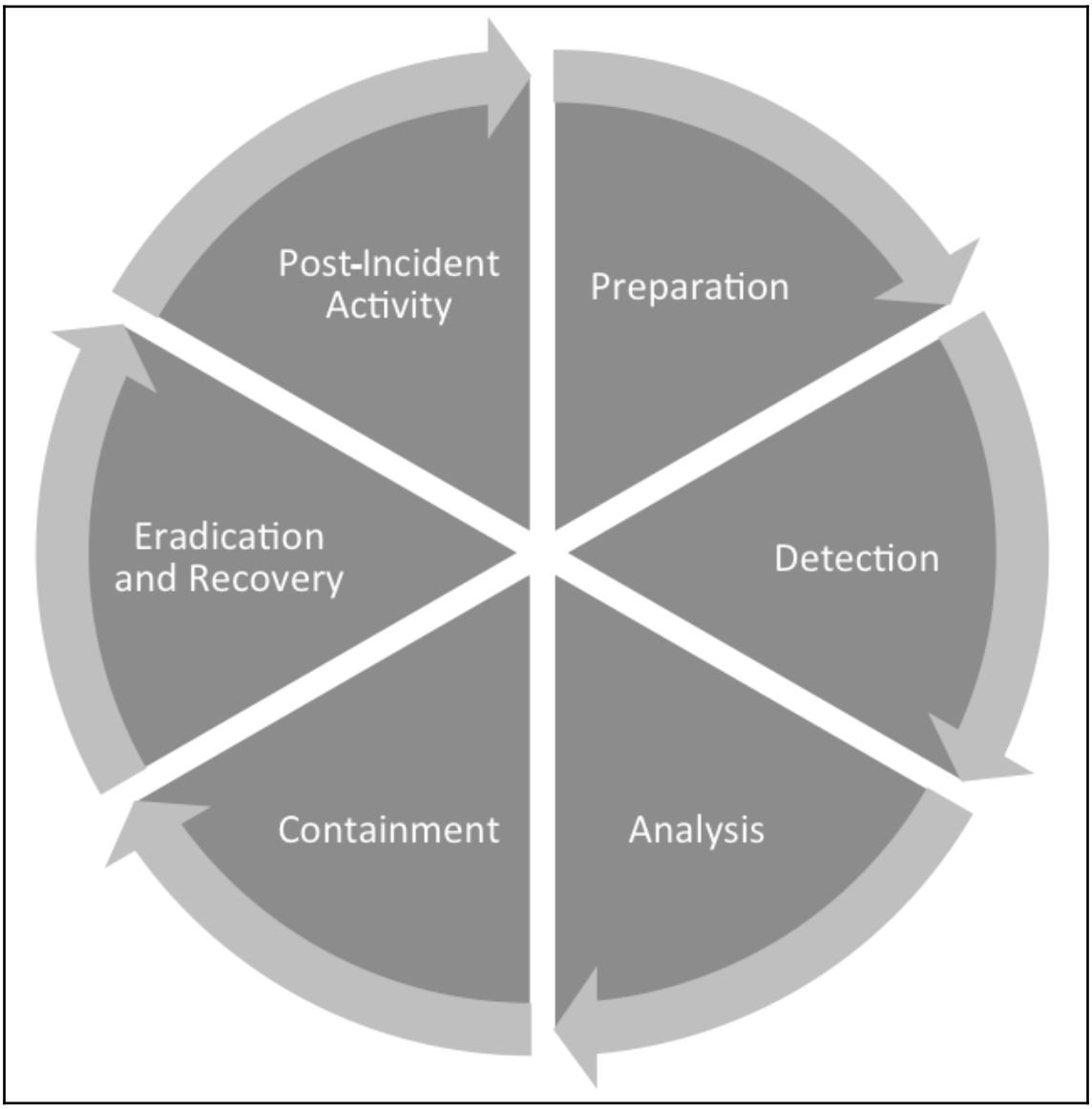
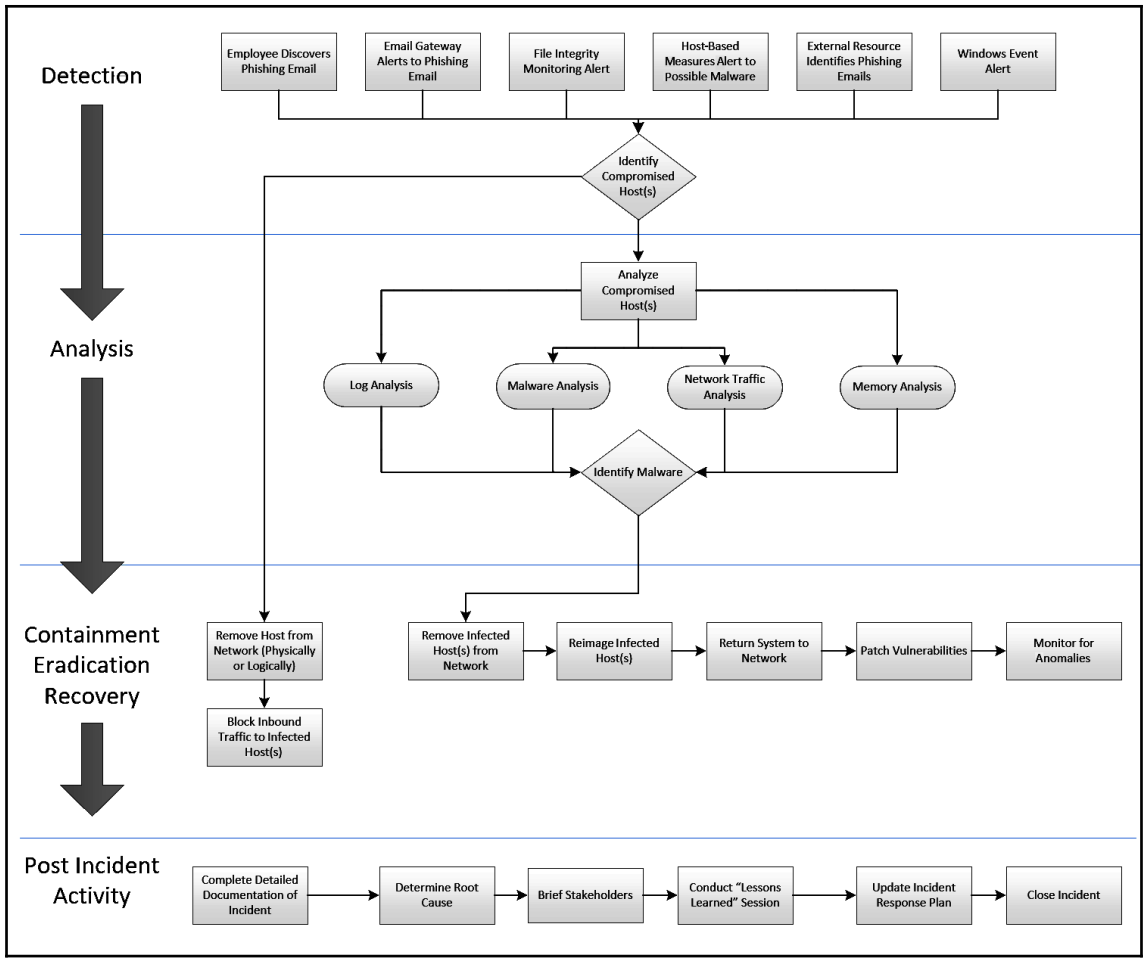
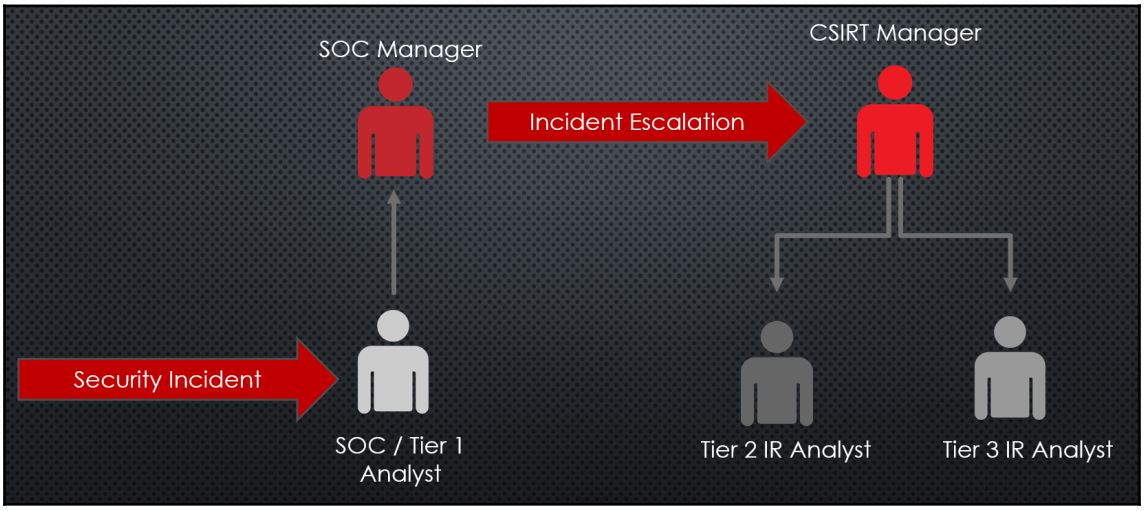
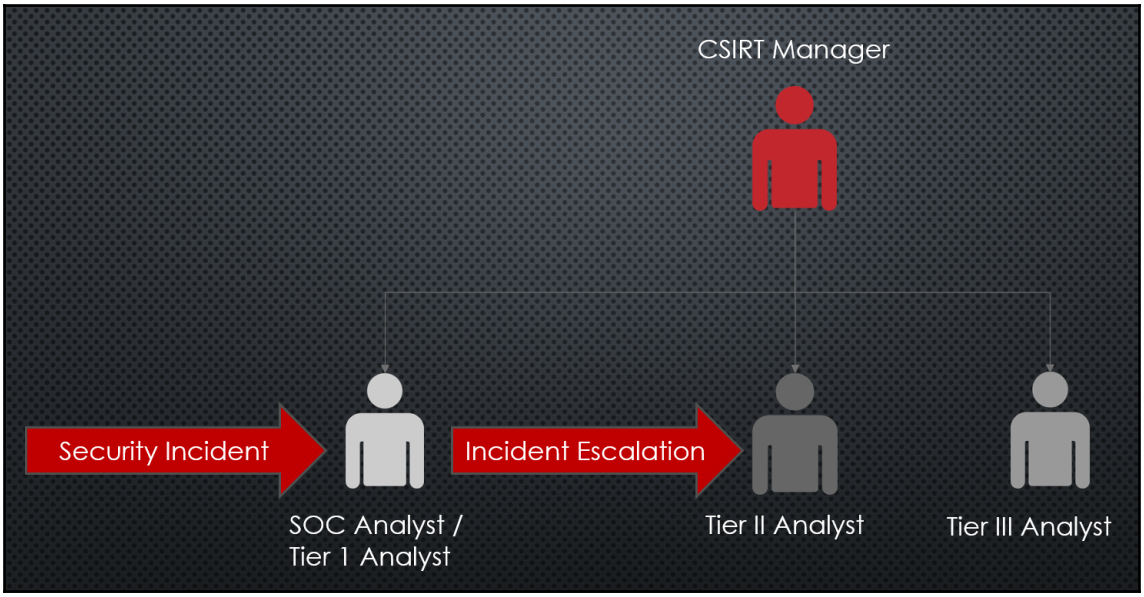
Chapter 1: Understanding Incident Response

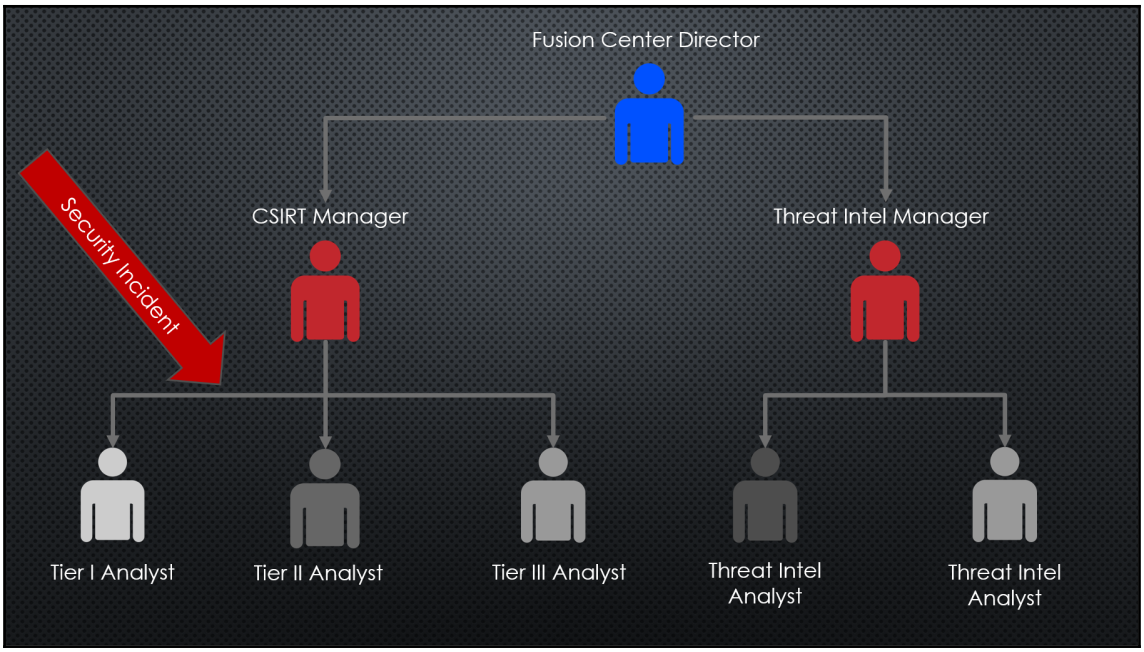



Detection
Employee Discovers Phishing Email
Email Gateway Alerts to Phishing Email
File Integrity Monitoring Alert
Host-Based Measures Alert to Possible Malware
External Resource Identifies Phishing Emails
Windows Event Alert
Identify Compromised Host(s)
Analysis
Analyze Compromised Host(s)
Log Analysis
Malware Analysis
Network Traffic Analysis
Memory Analysis
Identify Malware
Containment Eradication Recovery
Remove Host from Network (Physically or Logically)
Block Inbound Traffic to Infected Host(s)
Remove Infected Host(s) from Network
Reimage Infected Host(s)
Return System to Network
Patch Vulnerabilities
Monitor for Anomalies
Post Incident Activity
Complete Detailed Documentation of Incident
Determine Root Cause
Brief Stakeholders
Conduct "Lessons Learned" Session
Update Incident Response Plan
Close Incident

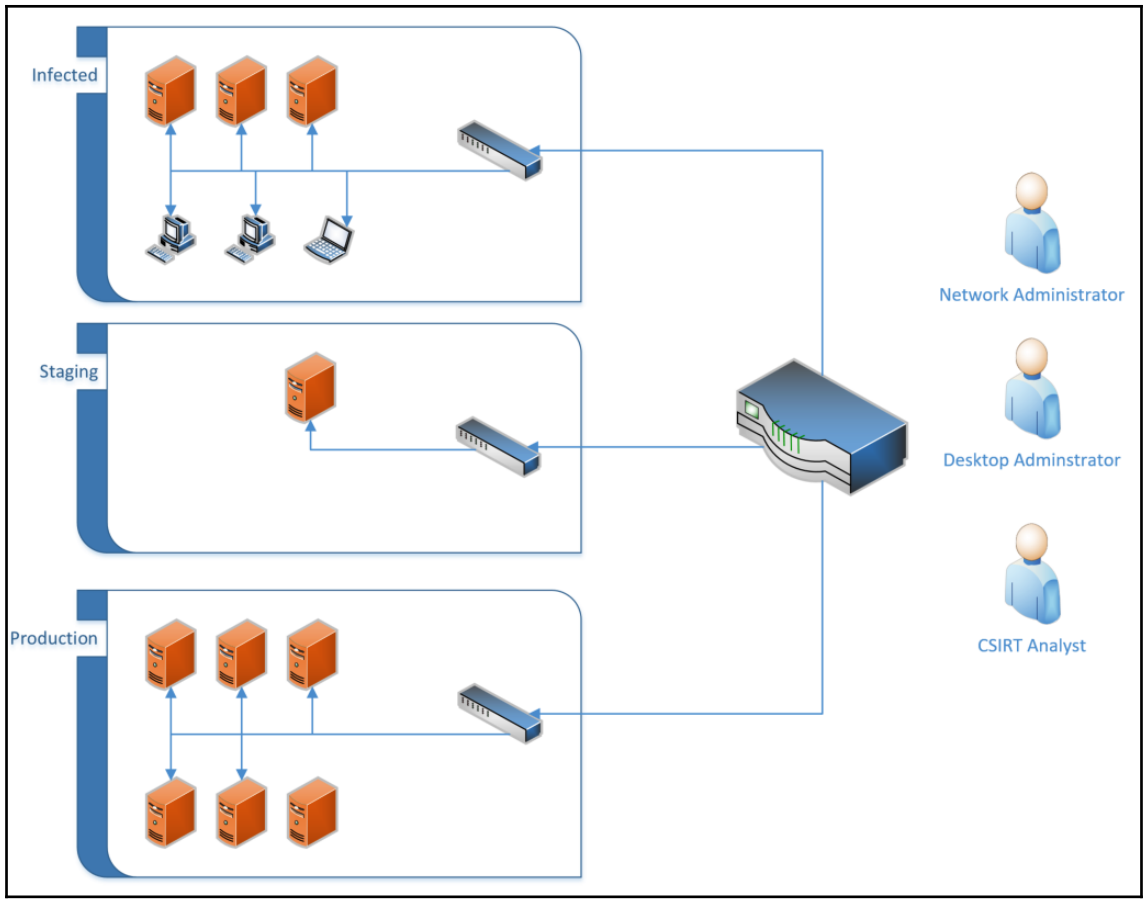
Chapter 2: Managing Cyber Incidents



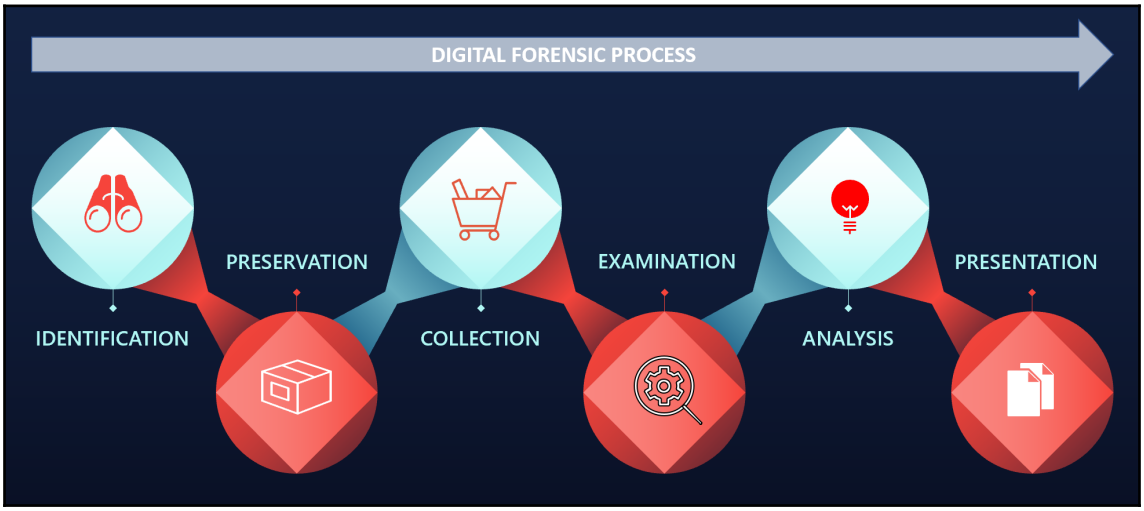



Fusion Center Director
CSIRT Manager
Threat Intel Manager
Security Incident
Tier I Analyst
Tier II Analyst
Tier III Analyst
Threat Intel Analyst
Threat Intel Analyst


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

CSIRT 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:	

Electronic Media Details

Item Number:	Description:		
1	Western Digital WD01EURS Hard Drive		
Manufacturer:		Model#	Serial Number:
Western Digital		WD01EURS	WMAV1234567

Image or File Details

Date / Time Acquired:	Created By:	Method:	Storage Drive:
5/30/19 1224 UTC	Gerard Johansen	Wireshark	USB Drive 1
File/Image Name:		Hash:	
EdgeFirewallCapture.PCAP / Packet Capture		1ceaa2393357d2ed88f81bec1e647af0	

Chain of Custody

Tracking No:	Date/Time:	FROM:	TO:	Reason:
1	Date: 5/30/19	Name/Org: Carol Davies Global Services Corp.	Name/Org: Gerard Johansen IRProactive	Evidence Acquisition
	Time: 1224 UTC	Signature: *Carol Davies*	Signature: *Gerard T Johansen*	
2	Date: 5/30/19	Name/Org: G Johansen IRProactive	Name/Org: David Michell ACME Forensics	Analysis
	Time: 1305 UTC	Signature: *Gerard T Johansen*	Signature: *David Michell*	


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


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


TALINO
FORENSIC WORKSTATIONS
RECON
MAC OS X FORENSICS
CARBON
VIRTUAL FORENSIC SUITE
PALADIN
7
FORENSIC MODE
SUMURI.COM
HONOR - INTEGRITY - COURAGE - LOYALTY - ATTITUDE - DISCIPLINE - SERVICE
SUMURI
Forensics Simplified
App Menu
22 Jan


Ubuntu Desktop
11:55 PM
cases
mount_points
memory-forensics-cheatshe...
network-forensics-cheatshe...
Poster_Find_Evil.pdf
Poster_Hunt_Evil.pdf
Poster_Memory
Poster_Windows_Forensic...
rekall_cheatsheet.pdf
SIFT WORKSTATION CHE...
Smartphone-Forensic...
windows-to-unix-cheatshe...
SIFT
WORKSTATION

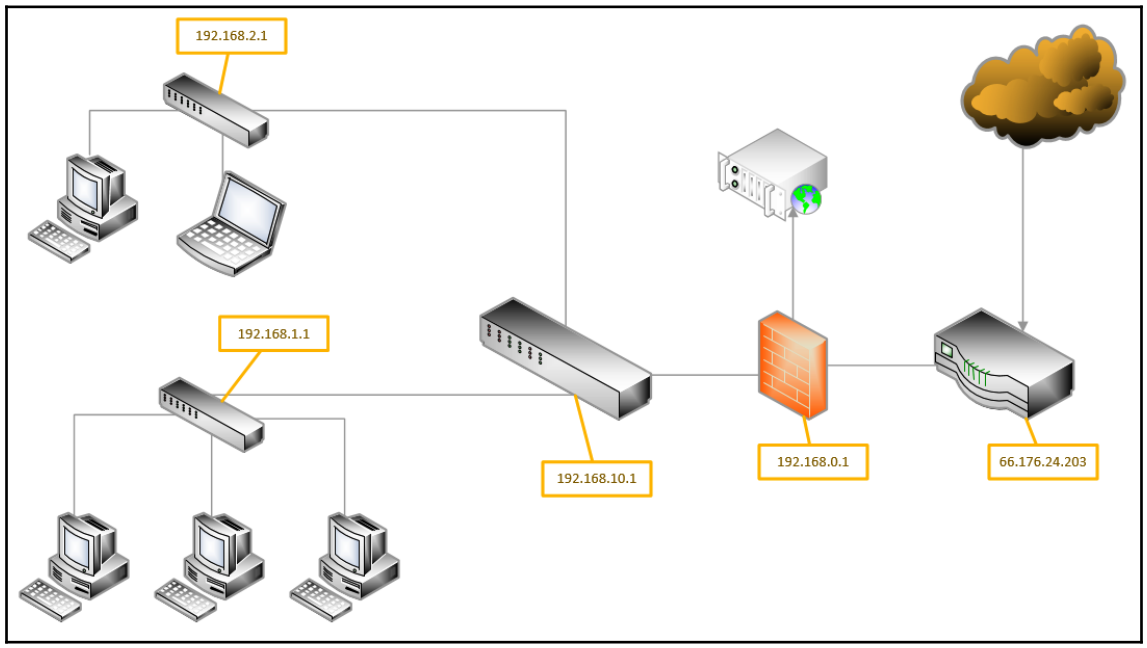

caine's Home
Caja-Root
Mixed scripts
Trash
Disk Image Mounter
Network
Autopsy
INFO
UnBlock
Install 18.04
XAll
Computer
keyboard
Network Servers
INFINITY
CAINE
Computer Aided INvestigative Environment
gio mag 30, 19:48
0 B/s
0 B/s
en

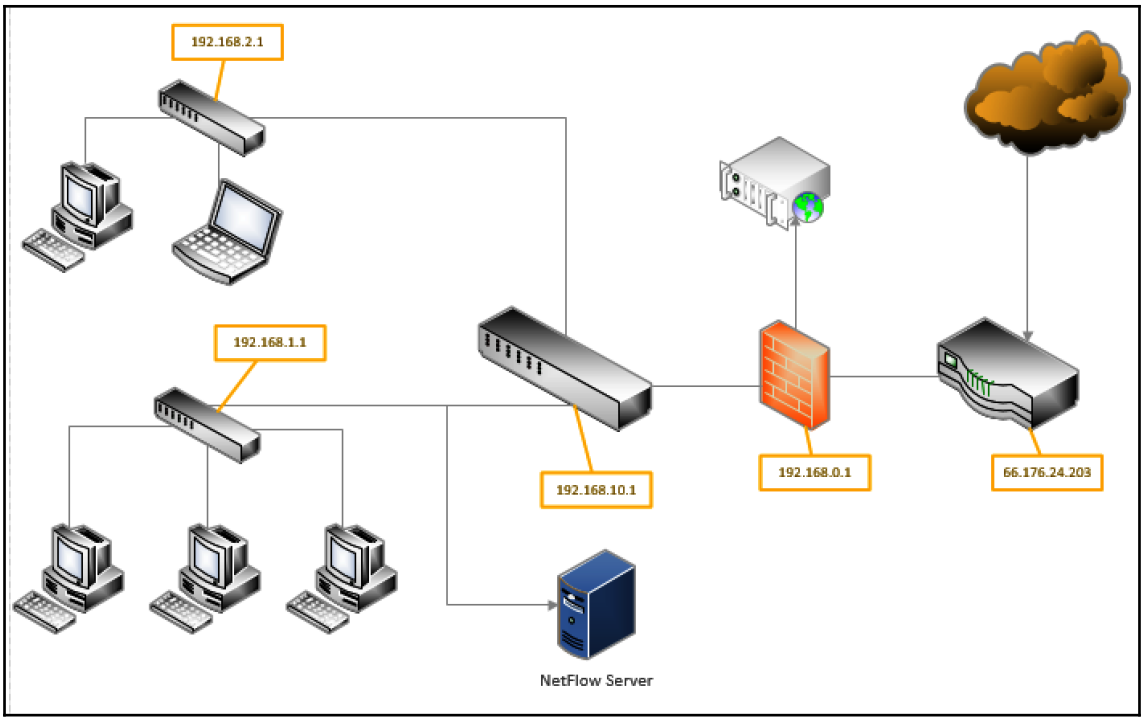

REMnux
Cheat Sheet
REMnux
Docs
REMnux
Tools Sheet
REMnux
21:28


TABLEAU


STANLEY
TAMPER GUARD
EVIDENCE TAPE
THE BEST METHOD FOR SEALING EVIDENCE
nik
Tel: 800.347.1200 • Re-order #B02100
SAFARILAND
STAPLES
Sharpie

Chapter 4: Collecting Network Evidence



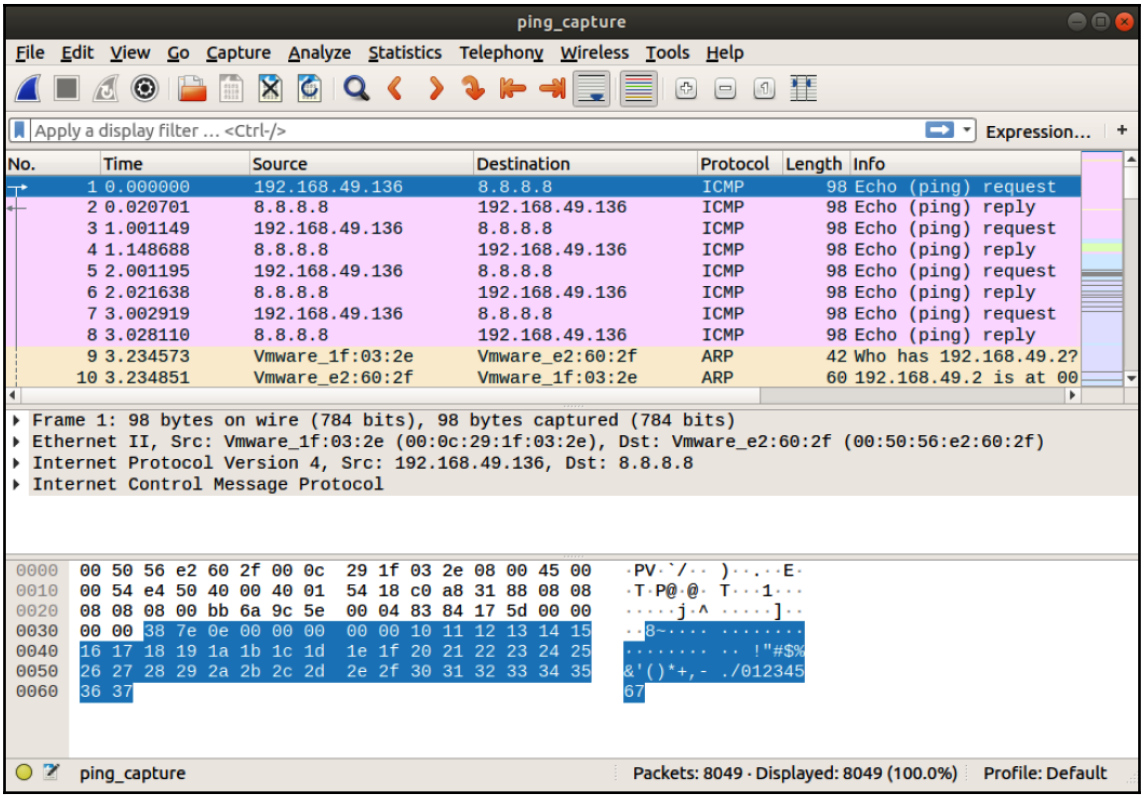



```
File  Edit  View  Search  Terminal  Help
dfir@ubuntu:~$ tcpdump -h
tcpdump version 4.9.2
libpcap version 1.8.1
OpenSSL 1.1.1  11 Sep 2018
Usage: tcpdump [-aAbdDefhHIJKlLnNOpqStuUvxX#] [ -B size ] [ -c count ]
                [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
                [ -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 ]
```

```
File  Edit  View  Search  Terminal  Help
dfir@ubuntu:~$ tcpdump -D
1.ens33 [Up, Running]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.bluetooth0 (Bluetooth adapter number 0)
5.nflog (Linux netfilter log (NFLOG) interface)
6.nfqueue (Linux netfilter queue (NFQUEUE) interface)
7.usbmon1 (USB bus number 1)
8.usbmon2 (USB bus number 2)
```

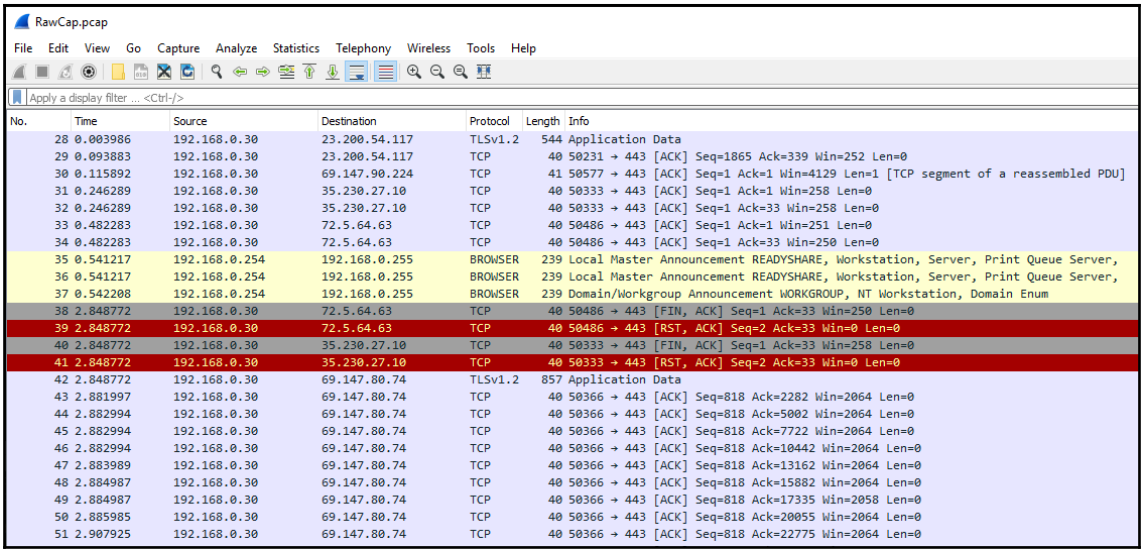
```
File  Edit  View  Search  Terminal  Help
(1), length 84)
    ubuntu > dns.google: ICMP echo request, id 40024, seq 47, length 64
08:31:08.437340 IP (tos 0x0, ttl 128, id 43477, offset 0, flags [none], proto IC
MP (1), length 84)
    dns.google > ubuntu: ICMP echo reply, id 40024, seq 47, length 64
08:31:09.420894 IP (tos 0x0, ttl 64, id 54227, offset 0, flags [DF], proto ICMP
(1), length 84)
    ubuntu > dns.google: ICMP echo request, id 40024, seq 48, length 64
08:31:09.440265 IP (tos 0x0, ttl 128, id 43478, offset 0, flags [none], proto IC
MP (1), length 84)
    dns.google > ubuntu: ICMP echo reply, id 40024, seq 48, length 64
08:31:10.423250 IP (tos 0x0, ttl 64, id 54439, offset 0, flags [DF], proto ICMP
(1), length 84)
    ubuntu > dns.google: ICMP echo request, id 40024, seq 49, length 64
08:31:10.443728 IP (tos 0x0, ttl 128, id 43479, offset 0, flags [none], proto IC
MP (1), length 84)
    dns.google > ubuntu: ICMP echo reply, id 40024, seq 49, length 64
08:31:11.424959 IP (tos 0x0, ttl 64, id 54559, offset 0, flags [DF], proto ICMP
(1), length 84)
```

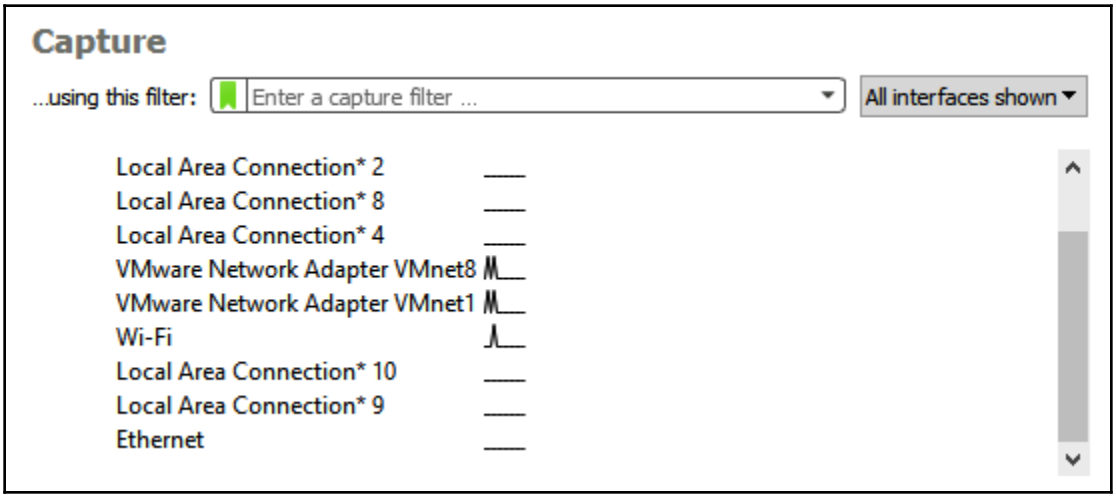
```
dfir@ubuntu:~$ sudo tcpdump -i ens33 -vvv -w ping_capture
tcpdump: listening on ens33, link-type EN10MB (Ethernet), capture size 262144 by
tes
^C4331 packets captured
4333 packets received by filter
0 packets dropped by kernel
```

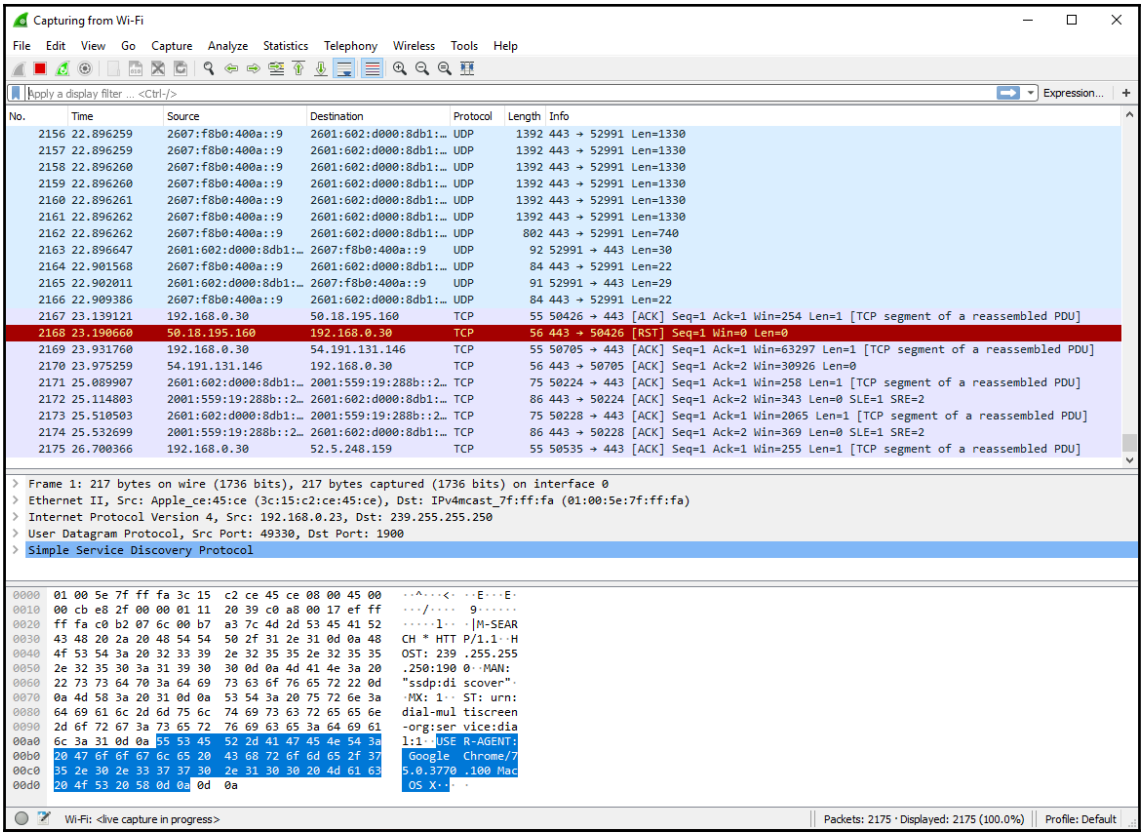

ping_capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.49.136 8.8.8.8 ICMP 98 Echo (ping) request
2 0.020701 8.8.8.8 192.168.49.136 ICMP 98 Echo (ping) 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

```
D:\>RawCap.exe --help
NETRESEC RawCap version 0.1.5.0
http://www.netresec.com

Usage: RawCap.exe [OPTIONS] <interface_nr> <target_pcap_file>

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

INTERFACES:
 0.     IP         : 169.254.166.101
        NIC Name   : Ethernet
        NIC Type   : Ethernet

 1.     IP         : 169.254.172.194
        NIC Name   : Npcap Loopback Adapter
        NIC Type   : Ethernet

 2.     IP         : 169.254.180.113
        NIC Name   : Local Area Connection* 2
        NIC Type   : Wireless80211

 3.     IP         : 192.168.80.1
        NIC Name   : VMware Network Adapter VMnet1
        NIC Type   : Ethernet

 4.     IP         : 192.168.49.1
        NIC Name   : VMware Network Adapter VMnet8
        NIC Type   : Ethernet

 5.     IP         : 192.168.0.30
        NIC Name   : Wi-Fi
        NIC Type   : Wireless80211
```

```
Sniffing IP : 192.168.0.30
File        : RawCap.pcap
Packets     : 4508
```


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
28 0.003986 192.168.0.30 23.200.54.117 TLSv1.2 544 Application Data
29 0.093883 192.168.0.30 23.200.54.117 TCP 40 50231 → 443 [ACK] Seq=1865 Ack=339 Win=252 Len=0
30 0.115892 192.168.0.30 69.147.90.224 TCP 41 50577 → 443 [ACK] Seq=1 Ack=1 Win=4129 Len=1 [TCP segment of a reassembled PDU]
31 0.246289 192.168.0.30 35.230.27.10 TCP 40 50333 → 443 [ACK] Seq=1 Ack=1 Win=258 Len=0
32 0.246289 192.168.0.30 35.230.27.10 TCP 40 50333 → 443 [ACK] Seq=1 Ack=33 Win=258 Len=0
33 0.482283 192.168.0.30 72.5.64.63 TCP 40 50486 → 443 [ACK] Seq=1 Ack=1 Win=251 Len=0
34 0.482283 192.168.0.30 72.5.64.63 TCP 40 50486 → 443 [ACK] Seq=1 Ack=33 Win=250 Len=0
35 0.541217 192.168.0.254 192.168.0.255 BROWSER 239 Local Master Announcement READYSHARE, Workstation, Server, Print Queue Server,
36 0.541217 192.168.0.254 192.168.0.255 BROWSER 239 Local Master Announcement READYSHARE, Workstation, Server, Print Queue Server,
37 0.542208 192.168.0.254 192.168.0.255 BROWSER 239 Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
38 2.848772 192.168.0.30 72.5.64.63 TCP 40 50486 → 443 [FIN, ACK] Seq=1 Ack=33 Win=250 Len=0
39 2.848772 192.168.0.30 72.5.64.63 TCP 40 50486 → 443 [RST, ACK] Seq=2 Ack=33 Win=0 Len=0
40 2.848772 192.168.0.30 35.230.27.10 TCP 40 50333 → 443 [FIN, ACK] Seq=1 Ack=33 Win=258 Len=0
41 2.848772 192.168.0.30 35.230.27.10 TCP 40 50333 → 443 [RST, ACK] Seq=2 Ack=33 Win=0 Len=0
42 2.848772 192.168.0.30 69.147.80.74 TLSv1.2 857 Application Data
43 2.881997 192.168.0.30 69.147.80.74 TCP 40 50366 → 443 [ACK] Seq=818 Ack=2282 Win=2064 Len=0
44 2.882994 192.168.0.30 69.147.80.74 TCP 40 50366 → 443 [ACK] Seq=818 Ack=5002 Win=2064 Len=0
45 2.882994 192.168.0.30 69.147.80.74 TCP 40 50366 → 443 [ACK] Seq=818 Ack=7722 Win=2064 Len=0
46 2.882994 192.168.0.30 69.147.80.74 TCP 40 50366 → 443 [ACK] Seq=818 Ack=10442 Win=2064 Len=0
47 2.883989 192.168.0.30 69.147.80.74 TCP 40 50366 → 443 [ACK] Seq=818 Ack=13162 Win=2064 Len=0
48 2.884987 192.168.0.30 69.147.80.74 TCP 40 50366 → 443 [ACK] Seq=818 Ack=15882 Win=2064 Len=0
49 2.884987 192.168.0.30 69.147.80.74 TCP 40 50366 → 443 [ACK] Seq=818 Ack=17335 Win=2058 Len=0
50 2.885985 192.168.0.30 69.147.80.74 TCP 40 50366 → 443 [ACK] Seq=818 Ack=20055 Win=2064 Len=0
51 2.907925 192.168.0.30 69.147.80.74 TCP 40 50366 → 443 [ACK] Seq=818 Ack=22775 Win=2064 Len=0


Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Local Area Connection* 2
Local Area Connection* 8
Local Area Connection* 4
VMware Network Adapter VMnet8
VMware Network Adapter VMnet1
Wi-Fi
Local Area Connection* 10
Local Area Connection* 9
Ethernet


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
2156 22.896259 2607:f8b0:400a::9 2601:602:d000:8db1:... UDP 1392 443 → 52991 Len=1330
2157 22.896259 2607:f8b0:400a::9 2601:602:d000:8db1:... UDP 1392 443 → 52991 Len=1330
2158 22.896260 2607:f8b0:400a::9 2601:602:d000:8db1:... UDP 1392 443 → 52991 Len=1330
2159 22.896260 2607:f8b0:400a::9 2601:602:d000:8db1:... UDP 1392 443 → 52991 Len=1330
2160 22.896261 2607:f8b0:400a::9 2601:602:d000:8db1:... UDP 1392 443 → 52991 Len=1330
2161 22.896262 2607:f8b0:400a::9 2601:602:d000:8db1:... UDP 1392 443 → 52991 Len=1330
2162 22.896262 2607:f8b0:400a::9 2601:602:d000:8db1:... UDP 802 443 → 52991 Len=740
2163 22.896647 2601:602:d000:8db1:... 2607:f8b0:400a::9 UDP 92 52991 → 443 Len=30
2164 22.901568 2607:f8b0:400a::9 2601:602:d000:8db1:... UDP 84 443 → 52991 Len=22
2165 22.902011 2601:602:d000:8db1:... 2607:f8b0:400a::9 UDP 91 52991 → 443 Len=29
2166 22.909386 2607:f8b0:400a::9 2601:602:d000:8db1:... UDP 84 443 → 52991 Len=22
2167 23.139121 192.168.0.30 50.18.195.160 TCP 55 50426 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1 [TCP segment of a reassembled PDU]
2168 23.190660 50.18.195.160 192.168.0.30 TCP 56 443 → 50426 [RST] Seq=1 Win=0 Len=0
2169 23.931760 192.168.0.30 54.191.131.146 TCP 55 50705 → 443 [ACK] Seq=1 Ack=1 Win=63297 Len=1 [TCP segment of a reassembled PDU]
2170 23.975259 54.191.131.146 192.168.0.30 TCP 56 443 → 50705 [ACK] Seq=1 Ack=2 Win=30926 Len=0
2171 25.089907 2601:602:d000:8db1:... 2001:559:19:288b::2... TCP 75 50224 → 443 [ACK] Seq=1 Ack=1 Win=258 Len=1 [TCP segment of a reassembled PDU]
2172 25.114803 2001:559:19:288b::2... 2601:602:d000:8db1:... TCP 86 443 → 50224 [ACK] Seq=1 Ack=2 Win=343 Len=0 SLE=1 SRE=2
2173 25.510503 2601:602:d000:8db1:... 2001:559:19:288b::2... TCP 75 50228 → 443 [ACK] Seq=1 Ack=1 Win=2065 Len=1 [TCP segment of a reassembled PDU]
2174 25.532699 2001:559:19:288b::2... 2601:602:d000:8db1:... TCP 86 443 → 50228 [ACK] Seq=1 Ack=2 Win=369 Len=0 SLE=1 SRE=2
2175 26.700366 192.168.0.30 52.5.248.159 TCP 55 50535 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1 [TCP segment of a reassembled PDU]
Frame 1: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface 0
Ethernet II, Src: Apple_ce:45:ce (3c:15:c2:ce:45:ce), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Internet Protocol Version 4, Src: 192.168.0.23, Dst: 239.255.255.250
User Datagram Protocol, Src Port: 49330, Dst Port: 1900
Simple Service Discovery Protocol
0000 01 00 5e 7f ff fa 3c 15 c2 ce 45 ce 08 00 45 00
0010 00 cb e8 2f 00 00 01 11 20 39 c0 a8 00 17 ef ff
0020 ff fa c0 b2 07 6c 00 b7 a3 7c 4d 2d 53 45 41 52
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48
0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35
0050 2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20
0060 22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d
0070 0a 4d 58 3a 20 31 0d 0a 53 54 3a 20 75 72 6e 3a
0080 64 69 61 6c 2d 6d 75 6c 74 69 73 63 72 65 65 6e
0090 2d 6f 72 67 3a 73 65 72 76 69 63 65 3a 64 69 61
00a0 6c 3a 31 0d 0a 55 53 45 52 2d 41 47 45 4e 54 3a
00b0 20 47 6f 6f 67 6c 65 20 43 68 72 6f 6d 65 2f 37
00c0 35 2e 30 2e 33 37 37 30 2e 31 30 30 20 4d 61 63
00d0 20 4f 53 20 58 0d 0a 0d 0a
Wi-Fi: <live capture in progress>
Packets: 2175 · Displayed: 2175 (100.0%)
Profile: Default

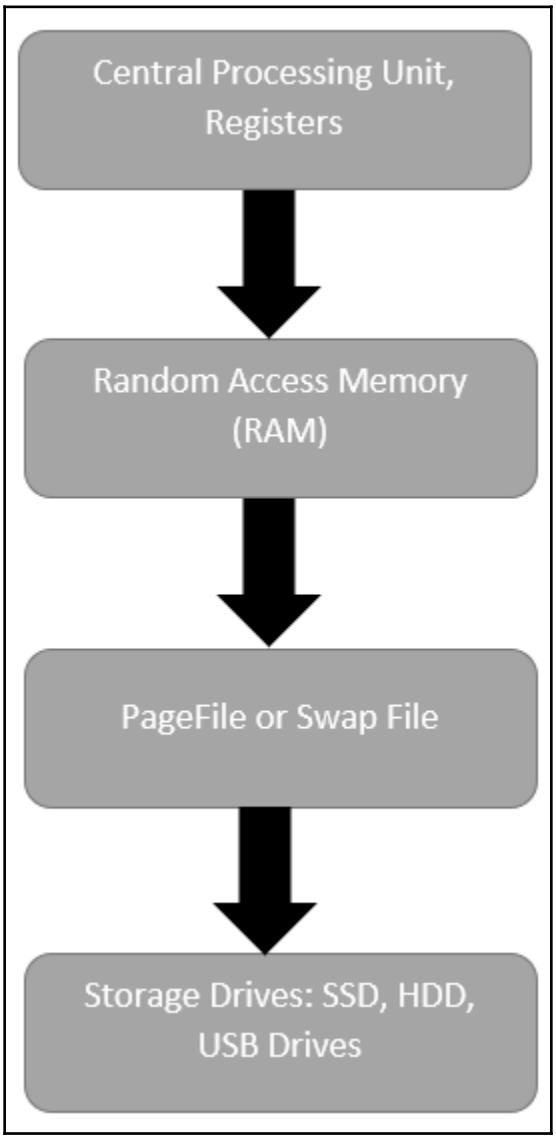
```
File  Edit  View  Search  Terminal  Help
dfir@ubuntu:~$ mergecap -help
Mergecap (Wireshark) 2.6.8 (Git v2.6.8 packaged as 2.6.8-1~ubuntu18.04.0)
Merge two or more capture files into one.
See https://www.wireshark.org for more information.

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; defau
lt is 'all'.
                      an empty "-I" option will list the merge modes.

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

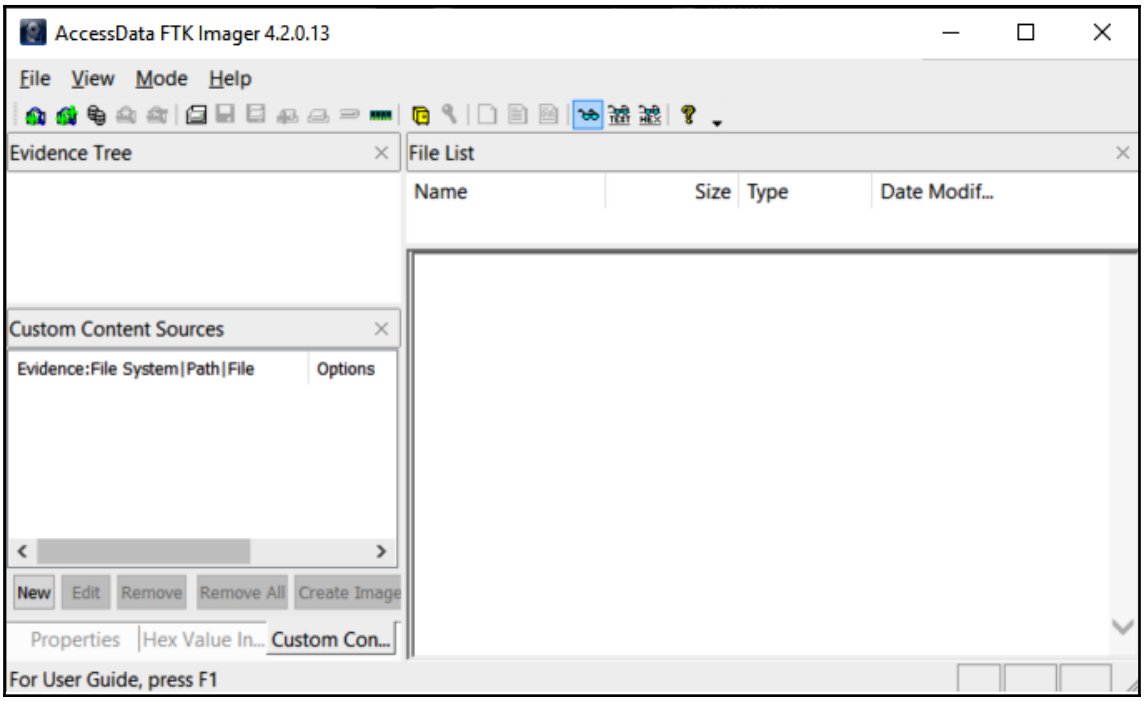
File Name	Description	Location	Date	Time	Collected By	MD5 Hash
Ping_capture	Packet Capture of Ping activity	192.168.2.1	6/26/19	1642	GTJ	7e559dc8eeeb66115566d93f96e7dfb8

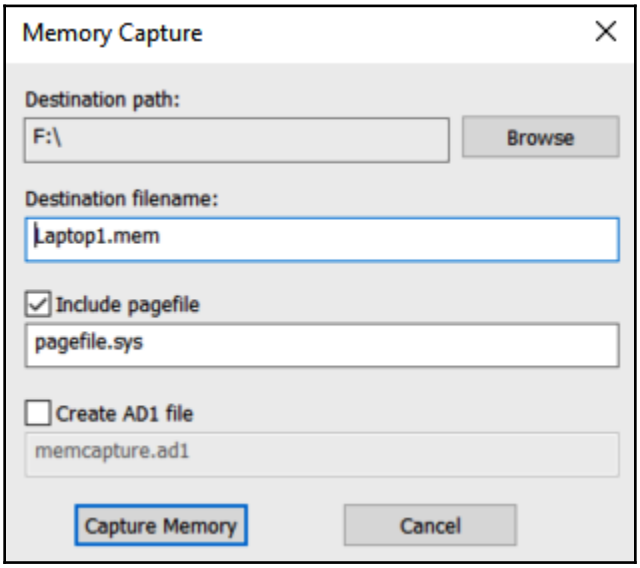
```
File  Edit  View  Search  Terminal  Help
dfir@ubuntu:~$ md5sum --help
Usage: md5sum [OPTION]... [FILE]...
Print or check MD5 (128-bit) checksums.

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)

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

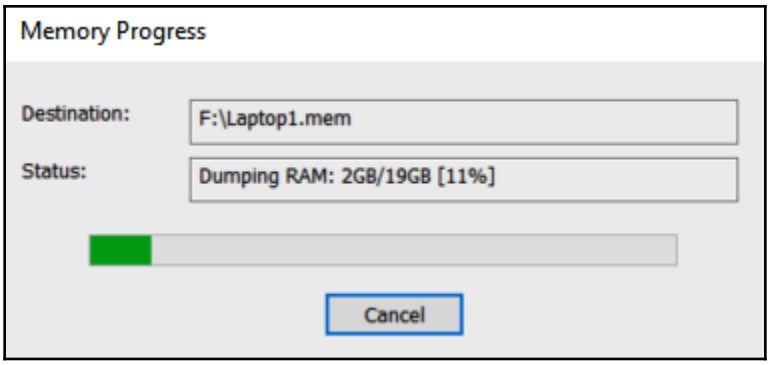
```
dfir@ubuntu: ~
File  Edit  View  Search  Terminal  Help
dfir@ubuntu:~$ md5sum ping_capture
7e559dc8eeeb66115566d93f96e7dfb8  ping_capture
```

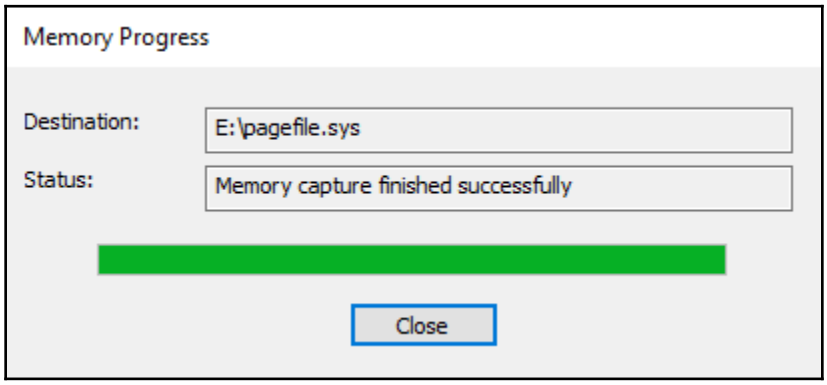
Chapter 5: Acquiring Host-Based Evidence




AccessData FTK Imager 4.2.0.13
File View Mode Help
Evidence Tree
File List
Name
Size
Type
Date Modif...
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:
F:\
Browse
Destination filename:
Laptop1.mem
Include pagefile
pagefile.sys
Create AD1 file
memcapture.ad1
Capture Memory
Cancel



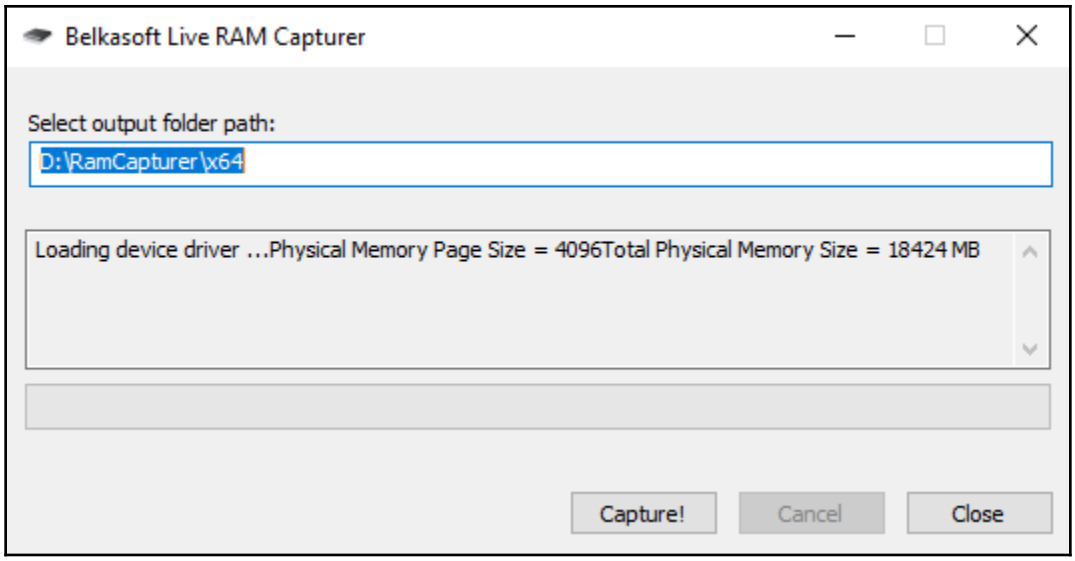


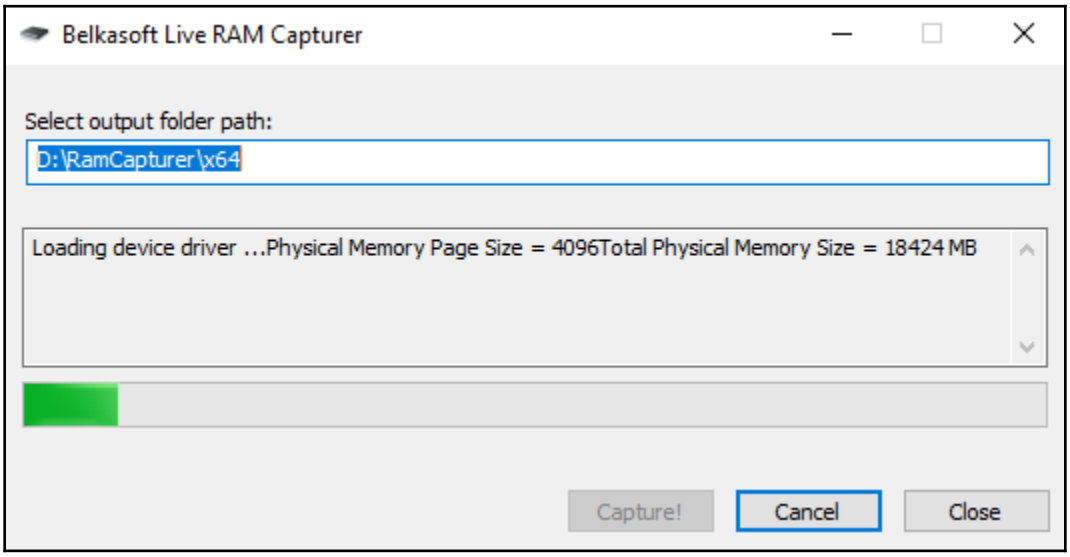
Name	Date modified	Type	Size
FTK Imager	7/28/2019 8:33 AM	File folder	
Acct_098_LT.mem	7/28/2019 8:41 AM	MEM File	2,097,152 KB
pagefile.sys	7/28/2019 8:42 AM	System file	1,179,648 KB

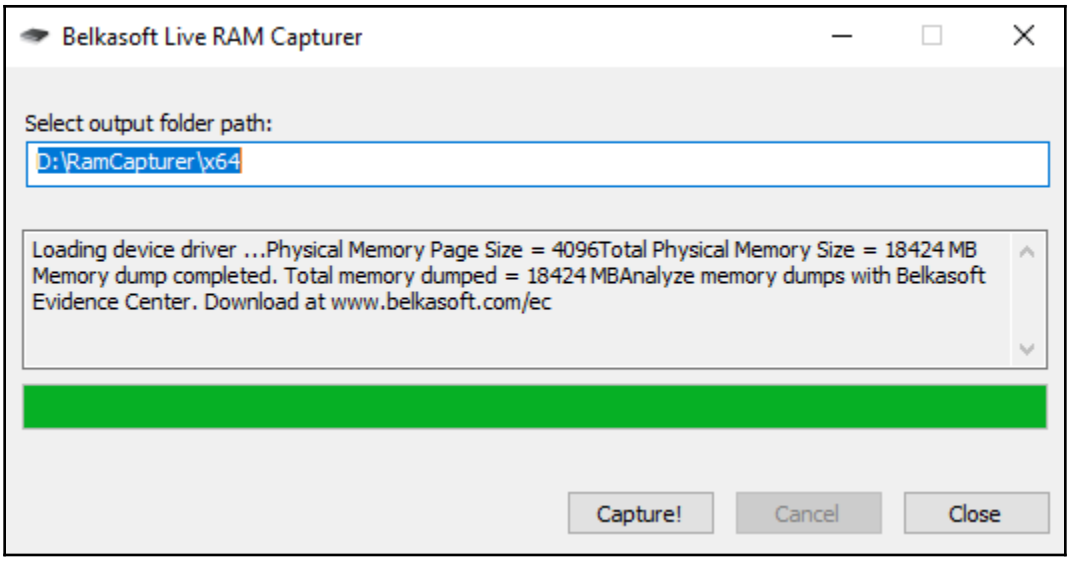
```
D:\>winpmem-2.1.exe -h

USAGE:

   winpmem-2.1.exe  [-l] [-u] [--write-mode] [--mode <MmMapIoSpace,
                    PhysicalMemory, PTERemapping>] [--driver <Path to
                    driver.>] [--format <map, elf, raw>] [-m] [-p
                    </path/to/pagefile>] ...  [-V] [-d] [-v] [-t] [-i
                    </path/to/file/or/device>] ...  [-e <string>] [-o
                    </path/to/file>] [-c <zlib, snappy, none>] [--]
                    [--version] [-h] </path/to/aff4/volume> ...
```

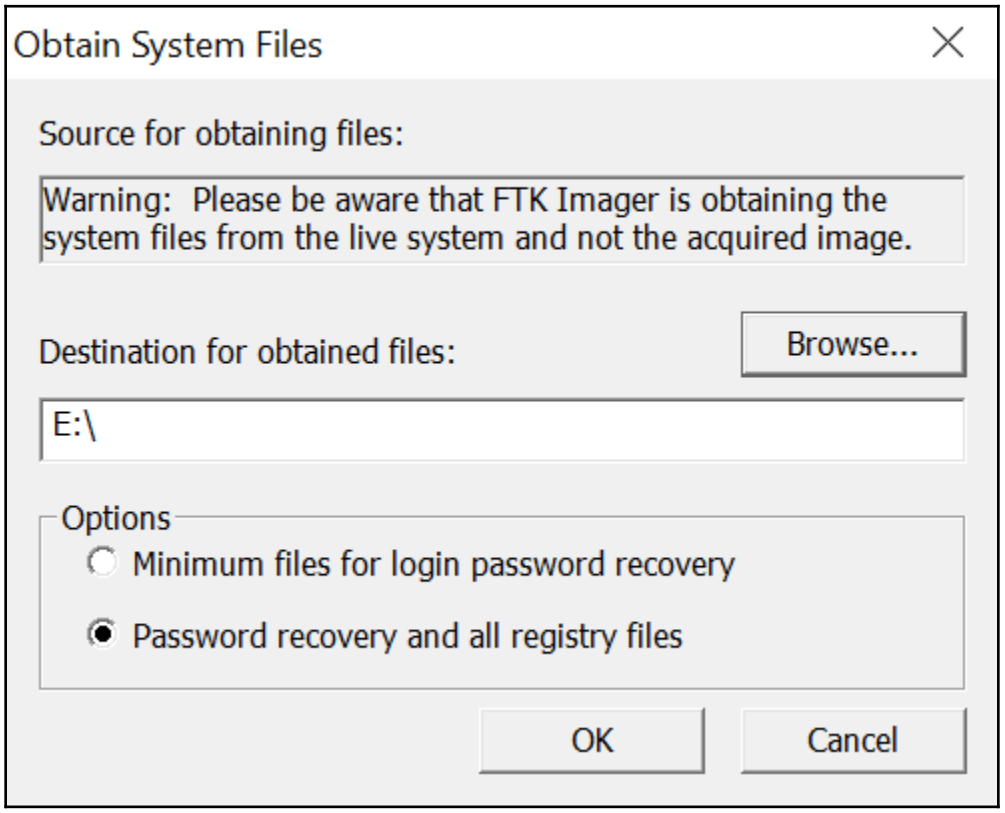
```
D:\>winpmem-2.1.exe --format raw -o e:\Laptop1
Driver Unloaded.
CR3: 0x00001AA000
 7 memory ranges:
Start 0x00001000 - Length 0x0009C000
Start 0x00100000 - Length 0x00002000
Start 0x00103000 - Length 0xBE2FE000
Start 0xBE889000 - Length 0x1BD7E000
Start 0xDA770000 - Length 0x00775000
Start 0xDBAFF000 - Length 0x00001000
Start 0x100000000 - Length 0x31E800000
```

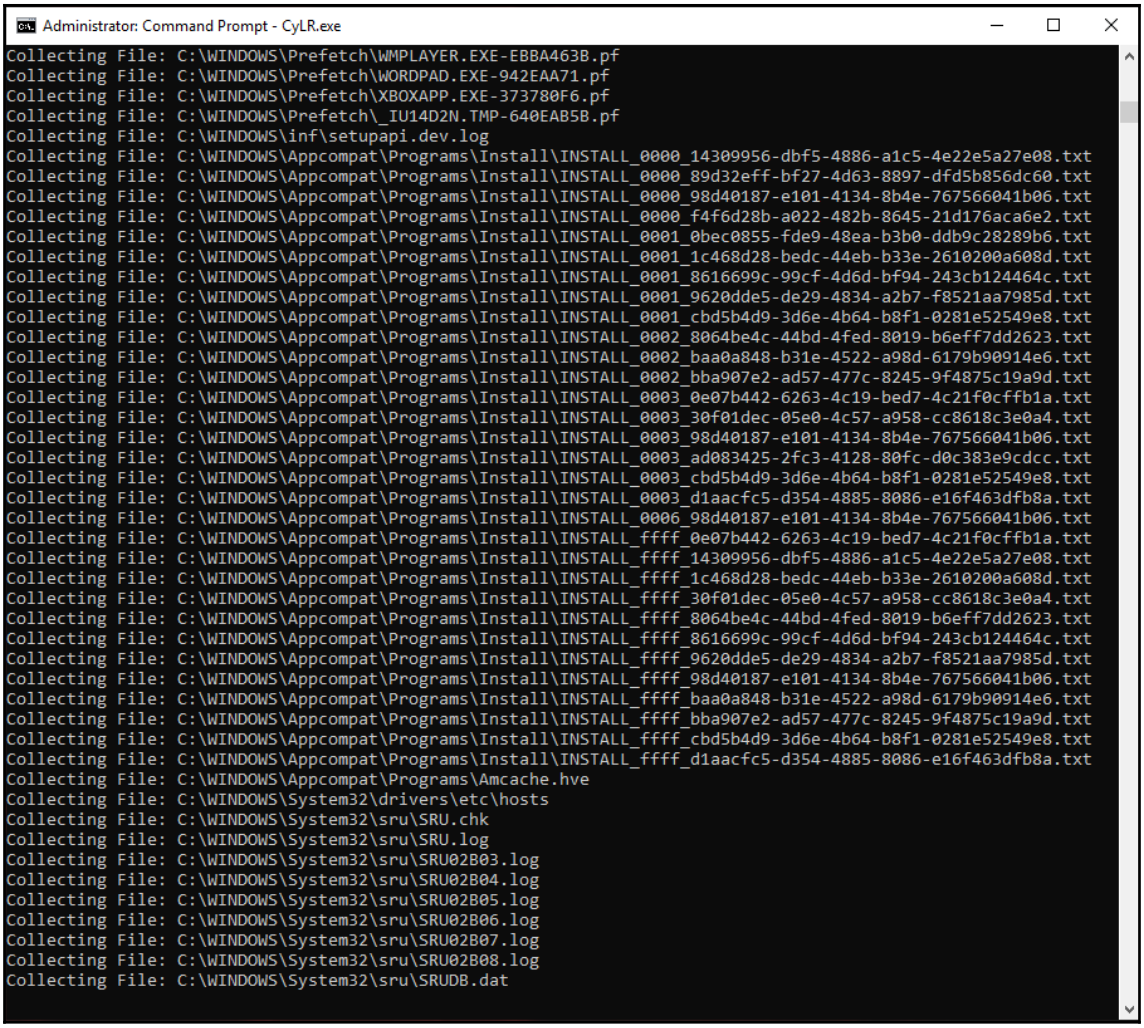
```
Creating output AFF4 Directory structure.
Dumping Range 0 (Starts at 1000, length 9c000)
Dumping Range 1 (Starts at 100000, length 2000)
Dumping Range 2 (Starts at 103000, length be2fe000)
Dumping Range 3 (Starts at be889000, length 1bd7e000)
Dumping Range 4 (Starts at da770000, length 775000)
Dumping Range 5 (Starts at dbaff000, length 1000)
Dumping Range 6 (Starts at 100000000, length 31e800000)
 Reading 0x8000  0MiB / 16272MiB 0MiB/s
 Reading 0x4398000  67MiB / 16272MiB 255MiB/s
 Reading 0x89b0000  137MiB / 16272MiB 275MiB/s
 Reading 0xd288000  210MiB / 16272MiB 276MiB/s
 Reading 0x11858000  280MiB / 16272MiB 274MiB/s
 Reading 0x15f48000  351MiB / 16272MiB 283MiB/s
 Reading 0x1a998000  425MiB / 16272MiB 295MiB/s
 Reading 0x1f3f0000  499MiB / 16272MiB 296MiB/s
 Reading 0x23cb8000  572MiB / 16272MiB 289MiB/s
 Reading 0x283c8000  643MiB / 16272MiB 283MiB/s
 Reading 0x2cb68000  715MiB / 16272MiB 285MiB/s
 Reading 0x310d0000  784MiB / 16272MiB 276MiB/s
 Reading 0x346f8000  838MiB / 16272MiB 206MiB/s
 Reading 0x38c70000  908MiB / 16272MiB 276MiB/s
 Reading 0x3cbe8000  971MiB / 16272MiB 252MiB/s
 Reading 0x41240000  1042MiB / 16272MiB 280MiB/s
 Reading 0x45580000  1109MiB / 16272MiB 267MiB/s
```

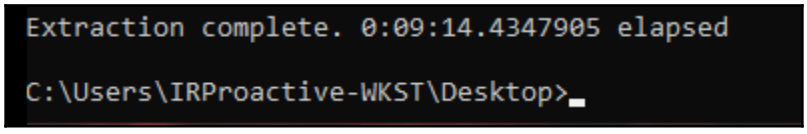

Belkasoft Live RAM Capturer
Select output folder path:
D:\RamCapturer\x64
Loading device driver ...Physical Memory Page Size = 4096Total Physical Memory Size = 18424 MB
Capture!
Cancel
Close

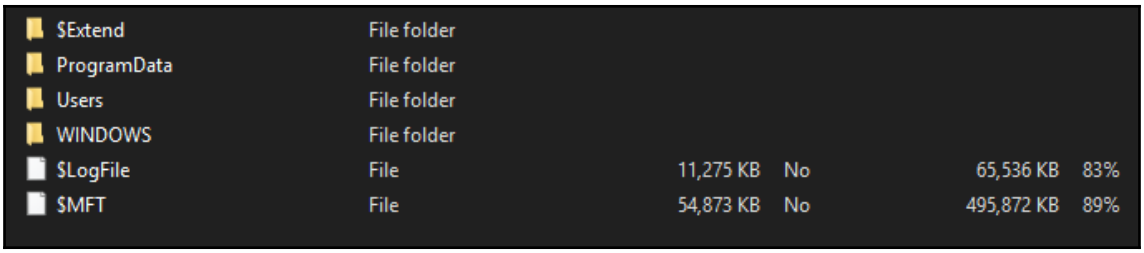

Belkasoft Live RAM Capturer
Select output folder path:
D:\RamCapturer\x64
Loading device driver ...Physical Memory Page Size = 4096Total Physical Memory Size = 18424 MB
Capture!
Cancel
Close


Belkasoft Live RAM Capturer
Select output folder path:
D:\RamCapturer\x64
Loading device driver ...Physical Memory Page Size = 4096Total Physical Memory Size = 18424 MB
Memory dump completed. Total memory dumped = 18424 MBAnalyze memory dumps with Belkasoft Evidence Center. Download at www.belkasoft.com/ec
Capture!
Cancel
Close

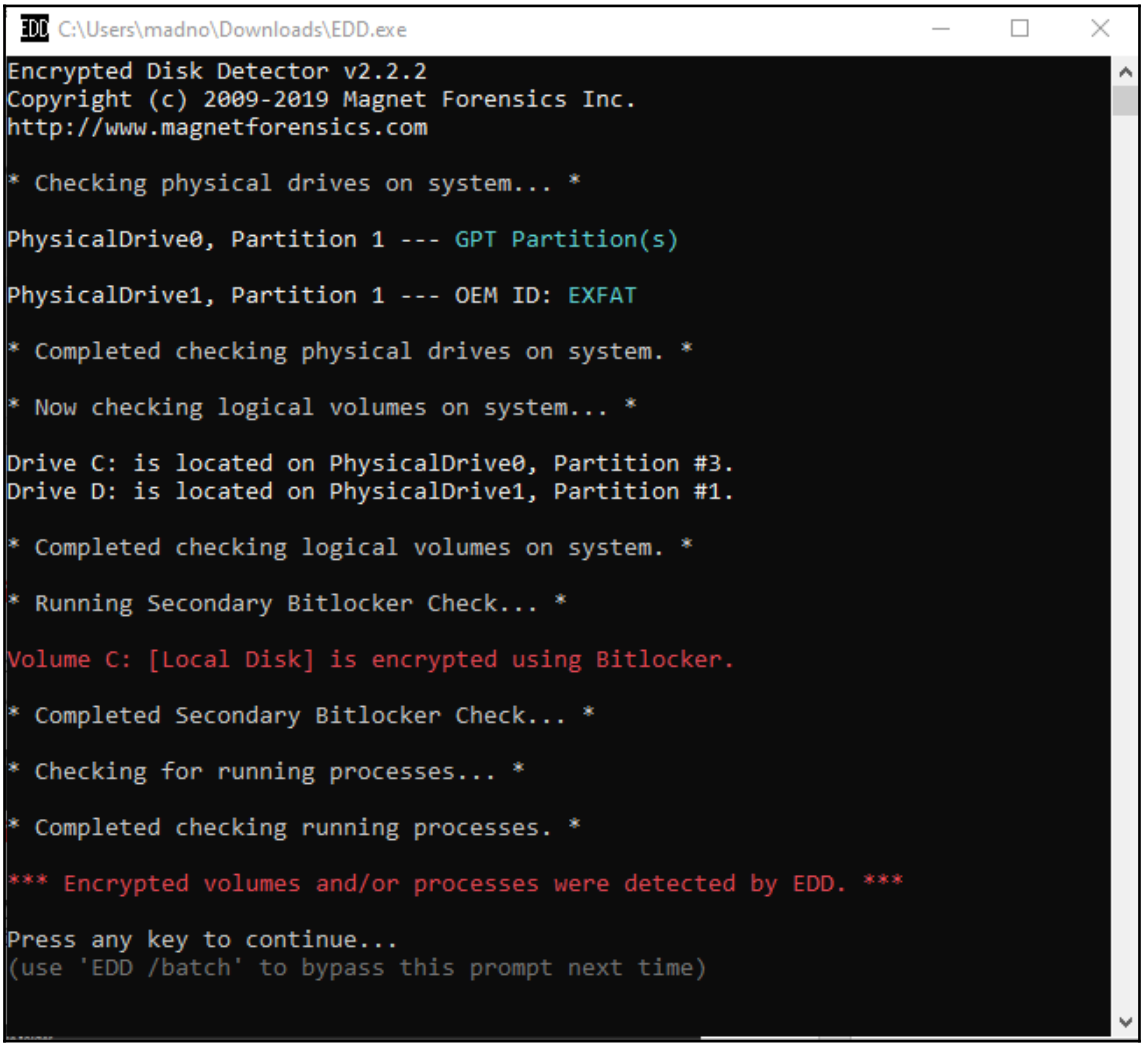

Obtain System Files
Source for obtaining files:
Warning: Please be aware that FTK Imager is obtaining the system files from the live system and not the acquired image.
Destination for obtained files:
Browse...
E:\
Options
Minimum files for login password recovery
Password recovery and all registry files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


Administrator: Command Prompt - CyLR.exe
Collecting File: C:\WINDOWS\Prefetch\WMPLAYER.EXE-EBBA463B.pf
Collecting File: C:\WINDOWS\Prefetch\WORDPAD.EXE-942EAA71.pf
Collecting File: C:\WINDOWS\Prefetch\XBOXAPP.EXE-373780F6.pf
Collecting File: C:\WINDOWS\Prefetch_IU14D2N.TMP-640EAB5B.pf
Collecting File: C:\WINDOWS\inf\setupapi.dev.log
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_0000_14309956-dbf5-4886-a1c5-4e22e5a27e08.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_0000_89d32eff-bf27-4d63-8897-dfd5b856dc60.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_0000_98d40187-e101-4134-8b4e-767566041b06.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_0000_f4f6d28b-a022-482b-8645-21d176aca6e2.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_0001_0bec0855-fde9-48ea-b3b0-ddb9c28289b6.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_0001_1c468d28-bedc-44eb-b33e-2610200a608d.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_0001_8616699c-99cf-4d6d-bf94-243cb124464c.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_0001_9620dde5-de29-4834-a2b7-f8521aa7985d.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_0001_cbd5b4d9-3d6e-4b64-b8f1-0281e52549e8.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_0002_8064be4c-44bd-4fed-8019-b6eff7dd2623.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_0002_baa0a848-b31e-4522-a98d-6179b90914e6.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_0002_bba907e2-ad57-477c-8245-9f4875c19a9d.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_0003_0e07b442-6263-4c19-bed7-4c21f0cffb1a.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_0003_30f01dec-05e0-4c57-a958-cc8618c3e0a4.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_0003_98d40187-e101-4134-8b4e-767566041b06.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_0003_ad083425-2fc3-4128-80fc-d0c383e9cdcc.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_0003_cbd5b4d9-3d6e-4b64-b8f1-0281e52549e8.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_0003_d1aacfc5-d354-4885-8086-e16f463dfb8a.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_0006_98d40187-e101-4134-8b4e-767566041b06.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_ffff_0e07b442-6263-4c19-bed7-4c21f0cffb1a.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_ffff_14309956-dbf5-4886-a1c5-4e22e5a27e08.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_ffff_1c468d28-bedc-44eb-b33e-2610200a608d.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_ffff_30f01dec-05e0-4c57-a958-cc8618c3e0a4.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_ffff_8064be4c-44bd-4fed-8019-b6eff7dd2623.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_ffff_8616699c-99cf-4d6d-bf94-243cb124464c.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_ffff_9620dde5-de29-4834-a2b7-f8521aa7985d.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_ffff_98d40187-e101-4134-8b4e-767566041b06.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_ffff_baa0a848-b31e-4522-a98d-6179b90914e6.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_ffff_bba907e2-ad57-477c-8245-9f4875c19a9d.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_ffff_cbd5b4d9-3d6e-4b64-b8f1-0281e52549e8.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Install\INSTALL_ffff_d1aacfc5-d354-4885-8086-e16f463dfb8a.txt
Collecting File: C:\WINDOWS\Appcompat\Programs\Amcache.hve
Collecting File: C:\WINDOWS\System32\drivers\etc\hosts
Collecting File: C:\WINDOWS\System32\sru\SRU.chk
Collecting File: C:\WINDOWS\System32\sru\SRU.log
Collecting File: C:\WINDOWS\System32\sru\SRU02B03.log
Collecting File: C:\WINDOWS\System32\sru\SRU02B04.log
Collecting File: C:\WINDOWS\System32\sru\SRU02B05.log
Collecting File: C:\WINDOWS\System32\sru\SRU02B06.log
Collecting File: C:\WINDOWS\System32\sru\SRU02B07.log
Collecting File: C:\WINDOWS\System32\sru\SRU02B08.log
Collecting File: C:\WINDOWS\System32\sru\SRUDB.dat

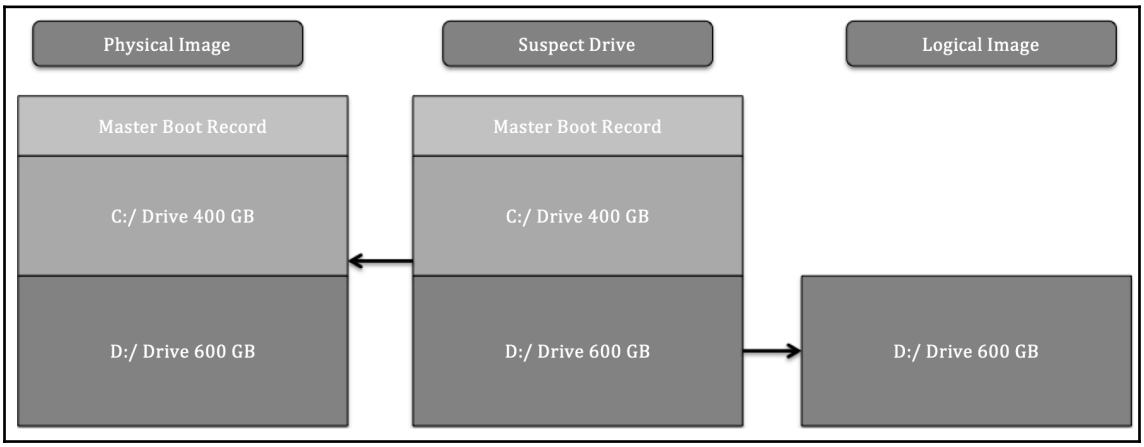

Extraction complete. 0:09:14.4347905 elapsed
C:\Users\IRProactive-WKST\Desktop>



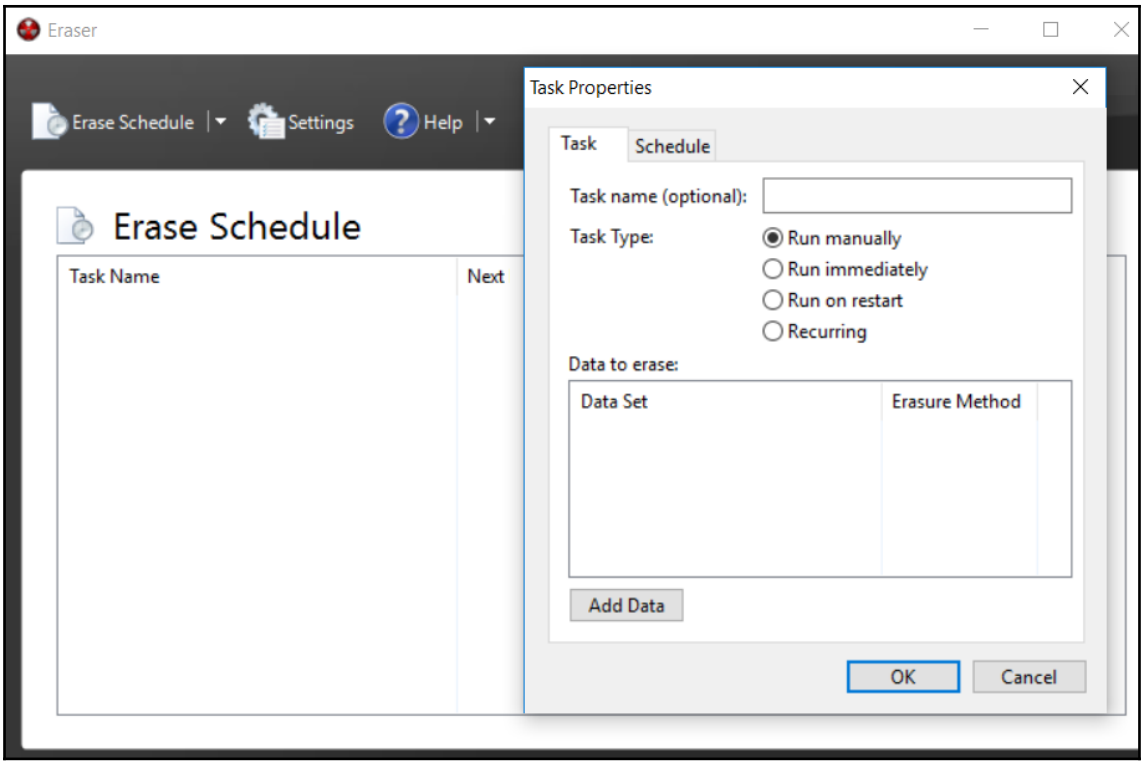
$Extend	File folder				
ProgramData	File folder				
Users	File folder				
WINDOWS	File folder				
$LogFile	File	11,275 KB	No	65,536 KB	83%
$MFT	File	54,873 KB	No	495,872 KB	89%

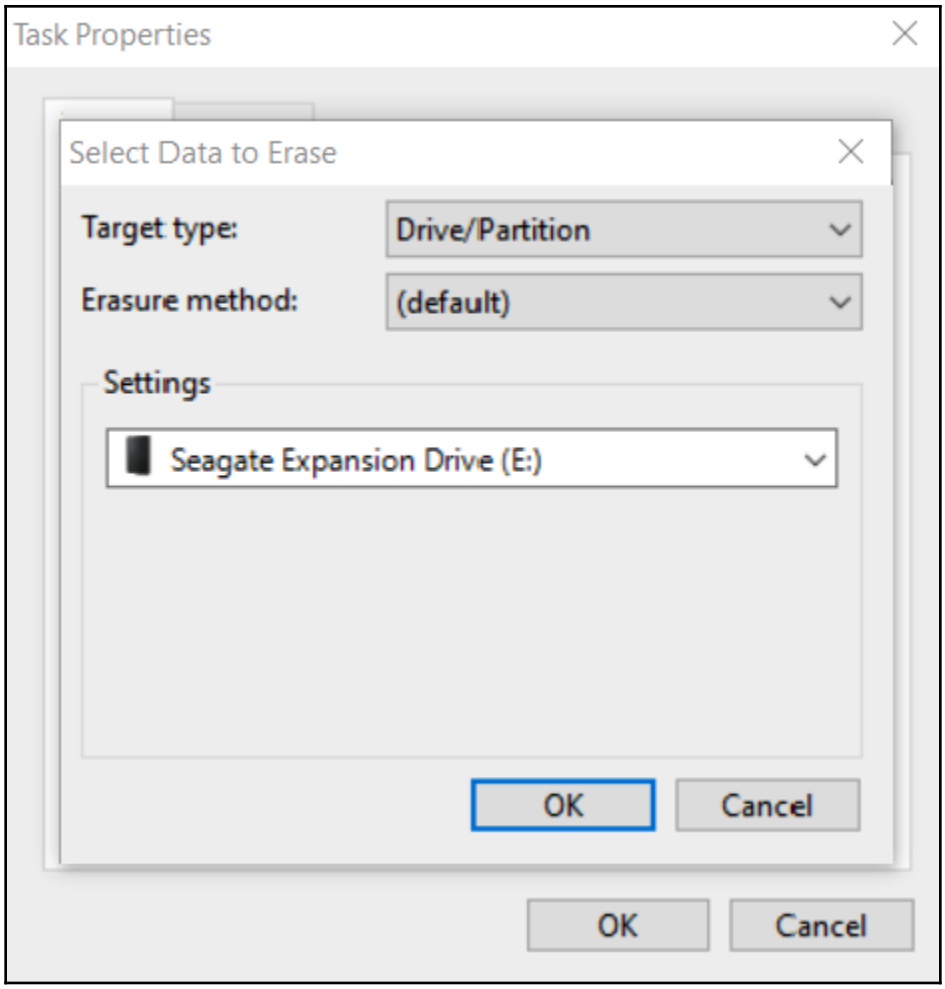


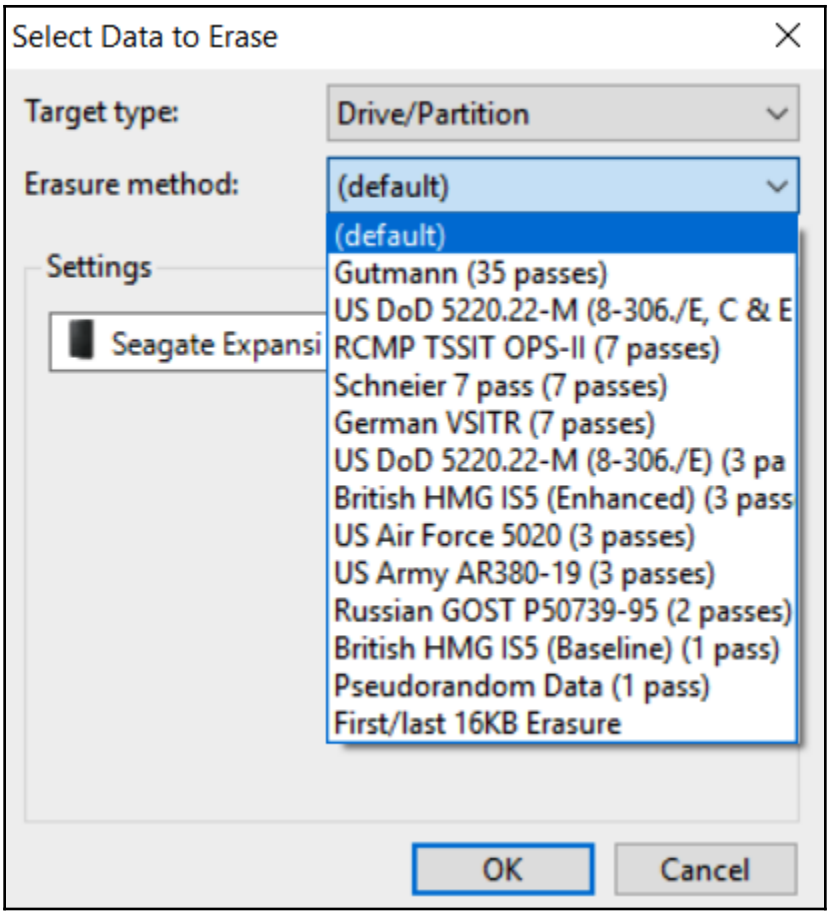
Chapter 6: Forensic Imaging

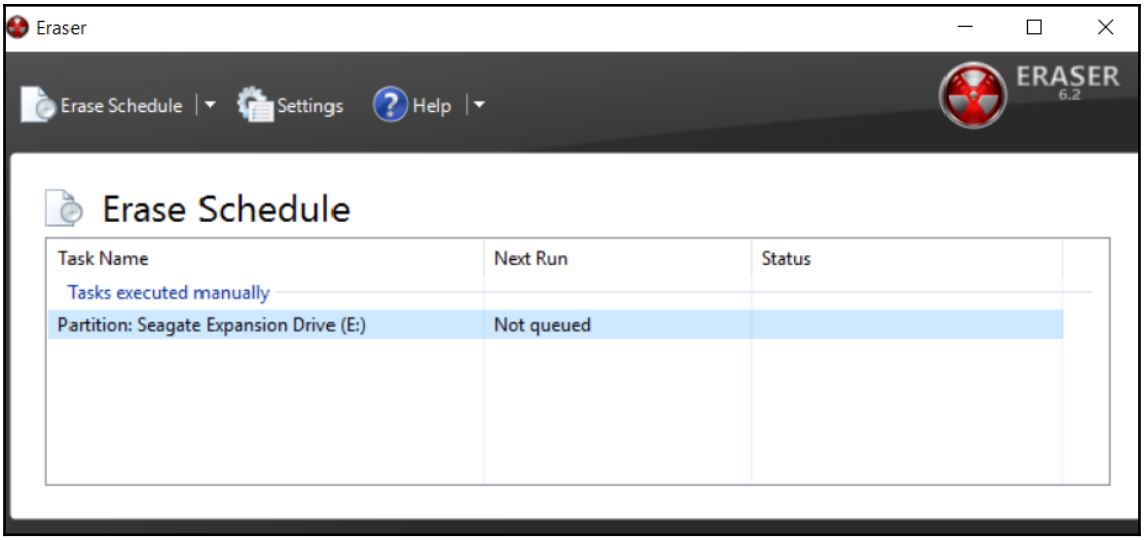


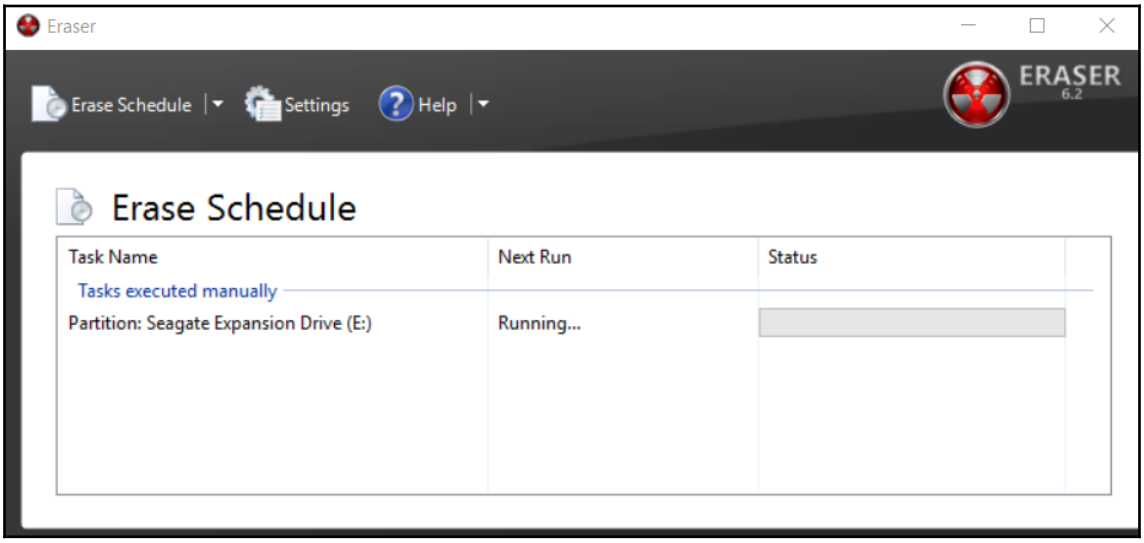
File Header	64 KB Data	CRC	64 KB Data	CRC	64 KB Data	CRC	64 KB Data	CRC	MD5


Eraser
Erase Schedule
Settings
Help
Erase Schedule
Task Name
Next
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

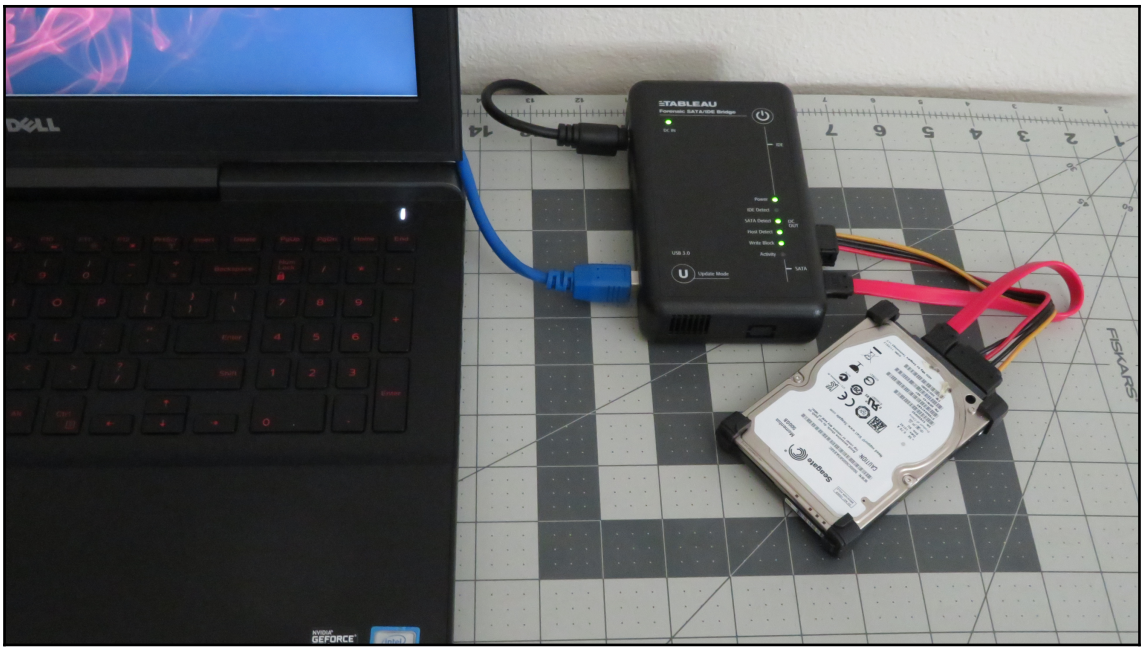

Select Data to Erase
Target type:
Drive/Partition
Erasure method:
(default)
Settings
Seagate Expansi
(default)
Gutmann (35 passes)
US DoD 5220.22-M (8-306./E, C & E
RCMP TSSIT OPS-II (7 passes)
Schneier 7 pass (7 passes)
German VSITR (7 passes)
US DoD 5220.22-M (8-306./E) (3 pa
British HMG IS5 (Enhanced) (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

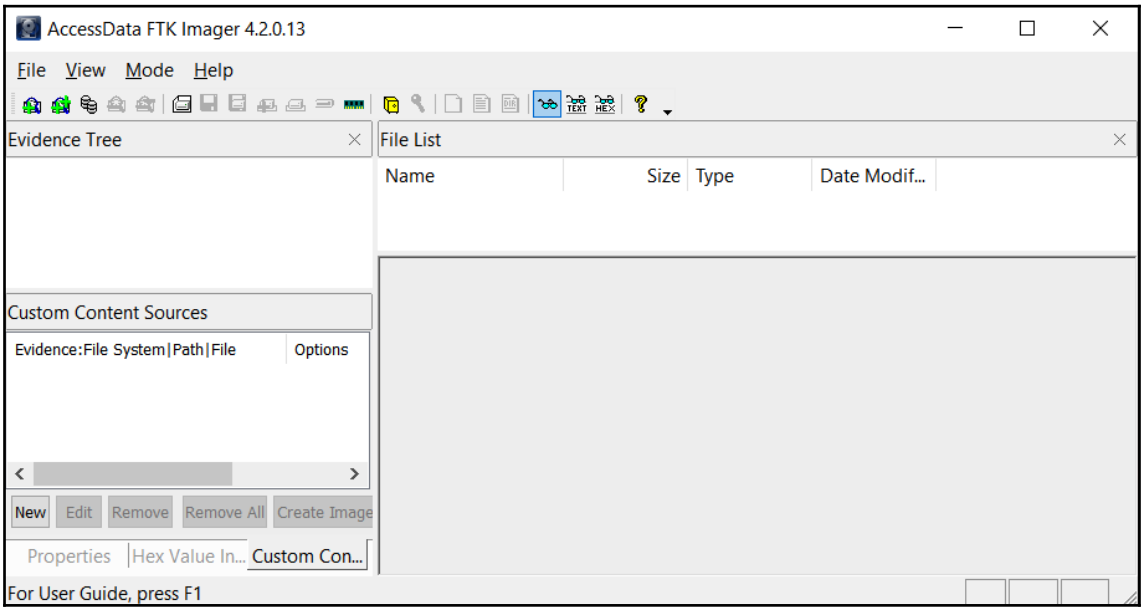

Eraser
Erase Schedule
Settings
Help
ERASER
6.2
Erase Schedule
Task Name
Next Run
Status
Tasks executed manually
Partition: Seagate Expansion Drive (E:)
Not queued

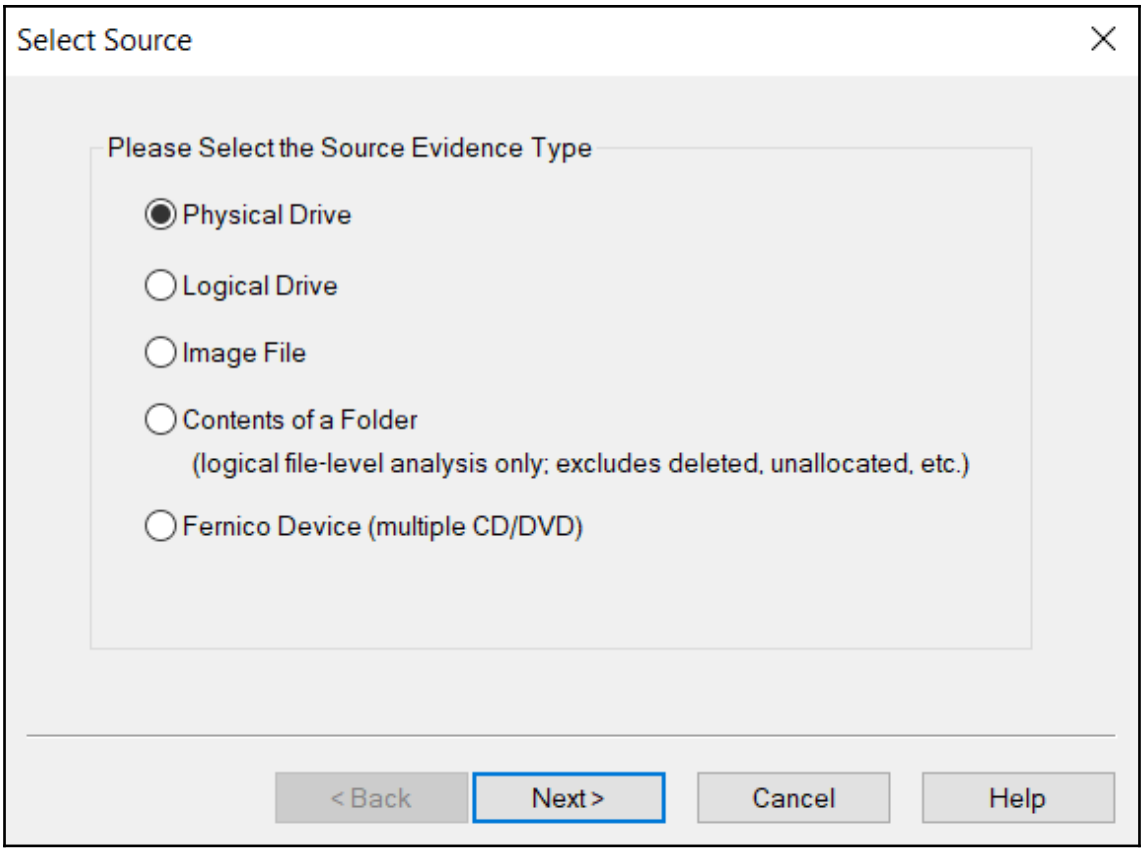

Eraser
Erase Schedule
Settings
Help
ERASER
6.2
Erase Schedule
Task Name
Next Run
Status
Tasks executed manually
Partition: Seagate Expansion Drive (E:)
Running...

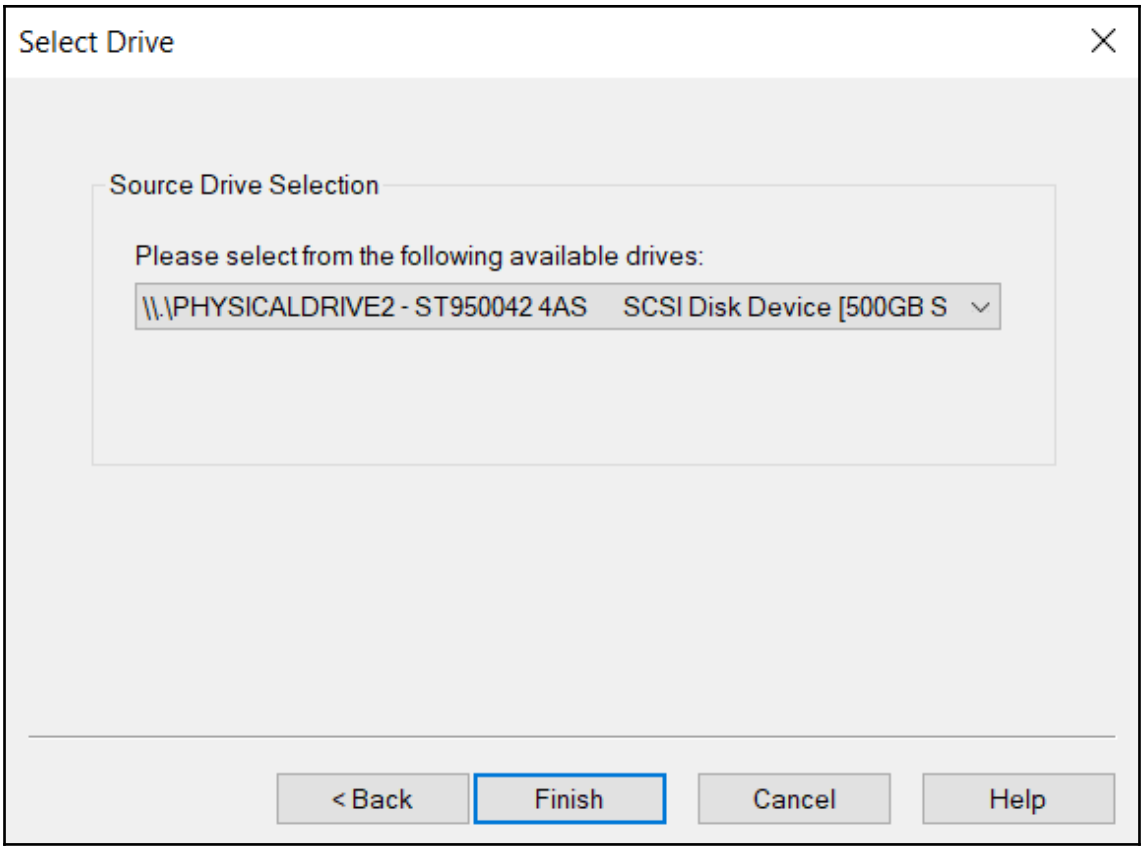

EVIDENCE
DO NOT OPEN
INITIALS
DATE 8.14.15
EVIDENCE
DO NOT OPEN
EVIDENCE
DO NOT OPEN
INITIALS
DATE
EVIDENCE
DO NOT OPEN
Item 1.
John Smith laptop

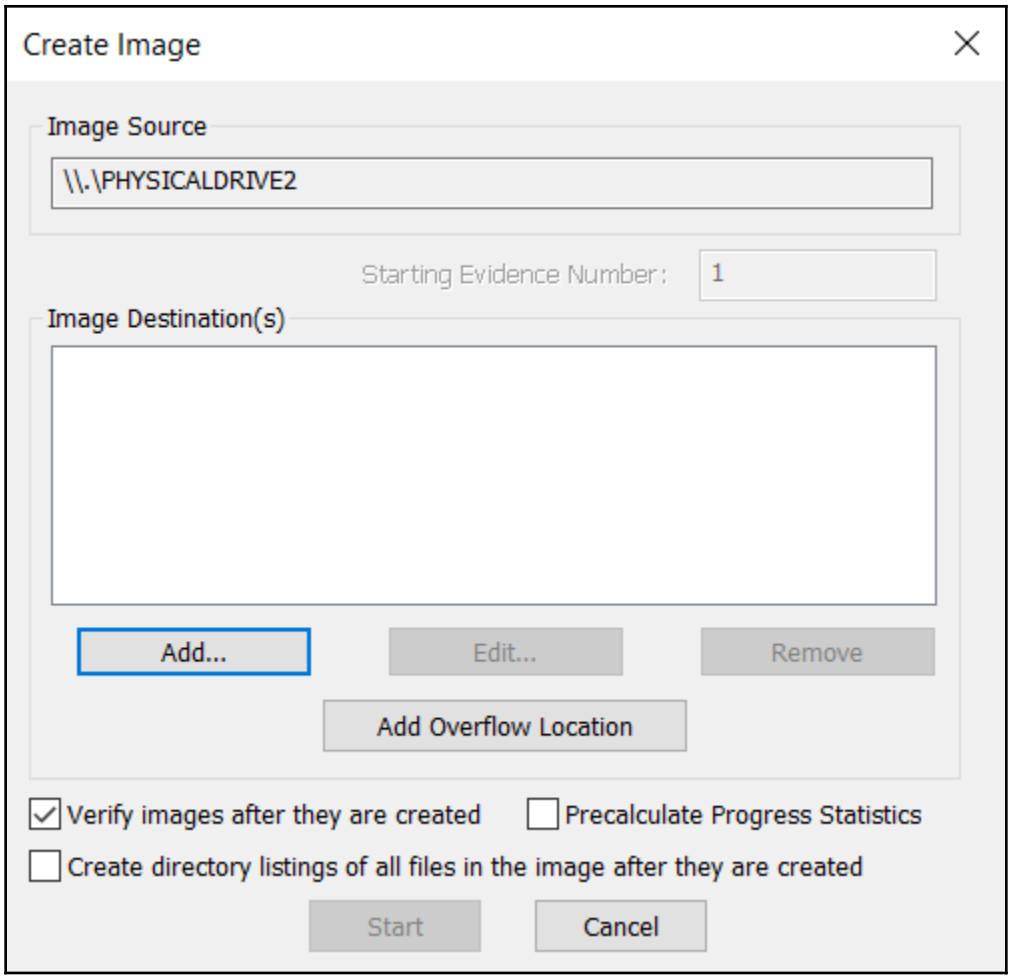

DO NOT COVER
BREATHER HOLE
Seagate
Momentus
500GB
WWN: 5000C500585AB88C
CAUTION: Avoid excessive shock; do not push on top cover or remove any seal or label.
Need support? Visit www.Seagate.com
SERIAL ATA
STX – Momentus (8)
+5V 0.70 A
Date: 13192
Site: SU
E190397
N176
中国产品
Product of China
D33027
SN: S2V0HV93
ST9500424AS
PN: 9RW143 – 567
FW: 0001BSM1
DOM: 11/2012
HDD Mfg by Seagate Technology LLC

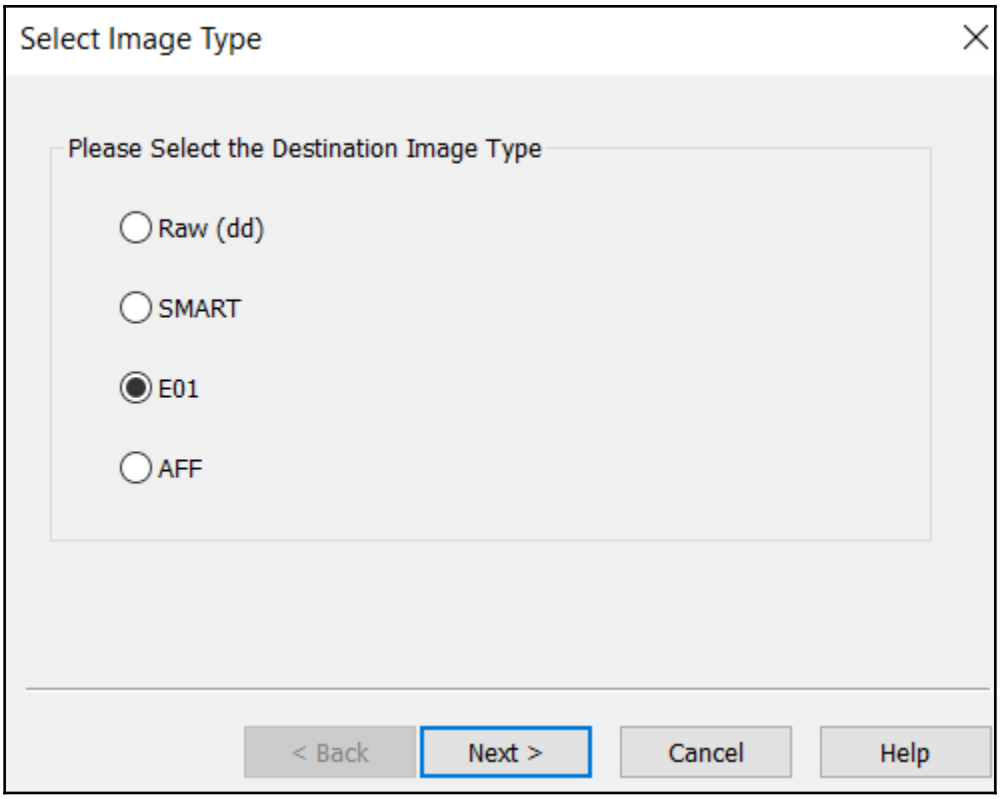

DELL
TABLEAU
FISKARS

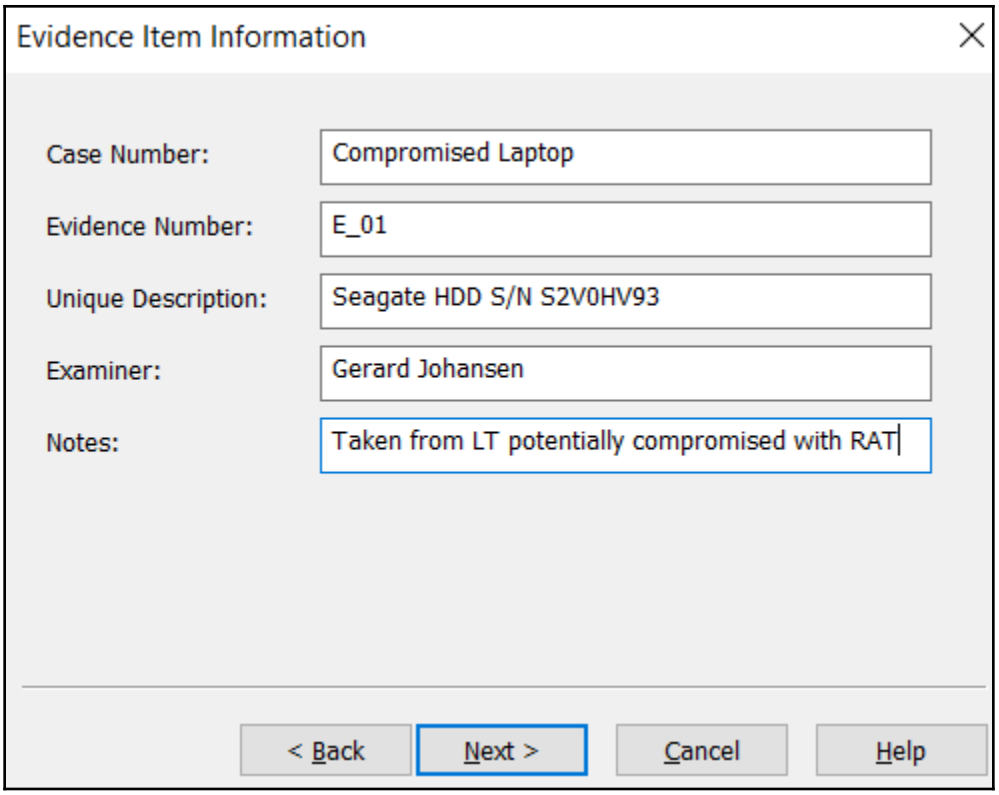

AccessData FTK Imager 4.2.0.13
File View Mode Help
Evidence Tree
File List
Name
Size
Type
Date Modif...
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value In...
Custom Con...
For User Guide, press F1

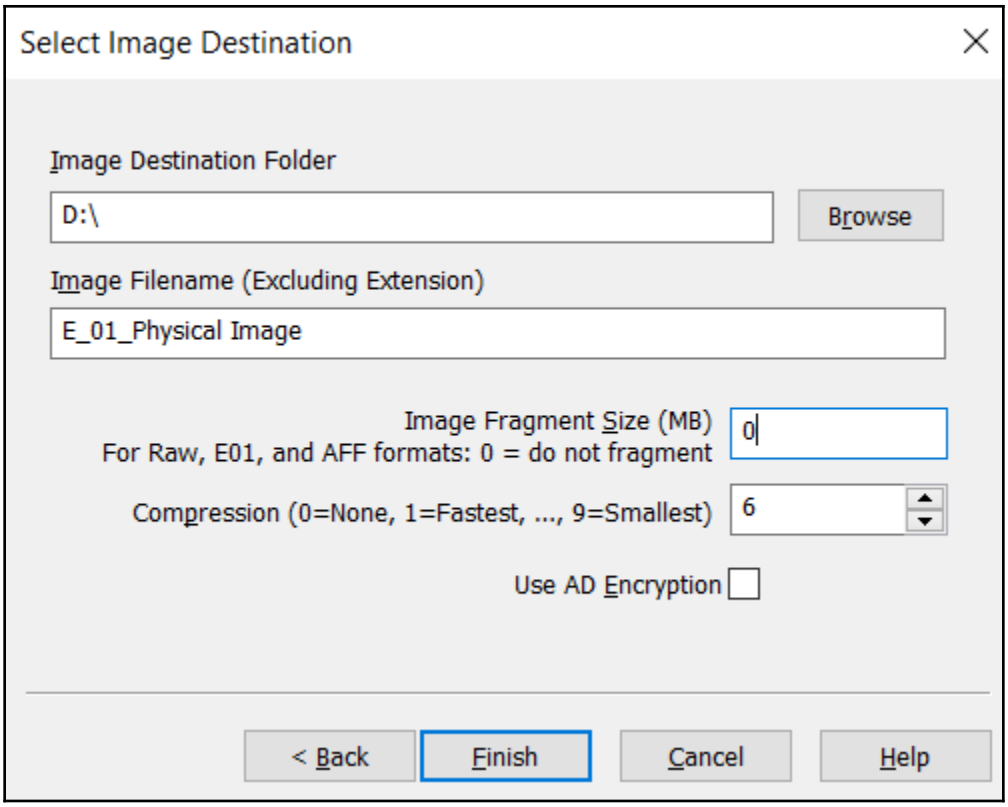

Select Source
Please Select the Source Evidence Type
Physical Drive
Logical Drive
Image File
Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
Fernico Device (multiple CD/DVD)
< Back
Next >
Cancel
Help

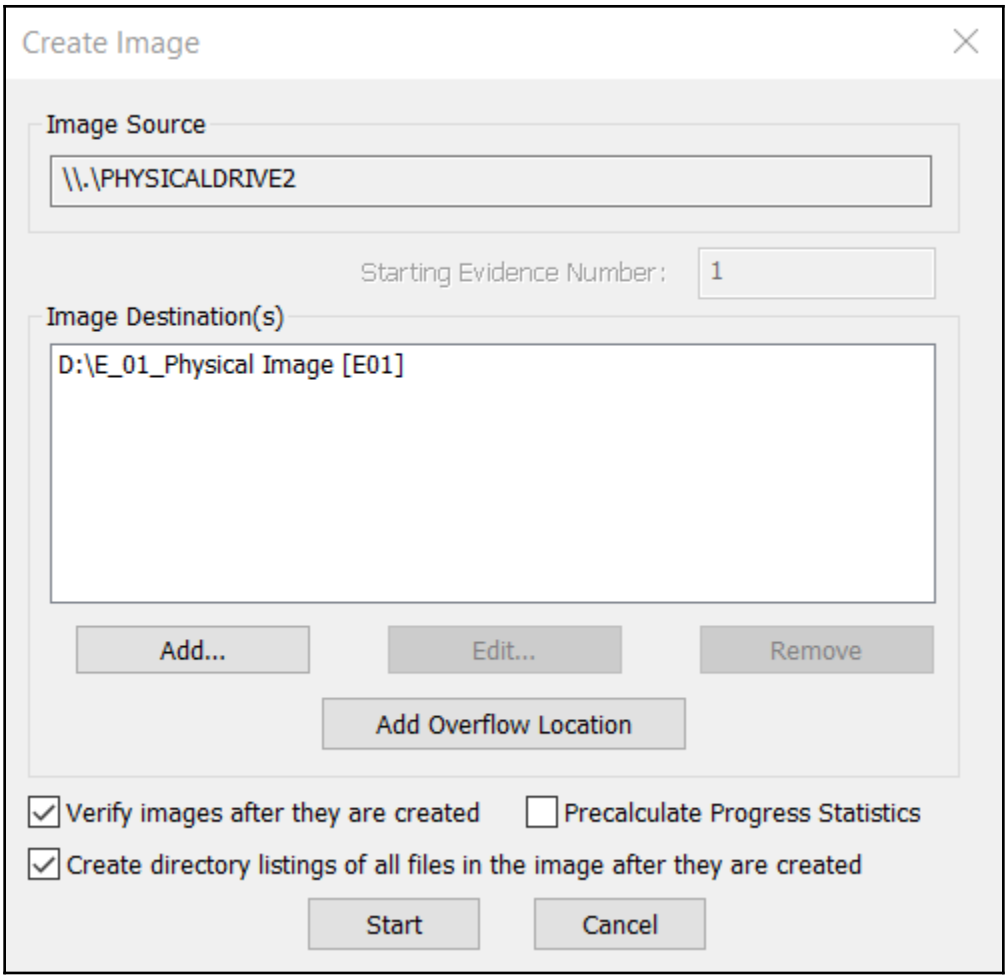

Select Drive
Source Drive Selection
Please select from the following available drives:
\\.\PHYSICALDRIVE2 - ST950042 4AS SCSI Disk Device [500GB S
< Back
Finish
Cancel
Help

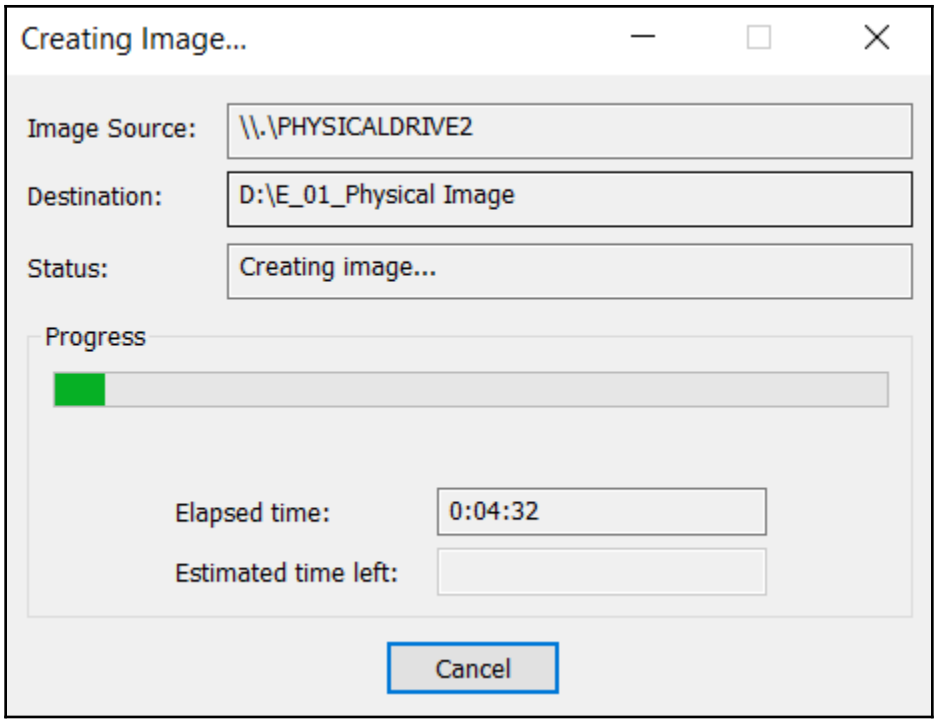

Create Image
Image Source
\\.\PHYSICALDRIVE2
Starting Evidence Number:
1
Image Destination(s)
Add...
Edit...
Remove
Add Overflow Location
Verify images after they are created
Precalculate Progress Statistics
Create directory listings of all files in the image after they are created
Start
Cancel

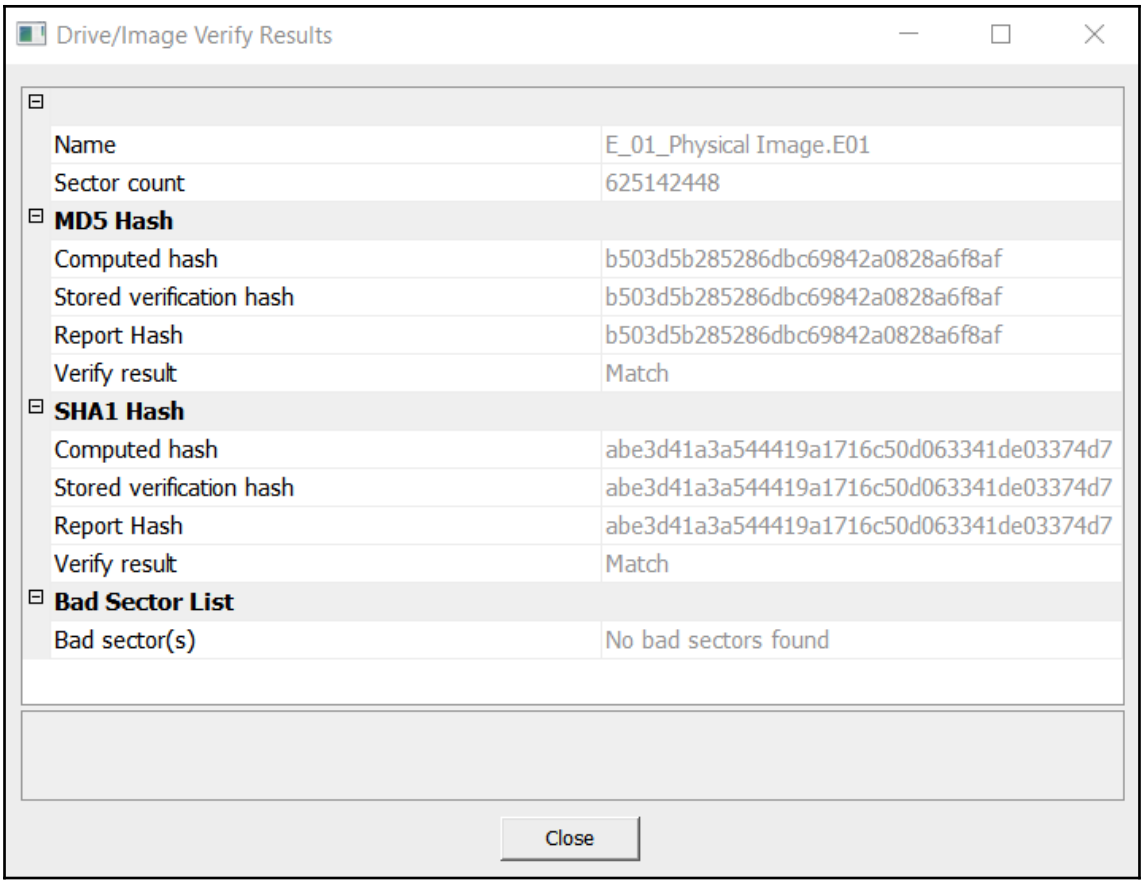

Select Image Type
Please Select the Destination Image Type
Raw (dd)
SMART
E01
AFF
< Back
Next >
Cancel
Help

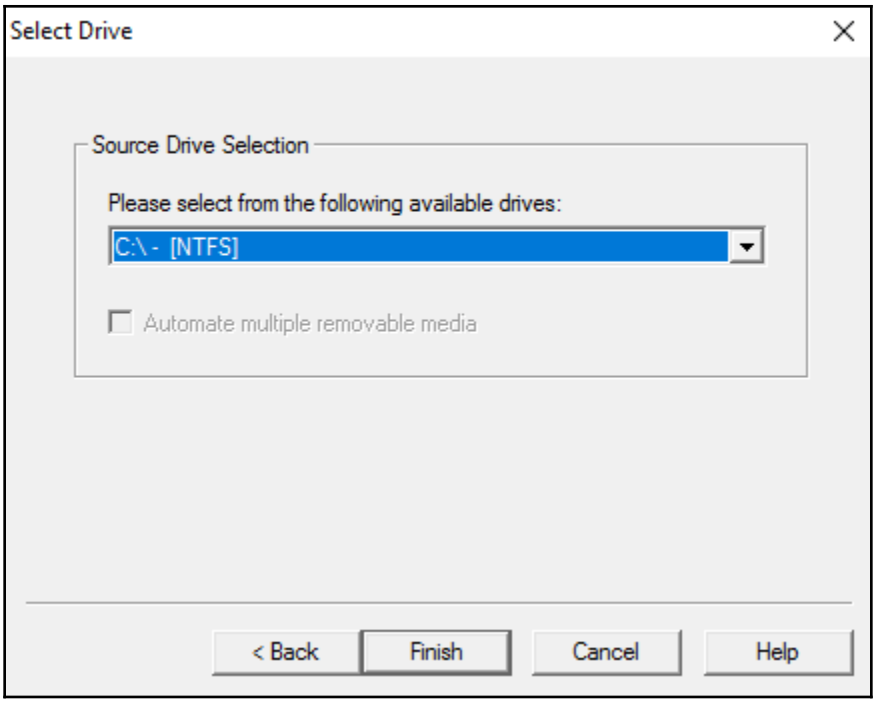

Evidence Item Information
Case Number:
Compromised Laptop
Evidence Number:
E_01
Unique Description:
Seagate HDD S/N S2V0HV93
Examiner:
Gerard Johansen
Notes:
Taken from LT potentially compromised with RAT
< Back
Next >
Cancel
Help

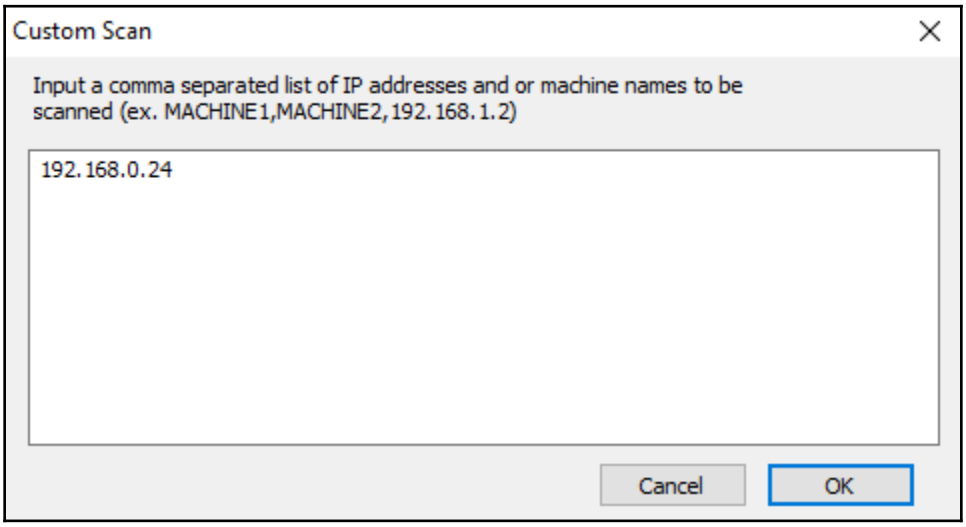

Select Image Destination
Image Destination Folder
D:\
Browse
Image Filename (Excluding Extension)
E_01_Physical Image
Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment
0
Compression (0=None, 1=Fastest, ..., 9=Smallest)
6
Use AD Encryption
< Back
Finish
Cancel
Help

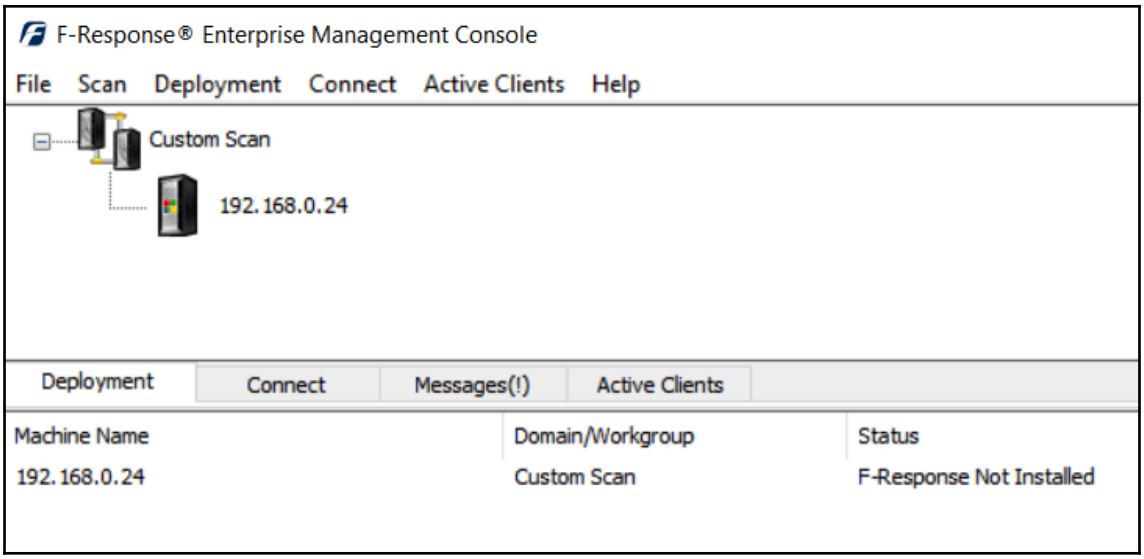

Create Image
Image Source
\\.\PHYSICALDRIVE2
Starting Evidence Number:
1
Image Destination(s)
D:\E_01_Physical Image [E01]
Add...
Edit...
Remove
Add Overflow Location
Verify images after they are created
Precalculate Progress Statistics
Create directory listings of all files in the image after they are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

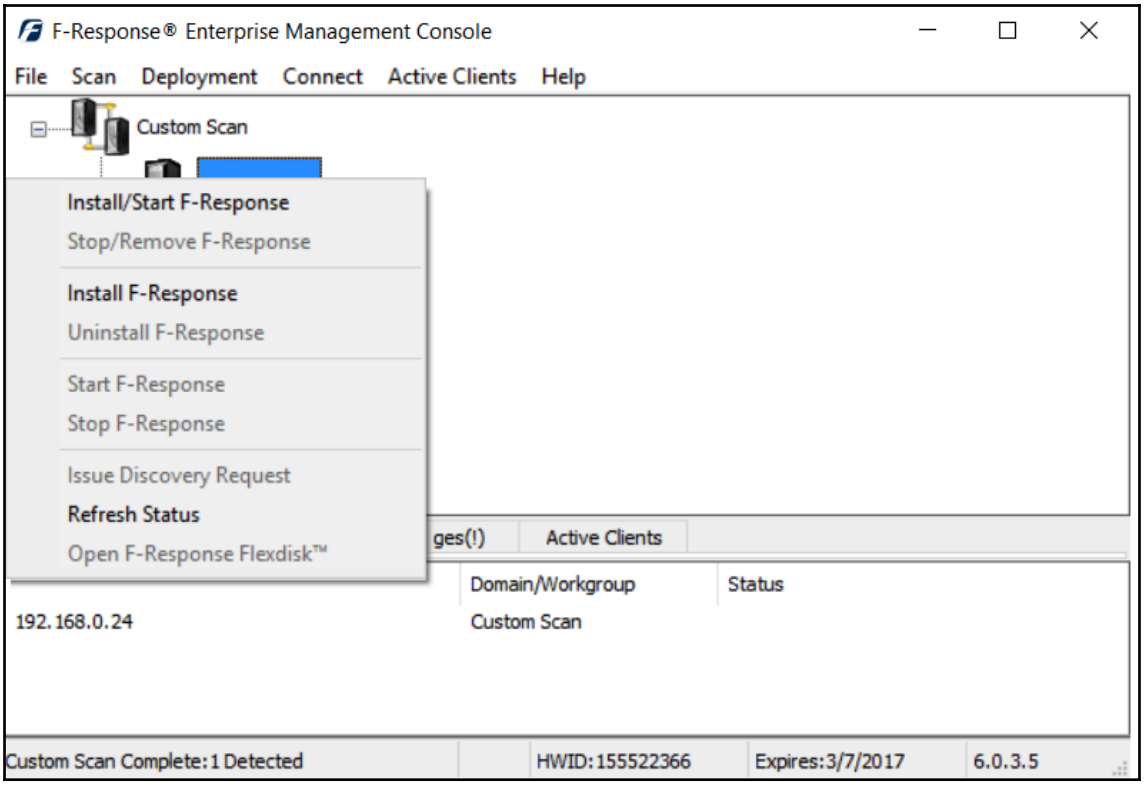

Creating Image...
Image Source:
\\.\PHYSICALDRIVE2
Destination:
D:\E_01_Physical Image
Status:
Creating image...
Progress
Elapsed time:
0:04:32
Estimated time left:
Cancel

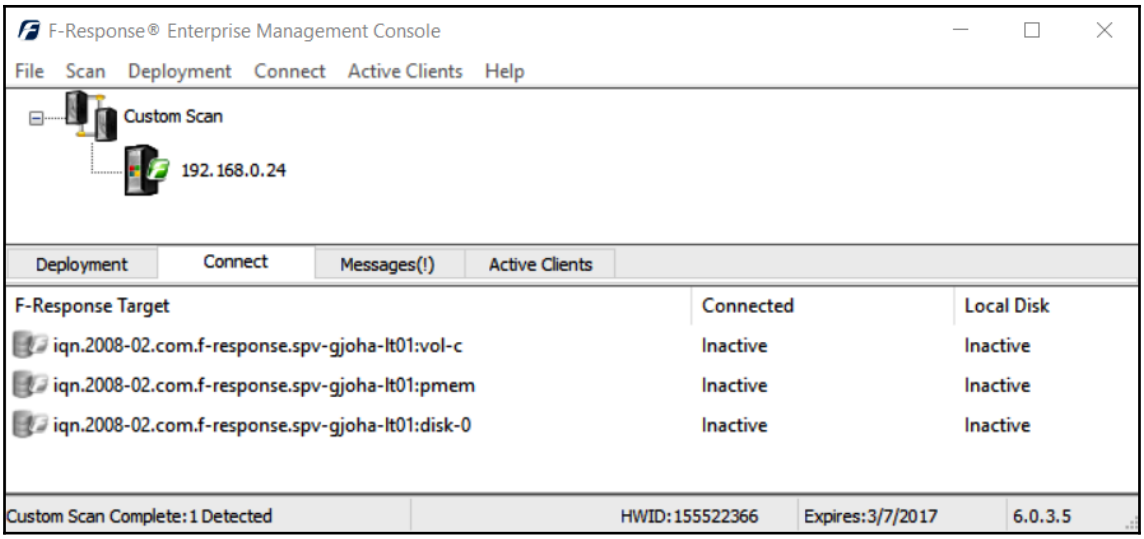

Drive/Image Verify Results
Name
E_01_Physical Image.E01
Sector count
625142448
MD5 Hash
Computed hash
b503d5b285286dbc69842a0828a6f8af
Stored verification hash
b503d5b285286dbc69842a0828a6f8af
Report Hash
b503d5b285286dbc69842a0828a6f8af
Verify result
Match
SHA1 Hash
Computed hash
abe3d41a3a544419a1716c50d063341de03374d7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

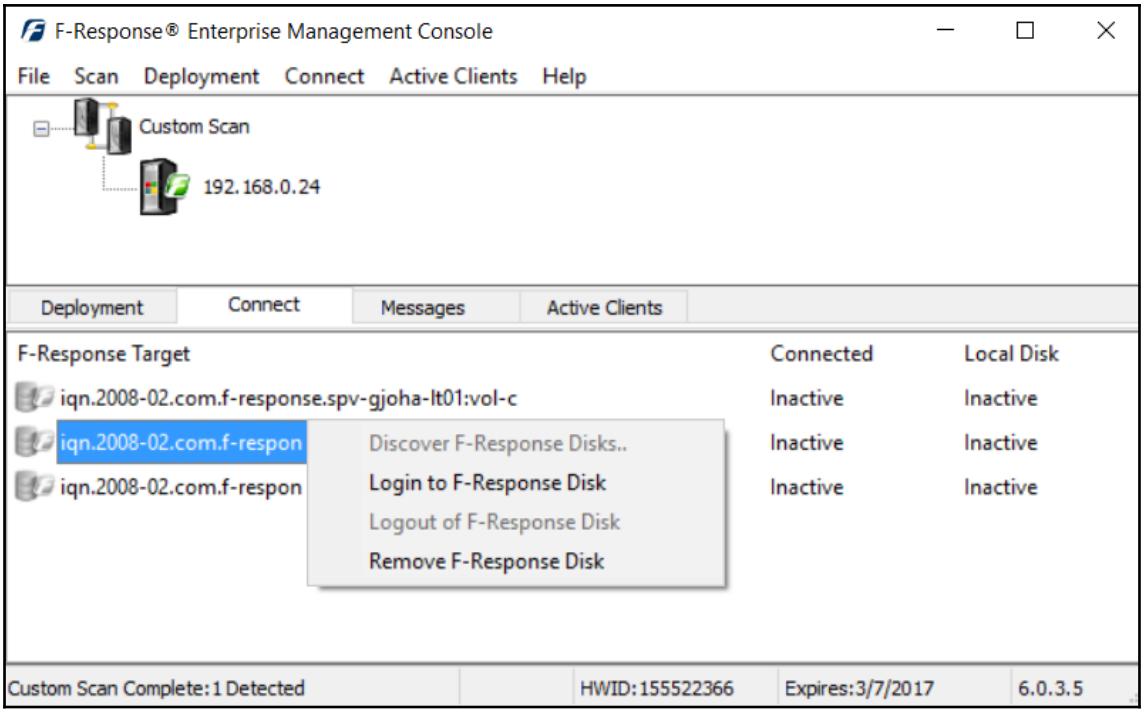

Select Drive
Source Drive Selection
Please select from the following available drives:
C:\ - [NTFS]
Automate multiple removable media
< Back
Finish
Cancel
Help

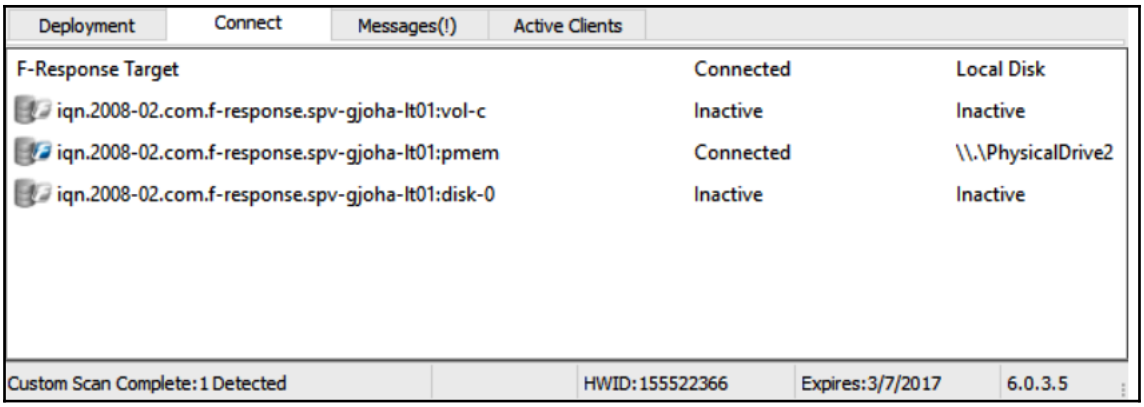

Custom Scan
Input a comma separated list of IP addresses and or machine names to be scanned (ex. MACHINE1,MACHINE2,192.168.1.2)
192.168.0.24
Cancel
OK

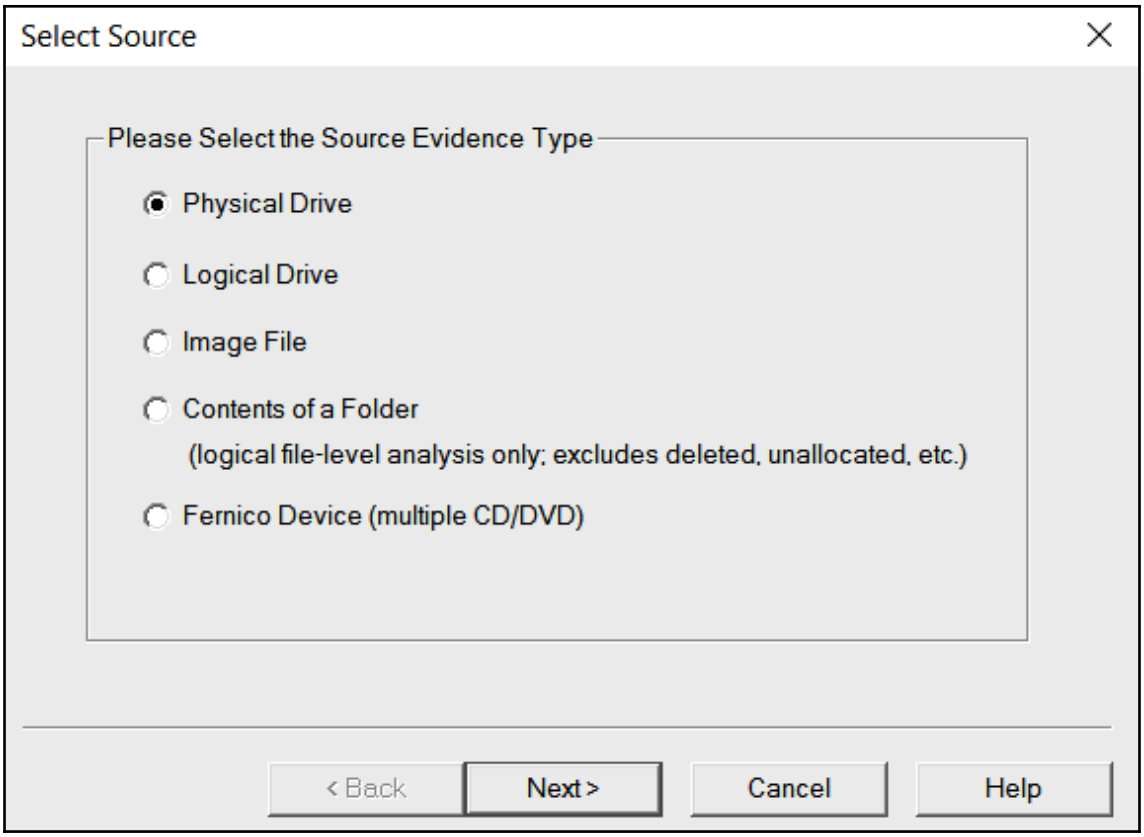

F-Response® Enterprise Management Console
File Scan Deployment Connect Active Clients Help
Custom Scan
192.168.0.24
Deployment
Connect
Messages(!)
Active Clients
Machine Name
Domain/Workgroup
Status
192.168.0.24
Custom Scan
F-Response Not Installed

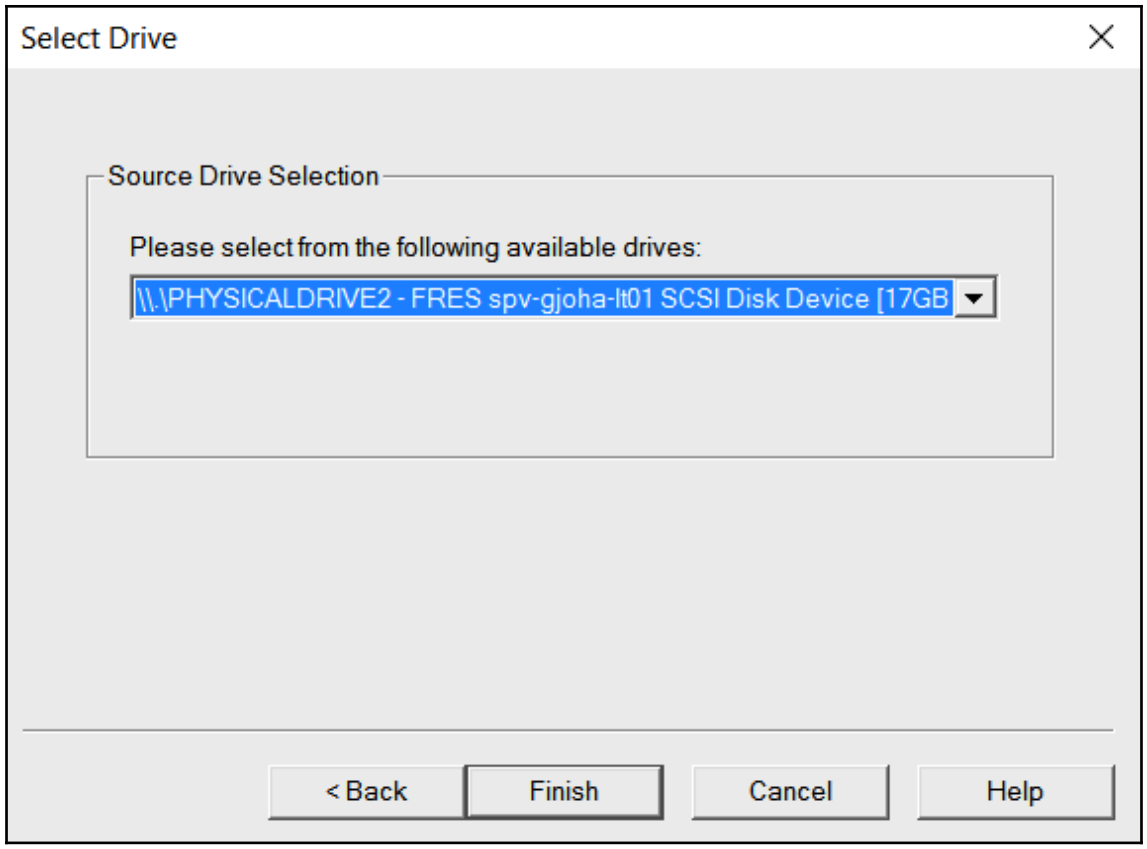

F-Response® Enterprise Management Console
File Scan Deployment Connect Active Clients Help
Custom Scan
Install/Start F-Response
Stop/Remove F-Response
Install F-Response
Uninstall F-Response
Start F-Response
Stop F-Response
Issue Discovery Request
Refresh Status
Open F-Response Flexdisk™
ges(!)
Active Clients
Domain/Workgroup
Status
192.168.0.24
Custom Scan
Custom Scan Complete: 1 Detected
HWID:155522366
Expires:3/7/2017
6.0.3.5

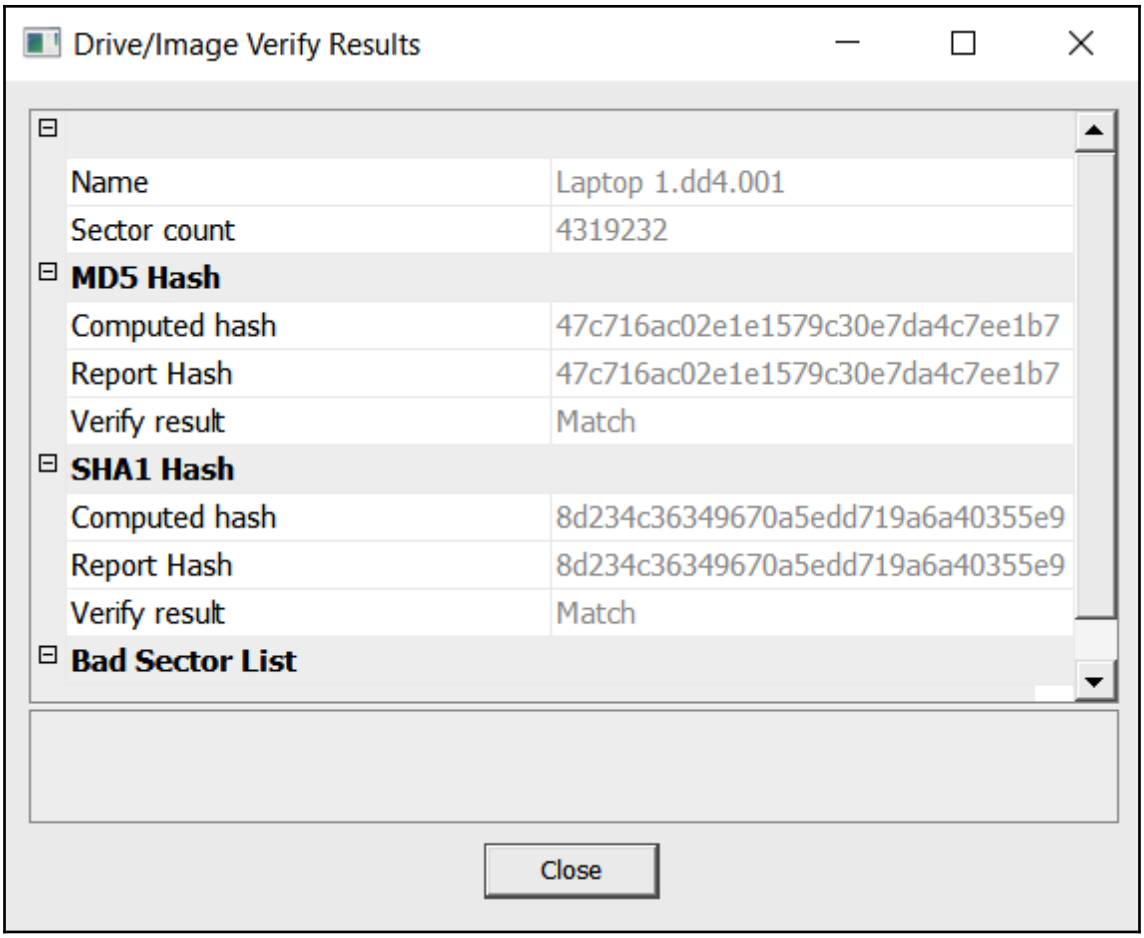

F-Response® Enterprise Management Console
File Scan Deployment Connect Active Clients Help
Custom Scan
192.168.0.24
Deployment Connect Messages(!) Active Clients
F-Response Target
Connected
Local Disk
iqn.2008-02.com.f-response.spv-gjoha-lt01:vol-c
Inactive
Inactive
iqn.2008-02.com.f-response.spv-gjoha-lt01:pmem
Inactive
Inactive
iqn.2008-02.com.f-response.spv-gjoha-lt01:disk-0
Inactive
Inactive
Custom Scan Complete: 1 Detected
HWID: 155522366
Expires: 3/7/2017
6.0.3.5


F-Response® Enterprise Management Console
File Scan Deployment Connect Active Clients Help
Custom Scan
192.168.0.24
Deployment Connect Messages Active Clients
F-Response Target
Connected
Local Disk
iqn.2008-02.com.f-response.spv-gjoha-lt01:vol-c
Inactive
Inactive
iqn.2008-02.com.f-respon
Inactive
Inactive
iqn.2008-02.com.f-respon
Inactive
Inactive
Discover F-Response Disks..
Login to F-Response Disk
Logout of F-Response Disk
Remove F-Response Disk
Custom Scan Complete: 1 Detected
HWID: 155522366
Expires: 3/7/2017
6.0.3.5

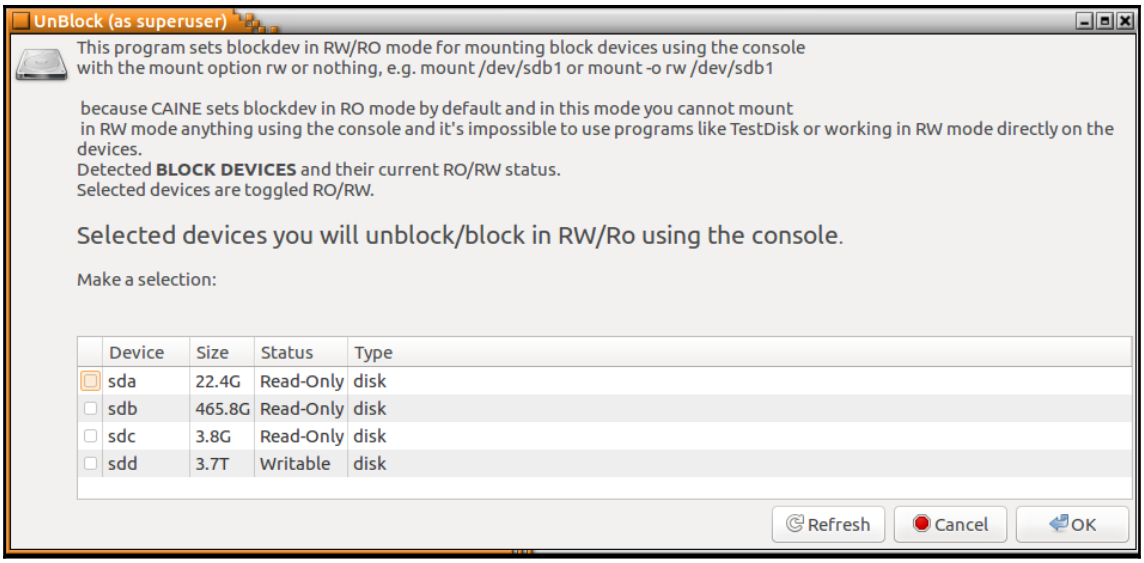

Deployment
Connect
Messages(!)
Active Clients
F-Response Target
Connected
Local Disk
iqn.2008-02.com.f-response.spv-gjoha-lt01:vol-c
Inactive
Inactive
iqn.2008-02.com.f-response.spv-gjoha-lt01:pmem
Connected
\\.\PhysicalDrive2
iqn.2008-02.com.f-response.spv-gjoha-lt01:disk-0
Inactive
Inactive
Custom Scan Complete: 1 Detected
HWID: 155522366
Expires: 3/7/2017
6.0.3.5


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 - FRES spv-gjoha-lt01 SCSI Disk Device [17GB
< Back
Finish
Cancel
Help


Drive/Image Verify Results
Name
Laptop 1.dd4.001
Sector count
4319232
MD5 Hash
Computed hash
47c716ac02e1e1579c30e7da4c7ee1b7
Report Hash
47c716ac02e1e1579c30e7da4c7ee1b7
Verify result
Match
SHA1 Hash
Computed hash
8d234c36349670a5edd719a6a40355e9
Report Hash
8d234c36349670a5edd719a6a40355e9
Verify result
Match
Bad Sector List
Close

```
Disk /dev/sdb: 465.8 GiB, 500107862016 bytes, 976773168 sectors
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: dos
Disk identifier: 0x345601e6

Device     Boot     Start       End   Sectors   Size Id Type
/dev/sdb1  *         2048   1026047   1024000   500M  7 HPFS/NTFS/exFAT
/dev/sdb2         1026048 975847423 974821376 464.9G  7 HPFS/NTFS/exFAT
/dev/sdb3       975847424 976769023    921600   450M 27 Hidden NTFS WinRE


Disk /dev/sdc: 3.8 GiB, 4060086272 bytes, 7929856 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
Disklabel type: dos
Disk identifier: 0x000f1d04

Device     Boot Start     End Sectors  Size Id Type
/dev/sdc1  *     2048 7929855 7927808  3.8G  c W95 FAT32 (LBA)


Disk /dev/sdd: 3.7 TiB, 4000787029504 bytes, 7814037167 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 33553920 bytes
Disklabel type: gpt
Disk identifier: 30B0BF34-42D8-41E5-A90C-E5735893CFB6

Device      Start        End    Sectors  Size Type
/dev/sdd1      34     262177     262144  128M Microsoft reserved
/dev/sdd2  264192 7814035455 7813771264  3.7T Microsoft basic data
```




```
caine@caine:/mnt/EvidenceDrive1/Case2017-01$ sudo dc3dd if=/dev/sdb of=ideapad.img hash=md5 log
=dc3ddlog.txt

dc3dd 7.2.641 started at 2017-04-02 19:18:35 +0100
compiled options:
command line: dc3dd if=/dev/sdb of=ideapad.img hash=md5 log=dc3ddlog.txt
device size: 976773168 sectors (probed),   500,107,862,016 bytes
sector size: 512 bytes (probed)
 6376849408 bytes ( 5.9 G ) copied (  1% ),   58 s, 105 M/s
```

```
dc3dd 7.2.641 started at 2017-04-02 19:18:35 +0100
compiled options:
command line: dc3dd if=/dev/sdb of=ideapad.img hash=md5 log=dc3ddlog.txt
device size: 976773168 sectors (probed),   500,107,862,016 bytes
sector size: 512 bytes (probed)
500107862016 bytes ( 466 G ) copied ( 100% ), 5854 s, 81 M/s

input results for device `/dev/sdb':
   976773168 sectors in
   0 bad sectors replaced by zeros
   d48a7ccafaead6fab7d284b4be300bd8 (md5)

output results for file `ideapad.img':
   976773168 sectors out

dc3dd completed at 2017-04-02 20:56:09 +0100
```

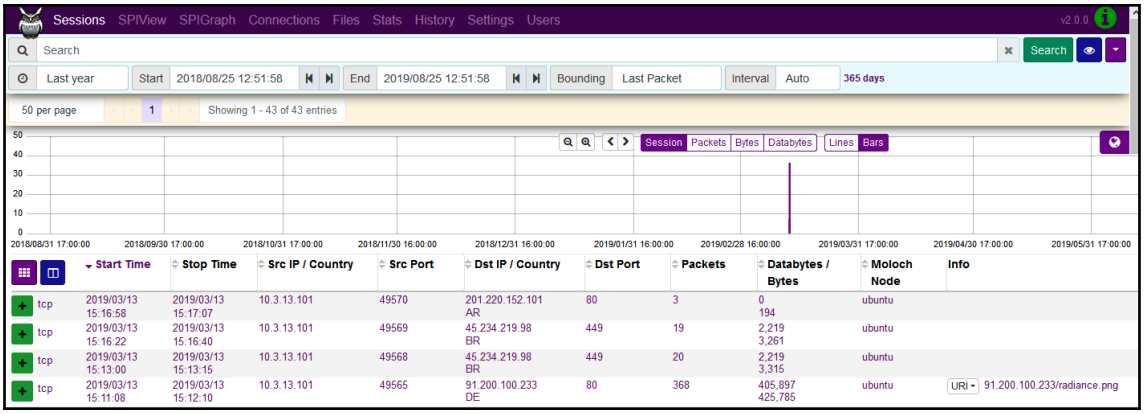

dc3ddlog 4/2/2017 12:56 PM Text Document 2 KB
ideapad 4/2/2017 12:56 PM Disc Image File 488,386,58...

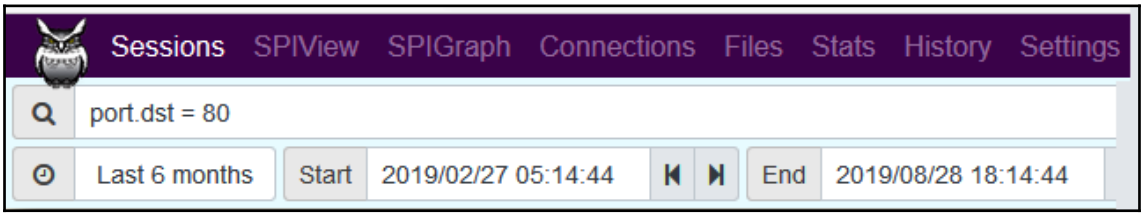
Chapter 7: Analyzing Network Evidence

```
Note: DNS resolution and reverse resolution is currently not supported.
Parsing blacklist files...
-------------------------------------------------------------------------------
EmotetIOC_01_17_19.txt
EmotetIOC_04_2019.txt
EmotetIOC_08_2019.txt

Parsing check files...
-------------------------------------------------------------------------------
Firewall Logs.txt

===============================================================================
The following hostnames were found in the blacklists:
===============================================================================
rozhan-hse.com
===============================================================================
The following IPs were found in the blacklists:
===============================================================================
```

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: 10 new, 10 total, EOF

Sources          Count      %   cum%
-----------  ---------  ------  ------
10.3.13.101         10   100.0   100.0
```





Dst IP / Country	Dst Port	Packets	Databytes / Bytes
83.220.141.232 DE	80	524	506,630 534,942
129.226.63.136 SG	80	291	246,151 261,881
31.44.184.33 RU	80	230	211,253 223,689
129.226.63.136 SG	80	221	195,452 207,402
31.44.184.33 RU	80	218	211,265 223,053

URI neu.x-sait.de/wp-content/plugins/mce-table-buttons/pp.exe

neu.x-sait.de/wp-content/plugins/mce-table-buttons/4.exe

URI

cd.pranahat.at/webstore/zSR1Z6AnDI0PfpsiGN_2F9W/7oYFSY47cH/9hfkJMvimgZEx3TIC/hR5_2BF3YKL1/WqZUwlQoia
O/9WGtTrqojm1Fpc/w4JGS_2BqOVVP9F5qP_2B/QcnCwcoZRFssnyQ8/6pxNROtgxS0JSSG/j_2B9TBJ5hwNSZU9f7/1ud
mNsp5a/TjPoAB3gEfW2yvZBcgGC/o1Z1ifT9HbS1Dg4Stts/AFZuGjnzhJzwDKC84R_2Fu/ZcUMga13Z/eNW1ffKY/VxS

URI 31.44.184.33/uDaB

URI

x1.narutik.at/webstore/Wlpdq7f64iZDVKdP/nNIPLUwRF2LoqfY/E5R_2FJjib_2Ba2k97/bcIDnPA_2/BkBxN61i7f8UEj0rGwAa
/dPKTXIMVsfT1EHFq3EY/G9gCfV7T5wEjN4HML4X7pG/NOM985YvHHdzP/5Lcb8zEq/NMGJwwOWXxbU6a6_2FuMdbR/V
av0v2m3j2/4GXc_2FXtmWGU6mJ_/2Fn_2BLwcjuW/sYrlBoHcbMb/Xpu043fnlxCp/Uay

URI 31.44.184.33/H7mp

URI cd.pranahat.at/jvassets/o1/s64.dat

URI 31.44.184.33/visit.js

URI ectcnepal.org/wp-includes/customize/a22.exe

Id 190722-LQ3wf_0vl_5ETpOliuwvnqP8 **Community Id:** 1:gkyHOSZKMLAR+92SulX3WgCWXaY=

Time 2019/07/22 09:18:57 - 2019/07/22 09:18:58

Node ubuntu

Protocols http tcp

IP Protocol tcp

Src **Packets** 36 **Bytes** 2,285 **Databytes** 329

Dst **Packets** 90 **Bytes** 123,905 **Databytes** 119,041

Ethernet **Src Mac** 00:08:02:1c:47:ae **OUI** Hewlett Packard **Dst Mac** 20:e5:2a:b6:93:f1 **OUI** Netgear

Src IP/Port 10.7.22.101 : 49183

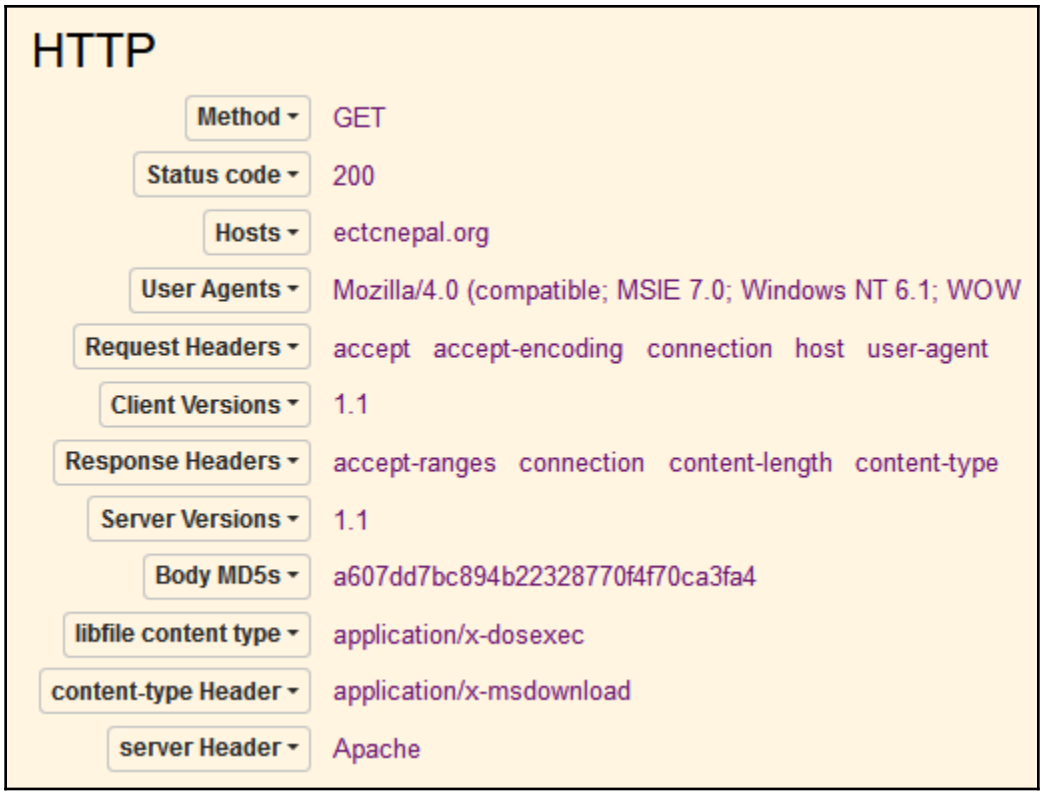
Dst IP/Port 85.222.228.142 : 80 (NL) [AS35470 CloudVPS B.V.] { RIPE }

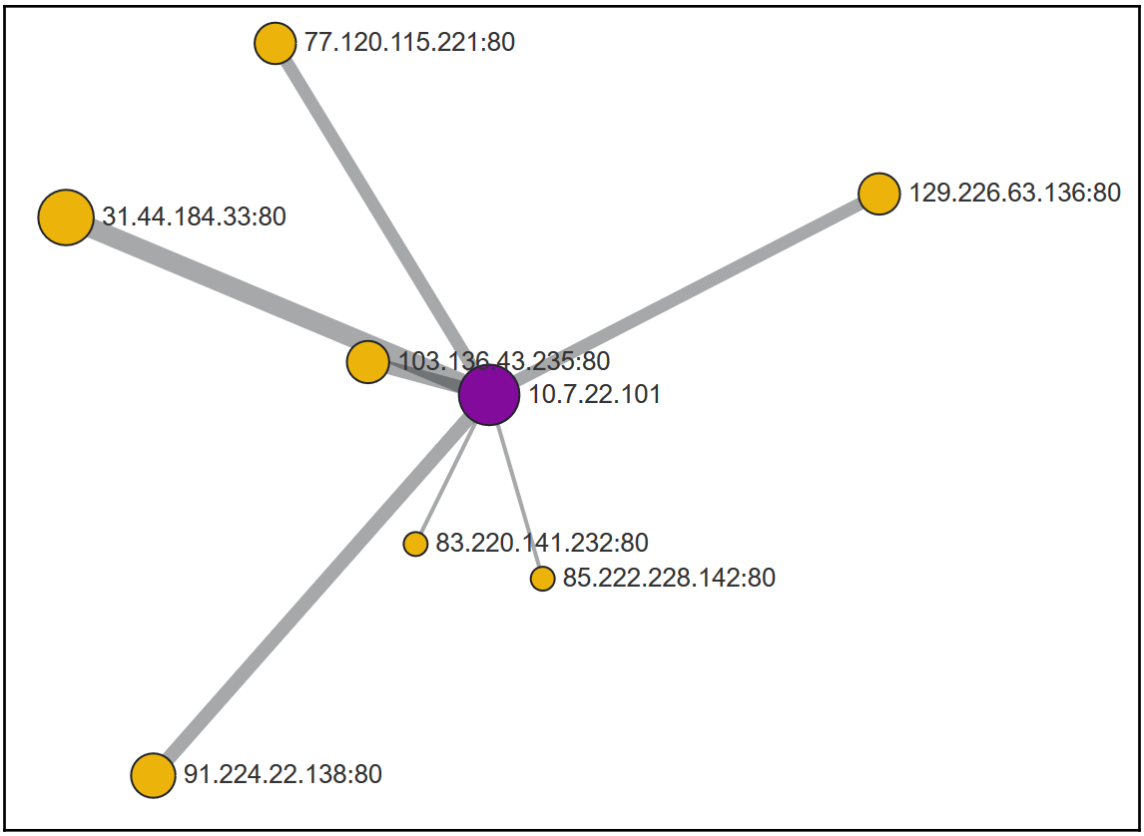
Payload8 **Src** 474554202f77702d (GET /wp-) **Dst** 485454502f312e31 (HTTP/1.1)

Tags

Files /data/moloch/raw/2019-07-22-Amadey-infection-with-Pony-and-Ursnif-and-Cobalt-Strike.pcap

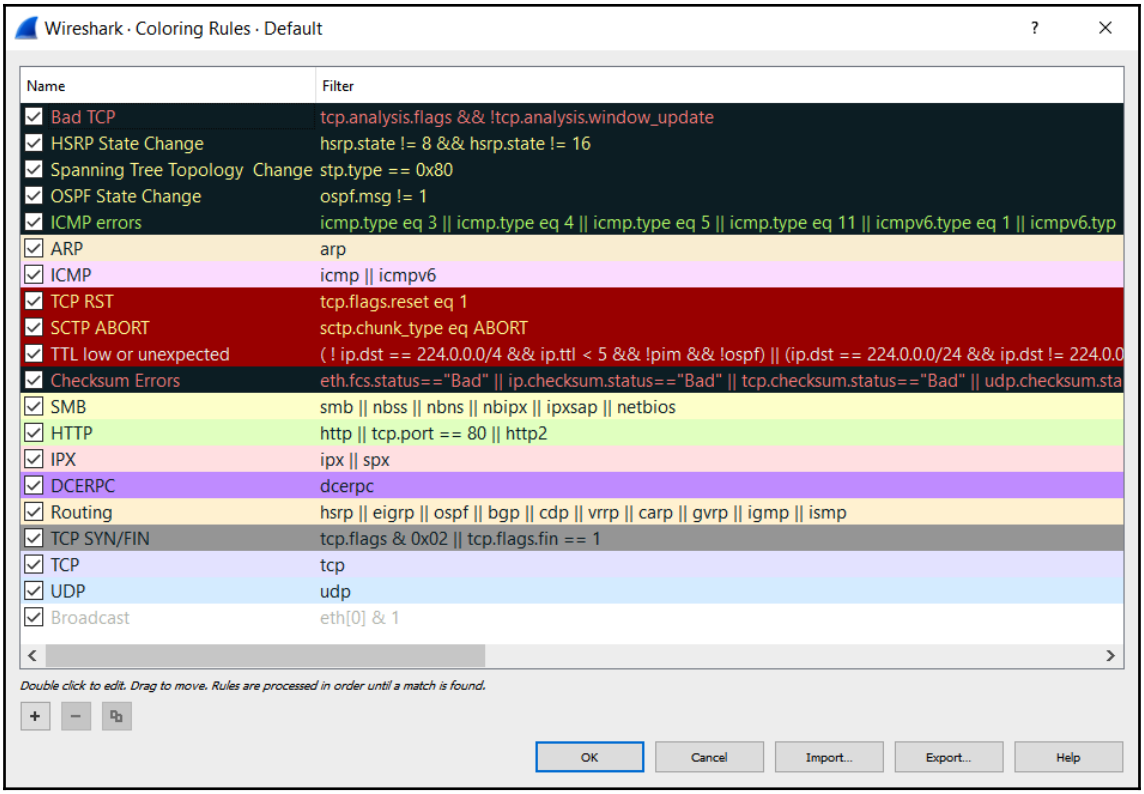
TCP Flags **SYN** 1 **SYN-ACK** 1 **ACK** 81 **PSH** 42 **RST** 0 **FIN** 2 **URG** 0


HTTP
Method
GET
Status code
200
Hosts
ectcnepal.org
User Agents
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW
Request Headers
accept accept-encoding connection host user-agent
Client Versions
1.1
Response Headers
accept-ranges connection content-length content-type
Server Versions
1.1
Body MD5s
a607dd7bc894b22328770f4f70ca3fa4
libfile content type
application/x-dosexec
content-type Header
application/x-msdownload
server Header
Apache


77.120.115.221:80
31.44.184.33:80
129.226.63.136:80
103.136.43.235:80
10.7.22.101
83.220.141.232:80
85.222.228.142:80
91.224.22.138:80

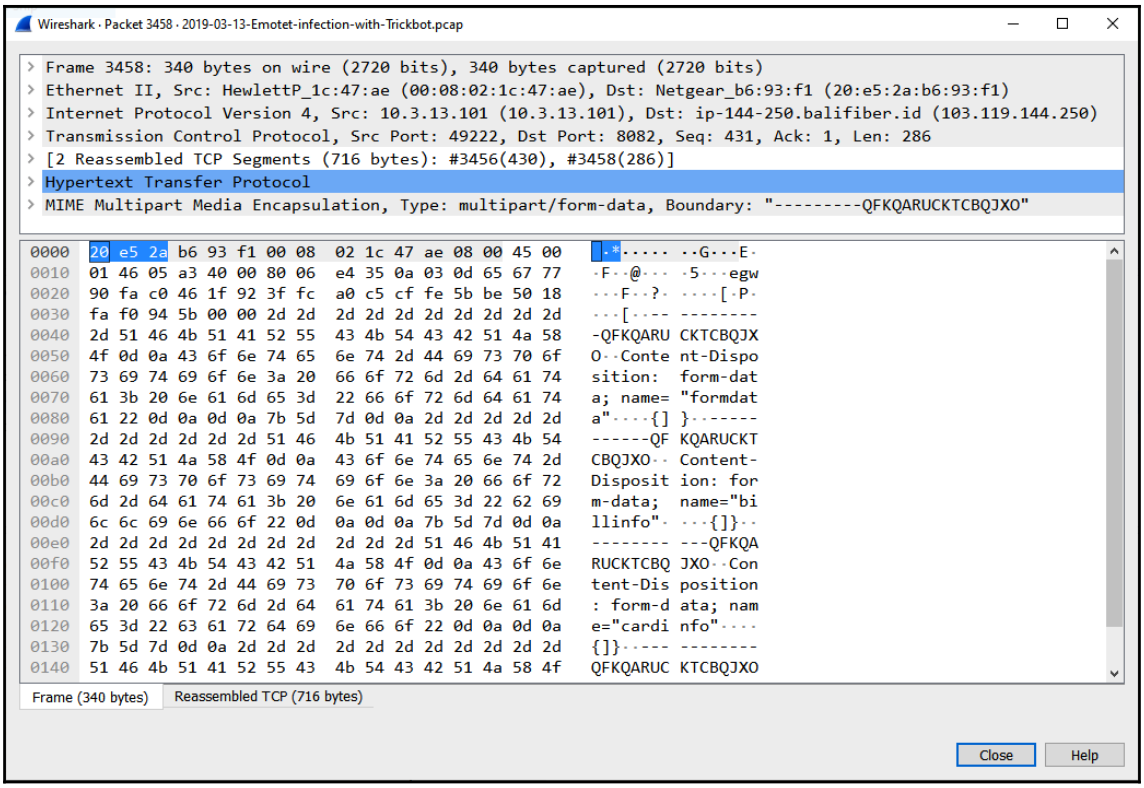
No.	Time	Source	Destination	Protocol
1	0.000000	10.3.13.101	10.3.13.1	DNS
2	0.030692	10.3.13.1	10.3.13.101	DNS
3	0.556303	10.3.13.101	88.198.14.102	TCP
4	0.739115	88.198.14.102	10.3.13.101	TCP
5	0.739762	10.3.13.101	88.198.14.102	TCP
6	0.739961	10.3.13.101	88.198.14.102	HTTP
7	0.740053	88.198.14.102	10.3.13.101	TCP
8	2.084099	88.198.14.102	10.3.13.101	TCP
9	2.084368	88.198.14.102	10.3.13.101	TCP
10	2.084401	88.198.14.102	10.3.13.101	TCP
11	2.084670	88.198.14.102	10.3.13.101	TCP
12	2.084701	10.3.13.101	88.198.14.102	TCP
13	2.084715	88.198.14.102	10.3.13.101	TCP
14	2.084740	88.198.14.102	10.3.13.101	TCP
15	2.084990	10.3.13.101	88.198.14.102	TCP
16	2.085834	88.198.14.102	10.3.13.101	TCP
17	2.085905	88.198.14.102	10.3.13.101	TCP
18	2.085924	88.198.14.102	10.3.13.101	TCP
19	2.085941	88.198.14.102	10.3.13.101	TCP

No.	Time	Source	Destination	Protocol
1	0.000000	10.3.13.101	10.3.13.1	DNS
2	0.030692	10.3.13.1	10.3.13.101	DNS
3	0.556303	10.3.13.101	rozhan-hse.com	TCP
4	0.739115	rozhan-hse.com	10.3.13.101	TCP
5	0.739762	10.3.13.101	rozhan-hse.com	TCP
6	0.739961	10.3.13.101	rozhan-hse.com	HTTP
7	0.740053	rozhan-hse.com	10.3.13.101	TCP
8	2.084099	rozhan-hse.com	10.3.13.101	TCP
9	2.084368	rozhan-hse.com	10.3.13.101	TCP
10	2.084401	rozhan-hse.com	10.3.13.101	TCP
11	2.084670	rozhan-hse.com	10.3.13.101	TCP
12	2.084701	10.3.13.101	rozhan-hse.com	TCP
13	2.084715	rozhan-hse.com	10.3.13.101	TCP
14	2.084740	rozhan-hse.com	10.3.13.101	TCP
15	2.084990	10.3.13.101	rozhan-hse.com	TCP
16	2.085834	rozhan-hse.com	10.3.13.101	TCP
17	2.085905	rozhan-hse.com	10.3.13.101	TCP
18	2.085924	rozhan-hse.com	10.3.13.101	TCP
19	2.085941	rozhan-hse.com	10.3.13.101	TCP

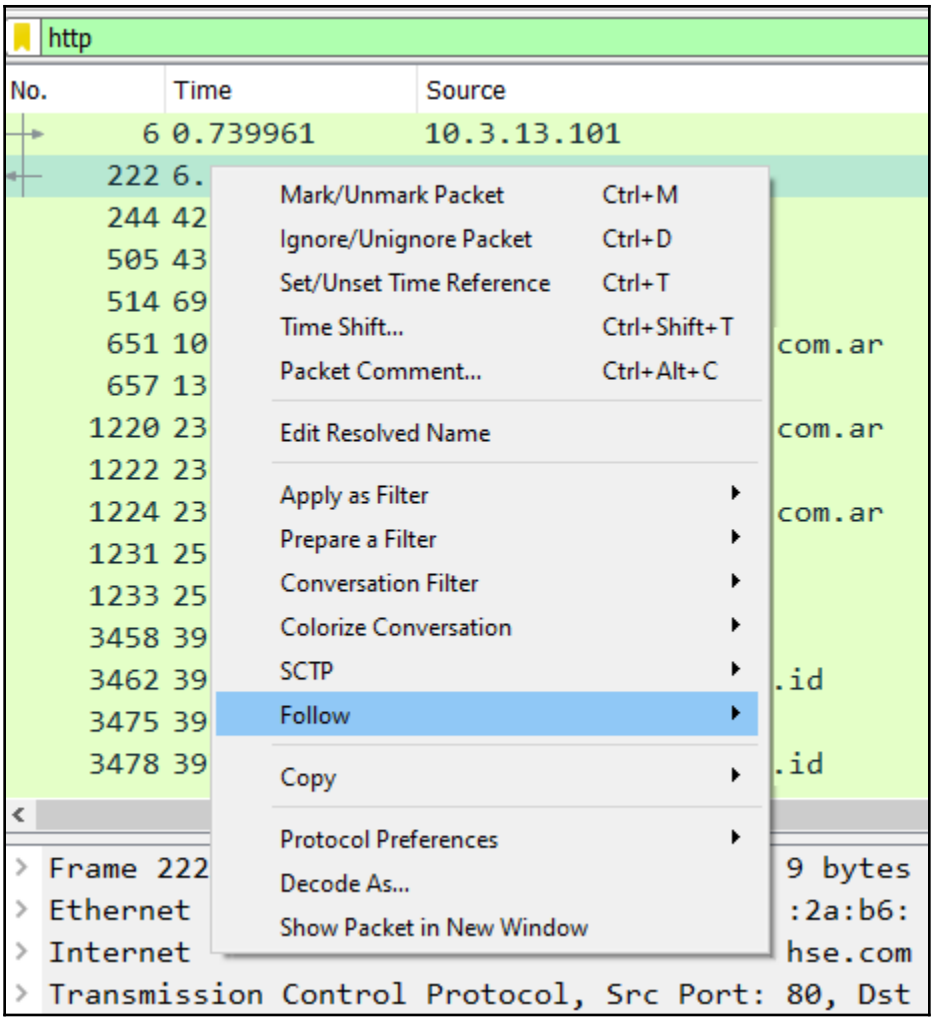

Wireshark · Coloring Rules · Default
Name
Filter
Bad TCP
tcp.analysis.flags && !tcp.analysis.window_update
HSRP State Change
hsrp.state != 8 && hsrp.state != 16
Spanning Tree Topology Change
stp.type == 0x80
OSPF State Change
ospf.msg != 1
ICMP errors
icmp.type eq 3 || icmp.type eq 4 || icmp.type eq 5 || icmp.type eq 11 || icmpv6.type eq 1 || icmpv6.typ
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 && !ospf) || (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0
Checksum Errors
eth.fcs.status=="Bad" || ip.checksum.status=="Bad" || tcp.checksum.status=="Bad" || udp.checksum.sta
SMB
smb || nbss || nbns || nbipx || ipxsap || netbios
HTTP
http || tcp.port == 80 || http2
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.
OK
Cancel
Import...
Export...
Help

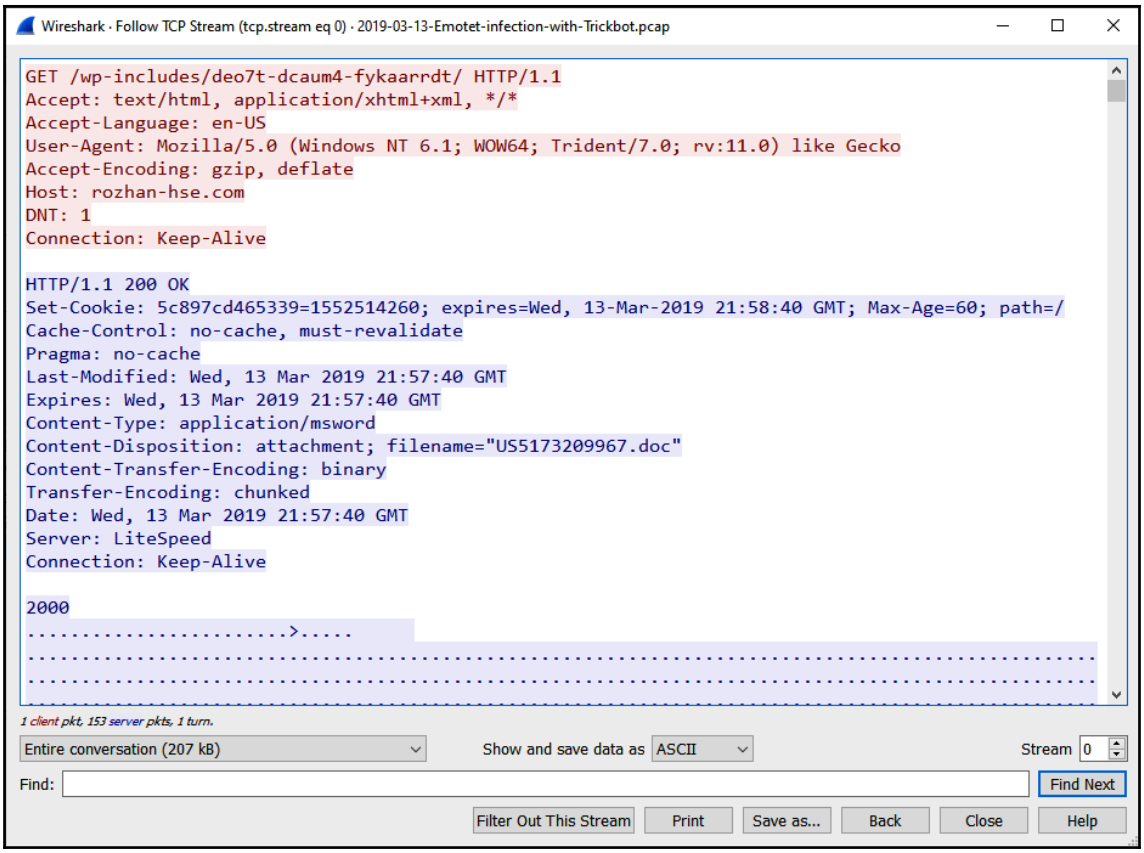
ip.src==10.3.13.101

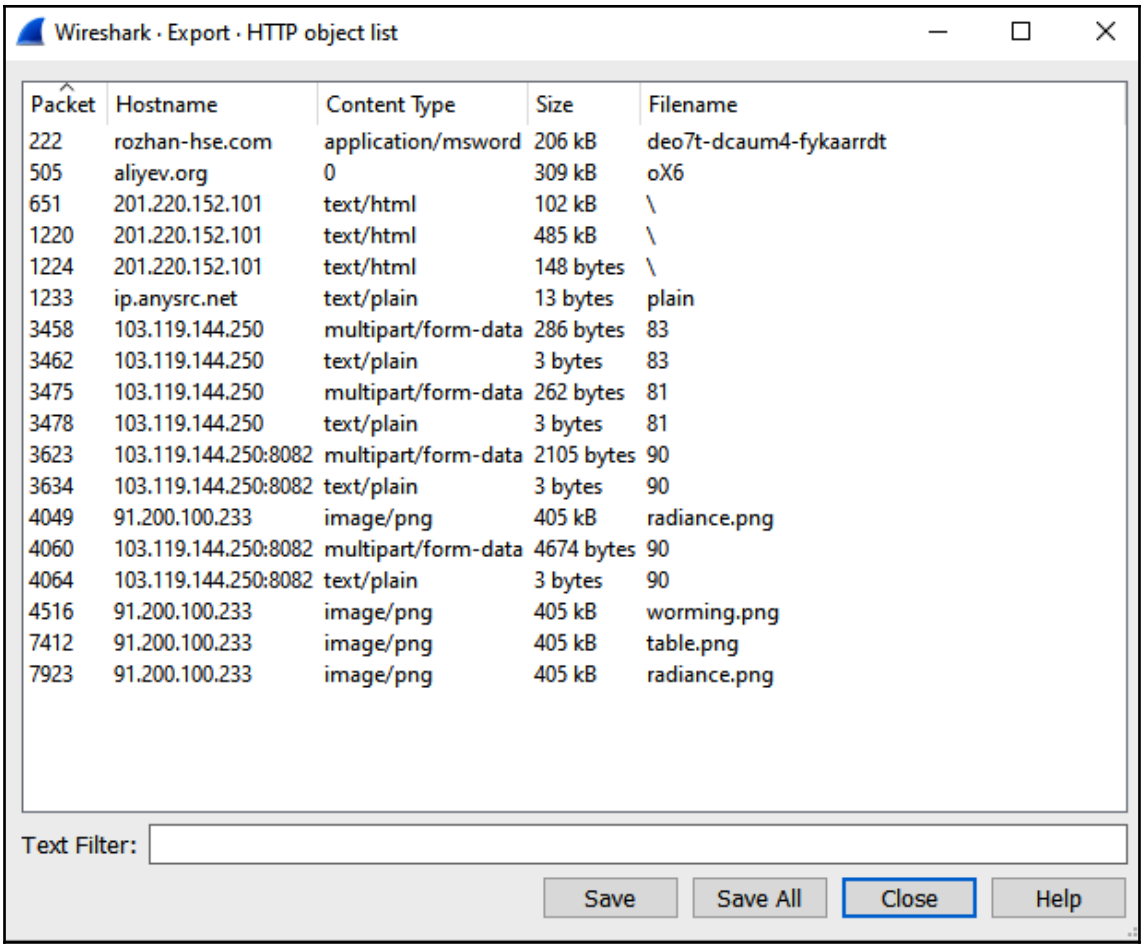
No.	Time	Source	Destination	Protocol
1	0.000000	10.3.13.101	10.3.13.1	DNS
3	0.556303	10.3.13.101	rozhan-hse.com	TCP
5	0.739762	10.3.13.101	rozhan-hse.com	TCP
6	0.739961	10.3.13.101	rozhan-hse.com	HTTP
12	2.084701	10.3.13.101	rozhan-hse.com	TCP
15	2.084990	10.3.13.101	rozhan-hse.com	TCP
20	2.086218	10.3.13.101	rozhan-hse.com	TCP
21	2.132104	10.3.13.101	rozhan-hse.com	TCP
23	2.237990	10.3.13.101	rozhan-hse.com	TCP
25	2.238930	10.3.13.101	rozhan-hse.com	TCP
28	2.240120	10.3.13.101	rozhan-hse.com	TCP
33	2.243412	10.3.13.101	rozhan-hse.com	TCP
34	2.243479	10.3.13.101	rozhan-hse.com	TCP
36	2.405627	10.3.13.101	rozhan-hse.com	TCP
42	2.406802	10.3.13.101	rozhan-hse.com	TCP
49	2.409928	10.3.13.101	rozhan-hse.com	TCP



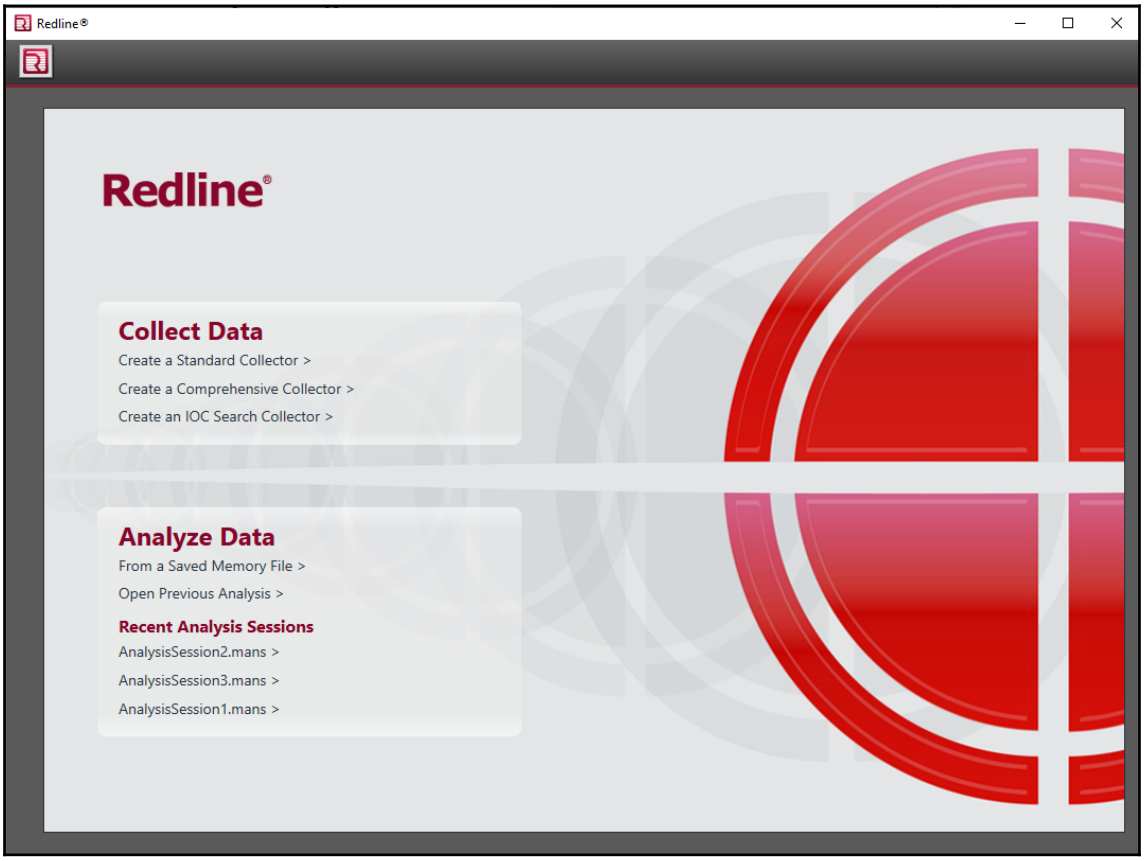
No.	Time	Source	Destination	Protocol
6	0.739961	10.3.13.101	rozhan-hse.com	HTTP
222	6.111115	rozhan-hse.com	10.3.13.101	HTTP
244	42.716145	10.3.13.101	aliyev.org	HTTP
505	43.744089	aliyev.org	10.3.13.101	HTTP
514	69.467806	10.3.13.101	101.152.220.201.itc.com.ar	HTTP
651	107.988909	101.152.220.201.itc.com.ar	10.3.13.101	HTTP
657	133.250172	10.3.13.101	101.152.220.201.itc.com.ar	HTTP
1220	236.160800	101.152.220.201.itc.com.ar	10.3.13.101	HTTP
1222	236.190844	10.3.13.101	101.152.220.201.itc.com.ar	HTTP
1224	237.025219	101.152.220.201.itc.com.ar	10.3.13.101	HTTP
1231	251.073395	10.3.13.101	ip.anysrc.net	HTTP
1233	251.219323	ip.anysrc.net	10.3.13.101	HTTP
3458	393.641008	10.3.13.101	ip-144-250.balifiber.id	HTTP
3462	394.534185	ip-144-250.balifiber.id	10.3.13.101	HTTP
3475	396.180268	10.3.13.101	ip-144-250.balifiber.id	HTTP
3478	397.048160	ip-144-250.balifiber.id	10.3.13.101	HTTP

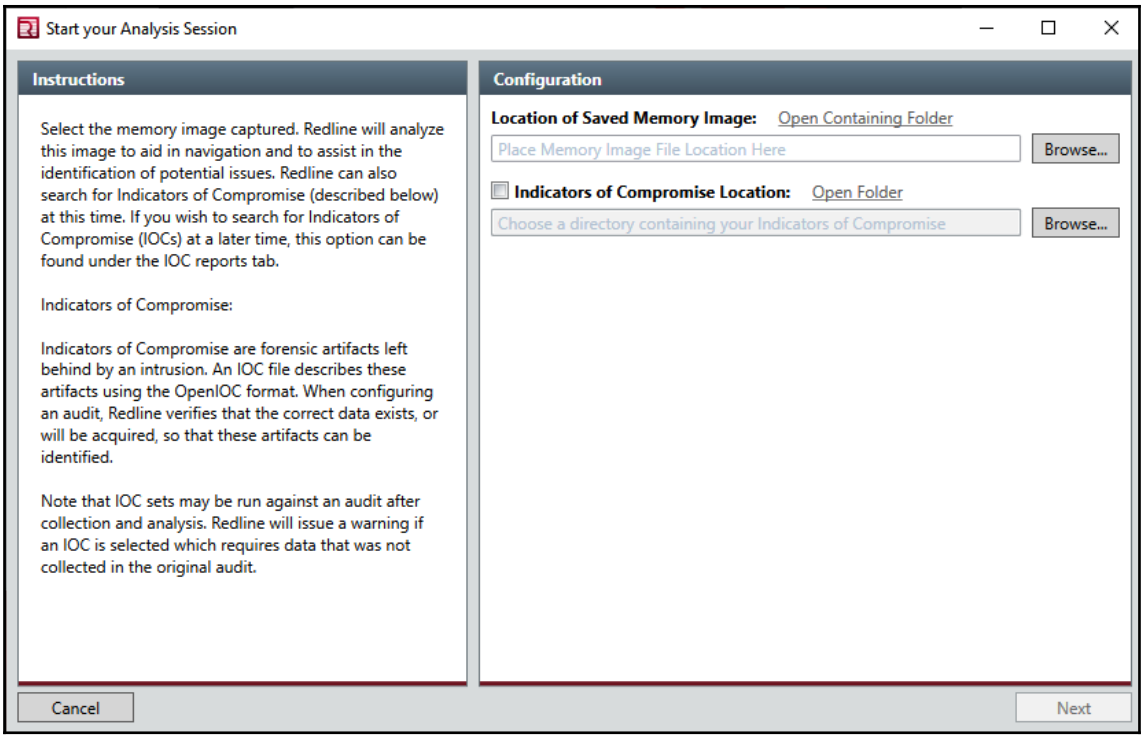

http
No.
Time
Source
6 0.739961
10.3.13.101
222 6.
244 42
505 43
514 69
651 10
657 13
1220 23
1222 23
1224 23
1231 25
1233 25
3458 39
3462 39
3475 39
3478 39
com.ar
com.ar
com.ar
.id
.id
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
Frame 222
9 bytes
Ethernet
:2a:b6:
Internet
hse.com
Transmission Control Protocol, Src Port: 80, Dst

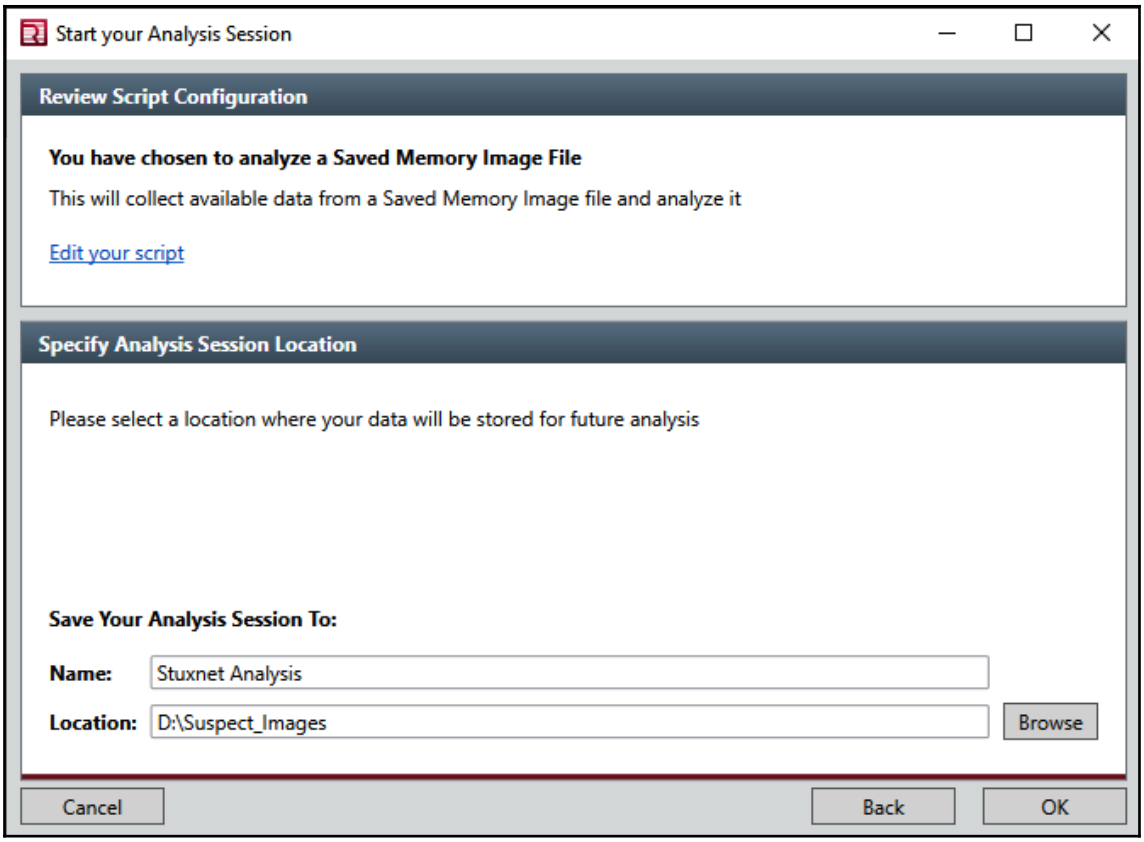

Wireshark · Follow TCP Stream (tcp.stream eq 0) · 2019-03-13-Emotet-infection-with-Trickbot.pcap
GET /wp-includes/deo7t-dcaum4-fykaarrdt/ HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: rozhan-hse.com
DNT: 1
Connection: Keep-Alive
HTTP/1.1 200 OK
Set-Cookie: 5c897cd465339=1552514260; expires=Wed, 13-Mar-2019 21:58:40 GMT; Max-Age=60; path=/
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Last-Modified: Wed, 13 Mar 2019 21:57:40 GMT
Expires: Wed, 13 Mar 2019 21:57:40 GMT
Content-Type: application/msword
Content-Disposition: attachment; filename="US5173209967.doc"
Content-Transfer-Encoding: binary
Transfer-Encoding: chunked
Date: Wed, 13 Mar 2019 21:57:40 GMT
Server: LiteSpeed
Connection: Keep-Alive
2000
1 client pkt, 153 server pkts, 1 turn.
Entire conversation (207 kB)
Show and save data as
ASCII
Stream
0
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help

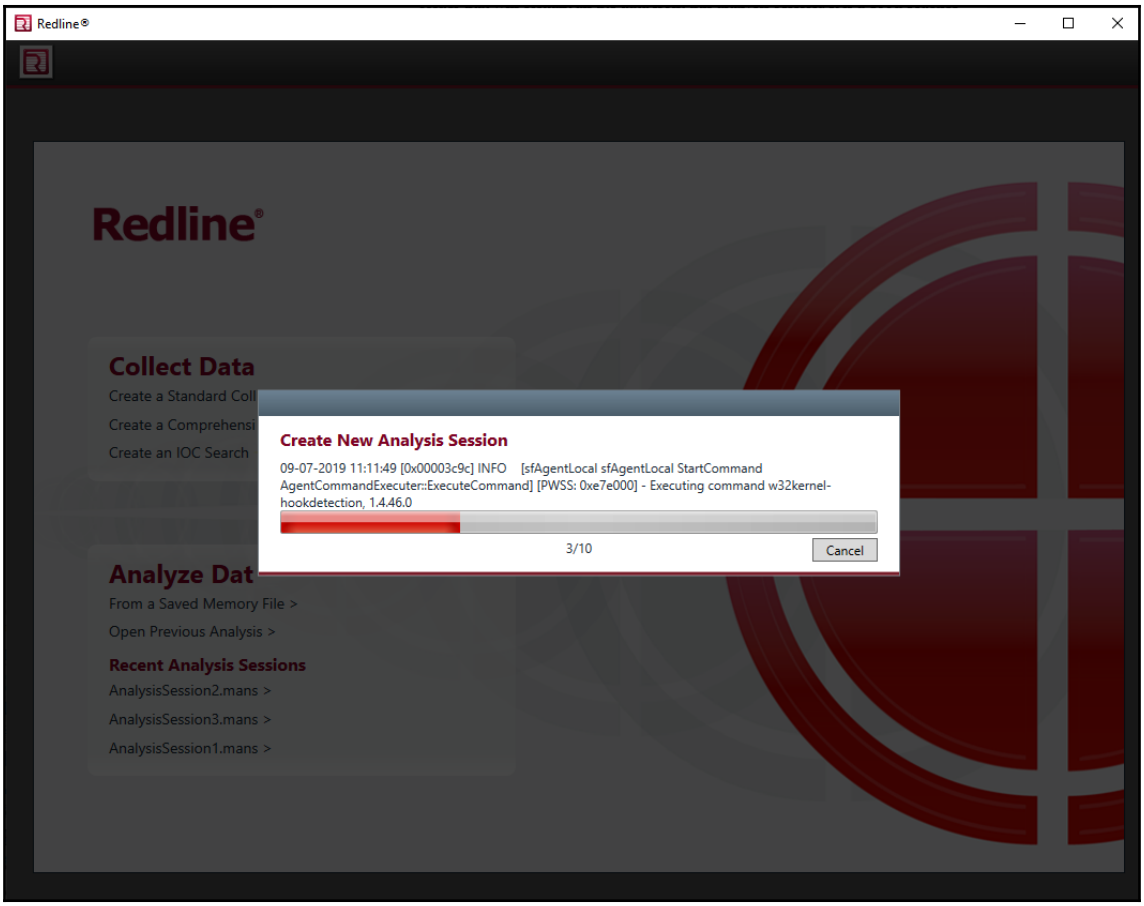

Wireshark · Export · HTTP object list
Packet
Hostname
Content Type
Size
Filename
222 rozhan-hse.com application/msword 206 kB deo7t-dcaum4-fykaarrdt
505 aliyev.org 0 309 kB oX6
651 201.220.152.101 text/html 102 kB \
1220 201.220.152.101 text/html 485 kB \
1224 201.220.152.101 text/html 148 bytes \
1233 ip.anysrc.net text/plain 13 bytes plain
3458 103.119.144.250 multipart/form-data 286 bytes 83
3462 103.119.144.250 text/plain 3 bytes 83
3475 103.119.144.250 multipart/form-data 262 bytes 81
3478 103.119.144.250 text/plain 3 bytes 81
3623 103.119.144.250:8082 multipart/form-data 2105 bytes 90
3634 103.119.144.250:8082 text/plain 3 bytes 90
4049 91.200.100.233 image/png 405 kB radiance.png
4060 103.119.144.250:8082 multipart/form-data 4674 bytes 90
4064 103.119.144.250:8082 text/plain 3 bytes 90
4516 91.200.100.233 image/png 405 kB worming.png
7412 91.200.100.233 image/png 405 kB table.png
7923 91.200.100.233 image/png 405 kB radiance.png
Text Filter:
Save
Save All
Close
Help

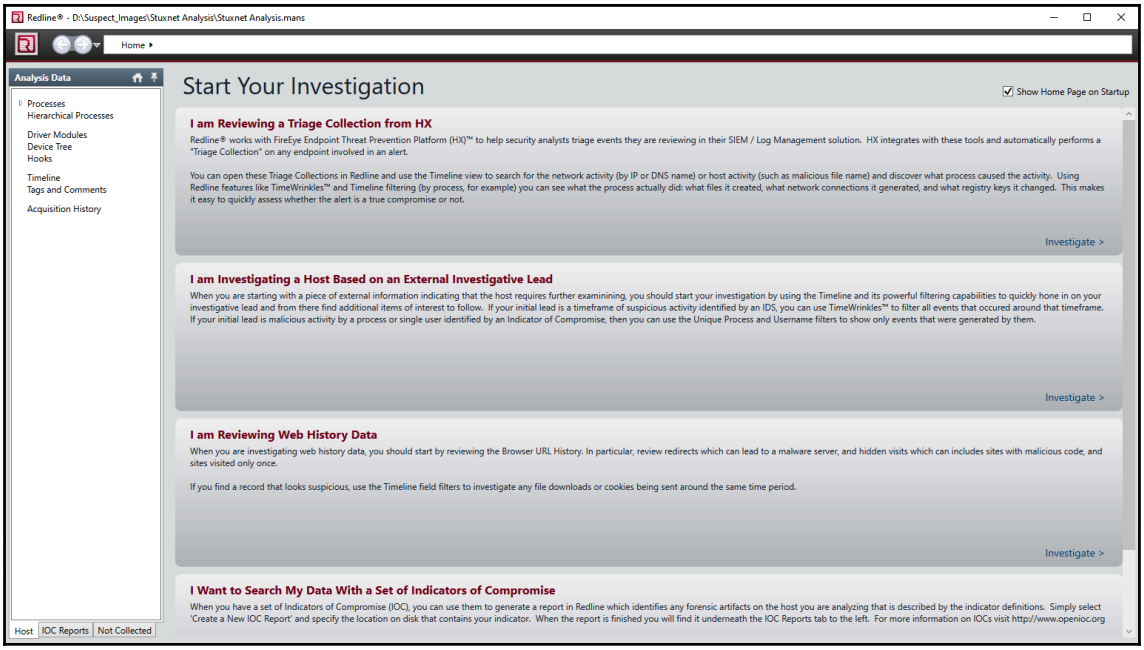
Chapter 8: Analyzing System Memory

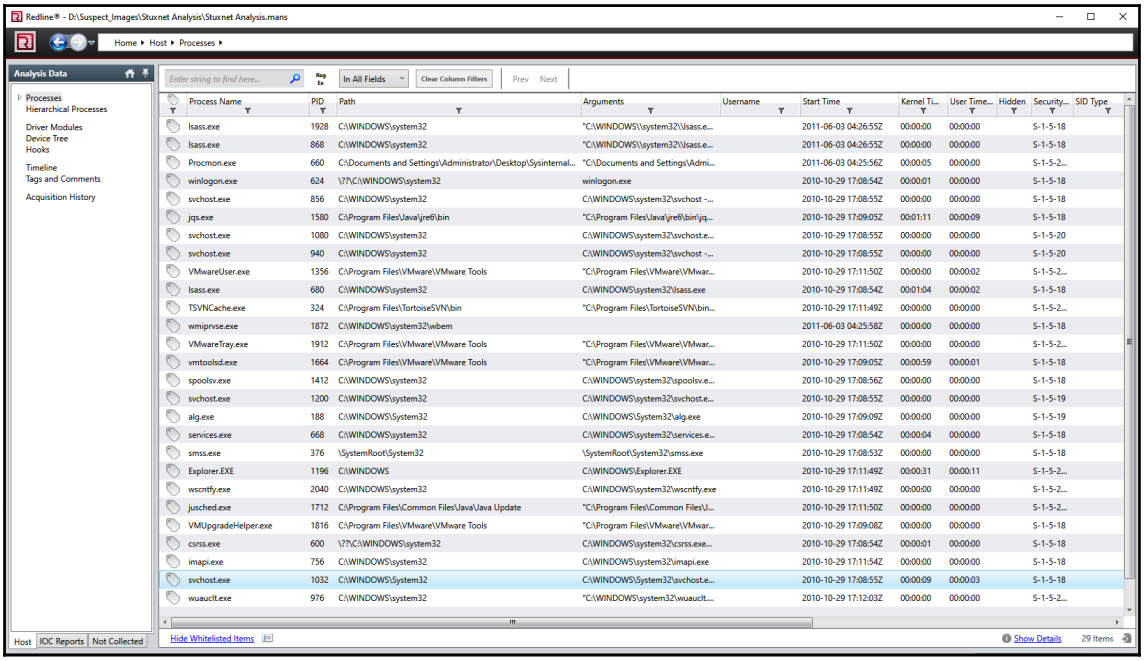



Start your Analysis Session
Instructions
Select the memory image captured. Redline will analyze this image to aid in navigation and to assist in the identification of potential issues. Redline can also search for Indicators of Compromise (described below) at this time. If you wish to search for Indicators of Compromise (IOCs) at a later time, this option can be found under the IOC reports tab.
Indicators of Compromise:
Indicators of Compromise are forensic artifacts left behind by an intrusion. An IOC file describes these artifacts using the OpenIOC format. When configuring an audit, Redline verifies that the correct data exists, or will be acquired, so that these artifacts can be identified.
Note that IOC sets may be run against an audit after collection and analysis. Redline will issue a warning if an IOC is selected which requires data that was not collected in the original audit.
Configuration
Location of Saved Memory Image:
Open Containing Folder
Place Memory Image File Location Here
Browse...
Indicators of Compromise Location:
Open Folder
Choose a directory containing your Indicators of Compromise
Browse...
Cancel
Next

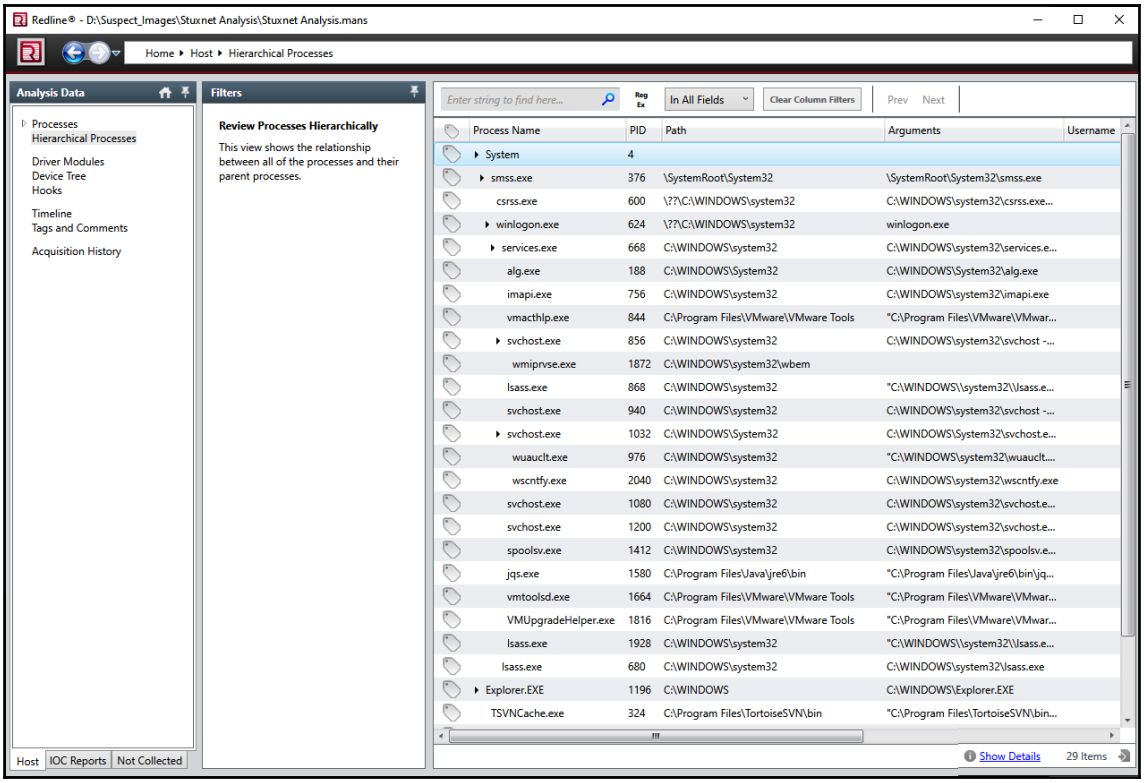

Start your Analysis Session
Review Script Configuration
You have chosen to analyze a Saved Memory Image File
This will collect available data from a Saved Memory Image file and analyze it
Edit your script
Specify Analysis Session Location
Please select a location where your data will be stored for future analysis
Save Your Analysis Session To:
Name:
Stuxnet Analysis
Location:
D:\Suspect_Images
Browse
Cancel
Back
OK

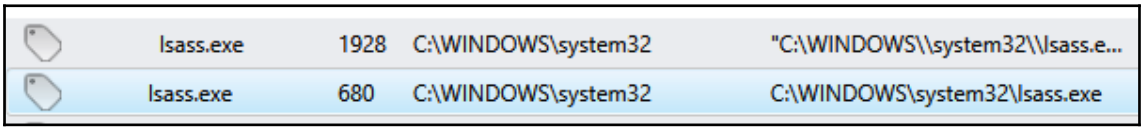

Redline®
Redline®
Collect Data
Create a Standard Coll
Create a Comprehensi
Create an IOC Search
Analyze Dat
From a Saved Memory File >
Open Previous Analysis >
Recent Analysis Sessions
AnalysisSession2.mans >
AnalysisSession3.mans >
AnalysisSession1.mans >
Create New Analysis Session
09-07-2019 11:11:49 [0x00003c9c] INFO [sfAgentLocal sfAgentLocal StartCommand AgentCommandExecuter::ExecuteCommand] [PWSS: 0xe7e000] - Executing command w32kernel-hookdetection, 1.4.46.0
3/10
Cancel

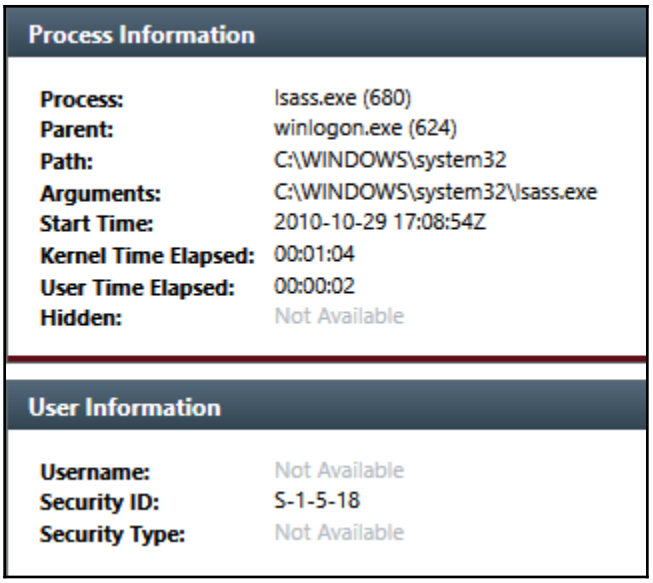

Redline® - D:\Suspect_Images\Stuxnet Analysis\Stuxnet Analysis.mans
Home
Analysis Data
Processes
Hierarchical Processes
Driver Modules
Device Tree
Hooks
Timeline
Tags and Comments
Acquisition History
Start Your Investigation
Show Home Page on Startup
I am Reviewing a Triage Collection from HX
Redline® works with FireEye Endpoint Threat Prevention Platform (HX)™ to help security analysts triage events they are reviewing in their SIEM / Log Management solution. HX integrates with these tools and automatically performs a "Triage Collection" on any endpoint involved in an alert.
You can open these Triage Collections in Redline and use the Timeline view to search for the network activity (by IP or DNS name) or host activity (such as malicious file name) and discover what process caused the activity. Using Redline features like TimeWrinkles™ and Timeline filtering (by process, for example) you can see what the process actually did: what files it created, what network connections it generated, and what registry keys it changed. This makes it easy to quickly assess whether the alert is a true compromise or not.
Investigate >
I am Investigating a Host Based on an External Investigative Lead
When you are starting with a piece of external information indicating that the host requires further examinining, you should start your investigation by using the Timeline and its powerful filtering capabilities to quickly hone in on your investigative lead and from there find additional items of interest to follow. If your initial lead is a timeframe of suspicious activity identified by an IDS, you can use TimeWrinkles™ to filter all events that occured around that timeframe. If your initial lead is malicious activity by a process or single user identified by an Indicator of Compromise, then you can use the Unique Process and Username filters to show only events that were generated by them.
Investigate >
I am Reviewing Web History Data
When you are investigating web history data, you should start by reviewing the Browser URL History. In particular, review redirects which can lead to a malware server, and hidden visits which can includes sites with malicious code, and sites visited only once.
If you find a record that looks suspicious, use the Timeline field filters to investigate any file downloads or cookies being sent around the same time period.
Investigate >
I Want to Search My Data With a Set of Indicators of Compromise
When you have a set of Indicators of Compromise (IOC), you can use them to generate a report in Redline which identifies any forensic artifacts on the host you are analyzing that is described by the indicator definitions. Simply select 'Create a New IOC Report' and specify the location on disk that contains your indicator. When the report is finished you will find it underneath the IOC Reports tab to the left. For more information on IOCs visit http://www.openioc.org
Host
IOC Reports
Not Collected

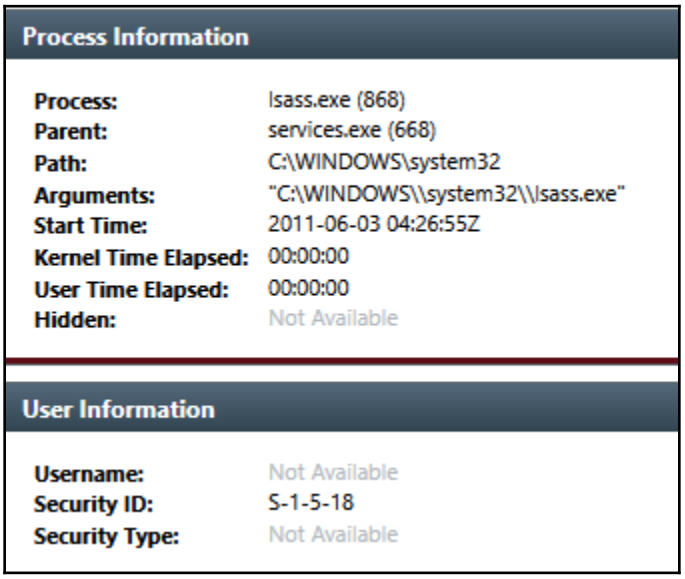

Redline® - D:\Suspect_Images\Stuxnet Analysis\Stuxnet Analysis.mans
Home ▸ Host ▸ Processes ▸
Analysis Data
Processes
Hierarchical Processes
Driver Modules
Device Tree
Hooks
Timeline
Tags and Comments
Acquisition History
Enter string to find here...
In All Fields
Clear Column Filters
Prev
Next
Process Name
PID
Path
Arguments
Username
Start Time
Kernel Ti...
User Time...
Hidden
Security...
SID Type
lsass.exe 1928 C:\WINDOWS\system32 "C:\WINDOWS\\system32\\lsass.e... 2011-06-03 04:26:55Z 00:00:00 00:00:00 S-1-5-18
lsass.exe 868 C:\WINDOWS\system32 "C:\WINDOWS\\system32\\lsass.e... 2011-06-03 04:26:55Z 00:00:00 00:00:00 S-1-5-18
Procmon.exe 660 C:\Documents and Settings\Administrator\Desktop\Sysinternal... "C:\Documents and Settings\Admi... 2011-06-03 04:25:56Z 00:00:05 00:00:00 S-1-5-2...
winlogon.exe 624 \??\C:\WINDOWS\system32 winlogon.exe 2010-10-29 17:08:54Z 00:00:01 00:00:00 S-1-5-18
svchost.exe 856 C:\WINDOWS\system32 C:\WINDOWS\system32\svchost -... 2010-10-29 17:08:55Z 00:00:00 00:00:00 S-1-5-18
jqs.exe 1580 C:\Program Files\Java\jre6\bin "C:\Program Files\Java\jre6\bin\jq... 2010-10-29 17:09:05Z 00:01:11 00:00:09 S-1-5-18
svchost.exe 1080 C:\WINDOWS\system32 C:\WINDOWS\system32\svchost.e... 2010-10-29 17:08:55Z 00:00:00 00:00:00 S-1-5-20
svchost.exe 940 C:\WINDOWS\system32 C:\WINDOWS\system32\svchost -... 2010-10-29 17:08:55Z 00:00:00 00:00:00 S-1-5-20
VMwareUser.exe 1356 C:\Program Files\VMware\VMware Tools "C:\Program Files\VMware\VMwar... 2010-10-29 17:11:50Z 00:00:00 00:00:02 S-1-5-2...
lsass.exe 680 C:\WINDOWS\system32 C:\WINDOWS\system32\lsass.exe 2010-10-29 17:08:54Z 00:01:04 00:00:02 S-1-5-18
TSVNCache.exe 324 C:\Program Files\TortoiseSVN\bin "C:\Program Files\TortoiseSVN\bin... 2010-10-29 17:11:49Z 00:00:00 00:00:00 S-1-5-2...
wmiprvse.exe 1872 C:\WINDOWS\system32\wbem 2011-06-03 04:25:58Z 00:00:00 00:00:00 S-1-5-18
VMwareTray.exe 1912 C:\Program Files\VMware\VMware Tools "C:\Program Files\VMware\VMwar... 2010-10-29 17:11:50Z 00:00:00 00:00:00 S-1-5-2...
vmtoolsd.exe 1664 C:\Program Files\VMware\VMware Tools "C:\Program Files\VMware\VMwar... 2010-10-29 17:09:05Z 00:00:59 00:00:01 S-1-5-18
spoolsv.exe 1412 C:\WINDOWS\system32 C:\WINDOWS\system32\spoolsv.e... 2010-10-29 17:08:56Z 00:00:00 00:00:00 S-1-5-18
svchost.exe 1200 C:\WINDOWS\system32 C:\WINDOWS\system32\svchost.e... 2010-10-29 17:08:55Z 00:00:00 00:00:00 S-1-5-19
alg.exe 188 C:\WINDOWS\System32 C:\WINDOWS\System32\alg.exe 2010-10-29 17:09:09Z 00:00:00 00:00:00 S-1-5-19
services.exe 668 C:\WINDOWS\system32 C:\WINDOWS\system32\services.e... 2010-10-29 17:08:54Z 00:00:04 00:00:00 S-1-5-18
smss.exe 376 \SystemRoot\System32 \SystemRoot\System32\smss.exe 2010-10-29 17:08:53Z 00:00:00 00:00:00 S-1-5-18
Explorer.EXE 1196 C:\WINDOWS C:\WINDOWS\Explorer.EXE 2010-10-29 17:11:49Z 00:00:31 00:00:11 S-1-5-2...
wscntfy.exe 2040 C:\WINDOWS\system32 C:\WINDOWS\system32\wscntfy.exe 2010-10-29 17:11:49Z 00:00:00 00:00:00 S-1-5-2...
jusched.exe 1712 C:\Program Files\Common Files\Java\Java Update "C:\Program Files\Common Files\J... 2010-10-29 17:11:50Z 00:00:00 00:00:00 S-1-5-2...
VMUpgradeHelper.exe 1816 C:\Program Files\VMware\VMware Tools "C:\Program Files\VMware\VMwar... 2010-10-29 17:09:08Z 00:00:00 00:00:00 S-1-5-18
csrss.exe 600 \??\C:\WINDOWS\system32 C:\WINDOWS\system32\csrss.exe... 2010-10-29 17:08:54Z 00:00:01 00:00:00 S-1-5-18
imapi.exe 756 C:\WINDOWS\system32 C:\WINDOWS\system32\imapi.exe 2010-10-29 17:11:54Z 00:00:00 00:00:00 S-1-5-18
svchost.exe 1032 C:\WINDOWS\System32 C:\WINDOWS\System32\svchost.e... 2010-10-29 17:08:55Z 00:00:09 00:00:03 S-1-5-18
wuauclt.exe 976 C:\WINDOWS\system32 "C:\WINDOWS\system32\wuauclt.... 2010-10-29 17:12:03Z 00:00:00 00:00:00 S-1-5-2...
Hide Whitelisted Items
Show Details
29 Items
Host
IOC Reports
Not Collected

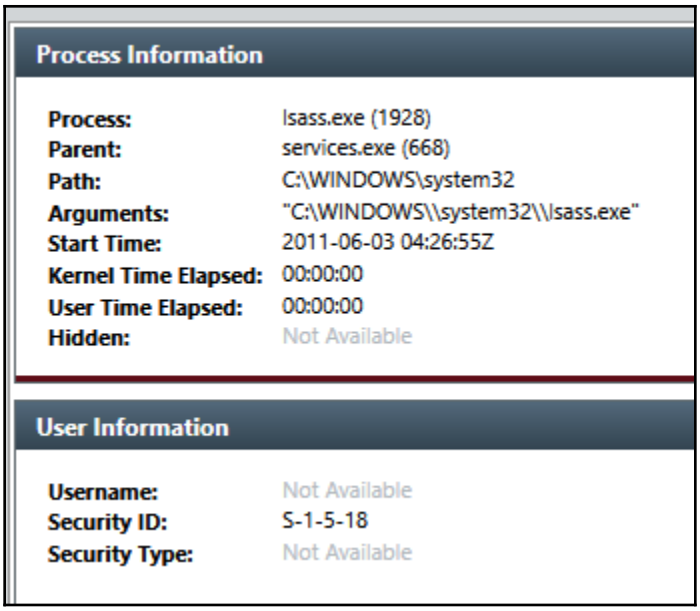
lsass.exe	1928	C:\WINDOWS\system32	"C:\WINDOWS\\system32\\lsass.exe"
lsass.exe	868	C:\WINDOWS\system32	"C:\WINDOWS\\system32\\lsass.exe"
Procmon.exe	660	C:\Documents and Settings\Administrator\Desktop\Sysinternal...	"C:\Documents and Settings\Administrator\Deskto...
winlogon.exe	624	\??\C:\WINDOWS\system32	winlogon.exe
svchost.exe	856	C:\WINDOWS\system32	C:\WINDOWS\system32\svchost -k DcomLaunch
jqs.exe	1580	C:\Program Files\Java\jre6\bin	"C:\Program Files\Java\jre6\bin\jqs.exe" -service -c...
svchost.exe	1080	C:\WINDOWS\system32	C:\WINDOWS\system32\svchost.exe -k NetworkSe...
svchost.exe	940	C:\WINDOWS\system32	C:\WINDOWS\system32\svchost -k rpcss
VMwareUser.exe	1356	C:\Program Files\VMware\VMware Tools	"C:\Program Files\VMware\VMware Tools\VMware...
lsass.exe	680	C:\WINDOWS\system32	C:\WINDOWS\system32\lsass.exe

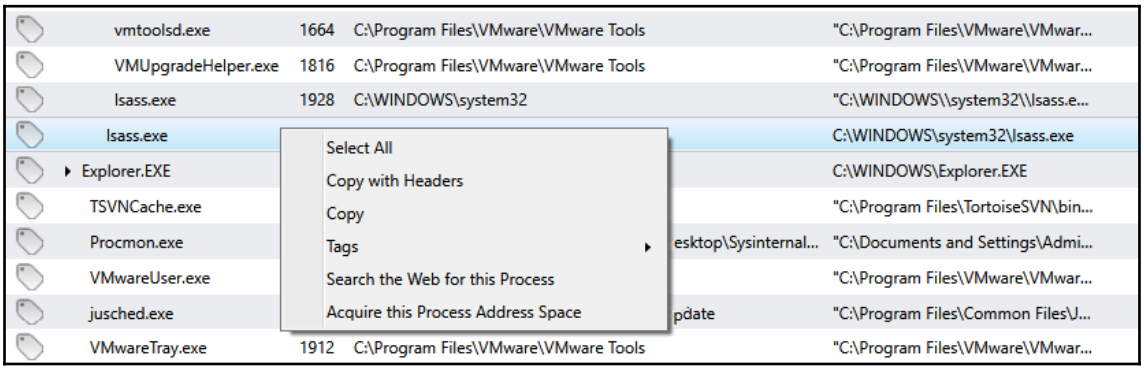


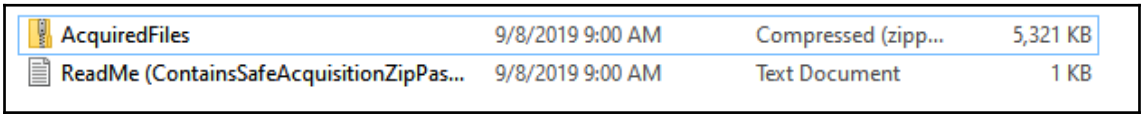



Process Information
Process: lsass.exe (680)
Parent: winlogon.exe (624)
Path: C:\WINDOWS\system32
Arguments: C:\WINDOWS\system32\lsass.exe
Start Time: 2010-10-29 17:08:54Z
Kernel Time Elapsed: 00:01:04
User Time Elapsed: 00:00:02
Hidden: Not Available
User Information
Username: Not Available
Security ID: S-1-5-18
Security Type: Not Available


Process Information
Process: lsass.exe (868)
Parent: services.exe (668)
Path: C:\WINDOWS\system32
Arguments: "C:\WINDOWS\\system32\\lsass.exe"
Start Time: 2011-06-03 04:26:55Z
Kernel Time Elapsed: 00:00:00
User Time Elapsed: 00:00:00
Hidden: Not Available
User Information
Username: Not Available
Security ID: S-1-5-18
Security Type: Not Available


Process Information
Process: lsass.exe (1928)
Parent: services.exe (668)
Path: C:\WINDOWS\system32
Arguments: "C:\WINDOWS\\system32\\lsass.exe"
Start Time: 2011-06-03 04:26:55Z
Kernel Time Elapsed: 00:00:00
User Time Elapsed: 00:00:00
Hidden: Not Available
User Information
Username: Not Available
Security ID: S-1-5-18
Security Type: Not Available


vmtoolsd.exe 1664 C:\Program Files\VMware\VMware Tools "C:\Program Files\VMware\VMwar...
VMUpgradeHelper.exe 1816 C:\Program Files\VMware\VMware Tools "C:\Program Files\VMware\VMwar...
lsass.exe 1928 C:\WINDOWS\system32 "C:\WINDOWS\\system32\\lsass.e...
lsass.exe C:\WINDOWS\system32\lsass.exe
Explorer.EXE C:\WINDOWS\Explorer.EXE
TSVNCache.exe "C:\Program Files\TortoiseSVN\bin...
Procmon.exe esktop\Sysinternal... "C:\Documents and Settings\Admi...
VMwareUser.exe "C:\Program Files\VMware\VMwar...
jusched.exe pdate "C:\Program Files\Common Files\J...
VMwareTray.exe 1912 C:\Program Files\VMware\VMware Tools "C:\Program Files\VMware\VMwar...
Select All
Copy with Headers
Copy
Tags
Search the Web for this Process
Acquire this Process Address Space


AcquiredFiles 9/8/2019 9:00 AM Compressed (zipp... 5,321 KB
ReadMe (ContainsSafeAcquisitionZipPas... 9/8/2019 9:00 AM Text Document 1 KB

```
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/mnt/d/Suspect_Images/cridex_laptop.mem)
                      PAE type : PAE
                           DTB : 0x2fe000L
                          KDBG : 0x80545ae0L
          Number of Processors : 1
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2012-07-22 02:45:08 UTC+0000
     Image local date and time : 2012-07-21 22:45:08 -0400
```

```
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------
0x823c89c8 System                    4      0     53      240 ------      0
0x822f1020 smss.exe                368      4      3       19 ------      0 2012-07-22 02:42:31 UTC+0000
0x822a0598 csrss.exe               584    368      9      326      0      0 2012-07-22 02:42:32 UTC+0000
0x82298700 winlogon.exe            608    368     23      519      0      0 2012-07-22 02:42:32 UTC+0000
0x81e2ab28 services.exe            652    608     16      243      0      0 2012-07-22 02:42:32 UTC+0000
0x81e2a3b8 lsass.exe               664    608     24      330      0      0 2012-07-22 02:42:32 UTC+0000
0x82311360 svchost.exe             824    652     20      194      0      0 2012-07-22 02:42:33 UTC+0000
0x81e29ab8 svchost.exe             908    652      9      226      0      0 2012-07-22 02:42:33 UTC+0000
0x823001d0 svchost.exe            1004    652     64     1118      0      0 2012-07-22 02:42:33 UTC+0000
0x821dfda0 svchost.exe            1056    652      5       60      0      0 2012-07-22 02:42:33 UTC+0000
0x82295650 svchost.exe            1220    652     15      197      0      0 2012-07-22 02:42:35 UTC+0000
0x821dea70 explorer.exe           1484   1464     17      415      0      0 2012-07-22 02:42:36 UTC+0000
0x81eb17b8 spoolsv.exe            1512    652     14      113      0      0 2012-07-22 02:42:36 UTC+0000
0x81e7bda0 reader_sl.exe          1640   1484      5       39      0      0 2012-07-22 02:42:36 UTC+0000
0x820e8da0 alg.exe                 788    652      7      104      0      0 2012-07-22 02:43:01 UTC+0000
0x821fcda0 wuauclt.exe            1136   1004      8      173      0      0 2012-07-22 02:43:46 UTC+0000
0x8205bda0 wuauclt.exe            1588   1004      5      132      0      0 2012-07-22 02:44:01 UTC+0000
```

```
Volatility Foundation Volatility Framework 2.6
Offset(P)          Name                PID   PPID PDB        Time created
------------------ ---------------- ------ ------ ---------- ------------------------------
0x0000000002029ab8 svchost.exe         908    652 0x079400e0 2012-07-22 02:42:33 UTC+0000
0x000000000202a3b8 lsass.exe           664    608 0x079400a0 2012-07-22 02:42:32 UTC+0000
0x000000000202ab28 services.exe        652    608 0x07940080 2012-07-22 02:42:32 UTC+0000
0x000000000207bda0 reader_sl.exe      1640   1484 0x079401e0 2012-07-22 02:42:36 UTC+0000
0x00000000020b17b8 spoolsv.exe        1512    652 0x079401c0 2012-07-22 02:42:36 UTC+0000
0x000000000225bda0 wuauclt.exe        1588   1004 0x07940200 2012-07-22 02:44:01 UTC+0000
0x00000000022e8da0 alg.exe             788    652 0x07940140 2012-07-22 02:43:01 UTC+0000
0x00000000023dea70 explorer.exe       1484   1464 0x079401a0 2012-07-22 02:42:36 UTC+0000
0x00000000023dfda0 svchost.exe        1056    652 0x07940120 2012-07-22 02:42:33 UTC+0000
0x00000000023fcda0 wuauclt.exe        1136   1004 0x07940180 2012-07-22 02:43:46 UTC+0000
0x0000000002495650 svchost.exe        1220    652 0x07940160 2012-07-22 02:42:35 UTC+0000
0x0000000002498700 winlogon.exe        608    368 0x07940060 2012-07-22 02:42:32 UTC+0000
0x00000000024a0598 csrss.exe           584    368 0x07940040 2012-07-22 02:42:32 UTC+0000
0x00000000024f1020 smss.exe            368      4 0x07940020 2012-07-22 02:42:31 UTC+0000
0x0000000025001d0 svchost.exe         1004    652 0x07940100 2012-07-22 02:42:33 UTC+0000
0x0000000002511360 svchost.exe         824    652 0x079400c0 2012-07-22 02:42:33 UTC+0000
0x00000000025c89c8 System                4      0 0x002fe000
```

```
Volatility Foundation Volatility Framework 2.6
Name                                           Pid   PPid   Thds   Hnds Time
---------------------------------------------- ------ ------ ------ ------ ----
 0x823c89c8:System                                4      0     53    240 1970-01-01 00:00:00 UTC+0000
. 0x822f1020:smss.exe                           368      4      3     19 2012-07-22 02:42:31 UTC+0000
.. 0x82298700:winlogon.exe                      608    368     23    519 2012-07-22 02:42:32 UTC+0000
... 0x81e2ab28:services.exe                     652    608     16    243 2012-07-22 02:42:32 UTC+0000
.... 0x821dfda0:svchost.exe                    1056    652      5     60 2012-07-22 02:42:33 UTC+0000
.... 0x81eb17b8:spoolsv.exe                    1512    652     14    113 2012-07-22 02:42:36 UTC+0000
.... 0x81e29ab8:svchost.exe                     908    652      9    226 2012-07-22 02:42:33 UTC+0000
.... 0x823001d0:svchost.exe                    1004    652     64   1118 2012-07-22 02:42:33 UTC+0000
..... 0x8205bda0:wuauclt.exe                   1588   1004      5    132 2012-07-22 02:44:01 UTC+0000
..... 0x821fcda0:wuauclt.exe                   1136   1004      8    173 2012-07-22 02:43:46 UTC+0000
.... 0x82311360:svchost.exe                     824    652     20    194 2012-07-22 02:42:33 UTC+0000
.... 0x820e8da0:alg.exe                         788    652      7    104 2012-07-22 02:43:01 UTC+0000
.... 0x82295650:svchost.exe                    1220    652     15    197 2012-07-22 02:42:35 UTC+0000
... 0x81e2a3b8:lsass.exe                        664    608     24    330 2012-07-22 02:42:32 UTC+0000
.. 0x822a0598:csrss.exe                         584    368      9    326 2012-07-22 02:42:32 UTC+0000
 0x821dea70:explorer.exe                       1484   1464     17    415 2012-07-22 02:42:36 UTC+0000
. 0x81e7bda0:reader_sl.exe                     1640   1484      5     39 2012-07-22 02:42:36 UTC+0000
```

```
0x821dea70:explorer.exe                        1484   1464
 0x81e7bda0:reader_sl.exe                      1640   1484
```

```
Volatility Foundation Volatility Framework 2.6
************************************************************************
reader_sl.exe pid:   1640
Command line : "C:\Program Files\Adobe\Reader 9.0\Reader\Reader_sl.exe"
Service Pack 3

Base             Size  LoadCount LoadTime                       Path
---------- ---------- ---------- ------------------------------ ----
0x00400000     0xa000     0xffff                                C:\Program Files\Adobe\Reader 9.0\Reader\Reader_sl.exe
0x7c900000    0xaf000     0xffff                                C:\WINDOWS\system32\ntdll.dll
0x7c800000    0xf6000     0xffff                                C:\WINDOWS\system32\kernel32.dll
0x7e410000    0x91000     0xffff                                C:\WINDOWS\system32\USER32.dll
0x77f10000    0x49000     0xffff                                C:\WINDOWS\system32\GDI32.dll
0x77dd0000    0x9b000     0xffff                                C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000    0x92000     0xffff                                C:\WINDOWS\system32\RPCRT4.dll
0x77fe0000    0x11000     0xffff                                C:\WINDOWS\system32\Secur32.dll
0x7c9c0000   0x817000     0xffff                                C:\WINDOWS\system32\SHELL32.dll
0x77c10000    0x58000     0xffff                                C:\WINDOWS\system32\msvcrt.dll
0x77f60000    0x76000     0xffff                                C:\WINDOWS\system32\SHLWAPI.dll
0x7c420000    0x87000     0xffff                                C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.762_x-ww_6b128700\MSVCP80.dll
0x78130000    0x9b000     0xffff                                C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.762_x-ww_6b128700\MSVCR80.dll
0x773d0000   0x103000        0x1                                C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
0x5d090000    0x9a000        0x1                                C:\WINDOWS\system32\comctl32.dll
0x5ad70000    0x38000        0x2                                C:\WINDOWS\system32\uxtheme.dll
0x71ab0000    0x17000        0x1                                C:\WINDOWS\system32\WS2_32.dll
0x71aa0000     0x8000        0x1                                C:\WINDOWS\system32\WS2HELP.dll
```

```
Volatility Foundation Volatility Framework 2.6
Offset(V)     Pid     Handle     Access Type            Details
---------- ------ ---------- ---------- --------------- -------
0xe10096e0   1640        0x4    0xf0003 KeyedEvent      CritSecOutOfMemoryEvent
0xe159c970   1640        0x8        0x3 Directory       KnownDlls
0x82211678   1640        0xc   0x100020 File            \Device\HarddiskVolume1\Documents and Settings\Robert
0x82210208   1640       0x10   0x100020 File            \Device\HarddiskVolume1\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.762_x-ww_6b128700
0xe14916d0   1640       0x14    0xf000f Directory       Windows
0xe1c6a588   1640       0x18  0x21f0001 Port
0x82319610   1640       0x1c  0x21f0003 Event
0x8205a2a0   1640       0x20    0xf037f WindowStation   WinSta0
0x822f8168   1640       0x24    0xf01ff Desktop         Default
0x8205a2a0   1640       0x28    0xf037f WindowStation   WinSta0
0x82311280   1640       0x2c   0x100003 Semaphore
0x82234dd0   1640       0x30   0x100003 Semaphore
0xe1c042d0   1640       0x34  0x20f003f Key             MACHINE
0xe16ce308   1640       0x38    0x2000f Directory       BaseNamedObjects
0x8213d0e0   1640       0x3c   0x1f0003 Semaphore       shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
0xe1835648   1640       0x40  0x20f003f Key             USER\S-1-5-21-789336058-261478967-1417001333-1003
0x820d2f28   1640       0x44   0x10002f File            \Device\HarddiskVolume1\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
0xe1c72300   1640       0x48   0x1f0001 Port
0xe17d3938   1640       0x4c        0x4 Section
0x81de18c8   1640       0x50   0x1f0003 Event
0x822924c8   1640       0x54   0x1f03ff Thread          TID 1648 PID 1640
0x821dd728   1640       0x58   0x1f0003 Event
0x82196418   1640       0x5c   0x1f0003 Event
0x820022e0   1640       0x60   0x1f0003 Event
0x82002a18   1640       0x64   0x1f0003 Event
0x822924c8   1640       0x68   0x1f03ff Thread          TID 1648 PID 1640
0x821dc270   1640       0x6c  0x100001 File            \Device\KsecDD
0xe1c5cfb8   1640       0x70       0x10 Key             USER\S-1-5-21-789336058-261478967-1417001333-1003\SOFTWARE\MICROSOFT\WSH\8149A9A8
0xe1c6c030   1640       0x74       0x18 Token
0x81de1e68   1640       0x78   0x1f0003 Event
0x81dd2e08   1640       0x7c   0x1f0003 IoCompletion
0x81de3c70   1640       0x80   0x1f0003 IoCompletion
0x81dd2e08   1640       0x84   0x1f0003 IoCompletion
0x822fdb00   1640       0x88   0x1f0001 Mutant          XMM00000668
0x822d0d98   1640       0x8c   0x1f0003 Event           XME00000668
0xe154db20   1640       0x90       0x10 Key             USER\S-1-5-21-789336058-261478967-1417001333-1003\SOFTWARE\MICROSOFT\WSH\9DBBCFAD
0x820fd260   1640       0x94   0x1f0003 Semaphore       shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}
0x81e9d708   1640       0x98   0x1f0001 Mutant          XMR8149A9A8
0x81e1d3c0   1640       0x9c   0x1f0003 Event
```

```
Volatility Foundation Volatility Framework 2.6
Pid      Process            Base       InLoad InInit InMem MappedPath
-------- ------------------ ---------- ------ ------ ----- ----------
    1640 reader_sl.exe      0x00400000 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      0x773d0000 True   True   True  \WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6
    1640 reader_sl.exe      0x7c420000 True   True   True  \WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b
    1640 reader_sl.exe      0x5d090000 True   True   True  \WINDOWS\system32\comctl32.dll
    1640 reader_sl.exe      0x77f60000 True   True   True  \WINDOWS\system32\shlwapi.dll
    1640 reader_sl.exe      0x77f10000 True   True   True  \WINDOWS\system32\gdi32.dll
    1640 reader_sl.exe      0x78130000 True   True   True  \WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b
    1640 reader_sl.exe      0x71aa0000 True   True   True  \WINDOWS\system32\ws2help.dll
    1640 reader_sl.exe      0x77e70000 True   True   True  \WINDOWS\system32\rpcrt4.dll
    1640 reader_sl.exe      0x71ab0000 True   True   True  \WINDOWS\system32\ws2_32.dll
    1640 reader_sl.exe      0x7c9c0000 True   True   True  \WINDOWS\system32\shell32.dll
    1640 reader_sl.exe      0x77dd0000 True   True   True  \WINDOWS\system32\advapi32.dll
    1640 reader_sl.exe      0x77fe0000 True   True   True  \WINDOWS\system32\secur32.dll
    1640 reader_sl.exe      0x7e410000 True   True   True  \WINDOWS\system32\user32.dll
    1640 reader_sl.exe      0x7c900000 True   True   True  \WINDOWS\system32\ntdll.dll
    1640 reader_sl.exe      0x77c10000 True   True   True  \WINDOWS\system32\msvcrt.dll
    1640 reader_sl.exe      0x5ad70000 True   True   True  \WINDOWS\system32\uxtheme.dll
```

```
0x00400000 True   False  True  \Program Files\Adobe\Reader 9.0\Reader\reader_sl.exe
```

```
Volatility Foundation Volatility Framework 2.6
Offset(P)  Name                PID pslist psscan thrdproc pspcid csrss session deskthrd ExitTime
---------- ---------------- ------ ------ ------ -------- ------ ----- ------- -------- --------
0x02498700 winlogon.exe        608 True   True   True     True   True  True    True
0x02511360 svchost.exe         824 True   True   True     True   True  True    True
0x022e8da0 alg.exe             788 True   True   True     True   True  True    True
0x020b17b8 spoolsv.exe        1512 True   True   True     True   True  True    True
0x0202ab28 services.exe        652 True   True   True     True   True  True    True
0x02495650 svchost.exe        1220 True   True   True     True   True  True    True
0x0207bda0 reader_sl.exe      1640 True   True   True     True   True  True    True
0x025001d0 svchost.exe        1004 True   True   True     True   True  True    True
0x02029ab8 svchost.exe         908 True   True   True     True   True  True    True
0x023fcda0 wuauclt.exe        1136 True   True   True     True   True  True    True
0x0225bda0 wuauclt.exe        1588 True   True   True     True   True  True    True
0x0202a3b8 lsass.exe           664 True   True   True     True   True  True    True
0x023dea70 explorer.exe       1484 True   True   True     True   True  True    True
0x023dfda0 svchost.exe        1056 True   True   True     True   True  True    True
0x024f1020 smss.exe            368 True   True   True     True   False False   False
0x025c89c8 System                4 True   True   True     True   False False   False
0x024a0598 csrss.exe           584 True   True   True     True   False True    True
```

```
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------ ---
0x02087620 172.16.112.128:1038      41.168.5.140:8080        1484
0x023a8008 172.16.112.128:1037      125.19.103.198:8080      1484
```

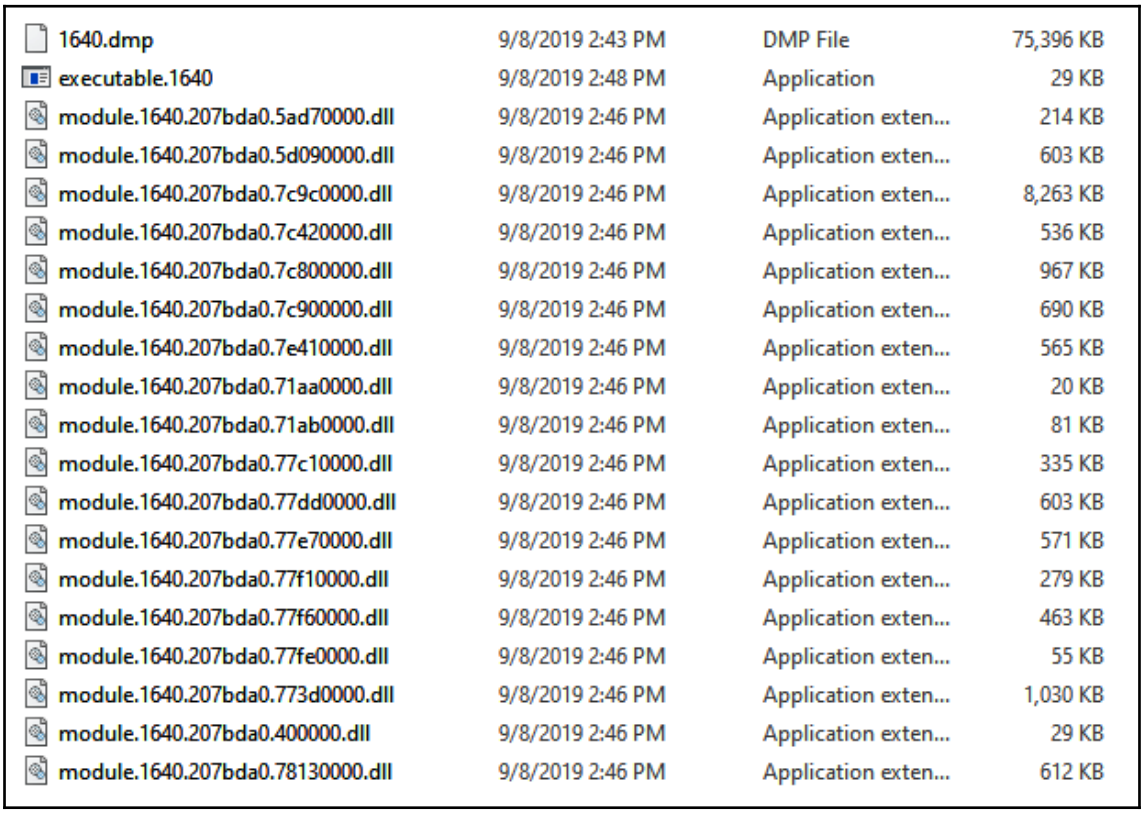
Communicating Files

Scanned	Detections	Type	Name
2019-07-26	54 / 70	Win32 EXE	MFC100JPN.DLL
2017-12-06	61 / 66	Win32 EXE	kb01445398.exe
2018-02-11	60 / 67	Win32 EXE	kb00113312.exe
2016-01-18	48 / 54	Win32 EXE	kb01397018.exe
2015-10-20	51 / 57	Win32 EXE	kb00591945.exe
2017-12-06	58 / 67	Win32 EXE	kb00421819.exe
2016-01-13	50 / 56	Win32 EXE	kb01382314.exe
2017-12-06	56 / 65	Win32 EXE	kb00578763.exe
2016-01-29	49 / 54	Win32 EXE	kb01300184.exe

```
Volatility Foundation Volatility Framework 2.6
************************************************************************
Writing reader_sl.exe [  1640] to 1640.dmp
```

```
Volatility Foundation Volatility Framework 2.6
Process(V) Name                 Module Base Module Name          Result
---------- -------------------- ----------- -------------------- ------
0x81e7bda0 reader_sl.exe        0x000400000 Reader_sl.exe        OK: module.1640.207bda0.400000.dll
0x81e7bda0 reader_sl.exe        0x07c900000 ntdll.dll            OK: module.1640.207bda0.7c900000.dll
0x81e7bda0 reader_sl.exe        0x078130000 MSVCR80.dll          OK: module.1640.207bda0.78130000.dll
0x81e7bda0 reader_sl.exe        0x07c420000 MSVCP80.dll          OK: module.1640.207bda0.7c420000.dll
0x81e7bda0 reader_sl.exe        0x077f10000 GDI32.dll            OK: module.1640.207bda0.77f10000.dll
0x81e7bda0 reader_sl.exe        0x077f60000 SHLWAPI.dll          OK: module.1640.207bda0.77f60000.dll
0x81e7bda0 reader_sl.exe        0x05ad70000 uxtheme.dll          OK: module.1640.207bda0.5ad70000.dll
0x81e7bda0 reader_sl.exe        0x077e70000 RPCRT4.dll           OK: module.1640.207bda0.77e70000.dll
0x81e7bda0 reader_sl.exe        0x05d090000 comctl32.dll         OK: module.1640.207bda0.5d090000.dll
0x81e7bda0 reader_sl.exe        0x071aa0000 WS2HELP.dll          OK: module.1640.207bda0.71aa0000.dll
0x81e7bda0 reader_sl.exe        0x071ab0000 WS2_32.dll           OK: module.1640.207bda0.71ab0000.dll
0x81e7bda0 reader_sl.exe        0x077c10000 msvcrt.dll           OK: module.1640.207bda0.77c10000.dll
0x81e7bda0 reader_sl.exe        0x07c9c0000 SHELL32.dll          OK: module.1640.207bda0.7c9c0000.dll
0x81e7bda0 reader_sl.exe        0x0773d0000 comctl32.dll         OK: module.1640.207bda0.773d0000.dll
0x81e7bda0 reader_sl.exe        0x077fe0000 Secur32.dll          OK: module.1640.207bda0.77fe0000.dll
0x81e7bda0 reader_sl.exe        0x07c800000 kernel32.dll         OK: module.1640.207bda0.7c800000.dll
0x81e7bda0 reader_sl.exe        0x07e410000 USER32.dll           OK: module.1640.207bda0.7e410000.dll
0x81e7bda0 reader_sl.exe        0x077dd0000 ADVAPI32.dll         OK: module.1640.207bda0.77dd0000.dll
```

```
Volatility Foundation Volatility Framework 2.6
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0x81e7bda0 0x00400000 reader_sl.exe        OK: executable.1640.exe
```



1640.dmp	9/8/2019 2:43 PM	DMP File	75,396 KB
executable.1640	9/8/2019 2:48 PM	Application	29 KB
module.1640.207bda0.5ad70000.dll	9/8/2019 2:46 PM	Application exten...	214 KB
module.1640.207bda0.5d090000.dll	9/8/2019 2:46 PM	Application exten...	603 KB
module.1640.207bda0.7c9c0000.dll	9/8/2019 2:46 PM	Application exten...	8,263 KB
module.1640.207bda0.7c420000.dll	9/8/2019 2:46 PM	Application exten...	536 KB
module.1640.207bda0.7c800000.dll	9/8/2019 2:46 PM	Application exten...	967 KB
module.1640.207bda0.7c900000.dll	9/8/2019 2:46 PM	Application exten...	690 KB
module.1640.207bda0.7e410000.dll	9/8/2019 2:46 PM	Application exten...	565 KB
module.1640.207bda0.71aa0000.dll	9/8/2019 2:46 PM	Application exten...	20 KB
module.1640.207bda0.71ab0000.dll	9/8/2019 2:46 PM	Application exten...	81 KB
module.1640.207bda0.77c10000.dll	9/8/2019 2:46 PM	Application exten...	335 KB
module.1640.207bda0.77dd0000.dll	9/8/2019 2:46 PM	Application exten...	603 KB
module.1640.207bda0.77e70000.dll	9/8/2019 2:46 PM	Application exten...	571 KB
module.1640.207bda0.77f10000.dll	9/8/2019 2:46 PM	Application exten...	279 KB
module.1640.207bda0.77f60000.dll	9/8/2019 2:46 PM	Application exten...	463 KB
module.1640.207bda0.77fe0000.dll	9/8/2019 2:46 PM	Application exten...	55 KB
module.1640.207bda0.773d0000.dll	9/8/2019 2:46 PM	Application exten...	1,030 KB
module.1640.207bda0.400000.dll	9/8/2019 2:46 PM	Application exten...	29 KB
module.1640.207bda0.78130000.dll	9/8/2019 2:46 PM	Application exten...	612 KB

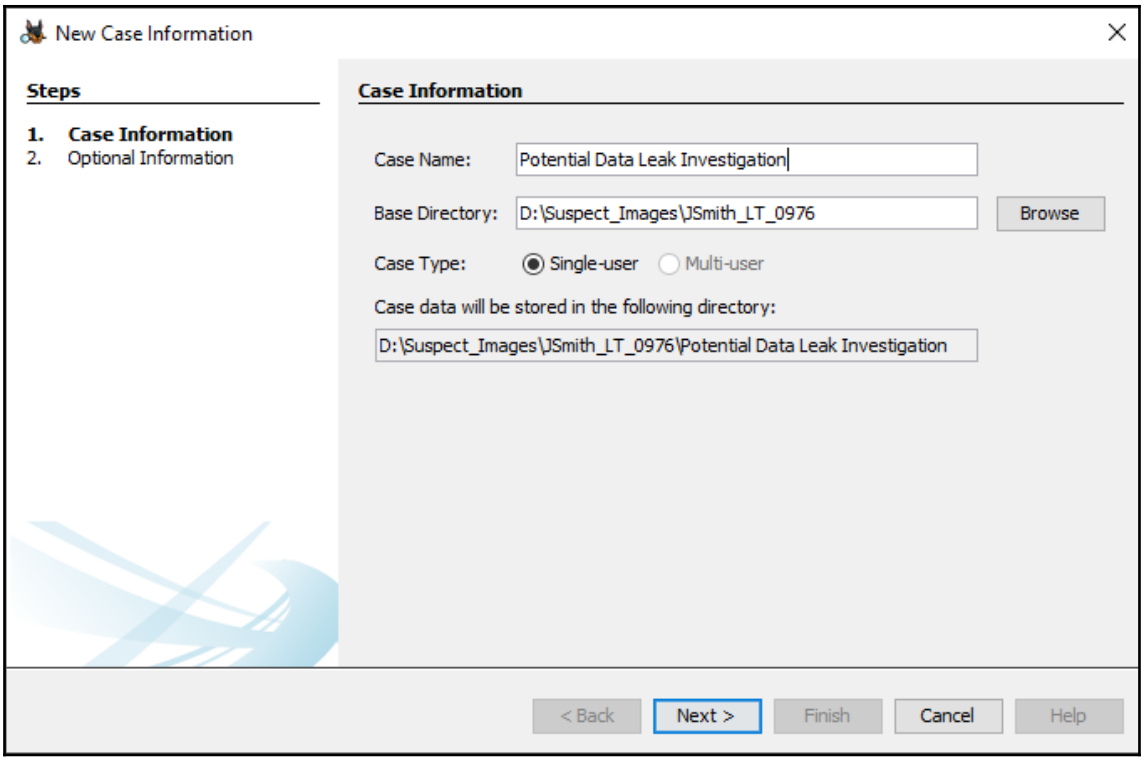
```
192.168.10.102
192.168.10.102
188.40.0.138
1.7.1.1
3.14.3.2
```

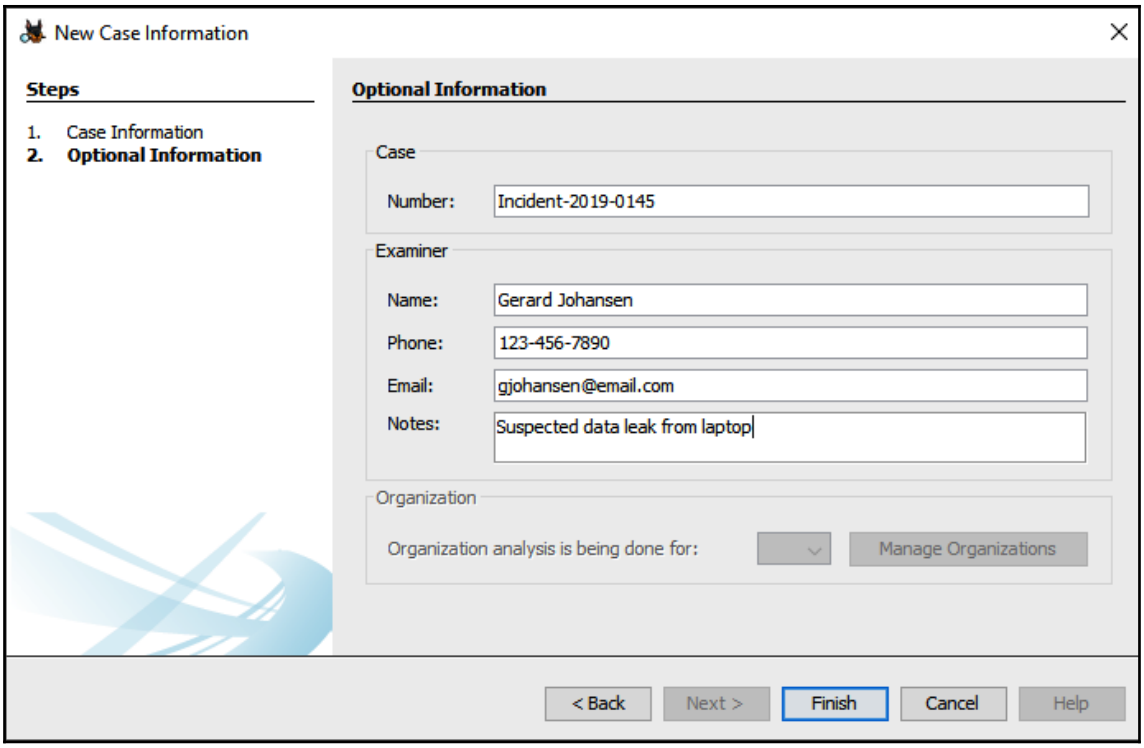
```
http://188.40.0.138:8080/zb/v_01_a/in/cp.php
http://188.40.0.138:8080/zb/v_01_a/in/cp.php
http://188.40.0.138:8080/zb/v_01_a/in/cp.php
```

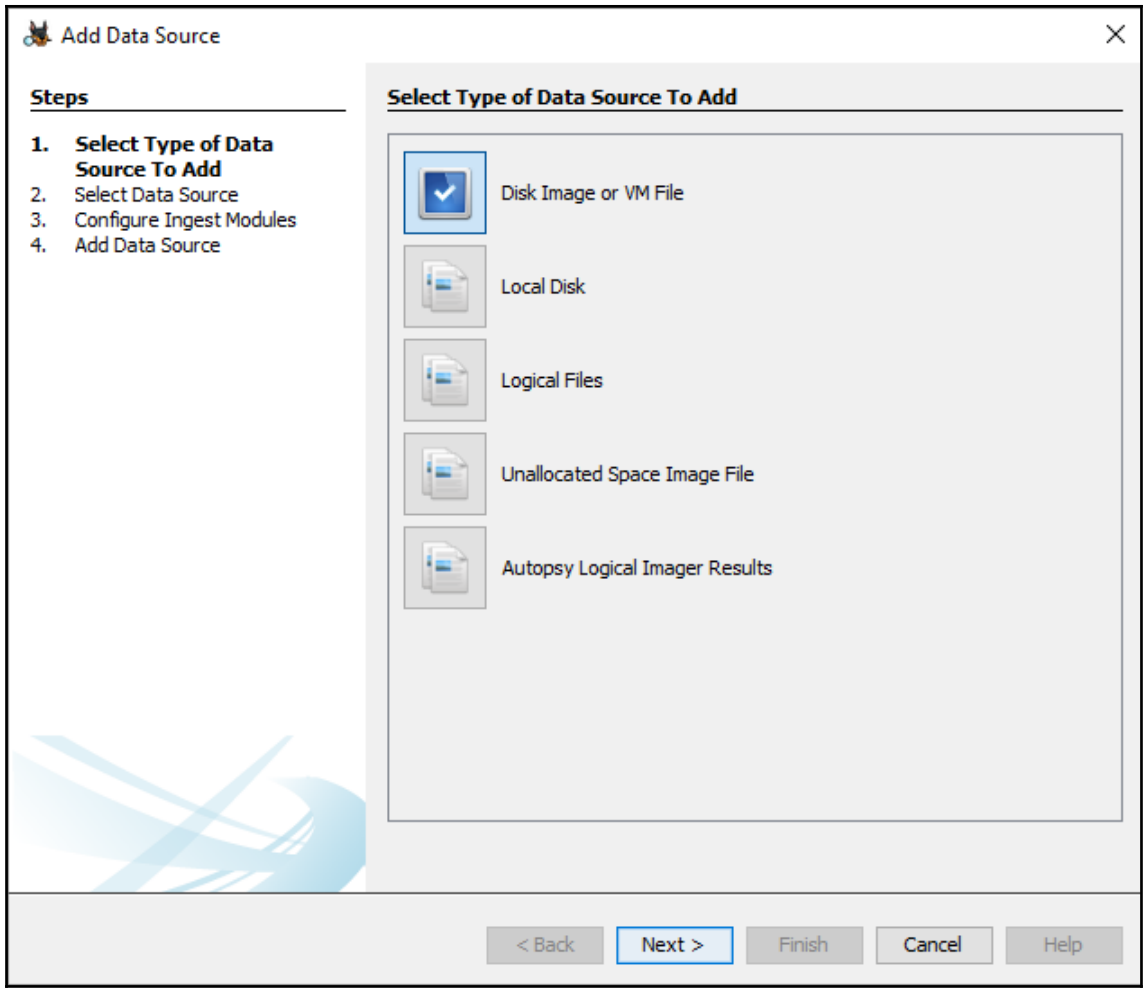
```
http://188.40.0.138:8080/zb/v_01_a/in/cp.php
<!-- BEGIN Global Navigation table --><table cellspacing="0" cellpaddin
://chaseonline.chase.com/images//ChaseNew.gif" alt="Chase Online Logo"
//www.chase.com/';" class="globalnavlinks">Chase.com</a>  </td>
<!--Footer--><table border="0" cellspacing="0" cellpadding="0" class="f
cal-align:top"> </td><td align="center" width="40%" valign="top"><span
/shared/assets/page/security_measures';" onBlur="window.status='';retur
Security</a> | <!-- mp_trans_remove_start --><a id="TermsLink" href="Ja
us='';return true" onMouseOver="window.status='';return true" onFocus="
dd<a id="TermsLink" href="JavaScript:document.location.href='https://ww
us='';return true" onFocus="window.status='';return true" onMouseOut="w
></table><div class="printable"><table border="0" cellspacing="0" cellp
```

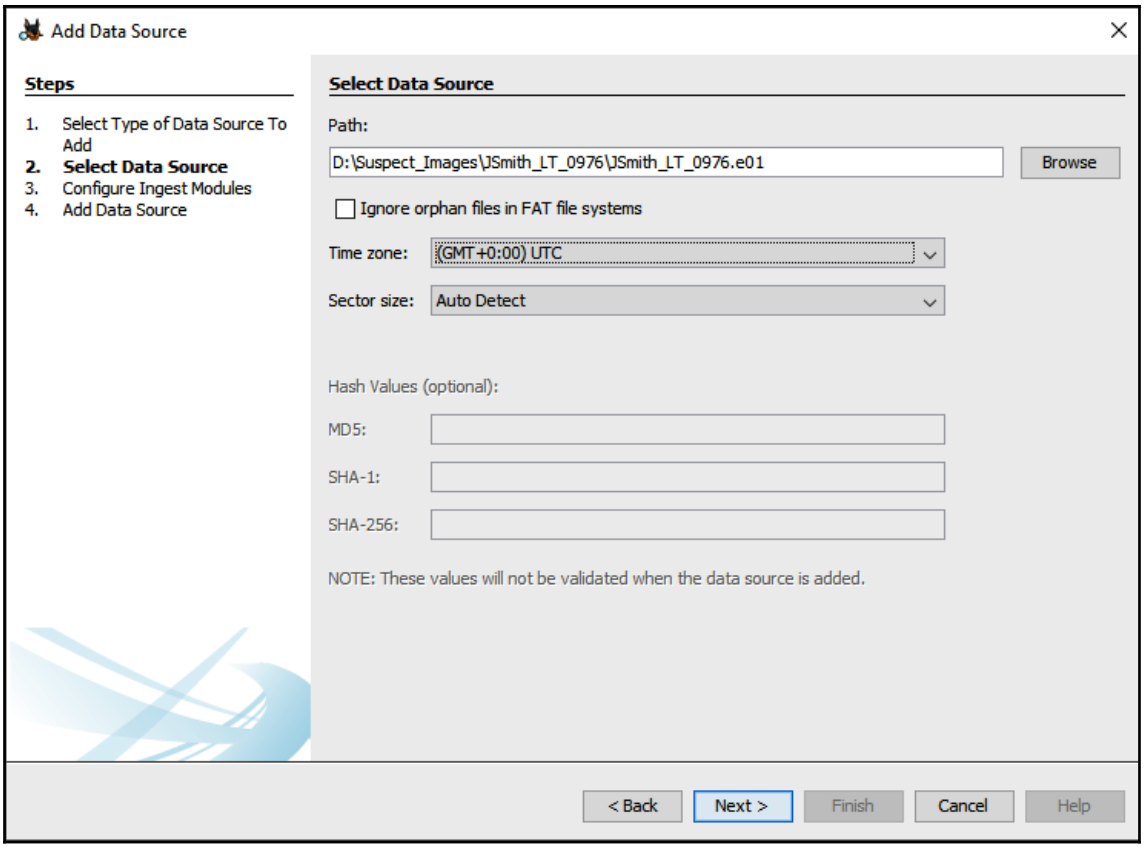
Chapter 9: Analyzing System Storage

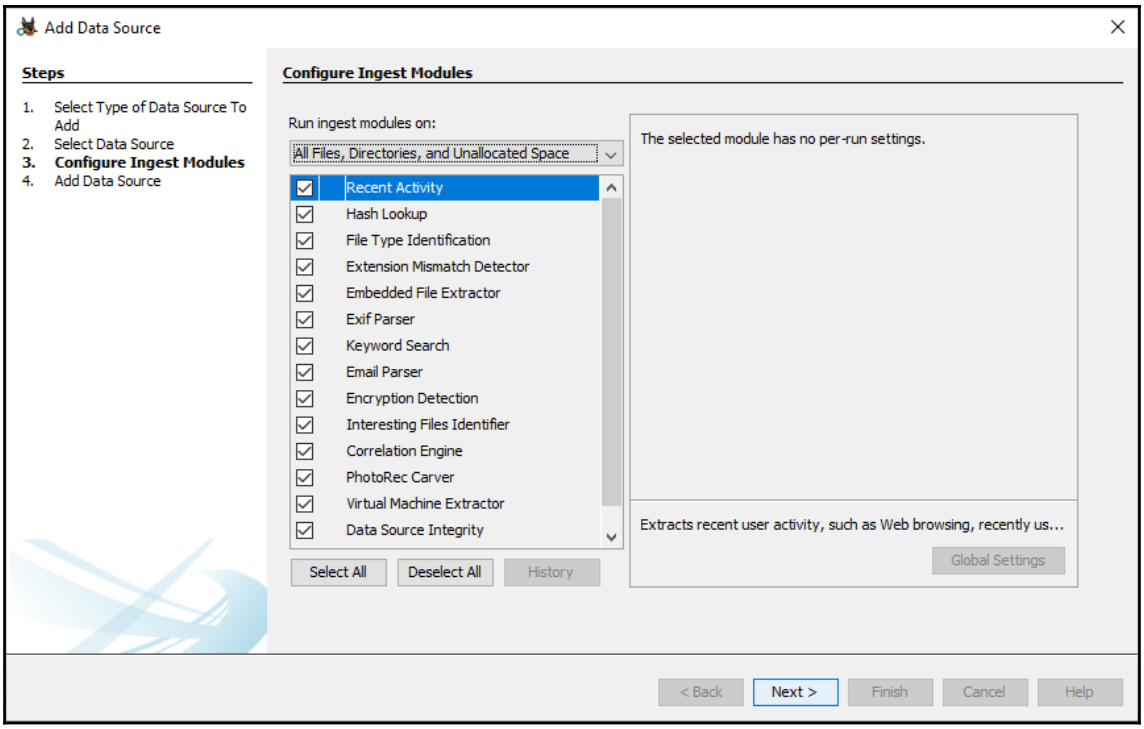
Name	Date modified	Type	Size
JSmith_LT_0976.e04	9/9/2019 3:26 PM	E04 File	1,350,414 KB
JSmith_LT_0976.e03	9/9/2019 3:11 PM	E03 File	2,097,138 KB
JSmith_LT_0976.e02	9/9/2019 2:35 PM	E02 File	2,097,123 KB
JSmith_LT_0976.e01	9/9/2019 2:10 PM	E01 File	2,097,133 KB

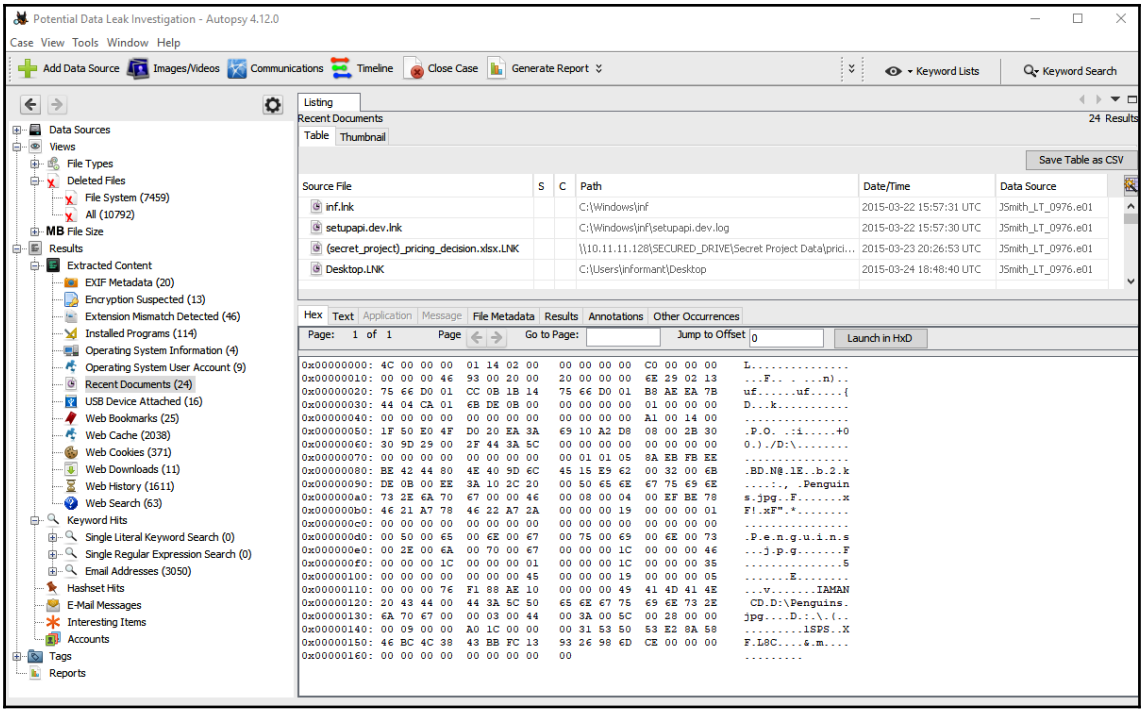

New Case Information
Steps
1. Case Information
2. Optional Information
Case Information
Case Name:
Potential Data Leak Investigation
Base Directory:
D:\Suspect_Images\JSmith_LT_0976
Browse
Case Type:
Single-user
Multi-user
Case data will be stored in the following directory:
D:\Suspect_Images\JSmith_LT_0976\Potential Data Leak Investigation
< Back
Next >
Finish
Cancel
Help

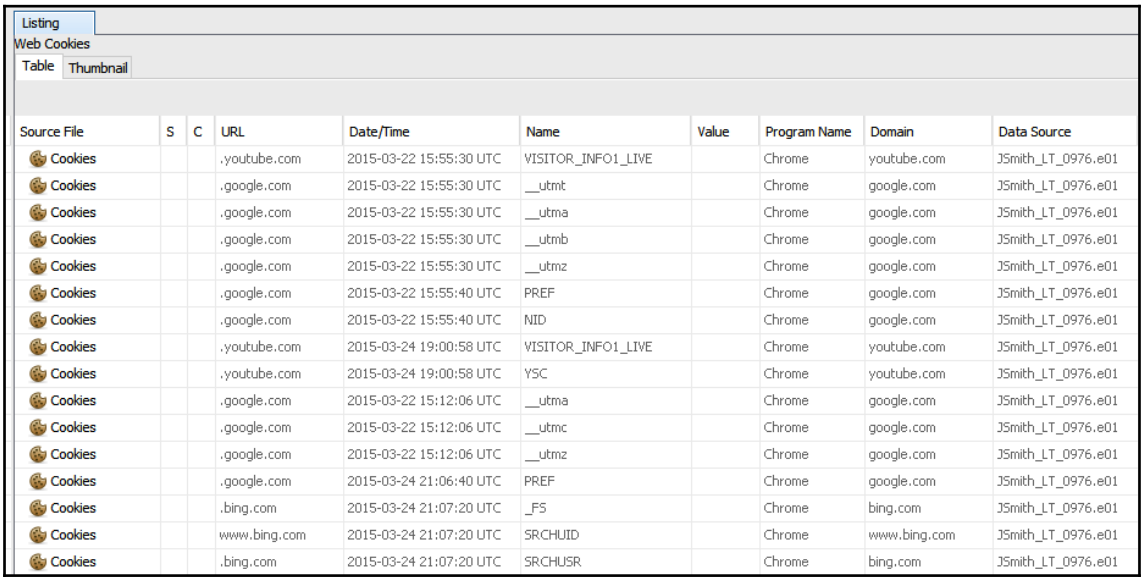

New Case Information
Steps
1. Case Information
2. Optional Information
Optional Information
Case
Number:
Incident-2019-0145
Examiner
Name:
Gerard Johansen
Phone:
123-456-7890
Email:
gjohansen@email.com
Notes:
Suspected data leak from laptop
Organization
Organization analysis is being done for:
Manage Organizations
< Back
Next >
Finish
Cancel
Help


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


Add Data Source
Steps
1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source
Select Data Source
Path:
D:\Suspect_Images\JSmith_LT_0976\JSmith_LT_0976.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

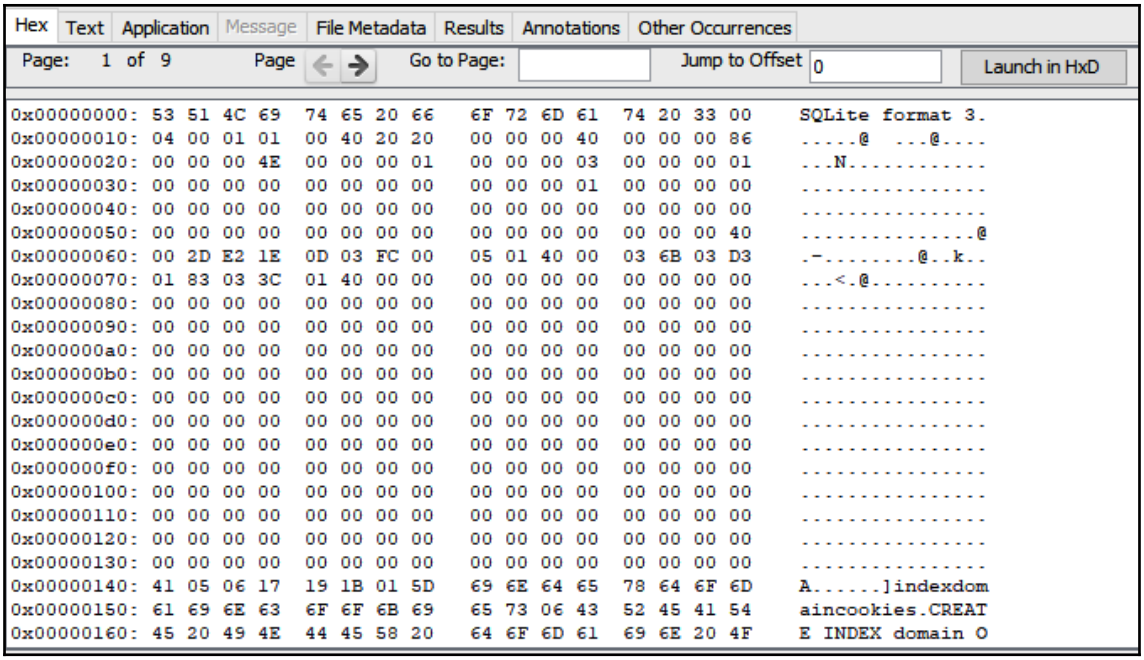

Add Data Source
Steps
1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source
Configure Ingest Modules
Run ingest modules on:
All Files, Directories, and Unallocated Space
Recent Activity
Hash Lookup
File Type Identification
Extension Mismatch Detector
Embedded File Extractor
Exif Parser
Keyword Search
Email Parser
Encryption Detection
Interesting Files Identifier
Correlation Engine
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

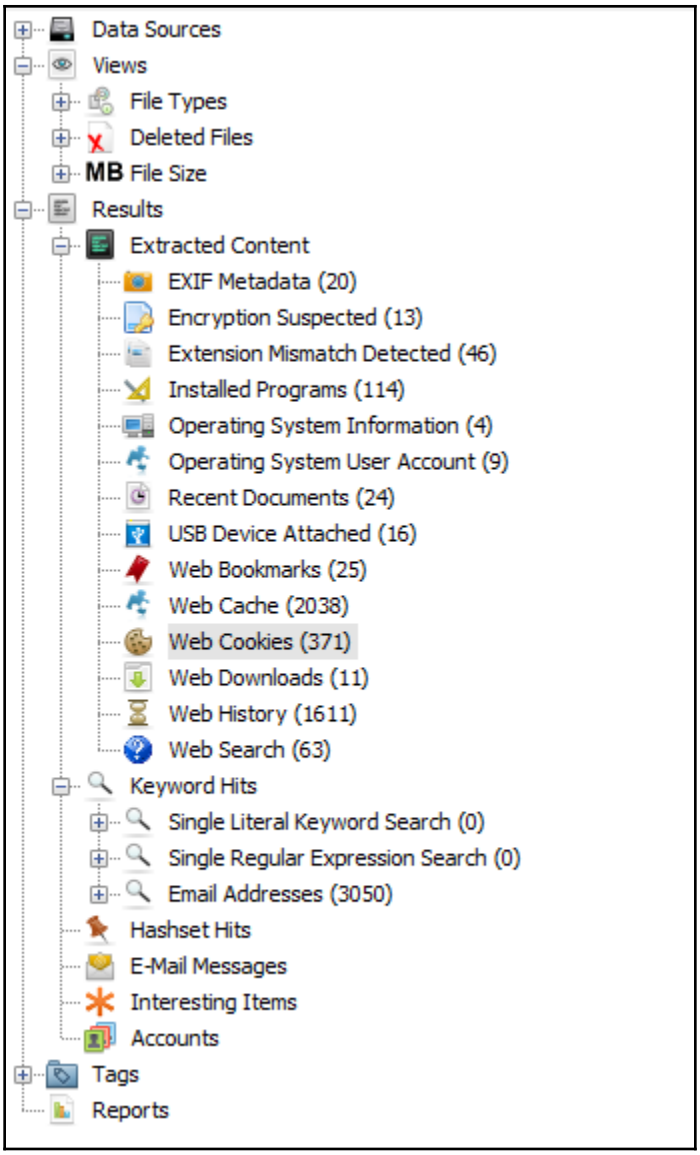

Potential Data Leak Investigation - Autopsy 4.12.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Timeline
Close Case
Generate Report
Keyword Lists
Keyword Search
Data Sources
Views
File Types
Deleted Files
File System (7459)
All (10792)
MB File Size
Results
Extracted Content
EXIF Metadata (20)
Encryption Suspected (13)
Extension Mismatch Detected (46)
Installed Programs (114)
Operating System Information (4)
Operating System User Account (9)
Recent Documents (24)
USB Device Attached (16)
Web Bookmarks (25)
Web Cache (2038)
Web Cookies (371)
Web Downloads (11)
Web History (1611)
Web Search (63)
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Email Addresses (3050)
Hashset Hits
E-Mail Messages
Interesting Items
Accounts
Tags
Reports
Listing
Recent Documents
24 Results
Table
Thumbnail
Save Table as CSV
Source File
S
C
Path
Date/Time
Data Source
inf.lnk
C:\Windows\inf
2015-03-22 15:57:31 UTC
JSmith_LT_0976.e01
setupapi.dev.lnk
C:\Windows\inf\setupapi.dev.log
2015-03-22 15:57:30 UTC
JSmith_LT_0976.e01
(secret_project)_pricing_decision.xlsx.LNK
\\10.11.11.128\SECURED_DRIVE\Secret Project Data\prici...
2015-03-23 20:26:53 UTC
JSmith_LT_0976.e01
Desktop.LNK
C:\Users\informant\Desktop
2015-03-24 18:48:40 UTC
JSmith_LT_0976.e01
Hex
Text
Application
Message
File Metadata
Results
Annotations
Other Occurrences
Page: 1 of 1
Page
Go to Page:
Jump to Offset 0
Launch in HxD

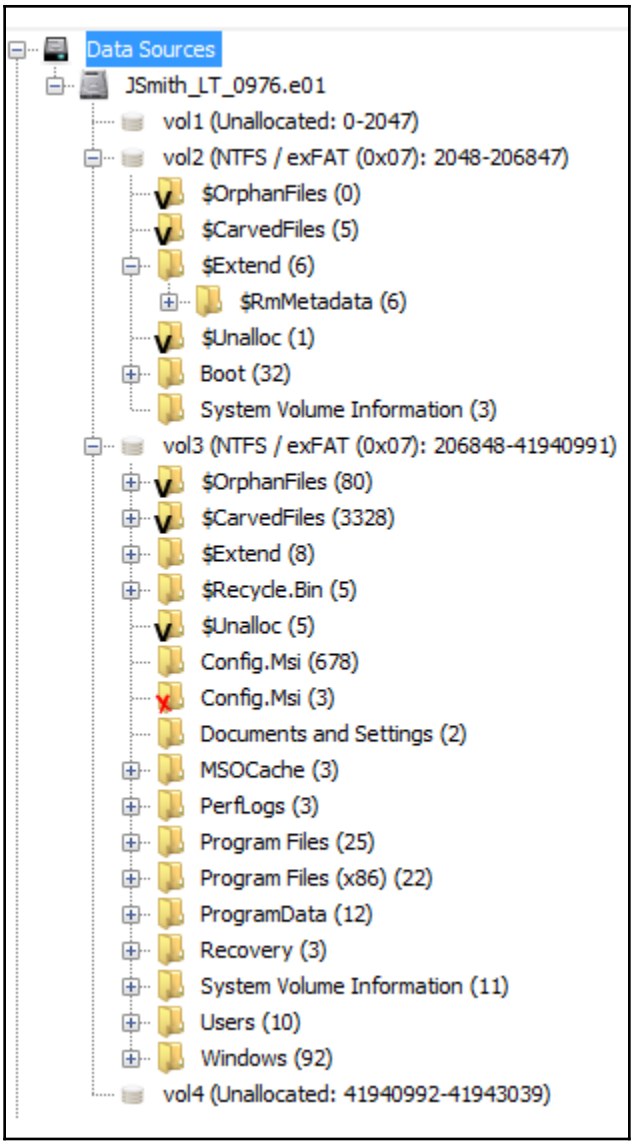

Listing
Web Cookies
Table
Thumbnail
Source File
S
C
URL
Date/Time
Name
Value
Program Name
Domain
Data Source
Cookies .youtube.com 2015-03-22 15:55:30 UTC VISITOR_INFO1_LIVE Chrome youtube.com JSmith_LT_0976.e01
Cookies .google.com 2015-03-22 15:55:30 UTC __utmt Chrome google.com JSmith_LT_0976.e01
Cookies .google.com 2015-03-22 15:55:30 UTC __utma Chrome google.com JSmith_LT_0976.e01
Cookies .google.com 2015-03-22 15:55:30 UTC __utmb Chrome google.com JSmith_LT_0976.e01
Cookies .google.com 2015-03-22 15:55:30 UTC __utmz Chrome google.com JSmith_LT_0976.e01
Cookies .google.com 2015-03-22 15:55:40 UTC PREF Chrome google.com JSmith_LT_0976.e01
Cookies .google.com 2015-03-22 15:55:40 UTC NID Chrome google.com JSmith_LT_0976.e01
Cookies .youtube.com 2015-03-24 19:00:58 UTC VISITOR_INFO1_LIVE Chrome youtube.com JSmith_LT_0976.e01
Cookies .youtube.com 2015-03-24 19:00:58 UTC YSC Chrome youtube.com JSmith_LT_0976.e01
Cookies .google.com 2015-03-22 15:12:06 UTC __utma Chrome google.com JSmith_LT_0976.e01
Cookies .google.com 2015-03-22 15:12:06 UTC __utmc Chrome google.com JSmith_LT_0976.e01
Cookies .google.com 2015-03-22 15:12:06 UTC __utmz Chrome google.com JSmith_LT_0976.e01
Cookies .google.com 2015-03-24 21:06:40 UTC PREF Chrome google.com JSmith_LT_0976.e01
Cookies .bing.com 2015-03-24 21:07:20 UTC _FS Chrome bing.com JSmith_LT_0976.e01
Cookies www.bing.com 2015-03-24 21:07:20 UTC SRCHUID Chrome www.bing.com JSmith_LT_0976.e01
Cookies .bing.com 2015-03-24 21:07:20 UTC SRCHUSR Chrome bing.com JSmith_LT_0976.e01

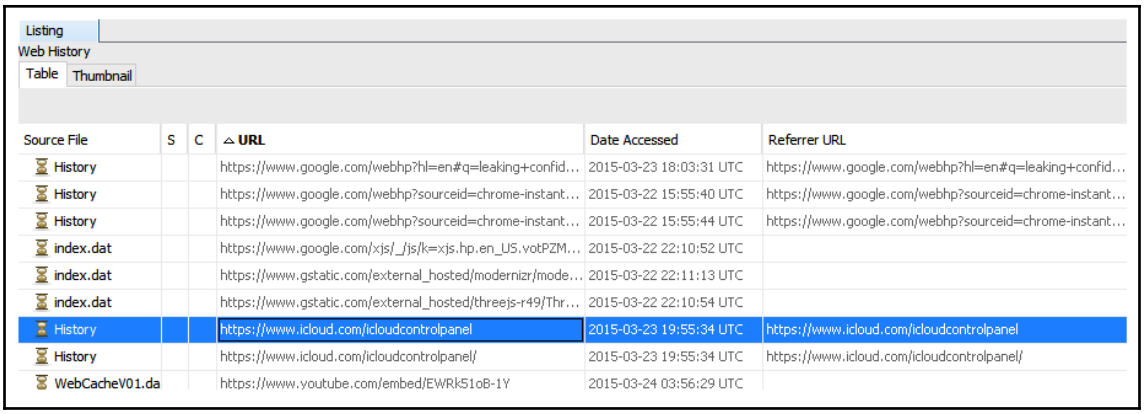
Type	Value
URL	.youtube.com
Date/Time	2015-03-24 19:00:58
Name	YSC
Value	
Program Name	Chrome
Domain	youtube.com
Source File Path	/img_JSmith_LT_0976.e01/vol_vol3/Users/informant/AppData/Local/Google/Chrome/User Data/Default/Cookies
Artifact ID	-9223372036854775654

Name	/img_JSmith_LT_0976.e01/vol_vol3/Users/informant/AppData/Local/Google/Chrome/User Data/Default/Cookies
Type	File System
MIME Type	application/x-sqlite3
Size	137216
File Name Allocation	Allocated
Metadata Allocation	Allocated
Modified	2015-03-24 21:07:21 UTC
Accessed	2015-03-22 15:11:57 UTC
Created	2015-03-22 15:11:57 UTC
Changed	2015-03-24 21:07:21 UTC
MD5	7a247be5ff943b90262c755dfdefeca7
Hash Lookup Results	UNKNOWN
Internal ID	9952


Hex
Text
Application
Message
File Metadata
Results
Annotations
Other Occurrences
Page: 1 of 9
Page
Go to Page:
Jump to Offset
0
Launch in HxD
0x00000000: 53 51 4C 69 74 65 20 66 6F 72 6D 61 74 20 33 00 SQLite format 3.
0x00000010: 04 00 01 01 00 40 20 20 00 00 00 40 00 00 00 86 .....@ ...@....
0x00000020: 00 00 00 4E 00 00 00 01 00 00 00 03 00 00 00 01 ...N............
0x00000030: 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 ....
0x00000040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x00000050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 ....@
0x00000060: 00 2D E2 1E 0D 03 FC 00 05 01 40 00 03 6B 03 D3 .-........@..k..
0x00000070: 01 83 03 3C 01 40 00 00 00 00 00 00 00 00 00 00 ...<.@..........
0x00000080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x00000090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x000000a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x000000b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x000000c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x000000d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x000000e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x000000f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x00000100: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x00000110: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x00000120: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x00000130: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x00000140: 41 05 06 17 19 1B 01 5D 69 6E 64 65 78 64 6F 6D A.....]indexdom
0x00000150: 61 69 6E 63 6F 6F 6B 69 65 73 06 43 52 45 41 54 aincookies.CREAT
0x00000160: 45 20 49 4E 44 45 58 20 64 6F 6D 61 69 6E 20 4F E INDEX domain O

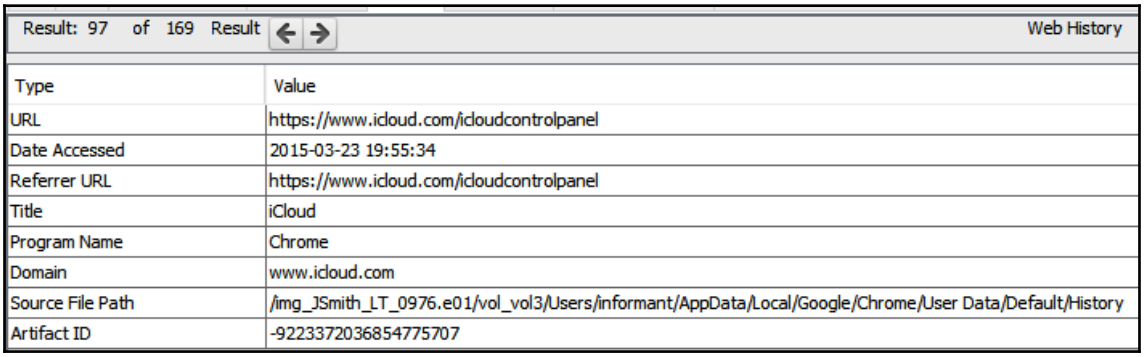

Data Sources
Views
File Types
Deleted Files
MB File Size
Results
Extracted Content
EXIF Metadata (20)
Encryption Suspected (13)
Extension Mismatch Detected (46)
Installed Programs (114)
Operating System Information (4)
Operating System User Account (9)
Recent Documents (24)
USB Device Attached (16)
Web Bookmarks (25)
Web Cache (2038)
Web Cookies (371)
Web Downloads (11)
Web History (1611)
Web Search (63)
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Email Addresses (3050)
Hashset Hits
E-Mail Messages
Interesting Items
Accounts
Tags
Reports


Data Sources
JSmith_LT_0976.e01
vol1 (Unallocated: 0-2047)
vol2 (NTFS / exFAT (0x07): 2048-206847)
$OrphanFiles (0)
$CarvedFiles (5)
$Extend (6)
$RmMetadata (6)
$Unalloc (1)
Boot (32)
System Volume Information (3)
vol3 (NTFS / exFAT (0x07): 206848-41940991)
$OrphanFiles (80)
$CarvedFiles (3328)
$Extend (8)
$Recycle.Bin (5)
$Unalloc (5)
Config.Msi (678)
Config.Msi (3)
Documents and Settings (2)
MSOCache (3)
PerfLogs (3)
Program Files (25)
Program Files (x86) (22)
ProgramData (12)
Recovery (3)
System Volume Information (11)
Users (10)
Windows (92)
vol4 (Unallocated: 41940992-41943039)



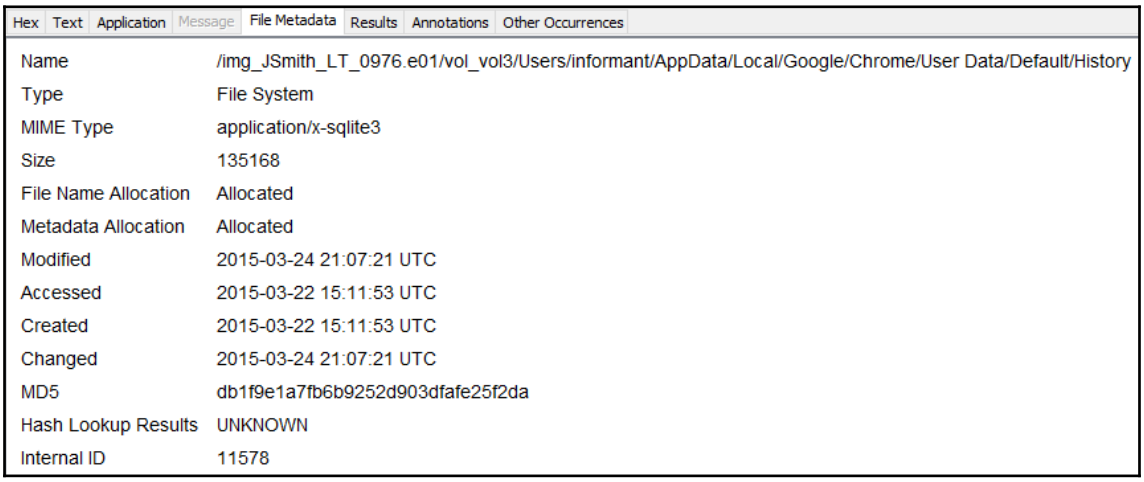
Listing
Web History
Table | Thumbnail

Source File	S	C	URL	Date Accessed	Referrer URL
History			https://www.google.com/webhp?hl=en#q=leaking+confid...	2015-03-23 18:03:31 UTC	https://www.google.com/webhp?hl=en#q=leaking+confid...
History			https://www.google.com/webhp?sourceid=chrome-instant...	2015-03-22 15:55:40 UTC	https://www.google.com/webhp?sourceid=chrome-instant...
History			https://www.google.com/webhp?sourceid=chrome-instant...	2015-03-22 15:55:44 UTC	https://www.google.com/webhp?sourceid=chrome-instant...
index.dat			https://www.google.com/xjs/_/js/k=xjs.hp.en_US.votPZM...	2015-03-22 22:10:52 UTC	
index.dat			https://www.gstatic.com/external_hosted/modernizr/mode...	2015-03-22 22:11:13 UTC	
index.dat			https://www.gstatic.com/external_hosted/threejs-r49/Thr...	2015-03-22 22:10:54 UTC	
History			https://www.icloud.com/icloudcontrolpanel	2015-03-23 19:55:34 UTC	https://www.icloud.com/icloudcontrolpanel
History			https://www.icloud.com/icloudcontrolpanel/	2015-03-23 19:55:34 UTC	https://www.icloud.com/icloudcontrolpanel/
WebCacheV01.da			https://www.youtube.com/embed/EWRk51oB-1Y	2015-03-24 03:56:29 UTC	



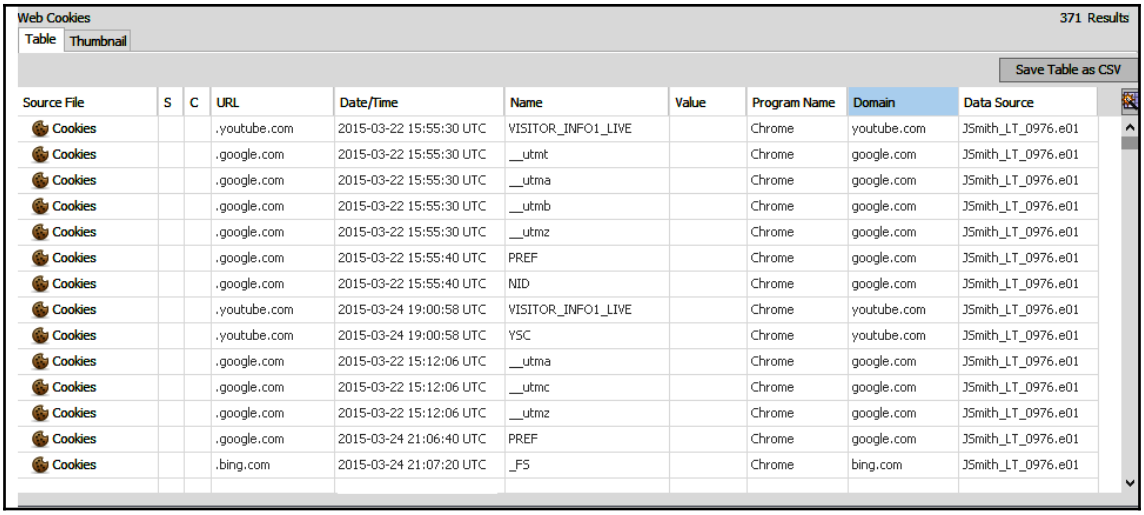
Result: 97 of 169 Result
Web History

Type	Value
URL	https://www.icloud.com/icloudcontrolpanel
Date Accessed	2015-03-23 19:55:34
Referrer URL	https://www.icloud.com/icloudcontrolpanel
Title	iCloud
Program Name	Chrome
Domain	www.icloud.com
Source File Path	/img_JSmith_LT_0976.e01/vol_vol3/Users/informant/AppData/Local/Google/Chrome/User Data/Default/History
Artifact ID	-9223372036854775707



Hex | Text | Application | Message | File Metadata | Results | Annotations | Other Occurrences

Name	/img_JSmith_LT_0976.e01/vol_vol3/Users/informant/AppData/Local/Google/Chrome/User Data/Default/History
Type	File System
MIME Type	application/x-sqlite3
Size	135168
File Name Allocation	Allocated
Metadata Allocation	Allocated
Modified	2015-03-24 21:07:21 UTC
Accessed	2015-03-22 15:11:53 UTC
Created	2015-03-22 15:11:53 UTC
Changed	2015-03-24 21:07:21 UTC
MD5	db1f9e1a7fb6b9252d903dfafe25f2da
Hash Lookup Results	UNKNOWN
Internal ID	11578



Web Cookies 371 Results

Table | Thumbnail

Save Table as CSV

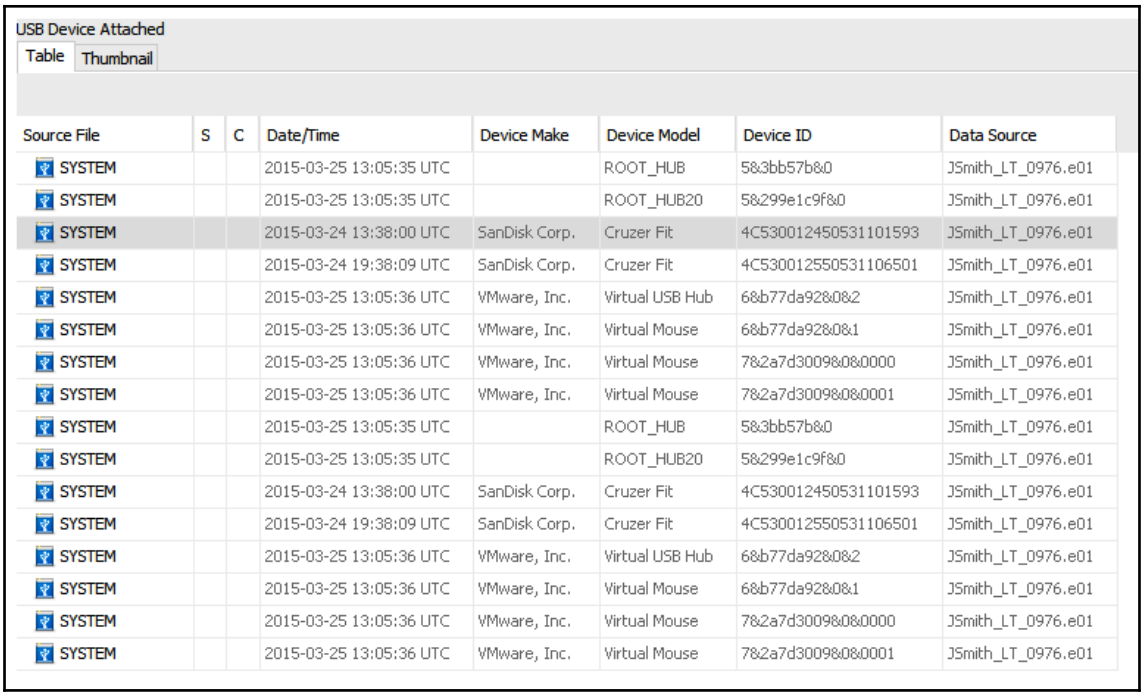
Source File	S	C	URL	Date/Time	Name	Value	Program Name	Domain	Data Source
Cookies			.youtube.com	2015-03-22 15:55:30 UTC	VISITOR_INFO1_LIVE		Chrome	youtube.com	JSmith_LT_0976.e01
Cookies			.google.com	2015-03-22 15:55:30 UTC	__utmt		Chrome	google.com	JSmith_LT_0976.e01
Cookies			.google.com	2015-03-22 15:55:30 UTC	__utma		Chrome	google.com	JSmith_LT_0976.e01
Cookies			.google.com	2015-03-22 15:55:30 UTC	__utmb		Chrome	google.com	JSmith_LT_0976.e01
Cookies			.google.com	2015-03-22 15:55:30 UTC	__utmz		Chrome	google.com	JSmith_LT_0976.e01
Cookies			.google.com	2015-03-22 15:55:40 UTC	PREF		Chrome	google.com	JSmith_LT_0976.e01
Cookies			.google.com	2015-03-22 15:55:40 UTC	NID		Chrome	google.com	JSmith_LT_0976.e01
Cookies			.youtube.com	2015-03-24 19:00:58 UTC	VISITOR_INFO1_LIVE		Chrome	youtube.com	JSmith_LT_0976.e01
Cookies			.youtube.com	2015-03-24 19:00:58 UTC	YSC		Chrome	youtube.com	JSmith_LT_0976.e01
Cookies			.google.com	2015-03-22 15:12:06 UTC	__utma		Chrome	google.com	JSmith_LT_0976.e01
Cookies			.google.com	2015-03-22 15:12:06 UTC	__utmc		Chrome	google.com	JSmith_LT_0976.e01
Cookies			.google.com	2015-03-22 15:12:06 UTC	__utmz		Chrome	google.com	JSmith_LT_0976.e01
Cookies			.google.com	2015-03-24 21:06:40 UTC	PREF		Chrome	google.com	JSmith_LT_0976.e01
Cookies			.bing.com	2015-03-24 21:07:20 UTC	_FS		Chrome	bing.com	JSmith_LT_0976.e01

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

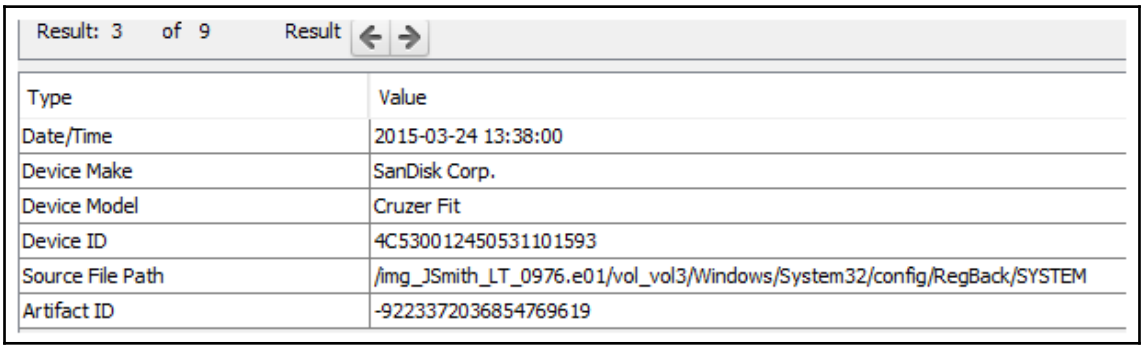
List Name	Files with Hits
cfoster@nist.gov (1)	1
cglein@microsoft.com (1)	1
chambersignroot@chambersign.org (8)	8
chambersroot@chambersign.org (8)	8
charles.camp@nist.gov (1)	1
chhan@microsoft.com (1)	1
chipc@microsoft.com (1)	1
chirag.parikh@nist.gov (1)	1
chrichristian.enloe@nist.gov (1)	1
chris.glein@gmail.com (1)	1
christian.enloe@nist.gov (1)	1
christopher.bertrand@nist.gov (1)	1
christopher.mckinney@nist.gov (1)	1
christopher.soles@nist.gov (1)	1
chrome@example.com (2)	2



USB Device Attached

Table | Thumbnail

Source File	S	C	Date/Time	Device Make	Device Model	Device ID	Data Source
SYSTEM			2015-03-25 13:05:35 UTC		ROOT_HUB	5&3bb57b8&0	JSmith_LT_0976.e01
SYSTEM			2015-03-25 13:05:35 UTC		ROOT_HUB20	5&299e1c9f8&0	JSmith_LT_0976.e01
SYSTEM			2015-03-24 13:38:00 UTC	SanDisk Corp.	Cruzer Fit	4C530012450531101593	JSmith_LT_0976.e01
SYSTEM			2015-03-24 19:38:09 UTC	SanDisk Corp.	Cruzer Fit	4C530012550531106501	JSmith_LT_0976.e01
SYSTEM			2015-03-25 13:05:36 UTC	VMware, Inc.	Virtual USB Hub	68&b77da92&0&2	JSmith_LT_0976.e01
SYSTEM			2015-03-25 13:05:36 UTC	VMware, Inc.	Virtual Mouse	68&b77da92&0&1	JSmith_LT_0976.e01
SYSTEM			2015-03-25 13:05:36 UTC	VMware, Inc.	Virtual Mouse	7&2a7d3009&0&0000	JSmith_LT_0976.e01
SYSTEM			2015-03-25 13:05:36 UTC	VMware, Inc.	Virtual Mouse	7&2a7d3009&0&0001	JSmith_LT_0976.e01
SYSTEM			2015-03-25 13:05:35 UTC		ROOT_HUB	5&3bb57b8&0	JSmith_LT_0976.e01
SYSTEM			2015-03-25 13:05:35 UTC		ROOT_HUB20	5&299e1c9f8&0	JSmith_LT_0976.e01
SYSTEM			2015-03-24 13:38:00 UTC	SanDisk Corp.	Cruzer Fit	4C530012450531101593	JSmith_LT_0976.e01
SYSTEM			2015-03-24 19:38:09 UTC	SanDisk Corp.	Cruzer Fit	4C530012550531106501	JSmith_LT_0976.e01
SYSTEM			2015-03-25 13:05:36 UTC	VMware, Inc.	Virtual USB Hub	68&b77da92&0&2	JSmith_LT_0976.e01
SYSTEM			2015-03-25 13:05:36 UTC	VMware, Inc.	Virtual Mouse	68&b77da92&0&1	JSmith_LT_0976.e01
SYSTEM			2015-03-25 13:05:36 UTC	VMware, Inc.	Virtual Mouse	7&2a7d3009&0&0000	JSmith_LT_0976.e01
SYSTEM			2015-03-25 13:05:36 UTC	VMware, Inc.	Virtual Mouse	7&2a7d3009&0&0001	JSmith_LT_0976.e01



Result: 3 of 9 Result

Type	Value
Date/Time	2015-03-24 13:38:00
Device Make	SanDisk Corp.
Device Model	Cruzer Fit
Device ID	4C530012450531101593
Source File Path	/img_JSmith_LT_0976.e01/vol_vol3/Windows/System32/config/RegBack/SYSTEM
Artifact ID	-9223372036854769619

Hex | Text | Application | Message | File Metadata | Results | Annotations | Other Occurrences

Name	/img_JSmith_LT_0976.e01/vol_vol3/Windows/System32/config/RegBack/SYSTEM
Type	File System
MIME Type	application/x.windows-registry
Size	12419072
File Name Allocation	Allocated
Metadata Allocation	Allocated
Modified	2015-03-25 13:24:16 UTC
Accessed	2015-03-25 13:24:10 UTC
Created	2015-03-25 10:15:18 UTC
Changed	2015-03-25 13:24:16 UTC
MD5	a26cbec95c053ca113b9bef2fdfd4878
Hash Lookup Results	UNKNOWN
Internal ID	76202

Name	S	C	Location	Modified Time	Change Time	Access Time
System.Data.Entity.dll			/img_JSmith_LT_0976.e01/vol_vol3/Program Files (x86)/Re...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
nb.lproj			/img_JSmith_LT_0976.e01/vol_vol3/Program Files (x86)/Ap...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
ko.lproj			/img_JSmith_LT_0976.e01/vol_vol3/Program Files (x86)/Bo...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
it.lproj			/img_JSmith_LT_0976.e01/vol_vol3/Program Files (x86)/Co...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
es.lproj			/img_JSmith_LT_0976.e01/vol_vol3/Program Files (x86)/Co...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
ru.lproj			/img_JSmith_LT_0976.e01/vol_vol3/Program Files (x86)/Co...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
ColorSync.resources			/img_JSmith_LT_0976.e01/vol_vol3/Program Files (x86)/Co...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
libdispatch.dll			/img_JSmith_LT_0976.e01/vol_vol3/Program Files (x86)/Co...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
es.lproj			/img_JSmith_LT_0976.e01/vol_vol3/Program Files (x86)/Co...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
pthreadVC2.dll			/img_JSmith_LT_0976.e01/vol_vol3/Program Files (x86)/Co...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
fi.lproj			/img_JSmith_LT_0976.e01/vol_vol3/Program Files (x86)/Co...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
AuditResultView.js			/img_JSmith_LT_0976.e01/vol_vol3/Program Files (x86)/Co...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
buildSystemOnly.js			/img_JSmith_LT_0976.e01/vol_vol3/Program Files (x86)/Co...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
ConsoleView.js			/img_JSmith_LT_0976.e01/vol_vol3/Program Files (x86)/Co...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
DOMAgent.js			/img_JSmith_LT_0976.e01/vol_vol3/Program Files (x86)/Co...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
ElementsPanelDescriptor.js			/img_JSmith_LT_0976.e01/vol_vol3/Program Files (x86)/Co...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00

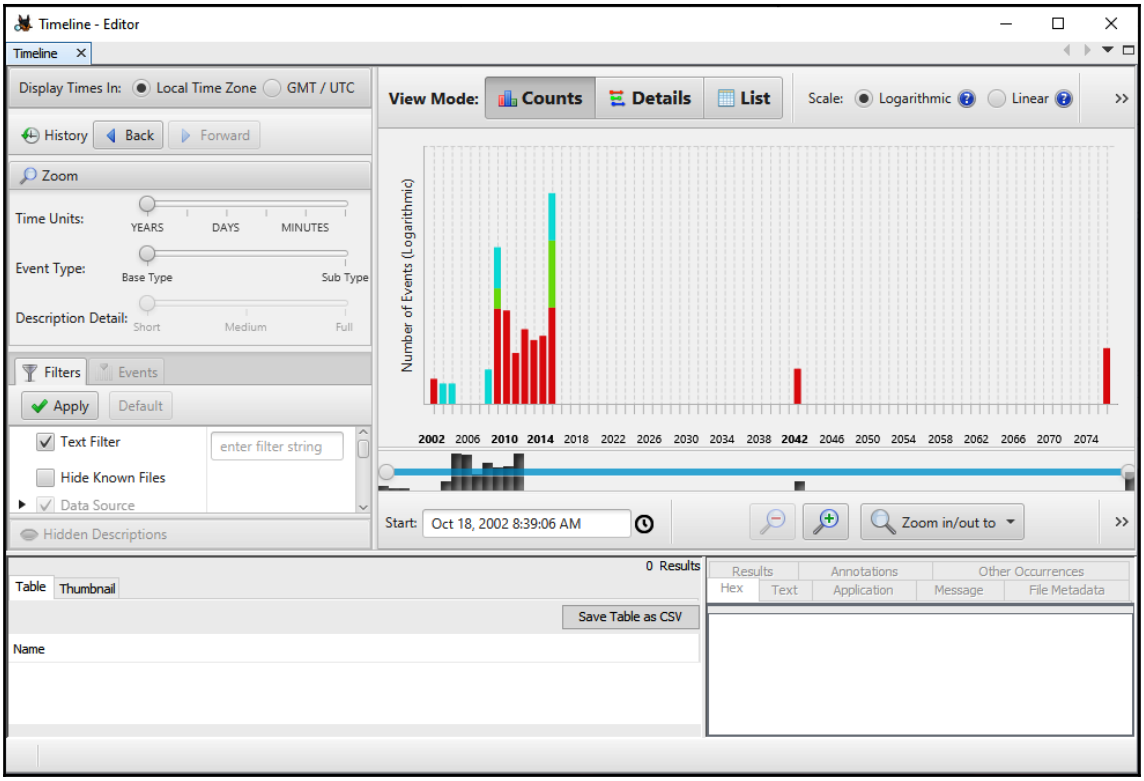
{9b365807-d2ef-11e4-b734-000c29ff2429}{3808876b-c176-4e48	/img_JSmith_LT_0976.e01/vol_vol3/System Volume Inform...	dvisory.zip(H «pricing decision«PRICIN~1FILE0|RCRD(
$MFT	/img_JSmith_LT_0976.e01/vol_vol3/$MFT	desktop.ini$I30«pricing decision«PRICIN~1progress
pricing decision.lnk	/img_JSmith_LT_0976.e01/vol_vol3/Users/Informant/AppD...	ret Project Data\«pricing decision«1SPS010.11.11.128

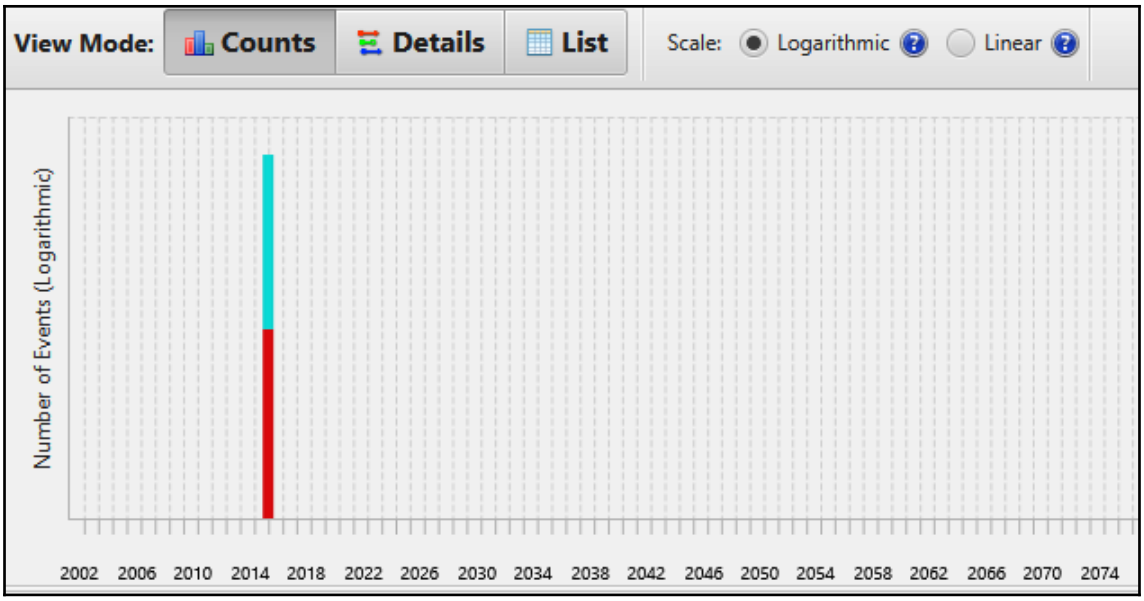
(secret_project)_pricing_decision.xlsx.lnk	/img_JSmith_LT_0976.e01/vol_vol3/Users/informant/AppD...
$UsnJrnl:$J	/img_JSmith_LT_0976.e01/vol_vol3/$Extend/$UsnJrnl:$J
(secret_project)_pricing_decision.xlsx.LNK	/img_JSmith_LT_0976.e01/vol_vol3/Users/informant/AppD...

```
(secret_project)_pricing_decision.xlsx.lnk \\10.11.11.128\SECURED_DRIVESecret Project Data\pricing decision\
icing decision
1SPS0
10.11.11.128
1SPS:
1SPSsC
\\10.11.11.128\secured_driveMicrosoft NetworkCompany's Secured Network Drive
SECRET~1
Secret Project Data
PRICIN~1
pricing decision
 (S2BBE~1.XLS
(secret_project)_pricing_decision.xlsx
\\10.11.11.128\secured_drive\Secret Project Data\pricing decision\(secret_project)_pricing_decision.xlsx
\\10.11.11.128\secured_drive\Secret Project Data\pricing decision\(secret_project)_pricing_decision.xlsx
1SPS
```

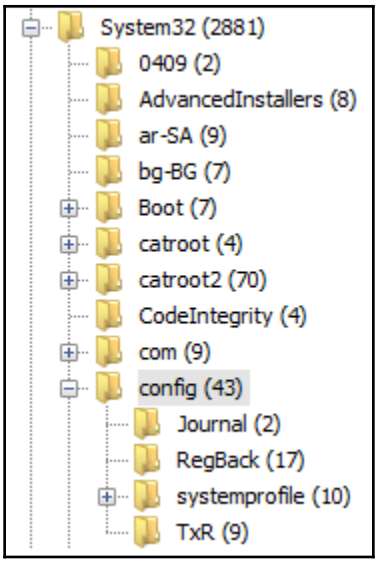
Name	/img_JSmith_LT_0976.e01/vol_vol3/Users/informant/AppData/Roaming/Microsoft/Windows/Recent/(secret_project)_pricing_decision.xlsx.lnk
Type	File System
MIME Type	application/octet-stream
Size	1952
File Name Allocation	Allocated
Metadata Allocation	Allocated
Modified	2015-03-23 20:26:53 UTC
Accessed	2015-03-23 20:26:53 UTC
Created	2015-03-23 20:26:53 UTC
Changed	2015-03-23 20:26:53 UTC
MD5	a9a4d030a0e6124ef8610617ee9125fc

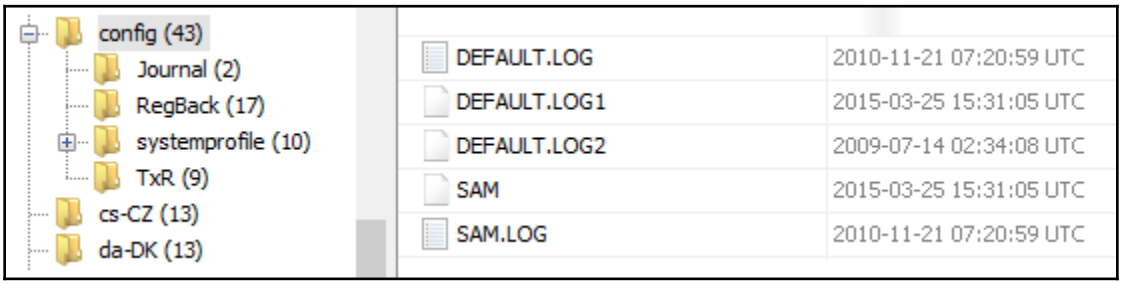
Type	Value
Username	informant
User ID	S-1-5-21-2425377081-3129163575-2985601102-1000

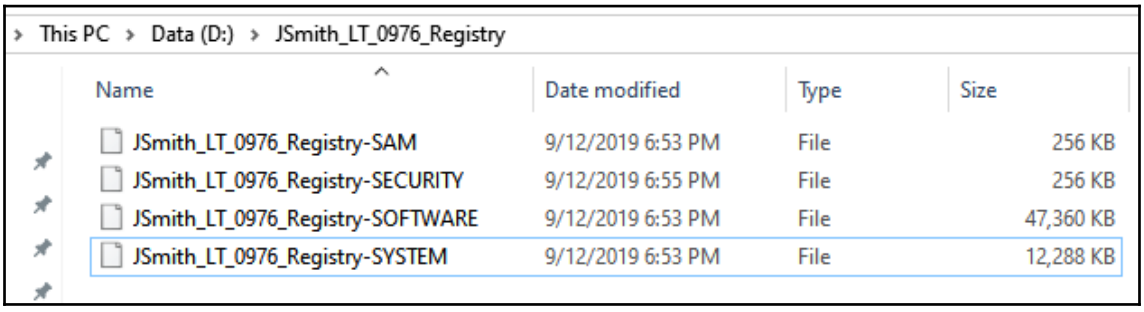

Timeline - Editor
Timeline
Display Times In:
Local Time Zone
GMT / UTC
History
Back
Forward
Zoom
Time Units:
YEARS
DAYS
MINUTES
Event Type:
Base Type
Sub Type
Description Detail:
Short
Medium
Full
Filters
Events
Apply
Default
Text Filter
enter filter string
Hide Known Files
Data Source
Hidden Descriptions
View Mode:
Counts
Details
List
Scale:
Logarithmic
Linear
Number of Events (Logarithmic)
2002 2006 2010 2014 2018 2022 2026 2030 2034 2038 2042 2046 2050 2054 2058 2062 2066 2070 2074
Start:
Oct 18, 2002 8:39:06 AM
Zoom in/out to
0 Results
Table
Thumbnail
Save Table as CSV
Name
Results
Annotations
Other Occurrences
Hex
Text
Application
Message
File Metadata

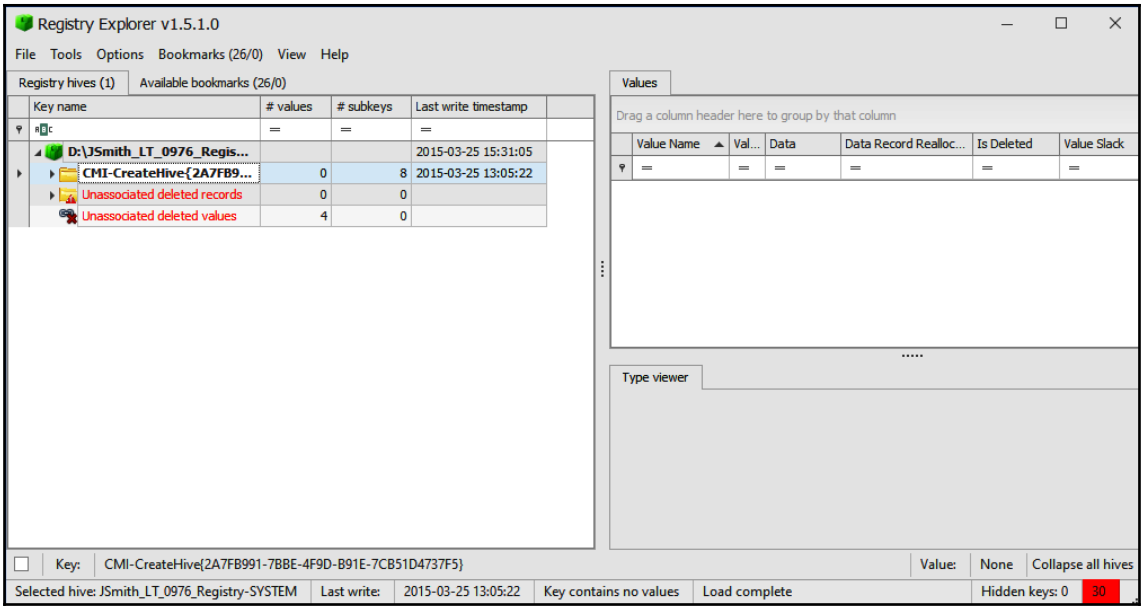


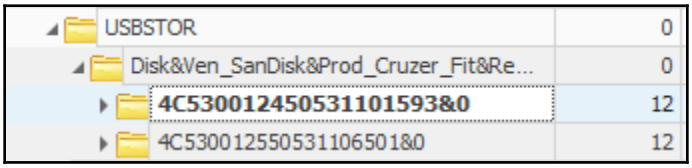
2010-11-21|07:06:15.881506|TZ|...B|FILE|NTFS	$MFT\|$FN	[...B]	time|user|host|/Windows/winsxs/amd64_microsoft-windows-alg.resources_31bf3856ad364e35_6.1.
2009-07-14|03:20:30.316587|TZ|...B|FILE|NTFS	$MFT\|$FN	[...B]	time|user|host|/Windows/winsxs/amd64_microsoft-windows-alg_31bf3856ad364e35_6.1.7600.1638
2010-11-21|07:06:26.337038|TZ|...B|FILE|NTFS	$MFT\|$FN	[...B]	time|user|host|/Windows/winsxs/amd64_microsoft-windows-alttab.resources_31bf3856ad364e35_
2009-07-14|05:30:18.216305|TZ|...B|FILE|NTFS	$MFT\|$FN	[...B]	time|user|host|/Windows/winsxs/amd64_microsoft-windows-alttab_31bf3856ad364e35_6.1.7600.16
2015-03-23|20:26:53.986593|TZ|...B|FILE|NTFS	$MFT\|$FN	[...B]	time|user|host|/Users/informant/AppData/Roaming/Microsoft/Windows/Recent/(secret_project)_
2015-03-23|20:26:54.002193|TZ|...B|FILE|NTFS	$MFT\|$FN	[...B]	time|user|host|/Users/informant/AppData/Roaming/Microsoft/Windows/Recent/pricing decision.ln
2009-07-14|05:30:10.993492|TZ|...B|FILE|NTFS	$MFT\|$FN	[...B]	time|user|host|/Windows/winsxs/amd64_microsoft-windows-appcompat-adm_31bf3856ad364e35_
2010-11-21|07:06:19.819912|TZ|...B|FILE|NTFS	$MFT\|$FN	[...B]	time|user|host|/Windows/winsxs/amd64_microsoft-windows-appid.resources_31bf3856ad364e35_
2010-11-21|03:17:30.539425|TZ|...B|FILE|NTFS	$MFT\|$FN	[...B]	time|user|host|/Windows/winsxs/amd64_microsoft-windows-appid_31bf3856ad364e35_6.1.7601.17
2010-11-21|07:06:15.881506|TZ|...B|FILE|NTFS	$MFT\|$FN	[...B]	time|user|host|/Windows/winsxs/amd64_microsoft-windows-appwiz.resources_31bf3856ad364e35_


System32 (2881)
0409 (2)
AdvancedInstallers (8)
ar-SA (9)
bg-BG (7)
Boot (7)
catroot (4)
catroot2 (70)
CodeIntegrity (4)
com (9)
config (43)
Journal (2)
RegBack (17)
systemprofile (10)
TxR (9)

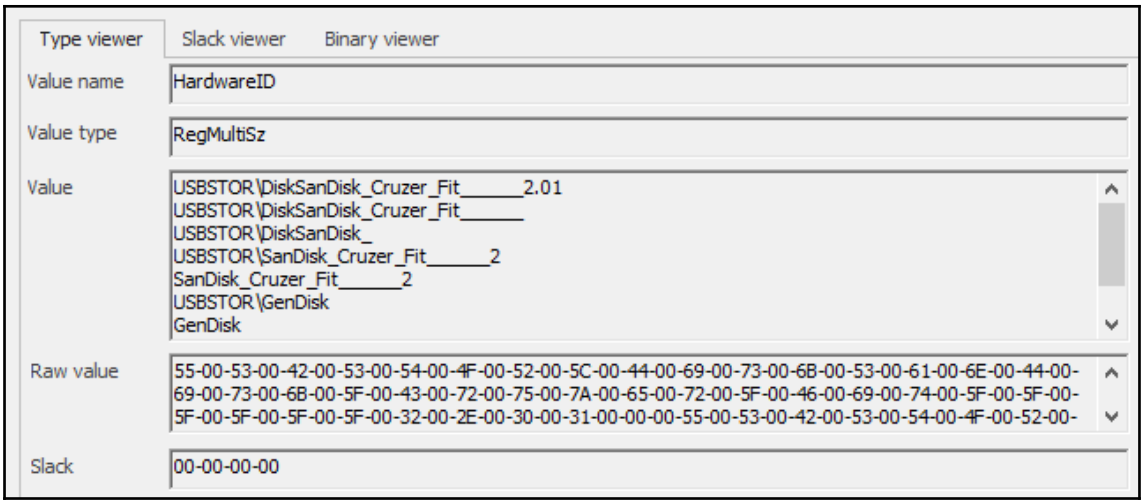

config (43)
Journal (2)
RegBack (17)
systemprofile (10)
TxR (9)
cs-CZ (13)
da-DK (13)
DEFAULT.LOG
2010-11-21 07:20:59 UTC
DEFAULT.LOG1
2015-03-25 15:31:05 UTC
DEFAULT.LOG2
2009-07-14 02:34:08 UTC
SAM
2015-03-25 15:31:05 UTC
SAM.LOG
2010-11-21 07:20:59 UTC


This PC › Data (D:) › JSmith_LT_0976_Registry
Name
Date modified
Type
Size
JSmith_LT_0976_Registry-SAM
9/12/2019 6:53 PM
File
256 KB
JSmith_LT_0976_Registry-SECURITY
9/12/2019 6:55 PM
File
256 KB
JSmith_LT_0976_Registry-SOFTWARE
9/12/2019 6:53 PM
File
47,360 KB
JSmith_LT_0976_Registry-SYSTEM
9/12/2019 6:53 PM
File
12,288 KB

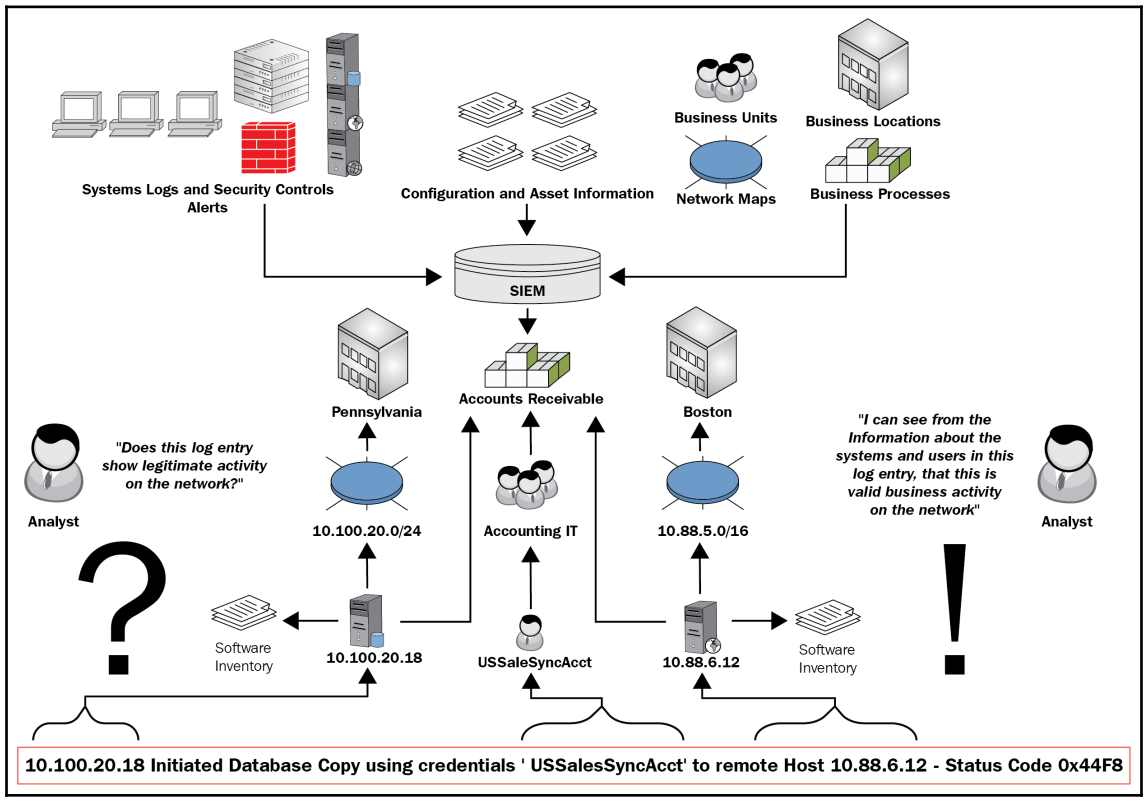


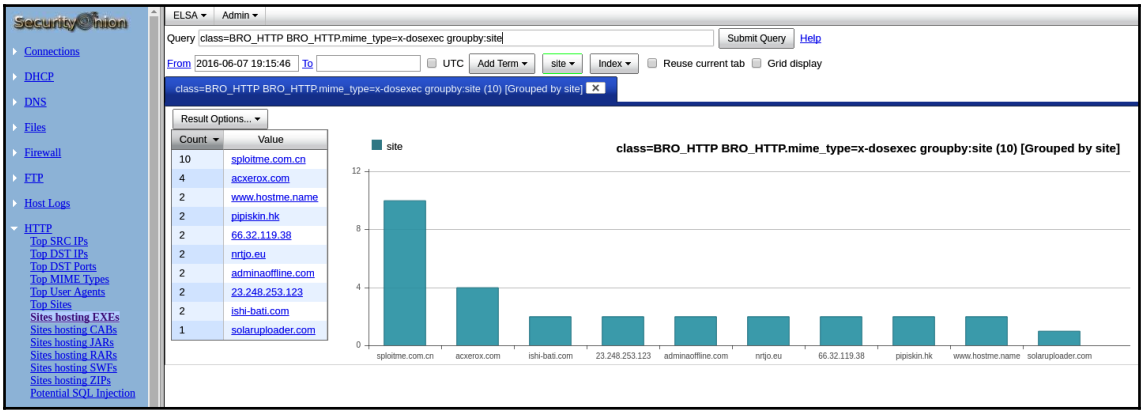


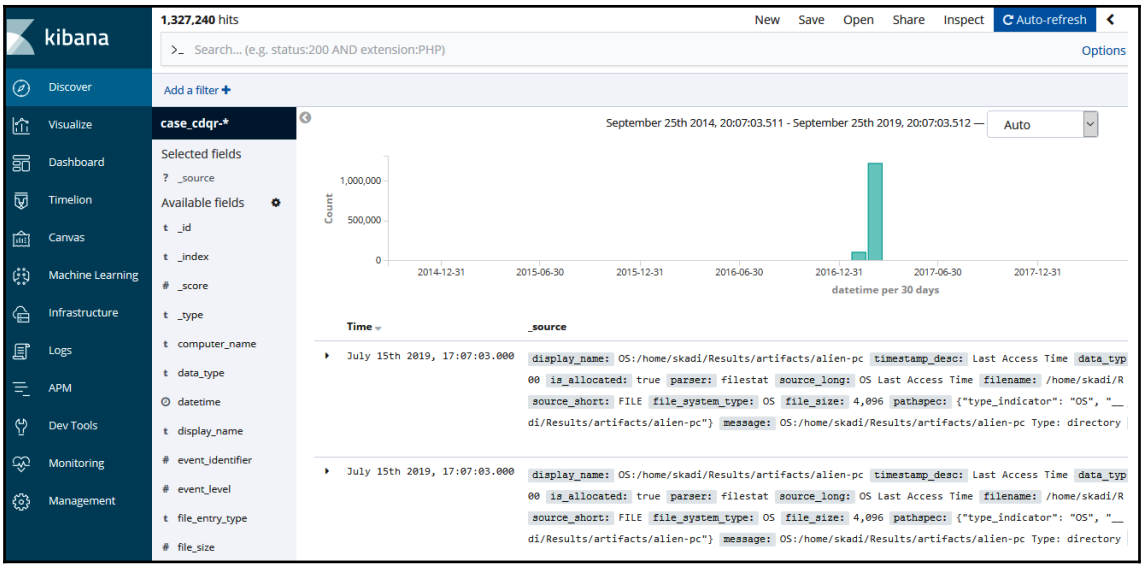
Value Name	Value Type	Data	Data Record Reall...	Is Deleted	Value Slack
Capabilities	RegDword	16	☐	☐	
Class	RegSz	DiskDrive	☐	☐	
ClassGUID	RegSz	{4d36e967-e325-...	☐	☐	00-00-00-00-00-00
CompatibleIDs	RegMultiSz	USBSTOR\Disk US...	☐	☐	
ConfigFlags	RegDword	0	☐	☐	
ContainerID	RegSz	{4933888a-6002-...	☐	☐	00-00-00-00-00-00
DeviceDesc	RegSz	@disk.inf,%disk_...	☐	☐	22-00-00-00
Driver	RegSz	{4d36e967-e325-...	☐	☐	00-00-00-00
FriendlyName	RegSz	SanDisk Cruzer Fit...	☐	☐	
HardwareID	RegMultiSz	USBSTOR\DiskSan...	☐	☐	00-00-00-00
Mfg	RegSz	@disk.inf,%genm...	☐	☐	B7-DA-00-00-00-00
Service	RegSz	disk	☐	☐	50-00

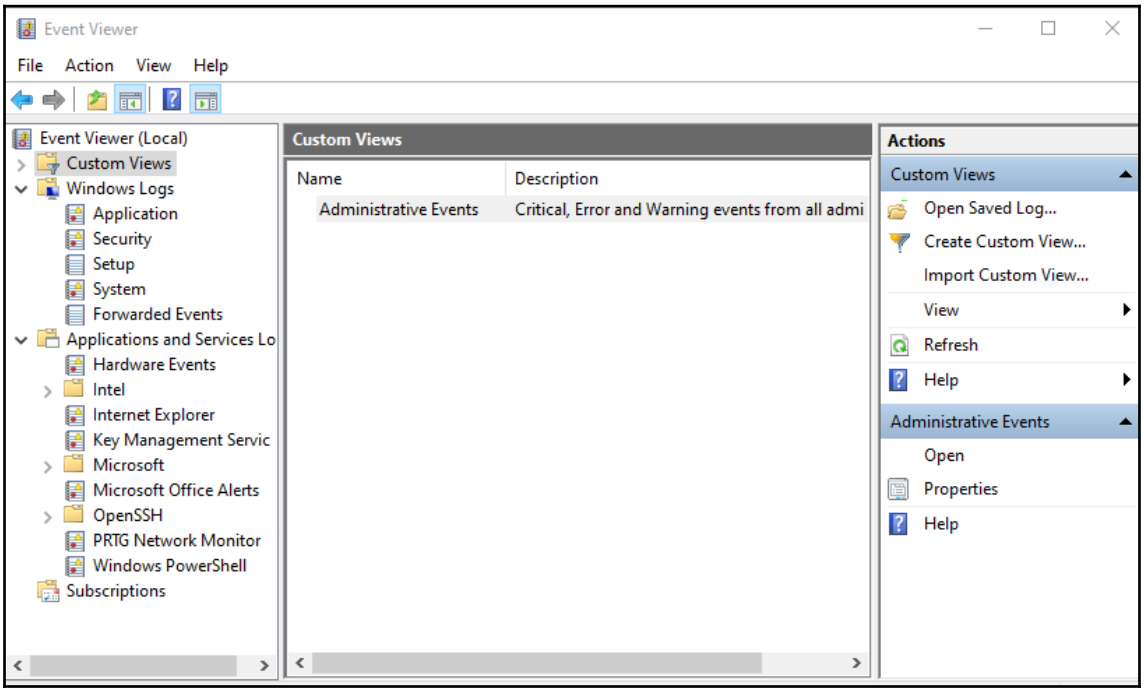

Type viewer
Slack viewer
Binary viewer
Value name
HardwareID
Value type
RegMultiSz
Value
USBSTOR\DiskSanDisk_Cruzer_Fit_____2.01
USBSTOR\DiskSanDisk_Cruzer_Fit_____
USBSTOR\DiskSanDisk_
USBSTOR\SanDisk_Cruzer_Fit_____2
SanDisk_Cruzer_Fit_____2
USBSTOR\GenDisk
GenDisk
Raw value
55-00-53-00-42-00-53-00-54-00-4F-00-52-00-5C-00-44-00-69-00-73-00-6B-00-53-00-61-00-6E-00-44-00-
69-00-73-00-6B-00-5F-00-43-00-72-00-75-00-7A-00-65-00-72-00-5F-00-46-00-69-00-74-00-5F-00-5F-00-
5F-00-5F-00-5F-00-5F-00-32-00-2E-00-30-00-31-00-00-00-55-00-53-00-42-00-53-00-54-00-4F-00-52-00-
Slack
00-00-00-00

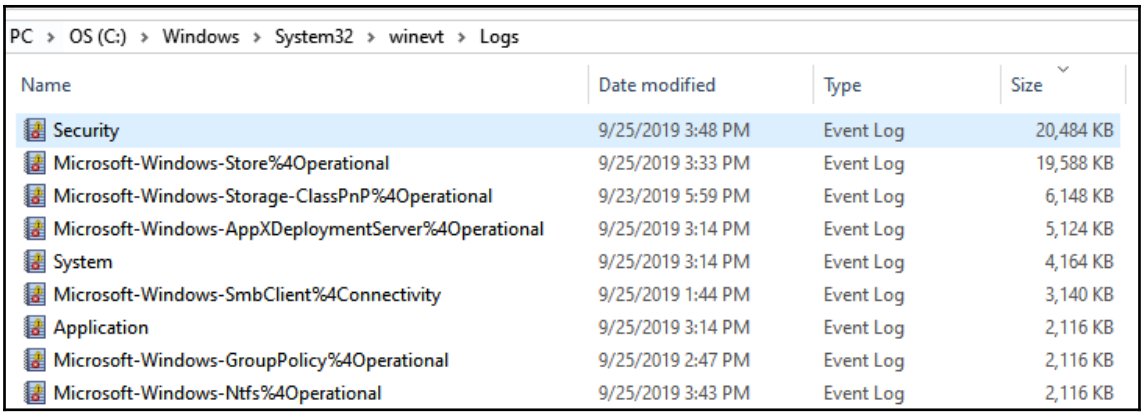
Chapter 10: Analyzing Log Files






kibana
1,327,240 hits
New
Save
Open
Share
Inspect
Auto-refresh
Search... (e.g. status:200 AND extension:PHP)
Options
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
computer_name
data_type
datetime
display_name
event_identifier
event_level
file_entry_type
file_size
September 25th 2014, 20:07:03.511 - September 25th 2019, 20:07:03.512 —
Auto
Count
1,000,000
500,000
0
2014-12-31
2015-06-30
2015-12-31
2016-06-30
2016-12-31
2017-06-30
2017-12-31
datetime per 30 days
Time
_source
July 15th 2019, 17:07:03.000
display_name: OS:/home/skadi/Results/artifacts/alien-pc timestamp_desc: Last Access Time data_typ
00 is_allocated: true parser: filestat source_long: OS Last Access Time filename: /home/skadi/R
source_short: FILE file_system_type: OS file_size: 4,096 pathspec: {"type_indicator": "OS", "__
di/Results/artifacts/alien-pc"} message: OS:/home/skadi/Results/artifacts/alien-pc Type: directory
July 15th 2019, 17:07:03.000
display_name: OS:/home/skadi/Results/artifacts/alien-pc timestamp_desc: Last Access Time data_typ
00 is_allocated: true parser: filestat source_long: OS Last Access Time filename: /home/skadi/R
source_short: FILE file_system_type: OS file_size: 4,096 pathspec: {"type_indicator": "OS", "__
di/Results/artifacts/alien-pc"} message: OS:/home/skadi/Results/artifacts/alien-pc Type: directory


Event Viewer
File
Action
View
Help
Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Lo
Hardware Events
Intel
Internet Explorer
Key Management Servic
Microsoft
Microsoft Office Alerts
OpenSSH
PRTG Network Monitor
Windows PowerShell
Subscriptions
Custom Views
Name
Description
Administrative Events
Critical, Error and Warning events from all admi
Actions
Custom Views
Open Saved Log...
Create Custom View...
Import Custom View...
View
Refresh
Help
Administrative Events
Open
Properties
Help



PC › OS (C:) › Windows › System32 › winevt › Logs

Name	Date modified	Type	Size
Security	9/25/2019 3:48 PM	Event Log	20,484 KB
Microsoft-Windows-Store%4Operational	9/25/2019 3:33 PM	Event Log	19,588 KB
Microsoft-Windows-Storage-ClassPnP%4Operational	9/23/2019 5:59 PM	Event Log	6,148 KB
Microsoft-Windows-AppXDeploymentServer%4Operational	9/25/2019 3:14 PM	Event Log	5,124 KB
System	9/25/2019 3:14 PM	Event Log	4,164 KB
Microsoft-Windows-SmbClient%4Connectivity	9/25/2019 1:44 PM	Event Log	3,140 KB
Application	9/25/2019 3:14 PM	Event Log	2,116 KB
Microsoft-Windows-GroupPolicy%4Operational	9/25/2019 2:47 PM	Event Log	2,116 KB
Microsoft-Windows-Ntfs%4Operational	9/25/2019 3:43 PM	Event Log	2,116 KB

```
echo Log Files
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
```

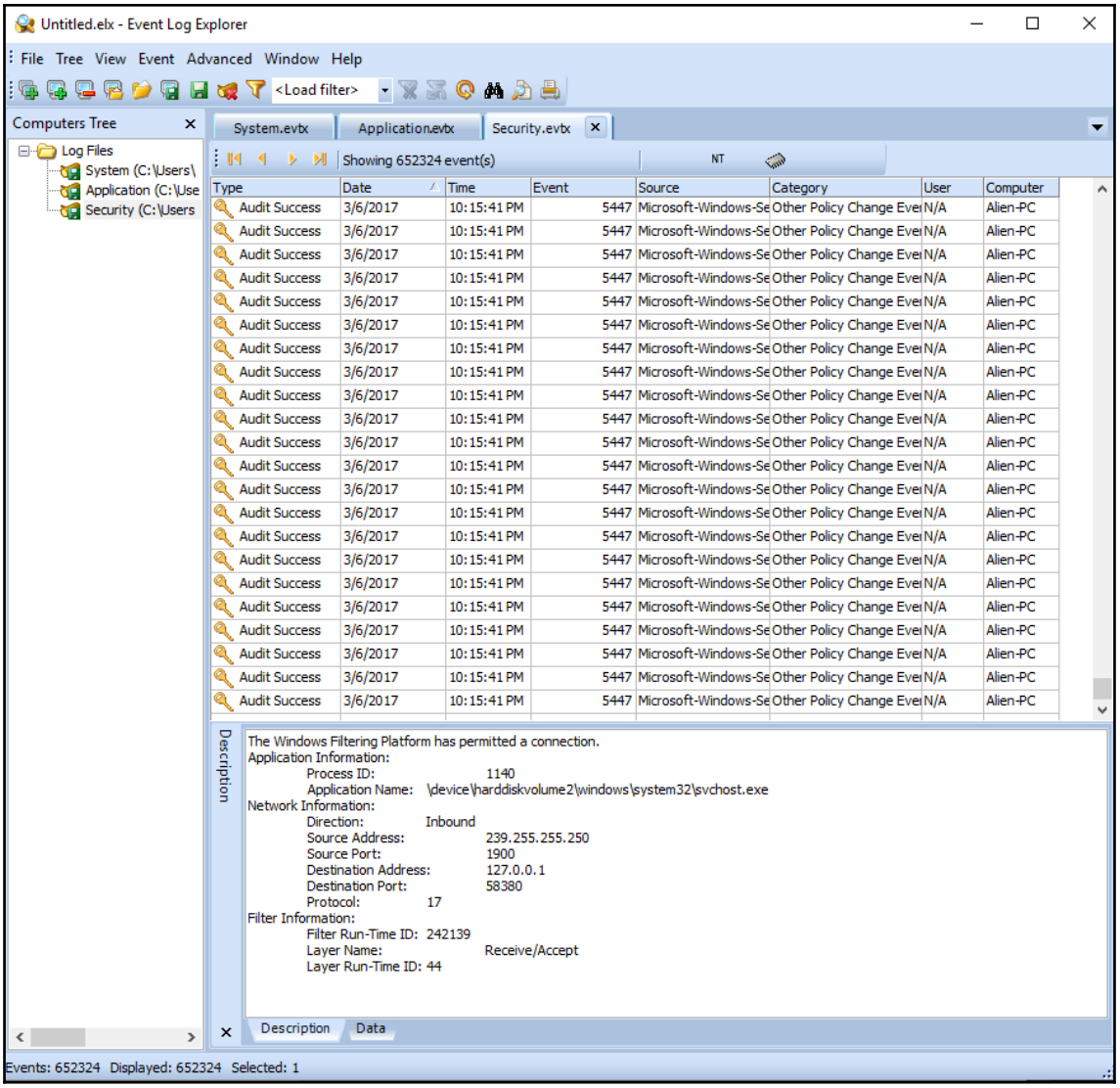
```
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-Security-Adminless%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-Security-Audit-Configuration-Client%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-Security-EnterpriseData-FileRevocationManager%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-Security-LessPrivilegedAppContainer%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-Security-Mitigations%4KernelMode.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-Security-Mitigations%4UserMode.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-Security-Netlogon%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-Security-SPP-UX-GenuineCenter-Logging%4Operational.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-Security-SPP-UX-Notifications%4ActionCenter.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-Security-UserConsentVerifier%4Audit.evtx
Collecting File: C:\WINDOWS\System32\winevt\logs\Microsoft-Windows-SecurityMitigationsBroker%4Operational.evtx
```

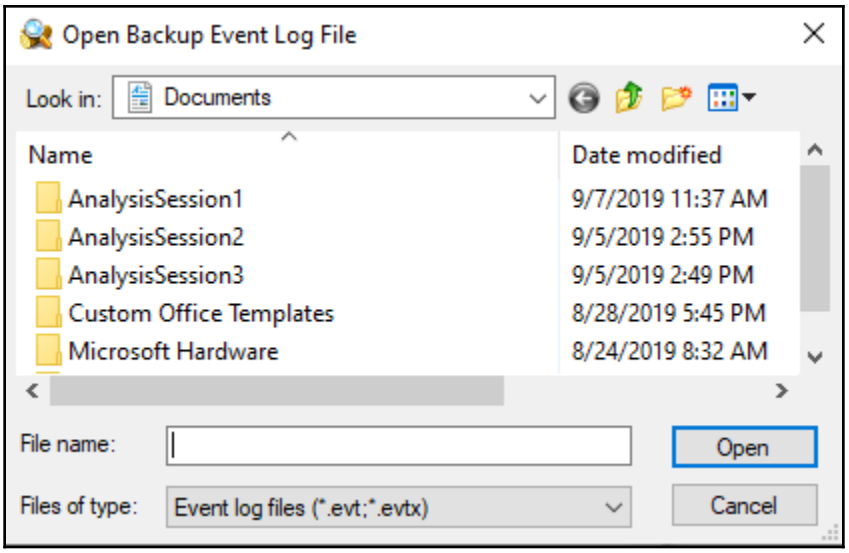
```
PS C:\Users\IRProactive-WKST\Desktop\DeepBlueCLI-master> .\DeepBlue.ps1 C:\Users\IRProactive-WKST\Desktop\evtx\Security.evtx
```

```
Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your
computer. If you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning
message. Do you want to run C:\Users\IRProactive-WKST\Desktop\DeepBlueCLI-master\DeepBlue.ps1?
[D] Do not run  [R] Run once  [S] Suspend  [?] Help (default is "D"): R
```

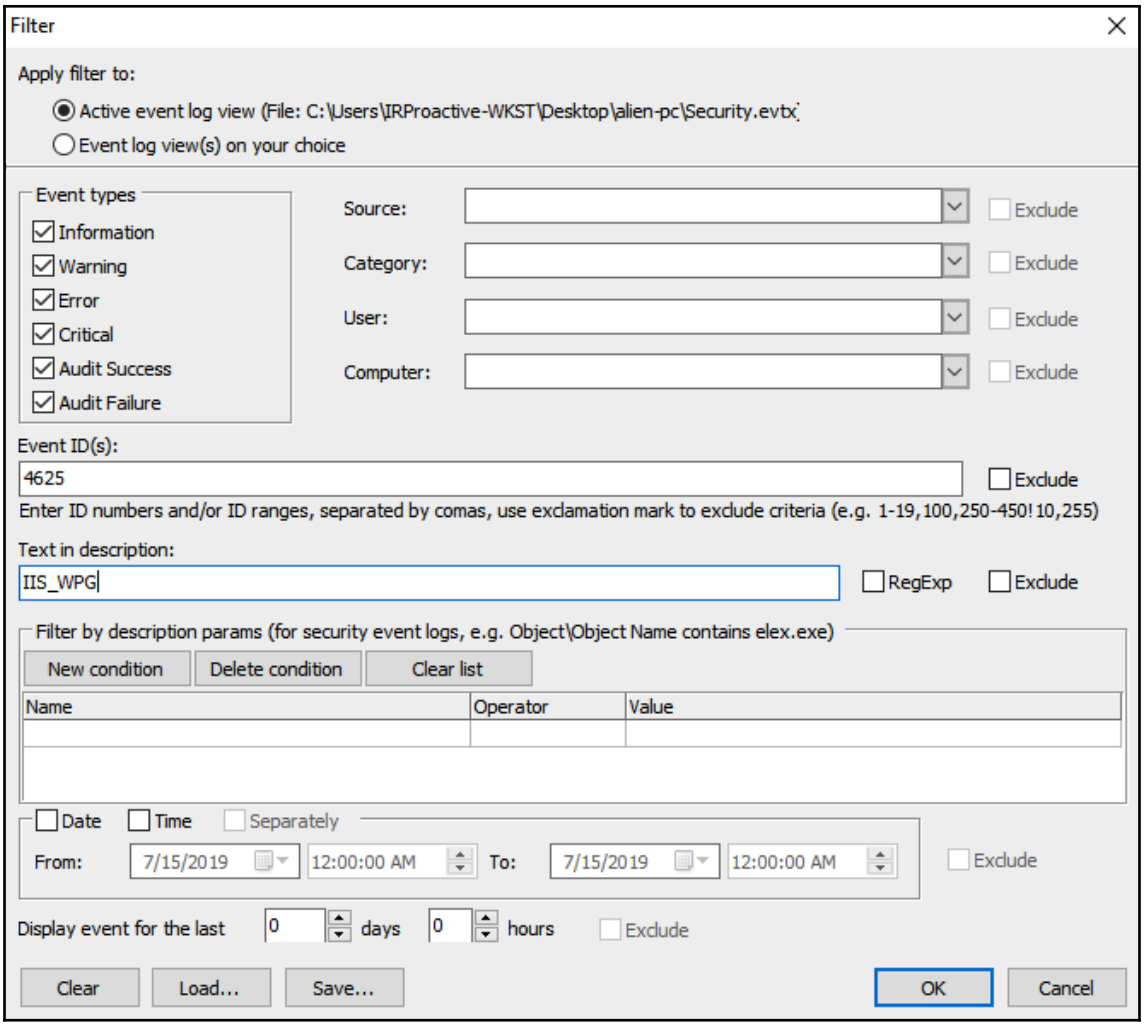
```
Date    : 2/15/2017 11:05:20 PM
Log     : Security
EventID : 4625
Message : High number of logon failures for one account
Results : Username: War_Machine
          Total logon failures: 2287
Command :
Decoded :

Date    : 2/15/2017 11:05:20 PM
Log     : Security
EventID : 4625
Message : High number of logon failures for one account
Results : Username: IIS_WPG
          Total logon failures: 2290
Command :
Decoded :

Date    : 2/15/2017 11:05:20 PM
Log     : Security
EventID : 4625
Message : High number of total logon failures for multiple accounts
Results : Total accounts: 7
          Total logon failures: 10006
```

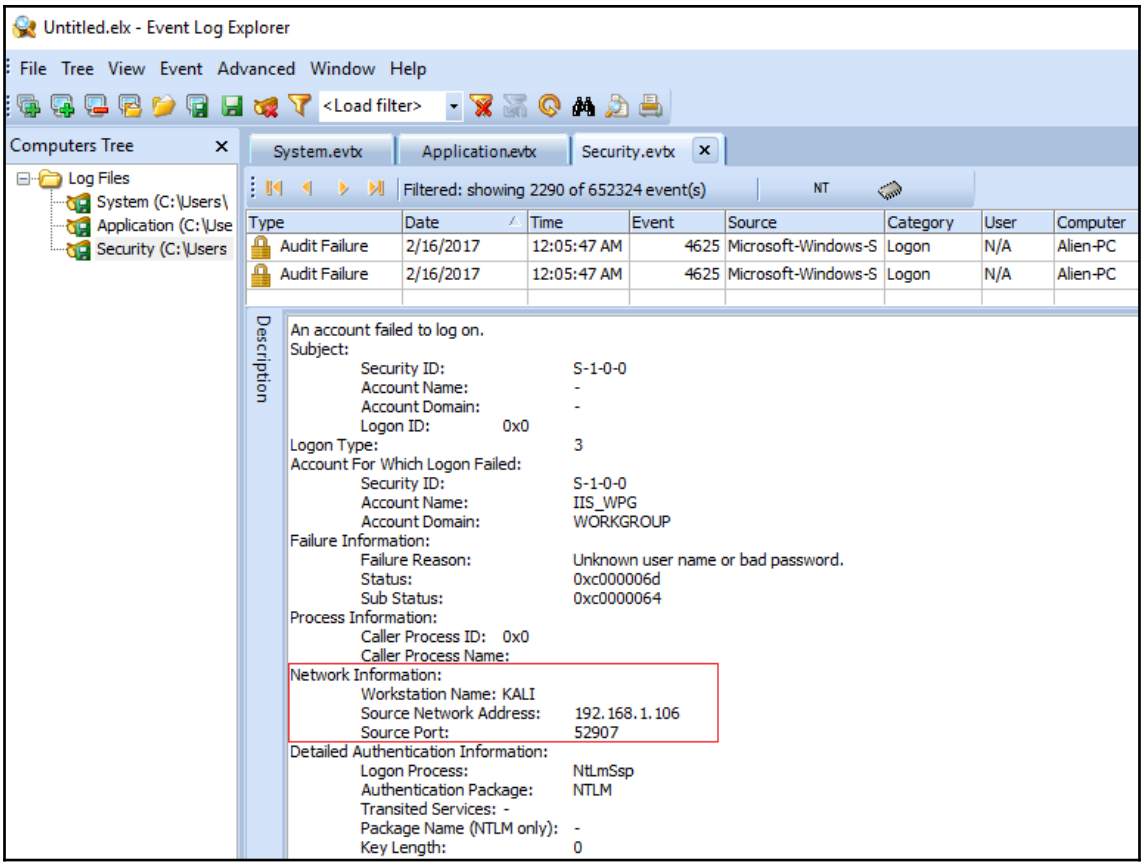
```
Date    : 2/22/2017 6:35:08 PM
Log     : Security
EventID : 4720
Message : New User Created
Results : Username: MBadegain
          User SID: S-1-5-21-2865824651-146060924-1132756725-1019

Command :
Decoded :

Date    : 2/22/2017 6:34:55 PM
Log     : Security
EventID : 4720
Message : New User Created
Results : Username: BFernandez
          User SID: S-1-5-21-2865824651-146060924-1132756725-1018

Command :
Decoded :

Date    : 2/22/2017 6:34:27 PM
Log     : Security
EventID : 4720
Message : New User Created
Results : Username: MMartin
          User SID: S-1-5-21-2865824651-146060924-1132756725-1017
```


Untitled.elx - Event Log Explorer
File Tree View Event Advanced Window Help
<Load filter>
Computers Tree
Log Files
System (C:\Users\
Application (C:\Use
Security (C:\Users
System.evtx
Application.evtx
Security.evtx
Showing 652324 event(s)
NT
Type Date Time Event Source Category User Computer
Audit Success 3/6/2017 10:15:41 PM 5447 Microsoft-Windows-Se Other Policy Change Evei N/A Alien-PC
Description
The Windows Filtering Platform has permitted a connection.
Application Information:
Process ID: 1140
Application Name: \device\harddiskvolume2\windows\system32\svchost.exe
Network Information:
Direction: Inbound
Source Address: 239.255.255.250
Source Port: 1900
Destination Address: 127.0.0.1
Destination Port: 58380
Protocol: 17
Filter Information:
Filter Run-Time ID: 242139
Layer Name: Receive/Accept
Layer Run-Time ID: 44
Description
Data
Events: 652324 Displayed: 652324 Selected: 1


Open Backup Event Log File
Look in:
Documents
Name
Date modified
AnalysisSession1
9/7/2019 11:37 AM
AnalysisSession2
9/5/2019 2:55 PM
AnalysisSession3
9/5/2019 2:49 PM
Custom Office Templates
8/28/2019 5:45 PM
Microsoft Hardware
8/24/2019 8:32 AM
File name:
Open
Files of type:
Event log files (*.evt;*.evtx)
Cancel

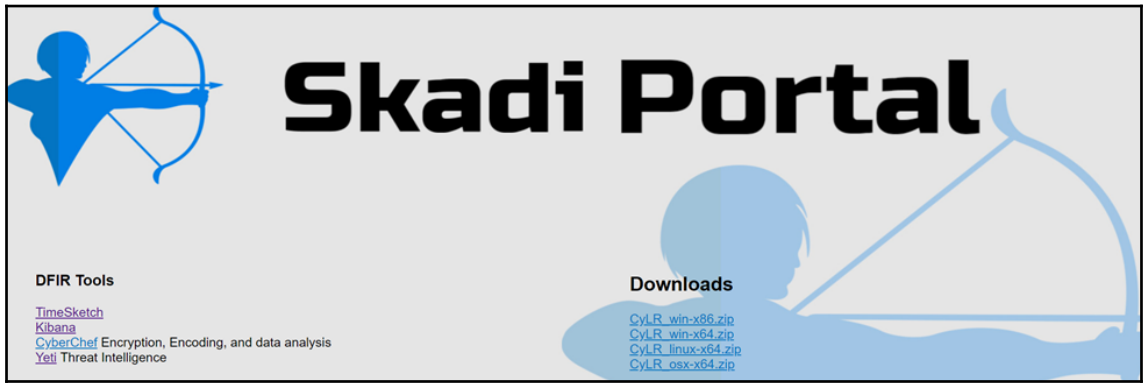

<Load filter>

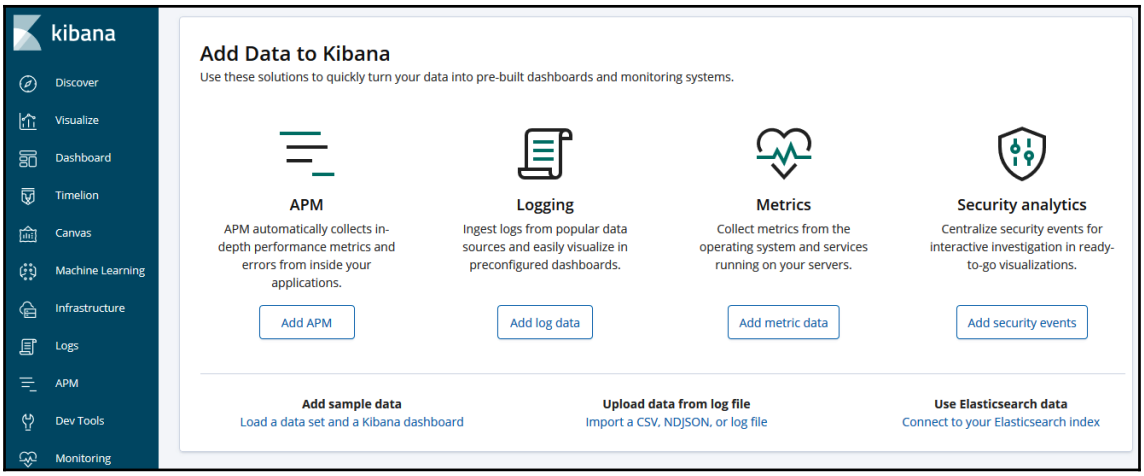

Filter
Apply filter to:
Active event log view (File: C:\Users\IRProactive-WKST\Desktop\alien-pc\Security.evtx
Event log view(s) on your choice
Event types
Information
Warning
Error
Critical
Audit Success
Audit Failure
Source:
Category:
User:
Computer:
Exclude
Event ID(s):
4625
Enter ID numbers and/or ID ranges, separated by comas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)
Text in description:
IIS_WPG
RegExp
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:
7/15/2019
12:00:00 AM
To:
Display event for the last
days
hours
Clear
Load...
Save...
OK
Cancel

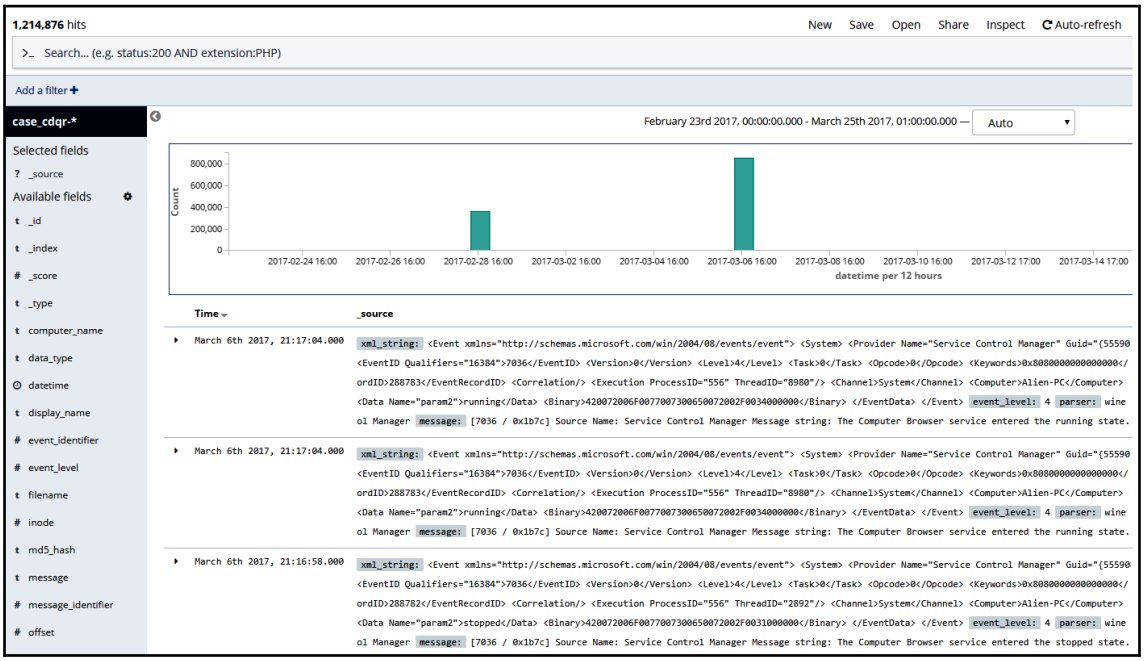


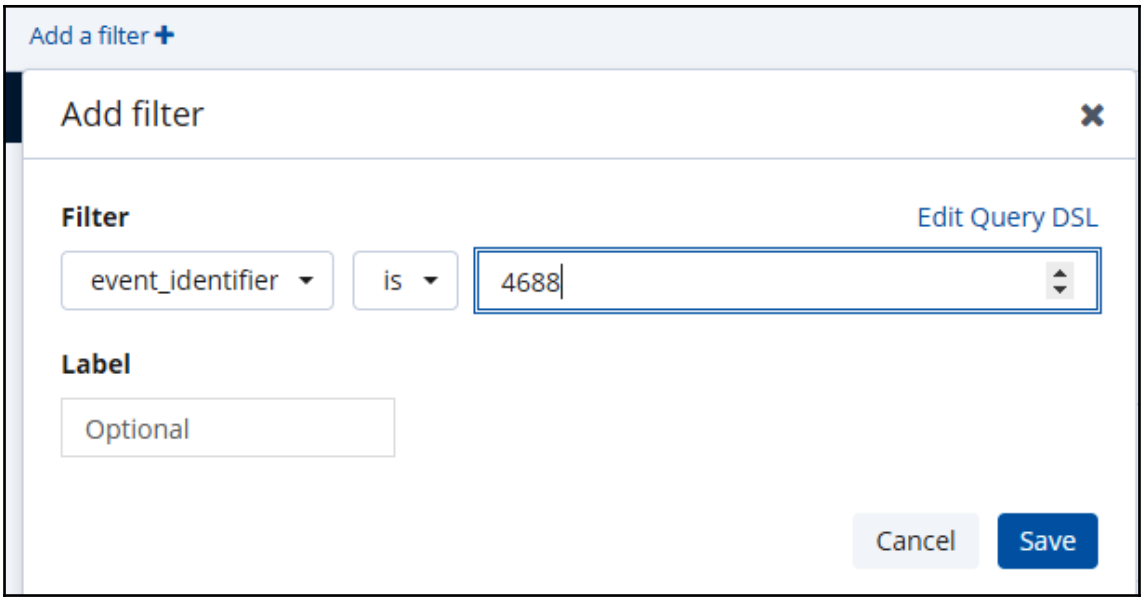

```
skadi@skadi:~$ cdqr in:alien-pc.zip out:Results -z --max_cpu
docker run   -v /etc/hosts:/etc/hosts:ro   --network host -v /home/skadi/alien-pc.zip:/home/skadi/al
ien-pc.zip -v /home/skadi/Results:/home/skadi/Results aorlikoski/cdqr:4.4.0 -y /home/skadi/alien-pc.
zip /home/skadi/Results -z --max_cpu
```

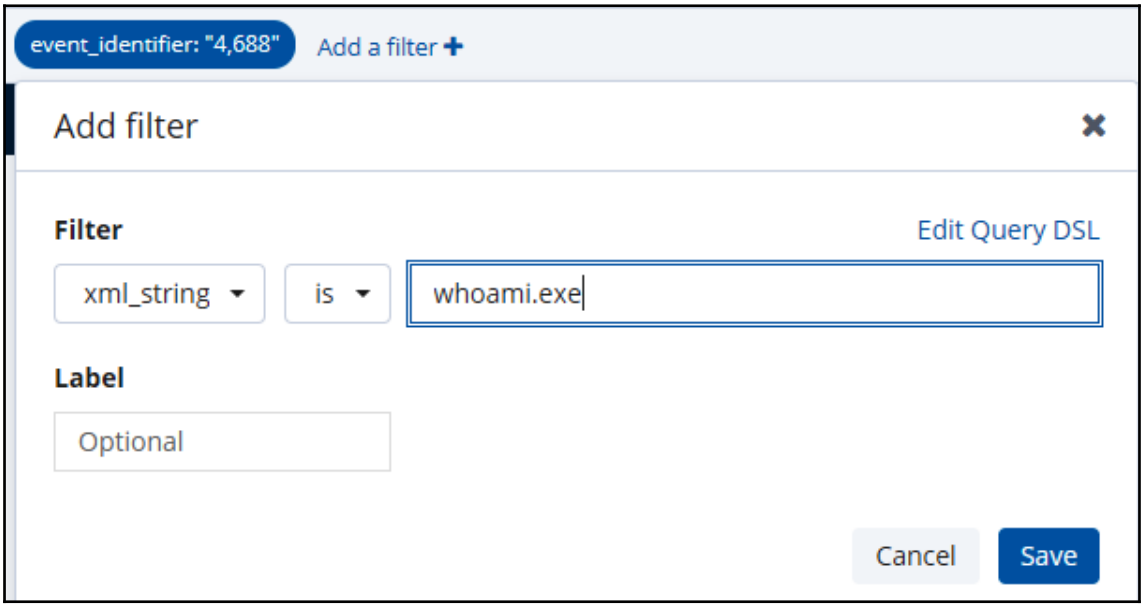
```
skadi@skadi:~$ cdqr in:Results/alien-pc.plaso --plaso_db --es_kb winevt
docker run   -v /etc/hosts:/etc/hosts:ro   --network host -v /home/skadi/Results/alien-pc.plaso:/hom
e/skadi/Results/alien-pc.plaso aorlikoski/cdqr:4.4.0 -y /home/skadi/Results/alien-pc.plaso --plaso_d
b --es_kb winevt
CDQR Version: 4.4
Plaso Version: 20190131
WARNING!! Known compatible version of Plaso NOT detected. Attempting to use default parser list. Try
 using the --no_dependencies_check if Plaso dependancies are the issue.
Using parser: win
Number of cpu cores to use: 1
Destination Folder: Results
Source data: /home/skadi/Results/alien-pc.plaso
Log File: Results/alien-pc.plaso.log
Database File: Results//home/skadi/Results/alien-pc.plaso

Total start time was: 2019-07-16 01:51:32.335461
WARNING: File must be plaso database file otherwise it will not work.  Example: artifact.plaso (from
 CDQR)

Process to export to ElasticSearch started
Exporting results in Kibana format to the ElasticSearch server
"psort.py" "-o" "elastic" "--status_view" "linear" "--index_name" "case_cdqr-winevt" "--server" "127
.0.0.1" "--port" "9200" "/home/skadi/Results/alien-pc.plaso"
All entries have been inserted into database with case: case_cdqr-winevt

Process to export to ElasticSearch completed
ElasticSearch export process duration was: 0:13:03.303455
```




kibana
Discover
Visualize
Dashboard
Timelion
Canvas
Machine Learning
Infrastructure
Logs
APM
Dev Tools
Monitoring
Add Data to Kibana
Use these solutions to quickly turn your data into pre-built dashboards and monitoring systems.
APM
APM automatically collects in-depth performance metrics and errors from inside your applications.
Add APM
Logging
Ingest logs from popular data sources and easily visualize in preconfigured dashboards.
Add log data
Metrics
Collect metrics from the operating system and services running on your servers.
Add metric data
Security analytics
Centralize security events for interactive investigation in ready-to-go visualizations.
Add security events
Add sample data
Load a data set and a Kibana dashboard
Upload data from log file
Import a CSV, NDJSON, or log file
Use Elasticsearch data
Connect to your Elasticsearch index


1,214,876 hits
New
Save
Open
Share
Inspect
Auto-refresh
Search... (e.g. status:200 AND extension:PHP)
Add a filter
case_cdqr-*
Selected fields
_source
Available fields
_id
_index
_score
_type
computer_name
data_type
datetime
display_name
event_identifier
event_level
filename
inode
md5_hash
message
message_identifier
offset
February 23rd 2017, 00:00:00.000 - March 25th 2017, 01:00:00.000 —
Auto
Count
800,000
600,000
400,000
200,000
0
2017-02-24 16:00
2017-02-26 16:00
2017-02-28 16:00
2017-03-02 16:00
2017-03-04 16:00
2017-03-06 16:00
2017-03-08 16:00
2017-03-10 16:00
2017-03-12 17:00
2017-03-14 17:00
datetime per 12 hours
Time
_source
March 6th 2017, 21:17:04.000
xml_string: <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"> <System> <Provider Name="Service Control Manager" Guid="{55590
<EventID Qualifiers="16384">7036</EventID> <Version>0</Version> <Level>4</Level> <Task>0</Task> <Opcode>0</Opcode> <Keywords>0x8080000000000000</
ordID>288783</EventRecordID> <Correlation/> <Execution ProcessID="556" ThreadID="8980"/> <Channel>System</Channel> <Computer>Alien-PC</Computer>
<Data Name="param2">running</Data> <Binary>420072006F00770073006500720 02F0034000000</Binary> </EventData> </Event> event_level: 4 parser: wine
ol Manager message: [7036 / 0x1b7c] Source Name: Service Control Manager Message string: The Computer Browser service entered the running state.
March 6th 2017, 21:17:04.000
xml_string: <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"> <System> <Provider Name="Service Control Manager" Guid="{55590
<EventID Qualifiers="16384">7036</EventID> <Version>0</Version> <Level>4</Level> <Task>0</Task> <Opcode>0</Opcode> <Keywords>0x8080000000000000</
ordID>288783</EventRecordID> <Correlation/> <Execution ProcessID="556" ThreadID="8980"/> <Channel>System</Channel> <Computer>Alien-PC</Computer>
<Data Name="param2">running</Data> <Binary>420072006F00770073006500720 02F0034000000</Binary> </EventData> </Event> event_level: 4 parser: wine
ol Manager message: [7036 / 0x1b7c] Source Name: Service Control Manager Message string: The Computer Browser service entered the running state.
March 6th 2017, 21:16:58.000
xml_string: <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"> <System> <Provider Name="Service Control Manager" Guid="{55590
<EventID Qualifiers="16384">7036</EventID> <Version>0</Version> <Level>4</Level> <Task>0</Task> <Opcode>0</Opcode> <Keywords>0x8080000000000000</
ordID>288782</EventRecordID> <Correlation/> <Execution ProcessID="556" ThreadID="2892"/> <Channel>System</Channel> <Computer>Alien-PC</Computer>
<Data Name="param2">stopped</Data> <Binary>420072006F00770073006500720 02F0031000000</Binary> </EventData> </Event> event_level: 4 parser: wine
ol Manager message: [7036 / 0x1b7c] Source Name: Service Control Manager Message string: The Computer Browser service entered the stopped state.

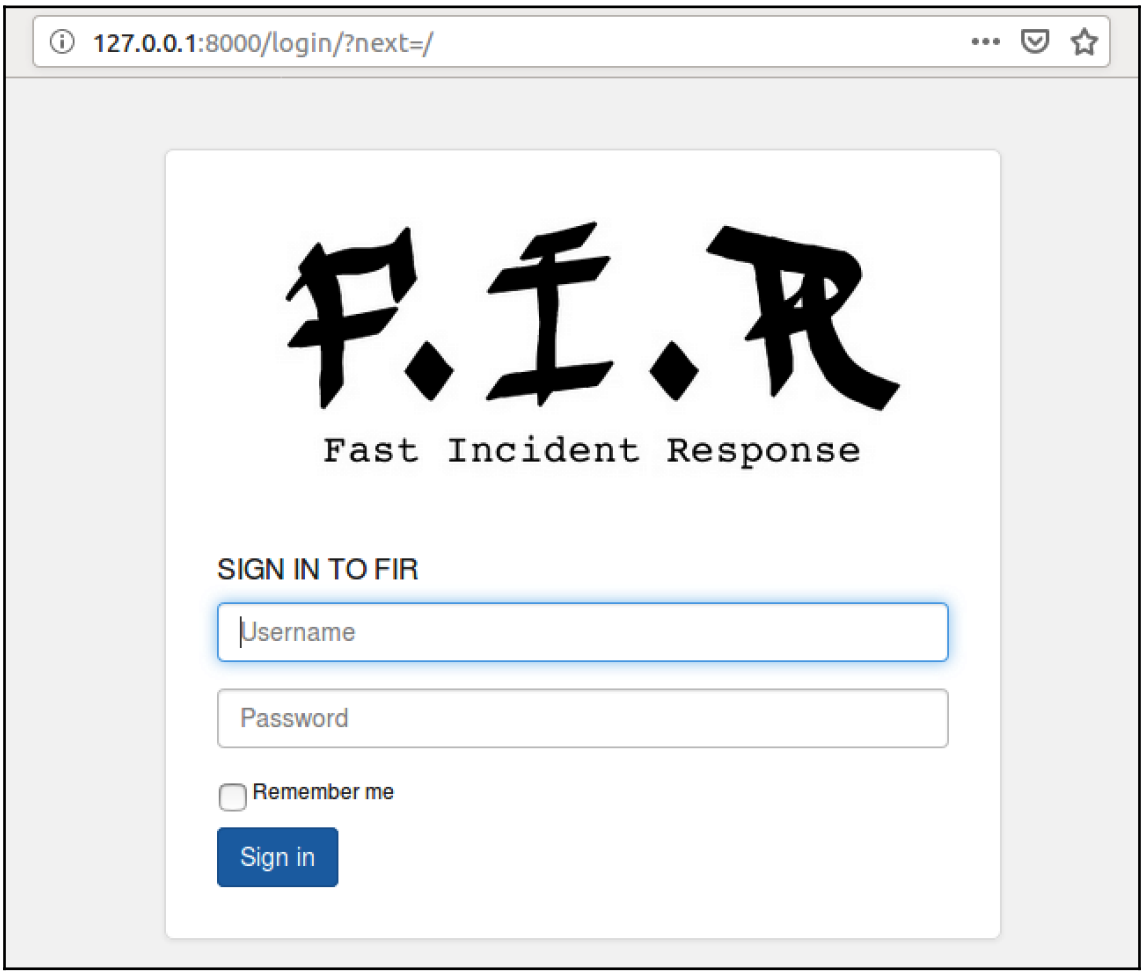

Add a filter +
Add filter
Filter
Edit Query DSL
event_identifier
is
4688
Label
Optional
Cancel
Save

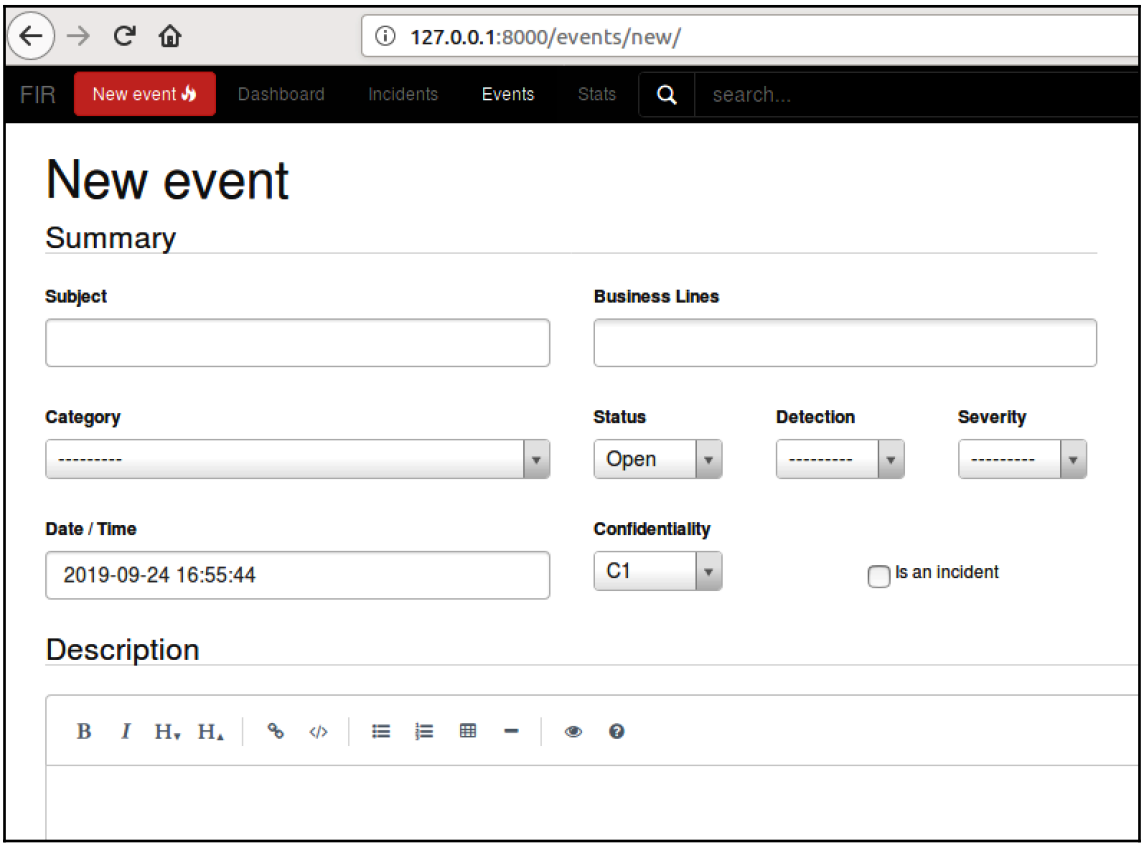

event_identifier: "4,688"
Add a filter +
Add filter
Filter
Edit Query DSL
xml_string
is
whoami.exe
Label
Optional
Cancel
Save

t xml_string

```
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  <System>
    <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-A5BA-3E3B0328C30D}"/>
    <EventID>4688</EventID>
    <Version>1</Version>
    <Level>0</Level>
    <Task>13312</Task>
    <Opcode>0</Opcode>
    <Keywords>0x8020000000000000</Keywords>
    <TimeCreated SystemTime="2017-03-07T05:11:01.568600000Z"/>
    <EventRecordID>9505938</EventRecordID>
    <Correlation/>
    <Execution ProcessID="4" ThreadID="68"/>
    <Channel>Security</Channel>
    <Computer>Alien-PC</Computer>
    <Security/>
  </System>
  <EventData>
    <Data Name="SubjectUserSid">S-1-5-21-2865824651-146060924-1132756725-500</Data>
    <Data Name="SubjectUserName">Administrator</Data>
    <Data Name="SubjectDomainName">Alien-PC</Data>
    <Data Name="SubjectLogonId">0x000000000162e98c</Data>
    <Data Name="NewProcessId">0x0000000000001a68</Data>
    <Data Name="NewProcessName">C:\Windows\System32\whoami.exe</Data>
    <Data Name="TokenElevationType">%%1936</Data>
    <Data Name="ProcessId">0x0000000000001a0c</Data>
    <Data Name="CommandLine"/>
  </EventData>
</Event>
```

Chapter 11: Writing the Incident Report

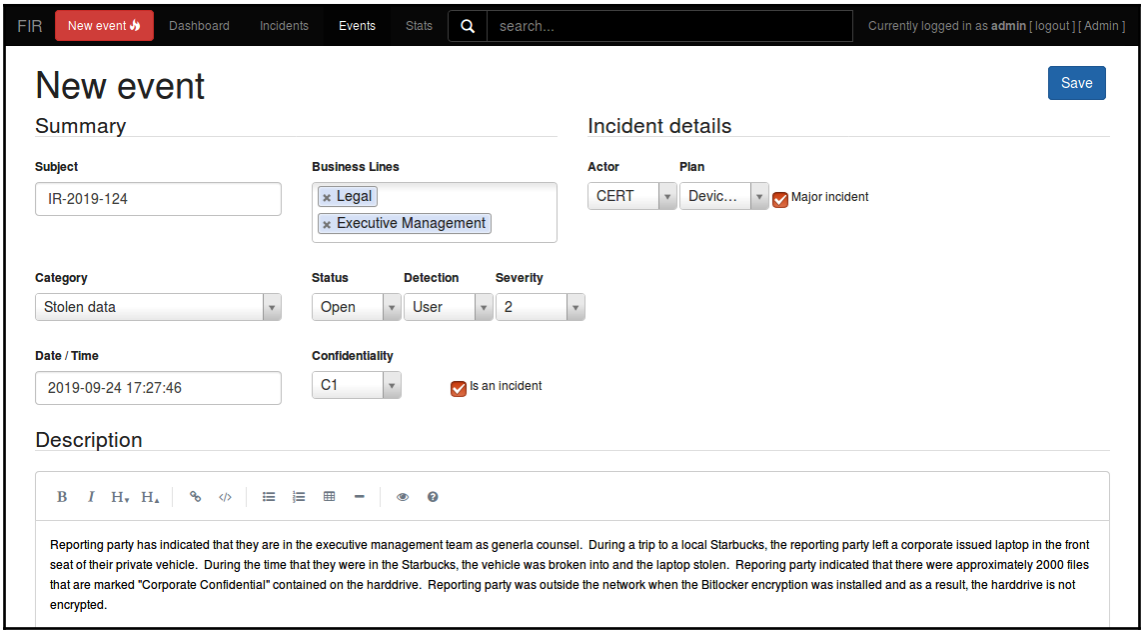



127.0.0.1:8000/events/new/
FIR
New event
Dashboard
Incidents
Events
Stats
search...
New event
Summary
Subject
Business Lines
Category

Status
Open
Detection

Severity

Date / Time
2019-09-24 16:55:44
Confidentiality
C1
Is an incident
Description


FIR
New event
Dashboard
Incidents
Events
Stats
search...
Currently logged in as admin [logout] [Admin]
New event
Save
Summary
Incident details
Subject
IR-2019-124
Business Lines
Legal
Executive Management
Actor
CERT
Plan
Devic...
Major incident
Category
Stolen data
Status
Open
Detection
User
Severity
2
Date / Time
2019-09-24 17:27:46
Confidentiality
C1
Is an incident
Description
Reporting party has indicated that they are in the executive management team as generla counsel. During a trip to a local Starbucks, the reporting party left a corporate issued laptop in the front seat of their private vehicle. During the time that they were in the Starbucks, the vehicle was broken into and the laptop stolen. Reporing party indicated that there were approximately 2000 files that are marked "Corporate Confidential" contained on the harddrive. Reporting party was outside the network when the Bitlocker encryption was installed and as a result, the harddrive is not encrypted.

Incident / Stolen data / IR-2019-124

Opened on Sept. 24, 2019, 5:27 p.m. by admin

DESCRIPTION

Reporting party has indicated that they are in the executive management team as generla counsel. During a trip to a local Starbucks, the reporting party left a corporate issued laptop in the front seat of their private vehicle. During the time that they were in the Starbucks, the vehicle was broken into and the laptop stolen. Reporing party indicated that there were approximately 2000 files that are marked "Corporate Confidential" contained on the harddrive. Reporting party was outside the network when the Bitlocker encryption was installed and as a result, the harddrive is not encrypted.

TO-DO LIST

Action	Accountable
Task	---------

+ Add To-Do Item

Comments (1)

		Comment	Action		
2019-09-24 17:27	admin	Incident opened	Opened	✎	✖

+ Add Comment Edit Block Close Incident followup Alert Takedown

STARRED INCIDENTS

No incidents to show.

Open | Blocked | Old | Tasks

Date		Category	Subject	Business Lines	Severity	Status	Detection	Leader	Last Action	Plan	Lvl	IH	Edit
2019-09-24	☆	Stolen data	IR-2019-124	Legal, Executive Management	2	Open	User	CERT	Opened in 9 hours	Device Loss	C1	admin	✎

(page 1 of 1)

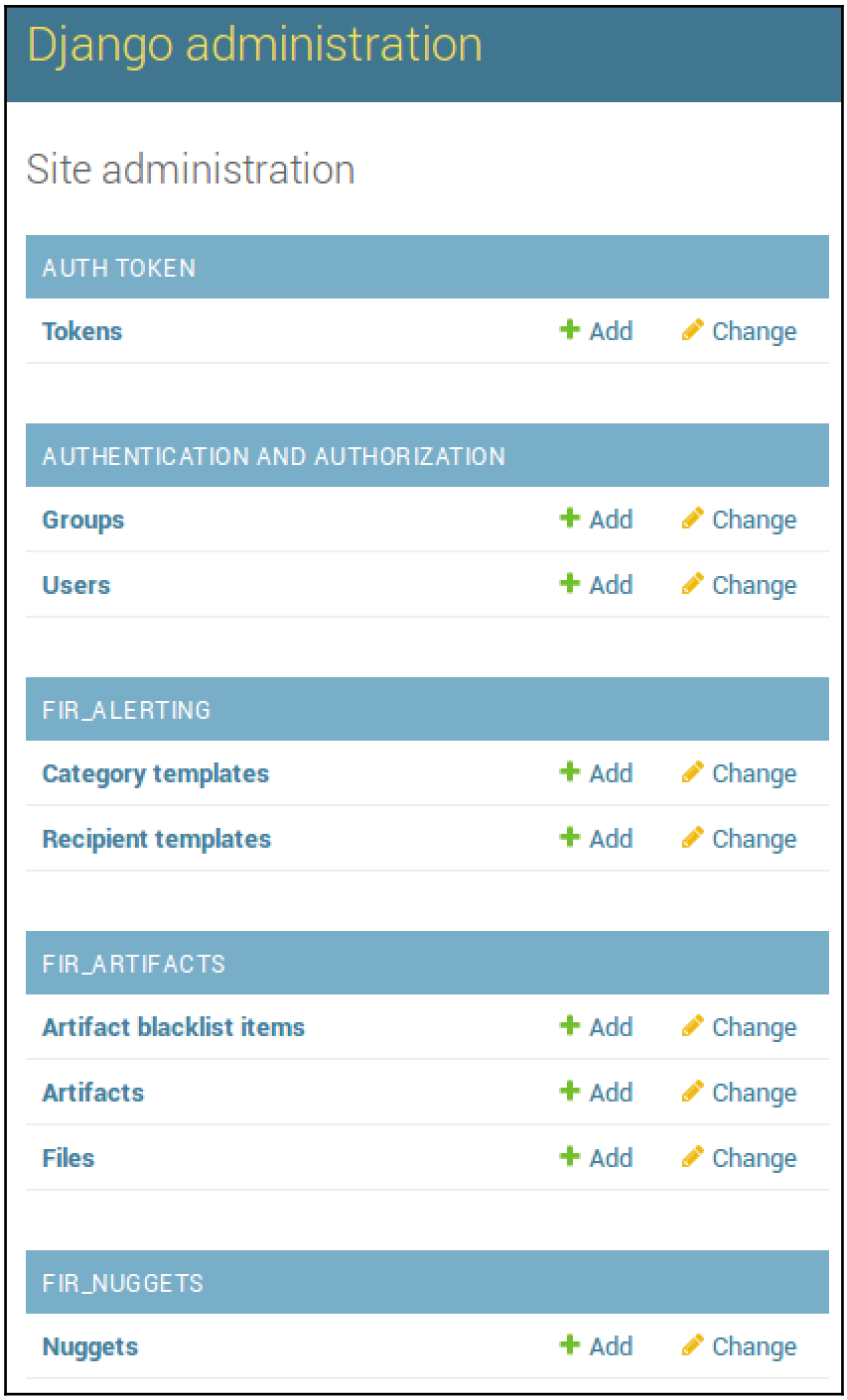
STARRED INCIDENTS

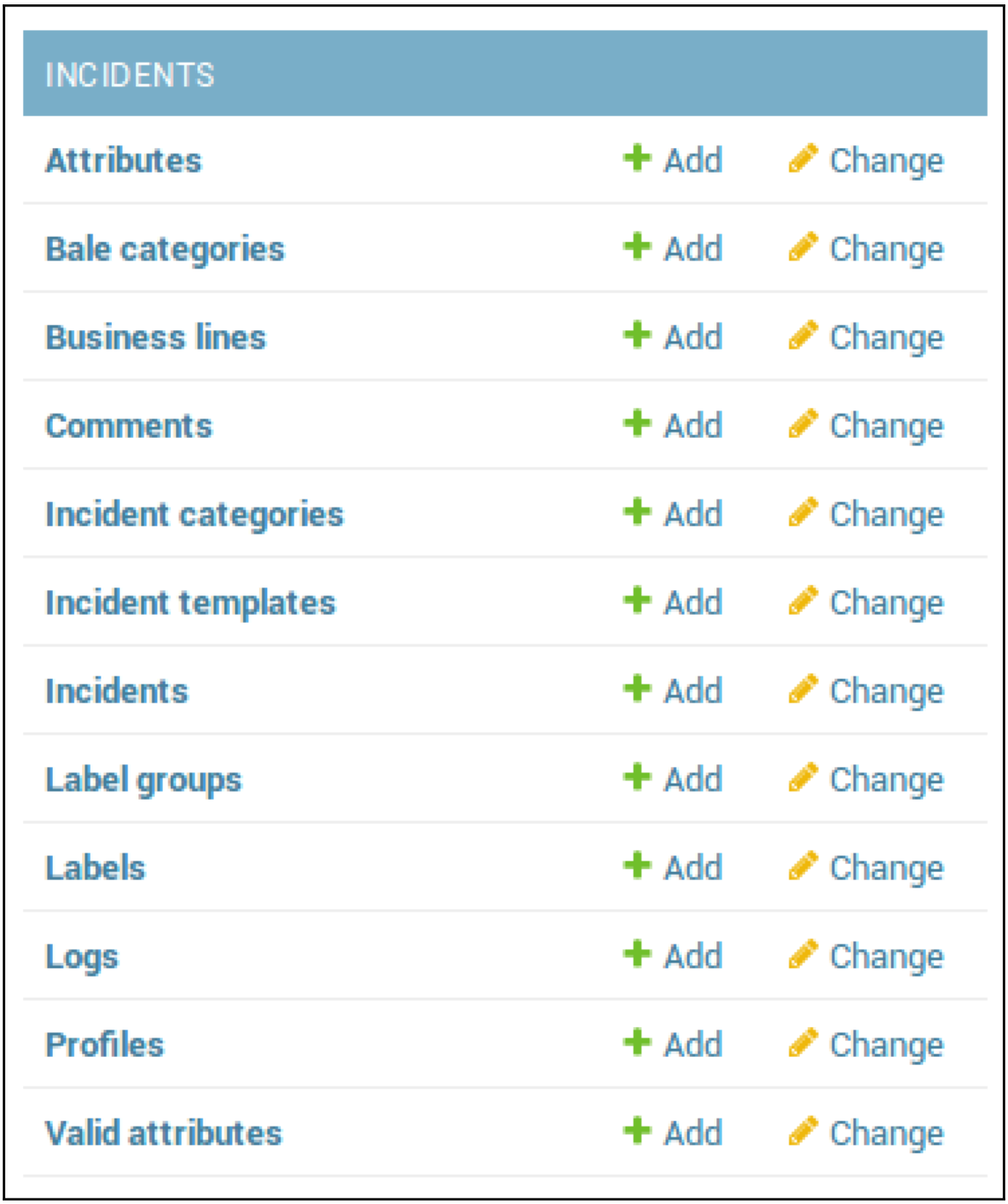
No incidents to show.

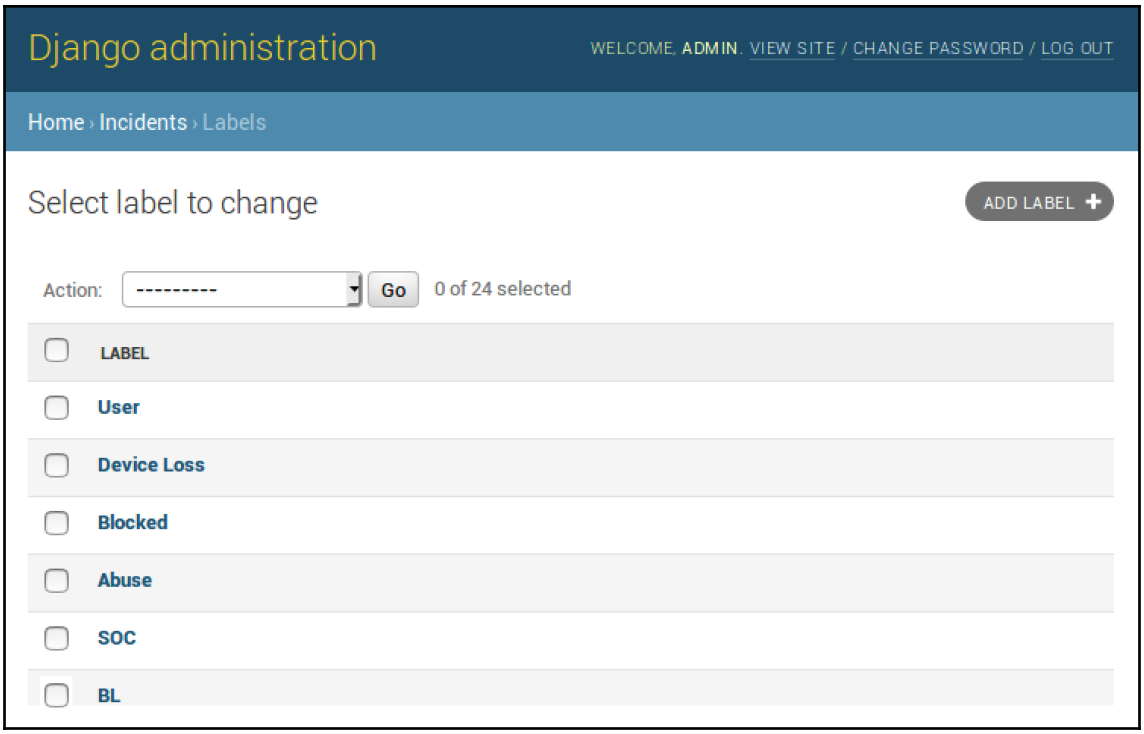
Open Blocked Old Tasks

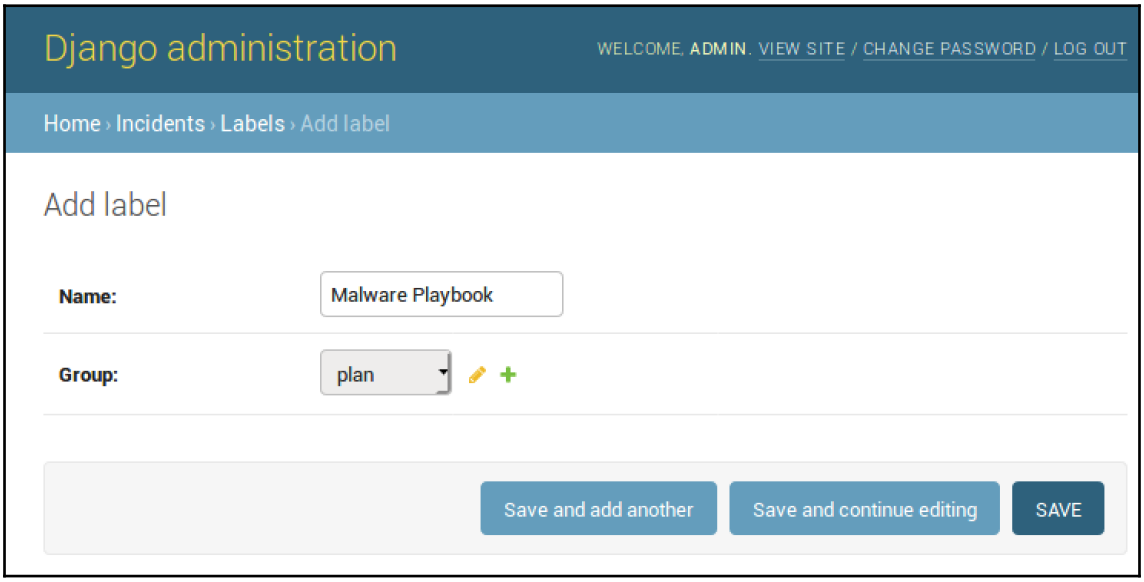
	Task	Incident	Category	Business line	Delete
☐	Execute Device Loss Playbook	IR-2019-124	Stolen data	CERT	🗑

(page 1 of 1)


Django administration
Site administration
AUTH TOKEN
Tokens
Add
Change
AUTHENTICATION AND AUTHORIZATION
Groups
Add
Change
Users
Add
Change
FIR_ALERTING
Category templates
Add
Change
Recipient templates
Add
Change
FIR_ARTIFACTS
Artifact blacklist items
Add
Change
Artifacts
Add
Change
Files
Add
Change
FIR_NUGGETS
Nuggets
Add
Change

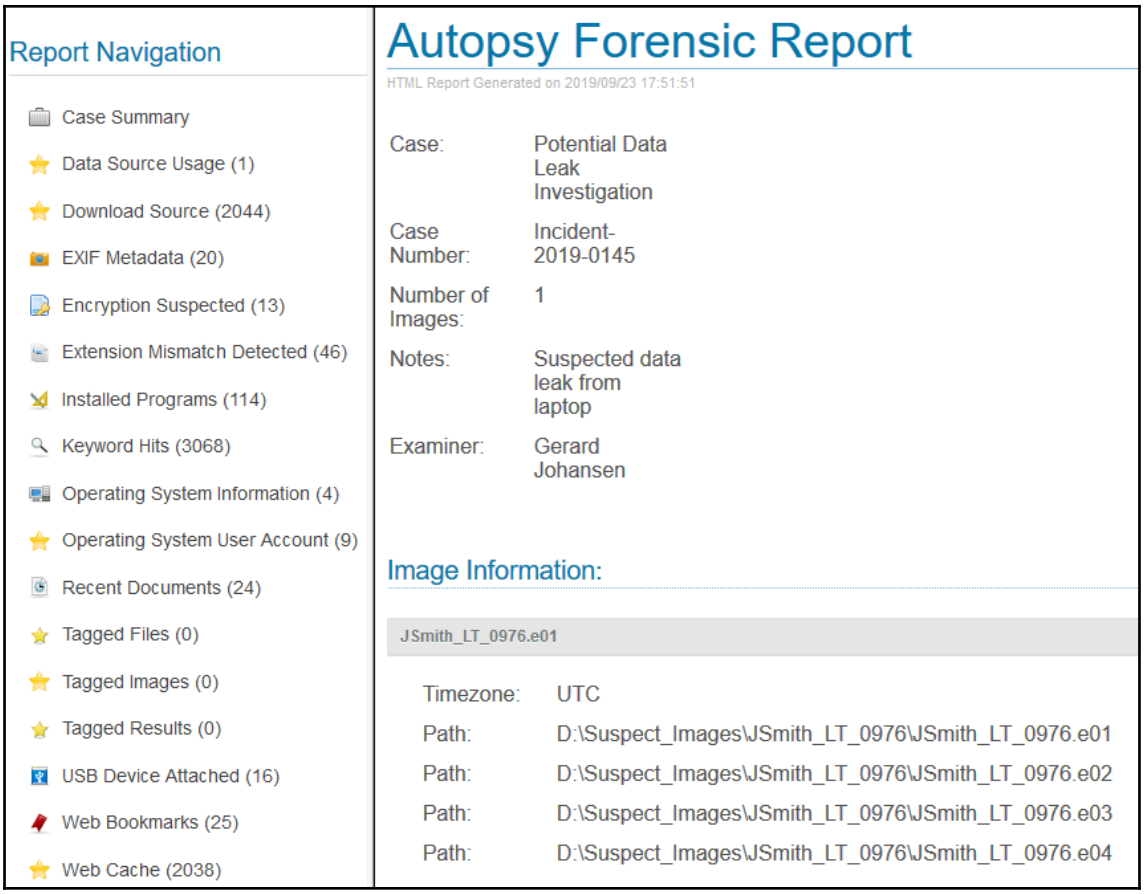

INCIDENTS
Attributes
Add
Change
Bale categories
Add
Change
Business lines
Add
Change
Comments
Add
Change
Incident categories
Add
Change
Incident templates
Add
Change
Incidents
Add
Change
Label groups
Add
Change
Labels
Add
Change
Logs
Add
Change
Profiles
Add
Change
Valid attributes
Add
Change


Django administration
WELCOME, ADMIN. VIEW SITE / CHANGE PASSWORD / LOG OUT
Home › Incidents › Labels
Select label to change
ADD LABEL +
Action: --------- Go 0 of 24 selected
LABEL
User
Device Loss
Blocked
Abuse
SOC
BL


Django administration
WELCOME, ADMIN. VIEW SITE / CHANGE PASSWORD / LOG OUT
Home › Incidents › Labels › Add label
Add label
Name: Malware Playbook
Group: plan
Save and add another
Save and continue editing
SAVE

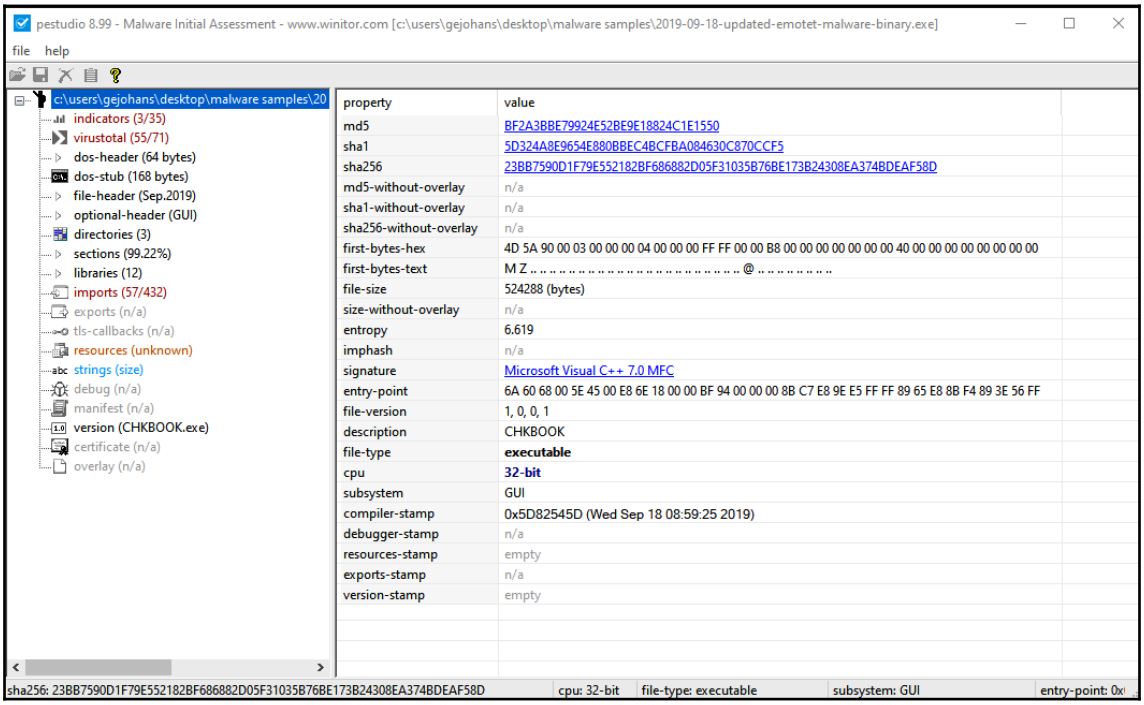

Incident details
Actor
Plan
CERT

Major incident
2
5
6
Device Loss Playbook
Malware Playbook


Report Navigation
Case Summary
Data Source Usage (1)
Download Source (2044)
EXIF Metadata (20)
Encryption Suspected (13)
Extension Mismatch Detected (46)
Installed Programs (114)
Keyword Hits (3068)
Operating System Information (4)
Operating System User Account (9)
Recent Documents (24)
Tagged Files (0)
Tagged Images (0)
Tagged Results (0)
USB Device Attached (16)
Web Bookmarks (25)
Web Cache (2038)
Autopsy Forensic Report
HTML Report Generated on 2019/09/23 17:51:51
Case: Potential Data Leak Investigation
Case Number: Incident-2019-0145
Number of Images: 1
Notes: Suspected data leak from laptop
Examiner: Gerard Johansen
Image Information:
JSmith_LT_0976.e01
Timezone: UTC
Path: D:\Suspect_Images\JSmith_LT_0976\JSmith_LT_0976.e01
Path: D:\Suspect_Images\JSmith_LT_0976\JSmith_LT_0976.e02
Path: D:\Suspect_Images\JSmith_LT_0976\JSmith_LT_0976.e03
Path: D:\Suspect_Images\JSmith_LT_0976\JSmith_LT_0976.e04

Chapter 12: Malware Analysis for Incident Response

```
2019-09-04-Windows-registry-updates-caused-by-Ursnif.txt: OK
2019-09-04-Word-doc-from-password-protected-zip-archive.doc: Doc.Malware.Sagent-7159046-0 FOUND
```



1430	The file references string(s) tagged as blacklist	count: 85	1
1120	The file is scored by virustotal	score: 55/71	1
1266	The file imports symbol(s) tagged as blacklist	count: 57	1

name (432)	group (14)	MITRE-Technique (5)	type (1)	anonymous (6)	blacklist (57)
GetCapture	windowing	-	implicit	-	x
GetClassLongA	windowing	-	implicit	-	x
GetForegroundWindow	windowing	-	implicit	-	x
SetForegroundWindow	windowing	-	implicit	-	x
SetWindowLongA	windowing	-	implicit	-	x
GetDesktopWindow	windowing	-	implicit	-	x
GetTimeZoneInformation	system-information	-	implicit	-	x
GetVolumeInformationA	storage	-	implicit	-	x
WinHelpA	shell	-	implicit	-	x
EnumResourceLanguagesA	resource	-	implicit	-	x
LockResource	resource	-	implicit	-	x
WritePrivateProfileStringA	registry	-	implicit	-	x
RegDeleteValueA	registry	T1112	implicit	-	x
RegSetValueA	registry	T1112	implicit	-	x
RegDeleteKeyA	registry	T1112	implicit	-	x
RegEnumKeyA	registry	T1012	implicit	-	x
RegCreateKeyA	registry	-	implicit	-	x
RegSetValueExA	registry	T1112	implicit	-	x
VirtualProtect	memory	-	implicit	-	x
GetKeyState	keyboard-and-mouse	-	implicit	-	x
SetWindowsHookExA	hooking	T1179	implicit	-	x
CallNextHookEx	hooking	T1179	implicit	-	x
UnhookWindowsHookEx	hooking	T1179	implicit	-	x
GetShortPathNameA	file	-	implicit	-	x
FindFirstFileA	file	-	implicit	-	x
FindClose	file	-	implicit	-	x
UnlockFile	file	-	implicit	-	x

unicode	6	0x000694A5	x	x	Port :
unicode	64	0x0006BE13	x	x	No error occurred.-An unknown error occurred while accessing %1.
ascii	13	0x0005F6AD	x	-	SetWindowLong
ascii	19	0x0005F7E8	x	-	SetForegroundWindow
ascii	19	0x0005F96C	x	-	GetForegroundWindow
ascii	12	0x0005FA11	x	-	GetClassLong
ascii	10	0x0005FA58	x	-	GetCapture
ascii	16	0x0005FC84	x	-	GetDesktopWindow
ascii	18	0x0005138D	x	-	EnumDisplayDevices
ascii	19	0x000513B0	x	-	EnumDisplayMonitors
ascii	22	0x0005F22C	x	-	GetTimeZoneInformation
ascii	20	0x0005EE8D	x	-	GetVolumeInformation
ascii	7	0x0005FA67	x	-	WinHelp
ascii	12	0x0005041C	x	-	LockResource
ascii	12	0x0005EB4A	x	-	LockResource
ascii	21	0x0005ED65	x	-	EnumResourceLanguages
ascii	25	0x0005EF43	x	-	WritePrivateProfileString
ascii	11	0x00060495	x	-	RegSetValue
ascii	12	0x000604FF	x	-	RegDeleteKey
ascii	10	0x0006050F	x	-	RegEnumKey
ascii	13	0x00060541	x	-	RegSetValueEx

```
remnux@remnux:~/MalwareSamples$ pescanner 2019-09-04-initial-Ursnif-binary.exe
########################################################################################################
[0] File: 2019-09-04-initial-Ursnif-binary.exe
########################################################################################################

Meta-data
========================================================================================================
Size            : 300032 bytes
Type            : PE32 executable (GUI) Intel 80386, for MS Windows
Architecture    : 32 Bits binary
MD5             : b2490c2f4f8d22ddb34b4cbecd3c69b3
SHA1            : 59154cb6a203e00fbe0431281b2bb33e1b00061a
ssdeep          : 6144:TJ8mth3sLtIAqj3FVzpe5ZFzbLXLe86HGrHnQ2Jx:uWJsIY5ZFzPy86HOHH
imphash         : 0e1c43d49561655b09b5f1bc6792fa38
Date            : 0x4AA0FBD5 [Fri Sep  4 11:36:53 2009 UTC]
Language        : ENGLISH
CRC:    (Claimed) : 0x0, (Actual): 0x54247 [SUSPICIOUS]
Entry Point     : 0x4207ae .text 0/5
```

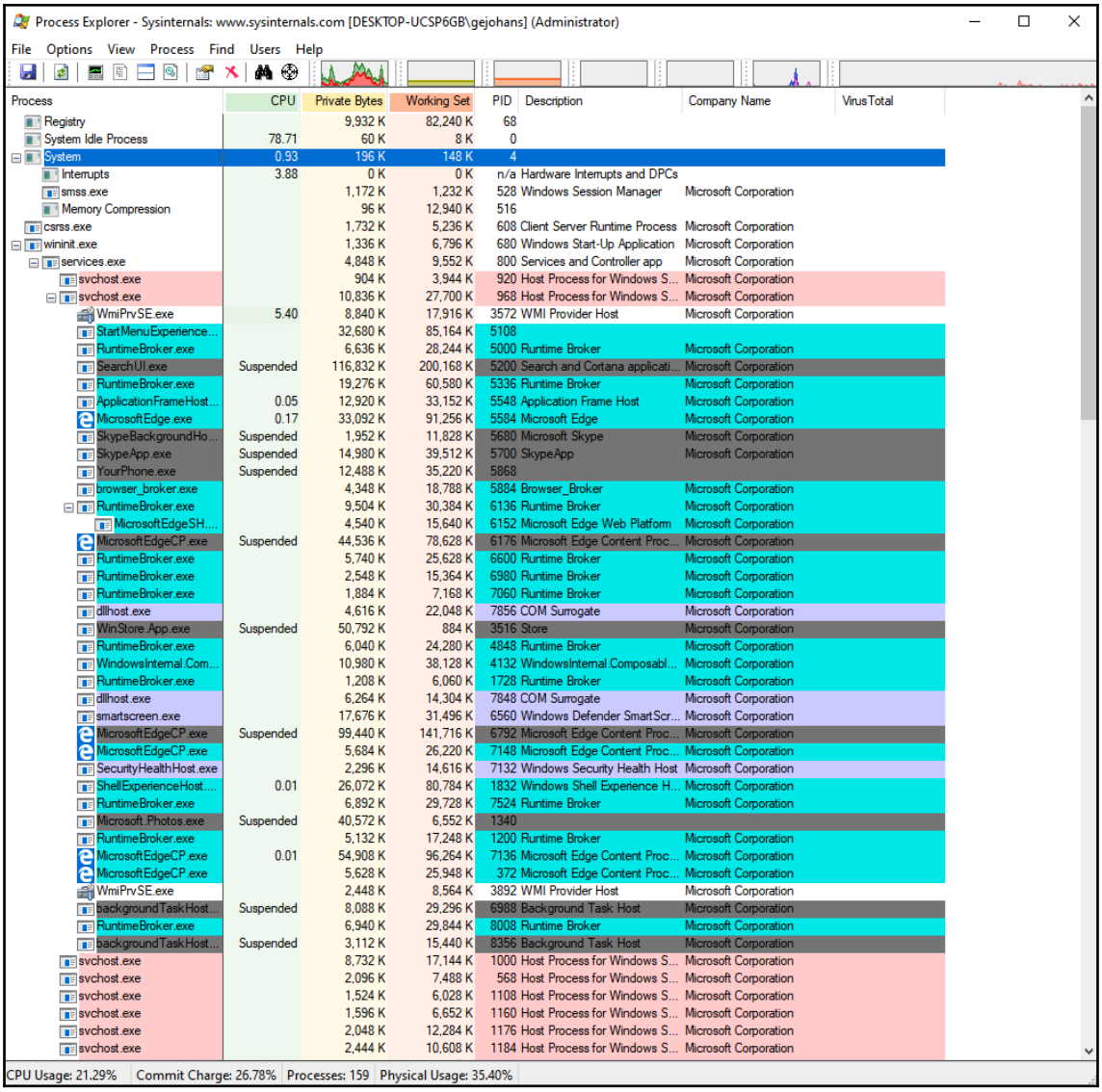
```
Offset | Instructions
----------------------------------------
0       call 0x423e7c
5       jmp 0x420631
10      push byte 0xc
12      push dword 0x43b3e0
17      call 0x4210f0
22      and dword [ebp-0x1c],0x0
26      mov esi,[ebp+0x8]
29      cmp esi,[0x44e2d0]
35      ja 0x4207f5
37      push byte 0x4
39      call 0x42408e
44      pop ecx
45      and dword [ebp-0x4],0x0
49      push esi
50      call 0x4248a0
55      pop ecx
56      mov [ebp-0x1c],eax
59      mov dword [ebp-0x4],0xfffffffe
66      call 0x4207fe
71      mov eax,[ebp-0x1c]
74      call 0x421135
79      ret
80      push byte 0x4
82      call 0x423fb4
87      pop ecx
88      ret
89      mov edi,edi
91      push ebp
92      mov ebp,esp
94      push esi
95      mov esi,[ebp+0x8]
98      cmp esi,0x0
```

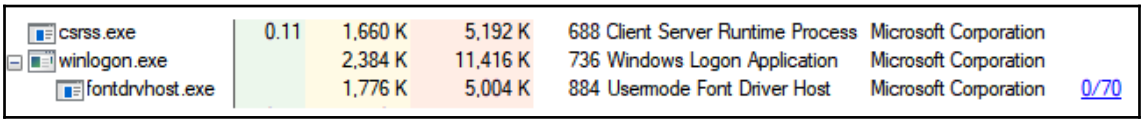
```
Sections
=================================================================================================
Name       VirtAddr     VirtSize     RawSize    MD5                                Entropy
-------------------------------------------------------------------------------------------------
.text      0x1000       0x2e9c7      0x2ea00    ea80d5c83da498d1b76c537bdfc80370 6.717635
.rdata     0x30000      0xdc66       0xde00     0f5ff6da63a54786b653ce46fe4c1830 5.805477
.data      0x3e000      0x1041c      0x4c00     a5297d66be916d217b1f5f18812916a5 5.463237
.rsrc      0x4f000      0x530        0x600      15f94e54fda75a4b78243579f4c48870 3.658907
.reloc     0x50000      0x742a       0x7600     8e489f790699d5a7eda31642e180e611 2.852141
```

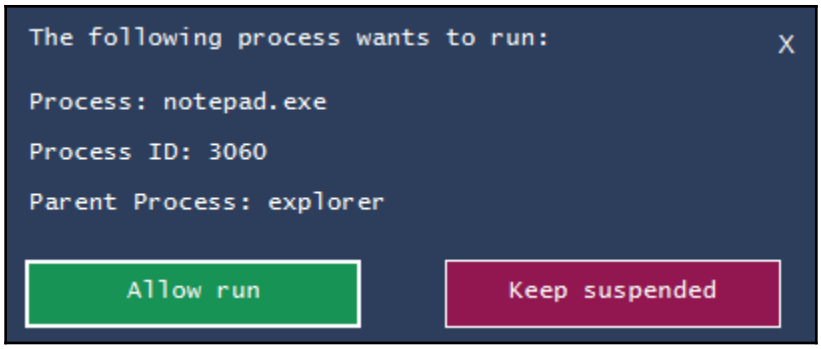
```
Imports
================================================
[1] KERNEL32.dll
[2] USER32.dll
[3] WINSPOOL.DRV
[4] COMCTL32.dll
[5] ole32.dll
[6] OLEAUT32.dll
[7] SHLWAPI.dll
[8] ADVAPI32.dll
[9] CLUSAPI.dll
[10] OLEACC.dll
[11] GDI32.dll
```

```
Suspicious IAT alerts
=====================================================================
[1] CreateDirectoryW
[2] CreateFileA
[3] CreateFileW
[4] FindResourceW
[5] GetCommandLineW
[6] GetModuleFileNameA
[7] GetModuleFileNameW
[8] GetModuleHandleA
[9] GetModuleHandleW
[10] GetProcAddress
[11] GetStartupInfoA
[12] GetStartupInfoW
[13] GetTickCount
```

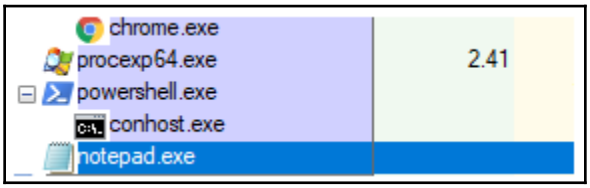
```
/*
   Yara Rule Set
   Author: yarGen Rule Generator
   Date: 2019-10-12
   Identifier: Malware
   Reference: https://github.com/Neo23x0/yarGen
*/

/* Rule Set ----------------------------------------------------------------- */

rule Malware_sample {
   meta:
      description = "Malware - file sample.doc"
      author = "yarGen Rule Generator"
      reference = "https://github.com/Neo23x0/yarGen"
      date = "2019-10-12"
      hash1 = "4e59d5e27d1109b3e2cb46b5dbe8d5c04aa82978177f4d29e3e986b88ff68894"
   strings:
      $x1 = "*\\G{0D452EE1-E08F-101A-852E-02608C4D0BB4}#2.0#0#C:\\WINDOWS\\system32\\FM20.DLL#Mic
      $s2 = "*\\G{00020430-0000-0000-C000-000000000046}#2.0#0#C:\\Windows\\System32\\stdole2.tlb#
      $s3 = "var rXvzpRtxp = function(){return \"\" + \"R\" + \"u\" + \"\\x6e\";};var pzLDkTdpjP
      $s4 = "*\\G{1ABB45AB-A1DB-4268-86A8-DAA4B48BD521}#2.0#0#C:\\Users\\Willy\\AppData\\Local\\T
      $s5 = "TdpjP(\"Ws\" + \"cript.Shell\")[[\"nbHqBJBJXBKzPPXJjLBtz\", rXvzpRtxp()][1]](\"C:\\\
      $s6 = "*\\G{2DF8D04C-5BFA-101B-BDE5-00AA0044DE52}#2.8#0#C:\\Program Files\\Common Files\\Mi
      $s7 = "22222222222222222222222222222222222222222222222222" ascii /* hex encoded string '""
      $s8 = "\\MSO.DLL" fullword ascii
      $s9 = "*\\G{000204EF-0000-0000-C000-000000000046}#4.2#9#C:\\PROGRA~1\\COMMON~1\\MICROS~1\\V
      $s10 = "OAC4AZABlAGYAbABBAFQAZQBgAFMAVABSAEUAQQBtACgAWwBzAHkAUwB0AGUAbQAuAEkATwAuAE0ARQBNAE
```

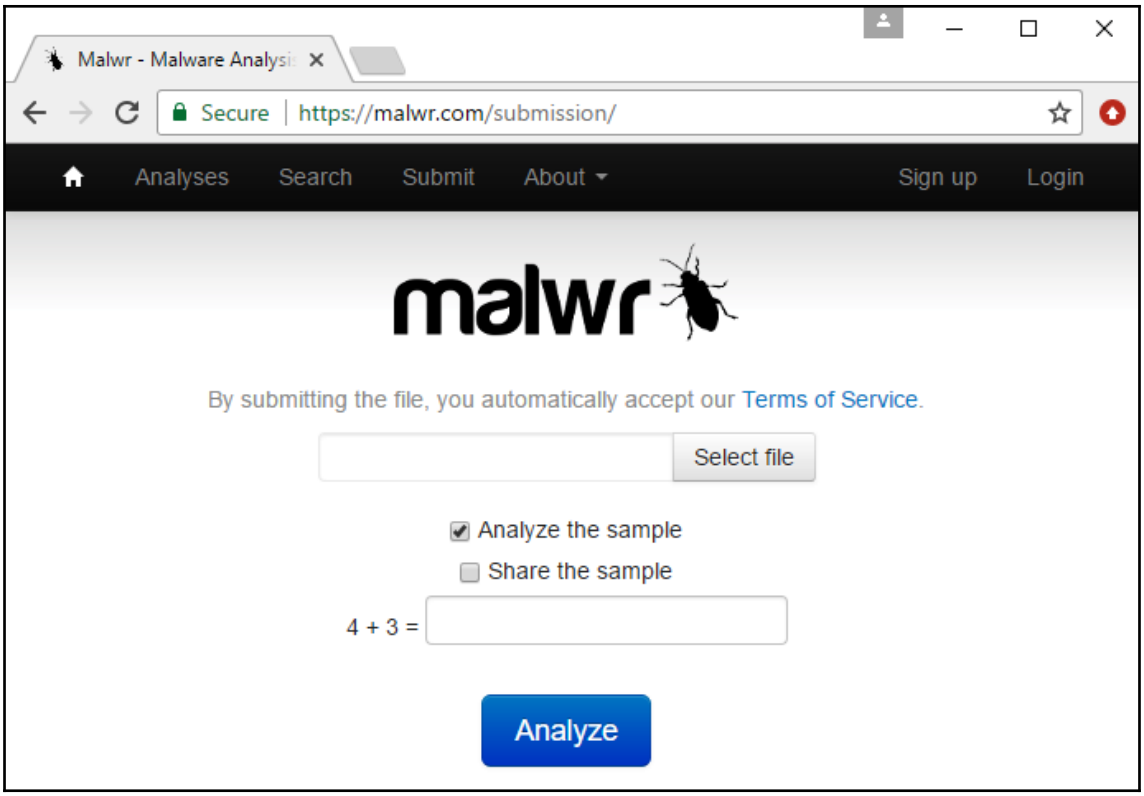

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-UCSP6GB\gejohans] (Administrator)
File Options View Process Find Users Help
Process CPU Private Bytes Working Set PID Description Company Name VirusTotal
Registry 9,932 K 82,240 K 68
System Idle Process 78.71 60 K 8 K 0
System 0.93 196 K 148 K 4
Interrupts 3.88 0 K 0 K n/a Hardware Interrupts and DPCs
smss.exe 1,172 K 1,232 K 528 Windows Session Manager Microsoft Corporation
Memory Compression 96 K 12,940 K 516
csrss.exe 1,732 K 5,236 K 608 Client Server Runtime Process Microsoft Corporation
wininit.exe 1,336 K 6,796 K 680 Windows Start-Up Application Microsoft Corporation
services.exe 4,848 K 9,552 K 800 Services and Controller app Microsoft Corporation
svchost.exe 904 K 3,944 K 920 Host Process for Windows S... Microsoft Corporation
svchost.exe 10,836 K 27,700 K 968 Host Process for Windows S... Microsoft Corporation
WmiPrvSE.exe 5.40 8,840 K 17,916 K 3572 WMI Provider Host Microsoft Corporation
StartMenuExperience... 32,680 K 85,164 K 5108
RuntimeBroker.exe 6,636 K 28,244 K 5000 Runtime Broker Microsoft Corporation
SearchUI.exe Suspended 116,832 K 200,168 K 5200 Search and Cortana applicati... Microsoft Corporation
RuntimeBroker.exe 19,276 K 60,580 K 5336 Runtime Broker Microsoft Corporation
ApplicationFrameHost... 0.05 12,920 K 33,152 K 5548 Application Frame Host Microsoft Corporation
MicrosoftEdge.exe 0.17 33,092 K 91,256 K 5584 Microsoft Edge Microsoft Corporation
SkypeBackgroundHo... Suspended 1,952 K 11,828 K 5680 Microsoft Skype Microsoft Corporation
SkypeApp.exe Suspended 14,980 K 39,512 K 5700 SkypeApp Microsoft Corporation
YourPhone.exe Suspended 12,488 K 35,220 K 5868
browser_broker.exe 4,348 K 18,788 K 5884 Browser_Broker Microsoft Corporation
RuntimeBroker.exe 9,504 K 30,384 K 6136 Runtime Broker Microsoft Corporation
MicrosoftEdgeSH.... 4,540 K 15,640 K 6152 Microsoft Edge Web Platform Microsoft Corporation
MicrosoftEdgeCP.exe Suspended 44,536 K 78,628 K 6176 Microsoft Edge Content Proc... Microsoft Corporation
RuntimeBroker.exe 5,740 K 25,628 K 6600 Runtime Broker Microsoft Corporation
RuntimeBroker.exe 2,548 K 15,364 K 6980 Runtime Broker Microsoft Corporation
RuntimeBroker.exe 1,884 K 7,168 K 7060 Runtime Broker Microsoft Corporation
dllhost.exe 4,616 K 22,048 K 7856 COM Surrogate Microsoft Corporation
WinStore.App.exe Suspended 50,792 K 884 K 3516 Store Microsoft Corporation
RuntimeBroker.exe 6,040 K 24,280 K 4848 Runtime Broker Microsoft Corporation
WindowsInternal.Com... 10,980 K 38,128 K 4132 WindowsInternal.Composabl... Microsoft Corporation
RuntimeBroker.exe 1,208 K 6,060 K 1728 Runtime Broker Microsoft Corporation
dllhost.exe 6,264 K 14,304 K 7848 COM Surrogate Microsoft Corporation
smartscreen.exe 17,676 K 31,496 K 6560 Windows Defender SmartScr... Microsoft Corporation
MicrosoftEdgeCP.exe Suspended 99,440 K 141,716 K 6792 Microsoft Edge Content Proc... Microsoft Corporation
MicrosoftEdgeCP.exe 5,684 K 26,220 K 7148 Microsoft Edge Content Proc... Microsoft Corporation
SecurityHealthHost.exe 2,296 K 14,616 K 7132 Windows Security Health Host Microsoft Corporation
ShellExperienceHost.... 0.01 26,072 K 80,784 K 1832 Windows Shell Experience H... Microsoft Corporation
RuntimeBroker.exe 6,892 K 29,728 K 7524 Runtime Broker Microsoft Corporation
Microsoft.Photos.exe Suspended 40,572 K 6,552 K 1340
RuntimeBroker.exe 5,132 K 17,248 K 1200 Runtime Broker Microsoft Corporation
MicrosoftEdgeCP.exe 0.01 54,908 K 96,264 K 7136 Microsoft Edge Content Proc... Microsoft Corporation
MicrosoftEdgeCP.exe 5,628 K 25,948 K 372 Microsoft Edge Content Proc... Microsoft Corporation
WmiPrvSE.exe 2,448 K 8,564 K 3892 WMI Provider Host Microsoft Corporation
backgroundTaskHost... Suspended 8,088 K 29,296 K 6988 Background Task Host Microsoft Corporation
RuntimeBroker.exe 6,940 K 29,844 K 8008 Runtime Broker Microsoft Corporation
backgroundTaskHost... Suspended 3,112 K 15,440 K 8356 Background Task Host Microsoft Corporation
svchost.exe 8,732 K 17,144 K 1000 Host Process for Windows S... Microsoft Corporation
svchost.exe 2,096 K 7,488 K 568 Host Process for Windows S... Microsoft Corporation
svchost.exe 1,524 K 6,028 K 1108 Host Process for Windows S... Microsoft Corporation
svchost.exe 1,596 K 6,652 K 1160 Host Process for Windows S... Microsoft Corporation
svchost.exe 2,048 K 12,284 K 1176 Host Process for Windows S... Microsoft Corporation
svchost.exe 2,444 K 10,608 K 1184 Host Process for Windows S... Microsoft Corporation
CPU Usage: 21.29% Commit Charge: 26.78% Processes: 159 Physical Usage: 35.40%

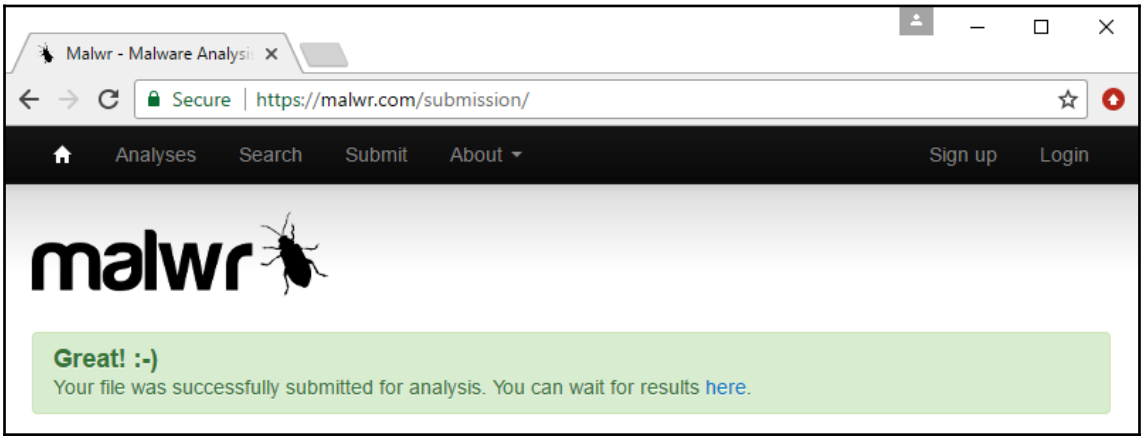

csrss.exe 0.11 1,660 K 5,192 K 688 Client Server Runtime Process Microsoft Corporation
winlogon.exe 2,384 K 11,416 K 736 Windows Logon Application Microsoft Corporation
fontdrvhost.exe 1,776 K 5,004 K 884 Usermode Font Driver Host Microsoft Corporation 0/70


The following process wants to run:
X
Process: notepad.exe
Process ID: 3060
Parent Process: explorer
Allow run
Keep suspended

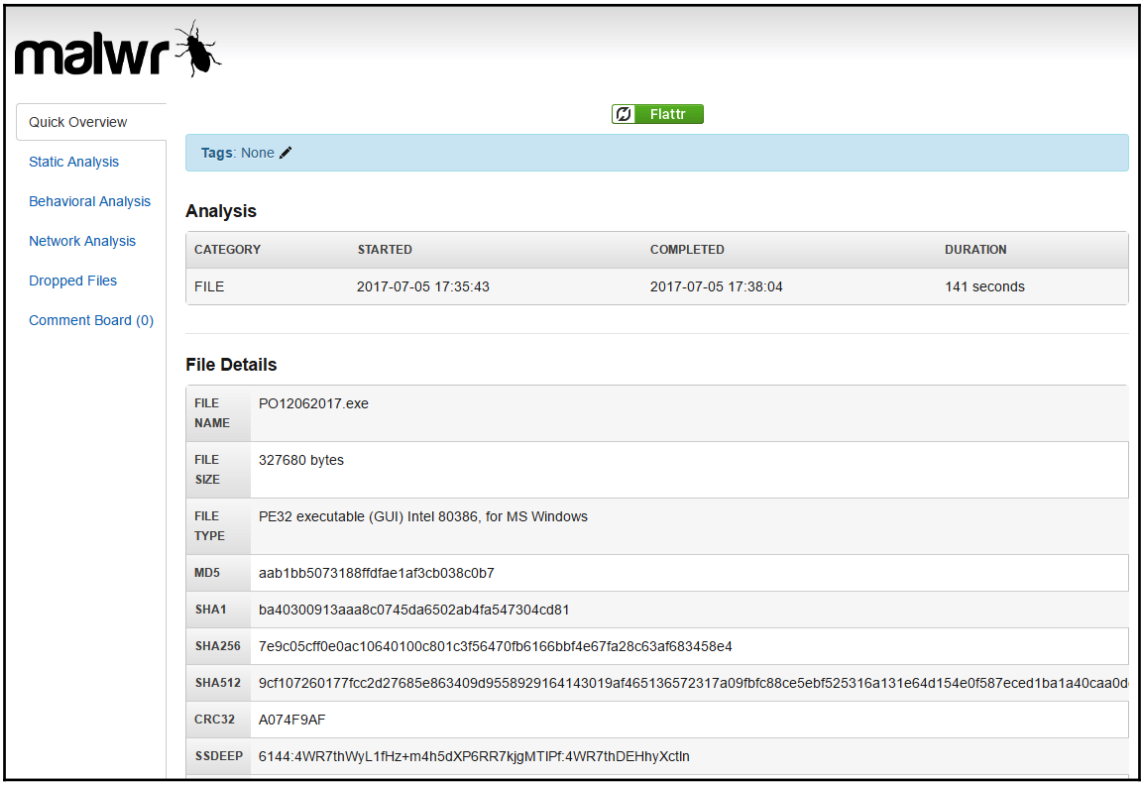

notepad.exe
Suspended
rundll32.exe
Suspended


chrome.exe
procexp64.exe
2.41
powershell.exe
conhost.exe
notepad.exe


Malwr - Malware Analysi
Secure | https://malwr.com/submission/
Analyses
Search
Submit
About
Sign up
Login
malwr
By submitting the file, you automatically accept our Terms of Service.
Select file
Analyze the sample
Share the sample
4 + 3 =
Analyze


Malwr - Malware Analysi
Secure | https://malwr.com/submission/
Analyses
Search
Submit
About
Sign up
Login
malwr
Great! :-)
Your file was successfully submitted for analysis. You can wait for results here.

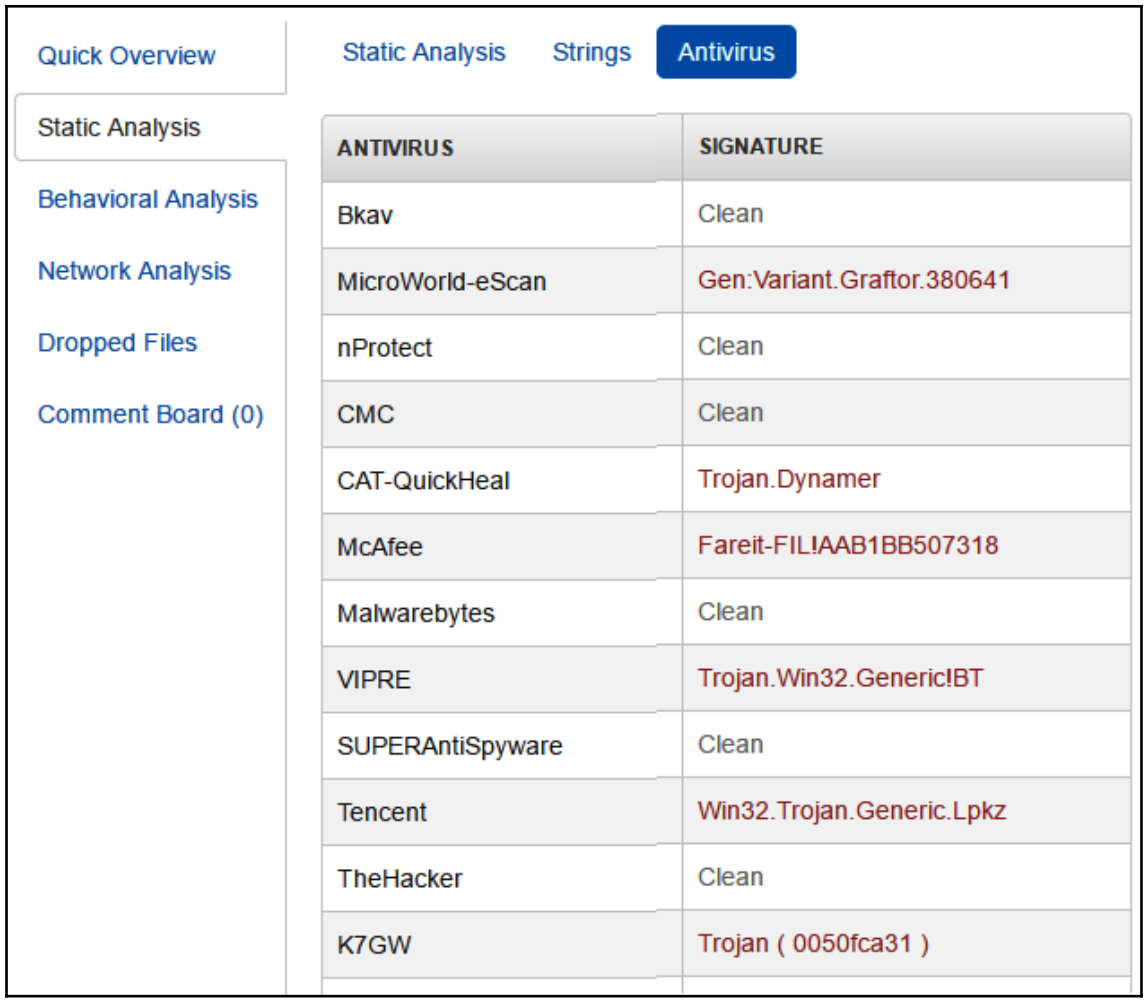

Malwr - Malware Analysi
Secure | https://malwr.com/submission/status/OTdmN2NmMzFlNThhNGNkZWFhODkwZmMzNmRmN2YxYTg/
Analyses
Search
Submit
About
Sign up
Login
malwr
Hang on...
The analysis is still pending or under processing. This page will refresh every 30 seconds.


malwr
Quick Overview
Static Analysis
Behavioral Analysis
Network Analysis
Dropped Files
Comment Board (0)
Flattr
Tags: None
Analysis
CATEGORY
STARTED
COMPLETED
DURATION
FILE
2017-07-05 17:35:43
2017-07-05 17:38:04
141 seconds
File Details
FILE NAME
PO12062017.exe
FILE SIZE
327680 bytes
FILE TYPE
PE32 executable (GUI) Intel 80386, for MS Windows
MD5
aab1bb5073188ffdfae1af3cb038c0b7
SHA1
ba40300913aaa8c0745da6502ab4fa547304cd81
SHA256
7e9c05cff0e0ac10640100c801c3f56470fb6166bbf4e67fa28c63af683458e4
SHA512
9cf107260177fcc2d27685e863409d9558929164143019af465136572317a09fbfc88ce5ebf525316a131e64d154e0f587eced1ba1a40caa0d
CRC32
A074F9AF
SSDEEP
6144:4WR7thWyL1fHz+m4h5dXP6RR7kjgMTlPf:4WR7thDEHhyXctln

Imports

Library MSVBVM60.DLL:

- 0x401000 __vbaStrI2
- 0x401004 _CIcos
- 0x401008 _adj_fptan
- 0x40100c __vbaVarMove
- 0x401010 __vbaFreeVar
- 0x401014 None
- 0x401018 __vbaFreeVarList
- 0x40101c None
- 0x401020 __vbaEnd
- 0x401024 _adj_fdiv_m64
- 0x401028 _adj_fprem1
- 0x40102c __vbaStrCat
- 0x401030 __vbaSetSystemError
- 0x401034 __vbaHresultCheckObj
- 0x401038 __vbaLenBstrB
- 0x40103c _adj_fdiv_m32
- 0x401040 __vbaExitProc
- 0x401044 None

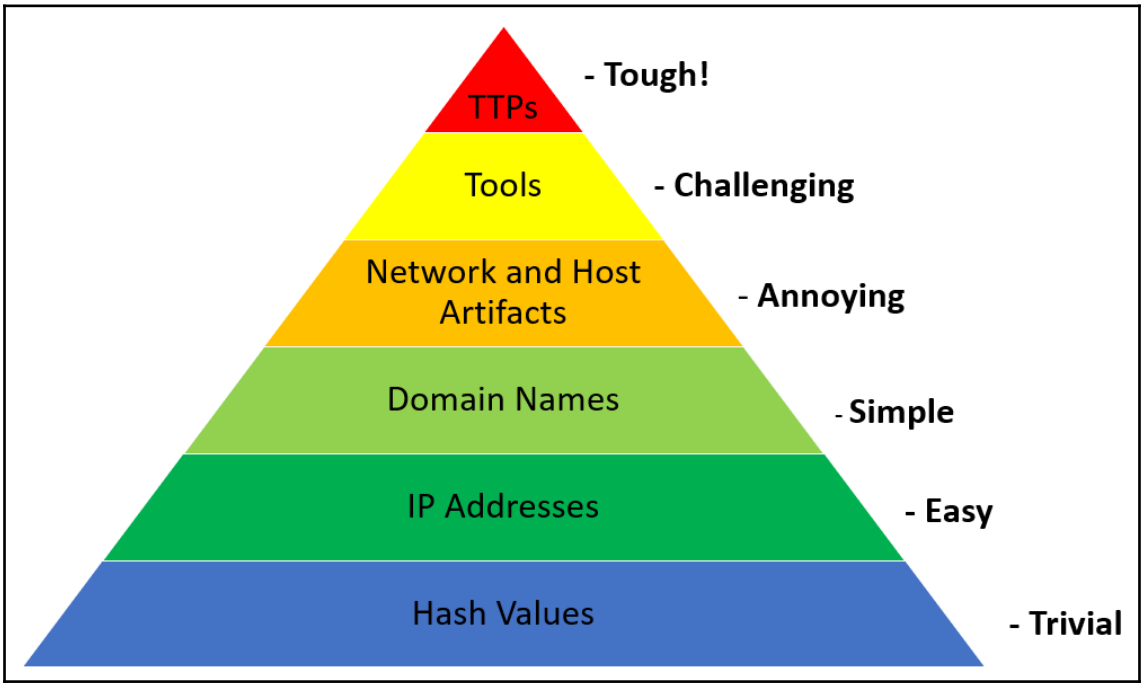

Quick Overview
Static Analysis
Behavioral Analysis
Network Analysis
Dropped Files
Comment Board (0)
Static Analysis
Strings
Antivirus
ANTIVIRUS
SIGNATURE
Bkav
Clean
MicroWorld-eScan
Gen:Variant.Graftor.380641
nProtect
Clean
CMC
Clean
CAT-QuickHeal
Trojan.Dynamer
McAfee
Fareit-FIL!AAB1BB507318
Malwarebytes
Clean
VIPRE
Trojan.Win32.Generic!BT
SUPERAntiSpyware
Clean
Tencent
Win32.Trojan.Generic.Lpkz
TheHacker
Clean
K7GW
Trojan (0050fca31)

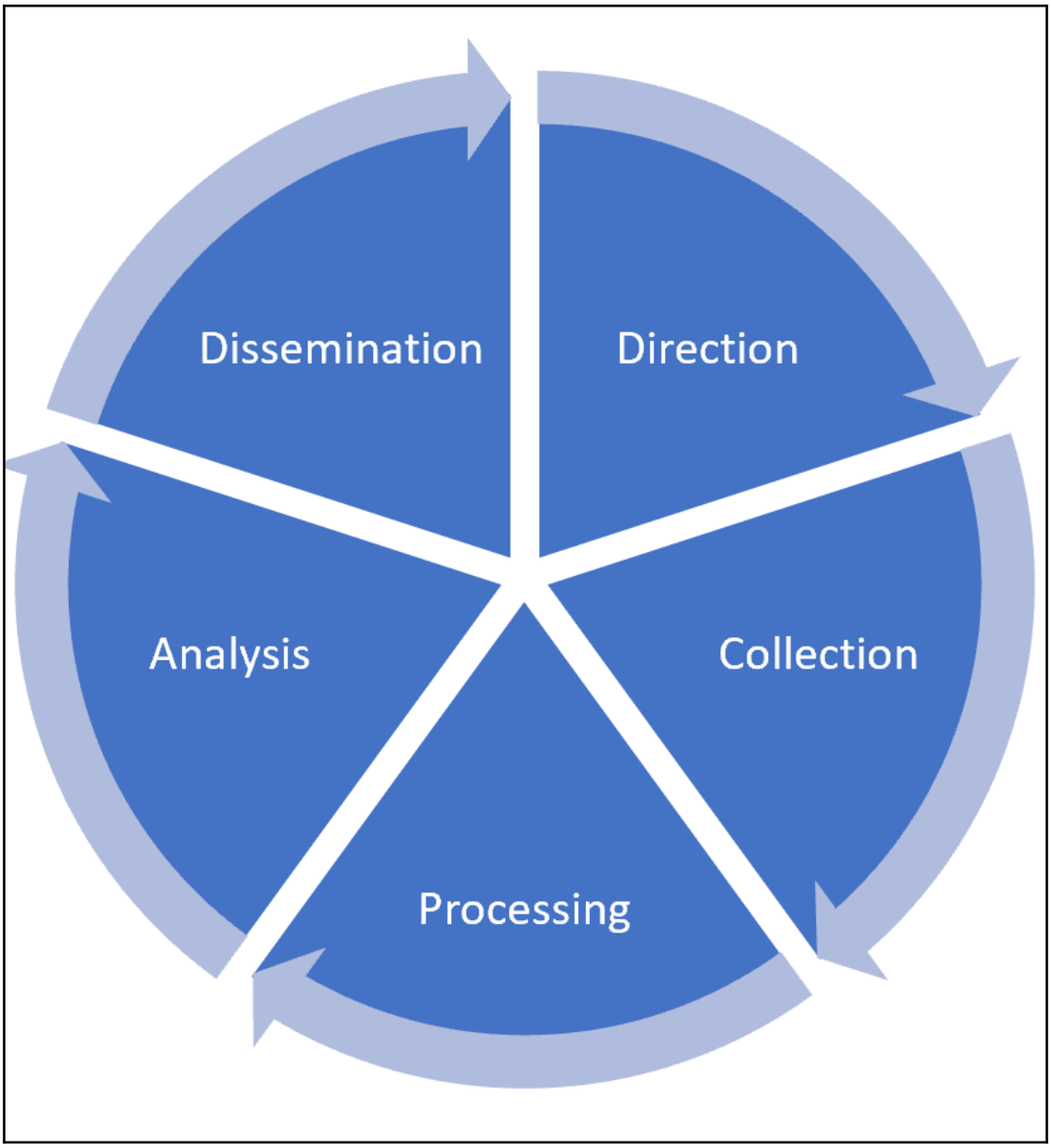

Analyses
Search
Submit
About
irproactive
Network Analysis
Dropped Files
Comment Board (0)
0
50
100
150
200
250
300
350
400
450
PO12062017.exe
X-axis by: event
Y-axis by: category
PO12062017.exe 788
PO12062017.exe
PO12062017.exe, PID: 788, Parent PID: 2016
1
2
3
...
5
network
filesystem
registry
process
services
synchronization
TIME
API
ARGUMENTS
STATUS
RETURN
REPEATED
2017-07-05 08:35:45,143
LdrGetDllHandle
ModuleHandle: 0x00000000
FileName: C:\WINDOWS\system32\rpcss.dll
failed
0xc0000135
1 time

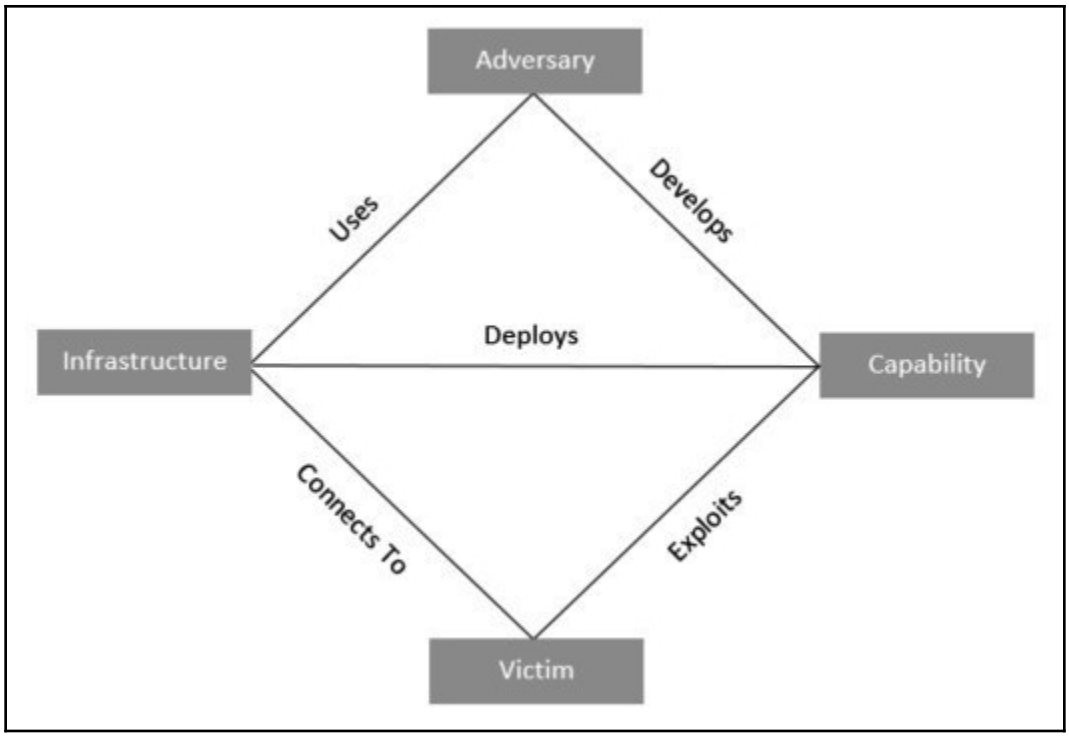
FILE NAME	**filename.vbs**
FILE SIZE	384 bytes
FILE TYPE	ASCII text, with CRLF line terminators
MD5	899dbb13af252b6cd89a6de23048cf8c
SHA1	857745ec21332c7e3a2f6f44af1113ecd9ec3f6a
SHA256	bf01560f94fd75d02a21b8cd133cab3d6e181f7eb4d41b6d415b65fe63665e96
CRC32	DA5FB4F1
SSDEEP	3:j+qAHmFEm86oQ/FERMQsNC2xA+KdlH1MARm5iRMQbm34MkWJJFHrLL:j+q9Nht6G9KdEARm5Mm34M9
YARA	• embedded_win_api - A non-Windows executable contains win32 API functions names

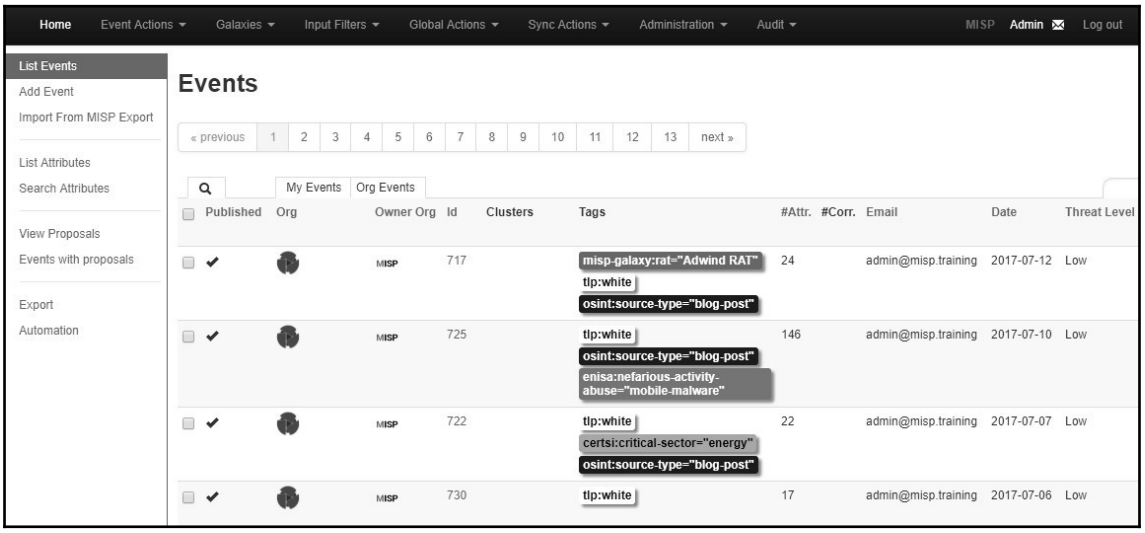
FILE NAME	**filename.exe**
FILE SIZE	327680 bytes
FILE TYPE	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	1f54f93c28df730aa1c13d0090c7eeb5
SHA1	c152e04d928a5397943d9285af8373813affed25
SHA256	75d49db3c12349a5be3da567ed9ca169e05d0ced8e6a15846bf9b884ed954f0c
CRC32	9E4A0D9D
SSDEEP	6144:9WR7thWyL1fHz+m4h5dXP6RR7kjgMTIPv:9WR7thDEHhyXctlX
YARA	None matched

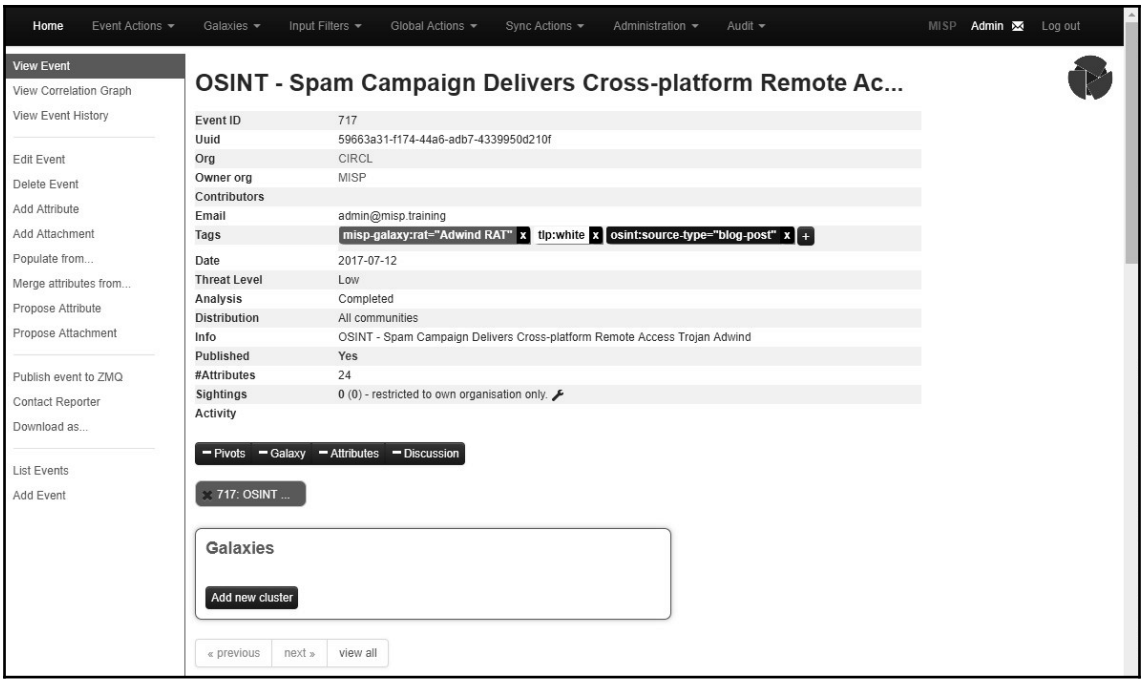
Chapter 13: Leveraging Threat Intelligence

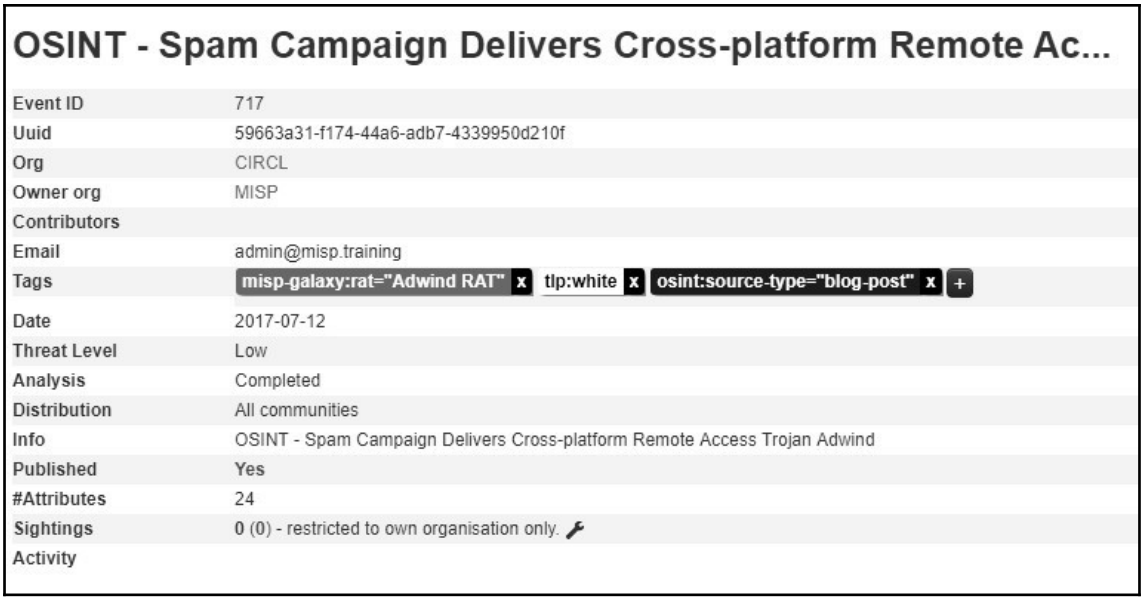



Dissemination
Direction
Analysis
Collection
Processing

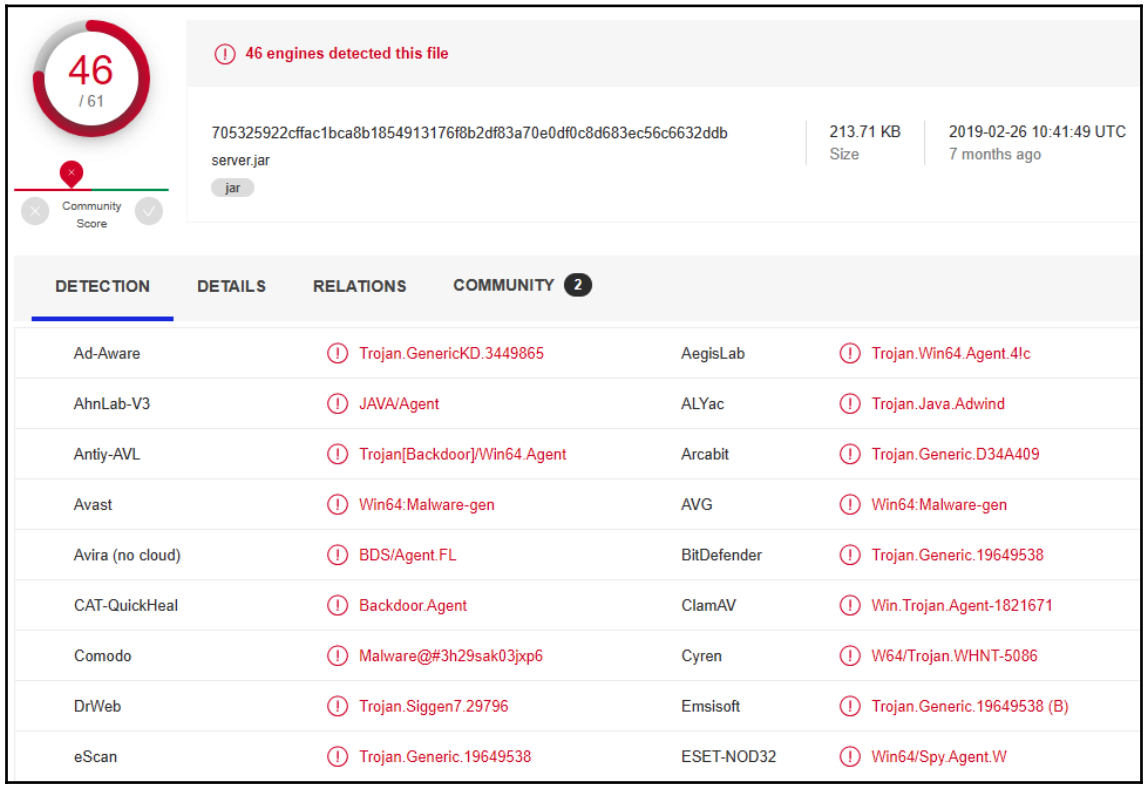

Adversary
Uses
Develops
Infrastructure
Deploys
Capability
Connects To
Exploits
Victim


Home
Event Actions
Galaxies
Input Filters
Global Actions
Sync Actions
Administration
Audit
MISP
Admin
Log out
List Events
Add Event
Import From MISP Export
List Attributes
Search Attributes
View Proposals
Events with proposals
Export
Automation
Events
« previous
1
2
3
4
5
6
7
8
9
10
11
12
13
next »
My Events
Org Events
Published
Org
Owner Org
Id
Clusters
Tags
#Attr.
#Corr.
Email
Date
Threat Level
717
misp-galaxy:rat="Adwind RAT"
tlp:white
osint:source-type="blog-post"
24
admin@misp.training
2017-07-12
Low
725
tlp:white
osint:source-type="blog-post"
enisa:nefarious-activity-abuse="mobile-malware"
146
admin@misp.training
2017-07-10
Low
722
tlp:white
certsi:critical-sector="energy"
osint:source-type="blog-post"
22
admin@misp.training
2017-07-07
Low
730
tlp:white
17
admin@misp.training
2017-07-06
Low


Home
Event Actions
Galaxies
Input Filters
Global Actions
Sync Actions
Administration
Audit
MISP
Admin
Log out
View Event
View Correlation Graph
View Event History
Edit Event
Delete Event
Add Attribute
Add Attachment
Populate from...
Merge attributes from...
Propose Attribute
Propose Attachment
Publish event to ZMQ
Contact Reporter
Download as...
List Events
Add Event
OSINT - Spam Campaign Delivers Cross-platform Remote Ac...
Event ID 717
Uuid 59663a31-f174-44a6-adb7-4339950d210f
Org CIRCL
Owner org MISP
Contributors
Email admin@misp.training
Tags misp-galaxy:rat="Adwind RAT" x tlp:white x osint:source-type="blog-post" x +
Date 2017-07-12
Threat Level Low
Analysis Completed
Distribution All communities
Info OSINT - Spam Campaign Delivers Cross-platform Remote Access Trojan Adwind
Published Yes
#Attributes 24
Sightings 0 (0) - restricted to own organisation only.
Activity
Pivots
Galaxy
Attributes
Discussion
717: OSINT ...
Galaxies
Add new cluster
« previous
next »
view all


OSINT - Spam Campaign Delivers Cross-platform Remote Ac...
Event ID 717
Uuid 59663a31-f174-44a6-adb7-4339950d210f
Org CIRCL
Owner org MISP
Contributors
Email admin@misp.training
Tags misp-galaxy:rat="Adwind RAT" x tlp:white x osint:source-type="blog-post" x +
Date 2017-07-12
Threat Level Low
Analysis Completed
Distribution All communities
Info OSINT - Spam Campaign Delivers Cross-platform Remote Access Trojan Adwind
Published Yes
#Attributes 24
Sightings 0 (0) - restricted to own organisation only.
Activity

2017-07-12	External analysis	link	https://www.virustotal.com/file/705325922cffac1bca8b1854913176f8b2df83a70e0df0c8d683ec56c6632ddb/analysis/1499247775/	+	BKDR64_AGENT.TYUCT - Xchecked via VT: 705325922cffac1bca8b1854913176f8b2df83a70e0df0c8d683ec56c6632ddb
2017-07-12	External analysis	link	https://www.virustotal.com/file/97d585b6aff62fb4e43e7e6a5f816dcd7a14be11a88b109a9ba9e8cd4c456eb9/analysis/1499851519/	+	JAVA_ADWIND.AUJC - Xchecked via VT: 97d585b6aff62fb4e43e7e6a5f816dcd7a14be11a88b109a9ba9e8cd4c456eb9



2017-07-12	Network activity	url	https://nup.pw/Qcaq5e.jar	+	Files and URLs related to Adwind/jRAT
2017-07-12	Network activity	url	http://vacanzaimmobiliare.it/testla/WebPanel/post.php	+	Related C&C servers:
2017-07-12	Network activity	url	http://ccb-ba.adv.br/wp-admin/network/ok/index.php	+	Files and URLs related to Adwind/jRAT
2017-07-12	Network activity	url	https://nup.pw/e2BXtK.exe	+	Files and URLs related to Adwind/jRAT

2017-07-12	Payload delivery	ip-dst|port	174.127.99.234:1033	+	Related C&C servers - Port 1033	☑

☐	2017-07-12	Payload delivery	sha1	9ce4518ebcb5be6d1f0b5477fa00c26860fe9a68	+	JAVA_ADWIND.AUJC - Xchecked via VT: 97d585b6aff62fb4e43e7e6a5f816dcd7a14be11a88b109a9ba9e8cd4c456eb9	☑
☐	2017-07-12	Payload delivery	md5	781fb531354d6f291f1ccab48da6d39f	+	JAVA_ADWIND.AUJC - Xchecked via VT: 97d585b6aff62fb4e43e7e6a5f816dcd7a14be11a88b109a9ba9e8cd4c456eb9	☑
☐	2017-07-12	Payload delivery	sha256	705325922cffac1bca8b1854913176f8b2df83a70e0df0c8d683ec56c6632ddb	+	BKDR64_AGENT.TYUCT	☑

Feeds

Generate feed lookup caches

All Freetext/CSV MISP

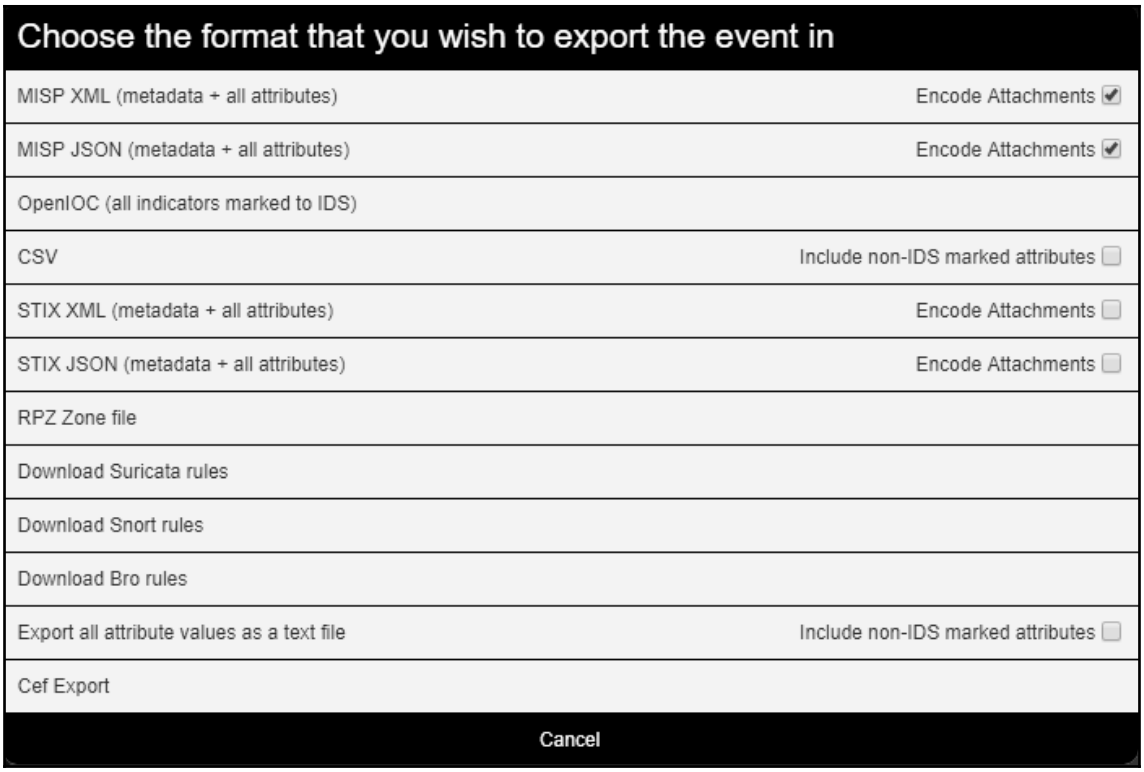
« previous next »

Default feeds | Custom Feeds | All Feeds | Enabled Feeds

Id	Name	Feed Format	Provider	Input	Url	Target	Publish	Delta Merge	Override IDS	Distribution	Tag	Enabled
1	CIRCL OSINT Feed MISP	MISP Feed	CIRCL	network	https://www.circl.lu/doc/misp/feed-osint					All communities		✔
2	The Botvrij.eu Data MISP	MISP Feed	Botvrij.eu	network	http://www.botvrij.eu/data/feed-osint					All communities		✔
3	inThreat OSINT Feed MISP	MISP Feed	inThreat	network	https://feeds.inthreat.com/osint/misp/					Your organisation only	osint:source-type="block-or-filter-list"	✖
4	ZeuS IP blocklist (Standard) MISP	Simple CSV Parsed Feed	zeustracker.abuse.ch	network	https://zeustracker.abuse.ch/blocklist.php?download=ipblocklist	New fixed event	✖	✔	✔	Your organisation only	osint:source-type="block-or-filter-list"	✖
5	ZeuS compromised URL blocklist MISP	Simple CSV Parsed Feed	zeustracker.abuse.ch	network	https://zeustracker.abuse.ch/blocklist.php?download=compromised	Fixed event 733	✖	✔	✔	Your organisation only	osint:source-type="block-or-filter-list"	✔
6	blockrules of rules.emergingthreats.net MISP	Simple CSV Parsed Feed	rules.emergingthreats.net	network	http://rules.emergingthreats.net/blockrules/compromised-ips.txt	New fixed event	✖	✔	✔	Your organisation only	osint:source-type="block-or-filter-list"	✖

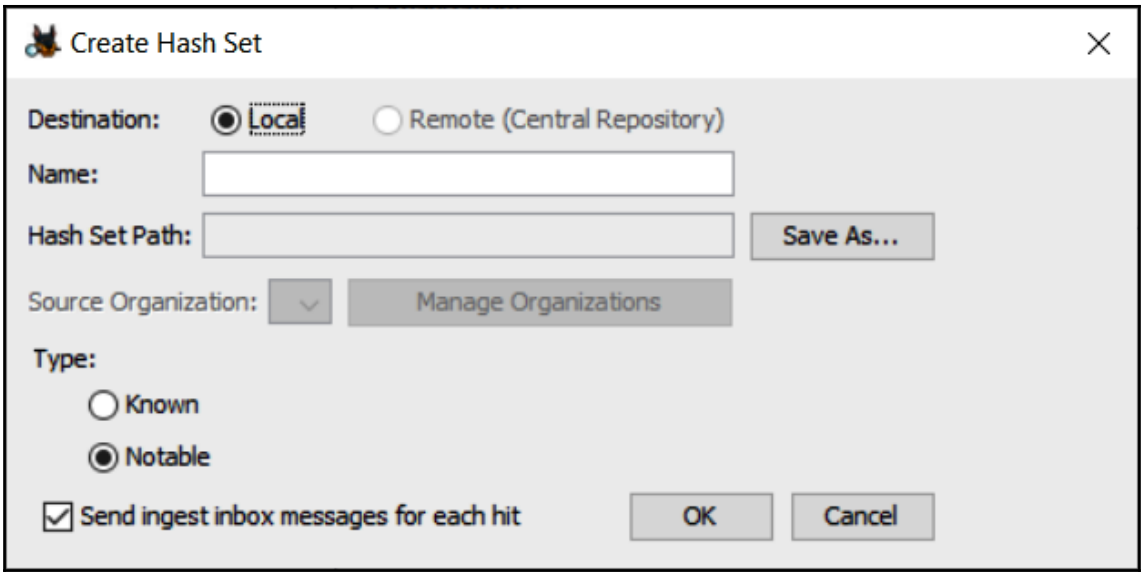

View Event
View Correlation Graph
View Event History
Edit Event
Delete Event
Add Attribute
Add Attachment
Populate from...
Merge attributes from...
Propose Attribute
Propose Attachment
Publish event to ZMQ
Contact Reporter
Download as...
List Events
Add Event
M2M - Locky 2017-06-26 : Affid=3 : "12_Invoice_3456" -...
Event ID 711
Uuid 5950fd85-deb8-4a7d-92c9-4ba8950d210f
Org CIRCL
Owner org MISP
Contributors
Email admin@misp.training
Tags tlp:white x ecsirt:malicious-code="ransomware" x misp-galaxy:ransomware="Locky" x +
Date 2017-06-26
Threat Level Low
Analysis Ongoing
Distribution All communities
Info M2M - Locky 2017-06-26 : Affid=3 : "12_Invoice_3456" - "001_4321.zip"
Published Yes
#Attributes 164
Sightings 0 (0) - restricted to own organisation only.
Activity
Pivots Galaxy Attributes Discussion
711: M2M - ...

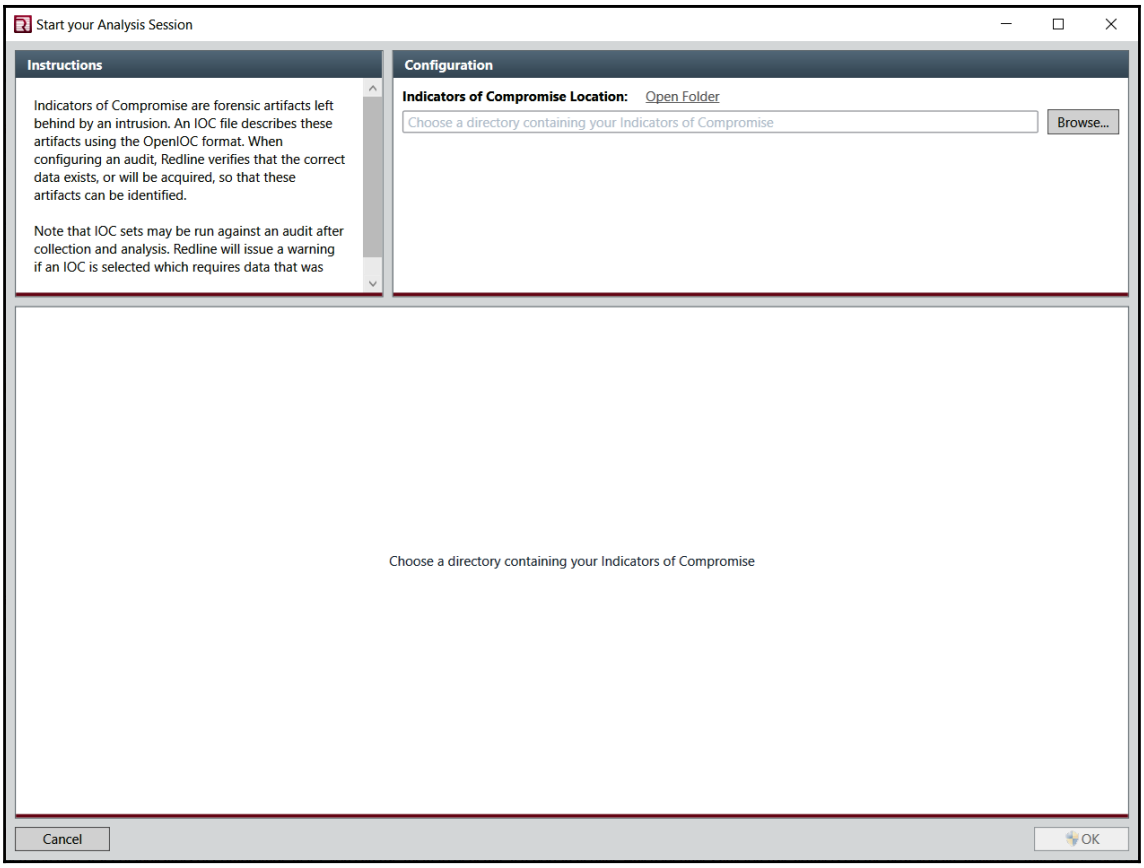
MISP MISP 733 osint:source-type="block-or-filter-list" 51 admin@misp.training 2017-07-14 Undefined Completed ZeuS compromised URL blocklist feed

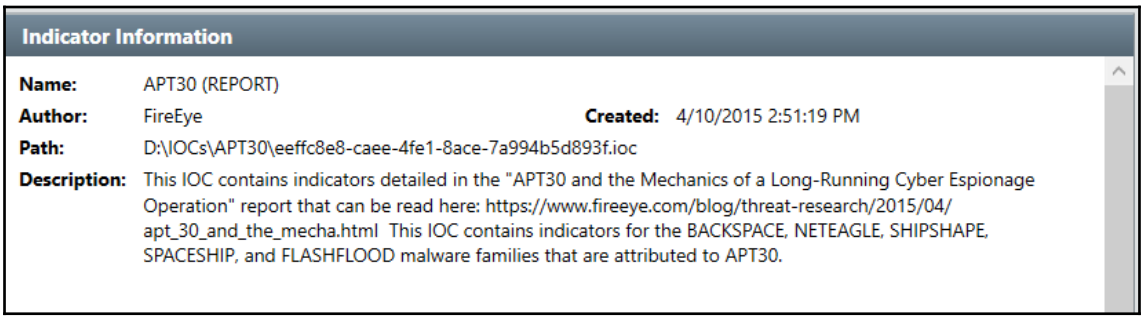


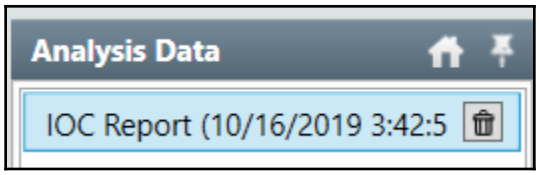

```
#This part might still contain bugs, use and your own risk and report any issues.
#
# MISP export of IDS rules - optimized for snort
#
# These NIDS rules contain some variables that need to exist in your configuration.
# Make sure you have set:
#
# $HOME_NET - Your internal network range
# $EXTERNAL_NET - The network considered as outside
# $SMTP_SERVERS - All your internal SMTP servers
# $HTTP_PORTS   - The ports used to contain HTTP traffic (not required with suricata export)
#
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg: "MISP e711 [] Outgoing HTTP URL:
alert udp any any -> any 53 (msg: "MISP e711 [] Hostname: 1010technologies.com"; content:"|
alert tcp any any -> any 53 (msg: "MISP e711 [] Hostname: 1010technologies.com"; content:"|
```

uuid	event_i	category	type	value	comme	to_ids	date
5950fd86-	711	Artifacts dropped	md5	8cd9f803947badddbfafc584edfdeebb		1	20170627
5950fd87-	711	Artifacts dropped	md5	a0d81f0bffb0e20a34191385031cf17a		1	20170627
59520c6b-	711	Artifacts dropped	sha1	f5fce485a72ab82a5e5b48b98befd5e0568a83e1	#NAME?	1	20170627
59520c6b-	711	Artifacts dropped	sha256	83b366204ef60cca5468c2db1baadeb7590f97493c451fa005f9b583ce691133	- Xchecked	1	20170627
59520c6b-	711	Artifacts dropped	sha1	3e19f754ea0fef9e62d91dfd4f22e6c73240bcbc	- Xchecked	1	20170627
59520c6b-	711	Artifacts dropped	sha256	8015133c16d41fdfbeb5f86f5d82ffb124a131ed012375d3cf70babe2f440ac8	#NAME?	1	20170627


Create Hash Set
Destination:
Local
Remote (Central Repository)
Name:
Hash Set Path:
Save As...
Source Organization:
Manage Organizations
Type:
Known
Notable
Send ingest inbox messages for each hit
OK
Cancel


Start your Analysis Session
Instructions
Indicators of Compromise are forensic artifacts left behind by an intrusion. An IOC file describes these artifacts using the OpenIOC format. When configuring an audit, Redline verifies that the correct data exists, or will be acquired, so that these artifacts can be identified.
Note that IOC sets may be run against an audit after collection and analysis. Redline will issue a warning if an IOC is selected which requires data that was
Configuration
Indicators of Compromise Location:
Open Folder
Choose a directory containing your Indicators of Compromise
Browse...
Choose a directory containing your Indicators of Compromise
Cancel
OK


Indicator Information
Name: APT30 (REPORT)
Author: FireEye
Created: 4/10/2015 2:51:19 PM
Path: D:\IOCs\APT30\eeffc8e8-caee-4fe1-8ace-7a994b5d893f.ioc
Description: This IOC contains indicators detailed in the "APT30 and the Mechanics of a Long-Running Cyber Espionage Operation" report that can be read here: https://www.fireeye.com/blog/threat-research/2015/04/apt_30_and_the_mecha.html This IOC contains indicators for the BACKSPACE, NETEAGLE, SHIPSHAPE, SPACESHIP, and FLASHFLOOD malware families that are attributed to APT30.



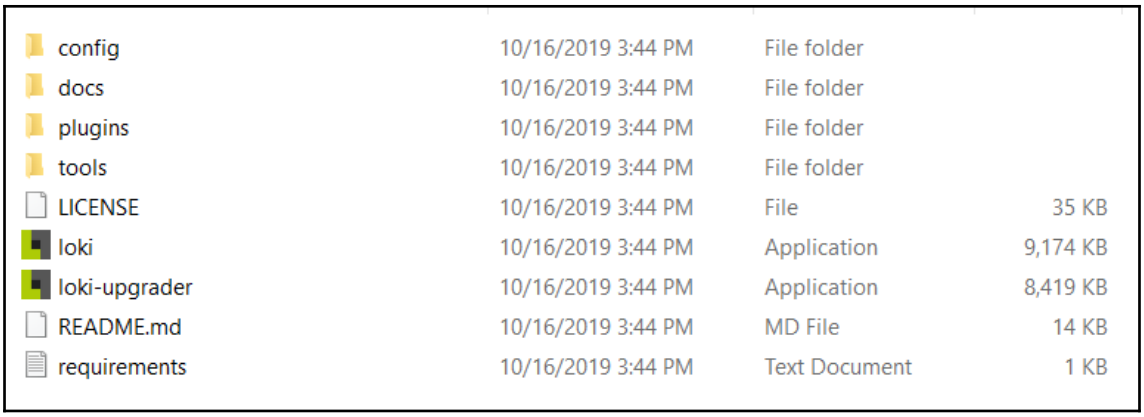
Branch: master ▾ rules / malware / APT_Cobalt.yar Find file Copy path

jholgui Updated and renamed name file APT_FIN7 76d87e8 on Sep 11

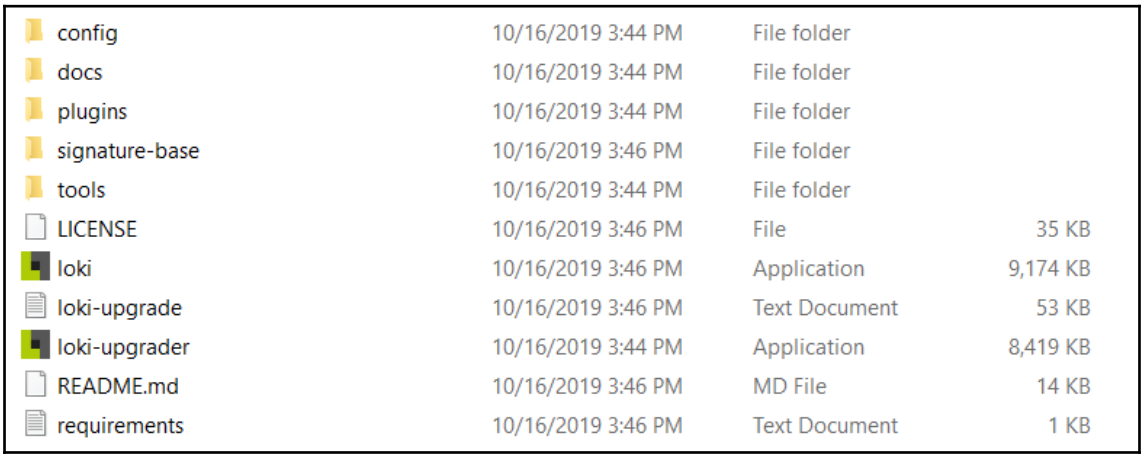
1 contributor

25 lines (18 sloc) | 705 Bytes Raw Blame History

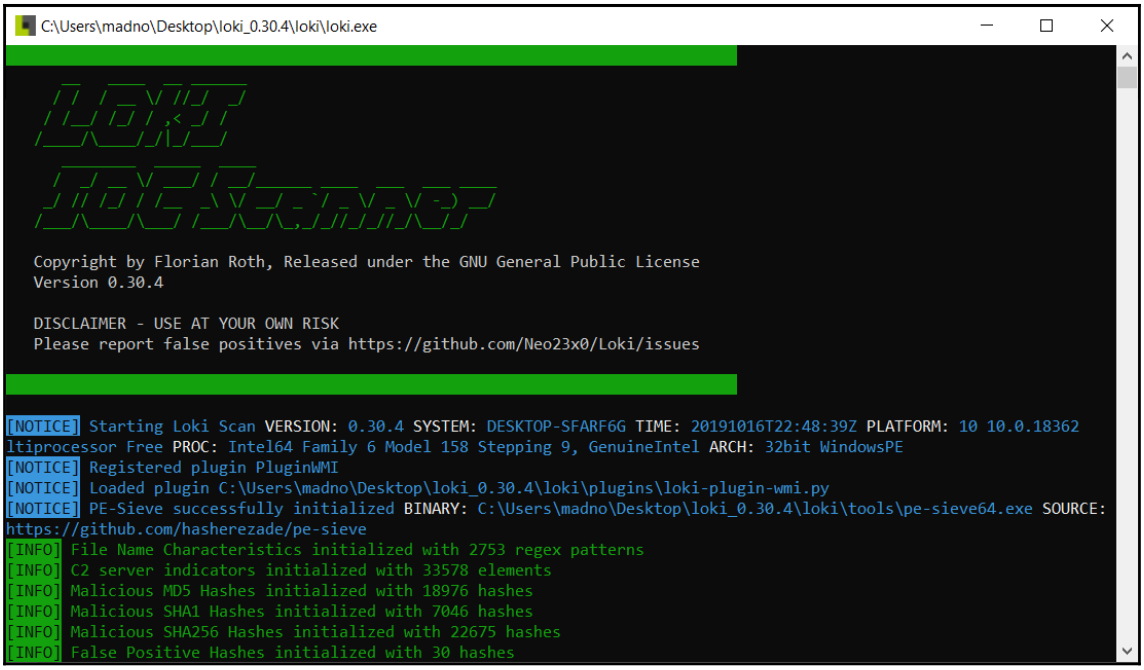
```
/*
    This Yara ruleset is under the GNU-GPLv2 license (http://www.gnu.org/licenses/gpl-2.0.html) and open to any user or organization, as

*/
rule Cobalt_functions
{

    meta:

        author="@j0sm1"
        url="https://www.securityartwork.es/2017/06/16/analisis-del-powershell-usado-fin7/"
        description="Detect functions coded with ROR edi,D; Detect CobaltStrike used by differents groups APT"

    strings:

        $h1={58 A4 53 E5} // VirtualAllocEx
        $h2={4C 77 26 07} // LoadLibraryEx
        $h3={6A C9 9C C9} // DNSQuery_UTF8
        $h4={44 F0 35 E0} // Sleep
        $h5={F4 00 8E CC} // lstrlen

    condition:
        2 of ( $h* )
}
```

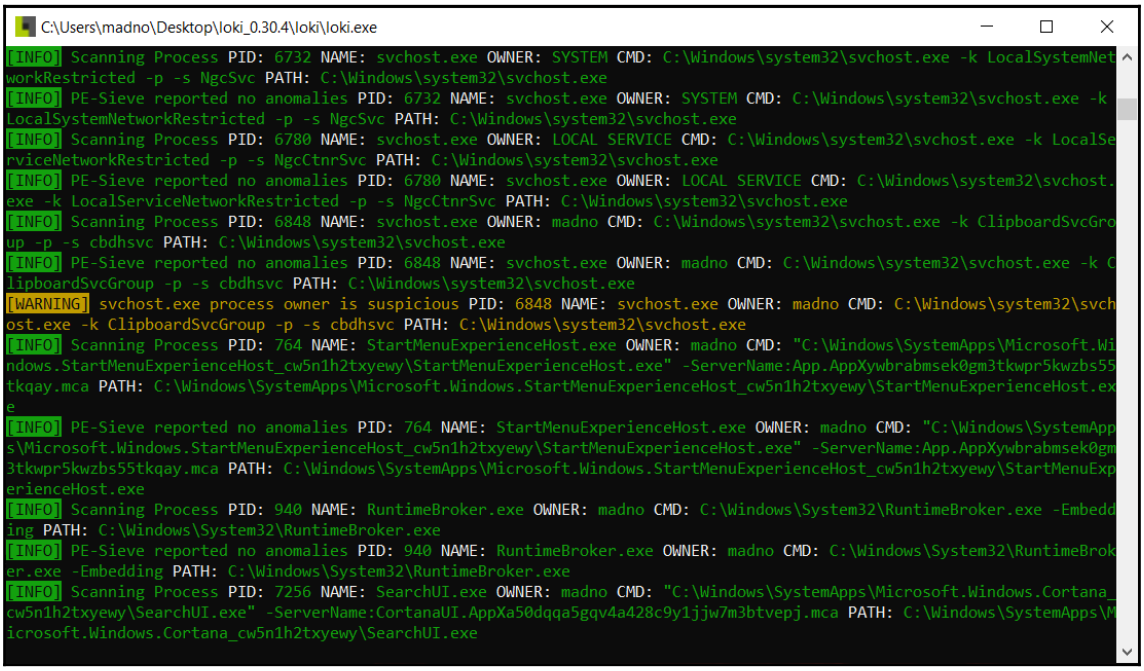


config	10/16/2019 3:44 PM	File folder	
docs	10/16/2019 3:44 PM	File folder	
plugins	10/16/2019 3:44 PM	File folder	
tools	10/16/2019 3:44 PM	File folder	
LICENSE	10/16/2019 3:44 PM	File	35 KB
loki	10/16/2019 3:44 PM	Application	9,174 KB
loki-upgrader	10/16/2019 3:44 PM	Application	8,419 KB
README.md	10/16/2019 3:44 PM	MD File	14 KB
requirements	10/16/2019 3:44 PM	Text Document	1 KB

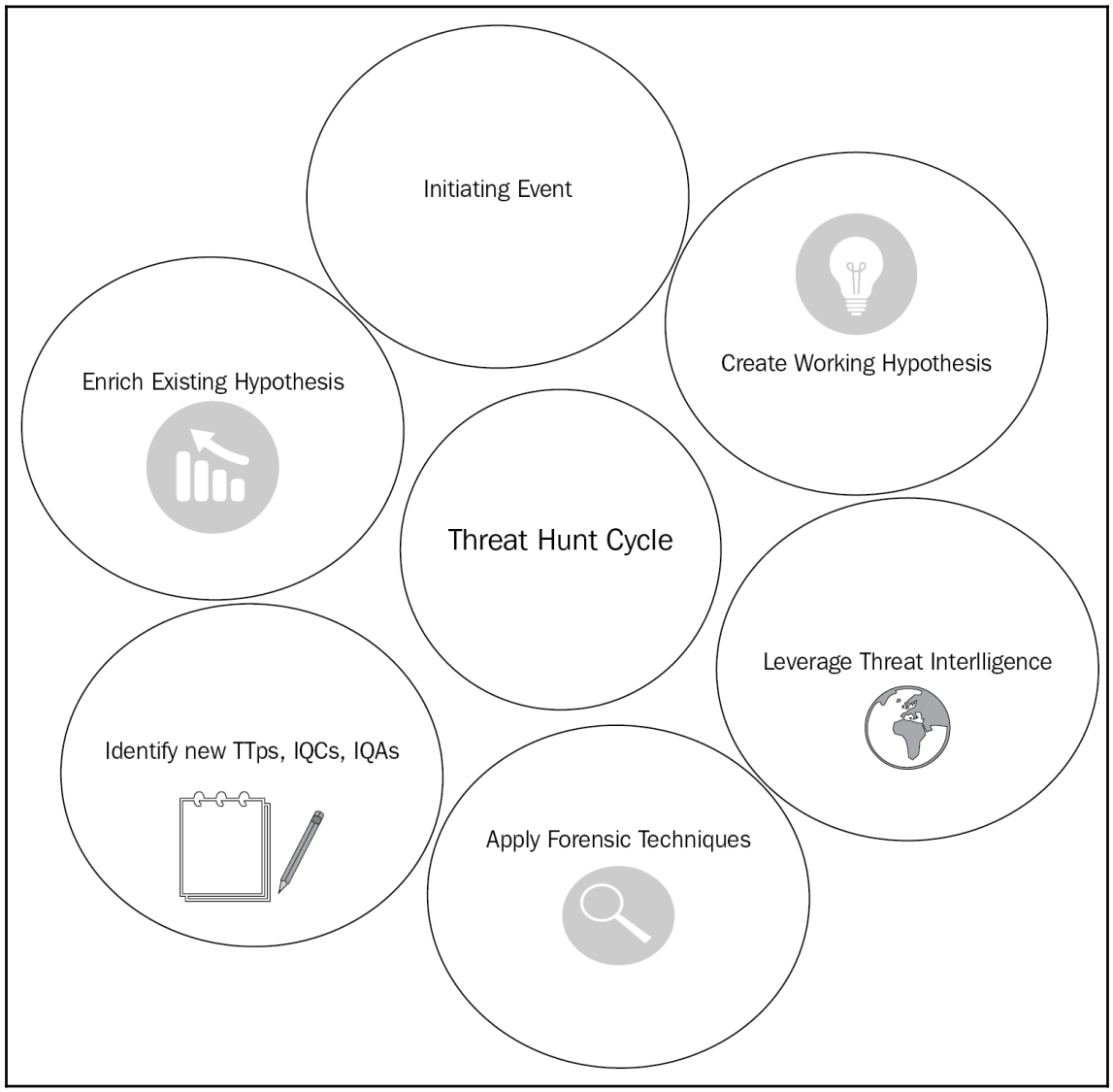


config	10/16/2019 3:44 PM	File folder	
docs	10/16/2019 3:44 PM	File folder	
plugins	10/16/2019 3:44 PM	File folder	
signature-base	10/16/2019 3:46 PM	File folder	
tools	10/16/2019 3:44 PM	File folder	
LICENSE	10/16/2019 3:46 PM	File	35 KB
loki	10/16/2019 3:46 PM	Application	9,174 KB
loki-upgrade	10/16/2019 3:46 PM	Text Document	53 KB
loki-upgrader	10/16/2019 3:44 PM	Application	8,419 KB
README.md	10/16/2019 3:46 PM	MD File	14 KB
requirements	10/16/2019 3:46 PM	Text Document	1 KB


C:\Users\madno\Desktop\loki_0.30.4\loki\loki.exe
Copyright by Florian Roth, Released under the GNU General Public License
Version 0.30.4
DISCLAIMER - USE AT YOUR OWN RISK
Please report false positives via https://github.com/Neo23x0/Loki/issues
[NOTICE] Starting Loki Scan VERSION: 0.30.4 SYSTEM: DESKTOP-SFARF6G TIME: 20191016T22:48:39Z PLATFORM: 10 10.0.18362
ltiprocessor Free PROC: Intel64 Family 6 Model 158 Stepping 9, GenuineIntel ARCH: 32bit WindowsPE
[NOTICE] Registered plugin PluginWMI
[NOTICE] Loaded plugin C:\Users\madno\Desktop\loki_0.30.4\loki\plugins\loki-plugin-wmi.py
[NOTICE] PE-Sieve successfully initialized BINARY: C:\Users\madno\Desktop\loki_0.30.4\loki\tools\pe-sieve64.exe SOURCE:
https://github.com/hasherezade/pe-sieve
[INFO] File Name Characteristics initialized with 2753 regex patterns
[INFO] C2 server indicators initialized with 33578 elements
[INFO] Malicious MD5 Hashes initialized with 18976 hashes
[INFO] Malicious SHA1 Hashes initialized with 7046 hashes
[INFO] Malicious SHA256 Hashes initialized with 22675 hashes
[INFO] False Positive Hashes initialized with 30 hashes


C:\Users\madno\Desktop\loki_0.30.4\loki\loki.exe
[INFO] Scanning Process PID: 6732 NAME: svchost.exe OWNER: SYSTEM CMD: C:\Windows\system32\svchost.exe -k LocalSystemNet
workRestricted -p -s NgcSvc PATH: C:\Windows\system32\svchost.exe
[INFO] PE-Sieve reported no anomalies PID: 6732 NAME: svchost.exe OWNER: SYSTEM CMD: C:\Windows\system32\svchost.exe -k
LocalSystemNetworkRestricted -p -s NgcSvc PATH: C:\Windows\system32\svchost.exe
[INFO] Scanning Process PID: 6780 NAME: svchost.exe OWNER: LOCAL SERVICE CMD: C:\Windows\system32\svchost.exe -k LocalSe
rviceNetworkRestricted -p -s NgcCtnrSvc PATH: C:\Windows\system32\svchost.exe
[INFO] PE-Sieve reported no anomalies PID: 6780 NAME: svchost.exe OWNER: LOCAL SERVICE CMD: C:\Windows\system32\svchost.
exe -k LocalServiceNetworkRestricted -p -s NgcCtnrSvc PATH: C:\Windows\system32\svchost.exe
[INFO] Scanning Process PID: 6848 NAME: svchost.exe OWNER: madno CMD: C:\Windows\system32\svchost.exe -k ClipboardSvcGro
up -p -s cbdhsvc PATH: C:\Windows\system32\svchost.exe
[INFO] PE-Sieve reported no anomalies PID: 6848 NAME: svchost.exe OWNER: madno CMD: C:\Windows\system32\svchost.exe -k C
lipboardSvcGroup -p -s cbdhsvc PATH: C:\Windows\system32\svchost.exe
[WARNING] svchost.exe process owner is suspicious PID: 6848 NAME: svchost.exe OWNER: madno CMD: C:\Windows\system32\svch
ost.exe -k ClipboardSvcGroup -p -s cbdhsvc PATH: C:\Windows\system32\svchost.exe
[INFO] Scanning Process PID: 764 NAME: StartMenuExperienceHost.exe OWNER: madno CMD: "C:\Windows\SystemApps\Microsoft.Wi
ndows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceHost.exe" -ServerName:App.AppXywbrabmsek0gm3tkwpr5kwzbs55
tkqay.mca PATH: C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceHost.ex
e
[INFO] PE-Sieve reported no anomalies PID: 764 NAME: StartMenuExperienceHost.exe OWNER: madno CMD: "C:\Windows\SystemApp
s\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceHost.exe" -ServerName:App.AppXywbrabmsek0gm
3tkwpr5kwzbs55tkqay.mca PATH: C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExp
erienceHost.exe
[INFO] Scanning Process PID: 940 NAME: RuntimeBroker.exe OWNER: madno CMD: C:\Windows\System32\RuntimeBroker.exe -Embedd
ing PATH: C:\Windows\System32\RuntimeBroker.exe
[INFO] PE-Sieve reported no anomalies PID: 940 NAME: RuntimeBroker.exe OWNER: madno CMD: C:\Windows\System32\RuntimeBrok
er.exe -Embedding PATH: C:\Windows\System32\RuntimeBroker.exe
[INFO] Scanning Process PID: 7256 NAME: SearchUI.exe OWNER: madno CMD: "C:\Windows\SystemApps\Microsoft.Windows.Cortana_
cw5n1h2txyewy\SearchUI.exe" -ServerName:CortanaUI.AppXa50dqqa5gqv4a428c9y1jjw7m3btvepj.mca PATH: C:\Windows\SystemApps\M
icrosoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe

Chapter 14: Hunting for Threats



02 MAY 019

Alert Number
MC-000103-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

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 in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber criminals.

This FLASH has been **TLP:WHITE**: Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

Indicators of Compromise Associated with Ryuk Ransomware

Summary

Unknown cybercriminals have targeted more than 100 US and international businesses with Ryuk ransomware since approximately August 2018. Ryuk encrypts files on network shares and an infected computer's filesystem. Once the victim has been compromised, the actors encrypt all the network's files and demand sums of up to $5 million worth of Bitcoin (BTC) in exchange for a decryptor program. Ryuk's targets are varied and indiscriminate, but attacks focus on organizations with high annual revenues in hopes of extracting larger ransoms from the victims. While Ryuk is generally undiscerning about victims, attacks have had a disproportionate impact on logistics companies, technology companies, and small municipalities.

ID	Name	Description
TA0001	Initial Access	The adversary is trying to get into your network.
TA0002	Execution	The adversary is trying to run malicious code.
TA0003	Persistence	The adversary is trying to maintain their foothold.
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0005	Defense Evasion	The adversary is trying to avoid being detected.
TA0006	Credential Access	The adversary is trying to steal account names and passwords.
TA0007	Discovery	The adversary is trying to figure out your environment.
TA0008	Lateral Movement	The adversary is trying to move through your environment.
TA0009	Collection	The adversary is trying to gather data of interest to their goal.
TA0011	Command and Control	The adversary is trying to communicate with compromised systems to control them.
TA0010	Exfiltration	The adversary is trying to steal data.
TA0040	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

Hypothesis	• An adversary has compromised a webserver in the DMZ and has gained access to the system and configured a remote access tool.
MITRE ATT&CK Tactics	• T1190 Exploit Public-Facing Application • T1219 Remote Access Tools • T1071 Standard Application Layer Protocol
Threat Intelligence	• VirusTotal • Alien Vault OTX • US-CERT
Sources	• Windows Event Logs, Packet Capture • IIS Logs, Web logs • Web application firewall logs
Tools	• Event log review tool • Wireshark or Moloch • File Search tools
Scope	• All Webservers in the DMZ
Timeframe	• Last 90 Days for Log Reviews