Name: M.Ahmad

Roll no:221570

Lab Task 2

Lab Task 1:

Case 1:

As a digital forensics investigator assisting a multinational corporation in a suspected data breach. Your goal is to examine the company's servers to determine if sensitive customer data was compromised.

Steps for Digital Forensics Investigation:

1. Identification

First step is to identify the affected systems and breach such as:

- I review system logs and firewall records to detect unusual activity.
- I Identify which servers store sensitive customer data.
- I Look for unauthorized access attempts.
- I analyze a time of suspicious activity

2. Preservation

To ensure the integrity I used the following steps like:

- I used to create forensic images of affected servers using FTK Imager to avoid altering original data.
- I used the write blockers to ensure data integrity.
- To Document all evidences and maintain the chain of custody.

3. Collection

For collecting the relevant data we follow such steps like:

- System logs, event logs, and security logs from the affected servers.
- Network traffic captures to analyze data exfiltration using tools like **Wireshark**.
- Hard drive images to look for deleted or hidden files.

4. Examination

For analyzing the collected the data, I used the following steps like:

- Analyze logs and files using **Autopsy Tool** for hidden or deleted data.
- Use Kali Linux tools like Wireshark for network analysis.
- Look for malware or viruses, unauthorized file modifications, or unusual activity.

5. Analysis

After gathering and examining the evidence, I analyze them by following the steps like:

- Identify the scope of the data breach.
- Determine the attack vectors like it was phishing, malware, or an insider threat.
- Cross-reference logs, timestamps, and recovered files to build a timeline of the incident.
- If encryption or data obfuscation is detected, attempt decryption using forensic techniques.

6. Presentation

- I document all steps taken, tools used, and evidence collected.
- Create visual timelines and graphs to illustrate the attack sequence.
- Present my report to company executives, ensuring it is suitable for use in legal proceedings.

Legal & Ethical Considerations:

Throughout the investigation, I ensure legal and ethical standards such as:

- I follow proper forensic procedures so the evidence is legally admissible.
- I only examine relevant data to protect privacy.
- I maintain a record of all evidence handling.

Lab Task 2:

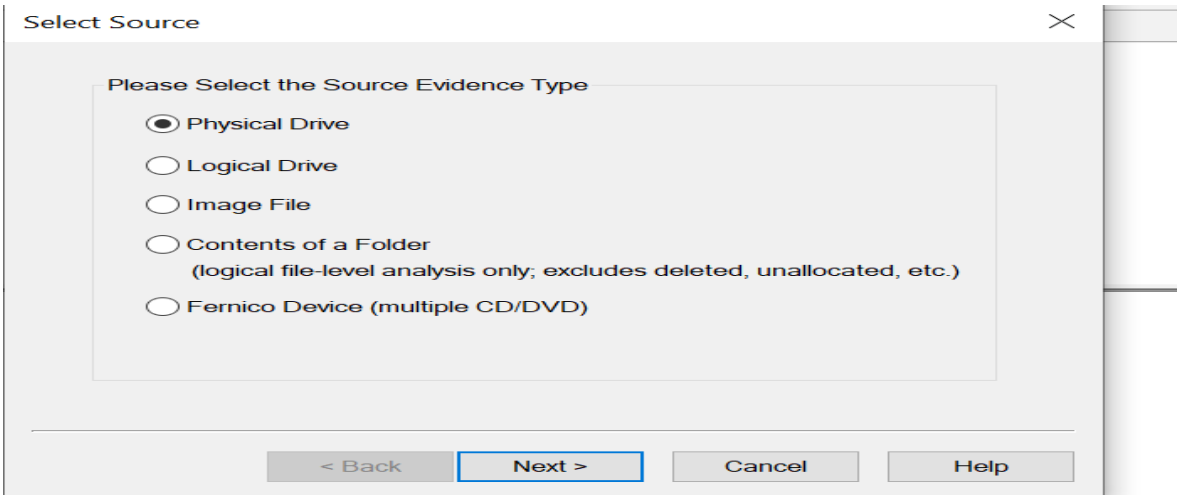
Add some random data in your USB, like simple docs and files then apply data acquisition on USB (Group USB) and make a report of the procedure you used to get data, and which format you used.

You should explain why you used certain method for acquisition. (Preferable is you must try bit-by-bit acquisition.)

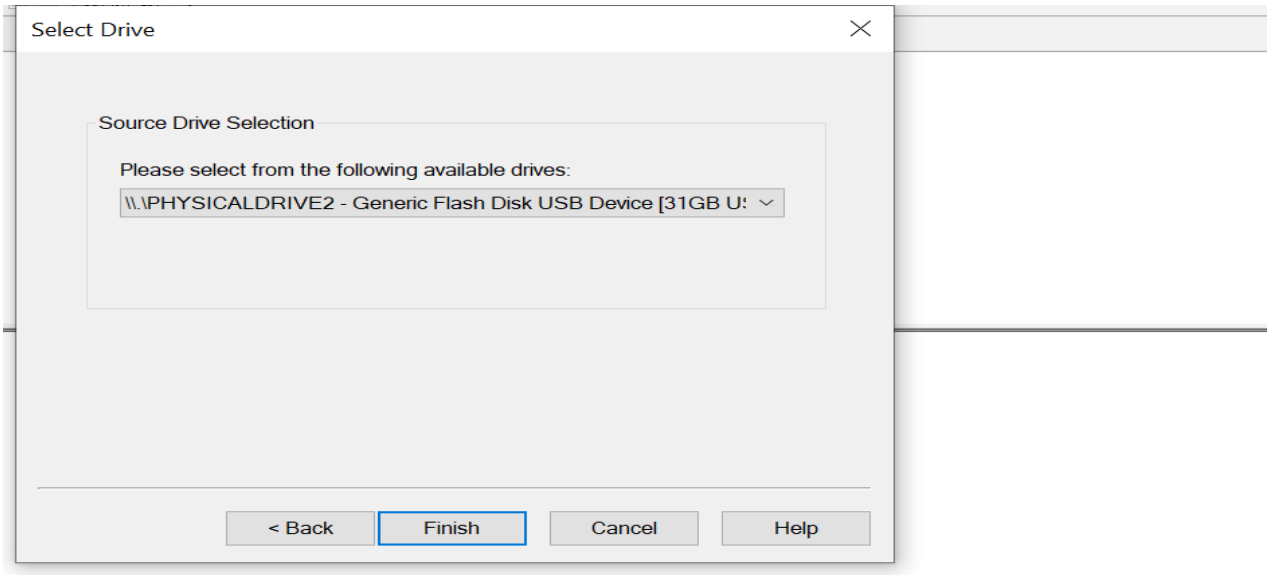
USB Content:

Name	Date modified	Type	Size
Image1	2/18/2025 12:49 PM	Python Source File	1 KB
Screenshot 2025-02-15 011130	2/15/2025 1:11 AM	PNG File	54 KB
Ahmad.txt	2/13/2025 6:49 PM	Text Document	3 KB

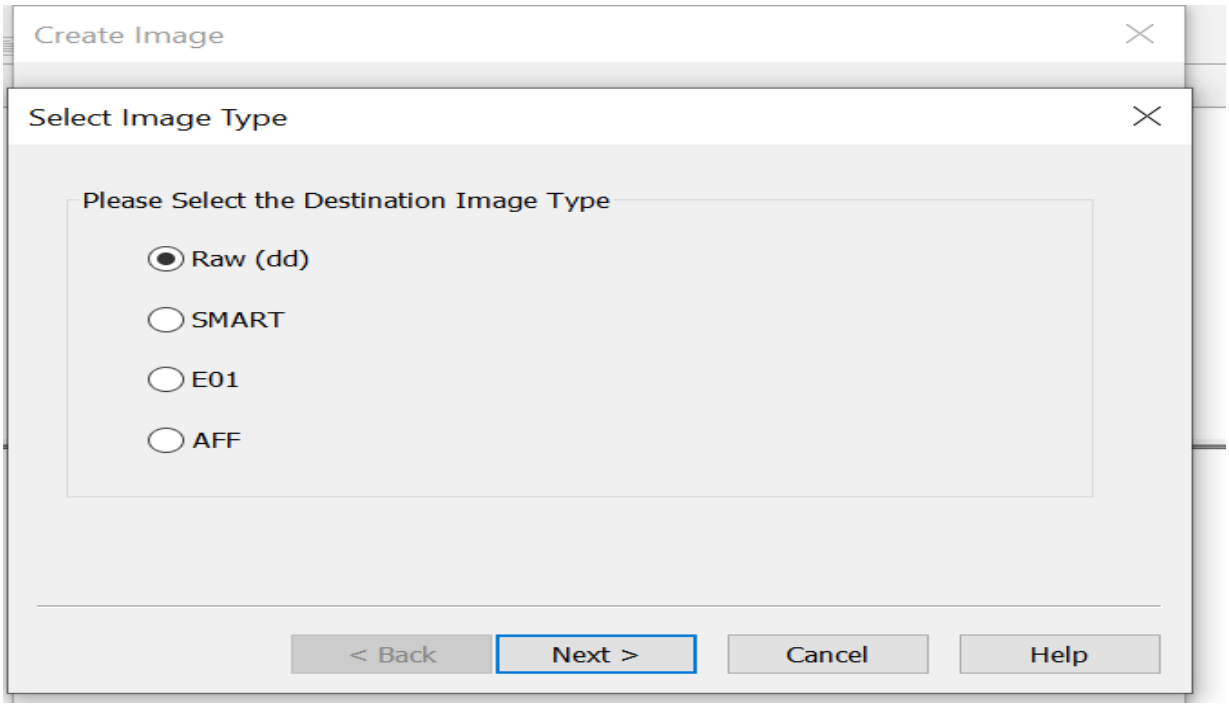
Create a Disk Image:



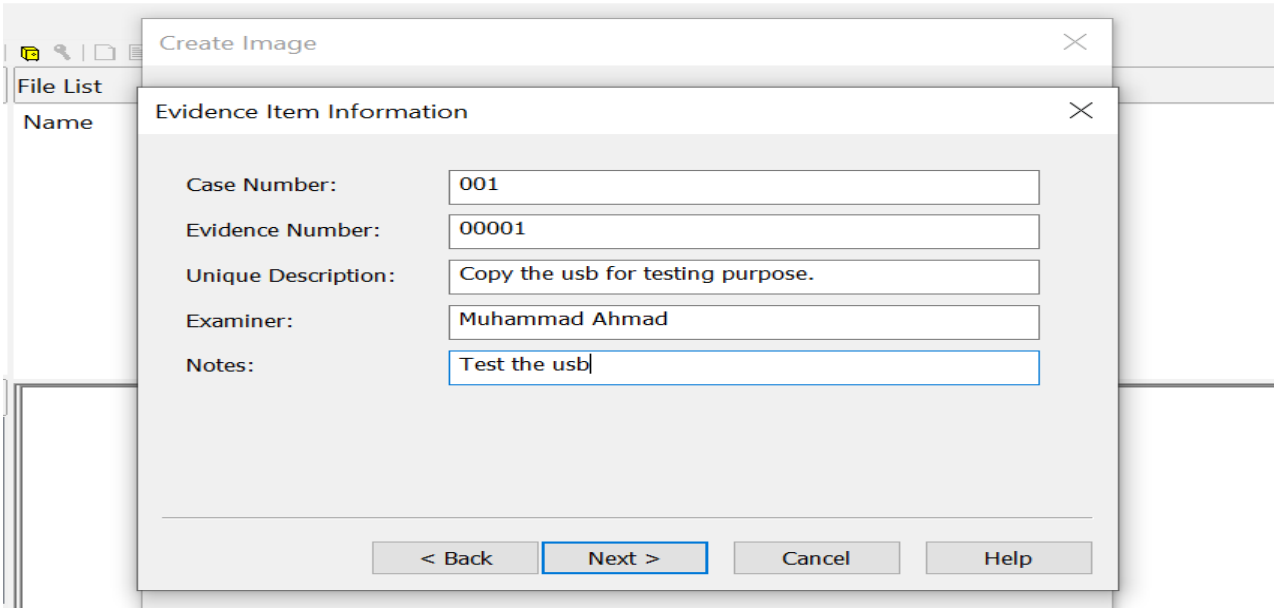
Select the usb for imaging bit by bit:



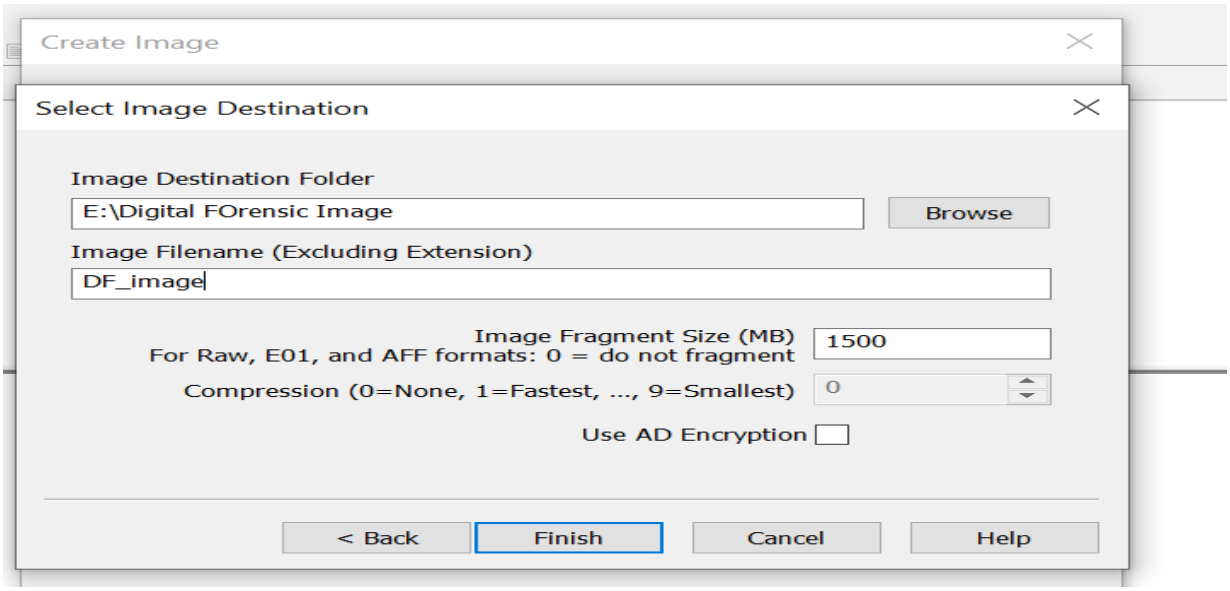
Select the Format:



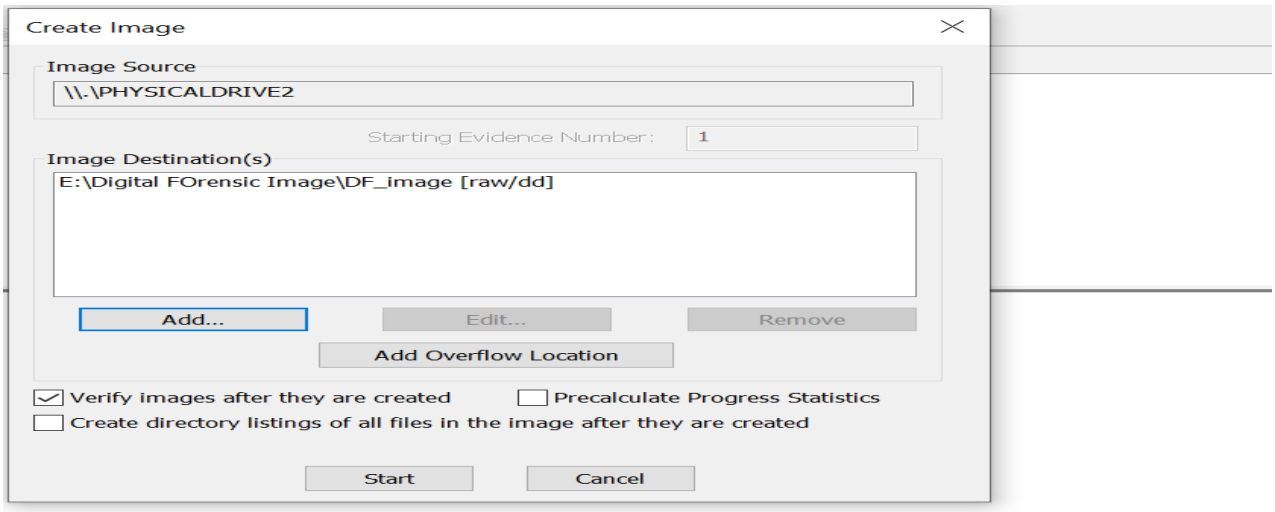
Evidence Image Inforamtion:



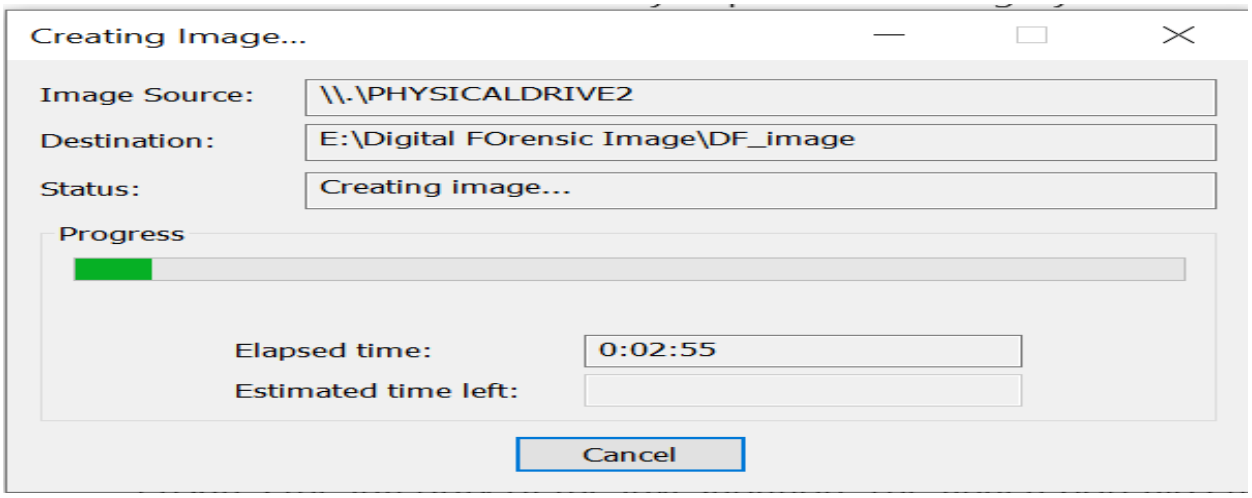
Store them in a file.



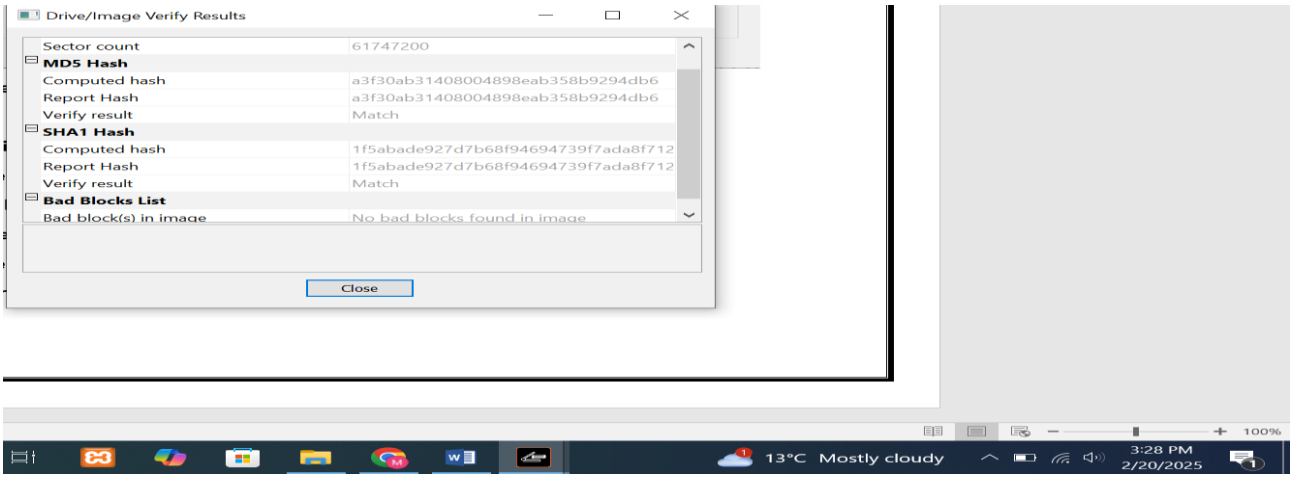
Verify the Images Hashes:



Click the start button:



Verify the hashes:



Select the image created:

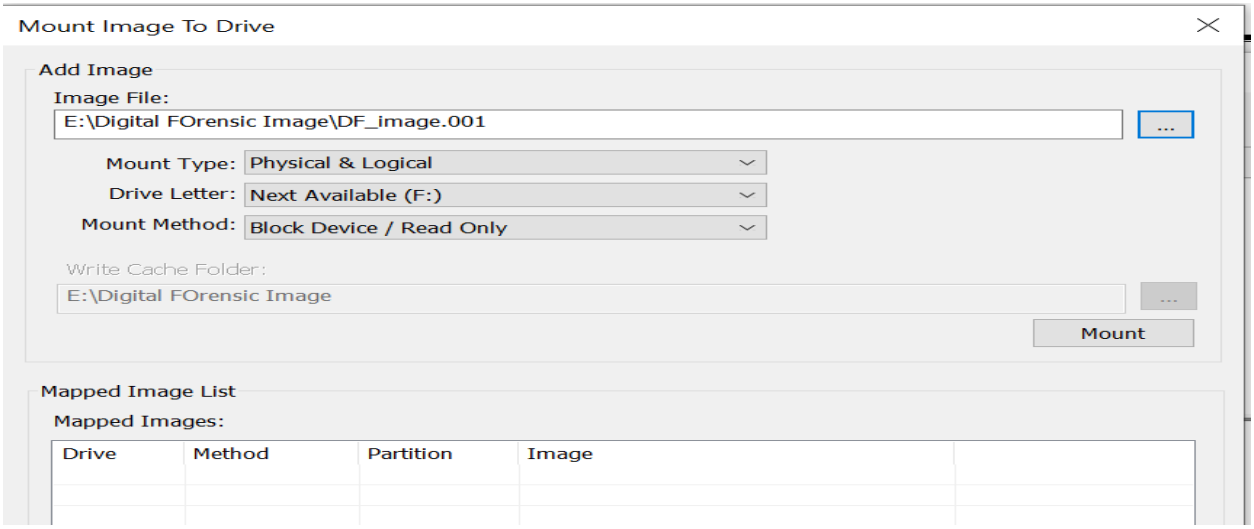
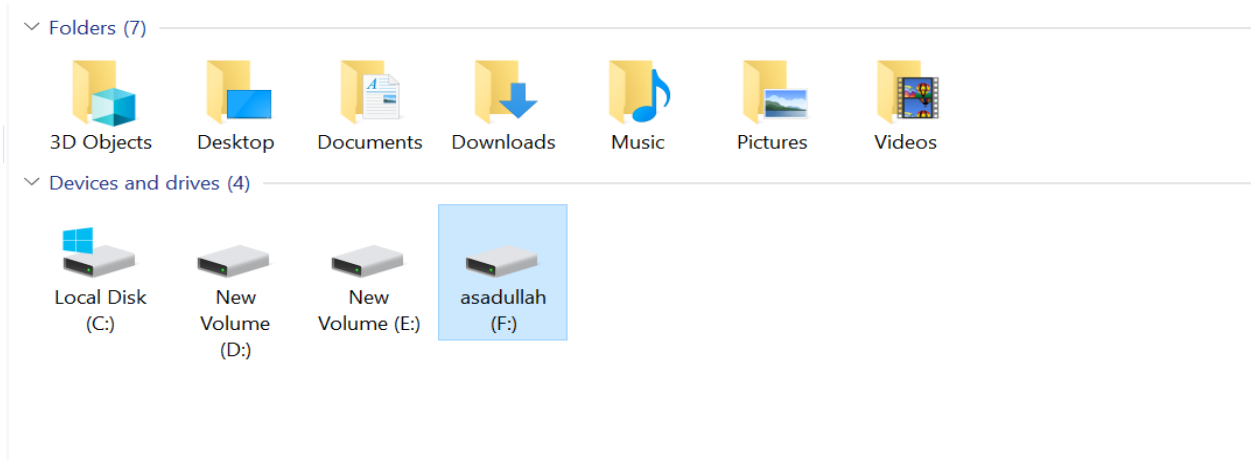
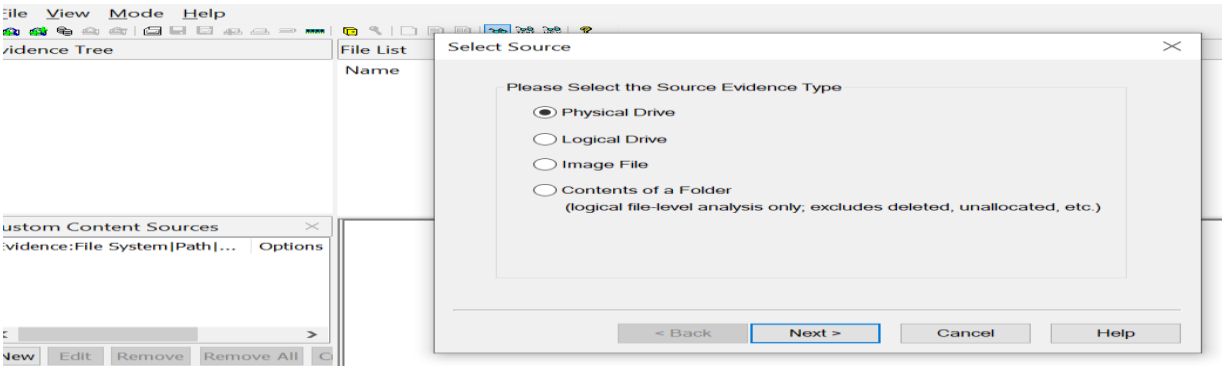


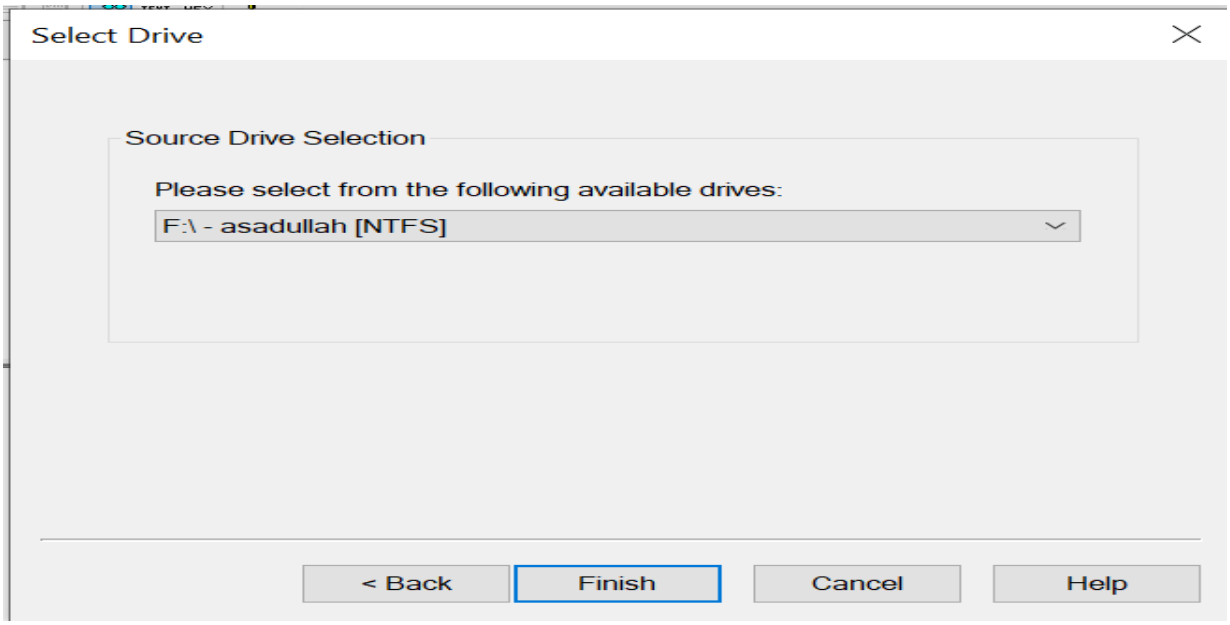
Image will be mounted and also appeared physical disk in the computer:



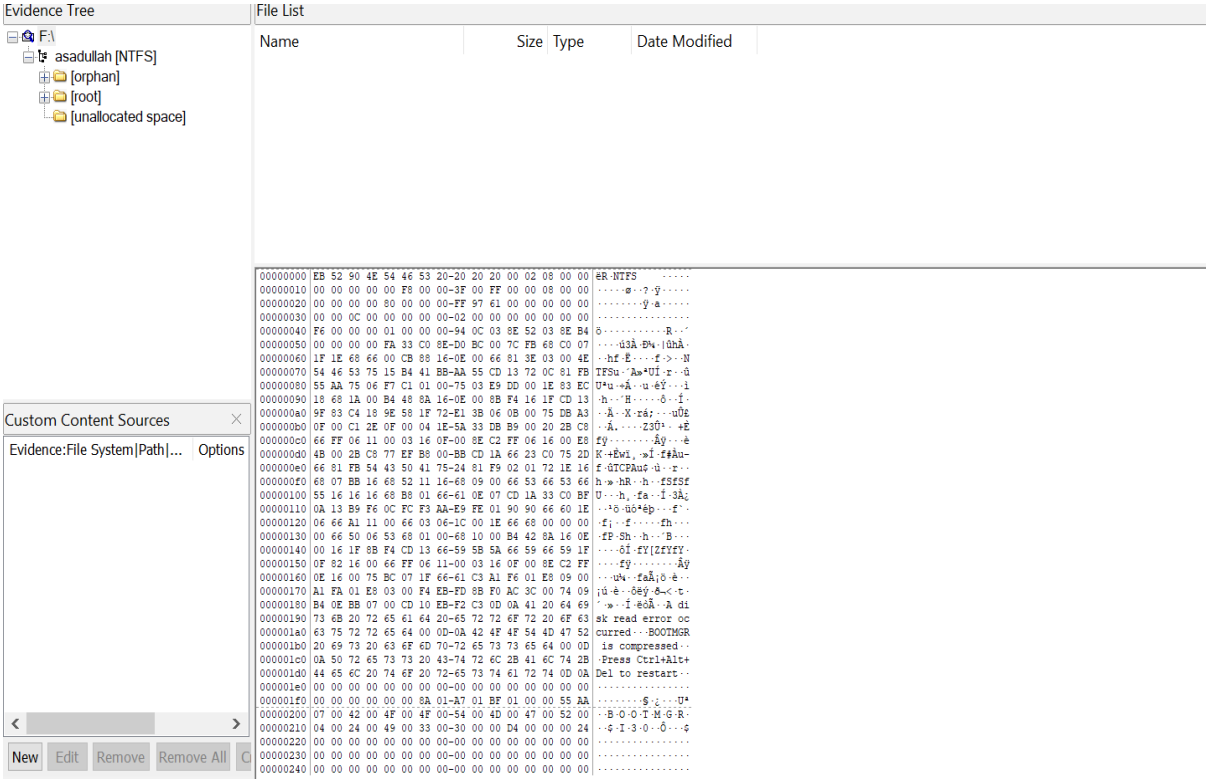
To see the contents of the image:



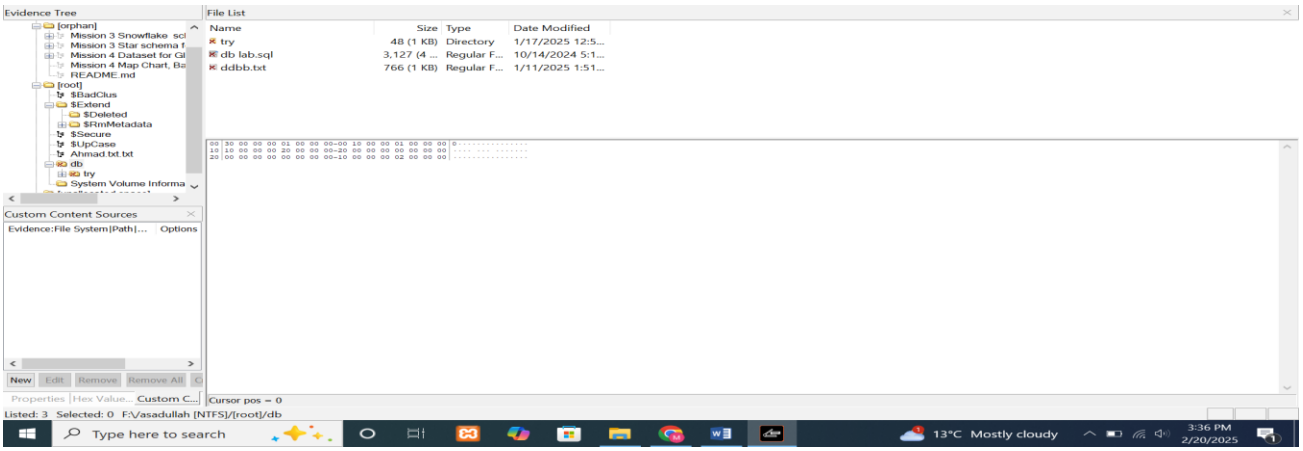
Select the drive that was mounted:



Click on the finish:



See the deleted Files:



See the File Content: