Lab Manual For
M.Sc. (IT)
Part II Sem IV Course:
Computer Forensics 2025-2026

SR. NO.	PARTICULARS
1.	File System Analysis using The Sleuth Kit
2.	Using Windows Forensics using FTK toolkit
3	Creating a forensic image using FTK imager
4	Recovering and inspecting deleted files using autopsy tool
5	Capturing and analysing network packets using wireshark
6	Study and implementation of e-mail forensics using AccessDataFTK
7.	Generating forensics report using sleuth kit.
8	Generating forensics report using AccessDataFTK

PRACTICAL - 1

AIM: File System Analysis using The Sleuth Kit

Tool Used: Autopsy 4.0.0

Theory:

Slueth Kit

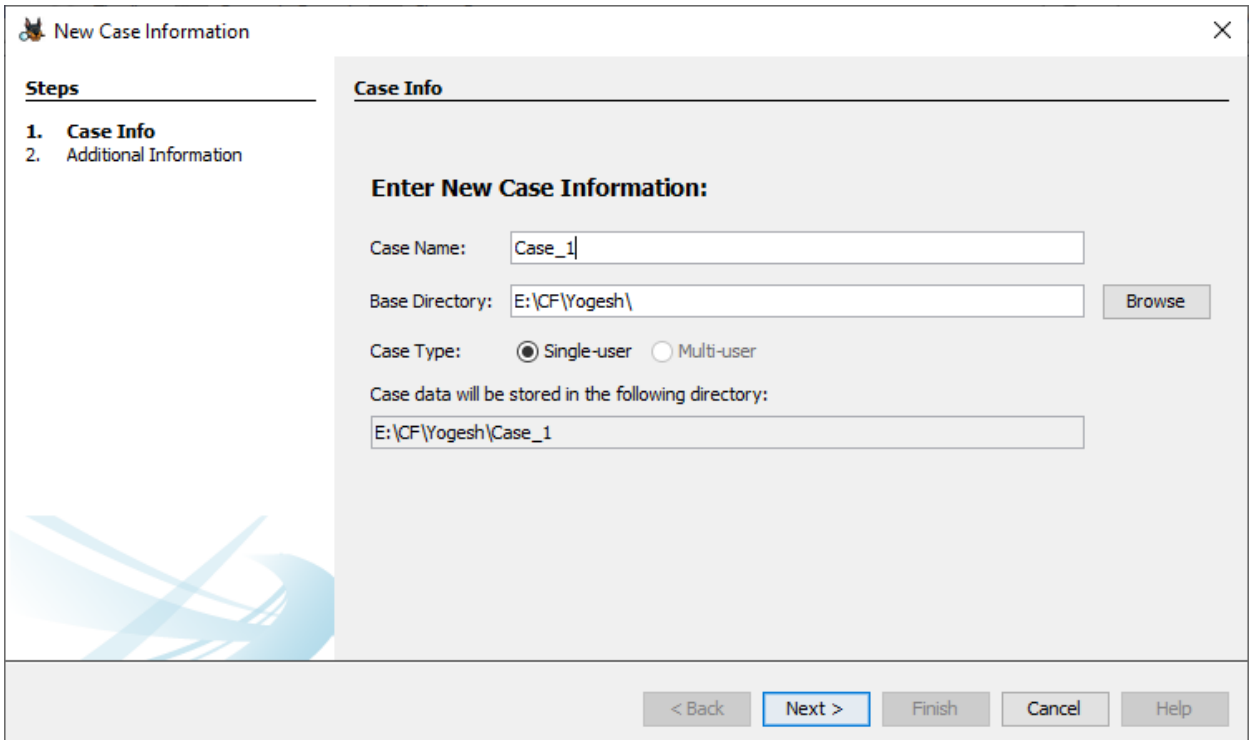
- Sleuth Kit is a C library and collection of command line file and volume system forensic analysis tools.
- The file system tools allow you to examine file systems of a suspect computer in a non- intrusive fashion.
- Because the tools do not rely on the operating system to process the file systems, deleted and hidden content is shown. It runs on Windows and Unix platforms.
- http://www.sleuthkit.org/

Autopsy

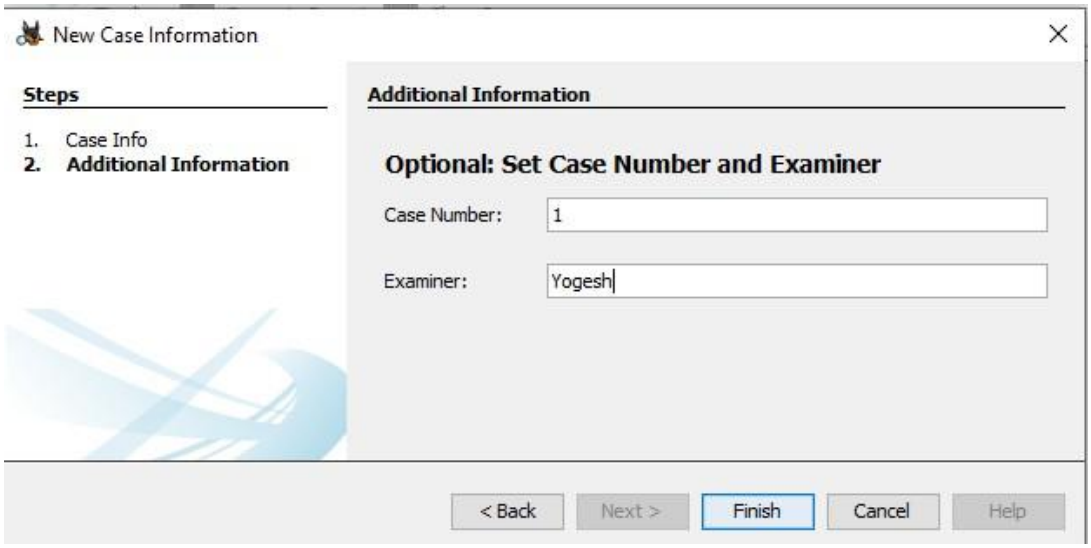
- Autopsy is an open source forensics tool that can be compared to FTK or EnCase and is able to assist investigators when working on cases.
- The Autopsy is a graphical interface to the command line digital investigation tools in The Sleuth Kit. Together, they allow you to investigate the file system and volumes of a computer.
- http://www.sleuthkit.org/autopsy/

Step 1: Upon starting Autopsy, a window will open with three selections to make: create a new case, open existing case, or to open a recent case.

Step 2: Select the "Create New Case" option and be directed to a new window that will have information to fill in. Fill in appropriate information and click Next.


New Case Information
Steps
1. Case Info
2. Additional Information
Case Info
Enter New Case Information:
Case Name:
Case_1
Base Directory:
E:\CF\Yogesh\
Browse
Case Type:
Single-user
Multi-user
Case data will be stored in the following directory:
E:\CF\Yogesh\Case_1
< Back
Next >
Finish
Cancel
Help

Step 3: Next window will allow the investigator to fill in the case number and examiner name. This is for the purpose of creating better documentation and logging. After the information is filled in select the finish button to continue.

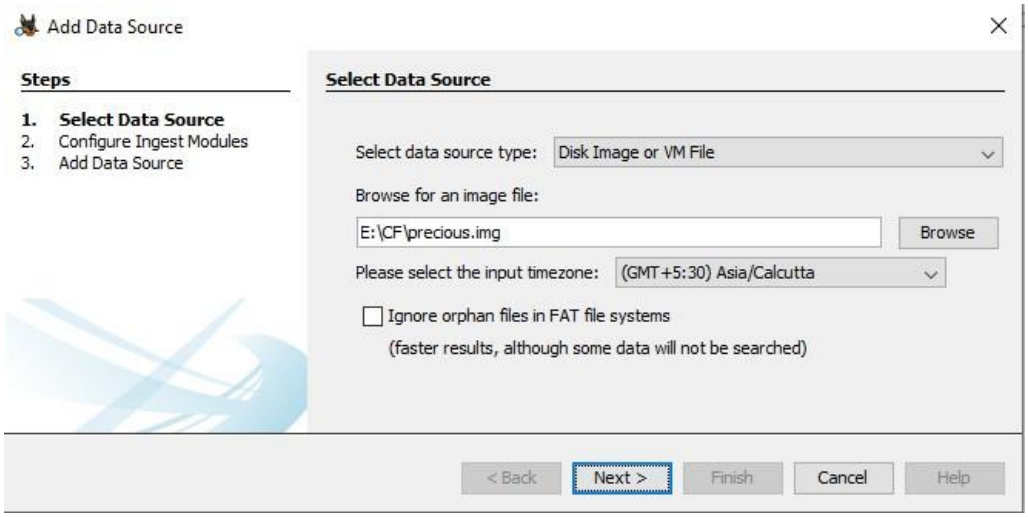


Step 4: The next step in the investigation will be to add an image file to the case. The image file can be chosen from a wide variety of formats including: **img, dd, 001, aa, and e01.**

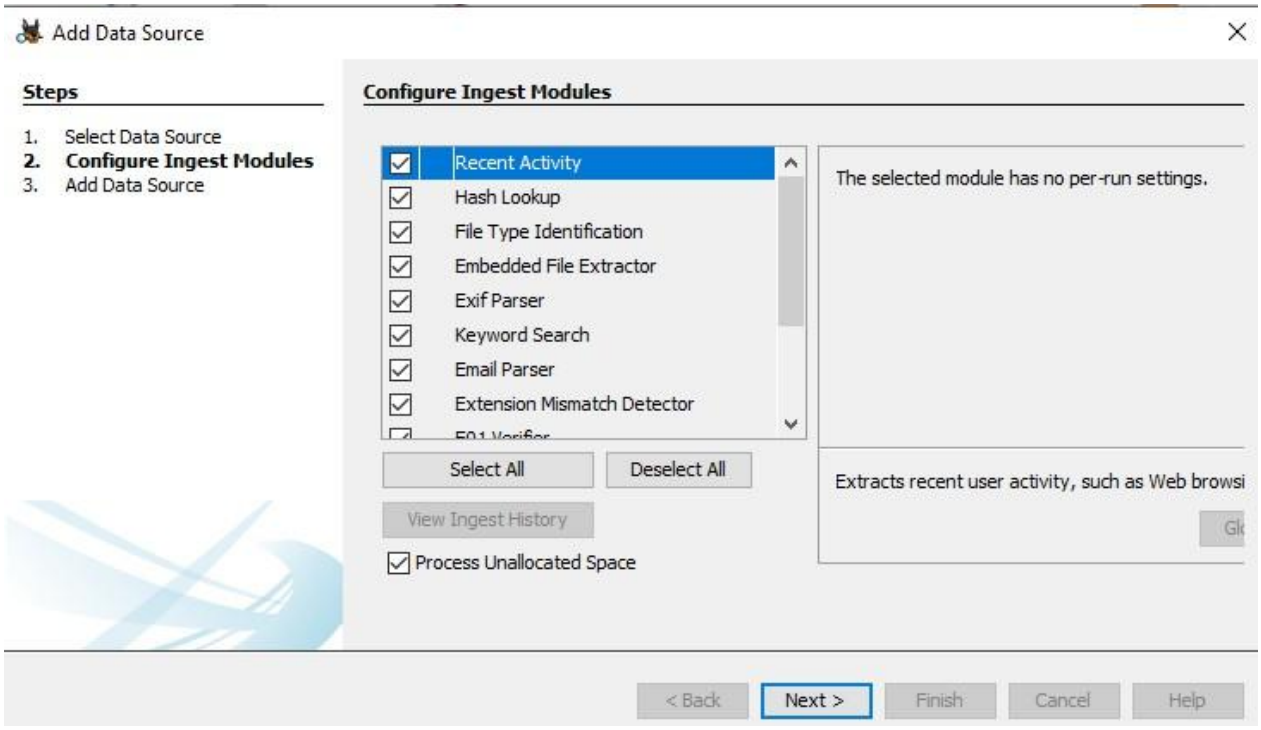
Use the browse button to find the image that is desired to work with and select add.

Options to choose the time zone of where the image came from as well as to ignore orphan files in FAT file systems are available to be selected based on the investigators preference and situation.

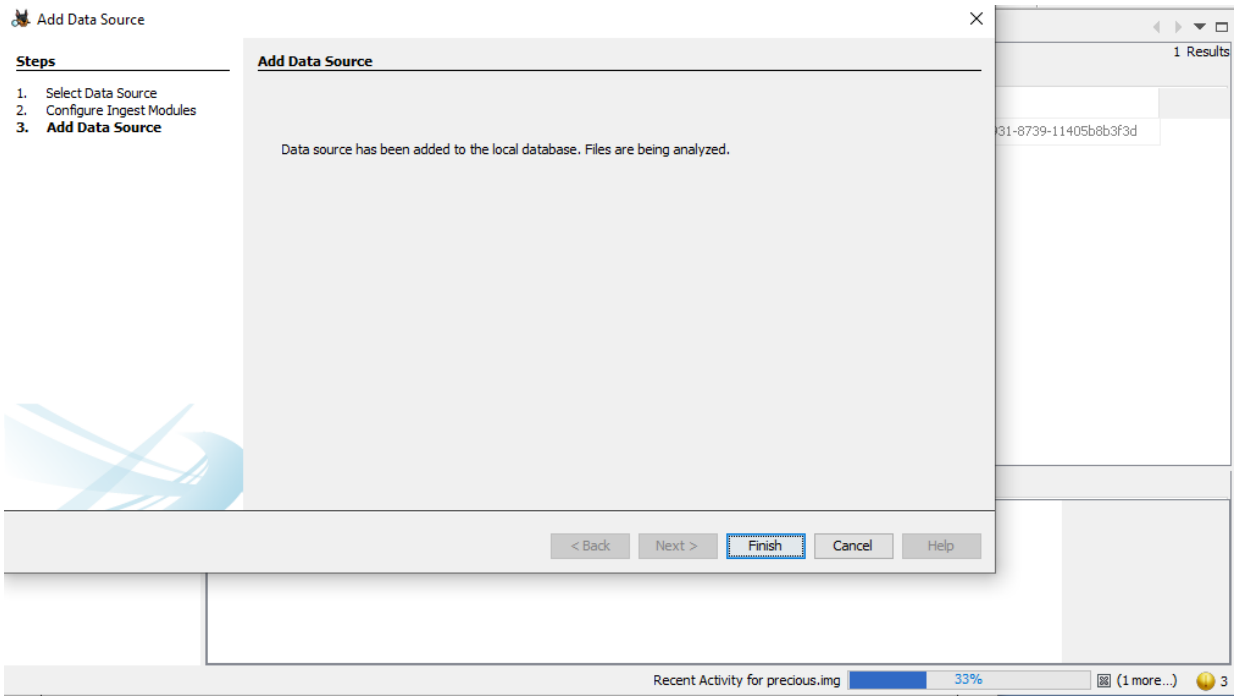
Since we have image file we will choose **"Image File Option"**, then browse an**d load "Precious.img"** and click on Next.


Add Data Source
Steps
1. Select Data Source
2. Configure Ingest Modules
3. Add Data Source
Select Data Source
Select data source type:
Disk Image or VM File
Browse for an image file:
E:\CF\precious.img
Browse
Please select the input timezone:
(GMT+5:30) Asia/Calcutta
Ignore orphan files in FAT file systems
(faster results, although some data will not be searched)
< Back
Next >
Finish
Cancel
Help

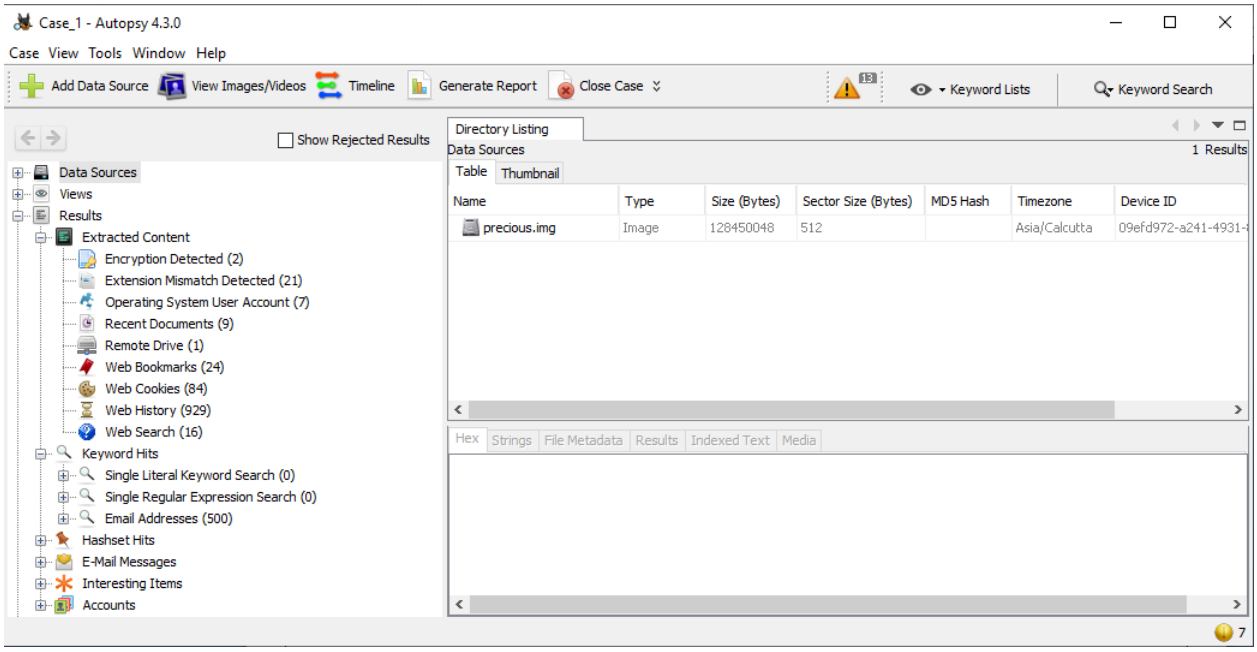
Step 5: Click on Next.



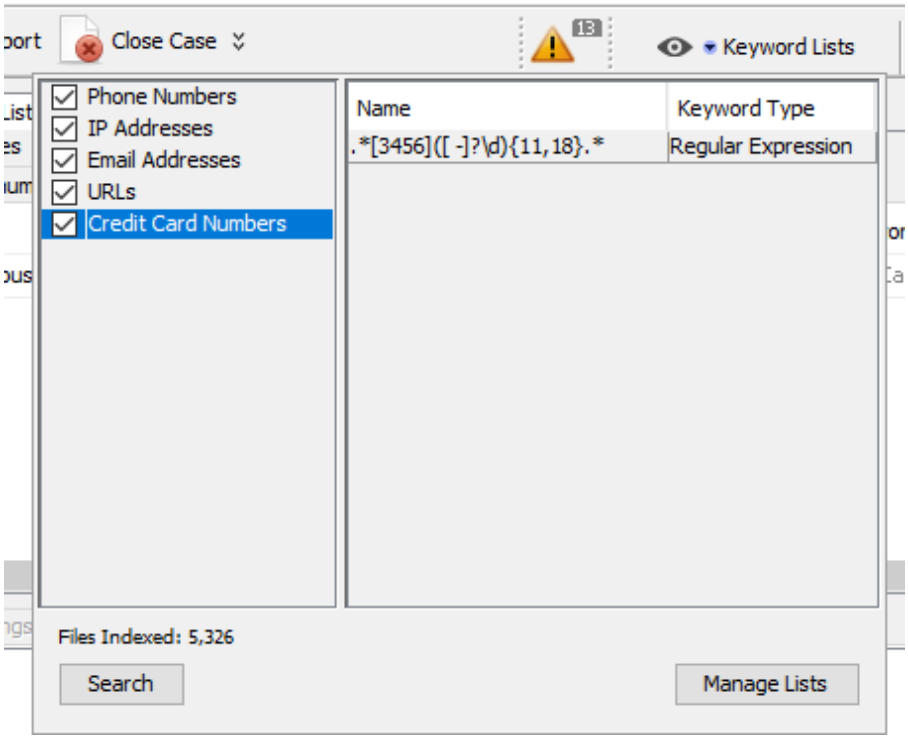
Step 6: Click on Next and wait for process to be finished.



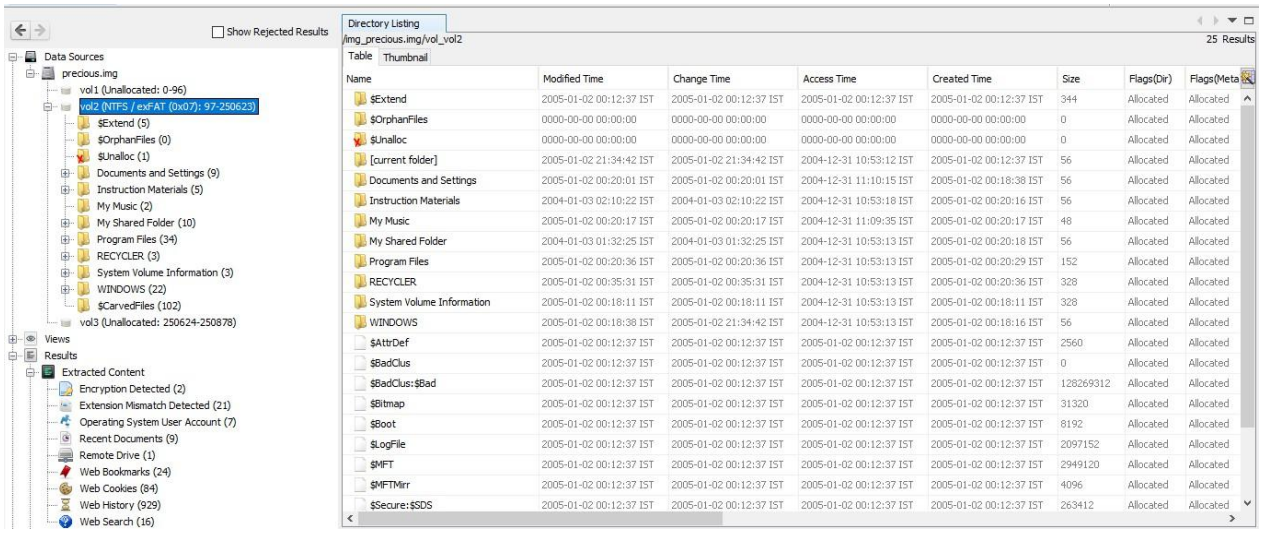
Step 7: You can explore the data from left pane expand data source, view etc.



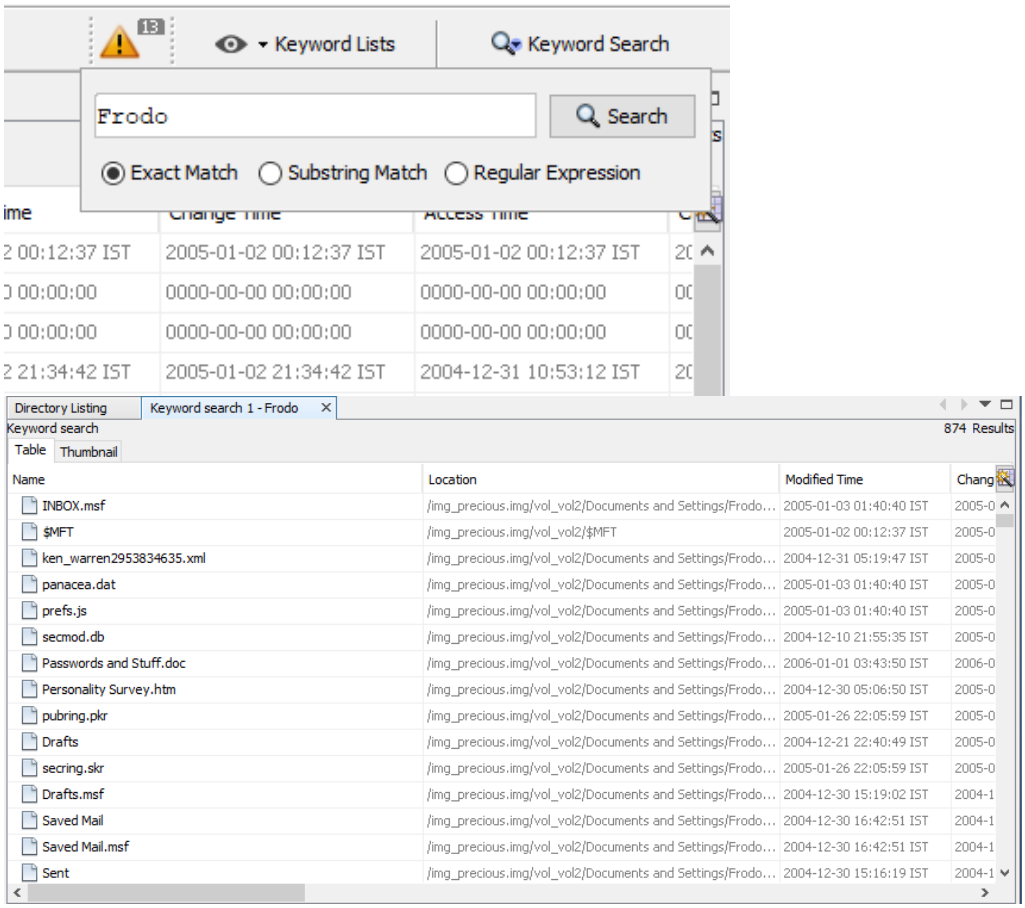
Step 8: Click on keyword list and select all check boxes to configure list.


Close Case
13
Keyword Lists
Phone Numbers
IP Addresses
Email Addresses
URLs
Credit Card Numbers
Name
Keyword Type
.*[3456]([-]?\d){11,18}.*
Regular Expression
Files Indexed: 5,326
Search
Manage Lists

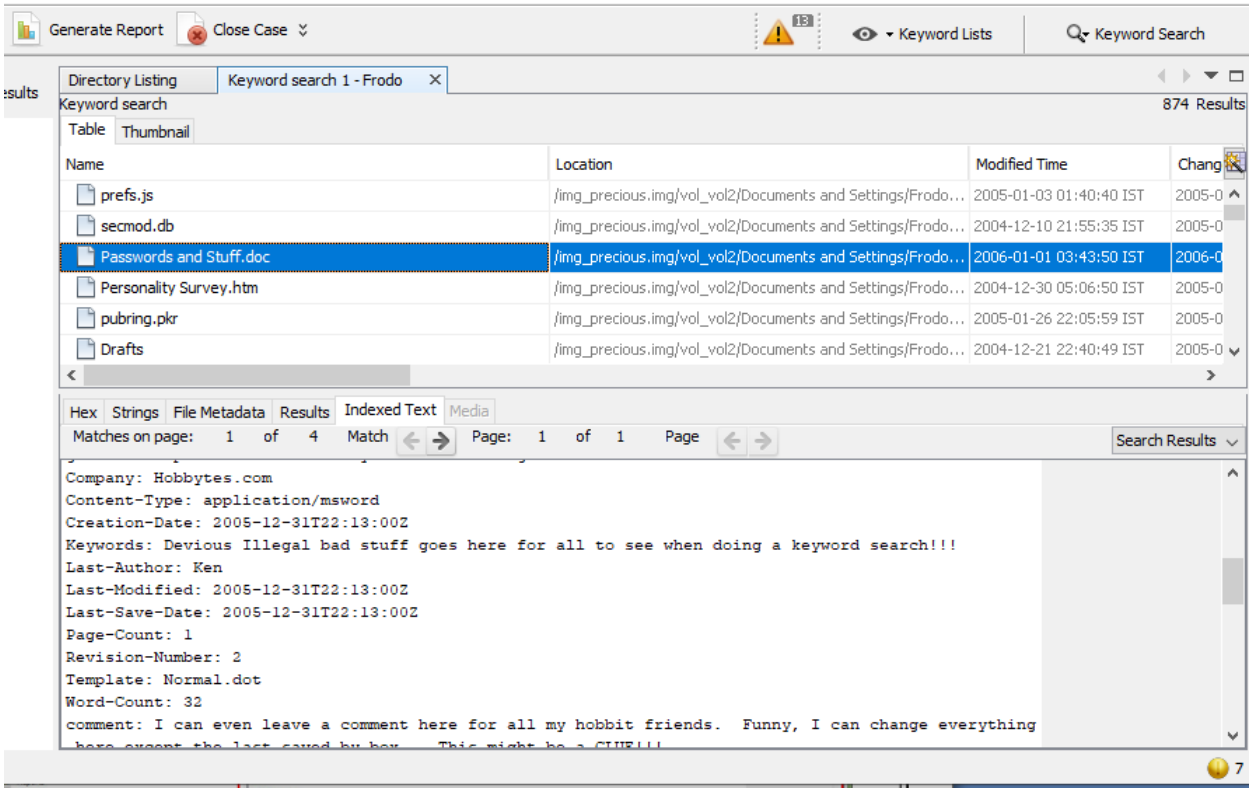
Step 9: Check for directory listing this will show all files, deleted files etc.



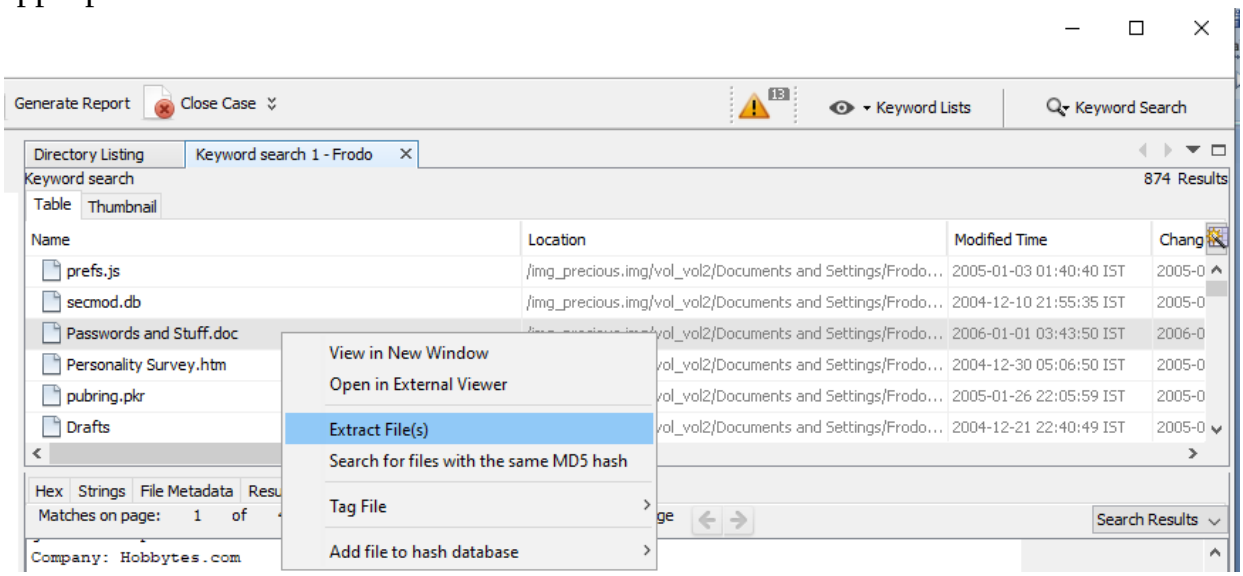
Step 10: To make keyword search click on Keyword Search and type the keyword to search, select the radio buttons for options and press Enter. This will result in all the occurrences of keyword.

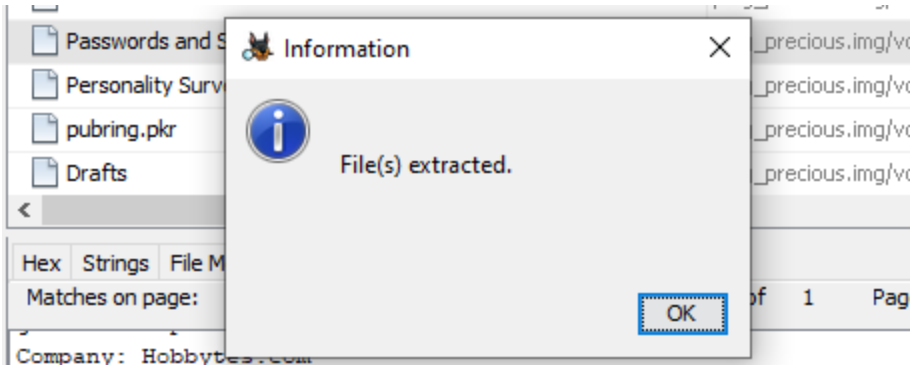

13
Keyword Lists
Keyword Search
Frodo
Search
Exact Match
Substring Match
Regular Expression
ime
Change Time
Access Time
2 00:12:37 IST
2005-01-02 00:12:37 IST
2005-01-02 00:12:37 IST
0 00:00:00
0000-00-00 00:00:00
0000-00-00 00:00:00
0 00:00:00
0000-00-00 00:00:00
0000-00-00 00:00:00
2 21:34:42 IST
2005-01-02 21:34:42 IST
2004-12-31 10:53:12 IST
Directory Listing
Keyword search 1 - Frodo
Keyword search
874 Results
Table
Thumbnail
Name
Location
Modified Time
Chang
INBOX.msf
/img_precious.img/vol_vol2/Documents and Settings/Frodo...
2005-01-03 01:40:40 IST
$MFT
/img_precious.img/vol_vol2/$MFT
2005-01-02 00:12:37 IST
ken_warren2953834635.xml
/img_precious.img/vol_vol2/Documents and Settings/Frodo...
2004-12-31 05:19:47 IST
panacea.dat
/img_precious.img/vol_vol2/Documents and Settings/Frodo...
2005-01-03 01:40:40 IST
prefs.js
/img_precious.img/vol_vol2/Documents and Settings/Frodo...
2005-01-03 01:40:40 IST
secmod.db
/img_precious.img/vol_vol2/Documents and Settings/Frodo...
2004-12-10 21:55:35 IST
Passwords and Stuff.doc
/img_precious.img/vol_vol2/Documents and Settings/Frodo...
2006-01-01 03:43:50 IST
Personality Survey.htm
/img_precious.img/vol_vol2/Documents and Settings/Frodo...
2004-12-30 05:06:50 IST
pubring.pkr
/img_precious.img/vol_vol2/Documents and Settings/Frodo...
2005-01-26 22:05:59 IST
Drafts
/img_precious.img/vol_vol2/Documents and Settings/Frodo...
2004-12-21 22:40:49 IST
secring.skr
/img_precious.img/vol_vol2/Documents and Settings/Frodo...
2005-01-26 22:05:59 IST
Drafts.msf
/img_precious.img/vol_vol2/Documents and Settings/Frodo...
2004-12-30 15:19:02 IST
Saved Mail
/img_precious.img/vol_vol2/Documents and Settings/Frodo...
2004-12-30 16:42:51 IST
Saved Mail.msf
/img_precious.img/vol_vol2/Documents and Settings/Frodo...
2004-12-30 16:42:51 IST
Sent
/img_precious.img/vol_vol2/Documents and Settings/Frodo...
2004-12-30 15:16:19 IST

Step 11: Select any file you want to analyze, and you can see details related to that file in below tabs.

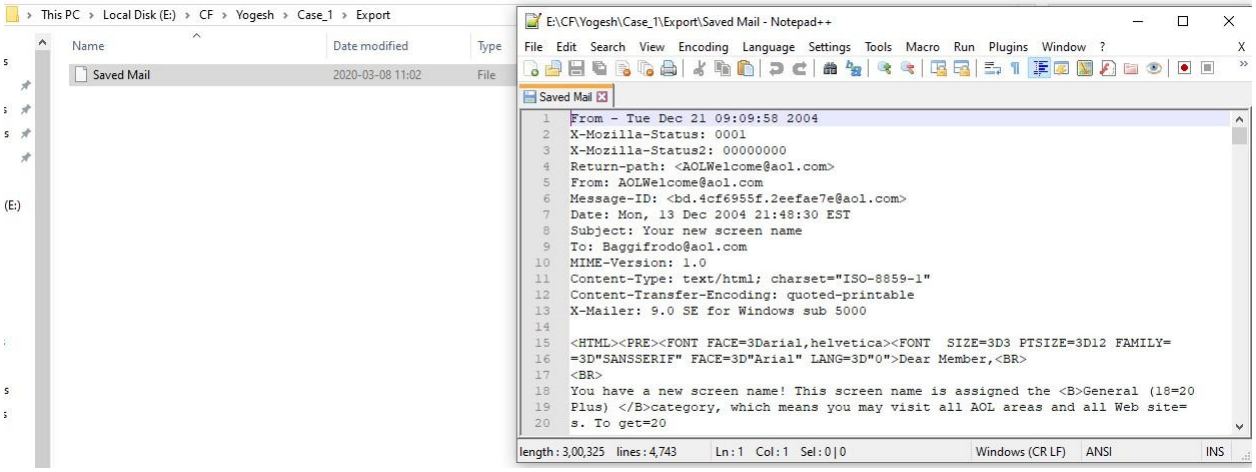


Step 12: You can also extract file just by right clicking the file and select the option Extract File. Browse the location to save that file and save with appropriate extension.

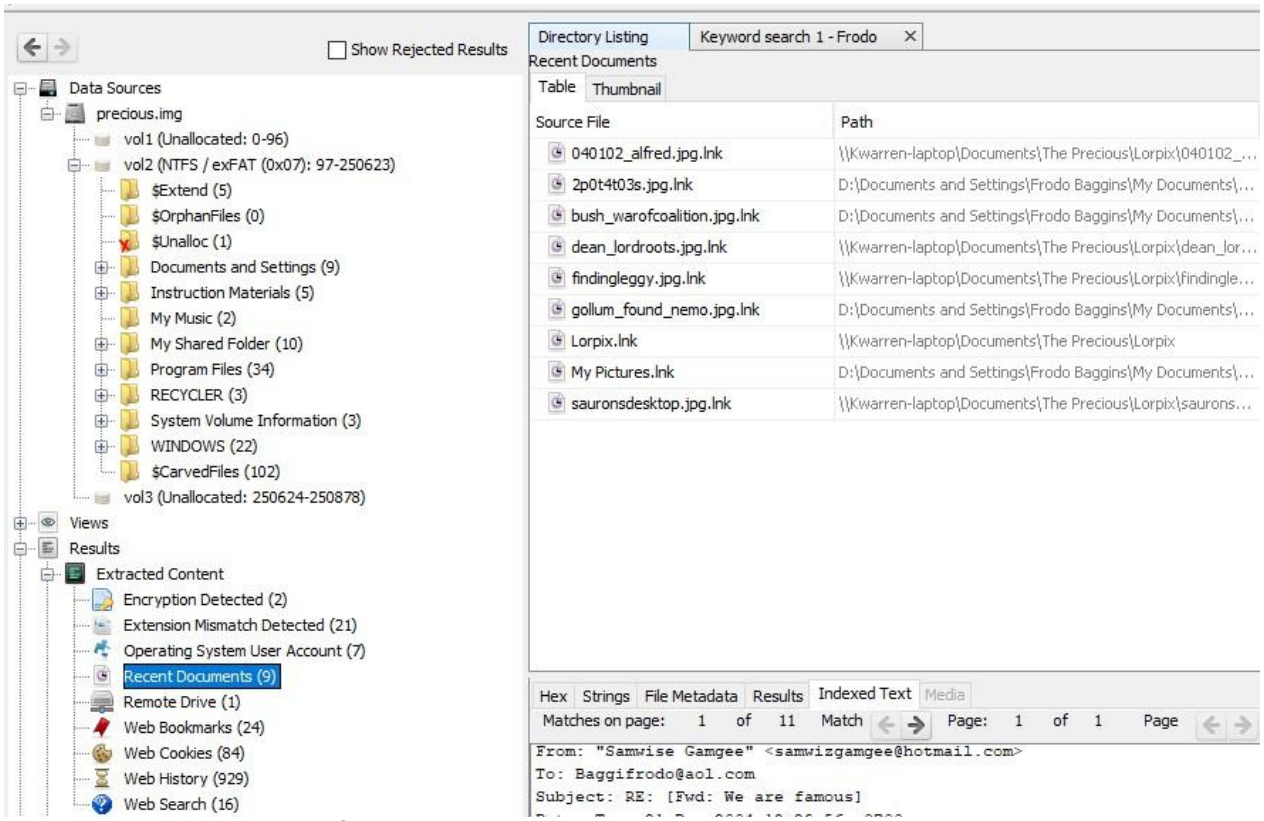




Step 13: Now browse to the location where you saved the file and open it with suitable application and you can now view the file details.
This extraction is useful in conditions where you need to show the proof or print it to present legally.

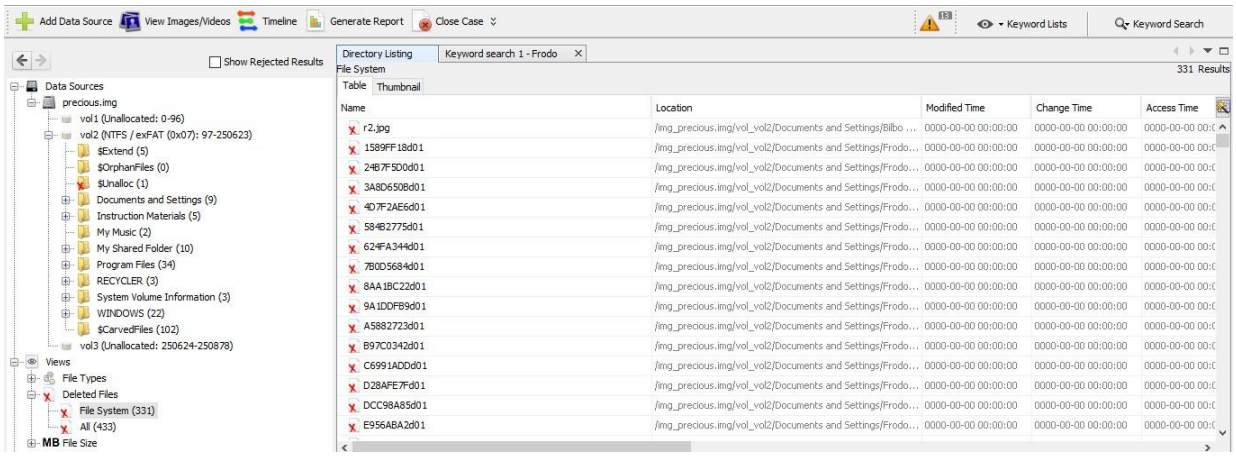


Step 14: In the left pane, you can select Recent Documents under Results to see

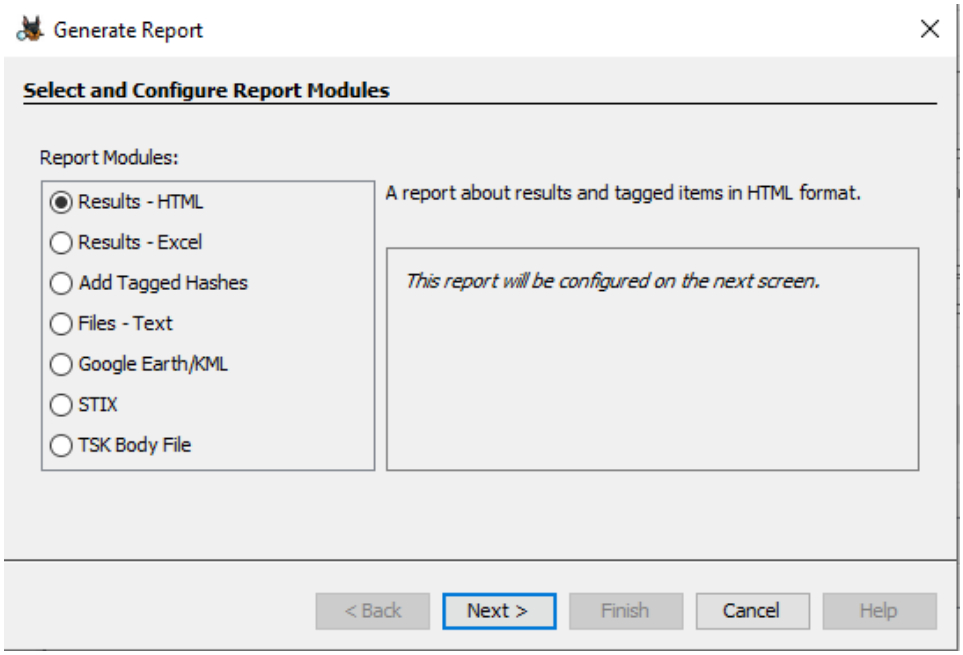


the recently accessed files and documents by the suspect, with the date and time of access.

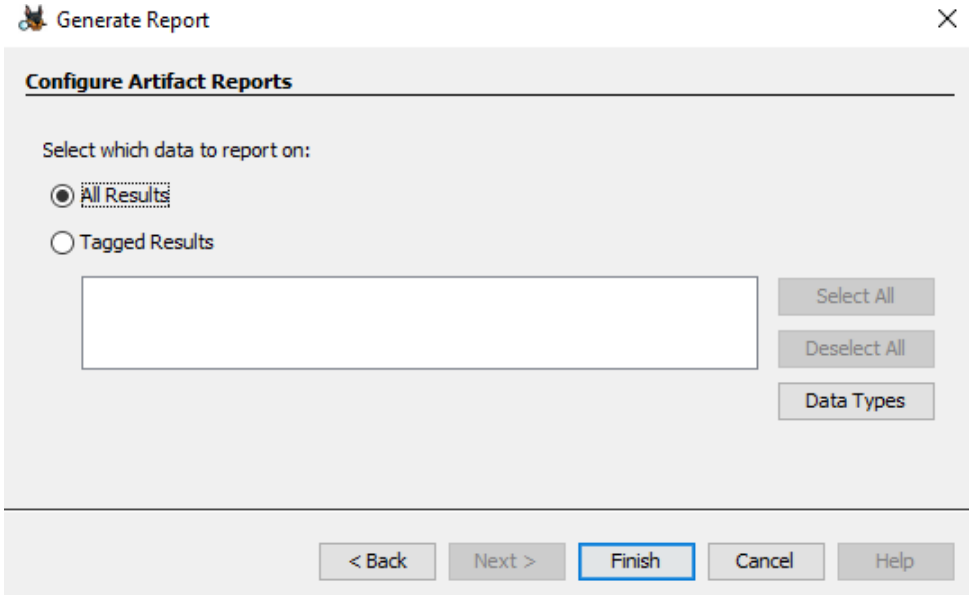
Step 15: Go to Deleted Files under View Option in left Pane to check for the file those were deleted by the suspect. Such files can be extracted but cannot be recovered. You can use any other tool to recover such files only if the memory location where it resided **didn't** override.



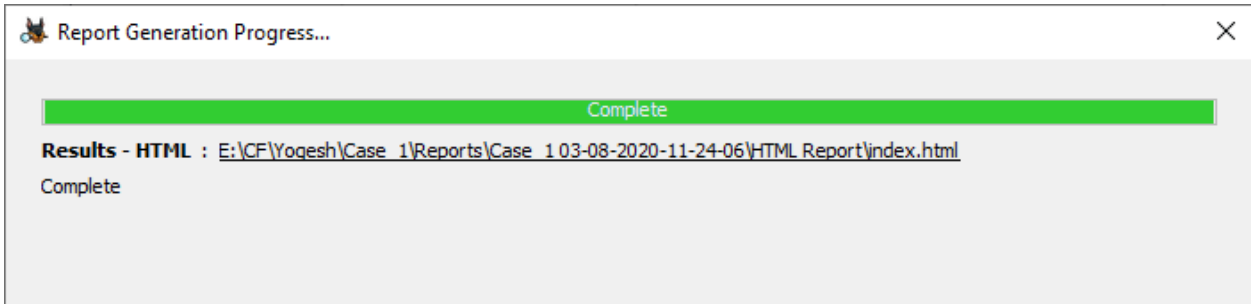
Step 16: To generate reports, click on Generate Report Option. It gives you a wizard to generate report.
Select the type you want to save results and click Next.



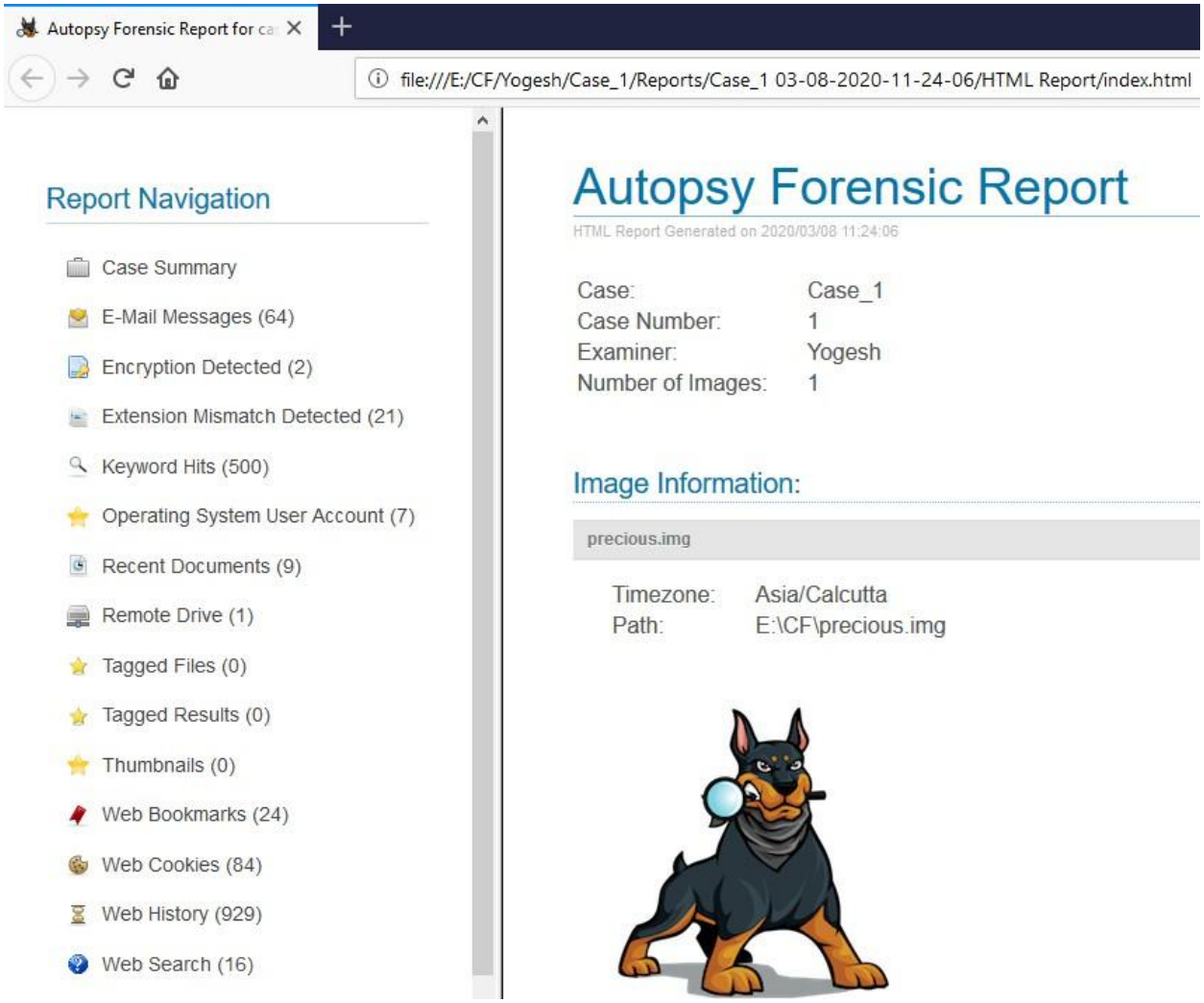
Step 17: Select All Results and click Finish.

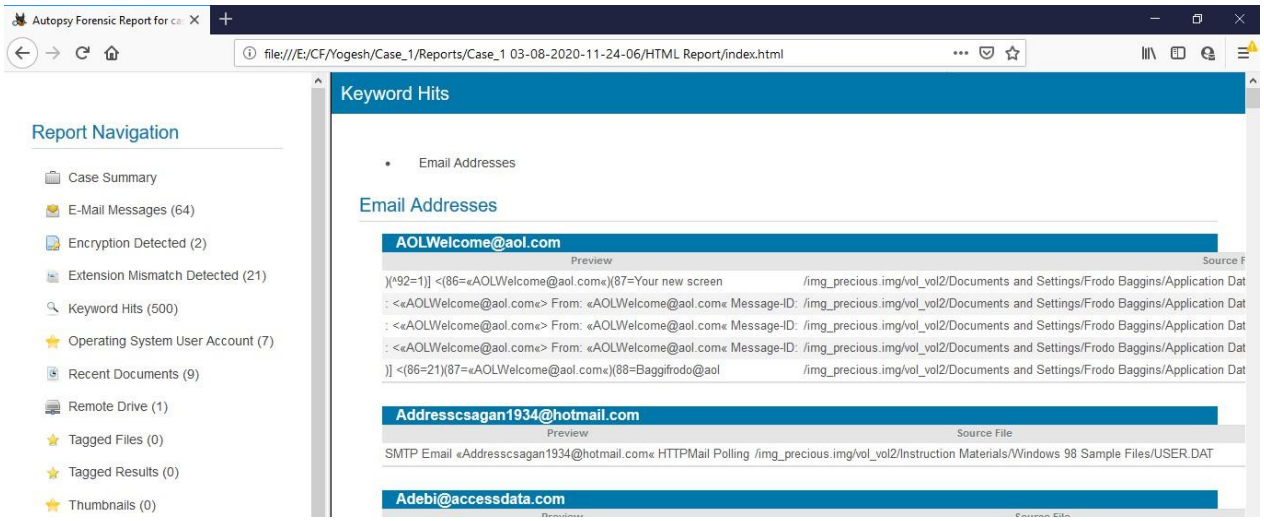


Step 18: The report generation is completed and results are stored in link specified. Click Close.



Step 19: Browse through path and open index.html file.





Conclusion: Hence, we successfully perform data analysis using sleuth kit.

PRACTICAL – 2

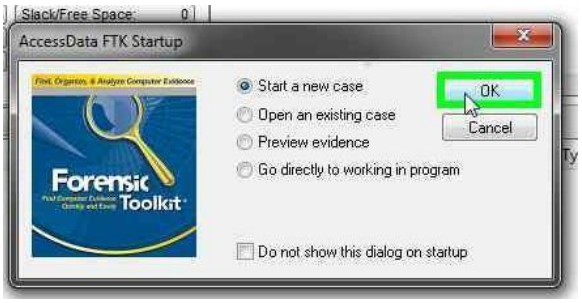
AIM: Using Windows Forensics using FTK

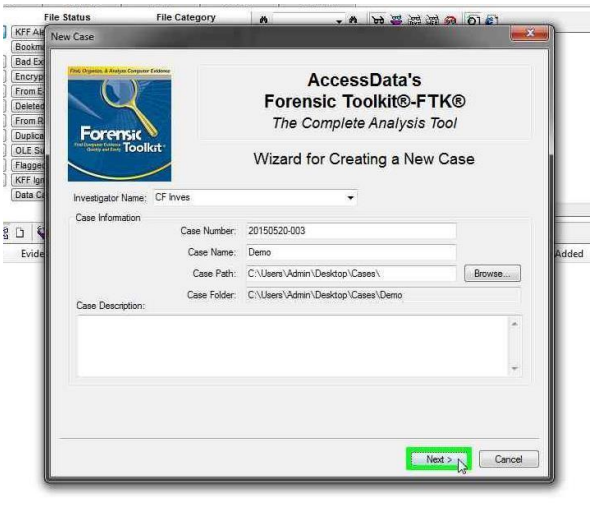
Tasks:

- **Creation of a Case**
- **Adding forensic image as evidence**
- **Analysing files of the image**
- **Creating bookmarks**
- **Searching**
- **Report Generation**

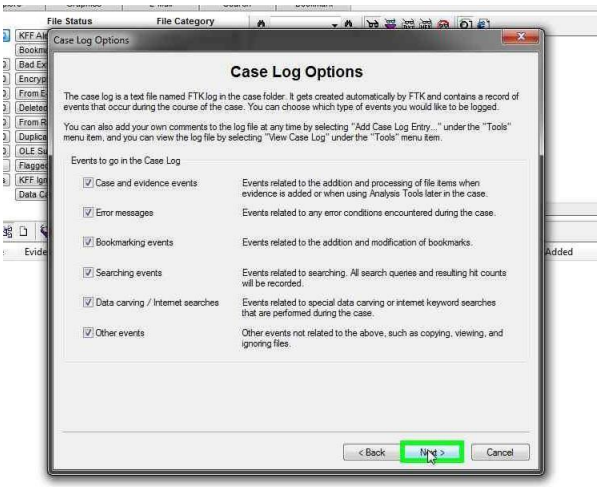
Creation of a Case

Start a new case and input the respective details

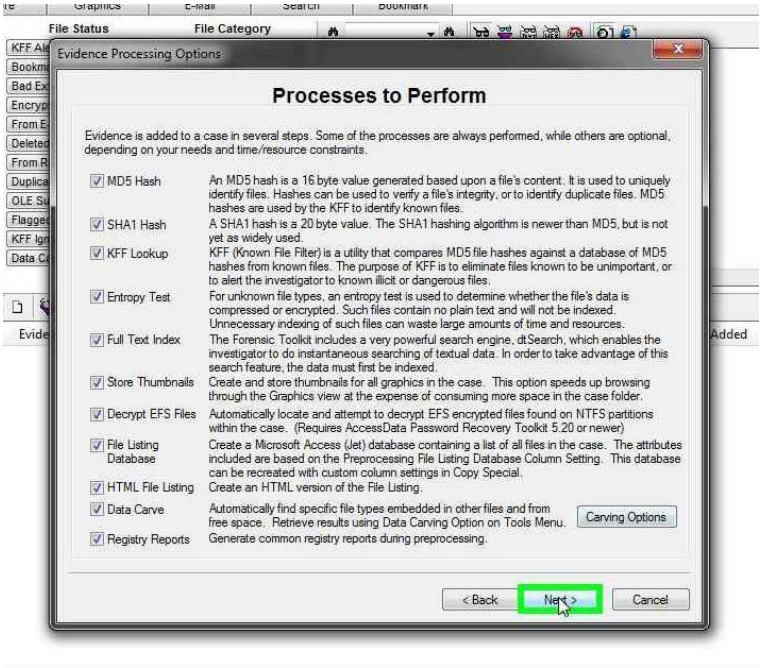




Case Log is the inbuilt logging utility. As you perform an investigation, it will keep a track of the modules used, searches performed, etc. It is like a journal that tells a lawyer/judge that you really have performed these steps.

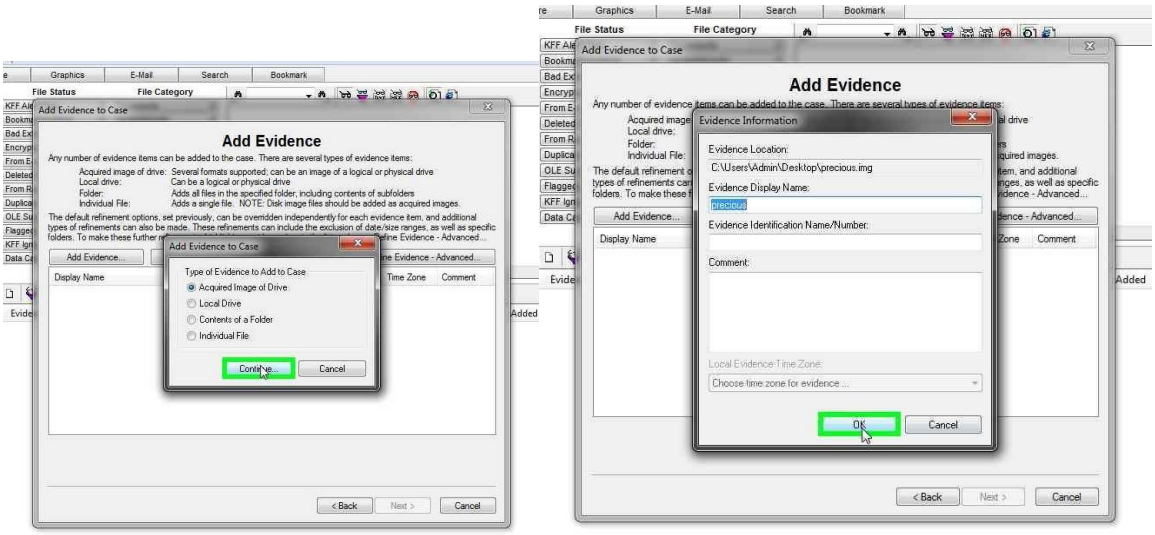


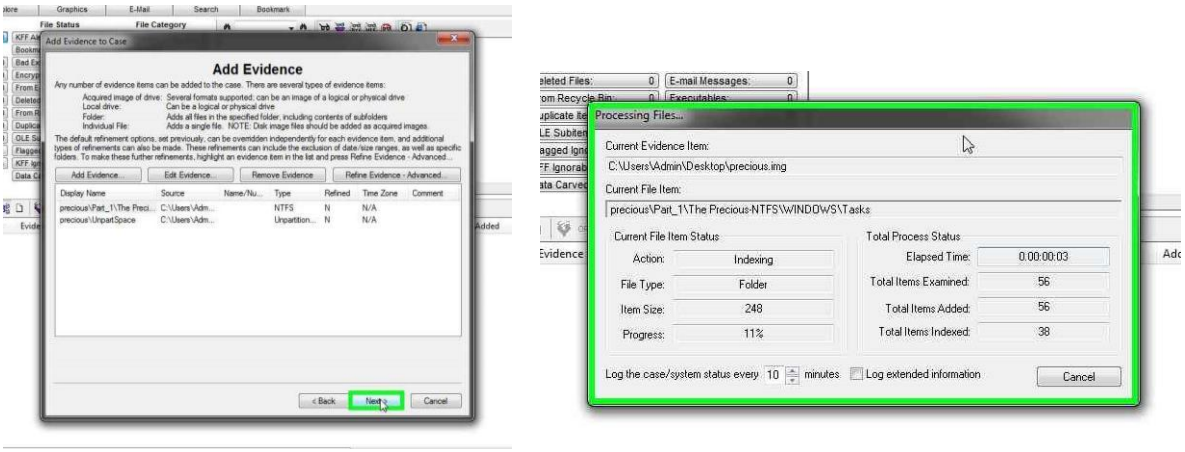
When adding the forensic image to the case, you need to specify the different processes that FTK should perform while importing. Processes like generating Hash values for the files, indexing the files, storage of thumbnails, creation of an Access Db for file listing, etc.



Adding forensic image as evidence

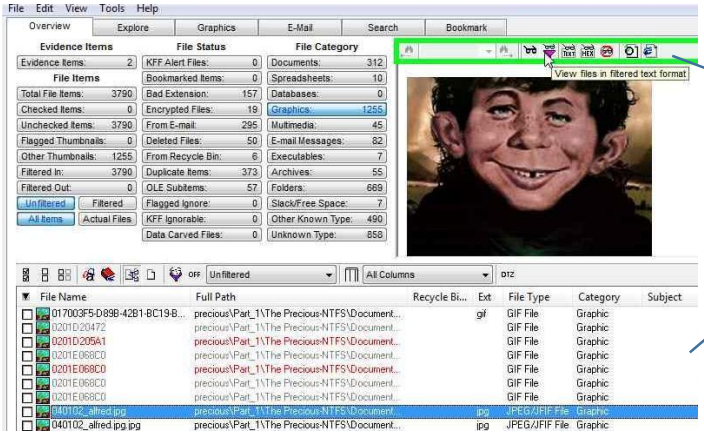
Add the Image file as Evidence. You can add an acquired image file, perform acquisition on a local drive or add an individual file (like a .pst). Fill in the required details. When the case setup is complete, FTK will begin processing the evidence.

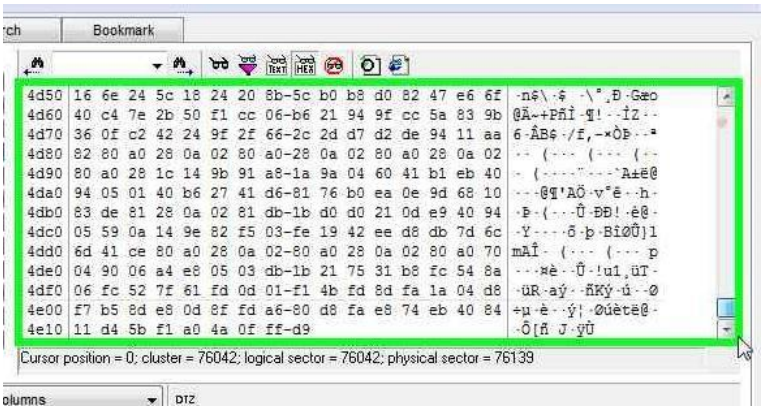


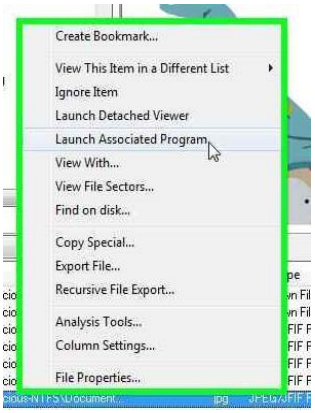


Analysing files of the image

Overview tab shows us an overview of the items in the image and lets us drill down depending on various parameters like file types. When we click on a file on the file list, we can see a preview of it on the top right. There are different preview formats like text, hex.


File Edit View Tools Help
Overview
Explore
Graphics
E-Mail
Search
Bookmark
Evidence Items
File Status
File Category
View files in filtered text format
File Name
Full Path
Recycle Bi...
Ext
File Type
Category
Subject
Unfiltered
All Columns
Preview Format
File List





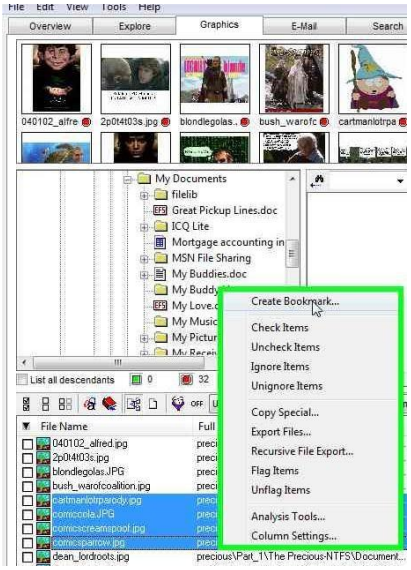
To view the file we have different options. We can view it with the program associated with its extension or launch the inbuilt viewer.

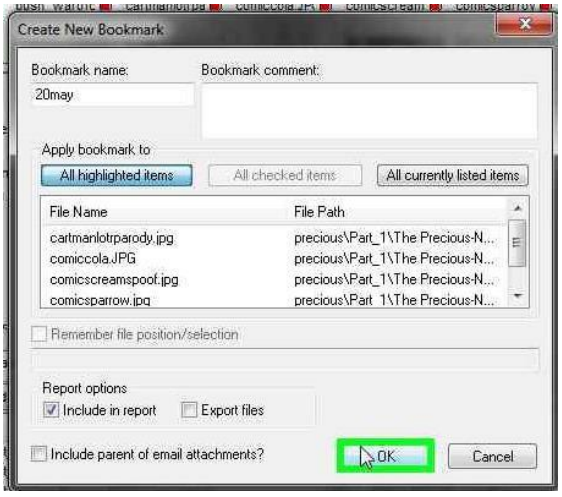
File Properties will show us the various properties of that file like Data/Time created, size, etc.

We can export the file from the case onto the host machine desktop

Creating Bookmarks

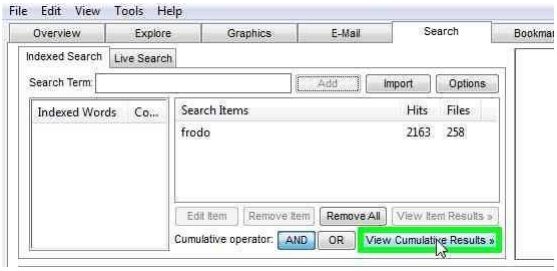
To create a bookmark, right click on any file(s) and choose Create Bookmark. Give the name for the bookmark

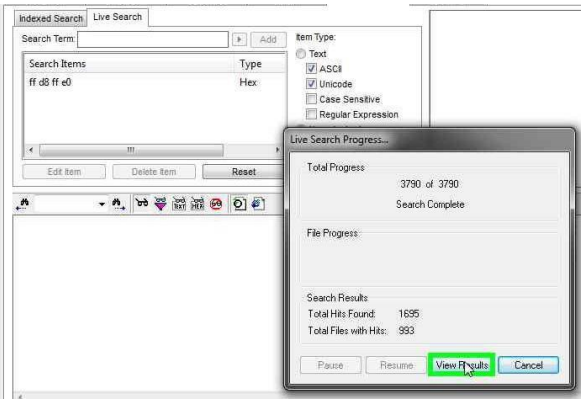




Searching

We can perform an Indexed Search or a Live Search from the Search tab. Search string can be plain text, or we can specify a hex string and search file contents for that hex string (Eg. Search for images using FFD8 FFE0, which is the header for JPG images)



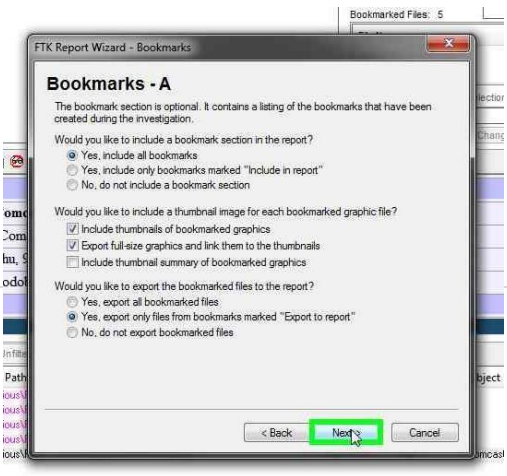


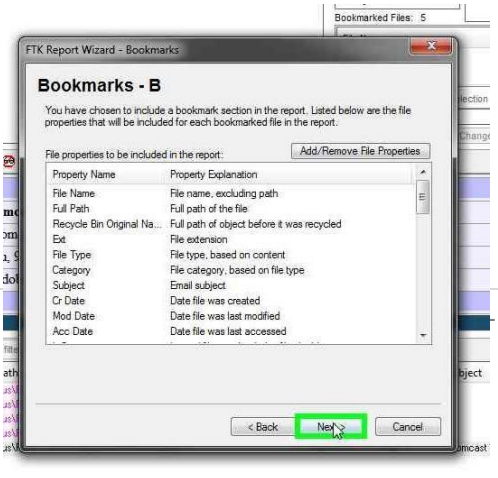
Report Generation

Make sure you have some bookmarks made Go to File – Report Wizard

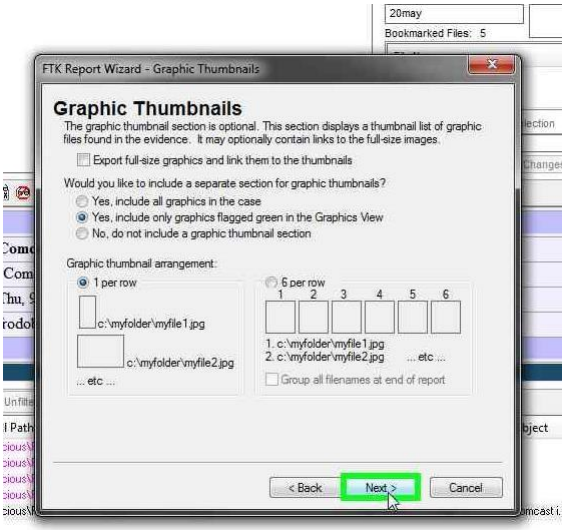
Bookmarks – A will ask you to choose various options you want to set for bookmarks

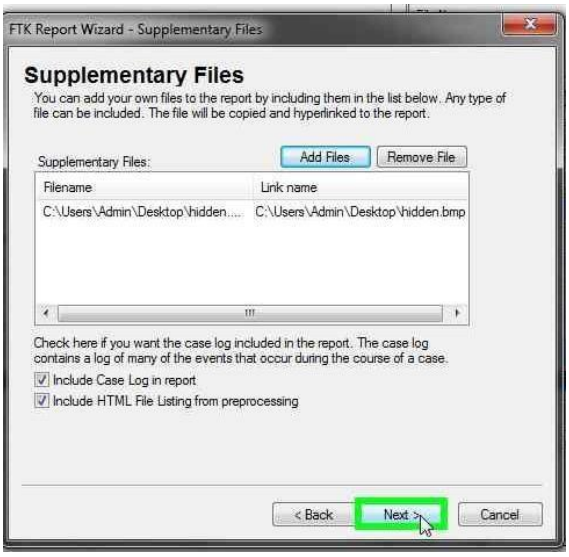
Bookmarks – B, will ask you to choose the various file properties to be displayed for the bookmarks



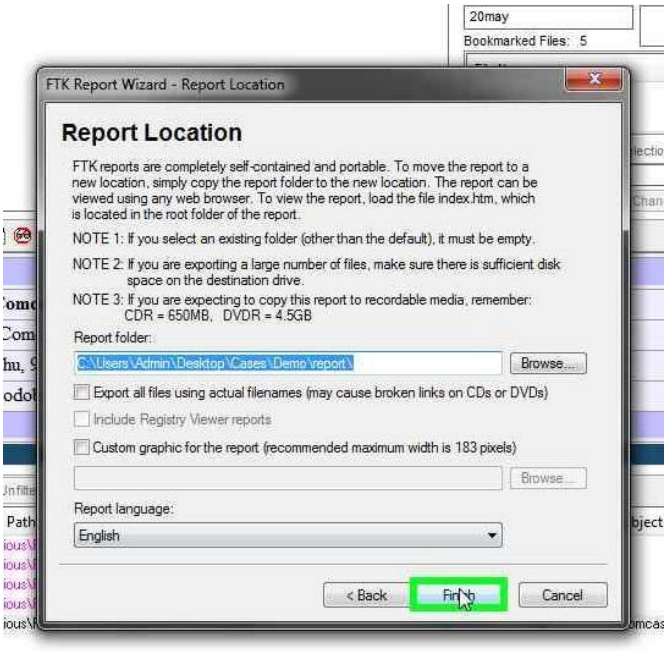


You can select whether you want to display Graphics Thumbnails in the report. If you want to add additional files (Eg. PDF of Affidavit) you can attach it in the Supplementary Files screen

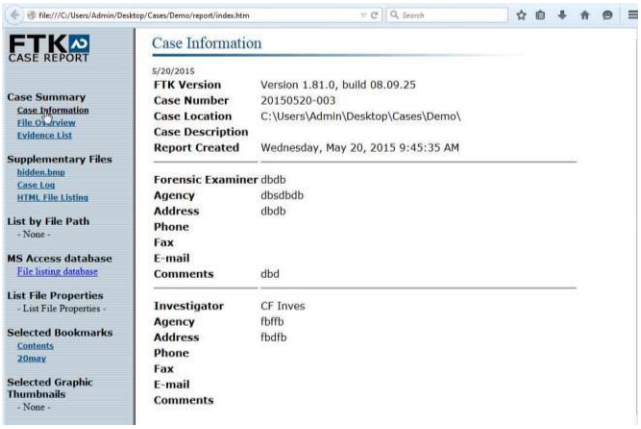




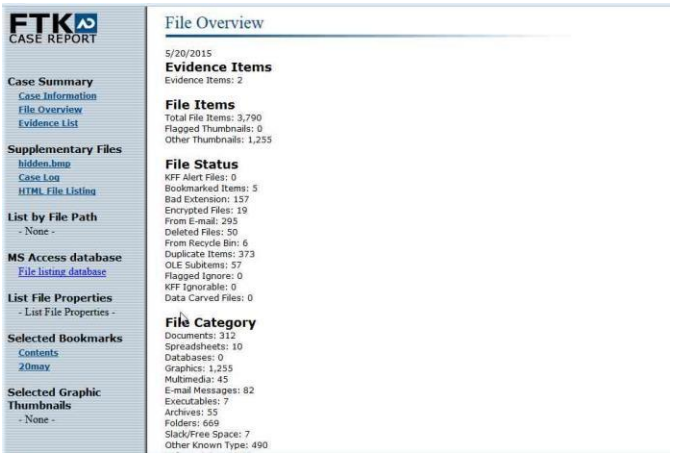
Choose the location to store the report. After the report is created, you can view the report



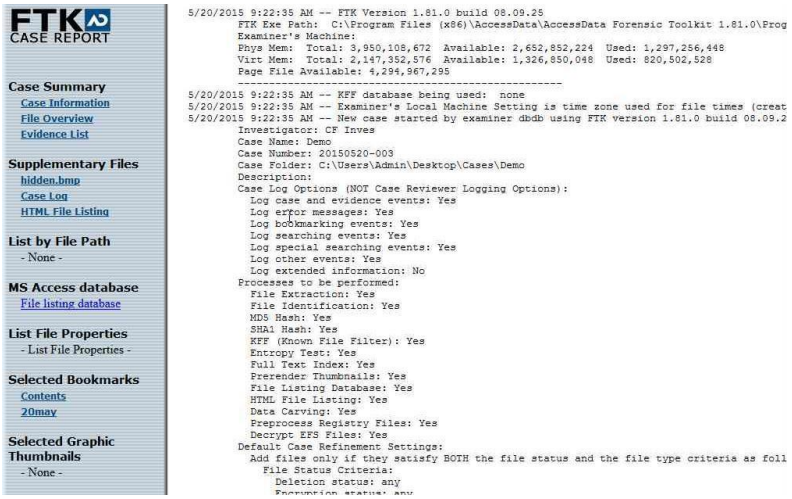
Case Information will show descriptive information about the Case depending on what was filled during the Case creation time



File overview will give an overview of the files found by FTK during evidence import



Case Log will show information about the various actions that were performed in FTK



FTK
CASE REPORT

Case Summary
- Case Information
- File Overview
- Evidence List

Supplementary Files
- hidden.bmp
- Case Log
- HTML File Listing

List by File Path
- None -

MS Access database
- File listing database

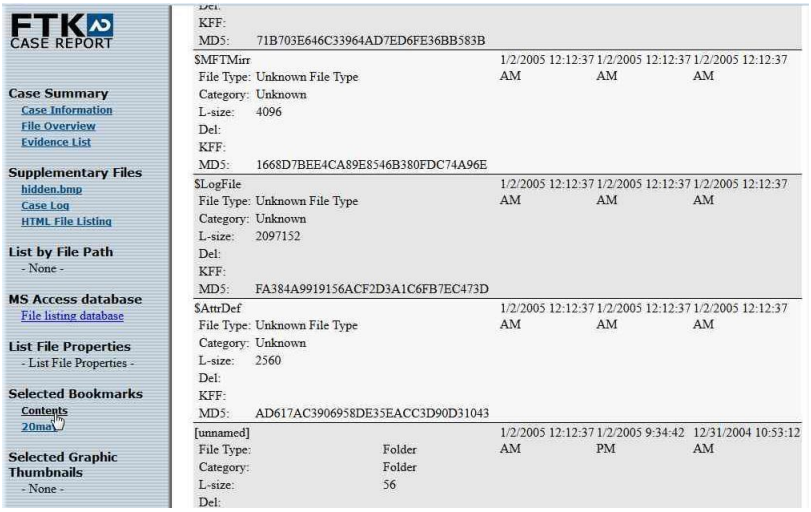
List File Properties
- List File Properties -

Selected Bookmarks
- Contents
- 20may

Selected Graphic Thumbnails
- None -

```
5/20/2015 9:22:35 AM -- FTK Version 1.81.0 build 08.09.25
        FTK Exe Path:  C:\Program Files (x86)\AccessData\AccessData Forensic Toolkit 1.81.0\Prog
        Examiner's Machine:
        Phys Mem:  Total: 3,950,108,672  Available: 2,652,852,224  Used: 1,297,256,448
        Virt Mem:  Total: 2,147,352,576  Available: 1,326,850,048  Used: 820,502,528
        Page File Available: 4,294,967,295
        ----------------------------------------------------------
5/20/2015 9:22:35 AM -- KFF database being used:  none
5/20/2015 9:22:35 AM -- Examiner's Local Machine Setting is time zone used for file times (creat
5/20/2015 9:22:35 AM -- New case started by examiner dbdb using FTK version 1.81.0 build 08.09.2
        Investigator: CF Inves
        Case Name: Demo
        Case Number: 20150520-003
        Case Folder: C:\Users\Admin\Desktop\Cases\Demo
        Description:
        Case Log Options (NOT Case Reviewer Logging Options):
          Log case and evidence events: Yes
          Log error messages: Yes
          Log bookmarking events: Yes
          Log searching events: Yes
          Log special searching events: Yes
          Log other events: Yes
          Log extended information: No
        Processes to be performed:
          File Extraction: Yes
          File Identification: Yes
          MD5 Hash: Yes
          SHA1 Hash: Yes
          KFF (Known File Filter): Yes
          Entropy Test: Yes
          Full Text Index: Yes
          Prerender Thumbnails: Yes
          File Listing Database: Yes
          HTML File Listing: Yes
          Data Carving: Yes
          Preprocess Registry Files: Yes
          Decrypt EFS Files: Yes
        Default Case Refinement Settings:
          Add files only if they satisfy BOTH the file status and the file type criteria as foll
            File Status Criteria:
              Deletion status: any
              Encryption status: any
```

If any bookmarks were attached, then Selected Bookmarks will show them



Questions to be asked:

1. To list information about a file (Date/Time, Properties, location on the disk, extension)
2. To search for particular files/extensions using Live Search
3. Report Generation having specific bookmarks

PRACTICAL -3

AIM: Creating a forensic image using FTK imager

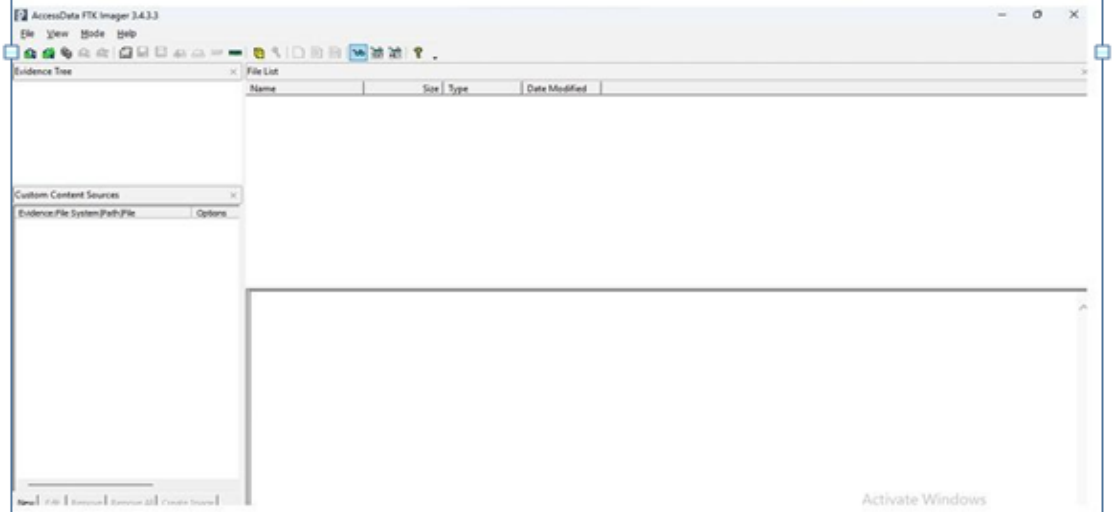
Aim:

Creating a Forensic Image using FTK Imager/Encase Imager:

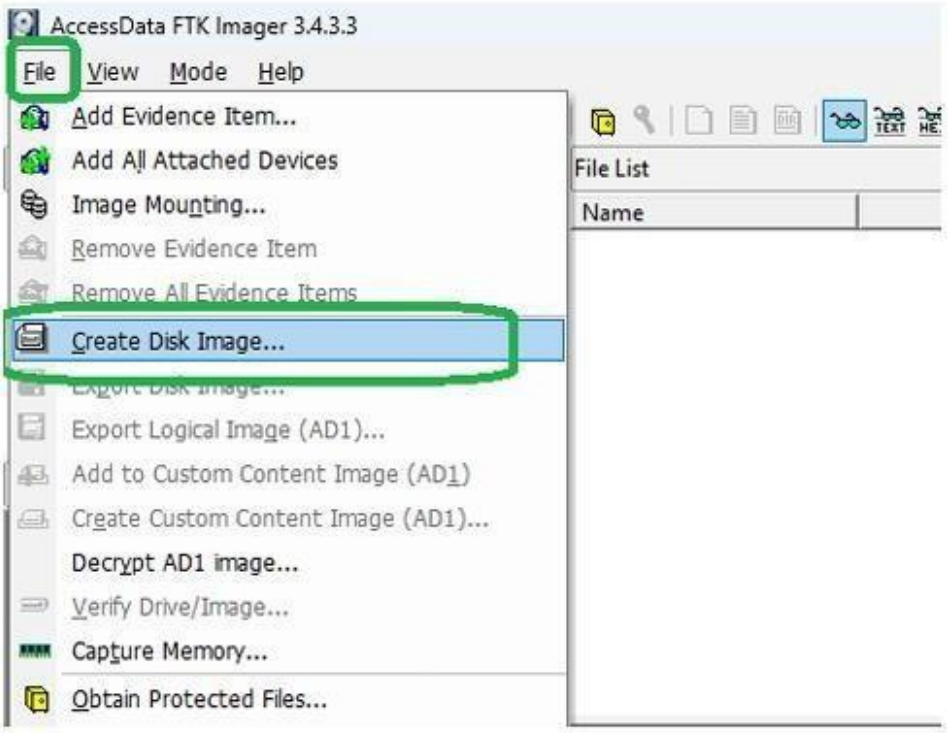
- Creating Forensic Image
- Check Integrity of Data
- Analyze Forensic Image

Practical:

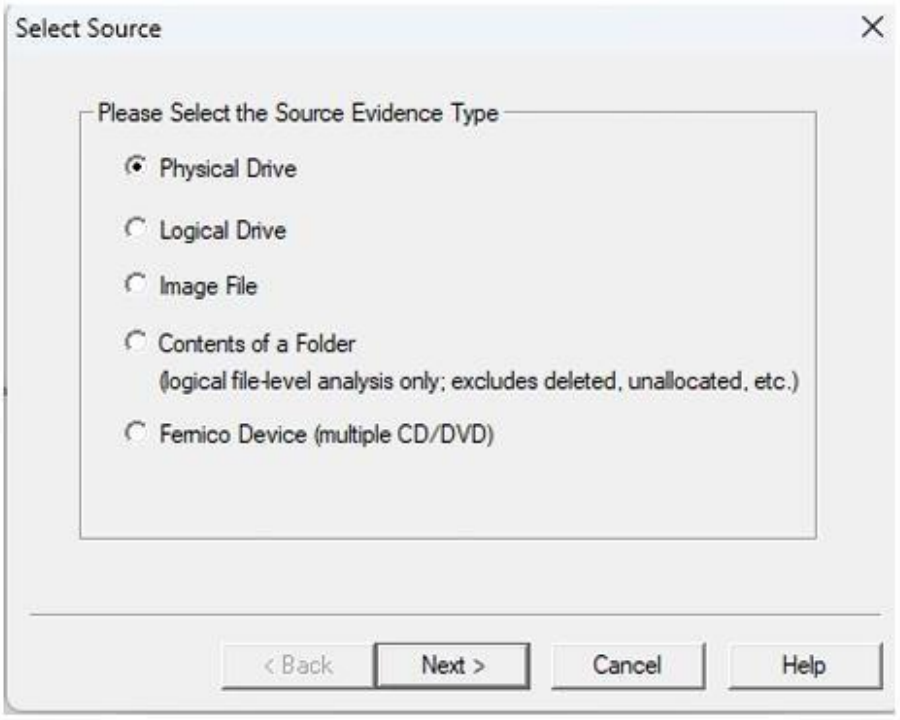
In this Practical we are going to use the FTK Imager to create Images of the evidences



Go to File → Create Disk Image

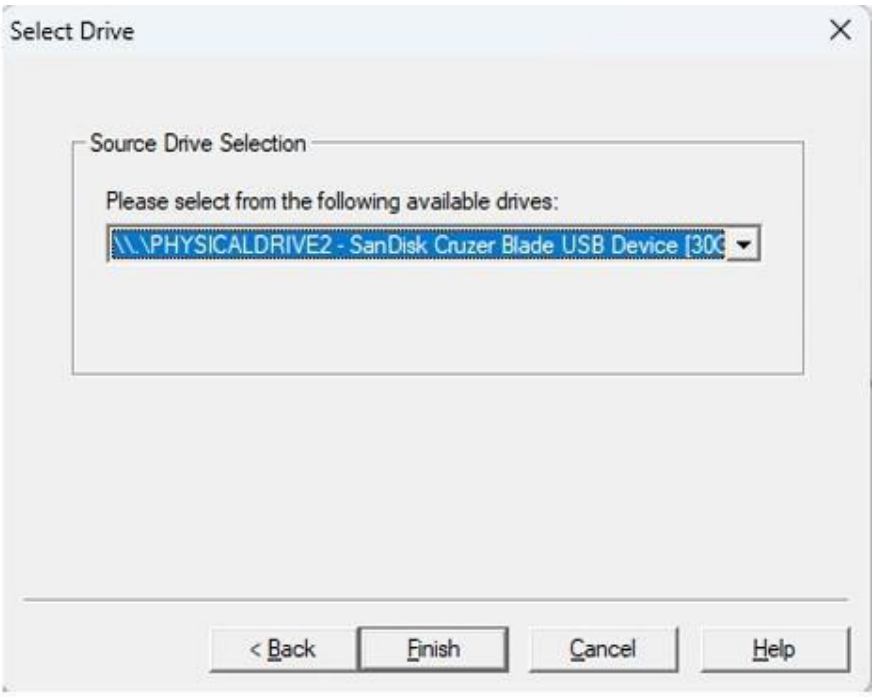


Select the source evidence type

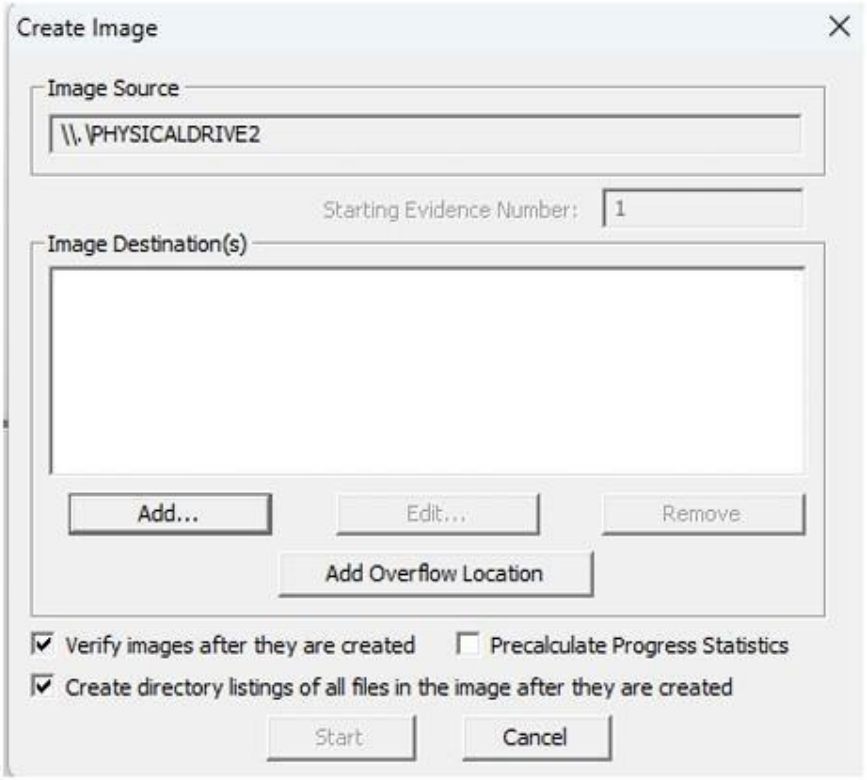


Here we are going to select the physical drive and proceed

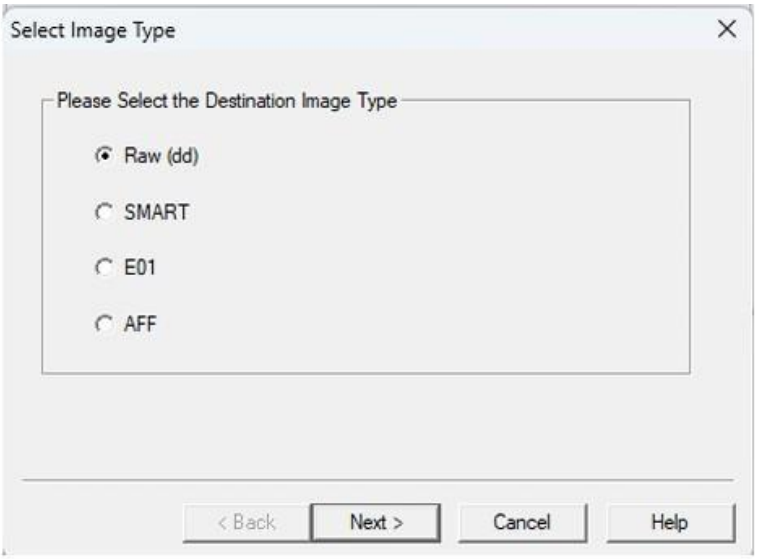
Then we browse the location of the **Pen drive** and click Finish



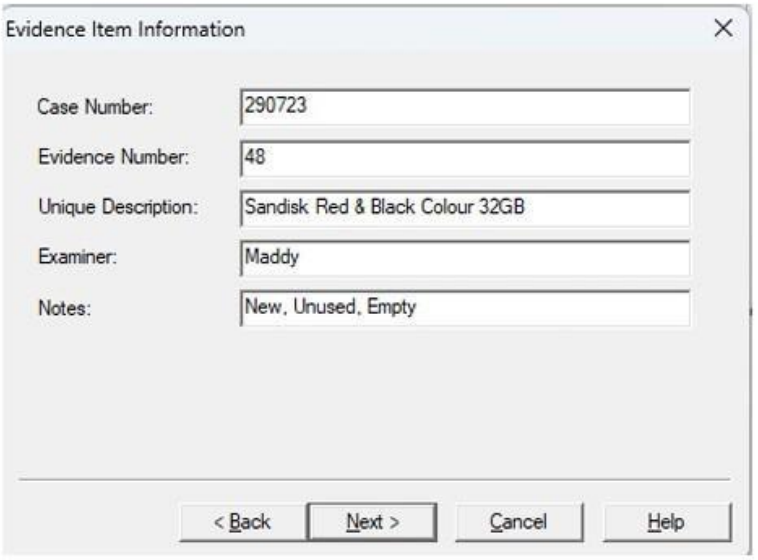
Now we add the location to create images



In this we are going to select the **raw (dd)** format

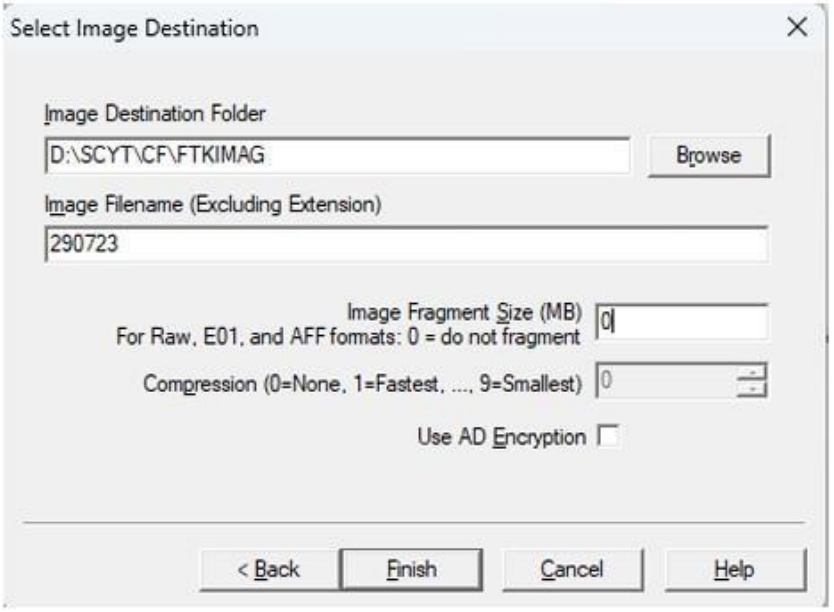


And now we fill the details required for the case

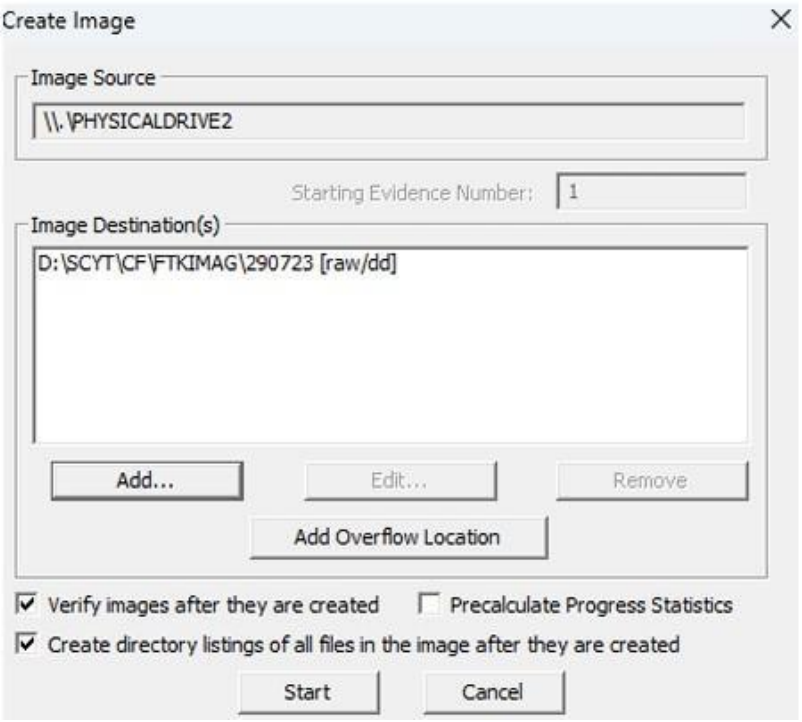


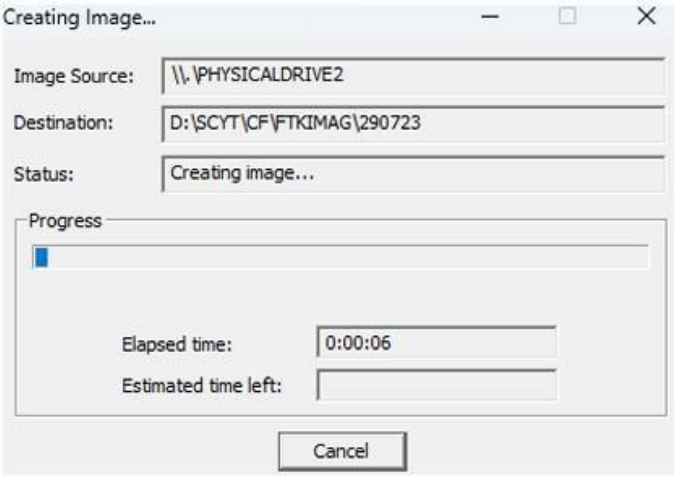
Create a folder to save the images to store in the system disk as the pen drive size cannot be stored in the same drive

Then paste that location to save the images and click Finish

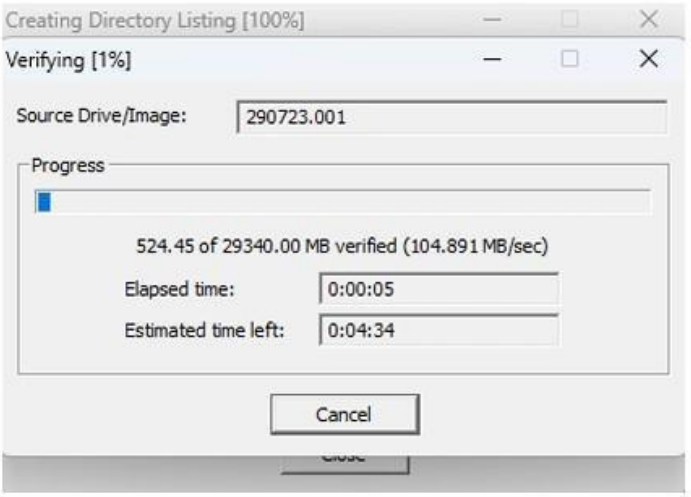


Then Click on Start and wait until the imaging is done

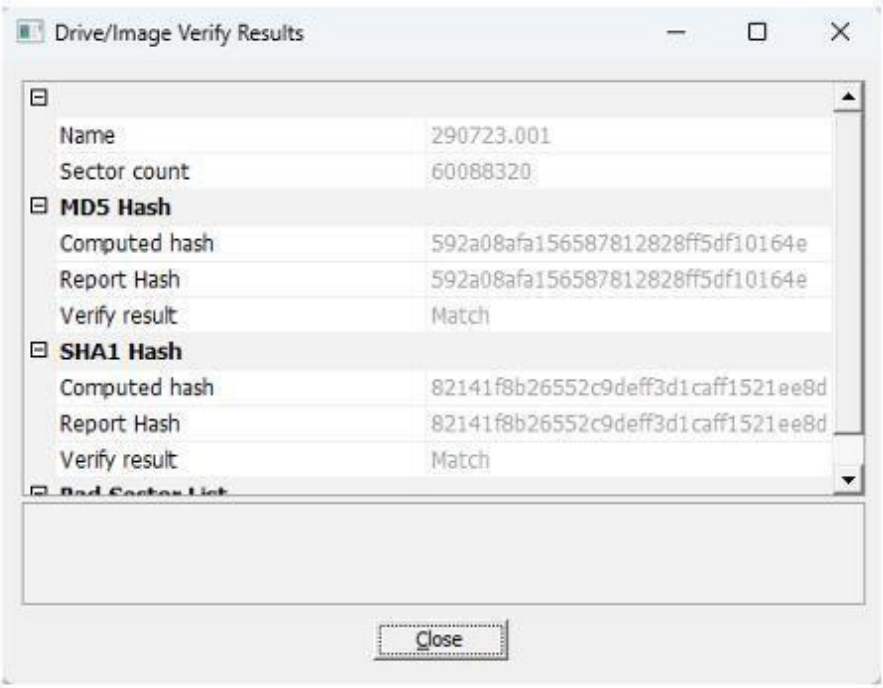




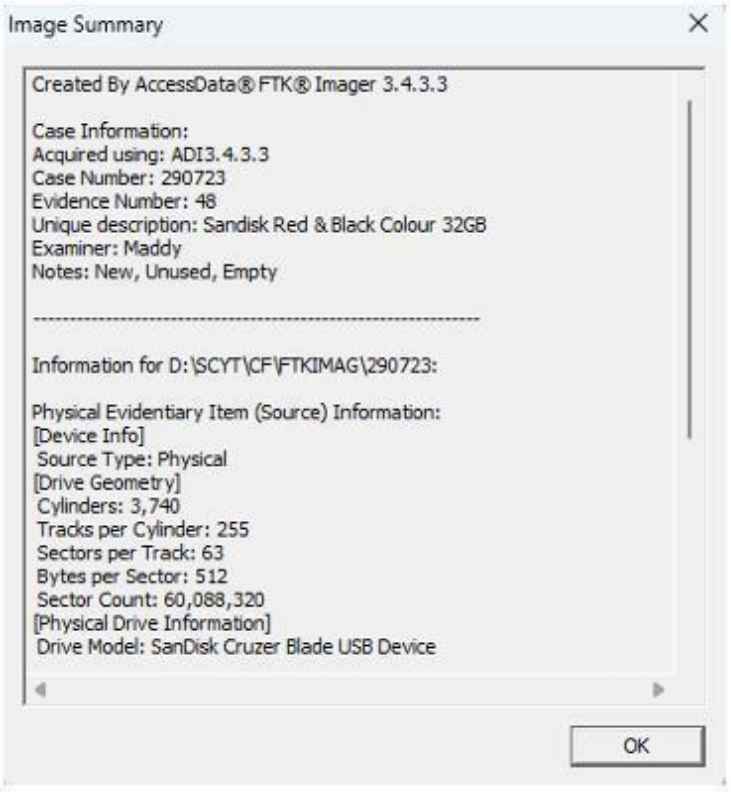
Now it will verify



This is the Hash Value CheckSum given if it matches the original values then the evidence is original if not the evidence is been misplaced

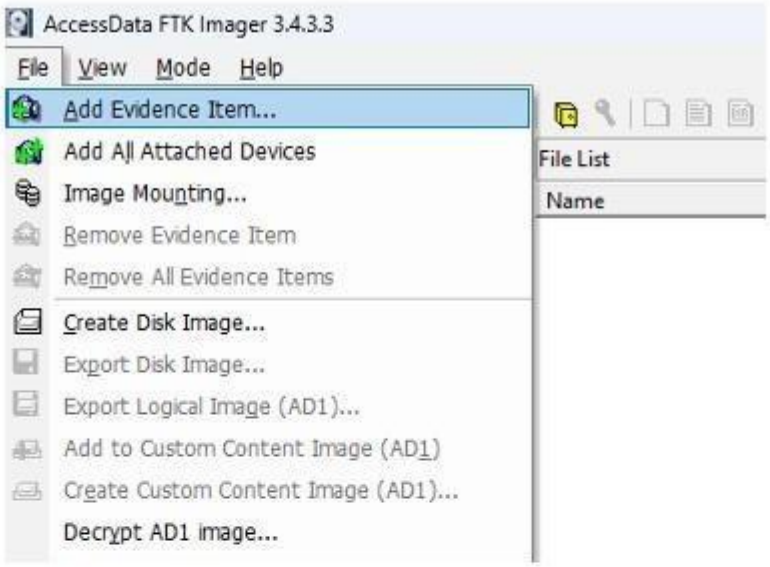


We take the image summary

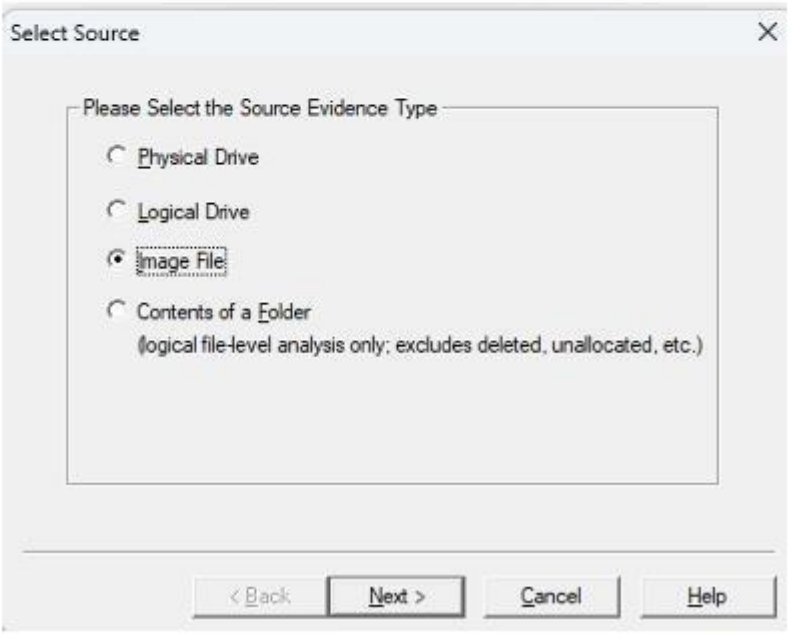


Now we are going to view the images in the FTK Imager

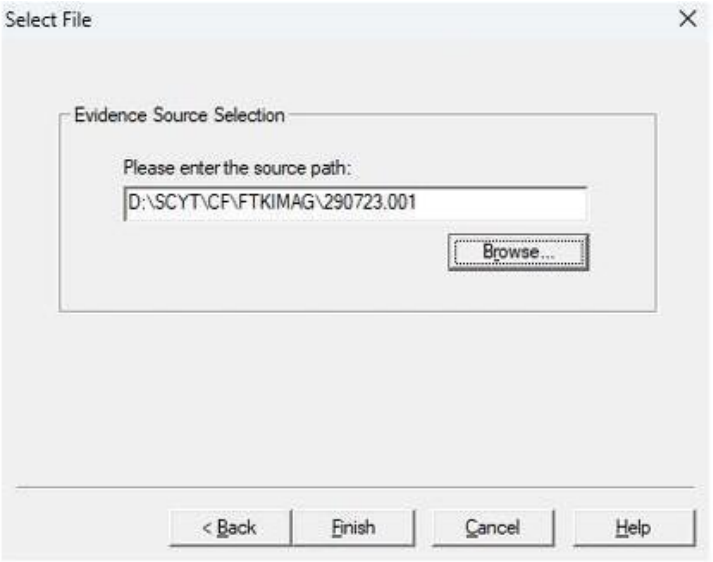
Go to File → Add Evidence Item



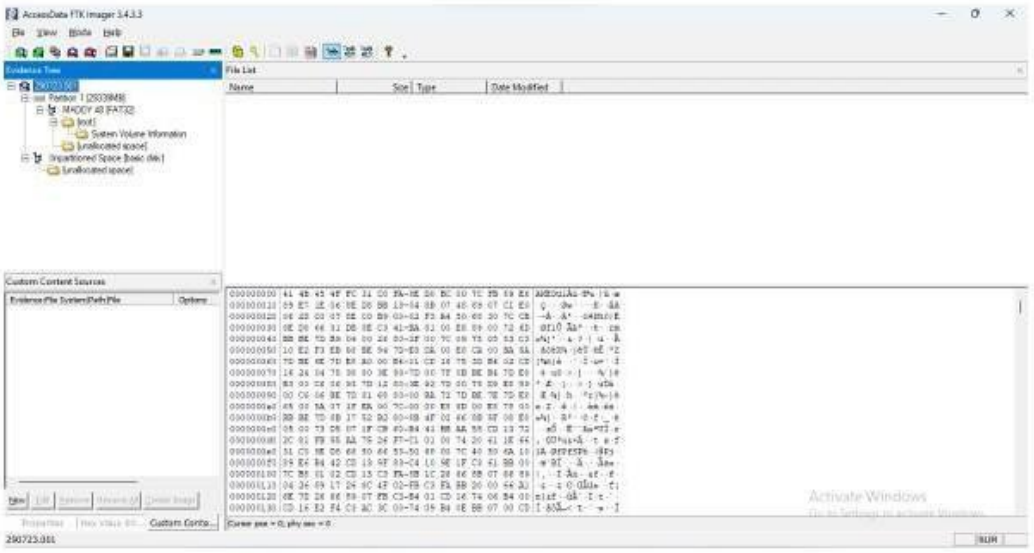
Then select the type of the evidence here it is Image File

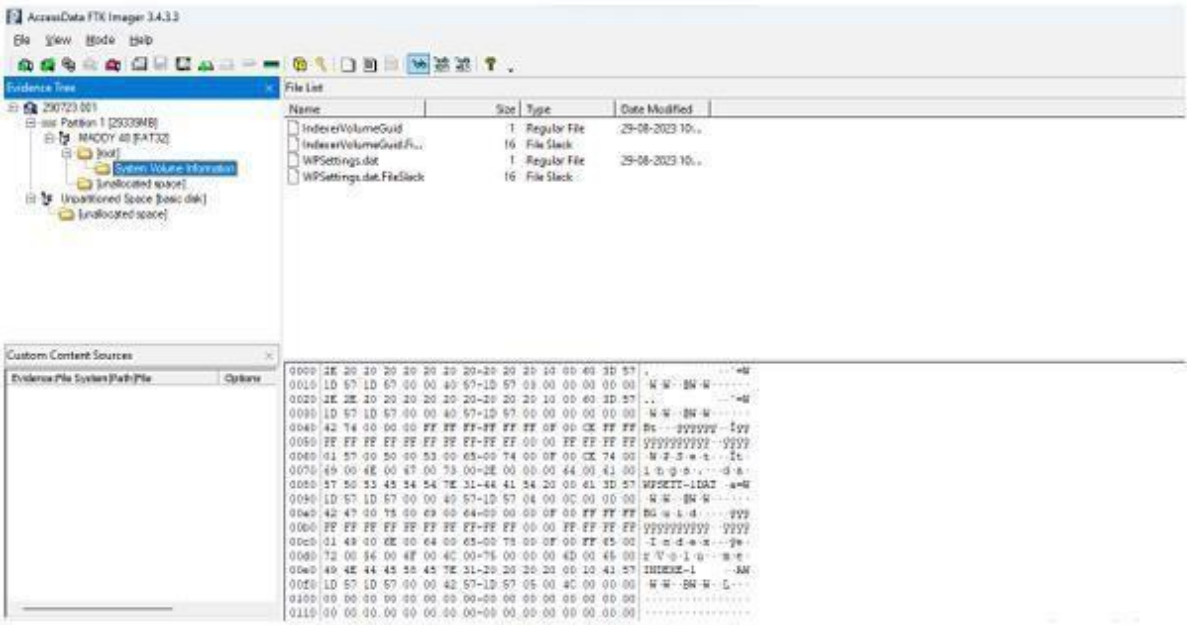


Give the directory of the images created using the FTK Imager and click Finish



Here we can see the data shown by the FTK Imager




AccessData FTK Imager 3.4.3.3
File View Mode Help
Evidence Tree
290723-001
Partition 1 [29339MB]
NIKKY 48 [FAT32]
[root]
System Volume Information
[unallocated space]
Unpartitioned Space [basic disk]
[unallocated space]
File List
Name Size Type Date Modified
IndexerVolumeGuid 1 Regular File 29-08-2023 10:..
IndexerVolumeGuid.Fi... 16 File Slack
WPSettings.dat 1 Regular File 29-08-2023 10:..
WPSettings.dat.FileSlack 16 File Slack
Custom Content Sources
Evidence:File System|Path|File
Options

PRACTICAL NO. 4

Aim: Recovering and inspecting deleted files using autopsy tool

Aim:

Recovering and Inspecting deleted files

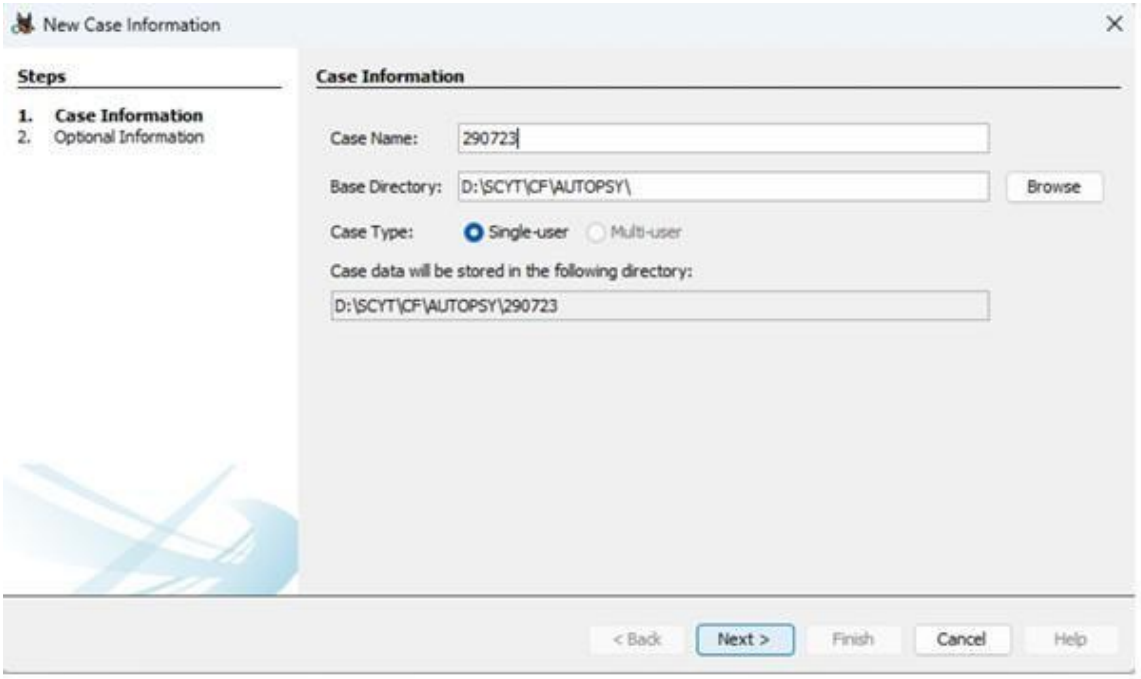
- Check for Deleted Files
- Recover the Deleted Files
- Analyzing and Inspecting the recovered files
- Perform this using recovery option in ENCASE and also Perform manually through command line

Practical:

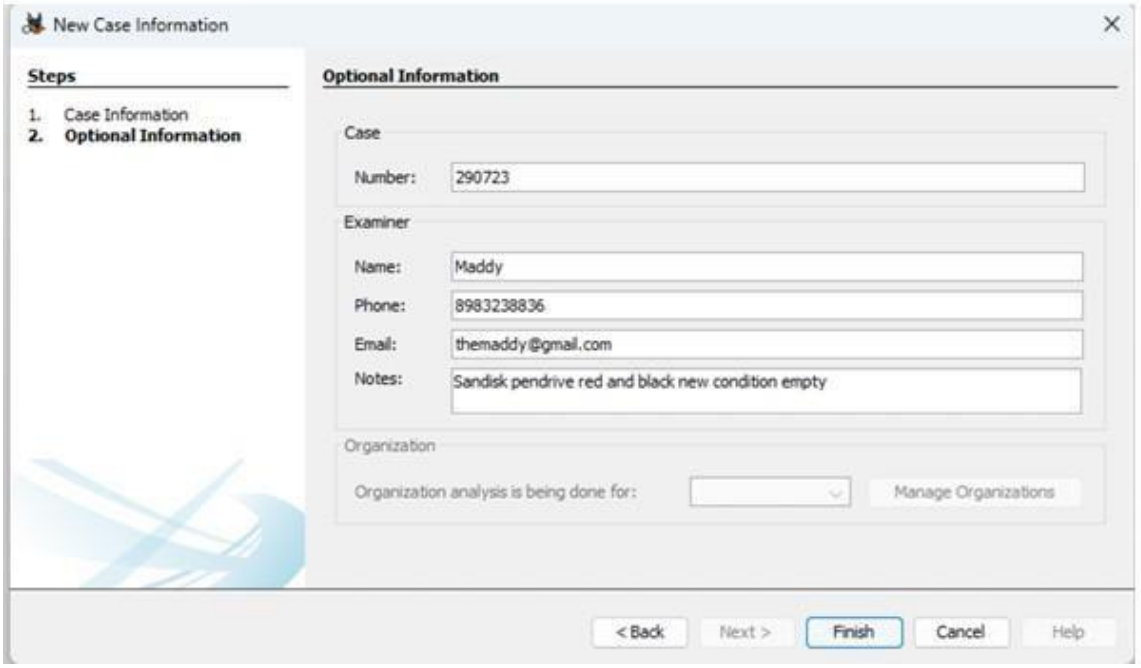
In this Practical we are going to use the Autopsy, an application used to check, recover, analyze and inspect the deleted files using the Image evidence created

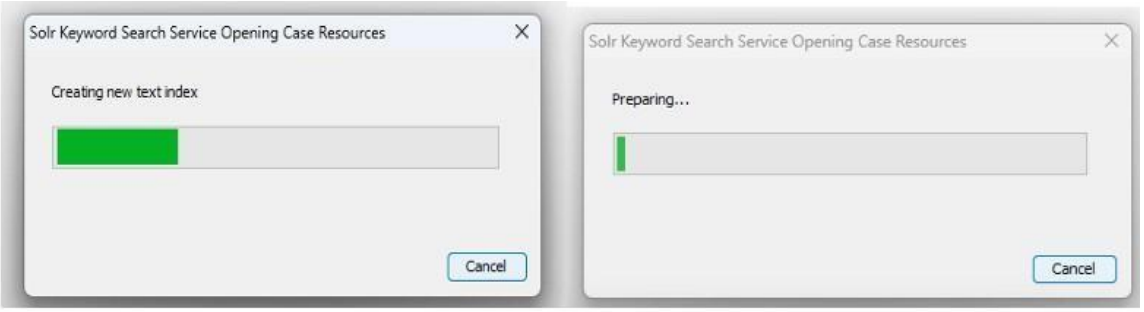
Open Autopsy and Click on New Case

Give a case name and browse the destination to save the autopsy file

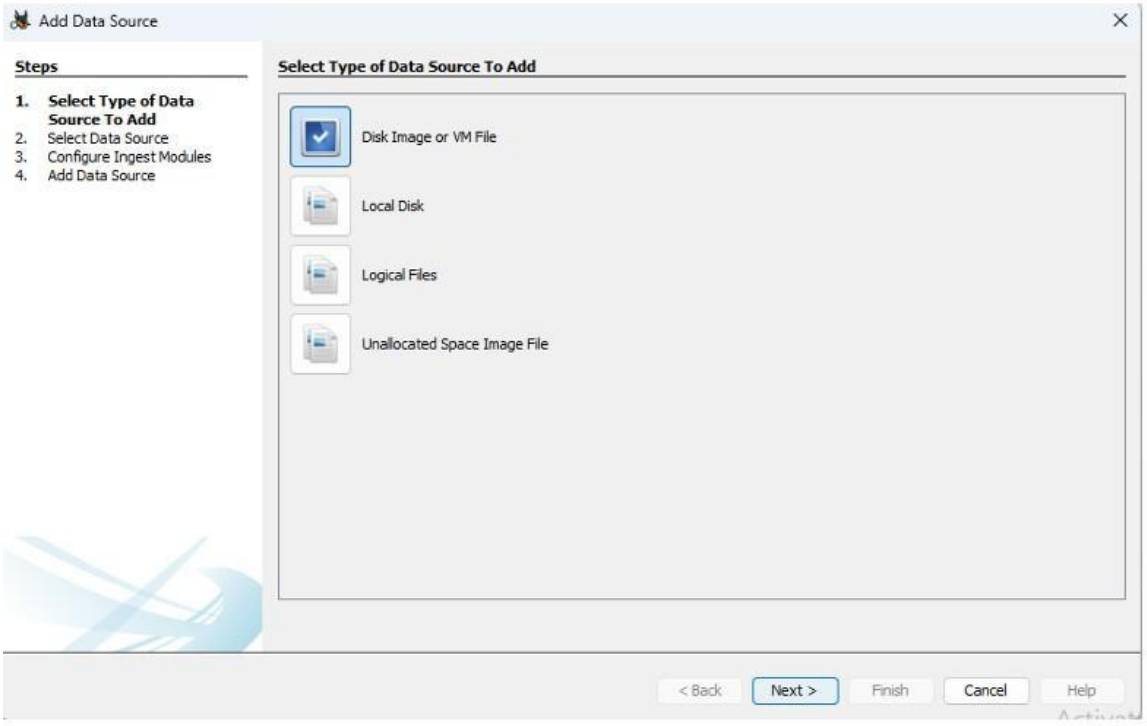


Then give the case number and the details as per the case number when performing the FTK Imager Practical 1

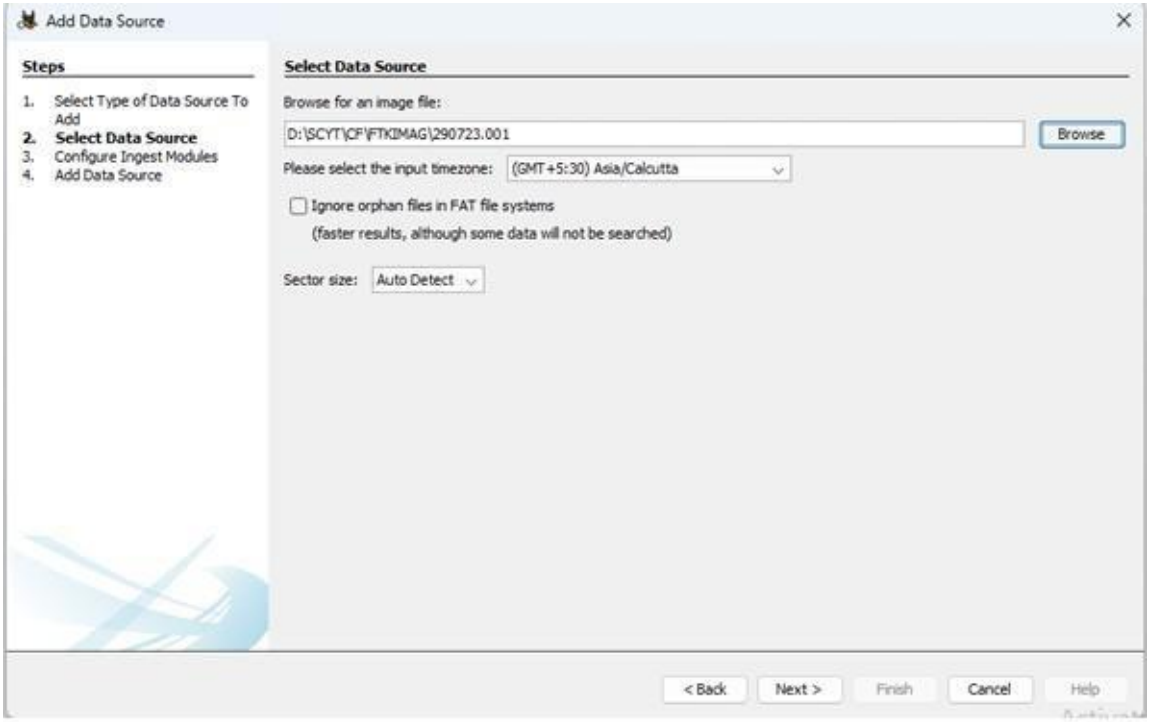




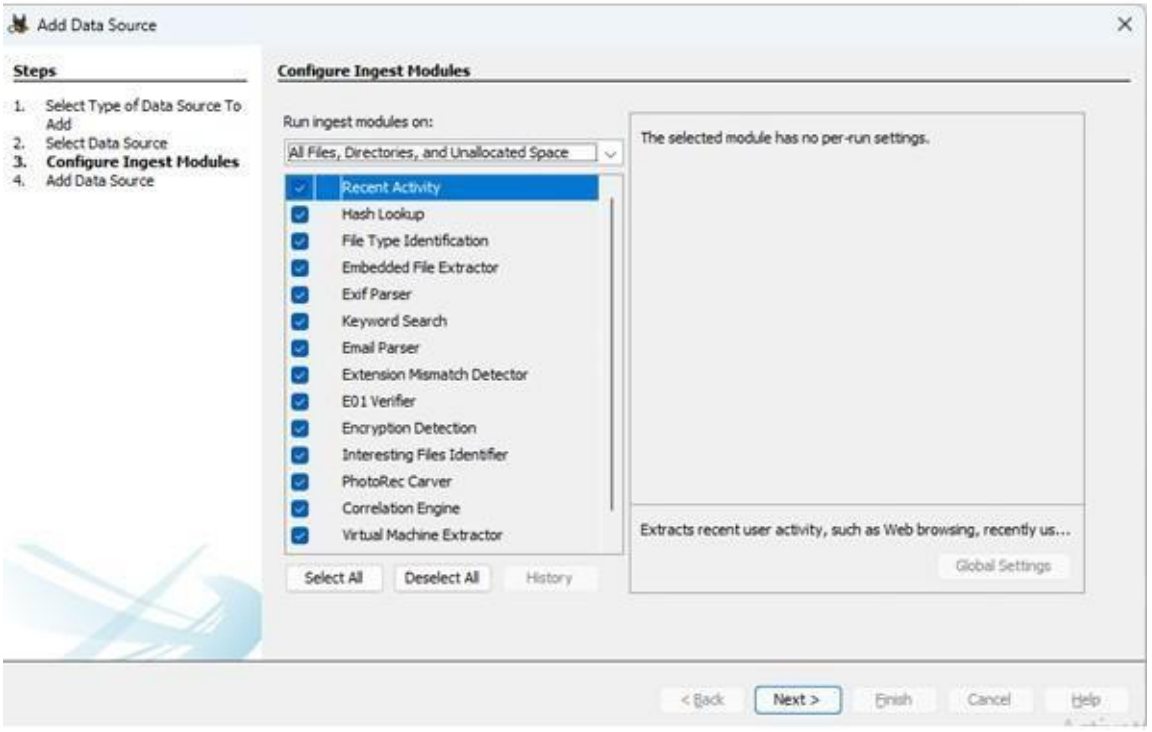
Select on Disk Image or VM File and Click Next



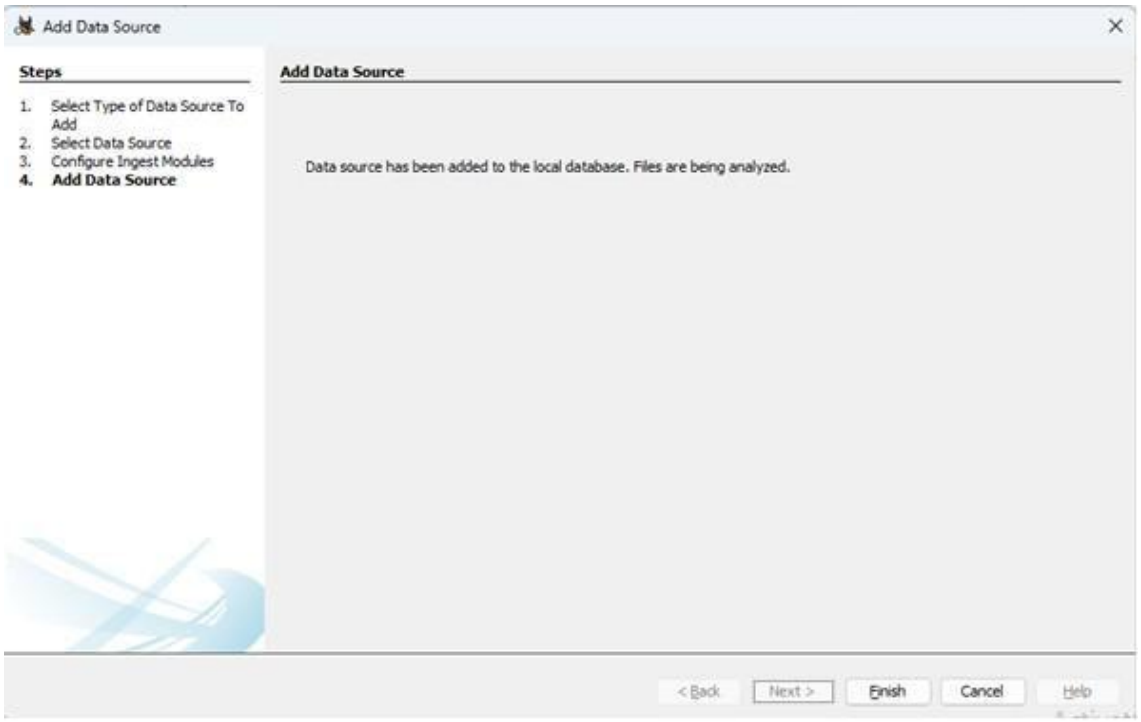
Give the destination of the image and click next



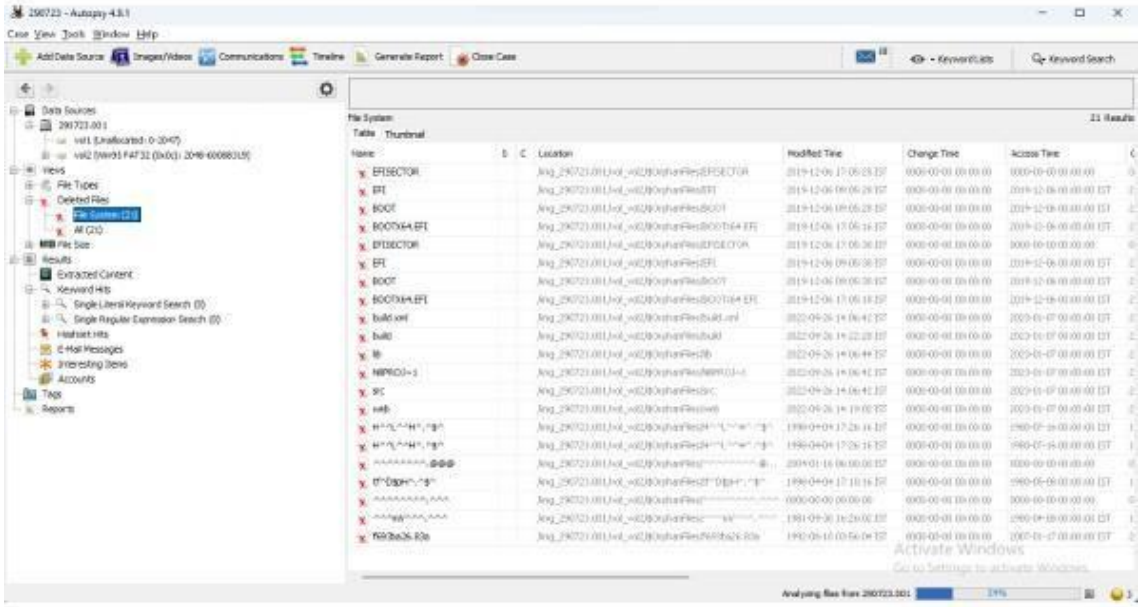
Select the ingest module and click next



See the acknowledgement and click finish

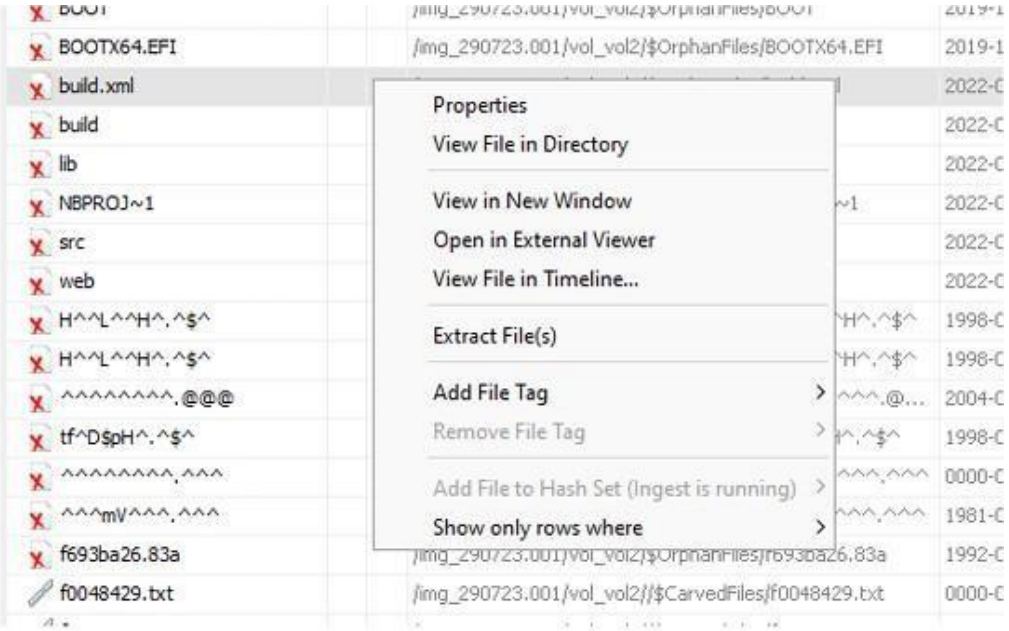


Now we check the files recovered

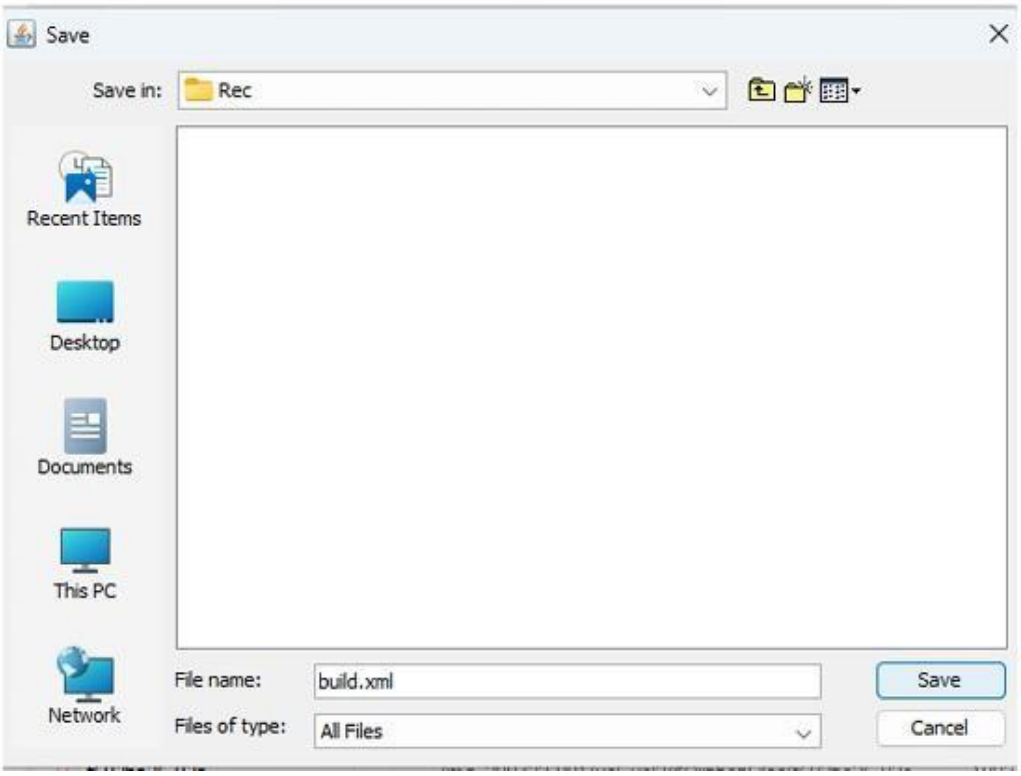


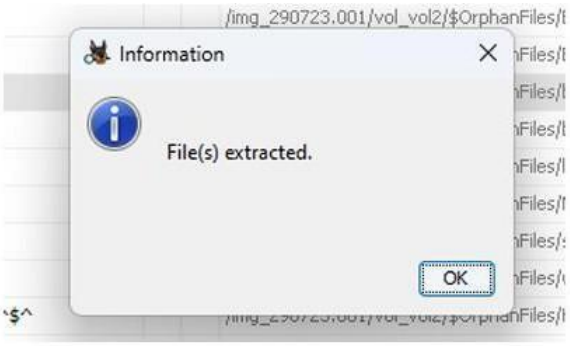
We see the Deleted Files

Now We Extract/Recover some deleted files

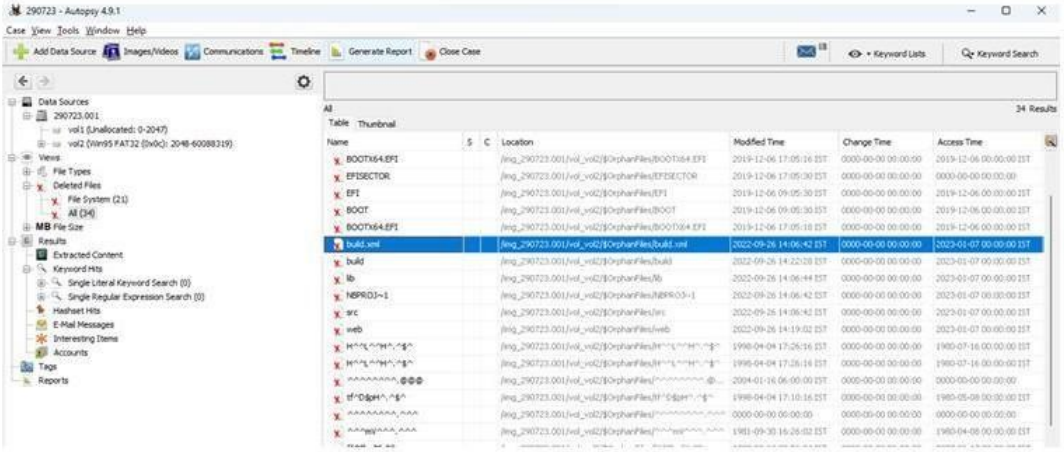


Set a directory for the recovered files

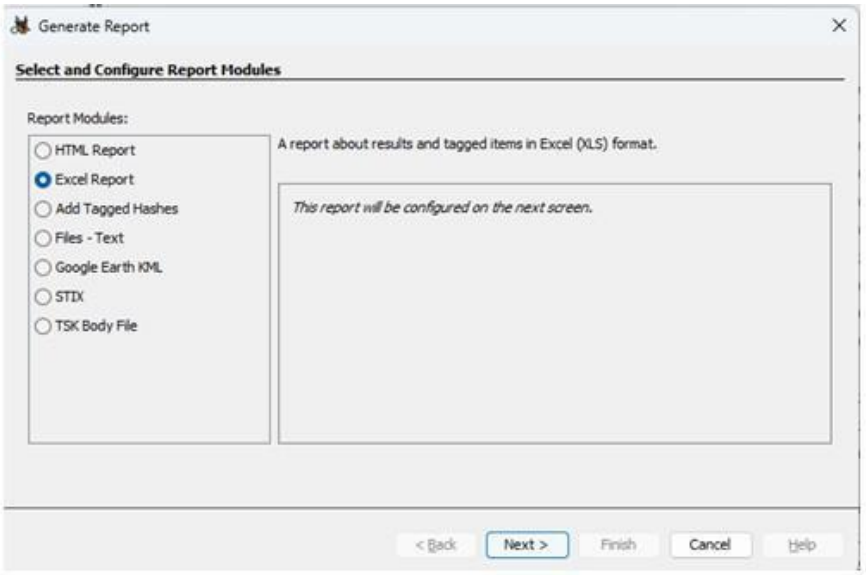




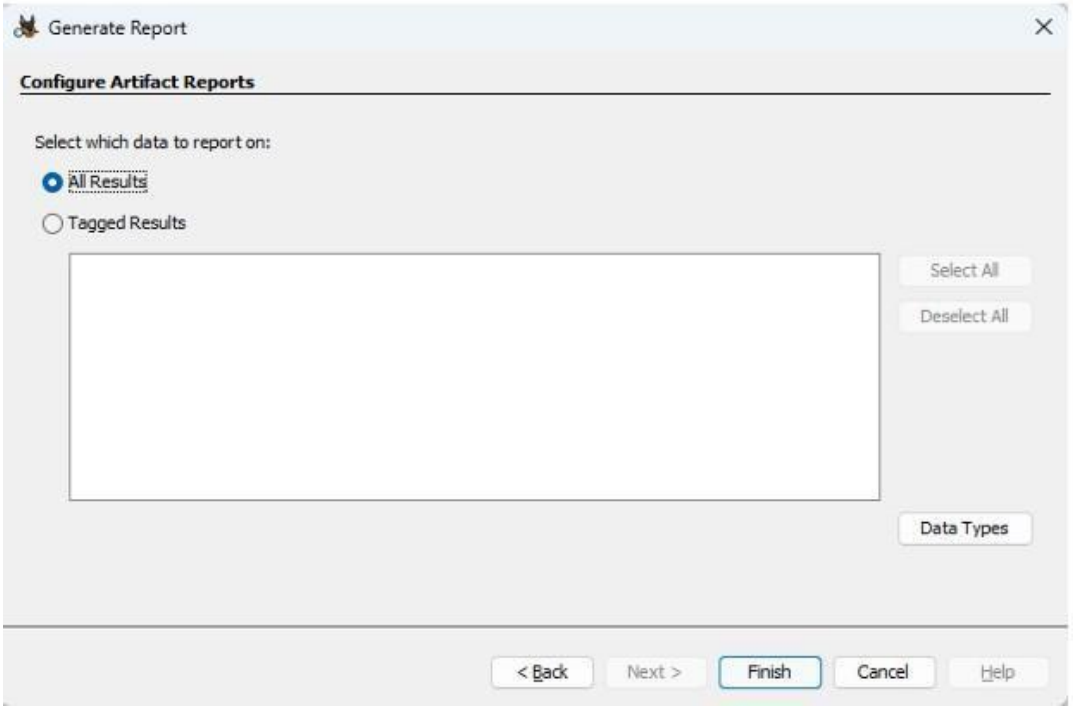
Now we Generate a Report of the Autopsy done

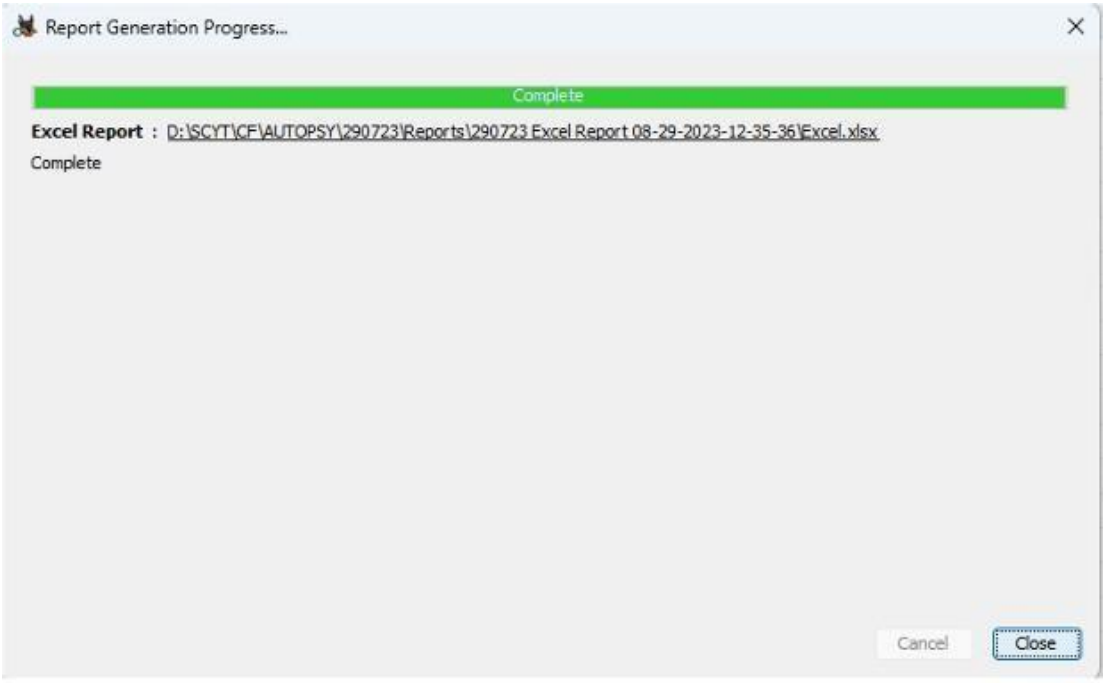


Select a type to store the data and click next. Here we are going to generate the report in Excel.

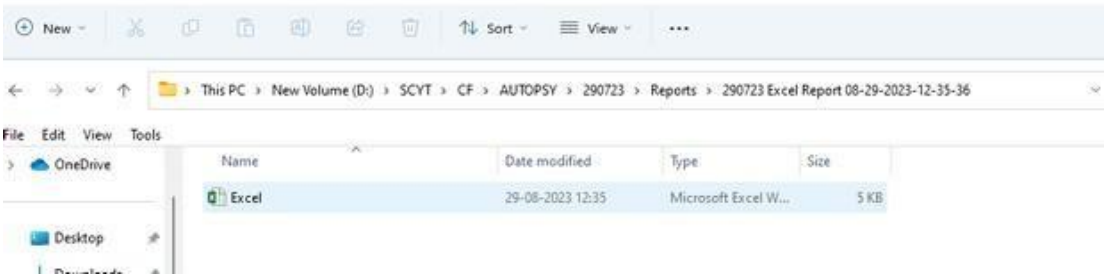


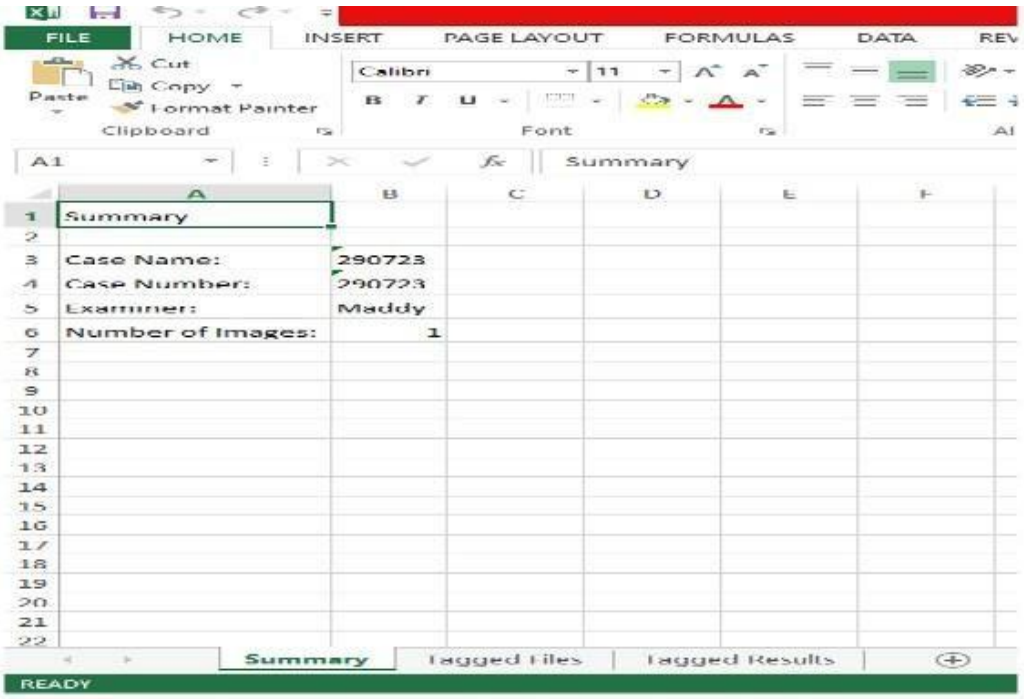
Now select all results this will generate all the reports and click finish. The other option only generate the report for tagged one only.





Click on close and open the excel from the directory it is stored





	A	B
1	Summary	
2		
3	Case Name:	290723
4	Case Number:	290723
5	Examiner:	Maddy
6	Number of Images:	1

Summary | Tagged Files | Tagged Results

READY

	A	B	C	D	E	F	G	H
1	Date Taken	Device Manufacturer	Device Model	Latitude	Longitude	Altitude	Source File	Tags
2	2022-06-10 18:10:21 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2/IMG20220610181021.jpg	
3	2022-06-10 18:10:27 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2/IMG20220610181027.jpg	
4	2022-06-10 18:10:30 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2/IMG20220610181030.jpg	
5	2022-06-10 18:10:34 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2/IMG20220610181034.jpg	
6	2022-06-10 18:23:26 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2//$CarvedFiles/f0000000.jpg	
7	2022-06-10 18:24:07 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2//$CarvedFiles/f0005120.jpg	
8	2022-06-10 18:24:13 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2//$CarvedFiles/f0012256.jpg	
9	2022-06-10 18:24:17 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2//$CarvedFiles/f0016320.jpg	
10	2022-06-10 18:24:37 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2//$CarvedFiles/f0020864.jpg	
11	2022-06-10 18:34:20 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2/IMG20220610183420.jpg	
12	2022-06-10 18:34:25 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2/IMG20220610183425.jpg	
13	2022-06-10 18:34:37 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2/IMG20220610183437.jpg	
14	2022-06-10 18:34:53 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2/IMG20220610183453.jpg	

	A	B	C	D	E	F
1	E-Mail To	E-Mail From	Subject	Date Sent	Date Received	Path
2	'Samspade@myway.com'	Jim Shu: Jim_shu@comcast.net	RE: Bike spec's	2006-12-04 07:39:00 IST	2006-12-04 07:39:00 IST	\\Top of Personal Folders\Sent Items
3	'Samspade@myway.com'	Jim Shu: Jim_shu@comcast.net	RE: Bike spec's	2006-12-04 07:39:00 IST	2006-12-04 07:39:00 IST	\\Top of Personal Folders\Sent Items
4	'Samspade@myway.com'	Jim Shu: Jim_shu@comcast.net	RE: Bike spec's	2006-12-04 08:37:00 IST	2006-12-04 08:37:00 IST	\\Top of Personal Folders\Deleted Items
5	'Samspade@myway.com'	Jim Shu: Jim_shu@comcast.net	RE: Bike spec's	2006-12-04 08:37:00 IST	2006-12-04 08:37:00 IST	\\Top of Personal Folders\Deleted Items
6	'baspen99@aol.com'	Jim Shu: Jim_shu@comcast.net	RE: Waiting	2006-12-07 07:51:00 IST	2006-12-07 07:51:00 IST	\\Top of Personal Folders\Sent Items
7	'baspen99@aol.com'	Jim Shu: Jim_shu@comcast.net	RE: Waiting	2006-12-07 07:51:00 IST	2006-12-07 07:51:00 IST	\\Top of Personal Folders\Sent Items
8	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Activate your account	2006-12-08 05:08:00 IST	2006-12-08 05:08:00 IST	\\Top of Personal Folders\Sent Items
9	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Activate your account	2006-12-08 05:08:00 IST	2006-12-08 05:08:00 IST	\\Top of Personal Folders\Sent Items
10	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bicycle offer	2006-12-08 05:07:00 IST	2006-12-08 05:07:00 IST	\\Top of Personal Folders\Sent Items
11	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bicycle offer	2006-12-08 05:07:00 IST	2006-12-08 05:07:00 IST	\\Top of Personal Folders\Sent Items
12	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bicycle offer	2006-12-08 05:08:00 IST	2006-12-08 05:08:00 IST	\\Top of Personal Folders\Sent Items
13	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bicycle offer	2006-12-08 05:08:00 IST	2006-12-08 05:08:00 IST	\\Top of Personal Folders\Sent Items
14	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bicycle offer	2006-12-08 05:08:00 IST	2006-12-08 05:08:00 IST	\\Top of Personal Folders\Sent Items
15	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bicycle offer	2006-12-08 05:08:00 IST	2006-12-08 05:08:00 IST	\\Top of Personal Folders\Sent Items
16	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bicycle offer	2006-12-08 05:09:00 IST	2006-12-08 05:09:00 IST	\\Top of Personal Folders\Sent Items
17	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bicycle offer	2006-12-08 05:09:00 IST	2006-12-08 05:09:00 IST	\\Top of Personal Folders\Sent Items
18	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bike spec's	2006-12-08 05:07:00 IST	2006-12-08 05:07:00 IST	\\Top of Personal Folders\Sent Items
19	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bike spec's	2006-12-08 05:07:00 IST	2006-12-08 05:07:00 IST	\\Top of Personal Folders\Sent Items
20	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bike spec's	2006-12-08 05:08:00 IST	2006-12-08 05:08:00 IST	\\Top of Personal Folders\Sent Items
21	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bike spec's	2006-12-08 05:08:00 IST	2006-12-08 05:08:00 IST	\\Top of Personal Folders\Sent Items
22	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bike spec's	2006-12-08 05:09:00 IST	2006-12-08 05:09:00 IST	\\Top of Personal Folders\Sent Items
23	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bike spec's	2006-12-08 05:09:00 IST	2006-12-08 05:09:00 IST	\\Top of Personal Folders\Sent Items

	A	B	C
1	Email Addresses		
2	%@clients.l.google.com		
3	Preview	Source File	Tags
4	lients.l.google.com>%@clients.l.google.com>%hclients.l.google.	/img_04092023_masood.001/vol_vol2//$Unalloc/Unalloc_1878_3915776_107772138	
5	lients.l.google.com>%@clients.l.google.com>%hclients.l.google.	/img_04092023_masood.001/vol_vol2/$OrphanFiles/_LLPLA~1.PCA	
6	lients.l.google.com>%@clients.l.google.com>%hclients.l.google.	/img_04092023_masood.001/vol_vol2/$OrphanFiles/_ROTEU~1.EXE	
7	lients.l.google.com>%@clients.l.google.com>%hclients.l.google.	/img_04092023_masood.001/vol_vol2/$OrphanFiles/afmmdbn.umd	
8			
9	-239034876-0-1001@flonetwork.com		
10	Preview	Source File	Tags
11	jjjd4zmt+-239034876-0-1001@flonetwork.com>!{work.com>]4676-0	/img_04092023_masood.001/vol_vol2//$Unalloc/Unalloc_1878_3915776_107772138	
12	jjjd4zmt+-239034876-0-1001@flonetwork.com>!{work.com>]4676-0	/img_04092023_masood.001/vol_vol2/_S/Proteus 8.11 SP0 Pro HomeMade Electronics.exe	
13			
14	20061203212123.60945738a225c@rly-xm04.mx.aol.com		
15	Preview	Source File	Tags
16	-0500>-reply-to: <<20061203212123.60945738a225c@rly-xm04.mx.aol.com>-x-mb-message-sour	/img_04092023_masood.001/vol_vol2//$Unalloc/Unalloc_1878_3915776_107772138	
17	-0500>-reply-to: <<20061203212123.60945738a225c@rly-xm04.mx.aol.com>-x-mb-message-sour	/img_04092023_masood.001/vol_vol2/_S/Proteus 8.11 SP0 Pro HomeMade Electronics.exe	
18			
19	20061204013940.a88906765f@mpmdmain.myway.com		
20	Preview	Source File	Tags
21	etmail.comcast.net<<20061204013940.a88906765f@mpmdmain.myway.com>-mail.comcast.net000	/img_04092023_masood.001/vol_vol2//$Unalloc/Unalloc_1878_3915776_107772138	
22	[illegible]	[illegible]	

	A	B	C	D
1	Review Status	ID	Tags	
2	Undecided	Samspade@myway.com		
3	Undecided	Samspade@myway.com		
4	Undecided	baspen99@aol.com		
5	Undecided	baspen99@aol.com		
6	Undecided	jim_shu1@yahoo.com		
7	Undecided	jim_shu1@yahoo.com		
8	Undecided	jim_shu@comcast.net		
9	Undecided	jim_shu@comcast.net		
10	Undecided	martha.dax@superiorbicycles.biz		
11	Undecided	martha.dax@superiorbicycles.biz		
12	Undecided	terrysadler@goowy.com		
13	Undecided	terrysadler@goowy.com		
14				

A1 File

	A	B	C	D
1	File	Extension	MIME Type	Path
2	AC19.gpj	gpj	image/jpeg	/img_04092023_masood.001/vol_vol2/$OrphanFiles/_IM_SH~1.PST/AC19.gpj
3	AC19.gpj	gpj	image/jpeg	/img_04092023_masood.001/vol_vol2//$CarvedFiles/f0333408.pst/AC19.gpj
4				
5				

PRACTICAL NO. 5

Aim:Capturing and analysing network packets using wireshark

Aim:

Capturing and analyzing network packets using WireShark (Fundamentals):

- Identification the live network
- Capture Packets
- Analyze the captured packets

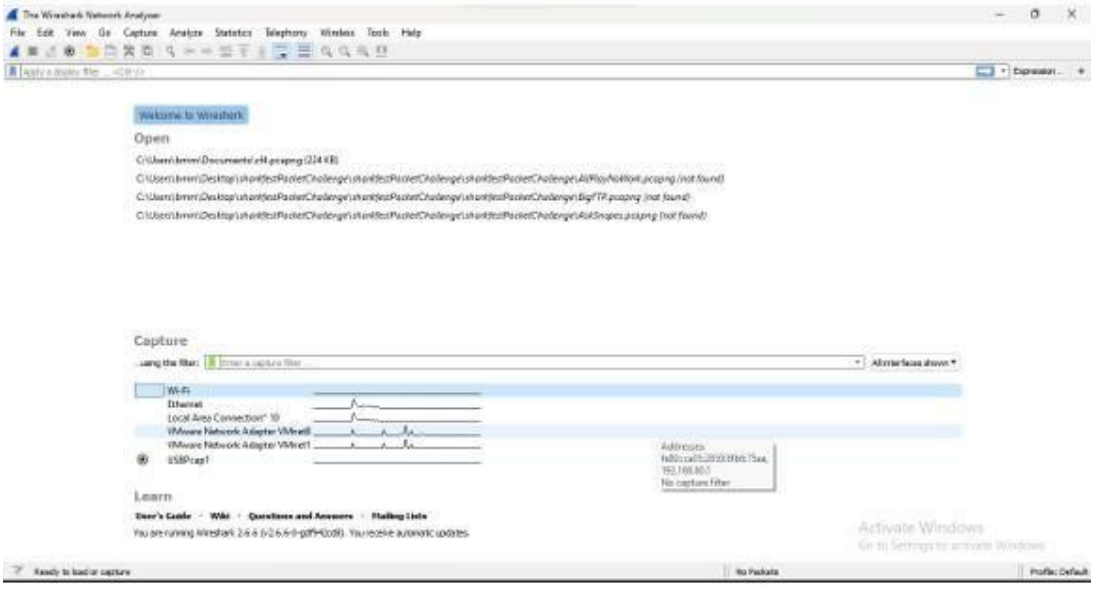
Practical:

In this practical only **identification**, **capturing** and **analysis** is done.

We will also **solve some cases to understand the practical clearly.**

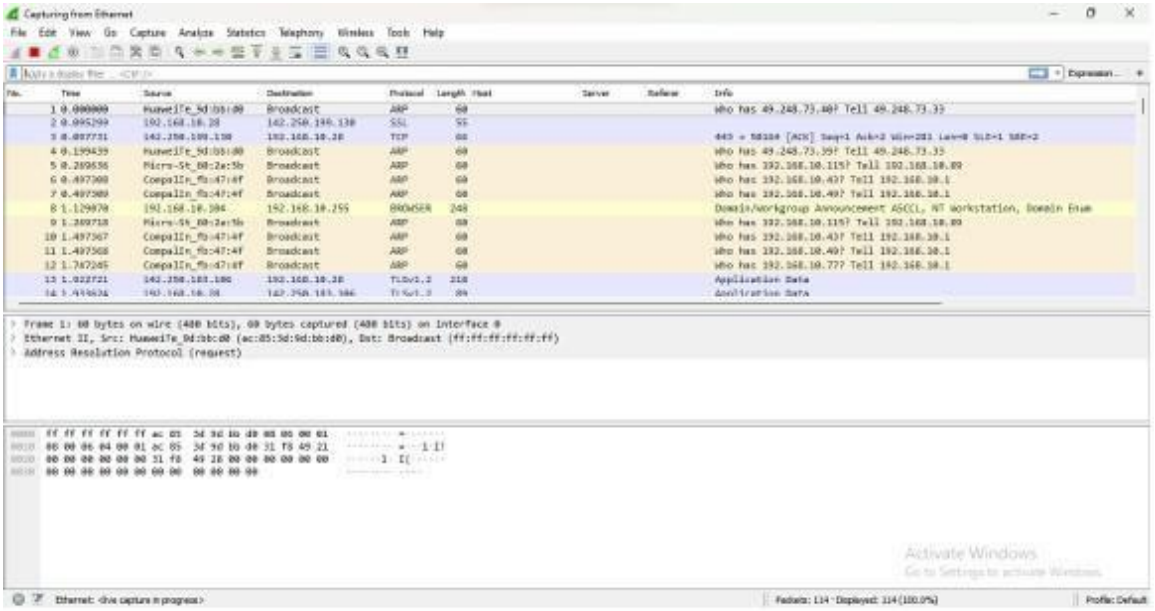
Identifying the Live Networks

We are using **WireShark**, an application used to identify, capture and analyze the network traffics.



Capturing Network

We are now going to capture a network of Ethernet



As soon as you single-click on your network interface's name, you can see how the packets are working in real time. WireShark will capture all the packets going in and out of our systems.

Analyze the Captured Packets

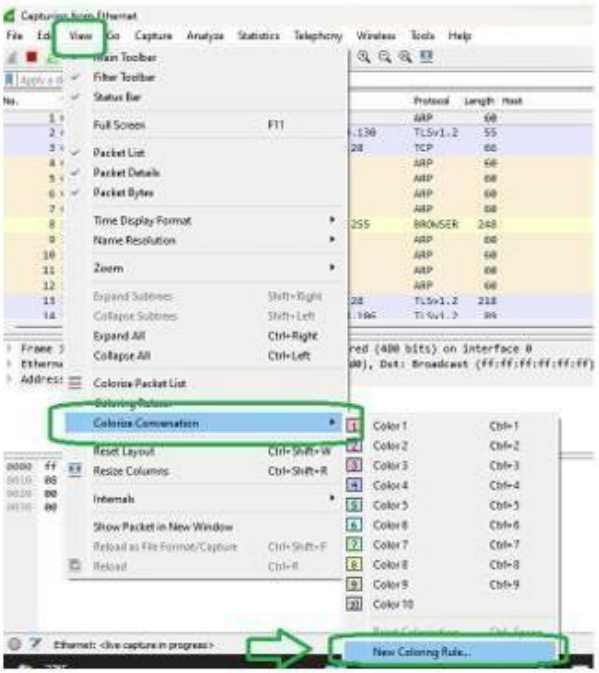
Color Coding Different packets are seen highlighted in various different colors. This is WireShark's way of displaying traffic to help you easily identify the types of it.

Default colors are:

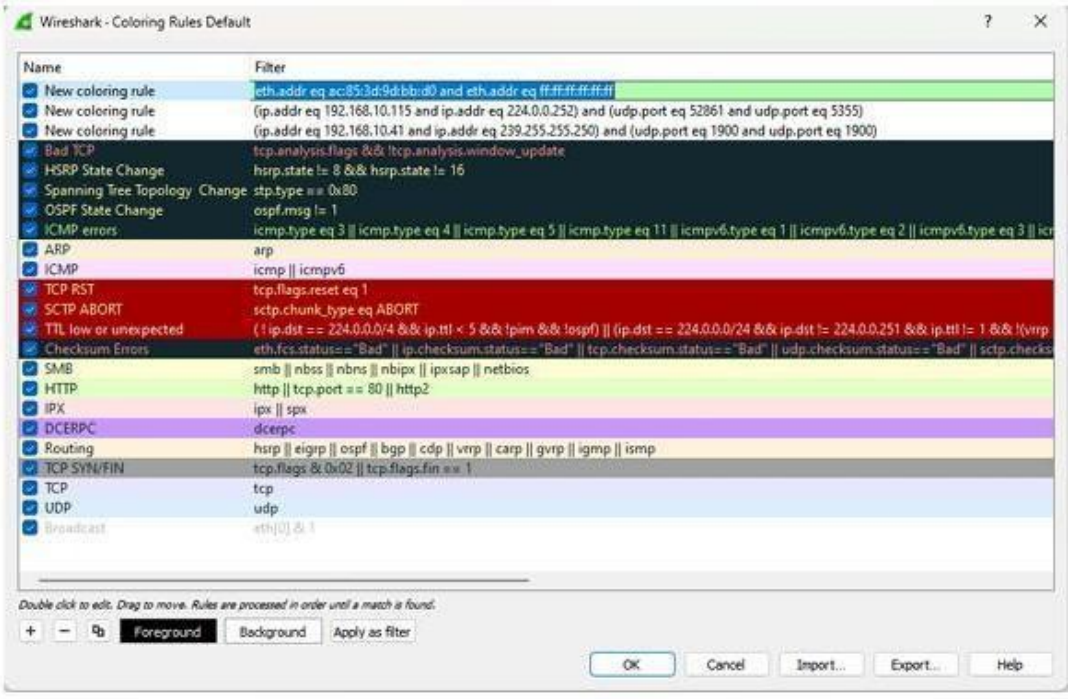
- Light Purple color for TCP traffic
- Light Blue color for UDP traffic
- Black color identifies packets with errors

Example these packets are delivered in an unordered manner.

Click on View → Colorize Conversation → New Coloring Rule

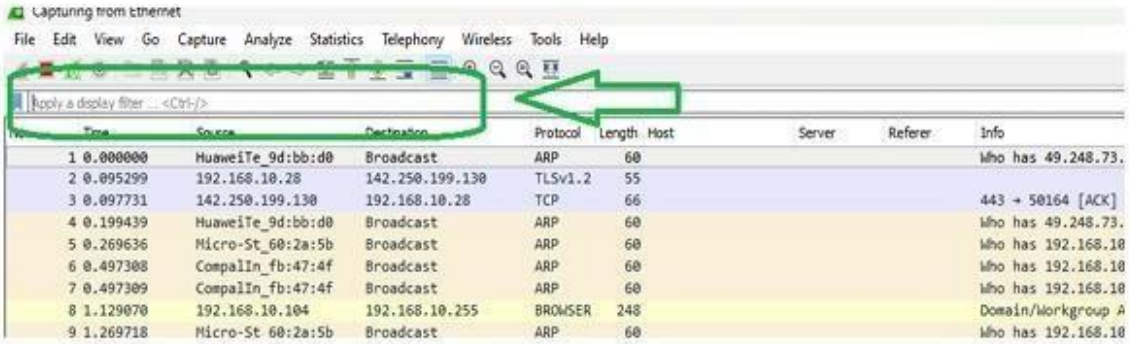


Here we can see the Default Colors given for every **Packet Capturing**



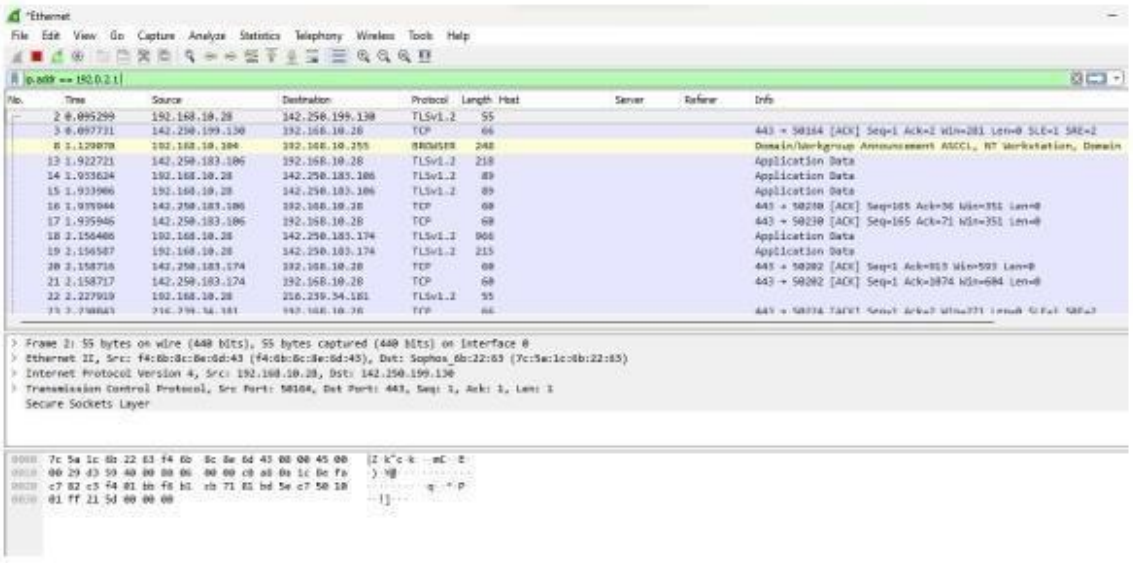
Now we analyze data using filters provided in the WireShark application

Write the following commands in the given area to apply filter

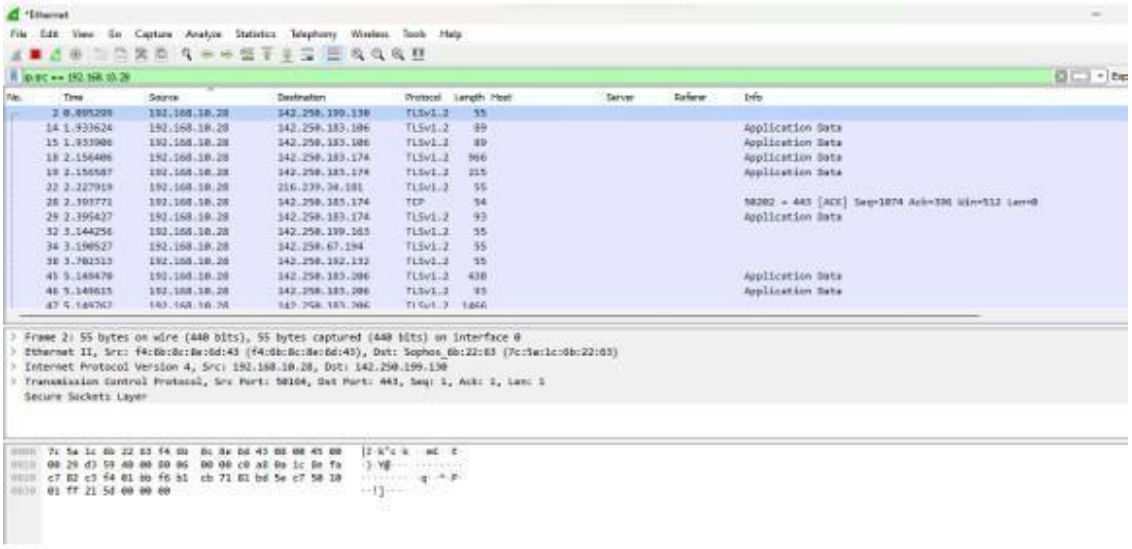


Display filter command

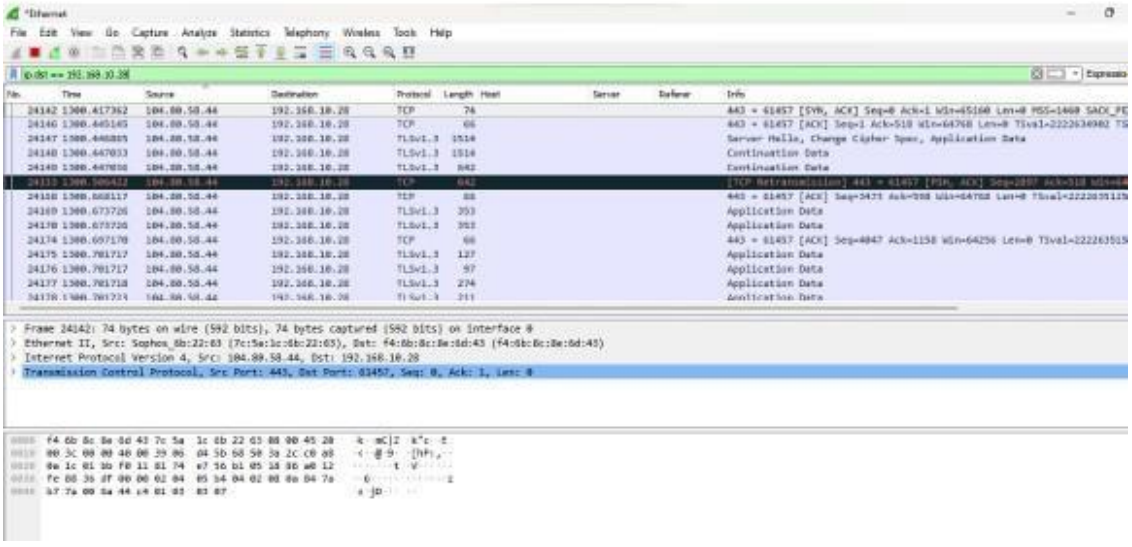
1. Display packets based on specific IP-address
   - ip.addr == 192.0.2.1



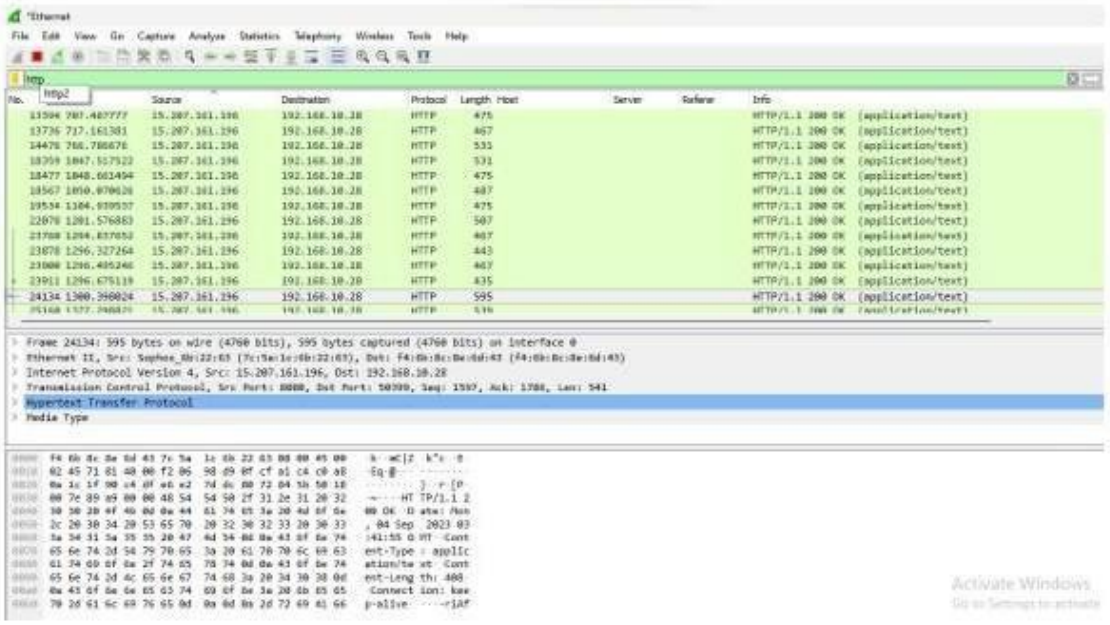
2. Display packets which are coming from specific IP-address
   - ip.src == 192.168.10.28



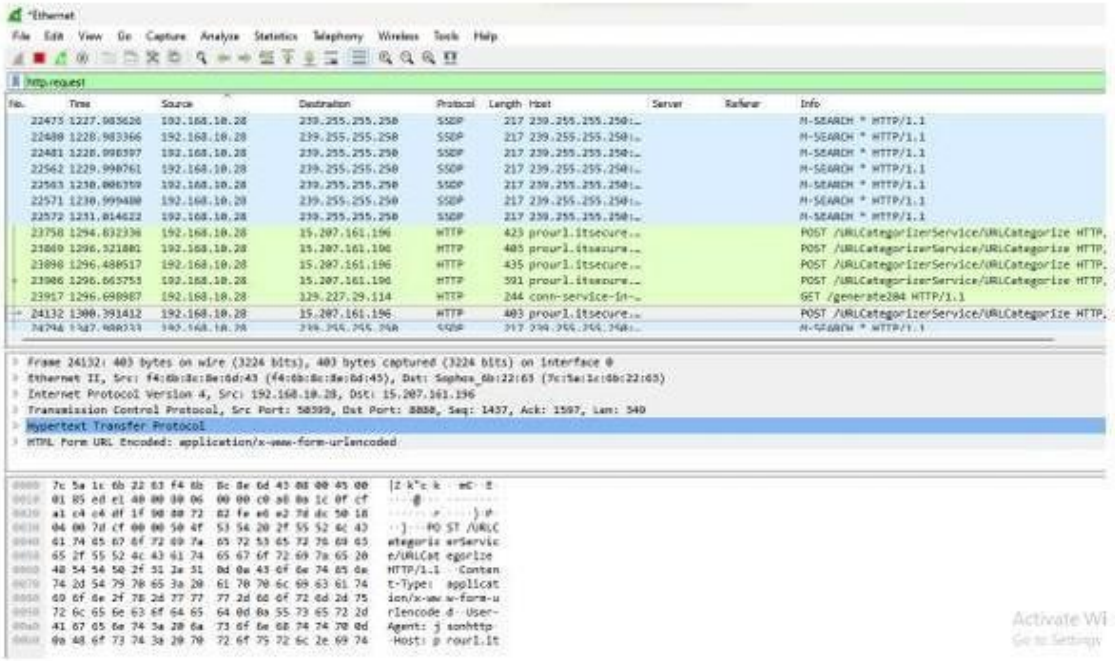
3. Display packets which are having specific IP-address destination
   - ip.dst == 192.168.10.28



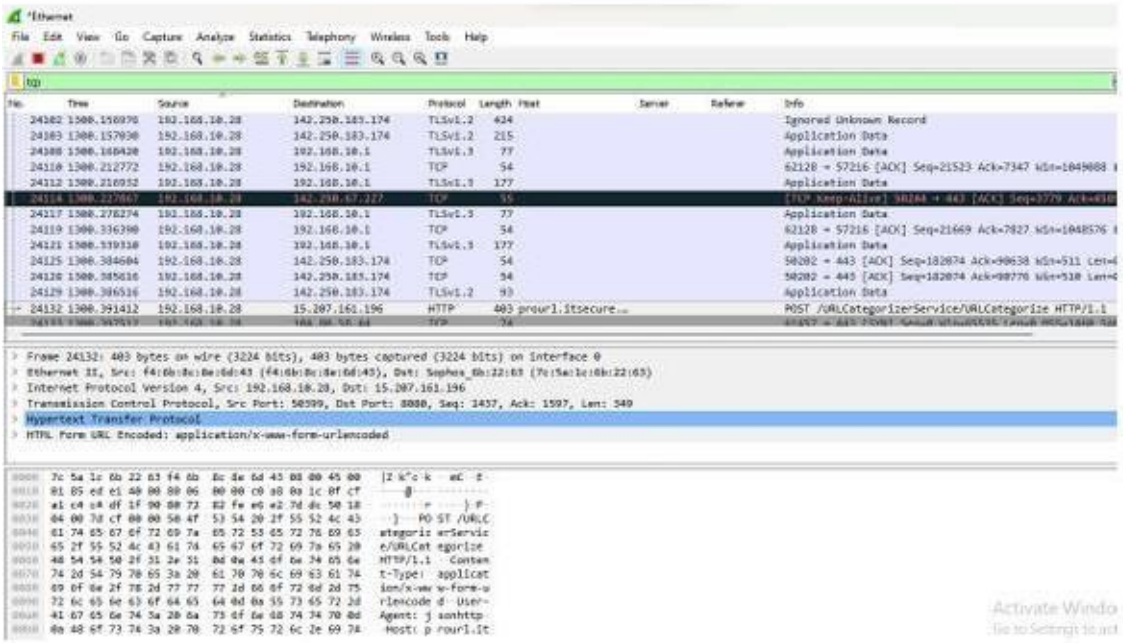
4. Display packets which are using http protocol
   - http



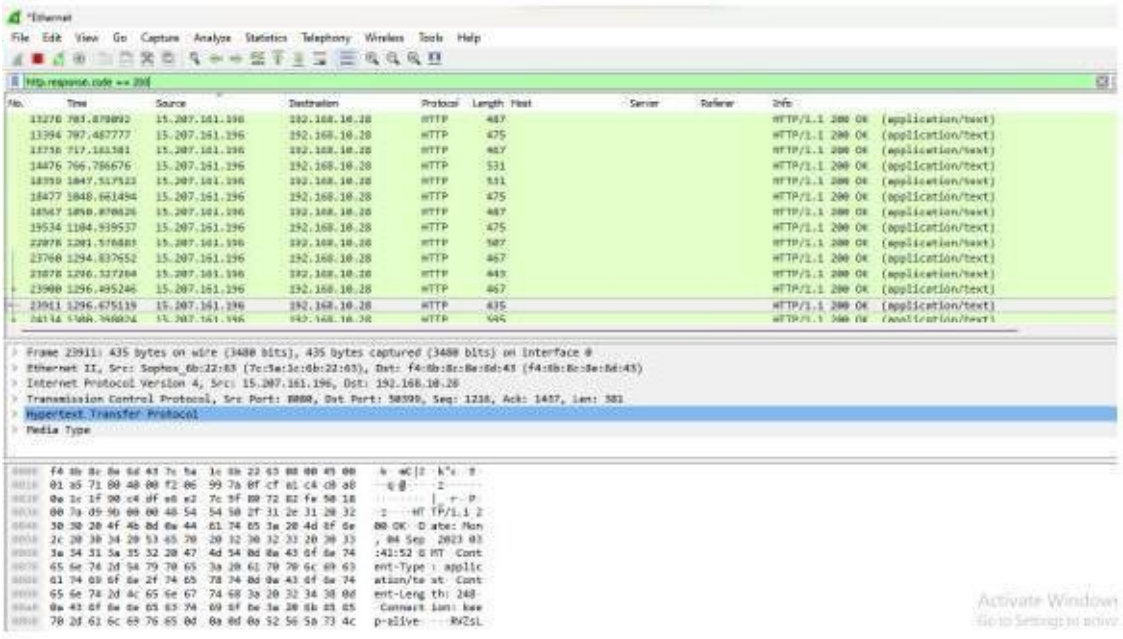
5. Display packets which are using http request
   - http.request



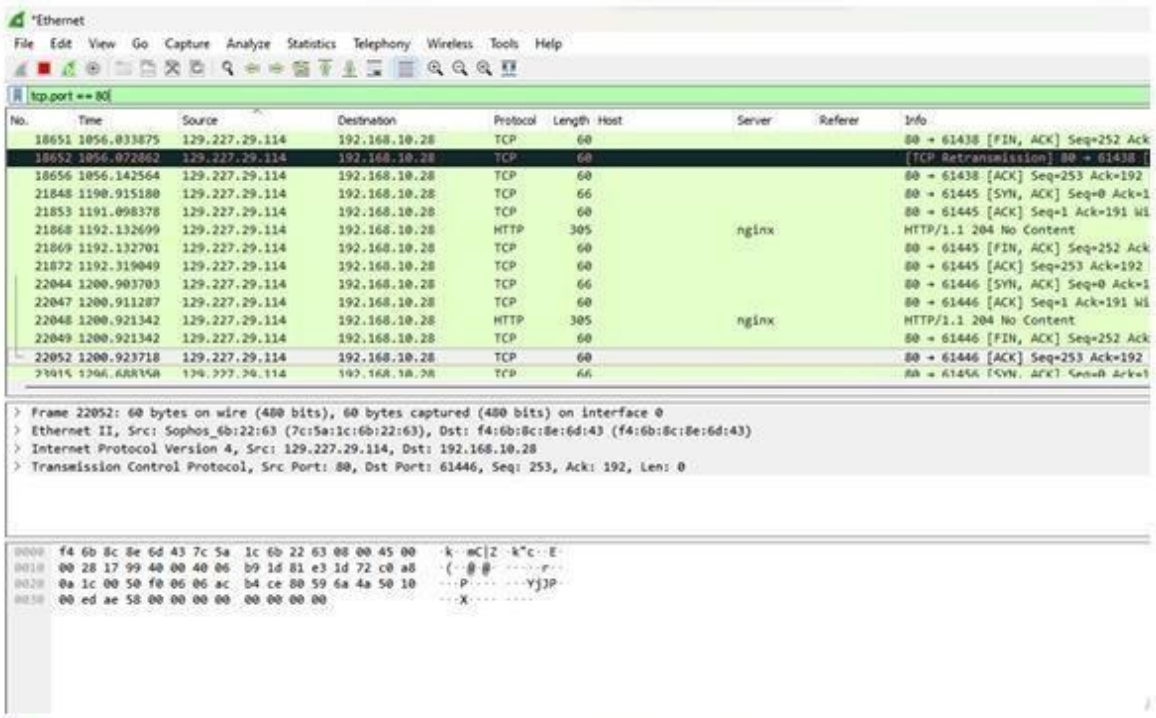
6. Display packets which are using TCP protocol
   - tcp

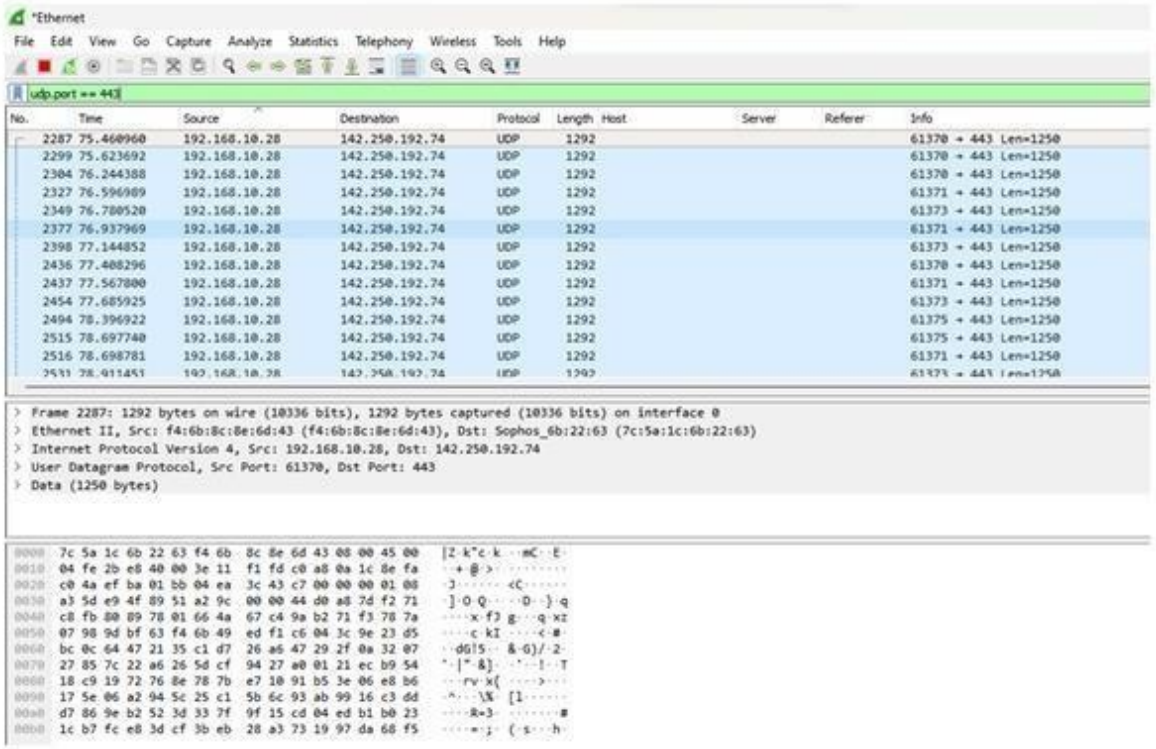


7. Display packets having no error connecting to server
   - http.response.code==200

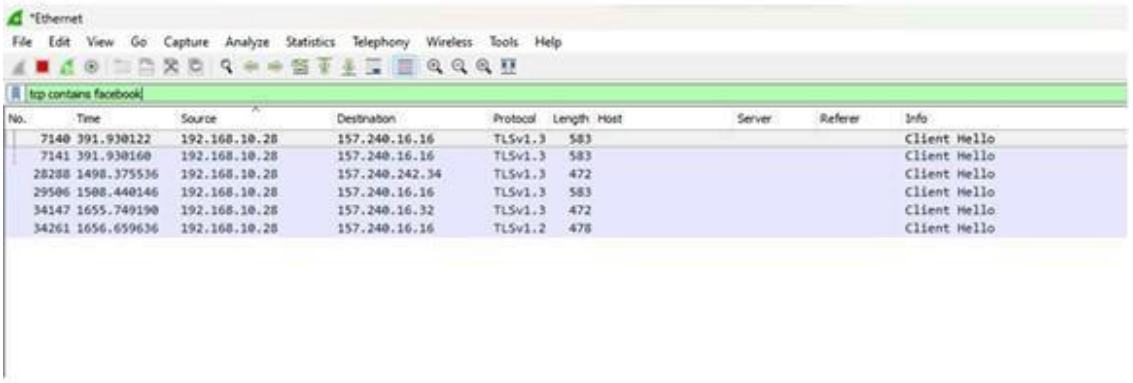


8. Display packets having port number 80, 443
   - tcp.port==80 || udp.port==443





9. Display packets which that contains keyword facebook
   - tcp contains facebook



Now we are going to perform a **Case Study**

AIM:

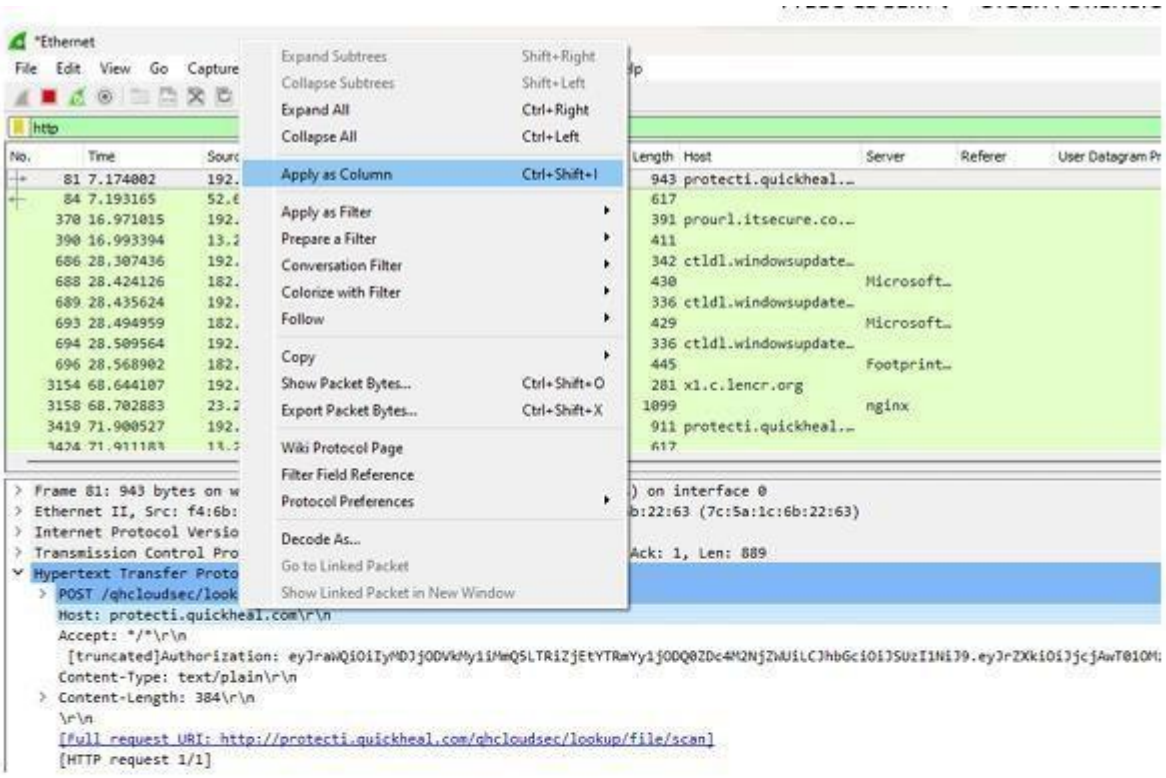
Analyze the packets provided in lab and solve the questions using Wireshark

1. What web server software issued by go.microsoft.com?

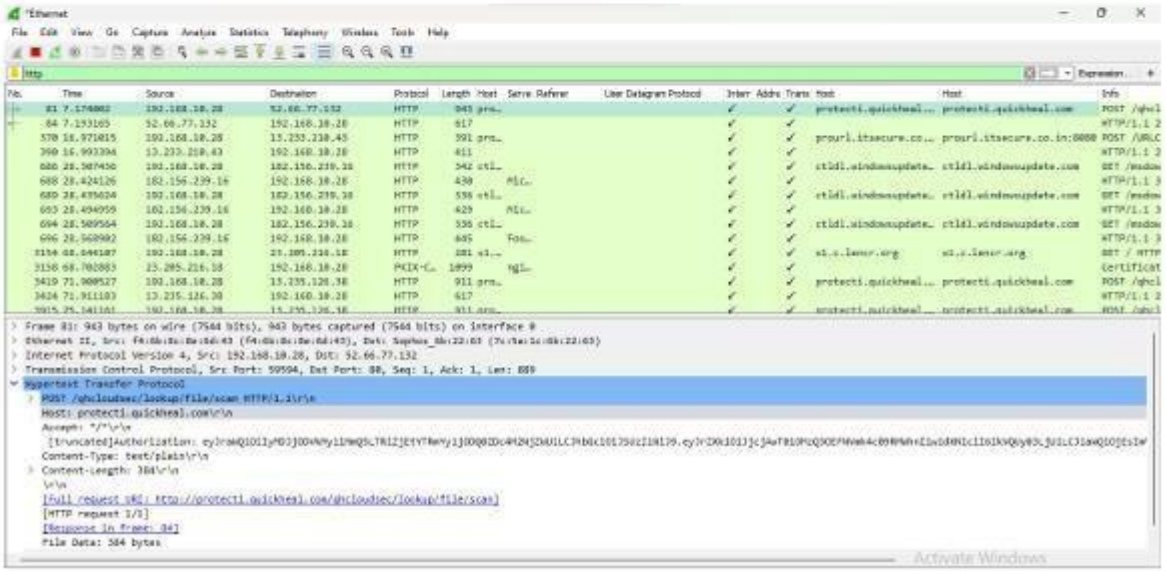
Analysis –

The domain name be found from host header so we will set host header column where we will see all domain name. Select any HTTP request and expand the Hypertext Transfer Protocol then right click on Host header and then Apply as Column

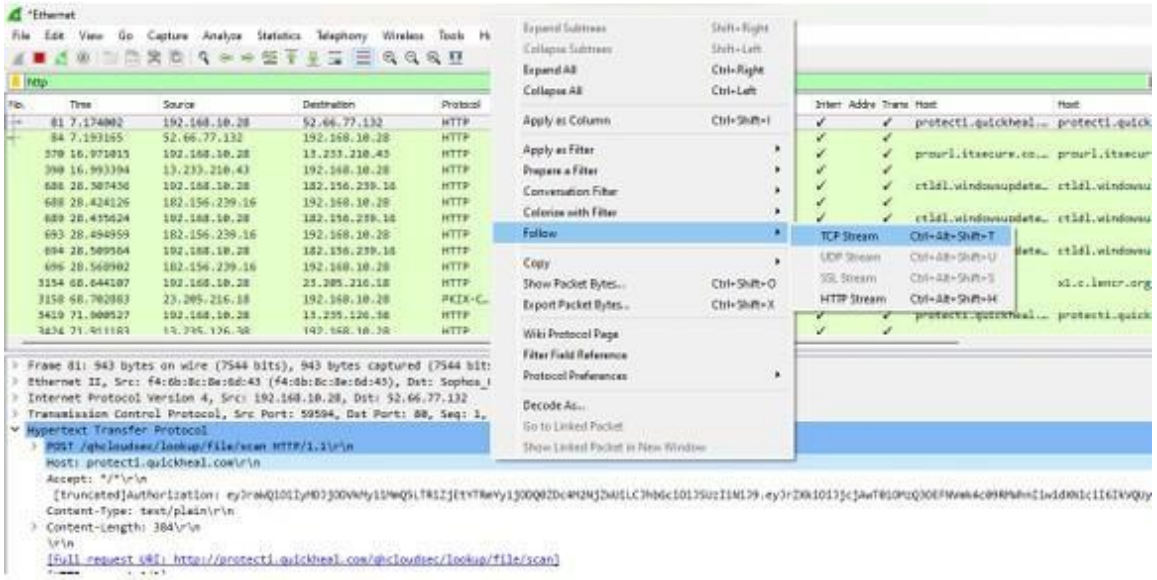
First find the requests from **HTTP** and click on and **request** then on the **lower table of details** Select on **HyperText Transfer Protocol** → **Host** and **Right Click** on that and Select **Apply as Filter**

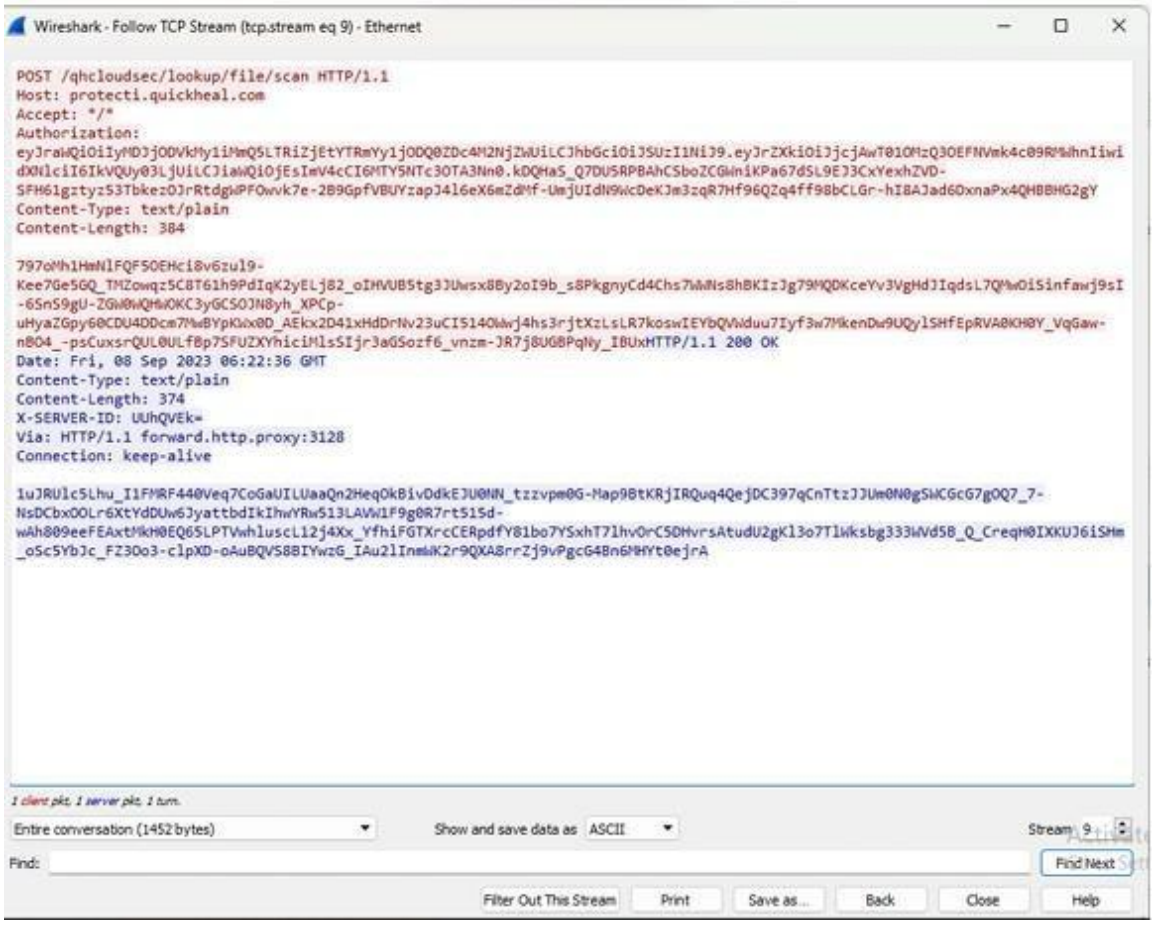


Now we can see the **Host**



Right click on the **selected packet** and then select **Follow** → **TCP stream**



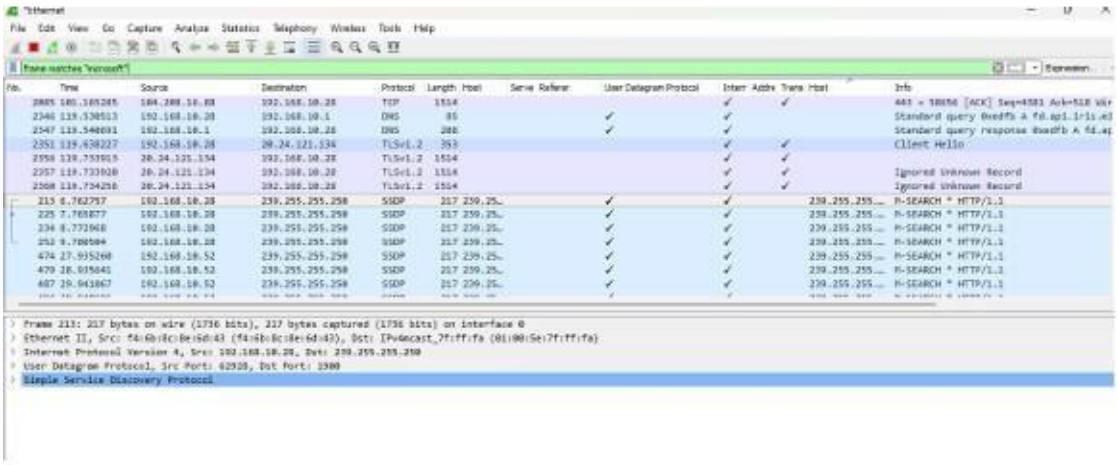


2. About what cell phone problem is the client concerned?

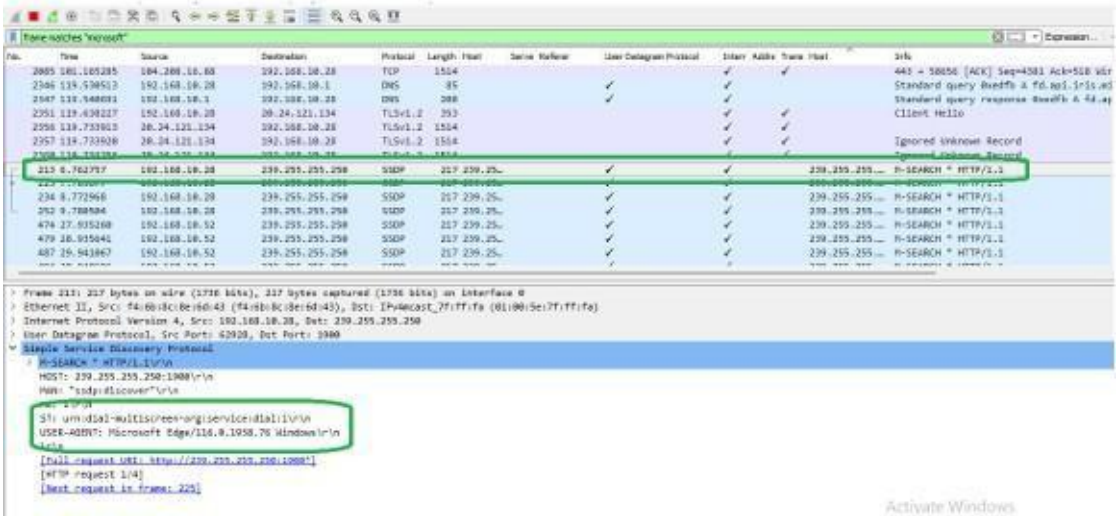
Analysis –

Client talking about cell so we search for cell keyword in whole packets. We will use regular express for searching the cell keyword. Apply frame matches "()"

In the **search frame** type **frame matches "microsoft"**



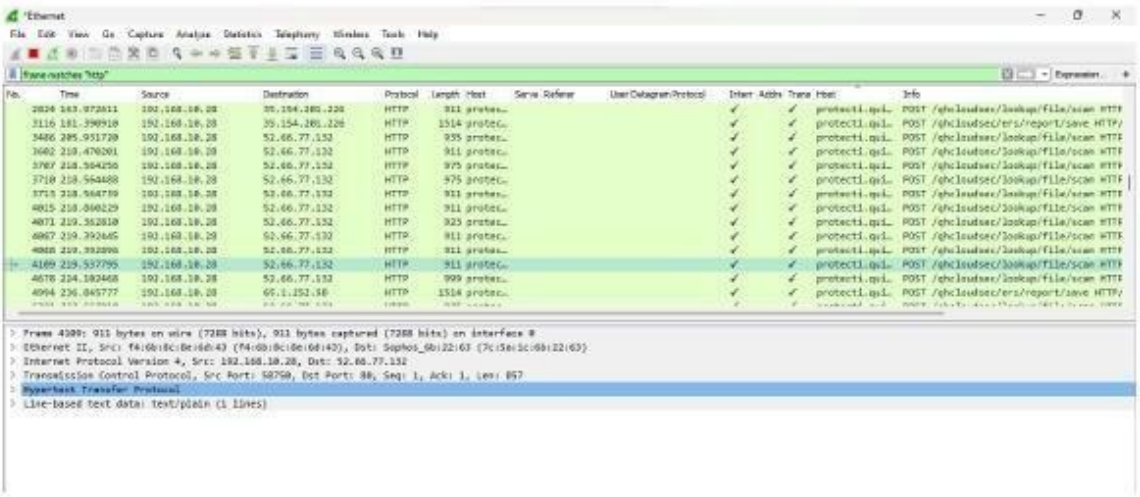
After applying the filter now, we will start to check every HTTP request. We noticed in the first HTTP request microsoft keyword is in URL and it was about Microsoft Edge connection.



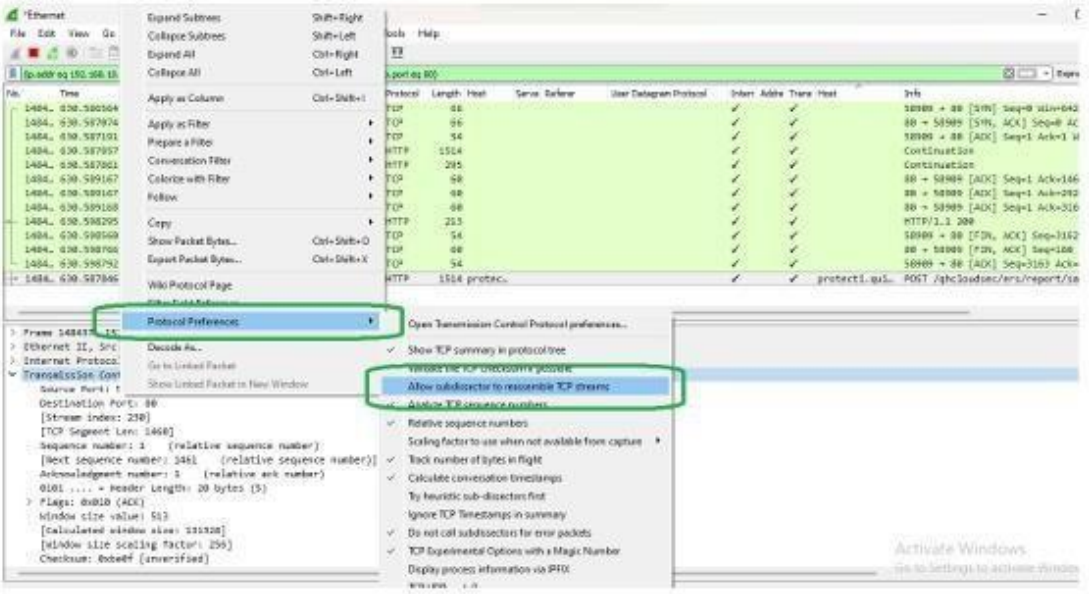
3. According to http, what data will TCP show?

Analysis –

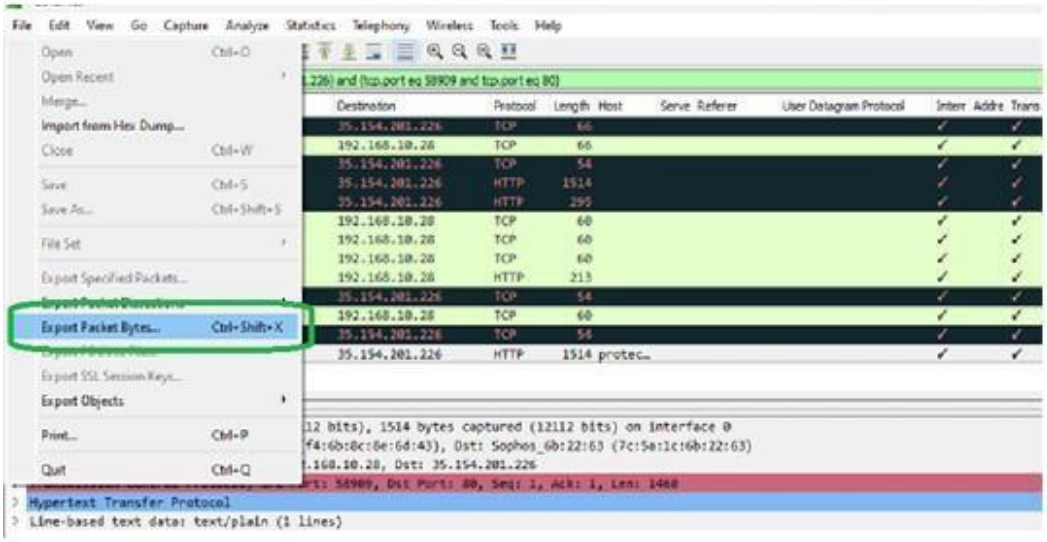
As we did in the last challenge, we will **apply a regular express filter** for the Google **keyword**. **Apply frame matched "http"** .



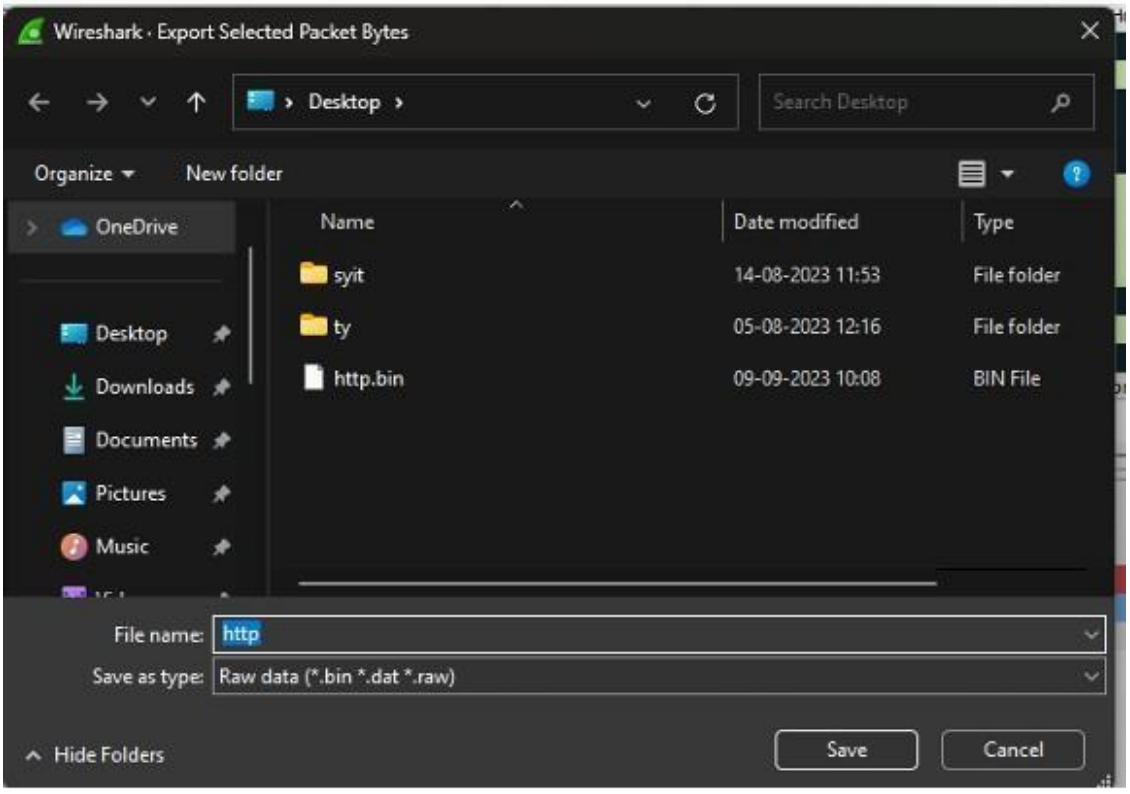
Select the packet and **expand the Hypertext Transfer Protocol** tab **right click** on **Transmission Control Protocol** **Go to Protocol Preferences** and **check Allow subdissector** to resemble TCP stream with HTTP spanning bodies.



Now **Go to file** and **select Export Objects** → **HTTP**. It will save all objects from the packet.



Click on save all.

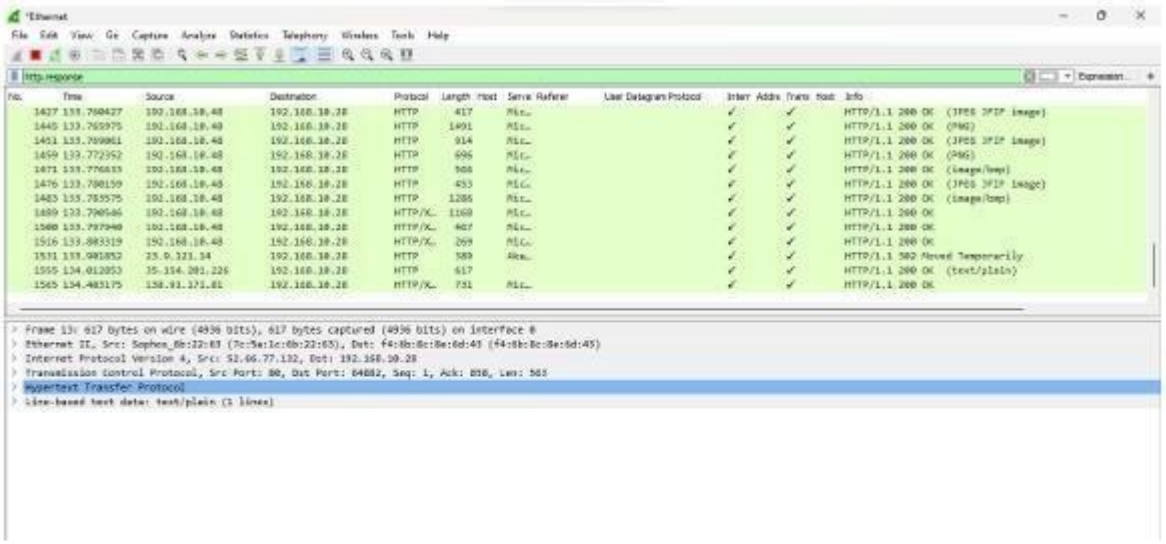


After checking it seems only the packets transfer were to connect the machine to the internet.

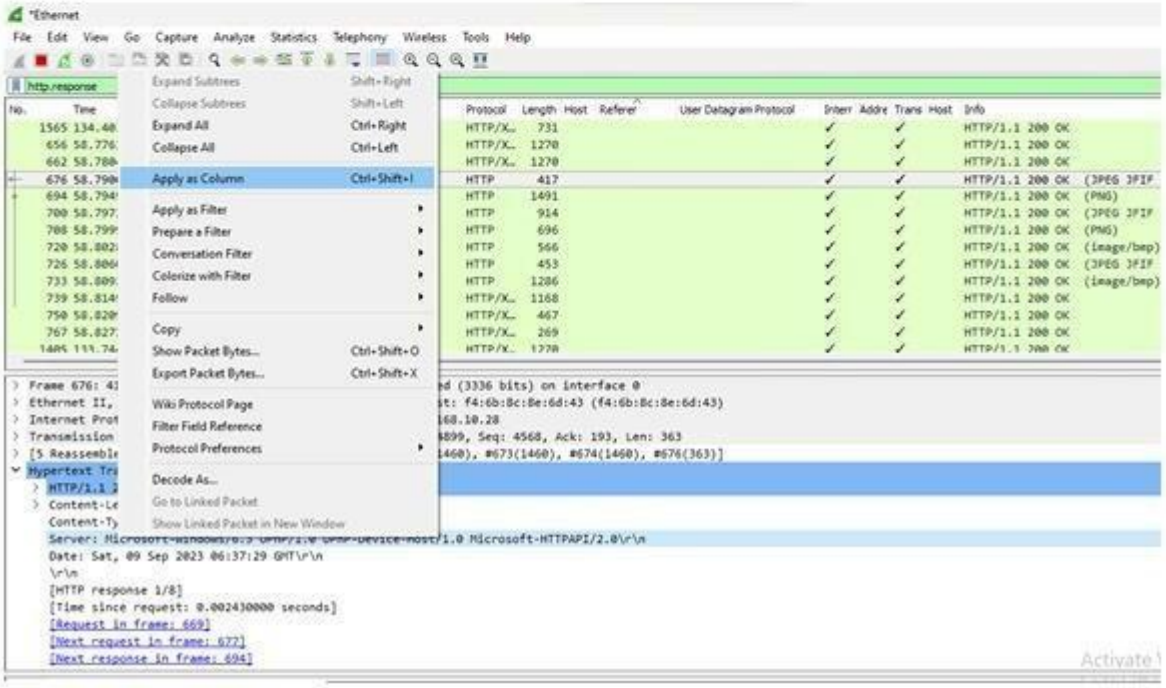
4. How many web servers are running Microsoft?

Analysis –

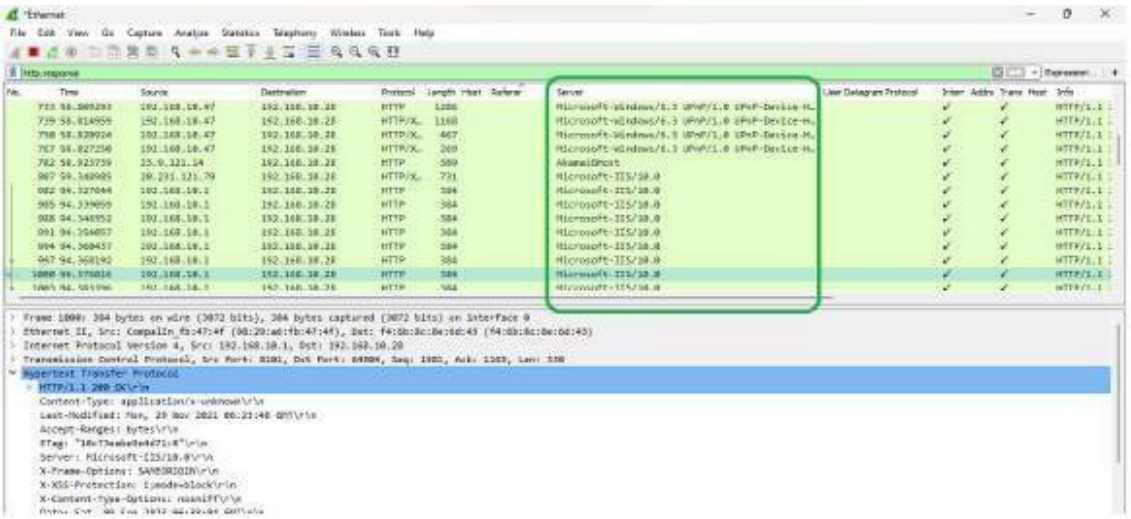
The web server name can be retrieved from **HTTP response header**. So will apply filter **http.response** and we can see all http response packets.



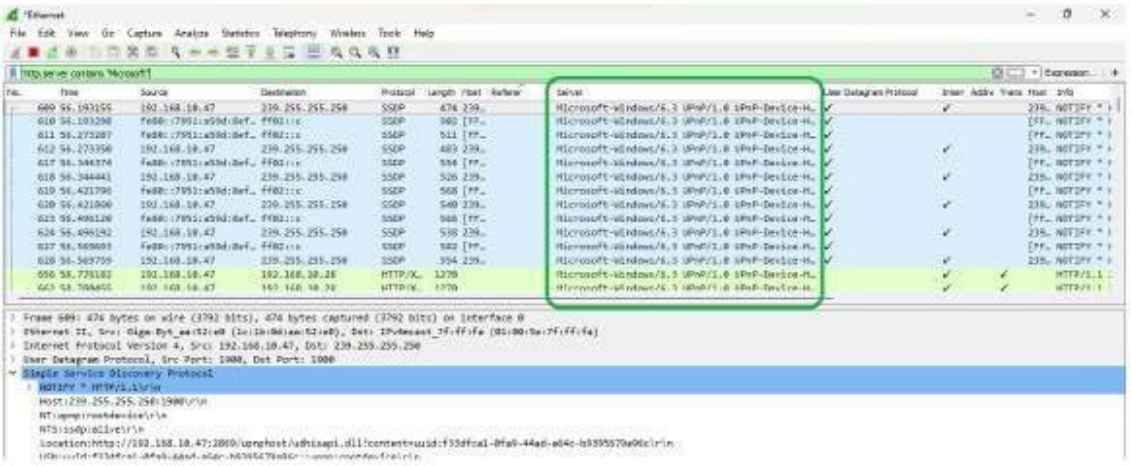
Now we will set the server header as column select any packet and right click on it then select Apply as Column.



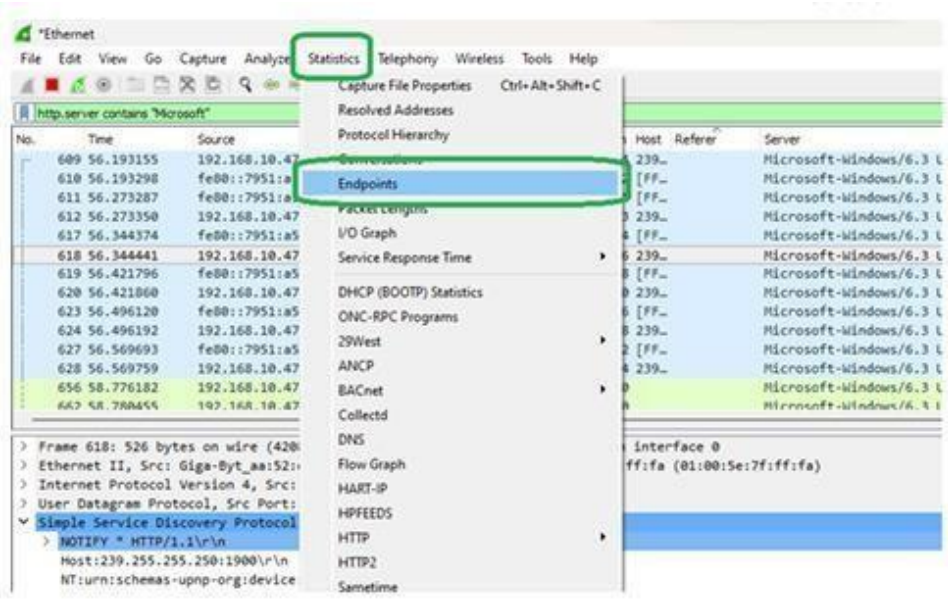
Now can see the server column where all server name is showing.



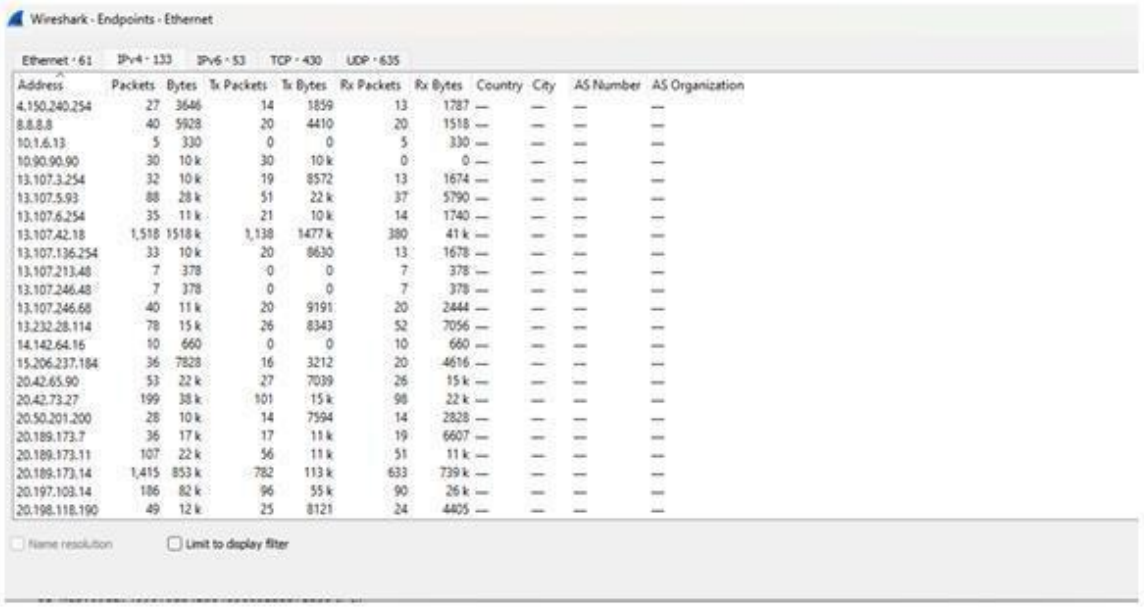
Now we have to check how many Apache packets are there we can't count manually for each packet so we will apply another filter **http.server contains "Microsoft"**



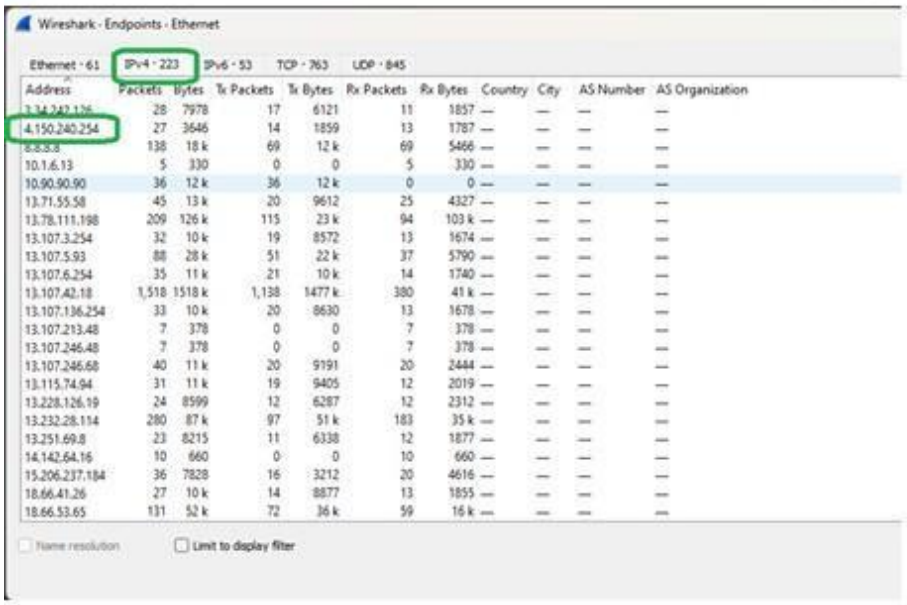
After applying filter **Go to Statistics** → **Endpoints**



It will show all connections.



Check the limit to display filter then it will show the actual Microsoft connections. Now there are showing 223 connections but will exclude 4.150.240.254 because it is client's IP not a server IP so there are actual 222 Microsoft servers.



CONCLUSION:

We have successfully analyzed the packets provided and solved the questions using WireShark

Practical No. 6

Aim: Study and implementation of e-mail forensics using AccessDataFTK.

Tool Used: AccessDataFTK.

Theory:

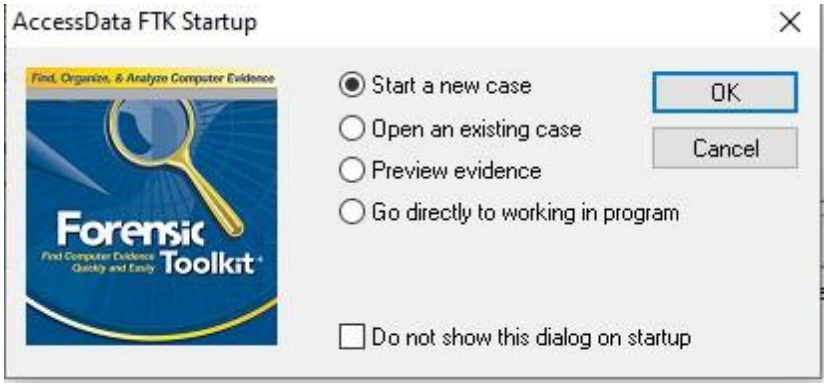
Forensic Toolkit® (FTK®)

- Recognized around the World as the Standard Digital Forensic Investigation Solution.
- FTK is a court-cited digital investigations platform built for speed, stability and ease of use.
- Furthermore, because of its architecture, FTK can be setup for distributed processing and incorporate web-based case management and collaborative analysis.
- FTK can filter or find files specific to e-mail clients and servers. You can configure these filters when you enter search parameters. In this section, we will learn how to use FTK and a hexadecimal editor to recover e-mails.
- To recover e-mail from Outlook and Outlook Express, AccessData integrated dtSearch (www.dtsearch.com) into FTK 1.x. dtSearch builds a B*-tree index of all text data in a drive, an image file, or a group of files.
- One unique feature is its capability to read .pst and .dbx files and index all text information, including attached files.

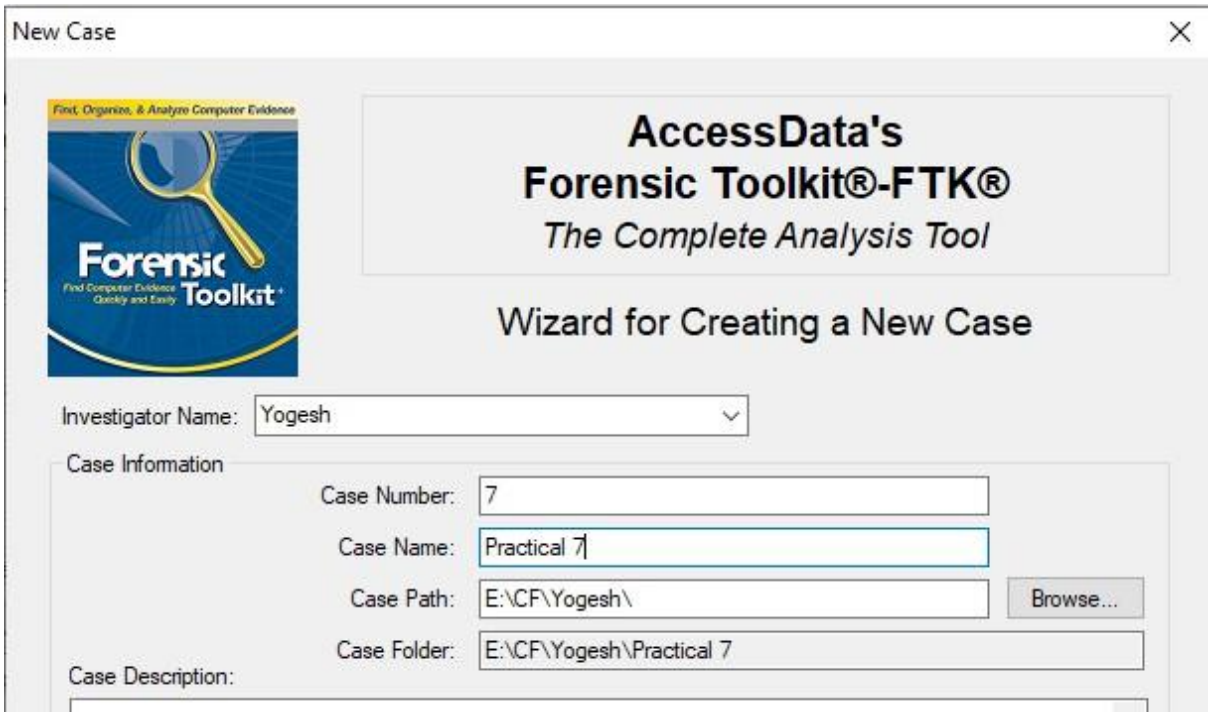
E-mail Window

- The E-mail window displays e-mail mailboxes, including Web e-mail, and their associated messages and attachments. The display is a coded HTML format.

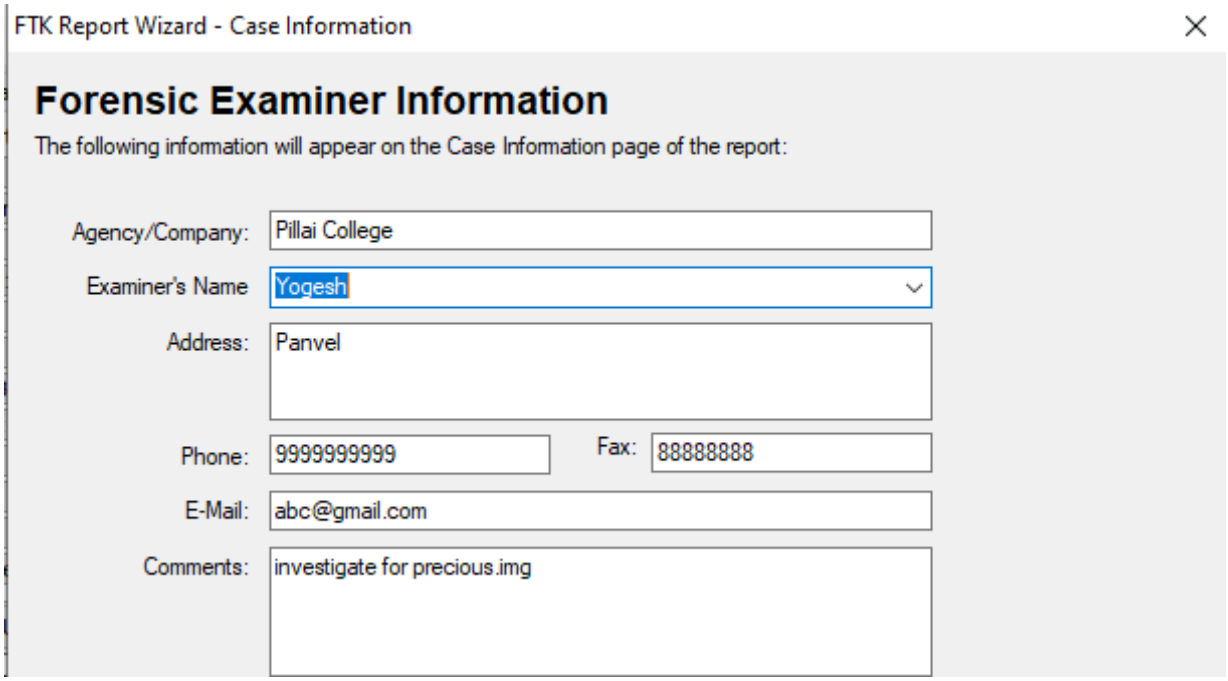
Step 1: When the AccessData FTK Startup dialog box opens, click Start a new case, and then click OK.



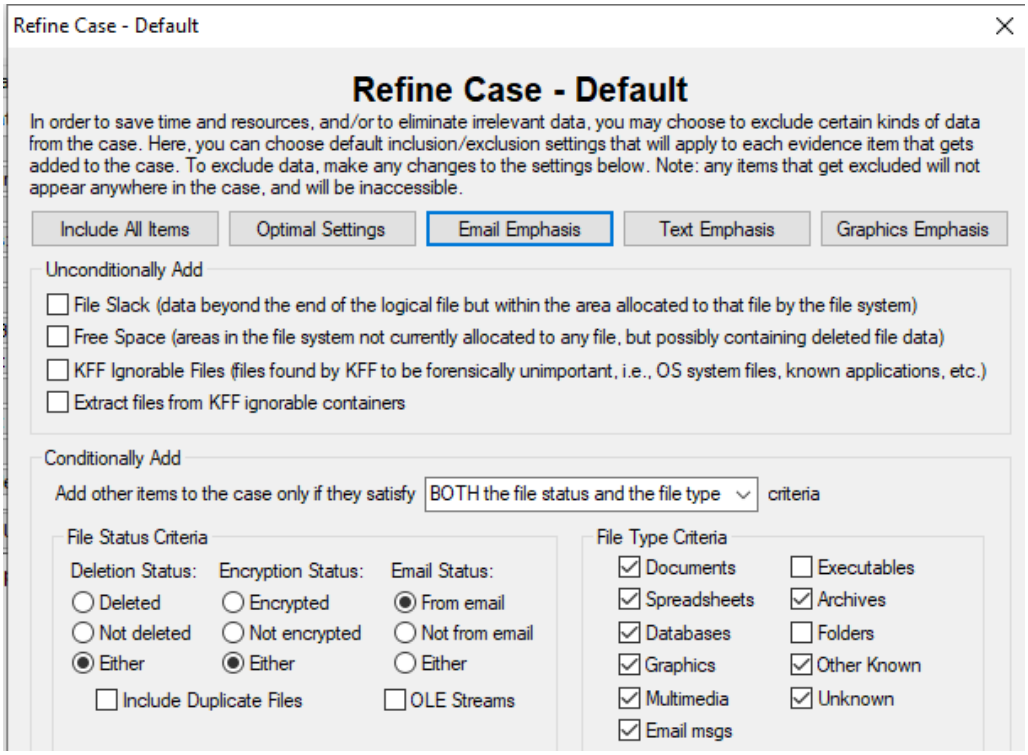
Step 2: Fill details as per the case and click Next.



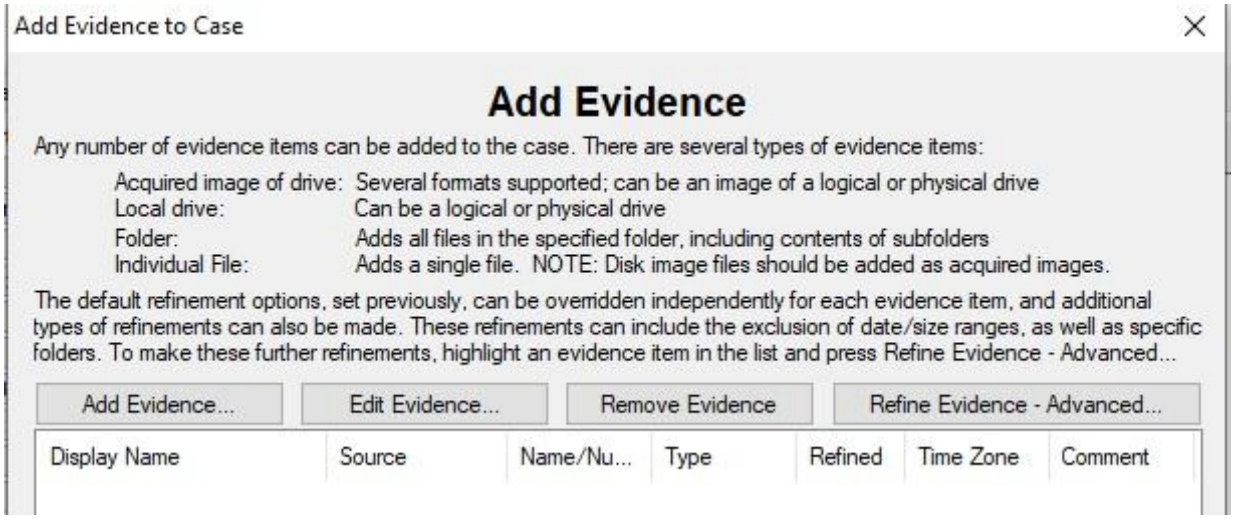
Step 3: In the Case Information dialog box, enter your investigator information, and then click Next.



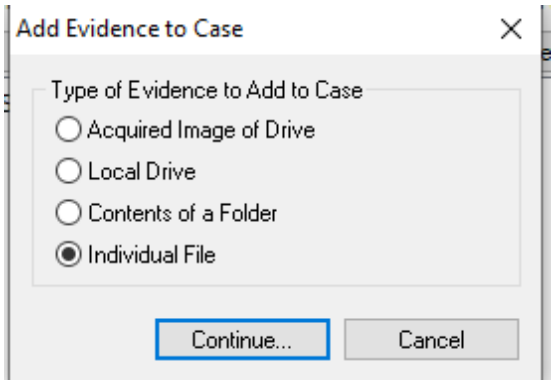
Step 4: Click Next until you reach the Refine Case - Default dialog box. Click the Email Emphasis button, and then click Next.


Refine Case - Default
Refine Case - Default
In order to save time and resources, and/or to eliminate irrelevant data, you may choose to exclude certain kinds of data from the case. Here, you can choose default inclusion/exclusion settings that will apply to each evidence item that gets added to the case. To exclude data, make any changes to the settings below. Note: any items that get excluded will not appear anywhere in the case, and will be inaccessible.
Include All Items
Optimal Settings
Email Emphasis
Text Emphasis
Graphics Emphasis
Unconditionally Add
File Slack (data beyond the end of the logical file but within the area allocated to that file by the file system)
Free Space (areas in the file system not currently allocated to any file, but possibly containing deleted file data)
KFF Ignorable Files (files found by KFF to be forensically unimportant, i.e., OS system files, known applications, etc.)
Extract files from KFF ignorable containers
Conditionally Add
Add other items to the case only if they satisfy BOTH the file status and the file type criteria
File Status Criteria
Deletion Status:
Deleted
Not deleted
Either
Encryption Status:
Encrypted
Not encrypted
Either
Email Status:
From email
Not from email
Either
Include Duplicate Files
OLE Streams
File Type Criteria
Documents
Spreadsheets
Databases
Graphics
Multimedia
Email msgs
Executables
Archives
Folders
Other Known
Unknown

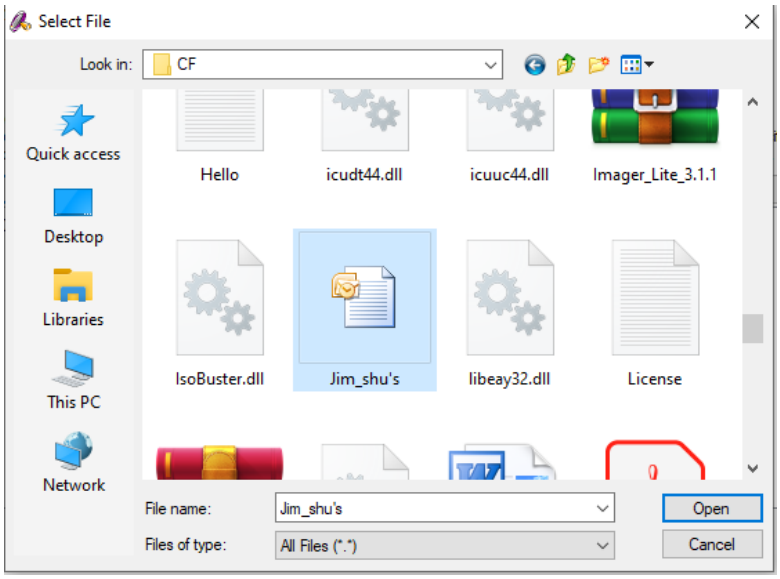
Step 5: Click Next until you reach the Add Evidence to Case dialog box, and then click the Add Evidence button.



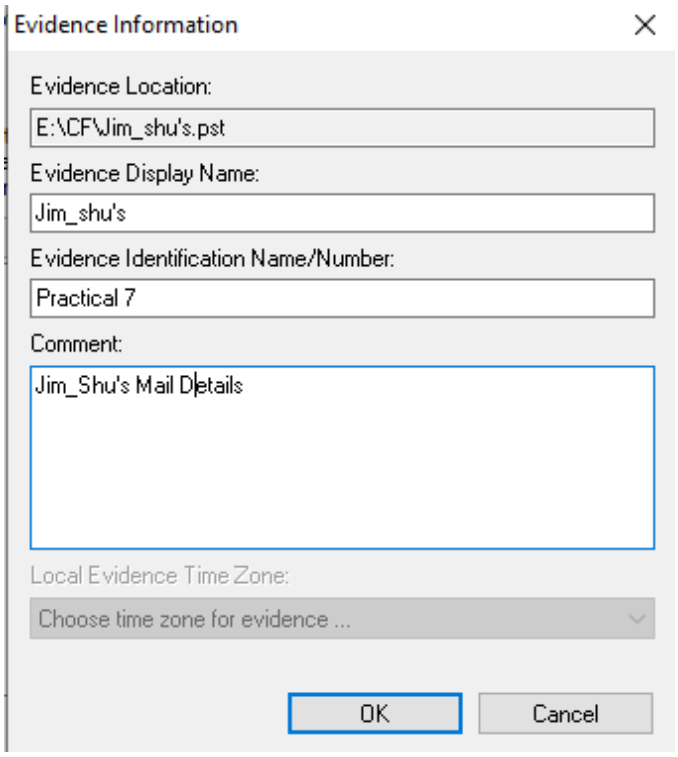
Step 6: In the Add Evidence to Case dialog box, click the Individual File option button, and then click Continue.



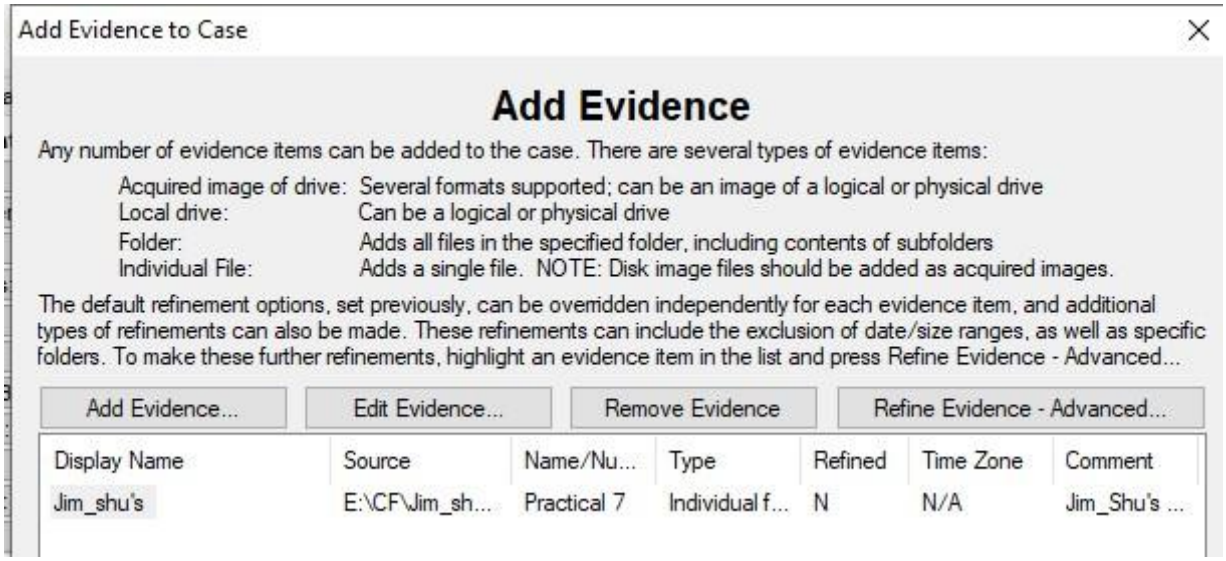
Step 7: Select the Jim_Shu's.pst and click on open.

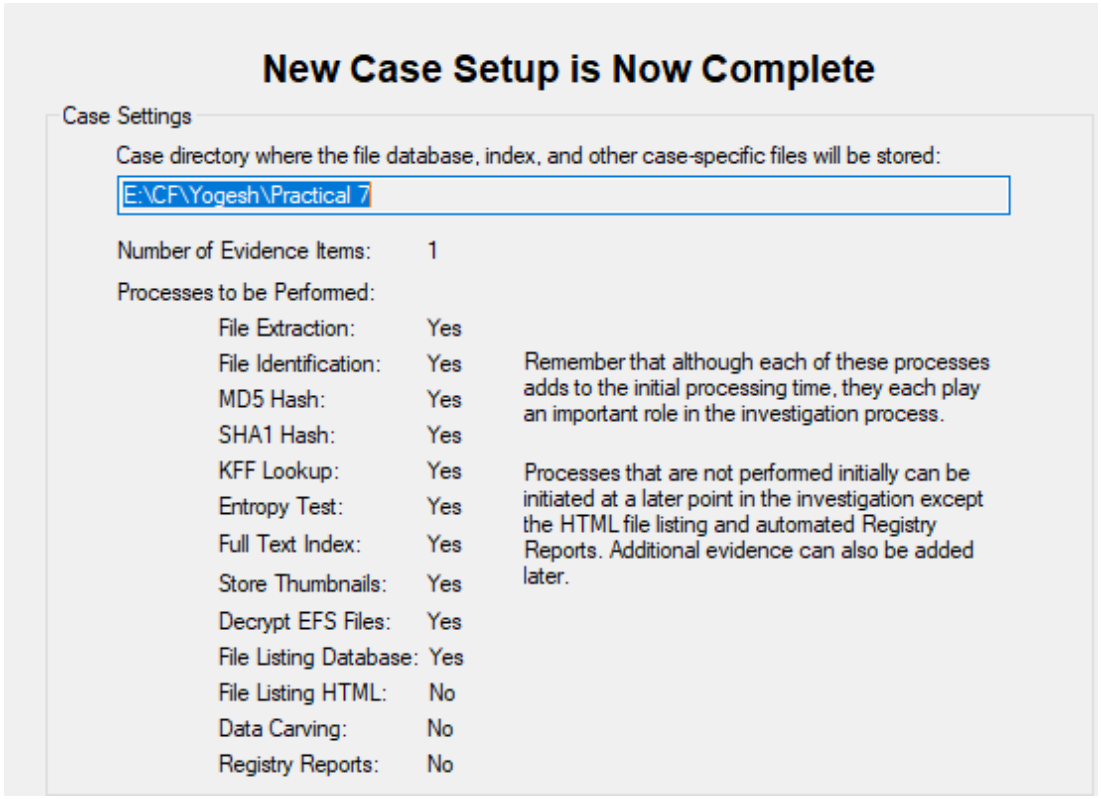


Step 8: In the Evidence Information dialog box, click OK.

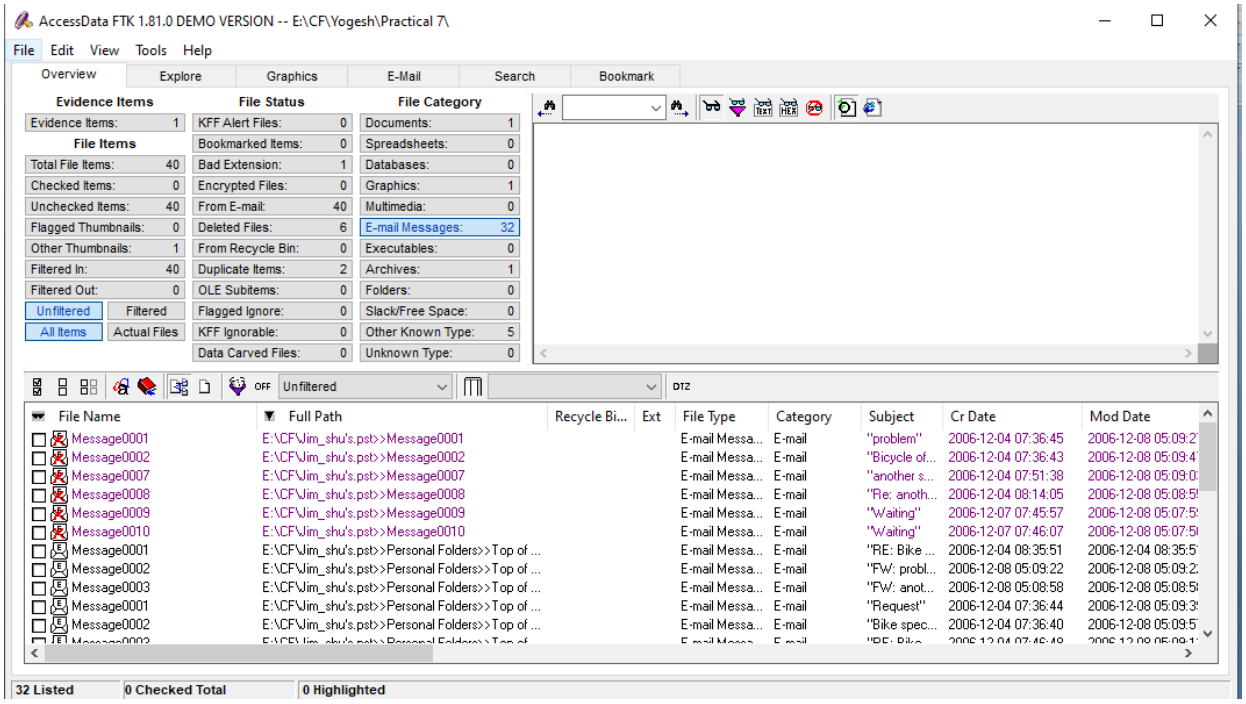


Step 9: When the Add Evidence to Case dialog box opens, click Next. In the Case summary dialog box, click Finish.

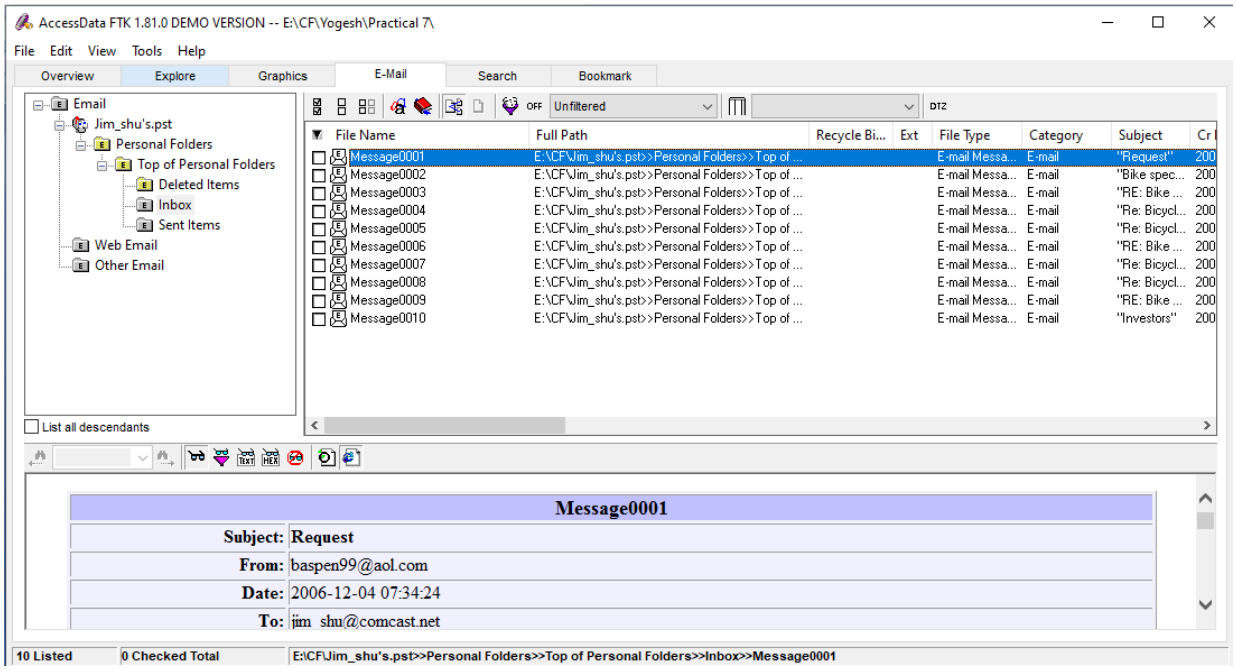




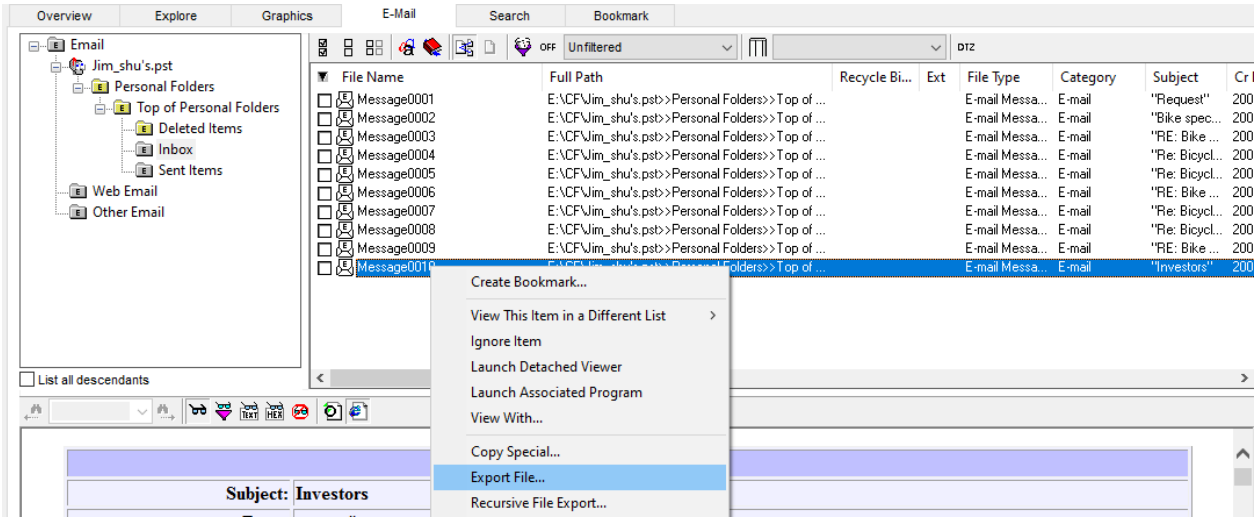
Step 10: When FTK finishes processing the file, in the main FTK window, click the E-mail Messages button, and then click the Full Path column header to sort the records.

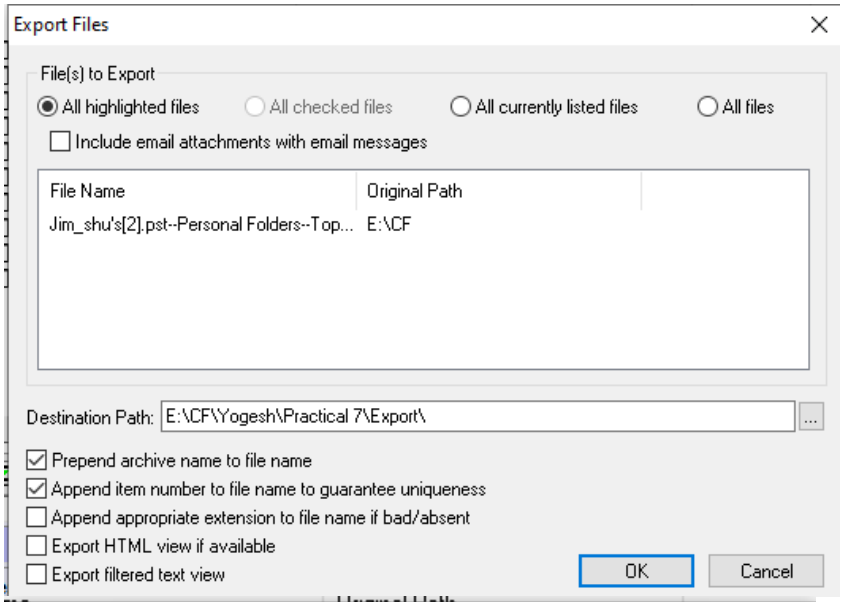


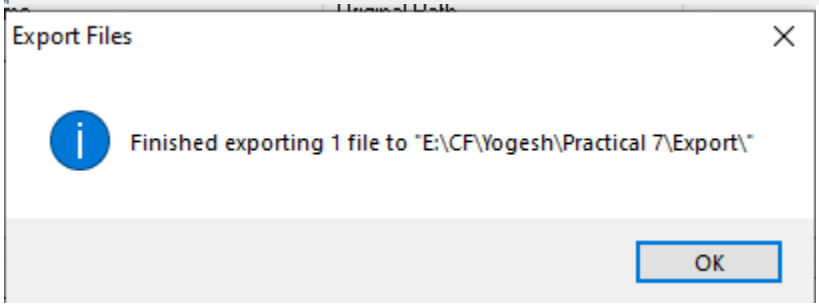
Step 11: Click the E-Mail tab. In the tree view, click to expand all folders, and then click the Inbox folder. If necessary, to view all messages, click the List all descendants check box.


AccessData FTK 1.81.0 DEMO VERSION -- E:\CF\Yogesh\Practical 7\
File Edit View Tools Help
Overview Explore Graphics E-Mail Search Bookmark
Email
Jim_shu's.pst
Personal Folders
Top of Personal Folders
Deleted Items
Inbox
Sent Items
Web Email
Other Email
List all descendants
Unfiltered
File Name Full Path Recycle Bi... Ext File Type Category Subject
Message0001 E:\CF\Jim_shu's.pst>>Personal Folders>>Top of ... E-mail Messa... E-mail "Request"
Message0002 E:\CF\Jim_shu's.pst>>Personal Folders>>Top of ... E-mail Messa... E-mail "Bike spec...
Message0003 E:\CF\Jim_shu's.pst>>Personal Folders>>Top of ... E-mail Messa... E-mail "RE: Bike ...
Message0004 E:\CF\Jim_shu's.pst>>Personal Folders>>Top of ... E-mail Messa... E-mail "Re: Bicycl...
Message0005 E:\CF\Jim_shu's.pst>>Personal Folders>>Top of ... E-mail Messa... E-mail "Re: Bicycl...
Message0006 E:\CF\Jim_shu's.pst>>Personal Folders>>Top of ... E-mail Messa... E-mail "RE: Bike ...
Message0007 E:\CF\Jim_shu's.pst>>Personal Folders>>Top of ... E-mail Messa... E-mail "Re: Bicycl...
Message0008 E:\CF\Jim_shu's.pst>>Personal Folders>>Top of ... E-mail Messa... E-mail "Re: Bicycl...
Message0009 E:\CF\Jim_shu's.pst>>Personal Folders>>Top of ... E-mail Messa... E-mail "RE: Bike ...
Message0010 E:\CF\Jim_shu's.pst>>Personal Folders>>Top of ... E-mail Messa... E-mail "Investors"
Message0001
Subject: Request
From: baspen99@aol.com
Date: 2006-12-04 07:34:24
To: jim_shu@comcast.net
10 Listed
0 Checked Total
E:\CF\Jim_shu's.pst>>Personal Folders>>Top of Personal Folders>>Inbox>>Message0001

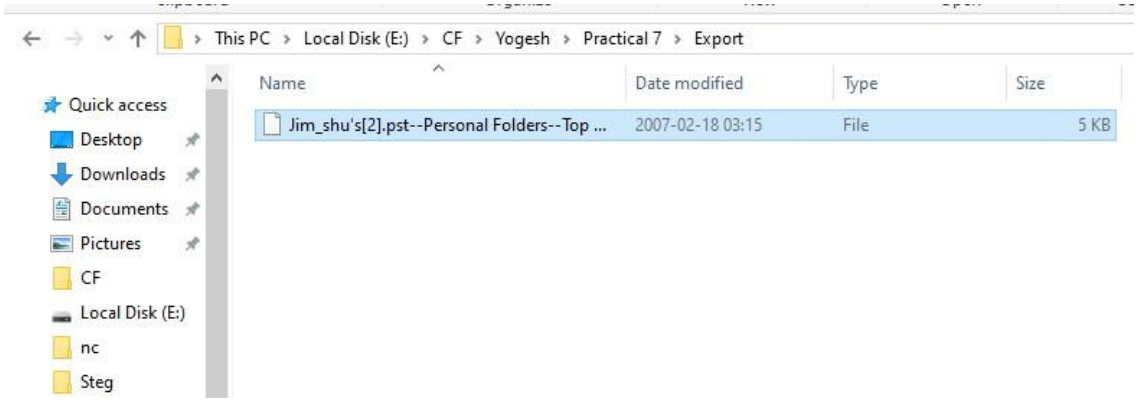
Step 12: Right-click Message0010 in the File List pane and click Export File. In the Export Files dialog box, click OK. Click OK again in the Export Files message box.

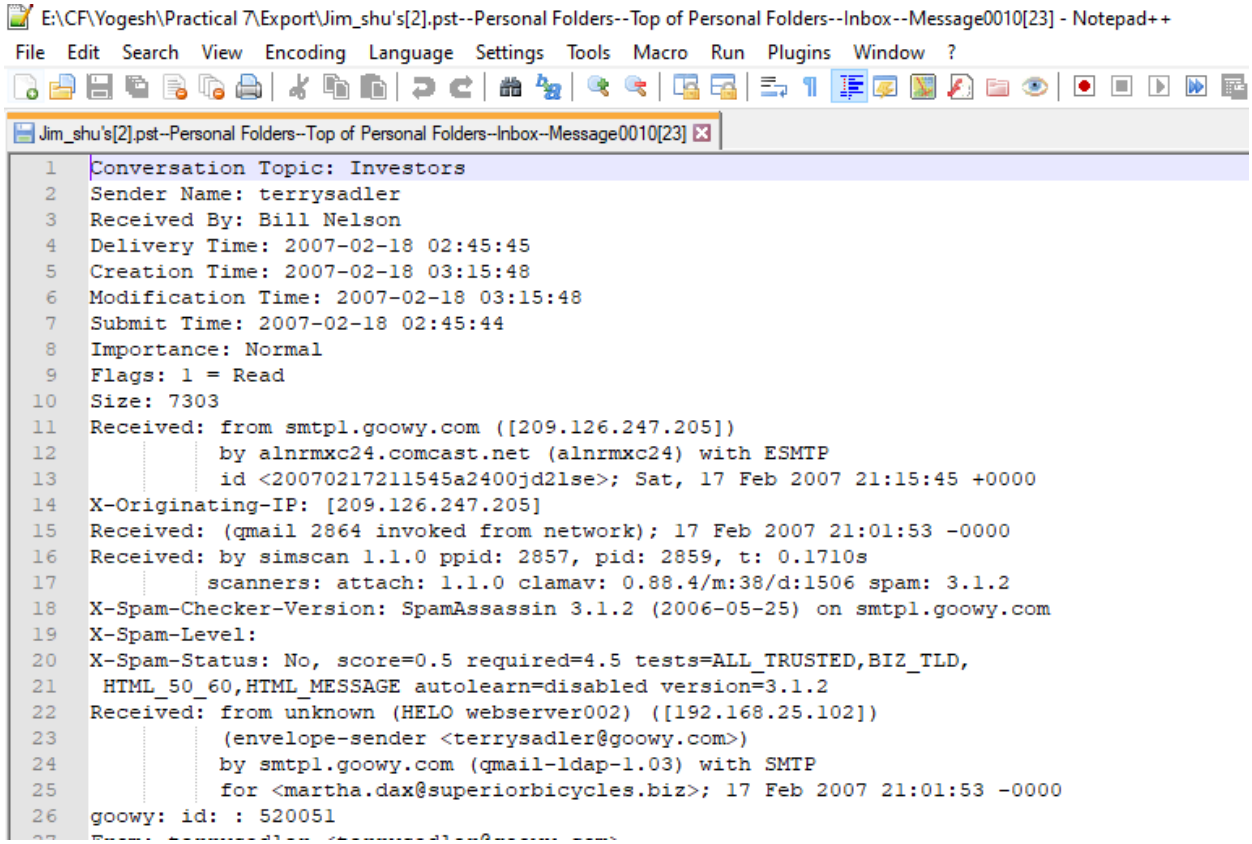






Step 13: To view the exported Message0010 file, go to your work folder.





Conclusion: Hence, we successfully perform e-mail forensics using AccessDataFTK on Jim_Shu's.pst.

Practical No. 7

Aim: Generating forensics report using sleuth kit.

Tool Used: Autopsy.

Theory:

Autopsy

- Autopsy is an open source forensics tool that can be compared to FTK or EnCase and is able to assist investigators when working on cases.

- The Autopsy is a graphical interface to the command line digital investigation tools in The Sleuth Kit. Together, they allow you to investigate the file system and volumes of a computer.

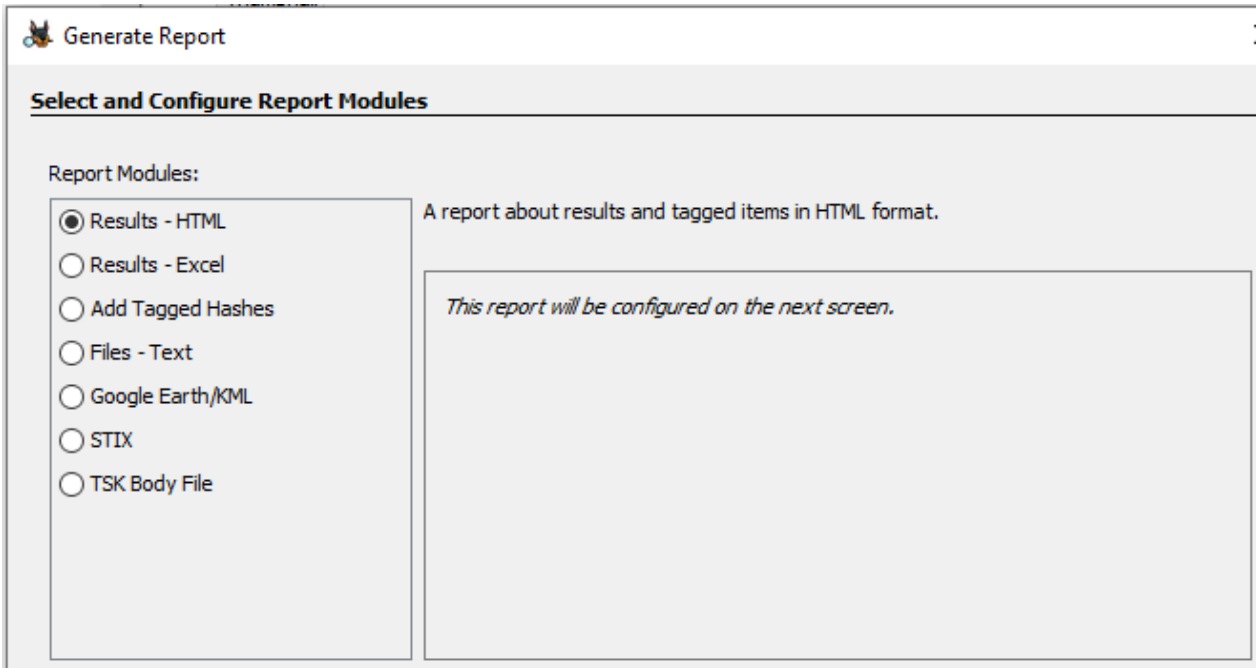
Why Reporting is important?

- Documentation is an ongoing process throughout the examination. It is important to accurately record the steps taken during the digital evidence examination.

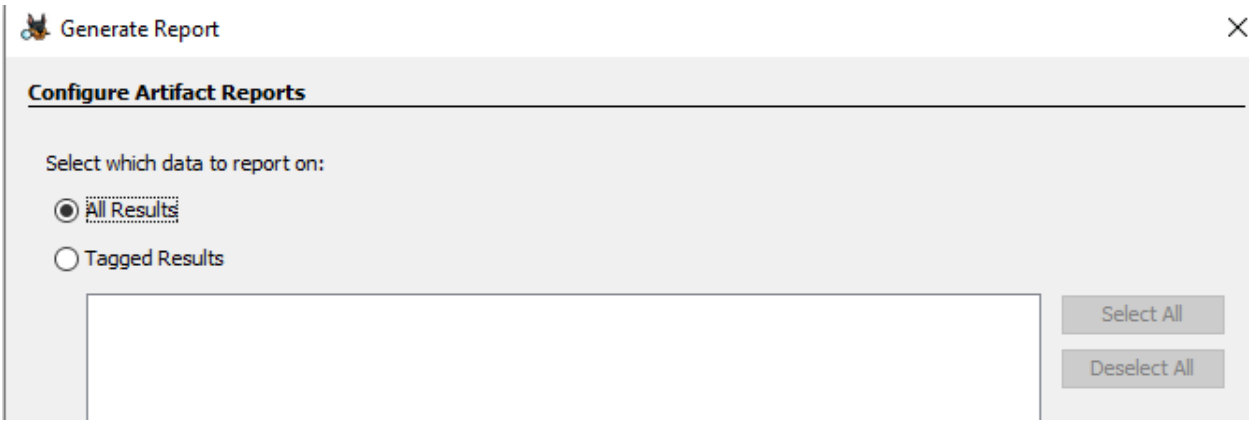
- The examiner is responsible for completely and accurately reporting his or her findings and the results of the analysis of the digital evidence examination.

Whether you are doing a forensic report that simply states facts coming from testing, or an expert report that expresses expert opinion

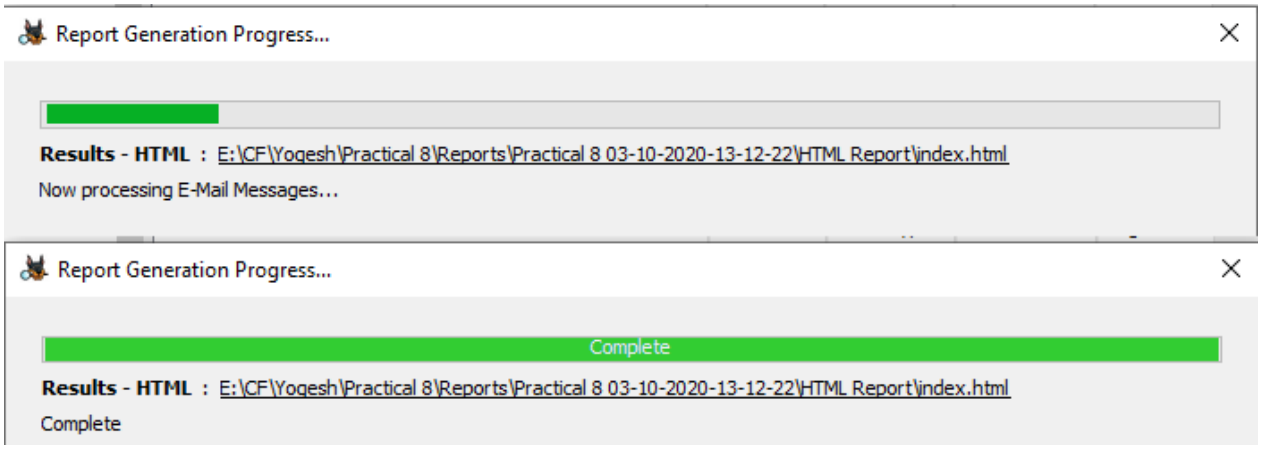
Step 1: To generate reports, click on Generate Report Option which opens up Generate Report Wizard Select the type you want to save results and click Next.



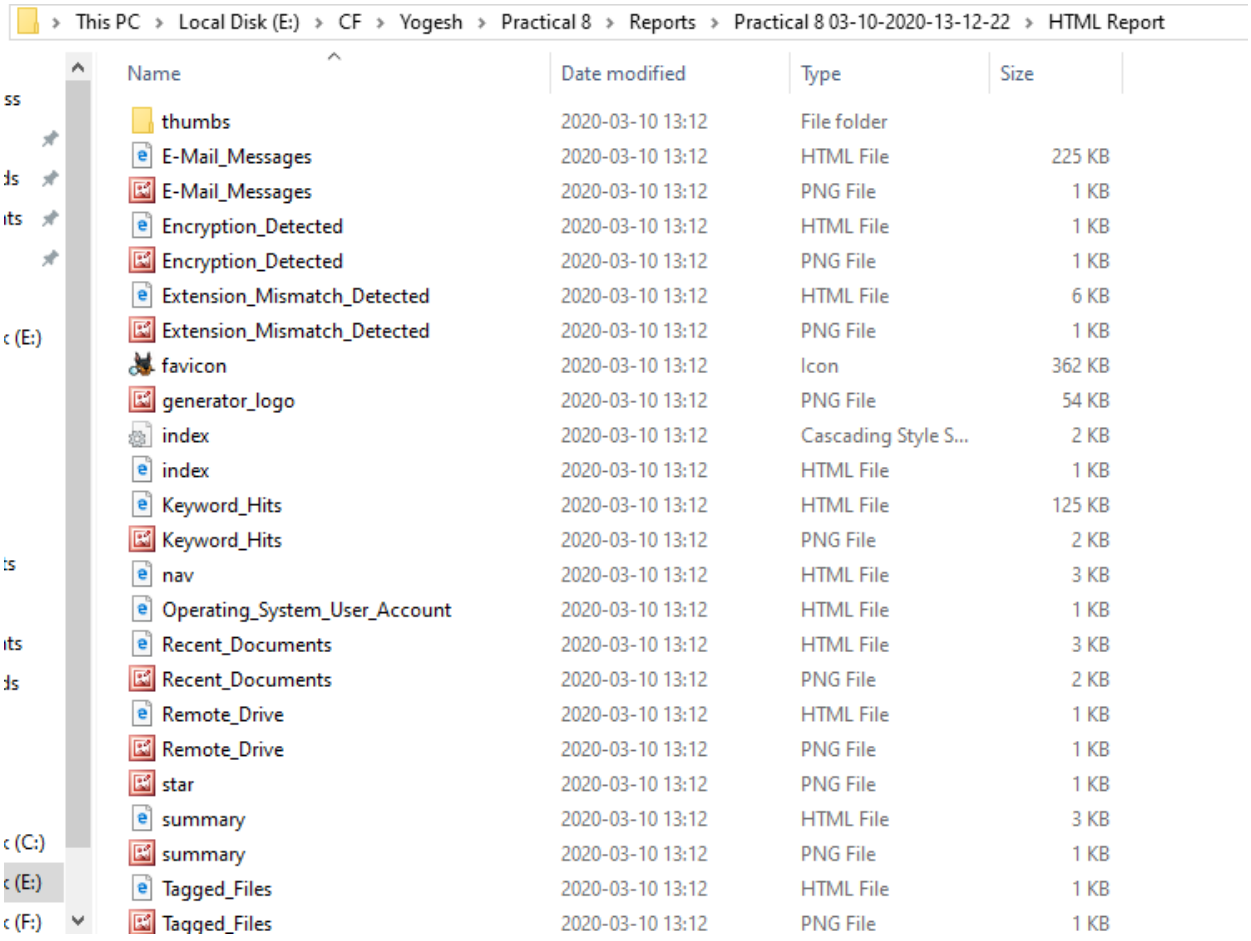
Step 2: Select All Results and click Finish.



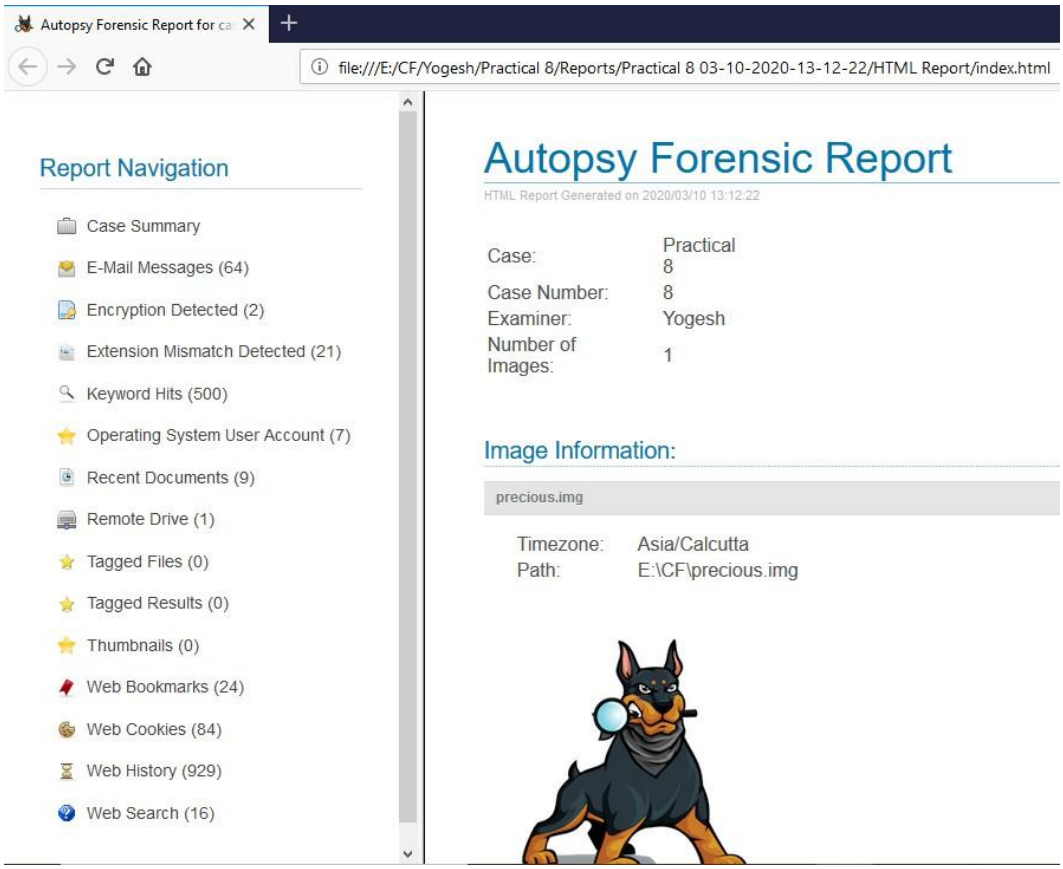
Step 3: The report generation is completed and results are stored in link specified. Click Close.

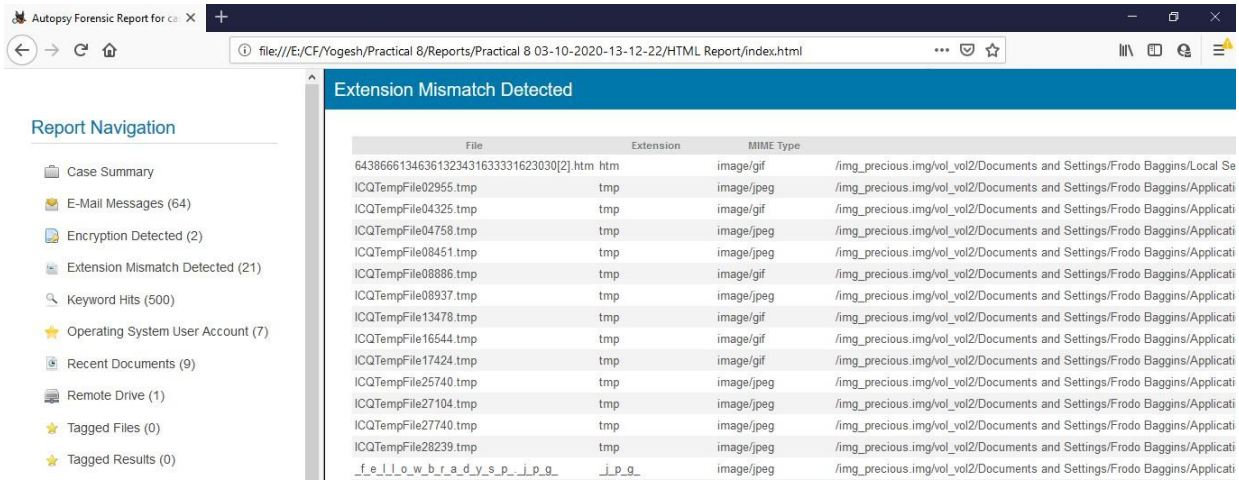


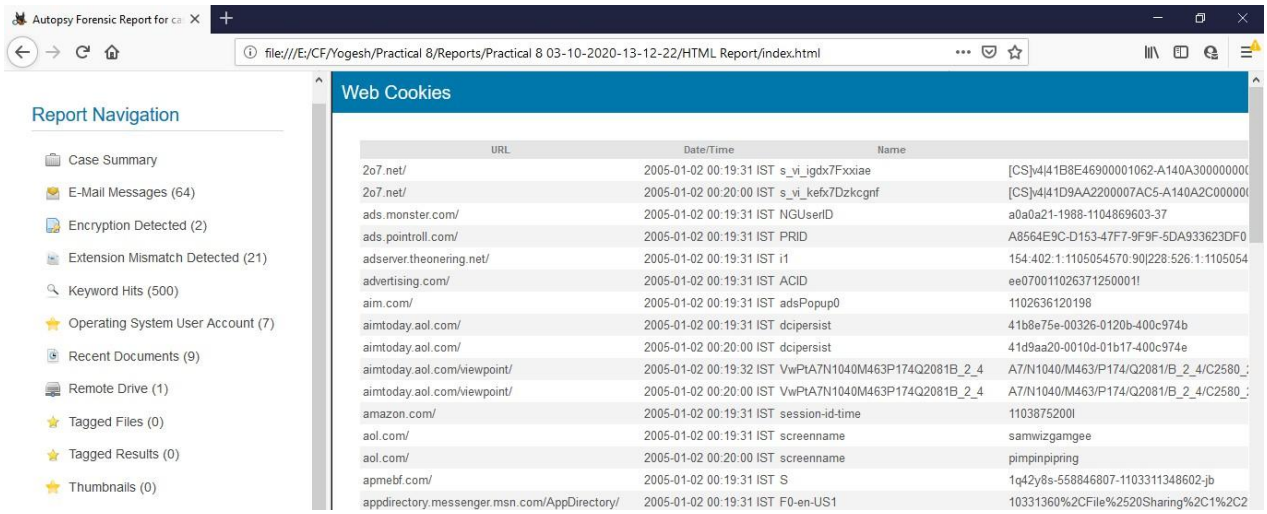
Step 4: Browse through path given and open index.html file.

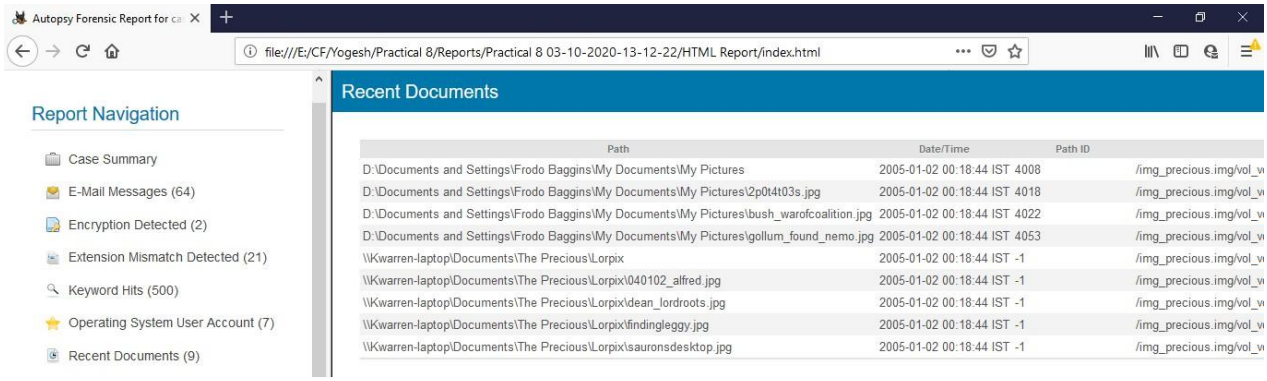


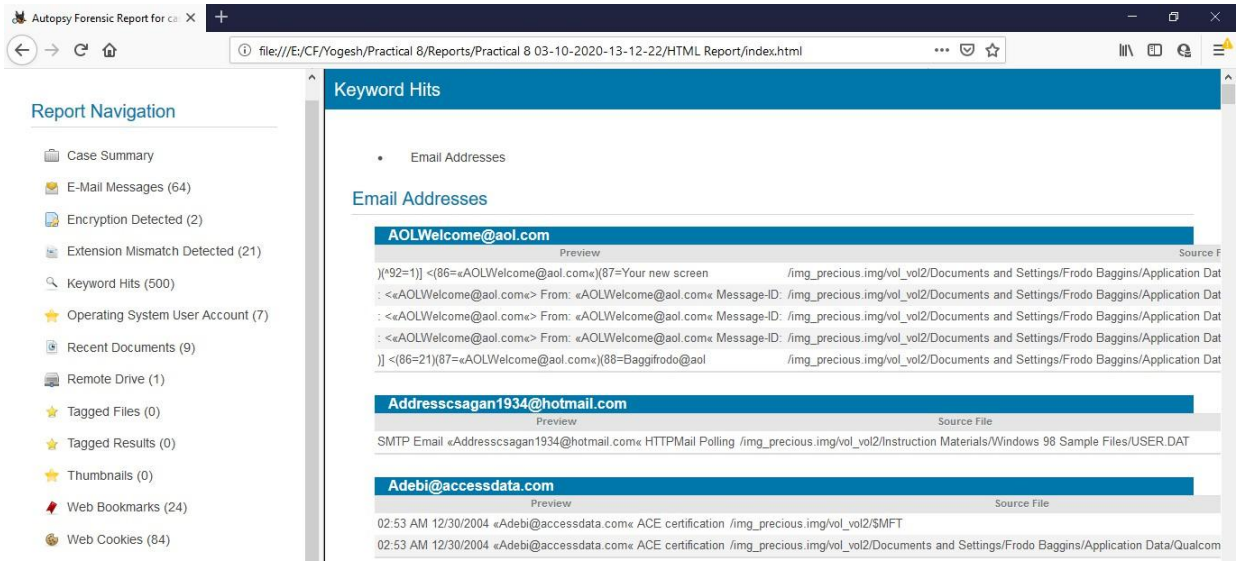
Step 5: The reports are generated in html file.



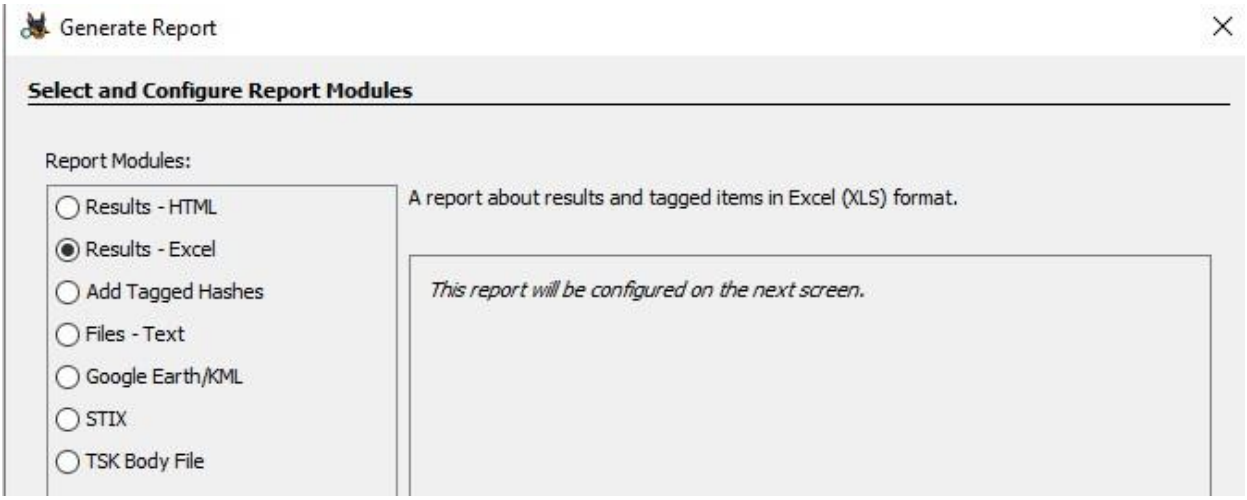


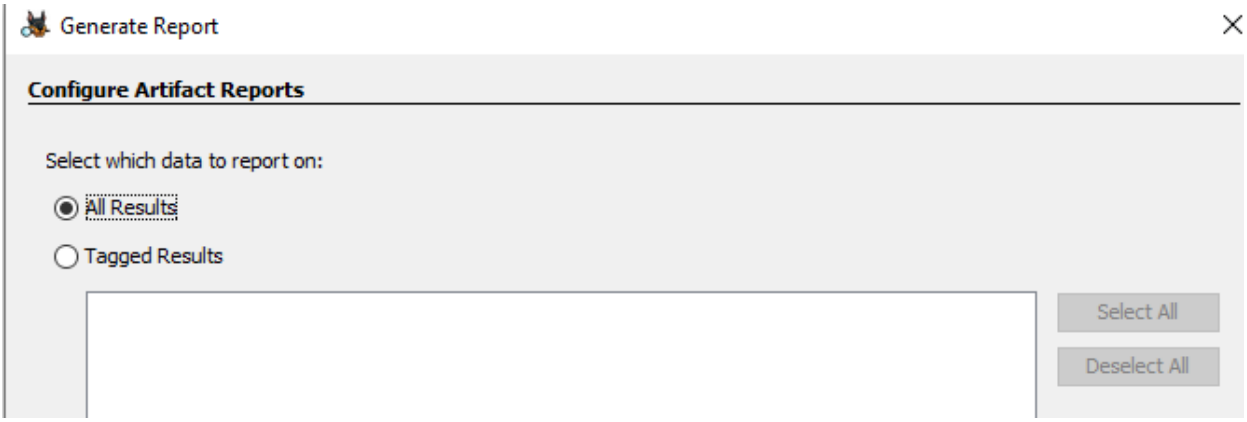

Autopsy Forensic Report for ca
file:///E:/CF/Yogesh/Practical 8/Reports/Practical 8 03-10-2020-13-12-22/HTML Report/index.html
Report Navigation
Case Summary
E-Mail Messages (64)
Encryption Detected (2)
Extension Mismatch Detected (21)
Keyword Hits (500)
Operating System User Account (7)
Recent Documents (9)
Remote Drive (1)
Tagged Files (0)
Tagged Results (0)
Thumbnails (0)
Web Cookies
URL Date/Time Name
2o7.net/ 2005-01-02 00:19:31 IST s_vi_igdx7Fxxiae
2o7.net/ 2005-01-02 00:20:00 IST s_vi_kefx7Dzkcgnf
ads.monster.com/ 2005-01-02 00:19:31 IST NGUserID a0a0a21-1988-110486960 3-37
ads.pointroll.com/ 2005-01-02 00:19:31 IST PRID A8564E9C-D153-47F7-9F9F-5DA933623DF0
adserver.theonering.net/ 2005-01-02 00:19:31 IST i1
advertising.com/ 2005-01-02 00:19:31 IST ACID
aim.com/ 2005-01-02 00:19:31 IST adsPopup0 1102636120198
aimtoday.aol.com/ 2005-01-02 00:19:31 IST dcipersist 41b8e75e-00326-0120b-400c974b
aimtoday.aol.com/ 2005-01-02 00:20:00 IST dcipersist 41d9aa20-0010d-01b17-400c974e
aimtoday.aol.com/viewpoint/ 2005-01-02 00:19:32 IST VwPtA7N1040M463P174Q2081B_2_4
aimtoday.aol.com/viewpoint/ 2005-01-02 00:20:00 IST VwPtA7N1040M463P174Q2081B_2_4
amazon.com/ 2005-01-02 00:19:31 IST session-id-time 1103875200l
aol.com/ 2005-01-02 00:19:31 IST screenname samwizgamgee
aol.com/ 2005-01-02 00:20:00 IST screenname pimpinpipring
apmebf.com/ 2005-01-02 00:19:31 IST S 1q42y8s-558846807-1103311348602-jb
appdirectory.messenger.msn.com/AppDirectory/ 2005-01-02 00:19:31 IST F0-en-US1 10331360%2CFile%2520Sharing%2C1%2C2

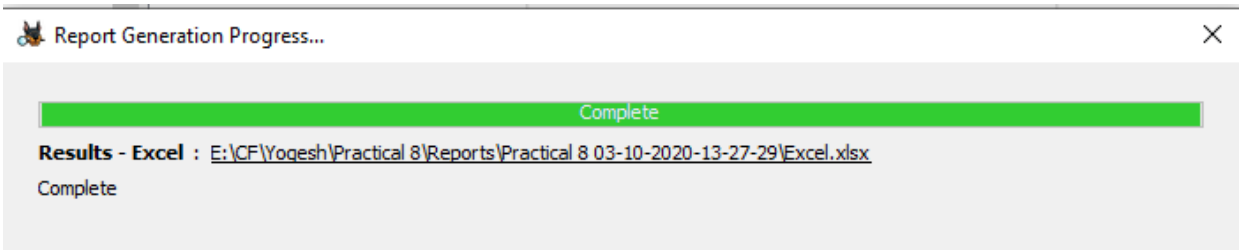

Autopsy Forensic Report for ca
file:///E:/CF/Yogesh/Practical 8/Reports/Practical 8 03-10-2020-13-12-22/HTML Report/index.html
Report Navigation
Case Summary
E-Mail Messages (64)
Encryption Detected (2)
Extension Mismatch Detected (21)
Keyword Hits (500)
Operating System User Account (7)
Recent Documents (9)
Recent Documents
Path Date/Time Path ID
D:\Documents and Settings\Frodo Baggins\My Documents\My Pictures 2005-01-02 00:18:44 IST 4008 /img_precious.img/vol_v
D:\Documents and Settings\Frodo Baggins\My Documents\My Pictures\2p0t4t03s.jpg 2005-01-02 00:18:44 IST 4018 /img_precious.img/vol_v
D:\Documents and Settings\Frodo Baggins\My Documents\My Pictures\bush_warofcoalition.jpg 2005-01-02 00:18:44 IST 4022 /img_precious.img/vol_v
D:\Documents and Settings\Frodo Baggins\My Documents\My Pictures\gollum_found_nemo.jpg 2005-01-02 00:18:44 IST 4053 /img_precious.img/vol_v
\\Kwarren-laptop\Documents\The Precious\Lorpix 2005-01-02 00:18:44 IST -1 /img_precious.img/vol_v
\\Kwarren-laptop\Documents\The Precious\Lorpix\040102_alfred.jpg 2005-01-02 00:18:44 IST -1 /img_precious.img/vol_v
\\Kwarren-laptop\Documents\The Precious\Lorpix\dean_lordroots.jpg 2005-01-02 00:18:44 IST -1 /img_precious.img/vol_v
\\Kwarren-laptop\Documents\The Precious\Lorpix\findingleggy.jpg 2005-01-02 00:18:44 IST -1 /img_precious.img/vol_v
\\Kwarren-laptop\Documents\The Precious\Lorpix\sauronsdesktop.jpg 2005-01-02 00:18:44 IST -1 /img_precious.img/vol_v


Autopsy Forensic Report for ca
file:///E:/CF/Yogesh/Practical 8/Reports/Practical 8 03-10-2020-13-12-22/HTML Report/index.html
Report Navigation
Case Summary
E-Mail Messages (64)
Encryption Detected (2)
Extension Mismatch Detected (21)
Keyword Hits (500)
Operating System User Account (7)
Recent Documents (9)
Remote Drive (1)
Tagged Files (0)
Tagged Results (0)
Thumbnails (0)
Web Bookmarks (24)
Web Cookies (84)
Keyword Hits
Email Addresses
Email Addresses
AOLWelcome@aol.com
Preview Source F
)(^92=1)] <(86=«AOLWelcome@aol.com«)(87=Your new screen /img_precious.img/vol_vol2/Documents and Settings/Frodo Baggins/Application Dat
: <«AOLWelcome@aol.com«> From: «AOLWelcome@aol.com« Message-ID: /img_precious.img/vol_vol2/Documents and Settings/Frodo Baggins/Application Dat
: <«AOLWelcome@aol.com«> From: «AOLWelcome@aol.com« Message-ID: /img_precious.img/vol_vol2/Documents and Settings/Frodo Baggins/Application Dat
: <«AOLWelcome@aol.com«> From: «AOLWelcome@aol.com« Message-ID: /img_precious.img/vol_vol2/Documents and Settings/Frodo Baggins/Application Dat
)] <(86=21)(87=«AOLWelcome@aol.com«)(88=Baggifrodo@aol /img_precious.img/vol_vol2/Documents and Settings/Frodo Baggins/Application Dat
Addresscsagan1934@hotmail.com
Preview Source File
SMTP Email «Addresscsagan1934@hotmail.com« HTTPMail Polling /img_precious.img/vol_vol2/Instruction Materials/Windows 98 Sample Files/USER.DAT
Adebi@accessdata.com
Preview Source File
02:53 AM 12/30/2004 «Adebi@accessdata.com« ACE certification /img_precious.img/vol_vol2/$MFT
02:53 AM 12/30/2004 «Adebi@accessdata.com« ACE certification /img_precious.img/vol_vol2/Documents and Settings/Frodo Baggins/Application Data/Qualcom

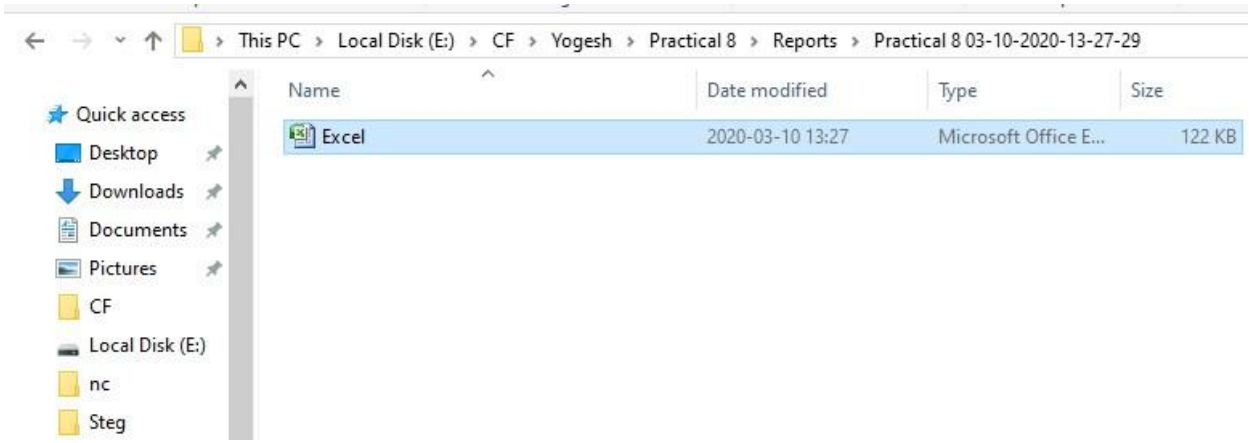
Step 6: To generate reports in Excel Format. Follow the same steps and select the option Results
– Excel and click next.



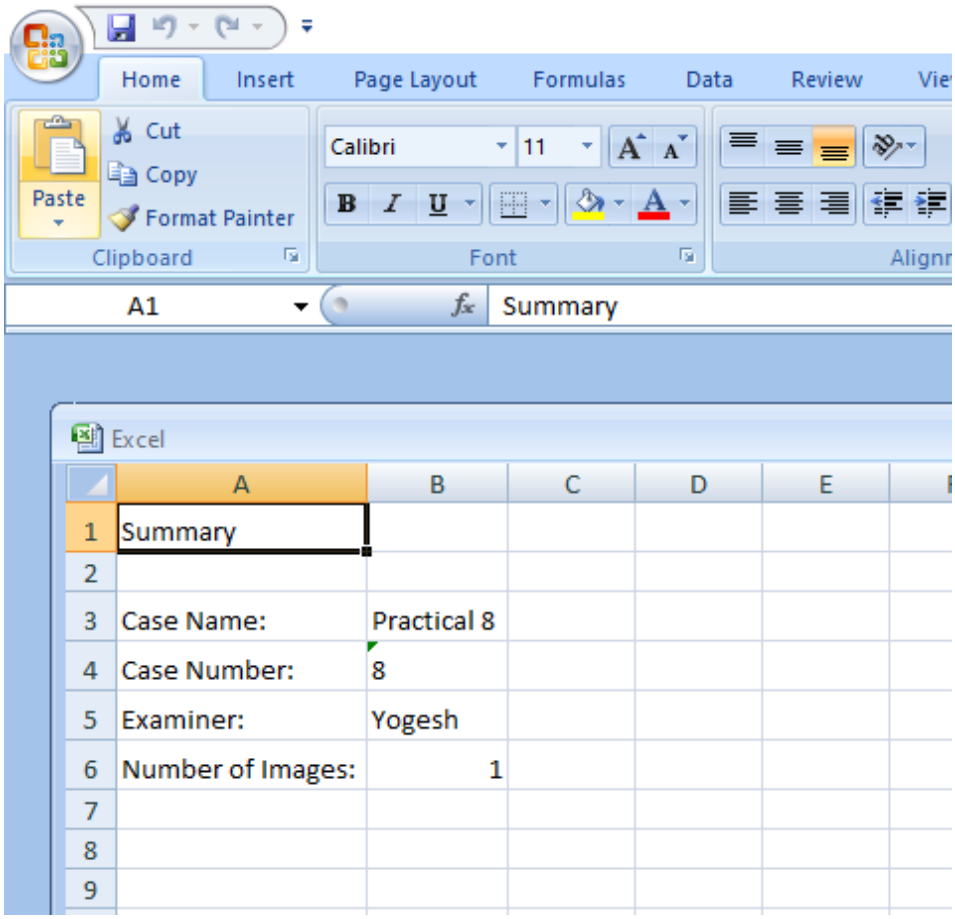


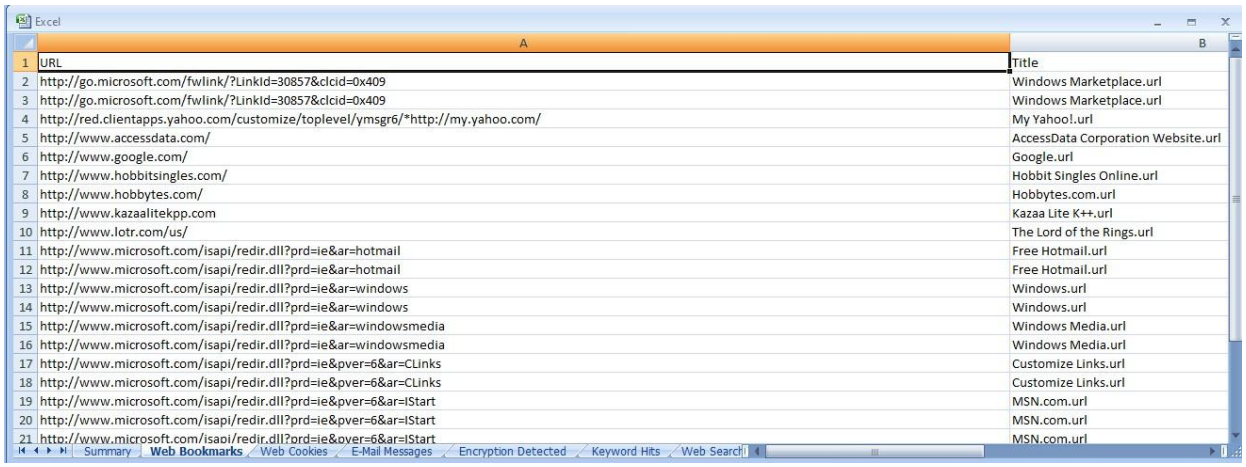


Step 7: Browse through path given and open Excel file.



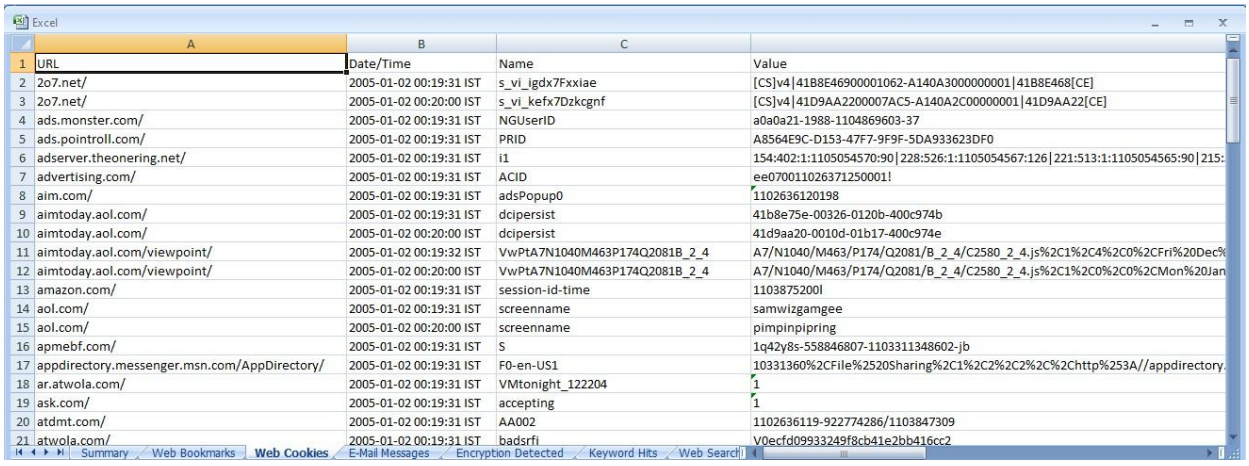
Step 8: Go through various pages to see the report.





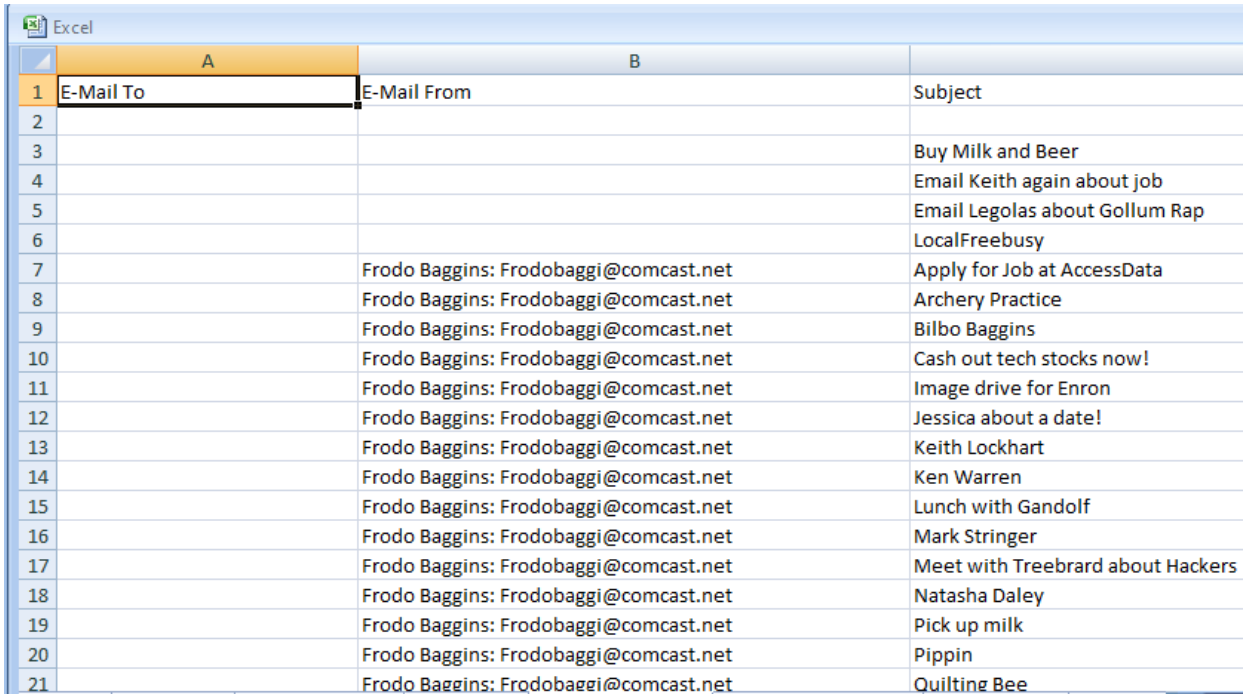
	A	B
1	URL	Title
2	http://go.microsoft.com/fwlink/?LinkId=30857&clcid=0x409	Windows Marketplace.url
3	http://go.microsoft.com/fwlink/?LinkId=30857&clcid=0x409	Windows Marketplace.url
4	http://red.clientapps.yahoo.com/customize/toplevel/ymsgr6/*http://my.yahoo.com/	My Yahoo!.url
5	http://www.accessdata.com/	AccessData Corporation Website.url
6	http://www.google.com/	Google.url
7	http://www.hobbitsingles.com/	Hobbit Singles Online.url
8	http://www.hobbytes.com/	Hobbytes.com.url
9	http://www.kazaalitekpp.com	Kazaa Lite K++.url
10	http://www.lotr.com/us/	The Lord of the Rings.url
11	http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=hotmail	Free Hotmail.url
12	http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=hotmail	Free Hotmail.url
13	http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=windows	Windows.url
14	http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=windows	Windows.url
15	http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=windowsmedia	Windows Media.url
16	http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=windowsmedia	Windows Media.url
17	http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=CLinks	Customize Links.url
18	http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=CLinks	Customize Links.url
19	http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=IStart	MSN.com.url
20	http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=IStart	MSN.com.url
21	http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=IStart	MSN.com.url

Summary | Web Bookmarks | Web Cookies | E-Mail Messages | Encryption Detected | Keyword Hits | Web Search

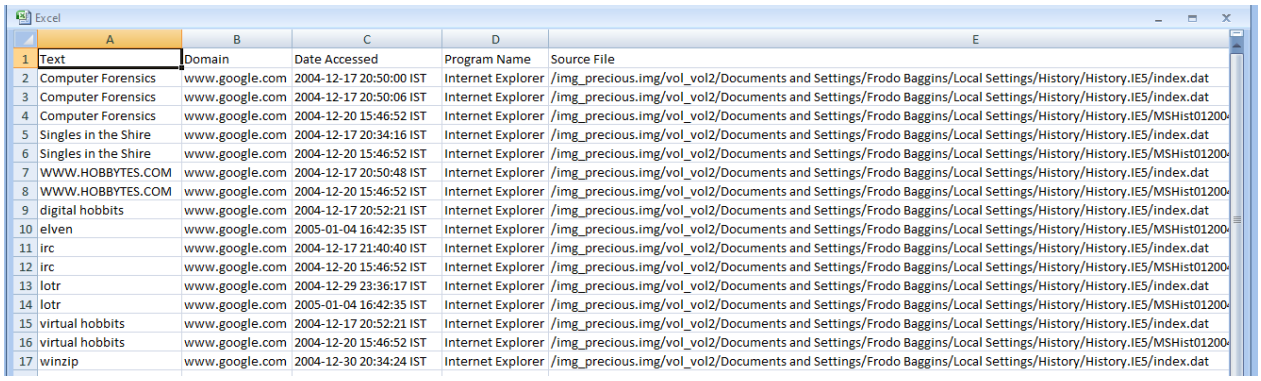


	A	B	C	
1	URL	Date/Time	Name	Value
2	2o7.net/	2005-01-02 00:19:31 IST	s_vi_igdx7Fxxiae	[CS]v4|41B8E46900001062-A140A3000000001|41B8E468[CE]
3	2o7.net/	2005-01-02 00:20:00 IST	s_vi_kefx7Dzkcgnf	[CS]v4|41D9AA2200007AC5-A140A2C00000001|41D9AA22[CE]
4	ads.monster.com/	2005-01-02 00:19:31 IST	NGUserID	a0a0a21-1988-1104869603-37
5	ads.pointroll.com/	2005-01-02 00:19:31 IST	PRID	A8564E9C-D153-47F7-9F9F-5DA933623DF0
6	adserver.theonering.net/	2005-01-02 00:19:31 IST	i1	154:402:1:1105054570:90|228:526:1:1105054567:126|221:513:1:1105054565:90|215:
7	advertising.com/	2005-01-02 00:19:31 IST	ACID	ee07001102637125000l!
8	aim.com/	2005-01-02 00:19:31 IST	adsPopup0	1102636120198
9	aimtoday.aol.com/	2005-01-02 00:19:31 IST	dcipersist	41b8e75e-00326-0120b-400c974b
10	aimtoday.aol.com/	2005-01-02 00:20:00 IST	dcipersist	41d9aa20-0010d-01b17-400c974e
11	aimtoday.aol.com/viewpoint/	2005-01-02 00:19:32 IST	VwPtA7N1040M463P174Q2081B_2_4	A7/N1040/M463/P174/Q2081/B_2_4/C2580_2_4.js%2C1%2C4%2C0%2CFri%20Dec%
12	aimtoday.aol.com/viewpoint/	2005-01-02 00:20:00 IST	VwPtA7N1040M463P174Q2081B_2_4	A7/N1040/M463/P174/Q2081/B_2_4/C2580_2_4.js%2C1%2C0%2C0%2CMon%20Jan
13	amazon.com/	2005-01-02 00:19:31 IST	session-id-time	1103875200l
14	aol.com/	2005-01-02 00:19:31 IST	screenname	samwizgamgee
15	aol.com/	2005-01-02 00:20:00 IST	screenname	pimpinpipring
16	apmebf.com/	2005-01-02 00:19:31 IST	S	1q42y8s-558846807-1103311348602-jb
17	appdirectory.messenger.msn.com/AppDirectory/	2005-01-02 00:19:31 IST	F0-en-US1	10331360%2CFile%2520Sharing%2C1%2C2%2C2%2C%2Chttp%253A//appdirectory.
18	ar.atwola.com/	2005-01-02 00:19:31 IST	VMtonight_122204	1
19	ask.com/	2005-01-02 00:19:31 IST	accepting	1
20	atdmt.com/	2005-01-02 00:19:31 IST	AA002	1102636119-922774286/1103847309
21	atwola.com/	2005-01-02 00:19:31 IST	badsrfi	V0ecfd09933249f8cb41e2bb416cc2

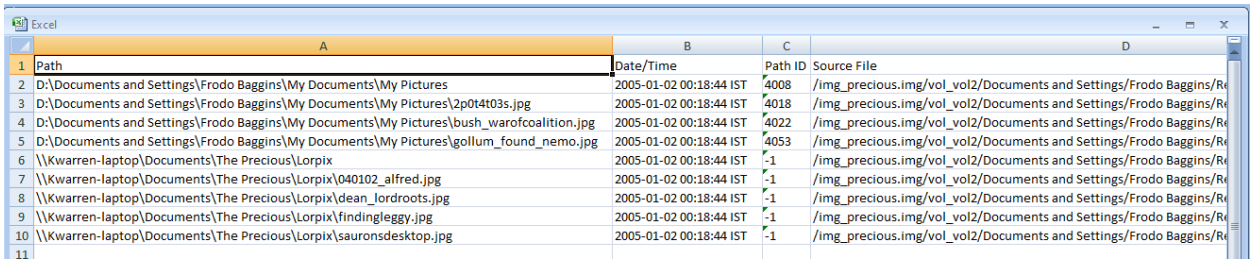
Summary | Web Bookmarks | Web Cookies | E-Mail Messages | Encryption Detected | Keyword Hits | Web Search



	A	B	
1	E-Mail To	E-Mail From	Subject
2			
3			Buy Milk and Beer
4			Email Keith again about job
5			Email Legolas about Gollum Rap
6			LocalFreebusy
7		Frodo Baggins: Frodobaggi@comcast.net	Apply for Job at AccessData
8		Frodo Baggins: Frodobaggi@comcast.net	Archery Practice
9		Frodo Baggins: Frodobaggi@comcast.net	Bilbo Baggins
10		Frodo Baggins: Frodobaggi@comcast.net	Cash out tech stocks now!
11		Frodo Baggins: Frodobaggi@comcast.net	Image drive for Enron
12		Frodo Baggins: Frodobaggi@comcast.net	Jessica about a date!
13		Frodo Baggins: Frodobaggi@comcast.net	Keith Lockhart
14		Frodo Baggins: Frodobaggi@comcast.net	Ken Warren
15		Frodo Baggins: Frodobaggi@comcast.net	Lunch with Gandolf
16		Frodo Baggins: Frodobaggi@comcast.net	Mark Stringer
17		Frodo Baggins: Frodobaggi@comcast.net	Meet with Treebrard about Hackers
18		Frodo Baggins: Frodobaggi@comcast.net	Natasha Daley
19		Frodo Baggins: Frodobaggi@comcast.net	Pick up milk
20		Frodo Baggins: Frodobaggi@comcast.net	Pippin
21		Frodo Baggins: Frodobaggi@comcast.net	Quilting Bee



	A	B	C	D	E
1	Text	Domain	Date Accessed	Program Name	Source File
2	Computer Forensics	www.google.com	2004-12-17 20:50:00 IST	Internet Explorer	/img_precious.img/vol_vol2/Documents and Settings/Frodo Baggins/Local Settings/History/History.IE5/index.dat
3	Computer Forensics	www.google.com	2004-12-17 20:50:06 IST	Internet Explorer	/img_precious.img/vol_vol2/Documents and Settings/Frodo Baggins/Local Settings/History/History.IE5/index.dat
4	Computer Forensics	www.google.com	2004-12-20 15:46:52 IST	Internet Explorer	/img_precious.img/vol_vol2/Documents and Settings/Frodo Baggins/Local Settings/History/History.IE5/MSHist01200
5	Singles in the Shire	www.google.com	2004-12-17 20:34:16 IST	Internet Explorer	/img_precious.img/vol_vol2/Documents and Settings/Frodo Baggins/Local Settings/History/History.IE5/index.dat
6	Singles in the Shire	www.google.com	2004-12-20 15:46:52 IST	Internet Explorer	/img_precious.img/vol_vol2/Documents and Settings/Frodo Baggins/Local Settings/History/History.IE5/MSHist01200
7	WWW.HOBBYTES.COM	www.google.com	2004-12-17 20:50:48 IST	Internet Explorer	/img_precious.img/vol_vol2/Documents and Settings/Frodo Baggins/Local Settings/History/History.IE5/index.dat
8	WWW.HOBBYTES.COM	www.google.com	2004-12-20 15:46:52 IST	Internet Explorer	/img_precious.img/vol_vol2/Documents and Settings/Frodo Baggins/Local Settings/History/History.IE5/MSHist01200
9	digital hobbits	www.google.com	2004-12-17 20:52:21 IST	Internet Explorer	/img_precious.img/vol_vol2/Documents and Settings/Frodo Baggins/Local Settings/History/History.IE5/index.dat
10	elven	www.google.com	2005-01-04 16:42:35 IST	Internet Explorer	/img_precious.img/vol_vol2/Documents and Settings/Frodo Baggins/Local Settings/History/History.IE5/MSHist01200
11	irc	www.google.com	2004-12-17 21:40:40 IST	Internet Explorer	/img_precious.img/vol_vol2/Documents and Settings/Frodo Baggins/Local Settings/History/History.IE5/index.dat
12	irc	www.google.com	2004-12-20 15:46:52 IST	Internet Explorer	/img_precious.img/vol_vol2/Documents and Settings/Frodo Baggins/Local Settings/History/History.IE5/MSHist01200
13	lotr	www.google.com	2004-12-29 23:36:17 IST	Internet Explorer	/img_precious.img/vol_vol2/Documents and Settings/Frodo Baggins/Local Settings/History/History.IE5/index.dat
14	lotr	www.google.com	2005-01-04 16:42:35 IST	Internet Explorer	/img_precious.img/vol_vol2/Documents and Settings/Frodo Baggins/Local Settings/History/History.IE5/MSHist01200
15	virtual hobbits	www.google.com	2004-12-17 20:52:21 IST	Internet Explorer	/img_precious.img/vol_vol2/Documents and Settings/Frodo Baggins/Local Settings/History/History.IE5/index.dat
16	virtual hobbits	www.google.com	2004-12-20 15:46:52 IST	Internet Explorer	/img_precious.img/vol_vol2/Documents and Settings/Frodo Baggins/Local Settings/History/History.IE5/MSHist01200
17	winzip	www.google.com	2004-12-30 20:34:24 IST	Internet Explorer	/img_precious.img/vol_vol2/Documents and Settings/Frodo Baggins/Local Settings/History/History.IE5/index.dat



	A	B	C	D
1	Path	Date/Time	Path ID	Source File
2	D:\Documents and Settings\Frodo Baggins\My Documents\My Pictures	2005-01-02 00:18:44 IST	4008	/img_precious.img/vol_vol2/Documents and Settings/Frodo Baggins/Re
3	D:\Documents and Settings\Frodo Baggins\My Documents\My Pictures\2p0t4t03s.jpg	2005-01-02 00:18:44 IST	4018	/img_precious.img/vol_vol2/Documents and Settings/Frodo Baggins/Re
4	D:\Documents and Settings\Frodo Baggins\My Documents\My Pictures\bush_warofcoalition.jpg	2005-01-02 00:18:44 IST	4022	/img_precious.img/vol_vol2/Documents and Settings/Frodo Baggins/Re
5	D:\Documents and Settings\Frodo Baggins\My Documents\My Pictures\gollum_found_nemo.jpg	2005-01-02 00:18:44 IST	4053	/img_precious.img/vol_vol2/Documents and Settings/Frodo Baggins/Re
6	\\Kwarren-laptop\Documents\The Precious\Lorpix	2005-01-02 00:18:44 IST	-1	/img_precious.img/vol_vol2/Documents and Settings/Frodo Baggins/Re
7	\\Kwarren-laptop\Documents\The Precious\Lorpix\040102_alfred.jpg	2005-01-02 00:18:44 IST	-1	/img_precious.img/vol_vol2/Documents and Settings/Frodo Baggins/Re
8	\\Kwarren-laptop\Documents\The Precious\Lorpix\dean_lordroots.jpg	2005-01-02 00:18:44 IST	-1	/img_precious.img/vol_vol2/Documents and Settings/Frodo Baggins/Re
9	\\Kwarren-laptop\Documents\The Precious\Lorpix\findingleggy.jpg	2005-01-02 00:18:44 IST	-1	/img_precious.img/vol_vol2/Documents and Settings/Frodo Baggins/Re
10	\\Kwarren-laptop\Documents\The Precious\Lorpix\sauronsdesktop.jpg	2005-01-02 00:18:44 IST	-1	/img_precious.img/vol_vol2/Documents and Settings/Frodo Baggins/Re
11				

Conclusion: Hence, we successfully generate forensics reports in html and excel file using sleuth kit.

Practical No. 8

Aim: Generating forensics report using AccessDataFTK.

Tool Used: AccessDataFTK.

Theory:

Forensic Toolkit® (FTK®)

- Recognized around the World as the Standard Digital Forensic Investigation Solution.

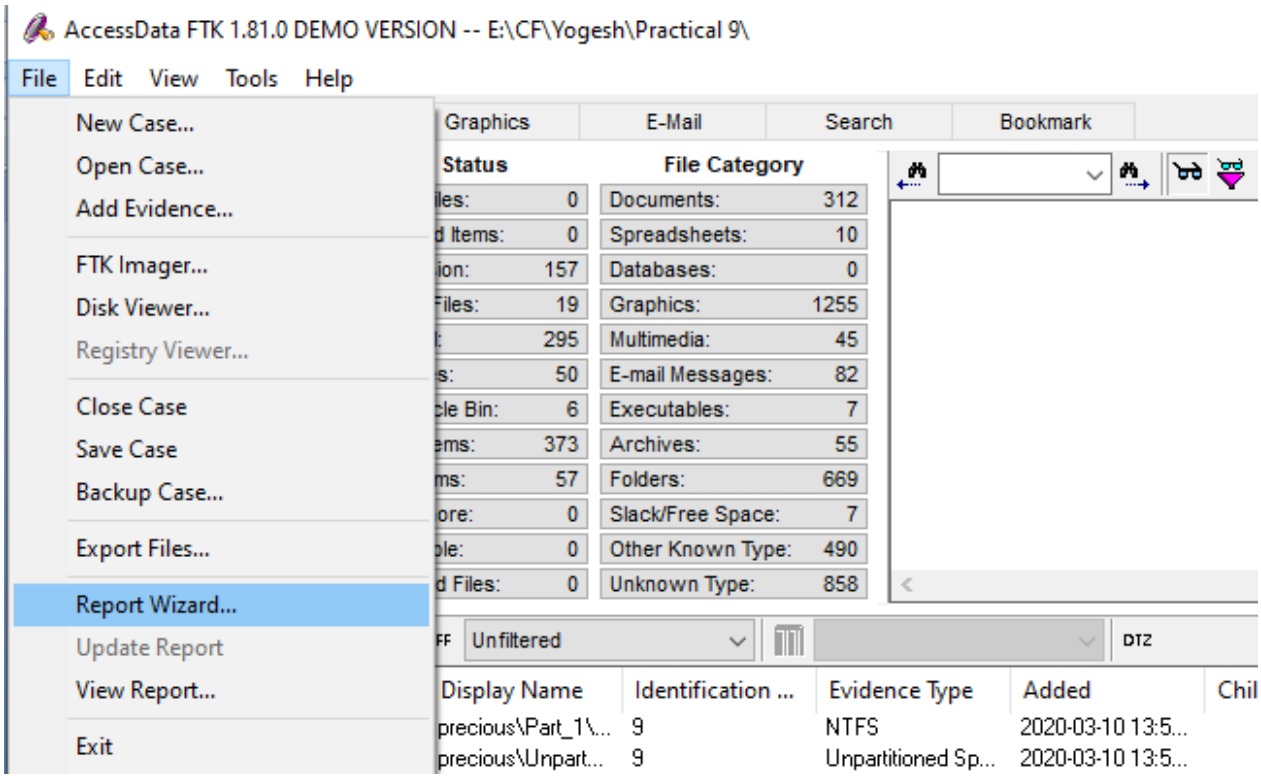
FTK is a court-cited digital investigations platform built for speed, stability and ease of use.

Why Reporting is important?

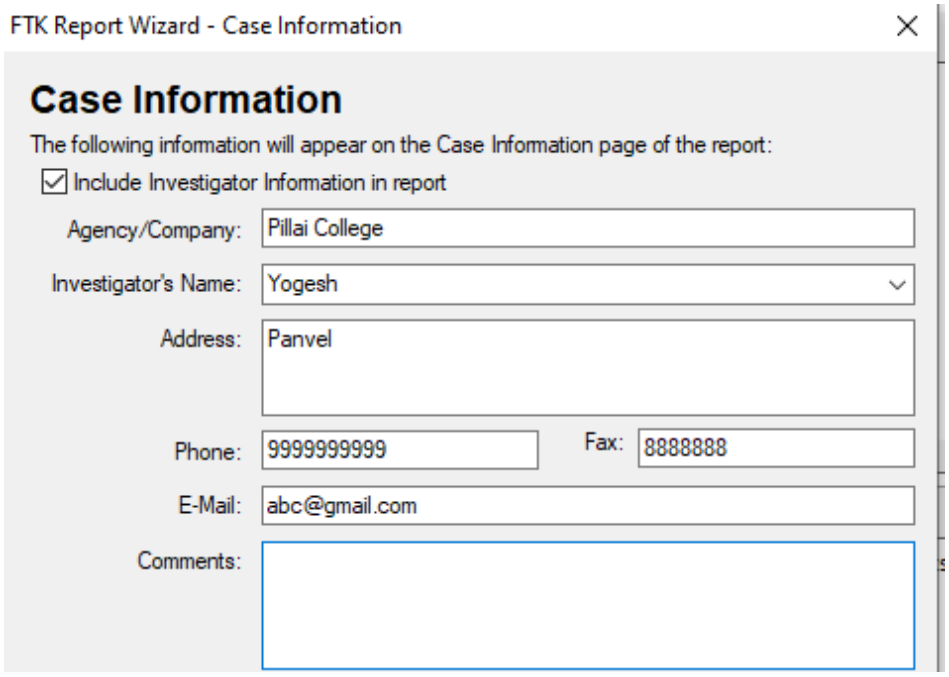
- Documentation is an ongoing process throughout the examination. It is important to accurately record the steps taken during the digital evidence examination.
- The examiner is responsible for completely and accurately reporting his or her findings and the results of the analysis of the digital evidence examination.
- With the report on hand the investigator will have an idea of what to expect as well as a list of programs that are installed on the machine.
- This can help investigators gather all the evidence they need to perform a complete investigation.

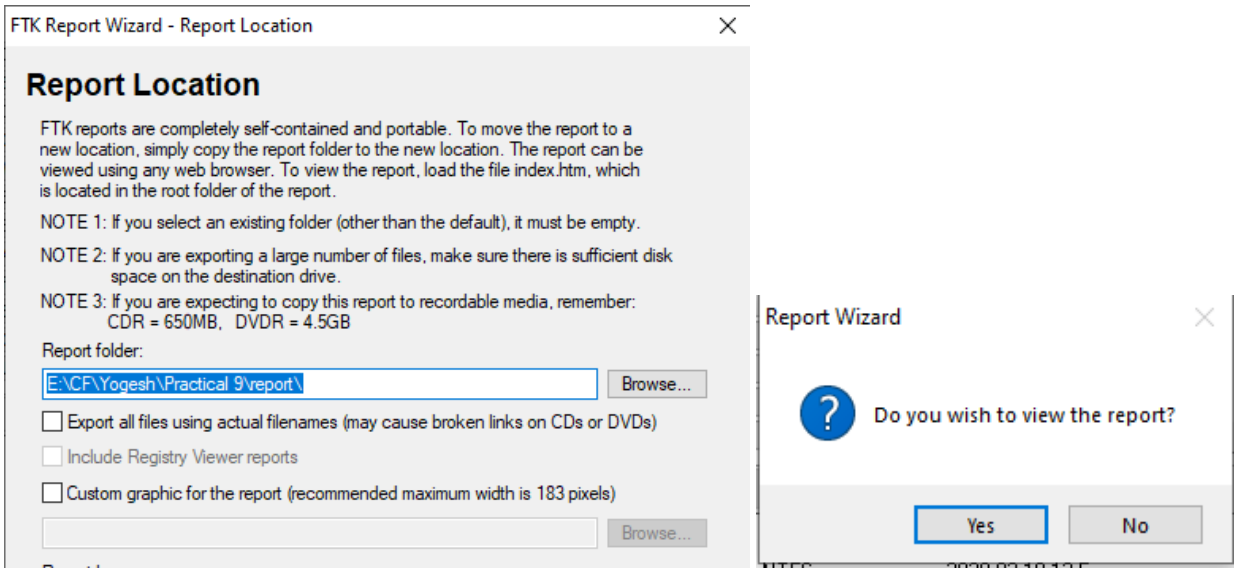
Whether you are doing a forensic report that simply states facts coming from testing, or an expert report that expresses expert opinion.

Step 1: Go to File and click on Report Wizard.

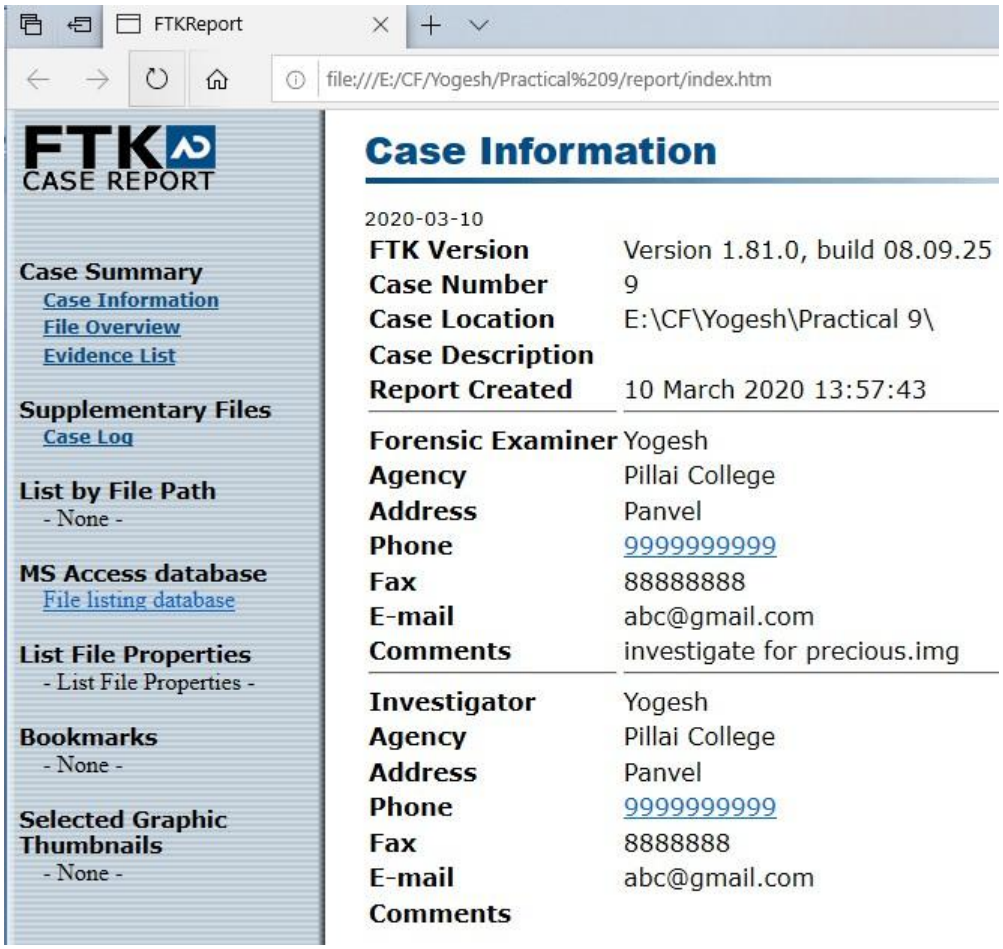


Step 2: Fill the details and click next until you reach Report Location Window.


FTK Report Wizard - Case Information
Case Information
The following information will appear on the Case Information page of the report:
Include Investigator Information in report
Agency/Company:
Pillai College
Investigator's Name:
Yogesh
Address:
Panvel
Phone:
9999999999
Fax:
8888888
E-Mail:
abc@gmail.com
Comments:



Step 3: Click yes and the reports will be displayed in browser.



FTK CASE REPORT

Case Summary
- Case Information
- File Overview
- Evidence List

Supplementary Files
- Case Log

List by File Path
- None -

MS Access database
- File listing database

List File Properties
- List File Properties -

Bookmarks
- None -

Selected Graphic Thumbnails
- None -

File Overview

2020-03-10

Evidence Items
Evidence Items: 2

File Items
Total File Items: 3,790
Flagged Thumbnails: 0
Other Thumbnails: 1,255

File Status
KFF Alert Files: 0
Bookmarked Items: 0
Bad Extension: 157
Encrypted Files: 19
From E-mail: 295
Deleted Files: 50
From Recycle Bin: 6
Duplicate Items: 373
OLE Subitems: 57
Flagged Ignore: 0
KFF Ignorable: 0
Data Carved Files: 0

File Category
Documents: 312
Spreadsheets: 10
Databases: 0
Graphics: 1,255
Multimedia: 45
E-mail Messages: 82
Executables: 7
Archives: 55
Folders: 669

FTK CASE REPORT

Case Summary
- Case Information
- File Overview
- Evidence List

Supplementary Files
- Case Log

List by File Path
- None -

MS Access database
- File listing database

List File Properties
- List File Properties -

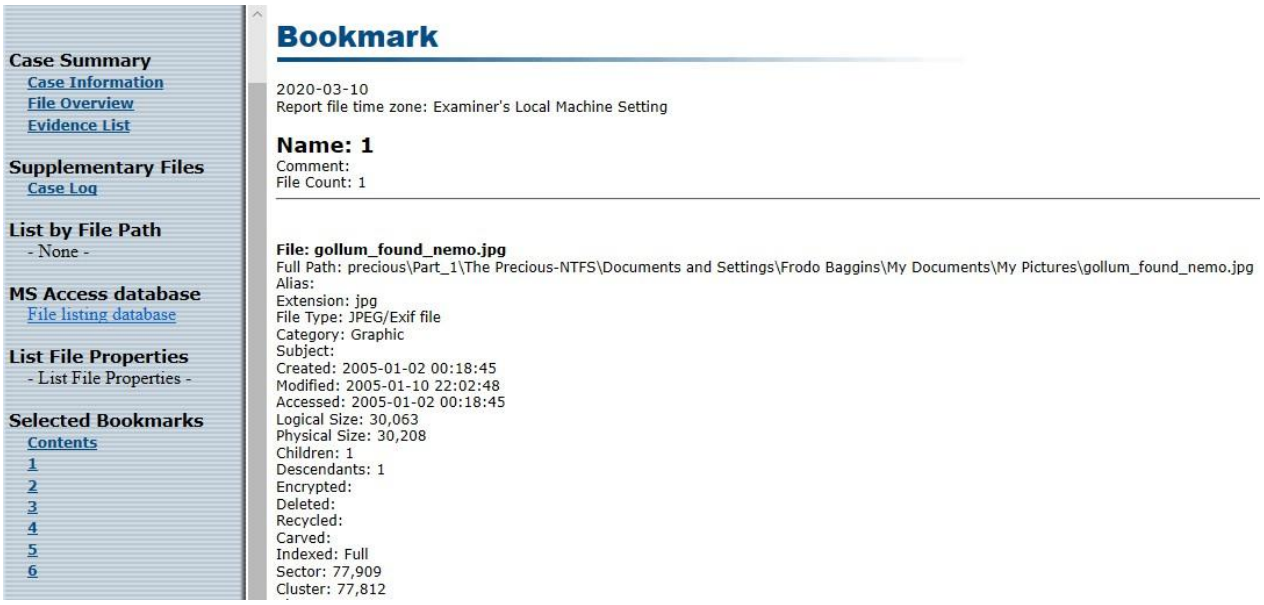
Evidence List

2020-03-10

Display Name: precious\Part_1\The Precious-NTFS
Evidence File Name: precious.img
Evidence Path: E:\CF
Identification Name/Number: 9
Evidence Type: NTFS
Added: 2020-03-10 13:50:52
Children: 2,782
Descendants: 3,788

Display Name: precious\UnpartSpace
Evidence File Name: precious.img
Evidence Path: E:\CF
Identification Name/Number: 9
Evidence Type: Unpartitioned Space
Added: 2020-03-10 13:53:30
Children: 2
Descendants: 2

AccessData Forensic Toolkit®



Conclusion: Hence, we successfully generate forensics report using AccessDataFTK.