ITIS 4250 / 5250

Pooja Haridasyam

Lab # 3

03/31/2023

**Overview:**

Agent Sampson gave me files related to a cold case for inquiry. Two pairs of registry and image files are included in the offer. The accused used the other device while using the internet kiosks at the Clarion Hotel; one was removed from him. A warrant covering every element of Agent Sampson's request has been submitted to a North Carolina superior court judge in order to obtain the images.

**Forensic Acquisition and Exam Preparation:**

**Steps that were undertaken to prepare the image for examination:**

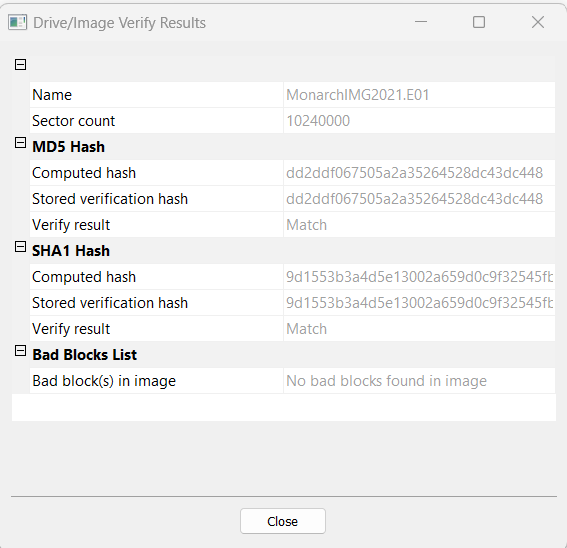
1. The MonarchIMG2021.E01 and ClarionIMG.E01 lab files were obtained from Canvas by going to Files> Labs> Lab 3 Files.

2. The computer was downloaded with the FTK imager installed. Navigate to canvas, then Files > Software > AccessData\_FTK\_imager\_4.7.l.2.exe, to accomplish this.

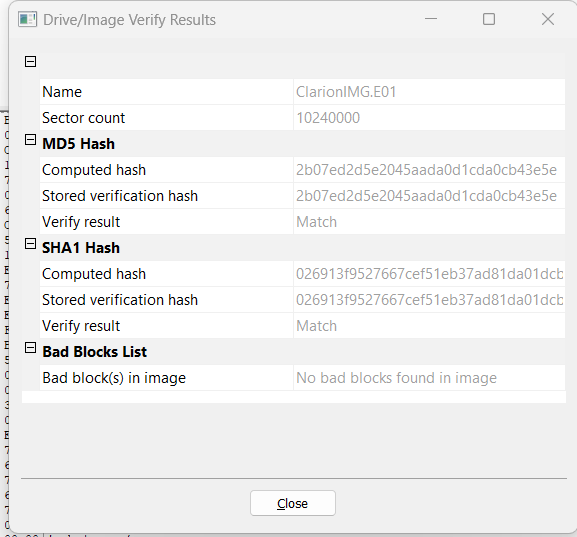
3. Launch the FTK imager application and submit evidence by clicking the green plus (+) symbol. To upload the image, browse the image file.

4. Select the verify drive/image option by right clicking and by selecting the image file that was inserted.

5. A portable hard disk with FTK imager installed on it was mounted on a Dell Inspiron 14 2-in-1 laptop with an AMD Ryzen 7 5825U processor and Radeon graphics, Windows 11 Home, a 64-bit operating system, and 16.0 GB of memory. (15.4 GB usable)



*Figure 1: Verified Hash values for MonarchIMG2021.E01*



*Figure 2: Verified Hash values for ClarionIMG.E01*

**Verified Hash values of both the images:**

MonarchIMG2021.E01: dd2ddf067505a2a35264528dc43dc448

ClarionIMG.E01: 2b07ed2d5e2045aada0d1cda0cb43e5e

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

1. AccessData FTK Imager – 4.7.1.2x64

2. Autopsy – 4.20.0 64-bit

3. Windows 11 Operating System on Dell Latitude 3510, 16GB RAM

4. Registry Explorer v2.0.0.0

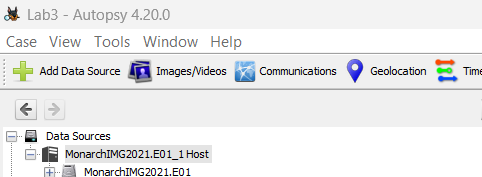
**Forensic Analysis:**

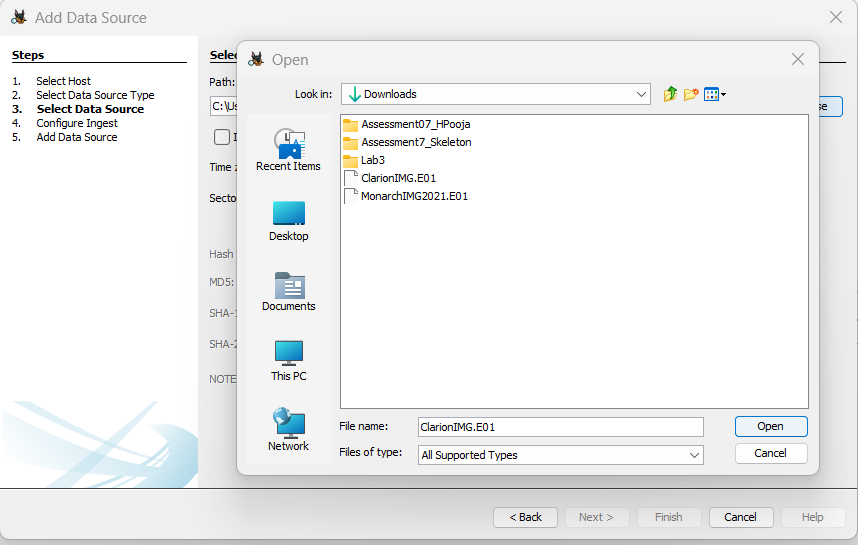
**Image loading on Autopsy 4.20.0**

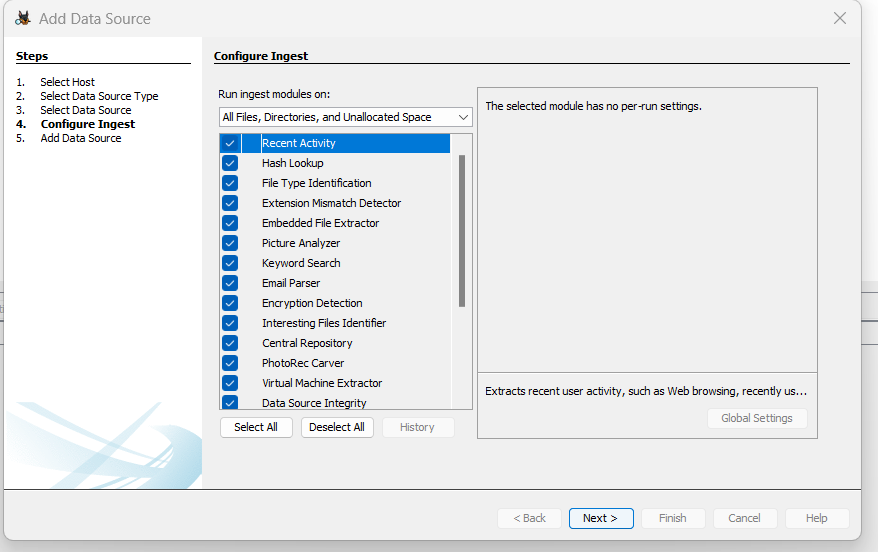
1. Download Autopsy 4.19.3 from www.autopsy.com/download.

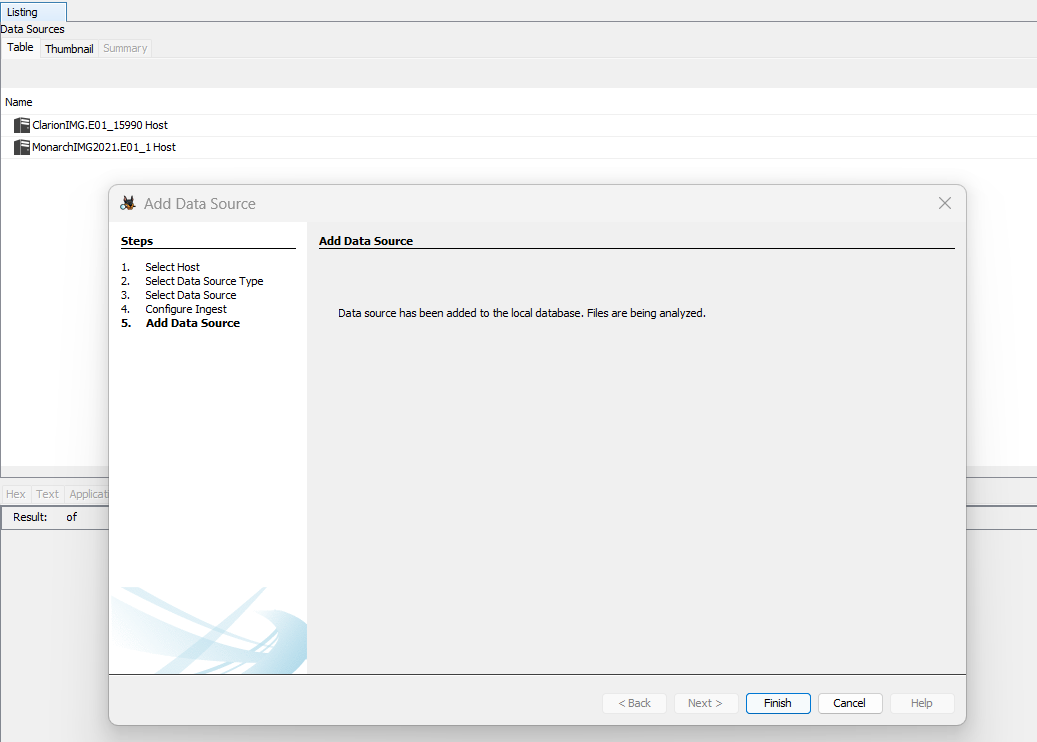
2. Create a new case in autopsy after installation and import the disk image.

3. A portable hard drive mounted on a Dell Inspiron 14 2-in-1 laptop with an AMD Ryzen 7 5825U CPU and Radeon graphics, Windows 11 Home, a 64-bit operating system, and 16.0 GB of RAM had Autopsy 4.19.3 installed on it. (15.4 GB usable)

****

****

****

****

*Fig: Adding data sources*

**Loading registry onto registry explorer 2.0.0.0:**

1. From the software's subdirectory in canvas files, install registry Explorer.

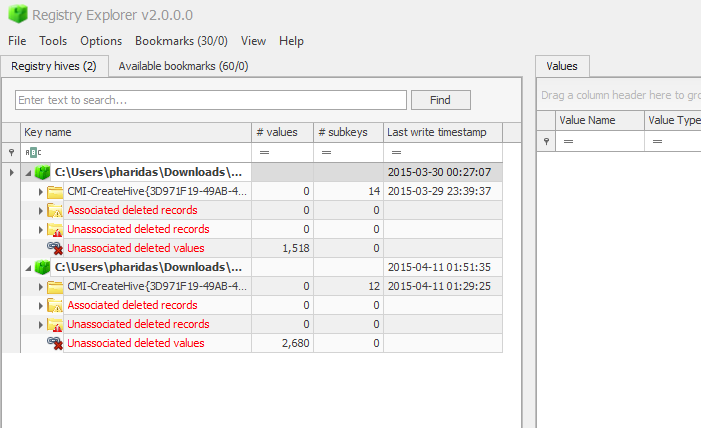
2. Following download, we access the registry file we want to analyze.

3. By selecting File > Load Offline Hive, we transfer the file to Registry Explorer.

5. This software is running on the hard disk that was mounted on the Dell Inspiron 14 2-in-1 laptop, AMD Ryzen 7 5825U with Radeon Graphics, Windows 11 Home, 64-bit operating system, x64-based processor, 16.0 GB. 4. We choose the software text file that we will be examining. (15.4 GB usable)

6. A registry file containing a list of software is the chosen file.

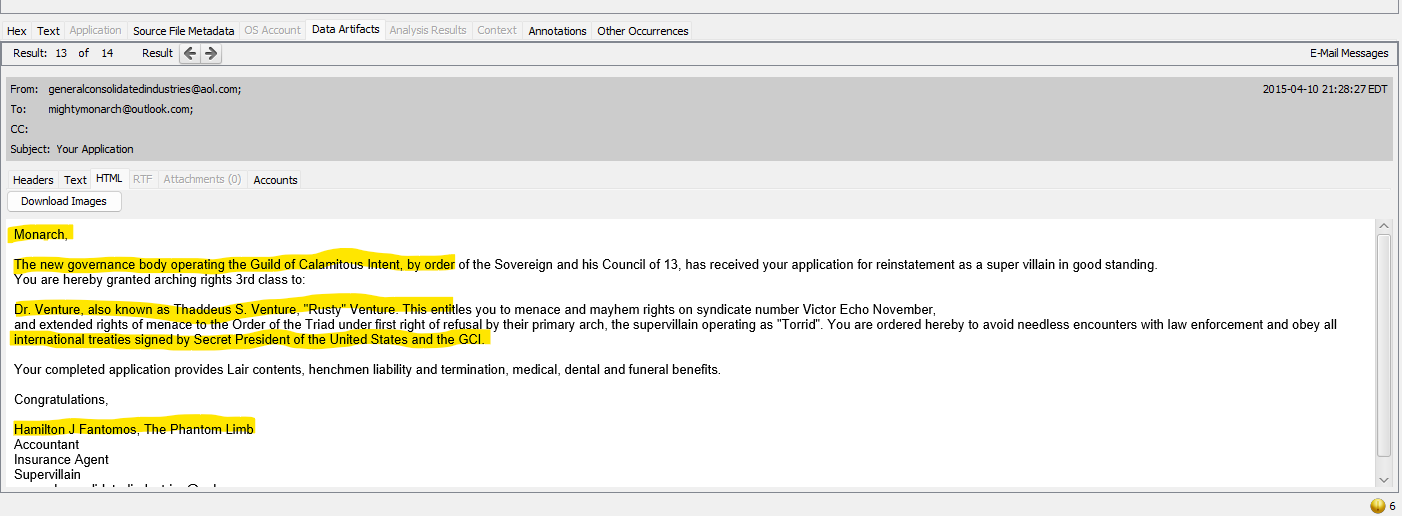
**RegistryM and RegistryC have been loaded into the Registry Explorer:**

****

*Figure: Adding the Registry Files*

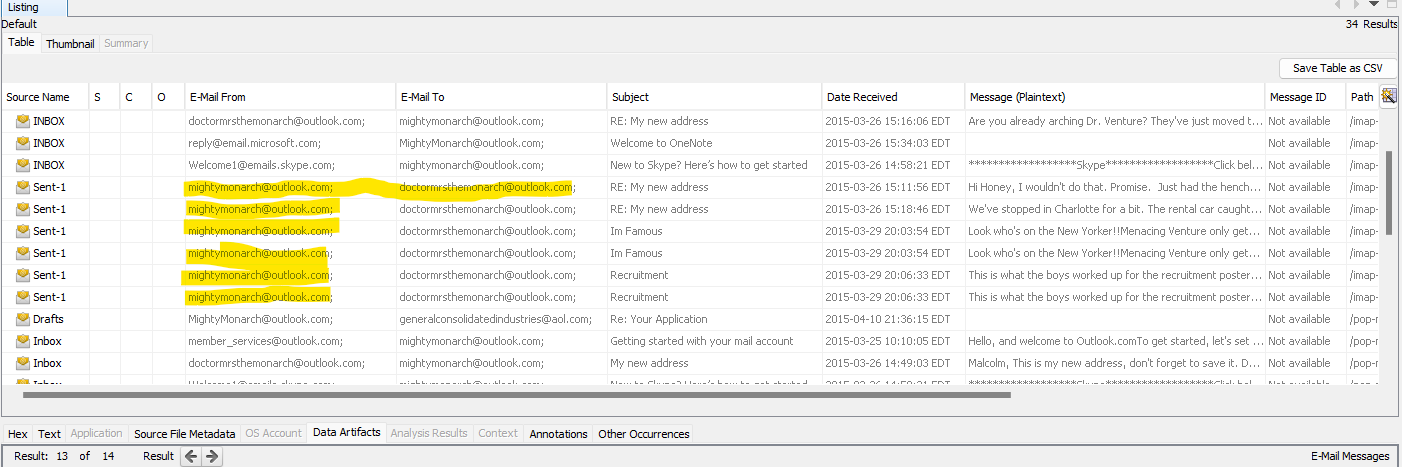
We can perform the analysis and discover answers to the following questions using the mentioned tools, Autopsy and Registry Explorer:

1. Was there communication from someone claiming to be the Guild's operative, or can you identify the operative’s name/email?
2. The email correspondence is visible under Data Objects -> Email messages -> Default- >Defaults. Congratulations to Monarch are expressed in an email from Hamilton J. Fantomos, The Phantom Limb, with the sender's email address as [generalconsolidatedindustries@aol.com.](mailto:generalconsolidatedindustries@aol.com.)



*Fig: Email Communication*

1. What is Malcom's email address? Did he send email to someone other than the guild operative? Who?
2. The email correspondence is visible under Data Objects -> Email messages -> Default- >Default (34)



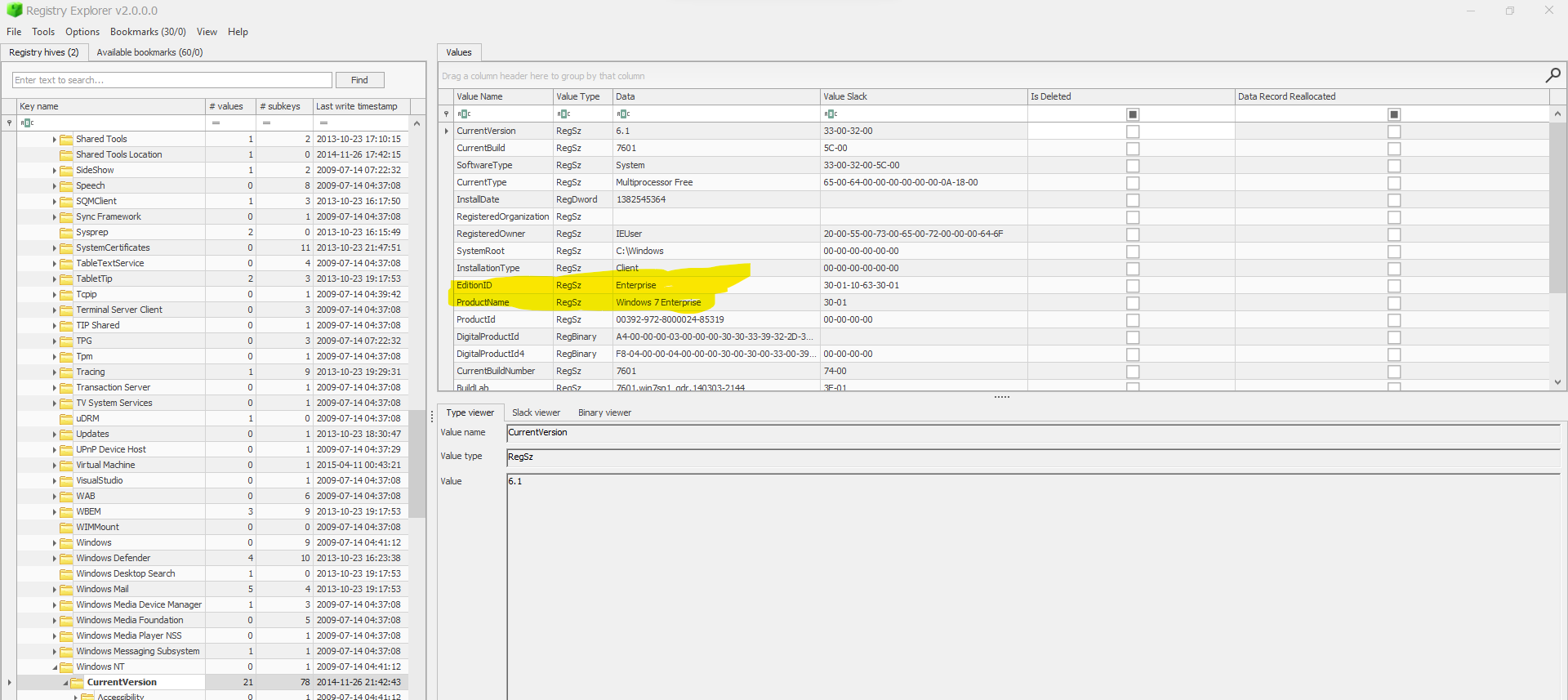
*Fig: Email Communication between Malcom and other person*

Malcom's mail is highlighted, and the other mail address is “doctormrsthemonarch@outlook.com” for the mail he sent that wasn't addressed to a guild operative.

1. What version OS was running on the computer in use?

CMI-CreateHive(3D971F9) -> Microsoft- > Windows NT-> CurrentVersion contains information about the OS version.

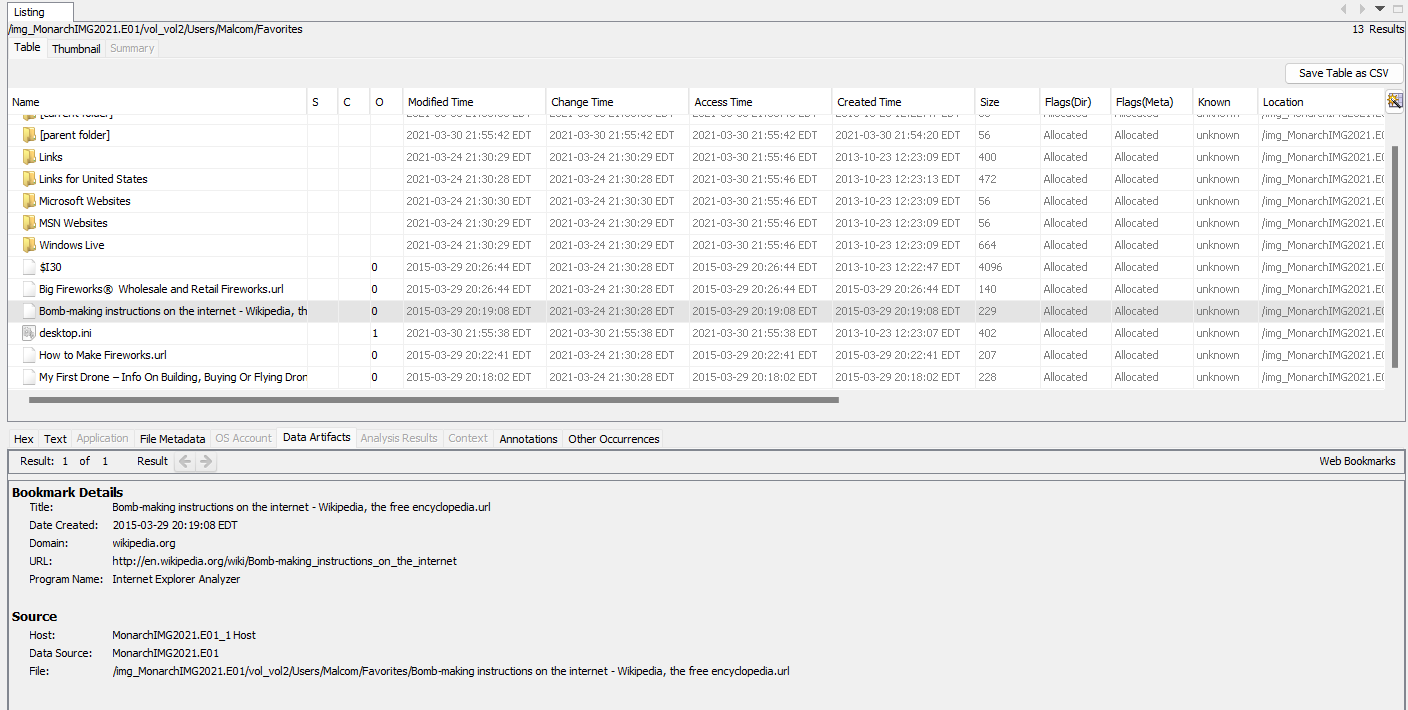
It is Windows 7 Enterprise Edition



*Fig: OS version*

1. Did Malcon ever search for any terms that might mean he was going to cause any explosions?

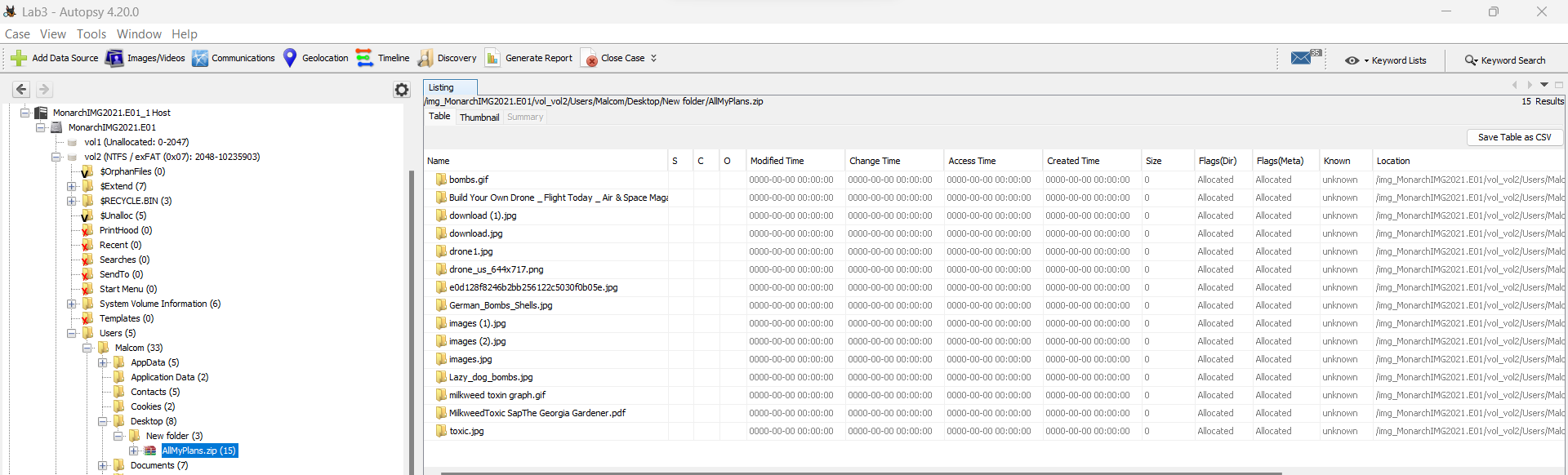
You can find the details under Data Artifacts->Web Bookmarks. A bookmark on the internet with the title "Bomb Making instructions" demonstrates that he is attempting to manufacture bombs.



*Fig: Web Bookmarks with the Bookmark on Bomb making instructions*

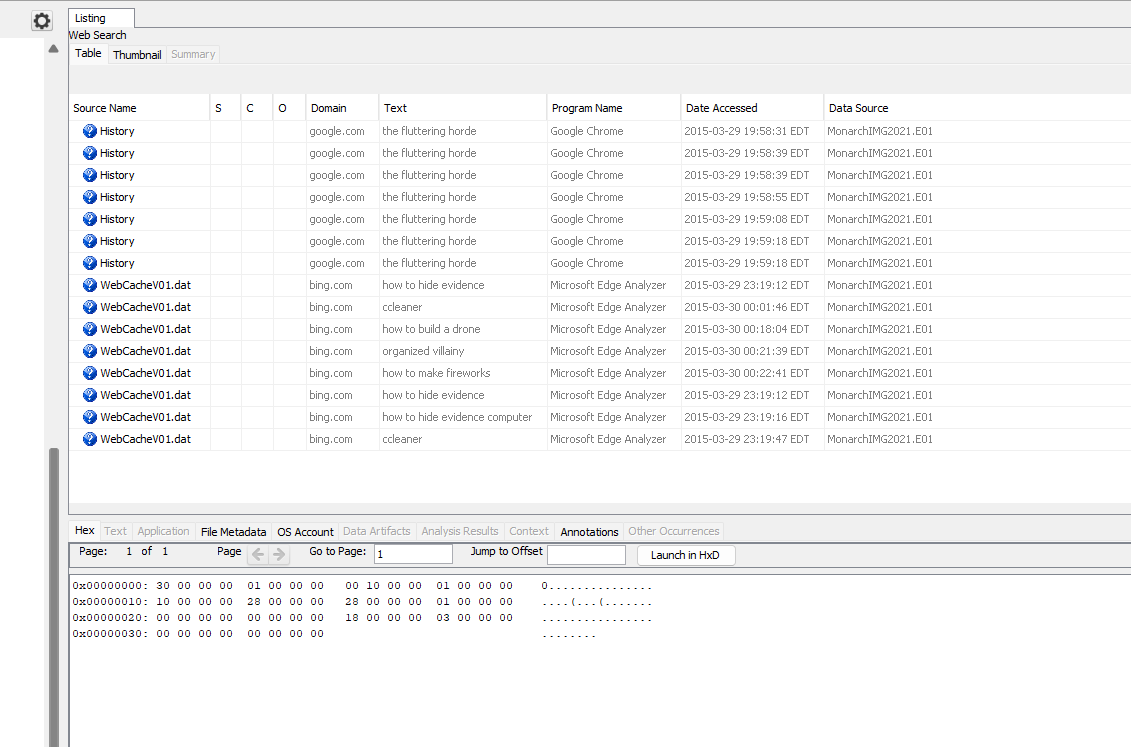
1. How about how to cover his tracks?

It has an encrypted subdirectory, and the following files are contained in the zip folder:



*Fig: Encrypted folderAllMyPlans.zip*

It can be seen from his web searches that he is looking up how to construct a drone, how to conceal evidence on a computer, etc.



*Fig: Web history for covering his tracks*

6) Explain in detail what he was doing, with what software and when.

He was looking up information online about how to make a drone, hide digital evidence, etc. He was also looking for the software needed to carry out the duties he was looking for.

Graphical user interface, text, application, email

Description automatically generated

He was looking for the Access Data FTK imager program, as shown by the following screenshot:

Graphical user interface, text, application

Description automatically generated

*Fig: He is downloading AccessData FTK Imager software for accomplishing his tasks*

1. Are there any photos that might have been downloaded? How do you know the photo was downloaded and not just moved to the folder where it was found? Is there a photo at this location that might tell us how he appears?

We can confirm that any photos that may have been downloaded using the path have been downloaded and saved locally on the computer.

Graphical user interface, application, Word

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, application

Description automatically generated

*Fig: Images downloaded from the browser.*

1. Did malcom do any research into forensics software? What specifically?

Graphical user interface, application

Description automatically generated

*Fig: Web Search*

We can check Data Artifacts -> Web History to collect that knowledge.

Graphical user interface, text, application, email

Description automatically generated

*Fig: Web History*

1. Is there any evidence he may have opened photos locally with an internet browser? Are those photos still available on the system?

Any files viewed locally in a web browser are saved as.temp files, which can be located in the Images/Videos tab of the Autopsy software:

->vol\_vol2->AppData->Local->Microsoft->Windows- >Temporary Internet Files->Low->Content.IE5 img\_ClarionIMG.E01

Graphical user interface, application

Description automatically generated

Fig: Temp files containing images

Each content.ie5 has multiple sets of images.

Similarly, we can navigate to temp images on the clarion image file img\_ClarionIMG.E01> vol\_vol2> AppData> Local> Microsoft> Windows> Temporary Internet Files> Low> Content.IE5

Graphical user interface

Description automatically generated

*Fig: Temp files containing images*

Images found on the monarch’s machine suggest malicious acts were intended.

Graphical user interface, application

Description automatically generated

Graphical user interface, table

Description automatically generated

Graphical user interface, application

Description automatically generated

Graphical user interface, table

Description automatically generated

Fig: Evidence

Graphical user interface

Description automatically generated

Fig: Evidence

**Conclusion:**

According to the research, there is a communication on the provided image file that purports to be from a guild agent. The operative's identity and email address were also accessible. We also managed to track down the monarch's email account and his outgoing emails. Using the registry file, we could also determine the OS version that is presently installed on the Clarison Hotel. History/bookmarks implied that Malcon was attempting to set off an explosion while also attempting to hide his traces. Images in the temporary folder imply that he was attempting to search for bombs and drones. The suspect looked into forensic tools as well. Agent Sampson receives the outcomes of the forensics picture and the forensic image. There is no need to analyze this information any further.