ITIS 5250

Sahil Bhirud – 801138029

Lab 5

**Overview:**

In this lab, I have been given forensic images of The Monarch’s laptop **Monarch2User.ad1** and that of the Clarion Hotel Internet kiosk **ClarionUser.ad1** and have been asked by Agent Sampson to identify communications of The Monarch with a member of the Guild of Calamitous Intent (GCI), location of the members of GCI, photographs of Monarch and his associates or any evidence of explosives, drones, poisons, bombs or other means to kill or injure the Monarch’s target Dr. Thaddeus Venture.

**Forensic Acquisition and Exam Preparation:**

I downloaded all the required files from Canvas and uploaded the two forensic images and calculated and verified the hash values. The softwares used for accessing and analyzing the information is **FTK Imager, Autopsy** and **PRTK (Password Recovery Toolkit)**.

A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated

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

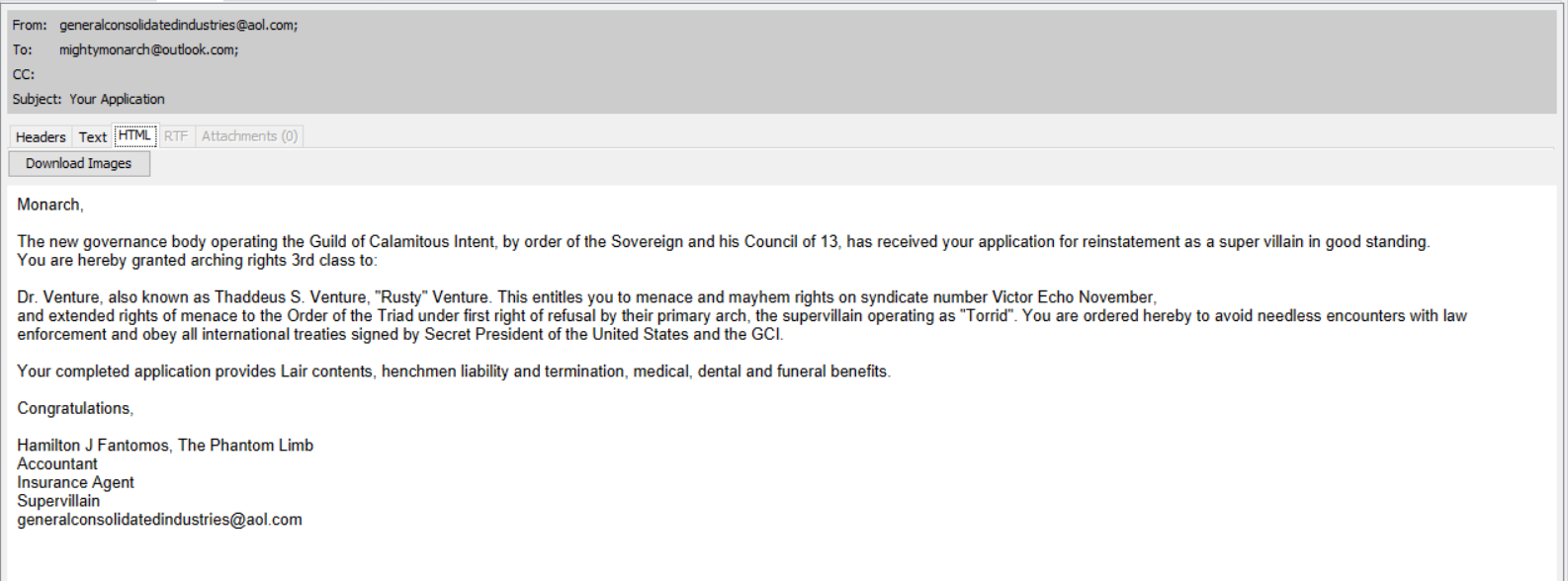
I have performed the forensic analysis of the images in Autopsy.

* **Was there communication from someone claiming to be the Guild's operative, or can you identify the operative?**

Yes, there was communication from a guy named **Hamilton Fantomos** who seems to be operating for the GCI. I have recovered an email sent by Hamilton to the Monarch saying that he has been reinstated as a supervillain and information about his next target.

This email is located at the following path:



**

* **Can you identify any pictures of this person?**

I found an email which was sent by Hamilton to the Monarch which had an attachment of a photo of him and Sheila.

Here’s the email:

*A screenshot of a cell phone

Description automatically generated*

And here is the photo of Hamilton and Sheila:

A picture containing television, table, sitting, monitor

Description automatically generated

* **Can you provide any pictures depicting the Monarch?**

I found a few pictures which are depicting the Monarch. I am certain that these are the Monarch’s photos since he has sent an email to his wife saying that he has appeared on the New Yorker.

A screenshot of a social media post

Description automatically generated

These pictures were located at ***/LogicalFileSet2/AppData/Roaming/Thunderbird/Profiles/mrltblnq.default/ImapMail/imap-mail.outlook.com/Sent-1/***

***A drawing of a cartoon character

Description automatically generated***

A picture containing screenshot

Description automatically generated

* **Can you find the Monarch's email address or the email address of the operative?**

Along with the recovery of the communication of the Monarch with the operative (Hamilton), we have also recovered their respective email addresses. They are mentioned below:

Monarch’s email address: <mightymonarch@outlook.com>

Operative’s (Hamilton) email address: [generalconsolidatedindustries@aol.com](mailto:generalconsolidatedindustries@aol.com)

A screenshot of a social media post

Description automatically generated

* **Are there any items related to the Monarch's plans for violence?**

Yes, there is an email in which the Monarch is seen telling Hamilton about the way in which he is about to perform a heinous crime on Dr. Venture.

A screenshot of a social media post

Description automatically generated

Also, there was a photo of a drone in his Downloads folder which shows he already has been doing research on his plan.

A picture containing screenshot, plane, monitor, air

Description automatically generated

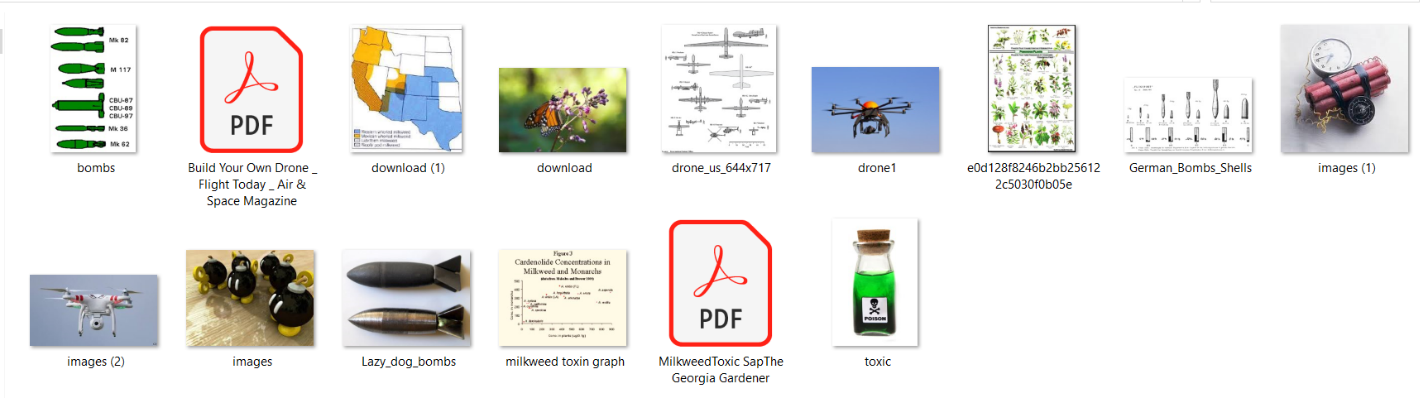
* **Can you recover any passwords?**

I found a file named **AllMyPlans.zip** which was password protected. I extracted this file from Autopsy and cracked the password to this file using PRTK. The password to the file was “**monarch”**.

A screenshot of a cell phone

Description automatically generated

In the extracted files, I further found evidence related to Monarch’s plans for violence.



* **What was the last time of login of the local user account?**

As observed in the SAM Registry Hive, the last login date of the local user account in the Monarch’s laptop is **29th March 2015 at 23:09:54 UTC**.

A screenshot of a cell phone

Description automatically generated

Also, the last login date for the local user account on the Clarion Hotel computer is **11th April 2015 at 01:51:52 UTC**.

A screenshot of a cell phone

Description automatically generated

* **What other programs was the user running around the time of the email (within 12 hours), if any?**

One program was running around the time of the email which was **thunderbird.exe**. The time in EDT converts to **10th April** **21:30** which is around the time when Monarch received the email.

**A close up of a logo

Description automatically generated**

* **Is there any evidence the Monarch planned to stay in the particular hotel?**

Yes, there is a lot of evidence suggesting that the Monarch had planned to stay in the Clarion Hotel. I have found pictures of maps showing the location of Clarion Hotel, its rooms and amenities and internet searches for the hotel from the forensic image **MonarchUser2** which is the image of the Monarch’s laptop.

A screenshot of a cell phone

Description automatically generated

A screenshot of a social media post

Description automatically generated

After my examination of the forensic files, I verified the hash values again to make sure I had not made any modifications to the image.

**Conclusion:**

I verified and examined the forensic images Monarch2User.ad1 and ClarionUser.ad1 using FTK Imager, Autopsy and PRTK and found relevant evidence of the Monarch’s plans to commit a crime on Dr. Venture. The evidence included but was not limited to a pre-planned at the Clarion Hotel, pictures of drones, bombs, poison, etc.