.

Part 1: Gather the Basic Information

In this part, you will review the alerts listed in **Security Onion VM** and gather basic information for the interested time frame.

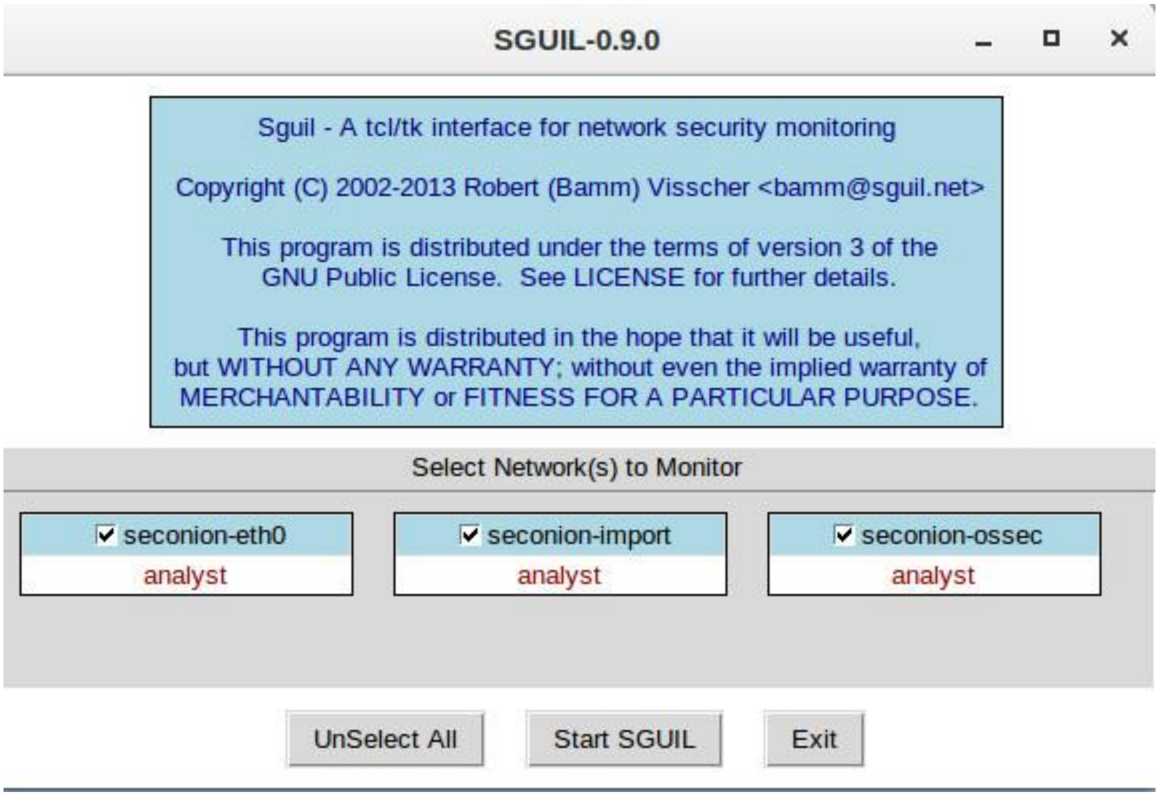
Step 1: Verify the status of services

a. Log into **Security Onion VM** using with the username **analyst** and password **cyberops**.
b. Open a **terminal** window. Enter the `sudo so-status` command to verify that all the services are ready.
Right click Desktop backgroud, go to **Open Terminal**

```
analyst@SecOnion:~$ sudo so-status

Status: securityonion

  * sguil server
[  OK  ]

Status: seconion-import

  * pcap_agent (sguil)
[  OK  ]

  * snort_agent-1 (sguil)
[  OK  ]

  * barnyard2-1 (spooler, unified2 format)
[  OK  ]

Status: Elastic stack

  * so-elasticsearch
[  OK  ]

  * so-logstash
[  OK  ]

  * so-kibana
[  OK  ]

  * so-freqserver
[  OK  ]
```

c. When the nsm service is ready, log into **Sguil** or **Kibana** with the username **analyst** and password **cyberops**.

Open **Sguil** using the shortcut on the **Desktop**. Login with the username **analyst** and password **cyberops**. Click **Select All** to select the interfaces and then **Start SGUIL**.



Sguil - A tcl/tk interface for network security monitoring

Copyright (C) 2002-2013 Robert (Bamm) Visscher <bamm@sguil.net>

This program is distributed under the terms of version 3 of the GNU Public License. See LICENSE for further details.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

Select Network(s) to Monitor

☑ seconion-eth0 analyst

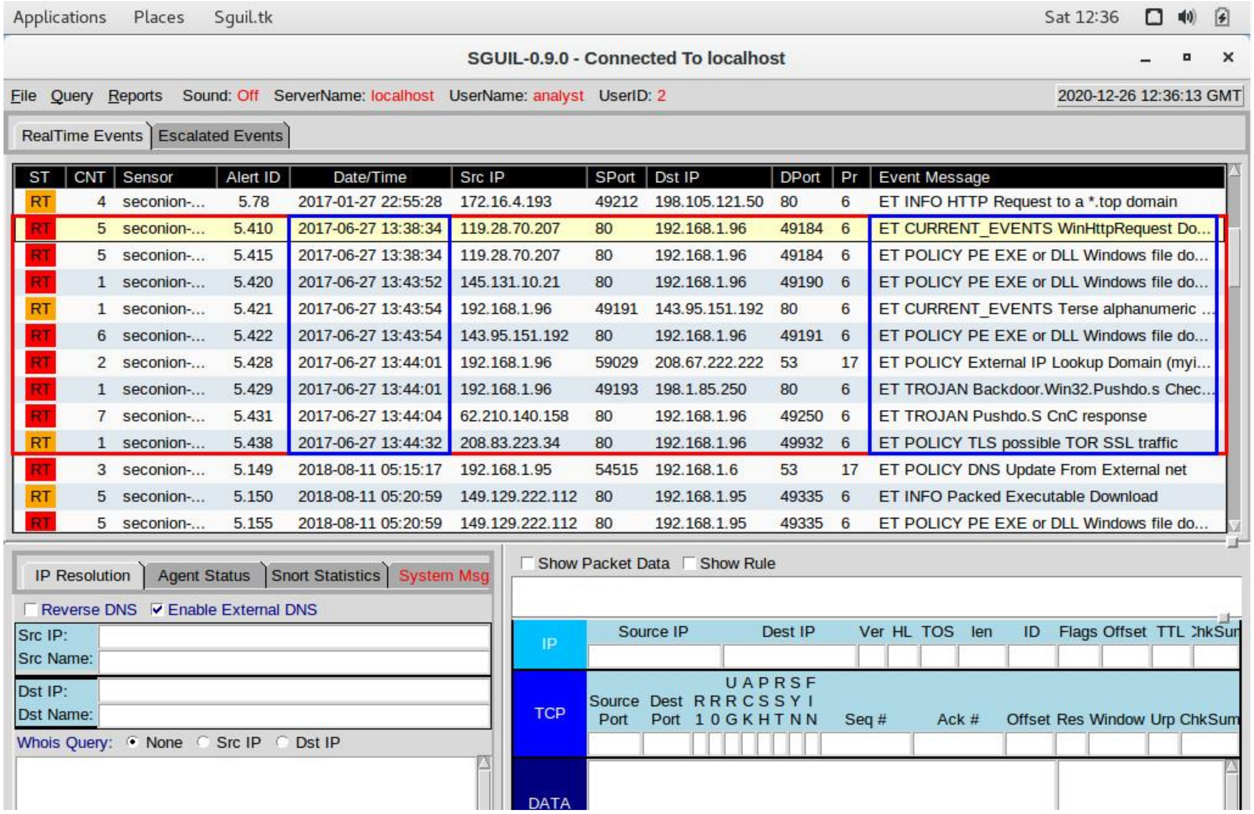
☑ seconion-import analyst

☑ seconion-ossec analyst

Step 2: Gather basic information.

a. Identify time frame of the **Pushdo** trojan attack, including the date and approximate time.

2017-06-27 from 13:38:34 to 13:44:32



Sound: Off ServerName: localhost UserName: analyst UserID: 2 2020-12-26 12:36:13 GMT

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	4	seconion-...	5.78	2017-01-27 22:55:28	172.16.4.193	49212	198.105.121.50	80	6	ET INFO HTTP Request to a *.top domain
RT	5	seconion-...	5.410	2017-06-27 13:38:34	119.28.70.207	80	192.168.1.96	49184	6	ET CURRENT_EVENTS WinHttpRequest Do...
RT	5	seconion-...	5.415	2017-06-27 13:38:34	119.28.70.207	80	192.168.1.96	49184	6	ET POLICY PE EXE or DLL Windows file do...
RT	1	seconion-...	5.420	2017-06-27 13:43:52	145.131.10.21	80	192.168.1.96	49190	6	ET POLICY PE EXE or DLL Windows file do...
RT	1	seconion-...	5.421	2017-06-27 13:43:54	192.168.1.96	49191	143.95.151.192	80	6	ET CURRENT_EVENTS Terse alphanumeric ...
RT	6	seconion-...	5.422	2017-06-27 13:43:54	143.95.151.192	80	192.168.1.96	49191	6	ET POLICY PE EXE or DLL Windows file do...
RT	2	seconion-...	5.428	2017-06-27 13:44:01	192.168.1.96	59029	208.67.222.222	53	17	ET POLICY External IP Lookup Domain (myi...
RT	1	seconion-...	5.429	2017-06-27 13:44:01	192.168.1.96	49193	198.1.85.250	80	6	ET TROJAN Backdoor.Win32.Pushdo.s Chec...
RT	7	seconion-...	5.431	2017-06-27 13:44:04	62.210.140.158	80	192.168.1.96	49250	6	ET TROJAN Pushdo.S CnC response
RT	1	seconion-...	5.438	2017-06-27 13:44:32	208.83.223.34	80	192.168.1.96	49932	6	ET POLICY TLS possible TOR SSL traffic
RT	3	seconion-...	5.149	2018-08-11 05:15:17	192.168.1.95	54515	192.168.1.6	53	17	ET POLICY DNS Update From External net
RT	5	seconion-...	5.150	2018-08-11 05:20:59	149.129.222.112	80	192.168.1.95	49335	6	ET INFO Packed Executable Download
RT	5	seconion-...	5.155	2018-08-11 05:20:59	149.129.222.112	80	192.168.1.95	49335	6	ET POLICY PE EXE or DLL Windows file do...

☐ Reverse DNS ☑ Enable External DNS

Src IP:
Src Name:
Dst IP:
Dst Name:

Whois Query: ● None ○ Src IP ○ Dst IP

☐ Show Packet Data ☐ Show Rule

b. List the alerts noted during this time frame associated with the trojan.

```
ET CURRENT_EVENTS WinHttpRequest Downloading EXE
ET POLICY PE EXE or DLL Windows file download HTTP
ET POLICY PE EXE or DLL Windows file download HTTP
ET CURRENT_EVENTS Terse alphanumeric executable downloader
high likelihood of being hostile
ET POLICY PE EXE or DLL Windows file download HTTP
ET POLICY External IP Lookup Domain (myip.opendns .com in
DNS lookup)
ET TROJAN Backdoor.Win32.Pushdo.s Checkin
ET TROJAN Pushdo.S CnC response
ET POLICY TLS possible TOR SSL traffic
```

c. List the internal IP addresses and external IP addresses involved.

Internal IP address:

- 192.168.1.96

External IP addresses:

- 143.95.151.192
- 119.28.70.207
- 145.131.10.21
- 62.210.140.158
- 119.28.70.207

- 208.67.222.222
- 208.83.223.34
- 198.1.85.250

Part 2: Learn about the Exploit

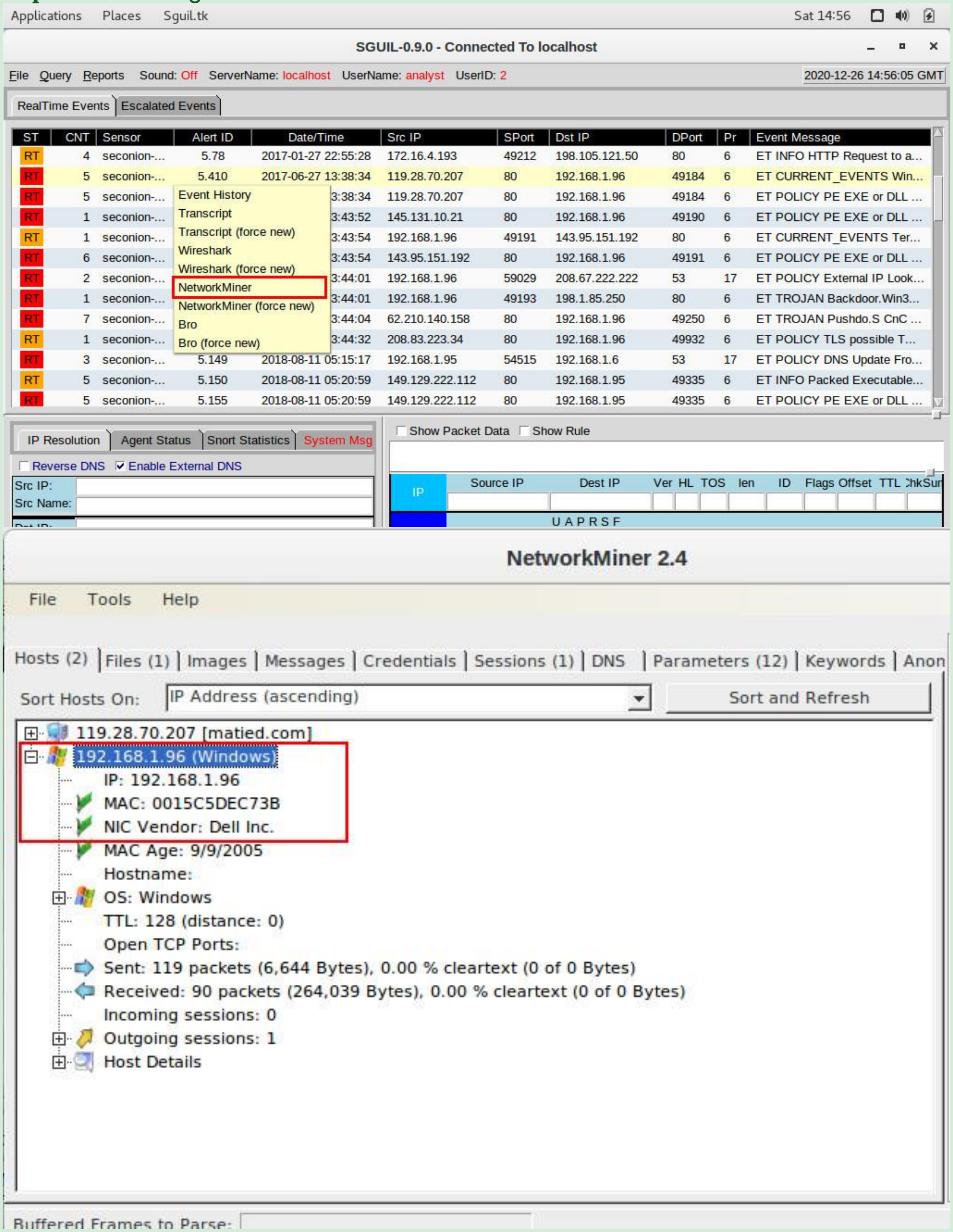
In this part, you will learn more about the exploit.

Step 1: Infected host

a. Based on the alerts, what is the IP and MAC addresses of the infected computer? Based on the MAC address, what is the vendor of the NIC chipset? (**Hint**: **NetworkMiner** or internet search)

IP: 192.168.1.96
MAC: 00-15-C5-DE-C7-3B
NIC Vendor: Dell Inc.

Explanation: Right-click **Alert ID: 5410** –> Select **NetworkMiner**.



Sound: Off ServerName: localhost UserName: analyst UserID: 2 2020-12-26 14:56:05 GMT

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	4	seconion-...	5.78	2017-01-27 22:55:28	172.16.4.193	49212	198.105.121.50	80	6	ET INFO HTTP Request to a...
RT	5	seconion-...	5.410	2017-06-27 13:38:34	119.28.70.207	80	192.168.1.96	49184	6	ET CURRENT_EVENTS Win...
RT	5	seconion-...		3:38:34	119.28.70.207	80	192.168.1.96	49184	6	ET POLICY PE EXE or DLL ...
RT	1	seconion-...		3:43:52	145.131.10.21	80	192.168.1.96	49190	6	ET POLICY PE EXE or DLL ...
RT	1	seconion-...		3:43:54	192.168.1.96	49191	143.95.151.192	80	6	ET CURRENT_EVENTS Ter...
RT	6	seconion-...		3:43:54	143.95.151.192	80	192.168.1.96	49191	6	ET POLICY PE EXE or DLL ...
RT	2	seconion-...		3:44:01	192.168.1.96	59029	208.67.222.222	53	17	ET POLICY External IP Look...
RT	1	seconion-...		3:44:01	192.168.1.96	49193	198.1.85.250	80	6	ET TROJAN Backdoor.Win3...
RT	7	seconion-...		3:44:04	62.210.140.158	80	192.168.1.96	49250	6	ET TROJAN Pushdo.S CnC ...
RT	1	seconion-...		3:44:32	208.83.223.34	80	192.168.1.96	49932	6	ET POLICY TLS possible T...
RT	3	seconion-...	5.149	2018-08-11 05:15:17	192.168.1.95	54515	192.168.1.6	53	17	ET POLICY DNS Update Fro...
RT	5	seconion-...	5.150	2018-08-11 05:20:59	149.129.222.112	80	192.168.1.95	49335	6	ET INFO Packed Executable...
RT	5	seconion-...	5.155	2018-08-11 05:20:59	149.129.222.112	80	192.168.1.95	49335	6	ET POLICY PE EXE or DLL ...

□ Reverse DNS ☑ Enable External DNS

Src IP:

Src Name:

□ Show Packet Data □ Show Rule

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum

U A P R S F

Sort Hosts On: IP Address (ascending)

```
⊞ 119.28.70.207 [matied.com]
⊟ 192.168.1.96 (Windows)
    IP: 192.168.1.96
    MAC: 0015C5DEC73B
    NIC Vendor: Dell Inc.
    MAC Age: 9/9/2005
    Hostname:
  ⊞ OS: Windows
    TTL: 128 (distance: 0)
    Open TCP Ports:
    Sent: 119 packets (6,644 Bytes), 0.00 % cleartext (0 of 0 Bytes)
    Received: 90 packets (264,039 Bytes), 0.00 % cleartext (0 of 0 Bytes)
    Incoming sessions: 0
  ⊞ Outgoing sessions: 1
  ⊞ Host Details
```

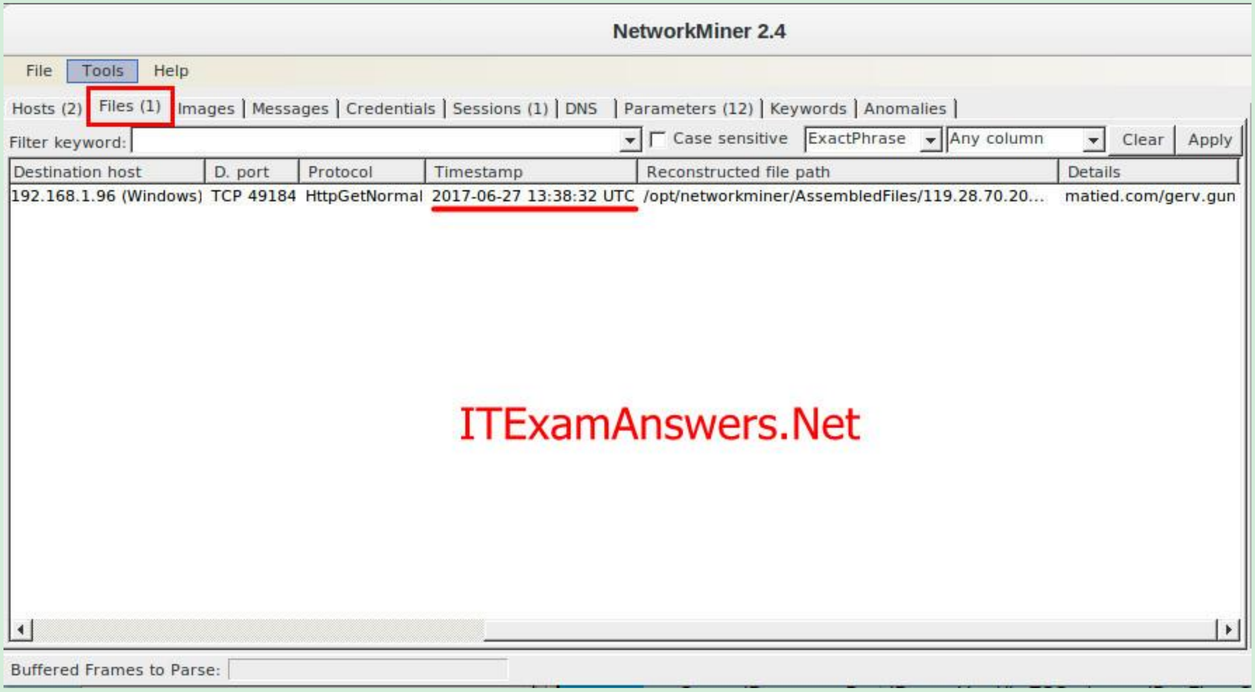
Buffered Frames to Parse:

b. Based on the alerts, when (date and time in UTC) and how was the PC infected? (**Hint**: Enter the command **date** in the terminal to determine the time zone for the displayed time)

2017-06-27 13:38:32 UTC

The **gerv.gun** malware was executed through the **Pushdo trojan**.

On **NetworkMiner** windows, click **Files** tab to determine date and time in UTC:



Filter keyword: ☐ Case sensitive ExactPhrase Any column

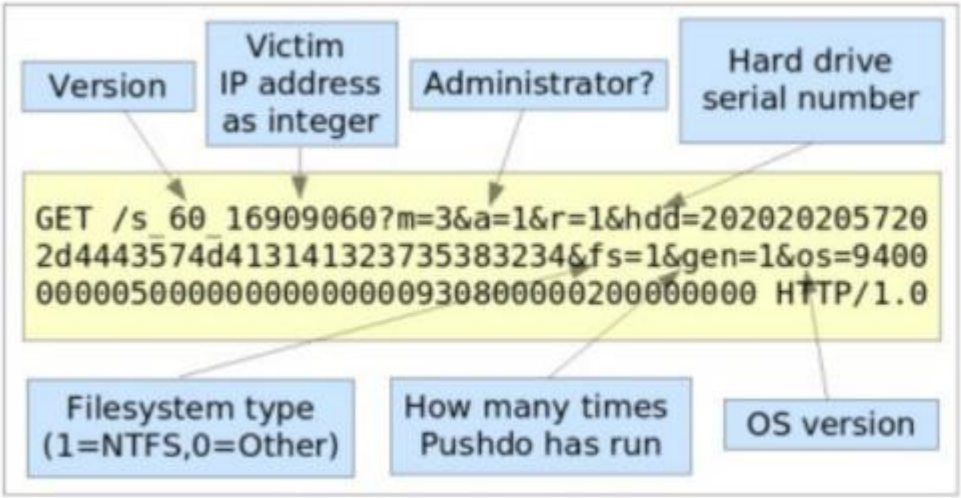
Destination host	D. port	Protocol	Timestamp	Reconstructed file path	Details
192.168.1.96 (Windows)	TCP 49184	HttpGetNormal	2017-06-27 13:38:32 UTC	/opt/networkminer/AssembledFiles/119.28.70.20...	matied.com/gerv.gun

Buffered Frames to Parse:

How did the malware infect the PC? Use an internet search as necessary.

The user in the **192.168.1.96** PC accessed a malicious domain, and the Pushdo trojan was used to install the malware.

Pushdo is a “downloader” trojan, meaning its purpose is to download and install additional malicious software. When executed, Pushdo reports back to one of several control server IP addresses embedded in it code. The server listens on TCP port 80, and pretends to be an Apache webserver. If the HTTP request contains the correct parameters, one or more executables will be delivered via HTTP. The malware to be downloaded by Pushdo depends on the value following the”s-underscore” part of the URL


Version
Victim IP address as integer
Administrator?
Hard drive serial number
Filesystem type (1=NTFS,0=Other)
How many times Pushdo has run
OS version

```
GET /s_60_16909060?m=3&a=1&r=1&hdd=202020205720
2d4443574d41314132373538323 4&fs=1&gen=1&os=9400
000005000000000000000930800000200000000 HTTP/1.0
```

Pushdo HTTP Request Variables

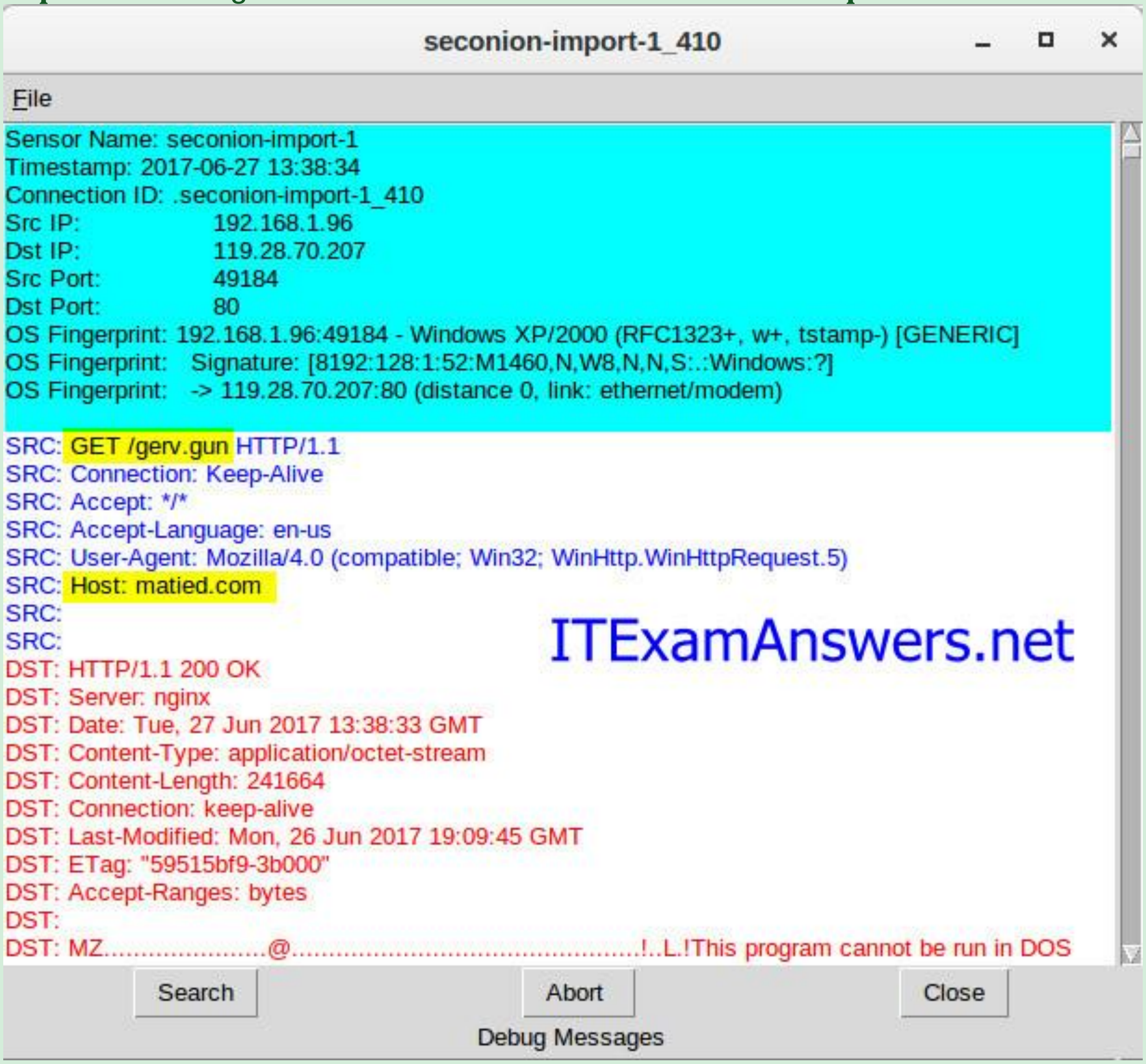
Pushdo keeps track of the IP address of the victim, whether or not that person is an administator on the computer, their primary hard drive serial number (obtained by SMART_RCV_DRIVE_DATA IO control code), whether the filesystem is NTFS, how many times the victim system has executed a Pushdo variant, and the Windows OS version as returned by the GetVersionEx API call.

Step 2: Examine the exploit.

a. Based on the alerts associated with HTTP GET request, what files were downloaded? List the malicious domains observed and the files downloaded.

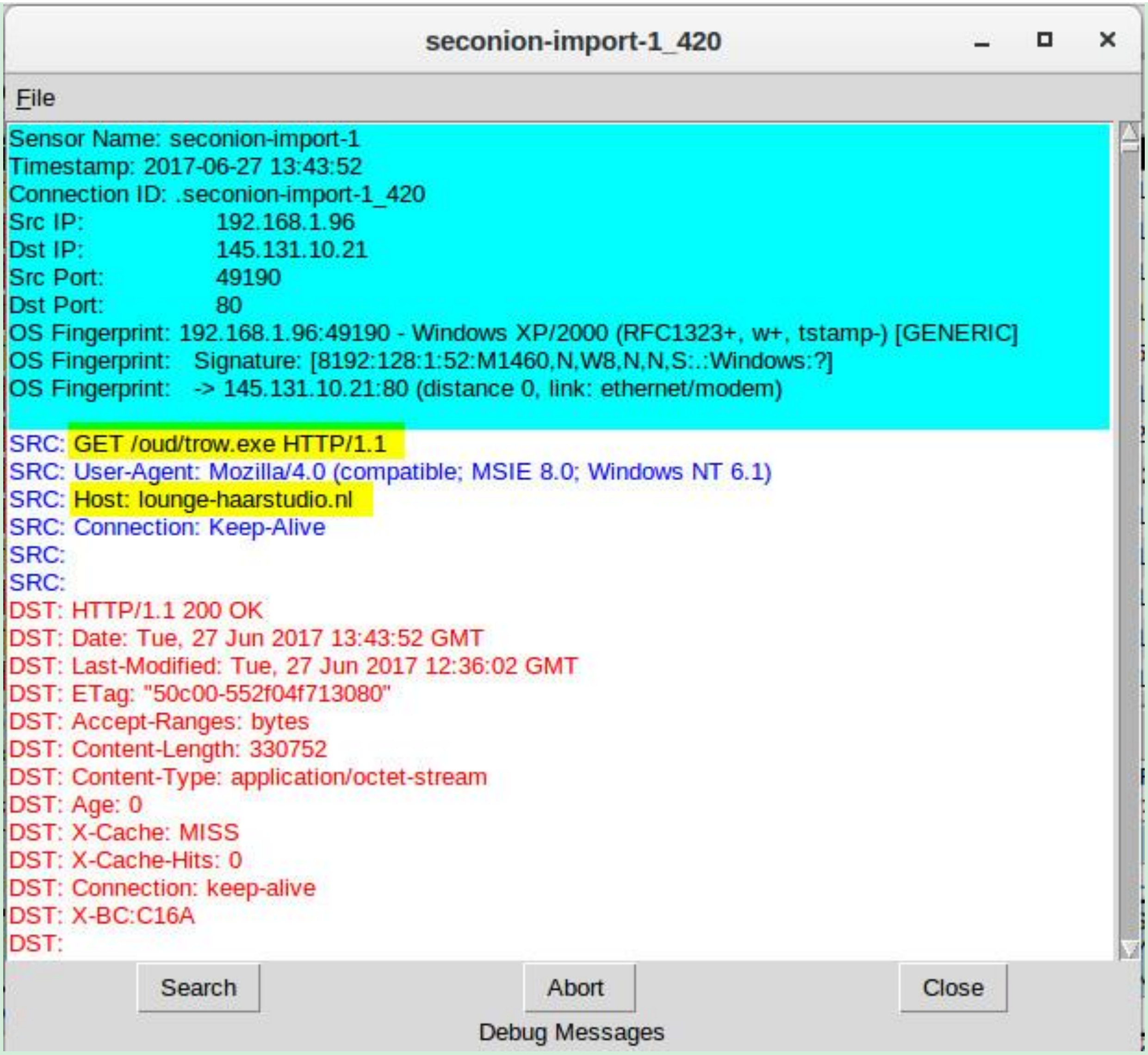
gerv.gun – matied.com/gerv.gun
trow.exe – lounge-haarstudio.nl/oud/trow.exe
wp.exe – vantagepointtechnologies.com/wp.exe

Explanation: Right-click **Alert ID: 5410** –> Select **Transcript**



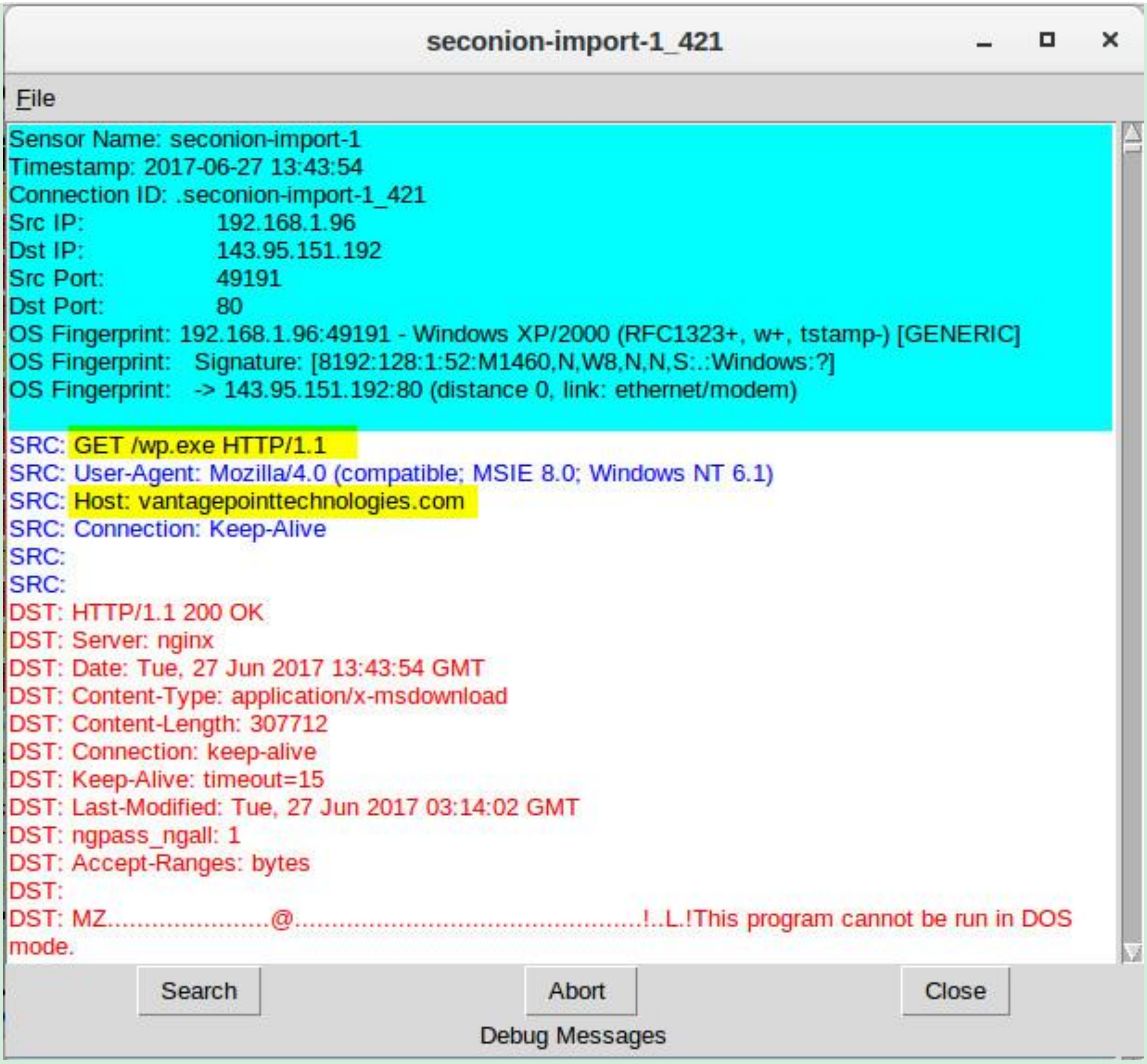
```
Sensor Name: seconion-import-1
Timestamp: 2017-06-27 13:38:34
Connection ID: .seconion-import-1_410
Src IP:             192.168.1.96
Dst IP:             119.28.70.207
Src Port:           49184
Dst Port:           80
OS Fingerprint: 192.168.1.96:49184 - Windows XP/2000 (RFC1323+, w+, tstamp-) [GENERIC]
OS Fingerprint:   Signature: [8192:128:1:52:M1460,N,W8,N,N,S:.:Windows:?]
OS Fingerprint:   -> 119.28.70.207:80 (distance 0, link: ethernet/modem)

SRC: GET /gerv.gun HTTP/1.1
SRC: Connection: Keep-Alive
SRC: Accept: */*
SRC: Accept-Language: en-us
SRC: User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
SRC: Host: matied.com
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Server: nginx
DST: Date: Tue, 27 Jun 2017 13:38:33 GMT
DST: Content-Type: application/octet-stream
DST: Content-Length: 241664
DST: Connection: keep-alive
DST: Last-Modified: Mon, 26 Jun 2017 19:09:45 GMT
DST: ETag: "59515bf9-3b000"
DST: Accept-Ranges: bytes
DST:
DST: MZ......................@...............................................!..L.!This program cannot be run in DOS
```

Right-click **Alert ID: 5420** –> Select **Transcript**



```
Sensor Name: seconion-import-1
Timestamp: 2017-06-27 13:43:52
Connection ID: .seconion-import-1_420
Src IP:             192.168.1.96
Dst IP:             145.131.10.21
Src Port:           49190
Dst Port:           80
OS Fingerprint: 192.168.1.96:49190 - Windows XP/2000 (RFC1323+, w+, tstamp-) [GENERIC]
OS Fingerprint:   Signature: [8192:128:1:52:M1460,N,W8,N,N,S:.:Windows:?]
OS Fingerprint:   -> 145.131.10.21:80 (distance 0, link: ethernet/modem)

SRC: GET /oud/trow.exe HTTP/1.1
SRC: User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
SRC: Host: lounge-haarstudio.nl
SRC: Connection: Keep-Alive
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Tue, 27 Jun 2017 13:43:52 GMT
DST: Last-Modified: Tue, 27 Jun 2017 12:36:02 GMT
DST: ETag: "50c00-552f04f713080"
DST: Accept-Ranges: bytes
DST: Content-Length: 330752
DST: Content-Type: application/octet-stream
DST: Age: 0
DST: X-Cache: MISS
DST: X-Cache-Hits: 0
DST: Connection: keep-alive
DST: X-BC:C16A
DST:
```

Right-click **Alert ID: 5421** –> Select **Transcript**



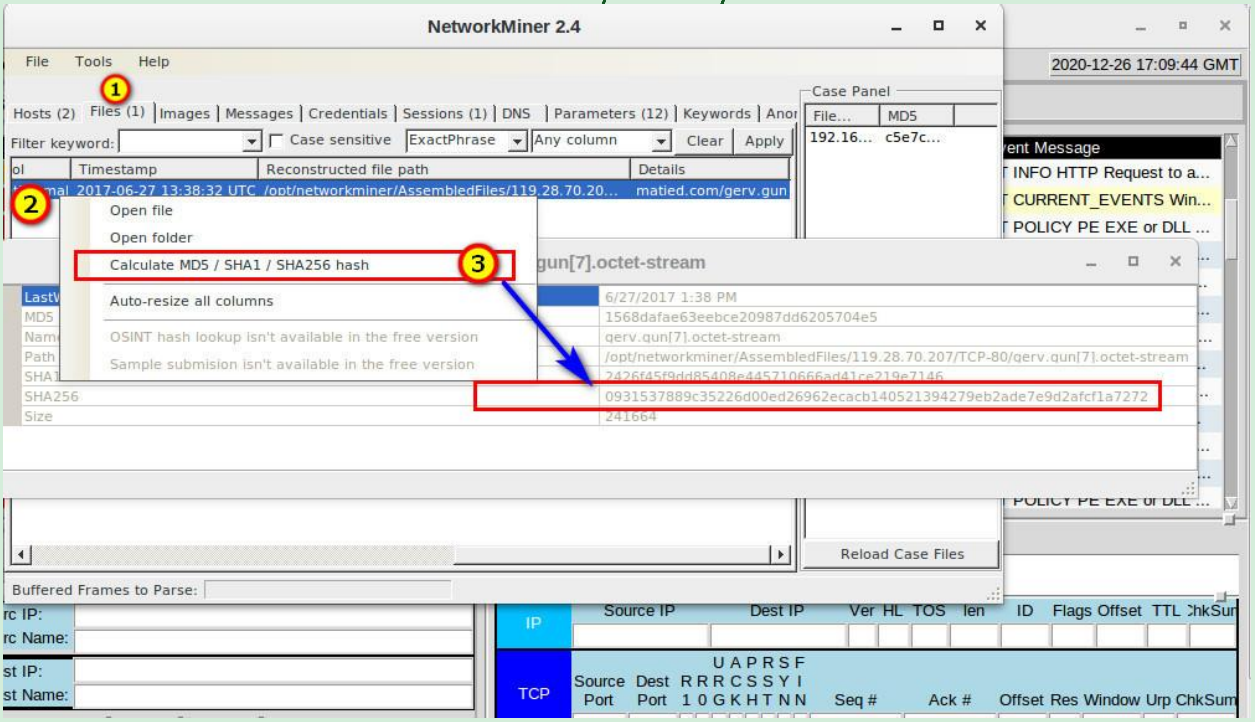
```
Sensor Name: seconion-import-1
Timestamp: 2017-06-27 13:43:54
Connection ID: .seconion-import-1_421
Src IP:             192.168.1.96
Dst IP:             143.95.151.192
Src Port:           49191
Dst Port:           80
OS Fingerprint: 192.168.1.96:49191 - Windows XP/2000 (RFC1323+, w+, tstamp-) [GENERIC]
OS Fingerprint:   Signature: [8192:128:1:52:M1460,N,W8,N,N,S:.:Windows:?]
OS Fingerprint:   -> 143.95.151.192:80 (distance 0, link: ethernet/modem)

SRC: GET /wp.exe HTTP/1.1
SRC: User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
SRC: Host: vantagepointtechnologies.com
SRC: Connection: Keep-Alive
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Server: nginx
DST: Date: Tue, 27 Jun 2017 13:43:54 GMT
DST: Content-Type: application/x-msdownload
DST: Content-Length: 307712
DST: Connection: keep-alive
DST: Keep-Alive: timeout=15
DST: Last-Modified: Tue, 27 Jun 2017 03:14:02 GMT
DST: ngpass_ngall: 1
DST: Accept-Ranges: bytes
DST:
DST: MZ......................@..............................................!..L.!This program cannot be run in DOS
mode.
```

Use any available tools in **Security Onion VM**, determine and record the **SHA256** hash for the downloaded files that probably infected the computer?

gerv.gun =
0931537889c35226d00ed26962ecacb140521394279eb2ade7e9d2afcf1a7272
trow.exe =
94a0a09ee6a21526ac34d41eabf4ba603e9a30c26e6a1dc072ff45749dfb1fe1
wp.exe =
79d503165d32176842fe386d96c04fb70f6ce1c8a4858379578492 97e625ea48

Explanation: Use **NetworkMiner** tool:
Right-click **Alert ID: 5410** –> Select **NetworkMiner** –> Click **Files** tab –> Right

click first line –> Select **Calculate MD5 / SHA1 / SHA256 hash**



ol	Timestamp	Reconstructed file path	Details
...mal	2017-06-27 13:38:32 UTC	/opt/networkminer/AssembledFiles/119.28.70.20...	matied.com/gerv.gun

File...	MD5
192.16...	c5e7c...

...vent Message
...T INFO HTTP Request to a...
...T CURRENT_EVENTS Win...
...T POLICY PE EXE or DLL ...
...T POLICY PE EXE or DLL ...

...gun[7].octet-stream

LastW...	6/27/2017 1:38 PM
MD5	1568dafae63eebce20987dd6205704e5
Nam...	gerv.gun[7].octet-stream
Path	/opt/networkminer/AssembledFiles/119.28.70.207/TCP-80/gerv.gun[7].octet-stream
SHA1	2426f45f9dd85408e445710666ad41ce219e7146
SHA256	0931537889c35226d00ed26962ecacb140521394279eb2ade7e9d2afcf1a7272
Size	241664

...rc IP:
...rc Name:
...st IP:
...st Name:

Source IP | Dest IP | Ver | HL | TOS | len | ID | Flags | Offset | TTL | ChkSum

Source Port | Dest Port | U A P R S F / R R R C S S Y I / 1 0 G K H T N N | Seq # | Ack # | Offset | Res | Window | Urp | ChkSum

Do the same for Alert ID: **5420 and 5421** to determine **SHA256** hash for the files: **trow.exe and wp.exe**

b. Navigate to www.virustotal.com input the SHA256 hash to determine if these were detected as malicious files. Record your findings, such as file type and size, other names, and target machine. You can also include any information that is provided by the community posted in **VirusTotal**.

gerv.gun:

- 58 engines detected this file
- File type: Win32 EXE
- File size: 236.00 KB (241664 bytes)
- Names:
    - gerv.gun
    - test
    - tmp523799.697
    - tmp246975.343
    - tmp213582.420
    - extract-1498570714.111294-HTTP-FG0jno3bJLiIzR4hrh.exe
    - 0931537889c35226d00ed26962ecacb140521394279eb2ade7e9d2afcf1a7272.bin
    - vector.tui
- Target Machine: Intel 386 or later processors and compatible processors

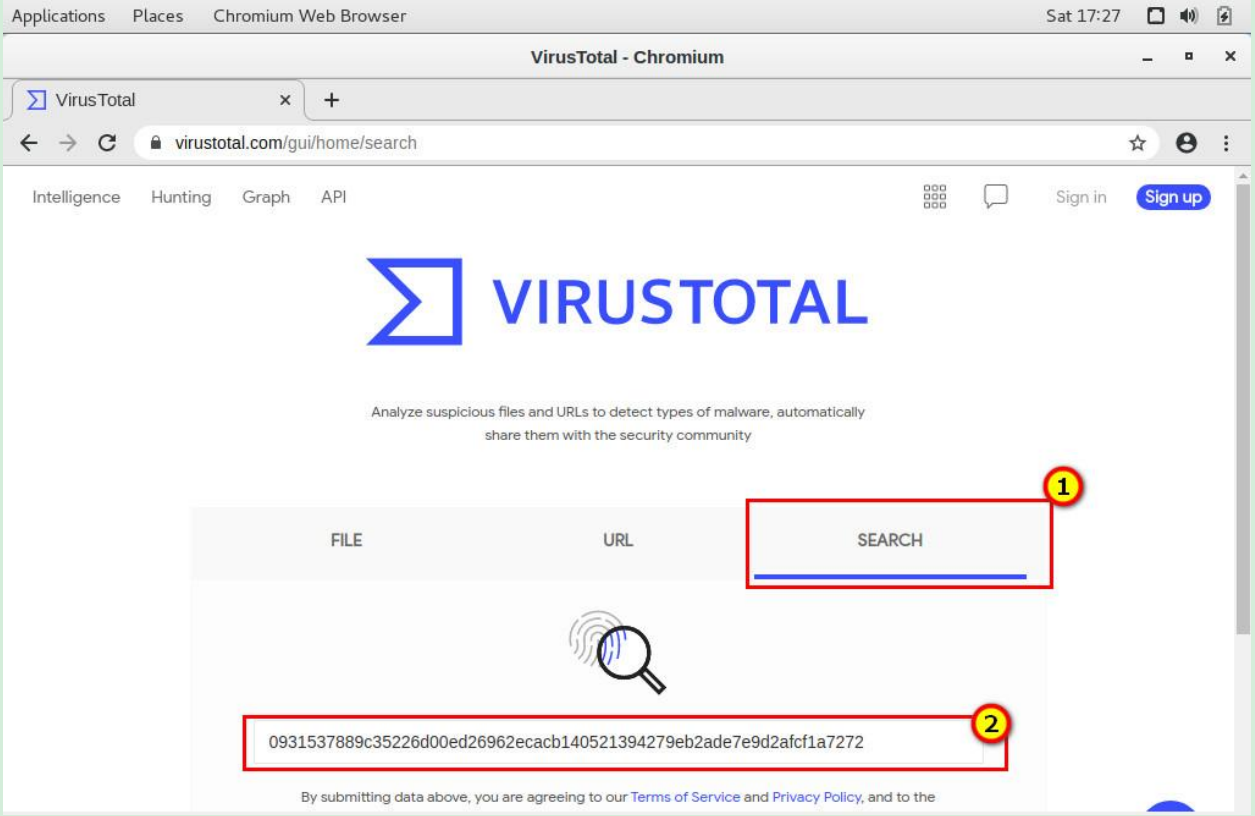
trow.exe:

- 63 engines detected this file
- File type: Win32 EXE
- File size: 323.00 KB (330752 bytes)
- Names:
    - Pedals
    - Pedals.exe
    - trow.exe
    - test3
    - 2017-06-28_18-18-14.exe
    - bma2beo4.exe
- Target Machine: Intel 386 or later processors and compatible processors

wp.exe:

- 55 engines detected this file
- File type: Win32 EXE
- File size: 300.50 KB (307712 bytes)
- Names:
    - wp.exe
    - test2
    - test_3
    - 4da48f6423d5f7d75de281a674c2e620.virobj
    - wp.exe.x-msdownload
- Target Machine: Intel 386 or later processors and compatible processors

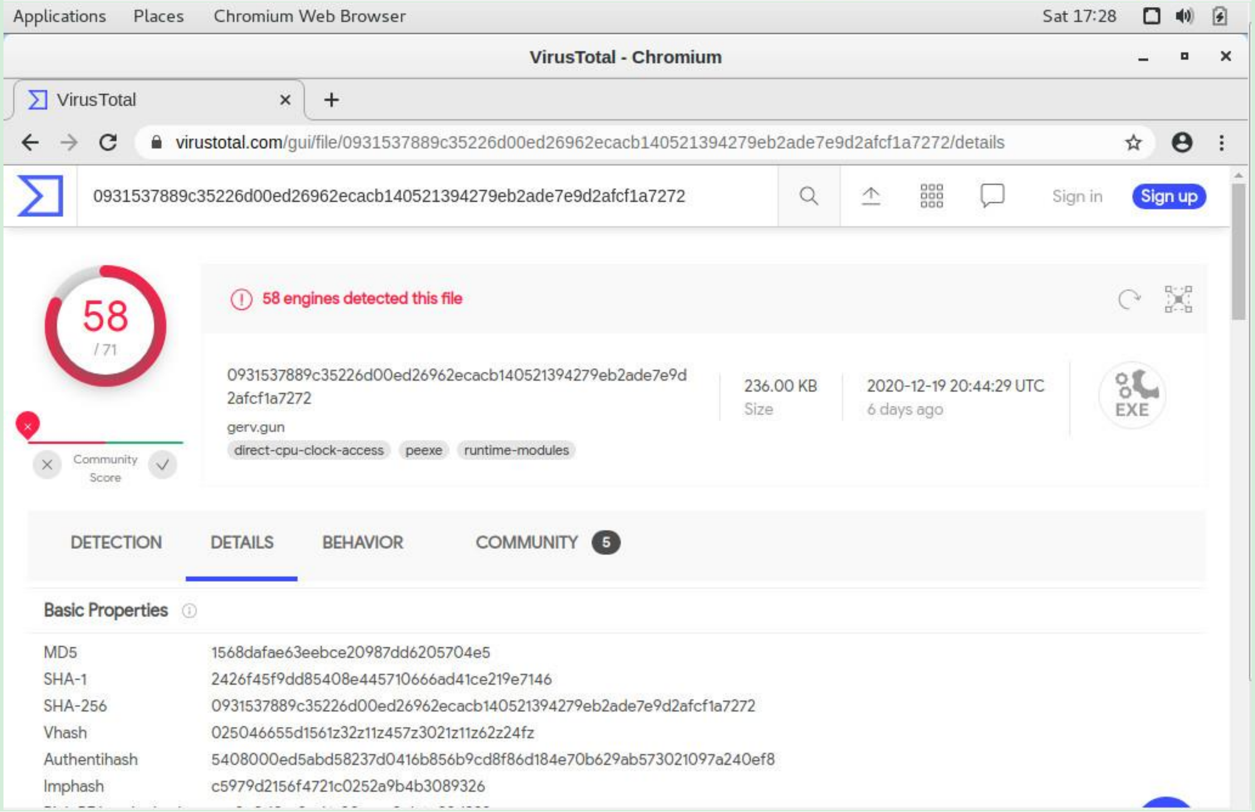
Explanation: Open Chromium Web Browser –> access to www.virustotal.com –> Click **Search** –> Enter **Hash**



Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community

0931537889c35226d00ed26962ecacb140521394279eb2ade7e9d2afcf1a7272

By submitting data above, you are agreeing to our Terms of Service and Privacy Policy, and to the



0931537889c35226d00ed26962ecacb140521394279eb2ade7e9d2afcf1a7272

58 engines detected this file

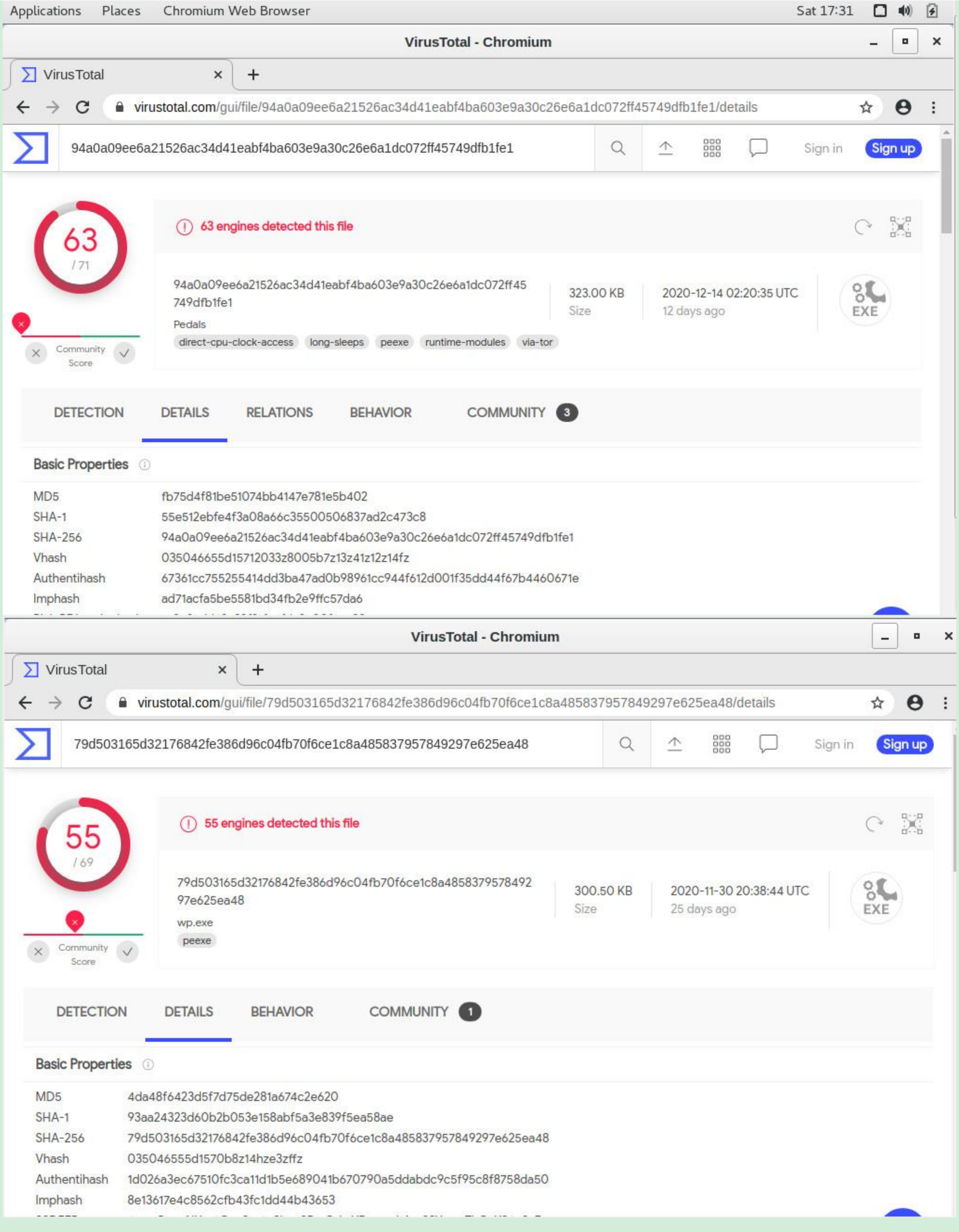
0931537889c35226d00ed26962ecacb140521394279eb2ade7e9d2afcf1a7272
gerv.gun
direct-cpu-clock-access peexe runtime-modules

236.00 KB
Size

2020-12-19 20:44:29 UTC
6 days ago

Basic Properties

MD5	1568dafae63eebce20987dd6205704e5
SHA-1	2426f45f9dd85408e445710666ad41ce219e7146
SHA-256	0931537889c35226d00ed26962ecacb140521394279eb2ade7e9d2afcf1a7272
Vhash	025046655d1561z32z11z457z3021z11z62z24fz
Authentihash	5408000ed5abd58237d0416b856b9cd8f86d184e70b629ab573021097a240ef8
Imphash	c5979d2156f4721c0252a9b4b3089326



94a0a09ee6a21526ac34d41eabf4ba603e9a30c26e6a1dc072ff45749dfb1fe1

63 engines detected this file

94a0a09ee6a21526ac34d41eabf4ba603e9a30c26e6a1dc072ff45749dfb1fe1
Pedals
direct-cpu-clock-access long-sleeps peexe runtime-modules via-tor

323.00 KB
Size

2020-12-14 02:20:35 UTC
12 days ago

Basic Properties

MD5	fb75d4f81be51074bb4147e781e5b402
SHA-1	55e512ebfe4f3a08a66c35500506837ad2c473c8
SHA-256	94a0a09ee6a21526ac34d41eabf4ba603e9a30c26e6a1dc072ff45749dfb1fe1
Vhash	035046655d15712033z8005b7z13z41z12z14fz
Authentihash	67361cc755255414dd3ba47ad0b98961cc944f612d001f35dd44f67b4460671e
Imphash	ad71acfa5be5581bd34fb2e9ffc57da6

79d503165d32176842fe386d96c04fb70f6ce1c8a485837957849297e625ea48

55 engines detected this file

79d503165d32176842fe386d96c04fb70f6ce1c8a485837957849297e625ea48
wp.exe
peexe

300.50 KB
Size

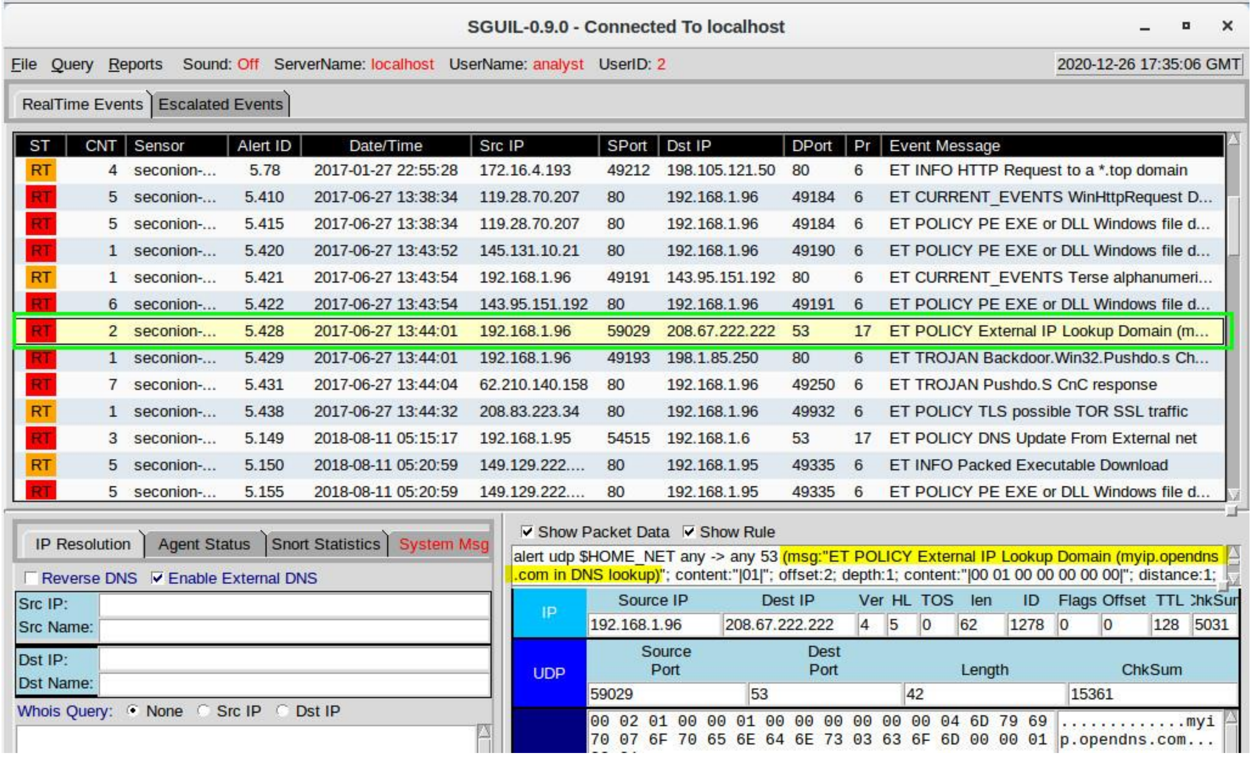
2020-11-30 20:38:44 UTC
25 days ago

Basic Properties

MD5	4da48f6423d5f7d75de281a674c2e620
SHA-1	93aa24323d60b2b053e158abf5a3e839f5ea58ae
SHA-256	79d503165d32176842fe386d96c04fb70f6ce1c8a485837957849297e625ea48
Vhash	035046555d1570b8z14hze3zffz
Authentihash	1d026a3ec67510fc3ca11d1b5e689041b670790a5ddabdc9c5f95c8f8758da50
Imphash	8e13617e4c8562cfb43fc1dd44b43653

c. Examine other alerts associated with the infected host during this timeframe and record your findings

ET POLICY External IP Lookup Domain (myip.opendns .com in DNS lookup) – infection started when the user of the **192.168.1.96** host performed a DNS lookup through a malicious domain – destination IP: **208.67.222.222**



Sound: Off ServerName: localhost UserName: analyst UserID: 2 2020-12-26 17:35:06 GMT

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	4	seconion-...	5.78	2017-01-27 22:55:28	172.16.4.193	49212	198.105.121.50	80	6	ET INFO HTTP Request to a *.top domain
RT	5	seconion-...	5.410	2017-06-27 13:38:34	119.28.70.207	80	192.168.1.96	49184	6	ET CURRENT_EVENTS WinHttpRequest D...
RT	5	seconion-...	5.415	2017-06-27 13:38:34	119.28.70.207	80	192.168.1.96	49184	6	ET POLICY PE EXE or DLL Windows file d...
RT	1	seconion-...	5.420	2017-06-27 13:43:52	145.131.10.21	80	192.168.1.96	49190	6	ET POLICY PE EXE or DLL Windows file d...
RT	1	seconion-...	5.421	2017-06-27 13:43:54	192.168.1.96	49191	143.95.151.192	80	6	ET CURRENT_EVENTS Terse alphanumeri...
RT	6	seconion-...	5.422	2017-06-27 13:43:54	143.95.151.192	80	192.168.1.96	49191	6	ET POLICY PE EXE or DLL Windows file d...
RT	2	seconion-...	5.428	2017-06-27 13:44:01	192.168.1.96	59029	208.67.222.222	53	17	ET POLICY External IP Lookup Domain (m...
RT	1	seconion-...	5.429	2017-06-27 13:44:01	192.168.1.96	49193	198.1.85.250	80	6	ET TROJAN Backdoor.Win32.Pushdo.s Ch...
RT	7	seconion-...	5.431	2017-06-27 13:44:04	62.210.140.158	80	192.168.1.96	49250	6	ET TROJAN Pushdo.S CnC response
RT	1	seconion-...	5.438	2017-06-27 13:44:32	208.83.223.34	80	192.168.1.96	49932	6	ET POLICY TLS possible TOR SSL traffic
RT	3	seconion-...	5.149	2018-08-11 05:15:17	192.168.1.95	54515	192.168.1.6	53	17	ET POLICY DNS Update From External net
RT	5	seconion-...	5.150	2018-08-11 05:20:59	149.129.222....	80	192.168.1.95	49335	6	ET INFO Packed Executable Download
RT	5	seconion-...	5.155	2018-08-11 05:20:59	149.129.222....	80	192.168.1.95	49335	6	ET POLICY PE EXE or DLL Windows file d...

☐ Reverse DNS ☑ Enable External DNS

Src IP:
Src Name:
Dst IP:
Dst Name:

Whois Query: ● None ○ Src IP ○ Dst IP

☑ Show Packet Data ☑ Show Rule

```
alert udp $HOME_NET any -> any 53 (msg:"ET POLICY External IP Lookup Domain (myip.opendns
.com in DNS lookup)"; content:"|01|"; offset:2; depth:1; content:"|00 01 00 00 00 00 00|"; distance:1;
```

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
	192.168.1.96	208.67.222.222	4	5	0	62	1278	0	0	128	5031

UDP	Source Port	Dest Port	Length	ChkSum
	59029	53	42	15361

```
00 02 01 00 00 01 00 00 00 00 00 00 04 6D 79 69   .............myi
70 07 6F 70 65 6E 64 6E 73 03 63 6F 6D 00 00 01   p.opendns.com...
```

Step 3: Report Your Findings

Summarizes your findings based on the information you have gathered from the previous parts, summarize your findings.

The host with IP 192.168.1.96, a PC running Windows, accessed a malicious domain for a DNS query, and was infected with the Pushdo trojan. The Pushdo trojan pretends to be an Apache webserver, listening on port 80. After infection, the Pushdo trojan downloads various malware. In the examined PC, three malwares were downloaded and installed – gerv.gun, trow.exe and wp.exe. These files were checked in virustotal.com, using their SHA256 hash, and verified as malware by most source.