

Mikiyas Solomon

Lab 6

4/19/2022

### **Overview**

The file I received from detective Fletcher was GP2020.E01. Detective Fletcher has tasked me with examining this forensic image and uncovering any and all evidence that is hidden in the image. The felon Eugene has been suspected to be involved with the manufacture and sale of drugs so I will have to look thoroughly to uncover any contacts or evidence to prove this.

### **Files Acquired**

The file acquired is GP\_2020.E01, GMOGUY\_backup.pst, GP\_2020.E01.txt

### **Files Acquired from**

The files were acquired from the CCI Forensics Lab

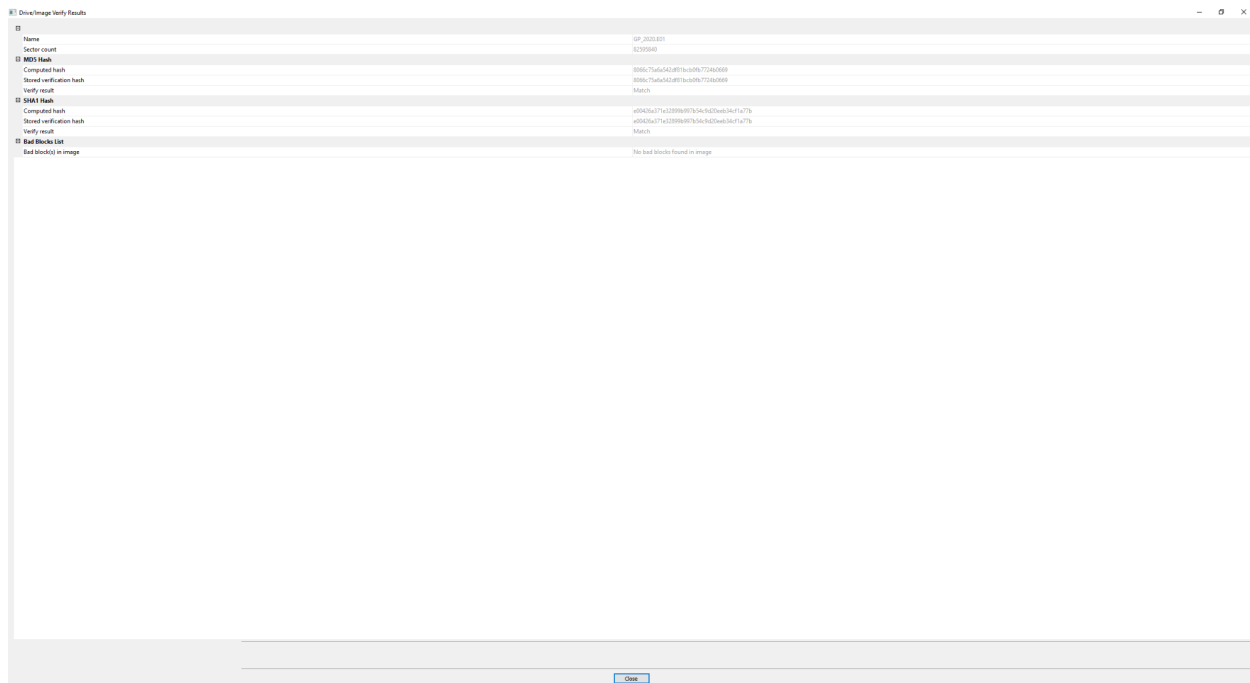
### **Forensic Acquisition and Examination Preparation**

The exam environment is performed at the home desktop using the Windows 10 operating system

## Software Used

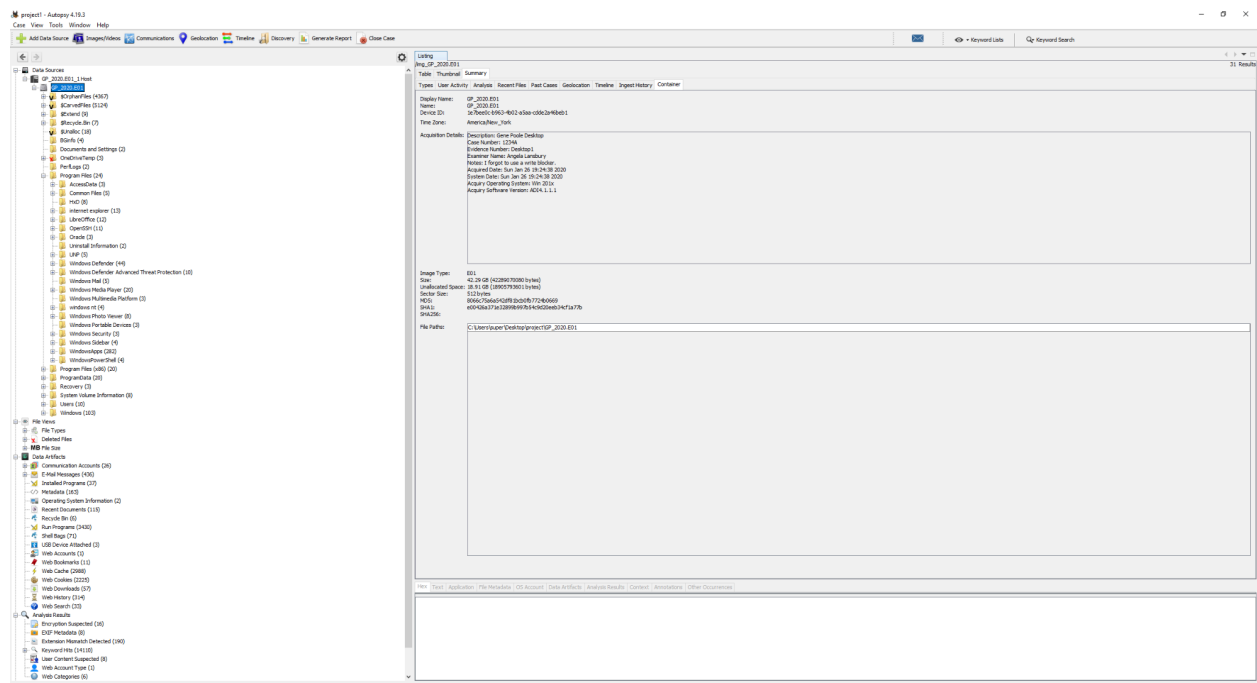
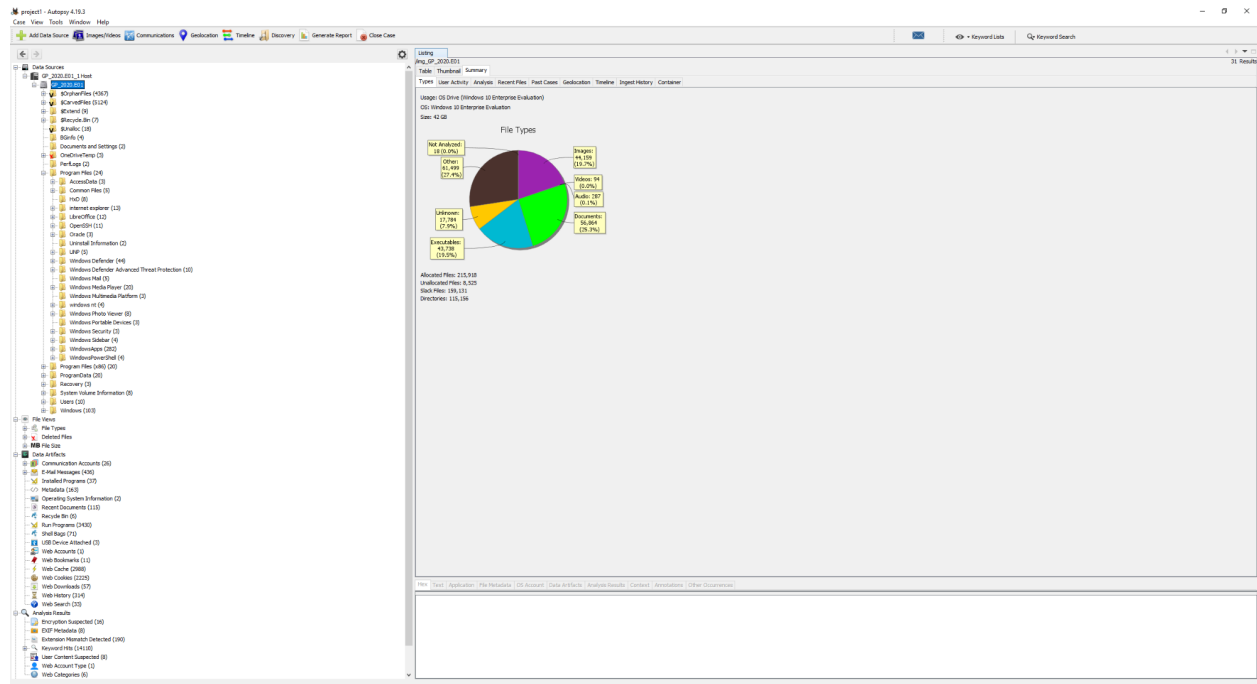
The software used is FTK imager, Autopsy and SQLite

## Verification of file



## Forensic Analysis

1. All the space on the hard drive was split up between images, documents, videos, documents, and audio and the rest is unknown. This can be found by going into GP\_2020.E01 and going into summary/types. By going into the container you can see that there is 18.91GB free.



- The type of file system in use is NTFS as \$MFT was found in the root of the image file and that is one of the most important files in the NTFS file system

3. The version of the operating system was found under data artifacts and in the operating system information. The operating system is windows 10 enterprise evaluation

Encryption Suspected (16)	Program Name	Windows 10 Enterprise Evaluation	Recent Activity
EXIF Metadata (8)	Date/Time	2018-04-25 11:48:06 EDT	Recent Activity
Extension Mismatch Detected (190)	Path	C:\Windows	Recent Activity
Keyword Hits (38580)	Product ID	00329-20000-00001-AA244	Recent Activity
User Content Suspected (8)	Owner	Eugene Poole	Recent Activity
Web Account Type (1)	Organization	The Guild of Calamitous Intent	Recent Activity
Web Categories (6)	Source File Path	/img_gp_2020.E01/Windows/System32/config/SOFTWARE	
OS Accounts	Artifact ID	-9223372036854775433	



- The date the os was installed was found under data artifacts and operating system information. By going into the software and looking at the source file metadata you can see it was created 2018-04-11 17:04:33 EDT

Metadata	
Name:	/img_GP_2020.E01/Windows/System32/config/SOFTWARE
Type:	File System
MIME Type:	application/x-windows-registry
Size:	8352496
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2020-01-26 13:40:13 EDT
Accessed:	2020-01-26 13:40:18 EDT
Created:	2018-04-11 17:04:33 EDT
Changed:	2018-04-11 12:45:08 EDT
MDS:	73b55ea4e7610877012d5b2334d4f401
SHA-256:	0d8804603115c245a7eb498b8bedad4f51dccc1b1858f63cc0e0036a65c8

- The timezone information was found in GP\_2020.E01 by clicking on the summary tab and going into the container and looking at the time zone which is America/New\_York

project1 - Autopsy 4.19.3

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Keyword Lists Keyword Search

Listing /img\_GP\_2020.E01 31 Results

Table Thumbnail Summary

Types User Activity Analysis Recent Files Past Cases Geolocation Timeline Ingest History Container

Display Name: GP\_2020.E01  
Name: GP\_2020.E01  
Device ID: 1e7bee0c-b963-4b02-a5aa-cdde2a46beb1  
Time Zone: America/New\_York

Acquisition Details:  
System Date: Sun Jan 26 19:24:38 2020  
Acquiry Operating System: Win 201x  
Acquiry Software Version: ADI4.1.1.1

Image Type: E01  
Size: 42.29 GB (4289070080 bytes)  
Unallocated Space: 18.91 GB (1890579360 bytes)  
Sector Size: 512 bytes  
MDS: 8066c75a6a542d81bcb0fb7724b0669  
SHA1: e00426a371e32859b997b54c3d20eeb34cf1a77b  
SHA256:

File Paths:  
C:\Users\super\Desktop\project\GP\_2020.E01

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Data Sources

- GP\_2020.E01\_1\_Host
  - GP\_2020.E01
    - \$OrphanFiles (4367)
    - \$CarvedFiles (5124)
    - \$Extend (9)
    - \$Recycle.Bin (7)
    - \$Unaloc (18)
    - BGInfo (4)
    - Documents and Settings (2)
    - OneDriveTemp (3)
    - PerfLogs (2)
    - Program Files (24)
    - Program Files (x86) (20)
    - ProgramData (20)
    - Recovery (3)
    - System Volume Information (8)
    - EDP (3)
    - Users (10)
    - Windows (103)

File Views

- File Types
- Deleted Files
- MB File Size

Data Artifacts

- Communication Accounts (26)
- E-Mail Messages (436)
- Installed Programs (37)
- Metadata (163)
- Operating System Information (2)
- Recent Documents (115)
- Recycle Bin (6)
- Run Programs (3430)
- Shell Bags (71)
- USB Device Attached (3)
- Web Accounts (1)

- The owner of the computer was found under data artifacts and operating system information. By going into software you can see the owner is Eugene Pool

project1 - Autopsy 4.19.3

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing 2 Results

Operating System Information

Source Name	S	C	O	Name	Domain	Version	Processor Architecture	Temporary Files Directory	Data Source	Program Name
SYSTEM				MSEDGEWIN10		Windows_NT	AMD64	%SystemRoot%\TEMP	GP_2020.E01	
SOFTWARE									GP_2020.E01	Windows 10 Enter

Save Table as CSV

Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Result: 1 of 38 Result

Operating System Information

Type	Value	Source(s)
Program Name	Windows 10 Enterprise Evaluation	Recent Activity
Date/Time	2018-04-25 11:48:06 EDT	Recent Activity
Path	C:\Windows	Recent Activity
Product ID	00329-20000-00001-AA244	Recent Activity
Owner	Eugene Poole	Recent Activity
Organization	The Guild of Calamitous Intent	Recent Activity
Source File Path	jmg_GP_2020.E01\Windows\System32\config\SOFTWARE	
Artifact ID	-9223372036854775433	

- The account used to log in is IEUser and the method is a normal username and password login. This can be found under os accounts.

project1 - Autopsy 4.19.3

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing 15 Results

Table Thumbnail Summary

Name	S	C	O	Login Name	Host	Scope	Root Name	Creation Time
IEUser				IEUser	GP_2020.E01_1 Host	Local		2018-04-25 11:47:54 EDT
IEUser				IEUser	GP_2020.E01_1 Host	Local		2018-04-25 11:47:54 EDT
IEUser				IEUser	GP_2020.E01_1 Host	Local		2018-04-25 11:47:54 EDT
IEUser				IEUser	GP_2020.E01_1 Host	Local		2018-04-25 11:47:54 EDT
IEUser				IEUser	GP_2020.E01_1 Host	Local		2018-04-25 11:47:54 EDT
IEUser				IEUser	GP_2020.E01_1 Host	Local		2018-04-25 11:47:54 EDT
IEUser				IEUser	GP_2020.E01_1 Host	Local		2018-04-25 11:47:54 EDT
IEUser				IEUser	GP_2020.E01_1 Host	Local		2018-04-25 11:47:54 EDT
IEUser				IEUser	GP_2020.E01_1 Host	Local		2018-04-25 11:47:54 EDT
IEUser				IEUser	GP_2020.E01_1 Host	Local		2018-04-25 11:47:54 EDT
IEUser				IEUser	GP_2020.E01_1 Host	Local		2018-04-25 11:47:54 EDT
IEUser				IEUser	GP_2020.E01_1 Host	Local		2018-04-25 11:47:54 EDT
IEUser				IEUser	GP_2020.E01_1 Host	Local		2018-04-25 11:47:54 EDT
IEUser				IEUser	GP_2020.E01_1 Host	Local		2018-04-25 11:47:54 EDT

Save Table as CSV

Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Basic Properties

Name: IEUser  
Full Name: IEUser  
Address: 9-5-21-208041120-208041120-401000128-1000  
Type: Local  
Creation Date: 2018-04-25 11:47:54 EDT

GP\_2020.E01\_1 Host Details

Last Login: 2018-04-25 11:44:30 EDT  
Login Count: 9  
Description: IEUser  
Email: gpm\_jan@bushnell.com  
Password Path: 2018-04-25 11:47:54 EDT  
Password Settings: Password: Blank not secure  
Flags: Normal user account  
Home Directory: C:\Users\IEUser

Basic Properties

Name: IEUser  
Address: 9-5-21-208041120-208041120-401000128-1000  
Scope: Local  
Confidence: Inferred

8. The associates that were identified in the criminal activity are Ret Harring, Rufus, and Malcolm monarch. This was found using autopsy under data artifacts and looking through the sent email messages.

Rett,

So far the plan is to give Malcom the Itch/Burn device and he will set it off sometime a day or two later, I'm taking his cash payment and going to my spiderhole up in the mountains. Hopefully you can keep your mouth shut about all this and I'll pay you when its all over.

Malcom is going to leave for Canada for a while so no worries there. Rufus is in my pocket and you are the only weak link.

Gene

Sent from [Mail](#) for Windows 10

---

**From:** Rett Harring <rett.harring@outlook.com>  
**Sent:** Monday, September 3, 2018 12:18:28 AM  
**To:** Gene Poole  
**Subject:** Re: Last email didn't get through

Yeah, meet you in a bit?

---

I have that thing built for you to use. Both plants you requested... this stuff is going to itch and cause some terrible sunburns.

I'll expect prompt payment -- this is outside my normal customer base.

Sent from [Mail](#) for Windows 10

---

**From:** Malcom Monarch <mighthymonarchfly@gmail.com>  
**Sent:** Monday, August 6, 2018 3:00:44 AM  
**To:** gmo\_guy@outlook.com  
**Subject:** Password

Use the one I left on the post-it.

I'll change my settings once you have the phone squared away.

---

**From:** Rett Harring <rett.harring@outlook.com>  
**Sent:** Sunday, July 22, 2018 11:56:18 PM  
**To:** Gene Poole  
**Subject:** Re: Yo Gene!

Oops... I just saw this. Drove by your place a few times, where ya been?

Do you still dabble in that apostrophe stuff.. Apostasy? The plant medicine junk? I am really into crystals and oils right now for healing but my knee doesn't seem to be getting any better. Thought you might have something "natural" to help with the pain.

Your parole officer is probably going to call you soon. We're cool. Rufus T. Firefly... what a goofy name for an officer of the law.

Anyhow, me and Rufus go back. He's not a rat.. you know, as long as he has an "incentive" to look the other way. Ya feel me?

So whenever you're back from vacation or what have you, let me know.

9. The user engaged in communications with multiple sources, this was found looking through email messages using autopsy

**From:** gmo\_guy@outlook.com  
**To:** rett.harring@outlook.com  
**CC:**  
**Subject:** Re: Yo Gene!

2018-09-02 12:08:47 EDT

Headers: [Text](#) [HTML](#) [PDF](#) [Attachments](#) [Accounts](#)

[Hide Images](#)

Hey -- I've been up in the mountains gathering plant samples and working at my hidden camp.

I have a project that's about to pay off big and I'll need to you to drive me.

Yes -- Rufus and I spoke, he is pleased with the arrangement.

Sent from [Mail](#) for Windows 10

---

**From:** Rett Harring <rett.harring@outlook.com>  
**Sent:** Sunday, July 22, 2018 11:56:18 PM  
**To:** Gene Poole  
**Subject:** Re: Yo Gene!

Oops... I just saw this. Drove by your place a few times, where ya been?

From: gmo.guy@outlook.com  
To: rett.harring@outlook.com  
CC:  
Subject: RE: Chemicals

2017-01-29 12:13:57 EST

Headers | Text | HTML | RTF | Attachments (0) | Accounts

Hide Images

ATTENTION: This message contains information that may be confidential, proprietary or otherwise subject to legal privilege. If you are not a named addressee, you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not a named addressee you should not disseminate, distribute or copy this e-mail.

To: [Rett Harring](#)  
Subject: RE: Chemicals

Whatever, do you want to buy this or not? It's going to be 5 for 800 or 400 for one of the big bags.

Sent from [Mail](#) for Windows 10

---

From: [Rett Harring](#)  
Sent: Sunday, January 29, 2017 11:58 AM  
To: [Gene Poole](#)  
Subject: RE: Chemicals

That looks great. Let me get some front money and some guys to push this stuff.  
We are going to make a lot of dough.

Sent from [Mail](#) for Windows 10

---

From: [Gene Poole](#)  
Sent: Sunday, January 29, 2017 8:56 AM  
To: [Rett Harring](#)  
Subject: RE: Chemicals

Here are pictures – see how fine this product is? Stacks of this stuff in my warehouse. You can see in one pic.

Sent from [Mail](#) for Windows 10

---

From: [Rett Harring](#)  
Sent: Sunday, January 29, 2017 11:51 AM  
To: [Gene Poole](#)  
Subject: RE: Chemicals

Nice – I'm more into making cash right now.

---

Rett,

Well – that is an interesting development. I've been in the mountains at some land that is secluded doing some work with various cultivars. I have just the thing for you and probably for Rufus. My own new blend – a breed of Sativa I'm calling Fragrans. The buds resemble strawberries and it smells less skunky and more fragrant.

Helps to hide the scent in summer on the mountainsides.

I will provide a sample. Thursday good for you? Maybe down near Ayrley?

GP

Sent from [Mail](#) for Windows 10

---

OK – I'll be there in 20 with a sample and the first shipment.  
You better have the cash or, Rett, I swear I will go Walter White on you.

Sent from [Mail](#) for Windows 10

---

From: [Rett Harring](#)  
Sent: Sunday, January 29, 2017 12:15 PM  
To: [Gene Poole](#)  
Subject: RE: Chemicals

Whoa – settle down.  
Cash for the white stuff, payment up front. Got it.

Your loss.

Sent from [Mail](#) for Windows 10

10. The last date and time the user was logged in was found by going into OS accounts in autopsy and finding the full name Gene Poole and his login date which is 2018-06-17 16:44:50 EDT

project1 - Autopsy 4.19.3

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Keyword Lists Keyword Search

Listing 15 Results

Table Thumbnail Summary

Save Table as CSV

Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time
S-1-5-80-956008885-3418522649-1831038044-185329			0		GP_2020....	Local		
S-1-5-18				systemprofile	GP_2020....	Local		
S-1-5-21-1058341133-2092417715-4019509128-1000			0	IEUser	GP_2020....	Local		2018-04-25 11:47:54 EDT
S-1-5-80-3028837079-3186095147-955107200-370196			0		GP_2020....	Local		
S-1-5-20				NetworkService	GP_2020....	Local		
S-1-5-19				LocalService	GP_2020....	Local		
S-1-5-21-1058341133-2092417715-4019509128-1006			0	Johnn	GP_2020....	Local		2020-01-26 13:10:56 EST
S-1-5-21-1058341133-2092417715-4019509128-1004			0		GP_2020....	Local		
S-1-5-21-1058341133-2092417715-4019509128-1003			0	sshd_server	GP_2020....	Local		2018-04-25 11:59:50 EDT
S-1-5-21-397955417-626881126-188441444-4882392			0		GP_2020....	Local		
S-1-5-21-1058341133-2092417715-4019509128-504			0	WDAGUtilityAccount	GP_2020....	Local		2018-04-25 11:47:57 EDT

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

**Basic Properties**

Login: IEUser  
 Full Name: Gene Poole  
 Address: S-1-5-21-1058341133-2092417715-4019509128-1000  
 Type:  
 Creation Date: 2018-04-25 11:47:54 EDT

**GP\_2020.E01\_1 Host Details**

Last Login: 2018-06-17 16:44:50 EDT  
 Login Count: 9  
 Description: IEUser  
 Email: gmo\_guy@outlook.com  
 Password Fail Date: 2018-06-17 16:31:25 EDT  
 Password Settings: Password does not expire  
 Flag: Normal user account  
 Home Directory: C:\Users\IEUser

**Data Sources**

- GP\_2020.E01\_1 Host
  - \$OrphanFiles (4367)
  - \$CarvedFiles (5124)
  - \$Extend (9)
  - \$Recycle.Bin (7)
  - \$halloc (18)
  - \$info (4)
  - Documents and Settings (2)
  - OneDriveTemp (3)
  - PerfLogs (2)
  - Program Files (24)
  - Program Files (x86) (20)
  - ProgramData (20)
  - Recovery (3)
  - System Volume Information (8)
  - EDP (3)
  - Users (10)
  - Windows (103)

**File Views**

- File Types
- Deleted Files
- MB File Size

**Data Artifacts**


- Communication Accounts (26)
  - Email (26)
- E-Mail Messages (436)
  - Default (Default)
  - Default (436)
- Installed Programs (37)
- Metadata (163)
- Operating System Information (2)
- Recent Documents (115)
- Recycle Bin (6)
- Run Programs (3430)
- Shell Process (7)

- The files placed in the recycle bin were identified by looking at the path to see which user had it and next to the path column it shows the date deleted for every file in the bin. This information was found in autopsy by going into the data artifacts tab.

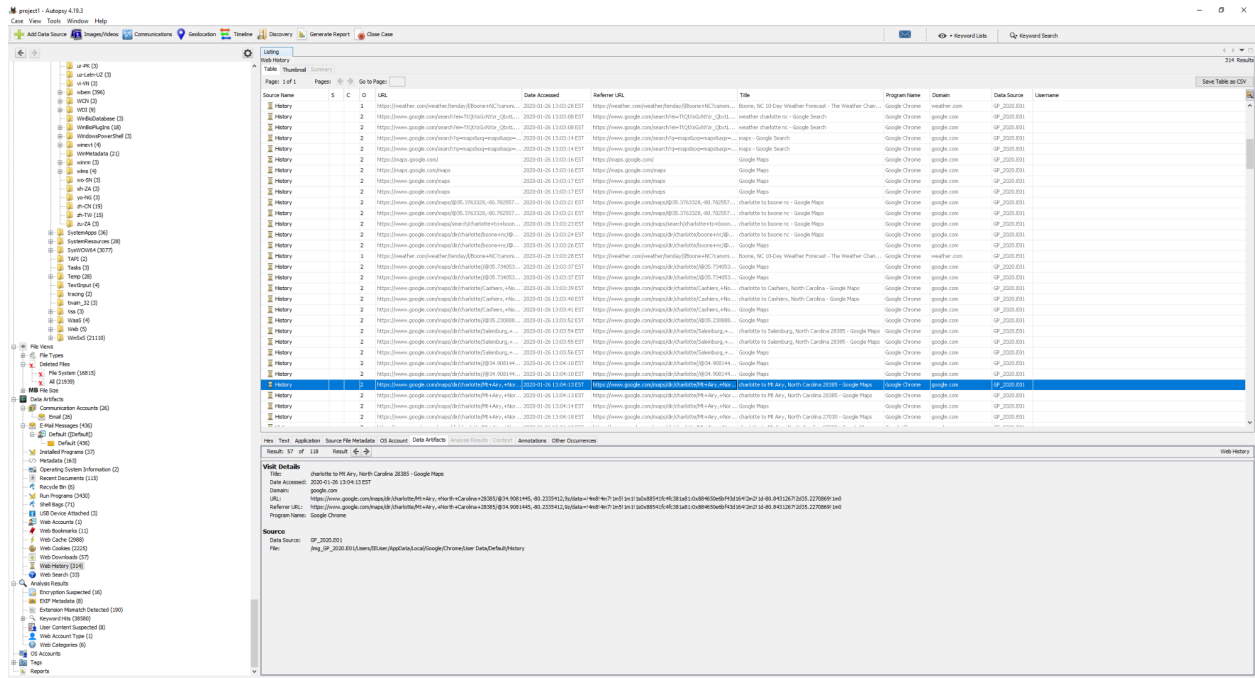
Listing						
Recycle Bin						
Table: Thumbs.db   Summary						
Pages: 1 of 1   Pages:   Go to Page:   Save Table						
Source Name	S	C	O	Path	Time Deleted	Username   Data Source
# RC97QF5.txt				C:\Users\ElUser\Desktop\TheMountains.txt	2018-09-03 09:36:49 EDT	GP_2020.E01
# #GLCXY3rk				C:\Users\ElUser\Desktop\panda3k	2019-06-19 21:41:23 EDT	GP_2020.E01
# #J3UQX3				C:\Users\ElUser\Desktop\ToDo	2018-09-03 09:37:34 EDT	GP_2020.E01
# #KQ52WE				C:\Users\ElUser\Desktop\FFS\FFS DOCS	2019-01-01 15:39:45 EST	GP_2020.E01
# #RTO3AU.adcf				C:\Users\ElUser\Desktop\HantooH32.E01.adcf	2019-01-01 17:47:00 EST	GP_2020.E01
# #RAOW12B.bmp				C:\Users\Johnn\Desktop\New Bitmap Image.bmp	2020-01-26 13:35:06 EST	GP_2020.E01

Hex	Text	Application	Source File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Result: 1 of 1   Result:									
Type				Value		Source(s)			
Path				C:\Users\ElUser\Desktop\TheMountains.txt		Recycle Bin			
Time Deleted				2018-09-03 09:36:49 EDT		Recycle Bin			
Username						Recycle Bin			
Source File Path				img_GP_2020.E01\Recycle.Bin\S-1-5-21-1058341133-2092417715-4019509128-1000\RC97QF5.txt					
Artifact ID				#223372036854775805					

12. The user's background was a blue and black panther and the file location was found under  
  
 /img\_GP\_2020.E01/Users/Public/AccountPictures/S-1-5-21-1058341133-2092417715-4019509128-1000





14. The pictures below are evidence that was found on the pc using autopsy the two pictures below were found in  
“img\_GP\_2020.E01/Users/IEUser/AppData/Roaming/Thunderbird/Profiles/9m7mu211.default-release/ImapMail/outlook.office365.com/Sent-1/= \_windows-1250\_Q\_800px-Uskla dn=ECn=E1=5Fmouka.JPG\_”, the rest of the pictures were found in  
/img\_GP\_2020.E01/Users/IEUser/Downloads.





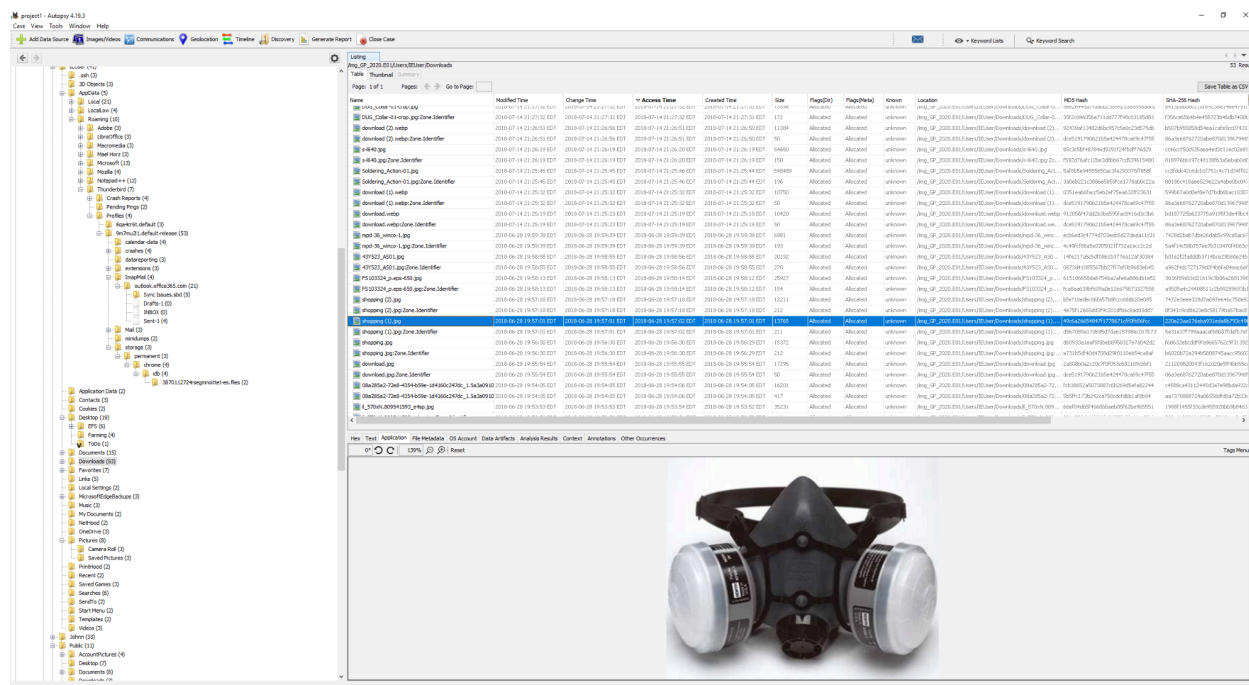
[Home](#)
[Text](#)
[Application](#)
[File Metadata](#)
[OS Account](#)
[Data Artifacts](#)
[Analysis Results](#)
[Content](#)
[Annotations](#)
[Other Occurrences](#)

**ALUMINUM SULFATE**  
**ETANAGARD GROUND**

CONTAINS 10% ALUMINUM SULFATE AND 90% SULFURIC ACID  
 100% WATER SOLUBLE

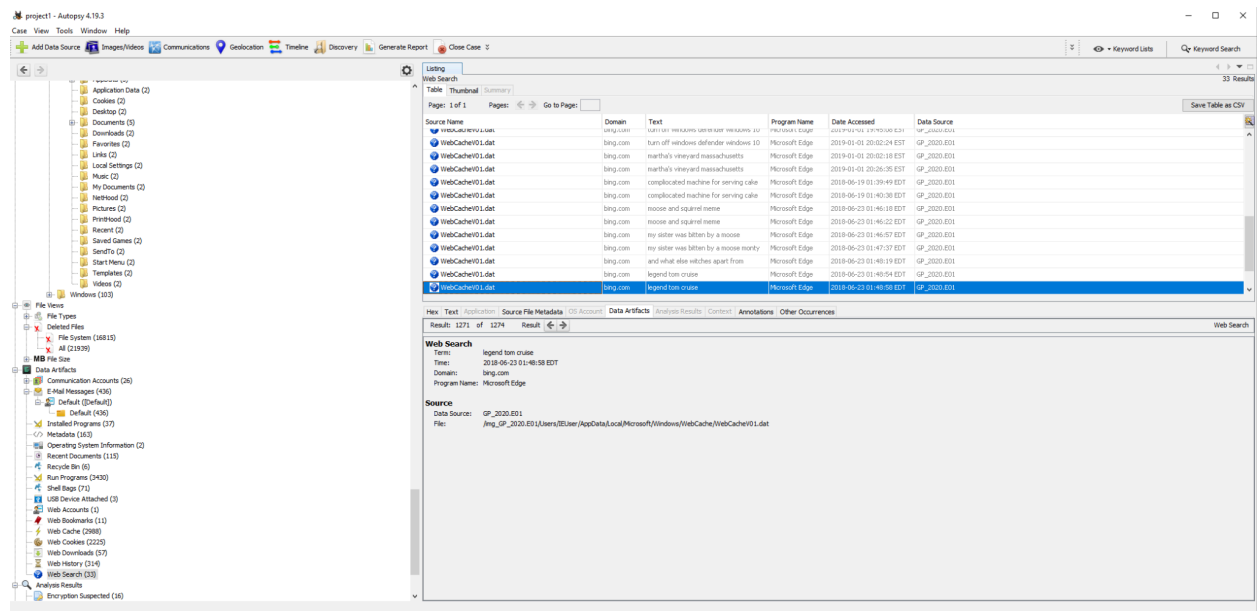
**INSTRUCTIONS:**  
 1. Apply 100 lbs. per acre for acid control and 50 lbs. per acre for aluminum.  
 2. Apply in the fall or early spring, before the plants start to grow.  
 3. Apply in the form of a broadcast or band application.  
 4. Do not apply to plants that are already growing.  
 5. Do not apply to plants that are already in flower.  
 6. Do not apply to plants that are already in fruit.  
 7. Do not apply to plants that are already in seed.

**NET WEIGHT 50 LBS. (22.7 kg)**



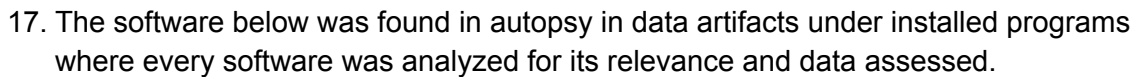
15. Identify programs used to download files from the internet.

Google Chrome and Microsoft Edge is the only program found on the image file that can download files from the internet. This was found using autopsy and by going into the installed programs section. Microsoft Edge was by going into the web search tab and looking into the data artifacts of the searches



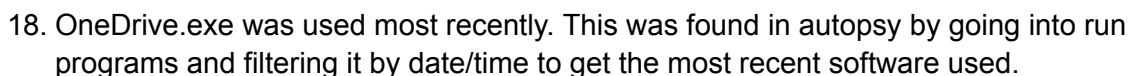
Path C:\Users\IEUser\Downloads\shopping(1).jpg

Path C:\Users\IEUser\Downloads\openssl-0.9.8h-1-setup.exe



AsccesData FTK Imager- 2020-01-26 13:45:19

OpenSSH for Windows- 2020-01-26 13:45:19





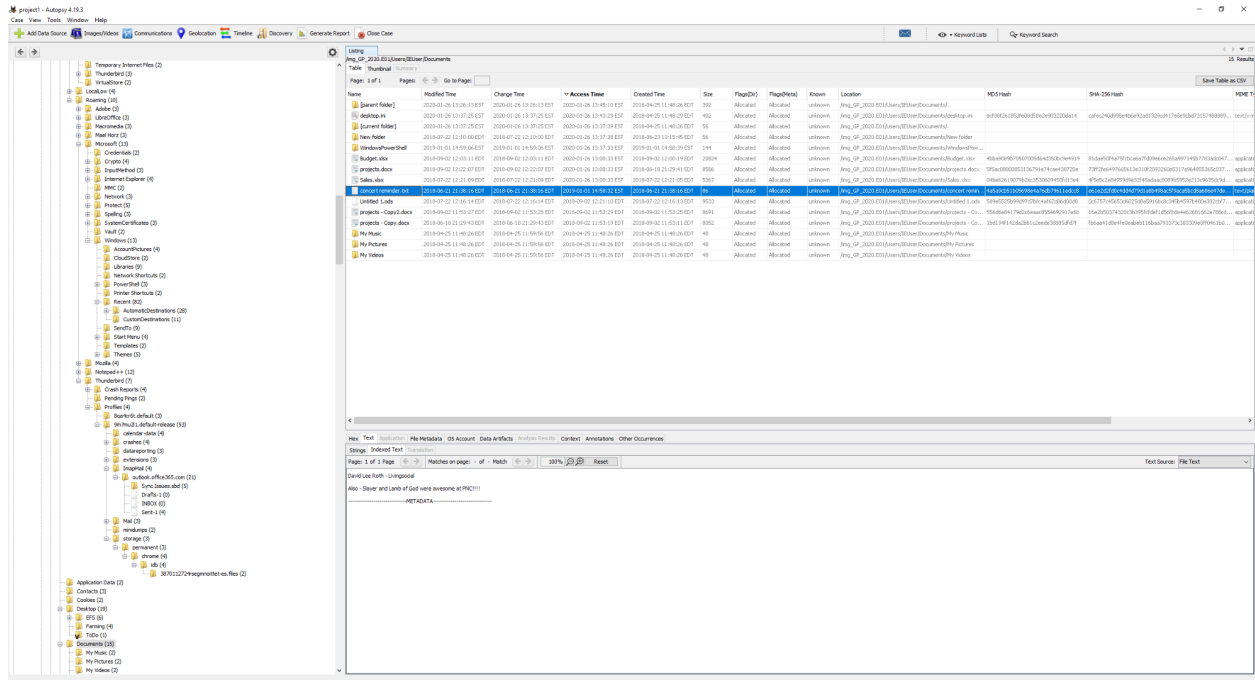
## 19. In the search for personal information a couple of files were found on the device

First 3 pics found under /img\_GP\_2020.E01/Users/IEUser/Documents

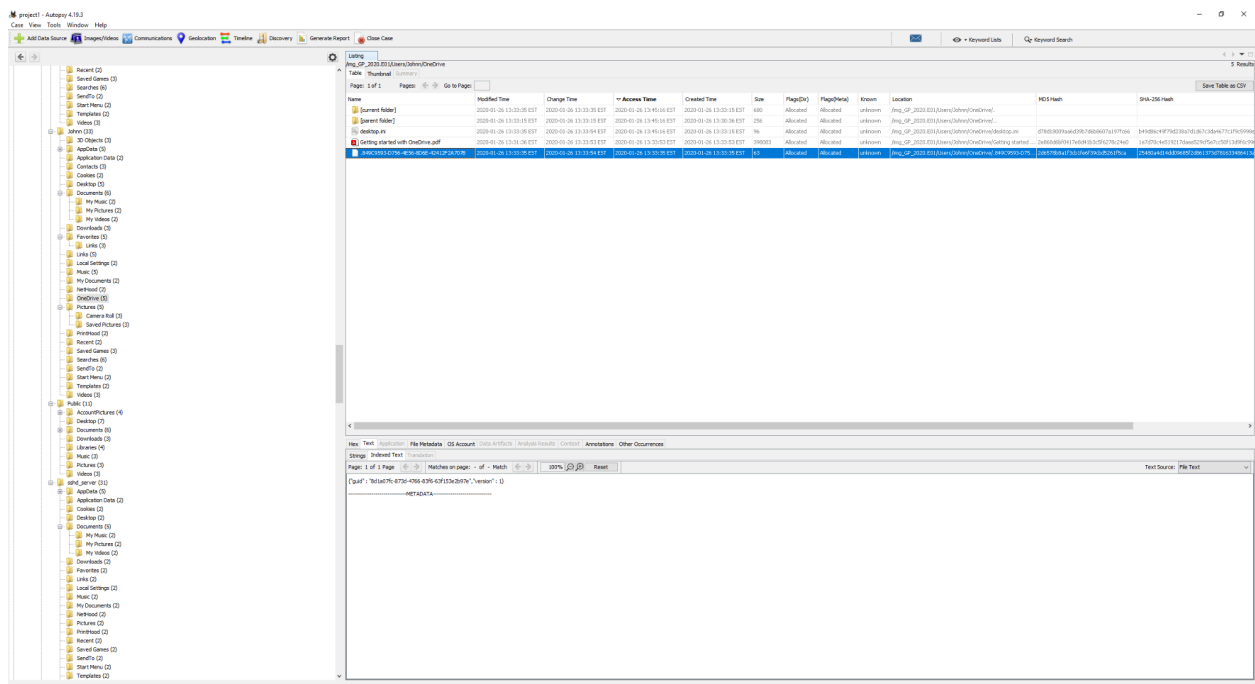
The screenshot displays a forensic analysis interface. On the left, a file tree shows the directory structure of the device, including folders like 'Applications', 'Documents', and 'Pictures'. The main pane shows a list of files found under the path '/img\_GP\_2020.E01/Users/IEUser/Documents'. The file 'Budget.xlsx' is highlighted. Below the file list, a detailed view of the selected file is shown, including its metadata and a preview of its contents. The preview shows a spreadsheet titled 'Gen's Personal Budget' with columns for 'Income', 'Expense', and 'Balance'. The spreadsheet data is as follows:

Category	Amount
Income	7200
Expense	1286
Balance	5914

The screenshot displays a forensic analysis interface, similar to the one above. It shows the same file list and the detailed view of the 'Budget.xlsx' file. The preview of the spreadsheet is identical to the one in the first screenshot. The interface also shows various toolbars and navigation options, including a search bar and a list of files found on the device.

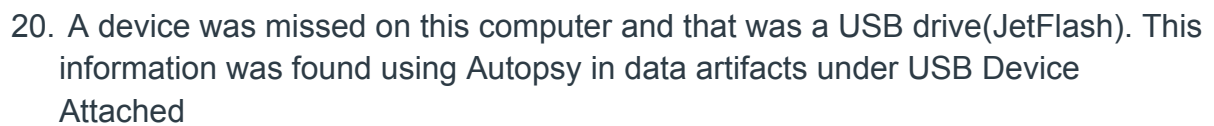


4th pic was found in /img\_GP\_2020.E01/Users/John/OneDrive

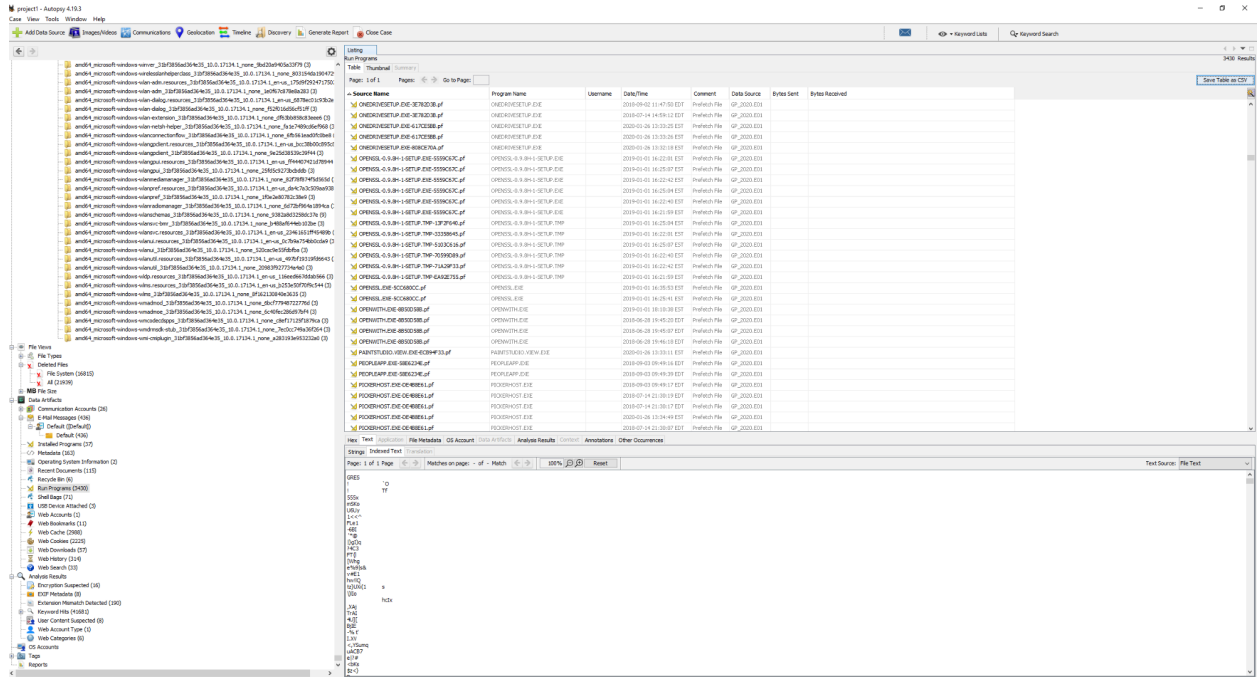


5th pic was found in  
/img\_GP\_2020.E01/Users/IEUser/Downloads/mimikatz\_trunk/x64/Crypto/57ab95eaae77d7c60d855c1f8d79bb26\_4a2bc28c-9cc0-47fe-9cb9-632ab751f45a





21. The 3 most often run programs are ondrive, chrome, and OpenSSL. This was found in autopsy in data artifacts under run programs and filtering by name to see which programs were shown the most.



22. The files that were recently worked on are Untitled. png, Music, New Bitmap Image, Microsoft account, and mimikatz\_trunk. This was found using autopsy in data artifacts under recent documents where it was organized by date accede to see the most recent ones.



[illegible][illegible]

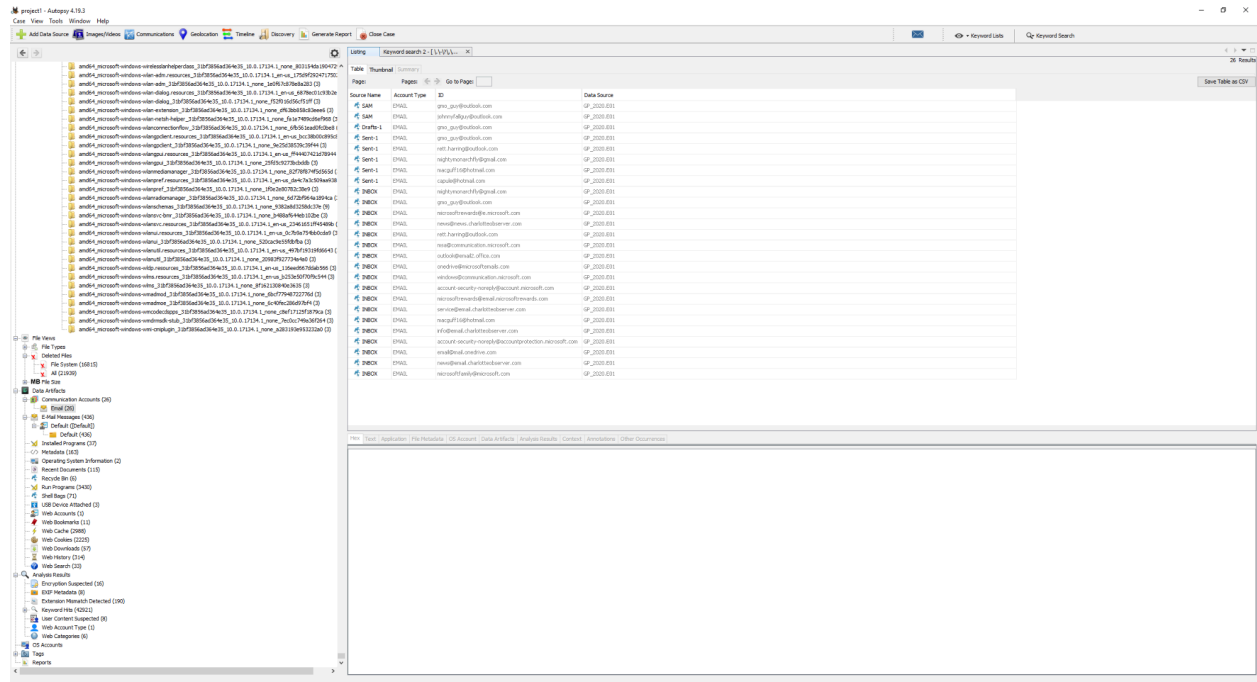
[illegible]



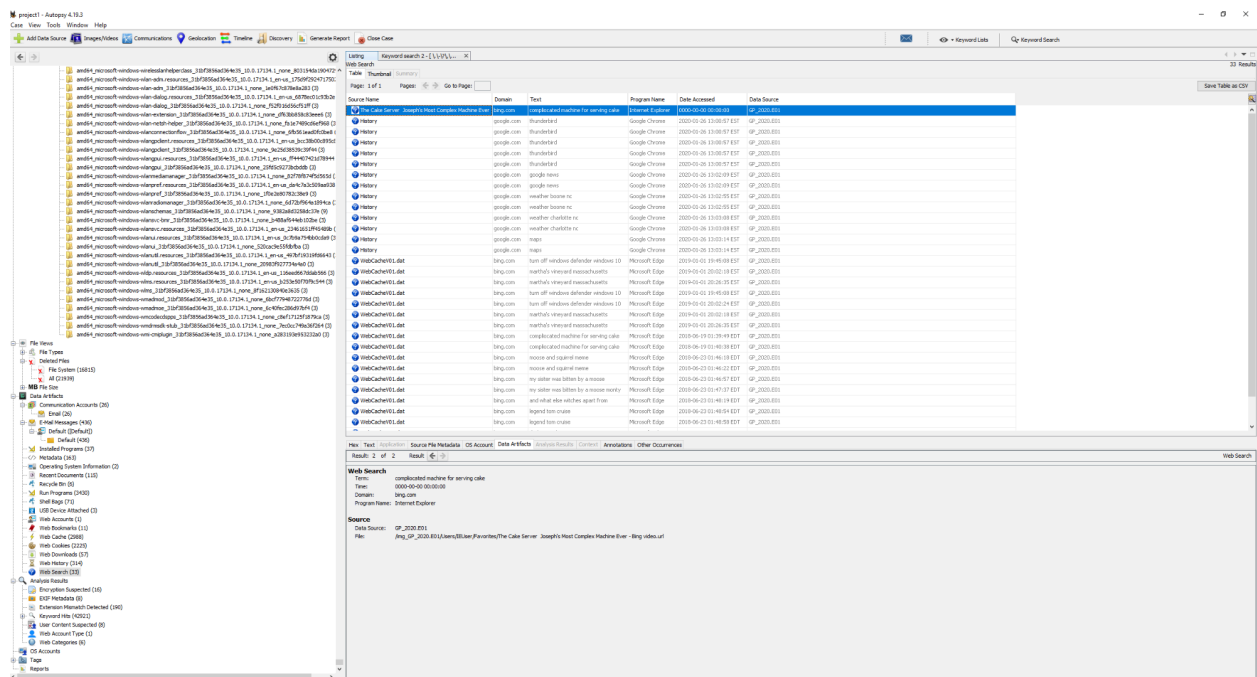
Autopsy 4.18.3 interface showing a file system tree on the left and a search results table on the right. The search results table contains columns for Name, Keyword Phrase, Location, Modified Time, Change Time, Access Time, Created Time, Size, PageID, Page/Total, Exam, and MD5 Hash. The table lists various files and folders, including system files like 'win32\_x86\_msvc' and 'win32\_x86\_msvc'.

25. The only email program that was found installed was Mozilla Thunderbird, this was found in autopsy in installed programs and researching if every program installed was email affiliated or not. A list of emails received from the user from multiple sources was found too under communication accounts.

Autopsy 4.18.3 interface showing a file system tree on the left and a search results table on the right. The search results table contains columns for Name, Keyword Phrase, Location, Modified Time, Change Time, Access Time, Created Time, Size, PageID, Page/Total, Exam, and MD5 Hash. The table lists various files and folders, including system files like 'win32\_x86\_msvc' and 'win32\_x86\_msvc'.



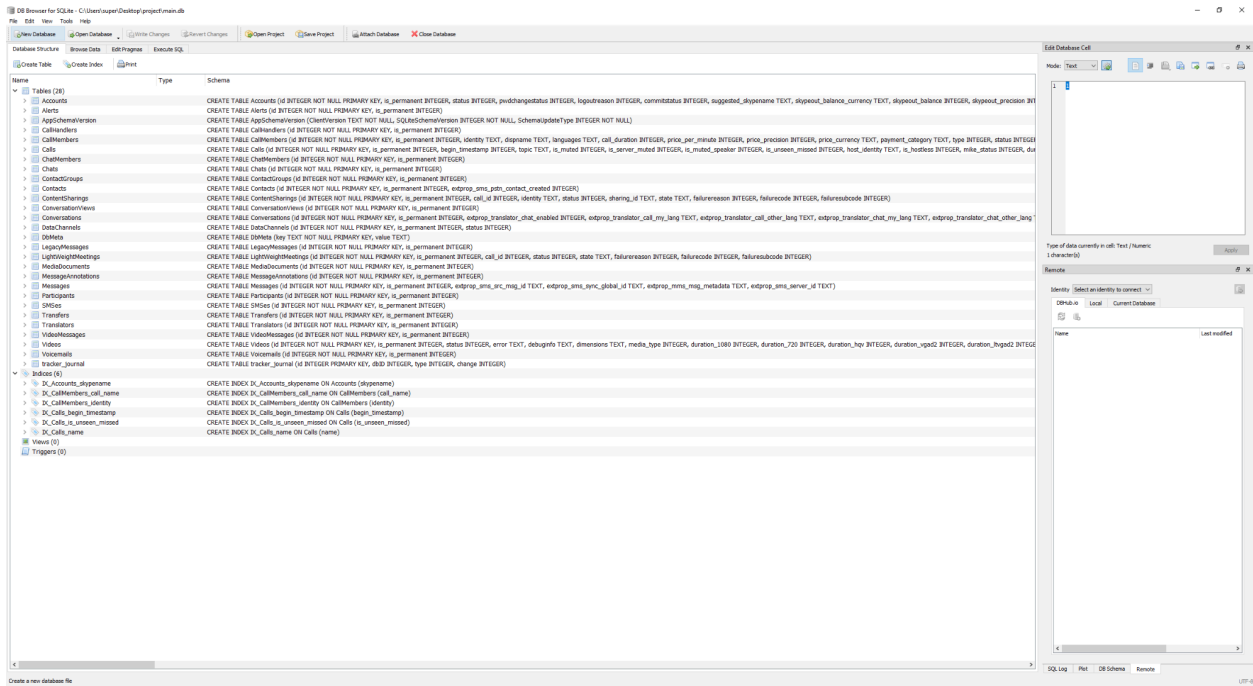
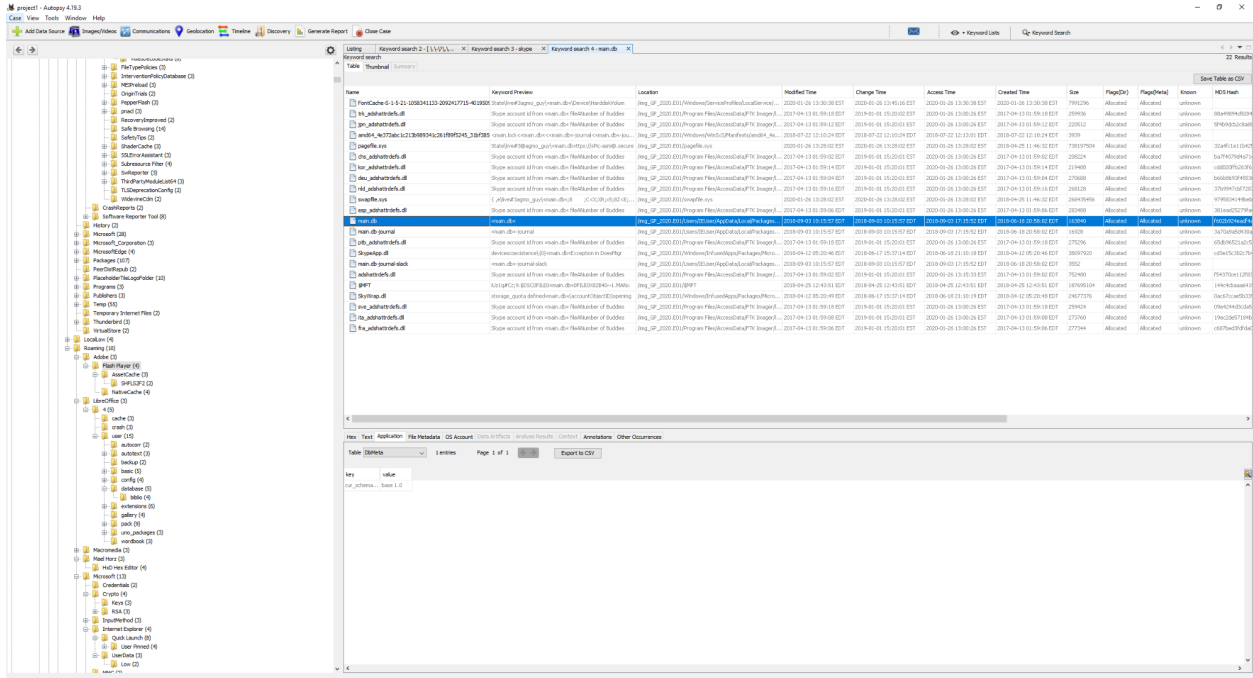
26. Internet Explorer, Microsoft Edge, and Google Chrome were the internet browsers identified. This was found in autopsy under data artifacts and web search. Each search history was looked into the data artifacts tab to see which program was used to search.



[illegible]

27. Using autopsy no skype chats have been identified. Main.DB of skype is empty.





28. A list of relevant results was picked based on Detective Fletcher's requirements using autopsy.

The screenshot displays the Autopsy 4.19.3 interface. On the left, a file system tree shows the structure of the analyzed image, including folders like RSA, InputMethod, Internet Explorer, Quick Launch, User Pinned, UserData, MMC, Network, Connections, Pbk, \_hiddenPbk, Protect, Spelling, SystemCertificates, Vault, Windows, AccountPictures, CloudStore, Libraries, Network Shortcuts, PowerShell, Printer Shortcuts, Recent, AutomaticDestinations, CustomDestinations, SendTo, Start Menu, Templates, Themes, Mozilla, Notepad++, backup, plugins, config, Hunspell, themes, Thunderbird, Crash Reports, Pending Pings, Profiles, 8qa4of6t.default, 9m7m2i1.default-release, calendar-data, crashes, datareporting, extensions, ImapMail, outlook.office365.com, Sync Issues.sbd, Drafts-1, INBOX, Sent-1, Mail, minidumps, storage, permanent, chrome, idb, 3870112724segmnoiltet-es.files, Application Data, Contacts, Cookies, Desktop, EFS, EFS DOCS, Farming, and ToDo.

On the right, the 'Keyword search 2' results are displayed in a table. The table has columns: Name, Modified Time, Change Time, Access Time, and Create Time. The results show a file named 'Shopping.txt' with a modified time of 2018-09-03 09:37:34 EDT, a change time of 2018-09-03 09:37:34 EDT, an access time of 2018-09-02 12:20:49 EDT, and a create time of 2018-09-02 12:20:49 EDT.

Result: 8 of 23   Result   ← →

E-Mail Messages

From: gmo\_guy@outlook.com  
To: rett.harring@outlook.com  
CC:  
Subject: RE: Yo Gene!

2018-09-02 12:08:47 EDT

Headers   Text   HTML   RTF   Attachments (0)   Accounts

Hide Images

Hey – I’ve been up in the mountains gathering plant samples and working at my hidden camp.

I have a project that’s about to pay off big and I’ll need to you to drive me.

Yes – Rufus and I spoke, he is pleased with the arrangement.

Sent from [Mail](#) for Windows 10

From: Rett Haring <rett.harring@outlook.com>  
Sent: Sunday, July 22, 2018 11:56:18 PM  
To: Gene Poole  
Subject: Re: Yo Gene!

Oops... I just saw this. Drove by your place a few times, where ya been?

From: rett.harring@outlook.com  
To: Rett.harring@outlook.com  
CC:  
Subject: Chemicals

2017-01-29 11:41:14 EST

Headers   Text   HTML   RTF   Attachments (0)   Accounts

Hide Images

I have some bulk chems if you are looking to sell or have a good time on your own.

Sodium Chloride  
Hydrogen Dioxide  
Disaccharides (I got the G made from the freshest S and F)  
Can also help you drop some Ascorbic Acid... trippy!

Your favorite Chemist,

Guy

Sent from [Mail](#) for Windows 10

[illegible]

Various sources of information have been found on the image files ranging from email messages, pictures, and suspicious encrypted files. My forensic examination of this device will come of use to Detective Fletcher in the incrimination of the suspect. Based on the information found the location of Eugene's friends has been documented in the forensic examination and will require the immediate action of the UNCC Police Department to catch Rett. Hidden pictures of the ingredients used to make their drugs and their pictures can be used as further proof to incriminate Eugene.

## 2nd Verification

Drive Image Verify Results	
01	
Name	GP_2023.001
Sector count	6299584
02 MD5 Hash	
Compared hash	8956c754a45424911b1a1a0b7714b2688
Stored verification hash	8956c754a45424911b1a1a0b7714b2688
Verify result	Match
03 SHA1 Hash	
Compared hash	a59423a177a1d389b497b1443a129a613a47a77b
Stored verification hash	a59423a177a1d389b497b1443a129a613a47a77b
Verify result	Match
04 Bad Blocks (if)	
Bad block(s) in image	No bad blocks found in image

