ITIS 5250

Sahil Bhirud – 801138029

Semester Project

**Overview:**

Detective Jessica Fletcher has requested me to process a forensic image of a desktop computer for her. This desktop computer belongs to Eugene “Gene” Poole, who is a suspect in the case of manufacturing and sale of drugs. She has provided me with an image **GP\_2020.E01** and has also asked me to be aware of anti-forensics as Gene and his associates showed varying degrees of technical ability.

**Forensic Acquisition and Exam Preparation:**

I downloaded the image file from Canvas and uploaded it to **FTK Imager** and **Autopsy**. I calculated and verified the hash values for the forensic image. The tools I have used in performing the analysis of the image are **FTK Imager, Autopsy, RegRipper and BEViewer**.

A screenshot of a cell phone

Description automatically generated

A screenshot of a social media post

Description automatically generated

**Findings and Report (Forensic Analysis):**

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

Total Size of the hard drive: 42,289,070,080 Bytes

A screenshot of a cell phone

Description automatically generated

Number of Partitions: 0

Used Space: 25,166,831,620 Bytes

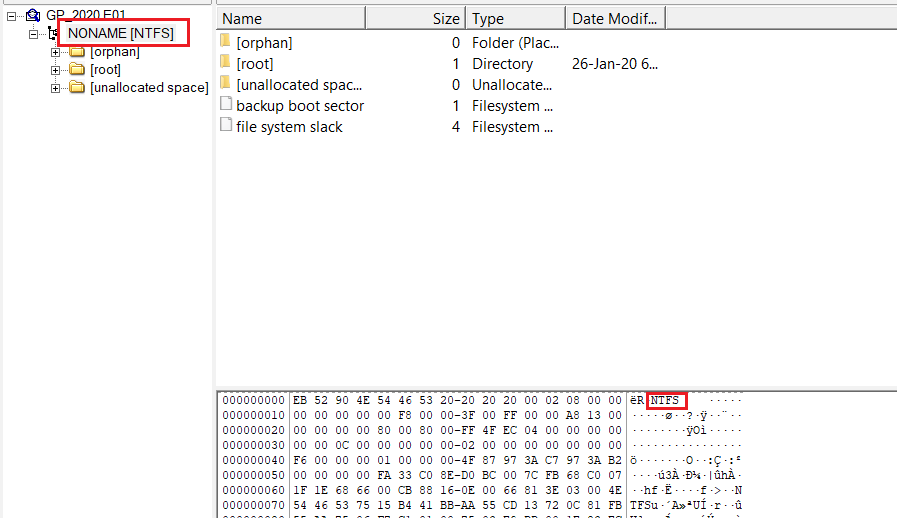
Free Space: 17,122,234,370 Bytes

A screenshot of a cell phone

Description automatically generated

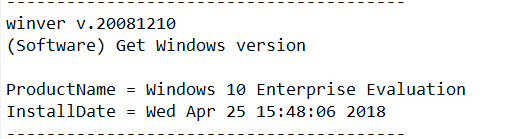
1. **Identify the type of file systems in use.**

NTFS is the file system which is being used.



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

The operating system installed is Windows 10 Enterprise Evaluation with Service Pack 6.3 as observed in the SOFTWARE Registry File.

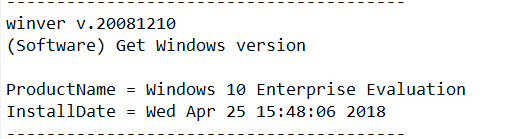


A screenshot of a cell phone

Description automatically generated

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

OS was installed on **25th April 2018 at 15:48:06**.



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

The Time Zone information for the computer is located in the SYSTEM registry file (shown below). The time zone of the computer is Western Australia Standard Time.

A screenshot of a cell phone

Description automatically generated

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

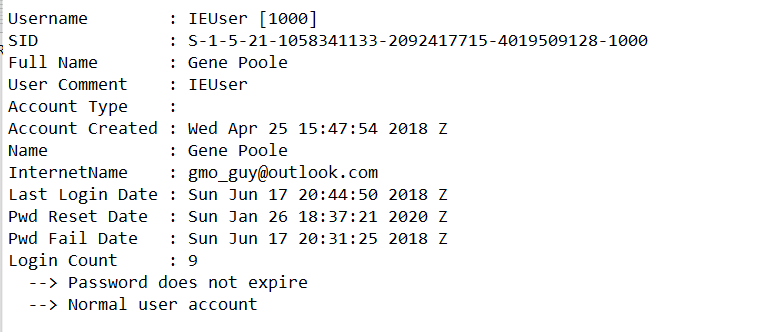
Eugene Poole is the owner of the computer as seen in the SOFTWARE Registry file report.

A screenshot of text

Description automatically generated

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

From the SAM Registry file, I found two accounts which were used to login. The first is a standard IEUser account associated with the name Gene Poole and required a password to log into the system.



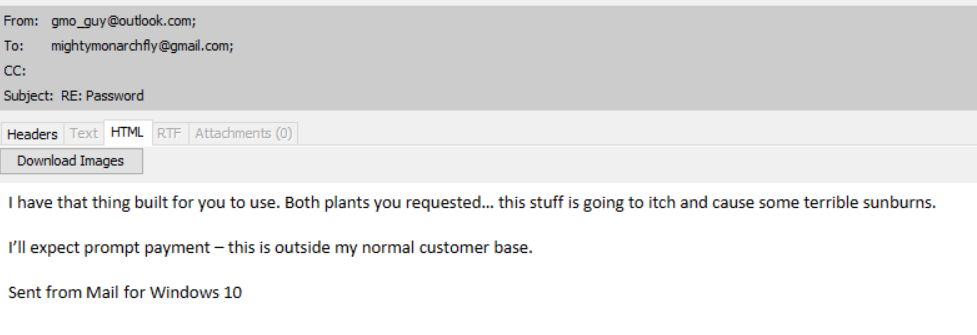
Second is a ssh server account which is a method of using an SSH Server for logging in and it also requires password to do so.

A picture containing bird

Description automatically generated

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

I was able to identify Gene’s associates through his email conversations with them. They are Malcolm Monarch ([mightymonarchfly@gmail.com](mailto:mightymonarchfly@gmail.com)),

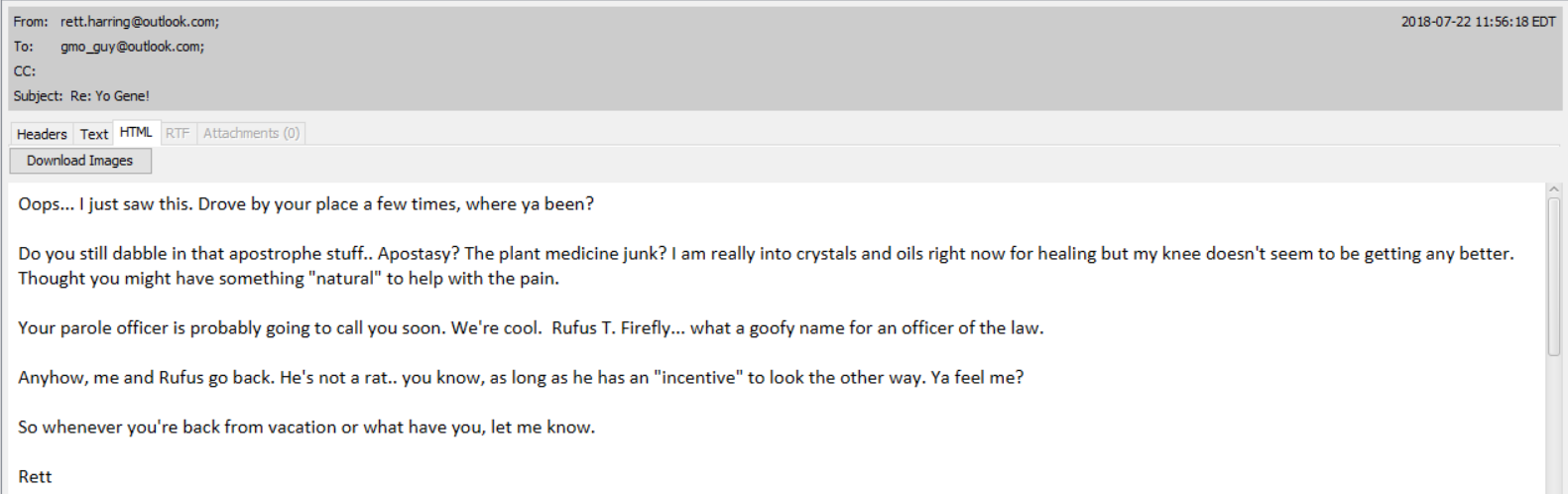


Rett Harring ([rett.harring@outlook.com](mailto:rett.harring@outlook.com)), the person having email address [macguff16@hotmail.com](mailto:macguff16@hotmail.com)

A screenshot of a social media post

Description automatically generated

and Gene’s parole officer Rufus T. Firefly.



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

An email sent from Gene to Rett shows Gene boasting about the quality of the drug he has in his possession.

A screenshot of a social media post

Description automatically generated

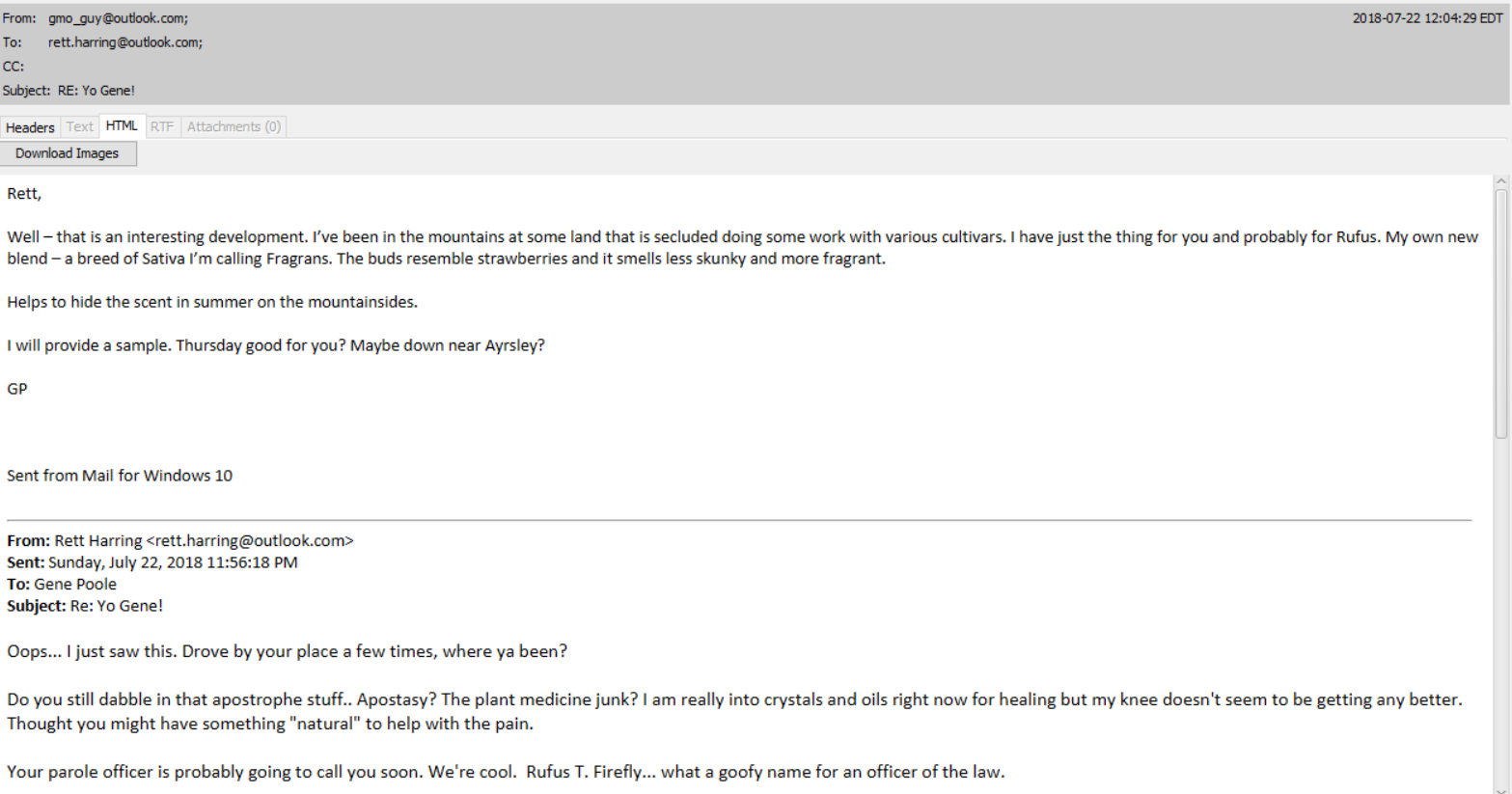


There is also a proof of communication between them about the negotiation of price for the drugs.

A screenshot of a social media post

Description automatically generated

Gene also talks about the new kind of marijuana he grows in the mountains.



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

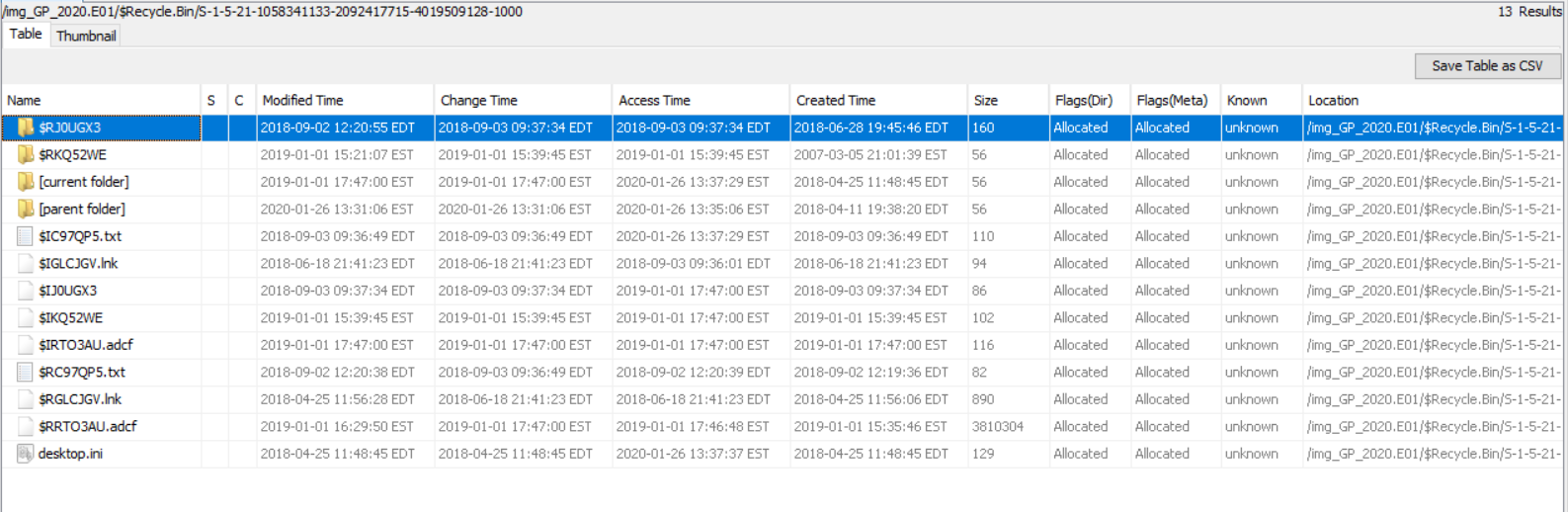
The last login date and time of the user is **26th January 2020 at 18:28:05 Z** as identified in the SAM Registry file.

A screenshot of a cell phone

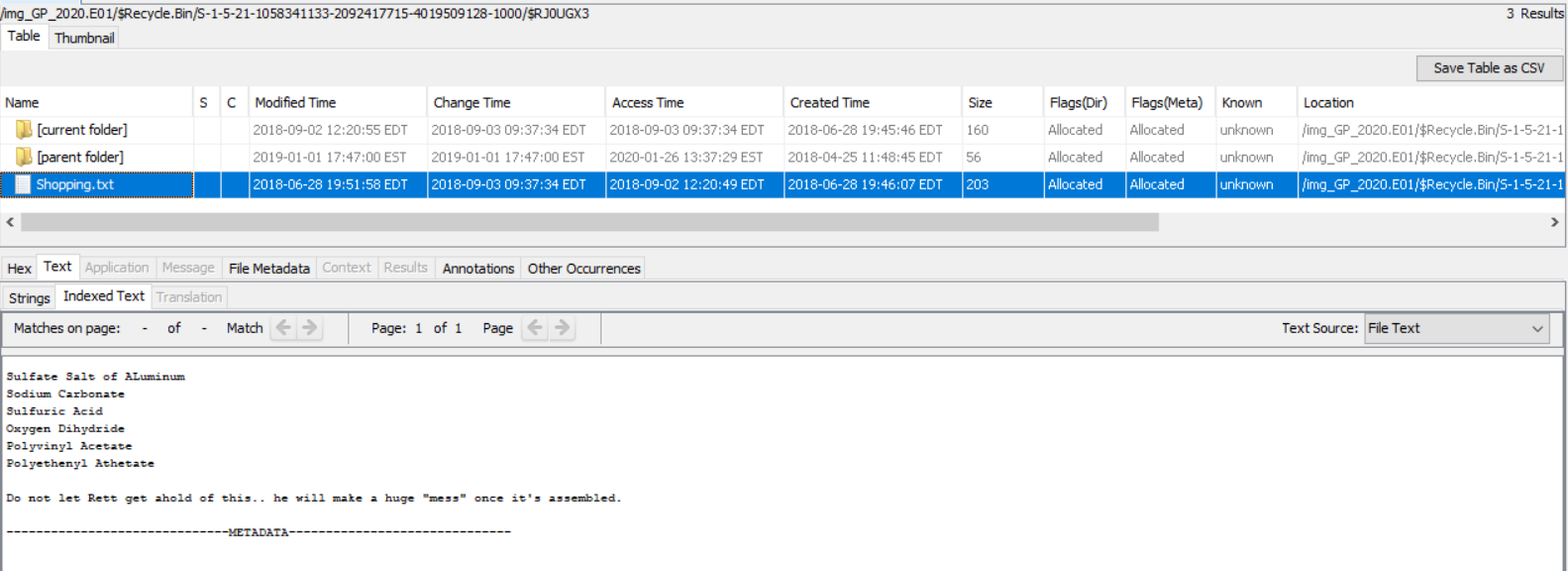
Description automatically generated

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

Files present in the Recycle Bin of Gene Pool’s account are shown below. The change time attribute of the files is indicating when the file is deleted.



Contents of $RJOUGX3 folder:



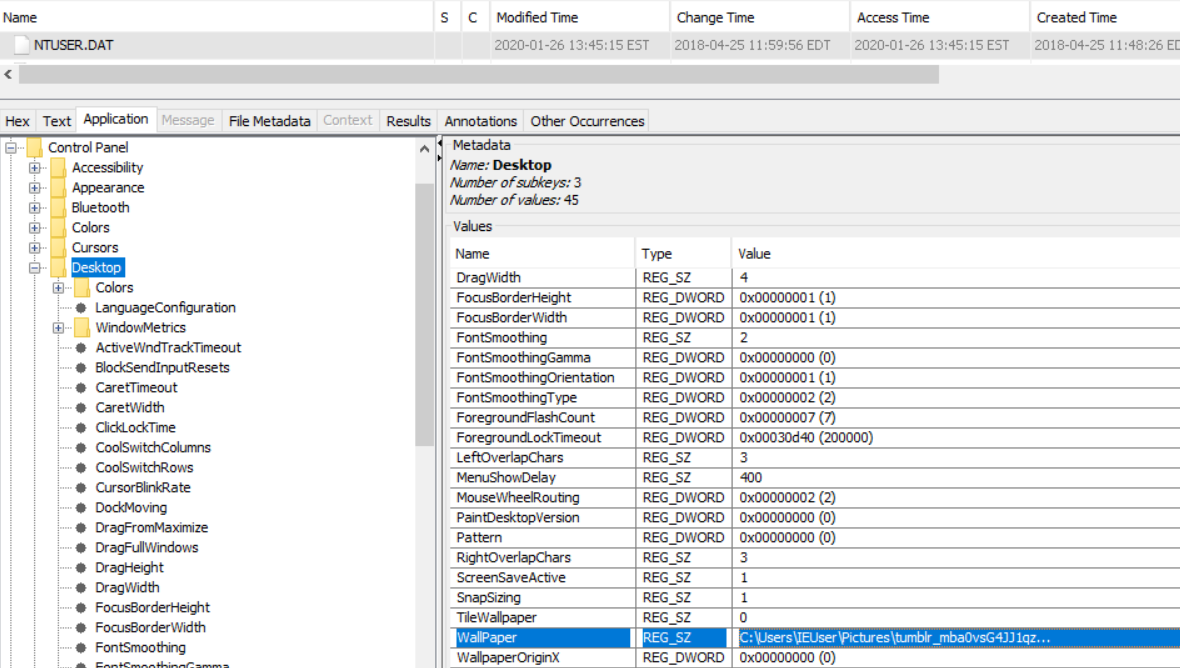
Contents of $RKQ52WE folder:

A screenshot of a social media post

Description automatically generated

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

I found the directory in which the wallpaper is located in the **NTUSER.dat** file.



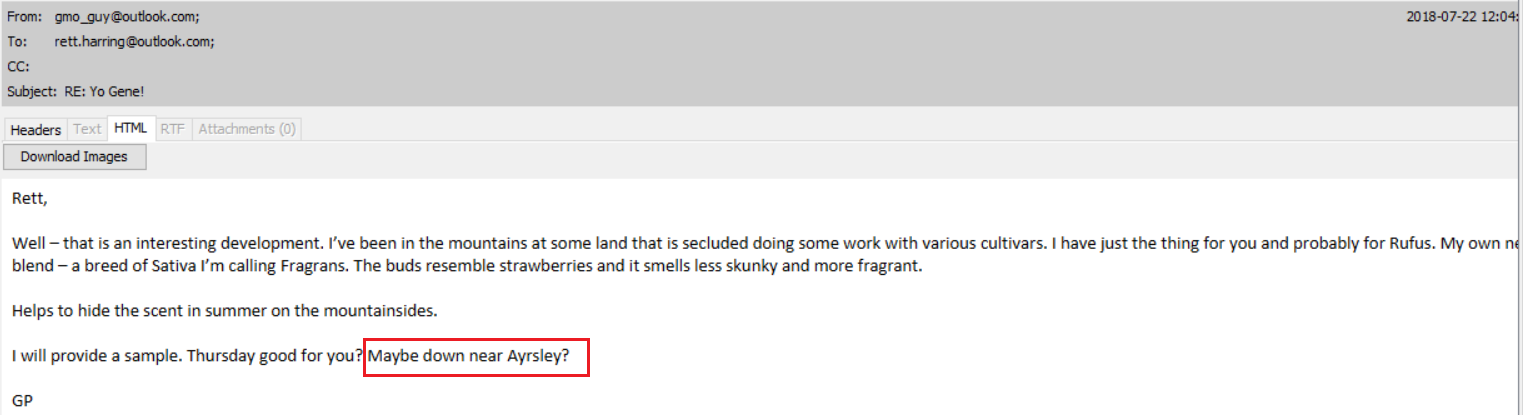
And after going to this location, I found out the wallpaper which is shown below:

A screenshot of a social media post

Description automatically generated

1. **Identify any locations other than the subject's home that may have been involved (this does not require an exact address).**

There was a mention of the town of Ayrsley in an email. Some mountains are also mentioned which seem to be located near Ayrsley.



I also found some locations in the images.

A screen shot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

One of Gene’s associates was also leaving for Canada.

A screenshot of a social media post

Description automatically generated

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

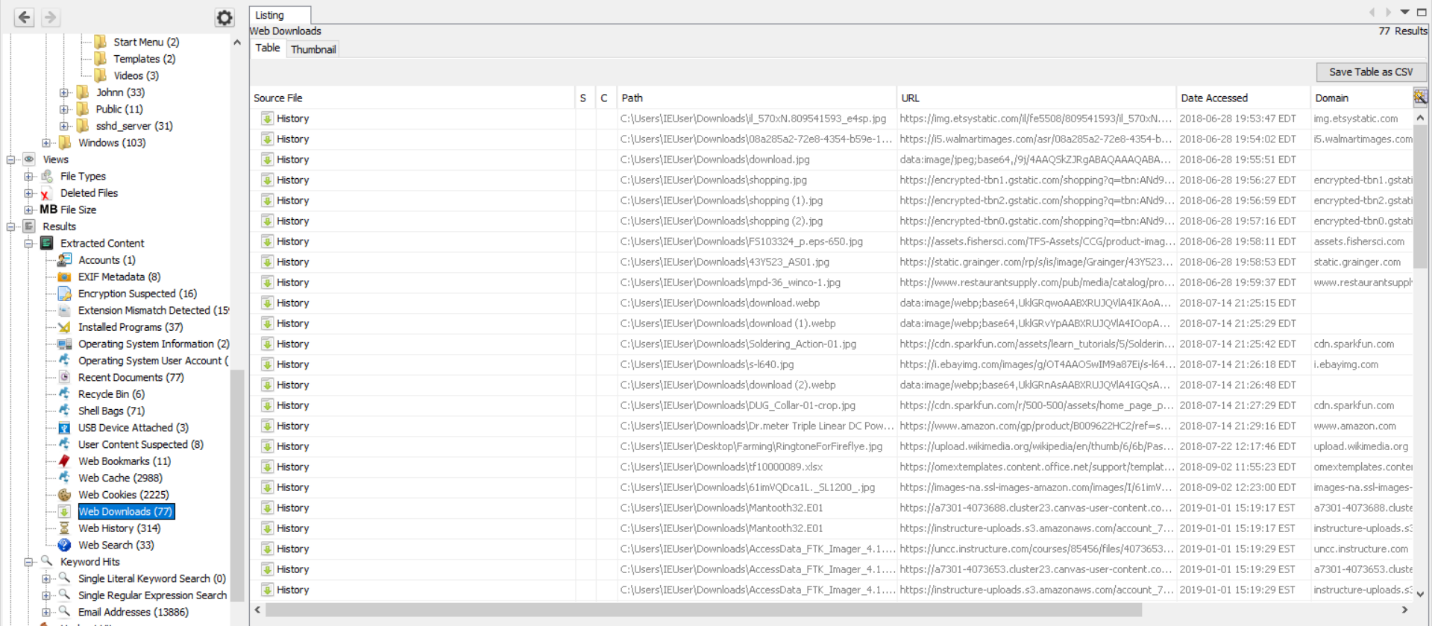
There are photos of the drug which Gene is selling. These were found in an attachment of an email which was sent by Gene to one of his associates, Rett Harring.



1. **Identify files downloaded from the internet.**

There is a total of 77 files which are downloaded from the internet. All the files were downloaded by the default user IEUser.



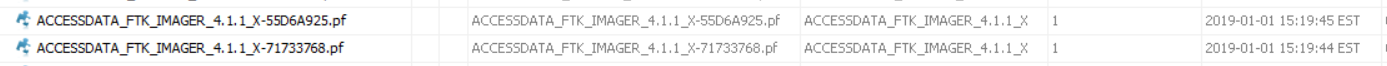
1. **Identify any software that could be used to encrypt, obscure or forensically analyze data, modify Hex data or defeat forensics and when that software was used.**

**HxD Editor** and **Access Dara FTK Imager 4.1.1** were the softwares which were in the system. I found this under “Installed Programs” in Autopsy.

A screenshot of a cell phone

Description automatically generated

FTK Imager was used on **1st January 2019 at 15:19:45 EST**



HxD Editor was used on **1st January 2019 at 18:19:39 EST**



1. **Identify software used most recently (within the last month before the image was made).**

The image was made on **26th January 2020**. The software which was used in this month is **Thunderbird**. I found it in the SOFTWARE Registry report.

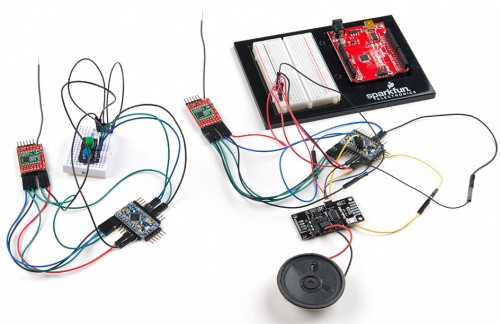


1. **Provide a list of files downloaded to the computer from the Internet that are relevant.**

The relevant downloaded files include images of ingredients which might be used for manufacturing of drugs and some images of electronics which might be of importance.







1. **Perform a file carving and describe any relevant files found.**

I used BEViewer to perform file carving and found relevant jpeg files.



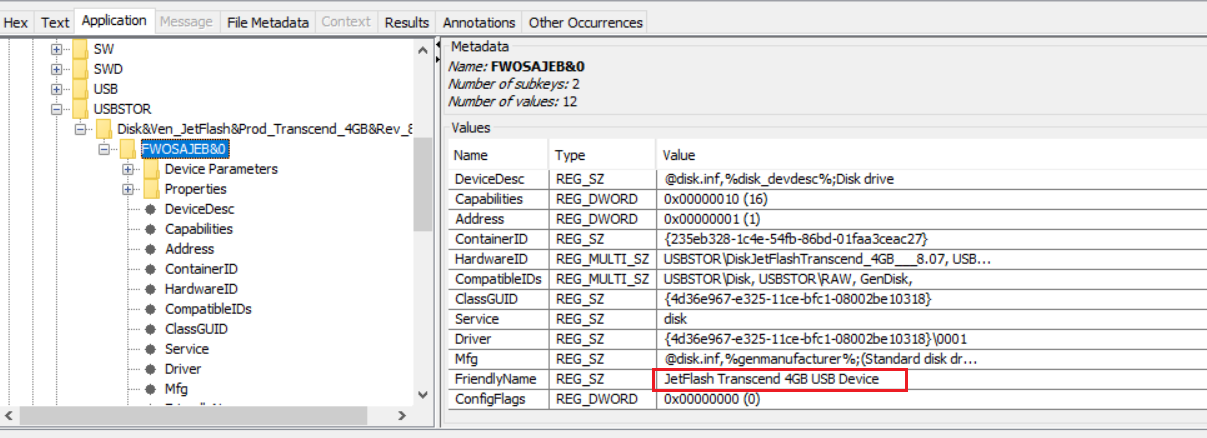






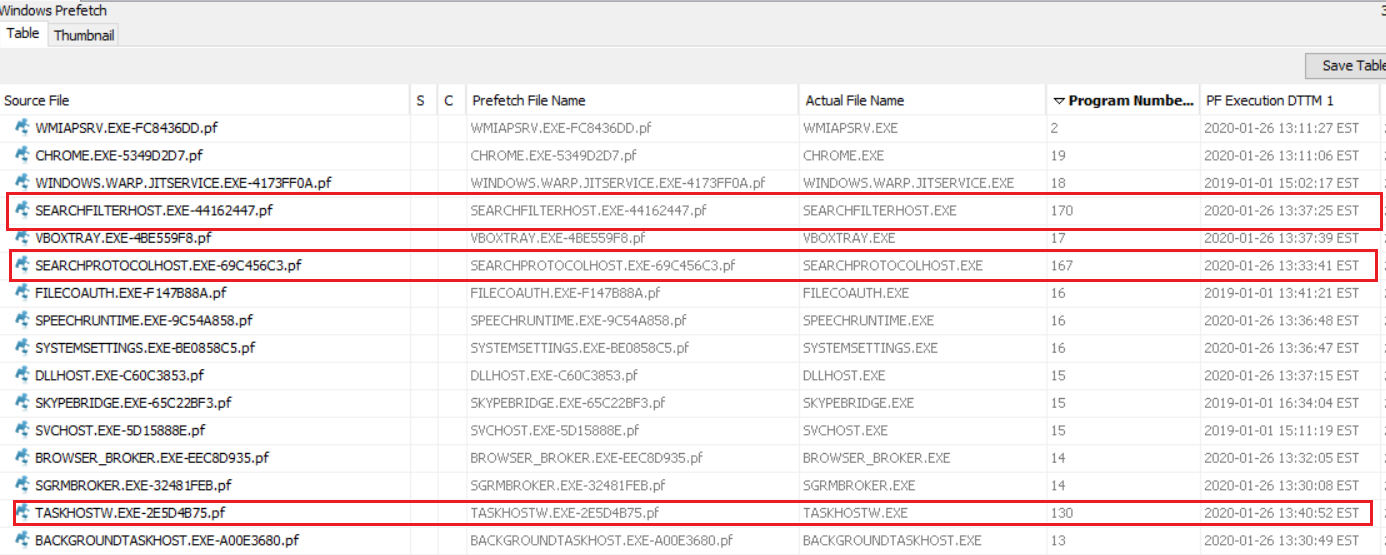
1. **Determine whether investigators or crime scene specialists may have missed any devices that were connected to the computer.**

I did find an USB Device which was connected to the computer at some point of the time. I found this in the USBSTOR folder in the SYSTEM Registry file.



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

The 3 most often run programs are shown below. I added the Windows Prefetch plugin to Autopsy and ran ingest module to get the results.



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

Recent Documents in Autopsy shows all the recent files and folders which were accessed. The latest 5 folders accessed are shown below:

User: **IEUser**

A screenshot of a cell phone

Description automatically generated

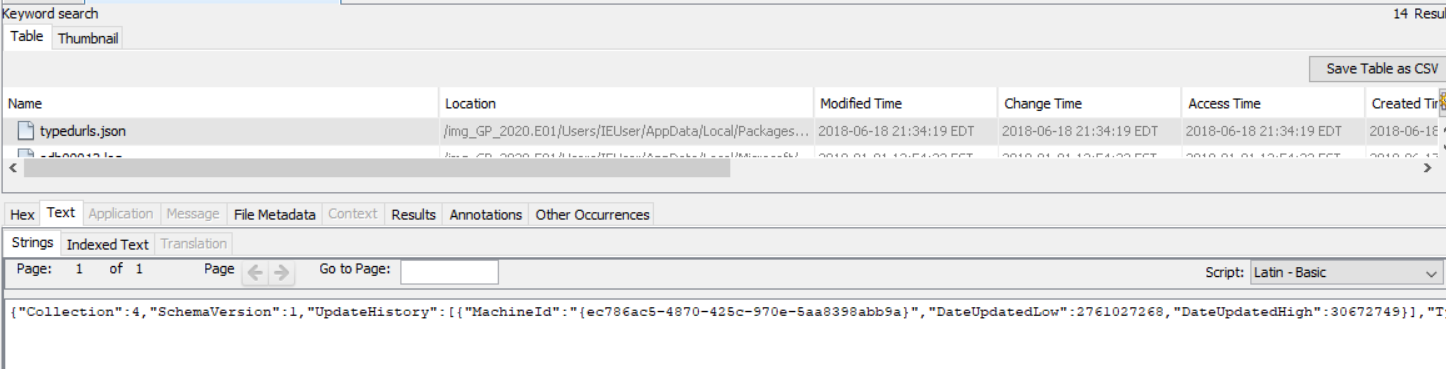
User: **Johnn**

A screenshot of a social media post

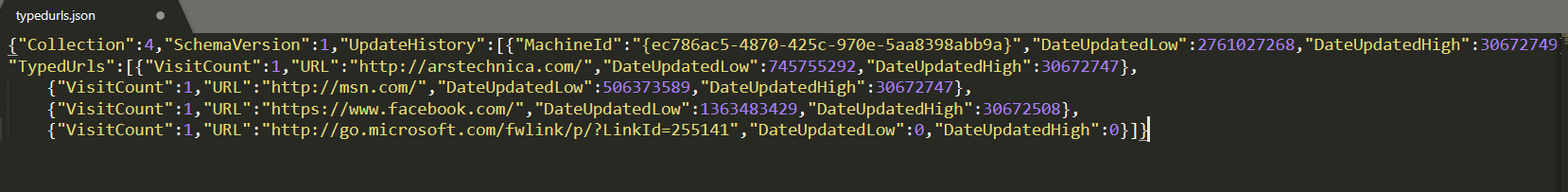
Description automatically generated

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

I searched for the typedurls in the keyword search and found a **typedurls.json** file



I extracted the file and opened it in a text editor. The contents of the file are shown below:



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

After using BEViewer for analyzing the forensic image, the software created two files, **ccn.txt** and **ccn\_histogram.txt** (shown below), showing possible credit card numbers and their number of occurrences in the system respectively.

A screenshot of a cell phone

Description automatically generated

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.**

I searched these terms in Autopsy using the Keyword Search feature in it and also used the help of the previous results which I obtained. Relevant results are shown below:

Search query: **Monarch**

There is an email in which Malcolm Monarch is communicating with Gene Poole.

A screenshot of a social media post

Description automatically generated

A screenshot of a social media post

Description automatically generated

Search query: **Drugs**

I found something which looks like a news article to me.

A screenshot of a social media post

Description automatically generated

Search query: **Mountain**

**A screenshot of a social media post

Description automatically generated**

Search query: **Powder**

Search query: **Chemical**

I found a file named projects-Copy.docx which has records of all the activities Gene is doing.

A screenshot of a social media post

Description automatically generated

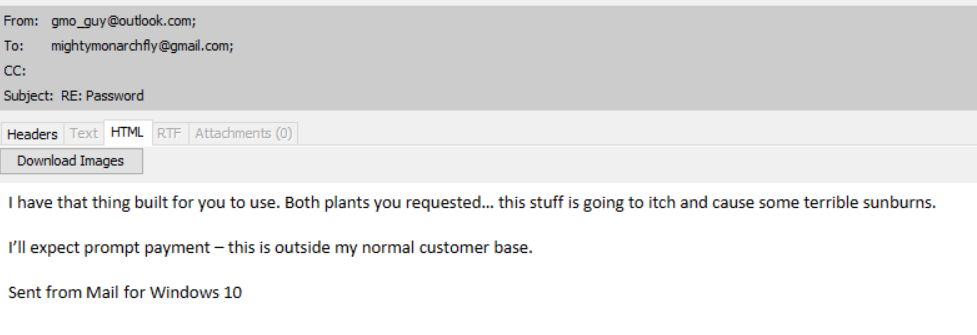
Also, I’m certain that the “Chemical Sales” refer to the drugs which have been sold.

A screenshot of a cell phone

Description automatically generated

1. **Identify associates of the subject with whom he may have been in communication.**

I was able to identify Gene’s associates through his email conversations with them. They are Malcolm Monarch ([mightymonarchfly@gmail.com](mailto:mightymonarchfly@gmail.com)),

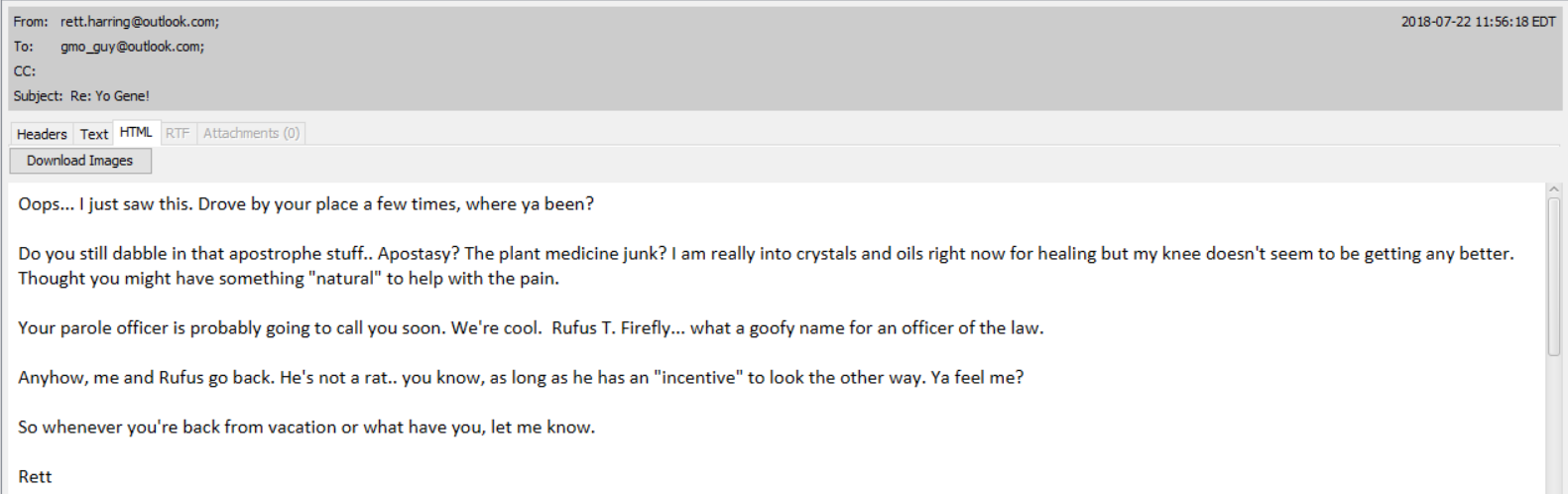


Rett Harring ([rett.harring@outlook.com](mailto:rett.harring@outlook.com)), the person having email address [macguff16@hotmail.com](mailto:macguff16@hotmail.com)

A screenshot of a social media post

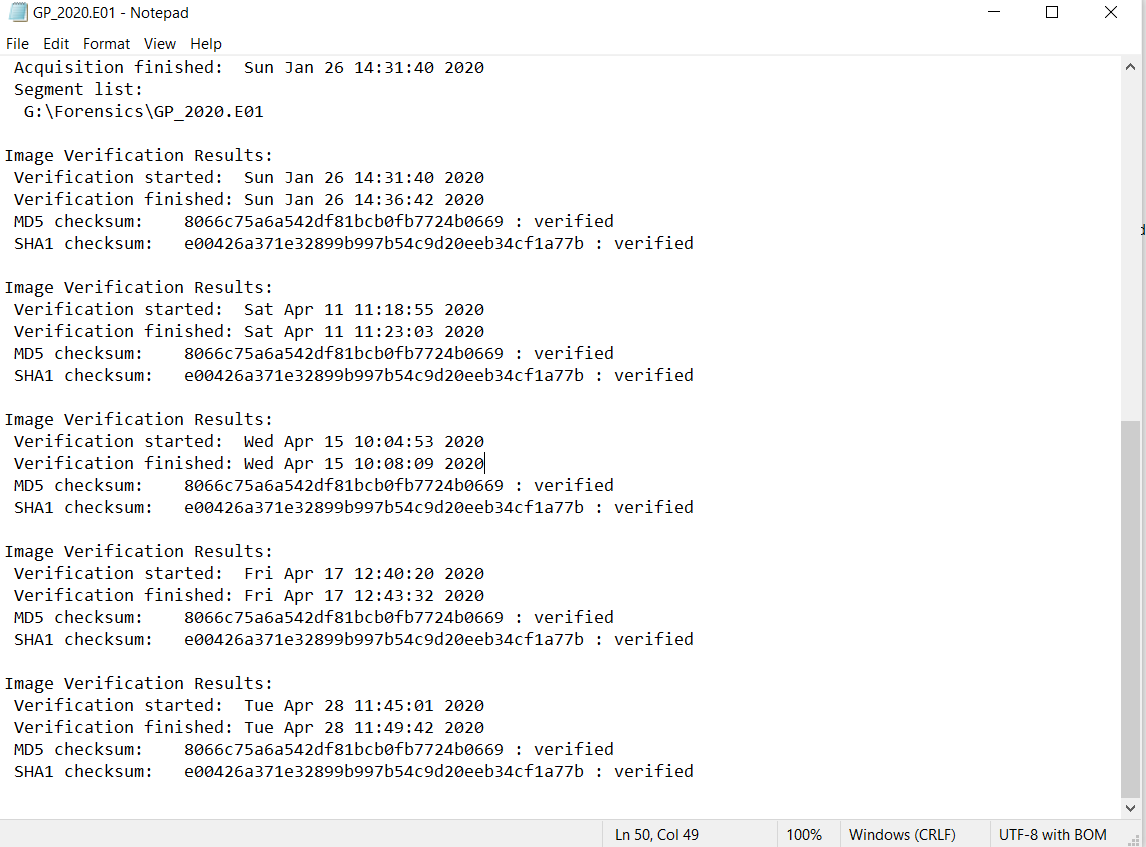
Description automatically generated

and Gene’s parole officer Rufus T. Firefly.



**Conclusion:**

After the examination of the forensic image, I verified the image again to make sure I haven’t made any changes to the image.



I have found significant amount of evidence which links Eugene Poole to the crime of manufacture and sale of drugs. I also found out the names of his associates who are involved in the crime and the images of the drugs.