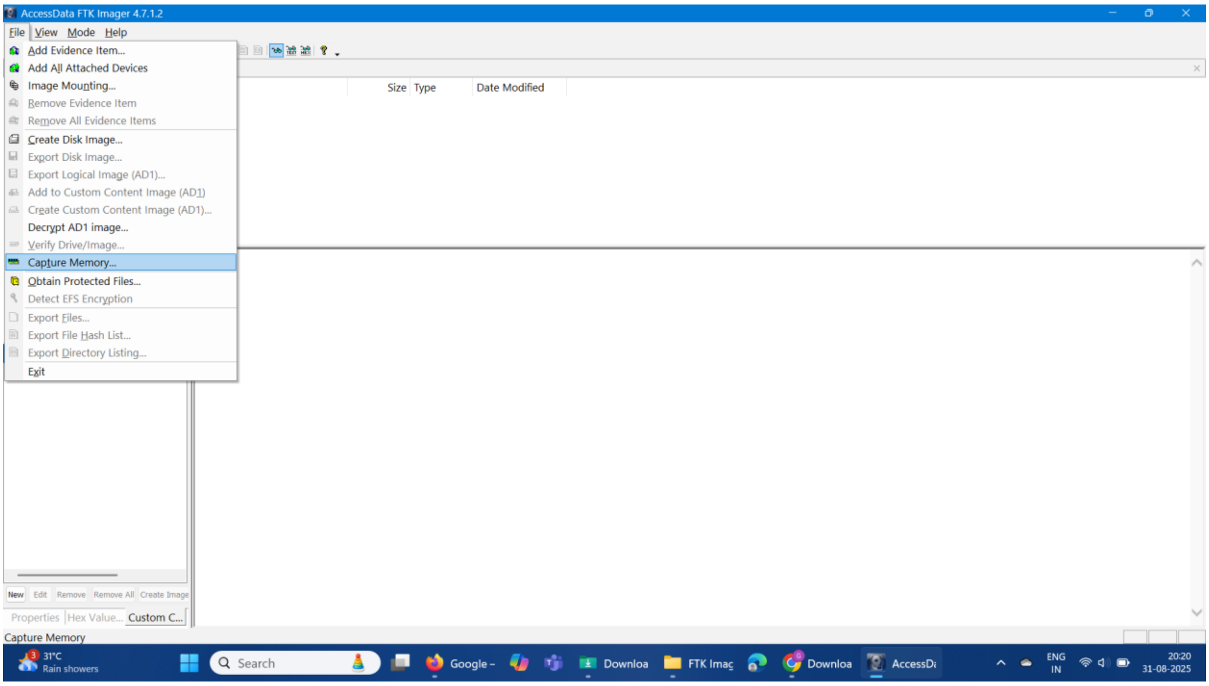
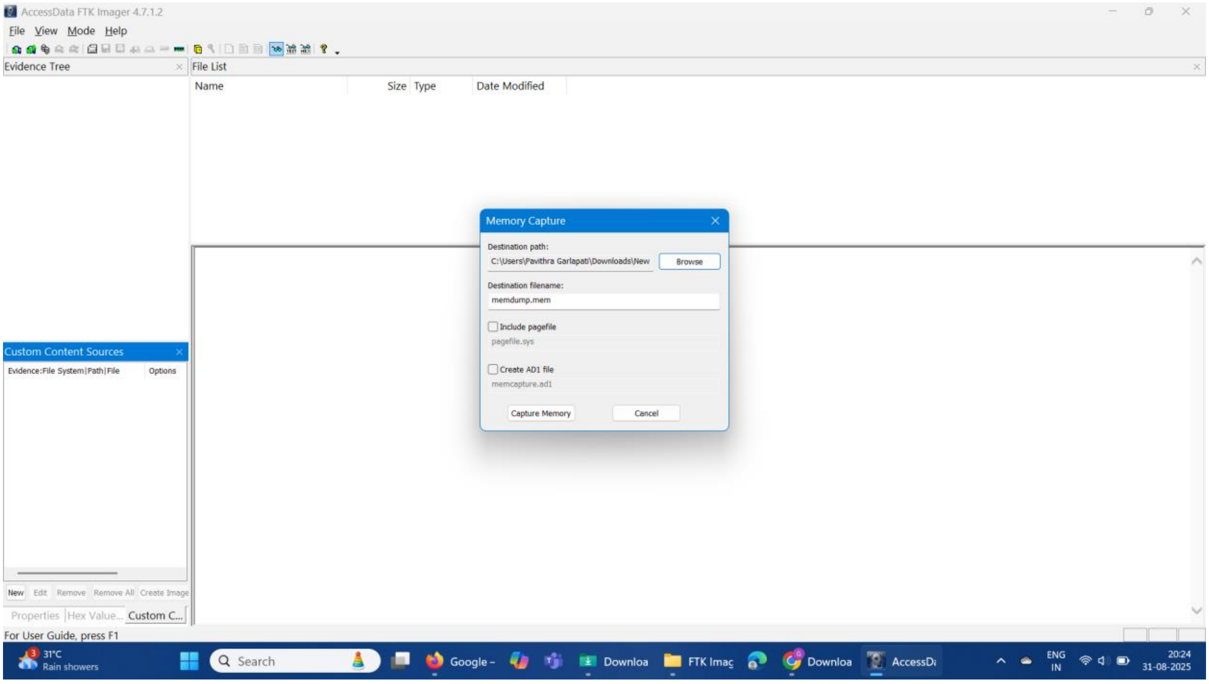
EXPERIMENT:1

FTK Imager

- **Aim:** To create and analyze forensic images of storage devices while preserving data integrity.
- **Tools/Features:**
  - Disk imaging (E01, RAW, etc.)
  - Hashing (MD5, SHA1) for integrity
  - Preview & export files (including deleted ones)
  - Memory dump (RAM capture)
  - Mount and verify images
- **Process:**
  - Open FTK Imager
  - Select evidence source (disk, partition, folder, image file)
  - Choose destination format & location
  - Enter case info (optional)
  - Create image → tool copies sector-by-sector
  - Verify hash values
  - Preview or mount image for analysis

OUT PUT:





Memory Capture

Destination path: C:\Users\Pavithra Garlapati\Downloads\New

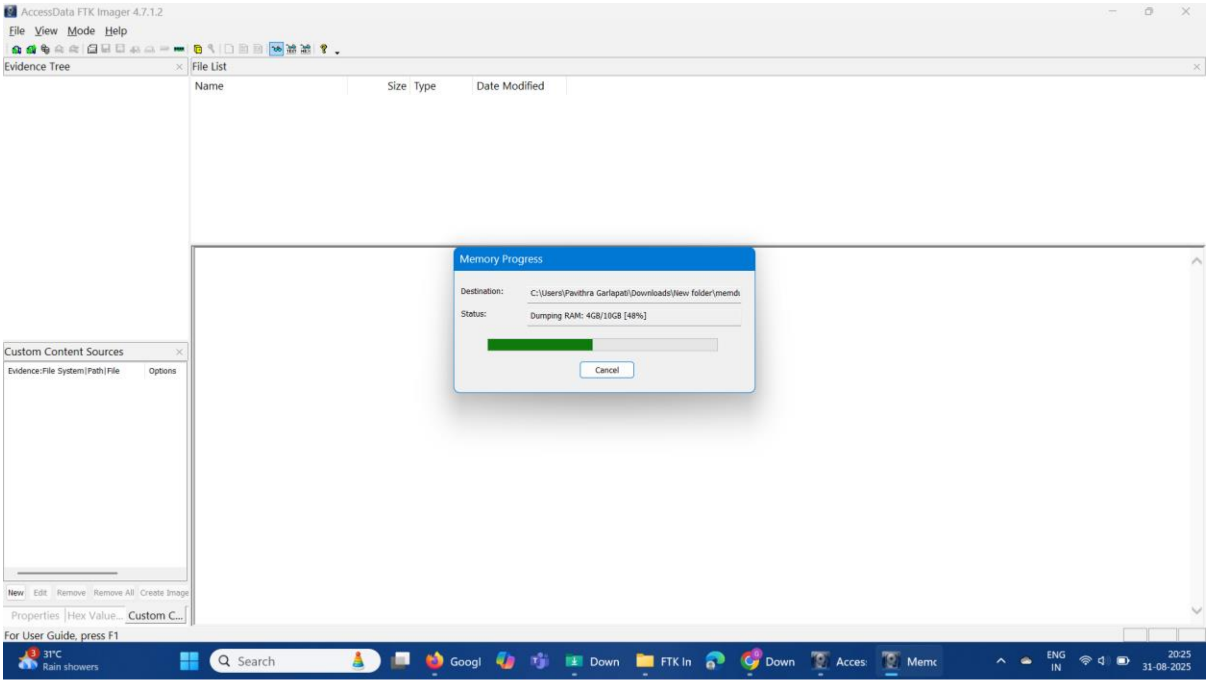
Destination filename: memdump.mem

□ Include pagefile

pagefile.sys

□ Create AD1 file

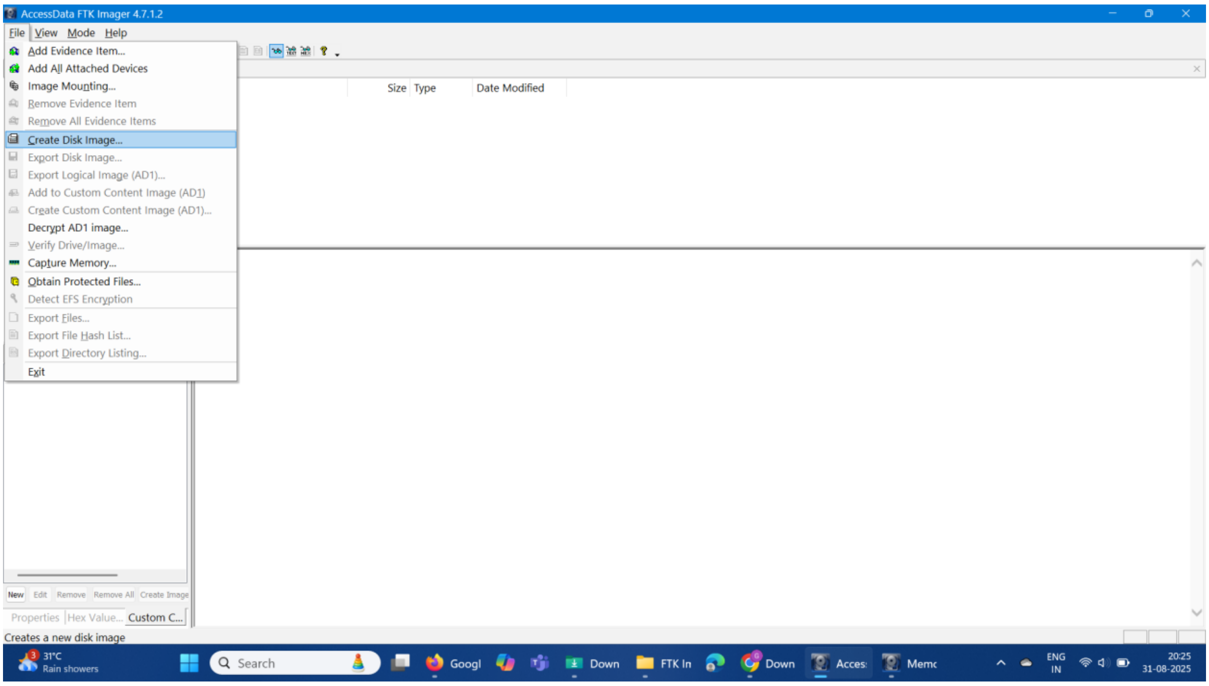
memcapture.ad1



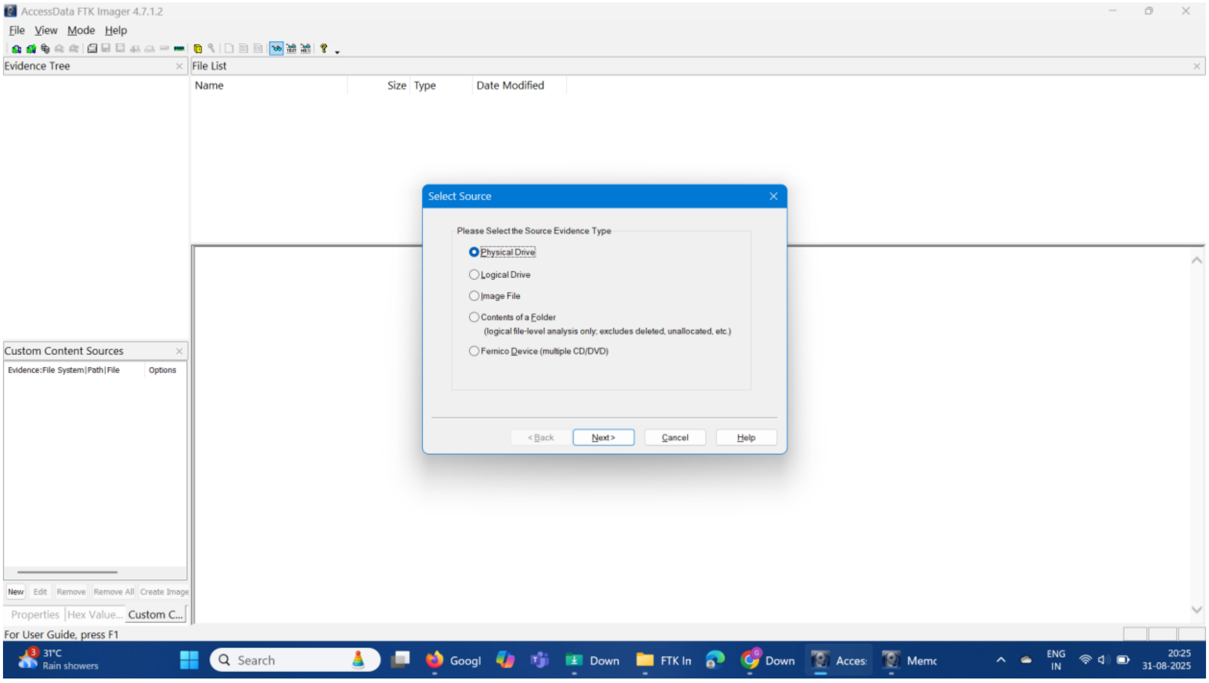
Memory Progress

Destination: C:\Users\Pavithra Garlapati\Downloads\New folder\memd

Status: Dumping RAM: 4GB/10GB [48%]

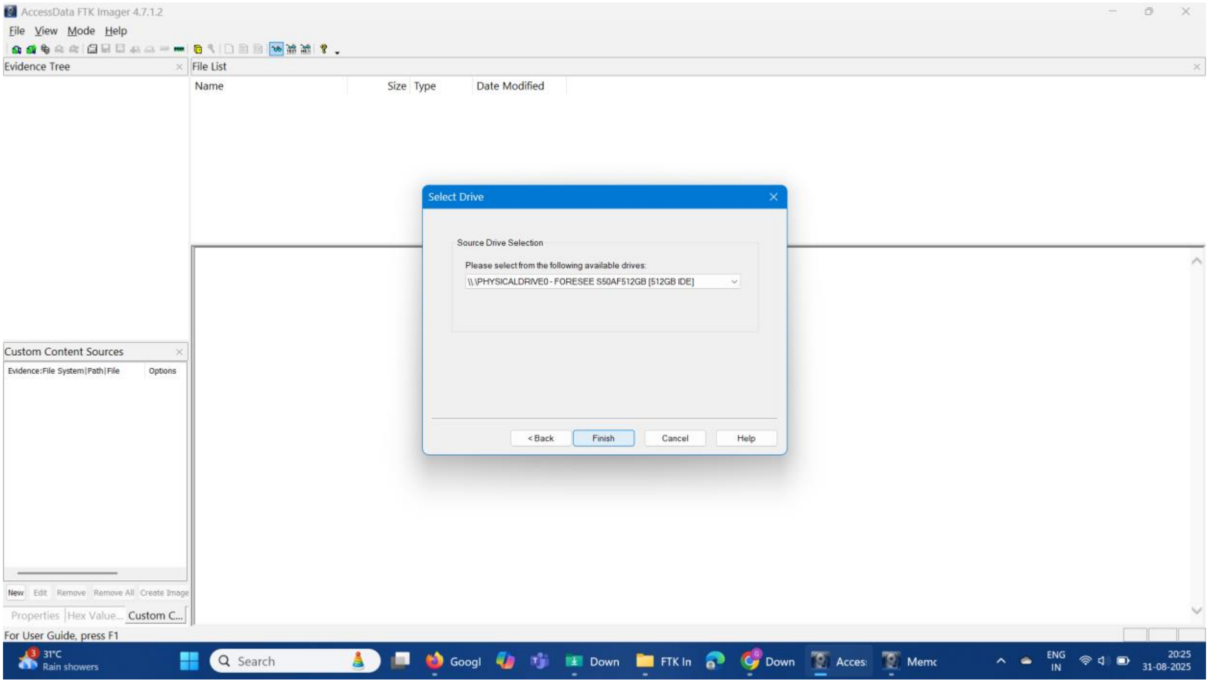


Creates a new disk image


AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value... Custom C...
For User Guide, press F1
Select Source
< Back Next > Cancel Help

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)

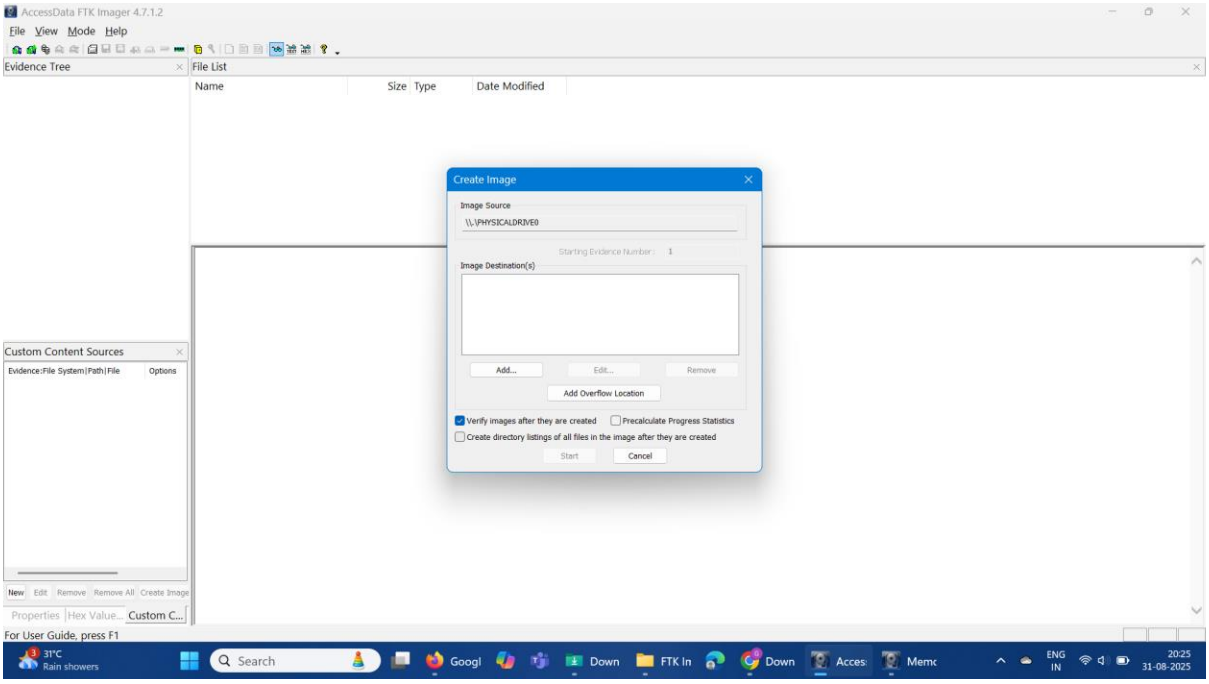


Select Drive

Source Drive Selection

Please select from the following available drives:

\\.\PHYSICALDRIVE0 - FORESEE S50AF512GB [512GB IDE]



Create Image

Image Source

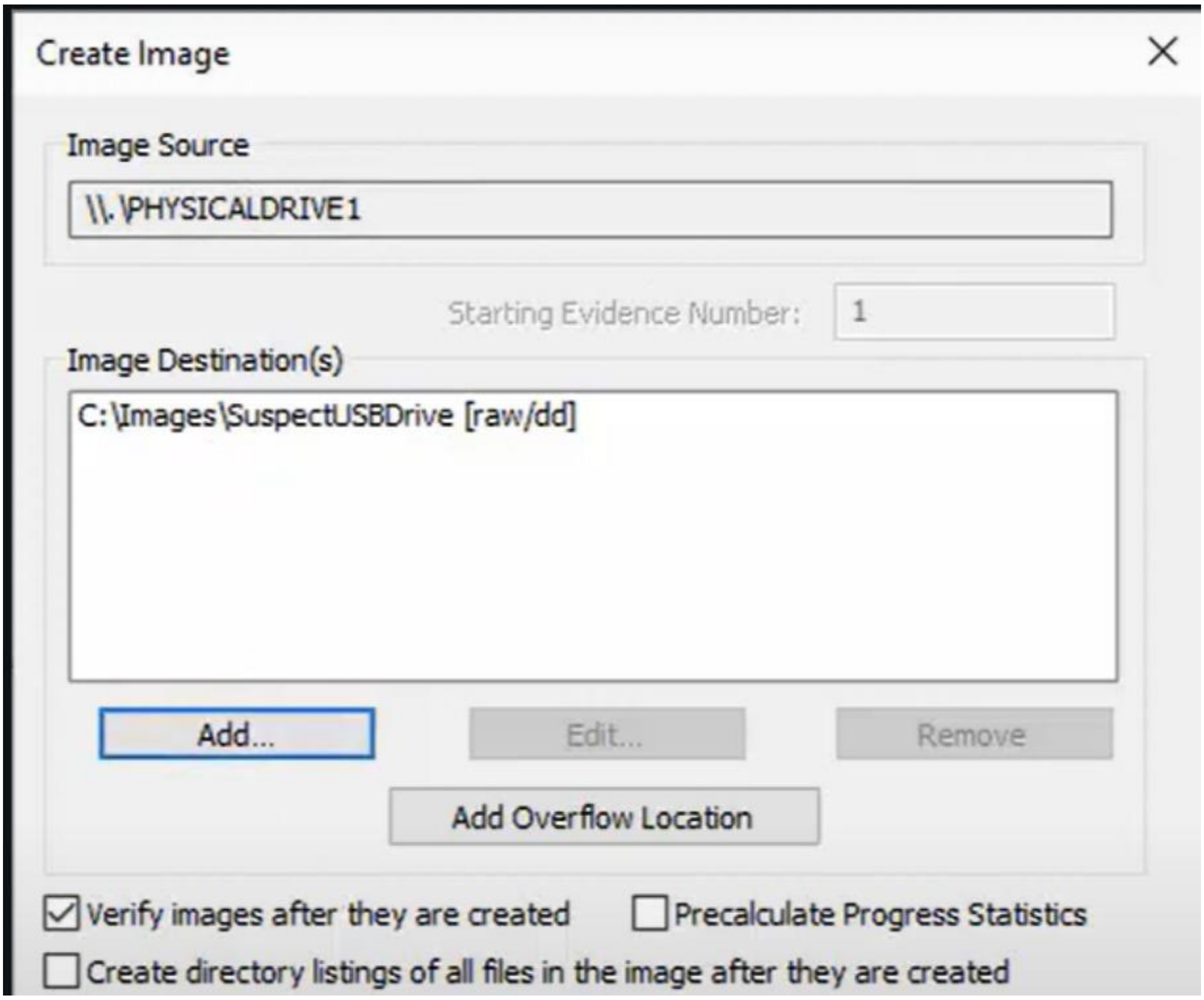
\\.\PHYSICALDRIVE0

Starting Evidence Number : 1

Image Destination(s)

☑ Verify images after they are created ☐ Precalculate Progress Statistics

☐ Create directory listings of all files in the image after they are created



Create Image

Image Source

\\.\PHYSICALDRIVE1

Starting Evidence Number: 1

Image Destination(s)

C:\Images\SuspectUSBDrive [raw/dd]

☑ Verify images after they are created

□ Precalculate Progress Statistics

□ Create directory listings of all files in the image after they are created

RESULT:

The forensic image of the given storage media was successfully created using **FTK Imager**.
The generated image was verified with hash values, confirming that the integrity of the original evidence was preserved.