Griffith University

7906ICT Digital Forensics Assignment

Task 1

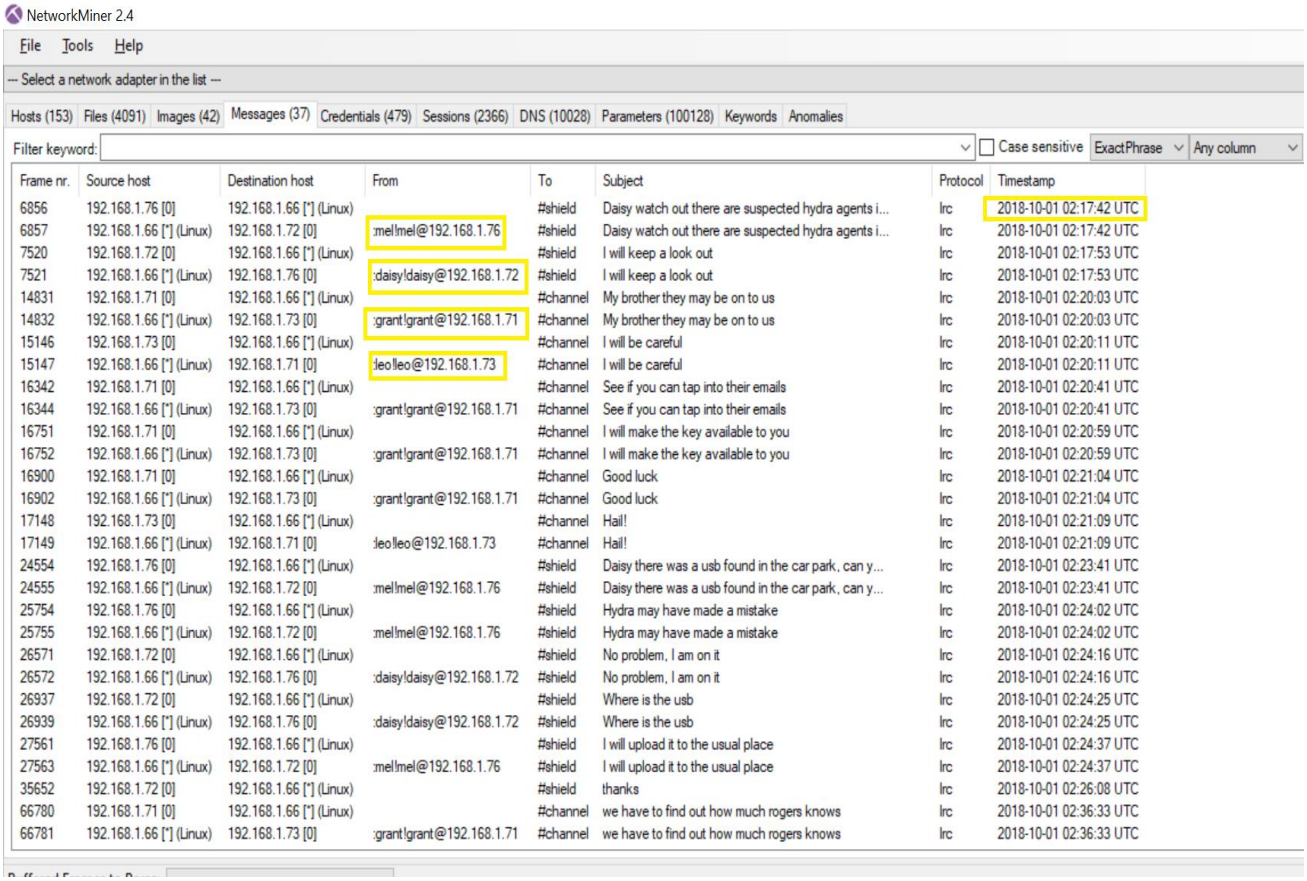
Gowtham Ravi
S5190712

Contents

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



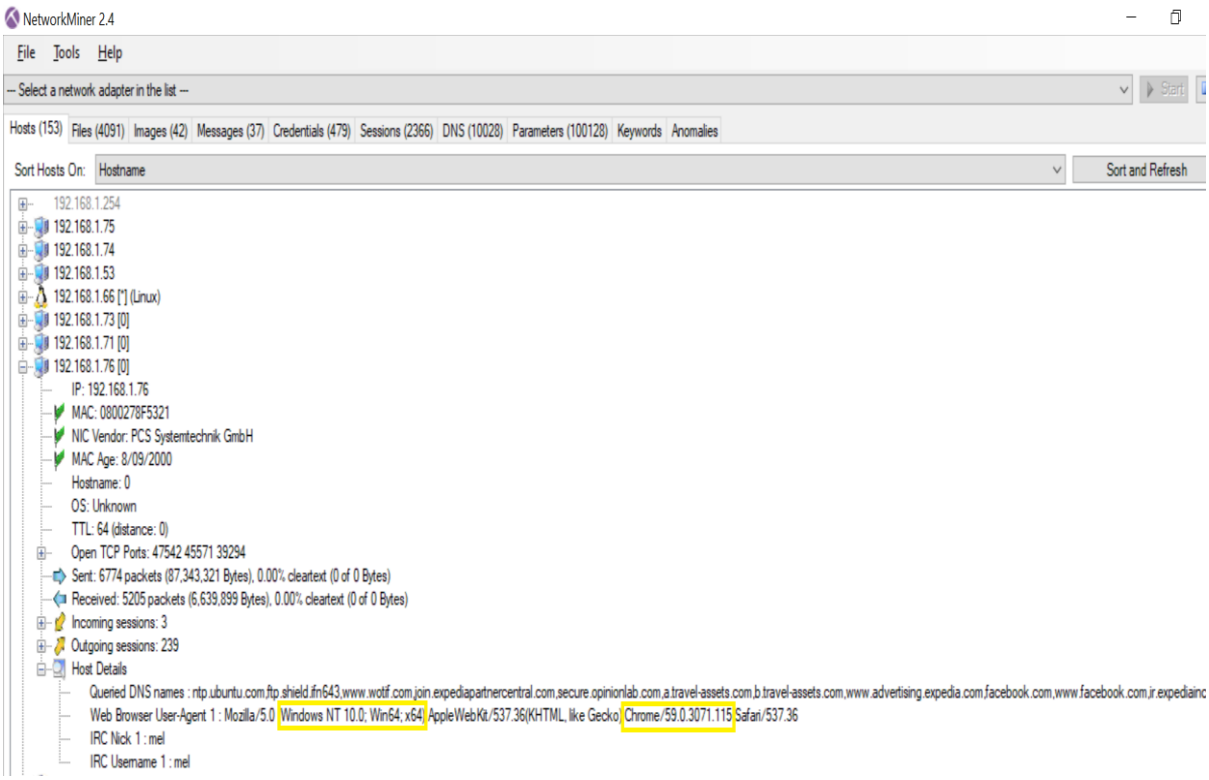
Frame nr.	Source host	Destination host	From	To	Subject	Protocol	Timestamp
6856	192.168.1.76 [0]	192.168.1.66 [*] (Linux)		#shield	Daisy watch out there are suspected hydra agents i...	Irc	2018-10-01 02:17:42 UTC
6857	192.168.1.66 [*] (Linux)	192.168.1.72 [0]	:mel!mel@192.168.1.76	#shield	Daisy watch 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

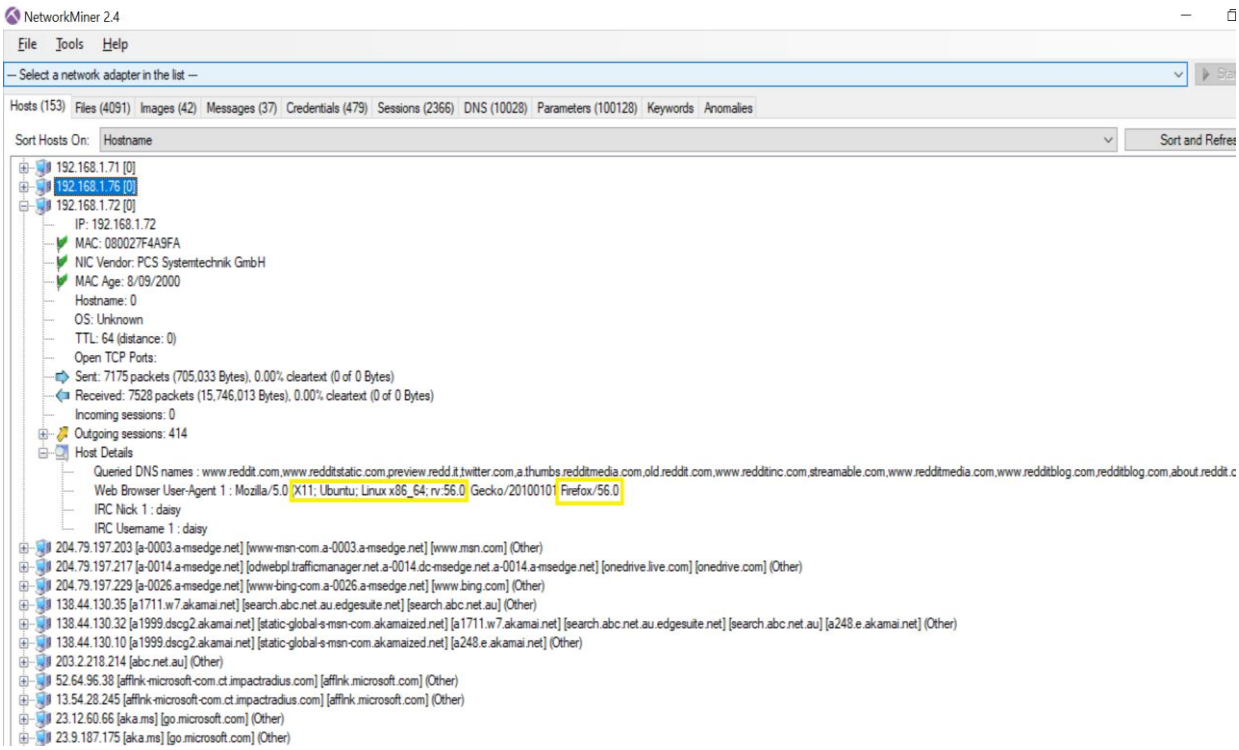
Solution 2.

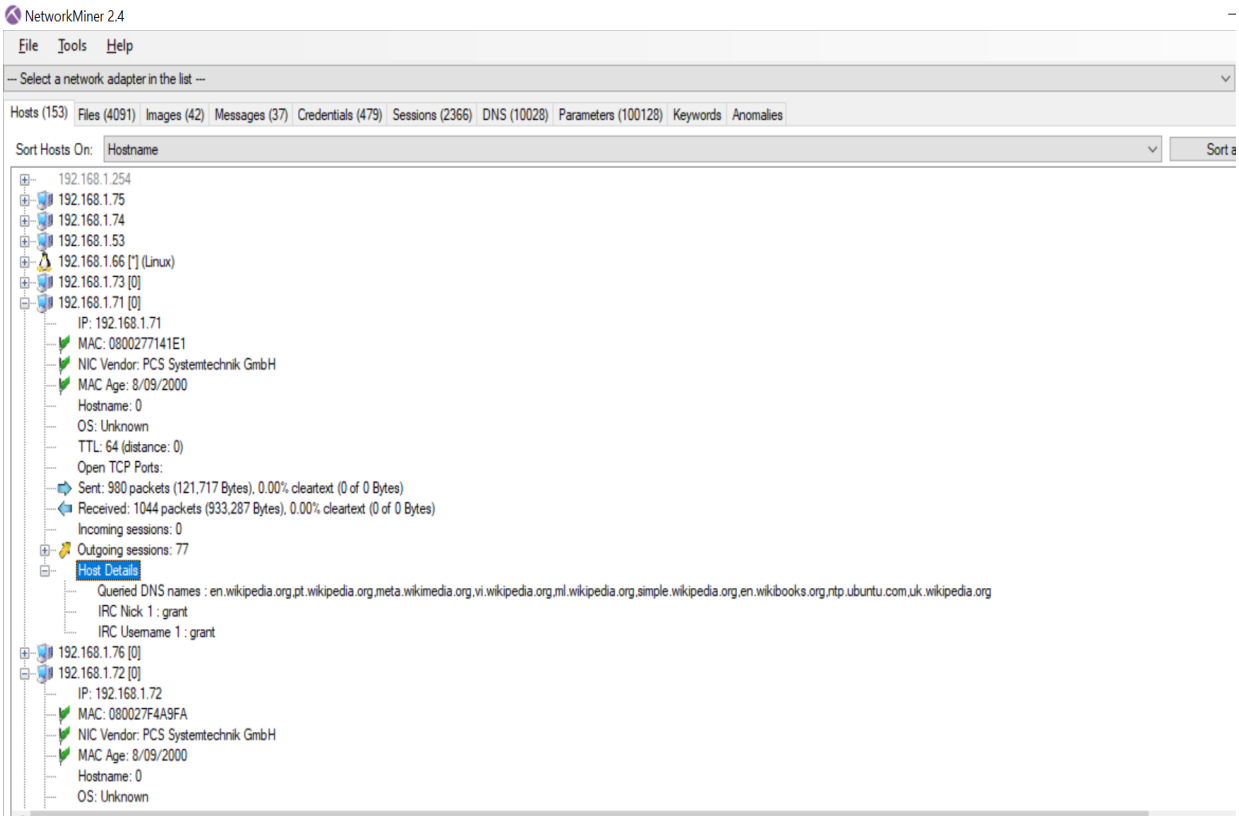
Network Miner 2.4 is used to identify the agents ' web browsers and operating systems.

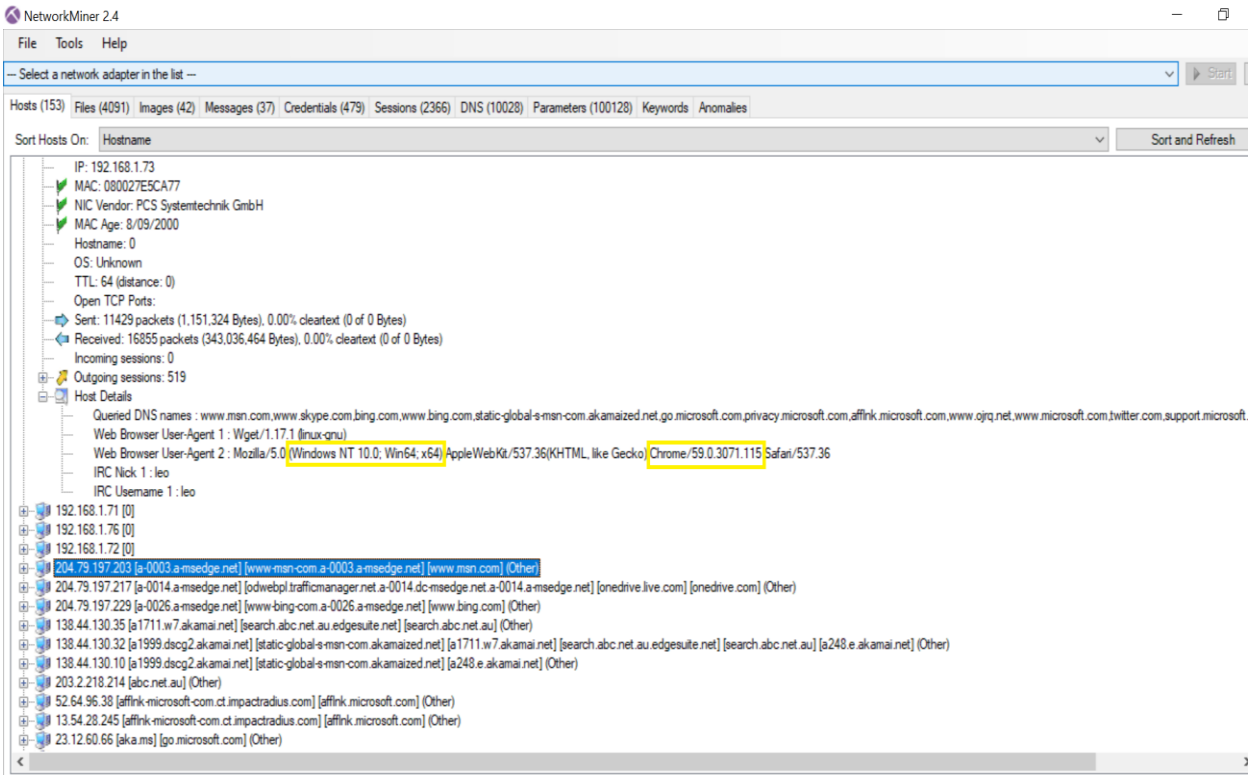
- The host details of the agents found by navigating to the Hosts page.
- The web browsers and operating systems used by agents are found as follows:

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
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.redd.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.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-msn-com.akamaized.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-msn-com.akamaized.net] [a248.e.akamai.net] (Other)
203.2.218.214 [abc.net.au] (Other)
52.64.96.38 [afflink-microsoft-com.ct.impactradius.com] [afflink.microsoft.com] (Other)
13.54.28.245 [afflink-microsoft-com.ct.impactradius.com] [afflink.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
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



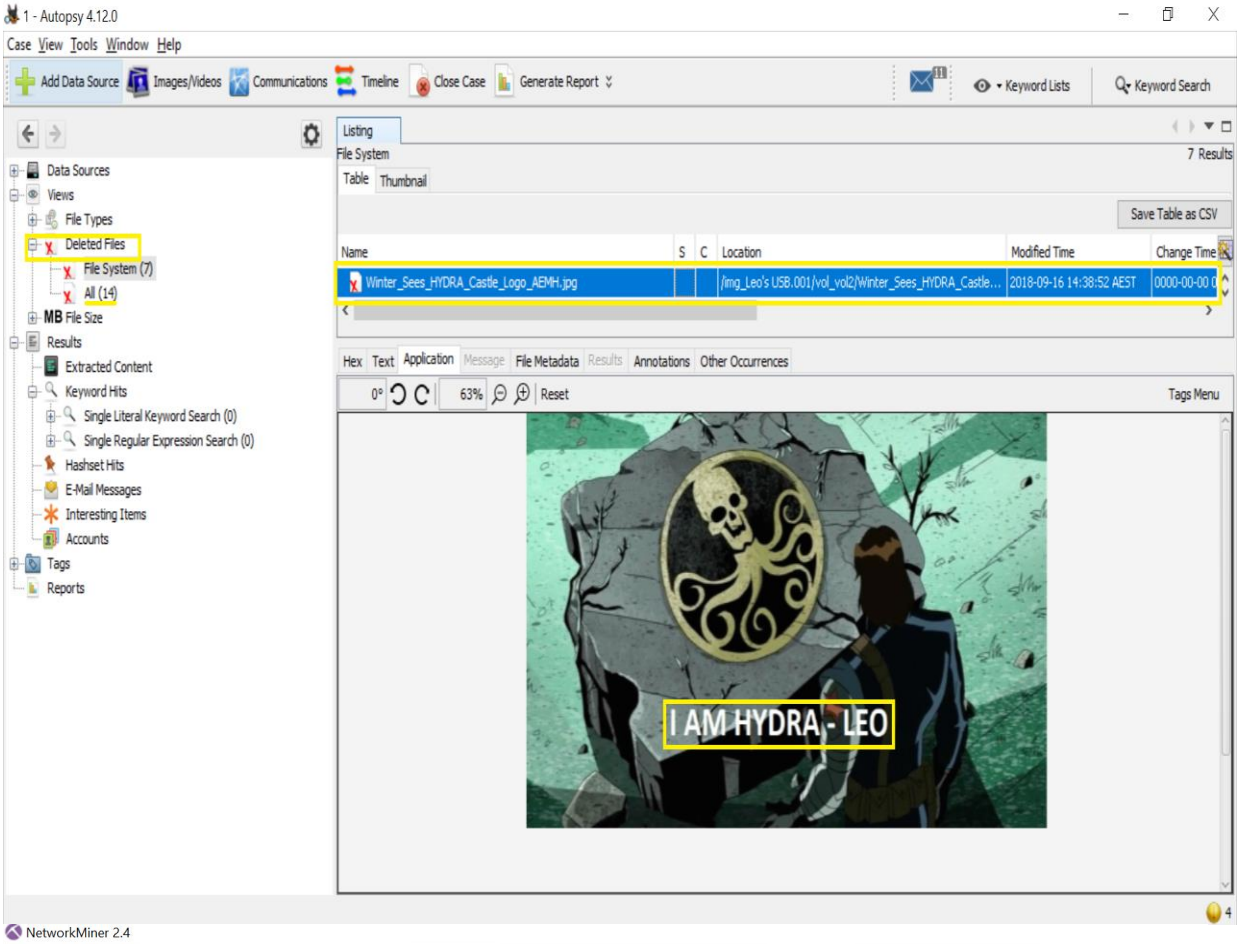
Solution 3.

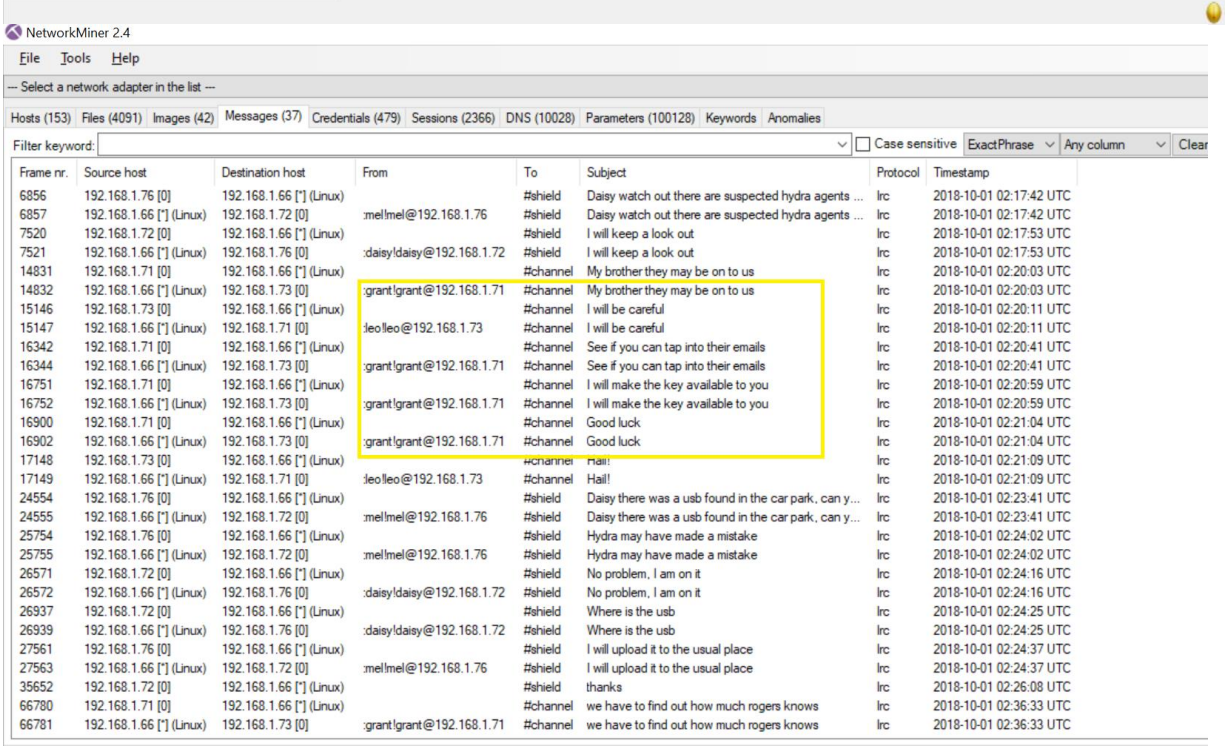
- CarParkUSB.zip folder is opened from NetworkMiner 2.4 through the FILES tab. The file is accessed in Autopsy 4.12 software to find the double agent for H.Y.D.R.A.

- There were several deleted files inside the USB between them we could see an image in jpg format with the filename “**Winter_Sees_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**.

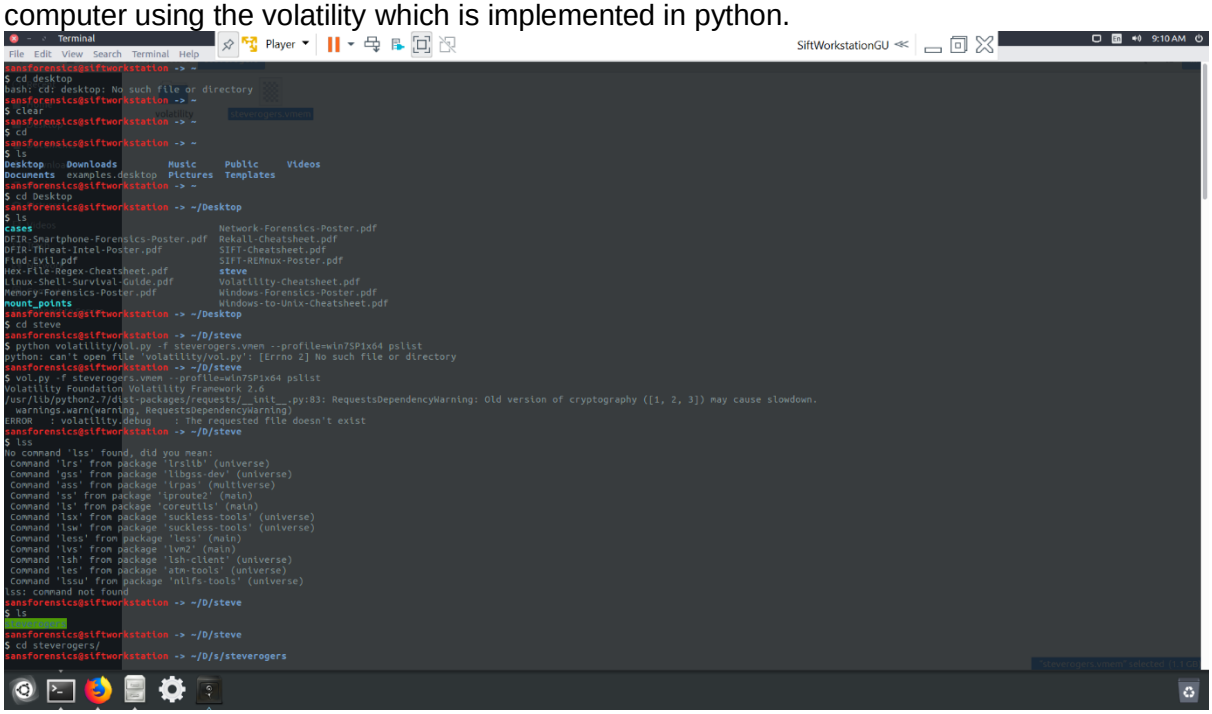


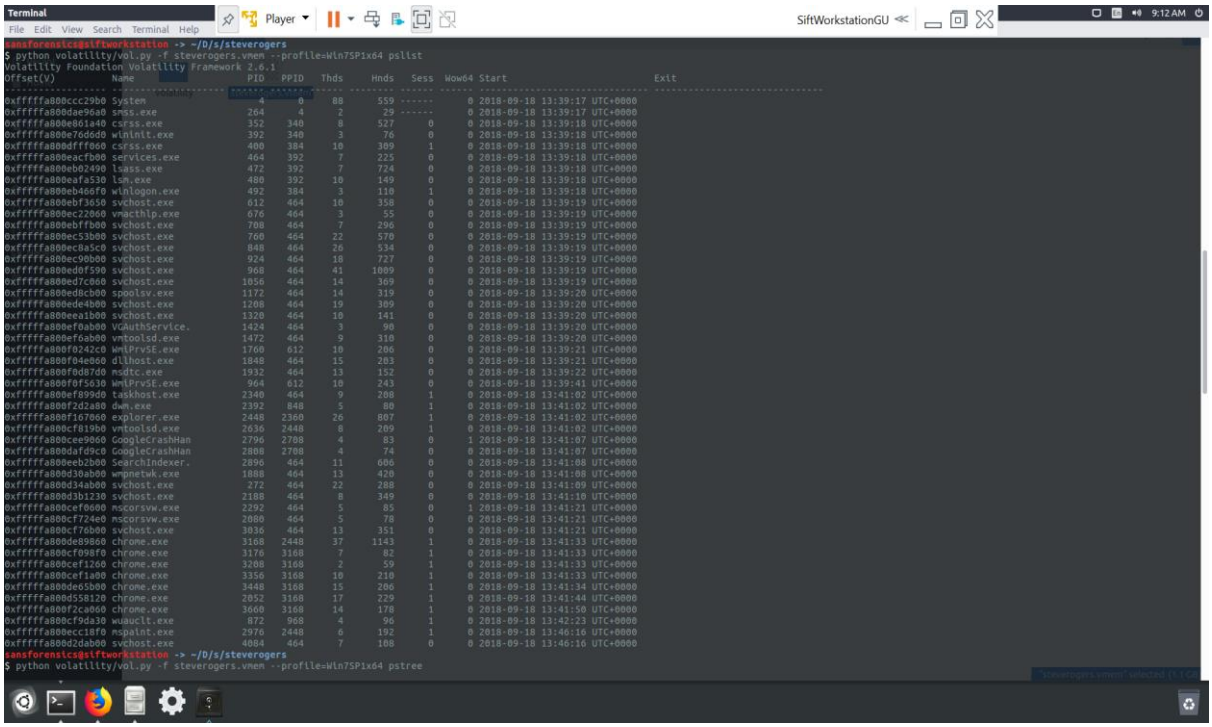


Frame nr.	Source host	Destination host	From	To	Subject	Protocol	Timestamp
6856	192.168.1.76 [0]	192.168.1.66 [*] (Linux)		#shield	Daisy watch out there are suspected hydra agents ...	Irc	2018-10-01 02:17:42 UTC
6857	192.168.1.66 [*] (Linux)	192.168.1.72 [0]	:mel!mel@192.168.1.76	#shield	Daisy watch out 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	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

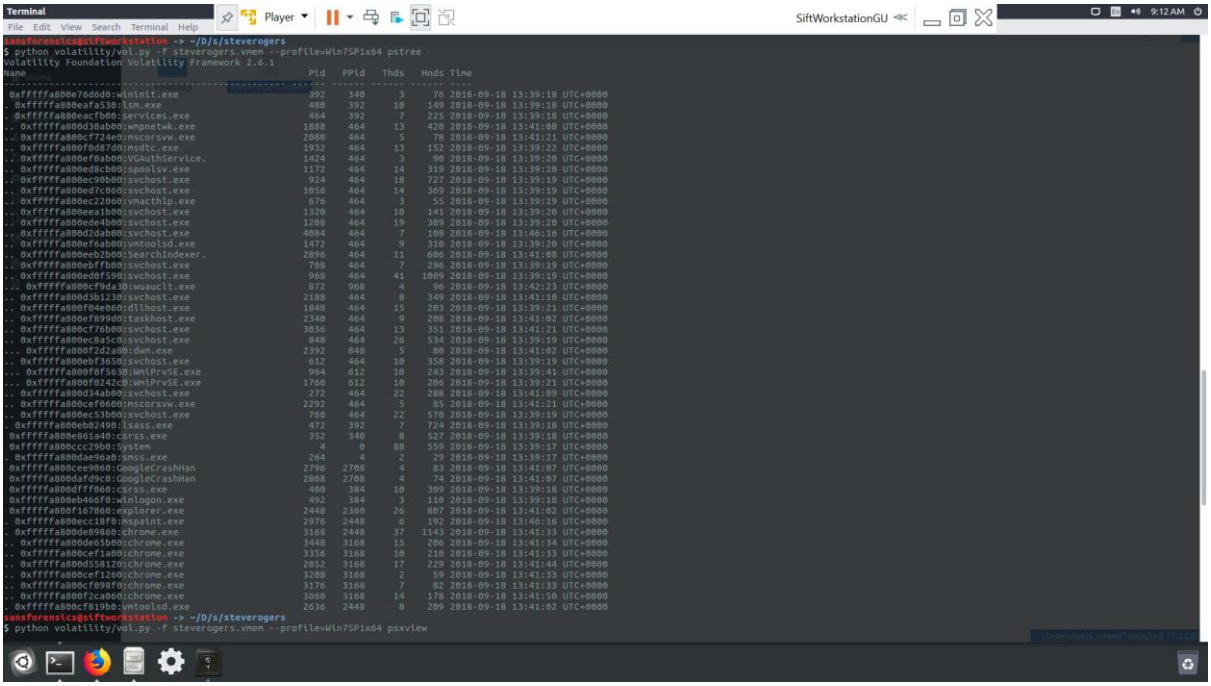
Solution 4.

- 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.

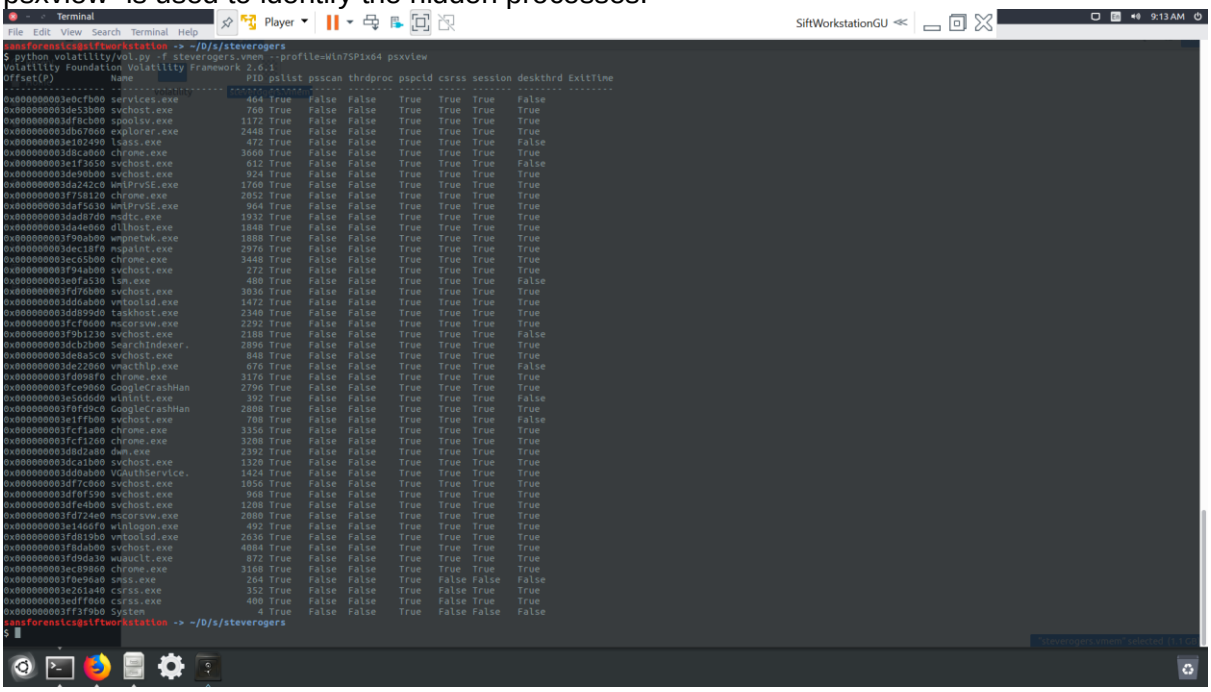




- The command “python volatility/vol.py -f steverogers.vmem --profile=Win7SP1x64 pstree” is used to find the parent & child processes.



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



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:

a) Gmail
b) Google
c) Last Pass

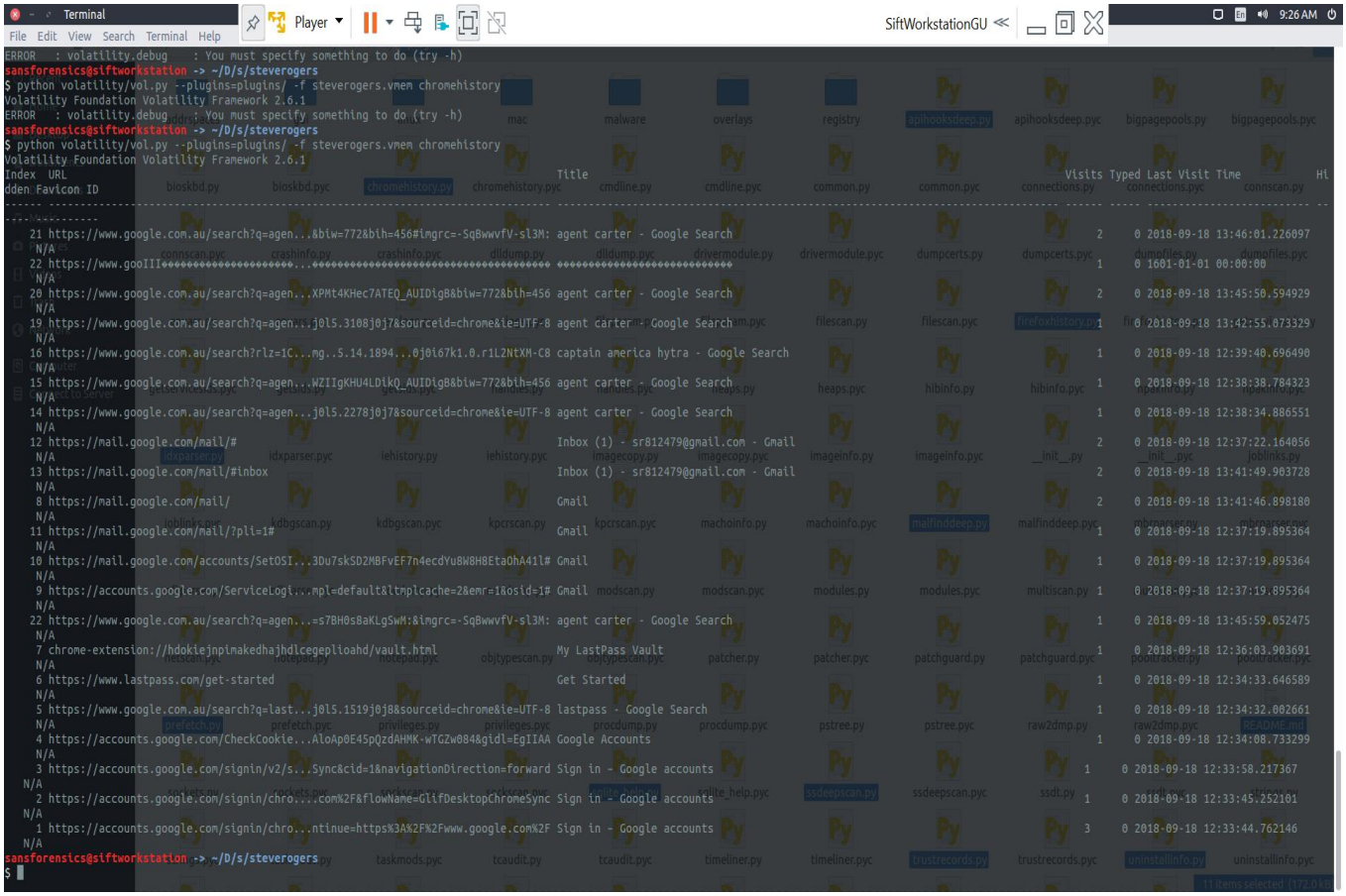
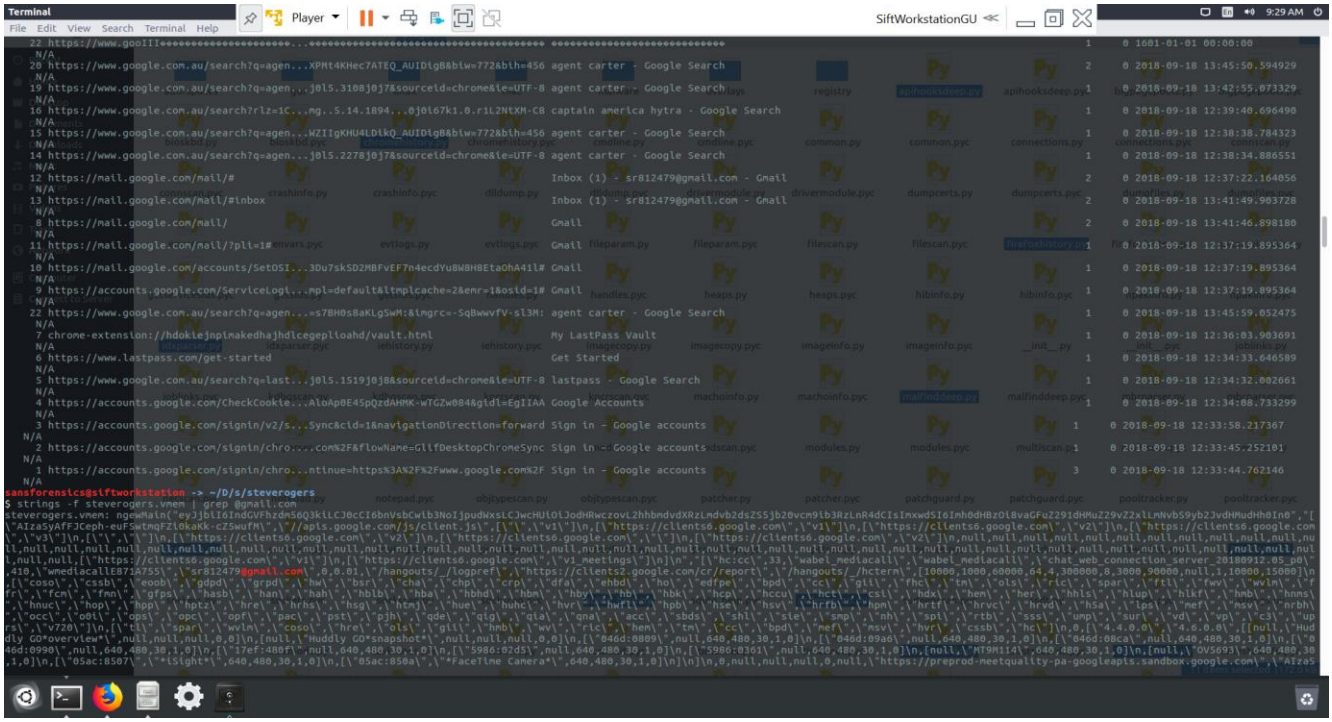


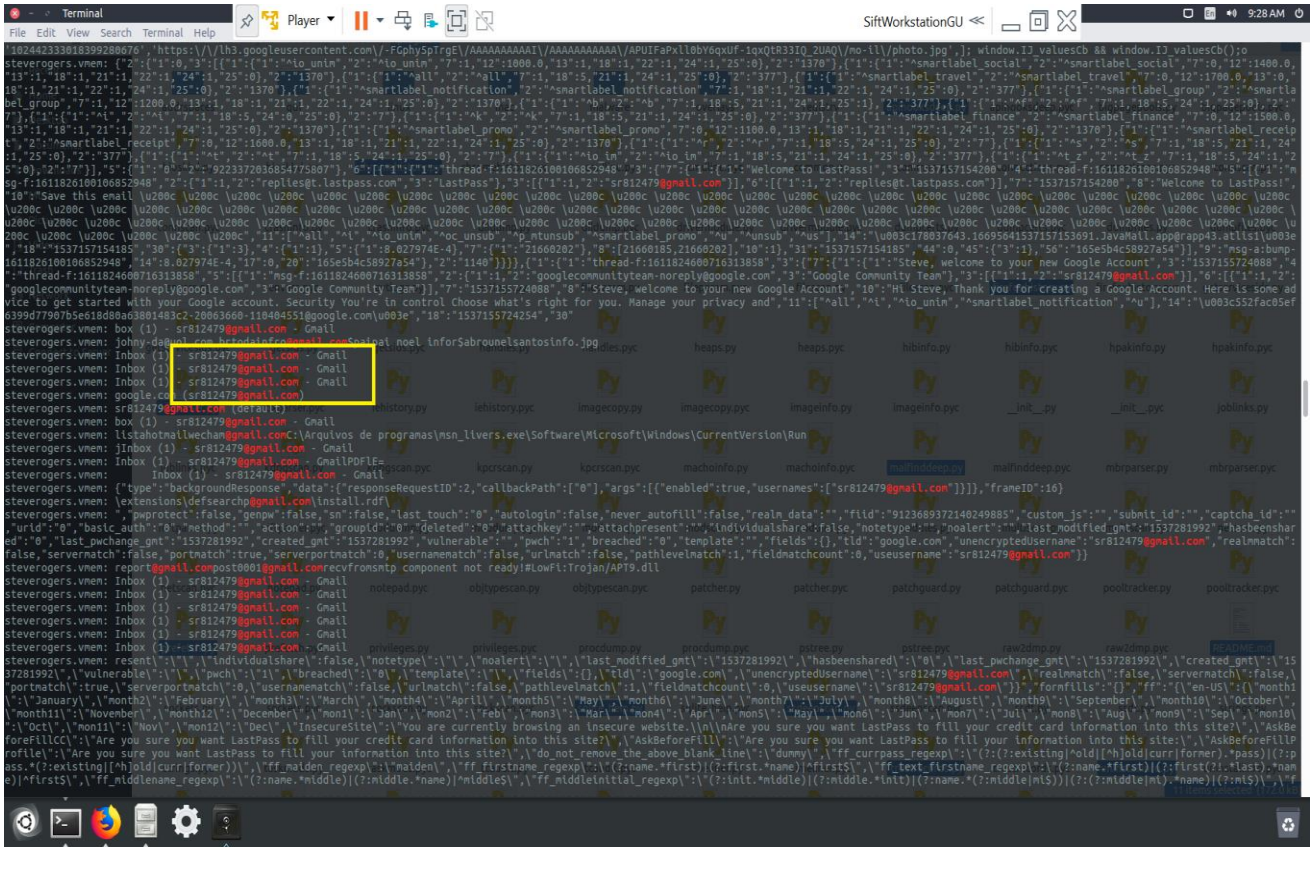
Figure 5.

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

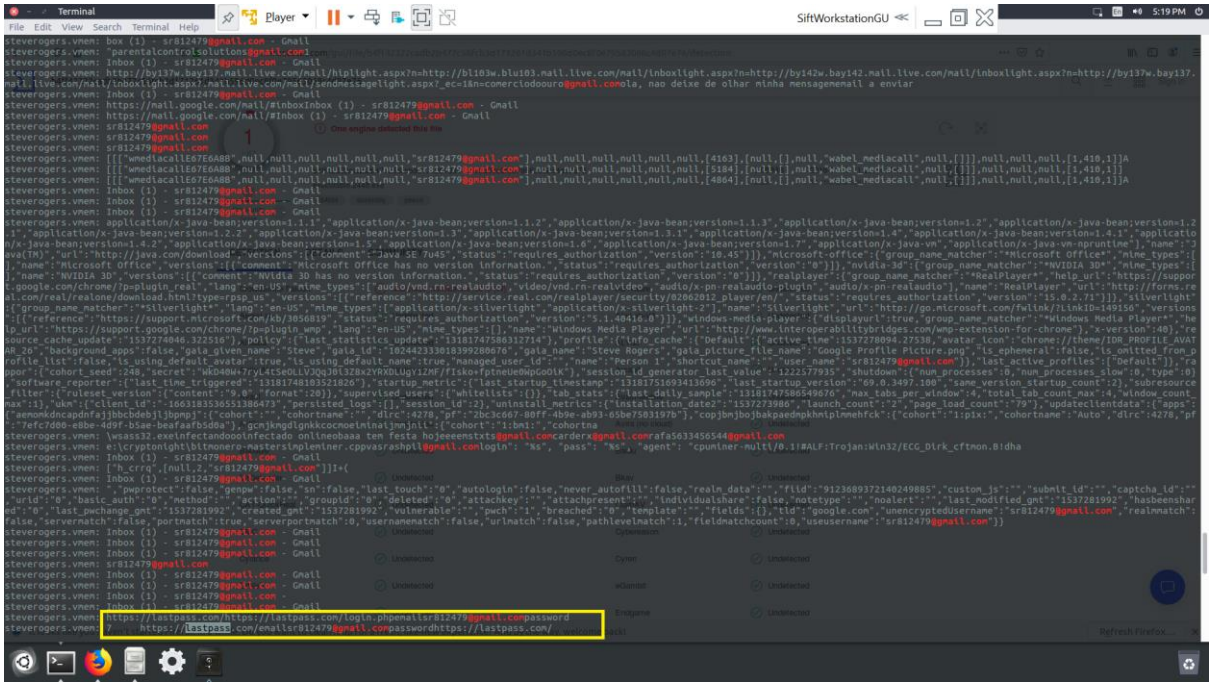

Terminal
File Edit View Search Terminal Help
Player
SiftWorkstationGU
9:29 AM
sansforensics@siftworkstation -> ~/D/s/steverogers
$ strings -f steverogers.vmem | grep @gmail.com


Terminal
File Edit View Search Terminal Help
Player
SiftWorkstationGU
9:28 AM

Solution 7.

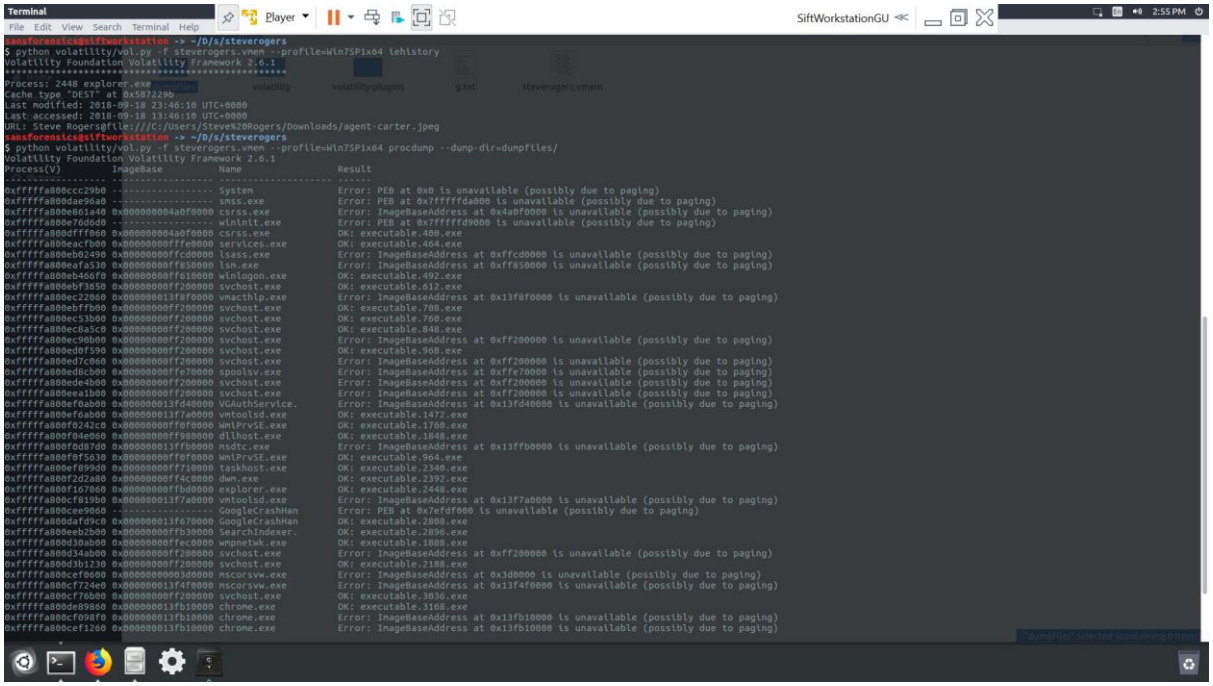
The steve rogers password cannot be found as he used the last pass website to manage his passwords**.**

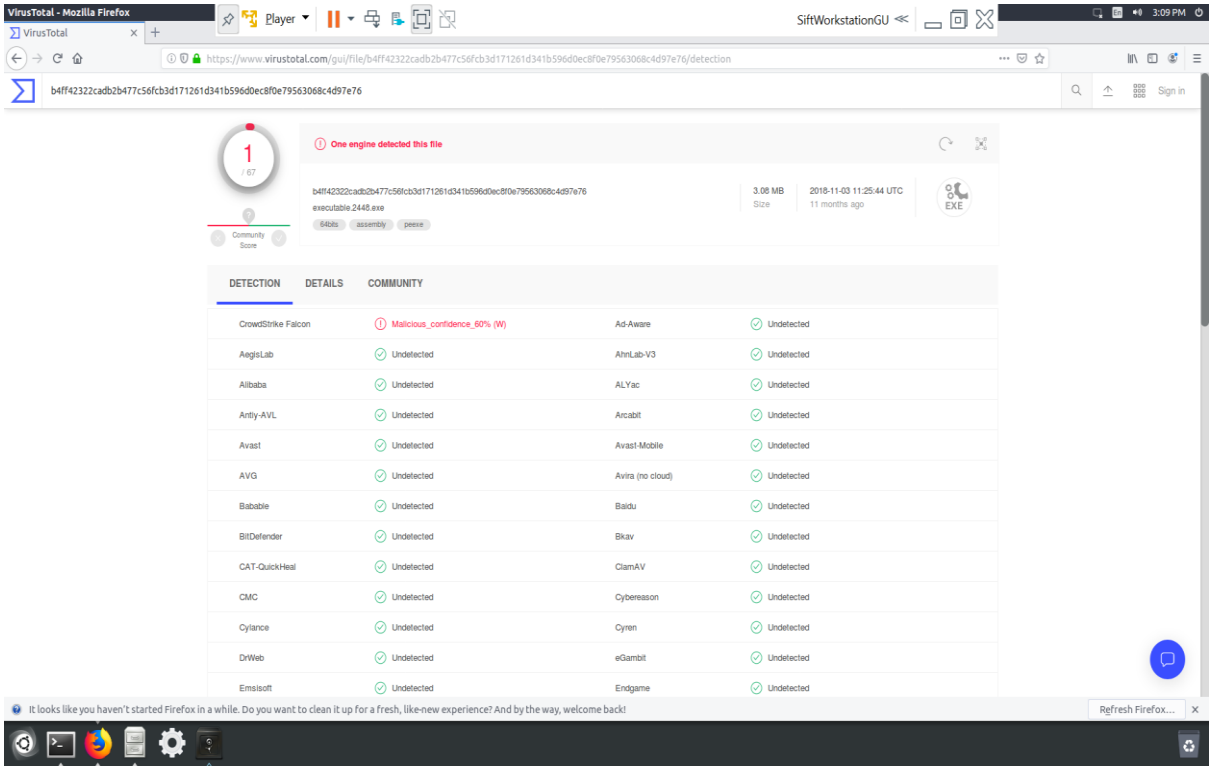
From Figure 7, it is found that steve rogers created an account in the last pass website and managed his password in it.



Solution 8.

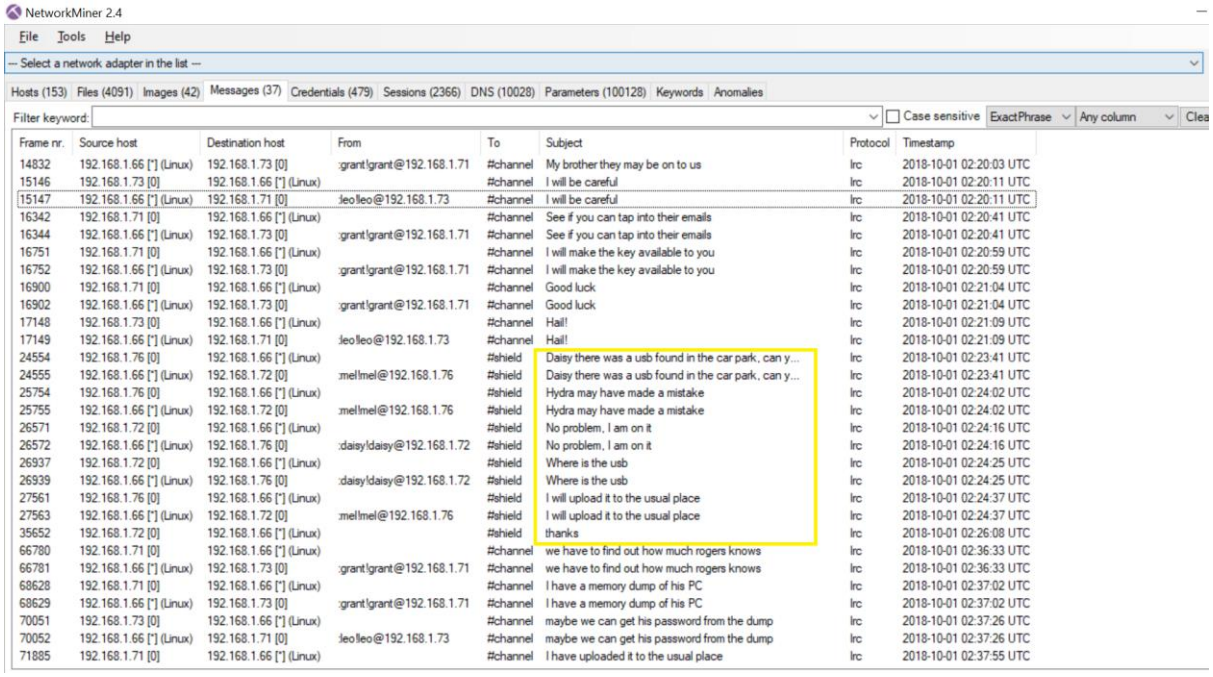
- The Steve roger pc, which is infected with a virus, is found by using the command “python volatility/vol.py -f steverogers.vmem --profile=Win7SP1x64 iehistory”.
- The image file in jpeg format with a filename as “agent-carter.jpeg” located at “C:/Users/Steve%20Rogers/Downloads/agent-carter.jpeg” is 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.

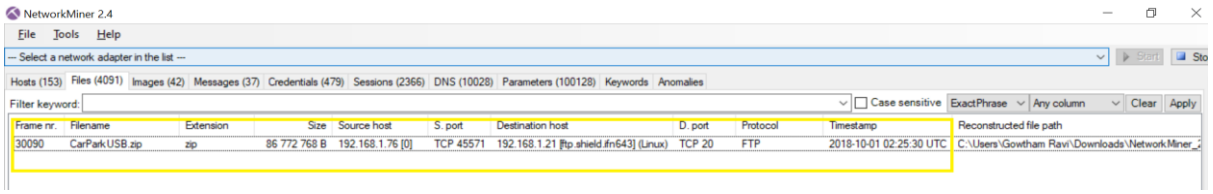




Solution 9.

- 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)





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)

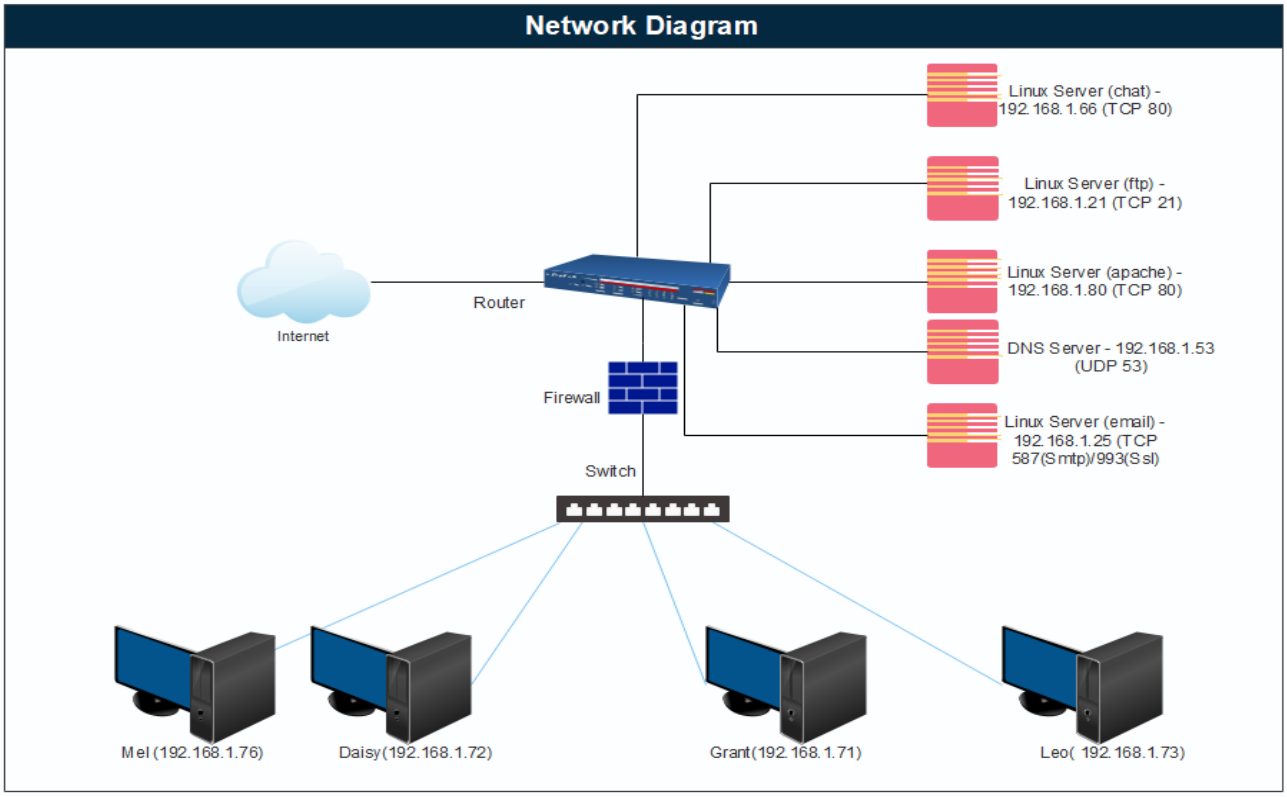


Figure 11.

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.