CYBER FORENSICS

A PRACTICAL REPORT

ON

CYBER FORENSICS

SUBMITTED BY
Mr. **SAYED FARHAN SHAHID ALI**
Roll No: **IT21015**

UNDER THE GUIDANCE OF
PROF. **AKSHAY NIMKAR**

Submitted in fulfillment of the requirements for qualifying
MSc. IT Part II Semester - IV Examination 2022-2023

University of Mumbai
Department of Information Technology

R.D. & S.H National College of Arts, Commerce & S.W.A.
Science College Bandra (West), Mumbai – 400 050

R. D. & S. H. National & S. W. A. Science College

Bandra (W), Mumbai – 400050.

Department of Information Technology
M.Sc. (IT – SEMESTER IV)

Certificate

This is to certify that ***Cyber Forensics Practicals*** *performed at R.D & S.H National & S.W.A. Science College by Mr.* ***Farhan Sayed*** *holding Seat No. _____ studying Master of Science in Information Technology Semester – IV has been satisfactorily completed as prescribed by the University of Mumbai, during the year 2022 – 2023.*

Subject In-Charge **Coordinator In-Charge** **External Examiner**

College Stamp

INDEX

Practical No 1

Aim: - File system Analysis using The Sleuth kit

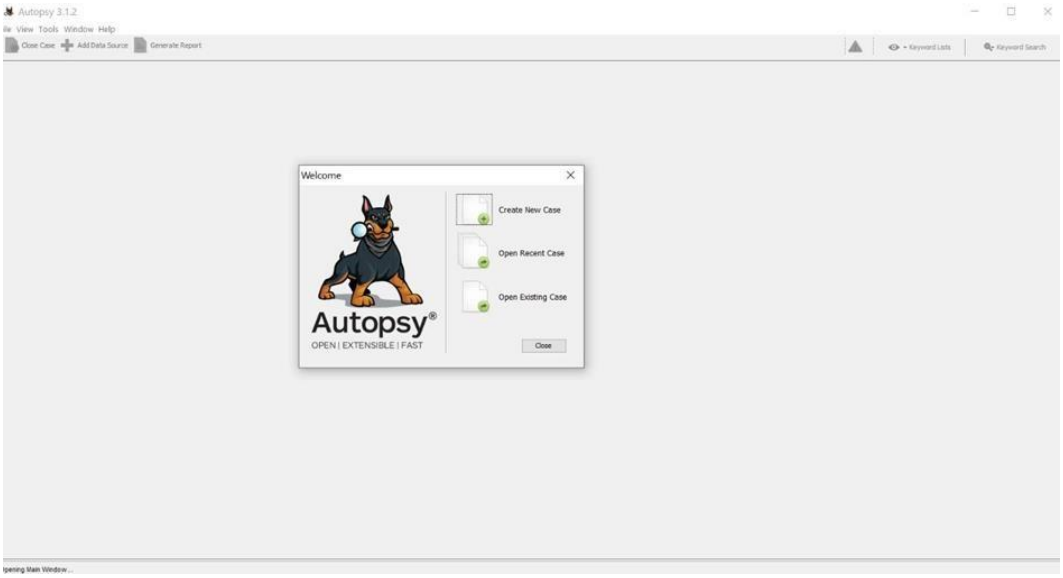
Practical No 1

Aim: - File system Analysis using The Sleuth kit

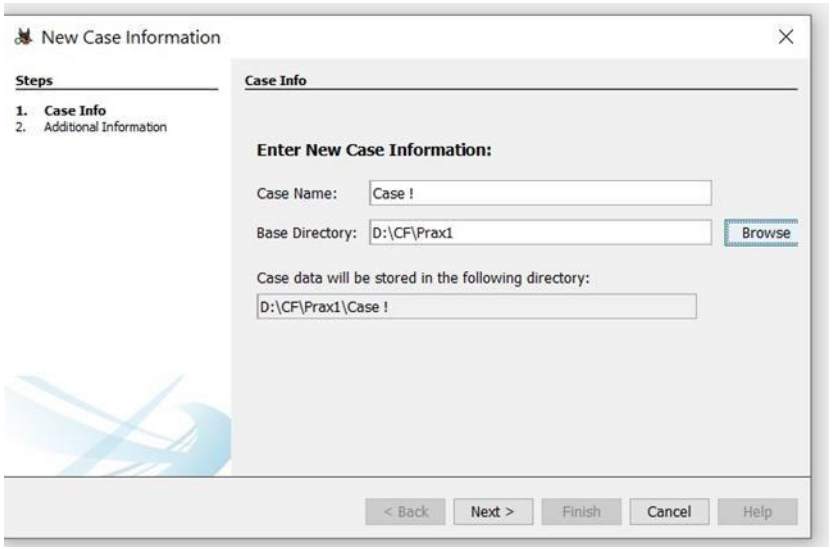
Exploring Autopsy

How to Start a Case

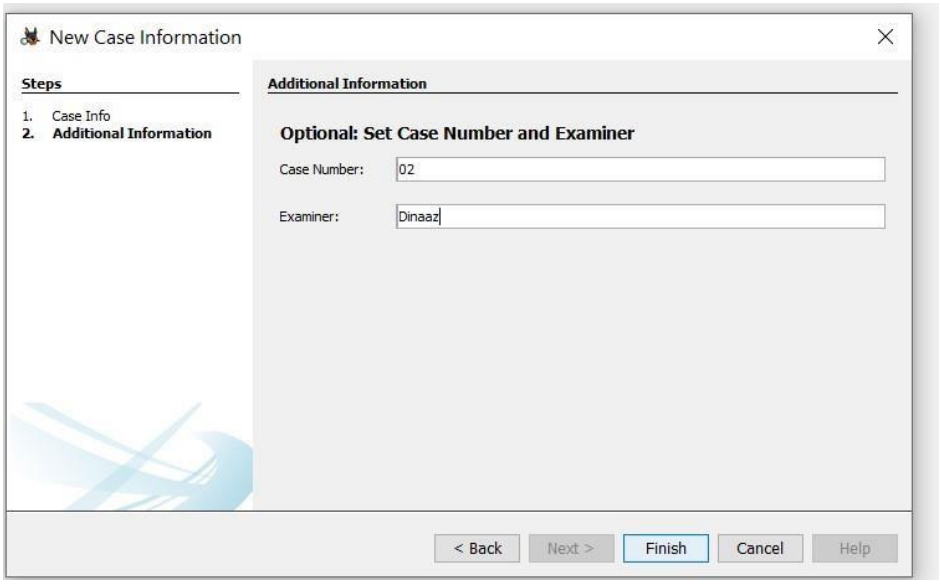
Upon starting Autopsy 3.1.2, a window will open with three selections to make: create a new case, open existing case, or to open a recent case.

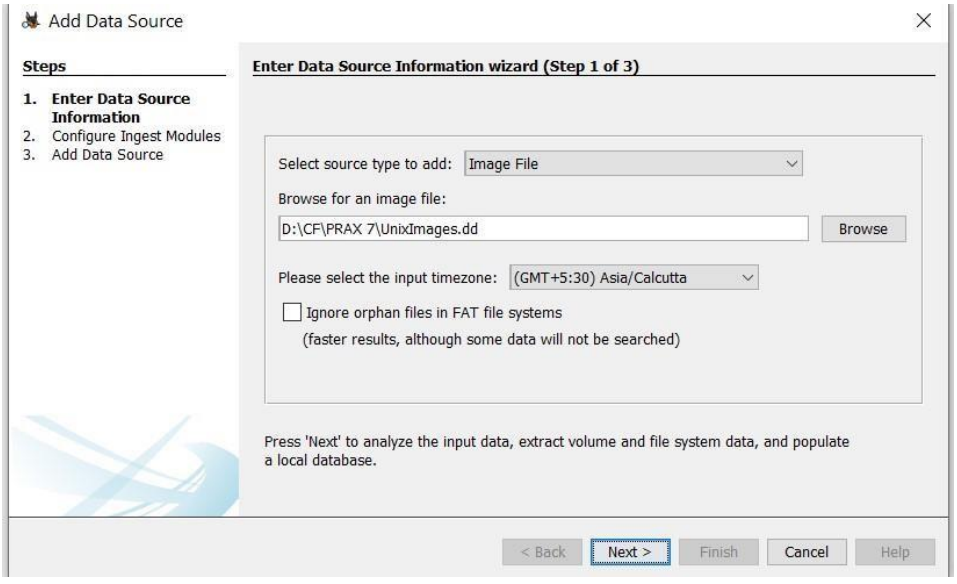


Step 1) Select the "Create New Case" option and be directed to a new window that will have information to fill in, we will be naming the case "Test."

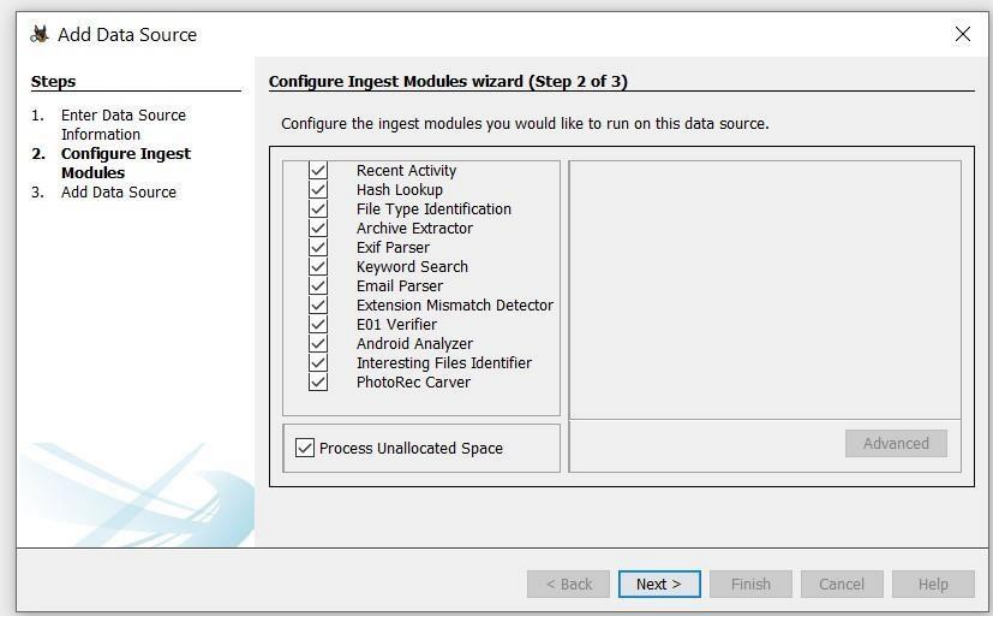


Step 2) After the information has been filled in select the next button. The next window will allow the investigator to fill in the case number and examiner name. This is for the purpose of creating better documentation and logging. After the information is filled in select the finish button to continue.

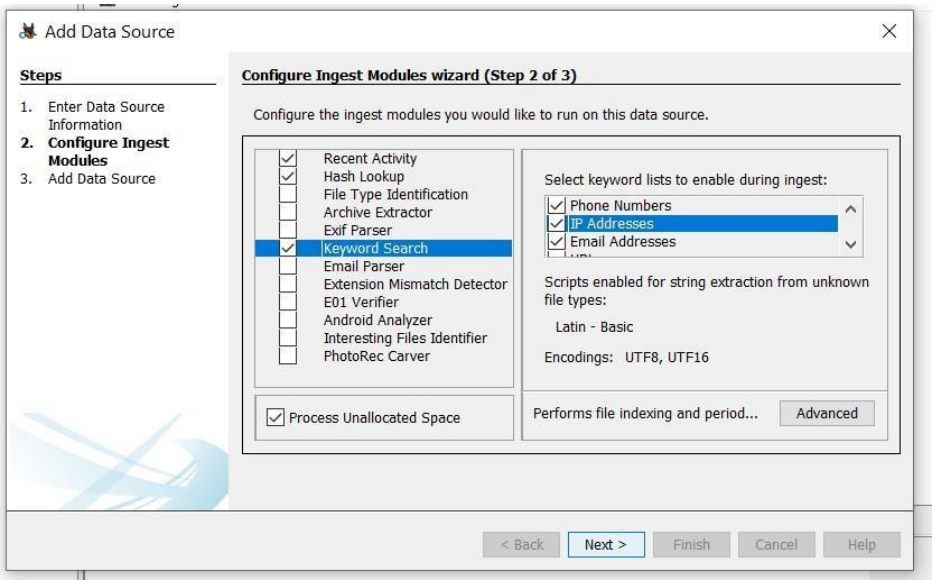




Step 3) The next step in the investigation will be to add an image file to the case. The image file can be chosen from a wide variety of formats including: img, dd, 001, aa, and e01. Use the browse button to find the image that is desired to work with and select add. Options to choose the timezone of 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.

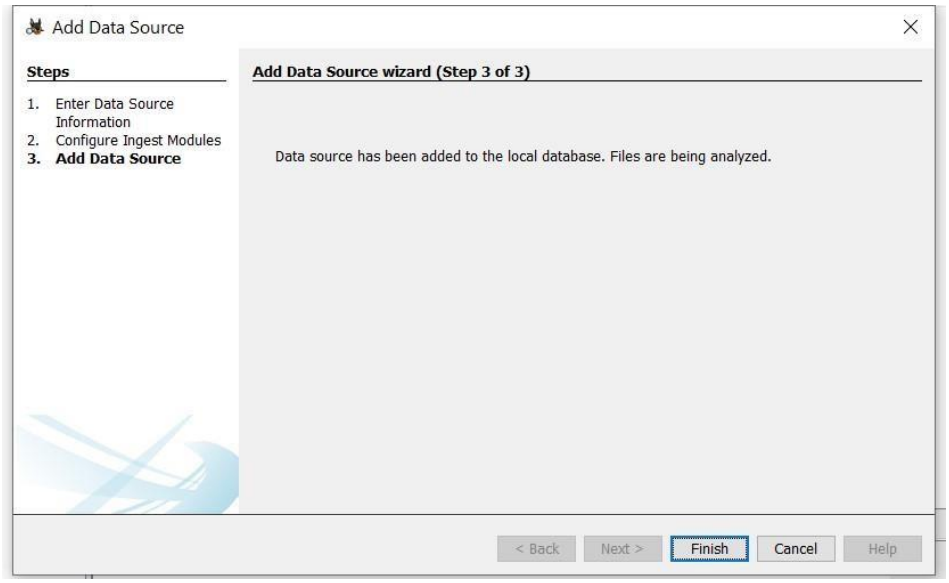


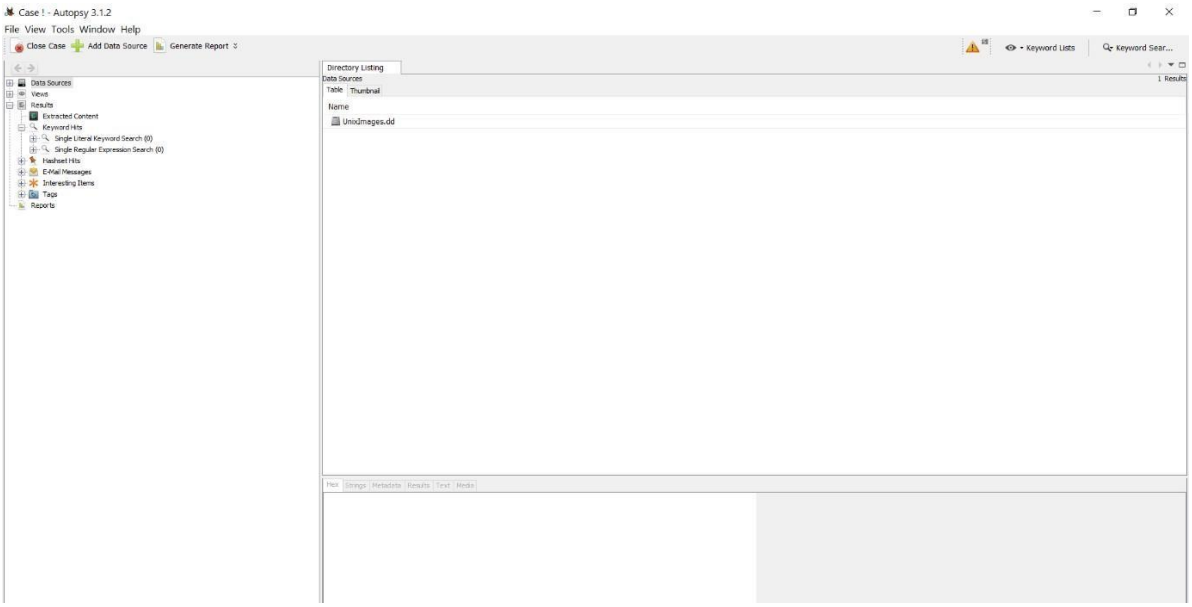
Step 5) The following window will bring the investigator to the Ingest wizard panel, which is one of the new features offered in Autopsy. There are three options in the first box: Recent Activity, Hash lookup, and Keyword Searches.

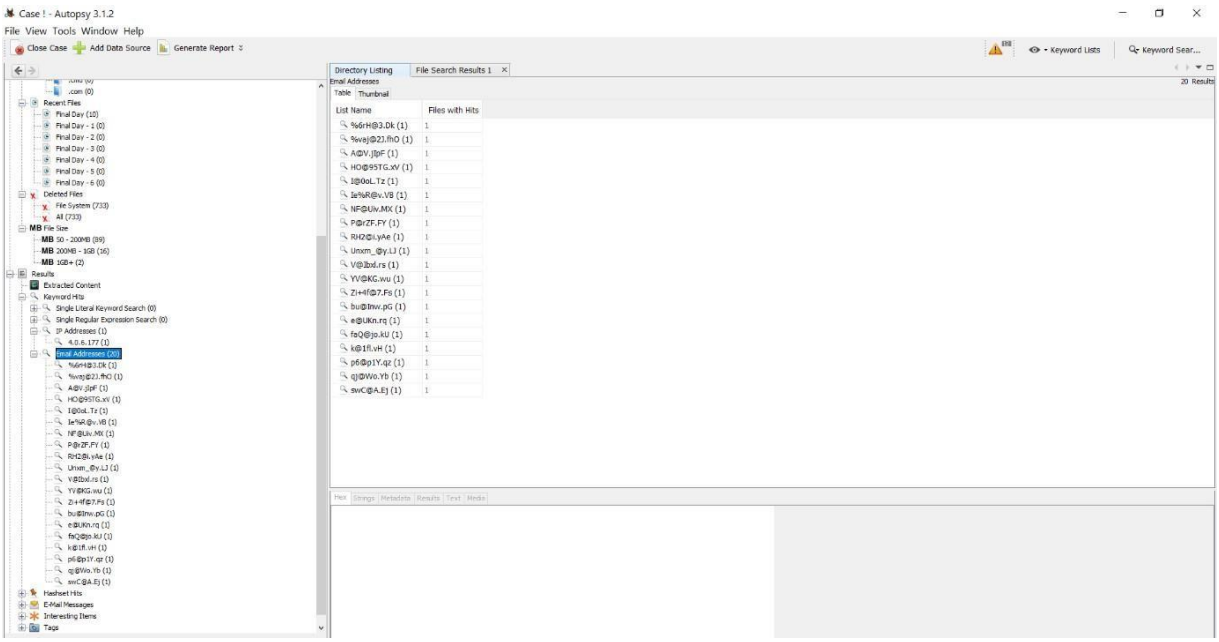


By selecting any of the options Global settings can be set to increase the capabilities of the search. Under the Hash Lookup option there is the advanced option to add databases of known hashes. Under the Keyword Search option are many different lists that can be used to search for information. By default, Phone Numbers, IP Addresses, Email Addresses, and URL's are available. Select the Advanced button and a Keyword List Configuration window will open. In this new window select New List and type the name that is desired for the list. This makes it

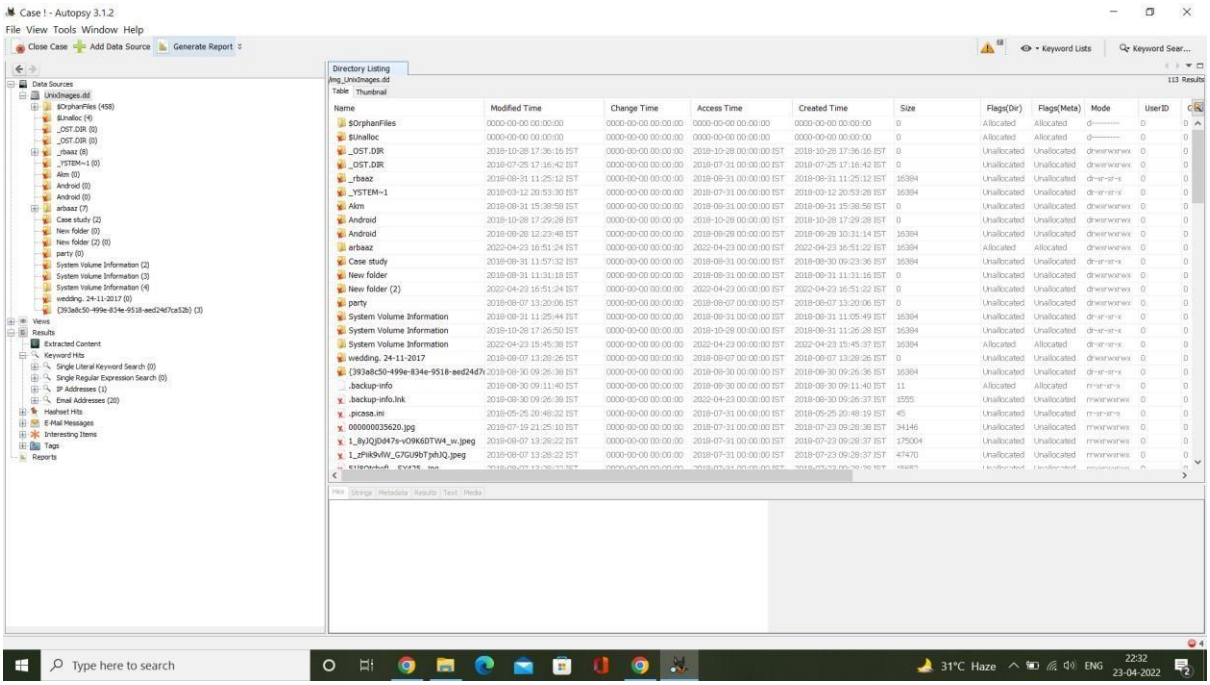
easier to search by subject matter or other organizational methods. For now the list Test keywords will be used to create a list. In the adjacent pane there is a blank section with a word bar and an Add button next to it. Type the keyword desired (case sensitive) and select Add to add the word to the list. There is also the option to select Regular Expression. This allows the investigator to further narrow the field to search in by selecting what the keyword is that is being searched for including: passwords, emails, text file name, domains, and many more options.



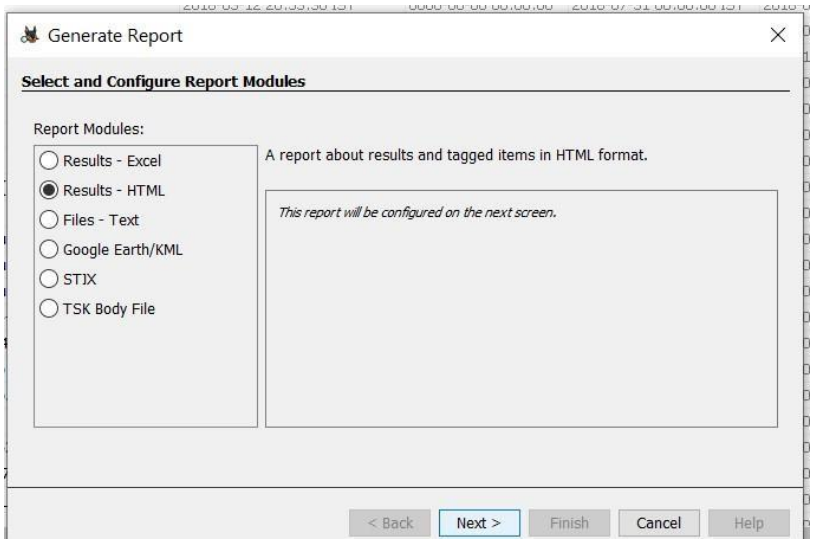


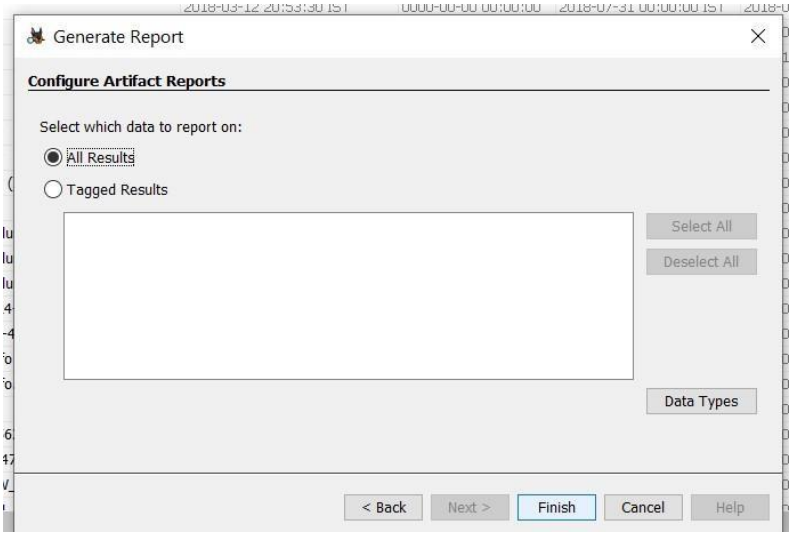


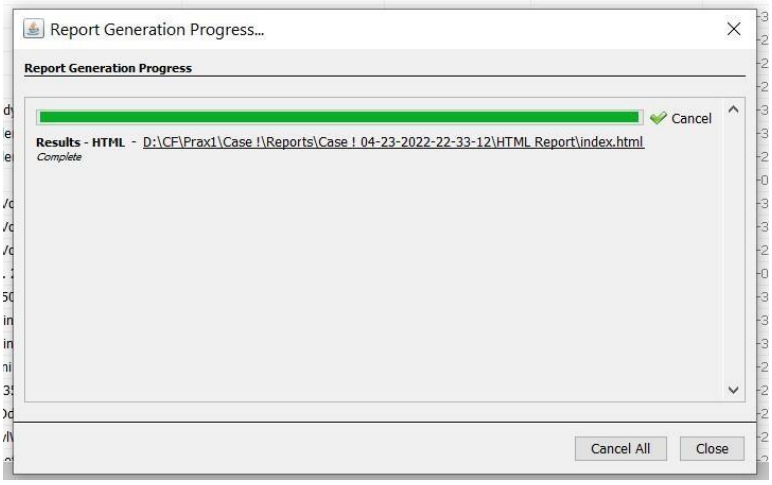
Step 6) After finishing the keyword parameters the screen will be laid out for the user.

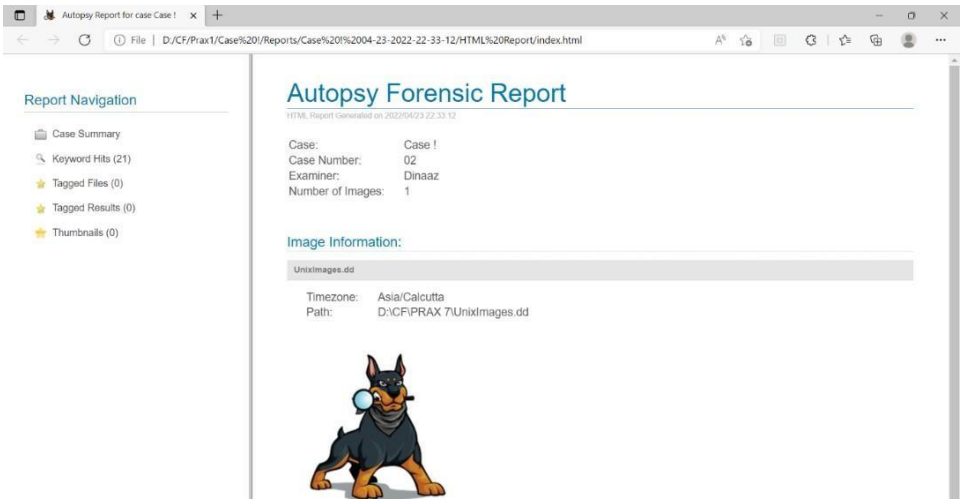


Step 7) After the image is indexed the tree will be populated by the file system, extracted content, keyword searches, and the hash list (if any were used). the investigator should generate a report. This will allow the investigator to have an idea of what type of information is available and what to expect. The report can be generated in three formats: Excel, XML, and HTML. It also has the ability to select what information to display with choices that can be seen in the image below.

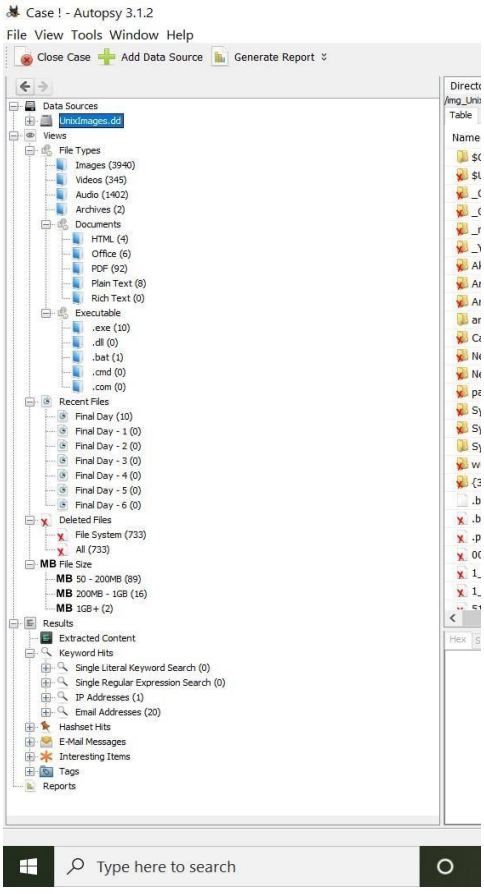

Generate Report
Select and Configure Report Modules
Report Modules:
Results - Excel
Results - HTML
Files - Text
Google Earth/KML
STIX
TSK Body File
A report about results and tagged items in HTML format.
This report will be configured on the next screen.
< Back
Next >
Finish
Cancel
Help


Generate Report
Configure Artifact Reports
Select which data to report on:
All Results
Tagged Results
Select All
Deselect All
Data Types
< Back
Next >
Finish
Cancel
Help

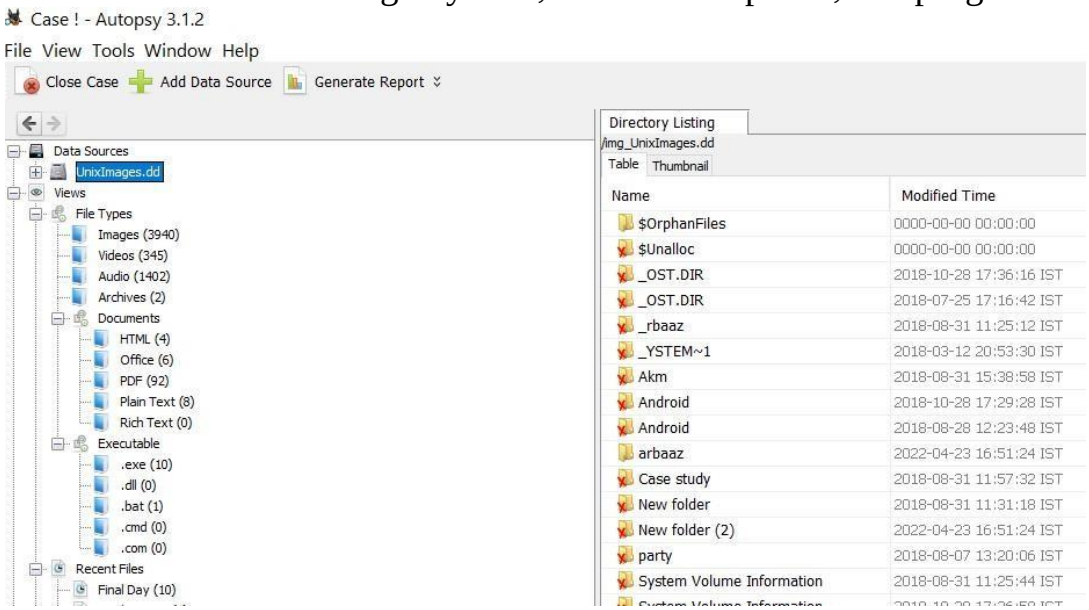

Report Generation Progress...
Report Generation Progress
Cancel
Results - HTML - D:\CF\Prax1\Case !\Reports\Case ! 04-23-2022-22-33-12\HTML Report\index.html
Complete
Cancel All
Close



Looking at the tree, the top selection is titled “Data Sources” this is where the acquired image is located and the bulk of the investigation, will take place. If the Images tab is expanded the investigator will see each image that was added to the investigation. By expanding an images tab the volumes of the image will be seen including the file system and unallocated space. Expanding the tab that contains the Operating System will give the investigator a look at the root directory and the tree that contains most of the relevant information. This is the same as if the investigator would open the default drive when browsing through a system.

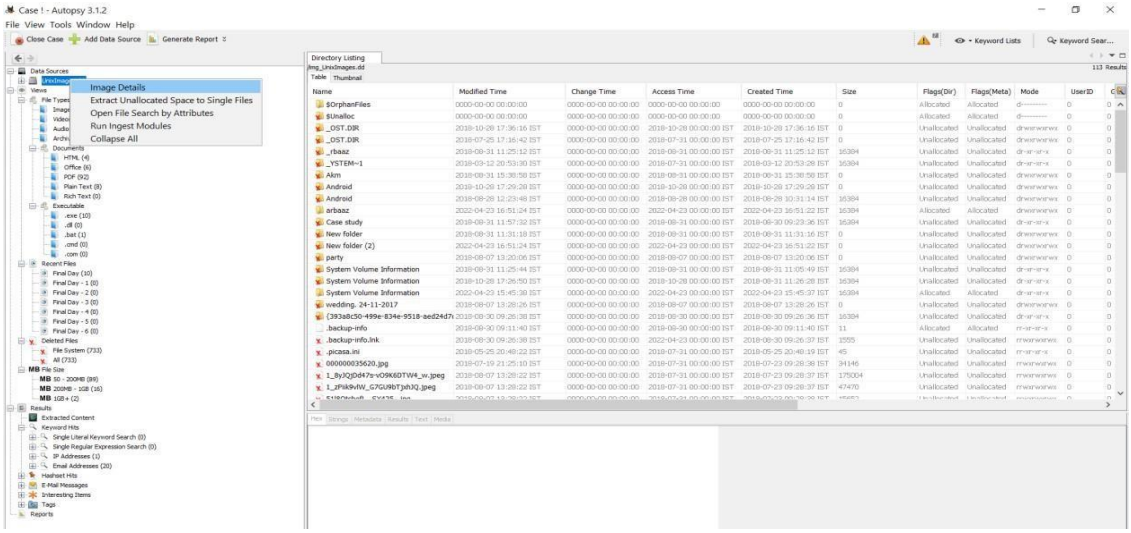


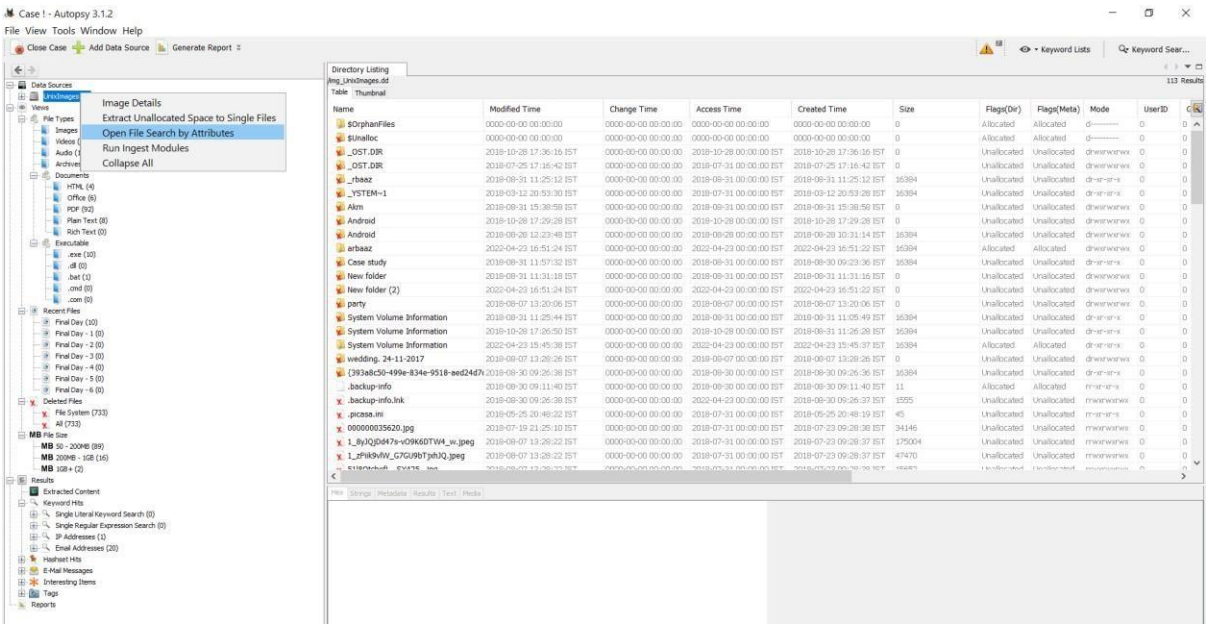
Below the Images tab is the "Views" tab that will allow the investigator to separate the information in the image into different categories such as by file types and by recent documents. The file type can be broken down into: images, video, audio, and documents which includes the major text formats. Another section in the Views tab is a new feature in Autopsy 3, the Recent Files tab. This tab allows the investigator to get a rough outline of what happened in the last 6 days of use by the suspect. The results include registry files, documents opened, and programs run.



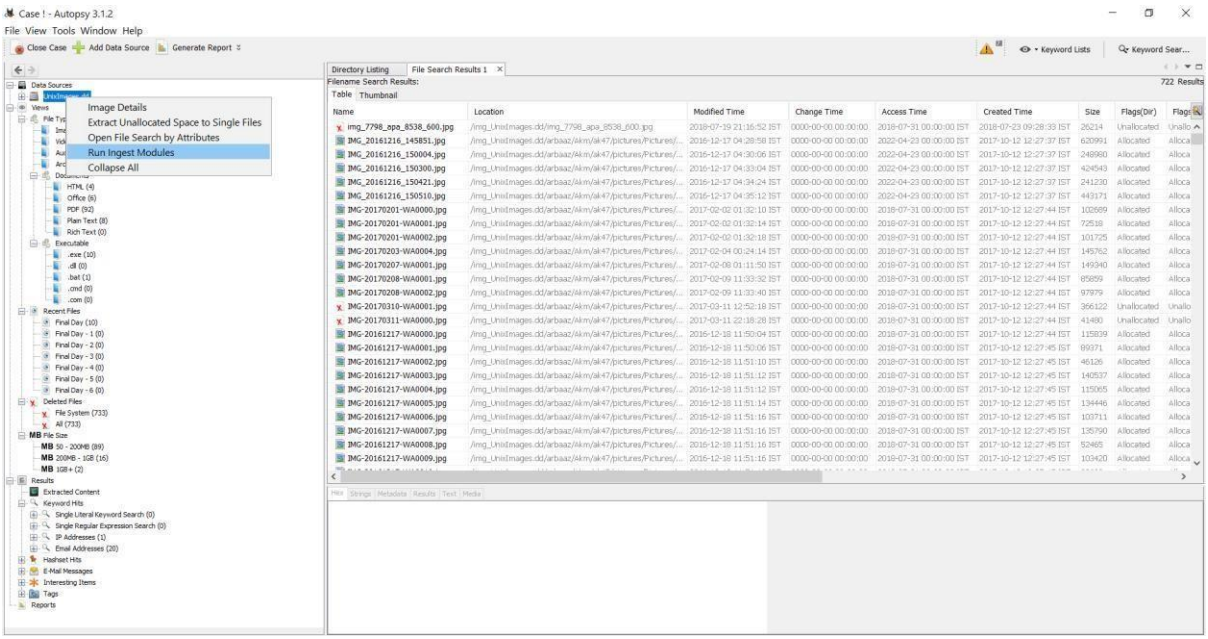
hand to run matches against. If the investigators had a hash library of known child pornography or pirated material they could run all the information on the computer against the library and all The next tab that is seen is the Results tab, this is a new feature that displays all the information from the ingest process. This uses the program BEViewer to look for certain information inside of the data and separate it into sections that make it easier to search for specific data instead of going through all of the information manually. Although this simplifies the investigation process, it does not mean that this is all of the information that is able to be gained through an investigation. There are 4 main categories when separating the Results tab: Extracted Content, Keyword Hits, Hashset Hits, and E-mail Messages. Each of these sections has subsections that allow for more specific information divisions. In the Extracted Content tab there are sections for: Bookmarks, Cookies, Web History, Downloads, Recent Documents, Installed Programs, and Device Attached. The bookmarks tab contains information on bookmarks created in the internet browsers so the investigator can see a list of sites that the suspect frequented enough to create a bookmark for. The cookies tab will allow investigators to see a general idea of where the suspect has been recently by looking through the cookies and seeing which sites have cookies stored on the computer. The Web history tab searches for .dat files and lists them to show another list of internet usage through web browsers. The download tab allows for the search for any downloads on the

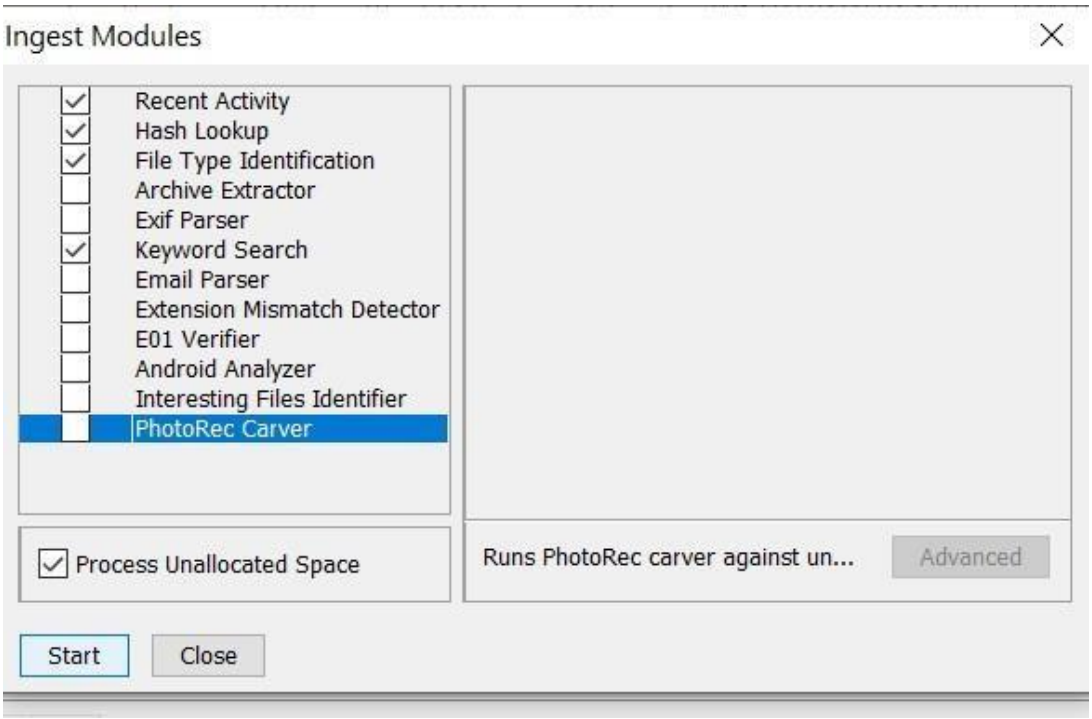
suspect computer. Recent documents will show documents that were opened on the machine recently by looking at their metadata and deciding how long ago a document was opened. The installed programs tab will give the investigator a list of programs that are currently installed on the machine. The tab for attached devices is obtained by looking through the registry files and determining which hardware devices have been plugged into the system at one point or another. Under the keyword hits tab the investigator will see all the options that were selected in the ingest index window when starting the case. The information includes: phone numbers, URLs, email addresses, search words by the user, IP addresses, and regular expression searches. The tab for hashset hits only has results if a list library was added to the case before

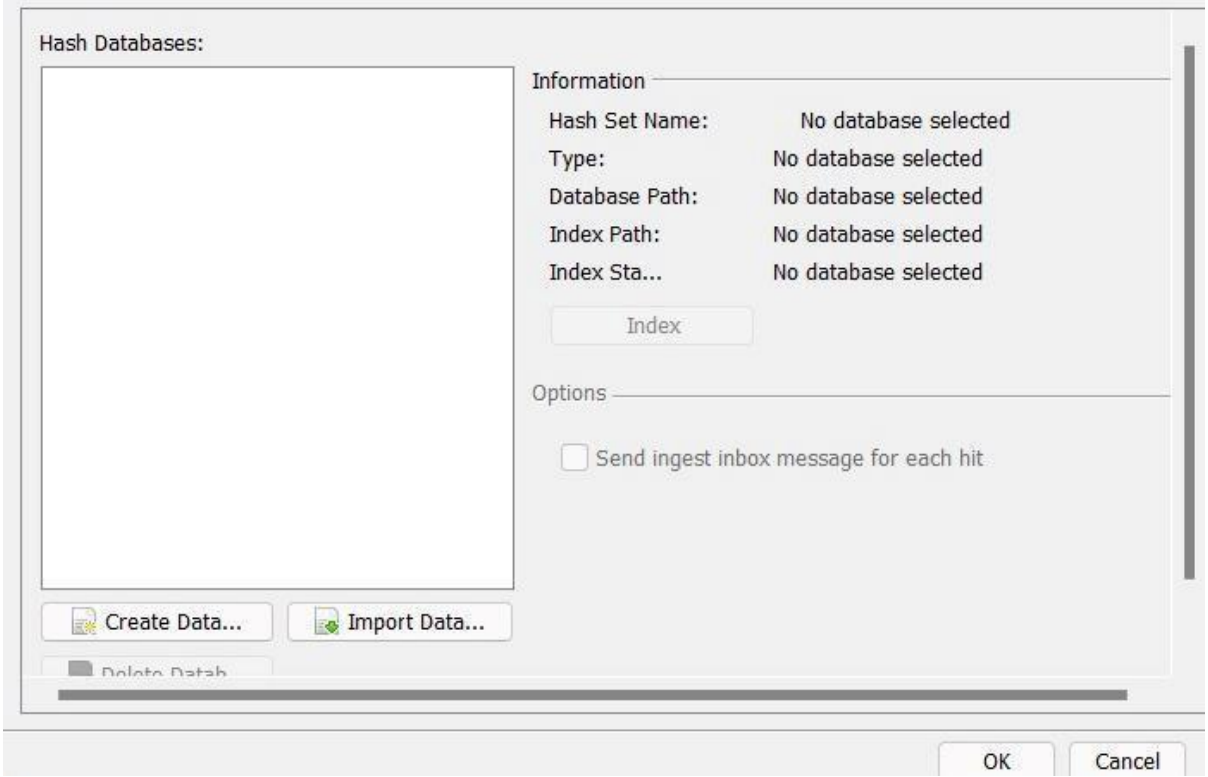


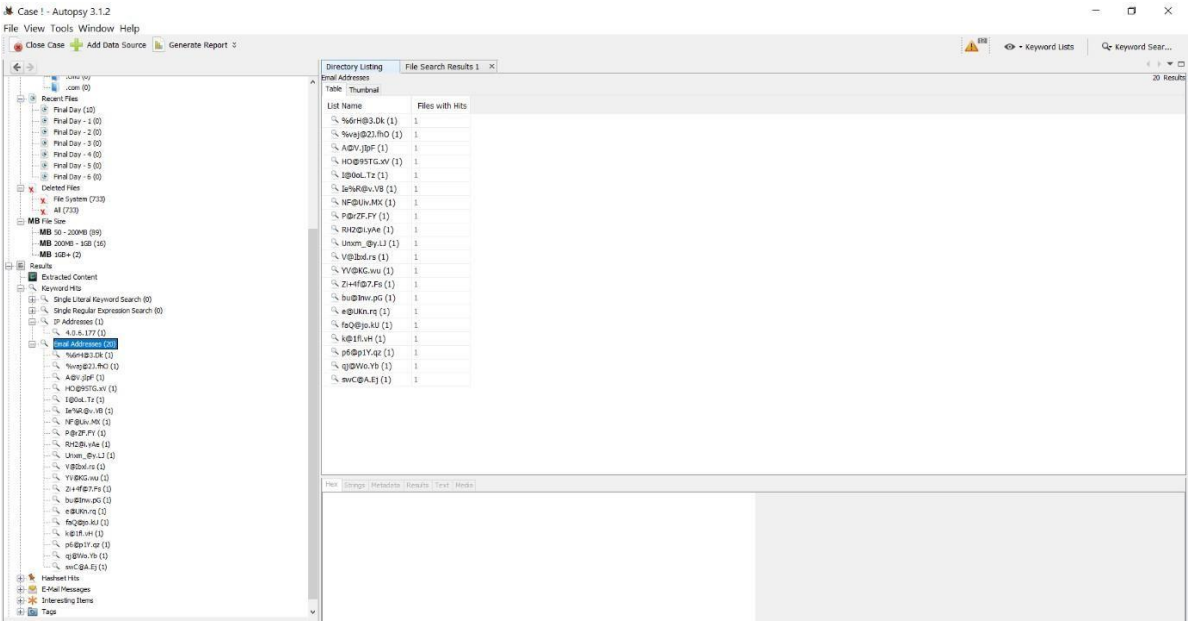

Case 1 - Autopsy 3.1.2
File View Tools Window Help
Close Case
Add Data Source
Generate Report
Keyword Lists
Keyword Sear...
Image Details
Extract Unallocated Space to Single Files
Open File Search by Attributes
Run Ingest Modules
Collapse All
Directory Listing
Table
Thumbnail
113 Results

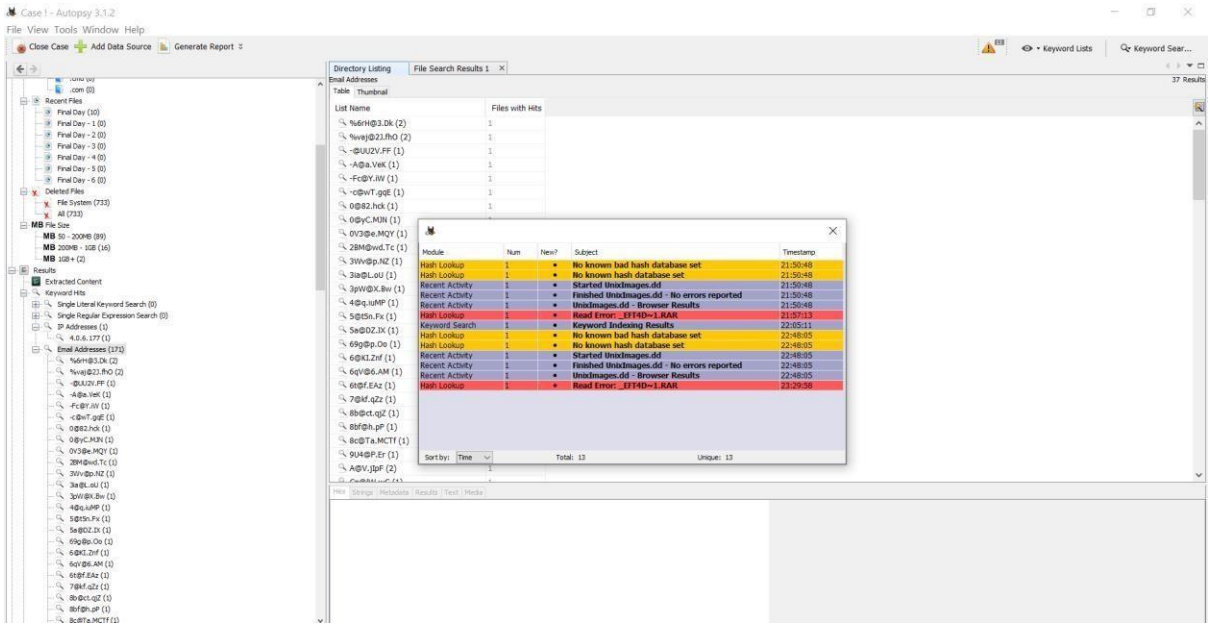

File Search by Attributes
Search for files that match the following criteria:
Name: img
*Note: Name match is case insensitive and matches any part of the file name. Regular expressions are not currently supported.
Size: equal to 0 Byte(s)
Date: to
Timezone: (GMT+5:30) Asia/Calcutta
Modified
Accessed
Changed
Created
*Empty fields mean "No Limit"
*The date format is mm/dd/yyyy
Known Status:
Unknown
Known (NSRL or other)
Known bad
Search


Case ! - Autopsy 3.1.2
File View Tools Window Help
Close Case
Add Data Source
Generate Report
Keyword Lists
Keyword Sear...
Image Details
Extract Unallocated Space to Single Files
Open File Search by Attributes
Run Ingest Modules
Collapse All
Directory Listing
File Search Results 1
Filename Search Results:
722 Results
Table
Thumbnail
Name
Location
Modified Time
Change Time
Access Time
Created Time
Size
Flags(Dir)


Ingest Modules
Recent Activity
Hash Lookup
File Type Identification
Archive Extractor
Exif Parser
Keyword Search
Email Parser
Extension Mismatch Detector
E01 Verifier
Android Analyzer
Interesting Files Identifier
PhotoRec Carver
Process Unallocated Space
Runs PhotoRec carver against un...
Advanced
Start
Close


Hash Databases:
Information
Hash Set Name: No database selected
Type: No database selected
Database Path: No database selected
Index Path: No database selected
Index Sta... No database selected
Index
Options
Send ingest inbox message for each hit
Create Data...
Import Data...
OK
Cancel


Case ! - Autopsy 3.1.2
File View Tools Window Help
Close Case
Add Data Source
Generate Report
Directory Listing
File Search Results 1
Email Addresses
Table
Thumbnail
List Name
Files with Hits


Case 1 - Autopsy 3.1.2
File View Tools Window Help
Close Case
Add Data Source
Generate Report
Keyword Lists
Keyword Sear...
Directory Listing
File Search Results 1
Email Addresses
37 Results
Table
Thumbnail
List Name
Files with Hits
Module
Num
New?
Subject
Timestamp
Hash Lookup
No known bad hash database set
Recent Activity
Started UnixImages.dd
Finished UnixImages.dd - No errors reported
UnixImages.dd - Browser Results
Keyword Search
Keyword Indexing Results
Sort by:
Time
Total: 13
Unique: 13

Practical No 2

Aim: - Exploring Access data FTK for the following:

Using Accessdata FTK

Practical No 2

Aim: - Exploring Access data FTK for the following:

Using Accessdata FTK

➡ Data Carving
- Searching for Embedded and Deleted Files (Data Carving)
- Data Carving Files in an Existing Case
- Adding Carved Files to the Case
- Bookmarking Carved Files

➡ Using Filters
- Applying an Existing Filter
- Using The File Filter Manager
- Modifying or Creating a Filter
- Deleting a Filter

➡ Searching the Registry
- Starting Registry Viewer
- Launching Registry Viewer as a Separate Application
- Launching Registry Viewer from FTK
- Understanding the Registry Viewer Windows
- The Full Registry Window
- The Common Areas Window
- The Report Window
- Opening Registry Files
- Opening a Registry File in Registry Viewer
- Opening Registry Files within FTK
- Obtaining Protected Registry Files Using FTK Imager
- Working with Registry Evidence
- Adding Keys to the Common Areas Window
- Deleting Keys from the Common Areas Window
- Adding Keys to the Report Window
- Deleting Keys from the Report Window
- Creating Registry Summary Reports
- Using Pre-defined AccessData Templates
- Creating Your Own Registry Report Templates
- Changing RSR Settings in the FtkSettings.0.ini File
- Searching for Specific Data
- Generating a Report

• Exporting a Word List

Data Carving

Searching for Embedded and Deleted Files (Data Carving)

Because embedded items and deleted files contain information that may be helpful in forensic investigations, Forensic Toolkit (FTK) simplifies the process of recovering these items and adding them to the case. The data carving feature allows you to search for items, such as graphics embedded in other files. It also allows you to recover previously deleted files located in unallocated space. To recover embedded or deleted files, FTK searches the index for specific file headers. When it finds a file header for a recognized file type, FTK carves the file's associated data. FTK can find any embedded or deleted item as long as the file header still exists.

Data carving can be done either during **evidence processing (when a new case is added)** or it can be done in **an existing case.**

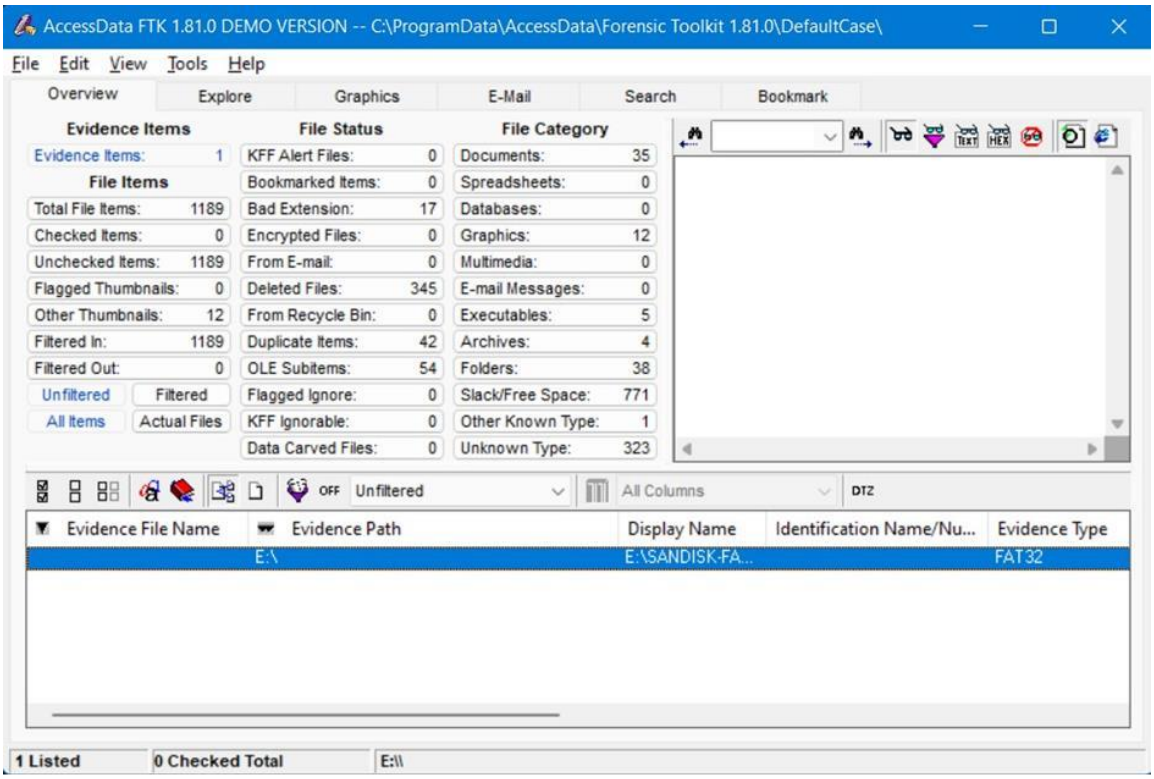
Data Carving Files During Evidence Processing in a New Case:

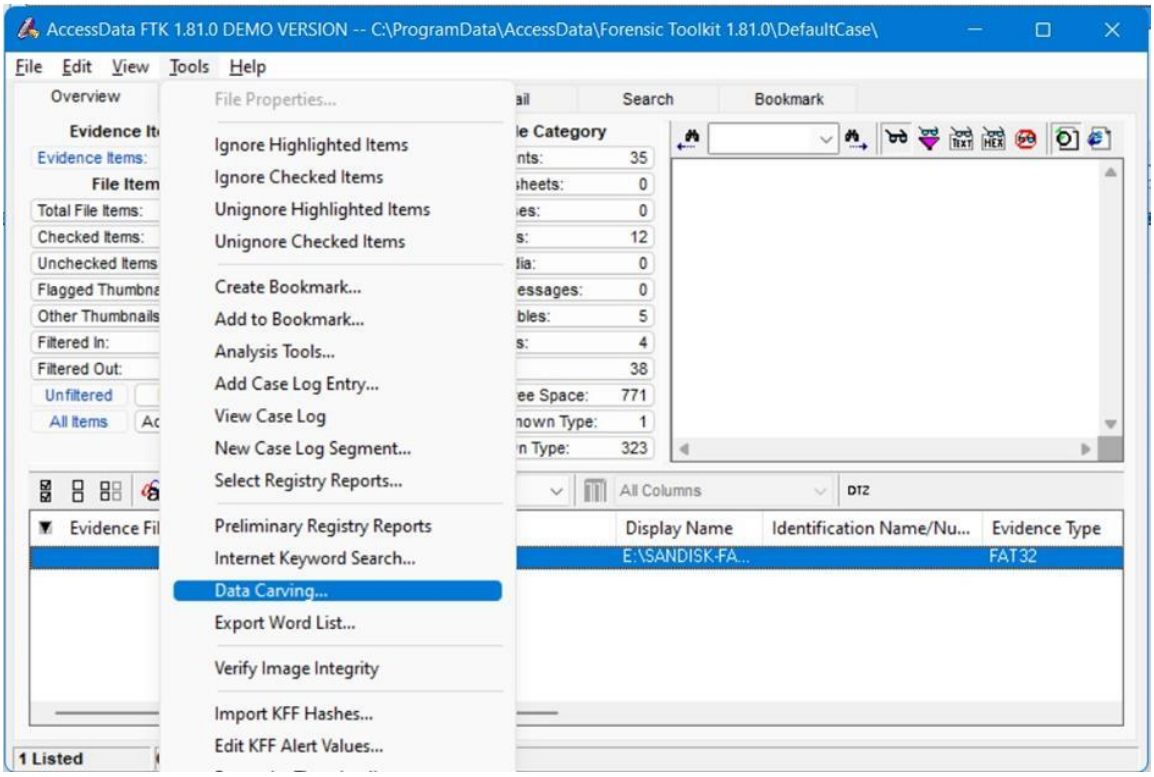
You can select to data carve when a case is added by selecting Data Carve in the Process to Perform Screen during the New Case Wizard. FTK carves data immediately after preprocessing.

When you select to data carve when creating a new case, FTK creates a cache for the carved data. If data is located, the cache is saved.

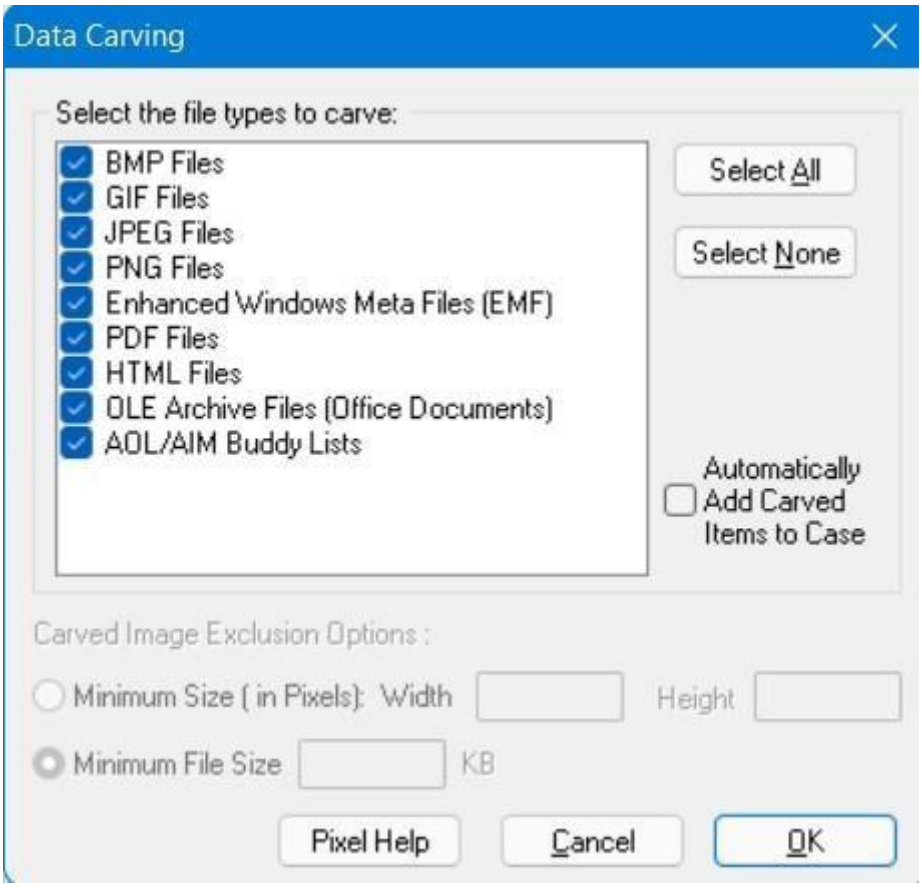
To access the cache:

Step 1) Select **Tools**, and then **Data Carving**.

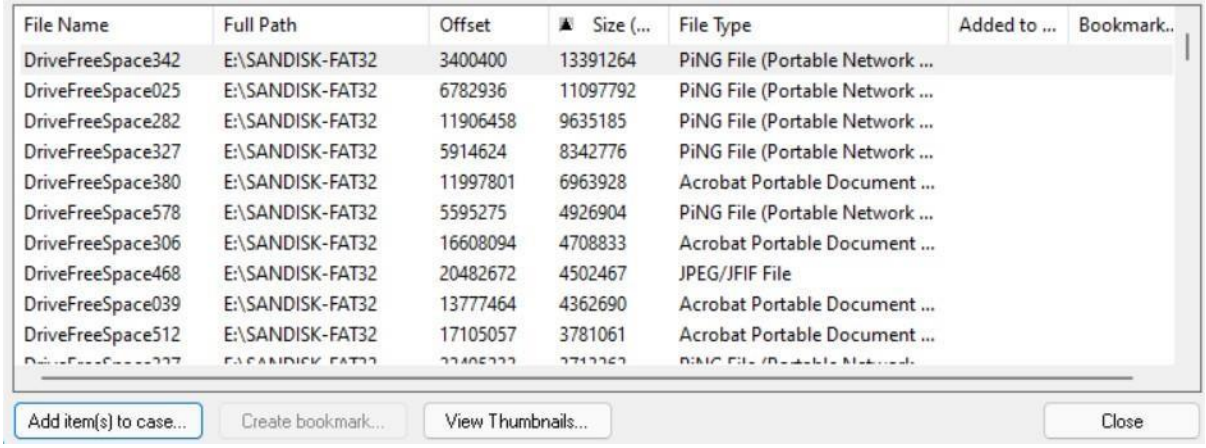


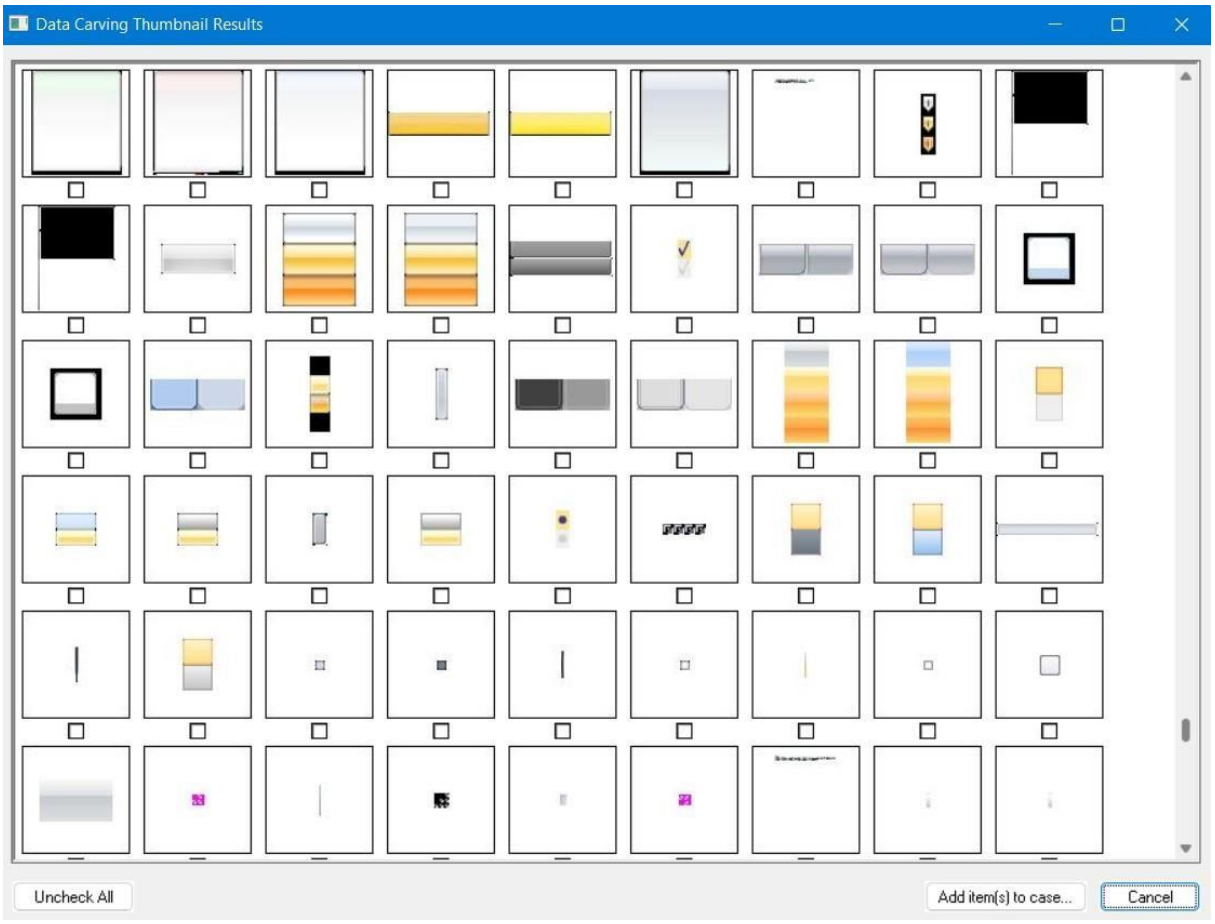


Step 2) Check the file types to carve. You can click **Select All** or **Select None** to speed up the selection process. Click **OK**.



When the process is complete, the detached viewer appears with the data carving results. A message appears if no data was located.



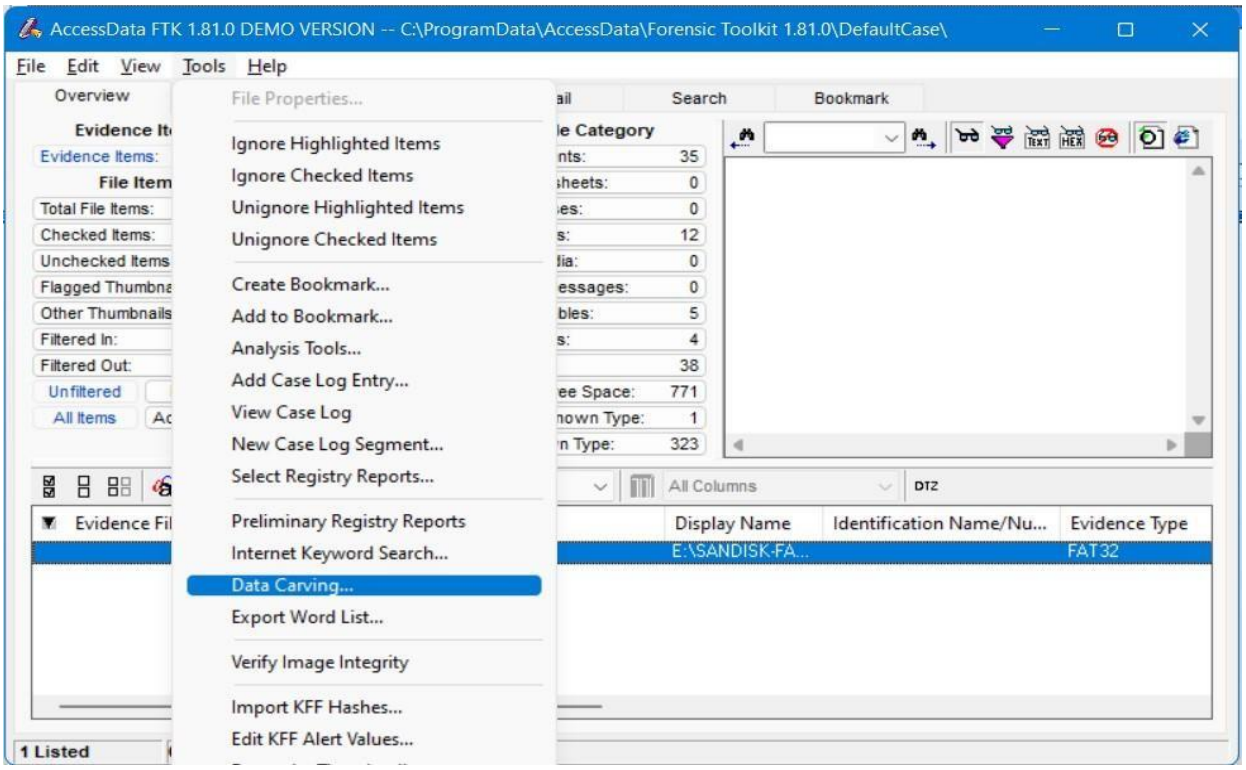


Or

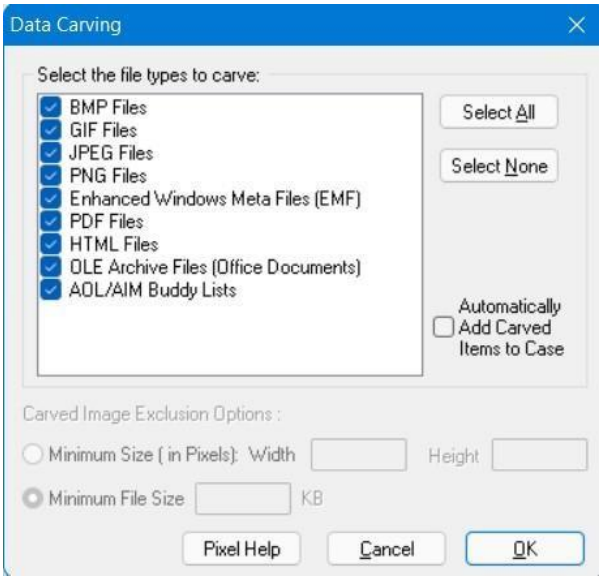
Data Carving Files in an Existing Case:

To search for embedded and deleted files:

[1] Select **Tools**, and then **Data Carving**.

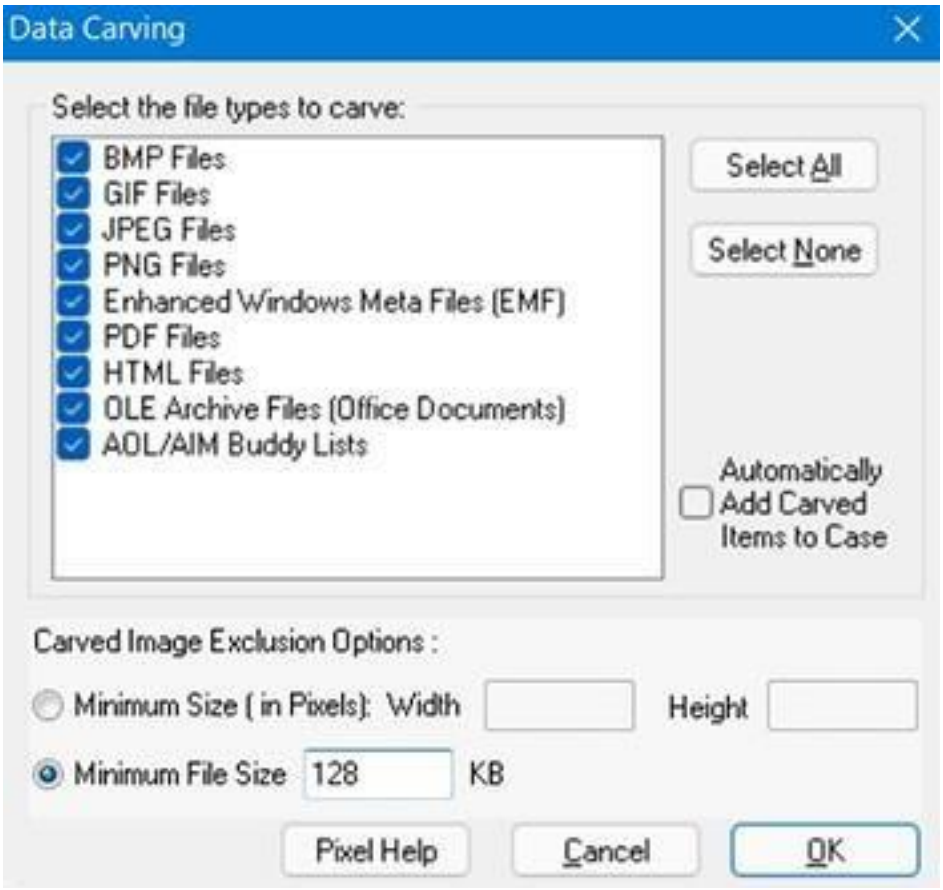


[2] Check the file types to carve. You can click **Select All** or **Select None** to speed up the selection process.

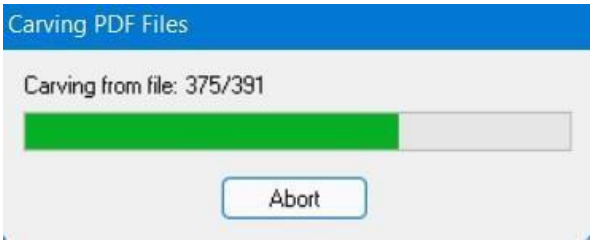


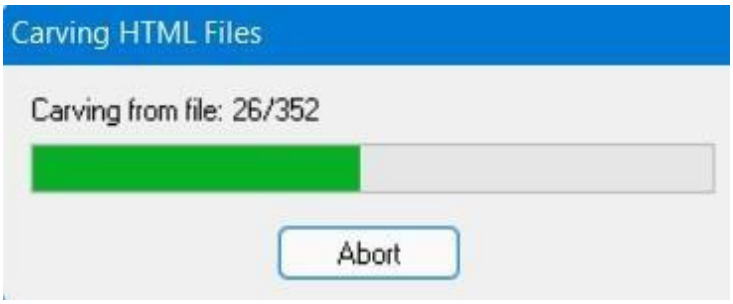
[3] (Optional) Check the **Automatically Add Carved Items to Case** option. The the Minimum Image Size fields activate. 3a Specify a minimum size in pixels in which to disply images. The program will question you about minimum sizes over 480 pixels.

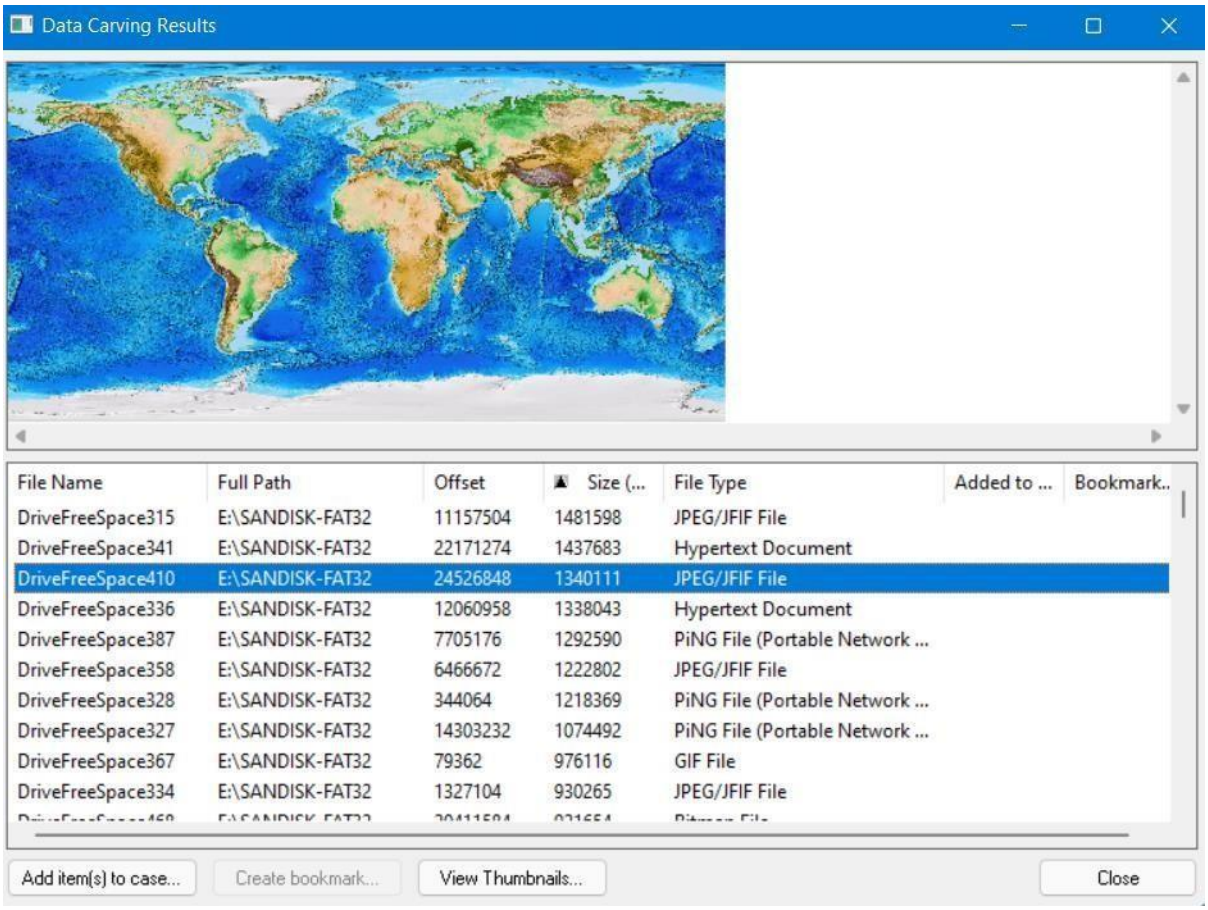
[4] Click **OK**.


Data Carving
Select the file types to carve:
BMP Files
GIF Files
JPEG Files
PNG Files
Enhanced Windows Meta Files (EMF)
PDF Files
HTML Files
OLE Archive Files (Office Documents)
AOL/AIM Buddy Lists
Select All
Select None
Automatically Add Carved Items to Case
Carved Image Exclusion Options :
Minimum Size (in Pixels): Width
Height
Minimum File Size
128
KB
Pixel Help
Cancel
OK


Carving BMP Files
Carving from file: 724/740
Abort


Carving PDF Files
Carving from file: 375/391
Abort


Carving HTML Files
Carving from file: 26/352
Abort

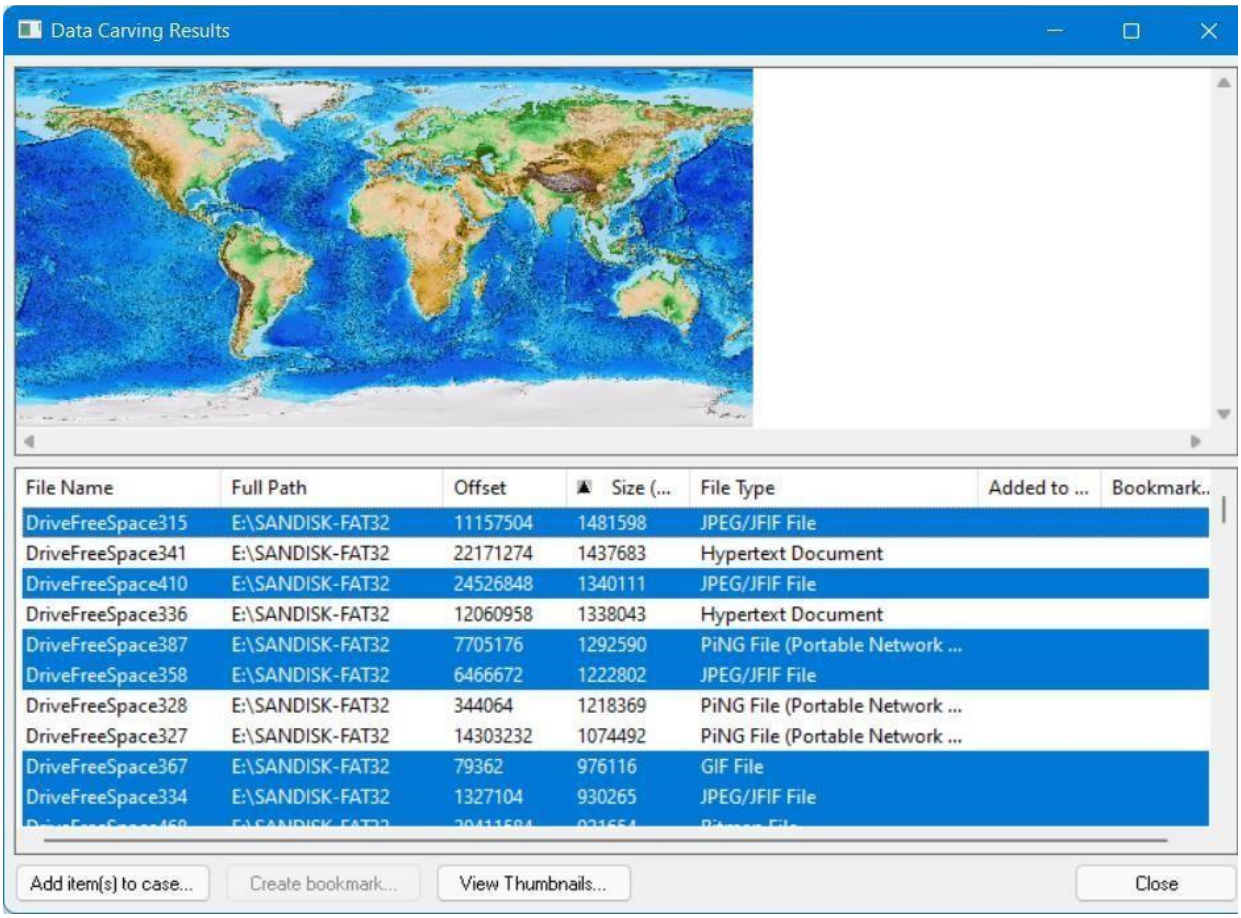


Adding Carved Files to the Case:

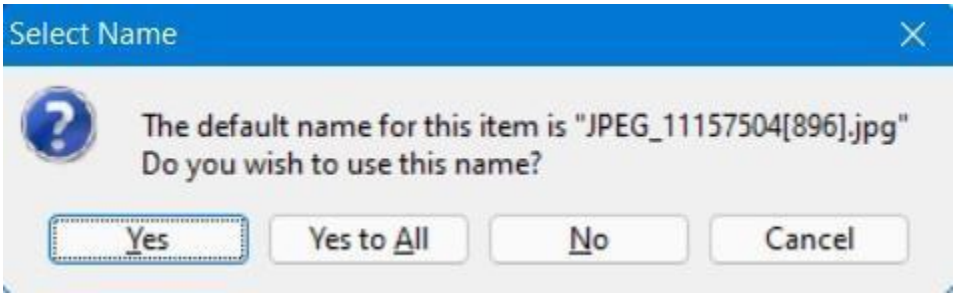
To add a carved file to the case:

1) Select the files you want to add to the case.
   You can Shift+click to select multiple contiguous files. or Ctrl+click to select multiple discontiguous files.

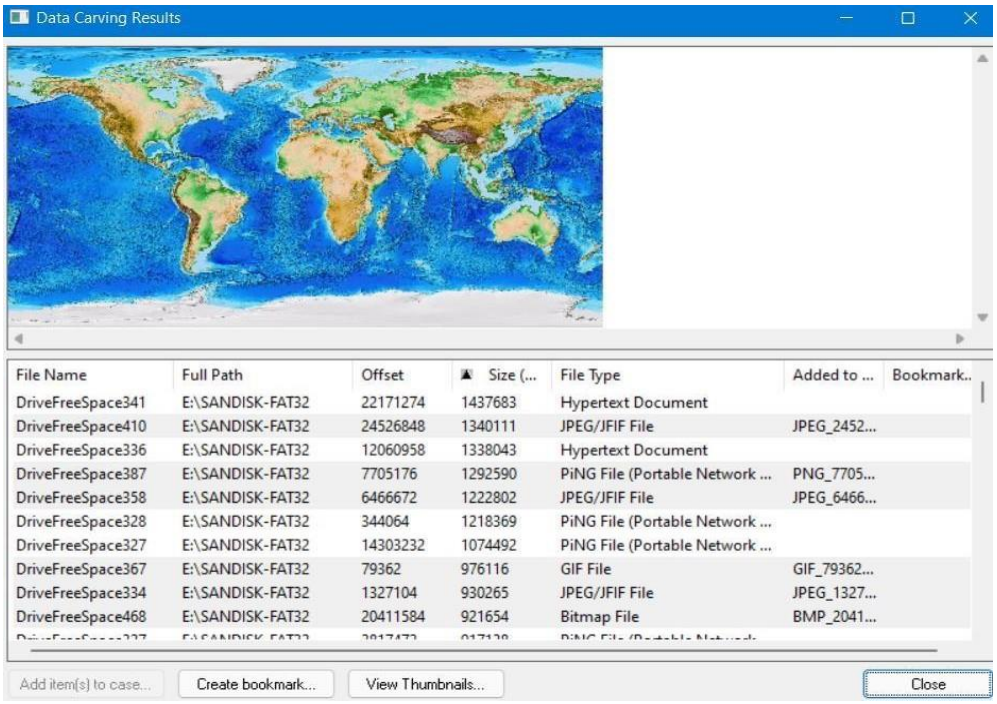
2) Click **Add Items to Case**.



1) Click **Yes** to accept the default name. or Click **No**, enter a different name, and click **OK**.



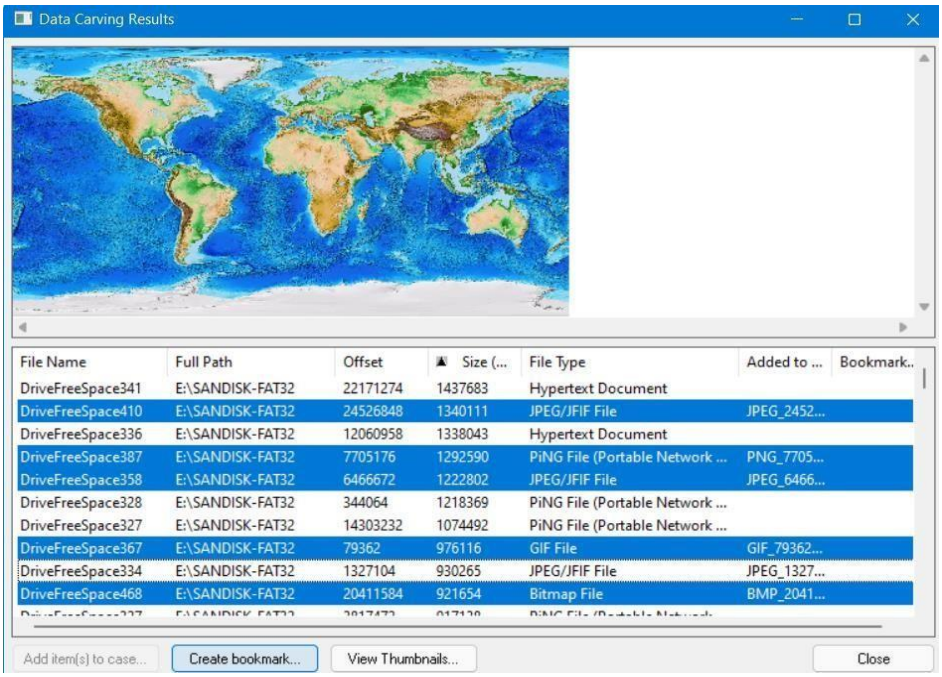
After a file is added to a case, FTK will not find it in subsequent data carving procedures. In other words, there is no redundancy. If a file is identified as case evidence, the data carving feature ignores it. The data carving feature only looks for files that are not individually identified in the body of evidence.



Bookmarking Carved Files:

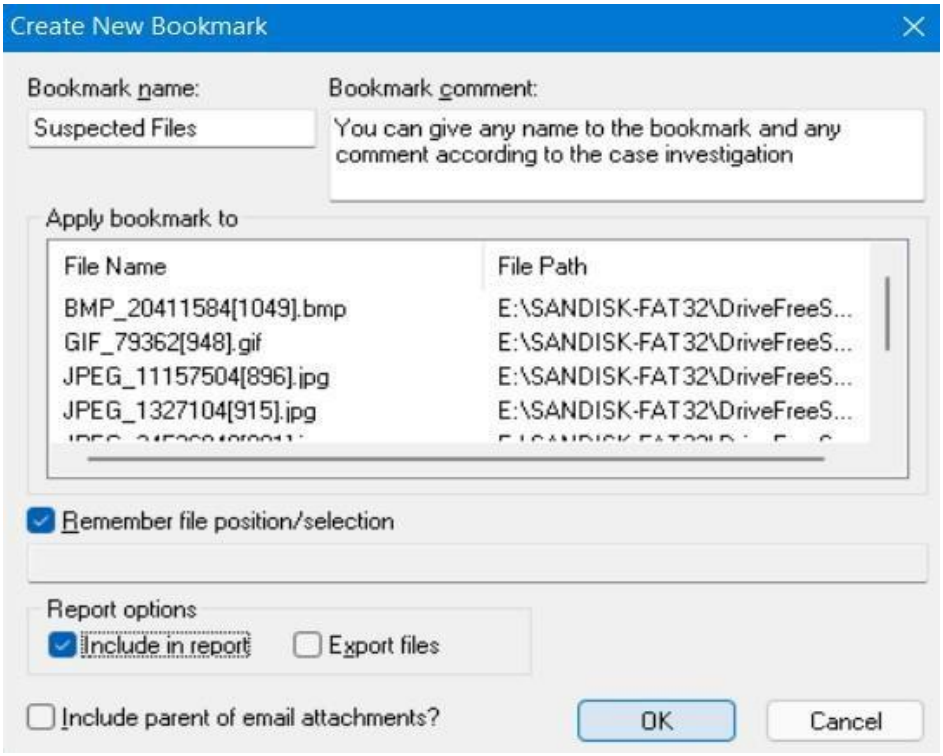
To bookmark a carved file:

Step 1.Select the files you want to include in the bookmark and click **Create Bookmark**.

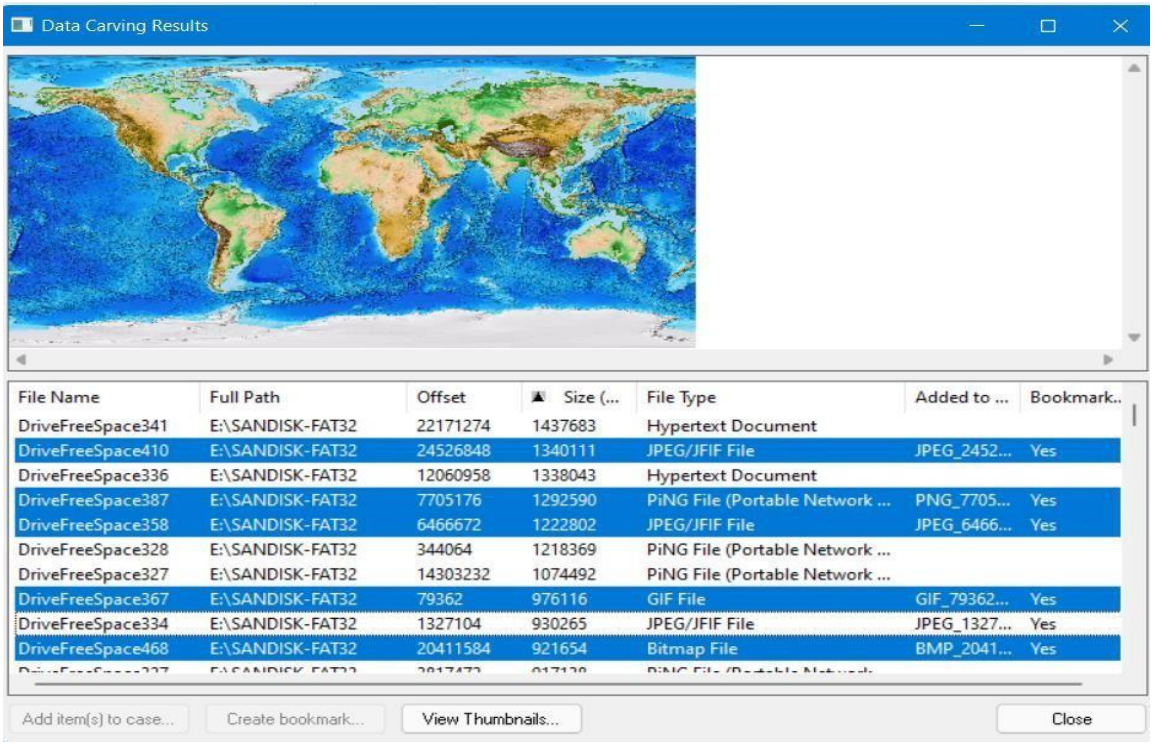


Step 2.In the Create New Bookmark form

Step 3. Enter the following & Click **OK**.



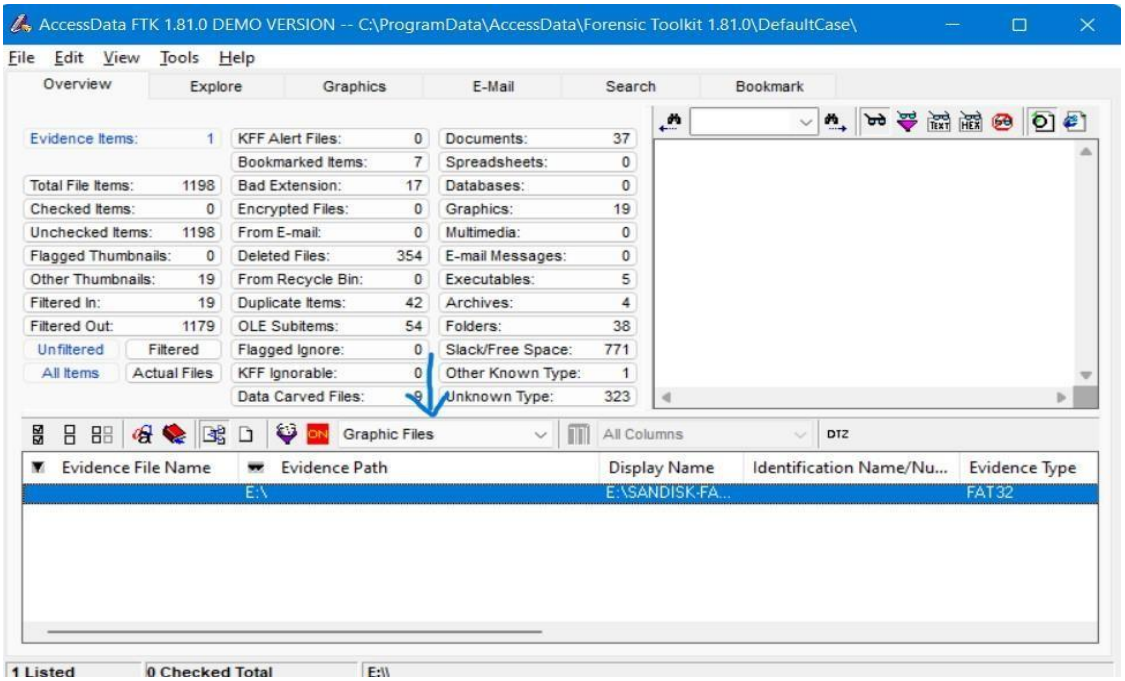
When the process is complete, the detached viewer appears with the bookmarked data carving results

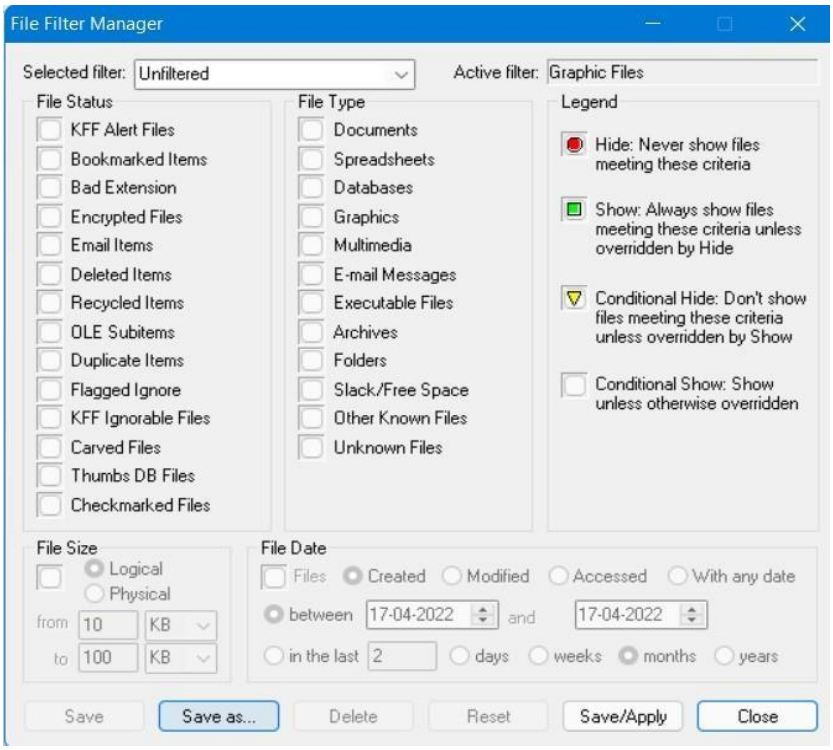


Using Filters

Applying an Existing Filter

To apply an existing filter, use the Filter drop-down list on the File List toolbar, shown below:



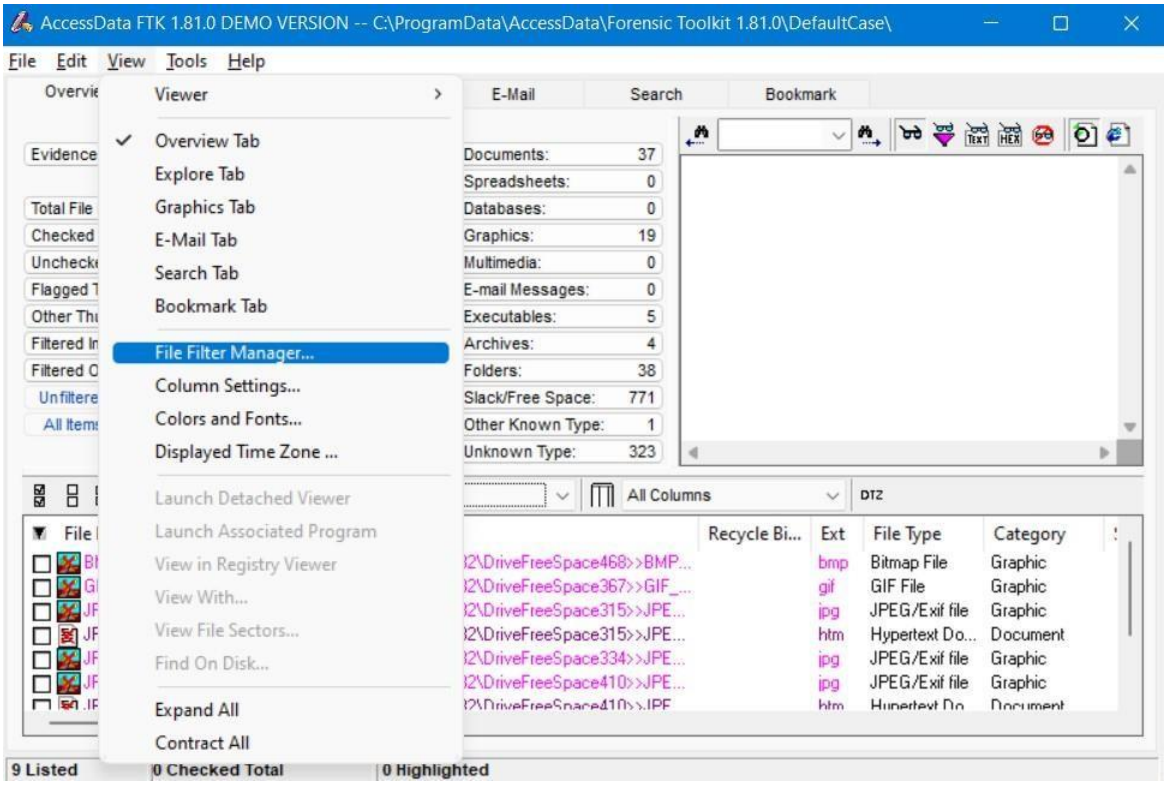


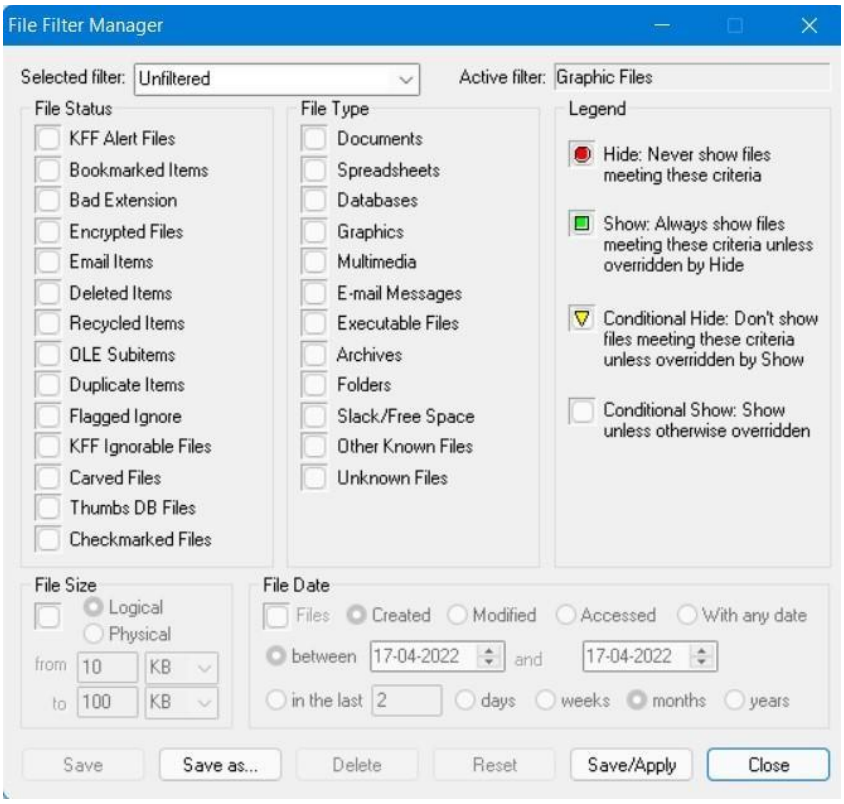
Filter	Description
E-mailed Items	Shows e-mail items such as e-mail messages, archive files, and attachments.
Encrypted Files	Shows encrypted files that are possibly in all file types.
Graphic Files	Only shows graphic files.
KFF Alert Files	Shows KFF alert files that are possibly in all file types.
No Deleted	Hides deleted items.
No Duplicates	Hides duplicate items.
No Ignorable	Hides duplicate items, KFF ignorable files, and files that were flagged ignorable.
No OLE	Hides items or pieces of information that were embedded in a file, such as text, graphics, or an entire file.
Unfiltered	Displays all items in the case.

Using the File Filter Manager:

The File Filter Manager allows you to create or modify file filters.

To access this menu, select **View**, and then **File Filter Manager**





The following sections review the categories in the File Filter Manager menu:

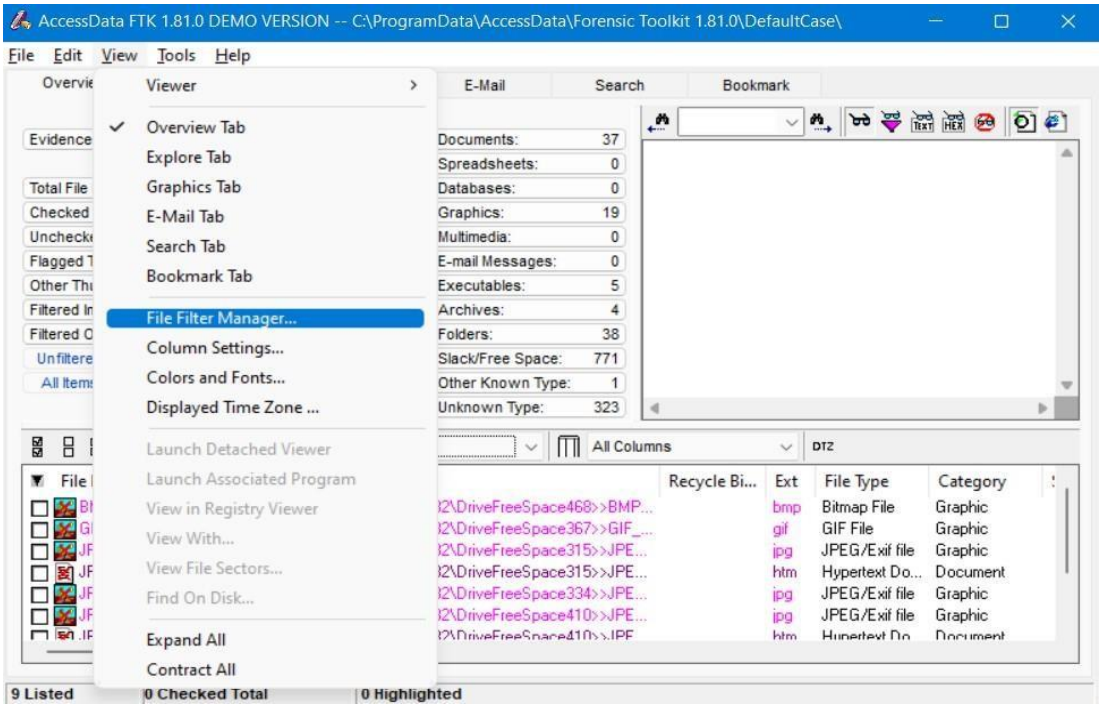
Icon	Description
	Hide: Never shows files meeting selected criteria. If you click this icon in the Legend column, all file statuses and types are marked Hide.
	Show: Always shows files meeting selected criteria unless overridden by Hide. If you click this icon in the Legend column, all file statuses and types are marked Show.
	Conditional Hide: Doesn't show files meeting selected criteria unless overridden by Show. If you click this icon in the Legend column, all file statuses and types are marked Conditional Hide.
	Conditional Show: Shows selected criteria unless otherwise overridden. If you click this icon in the Legend column, all file statuses and types are marked Conditional Show.

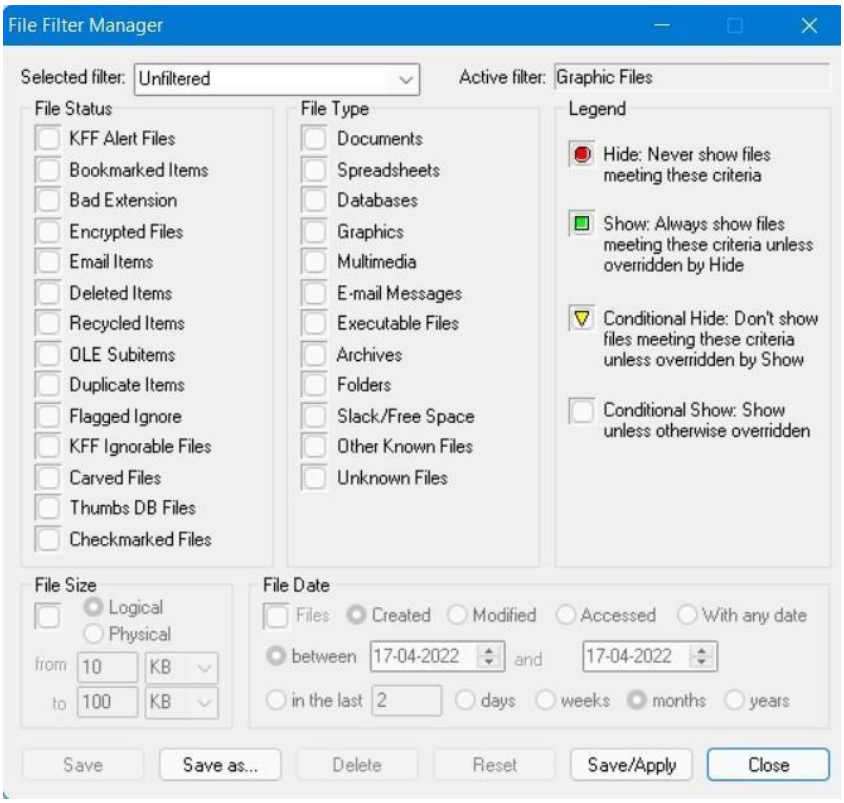
Category	Description
Bookmarked Items	Files that you bookmarked in FTK.
Deleted Files	Complete files or folders recovered from slack or free space.
Duplicate Items	Any items that have an identical hash. Because the filename is not part of the hash, identical files may actually have different filenames. The primary item is the first one found by FTK. The secondary item is any file that has an identical hash of the primary item.
Encrypted Files	Files that are encrypted or have a password. This includes files that have a read-only password. Files with a read-only password may be opened and viewed, but not modified by the reader.
Flagged Ignore	Files that you flagged to ignore.
From E-mail	Files that were embedded in an e-mail message, such as an attachment.
From Recycle Bin	Files derived from the recycled/recycler file structure.
KFF Alert Files	Files identified by the current hash set as illicit or contraband files.
KFF Ignorable	Files identified by the HashKeeper database as common, known files, such as program files.
OLE Subitems	Items or pieces of information that were embedded in a file, such as text, graphics, or an entire file.

Modifying or Creating a Filter

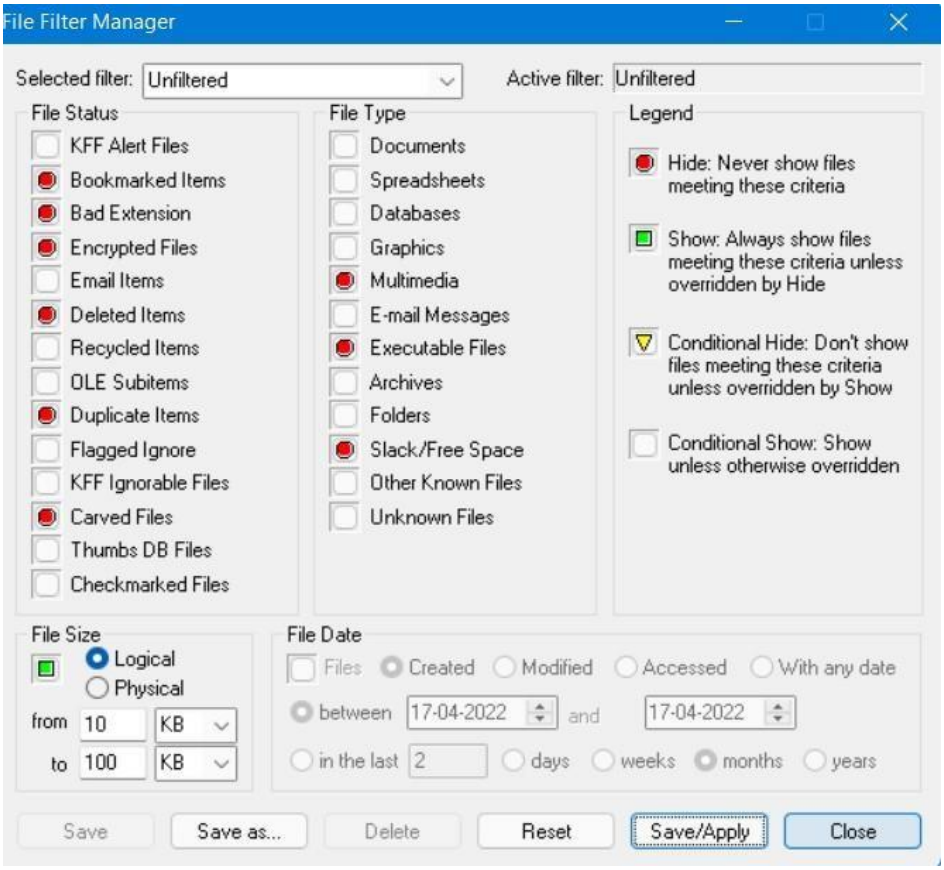
To modify or create a filter:

Step 1. Select **View**, and then **File Filter Manager**.



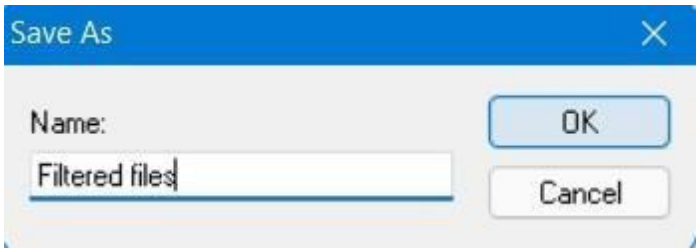


Step 2.Select the filter that you want to modify.



Step 3.If you are modifying an existing filter, click **Save/Apply**. Or

If you are creating a new filter, click **Save As**, enter the name, and click **OK**.

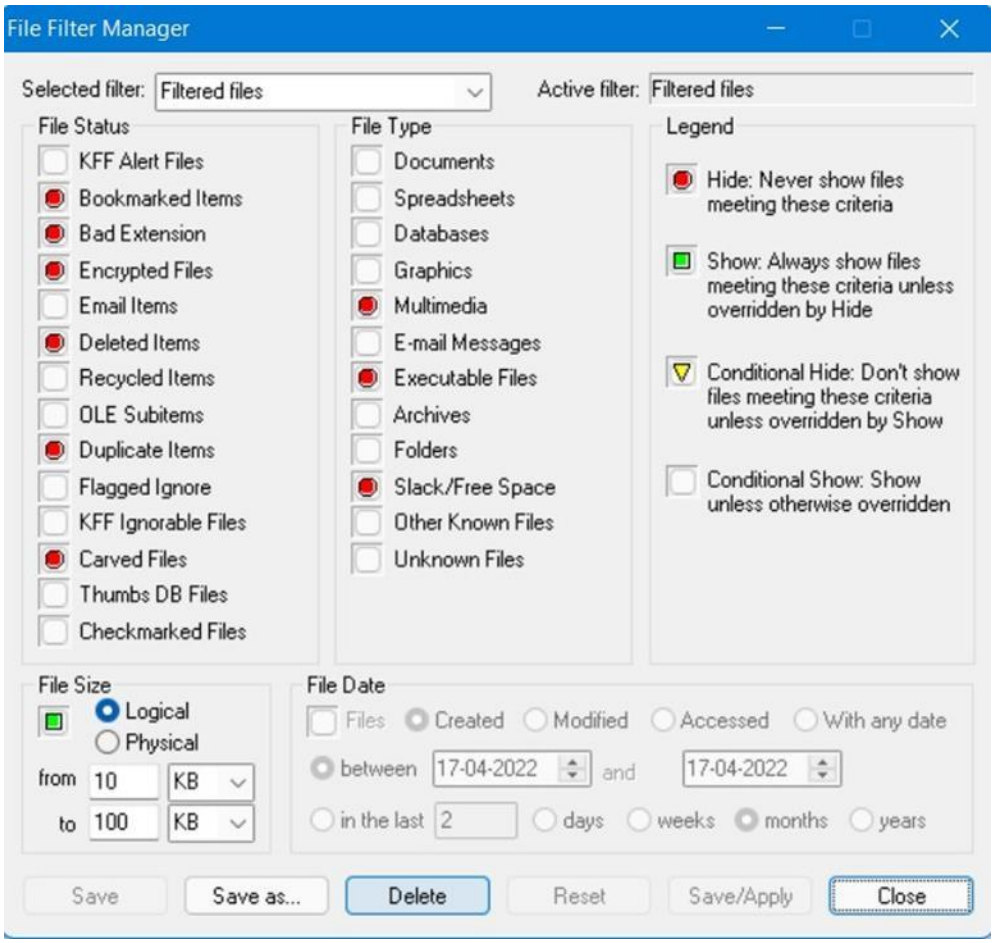


Deleting a Filter

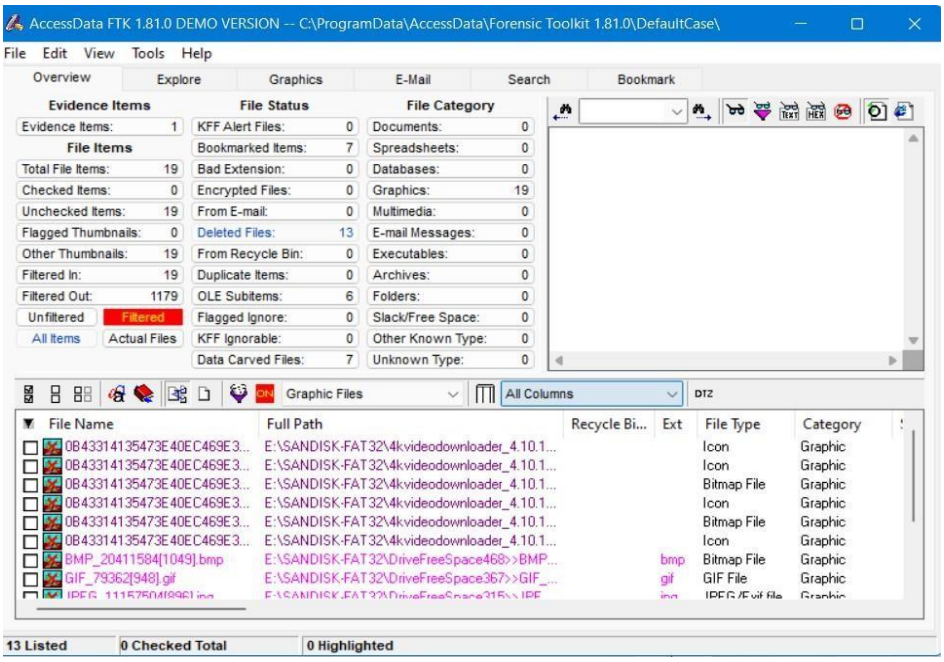
You can delete a filter if you no longer need it. To delete a filter:

Step 1.Select **View**, and then **File Filter Manager**.

Step 2.In the **Selected Filter** drop-down list, select the filter that you want to delete.



Step 3.Click **Delete**.



Searching the Registry

Launching Registry Viewer as a Separate Application:

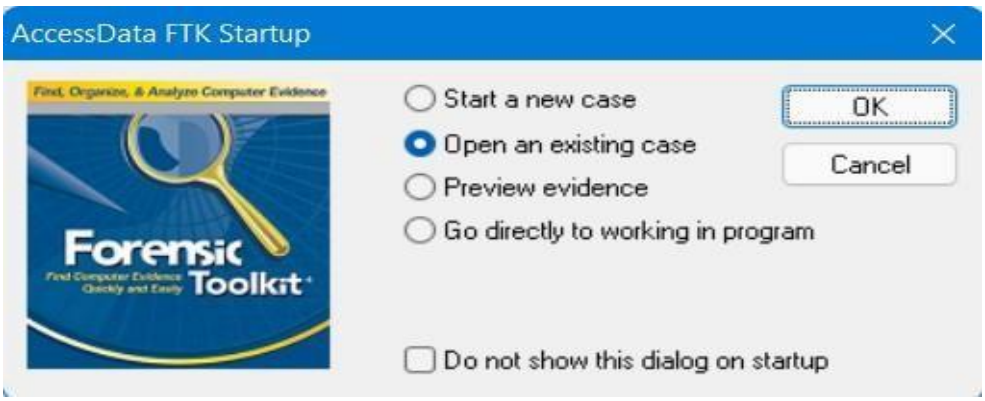
To run Registry Viewer as a separate application, select **Start**, then **Programs**, then **AccessData**, and then **Registry Viewer**, and then **Registry Viewer**.

Launching Registry Viewer from FTK:

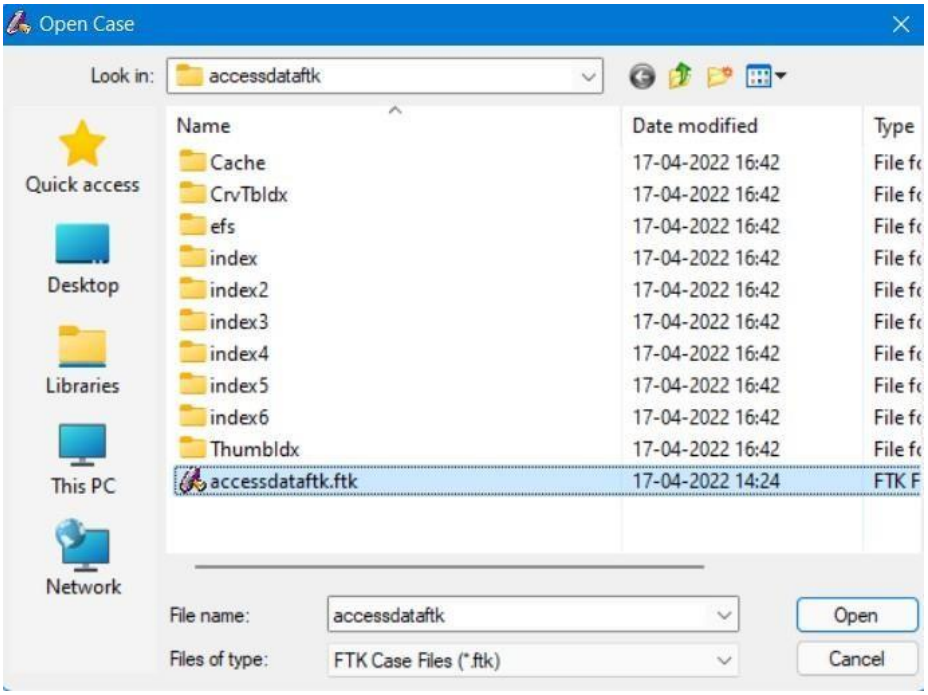
To run Registry Viewer from FTK:

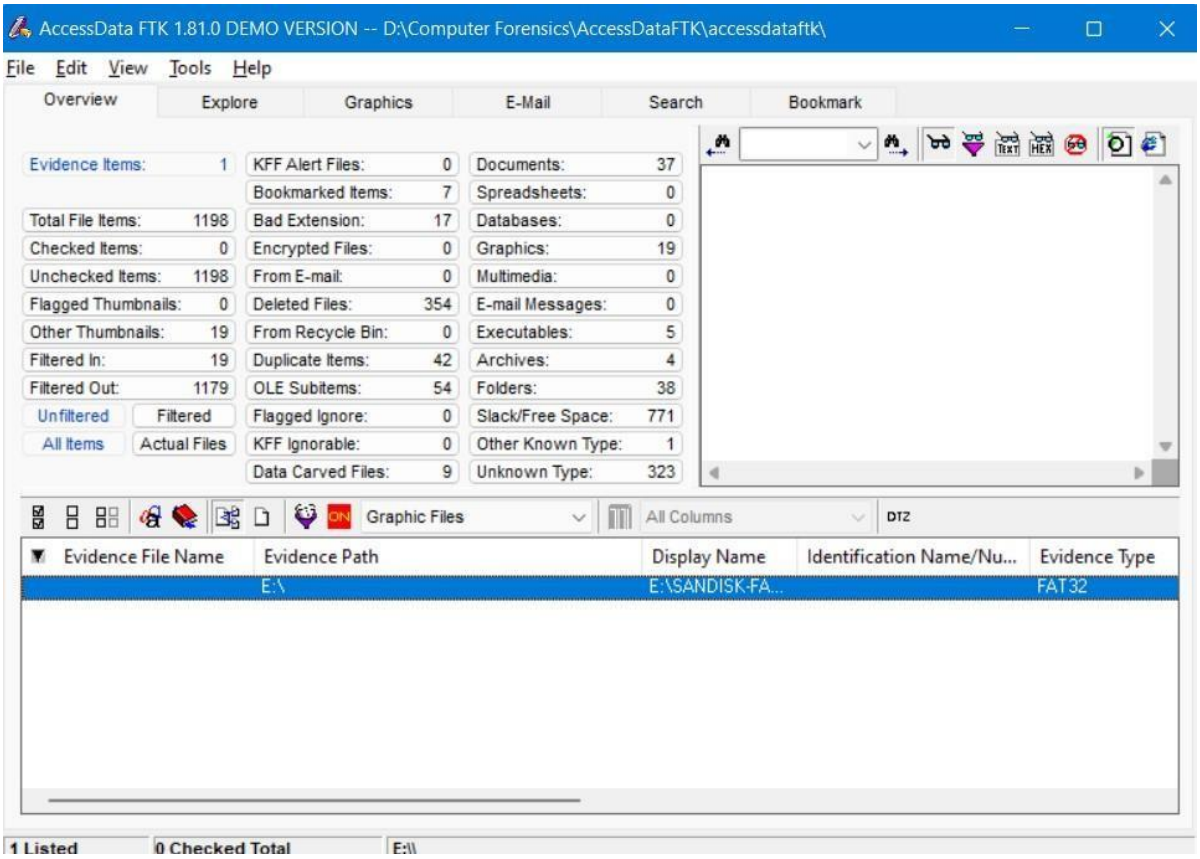
Step 1.In FTK, open an existing case by selecting **File**, and then **Open Case**.

Or if you have chosen to always display the FTK Startup screen, select **Open an Existing Case** and click **OK**

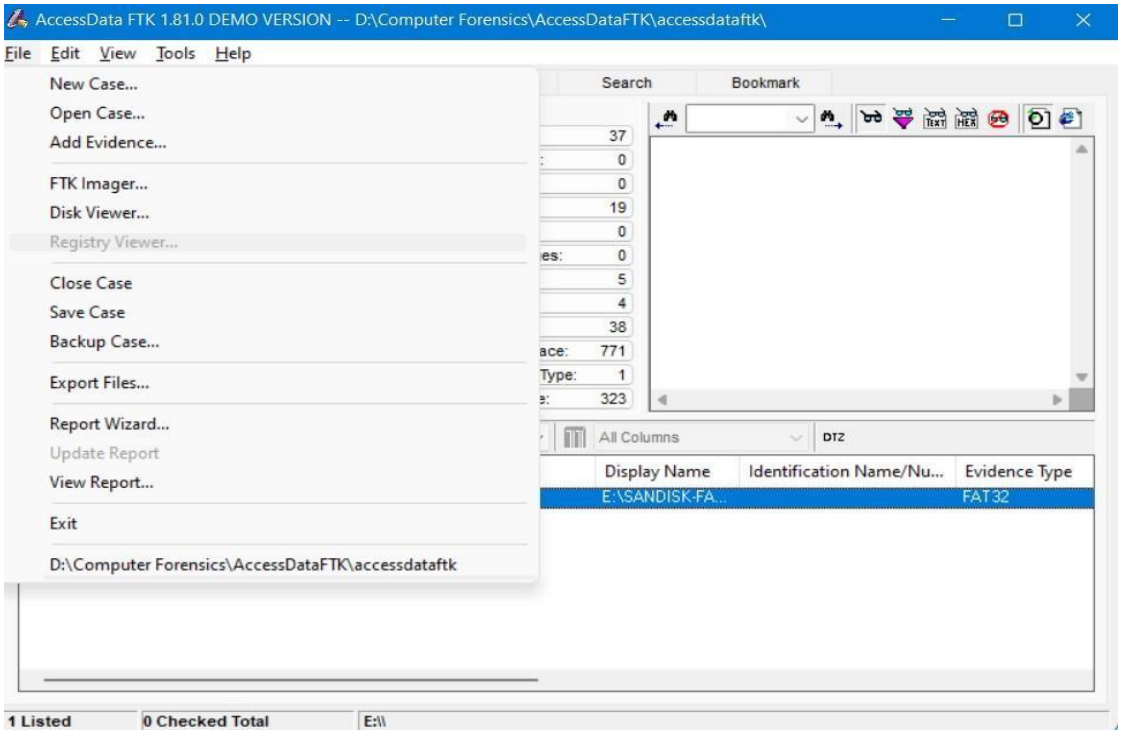


Step 2.Select the case you want to open.





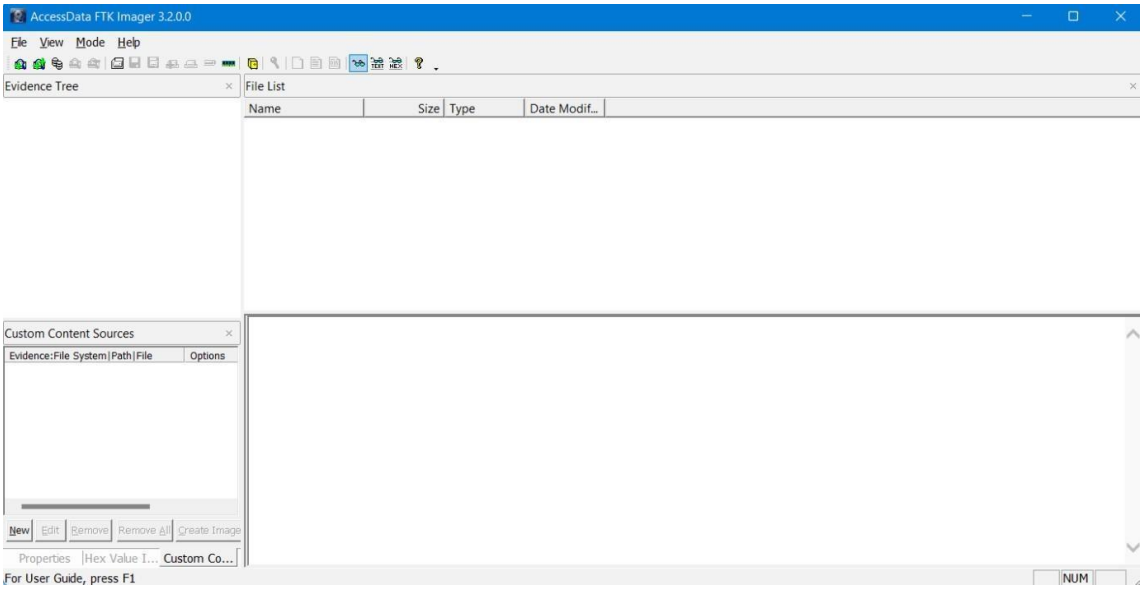
Step 3. Select **File**, and then **Registry Viewer** to open Registry Viewer. (Can't perform ahead of this step because Registry viewer is disabled in demo version)



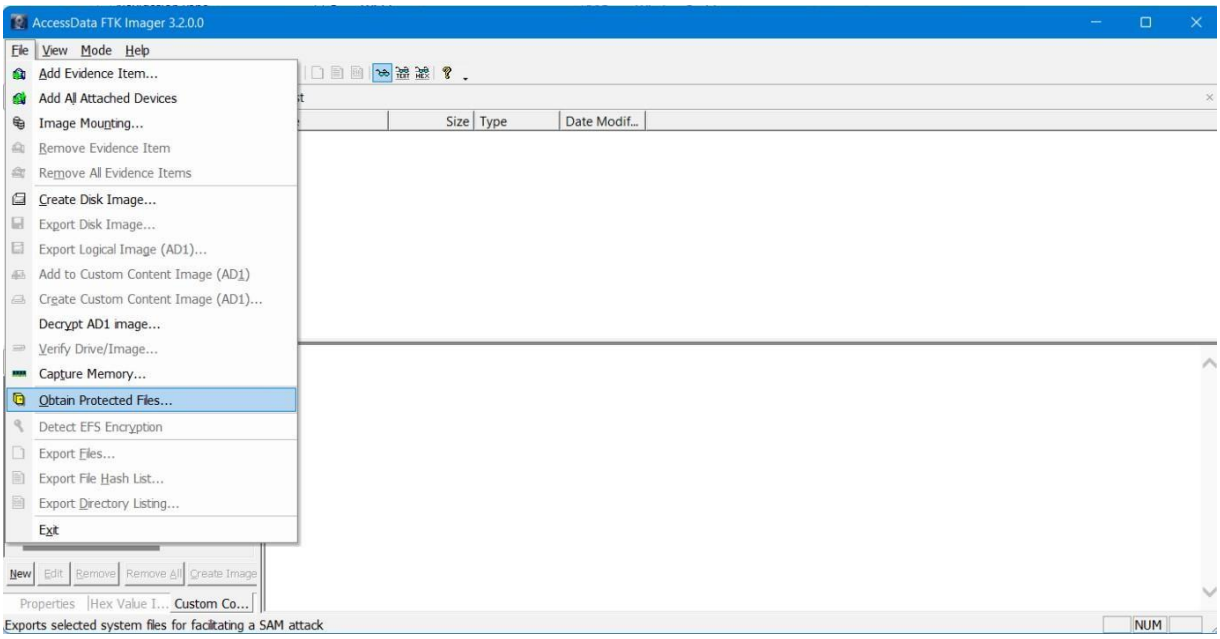
Obtaining Protected Registry Files Using FTK Imager

To obtain the protected registry files using FTK Imager:

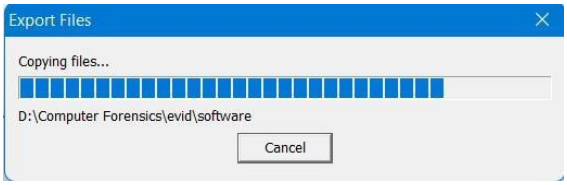
Step 1. Launch FTK Imager.

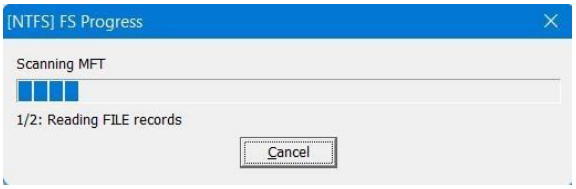


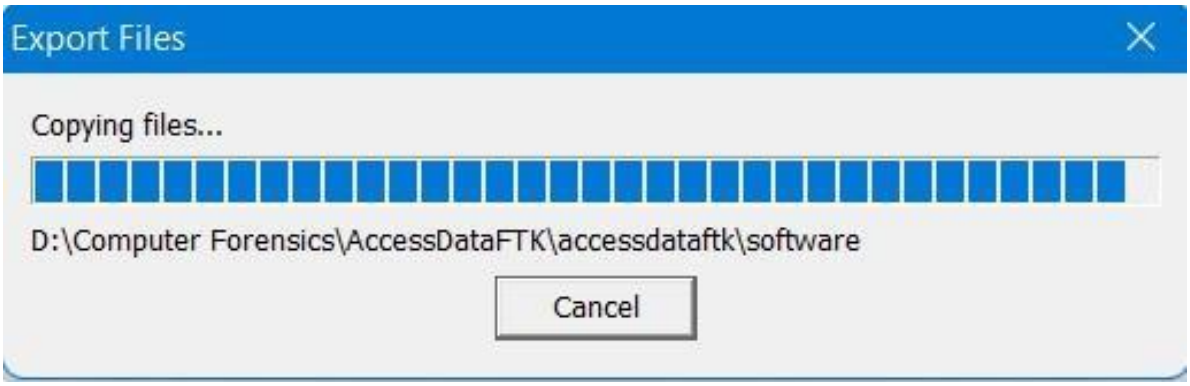
Step 2.Click **File**, and then **Obtain Protected Files**



Step 3.Designate a destination directory and file options, then click **OK**.







FTK Imager exports the selected files to the designated location.

Add the files to the case in FTK.

The following can't be performed in demo version of FTK:

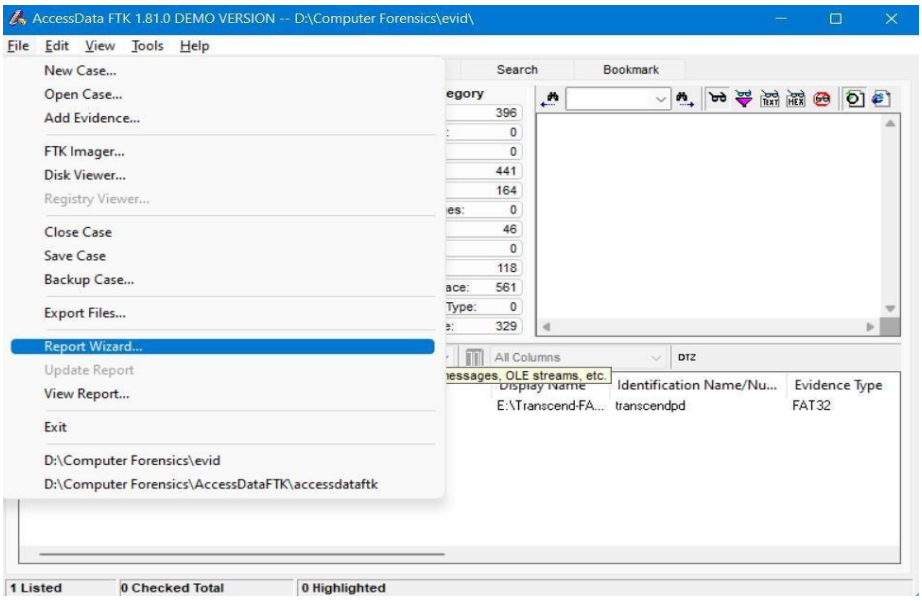
- The Full Registry Window
- The Common Areas Window
- The Report Window
- Opening Registry Files
- Opening a Registry File in Registry Viewer
- Opening Registry Files within FTK
- Obtaining Protected Registry Files Using FTK Imager
- Working with Registry Evidence
- Adding Keys to the Common Areas Window
- Deleting Keys from the Common Areas Window
- Adding Keys to the Report Window
- Deleting Keys from the Report Window
- Creating Registry Summary Reports
- Using Pre-defined AccessData Templates
- Creating Your Own Registry Report Templates
- Changing RSR Settings in the FtkSettings.0.ini File

❖ **Searching for Specific Data**

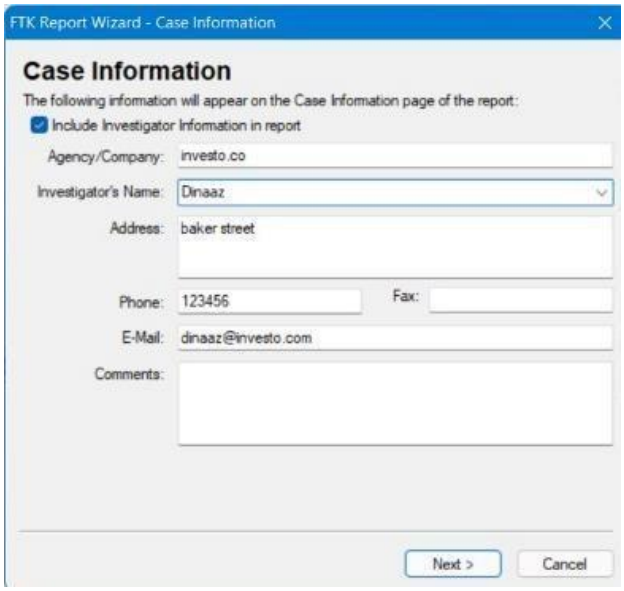
Generating a Report

To generate a report file,

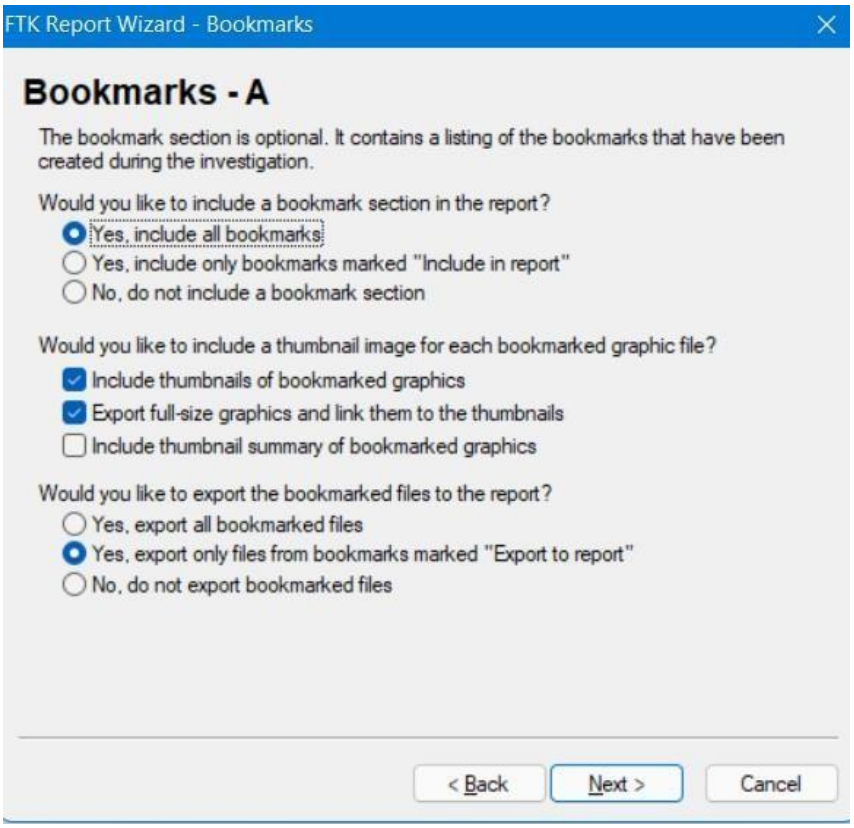
1. From the menu, select **Report**, and then **Generate Report** or click the button on the toolbar.



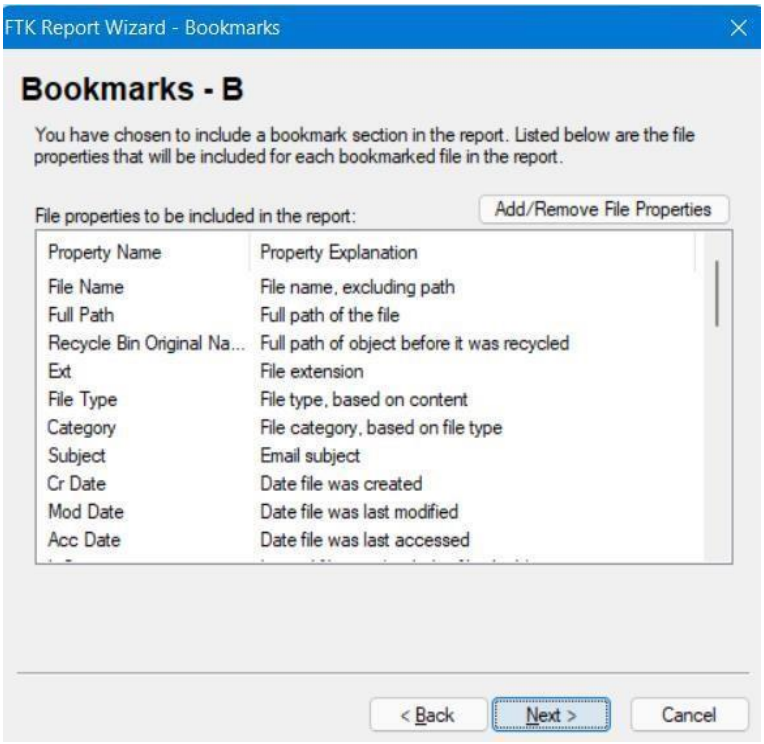
2. The Case Information dialog appears.



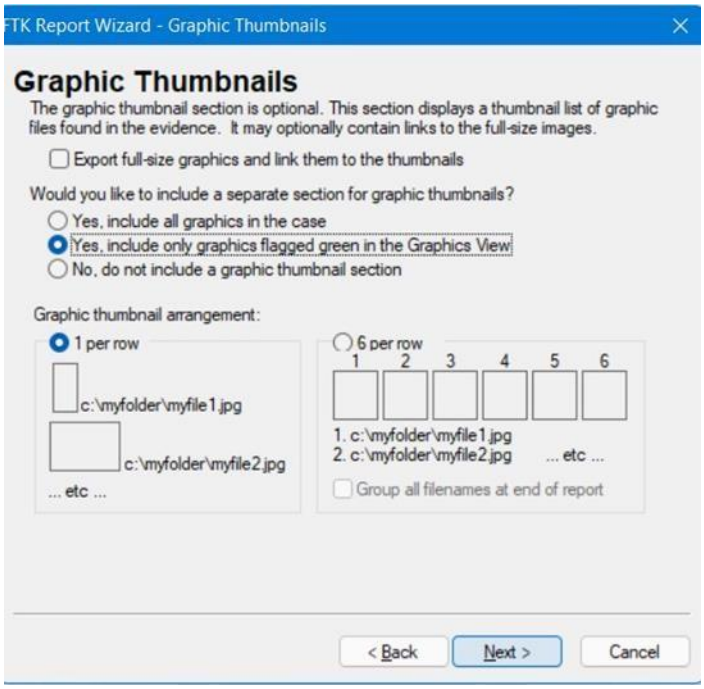
3. The Bookmarks-A dialog appears.



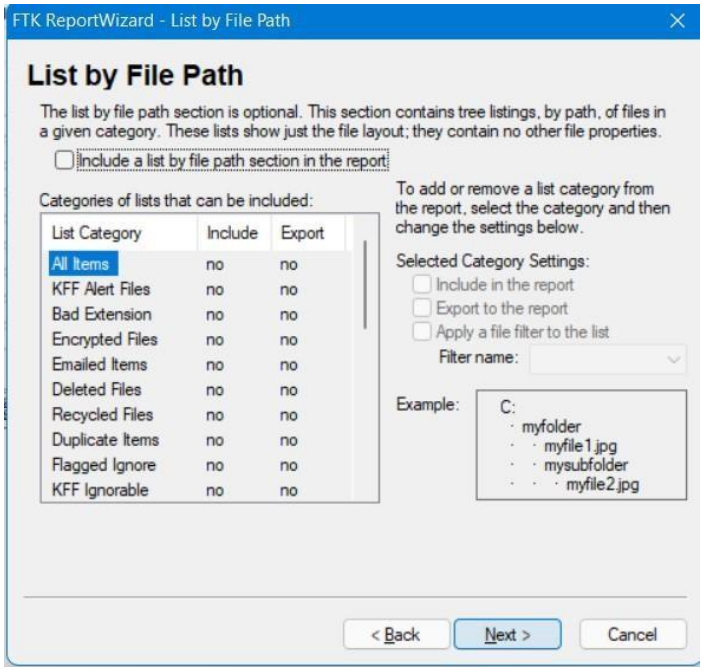
4. The Bookmarks-B dialog appears



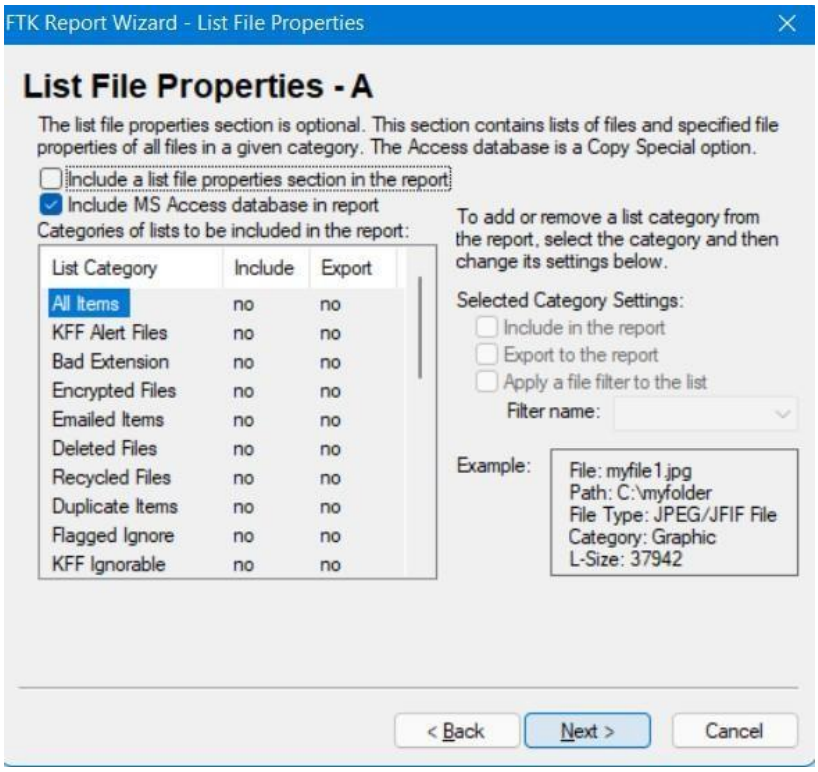
5. The Graphics Thumbnail dialog appears

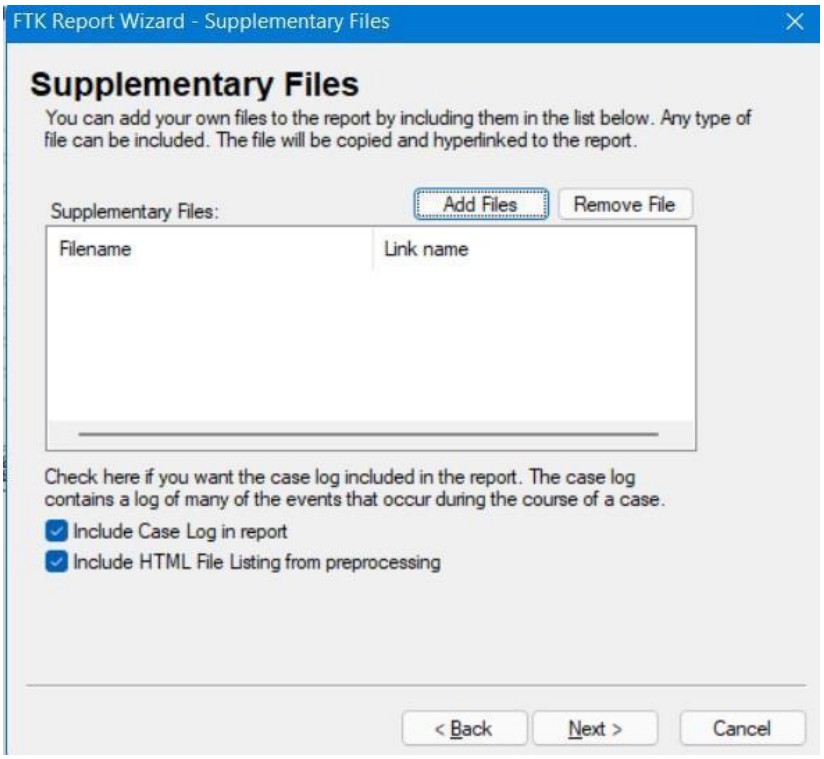


6. The List by File Path dialog appears

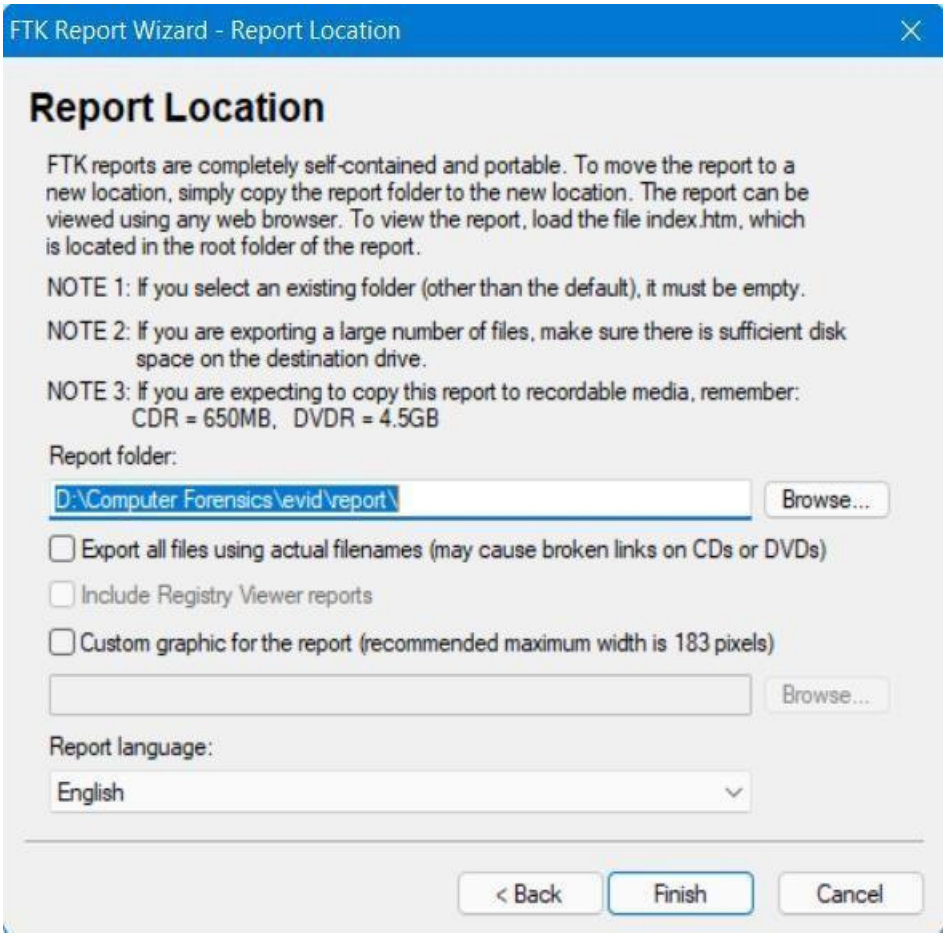


7. Then List File Properties-A dialog appears

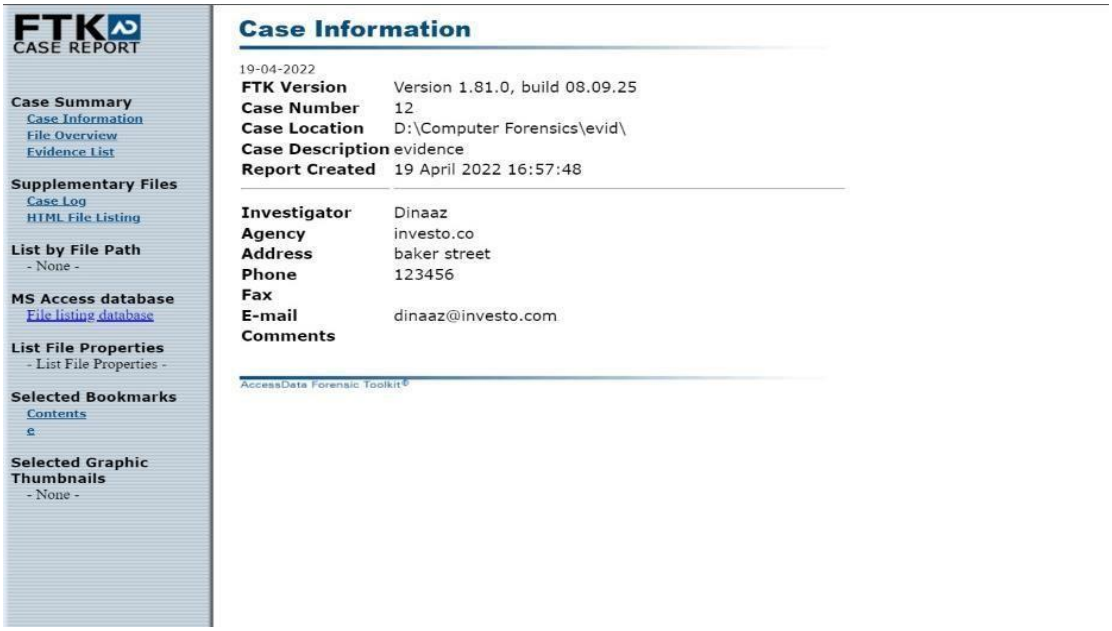




8. The Create Report dialog appears. In the Report Title field, enter a name for the report file. In the Report Location field, enter the location where you want to save the report file or click **Browse** to navigate to the desired location.


FTK Report Wizard - Report Location
Report Location
FTK reports are completely self-contained and portable. To move the report to a new location, simply copy the report folder to the new location. The report can be viewed using any web browser. To view the report, load the file index.htm, which is located in the root folder of the report.
NOTE 1: If you select an existing folder (other than the default), it must be empty.
NOTE 2: If you are exporting a large number of files, make sure there is sufficient disk space on the destination drive.
NOTE 3: If you are expecting to copy this report to recordable media, remember: CDR = 650MB, DVDR = 4.5GB
Report folder:
D:\Computer Forensics\evid\report\
Browse...
Export all files using actual filenames (may cause broken links on CDs or DVDs)
Include Registry Viewer reports
Custom graphic for the report (recommended maximum width is 183 pixels)
Browse...
Report language:
English
< Back
Finish
Cancel


Report Wizard
Do you wish to view the report?
Yes
No



FTK CASE REPORT

Case Summary
Case Information
File Overview
Evidence List

Supplementary Files
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
e

Selected Graphic Thumbnails
- None -

Case Information

19-04-2022

FTK Version	Version 1.81.0, build 08.09.25
Case Number	12
Case Location	D:\Computer Forensics\evid\
Case Description	evidence
Report Created	19 April 2022 16:57:48
Investigator	Dinaaz
Agency	investo.co
Address	baker street
Phone	123456
Fax	
E-mail	dinaaz@investo.com
Comments	

AccessData Forensic Toolkit®

FTK CASE REPORT

Case Summary
Case Information
File Overview
Evidence List

Supplementary Files
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
e

Selected Graphic Thumbnails
- None -

File Overview

19-04-2022

Evidence Items
Evidence Items: 1

File Items
Total File Items: 2,055
Flagged Thumbnails: 0
Other Thumbnails: 441

File Status
KFF Alert Files: 0
Bookmarked Items: 4
Bad Extension: 1
Encrypted Files: 0
From E-mail: 0
Deleted Files: 529
From Recycle Bin: 0
Duplicate Items: 233
OLE Subitems: 0
Flagged Ignore: 0
KFF Ignorable: 0
Data Carved Files: 5

File Category
Documents: 396
Spreadsheets: 0
Databases: 0
Graphics: 441
Multimedia: 164
E-mail Messages: 0
Executables: 46
Archives: 0
Folders: 118
Slack/Free Space: 561
Other Known Type: 0
Unknown Type: 329

AccessData Forensic Toolkit®

Practical No 3

Aim: - Understanding & working with the process of taking a drive image using AccessData's FTK Imager tool.

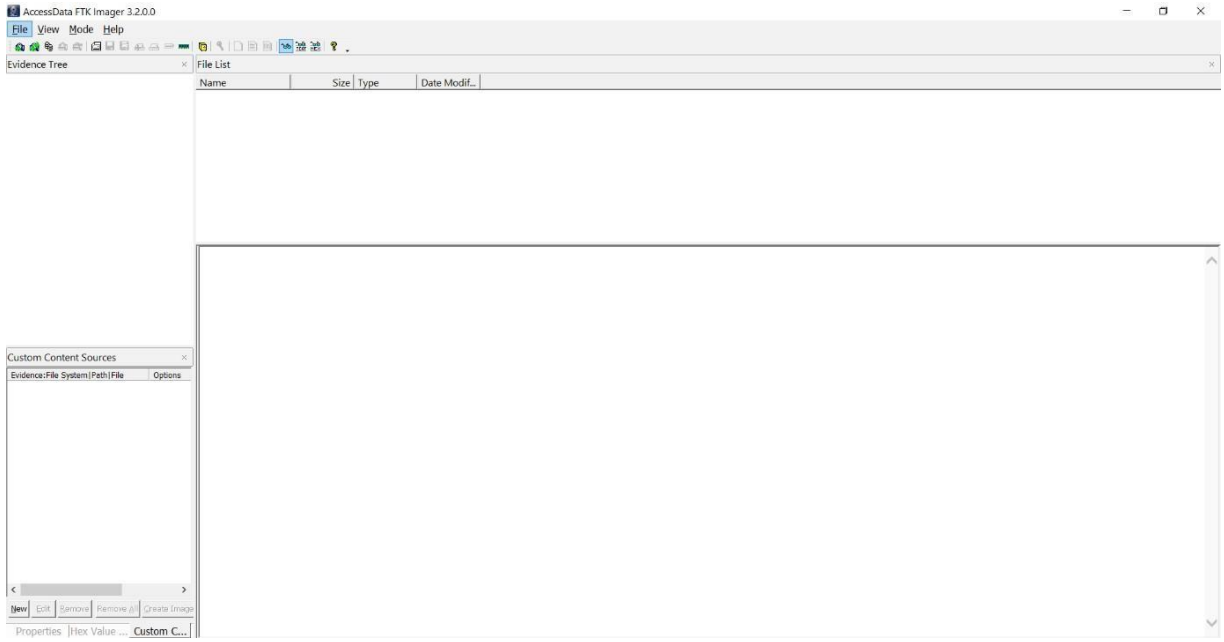
Using File recovery Tools

Practical No 3

Aim: - Understanding & working with the process of taking a drive image using AccessData's FTK Imager tool.

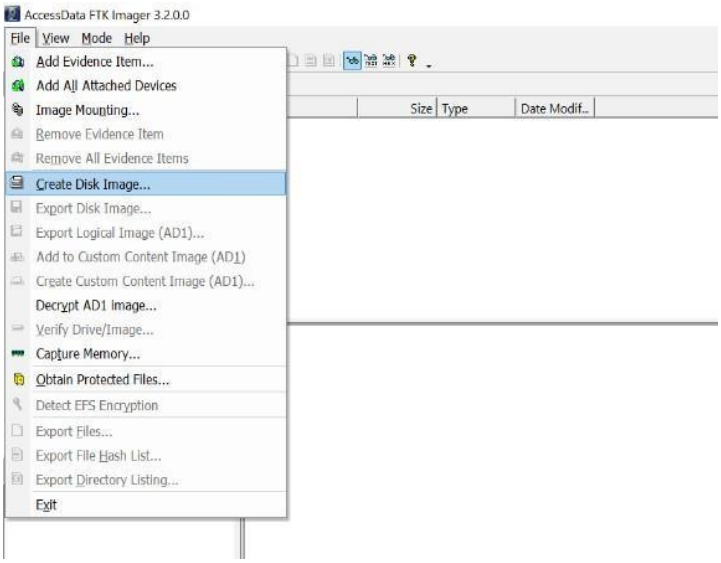
Using File recovery Tools

Step 1) Run **FTK Imager.exe** to start the tool.



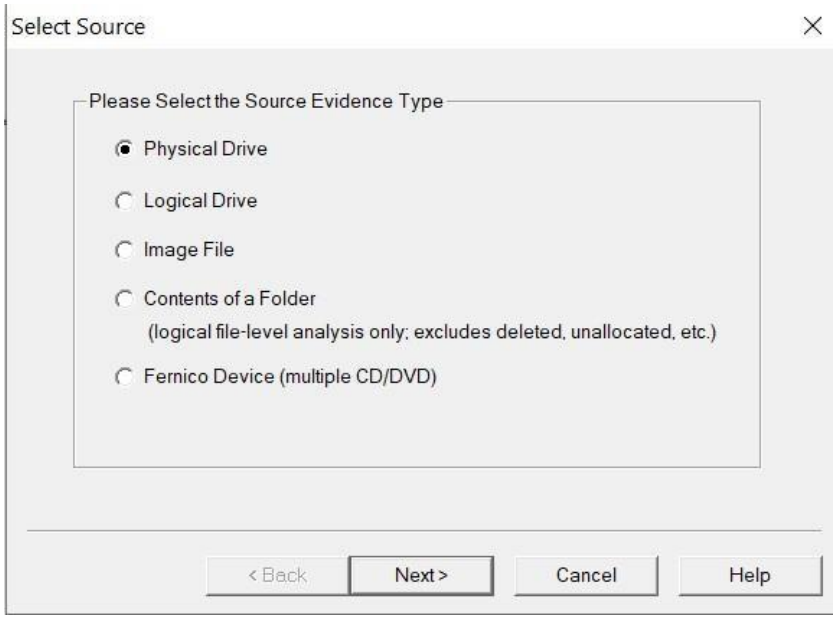
Step 2) To create a forensic image:

Click File > Create Disk Image

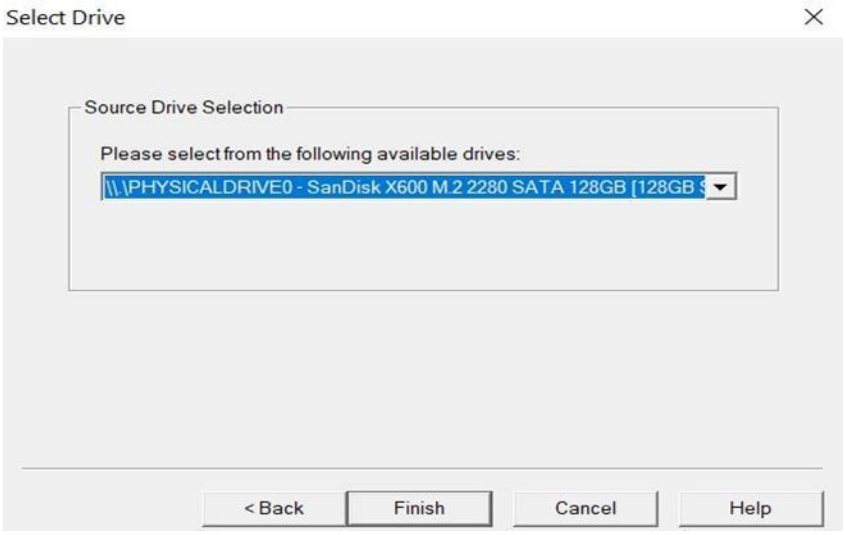


Step 3) In the Select Source dialog box, select the source you want to make an image of. Click Next.

If you select Logical Drive and need to select a floppy or CD as a source, you can check the Automate multiple removable media box to create groups of images. Imager will automatically increment the case numbers with each image, and if something interrupts the process, you may assign case number manually.



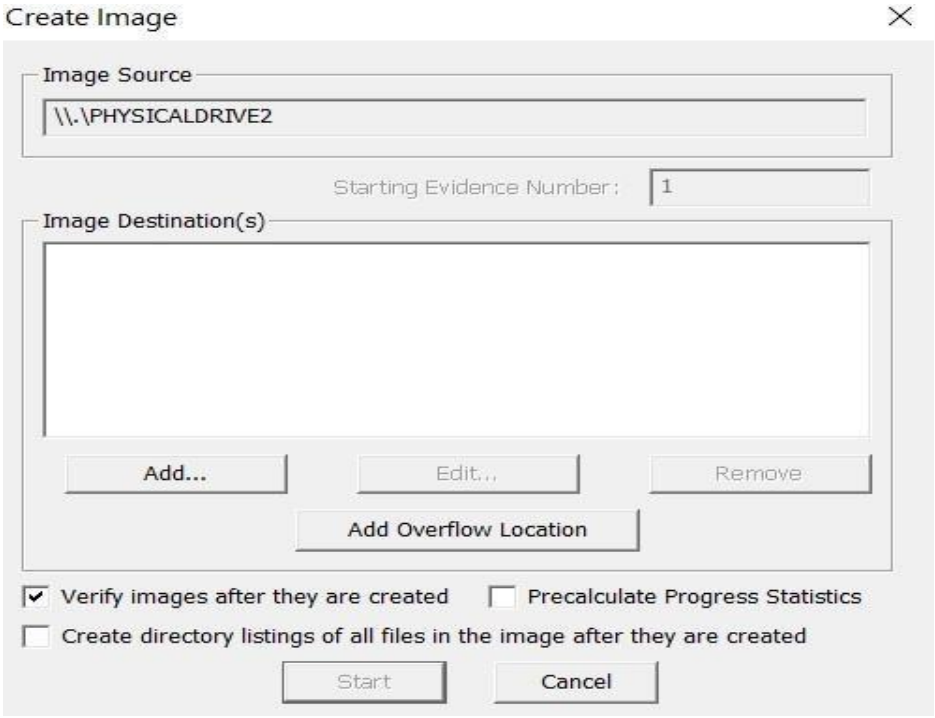
Step 4) Select the drive or browse to the source of the image you want, and then click Finish.



Step 5) In the Create Image dialog, click Add .... to add the image destination.

- Compare the stored hashes of your image content by checking the Verify images after they are created box. If a file doesn't have a hash, this option will generate one.

List the entire contents of your images with path, creation dates, whether files were deleted, and other metadata. The list is saved in tab-separated value (.TSV) format.

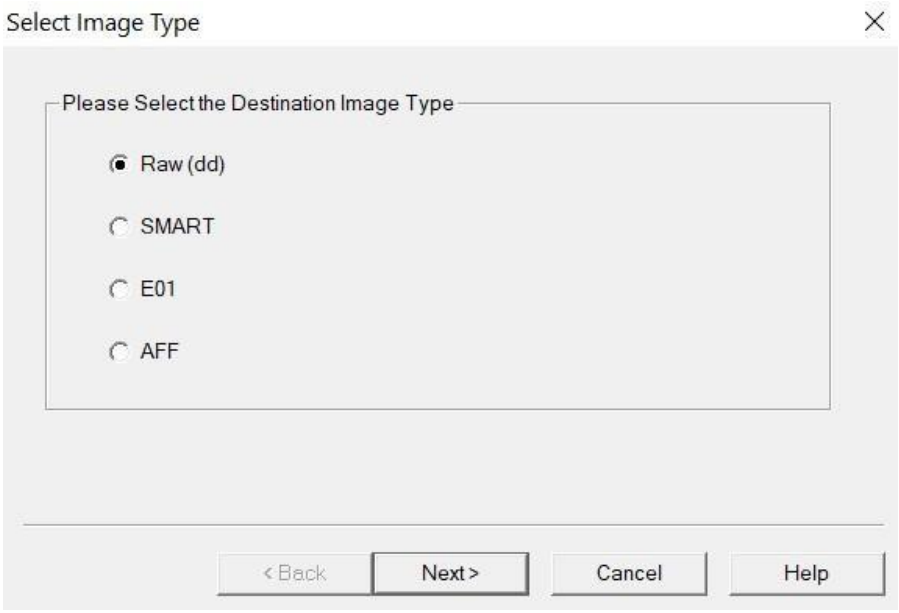


Step 6) Select the type of image you want to create.

The type you choose will usually depend on what tools you plan to use on the image. The dd format will work with more open source tools, but you might want SMART or E01 if you will primarily be working with ASR Expert Witness or EnCase, respectively.

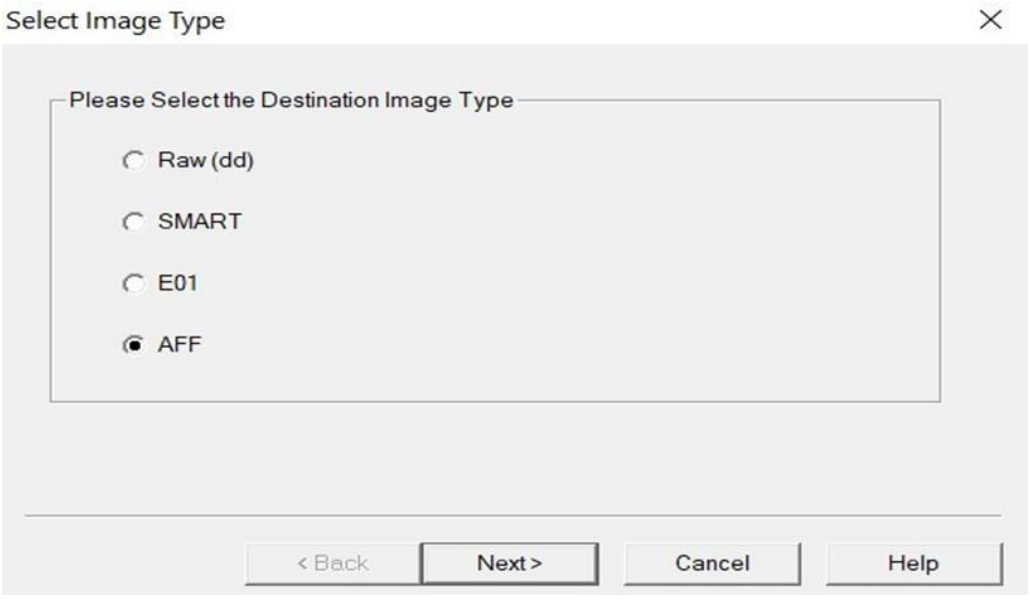
Note: If you are creating an image of a CD or DVD, this step is skipped because all CD/DVD images are created in the IsoBuster CUE format. Hashes are not generated for CD and DVD images so they will not be verified, as well.

Important: The raw image type is not compressed. If you select the Raw (dd) type, be sure to have adequate available drive space for the resulting image.

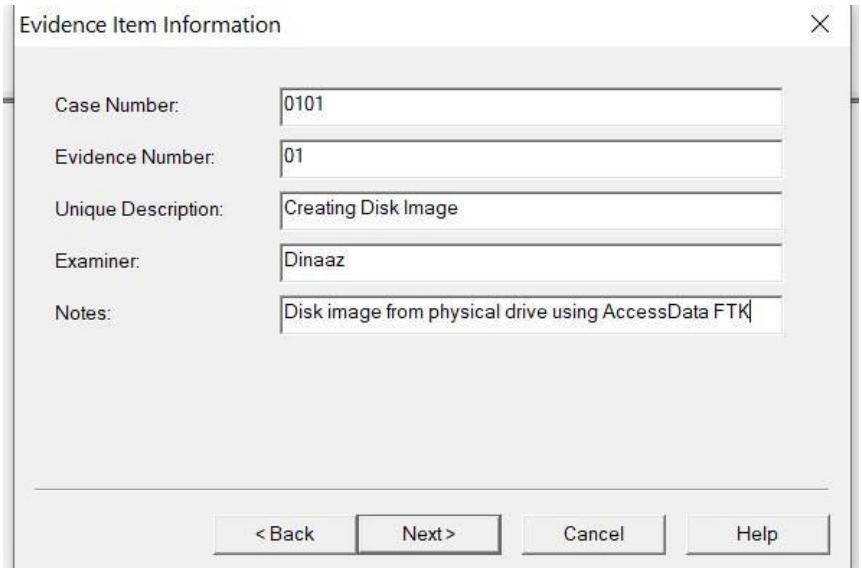


Step 7) If you are creating an AFF image type, choose AFF. Click Next.

The Image Destination Folder dialog box you see will be different than that seen when selecting any other image type



Step 8) If your version of FTK requests evidence information, you can provide it. Specify Evidence Item Information. All Evidence Item Information is optional, but it is helpful to have the information easily accessible in case it is called into question at any time after creation



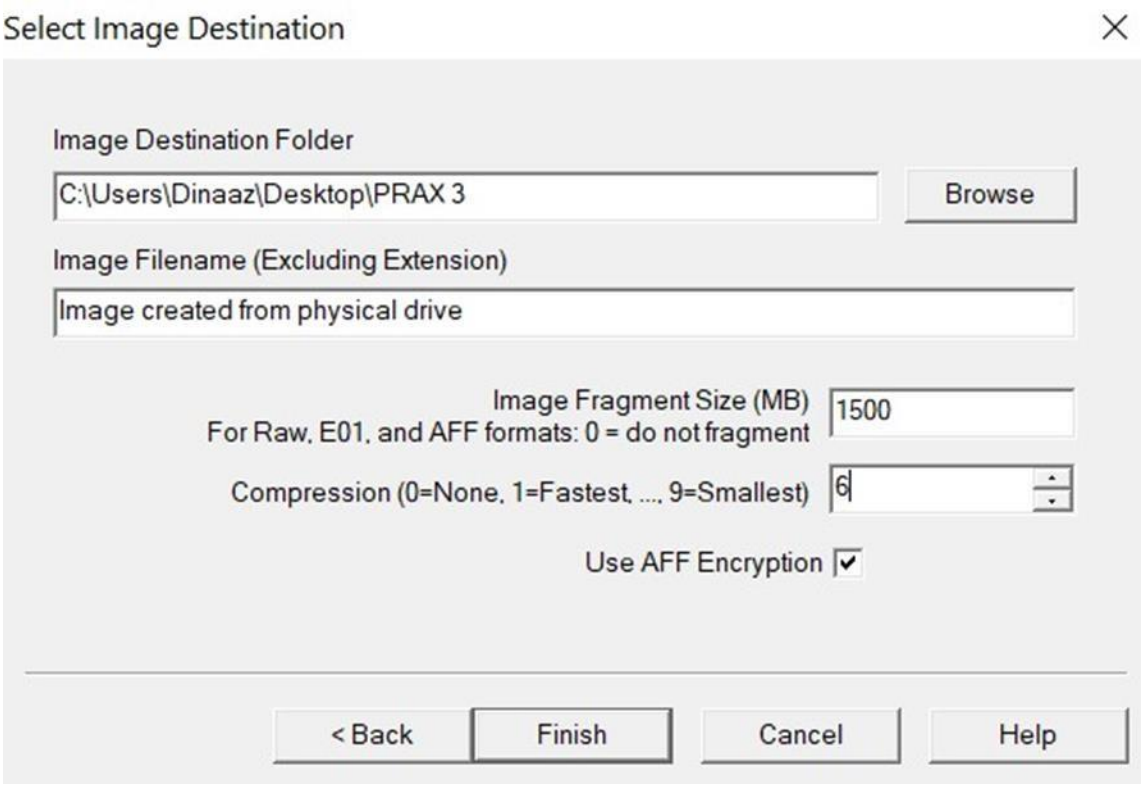
Complete the fields in the Evidence Item Information dialog. Click Next.

Step 9) Select the Image Destination folder and file name. You can also set the maximum fragment size of image split files. Click Finish to complete the wizard.

In the Image Destination Folder field, do one of the following:

- Type the location path where you want to save the image file.
- Click Browse to find and select the desired location.

In the Image Filename field, specify a name for the image file but do not specify a file extension.



Step 10) Specify the Image fragment Size:

- Default Image Fragment Size = 1500 MB
- To save images segments that can be burned to a CD, specify 650 MB.
- To save image segments that can be burned to a DVD, specify 4000 MB.
- The .S01 format is limited by design to sizes between 1 MB and 2047 MB (2 GB). Compressed block pointers are 31-bit numbers (the high bit is a compressed flag), which limits the size of any one segment to two gigabytes.

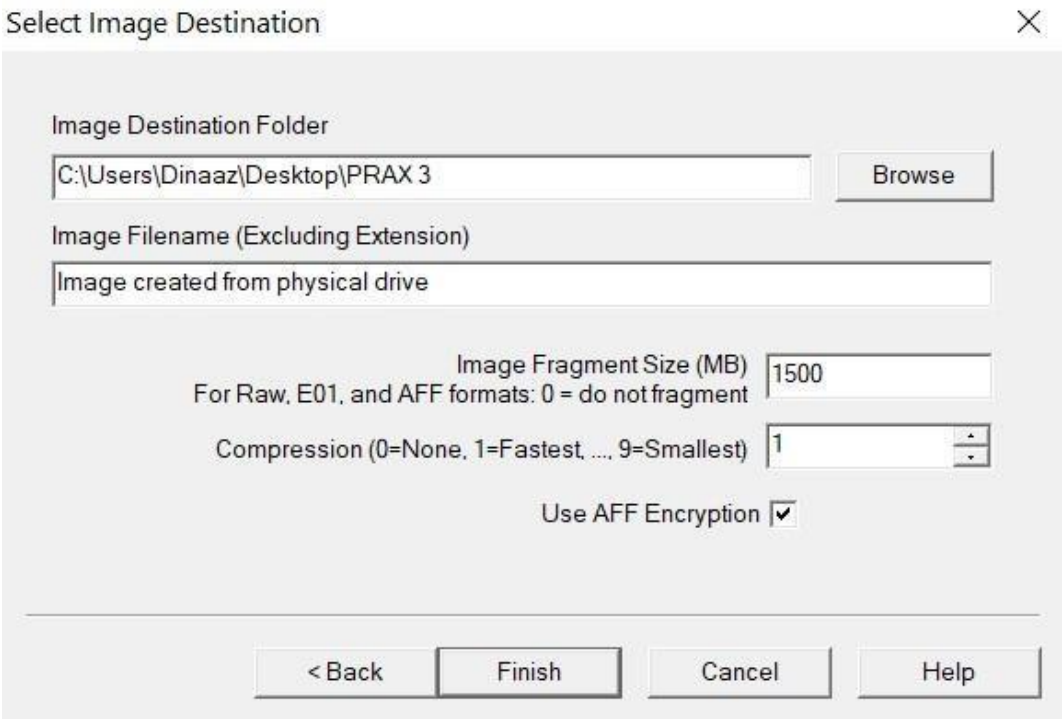
Step 10 a) Select the compression level to use.

- 0=No Compression
- 1=Fastest, Least Compression (faster, and also slightly smaller than a 0-compression file)
- 9=Slowest, Most Compression (smallest file, slowest to create).

Numbers between 1 and 9 produce an image with varying levels of compression to speed ratio.

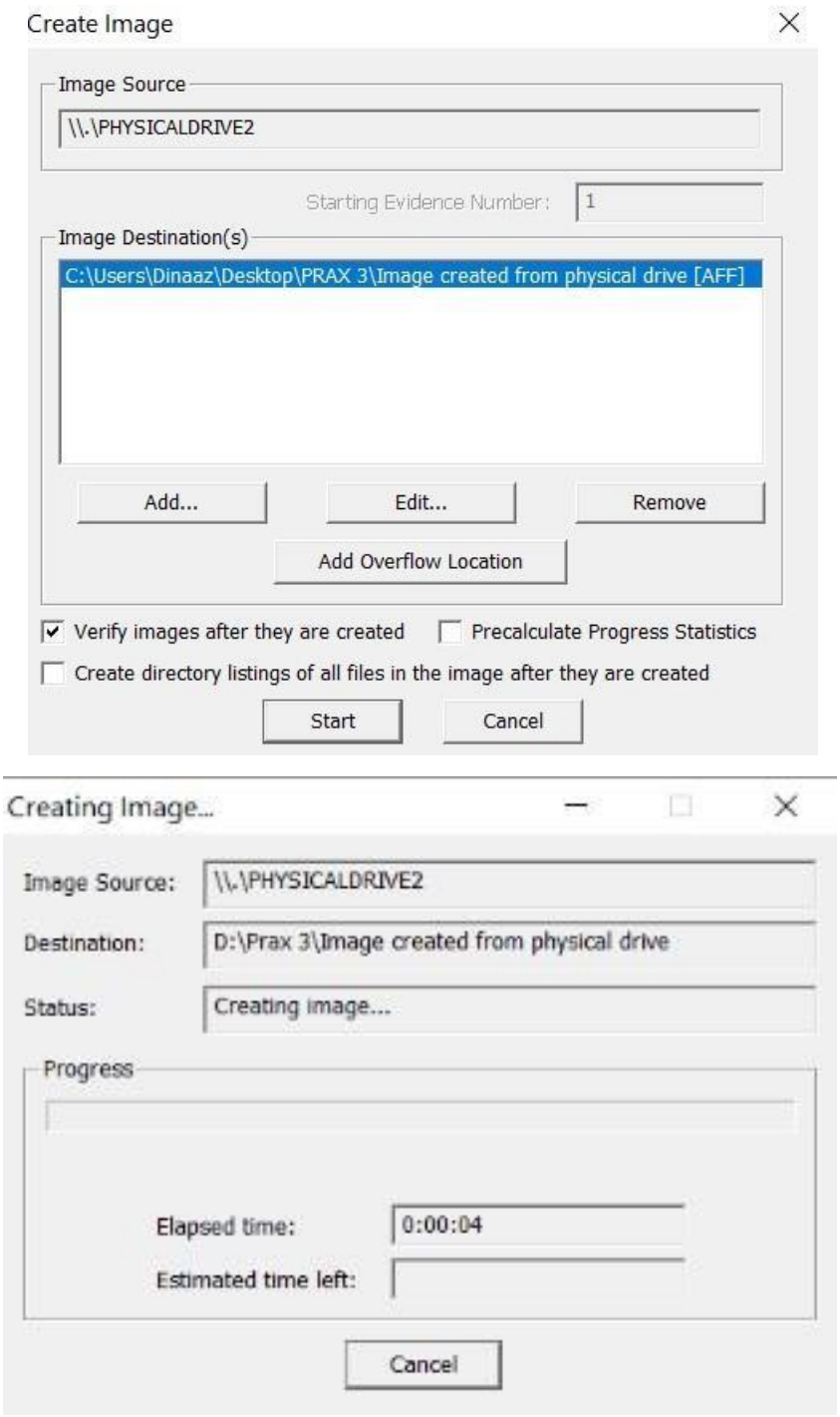
Step 11) To encrypt the image, choose the correct encryption box as explained below: a. To encrypt the new image with AD Encryption, mark the Use AD Encryption box.
b. To encrypt the new image with AFF Encryption, mark the Use AFF Encryption box.

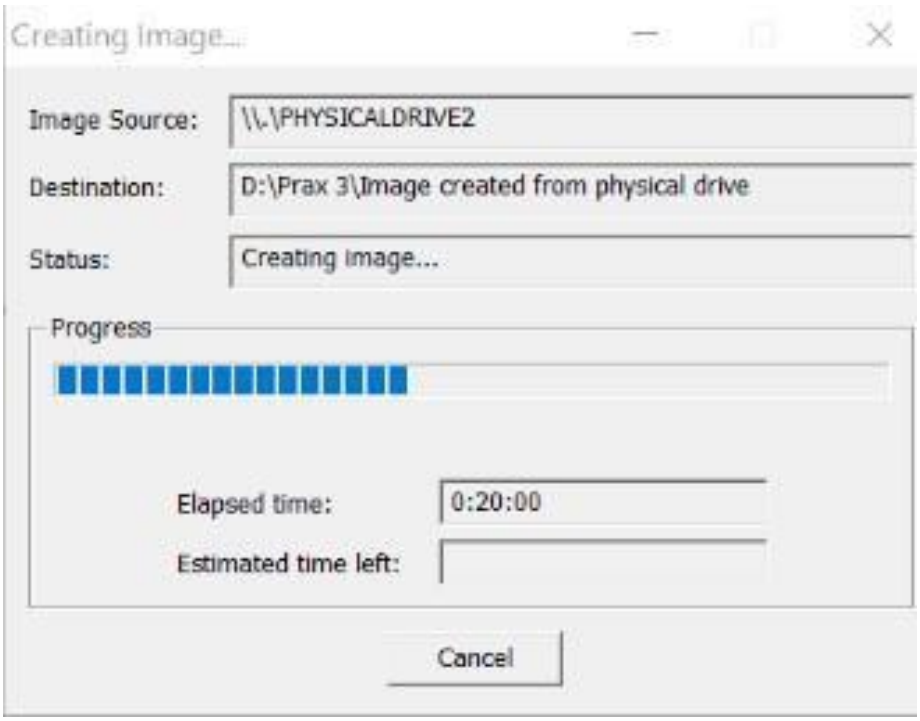
Step 12) Click Finish.

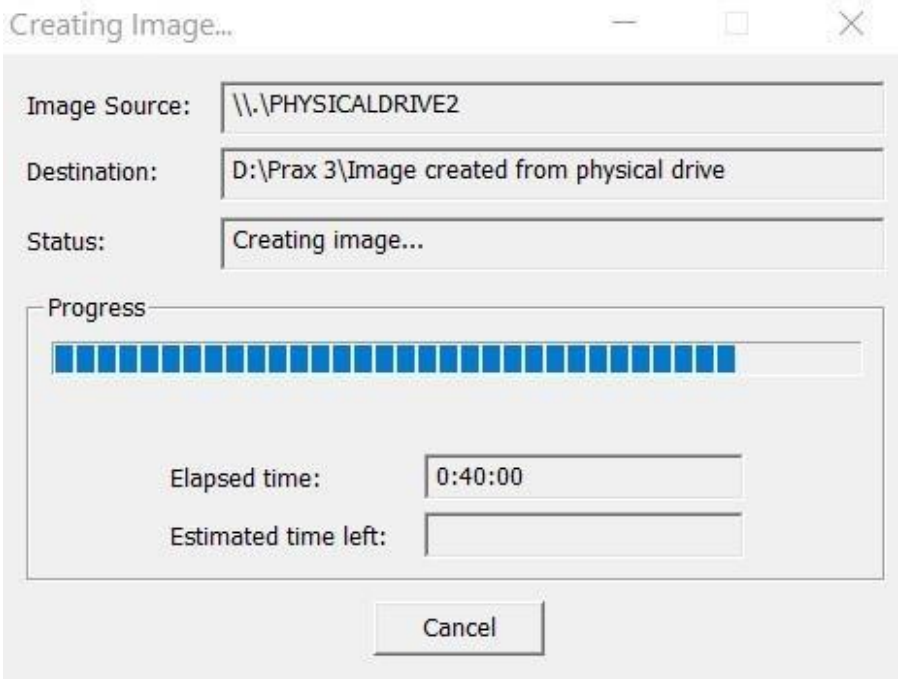


Step 13) When AFF Encryption is selected, type the password, and retype the password to confirm. Click Show Password to see that you have typed it correctly the first time.

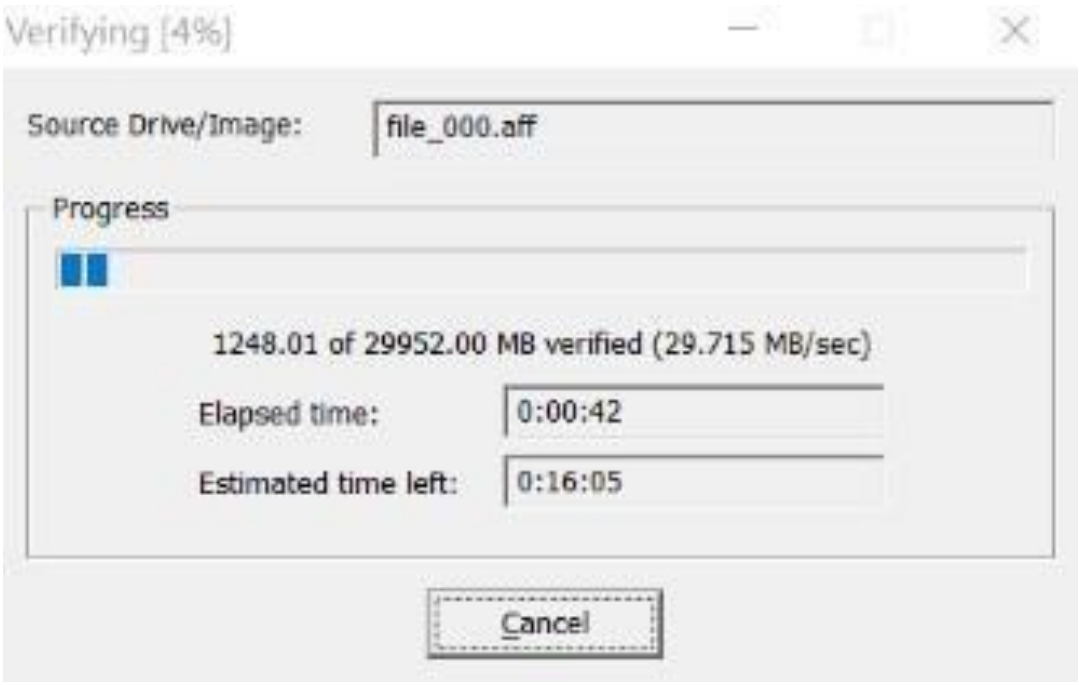
Step 14) When encryption selections are made, click OK to save selections and return to the Create Image dialog. Click Start to begin the imaging process.



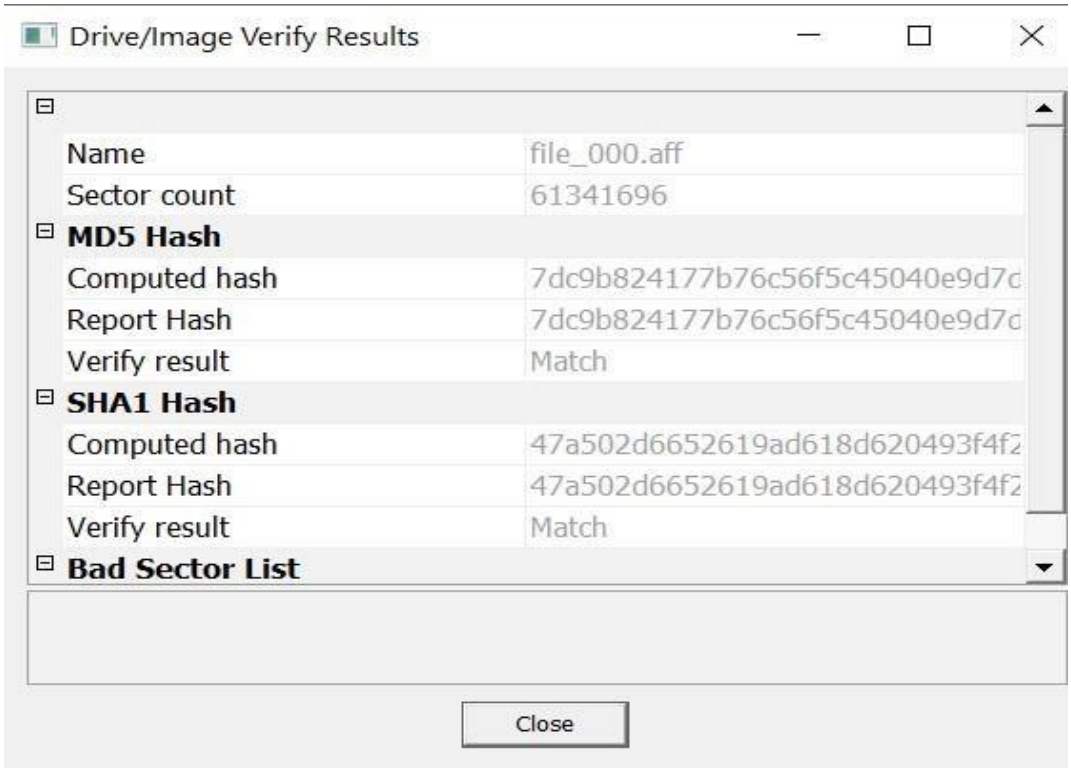


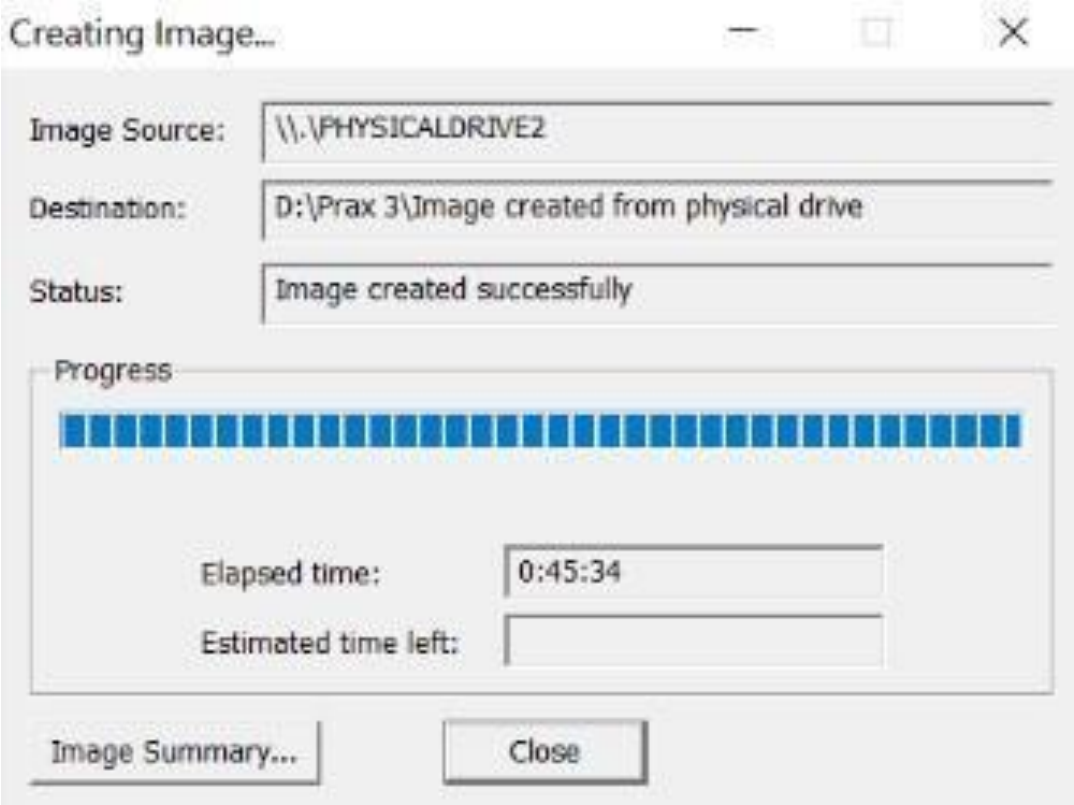


After the images are successfully created, the Drive/Image Verify Results box shows detailed image information, including MD5 and SHA1 check sums, and bad sectors.



Now is a good time to refill that coffee cup! Once the acquisition is complete, you can view an image summary and the drive will appear in the evidence list in the left hand side of the main FTK Imager window. You can right-click on the drive name to Verify the Image:





A progress dialog appears that shows the following:

- The source that is being imaged
- The location where the image is being saved
- The status of the imaging process
- A graphical progress bar
- The amount of data in MB that has been copied and the total amount to be copied
- Elapsed time since the imaging process began
- Estimated time remaining until the process is complete
- Image Summary button. Click it to open the Image Summary window as shown below:

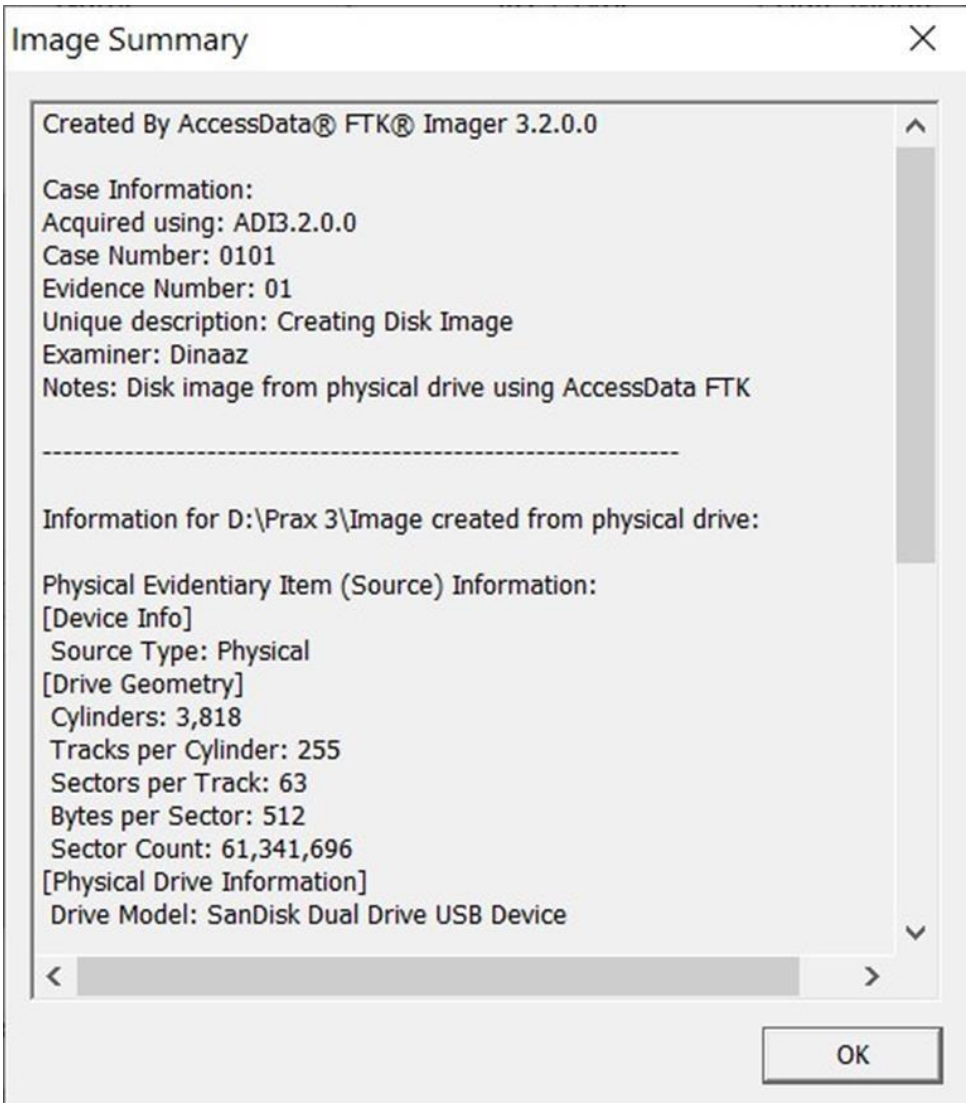


Image Summary
Created By AccessData® FTK® Imager 3.2.0.0
Case Information:
Acquired using: ADI3.2.0.0
Case Number: 0101
Evidence Number: 01
Unique description: Creating Disk Image
Examiner: Dinaaz
Notes: Disk image from physical drive using AccessData FTK

Information for D:\Prax 3\Image created from physical drive:
Physical Evidentiary Item (Source) Information:
[Device Info]
Source Type: Physical
[Drive Geometry]
Cylinders: 3,818
Tracks per Cylinder: 255
Sectors per Track: 63
Bytes per Sector: 512
Sector Count: 61,341,696
[Physical Drive Information]
Drive Model: SanDisk Dual Drive USB Device
OK

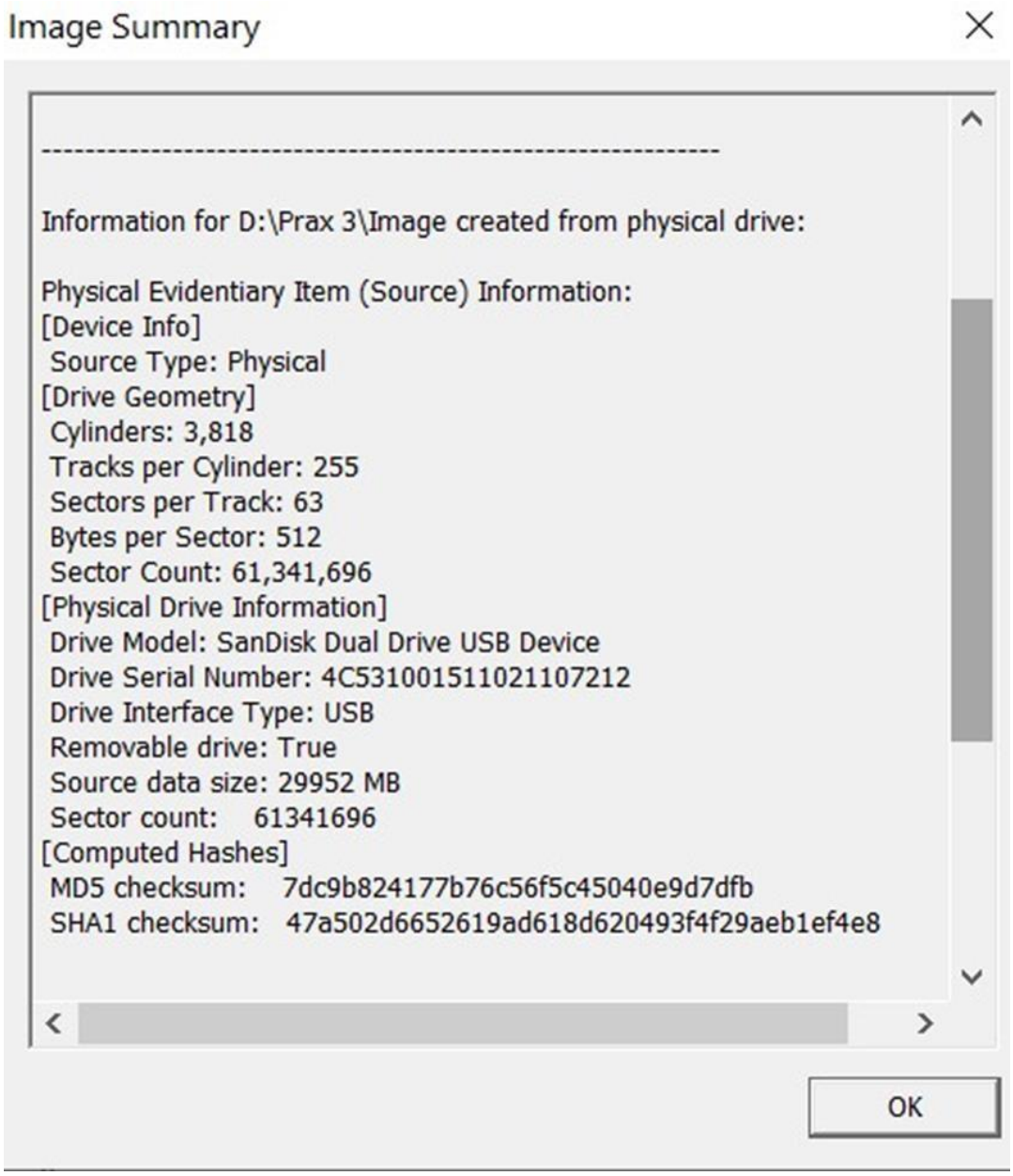


Image Summary

Information for D:\Prax 3\Image created from physical drive:
Physical Evidentiary Item (Source) Information:
[Device Info]
Source Type: Physical
[Drive Geometry]
Cylinders: 3,818
Tracks per Cylinder: 255
Sectors per Track: 63
Bytes per Sector: 512
Sector Count: 61,341,696
[Physical Drive Information]
Drive Model: SanDisk Dual Drive USB Device
Drive Serial Number: 4C531001511021107212
Drive Interface Type: USB
Removable drive: True
Source data size: 29952 MB
Sector count: 61341696
[Computed Hashes]
MD5 checksum: 7dc9b824177b76c56f5c45040e9d7dfb
SHA1 checksum: 47a502d6652619ad618d620493f4f29aeb1ef4e8
OK

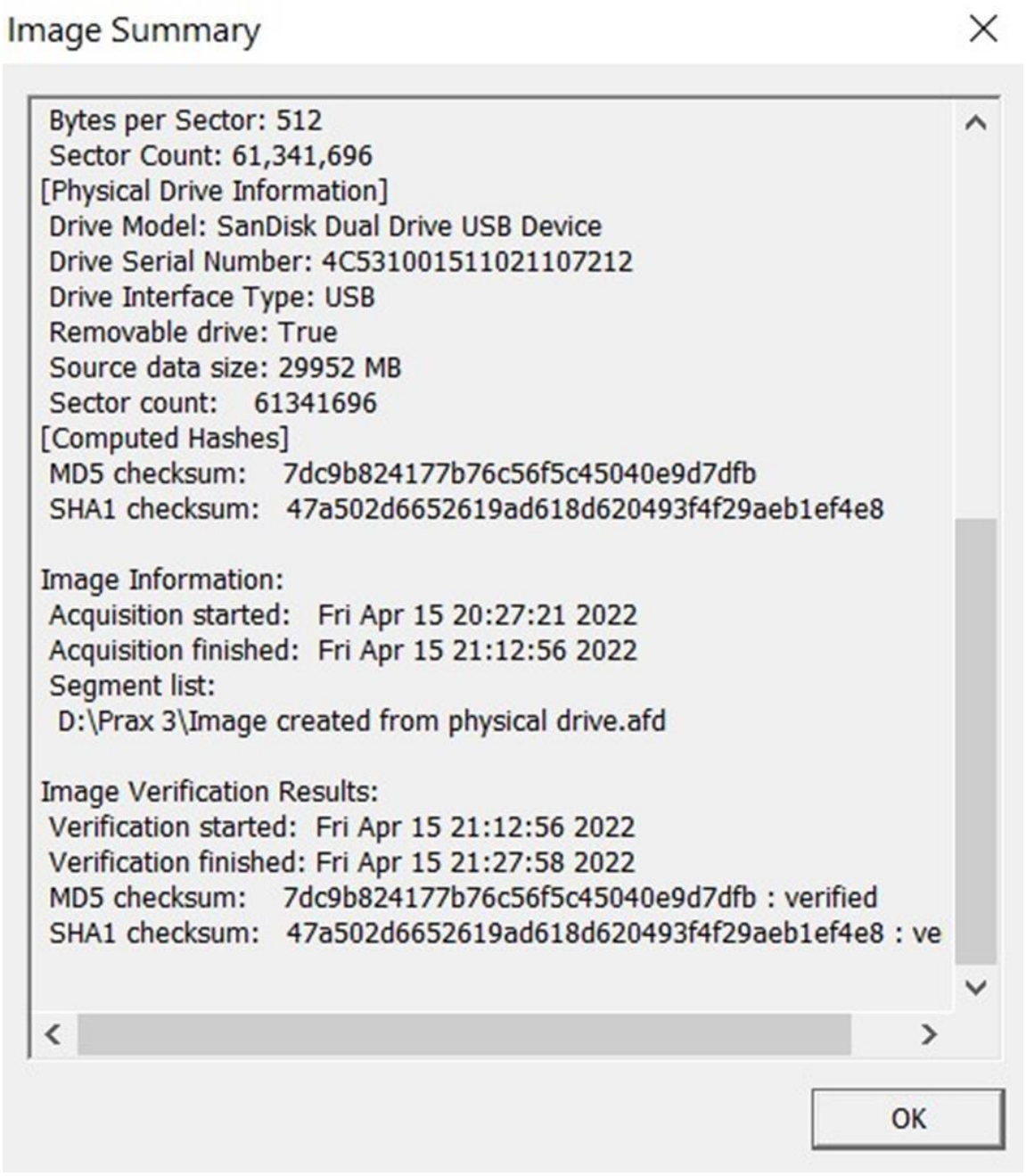


Image Summary
Bytes per Sector: 512
Sector Count: 61,341,696
[Physical Drive Information]
Drive Model: SanDisk Dual Drive USB Device
Drive Serial Number: 4C531001511021107212
Drive Interface Type: USB
Removable drive: True
Source data size: 29952 MB
Sector count: 61341696
[Computed Hashes]
MD5 checksum: 7dc9b824177b76c56f5c45040e9d7dfb
SHA1 checksum: 47a502d6652619ad618d620493f4f29aeb1ef4e8
Image Information:
Acquisition started: Fri Apr 15 20:27:21 2022
Acquisition finished: Fri Apr 15 21:12:56 2022
Segment list:
D:\Prax 3\Image created from physical drive.afd
Image Verification Results:
Verification started: Fri Apr 15 21:12:56 2022
Verification finished: Fri Apr 15 21:27:58 2022
MD5 checksum: 7dc9b824177b76c56f5c45040e9d7dfb : verified
SHA1 checksum: 47a502d6652619ad618d620493f4f29aeb1ef4e8 : ve
OK

Practical No 4

Aim: - Exploring Wireshark

Using Log Capturing and Analysis tools

Practical No 4

Aim: - Exploring Wireshark

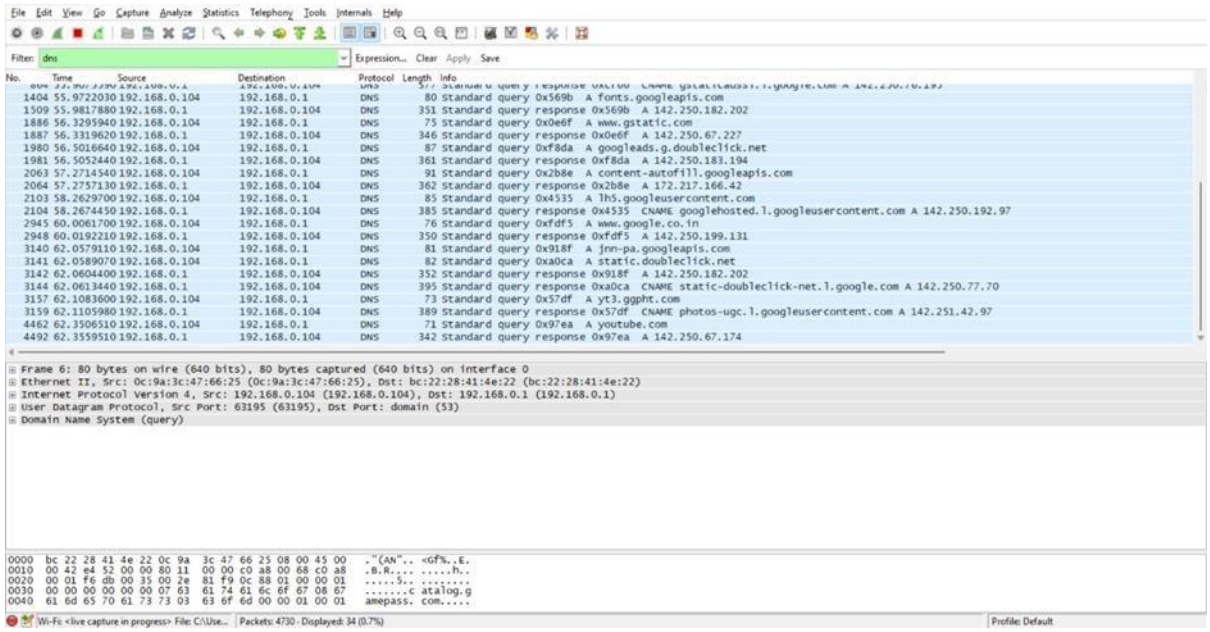
Using Log Capturing and Analysis tools

Wireshark is a network packet analyzer that intercepts, captures and logs information about packets passing through a network interface. This is useful for analyzing network problems, detecting network intrusions, network misuse, and other security problems, monitor usage and gather statistics, and many other applications.

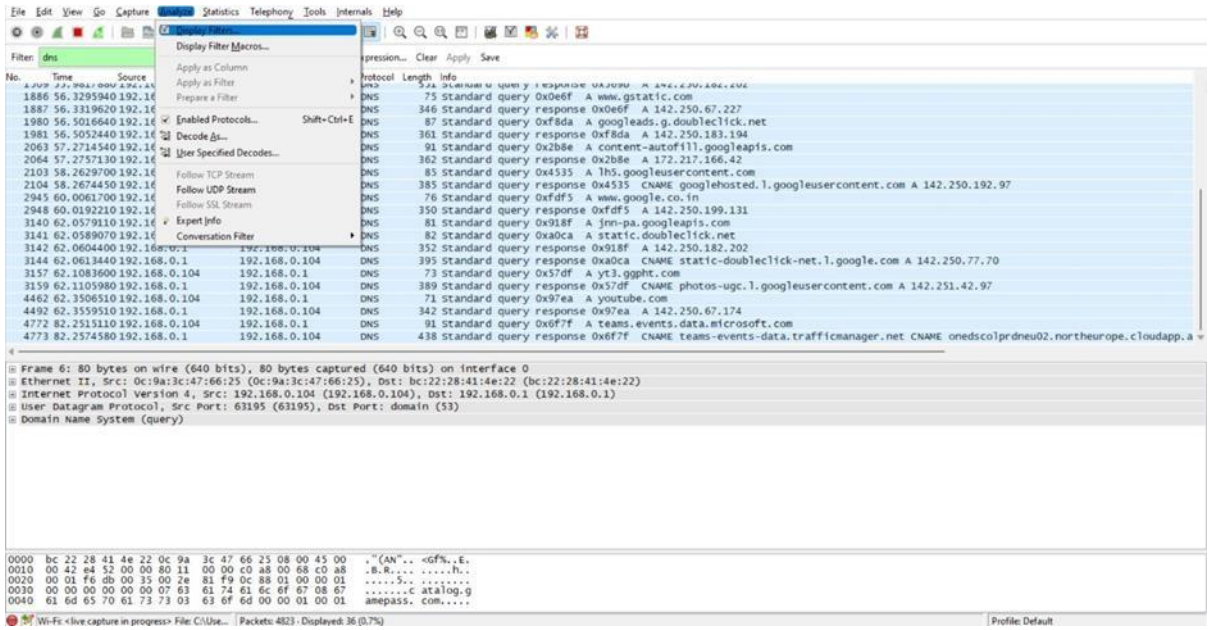
Filtering Packets

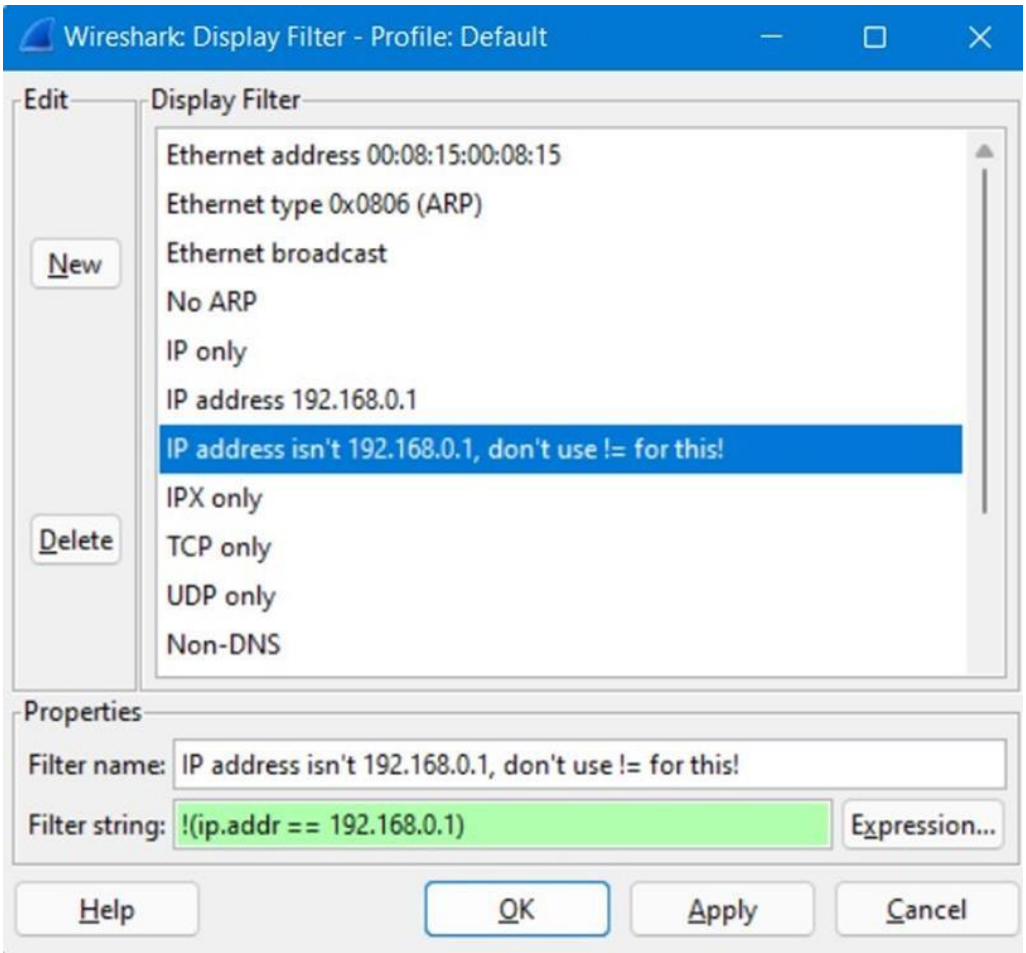
If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the traffic. Still, you'll likely have a large amount of packets to sift through. That's where Wireshark's filters come in.

The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type "dns" and you'll see only DNS packets. When you start typing, Wireshark will help you autocomplete your filter.

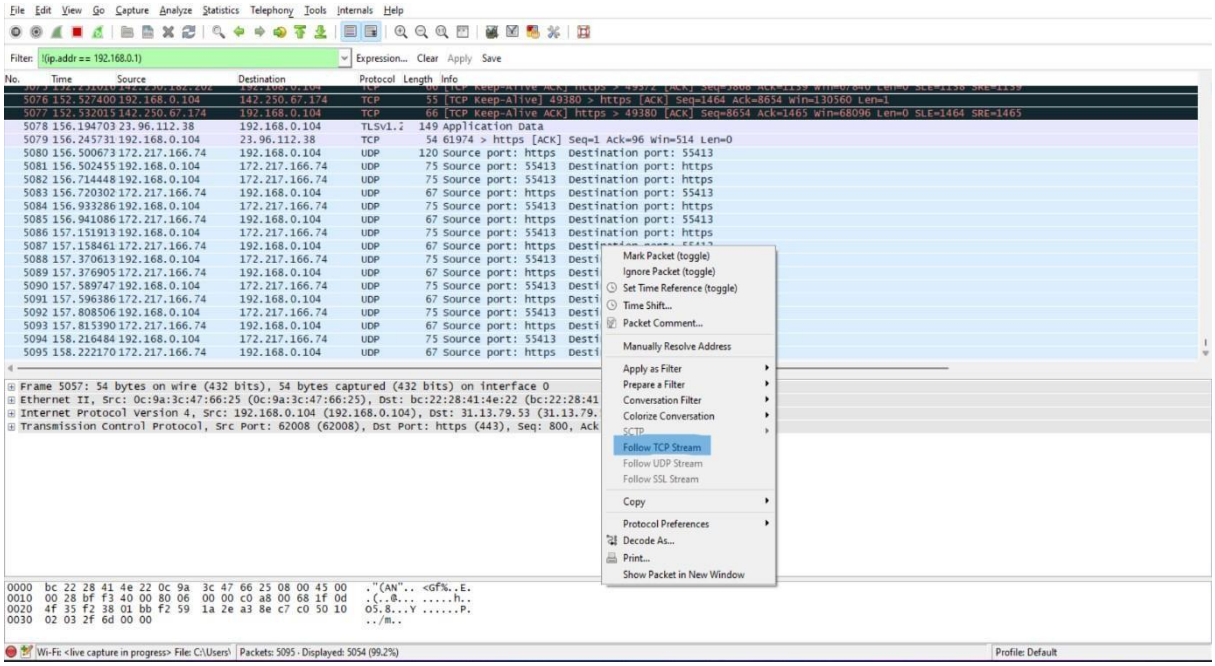


You can also click the Analyze menu and select Display Filters to create a new filter.

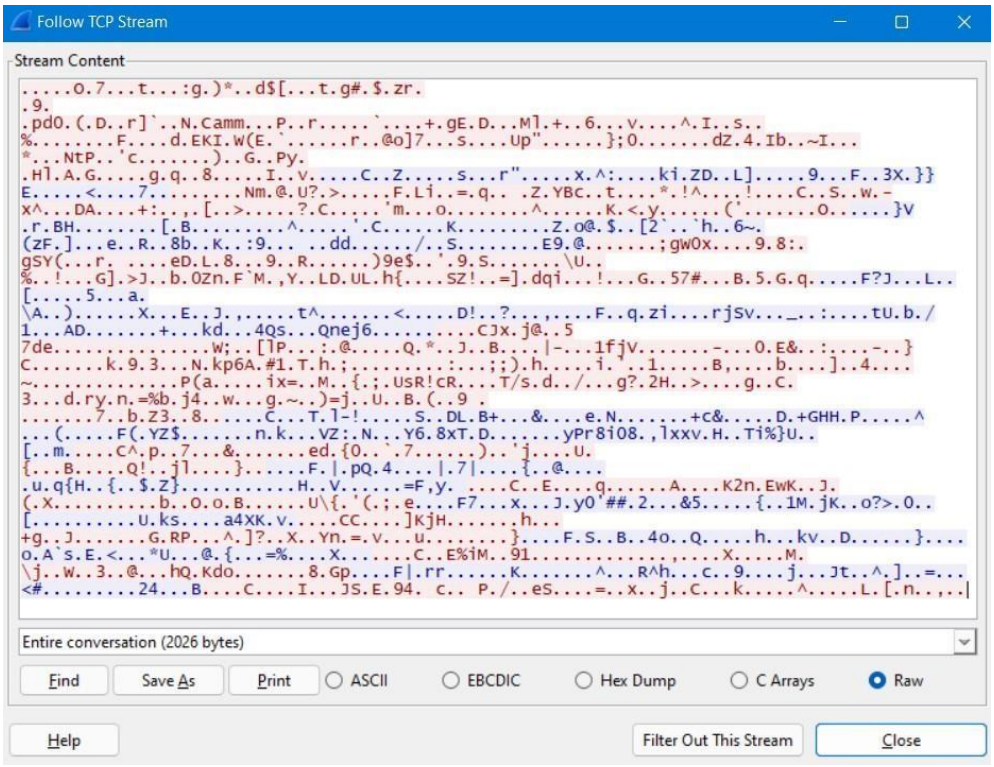

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Display Filters...
Display Filter Macros...
Apply as Column
Apply as Filter
Prepare a Filter
Enabled Protocols... Shift+Ctrl+E
Decode As...
User Specified Decodes...
Follow TCP Stream
Follow UDP Stream
Follow SSL Stream
Expert Info
Conversation Filter
Filter: dns
Frame 6: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface 0
Ethernet II, Src: 0c:9a:3c:47:66:25 (0c:9a:3c:47:66:25), Dst: bc:22:28:41:4e:22 (bc:22:28:41:4e:22)
Internet Protocol Version 4, Src: 192.168.0.104 (192.168.0.104), Dst: 192.168.0.1 (192.168.0.1)
User Datagram Protocol, Src Port: 63195 (63195), Dst Port: domain (53)
Domain Name System (query)


Wireshark: Display Filter - Profile: Default
Edit
Display Filter
New
Delete
Ethernet address 00:08:15:00:08:15
Ethernet type 0x0806 (ARP)
Ethernet broadcast
No ARP
IP only
IP address 192.168.0.1
IP address isn't 192.168.0.1, don't use != for this!
IPX only
TCP only
UDP only
Non-DNS
Properties
Filter name: IP address isn't 192.168.0.1, don't use != for this!
Filter string: !(ip.addr == 192.168.0.1)
Expression...
Help
OK
Apply
Cancel

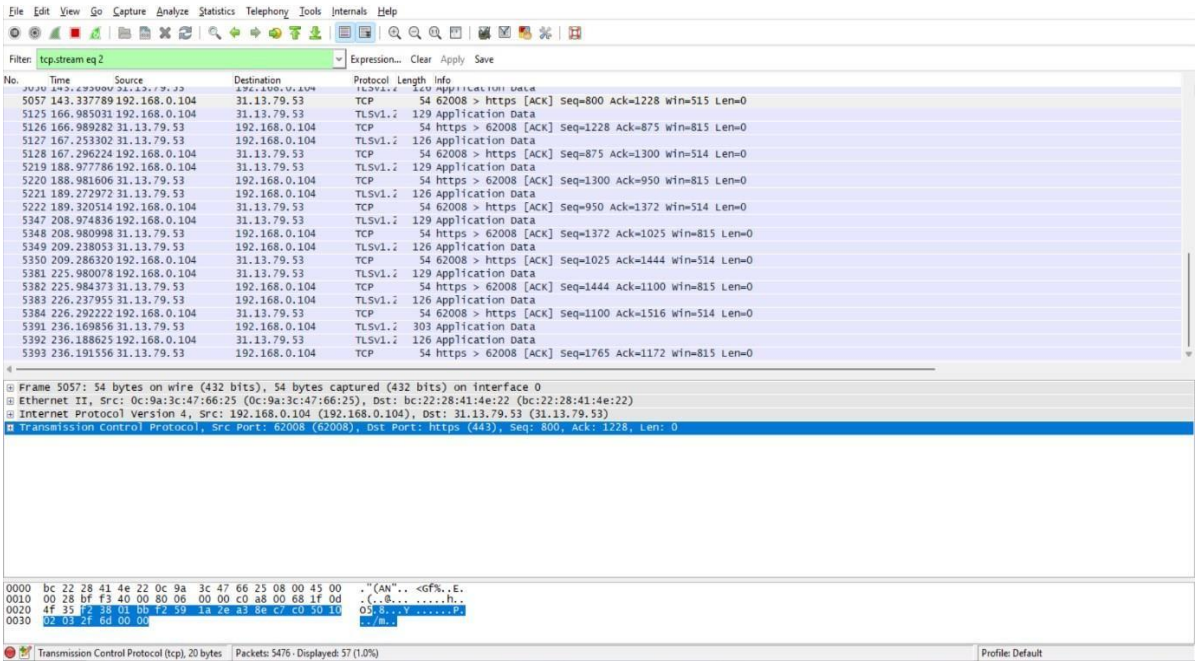
Another interesting thing you can do is right-click a packet and select Follow TCP Stream.

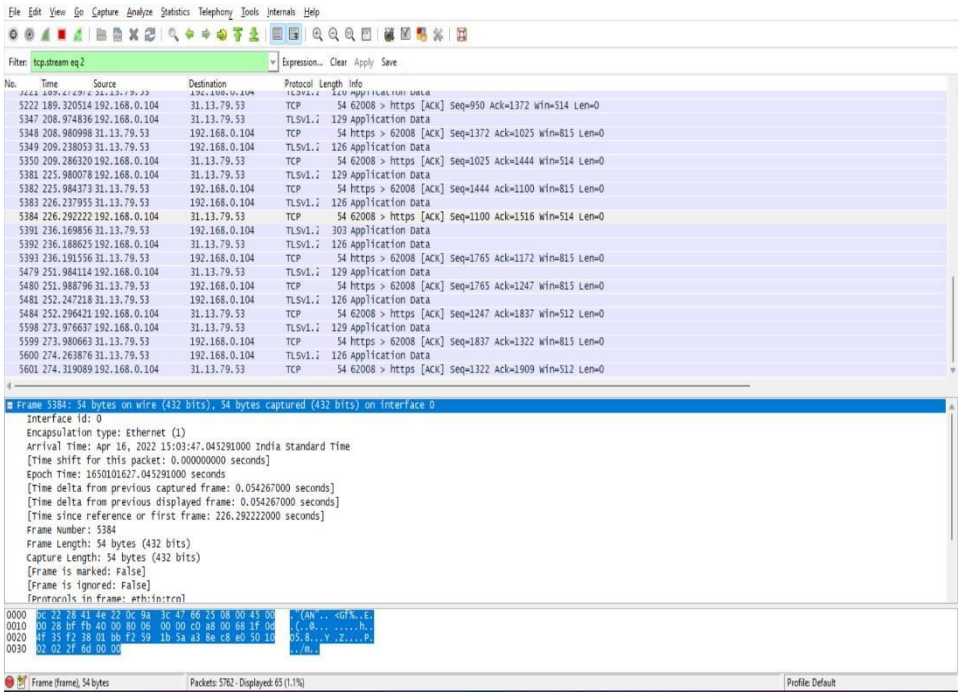


You'll see the full conversation between the client and the server.



Close the window and you'll find a filter has been applied automatically — Wireshark is showing you the packets that make up the conversation.

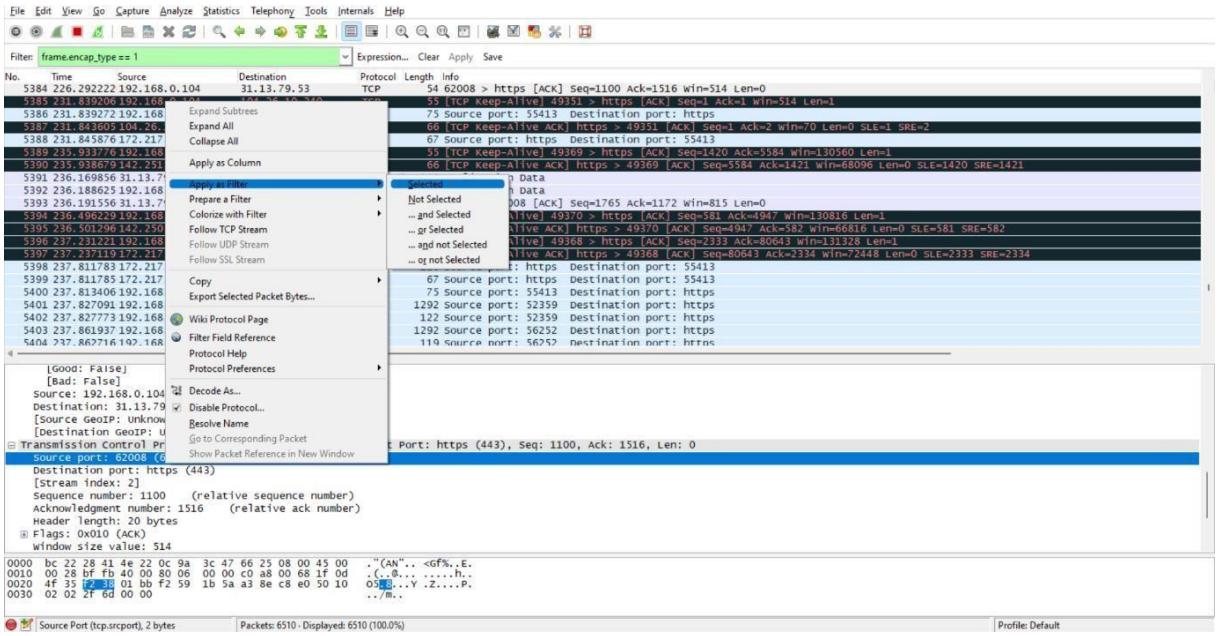


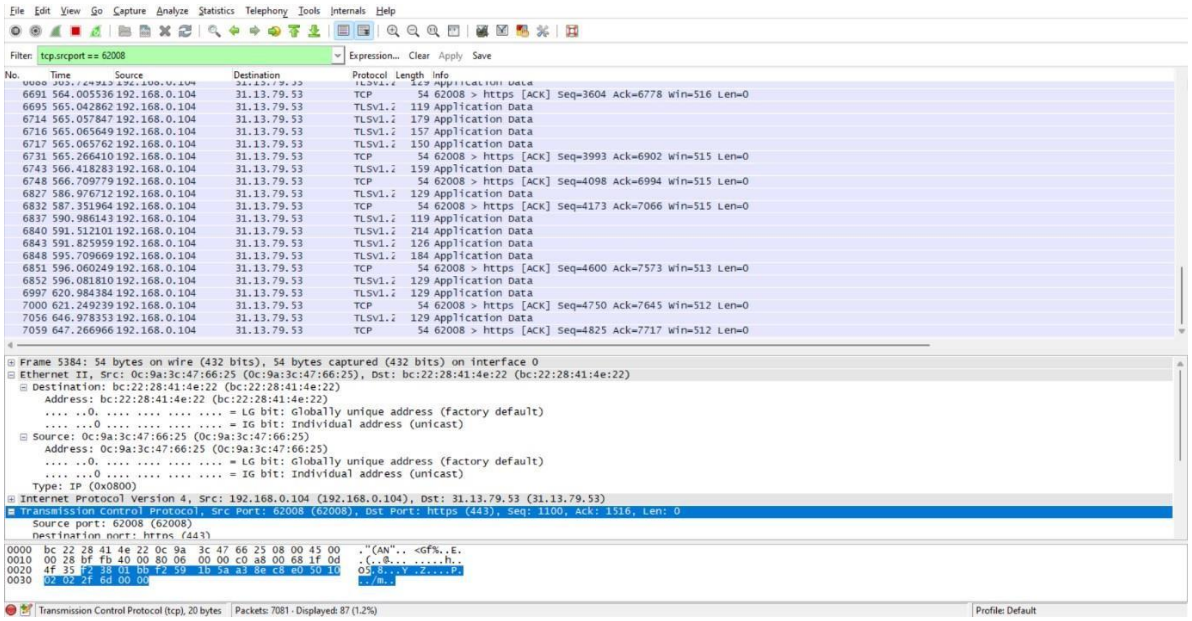


Inspecting Packets

Click a packet to select it and you can dig down to view its details

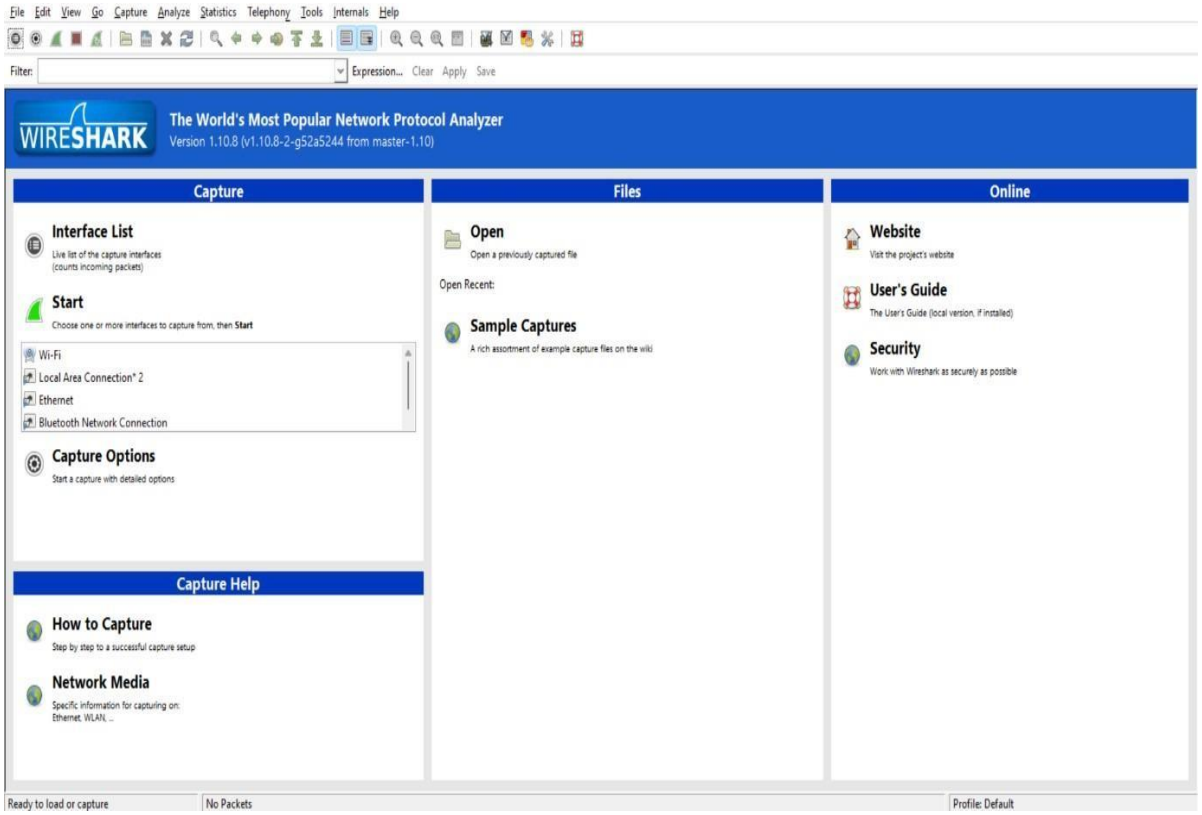
You can also create filters from here — just right-click one of the details and use the Apply as Filter submenu to create a filter based on it.


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: frame.encap_type == 1
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
5384 226.292222 192.168.0.104 31.13.79.53 TCP 54 62008 > https [ACK] Seq=1100 Ack=1516 Win=514 Len=0
5385 231.839206 192.168
5386 231.839272 192.168
5387 231.843605 104.26.
5388 231.845876 172.217
5389 235.933776 192.168
5390 235.938679 142.251
5391 236.169856 31.13.7
5392 236.188625 192.168.
5393 236.191556 31.13.7
5394 236.496229 192.168
5395 236.501296 142.250
5396 237.231221 192.168
5397 237.237119 172.217
5398 237.811783 172.217
5399 237.811785 172.217
5400 237.813406 192.168
5401 237.827091 192.168
5402 237.827773 192.168
5403 237.861937 192.168
5404 237.862716 192.168
Expand Subtrees
Expand All
Collapse All
Apply as Column
Apply as Filter
Prepare a Filter
Colorize with Filter
Follow TCP Stream
Follow UDP Stream
Follow SSL Stream
Copy
Export Selected Packet Bytes...
Wiki Protocol Page
Filter Field Reference
Protocol Help
Protocol Preferences
Decode As...
Disable Protocol...
Resolve Name
Go to Corresponding Packet
Show Packet Reference in New Window
Selected
Not Selected
... and Selected
... or Selected
... and not Selected
... or not Selected
[Good: False]
[Bad: False]
Source: 192.168.0.104
Destination: 31.13.79
[Source GeoIP: Unknow
[Destination GeoIP: U
Transmission Control Pr
Source port: 62008 (6
Destination port: https (443)
[Stream index: 2]
Sequence number: 1100 (relative sequence number)
Acknowledgment number: 1516 (relative ack number)
Header length: 20 bytes
Flags: 0x010 (ACK)
Window size value: 514
0000 bc 22 28 41 4e 22 0c 9a 3c 47 66 25 08 00 45 00
0010 00 28 bf fb 40 00 80 06 00 00 c0 a8 00 68 1f 0d
0020 4f 35 f2 38 01 bb f2 59 1b 5a a3 8e c8 e0 50 10
0030 02 02 2f 6d 00 00
Source Port (tcp.srcport), 2 bytes
Packets: 6510 · Displayed: 6510 (100.0%)
Profile: Default


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: tcp.srcport == 62008
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
6691 564.005536 192.168.0.104 31.13.79.53 TCP 54 62008 > https [ACK] Seq=3604 Ack=6778 Win=516 Len=0
6695 565.042862 192.168.0.104 31.13.79.53 TLSv1.2 119 Application Data
6714 565.057847 192.168.0.104 31.13.79.53 TLSv1.2 179 Application Data
6716 565.065649 192.168.0.104 31.13.79.53 TLSv1.2 157 Application Data
6717 565.065762 192.168.0.104 31.13.79.53 TLSv1.2 150 Application Data
6731 565.266410 192.168.0.104 31.13.79.53 TCP 54 62008 > https [ACK] Seq=3993 Ack=6902 Win=515 Len=0
6743 566.418283 192.168.0.104 31.13.79.53 TLSv1.2 159 Application Data
6748 566.709779 192.168.0.104 31.13.79.53 TCP 54 62008 > https [ACK] Seq=4098 Ack=6994 Win=515 Len=0
6827 586.976712 192.168.0.104 31.13.79.53 TLSv1.2 129 Application Data
6832 587.351964 192.168.0.104 31.13.79.53 TCP 54 62008 > https [ACK] Seq=4173 Ack=7066 Win=515 Len=0
6837 590.986143 192.168.0.104 31.13.79.53 TLSv1.2 119 Application Data
6840 591.512101 192.168.0.104 31.13.79.53 TLSv1.2 214 Application Data
6843 591.825959 192.168.0.104 31.13.79.53 TLSv1.2 126 Application Data
6848 595.709669 192.168.0.104 31.13.79.53 TLSv1.2 184 Application Data
6851 596.060249 192.168.0.104 31.13.79.53 TCP 54 62008 > https [ACK] Seq=4600 Ack=7573 Win=513 Len=0
6852 596.081810 192.168.0.104 31.13.79.53 TLSv1.2 129 Application Data
6997 620.984384 192.168.0.104 31.13.79.53 TLSv1.2 129 Application Data
7000 621.249239 192.168.0.104 31.13.79.53 TCP 54 62008 > https [ACK] Seq=4750 Ack=7645 Win=512 Len=0
7056 646.978353 192.168.0.104 31.13.79.53 TLSv1.2 129 Application Data
7059 647.266966 192.168.0.104 31.13.79.53 TCP 54 62008 > https [ACK] Seq=4825 Ack=7717 Win=512 Len=0
Frame 5384: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
Ethernet II, Src: 0c:9a:3c:47:66:25 (0c:9a:3c:47:66:25), Dst: bc:22:28:41:4e:22 (bc:22:28:41:4e:22)
Destination: bc:22:28:41:4e:22 (bc:22:28:41:4e:22)
Address: bc:22:28:41:4e:22 (bc:22:28:41:4e:22)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: 0c:9a:3c:47:66:25 (0c:9a:3c:47:66:25)
Address: 0c:9a:3c:47:66:25 (0c:9a:3c:47:66:25)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IP (0x0800)
Internet Protocol Version 4, Src: 192.168.0.104 (192.168.0.104), Dst: 31.13.79.53 (31.13.79.53)
Transmission Control Protocol, Src Port: 62008 (62008), Dst Port: https (443), Seq: 1100, Ack: 1516, Len: 0
Source port: 62008 (62008)
Destination port: https (443)
0000 bc 22 28 41 4e 22 0c 9a 3c 47 66 25 08 00 45 00
0010 00 28 bf fb 40 00 80 06 00 00 c0 a8 00 68 1f 0d
0020 4f 35 f2 38 01 bb f2 59 1b 5a a3 8e c8 e0 50 10
0030 02 02 2f 6d 00 00
Transmission Control Protocol (tcp), 20 bytes
Packets: 7081 · Displayed: 87 (1.2%)
Profile: Default

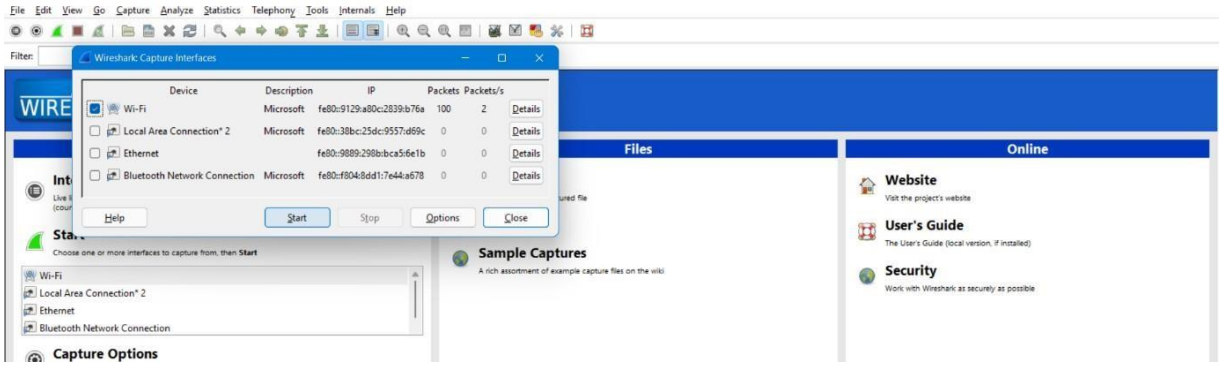
Using Traffic Capturing and Analysis tools

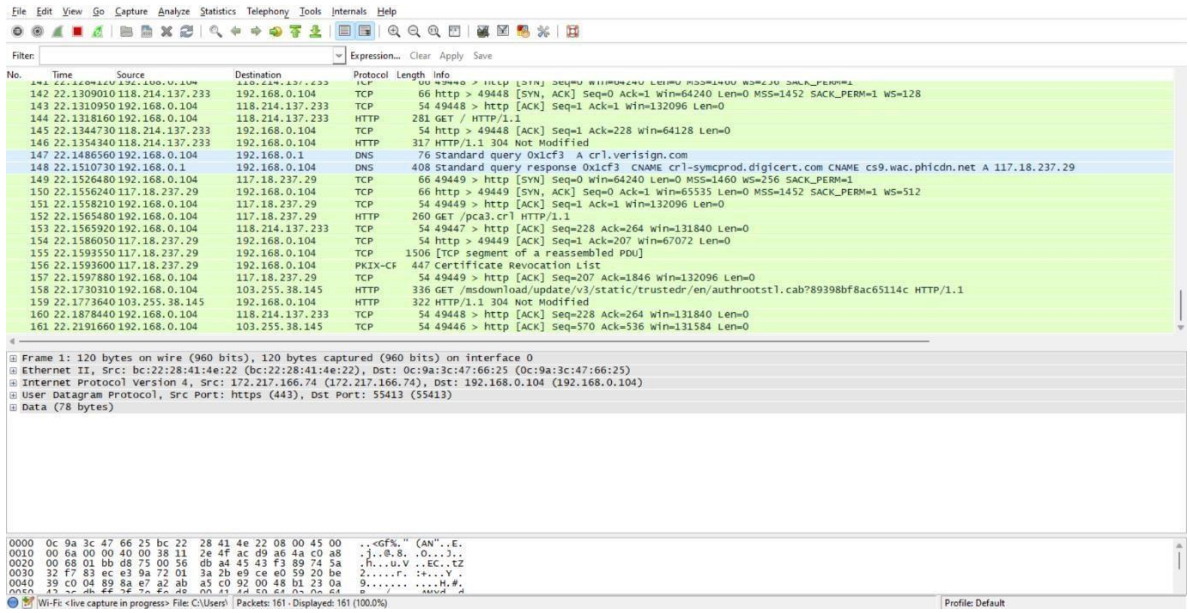
Aim: Exploring Wireshark



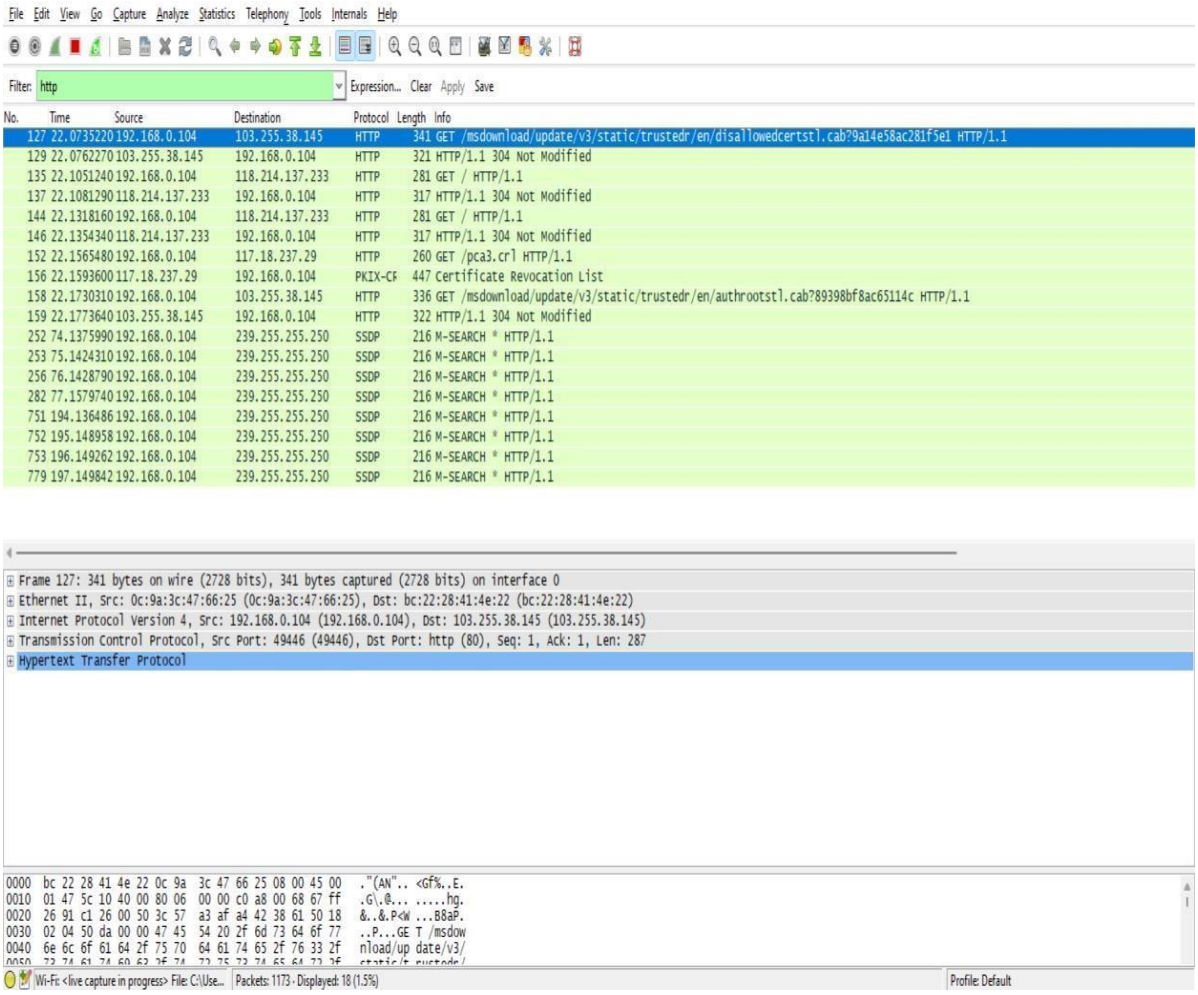
Step 2: On menu bar select Capture. Select interfaces.

Step 3: Select Once you click on start, then Wireshark starts to capture the packets on that interface.



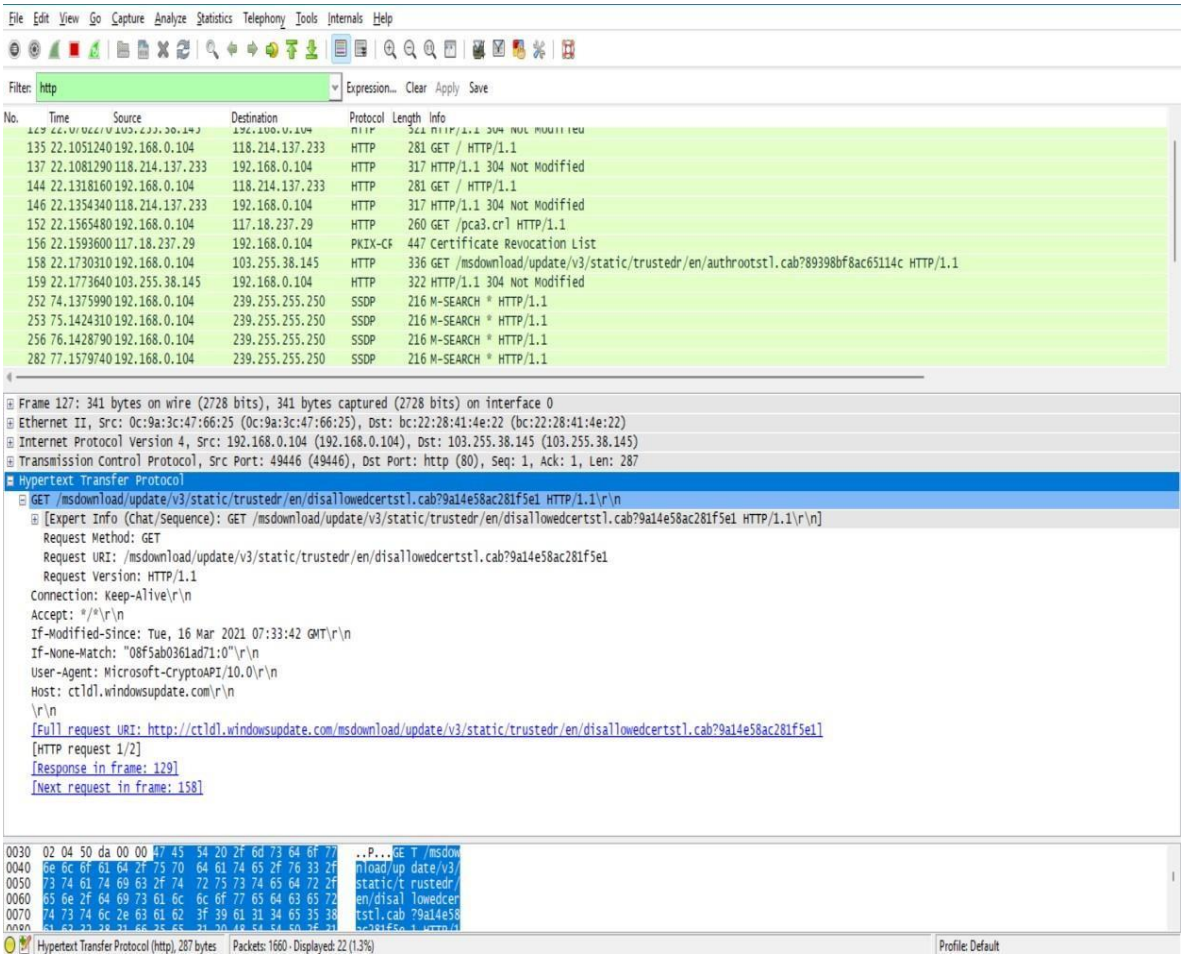


Step 4: Filter packets with HTTP protocol.



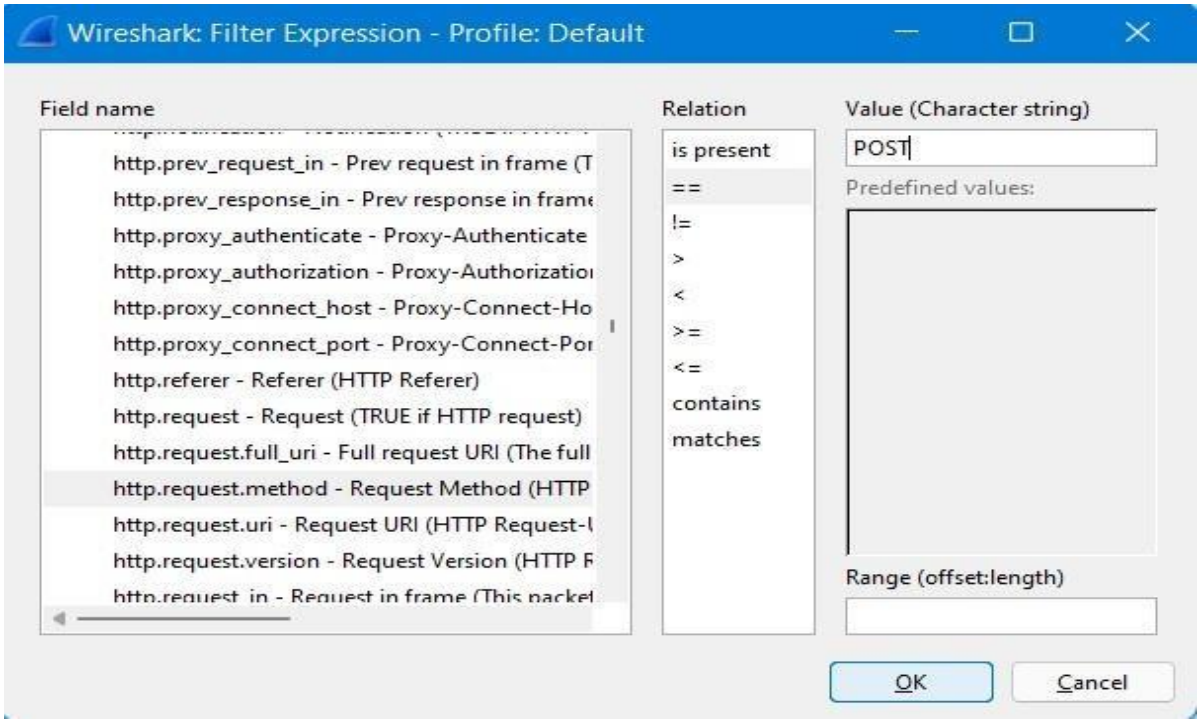
Step 5: A file with only text:

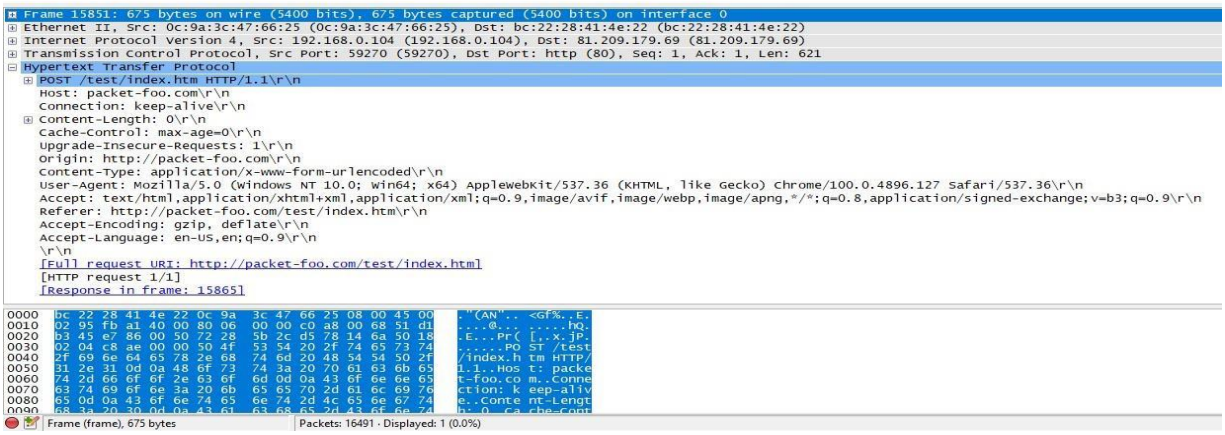
http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?9a 14e58ac281f5e1



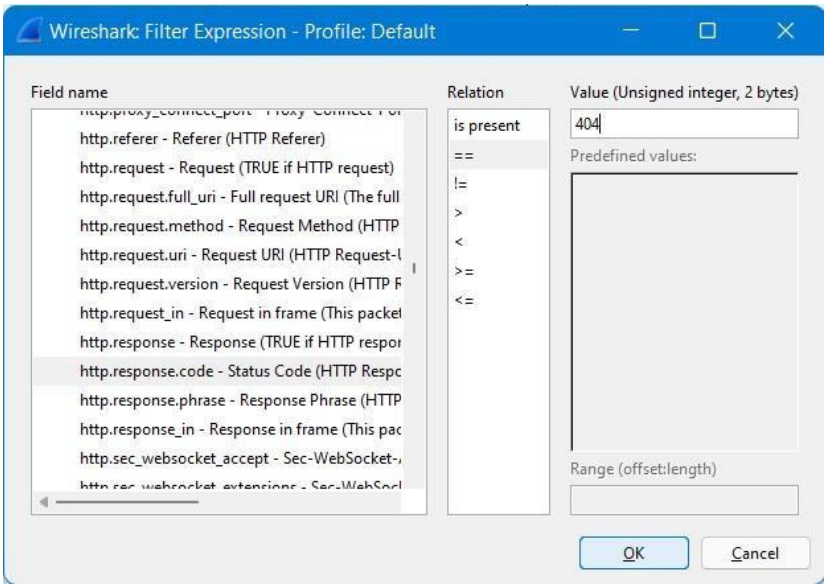
Step 6: Applying different filters using expressions.

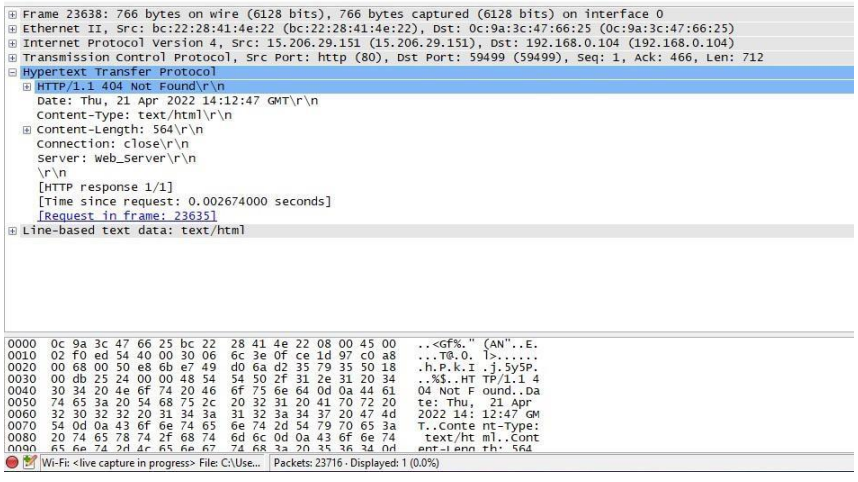
1) Filtering HTTP POST request



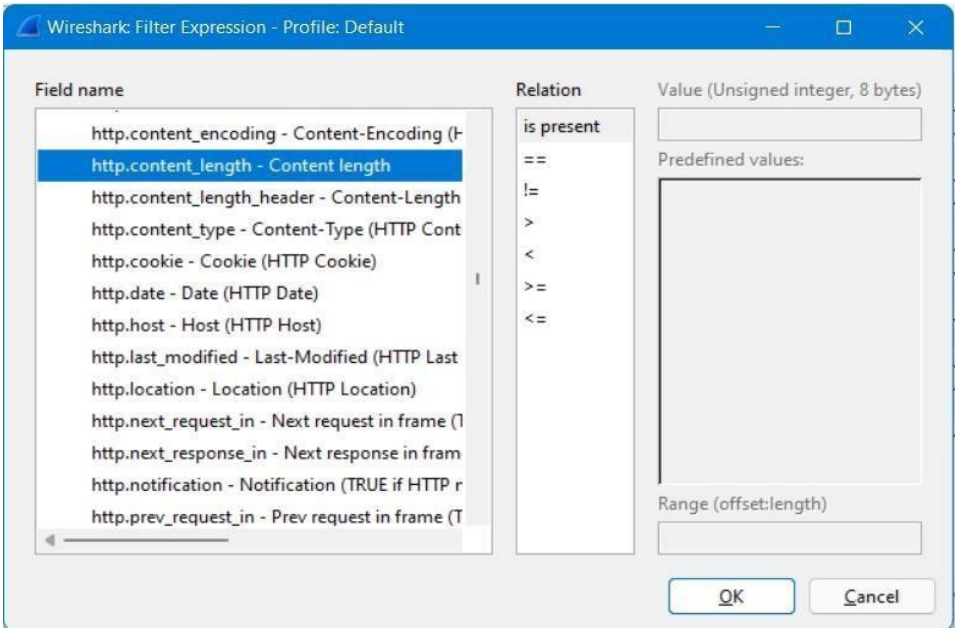


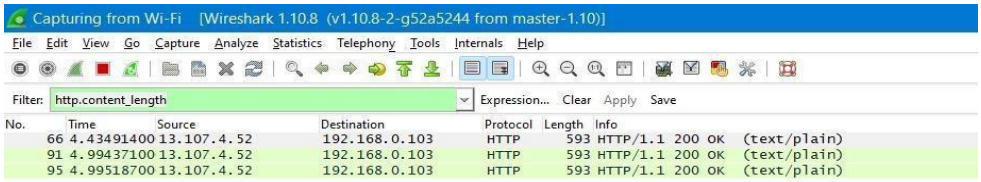
2) Filtering 404 not found error

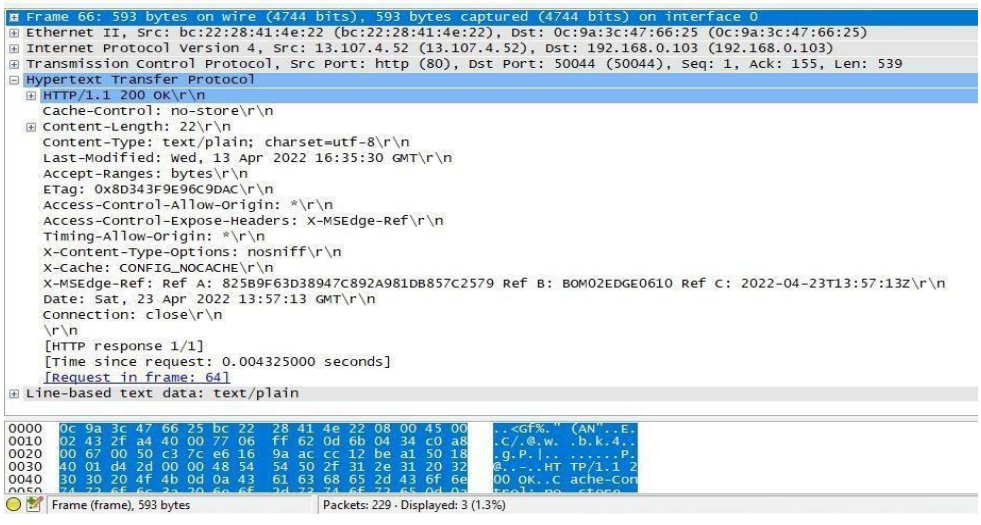




3) Filtering using HTTP Content Length







Practical No 5

Aim: - Using Data Acquisition Tools

Practical No 5

Aim: - Using Data Acquisition Tools

Tasks to be performed:

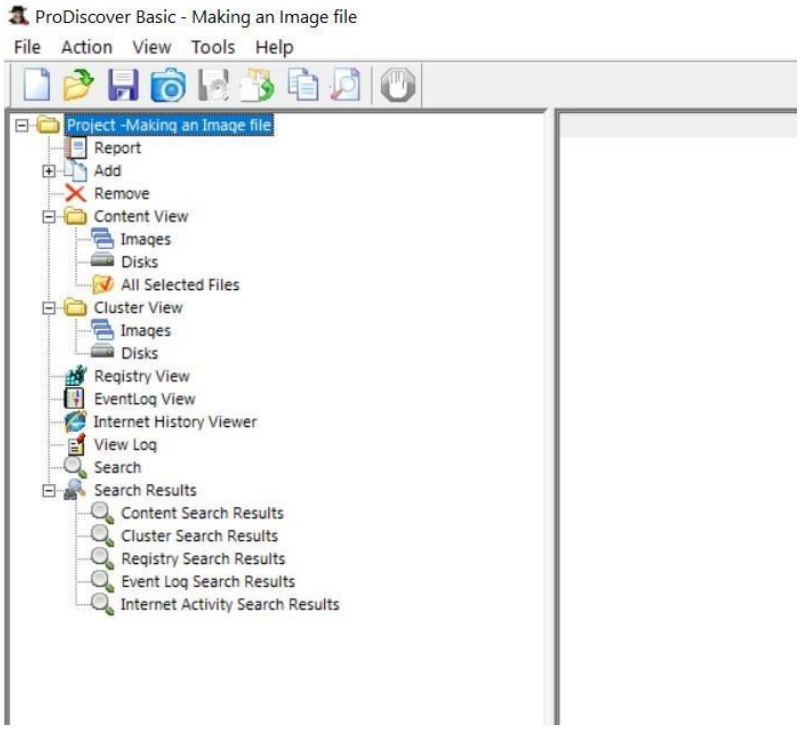
1) Creating a New Project
2) Save a project
3) Preview a directly connected evidence drive
4) Conducting Live Preview of a Remote Disk
5) Capture an image of an attached drive
6) Capturing Physical Memory
7) Add an image file to a project
8) Restore an Image to directly connected drive

Creating a New Project:

Step 1) Start ProDiscover. ProDiscover presents the launch dialog.

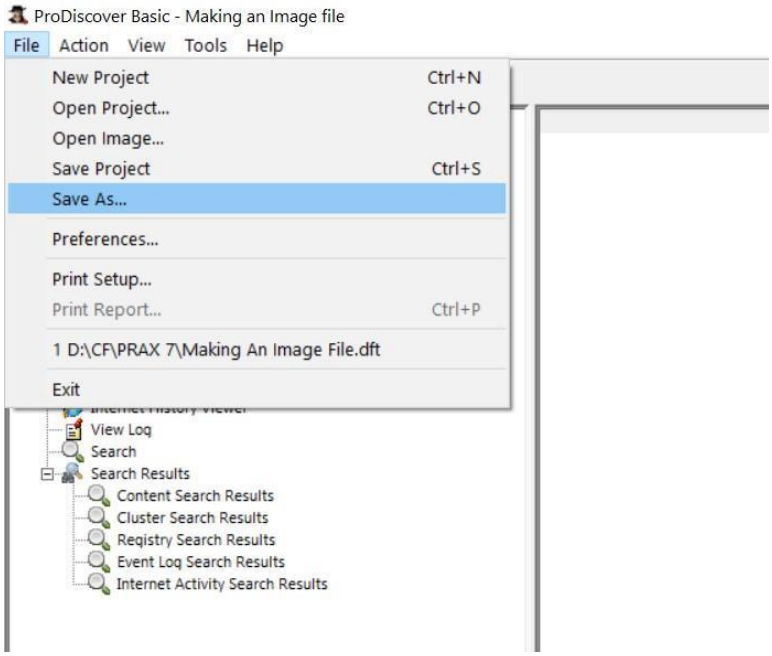
Step 2) Enter a project number, project name, and description of the project in the new project tab option, and then click the Open button.

ProDiscover will then create a project and generate a template report in the work area.

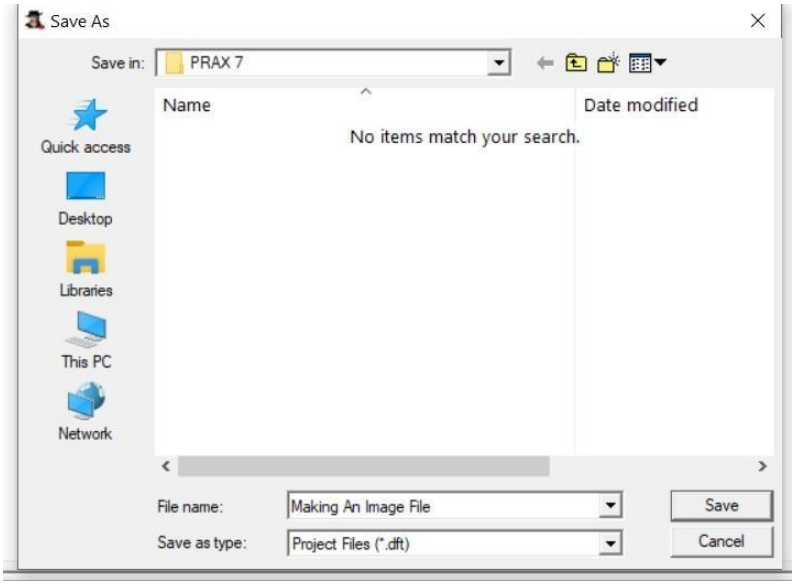


2) <u>Saving a project:</u>

1] Select save project option from the file menu, or button bar.



2] ProDiscover presents file Save As dialog if the current project has not yet been saved, otherwise the current project file will be updated without further action.



3] Select the destination path and click the Save button.

4] ProDiscover saves the project at the path specified.

3)Preview a directly connected evidence drive

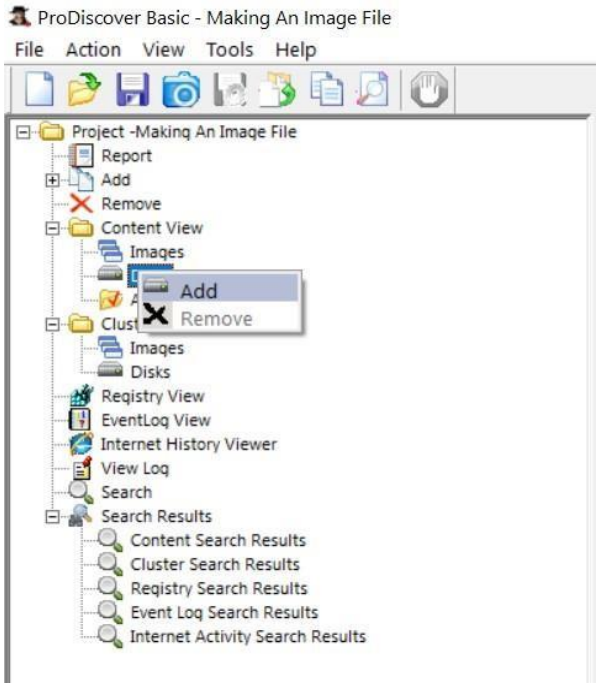
1] Launch ProDiscover.

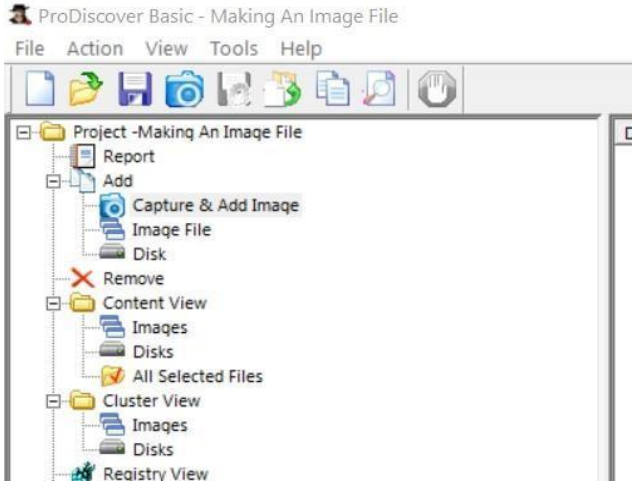
2] Select **open project** tab option.

3] Select the project file to open and click **Open** button.

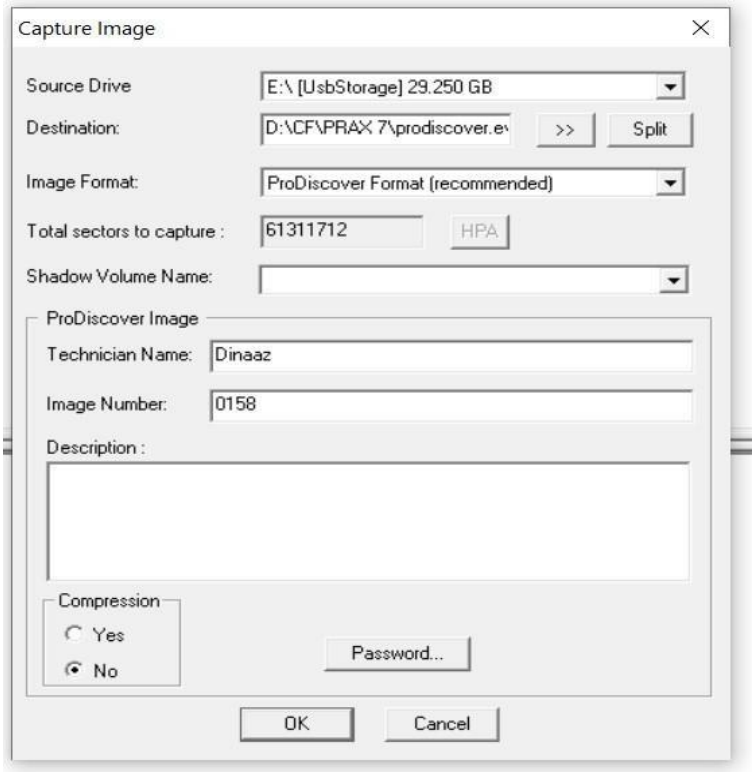
4] ProDiscover opens the project file and generates a template report in the work area.

5] Select the **Add Disk** option from the action menu, or tree-view.

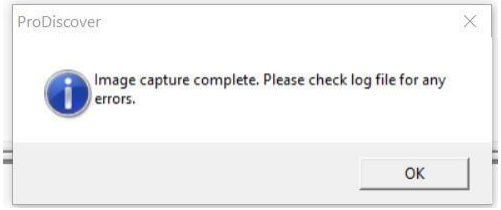




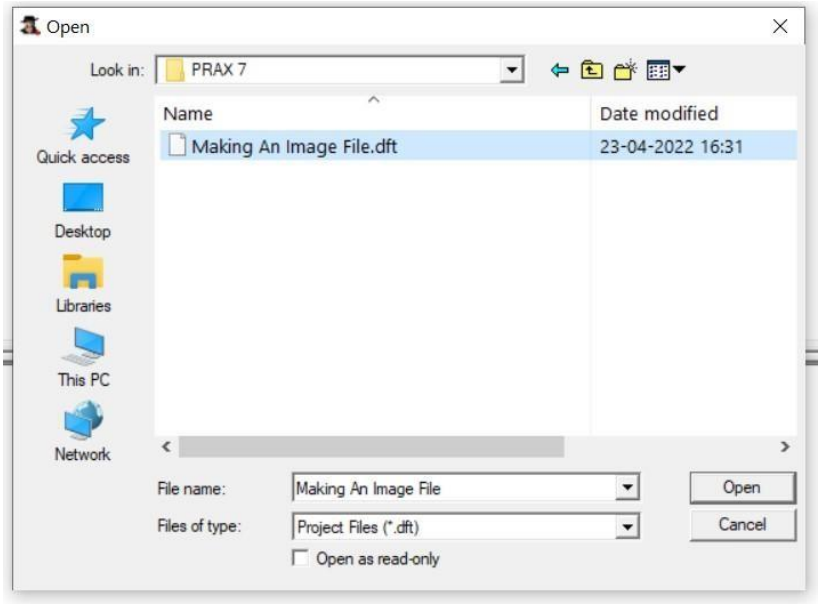
6] ProDiscover presents a dialog with all physical disk available for viewing.



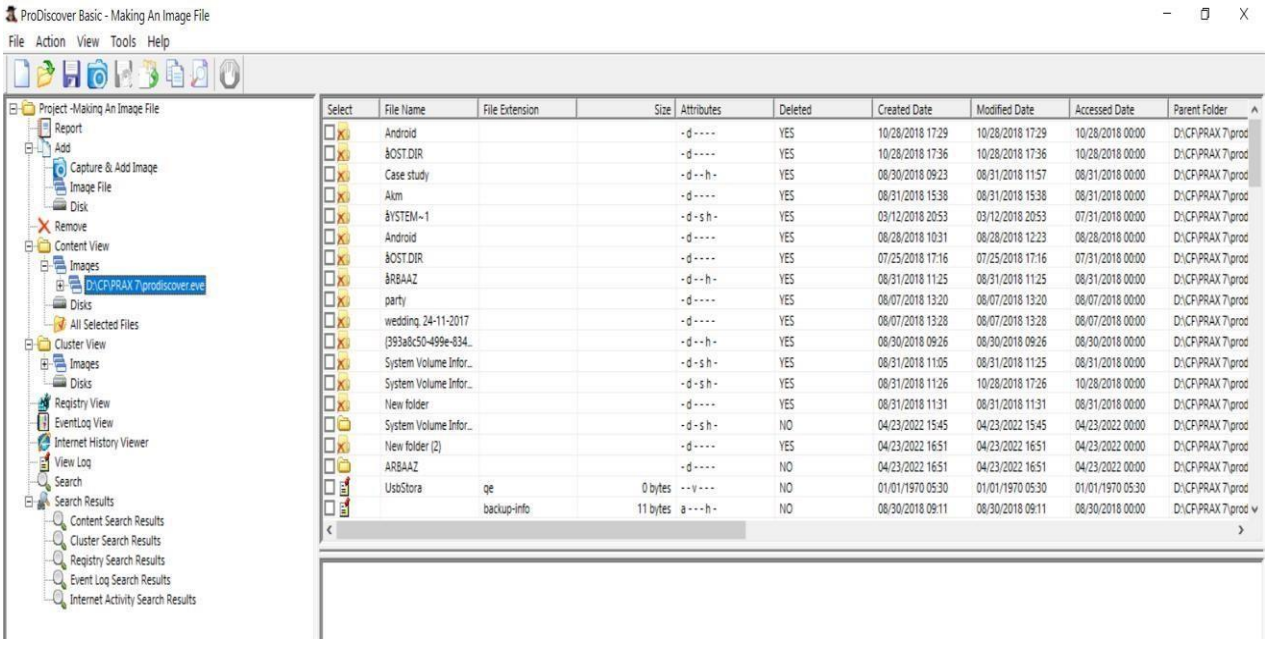
Once the image capturing is completed, click on OK



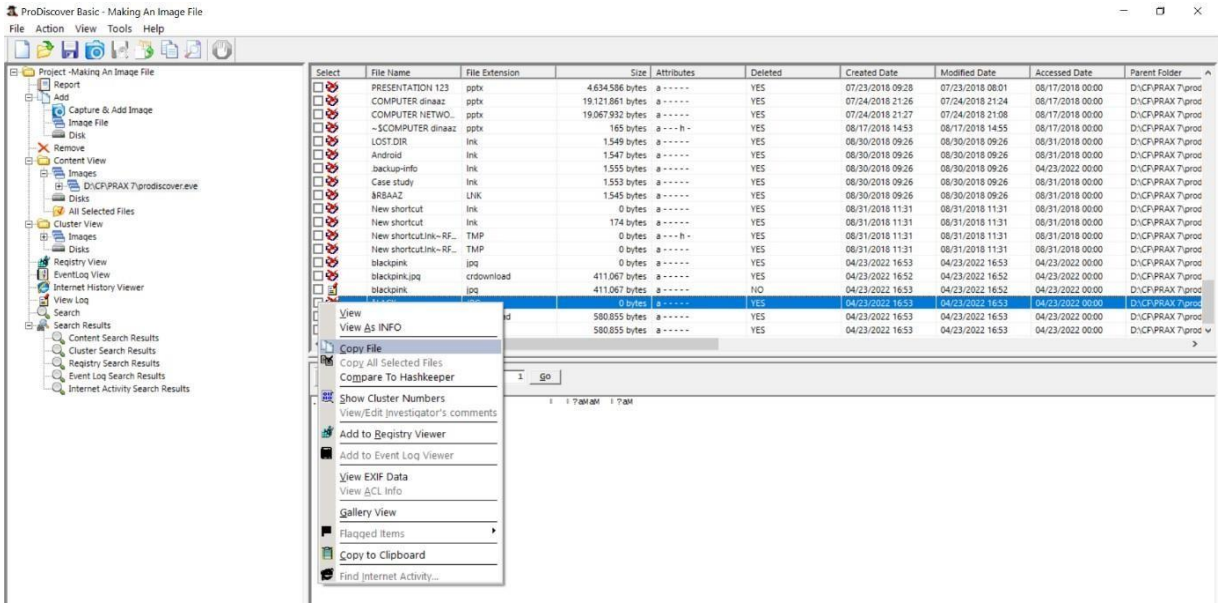
7] Under Add, click on Image File, click on the image that you created and click Open.



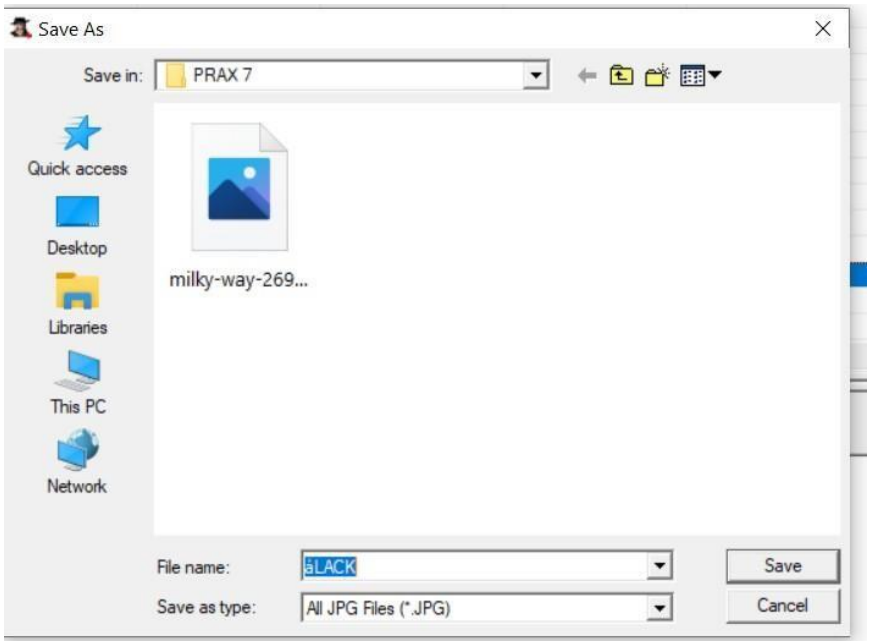
8] The image file will get added. Then under Content view, click on images and select the image.



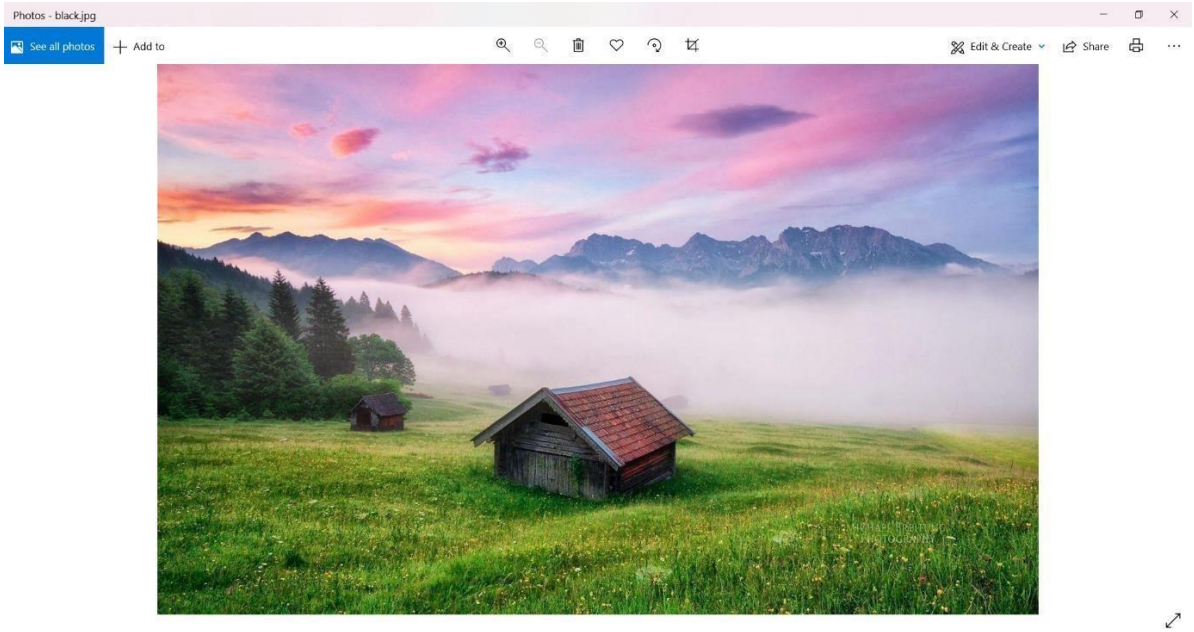
9] Right click on deleted file, either view it or copy the file to a folder.



10] Save the file**.**



11] Navigate to the folder and there you can see the deleted file. You can view the deleted file once saved in a folder.



Practical No 6

Aim: - Exploring S tools

Using Steganography tools

Practical No 6

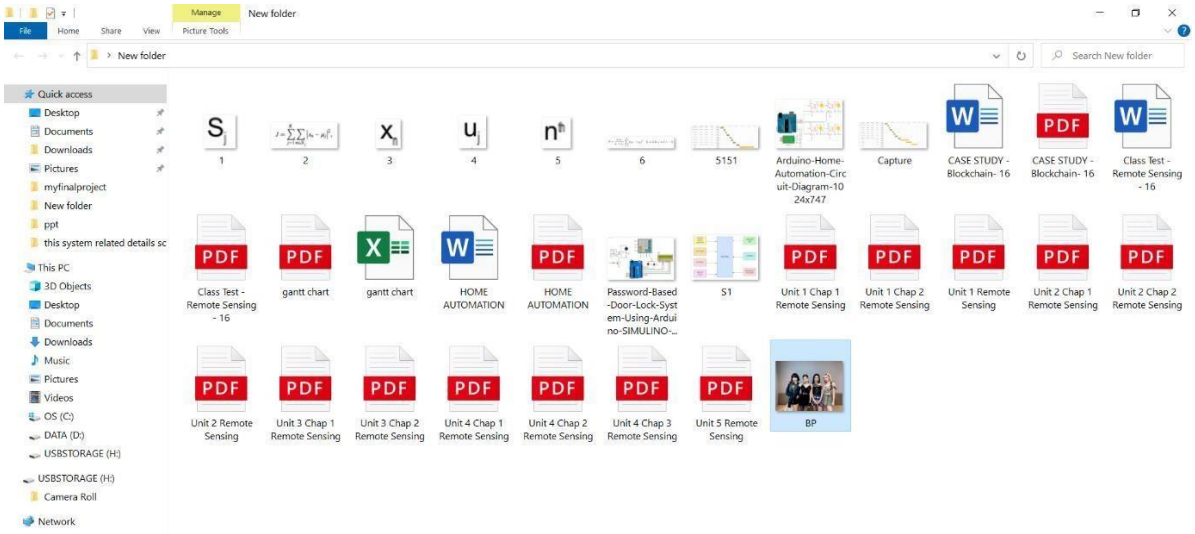
Aim: - Exploring S tools

Using Steganography tools

Following steps Show how to use freeware S-Tools utility to hide and reveal files inside pictures

Step 1) Select the S-Tools.exe file and open the steganography software tool.

Step 2) With both the working directory and the S-Tools program open minimize both windows and place side-by-side.



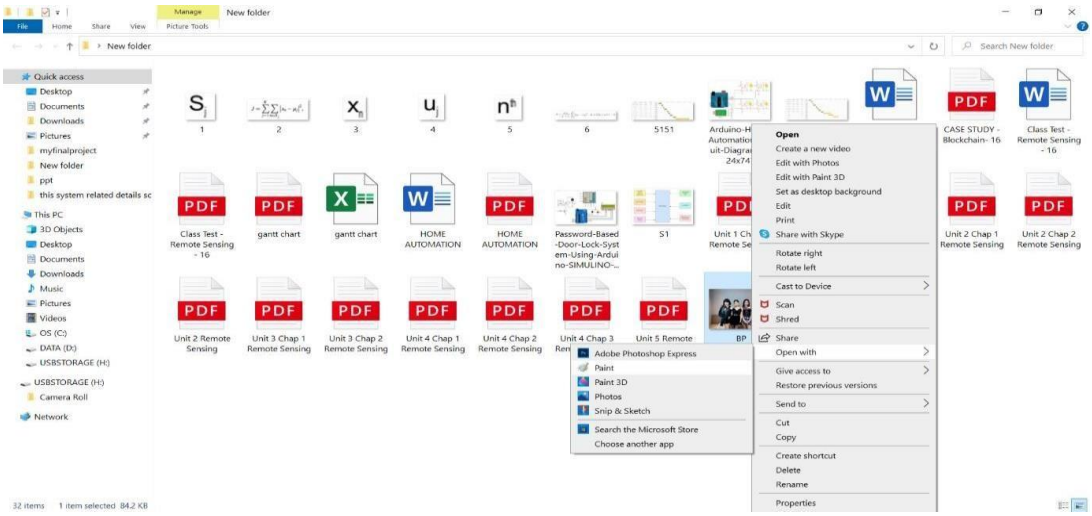
The S-Tools program is a drag and drop software. The files used to create the steganography file can be dragged from the directory into the S-Tools program.

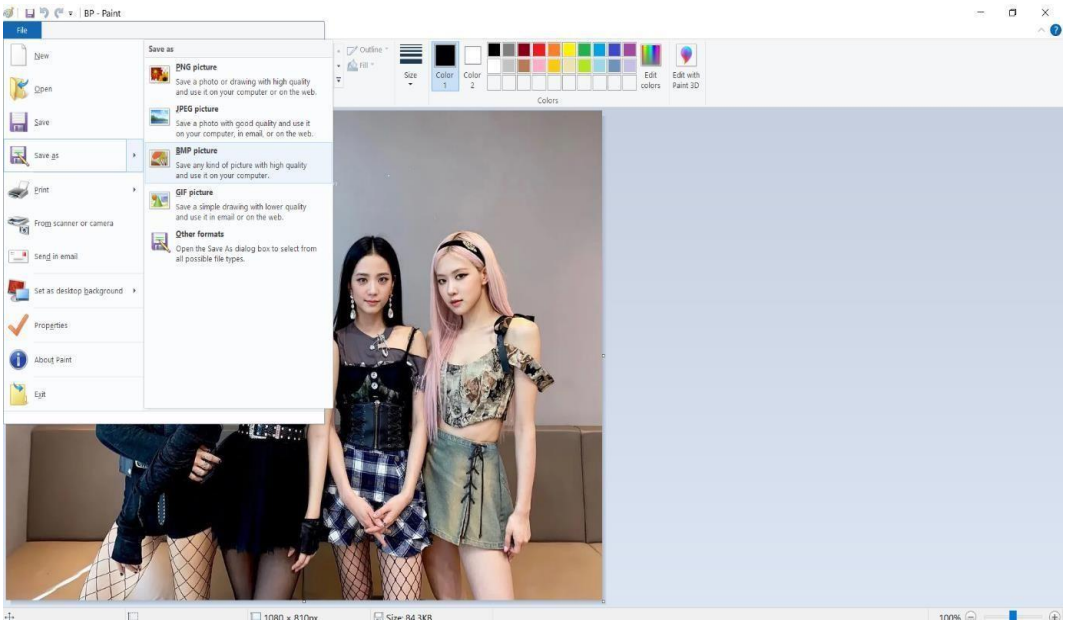
Step 3) Select the file from the directory and drag it over the S-Tools main window and release the file.

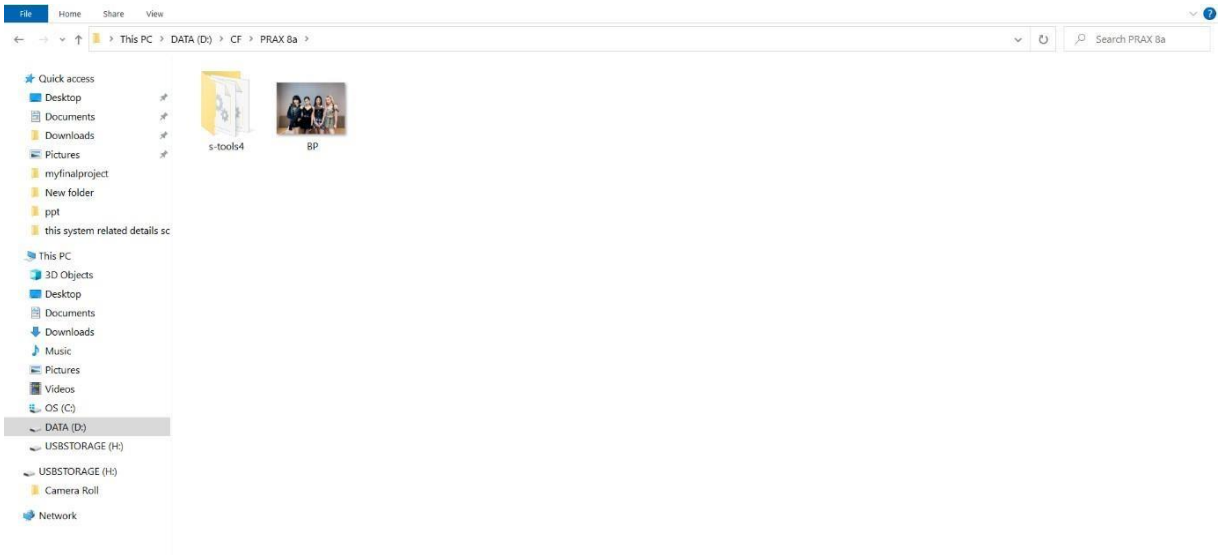
A dialogue box appears indicating that the file type is unknown. Supported file types for audio and image files are shown below:

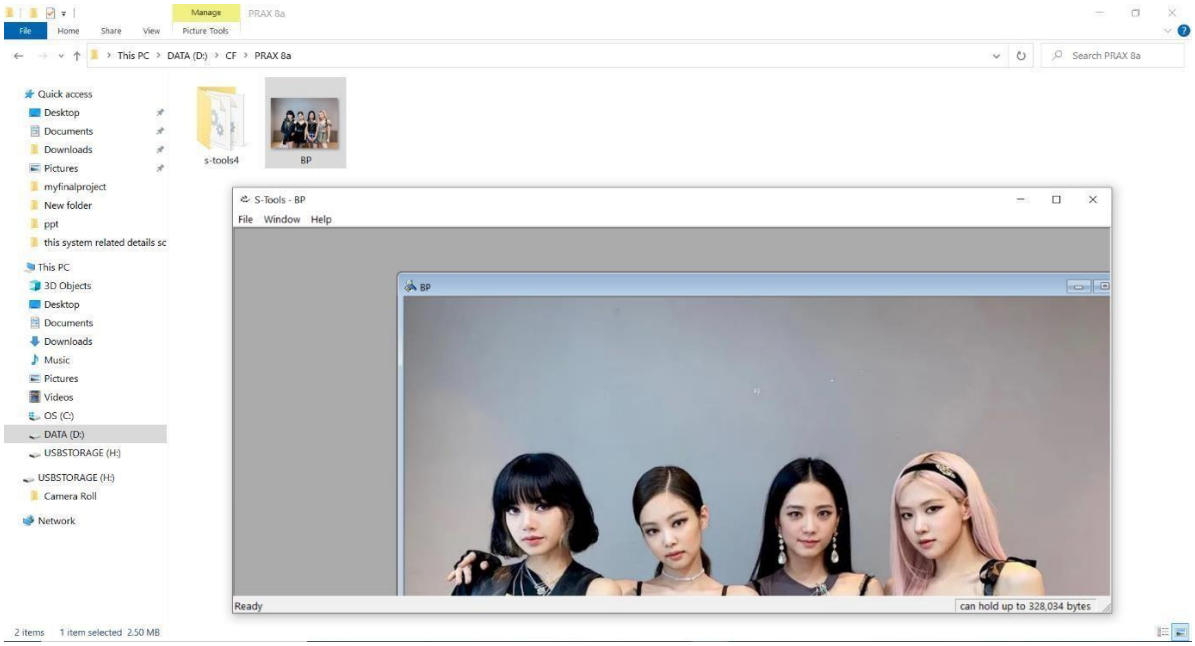
- Audio - *.wav
- Image - *.bmp and *.gif

If your image is in .jpg format, convert it to .bmp format by doing the following steps using Paint:

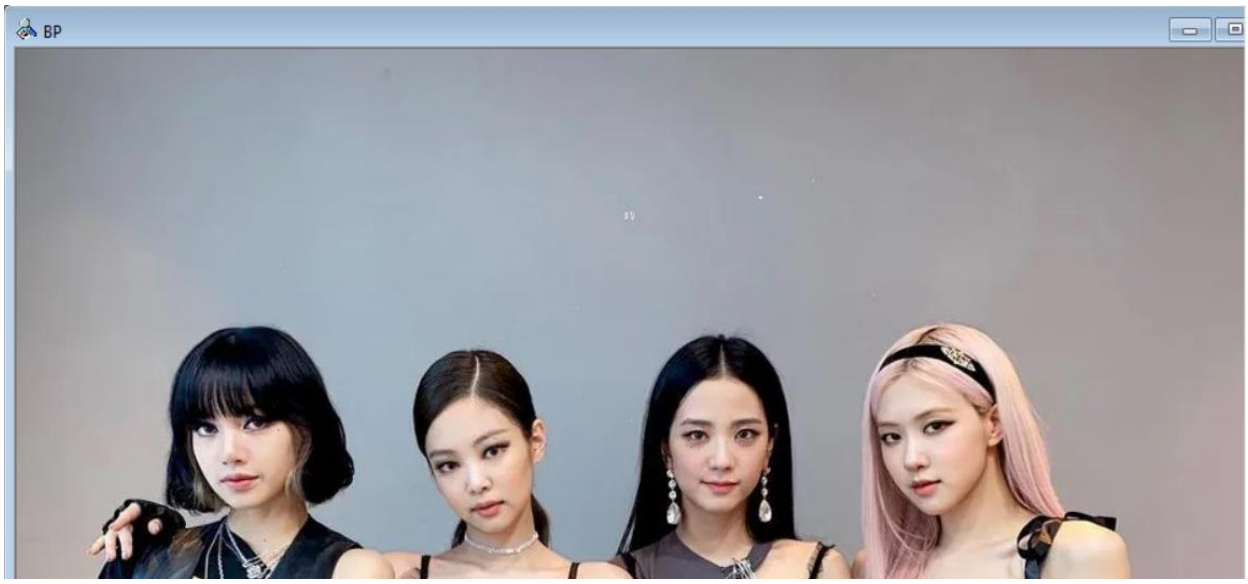




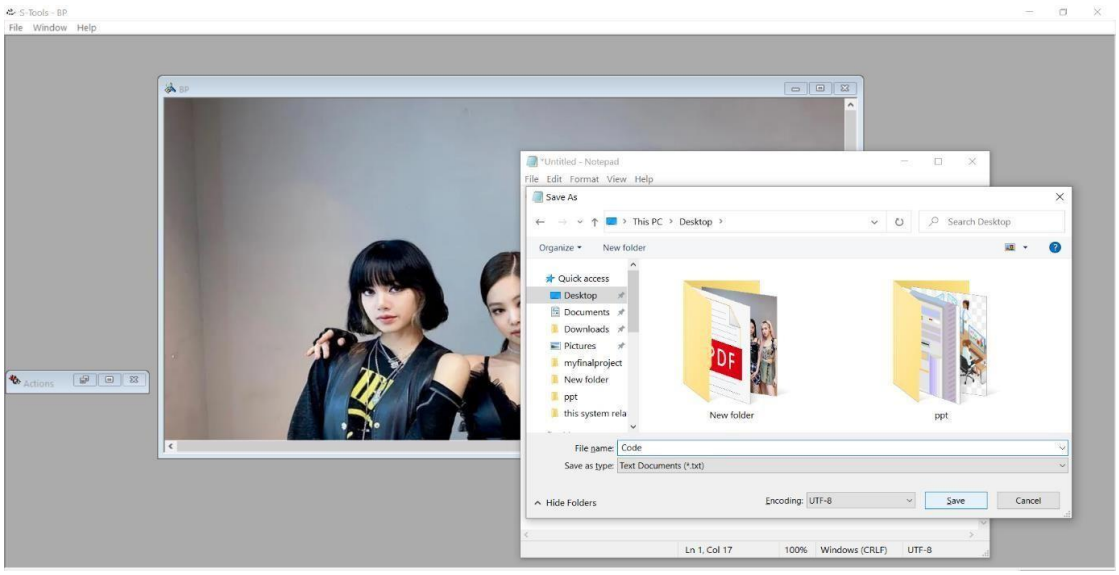

File
Home
Share
View
This PC
DATA (D:)
CF
PRAX 8a
Search PRAX 8a
Quick access
Desktop
Documents
Downloads
Pictures
myfinalproject
New folder
ppt
this system related details sc
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
OS (C:)
DATA (D:)
USBSTORAGE (H:)
USBSTORAGE (H:)
Camera Roll
Network
s-tools4
BP

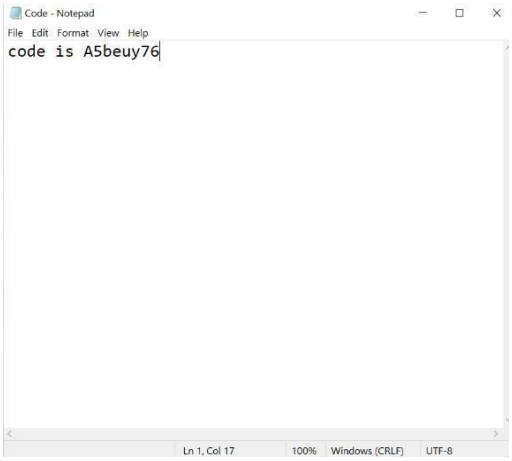

Manage
PRAX 8a
File
Home
Share
View
Picture Tools
This PC
DATA (D:)
CF
PRAX 8a
Search PRAX 8a
Quick access
Desktop
Documents
Downloads
Pictures
myfinalproject
New folder
ppt
this system related details sc
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
OS (C:)
DATA (D:)
USBSTORAGE (H:)
USBSTORAGE (H:)
Camera Roll
Network
s-tools4
BP
S-Tools - BP
File Window Help
BP
Ready
can hold up to 328,034 bytes
2 items
1 item selected 2.50 MB

Step 4) Select a valid audio file or image as the base file for the steganography file. The Tulips.bmp was selected and dragged onto the main window of the S-Tools program. The image is opened.

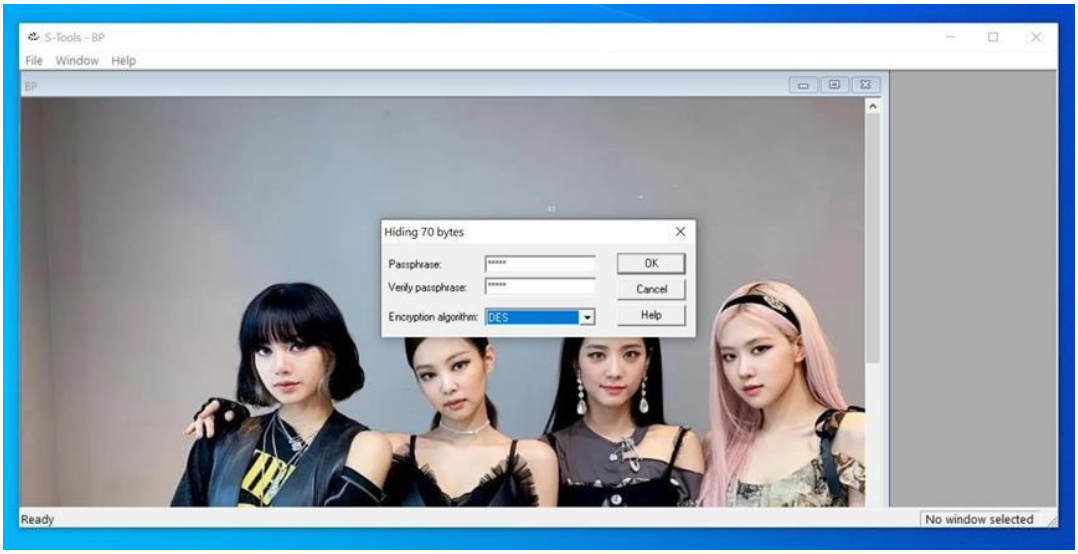


Step 5) Select a file to hide within the base file. If it's not there, create a txt file and Save the file.





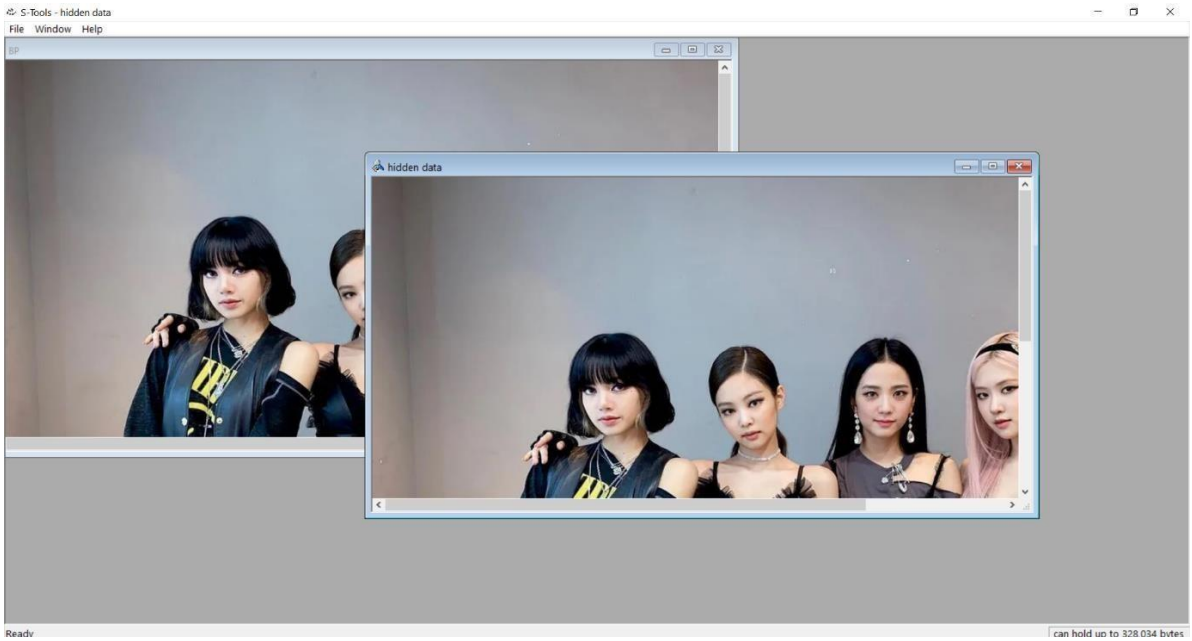
Step 7) A dialogue box will appear asking the user to enter and verify a passphrase. Additionally, the user will have to select an encryption algorithm.



Step 8) Enter a passphrase in both the passphrase and verify passphrase text boxes. If the same passphrase is not entered in both text boxes the 'OK' button will be grayed out and the user will not be able to proceed to creating the steganography file.

Step 9) Select the 'OK' button after entering a valid passphrase.

Step 10) The S-Tools main window will appear and a new file will be visible. The name of the file will be called hidden_data by default.



Step 11) Place the cursor on top of the hidden data image and select the right mouse button. The user will have four options available to them:

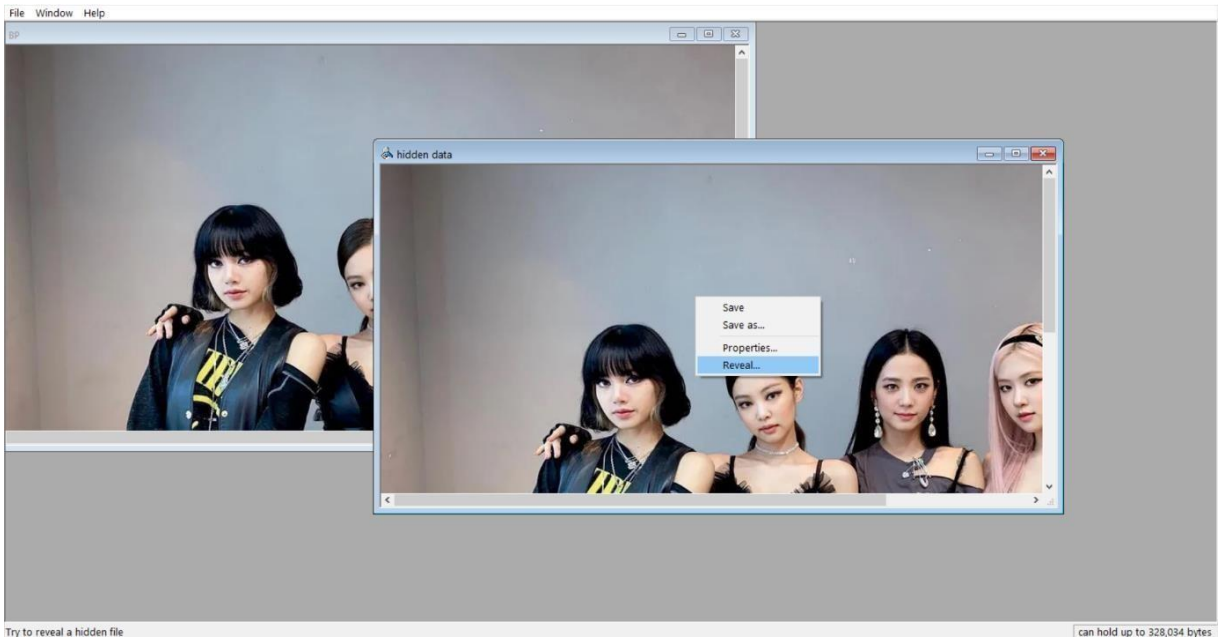
- Save
- Save As
- Properties
- Reveal

Step 12) Selecting the ‘Properties’ button while the cursor is over any image will display the following properties:

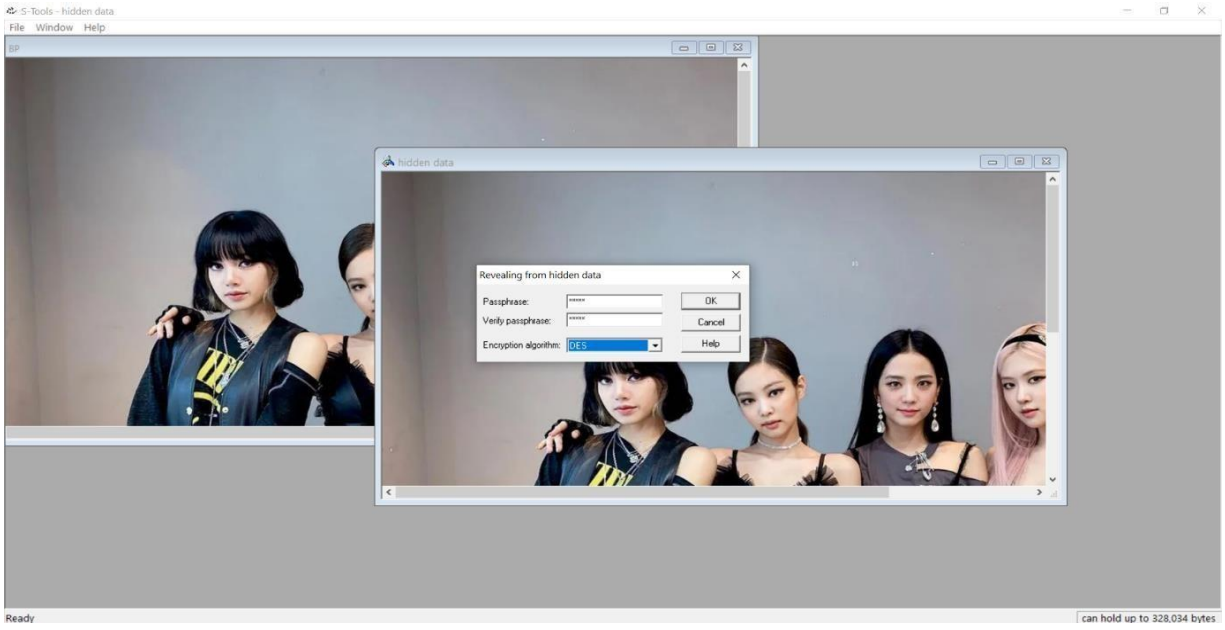
- Width and Height of the image
- Bits per pixel
- Memory Usage (file size in bytes)
- Compression

Step 13) Selecting the 'Reveal' button will display a passphrase dialogue box. A passphrase must be entered twice in the dialogue box and the correct encryption algorithm must be selected.

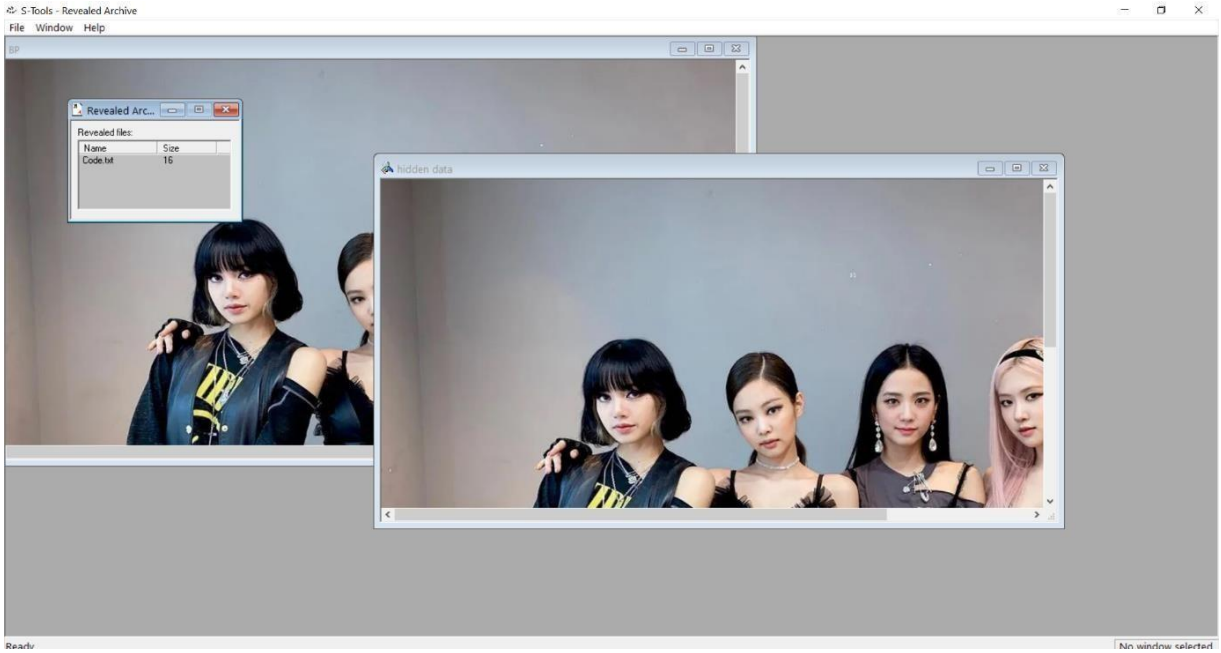
Notice that the title of the dialogue box has changed to 'Revealing from Cosmos.bmp'



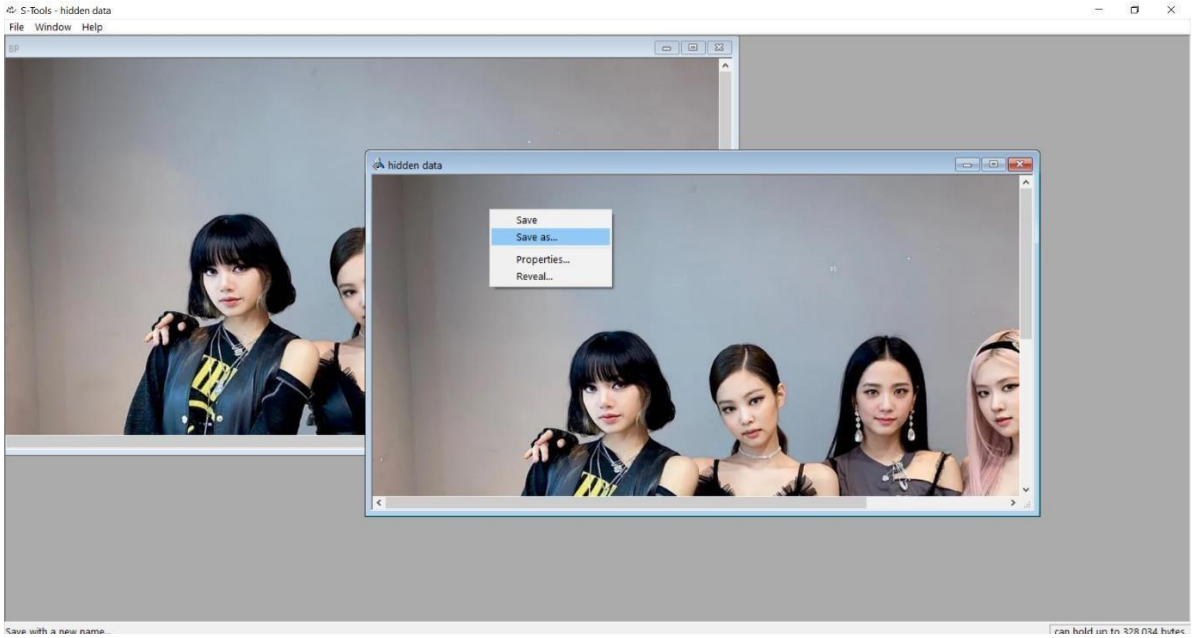
Step 14) Enter a passphrase twice, select the encryption algorithm, and select the 'OK' button.



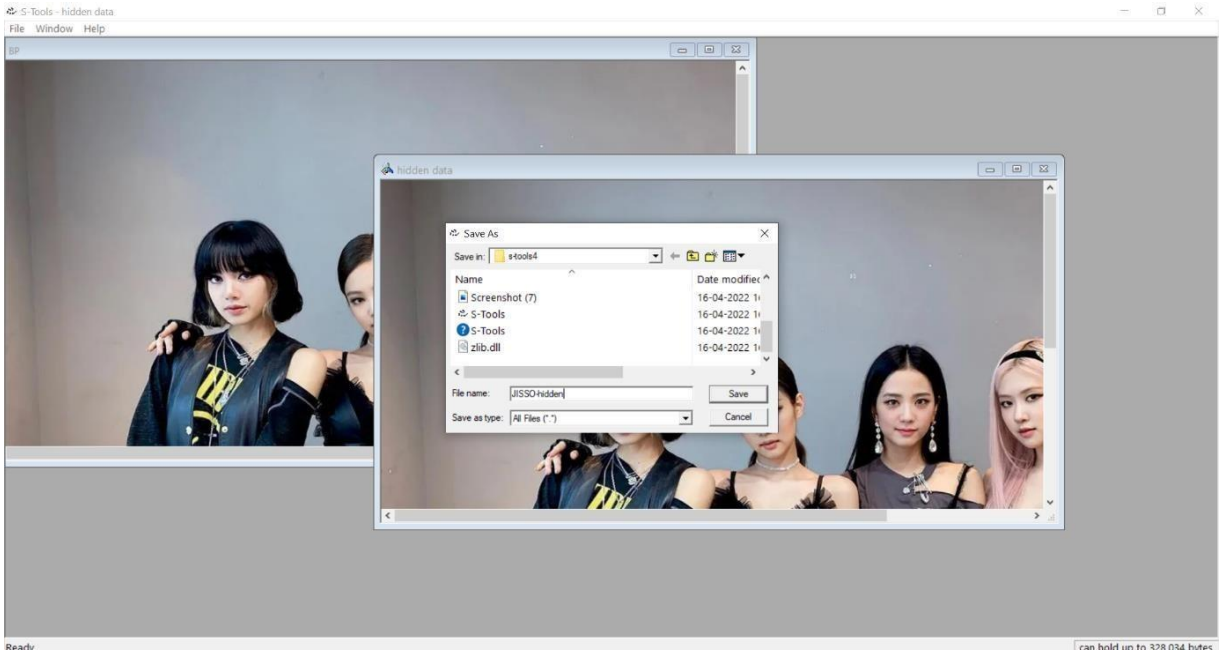
Step 15) A ‘Revealed Archive’ dialogue box will display which contains the file name and size of the hidden file.



Step 16) Select the ‘Save As’ button.

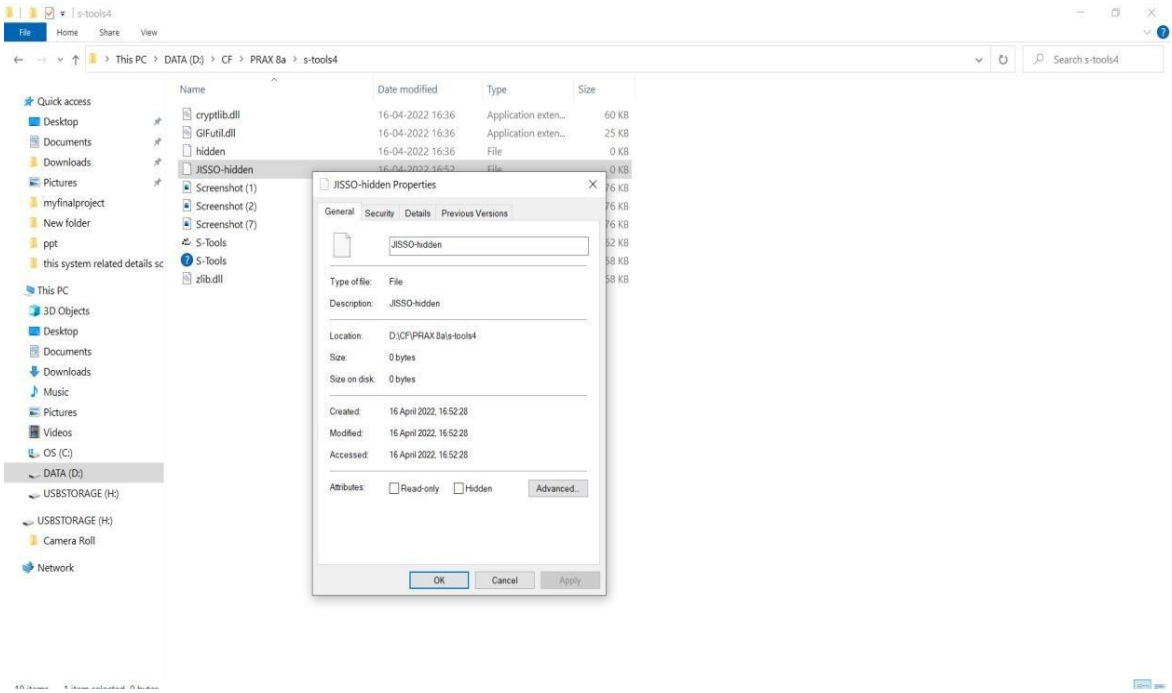


Step 17) A ‘Save As’ dialogue box will appear. Enter a valid file name, select the working directory and select the ‘Save’ button.



Step 18) Locate the files in the working directory.

Step 19) Open the files using a multimedia software program and ensure that the files were extracted from the steganography file successfully.



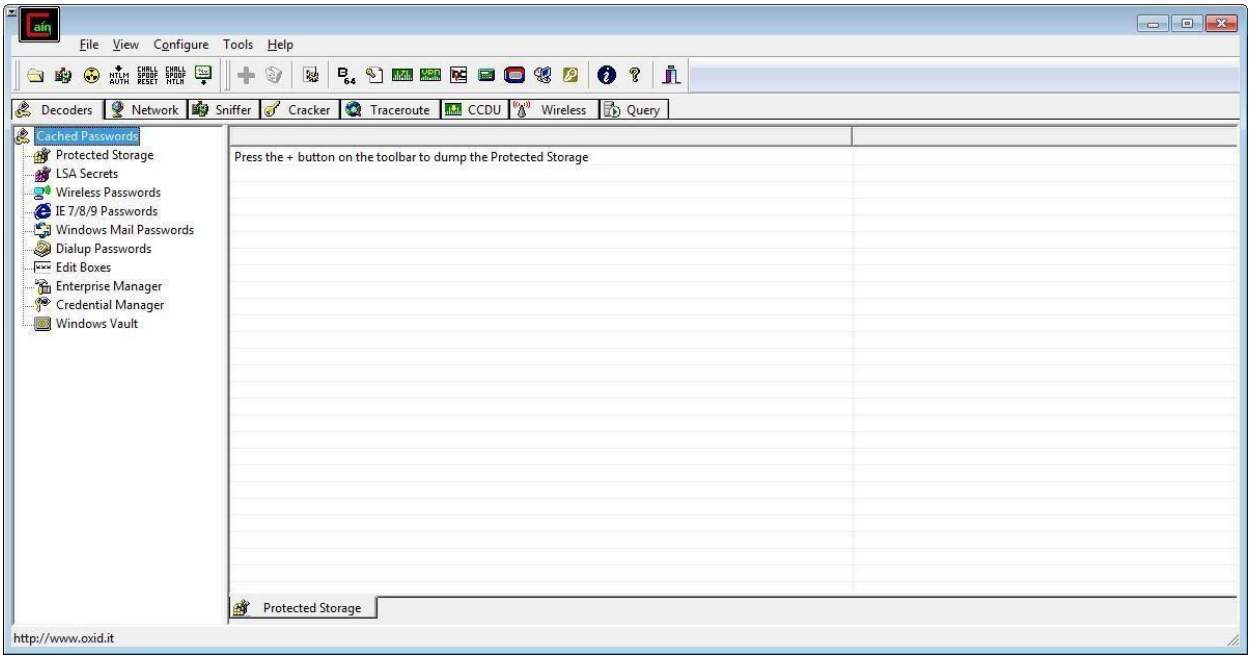
Practical No 7

Aim: - Performing Sniffing and Password Cracking Using Cain and Abel.

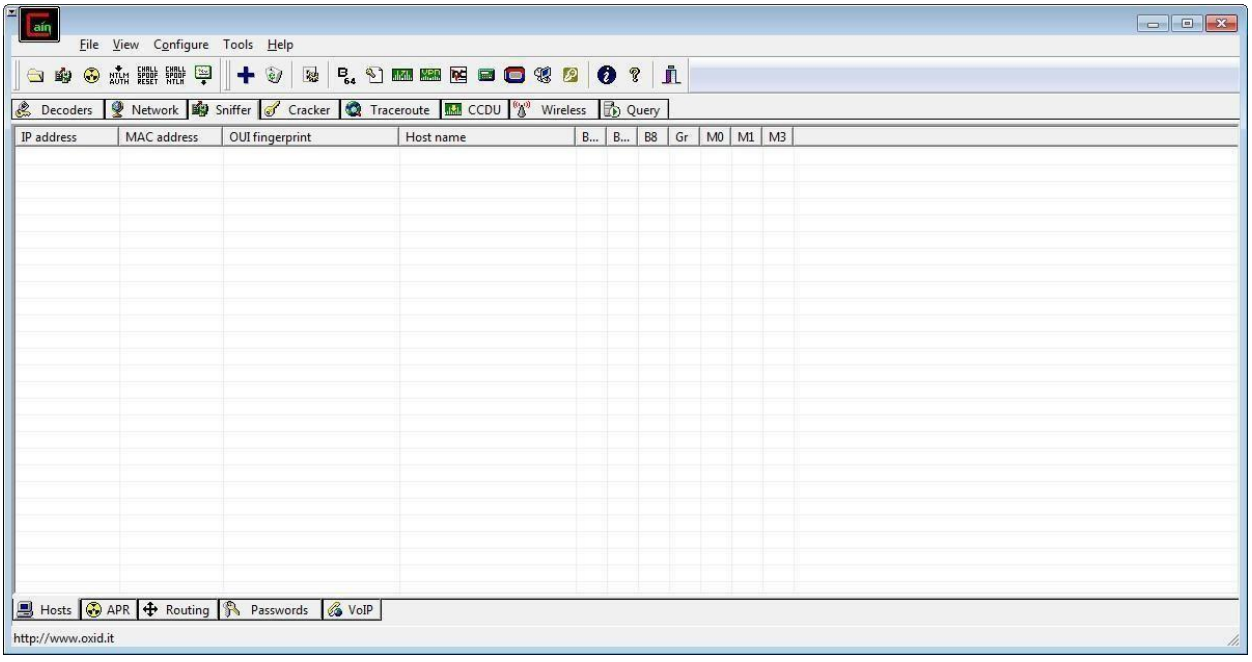
Practical No 7

Aim: - Performing Sniffing and Password Cracking Using Cain and Abel.

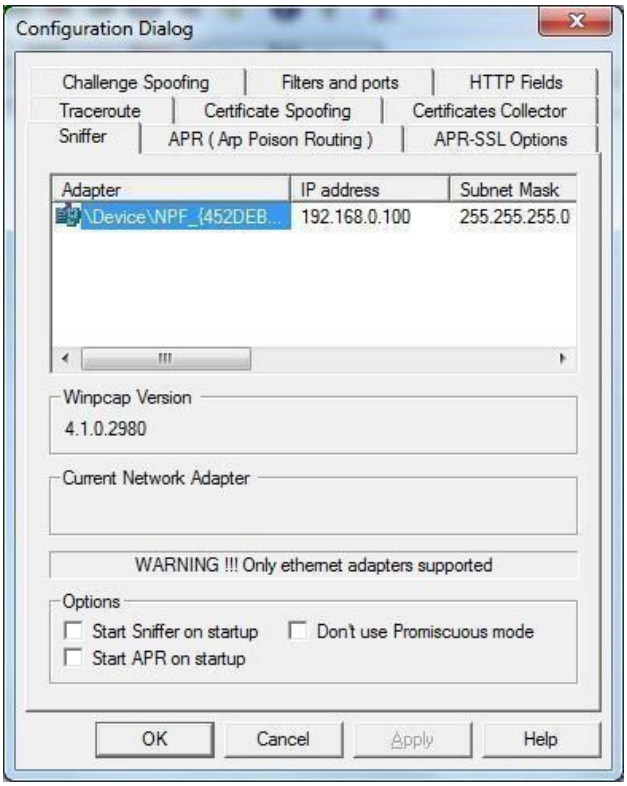
Step 1 : Install and open cain and abel.



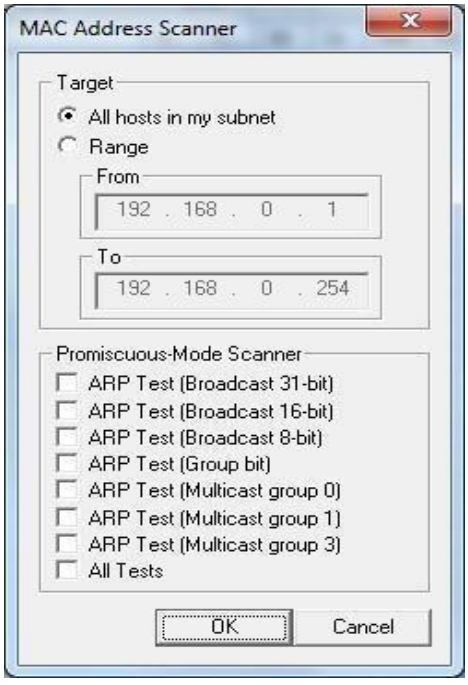
Step 2 : Select sniffer on the top.



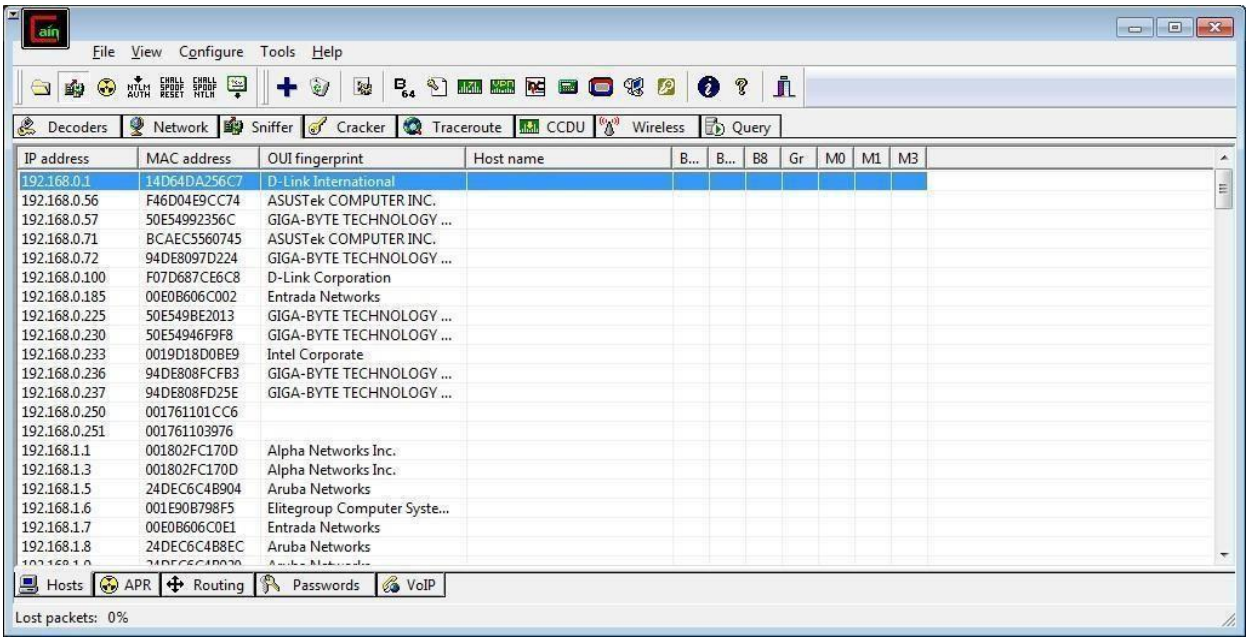
Step 3 : Next to folder icon click on icon name start/stop sniffer. Select device and click on ok.



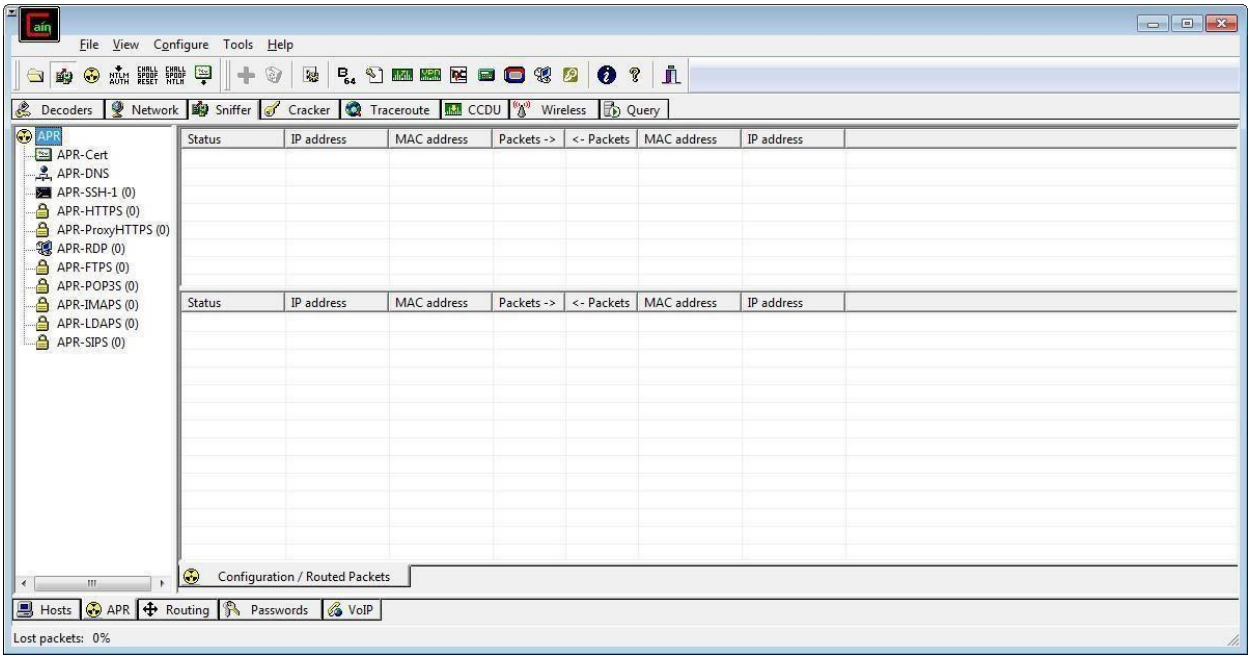
Step 4 : Click on "+" icon on the top. Click on ok.



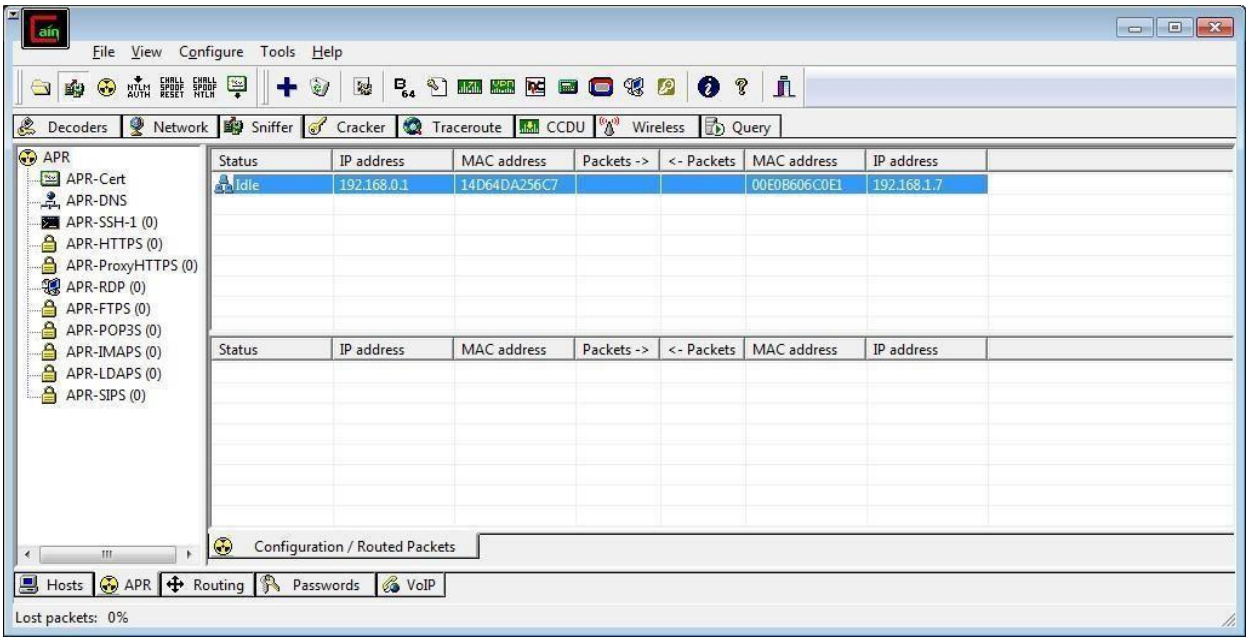
Step 5 : Shows the Connected host.



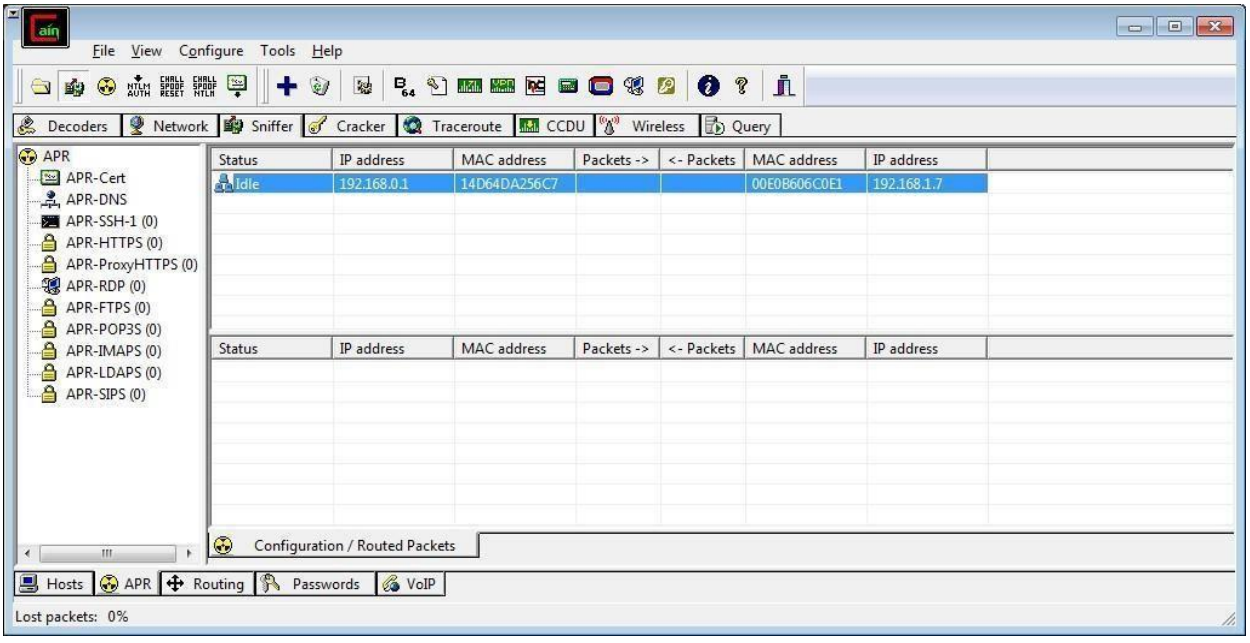
Step 6 : Select Arp at bottom.



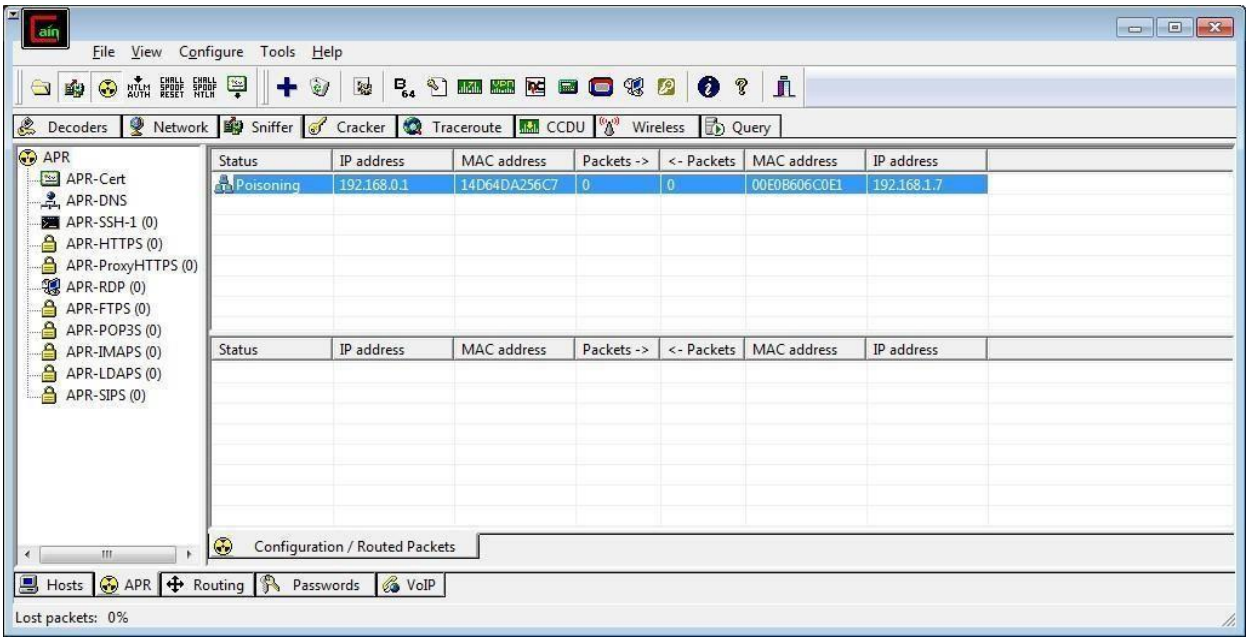
Step 7 : Click on "+" icon at the top.



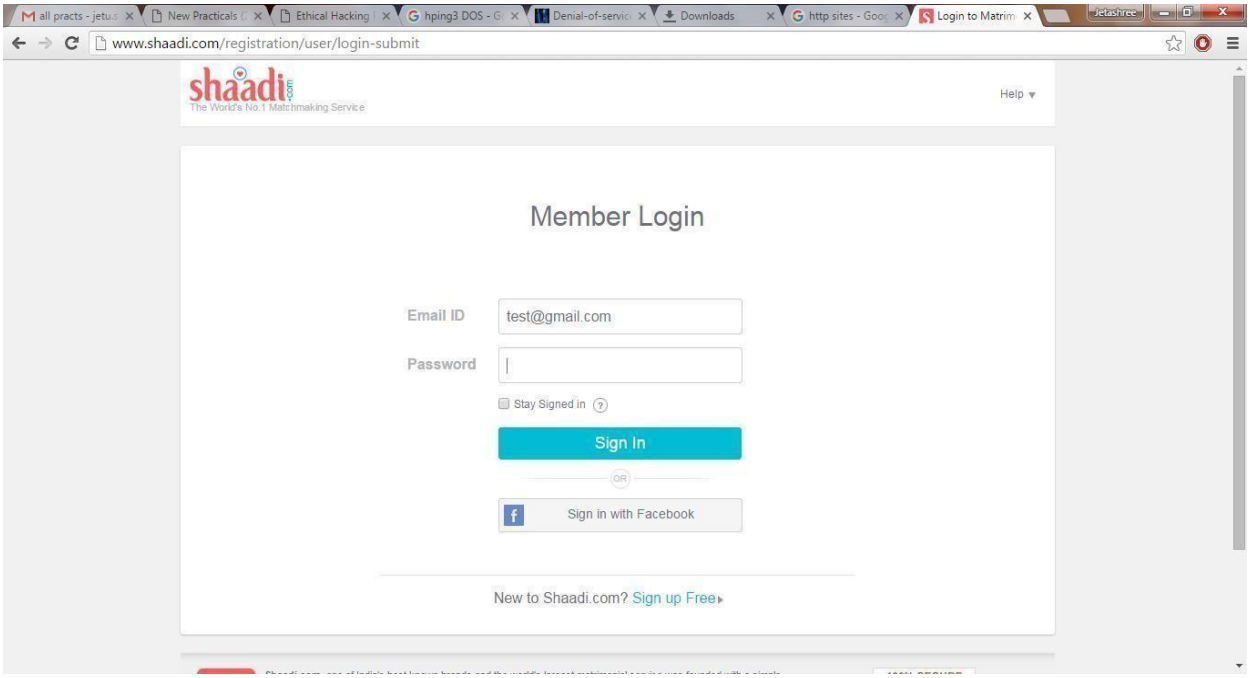
Step 8 : Click on start/stop ARP icon on top.



Step 9 : Poisoning the source.



Step 10 : Go to any website on source ip address.



Step 11 : Go to password option in the cain & abel and see the visited site password.