CYBER FORENSICS

A PRACTICAL REPORT

ON
CYBER FORENSICS

SUBMITTED BY
Mr. ASHISH JITENDRA RAWAL
Roll No: 2511036

UNDER THE GUIDANCE OF
PROF. AQSA ABBASI

Submitted in fulfillment of the requirements for qualifying
MSc. IT Part II Semester - IV Examination 2021-2022

University of Mumbai
Department of Information Technology

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

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

Bandra (W), Mumbai _ 400050.

Department of Information Technolog y
M.Sc. (IT)

Certificate

*This is to certify that **Cyber Forensics Practicals** performed at R.D & S.H National & W.A.Science College by Mr./Miss. **Ashish Jitendra Rawal** holding Seat No. **2511036** studying Master of Science in Information Technology Semester – IV has been satisfactorily completed as prescribed by the University of Mumbai, during the year 2021 – 2022.*

Lecturer In charge **External Examiner** **Head of Department**

College Stamp

INDEX

Practical No: 01

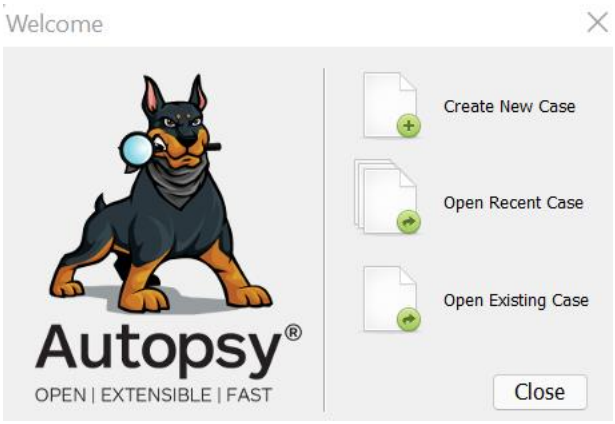
Practical No: 01

File system Analysis using The Sleuth kit

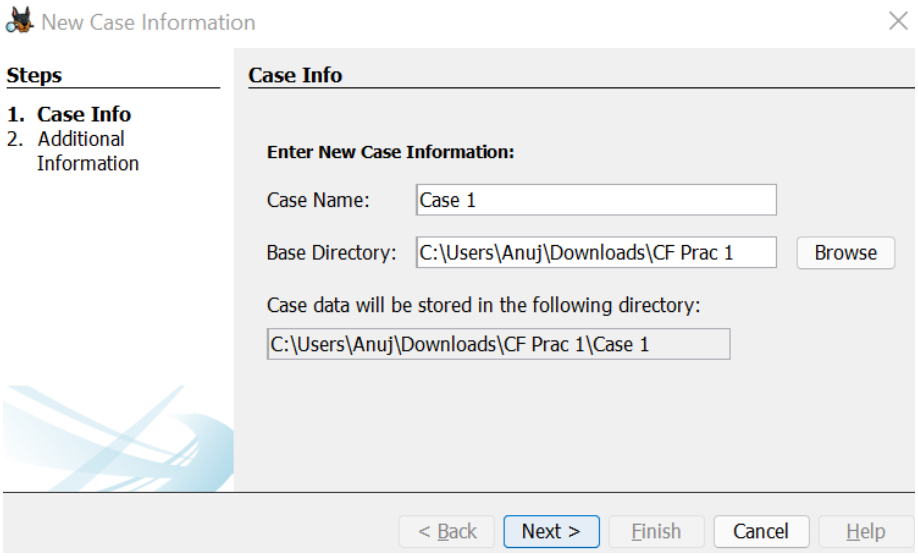
Aim: Exploring Autopsy.

How to Start a Case

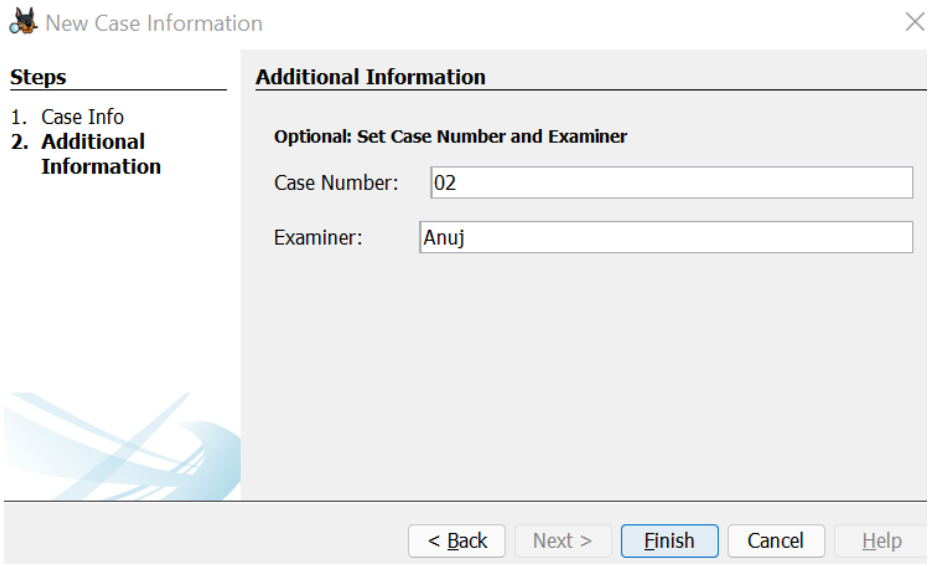
Upon starting Autopsy 3.1.2, a window will open with three selections to make: create a new case, open existing case, or to open a recent case.



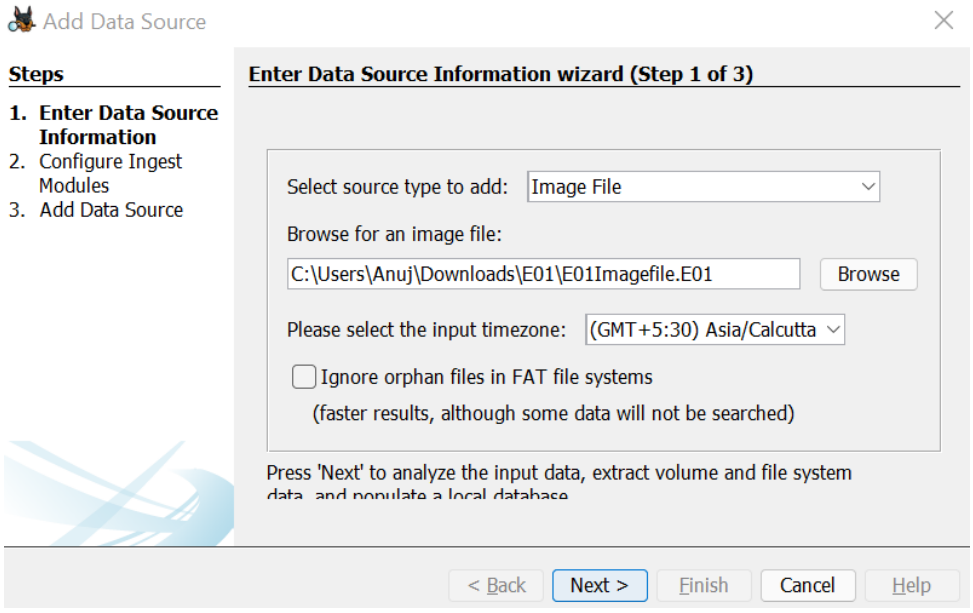
Step 1) Select the "Create New Case" option and be directed to a new window that will have information to fill in, we will be naming the case "Test."



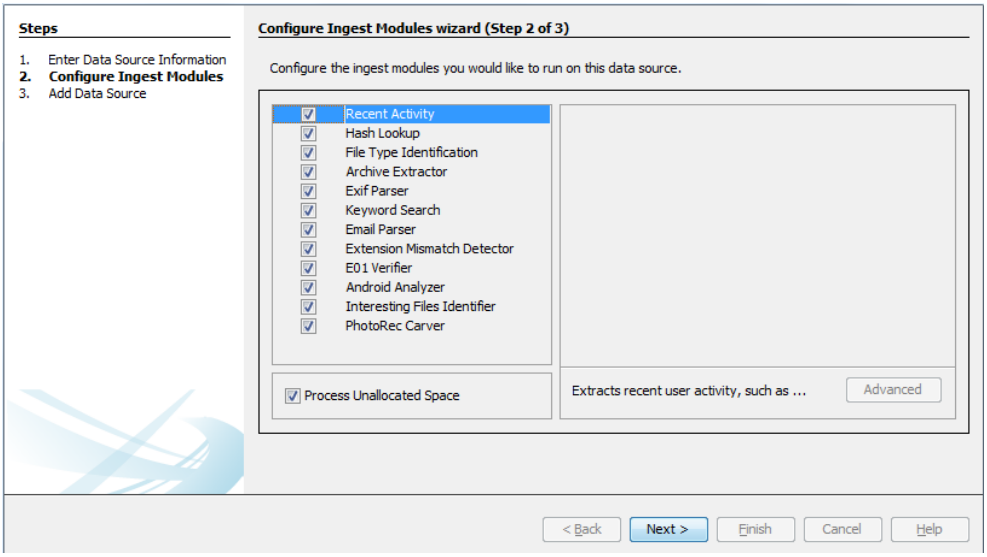
Step 2) After the information has been filled in select the next button. The next window will allow the investigator to fill in the case number and examiner name. This is for the purpose of creating better documentation and logging. After the information is filled in select the finish button to continue.



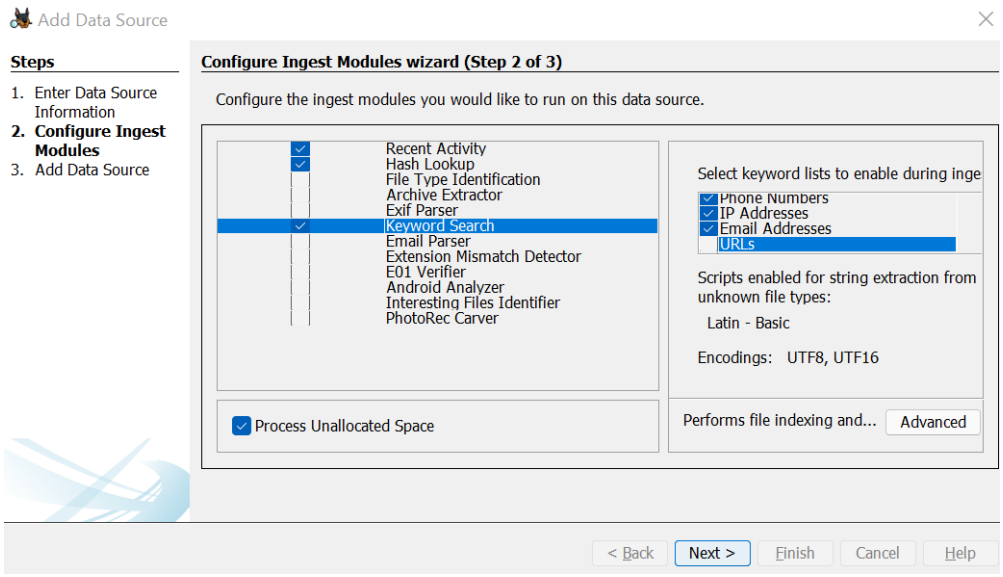
Step 3) The next step in the investigation will be to add an image file to the case. The image file can be chosen from a wide variety of formats including: img, dd, 001, aa, and e01. Use the browse button to find the image that is desired to work with and select add. Options to choose the timezone of 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 4) After selecting the next button the image will be added to the case and the next button should be selected again if there are no errors.



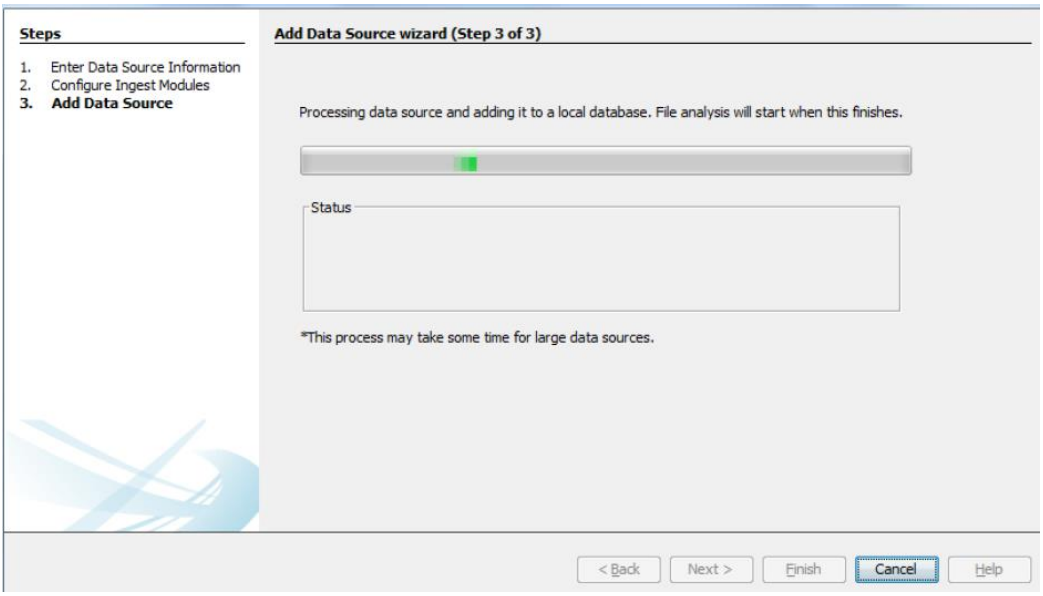
Step 5) The following window will bring the investigator to the Ingest wizard panel, which is one of the new features offered in Autopsy. There are three options in the first box: Recent Activity, Hash lookup, and Keyword Searches.

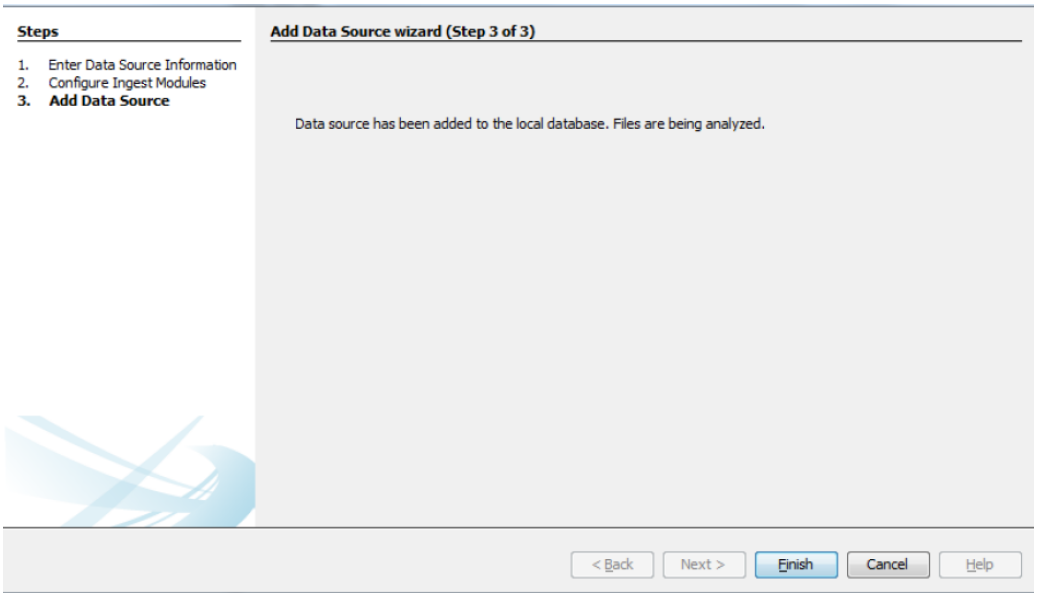


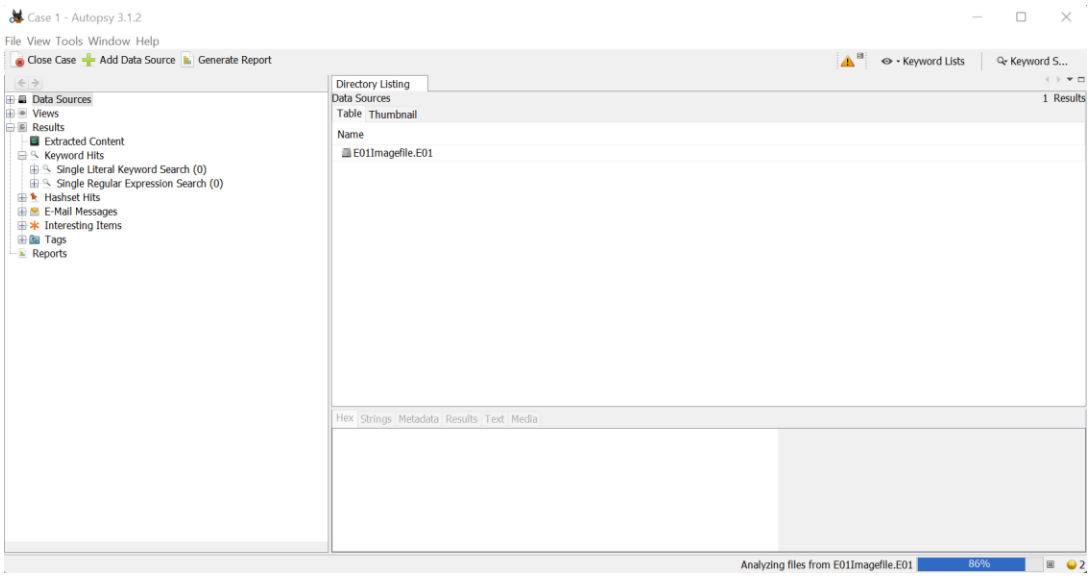
By selecting any of the options advanced settings can be set to increase the capabilities of the search. Under the Hash Lookup option there is the advanced option to add databases of known hashes.

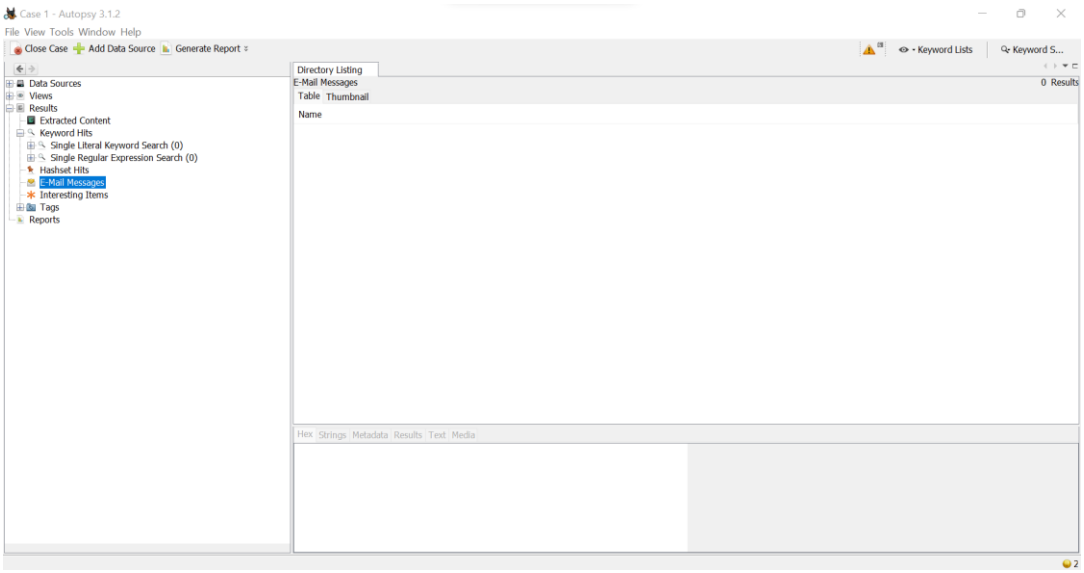
Under the Keyword Search option are many different lists that can be used to search for information. By default, Phone Numbers, IP Addresses, Email Addresses, and URL's are available. Select the Advanced button and a Keyword List Configuration window will open. In this new window select New List and 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.

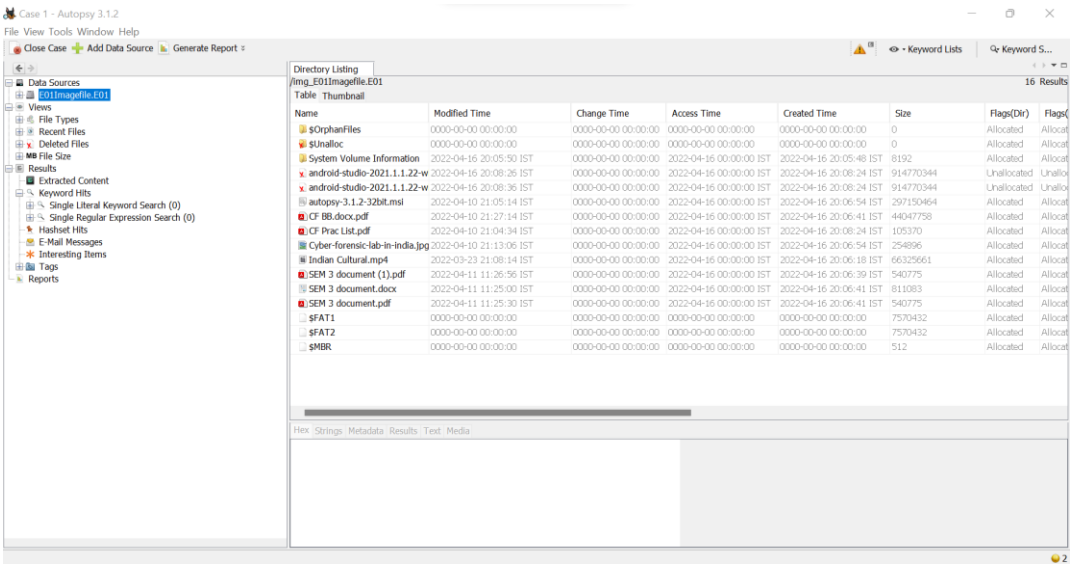




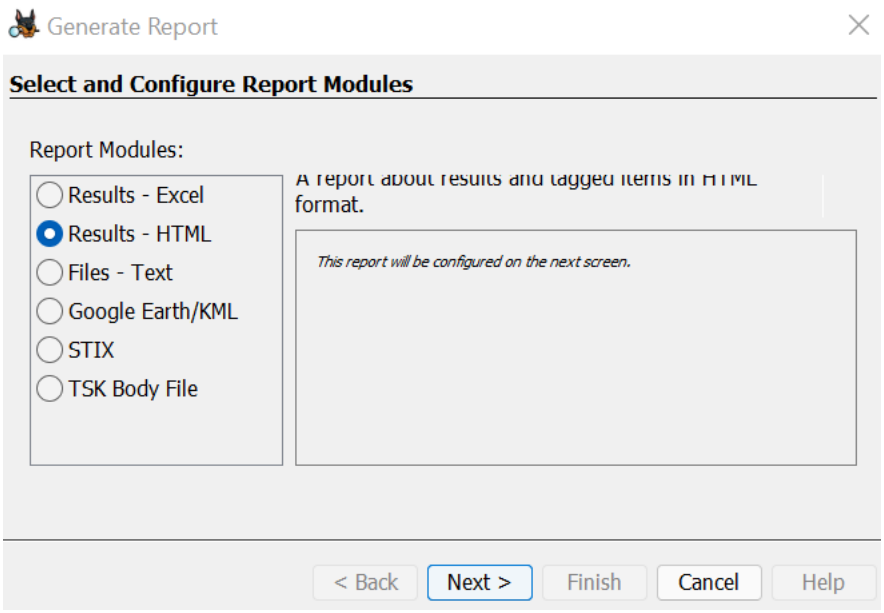


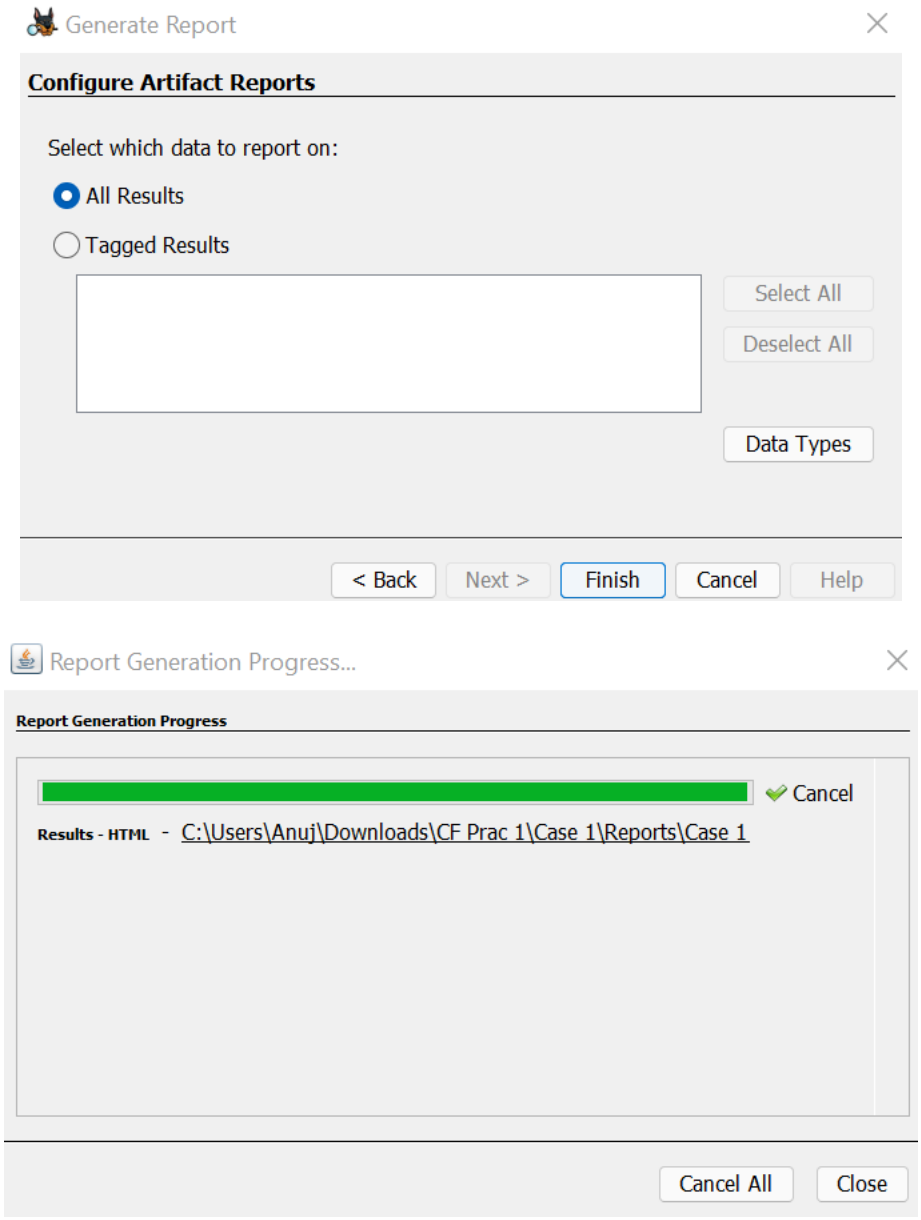


Step 6) After finishing the keyword parameters the screen will be laid out for the user.

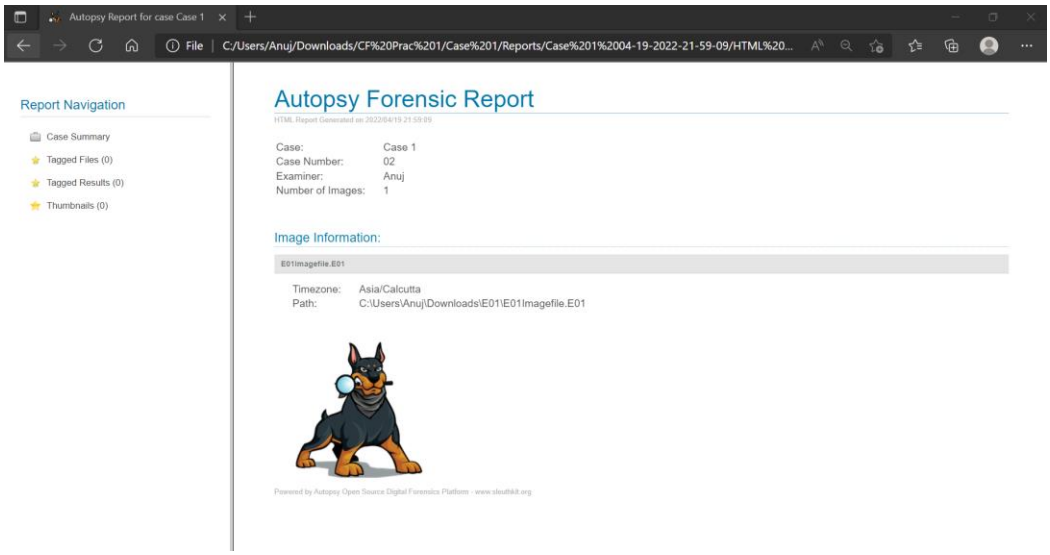


Step 7) After the image is indexed the tree will be populated by the file system, extracted content, keyword searches, and the hash list (if any were used).
the investigator should generate a report. This will allow the investigator to have an idea of what type of information is available and what to 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.

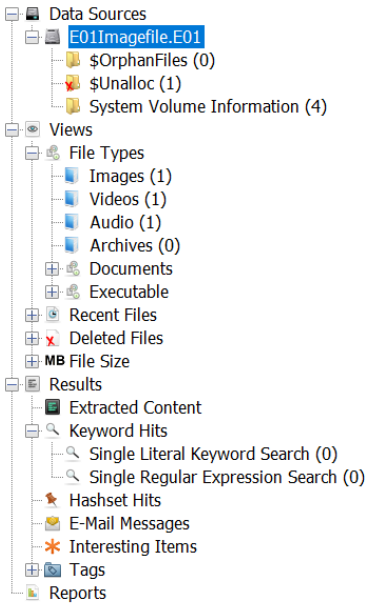




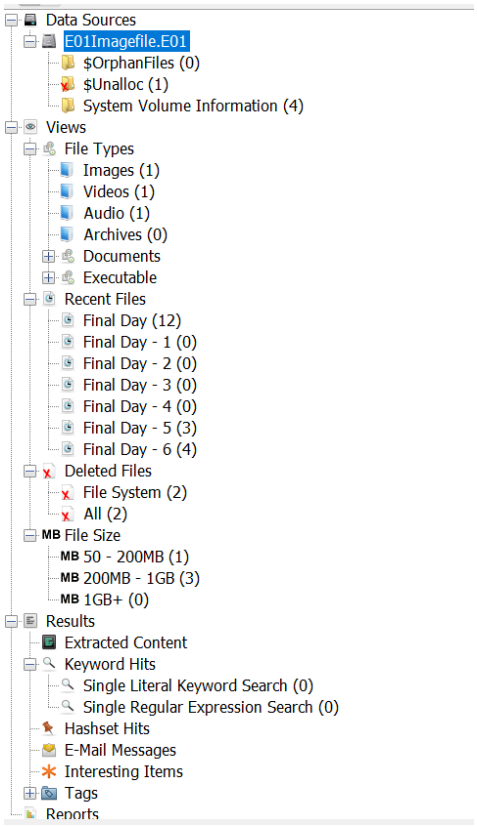
Step 8) With the report on hand the investigator will have an idea of what to expect as well as a list of programs that are installed on the machine. This can help investigators gather all the evidence they need to perform a complete investigation.



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



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.



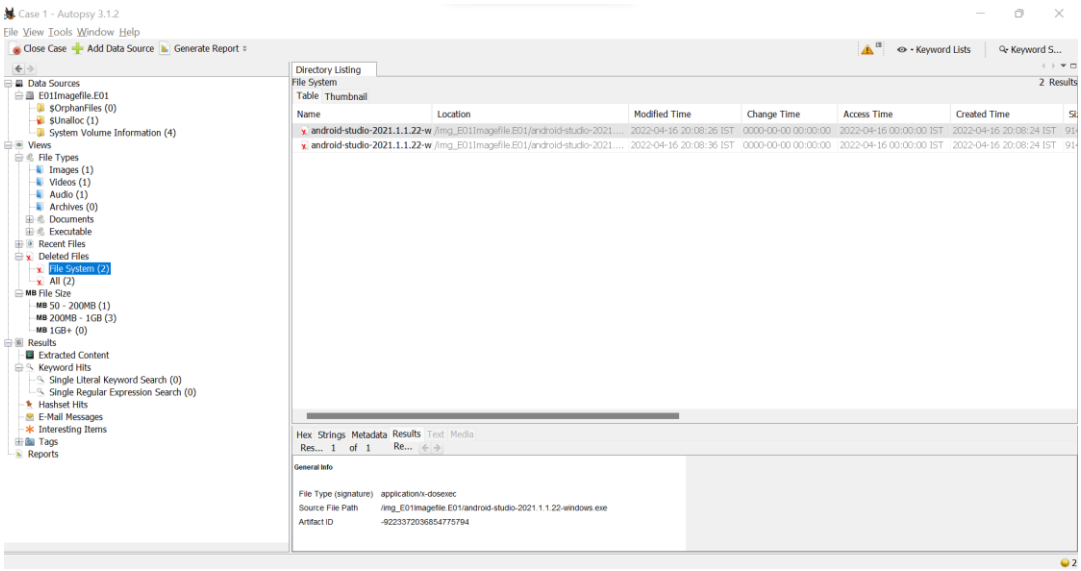
The next tab that is seen is the Results tab, this is a new feature that displays all the information from the ingest process. This uses the program BEViewer to look for certain information inside of the data and separate it into sections that make it easier to search for specific data instead of going 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.

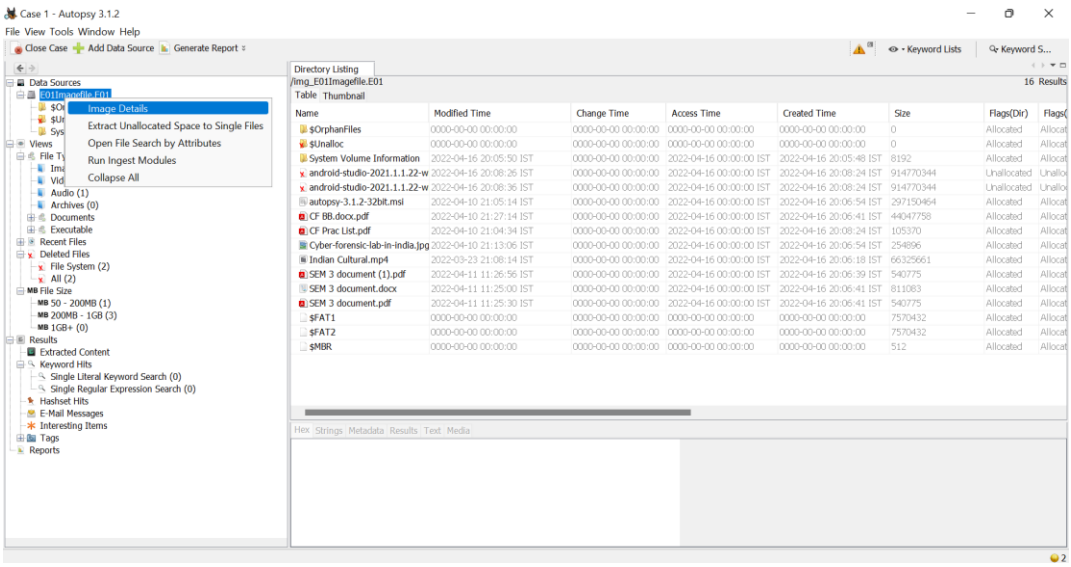
There are 4 main categories when separating the Results tab: Extracted Content, Keyword Hits, Hashset Hits, and E-mail Messages. Each of these sections has subsections that allow for more specific information divisions. In the Extracted Content tab there are sections for: Bookmarks, Cookies, Web History, 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 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 of the results would be placed in the hashset hits tab. The e-mail message tab will place any emails from a desktop client in the tab for review. The supported programs are Microsoft Outlook and Mozilla Thunderbird as of now but more are scheduled for support in the future.




Case 1 - Autopsy 3.1.2
File View Tools Window Help
Close Case
Add Data Source
Generate Report
Keyword Lists
Keyword S...
Data Sources
E01Imagefile.E01
Image Details
Extract Unallocated Space to Single Files
Open File Search by Attributes
Run Ingest Modules
Collapse All
Views
File Types
Audio (1)
Archives (0)
Documents
Executable
Recent Files
Deleted Files
File System (2)
All (2)
File Size
50 - 200MB (1)
200MB - 1GB (3)
1GB+ (0)
Results
Extracted Content
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Hashset Hits
E-Mail Messages
Interesting Items
Tags
Reports
Directory Listing
/img_E01Imagefile.E01
16 Results
Table
Thumbnail
Name
Modified Time
Change Time
Access Time
Created Time
Size
Flags(Dir)
$OrphanFiles
$Unalloc
System Volume Information
android-studio-2021.1.1.22-w
android-studio-2021.1.1.22-w
autopsy-3.1.2-32bit.msi
CF BB.docx.pdf
CF Prac List.pdf
Cyber-forensic-lab-in-india.jpg
Indian Cultural.mp4
SEM 3 document (1).pdf
SEM 3 document.docx
SEM 3 document.pdf
$FAT1
$FAT2
$MBR
Hex
Strings
Metadata
Results
Text
Media

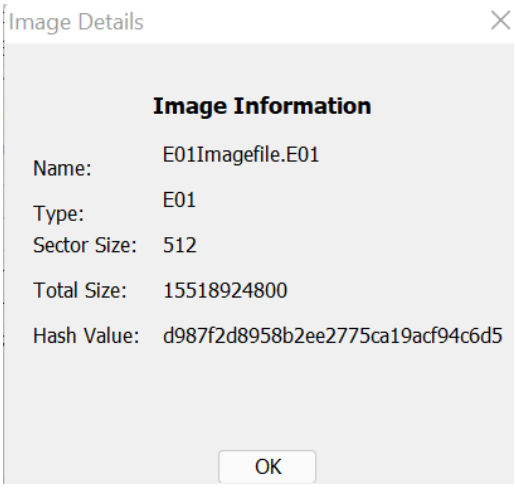
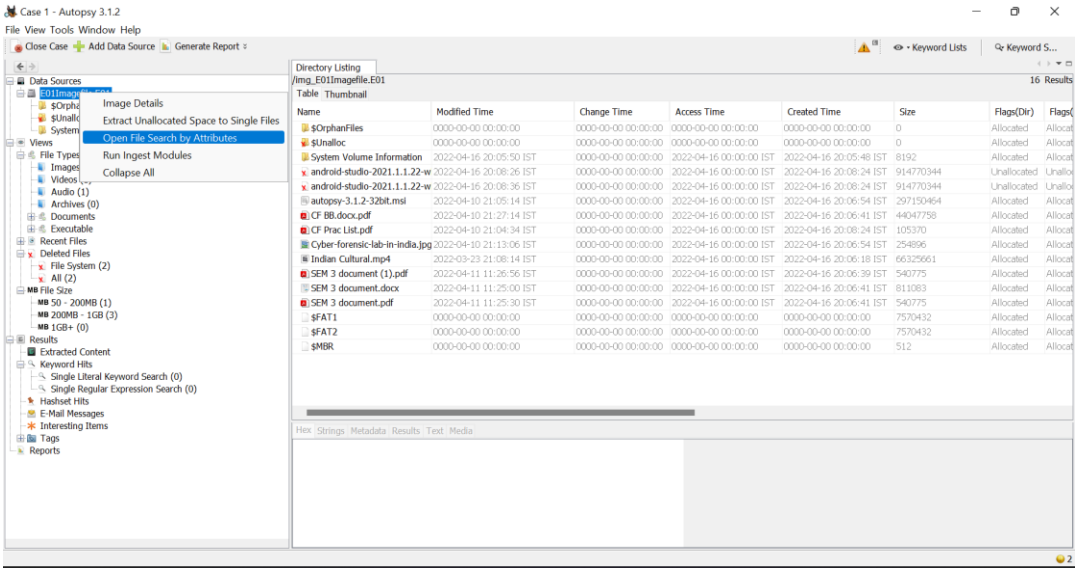
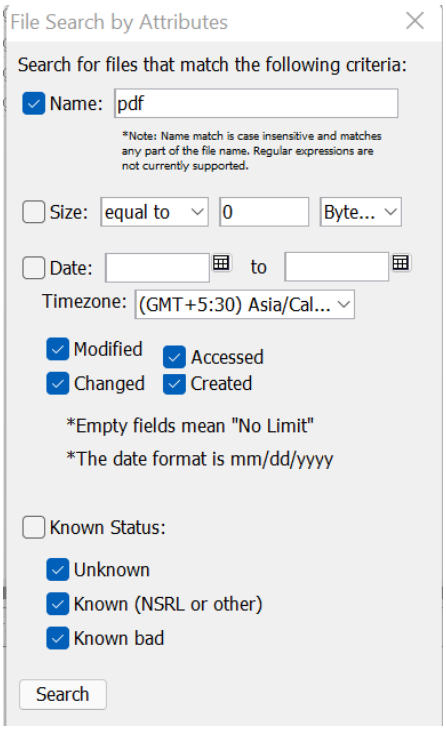
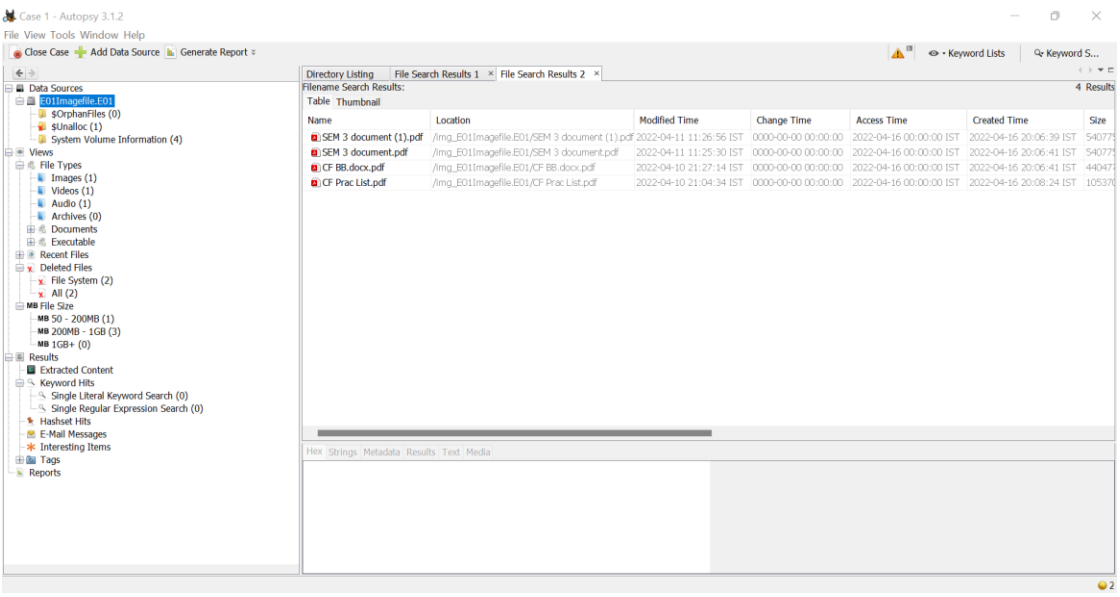
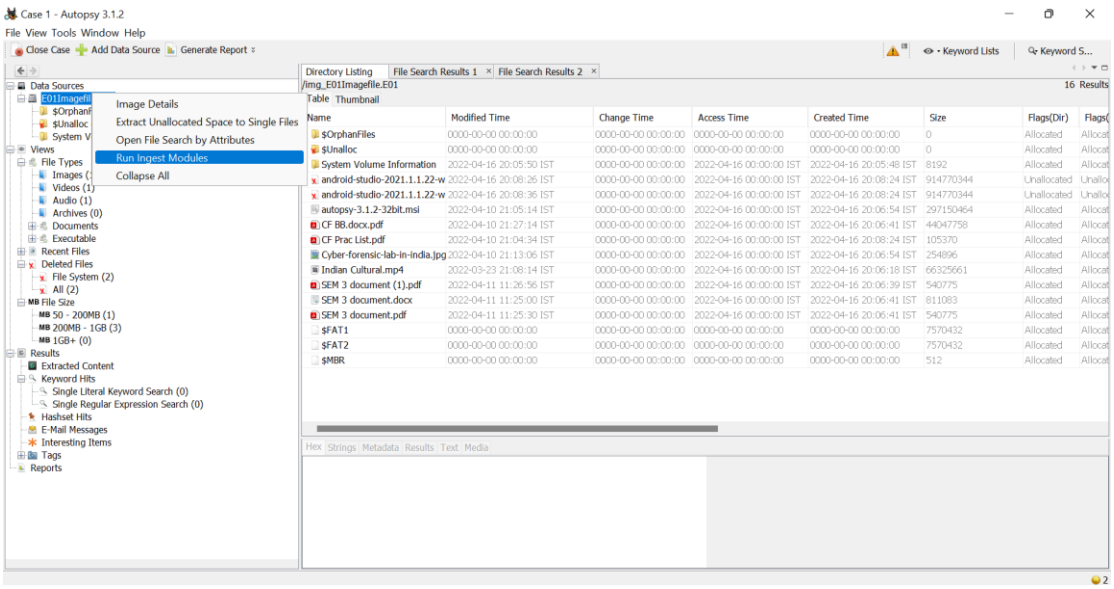


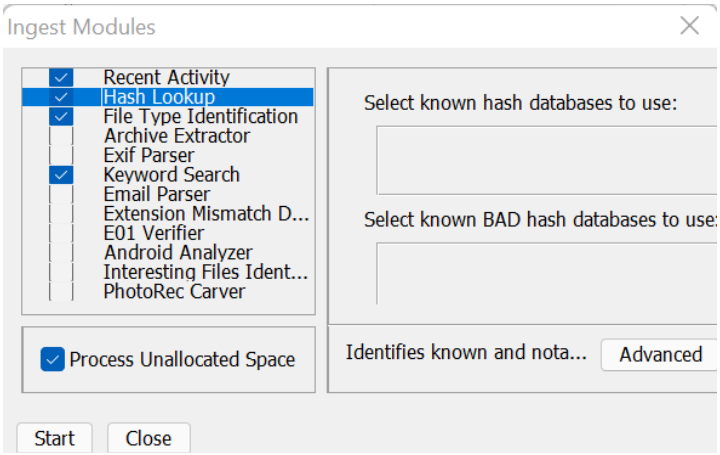
Image Details
Image Information
Name: E01Imagefile.E01
Type: E01
Sector Size: 512
Total Size: 15518924800
Hash Value: d987f2d8958b2ee2775ca19acf94c6d5
OK

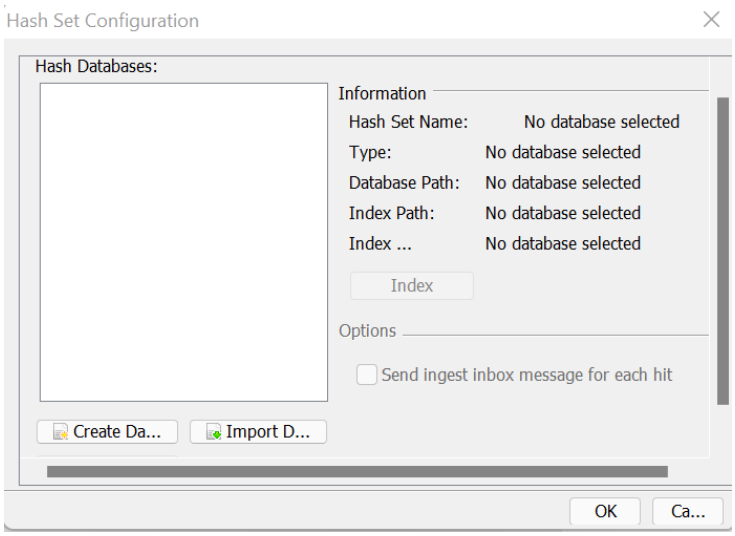

Case 1 - Autopsy 3.1.2
File View Tools Window Help
Close Case
Add Data Source
Generate Report
Keyword Lists
Keyword S...
Image Details
Extract Unallocated Space to Single Files
Open File Search by Attributes
Run Ingest Modules
Collapse All
Directory Listing
/img_E01Imagefile.E01
16 Results
Table
Thumbnail

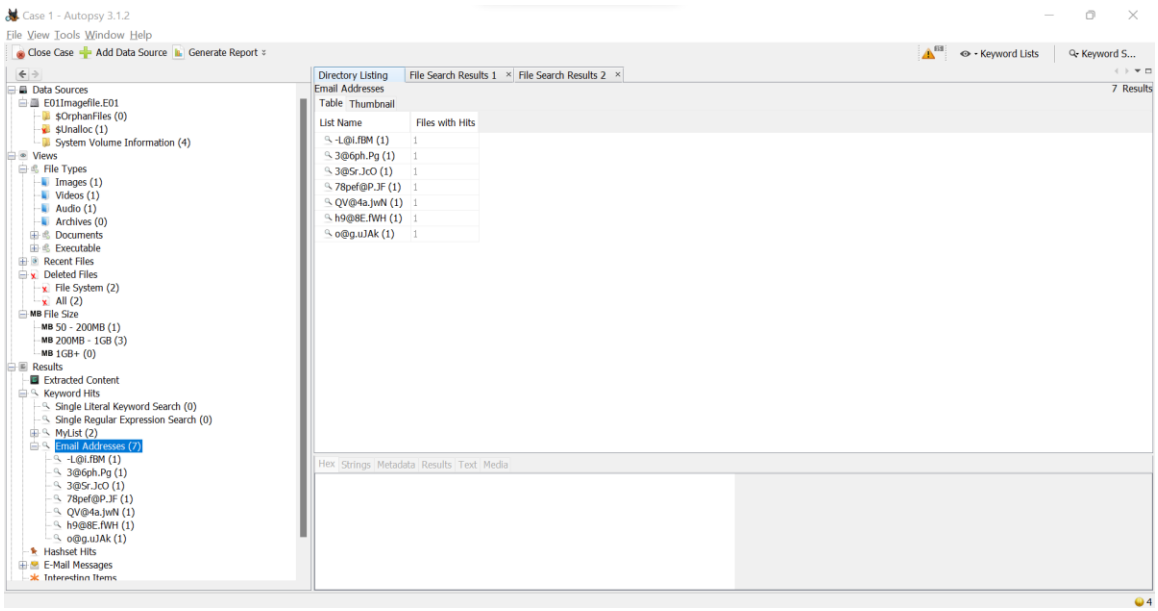

File Search by Attributes
Search for files that match the following criteria:
Name: pdf
*Note: Name match is case insensitive and matches any part of the file name. Regular expressions are not currently supported.
Size: equal to 0 Byte...
Date: to
Timezone: (GMT+5:30) Asia/Cal...
Modified
Accessed
Changed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


Case 1 - Autopsy 3.1.2
File View Tools Window Help
Close Case
Add Data Source
Generate Report
Keyword Lists
Directory Listing
File Search Results 1
File Search Results 2
Filename Search Results:
4 Results
Table
Thumbnail
Name
Location
Modified Time
Change Time
Access Time
Created Time
Size
SEM 3 document (1).pdf
SEM 3 document.pdf
CF BB.docx.pdf
CF Prac List.pdf
Data Sources
E01Imagefile.E01
$OrphanFiles (0)
$Unalloc (1)
System Volume Information (4)
Views
File Types
Images (1)
Videos (1)
Audio (1)
Archives (0)
Documents
Executable
Recent Files
Deleted Files
File System (2)
All (2)
File Size
50 - 200MB (1)
200MB - 1GB (3)
1GB+ (0)
Results
Extracted Content
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Hashset Hits
E-Mail Messages
Interesting Items
Tags
Reports
Hex
Strings
Metadata
Results
Text
Media


Case 1 - Autopsy 3.1.2
File View Tools Window Help
Close Case
Add Data Source
Generate Report
Keyword Lists
Keyword S...
Data Sources
E01Imagefile
$OrphanF
$Unalloc
System V
Views
File Types
Images (
Videos (1)
Audio (1)
Archives (0)
Documents
Executable
Recent Files
Deleted Files
File System (2)
All (2)
File Size
50 - 200MB (1)
200MB - 1GB (3)
1GB+ (0)
Results
Extracted Content
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Hashset Hits
E-Mail Messages
Interesting Items
Tags
Reports
Image Details
Extract Unallocated Space to Single Files
Open File Search by Attributes
Run Ingest Modules
Collapse All
Directory Listing
File Search Results 1
File Search Results 2
/img_E01Imagefile.E01
16 Results
Table
Thumbnail
Name
Modified Time
Change Time
Access Time
Created Time
Size
Flags(Dir)
$OrphanFiles
$Unalloc
System Volume Information
android-studio-2021.1.1.22-w
android-studio-2021.1.1.22-w
autopsy-3.1.2-32bit.msi
CF BB.docx.pdf
CF Prac List.pdf
Cyber-forensic-lab-in-india.jpg
Indian Cultural.mp4
SEM 3 document (1).pdf
SEM 3 document.docx
SEM 3 document.pdf
$FAT1
$FAT2
$MBR
Hex
Strings
Metadata
Results
Text
Media

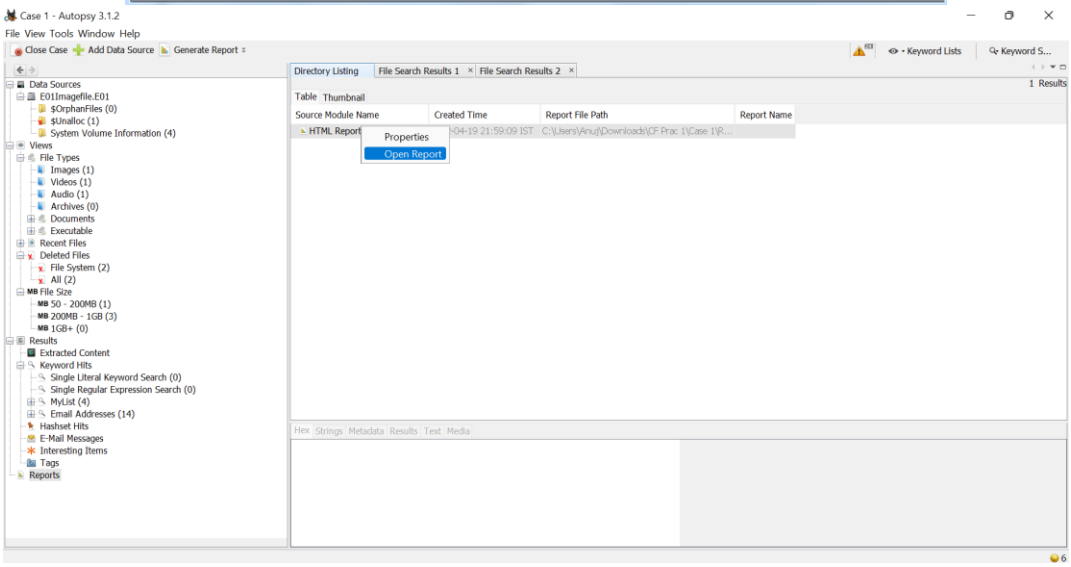

Ingest Modules
Recent Activity
Hash Lookup
File Type Identification
Archive Extractor
Exif Parser
Keyword Search
Email Parser
Extension Mismatch D...
E01 Verifier
Android Analyzer
Interesting Files Ident...
PhotoRec Carver
Select known hash databases to use:
Select known BAD hash databases to use:
Process Unallocated Space
Identifies known and nota...
Advanced
Start
Close

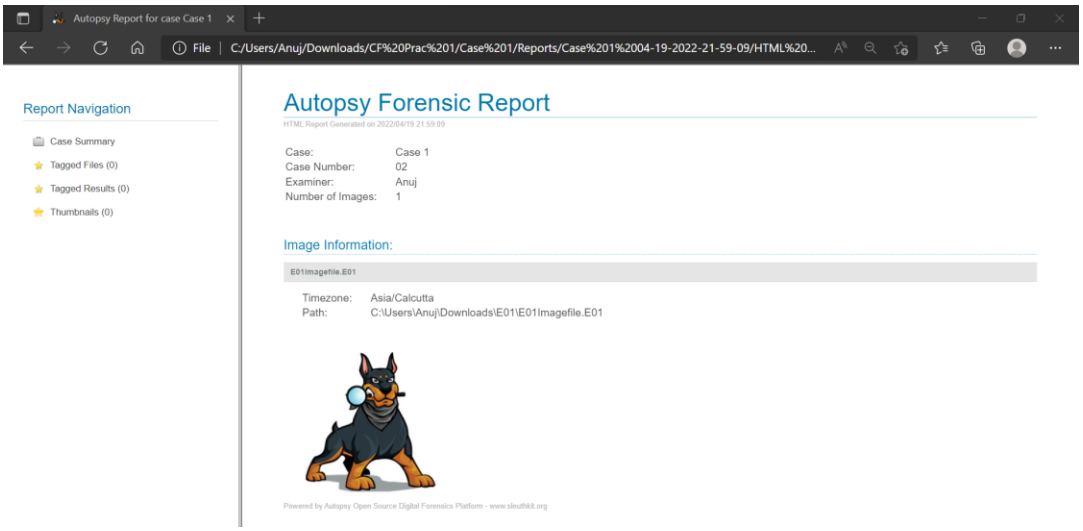

Hash Set Configuration
Hash Databases:
Information
Hash Set Name:
No database selected
Type:
No database selected
Database Path:
No database selected
Index Path:
No database selected
Index ...
No database selected
Index
Options
Send ingest inbox message for each hit
Create Da...
Import D...
OK
Ca...



Module	Num	New?	Subject	Timestamp
Hash Lookup	1		No known bad hash database set	19:16:15
Hash Lookup	1		No known hash database set	19:16:15
Recent Activity	1		Started UnixImageFile.dd	19:16:20
Recent Activity	1		Finished UnixImageFile.dd - No errors reported	19:16:20
Recent Activity	1		UnixImageFile.dd - Browser Results	19:16:20
Android Analyzer	1		Started Analysis	19:16:20
Android Analyzer	1		Finished Analysis: No errors	19:16:22
Archive Extractor	1		Encrypted files in archive detected.	20:49:06
File Type Identification	1		File Type Id Results	21:17:25

Sort by: Time Total: 9 Unique: 9




Autopsy Report for case Case 1
File | C:/Users/Anuj/Downloads/CF%20Prac%201/Case%201/Reports/Case%201%2004-19-2022-21-59-09/HTML%20...
Report Navigation
Case Summary
Tagged Files (0)
Tagged Results (0)
Thumbnails (0)
Autopsy Forensic Report
HTML Report Generated on 2022/04/19 21:59:09
Case: Case 1
Case Number: 02
Examiner: Anuj
Number of Images: 1
Image Information:
E01Imagefile.E01
Timezone: Asia/Calcutta
Path: C:\Users\Anuj\Downloads\E01\E01Imagefile.E01
Powered by Autopsy Open Source Digital Forensics Platform - www.sleuthkit.org

Practical No: 02

Practical No: 02

Using AccessData FTK

Aim: Exploring Access data FTK for the following:

→ 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.**

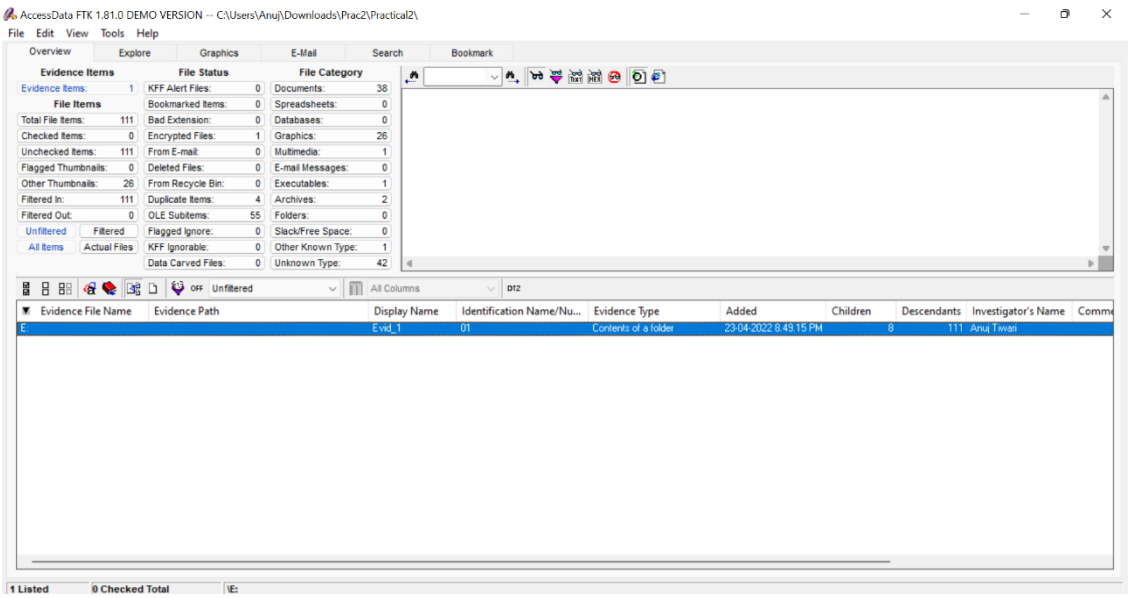
Data Carving Files During Evidence Processing in a New Case:

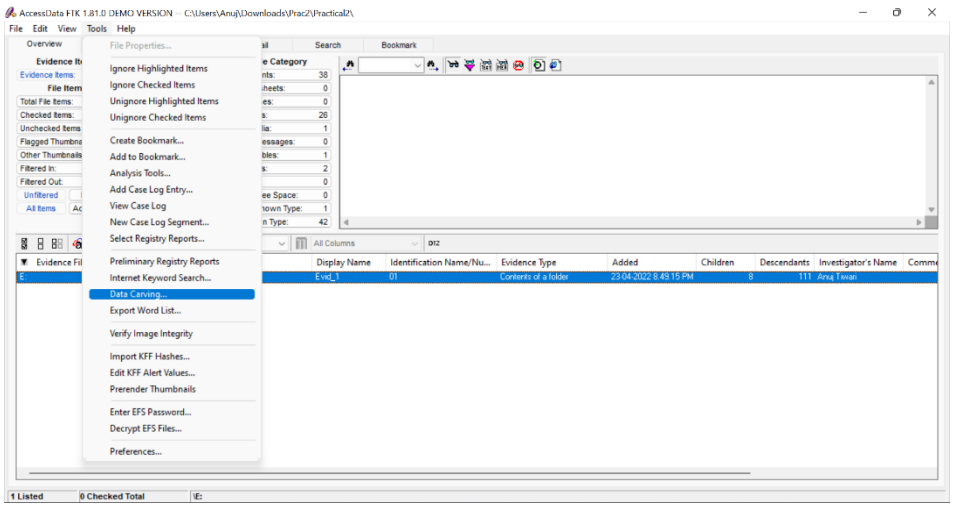
You can select to data carve when a case is added by selecting Data Carve in the Process to Perform Screen during the New Case Wizard. FTK carves data immediately after pre-processing.

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.

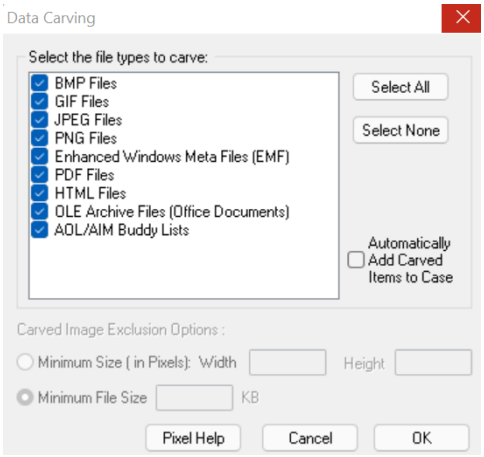
To access the cache:

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

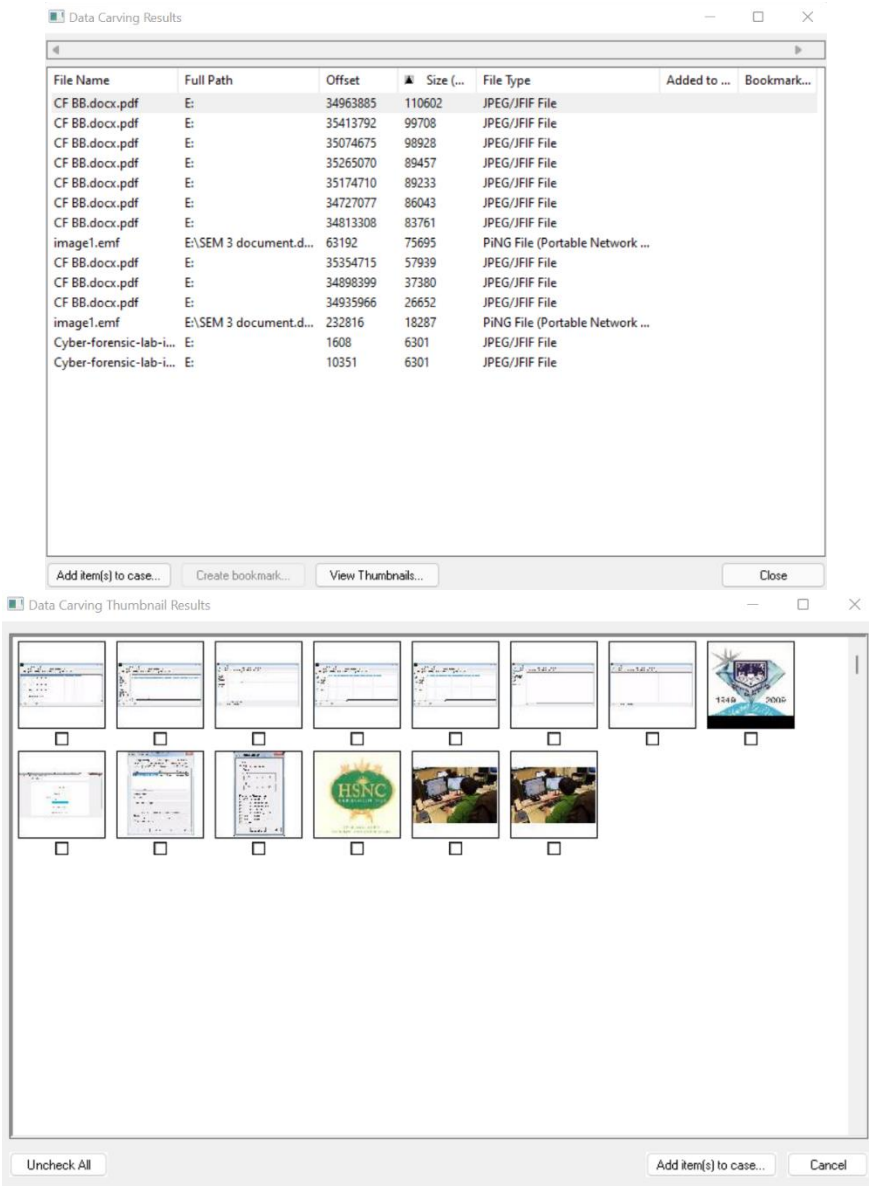




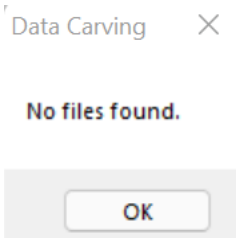
Step 2) Check the file types to carve. You can click **Select All** or **Select None** to speed up the selection process. Click **OK**.



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

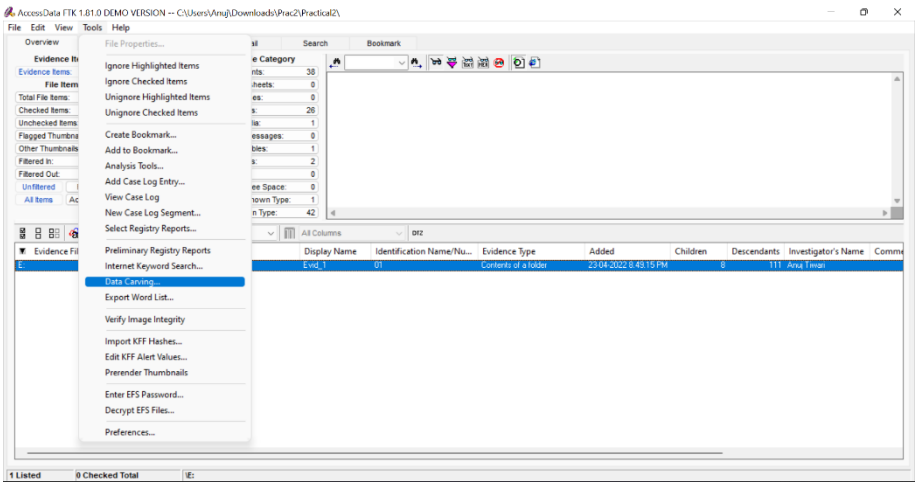


Or

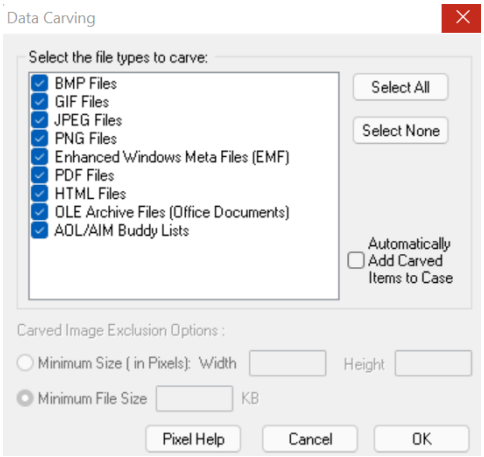


Data Carving Files in an Existing Case:
To search for embedded and deleted files:

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

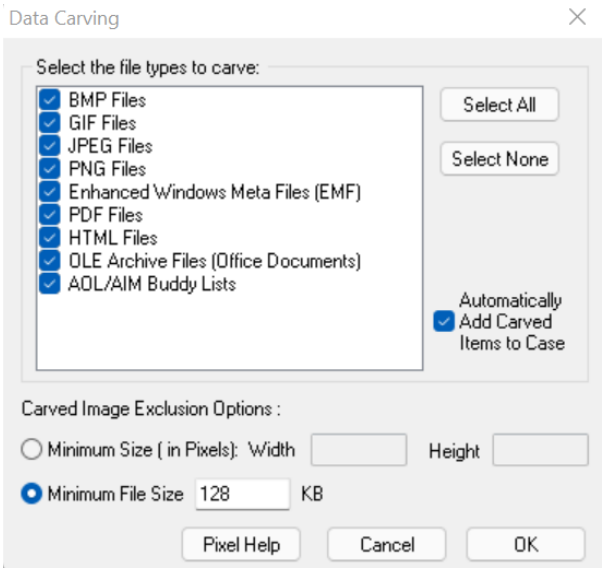


[2] Check the file types to carve. You can click **Select All** or **Select None** to speed up the selection process.



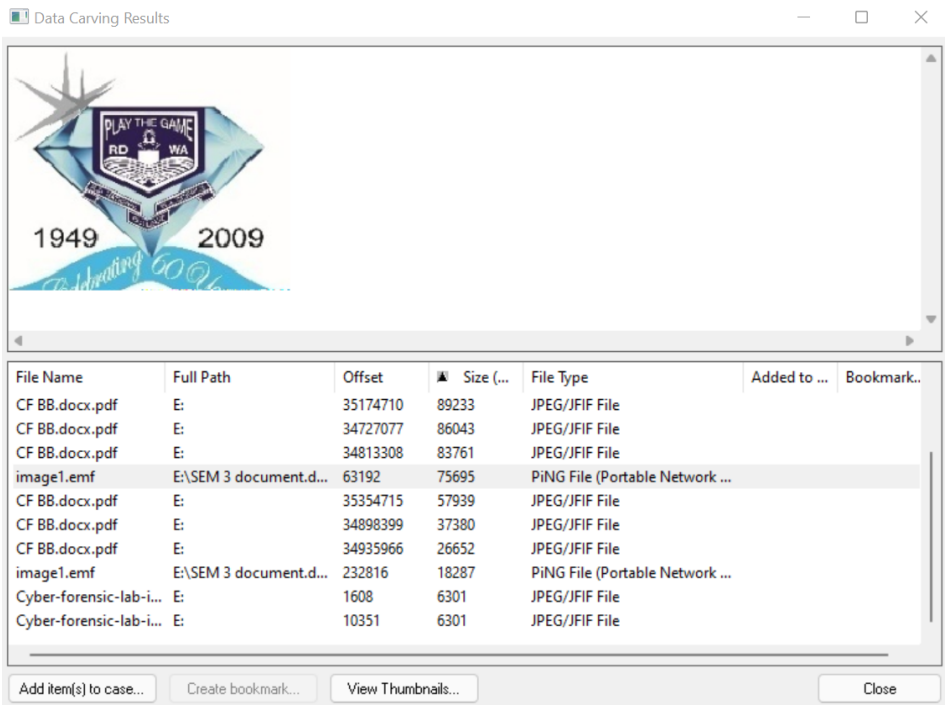
[3] (Optional) Check the **Automatically Add Carved Items to Case** option. The Minimum Image Size fields activate. 3a Specify a minimum size in pixels in which to disply images. The program will question you about minimum sizes over 480 pixels.

[4] Click **OK**.



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

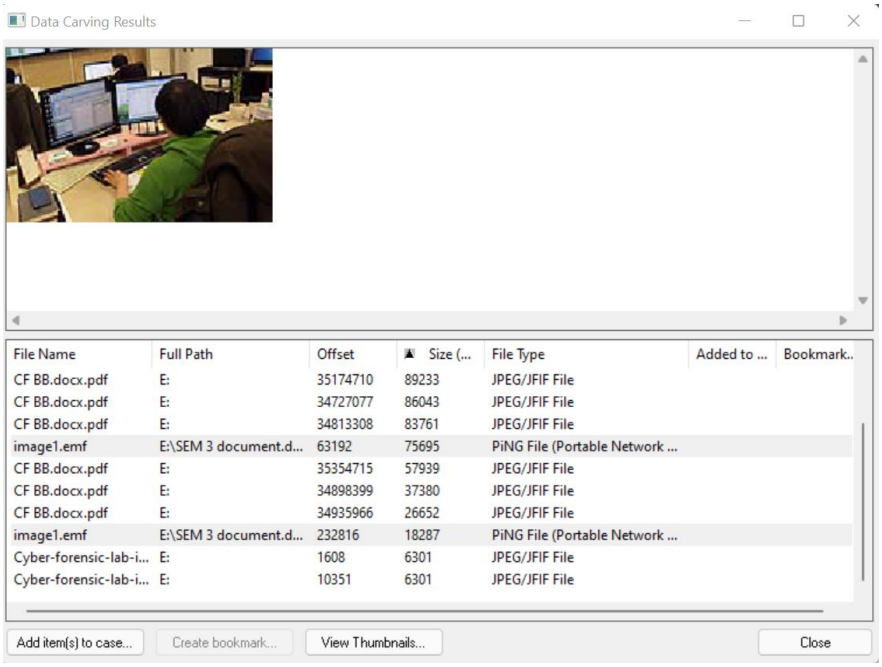
Adding Carved Files to the Case:



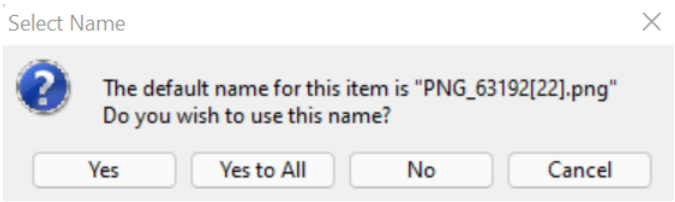
To add a carved file to the case:

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.

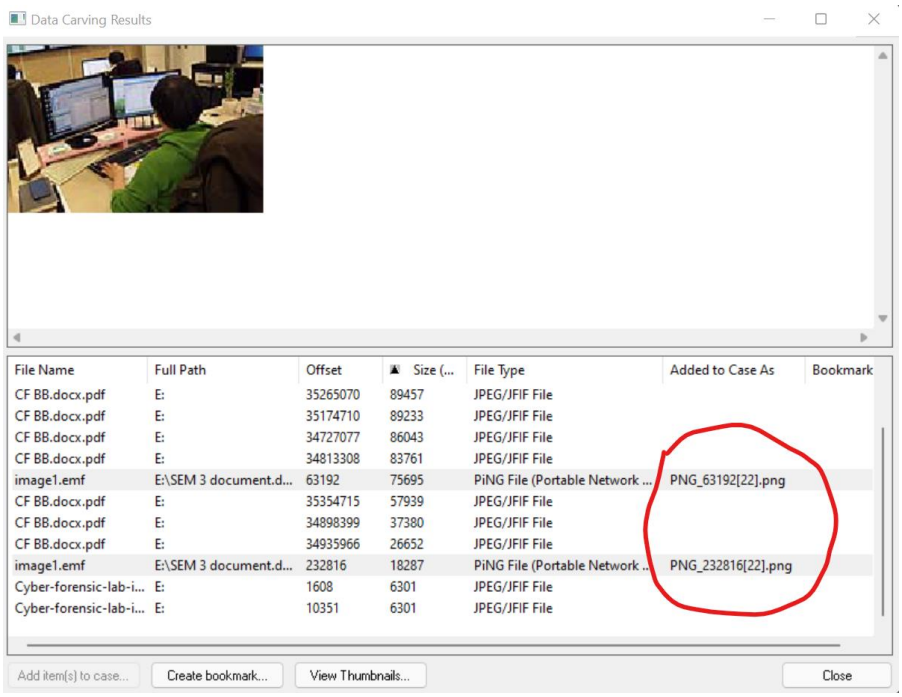
2) Click **Add Items to Case**.



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



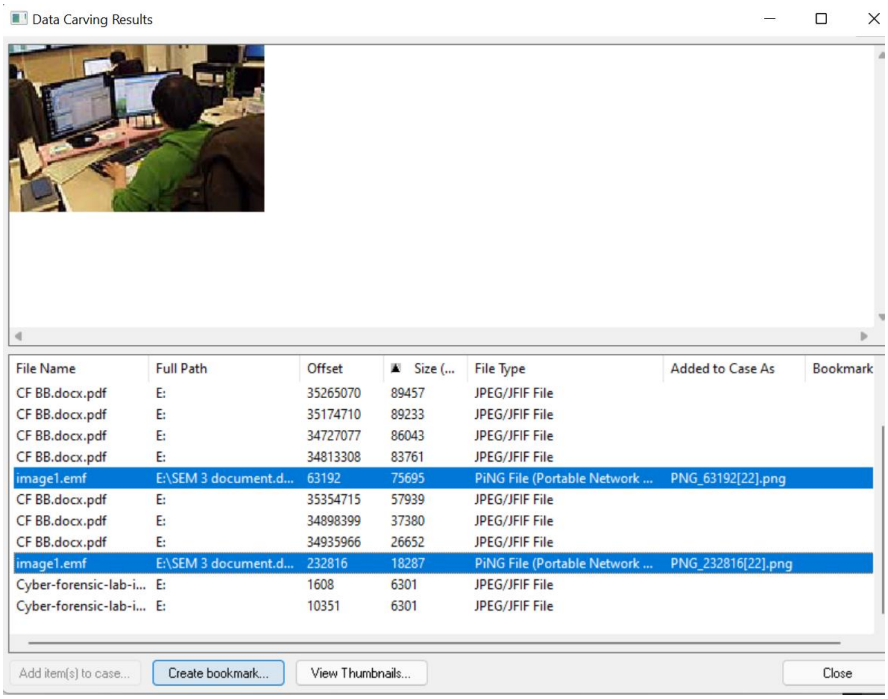
After a file is added to a case, FTK will not find it in subsequent data carving procedures. In other words, there is no redundancy. If a file is identified as case evidence, the data carving feature ignores it. The data carving feature only looks for files that are not individually identified in the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



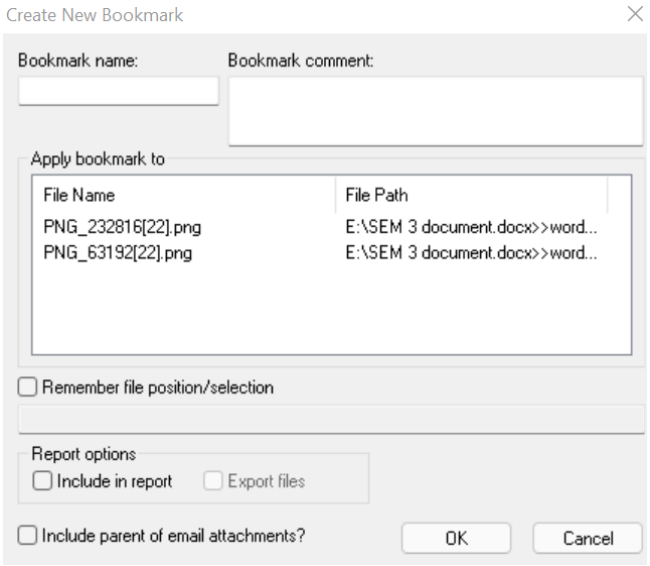
Bookmarking Carved Files:

To bookmark a carved file:

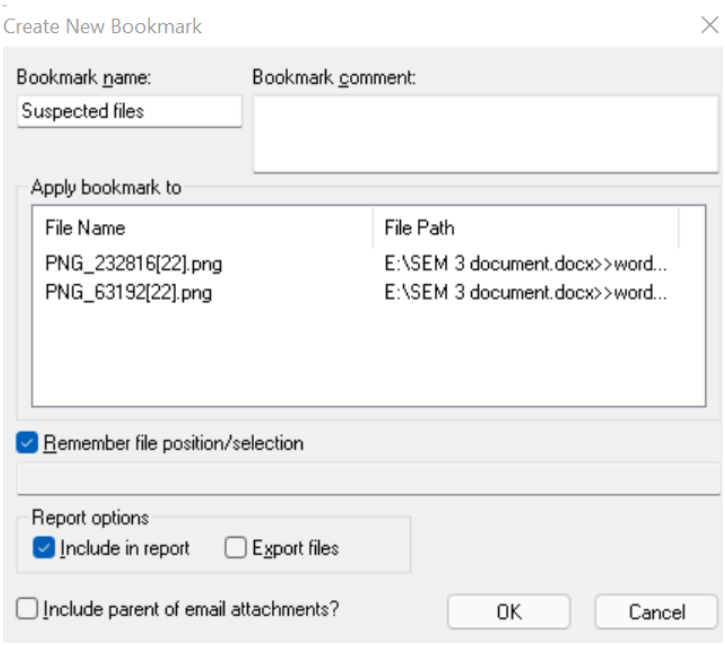
Step 1.Select the files you want to include in the bookmark and click **Create Bookmark**.



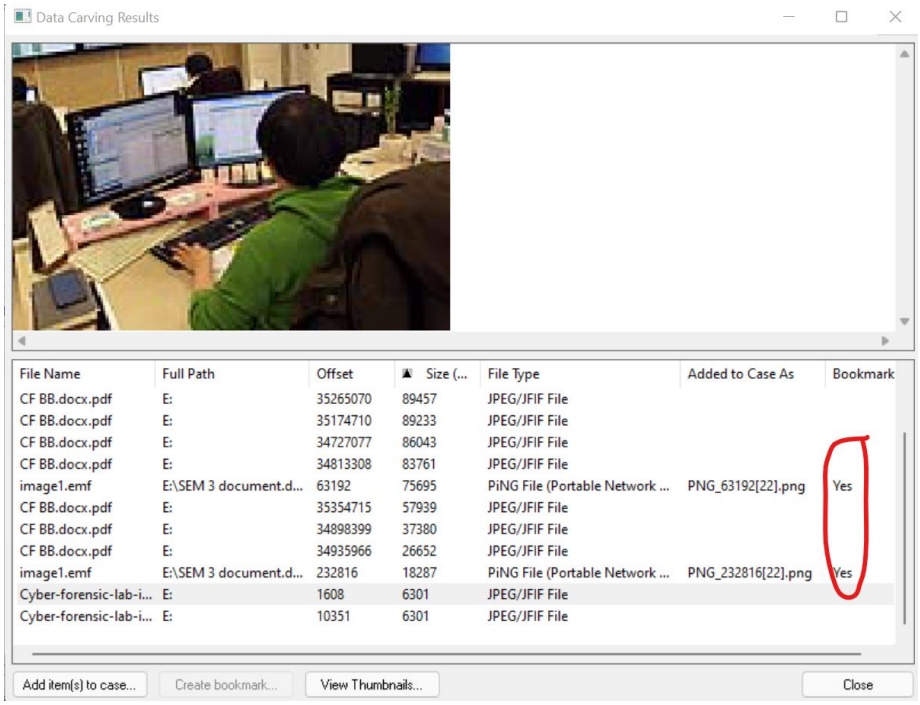
Step 2.In the Create New Bookmark form



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



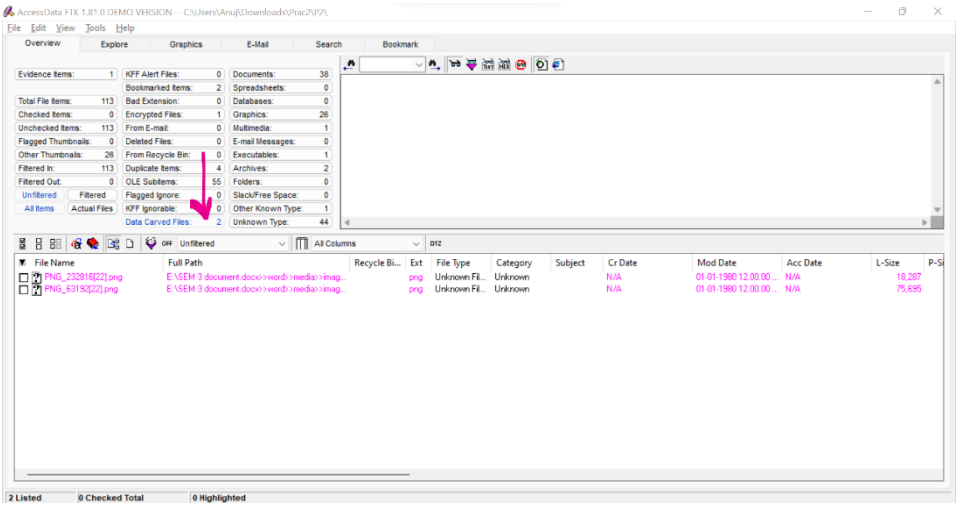
When the process is complete, the detached viewer appears with the bookmarked data carving results

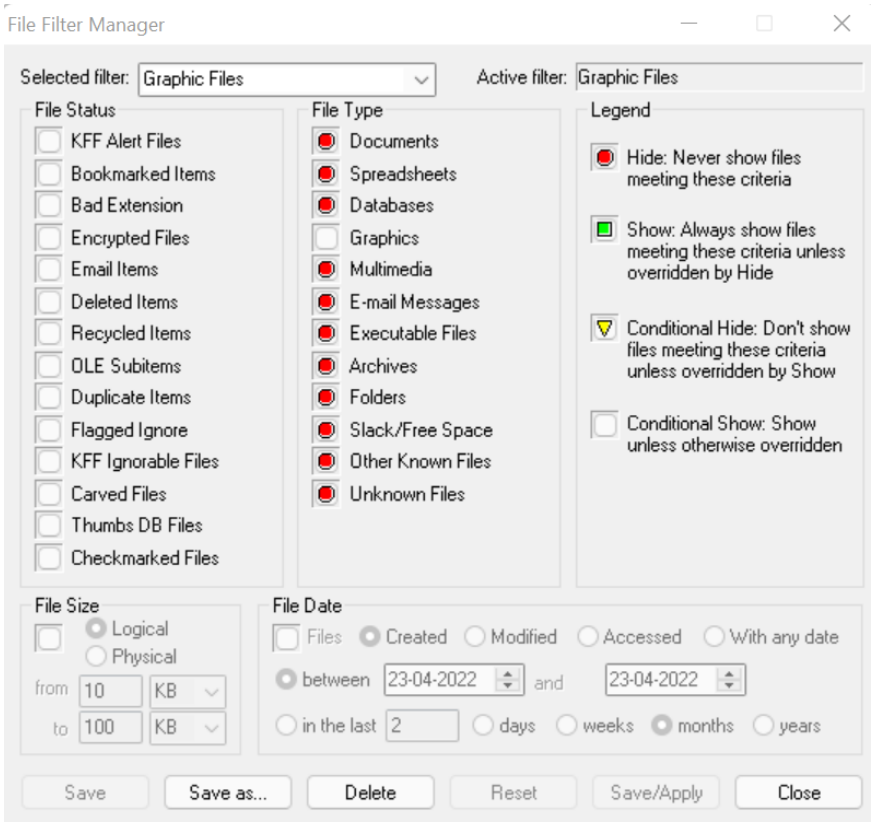


Using Filters

Applying an Existing Filter

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


File Edit View Tools Help
Overview
Explore
Graphics
E-Mail
Search
Bookmark
Evidence Items: 1
Total File Items: 113
Checked Items: 0
Unchecked Items: 113
Flagged Thumbnails: 0
Other Thumbnails: 26
Filtered In: 113
Filtered Out: 0
Unfiltered
Filtered
All Items
Actual Files
KFF Alert Files: 0
Bookmarked Items: 2
Bad Extension: 0
Encrypted Files: 1
From E-mail: 0
Deleted Files: 0
From Recycle Bin: 0
Duplicate Items: 4
OLE Subitems: 55
Flagged Ignore: 0
KFF Ignorable: 0
Data Carved Files: 2
Documents: 38
Spreadsheets: 0
Databases: 0
Graphics: 26
Multimedia: 1
E-mail Messages: 0
Executables: 1
Archives: 2
Folders: 0
Slack/Free Space: 0
Other Known Type: 1
Unknown Type: 44
Unfiltered
All Columns
File Name
Full Path
Recycle Bi...
Ext
File Type
Category
Subject
Cr Date
Mod Date
Acc Date
L-Size
2 Listed
0 Checked Total
0 Highlighted

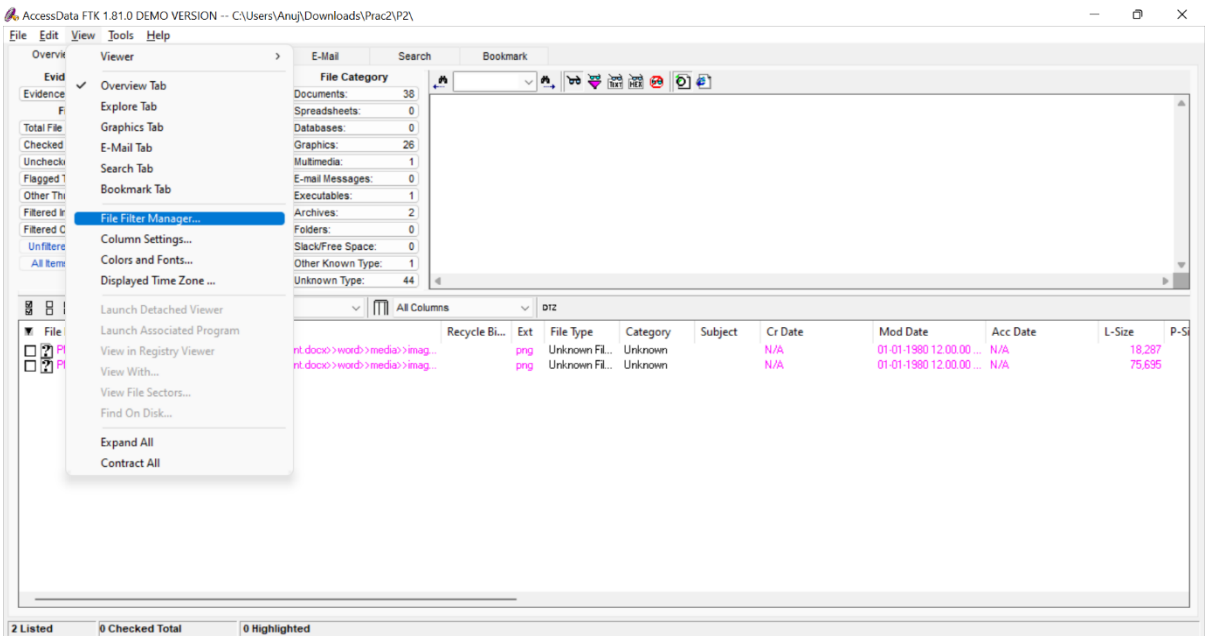

File Filter Manager
Selected filter: Graphic Files
Active filter: Graphic Files
File Status
KFF Alert Files
Bookmarked Items
Bad Extension
Encrypted Files
Email Items
Deleted Items
Recycled Items
OLE Subitems
Duplicate Items
Flagged Ignore
KFF Ignorable Files
Carved Files
Thumbs DB Files
Checkmarked Files
File Type
Documents
Spreadsheets
Databases
Graphics
Multimedia
E-mail Messages
Executable Files
Archives
Folders
Slack/Free Space
Other Known Files
Unknown Files
Legend
Hide: Never show files meeting these criteria
Show: Always show files meeting these criteria unless overridden by Hide
Conditional Hide: Don't show files meeting these criteria unless overridden by Show
Conditional Show: Show unless otherwise overridden
File Size
Logical
Physical
from 10 KB
to 100 KB
File Date
Files
Created
Modified
Accessed
With any date
between 23-04-2022 and 23-04-2022
in the last 2 days weeks months years
Save
Save as...
Delete
Reset
Save/Apply
Close

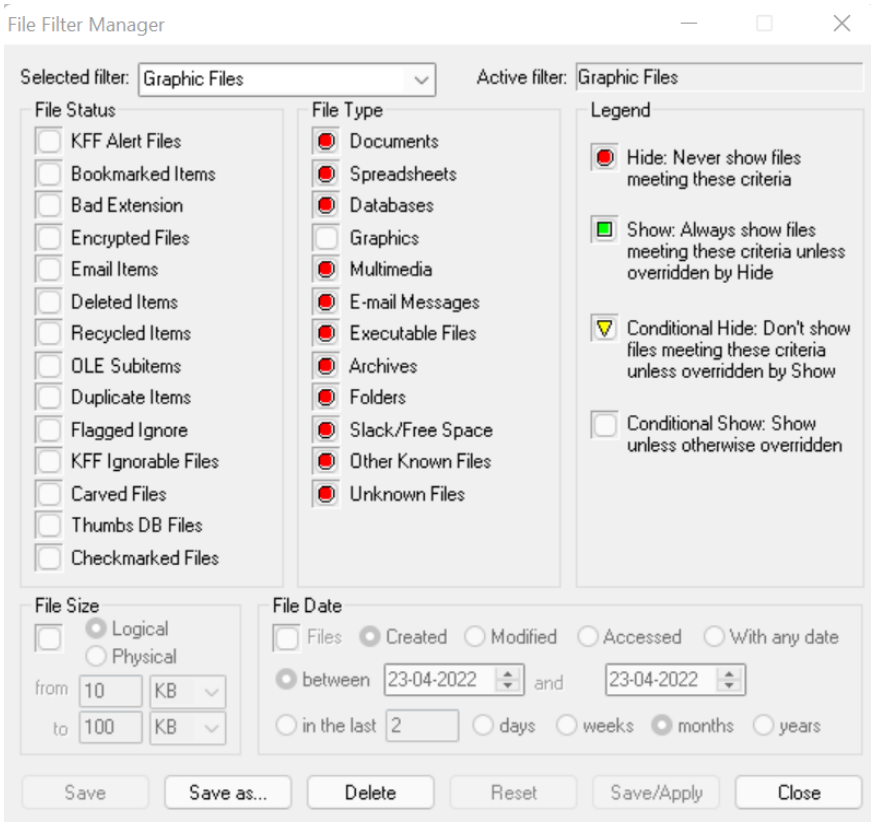
Filter	Description
E-mailed Items	Shows e-mail items such as e-mail messages, archive files, and attachments.
Encrypted Files	Shows encrypted files that are possibly in all file types.
Graphic Files	Only shows graphic files.
KFF Alert Files	Shows KFF alert files that are possibly in all file types.
No 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:

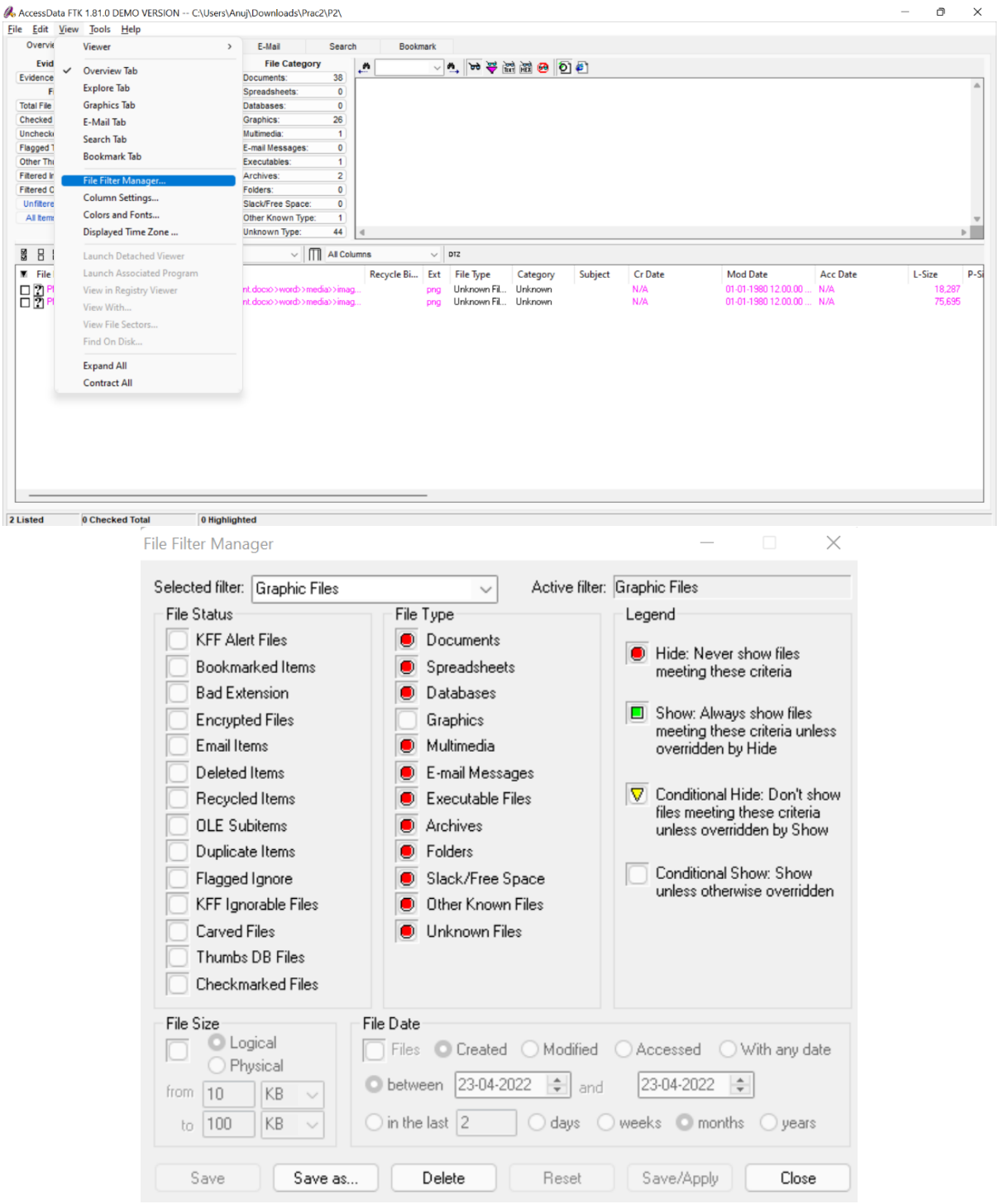
Icon	Description
	Hide: Never shows files meeting selected criteria. If you click this icon in the Legend column, all file statuses and types are marked Hide.
	Show: Always shows files meeting selected criteria unless overridden by Hide. If you click this icon in the Legend column, all file statuses 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.

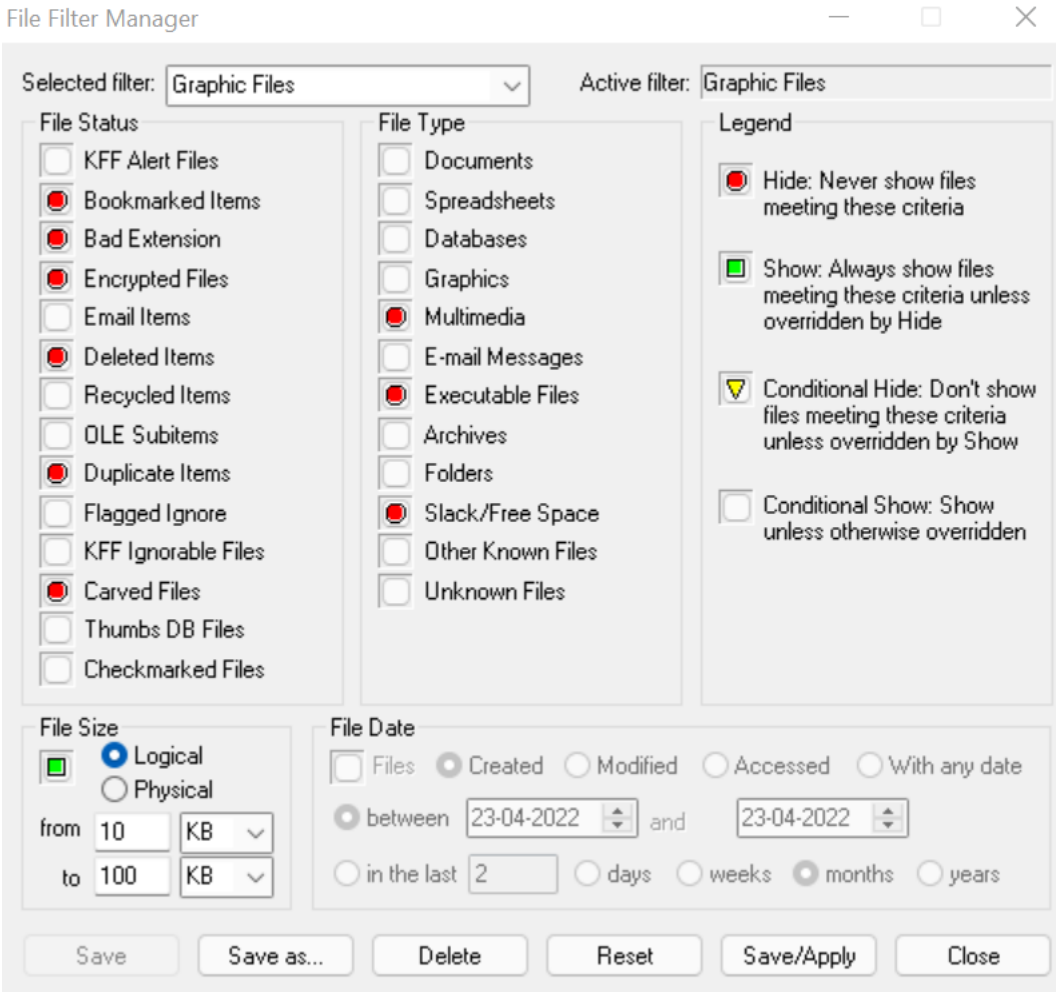
Modifying or Creating a Filter

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

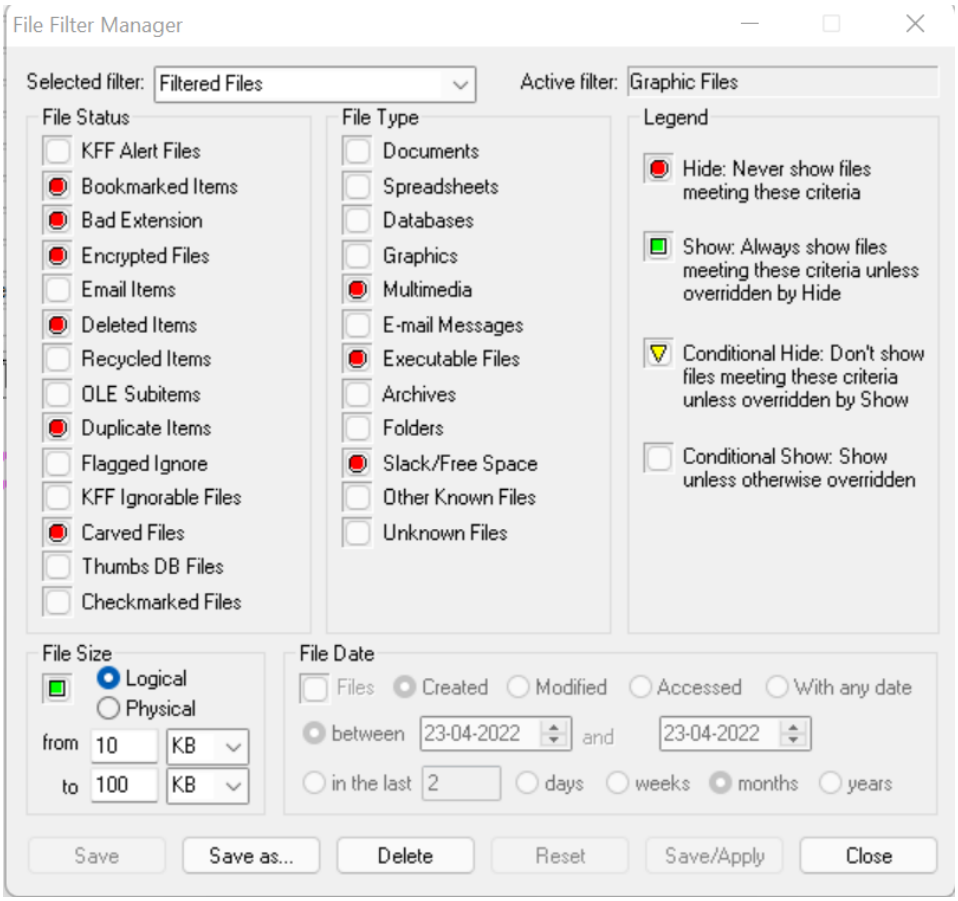
If you are creating a new filter, click **Save As**, enter the name, and click **OK**.

Deleting a Filter

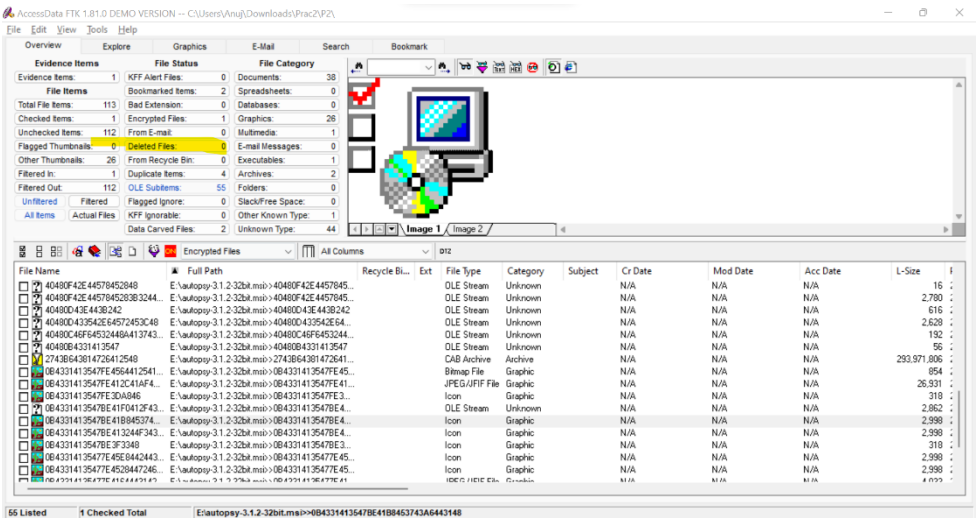
You can delete a filter if you no longer need it. To delete a filter:

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**.

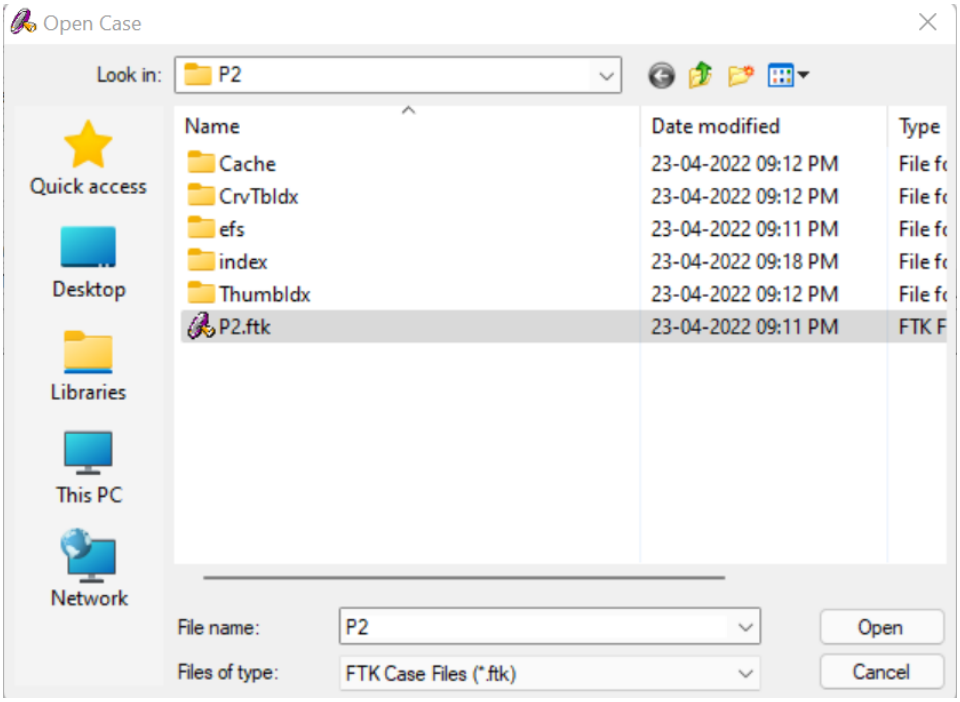
Launching Registry Viewer from FTK:

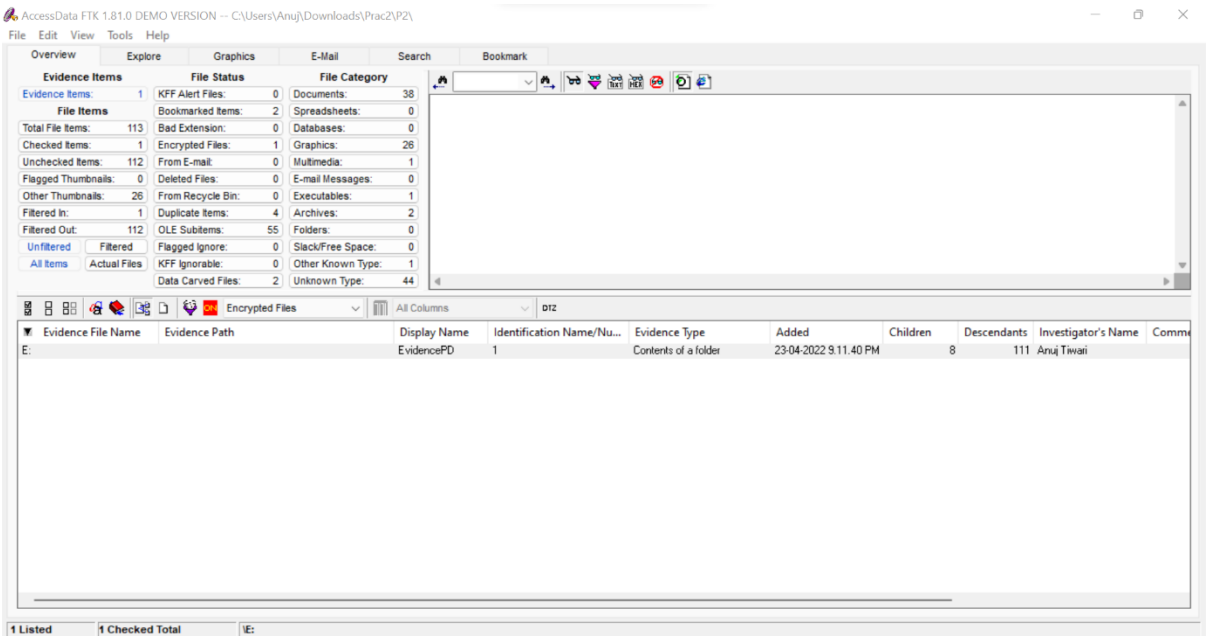
To run Registry Viewer from FTK:

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

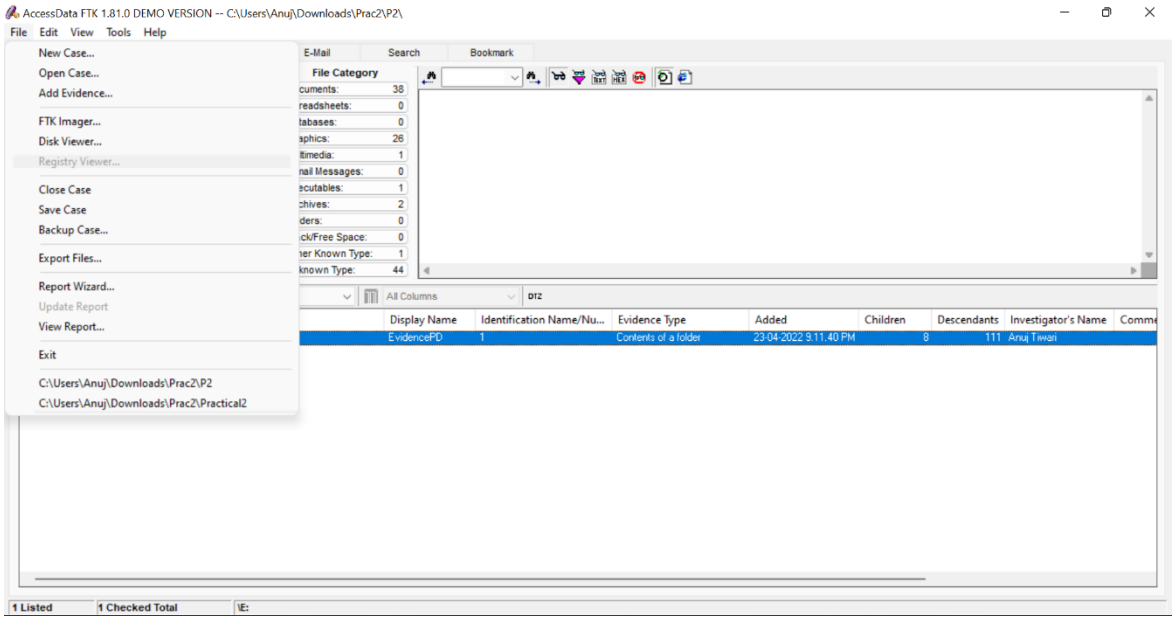
Or if you have chosen to always display the FTK Startup screen, select **Open an Existing Case** and click **OK**.

Step 2.Select the case you want to open.





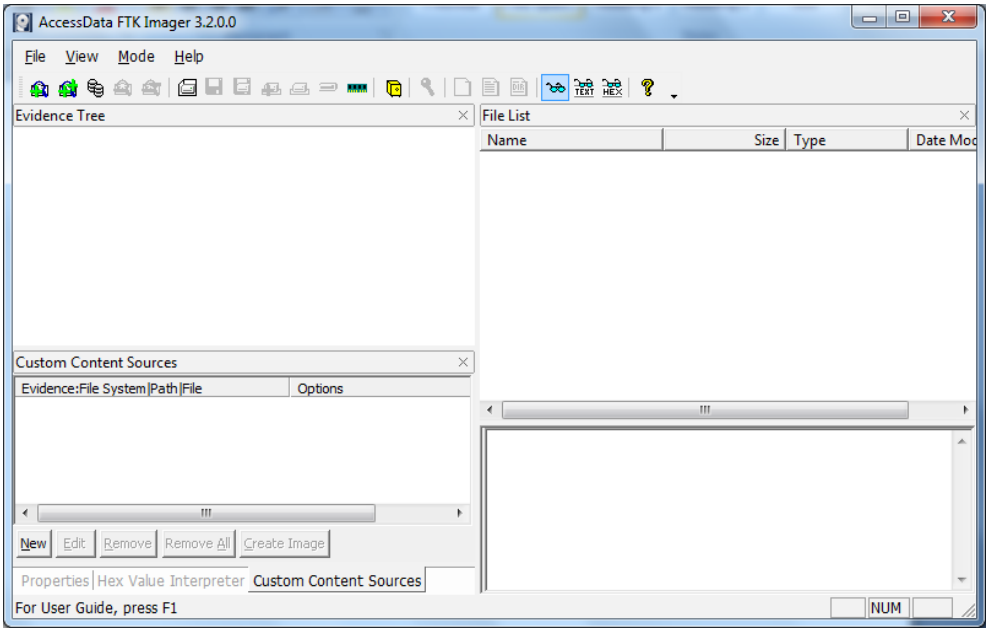
Step 3. Select **File**, and then **Registry Viewer** to open Registry Viewer.
(Can't perform ahead of this step because Registry viewer is disabled in demo version)



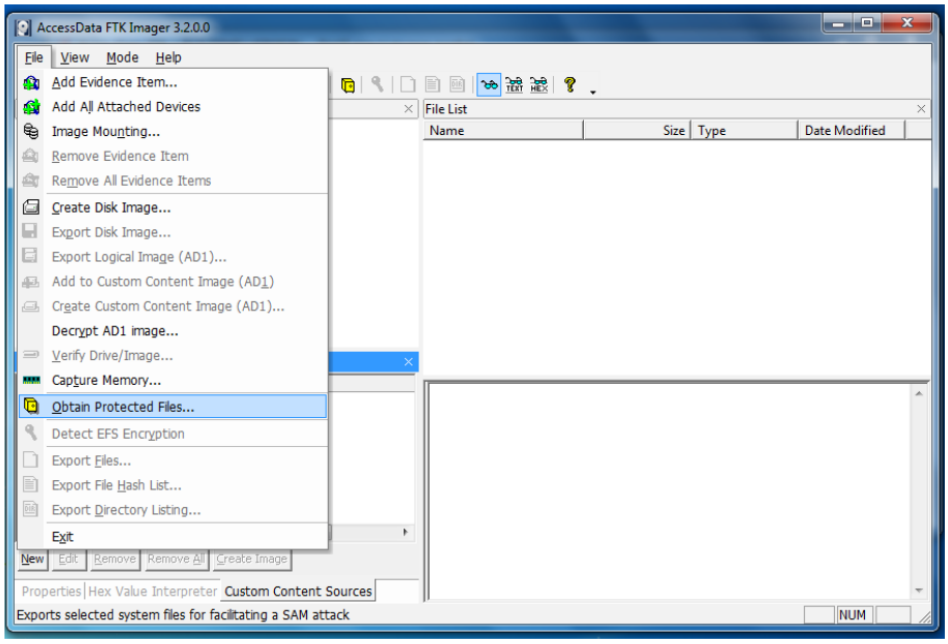
Obtaining Protected Registry Files Using FTK Imager

To obtain the protected registry files using FTK Imager:

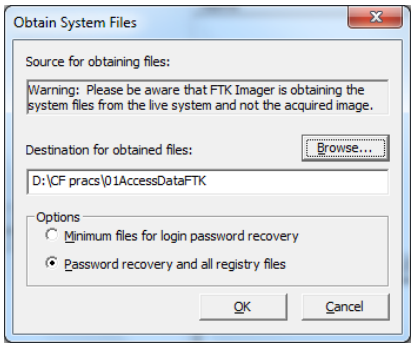
Step 1. Launch FTK Imager.

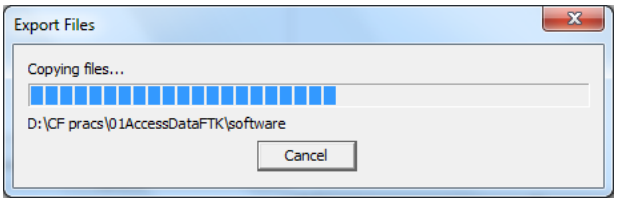


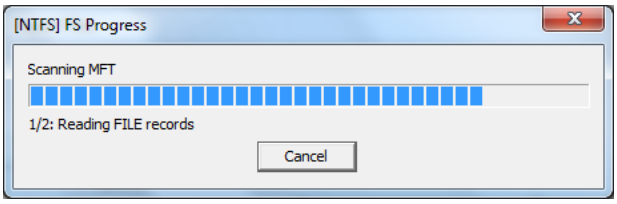
Step 2.Click **File**, and then **Obtain Protected Files**

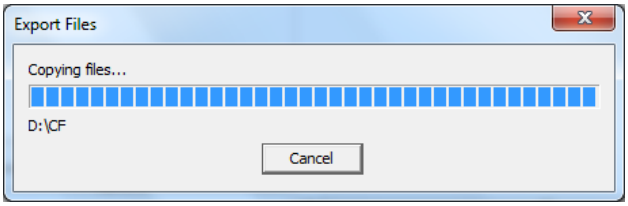


Step 3.Designate a destination directory and file options, then click **OK**.









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

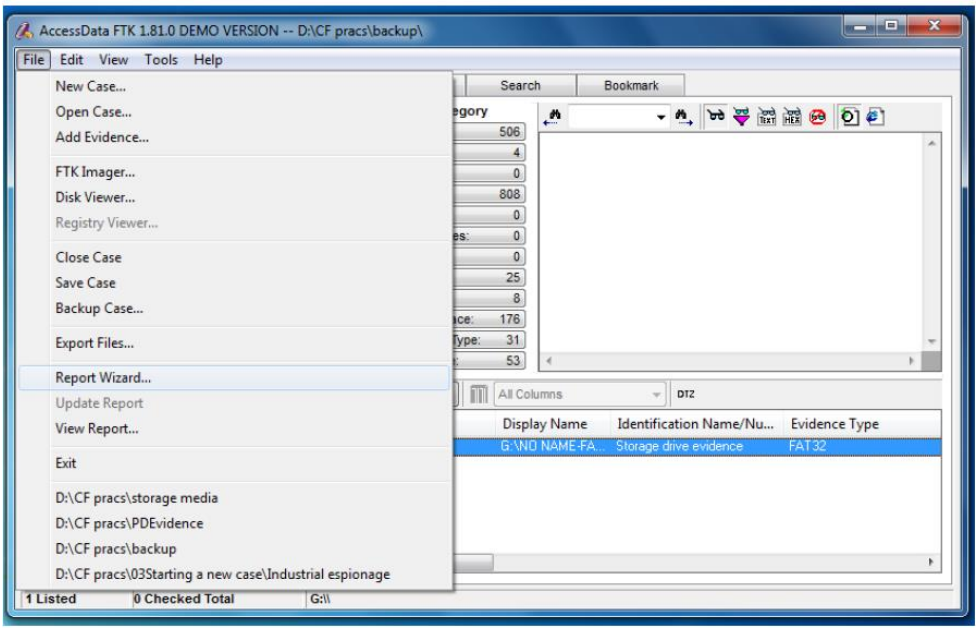
- Deleting Keys from the Report Window
- Creating Registry Summary Reports
- Using Pre-defined AccessData Templates
- Creating Your Own Registry Report Templates
- Changing RSR Settings in the FtkSettings.0.ini File

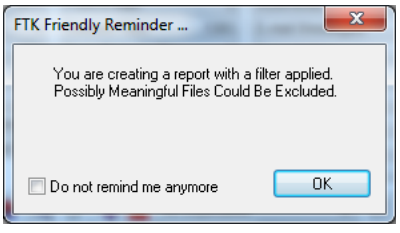
❖ **Searching for Specific Data**

Generating a Report

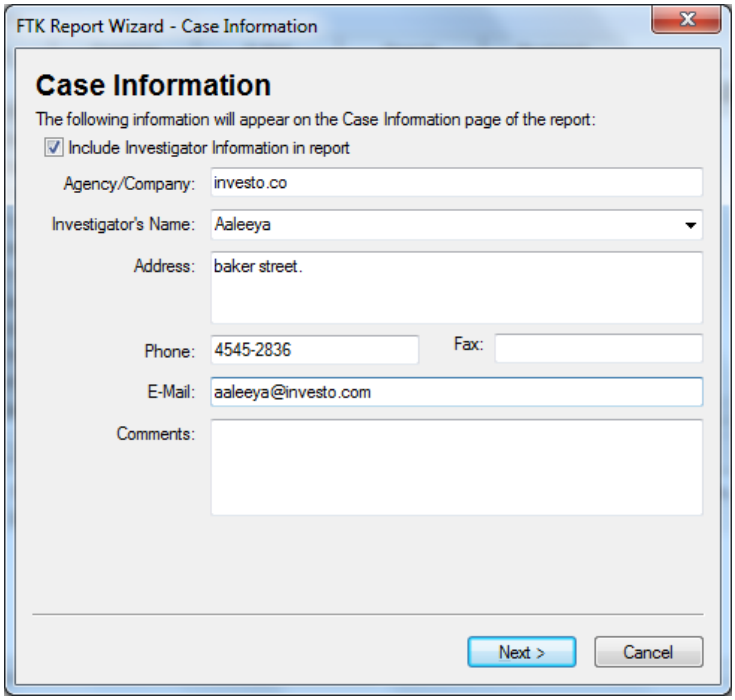
To generate a report file,

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

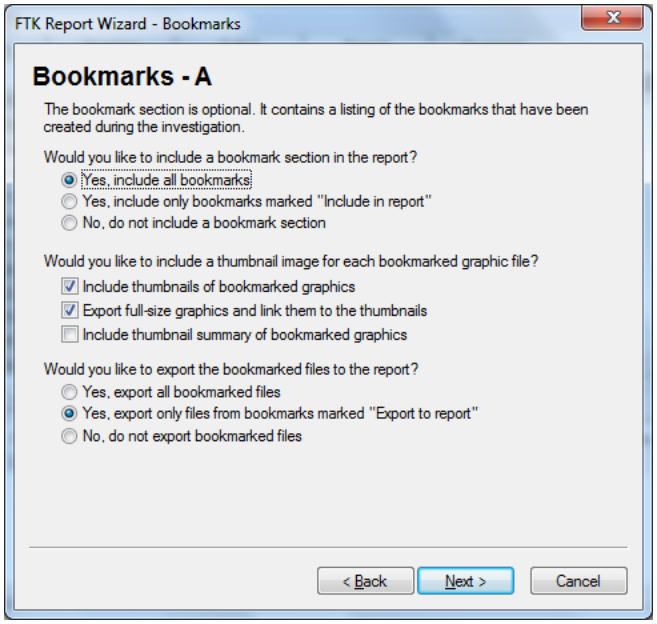




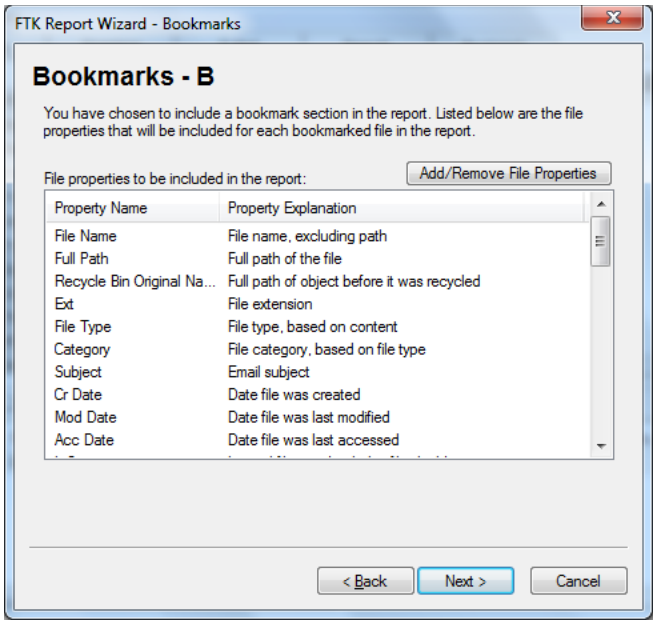
2. The Case Information dialog appears.



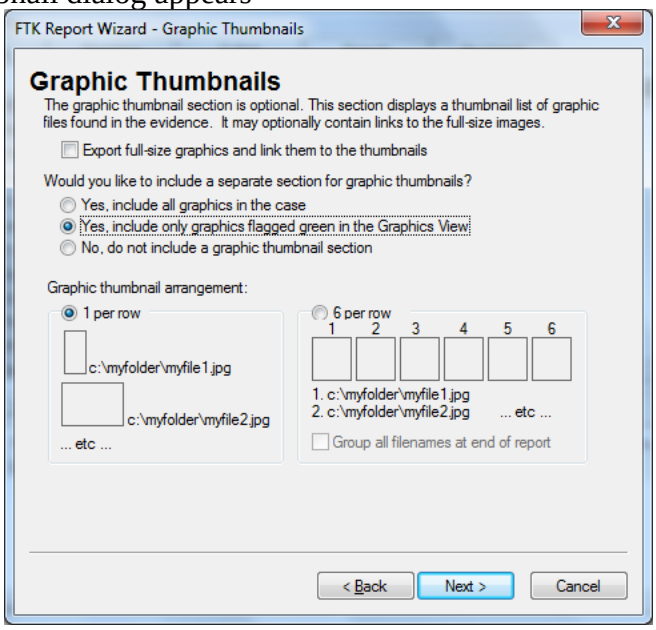
3. The Bookmarks-A dialog appears.



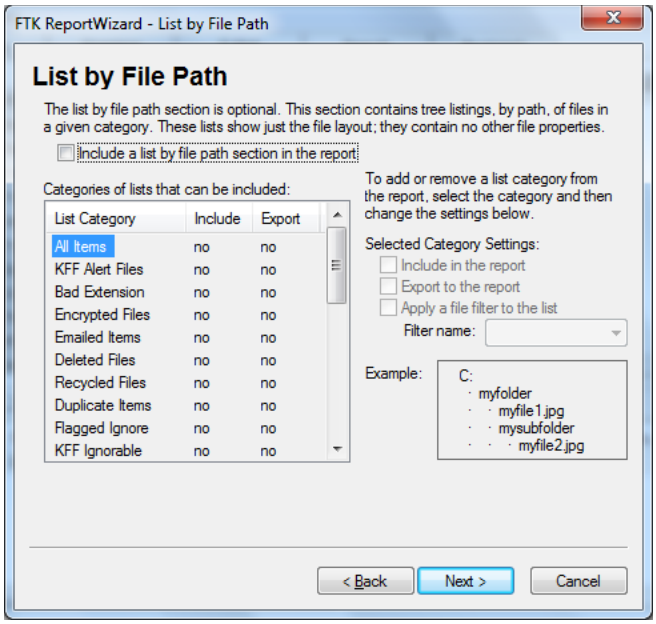
4.The Bookmarks-B dialog appears



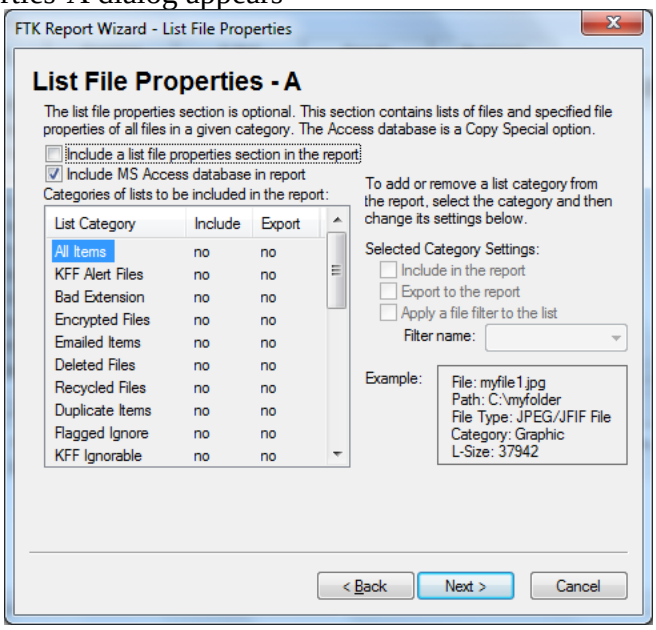
5. The Graphics Thumbnail dialog appears

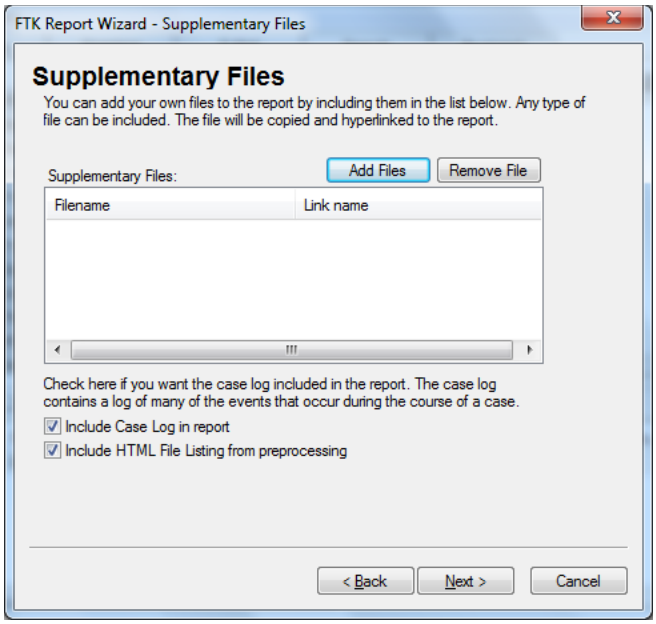


6. The List by File Path dialog appears

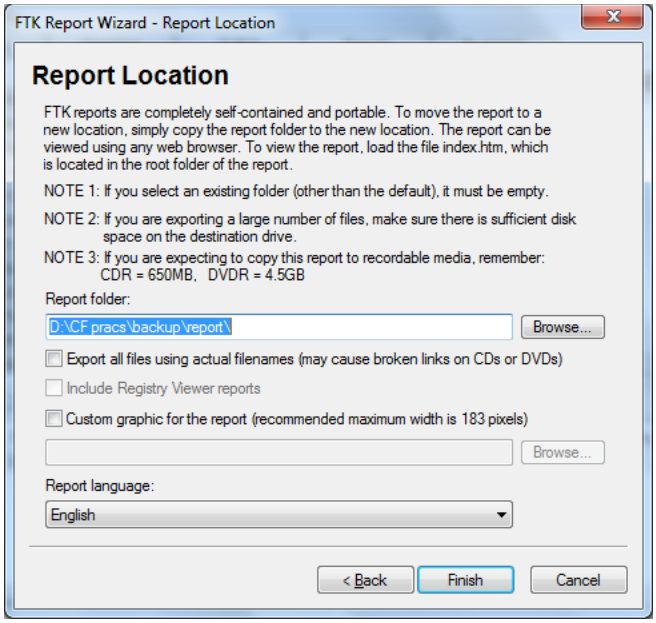


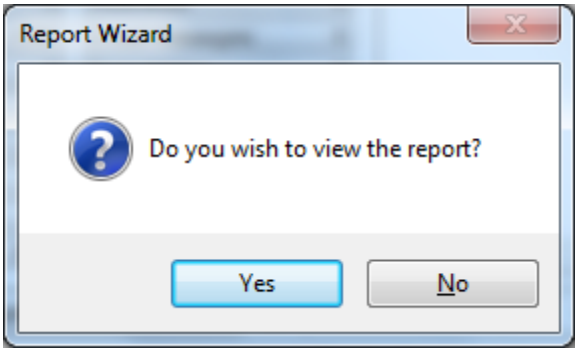
7. Then List File Properties-A dialog appears

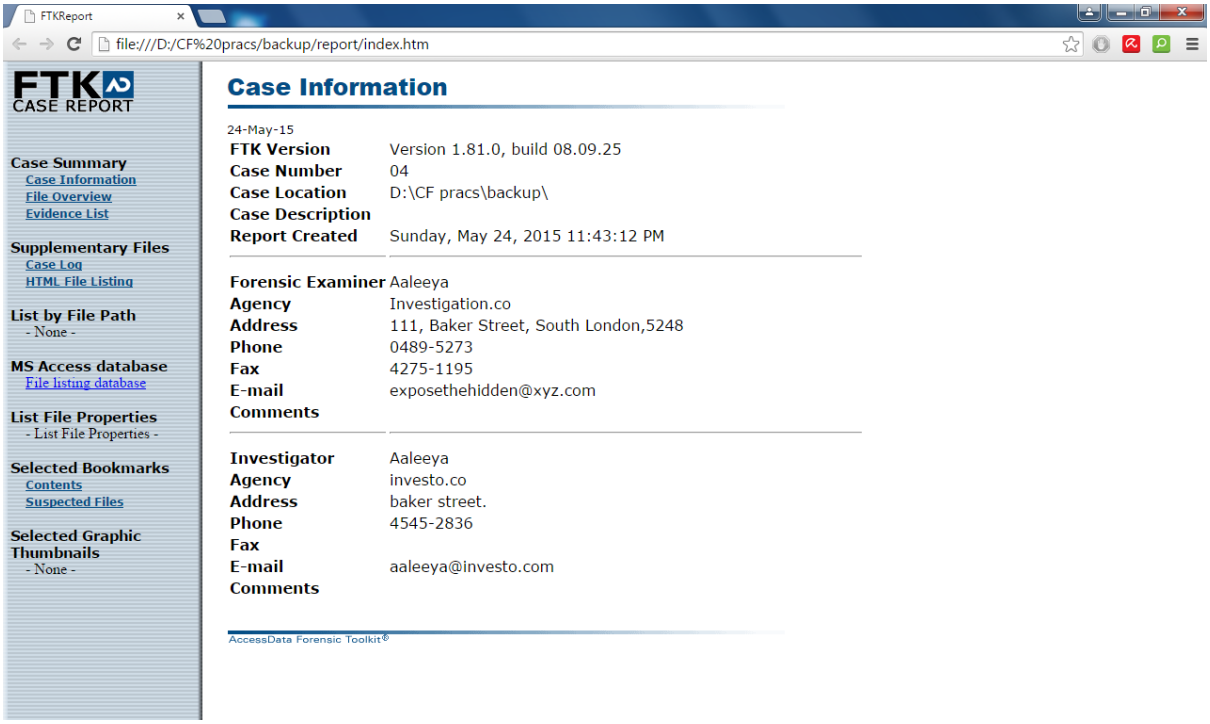


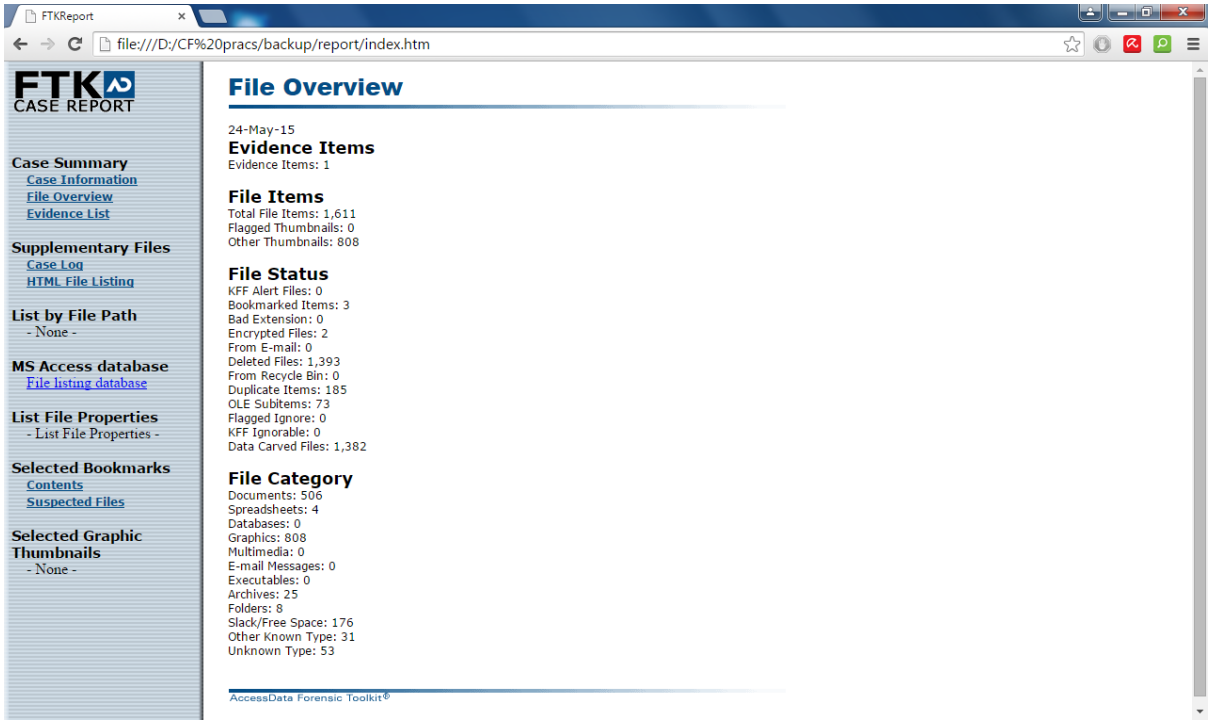


8.The Create Report dialog appears. In the Report Title field, enter a name for the report file. In the Report Location field, enter the location where you want to save the report file or click **Browse** to navigate to the desired location.




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


FTKReport
file:///D:/CF%20pracs/backup/report/index.htm
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
Suspected Files
Selected Graphic Thumbnails
- None -
Case Information
24-May-15
FTK Version Version 1.81.0, build 08.09.25
Case Number 04
Case Location D:\CF pracs\backup\
Case Description
Report Created Sunday, May 24, 2015 11:43:12 PM
Forensic Examiner Aaleeya
Agency Investigation.co
Address 111, Baker Street, South London,5248
Phone 0489-5273
Fax 4275-1195
E-mail exposethehidden@xyz.com
Comments
Investigator Aaleeya
Agency investo.co
Address baker street.
Phone 4545-2836
Fax
E-mail aaleeya@investo.com
Comments
AccessData Forensic Toolkit®


FTKReport
file:///D:/CF%20pracs/backup/report/index.htm
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
Suspected Files
Selected Graphic Thumbnails
- None -
File Overview
24-May-15
Evidence Items
Evidence Items: 1
File Items
Total File Items: 1,611
Flagged Thumbnails: 0
Other Thumbnails: 808
File Status
KFF Alert Files: 0
Bookmarked Items: 3
Bad Extension: 0
Encrypted Files: 2
From E-mail: 0
Deleted Files: 1,393
From Recycle Bin: 0
Duplicate Items: 185
OLE Subitems: 73
Flagged Ignore: 0
KFF Ignorable: 0
Data Carved Files: 1,382
File Category
Documents: 506
Spreadsheets: 4
Databases: 0
Graphics: 808
Multimedia: 0
E-mail Messages: 0
Executables: 0
Archives: 25
Folders: 8
Slack/Free Space: 176
Other Known Type: 31
Unknown Type: 53
AccessData Forensic Toolkit®

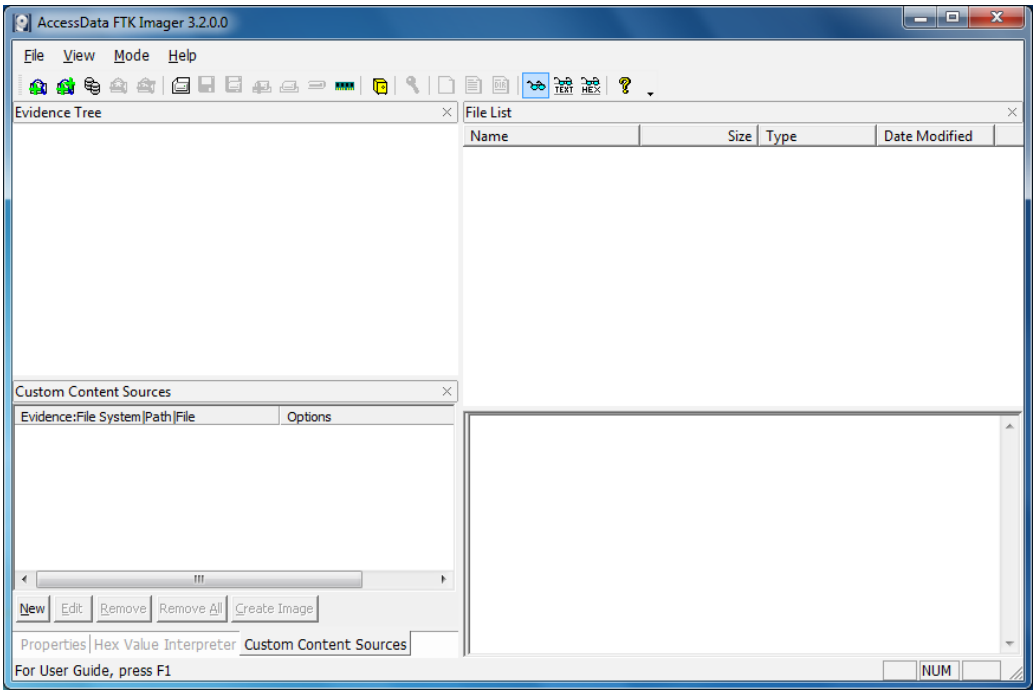
Practical No: 03

Practical No: 03

Using File recovery Tools

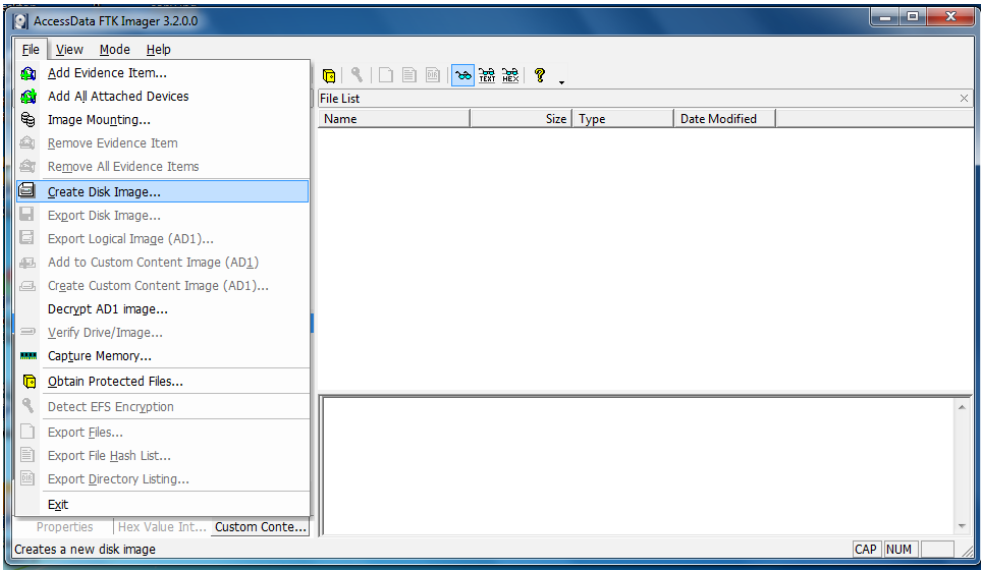
Aim: Understanding & working with the process of the process of taking a drive image using AccessData's FTK Imager tool.

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



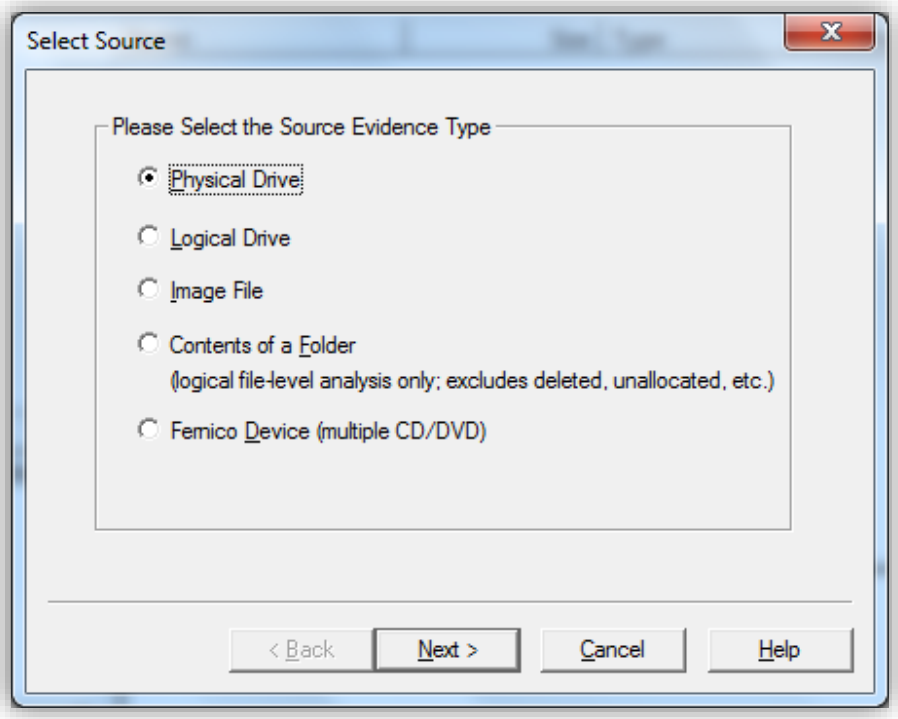
Step 2) To create a forensic image:

Click File > Create Disk Image

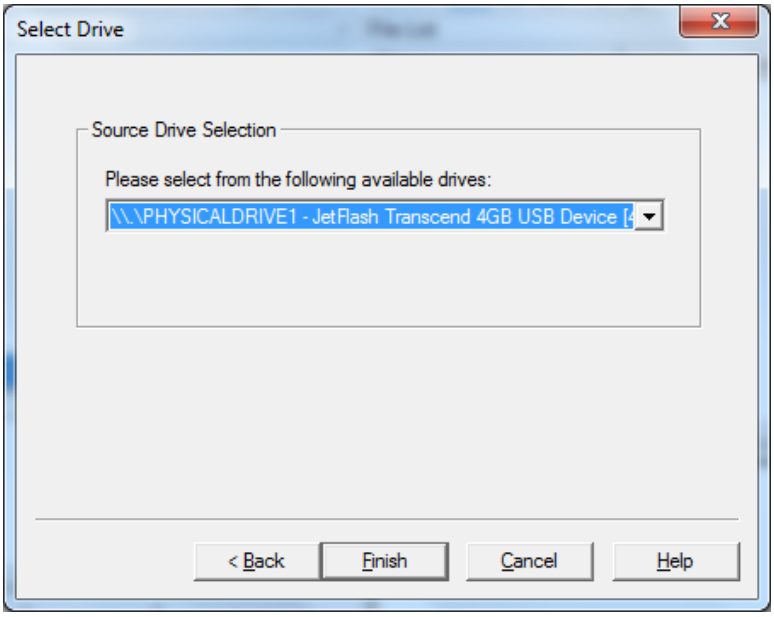


Step 3) In the Select Source dialog box, select the source you want to make an image of. Click Next.

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.



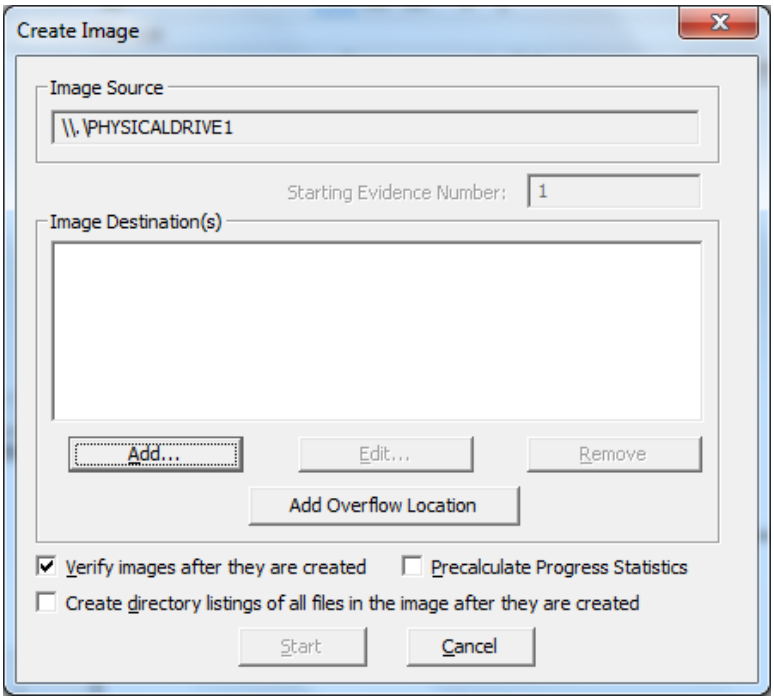
Step 4) Select the drive or browse to the source of the image you want, and then click Finish.



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.

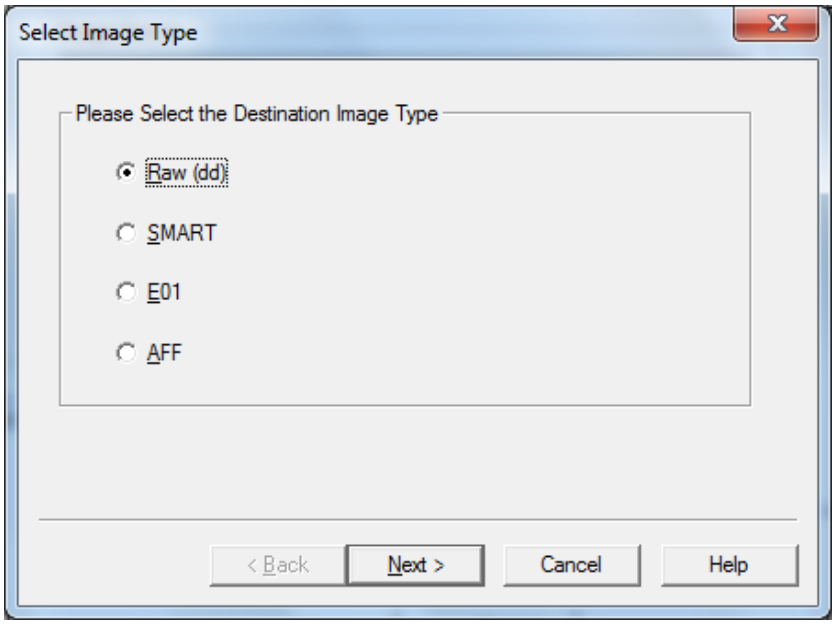


Step 6) Select the type of image you want to create.

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.

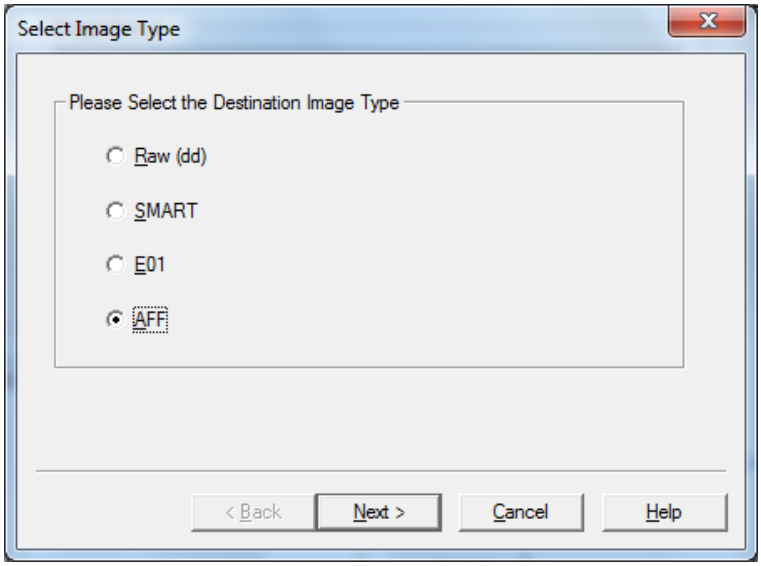
Note: If you are creating an image of a CD or DVD, this step is skipped because all CD/DVD images are created in the IsoBuster CUE format. Hashes are not generated for CD and DVD images so they will not be verified, as well.

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.

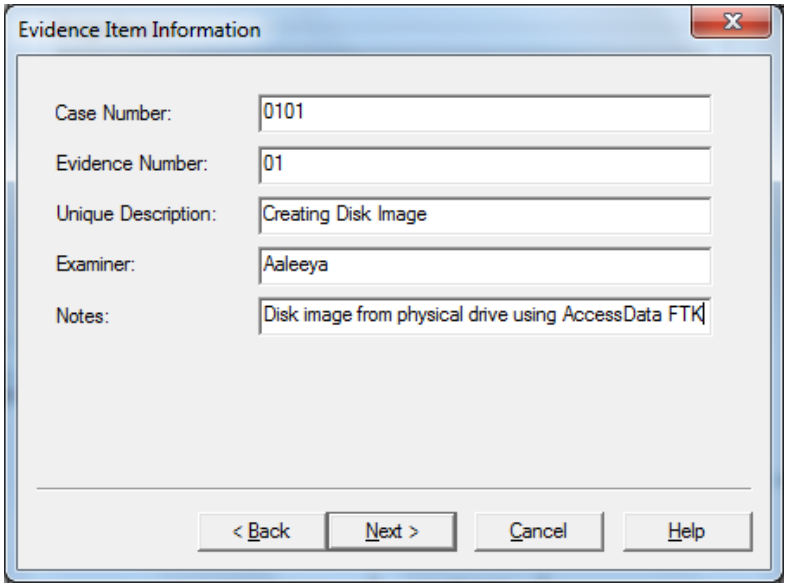


Step 7) If you are creating an AFF image type, choose AFF. Click Next.

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



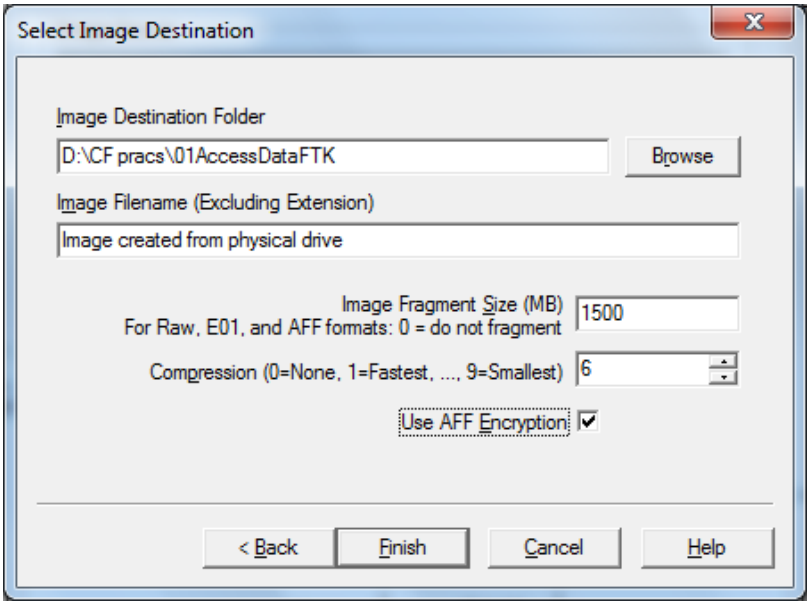
Complete the fields in the Evidence Item Information dialog. Click Next.

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.

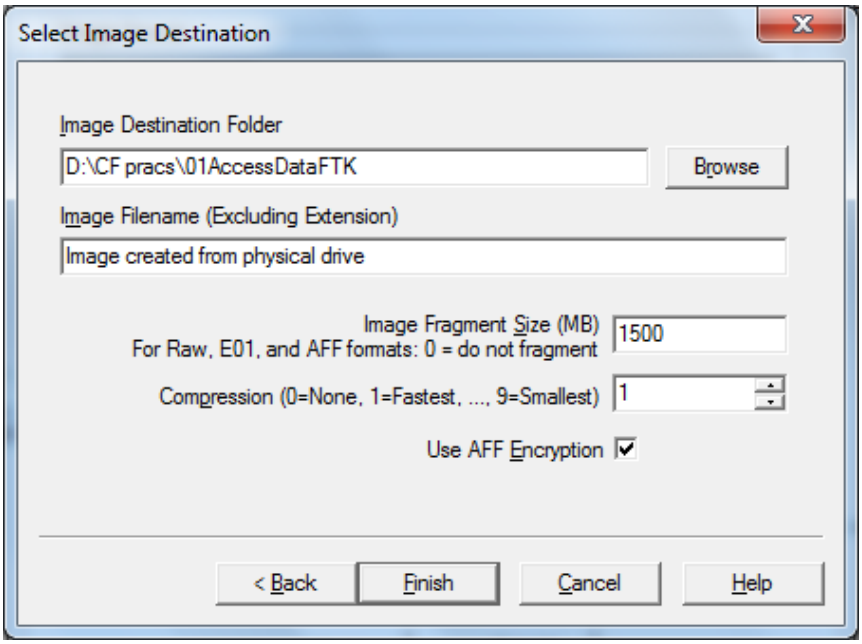
Step 10 a) Select the compression level to use.

- 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).

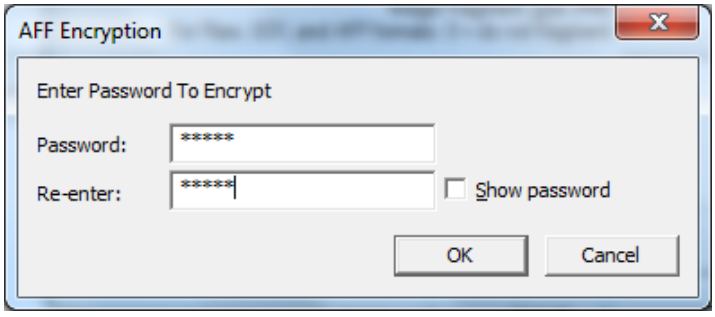
Numbers between 1 and 9 produce an image with varying levels of compression to speed ratio.

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.

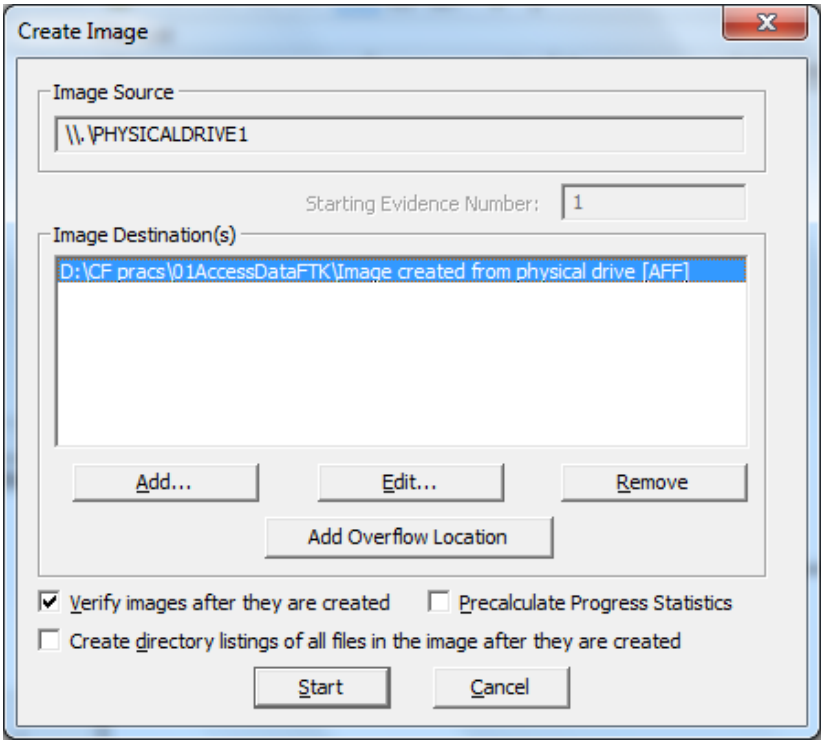
Step 12) Click Finish.

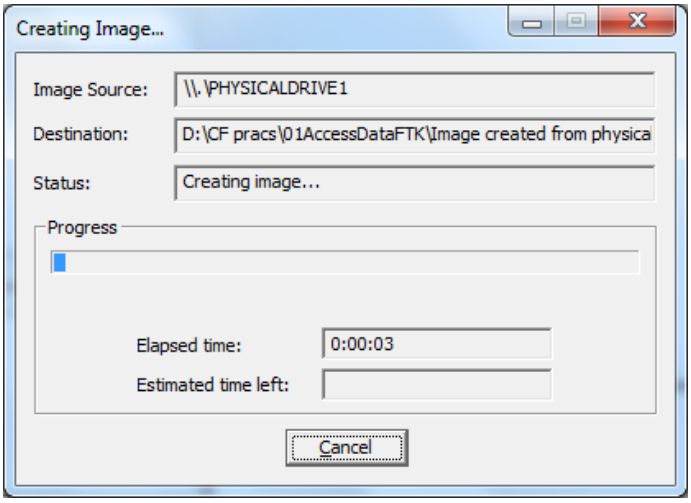


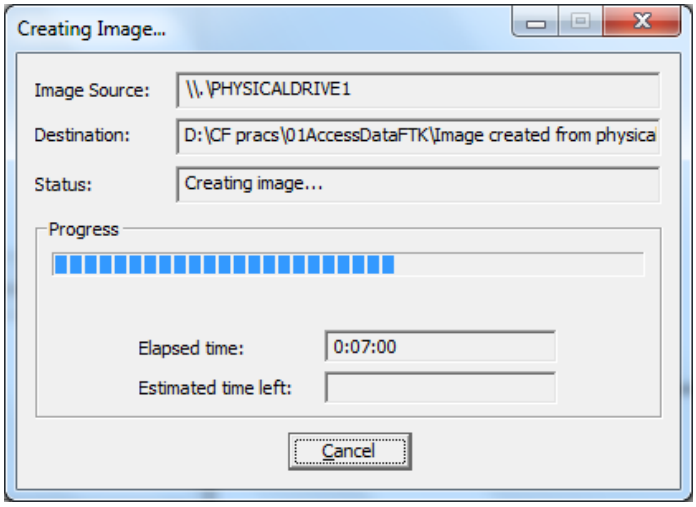
Step 13) When AFF Encryption is selected, type the password, and retype the password to confirm. Click Show Password to see that you have typed it correctly the first time.

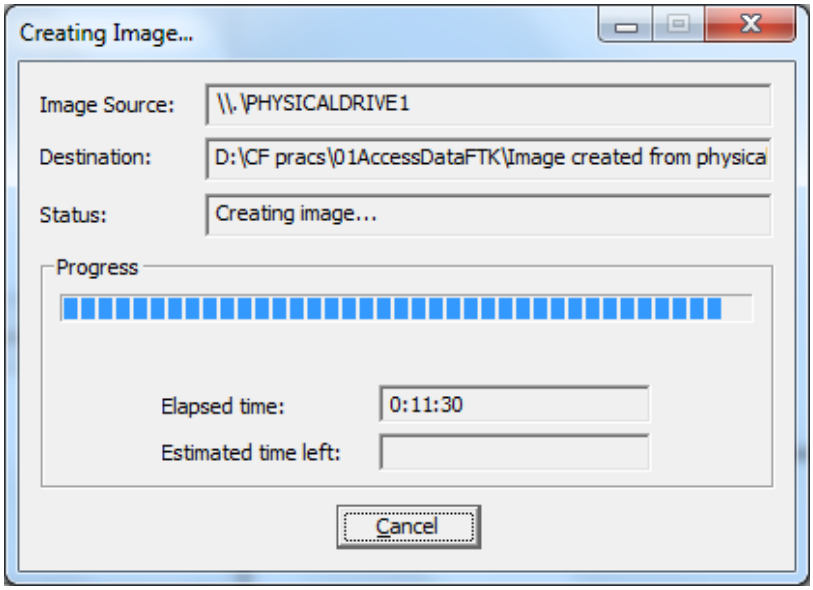


Step 14) When encryption selections are made, click **OK** to save selections and return to the **Create Image dialog.** Click **Start** to begin the imaging process.

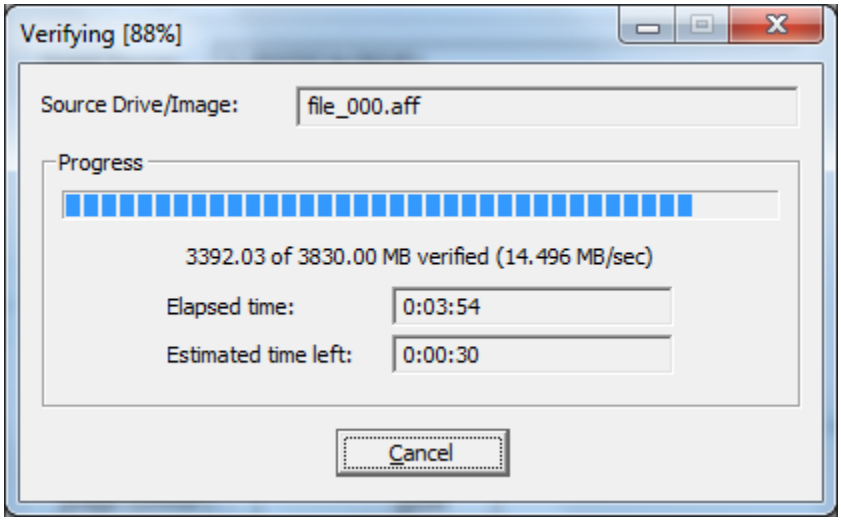

Create Image
Image Source
\\.\PHYSICALDRIVE1
Starting Evidence Number:
1
Image Destination(s)
D:\CF pracs\01AccessDataFTK\Image created from physical drive [AFF]
Add...
Edit...
Remove
Add Overflow Location
Verify images after they are created
Precalculate Progress Statistics
Create directory listings of all files in the image after they are created
Start
Cancel


Creating Image...
Image Source:
\\.\PHYSICALDRIVE1
Destination:
D:\CF pracs\01AccessDataFTK\Image created from physica
Status:
Creating image...
Progress
Elapsed time:
0:00:03
Estimated time left:
Cancel

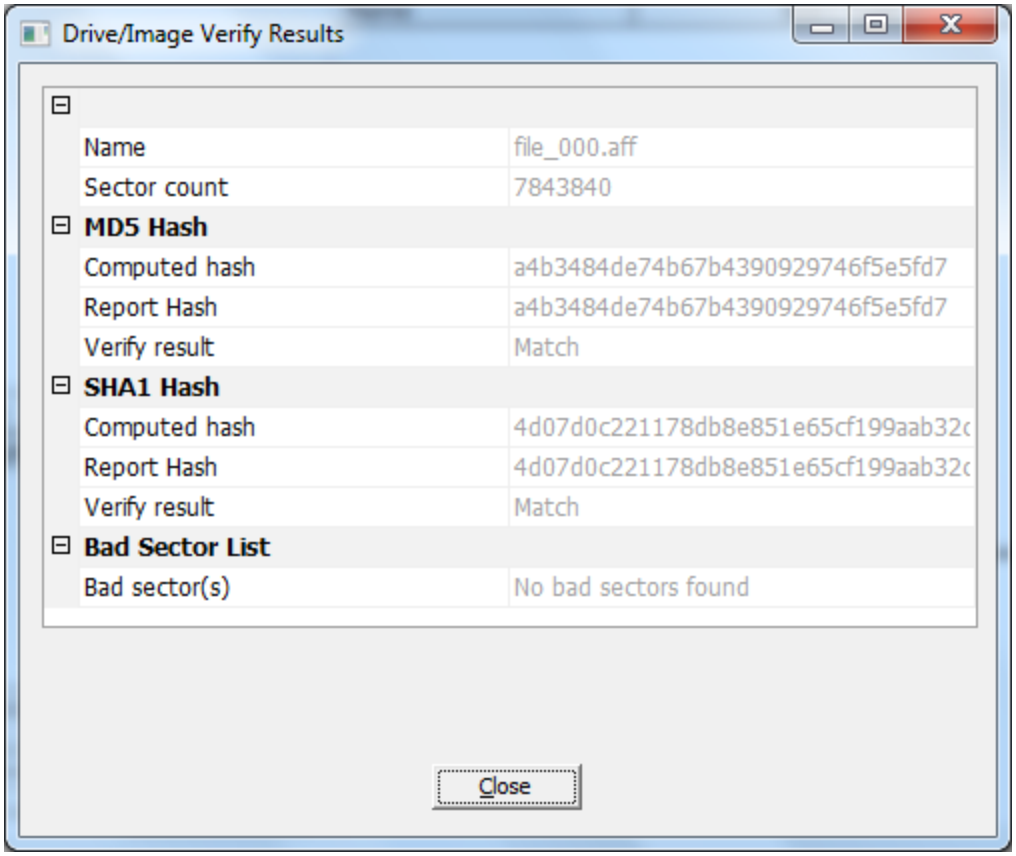

Creating Image...
Image Source:
\\.\PHYSICALDRIVE1
Destination:
D:\CF pracs\01AccessDataFTK\Image created from physica
Status:
Creating image...
Progress
Elapsed time:
0:07:00
Estimated time left:
Cancel

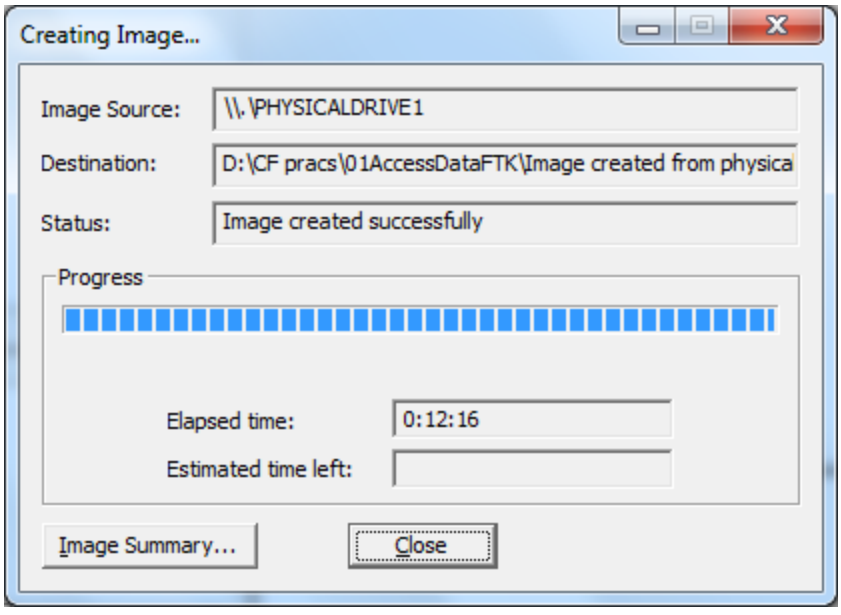


After the images are successfully created, the Drive/Image Verify Results box shows detailed image information, including MD5 and SHA1 check sums, and bad sectors.



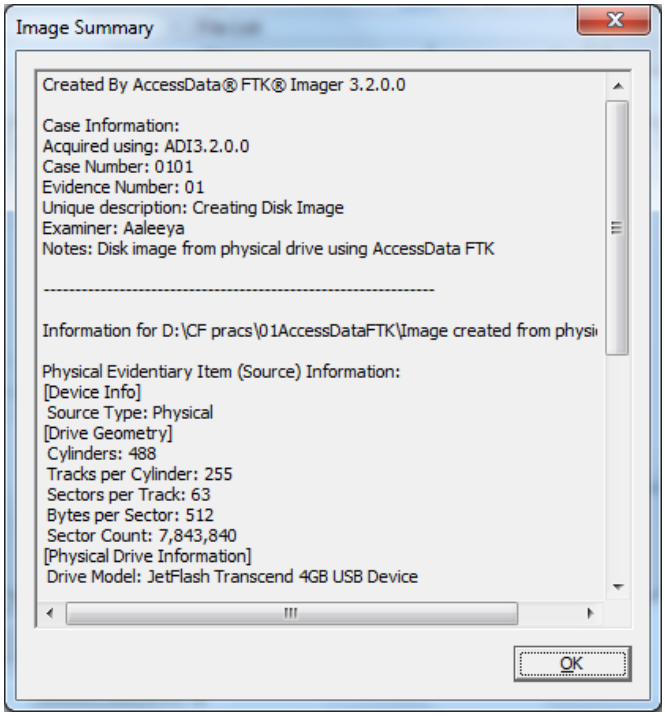
Now is a good time to refill that coffee cup! Once the acquisition is complete, you can view an image summary and the drive will appear in the evidence list in the left hand side of the main FTK Imager window. You can right-click on the drive name to Verify the Image:

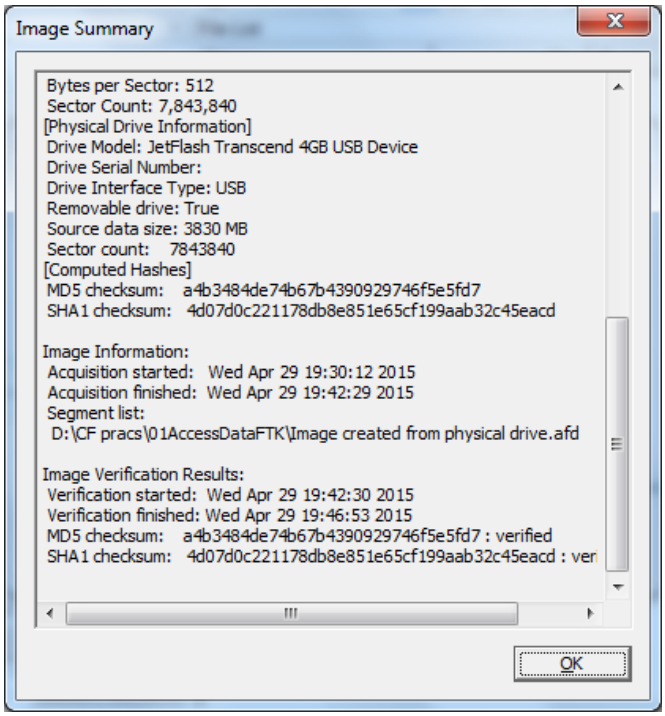

Drive/Image Verify Results
Name
file_000.aff
Sector count
7843840
MD5 Hash
Computed hash
a4b3484de74b67b4390929746f5e5fd7
Report Hash
a4b3484de74b67b4390929746f5e5fd7
Verify result
Match
SHA1 Hash
Computed hash
4d07d0c221178db8e851e65cf199aab32c
Report Hash
4d07d0c221178db8e851e65cf199aab32c
Verify result
Match
Bad Sector List
Bad sector(s)
No bad sectors found
Close


Creating Image...
Image Source:
\\.\PHYSICALDRIVE1
Destination:
D:\CF pracs\01AccessDataFTK\Image created from physica
Status:
Image created successfully
Progress
Elapsed time:
0:12:16
Estimated time left:
Image Summary...
Close

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 show





Practical No: 04

Practical No: 04

A) Using Log Capturing and Analysis tools

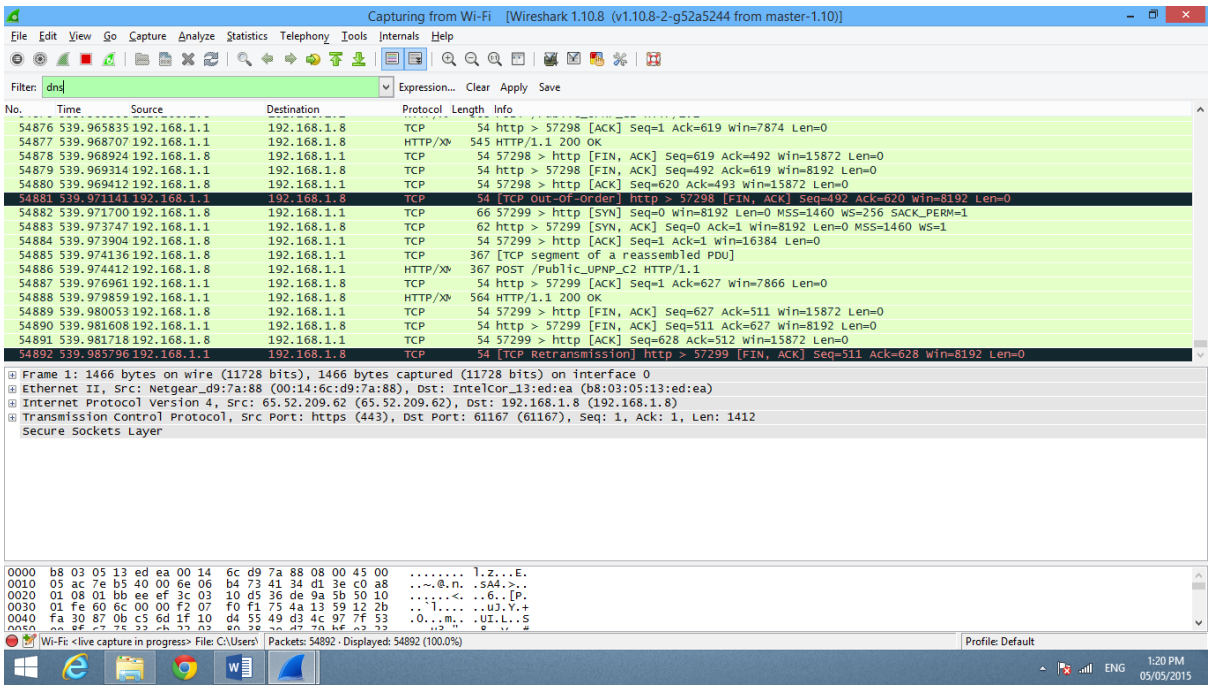
Aim: Exploring Wireshark

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.

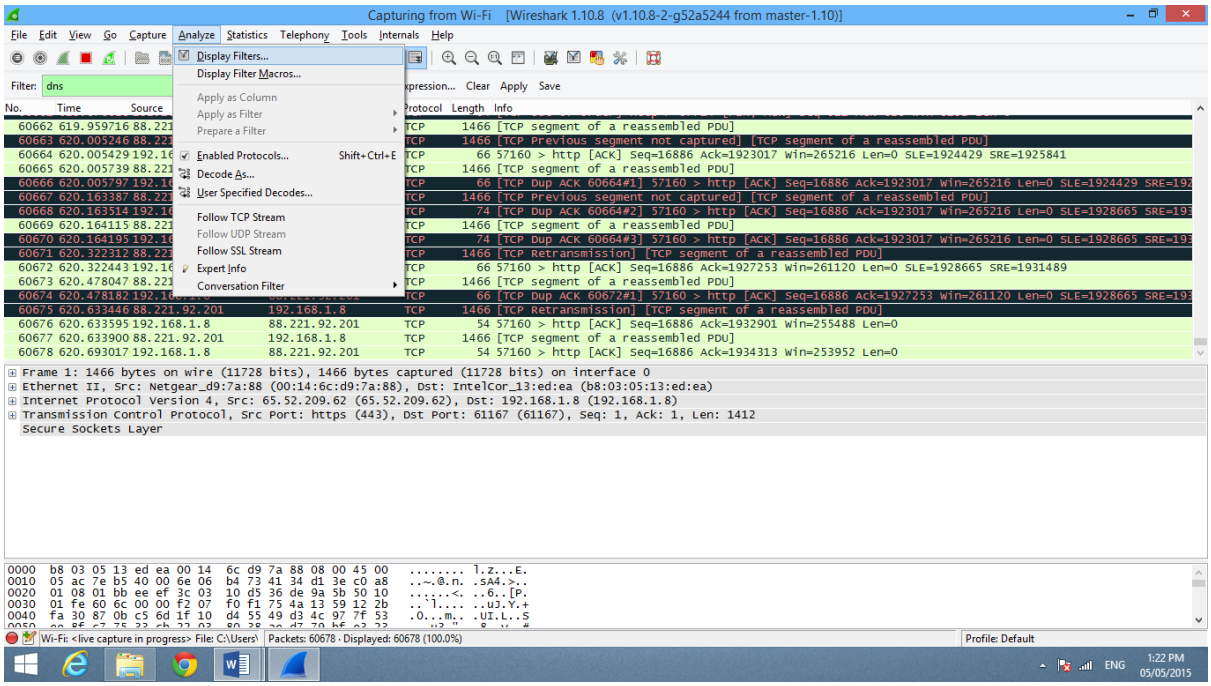
Filtering Packets

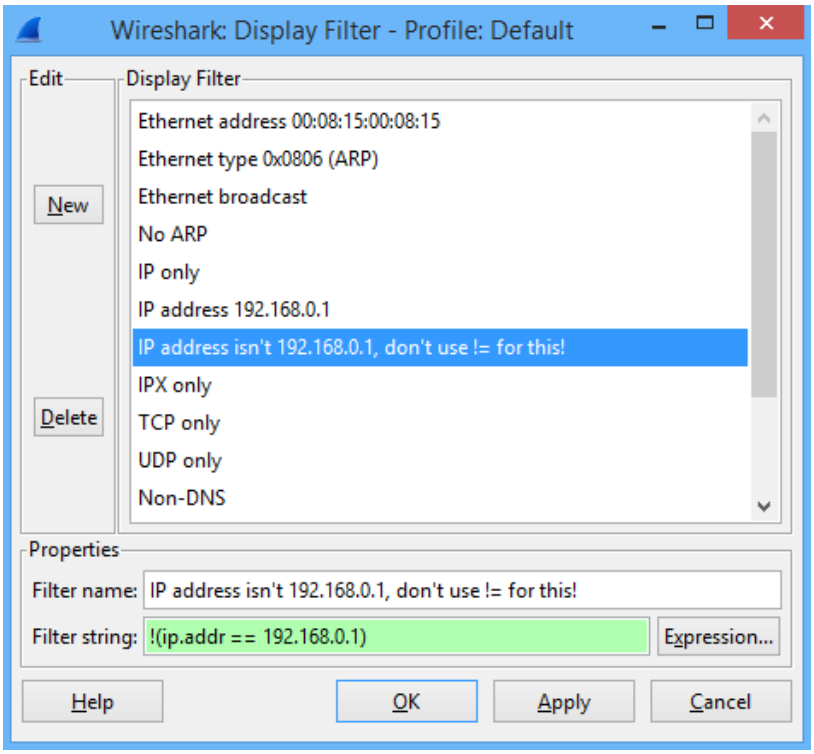
If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the traffic. Still, you'll likely have a large amount of packets to sift through. That's where Wireshark's filters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

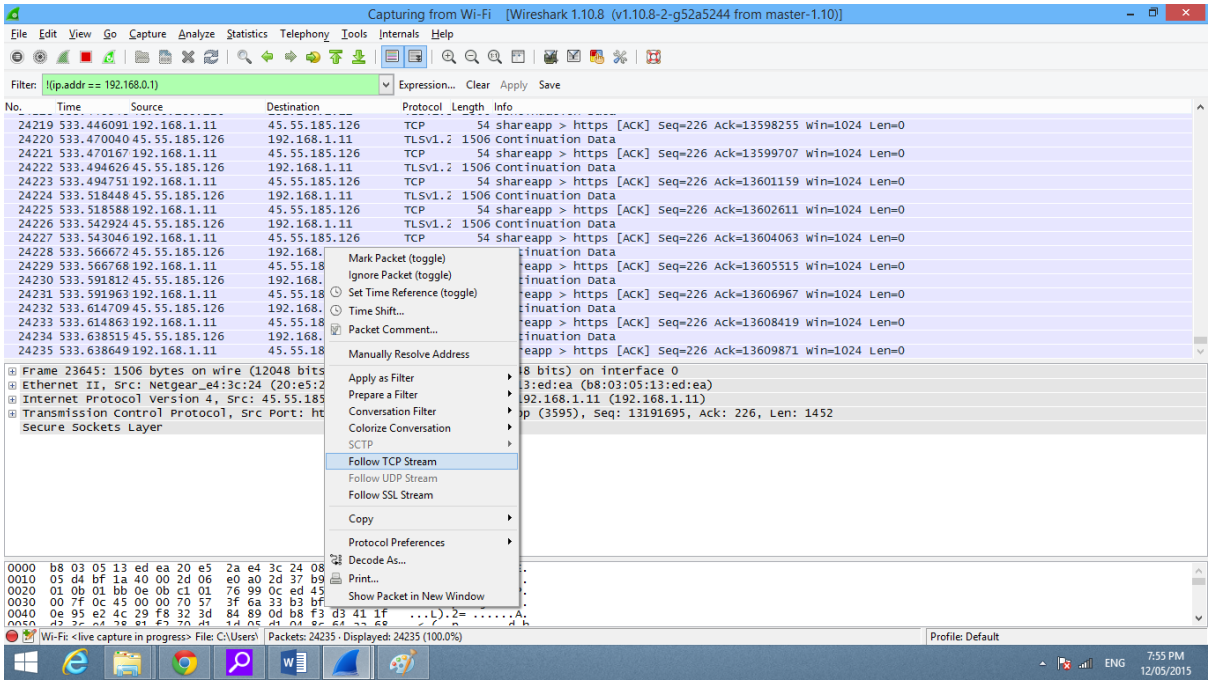


You can also click the Analyze menu and select Display Filters to create a new filter.

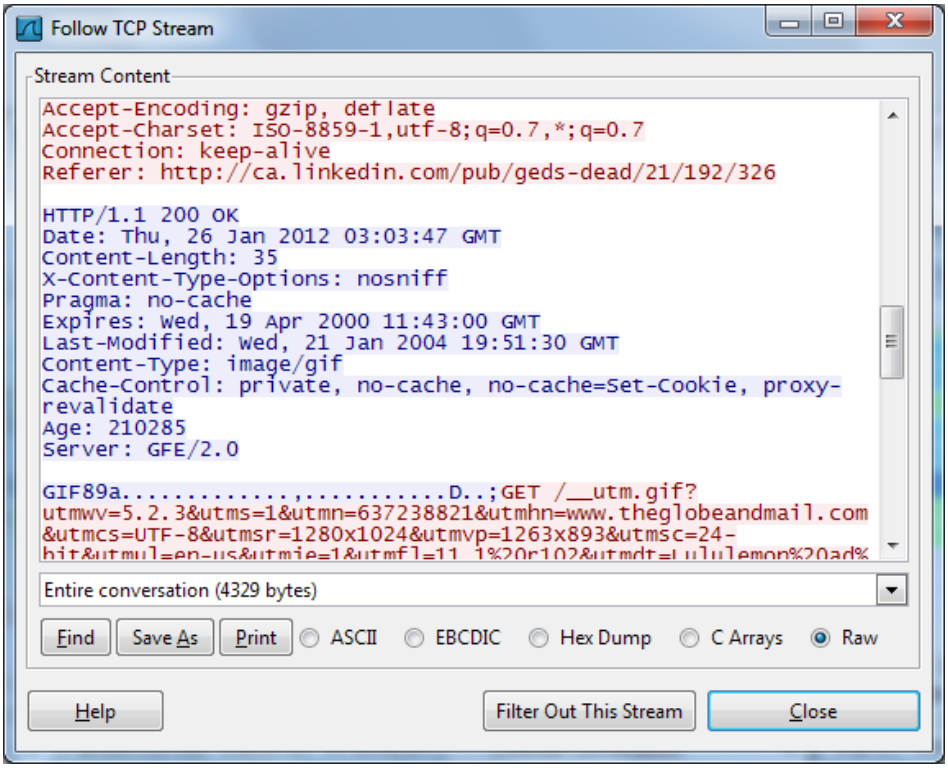




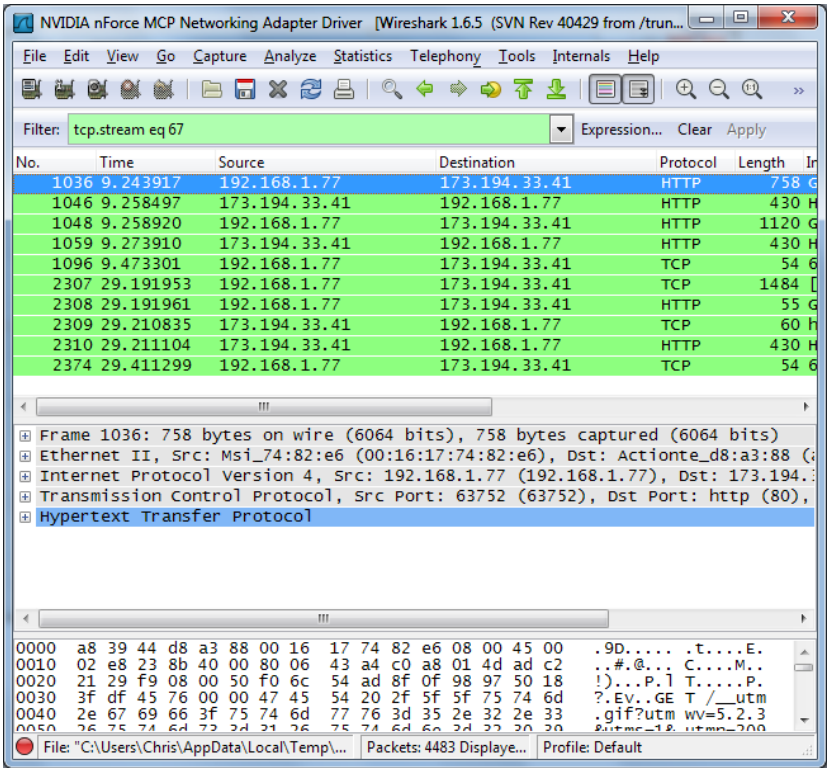
Another interesting thing you can do is right-click a packet and select Follow TCP Stream.



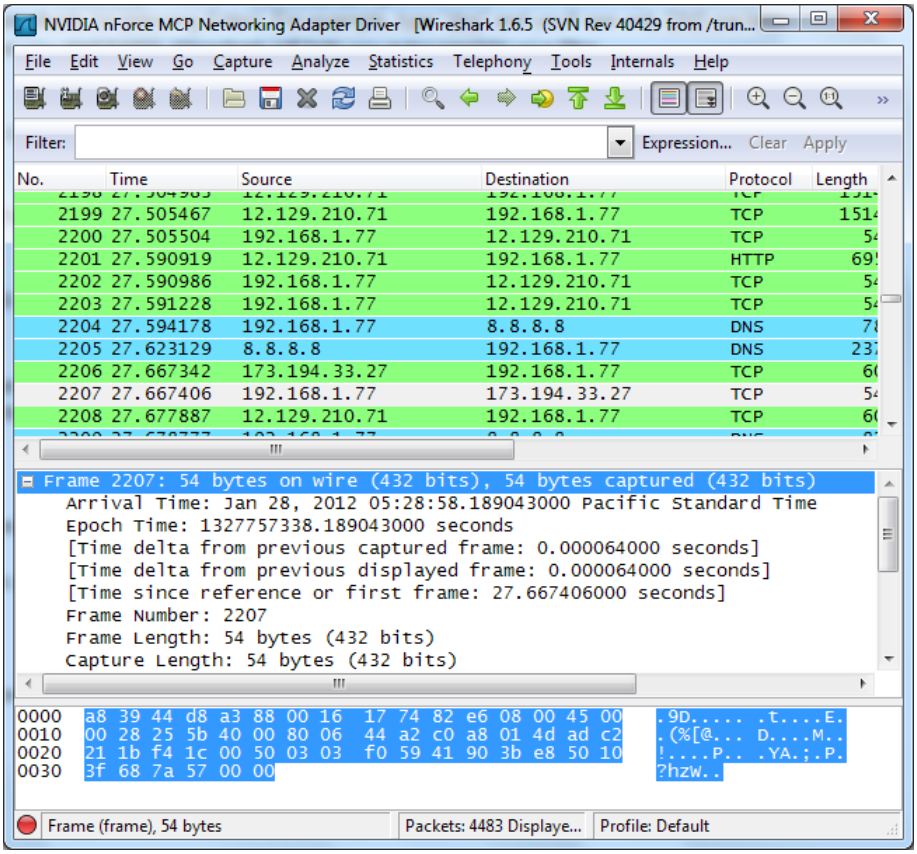
You'll see the full conversation between the client and the server.



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

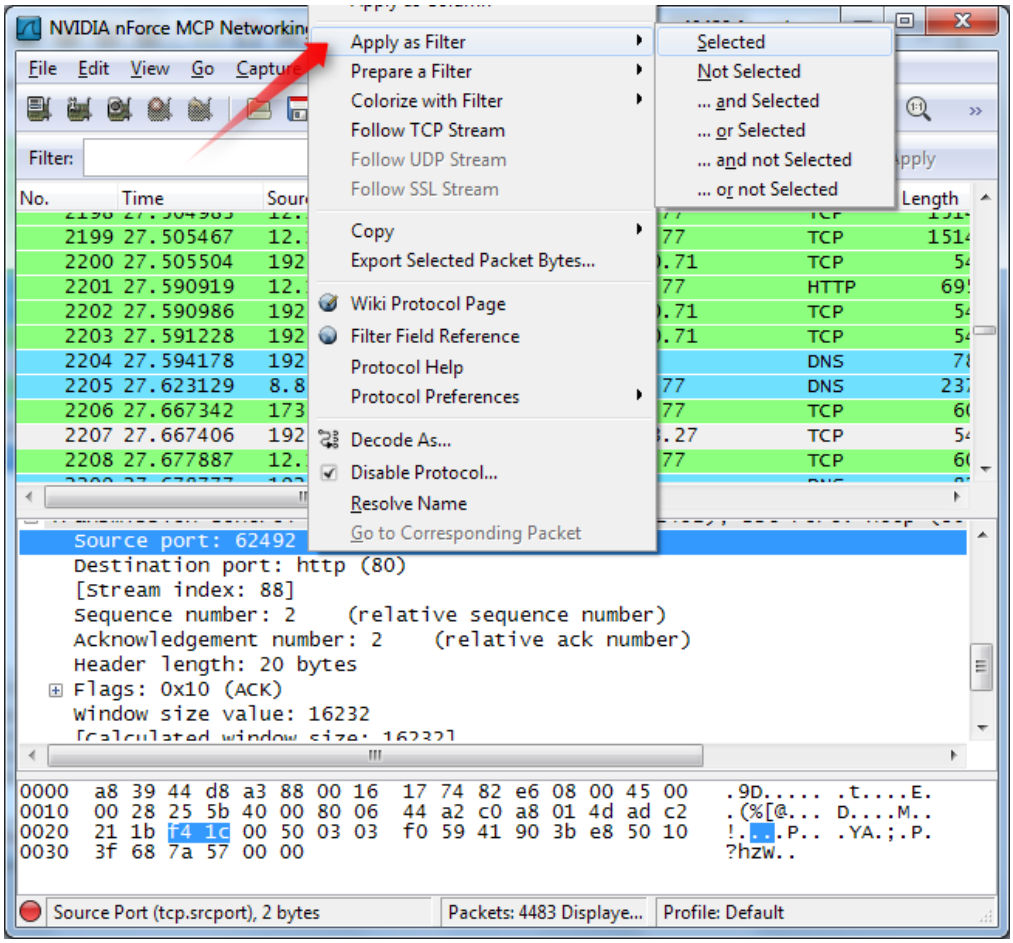


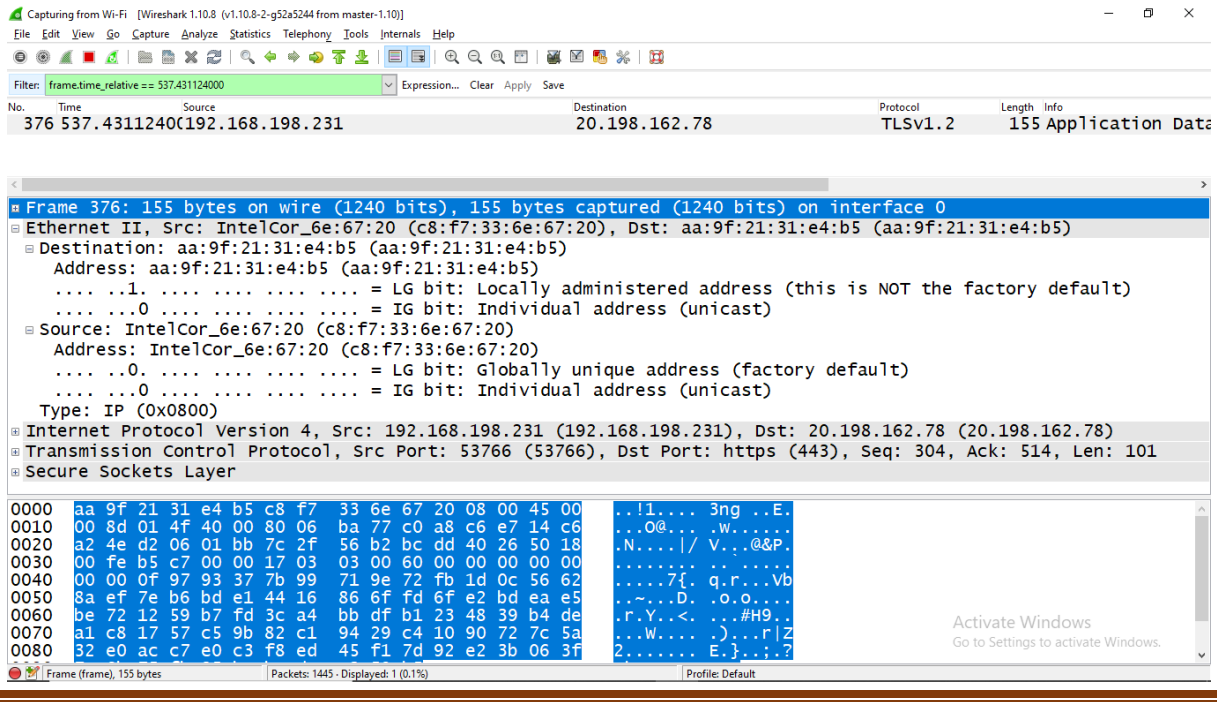
Inspecting Packets



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

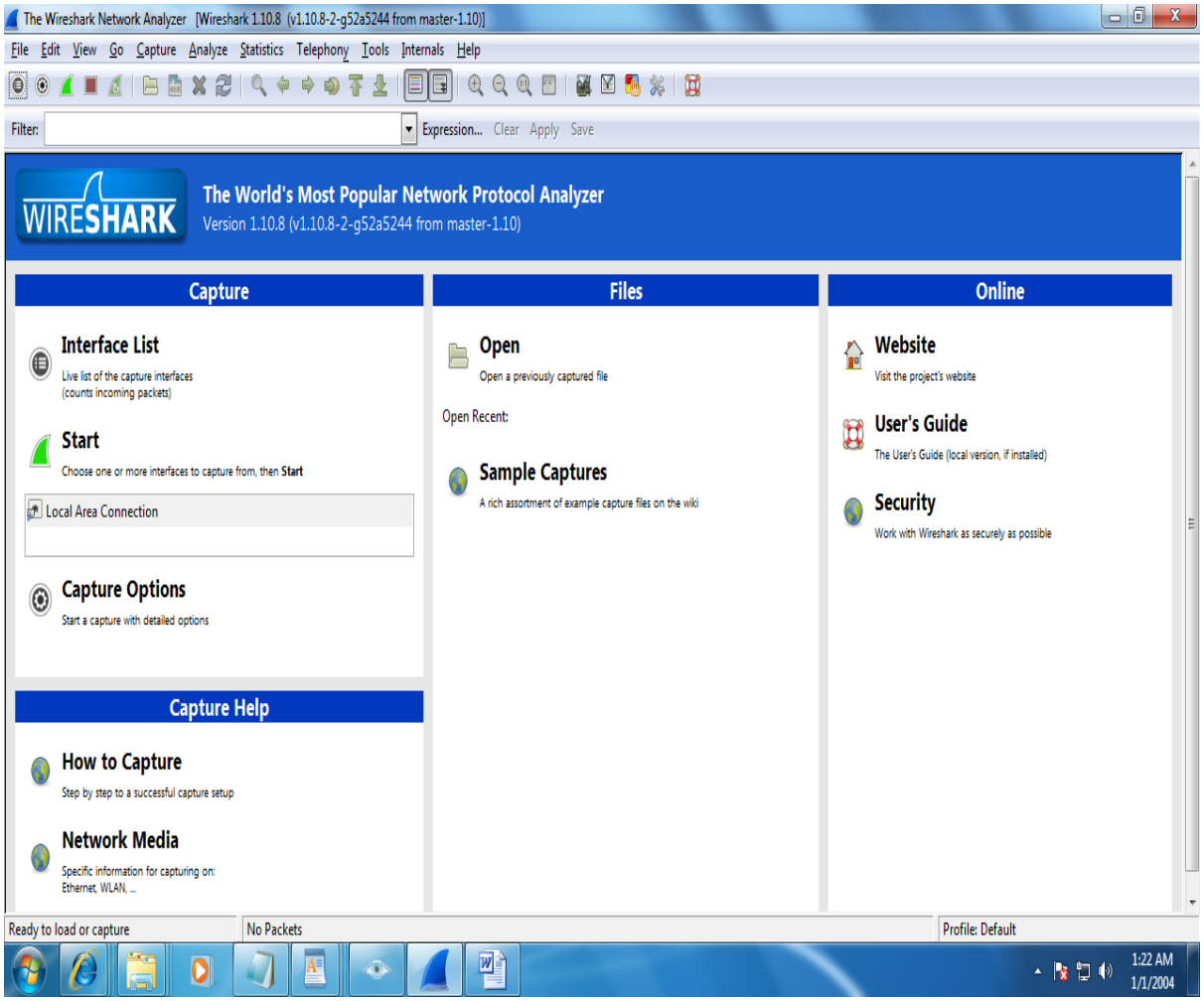
You can also create filters from here — just right-click one of the details and use the Apply as Filter submenu to create a filter based on it.


NVIDIA nForce MCP Networkin
File Edit View Go Capture
Filter:
No. Time Length
2199 27.505467 TCP
2200 27.505504 TCP
2201 27.590919 HTTP
2202 27.590986 TCP
2203 27.591228 TCP
2204 27.594178 DNS
2205 27.623129 DNS
2206 27.667342 TCP
2207 27.667406 TCP
2208 27.677887 TCP
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
Selected
Not Selected
... and Selected
... or Selected
... and not Selected
... or not Selected
Source port: 62492
Destination port: http (80)
[Stream index: 88]
Sequence number: 2 (relative sequence number)
Acknowledgement number: 2 (relative ack number)
Header length: 20 bytes
Flags: 0x10 (ACK)
Window size value: 16232
0000 a8 39 44 d8 a3 88 00 16 17 74 82 e6 08 00 45 00 .9D..... .t....E.
0010 00 28 25 5b 40 00 80 06 44 a2 c0 a8 01 4d ad c2 .(%[@... D....M..
0020 21 1b f4 1c 00 50 03 03 f0 59 41 90 3b e8 50 10 !....P.. .YA.;.P.
0030 3f 68 7a 57 00 00 ?hzW..
Source Port (tcp.srcport), 2 bytes
Packets: 4483 Displaye...
Profile: Default

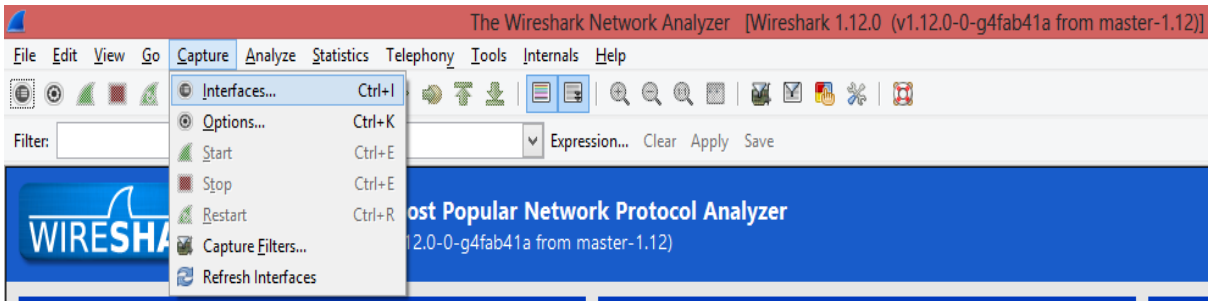

Capturing from Wi-Fi [Wireshark 1.10.8 (v1.10.8-2-g52a5244 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: frame.time_relative == 537.431124000
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
376 537.4311240 192.168.198.231 20.198.162.78 TLSv1.2 155 Application Data
Frame 376: 155 bytes on wire (1240 bits), 155 bytes captured (1240 bits) on interface 0
Ethernet II, Src: IntelCor_6e:67:20 (c8:f7:33:6e:67:20), Dst: aa:9f:21:31:e4:b5 (aa:9f:21:31:e4:b5)
Destination: aa:9f:21:31:e4:b5 (aa:9f:21:31:e4:b5)
Address: aa:9f:21:31:e4:b5 (aa:9f:21:31:e4:b5)
.... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)
....0 .... = IG bit: Individual address (unicast)
Source: IntelCor_6e:67:20 (c8:f7:33:6e:67:20)
Address: IntelCor_6e:67:20 (c8:f7:33:6e:67:20)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IP (0x0800)
Internet Protocol Version 4, Src: 192.168.198.231 (192.168.198.231), Dst: 20.198.162.78 (20.198.162.78)
Transmission Control Protocol, Src Port: 53766 (53766), Dst Port: https (443), Seq: 304, Ack: 514, Len: 101
Secure Sockets Layer
0000 aa 9f 21 31 e4 b5 c8 f7 33 6e 67 20 08 00 45 00 ..!1.... 3ng ..E.
0010 00 8d 01 4f 40 00 80 06 ba 77 c0 a8 c6 e7 14 c6 ...O@... .w......
0020 a2 4e d2 06 01 bb 7c 2f 56 b2 bc dd 40 26 50 18 .N....|/ V...@&P.
0030 00 fe b5 c7 00 00 17 03 03 00 60 00 00 00 00 00 ....`.....
0040 00 00 0f 97 93 37 7b 99 71 9e 72 fb 1d 0c 56 62 .....7{. q.r...Vb
0050 8a ef 7e b6 bd e1 44 16 86 6f fd 6f e2 bd ea e5 ..~...D. .o.o....
0060 be 72 12 59 b7 fd 3c a4 bb df b1 23 48 39 b4 de .r.Y..<. ...#H9..
0070 a1 c8 17 57 c5 9b 82 c1 94 29 c4 10 90 72 7c 5a ...W.... .)...r|Z
0080 32 e0 ac c7 e0 c3 f8 ed 45 f1 7d 92 e2 3b 06 3f 2....... E.}..;.?
Frame (frame), 155 bytes
Packets: 1445 · Displayed: 1 (0.1%)
Profile: Default
Activate Windows
Go to Settings to activate Windows.

B) Using Traffic Capturing and Analysis tools

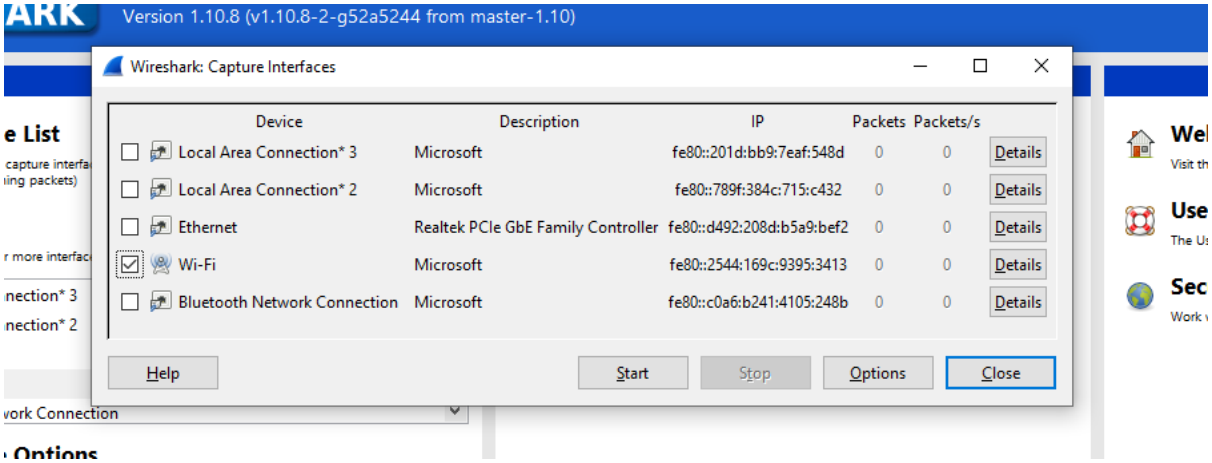
Aim: Exploring Wireshark

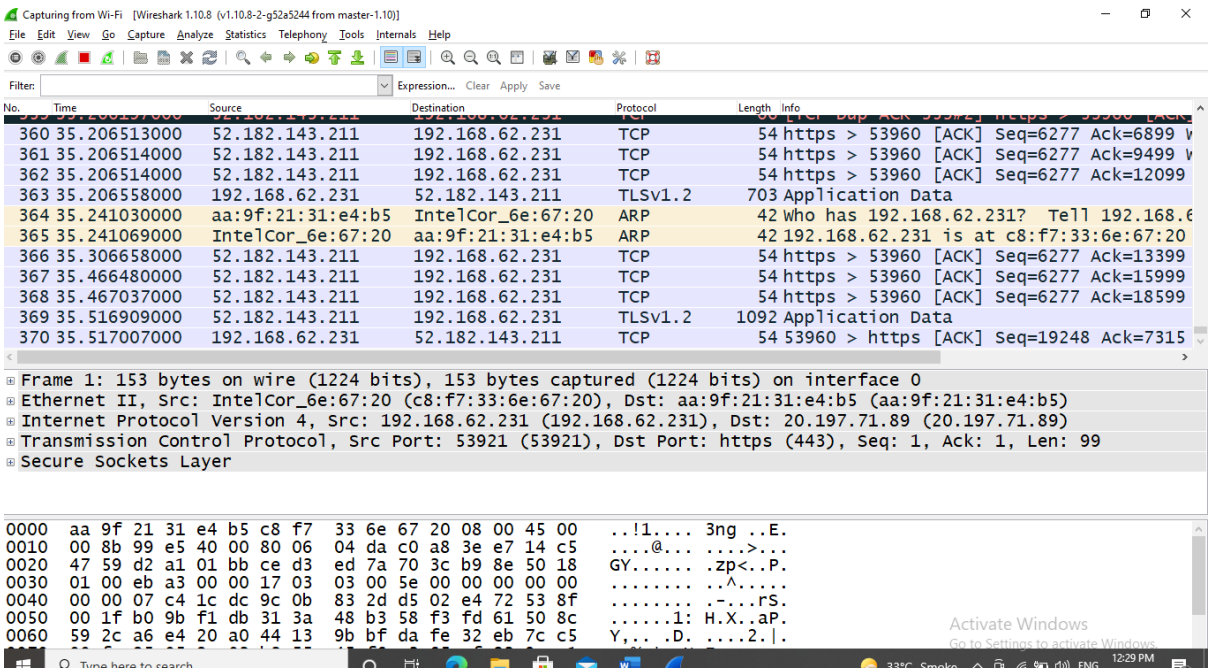


Step 2: On menu bar select Capture. Select interfaces.

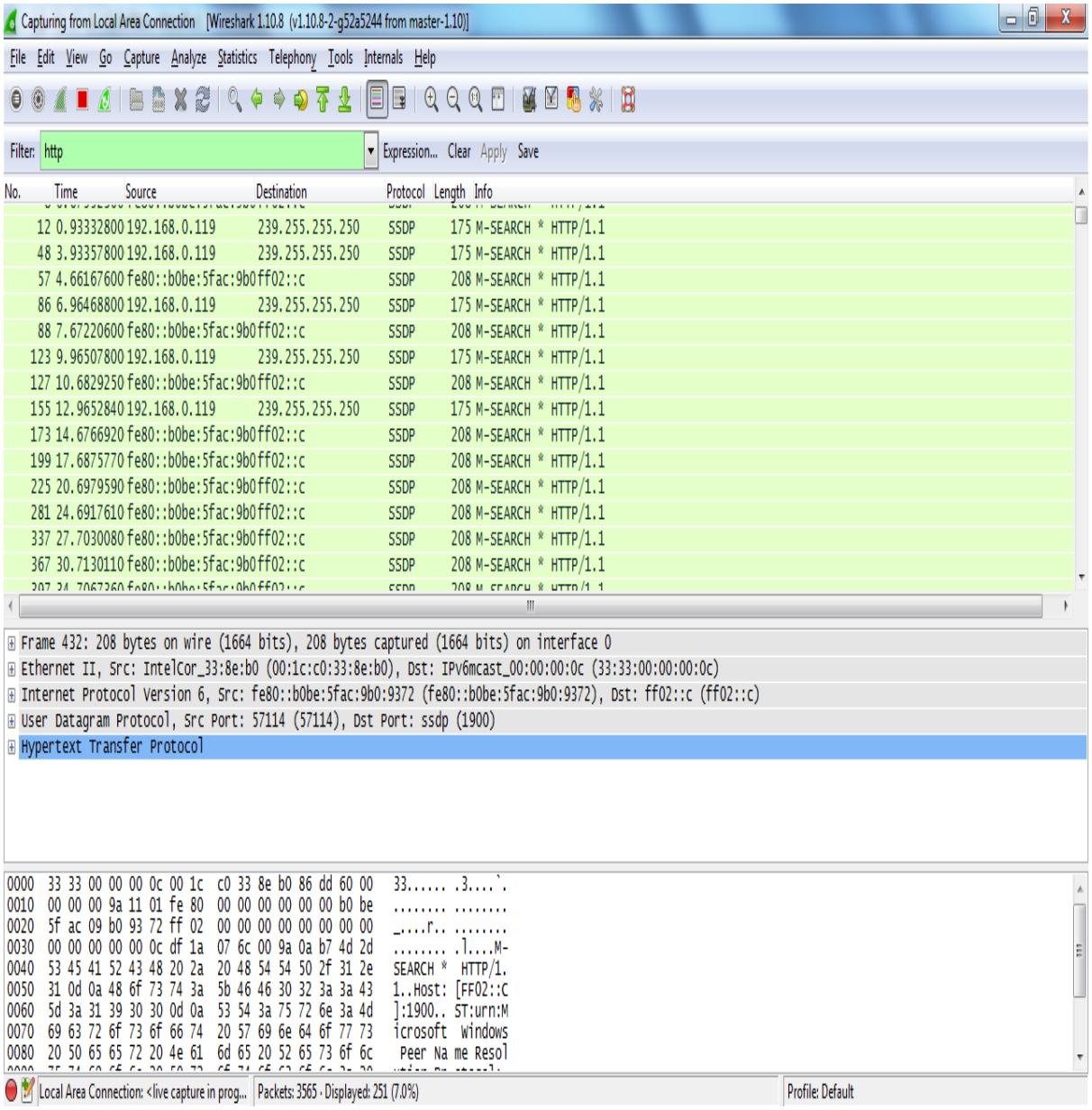


Step 3: Select Once you click on start, then Wireshark starts to capture the packets on that interface.

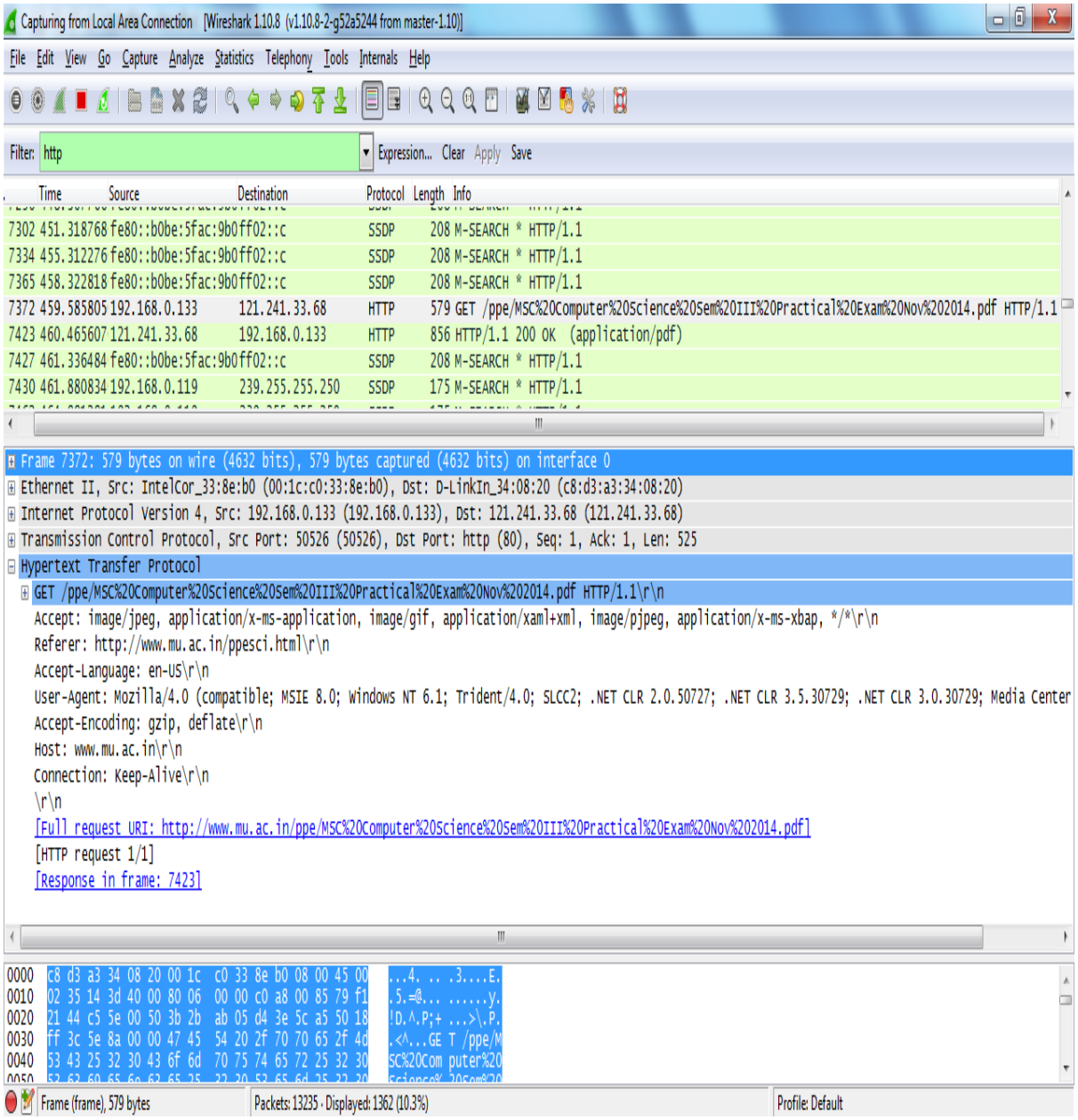




Step 4: Filter packets with HTTP protocol.

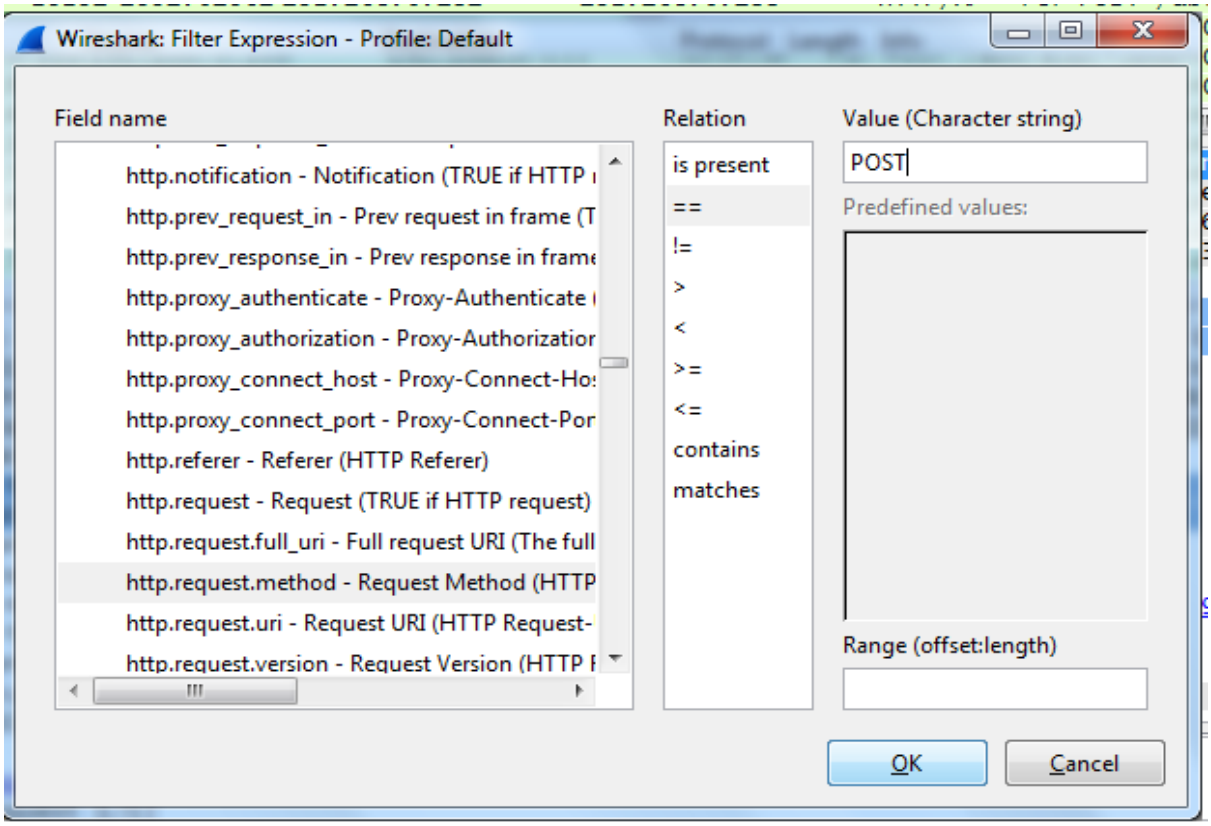


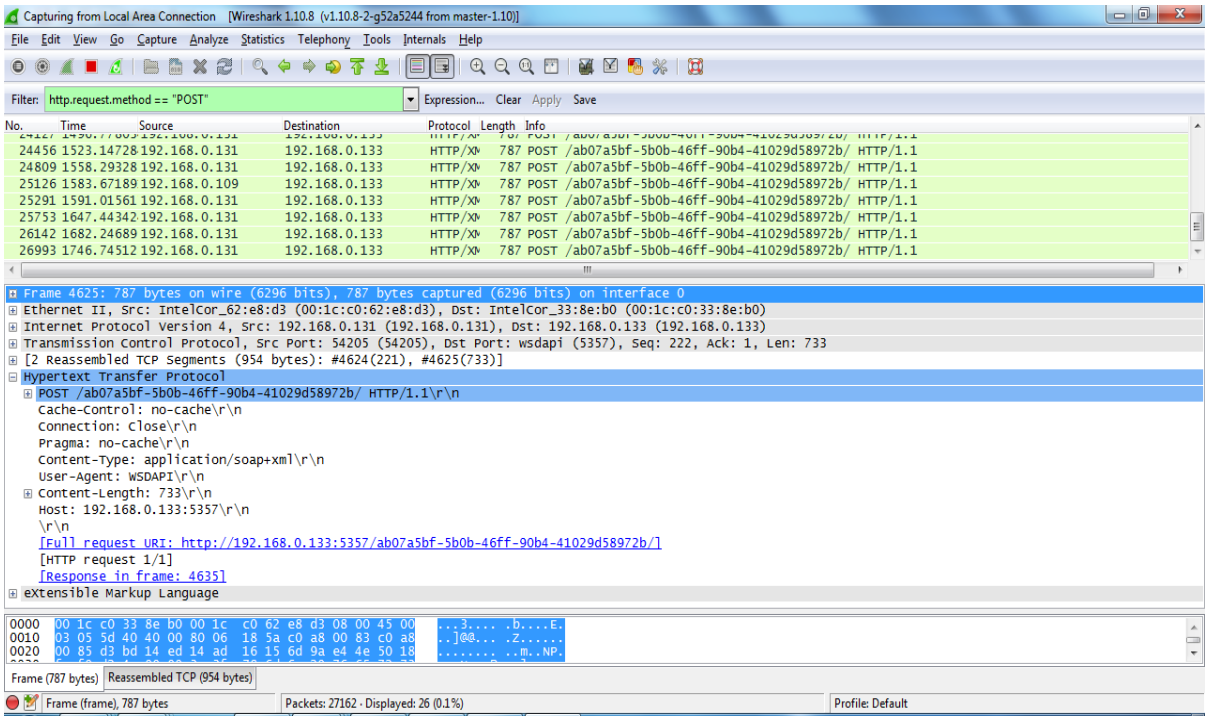
Step 5: A file with only text: http://www.mu.ac.in/ppe/LIBRARY%20SCIENCE-(SEM.I)-SH-2014.pdf



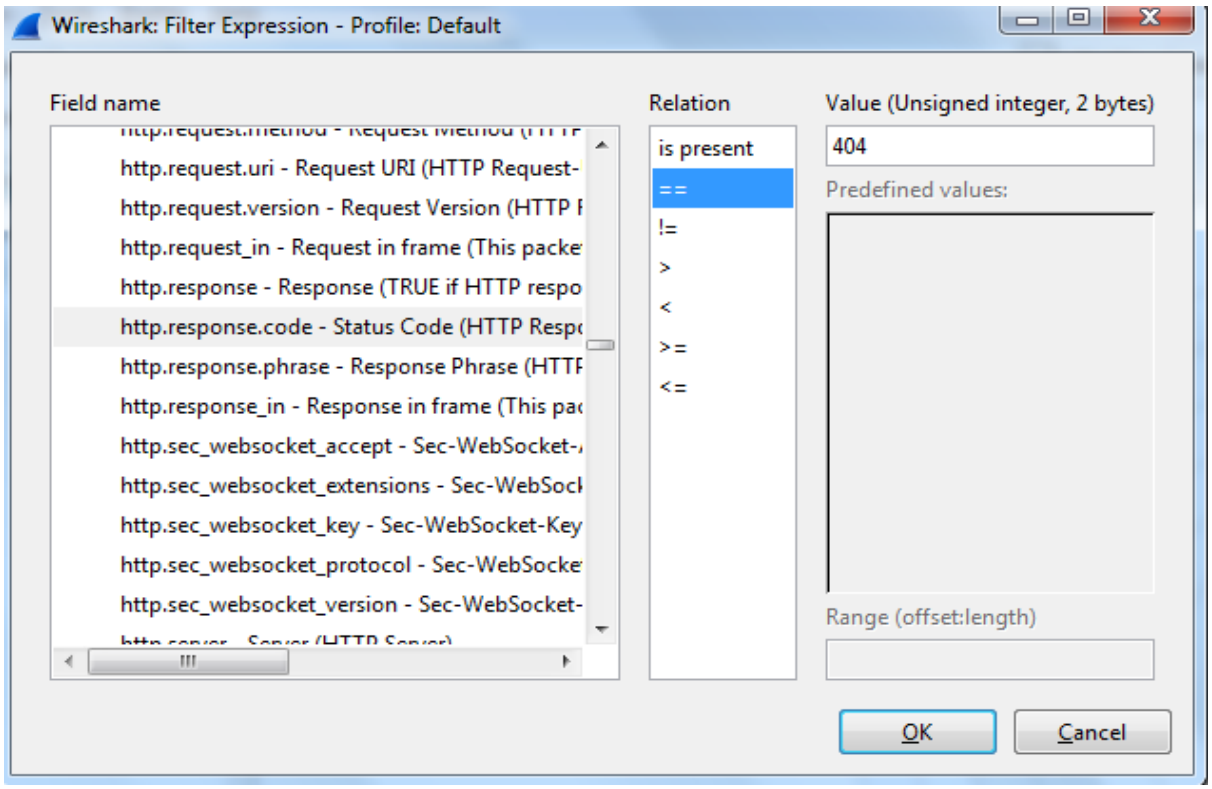
Step 6: Applying different filters using expressions.

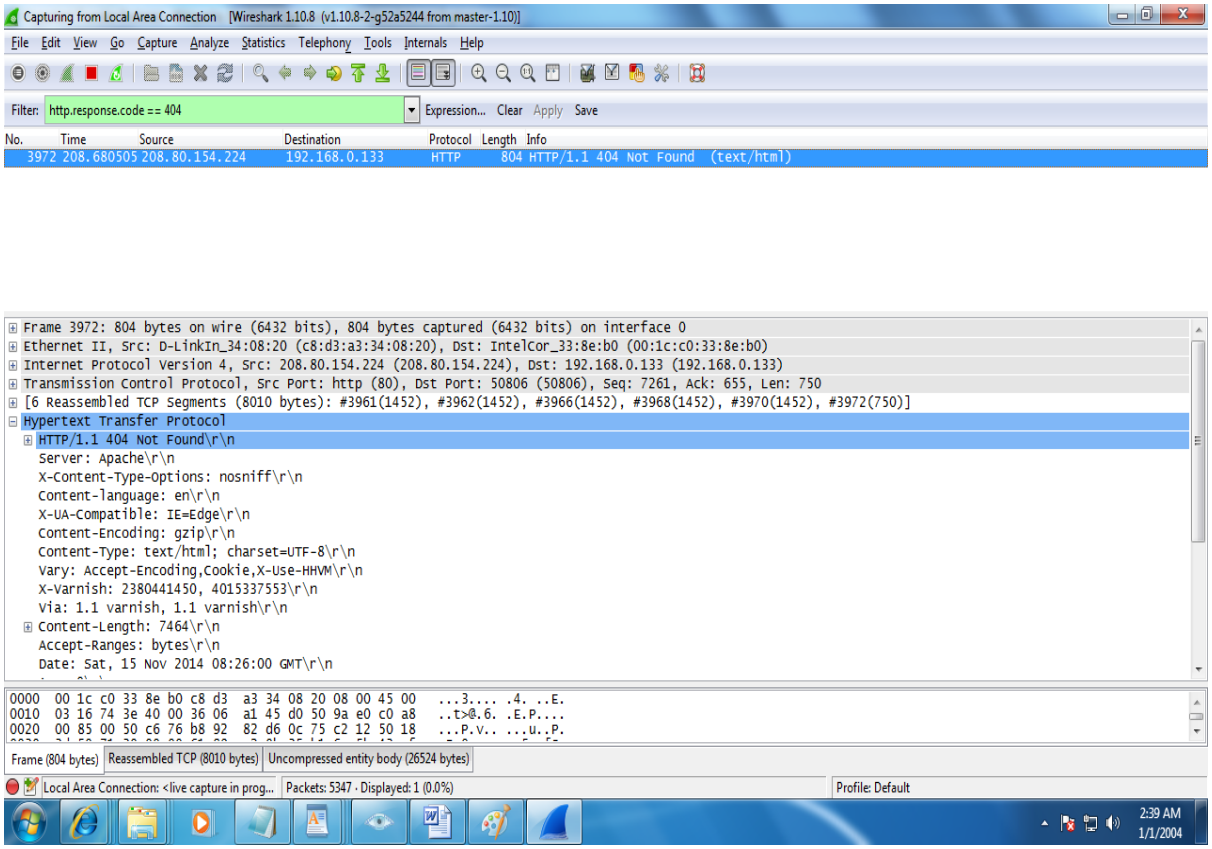
1) Filtering HTTP POST request



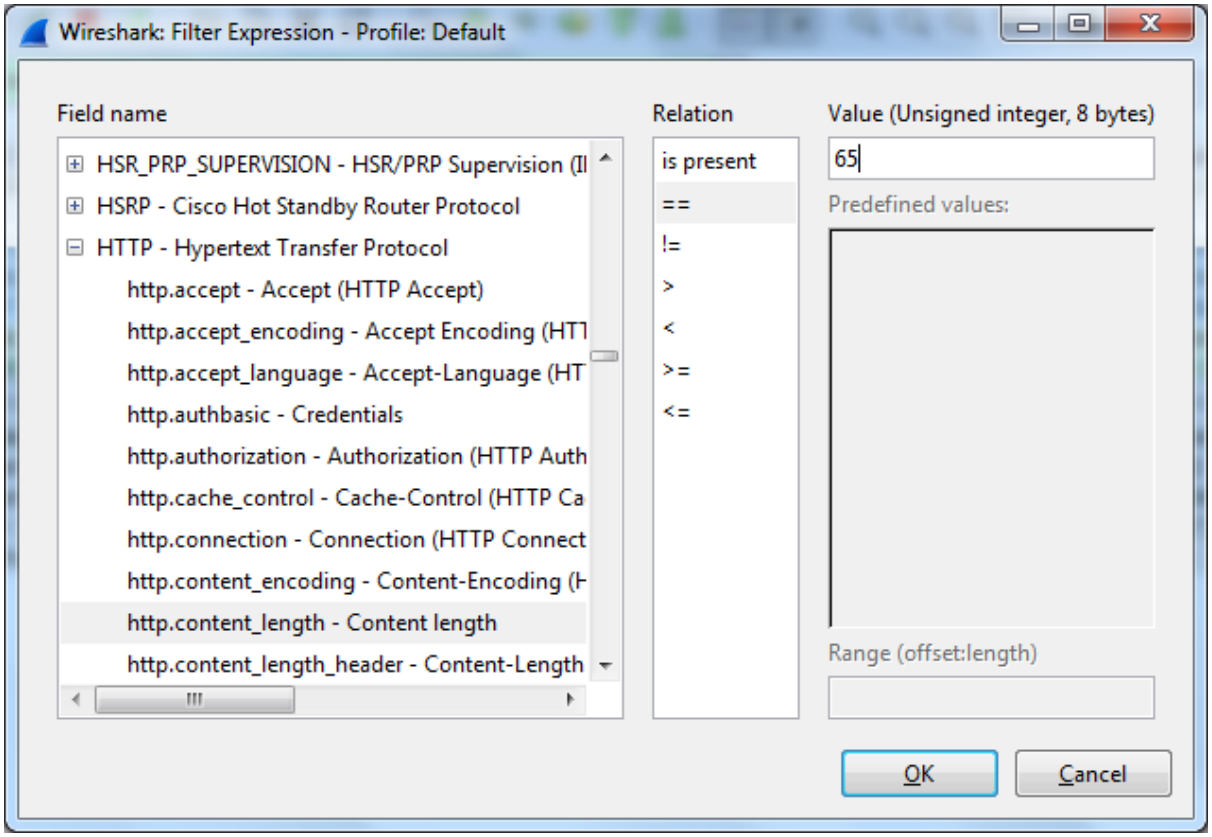


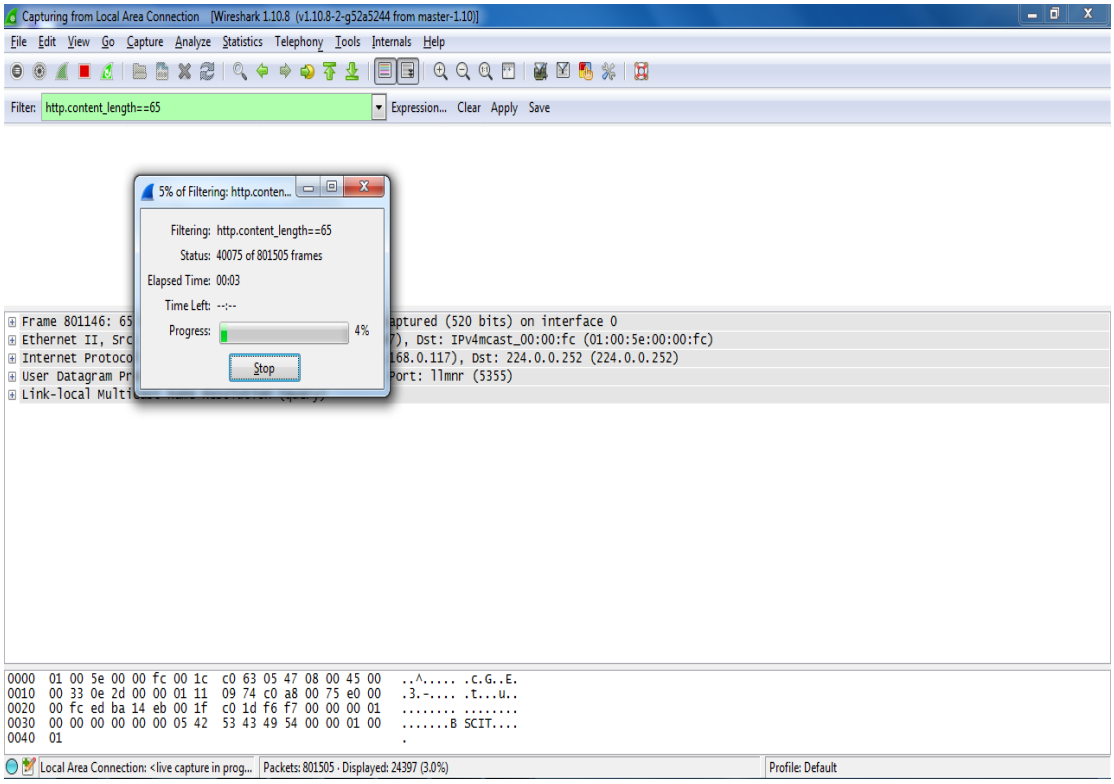
2) Filtering 404 not found error





3) Filtering using HTTP Content Length


Wireshark: Filter Expression - Profile: Default
Field name
Relation
Value (Unsigned integer, 8 bytes)
HSR_PRP_SUPERVISION - HSR/PRP Supervision (I
HSRP - Cisco Hot Standby Router Protocol
HTTP - Hypertext Transfer Protocol
http.accept - Accept (HTTP Accept)
http.accept_encoding - Accept Encoding (HT
http.accept_language - Accept-Language (HT
http.authbasic - Credentials
http.authorization - Authorization (HTTP Auth
http.cache_control - Cache-Control (HTTP Ca
http.connection - Connection (HTTP Connect
http.content_encoding - Content-Encoding (H
http.content_length - Content length
http.content_length_header - Content-Length
is present
==
!=
>
<
>=
<=
65
Predefined values:
Range (offset:length)
OK
Cancel


Capturing from Local Area Connection [Wireshark 1.10.8 (v1.10.8-2-g52a5244 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: http.content_length==65
Expression... Clear Apply Save
5% of Filtering: http.conten...
Filtering: http.content_length==65
Status: 40075 of 801505 frames
Elapsed Time: 00:03
Time Left: --:--
Progress: 4%
Stop
Frame 801146: 65
Ethernet II, Src
Internet Protoco
User Datagram Pr
Link-local Multi
aptured (520 bits) on interface 0
7), Dst: IPv4mcast_00:00:fc (01:00:5e:00:00:fc)
168.0.117), Dst: 224.0.0.252 (224.0.0.252)
Port: llmnr (5355)
0000 01 00 5e 00 00 fc 00 1c c0 63 05 47 08 00 45 00 ..^..... .c.G..E.
0010 00 33 0e 2d 00 00 01 11 09 74 c0 a8 00 75 e0 00 .3.-.... .t...u..
0020 00 fc ed ba 14 eb 00 1f c0 1d f6 f7 00 00 00 01 ....
0030 00 00 00 00 00 00 05 42 53 43 49 54 00 00 01 00 ....B SCIT....
0040 01 .
Local Area Connection: <live capture in prog...
Packets: 801505 · Displayed: 24397 (3.0%)
Profile: Default

Practical No: 05

Practical No: 05

Aim: Using Data Acquisition Tools Tasks to be

performed:

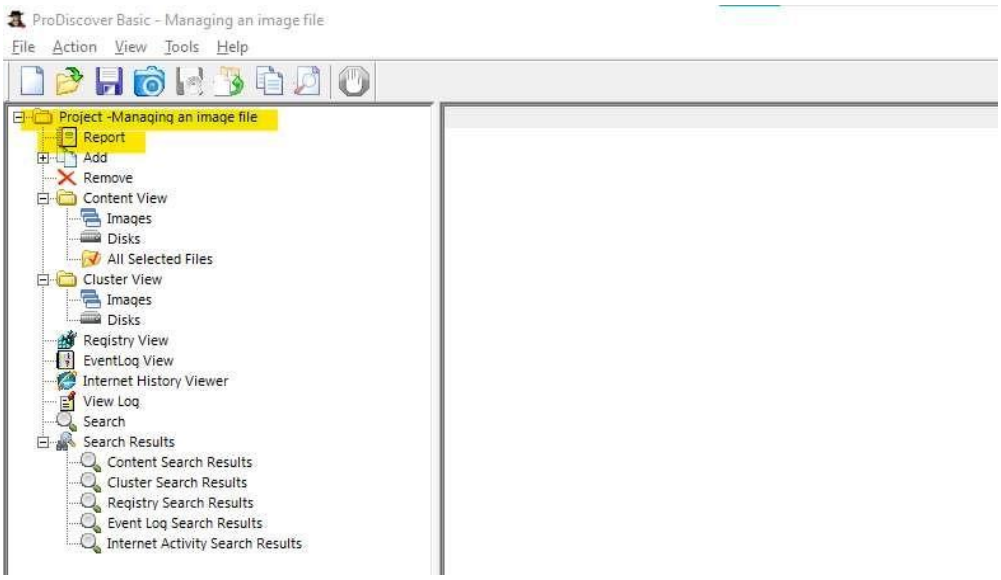
1) Creating a New Project
2) Save a project
3) Preview a directly connected evidence drive
4) Conducting Live Preview of a Remote Disk
5) Capture an image of an attached drive
6) Capturing Physical Memory
7) Add an image file to a project
8) Restore an Image to directly connected drive

Creating a New Project:

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

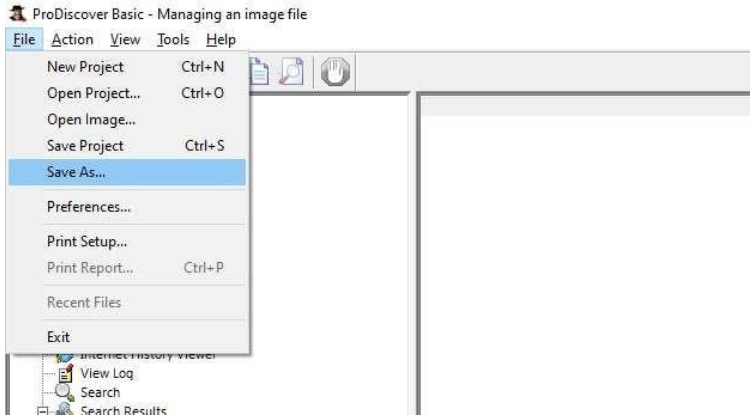
Step 2) Enter a project number, project name, and description of the project in the new project tab option, and then click the Open button.

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

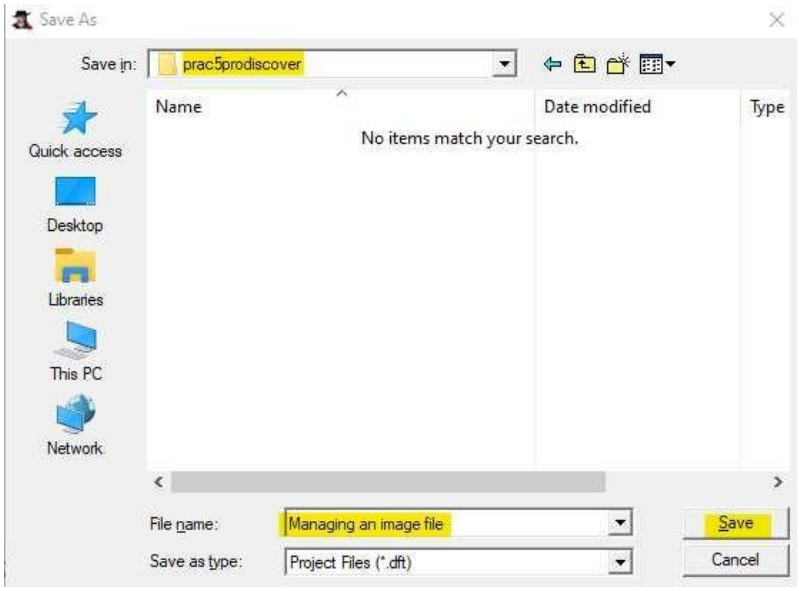

ProDiscover Basic - Managing an image file
File Action View Tools Help
Project -Managing an image file
Report
Add
Remove
Content View
Images
Disks
All Selected Files
Cluster View
Images
Disks
Registry View
EventLog View
Internet History Viewer
View Log
Search
Search Results
Content Search Results
Cluster Search Results
Registry Search Results
Event Log Search Results
Internet Activity Search Results

2) Saving a project:

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

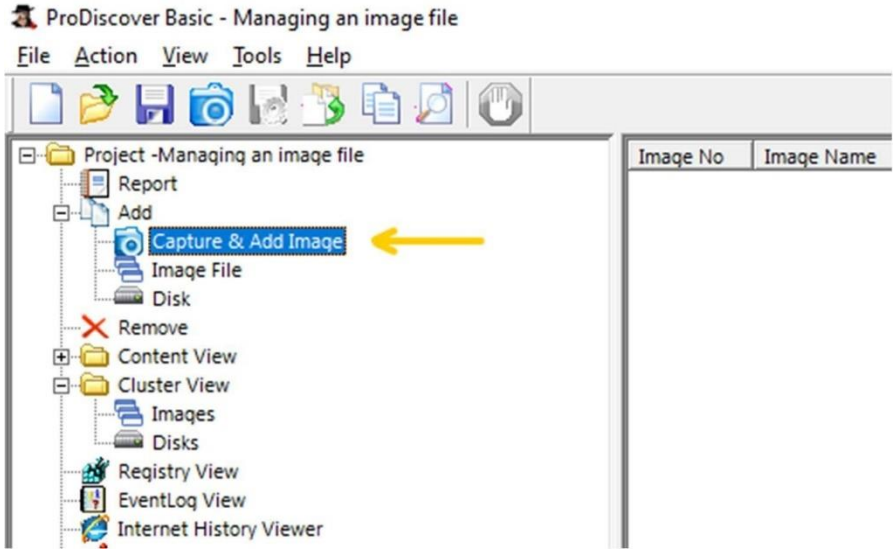
1] Launch ProDiscover.

2] Select open project tab option.

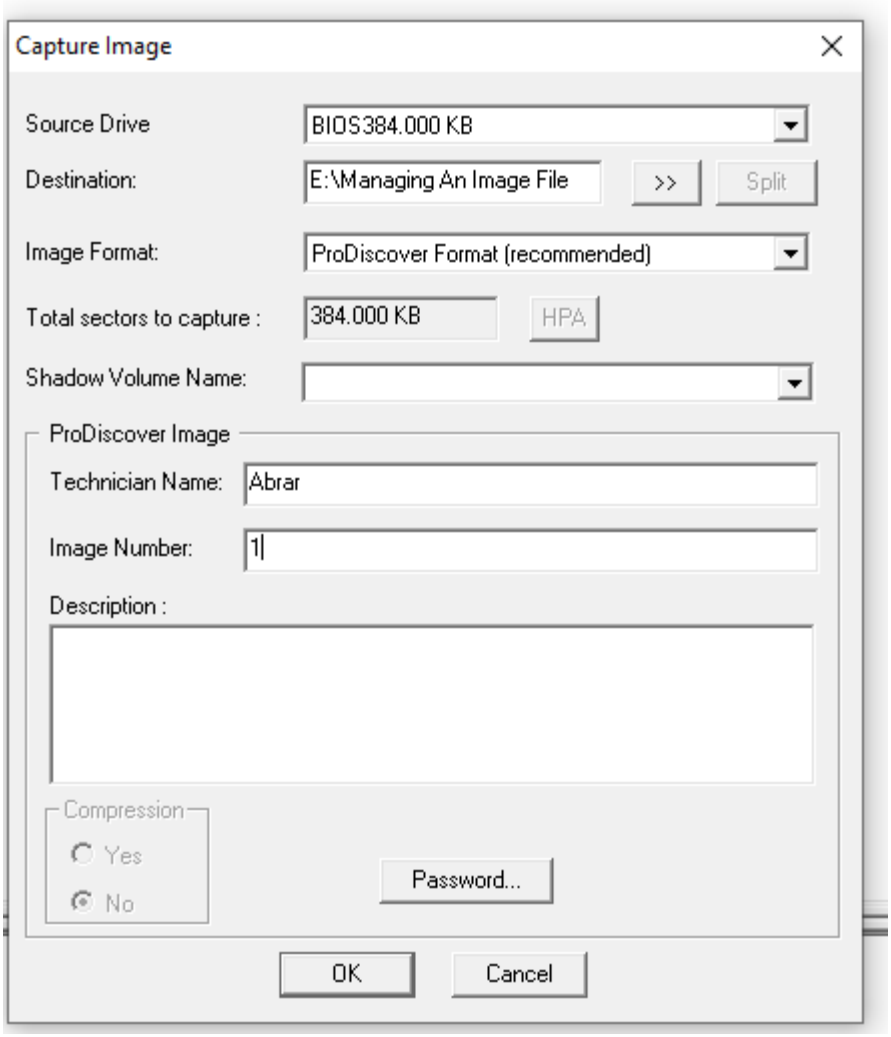
3] Select the project file to open and click Open button.

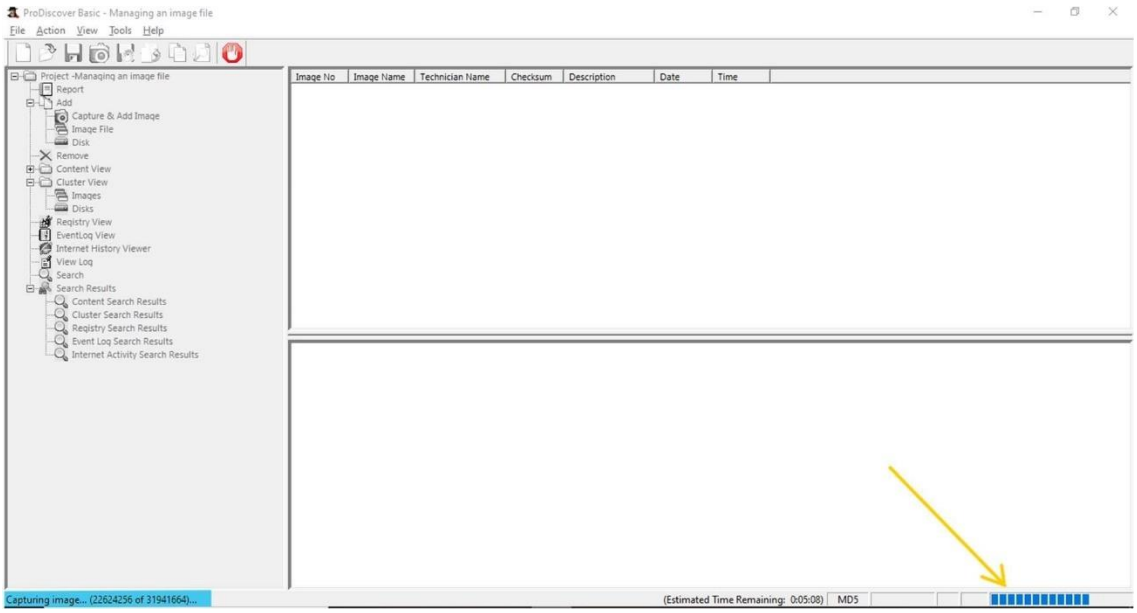
4] ProDiscover opens the project file and generates a template report in the work area.

5] Under Report, expand Add and click on Capture & Add Image.

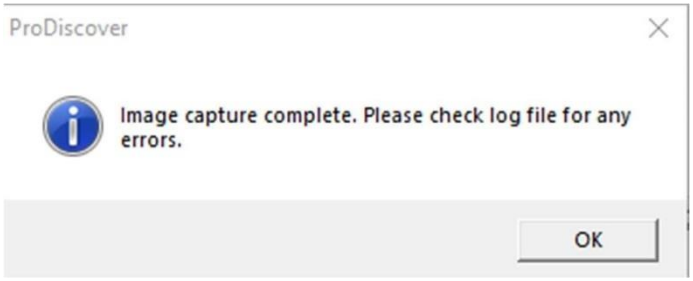


6] Give Destination, add Technician Name and image number and click on OK

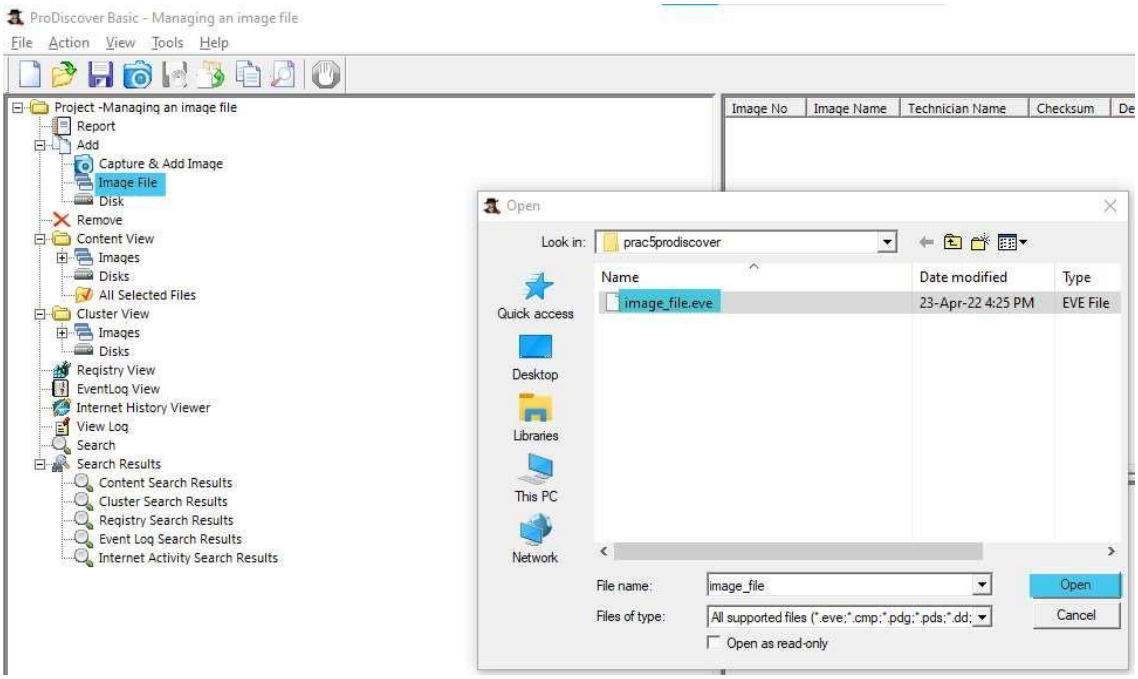

Capture Image
Source Drive
BIOS384.000 KB
Destination:
E:\Managing An Image File
>>
Split
Image Format:
ProDiscover Format (recommended)
Total sectors to capture :
384.000 KB
HPA
Shadow Volume Name:
ProDiscover Image
Technician Name:
Abrar
Image Number:
1
Description :
Compression
Yes
No
Password...
OK
Cancel


ProDiscover Basic - Managing an image file
File Action View Tools Help
Project -Managing an image file
Report
Add
Capture & Add Image
Image File
Disk
Remove
Content View
Cluster View
Images
Disks
Registry View
EventLog View
Internet History Viewer
View Log
Search
Search Results
Content Search Results
Cluster Search Results
Registry Search Results
Event Log Search Results
Internet Activity Search Results
Image No
Image Name
Technician Name
Checksum
Description
Date
Time
Capturing image... (22624256 of 31941664)...
(Estimated Time Remaining: 0:05:08)
MD5

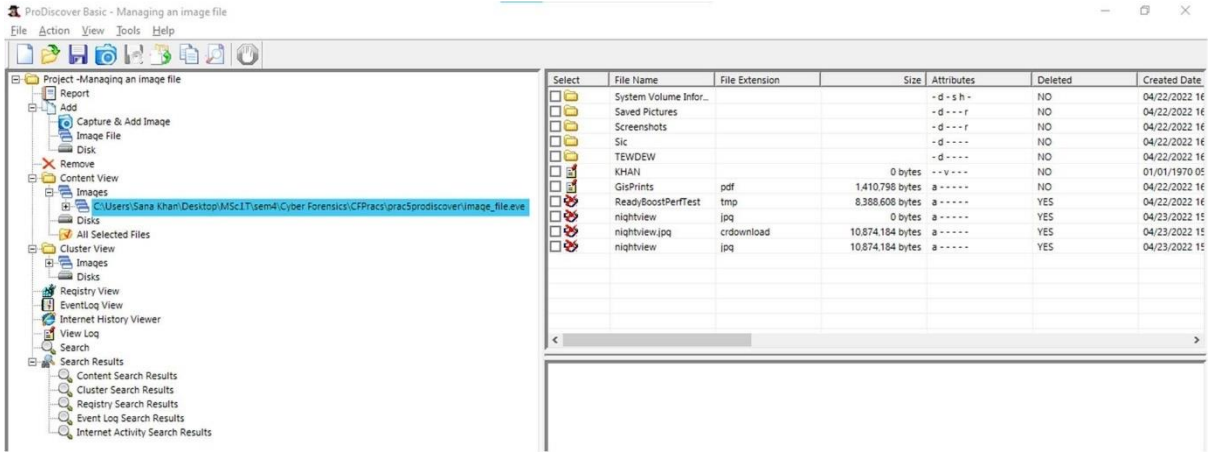
Once the image capturing is completed, click on OK



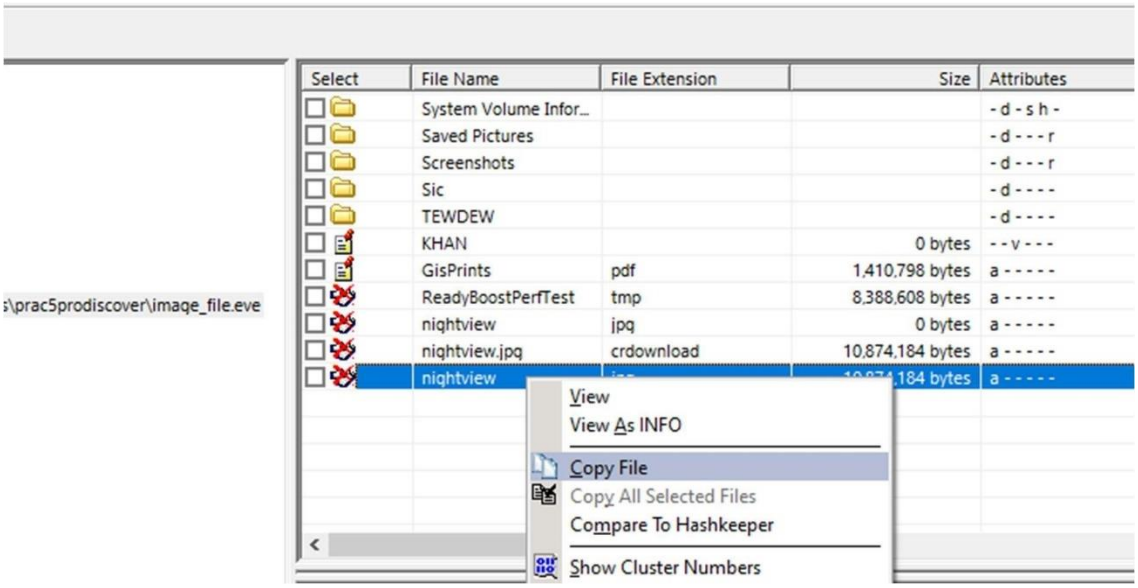
7] Under Add, click on Image File, click on the image that you created and click Open



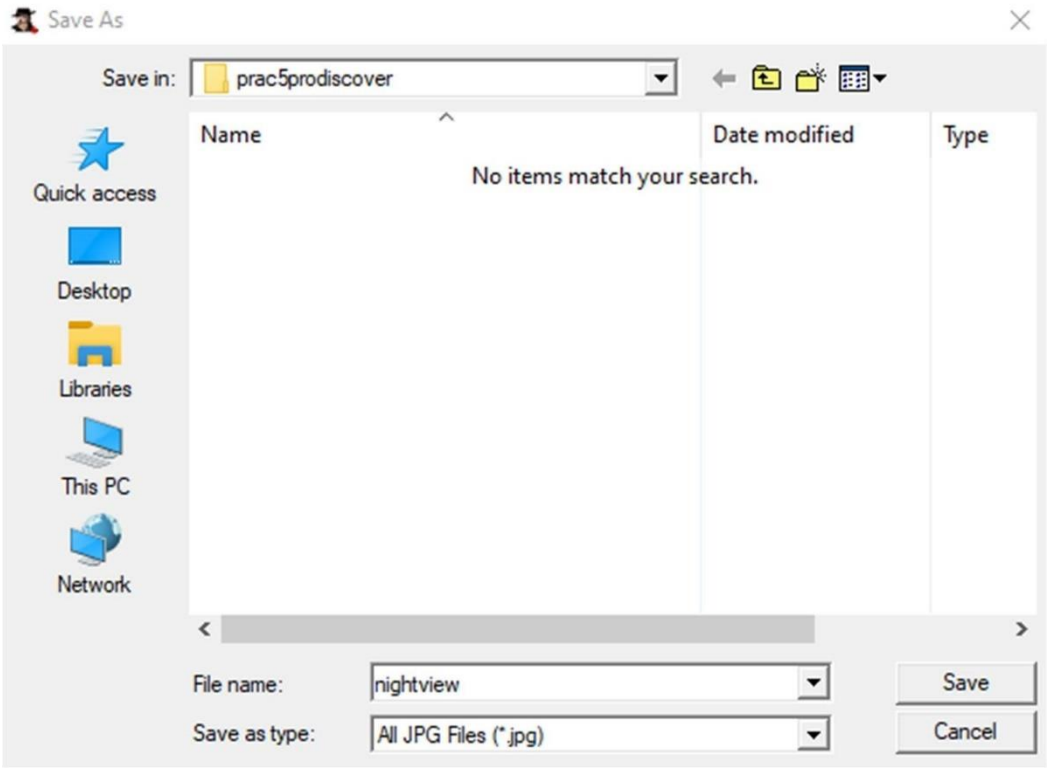
8] The image file will get added. Then under Content view, click on images and select the image.



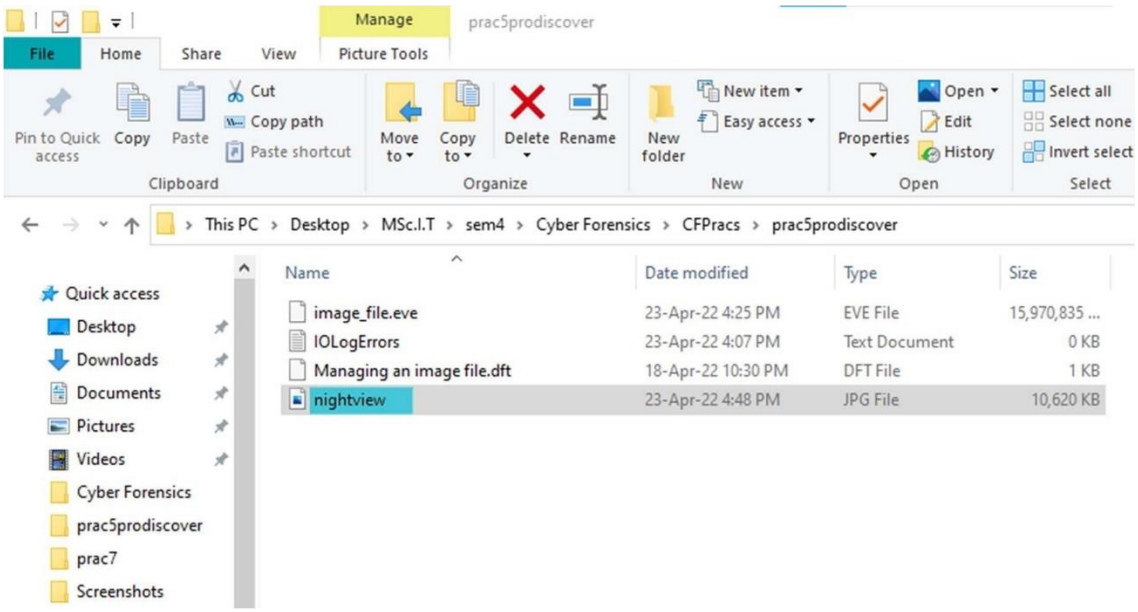
9] Right click on deleted file, either view it or copy the file to a folder.



10] Save the file



11] Navigate to the folder and there you can see the deleted file.



12] You can view the deleted file once saved in a folder.

Practical No: 06

Practical No: 06

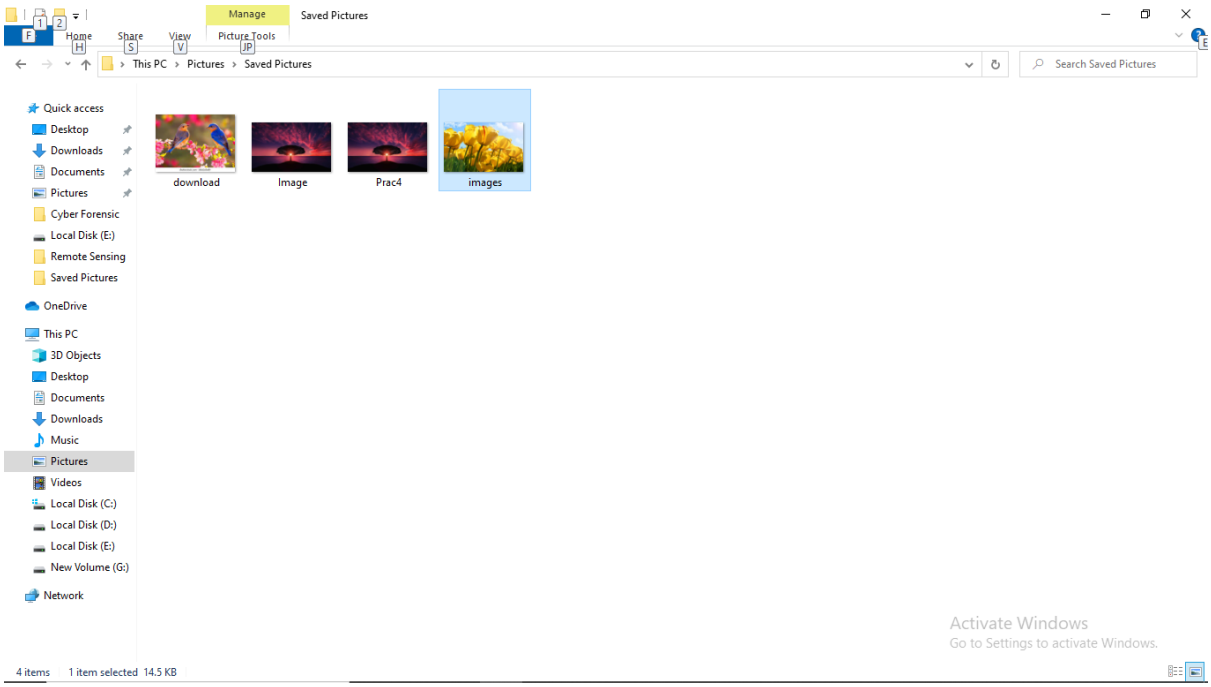
Using Steganography tools

Aim: Exploring S 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.



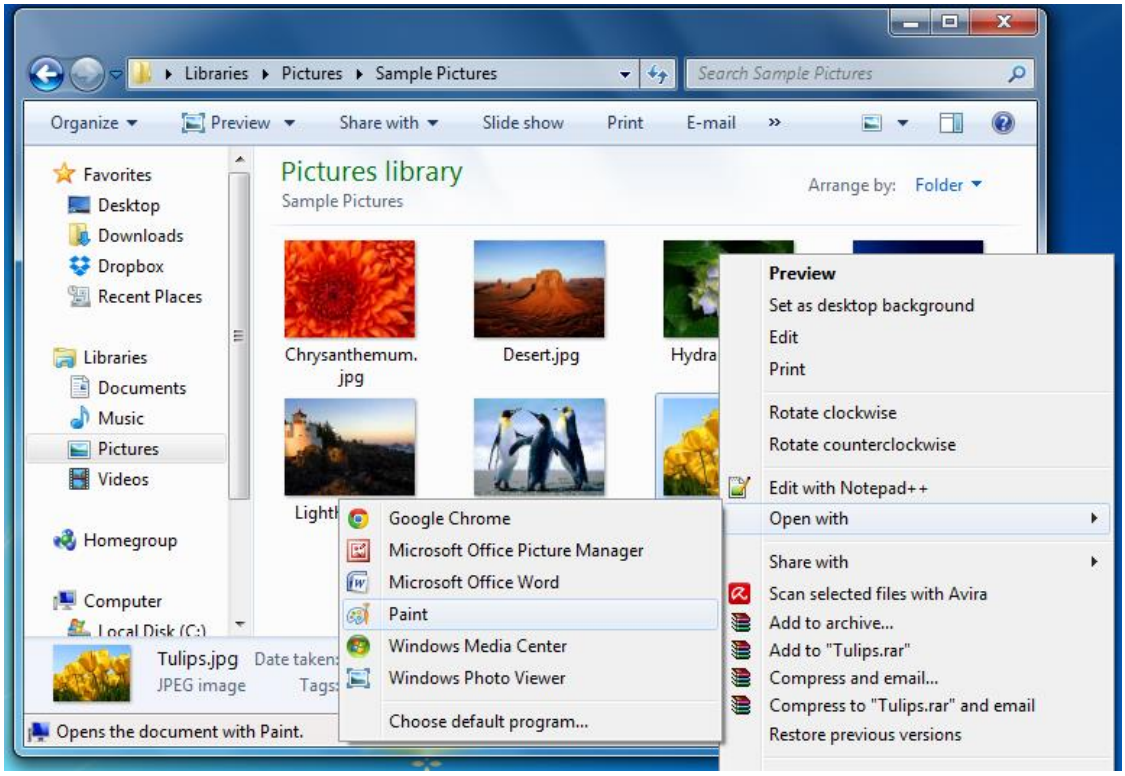
The S-Tools program is a drag and drop software. The files used to create the steganography file can be dragged from the directory into the S-Tools program.

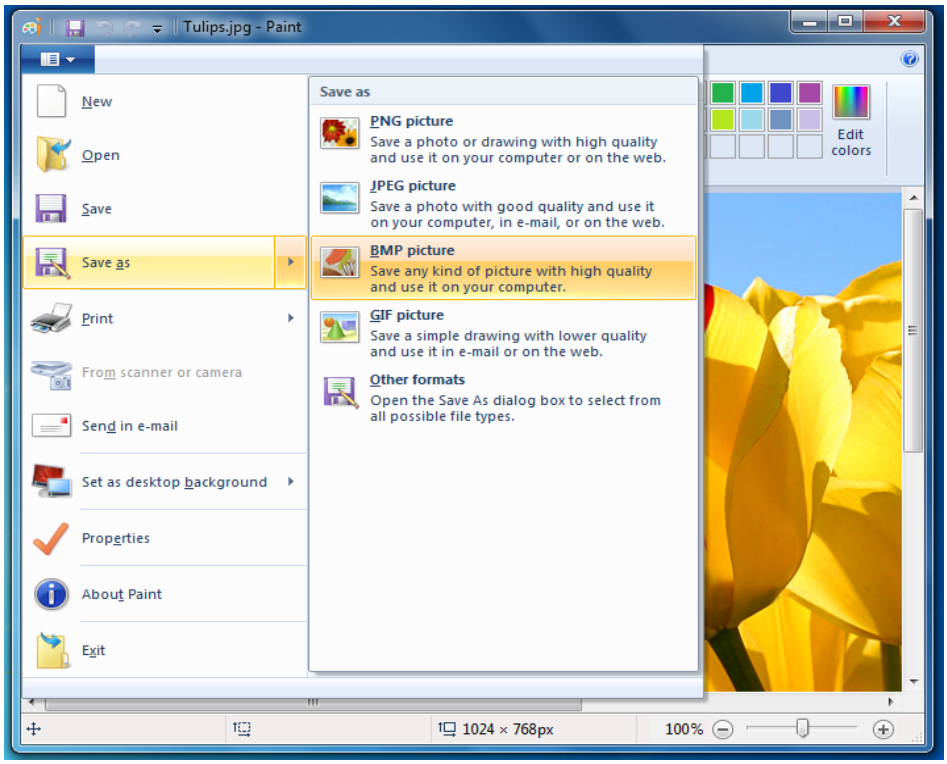
Step 3) Select the file from the directory and drag it over the S-Tools main window and release the
file.

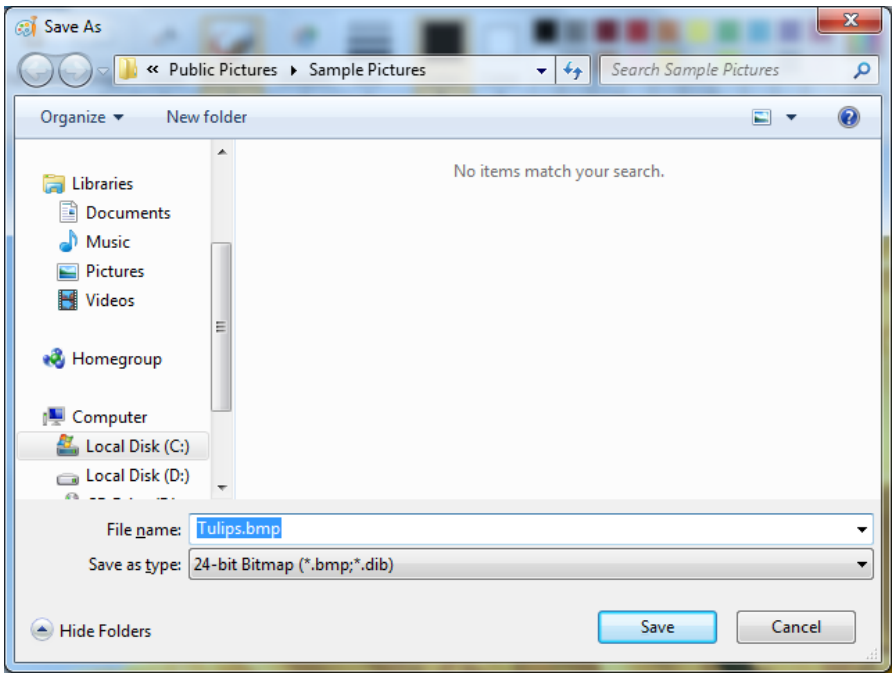
A dialogue box appears indicating that the file type is unknown. Supported file types for audio and image files are shown below:

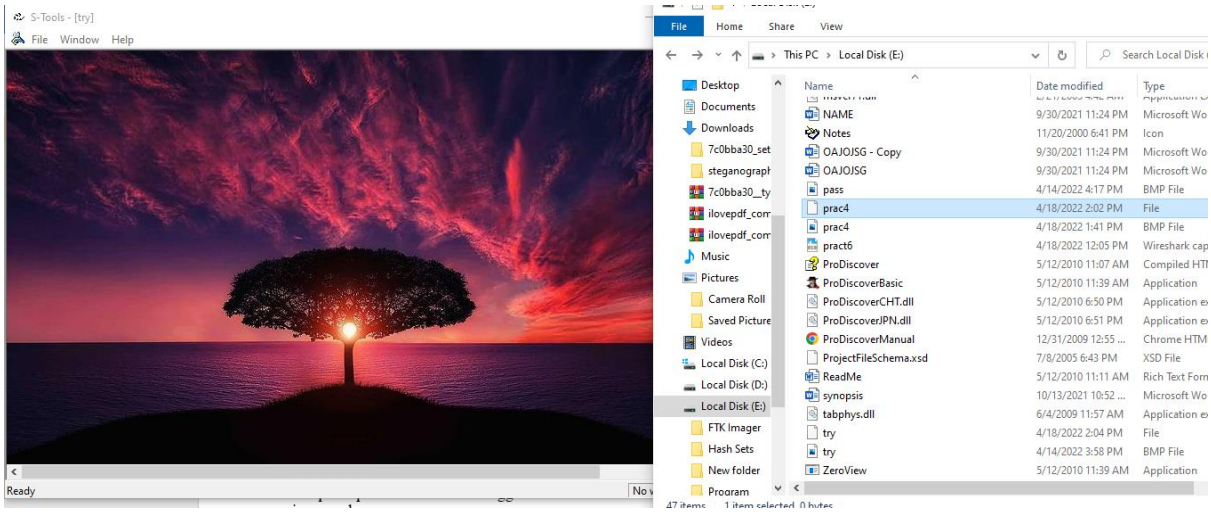
- Audio - *.wav
- Image - *.bmp and *.gif

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



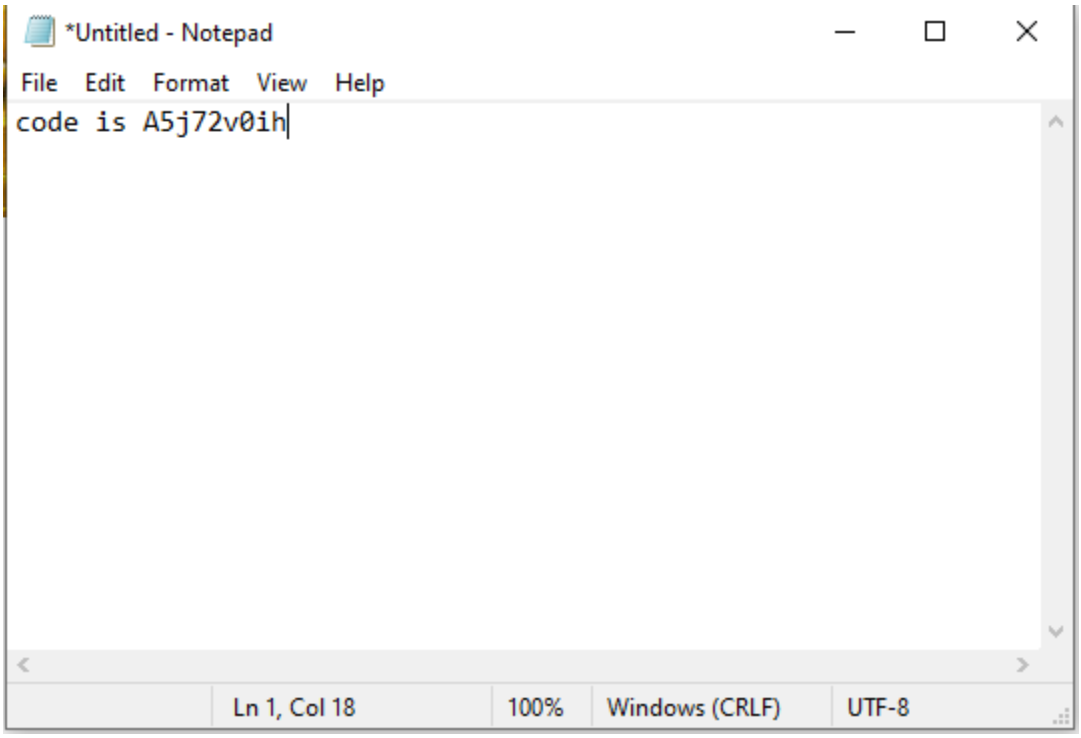

Tulips.jpg - Paint
New
Open
Save
Save as
Print
From scanner or camera
Send in e-mail
Set as desktop background
Properties
About Paint
Exit
Save as
PNG picture
Save a photo or drawing with high quality and use it on your computer or on the web.
JPEG picture
Save a photo with good quality and use it on your computer, in e-mail, or on the web.
BMP picture
Save any kind of picture with high quality and use it on your computer.
GIF picture
Save a simple drawing with lower quality and use it in e-mail or on the web.
Other formats
Open the Save As dialog box to select from all possible file types.
Edit colors
1024 × 768px
100%

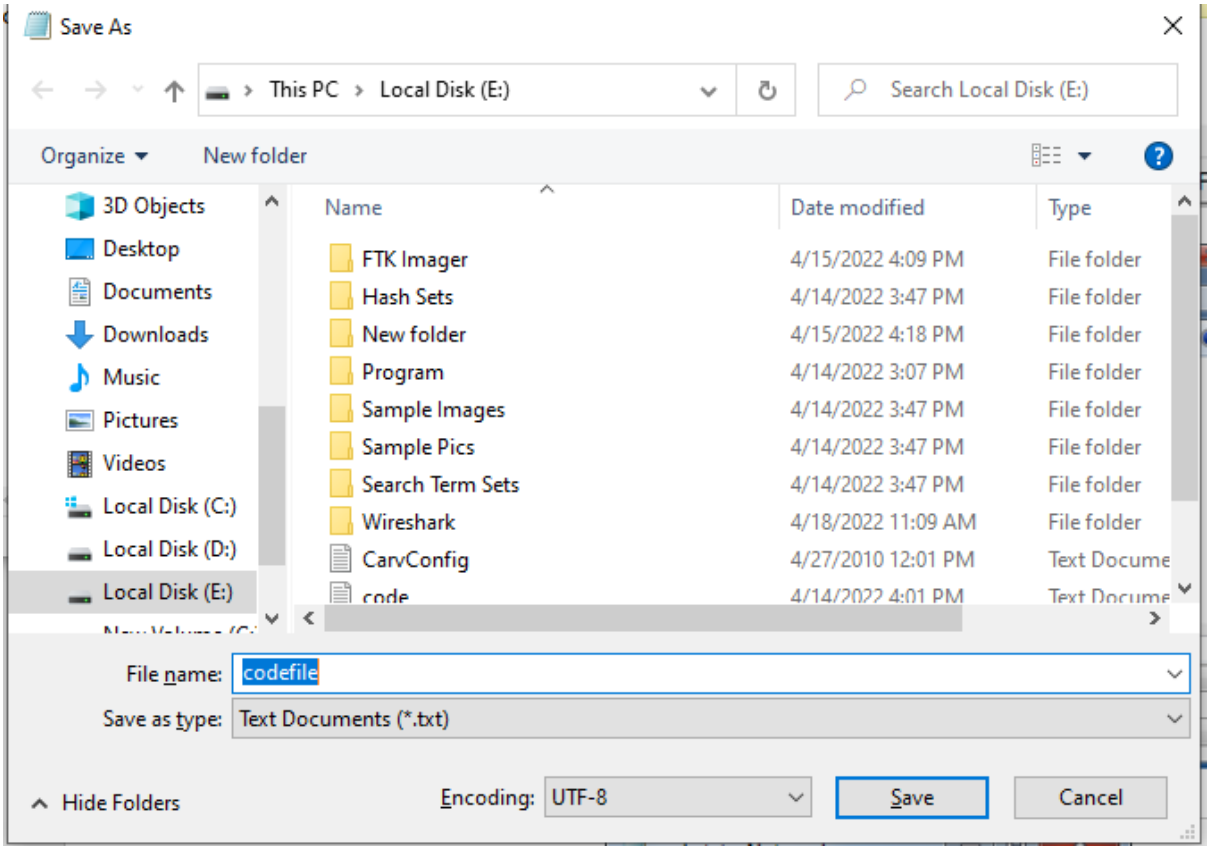

Save As
Public Pictures ▸ Sample Pictures
Search Sample Pictures
Organize
New folder
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Local Disk (C:)
Local Disk (D:)
No items match your search.
File name: Tulips.bmp
Save as type: 24-bit Bitmap (*.bmp;*.dib)
Hide Folders
Save
Cancel

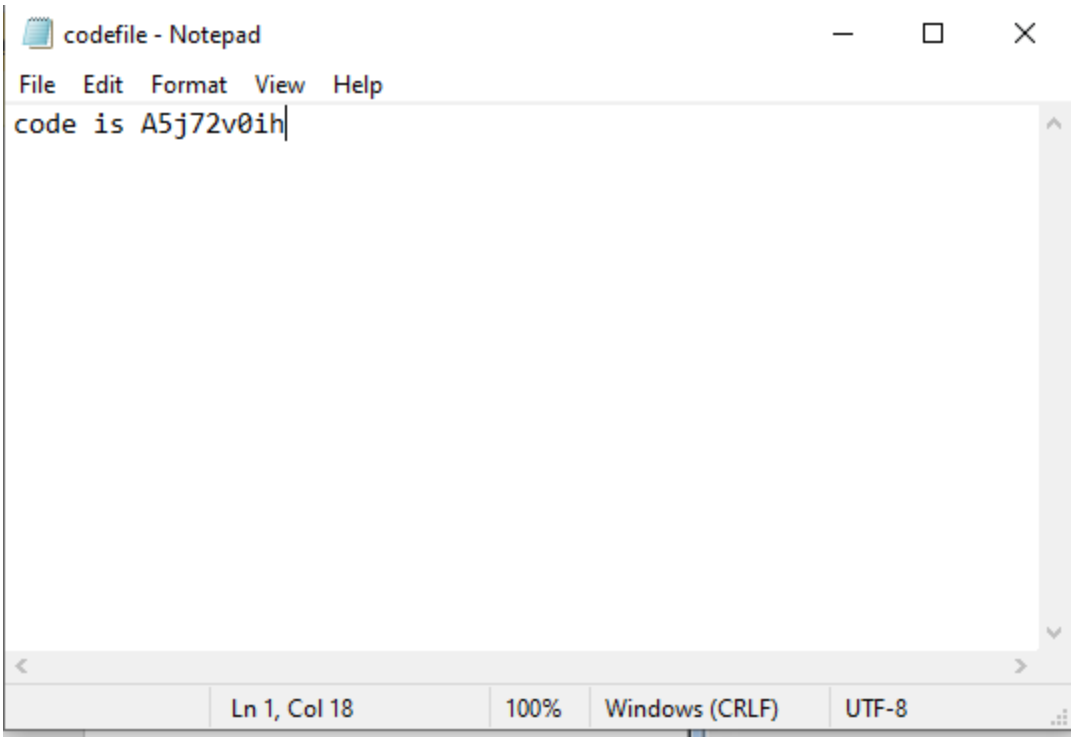


Step 4) Select a valid audio file or image as the base file for the steganography file. The Tulips.bmp was selected and dragged onto the main window of the S-Tools program. The image is opened.

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

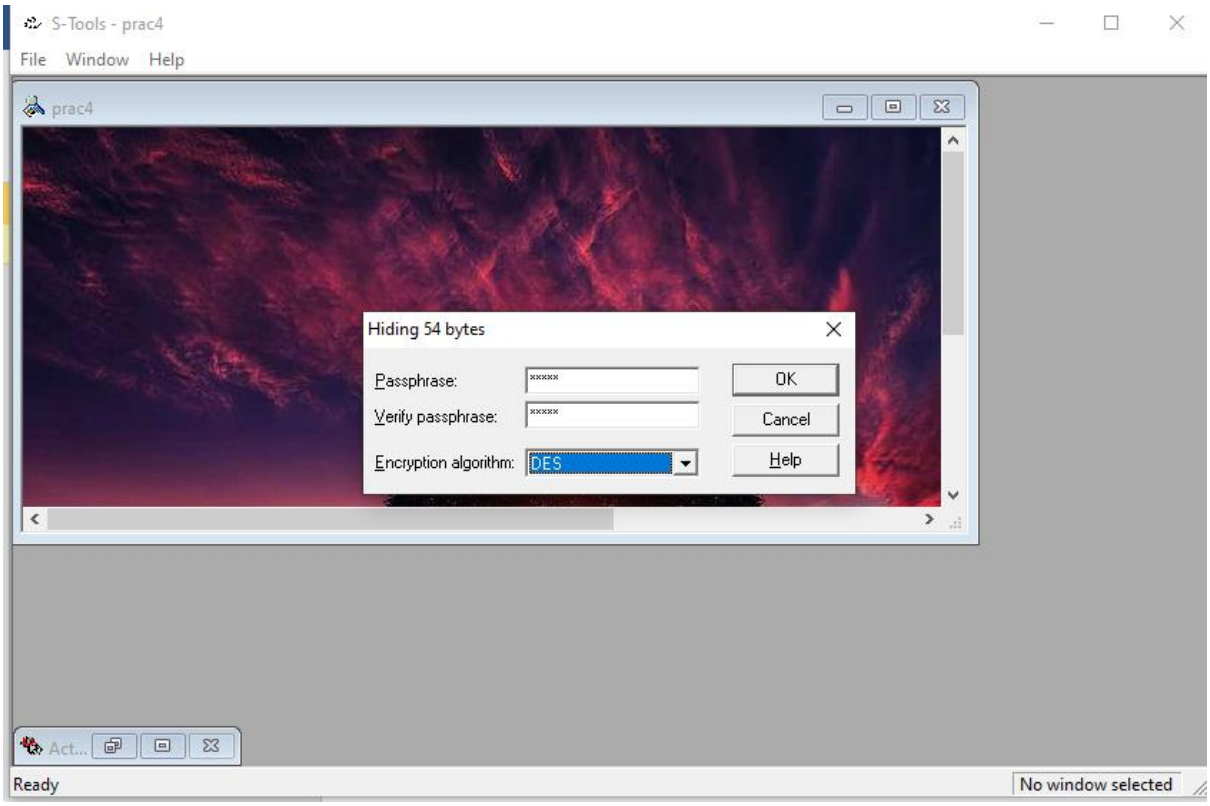

*Untitled - Notepad
File Edit Format View Help
code is A5j72v0ih
Ln 1, Col 18
100%
Windows (CRLF)
UTF-8


Save As
This PC › Local Disk (E:)
Search Local Disk (E:)
Organize
New folder
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Local Disk (D:)
Local Disk (E:)
Name
Date modified
Type
FTK Imager 4/15/2022 4:09 PM File folder
Hash Sets 4/14/2022 3:47 PM File folder
New folder 4/15/2022 4:18 PM File folder
Program 4/14/2022 3:07 PM File folder
Sample Images 4/14/2022 3:47 PM File folder
Sample Pics 4/14/2022 3:47 PM File folder
Search Term Sets 4/14/2022 3:47 PM File folder
Wireshark 4/18/2022 11:09 AM File folder
CarvConfig 4/27/2010 12:01 PM Text Docume
code 4/14/2022 4:01 PM Text Docume
File name: codefile
Save as type: Text Documents (*.txt)
Hide Folders
Encoding: UTF-8
Save
Cancel



Step 6) The *.txt text file is selected and dragged on top of the base image. Release the file while the cursor is still on top of the base file.

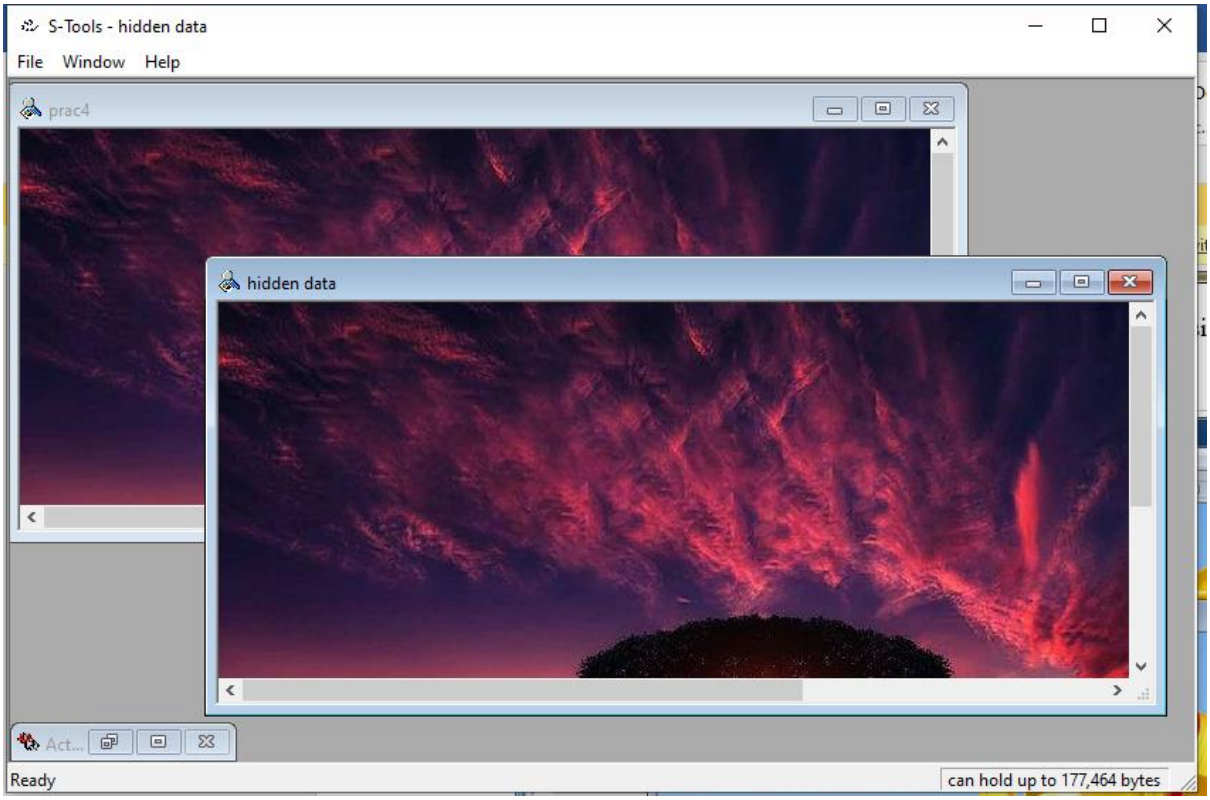
Step 7) A dialogue box will appear asking the user to enter and verify a passphrase. Additionally, the user will have to select an encryption algorithm.



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:

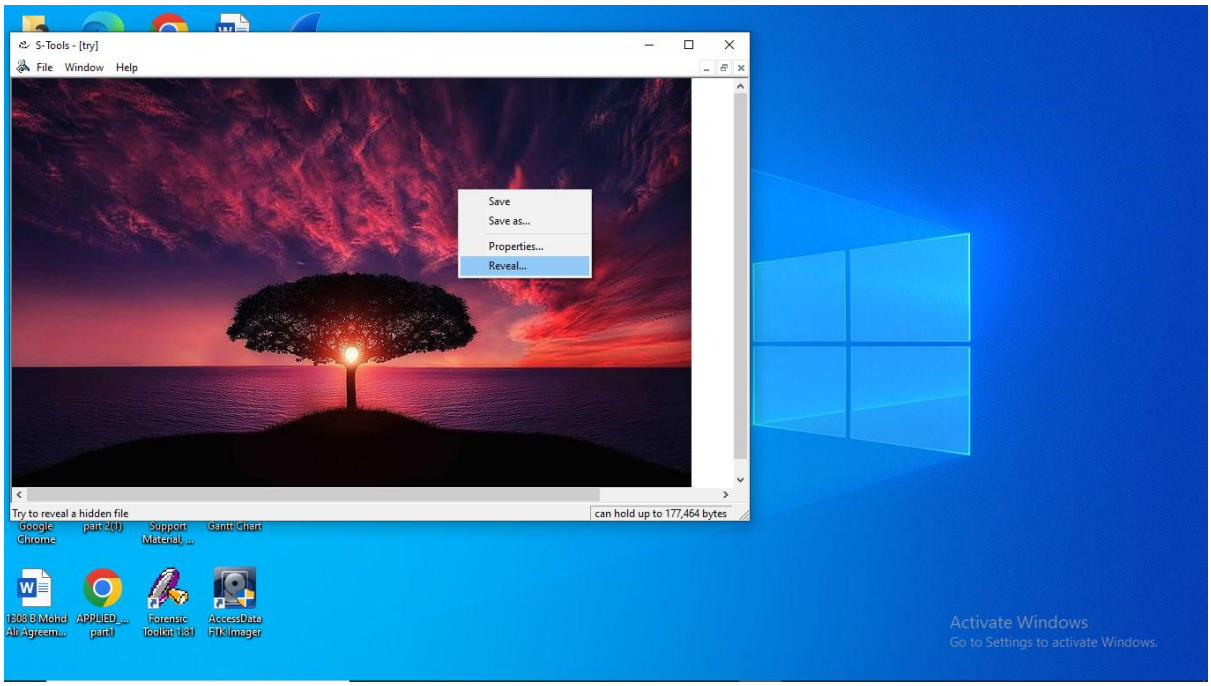
- Save
- Save As
- Properties
- Reveal

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

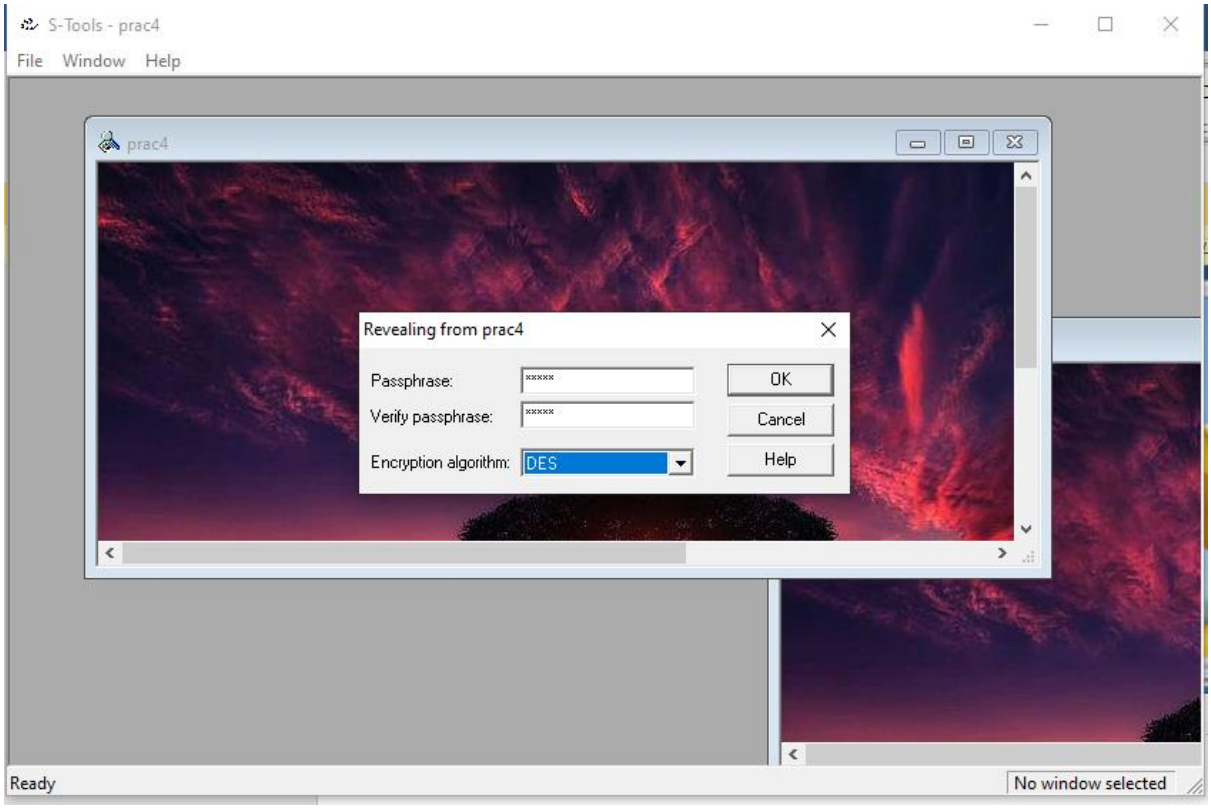
- Width and Height of the image
- Bits per pixel
- Memory Usage (file size in bytes)
- Compression

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.

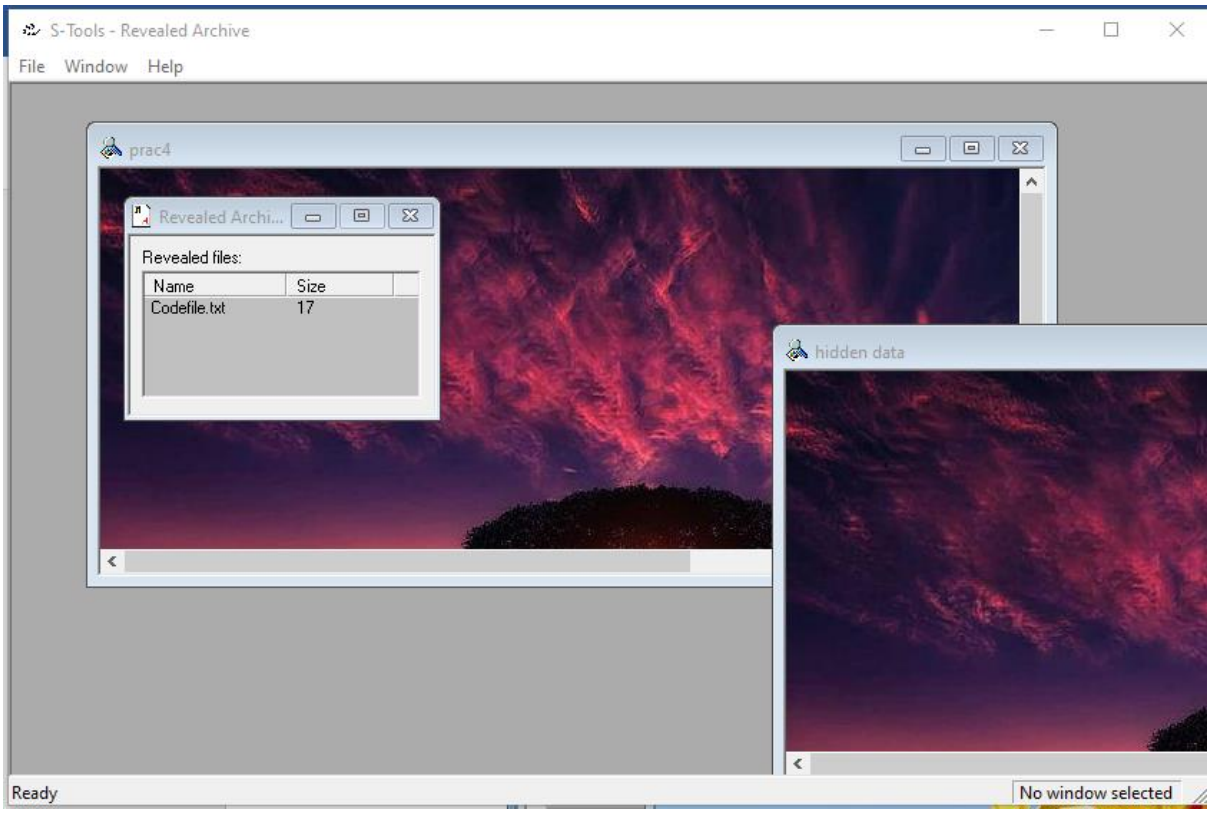
Notice that the title of the dialogue box has changed to ‘Revealing from Tulips.bmp’



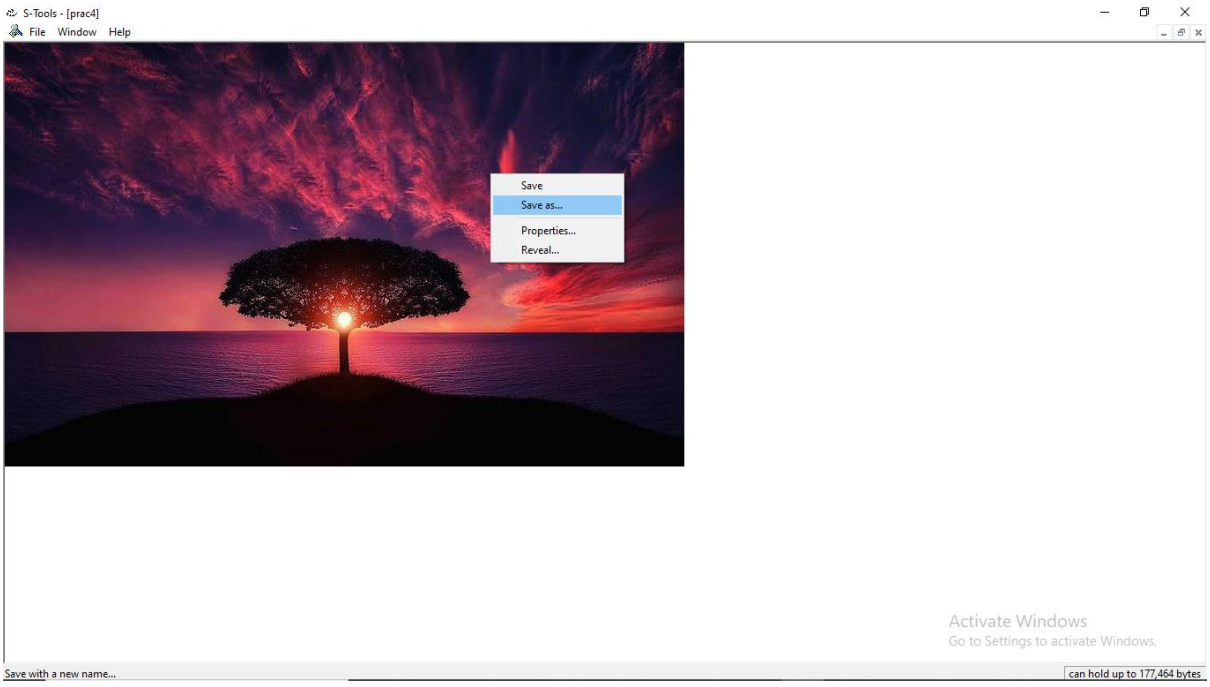
Step 14) Enter a passphrase twice, select the encryption algorithm, and select the 'OK' button.



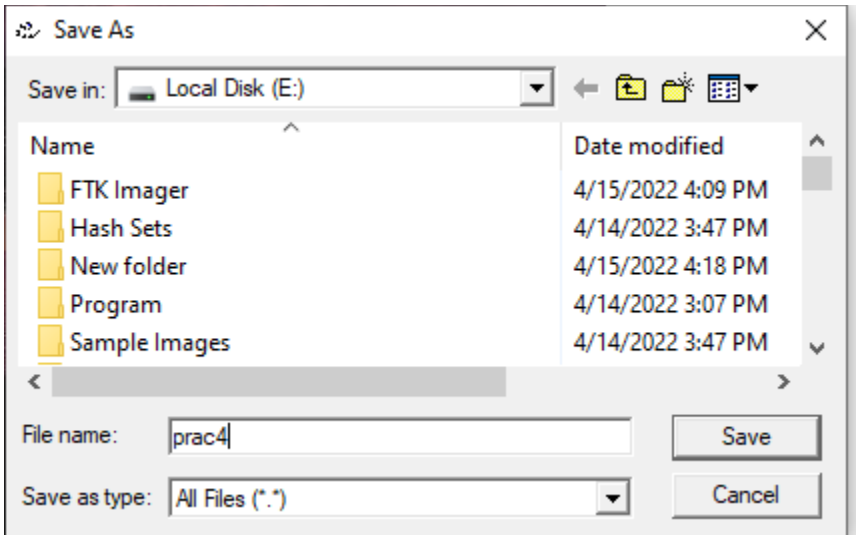
Step 15) A 'Revealed Archive' dialogue box will display which contains the file name and size of the hidden file.



Step 16) Select the 'Save As' button.

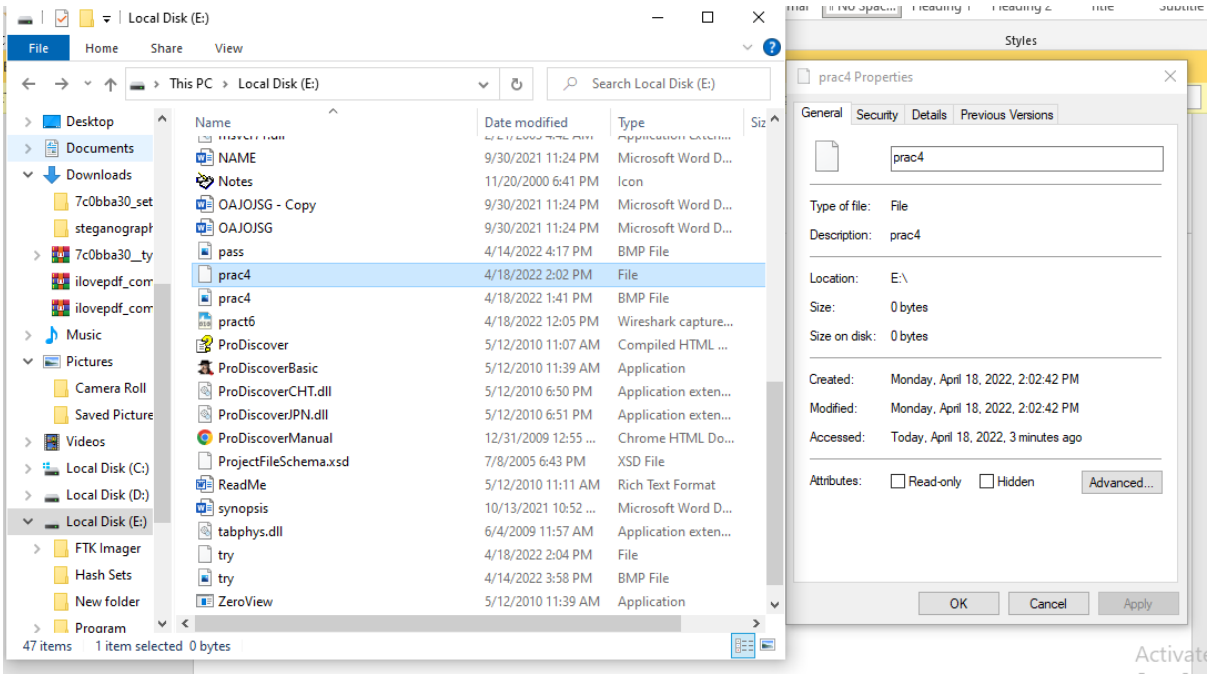


Step 17) A ‘Save As’ dialogue box will appear. Enter a valid file name, select the working directory and select the ‘Save’ button.



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.

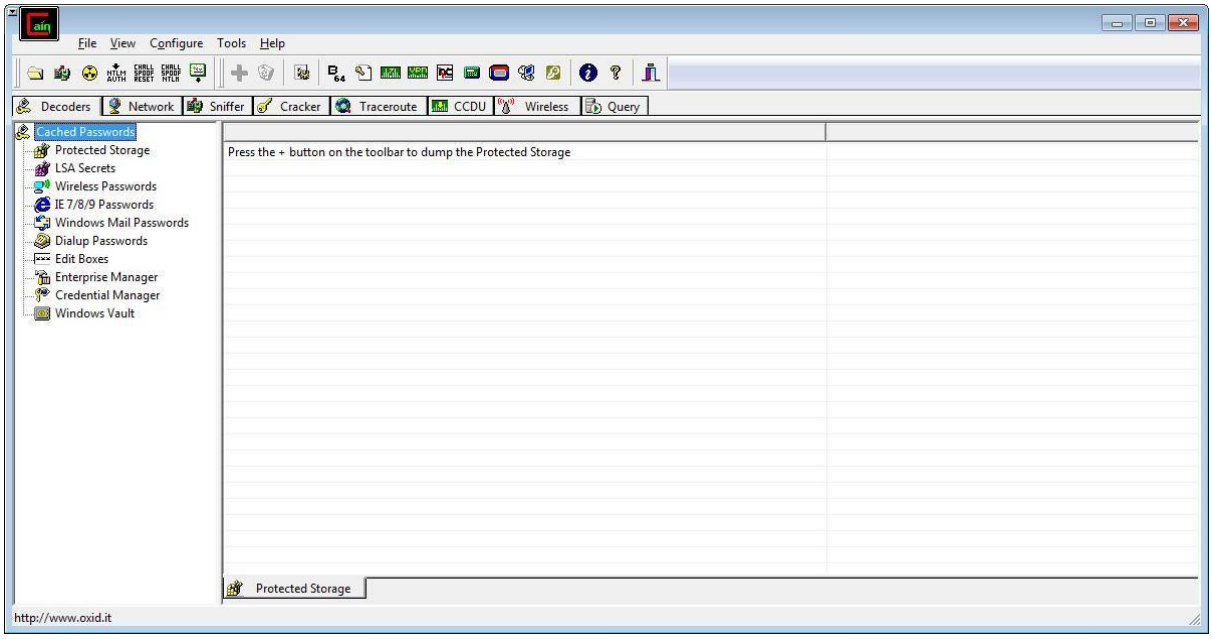


Practical No: 07

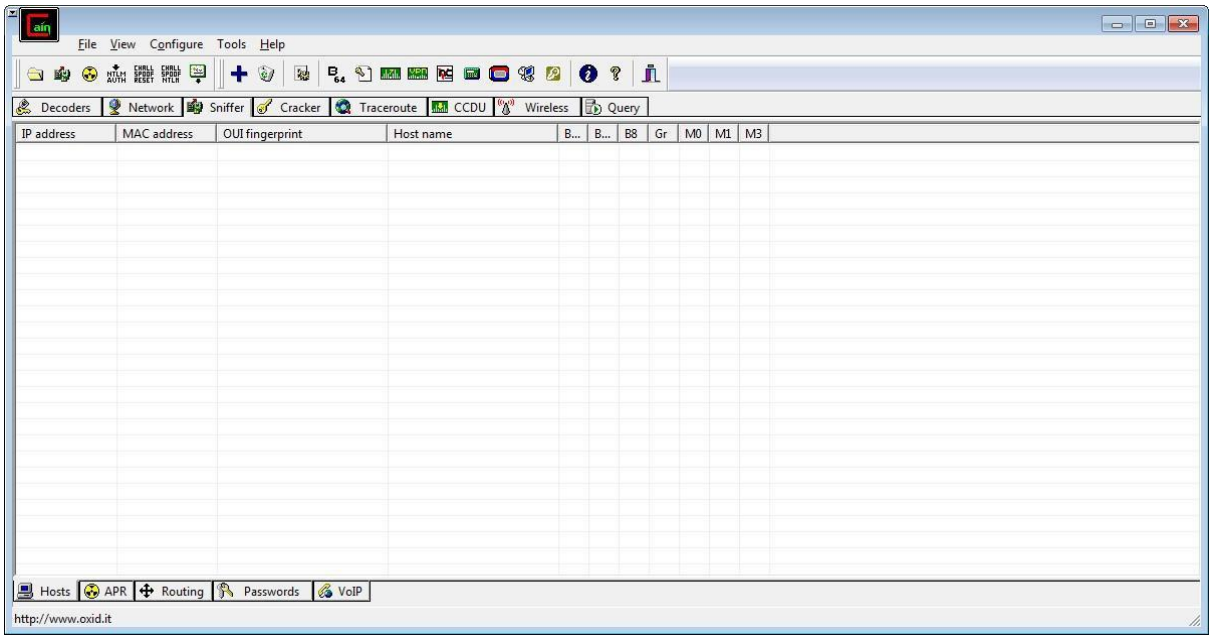
Practical No: 07

Aim: Password Cracking Using Cain and Abel.

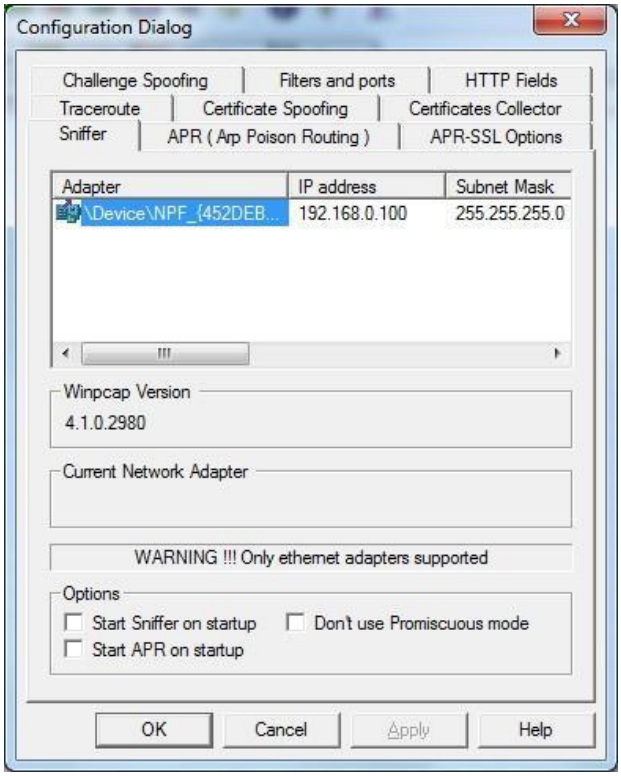
Step 1 : Install and open cain and abel.



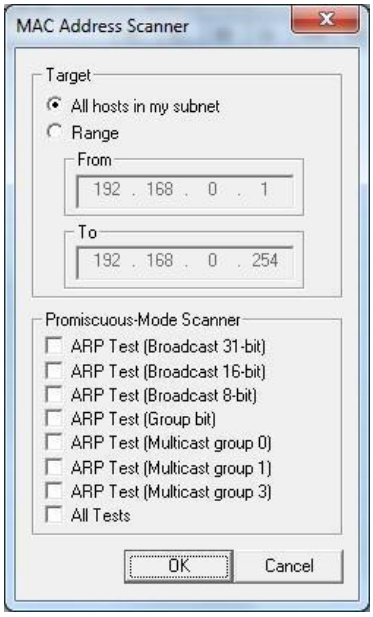
Step 2 : Select sniffer on the top.



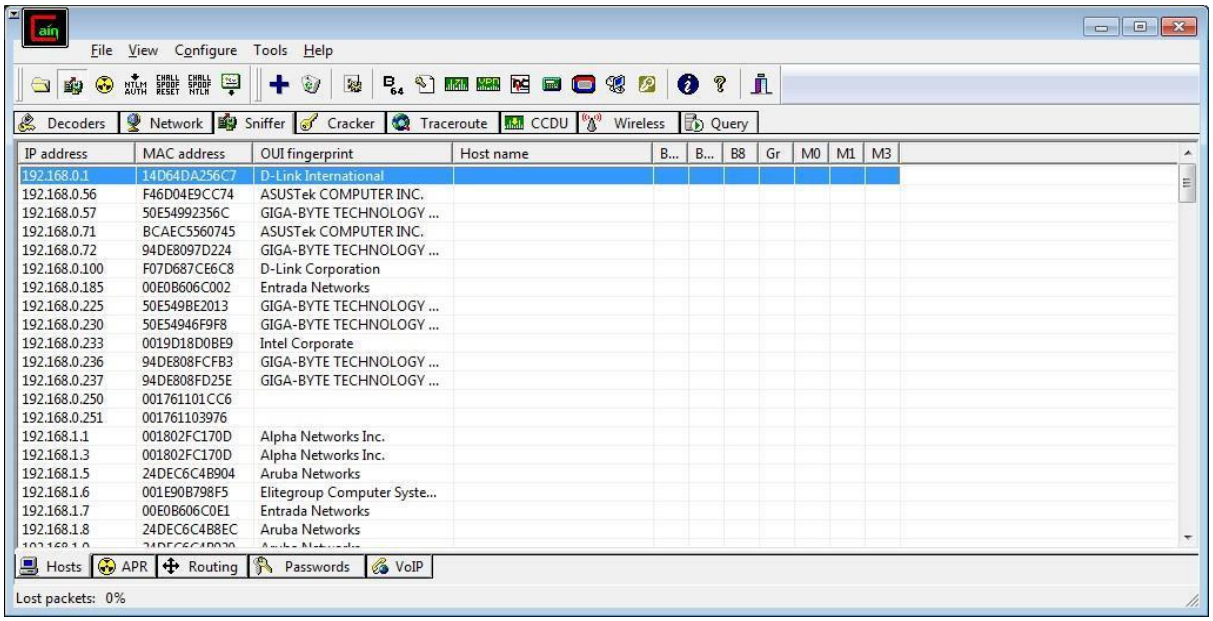
Step 3 : Next to folder icon click on icon name start/stop sniffer. Select device and click on ok.



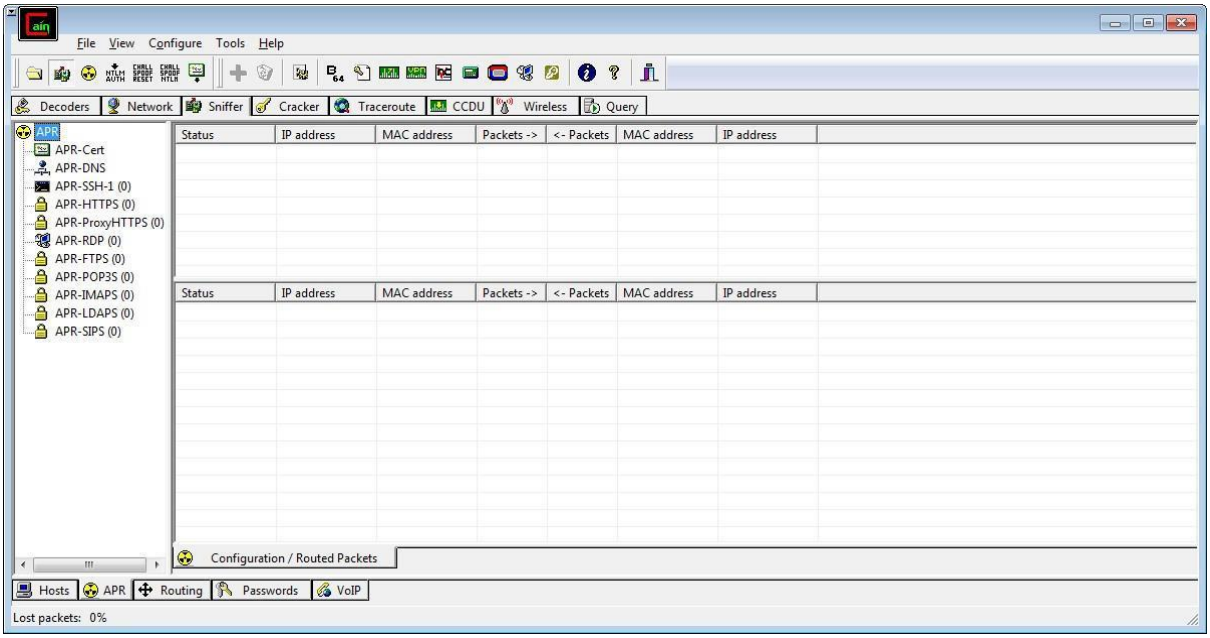
Step 4 : Click on “+” icon on the top. Click on ok.


MAC Address Scanner
Target
All hosts in my subnet
Range
From
192 . 168 . 0 . 1
To
192 . 168 . 0 . 254
Promiscuous-Mode Scanner
ARP Test (Broadcast 31-bit)
ARP Test (Broadcast 16-bit)
ARP Test (Broadcast 8-bit)
ARP Test (Group bit)
ARP Test (Multicast group 0)
ARP Test (Multicast group 1)
ARP Test (Multicast group 3)
All Tests
OK
Cancel

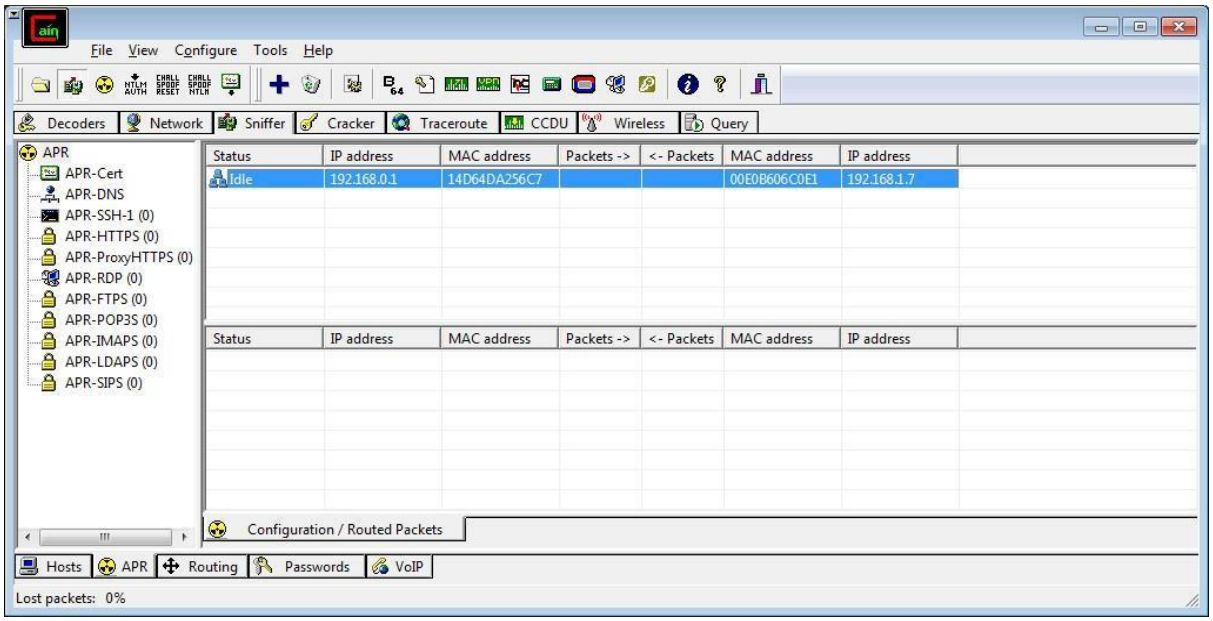
Step 5 : Shows the Connected host.



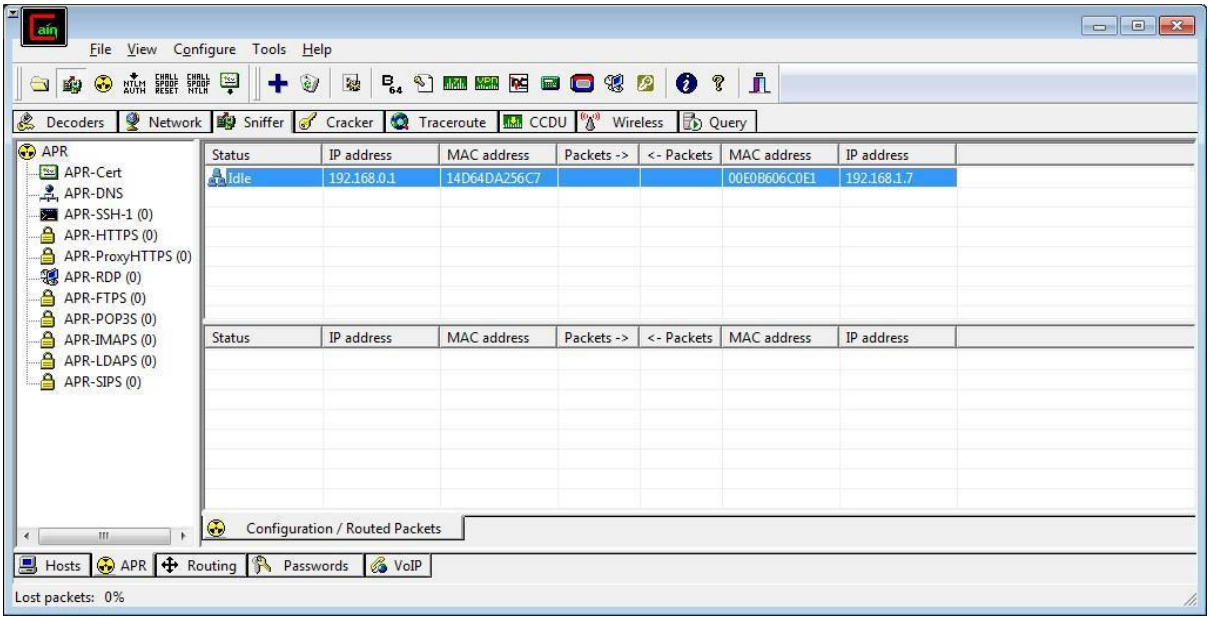
Step 6 : Select Arp at bottom.



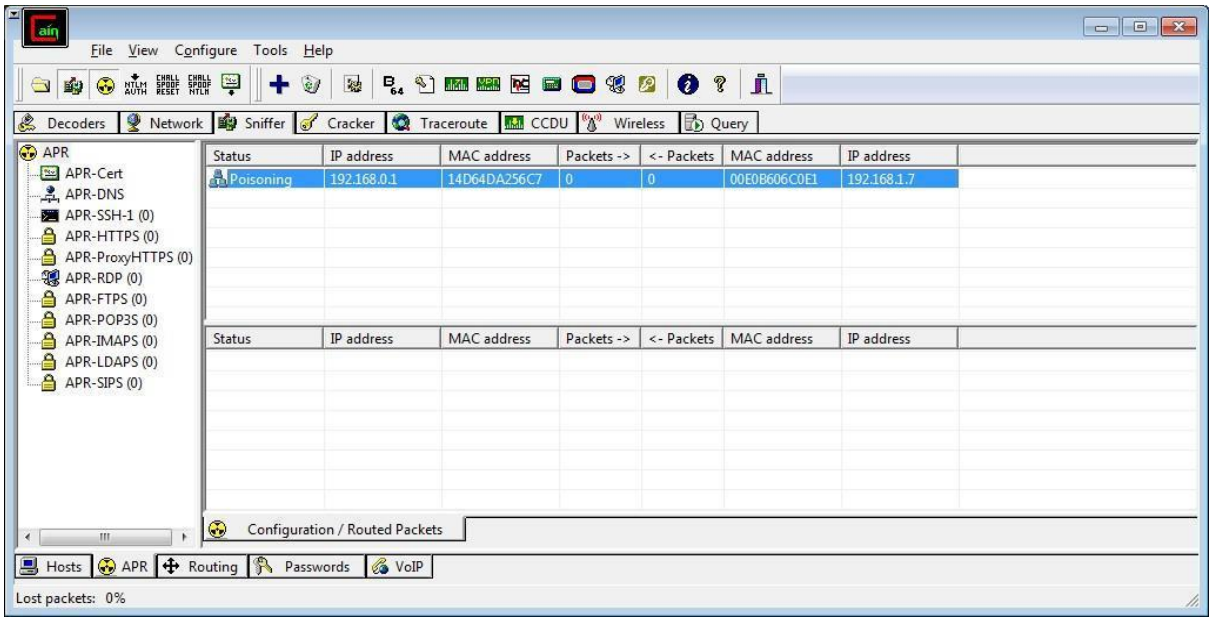
Step 7 : Click on “+” icon at the top.



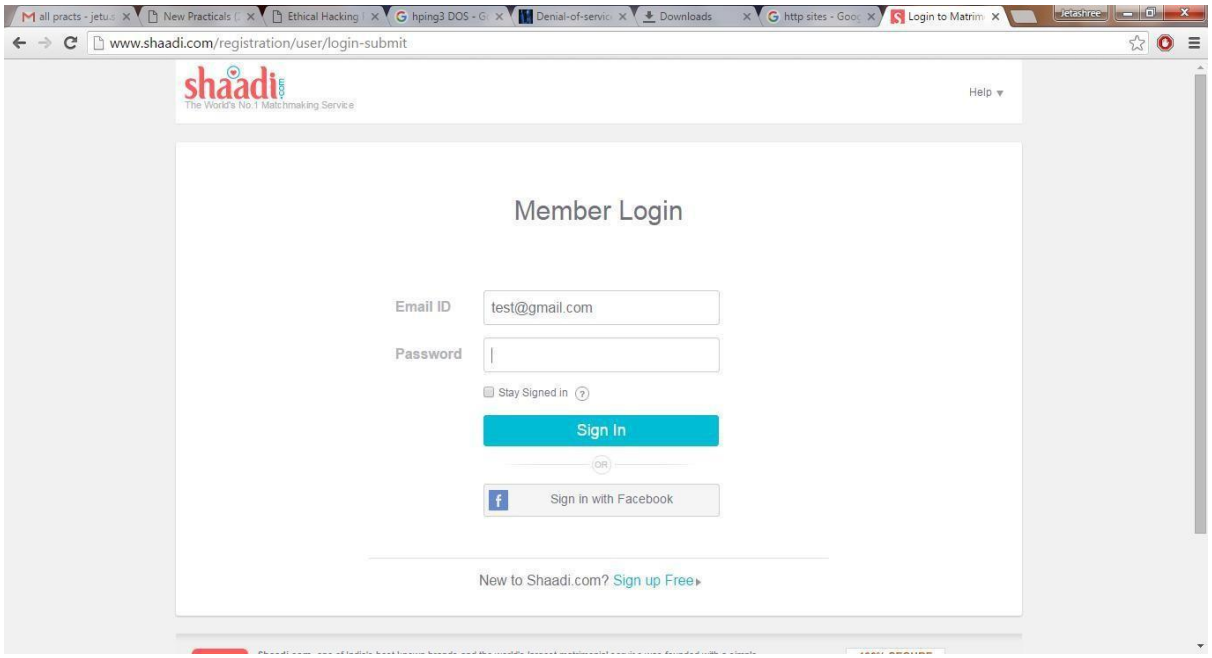
Step 8 : Click on start/stop ARP icon on top.



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.