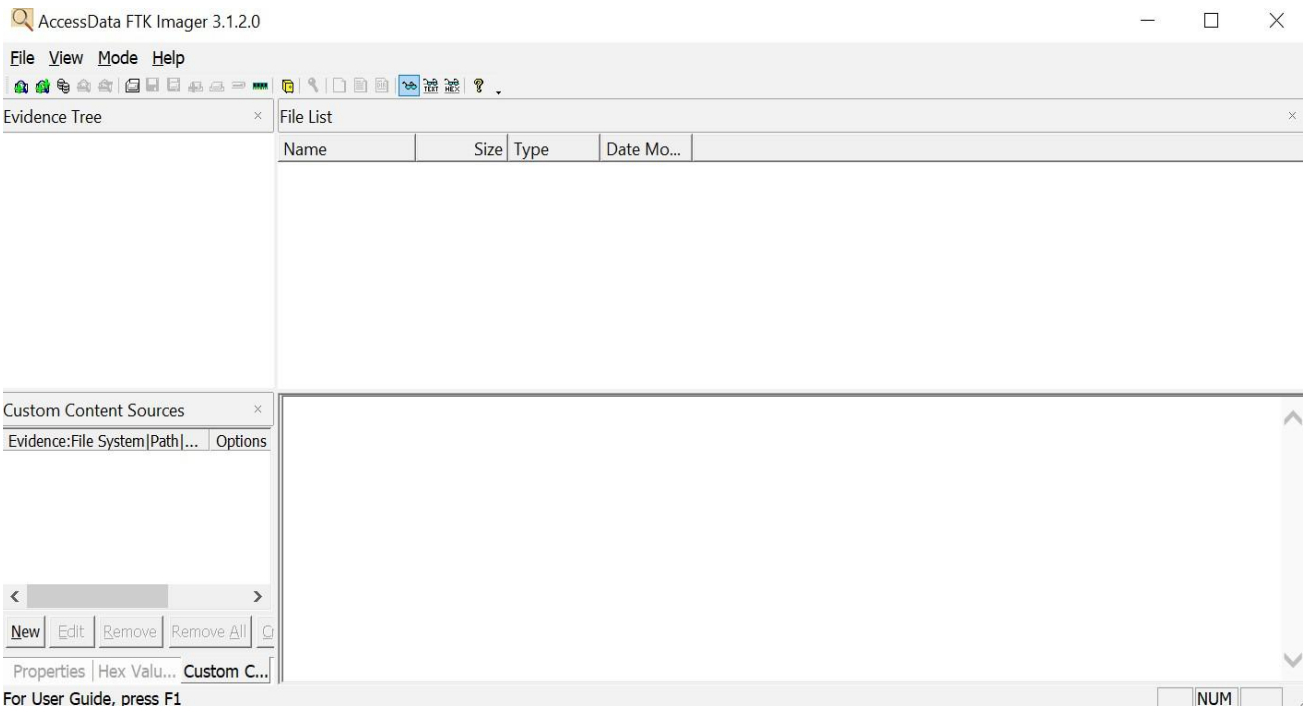
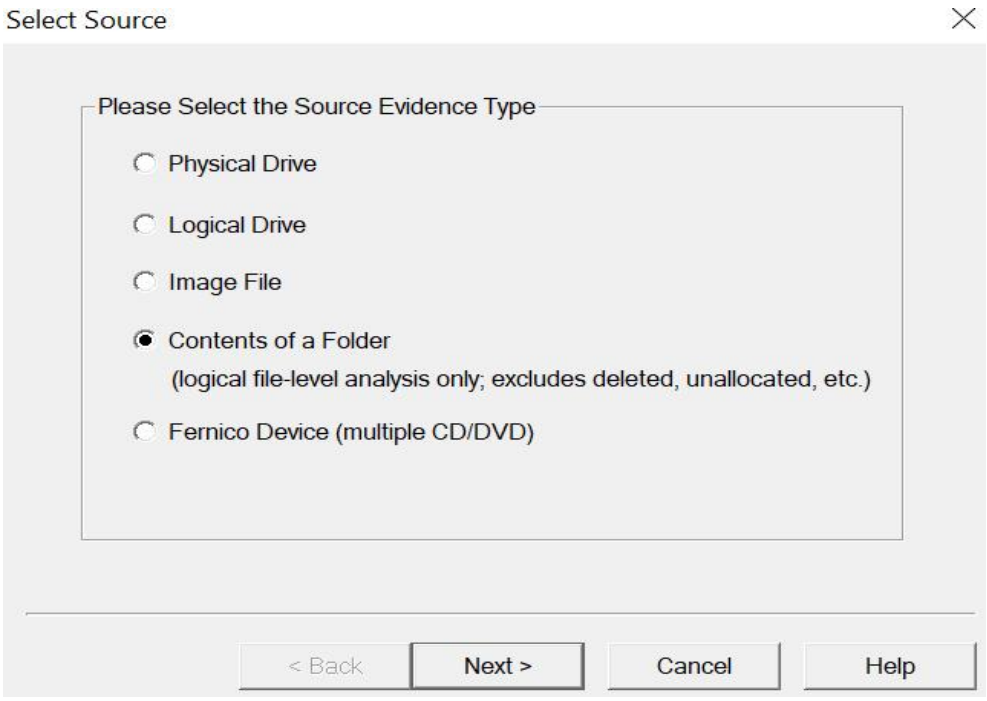
Title: Creating a Forensic Image using FTK Imager.

A. Creating Forensic Image.

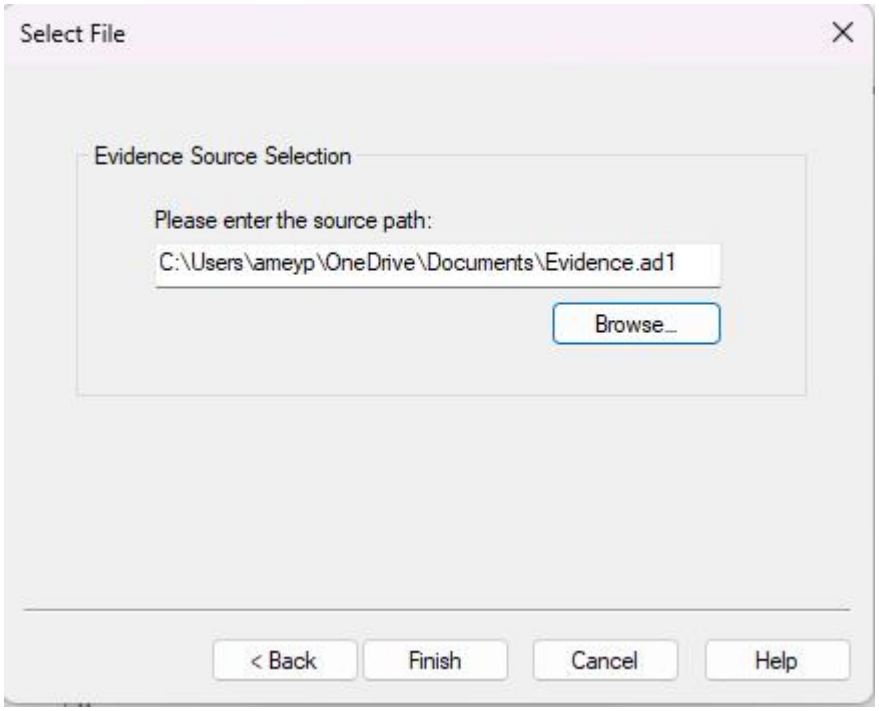
Step 1: Open AccessData FTK Imager.



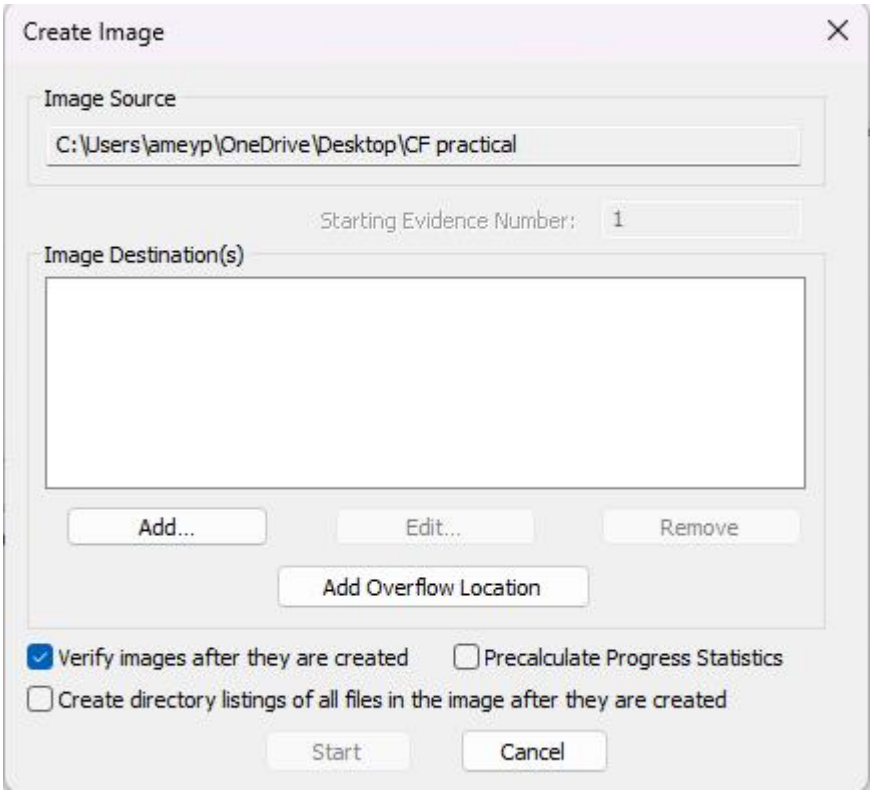
Step 2: Go to File -> Create Image Disk and Select Contents of a Folder.



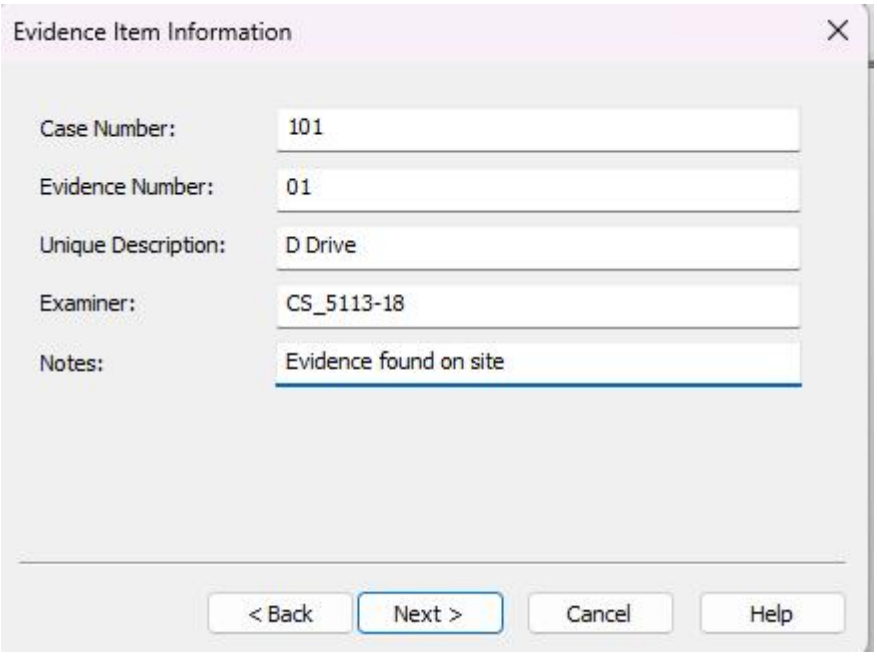
Step 3: Browse & Select the any folder and Click on Finish.



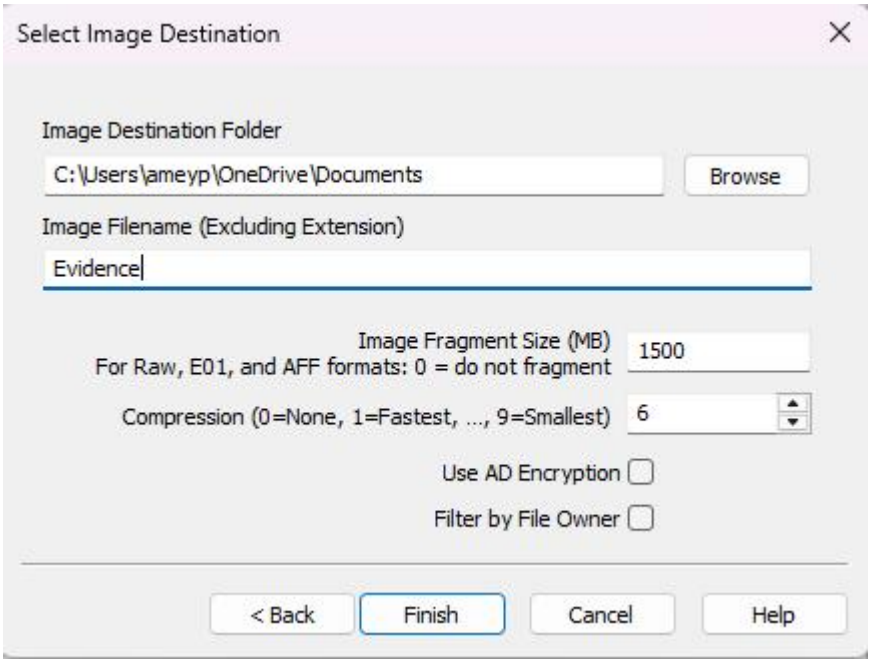
Step 4: Click on Add.



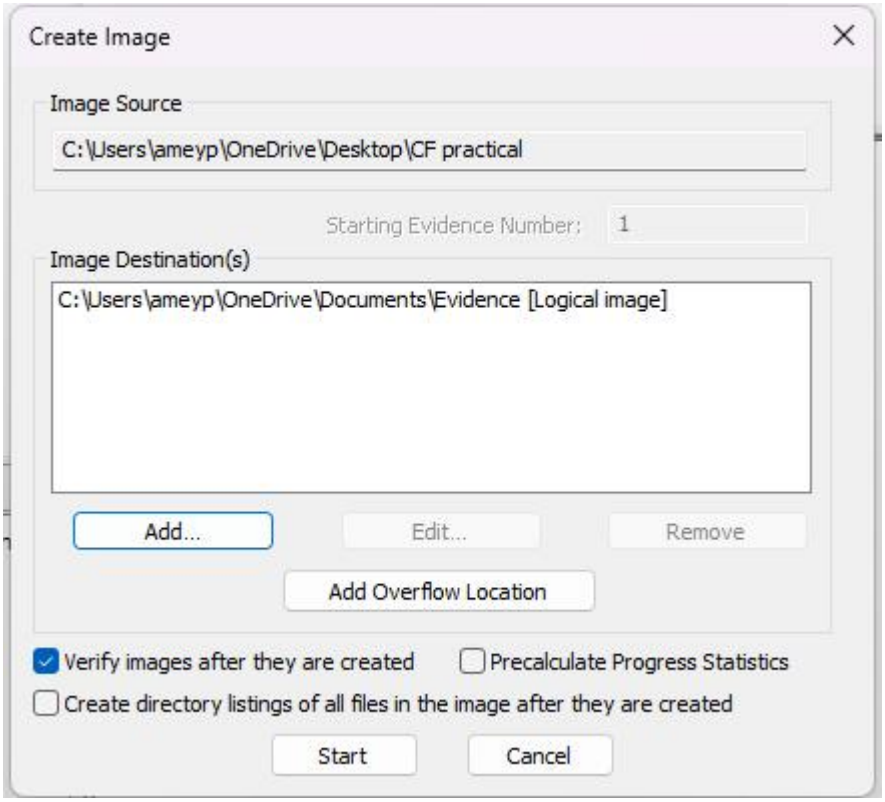
Step 5: Fill all the information and Click on Next.



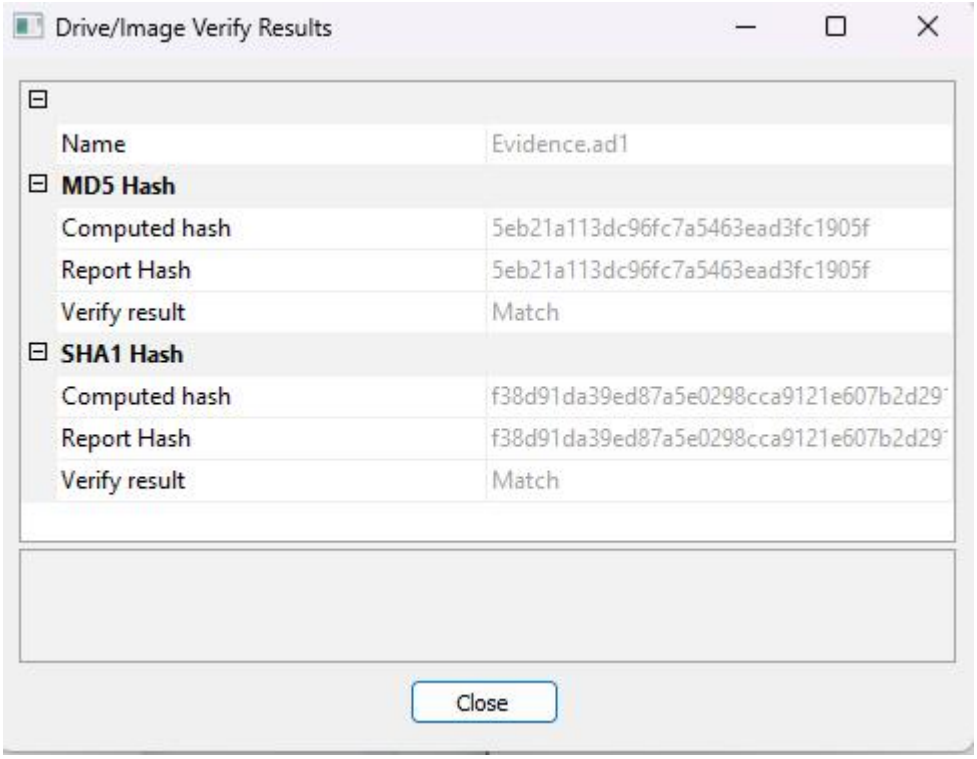
Step 6: Browse the Destination Folder & Give Image Filename and Click on Finish.



Step 7: Click on Start.

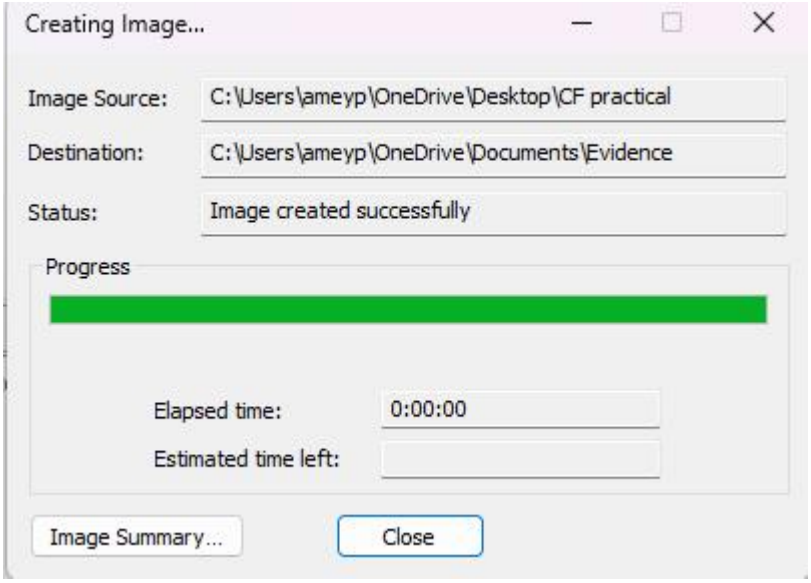


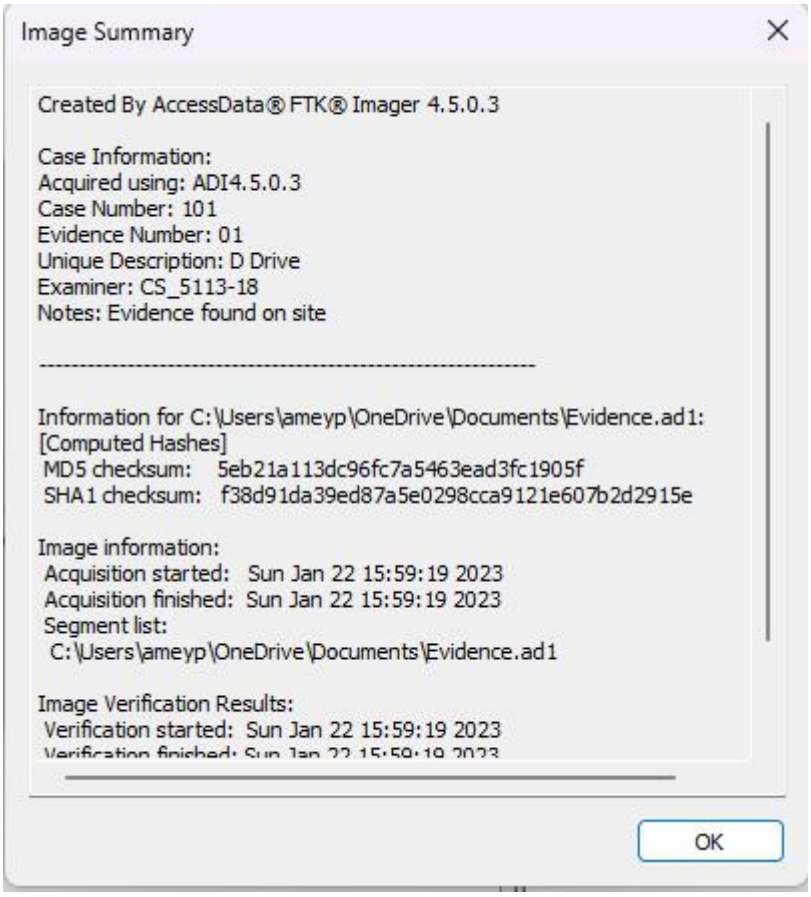
Step 8: Click on Close.



B. Check Integrity of Data.

Step 9: Click on Image Summary.





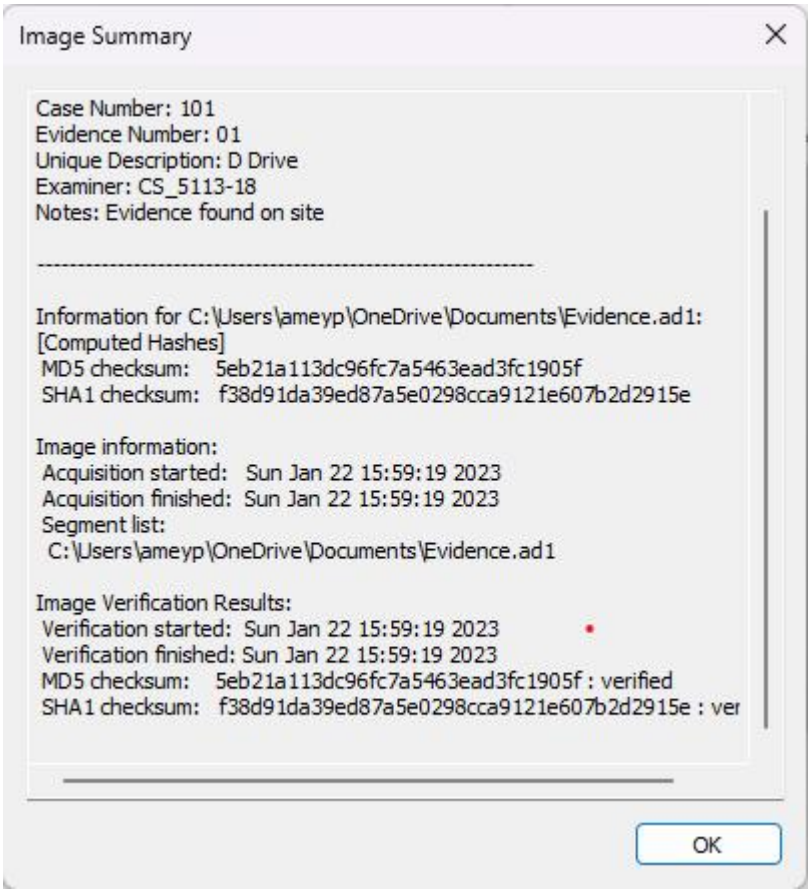
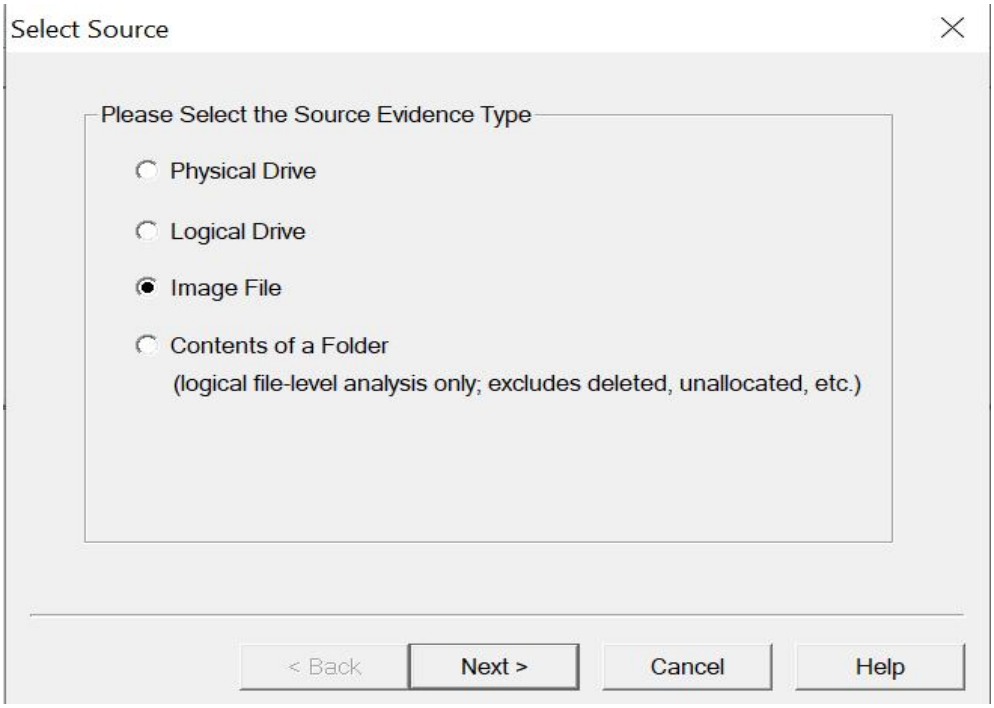


Image Summary
Case Number: 101
Evidence Number: 01
Unique Description: D Drive
Examiner: CS_5113-18
Notes: Evidence found on site

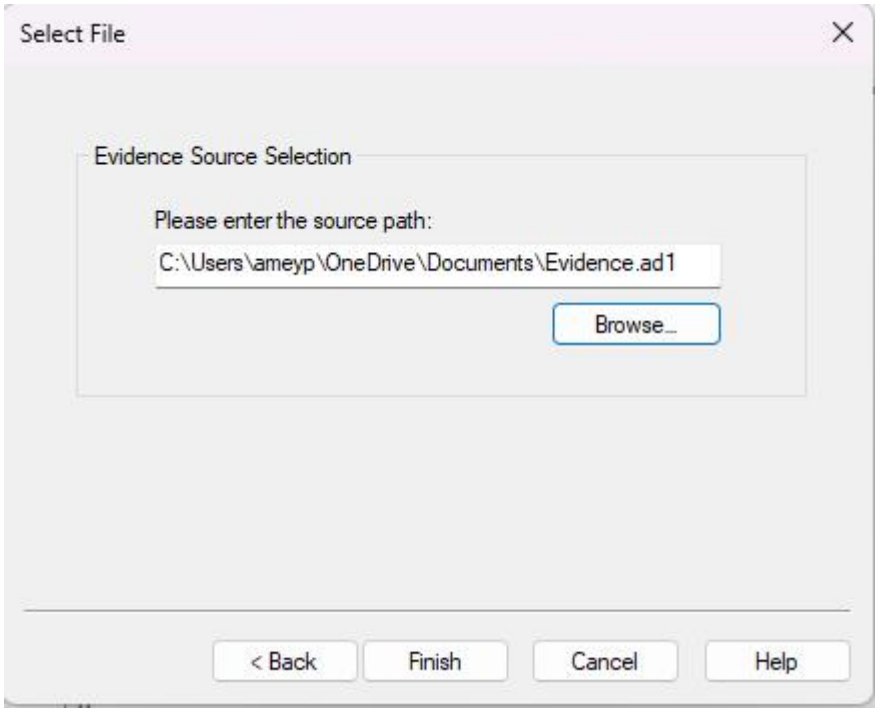
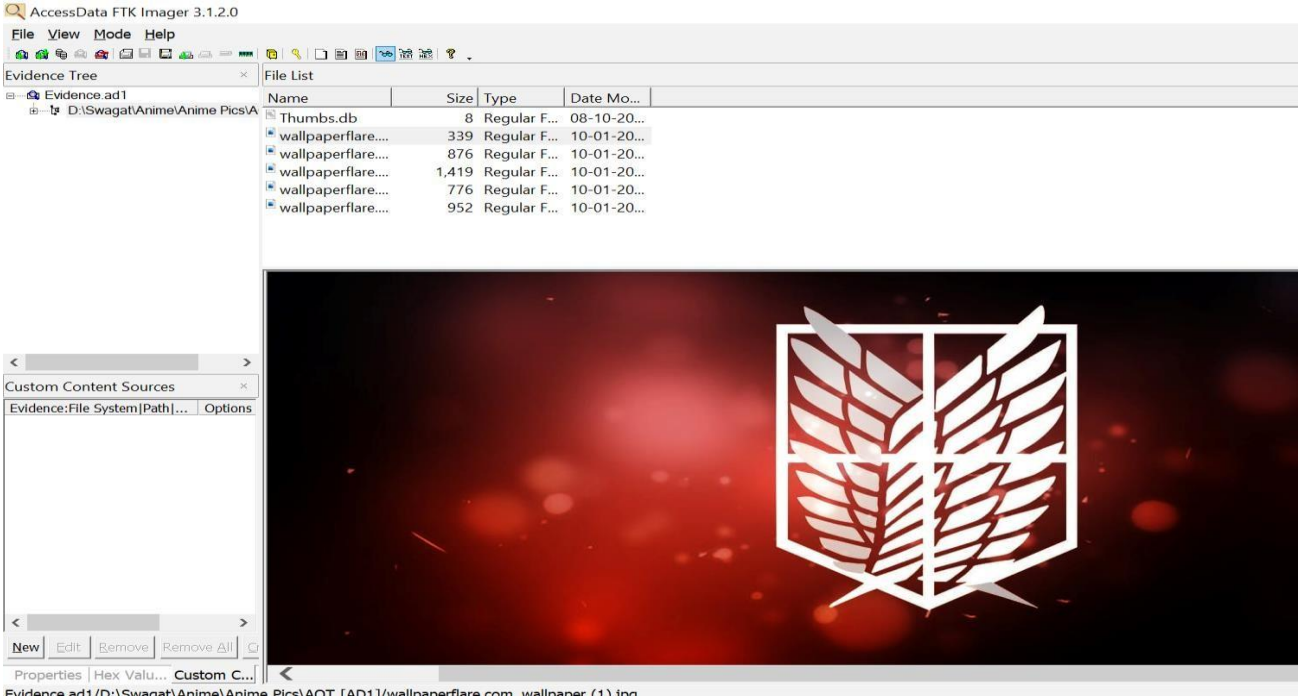
Information for C:\Users\ameyp\OneDrive\Documents\Evidence.ad1:
[Computed Hashes]
MD5 checksum: 5eb21a113dc96fc7a5463ead3fc1905f
SHA1 checksum: f38d91da39ed87a5e0298cca9121e607b2d2915e
Image information:
Acquisition started: Sun Jan 22 15:59:19 2023
Acquisition finished: Sun Jan 22 15:59:19 2023
Segment list:
C:\Users\ameyp\OneDrive\Documents\Evidence.ad1
Image Verification Results:
Verification started: Sun Jan 22 15:59:19 2023
Verification finished: Sun Jan 22 15:59:19 2023
MD5 checksum: 5eb21a113dc96fc7a5463ead3fc1905f : verified
SHA1 checksum: f38d91da39ed87a5e0298cca9121e607b2d2915e : ver
OK

C. Analyze Forensic Image

Step 10: Go to File -> Create Image Disk and Select Image File.



Step 11: Browse & Select the Image File we have created and Click on Finish.



Step 12: Analyzed Image File.