EXPERIMENT-01

Aim:
To create, verify, and analyse a forensic image using FTK Imager.

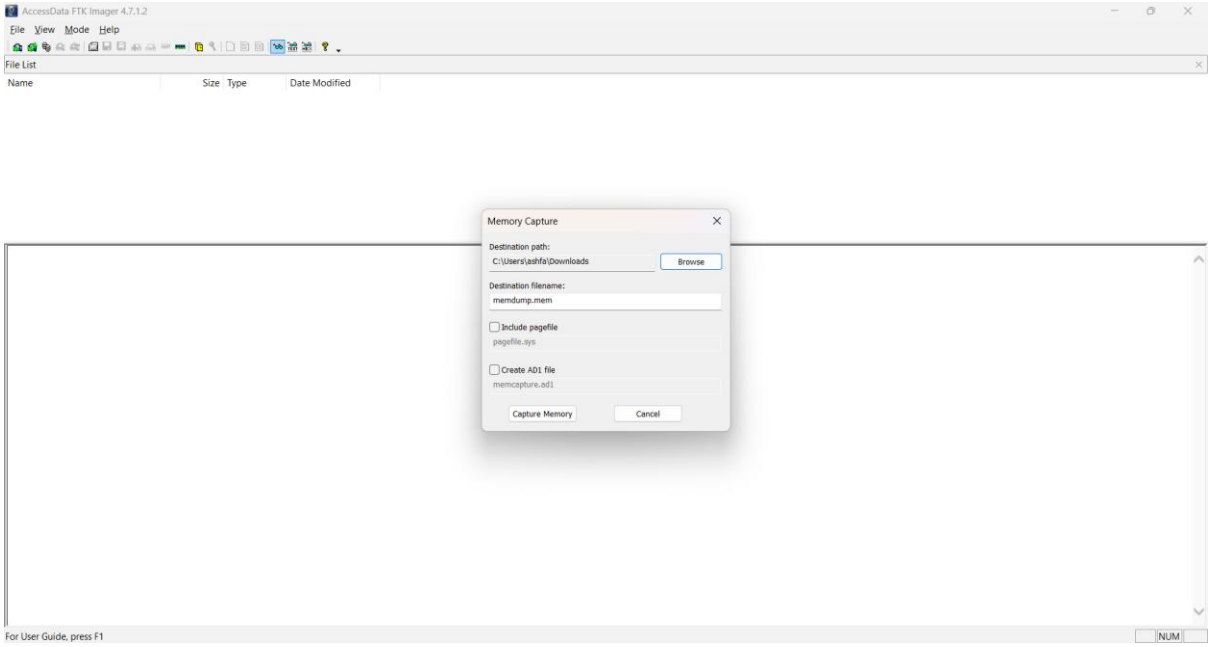
Tools Used:

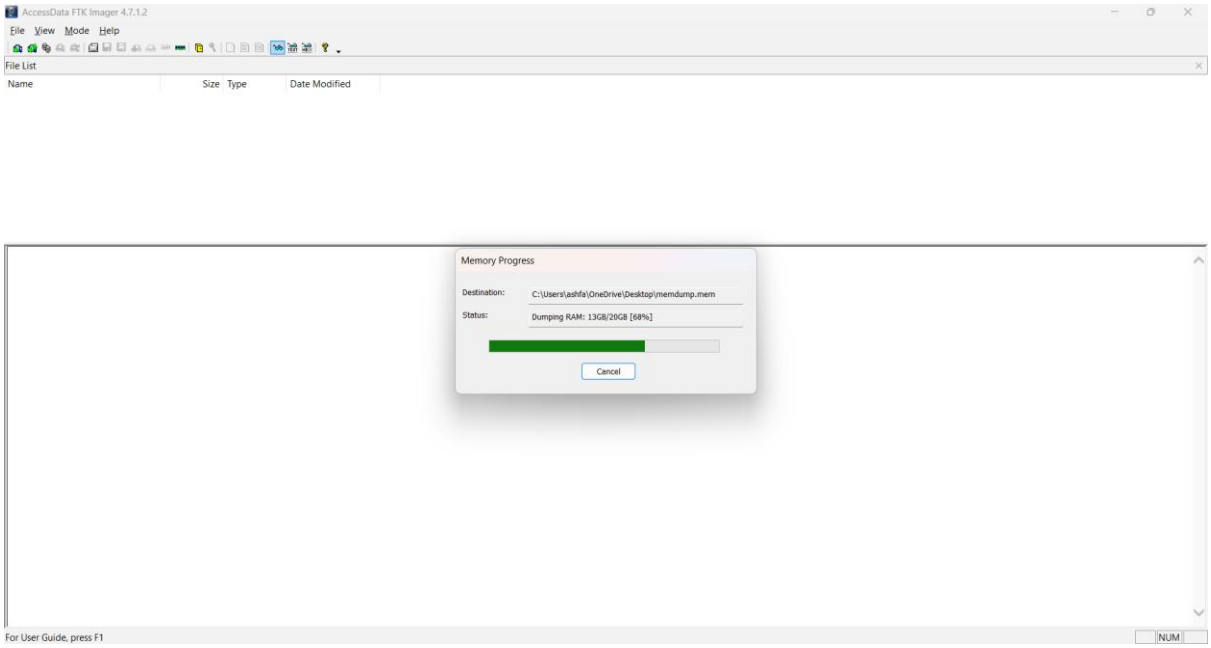
- FTK Imager
- Windows Operating System

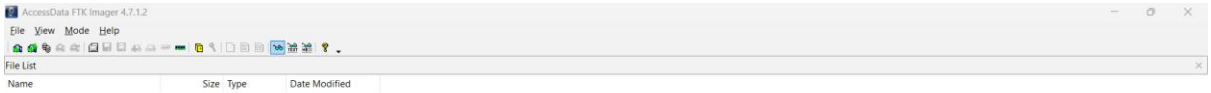
Procedure:

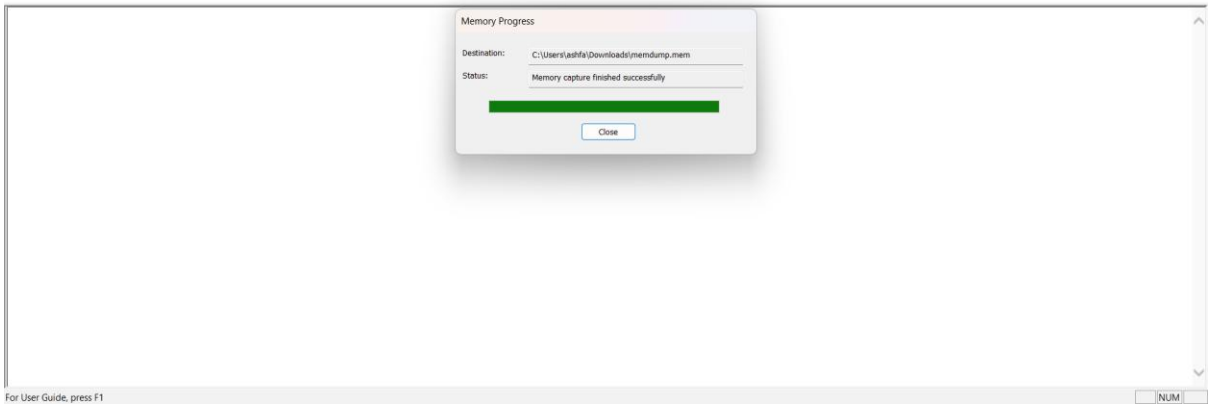
1. Open FTK Imager and choose Create Disk Image.
2. Select Contents of a Folder as the source.
3. Choose a folder and set the destination path for saving the image.
4. FTK generates the image file along with hash values.
5. Verify the image using Verify Image option.
6. Add the image as evidence and explore its contents.

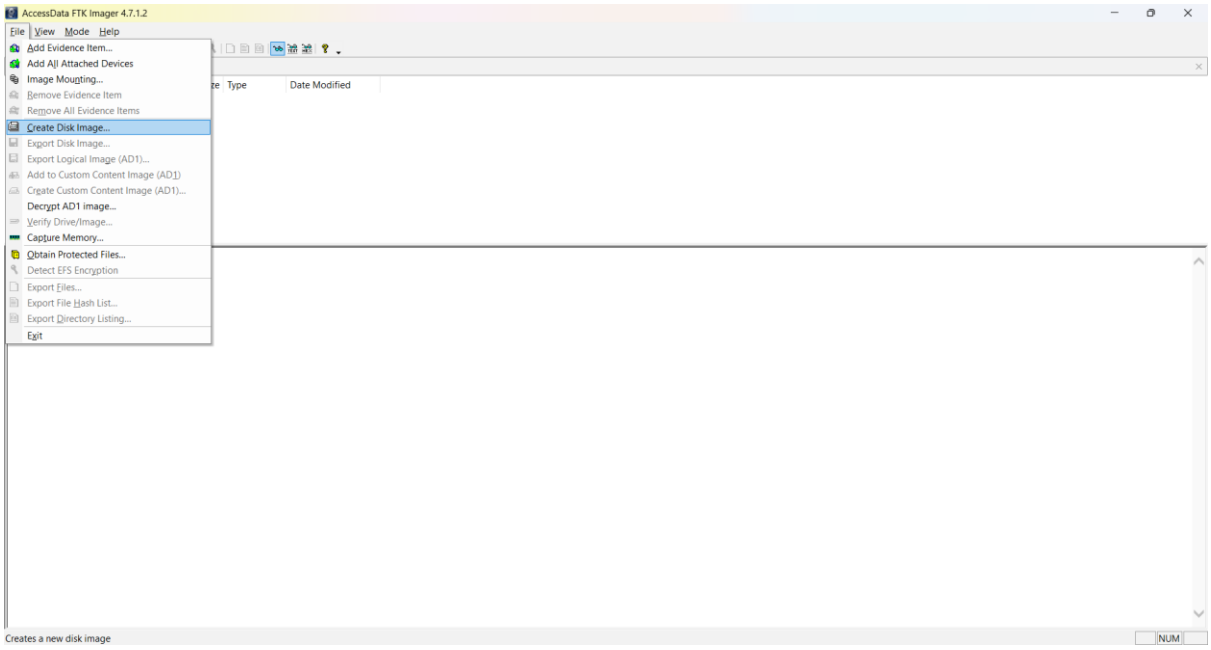
Outputs:

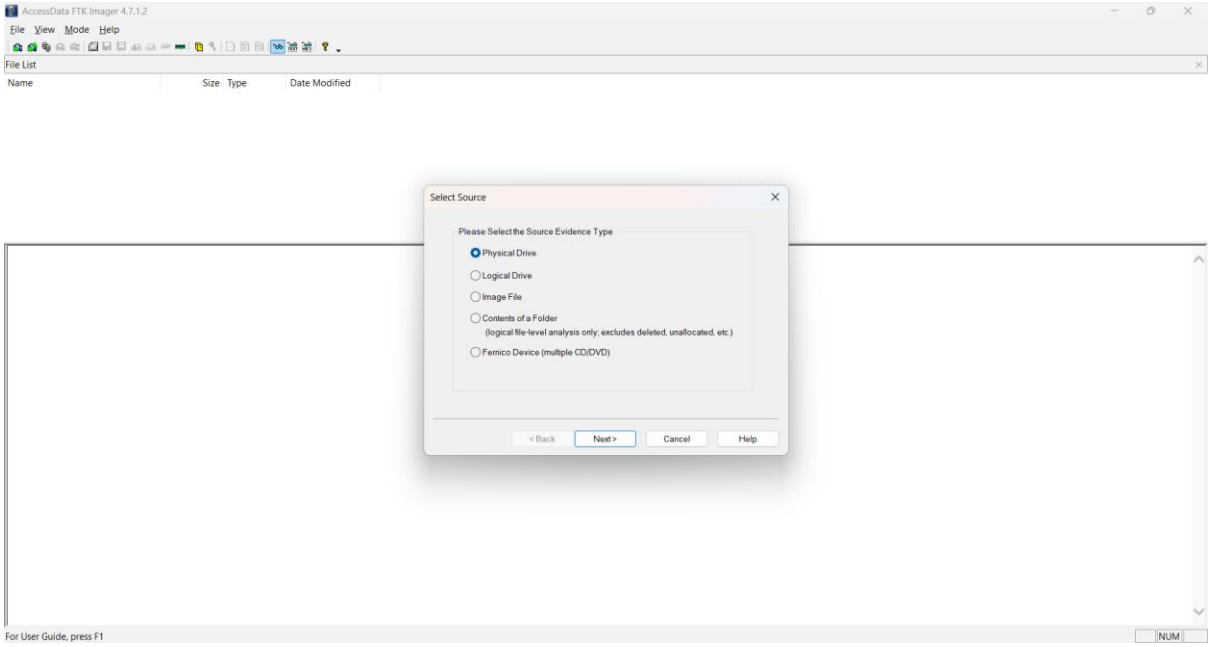

AccessData FTK Imager 4.7.1.2
File View Mode Help
File List
Name Size Type Date Modified
Memory Capture
Destination path:
C:\Users\ashfa\Downloads
Browse
Destination filename:
memdump.mem
Include pagefile
pagefile.sys
Create AD1 file
memcapture.ad1
Capture Memory
Cancel
For User Guide, press F1
NUM

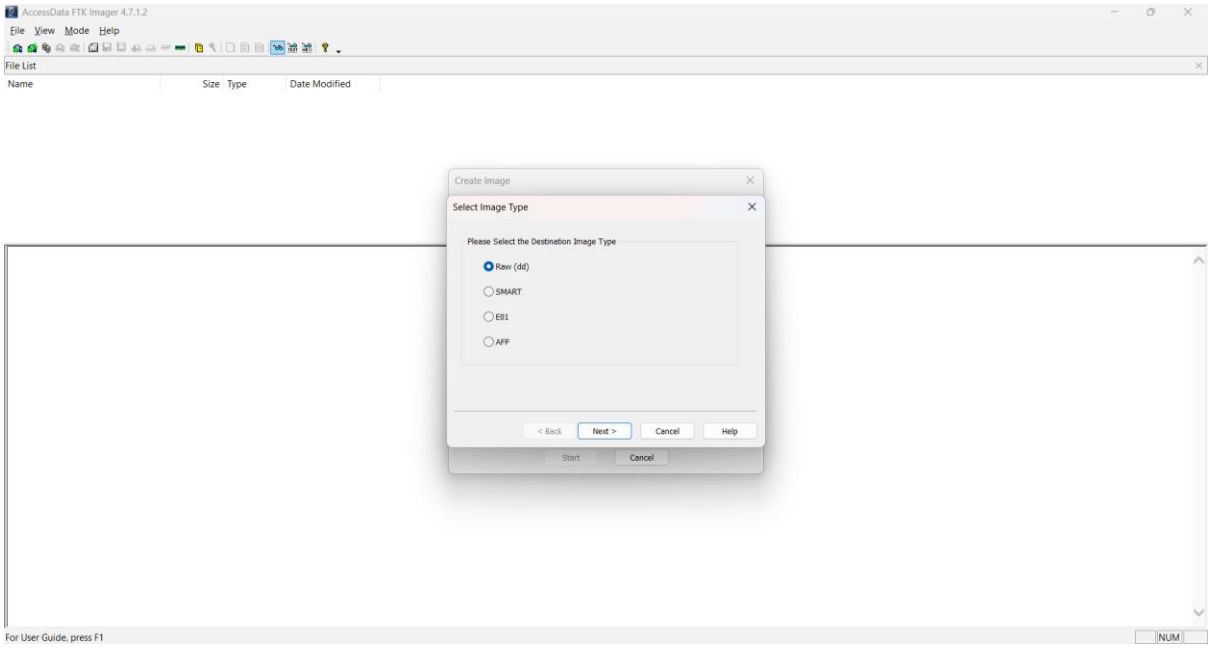

AccessData FTK Imager 4.7.1.2
File View Mode Help
File List
Name Size Type Date Modified
Memory Progress
Destination:
C:\Users\ashfa\OneDrive\Desktop\memdump.mem
Status:
Dumping RAM: 13GB/20GB [68%]
Cancel
For User Guide, press F1
NUM

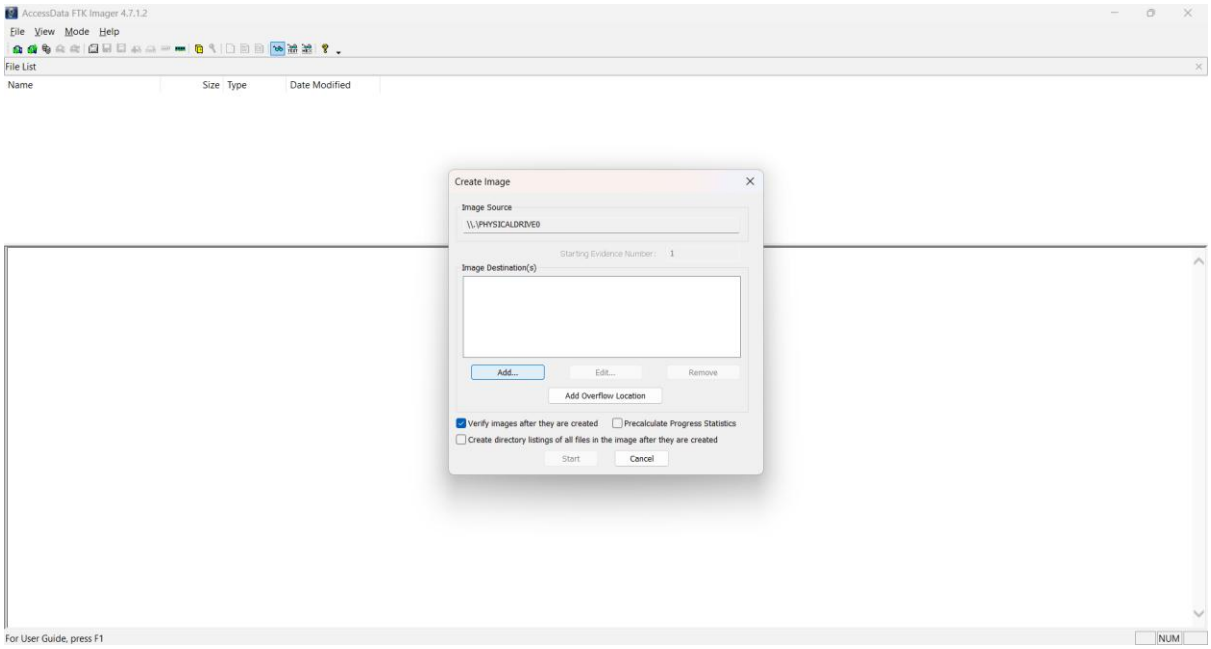

AccessData FTK Imager 4.7.1.2
File View Mode Help
File List
Name Size Type Date Modified

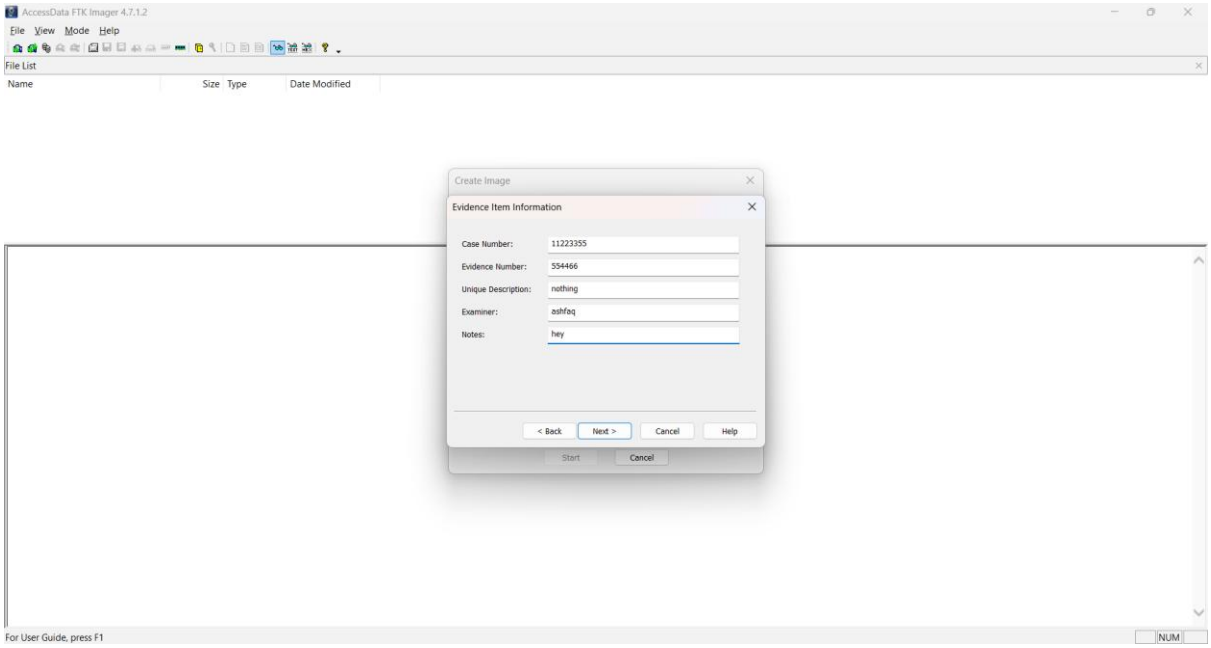

Memory Progress
Destination:
C:\Users\ashfa\Downloads\memdump.mem
Status:
Memory capture finished successfully
Close
For User Guide, press F1
NUM

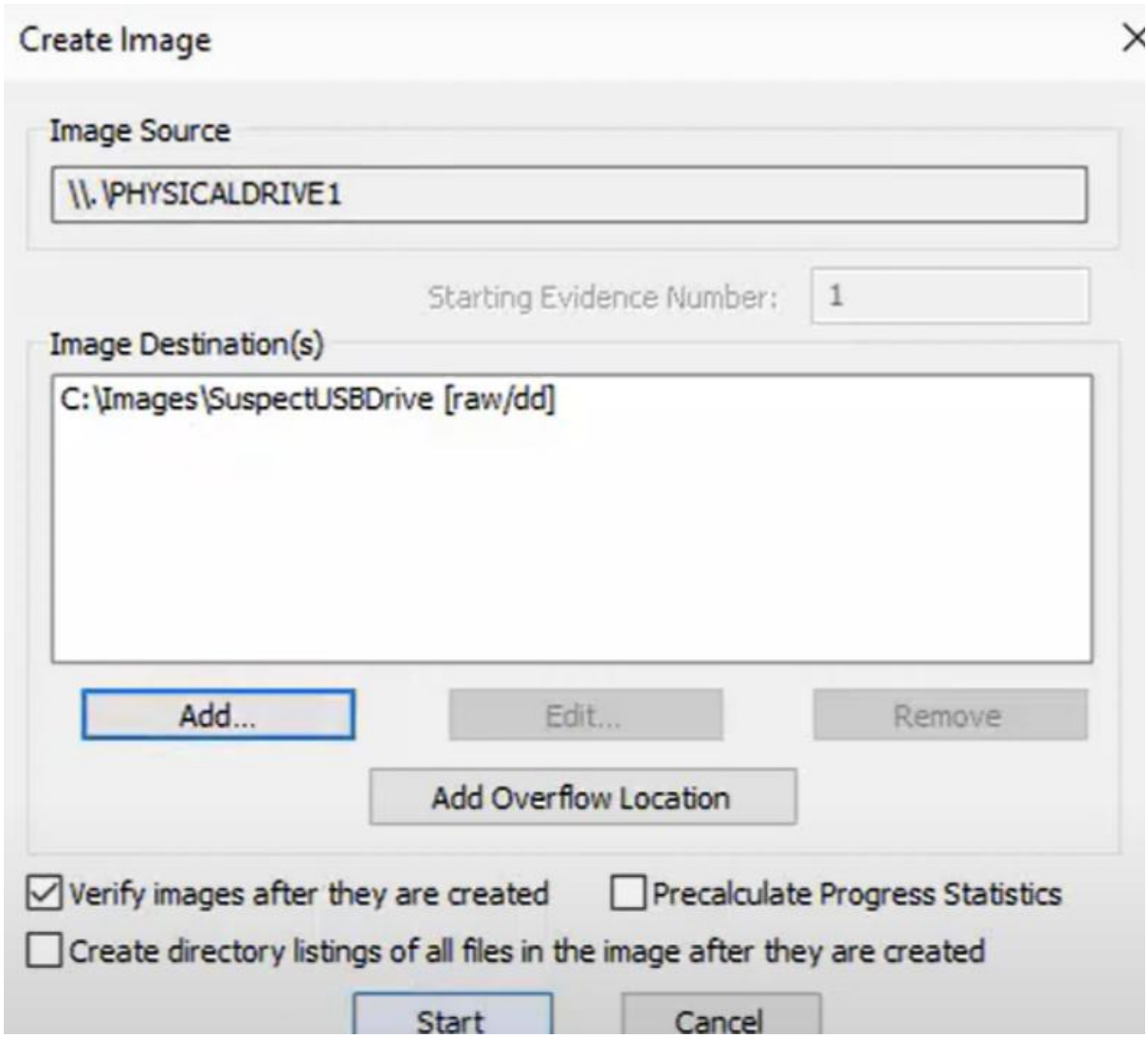

AccessData FTK Imager 4.7.1.2
File View Mode Help
Add Evidence Item...
Add All Attached Devices
Image Mounting...
Remove Evidence Item
Remove All Evidence Items
Create Disk Image...
Export Disk Image...
Export Logical Image (AD1)...
Add to Custom Content Image (AD1)
Create Custom Content Image (AD1)...
Decrypt AD1 image...
Verify Drive/Image...
Capture Memory...
Obtain Protected Files...
Detect EFS Encryption
Export Files...
Export File Hash List...
Export Directory Listing...
Exit
Type
Date Modified
Creates a new disk image
NUM


AccessData FTK Imager 4.7.1.2
File View Mode Help
File List
Name Size Type Date Modified
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
For User Guide, press F1
NUM


AccessData FTK Imager 4.7.1.2
File View Mode Help
File List
Name Size Type Date Modified
Create Image
Select Image Type
Please Select the Destination Image Type
Raw (dd)
SMART
E01
AFF
< Back
Next >
Cancel
Help
Start
Cancel
For User Guide, press F1
NUM


AccessData FTK Imager 4.7.1.2
File View Mode Help
File List
Name Size Type Date Modified
Create Image
Image Source
\\.\PHYSICALDRIVE0
Starting Evidence Number: 1
Image Destination(s)
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
For User Guide, press F1
NUM


AccessData FTK Imager 4.7.1.2
File View Mode Help
File List
Name Size Type Date Modified
Create Image
Evidence Item Information
Case Number: 11223355
Evidence Number: 554466
Unique Description: nothing
Examiner: ashfaq
Notes: hey
< Back Next > Cancel Help
Start Cancel
For User Guide, press F1
NUM



Result:

A forensic image of the selected folder was successfully created, verified, and analysed using FTK Imager. The experiment demonstrated the process of evidence acquisition and integrity verification in digital forensics.