Sanjana Asrani
D17B/01/Batch B

DF Lab 01
FTK Imager &Autopsy

AIM: Analysis of forensic images using open source tools like Autopsy and commercial tool: FTK Imager.

THEORY:

Digital forensics is the process of collecting, analyzing, and preserving electronic evidence to investigate and prevent cybercrimes. It involves the extraction and examination of digital artifacts from various devices to reconstruct and understand events.

FTK Imager:
FTK Imager is a forensic imaging tool that creates a forensic copy (image) of a storage device. It captures not only file data but also unallocated space, slack space, and file system metadata, maintaining the integrity of the original data. FTK Imager is crucial for preserving evidence without altering the original content.

Autopsy:
Autopsy is an open-source digital forensics platform used for analyzing disk images and files. It provides a user-friendly interface for investigators to examine artifacts, recover deleted data, and generate comprehensive reports. Autopsy streamlines the process of investigating digital evidence, facilitating a thorough analysis of file systems and uncovering relevant information.

Basic Digital Forensics Process:

1. Identification: Recognize and document potential sources of evidence, such as computers, storage devices, or network logs.

2. Collection: Safely gather electronic evidence, ensuring the preservation of its integrity. FTK Imager plays a vital role in creating forensic images of storage media.

3. Analysis: Utilize tools like Autopsy to examine the acquired data. This involves searching for relevant information, recovering deleted files, and identifying patterns or anomalies.

4. Documentation: Record findings in a detailed and organized manner. Generate reports that summarize the analysis, providing a clear overview of the investigation process and its results.

5. Presentation: Present the findings in a format suitable for legal proceedings. Clear documentation and reports are crucial for communicating the results of the digital forensic investigation effectively.

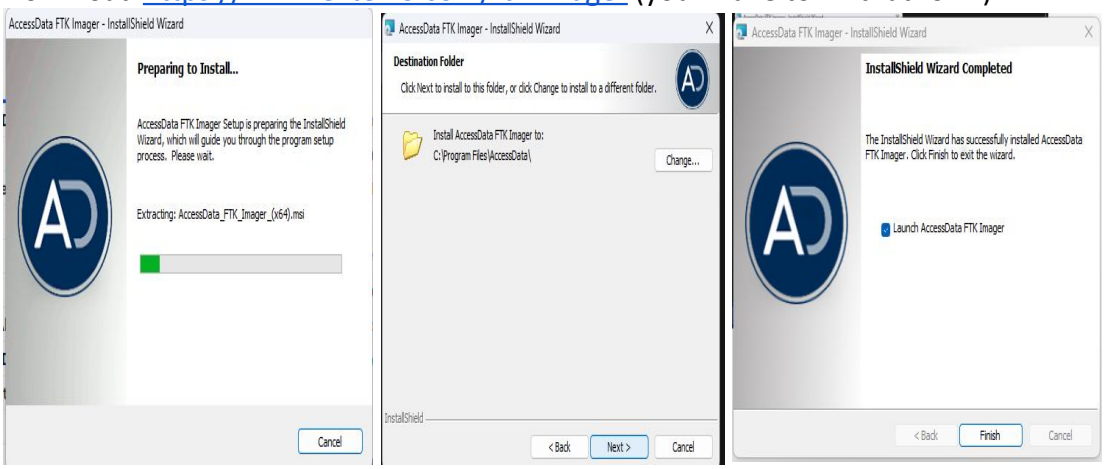
In essence, digital forensics relies on meticulous processes facilitated by tools like FTK Imager and Autopsy to uncover, analyze, and document electronic evidence, aiding in the resolution of cybercrimes and legal investigations.

Image – The copy of a hard drive that is compressed into one file.
Acquisition – The viewing of the image in a program in order to gather data and information.
Data Compression – When the information from a hard drive or other form of storage is compressed together to take up less space on the computer.
Verification – The information on the image is checked with the original information on the hard drive to make sure nothing was altered.

Description :
FTK® Imager is a data preview and imaging tool used to acquire data (evidence) in a forensically sound manner by creating copies of data without making changes to the original evidence. After you create an image of the data, use Forensic Toolkit® (FTK®) to perform a thorough forensic examination and create a report of your findings. FTK Imager will:
• **Create forensic images** of local hard drives, CDs and DVDs, thumb drives or other USB devices, entire folders, or individual files from various places within the media.
• **Preview files and folders** on local hard drives, network drives, CDs and DVDs, thumb drives or other USB devices.
• **Preview the contents** of forensic images stored on the local machine or on a network drive.
• **Mount an image for a read-only view** that leverages Windows® Internet Explorer® to see the content of the image exactly as the user saw it on the original drive.
• **Export** files and folders from forensic images.
• See and **recover files that have been deleted** from the Recycle Bin, but have not yet been overwritten on the drive.
• **Create hashes of files** to check the integrity of the data by using either of the two hash functions available in FTK Imager: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA-1).• **Generate hash reports** for regular files and disk images (including files inside disk images) that you can later use as a benchmark to prove the integrity of your case
evidence. When a full drive is imaged, a hash generated by FTK Imager can be used to verify that the image hash and the drive hash match after the image is created, and that the image has remained unchanged since acquisition

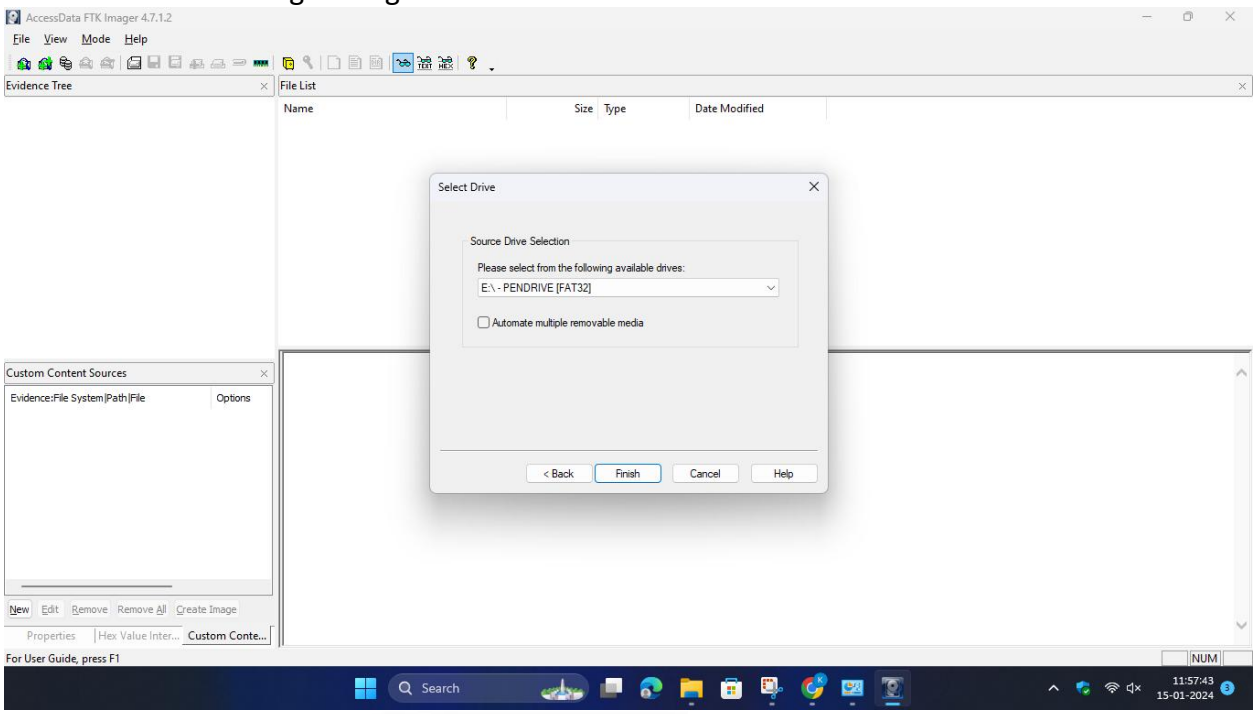
STEPS:

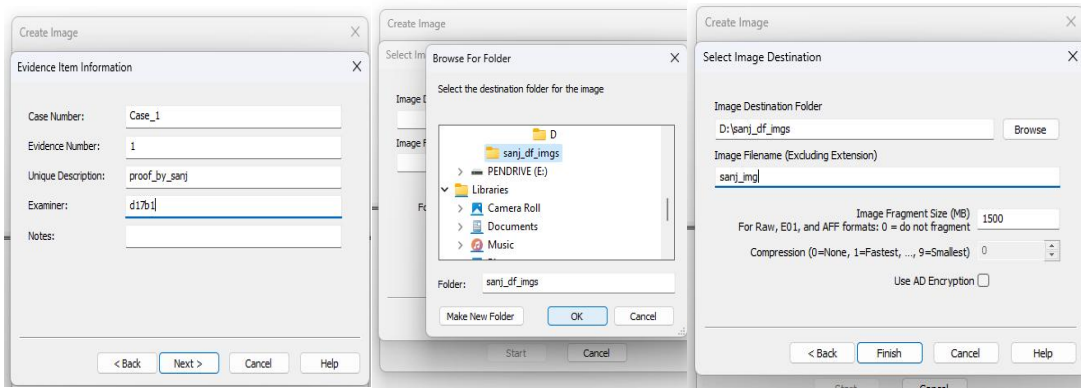
Download https://www.exterro.com/ftk-imager (youll have to fill that form)

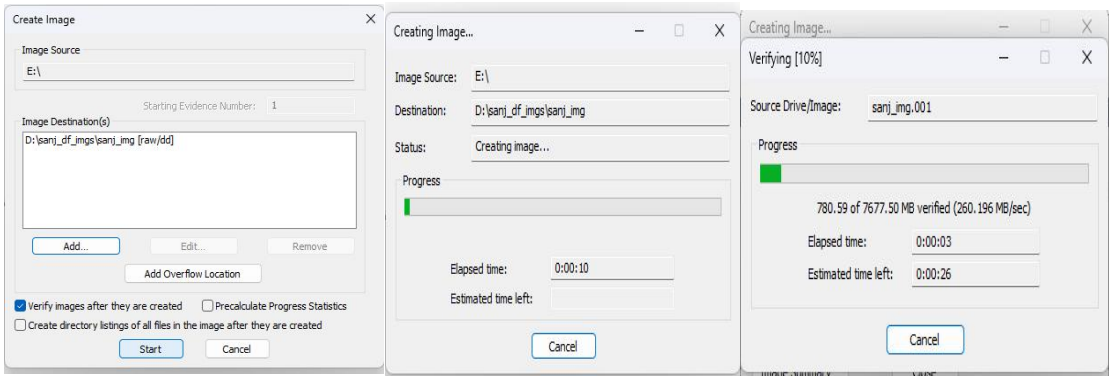


Launch it

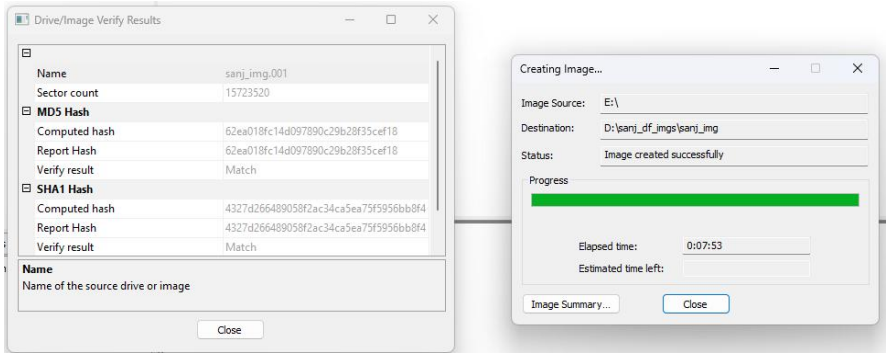
File -> Create disk image -> logical drive



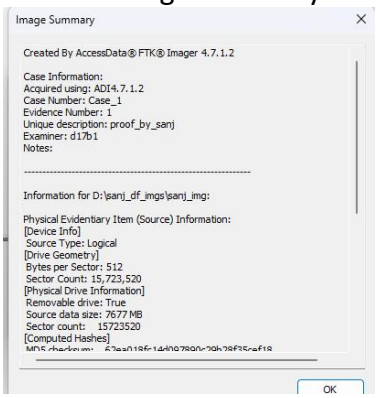




Let it finish:



Click on Image Summary:



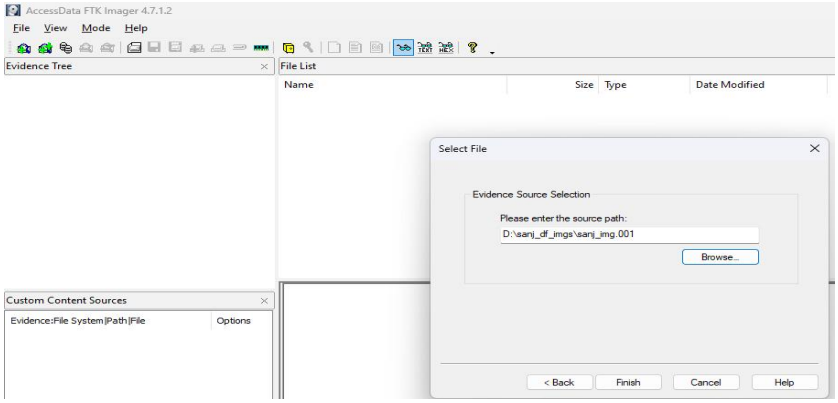
MD5 checksum: 62ea018fc14d097890c29b28f35cef18
SHA1 checksum: 4327d266489058f2ac34ca5ea75f5956bb8f418a

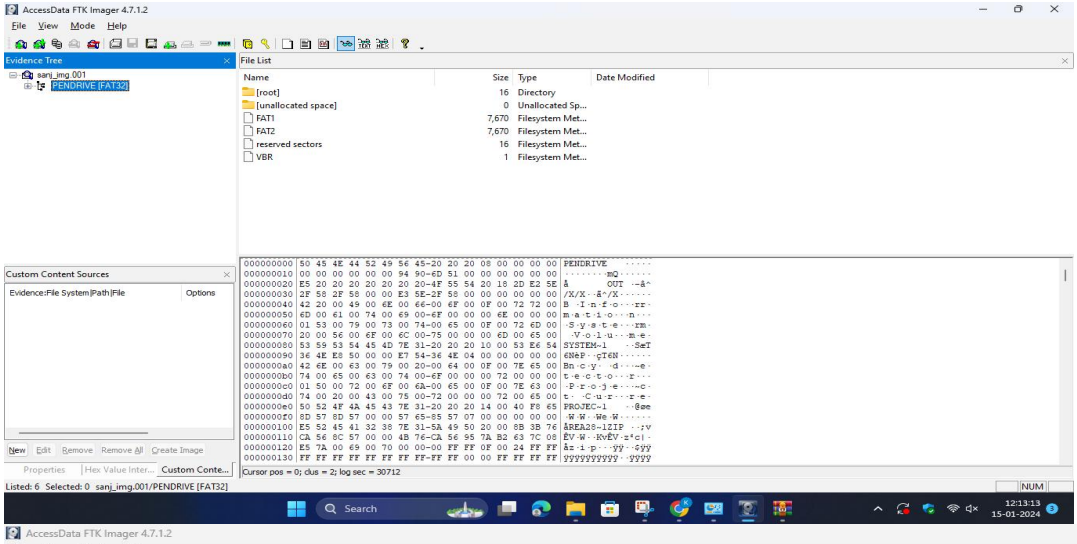
Image Information:
Acquisition started: Mon Jan 15 11:59:13 2024
Acquisition finished: Mon Jan 15 12:07:06 2024
Segment list:
D:\sanj_df_imgs\sanj_img.001
D:\sanj_df_imgs\sanj_img.002
D:\sanj_df_imgs\sanj_img.003
D:\sanj_df_imgs\sanj_img.004
D:\sanj_df_imgs\sanj_img.005
D:\sanj_df_imgs\sanj_img.006

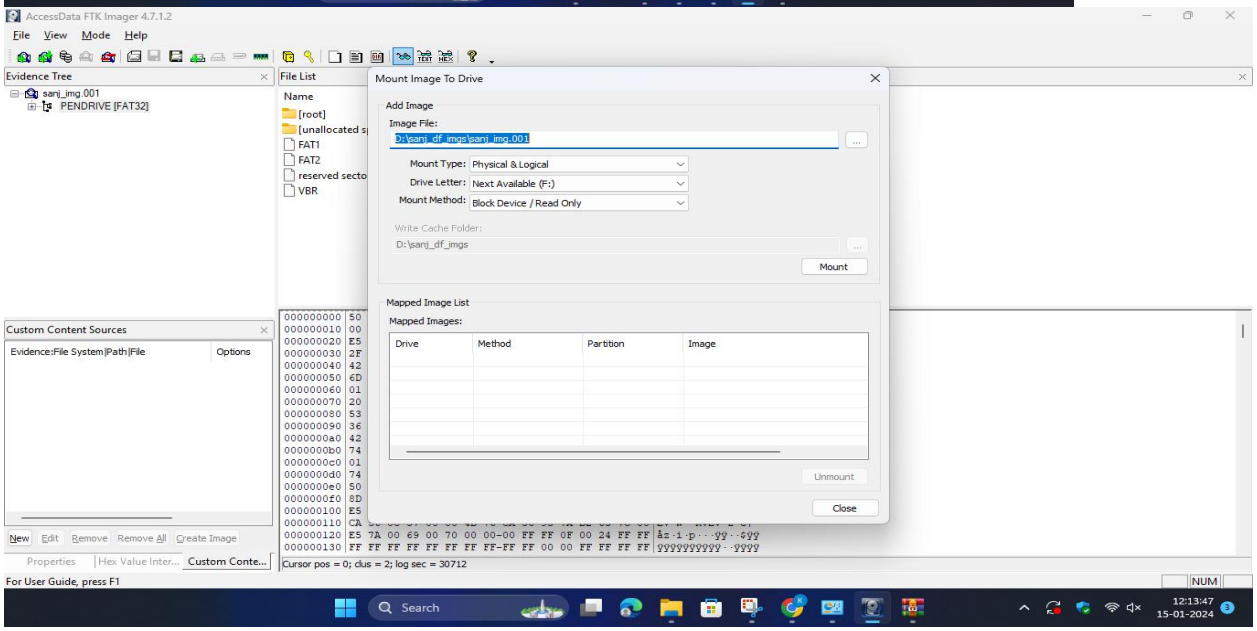
Image Verification Results:
Verification started: Mon Jan 15 12:07:06 2024

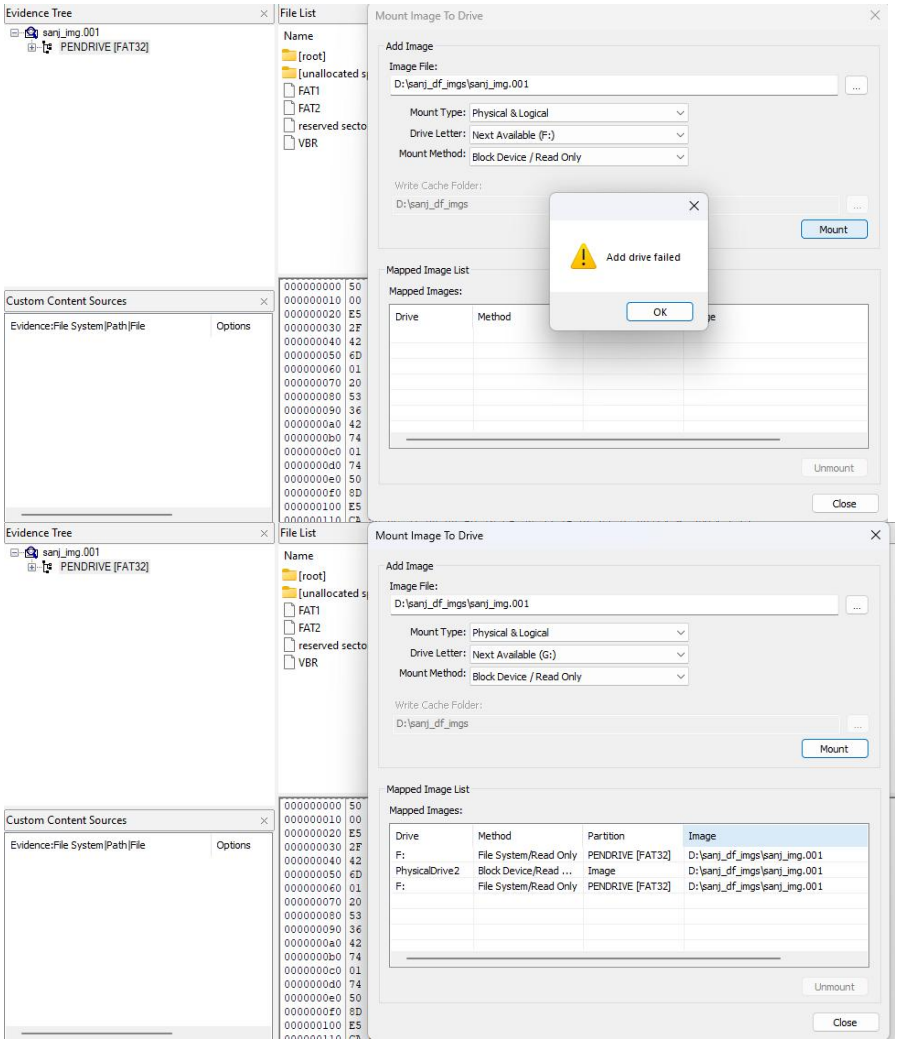
Verification finished: Mon Jan 15 12:07:30 2024
MD5 checksum: 62ea018fc14d097890c29b28f35cef18 : verified
SHA1 checksum: 4327d266489058f2ac34ca5ea75f5956bb8f418a : verified

Now go to file -> Add evidence item
(select ur raw img folder)

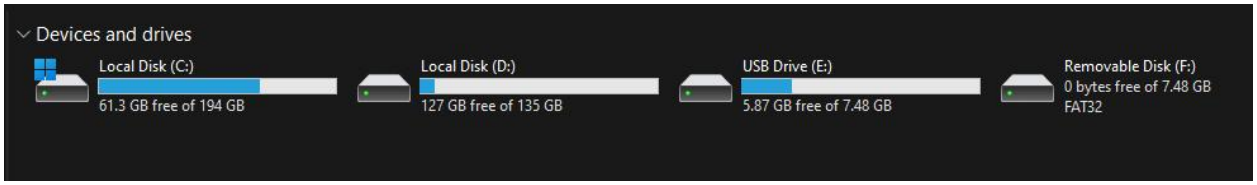






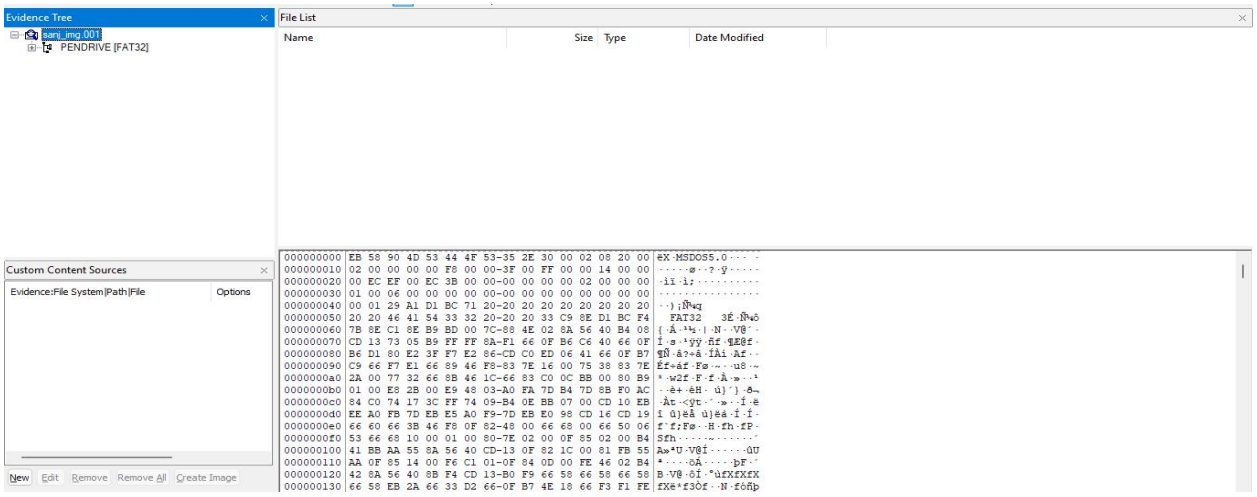


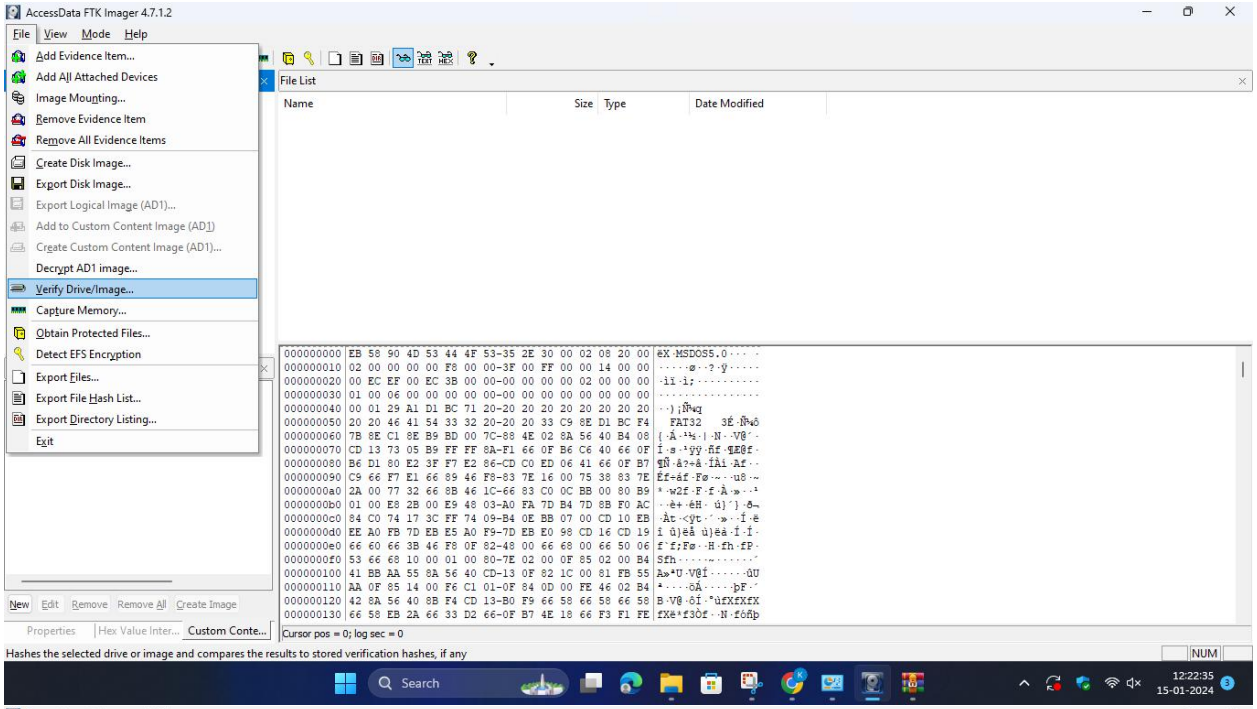
A new drive F has been created:

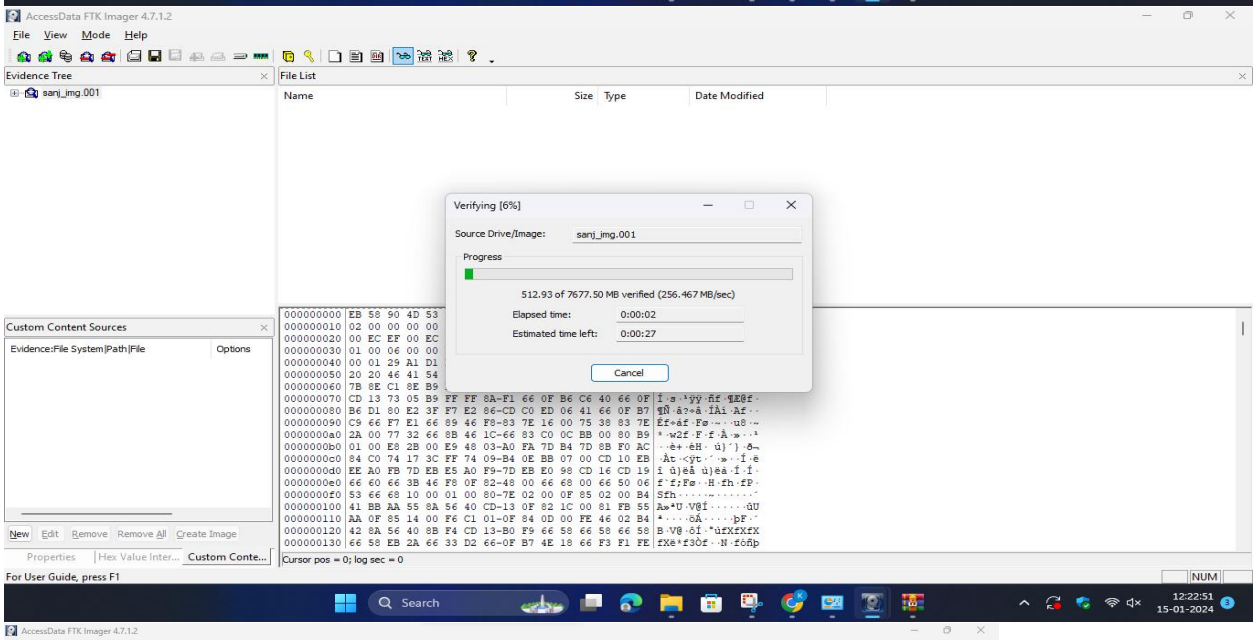


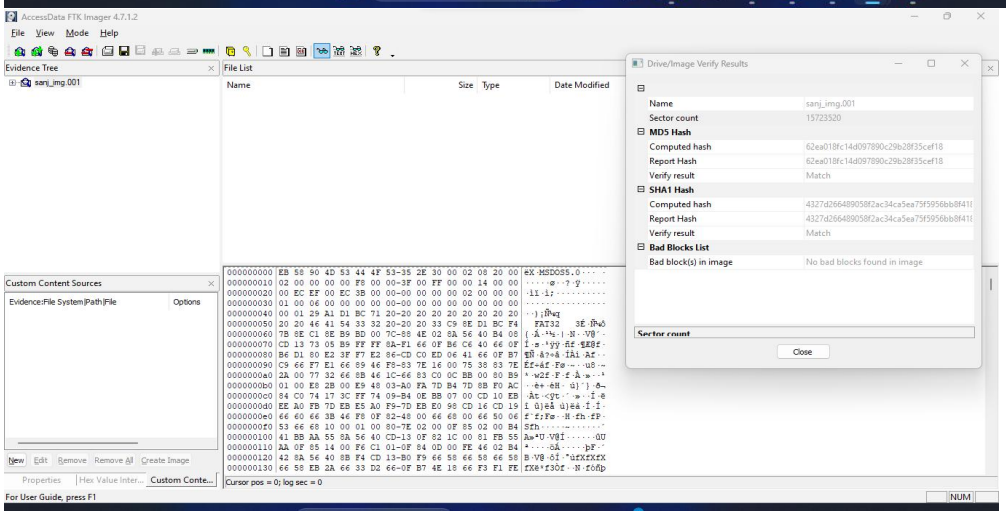
Now verify:

Select the folder .001 extension

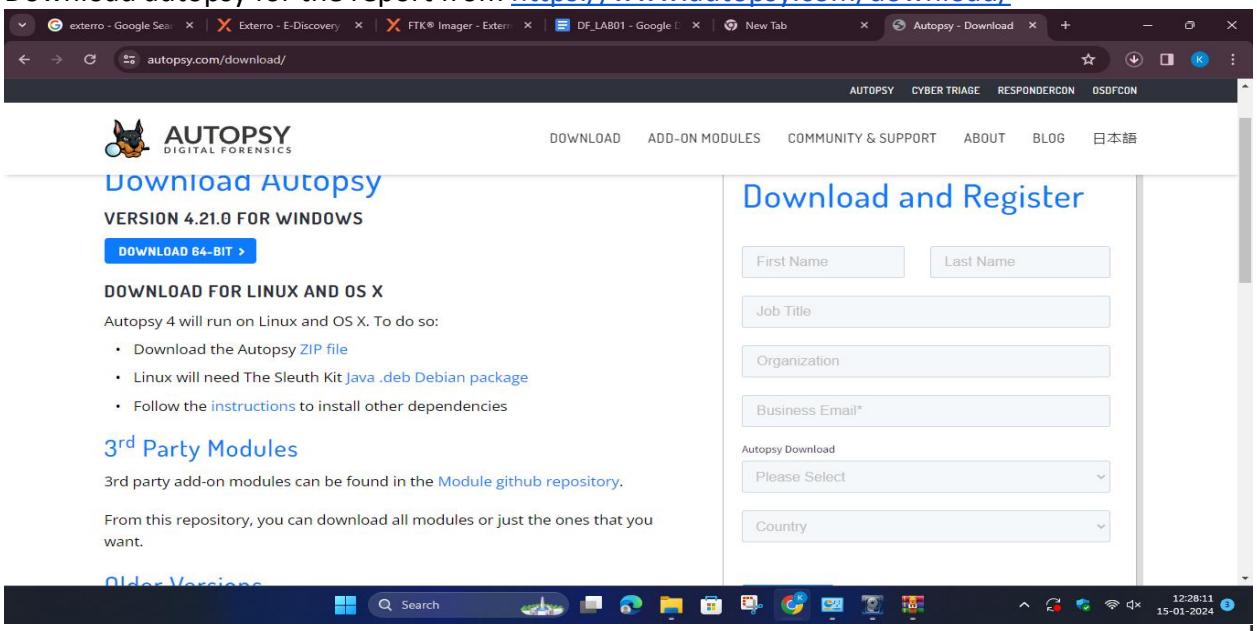


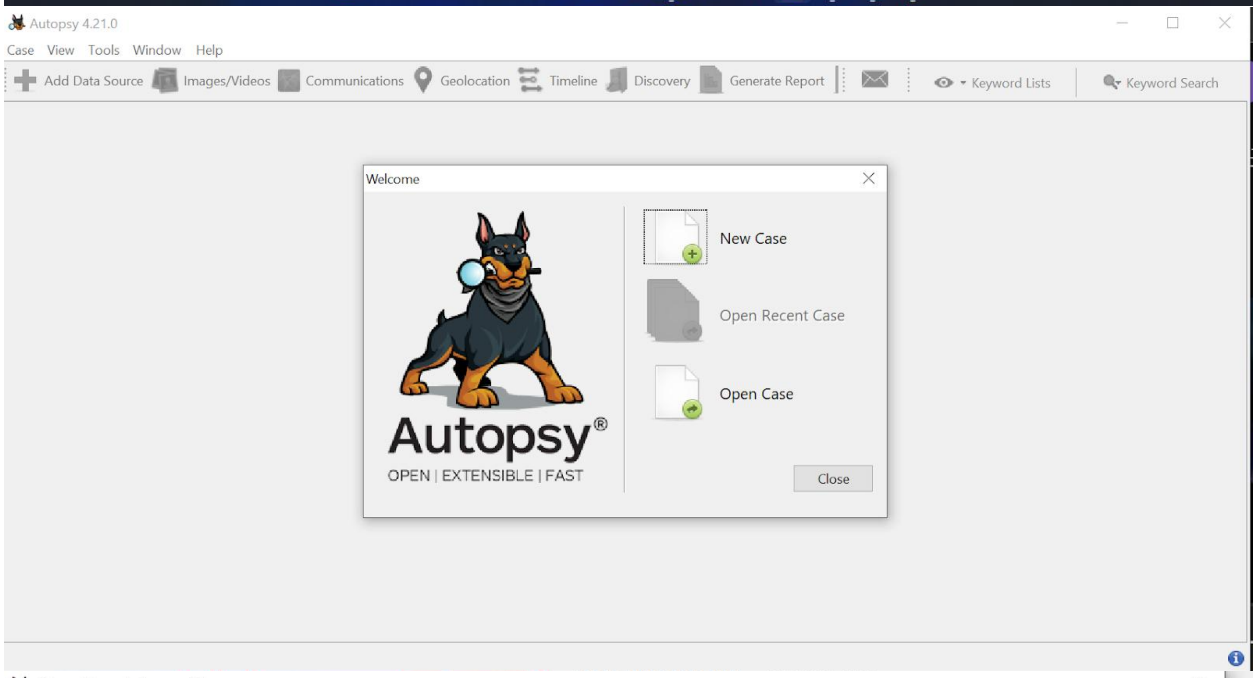

AccessData FTK Imager 4.7.1.2
File View Mode Help
Add Evidence Item...
Add All Attached Devices
Image Mounting...
Remove Evidence Item
Remove All Evidence Items
Create Disk Image...
Export Disk Image...
Export Logical Image (AD1)...
Add to Custom Content Image (AD1)
Create Custom Content Image (AD1)...
Decrypt AD1 image...
Verify Drive/Image...
Capture Memory...
Obtain Protected Files...
Detect EFS Encryption
Export Files...
Export File Hash List...
Export Directory Listing...
Exit
File List
Name
Size
Type
Date Modified
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
Cursor pos = 0; log sec = 0
Hashes the selected drive or image and compares the results to stored verification hashes, if any
NUM
Search
12:22:35
15-01-2024

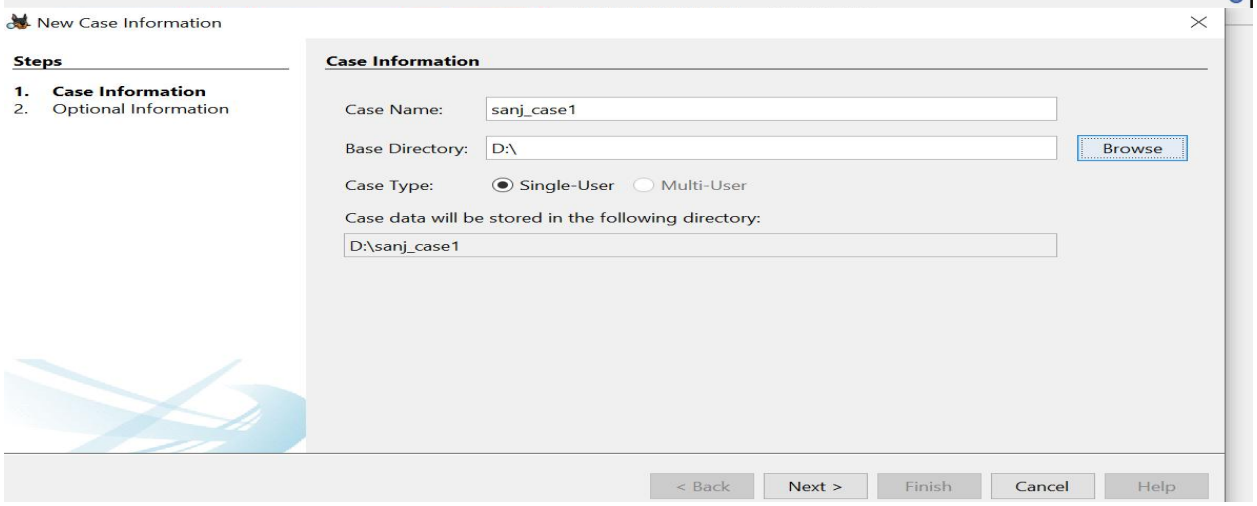

AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
sanj_img.001
File List
Name
Size
Type
Date Modified
Verifying [6%]
Source Drive/Image: sanj_img.001
Progress
512.93 of 7677.50 MB verified (256.467 MB/sec)
Elapsed time: 0:00:02
Estimated time left: 0:00:27
Cancel
Custom Content Sources
Evidence:File System|Path|File
Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
Cursor pos = 0; log sec = 0
For User Guide, press F1
NUM
Search
12:22:51
15-01-2024


AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
sanj_img.001
File List
Name
Size
Type
Date Modified
Drive/Image Verify Results
Name sanj_img.001
Sector count 15723520
MD5 Hash
Computed hash 62ea018fc14d097890c29b28f35cef18
Report Hash 62ea018fc14d097890c29b28f35cef18
Verify result Match
SHA1 Hash
Computed hash 4327d266489058f2ac34ca5ea75f5956bb8f41
Report Hash 4327d266489058f2ac34ca5ea75f5956bb8f41
Verify result Match
Bad Blocks List
Bad block(s) in image No bad blocks found in image
Sector count
Close
Custom Content Sources
Evidence:File System|Path|File
Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
Cursor pos = 0; log sec = 0
For User Guide, press F1
NUM

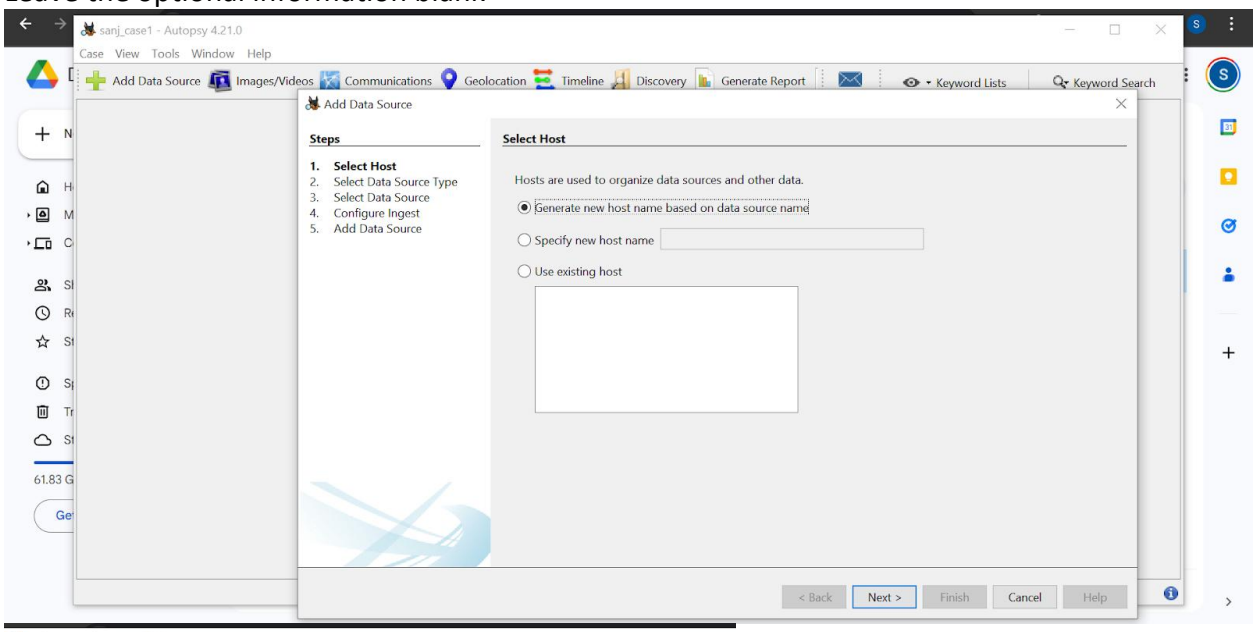
Download autopsy for the report from https://www.autopsy.com/download/

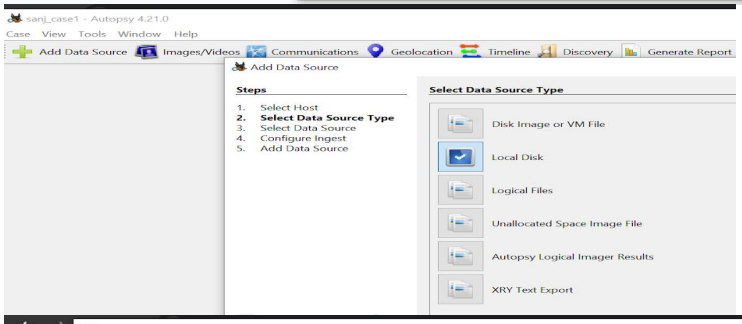


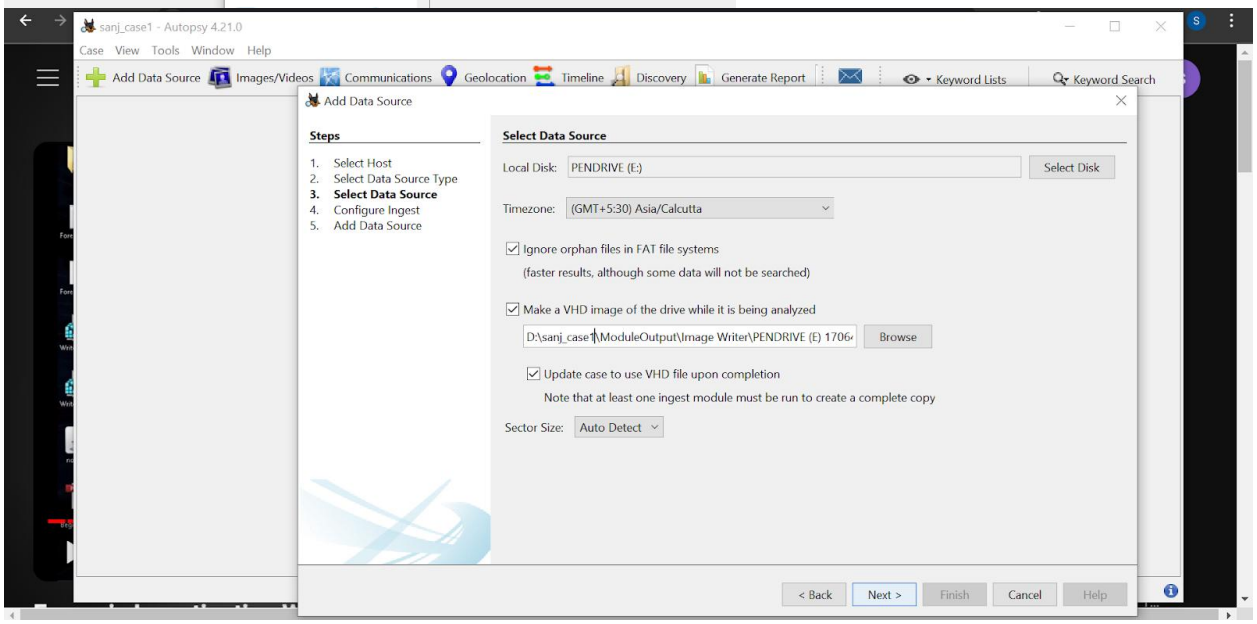


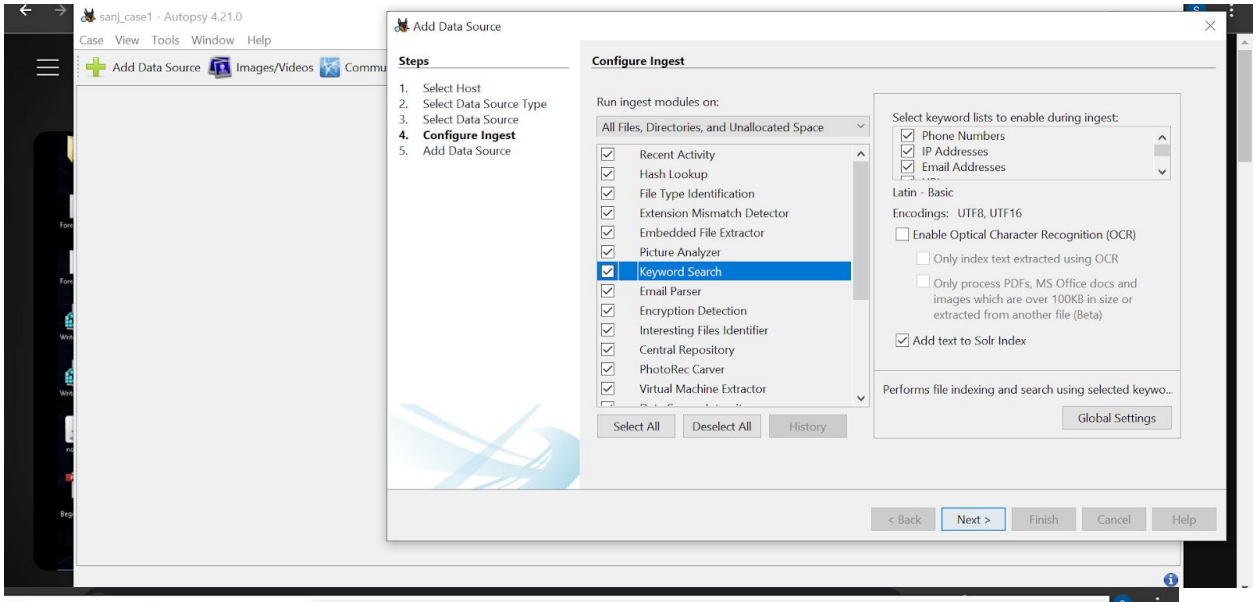


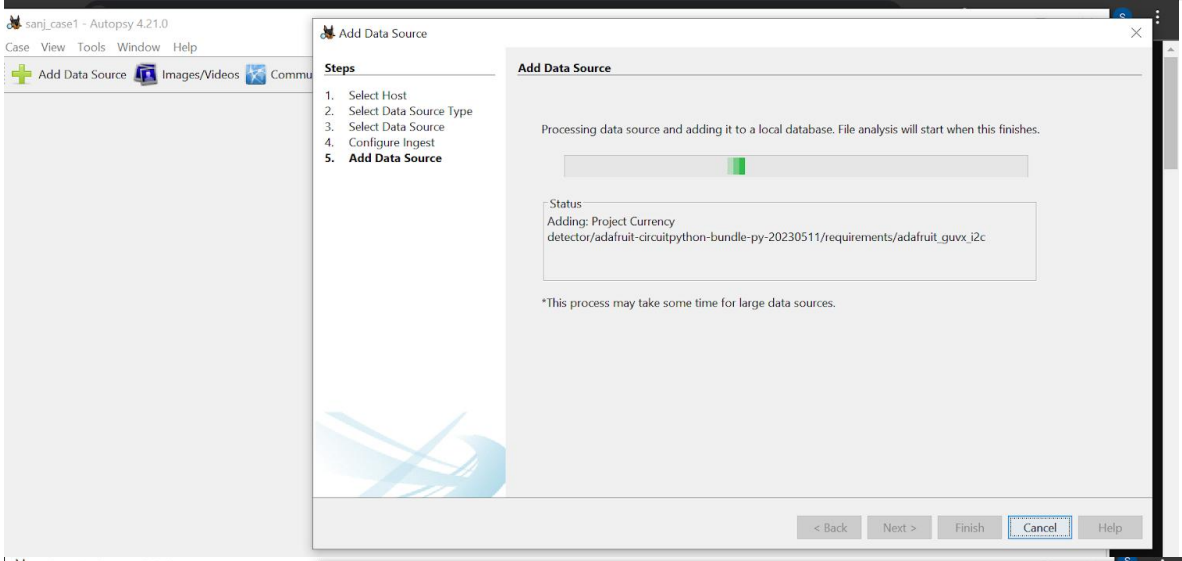
Leave the optional information blank

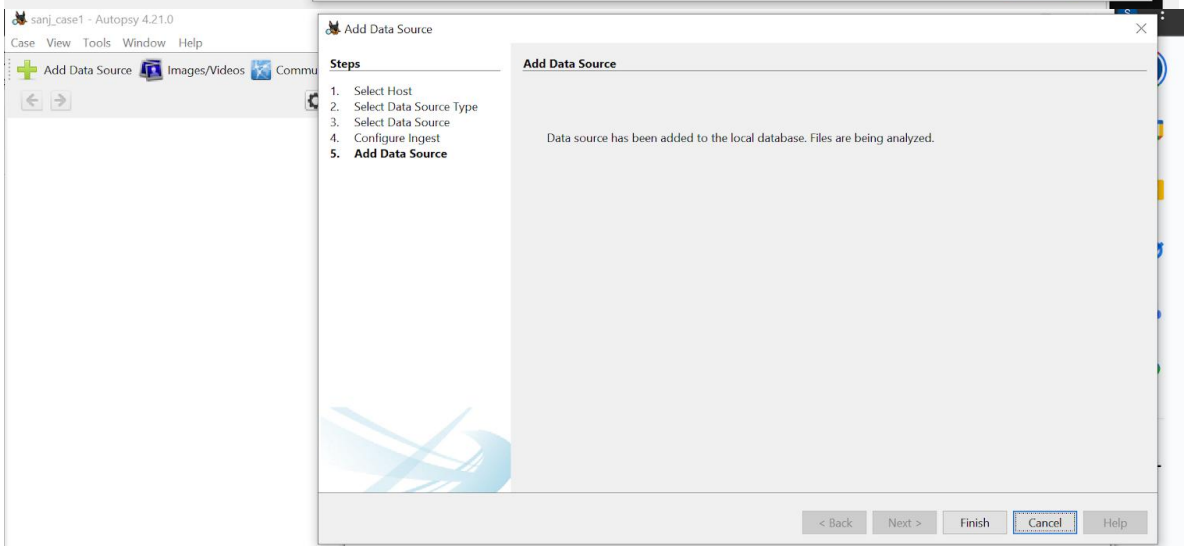




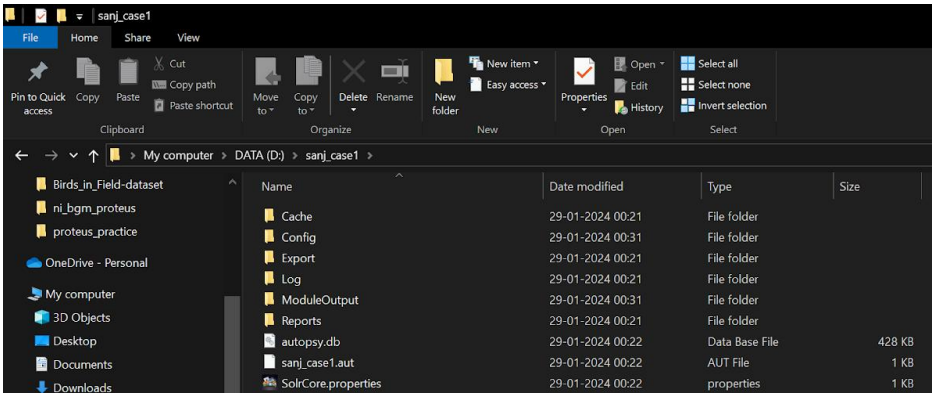




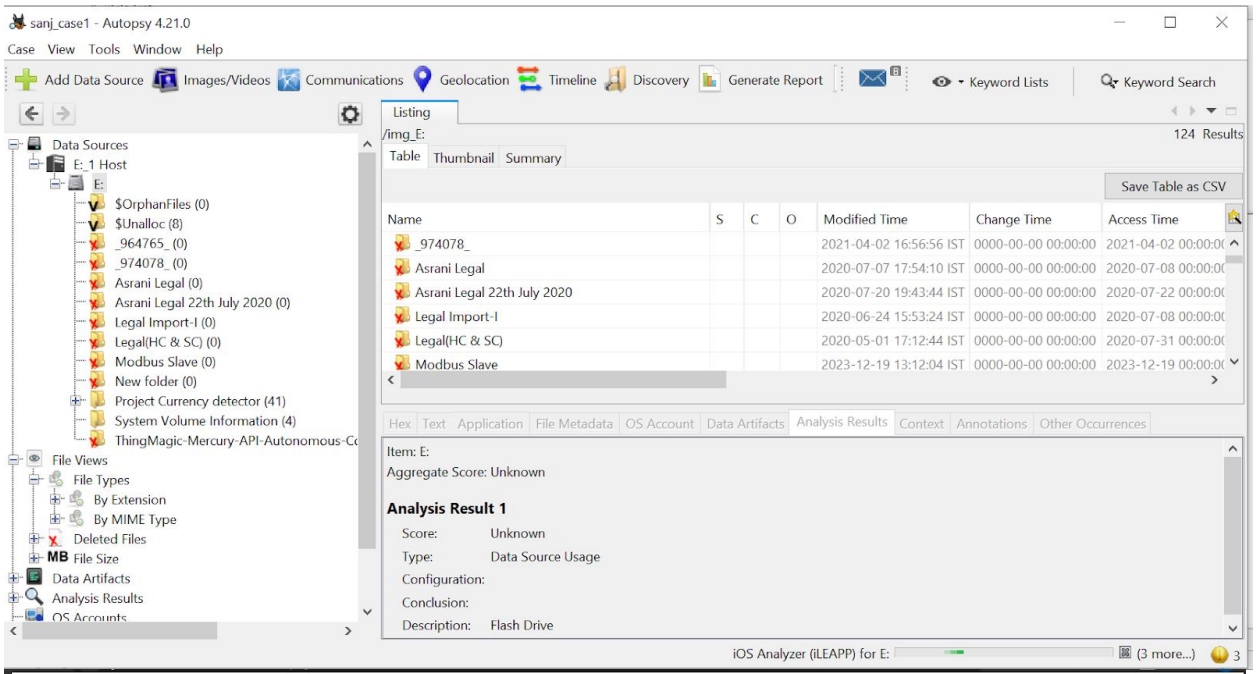


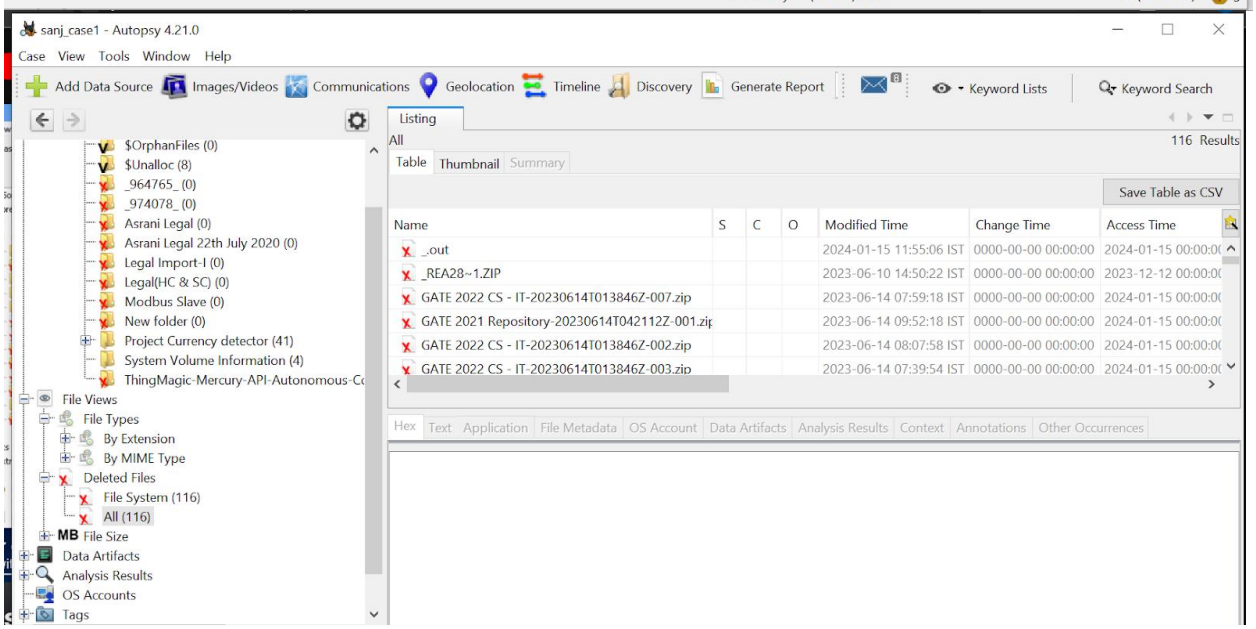


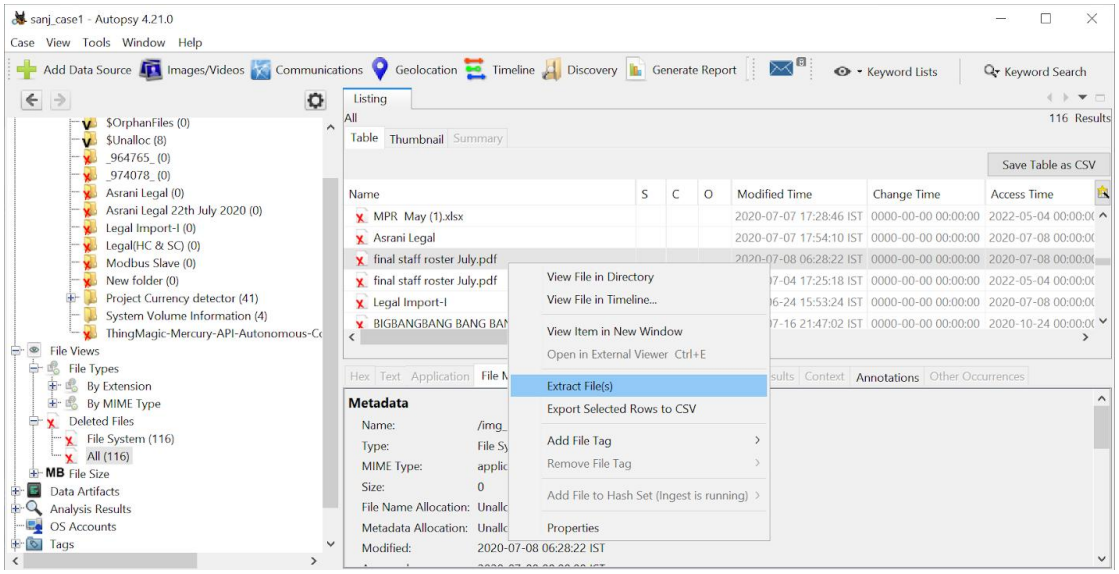
This is the folder:



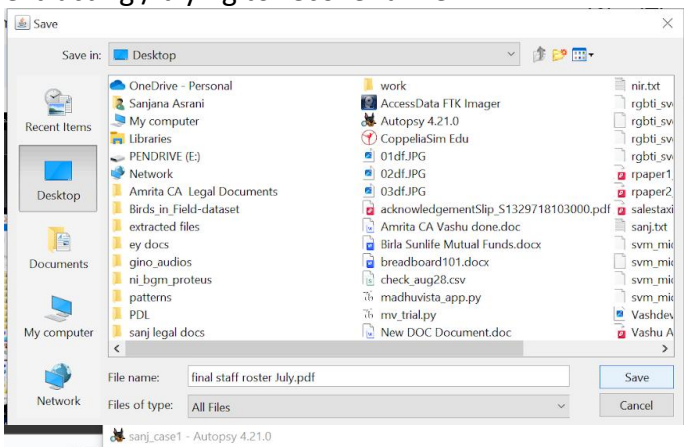
All the deleted folders can be seen:

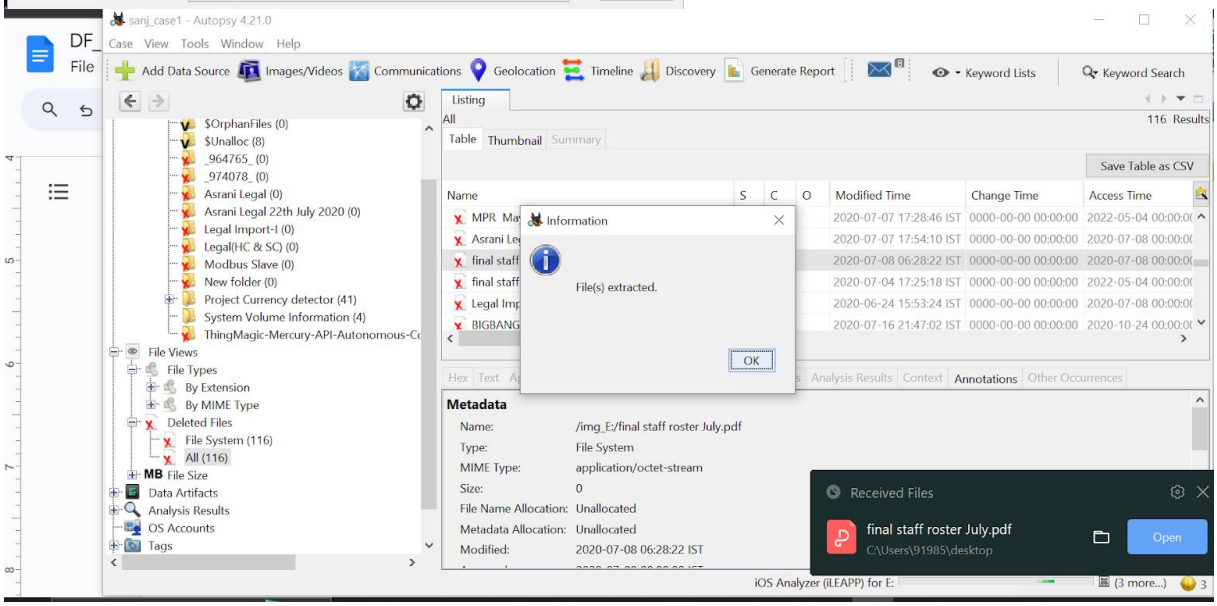




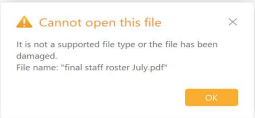


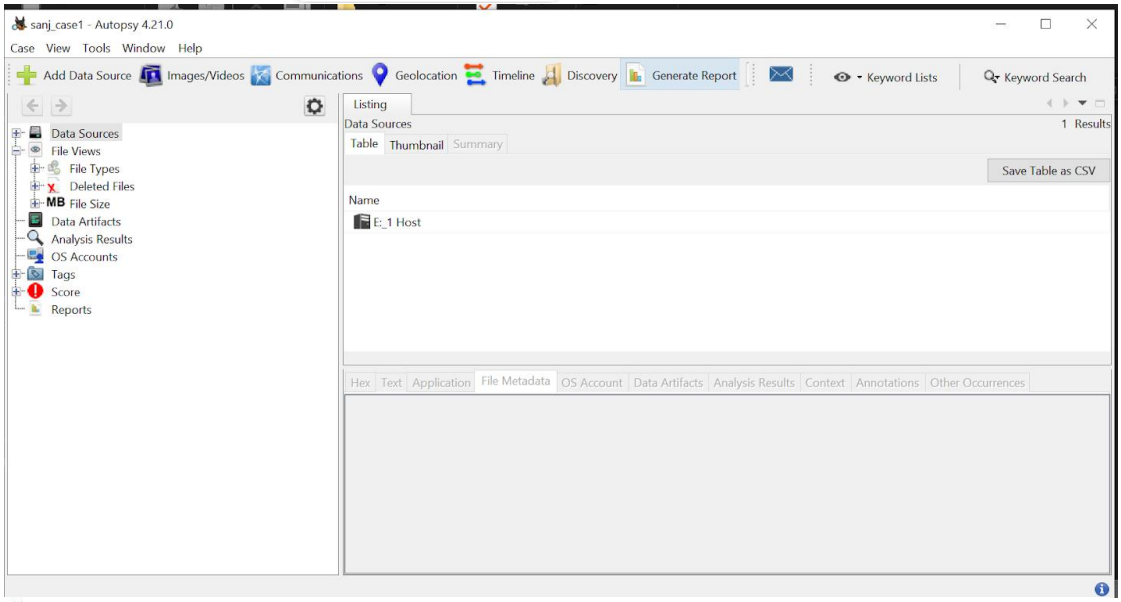
extracting / trying to recover a file

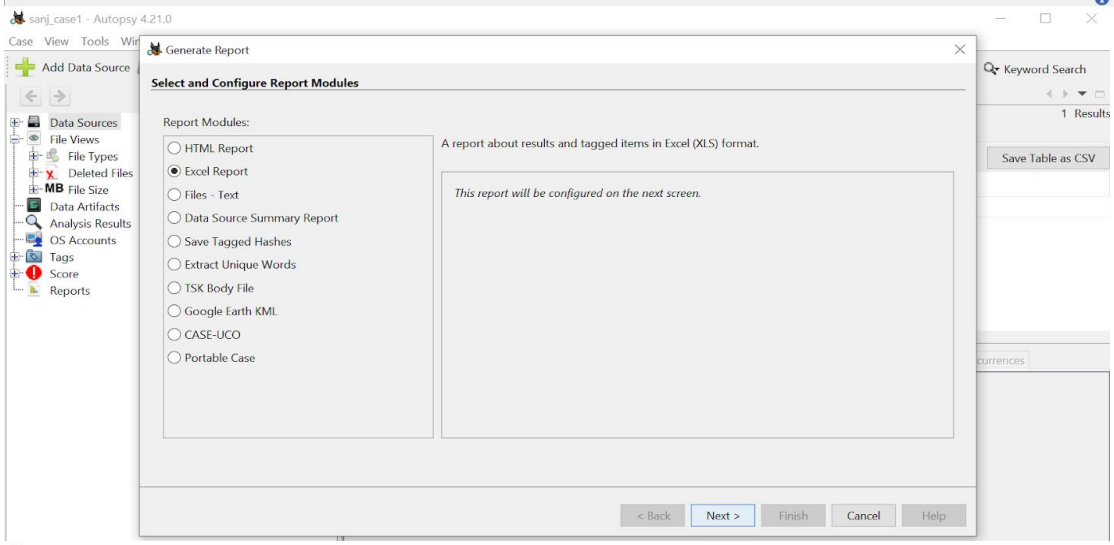


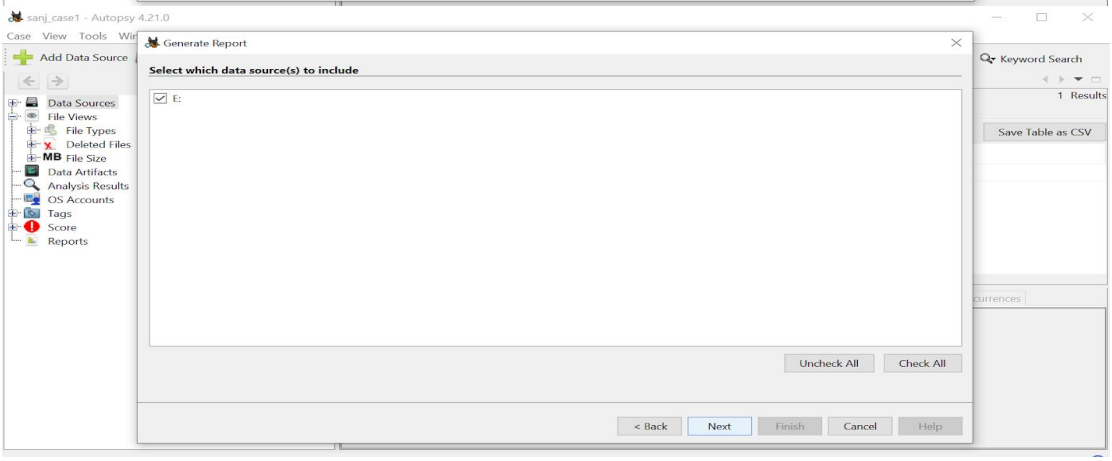


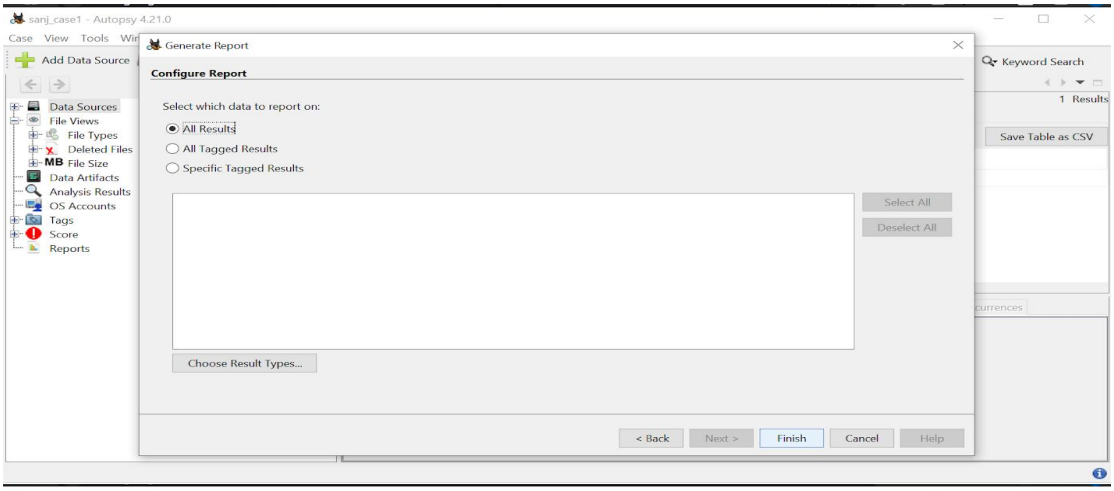
Home
final staff roster July

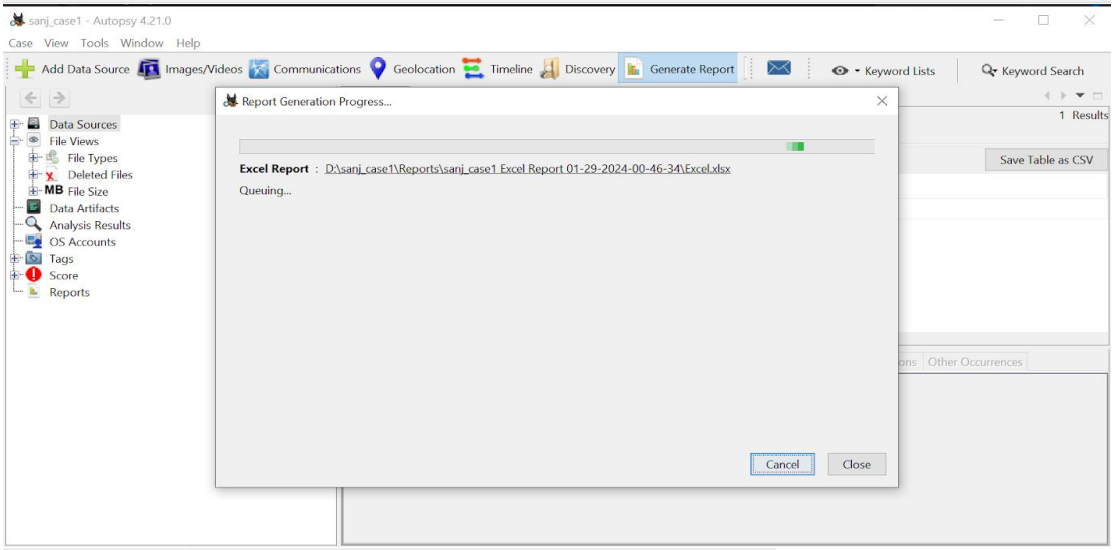

Cannot open this file
It is not a supported file type or the file has been damaged.
File name: "final staff roster July.pdf"
OK

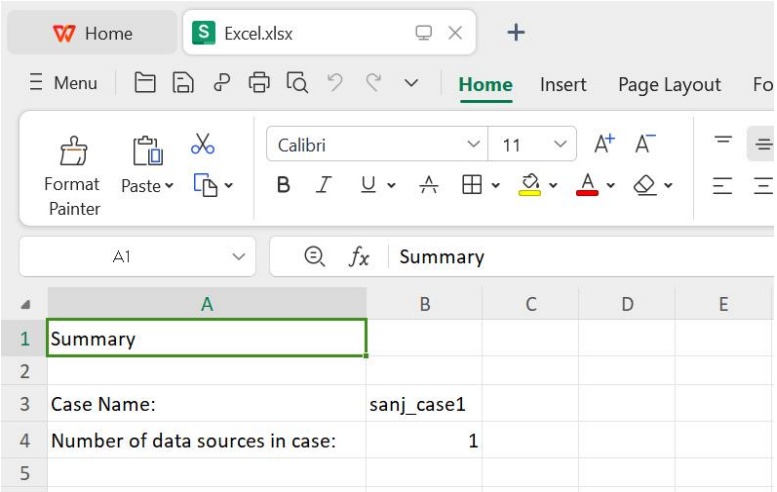

sanj_case1 - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Keyword Lists
Keyword Search
Data Sources
File Views
File Types
Deleted Files
File Size
Data Artifacts
Analysis Results
OS Accounts
Tags
Score
Reports
Listing
Data Sources
1 Results
Table
Thumbnail
Summary
Save Table as CSV
Name
E:_1 Host
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences


sanj_case1 - Autopsy 4.21.0
Generate Report
Select and Configure Report Modules
Report Modules:
HTML Report
Excel Report
Files - Text
Data Source Summary Report
Save Tagged Hashes
Extract Unique Words
TSK Body File
Google Earth KML
CASE-UCO
Portable Case
A report about results and tagged items in Excel (XLS) format.
This report will be configured on the next screen.
< Back
Next >
Finish
Cancel
Help

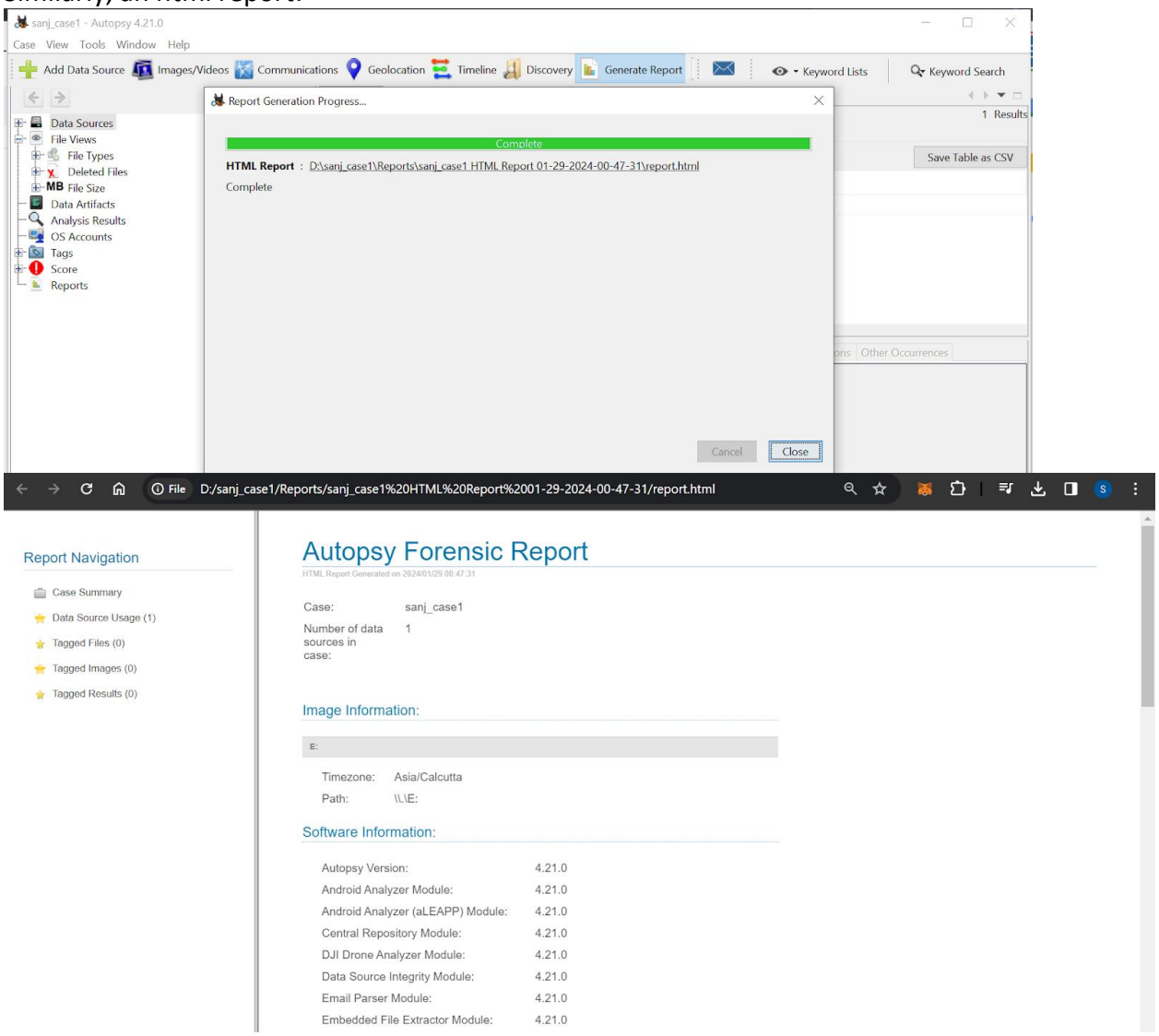

sanj_case1 - Autopsy 4.21.0
Generate Report
Select which data source(s) to include
E:
Uncheck All
Check All
< Back
Next
Finish
Cancel
Help


sanj_case1 - Autopsy 4.21.0
Case View Tools Wir
Add Data Source
Data Sources
File Views
File Types
Deleted Files
File Size
Data Artifacts
Analysis Results
OS Accounts
Tags
Score
Reports
Generate Report
Configure Report
Select which data to report on:
All Results
All Tagged Results
Specific Tagged Results
Select All
Deselect All
Choose Result Types...
< Back
Next >
Finish
Cancel
Help
Keyword Search
1 Results
Save Table as CSV


sanj_case1 - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Keyword Lists
Keyword Search
Report Generation Progress...
Excel Report : D:\sanj_case1\Reports\sanj_case1 Excel Report 01-29-2024-00-46-34\Excel.xlsx
Queuing...
Cancel
Close
1 Results
Save Table as CSV
Other Occurrences


Home
Excel.xlsx
Menu
Home
Insert
Page Layout
Format Painter
Paste
Calibri
11
A1
Summary
A
B
C
D
E
1 Summary
2
3 Case Name: sanj_case1
4 Number of data sources in case: 1
5

Similarly, an html report:



CONCLUSION:

Thereby I have explored the basic steps of creating a forensic image using FTK Imager. by acquiring a bit-for-bit copy of the target drive, ensuring data integrity throughout the process. Subsequently, a report using Autopsy has been generated, employing its powerful tools to analyze the imaged drive comprehensively.I have navigated through the file systems, examined artifacts, and applied keyword searches to uncover potential evidence