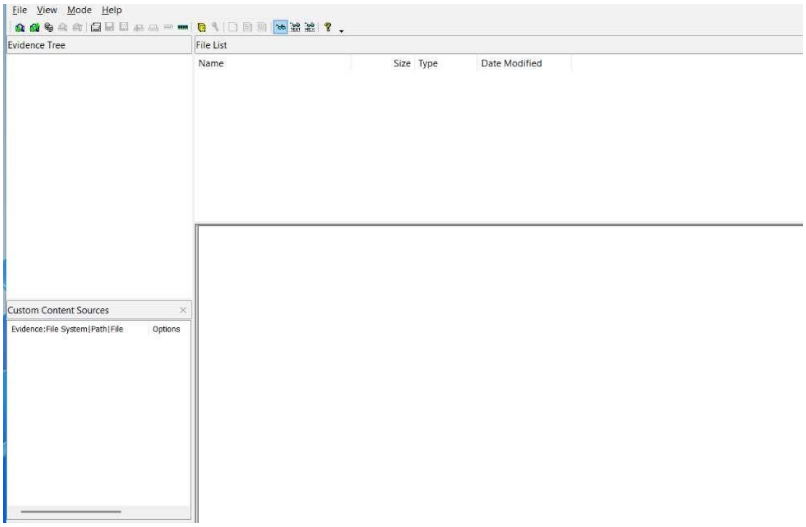
Digital Forensics

ASSIGMENT: 01

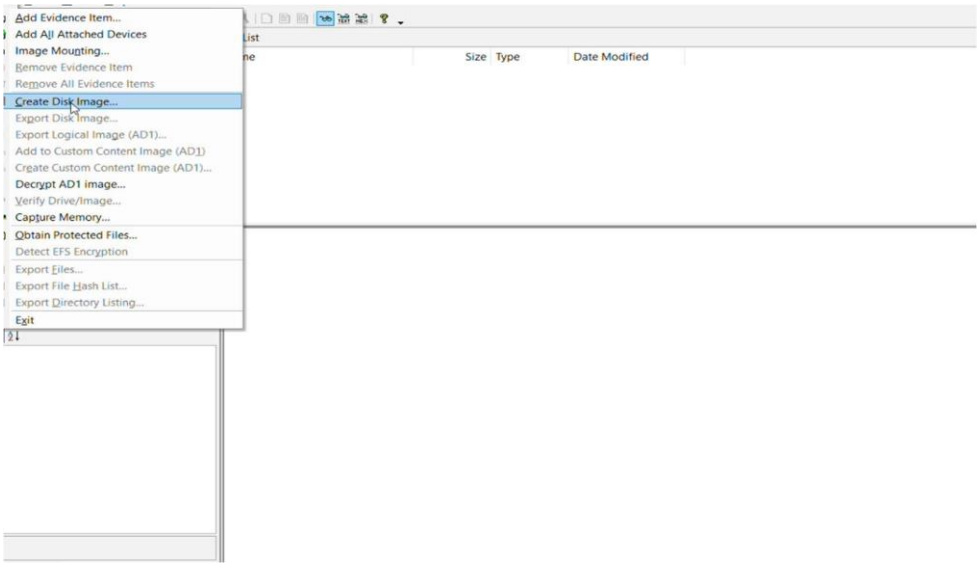
Muhammad Sohaib (24109111)

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.

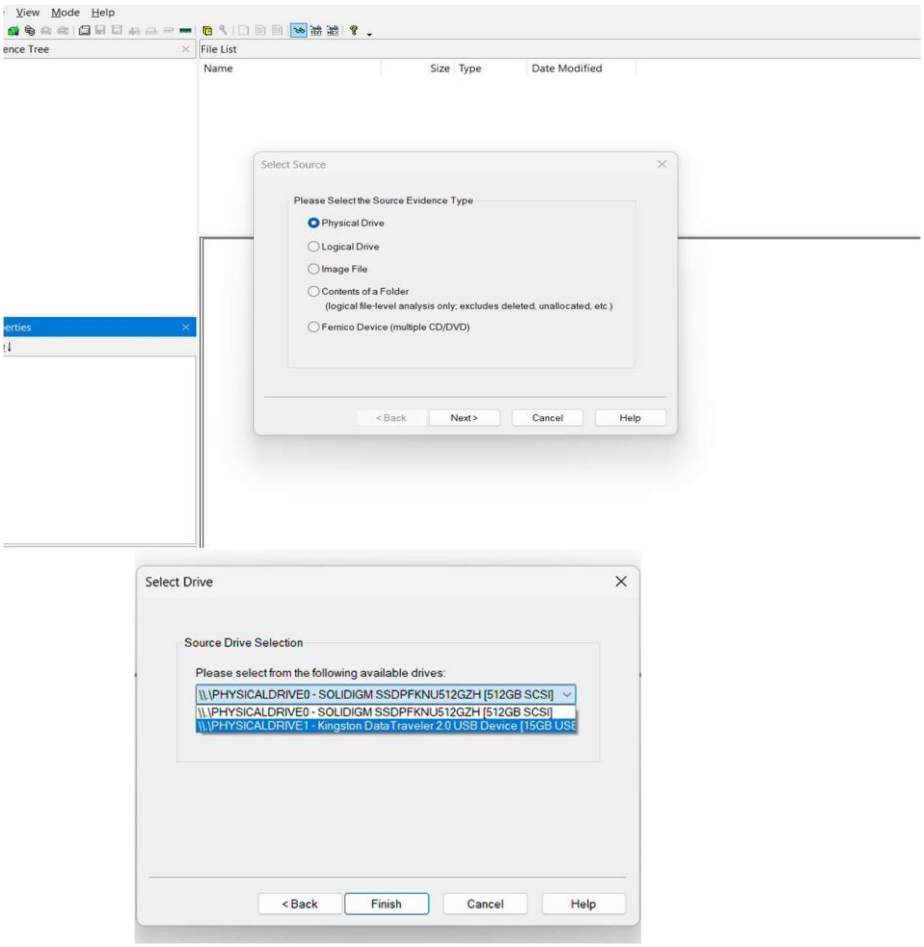


Step 2: After launching FTK Imager, I clicked on "File" in the top menu and selected "Create Disk Image" to begin the forensic imaging process.

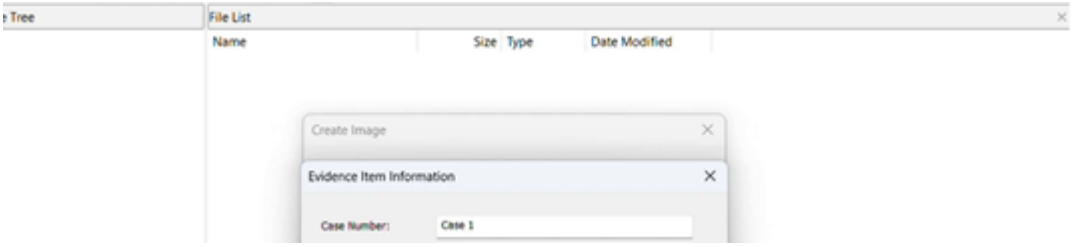


1. In the dialog box, I selected the appropriate source type (such as Physical Drive or Logical Drive) based on the target device.

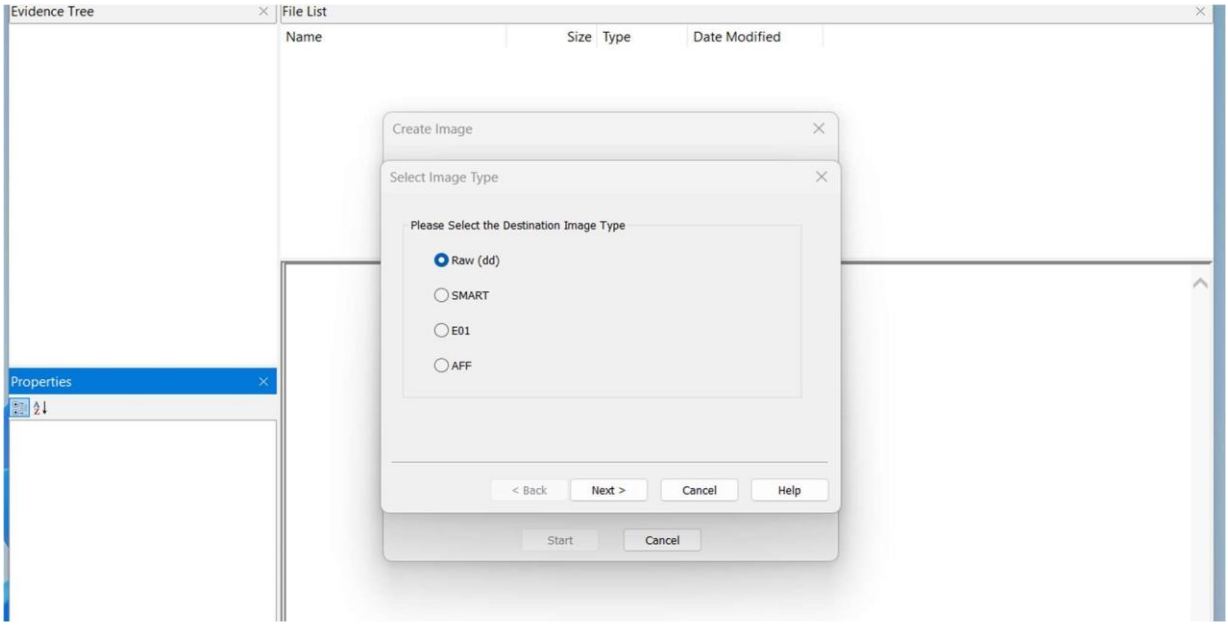
2. I selected the correct drive to image by choosing my USB drive from the available list.



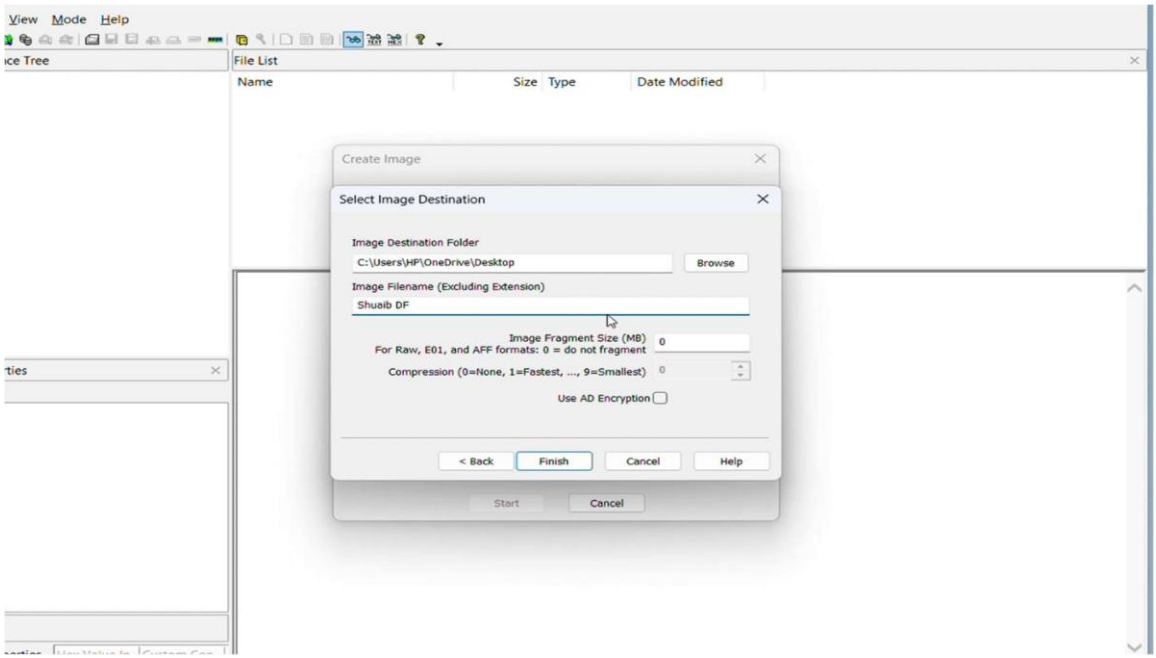
3. I chose "Raw (dd)" as the image type to obtain an exact bit-by-bit copy of the USB drive.



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 des na on 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.