KURUKULASOORIYA KVR **200332X**

Analysis of Disk Image of USB drive using FTK Lite and Finding Deleted Files

CS 3460 MINI PROJECT REPORT

Overview

FTK Imager Lite is a free digital forensics tool designed by AccessData, a leading provider of computer forensics software and services. It is a simplified version of the full-featured FTK Imager. It offers an essential set of functionalities for imaging, analyzing, and recovery of data from the digital evidence, and some of these would be as follows:

- **Forensic Imaging:**

It allows users to access physical or mounted logical volumes (ex: hard drives, solid-state drives, USB drives, and memory cards) and create a bit-by-bit copy of their content in various formats, such as Advanced Forensic Format (AFF) and raw dd images etc.

- **Recovery of Deleted Data from Digital Evidence:**

This software includes powerful tools to recover deleted files and fragments within the forensic image generated.

- **Verification and Integrity Checking:**

The tool also contains some built-in verification and integrity-checking mechanisms to ensure the integrity of the acquired images while confirming that the created forensic image is an exact replica of the original data source.

- **Hash Calculations:**

This also provides facilities to calculate and display hash values of the acquired images by using a variety of hashing algorithms as at the user's preference (e.g., MD5, SHA-1, SHA-256).

- **Allows Mounting and Exporting:**

This software provides the ability to mount forensic images as logical drives allowing the investigators to perform manual searches, traverse the file structure, and view their content. And it also allows to export the content of the device connected as a Zip file or any other format to save it as a copy.

- **Reporting:**

The tool often provides basic reporting capabilities, allowing users to generate summaries of their forensic acquisitions and analysis results.

FTK Imager Lite is widely used by digital forensics professionals, law enforcement agencies, and cybersecurity experts to conduct analysis and examinations of digital evidence obtained from various sources. Meanwhile, it also provides an intuitive and neatly organized user interface, making the users easily engaged with the software but the commonly occurring con is that there would be an issue of performance degradation as it takes more time to create the forensic image of large storage volumes.

Preparation

To install FTK Lite Imager

1. Download the setup using following link.

   https://accessdata-ftk-imager.software.informer.com/download/

2. Execute the setup file.
3. Read and accept the License Agreement.
4. Click on Finish the wizard once it completed getting installed.

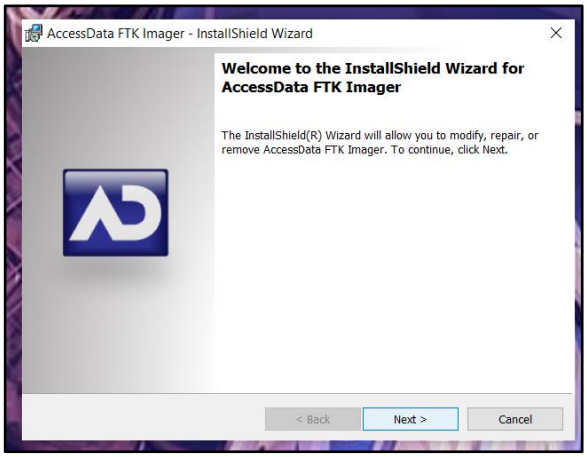

Figure 01

To run FTK Lite Imager

1. Double Click on the desktop icon
2. Allow access to the device by selecting the option "Yes" to the pop-up window.
3. The UI will be loaded as shown in the figure 02.

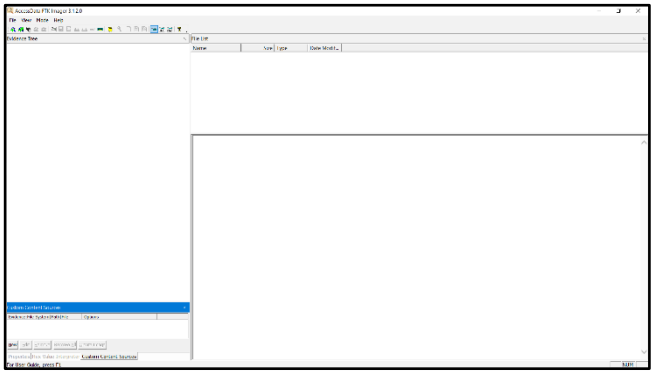

Figure 02

To add an digital evidence for the analyzing purpose:

1. Connect the USB drive to the PC
2. Go to File > Add Evidence Item (Figure 03)
3. Select the Source Evidence Type (Figure 04)
4. Select the Source device from the drop-down menu (Figure 05)

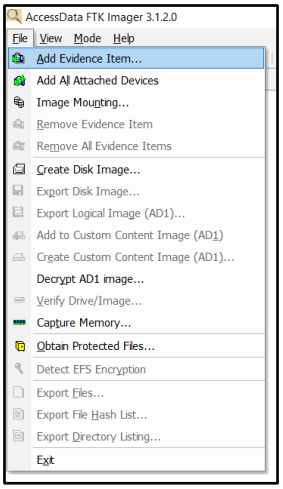

Figure 03

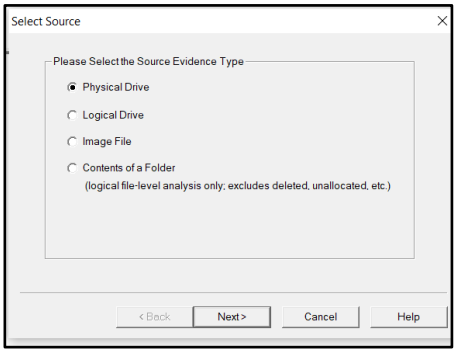

Figure 04

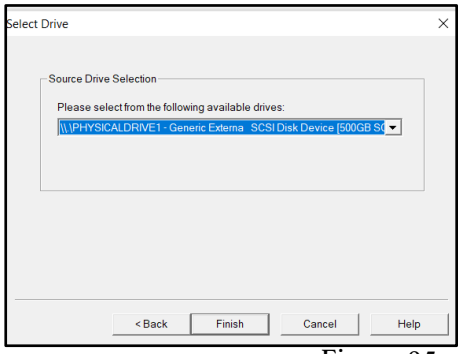

Figure 05

5. Click on Finish

6. The content of the device will be loaded in a structure of a tree (called an Evidence Tree) and the content and metadata of folders and files can be explored & analyzed from there. (Figure 06)

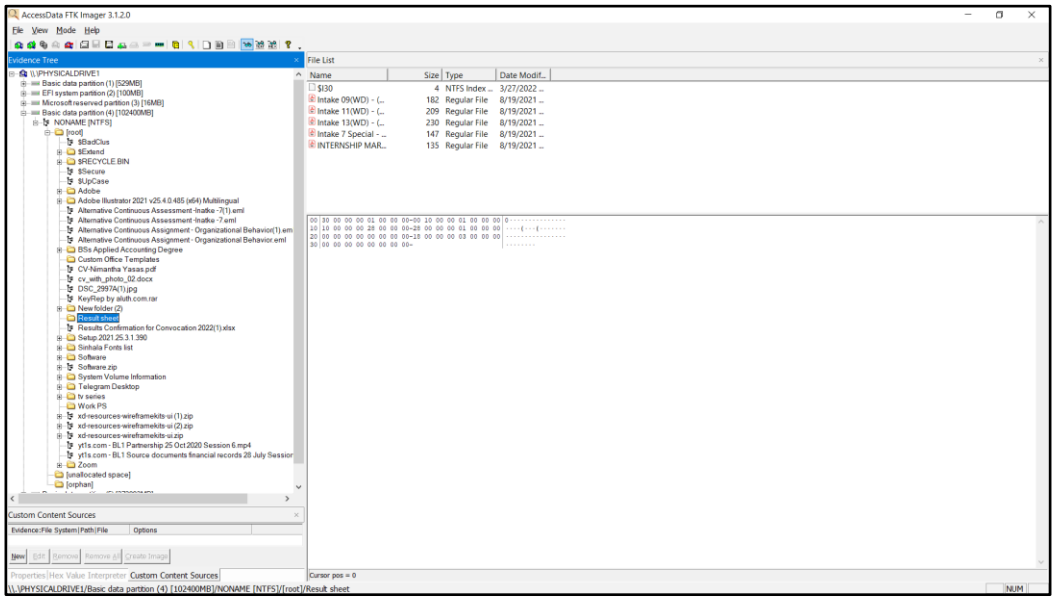

Figure 06

Activities Performed

a. Disk Image Creation

Step 01:

Refer into the following USB Drive and its content shown at Figure 07 & 08. That would be what we are going to used to create the Forensic Image using above tool.

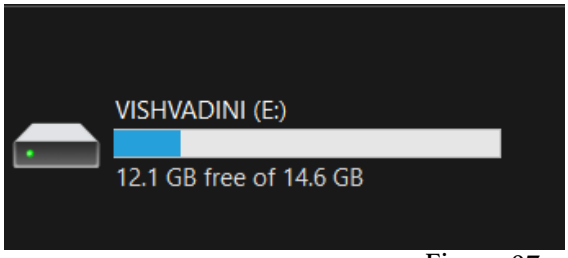

Figure 07

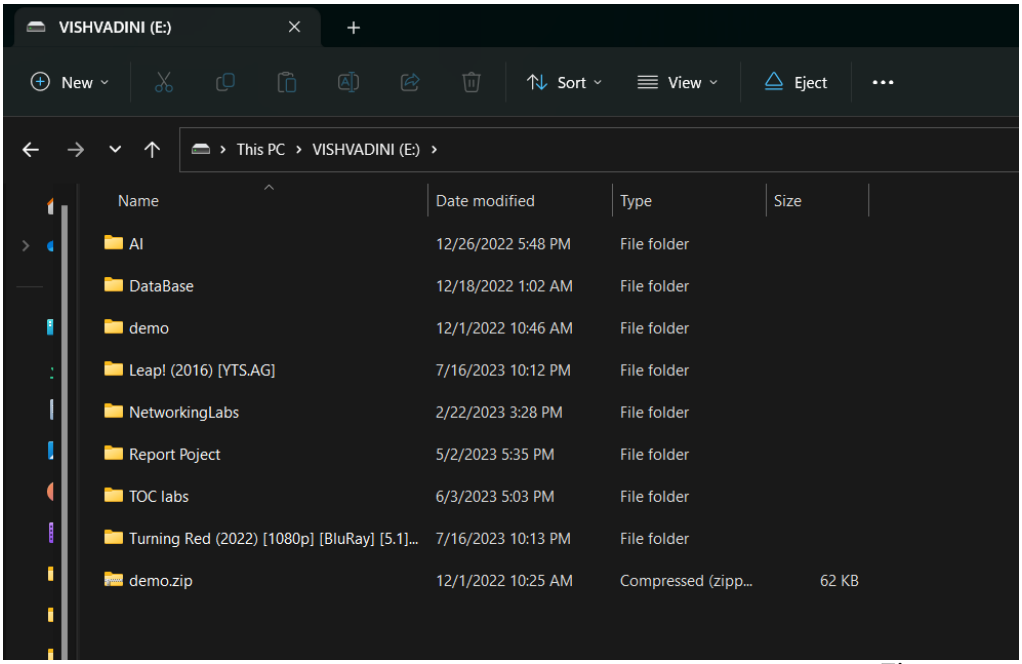

Figure 08

To recover and analyze the deleted files in the USB Drive for part b, the files called Turning Red, Report Project, and ToC labs are deleted. So the new content of the USB drive would be as follows (shown in Figure 09):

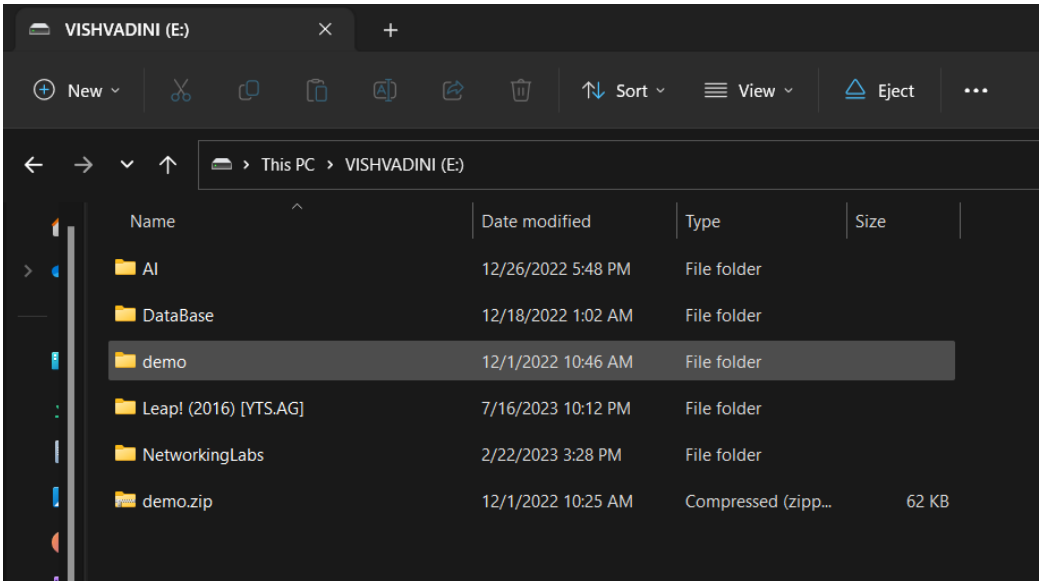

Figure 09

Step 02:

1. Open FTK Lite & Go to File > Create Disk Image. (Figure 10)

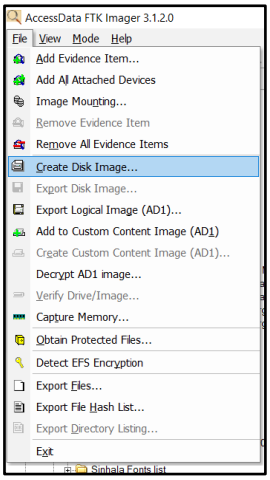

Figure 10

2. Select Physical Drive as the Source Evidence Type. (Figure 11)

Important:

- **Physical Drives refer to any kind of storage drive that is externally and physically connected to the machine.**
- **Logical Drives refer to the disk partitions of the hard drive in the same machine.**

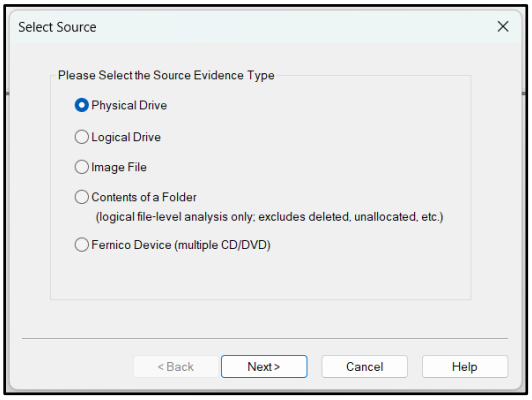

Figure 11

3. Choose the relevant USB drive from the Source Drive Selection drop-down menu. (Figure 12)

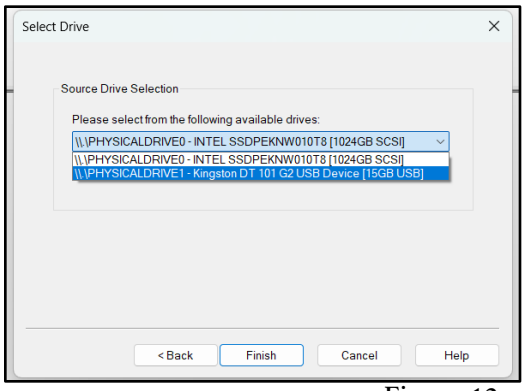

Figure 12

4. Now it is asking for the destination information to save the Image of this USB drive.
   i) Click ADD and the window will get appeared as shown in Figure 13.
   ii) Choose the file format as Raw(dd) which is Commonly used for saving Images for Investigation Purposes. (Figure 14)
   iii) Fill the form of Evidence Item Information for future referencing. (Figure 15)

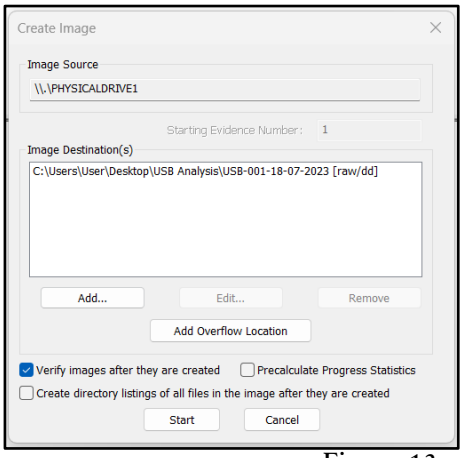

Figure 13

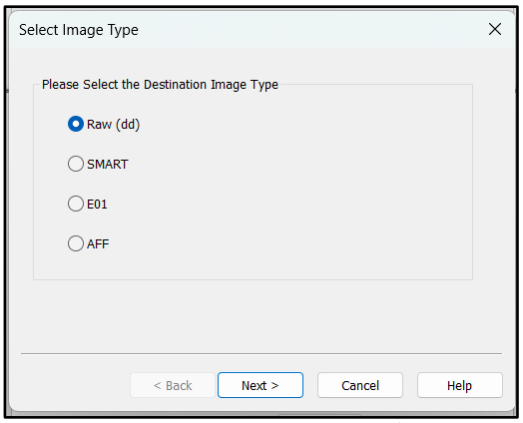

Figure 14

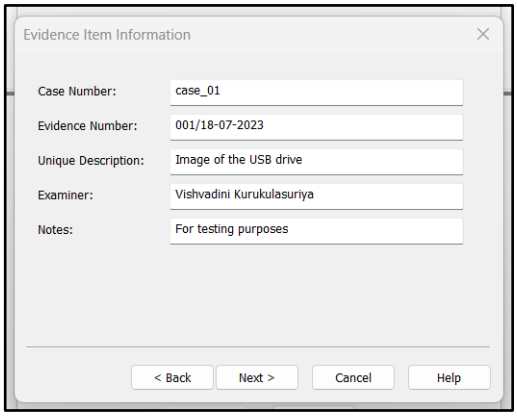

Figure 15

5. On the next window as shown in Figure 16,
   i) Browse > Choose the destination Folder
   ii) Give a name for the Image
   iii) Set the fragment size using a suitable value if the attached device is huge. Since it is a USB Drive is used in our case, the value is kept at its default (1500 MB)

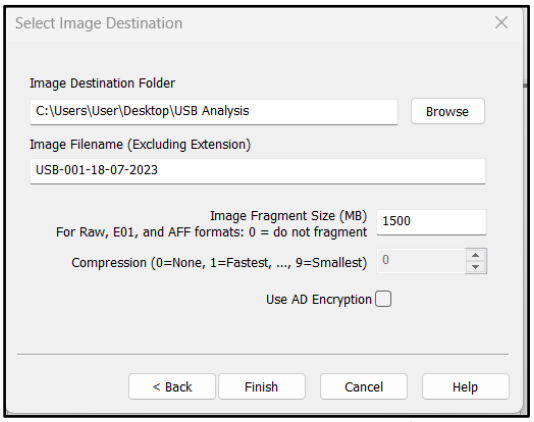

Figure 16

6. Once finished, Tick the Verify Image after they are created option. (Figure 17)
7. The Image will get started to create. (Figure 18)

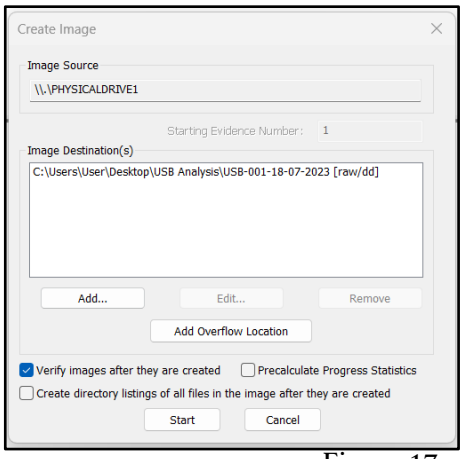

Figure 17

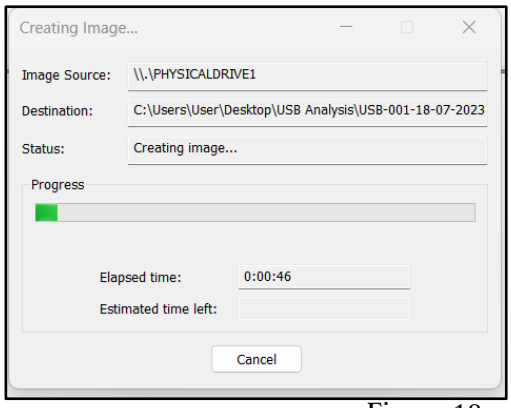

Figure 18

Step 03:

While the creation task is being processing, it's actual progress can be seen at the destination folder.

i) The Progress is closer to 50%

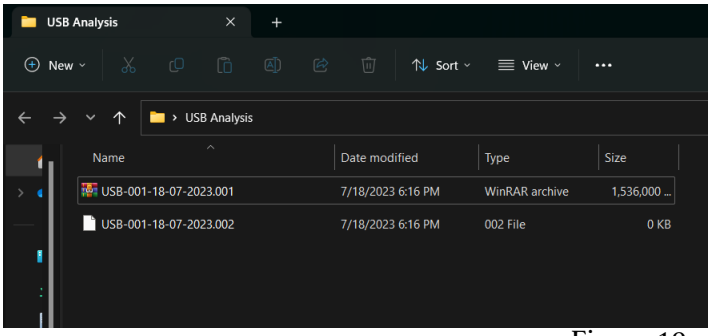

Figure 19

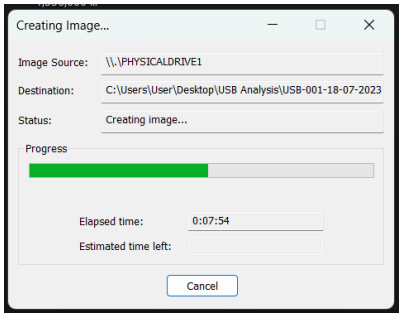

Figure 20

ii) The Progress is closer to 100%

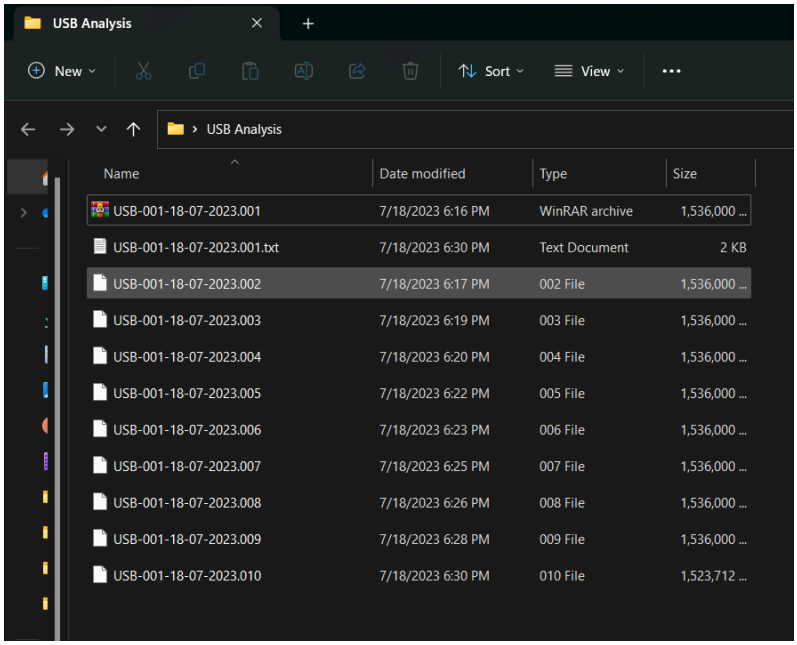

Figure 21

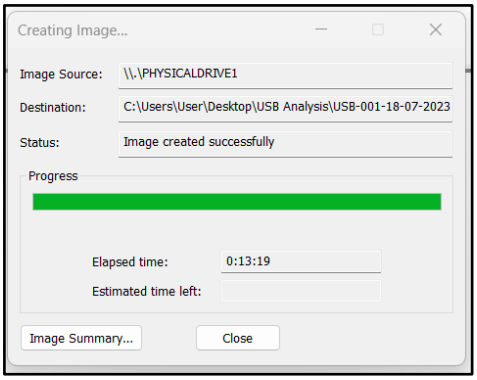

Figure 22

Step 04:

1. Once the creation is finished, the summary of verification will pop up.

As it is shown in the figure 23, the Computed hash and the Report hash values are the same. Thus, it will ensure the integrity and preservation of original data.

Plus, at the bottom of the list, it says that No bad locks found in the Image. This is also a good sign of our Image creation was completed successfully.

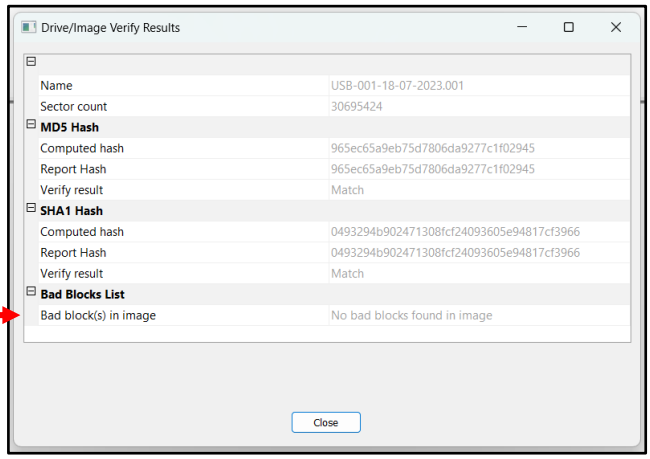

Figure 23

2. When we access the destination folder, we can see that the image of the USB Drive has been created in approx. 1500 MB chunks. (Figure 24)

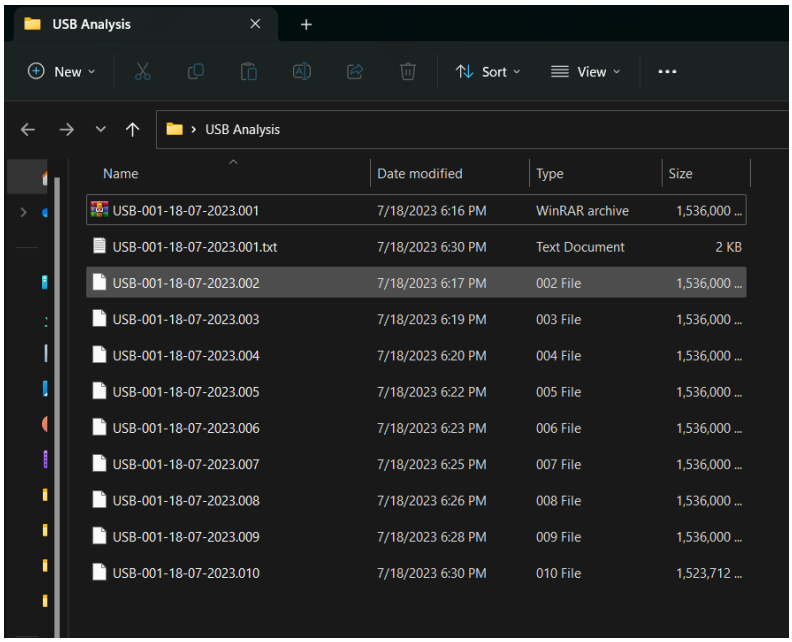

Figure 24

Important:

It is necessary to check whether all the pieces are sequentially ordered. If one file is missing, it would be unable to load/mount the Image.

3. If we select the text document shown as **" USB-001-18-07-2023.001.txt"** in Figure 24, it would be the Image of the FTK lite imager has used. It will give us very important details on the Creation of this Image including version number, evidence item info provided at the beginning, followed by elemental information about the Image created and timestamp of it's process, paths to the segments and much more.

The content of txt file is shown as follows in Figure 25.

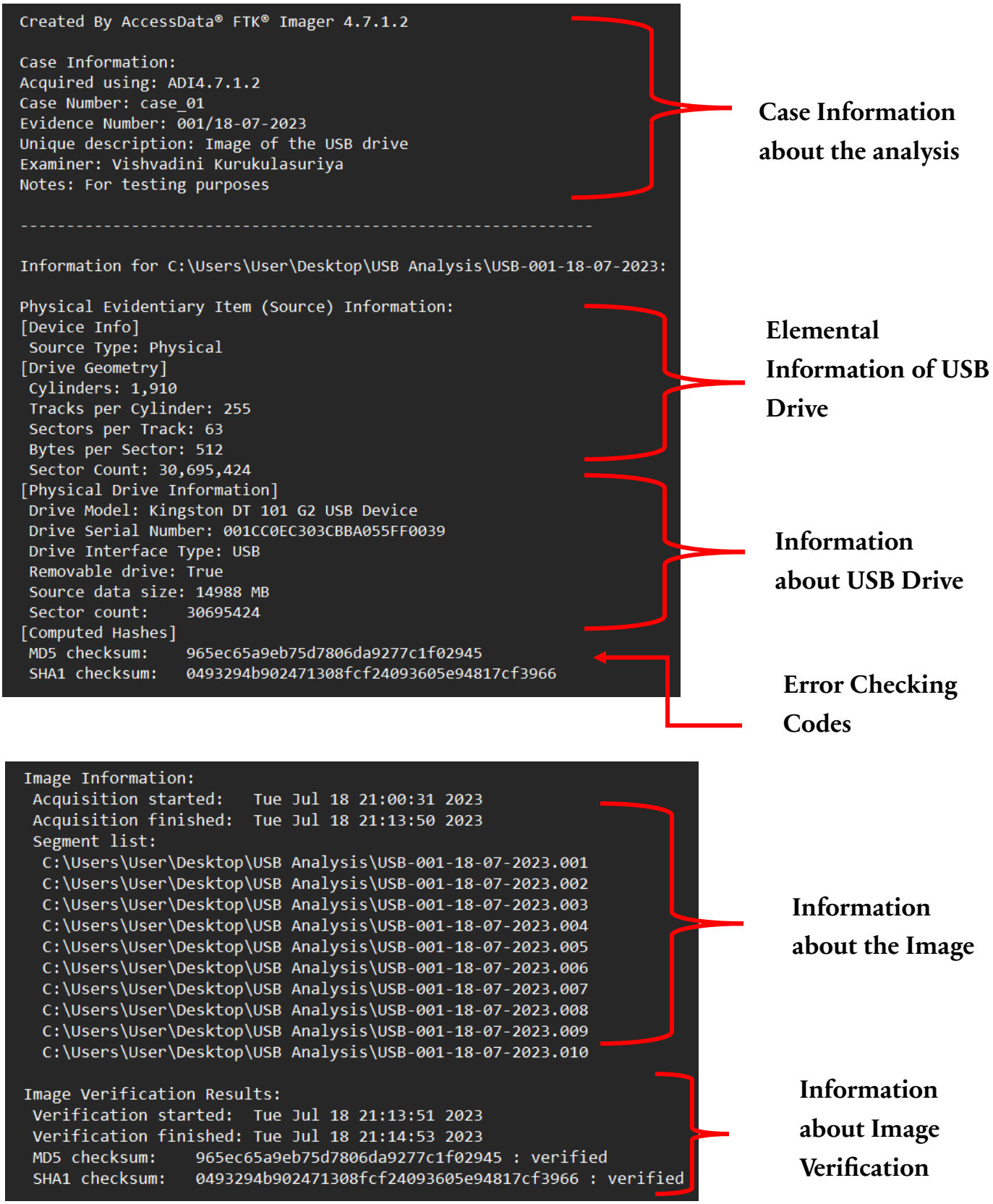

Figure 25

Step 05:

Next, we need to Mount the Image and recover it's content as a separate drive.

1. Go to File > Image Mounting
   (Refer to Figure 26)
2. Choose the Image from the destination
3. Choose the Mount Type as Physical Only
4. Choose the Mount Method as Block Device/ Read Only

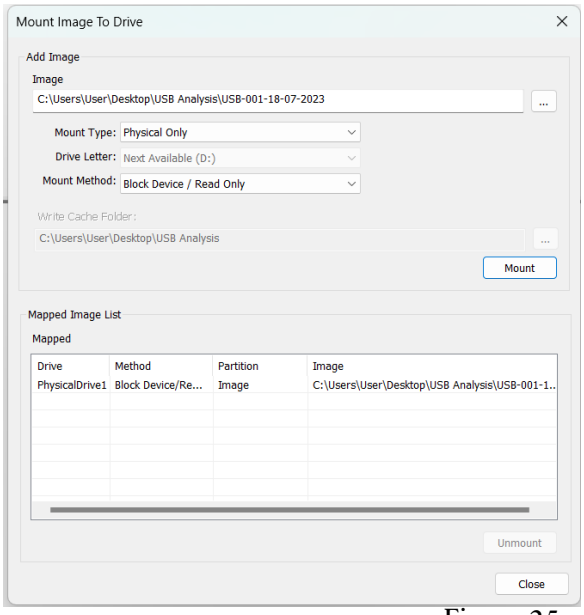

Figure 25

Important:

In Mount method Selection, two options are given as Block Device Read Only or Block Device Writable. Since we are doing a Forensic investigation, it is important to ensure that no altering or manipulation is done to the image while maintaining the integrity.

<u>So, In our case, we choose "Read Only" option.</u>

5. Mount the Image and Close the Window.

Now, when we access Disk Manager or This PC, we can see a separate Copy of The USB Drive that is mounted from the image (Figure 26)

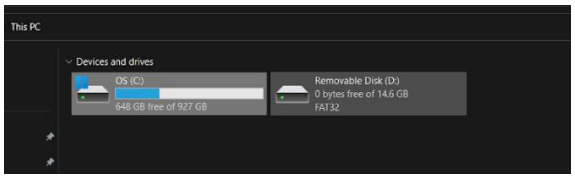

Figure 26

Important:

Since we have created a Read Only copy,

- **If we try to create new folder inside (Figure 27)**
  Or
- **If we try to delete the content inside(Figure 28)**

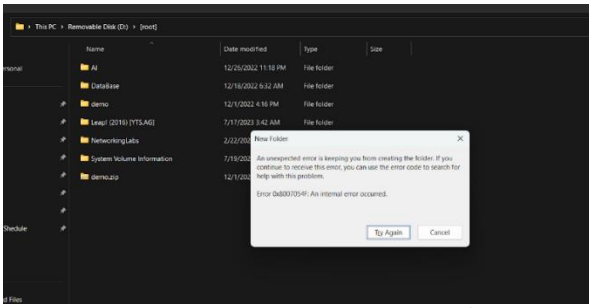
Figure 27

an error message will pop out while preventing any access to it other than reading. (Figure 29)

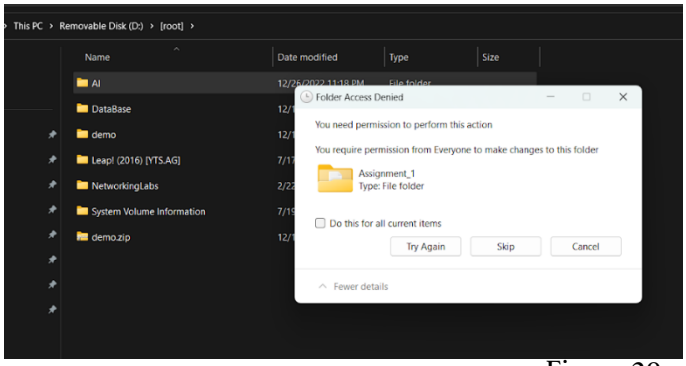

Figure 29

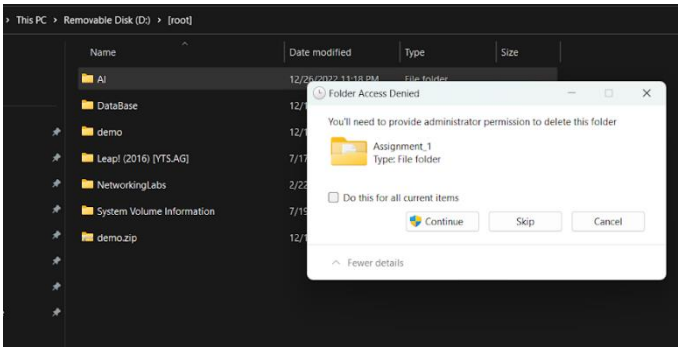

Figure 28

b. Deleted File Analysis

Step 01:

Since the Image of the USB Drive is mounted to the PC and held as a read-only logical partition within the local disk,

- Go to Add digital evidence > open and load the content as a logical drive (Figure 30)

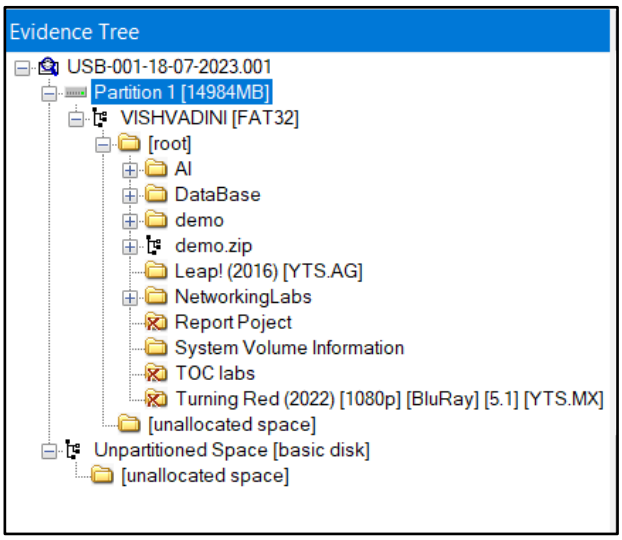

Figure 30

Important :

As it is seen in the Evidence tree the deleted files are represented as a file icon with a cross on it.

Step 02:

To recover it back,

- Right Click on the relevant file icon > Export File > Choose the destination for saving > OK (Figure 31)
- The File will then get exported.

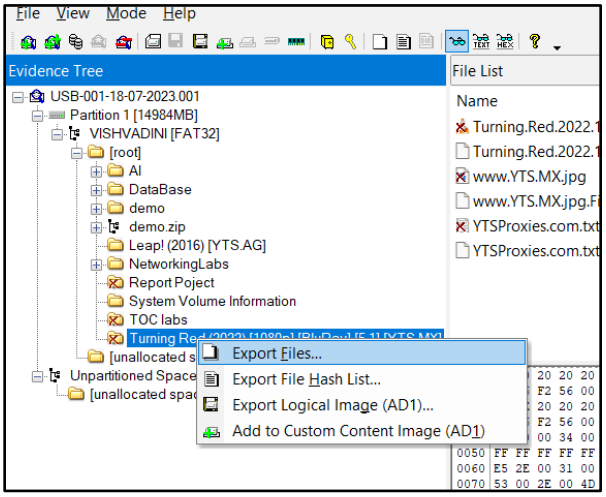

Figure 31

Step 03:

Once done exporting, access the destination and explore the file that is just recovered. (Figure 32)

Important :

Though we don't export it, still we can traverse and explore its subdirectories, it's content, and metadata in hexadecimal values at the FTK Imager Lite.

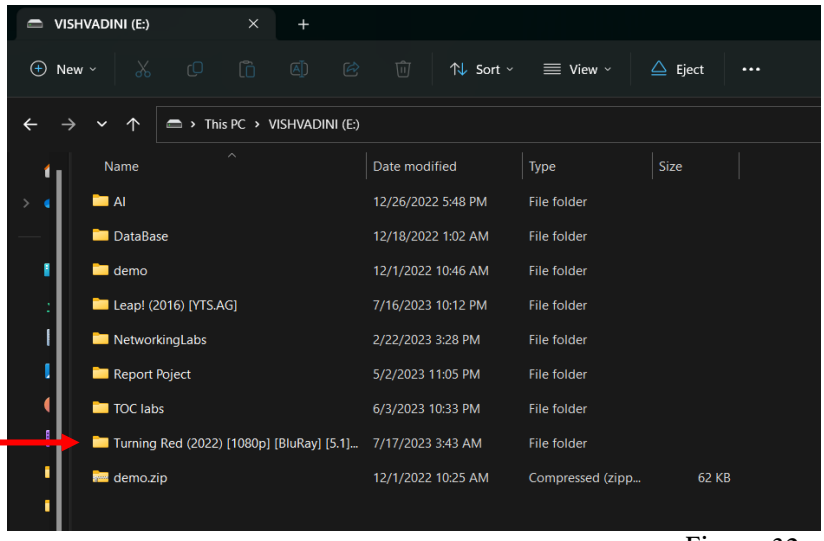

Figure 32

NO RECOVERY OF DELETED FILES WOULD BE POSSIBLE ONCE THE USB DRIVE IS FORMATTED. (PRUNGED)

Interpretations and Findings

Since the above demonstration is done using a USB Drive belonging to me, a random USB drive belonging to some other individual was analyzed again for this part.

The content that was shown on the USB drive was as follows in Figure 33:

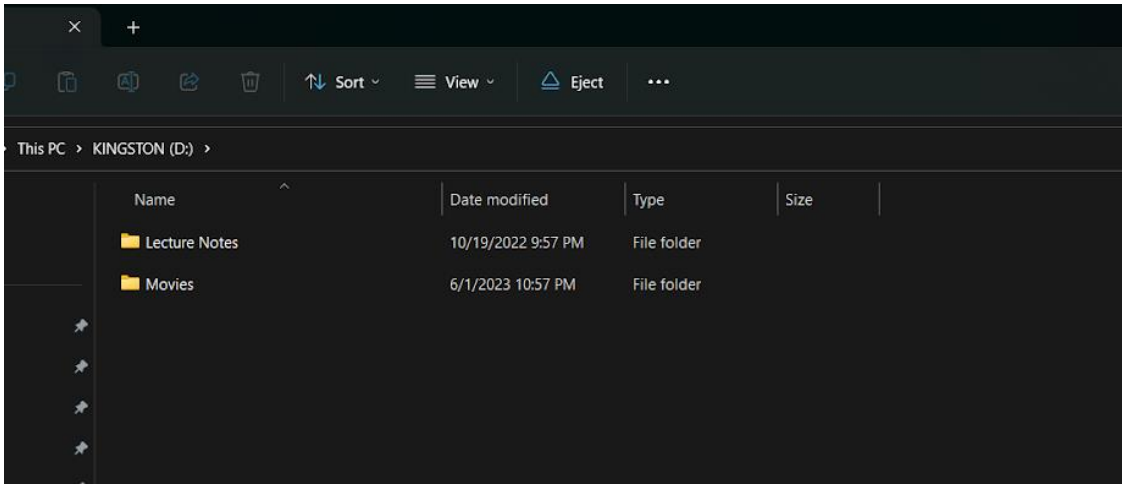

Figure 33

After analyzing using FTK Imager Lite, the following deleted files could be found:

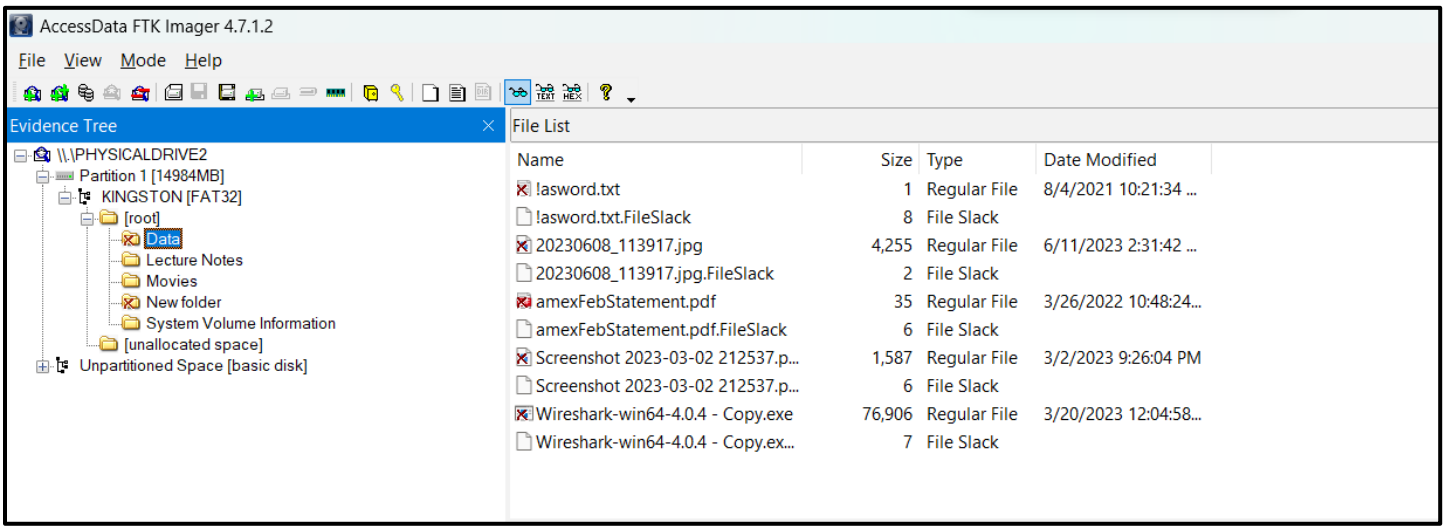

Figure 34

Thus the Deleted Files are :

- 20230608_113917.jpg
- Screenshot 2023-03-02 212537.png
- !asword.txt
- Wireshark-win64-4.0.4 – Copy.exe
- amexFebStatement.pdf

Results and Observations

Let's consider each deleted item one by one:

Due to ethical and privacy considerations, though the deleted files were recovered, they were not exported to discover and analyze their internal content.

1. **Two Image files: 20230608_113917.jpg & Screenshot 2023-03-02 212537.png**

20230608_113917.jpg should be a photograph that was taken on 8th June 2023 as specified in its file name. By analyzing a photograph, basic visual information can be obtained such as appearance, clothing style, closest connections, etc. By inferencing emotions, expressions, and facial features, an idea about their mood and traits at the time photo was taken can be identified. By referring to the background and objects in the photo, the location and context can be revealed.

By analyzing the **Screenshot 2023-03-02 212537.png**, some valuable insights related to his digital activities and interests can be obtained. As mentioned in the name, it was taken on 2nd march 2023 and the content may reveal the applications or websites the owner was using, indicating his online behavior and preferences. Plus, it may offer some clues about his work, hobbies, communication patterns, or sometimes some sensitive data like PINs or Passwords that he has put at the account creation.

2. **!asswords.txt file**

It is possible that this file contains some of the passwords that he has used for accessing email or social media or any other kind of accounts. If someone could export it and access this file, it can be used to unauthorizedly log in to those accounts to manipulate the content or hijack them. Plus, this is also a very critical indicator that, the person who belongs to this USB drive usually forgets passwords and that's why he tends to store them in a text file to refer to when needed. Since it is like a usual behavior of this person, we can conclude that there could be some other similar copies like this may exists (maybe in his mobile phone or laptop) which can be used to log in and compromise his user accounts.

3. **Wireshark.exe file**

This is a great indicator that the owner of the USB Drive uses Wireshark which is a powerful network analysis tool that helps to monitor and analyze packets flowing through networks. So, it implies that he would be an enthusiastic network security field and it is also possible that he may practice and expertise some other similar tools like this too.

4. **amex_febStatement.pdf file**

By referring to the filename, this pdf should be a February month's statement for an American Express credit card. If someone could access this file, it would be very risky, because he would be able to arrive at a very comprehensive insight about this card owner's financial health and credit state by referring to

its details like Account number, card number, available balance, spending and repaying patterns, installment agreements that the owner has entered into and much more

Insights on the history of the Owner of the USB Driver:

- It can be concluded that the owner of this USB drive has used it without being aware of the possibility of recovering its deleted content. He also has tended to store sensitive data like passwords, photographs, etc. while risking his privacy and security.
- Therefore it is crucial to convince him to take precautions like encryption and password protection on USB Drives to safeguard their sensitive information while protecting their privacy.

Summary

Disk imaging has significantly contributed to the preservation of the integrity of digital evidence by making a complete and unaltered copy of the owner's USB drive. This made guaranteed that the investigators had a trustworthy image of the whole disk, including concealed data and erased files.

Deleted files were successfully recovered and inspected using the FTK Imager Lite software, giving important details about the USB Drive owner's actions, intents, or attempts to hide information. Its powerful features made it easy to find and recreate erased files, helping to reconstruct the digital trail and create a comprehensive case.