ITIS 4250 / 5250

Shivani Sathe

Semester Project

5th December 2021

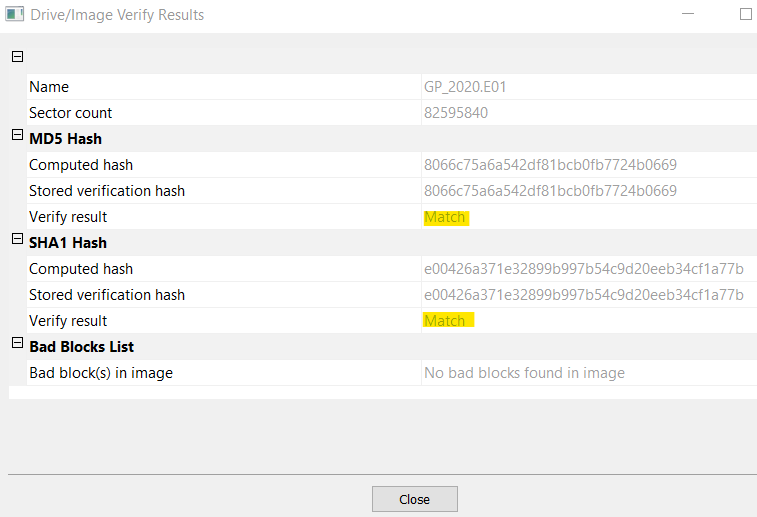
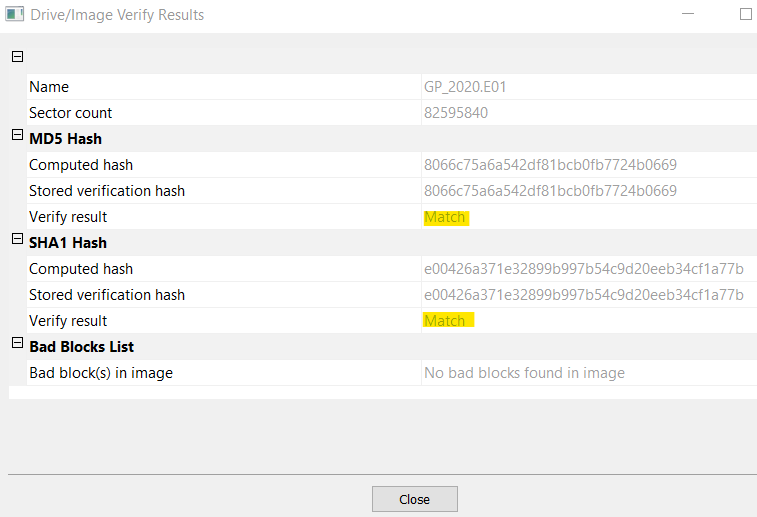
**Overview:**

On December 5, 2021, Detective Jessica Fletcher of the UNC Charlotte police department had asked me to process a desktop computer for her. With the help of North Carolina District Court Search Warrant, a computer belonging to Gene Poole was brought to forensics lab of the University of North Carolina at Charlotte since NC Charlotte police department does not have their own forensics lab, the University had agreed to have the student lab process cases for them. One of the lab techs produced an EnCase E01 format forensic image of the subject’s computer in preparation for the examination (named GP2020.E01). An archive of the subject's email account was also provided. No other evidence items were found at the scene. Detective Jessica Fletcher was determined that to further the investigation, the forensic analysis to include finding the owner of the picture, the timezone, the file system used in the criminal activity conversation, and other factors that would aid in solving the case.

For reference, Eugene "Gene" Poole is a prior felon, who is believed to be involved in the manufacture and sale of drugs. His current associates are unknown. He and his associates have shown varying degrees of technical ability with computers.

**Forensic Acquisition & Exam Preparation**

To begin the analysis, Windows 10, 64-bit system was used. The forensic image files GP\_2020.E01 were placed in a newly created folder named ‘**Semester Project**’ on desktop.. Later, AccessData FTK Imager 4.5.0.3 was used to verify the MD5 hash value of both the images before starting the analysis and also at the end of the analysis. RegRipper tool was used to find the last login through SAM file and NTUSER.Dat file and DB Browser for SQLite was used to analyze the skype chats.

*Hash verification before analysis Hash verification after analysis*

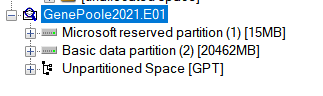
**Findings and Report (Forensic Analysis)**

1. **Account for how all the space on the computer hard drive was used (partitions, used/free).**

Ans. Using AccessData FTK Imager, it was seen that the image had 3 partitions. 1 of them is

Unpartitioned Space and the other two are Microsoft reserved partition – 15 MB Basic Data

Partition – 20462 MB



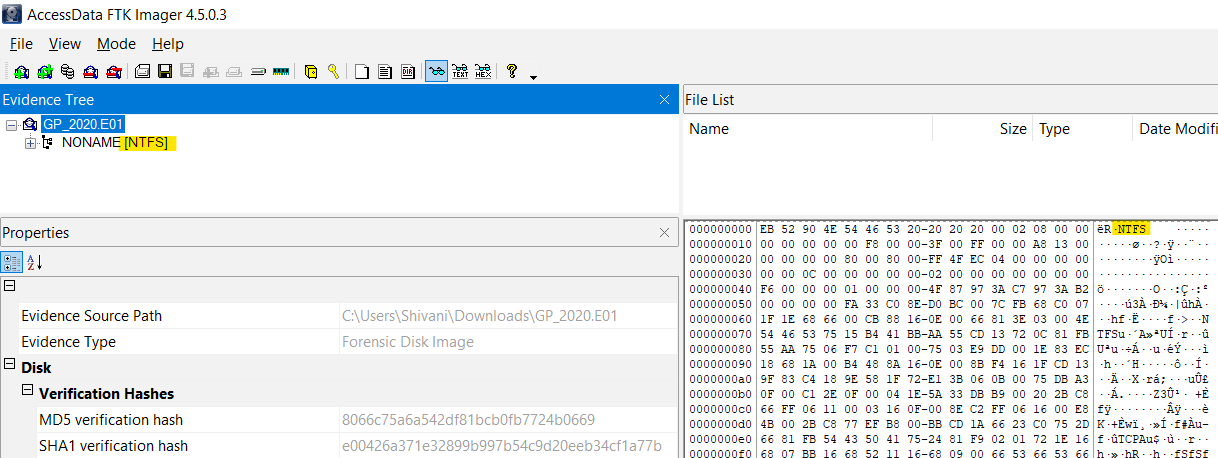
From Autopsy, 4 partitions of the image file were observed. 2 of them were Unallocated

and other two were Microsoft reserved partition and Basic Data Partition



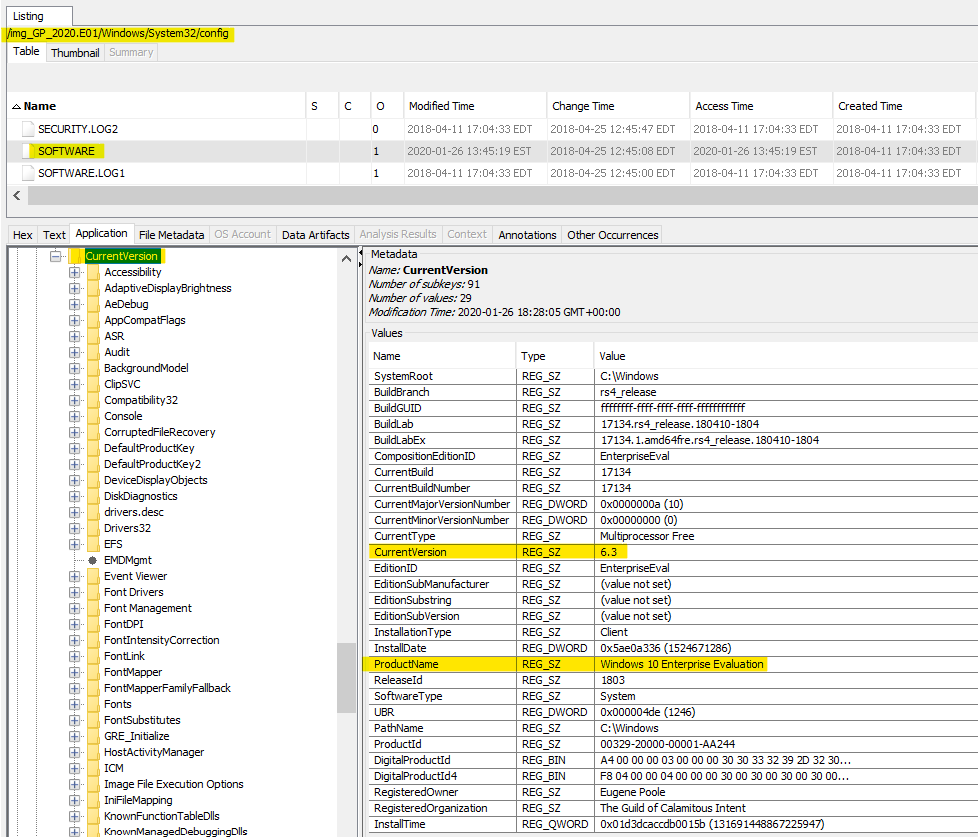
1. **Identify the type of file systems in use.**

Ans. When loaded the image file in Access Data FTK Imager, its seen that the file system in use is **NTFS**.

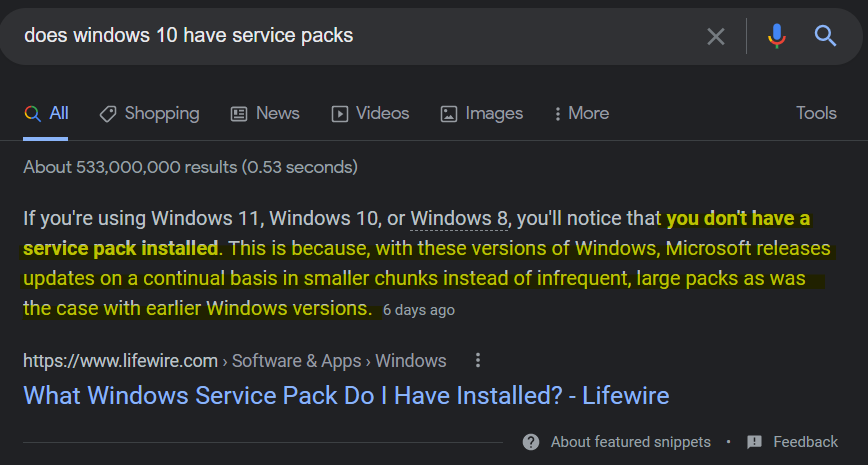
****

1. **Identify the version and service pack of the Operating System.**

Ans: Using Autopsy, the current version is 6.3 which was found in Software hive at path /Windows/System32/config/SOFTWARE:/ Microsoft\Windows NT\CurrentVersion.

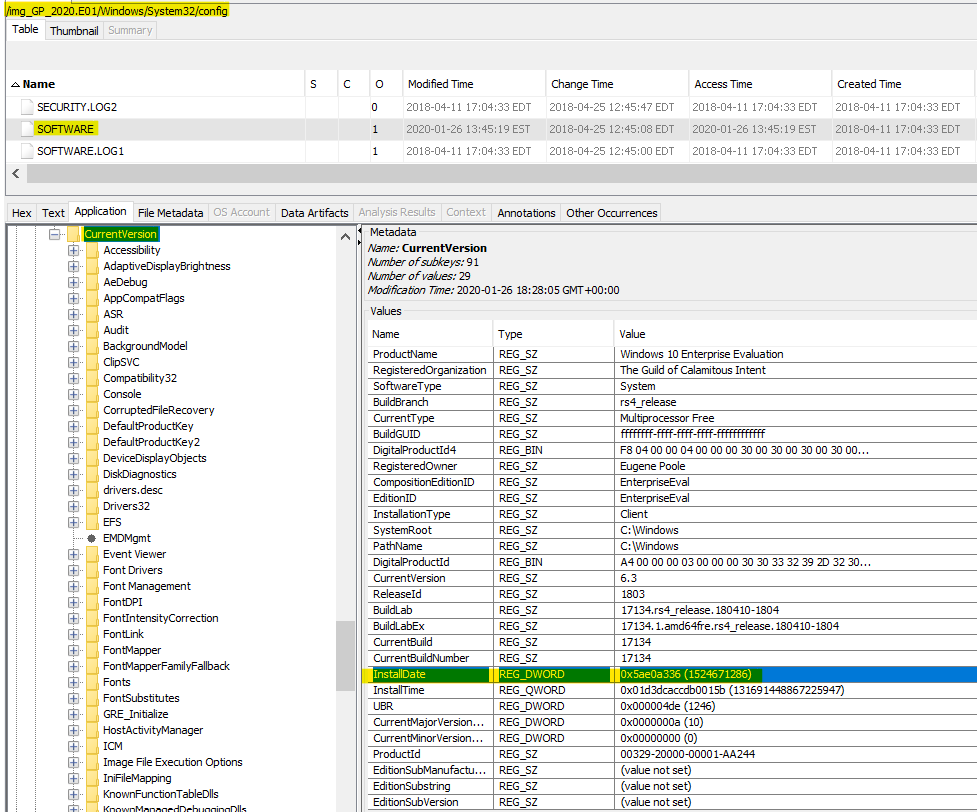


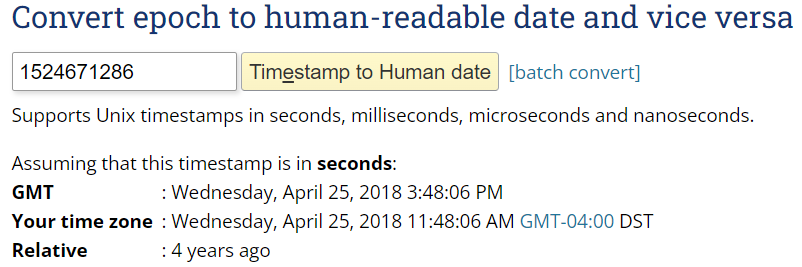
Windows 10 does not have a service pack. Please refer to below screenshot.

****

1. **Find the date the OS was installed.**

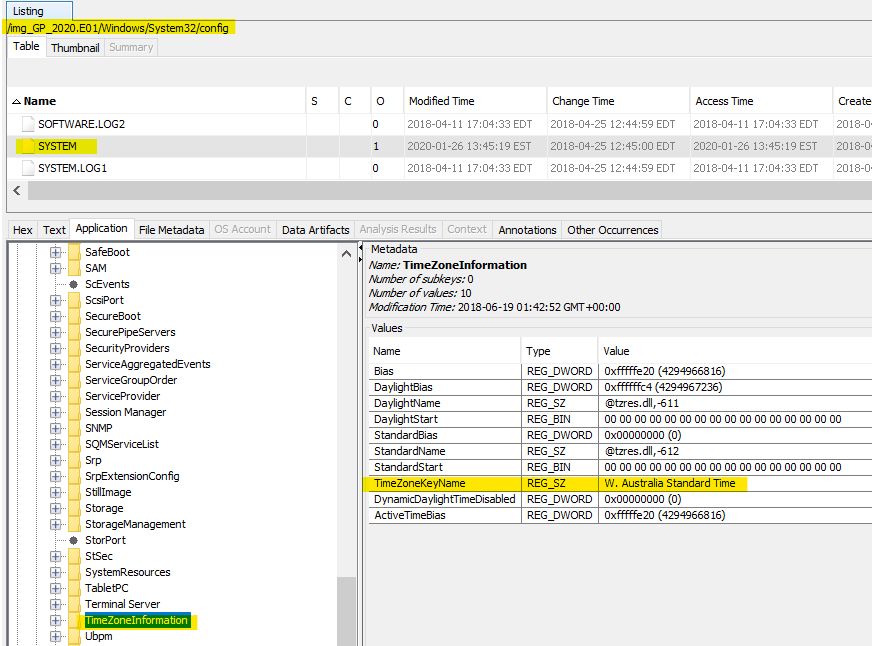
Ans: The OS was installed on date Wednesday, April 25, 2018 3:48:06 PM GMT. This was found using Autopsy in Software hive under InstalledDate field at path /Windows/System32/config/SOFTWARE:/ Microsoft\Windows NT\CurrentVersion. The date was in epoch format as seen in below screenshot. <https://www.epochconverter.com/> was used to convert it into human readable format.



****

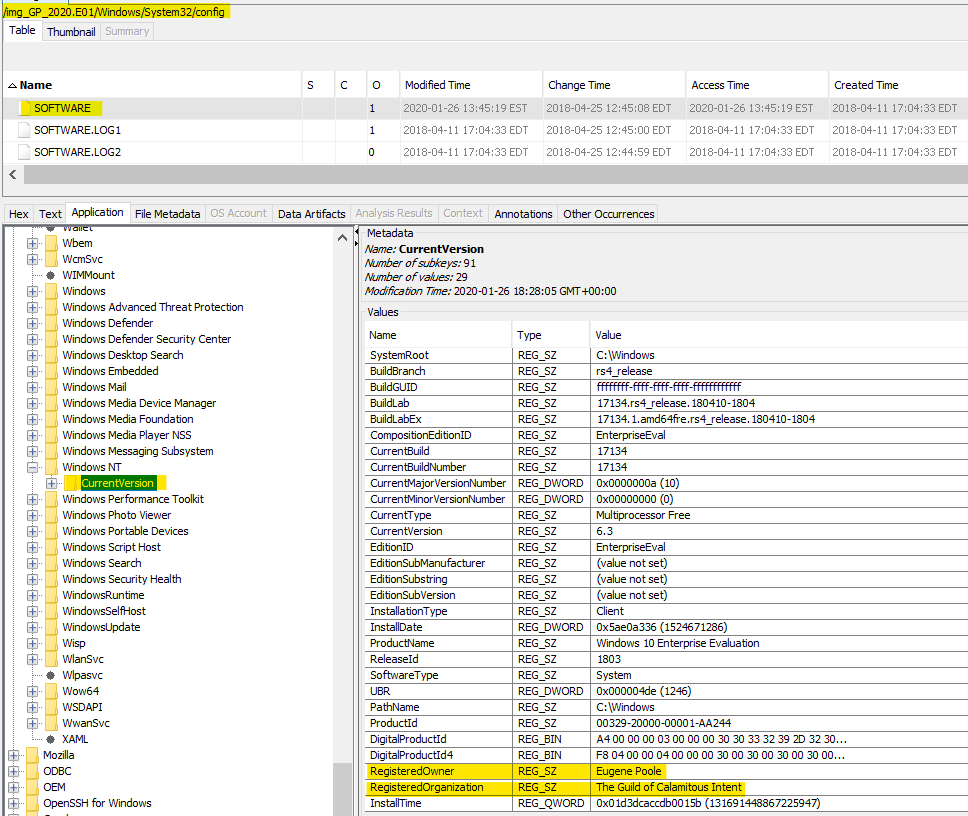
1. **Identify the Time Zone information for the computer.**

Ans: The Time Zone of the computer is W. Australia Standard Time. This was found using Autopsy in System hive under TimeZoneKeyName field at path **/Windows/System32/config/SYSTEM:/ControlSet001/Control/TimeZoneInformation**



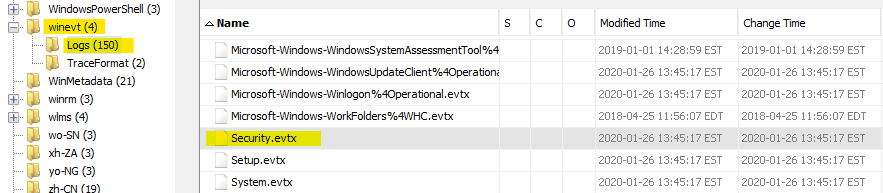
1. **Show the owner of the computer.**

Ans: The owner of the computer is Eugene Poole and the organization is the Guild of Calamitous Intent. This information was found using Autopsy under Software Hive in RegisteredOwner and RegisteredOrganization fields at path /Windows/System32/config/SOFTWARE:/ Microsoft\Windows NT\CurrentVersion

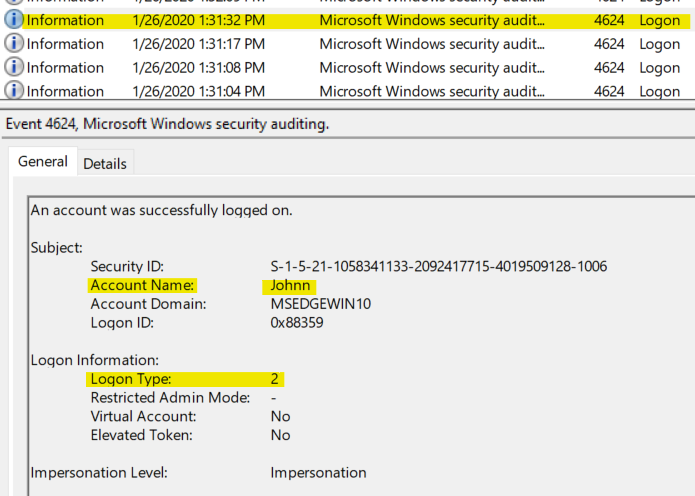
****

1. **Show what account was used to log in and the log in method.**

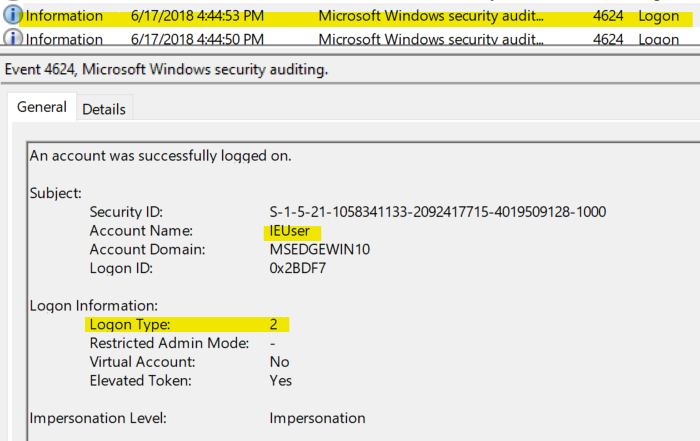
Ans: To find the account used to log in and the login method, Security.evtx file was opened in Event Viewer from path Data Sources - GP\_2020.E01 - Windows - System32 - winevt – logs.

****

After opening the file in Event Viewer, the logs were filtered based on Event ID 4624 which showed all logon logs only. Account with name Johnn was seen to be used for login with logon type 2 i.e Interactive (Keyboard) which was the login method

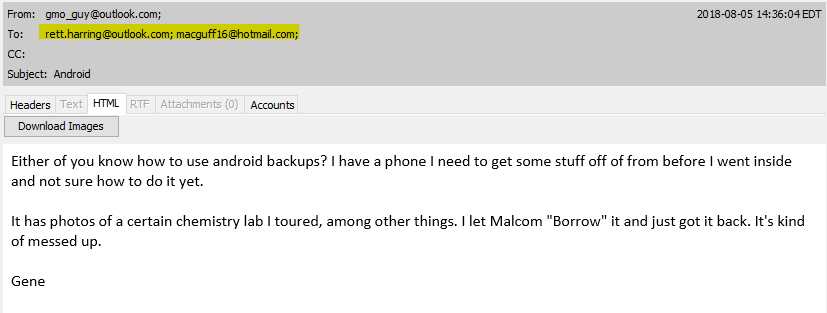


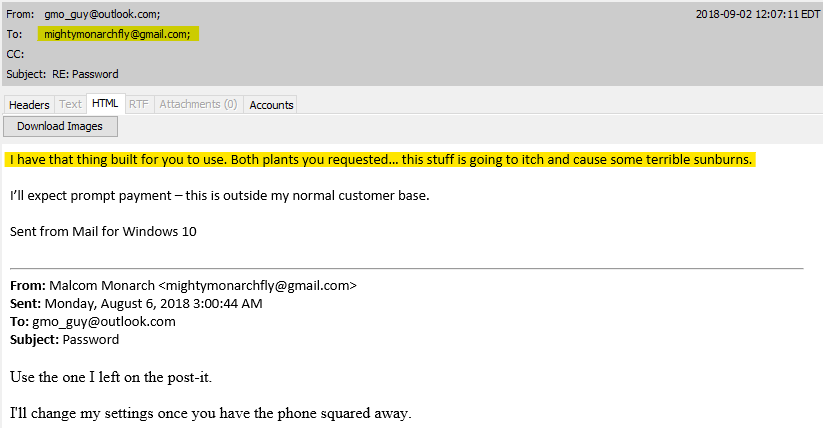
Similarly, another account with name IEUser was seen to be used for login with logon type 2 i.e Interactive (Keyboard) which was the login method.



1. **Identify any associates involved in the criminal activity.**

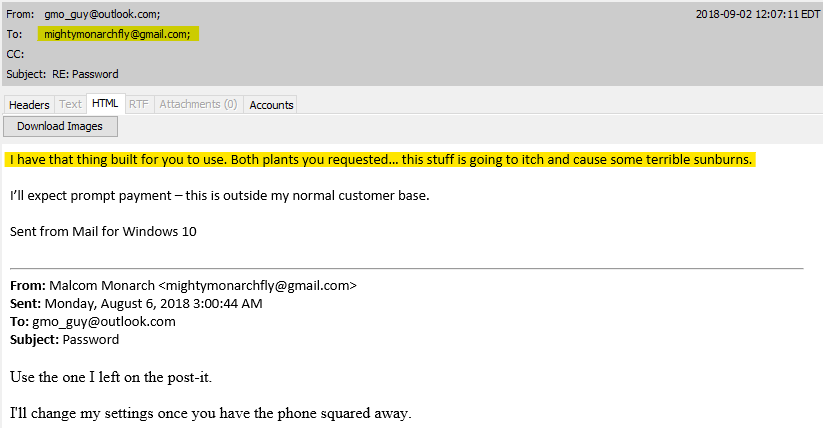
Ans: The associates who are involved in criminal activity are **rett.harring@outlook.com macguff16@hotmail.com and mightymonarchfly@gmail.com**. In Autopsy, few emails were observed to be exchanged with above mail aliases. This was found at path Data Artifacts - E-Mail Messages - Default ([Default)] – Default. Below are screenshots of criminal activity email communications.

****

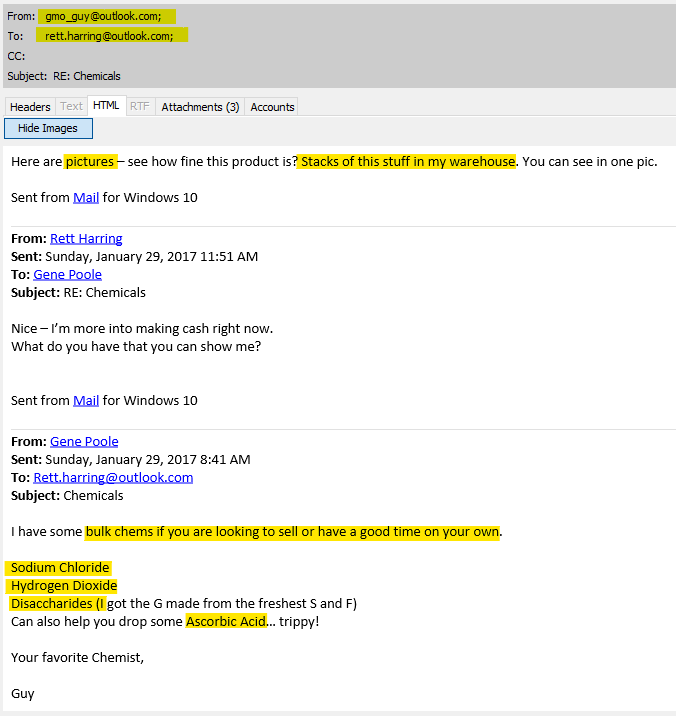
****

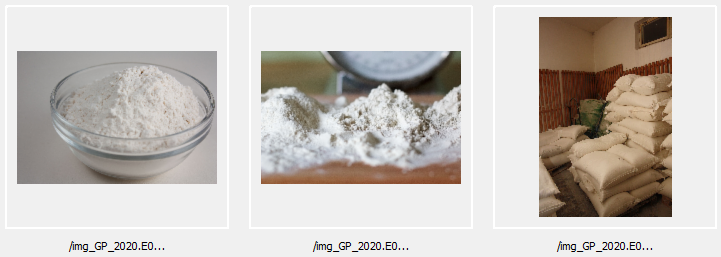
1. **Provide any communications the user engaged in with associates about criminal activity.**

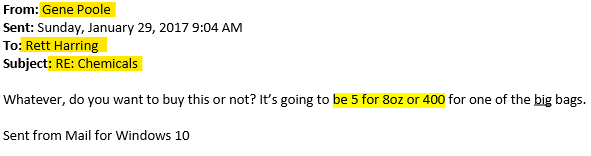
Ans: Some email communications were found at Data Artifacts - E-Mail Messages - Default ([Default)] – Default. Below is a communication between Gene Poole and Malcom Monarch about a harmful stuff Malcom must have asked Gene to make.

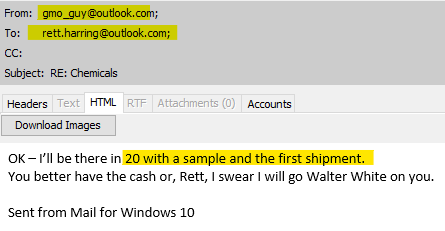
****

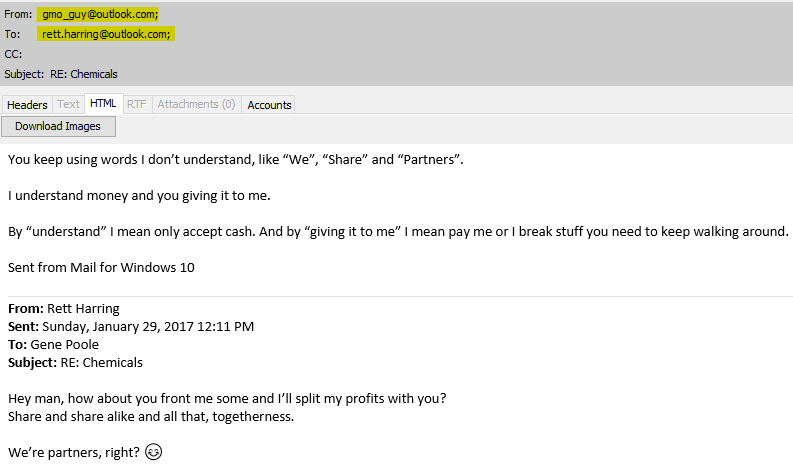
Below is another communication between Gene Poole and Rett Harring about Gene Poole selling some chemicals and Rett Harring is interested in buying them.





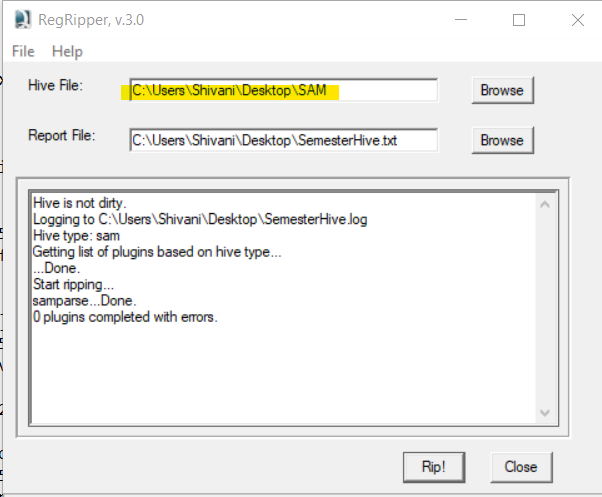




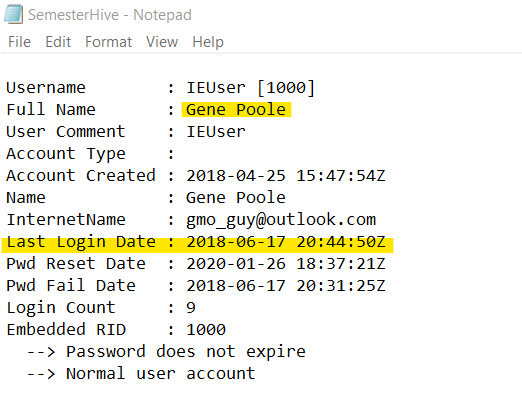


1. **Identify the last date and time the user logged on.**

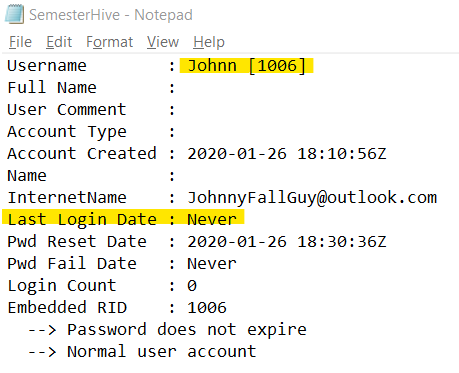
Ans: To find the last login date, from Autopsy, the SAM file was extracted from path Windows\System32\Config\SAM. Using RegRipper tool, this SAM file was ripped to observe its contents.



The last login date is of user Gene Poole is 2018-06-17 20:44:50Z

****

The last login date of user Johnn is Never.

****

1. **Identify files placed in the recycle bin by the user, to include date deleted.**

Ans: Using Autopsy, the files placed recycle bin were found at path Data Artifacts - Recycle Bin. The files placed in recycle bins were:

- TheMountains.txt

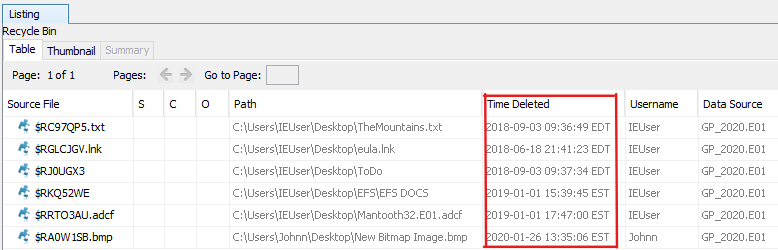
- eula.lnk

- ToDo

- EFS DOCS

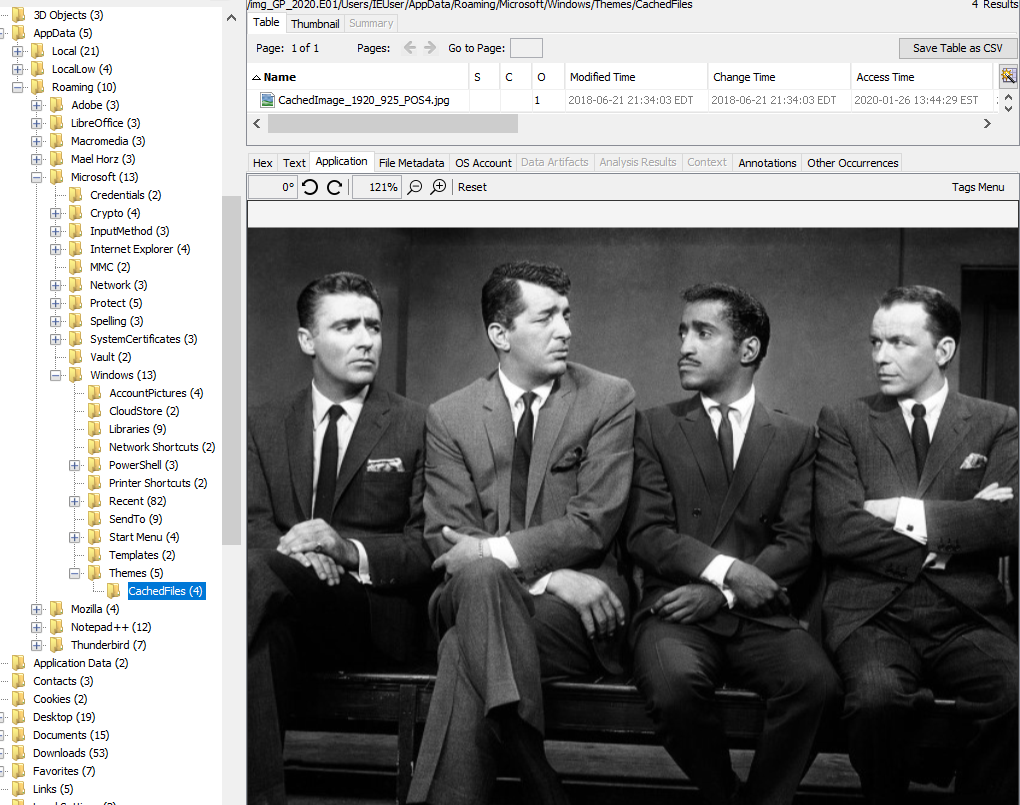
- Mantooth32.E01.adcf

- New Bitmap Image.bmp

****

1. **Recover the user's background image.**

Ans: The user’s background image was found using Autopsy at path Data Sources -GP\_2020.E01 - Users - IEUser - AppData - Roaming - Microsoft - Windows - Themes CachedFiles

****

1. **Identify any locations other than the subject's home that may have been involved (this does not require an exact address and may include directions, maps, conversations, notes, etc).**

Ans: Using Autopsy, at path Data Artifacts – Web History multiple search results regarding directions to the following places were found.

- charlotte to boone nc,

- charlotte to Cashiers, North Carolina,

- charlotte to Salemburg, North Carolina,

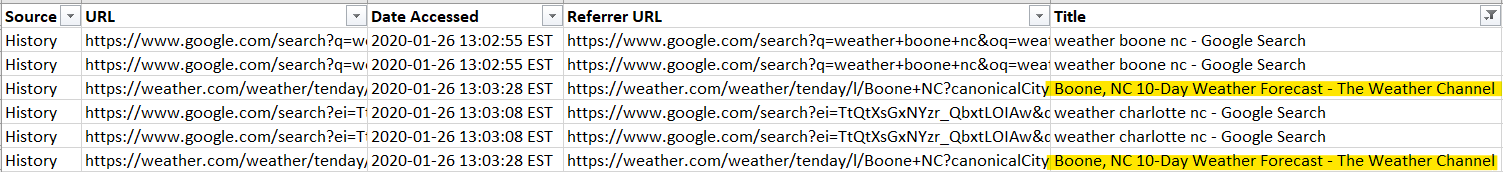
- charlotte to Mt Airy, North Carolina,

- charlotte to Pinebluff, North Carolina.

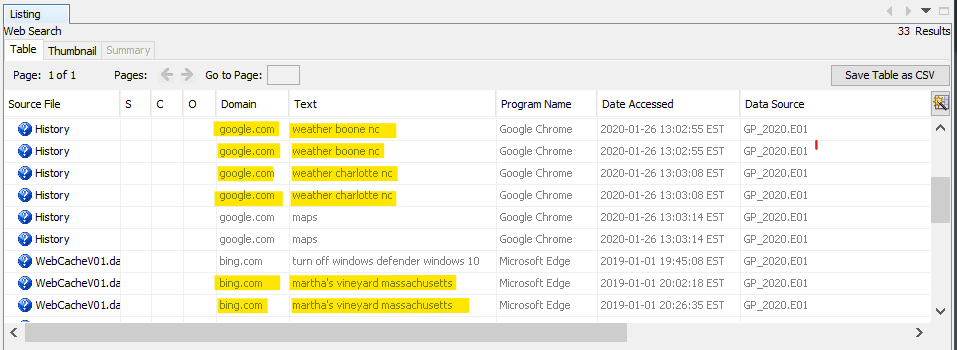
To inspect the Web History, the table was exported as a CSV from Autopsy. The title column in the CSV file was filtered with the keyword ‘maps’. Below is the screenshot of the results.

****

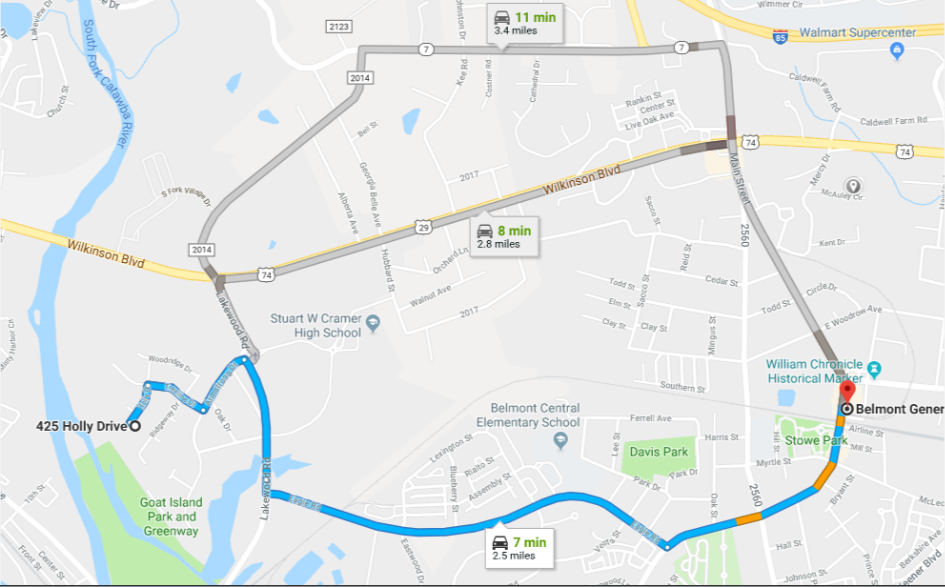
On filtering the Title column with keyword ‘weather’, searches regarding 10-day weather forecast of Boone, NC was observed.

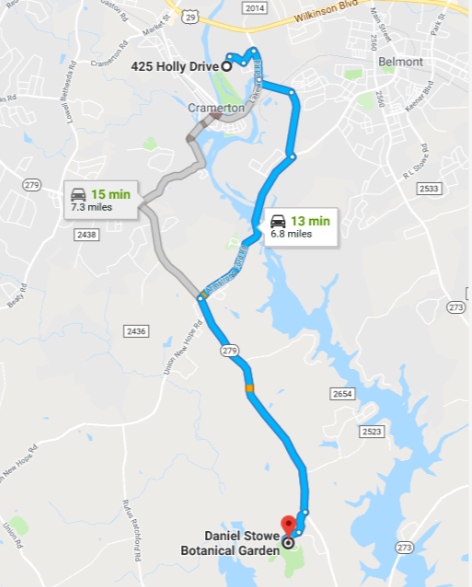
****

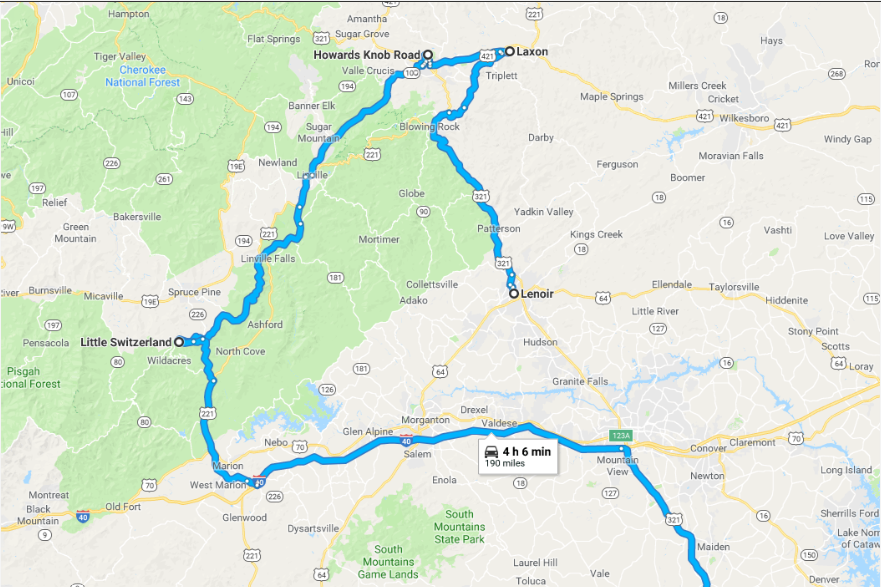
Also, at the path Data Artifacts – Web Search, searches regarding the weather of charlotte nc, boone nc, and place Martha's vineyard Massachusetts were found.

****

The images of maps were found at location Data Sources – GP\_2020.E01 – Users – IEUser – Documents – New Folder

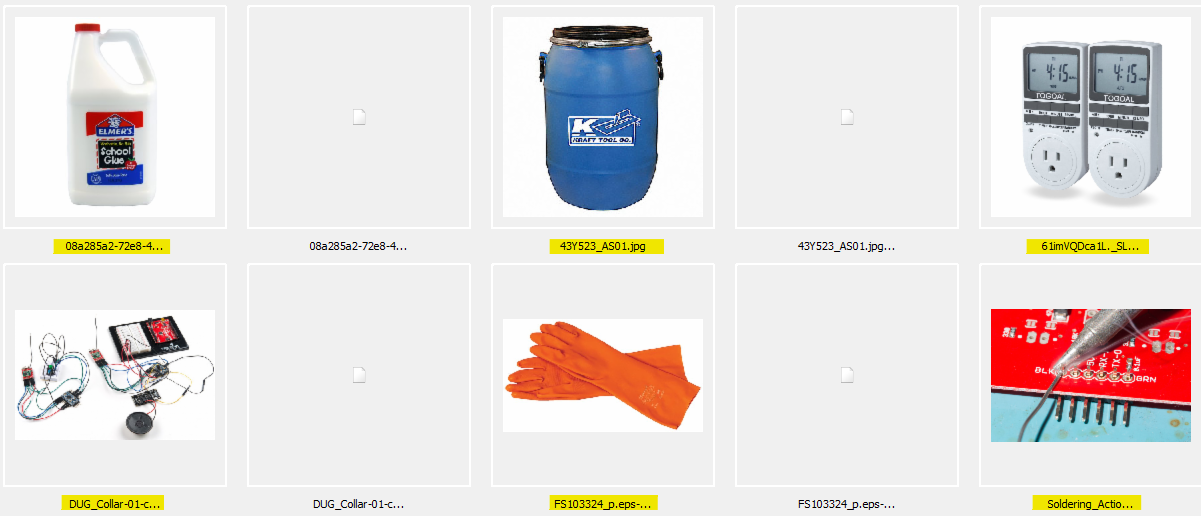
****

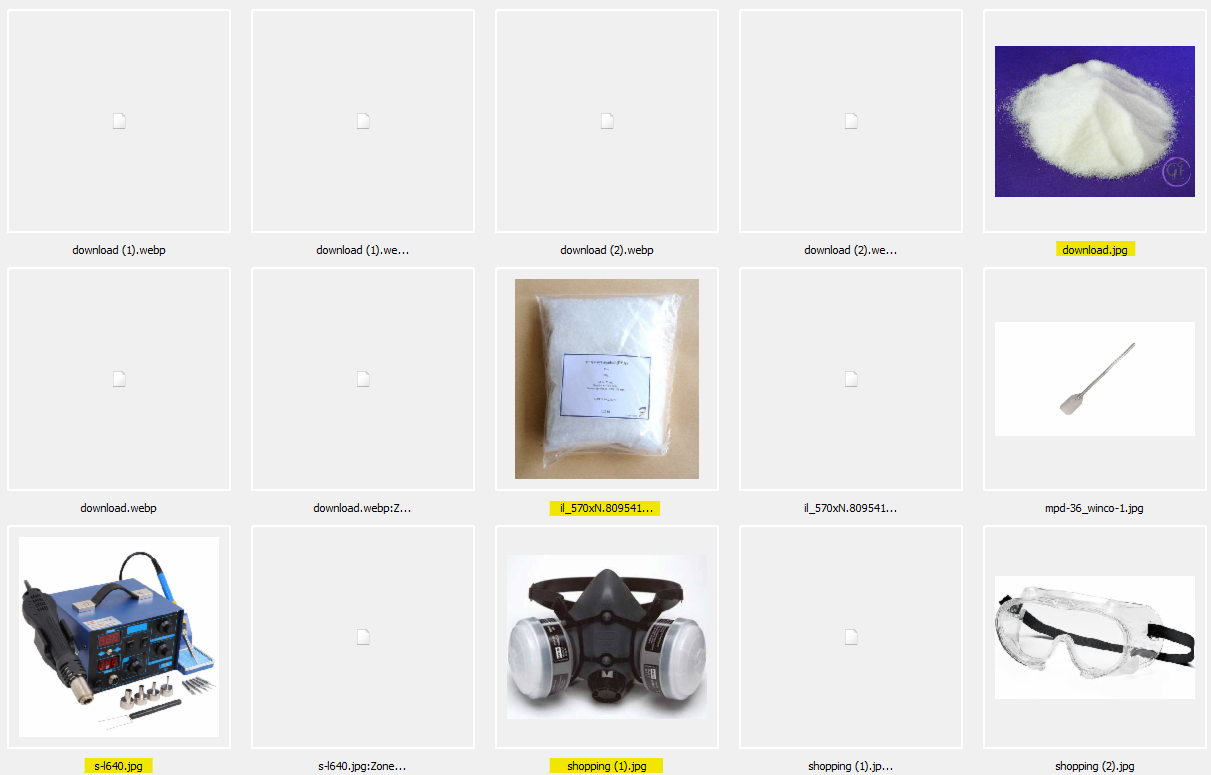
****

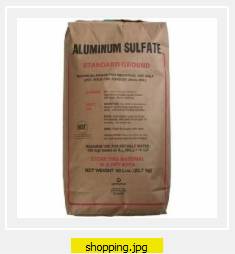
****

1. **Identify any pictures related to the crimes mentioned above.**

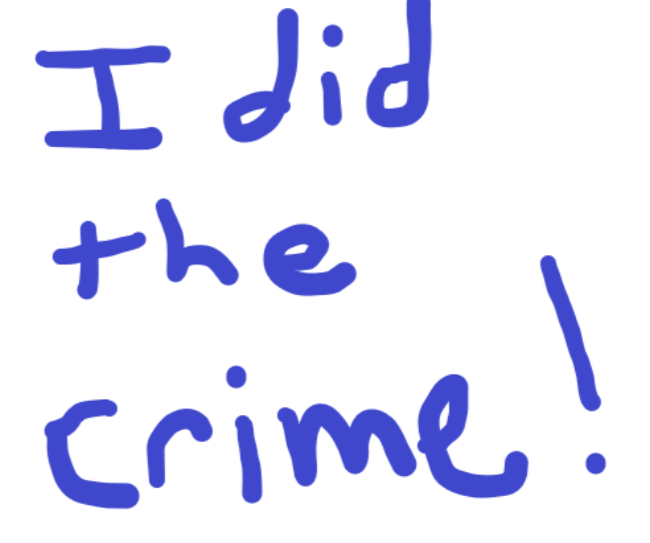
Ans: At path Data Sources – GP\_2020.E01 – Users – IEUser – Downloads, multiple images were found which could be related to the crimes mentioned above.

****

****

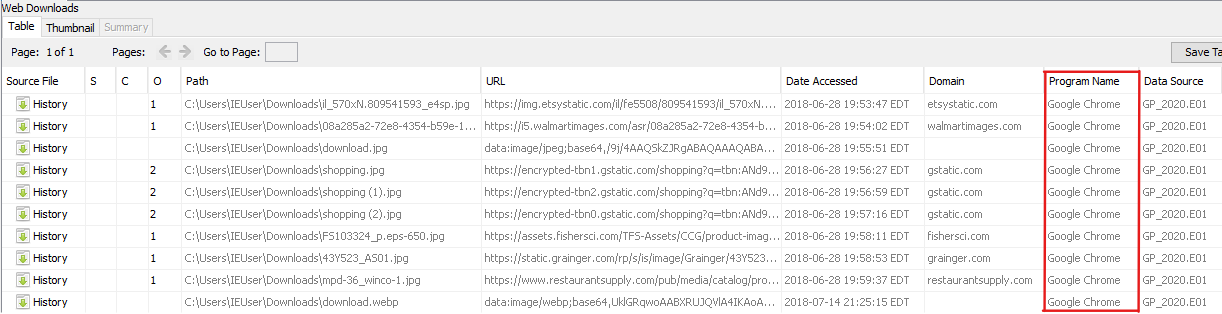
****

At path /img\_GP\_2020.E01/Users/Johnn/Music/Untitled.png, below image was found.

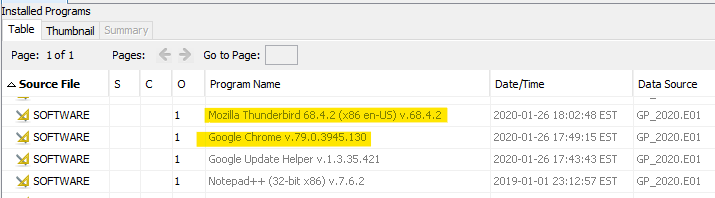
****

1. **Identify programs used to download files from the internet.**

Ans: The program used to download files from internet was Google Chrome. This was found at path Data Artifacts – Web Downloads. Under the Program Name column Google Chrome was observed to be used.

****

And in Autopsy, under Data Artifacts - Installed Programs, its seen that Google Chrome is installed which could be used to download files.

****

Also, in autopsy, the windows prefetch files at location Data Sources -> GP\_2020.E01-> Windows -> Prefetch shows that OneDrive application was accessed which could also be used to download files.

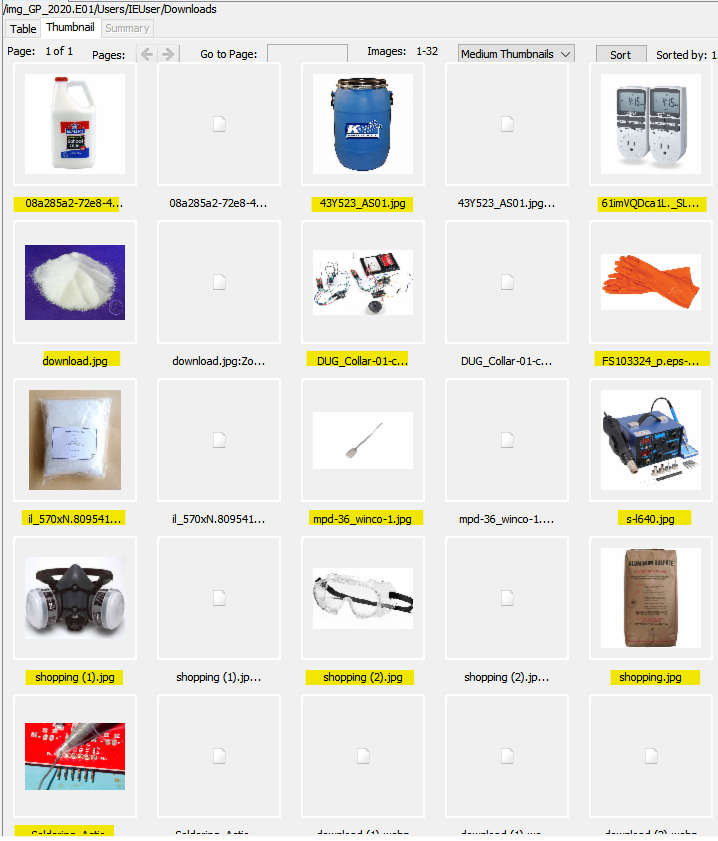
****

1. **Provide a list of files downloaded to the computer from the Internet that are relevant.**

Ans: Below is the list of relevant files downloaded from the internet. These files were found at location Data Artifacts -> Web Downloads. They were saved as a CSV and extracted from Autopsy to analyze the data.

|  |  |
| --- | --- |
| Path | Date Accessed |
| C:\Users\IEUser\Downloads\il\_570xN.809541593\_e4sp.jpg | 2018-06-28 19:53:47 EDT |
| C:\Users\IEUser\Downloads\08a285a2-72e8-4354-b59e-1d4160c247dc\_1.5a3a09108a59b2a3995738cf104c2687.jpeg | 2018-06-28 19:54:02 EDT |
| C:\Users\IEUser\Downloads\download.jpg | 2018-06-28 19:55:51 EDT |
| C:\Users\IEUser\Downloads\shopping.jpg | 2018-06-28 19:56:27 EDT |
| C:\Users\IEUser\Downloads\FS103324\_p.eps-650.jpg | 2018-06-28 19:58:11 EDT |
| C:\Users\IEUser\Downloads\43Y523\_AS01.jpg | 2018-06-28 19:58:53 EDT |
| C:\Users\IEUser\Downloads\mpd-36\_winco-1.jpg | 2018-06-28 19:59:37 EDT |
| C:\Users\IEUser\Downloads\download.webp | 2018-07-14 21:25:15 EDT |
| C:\Users\IEUser\Downloads\Soldering\_Action-01.jpg | 2018-07-14 21:25:42 EDT |
| C:\Users\IEUser\Downloads\s-l640.jpg | 2018-07-14 21:26:18 EDT |
| C:\Users\IEUser\Downloads\DUG\_Collar-01-crop.jpg | 2018-07-14 21:27:29 EDT |
| C:\Users\IEUser\Downloads\Dr.meter Triple Linear DC Power Supply 30V 5A, Input voltage 104-127V, Alligator to Banana and AC Power Cable Included\_ Power Distribution Units\_ Amazon.com\_ Industrial & Scientific.html | 2018-07-14 21:29:16 EDT |
| C:\Users\IEUser\Desktop\Farming\RingtoneForFireflye.jpg | 2018-07-22 12:17:46 EDT |
| C:\Users\IEUser\Downloads\tf10000089.xlsx | 2018-09-02 11:55:23 EDT |
| C:\Users\IEUser\Downloads\61imVQDca1L.\_SL1200\_.jpg | 2018-09-02 12:23:00 EDT |
| C:\Users\IEUser\Downloads\Mantooth32.E01 | 2019-01-01 15:19:17 EST |
| C:\Users\IEUser\Downloads\Mantooth32.E01 | 2019-01-01 15:19:17 EST |
| C:\Users\IEUser\Downloads\mimikatz\_trunk.zip | 2019-01-01 16:01:00 EST |
| C:\Users\IEUser\Downloads\mimikatz\_trunk.zip | 2019-01-01 16:01:00 EST |
| C:\Users\IEUser\Downloads\openssl-0.9.8h-1-setup.exe | 2019-01-01 16:21:54 EST |
| C:\Users\IEUser\Downloads\openssl-0.9.8h-1-setup.exe | 2019-01-01 16:21:54 EST |
| C:\Users\IEUser\Downloads\npp.7.6.2.Installer.exe | 2019-01-01 18:11:01 EST |
| C:\Users\IEUser\Downloads\HxDSetup.zip | 2019-01-01 18:18:59 EST |
| C:\Users\IEUser\Downloads\Thunderbird Setup 68.4.2.exe | 2020-01-26 13:01:50 EST |

Also, in Autopsy, more interesting image files were found at location Data Sources – GP2020.E01\_1Host –> Users –> IEUser –> Downloads which could be used for malicious purposes.



1. **Identify any software that could be used to encrypt, obscure or forensically analyze data, modify Hex data or defeat forensics and when that software was used.**

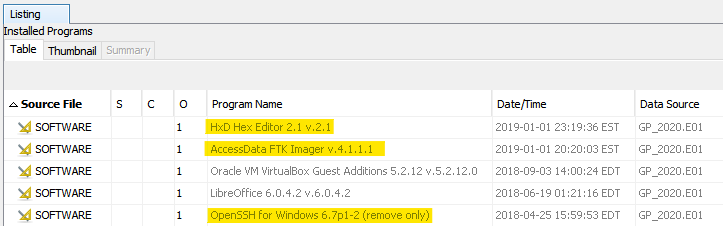
Ans: Below is the list of identified installed software in the image that could be used to encrypt, obscure, or forensically analyze data, modify Hex data or defeat forensics:

Software to encrypt data: OpenSSH for Windows 6.7p1-2, GnuWin32: OpenSSL0.9.8h-1 v.0.9.8h-1

Software to modify Hex data: HXD Hex Editor

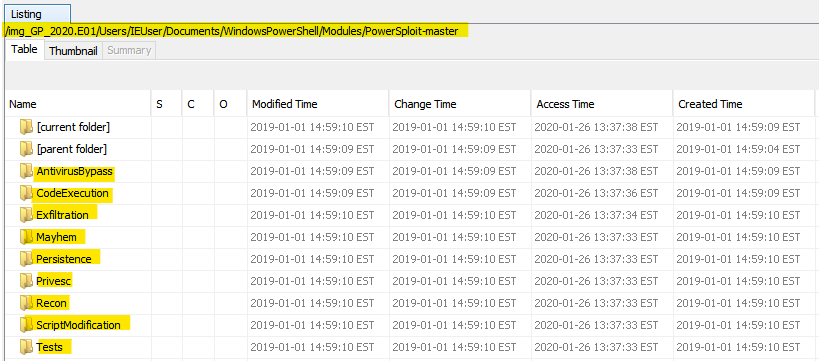
Software to forensically analyze data: AccessData FTK Imager

The above list of softwares were found using Autopsy, under Data Artifacts –> Installed Programs.



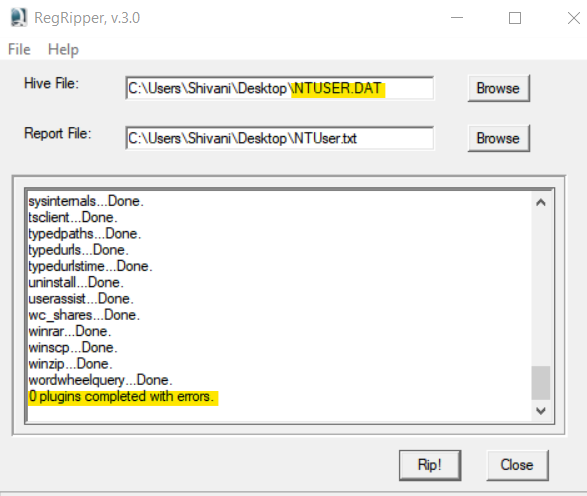


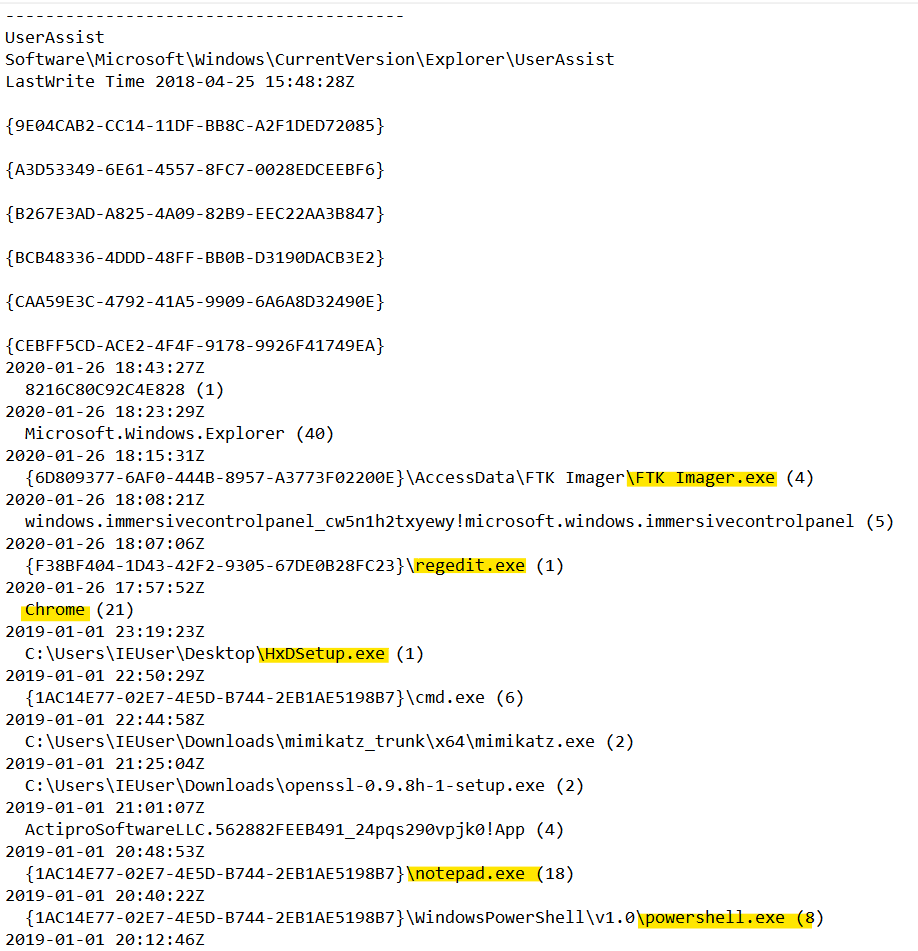
Also, in Autopsy, multiple software folders were observed named Antivirusbypass, CodeExecution, Exfiltration, Mayhem, Persistence, Privesc, Recon, ScriptModification, Tests under path Data Sources –> GP\_2020.E01\_1Host –> Users –> IEUser –> Documents - WindowsPowerShell –> Modules –> PowerSploit- master, which could be used to encrypt, obscure, or forensically analyze data, modify Hex data or defeat forensics.



1. **Identify software used most recently, (this may span a long time period).**

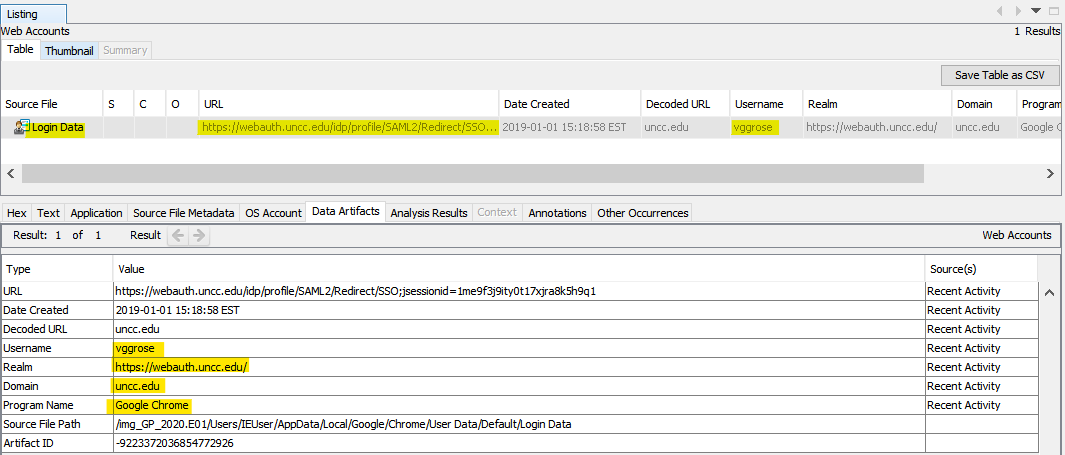
Ans: Some of the most recently used software were FTK Imager, Regedit, Chrome, HxD Setup, notepad, powershell. This was found using Autopsy, in NTUSER.dat file at location Data Sources -> GP\_2020.E01\_1Host –> Users –> IEUser. The NTUSER.dat file was extracted and ripped using regripper tool to observe its contents. Below is the screenshot of details-

****

****

1. **Search for any personal information that may have been stolen or used by the user of this computer.**

Ans: In Autopsy, at location Data Artifacts –> Web Accounts, a file is observed, Source file – Login Data, with username vggrose as seen in the below image. This may have been stolen.

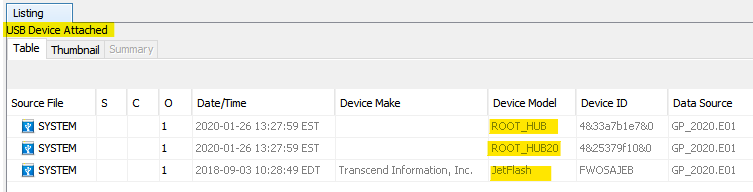
****

1. **Determine whether investigators or crime scene specialists may have missed any devices that were connected to the computer.**

Ans: In Autopsy, 3 devices as following were seen to be attached to the system and were found at location Data Artifacts -> USB Device Attached.

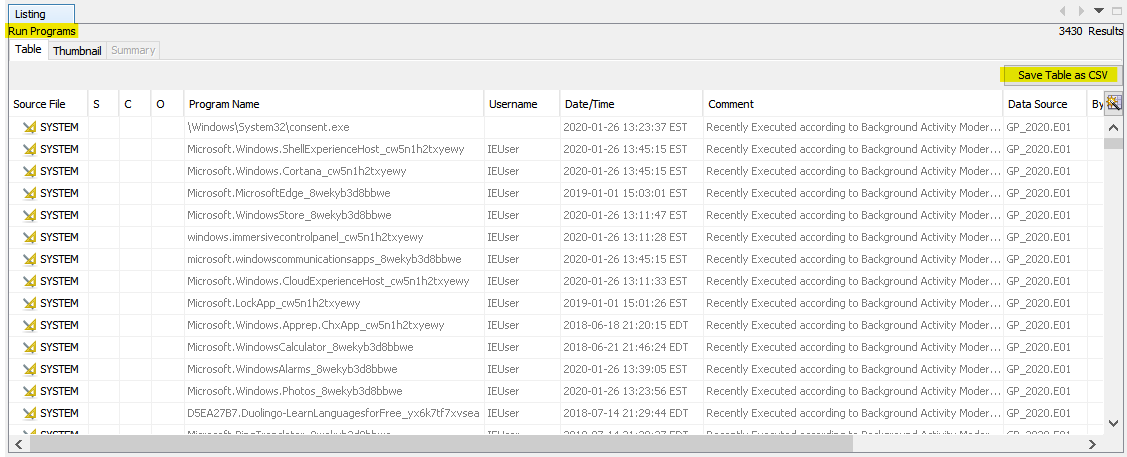
* ROOT\_HUB,
* ROOT\_HUB20 and
* JetFlash.

Of the above ROOT\_HUB, ROOT\_HUB20 are hubs, and JetFlash is a USB drive. As no image files of any of the above devices were provided by the investigators, they are believed to have been missed.

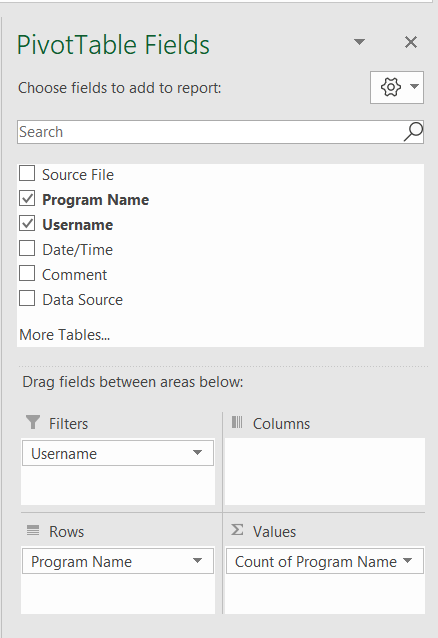
****

1. **Identify the 3 most often run programs.**

Ans: To identify the 3 most often run programs, using Autopsy the table was exported as a CSV from location Data Artifacts -> Run Programs.

****

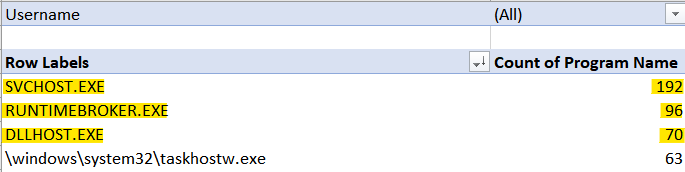
A pivot table was created as below to get the count of the programs.

****

On sorting the pivot table in descending order, it was observed that SVCHOST.EXE,

RUNTIMEBROKER.EXE and DLLHOST.EXE were the most run programs with count

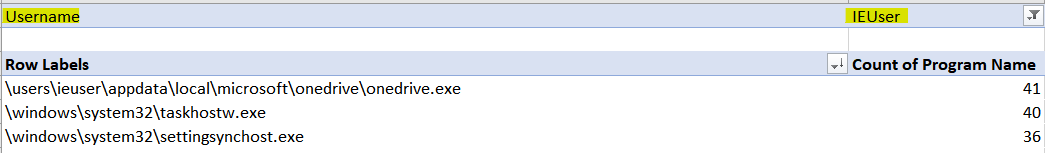
192, 96 and 70 respectively.

****

On filtering the username with ‘IEUSser’, the top 3 run programs observed were:

Onedrive.exe, taskhostw.exe and settingsynchost.exe with run count 41, 40 and 36

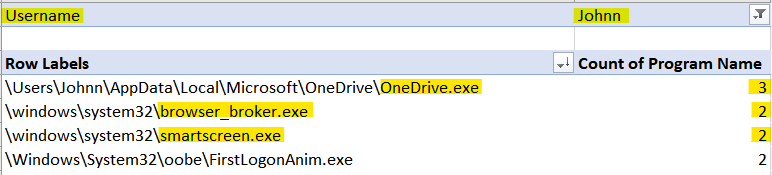
respectively.



Similarly, on filtering the username with ‘Johnn’, the top 3 run programs observed were:

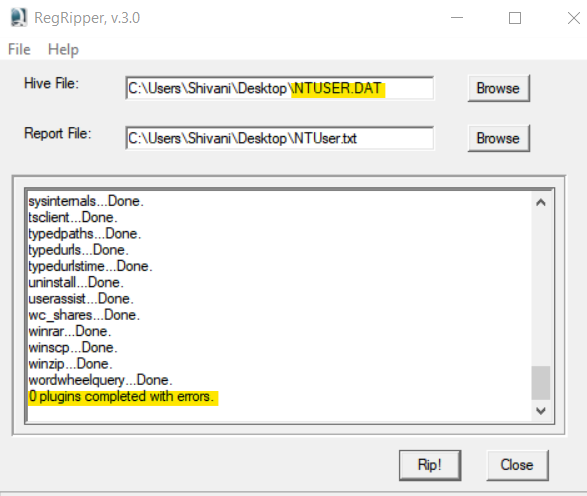
OneDrive.exe, browser\_broker.exe and smartscreen.exe and they ran 3, 2 and 2 times

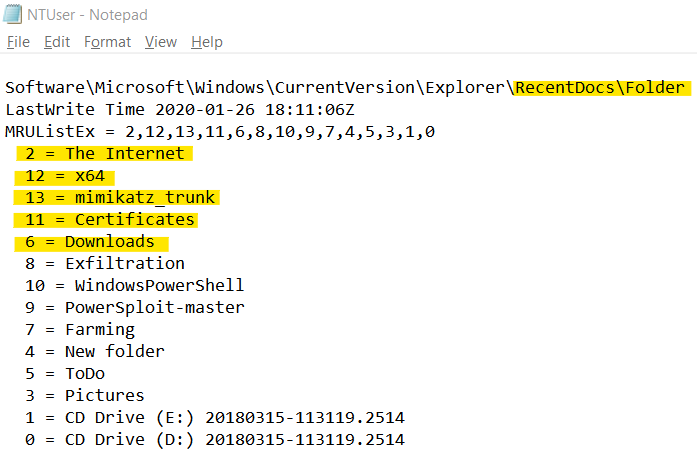
respectively.



1. **Identify the last 5 folders the subject opened or worked in.**

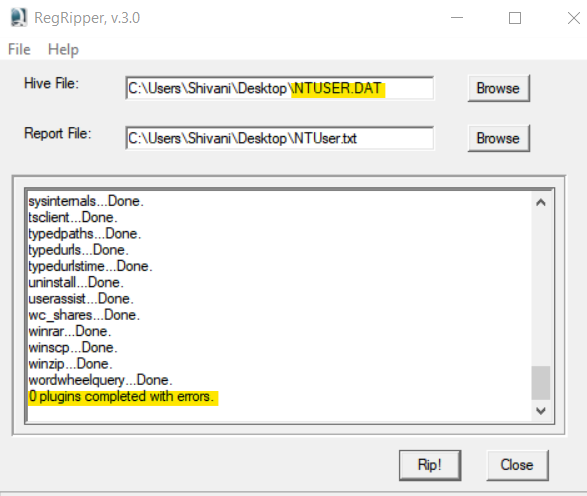
Ans:The last 5 folders opened were The Internet, X64, mimikatz\_trunk, Certificates, Downloads. This was found using Autopsy, in NTUSER.dat file at location Data Sources -> GP\_2020.E01\_1Host –> Users –> IEUser. The NTUSER.dat file was extracted and ripped using regripper tool to observe its contents. Below is the screenshot of details-

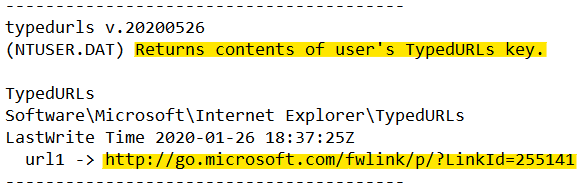
****



1. **Identify any URLs that were visited by manually typing the address.**

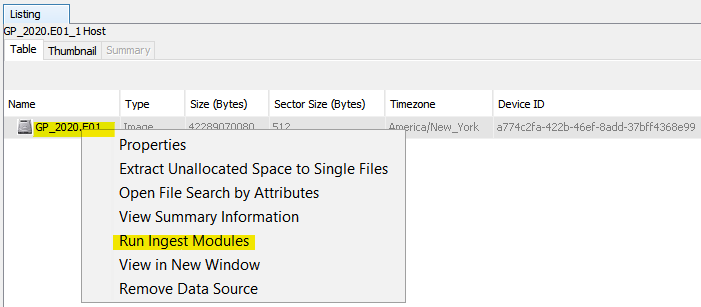
Ans: Manually typed URL address identified was <http://go.microsoft.com/fwlink/p/?LinkId=255141> .This was found using Autopsy, in NTUSER.dat file at location Data Sources -> GP\_2020.E01\_1Host –> Users –> IEUser. The NTUSER.dat file was extracted and ripped using regripper tool to observe its contents. Below is the screenshot of details-

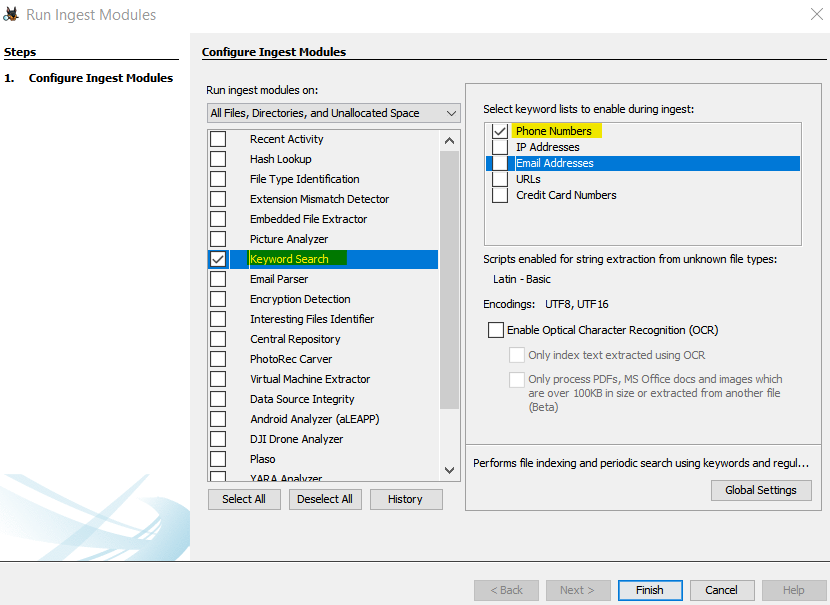
****

****

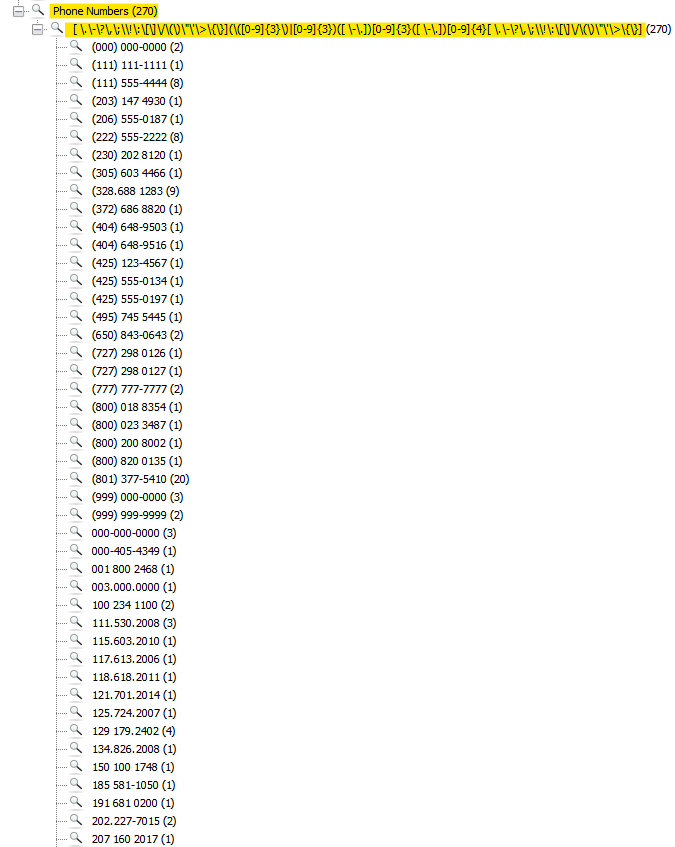
1. **Identify any phone numbers on the drive. (This will require search with a regular expression)**

Ans: In Autopsy, by right clicking on the GP\_2020.E01 data source, ‘Run Ingest Modules’ option was selected. Then, only Keyword Search ingest was run with Phone Numbers as the keyword list as seen in below screenshot.

****

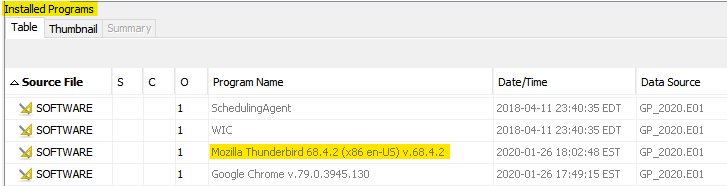
****

Under Analysis Results -> Keywords Hits -> Phone Numbers, a list of phone numbers on the drive were found.

****

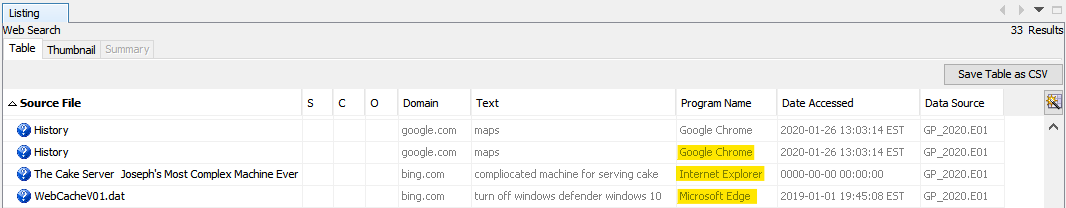
1. **Identify any email programs installed or used on the computer.**

Ans: The email program installed on the computer is **Mozilla Thunderbird**. This was found at location Data Artifacts -> Installed Programs.



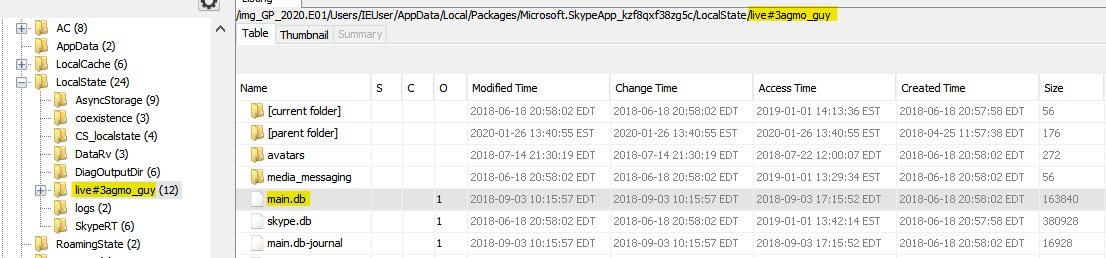
1. **Identify internet browsers on the computer that were used to connect to web pages.**

Ans: The internet browsers on the computer are Google Chrome, Internet Explorer, Microsoft Edge. This was found at location Data Artifacts -> Web Search.



1. **Identify any Skype chats the user may have had.**

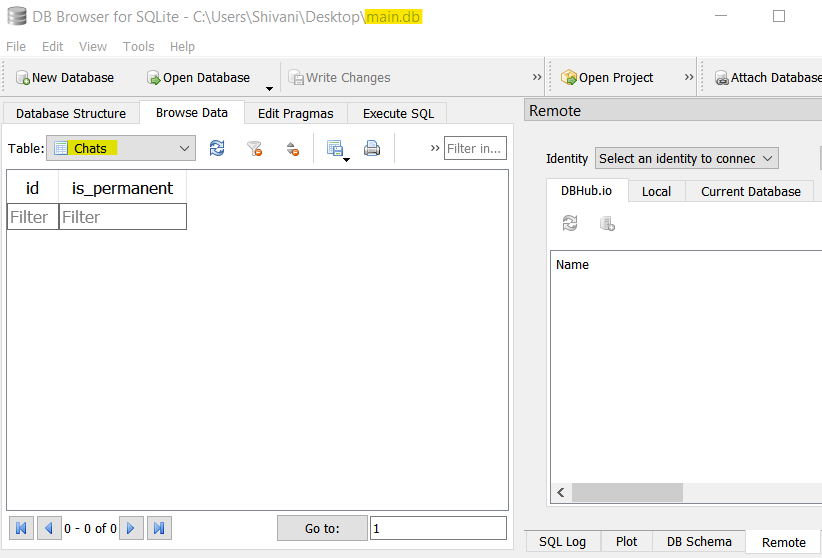
Ans: The main.db file was extracted from the location Data sources –>Users -> IEUser –> AppData –> Local –> Packages -> Microsoft.SkypeApp\_kzf8qxf38zg5c –> LocalState -> live#3agmo\_guy.

****

The main.db file was then loaded into DB Browser for SQLite. To find the chats, Under

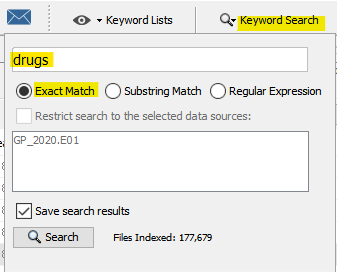
Browse Data Tab, chats table was selected. As observed, no chats were found and were

present.

****

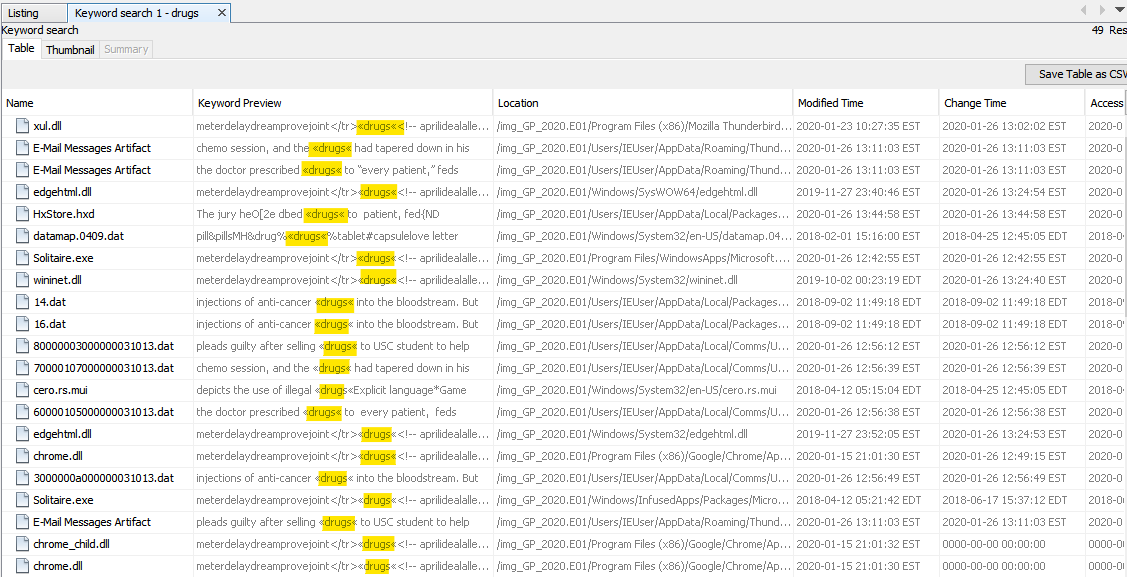
1. **Detective Fletcher has provided a list of search terms: Monarch, drugs, mountain, powder, chemical. Provide ONLY (a few examples of) results of these that you believe may be relevant.**

Ans: In Autopsy, using the Keyword Search bar and Exact Match option,

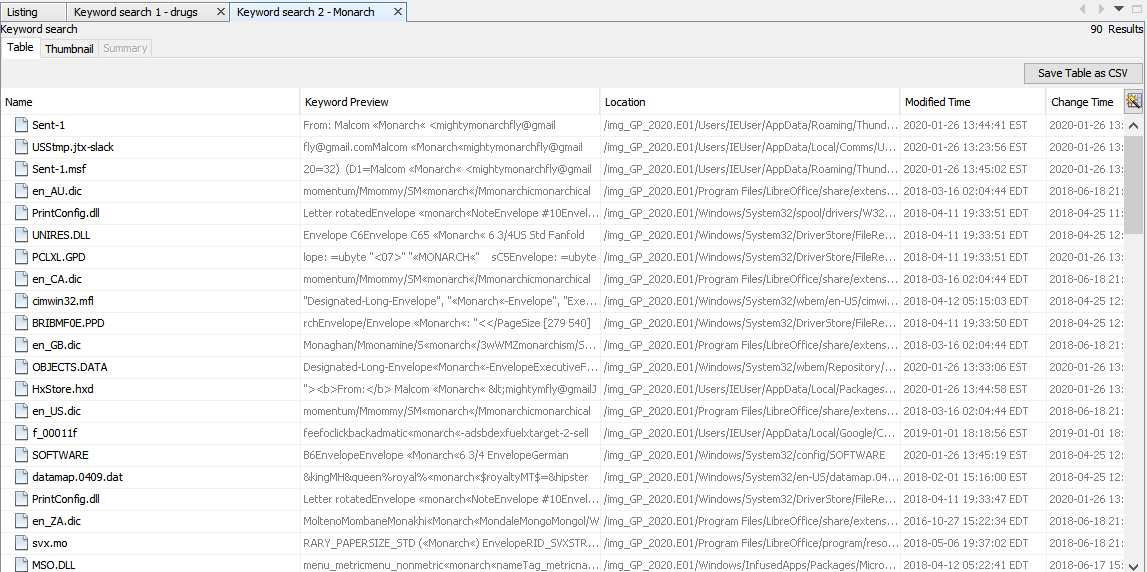
****

Similarly, keyword searches for all the above-mentioned keywords were done. Below are the screenshots of the results.

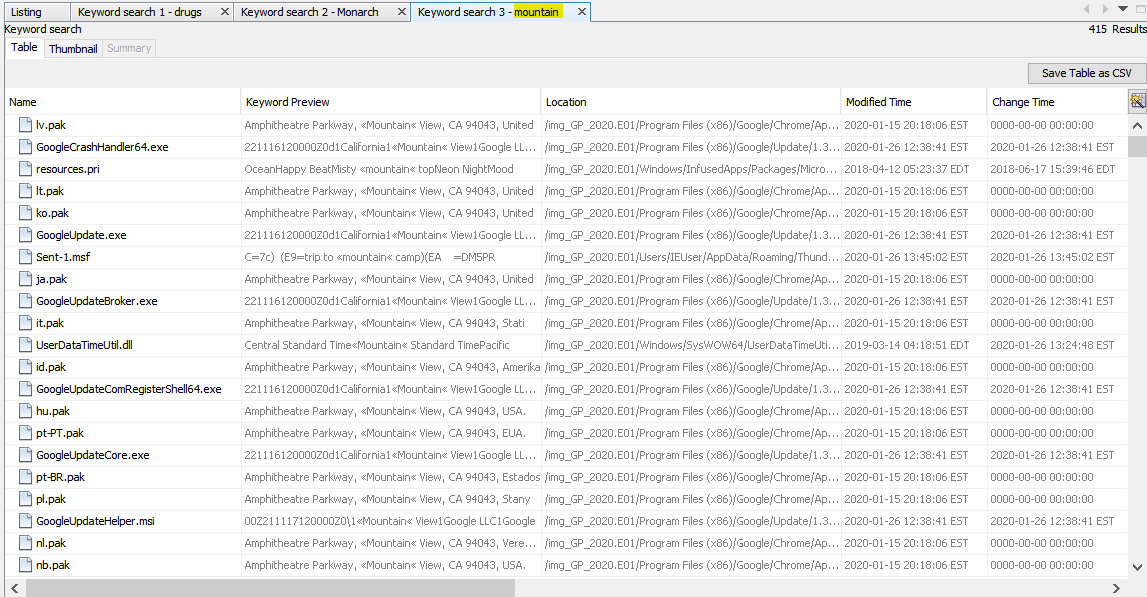
Keyword- drugs

****

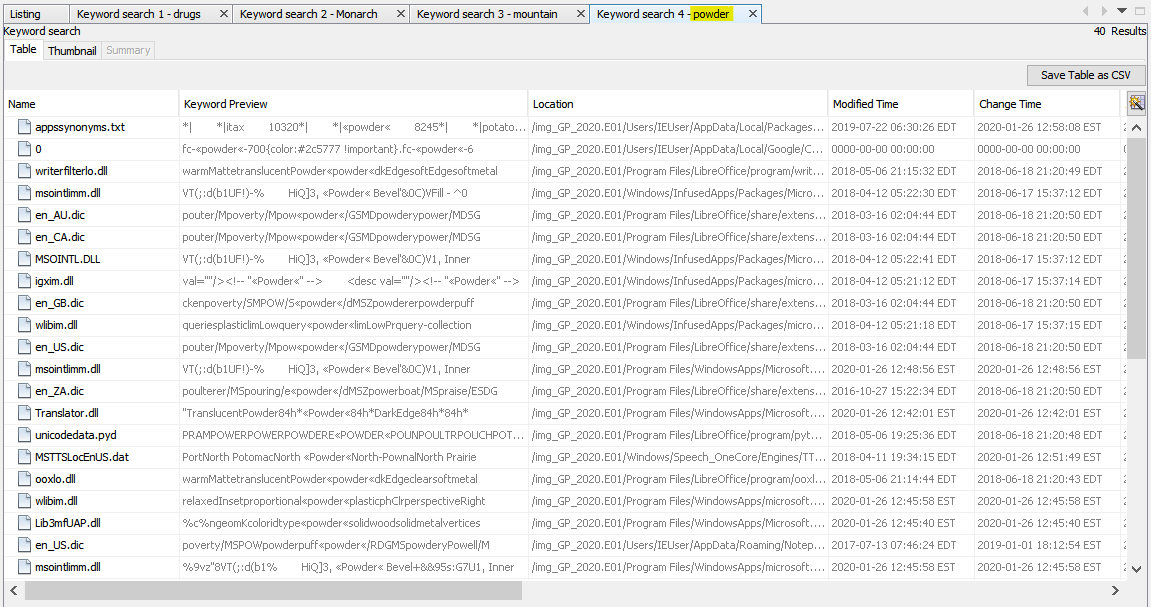
Keyword- Monarch



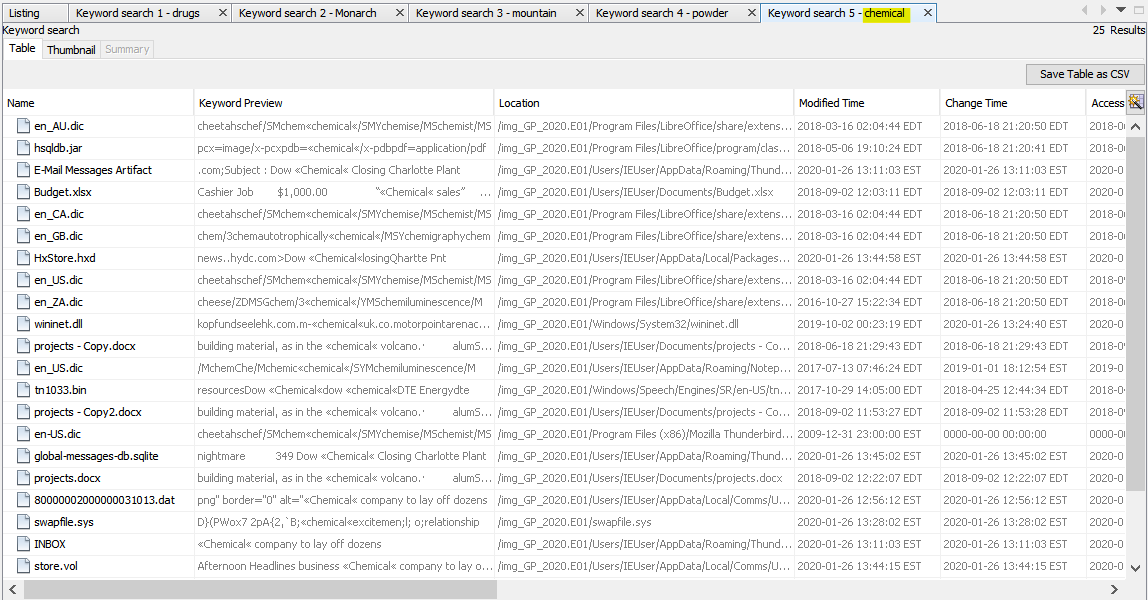
Keyword- mountain



Keyword- powder



Keyword- chemical



**Conclusion**

Overall, in this lab I was asked to process a desktop computer belonging to Gene Poole who is believed to be involved in the manufacture and sale of drugs. To begin the analysis, the image was loaded using AccessData FTK Imager 4.5.0.3 on a Windows 10 Machine and the hash value of image was verified to conclude that it was not tampered before the analysis process. With the help of Autopsy, the provided images were examined and all the questions regarding this case were successfully answered. The computer's owner, timezone information, device information, most used programs, recently used programs, all email programs installed or used, and other information about the user and the system was discovered. The image was again verified using AccessData FTK Imager to ensure it was not altered. No evidence has been retained. The forensic image files, and answered questions regarding it, were returned to the UNCC Forensic Lab and then to UNC Charlotte Police Department Detective Jessica Fletcher.