ITIS 4250 / 5250

XXXXXX

Lab # Semester Project

XX/XX/XXXX

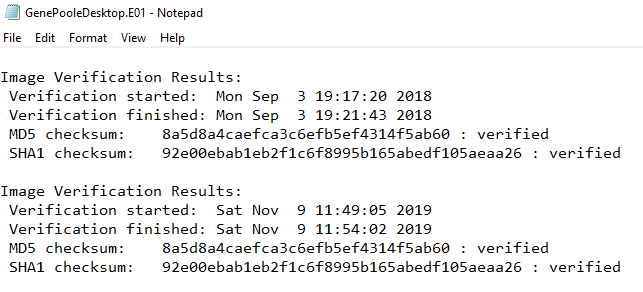
**Overview:**

I have been tasked by Detective Jessica Fletcher to process a desktop computer for her from a prior felon by the name of Eugene Poole. He is believed to be involved in the manufacturing and sale of narcotics. I have received all legal approval to go ahead and investigate the computer.

**Forensic Acquisition & Exam Preparation**

A lab technician was able to make an image (GenePooleDesktop.E01) from the desktop computer for analysis. The first step was transferring the file ‘GenePooleDesktop.E01’ from Canvas into a fresh folder on my work machine. My machine is a Lenovo Yoga 13 with 8gb of ddr4 ram along with an i5-8500. After transferring ‘GenePooleDesktop.E01’ on my machine I verified the hash to make sure the file hasn’t been tampered with

MD5: 8a5d8a4caefca3c6efb5ef4314f5ab60

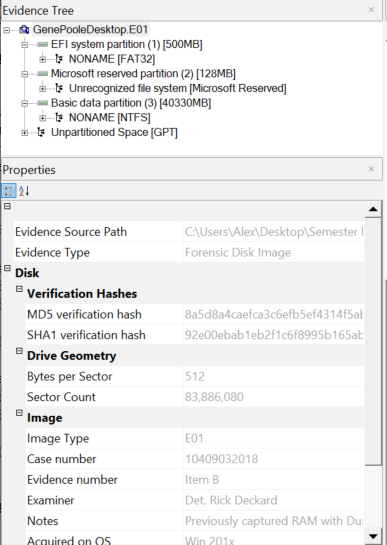


Software that I will be using for this report is as follows. Autopsy. Registry Explorer, Access Data Registry Viewer, Access Data FTK, and Jump List Viewer. Autopsy will be used for the bulk of the image analysis. Access Data Registry Viewer and Registry Explorer are used to investigate registry entries. Jump List Viewer will be used to investigate Jump Lists. Access Data FTK will be used to verify the image both before and after the invesitagion to make sure nothing has changed.

**Findings and Report (Forensic Analysis)**

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

There are 3 partitions on the drive. The first one is a EFI system partition [500mb], the second is a Microsoft reserved partition[128mb], the third is basic data partition[40233mb] and the unpartitioned space.



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

NTFS is Used on the basic data partition, and FAT32 is used on the EFI system Partition.

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



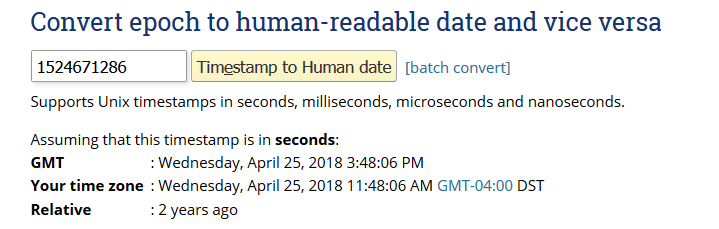
Windows 10 Enterprise

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

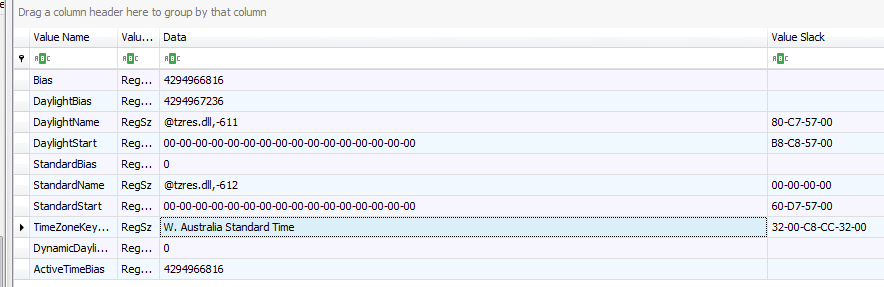
Using Registry Viewer I was able to load the windows registry into it and navigate to H:\Windows\System32\config\SOFTWARE: Microsoft\Windows NT\CurrentVersion

After navigating here I found the epoc date for the time that it was installed and converted it to normal time





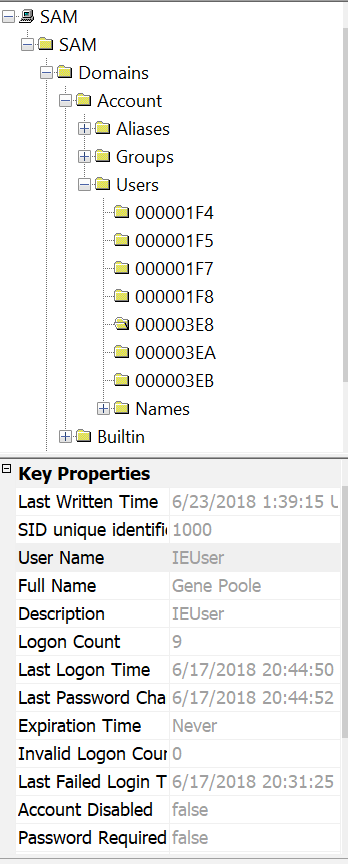
It was installed 2 years ago. April 25th, 2018

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

This was found by investigating the system registry found H:\Windows\System32\config\SYSTEM: ControlSet001\Control\TimeZoneInformation using Registry Viewer

UTC - 8

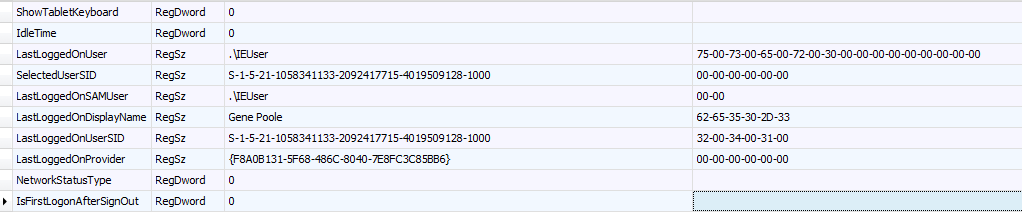
**Show the owner of the computer.**





The username IEUser is the owner who is Gene Poole

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



Gene Poole is the last user to login.

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

Rett Harring [rett.harring@outlook.com](mailto:rett.harring@outlook.com)

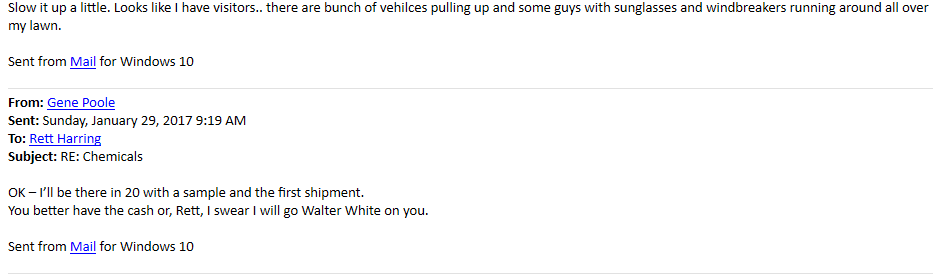
Malcon Monarch [mightymonarchfly@gmail.com](mailto:mightymonarchfly@gmail.com)

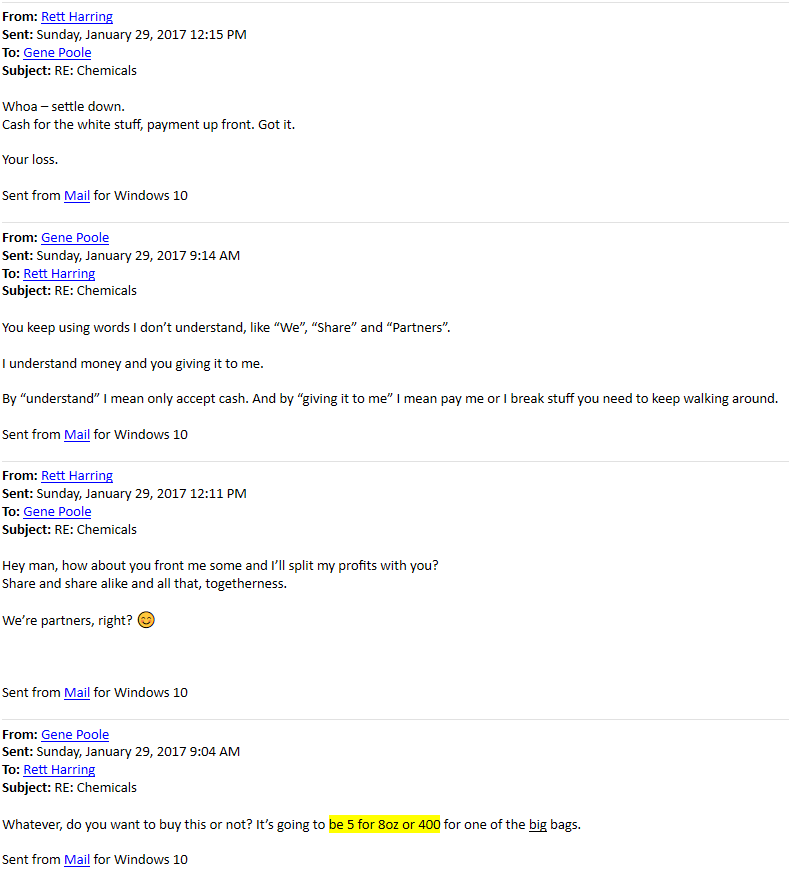
**Provide any communications the user engaged in with associates about criminal activity.**

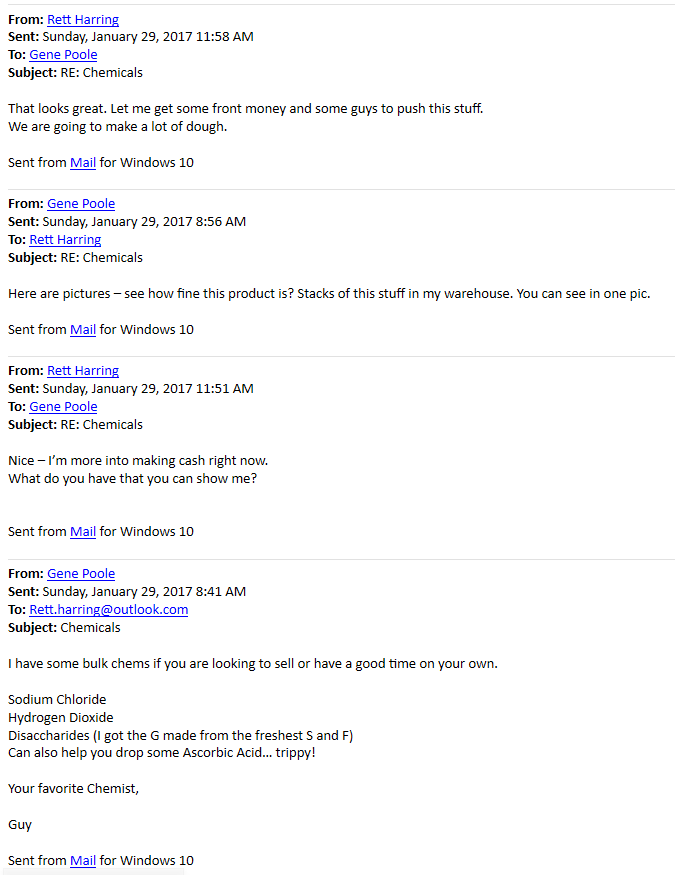
There are multiple emails

The threads between Rett Harring and Gene Poole

This conversation in early 2017 appears to discuss the selling and movement of drugs.



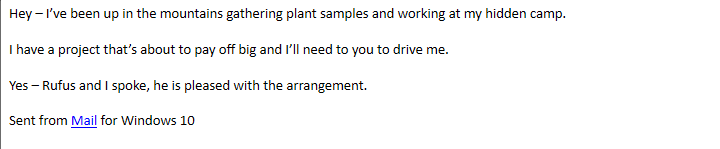


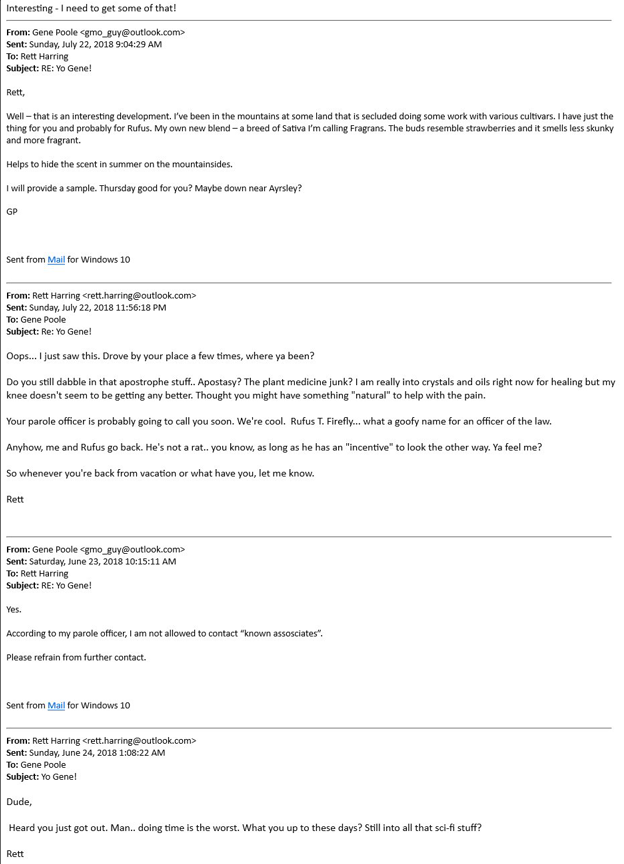


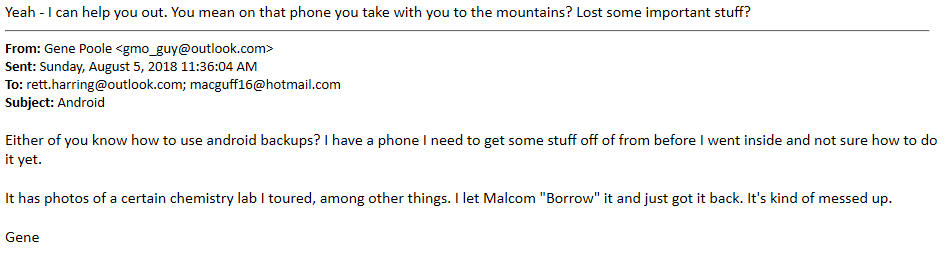
There is roughly a 1 year plus break between this conversation and the email from the next.

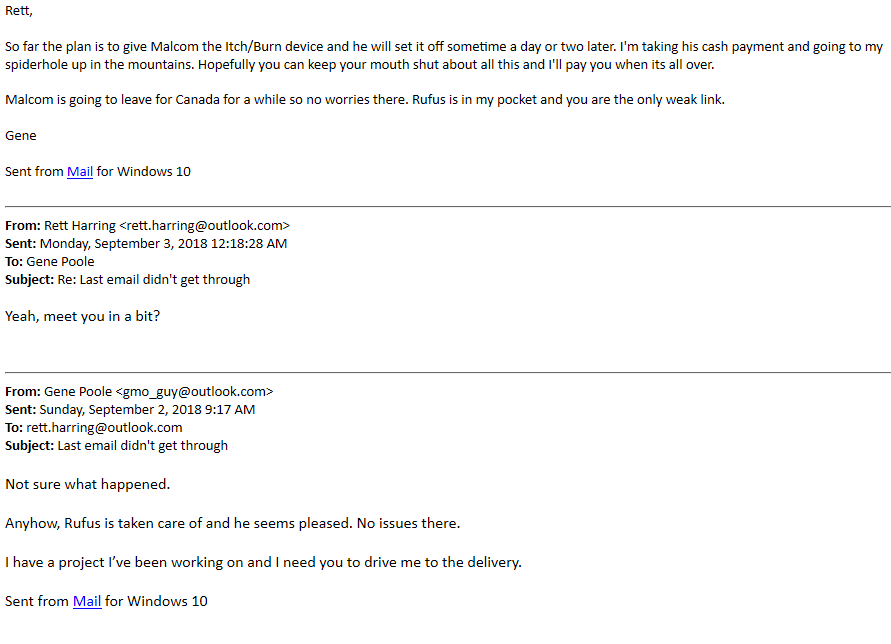
This next message threads takes place from June to September 2019.

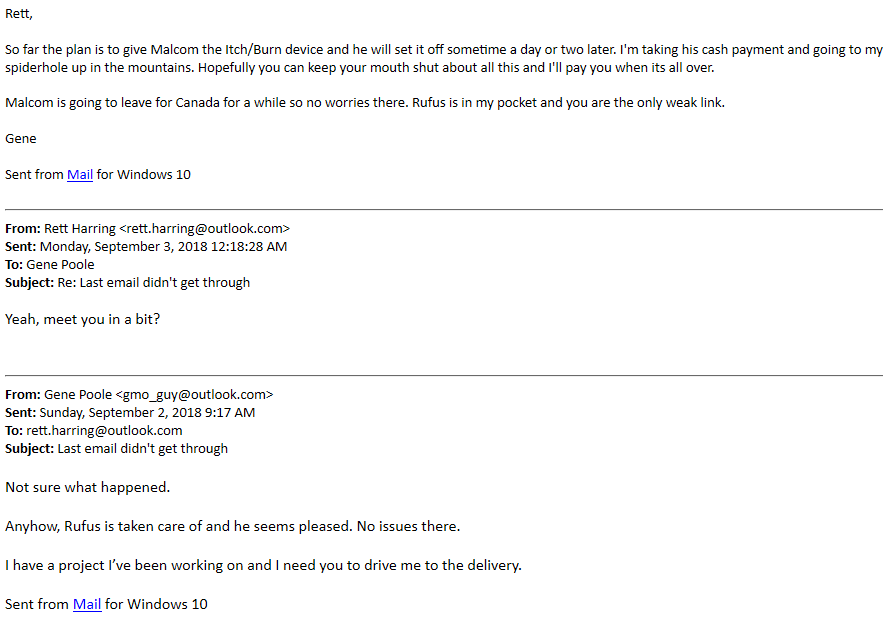
They discuss the creation of a chemical that Gene needs Rufus help within regards for someone named Malcom. In the messages they talk about Gene’s parole officer and how he is “not a rat”.



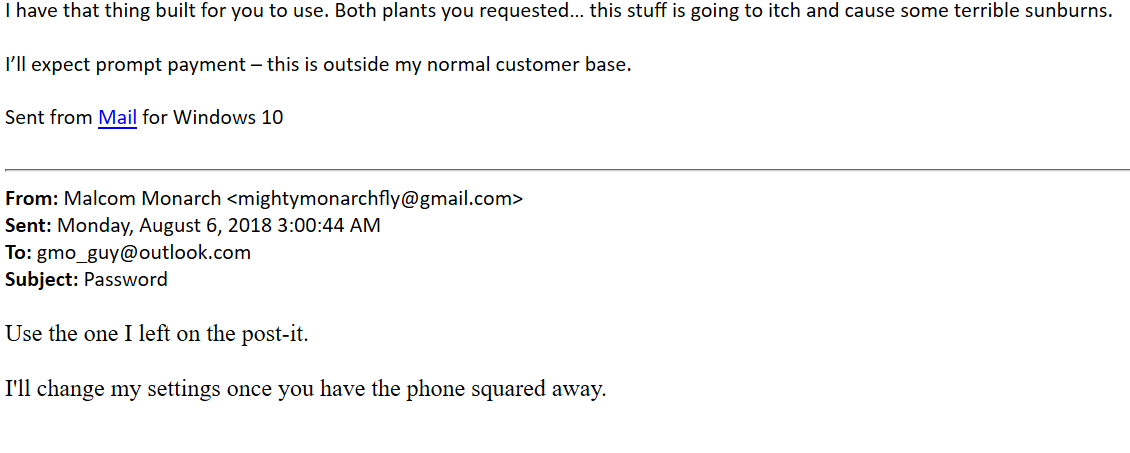




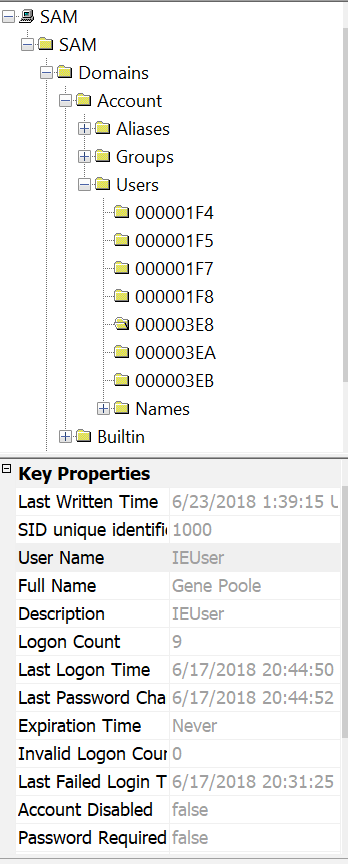




Then I found a discussion thread between Gene Poole and Malcom Monarch

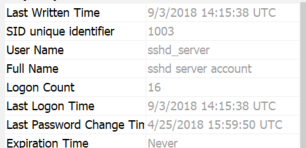


**Identify the last date and time the user logged on.**

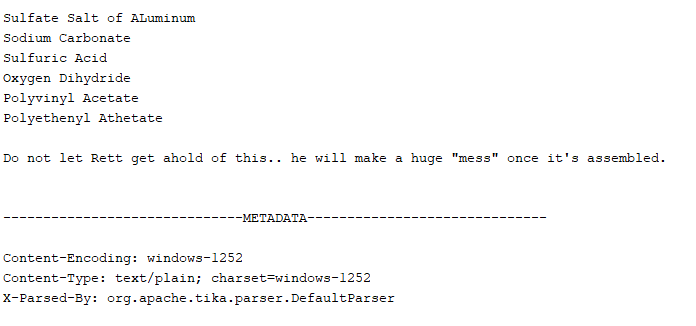


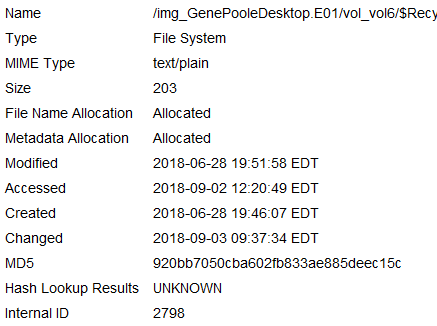
The user IEUser last logged on 6/17/2018 20:44:50 UTC

The last user to login, however, was sshd\_server user who logged in on 9/3/2018 at 14:15:38 UTC

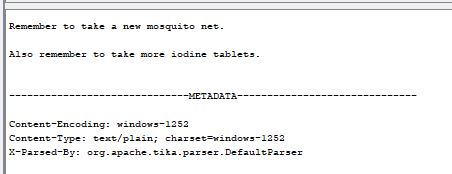


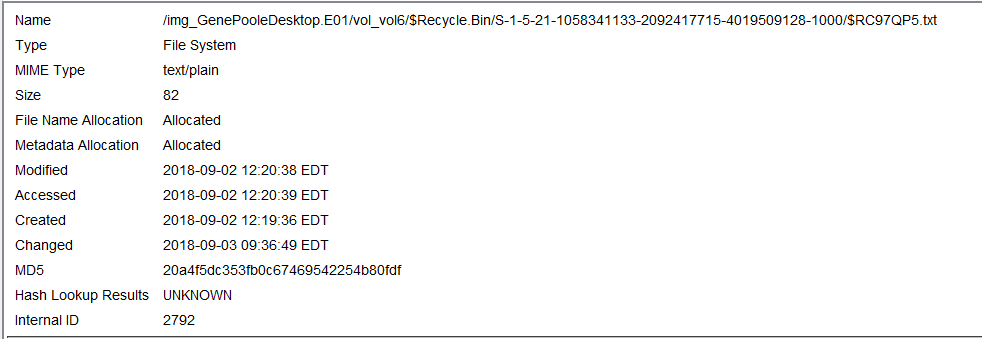
**Identify files placed in the recycle bin by the user, to include date deleted.**





This document was found in the recycling bin. This file is called Shopping.txt which was recycled by Gene Poole IEUser.





Another text file was also found with information regard iodine tablets.

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

The user’s background was found in

/img\_GenePooleDesktop.E01/vol\_vol6/Users/IEUser/AppData/Roaming/Microsoft/Windows/Themes

c

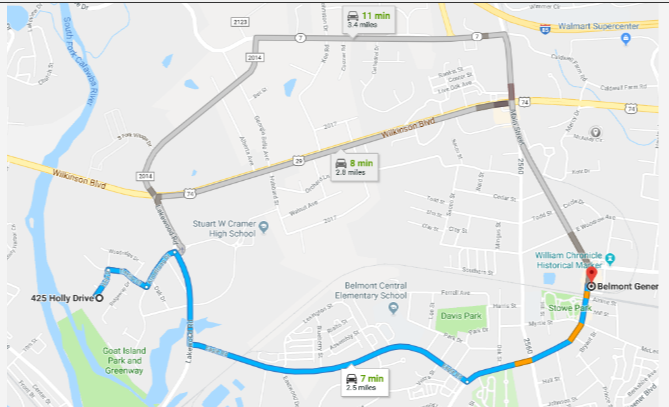
**Identify any locations other than the subject's home that may have been involved (this does not require an exact address).**

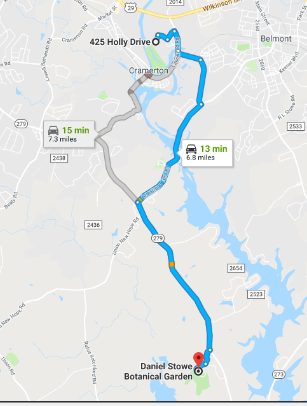
The subject has Google route photos of different locations

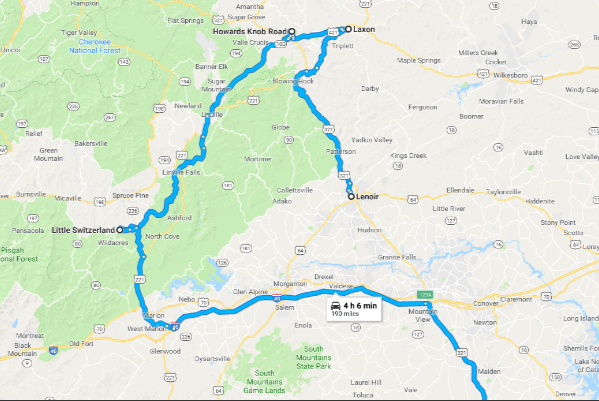
These other locations (all North Carolina) from these screenshots include

A location within the town of Belmont, not far from the subjects home at 435 Holly Drive

* Daniel Stowe Botanical Garden
* Little Switzerland
* Howards Knob Road
* Laxon

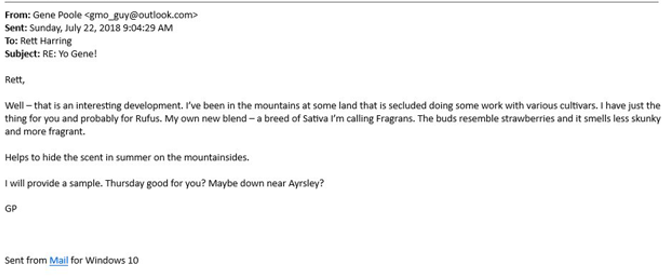






Things to Note:

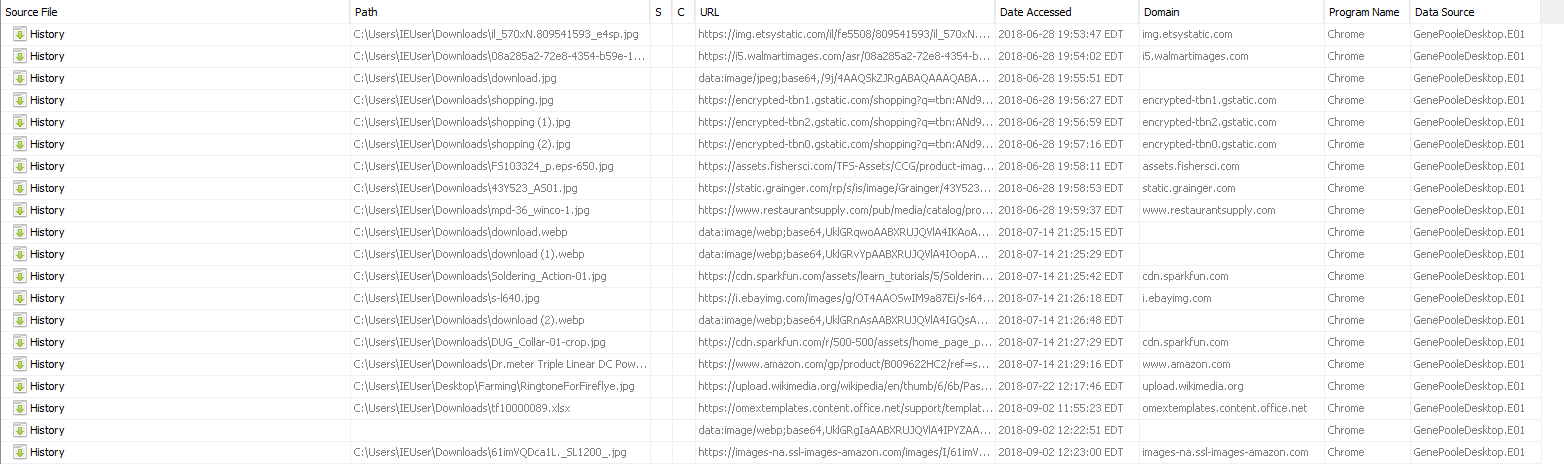
In pervious contacts with a possible accomplish, Gene was talking about a camp in the mountains which is secluded.



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

The pictures of the possible locations where activity may have been involved have been posted above. There are also images that have been found from the internet that have been posted below, in these photos there are images of drugs and other items that are possibly used to make drugs.

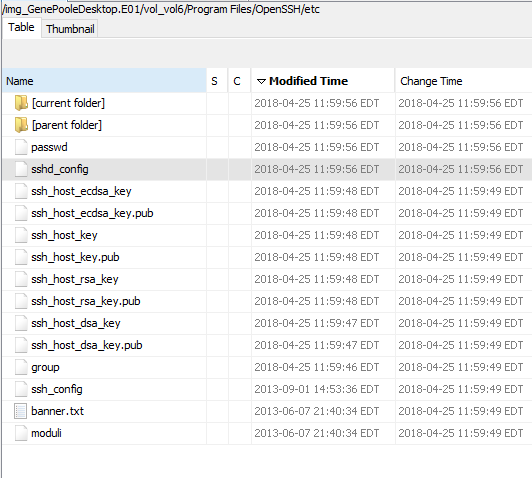
**Identify files downloaded from the internet.**

This is a list of the files downloaded from the internet 

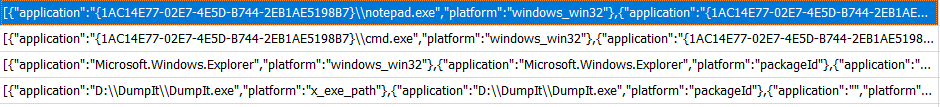
Some of the thumbnails are listed further below in the document as well.

**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.**

The Machine has SSH installed, which could mean that the user has the ability to remote in without needing the computer present.

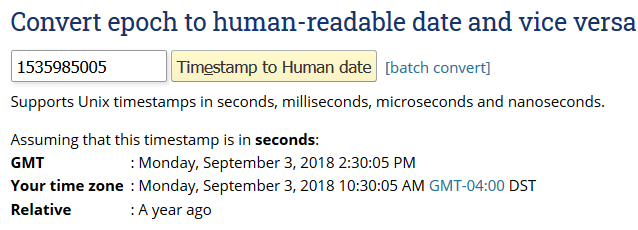


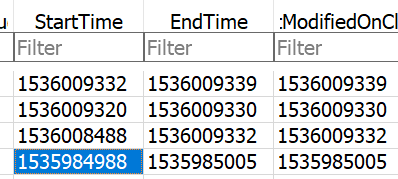
Another Application that I found was dumpit.exe, this appears to be a memory dumping application which is used to dump the memory.



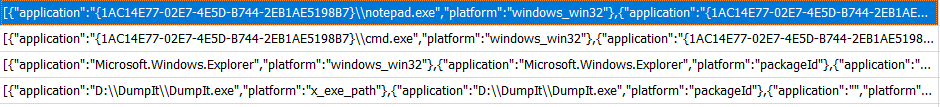
**Identify software used most recently (within the last month before the image was made).**

The last software that was used (if not considering notepad.exe, or cmd) was a executable called dumpit.exe. This was used September 3, 2018. After more research it appears that dumpit.exe is software to dump the memory in windows.



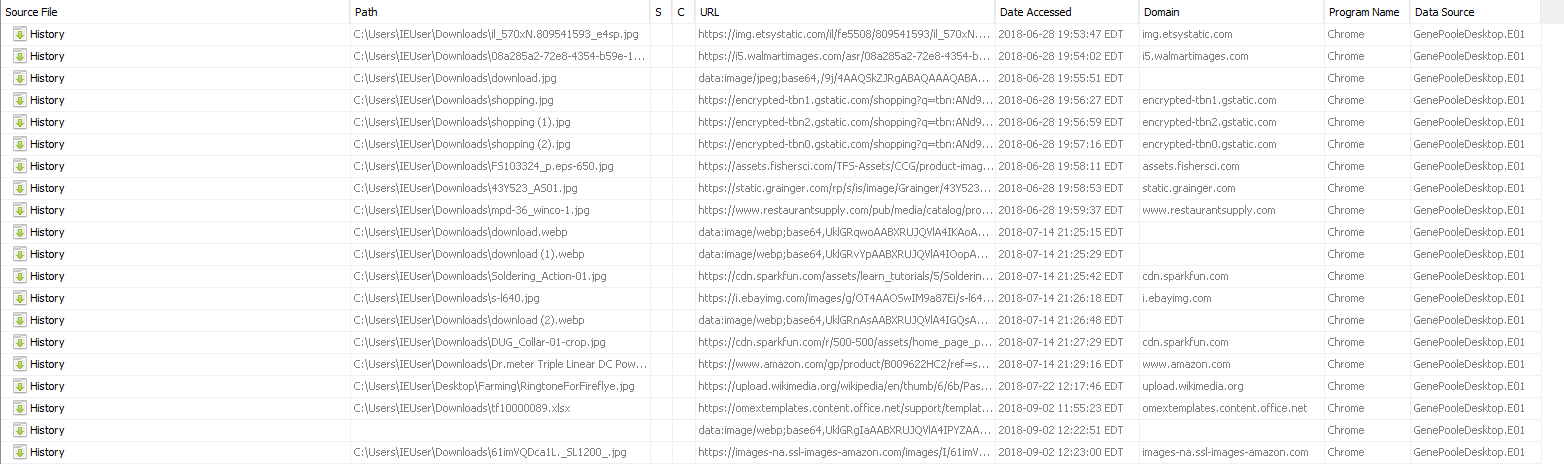


Location: /img\_GenePooleDesktop.E01/vol\_vol6/Users/IEUser/AppData/Local/ConnectedDevicesPlatform/e3c7c18e30e40cfe/.



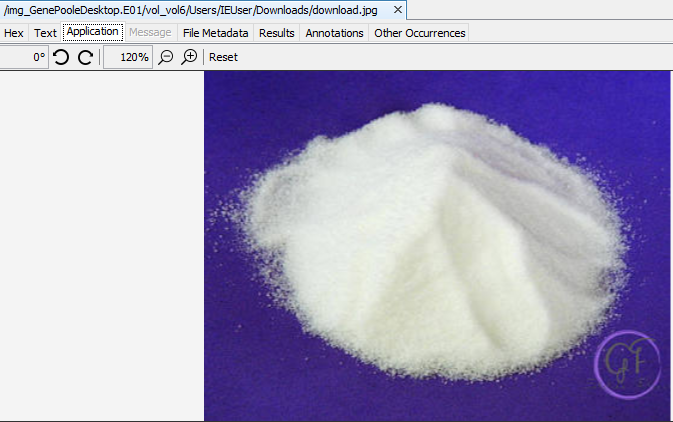
**Provide a list of files downloaded to the computer from the Internet that are relevant.**

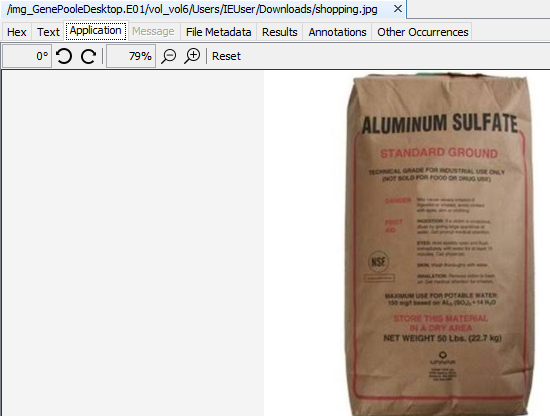
It appears that there are many files that the user has downloaded from the internet



After further investigation I found many that are relevant and have included a few screen shots of them below, most appear to be drugs, and safety equipment.

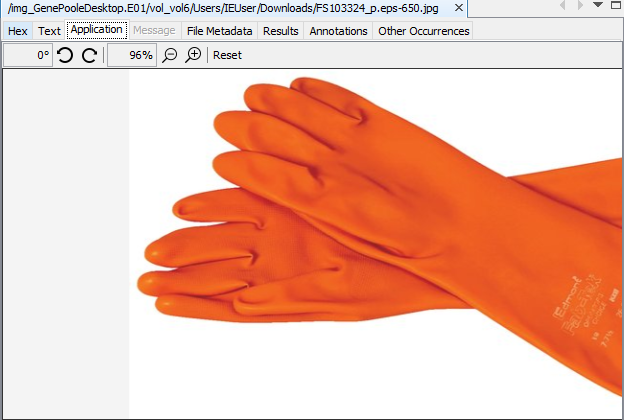


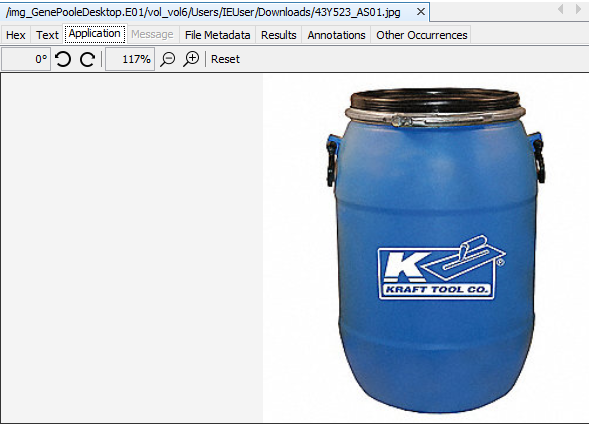








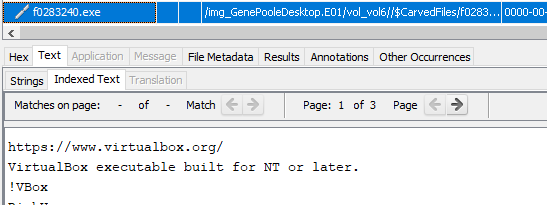




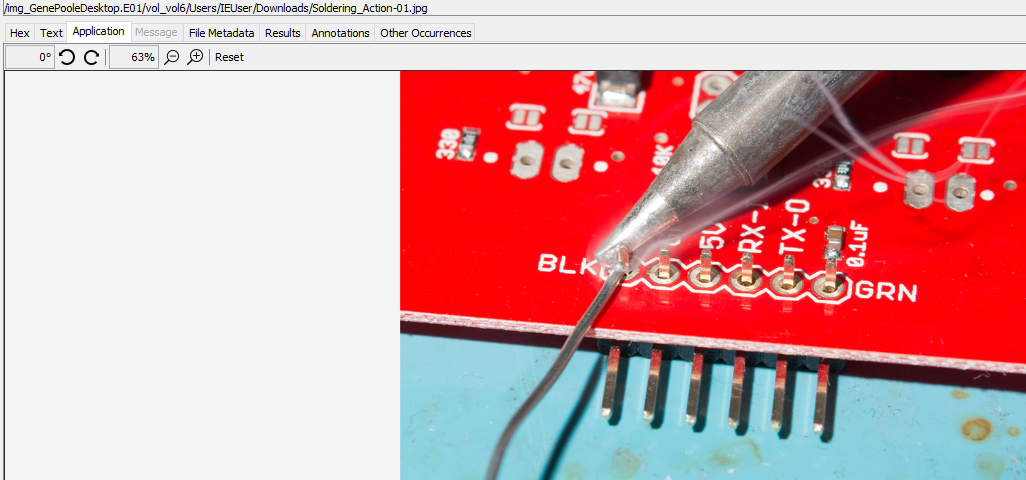
**Perform a file carving and describe any relevant files found.**

After conducting a file carve, I found some additional files that are relevant.

I found a VirtualBox executable, VirtualBox could be used in a way to conceal activity on the computer, by having it done through a VM

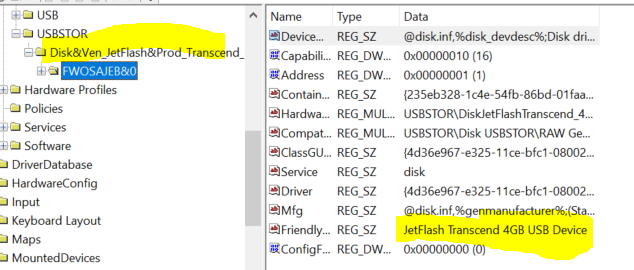


I was also able to find another relevant image from the exif metadata



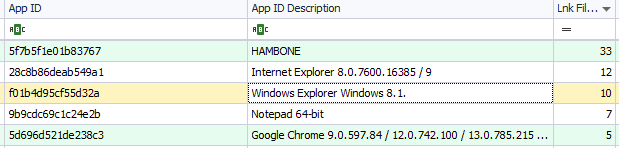
**Determine whether investigators or crime scene specialists may have missed any devices that were connected to the computer.**

After checking the registry, I was able to find that JetFlash Transcend 4gb USB flash drive.



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

The 3 most often runs programs are as follows

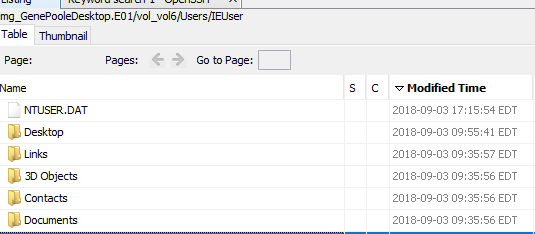


An app called Hambone, Internet Explorer (two versions), and then notepad.

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

The Last 5 folders edited by the user are as follows:

* Desktop
* Links
* 3D Objects
* Contacts
* Documents



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

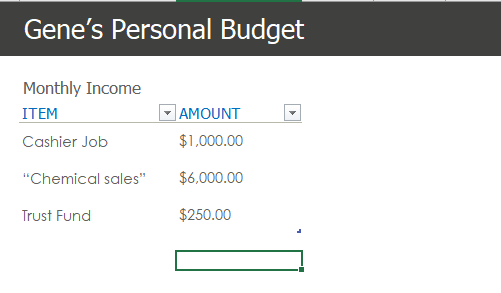
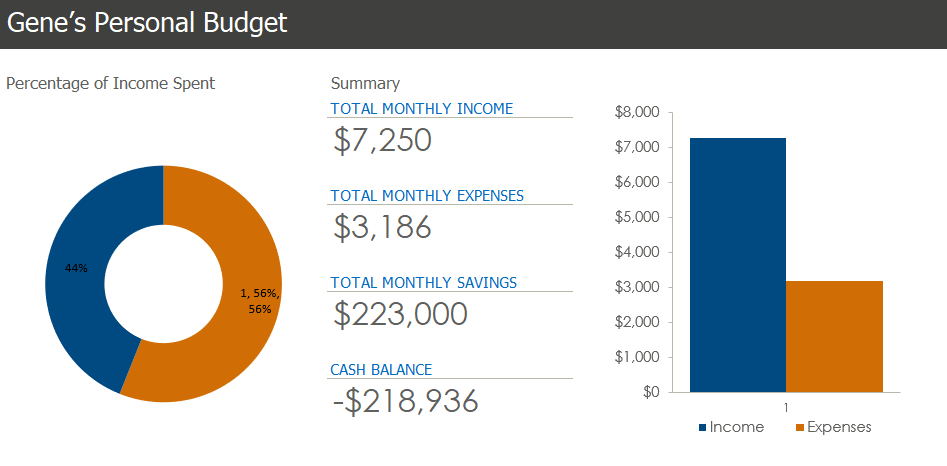
The registry entries and other locations that I have checked for the last manually typed addresses did not have any data regarding the history of manually typed addresses, I am unable to verify this to the best of my ability.

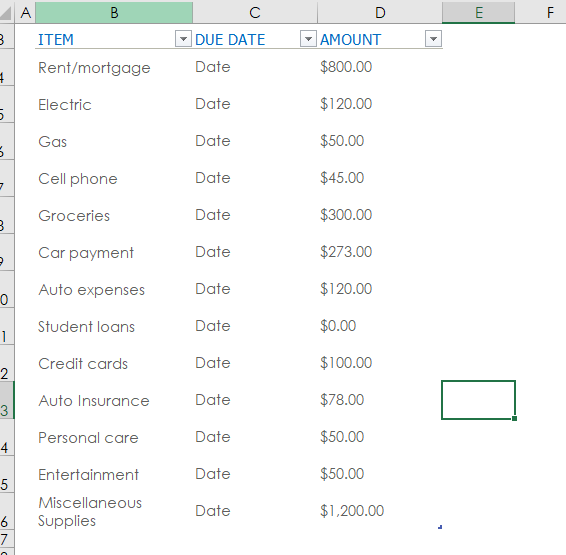
**Identify any credit card numbers on the drive. (This will require search with a regular expression)**

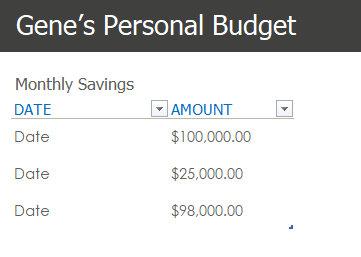
After Searching for Credit Card Files I found an interesting Excel documents that contained information regarding to the case

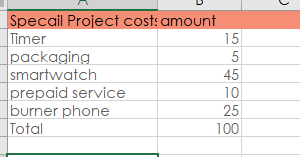


The Budget.xlsx file









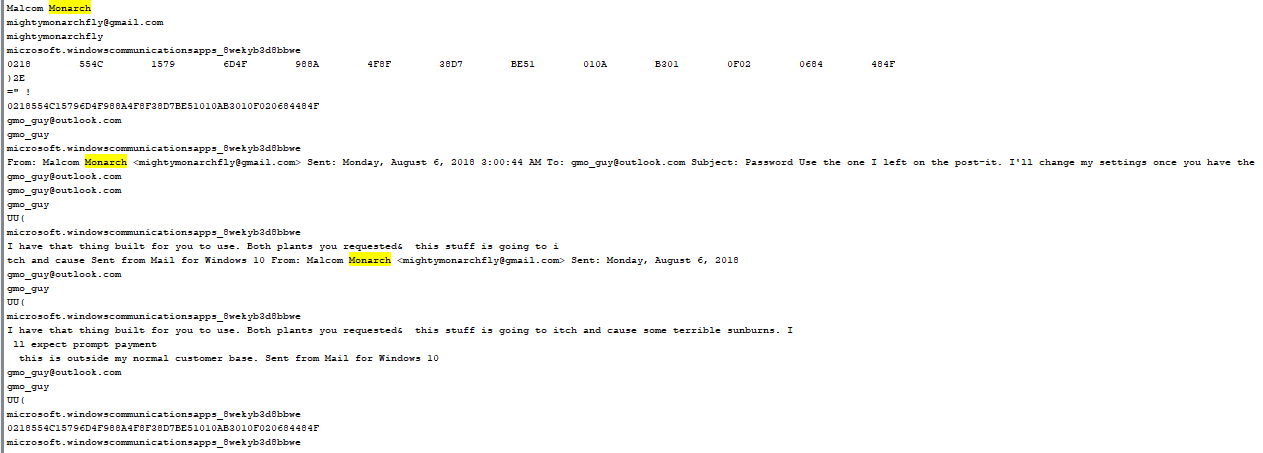
In this excel document you can see how he refers to a major part of his income as “Chemical Sales” Along with a sheet pertaining to a “Specail Project” and its costs. Here there is a list for Timer, packaging, smartwatch, prepaid service, burner phone.

**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.**

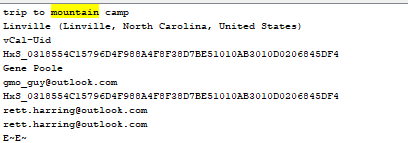










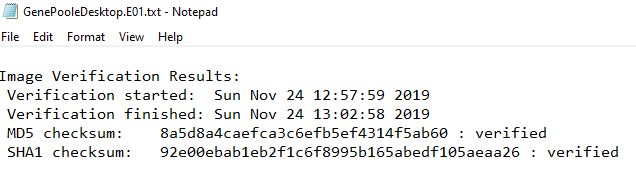


**Identify associates of the subject with whom he may have been in communication.**

Malcom Monarch mightymonarchfly@gmail.com

Rett Harring rett.harring@outlook.com

After conducting my analysis I re-verified the image to make sure that it hasn’t been altered



**Conclusion:**

During this investigation I was able to find evidence of email conversations between the suspect Gene Poole and other accomplishes, these include Rett Harring and Malcom Monarch. Within these emails it seems that there is discussion of producing and selling drugs, one of them being for Malcom Monarch. There was also discussion of materials needed that included photos downloaded from the internet that contained chemicals and safety equipment. There were also screenshots of google routes to the mountains which should be investigated considering there was discussion of a secluded base in the mountains. Found on the computer was also software that is/was installed regarding to anti-forensics. An excel document has also been found to contain a budget regarding a plan that included “burner phone” and “timer”.