



Bhuvaneshwar-Naidu / DF_Lab



Code

Issues

Pull requests

Actions

Projects

Wiki

Security



DF_Lab / Exp_1_FTK Imager.md



Bhuvaneshwar-Naidu Update Exp_1_FTK Imager.md

57e0674 · now



178 lines (109 loc) · 5.33 KB

Preview

Code

Blame



Raw



Ex.No.1 Evidence Acquisition with FTK Imager

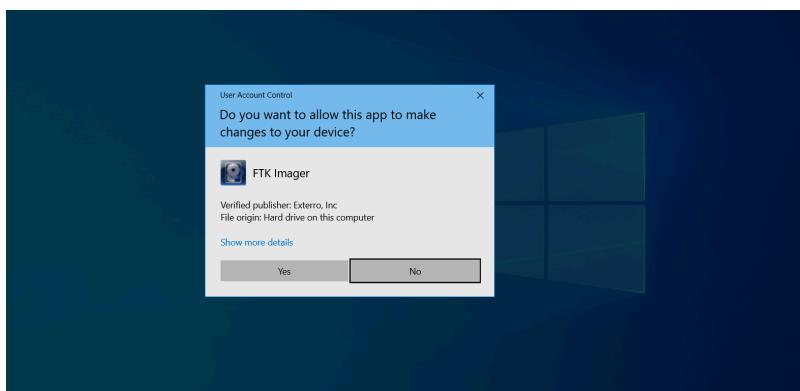
Aim

To acquire volatile memory (RAM) and non-volatile memory (disk image) from a target system using AccessData FTK Imager, while preserving integrity through hashing and proper documentation.

Acquiring Volatile Memory (RAM)

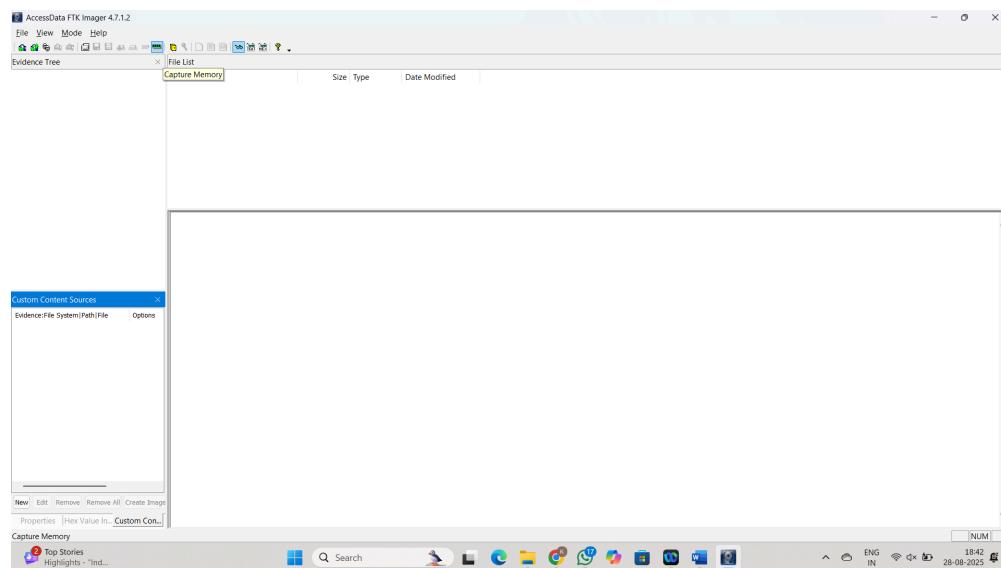
Step 1: Launch FTK Imager as Administrator

- Right-click on FTK Imager and select Run as Administrator.
- This ensures the tool has sufficient privileges to access system memory.



Step 2: Open Capture Memory Utility

- Below the Menu Bar, click Capture Memory...

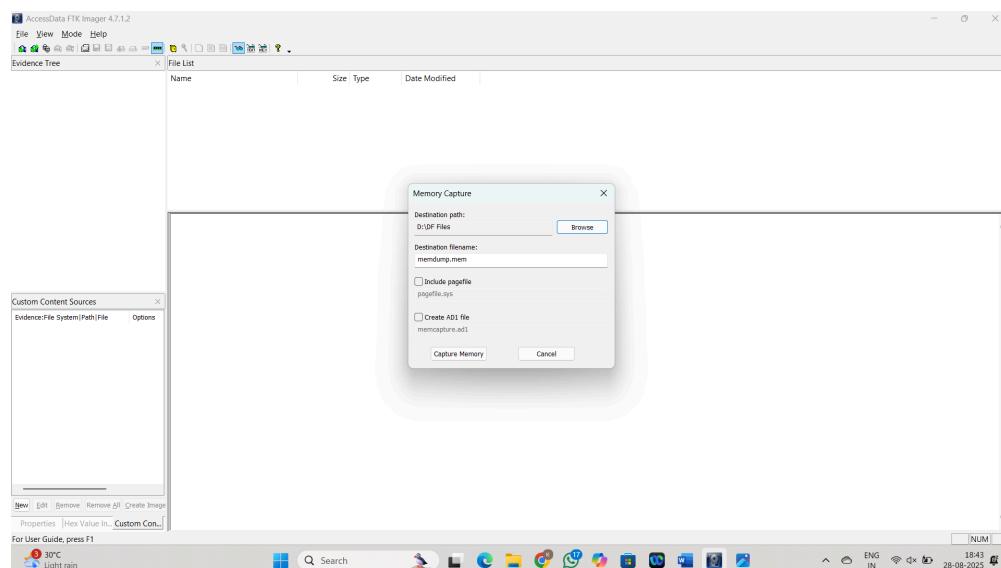


Step 3: Configure Capture Options

In the pop-up dialog:

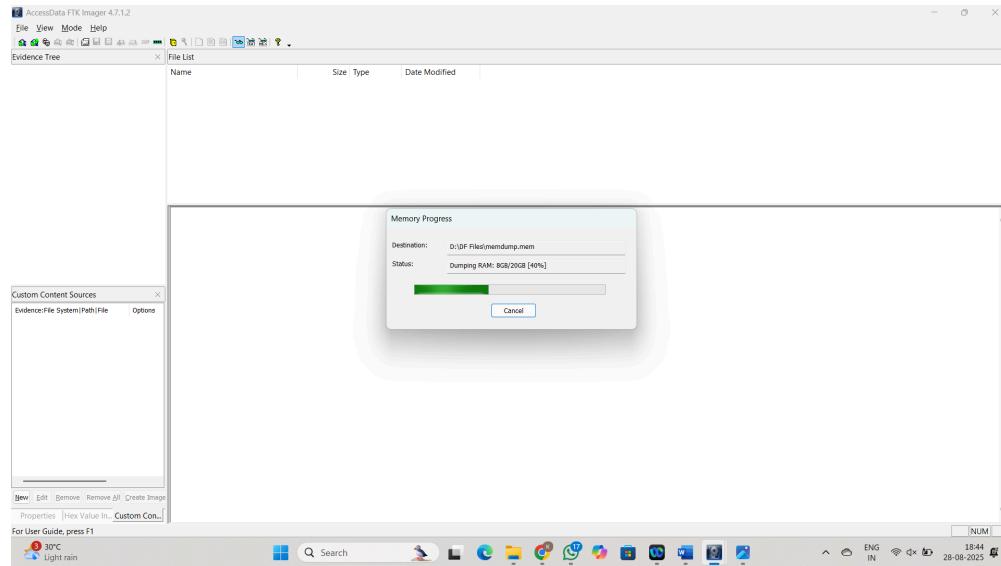
- Destination Path** → Choose an **external drive** (not the system drive).
- Destination Filename** → Default is `memdump.mem` (rename if required).
- Include Pagefile.sys (Optional)** → Captures virtual memory stored on disk.
- Create AD1 File (Optional)** → Wraps output into an AccessData container.

Tip: Including `pagefile.sys` can reveal hidden processes and artifacts.



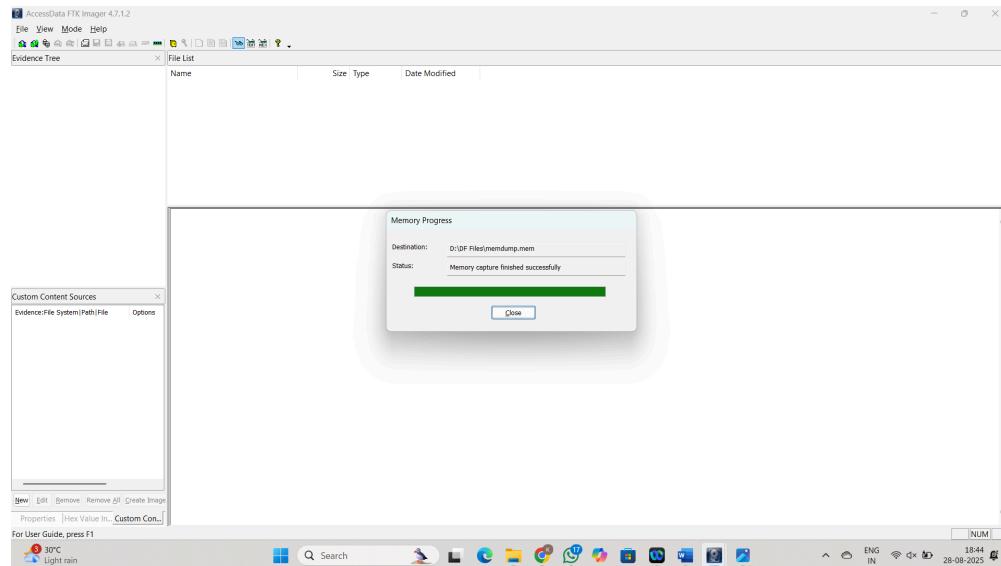
Step 4: Begin Capture

- Click Capture Memory to start.
- A progress bar shows the status.



Step 5: Completion

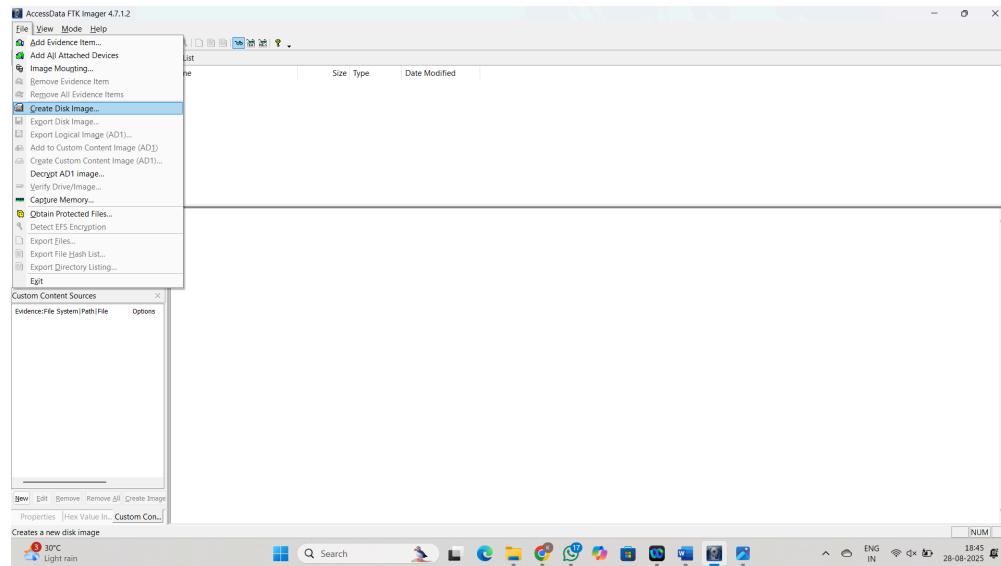
- The `.mem` file will be created in the destination folder.
- Capture time depends on installed RAM size.



Acquiring Non-Volatile Memory (Disk Image)

Step 1: Start Disk Imaging

- In FTK Imager, go to File → Create Disk Image...

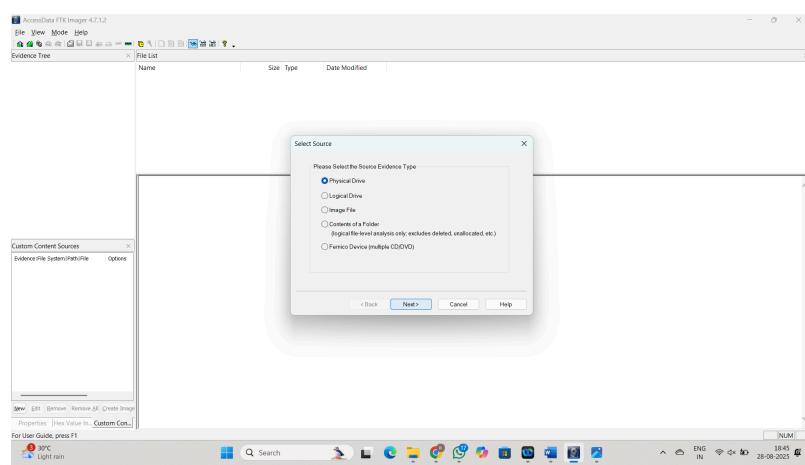


Step 2: Select Source Type

Choose based on requirement:

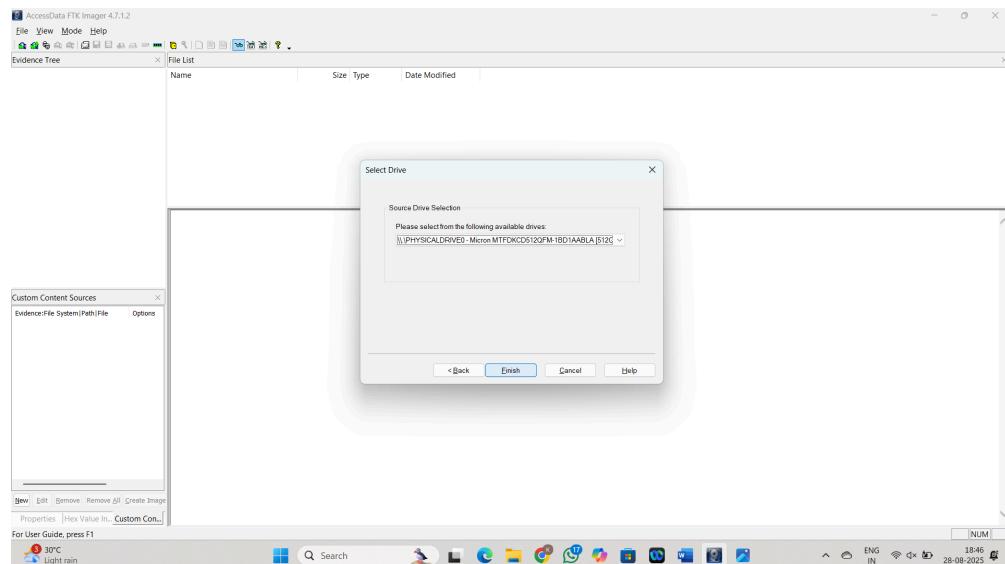
- Physical Drive** → Entire disk (preferred).
- Logical Drive** → Single partition (e.g., C:).
- Image File** → Re-image an existing file.
- Folder / CD/DVD** → Acquire folder or removable media.

Forensic best practice: Always select **Physical Drive** with a write blocker.



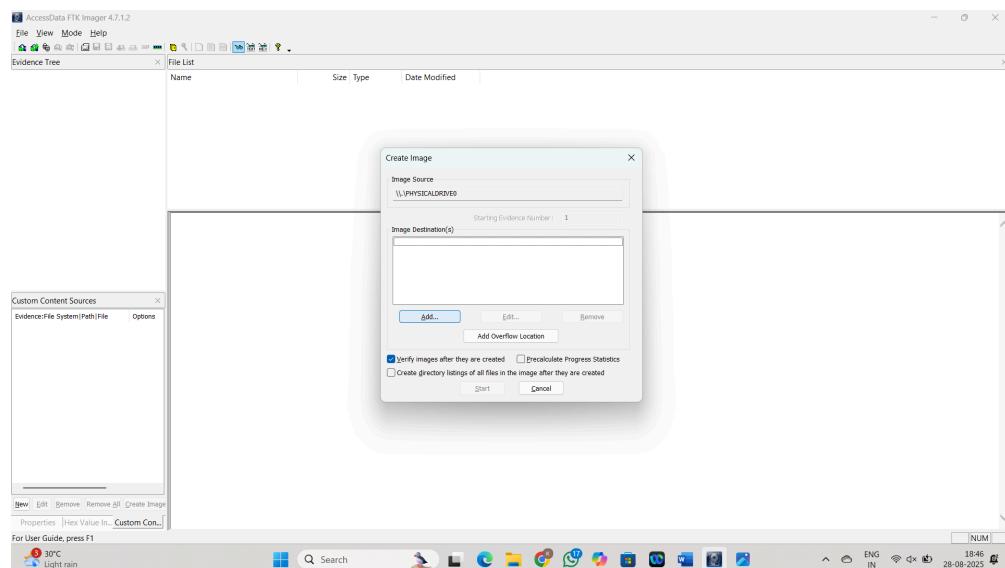
Step 3: Select Drive

- Pick the drive from the list.
- Confirm and click **Finish**.



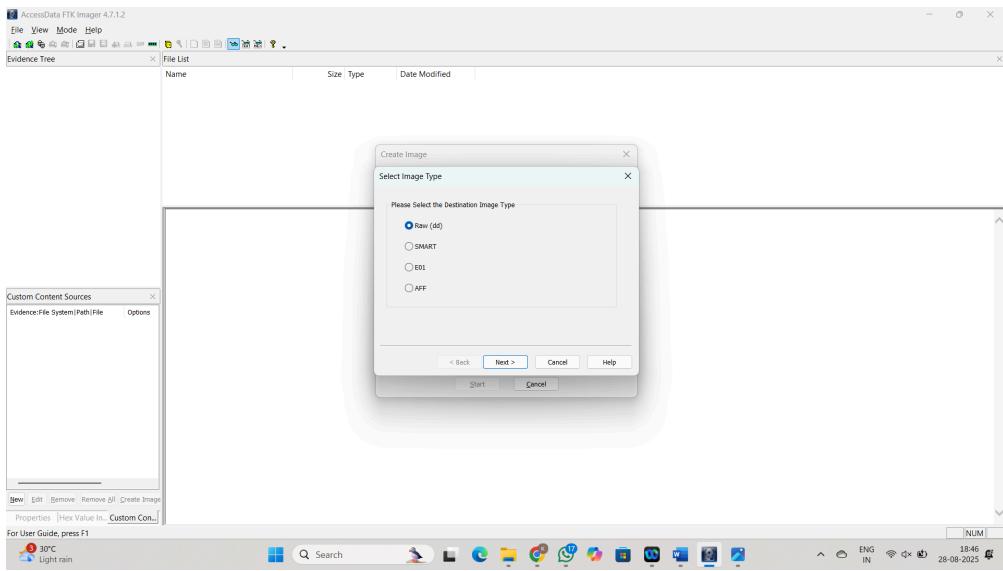
Step 4: Configure Destination & Format

- Click **Add...** to define image format and storage path.

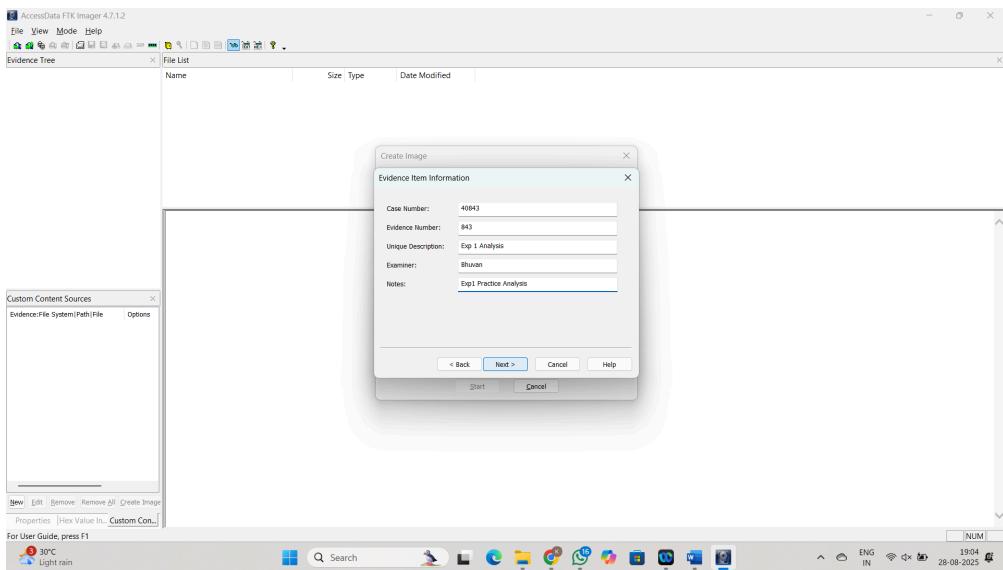


- **Image Type:**

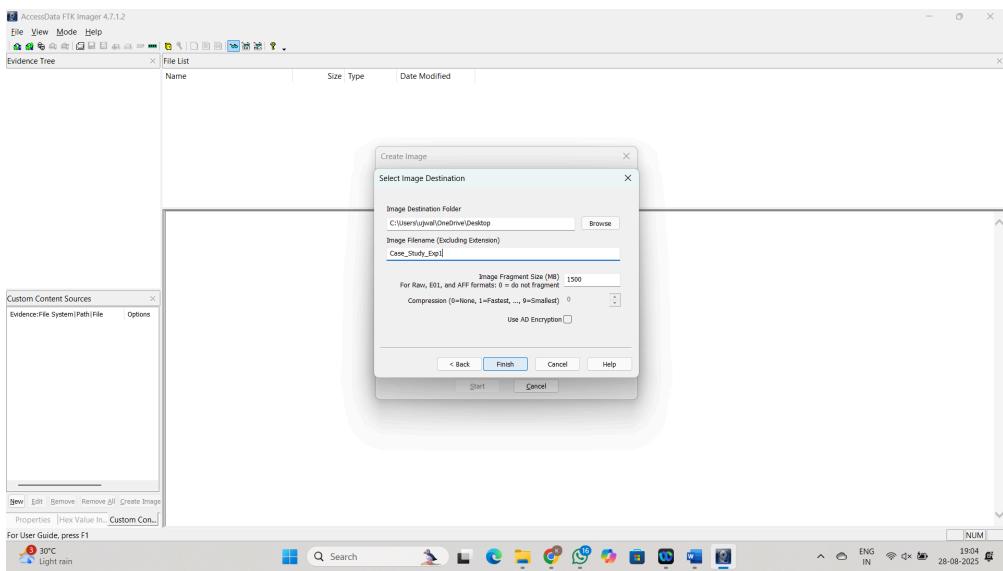
- **E01 (EnCase)** → Recommended (metadata + compression).
- **RAW (dd)** → Bit-for-bit copy.



- Enter Case Info: Examiner, Case No., Notes.

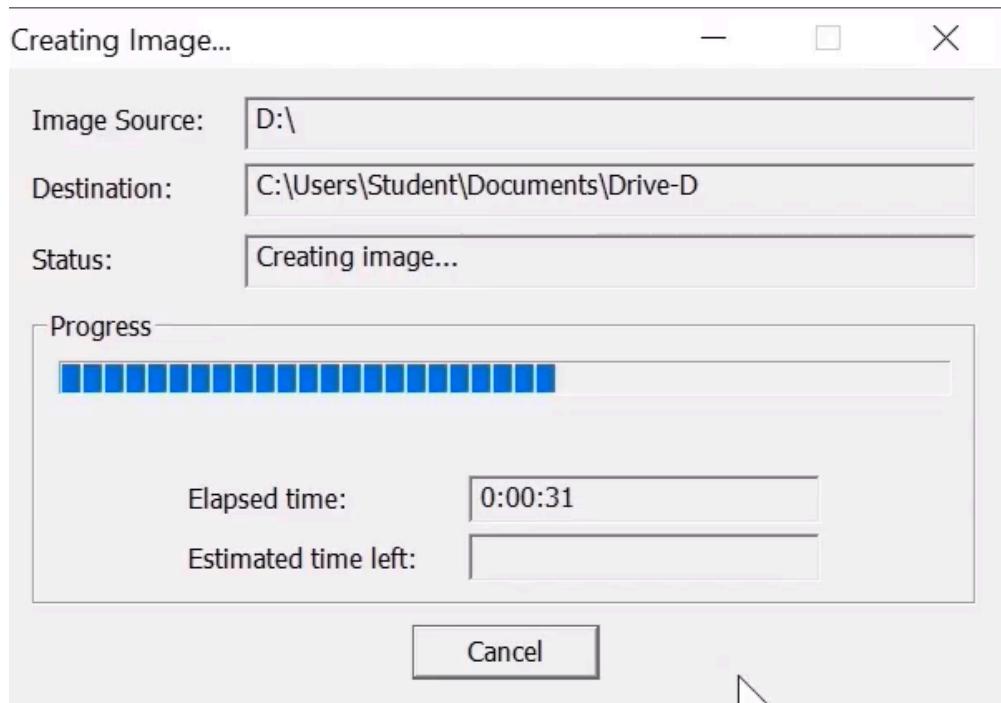
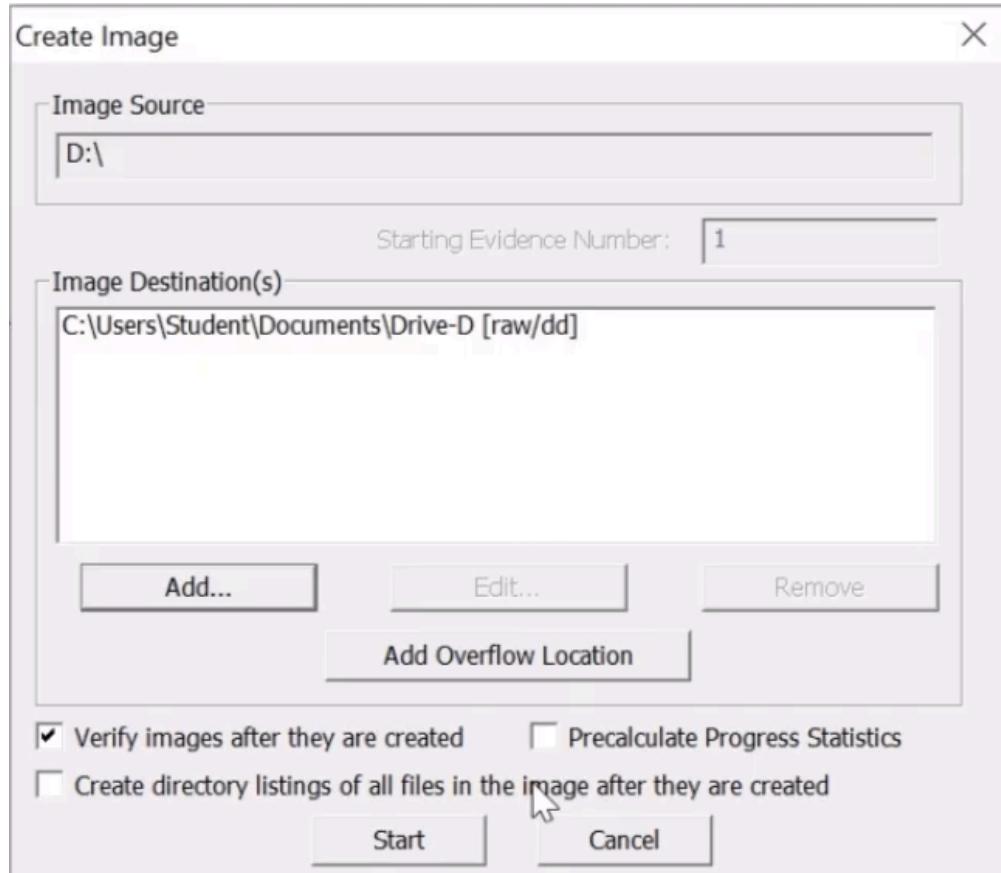


- Set Destination Folder (different from source).
- Fragment Size: Set 0 for a single file.



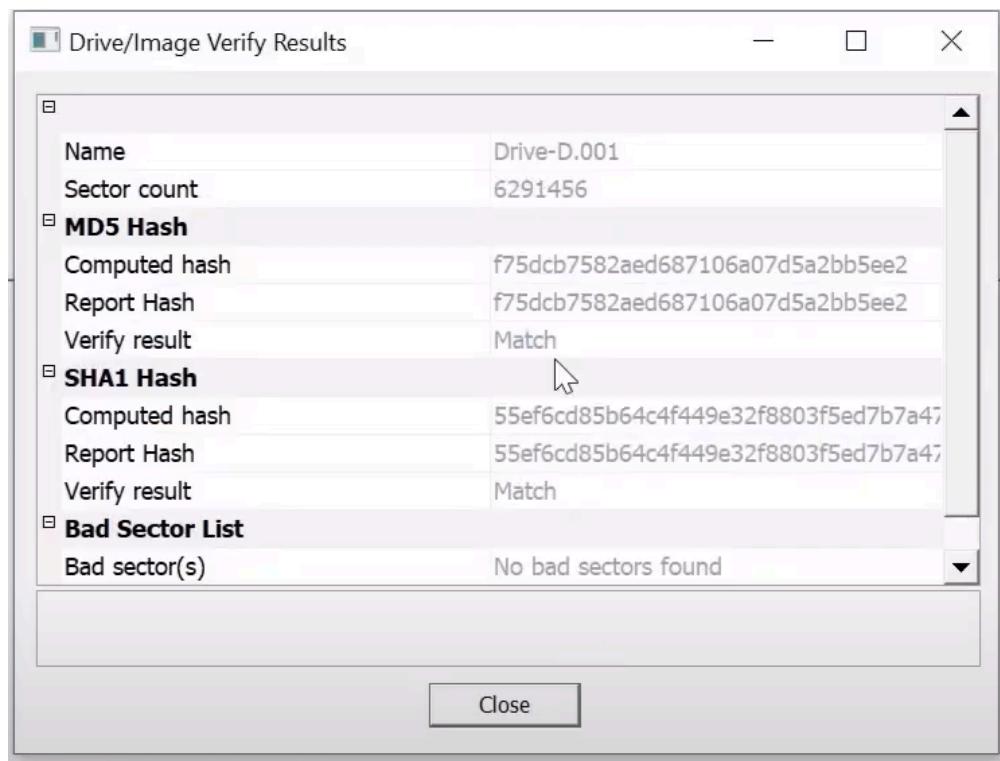
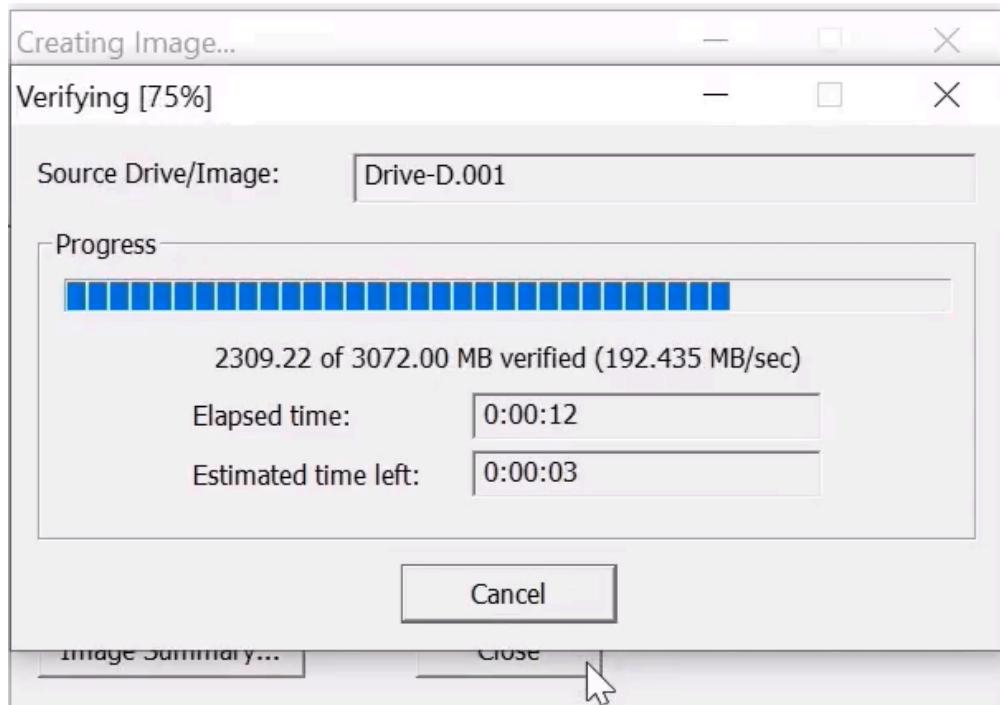
Step 5: Imaging Process

- Check **Verify images after creation** to generate hash values.
- Click **Start** to begin acquisition.



Step 6: Verify Integrity

- On completion, FTK Imager displays **MD5/SHA1** hashes.
- If hashes match, the image is valid and unaltered.



Rubrics

Criteria	Mark Allotted	Mark Awarded
1. GitHub Activity & Submission Regularity	3	
2. Application of Forensic Tools & Practical Execution	3	
3. Documentation & Reporting	2	
4. Engagement, Problem-Solving & Team Collaboration	2	
<i>Total</i>	<i>10</i>	

Result

Successfully acquired the **RAM dump (.mem)** and **disk image (.E01)** of the target system using **FTK Imager**.

The **MD5/SHA1 hash values** of the acquired images were verified, confirming that the evidence was collected without alteration and is **forensically sound**.