

Ethan Kalika  
ITIS 4250 / 5250  
April 28, 2023

### **Overview:**

Dr. Quincy has given me the responsibility of handling Detective Jessica Fletcher's final case. In this case, a forensic investigation of Gene Poole's most recent PC will be carried out utilizing a KAPE capture. The order issued to Detective Fletcher permits the examination of any suspected online criminal activity, including the manufacturing of drugs and chemical weapons as well as theft and ecoterrorism. Gene Poole is familiar with several anti-forensic methods and could have tried to destroy evidence. I've been given an EnCase E01 file from Gene's PC by the lab to examine.

### **Forensic Acquisition & Exam Preparation**

In the beginning, I downloaded GP2022.e01 from the Canvas website and checked it using FTK Imager. The picture was then opened with Arsenal image Mounter, and Autopsy was instructed to access the g file inside the mounted image.

Name	GP2022.E01
Sector count	174557184
<input checked="" type="checkbox"/> MD5 Hash	
Computed hash	fb614cb8a0b87ca6ae4365061cf39a22
Stored verification hash	fb614cb8a0b87ca6ae4365061cf39a22
Report Hash	fb614cb8a0b87ca6ae4365061cf39a22
Verify result	Match
<input checked="" type="checkbox"/> SHA1 Hash	
Computed hash	bb73ecabc7a988063484775dc3005e1e5cd40
Stored verification hash	bb73ecabc7a988063484775dc3005e1e5cd40
Report Hash	bb73ecabc7a988063484775dc3005e1e5cd40
Verify result	Match
<input checked="" type="checkbox"/> Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

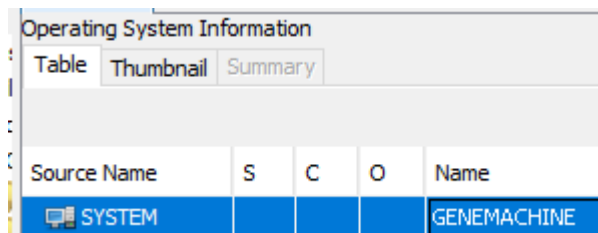
-FTK Imager version: 4.7.1.2  
-Autopsy version: 4.19.3  
-Arsenal Image Mounter version: 3.6.188  
-Registry Explorer: 2.0.0.0  
-HxD: 2.5.0.0  
-Notepad++: v8.4.5  
-Microsoft Photos: 2023.11030.27009.0

-Dell computer with 16.0 GB of RAM, Windows 11 version, and 64-bit operating system

### Findings and Report (Forensic Analysis)

**a. Gene denies the computer is his. What was the name of the computer?**

I learned the computer's name is GENEMACHINE by looking at the operating system information revealed by Autopsy.

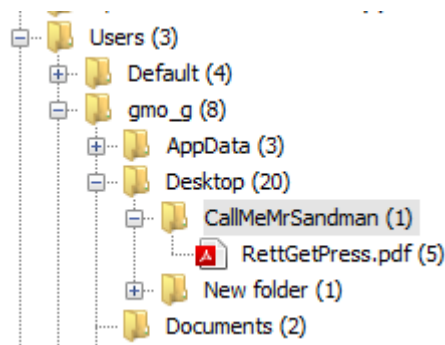


Operating System Information				
Table Thumbnail Summary				
Source Name	S	C	O	Name
SYSTEM				GENEMACHINE

**b. Rett Harring admitted during an interview with Bladen County Sheriff's Department Detectives that he picked up a pill press on a trip for Gene down to Dublin, NC, but denied delivering several crates of genetically modified peanuts to Houston's Peanuts in Dublin. The diligent workers as Houston's thought something was weird about the delivery and called the Sheriff's Department. Is there any evidence Gene knew Rett would travel to Dublin from his home in Salemburg, NC?**

There is a PDF file on this computer called "RettGetPress" that shows a Google Maps path from Salemburg, North Carolina to Dublin. The file may be found by checking the metadata details identified by Autopsy or by going to the desktop's "CallMeMrSandman" directory.

#### Pdf location:



#### Inside the Pdf:

8/14/22, 2:03 PM

salemburg nc to Houston' Peanuts - Google Maps

Google Maps

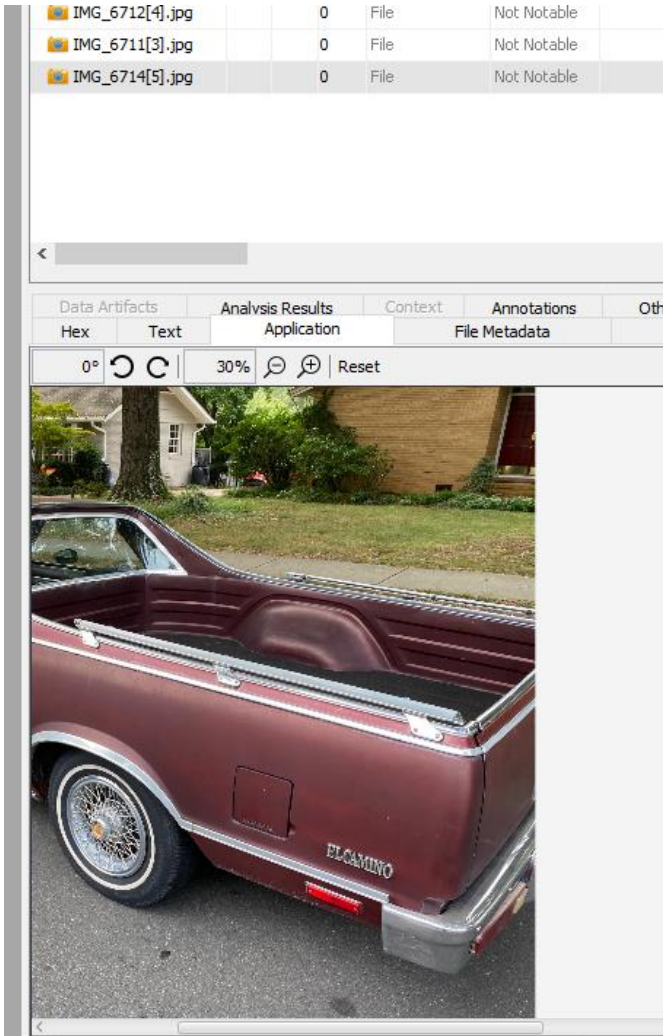
Salemburg, North Carolina 28385 to Houston' Peanuts, 7329 Albert St, Dublin, NC 28332

Drive 37.3 miles, 46 min



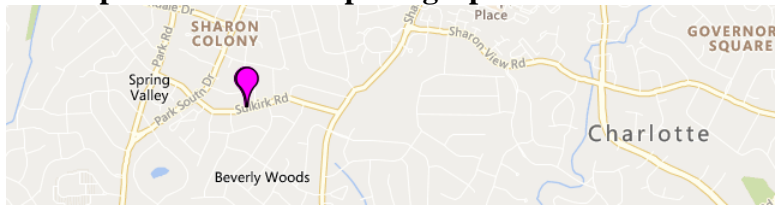
- c. The employees at Houston's told Sheriff's Deputies that Rett arrived in an old red truck. Rett asked for a lawyer prior to detectives asking him about his vehicle in use that day. Can you find any evidence on Gene's computer about the truck Rett might have used? We know the two were in frequent communication and have an informant who said Rett likes to brag to Gene about any crimes he commits or is thinking about.

The computer has images of a vintage red El Camino vehicle, which may be viewed in Autopsy's Exif information section.



- d. The truck may have been stolen as Rett often steals vehicles for use in his criminal activity. If you found a possible match, can you determine where the vehicle may have come from?

The historical red El Camino vehicle seen in the pictures was found to have its origins in the Spring Valley area of Charlotte according to Autopsy's geolocation tool. Purple pins on the map show where the photographs were taken.



- e. Are there any photos of military rockets on his computer apart from web browser cache? If so, where. If not, where might they have been saved?

Images of a Javelin 3 rocket and a Stinger FIM-92 missile on the computer were hidden by console instructions. However, it is clear that these pictures do in fact exist by looking at the console command history. The Roaming folder contains the console command history, which may be retrieved via Autopsy.

Name	S	C	O	Modified Time	Change Time
ConsoleHost_history.txt			0	0000-00-00 00:00:00	0000-00-00 00:00:00

Strings Indexed Text Translation

Page: 1 of 1 Page Matches on page: - of - Match

100% Reset Text Source: File Text

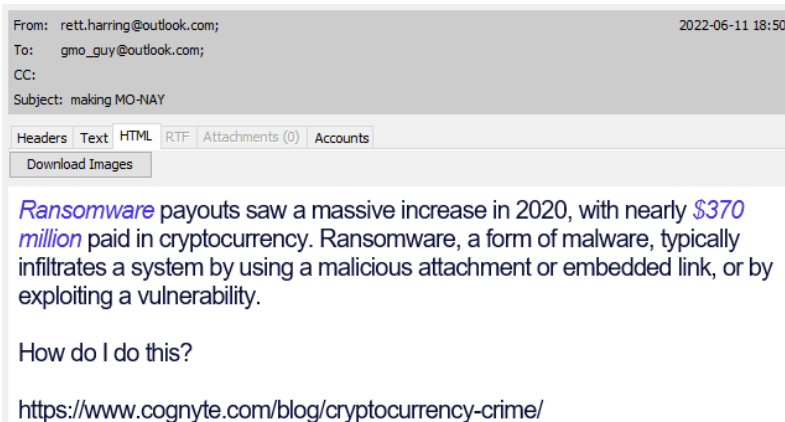
```
cd ..
cd ...
cd desktop
js
ls
cd ..gmo_g\
cd ..Desktop\
ls
Set-Content .\NothingToSeehere.txt $hidehole -value E:\T34_Callope_M4_2.jpg
Set-Content .\NothingToSeehere.txt $hidehole2 -value E:\Javelin_3.jpg
Set-Content .\NothingToSeehere.txt $hidehole3 -value E:\86399_stingerfim92usindopacom_121330.jpg
```

-----METADATA-----

- f. Has Gene discussed malware with anyone?

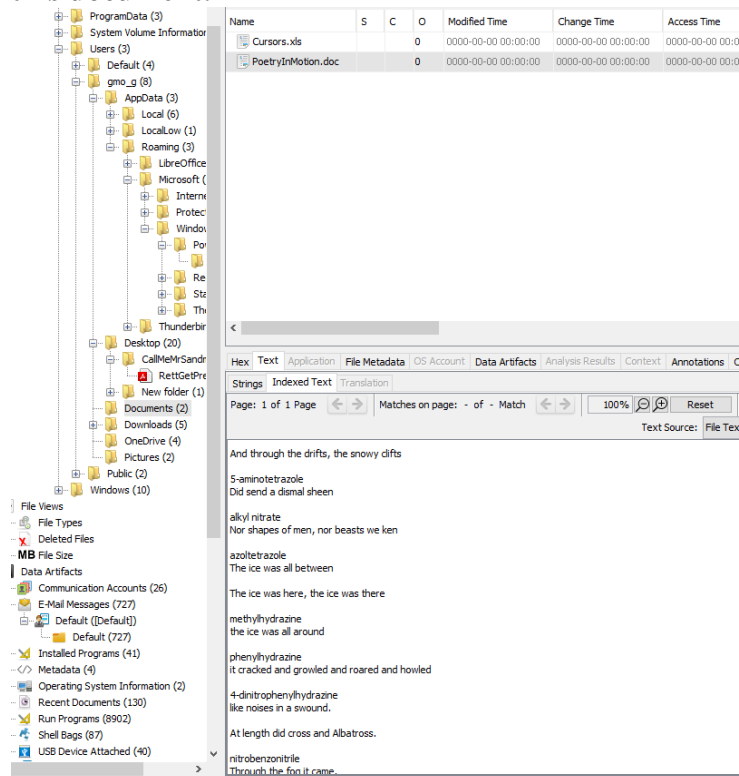


Using Autopsy, a recovered email from Rett Harring describes ransomware and how it cost businesses close to 370 million dollars in damages in 2020. Rett asks Gene how to execute this kind of assault in the email.



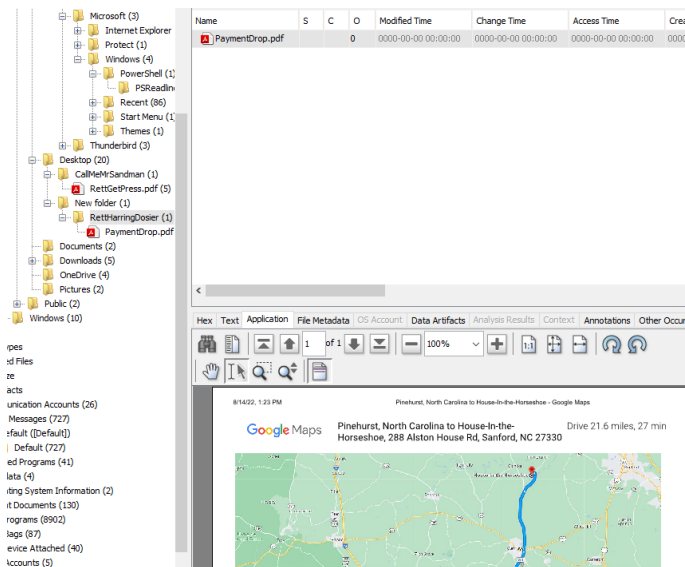
**g. Are there any hidden lists of chemicals you can find? Gene is known to hide his shopping lists after his first bust.**

The computer has a list of substances in a document called "PoetryInMotion". Either using Autopsy's Metadata tab or by going to the computer's Documents folder, you can access this document.



**h. Where was Gene going to drop the payment to Rett?**

Metadata found during autopsy revealed that Gene had intended to deliver a payment to the House in the Horseshoe location. A PDF file called "PaymentDrop," which is housed in the RettHarringDosier folder, may be opened to verify this information.



**i. Gene denies obstructing justice. Does he have any anti-forensics tools installed?**

Eraser and CCleaner are two applications that Gene has set up on his computer. Both of these programs are made to remove evidence of computer usage, making it challenging to recover files and determine what files were present on the system. By looking at the installed programs page, which provides a list of every application installed on Gene's computer, Autopsy has discovered these apps.

Source Name	S	C	O	Program Name
SOFTWARE			0	Eraser 6.2.0.2993 v.6.2.2993
SOFTWARE			0	DB Browser for SQLite v.3.12.2
SOFTWARE			0	CCleaner v.6.03

**j. Has Gene run any anti-forensics programs?**

As can be seen in the "Run Programs" portion of Autopsy's analysis, Gene Poole ran both CCleaner and Eraser on his computer.

Run Programs							8902 Res
Table Thumbnail Summary							
							Save Table as CSV
Source Name	S	C	O	Program Name	Username	Date/Time	
SRUDB.dat				\Program Files\CCleaner\CCleaner64.exe	gmo_g	2022-09-18 08:11	
SRUDB.dat				\Program Files\CCleaner\CCleaner64.exe	gmo_g	2022-09-18 09:11	
SRUDB.dat				\Program Files\CCleaner\CCleaner64.exe	gmo_g	2022-09-18 10:11	
SRUDB.dat				\Program Files\CCleaner\CCleaner64.exe	gmo_g	2022-09-18 11:11	
SRUDB.dat				\Program Files\DB Browser for SQLite\DB Browser for SQLite...	gmo_g	2022-09-15 16:05	
SRUDB.dat				\Program Files\DB Browser for SQLite\DB Browser for SQLite...	gmo_g	2022-09-15 17:05	
SRUDB.dat				\Program Files\DB Browser for SQLite\DB Browser for SQLite...	gmo_g	2022-09-15 16:05	
SRUDB.dat				\Program Files\DB Browser for SQLite\DB Browser for SQLite...	gmo_g	2022-09-15 17:05	
SRUDB.dat				\Program Files\Eraser\Eraser.exe	gmo_g	2022-09-15 16:05	
SRUDB.dat				\Program Files\Eraser\Eraser.exe	gmo_g	2022-09-15 17:05	
SRUDB.dat				\Program Files\Eraser\Eraser.exe	gmo_g	2022-09-15 18:05	
SRUDB.dat				\Program Files\Eraser\Eraser.exe	gmo_g	2022-09-15 19:05	
SRUDB.dat				\Program Files\Eraser\Eraser.exe	gmo_g	2022-09-15 20:05	
SRUDB.dat				\Program Files\Eraser\Eraser.exe	gmo_g	2022-09-15 21:05	
SRUDB.dat				\Program Files\Eraser\Eraser.exe	gmo_g	2022-09-15 22:05	

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

Result: 8166 of 8172    Result    < >    Run Program

Type	Value	Source(s)
Program Name	\Program Files\CCleaner\CCleaner64.exe	System Resources
Username	gmo_g	System Resources
Date/Time	2022-09-18 11:17:00 EDT	System Resources
Comment	System Resource Usage - Application Usage	System Resources
Source File Path	/LogicalFileSet1/G/Windows/System32/SRU/SRUDB.dat	
Artifact ID	-9223372036854744762	

**k. Has Gene instructed anyone else how to do this?**

**According to the emails that Autopsy was able to obtain, Gene helped Rett clean up his computer by using Ccleaner and Eraser.**

com;	gmo_guy@outlook.com;	Re: Get rid of internet junk	2022-06-11 18:45:44 EDT	Oh that's
com;	gmo_guy@outlook.com;	Re: Last email didn't get through	2018-09-02 12:18:28 EDT	Yeah, m
com;	gmo_guy@outlook.com;	Re: Last email didn't get through	2022-05-14 16:30:58 EDT	Hey man
com;	gmo_guy@outlook.com;	Re: Yo Gene!	2018-09-02 12:11:09 EDT	Interesti
com;	gmo_guy@outlook.com;	Re: Yo Gene!	2018-07-22 11:56:18 EDT	Oops... :
n;	gmo_guy@outlook.com;	Re: self email check	2022-05-14 16:49:08 EDT	Trying o
microsoft.com;	gmo_guy@outlook.com;	Ready for bonus points, Gene?	2019-02-19 07:58:28 EST	<head>
observer.com;	gmo_guy@outlook.com;	Register for our virtual ancestry event + Wells Fargo 401(...	2022-02-23 16:53:02 EST	The Cha
observer.com;	gmo_guy@outlook.com;	Remembering CMS principal who died + Today's developme...	2021-09-23 16:51:53 EDT	The Cha
observer.com;	gmo_guy@outlook.com;	Renovations are underway at Bank of America Stadium. He...	2020-01-24 16:07:54 EST	The Cha
observer.com;	gmo_guy@outlook.com;	Report of sexual assault at Butler High School + 70 Charlot...	2021-12-17 16:52:11 EST	The Cha

Hex

Text

Application

Source File Metadata

OS Account

Data Artifacts

Analysis Results

Context

Annotations

Other Occurrences

Result: 726 of 750

Result

←

→

E-Mail Message

From: rett.harring@outlook.com;

To: gmo\_guy@outlook.com;

CC:

Subject: Re: Get rid of internet junk

2022-06-11 18:45:44 ET

Headers

Text

HTML

RTF

Attachments (1)

Accounts

Download Images

Oh that's neat. Hey I heard about people doing science stuff to get things from my computer I deleted. Can this do that?

---

**From:** Gene Poole <gmo\_guy@outlook.com>  
**Sent:** Saturday, May 14, 2022 11:07 AM  
**To:** Rett.harring@outlook.com <Rett.harring@outlook.com>  
**Subject:** Get rid of internet junk

You can download this tool and get rid of all this stuff left over in your browser.

- Gene denies having used specific chemicals obtained from Dow, but admits he may have casually browsed their website. Is there anything more than browser history to suggest he might have saved information from Dow or intended to revisit their site later?**

**Upon autopsy, it was discovered that Gene had marked a bookmark to the Dow website as "chems". The text of the bookmark supports this categorization, and it may be accessed**



under the Web Bookmarks tab.

New folder (1)  
Documents  
Downloads  
OneDrive  
Pictures (1)  
Public (2)  
Windows (10)

File Views  
File Types  
Deleted Files  
File Size  
Data Artifacts  
Communication Accounts (26)  
E-Mail Messages (727)  
Default (Default)  
Default (727)  
Installed Programs (41)  
Metadata (4)  
Operating System Information  
Recent Documents (130)  
Run Programs (8902)  
Shell Bags (87)  
USB Device Attached (40)  
Web Accounts (5)  
Web Bookmarks (3)  
Web Cache (9923)  
Web Cookies (1354)  
Web Downloads (47)  
Web Form Addresses (2)  
Web Form Autofill (9)  
Web History (493)  
Web Search (235)  
Analysis Results  
Encryption Suspected (1)  
EXIF Metadata (7)  
Extension Mismatch Detected  
Keyword Hits (3346)  
User Content Suspected (7)  
Web Account Type (2)  
Web Categories (7)  
Accounts  
Logs  
Sports

Source Name	S	C	O	URL	Title
Bookmarks					chems
Bookmarks					chems
Bookmarks			1	https://act.audubon.org/a/donate-monthly-search?ms=dig... Donate Now to Protect Birds   National	

HexTextApplicationSource File MetadataOS AccountData ArtifactsAnalysis ResultsContextAnnotationsOther Occurrences

StringsIndexed TextTranslation

Page: 1 of 1 PageMatches on page: - of - Match100%Reset

Text Source:File Text

```
{
  "checksum": "6f74e39580a839fc76450a63c6fb35c1",
  "roots": {
    "bookmark_bar": {
      "children": [ {
        "children": [ {
          "date_added": "13299461899988571",
          "guid": "d8cf81e7-921d-403e-b523-2aa77c8620a3",
          "id": "10",
          "name": "ACOUSTICRYLTM AV-2240 Emulsion",
          "show_icon": false,
          "source": "import_continuous_from_chrome",
          "type": "url",
          "url": "https://www.dow.com/en-us/pdp/acousticryl-av-2240-emulsion.245628z.html?productCatalogFlag=1#overview"
        } ],
        "date_added": "13299462744100635",
        "date_modified": "0",
        "guid": "087f4d23-b3bf-4709-86ca-0dc95c27e454",
        "id": "9",
        "name": "chems",
        "source": "import_continuous_from_chrome",
        "type": "folder"
      } ],
      "date_added": "13297011471088112",
      "date_modified": "0",
      "guid": "1bdc5d13f2c8a-5d74-951f-3f233f6c908"
    }
  }
}
```

m. How many external storage devices were connected to the computer?

Two external storage devices were attached to Gene's PC, according to the autopsy. It was discovered that only two devices were storage devices by looking at the "USB Device Attached" page , one of which was a flash drive and the other a portable storage device.

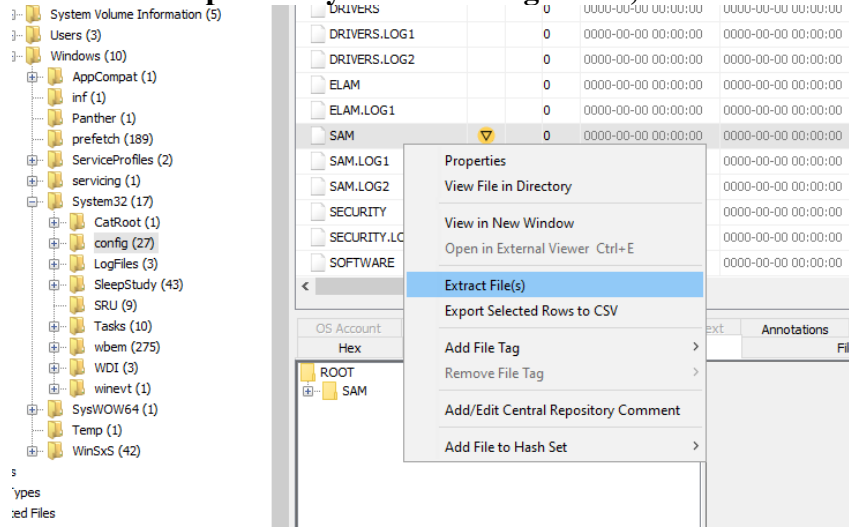
Type	Value
Date/Time	2022-09-10 14:06:24 EDT
Device Make	Silicon Motion, Inc. - Taiwan (formerly Feiya Technology Corp.)
Device Model	Flash Drive
Device ID	030380000001163
Source File Pat	/LogicalFileSet1/G/Windows/System32/config/SYSTEM
Artifact ID	-9223372036854775574

Result: 40 of 246Result

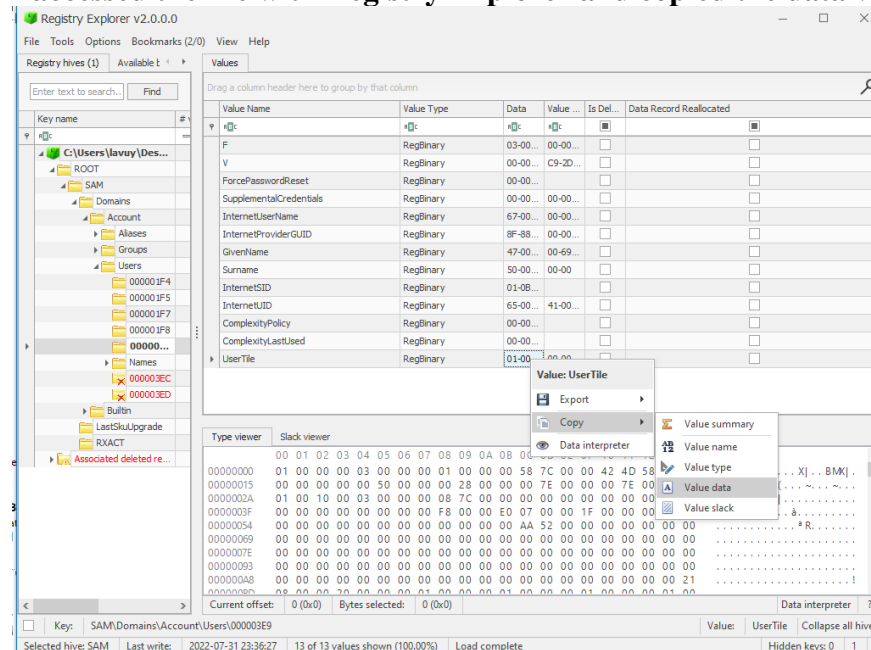
Type	Value	Source(s)
Date/Time	2022-07-31 19:22:00 EDT	Recent Activity
Device Make	Dell Computer Corp.	Recent Activity
Device Model	Portable Device	Recent Activity
Device ID	MSFT30NZ053FCS	Recent Activity
Source File Pat	/LogicalFileSet1/G/Windows/System32/config/SYSTEM	
Artifact ID	-9223372036854775550	

## n. Can you recover the user tile for the main user?

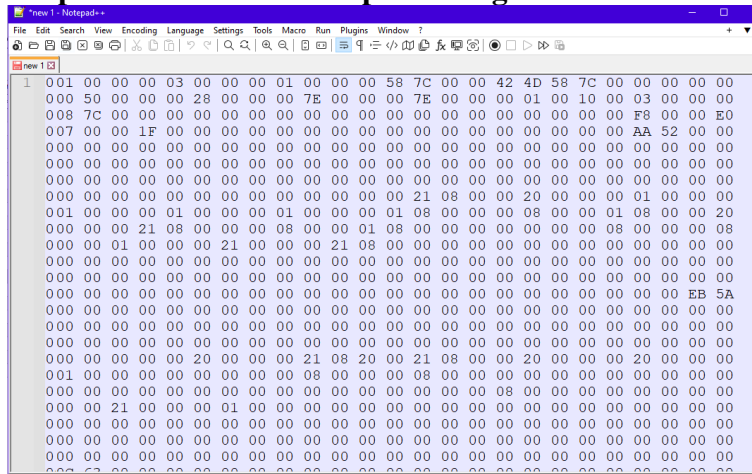
Yes, however the procedure was a little complicated. I started by locating the SAM registry file in the computer's System32/Config folder, which is where user tiles are kept.



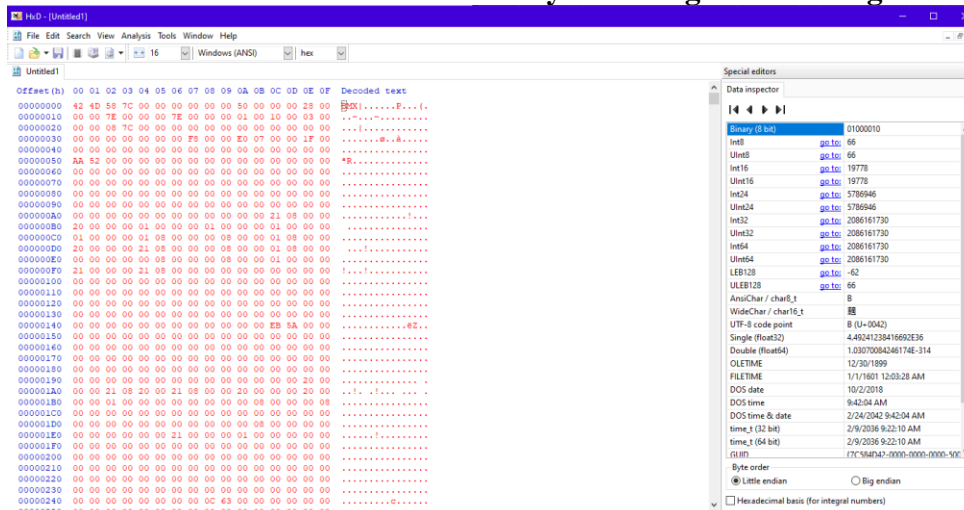
I accessed the file with Registry Explorer and copied the data values related to the user tile.



I copied the info into Notepad++ to get rid of the dashes that were there.



**Since the file needed to begin with 42 4D and the top line contained extra information, the data was edited in the hex editor HxD by removing it and saving it as a BMP file type.**



**The user tile was retrieved and viewed in Windows Photo Viewer as seen below:**



**Conclusion:**

I mounted the downloaded picture with Arsenal picture Mounter after using FTK Imager to verify its hash. The majority of the computer's information was then obtained by directing Autopsy to the g folder in the mounted image. This information includes the owner, proof that Gene was aware of Rett's travel, specifics about Rett's old red truck, the potential location of the truck's theft, the location of secret military rocket photos, information about the malware discussed between Gene and Rett, specifics about the chemicals Gene listed, the location of Rett's payment drop-off, specifics about the anti-forensic tools on the computer, the anti-forensic actions taken, specifics about Gene's email to Rett on anti-forensic tools, Gene's bookmarks to the Dow website, and the external storage devices attached to the computer. Lastly, I was able to find the user tile of the main user using Autopsy and a few other programs.