PRACTICAL: 1

Forensic imaging and analysis tool designed to acquire, create forensic images, and perform detailed analysis using FTK imager tool.

Aim: To create a forensically sound image file of a storage device using FTK Imager while ensuring data integrity for digital forensic investigation.

System Prerequisites

- Computer system with **Windows Operating System**
- **FTK Imager** installed on the system
- Minimum **4 GB RAM** (8 GB recommended)
- Sufficient **free disk space** to store the forensic image file
- **Administrator privileges** on the system

Tools Required

- FTK Imager
- External storage device (to store the image file)

About FTK (Forensic Toolkit)

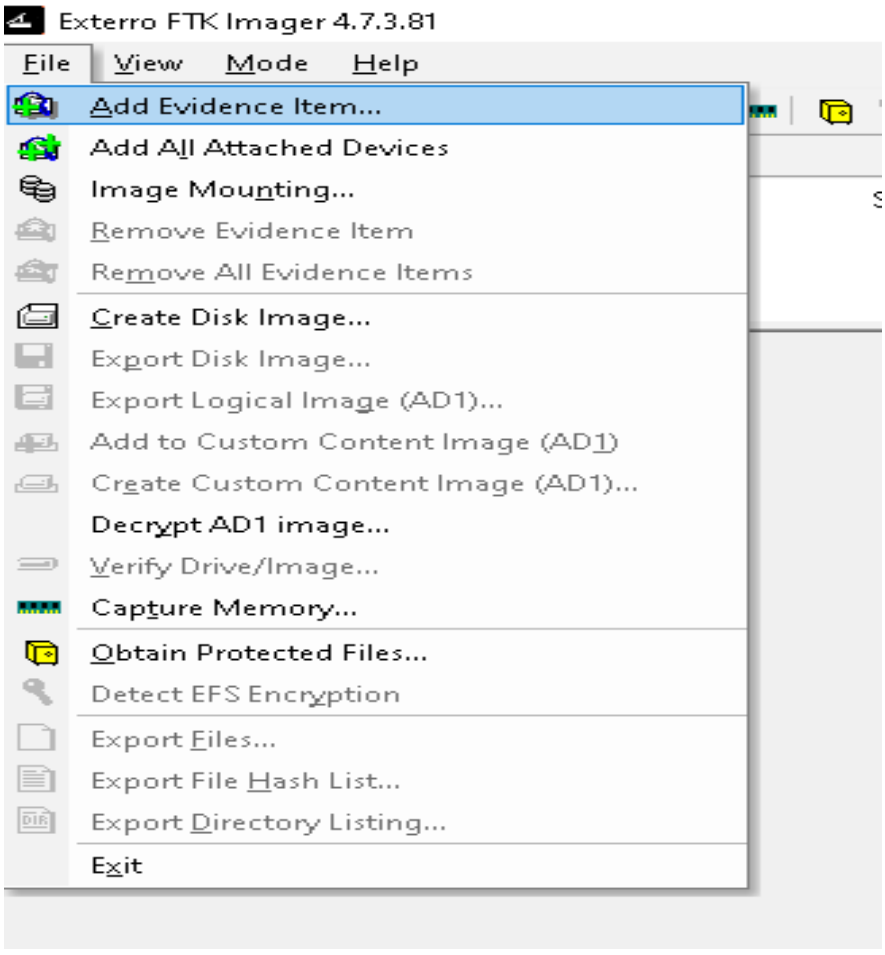
FTK (Forensic Toolkit) is a comprehensive digital forensic software developed by AccessData. It is widely used by forensic investigators to acquire, analyze, and report digital evidence from various storage media. FTK supports in-depth analysis of file systems, deleted files, system artifacts, and metadata while ensuring evidence integrity.

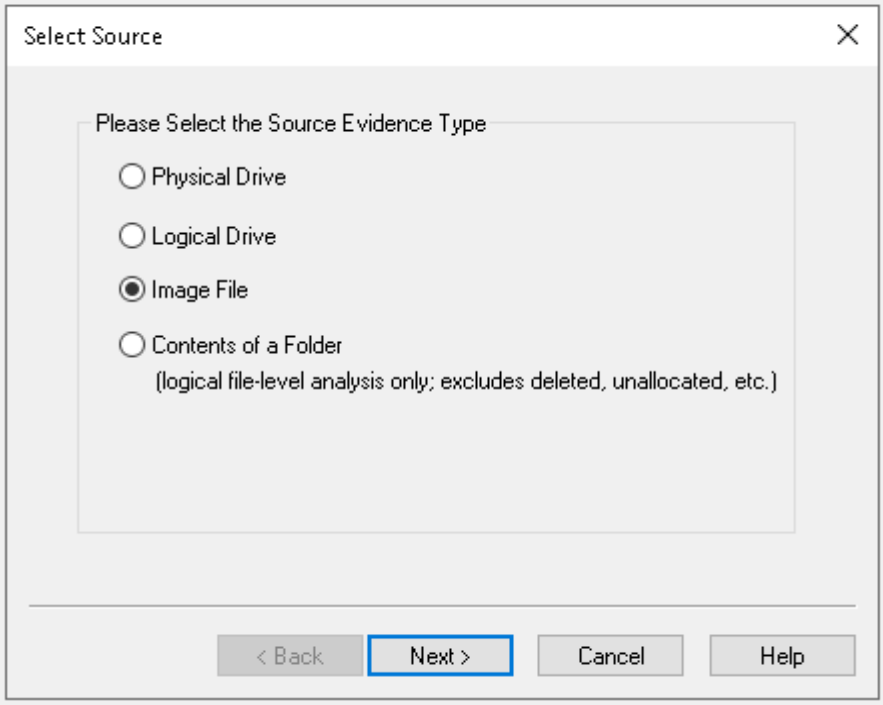
FTK works closely with FTK Imager, which is used for forensic acquisition. The acquired image files are then processed and analyzed in FTK for investigation purposes. The tool provides advanced features such as keyword searching, data carving, registry analysis, email analysis, and bookmarking of evidence, making it suitable for professional and academic forensic investigations.

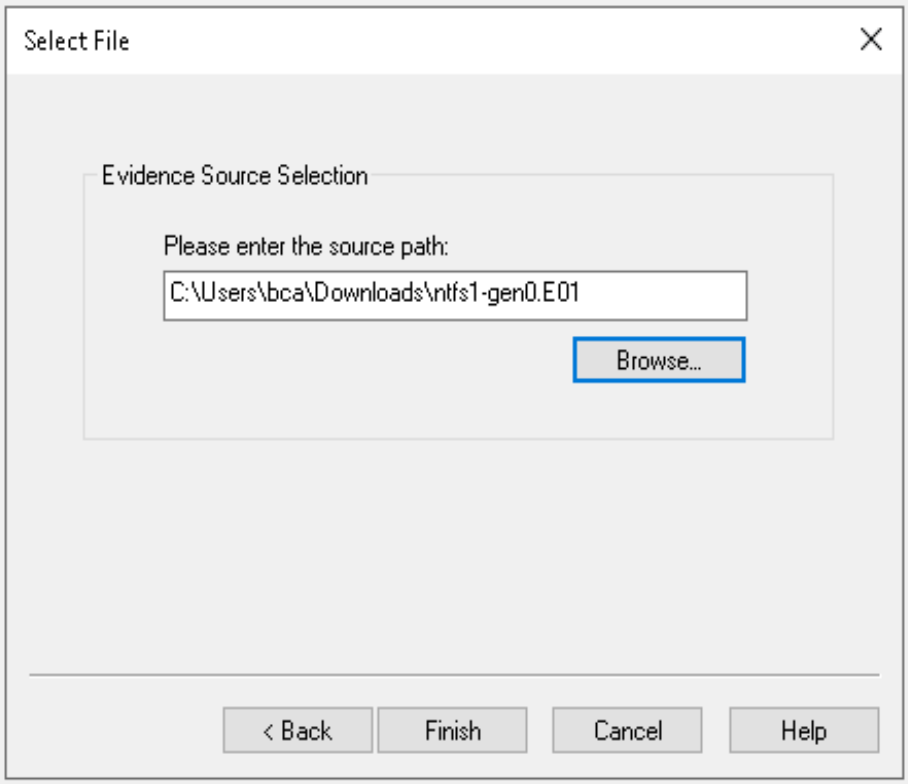
FTK is commonly used in cyber crime investigations, incident response, corporate investigations, and academic digital forensics laboratories.

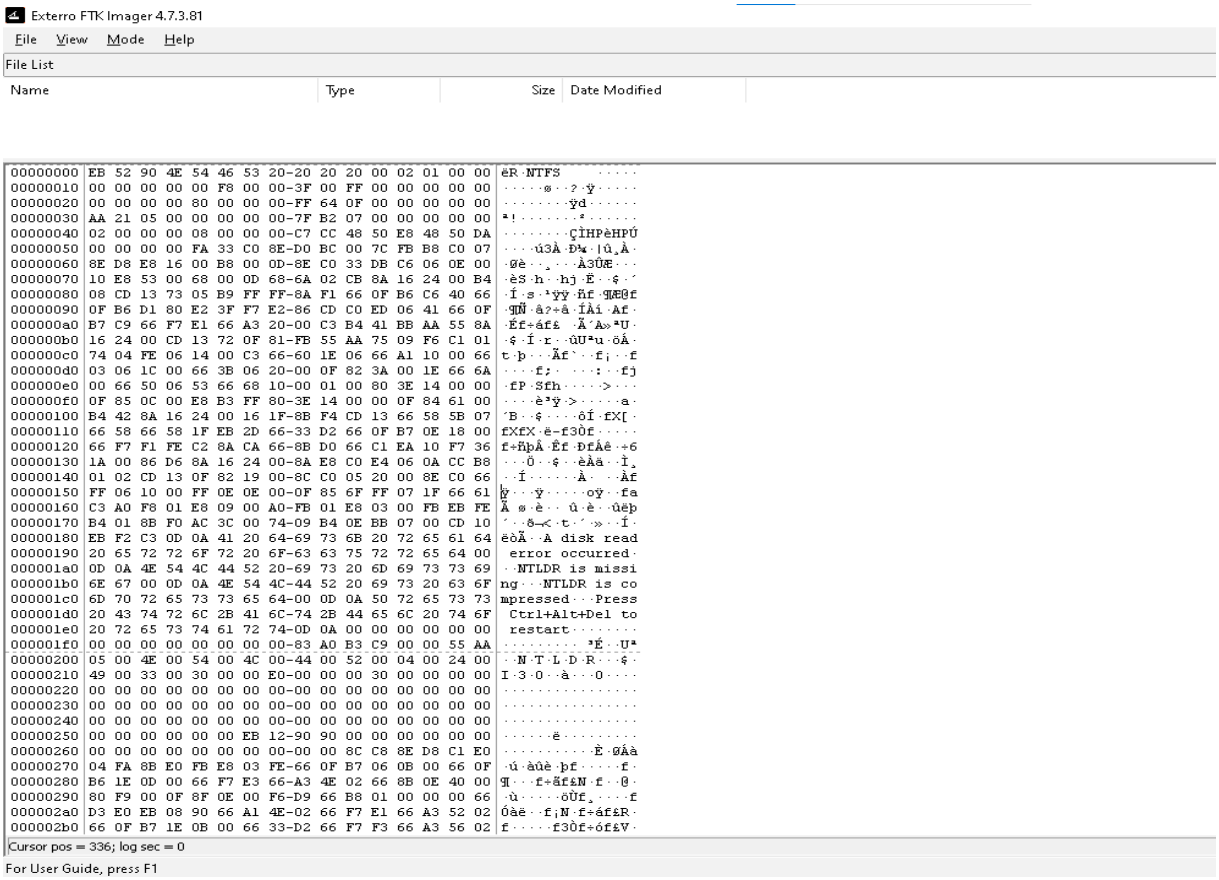
Procedure: (ATTACH SCREENSHOTS ALONG WITH EACH STEP)

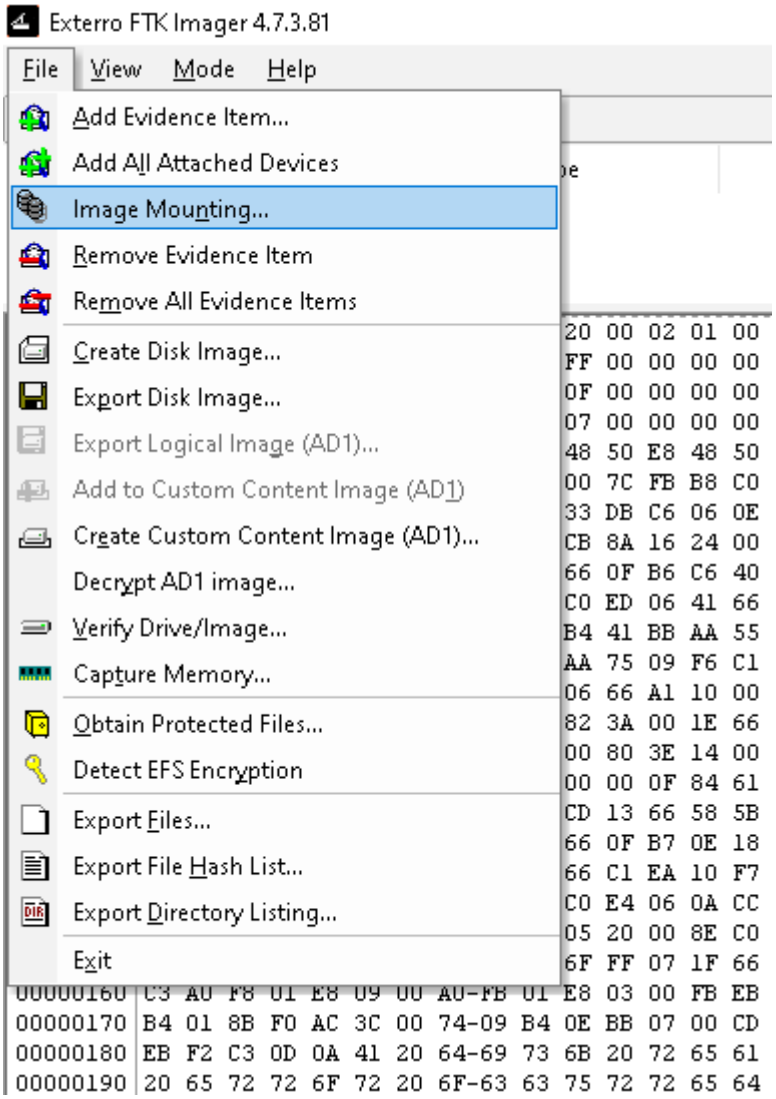
1. Open FTK Imager with administrator privileges.
2. Click on File → Create Disk Image.
3. Select the source type (Physical Drive / Logical Drive / Image File / Folder contents).
4. Choose the required drive or partition and click Next.
5. Select the image format such as RAW (dd) or E01.
6. Enter case details including case number, evidence number, examiner name, and description.
7. Select the destination path to save the image file.
8. Configure image fragmentation size if required.
9. Enable hash calculation (MD5/SHA1/SHA256).
10. Click Start to begin the imaging process.
11. Wait until the image acquisition is completed.
12. Verify that the generated hash values match.

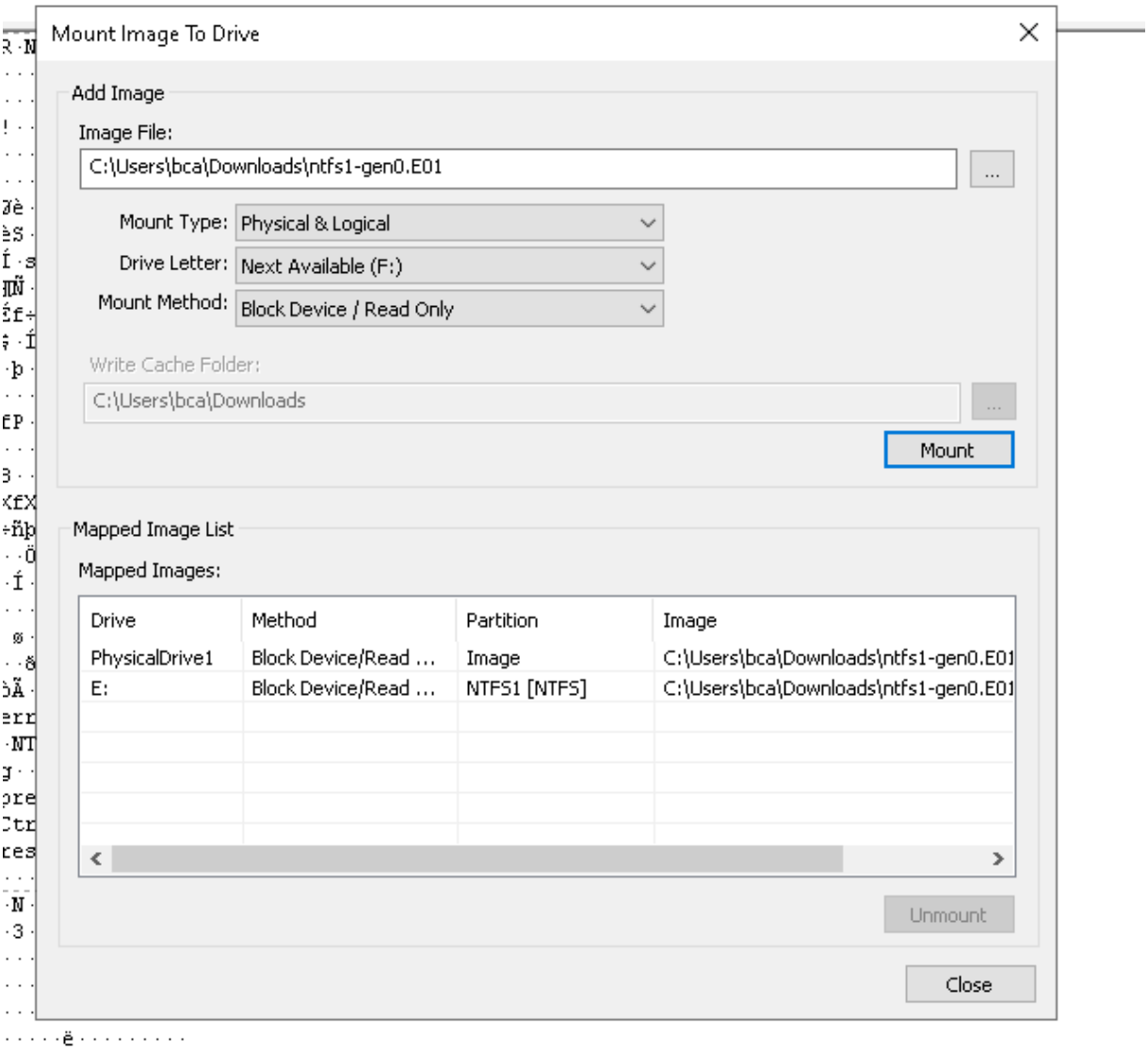



Select Source
Please Select the Source Evidence Type
Physical Drive
Logical Drive
Image File
Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
< Back
Next >
Cancel
Help


Select File
Evidence Source Selection
Please enter the source path:
C:\Users\bca\Downloads\ntfs1-gen0.E01
Browse...
< Back
Finish
Cancel
Help


Exterro FTK Imager 4.7.3.81
File View Mode Help
File List
Name Type Size Date Modified
Cursor pos = 336; log sec = 0
For User Guide, press F1


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



Observation:

- Forensic image file was successfully created
- Hash values before and after imaging were identical
- Data integrity was preserved

Conclusion:

FTK Imager was successfully used to create a forensic image file of a storage device. The matching hash values confirm the integrity and authenticity of the acquired evidence, making it suitable for further forensic analysis.