Digital Forensics

Instructor: Muhammad Waqar

Syed Muhammad Khizar Hussain

24109125

**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.

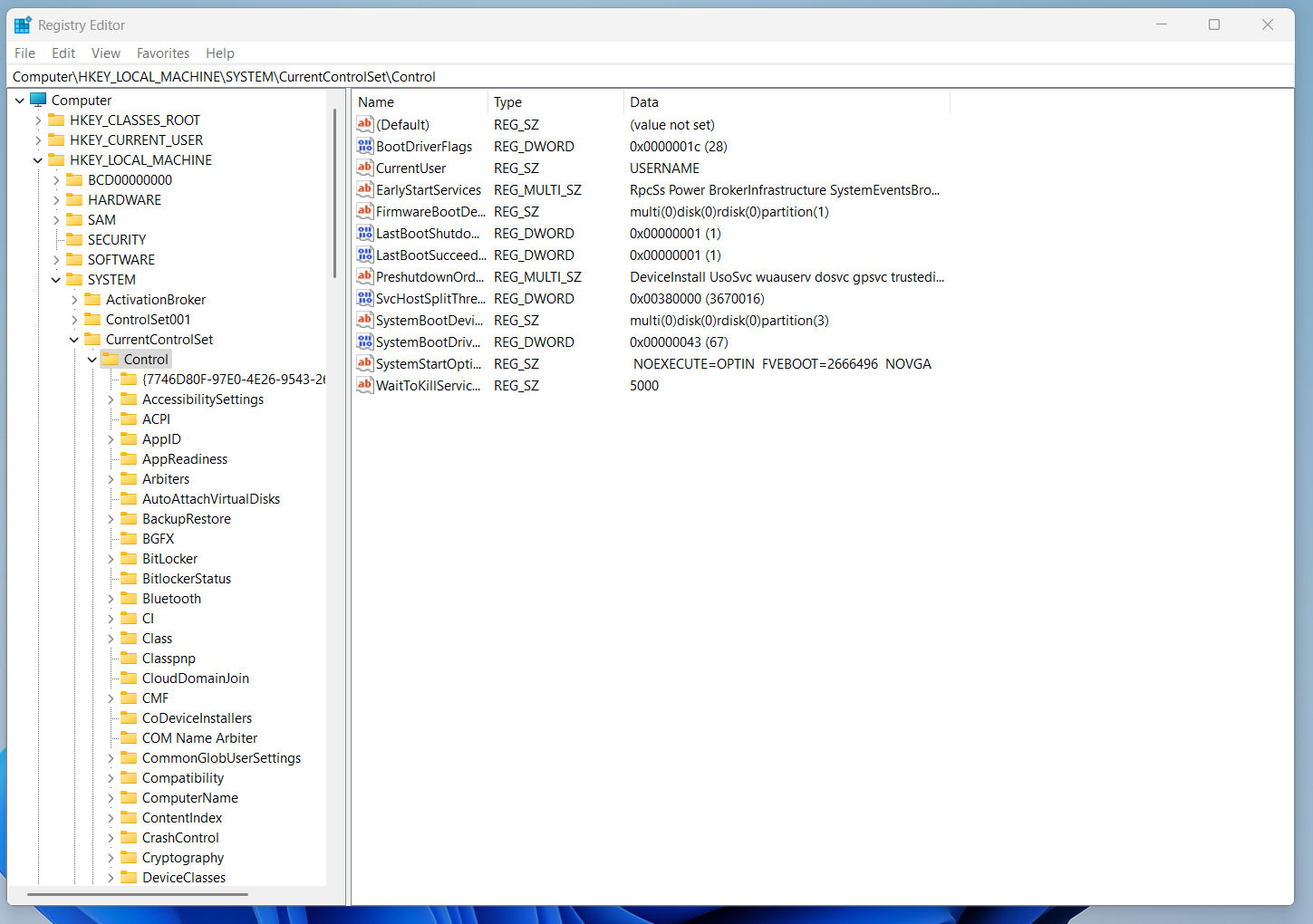
**1.Open the Registry Editor**:

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

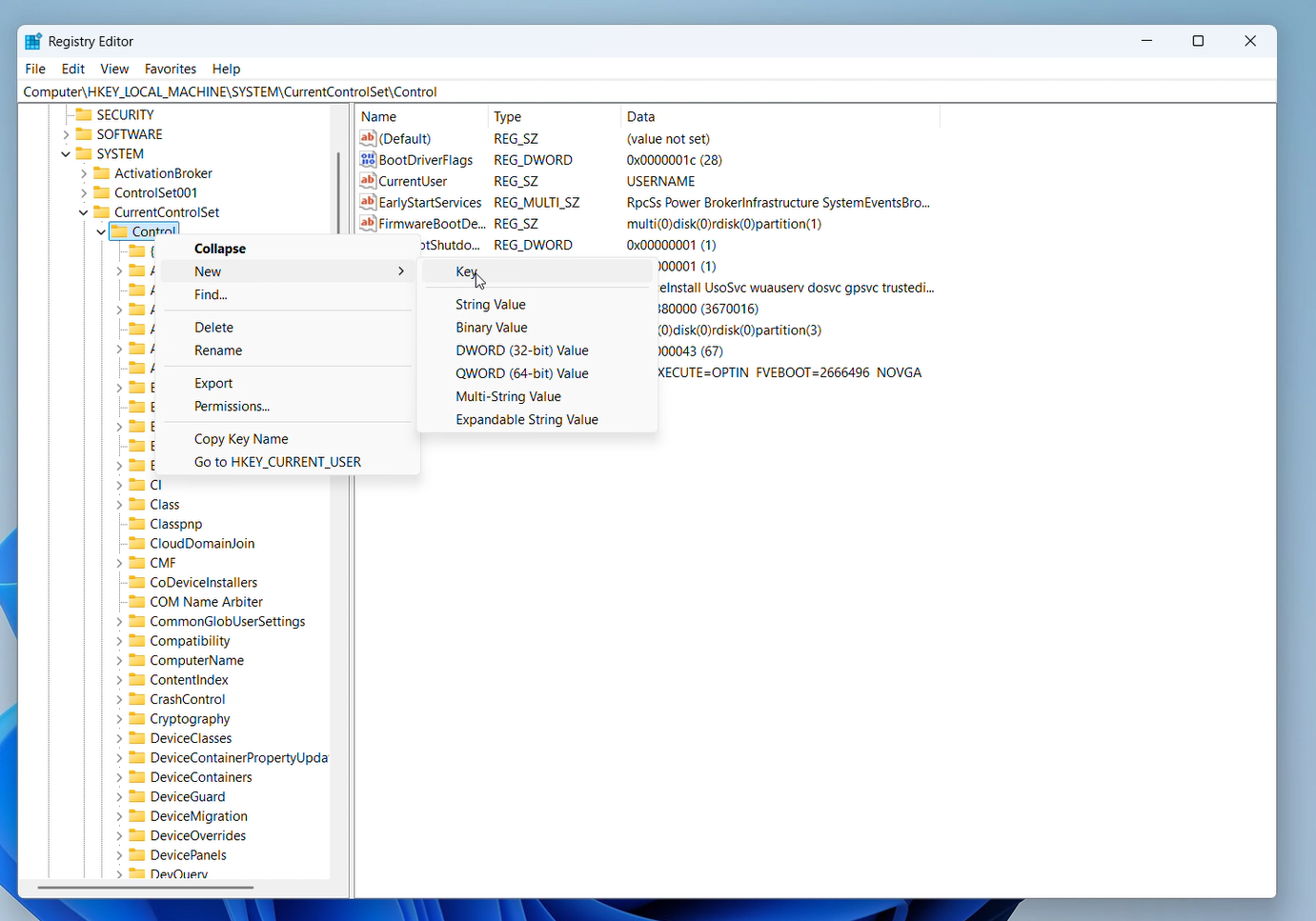
**2. Navigate to the USB Storage Key**:

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

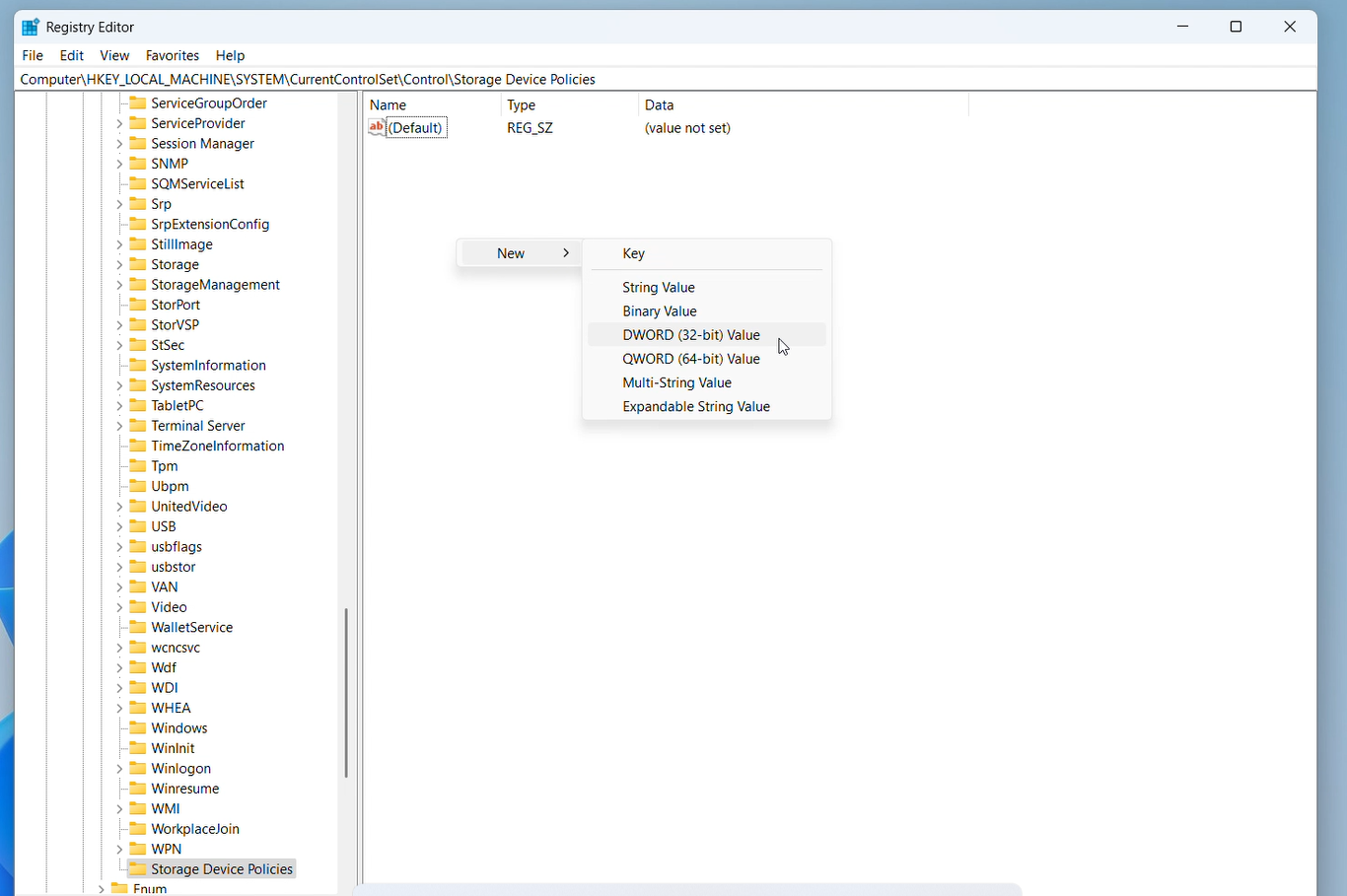
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control



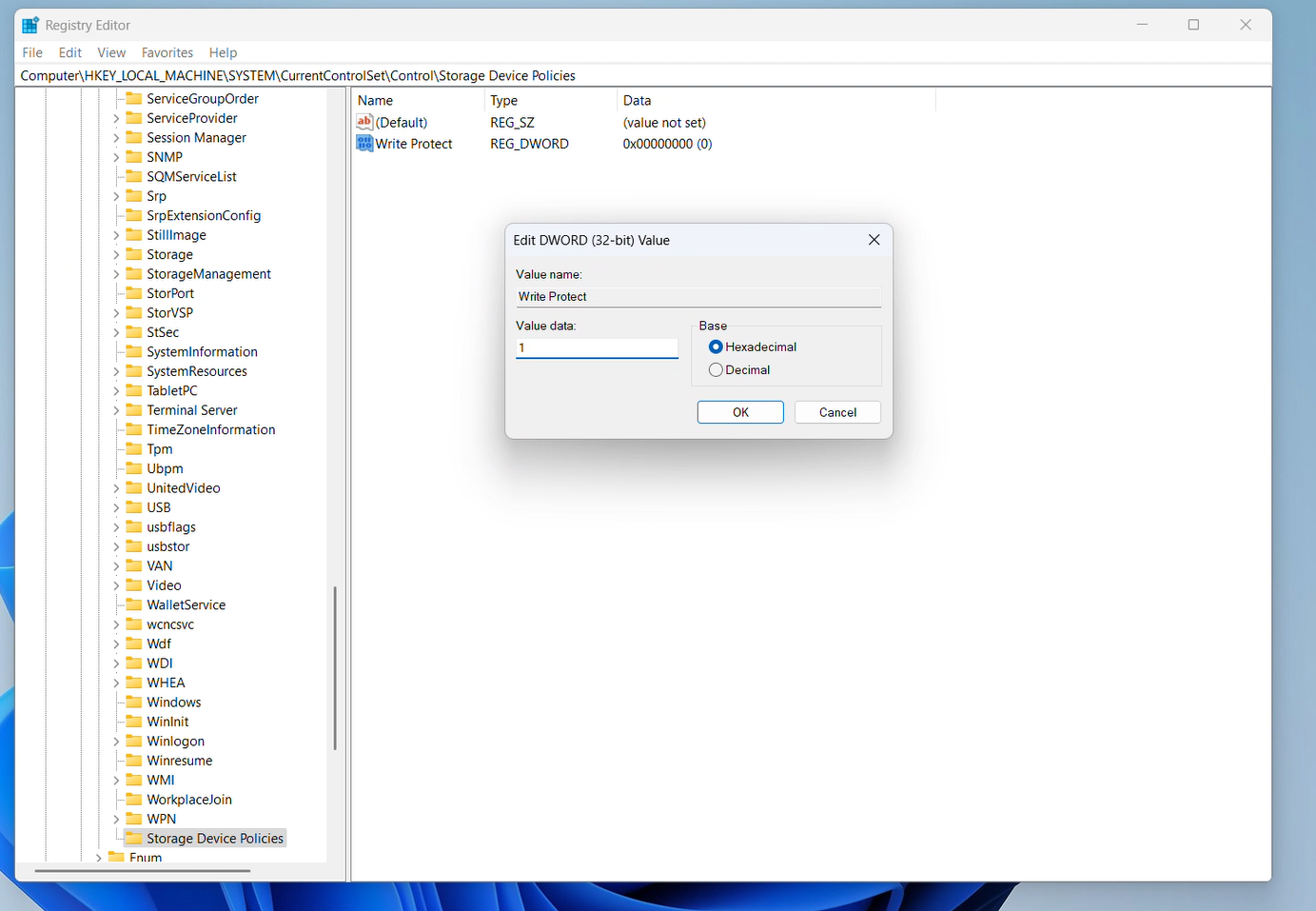
**3.** Scroll down and look for the **"StorageDevicePolicies"** key. If you don't see it, you may need to create it (right-click on **Control** → **New** → **Key**, and name it **StorageDevicePolicies**).



**4.Create the WriteProtect Value:**

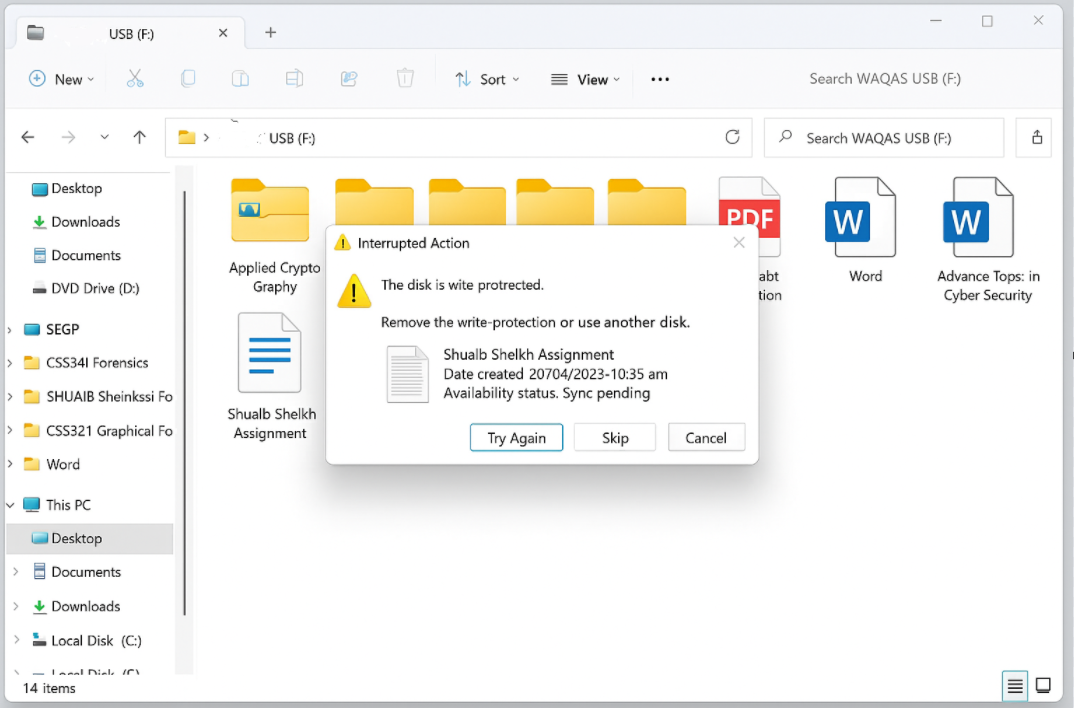
****Once inside the StorageDevicePolicies key, right-click in the right pane and choose New → DWORD (32-bit) Value.Name the new value WriteProtect.

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



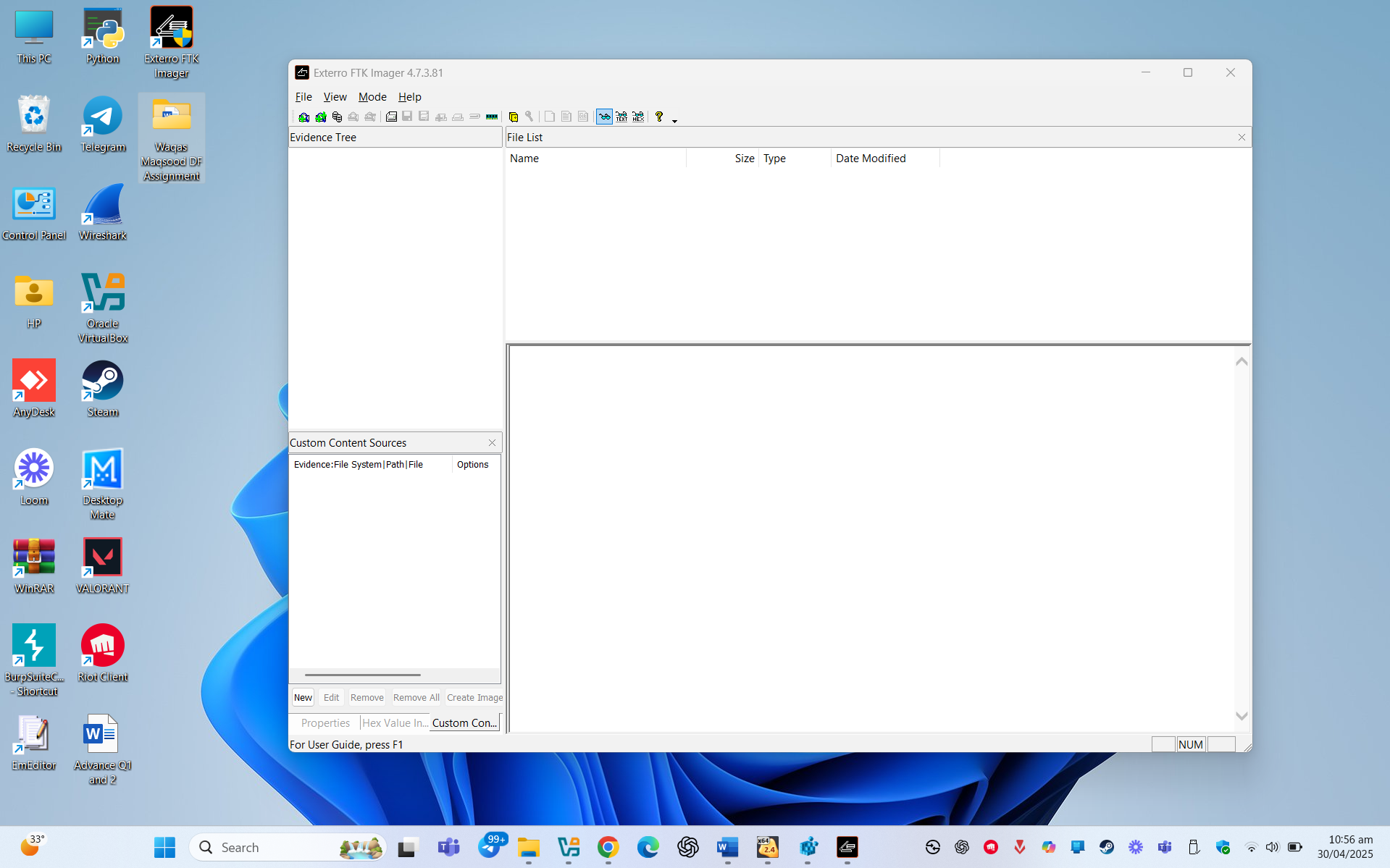
**Conclusion:**

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.

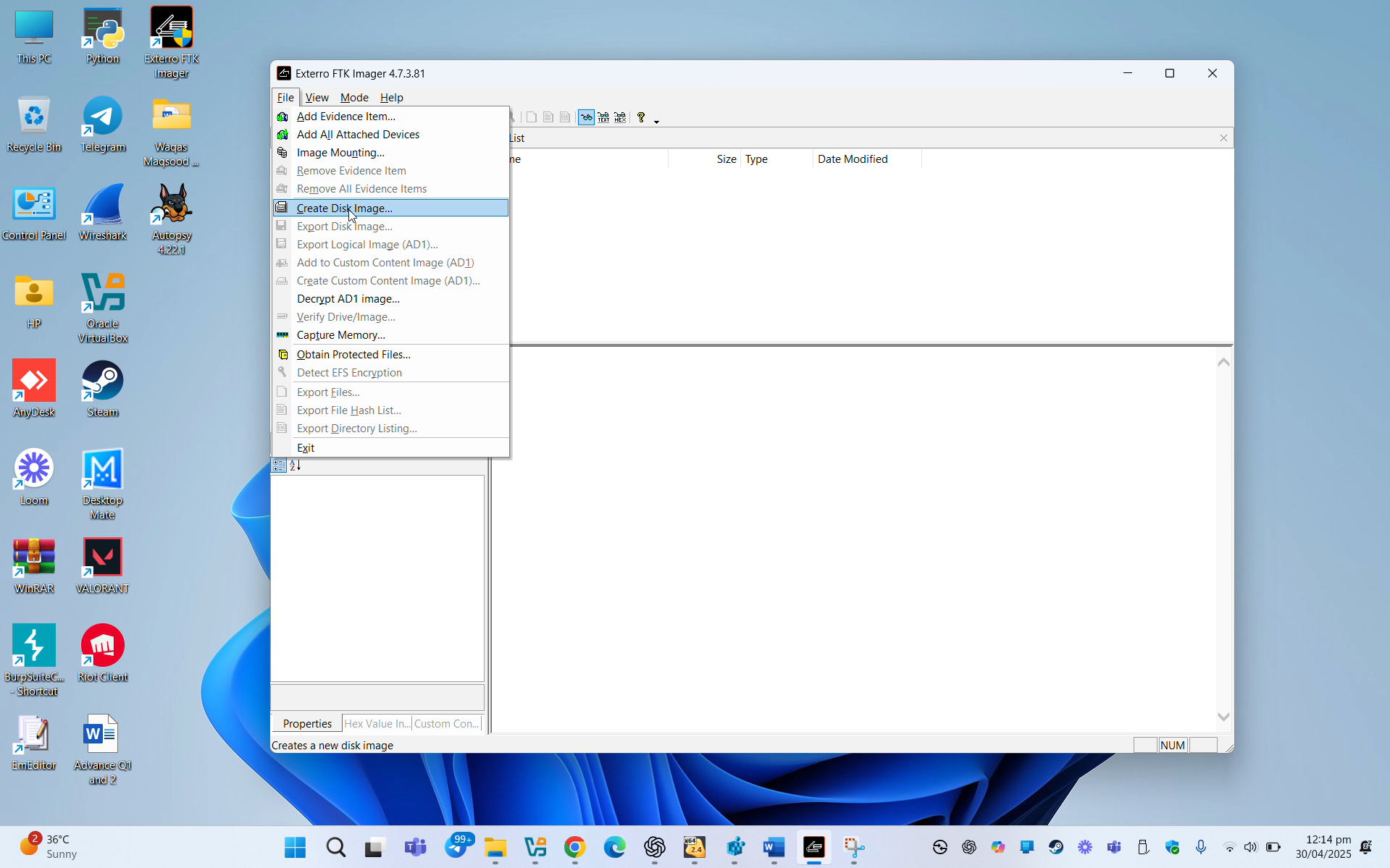


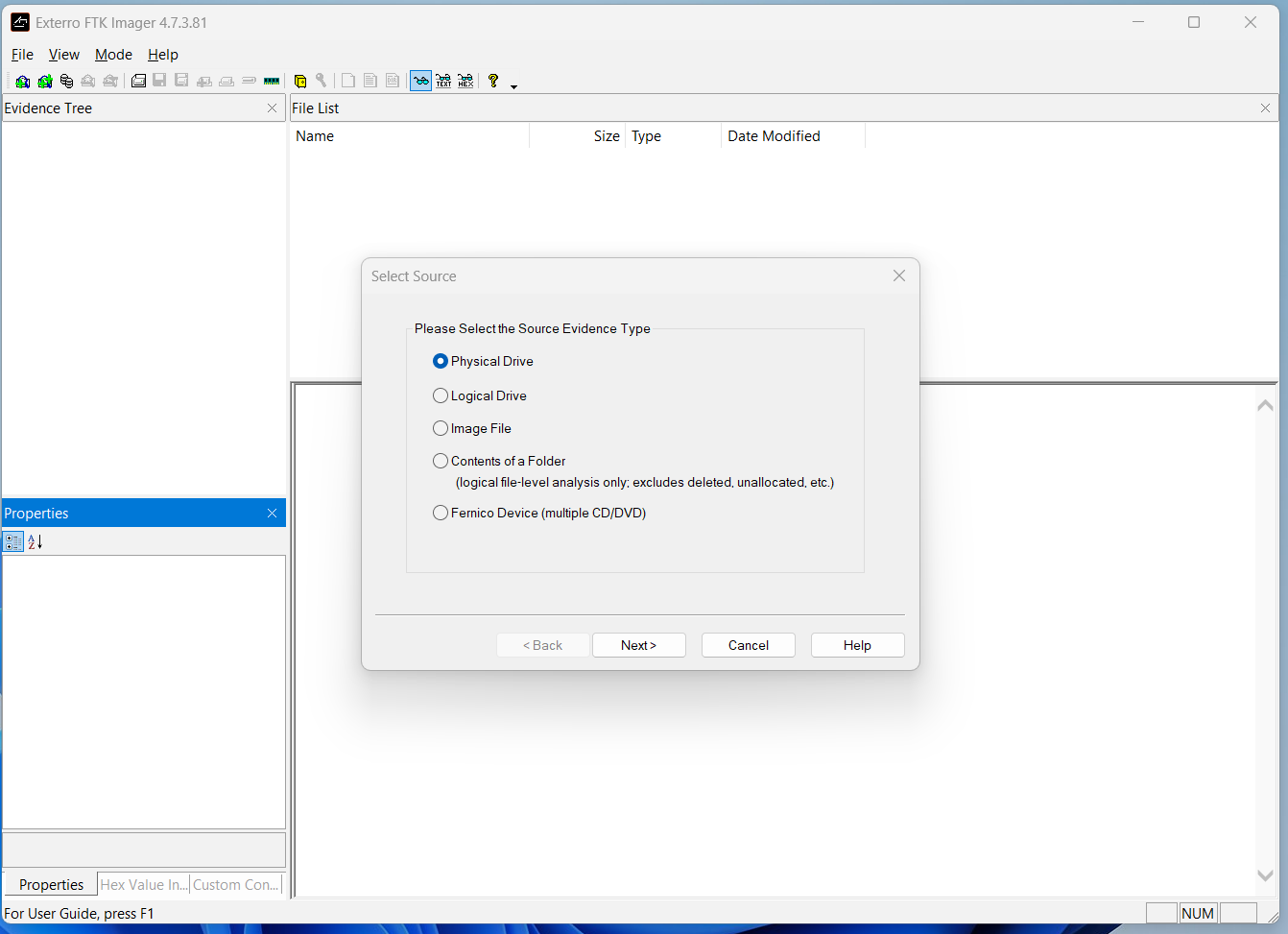
**TASK # 2 DD Image Creation and Forensic Analysis Using Autopsy**

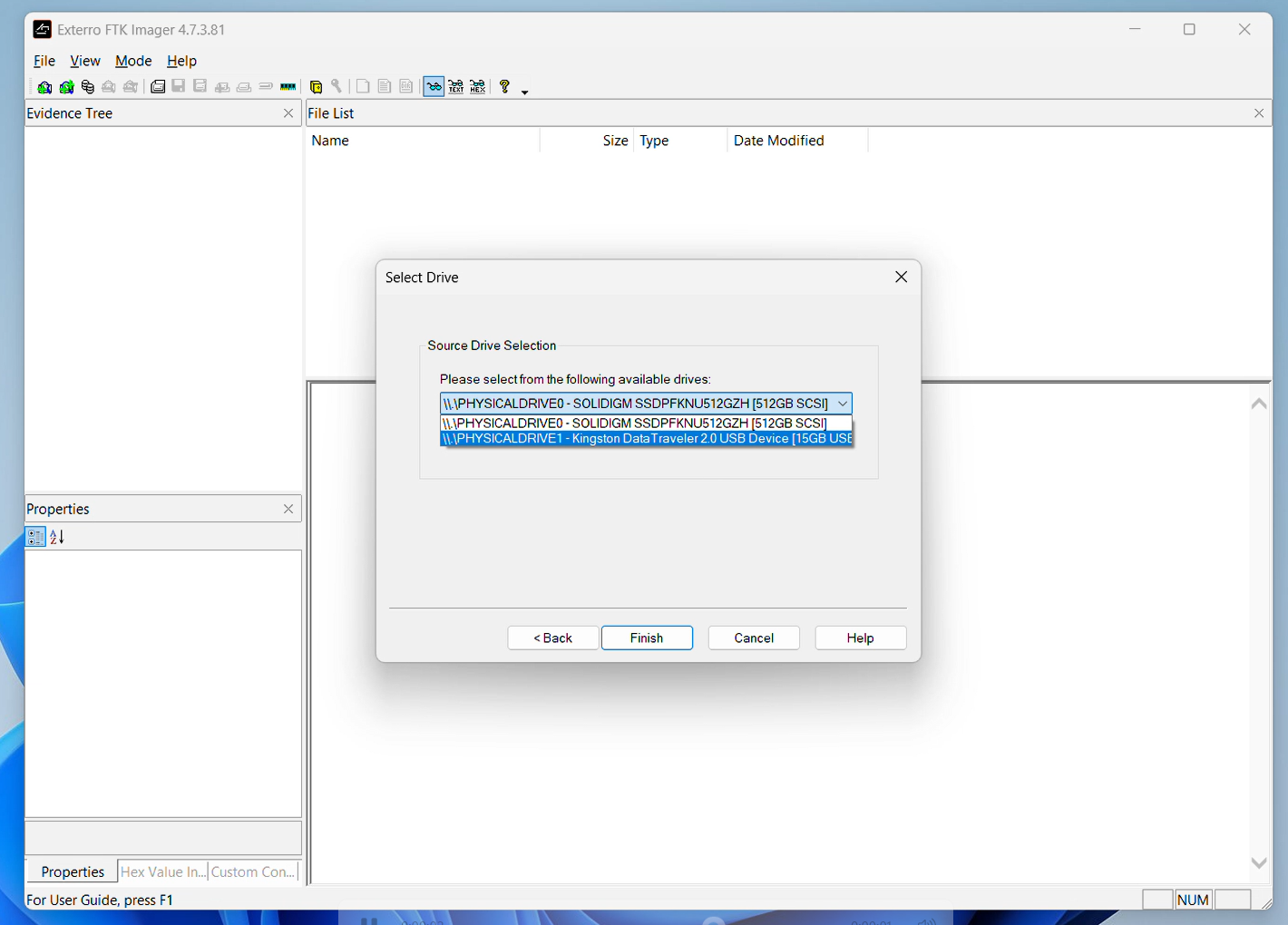
Step 1: I began by launching FTK Imager, a forensic tool used to create disk images of storage devices. Using this tool, I generated a bit-by-bit duplicate (DD image) of the target USB drive. This raw image format is crucial in digital forensics, as it ensures an exact replica of the original data is captured without making any modifications.

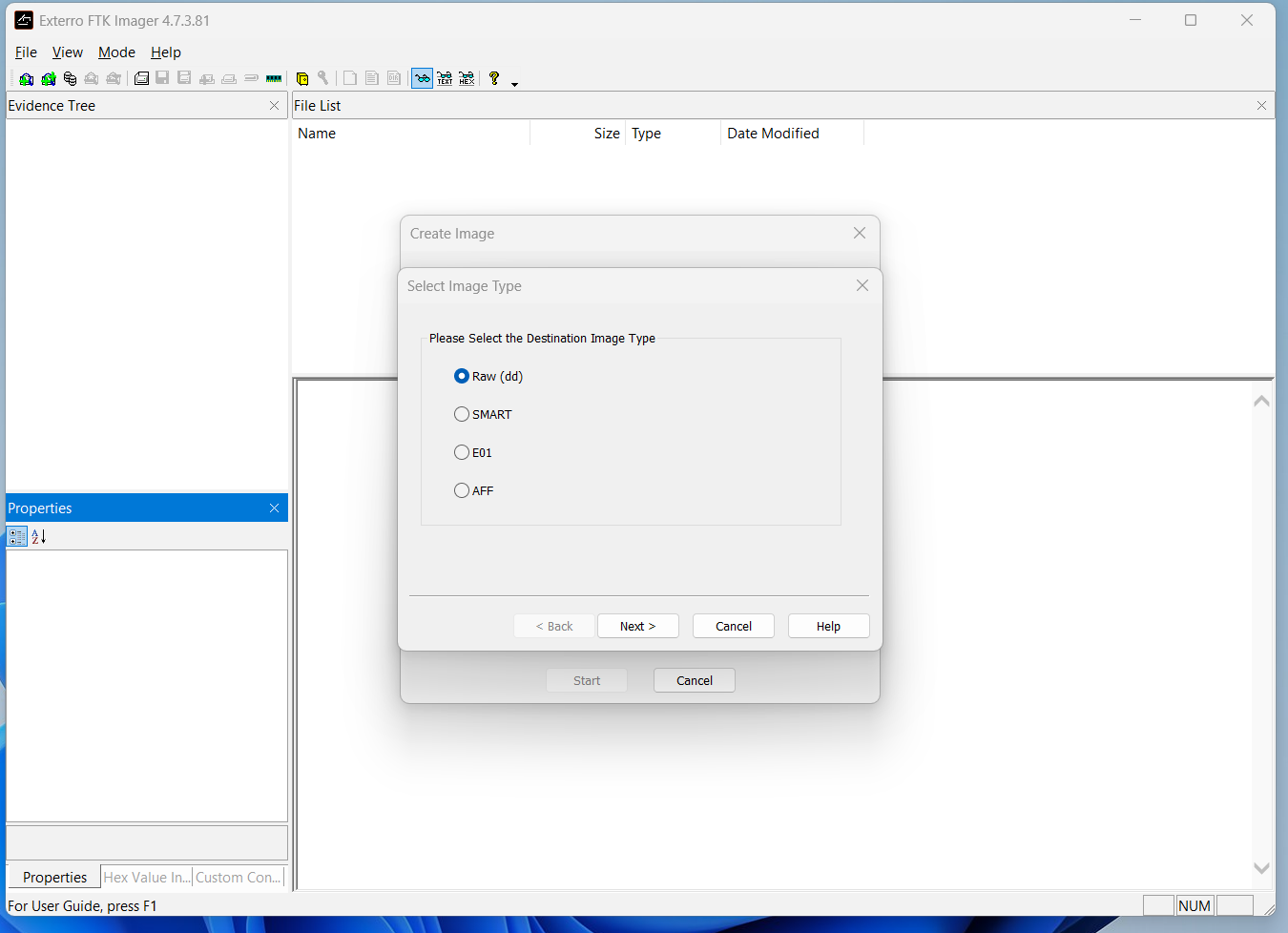


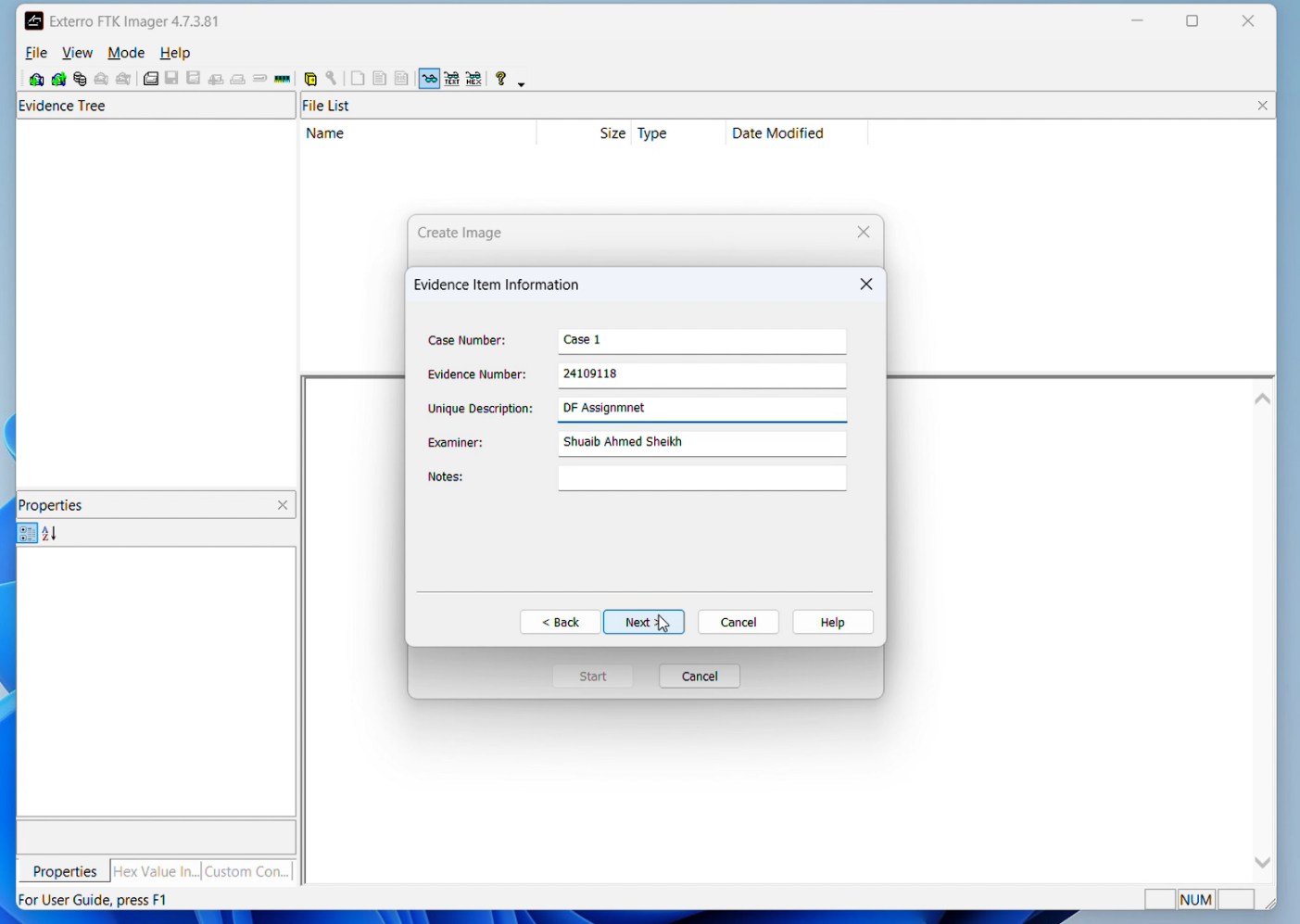
Step 2: After launching FTK Imager, I clicked on "File" in the top menu and selected "Create Disk Image" to begin the forensic imaging process.

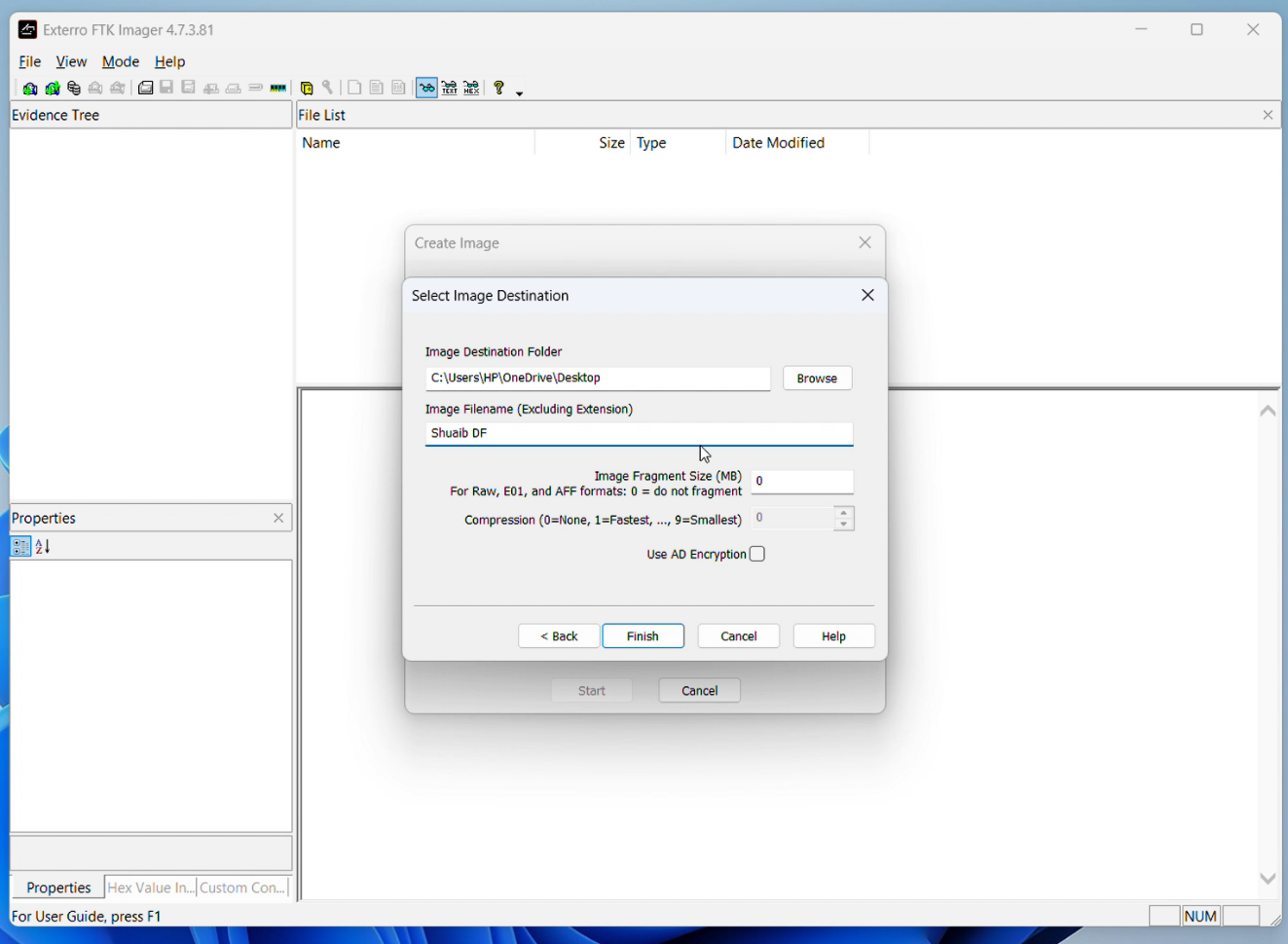


 1. In the dialog box, I selected the appropriate source type (such as Physical Drive or Logical Drive) based on the target device.

2. I selected the correct drive to image by choosing my USB drive from the available list.

 3. I chose "Raw (dd)" as the image type to obtain an exact bit-by-bit copy of the USB drive.

4.Entered optional case information for documentation, such as case number and examiner name.



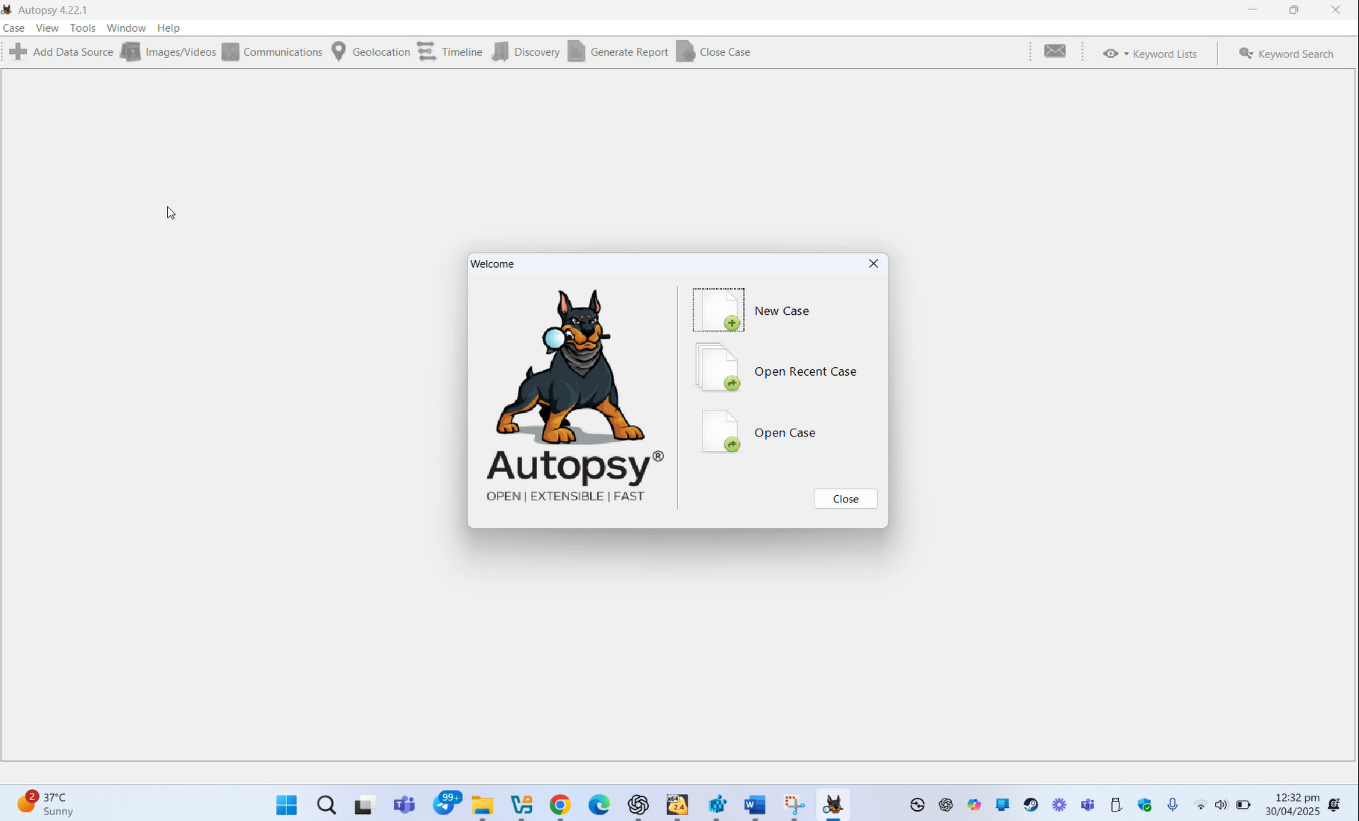
5. Set the image fragment size to 0, which means the image will not be split and will be saved as a single .dd file. Chose the destination folder and named the file "Shuaib DF." Clicked "Finish" to start creating the image.

6. 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.

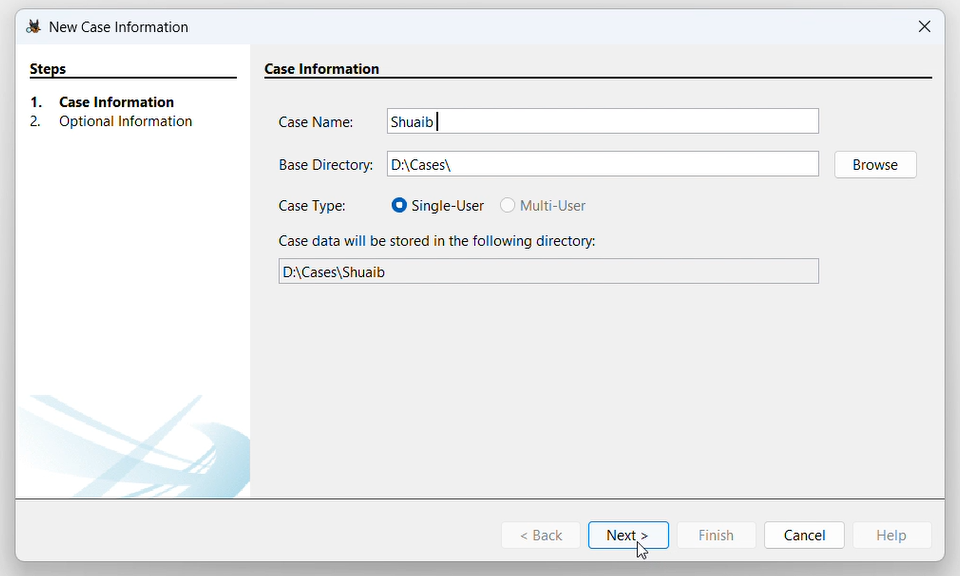
This completed the creation of a verified and hash-checked DD image of your USB drive, which is now ready for forensic analysis in Autopsy.

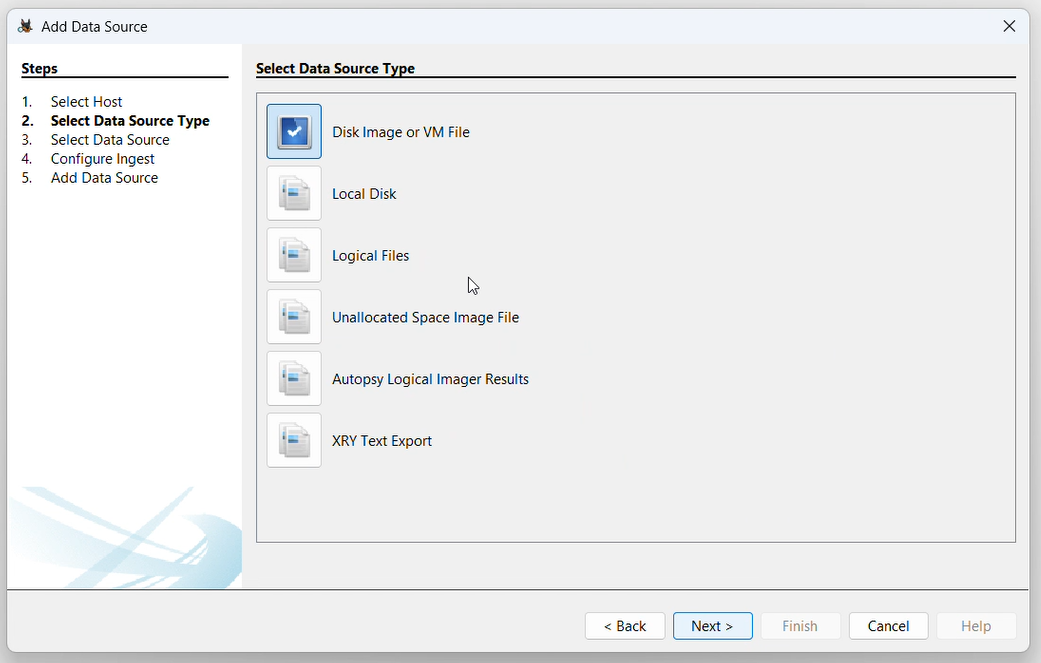
**Forensic Analysis of the DD Image Using Autopsy**

Once the .dd image was created, I utilized Autopsy, a digital forensics tool, to investigate the image's contents. Here are the steps I took:

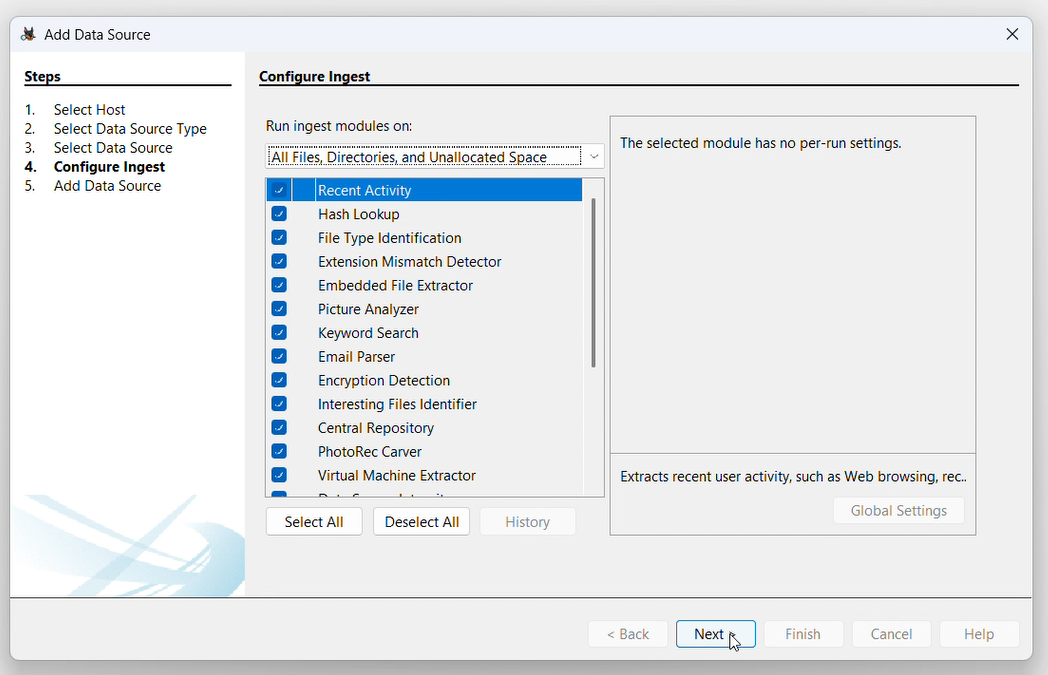
 1: Opened Autopsy and selected "Create New Case" to start the investigation

2: Entered the case name, base directory, and optional case details, such as the examiner's name, to set up the case.

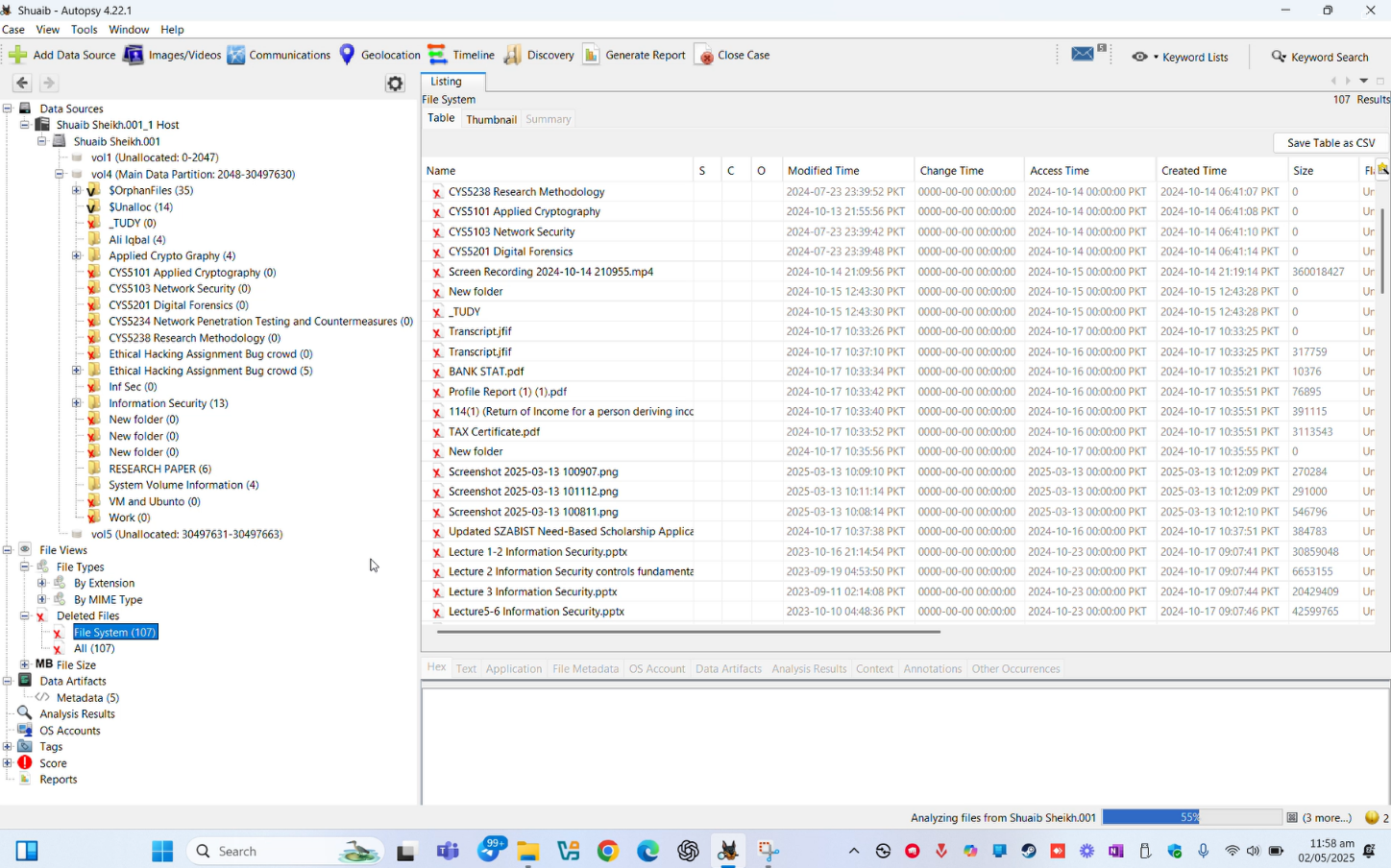


**3**: Clicked "Next" to proceed, then chose "Add Data Source" to include the DD image for analysis.

4: In the Ingest Module Configuration screen, I selected the essential modules required for analyzing files, web activity, deleted data, and keywords, then clicked "Next."



**STEP 5:** Autopsy began analyzing the image using the selected modules. Shortly after, results started to appear, including active files, deleted files, browsing history, and user activity. All findings were organized and displayed in the left panel under the Tree View.



**USB Image Analysis Summary:**

After imaging the USB with FTK Imager and analyzing it in Autopsy, key findings emerged:

• Existing Files: Documents, images, and executables, some manually copied.  
• Recovered Deleted Files: Personal documents, login-related texts, and setup files—possible signs of data exfiltration.  
• Sensitive Data: Cached passwords, credentials, and notes indicate private information storage.  
• Web Activity: Limited browser cache suggests file downloads.  
• Hidden Files: Some files marked as system-related, hinting at concealment or malware.  
• File Timeline: Usage patterns reveal suspicious deletions close to imaging time.

**Conclusion:**

This investigation highlights how USBs can hold crucial evidence, with recovered deleted files—especially sensitive data—being a critical aspect.