**Exp:03** **Name: Hemanth kumar**

**Roll no:231901010**

# Recover Deleted Files using Forensics Tools

### Aim

To recover accidentally or intentionally deleted files from a storage device or disk image using forensic tools such as **Autopsy**, **FTK Imager** and verify the integrity of recovered data.

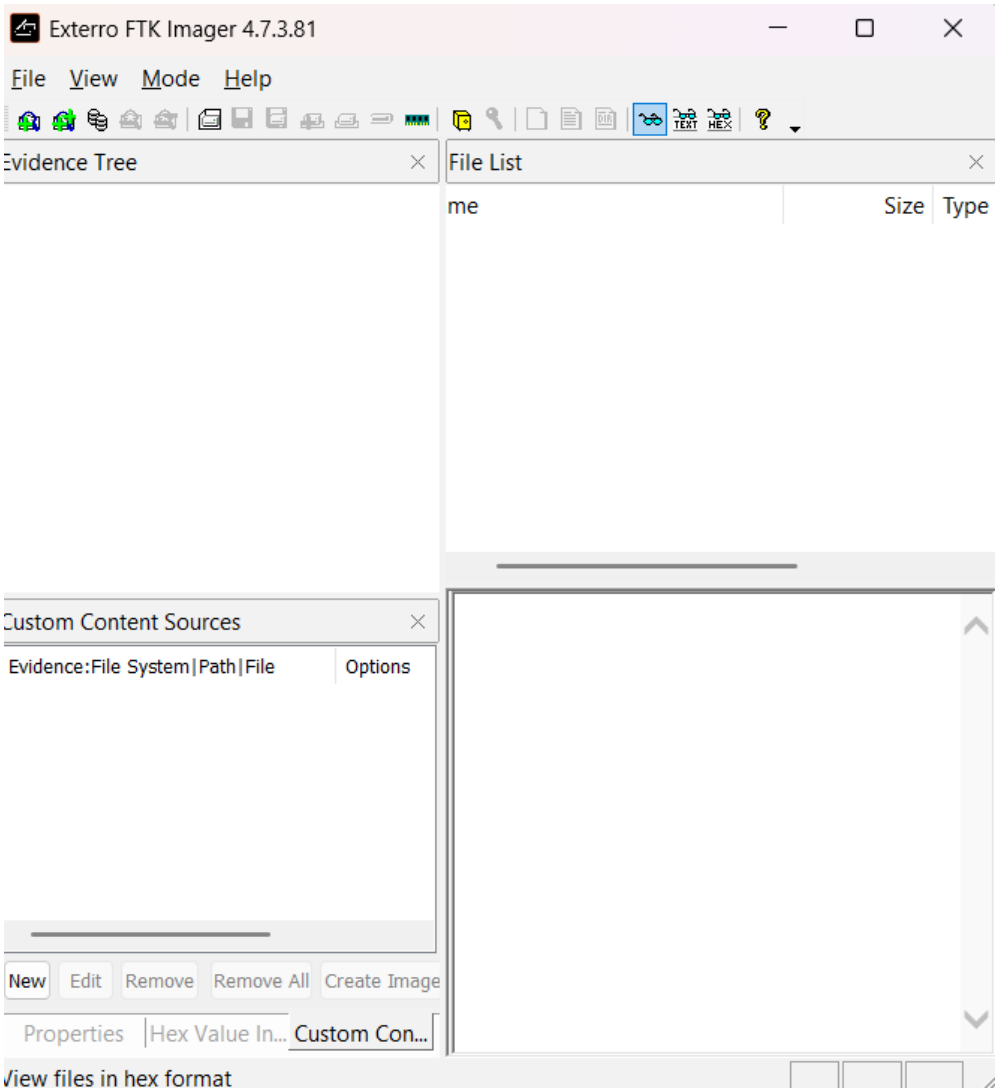
### Algorithm / Steps

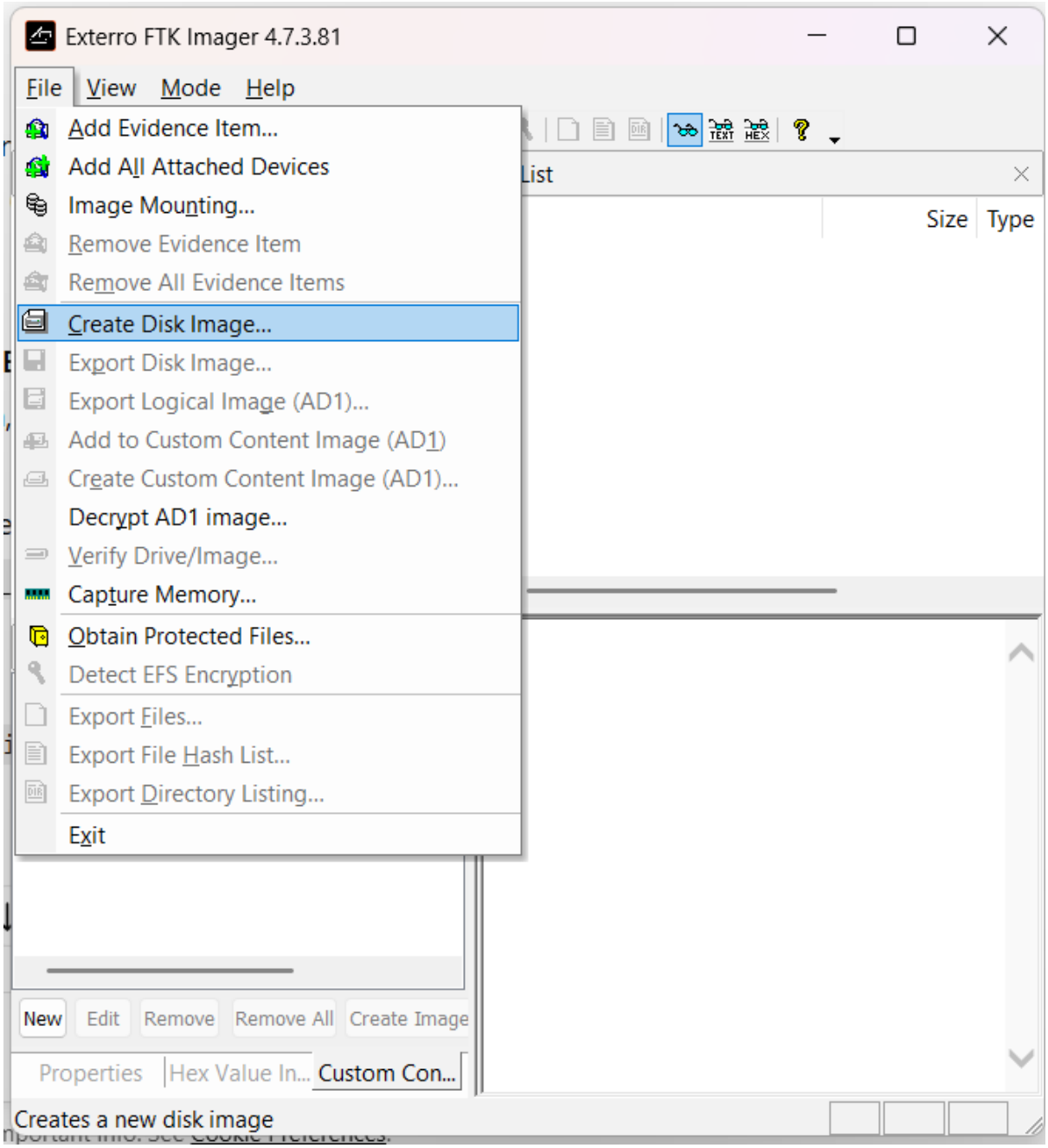
1. **Prepare the Evidence Source**
    - Acquire a forensic image of the target disk/USB drive (using FTK Imager or dd).
    - Alternatively, mount the storage device in read-only mode.
2. **Open Forensic Tool**
    - Launch Autopsy / FTK Imager .
3. **Load Data Source**
    - Select *Add Data Source* → Provide the acquired image file or physical drive.
4. **Scan for Deleted Files**
    - Enable file system analysis and data recovery modules.
    - Locate “Unallocated Space” or “Deleted Files” sections.
5. **Recover Files**
    - Select identified deleted files.
    - Export/recover them to a safe forensic folder.
6. **Verify Recovered Data**
    - Compare file hashes (MD5/SHA1) before and after recovery to ensure integrity.
7. **Generate Report**
    - Document the recovered files, metadata (file name, size, location), and verification details.

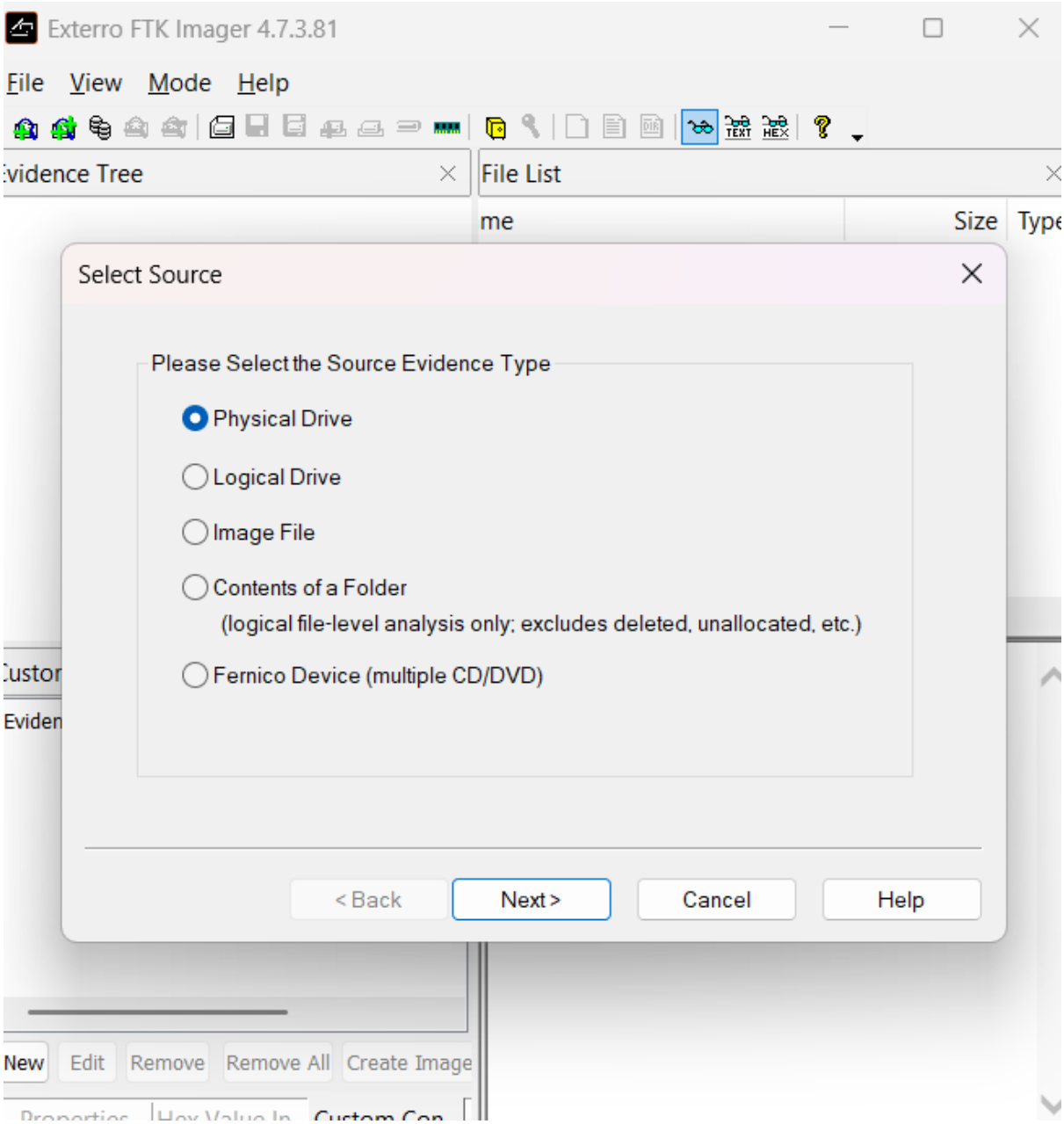
**Step-by-Step Procedure**

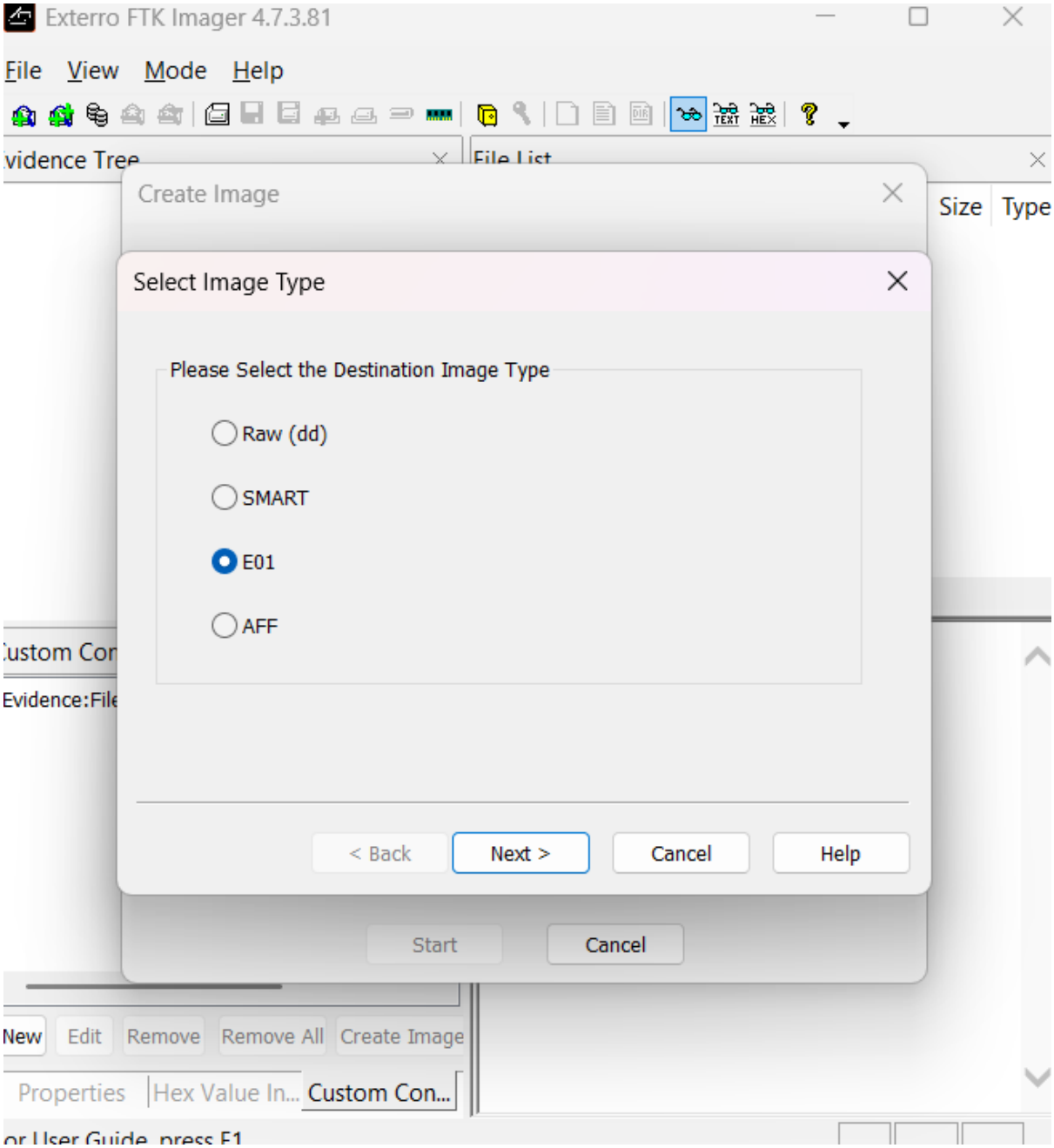
**A. With FTK Imager**

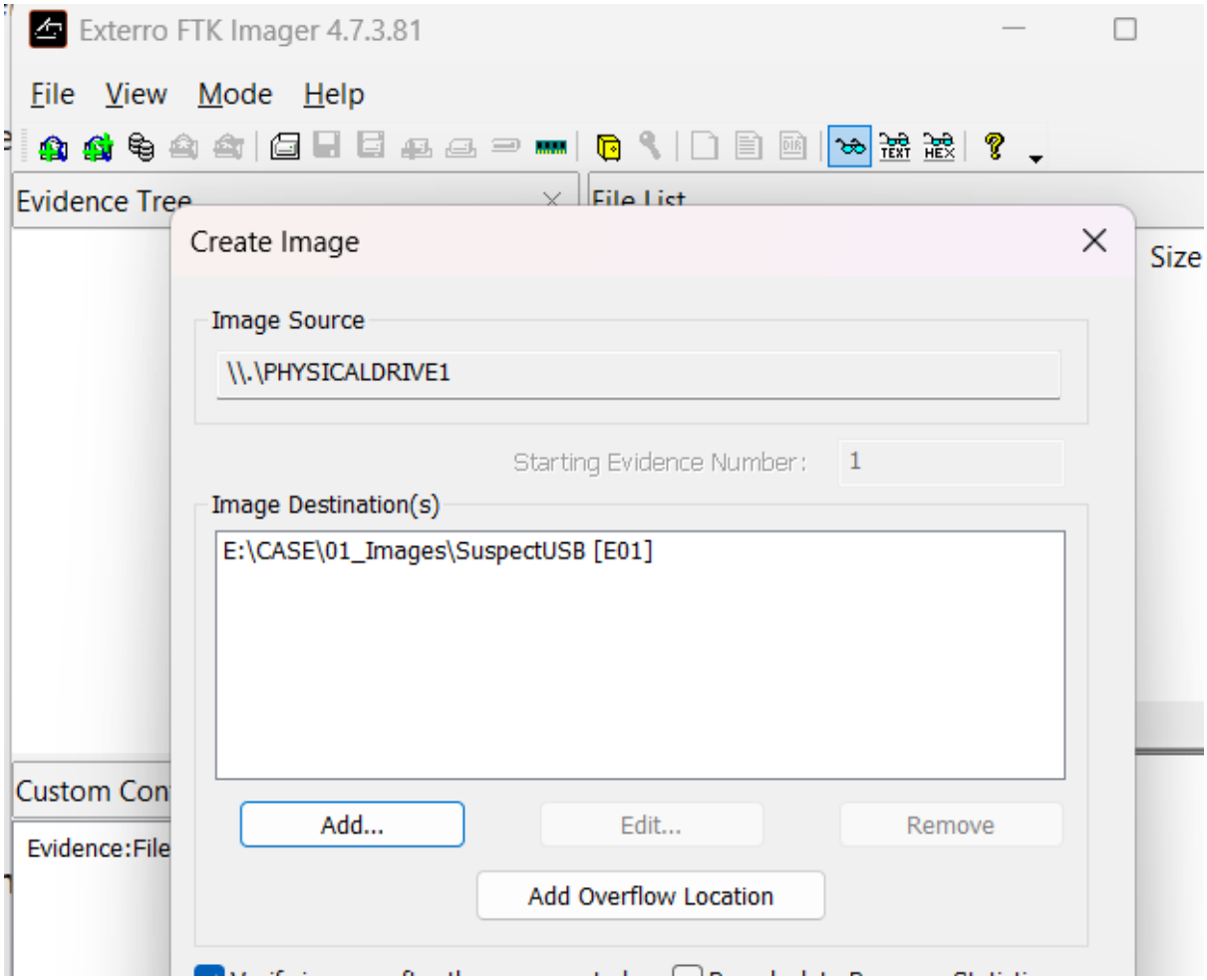
1. Run **FTK Imager (as Administrator)**.
2. **File → Create Disk Image**.
3. Select **Physical Drive** → choose the USB stick.
4. Format: choose **E01** (preferred forensic format).
5. Destination: save in a folder like C:\Case\01_Images\.
6. Tick **Verify images after creation**.
7. FTK will output MD5 & SHA1 → copy/save these hash values.

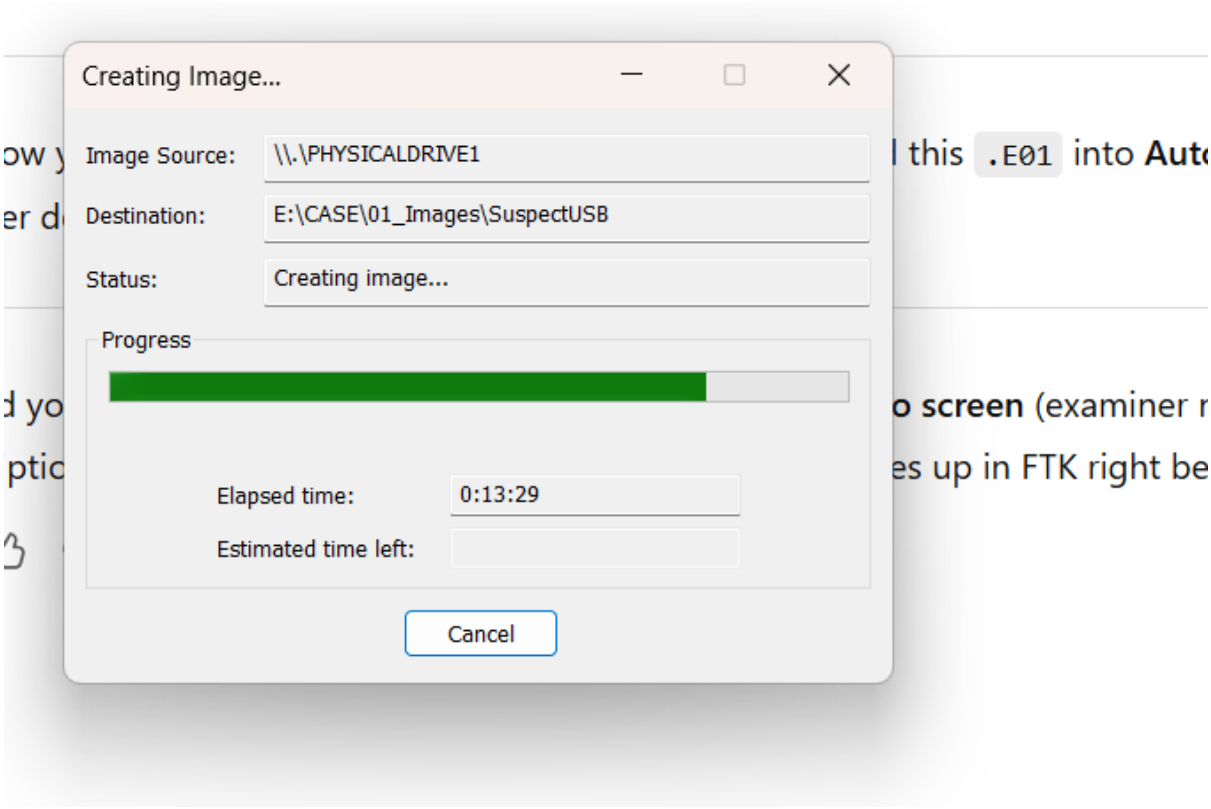

Exterro FTK Imager 4.7.3.81
File View Mode Help
Evidence Tree
File List
me
Size
Type
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value In...
Custom Con...
View files in hex format

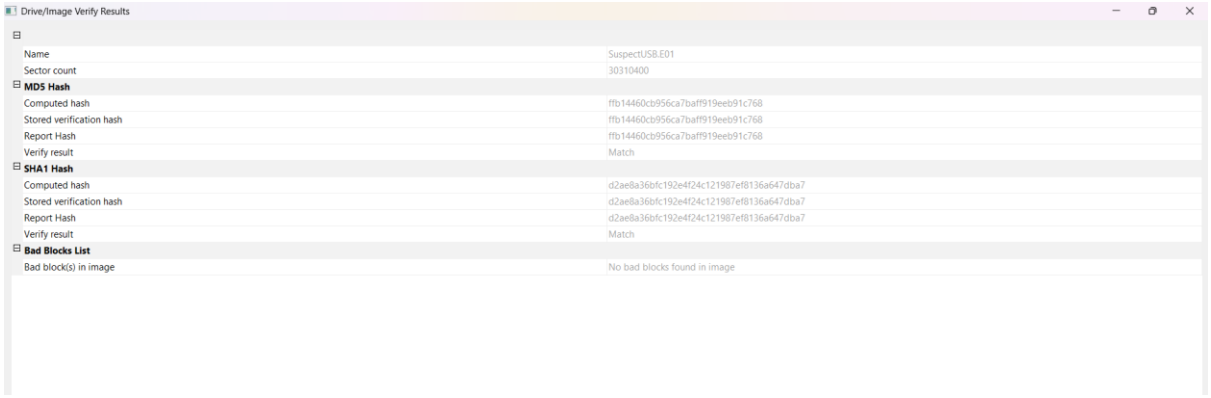

Exterro FTK Imager 4.7.3.81
File
View
Mode
Help
Add Evidence Item...
Add All Attached Devices
Image Mounting...
Remove Evidence Item
Remove All Evidence Items
Create Disk Image...
Export Disk Image...
Export Logical Image (AD1)...
Add to Custom Content Image (AD1)
Create Custom Content Image (AD1)...
Decrypt AD1 image...
Verify Drive/Image...
Capture Memory...
Obtain Protected Files...
Detect EFS Encryption
Export Files...
Export File Hash List...
Export Directory Listing...
Exit
List
Size
Type
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value In...
Custom Con...
Creates a new disk image


Exterro FTK Imager 4.7.3.81
File View Mode Help
Evidence Tree
File List
me
Size
Type
Select Source
Please Select the Source Evidence Type
Physical Drive
Logical Drive
Image File
Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
Fernico Device (multiple CD/DVD)
< Back
Next >
Cancel
Help
New
Edit
Remove
Remove All
Create Image


Exterro FTK Imager 4.7.3.81
File View Mode Help
Create Image
Select Image Type
Please Select the Destination Image Type
Raw (dd)
SMART
E01
AFF
< Back
Next >
Cancel
Help
Start
Cancel
Size
Type
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value In...
Custom Con...


Exterro FTK Imager 4.7.3.81
File View Mode Help
Evidence Tree
File List
Size
Create Image
Image Source
\\.\PHYSICALDRIVE1
Starting Evidence Number: 1
Image Destination(s)
E:\CASE\01_Images\SuspectUSB [E01]
Add...
Edit...
Remove
Add Overflow Location
Custom Con
Evidence:File



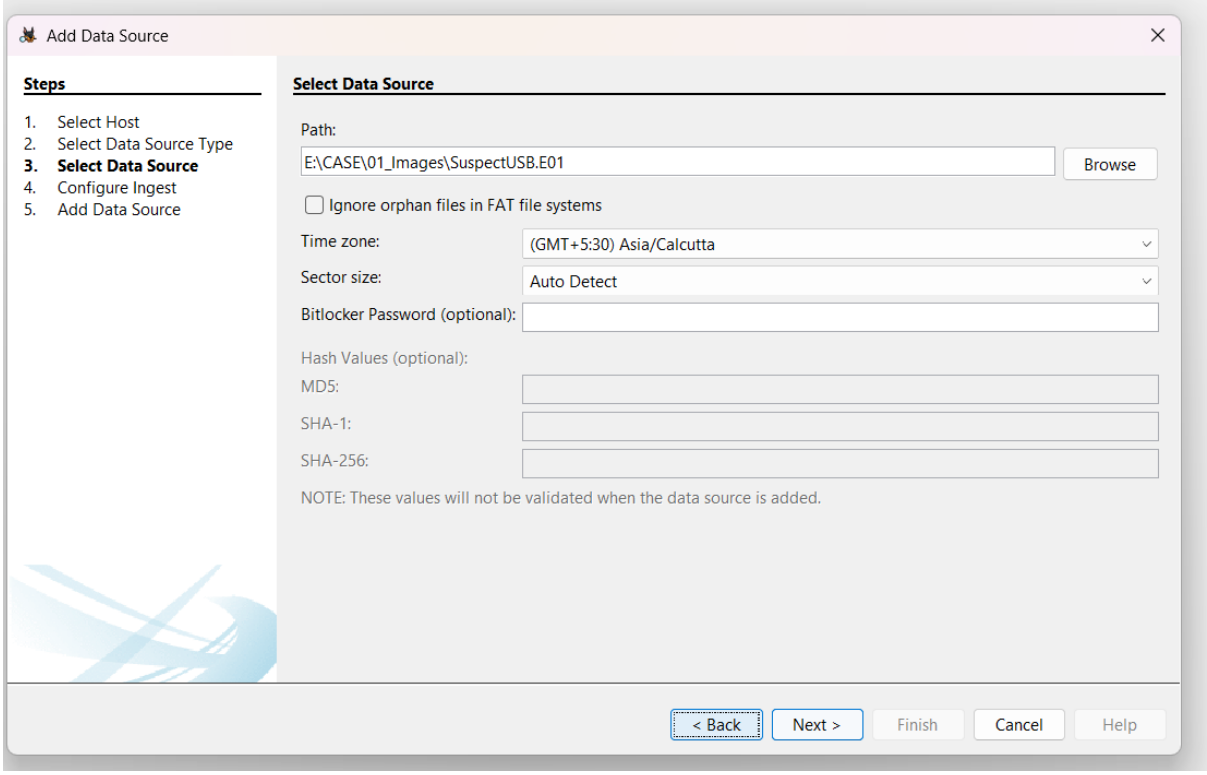



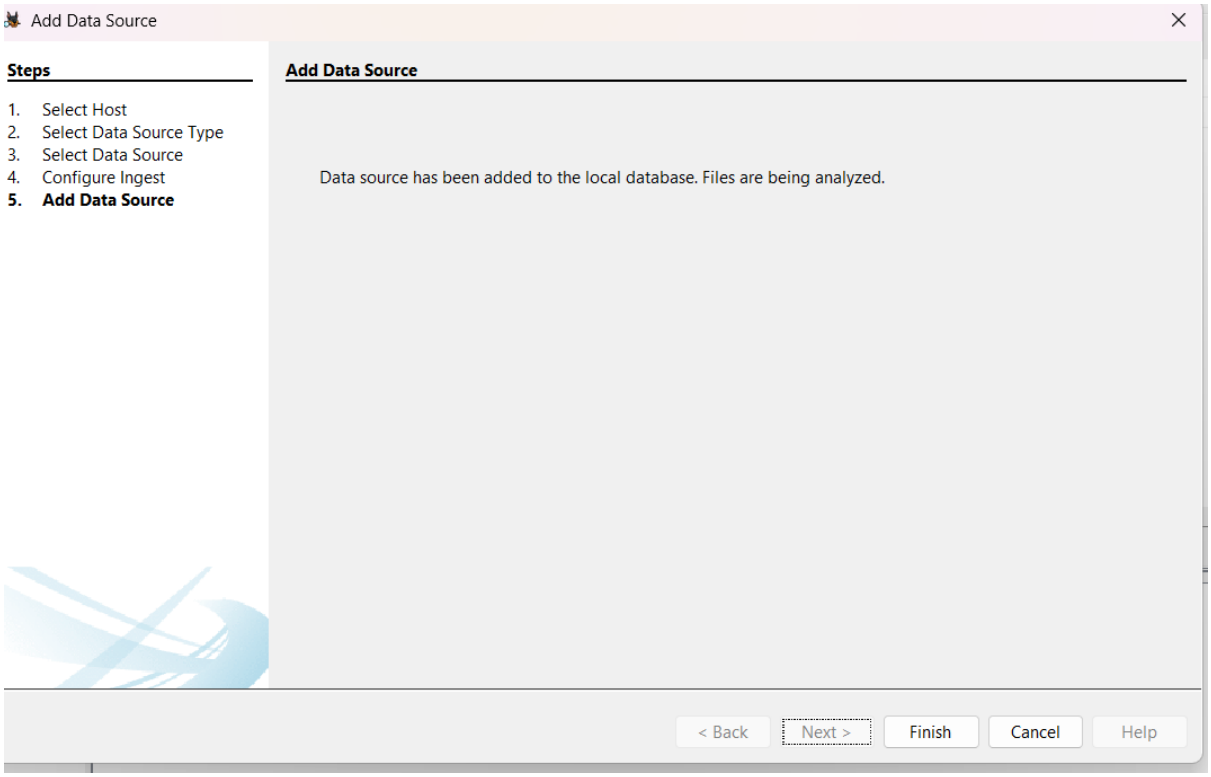

**B.Open Evidence in Autopsy**

1. Launch **Autopsy**.
2. **Create New Case**:
    - Case Name: USB Deleted File Recovery.
    - Base Directory: C:\Case\02_Working\.
3. **Add Data Source → Disk Image / VM File**.

- Browse to your .E01 or .dd image file from step 2.
- Select **Time Zone**.

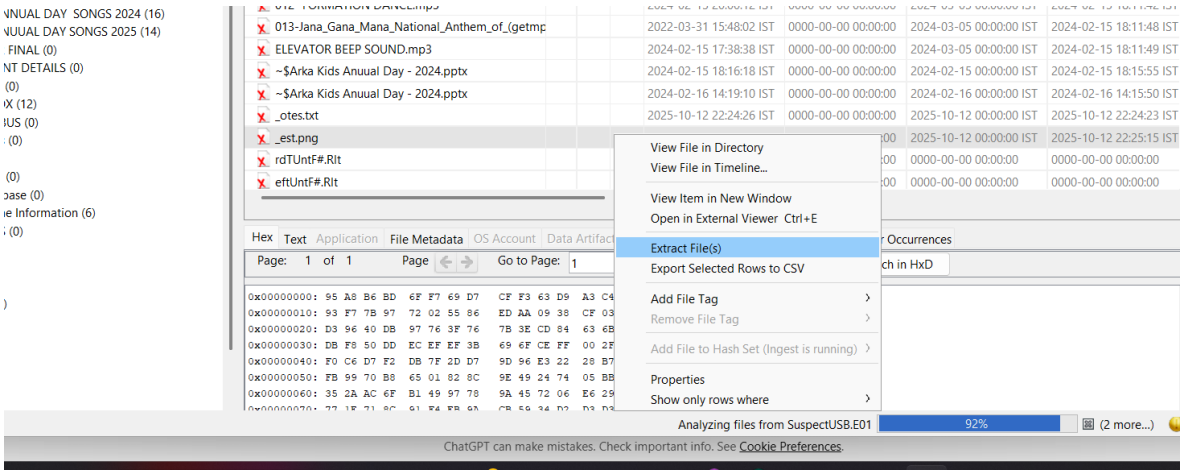
4. **Configure Ingest Modules** → tick:
   - File Type Identification
   - Deleted Files / Carved Files
   - (Optional) Keyword Search, Hash Lookup
5. Start ingest → wait for Autopsy to process.






## C.Locate & Recover Deleted Files

1. Left panel → **Views → Deleted Files**.
2. Browse recovered entries (e.g., confidential.docx, image1.jpg).
3. Right-click file → **Extract File(s)**.
4. Save to: C:\Case\03_Recovered_Files\.



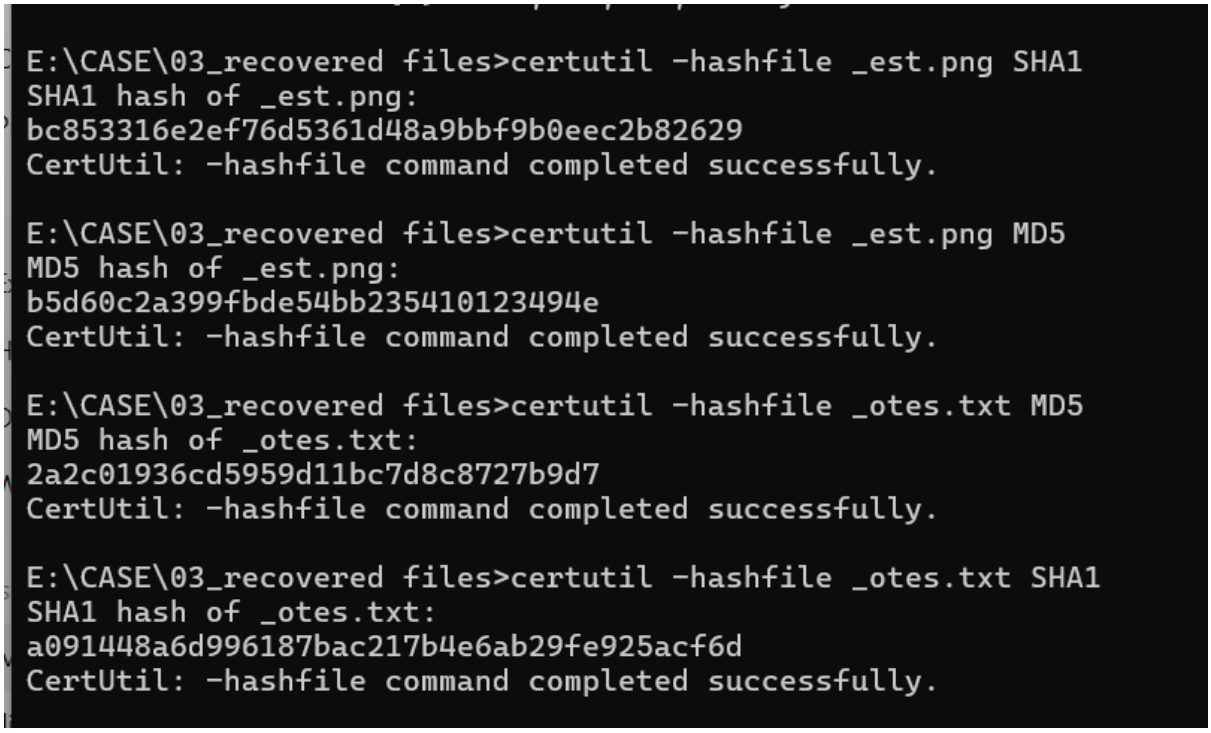
---

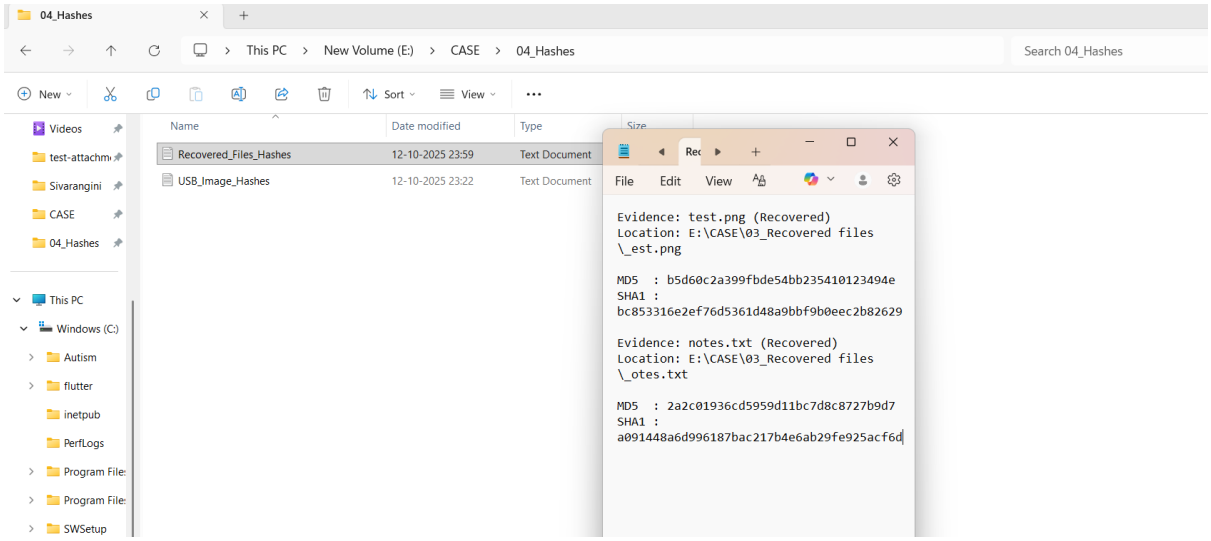
**D. Verify Integrity with Hashes**

1. Open **Command Prompt** in C:\Case\03_Recovered_Files\.
2. Run:
3. certutil -hashfile confidential.docx MD5
4. certutil -hashfile confidential.docx SHA1

Save results into a text file in C:\Case\04_Hashes\.

5. Repeat for all recovered files.






**CONCLUSION:**

The deleted-files recovery was completed successfully from a verified forensic image (E01) using Autopsy/FTK Imager. Recovered files were exported to 03_Recovered_Files/ and MD5/SHA1 hashes recorded in 04_Hashes/ to preserve integrity. No changes were made to the original media; some files may be partially unrecoverable if overwritten prior to imaging.