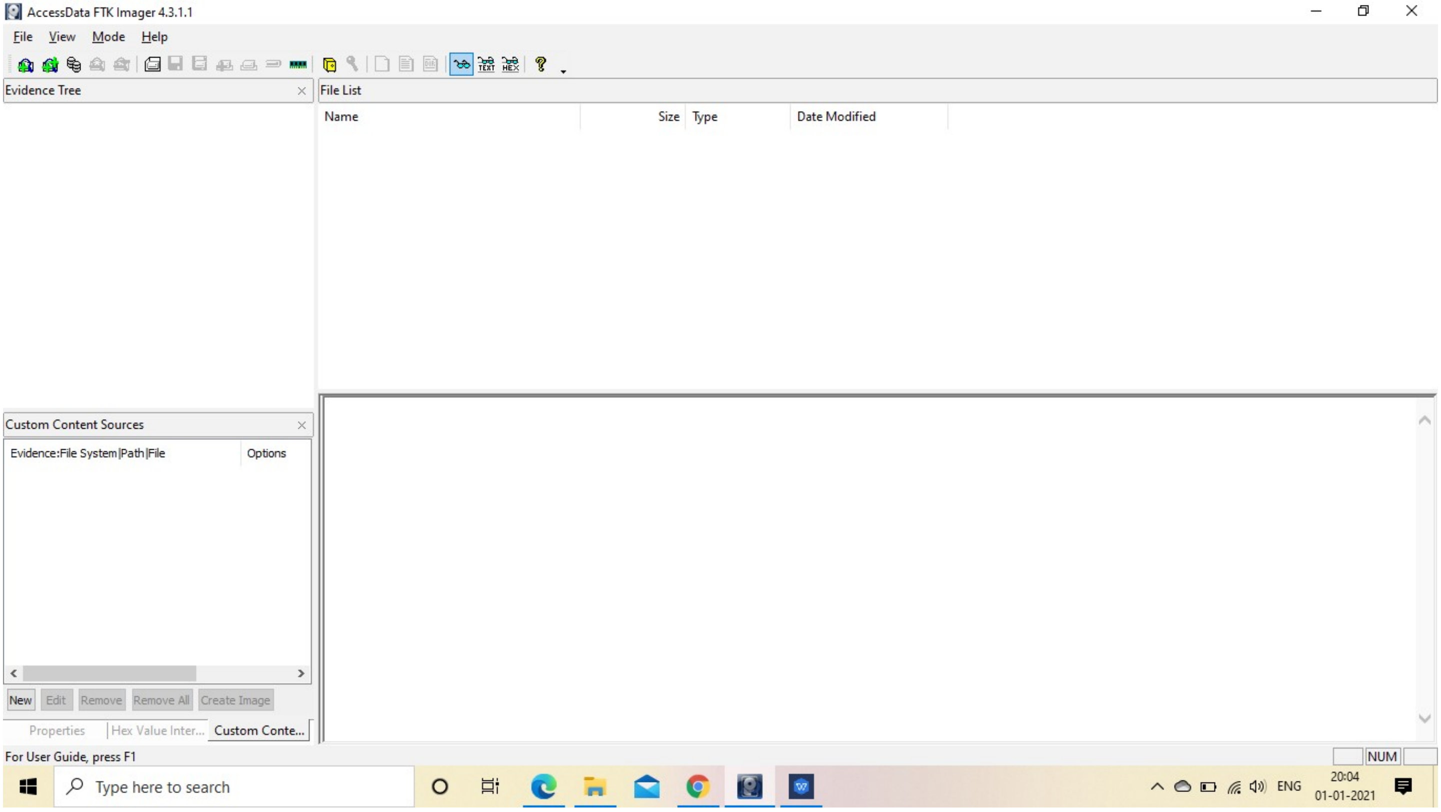
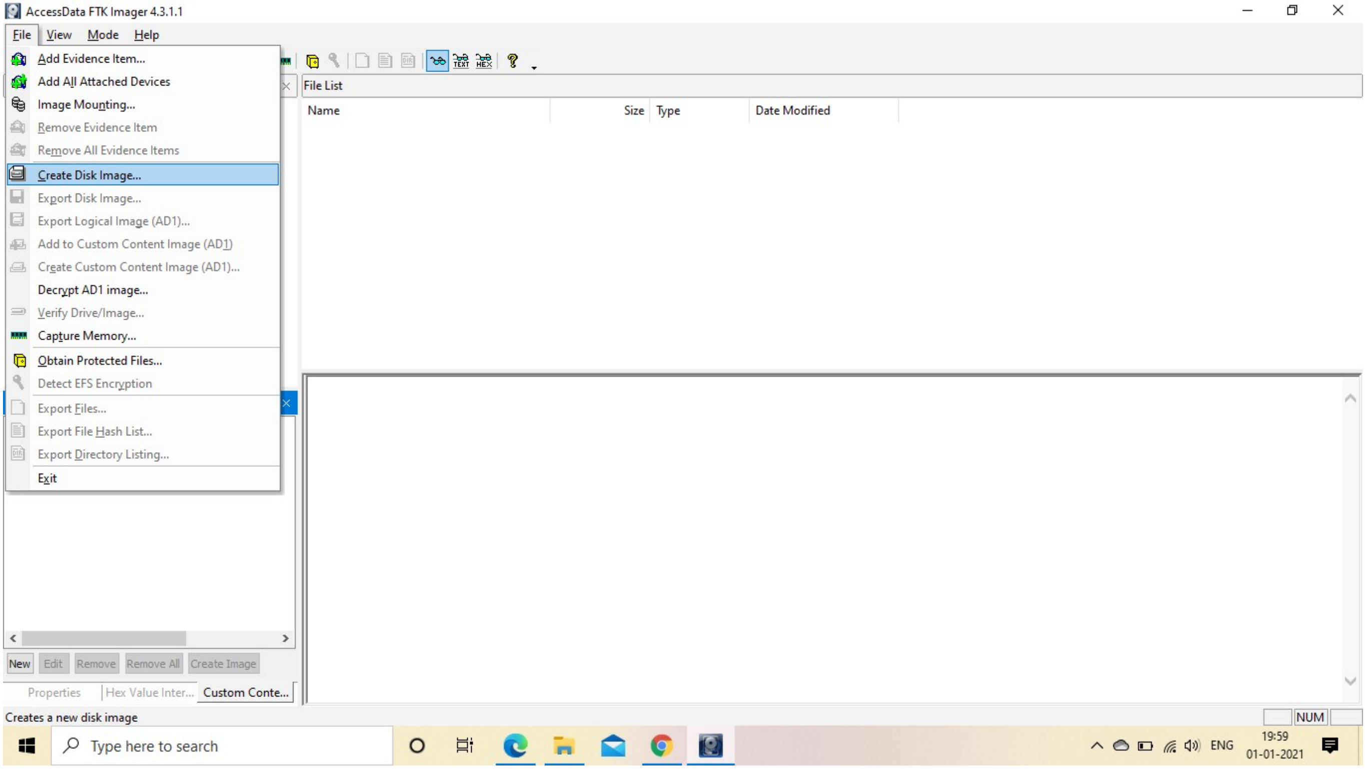
Practical No:7

Aim:Create forensic images of digital devices from volatile data such as memory using Imager for Computer System

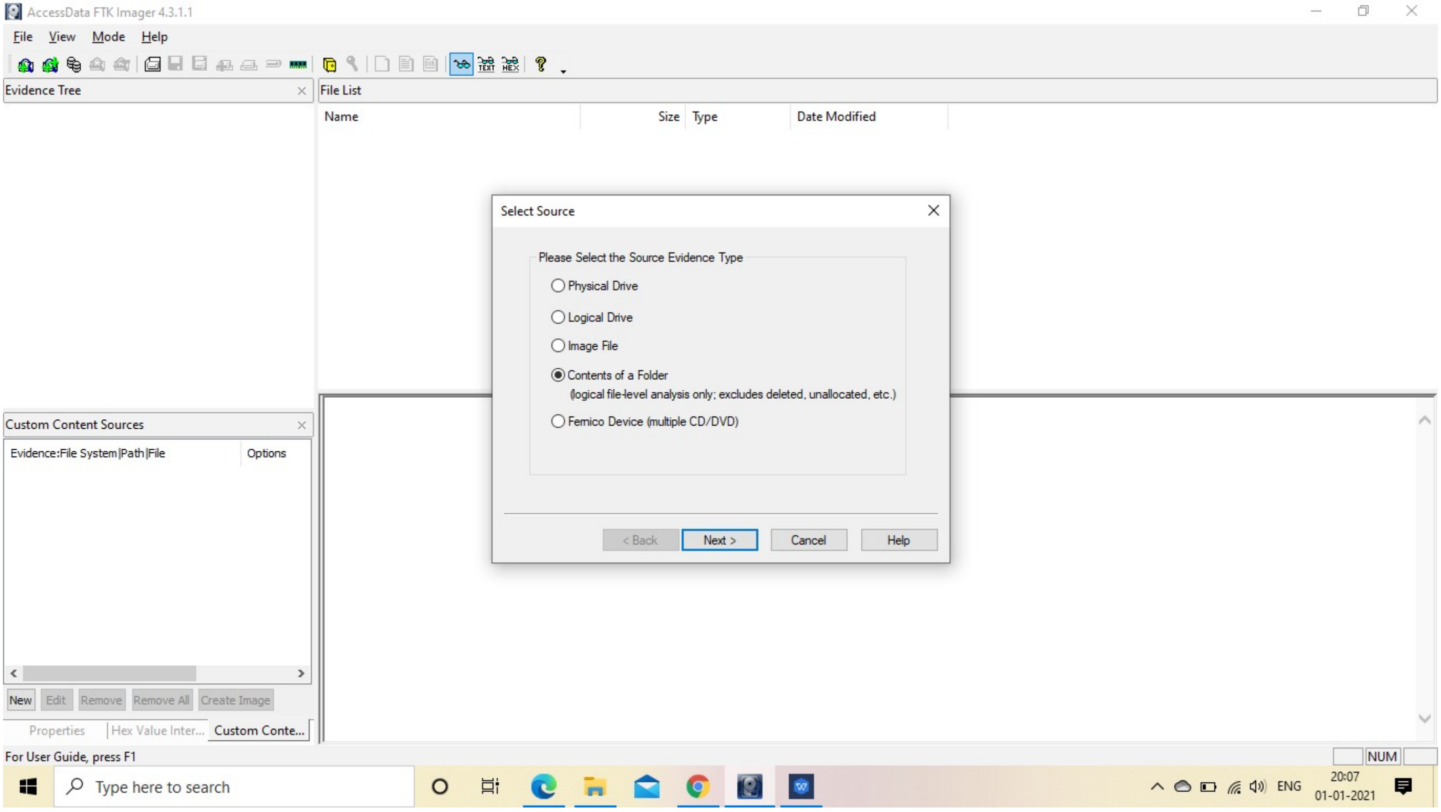
Open Access FTK Imager



Click on File and select Create Disk Image



A popup window will appear and select source as Contents of Folder


AccessData FTK Imager 4.3.1.1
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 Inter... Custom Conte...
For User Guide, press F1
NUM
Type here to search
ENG 20:07 01-01-2021

Select Source

Please Select the Source Evidence Type

○ Physical Drive

○ Logical Drive

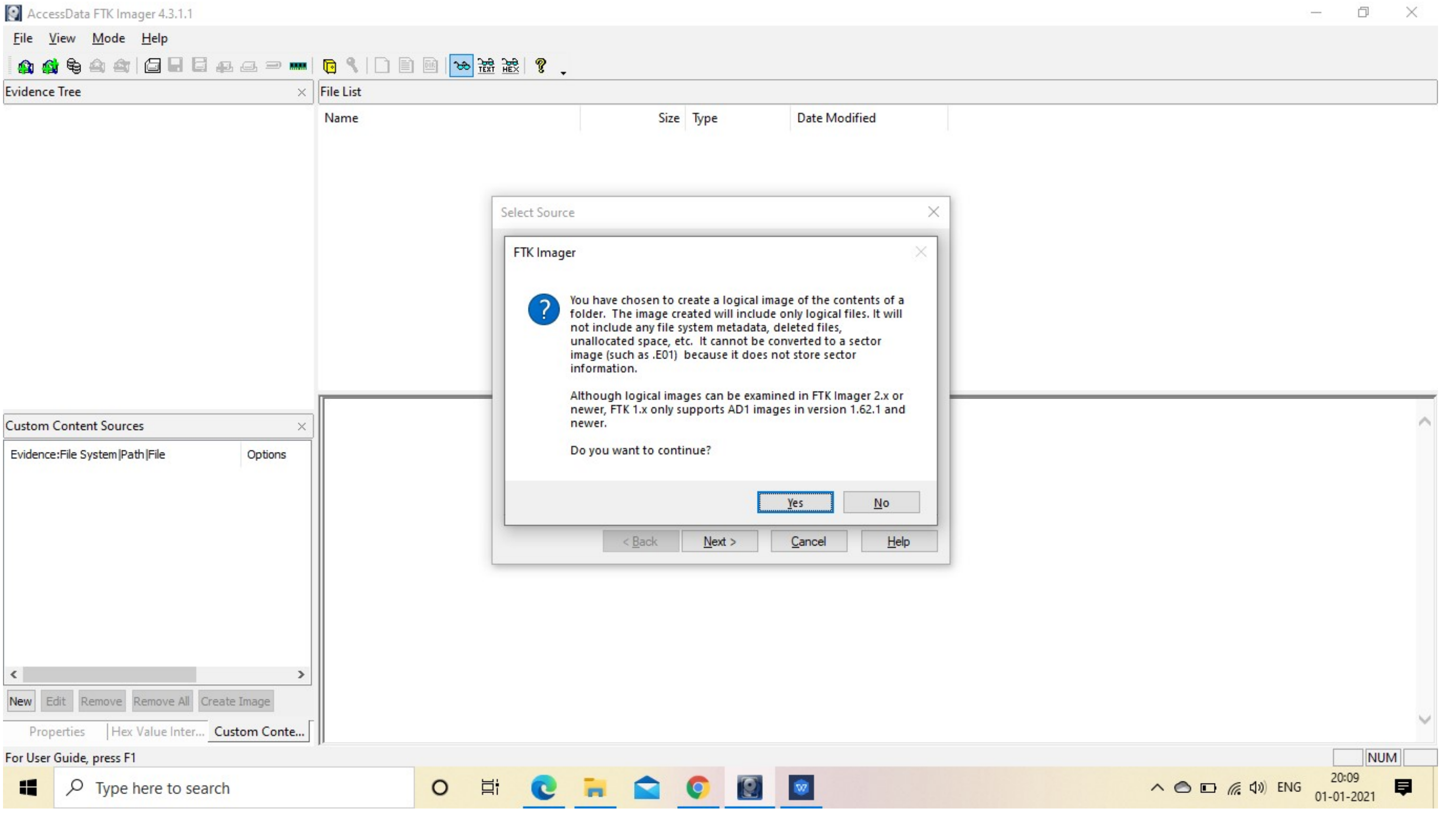
○ Image File

● Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

○ Femico Device (multiple CD/DVD)

< Back | Next > | Cancel | Help

Click on Next and Click Yes


AccessData FTK Imager 4.3.1.1
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
Select Source
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
< Back Next > Cancel Help
For User Guide, press F1
NUM
Type here to search
ENG 20:09 01-01-2021

FTK Imager

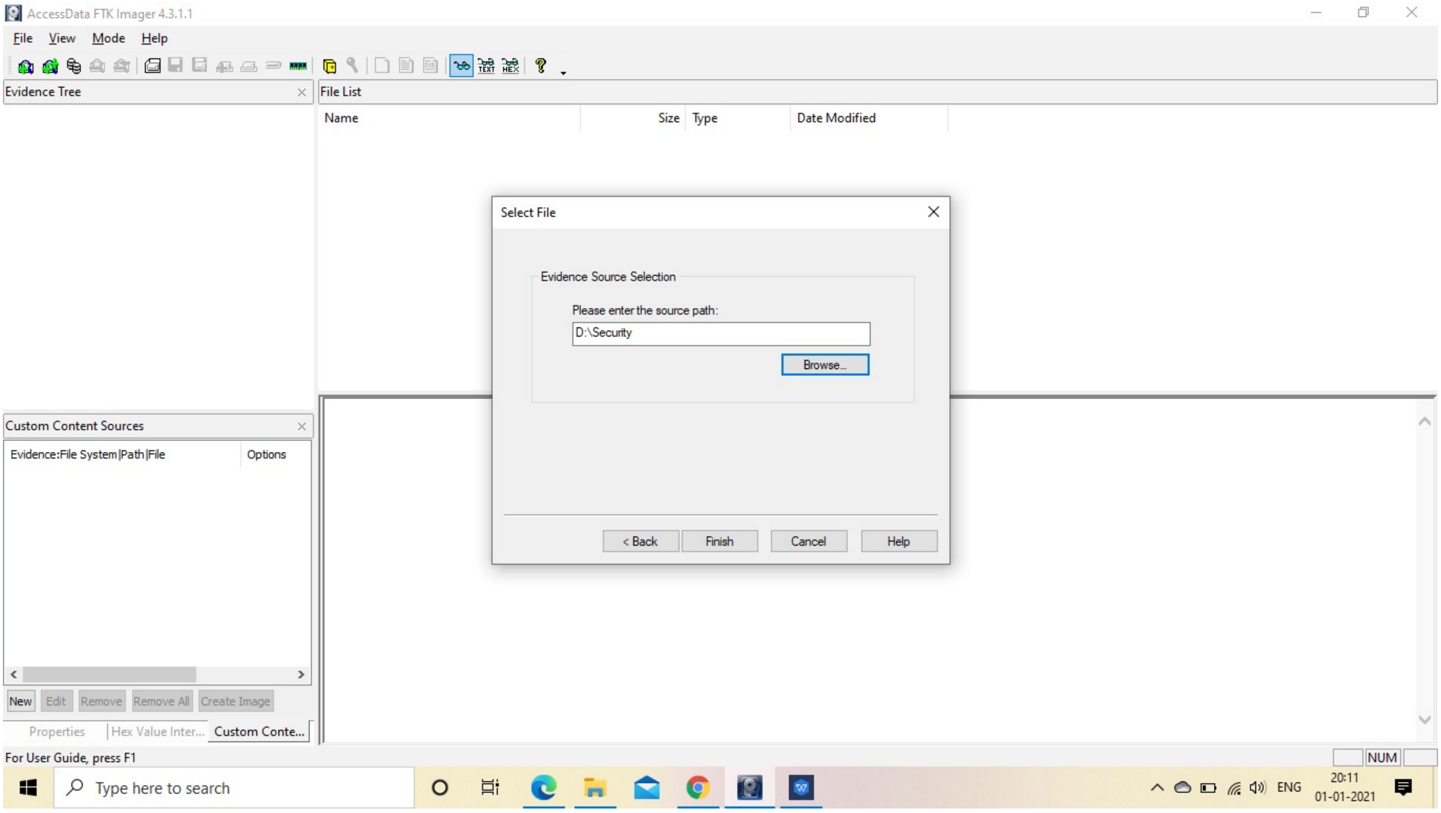
You have chosen to create a logical image of the contents of a folder. The image created will include only logical files. It will not include any file system metadata, deleted files, unallocated space, etc. It cannot be converted to a sector image (such as .E01) because it does not store sector information.

Although logical images can be examined in FTK Imager 2.x or newer, FTK 1.x only supports AD1 images in version 1.62.1 and newer.

Do you want to continue?

Yes | No

Select the File and Click on Finish


AccessData FTK Imager 4.3.1.1
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 Inter... Custom Conte...
For User Guide, press F1
NUM
Type here to search
ENG 20:11 01-01-2021

Select File

Evidence Source Selection

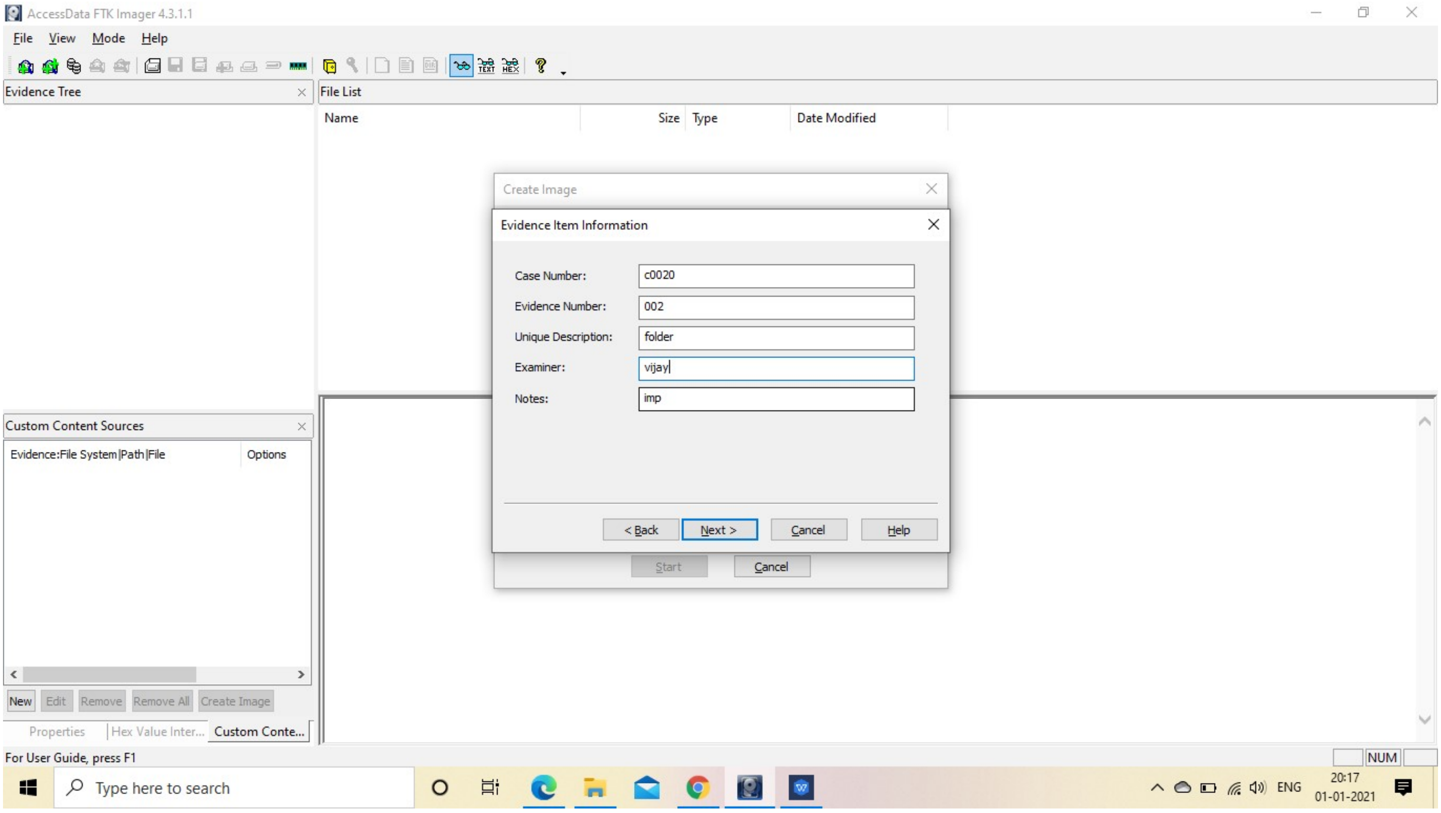
Please enter the source path:

D:\Security

Browse...

< Back Finish Cancel Help

Add the Evidence Information and click on next


AccessData FTK Imager 4.3.1.1
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 Inter... Custom Conte...
For User Guide, press F1
NUM
Type here to search
ENG 20:17 01-01-2021

Create Image

Evidence Item Information

Case Number:	c0020
Evidence Number:	002
Unique Description:	folder
Examiner:	vijay
Notes:	imp

< Back Next > Cancel Help

Start Cancel

Select the Image Destination and Click on Finish

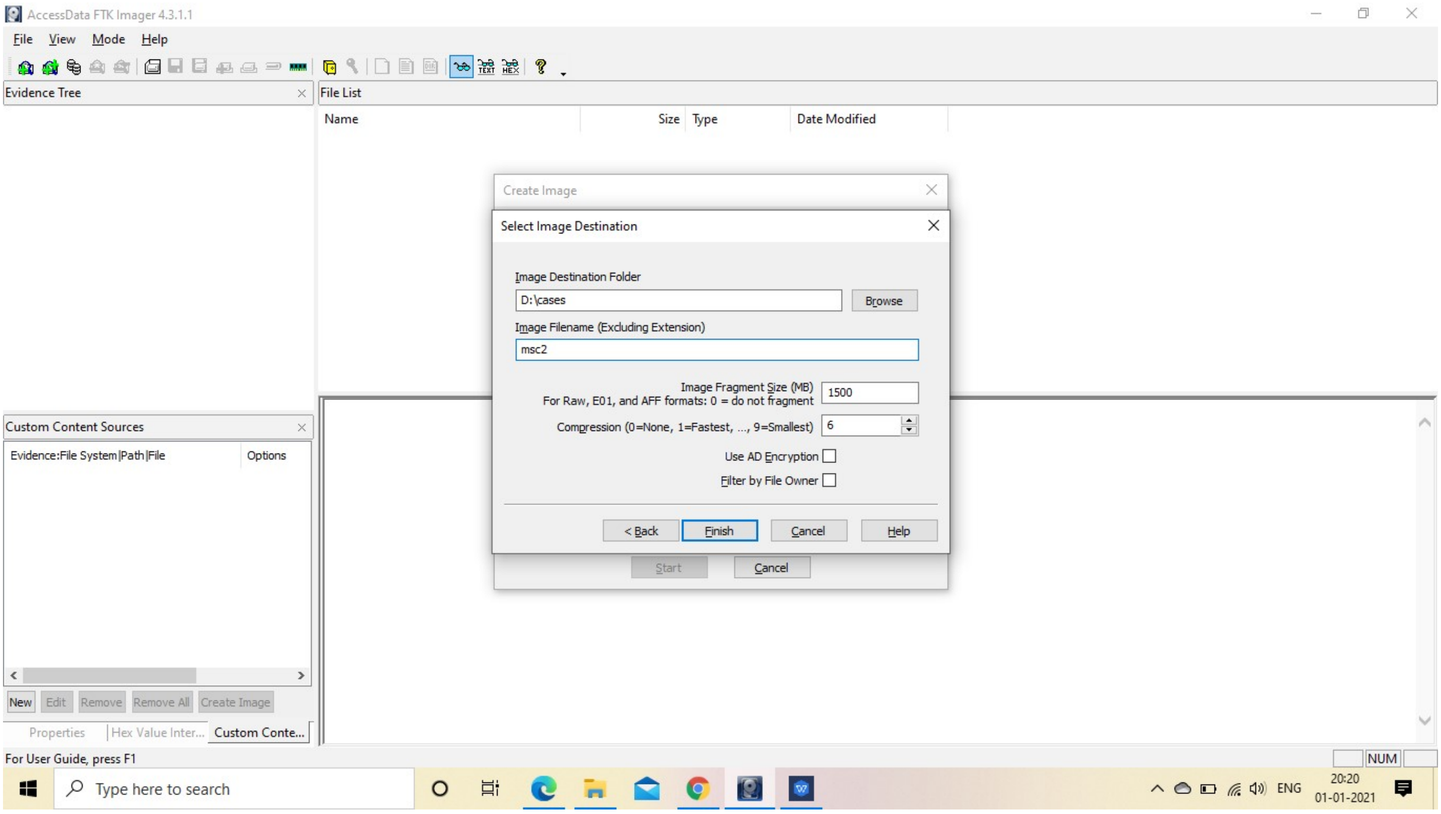

AccessData FTK Imager 4.3.1.1
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
Create Image
Select Image Destination
Browse
< Back Finish Cancel Help
Start Cancel
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
For User Guide, press F1
NUM
Type here to search
ENG 20:20 01-01-2021

Image Destination Folder: D:\cases

Image Filename (Excluding Extension): msc2

Image Fragment Size (MB) For Raw, E01, and AFF formats: 0 = do not fragment: 1500

Compression (0=None, 1=Fastest, ..., 9=Smallest): 6

Use AD Encryption □

Filter by File Owner □

We can see that the Image Source and Destination has been created, just click on Add button

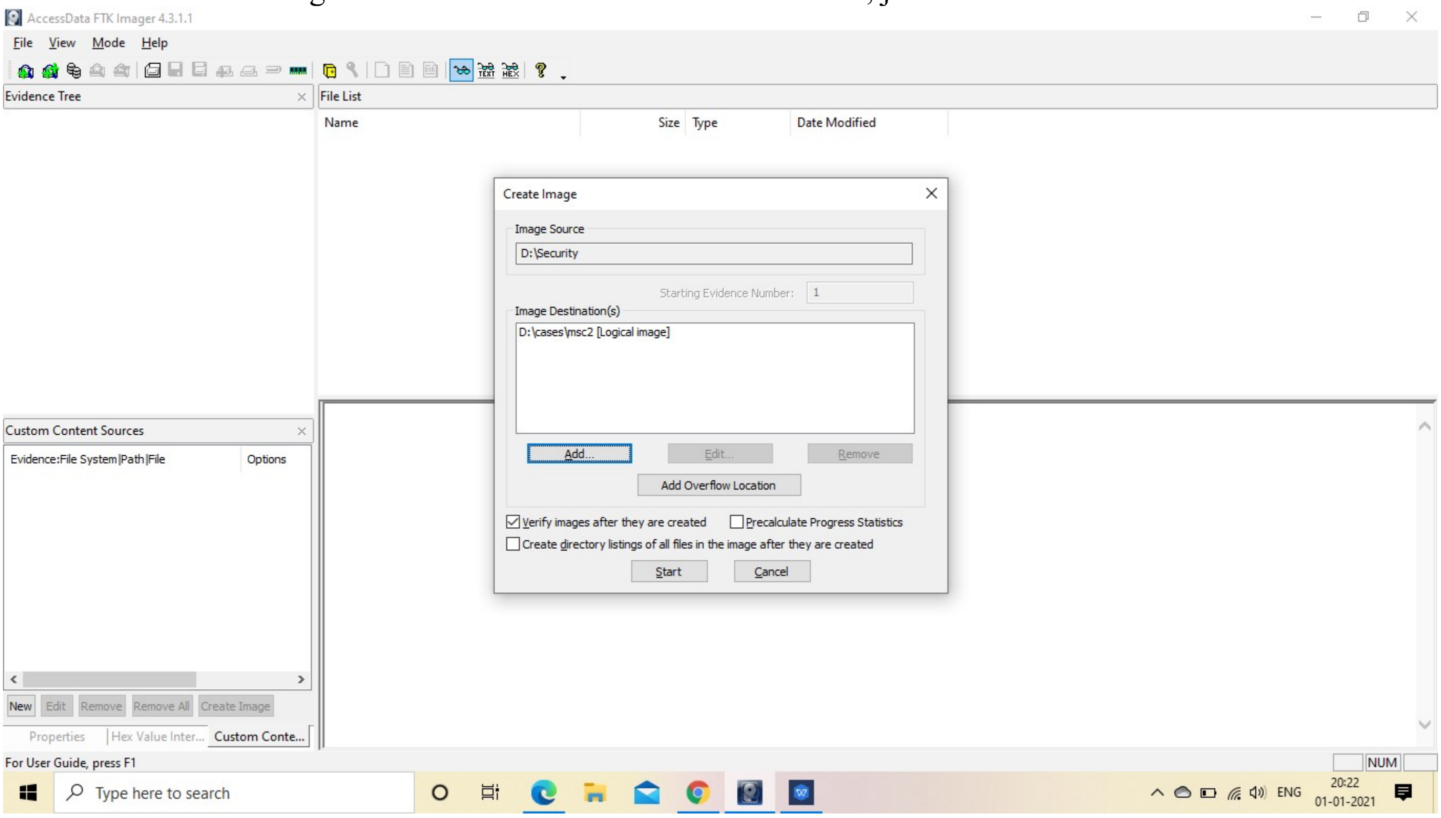


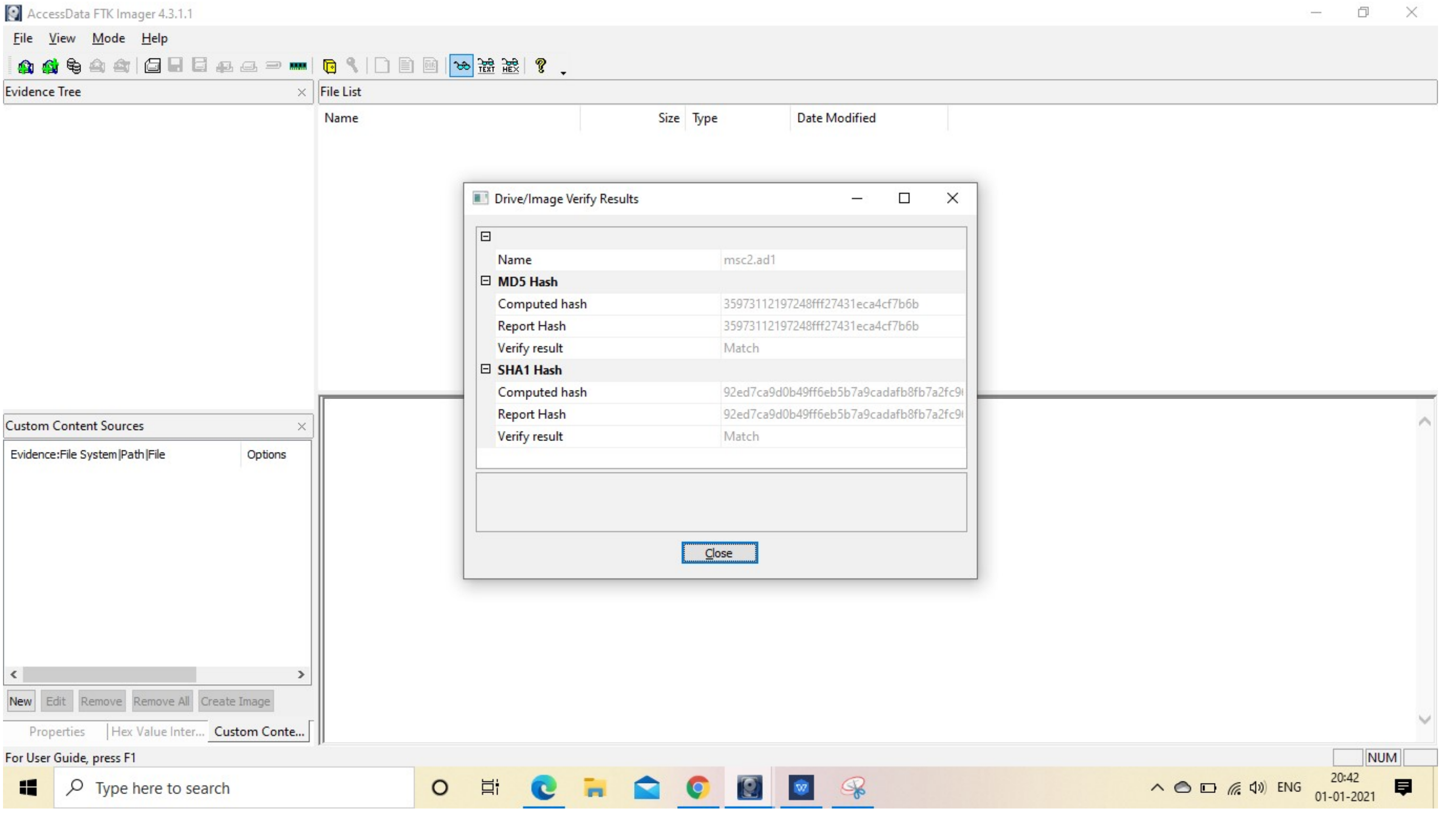
Image Source: D:\Security

Starting Evidence Number: 1

Image Destination(s): D:\cases\msc2 [Logical image]

☑ Verify images after they are created □ Precalculate Progress Statistics

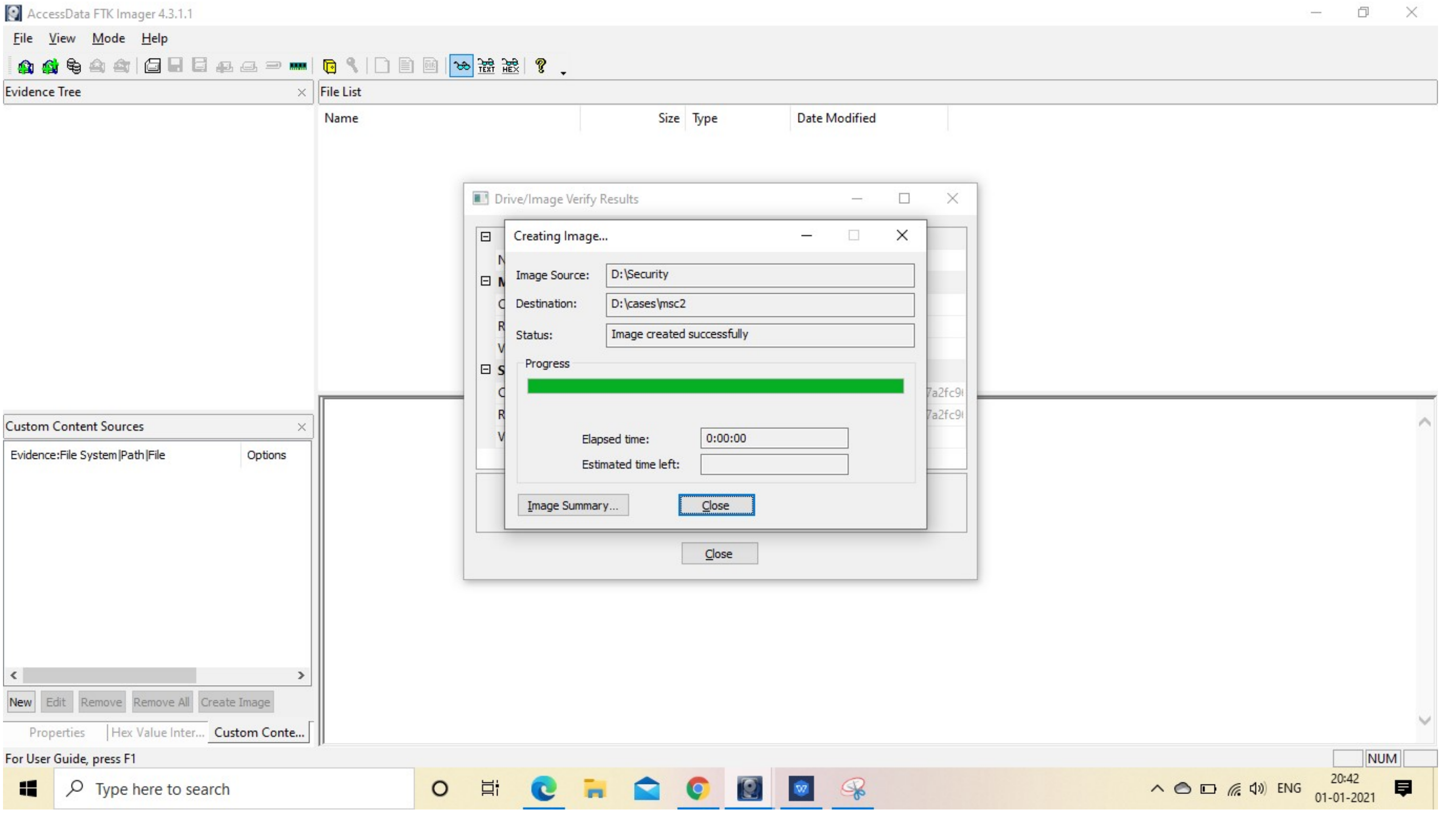
□ Create directory listings of all files in the image after they are created



AccessData FTK Imager 4.3.1.1
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 Inter... Custom Conte...
For User Guide, press F1
NUM
Type here to search
ENG
20:42
01-01-2021

Drive/Image Verify Results

Name	msc2.ad1
MD5 Hash	
Computed hash	35973112197248fff27431eca4cf7b6b
Report Hash	35973112197248fff27431eca4cf7b6b
Verify result	Match
SHA1 Hash	
Computed hash	92ed7ca9d0b49ff6eb5b7a9cadafb8fb7a2fc9
Report Hash	92ed7ca9d0b49ff6eb5b7a9cadafb8fb7a2fc9
Verify result	Match



AccessData FTK Imager 4.3.1.1
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
Drive/Image Verify Results
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
For User Guide, press F1
NUM
Type here to search
ENG
20:42
01-01-2021

Creating Image...

Image Source: D:\Security

Destination: D:\cases\msc2

Status: Image created successfully

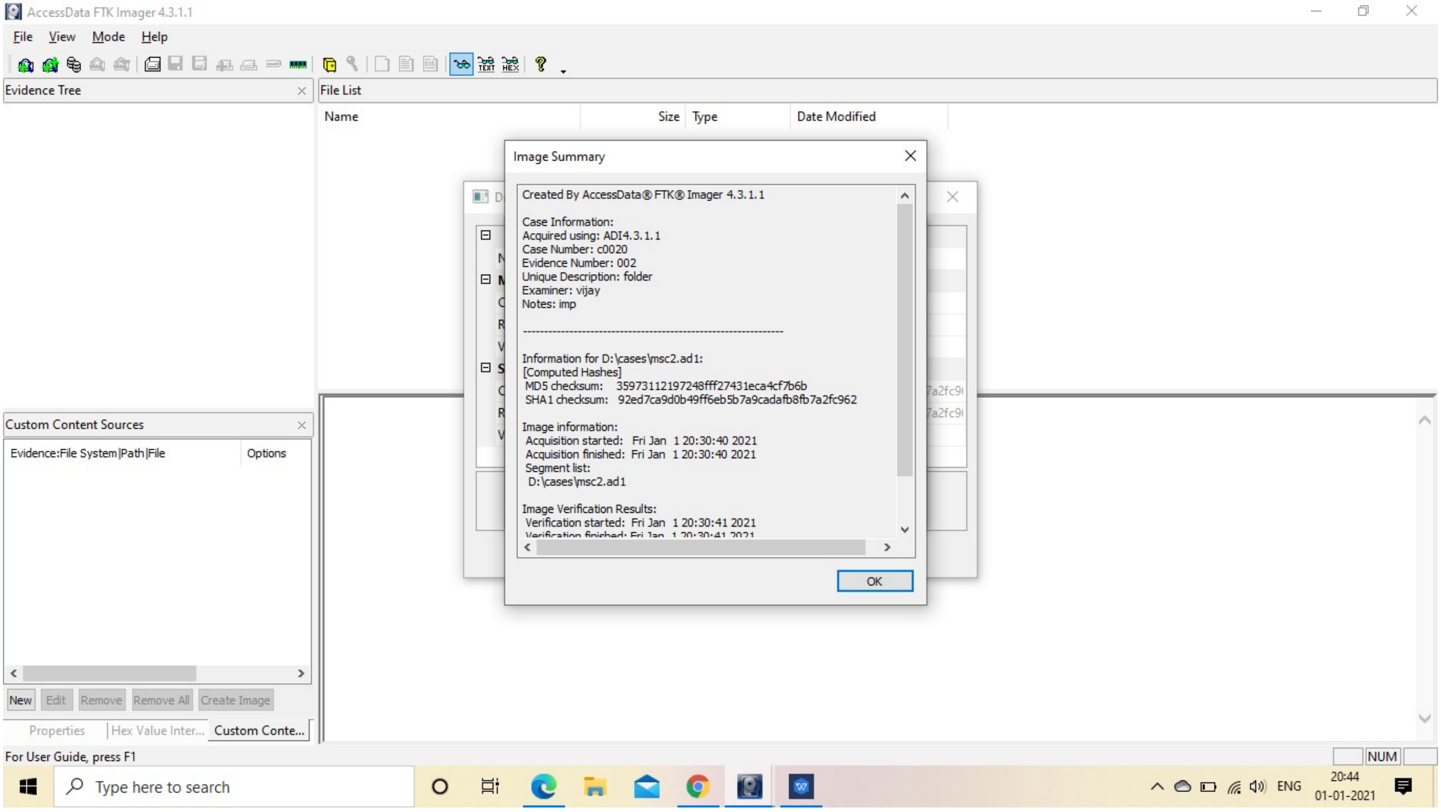
Progress

Elapsed time: 0:00:00

Estimated time left:

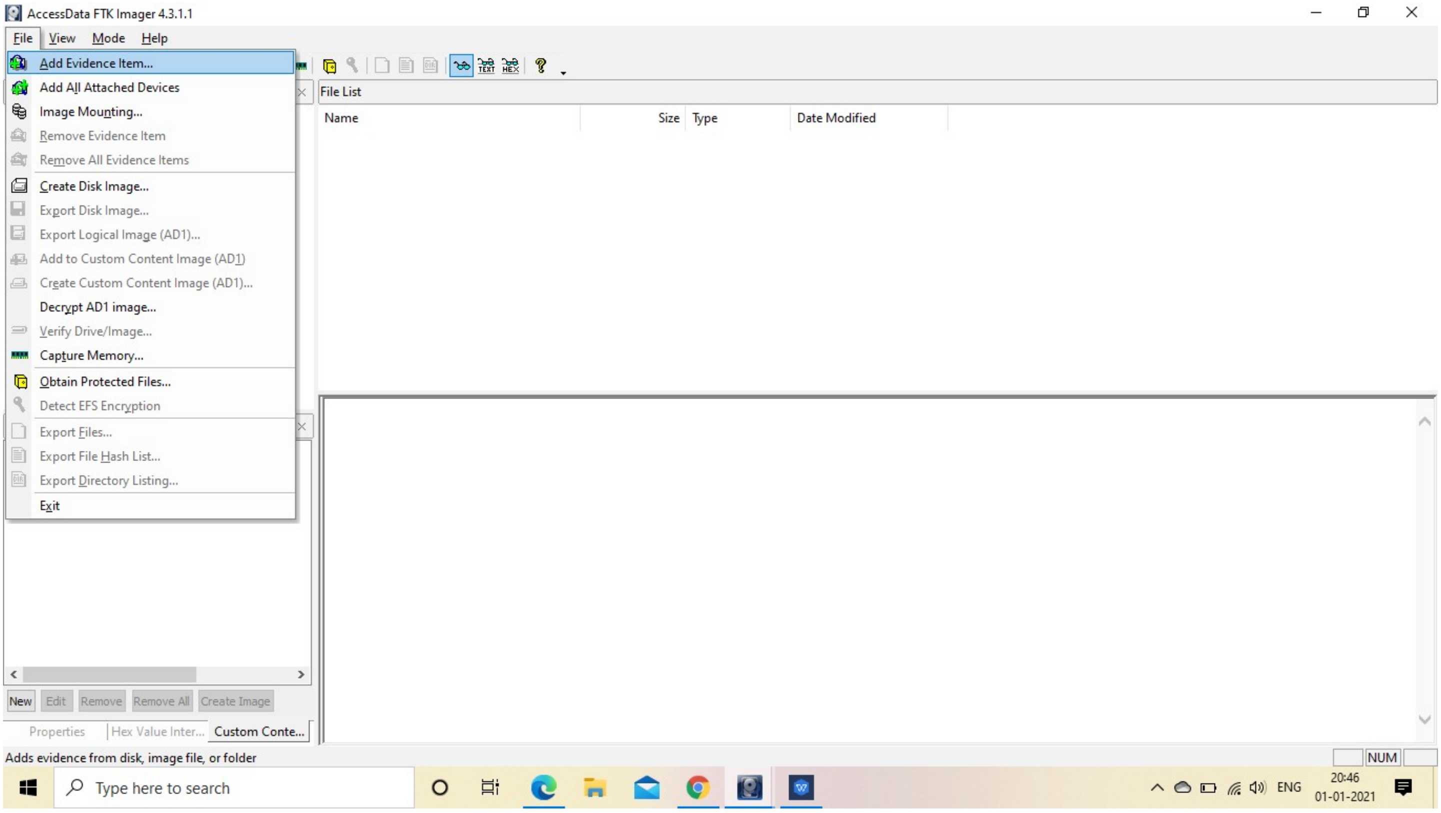
Image Summary...
Close
Close

Click on Image Summary and Close

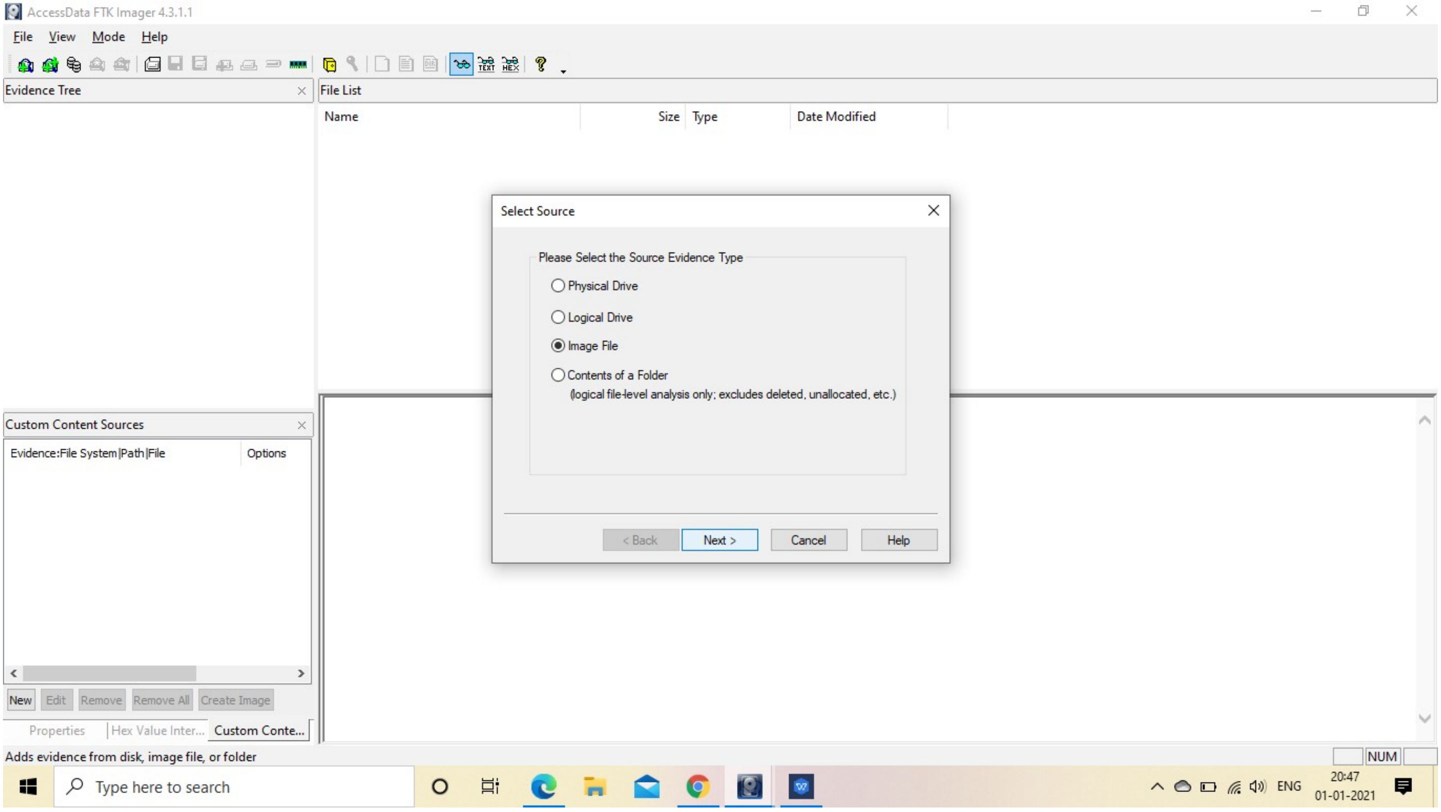


```
Created By AccessData® FTK® Imager 4.3.1.1

Case Information:
Acquired using: ADI4.3.1.1
Case Number: c0020
Evidence Number: 002
Unique Description: folder
Examiner: vijay
Notes: imp

--------------------------------------------------------------

Information for D:\cases\msc2.ad1:
[Computed Hashes]
 MD5 checksum:    35973112197248fff27431eca4cf7b6b
 SHA1 checksum:   92ed7ca9d0b49ff6eb5b7a9cadafb8fb7a2fc962

Image information:
 Acquisition started:   Fri Jan  1 20:30:40 2021
 Acquisition finished:  Fri Jan  1 20:30:40 2021
 Segment list:
  D:\cases\msc2.ad1

Image Verification Results:
 Verification started:  Fri Jan  1 20:30:41 2021
 Verification finished: Fri Jan  1 20:30:41 2021
```

Click again on File and Select Add Evidence Item



Select the Source as Image File and click Next



Select Source

Please Select the Source Evidence Type

○ Physical Drive

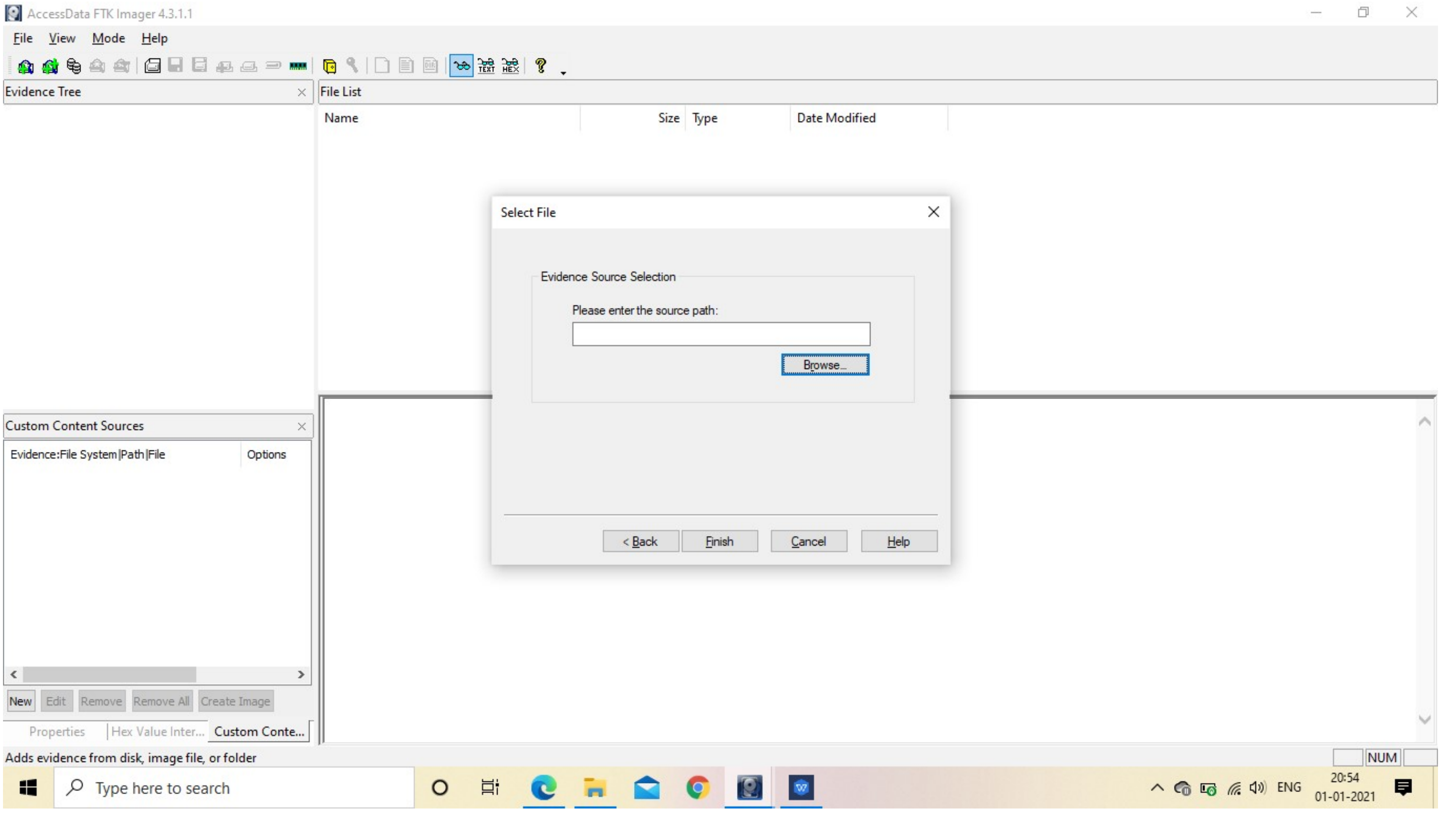
○ Logical Drive

● Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

Adds evidence from disk, image file, or folder

Browse the file



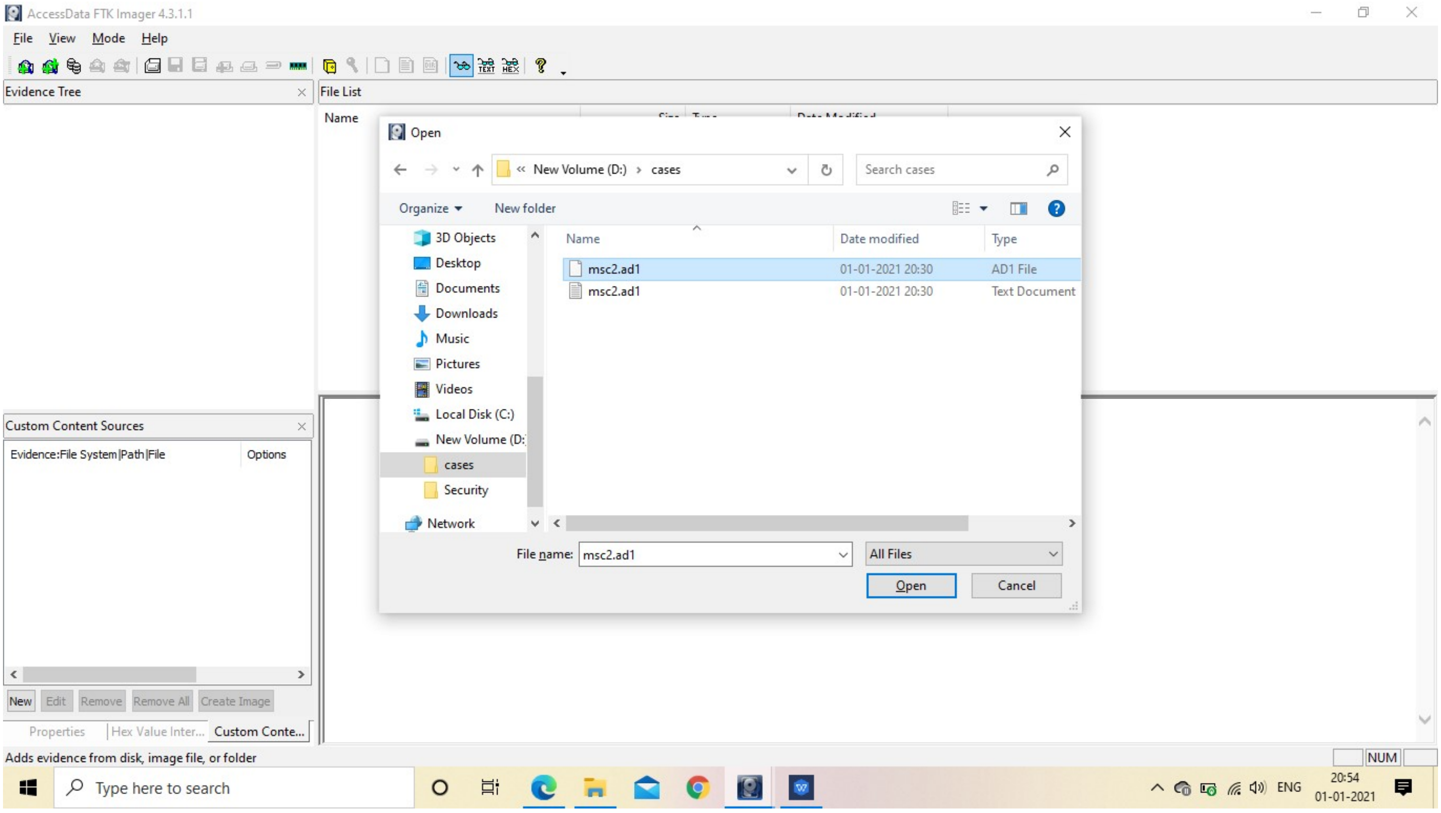
Select File

Evidence Source Selection

Please enter the source path:

Adds evidence from disk, image file, or folder

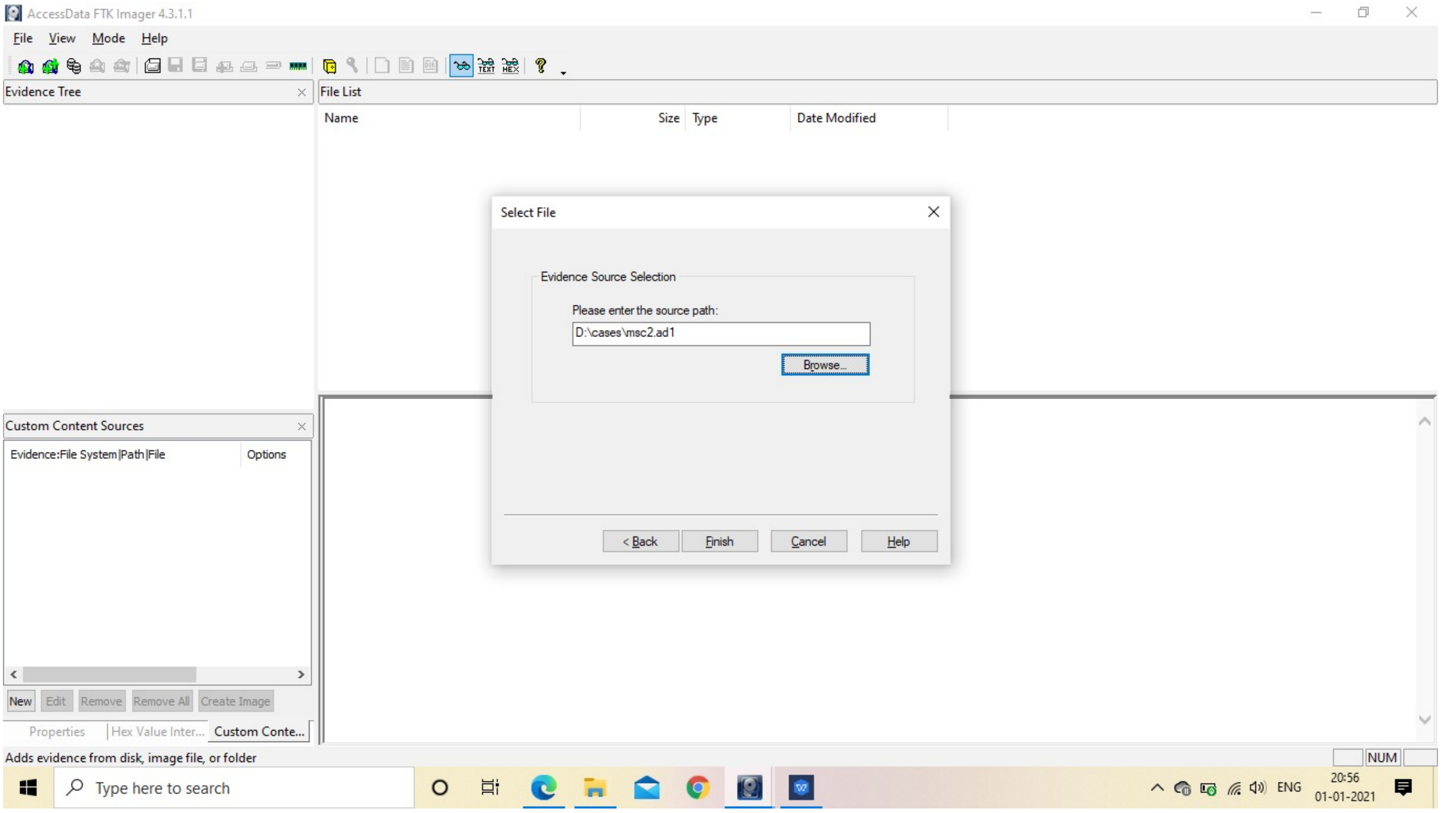
Select any one file and click on Open and Finish



Name	Date modified	Type
msc2.ad1	01-01-2021 20:30	AD1 File
msc2.ad1	01-01-2021 20:30	Text Document

File name: msc2.ad1

All Files

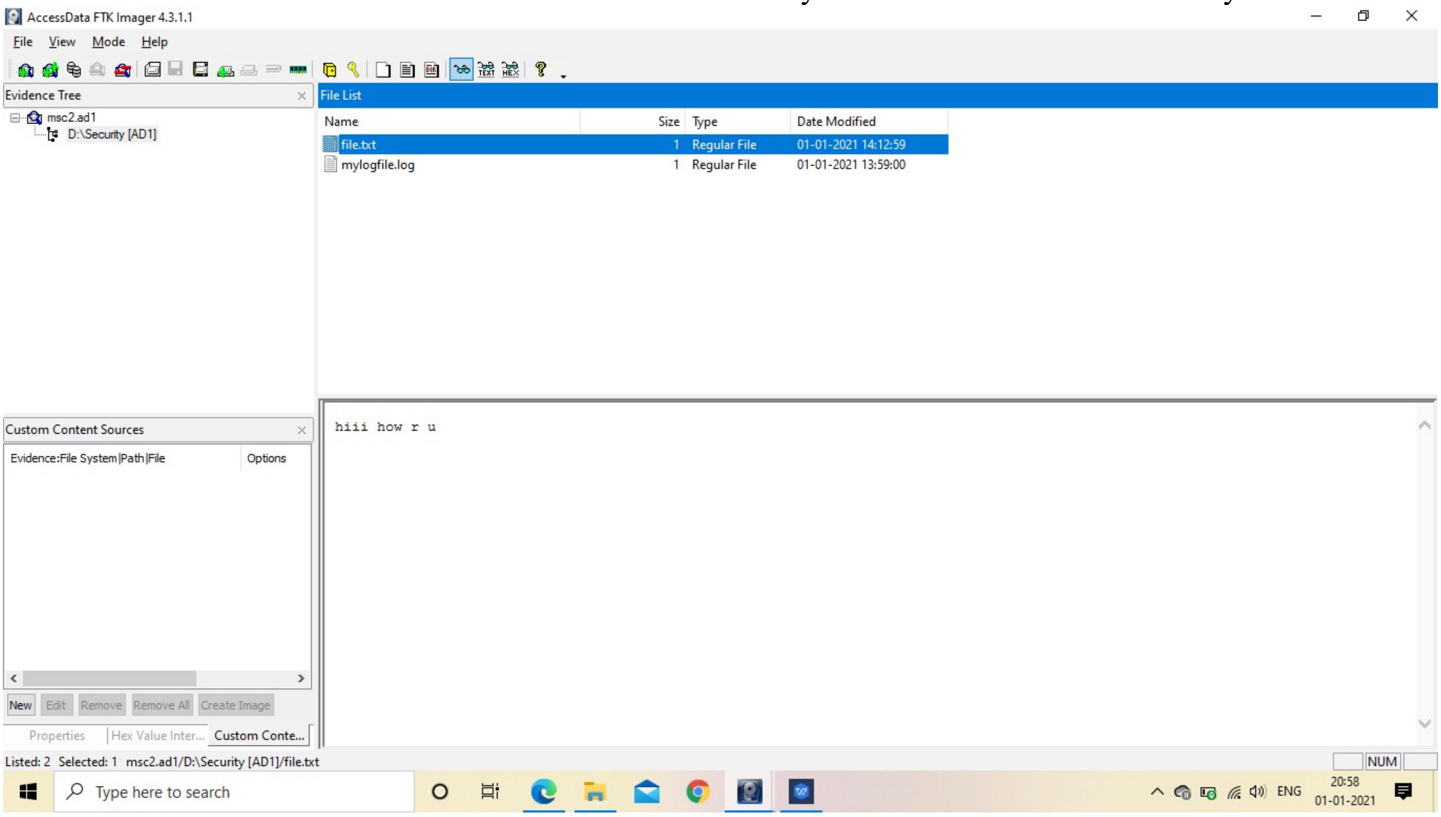


Evidence Source Selection

Please enter the source path:

D:\cases\msc2.ad1

In the Evidence Tree we will see that the tree with the directory has bee created and click on any one file.



Name	Size	Type	Date Modified
file.txt	1	Regular File	01-01-2021 14:12:59
mylogfile.log	1	Regular File	01-01-2021 13:59:00

```
hiii how r u
```

Listed: 2 Selected: 1 msc2.ad1/D:\Security [AD1]/file.txt