Ex. No 1: Evidence Acquisition Using AccessData FTK Imager

AIM:

To use **AccessData FTK Imager** for acquiring a **forensic image** of digital evidence and to verify its integrity using hash values.

DESCRIPTION / THEORY:

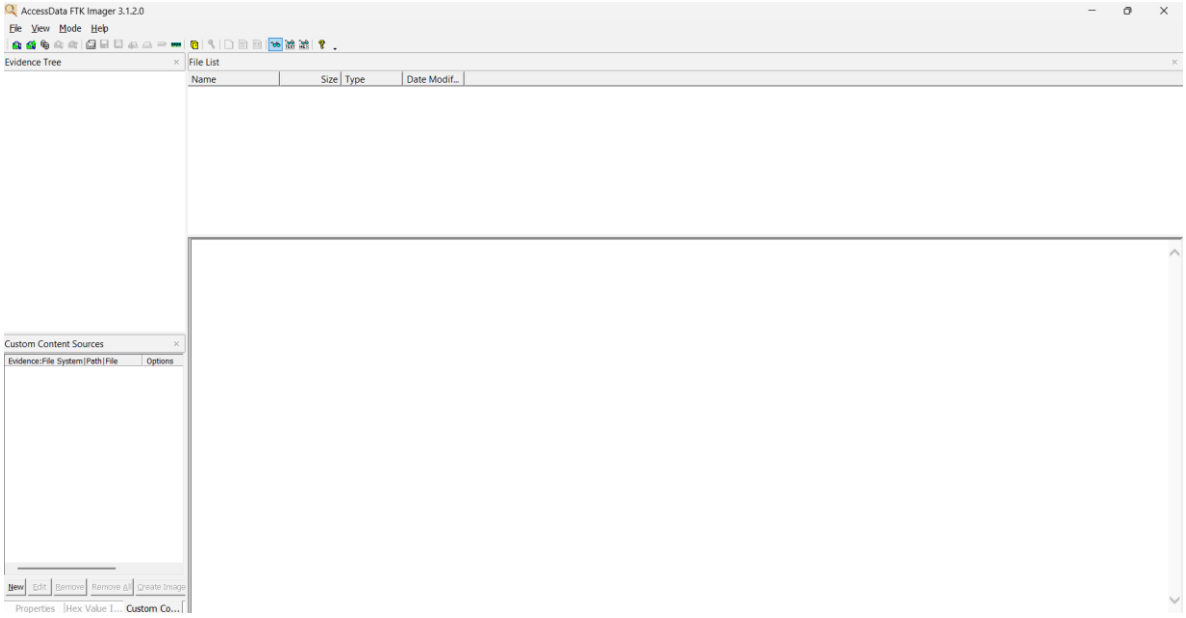
FTK Imager is a forensic imaging tool developed by AccessData that allows investigators to capture exact copies (bit-by-bit images) of storage media such as hard drives, USB devices, or disk partitions.

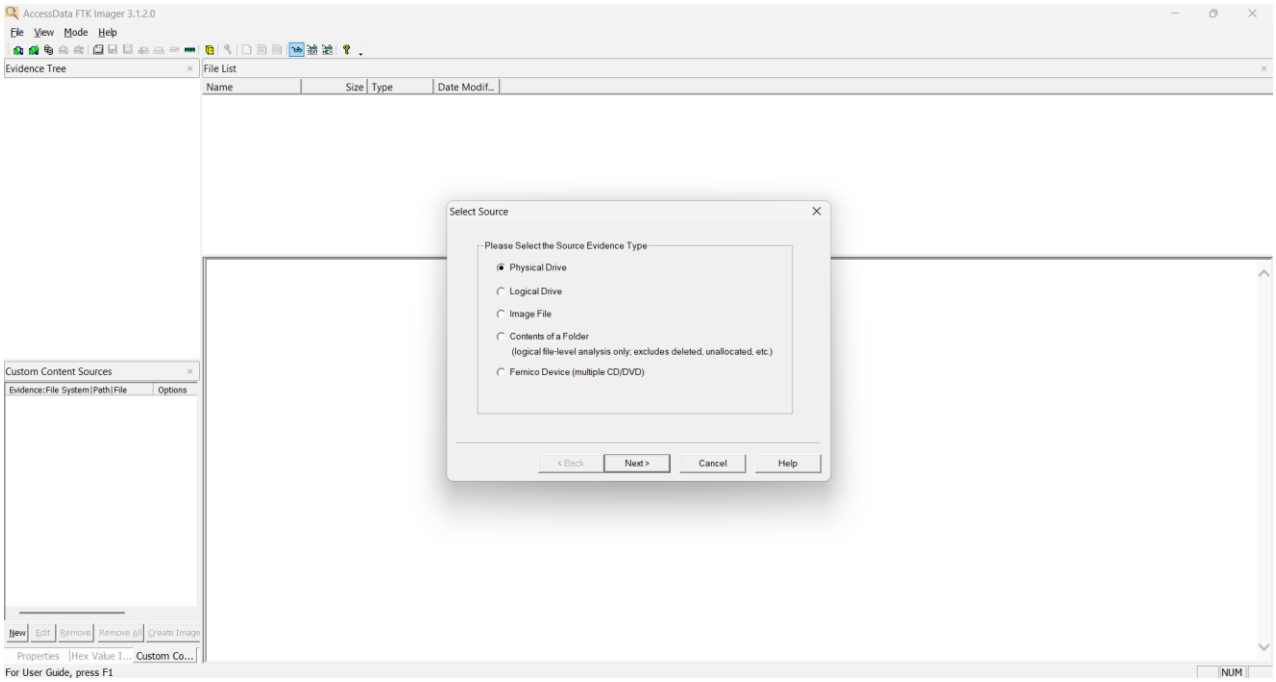
In digital forensics, evidence acquisition is the first and most critical step. It ensures that data is collected without altering the original media, maintaining the chain of custody. FTK Imager can create images in multiple formats such as:

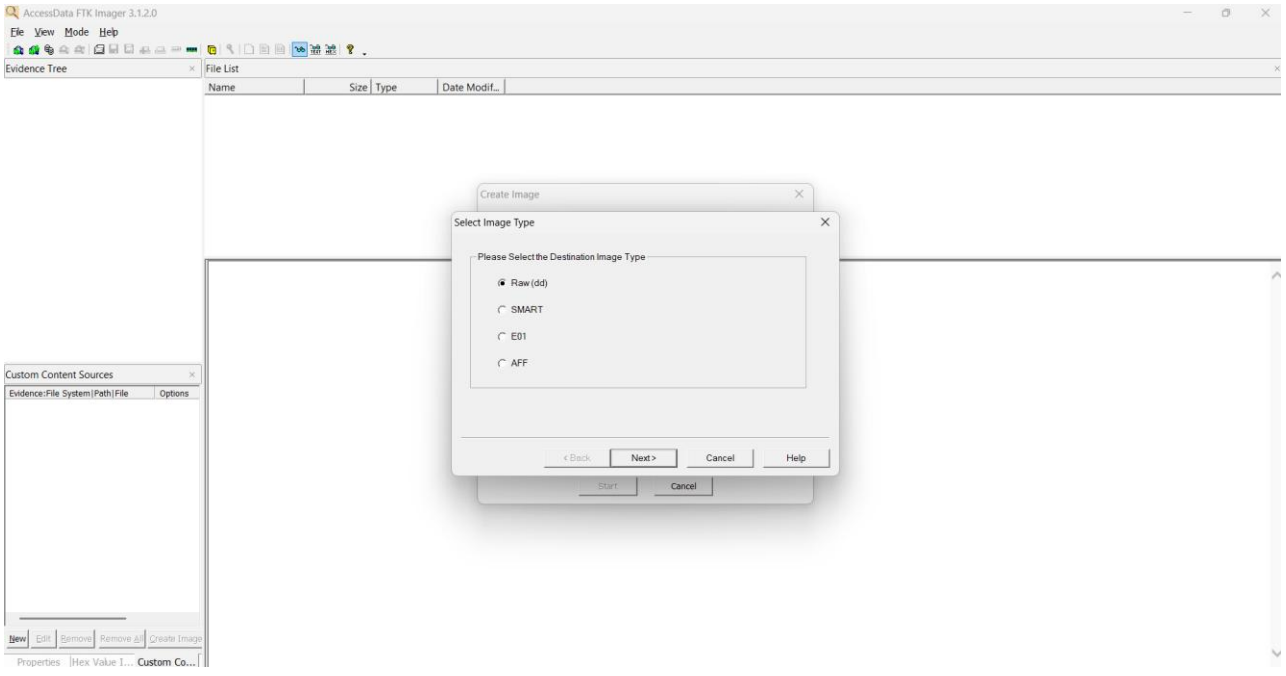
- E01 (EnCase format)
- RAW (dd format)
- SMART / AFF formats

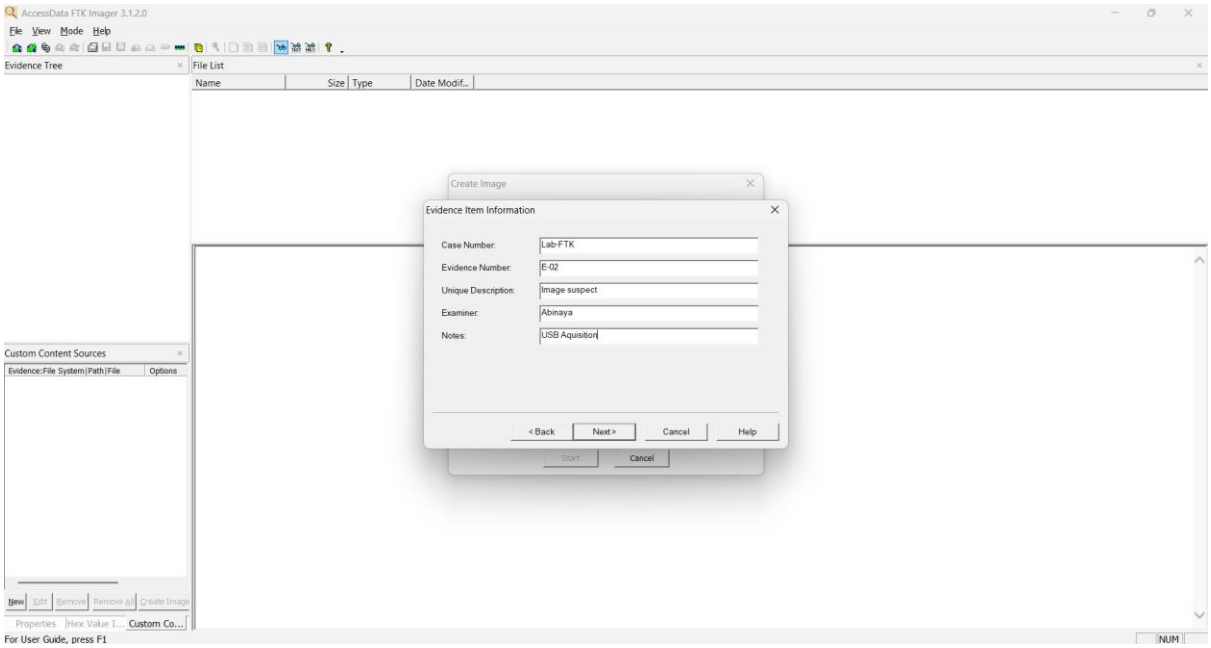
It also provides hash verification (MD5/SHA1) to confirm image integrity and can preview files before acquisition without making changes to the original evidence.

PROCEDURE:

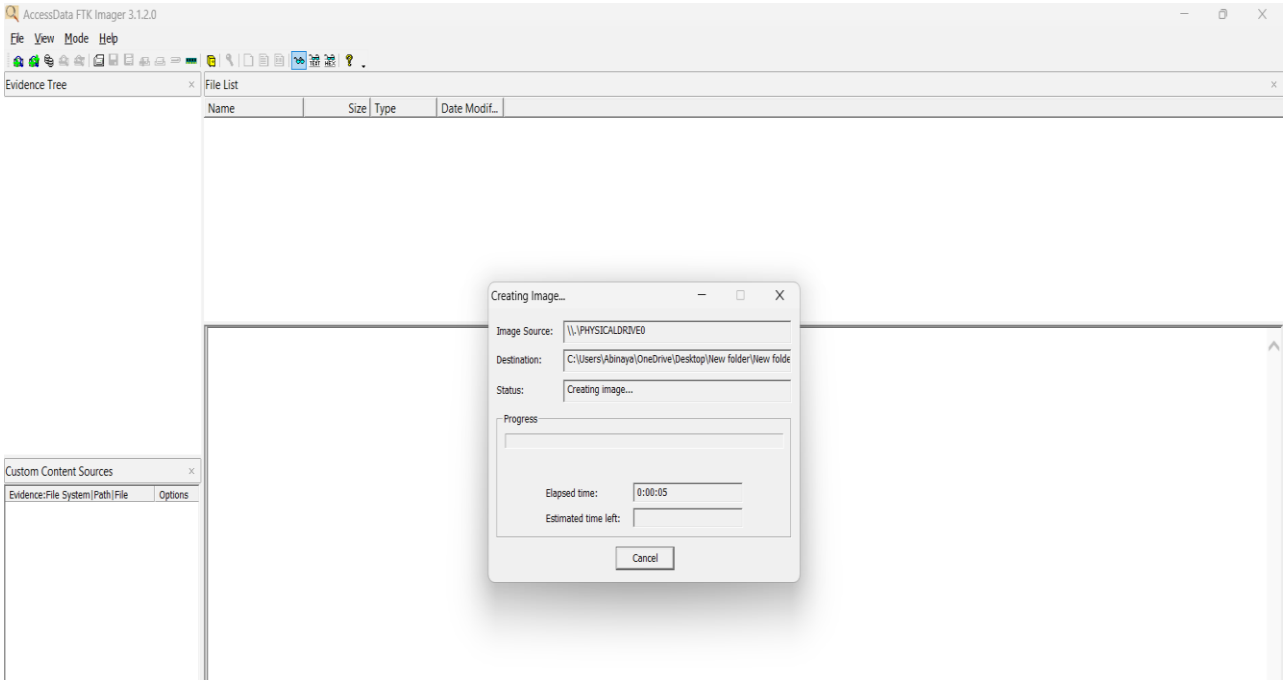



AccessData FTK Imager 3.1.2.0
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modif...
Select Source
Please Select the Source Evidence Type
Physical Drive
Logical Drive
Image File
Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
Fernico Device (multiple CD/DVD)
< Back Next > Cancel Help
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value I... Custom Co...
For User Guide, press F1
NUM


AccessData FTK Imager 3.1.2.0
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modif...
Create Image
Select Image Type
Please Select the Destination Image Type
Raw (dd)
SMART
E01
AFF
< Back Next > Cancel Help
Start Cancel
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value I... Custom Co...



OUTPUT:



RESULT:

The **FTK Imager tool** was successfully used to acquire a forensic image of the given evidence without altering the original data.