



MALWARE ANALYSIS

Basic Dynamic Analysis

Dr. Zeyad Safaa Younus Saffawi

Dynamic Analysis

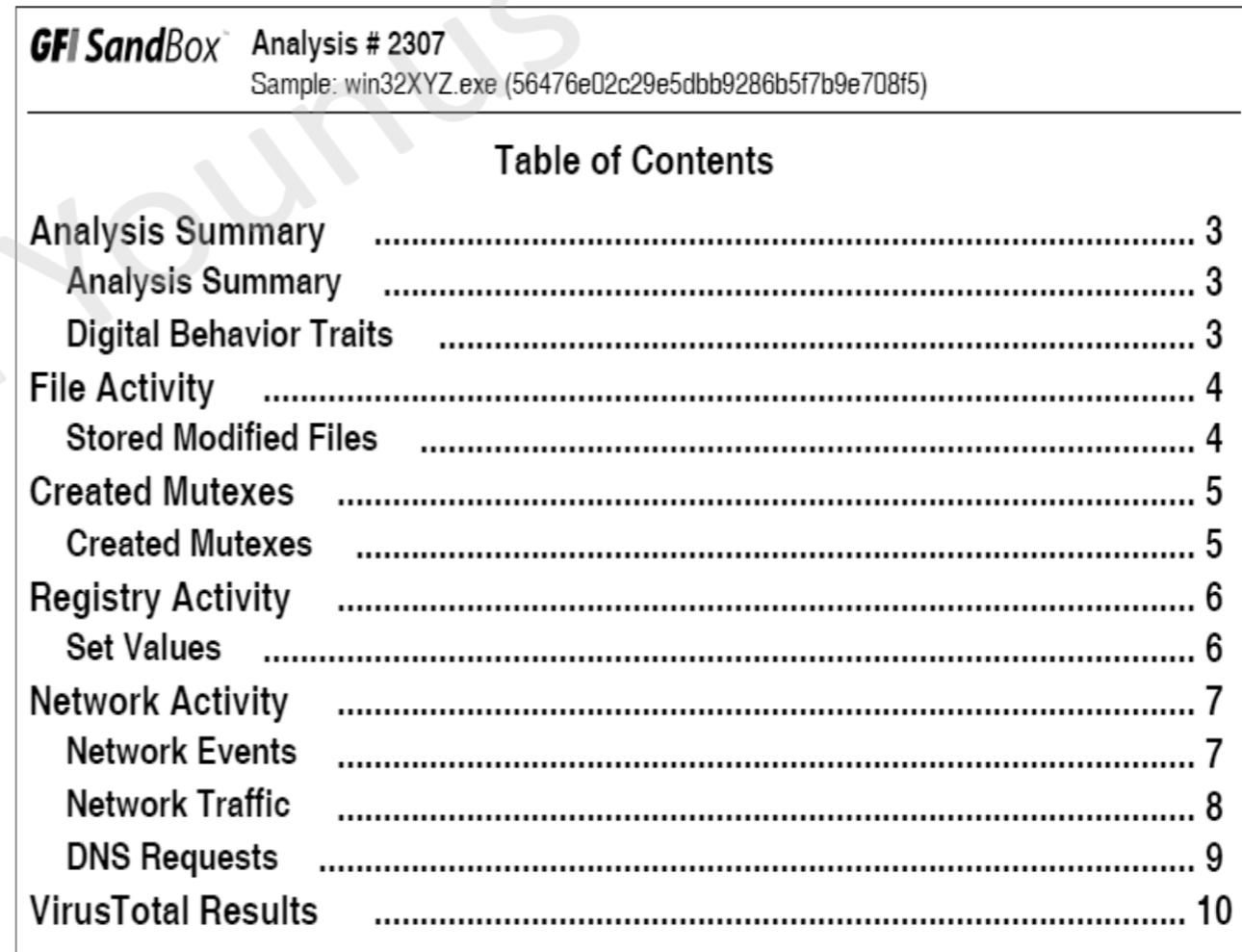
- **Dynamic analysis** involves **examining malware during its execution** to observe its actual behavior. This approach is highly effective because it reveals precisely how the malware interacts with the system, modifies files or the registry, communicates over the network, and performs other malicious actions.
- **Dynamic analysis** is generally **conducted** as the **second step in malware analysis, following static analysis**. It is particularly **necessary when static analysis cannot provide sufficient information due to challenges** such as:
 - **Obfuscation**: Techniques used by malware authors to hide program logic.
 - **Packing**: Compression or encryption of the executable code that prevents direct inspection.
 - **Limitations of static techniques**: Inability to observe runtime behavior, system interactions, or network communications.
- By executing malware in a controlled environment, analysts can overcome these obstacles and gain a comprehensive understanding of the malware's functionality.

Sandbox

- A **sandbox** is a **safe, isolated environment** used to run **untrusted programs (like malware)** for **basic dynamic analysis** without **harming real systems**.
- Sandboxes often **simulate network services** so malware can run normally.
- **Examples: Norman Sandbox, GFI Sandbox, Anubis, Joe Sandbox, Joe Sandbox, ThreatExpert, BitBlaze, Comodo Instant Malware Analysis.**
 - **paid versions are in-house and expensive but easy to use.**
 - **They produce a nice PDF report of results**

Using a Sandbox (Example: GFI Sandbox):

- Automates malware execution and generates reports.
- Key report sections:
 - **Analysis Summary:** static analysis information and a high-level overview of the dynamic analysis results
 - **File Activity:** Created, opened, or deleted files
 - **Created Mutexes:** Synchronization objects used by malware
 - **Registry Activity:** Changes to the Windows registry
 - **Network Activity:** Connections, setting up a listening port, or performing a DNS request
 - **VirusTotal Results:** Scan results for malware detection



The image shows a screenshot of a GFI SandBox report. At the top, it displays 'GFI SandBox Analysis # 2307' and 'Sample: win32XYZ.exe (56476e02c29e5dbb9286b5f7b9e708f5)'. Below this is a 'Table of Contents' section with the following items and page numbers:

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

Running Malware

- Running malware is a critical step in **dynamic analysis**.
- Most **EXE** files can be run easily.
- **DLL** files require special methods because Windows does not execute them directly.
- Before running, it's important to **identify exported functions** (using tools like **PEview** or **PE Explorer**, Dependency Walker) to know how to launch the DLL correctly.

• Running EXE Files

- Normally, you can double-click the file or use the command line:

```
C:\> sample.exe
```

- Before execution, always start your monitoring tools (ProcMon, Wireshark, Regshot...) and take a **snapshot** of the VM.

• Running DLL Files using rundll32.exe

- rundll32.exe is built into Windows and allows executing an exported DLL function:

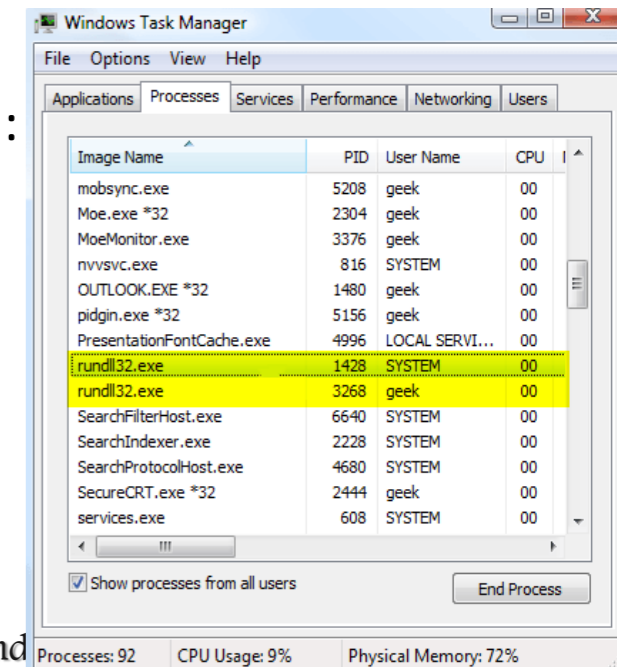
```
C:\> rundll32.exe DLLname,ExportName arguments
```

- If the function is exported by **ordinal number** instead of names, use #:

```
C:\> rundll32.exe mydll.dll,#5
```

- rip.dll has these export functions: **Install** and **Uninstall**

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



Process Monitor (Procmon)

- An advanced **Windows monitoring tool** that captures registry, file system, network, process/thread activity (**combines FileMon + RegMon features**)
- Starts capturing immediately when you enable capture; it buffers events in RAM until you stop.
- Because it can generate **tens of thousands** of events per minute, it can **exhaust memory and crash** a VM if left running too long.
- All recorded events are kept, but you can **filter the display to make it easier to focus on relevant items**

Process Monitor

Start/Stop Capture Erase Filter Default Filters
Registry, File system, Network, Processes

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-FAA4-4...	NAME NOT FOUND	Desired Access: Read
1:17:48.6015797 PM	calc.exe	2072	RegOpenKey	HKCR\CLSID\{FAE3D380-FAA4-4623-8C75-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-FAA4-4...	NAME NOT FOUND	Desired Access: Read
1:17:48.6016130 PM	calc.exe	2072	RegOpenKey	HKCR\CLSID\{FAE3D380-FAA4-4623-8C75-C6B6111...	NAME NOT FOUND	Desired Access: Read

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

Time of Day	Process Name	Operation	Path
1:14:...	svchost.exe	RegOpenKey	HKLM\System\CurrentControlSet\Control\Cryptography\Providers
1:14:...	svchost.exe	RegOpenKey	HKLM\System\CurrentControlSet\Control\Cryptography\Providers
1:14:...	svchost.exe	RegCloseKey	HKLM\System\CurrentControlSet\Control\Cryptography\Providers
1:14:...	svchost.exe	RegOpenKey	HKLM\System\CurrentControlSet\Control\Cryptography\Configuration
1:14:...	svchost.exe	RegOpenKey	HKLM\System\CurrentControlSet\Control\Cryptography\Configuration
1:14:...	svchost.exe	RegCloseKey	HKLM\System\CurrentControlSet\Control\Cryptography\Configuration
1:14:...	svchost.exe	RegQueryValue	HKLM\System\CurrentControlSet\Services\BTHPORT\Parameters\Devices\
1:14:...	svchost.exe	RegQueryValue	HKLM\System\CurrentControlSet\Services\BTHPORT\Parameters\Devices\
1:14:...	svchost.exe	RegQueryValue	HKLM\System\CurrentControlSet\Services\BTHPORT\Parameters\Devices\
1:14:...	svchost.exe	RegCloseKey	HKLM\System\CurrentControlSet\Services\BTHPORT\Parameters\Devices\
1:14:...	svchost.exe	WriteFile	C:\Windows\System32\winevt\Logs\Microsoft-Windows-AppXDeployment%4
1:14:...	svchost.exe	WriteFile	C:\Windows\System32\winevt\Logs\Microsoft-Windows-UniversalTelemetryC
1:14:...	svchost.exe	WriteFile	C:\Windows\System32\winevt\Logs\Microsoft-Windows-PushNotification-Pla
1:14:...	svchost.exe	WriteFile	C:\Windows\System32\winevt\Logs\Microsoft-Windows-AppModel-Runtime%
1:14:...	svchost.exe	WriteFile	C:\Windows\System32\winevt\Logs\Microsoft-Windows-Hyper-V-VmSwitch-(
1:14:...	svchost.exe	WriteFile	C:\Windows\System32\winevt\Logs\Microsoft-Windows-CodeIntegrity%4Ope
1:14:...	svchost.exe	WriteFile	C:\Windows\System32\winevt\Logs\Microsoft-Windows-SettingSync-OneDri
1:14:...	svchost.exe	WriteFile	C:\Windows\System32\winevt\Logs\Microsoft-Windows-WindowsUpdateClie
1:14:...	svchost.exe	WriteFile	C:\Windows\System32\winevt\Logs\Application.evtx
1:14:...	svchost.exe	Thread Create	

Showing 1,209,018 of 2,139,796 events (56%) Backed by virtual memory

Filtering in Process Monitor tool

- When Procmon (Process Monitor) is running, it records **thousands of events**, making it hard to find relevant information.
- **Filtering** helps reduce noise and focus only on suspicious or important activities — especially during malware analysis.
 - Go to Filter → Filter.
 - Select a column (e.g., Process Name, Operation, or Detail).
 - Choose a condition (e.g., Is, Contains).
 - Decide to Include or Exclude the events.
 - Click Add, then Apply.

Filtering in Process Monitor tool

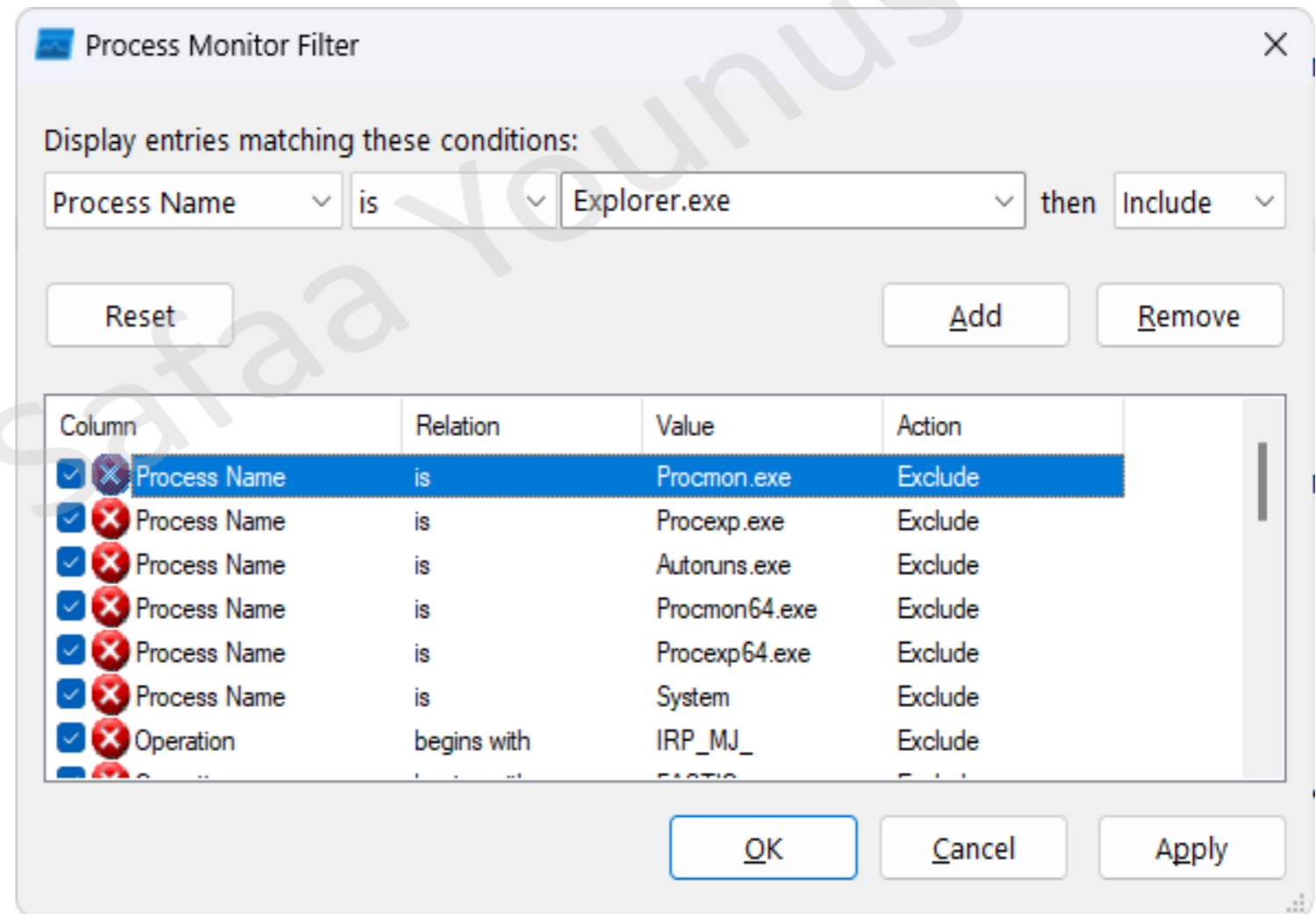
- Filtering with Exclude

- 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

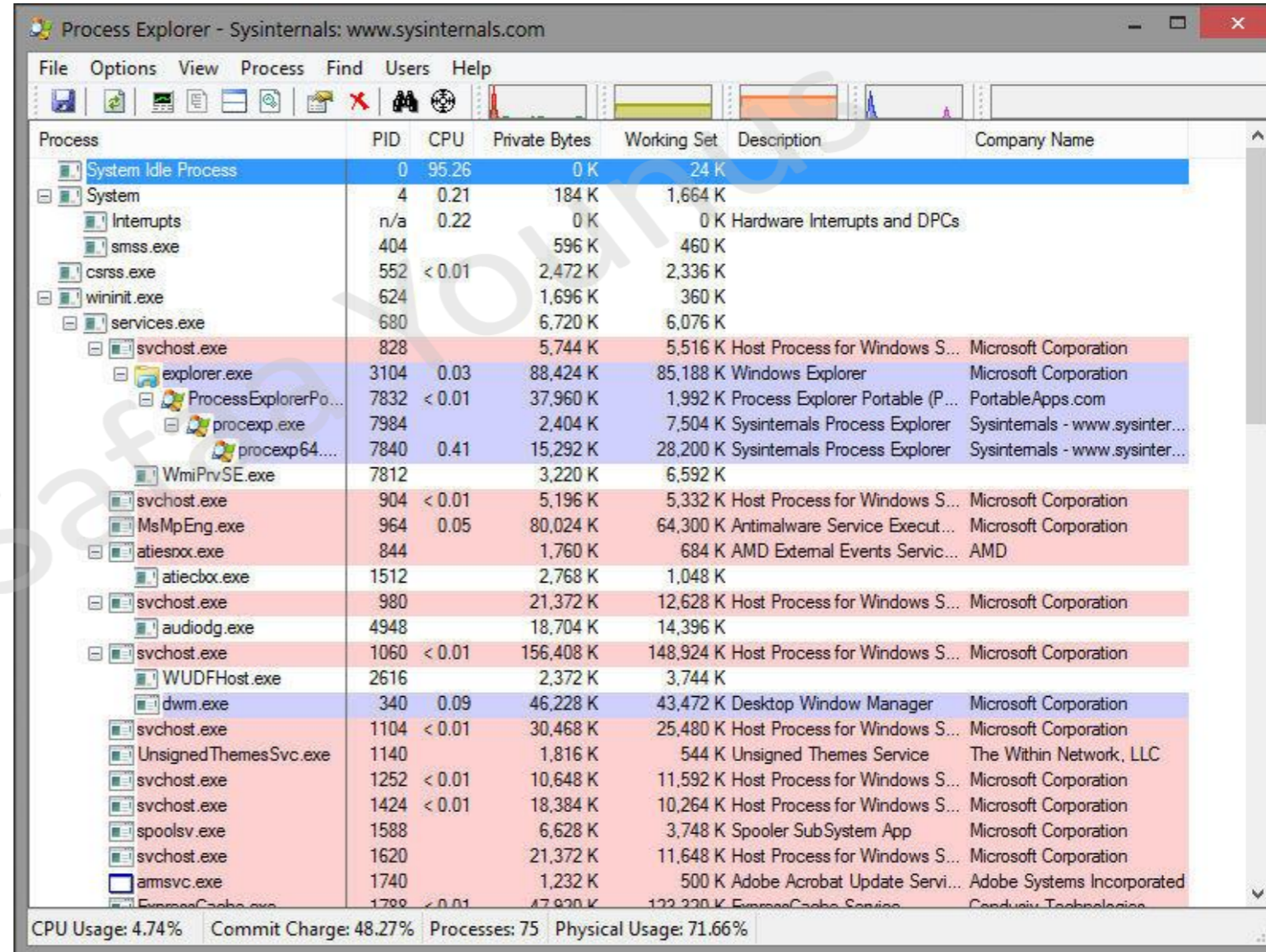


Viewing Processes with Process Explorer

- **Process Explorer** is a powerful task manager tool from Microsoft used in dynamic malware analysis. It shows processes in a tree structure
- It provides real-time visibility into:
 - **Running processes**
 - **Loaded DLLs**
 - **System resource usage**
 - **Network connections**
 - **Process properties** (threads, handles, etc.)
- Default columns:
 - **Process**
 - **PID**
 - **CPU**
 - **Description**
 - **Company Name**

Color coding

- **Pink** = services
- **Blue** = processes
- **Green** = new processes
- **Red** = terminated processes.
- Helps track new or suspicious processes created by malware.



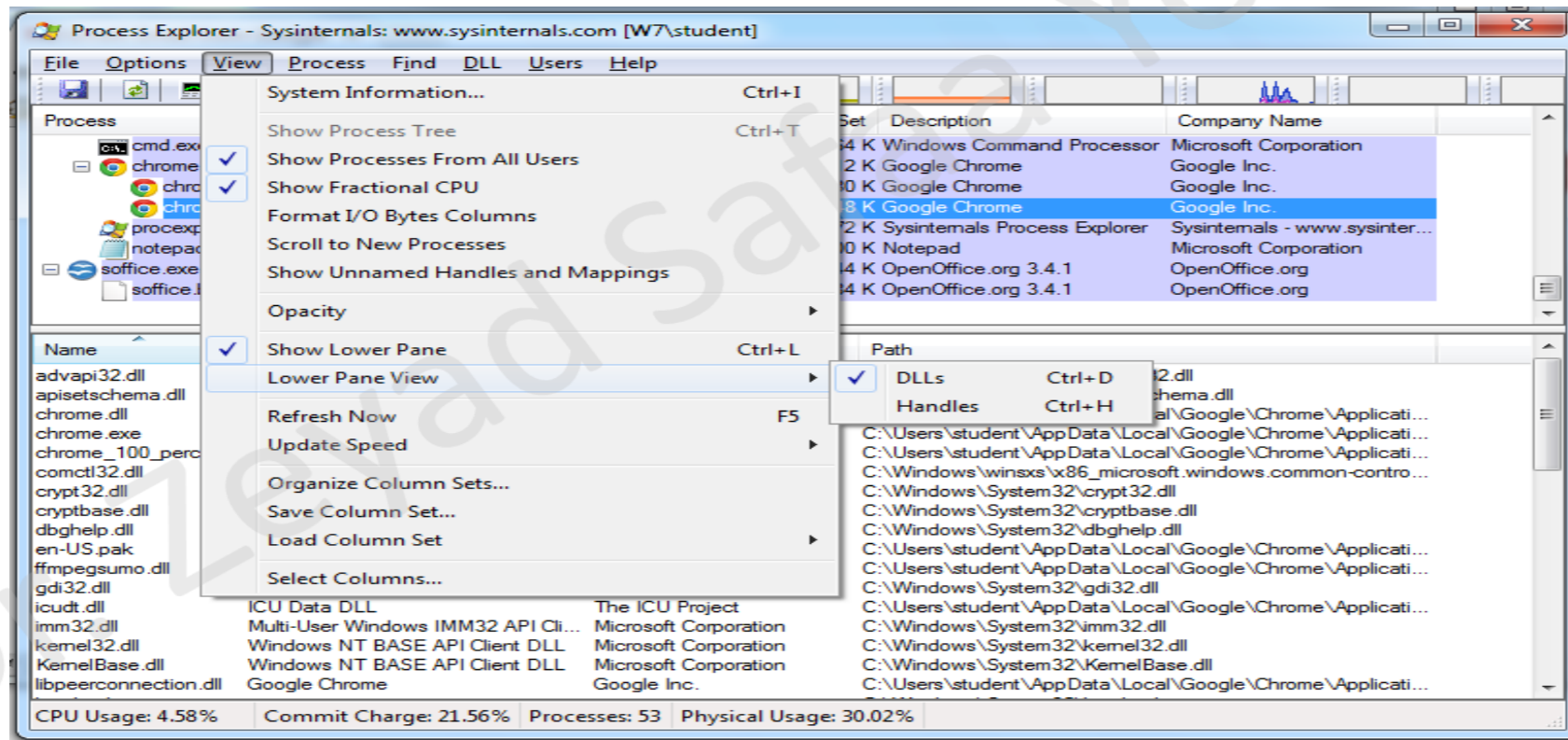
Process Explorer - Sysinternals: www.sysinternals.com

Process	PID	CPU	Private Bytes	Working Set	Description	Company Name
System Idle Process	0	95.26	0 K	24 K		
System	4	0.21	184 K	1,664 K		
Interrupts	n/a	0.22	0 K	0 K	Hardware Interrupts and DPCs	
smss.exe	404		596 K	460 K		
csrss.exe	552	< 0.01	2,472 K	2,336 K		
wininit.exe	624		1,696 K	360 K		
services.exe	680		6,720 K	6,076 K		
svchost.exe	828		5,744 K	5,516 K	Host Process for Windows S...	Microsoft Corporation
explorer.exe	3104	0.03	88,424 K	85,188 K	Windows Explorer	Microsoft Corporation
ProcessExplorerPo...	7832	< 0.01	37,960 K	1,992 K	Process Explorer Portable (P...	PortableApps.com
procexp.exe	7984		2,404 K	7,504 K	Sysinternals Process Explorer	Sysinternals - www.sysinter...
procexp64...	7840	0.41	15,292 K	28,200 K	Sysinternals Process Explorer	Sysinternals - www.sysinter...
WmiPrivSE.exe	7812		3,220 K	6,592 K		
svchost.exe	904	< 0.01	5,196 K	5,332 K	Host Process for Windows S...	Microsoft Corporation
MsMpEng.exe	964	0.05	80,024 K	64,300 K	Antimalware Service Execut...	Microsoft Corporation
atiesnox.exe	844		1,760 K	684 K	AMD External Events Servic...	AMD
atiecbox.exe	1512		2,768 K	1,048 K		
svchost.exe	980		21,372 K	12,628 K	Host Process for Windows S...	Microsoft Corporation
audiodg.exe	4948		18,704 K	14,396 K		
svchost.exe	1060	< 0.01	156,408 K	148,924 K	Host Process for Windows S...	Microsoft Corporation
WUDFHost.exe	2616		2,372 K	3,744 K		
dwm.exe	340	0.09	46,228 K	43,472 K	Desktop Window Manager	Microsoft Corporation
svchost.exe	1104	< 0.01	30,468 K	25,480 K	Host Process for Windows S...	Microsoft Corporation
Unsigned ThemesSvc.exe	1140		1,816 K	544 K	Unsigned Themes Service	The Within Network, LLC
svchost.exe	1252	< 0.01	10,648 K	11,592 K	Host Process for Windows S...	Microsoft Corporation
svchost.exe	1424	< 0.01	18,384 K	10,264 K	Host Process for Windows S...	Microsoft Corporation
spoolsv.exe	1588		6,628 K	3,748 K	Spooler SubSystem App	Microsoft Corporation
svchost.exe	1620		21,372 K	11,648 K	Host Process for Windows S...	Microsoft Corporation
amsvc.exe	1740		1,232 K	500 K	Adobe Acrobat Update Servi...	Adobe Systems Incorporated
ExpressCache.exe	1788	< 0.01	47,920 K	122,220 K	ExpressCache Service	Conduity Technologies

CPU Usage: 4.74% Commit Charge: 48.27% Processes: 75 Physical Usage: 71.66%

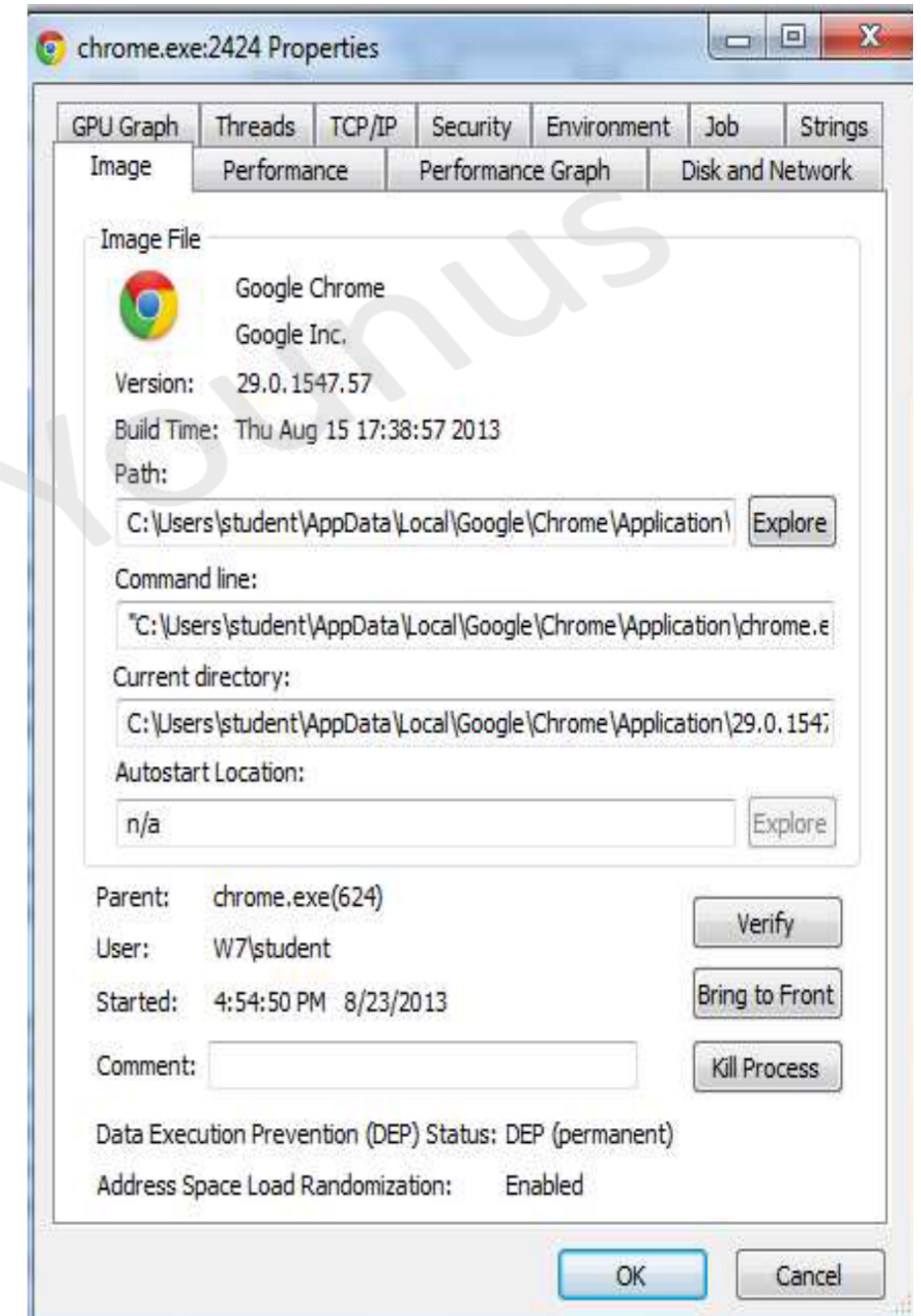
Inspecting Processes

- DLL View: Shows all DLLs loaded into a process.
- Handles View: Displays files, mutexes, events, and handles used.



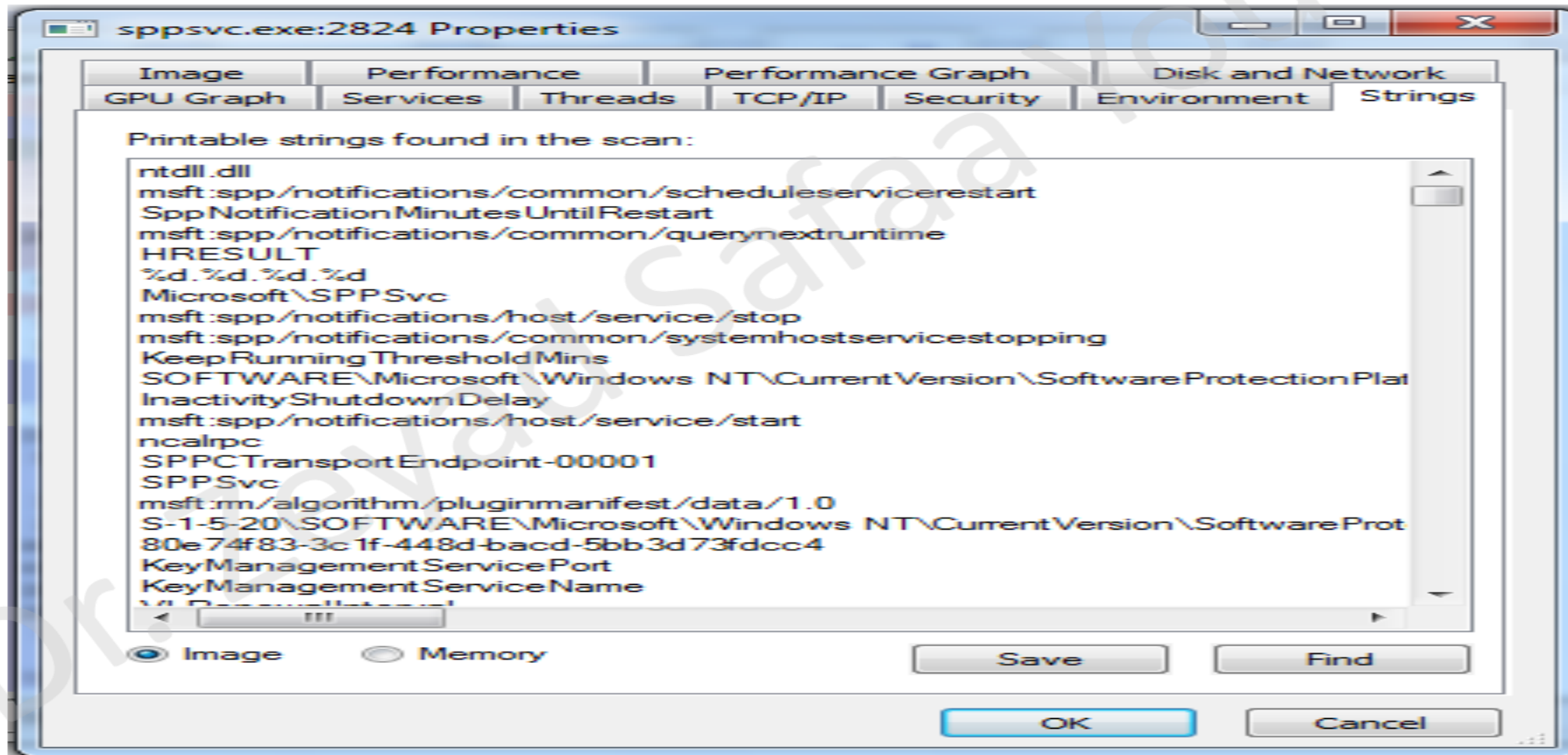
Properties

- **Threads tab**: Active threads
- **TCP/IP tab**: Active network connections or ports
- **Image tab**: File path on disk
 - Displays **DEP (Data Execution Prevention)** and **ASLR (Address Space Layout Randomization)** status.
- **Verify button** checks the **digital signature of the file on disk**.
 - Does not verify the in-memory image, so it **cannot detect process replacement**.



Properties

- Use the Strings tab to compare:
 - Disk image strings vs. memory strings.
 - A big difference may indicate process replacement (e.g., svchost.exe case).

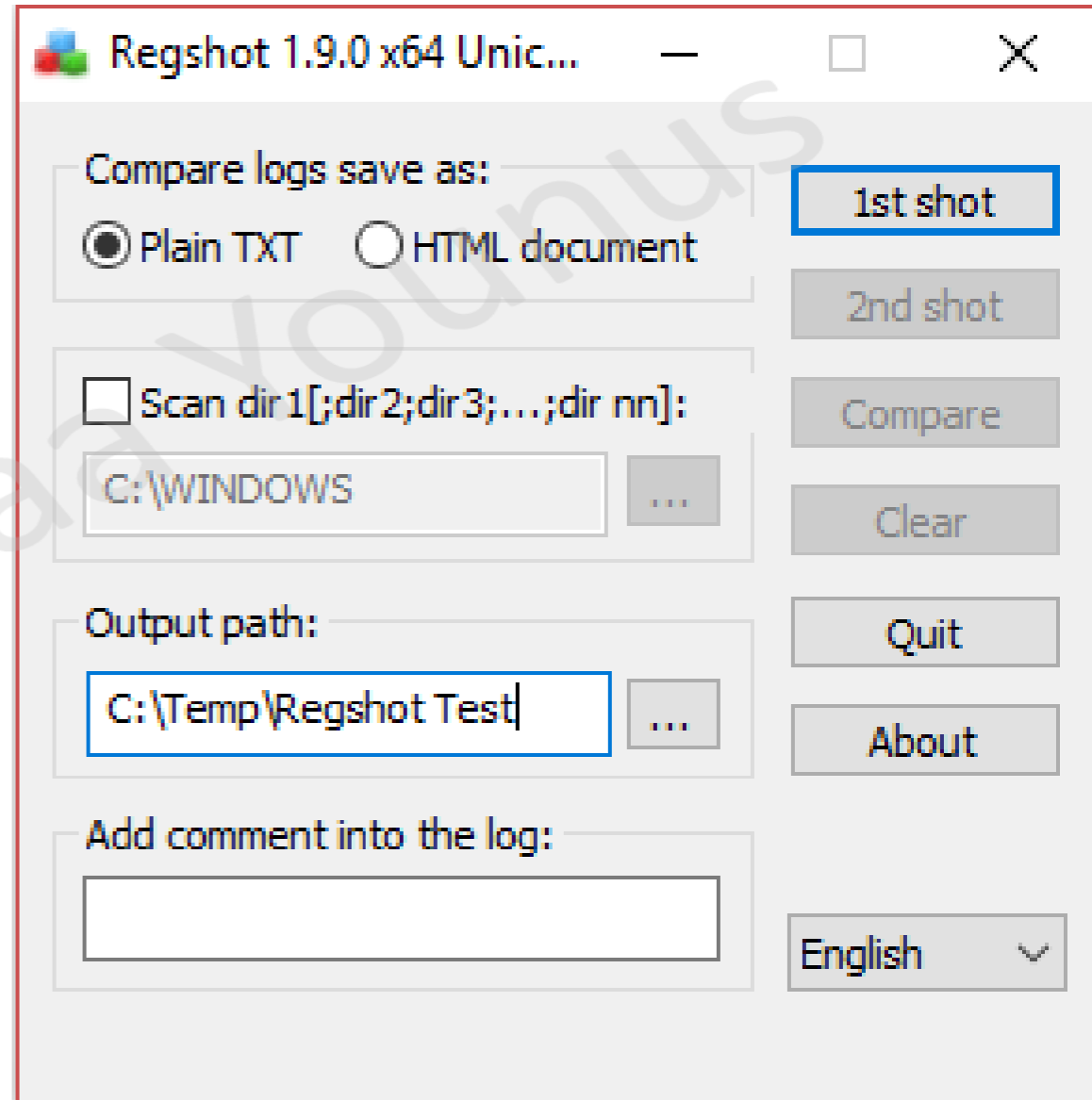


Detecting Malicious Documents

- Open **suspicious PDFs or Word** files while Process Explorer runs.
- 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 located**

Regshot tool

- **Regshot** is an open-source tool for taking and comparing Windows registry snapshots.
- Identify changes made by malware to the registry, such as added or modified keys and values.
- **Regshot for malware analysis:**
- Take the **first snapshot** before running the malware by clicking **1st Shot**.
- Run the malware and let it complete its actions.
- Take the **second snapshot** by clicking **2nd Shot**.
- Click **Compare** to see all registry changes.

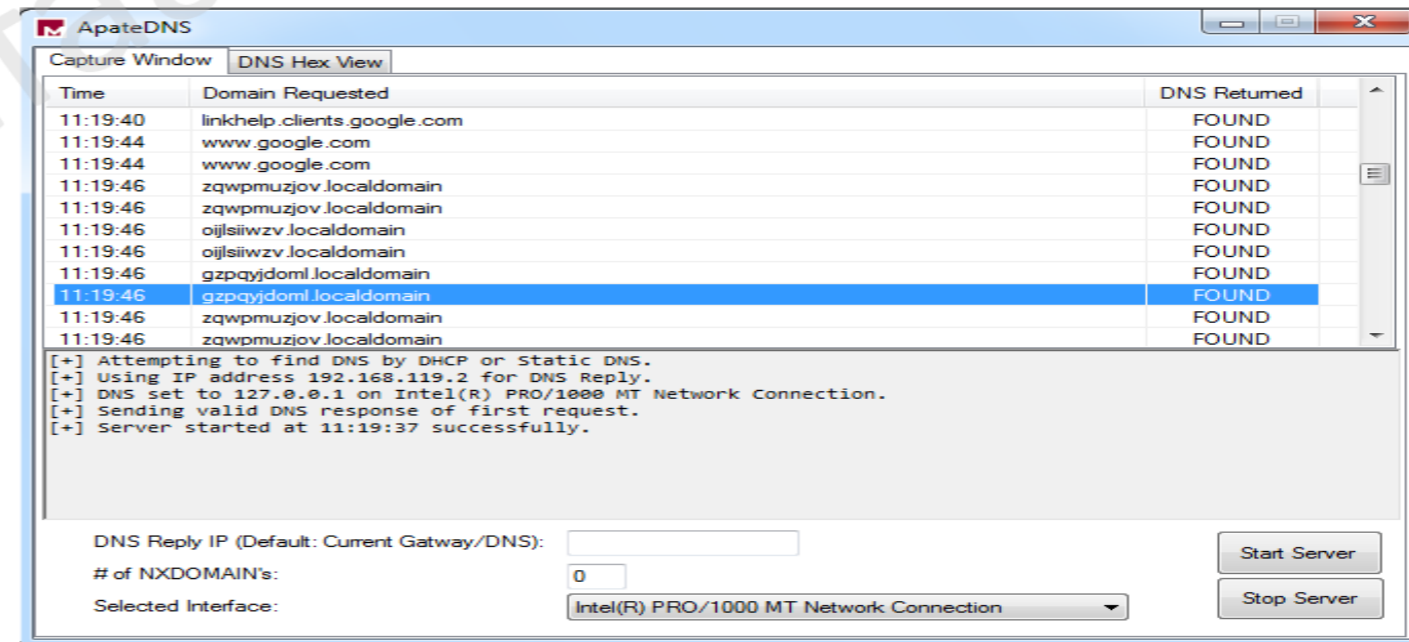
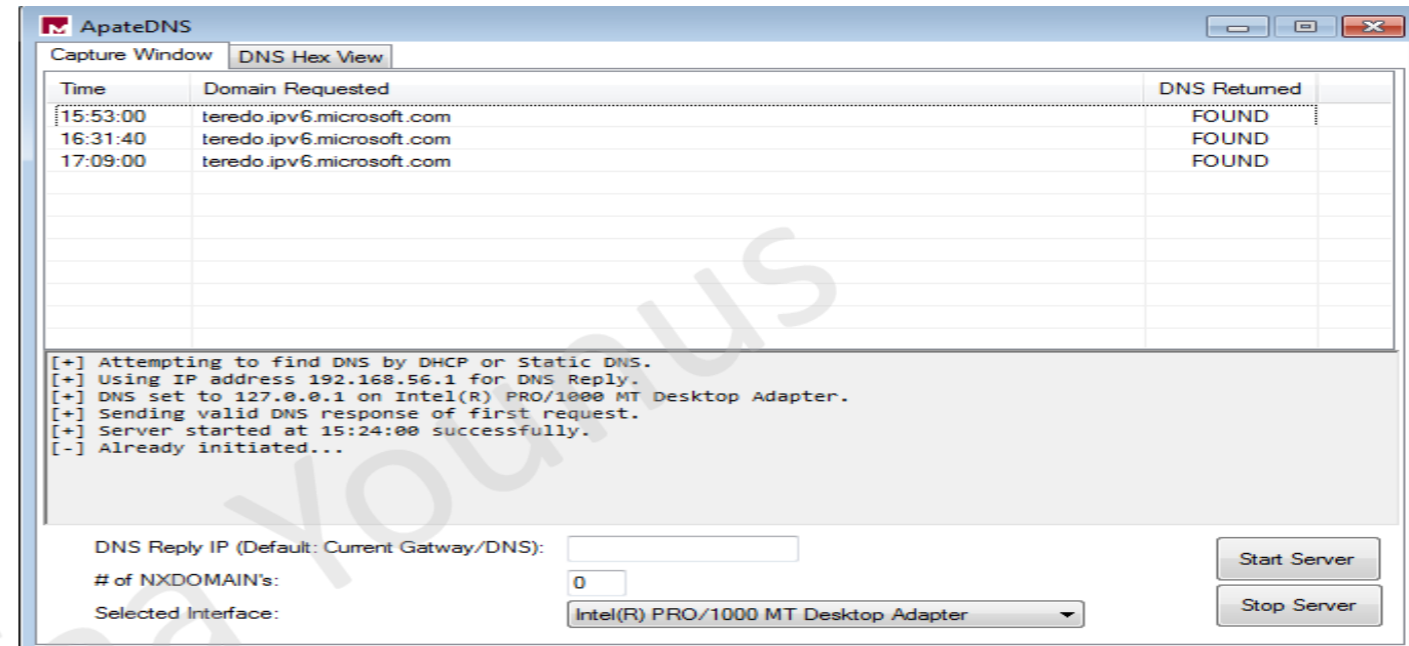


Faking a Network

- **let malware believe it has normal Internet connectivity so it will perform network behavior** (beacons, DNS lookups, C2 traffic) without actually touching the real Internet.
- Collect network indicators (domains, IPs, request patterns, packet signatures) safely for analysis and signature creation.
- tools
 - FakeNet-NG — lightweight network simulator that intercepts and responds to many protocols. Easy for quick sorting.
 - INetSim — more full-featured Internet services simulator (DNS, HTTP, SMTP, FTP, etc.).
 - **Network redirection/iptables and DNS spoofing** (for custom responses).
 - Proxy tools (mitmproxy) — for inspecting HTTP/HTTPS if you control certs.
 - Wireshark / tcpdump — capture traffic for offline analysis.

ApateDNS

- **ApateDNS** is a lightweight DNS responder/spoofing tool that listens on UDP/53 and replies to DNS queries with an IP address you choose.
- quickly see which domain names malware tries to resolve and direct those names to a local or fake server (so malware continues execution without touching the real Internet).



Monitoring with Netcat

- Netcat (nc) is a lightweight, flexible TCP/UDP tool — “the TCP/IP Swiss Army knife.”
- Two main modes:
 - Listen/server mode (-l) — waits for inbound connections.
 - Connect/client mode — initiates outbound connections to a target.
- Data read from stdin is sent over the network; data received is written to stdout.
- Run Netcat in listen mode on the expected port (e.g., port 80 for HTTP-based C2)
 - C2 (Command and Control): The malware uses the C2 channel to send commands (from the attacker) and receive results (from the victim).
- so you can capture whatever the malware sends:
nc -l -p 80
- Start the malware in the isolated guest VM. When the malware connects, Netcat will print the raw request (HTTP headers, POST body, or shell input) to your terminal.

```
POST /cq/frame.htm HTTP/1.1
Host: www.google.com
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

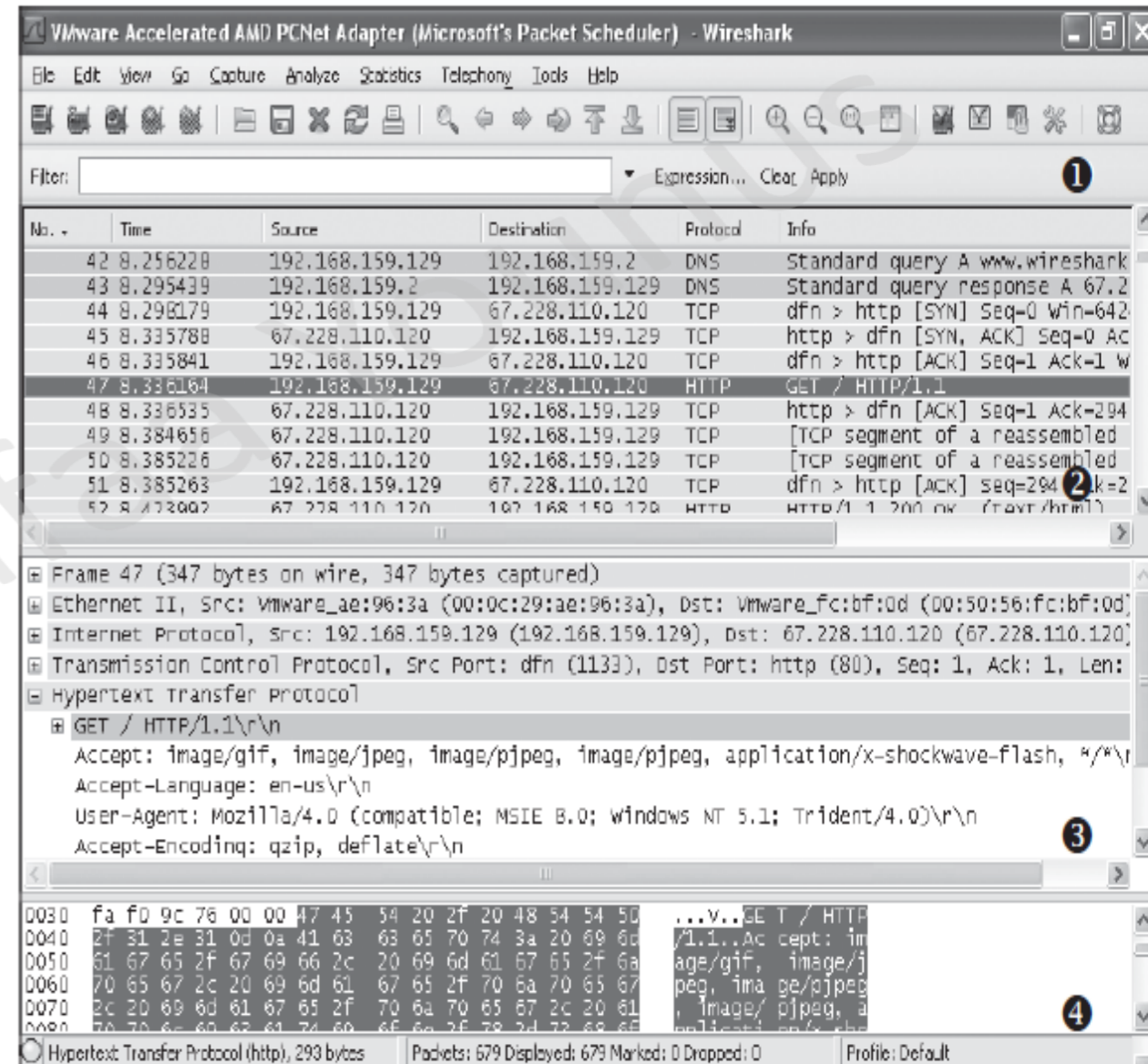
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

Z:\Malware>
```

Packet Sniffing with Wireshark

- **Wireshark is an Open-source** packet capture and analysis tool.
- Captures network traffic, lets you inspect packet details, follow sessions, and analyze protocols.

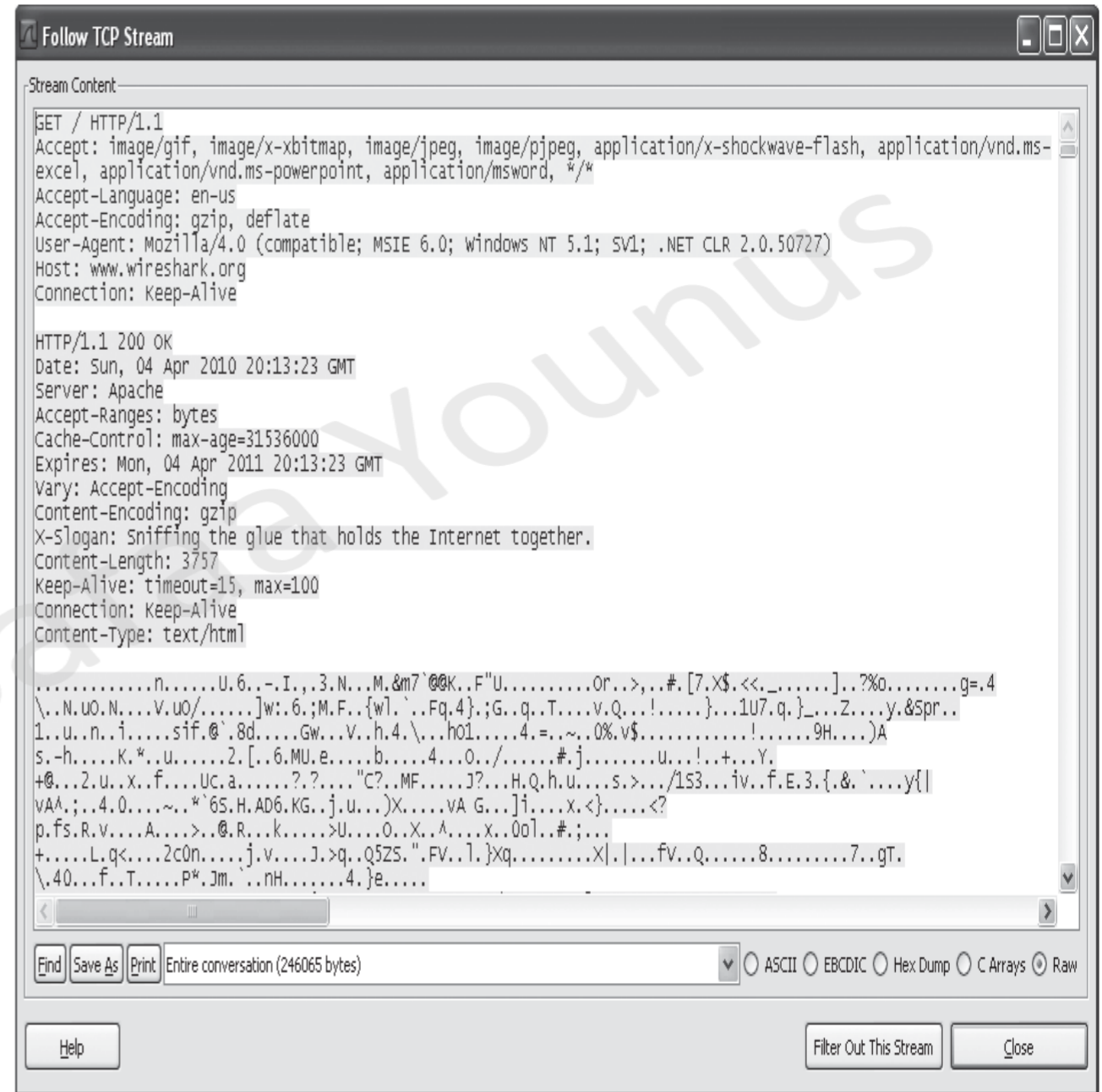
1. **Filter box** — enter display filters (e.g., http, ip.addr == 10.0.0.5, tcp.port == 80).
2. **Packet list** — all packets that match the display filter (one line per packet).
3. **Packet details** — decoded protocol tree for the selected packet.
4. **Hex / bytes pane** — raw packet bytes; linked to the decoded fields.



Follow a session: Right-click a TCP packet → **Follow** → **TCP Stream** to view the full conversation (colored per side). Great for reading HTTP POST bodies or command channels.

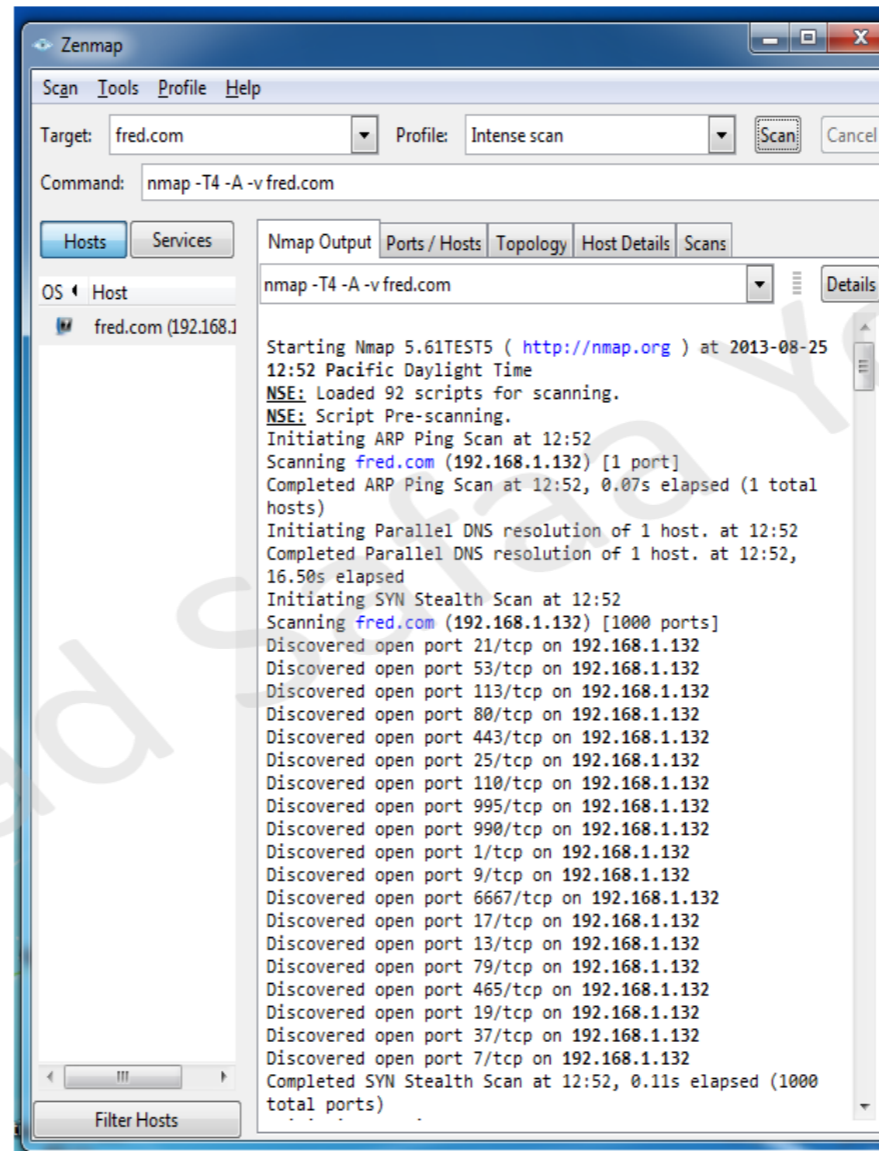
Save PCAP: File → Save/Export — keep PCAPs for later analysis or evidence.

Use with other tools: correlate PCAPs with Procmon, Netcat logs, and system artifacts.



INetSim

- INetSim is a free Linux-based suite that simulates common Internet services (HTTP, DNS, SMTP, FTP, IRC, etc.) for malware analysis.
- Run it on a Linux VM on the same isolated virtual network as your malware analysis VM.
- Let malware believe it has Internet access so it will perform network actions (beacons, C2, downloads) without touching the real Internet.
- Collects network indicators (domains, URIs, payloads) safely.
- Emulates many services by default (DNS 53, HTTP 80, HTTPS 443, SMTP 25, FTP 21, IRC 6667, TFTP 69, POP3 110, and many more).
- HTTP/HTTPS: serves almost any requested file (prevents 404s that would stop malware).



- * 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

- **Start Procmon and clear display.**
 - Add a filter for the malware process name (e.g., msts.exe) so you only see its events.
- **Open Process Explorer** to watch processes, DLLs, handles, network connections.
- **Take a registry snapshot** with Regshot (click **1st Shot**).
- **Prepare the virtual network:**
 - Run **INetSim** on a Linux analysis VM (HTTP/HTTPS/DNS/etc.).
 - Run **ApateDNS** on the Windows analysis host (redirect guest DNS to INetSim).
- **Start packet capture** with Wireshark on the internal/host-only network interface.

References

- Sikorski, M., & Honig, A. (2012). *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software*. No Starch Press.
- Bowne, S. (n.d.). *CNIT 126 Ch 2: Malware Analysis in Virtual Machines & 3: Basic Dynamic Analysis* [PowerPoint slides]. SlideShare.
<https://www.slideshare.net/slideshow/cnit-126-2-malware-analysis-in-virtual-machines-3-basic-dynamic-analysis/71069826>
- Bowne, S. (n.d.). *CNIT 126: Ch 2-3 Basic Dynamic Analysis* [Video]. YouTube. <https://www.youtube.com/watch?v=Nsy8U8UAbHk>