

Ex. No 1: Evidence Acquisition Using FTK Imager

Aim: To capture RAM data and create a forensic disk image using FTK Imager

Requirements:

- FTK imager
- Windows operating system

Description:

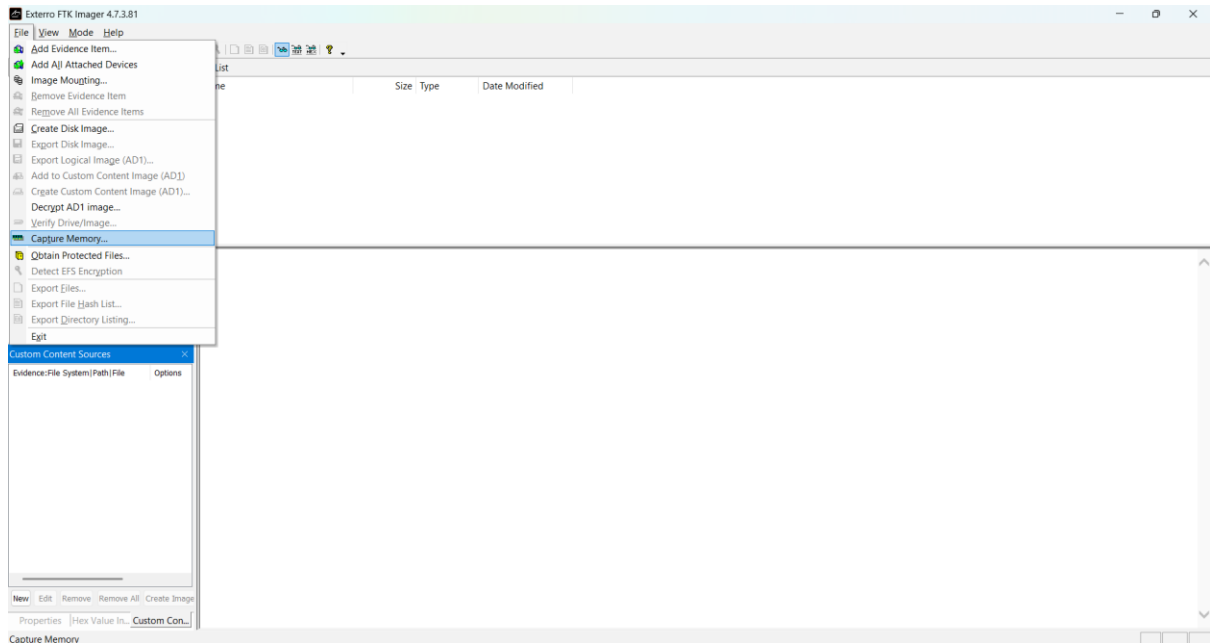
- FTK Imager is a forensic acquisition tool used to create exact copies (disk images) of storage devices.
- It allows capturing RAM data, entire drives, or specific partitions without altering original evidence.
- Investigators use it to preview, preserve, and export data for further forensic analysis.

Acquiring Volatile Memory (RAM) Using FTK Imager

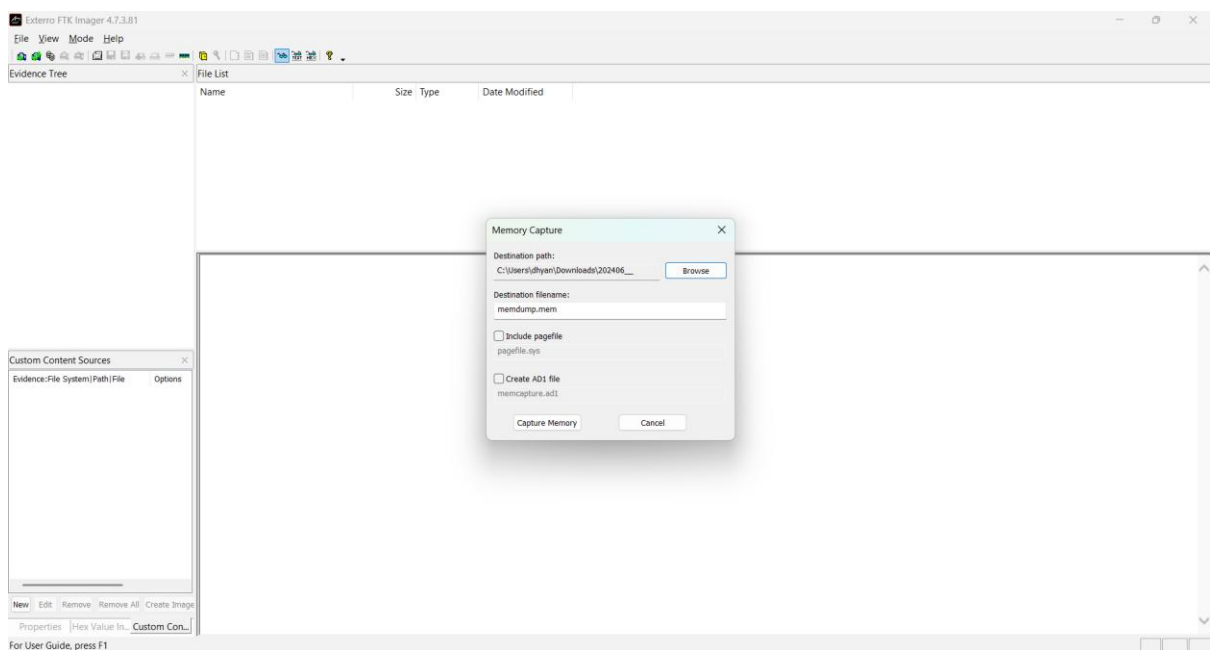
Step-1: Right click on the FTK imager tool and select run as administrator



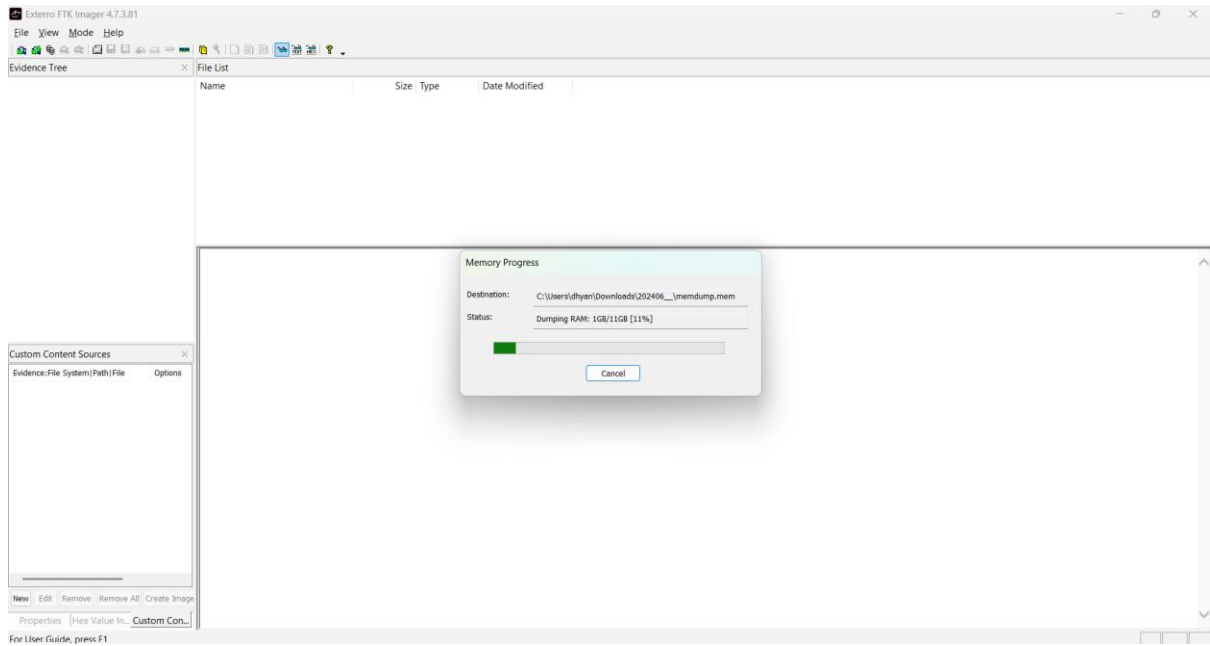
Step-2: On right top menu bar click file and select capture memory from drop down list



Step-3: A dialog box will appear select the destination path to your file and provide the file name with “mem” extension and pagefile and AD1 file are optional.



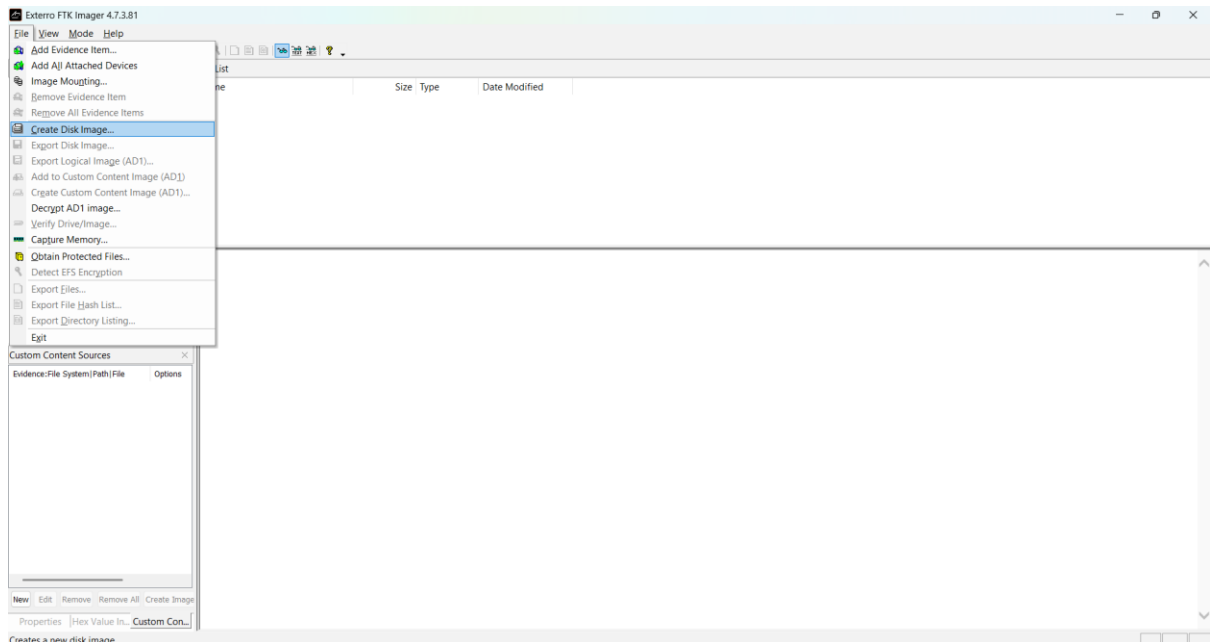
Step-4: click the “capture memory” to start acquisition of memory



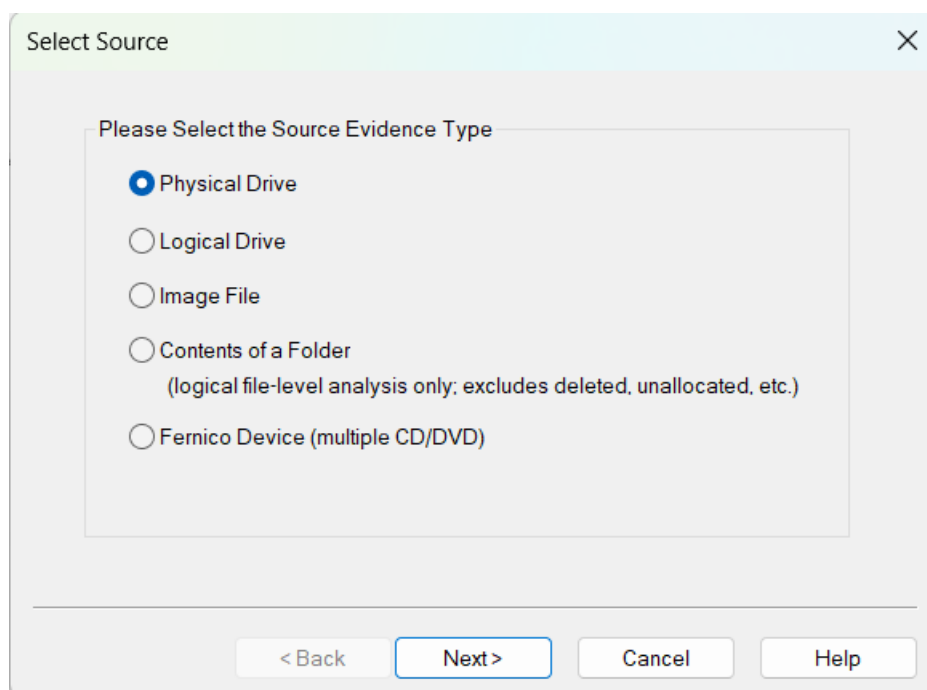
Step-5: A progress bar in green colour will indicate the capture status and the time taken to capture the RAM will depends on RAM size. After completion of capturing the memory dump file will be available in the destination folder

Acquiring Non-Volatile Memory (Disk Image) Using FTK Imager

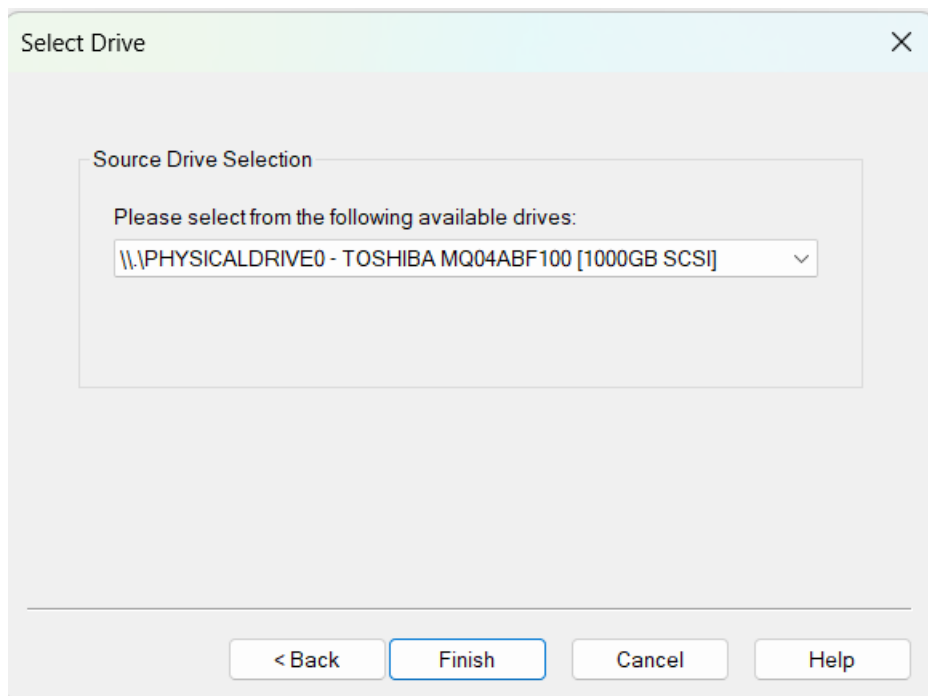
Step-1: On the top right menu bar click file and select the “Create Disk Image” from the drop-down menu



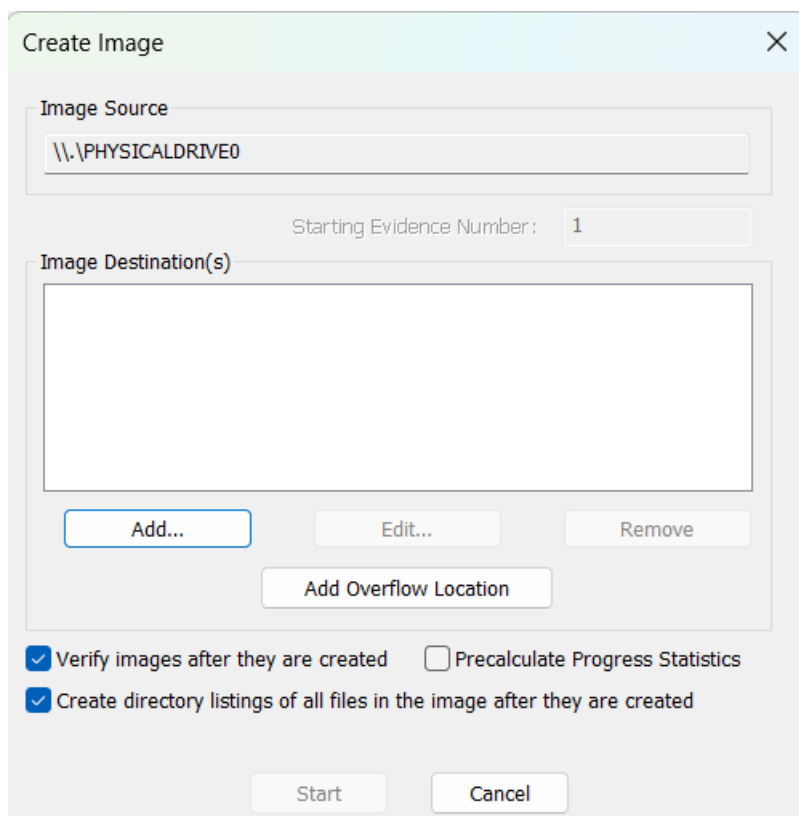
Step-2: In the dialog box, choose the source evidence type like Physical Drive, Logical Drive, Image File or Contents of a folder



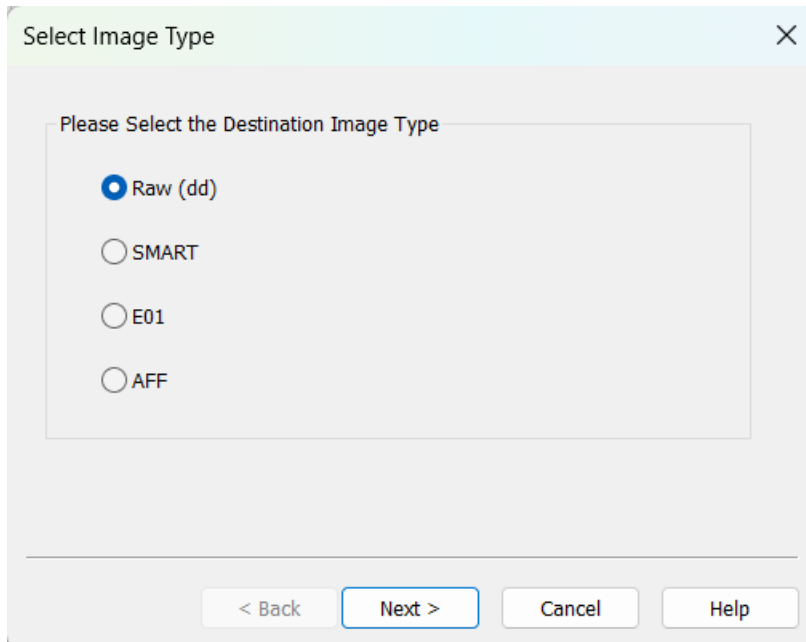
Step-3: Select the drive you want to image and click Finish



Step-4: In the “Create Image” dialog, click Add to define image type

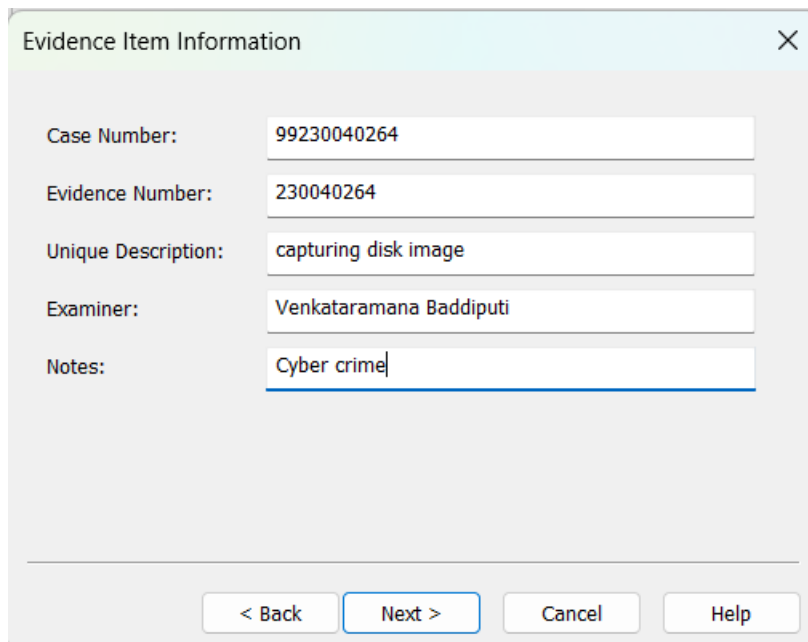


Step-5: Select the image type from the dialog box (Raw/SMART/E01/AFF) among all E01 is recommended



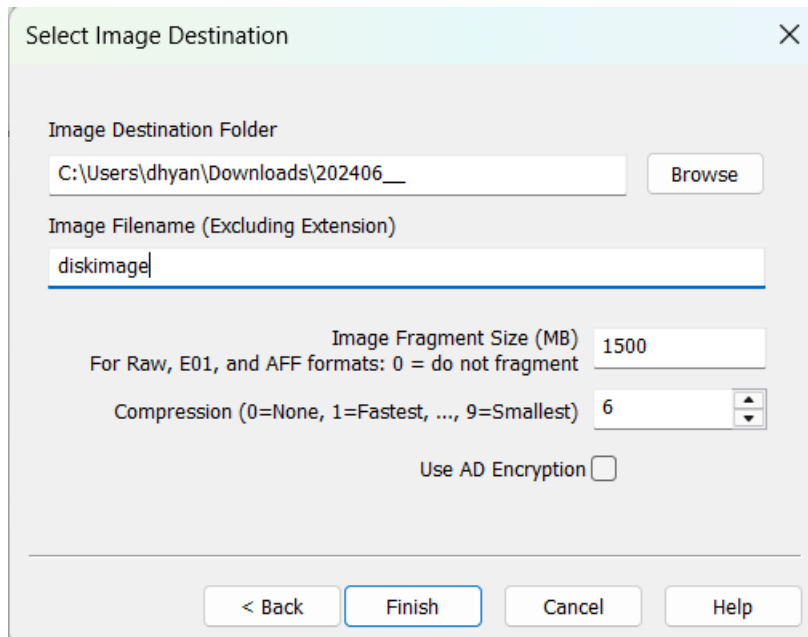
A dialog box titled "Select Image Type" with a close button (X) in the top right corner. The main area contains the text "Please Select the Destination Image Type" followed by four radio button options: "Raw (dd)" (selected), "SMART", "E01", and "AFF". At the bottom, there are four buttons: "< Back", "Next >" (highlighted with a blue border), "Cancel", and "Help".

Step-6: Fill in the case information (case number, evidence number, examiner name, unique description and notes) click Next.

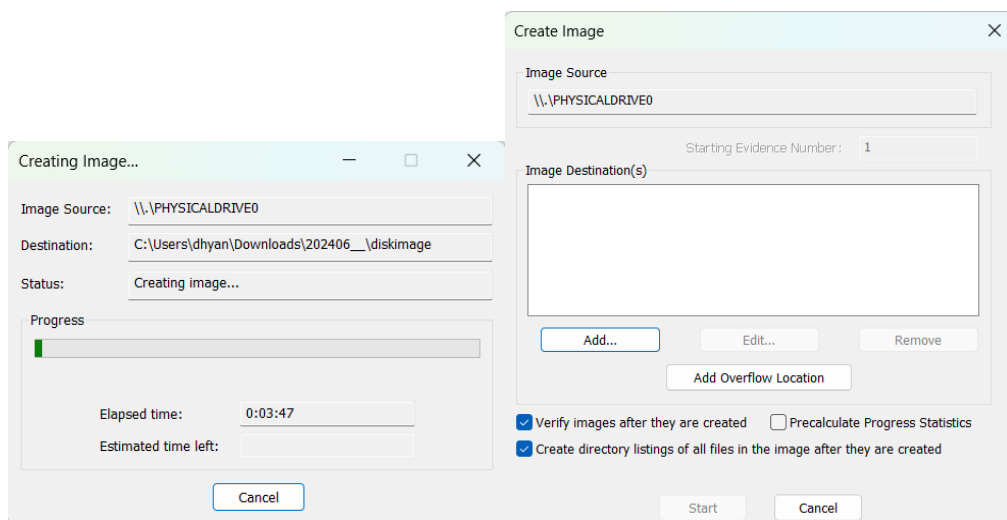


A dialog box titled "Evidence Item Information" with a close button (X) in the top right corner. It contains five text input fields with labels to their left: "Case Number:" (99230040264), "Evidence Number:" (230040264), "Unique Description:" (capturing disk image), "Examiner:" (Venkataramana Baddiputi), and "Notes:" (Cyber crime). At the bottom, there are four buttons: "< Back", "Next >" (highlighted with a blue border), "Cancel", and "Help".

Step-7: Choose the destination folder and give a file name for the image.



Step-8: Set options like compression, splitting size, and click Finish after that Start the imaging process.



FTK Imager will display progress along with hash values. The imaging process may take time depending on the drive size. After completion, FTK imager verifies the hash values automatically and it maintains the forensics integrity.

Finally, the hash values are matched