

Madhesh M A  
231901029

**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.

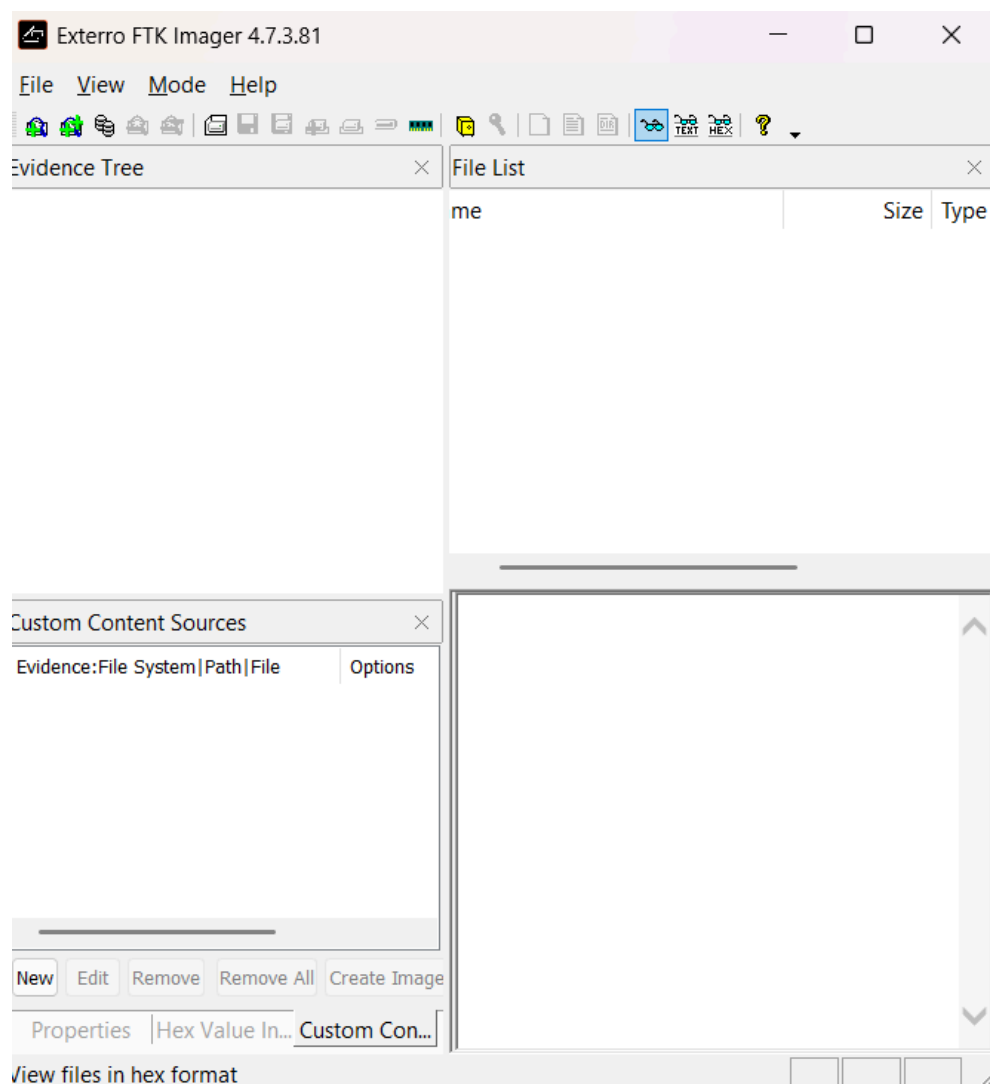
**Step-by-Step Procedure**

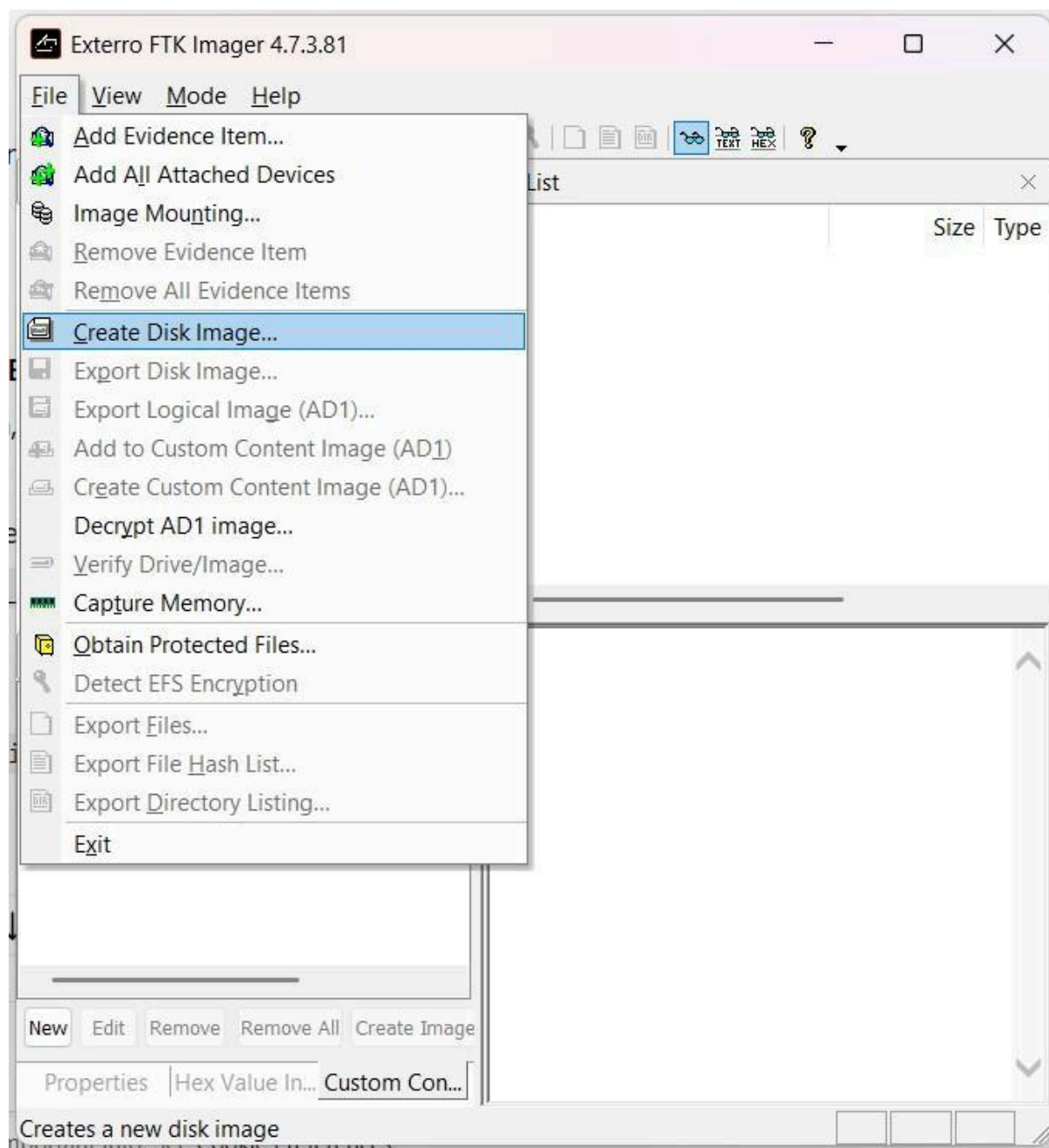
**A. With FTK Imager**

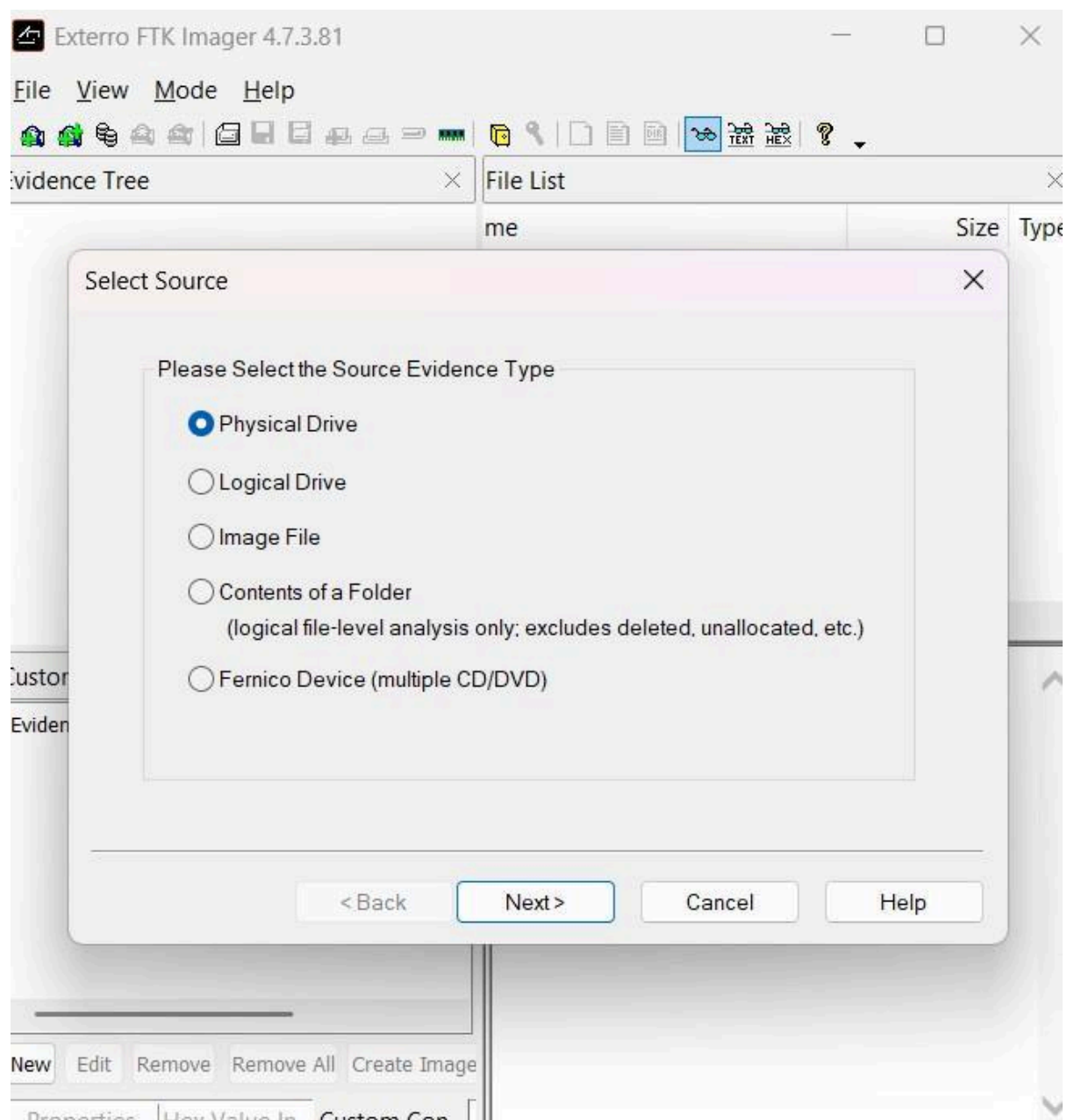
1. Run **FTK Imager (as Administrator)**.
2. **File** → **Create Disk Image**.
3. Select **Physical Drive** → choose the USB stick.
4. Format: choose **E01** (preferred forensic format).
5. Destination: save in a folder like C:\Case\01\_Images\.
6. Tick **Verify images after creation**.
7. FTK will output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

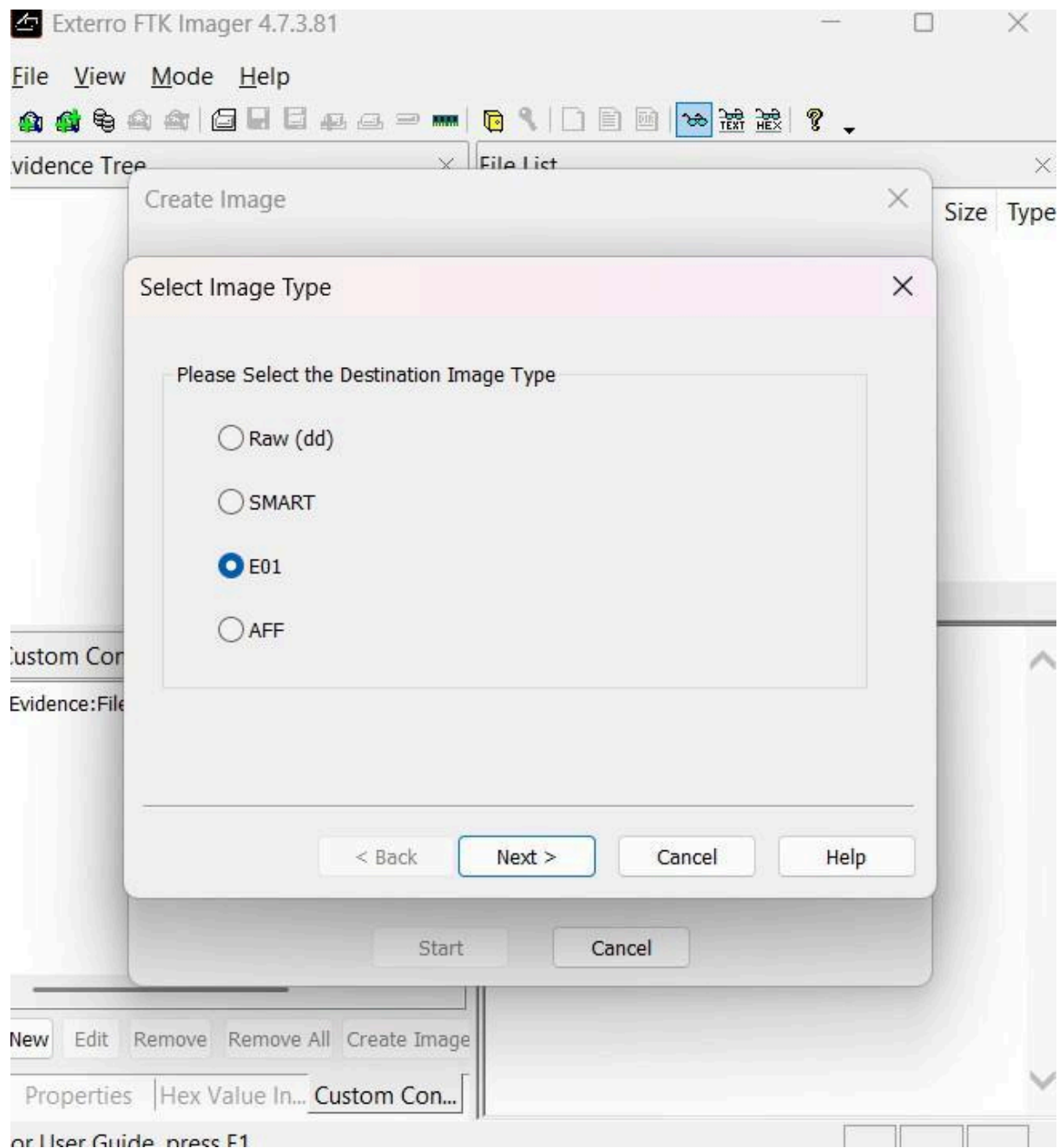
## EXP NO:3

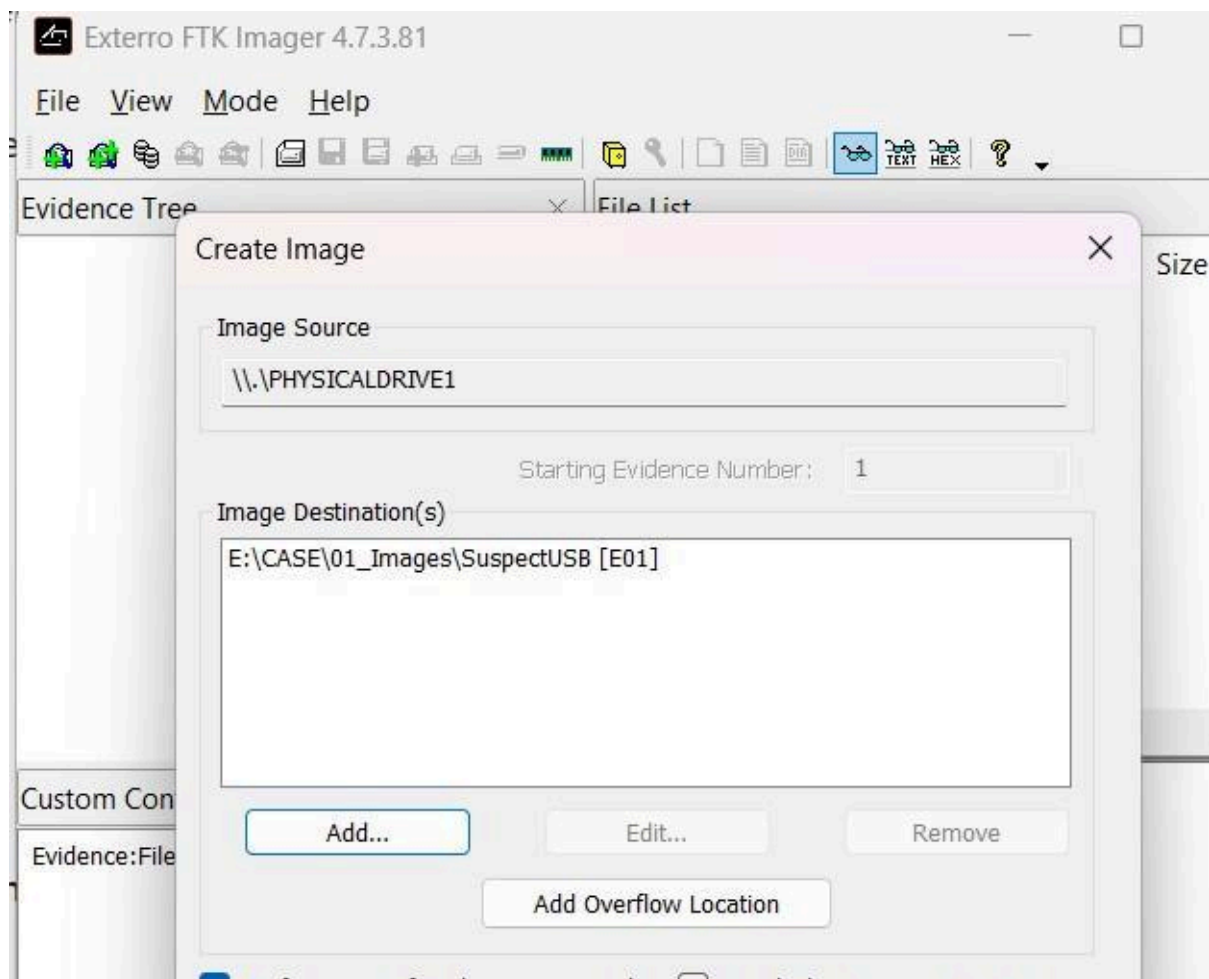
## Recover Deleted Files using Forensics Tools





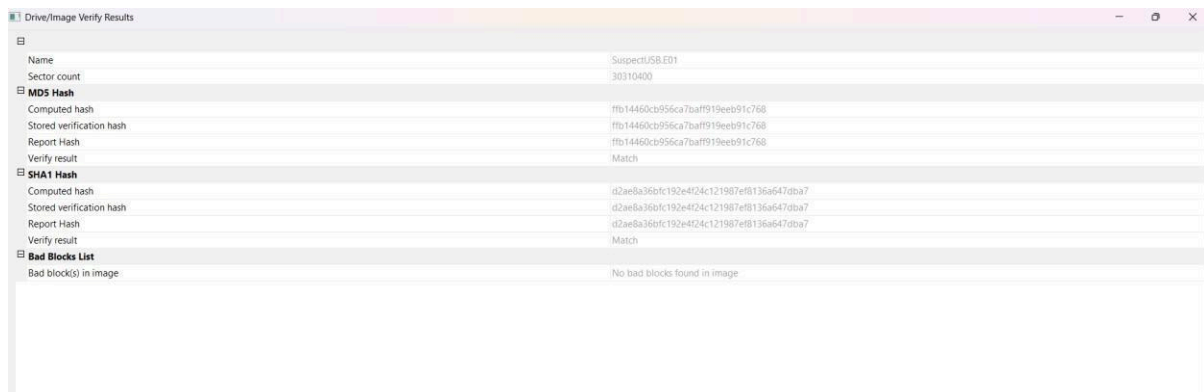
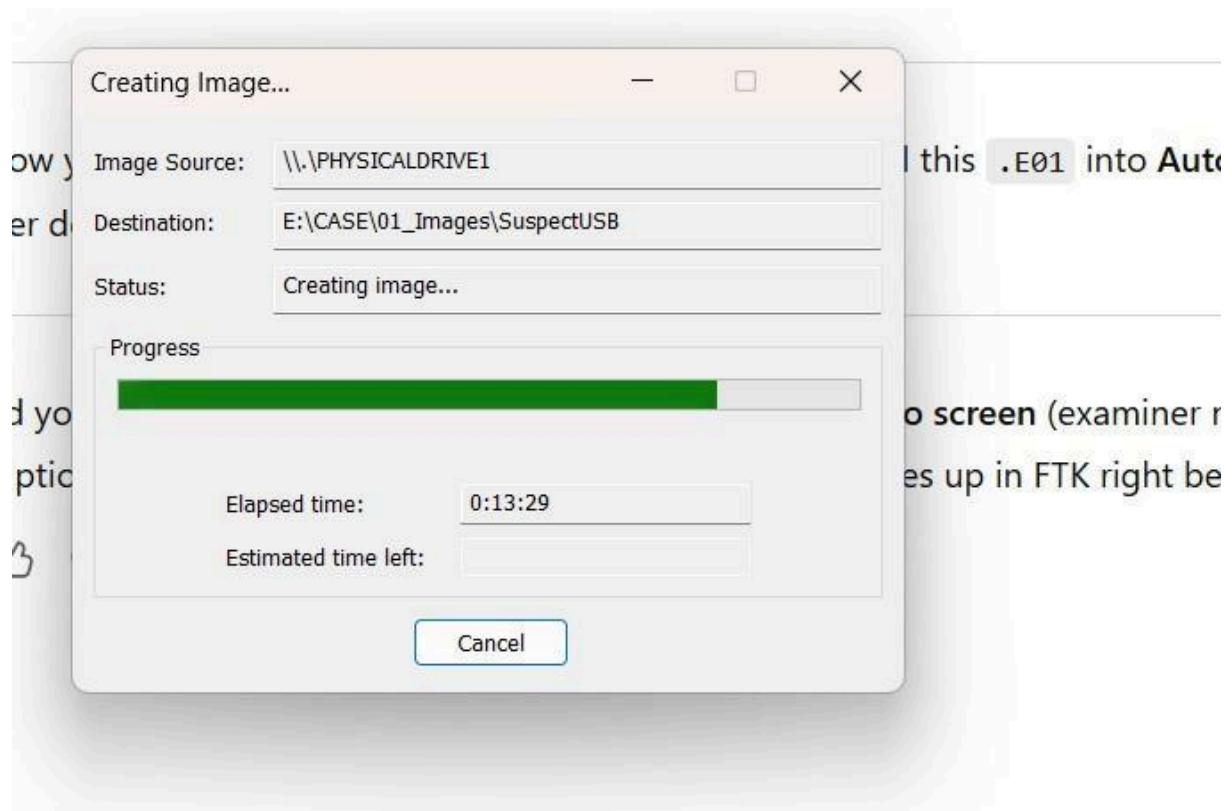






## EXP NO:3

## Recover Deleted Files using Forensics Tools



### B. Open Evidence in Autopsy

1. Launch **Autopsy**.
2. **Create New Case:**
  - o Case Name: USB Deleted File Recovery.
  - o Base Directory: C:\Case\02\_Working\.



3. **Add Data Source** → **Disk Image / VM File.**

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

4. **Configure Ingest Modules** → tick:

- o File Type Identification
- o Deleted Files / Carved Files
- o (Optional) Keyword Search, Hash Lookup

## 5. Start ingest → wait for Autopsy to process.

**Add Data Source**

**Steps**

1. Select Host
2. Select Data Source Type
- 3. Select Data Source**
4. Configure Ingest
5. Add Data Source

**Select Data Source**

Path:

☐ Ignore orphan files in FAT file systems

Time zone:

Sector size:

Bitlocker Password (optional):

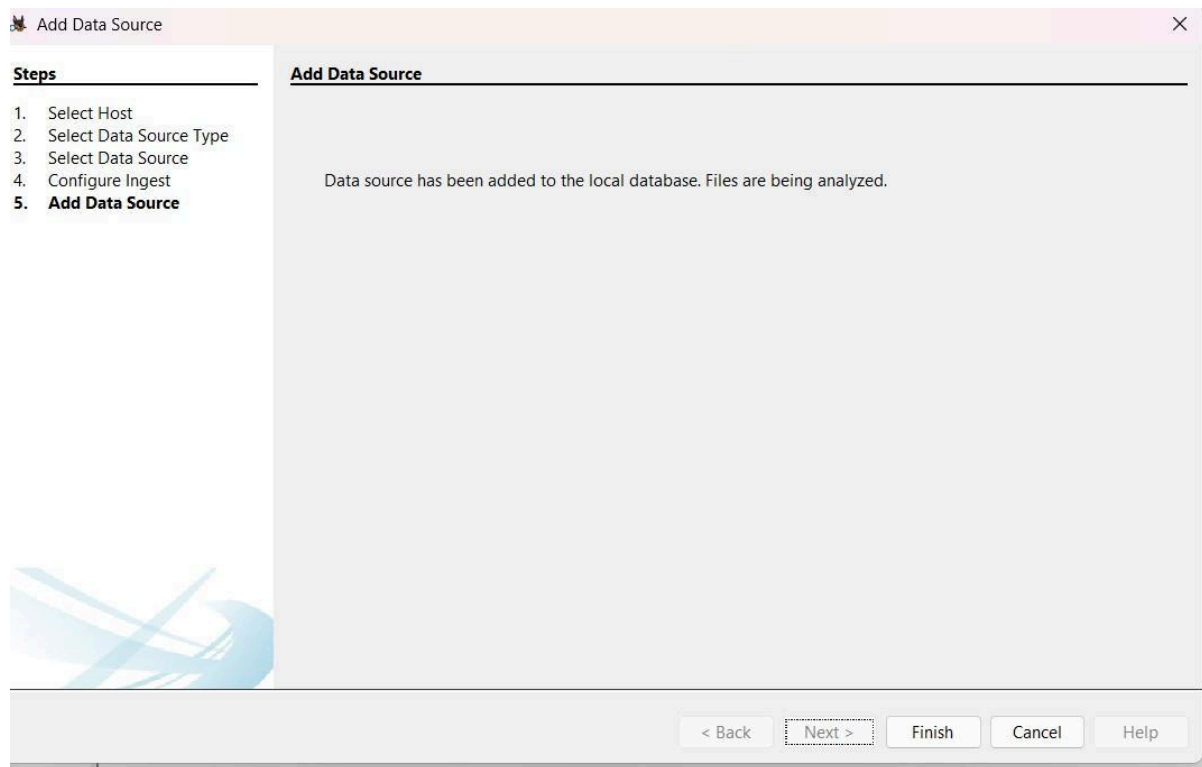
Hash Values (optional):

MD5:

SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

**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\.

## EXP NO:3

## Recover Deleted Files using Forensics Tools

The screenshot displays a forensic tool interface with a list of recovered files on the left and a main pane showing file details and a context menu. The file list includes:

- ANNUAL DAY SONGS 2024 (16)
- ANNUAL DAY SONGS 2025 (14)
- FINAL (0)
- NT DETAILS (0)
- (0)
- X (12)
- IUS (0)
- (0)
- (0)
- ase (0)
- ie Information (6)
- (0)

The main pane shows a table of file details with columns for File Name, Date, Time, and Size. The context menu is open, showing options like 'View File in Directory', 'View File in Timeline...', 'View Item in New Window', 'Open in External Viewer Ctrl+E', 'Extract File(s)', 'Export Selected Rows to CSV', 'Add File Tag', 'Remove File Tag', 'Add File to Hash Set (Ingest is running)', 'Properties', and 'Show only rows where'. The bottom status bar indicates 'Analyzing files from SuspectUSB.E01' with a progress bar at 92%.

### 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.

## EXP NO:3

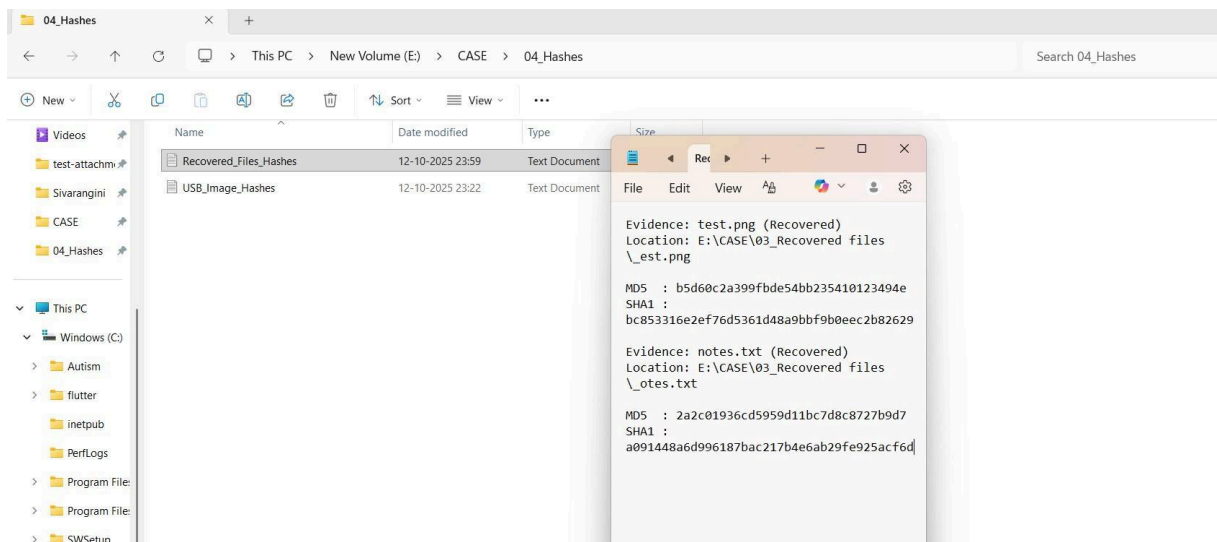
## Recover Deleted Files using Forensics Tools

```
E:\CASE\03_recovered files>certutil -hashfile _est.png SHA1
SHA1 hash of _est.png:
bc853316e2ef76d5361d48a9bbf9b0eec2b82629
CertUtil: -hashfile command completed successfully.

E:\CASE\03_recovered files>certutil -hashfile _est.png MD5
MD5 hash of _est.png:
b5d60c2a399fbde54bb235410123494e
CertUtil: -hashfile command completed successfully.

E:\CASE\03_recovered files>certutil -hashfile _otes.txt MD5
MD5 hash of _otes.txt:
2a2c01936cd5959d11bc7d8c8727b9d7
CertUtil: -hashfile command completed successfully.

E:\CASE\03_recovered files>certutil -hashfile _otes.txt SHA1
SHA1 hash of _otes.txt:
a091448a6d996187bac217b4e6ab29fe925acf6d
CertUtil: -hashfile command completed successfully.
```



## 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

**EXP NO:3**

**Recover Deleted Files using Forensics  
Tools**

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.