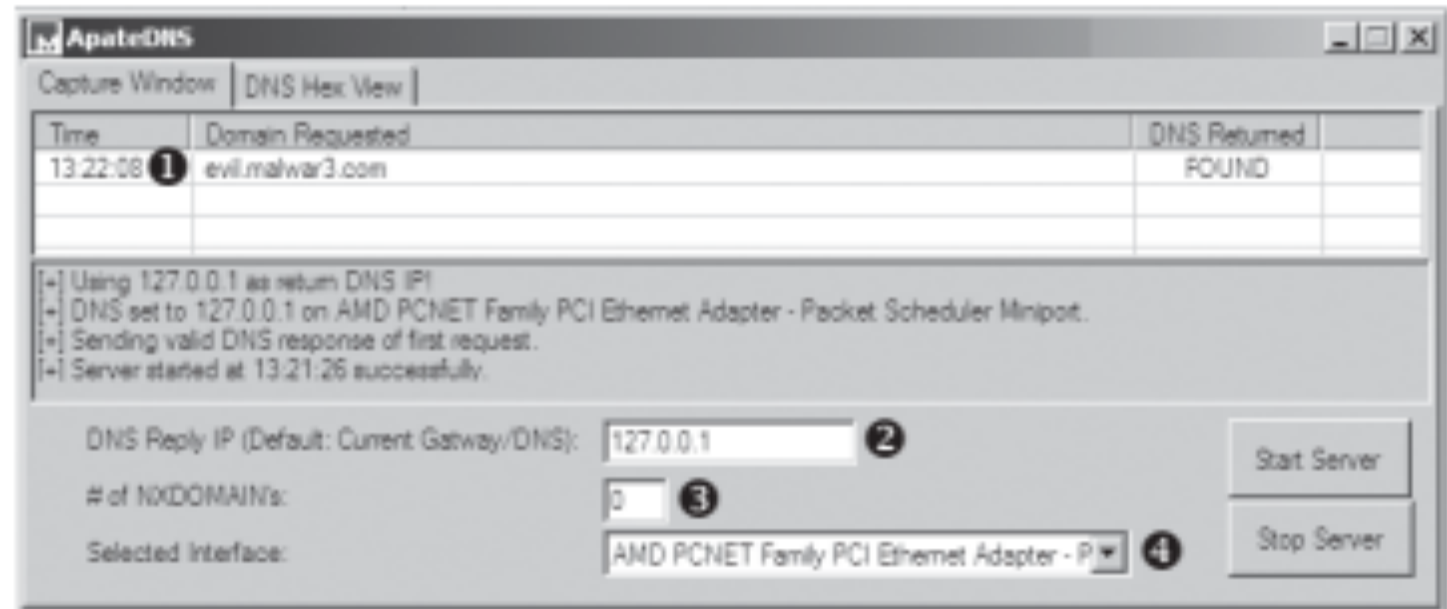
-
- ② HKLM\SOFTWARE\Microsoft\Cryptography\ RNG\Seed: 00 43 7C 25 9C 68 DE 59 C6 C8
9D C3 1D E6 DC 87 1C 3A C4 E4 D9 0A B1 BA C1 FB 80 EB 83 25 74 C4 C5 E2 2F CE
4E E8 AC C8 49 E8 E8 10 3F 13 F6 A1 72 92 28 8A 01 3A 16 52 86 36 12 3C C7 EB
5F 99 19 1D 80 8C 8E BD 58 3A DB 18 06 3D 14 8F 22 A4
...

Total changes:5

Faking a Network

- Using ApateDNS to Redirect DNS Resolutions

- DNS information is requested for evil.malwar3.com and that request was made at 13:22:08
- Set the IP address you want sent in DNS responses
- You can catch additional domains used by a malware sample through the use of the nonexistent domain (NXDOMAIN) option
- select the interface



Redirect the DNS requests made by malware known as RShell.

Ncat Listener

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

Monitoring with Ncat(included with Nmap)

- Netcat, the “TCP/IP Swiss Army knife,” can be used over both inbound and outbound connections for port scanning, tunneling, proxying, port forwarding, and much more.
- In listen mode, Netcat acts as a server, while in connect mode it acts as a client.
- Netcat takes data from standard input for transmission over the network. All the data it receives is output to the screen via standard output.

Monitoring with Ncat

```
C:\> nc -l -p 80 ❶
POST /cq/frame.htm HTTP/1.1
Host: www.google.com ❷
User-Agent: Mozilla/5.0 (Windows; Windows NT 5.1; TWfSd2FyZUh1bnRlcg==;
rv:1.38)
Accept: text/html, application
Accept-Language: en-US, en;q=
Accept-Encoding: gzip, deflate
Keep-Alive: 300
Content-Type: application/x-form-urlencoded
Content-Length

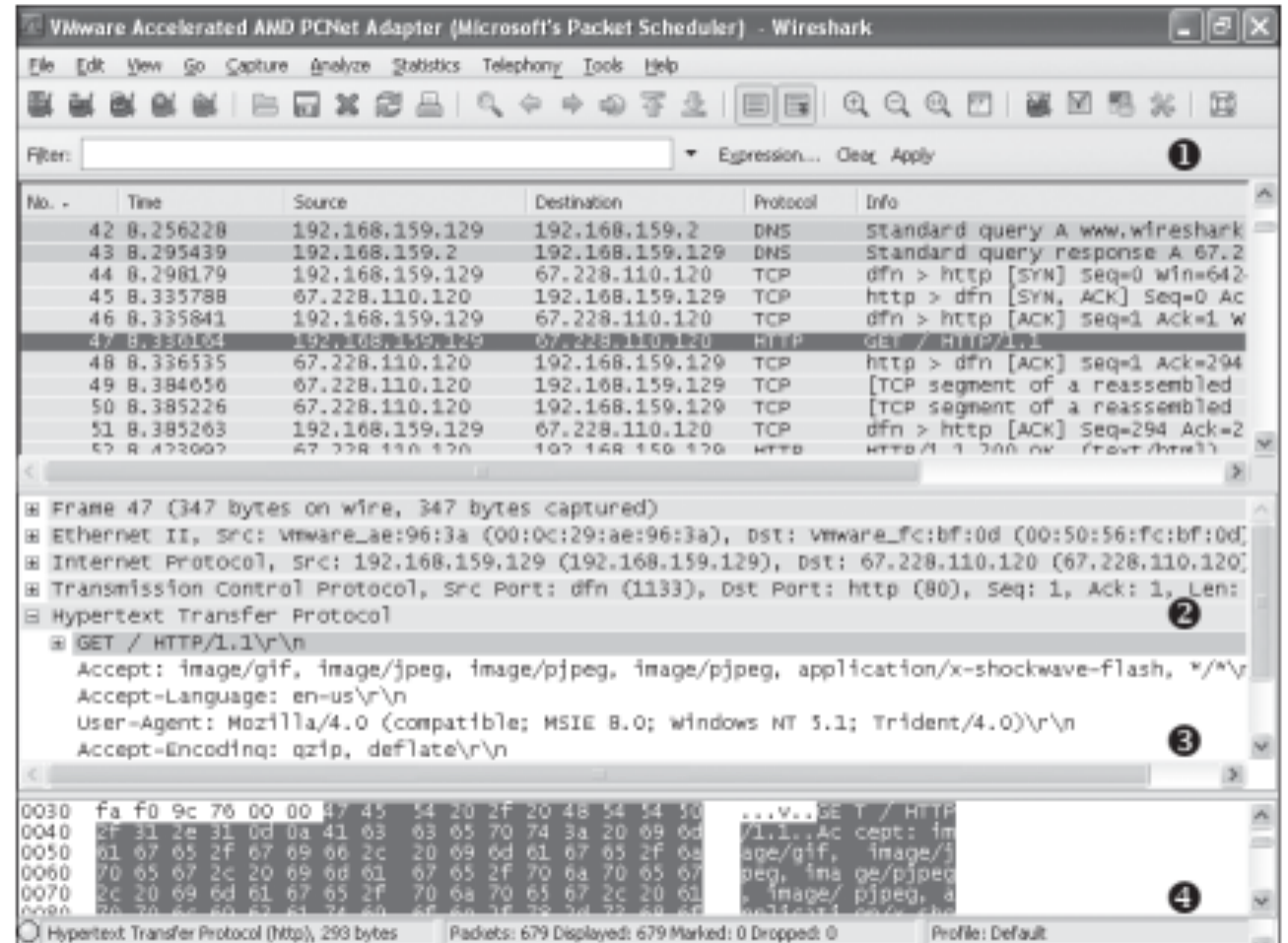
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

Z:\Malware> ❸
```

Netcat example listening on port 80

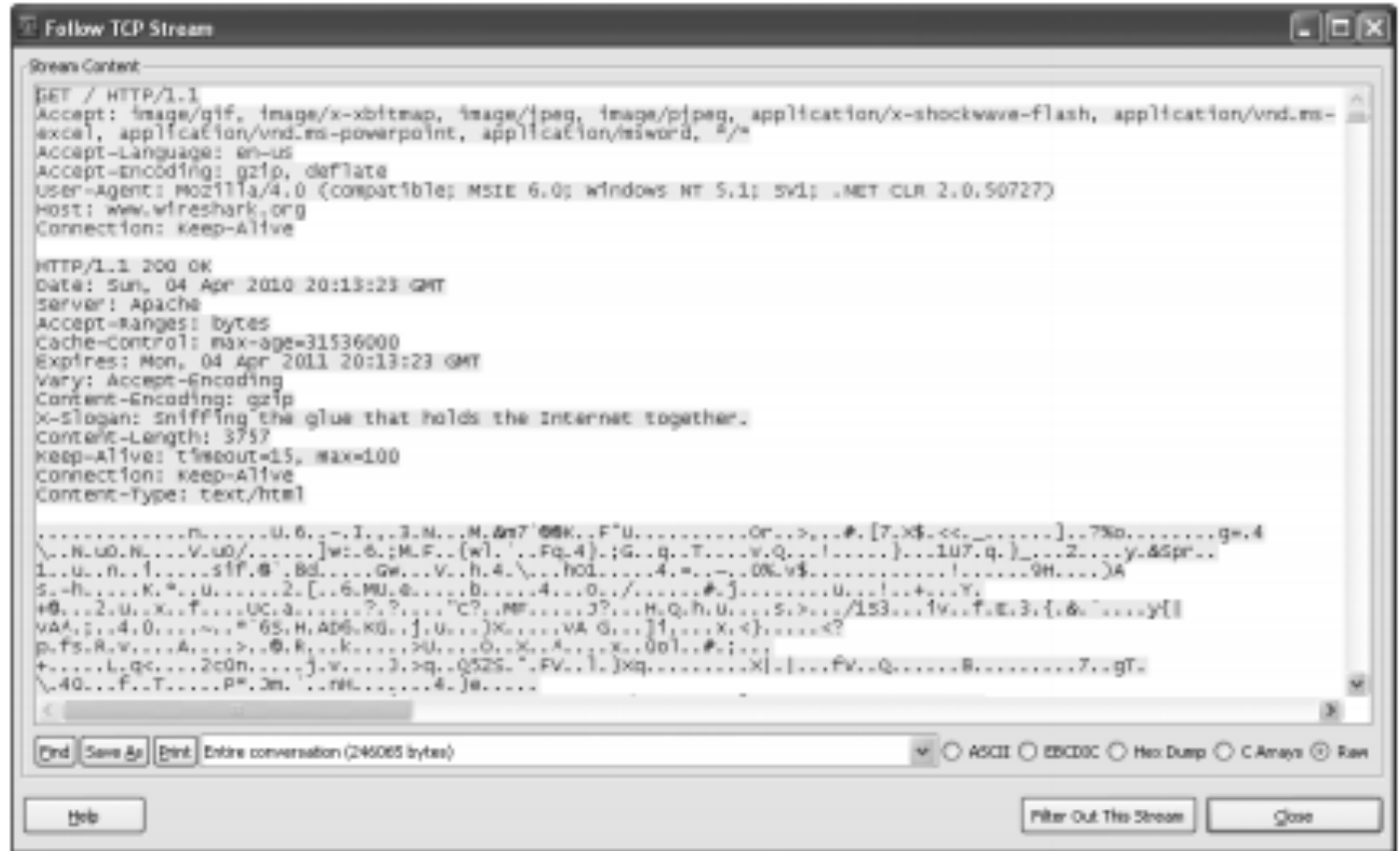
Packet Sniffing with Wireshark

- The Filter box is used to filter the packets displayed
- The packet listing window shows all packets that satisfy the display filter.
- The packet detail window displays the contents of the currently selected packet
- The hex window displays the hex contents of the current packet.
- The hex window is linked with the packet detail window and will highlight any fields you select.



Follow TCP Stream

- Can save files from streams here too



Wireshark's Follow TCP Stream window

Using INetSim

- INetSim is a free, Linux-based software suite for simulating common Internet services
- INetSim is the best free tool for providing fake services
- allowing you to analyze the network behavior of unknown malware samples by emulating services such as HTTP, HTTPS, FTP, IRC, DNS, SMTP, and others

INetSim default emulated services

```
* dns 53/udp/tcp - started (PID 9992)
* http 80/tcp - started (PID 9993)
* https 443/tcp - started (PID 9994)
* smtp 25/tcp - started (PID 9995)
* irc 6667/tcp - started (PID 10002)
* smtps 465/tcp - started (PID 9996)
* ntp 123/udp - started (PID 10003)
* pop3 110/tcp - started (PID 9997)
* finger 79/tcp - started (PID 10004)
* syslog 514/udp - started (PID 10006)
* tftp 69/udp - started (PID 10001)
* pop3s 995/tcp - started (PID 9998)
* time 37/tcp - started (PID 10007)
* ftp 21/tcp - started (PID 9999)
* ident 113/tcp - started (PID 10005)
* time 37/udp - started (PID 10008)
* ftps 990/tcp - started (PID 10000)
* daytime 13/tcp - started (PID 10009)
* daytime 13/udp - started (PID 10010)
* echo 7/tcp - started (PID 10011)
* echo 7/udp - started (PID 10012)
* discard 9/udp - started (PID 10014)

* discard 9/tcp - started (PID 10013)
* quotd 17/tcp - started (PID 10015)
* quotd 17/udp - started (PID 10016)
* chargen 19/tcp - started (PID 10017)
* dummy 1/udp - started (PID 10020)
* chargen 19/udp - started (PID 10018)
* dummy 1/tcp - started (PID 10019)
```

Basic Dynamic Tools in Practice

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

Example of virtual Network

