



Griffith University

7906ICT Digital Forensics Assignment

Task 1

Gowtham Ravi
S5190712

Contents

Solution 1.....	3
Solution 2.	3
Solution 3.	6
Solution 4.	8
Solution 5.	9
Solution 6.	10
Solution 7.	12
Solution 8.	12
Solution 9.	13
Solution 10.	14
Solution 11.	14
Solution 12.	15
Executive Summary:.....	15

Solution 1.

- Network Miner 2.4 software is used to access the pcap file and to obtain information about the transmitting agents and when the first contact starts.
- The first communication occurrence is found by navigating to the Messages page.
- The first contact was from Mel to Daisy on 2018-10-01 at 2:17:42 UTC.
- The four agents are Mel, Daisy, Grant and Leo.
- The four agent's information are found as follows:
 - a) Mel - 192.168.1.76
 - b) Daisy - 192.168.1.72
 - c) Grant - 192.168.1.71
 - d) Leo - 192.168.1.73

NetworkMiner 2.4

File Tools Help

--- Select a network adapter in the list ---

Hosts (153) Files (4091) Images (42) Messages (37) Credentials (479) Sessions (2366) DNS (10028) Parameters (100128) Keywords Anomalies

Filter keyword: ☐ Case sensitive ExactPhrase Any column

Frame nr.	Source host	Destination host	From	To	Subject	Protocol	Timestamp
6856	192.168.1.76 [0]	192.168.1.66 [*] (Linux)		#shield	Daisy watch out there are suspected hydra agents i...	irc	2018-10-01 02:17:42 UTC
6857	192.168.1.66 [*] (Linux)	192.168.1.72 [0]	mel@192.168.1.76	#shield	Daisy watch out there are suspected hydra agents i...	irc	2018-10-01 02:17:42 UTC
7520	192.168.1.72 [0]	192.168.1.66 [*] (Linux)		#shield	I will keep a look out	irc	2018-10-01 02:17:53 UTC
7521	192.168.1.66 [*] (Linux)	192.168.1.76 [0]	daisy@daisy@192.168.1.72	#shield	I will keep a look out	irc	2018-10-01 02:17:53 UTC
14831	192.168.1.71 [0]	192.168.1.66 [*] (Linux)		#channel	My brother they may be on to us	irc	2018-10-01 02:20:03 UTC
14832	192.168.1.66 [*] (Linux)	192.168.1.73 [0]	grant@grant@192.168.1.71	#channel	My brother they may be on to us	irc	2018-10-01 02:20:03 UTC
15146	192.168.1.73 [0]	192.168.1.66 [*] (Linux)		#channel	I will be careful	irc	2018-10-01 02:20:11 UTC
15147	192.168.1.66 [*] (Linux)	192.168.1.71 [0]	leo@leo@192.168.1.73	#channel	I will be careful	irc	2018-10-01 02:20:11 UTC
16342	192.168.1.71 [0]	192.168.1.66 [*] (Linux)		#channel	See if you can tap into their emails	irc	2018-10-01 02:20:41 UTC
16344	192.168.1.66 [*] (Linux)	192.168.1.73 [0]	grant@grant@192.168.1.71	#channel	See if you can tap into their emails	irc	2018-10-01 02:20:41 UTC
16751	192.168.1.71 [0]	192.168.1.66 [*] (Linux)		#channel	I will make the key available to you	irc	2018-10-01 02:20:59 UTC
16752	192.168.1.66 [*] (Linux)	192.168.1.73 [0]	grant@grant@192.168.1.71	#channel	I will make the key available to you	irc	2018-10-01 02:20:59 UTC
16900	192.168.1.71 [0]	192.168.1.66 [*] (Linux)		#channel	Good luck	irc	2018-10-01 02:21:04 UTC
16902	192.168.1.66 [*] (Linux)	192.168.1.73 [0]	grant@grant@192.168.1.71	#channel	Good luck	irc	2018-10-01 02:21:04 UTC
17148	192.168.1.73 [0]	192.168.1.66 [*] (Linux)		#channel	Hail!	irc	2018-10-01 02:21:09 UTC
17149	192.168.1.66 [*] (Linux)	192.168.1.71 [0]	leo@leo@192.168.1.73	#channel	Hail!	irc	2018-10-01 02:21:09 UTC
24554	192.168.1.76 [0]	192.168.1.66 [*] (Linux)		#shield	Daisy there was a usb found in the car park, can y...	irc	2018-10-01 02:23:41 UTC
24555	192.168.1.66 [*] (Linux)	192.168.1.72 [0]	mel@mel@192.168.1.76	#shield	Daisy there was a usb found in the car park, can y...	irc	2018-10-01 02:23:41 UTC
25754	192.168.1.76 [0]	192.168.1.66 [*] (Linux)		#shield	Hydra may have made a mistake	irc	2018-10-01 02:24:02 UTC
25755	192.168.1.66 [*] (Linux)	192.168.1.72 [0]	mel@mel@192.168.1.76	#shield	Hydra may have made a mistake	irc	2018-10-01 02:24:02 UTC
26571	192.168.1.72 [0]	192.168.1.66 [*] (Linux)		#shield	No problem, I am on it	irc	2018-10-01 02:24:16 UTC
26572	192.168.1.66 [*] (Linux)	192.168.1.76 [0]	daisy@daisy@192.168.1.72	#shield	No problem, I am on it	irc	2018-10-01 02:24:16 UTC
26937	192.168.1.72 [0]	192.168.1.66 [*] (Linux)		#shield	Where is the usb	irc	2018-10-01 02:24:25 UTC
26939	192.168.1.66 [*] (Linux)	192.168.1.76 [0]	daisy@daisy@192.168.1.72	#shield	Where is the usb	irc	2018-10-01 02:24:25 UTC
27561	192.168.1.76 [0]	192.168.1.66 [*] (Linux)		#shield	I will upload it to the usual place	irc	2018-10-01 02:24:37 UTC
27563	192.168.1.66 [*] (Linux)	192.168.1.72 [0]	mel@mel@192.168.1.76	#shield	I will upload it to the usual place	irc	2018-10-01 02:24:37 UTC
35652	192.168.1.72 [0]	192.168.1.66 [*] (Linux)		#shield	thanks	irc	2018-10-01 02:26:08 UTC
66780	192.168.1.71 [0]	192.168.1.66 [*] (Linux)		#channel	we have to find out how much rogers knows	irc	2018-10-01 02:36:33 UTC
66781	192.168.1.66 [*] (Linux)	192.168.1.73 [0]	grant@grant@192.168.1.71	#channel	we have to find out how much rogers knows	irc	2018-10-01 02:36:33 UTC

Solution 2.

Network Miner 2.4 is used to identify the agents ' web browsers and operating systems.

- The host details of the agents found by navigating to the Hosts page.
- The web browsers and operating systems used by agents are found as follows:

Agent	Web Browser	Operating System
Mel	Chrome 59.0.3071.115	Windows 10 x64
Daisy	Firefox 56.0	Ubuntu 11 x64
Grant	-	-
Leo	Chrome 59.0.3071.115	Windows 10 x64

NetworkMiner 2.4

File Tools Help

-- Select a network adapter in the list --

Hosts (153) Files (4091) Images (42) Messages (37) Credentials (479) Sessions (2366) DNS (10028) Parameters (100128) Keywords Anomalies

Sort Hosts On: Hostname Sort and Refresh

- 192.168.1.254
- 192.168.1.75
- 192.168.1.74
- 192.168.1.53
- 192.168.1.66 [*] (Linux)
- 192.168.1.73 [0]
- 192.168.1.71 [0]
- 192.168.1.76 [0]
- IP: 192.168.1.76
- MAC: 0800278F5321
- NIC Vendor: PCS Systemtechnik GmbH
- MAC Age: 8/09/2000
- Hostname: 0
- OS: Unknown
- TTL: 64 (distance: 0)
- Open TCP Ports: 47542 45571 39294
- Sent: 6774 packets (87,343,321 Bytes), 0.00% cleartext (0 of 0 Bytes)
- Received: 5205 packets (6,639,899 Bytes), 0.00% cleartext (0 of 0 Bytes)
- Incoming sessions: 3
- Outgoing sessions: 239
- Host Details
 - Queried DNS names: ntp.ubuntu.com,ftp.shield.fm643.www.wotif.com,join.expediapartnercentral.com,secure.opinionlab.com,a.travel-assets.com,b.travel-assets.com,www.advertising.expedia.com,facebook.com,www.facebook.com,ir.expediainc
 - Web Browser User-Agent 1: Mozilla/5.0 Windows NT 10.0; Win64; x64 AppleWebKit/537.36(KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36
 - IRC Nick 1: mel
 - IRC Username 1: mel

NetworkMiner 2.4

File Tools Help

Select a network adapter in the list --

Hosts (153) Files (4091) Images (42) Messages (37) Credentials (479) Sessions (2366) DNS (10028) Parameters (100128) Keywords Anomalies

Sort Hosts On: Hostname

Sort and Refresh

- 192.168.1.71 [0]
- 192.168.1.76 [0]
- 192.168.1.72 [0]
 - IP: 192.168.1.72
 - MAC: 080027F4A9FA
 - NIC Vendor: PCS Systemtechnik GmbH
 - MAC Age: 8/09/2000
 - Hostname: 0
 - OS: Unknown
 - TTL: 64 (distance: 0)
 - Open TCP Ports:
 - Sent: 7175 packets (705,033 Bytes), 0.00% cleartext (0 of 0 Bytes)
 - Received: 7528 packets (15,746,013 Bytes), 0.00% cleartext (0 of 0 Bytes)
 - Incoming sessions: 0
 - Outgoing sessions: 414
 - Host Details
 - Queried DNS names : www.reddit.com, www.redditstatic.com, preview.reddit.it, twitter.com, a.thumbs.redditmedia.com, old.reddit.com, www.redditinc.com, streamable.com, www.redditmedia.com, www.redditblog.com, redditblog.com, about.reddit.c
 - Web Browser User-Agent 1 : Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:56.0) Gecko/20100101 Firefox/56.0
 - IRC Nick 1 : daisy
 - IRC Username 1 : daisy
- 204.79.197.203 [a-0003.a-msedge.net] [www.msn.com] (Other)
- 204.79.197.217 [a-0014.a-msedge.net] [odwebpl.trafficmanager.net, a-0014.dc-msedge.net, a-0014.a-msedge.net] [onedrive.live.com] [onedrive.com] (Other)
- 204.79.197.229 [a-0026.a-msedge.net] [www.bing.com, a-0026.a-msedge.net] [www.bing.com] (Other)
- 138.44.130.35 [a1711.w7.akamai.net] [search.abc.net.au, edgesuite.net] [search.abc.net.au] (Other)
- 138.44.130.32 [a1999.dscg2.akamai.net] [static-global-s-mn-com.akamai.net] [a1711.w7.akamai.net] [search.abc.net.au, edgesuite.net] [search.abc.net.au] [a248.e.akamai.net] (Other)
- 138.44.130.10 [a1999.dscg2.akamai.net] [static-global-s-mn-com.akamai.net] [a248.e.akamai.net] (Other)
- 203.2.218.214 [abc.net.au] (Other)
- 52.64.96.38 [affink-microsoft-com.ct.impactradius.com] [affink.microsoft.com] (Other)
- 13.54.28.245 [affink-microsoft-com.ct.impactradius.com] [affink.microsoft.com] (Other)
- 23.12.60.66 [aka.ms] [go.microsoft.com] (Other)
- 23.9.187.175 [aka.ms] [go.microsoft.com] (Other)

NetworkMiner 2.4

File Tools Help

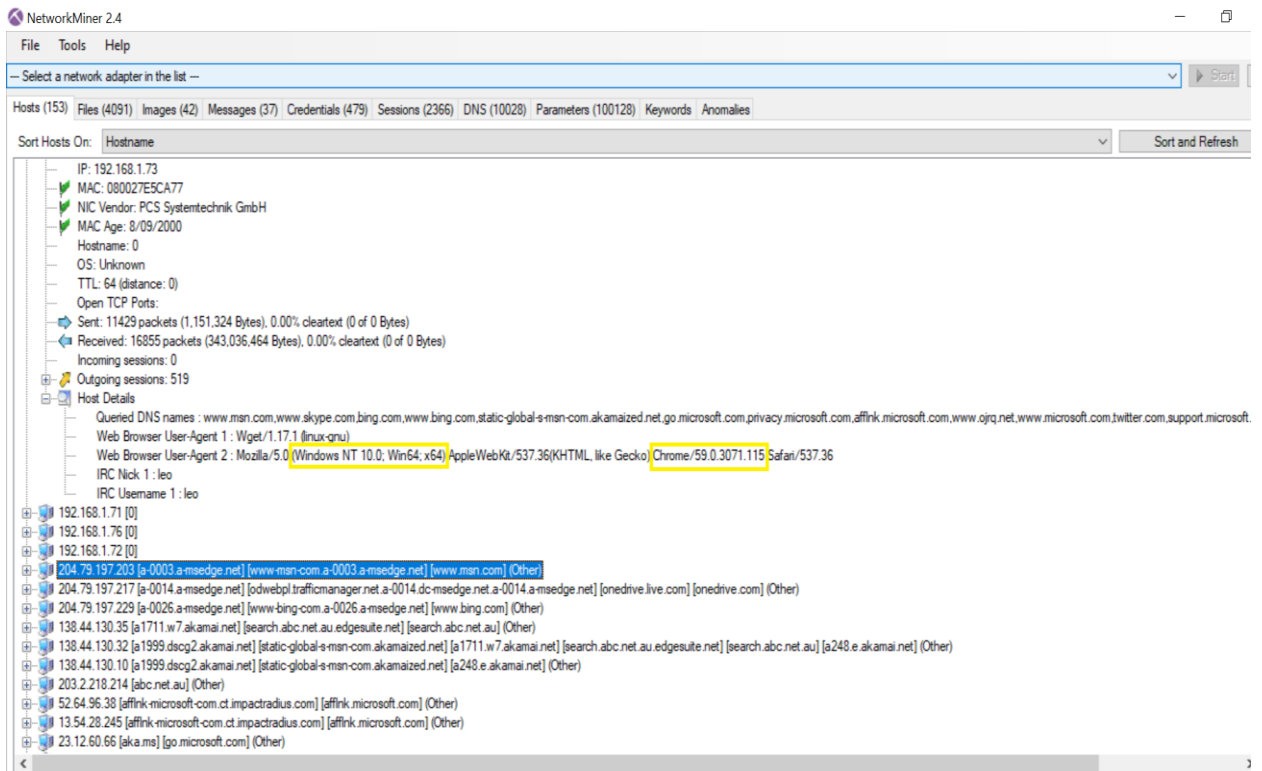
Select a network adapter in the list --

Hosts (153) Files (4091) Images (42) Messages (37) Credentials (479) Sessions (2366) DNS (10028) Parameters (100128) Keywords Anomalies

Sort Hosts On: Hostname

Sort and Refresh

- 192.168.1.254
- 192.168.1.75
- 192.168.1.74
- 192.168.1.53
- 192.168.1.66 [*] (Linux)
- 192.168.1.73 [0]
- 192.168.1.71 [0]
 - IP: 192.168.1.71
 - MAC: 0800277141E1
 - NIC Vendor: PCS Systemtechnik GmbH
 - MAC Age: 8/09/2000
 - Hostname: 0
 - OS: Unknown
 - TTL: 64 (distance: 0)
 - Open TCP Ports:
 - Sent: 980 packets (121,717 Bytes), 0.00% cleartext (0 of 0 Bytes)
 - Received: 1044 packets (933,287 Bytes), 0.00% cleartext (0 of 0 Bytes)
 - Incoming sessions: 0
 - Outgoing sessions: 77
 - Host Details
 - Queried DNS names : en.wikipedia.org, pt.wikipedia.org, meta.wikimedia.org, vi.wikipedia.org, ml.wikipedia.org, simple.wikipedia.org, en.wikibooks.org, ntp.ubuntu.com, uk.wikipedia.org
 - IRC Nick 1 : grant
 - IRC Username 1 : grant
- 192.168.1.76 [0]
- 192.168.1.72 [0]
 - IP: 192.168.1.72
 - MAC: 080027F4A9FA
 - NIC Vendor: PCS Systemtechnik GmbH
 - MAC Age: 8/09/2000
 - Hostname: 0
 - OS: Unknown



Solution 3.

- CarParkUSB.zip folder is opened from NetworkMiner 2.4 through the FILES tab. The file is accessed in Autopsy 4.12 software to find the double agent for H.Y.D.R.A.
- There were several deleted files inside the USB between them we could see an image in jpg format with the filename "**Winter_Seas_HYDRA_Castle_Logo_AEMH**" and Leo owns the USB as well.
- The agent named Leo is working for H.Y.D.R.A as a double agent .
- As the conversation between Leo and Grant suggest that the other double agent is **Grant**.

Autopsy 4.12.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Timeline Close Case Generate Report

Keyword Lists Keyword Search

Listing

File System

Table Thumbnail

Save Table as CSV

Name	S	C	Location	Modified Time	Change Time
Winter_Seas_HYDRA_Castle_Logo_AEMH.jpg			/img_Leo's USB.001/vol2/Winter_Seas_HYDRA_Castle...	2018-09-16 14:38:52 AEST	0000-00-00 0

Hex Text Application Message File Metadata Results Annotations Other Occurrences

0% 63% Reset

Tags Menu

NetworkMiner 2.4

File Tools Help

Select a network adapter in the list

Hosts (153) Files (4091) Images (42) Messages (37) Credentials (479) Sessions (2366) DNS (10028) Parameters (100128) Keywords Anomalies

Filter keyword: Case sensitive ExactPhrase Any column Clear

Frame nr.	Source host	Destination host	From	To	Subject	Protocol	Timestamp
6856	192.168.1.76 [0]	192.168.1.66 [*] (Linux)		#shield	Daisy watch out there are suspected hydra agents ...	irc	2018-10-01 02:17:42 UTC
6857	192.168.1.66 [*] (Linux)	192.168.1.72 [0]	.melmel@192.168.1.76	#shield	Daisy watch out there are suspected hydra agents ...	irc	2018-10-01 02:17:42 UTC
7520	192.168.1.72 [0]	192.168.1.66 [*] (Linux)		#shield	I will keep a look out	irc	2018-10-01 02:17:53 UTC
7521	192.168.1.66 [*] (Linux)	192.168.1.76 [0]	.daisy/daisy@192.168.1.72	#shield	I will keep a look out	irc	2018-10-01 02:17:53 UTC
14831	192.168.1.71 [0]	192.168.1.66 [*] (Linux)		#channel	My brother they may be on to us	irc	2018-10-01 02:20:03 UTC
14832	192.168.1.66 [*] (Linux)	192.168.1.73 [0]	.grant/grant@192.168.1.71	#channel	My brother they may be on to us	irc	2018-10-01 02:20:03 UTC
15146	192.168.1.73 [0]	192.168.1.66 [*] (Linux)		#channel	I will be careful	irc	2018-10-01 02:20:11 UTC
15147	192.168.1.66 [*] (Linux)	192.168.1.71 [0]	.leo/leo@192.168.1.73	#channel	I will be careful	irc	2018-10-01 02:20:11 UTC
16342	192.168.1.71 [0]	192.168.1.66 [*] (Linux)		#channel	See if you can tap into their emails	irc	2018-10-01 02:20:41 UTC
16344	192.168.1.66 [*] (Linux)	192.168.1.73 [0]	.grant/grant@192.168.1.71	#channel	See if you can tap into their emails	irc	2018-10-01 02:20:41 UTC
16751	192.168.1.71 [0]	192.168.1.66 [*] (Linux)		#channel	I will make the key available to you	irc	2018-10-01 02:20:59 UTC
16752	192.168.1.66 [*] (Linux)	192.168.1.73 [0]	.grant/grant@192.168.1.71	#channel	I will make the key available to you	irc	2018-10-01 02:20:59 UTC
16900	192.168.1.71 [0]	192.168.1.66 [*] (Linux)		#channel	Good luck	irc	2018-10-01 02:21:04 UTC
16902	192.168.1.66 [*] (Linux)	192.168.1.73 [0]	.grant/grant@192.168.1.71	#channel	Good luck	irc	2018-10-01 02:21:04 UTC
17148	192.168.1.73 [0]	192.168.1.66 [*] (Linux)		#channel	Hi!	irc	2018-10-01 02:21:09 UTC
17149	192.168.1.66 [*] (Linux)	192.168.1.71 [0]	.leo/leo@192.168.1.73	#channel	Hi!	irc	2018-10-01 02:21:09 UTC
24554	192.168.1.76 [0]	192.168.1.66 [*] (Linux)		#shield	Daisy there was a usb found in the car park, can y...	irc	2018-10-01 02:23:41 UTC
24555	192.168.1.66 [*] (Linux)	192.168.1.72 [0]	.melmel@192.168.1.76	#shield	Daisy there was a usb found in the car park, can y...	irc	2018-10-01 02:23:41 UTC
25754	192.168.1.76 [0]	192.168.1.66 [*] (Linux)		#shield	Hydra may have made a mistake	irc	2018-10-01 02:24:02 UTC
25755	192.168.1.66 [*] (Linux)	192.168.1.72 [0]	.melmel@192.168.1.76	#shield	Hydra may have made a mistake	irc	2018-10-01 02:24:02 UTC
26571	192.168.1.72 [0]	192.168.1.66 [*] (Linux)		#shield	No problem, I am on it	irc	2018-10-01 02:24:16 UTC
26572	192.168.1.66 [*] (Linux)	192.168.1.76 [0]	.daisy/daisy@192.168.1.72	#shield	No problem, I am on it	irc	2018-10-01 02:24:16 UTC
26937	192.168.1.72 [0]	192.168.1.66 [*] (Linux)	.daisy/daisy@192.168.1.72	#shield	Where is the usb	irc	2018-10-01 02:24:25 UTC
27561	192.168.1.76 [0]	192.168.1.66 [*] (Linux)		#shield	I will upload it to the usual place	irc	2018-10-01 02:24:37 UTC
27563	192.168.1.66 [*] (Linux)	192.168.1.72 [0]	.melmel@192.168.1.76	#shield	I will upload it to the usual place	irc	2018-10-01 02:24:37 UTC
35652	192.168.1.72 [0]	192.168.1.66 [*] (Linux)		#shield	thanks	irc	2018-10-01 02:26:08 UTC
66780	192.168.1.71 [0]	192.168.1.66 [*] (Linux)		#channel	we have to find out how much rogers knows	irc	2018-10-01 02:36:33 UTC
66781	192.168.1.66 [*] (Linux)	192.168.1.73 [0]	.grant/grant@192.168.1.71	#channel	we have to find out how much rogers knows	irc	2018-10-01 02:36:33 UTC

Solution 4.

- The steverogers zip file is shared with siftworkstation, and the zip file is compressed in the folder named “**steve**”.
- The command “python volatility/vol.py -f steverogers.vmem --profile=win7SP1x64 pslist” is used to list the information of applications which are running on the computer using the volatility which is implemented in python.

```
Terminal
File Edit View Search Terminal Help
ansforensics@stfworkstation -> ~
$ cd desktop
bash: cd: desktop: No such file or directory
ansforensics@stfworkstation -> ~
$ clear
ansforensics@stfworkstation -> ~
$ cd
ansforensics@stfworkstation -> ~
$ ls
Desktop Downloads Music Public Videos
Documents examples.desktop Pictures Templates
ansforensics@stfworkstation -> ~
$ cd Desktop
ansforensics@stfworkstation -> ~/Desktop
$ ls
cases Network-Forensics-Poster.pdf
DIR-Smartphone-Forensics-Poster.pdf Recall-Cheatsheet.pdf
VIR-Threat-Intel-Poster.pdf SIFT-Cheatsheet.pdf
Kind-Evil.pdf SIFT-REMux-Poster.pdf
Hex-File-Regex-Cheatsheet.pdf steve
Linux-Shell-survival-guide.pdf volatility-Cheatsheet.pdf
Memory-Forensics-Poster.pdf Windows-Forensics-Poster.pdf
Mount_points Windows-to-Uinx-Cheatsheet.pdf
ansforensics@stfworkstation -> ~/Desktop
$ cd steve
ansforensics@stfworkstation -> ~/D/steve
$ python volatility/vol.py -f steverogers.vmem --profile=win7SP1x64 pslist
python: can't open file 'volatility/vol.py': [Errno 2] No such file or directory
ansforensics@stfworkstation -> ~/D/steve
$ vol.py -f steverogers.vmem --profile=win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6
/usr/lib/python2.7/dist-packages/requests/__init__.py:83: RequestsDependencyWarning: Old version of cryptography ({1, 2, 3}) may cause slowdown.
RequestsDependencyWarning: RequestsDependencyWarning
ERROR : volatility.debug : The requested file doesn't exist
ansforensics@stfworkstation -> ~/D/steve
$ ls
No command 'ls' found, did you mean:
Command 'lrs' from package 'lrslib' (universe)
Command 'gss' from package 'libgsf-dev' (universe)
Command 'ass' from package 'lrpas' (multiverse)
Command 'as' from package 'lrouted' (main)
Command 'is' from package 'coreutils' (main)
Command 'lsw' from package 'suckless-tools' (universe)
Command 'lw' from package 'suckless-tools' (universe)
Command 'less' from package 'less' (main)
Command 'lvs' from package 'lvmd' (main)
Command 'lah' from package 'labeltext' (universe)
Command 'les' from package 'atm-tools' (universe)
Command 'lsou' from package 'nrlfs-tools' (universe)
ls: command not found
ansforensics@stfworkstation -> ~/D/steve
$ ls
ansforensics@stfworkstation -> ~/D/steve
$ cd steverogers/
ansforensics@stfworkstation -> ~/D/s/steverogers
```

```
Terminal
File Edit View Search Terminal Help
Python venvs Player
siftworkstation -> ~/sift/steveragers
$ python volatility/vol.py -f steveagers.vmem --profile=Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V) Name PID PPID Thds Hnds Sess Wow64 Start Exit
-----
0xfffffa800cc20800 System 4 88 550 ----- 0 2018-09-18 13:39:17 UTC+0000
0xfffffa800da09a00 smss.exe 264 4 2 29 ----- 0 2018-09-18 13:39:17 UTC+0000
0xfffffa800e0a1400 csrss.exe 352 340 8 527 0 0 2018-09-18 13:39:18 UTC+0000
0xfffffa800d6d0000 wininit.exe 392 392 3 76 0 0 2018-09-18 13:39:18 UTC+0000
0xfffffa800d0d1f00 csrss.exe 400 384 10 309 1 0 2018-09-18 13:39:18 UTC+0000
0xfffffa800eacfb00 services.exe 464 392 7 225 0 0 2018-09-18 13:39:18 UTC+0000
0xfffffa800e024900 lsass.exe 472 392 7 724 0 0 2018-09-18 13:39:18 UTC+0000
0xfffffa800e1c3300 lsm.exe 480 392 10 149 0 0 2018-09-18 13:39:18 UTC+0000
0xfffffa800e0e4600 winlogon.exe 492 384 3 110 1 0 2018-09-18 13:39:18 UTC+0000
0xfffffa800ebf3350 svchost.exe 612 464 10 358 0 0 2018-09-18 13:39:19 UTC+0000
0xfffffa800ec23600 vmacthlp.exe 676 464 3 55 0 0 2018-09-18 13:39:19 UTC+0000
0xfffffa800ebfbf00 svchost.exe 708 464 7 296 0 0 2018-09-18 13:39:19 UTC+0000
0xfffffa800ec53b00 svchost.exe 760 464 22 576 0 0 2018-09-18 13:39:19 UTC+0000
0xfffffa800ec0ca50 svchost.exe 848 464 26 534 0 0 2018-09-18 13:39:19 UTC+0000
0xfffffa800eb80000 svchost.exe 924 464 18 727 0 0 2018-09-18 13:39:19 UTC+0000
0xfffffa800ed0f590 svchost.exe 968 464 41 1099 0 0 2018-09-18 13:39:19 UTC+0000
0xfffffa800ed7c600 svchost.exe 1056 464 14 369 0 0 2018-09-18 13:39:19 UTC+0000
0xfffffa800ed3cd00 spoolsv.exe 1172 464 17 119 0 0 2018-09-18 13:39:20 UTC+0000
0xfffffa800e0c1900 svchost.exe 1208 464 19 809 0 0 2018-09-18 13:39:20 UTC+0000
0xfffffa800e0a1b00 svchost.exe 1320 464 10 141 0 0 2018-09-18 13:39:20 UTC+0000
0xfffffa800ebf0a00 VGAuthService.exe 1424 464 3 98 0 0 2018-09-18 13:39:20 UTC+0000
0xfffffa800ebfca00 vmtoolsd.exe 1472 464 9 316 0 0 2018-09-18 13:39:20 UTC+0000
0xfffffa800ef02420 VMToolsd.exe 1760 612 10 206 0 0 2018-09-18 13:39:21 UTC+0000
0xfffffa800bf04e00 dlh.exe 1848 464 15 203 0 0 2018-09-18 13:39:21 UTC+0000
0xfffffa800ef0d870 msctf.exe 1932 464 13 152 0 0 2018-09-18 13:39:22 UTC+0000
0xfffffa800ef03300 VMToolsd.exe 204 612 10 143 0 0 2018-09-18 13:39:21 UTC+0000
0xfffffa800ef89900 taskhost.exe 2340 464 9 208 1 0 2018-09-18 13:41:02 UTC+0000
0xfffffa800ef2d2a0 dm.exe 2392 848 5 80 1 0 2018-09-18 13:41:02 UTC+0000
0xfffffa800ef03600 explorer.exe 2448 2360 26 807 0 0 2018-09-18 13:41:02 UTC+0000
0xfffffa800ef01900 vmtoolsd.exe 2636 1448 8 209 1 0 2018-09-18 13:41:02 UTC+0000
0xfffffa800ef00600 GoogleCrashHan 2796 2798 4 83 0 0 2018-09-18 13:41:07 UTC+0000
0xfffffa800dadfd00 GoogleCrashHan 2808 2708 4 74 0 0 2018-09-18 13:41:07 UTC+0000
0xfffffa800ebf0000 SearchIndexer.exe 2896 464 11 960 0 0 2018-09-18 13:41:08 UTC+0000
0xfffffa800d30a000 wmpnetwk.exe 1088 464 13 420 0 0 2018-09-18 13:41:08 UTC+0000
0xfffffa800d34b000 svchost.exe 272 464 22 288 0 0 2018-09-18 13:41:09 UTC+0000
0xfffffa800d313000 svchost.exe 2108 464 8 349 0 0 2018-09-18 13:41:10 UTC+0000
0xfffffa800c0ef000 mcsorvsw.exe 2292 464 5 85 0 1 2018-09-18 13:41:21 UTC+0000
0xfffffa800c0f7240 mcsorvsw.exe 2080 464 5 78 0 0 2018-09-18 13:41:21 UTC+0000
0xfffffa800c076000 svchost.exe 3036 464 13 351 0 0 2018-09-18 13:41:21 UTC+0000
0xfffffa800c033600 chrome.exe 3168 2440 37 1143 0 0 2018-09-18 13:41:23 UTC+0000
0xfffffa800c0f98f0 chrome.exe 3176 3168 7 82 1 0 2018-09-18 13:41:33 UTC+0000
0xfffffa800c0f1260 chrome.exe 3208 3168 2 59 1 0 2018-09-18 13:41:33 UTC+0000
0xfffffa800c0f1a00 chrome.exe 3356 3168 10 210 1 0 2018-09-18 13:41:33 UTC+0000
0xfffffa800c0f5b00 chrome.exe 3448 3168 15 186 0 0 2018-09-18 13:41:34 UTC+0000
0xfffffa800d558120 chrome.exe 2052 3168 17 229 1 0 2018-09-18 13:41:44 UTC+0000
0xfffffa800efc2a60 chrome.exe 3600 3168 14 178 1 0 2018-09-18 13:41:50 UTC+0000
0xfffffa800c0f3900 vmtoolsd.exe 872 464 9 6 0 0 2018-09-18 13:42:23 UTC+0000
0xfffffa800ec31f00 mspsalnt.exe 2976 2448 6 192 1 0 2018-09-18 13:46:16 UTC+0000
0xfffffa800d2d0000 svchost.exe 4084 464 7 108 0 0 2018-09-18 13:46:16 UTC+0000

siftworkstation -> ~/sift/steveragers
$ python volatility/vol.py -f steveagers.vmem --profile=Win7SP1x64 pstree
```

- The command “python volatility/vol.py -f steverogers.vmem --profile=Win7SP1x64 pstree” is used to find the parent & child processes.


```

Terminal
File Edit View Search Terminal Help
python volatility/vol.py -f steverogers.vmem --profile=Win7SP1x64 pstree
Volatility Foundation Volatility Framework 2.6.1
Name PId PPId Thds Hnds Time
-----
0xfffffa80e7d0d000 wininit.exe 392 340 3 76 2018-09-18 13:39:18 UTC+0000
0xfffffa80e7a53000 lsass.exe 480 392 10 149 2018-09-18 13:39:18 UTC+0000
0xfffffa80e7a53000 services.exe 464 392 7 225 2018-09-18 13:39:18 UTC+0000
0xfffffa80e73a0000 wsmnetwk.exe 1888 464 13 420 2018-09-18 13:41:08 UTC+0000
0xfffffa80e724e000 ncsrsvw.exe 2880 464 5 78 2018-09-18 13:41:21 UTC+0000
0xfffffa80e7a53000 svchost.exe 1932 464 13 152 2018-09-18 13:39:22 UTC+0000
0xfffffa80e7a0b000 VGAuthService.exe 1424 464 3 90 2018-09-18 13:39:20 UTC+0000
0xfffffa80e7d0c000 spoolsv.exe 1172 464 14 319 2018-09-18 13:39:20 UTC+0000
0xfffffa80e7c0b000 svchost.exe 324 464 18 727 2018-09-18 13:39:19 UTC+0000
0xfffffa80e7c0b000 svchost.exe 1056 464 14 369 2018-09-18 13:39:19 UTC+0000
0xfffffa80e7c20000 vmacthlp.exe 676 464 3 55 2018-09-18 13:39:19 UTC+0000
0xfffffa80e7c1b000 svchost.exe 1320 464 10 143 2018-09-18 13:39:20 UTC+0000
0xfffffa80e7c4b000 svchost.exe 1288 464 19 309 2018-09-18 13:39:20 UTC+0000
0xfffffa80e7d4a000 svchost.exe 4884 464 7 108 2018-09-18 13:46:16 UTC+0000
0xfffffa80e7c4b000 vmtoolsd.exe 1472 464 9 318 2018-09-18 13:39:20 UTC+0000
0xfffffa80e7c2b000 SearchIndexer.exe 2896 464 11 606 2018-09-18 13:41:08 UTC+0000
0xfffffa80e7f1b000 svchost.exe 788 464 7 296 2018-09-18 13:39:19 UTC+0000
0xfffffa80e7d0d000 dlhost.exe 1848 464 41 1009 2018-09-18 13:39:19 UTC+0000
0xfffffa80e7c9d000 wuaucnt.exe 872 968 4 96 2018-09-18 13:42:23 UTC+0000
0xfffffa80e7d13100 svchost.exe 2188 464 8 349 2018-09-18 13:41:10 UTC+0000
0xfffffa80e7c4b000 dlhost.exe 1848 464 15 103 2018-09-18 13:39:21 UTC+0000
0xfffffa80e7f89000 taskhost.exe 2340 464 9 208 2018-09-18 13:41:02 UTC+0000
0xfffffa80e7c7b000 svchost.exe 3036 464 13 351 2018-09-18 13:41:21 UTC+0000
0xfffffa80e7c4b000 chrome.exe 848 464 26 534 2018-09-18 13:39:19 UTC+0000
0xfffffa80e72da000 dm.exe 2392 848 5 88 2018-09-18 13:41:02 UTC+0000
0xfffffa80e7365000 svchost.exe 612 464 10 358 2018-09-18 13:39:19 UTC+0000
0xfffffa80e7f3a000 WmPrvSE.exe 964 612 10 266 2018-09-18 13:39:21 UTC+0000
0xfffffa80e7c4b000 svchost.exe 1760 612 10 266 2018-09-18 13:39:21 UTC+0000
0xfffffa80e7c4b000 svchost.exe 272 464 22 288 2018-09-18 13:41:09 UTC+0000
0xfffffa80e7c0b000 ncsrsvw.exe 2292 464 5 85 2018-09-18 13:41:21 UTC+0000
0xfffffa80e7c3b000 svchost.exe 760 464 22 570 2018-09-18 13:39:19 UTC+0000
0xfffffa80e7d49000 lsass.exe 472 392 7 724 2018-09-18 13:39:18 UTC+0000
0xfffffa80e7a53000 csrss.exe 352 340 8 627 2018-09-18 13:39:18 UTC+0000
0xfffffa80e7c29b00 System 4 0 88 559 2018-09-18 13:39:17 UTC+0000
0xfffffa80e7a53000 smss.exe 264 4 2 29 2018-09-18 13:39:17 UTC+0000
0xfffffa80e7c4b000 GoogleCrashHan 2796 2784 4 83 2018-09-18 13:39:41 UTC+0000
0xfffffa80e7d4d000 GoogleCrashHan 2888 2784 4 74 2018-09-18 13:41:07 UTC+0000
0xfffffa80e7f1b000 csrss.exe 480 384 10 309 2018-09-18 13:39:18 UTC+0000
0xfffffa80e7c4b000 csrss.exe 492 384 3 119 2018-09-18 13:39:18 UTC+0000
0xfffffa80e7f16000 explorer.exe 2448 2360 26 807 2018-09-18 13:41:02 UTC+0000
0xfffffa80e7c18f00 mspaint.exe 2976 2448 6 192 2018-09-18 13:40:16 UTC+0000
0xfffffa80e7c4b000 chrome.exe 3168 2448 37 1143 2018-09-18 13:41:33 UTC+0000
0xfffffa80e7c5b000 chrome.exe 3448 3168 15 206 2018-09-18 13:41:34 UTC+0000
0xfffffa80e7c4b000 chrome.exe 3356 3168 10 210 2018-09-18 13:41:33 UTC+0000
0xfffffa80e7c31b00 chrome.exe 2892 3168 17 229 2018-09-18 13:41:44 UTC+0000
0xfffffa80e7c12000 chrome.exe 3208 3168 2 59 2018-09-18 13:41:33 UTC+0000
0xfffffa80e7c0f900 chrome.exe 3176 3168 7 82 2018-09-18 13:41:33 UTC+0000
0xfffffa80e7c4b000 chrome.exe 3608 3168 14 178 2018-09-18 13:41:50 UTC+0000
0xfffffa80e7c19b00 vmtoolsd.exe 2636 2448 8 209 2018-09-18 13:41:02 UTC+0000
python volatility/vol.py -f steverogers.vmem --profile=Win7SP1x64 psxview

```

- The command “python volatility/vol.py -f steverogers.vmem --profile=Win7SP1x64 psxview” is used to identify the hidden processes.

```

Terminal
File Edit View Search Terminal Help
python volatility/vol.py -f steverogers.vmem --profile=Win7SP1x64 psxview
Volatility Foundation Volatility Framework 2.6.1
Name PId PPId Thds Hnds Time ExitTime
-----
0xfffffa80e7d0d000 wininit.exe 392 340 3 76 2018-09-18 13:39:18 UTC+0000
0xfffffa80e7a53000 lsass.exe 480 392 10 149 2018-09-18 13:39:18 UTC+0000
0xfffffa80e7a53000 services.exe 464 392 7 225 2018-09-18 13:39:18 UTC+0000
0xfffffa80e73a0000 wsmnetwk.exe 1888 464 13 420 2018-09-18 13:41:08 UTC+0000
0xfffffa80e724e000 ncsrsvw.exe 2880 464 5 78 2018-09-18 13:41:21 UTC+0000
0xfffffa80e7a53000 svchost.exe 1932 464 13 152 2018-09-18 13:39:22 UTC+0000
0xfffffa80e7a0b000 VGAuthService.exe 1424 464 3 90 2018-09-18 13:39:20 UTC+0000
0xfffffa80e7d0c000 spoolsv.exe 1172 464 14 319 2018-09-18 13:39:20 UTC+0000
0xfffffa80e7c0b000 svchost.exe 324 464 18 727 2018-09-18 13:39:19 UTC+0000
0xfffffa80e7c0b000 svchost.exe 1056 464 14 369 2018-09-18 13:39:19 UTC+0000
0xfffffa80e7c20000 vmacthlp.exe 676 464 3 55 2018-09-18 13:39:19 UTC+0000
0xfffffa80e7c1b000 svchost.exe 1320 464 10 143 2018-09-18 13:39:20 UTC+0000
0xfffffa80e7c4b000 svchost.exe 1288 464 19 309 2018-09-18 13:39:20 UTC+0000
0xfffffa80e7d4a000 svchost.exe 4884 464 7 108 2018-09-18 13:46:16 UTC+0000
0xfffffa80e7c4b000 vmtoolsd.exe 1472 464 9 318 2018-09-18 13:39:20 UTC+0000
0xfffffa80e7c2b000 SearchIndexer.exe 2896 464 11 606 2018-09-18 13:41:08 UTC+0000
0xfffffa80e7f1b000 svchost.exe 788 464 7 296 2018-09-18 13:39:19 UTC+0000
0xfffffa80e7d0d000 dlhost.exe 1848 464 41 1009 2018-09-18 13:39:19 UTC+0000
0xfffffa80e7c9d000 wuaucnt.exe 872 968 4 96 2018-09-18 13:42:23 UTC+0000
0xfffffa80e7d13100 svchost.exe 2188 464 8 349 2018-09-18 13:41:10 UTC+0000
0xfffffa80e7c4b000 dlhost.exe 1848 464 15 103 2018-09-18 13:39:21 UTC+0000
0xfffffa80e7f89000 taskhost.exe 2340 464 9 208 2018-09-18 13:41:02 UTC+0000
0xfffffa80e7c7b000 svchost.exe 3036 464 13 351 2018-09-18 13:41:21 UTC+0000
0xfffffa80e7c4b000 chrome.exe 848 464 26 534 2018-09-18 13:39:19 UTC+0000
0xfffffa80e72da000 dm.exe 2392 848 5 88 2018-09-18 13:41:02 UTC+0000
0xfffffa80e7365000 svchost.exe 612 464 10 358 2018-09-18 13:39:19 UTC+0000
0xfffffa80e7f3a000 WmPrvSE.exe 964 612 10 266 2018-09-18 13:39:21 UTC+0000
0xfffffa80e7c4b000 svchost.exe 1760 612 10 266 2018-09-18 13:39:21 UTC+0000
0xfffffa80e7c4b000 svchost.exe 272 464 22 288 2018-09-18 13:41:09 UTC+0000
0xfffffa80e7c0b000 ncsrsvw.exe 2292 464 5 85 2018-09-18 13:41:21 UTC+0000
0xfffffa80e7c3b000 svchost.exe 760 464 22 570 2018-09-18 13:39:19 UTC+0000
0xfffffa80e7d49000 lsass.exe 472 392 7 724 2018-09-18 13:39:18 UTC+0000
0xfffffa80e7a53000 csrss.exe 352 340 8 627 2018-09-18 13:39:18 UTC+0000
0xfffffa80e7c29b00 System 4 0 88 559 2018-09-18 13:39:17 UTC+0000
0xfffffa80e7a53000 smss.exe 264 4 2 29 2018-09-18 13:39:17 UTC+0000
0xfffffa80e7c4b000 GoogleCrashHan 2796 2784 4 83 2018-09-18 13:39:41 UTC+0000
0xfffffa80e7d4d000 GoogleCrashHan 2888 2784 4 74 2018-09-18 13:41:07 UTC+0000
0xfffffa80e7f1b000 csrss.exe 480 384 10 309 2018-09-18 13:39:18 UTC+0000
0xfffffa80e7c4b000 csrss.exe 492 384 3 119 2018-09-18 13:39:18 UTC+0000
0xfffffa80e7f16000 explorer.exe 2448 2360 26 807 2018-09-18 13:41:02 UTC+0000
0xfffffa80e7c18f00 mspaint.exe 2976 2448 6 192 2018-09-18 13:40:16 UTC+0000
0xfffffa80e7c4b000 chrome.exe 3168 2448 37 1143 2018-09-18 13:41:33 UTC+0000
0xfffffa80e7c5b000 chrome.exe 3448 3168 15 206 2018-09-18 13:41:34 UTC+0000
0xfffffa80e7c4b000 chrome.exe 3356 3168 10 210 2018-09-18 13:41:33 UTC+0000
0xfffffa80e7c31b00 chrome.exe 2892 3168 17 229 2018-09-18 13:41:44 UTC+0000
0xfffffa80e7c12000 chrome.exe 3208 3168 2 59 2018-09-18 13:41:33 UTC+0000
0xfffffa80e7c0f900 chrome.exe 3176 3168 7 82 2018-09-18 13:41:33 UTC+0000
0xfffffa80e7c4b000 chrome.exe 3608 3168 14 178 2018-09-18 13:41:50 UTC+0000
0xfffffa80e7c19b00 vmtoolsd.exe 2636 2448 8 209 2018-09-18 13:41:02 UTC+0000
python volatility/vol.py -f steverogers.vmem --profile=Win7SP1x64 psxview

```

It is found that there are no suspicious files.

Solution 5.

- The web pages running in steve rogers system is found by using the command “python volatility/vol.py --plugins=plugins/ -f steverogers.vmem chromehistory”.
- The web pages which steve rogers visited are listed as follows:

- Gmail
- Google
- Last Pass

```

ERROR : volatility.debug : You must specify something to do. (try -h)
sansforensics@siftworkstation -> ~/D/s/steverogers
$ python volatility/vol.py --plugins=plugins/ -f steverogers.vmem chromehistory
Volatility Foundation Volatility Framework 2.6.1
ERROR : volatility.debug : You must specify something to do. (try -h)
sansforensics@siftworkstation -> ~/D/s/steverogers
$ python volatility/vol.py --plugins=plugins/ -f steverogers.vmem chromehistory
Volatility Foundation Volatility Framework 2.6.1
Index URL ID bioskbd.py bioskbd.pyc chromehistory.py chromehistory.pyc Title cmdline.py cmdline.pyc common.py common.pyc connections.py connections.pyc connscan.py connscan.pyc
-----
21 https://www.google.com.au/search?q=agen...&blw=772&bih=456&imgsrc=...&SqBwvFV-s13M: agent carter - Google Search
N/A
22 https://www.google.com.au/search?q=agen...&blw=772&bih=456&imgsrc=...&SqBwvFV-s13M: agent carter - Google Search
N/A
20 https://www.google.com.au/search?q=agen...&blw=772&bih=456&imgsrc=...&SqBwvFV-s13M: agent carter - Google Search
N/A
19 https://www.google.com.au/search?q=agen...&blw=772&bih=456&imgsrc=...&SqBwvFV-s13M: agent carter - Google Search
N/A
16 https://www.google.com.au/search?q=agen...&blw=772&bih=456&imgsrc=...&SqBwvFV-s13M: agent carter - Google Search
N/A
15 https://www.google.com.au/search?q=agen...&blw=772&bih=456&imgsrc=...&SqBwvFV-s13M: agent carter - Google Search
N/A
14 https://www.google.com.au/search?q=agen...&blw=772&bih=456&imgsrc=...&SqBwvFV-s13M: agent carter - Google Search
N/A
12 https://mail.google.com/mail/#inbox
N/A
13 https://mail.google.com/mail/#inbox
N/A
8 https://mail.google.com/mail/#inbox
N/A
11 https://mail.google.com/mail/#inbox
N/A
10 https://mail.google.com/mail/#inbox
N/A
9 https://mail.google.com/mail/#inbox
N/A
22 https://www.google.com.au/search?q=agen...&blw=772&bih=456&imgsrc=...&SqBwvFV-s13M: agent carter - Google Search
N/A
7 chrome-extension://hdokiejnpimakedhajhdlcegeplioahd/vault.html
N/A
6 https://www.lastpass.com/get-started
N/A
5 https://www.google.com.au/search?q=lastpass...&blw=772&bih=456&imgsrc=...&SqBwvFV-s13M: lastpass - Google Search
N/A
4 https://accounts.google.com/CheckCookie...&blw=772&bih=456&imgsrc=...&SqBwvFV-s13M: Google Accounts
N/A
3 https://accounts.google.com/signin/v2/s...&blw=772&bih=456&imgsrc=...&SqBwvFV-s13M: Sign in - Google accounts
N/A
2 https://accounts.google.com/signin/v2/s...&blw=772&bih=456&imgsrc=...&SqBwvFV-s13M: Sign in - Google accounts
N/A
1 https://accounts.google.com/signin/v2/s...&blw=772&bih=456&imgsrc=...&SqBwvFV-s13M: Sign in - Google accounts
N/A

```

Figure 5.

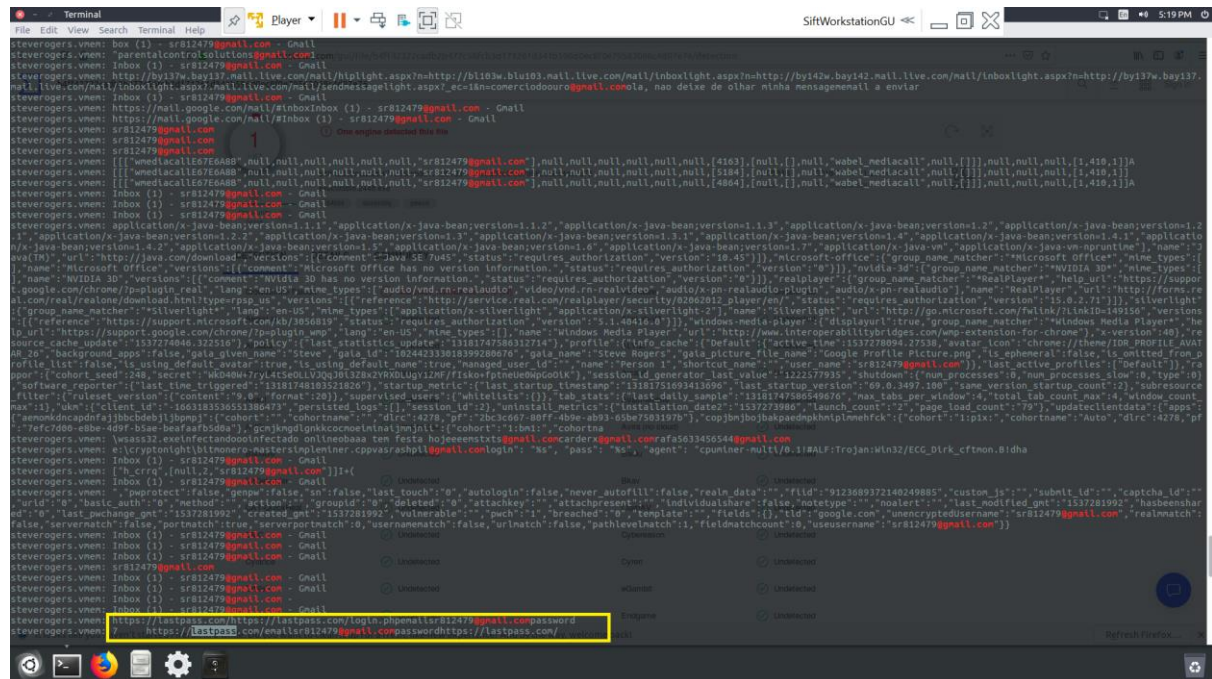
Solution 6.

- The Steve roger email address is found by using the command “strings -f steverogers.vmem | grep @gmail.com”. The grep command is used to search the strings in the file.
- Email - sr812479@gmail.com

Solution 7.

The steve rogers password cannot be found as he used the last pass website to manage his passwords.

From Figure 7, it is found that Steve Rogers created an account in the last pass website and managed his password in it.



Solution 8.

- The Steve roger pc, which is infected with a virus, is found by using the command “python volatility/vol.py -f steverogers.vmem --profile=Win7SP1x64 iehistory”.
- The image file in jpeg format with a filename as “agent-carter.jpeg” located at “C:/Users/Steve%20Rogers/Downloads/agent-carter.jpeg” is the infected file.
- The command “python volatility/vol.py -f steverogers.vmem --profile=Win7SP1x64 procdump --dump-dir=dumpfiles/” is used to monitor the application to create a dump file.
- Using the <https://www.virustotal.com>, an Ad-Aware virus was found.


```

Terminal
File Edit View Search Terminal Help
SiftWorkstationGU
2:55 PM

C:\Users\steve\Documents> cd ~\sift\steverogers
C:\Users\steve\Documents> python volatility.py --profile=Win7SP1x64 --memory=steverogers.vmem --dump-dir=dumpfiles/
Volatility Foundation Volatility Framework 2.6.1
Process: 2448 explorer.exe
Cache type: 'DESI' at 0x587229b
Last modified: 2018-09-18 23:46:10 UTC-0000
Last accessed: 2018-09-18 13:46:10 UTC-0000
URL: Steve RogersFile:///C:/Users/Steve20Rogers/Downloads/agent-carter.jpeg
C:\Users\steve\Documents> cd ~\sift\steverogers
C:\Users\steve\Documents> python volatility.py --profile=Win7SP1x64 --memory=steverogers.vmem --dump-dir=dumpfiles/
Volatility Foundation Volatility Framework 2.6.1
Process(V) ImageBase Name Result
-----
0xfffffa800cc29b00 0xfffffa800cc29b00 System Error: PEB at 0x0 is unavailable (possibly due to paging)
0xfffffa800da96a00 0xfffffa800da96a00 smss.exe Error: PEB at 0x7ffffda000 is unavailable (possibly due to paging)
0xfffffa800e0b1e40 0xfffffa800e0b1e40 csrss.exe Error: ImageBaseAddress at 0x4a0f0000 is unavailable (possibly due to paging)
0xfffffa800e76d6d0 0xfffffa800e76d6d0 wininit.exe Error: PEB at 0x7ffffd9000 is unavailable (possibly due to paging)
0xfffffa800d7ff060 0xfffffa800d7ff060 csrss.exe OK: executable.400.exe
0xfffffa800ecf7000 0xfffffa800ecf7000 services.exe OK: executable.464.exe
0xfffffa800eb2490 0xfffffa800eb2490 lsass.exe Error: ImageBaseAddress at 0xffc00000 is unavailable (possibly due to paging)
0xfffffa800eaf5330 0xfffffa800eaf5330 lan.exe Error: ImageBaseAddress at 0xff850000 is unavailable (possibly due to paging)
0xfffffa800b46c6f0 0xfffffa800b46c6f0 winlogon.exe OK: executable.492.exe
0xfffffa800ebf3630 0xfffffa800ebf3630 svchost.exe OK: executable.612.exe
0xfffffa800ec220a0 0xfffffa800ec220a0 vmacthlp.exe Error: ImageBaseAddress at 0x13f0f0000 is unavailable (possibly due to paging)
0xfffffa800ebf7f00 0xfffffa800ebf7f00 svchost.exe OK: executable.700.exe
0xfffffa800ec33b00 0xfffffa800ec33b00 svchost.exe OK: executable.700.exe
0xfffffa800ec8a5c0 0xfffffa800ec8a5c0 svchost.exe OK: executable.848.exe
0xfffffa800ec30b00 0xfffffa800ec30b00 svchost.exe Error: ImageBaseAddress at 0xff200000 is unavailable (possibly due to paging)
0xfffffa800edf530 0xfffffa800edf530 svchost.exe OK: executable.908.exe
0xfffffa800ed7c0a0 0xfffffa800ed7c0a0 svchost.exe Error: ImageBaseAddress at 0xff200000 is unavailable (possibly due to paging)
0xfffffa800edc3b0 0xfffffa800edc3b0 svchost.exe Error: ImageBaseAddress at 0xff200000 is unavailable (possibly due to paging)
0xfffffa800edc4b00 0xfffffa800edc4b00 svchost.exe Error: ImageBaseAddress at 0xff200000 is unavailable (possibly due to paging)
0xfffffa800e9a1b00 0xfffffa800e9a1b00 svchost.exe Error: ImageBaseAddress at 0xff200000 is unavailable (possibly due to paging)
0xfffffa800efab00 0xfffffa800efab00 vdsutil.exe OK: executable.1472.exe
0xfffffa800efab00 0xfffffa800efab00 vntool.exe OK: executable.1472.exe
0xfffffa800f0242c0 0xfffffa800f0242c0 WMIrvsl.exe OK: executable.1760.exe
0xfffffa800f04e00 0xfffffa800f04e00 dlhst.exe OK: executable.1848.exe
0xfffffa800f0d70d0 0xfffffa800f0d70d0 msdtc.exe Error: ImageBaseAddress at 0x13ff00000 is unavailable (possibly due to paging)
0xfffffa800f0530 0xfffffa800f0530 WMIrvsl.exe OK: executable.904.exe
0xfffffa800f05900 0xfffffa800f05900 svchost.exe OK: executable.2180.exe
0xfffffa800f2d2a80 0xfffffa800f2d2a80 dm.exe OK: executable.2392.exe
0xfffffa800f107000 0xfffffa800f107000 explorer.exe OK: executable.2448.exe
0xfffffa800f1900 0xfffffa800f1900 explorer.exe Error: ImageBaseAddress at 0x13f7a0000 is unavailable (possibly due to paging)
0xfffffa800ce9000 0xfffffa800ce9000 GoogleCrashhan Error: PEB at 0x7efdf000 is unavailable (possibly due to paging)
0xfffffa800da96a00 0xfffffa800da96a00 GoogleCrashhan OK: executable.2880.exe
0xfffffa800ebf3630 0xfffffa800ebf3630 SearchIndexer.exe OK: executable.2896.exe
0xfffffa800d3ab00 0xfffffa800d3ab00 wmpnetw.exe OK: executable.1888.exe
0xfffffa800d3ab00 0xfffffa800d3ab00 wmpnetw.exe Error: ImageBaseAddress at 0xff200000 is unavailable (possibly due to paging)
0xfffffa800d3ab00 0xfffffa800d3ab00 wmpnetw.exe OK: executable.2180.exe
0xfffffa800c72400 0xfffffa800c72400 mscorsvw.exe Error: ImageBaseAddress at 0x3d00000 is unavailable (possibly due to paging)
0xfffffa800c72400 0xfffffa800c72400 mscorsvw.exe Error: ImageBaseAddress at 0x13f4f0000 is unavailable (possibly due to paging)
0xfffffa800c72400 0xfffffa800c72400 mscorsvw.exe OK: executable.3036.exe
0xfffffa800d98800 0xfffffa800d98800 chrome.exe OK: executable.3168.exe
0xfffffa800c72400 0xfffffa800c72400 chrome.exe Error: ImageBaseAddress at 0x13fb10000 is unavailable (possibly due to paging)
0xfffffa800c72400 0xfffffa800c72400 chrome.exe Error: ImageBaseAddress at 0x13fb10000 is unavailable (possibly due to paging)

```

VirusTotal - Mozilla Firefox

https://www.virustotal.com/gui/file/b4ff4232cadb2b477c56fcb3d171261d341b596dec8f0e79563068c4d97e76/detection

b4ff4232cadb2b477c56fcb3d171261d341b596dec8f0e79563068c4d97e76

1 / 67

One engine detected this file

b4ff4232cadb2b477c56fcb3d171261d341b596dec8f0e79563068c4d97e76

Size 3.08 MB

2018-11-03 11:25:44 UTC

11 months ago

EXE

DETECTION	DETAILS	COMMUNITY
CrowdStrike Falcon	Malicious_confidence_80% (W)	Ad-Aware
AegisLab	Undetected	AhnLab-V3
Alibaba	Undetected	ALYac
Antiy-AVL	Undetected	Arcabit
Avast	Undetected	Avast-Mobile
AVG	Undetected	Avira (no cloud)
Babable	Undetected	Baidu
BitDefender	Undetected	Bkav
CAT-QuickHeal	Undetected	ClimAV
CMC	Undetected	Cybereason
Cylance	Undetected	Cyren
DrWeb	Undetected	eGambit
Emisoft	Undetected	Endgame

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Refresh Firefox...

Solution 9.

- The agent “Mel” sent a message to Daisy with the note as follows:
“Daisy there was a USB found in the car park, can you check it out?” (Figure 9.1)
- The CarPark.zip file can be found in the Files tab(Figure 9.2)

NetworkMiner 2.4

File Tools Help

-- Select a network adapter in the list --

Hosts (153) Files (4091) Images (42) Messages (37) Credentials (479) Sessions (2366) DNS (10028) Parameters (100128) Keywords Anomalies

Filter keyword: Case sensitive ExactPhrase Any column Clear

Frame nr.	Source host	Destination host	From	To	Subject	Protocol	Timestamp
14832	192.168.1.66 [*] (Linux)	192.168.1.73 [0]	grant grant@192.168.1.71	#channel	My brother they may be on to us	Irc	2018-10-01 02:20:03 UTC
15146	192.168.1.73 [0]	192.168.1.66 [*] (Linux)		#channel	I will be careful	Irc	2018-10-01 02:20:11 UTC
15147	192.168.1.66 [*] (Linux)	192.168.1.71 [0]	leo leo@192.168.1.73	#channel	I will be careful	Irc	2018-10-01 02:20:11 UTC
16342	192.168.1.71 [0]	192.168.1.66 [*] (Linux)		#channel	See if you can tap into their emails	Irc	2018-10-01 02:20:41 UTC
16344	192.168.1.66 [*] (Linux)	192.168.1.73 [0]	grant grant@192.168.1.71	#channel	See if you can tap into their emails	Irc	2018-10-01 02:20:41 UTC
16751	192.168.1.71 [0]	192.168.1.66 [*] (Linux)		#channel	I will make the key available to you	Irc	2018-10-01 02:20:59 UTC
16752	192.168.1.66 [*] (Linux)	192.168.1.73 [0]	grant grant@192.168.1.71	#channel	I will make the key available to you	Irc	2018-10-01 02:20:59 UTC
16900	192.168.1.71 [0]	192.168.1.66 [*] (Linux)		#channel	Good luck	Irc	2018-10-01 02:21:04 UTC
16902	192.168.1.66 [*] (Linux)	192.168.1.73 [0]	grant grant@192.168.1.71	#channel	Good luck	Irc	2018-10-01 02:21:04 UTC
17148	192.168.1.73 [0]	192.168.1.66 [*] (Linux)		#channel	Hail!	Irc	2018-10-01 02:21:09 UTC
17149	192.168.1.66 [*] (Linux)	192.168.1.71 [0]	leo leo@192.168.1.73	#channel	Hail!	Irc	2018-10-01 02:21:09 UTC
24554	192.168.1.76 [0]	192.168.1.66 [*] (Linux)		#shield	Daisy there was a usb found in the car park, can y...	Irc	2018-10-01 02:23:41 UTC
24555	192.168.1.66 [*] (Linux)	192.168.1.72 [0]	mel mel@192.168.1.76	#shield	Daisy there was a usb found in the car park, can y...	Irc	2018-10-01 02:23:41 UTC
25754	192.168.1.76 [0]	192.168.1.66 [*] (Linux)		#shield	Hydra may have made a mistake	Irc	2018-10-01 02:24:02 UTC
25755	192.168.1.66 [*] (Linux)	192.168.1.72 [0]	mel mel@192.168.1.76	#shield	Hydra may have made a mistake	Irc	2018-10-01 02:24:02 UTC
26571	192.168.1.72 [0]	192.168.1.66 [*] (Linux)		#shield	No problem, I am on it	Irc	2018-10-01 02:24:16 UTC
26572	192.168.1.66 [*] (Linux)	192.168.1.76 [0]	daisy daisy@192.168.1.72	#shield	No problem, I am on it	Irc	2018-10-01 02:24:16 UTC
26937	192.168.1.72 [0]	192.168.1.66 [*] (Linux)		#shield	Where is the usb	Irc	2018-10-01 02:24:25 UTC
26939	192.168.1.66 [*] (Linux)	192.168.1.76 [0]	daisy daisy@192.168.1.72	#shield	Where is the usb	Irc	2018-10-01 02:24:25 UTC
27561	192.168.1.76 [0]	192.168.1.66 [*] (Linux)		#shield	I will upload it to the usual place	Irc	2018-10-01 02:24:37 UTC
27563	192.168.1.66 [*] (Linux)	192.168.1.72 [0]	mel mel@192.168.1.76	#shield	I will upload it to the usual place	Irc	2018-10-01 02:24:37 UTC
35652	192.168.1.72 [0]	192.168.1.66 [*] (Linux)		#shield	thanks	Irc	2018-10-01 02:26:08 UTC
66780	192.168.1.71 [0]	192.168.1.66 [*] (Linux)		#channel	we have to find out how much rogers knows	Irc	2018-10-01 02:36:33 UTC
66781	192.168.1.66 [*] (Linux)	192.168.1.73 [0]	grant grant@192.168.1.71	#channel	we have to find out how much rogers knows	Irc	2018-10-01 02:36:33 UTC
68628	192.168.1.71 [0]	192.168.1.66 [*] (Linux)		#channel	I have a memory dump of his PC	Irc	2018-10-01 02:37:02 UTC
68629	192.168.1.66 [*] (Linux)	192.168.1.73 [0]	grant grant@192.168.1.71	#channel	I have a memory dump of his PC	Irc	2018-10-01 02:37:02 UTC
70051	192.168.1.73 [0]	192.168.1.66 [*] (Linux)		#channel	maybe we can get his password from the dump	Irc	2018-10-01 02:37:26 UTC
70052	192.168.1.66 [*] (Linux)	192.168.1.71 [0]	leo leo@192.168.1.73	#channel	maybe we can get his password from the dump	Irc	2018-10-01 02:37:26 UTC
71885	192.168.1.71 [0]	192.168.1.66 [*] (Linux)		#channel	I have uploaded it to the usual place	Irc	2018-10-01 02:37:55 UTC

NetworkMiner 2.4

File Tools Help

-- Select a network adapter in the list --

Hosts (153) Files (4091) Images (42) Messages (37) Credentials (479) Sessions (2366) DNS (10028) Parameters (100128) Keywords Anomalies

Filter keyword: Case sensitive ExactPhrase Any column Clear Apply

Frame nr.	Filename	Extension	Size	Source host	S. port	Destination host	D. port	Protocol	Timestamp	Reconstructed file path
30090	CarParkUSB.zip	zip	86 772 768 B	192.168.1.76 [0]	TCP 45571	192.168.1.21 [ftp.shield.frn643] (Linux)	TCP 20	FTP	2018-10-01 02:25:30 UTC	C:\Users\Gowtham Ravi\Downloads\NetworkMiner...

Solution 10.

No, Daisy is not an H.Y.D.R.A agent as any evidence cannot be determined to prove the case.

Solution 11.

The four agents are as follows:

Mel - 192.168.1.76

Daisy - 192.168.1.72

Grant - 192.168.1.71

Leo - 192.168.1.73

The servers are listed as follows:

Linux Server (chat) - 192.168.1.66 (TCP 80)

Linux Server (ftp) - 192.168.1.21 (TCP 21)

Linux Server (apache) - 192.168.1.80 (TCP 80)

DNS Server - 192.168.1.53 (UDP 53)

Linux Server (email) - 192.168.1.25 (TCP 587(Smtp)/993(Ssl))

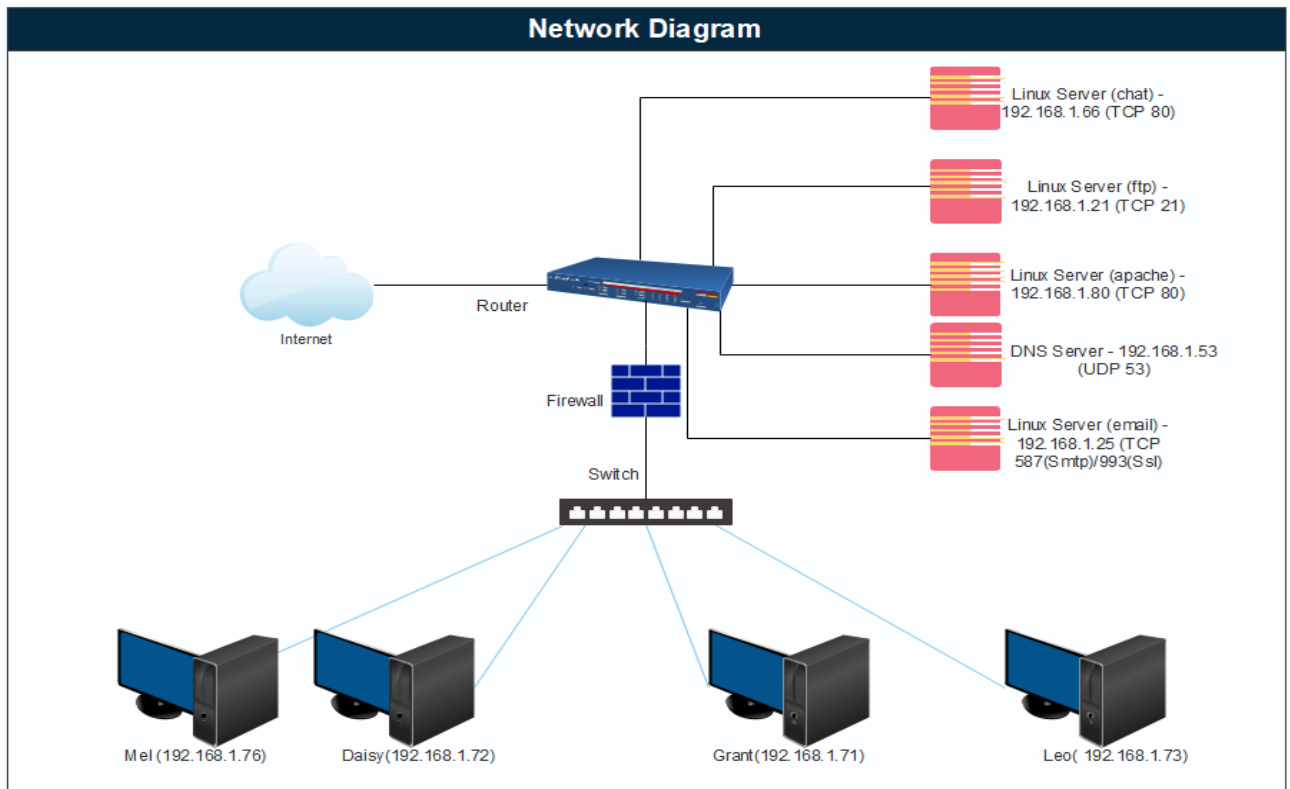


Figure 11.

Solution 12.

Event 1:

The first contact between agent named Mel and agent named Daisy happens on 2018-10-01 at 02:17:42 UTC.

Event 2:

Grant keeps the key ready for Leo on 2018-10-01 at 02:20:59 UTC.

Event 3:

The agent named Mel transfers the files in the USB to the server at 2018-10-01 at 02:24:37 UTC.

Event 4:

The agent named Leo uploaded the information to the server at 2018-10-01 at 02:37:55 UTC.

Executive Summary:

The Winter soldier enters the house of Steve Rogers and gives a flash drive to him. Nick Fury is gun down by Winter soldier. While using the flash drive using Wireshark, Network Miner and SiftWorkstation, it is found that there are four agents named Mel, Daisy, Leo and Grant. The double agent for H.Y.D.R.A is Leo and Grant which is found using the AutoSpy analysing the Car USB file. These software's are used to analyse the data and find the information which is an evidence for the case.