ASSIGNMENT # 1
DIGITAL FORENSICS

WAQAS MAQSOOD
REG# 24109121
MS CYBER SECURITY

Submitted to: Sir Muhammad Waqar

TASK # 1: Set USB to "Read-Only" Mode When Inserted into a System

To prevent any accidental modifications or data tampering, the goal is to configure the USB drive so that it becomes read-only when connected to a system. This ensures that the data on the USB can only be viewed and not altered.

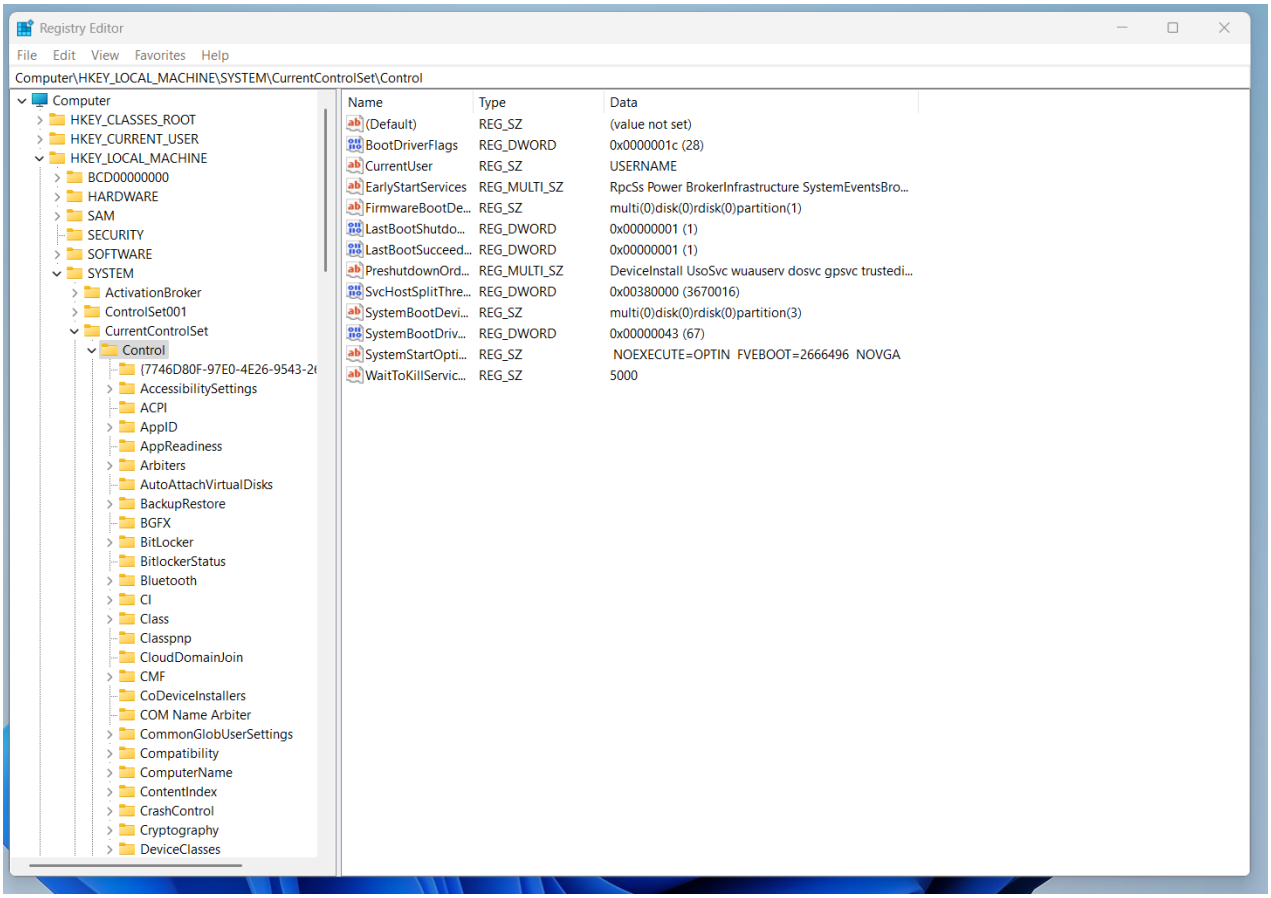
1.Open the Registry Editor:

- Press **Win + R** to open the **Run** dialog box.
- Type regedit and press **Enter**.

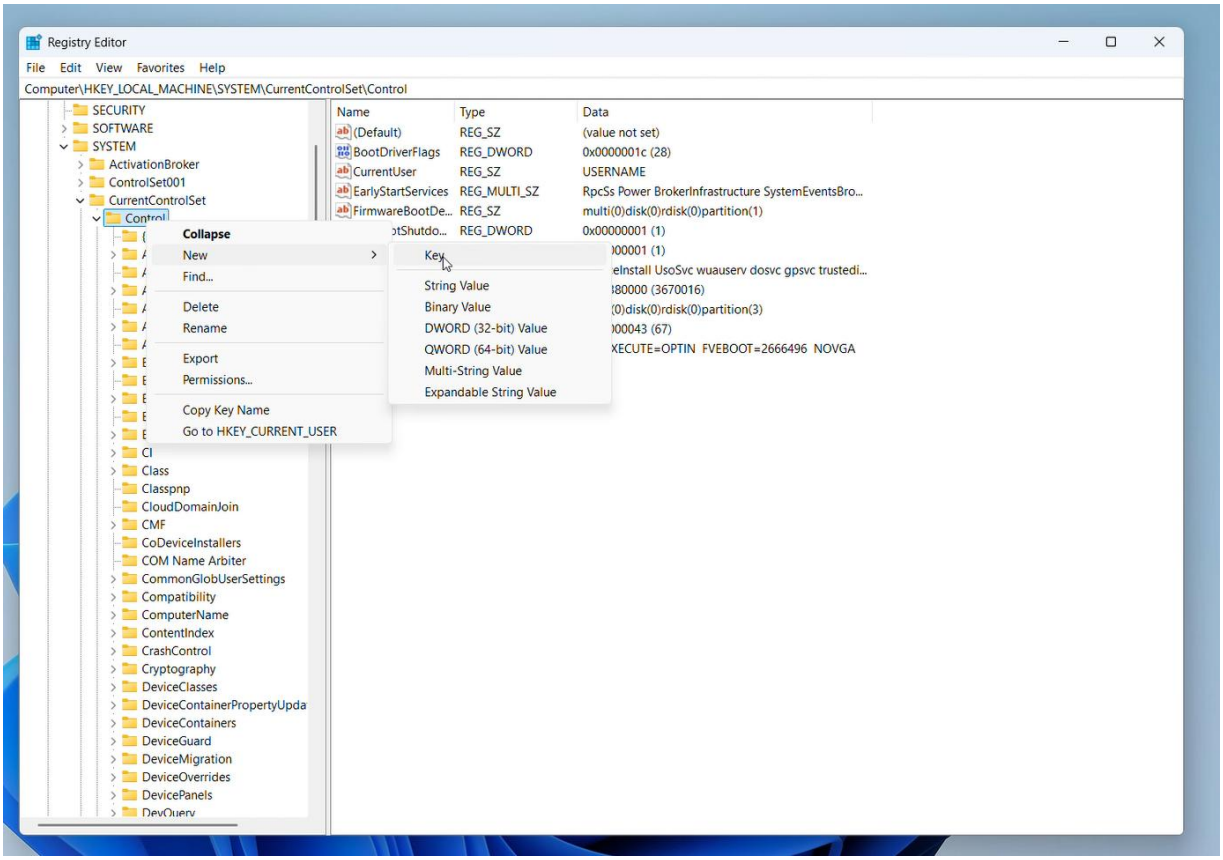
2. Navigate to the USB Storage Key:

- In the Registry Editor, go to the following path:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control

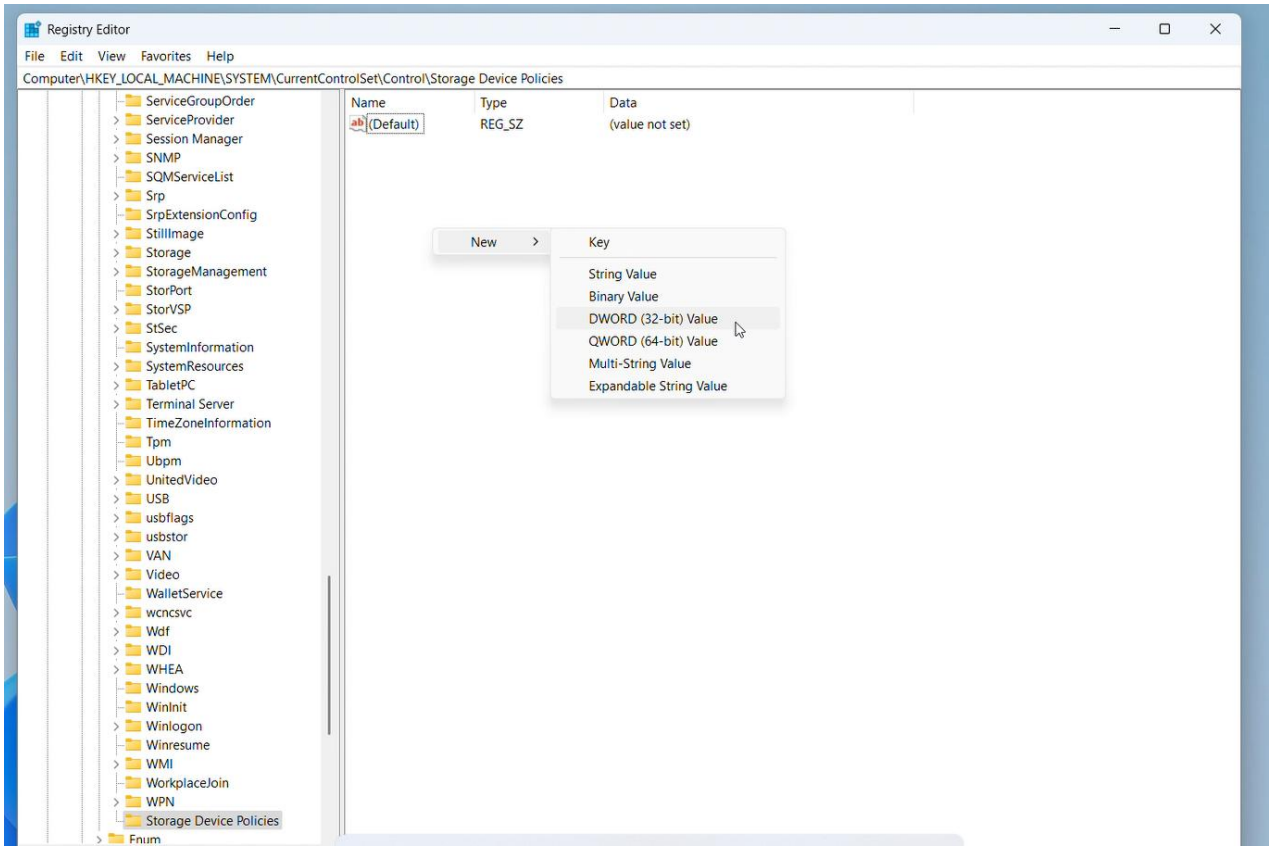


3. Scroll down and look for the **"StorageDevicePolicies"** key. If you don't see it, you may need to create it (right-click on **Control → New → Key**, and name it **StorageDevicePolicies**).

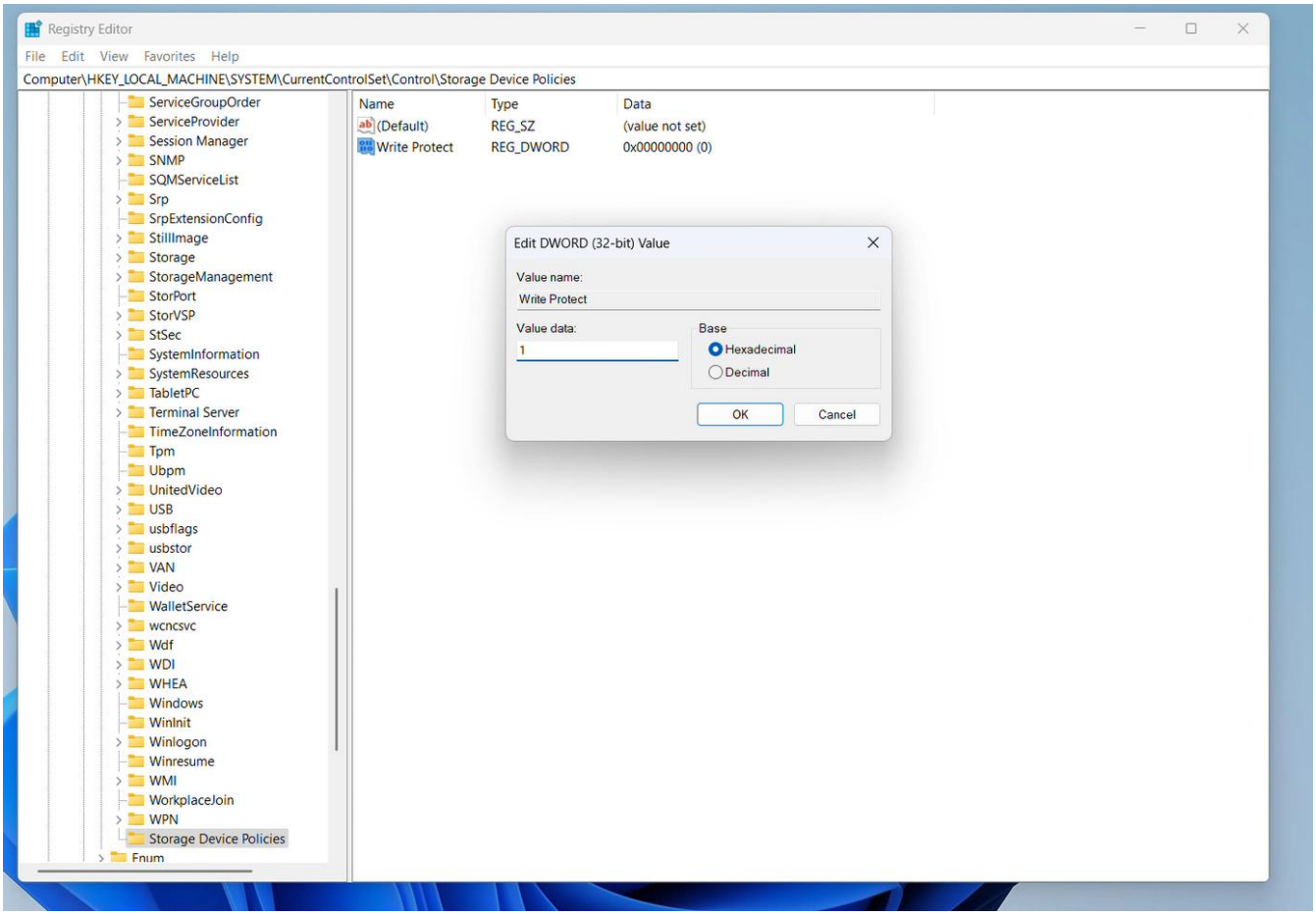


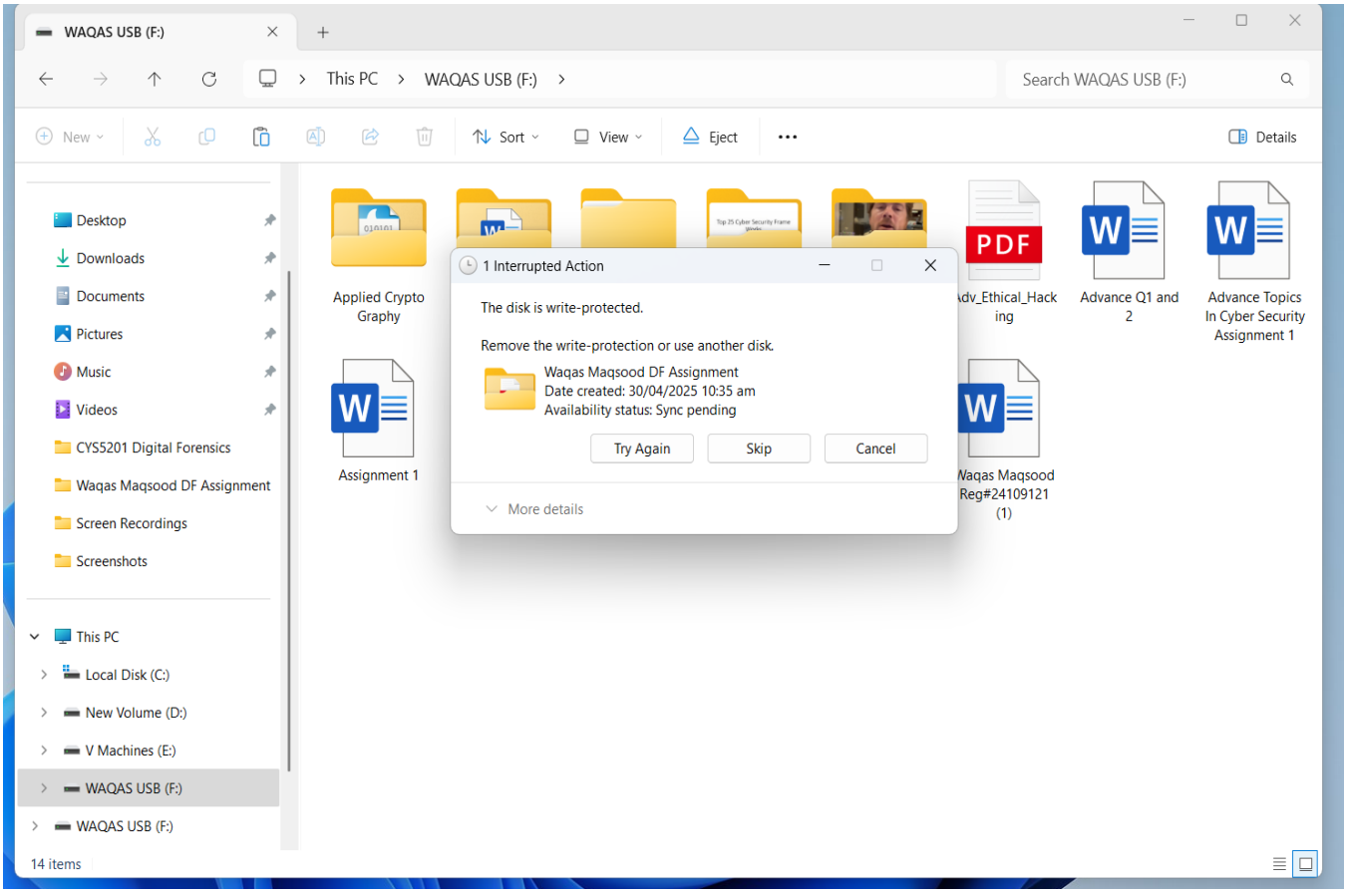
4.Create the WriteProtect Value:

Once inside the StorageDevicePolicies key, right-click in the right pane and choose New → DWORD (32-bit) Value.Name the new value WriteProtect.



5.**Set WriteProtect to 1**: Double-click on **WriteProtect** and change the **Value data** to 1 to enable read-only mode then click **OK**.





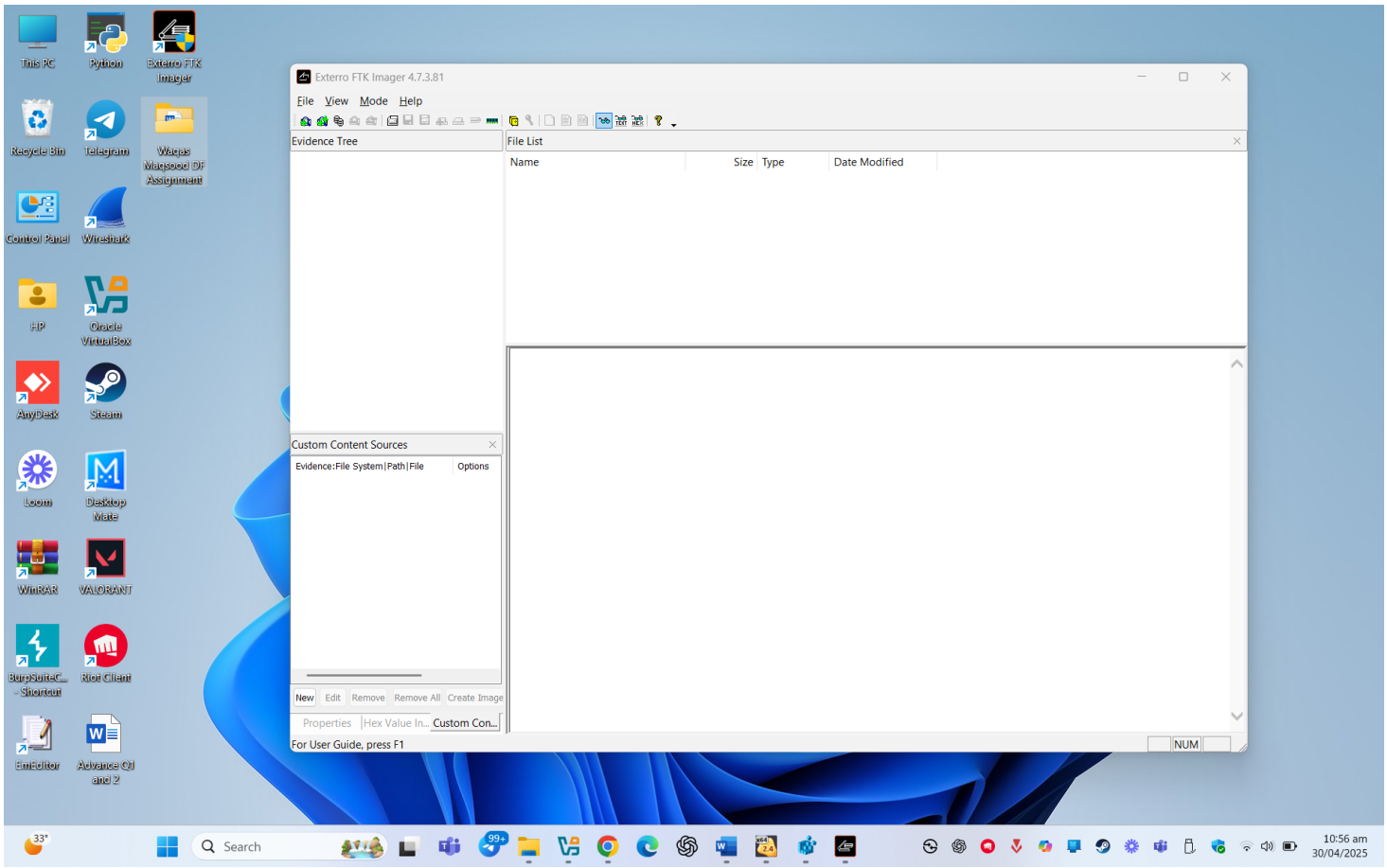
Conclusion:

In this task, we successfully created a **read-only environment for the USB device** to ensure the integrity of digital evidence. By modifying the Windows Registry and/or using diskpart, we prevented any accidental write operations. A **system restart** was required for the changes to take effect. This setup is crucial in digital forensics to maintain evidence in its original state.

TASK # 2: Forensic Imaging and Analysis: Creating a DD Image and Investigating with Autopsy

Step 1: Launching FTK Imager for Image Creation

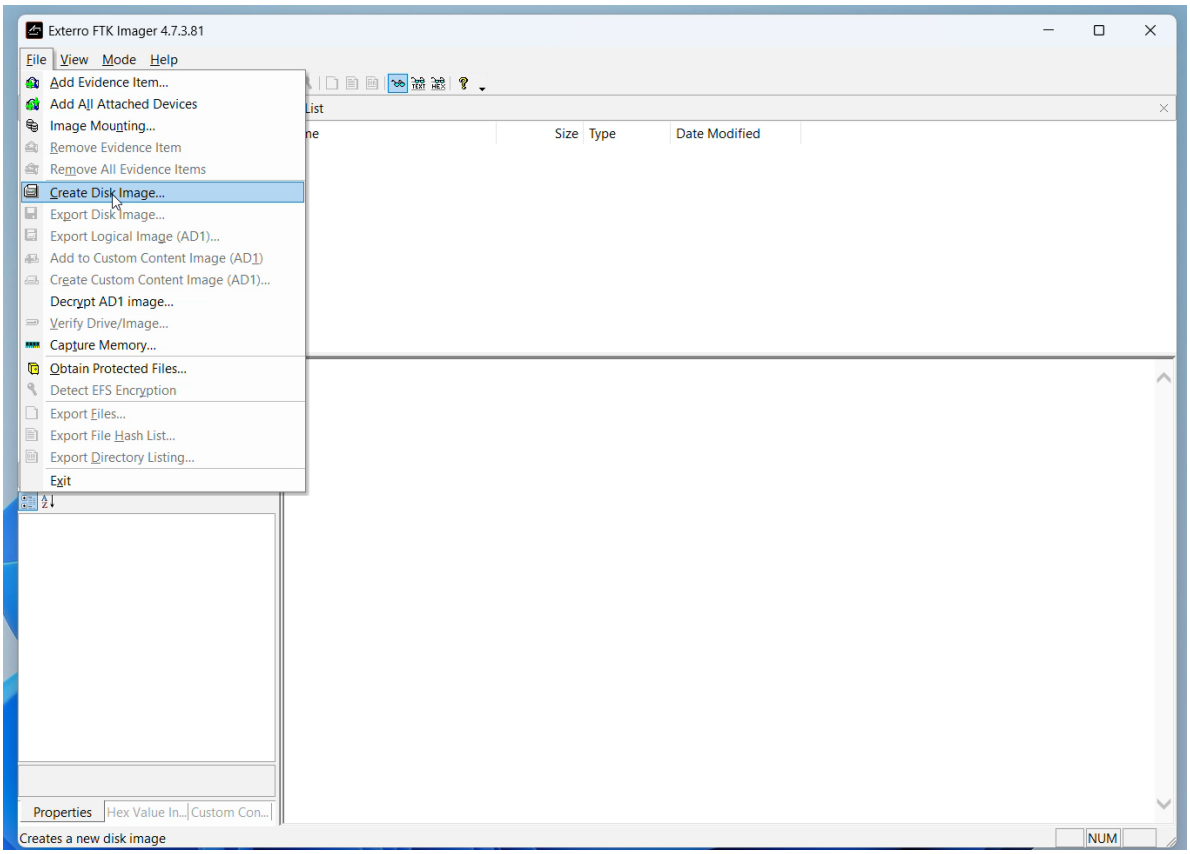
First, I opened **FTK Imager**, a forensic imaging tool, to create a disk image of the target USB drive. FTK Imager allows capturing an exact bit-by-bit copy DD image (also known as a **raw disk image)** of the drive, which is essential for forensic analysis without altering the original data.



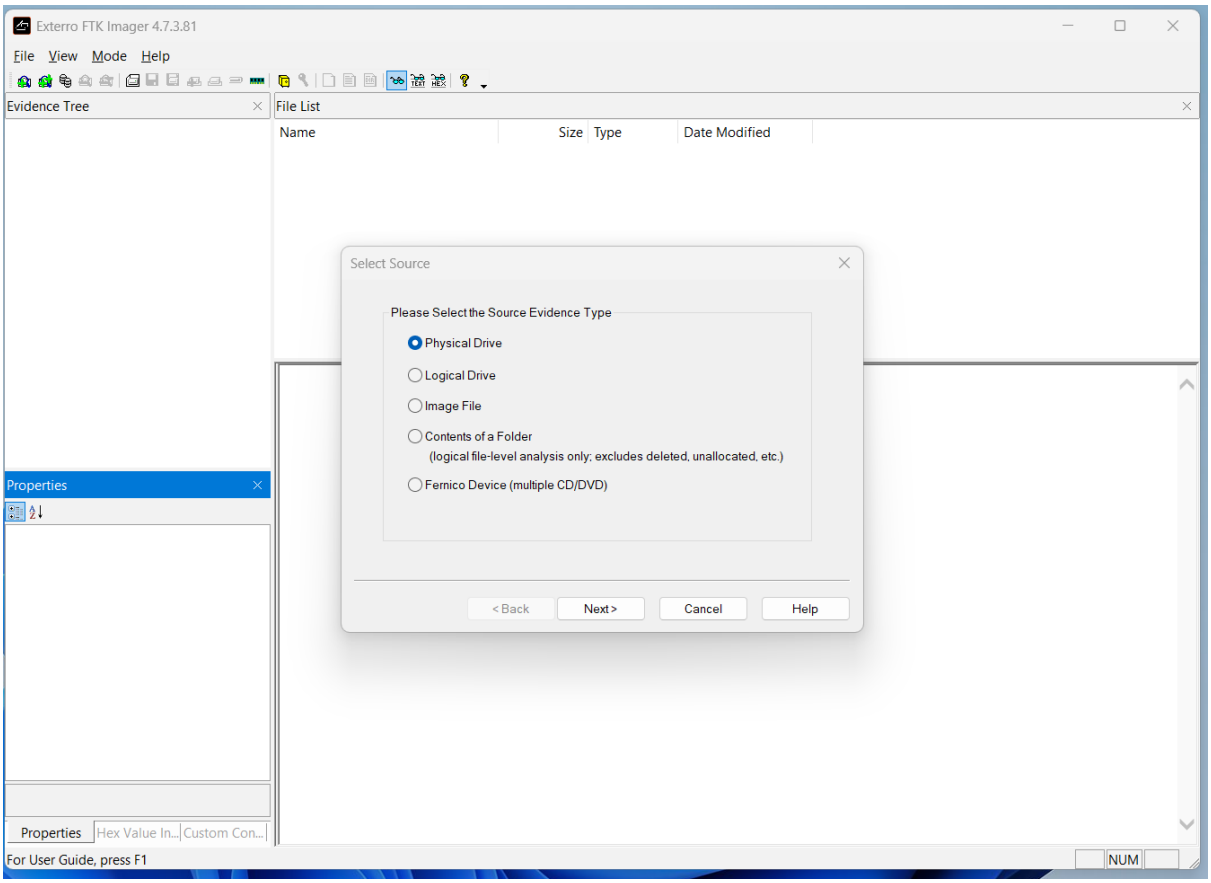
Step 2: Creating a Disk Image Using FTK Imager

After launching FTK Imager, I followed these steps to create a forensic disk image:

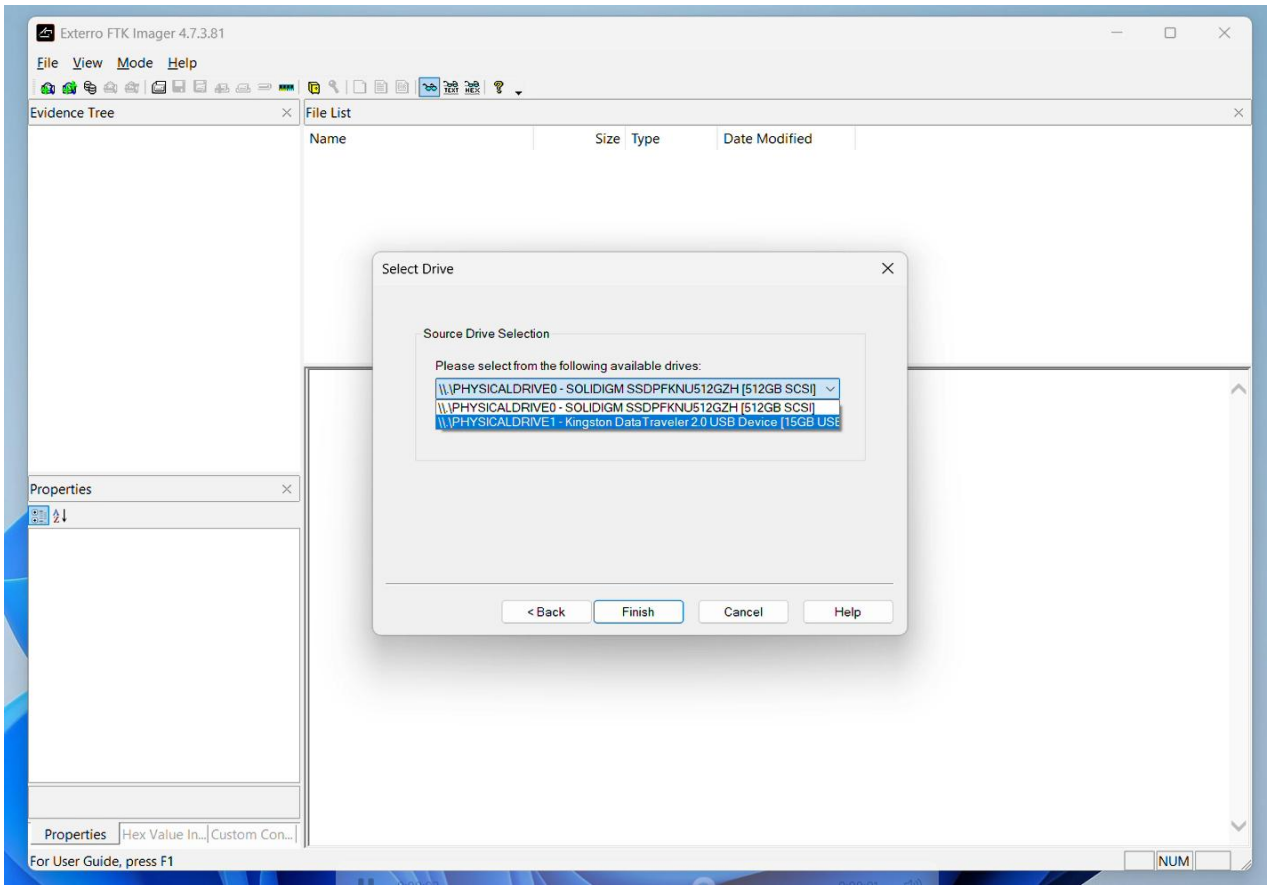
1.Clicked on **"File"** in the top menu, then selected **"Create Disk Image"**.



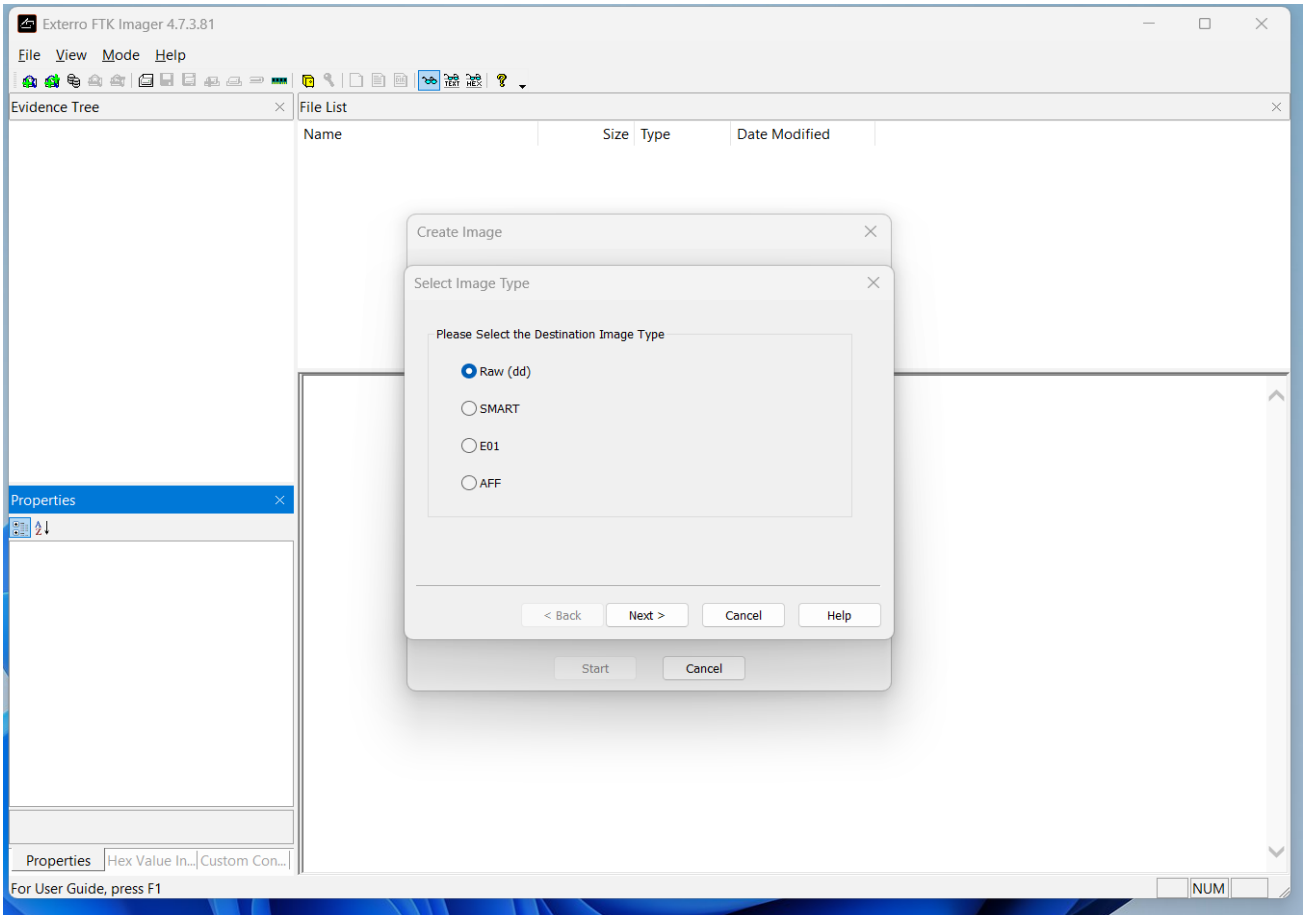
2.In the dialog box, chose the source type (e.g., **Physical Drive** or **Logical Drive**) depending on the target.



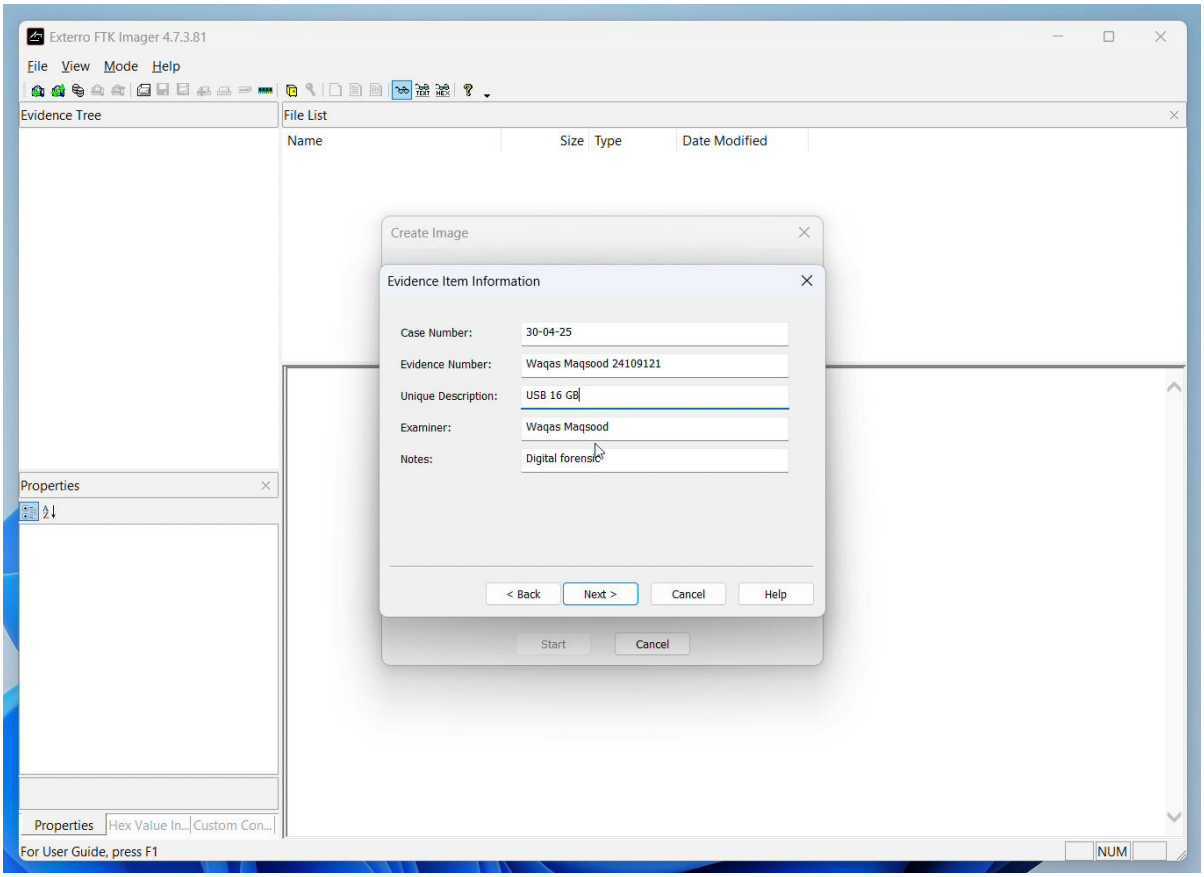
3. Selected the correct drive I wanted to image. From the list, I **selected my USB drive.**



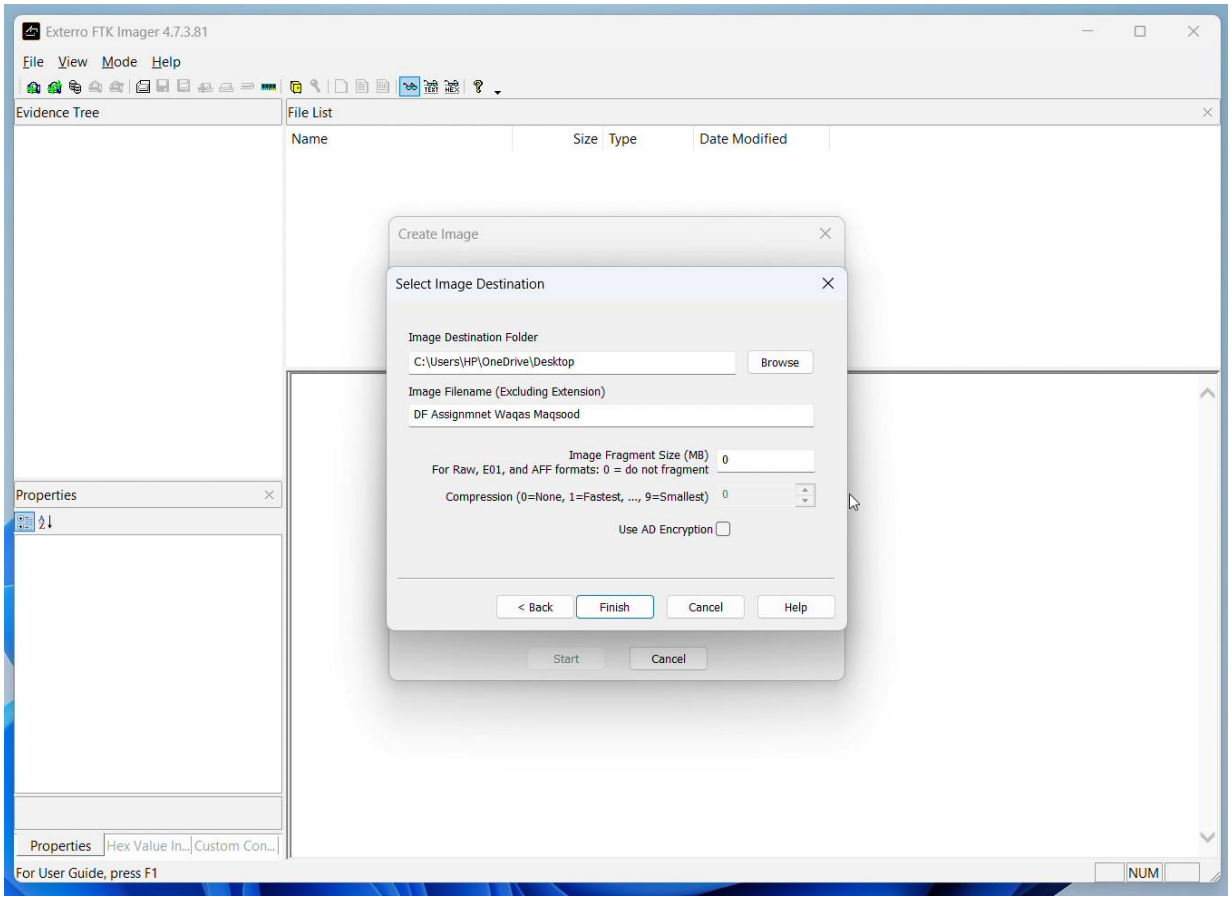
4. Selected **"Raw (dd)"** as the image type to get a bit-by-bit copy.



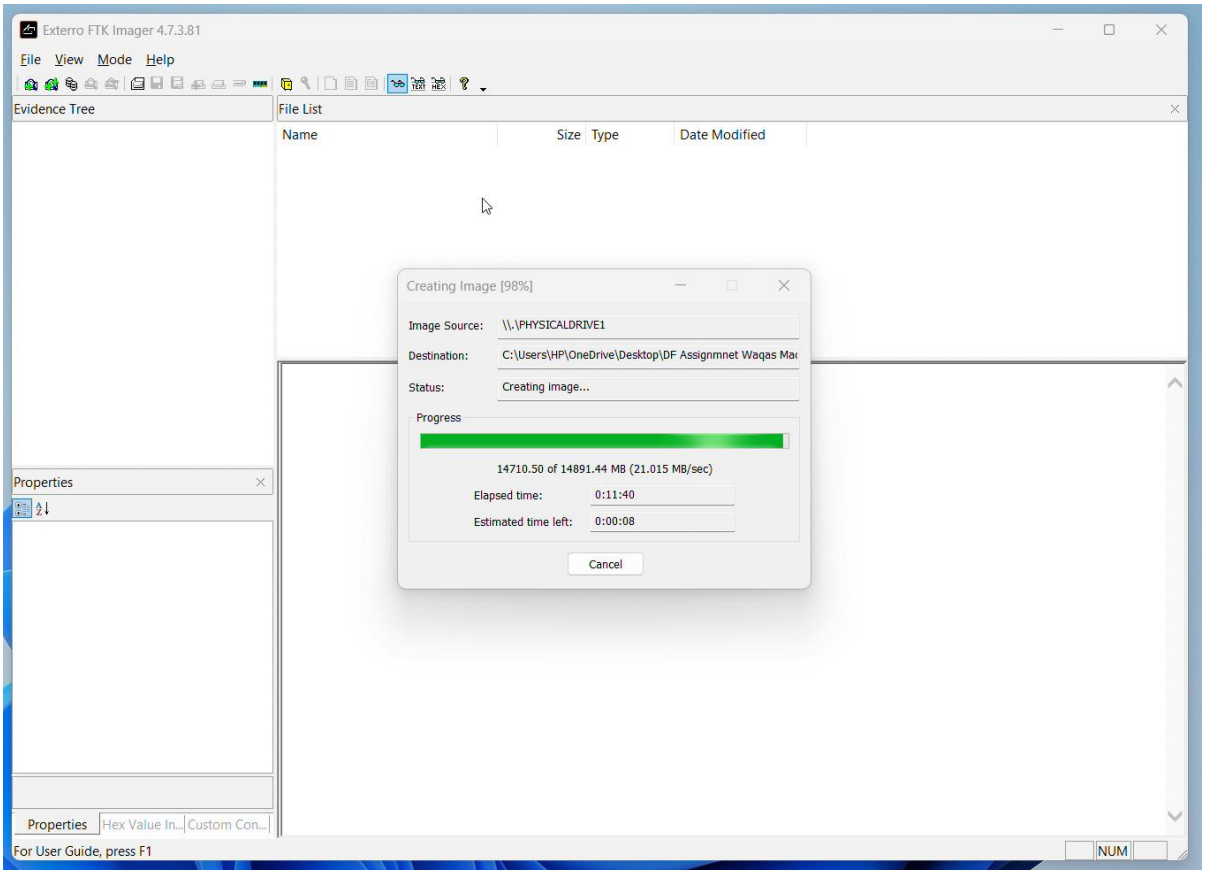
5. Entered optional **case details** for documentation (e.g., case number, examiner name).



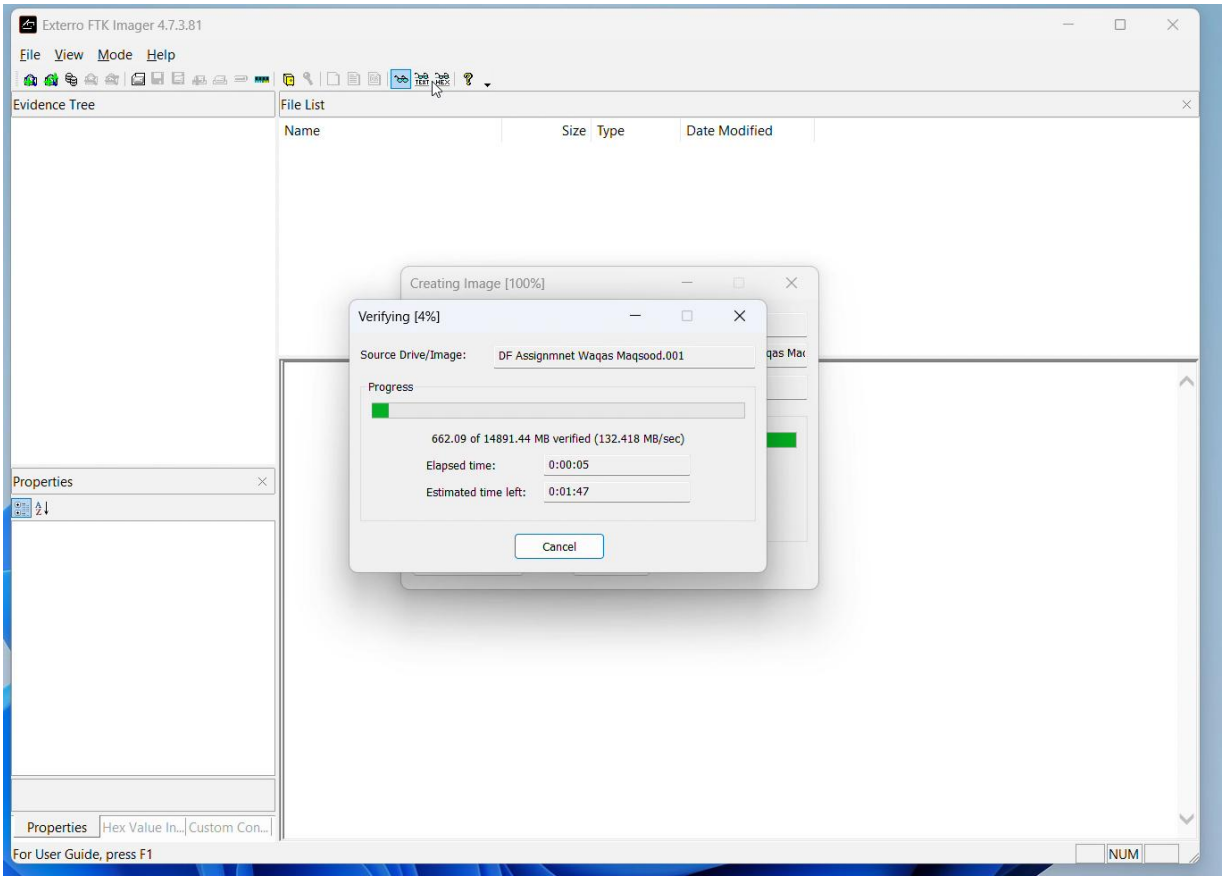
6. Set the **image fragment size to 0**, which means the image will not be split and will be saved as a single .dd file. Chose the destination folder and named the file DF ASSIGNMENT WAQAS MAQSOOD. Clicked **"Finish"** to start creating the image.



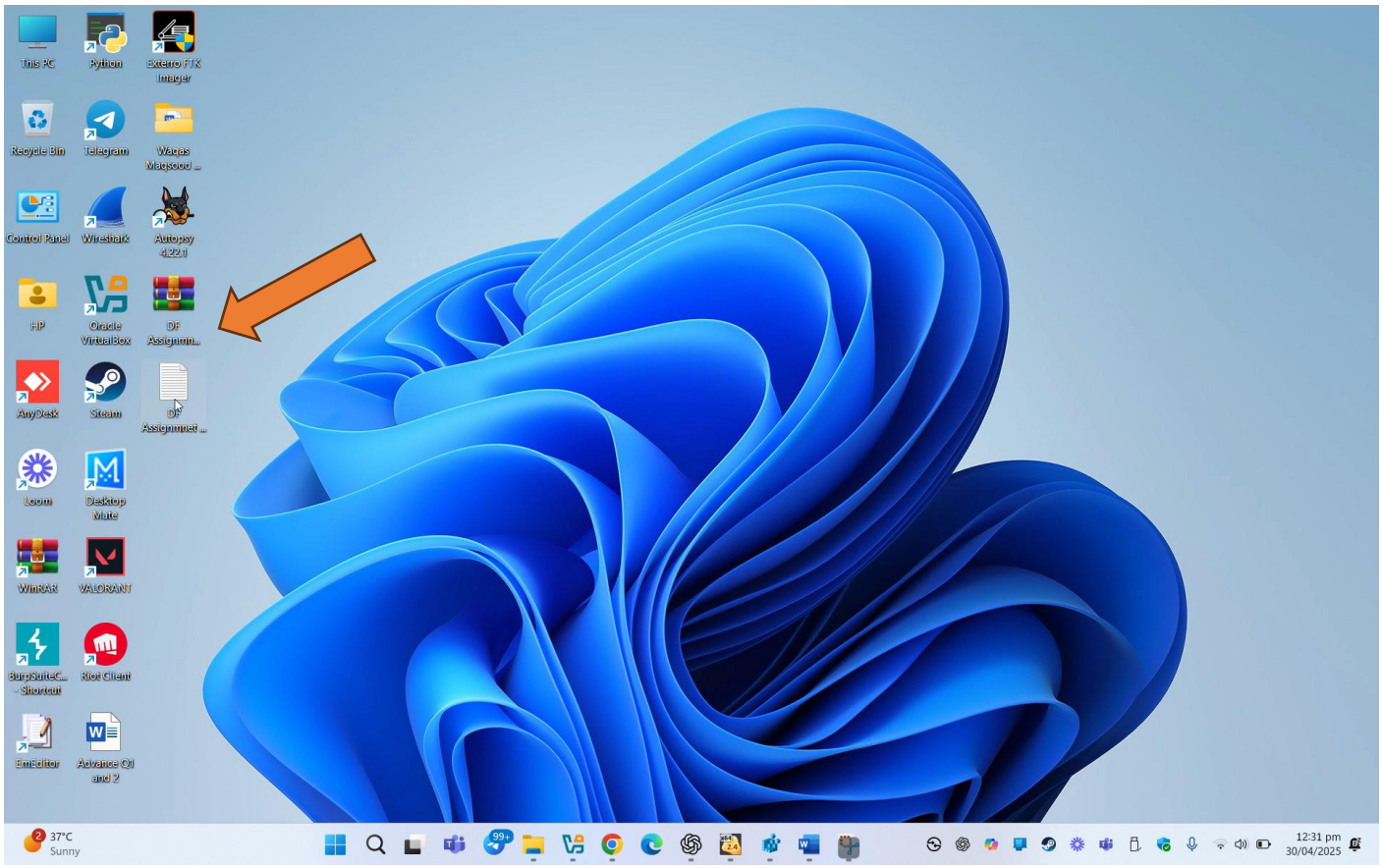
7. Once I clicked **"Finish"**, FTK Imager began creating the DD image of the USB drive. The **progress bar** displayed the status of the imaging process in real-time.



8. FTK Imager also **calculated MD5 and SHA1 hashes** during the process to ensure the integrity of the image. These hashes help confirm that the image is an exact, untampered copy of the original device.



9. The image is now ready for forensic analysis.

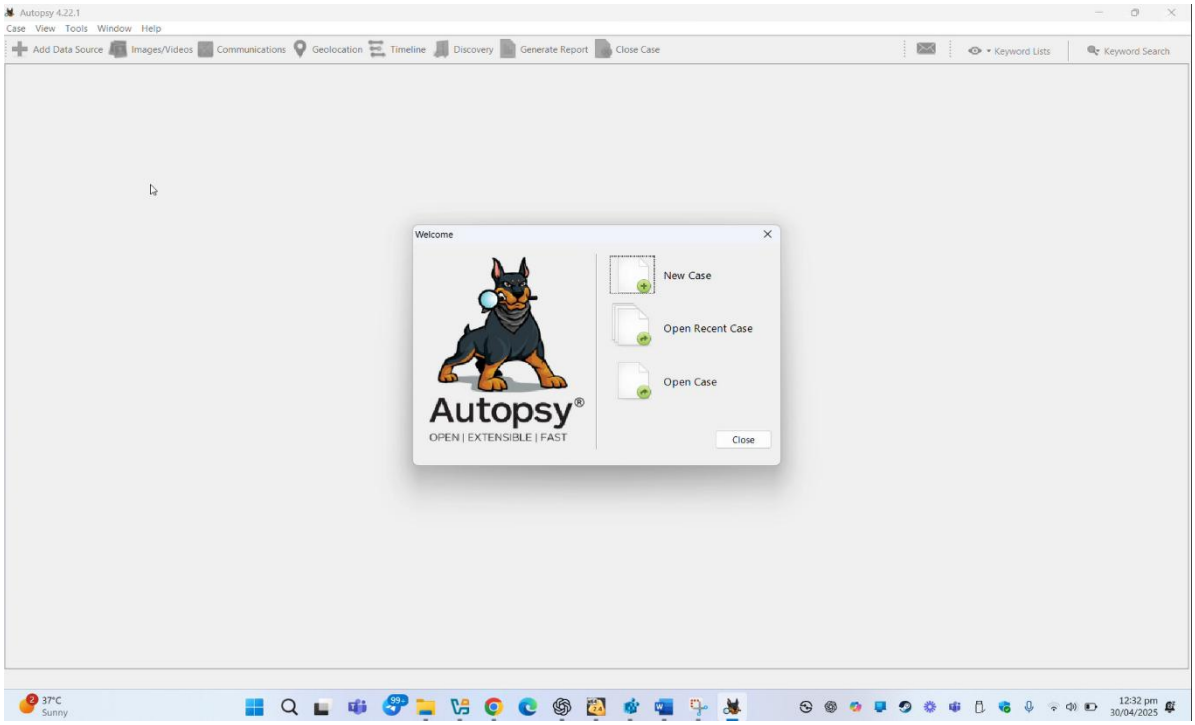


10.This completed the creation of a verified and hash-checked DD image of my USB drive, ready for forensic analysis in **Autopsy.**

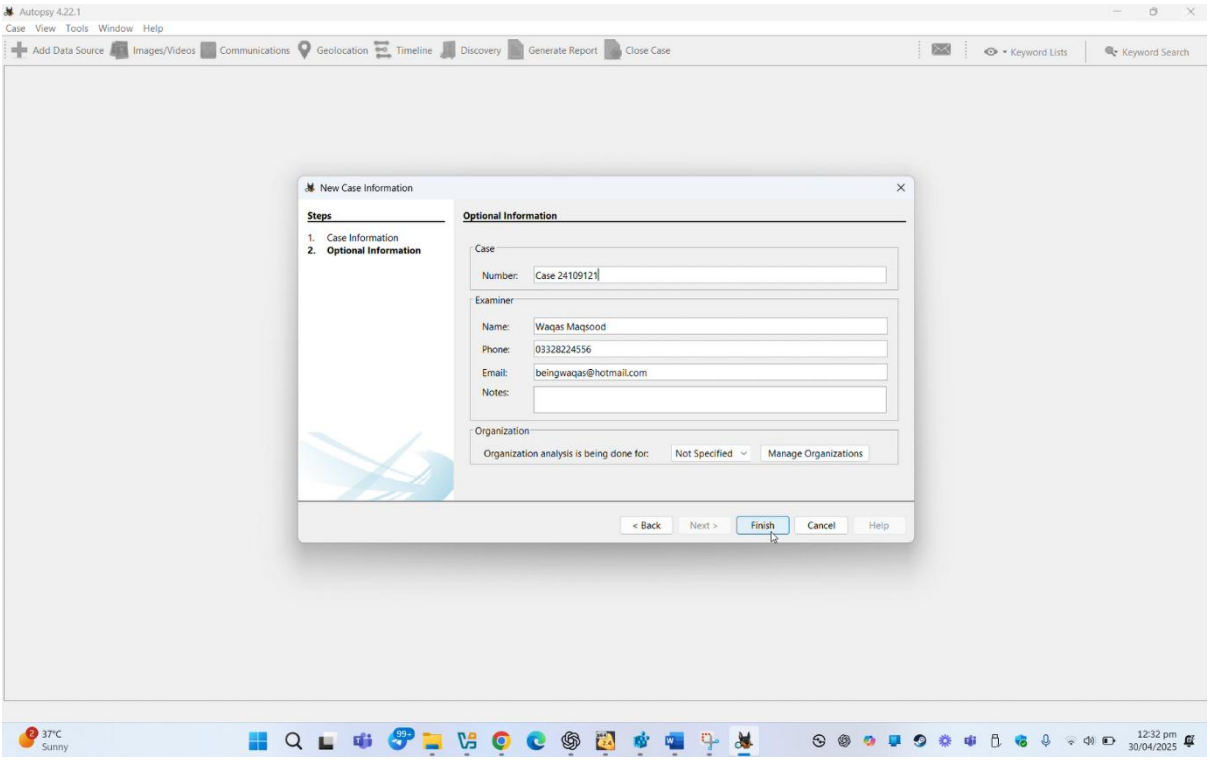
Analyzing the DD Image Using Autopsy

After creating the .dd image, I used Autopsy, a digital forensics tool, to analyze the contents of the image. Here are the steps I followed:

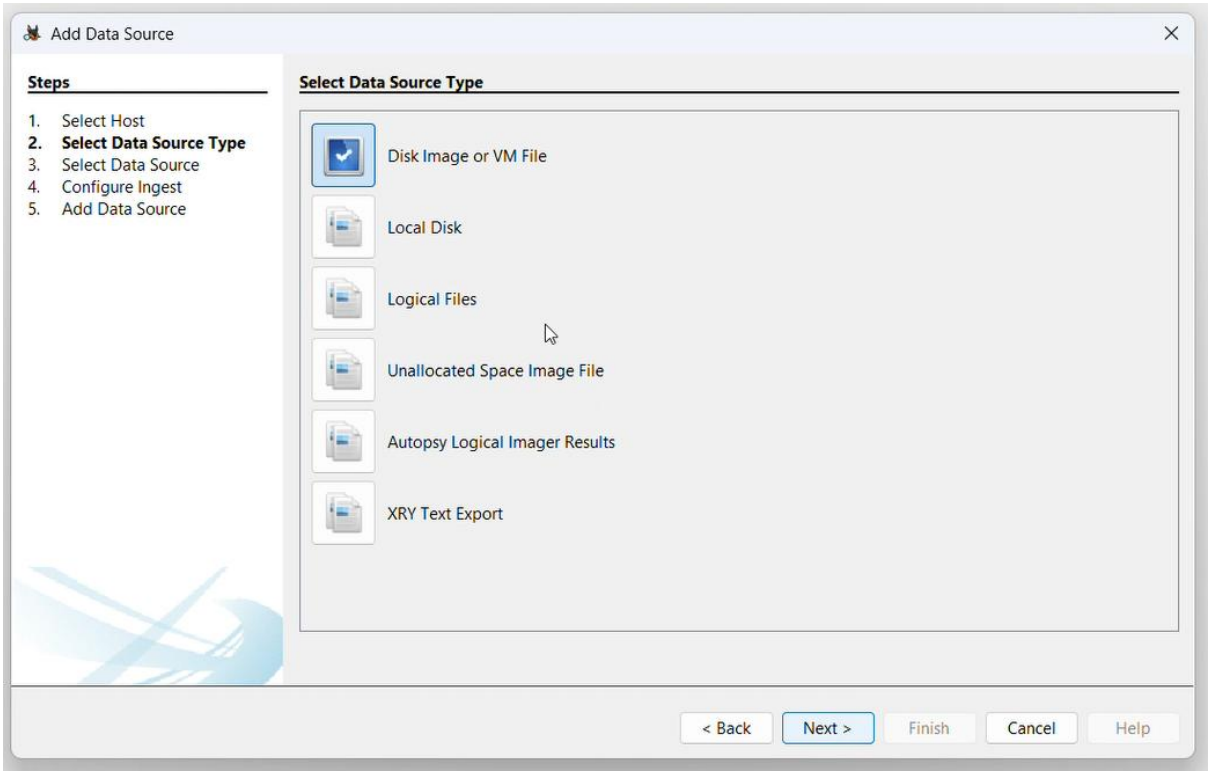
STEP 1: Opened **Autopsy** and clicked on **"Create New Case"**.

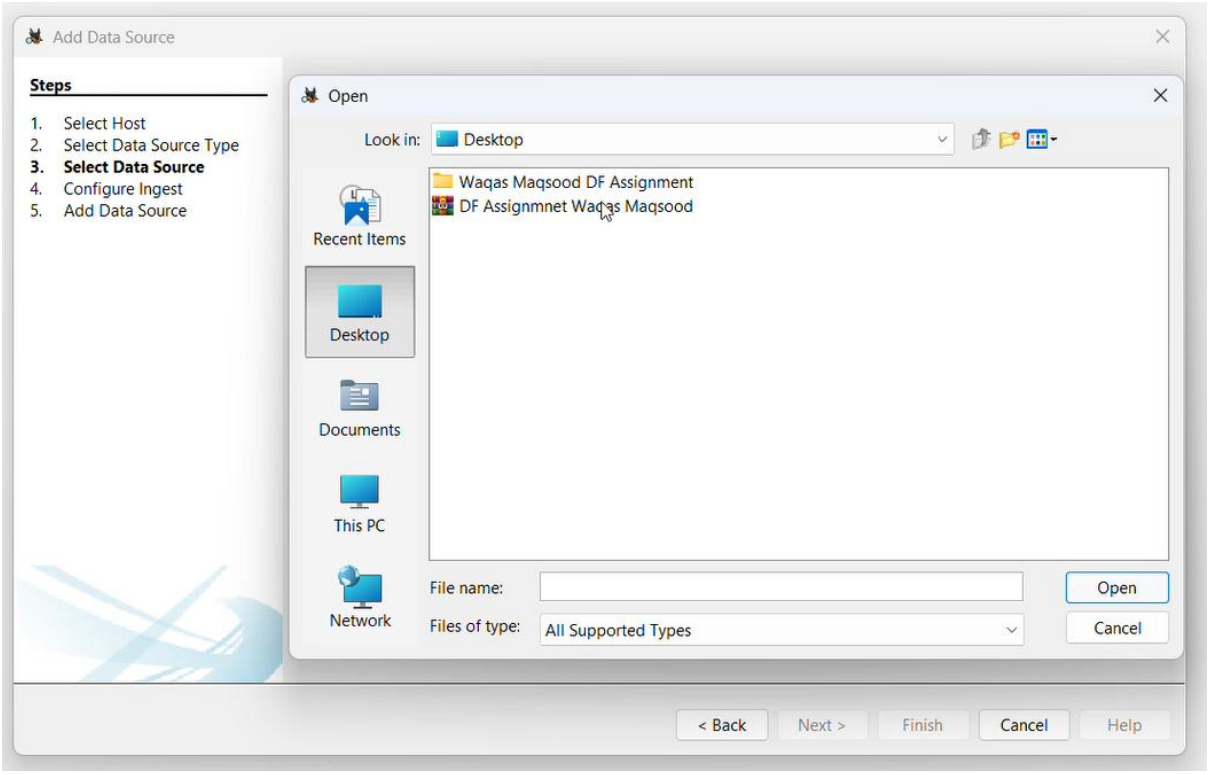


STEP 2: Entered the **case name**, **base directory**, and optional case details (e.g., examiner name).

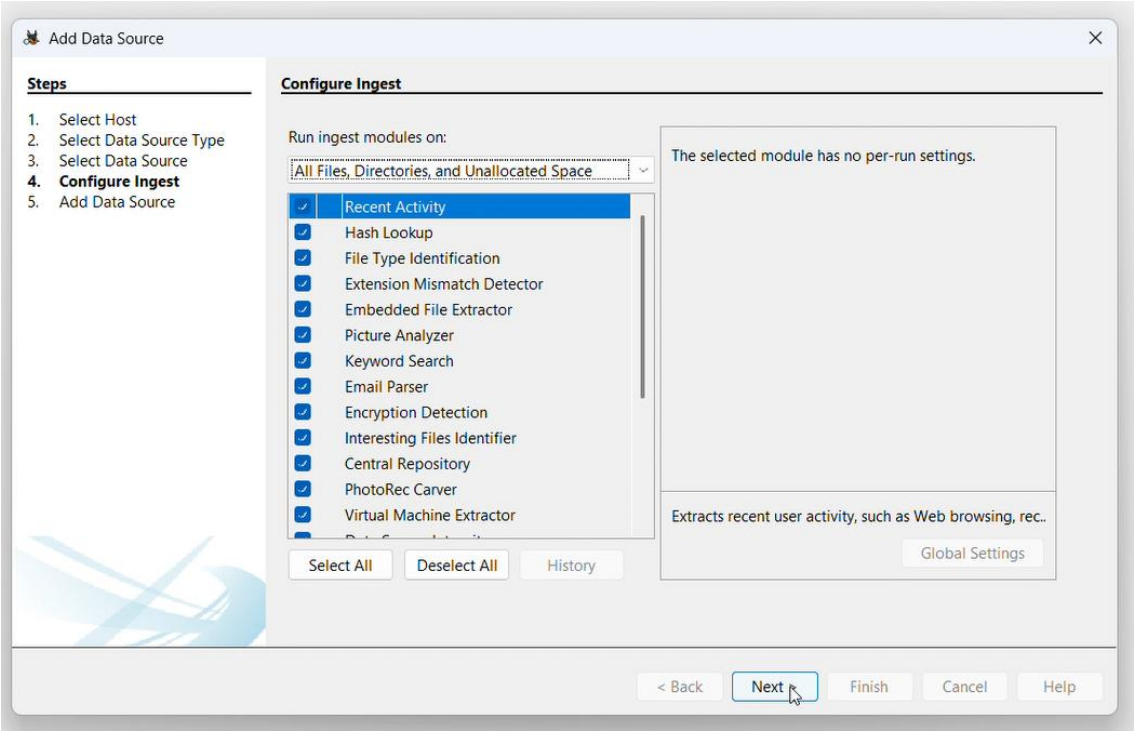


STEP 3: Clicked **"Next"** to proceed, then selected **"Add Data Source"**.

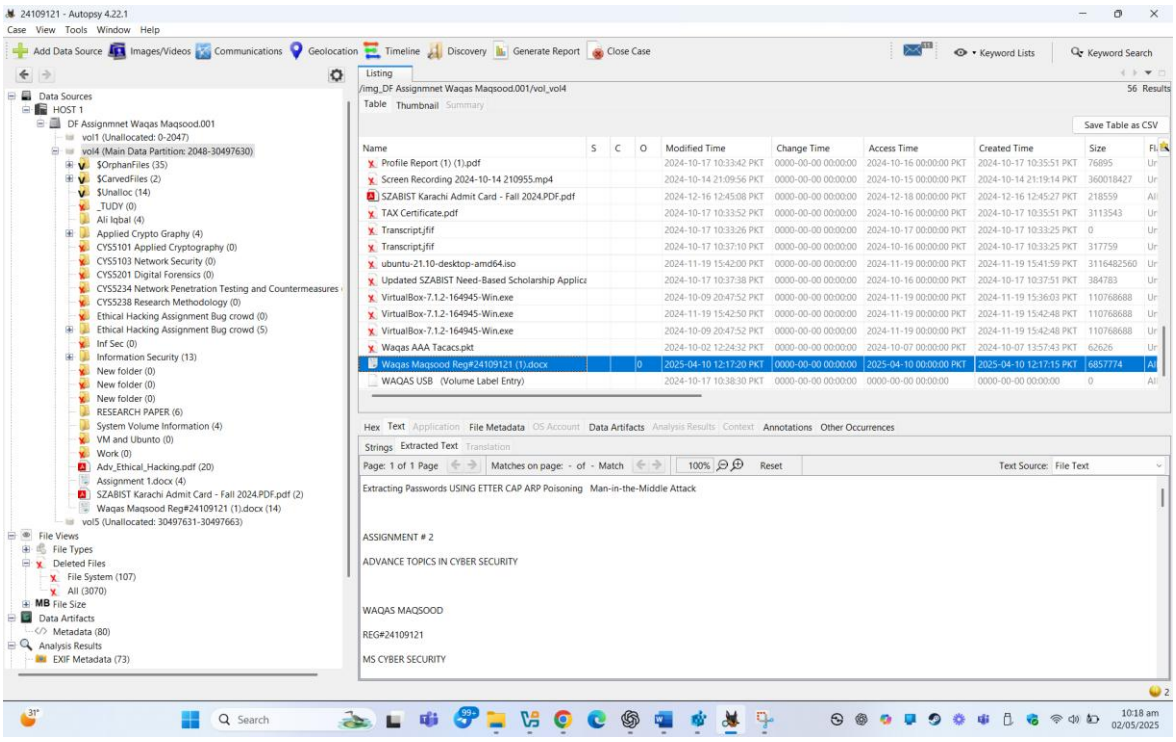




STEP 4: In the Ingest Module Configuration screen, I selected important modules needed for analyzing files, web activity, deleted data, and keywords then click next.



STEP 5: Autopsy began analyzing the image using the selected modules. After a short time, results started appearing, including active files, deleted files, browsing history, and user activity. All findings were organized and displayed in the left panel under the Tree View.



Findings & Conclusion (USB Image Analysis):

After successfully imaging the USB drive using FTK Imager and analyzing it in Autopsy, several significant findings were uncovered:

- ✅ **Active Files:** The USB contained documents, images, and executable files. Some files seemed to be manually copied from other systems.
- 🗑️ **Deleted Files:** Multiple deleted files were recovered, including personal documents, login-related text files, and setup executables. These could indicate data exfiltration or file wiping attempts.
- 🔐 **Potentially Sensitive Data:** Among the recovered deleted files were credentials, notes, and cached passwords, suggesting the USB may have been used for storing or transferring private information.
- 🌐 **Web Artifacts:** Though limited, cached browser data indicated the USB was used on systems with web activity, possibly for downloading files.
- 🧩 **Hidden/System Files:** Some files were hidden or marked as system-related, pointing to intentional concealment or malware traces.
- 🕒 **Activity Timeline:** A timeline of file operations (created, modified, deleted) revealed patterns of USB usage — including suspicious deletion close to imaging time.

Final Remark:
This analysis confirms that even a small USB drive can hold critical evidence. Recovered deleted files, especially those containing sensitive or login-related data, were the most important part of this forensic investigation.