Group 2 Assignment: Disk Imaging and file recovery.

This assignment was completed by 3 participants namely:

1. **Fumnanya Divine Chukwuma**
2. **Apena Dare David**
3. **Maxwell Malon**

For this assignment, we were tasked to learn hands-on digital evidence collection techniques and to be able to accomplish that we utilized an FTK Imager tool and an Autopsy tool.

FTK Imager:

This is a forensic imaging tool made by AccessData. It creates forensic images and it is used to capture either a bit-for bit copy of a disk or even just a partition for analysis. It's a proper way for analysis to avoid analysing a live disk.

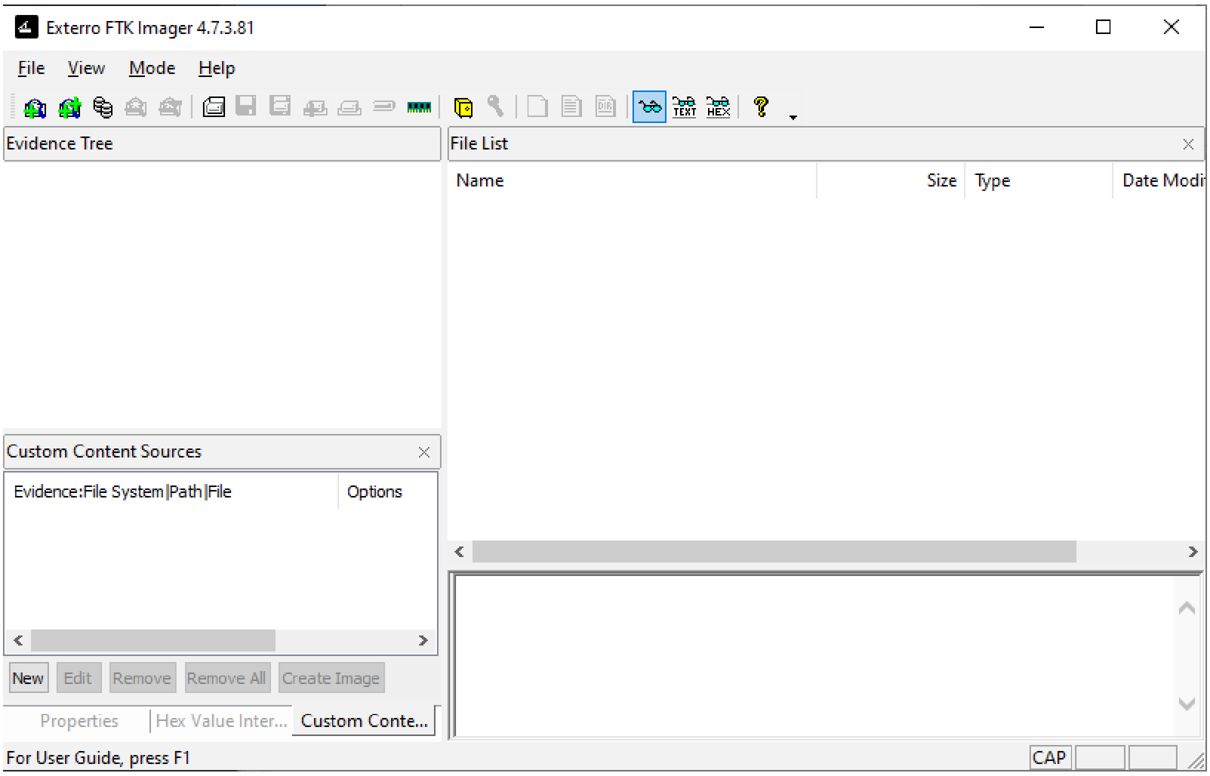
Autopsy:

This is an open-source digital forensics platform and it is used for analysis and recovery.

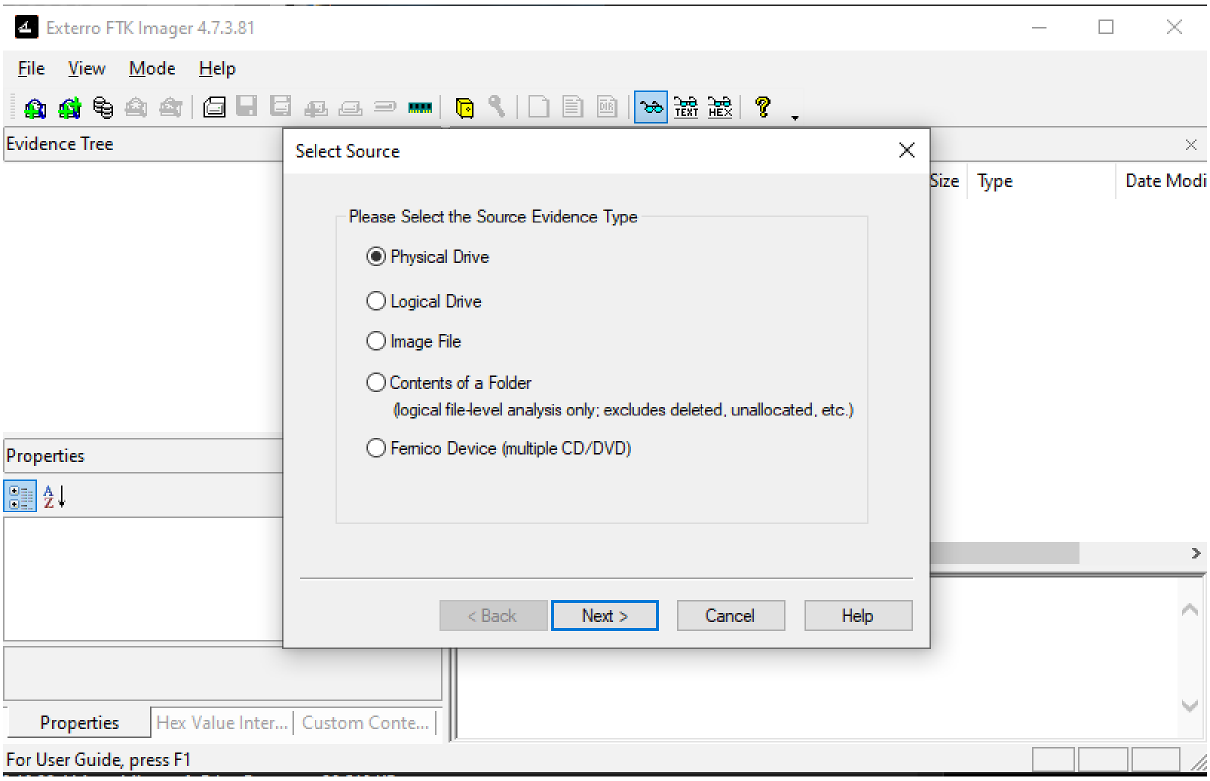
For FTK Imager:

Creating a forensic image:

A live logical image was done and no write-blocker was available.



We will be using the Physical drive source evidence type because it would image the contents of the physical drive that has been attached to this forensic workspace (this device). Other source evidence types are available for use and differ in speed as regards to the imaging process.



Select Source

Please Select the Source Evidence Type

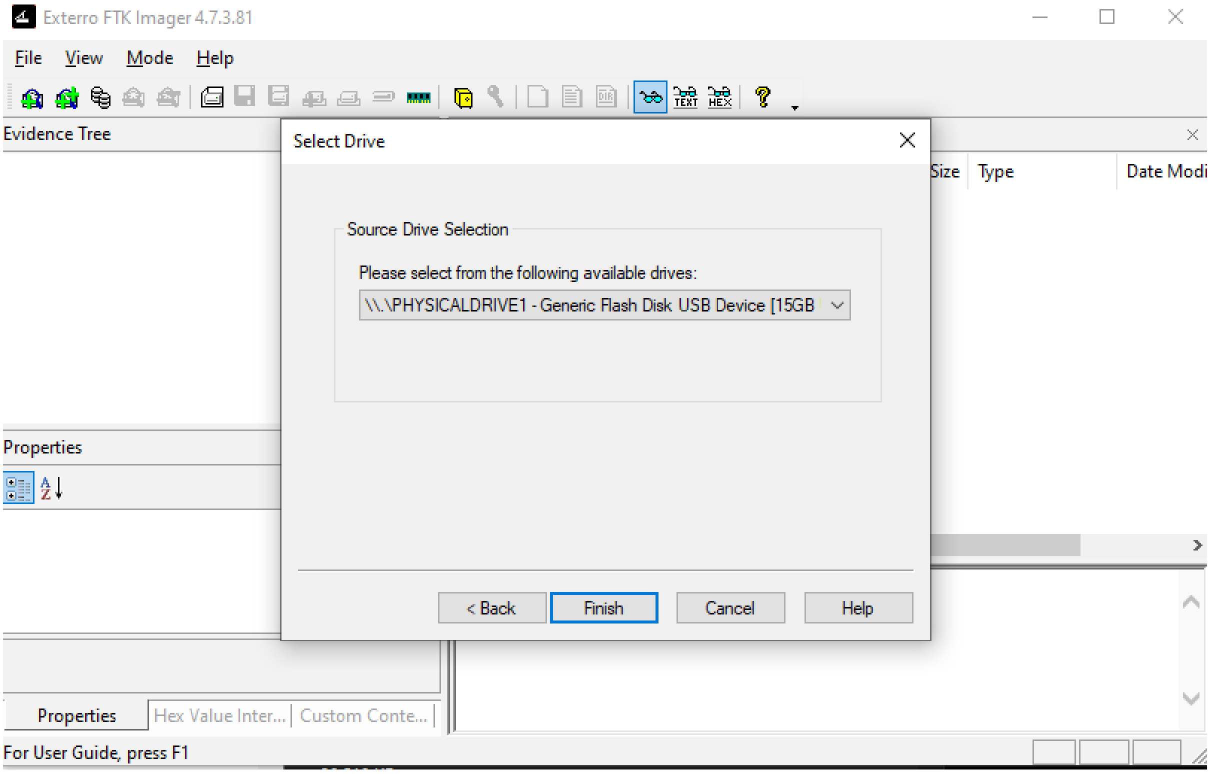
● Physical Drive

○ Logical Drive

○ Image File

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

○ Femico Device (multiple CD/DVD)

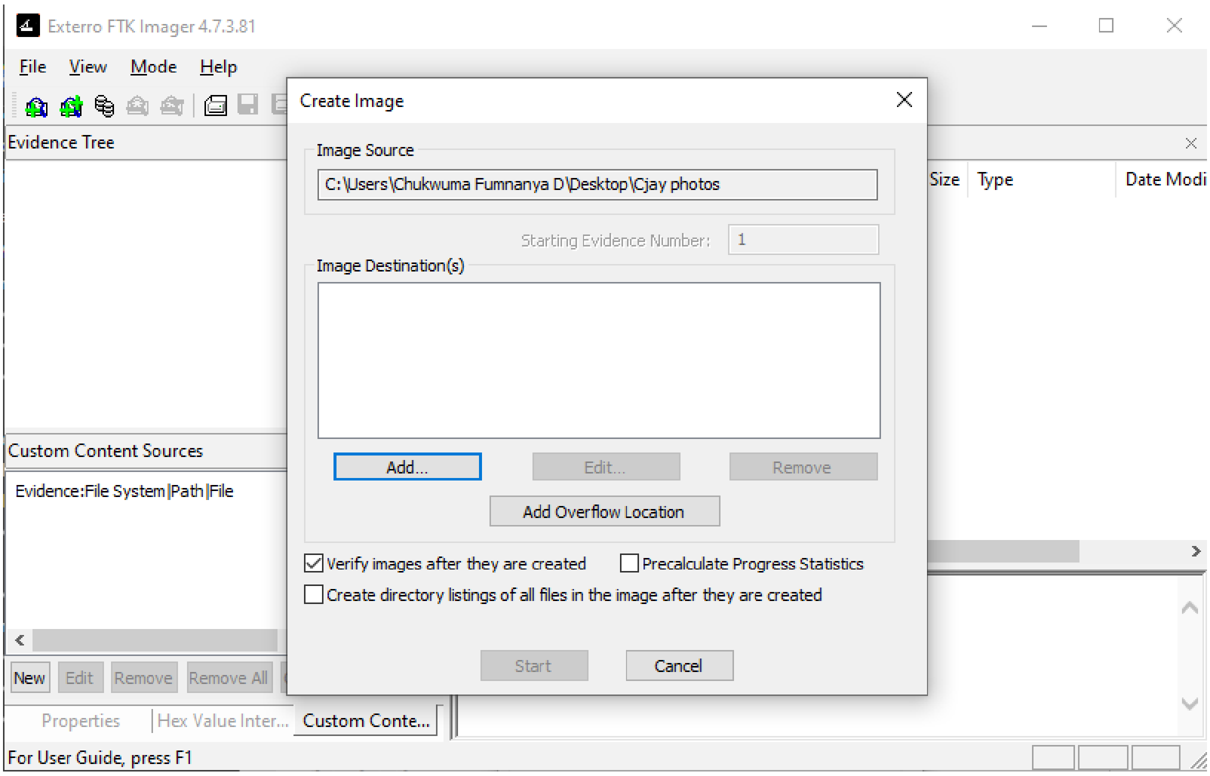


Select Drive

Source Drive Selection

Please select from the following available drives:

\\.\PHYSICALDRIVE1 - Generic Flash Disk USB Device [15GB



Create Image

Image Source

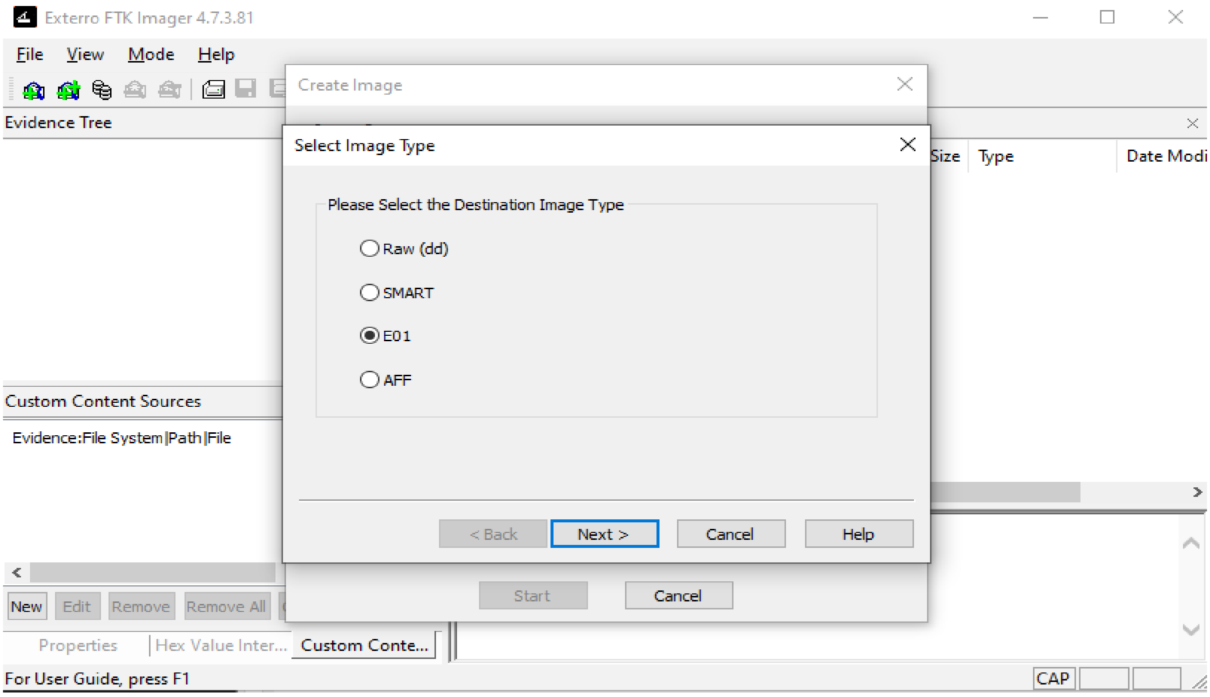
C:\Users\Chukwuma Fumnanya D\Desktop\Cjay photos

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



Select Image Type

Please Select the Destination Image Type

○ Raw (dd)

○ SMART

● E01

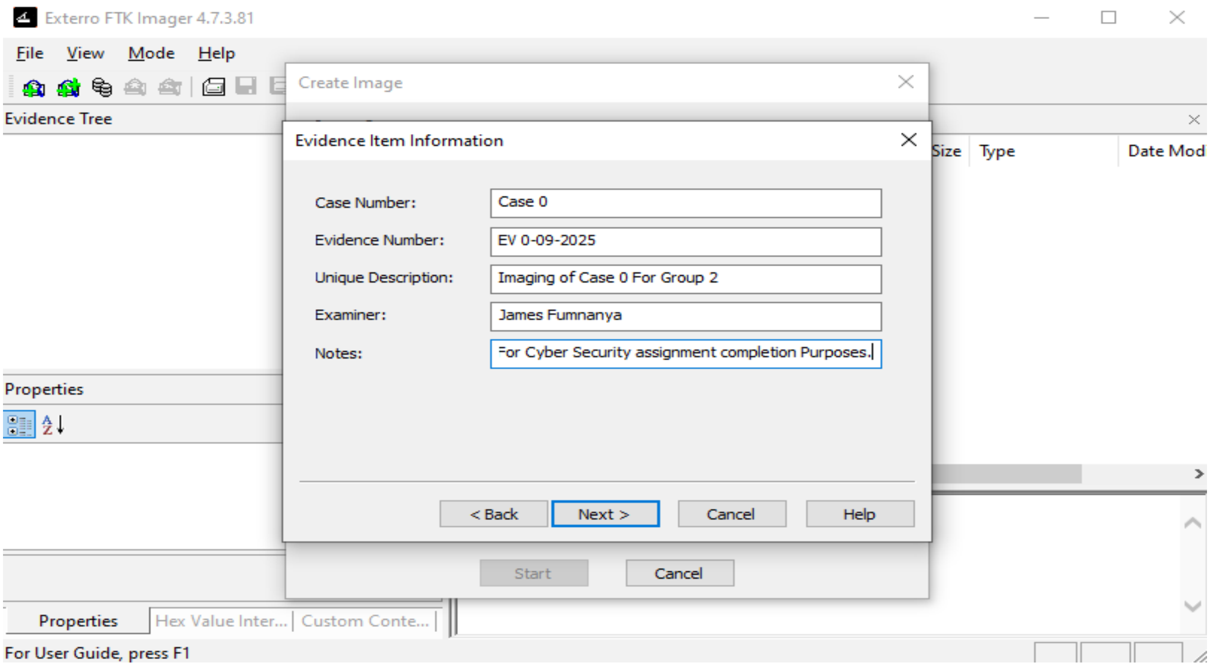
○ AFF

Common choices of image types are:

- Raw (dd): This is raw bit-for-bit. It is a very simple image type and it is widely compatible.
- E01 (Expert witness): This supports compression and metadata, it is often used in forensics.

We will utilize “Raw.dd” for this assignment.

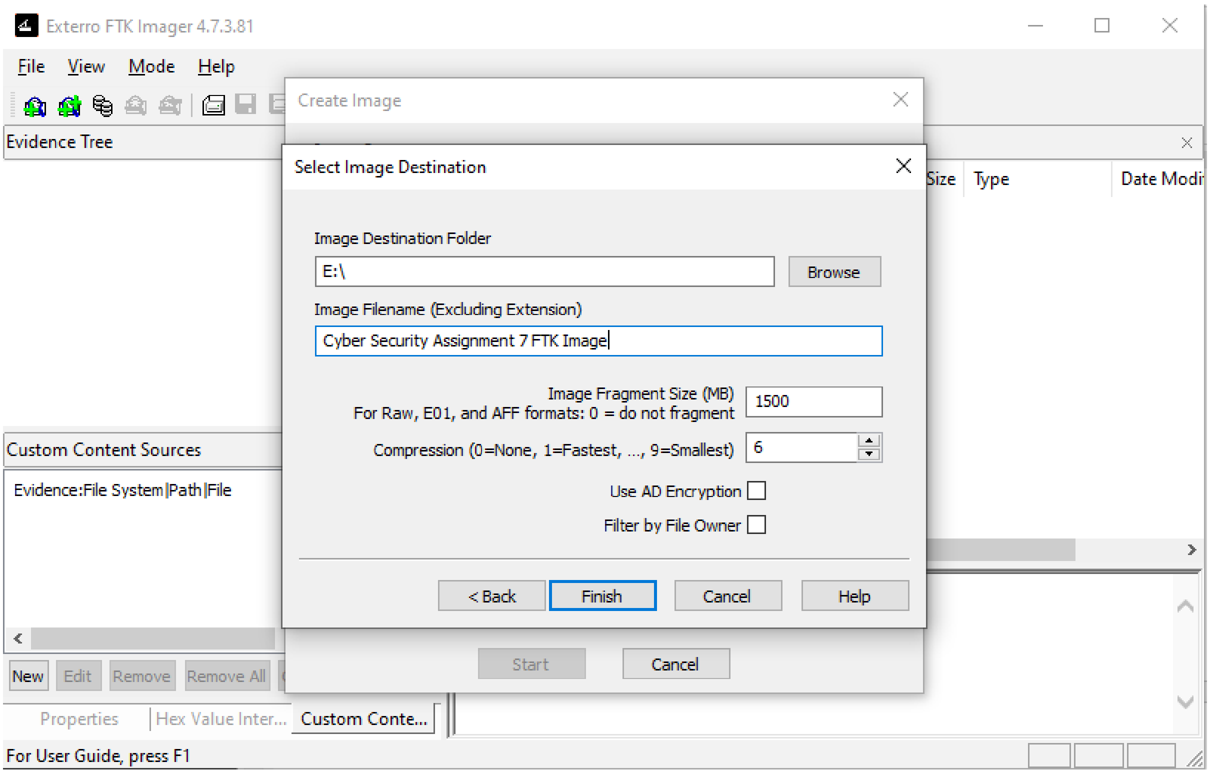
This is where we name our evidence item for easy identification.



Evidence Item Information

Case Number:	Case 0
Evidence Number:	EV 0-09-2025
Unique Description:	Imaging of Case 0 For Group 2
Examiner:	James Fumnanya
Notes:	=or Cyber Security assignment completion Purposes.

And this is where we choose destination folder and set the image filename (also important for easy identification).


Exterro FTK Imager 4.7.3.81
File View Mode Help
Evidence Tree
Create Image
Size Type Date Modi
Custom Content Sources
Evidence:File System|Path|File
New Edit Remove Remove All
Properties Hex Value Inter... Custom Conte...
For User Guide, press F1
Start Cancel

Select Image Destination

Image Destination Folder: E:\

Image Filename (Excluding Extension): Cyber Security Assignment 7 FTK Image

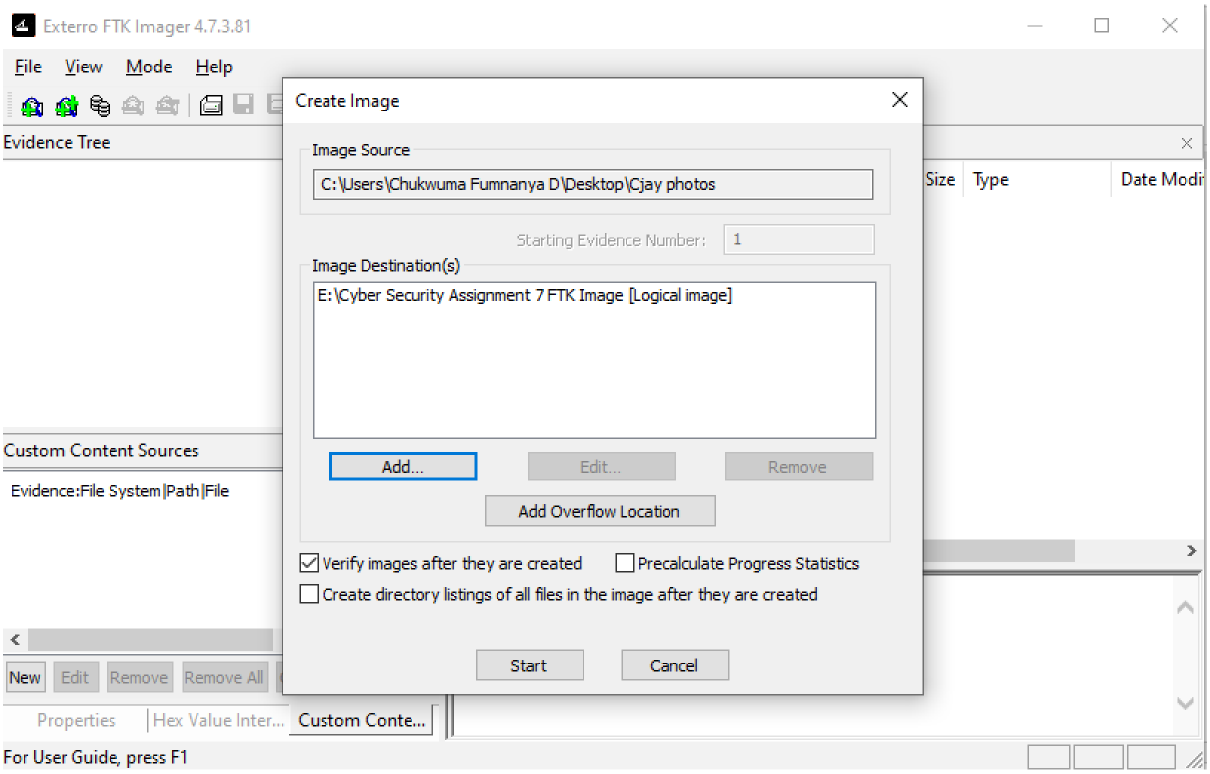
Image Fragment Size (MB): 1500
For Raw, E01, and AFF formats: 0 = do not fragment

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

Use AD Encryption □

Filter by File Owner □

After setting all these permissions and parameters, we can now start the FTK image creation.


Exterro FTK Imager 4.7.3.81
File View Mode Help
Evidence Tree
Size Type Date Modi
Custom Content Sources
Evidence:File System|Path|File
New Edit Remove Remove All
Properties Hex Value Inter... Custom Conte...
For User Guide, press F1

Create Image

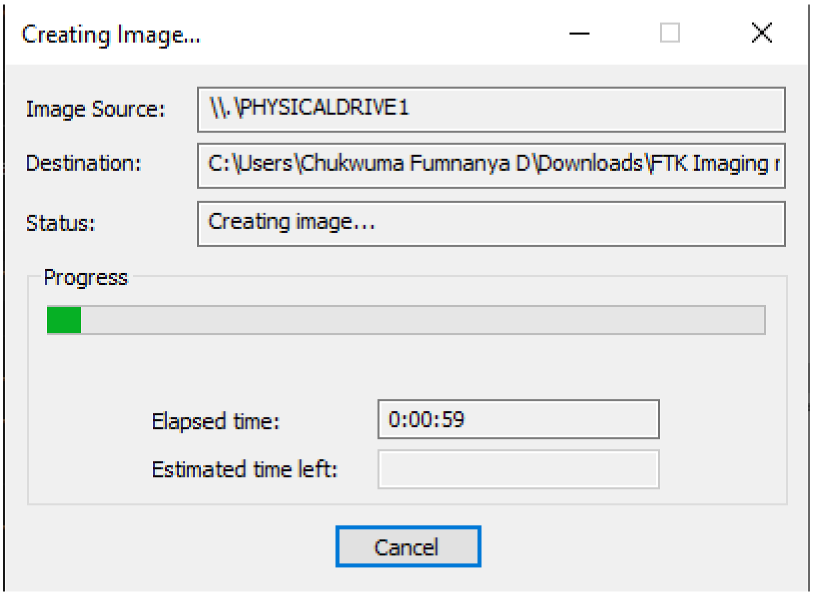
Image Source: C:\Users\Chukwuma Fumnanya D\Desktop\Cjay photos

Starting Evidence Number: 1

Image Destination(s): E:\Cyber Security Assignment 7 FTK Image [Logical image]

☑ Verify images after they are created □ Precalculate Progress Statistics

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



Creating Image...

Image Source: \\.\PHYSICALDRIVE1

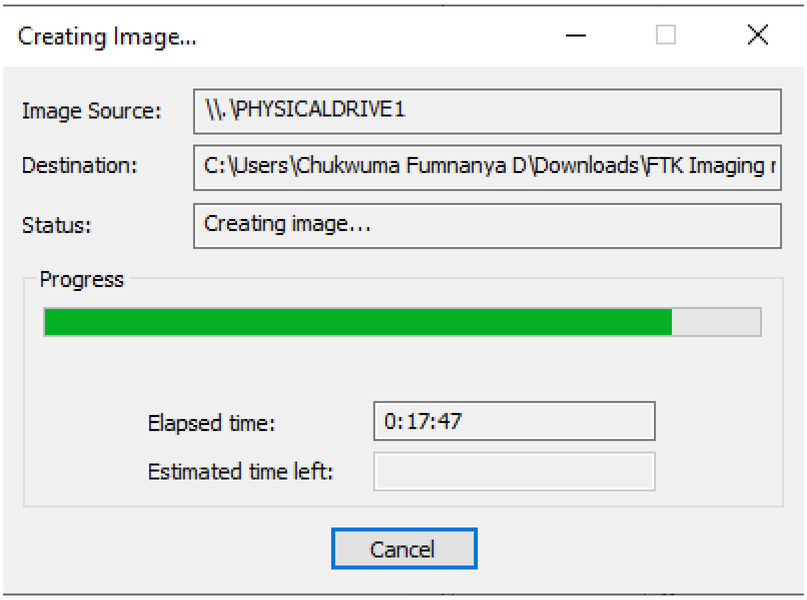
Destination: C:\Users\Chukwuma Fumnanya D\Downloads\FTK Imaging r

Status: Creating image...

Progress

Elapsed time: 0:00:59

Estimated time left:



Creating Image...

Image Source: \\.\PHYSICALDRIVE1

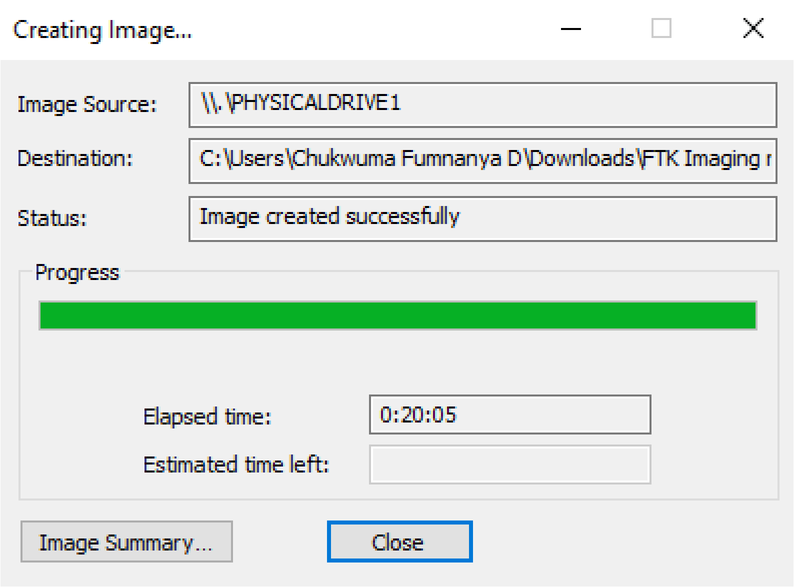
Destination: C:\Users\Chukwuma Fumnanya D\Downloads\FTK Imaging r

Status: Creating image...

Progress

Elapsed time: 0:17:47

Estimated time left:



Creating Image...

Image Source: \\.\PHYSICALDRIVE1

Destination: C:\Users\Chukwuma Fumnanya D\Downloads\FTK Imaging r

Status: Image created successfully

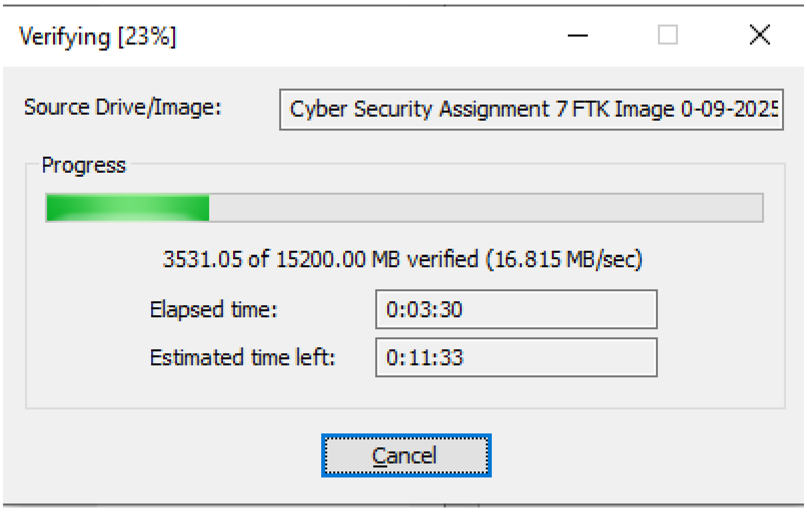
Progress

Elapsed time: 0:20:05

Estimated time left:

Elapsed time of image creation is estimated at 20 mins and 5 Seconds.

This process is the verification process of the image created so as to generate the hashes used.



Verifying [23%]

Source Drive/Image: Cyber Security Assignment 7 FTK Image 0-09-2025

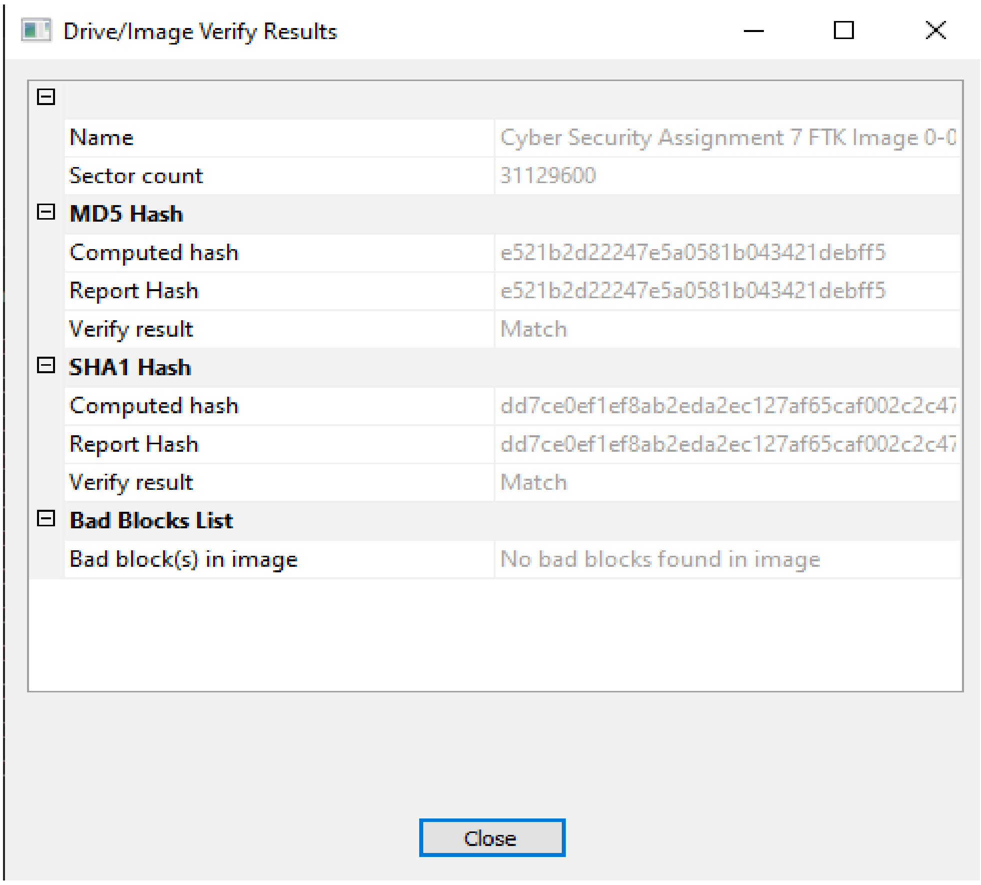
Progress

3531.05 of 15200.00 MB verified (16.815 MB/sec)

Elapsed time: 0:03:30

Estimated time left: 0:11:33

As we can see, the computed hashes have been generated successfully and we can see that they are no errors or bad blocks found in the image.



Drive/Image Verify Results

Name	Cyber Security Assignment 7 FTK Image 0-0
Sector count	31129600
MD5 Hash	
Computed hash	e521b2d22247e5a0581b043421debff5
Report Hash	e521b2d22247e5a0581b043421debff5
Verify result	Match
SHA1 Hash	
Computed hash	dd7ce0ef1ef8ab2eda2ec127af65caf002c2c47
Report Hash	dd7ce0ef1ef8ab2eda2ec127af65caf002c2c47
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

This is the text document also generated after the FTK image creation was complete. This text document entails all information as regards the image creation like the type of device imaged (In this case a USB drive), date and time of creation down to the entire time the FTK imager used to create the image and many more.

Creation Report:

```
Created By Exterro® FTK® Imager 4.7.3.81


Case Information:
Acquired using: ADI4.7.3.81
Case Number: Case 0
Evidence Number: EV 0-09-2025
Unique description: Imaging of Case 0 For Group 2
Examiner: James Fumnanya
Notes: For Cyber Security assignment completion Purposes.


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


Information for C:\Users\Chukwuma Fumnanya D\Downloads\FTK Imaging
results\Cyber Security Assignment 7 FTK Image 0-09-2025:


Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 1,937
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 31,129,600
[Physical Drive Information]
 Drive Model: Generic Flash Disk USB Device
 Drive Serial Number: ————————————C
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 15200 MB
 Sector count:    31129600
[Computed Hashes]
 MD5 checksum:    e521b2d22247e5a0581b043421debff5
 SHA1 checksum:   dd7ce0ef1ef8ab2eda2ec127af65caf002c2c472

Image Information:
 Acquisition started:   Wed Sep 17 01:17:15 2025
 Acquisition finished:  Wed Sep 17 01:37:20 2025
 Segment list:
  C:\Users\Chukwuma Fumnanya D\Downloads\FTK Imaging results\Cyber Security Assignment 7 FTK Image 0-09-2025.001
  C:\Users\Chukwuma Fumnanya D\Downloads\FTK Imaging results\Cyber Security Assignment 7 FTK Image 0-09-2025.002
  C:\Users\Chukwuma Fumnanya D\Downloads\FTK Imaging results\Cyber Security Assignment 7 FTK Image 0-09-2025.003
  C:\Users\Chukwuma Fumnanya D\Downloads\FTK Imaging results\Cyber Security Assignment 7 FTK Image 0-09-2025.004
  C:\Users\Chukwuma Fumnanya D\Downloads\FTK Imaging results\Cyber Security Assignment 7 FTK Image 0-09-2025.005
```

C:\Users\Chukwuma Fumnanya D\Downloads\FTK Imaging results\Cyber Security Assignment 7 FTK Image 0-09-2025.006

C:\Users\Chukwuma Fumnanya D\Downloads\FTK Imaging results\Cyber Security Assignment 7 FTK Image 0-09-2025.007

C:\Users\Chukwuma Fumnanya D\Downloads\FTK Imaging results\Cyber Security Assignment 7 FTK Image 0-09-2025.008

C:\Users\Chukwuma Fumnanya D\Downloads\FTK Imaging results\Cyber Security Assignment 7 FTK Image 0-09-2025.009

C:\Users\Chukwuma Fumnanya D\Downloads\FTK Imaging results\Cyber Security Assignment 7 FTK Image 0-09-2025.010

C:\Users\Chukwuma Fumnanya D\Downloads\FTK Imaging results\Cyber Security Assignment 7 FTK Image 0-09-2025.011

COMPUTED HASH : e521b2d22247e5a0581b043421debff5

COMPUTED HASH : dd7ce0ef1ef8ab2eda2ec127af65caf002c2c472

Image Verification Results:

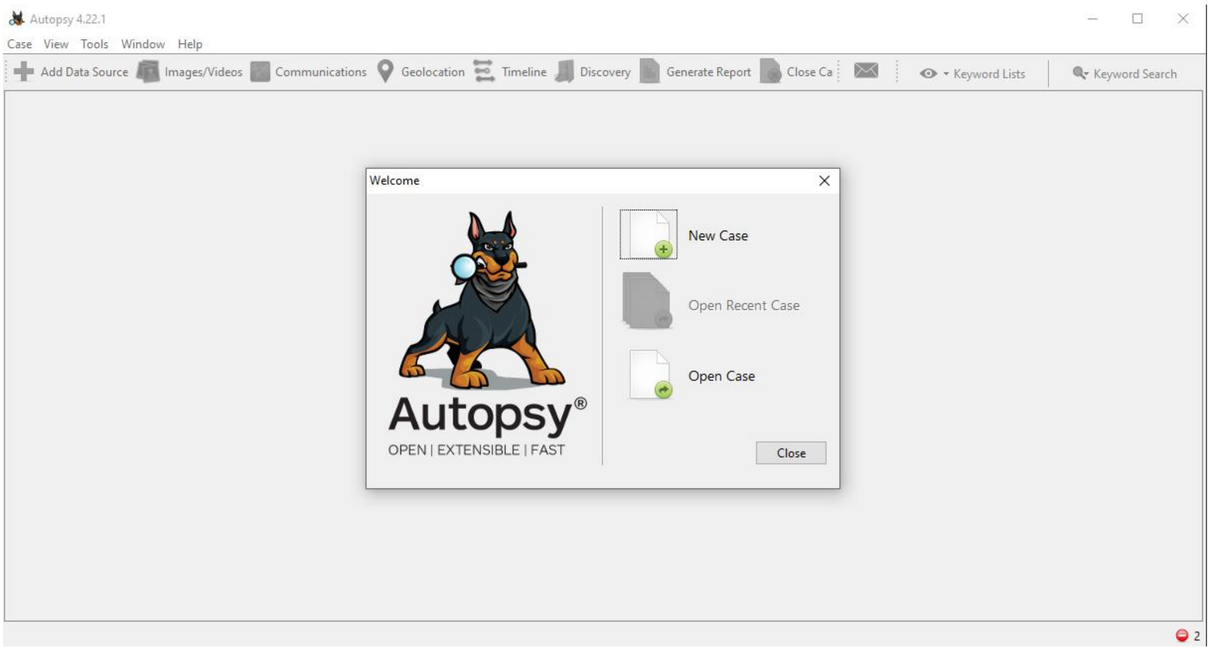
Verification started: Wed Sep 17 01:37:32 2025

Verification finished: Wed Sep 17 01:46:32 2025

MD5 checksum: e521b2d22247e5a0581b043421debff5 : verified

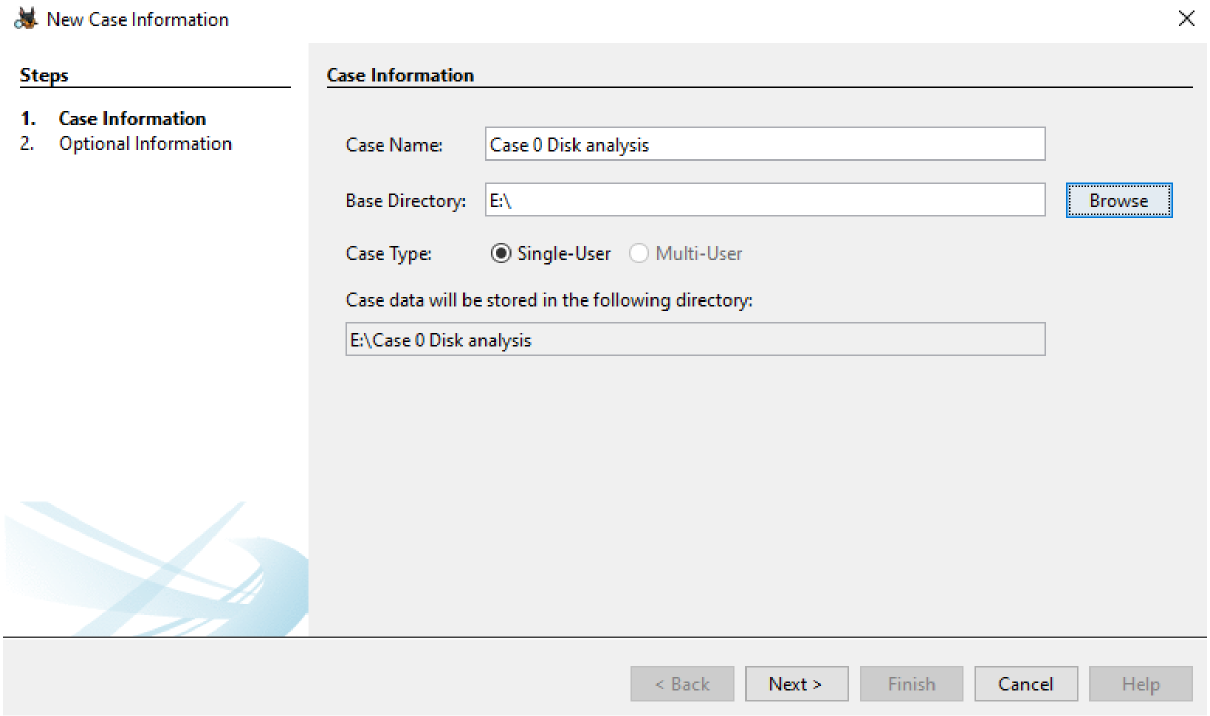
SHA1 checksum: dd7ce0ef1ef8ab2eda2ec127af65caf002c2c472 : verified

For Autopsy:



This is the UI of the open source Autopsy software.

To begin the process of investigation we have to create a "New case" and as usual set the case name and the base directory. Please note that we created a disk image of the external drive into our forensic environment/device so therefore to avoid complications of the process during our investigation/autopsy we will need to move the results of this investigation outside this forensic environment (moving it out of the same drive where investigation is being conducted).



New Case Information

Steps

1. **Case Information**
2. Optional Information

Case Information

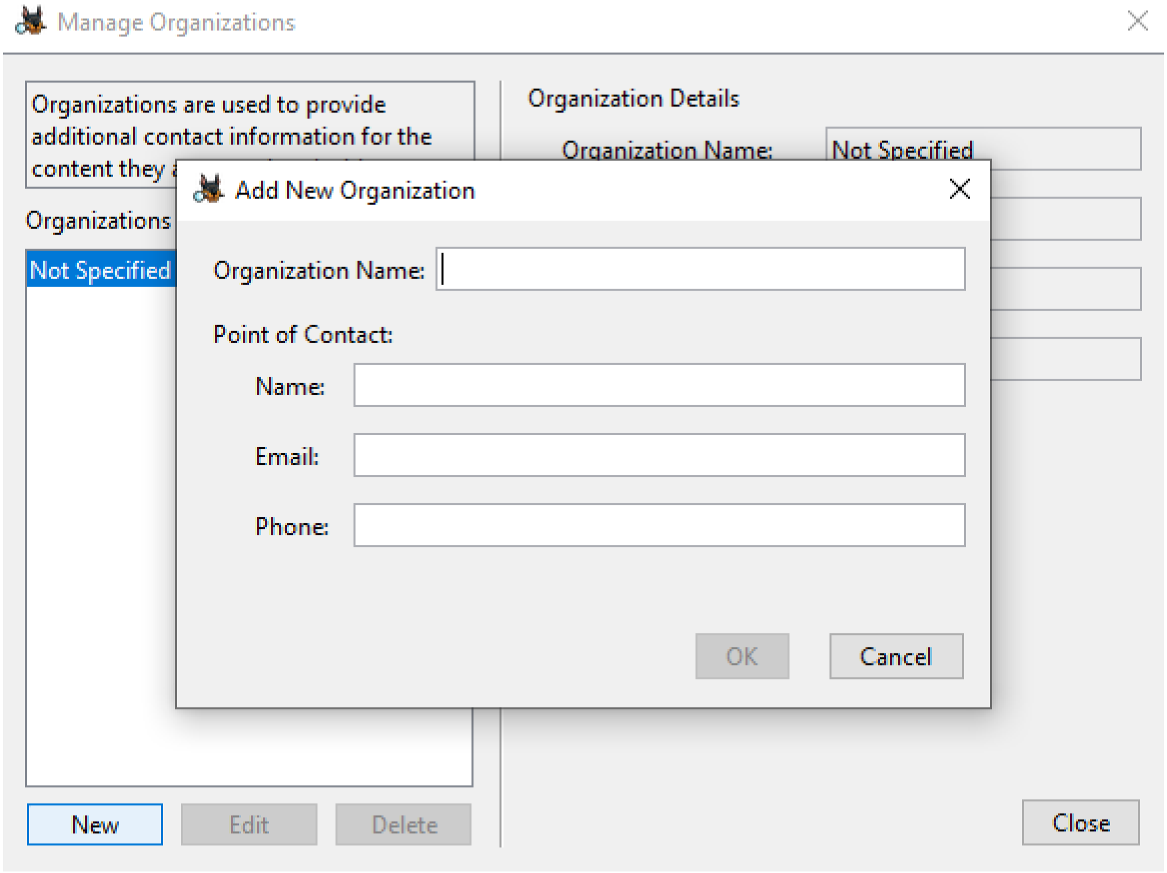
Case Name: Case 0 Disk analysis

Base Directory: E:\

Case Type: ● Single-User ○ Multi-User

Case data will be stored in the following directory:

E:\Case 0 Disk analysis



Manage Organizations

Organizations are used to provide additional contact information for the content they a

Organizations

Not Specified

Organization Details

Organization Name: Not Specified

Add New Organization

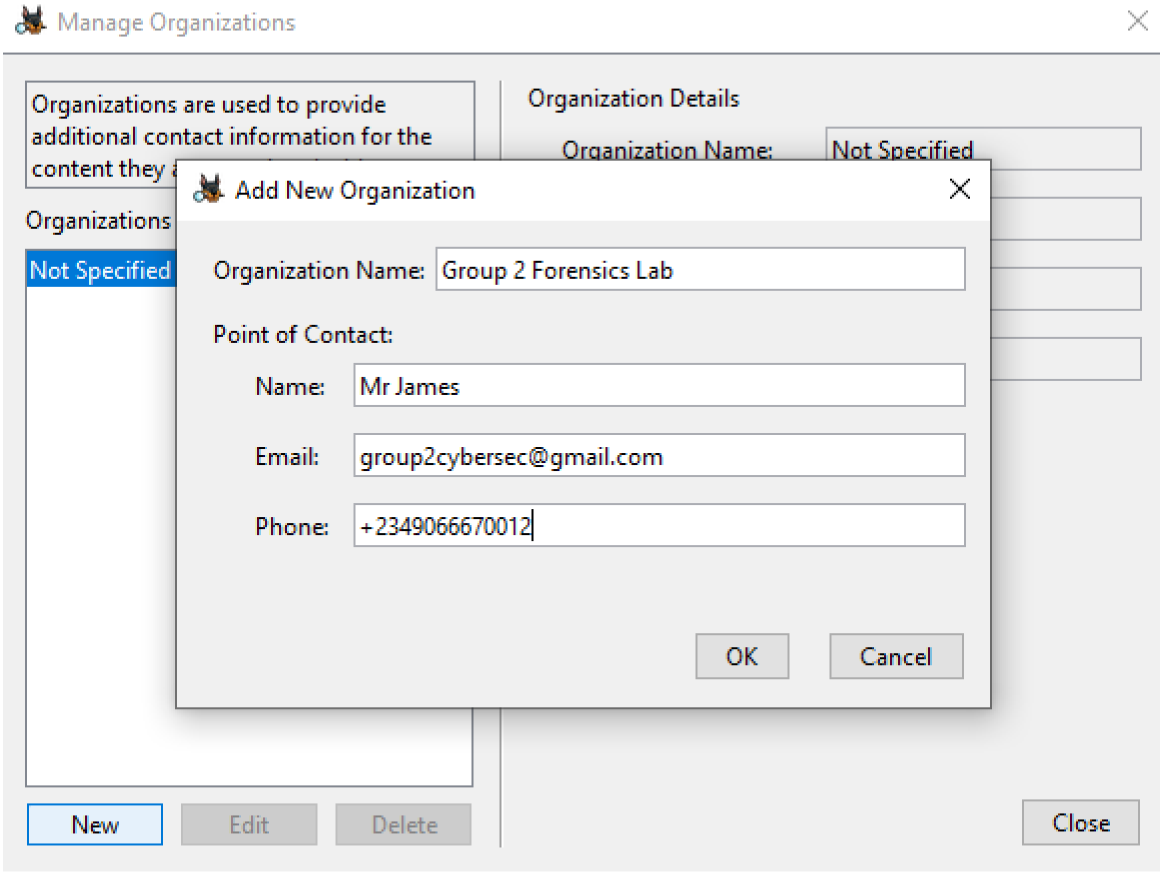
Organization Name:

Point of Contact:

Name:

Email:

Phone:



Manage Organizations

Organizations are used to provide additional contact information for the content they a

Organizations

Not Specified

Organization Details

Organization Name: Not Specified

Add New Organization

Organization Name: Group 2 Forensics Lab

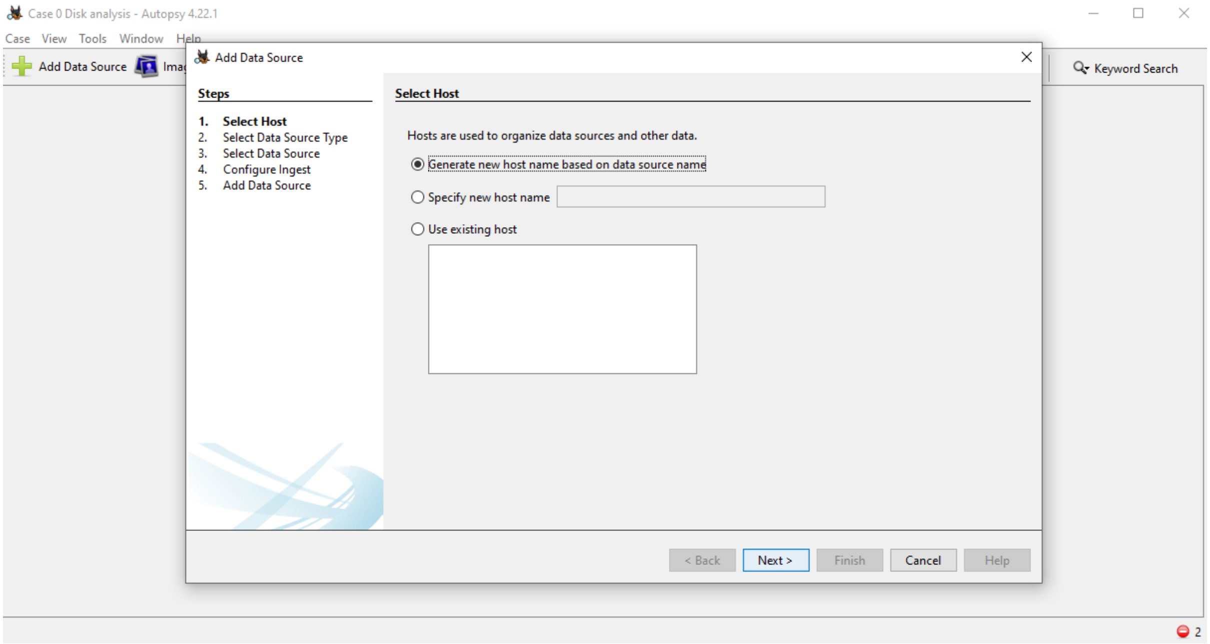
Point of Contact:

Name: Mr James

Email: group2cybersec@gmail.com

Phone: +2349066670012

We could also fill the forms provided for identification purposes and accountability.



Case 0 Disk analysis - Autopsy 4.22.1

Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Host

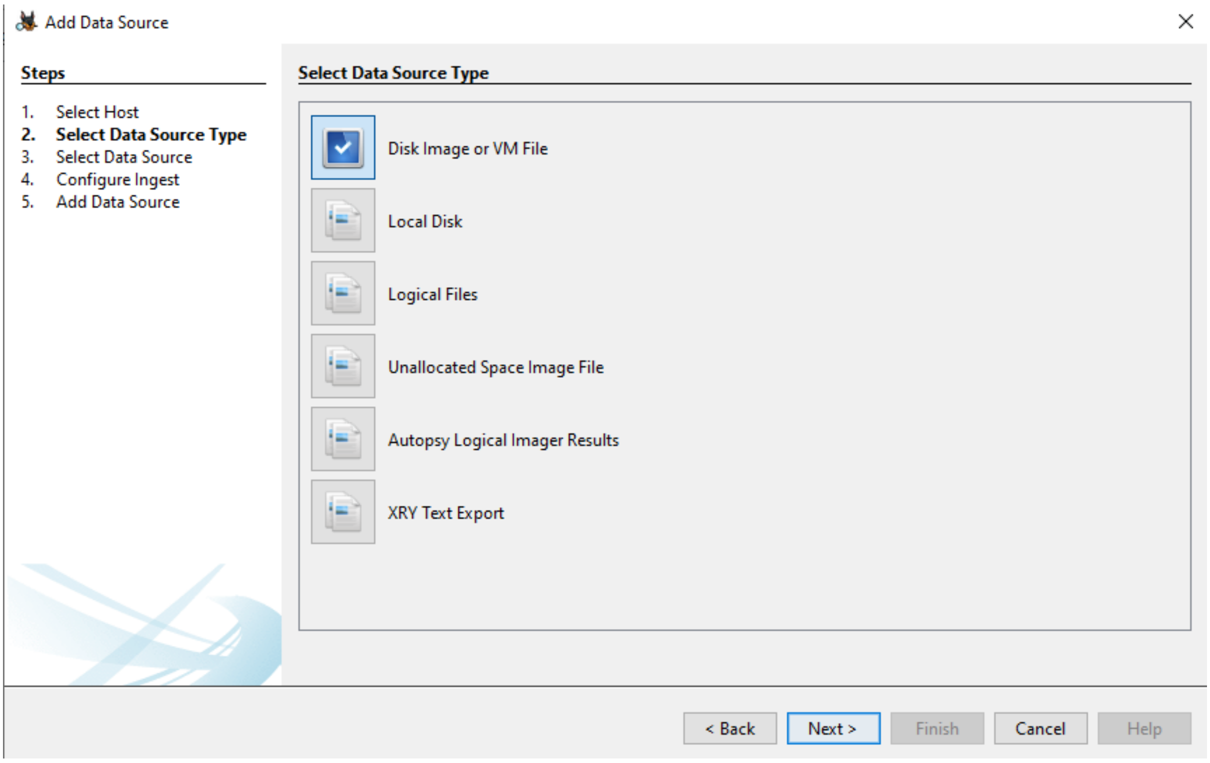
Hosts are used to organize data sources and other data.

● Generate new host name based on data source name

○ Specify new host name

○ Use existing host

Now we create a “new host” and hostname because we are first time users of the software.


Add Data Source

Steps

1. Select Host
2. **Select Data Source Type**
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Data Source Type

☑ Disk Image or VM File

Local Disk

Logical Files

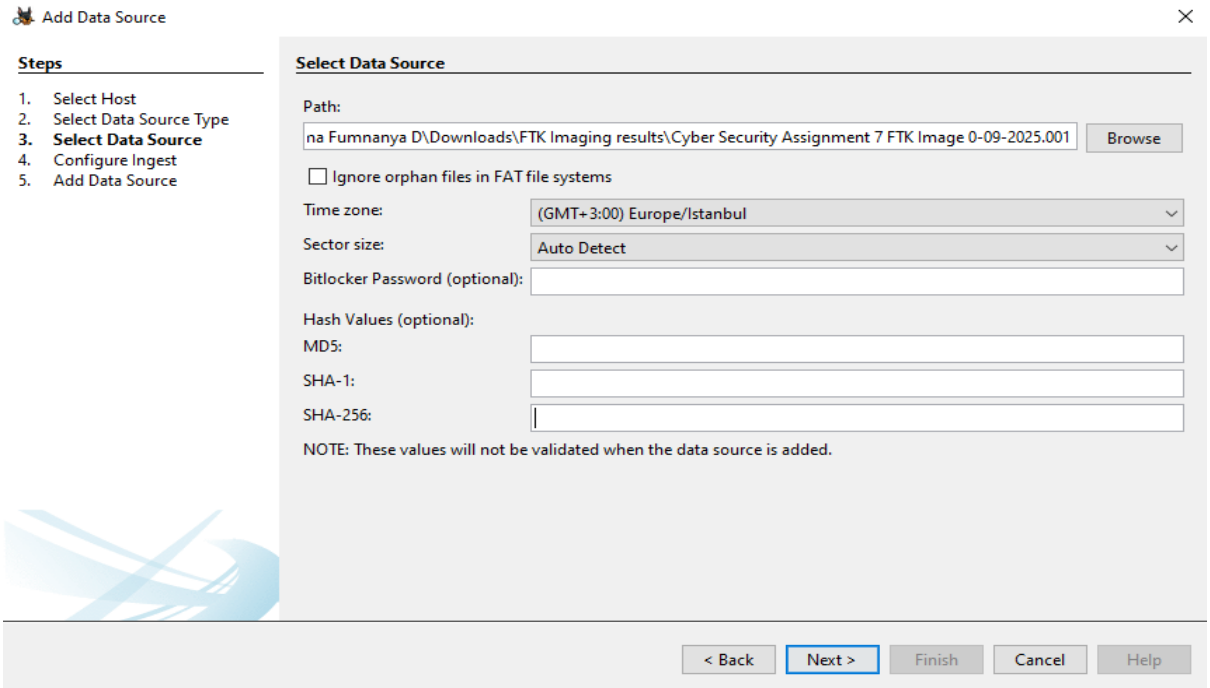
Unallocated Space Image File

Autopsy Logical Imager Results

XRY Text Export

Thereafter, we look for our FTK image file where we have our image that requires investigation. We do that by clicking on “Disk image or VM file” and click “Next” which would take us to the next page.

This is the next page and we have to select the file path using the “Browse” option and select the FTK image file. Thereafter, it would select the sector size and will give us the hash information (for accountability).


Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. **Select Data Source**
4. Configure Ingest
5. Add Data Source

Select Data Source

Path: na Fumnanya D\Downloads\FTK Imaging results\Cyber Security Assignment 7 FTK Image 0-09-2025.001

□ Ignore orphan files in FAT file systems

Time zone: (GMT+3:00) Europe/Istanbul

Sector size: Auto Detect

Bitlocker Password (optional):

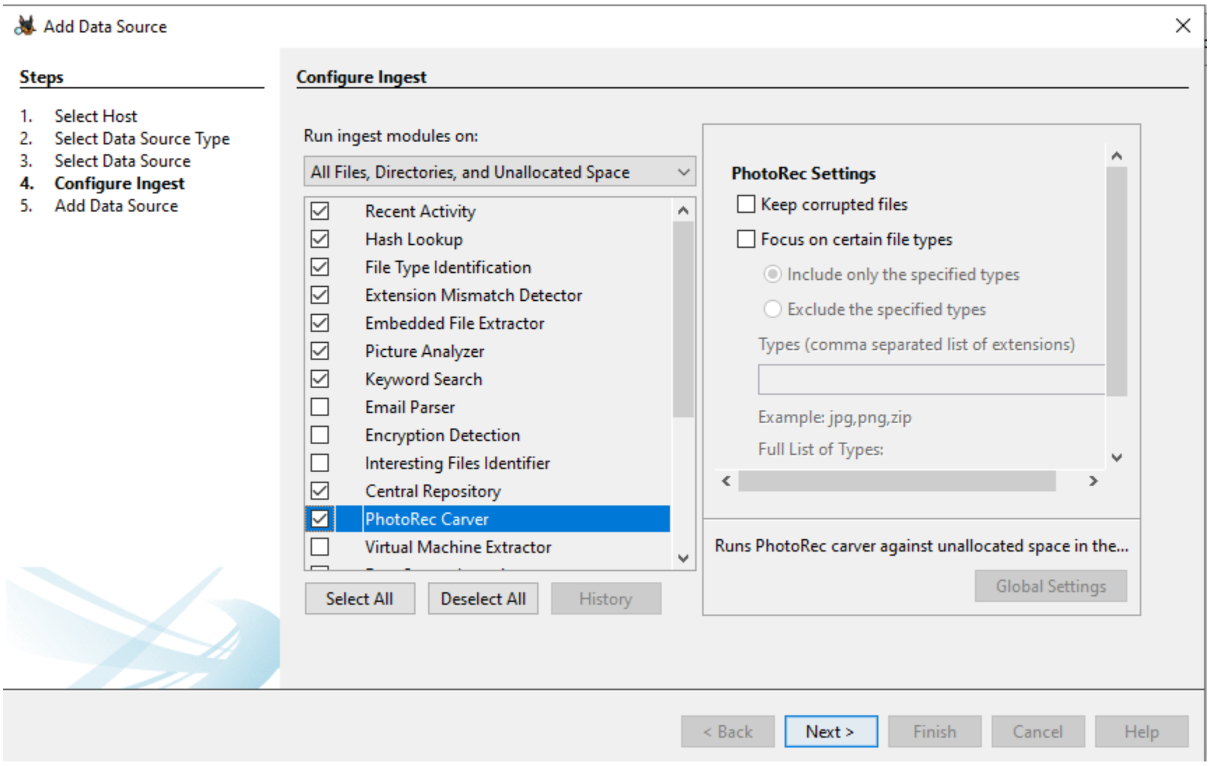
Hash Values (optional):

MD5:

SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.



1. Select Host
2. Select Data Source Type
3. Select Data Source
4. **Configure Ingest**
5. Add Data Source

Configure Ingest

Run ingest modules on: All Files, Directories, and Unallocated Space

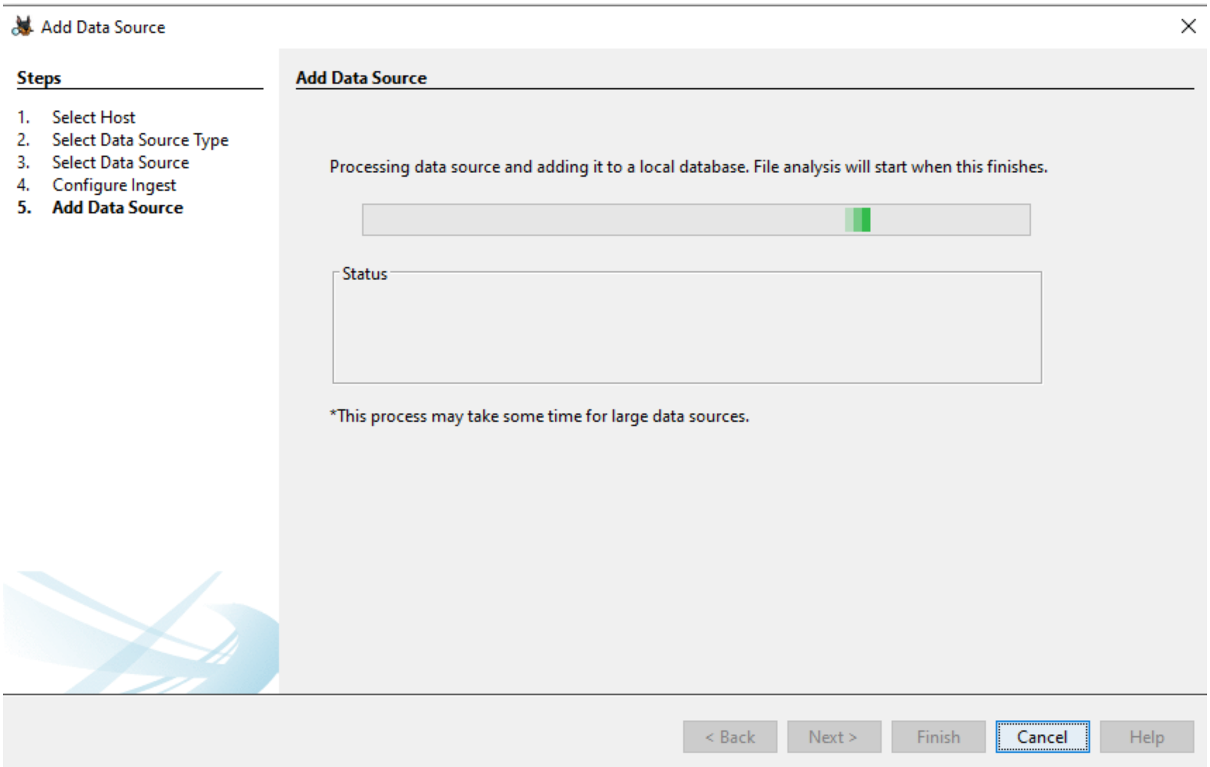
☑ Recent Activity
☑ Hash Lookup
☑ File Type Identification
☑ Extension Mismatch Detector
☑ Embedded File Extractor
☑ Picture Analyzer
☑ Keyword Search
☐ Email Parser
☐ Encryption Detection
☐ Interesting Files Identifier
☑ Central Repository
☑ PhotoRec Carver
☐ Virtual Machine Extractor

PhotoRec Settings

☐ Keep corrupted files
☐ Focus on certain file types
● Include only the specified types
○ Exclude the specified types
Types (comma separated list of extensions)
Example: jpg,png,zip
Full List of Types:

Runs PhotoRec carver against unallocated space in the...

This is the stage of “Ingest” where autopsy uses investigation filters to generate results concerning a particular image that is being investigated. Marking more filters means more time and items for autopsy to generate results but for this assignment, we will only use the File type identification, PhotoRec Carver, EXI, Hash lookup, Picture Analyzer, Keyword search, Recent Activity and others as marked in the screenshot and then click “Next”.



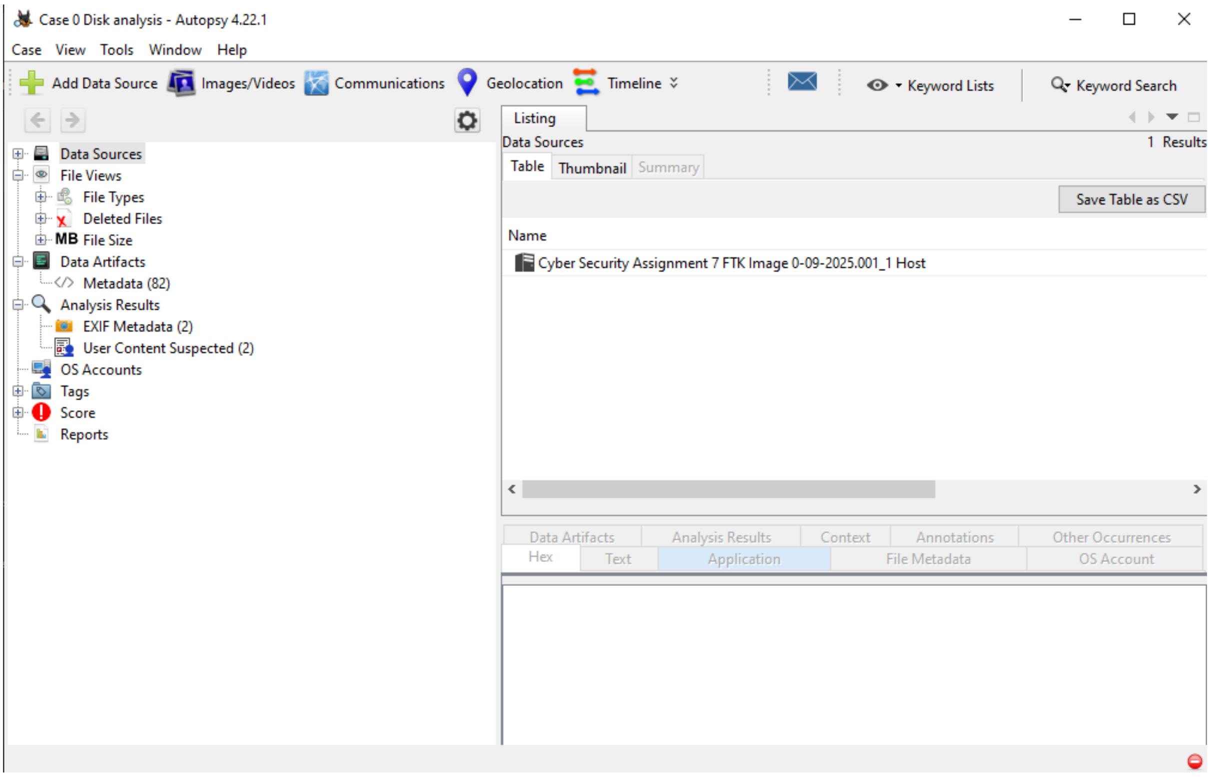
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. **Add Data Source**

Processing data source and adding it to a local database. File analysis will start when this finishes.

Status

*This process may take some time for large data sources.

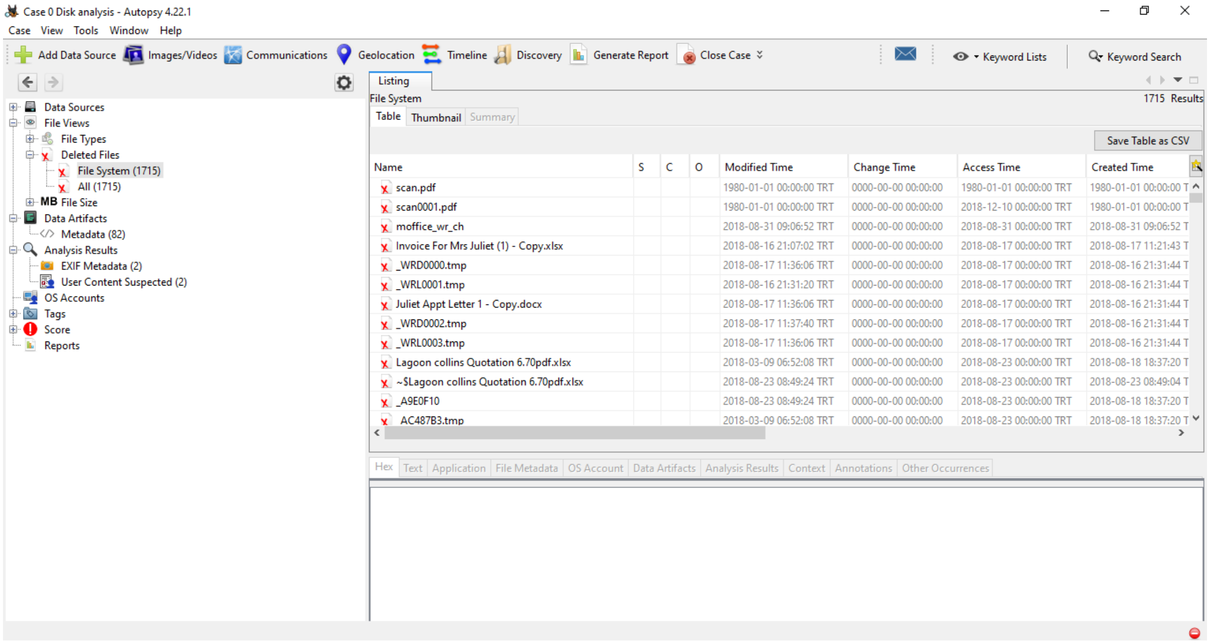
The process will take a lot of time and we need to leave it for a while so as to enable it generate all the information needed to perform the investigation.



Name
Cyber Security Assignment 7 FTK Image 0-09-2025.001_1 Host

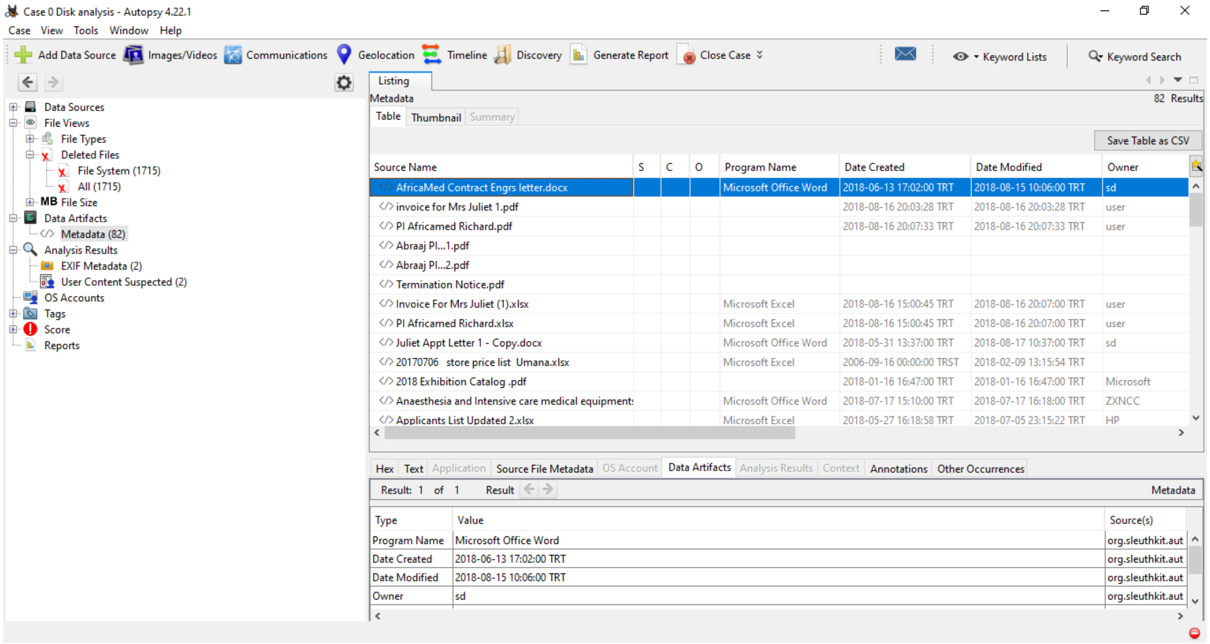
This page is displayed once Autopsy is done generating all the items for investigation. Now you can click them one by one to commence your investigation.

If we decide to check the files that have been deleted previously from the device being investigated, we can see the files listed with the timestamp of their deletion, creation and modification and there is also option to recover the deleted file discovered.



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
scan.pdf				1980-01-01 00:00:00 TRT	0000-00-00 00:00:00	1980-01-01 00:00:00 TRT	1980-01-01 00:00:00 T
scan0001.pdf				1980-01-01 00:00:00 TRT	0000-00-00 00:00:00	2018-12-10 00:00:00 TRT	1980-01-01 00:00:00 T
moffice_wr_ch				2018-08-31 09:06:52 TRT	0000-00-00 00:00:00	2018-08-31 00:00:00 TRT	2018-08-31 09:06:52 T
Invoice For Mrs Juliet (1) - Copy.xlsx				2018-08-16 21:07:02 TRT	0000-00-00 00:00:00	2018-08-17 00:00:00 TRT	2018-08-17 11:21:43 T
_WRD0000.tmp				2018-08-17 11:36:06 TRT	0000-00-00 00:00:00	2018-08-17 00:00:00 TRT	2018-08-16 21:31:44 T
_WRL0001.tmp				2018-08-16 21:31:20 TRT	0000-00-00 00:00:00	2018-08-17 00:00:00 TRT	2018-08-16 21:31:44 T
Juliet Appt Letter 1 - Copy.docx				2018-08-17 11:36:06 TRT	0000-00-00 00:00:00	2018-08-17 00:00:00 TRT	2018-08-16 21:31:44 T
_WRD0002.tmp				2018-08-17 11:37:40 TRT	0000-00-00 00:00:00	2018-08-17 00:00:00 TRT	2018-08-16 21:31:44 T
_WRL0003.tmp				2018-08-17 11:36:06 TRT	0000-00-00 00:00:00	2018-08-17 00:00:00 TRT	2018-08-16 21:31:44 T
Lagoon collins Quotation 6.70pdf.xlsx				2018-03-09 06:52:08 TRT	0000-00-00 00:00:00	2018-08-23 00:00:00 TRT	2018-08-18 18:37:20 T
~$Lagoon collins Quotation 6.70pdf.xlsx				2018-08-23 08:49:24 TRT	0000-00-00 00:00:00	2018-08-23 00:00:00 TRT	2018-08-23 08:49:04 T
_A9E0F10				2018-08-23 08:49:24 TRT	0000-00-00 00:00:00	2018-08-23 00:00:00 TRT	2018-08-18 18:37:20 T
AC487B3.tmp				2018-03-09 06:52:08 TRT	0000-00-00 00:00:00	2018-08-23 00:00:00 TRT	2018-08-18 18:37:20 T

We can also decide to check the metadata generated for each file on the device undergoing forensic analysis and the metadata is very important because it shows whatever has been done to that device or with that file. And also, an investigator could also download whatever information discovered during investigation by saving it as a CSV file and can use that to create whatever investigative report he or she wanted to create.



Source Name	S	C	O	Program Name	Date Created	Date Modified	Owner
AfricaMed Contract Engrs letter.docx				Microsoft Office Word	2018-06-13 17:02:00 TRT	2018-08-15 10:06:00 TRT	sd
invoice for Mrs Juliet 1.pdf					2018-08-16 20:03:28 TRT	2018-08-16 20:03:28 TRT	user
PI Africamed Richard.pdf					2018-08-16 20:07:33 TRT	2018-08-16 20:07:33 TRT	user
Abraaj PI...1.pdf							
Abraaj PI...2.pdf							
Termination Notice.pdf							
Invoice For Mrs Juliet (1).xlsx				Microsoft Excel	2018-08-16 15:00:45 TRT	2018-08-16 20:07:00 TRT	user
PI Africamed Richard.xlsx				Microsoft Excel	2018-08-16 15:00:45 TRT	2018-08-16 20:07:00 TRT	user
Juliet Appt Letter 1 - Copy.docx				Microsoft Office Word	2018-05-31 13:37:00 TRT	2018-08-17 10:37:00 TRT	sd
20170706 store price list Umana.xlsx				Microsoft Excel	2006-09-16 00:00:00 TRST	2018-02-09 13:15:54 TRT	
2018 Exhibition Catalog .pdf					2018-01-16 16:47:00 TRT	2018-01-16 16:47:00 TRT	Microsoft
Anaesthesia and Intensive care medical equipment:				Microsoft Office Word	2018-07-17 15:10:00 TRT	2018-07-17 16:18:00 TRT	ZXNCC
Applicants List Updated 2.xlsx				Microsoft Excel	2018-05-27 16:18:58 TRT	2018-07-05 23:15:22 TRT	HP

Type	Value	Source(s)
Program Name	Microsoft Office Word	org.sleuthkit.aut
Date Created	2018-06-13 17:02:00 TRT	org.sleuthkit.aut
Date Modified	2018-08-15 10:06:00 TRT	org.sleuthkit.aut
Owner	sd	org.sleuthkit.aut

So all this and many more can be done on any device subject to investigation. All you need are these important tools.

The FTK imager for creating the image of the device in question and then Autopsy for investigative analysis.