**ITIS 4250/5250**

**Lab #5**

**Pooja Haridasyam**

**Overview:**

Detective Jessica Fletcher made a request on October 30th, 2022, for a desktop computer to be processed. She had a Search Warrant from the North Carolina District Court and brought along Gene Poole's computer. I was tasked with analyzing the forensic image of the computer. Gene Poole, who has a criminal record, is known for being involved in the production and distribution of illegal drugs. He also uses anti-forensic technology.

**Forensic Acquisition and Exam Preparation:**

Open AccessDataFTKImager and load the image named Gene2021.E01, then proceed to verify it.

Graphical user interface, text, application

Description automatically generated

*Figure: Verified Hash values*

Verified Hash value: 75b28a2dd3d0c58fd1b944d1707cba1a

Mount the image file onto Arsenal Image Mounter v3.9.228:

Graphical user interface, application

Description automatically generated

**Software used for examination of the task :**

1. AccessData FTK Imager 4.7.12

2. Dell Latitude 3510 with Windows 11 Operating System, 16GB RAM

3. Autopsy - 64-bit 4.20.0

4. Arsenal Image Mounter v3.9.228

5. Win Prefetch viewer x64

**Forensic Analysis:**

Launch Autopsy and initiate a new case, followed by selecting Gene2021.E01 file as the data source to be included.

Graphical user interface, application

Description automatically generated

Graphical user interface, application

Description automatically generated

Graphical user interface

Description automatically generated

Graphical user interface, application

Description automatically generated

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Using the above tools Autopsy and Registry explorer we can find answers to the following questions and perform the analysis:

1. Gene denies the computer is his. Who was the Owner and the Organization to whom it was registered?

The registry entry contained details regarding multiple users, including Gene Polle who possessed an administrative account. Information pertaining to GenePole's account creation date, total number of logins, and most recent login time is accessible. Based on the latest login time, it appears that the account was last used on June 17, 2018. Subsequently, a different account was established, followed by another one named John, which is currently in use. Given that an account was created using Gene's name, it's plausible that Gene is the lawful owner of the system. However, John's account is the one that is currently active.

Text, table

Description automatically generated with medium confidence

Graphical user interface, text, application

Description automatically generated

*Figure: Registered Owner details*

The Registered Owner Details: Eugene Poole

Organization: The Guild of Calamitous Intent

1. We believe the location of his mountain hideout might been in a text file. Can you tell us anything about that?

The recycle bin contained a file named "TheMountain.txt" which had the same text as the image displayed below.

Graphical user interface, application

Description automatically generated

It says “Remember to take a new mosquito net.”

1. We found a flash drive we believe may have been used with Gene's computer, but it was at the home of his associate. Can you determine what thumb drives may have been attached to Gene's computer to help us get new legal authority?

In the section titled "USB Devices Attached" under "Data Artifacts," we notice a flash drive labeled Transcend Jet connected to Gene's computer. We can also see other devices with the names ROOT\_HUB and ROOT\_HUB20.

Graphical user interface, application

Description automatically generated

*Figure: Three devices are informed about thumb drives.*

1. Was he using an office program to make documents? We think some files we got from our informant may have been created by Gene. Any idea how often he used the software?

We must navigate to root->F- >Windows>Prefetch, right-click, and extract files to get the data. Go to WinPrefetchView now, then pick the Options tab, Advanced Options, and then choose the extracted files you saved to the exports folder.

Graphical user interface, text, application

Description automatically generated

Graphical user interface, application, table

Description automatically generated

Graphical user interface, text, application, Excel

Description automatically generated

In the Run Counter column, we can see that SOFFICE.BIN-f133562F.pf was executed 8 times in total.

1. Gene may have had an interest in Cybersecurity and "hacking", even though his strengths are in chemistry, bio-engineering and machining. Is there any evidence he may have tried to use or learn anything about hacking tools?

For these terms, we may search the web history. choose Web search from Data Artifacts. He looked up "How to disable Windows Defender," as can be seen.



1. Gene may have used a phone to photograph a secure location, according to our source. Any idea what? What happened to the device?

Default Email Messages can be found under Data Artifacts.By default, we can locate emails with the subject line "Android”.

Graphical user interface, text, application, email

Description automatically generated

*Figure: Email Communication*

1. Any other devices he might have used to photograph sensitive technology?

Yes, you may find a photo of soldered equipment under Analysis Results -> EXIF Metadata.

A picture containing graphical user interface

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, application, Word

Description automatically generated

From the above pictures we can say the device used to capture is NIKON D800.

1. Gene has mentioned in recorded conversations he has a stash of drugs he keeps at a beach house just in case his lab gets raided. Is there anything that might tell us he is familiar with particular beaches, or towns near beaches?

In autopsy, there was proof that Gene had previously searched for information about the Marina Resort in the browser cache artifact. Another piece of evidence indicating that the gene has bookmarked the links to neighboring restaurants on the internet. All of these information demonstrates that Gene was acquainted with the local cities and beaches.

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, application, PowerPoint

Description automatically generated

**Conclusion:**

We have obtained relevant information related to the case and those involved through sources such as pictures, emails, and software usage. From this information, we have extracted the necessary data.