|  |  |  |
| --- | --- | --- |
| Admission No | Student Name | Lab PC |
| 220274X | Olfsen Valones | Home PC (VM) |

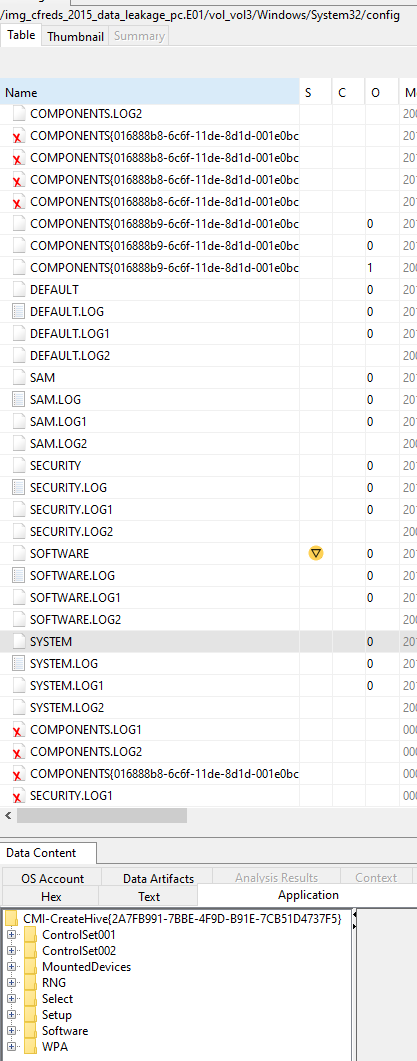
**Task 1 Windows Computer Forensics (14 marks)**

* 1. What is the time zone set in the Windows PC?

Answer:

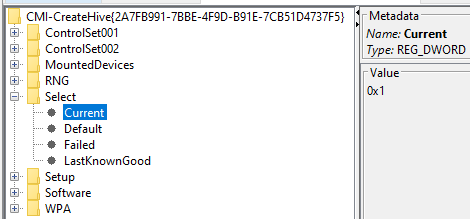
*The set timezone is Eastern Standard Time*

*To view the timezone set in the PC, an investigator would go to C:\Windows\System32\Config\SYSTEM*

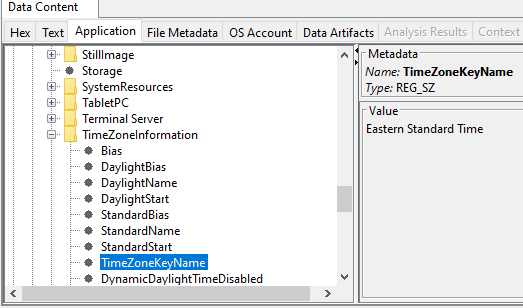
**

*\*Only drives that contain the Windows folder can be used to search for the timezone set.*

*In the system file, the Select folder is chosen to look into which ControlSet is used currently. Based on findings, ControlSet001 is used:*

**

*Exploring ControlSet001, the Control subfolder is opened to find TimeZoneInformation. This yields time zone information set on the PC:*

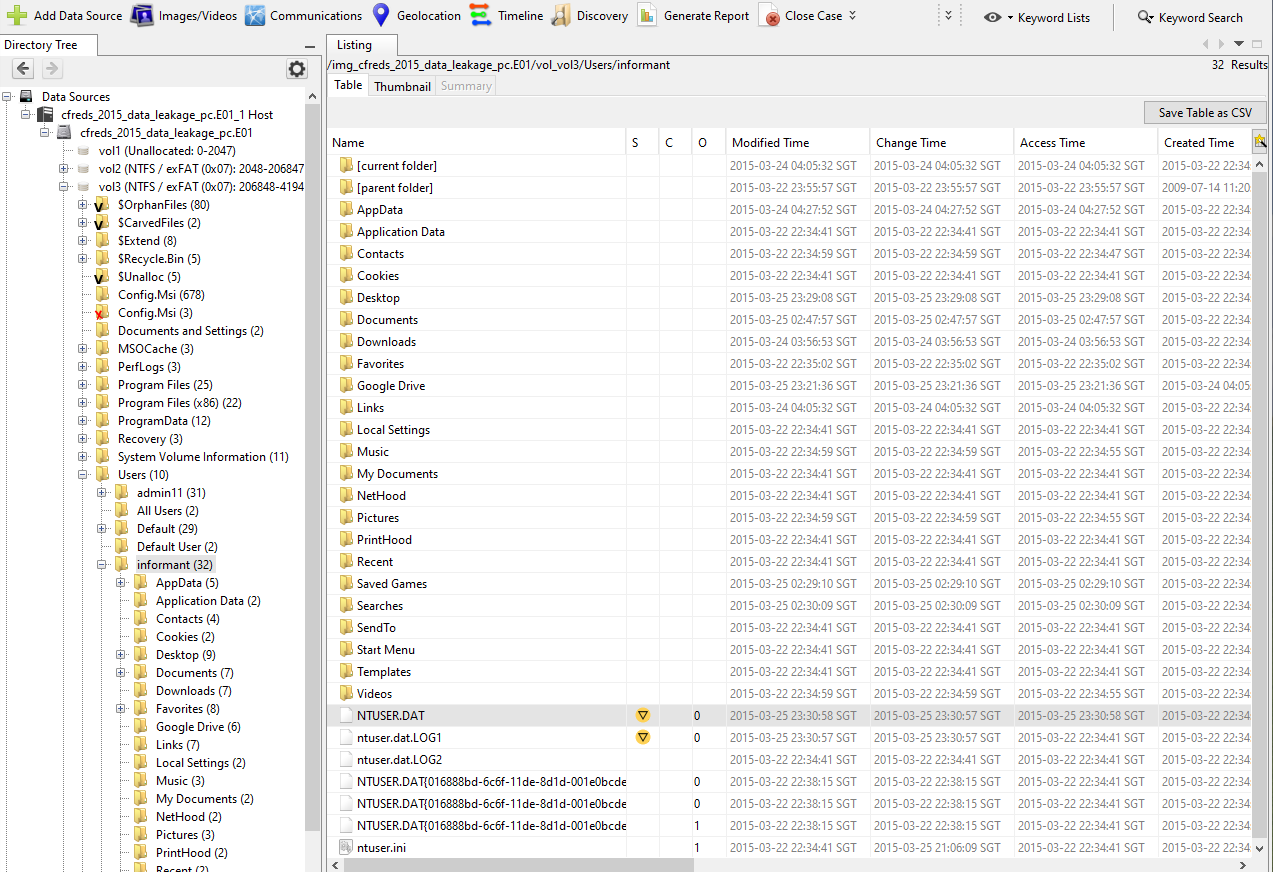
**

* 1. When did Mr. Informant last log on to the Windows PC?

Answer:

*To view Mr. Informant’s last log on in the PC, an investigator would navigate as such:*

*C:\Users\Informant\NTUser.DAT*

**

*By examining the file, the following is observed:*

*A screenshot of a computer

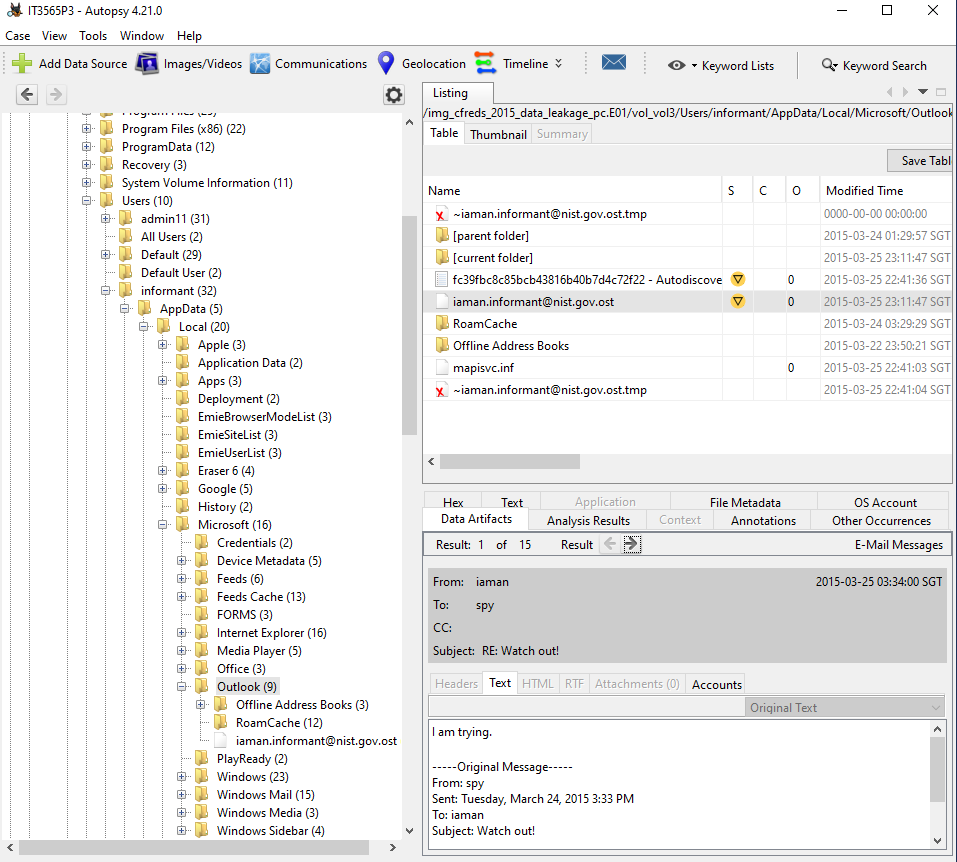
Description automatically generated*

*The Informant had a failed login attempt at 22:45:43 SGT time, and they successfully logged on at* ***2015-03-25 22:45:59*** *SGT time.*

List all e-mail messages sent or received by Mr. Informant related to the data leakage case.

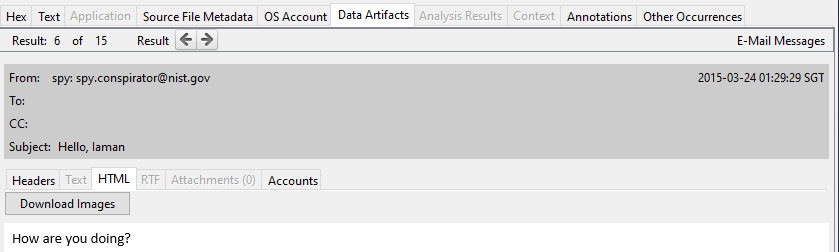
Answer:

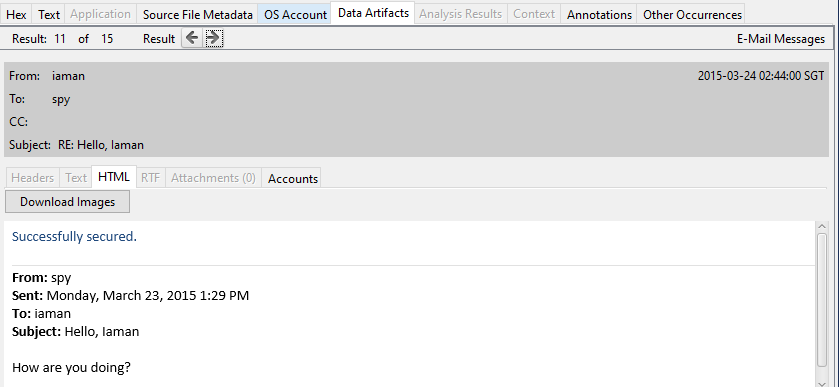
*Using Autopsy, emails sent or received by Mr. Informant can be viewed in the C:\Users\Informant\AppData\Local\Microsoft\Outlook directory. From there, the ‘*[*iaman.informant@nist.gov.ost*](mailto:iaman.informant@nist.gov.ost)*’ file is selected to view all the emails.*

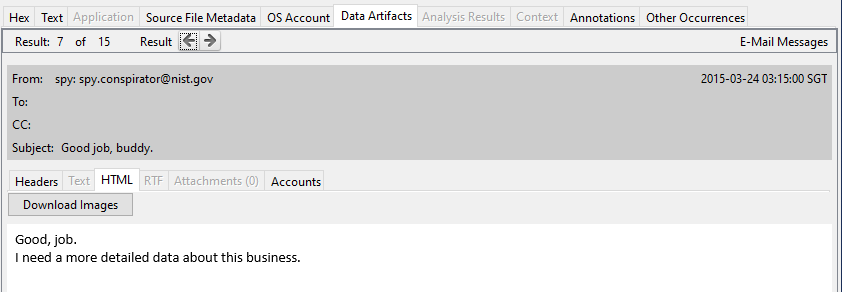
**

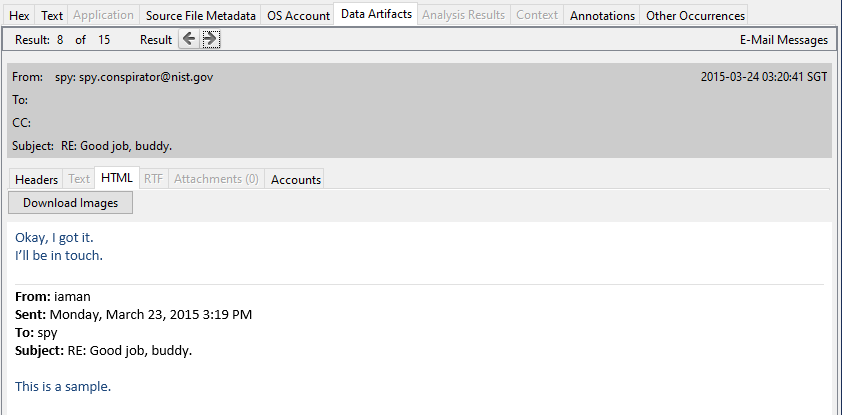
*The following emails are related to the leakage case:*

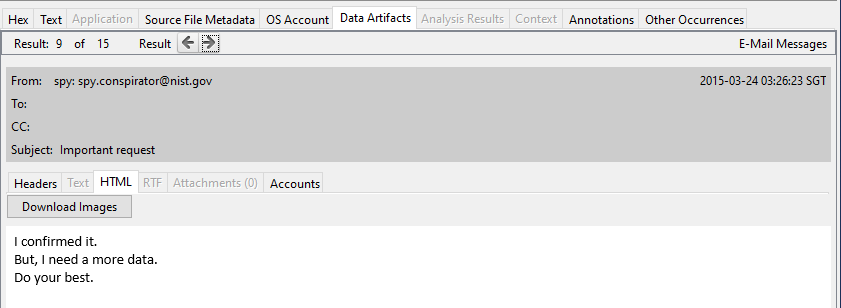
*Email order: 6,11, 7, 8, 9, 12, 4, 10, 2, 1, 5*

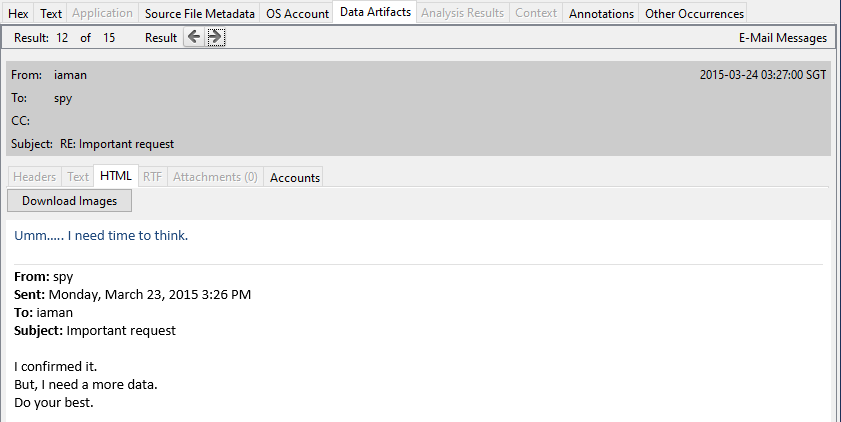
**

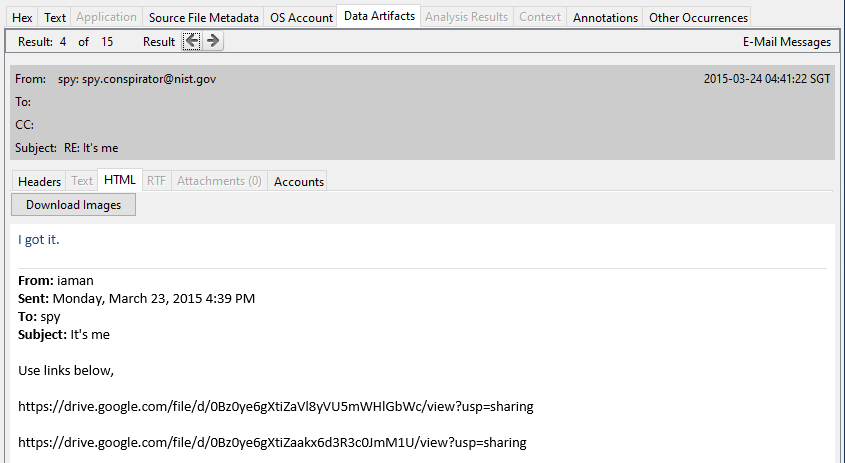
**

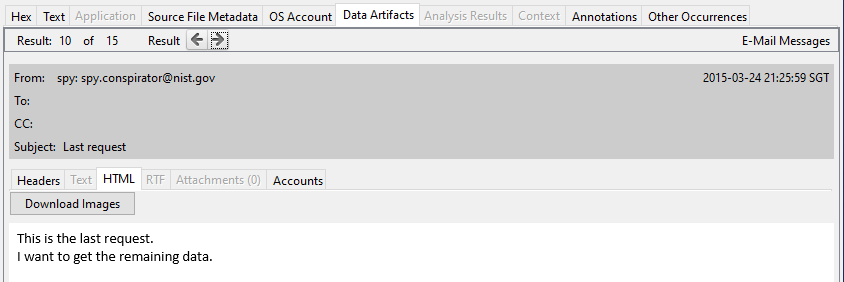
**

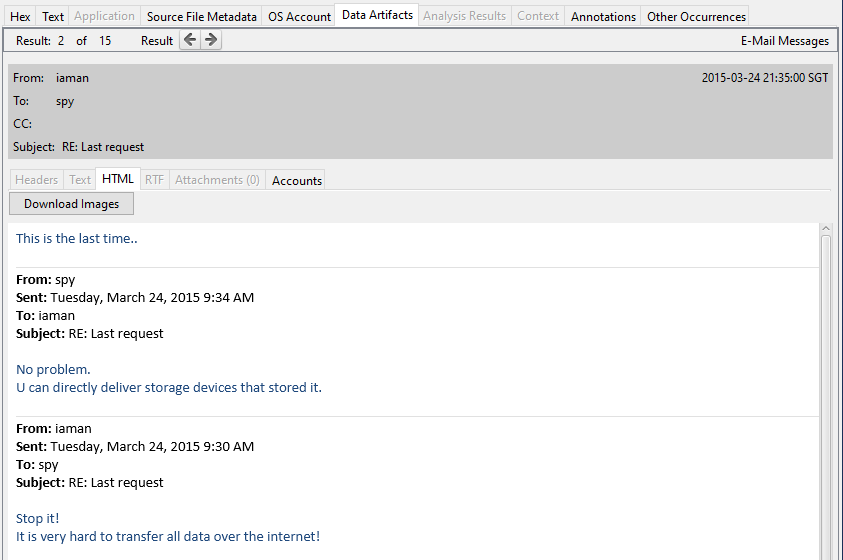
**

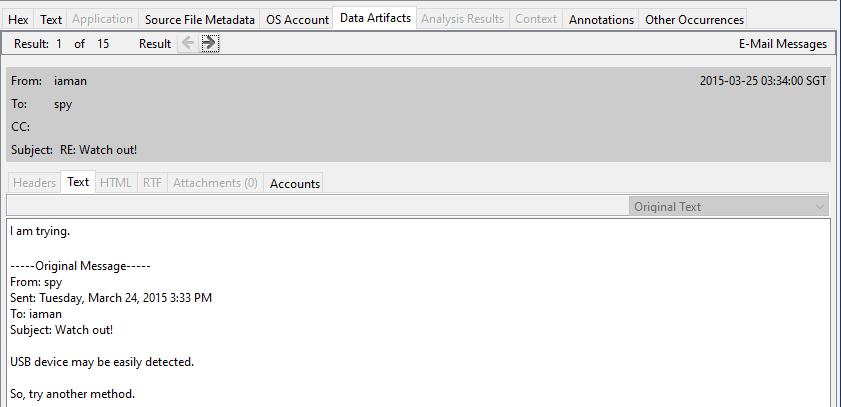
**

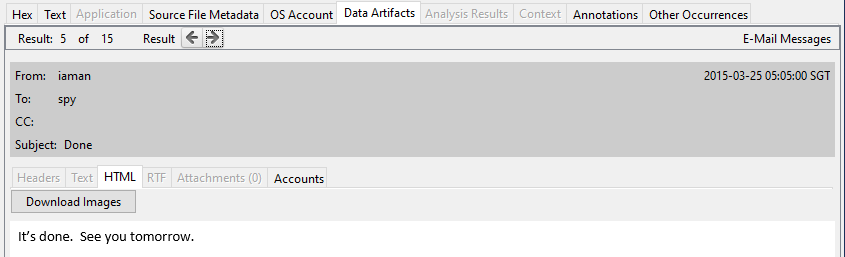
**

******

**

**

**

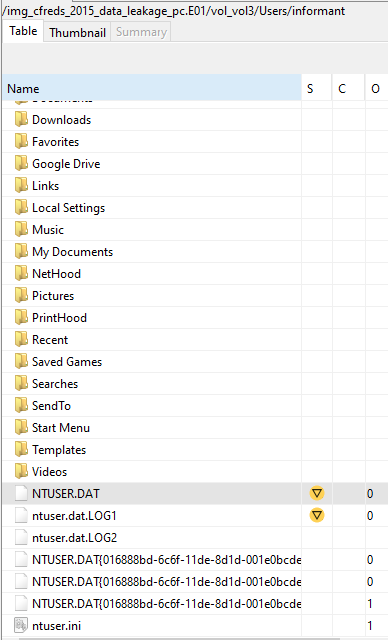
**

* 1. What is the name of the shared network folder and its network IP address, accessed by Mr. Informant?

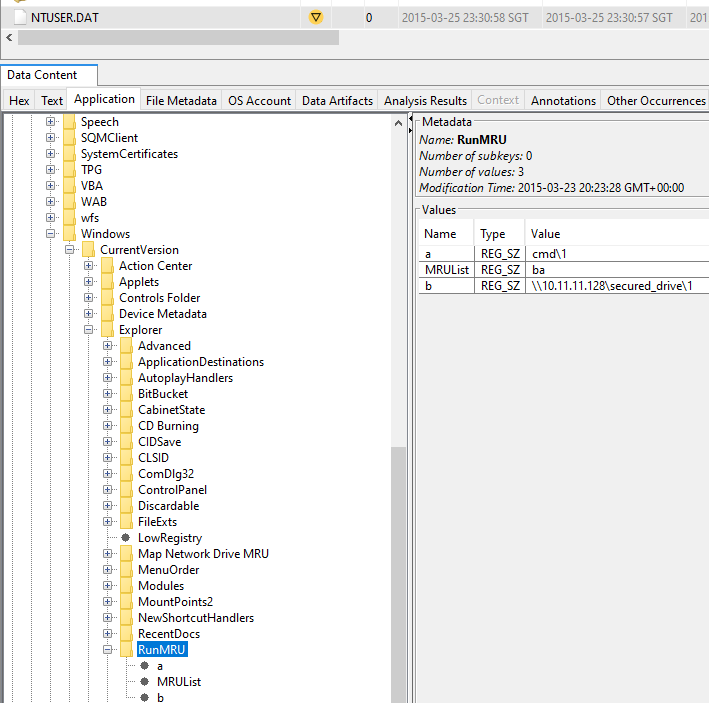
Answer:

*To look up the accessed name of the shared network folder and its IP address by the informant, the path to it are as follows:*

*C:\Users\Informant*

**

*The file contains information on where the user has browsed, which includes shared network drives. In the NTUSER.dat file itself, the Software folder has to be selected for further exploration. From there, the Microsoft, Windows, CurrentVersion, and then RunMRU.*

**

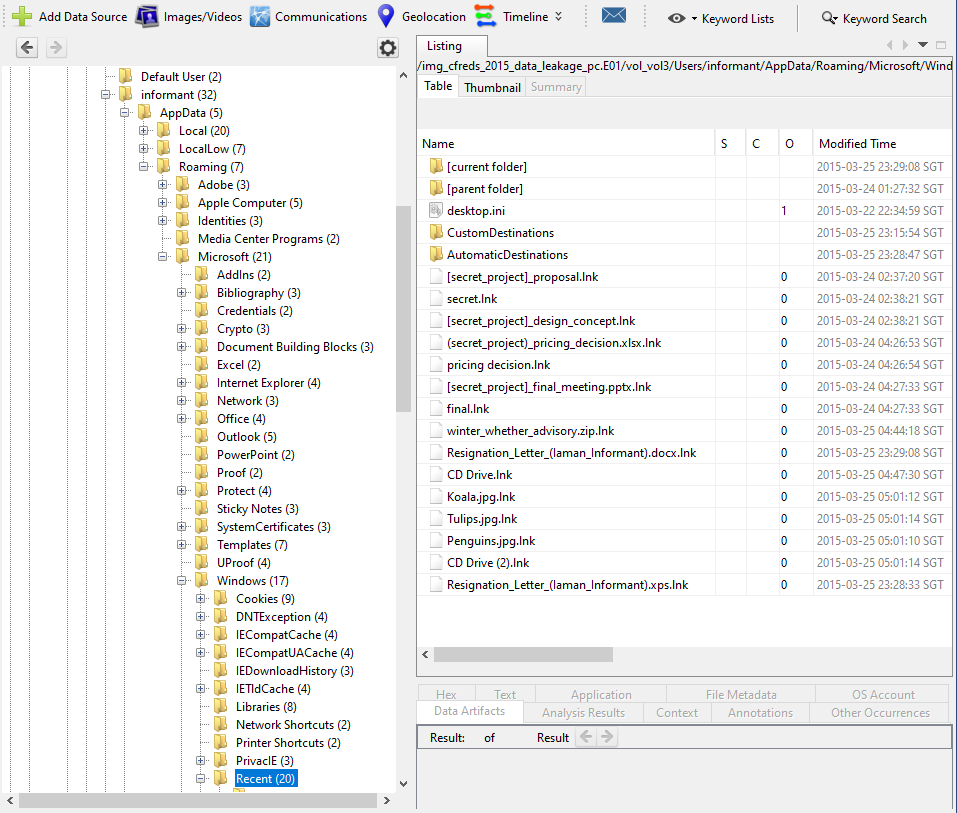
*As shown, the shared network drive’s IP address is 10.11.11.128*

* 1. What are the names of the confidential documents files in the shared network folder accessed by Mr. Informant and the date/time of the access?

Answer:

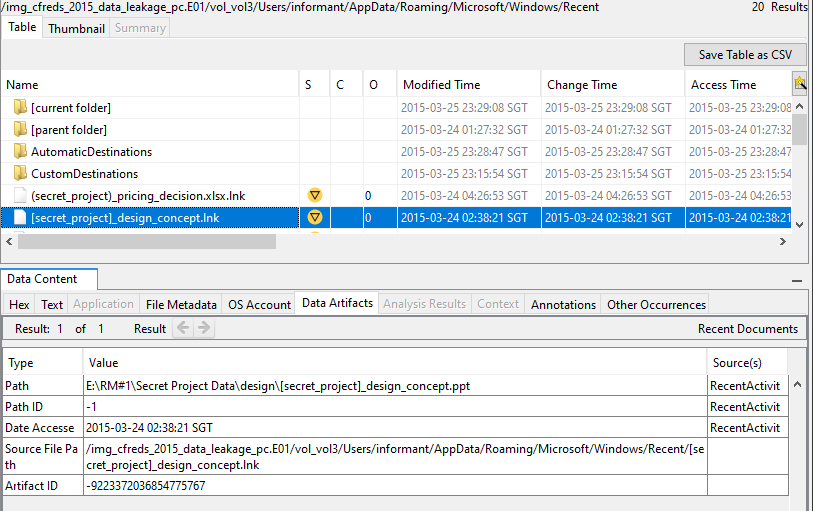
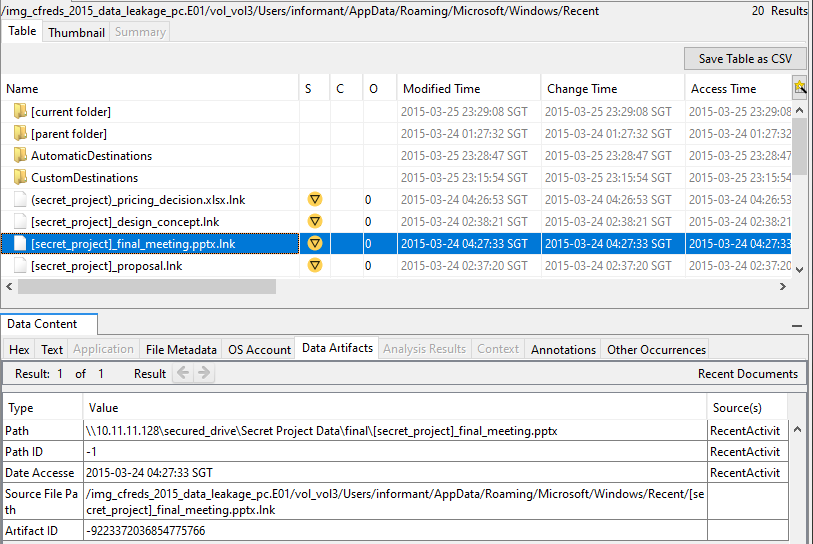
*To look up the name of the confidential files in the shared by the informant, the path to it are as follows:*

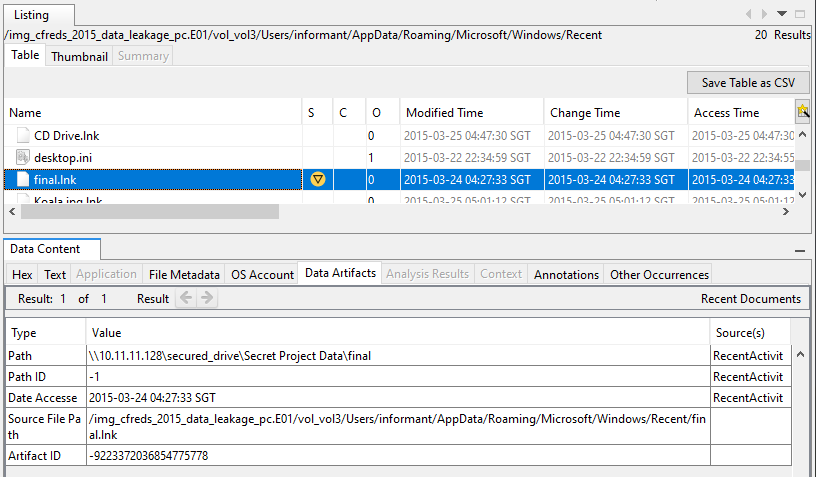
*C:\Users\Informant\AppData\Roaming\Microsoft\Windows\Recent*

**

*There are 5 confidential files accessed by Mr. Informant. They are:*

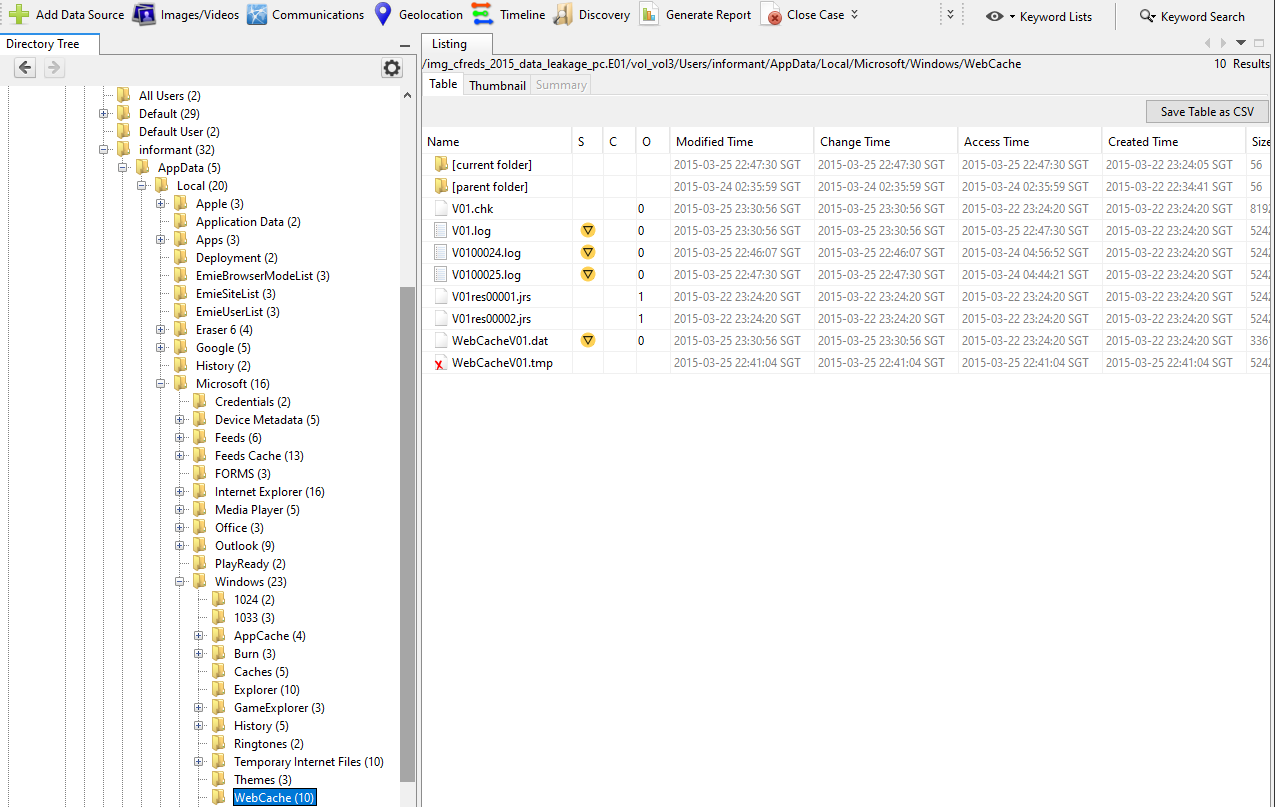
1. *Pricing\_decision.xlsx  
   A screenshot of a computer

   Description automatically generated*
   1. *Last time accessed: 2015-03-24 04:26:53 SGT*
2. *Design\_concept.lnk  
   *
   1. *Last time accessed: 2015-03-24 02:38:21 SGT*
3. *Final\_meeting.pptx.lnk  
   *
   1. *Last time accessed: 2015-03-24 04:27:33 SGT*
4. *Proposal.lnk  
   A screenshot of a computer

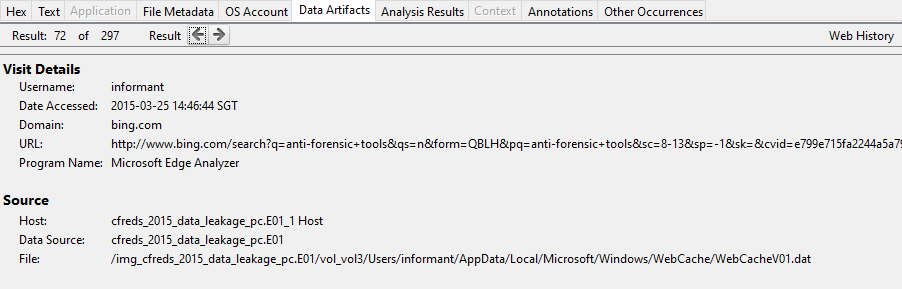
   Description automatically generated*
   1. *Last time accessed: 2015-03-24 02:37:20 SGT*
5. *Final.lnk  
   *
   1. *Last time accessed: 2015-03-24 04:27:33 SGT*
   2. Where did Mr. Informant obtain the anti-forensic tools such as eraser, and when these tools were installed onto the PC?

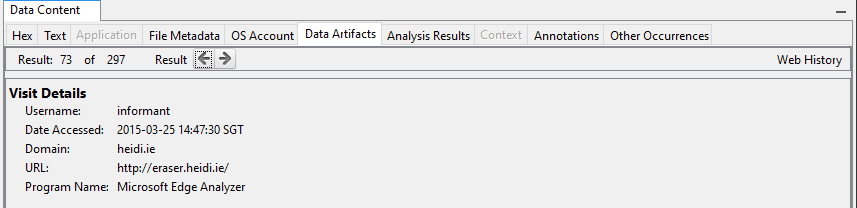
Answer:

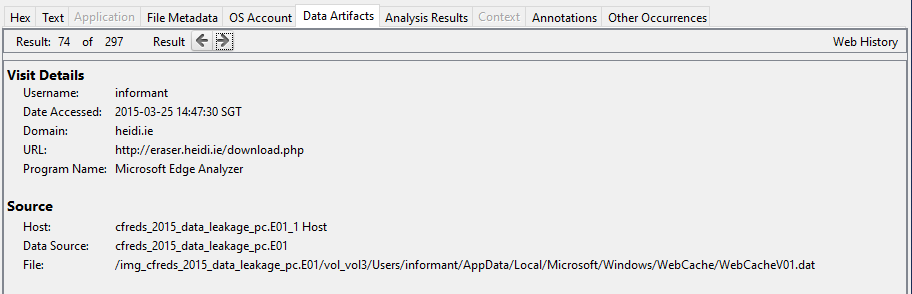
To find the where the anti-forensic tools were obtained, the WebCache file must be located, which is found in the C:\Users\Informant\AppData\Local\Microsoft\Windows\WebCache directory:

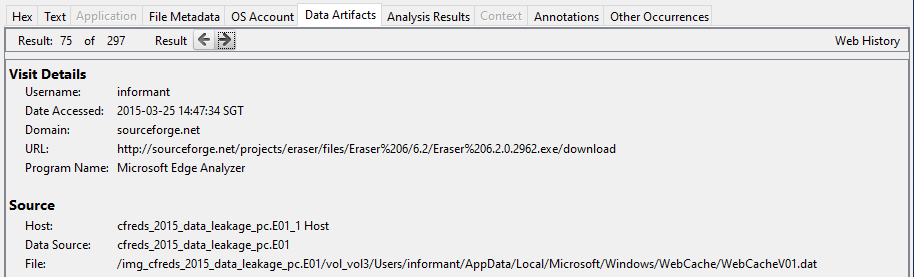


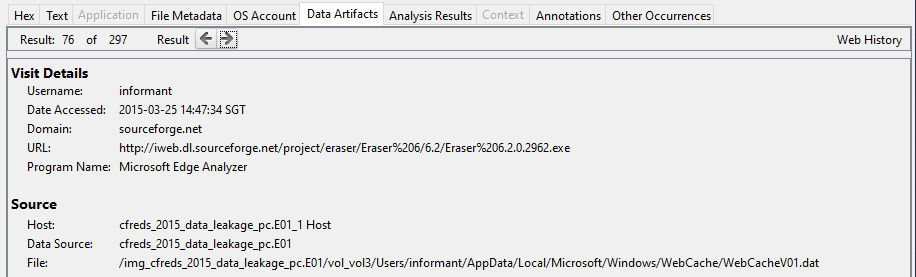
Using the WebCacheV01.dat file, the Informant’s web history can be searched. The following, entries 72-76, show the Informant searching, and downloading ‘Eraser’:









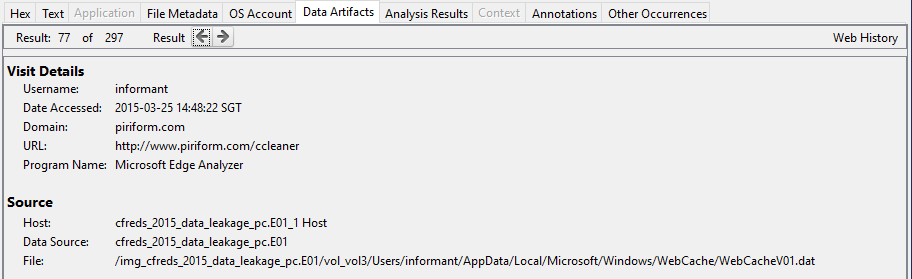


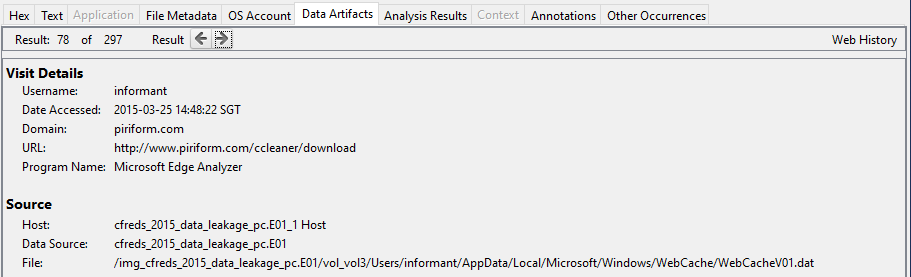
Eraser was downloaded from a website called ***sourceforge***. Its known creation time can be found in C:\Users\Informant\AppData\Local\Eraser 6. By checking the properties, the following can be obtained:

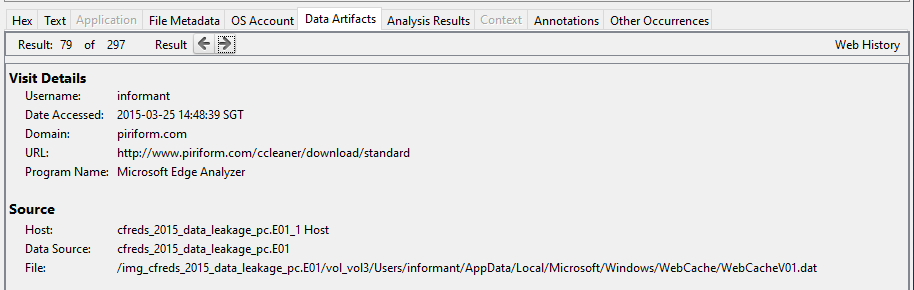


Creation Time: 2015-03-25 23:29:37 SGT

The next entries, 77-79, contain information of Informant downloading CCleaner:



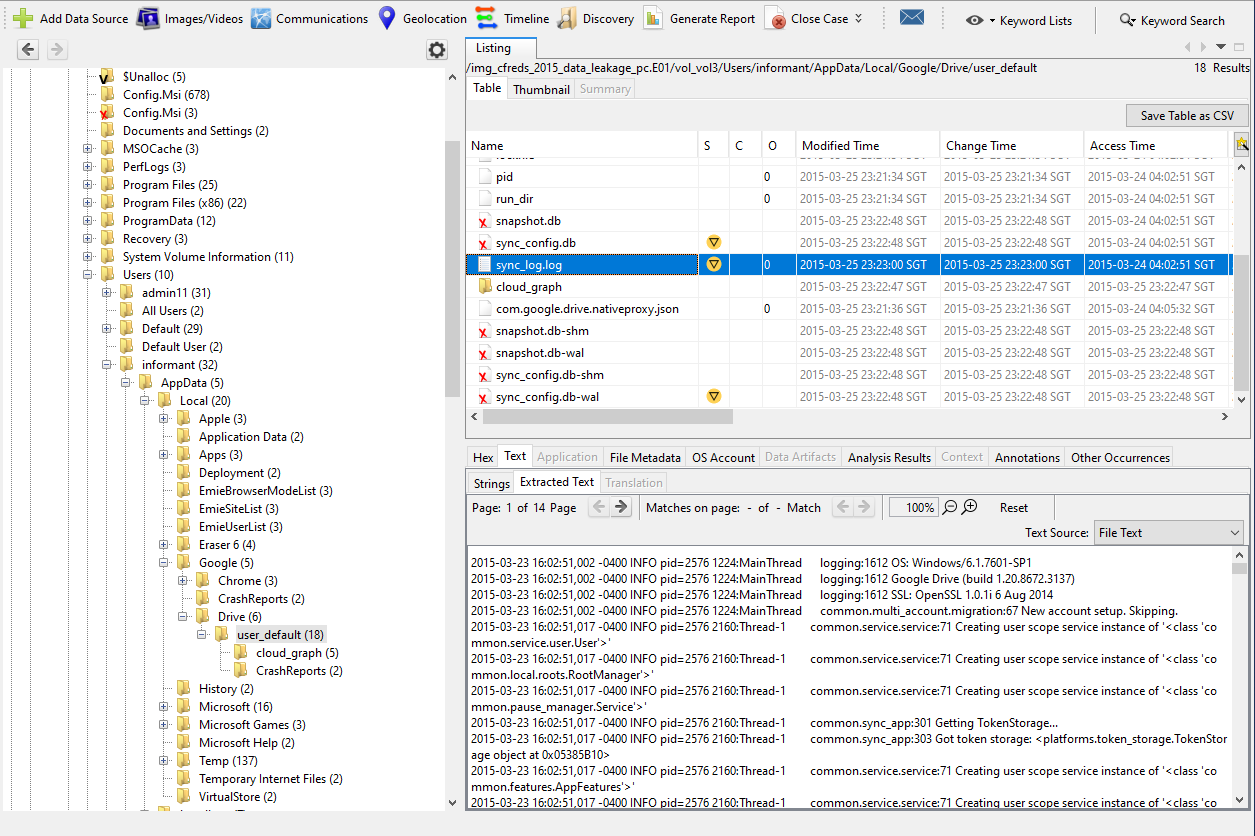




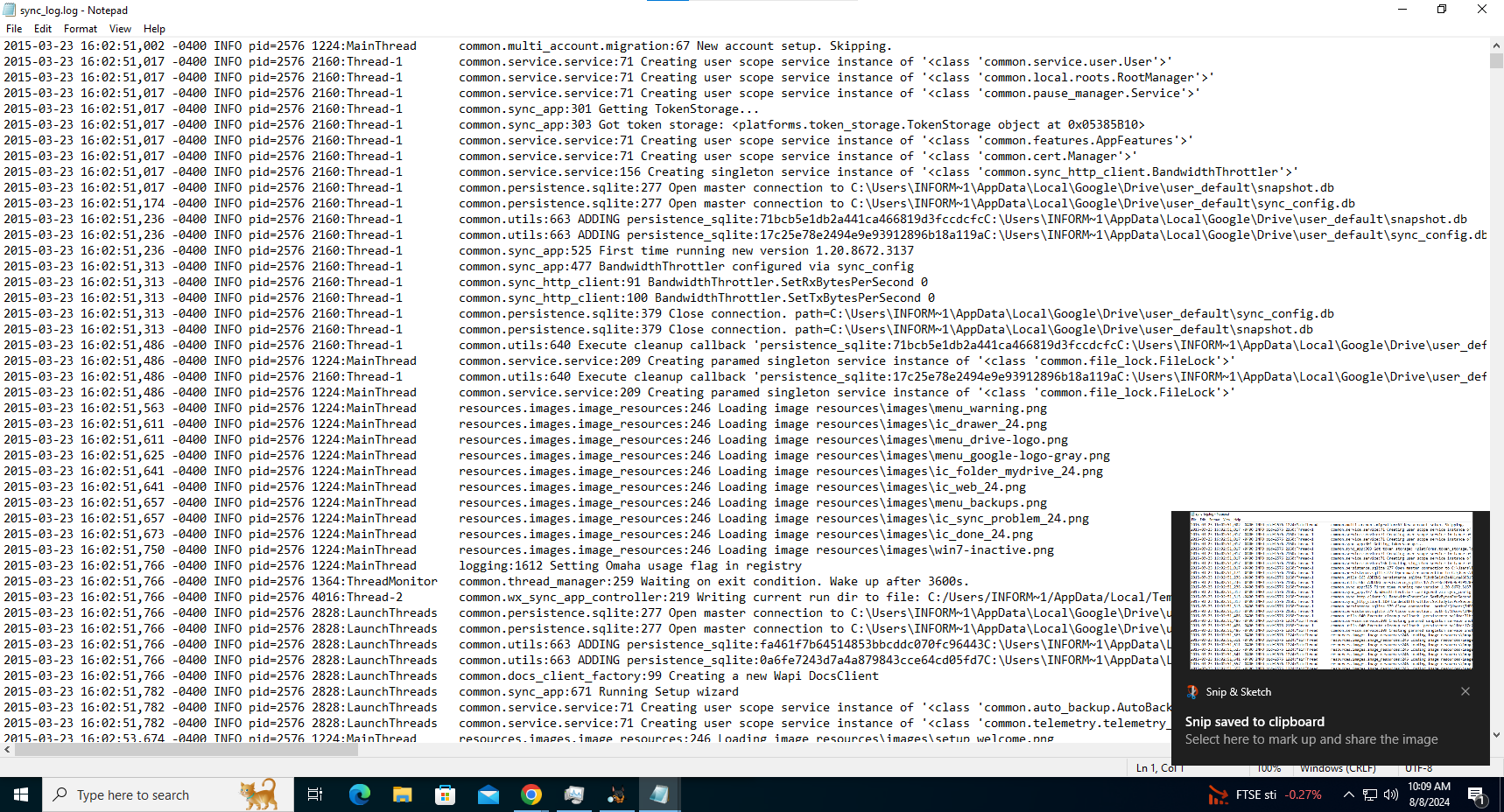
* 1. What were the files deleted by Mr. Informant from his Google Drive, and when?

Answer:

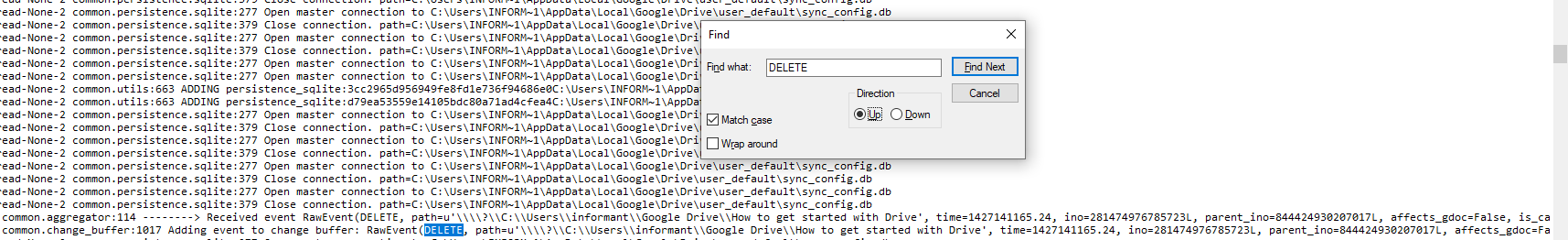
*To find files deleted by Mr.Informant from his Google Drive, information can be found in the C:\Users\Informant\AppData\Local\Google\Drive\user\_default directory. The ‘sync\_log.log’ file is selected to view all the activities done by the Informant:*

**

*The sync\_log.log file is then opened into an external viewer to read the logs:*

**

*To look for files that were deleted, the keyword ‘delete’ is entered for searching:*

**

The first item that was deleted was a file named ‘How to get started with Drive’.

Log entry:

*2015-03-23 16:06:05,256 -0400 INFO pid=2576 4004:LocalWatcher common.aggregator:114 --------> Received event RawEvent(****DELETE****, path=u'\\\\?\\C:\\Users\\informant\\Google Drive\****\How to get started with Drive****', time=1427141165.24, ino=281474976785723L, parent\_ino=844424930207017L, affects\_gdoc=False, is\_cancelled=<RawEventIsCancelledFlag.FALSE: 0>, backup=<Backup.NO\_BACKUP\_CONTENT: (False, False)>) None*

*2015-03-23 16:06:05,256 -0400 INFO pid=2576 4004:LocalWatcher common.change\_buffer:1017 Adding event to change buffer: RawEvent(****DELETE****, path=u'\\\\?\\C:\\Users\\informant\\Google Drive\****\How to get started with Drive****', time=1427141165.24, ino=281474976785723L, parent\_ino=844424930207017L, affects\_gdoc=False, is\_cancelled=<RawEventIsCancelledFlag.FALSE: 0>, backup=<Backup.NO\_BACKUP\_CONTENT: (False, False)>)*

*INFO pid=2576 3568:Worker-0 common.workers:188 Worker starting on [ImmutableChange(Direction.UPLOAD, Action.****DELETE****, ino=281474976785723, path=u'\\\\?\\C:\\Users\\informant\\Google Drive', name=u'****How to get started with Driv****e', parent\_ino=844424930207017, affects\_gdoc=False, backup=Backup.NO\_BACKUP\_CONTENT, is\_cancelled=False, is\_priority=False, hash=1109861798, \_constructor\_called=True)]*

*2015-03-23 16:06:07,426 -0400*

*INFO pid=2576 3568:Worker-0 common.workers:199 Worker successfully completed [ImmutableChange(Direction.UPLOAD, Action.****DELETE****, ino=281474976785723, path=u'\\\\?\\C:\\Users\\informant\\Google Drive', name=u'****How to get started with Drive****', parent\_ino=844424930207017, affects\_gdoc=False, backup=Backup.NO\_BACKUP\_CONTENT, is\_cancelled=False, is\_priority=False, hash=1109861798, \_constructor\_called=True)]*

*2015-03-23 16:06:08,456 -0400*

*2015-03-23 16:42:17,026 -0400 INFO pid=2576 4004:LocalWatcher common.aggregator:114 --------> Received event RawEvent(****DELETE****, path=u'\\\\?\\C:\\Users\\informant\\Google Drive\\****do\_u\_wanna\_build\_a\_snow\_man.mp3****', time=1427143336.964, ino=1125899906846942L, parent\_ino=844424930207017L, affects\_gdoc=False, is\_cancelled=<RawEventIsCancelledFlag.FALSE: 0>, backup=<Backup.NO\_BACKUP\_CONTENT: (False, False)>) None*

The second file, an mp3 file named ‘do\_you\_wanna\_build\_a\_snow\_man.mp3’:

*2015-03-23 16:42:19,369 -0400 INFO pid=2576 3568:Worker-0 common.workers:188 Worker starting on [ImmutableChange(Direction.UPLOAD, Action.****DELETE****, ino=1125899906846942, path=u'\\\\?\\C:\\Users\\informant\\Google Drive', name=u'****do\_u\_wanna\_build\_a\_snow\_man.mp3'****, parent\_ino=844424930207017, affects\_gdoc=False, backup=Backup.NO\_BACKUP\_CONTENT, is\_cancelled=False, is\_priority=False, hash=-1363400622, \_constructor\_called=True)]*

And the last file to be deleted from the Informant’s Google Drive, is an image file named ‘happy\_holiday.jpg’:

*2015-03-23 16:42:19,385 -0400 INFO pid=2576 2820:Worker-1 common.workers:188 Worker starting on [ImmutableChange(Direction.UPLOAD, Action.****DELETE****, ino=4503599627374809, path=u'\\\\?\\C:\\Users\\informant\\Google Drive', name=u****'happy\_holiday.jpg'****, parent\_ino=844424930207017, affects\_gdoc=False, backup=Backup.NO\_BACKUP\_CONTENT, is\_cancelled=False, is\_priority=False, hash=481398202, \_constructor\_called=True)]*

*2015-03-23 16:42:20,072 -0400 INFO pid=2576 2820:Worker-1 common.workers:199 Worker successfully completed [ImmutableChange(Direction.UPLOAD, Action.****DELETE****, ino=4503599627374809, path=u'\\\\?\\C:\\Users\\informant\\Google Drive', name=u****'happy\_holiday.jpg'****, parent\_ino=844424930207017, affects\_gdoc=False, backup=Backup.NO\_BACKUP\_CONTENT, is\_cancelled=False, is\_priority=False, hash=481398202, \_constructor\_called=True)]*

**Task 2 Network Traffic Data Forensics (6 marks)**

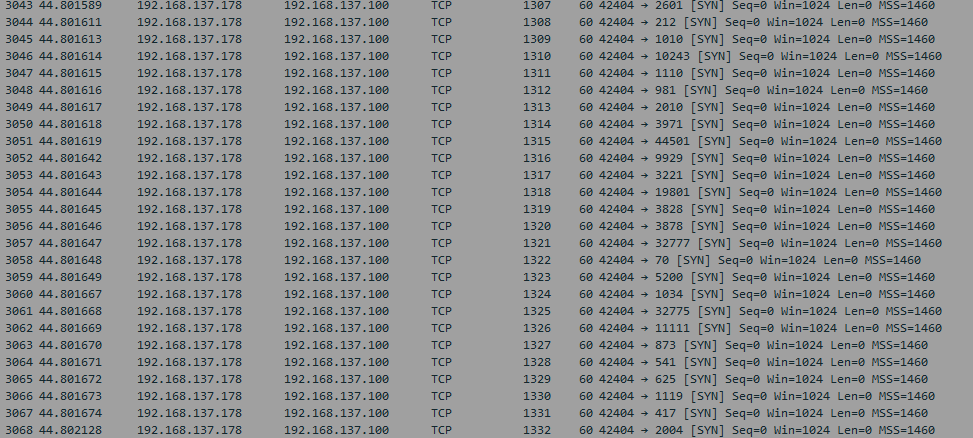
1. What are the IP addresses (or MAC addresses) of the suspected attackers? Given reasons and screenshots to justify your answer.

Answer:

From Question (2), it has been noticed that the suspected victims have sent a lot of RST ACK TCP packets to a particular address, which is 192.168.137.178 (MAC address dc:a6:32:dc:27:d5). Therefore, that address will be checked for suspicious activity.

And as it turns out, that address has sent a lot of SYN packets to the suspected victim addresses:

192.168.137.178 -> 192.168.137.100



192.168.137.178 -> 192.168.137.206

A screenshot of a computer screen

Description automatically generated

192.168.137.178 -> 192.168.137.234

A screenshot of a computer

Description automatically generated

192.168.137.178 -> 192.168.137.59

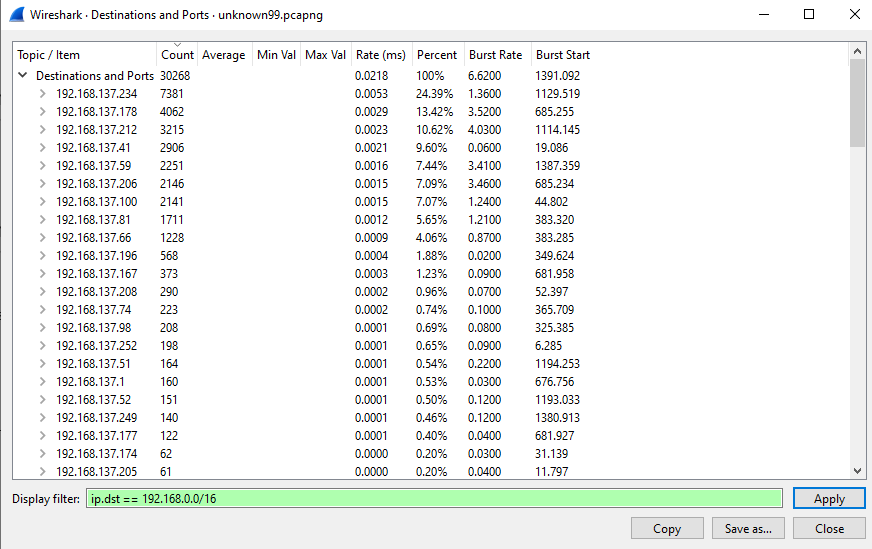
A screenshot of a computer screen

Description automatically generated

1. What are the IP addresses (or MAC addresses) of the suspected victims? Given reasons and screenshots to justify your answer.

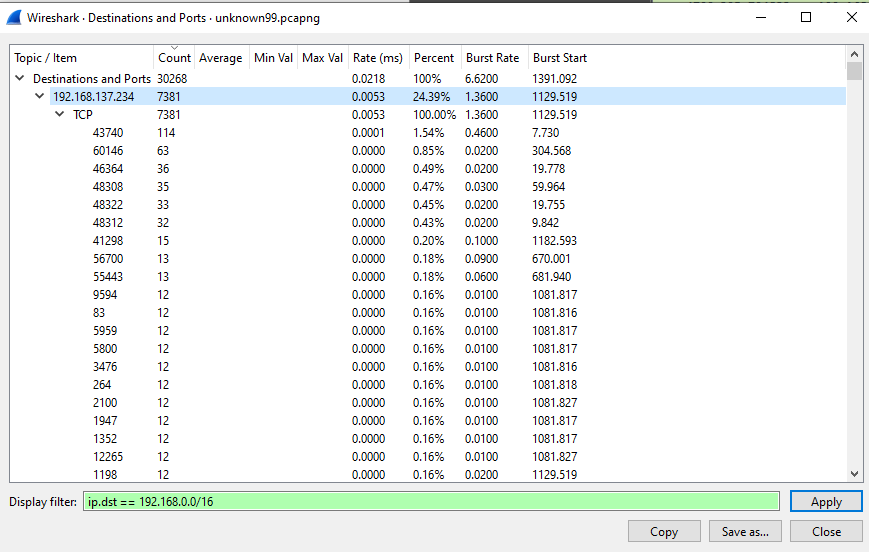
Answer:

To search for suspected victims, the Statistics feature is first used to get an overview of the most popular destinations:



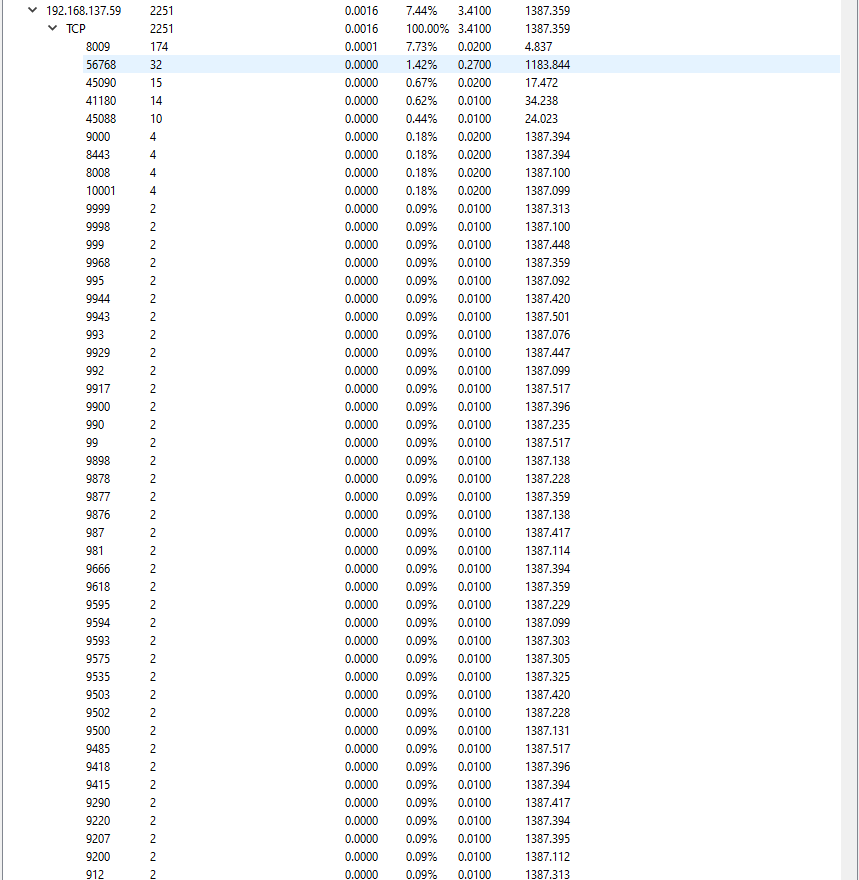
The filter of ip.dst == 192.168.0.0/16 looks for private Class C address. By expanding the addresses that received the most traffic, several observations are made:

The address 192.168.137.234 (MAC address 08:7c:39:ce:6e:2a) has communicated on many uncommon TCP ports:



This is also true for the following addresses:

192.168.137.59 (MAC address cc:f4:11:9c:d0:00)

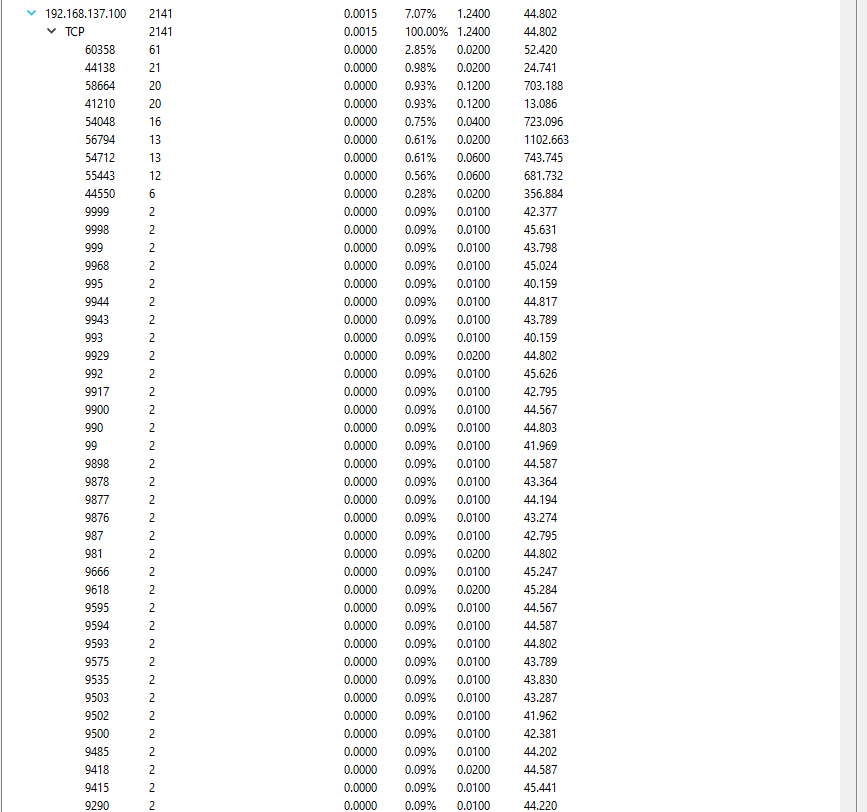


192.168.137.206 (MAC address 1c:12:b0:9b:0c:ec)

A screenshot of a computer

Description automatically generated

192.168.137.100 (MAC address 1c:fe:2b:98:16:dd)

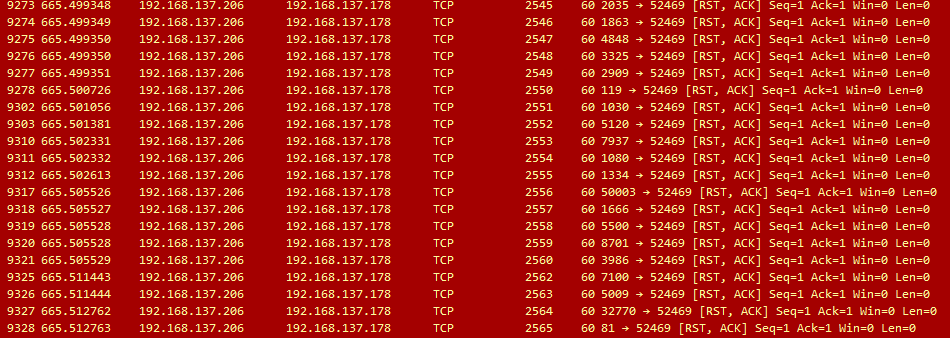


To prove that those addresses are victims, the next thing to do is to observe the traffic these addresses received. The mentioned addresses have a common trend in the types of traffic they receive:

192.168.137.234



192.168.137.206

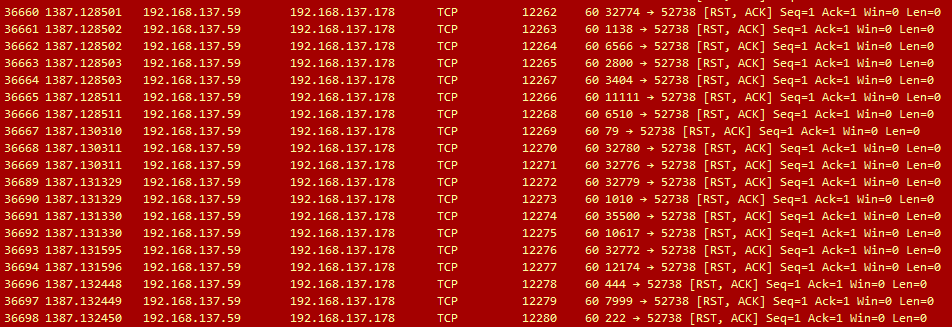


192.168.137.100

A screenshot of a red screen

Description automatically generated

192.168.137.59



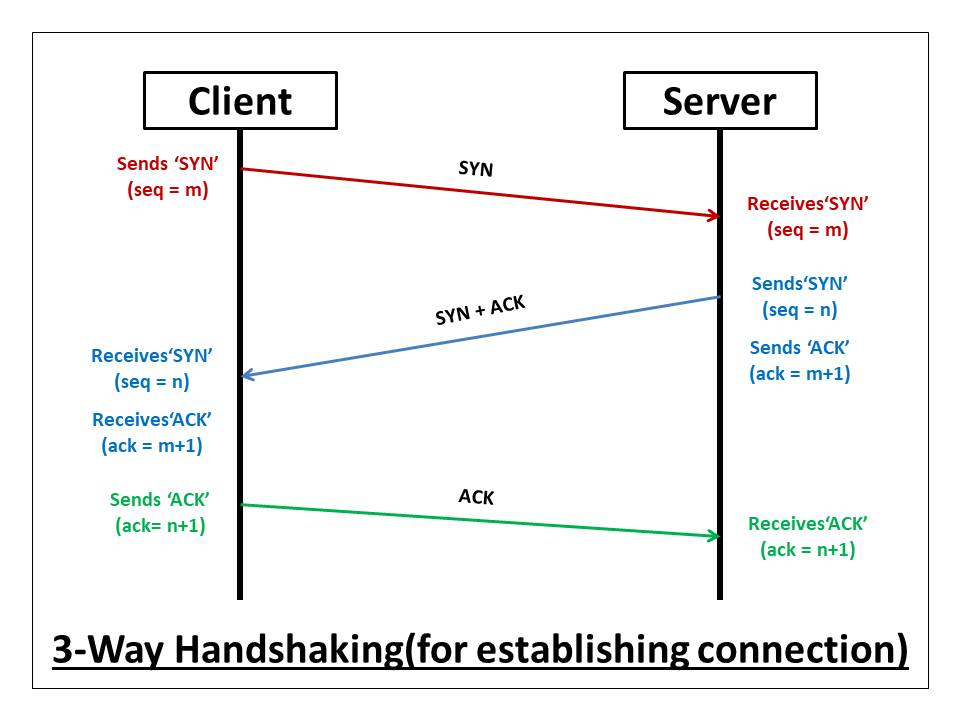
As shown, all 4 victims have sent a worrying amount of RST ACK TCP packets back to a particular address. This could be a possible Port Scanning attack and should be investigated.

1. What are the suspected network attacks? Given reasons and screenshots to justify your answer.

Answer:

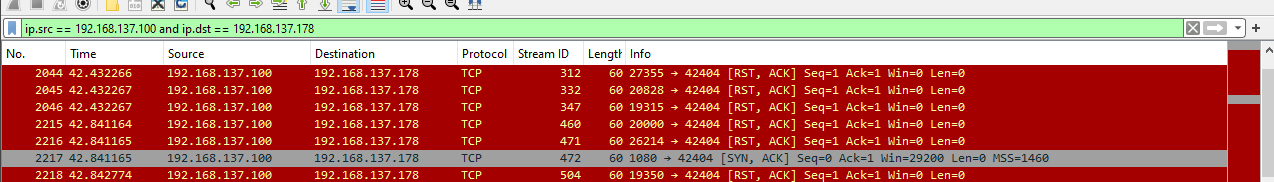
Given Question (1)’s observation that 192.168.137.178 is sending a lot of SYN to packets to its victims (.234, .206, .100, and .59) as seen in Question (2), who replies with a lot of RST ACK packets, the suspected network attack done is a TCP Port Scanning attack.

Typically, during a TCP connection, the 3-way handshake is made.



This process is completed by the target sending a SYN ACK and the client responding with an ACK to create the connection. In this case, the client (attacker) sends many SYN packets to multiple addresses, attempting to get a response from various port numbers (e.g. 20011, 3325, 32772, etc.). However, the targets respond by sending an RST, ACK back. By receiving this information, the attacker will know those ports are turned off, and will continue the search until a port is open.

Looking into the entries, 192.168.137.178 has received a SYN ACK during its port scanning with 192.168.137.100



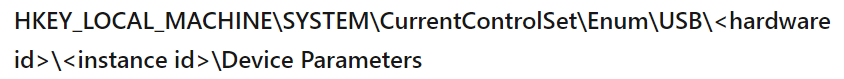
The response shows that port 1080 is open. With this information, an attacker can look into vulnerabilities regarding this port, and therefore exploit it to gain access into the system.

Example of Questions and Answer

Question 1) What USB device is connected to the computer on 3 July 2013 and who logged onto the computer at that time?

Answer:

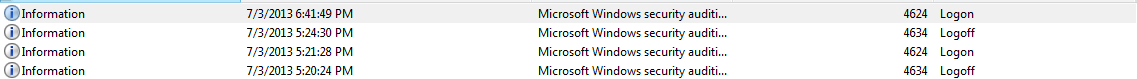
**Data Source**: SYSTEM Registry Hive File





From the system registry hive file shown in the above screenshot, USB drive with the USB device serial no ABBECF17 was first connected on 3 July 2013, 18:52:38 SGT

**Data Source**: Windows Security event log





From the Windows Security event shown in the screenshot above, Account name Michael logged onto the computer on 3 July 2013 at 6:41:49 PM SGT