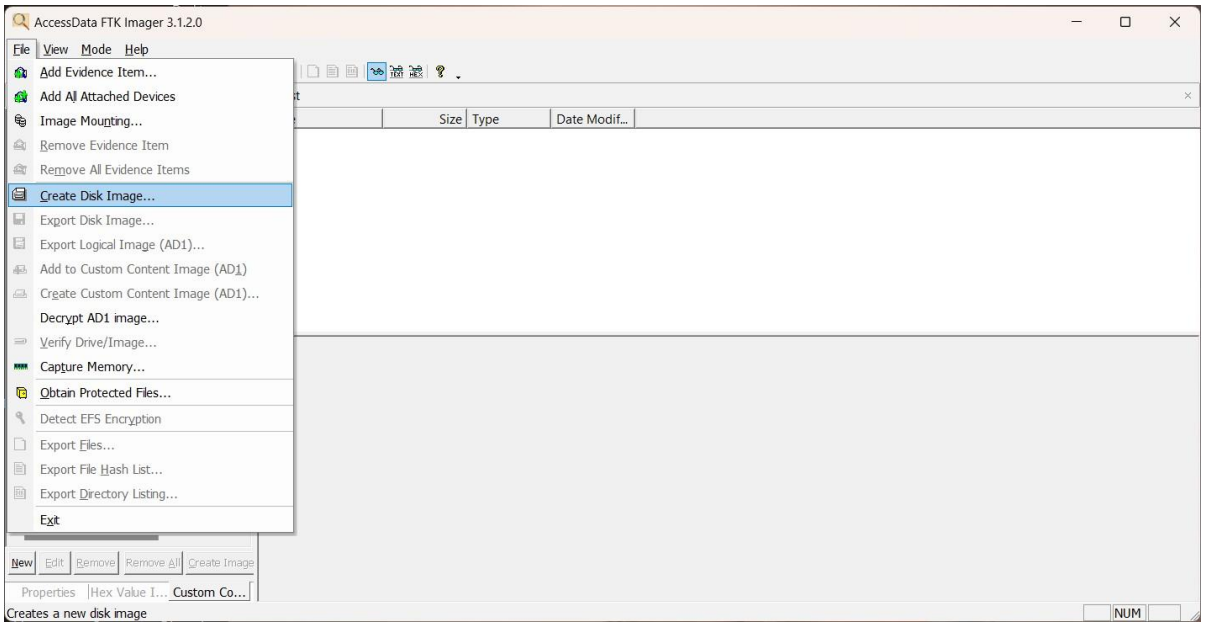
EXP NO:1 Evidence Acquisition Using AccessData FTK Imager

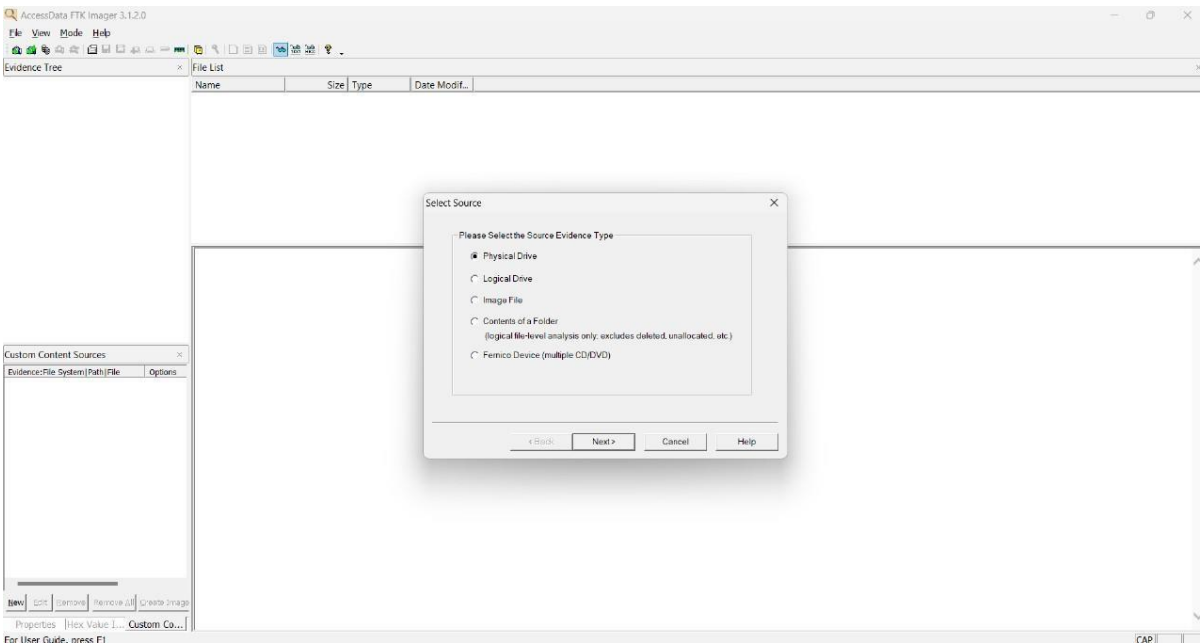
Aim:

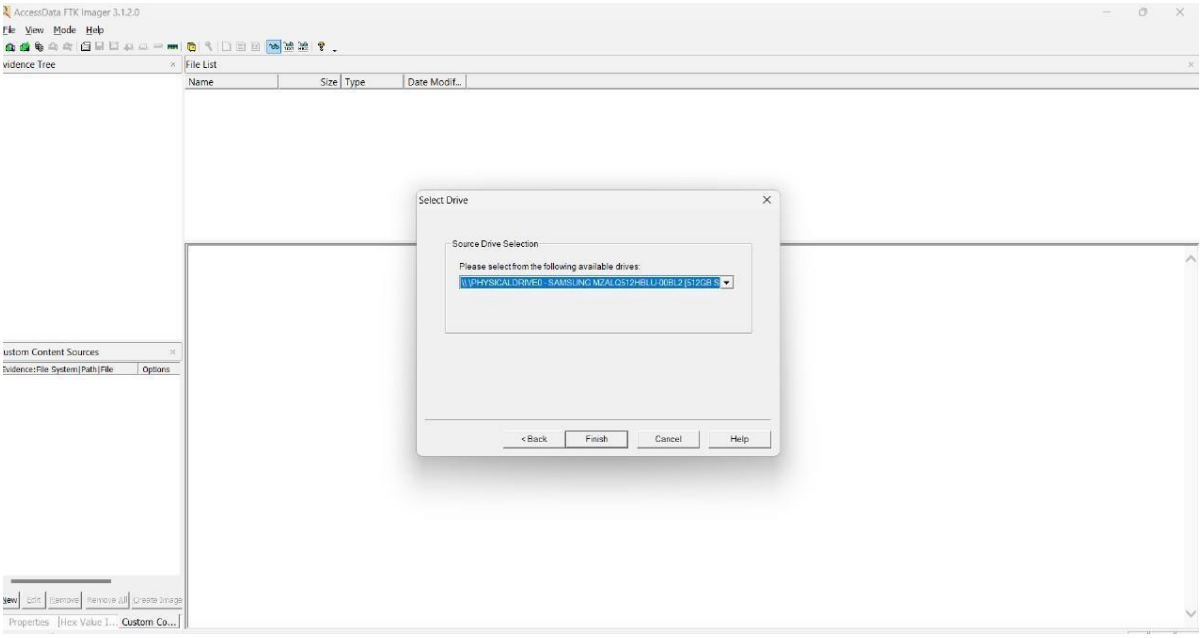
To acquire both volatile (RAM) and non-volatile (disk) memory evidence from a computer system using AccessData FTK Imager for forensic analysis while maintaining data integrity.

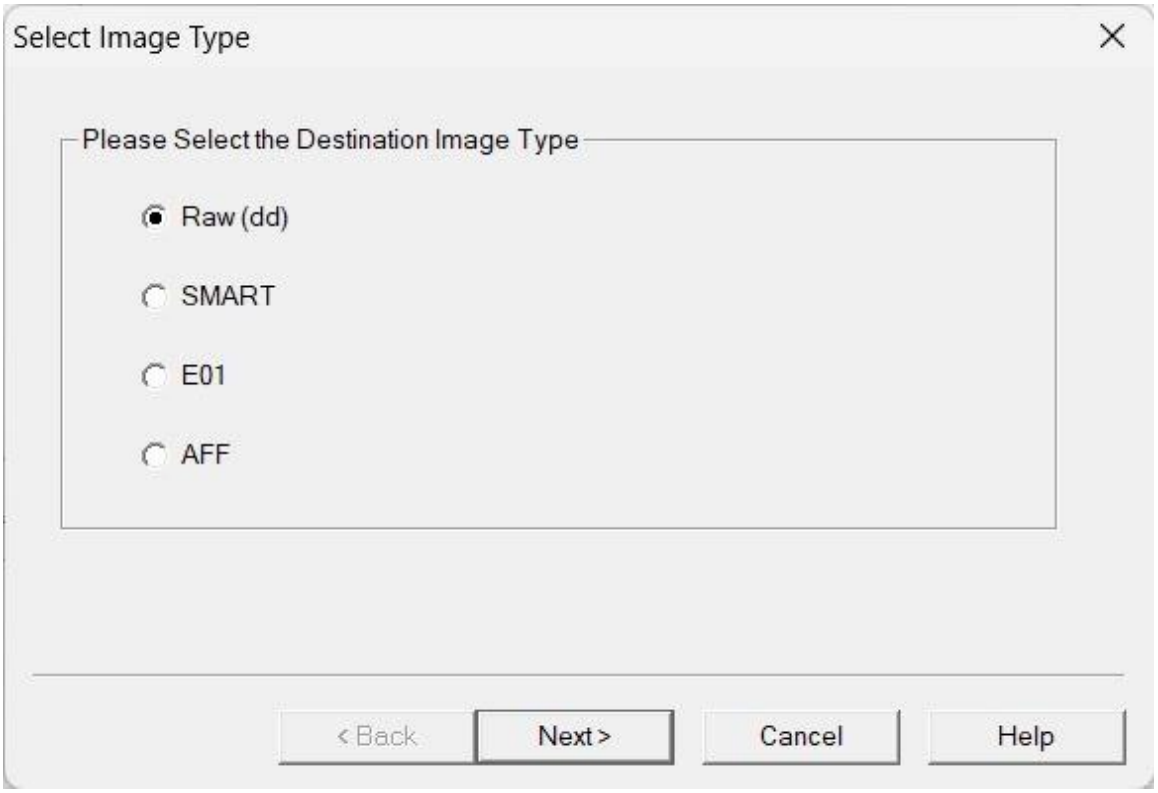
Procedure:

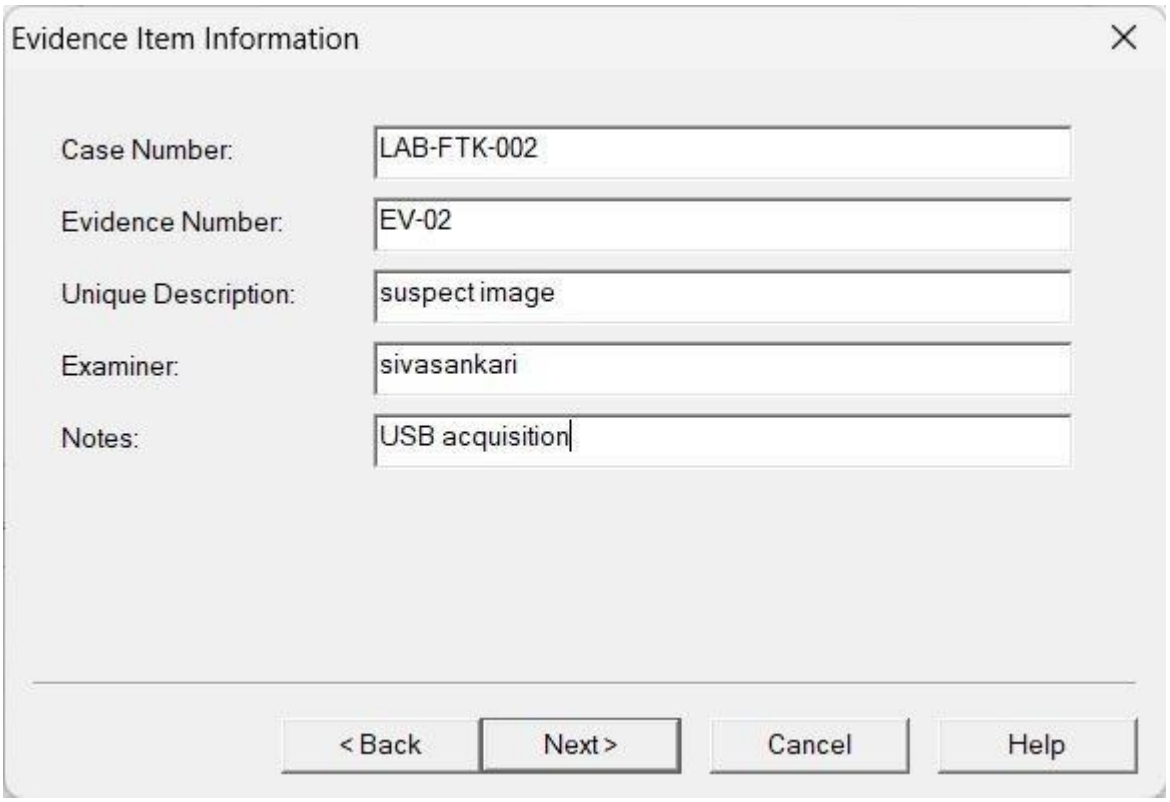
1. Open FTK Imager and use the **Capture Memory** option to acquire volatile memory (.mem file).
   Use the **Create Disk Image** option to acquire non-volatile memory (disk image) in a desired format (E01, RAW, etc.).Enter case details, choose destination, enable verification, and start acquisition to generate image and hash verification report.

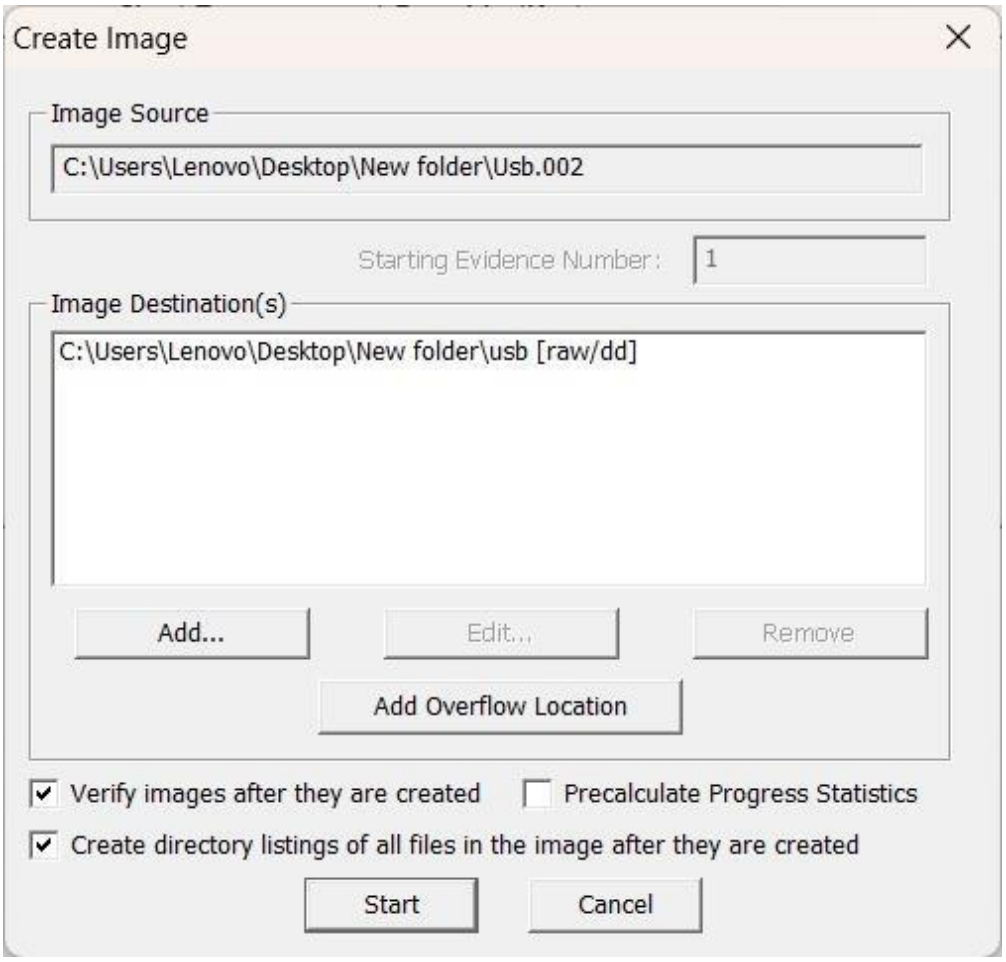


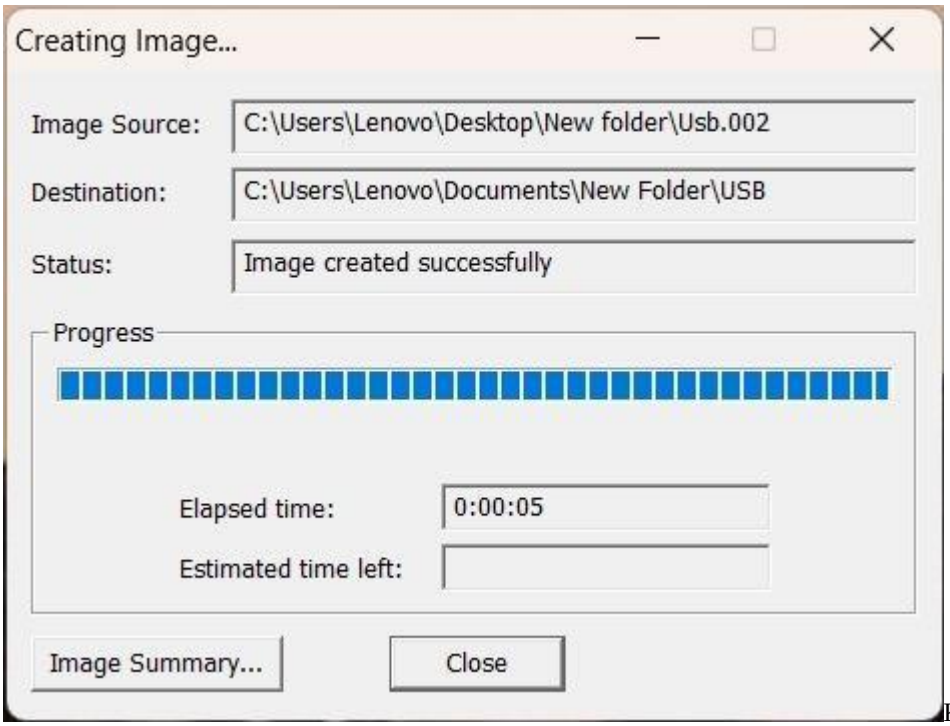



AccessData FTK Imager 3.1.2.0
File View Mode Help
File List
Name
Size
Type
Date Modif...
Select Drive
Source Drive Selection
Please select from the following available drives:
< Back
Finish
Cancel
Help

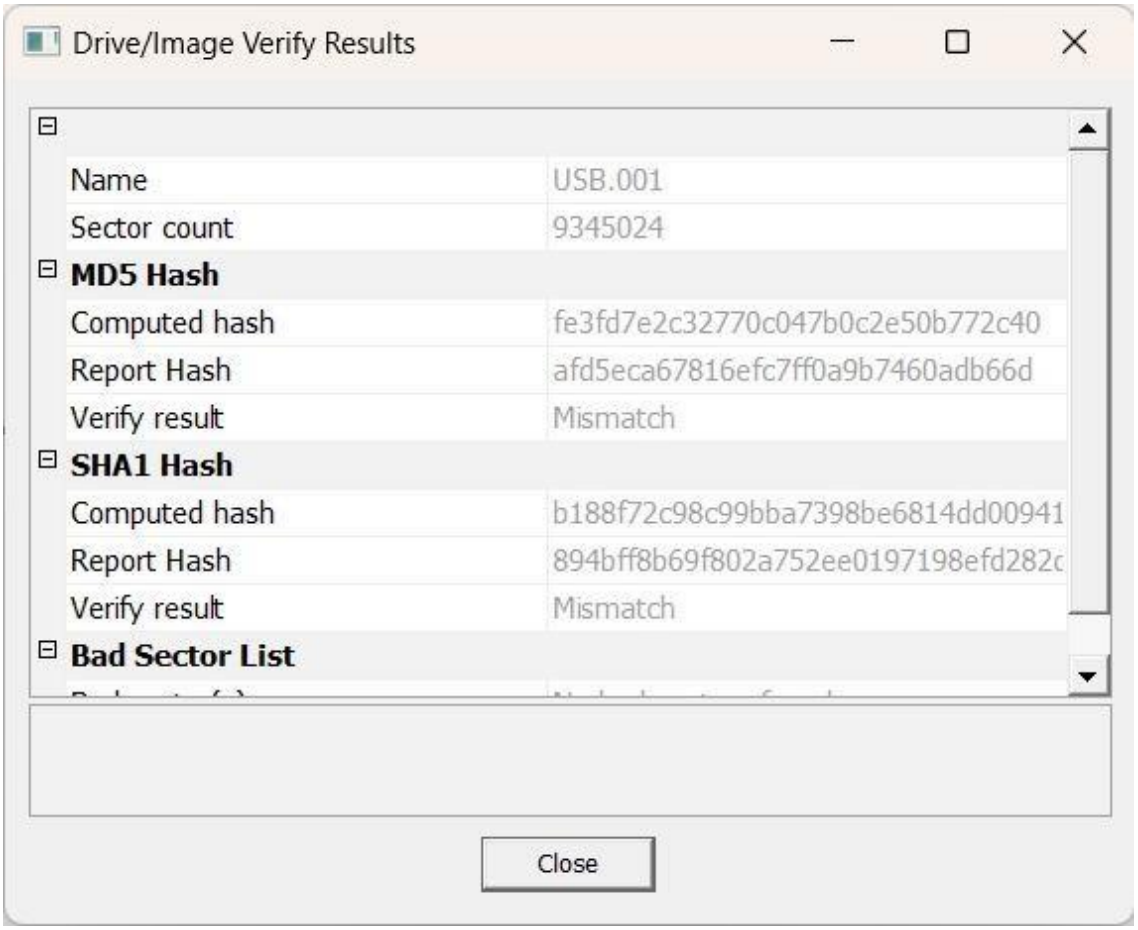

Select Image Type
Please Select the Destination Image Type
Raw (dd)
SMART
E01
AFF
< Back
Next >
Cancel
Help


Evidence Item Information
Case Number:
LAB-FTK-002
Evidence Number:
EV-02
Unique Description:
suspect image
Examiner:
sivasankari
Notes:
USB acquisition
< Back
Next >
Cancel
Help


Create Image
Image Source
C:\Users\Lenovo\Desktop\New folder\Usb.002
Starting Evidence Number:
1
Image Destination(s)
C:\Users\Lenovo\Desktop\New folder\usb [raw/dd]
Add...
Edit...
Remove
Add Overflow Location
Verify images after they are created
Precalculate Progress Statistics
Create directory listings of all files in the image after they are created
Start
Cancel


Creating Image...
Image Source:
C:\Users\Lenovo\Desktop\New folder\Usb.002
Destination:
C:\Users\Lenovo\Documents\New Folder\USB
Status:
Image created successfully
Progress
Elapsed time:
0:00:05
Estimated time left:
Image Summary...
Close
K

RESULT:


Drive/Image Verify Results
Name
USB.001
Sector count
9345024
MD5 Hash
Computed hash
fe3fd7e2c32770c047b0c2e50b772c40
Report Hash
afd5eca67816efc7ff0a9b7460adb66d
Verify result
Mismatch
SHA1 Hash
Computed hash
b188f72c98c99bba7398be6814dd00941
Report Hash
894bff8b69f802a752ee0197198efd282c
Verify result
Mismatch
Bad Sector List
Close