

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)

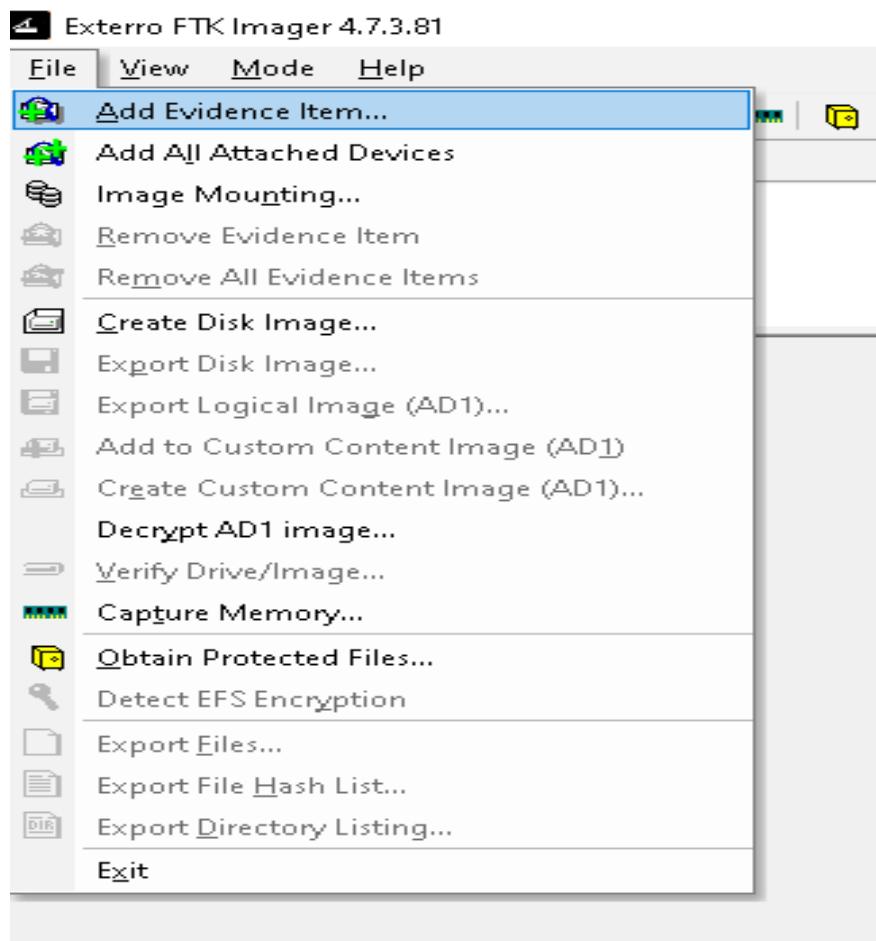
FTK (Forensic Toolkit) is a comprehensive digital forensic software developed by AccessData. It is widely used by forensic investigators to acquire, analyze, and report digital evidence from various storage media. FTK supports in-depth analysis of file systems, deleted files, system artifacts, and metadata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

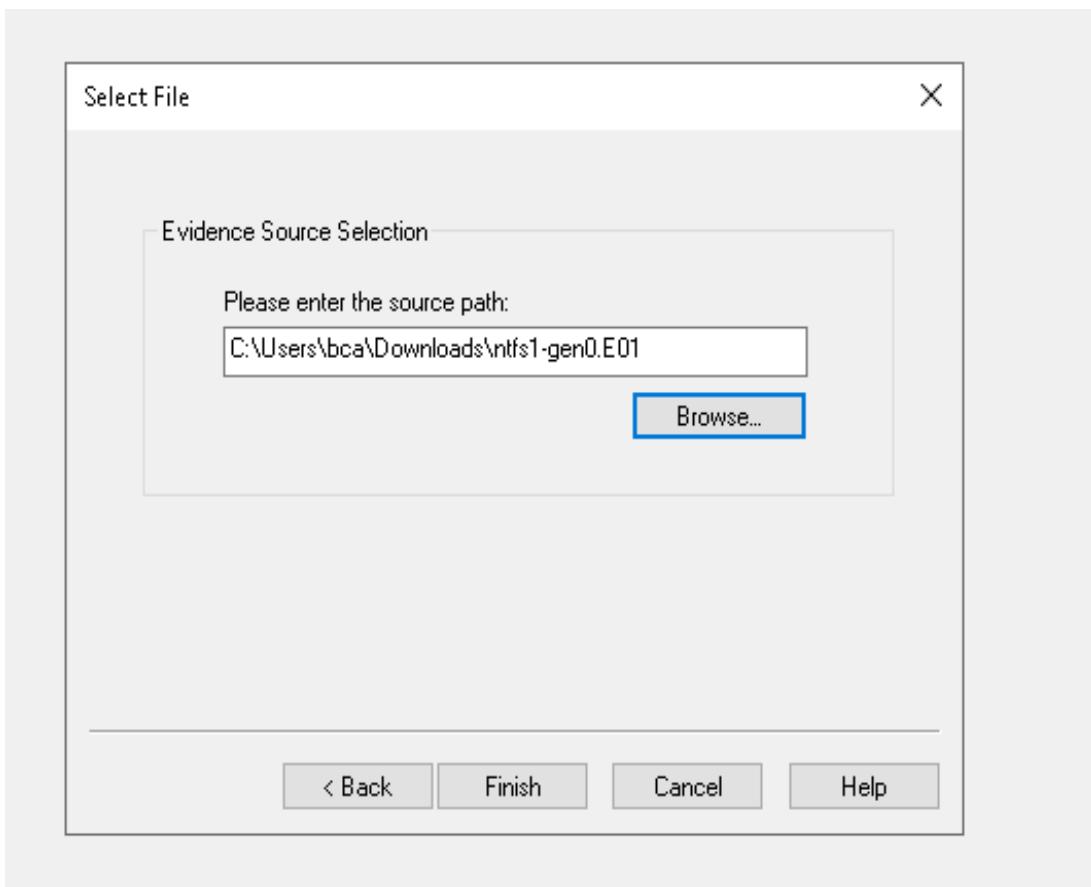
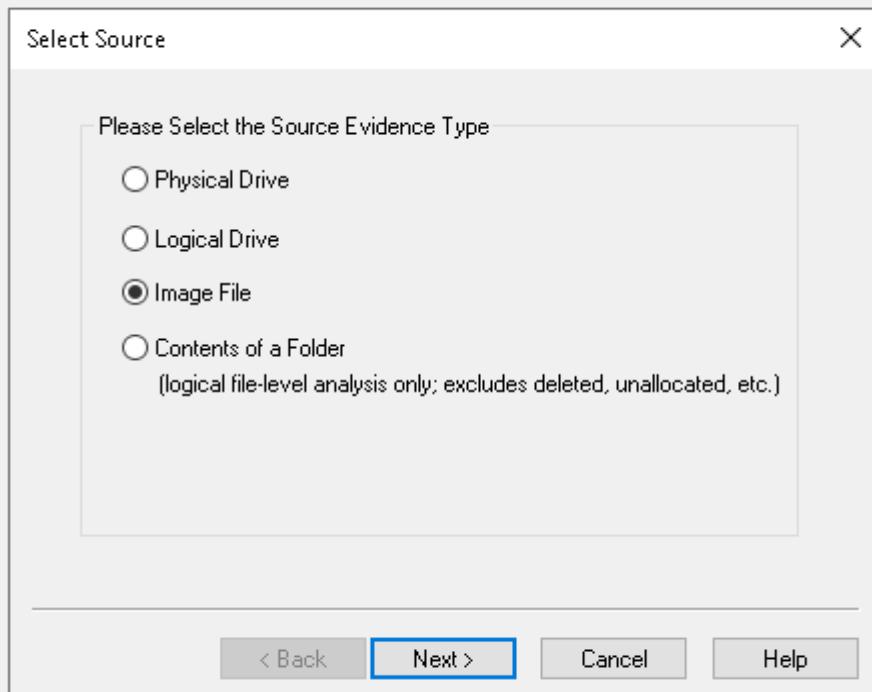
FTK works closely with FTK Imager, which is used for forensic acquisition. The acquired image files are then processed and analyzed in FTK for investigation purposes. The tool provides advanced features such as keyword searching, data carving, registry analysis, email analysis, and bookmarking of evidence,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





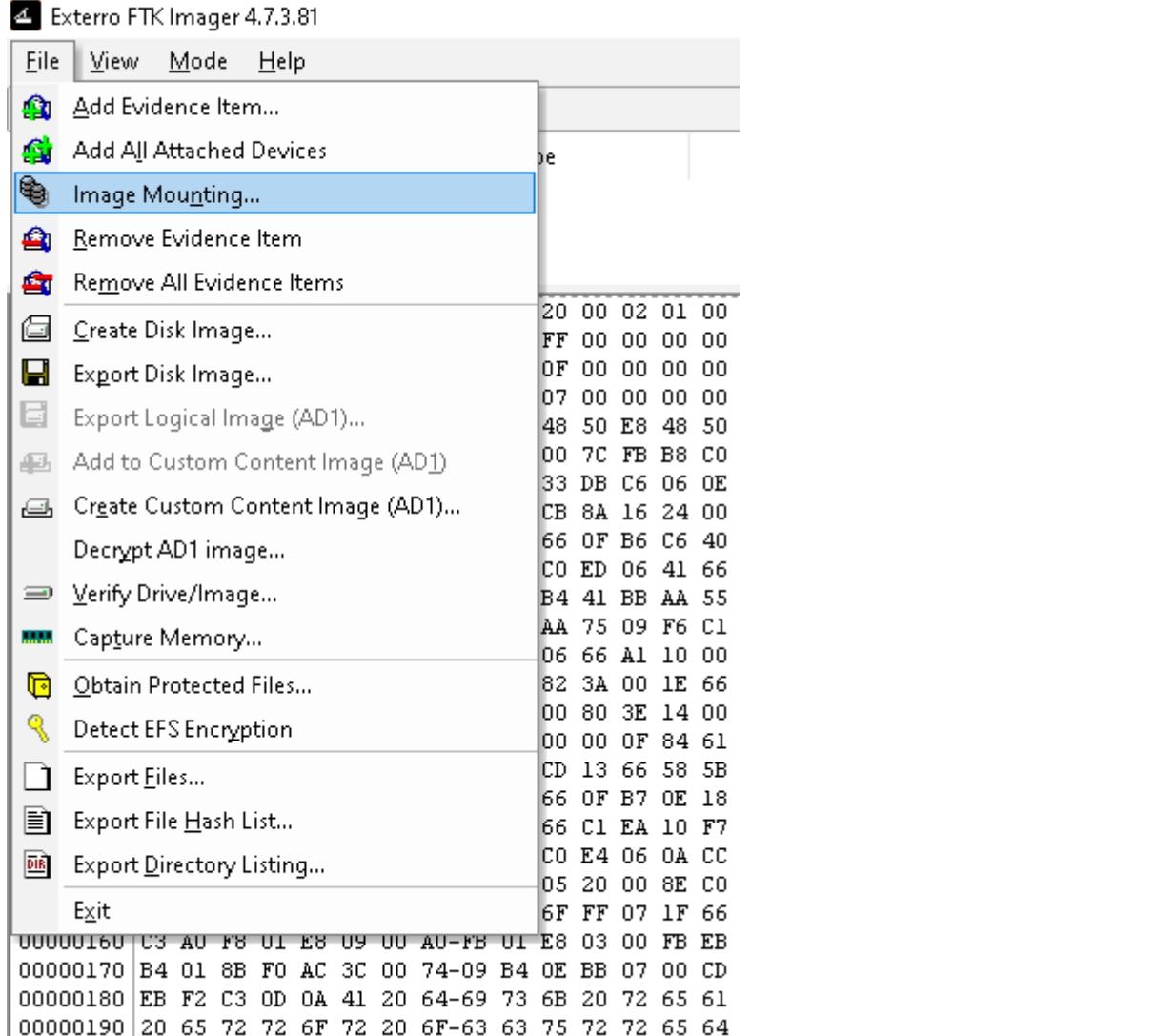
Exterro FTK Imager 4.7.3.81

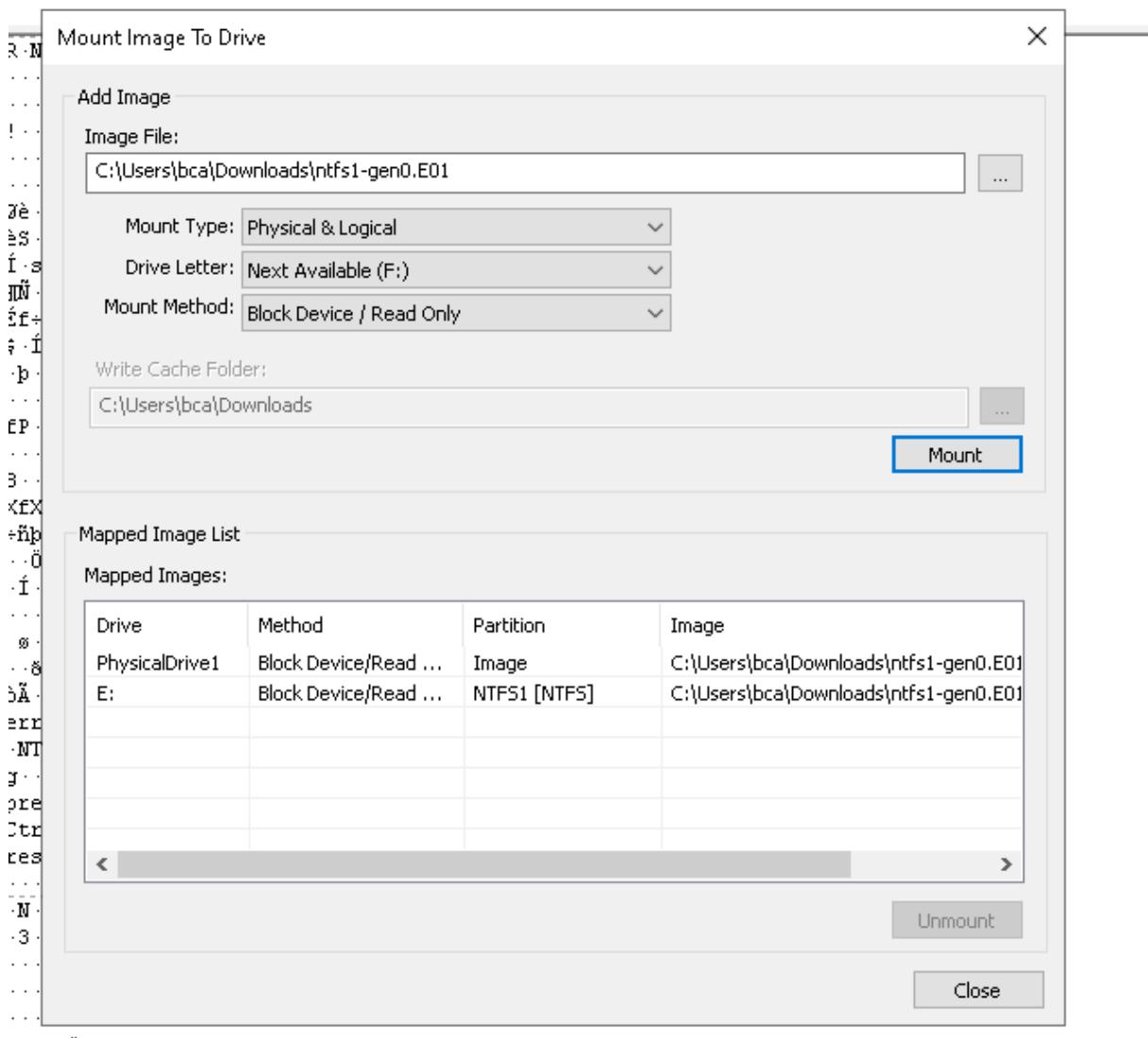
File View Mode Help

File List

Name	Type	Size	Date Modified
000000000 EB 52 90 4E 54 46 53 20-20 20 20 00 02 01 00 00 eR-NTFS			
000000010 00 00 00 00 F8 00 FF 00 00 00 00 00 00 00 00 00 00			
000000020 00 00 00 00 80 00 00 00-FF 64 0F 00 00 00 00 00 00			
000000030 AA 21 05 00 00 00 00-7F B2 07 00 00 00 00 00 00 00			
000000040 02 00 00 00 08 00 00 00-C7 C0 48 50 E8 48 50 DA			
000000050 00 00 00 00 FA 33 C0 8E-D0 BC 00 7C FB B8 C0 07			
000000060 8E D8 E8 16 8B 00 OD-8E C0 33 DB C6 06 OE 00			
000000070 10 E8 53 00 68 00 00 68-6A 02 CB 8A 16 24 00 B4			
000000080 08 CD 13 73 05 B9 FF FF-8A F1 66 0F B6 C6 40 66			
000000090 0F B6 D1 80 82 3F F7 E2-86 CD CO ED 06 41 66 0F			
0000000A0 B7 C9 66 F7 E1 66 A3 20-00 C3 B4 41 BB AA 55 8A			
0000000B0 16 24 00 CD 13 72 0F 81-FB 55 AA 75 09 F6 C1 01			
0000000C0 74 04 FE 06 14 00 C3 66-60 1E 06 66 A1 10 00 66			
0000000D0 03 00 1C 00 66 3B 06 20-00 0F 82 3A 00 1E 66 6A			
0000000E0 00 68 50 08 53 66 68 10-00 01 00 80 3E 14 00 00			
0000000F0 0F 85 0C 00 E8 B3 FF 80-3E 14 00 00 0F 84 61 00			
000000100 B4 42 8A 16 24 00 16 1F-8B F4 CD 13 66 58 58 07			
000000110 66 58 66 58 1F EB 2D 66-33 D2 66 0F B7 0E 18 00			
000000120 66 F7 F1 FE C2 8A CA 66-88 D0 66 C1 EA 10 F7 30			
000000130 1A 00 86 D6 8A 16 24 00-8A E8 CO E4 06 OA CC B8			
000000140 01 02 CD 13 0F B2 19 00-8C CO 05 20 00 8E CO 66			
000000150 FF 00 10 00 FF 0E 0E 00-0F 85 6F FF 07 1F 66 61			
000000160 C3 A0 F8 01 E8 09 00 A0-FB 01 E8 03 00 FB EB FE			
000000170 B4 01 8B F0 AC 3C 00 74-09 B4 0E BB 07 00 CD 10			
000000180 EB F2 C3 OD 0A 41 20 64-69 73 6B 20 72 65 61 64			
000000190 20 65 72 72 6F 72 20 6F-63 63 75 72 72 65 64 00			
0000001A0 OD 0A 4E 54 4C 54 54 4C-44 52 20 69 73 20 63 6F			
0000001B0 6E 67 00 0D 0A 4E 54 4C-44 52 20 69 73 20 63 6F			
0000001C0 6D 70 72 65 73 73 65 64-00 0A 50 72 65 73 73			
0000001D0 20 43 74 72 6C 2B 41 6C-74 2B 44 65 6C 20 74 6F			
0000001E0 20 72 65 73 74 61 72 74-0D 0A 00 00 00 00 00 00			
0000001F0 00 00 00 00 00 00 00-83 A0 B3 C9 00 00 55 AA			
000000200 05 00 4E 00 54 00 4C 00-44 00 52 00 00 04 24 00			
000000210 49 00 33 00 30 00 00 E0-00 00 30 00 00 00 00 00			
000000220 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00			
000000230 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00			
000000240 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00			
000000250 00 00 00 00 00 EB 12-90 90 00 00 00 00 00 00 00			
000000260 00 00 00 00 00 00 00-00 00 8C 8E D8 C1 EO			
000000270 04 FA 8B EO FB E8 03 FE-66 07 B7 06 0B 00 66 0F			
000000280 B6 1E 00 66 F7 E3 66-A3 4E 02 66 8B 0E 40 00			
000000290 80 F9 00 0F 8F 0E F6-D9 66 B8 01 00 00 00 66			
0000002A0 D3 EO EB 08 90 66 A1 4E-02 66 F7 EL 66 A3 52 02			
0000002B0 66 EO B7 1E 0B 00 66 33-D2 66 F7 F3 66 A3 56 02			
Cursor pos = 336; log sec = 0			

For User Guide, press F1





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.