INDEX

Sr. no	Topic	Date	Sign
1	File System Analysis using The SleuthKit (Autospy)		
2	Explore Windows forensic tools (OSForensics)		
3	a. Creating a Forensic Image using FTK Imager/Encase Imager: -Creating Forensic Image -Check Integrity of Data -Analyze Forensic Image b. Perform data acquisition using USB Write Blocker		
4	a. Exploring Access data FTK to recover deleted files. b. Exploring Access data FTK for Data Carving, Using Filters, Searching the Registry. c. Email Forensic using Forensic Toolkit d. Recover Deleted files using Recuva, PC Inspector File Recovery, Recover My Files		
5	a. Using Web attack detection tools & Using Log & Traffic Capturing & Analysis Tools [Wireshark] b. Using Network Forensic Analysis Tool (NetworkMiner) c. Using Network Traffic Analyser tool Iris		
6	Using Data Acquisition Tools [ProDiscoverPro]		
7	a. Using Steganography Tools [S-Tools] b. Using Whitespace Steganography tool SNOW		
8	Performing Sniffing [Cain & Abel]		
9	a. Scan Registry using RegScanner and tools for RAM capture, Virtual memory etc. b. Study Registry Viewer tool (Alien Registry Viewer)		
10	Mobile Forensic Analysis.		

Practical No – 1

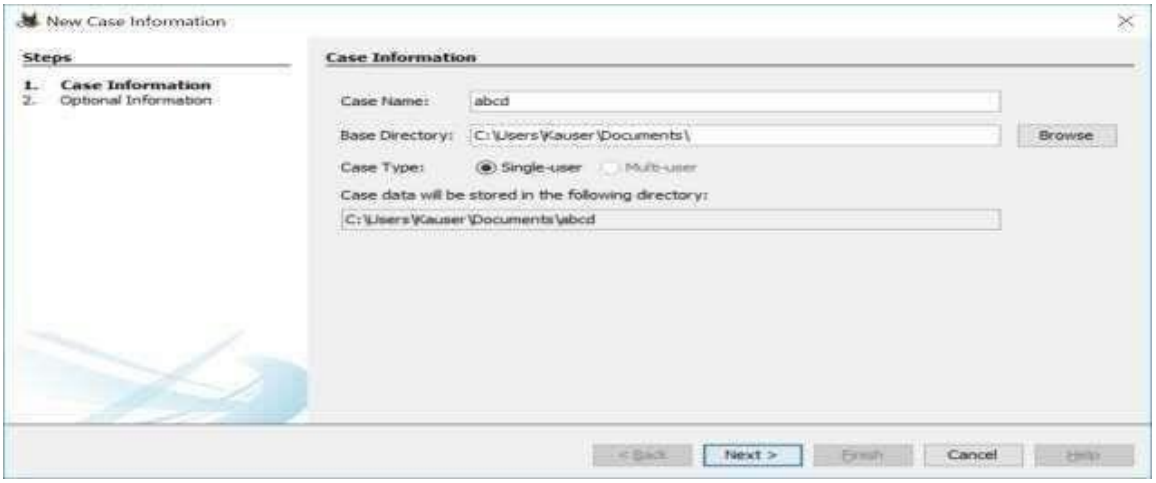
Aim: Forensics Case Study:

Solve the Case study (image file) provide in lab using Autopsy

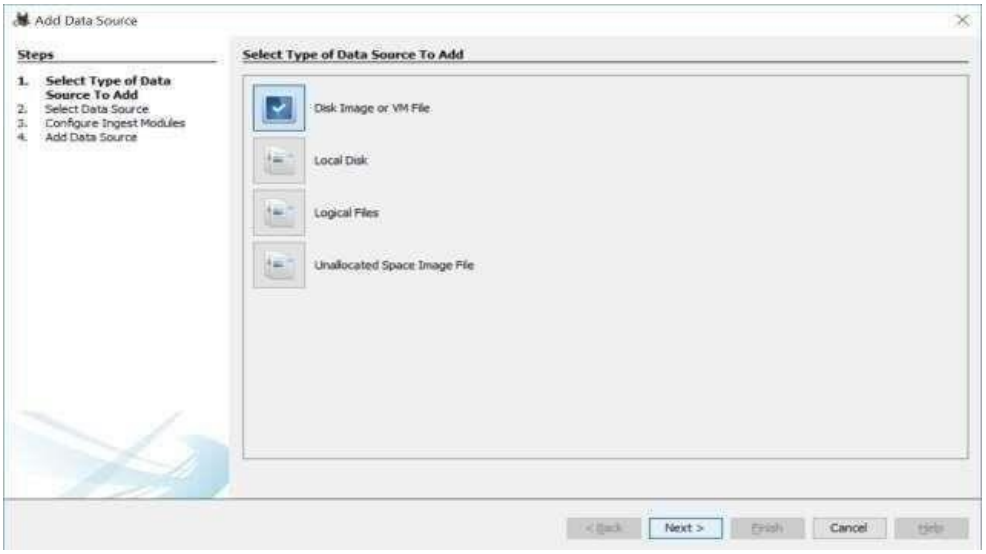
Steps:

1. Start Autopsy
2. Select New Case

3. Enter Case Information and Base Directory & click on finish

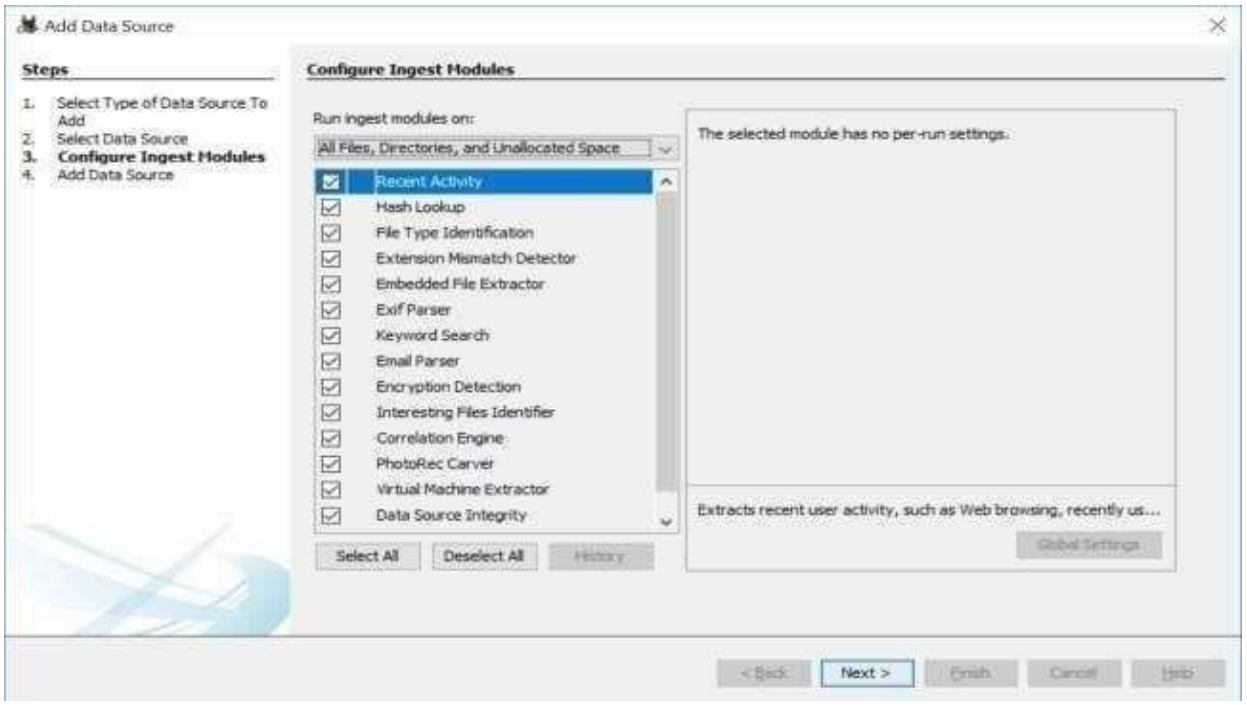


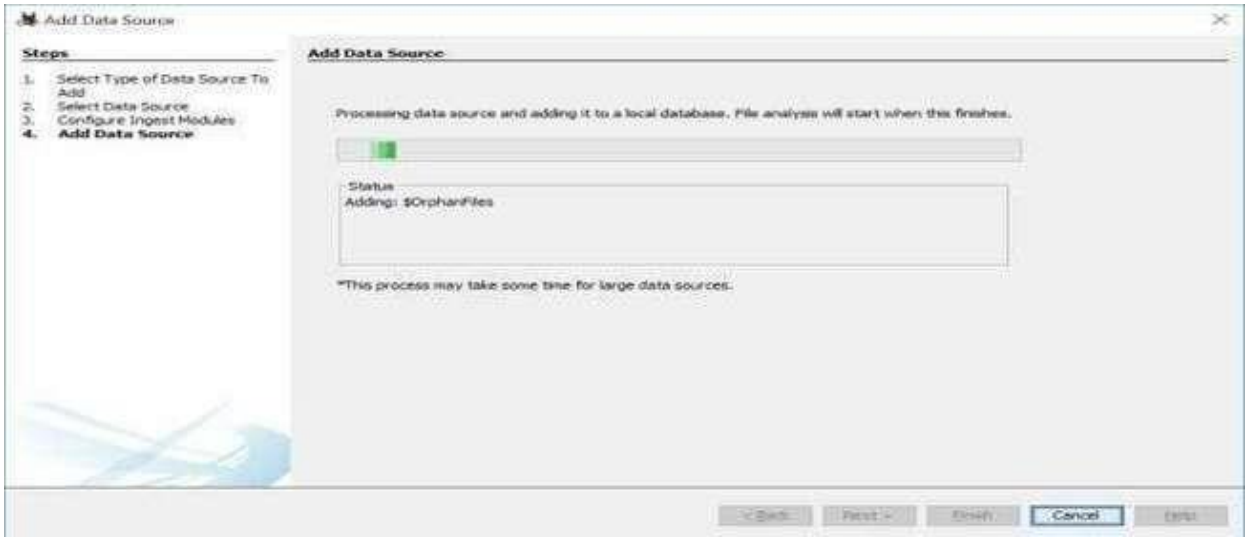
4. Select the type of Data Source that has to be added



5. Select Data Source(here a previously made image file of a USB is selected)

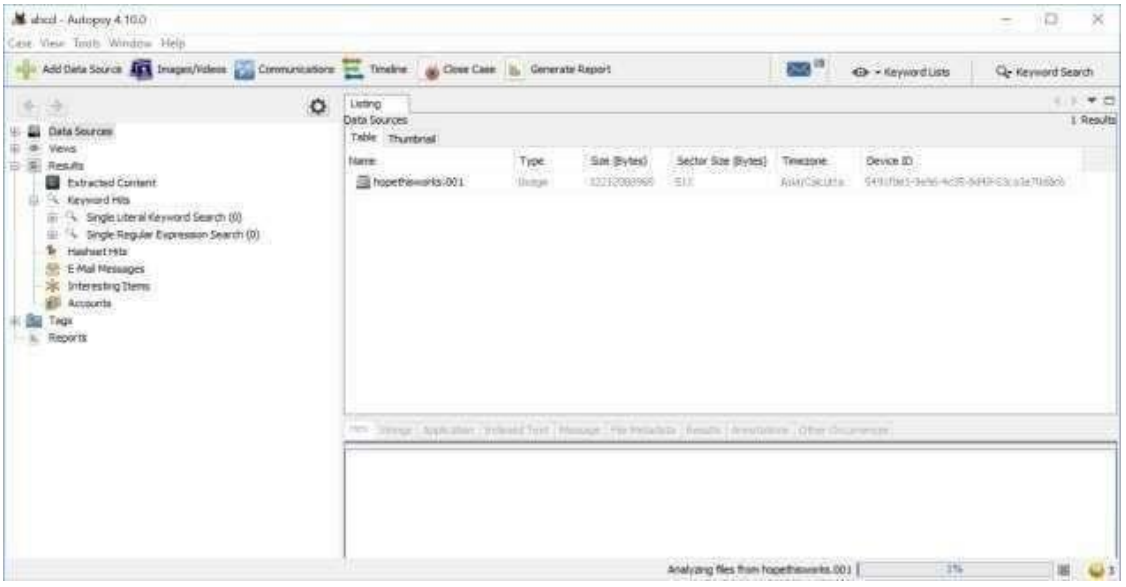
6. Select all ingest modules



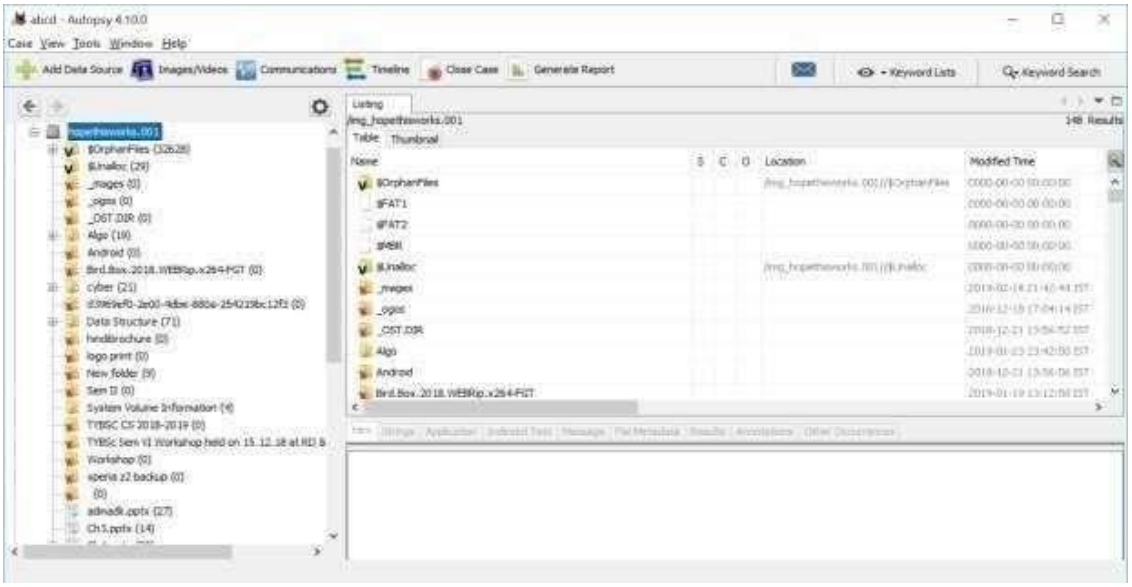


7.Wait for Data source to process and be added to local database. Click Finish

8. Now Autopsy window will appear and it will analyzing the disk that we have selected

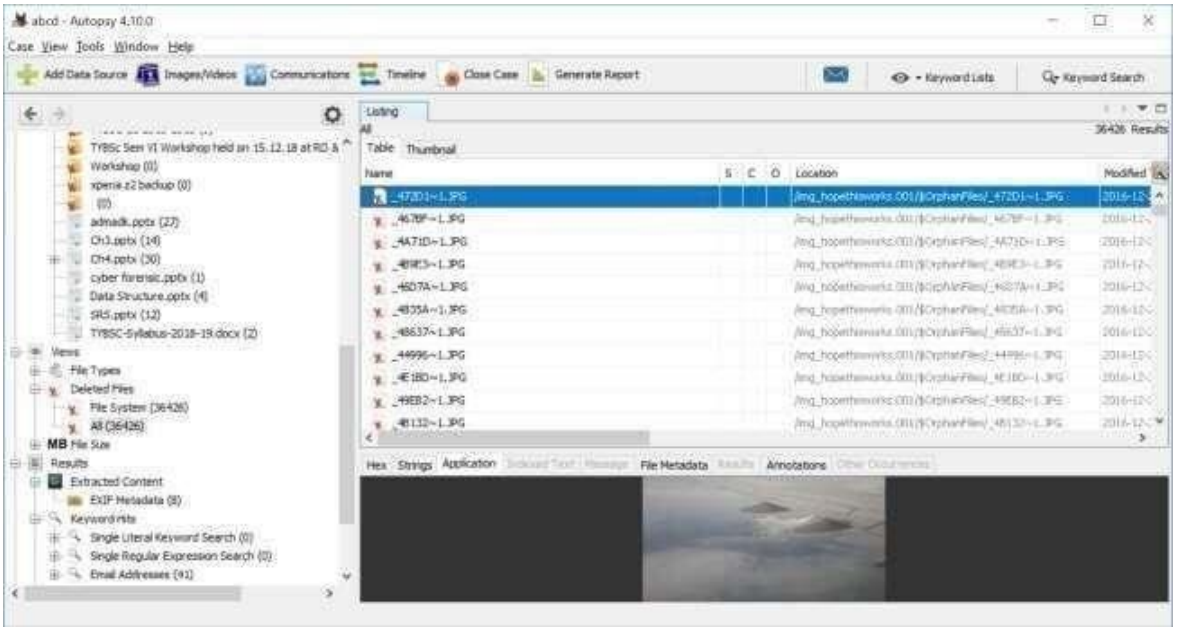


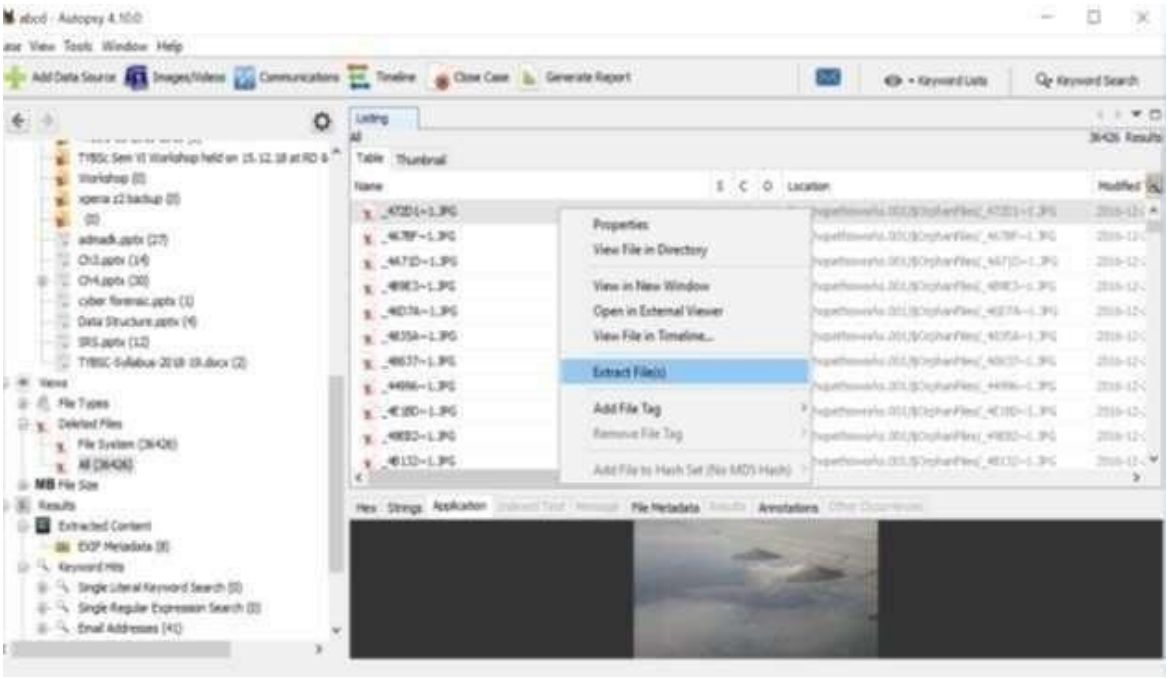
9. All files will appear in table tab select any file to see the data.



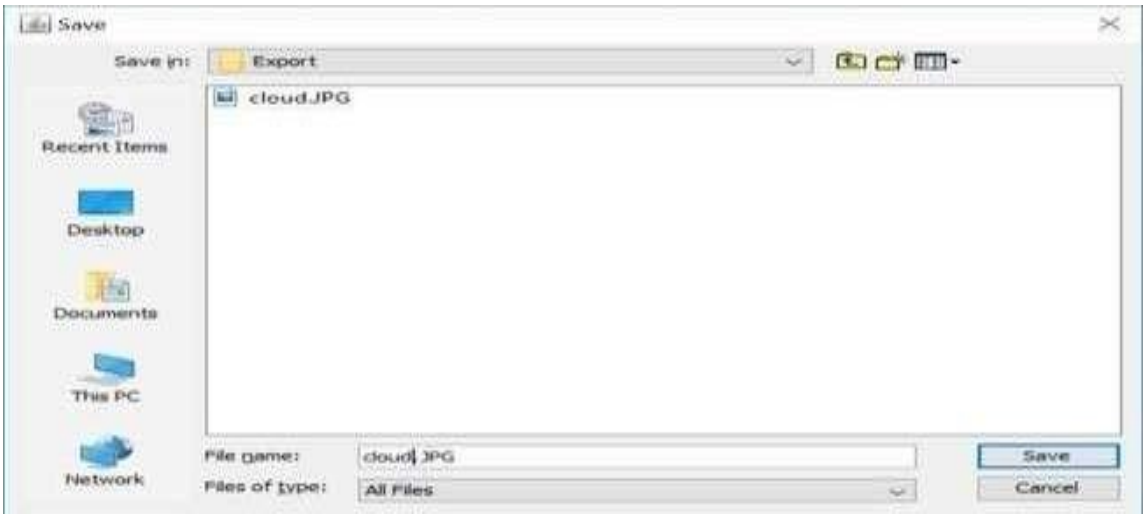
10. Expand the tree from left side panel to view the files and then expand the deletedfiles node

11. To recover the file, go to view node-> Deleted Files node , here select any file andright click on it than select Extract Files option.

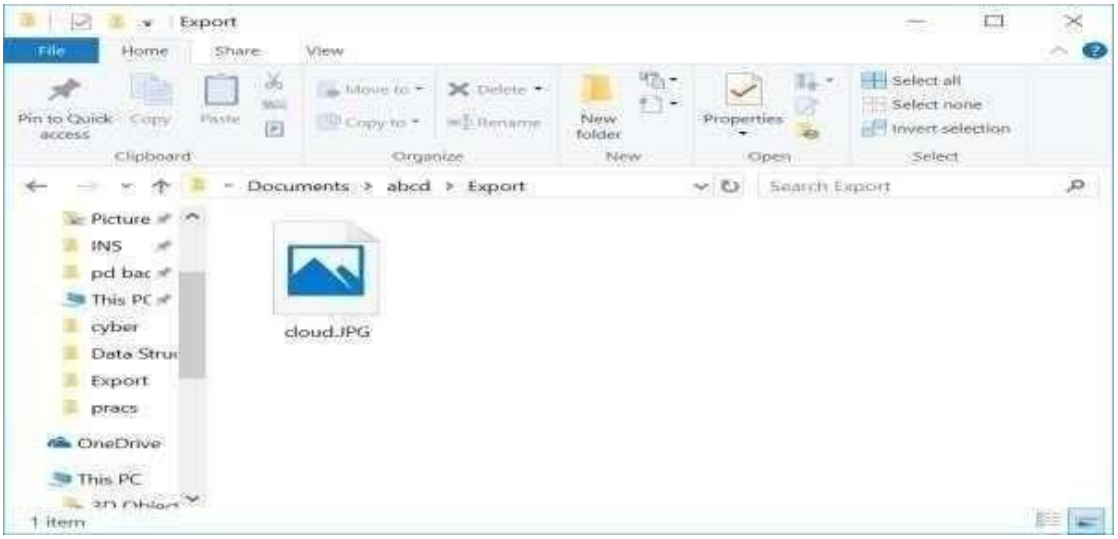




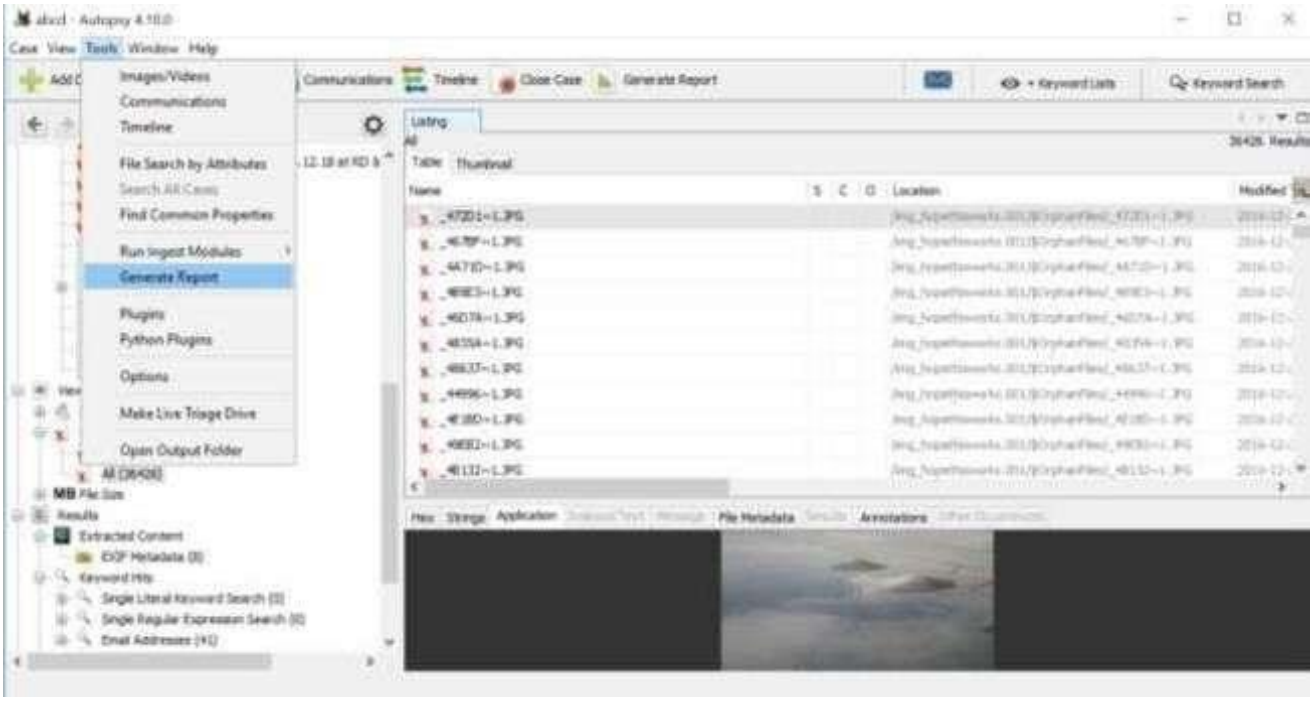
12. By default Export folder is choose to save the recovered file.



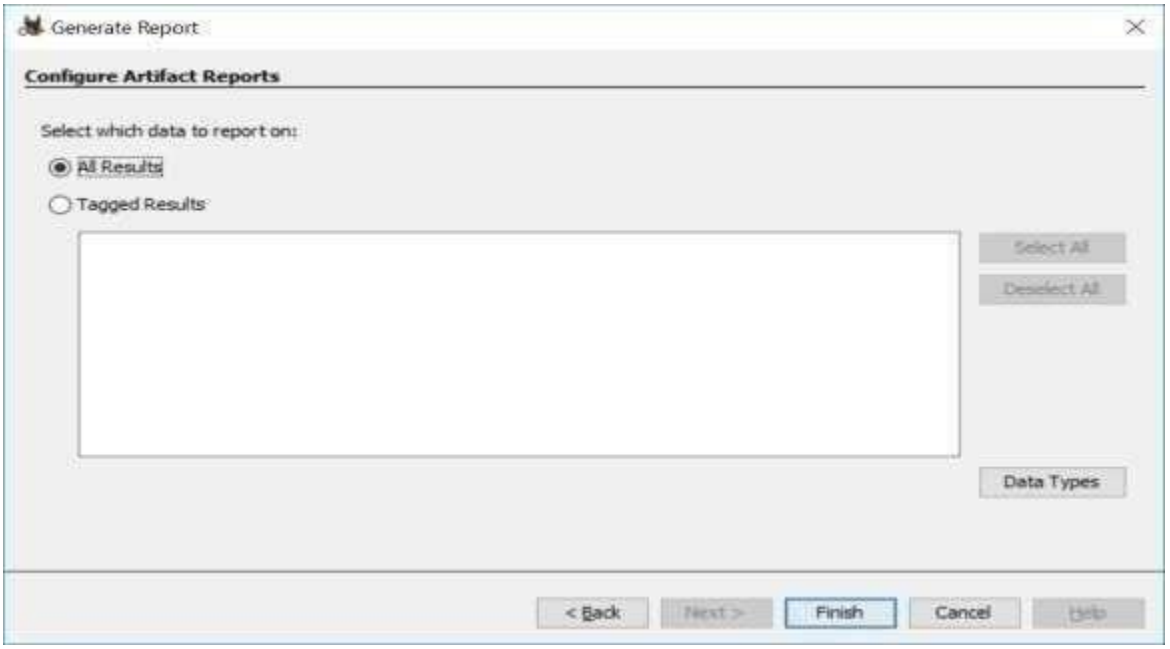
13. Now go to the Export Folder to view Recover file.

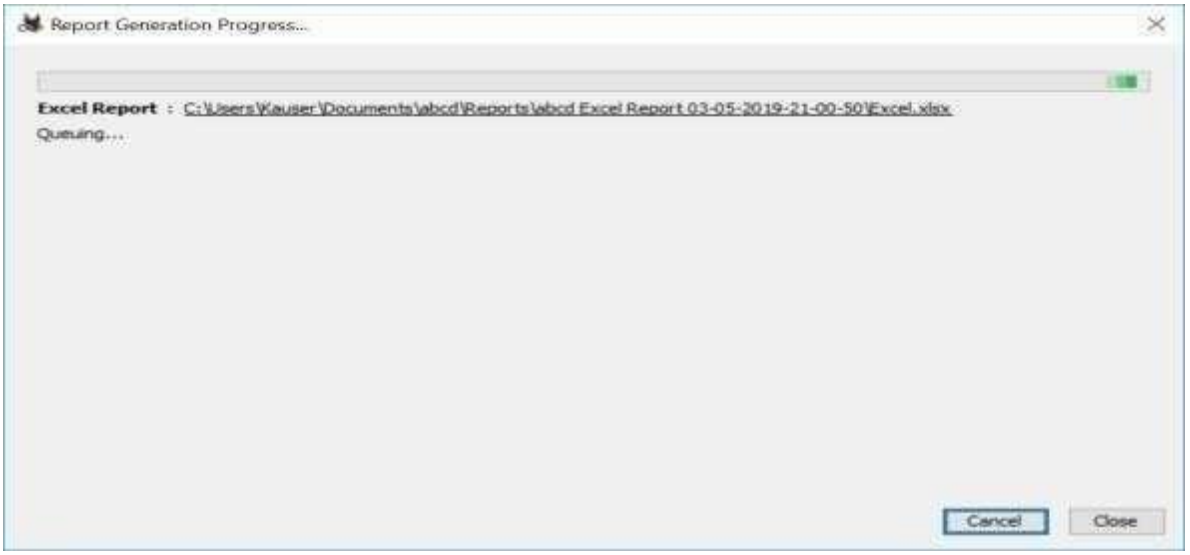


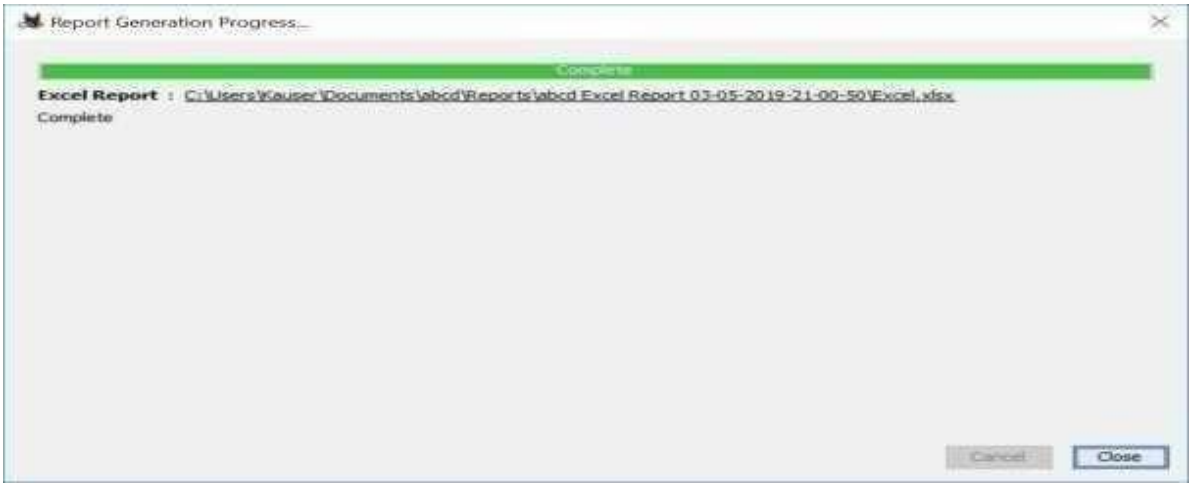
14. Click on Generate Report from autopsy window and Select the Excel format and click on next



15. Click Finish after selecting All Results

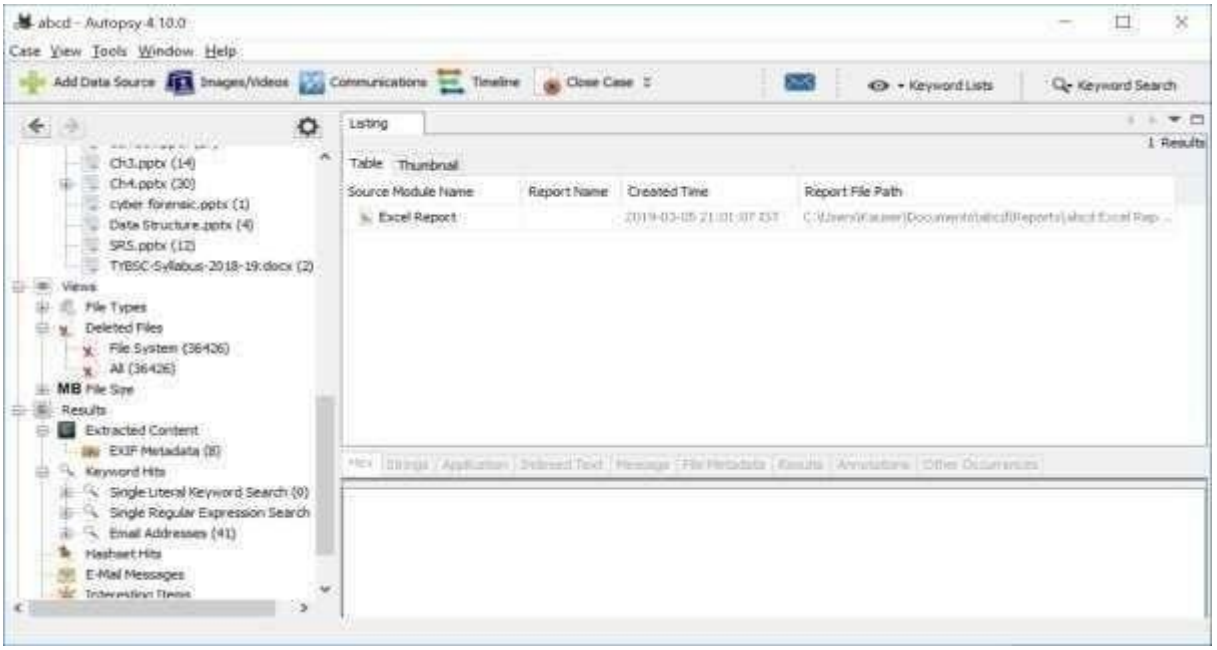


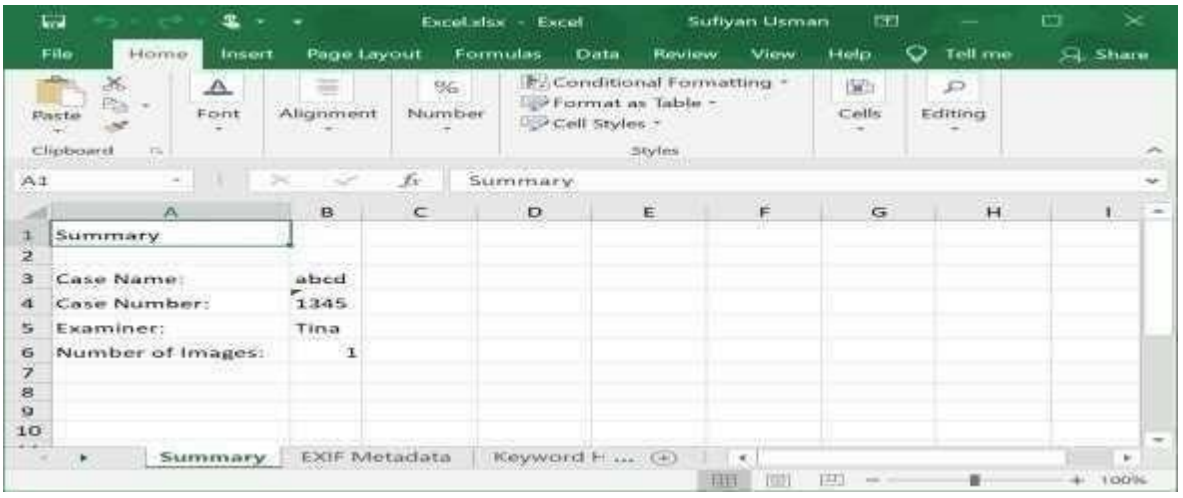


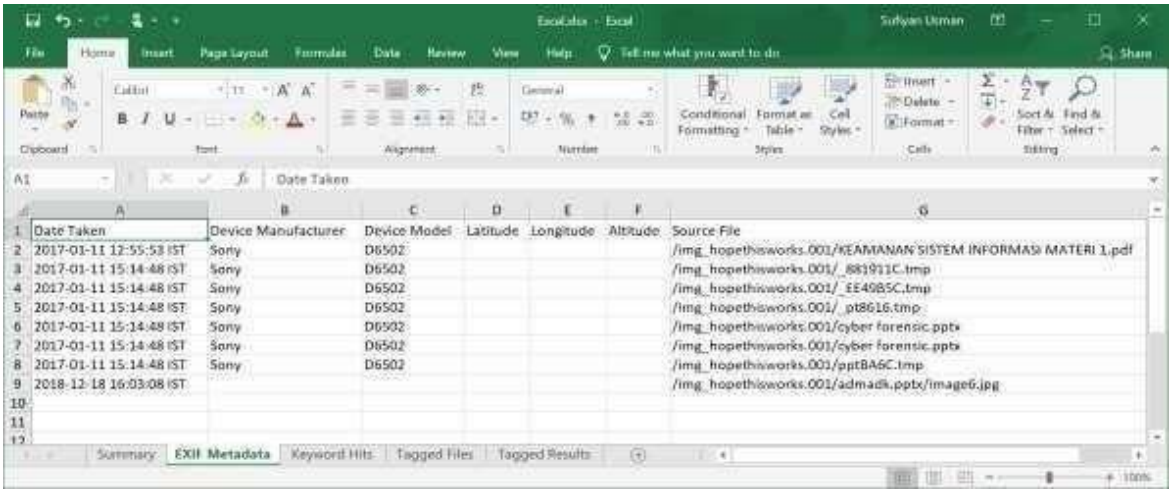


Now Report is Generated So click on close Button, We can see the Report on Report Node.

Double click on the excel file and open it to view the report







Practical No – 2

Aim: Explore Windows Forensic Tools (OS Forensics)

Windows forensic tools are essential for investigating, analyzing, and collecting digital evidence from Windows operating systems. These tools can be used by cybersecurity professionals, law enforcement, and digital forensic experts to examine and recover data, understand user activities, and trace potential security breaches. Below are some widely used Windows forensic tools, focusing on OS forensics:

1. Autopsy

Autopsy is an open-source digital forensics platform. It allows you to analyze hard drives and smartphones, recovering and examining artifacts like deleted files, browser history, and emails.

2. FTK Imager

Forensic Toolkit (FTK) Imager is a lightweight, free tool from AccessData used to capture and analyze forensic images of hard drives, CDs, DVDs, and flash drives

Key Features

- Creation of forensic images (bit-by-bit copies)

- Data integrity verification

- File and folder browsing within forensic images

- Recovery of deleted files

3. EnCase Forensic

EnCase is a comprehensive forensic tool used by law enforcement and enterprises to collect and analyze digital evidence from various sources.

Key Features

- Data acquisition from various sources (local disks, networked computers, mobile devices)

- Powerful search capabilities

- Integration with other forensic tools

- Extensive reporting feature

4. Wireshark

Wireshark is a network protocol analyzer. It captures and analyzes network traffic, helping investigators understand network activity, identify anomalies, and trace unauthorized access.

- Key Features

- Live network data capture

- Protocol analysis

- Detailed packet inspection

- Filtering and search capabilities

Applications and Use Cases:

- Digital Forensics: Collecting and analyzing digital evidence in criminal investigations.

- Incident Response: Identifying and mitigating security breaches and cyber attacks.

- Data Recovery: Recovering lost or deleted files and data from storage media.

- Malware Analysis: Investigating and understanding the behavior of malware and other malicious software.

These tools vary in complexity and focus, ranging from beginner-friendly options to more advanced tools suited for professional forensic investigators.

Practical No – 3

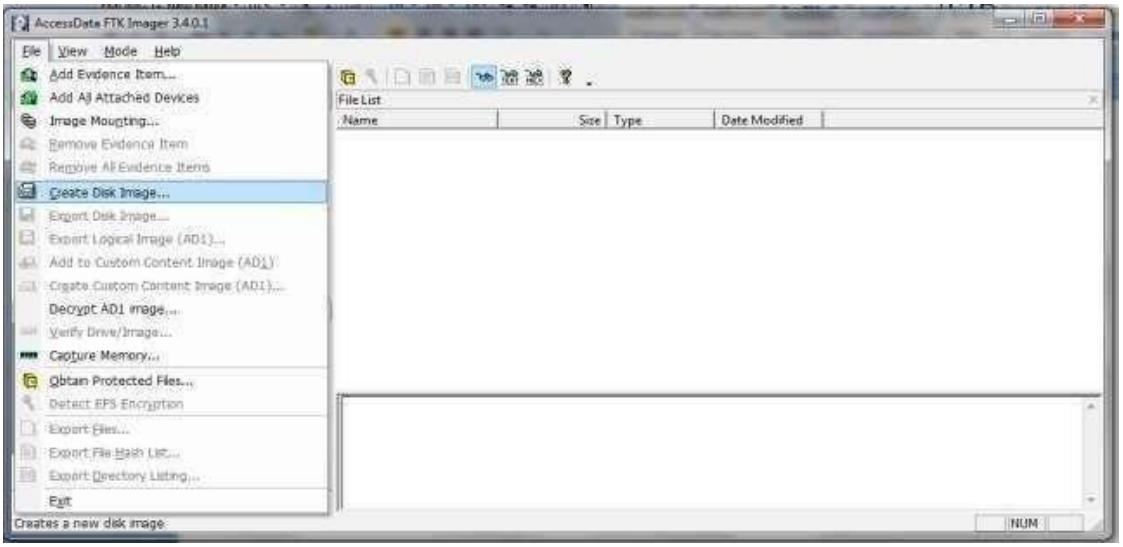
A. Creating a Forensic Image using FTK Imager/Encase Imager:

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

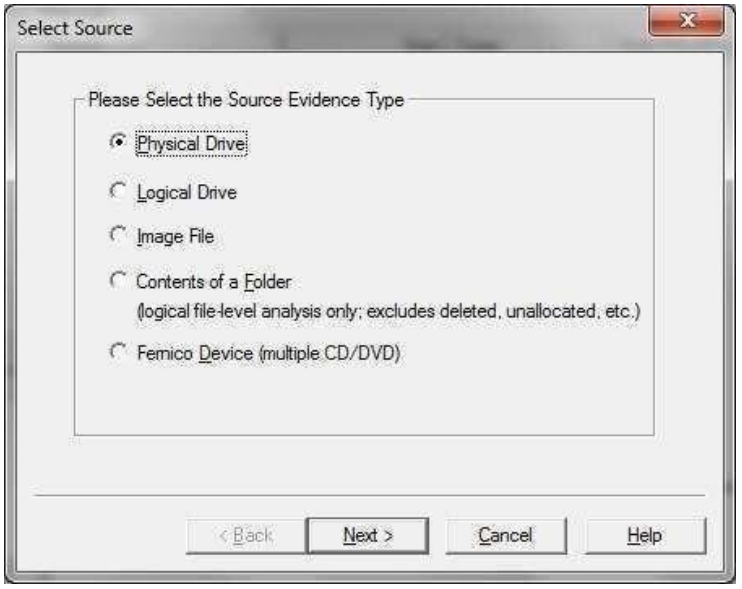
Steps:

Creating Forensic Image

1. Click File, and then Create Disk Image, or click the button on the tool bar.

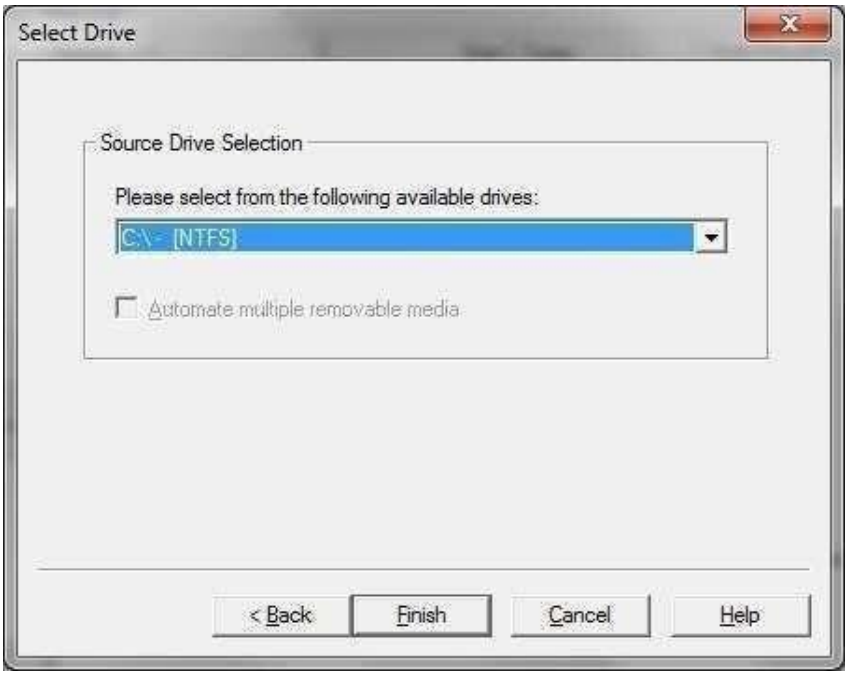


2. Select the source you want to make an image of and click Next.

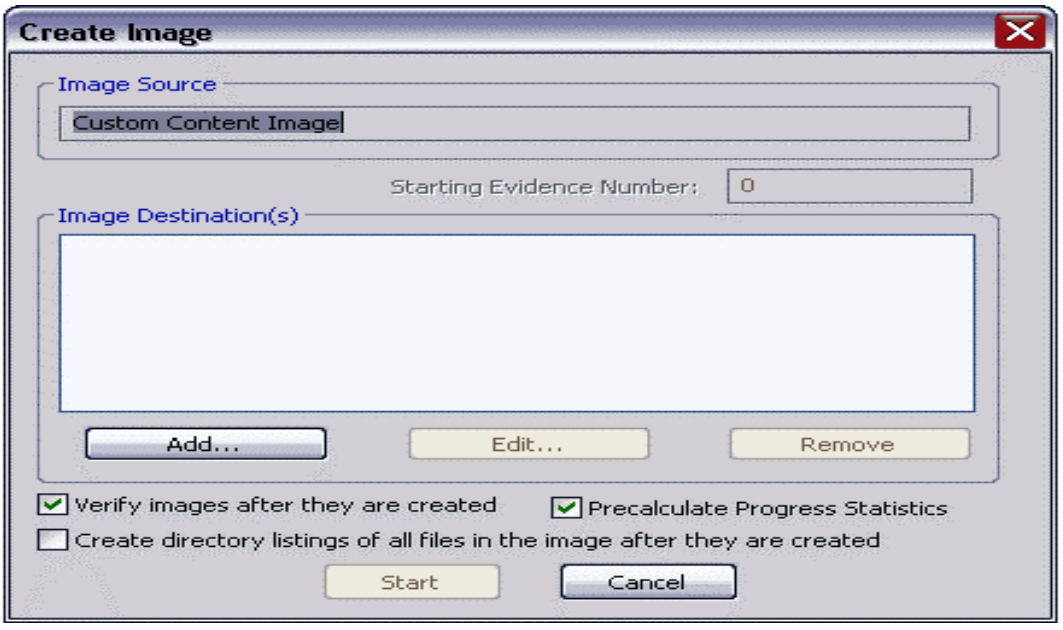


If you select Logical Drive to select a floppy or CD as a source, you can check the Automate multiple removable media box to create groups of images. Imager will automatically increment the case numbers with each image, and if something interrupts the process, you may assign case number manually.

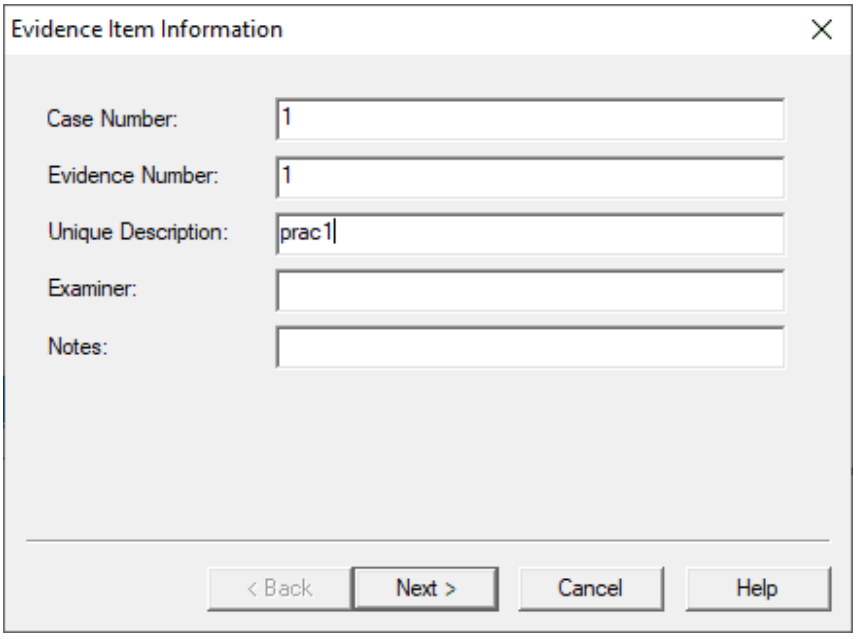
3. Select the drive or browse to the source of the image you want, and then click Finish.



4. In the Create Image dialog, click Add.

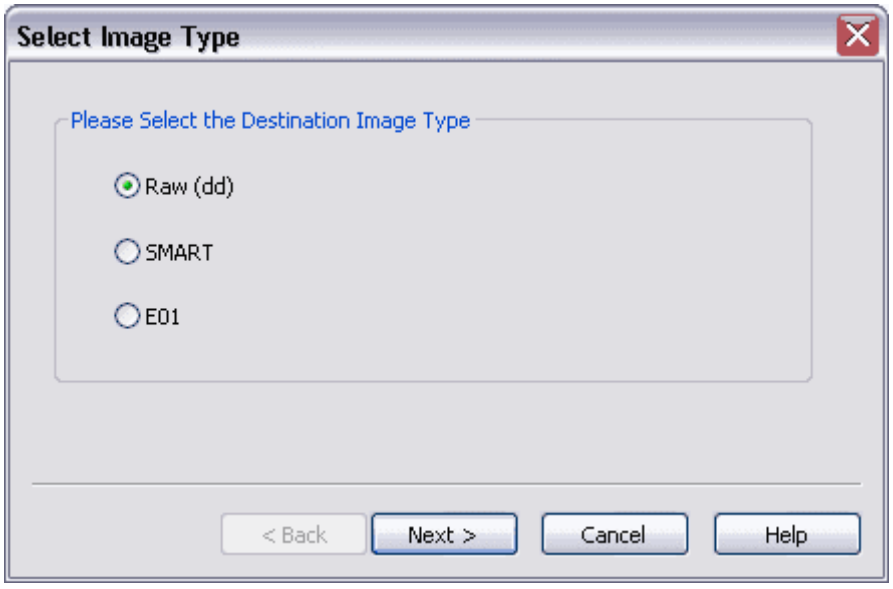


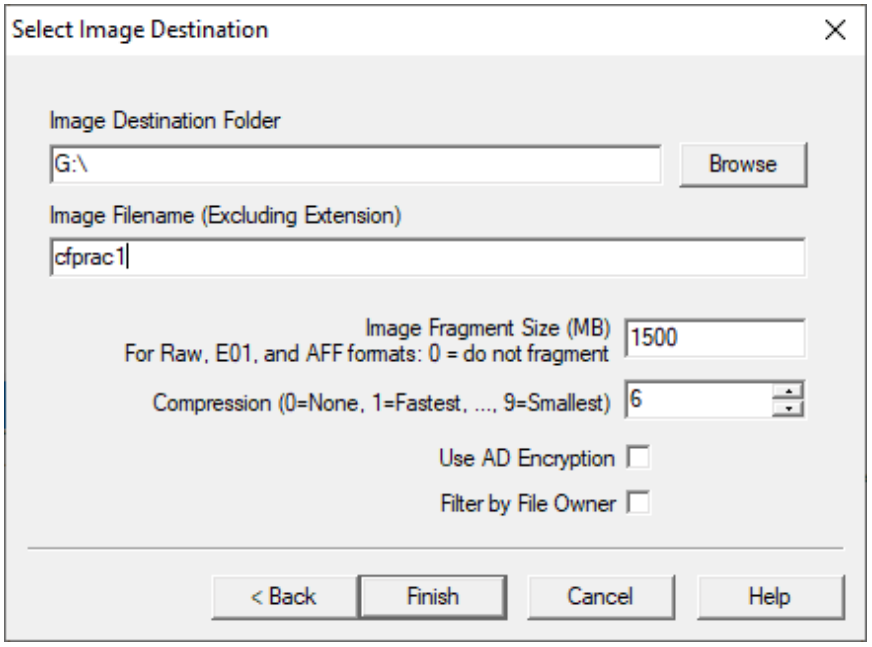
- You can compare the stored hashes of your image content by checking the Verify images after they are created box. If a file doesn't have a hash, this option will generate one.
- You can list the entire contents of your images with path, creation dates, whether files were deleted, and other metadata. The list is saved in a tab-separated value format



5. Select the type of image you want to create, and then click Next.

   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.





6. In the Image Destination Folder field, type the location path where you want to save the image file, or click **Browse** to find to the desired location.

> **Note:** If the destination folder you select is on a drive that does not have sufficient free space to store the entire image file, FTK Imager prompts for a new destination folder when all available space has been used in the first location.

7. In the Image Filename field, specify a name for the image file but do not specify a file extension.
8. In the Image Fragment Size field, specify the maximum size in MB for each fragment of the image file. 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.

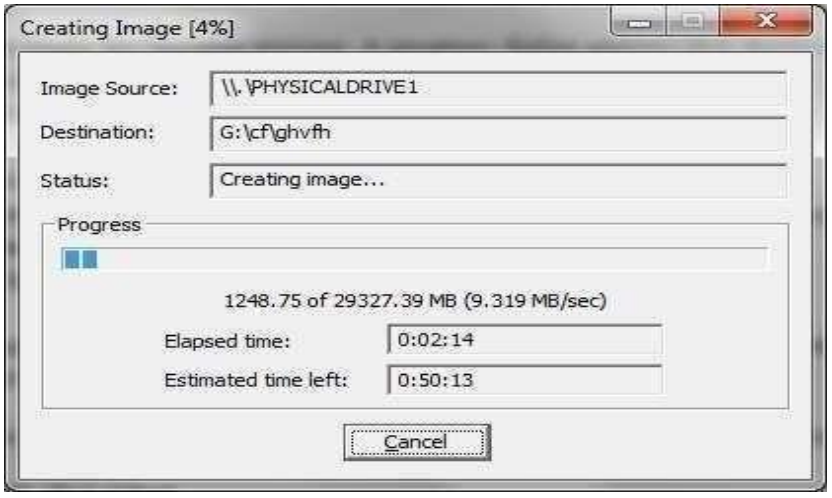
> **Tip:** If you want to transfer the image file to CD, accept the default fragment size of 650 MB.

9. Click **Finish**. You return to the Create Image dialog.
10. To add another image destination (i.e., a different saved location or image file type), click **Add**, and repeat steps 5– 10. To make changes to an image destination, select the destination you want to change and click **Edit.**

To delete an image destination, select the destination and click **Remove**.

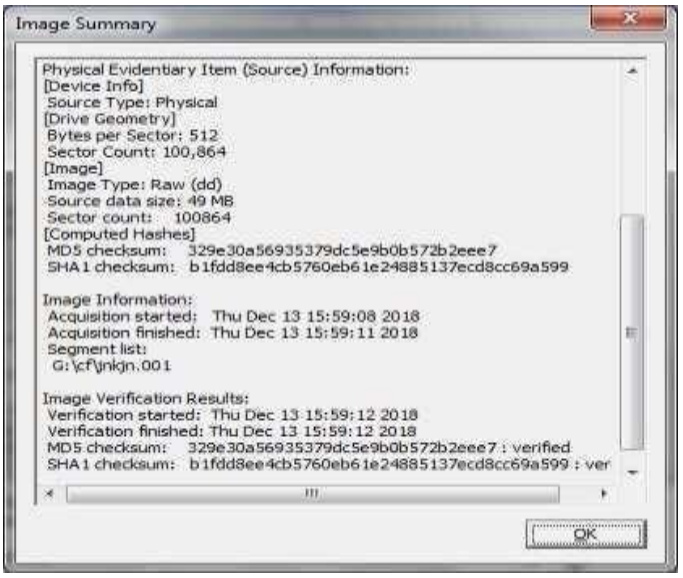
11. Click **Start** to begin the imaging process. A progress dialog appears that shows the following:

- 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 after the imaging process began
- Estimated time left until the process is complete



After the images are successfully created, click Image Summary to view detailed file information, including MD5 and SHA1 checksums.

Note: This option is available only if you created an image file of a physical or logical drive.

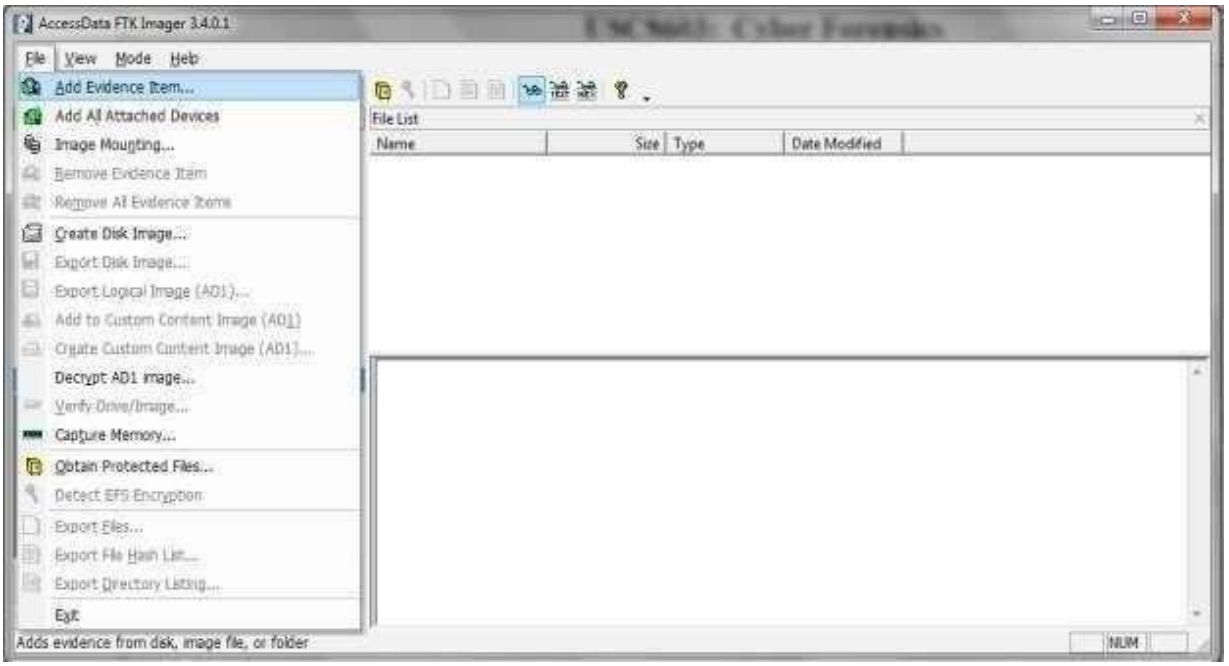


12. When finished, click **Close**

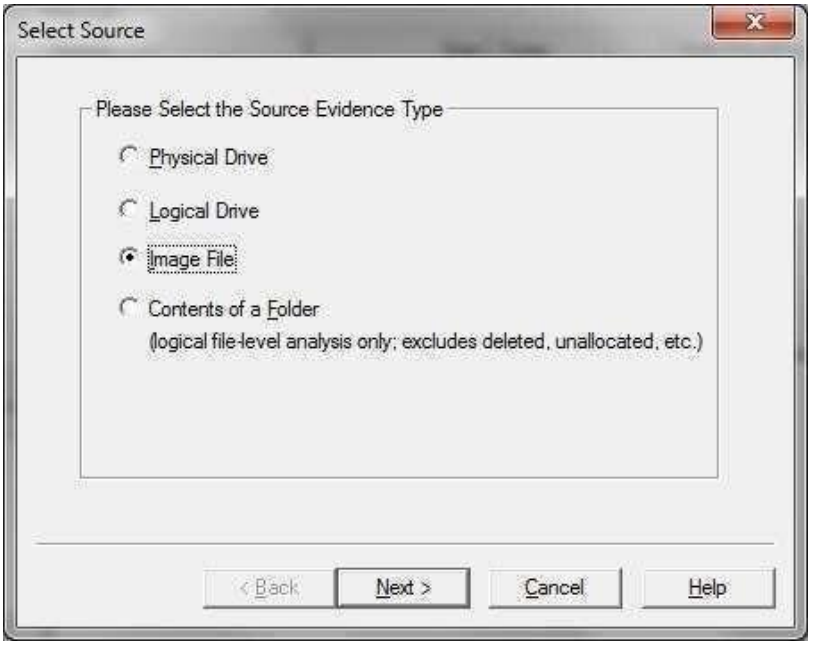
Note that the image file (*.001) as well as the image summary file from above (*.txt) have been saved onto the 'Drive'. The .001 extension may be left as is, or can be changed to .dd. The .001 extension is used due to the fact that many times the file to be imaged is very large and must be split into multiple chunks. In that case, you would have *.001, *.002, etc

Analyze Forensic Image:

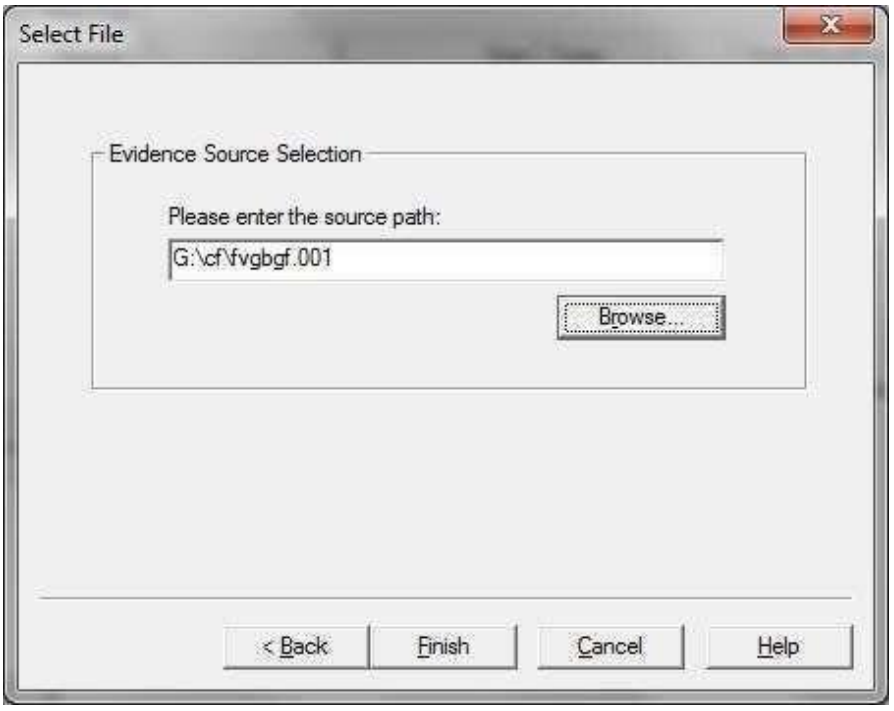
Click on Add Evidence Item to add evidence from disk, image file or folder.



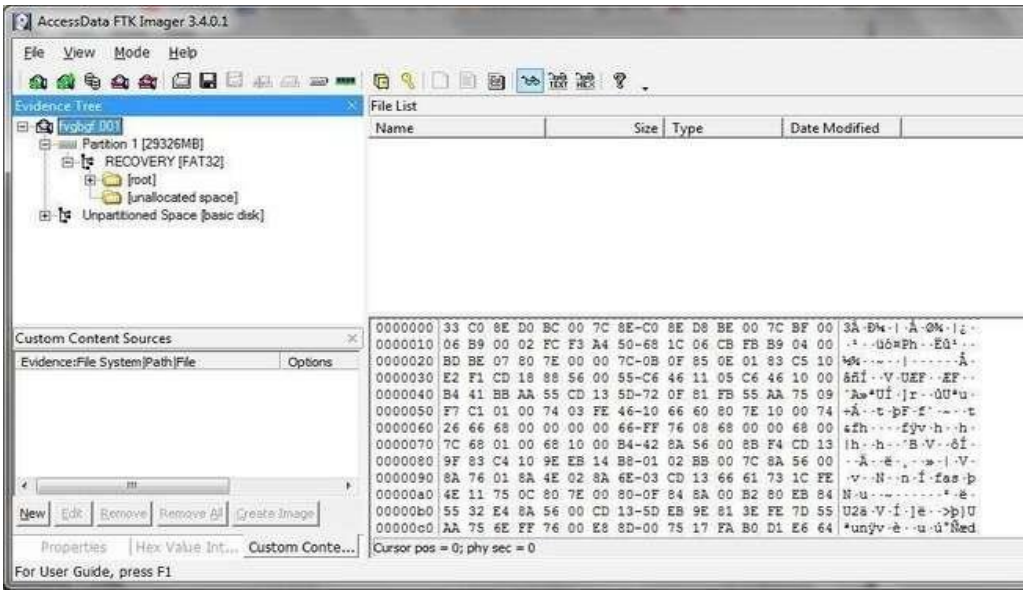
Now select the source evidence type as physical drive, logical drive or image file. We have selected image file and click on next.



Select virtual drive image & click on open option. Select the source path and click on finish.



Now select Evidence Tree and analyze the virtual disk as physical disk.



Similarly to add raw image select again add evidence item and click on image file and click on open option.

Click on finish.

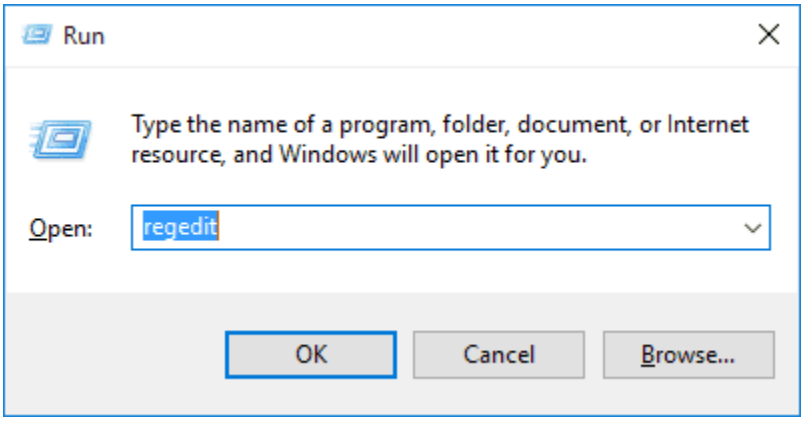
Now raw image will be added as physical drive to analyze.

B. Perform data acquisition using USB Write Blocker

Steps:

Enable USB Write Block in Windows 10, 8 and 7 using registry

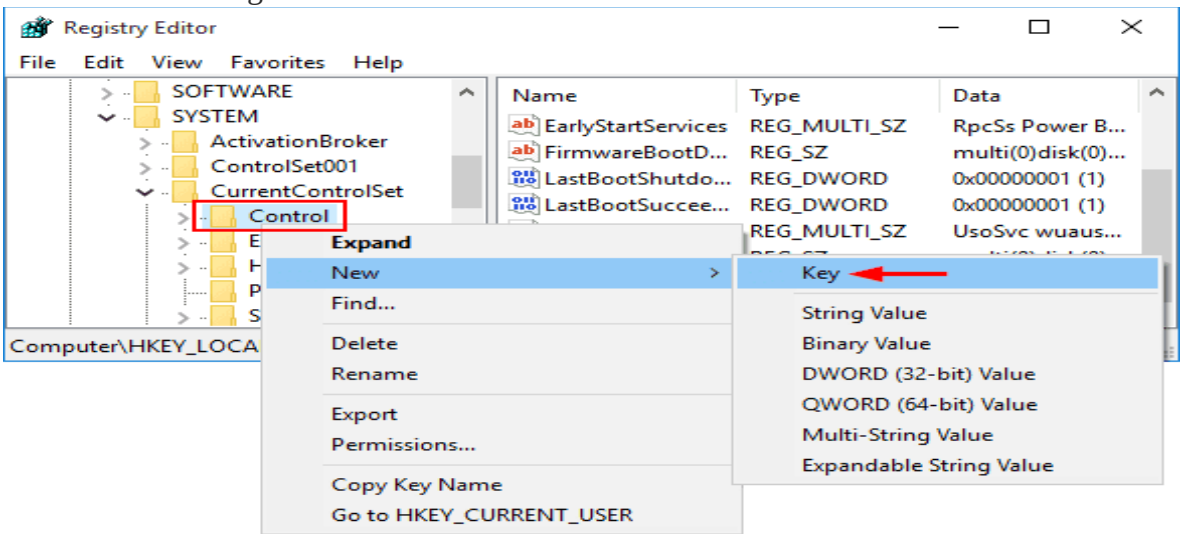
1. Press the Windows key + R to open the Run box. Type regedit and press Enter.



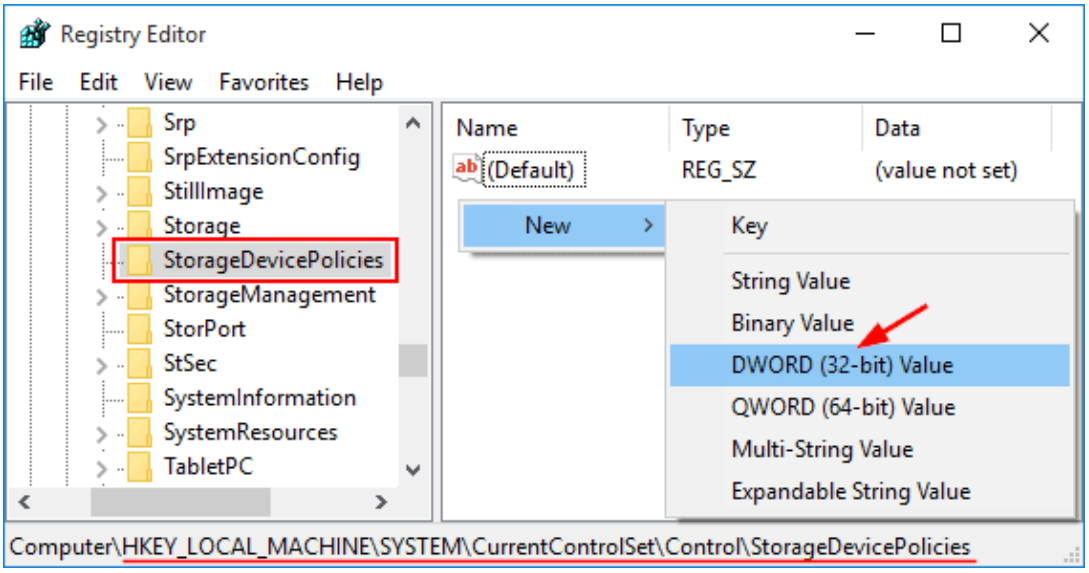
2. This will open the Registry Editor. Navigate to the following key:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control

3. Right-click on the Control key in the left pane, select New -> Key.

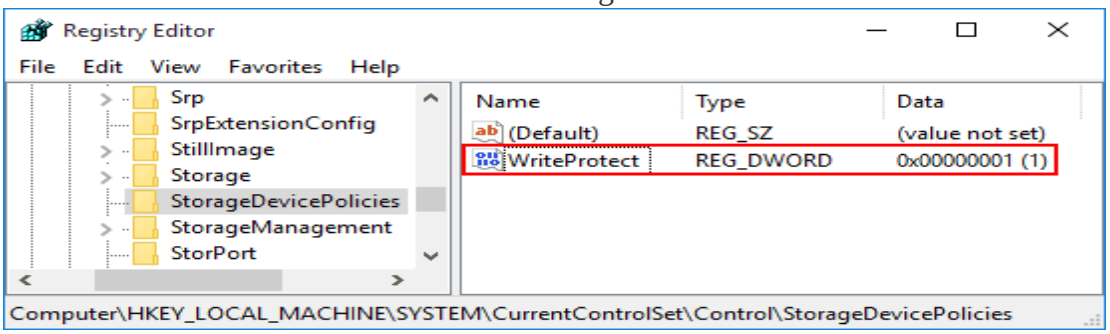
4. Name it as StorageDevicePolicies.



5. Select the StorageDevicePolicies key in the left pane, then right-click on any empty space in the right pane and select New -> DWORD (32-bit) Value. Name it WriteProtect.

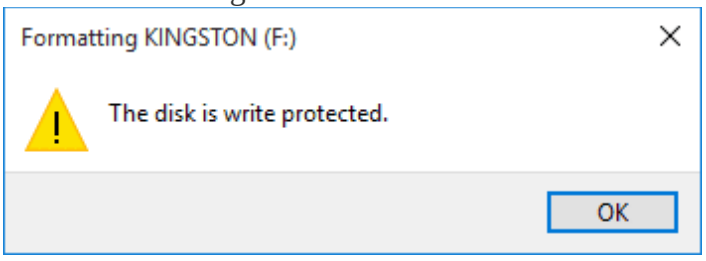


6. Double-click on WriteProtect and then change the value data from 0 to 1.



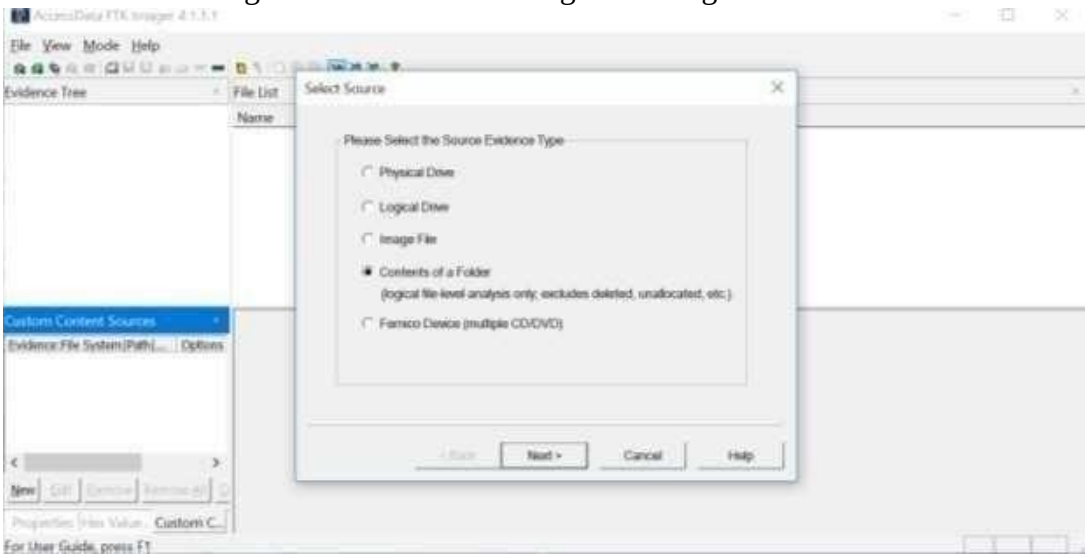
7. The new setting takes effect immediately. Every user who tries to copy / move data to USB devices or format USB drive will get the error message
"*The disk is write-protected*".

8. We can only open the file in the USB drive for reading, but it's not allowed to modify and save the changes back to USB drive.



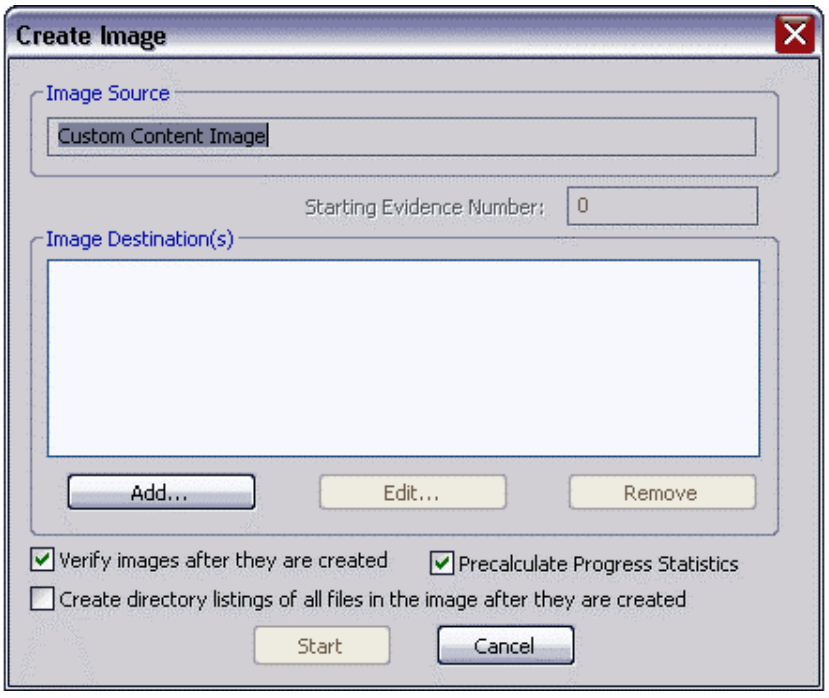
So this is how you can enable write protection to all connected USB drives. If you want to disable write protection at a later time, just open Registry Editor and set the WriteProtect value to 0.

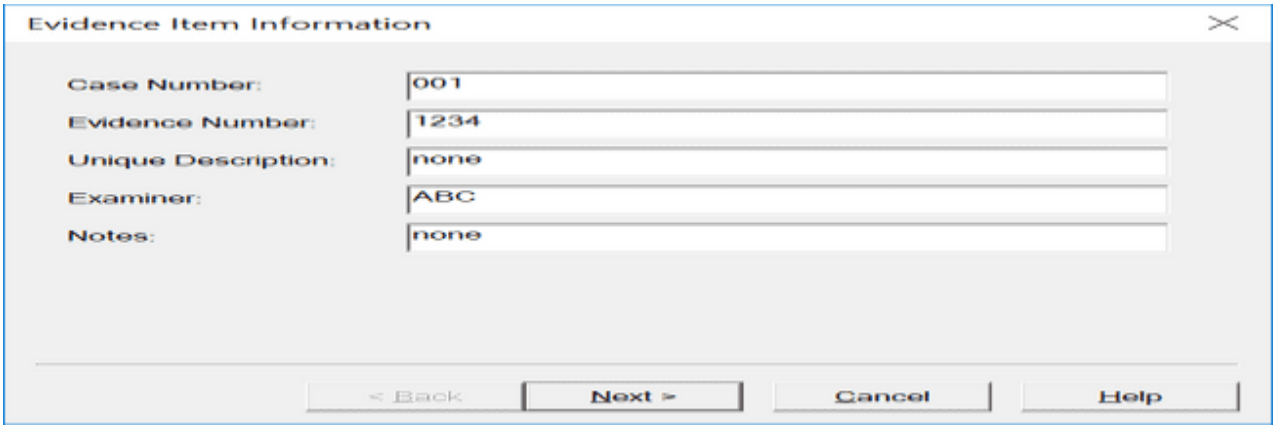
9. Now Create image of the USB drive using FTK imager



10. Select the USB drive folder by browsing and click next &

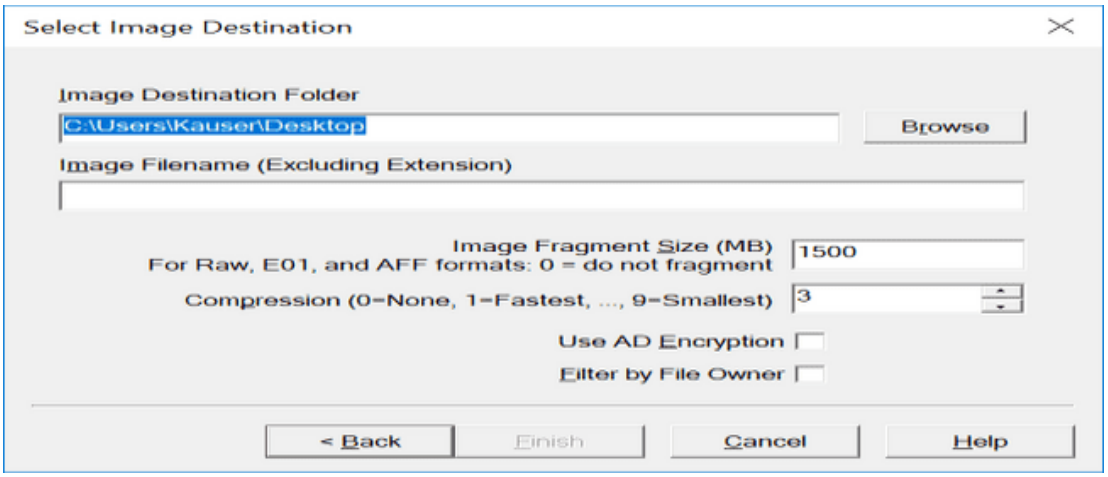
Finish 11.In the Create Image dialog, click Add.

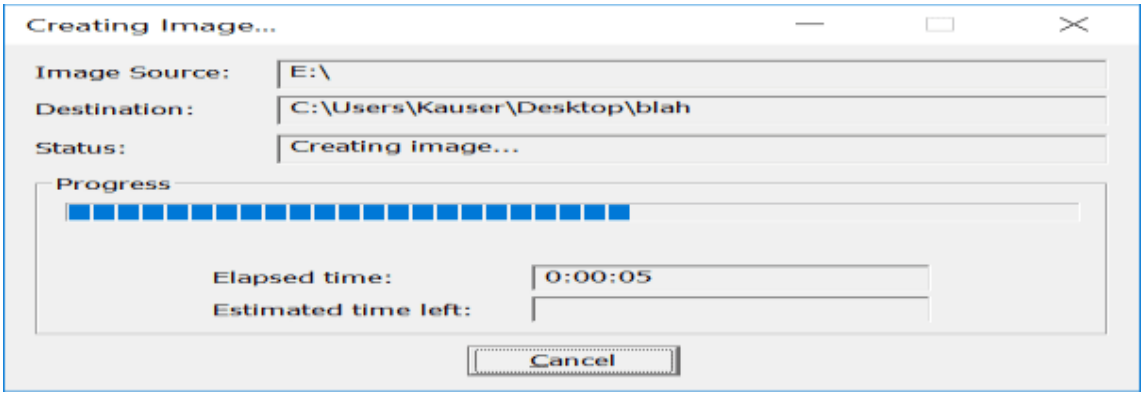




- You can compare the stored hashes of your image content by checking the Verify images after they are created box. If a file doesn't have a hash, this option will generate one.
- You can list the entire contents of your images with path, creation dates, whether files were deleted, and other metadata. The list is saved in a tab-separated value format

Select the type of image you want to create, and then click Next





Practical No: 4

a.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.**

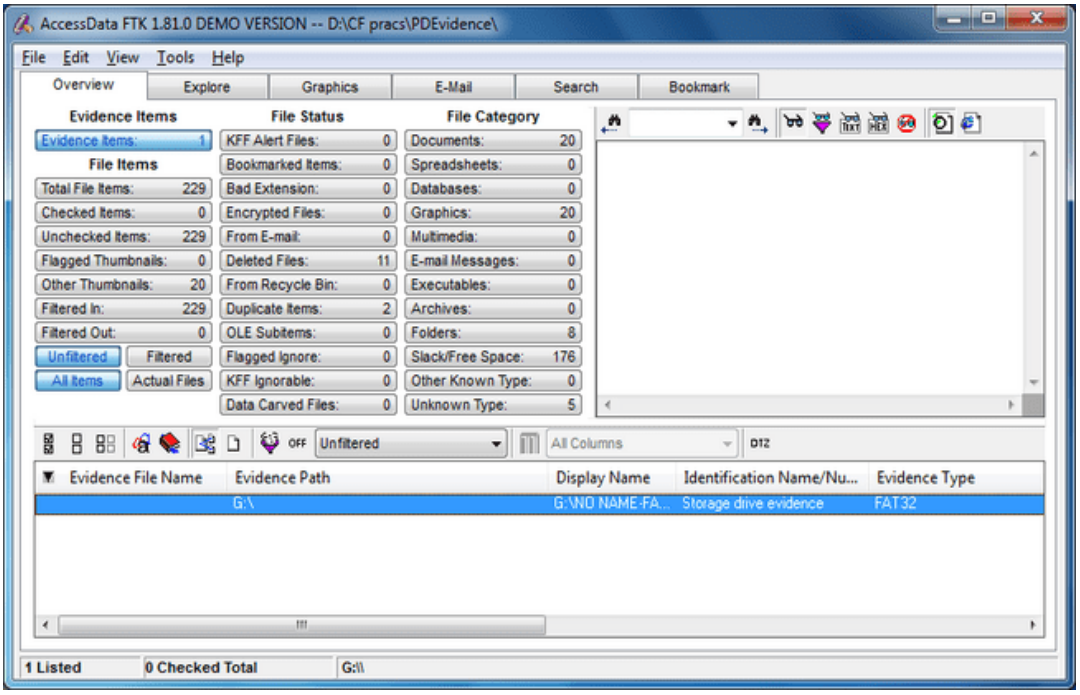
Data Carving Files During Evidence Processing in a New Case:

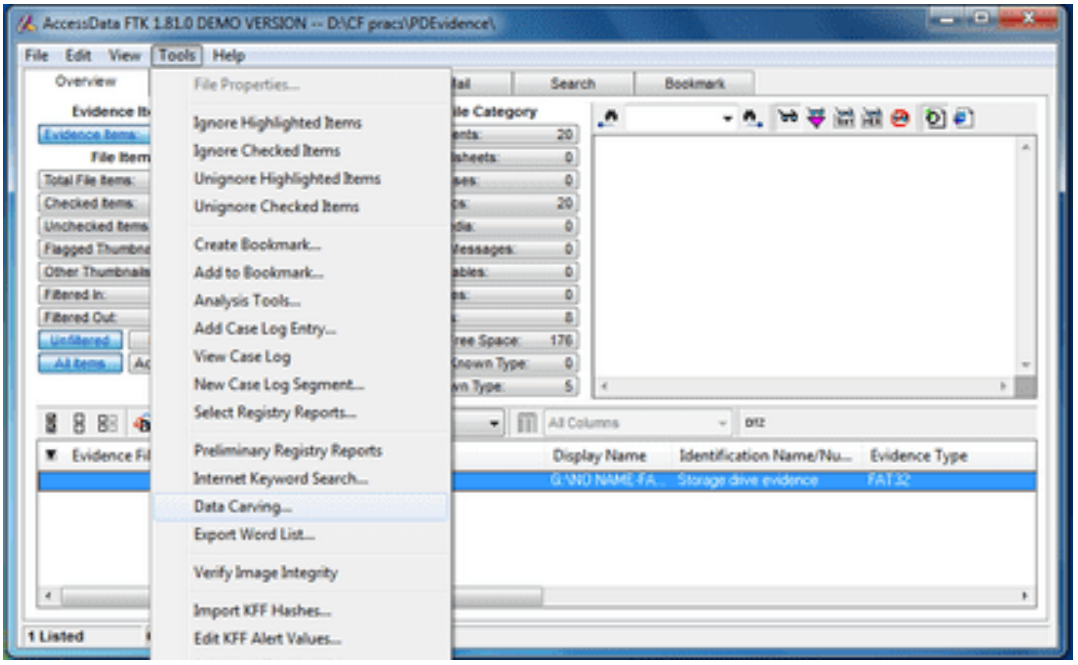
You can select to data carve when a case is added by selecting Data Carve in the Process to Perform Screen during the New Case Wizard. FTK carves data immediately after pre-processing.

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.

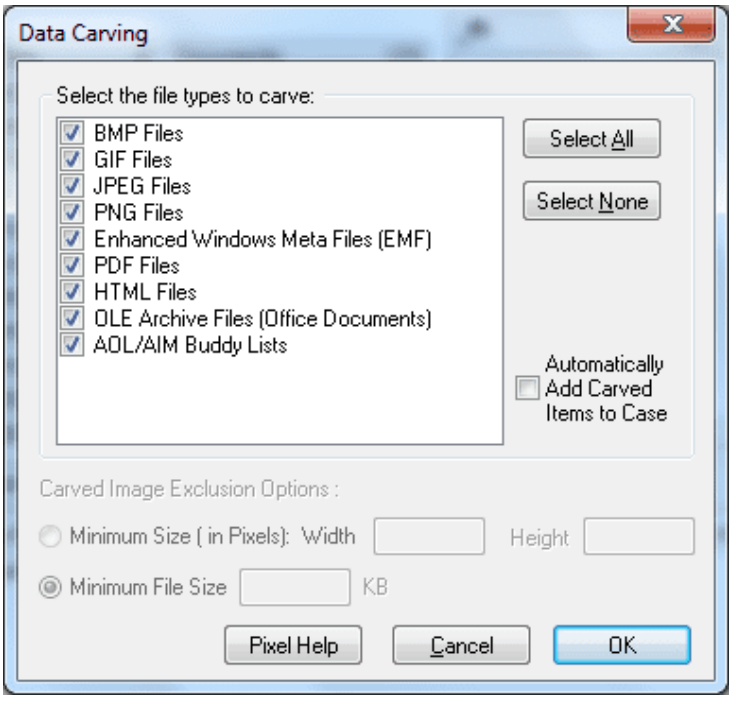
To access the cache:

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

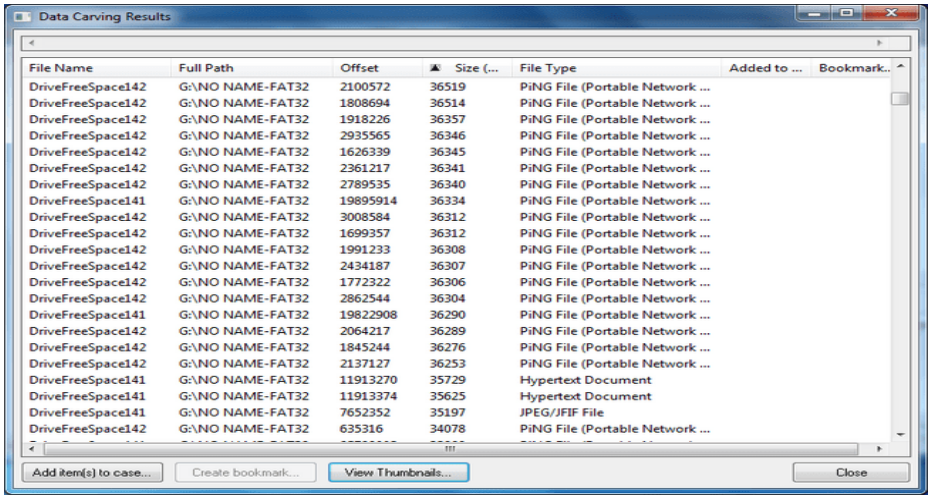


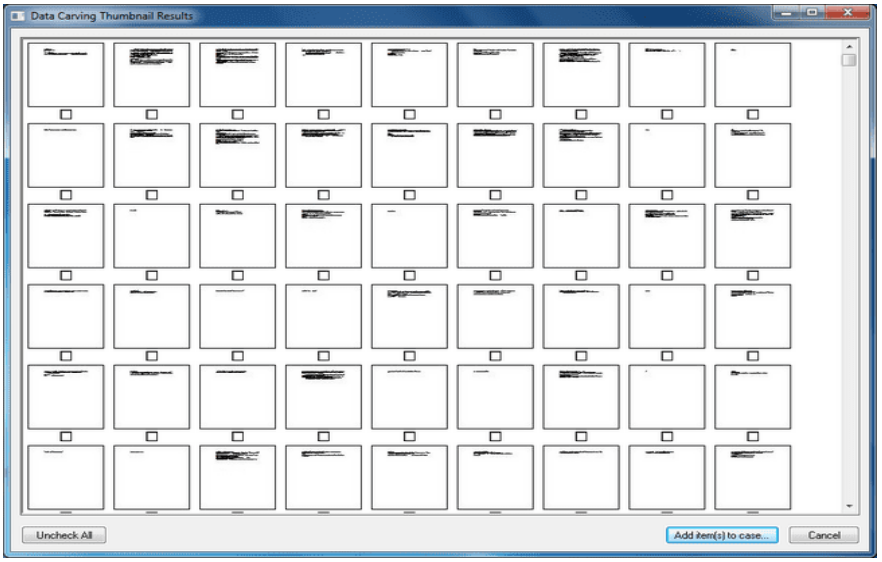


Step 2) Check the file types to carve. You can click **Select All** or **Select None** to speed up the selection process. Click **OK**.

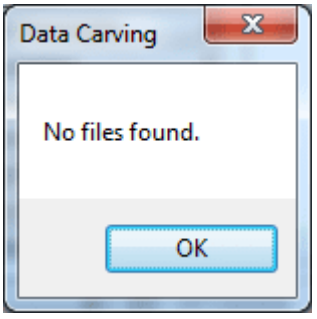


When the process is complete, the detached viewer appears with the data carving results. A message appears if no data was located.





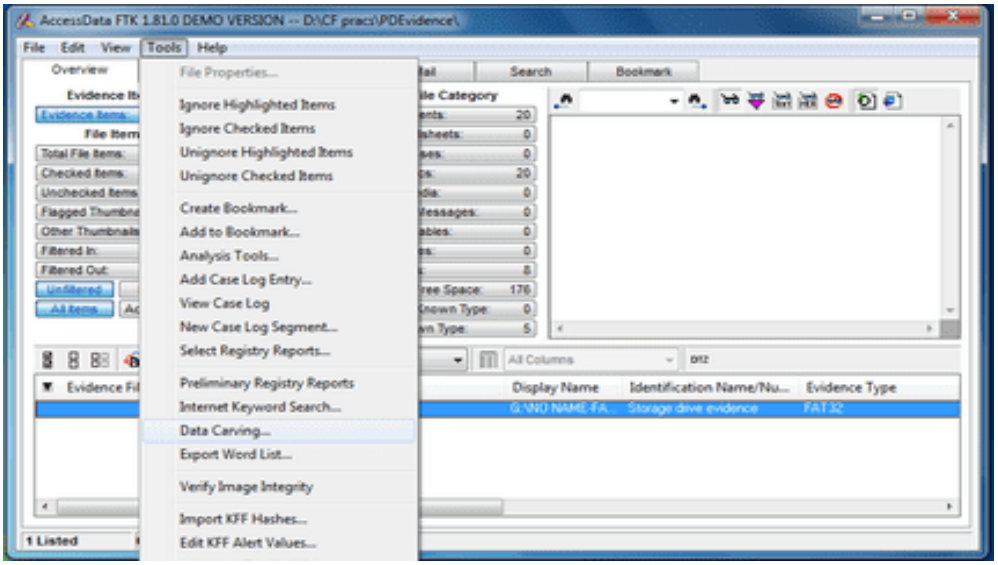
Or



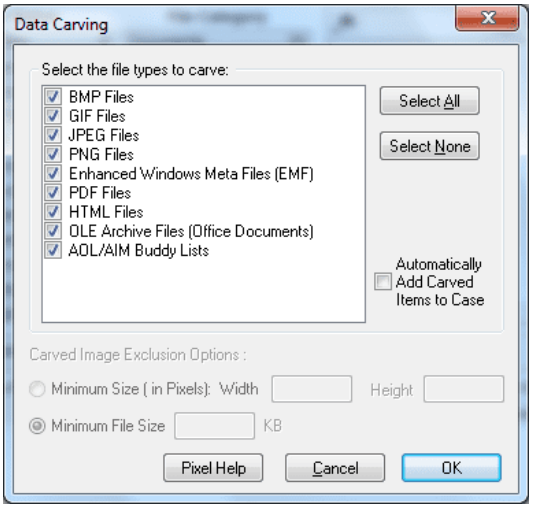
Data Carving Files in an Existing Case:

To search for embedded and deleted files:

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

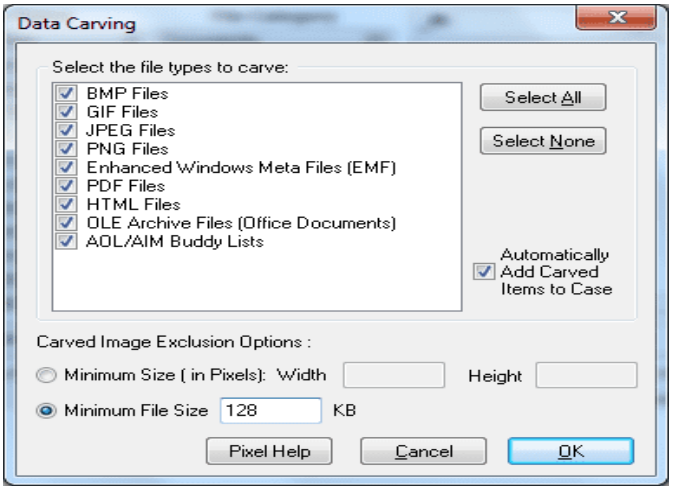


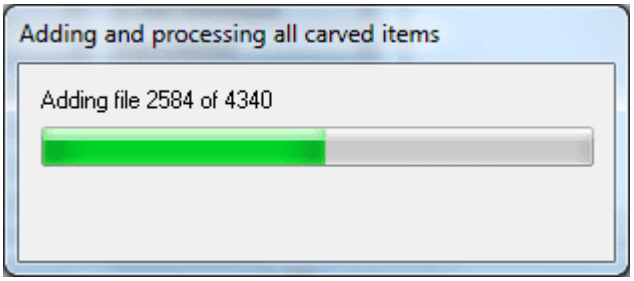
[2] Check the file types to carve. You can click **Select All** or **Select None** to speed up the selection process.



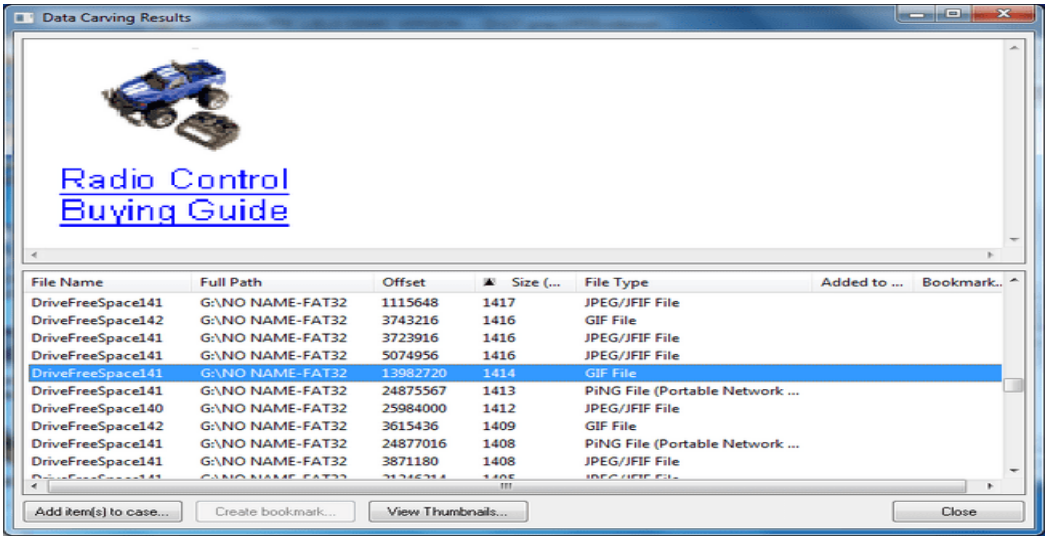
[3] (Optional) Check the **Automatically Add Carved Items to Case** option. The the Minimum Image Size fields activate. 3a Specify a minimum size in pixels in which to disply images. The program will question you about minimum sizes over 480 pixels.

[4] Click **OK**.





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

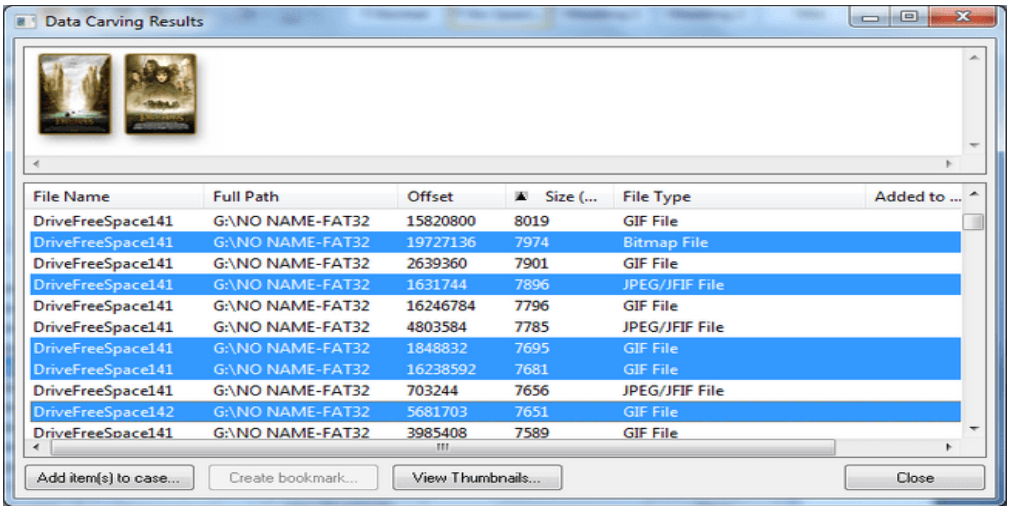


Adding Carved Files to the Case:

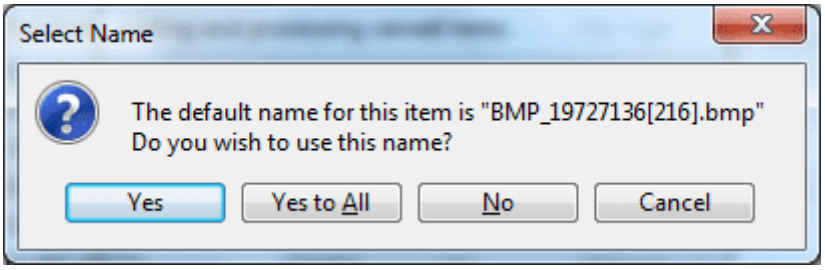
To add a carved file to the case:

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.

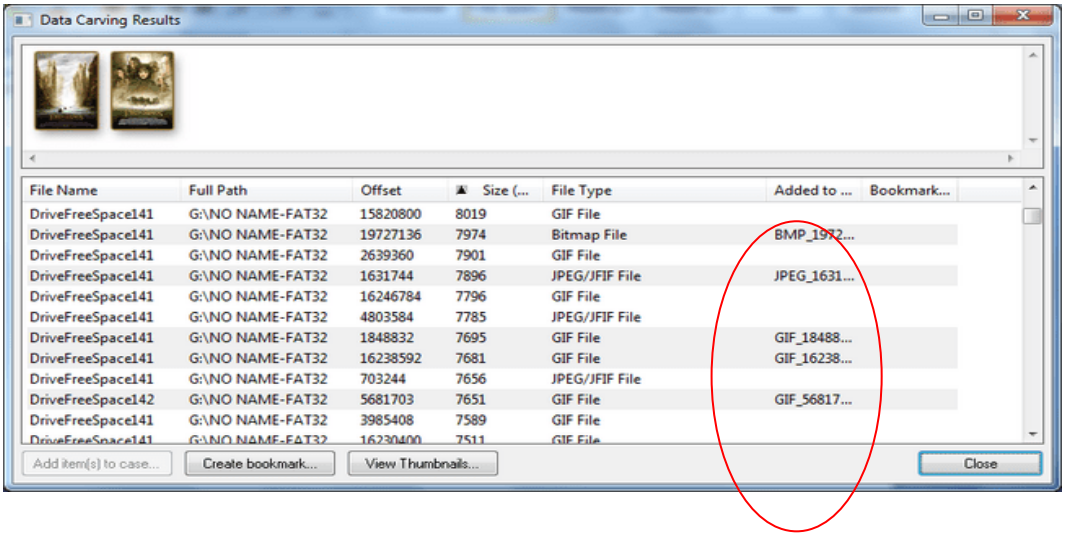
2) Click **Add Items to Case**.



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



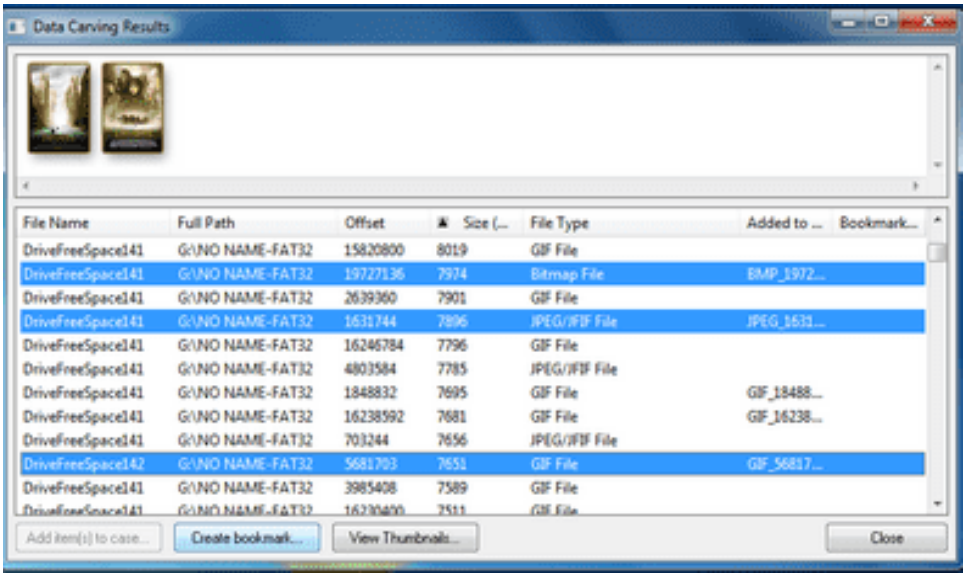
After a file is added to a case, FTK will not find it in subsequent data carving procedures. In other words, there is no redundancy. If a file is identified as case evidence, the data carving feature ignores it. The data carving feature only looks for files that are not individually identified in the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



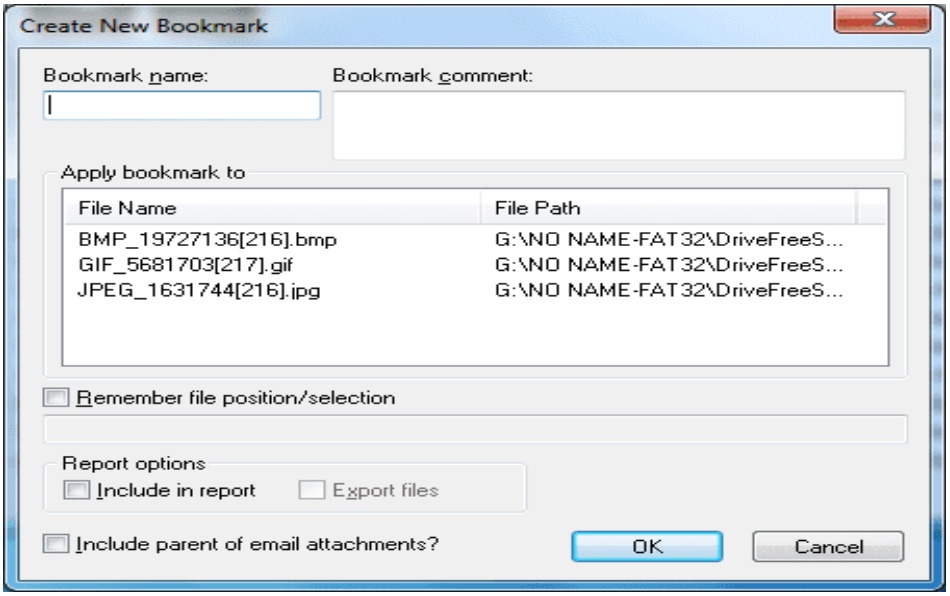
Bookmarking Carved Files:

To bookmark a carved file:

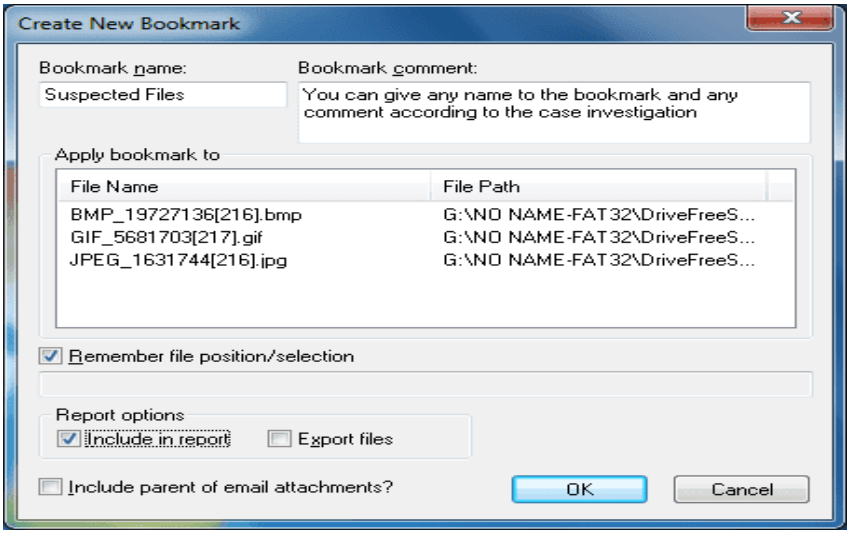
Step 1.Select the files you want to include in the bookmark and click **Create Bookmark**.



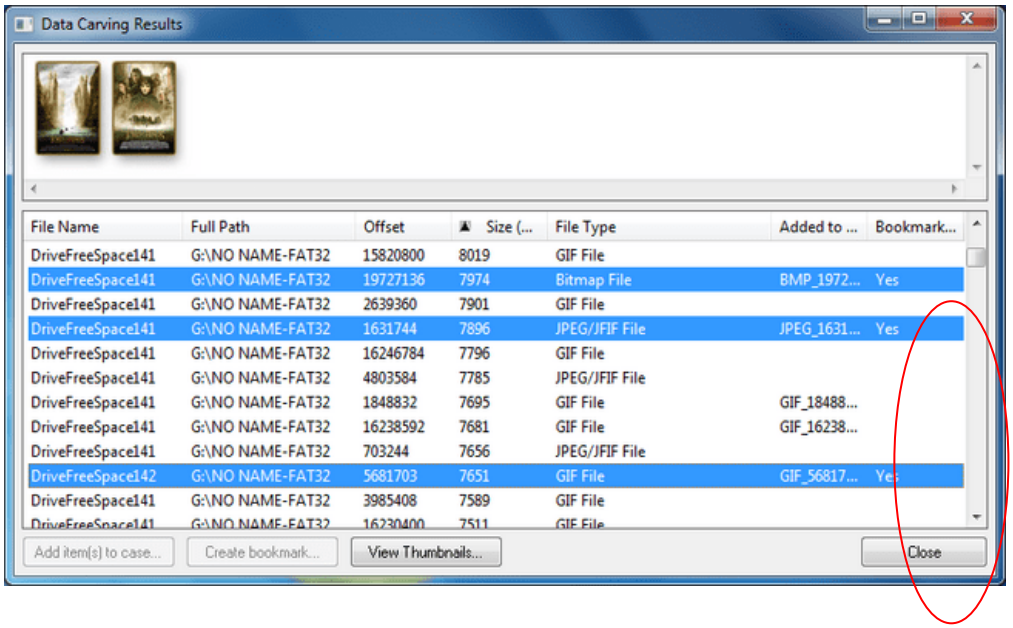
Step 2.In the Create New Bookmark form



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



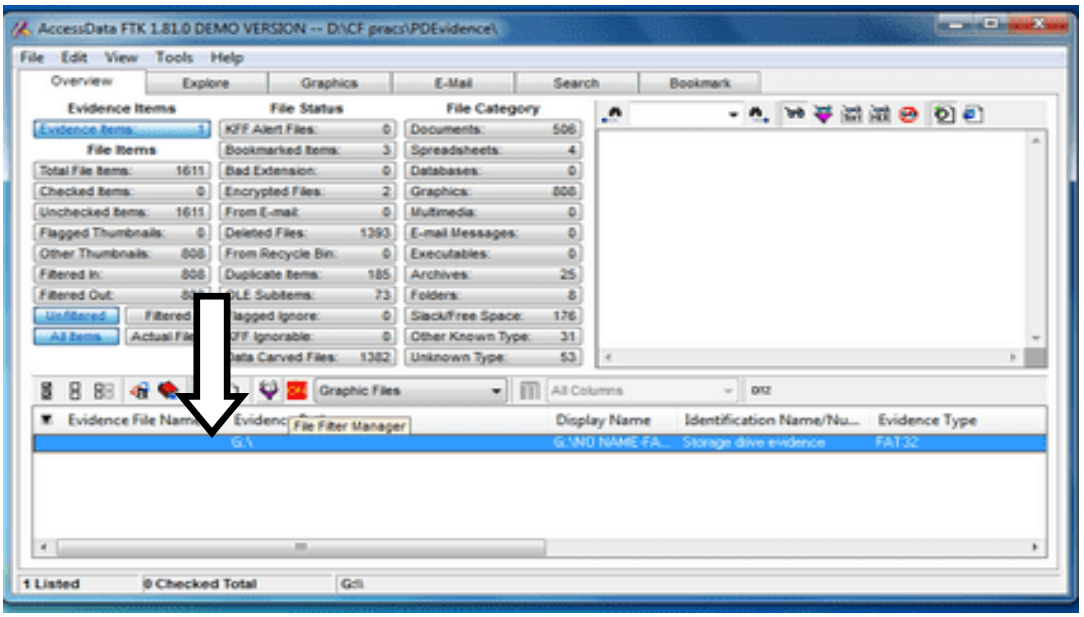
When the process is complete, the detached viewer appears with the bookmarked data carving results

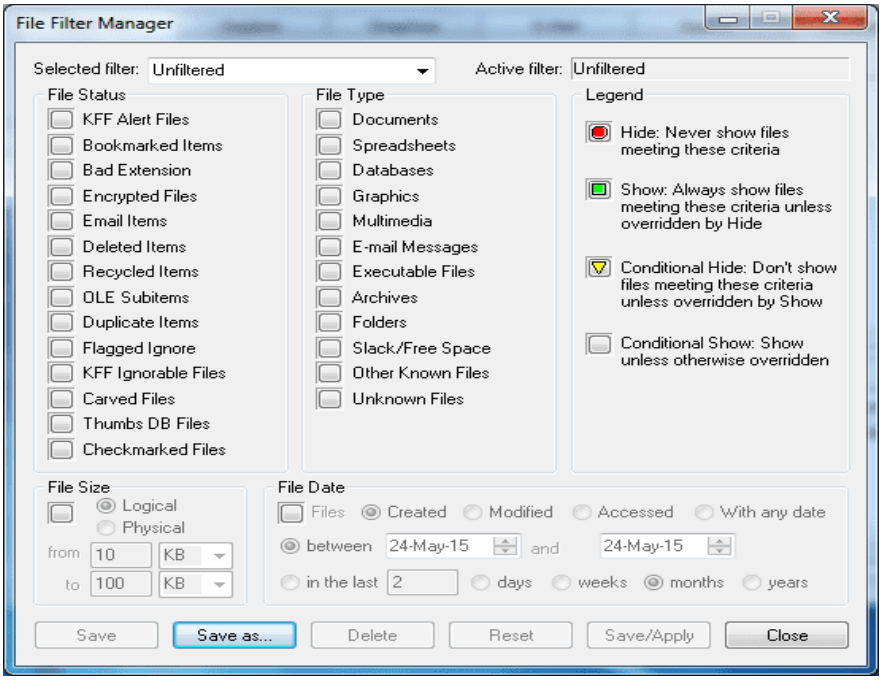


Using Filters

Applying an Existing Filter

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

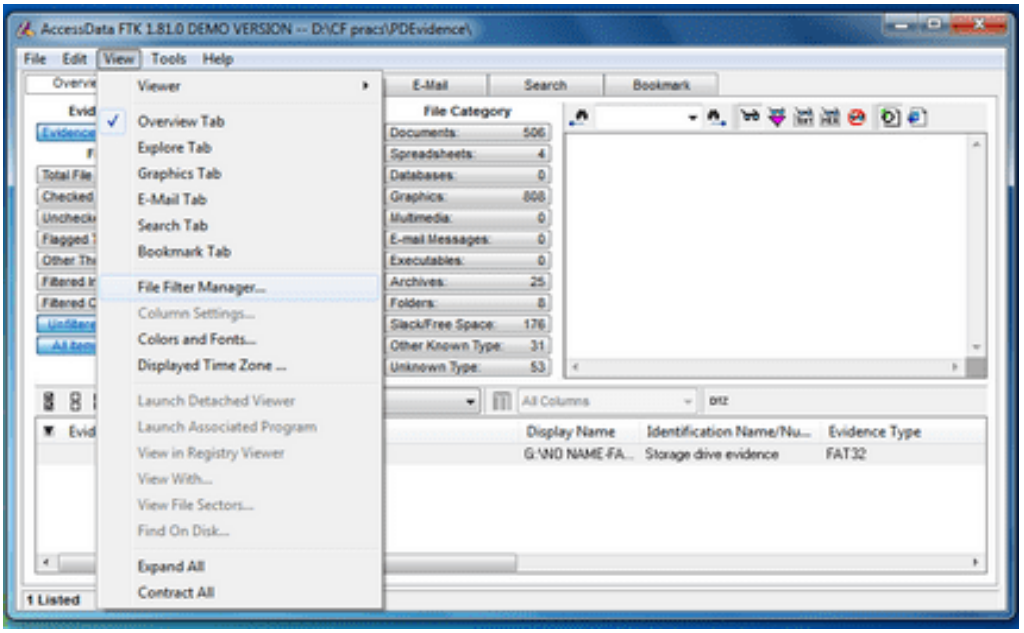


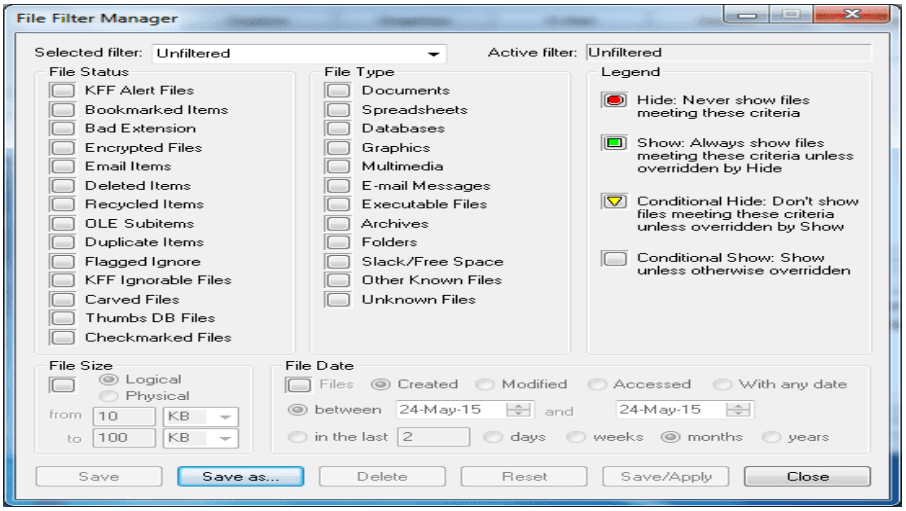


Using the File Filter Manager:

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:

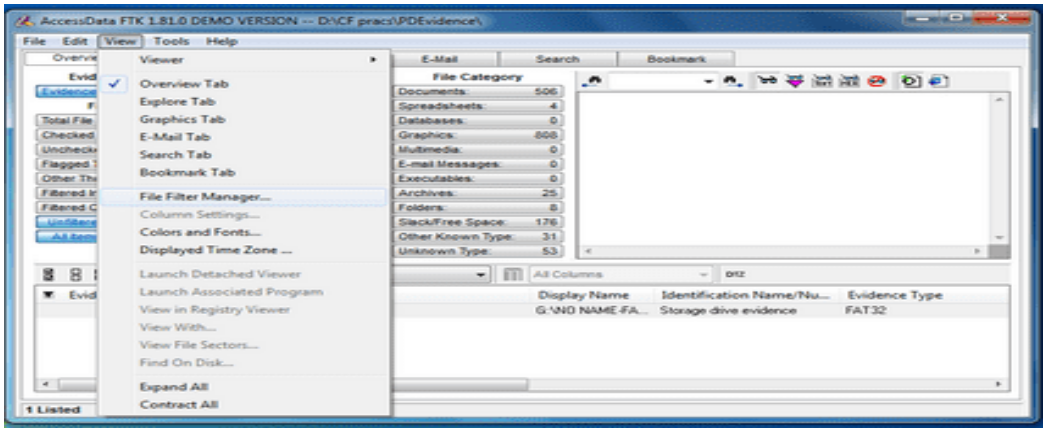
Icon	Description
	Hide: Never shows files meeting selected criteria. If you click this icon in the Legend column, all file statuses and types are marked Hide.
	Show: Always shows files meeting selected criteria unless overridden by Hide. If you click this icon in the Legend column, all file statuses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

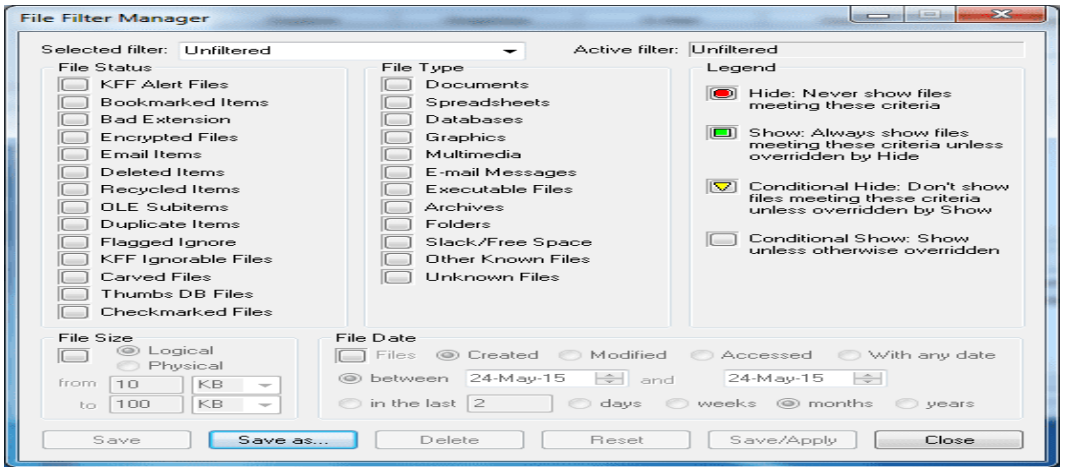
Category	Description
Bookmarked Items	Files that you bookmarked in PTK.
Deleted Files	Complete files or folders recovered from slack or free space.
Duplicate Items	Any items that have an identical hash. Because the filename is not part of the hash, identical files may actually have different filenames. The primary item is the first one found by PTK. 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 Email	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

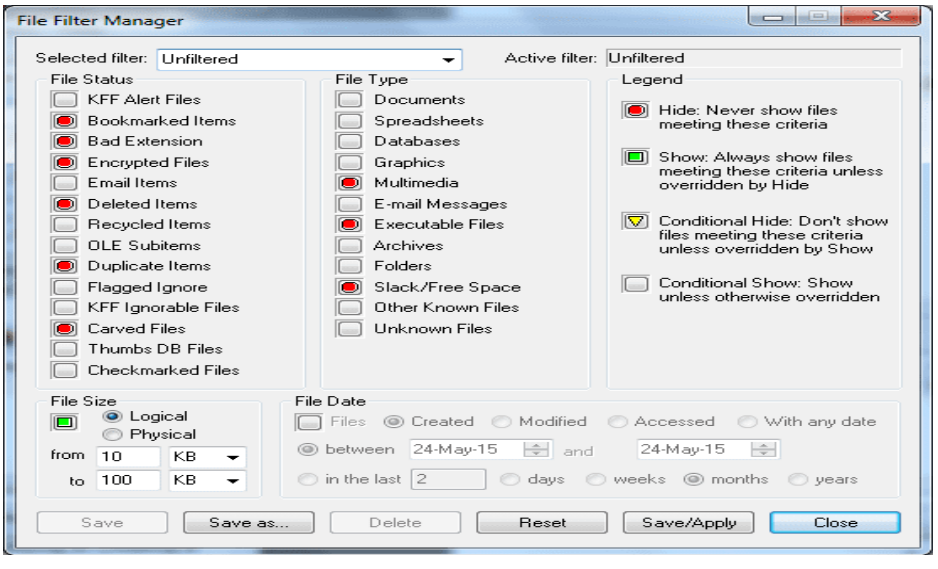
To modify or create a filter:

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



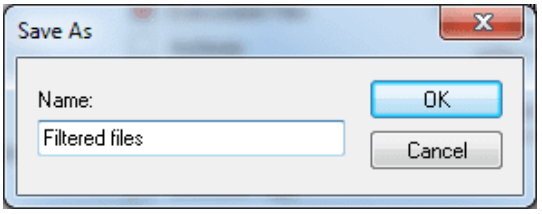


Step 2.Select the filter that you want to modify.



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**.

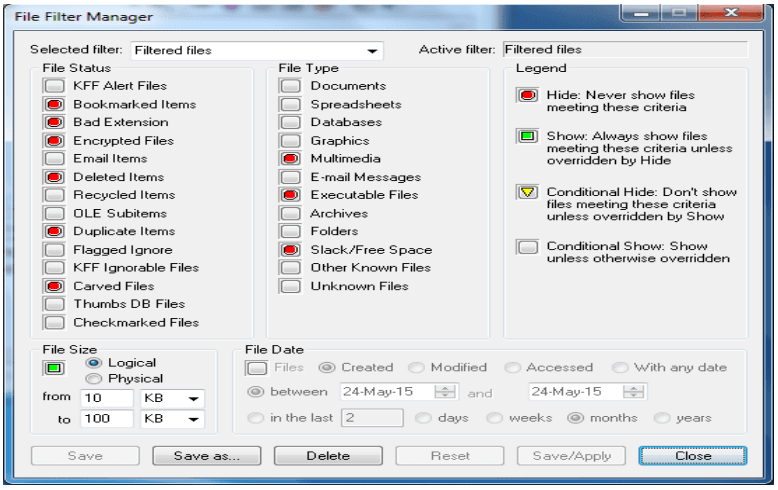


Deleting a Filter

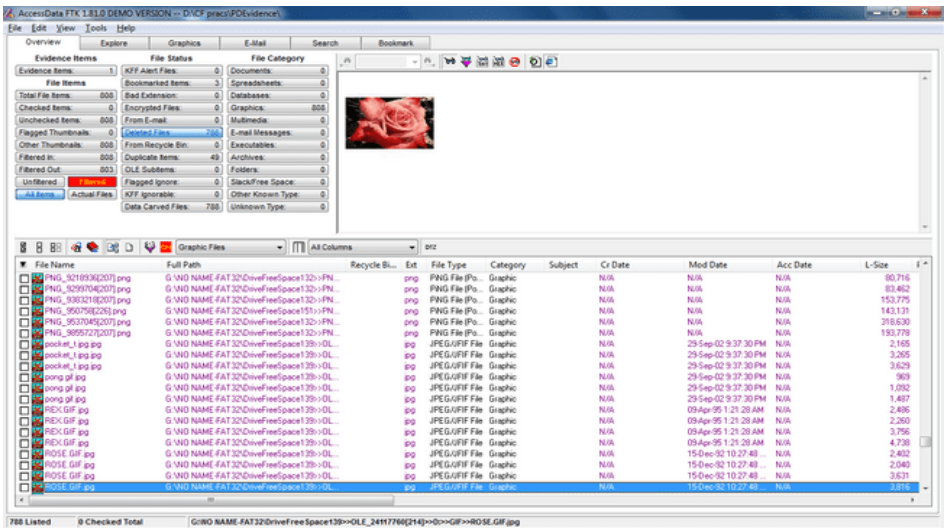
You can delete a filter if you no longer need it. To delete a filter:

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

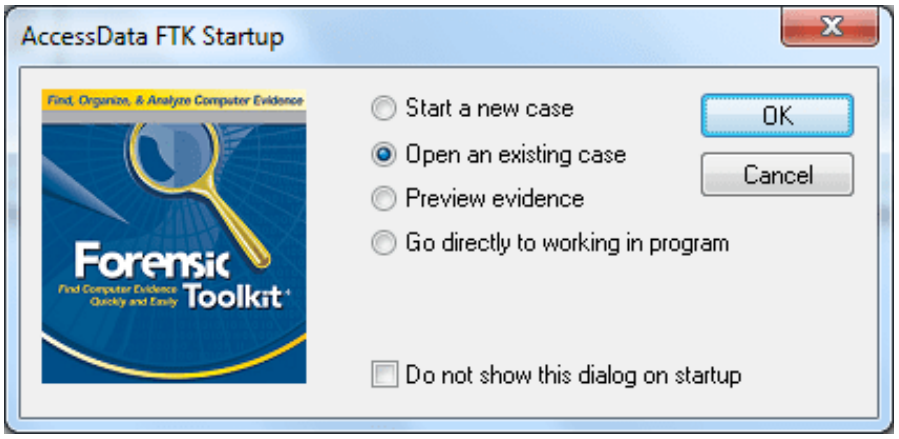
Registry Viewer, and then **Registry Viewer**.

Launching Registry Viewer from FTK:

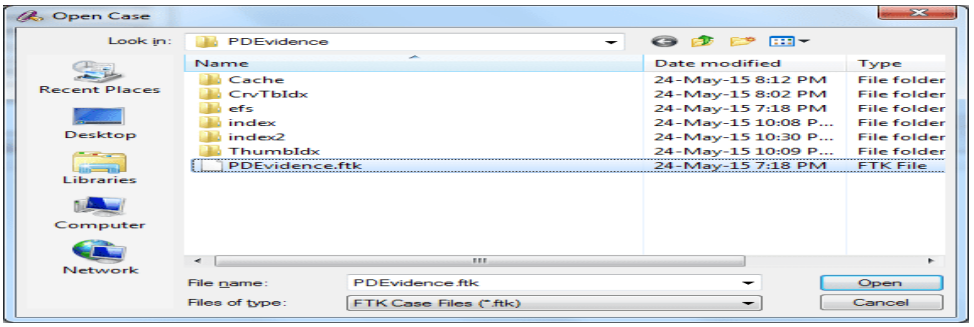
To run Registry Viewer from FTK:

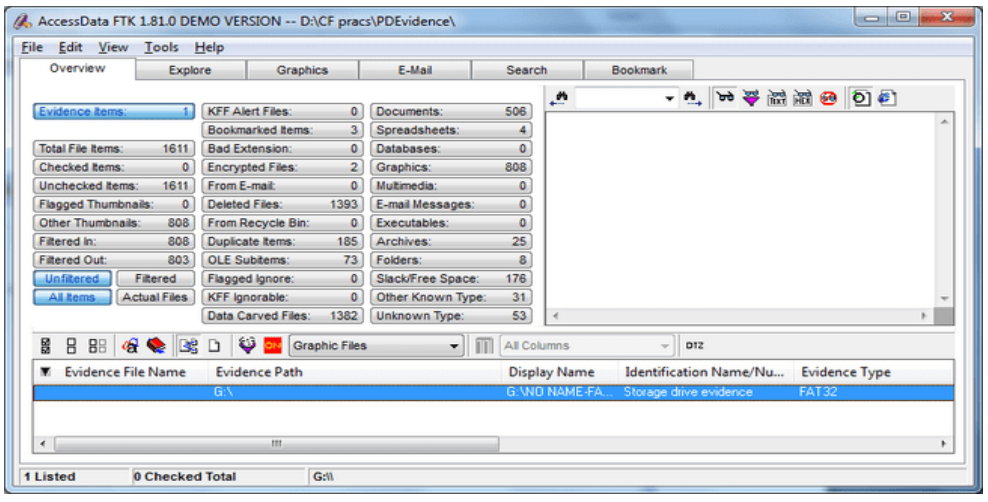
Step 1.In FTK, open an existing case by selecting **File**, and then **Open Case**.

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

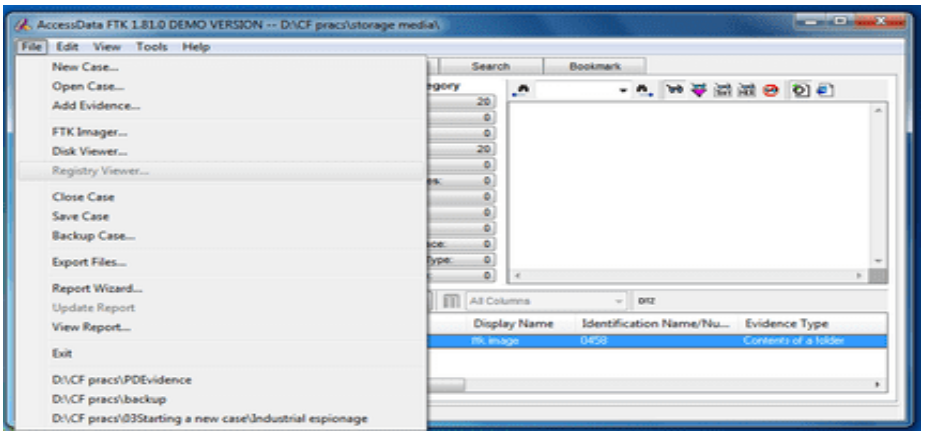


Step 2.Select the case you want to open.





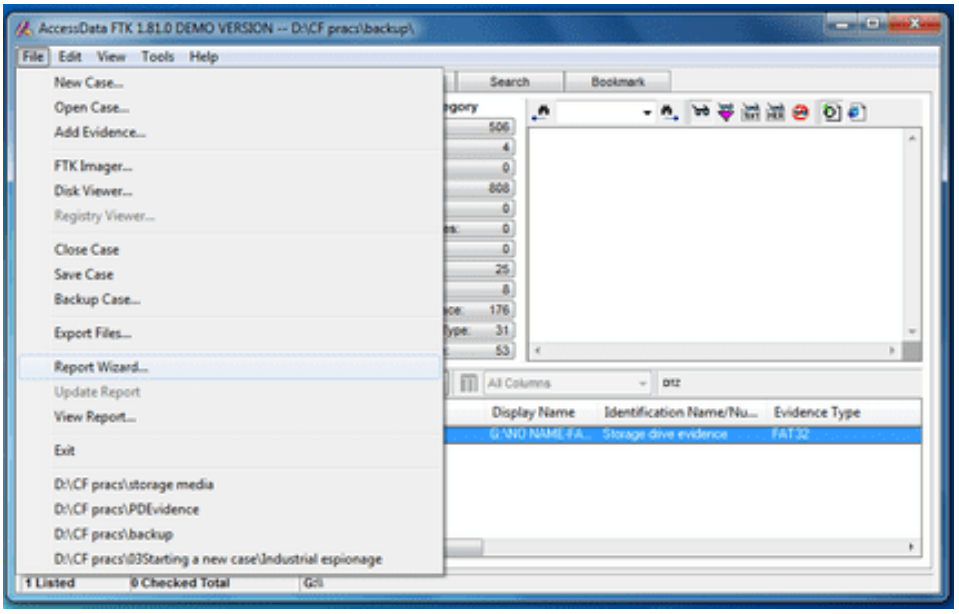
Step 3. Select **File**, and then **Registry Viewer** to open Registry Viewer.
(Can't perform ahead of this step because Registry viewer is disabled in demo version)

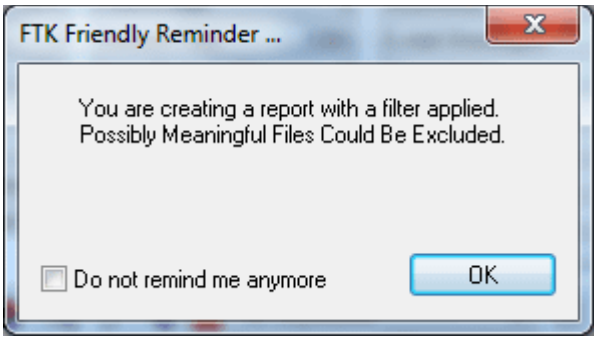


Generating a Report

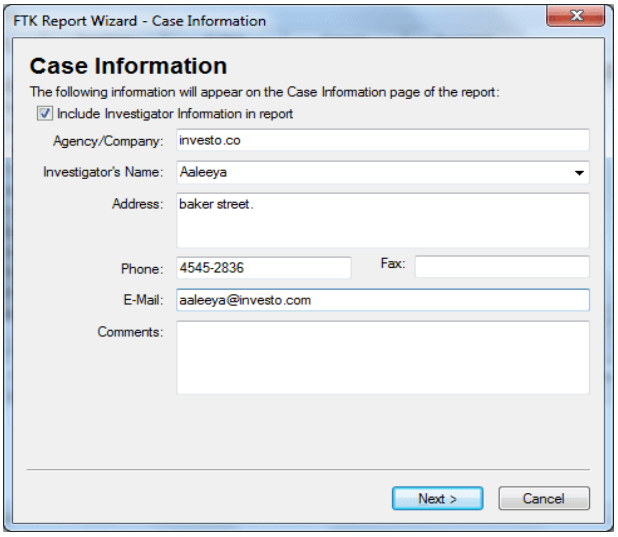
To generate a report file,

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

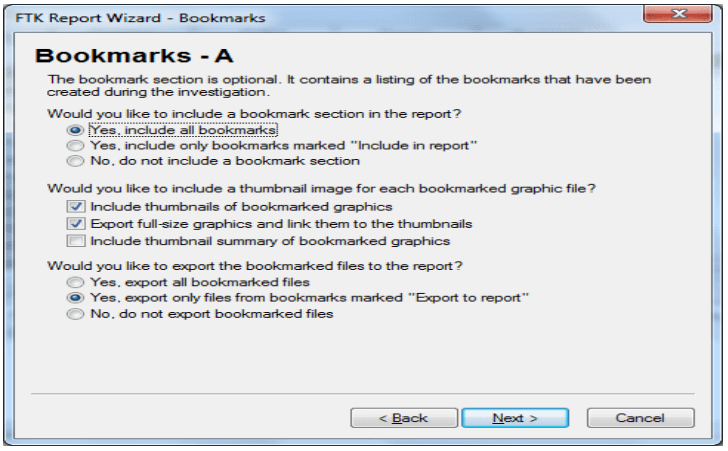




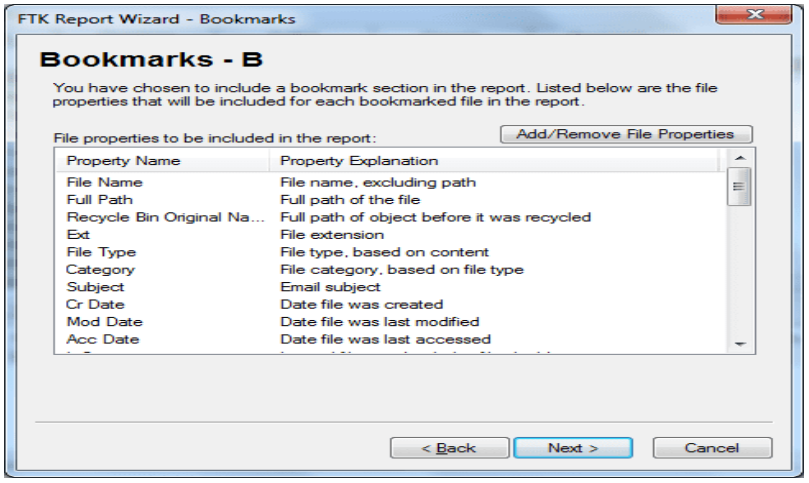
2. The Case Information dialog appears.



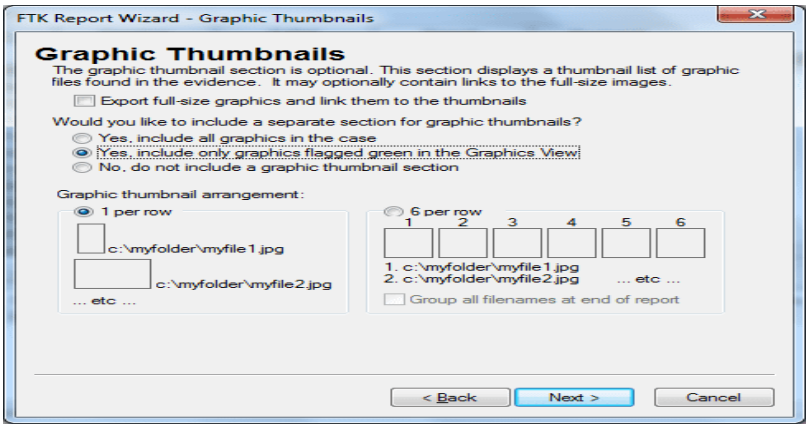
3. The Bookmarks-A dialog appears.



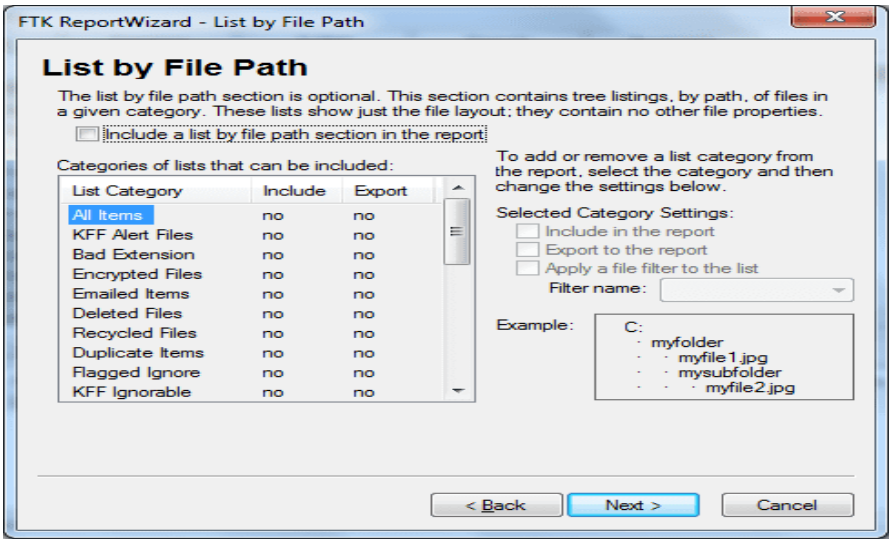
4.The Bookmarks-B dialog appears



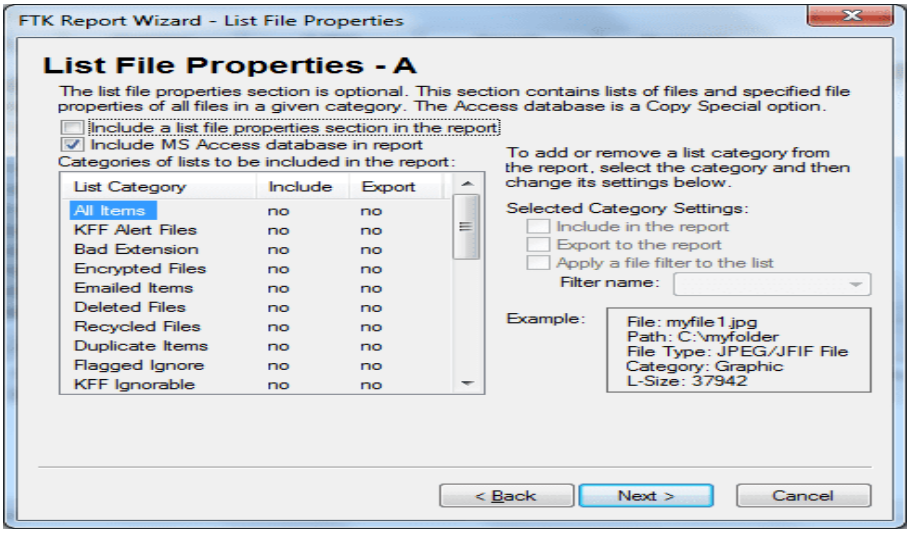
5. The Graphics Thumbnail dialog appears

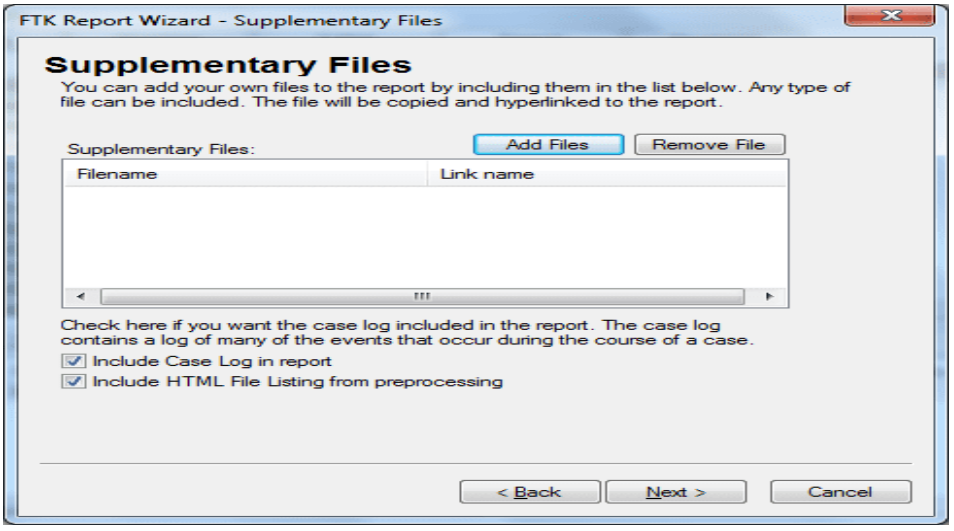


6. The List by File Path dialog appears

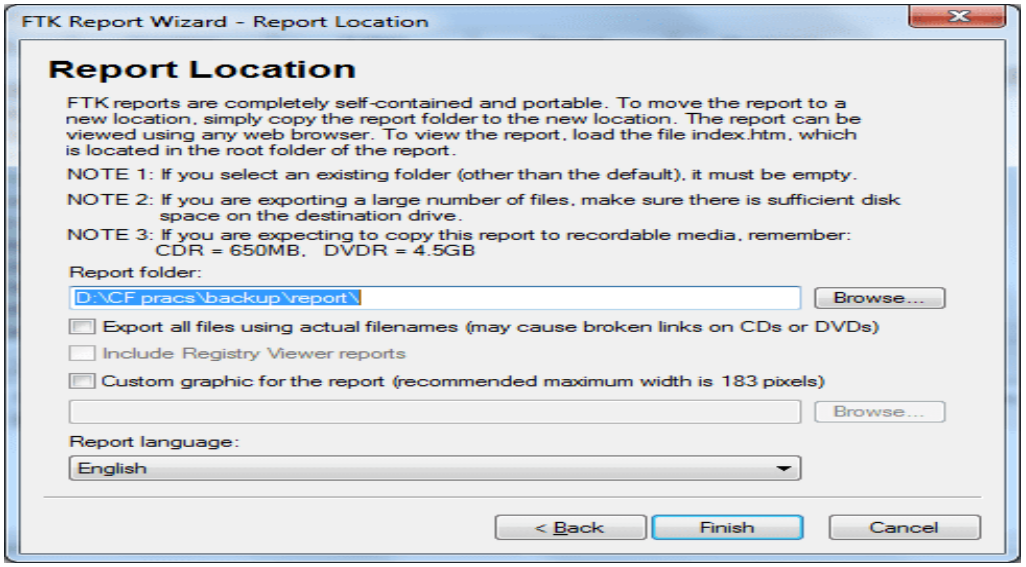


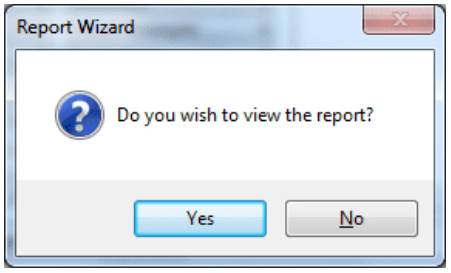
7. Then List File Properties-A dialog appears

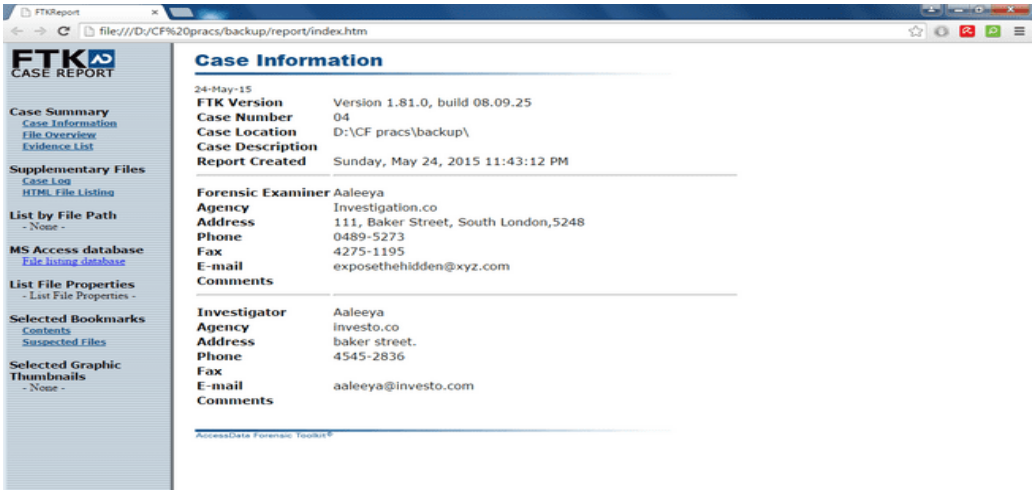


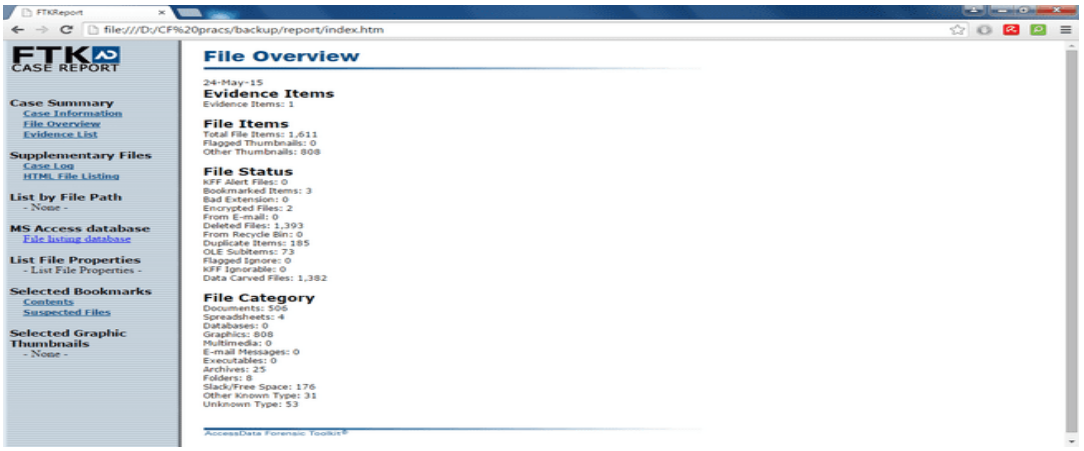


8.The Create Report dialog appears. In the Report Title field, enter a name for the report file. In the Report Location field, enter the location where you want to save the report file or click **Browse** to navigate to the desired location.









B. Email Forensics

- **Email protocols**
- **Recovering emails**
- **Analyzing email header**

Mail Service Providers

An email service provider (ESP) is a company that offers email marketing or bulk email services. An ESP may provide tracking information showing the status of email sent to each member of an address list. ESPs also often provide the ability to segment an address list into interest groups or categories, allowing the user to send targeted information to people who they believe will value the correspondence.

Email Protocols

E-mail Protocols are set of rules that help the client to properly transmit the information to or from the mail server

The most commonly used Email protocols on the internet - POP3, IMAP and SMTP. Each one of them has specific function and way of work.

POP3

Post Office Protocol version 3 (POP3) is a standard mail protocol used to receive emails

from a remote server to a local email client. POP3 allows you to download email messages on your local computer and read them even when you are offline. Note, that when you use POP3 to connect to your email account, messages are downloaded locally and removed from the email server. This means that if you access your account from multiple locations, that may not be the best option for you. On the other hand, if you use POP3, your messages are stored on your local computer, which reduces the space your email account uses on your web server.

By default, the POP3 protocol works on two ports:

Port 110 - this is the default POP3 non-encrypted port

Port 995 - this is the port you need to use if you want to connect using POP3 securely

IMAP

The Internet Message Access Protocol (IMAP) is a mail protocol used for accessing email on a remote web server from a local client. IMAP and POP3 are the two most commonly used Internet mail protocols for retrieving emails. Both protocols are supported by all modern email clients and web servers.

While the POP3 protocol assumes that your email is being accessed only from one application, IMAP allows simultaneous access by multiple clients. This is why IMAP is more suitable for you if you're going to access your email from different locations or if your messages are managed by multiple users.

By default, the IMAP protocol works on two ports:

Port 143 - this is the default IMAP non-encrypted port

Port 993 - this is the port you need to use if you want to connect using IMAP securely

SMTP

SMTP stands for Simple Mail Transfer Protocol. It was first proposed in 1982. It is a standard protocol used for sending e-mail efficiently and reliably over the internet. Simple Mail Transfer Protocol (SMTP) is the standard protocol for sending emails across the Internet.

By default, the SMTP protocol works on three ports:

Port 25 - this is the default SMTP non-encrypted port

Port 2525 - this port is opened on all SiteGround servers in case port 25 is filtered (by your ISP for example) and you want to send non-encrypted emails with SMTP

Port 465 - this is the port used if you want to send messages using SMTP securely

Recovering email using AccessData FTK:

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

2. In the New Case dialog box, type your name for the investigator name, and type the case number and case name. Click Browse, navigate to and click your work folder, click OK, and then click Next.

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

4. Click Next until you reach the Refine Case - Default dialog box, shown in Figure below.

5. Click the Email Emphasis button, and then click Next.

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

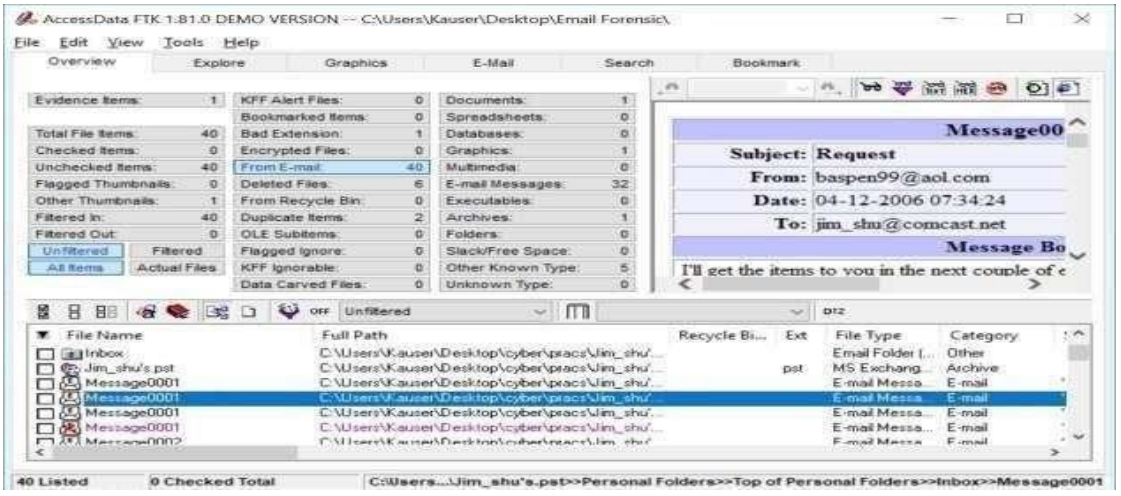
7. In the Add Evidence to Case dialog box, click the Individual File option button (see Figure below), and then click Continue.

8. In the Select File dialog box, navigate to your work folder, click the Jim_shu's.pst file, and then click Open.

9. In the Evidence Information dialog box, click OK.

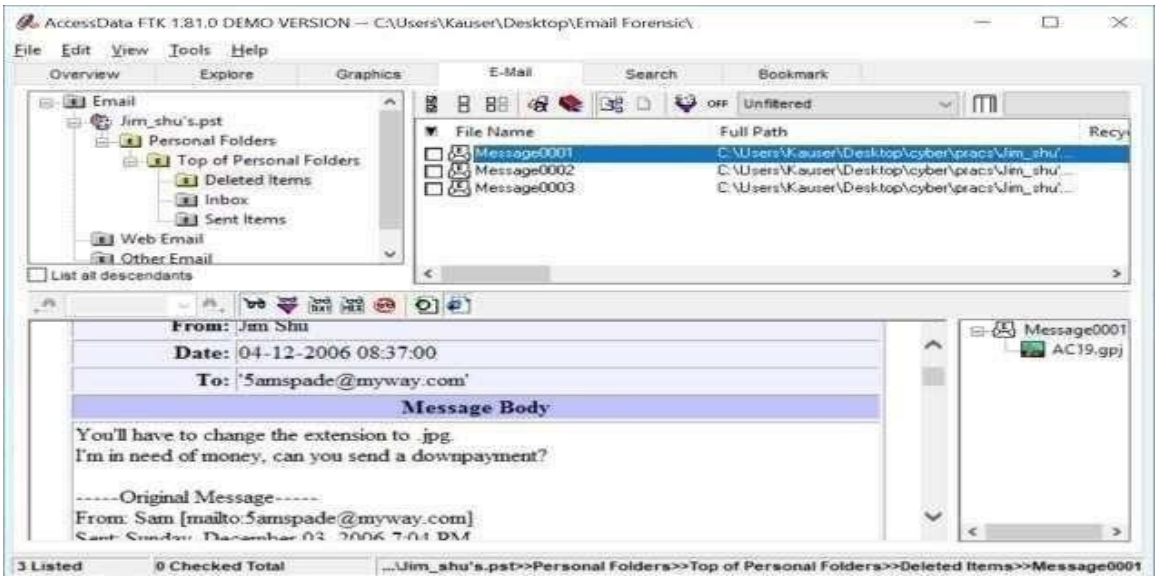
10. When the Add Evidence to Case dialog box opens, click Next. In the Case summary dialog box, click Finish.

11. When FTK finishes processing the file, in the main FTK window, click the E-mail Messages button, and then click the Full Path column header to sort the records (see Figure below).

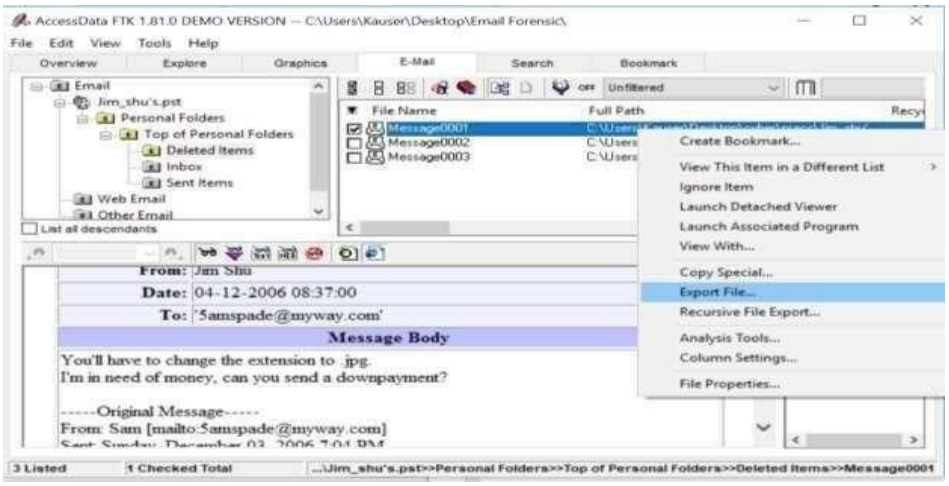


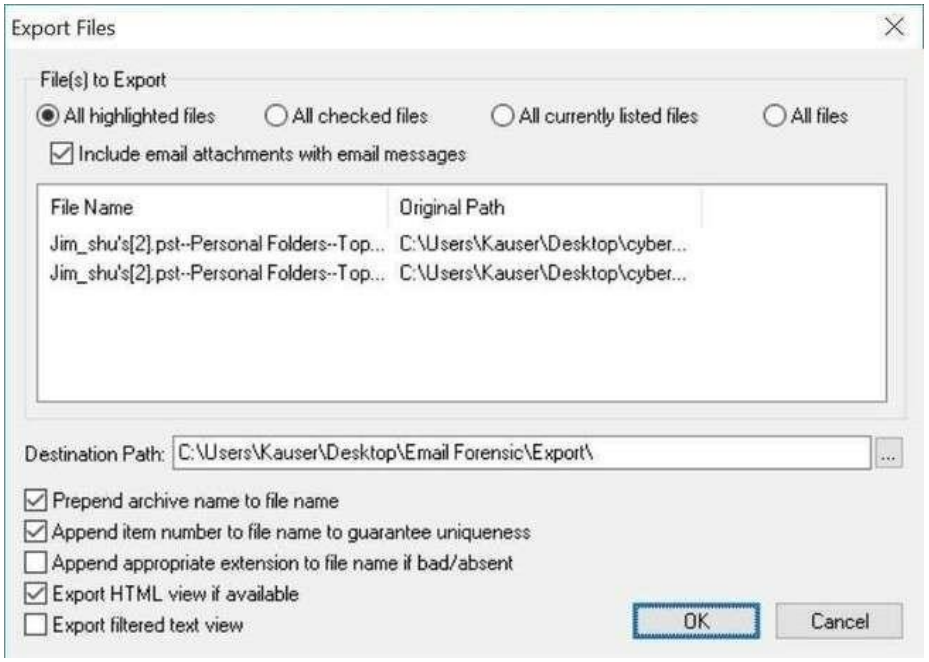
- For email recovery follow following steps:

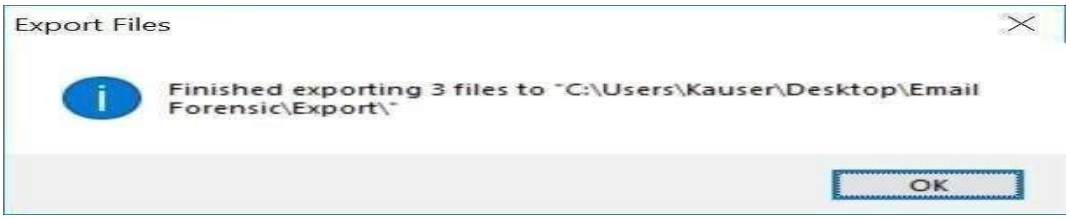
1. Click the E-Mail tab. In the tree view, click to expand all folders, and then click the Deleted Items folder



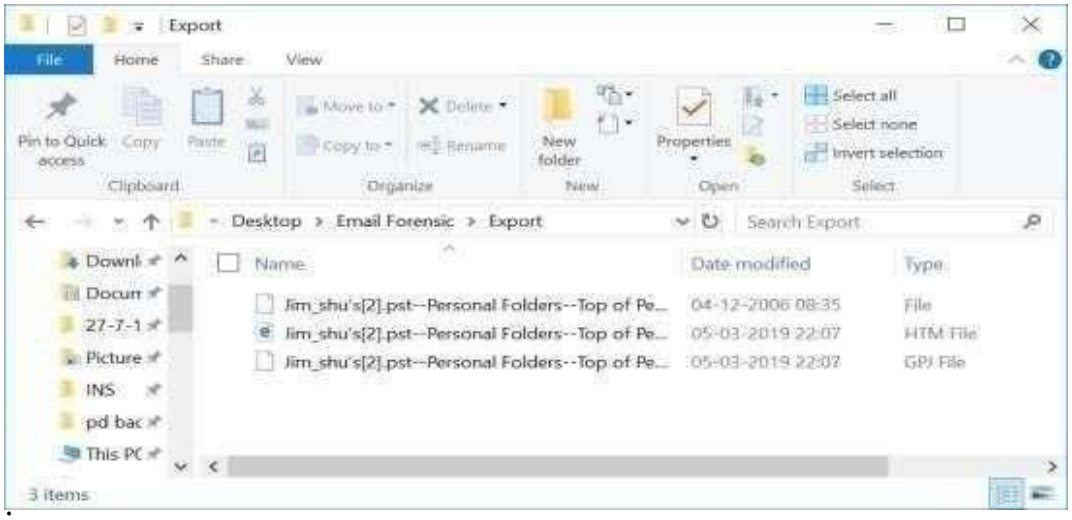
2. Right-click Message0010 in the File List pane and click Export File. In the Export Files dialog box, click OK

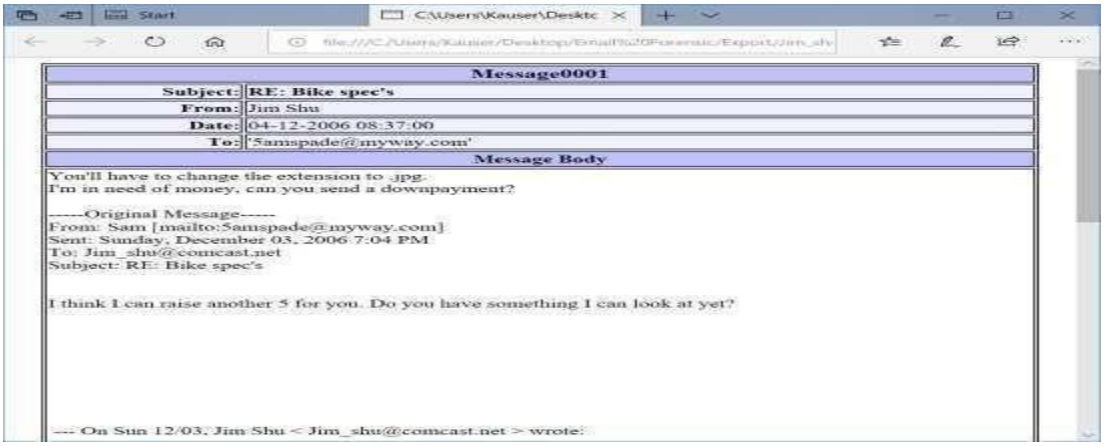






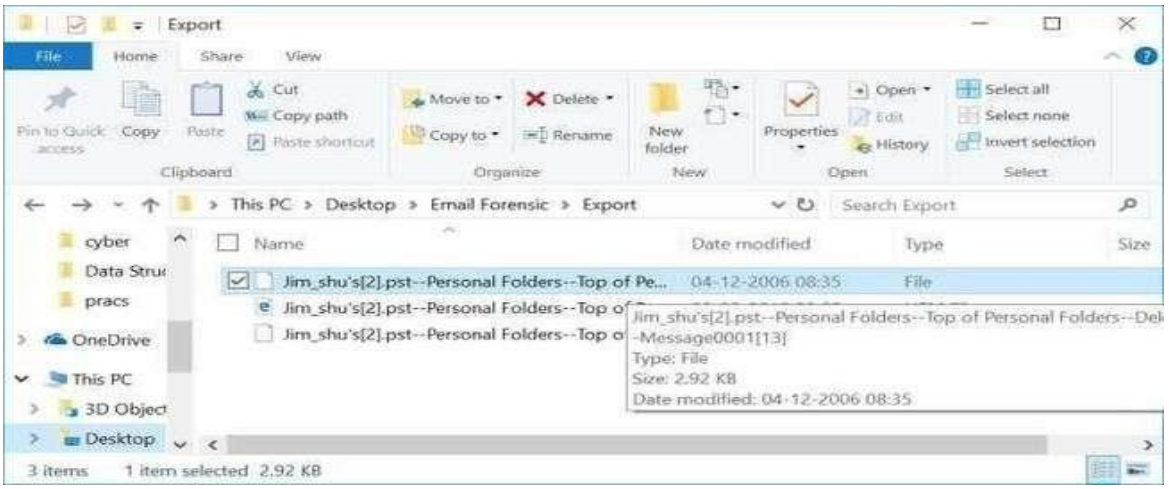
3. Open the Export folder to view the Email Files, Open the HTML file in browser





- For analyzing header follow following steps:

1. Right Click the file type and Rename it to HTML and open in browser to view header information



C. Recovering and Inspecting deleted files

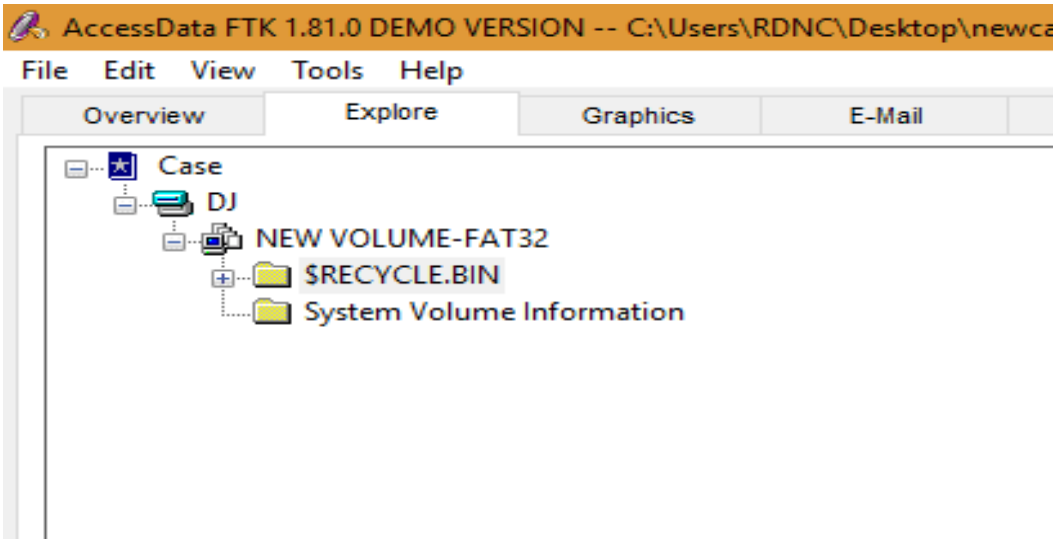
-Check for Deleted Files

-Recover the Deleted Files

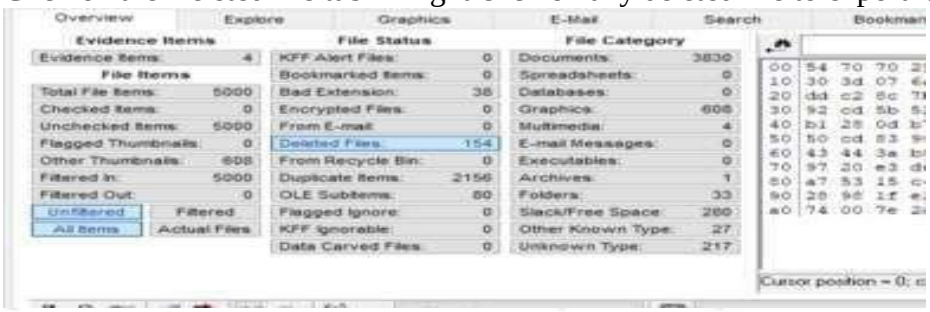
-Analyzing and Inspecting the recovered files

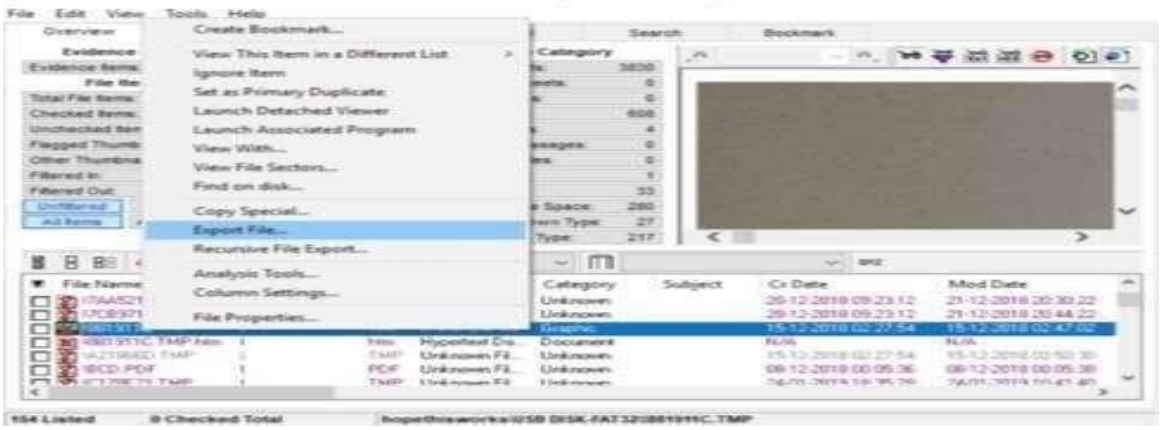
1. Type the destination path.
2. Click on Logical drive.
3. Click on Add > Browse.
4. Select the type of data format and click next.
5. Open the Forensic toolkit and click on file > new case.
6. Enter the details and click on next.
7. Click on next.
8. Click on Add Evidence > Acquired Image of Drive > Continue.
9. Select the image file.
10. Click on OK.

In the left panel you can see all the recovered files.

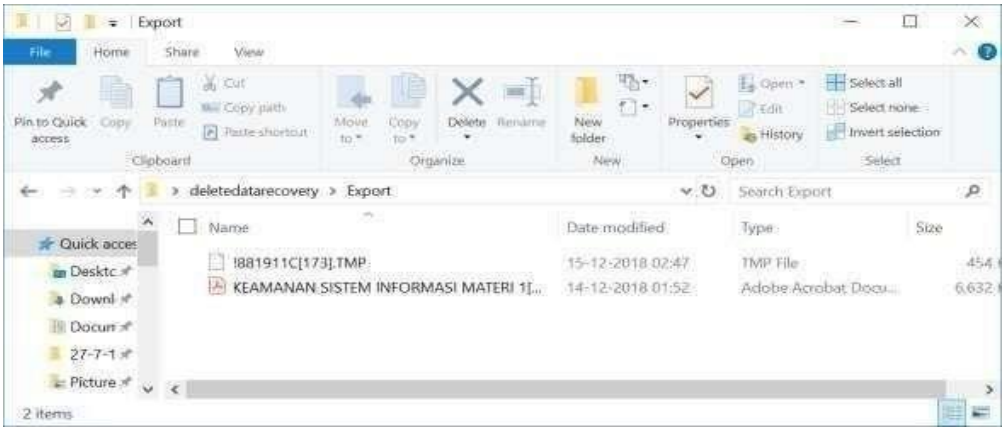


Click on the Deleted file tab-> Right click on any deleted file to export it





Browse and choose the destination folder to export the deleted file



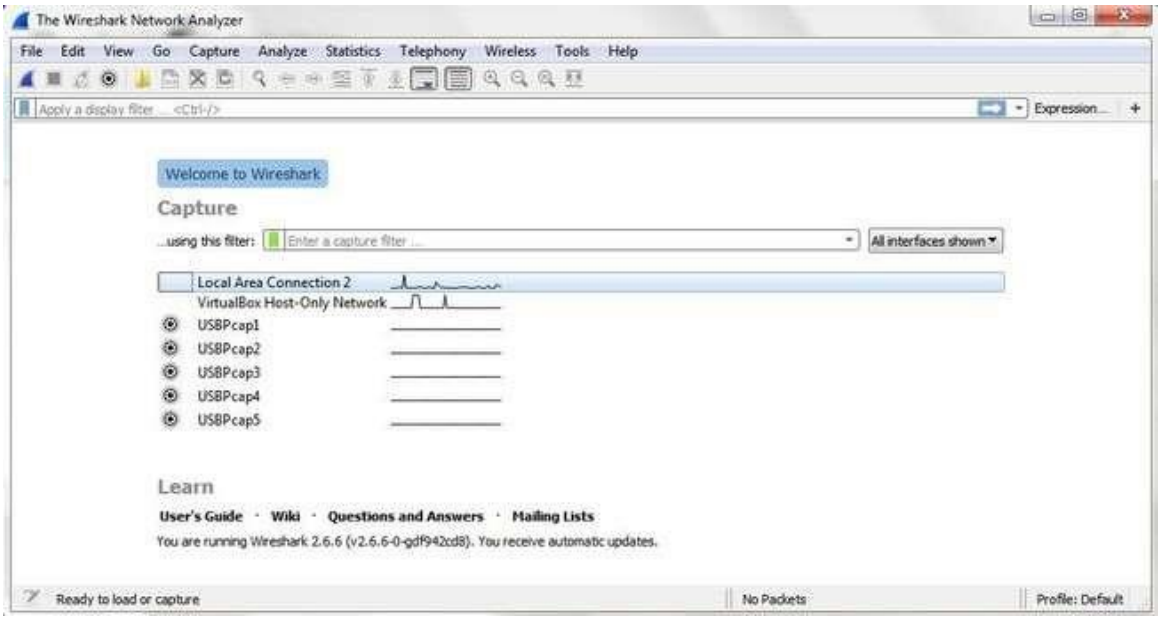
Practical No – 5

Aim: Capturing and analyzing network packets using Wireshark
Identification the live network

- **Capture Packets**
- **Analyze the captured packets**

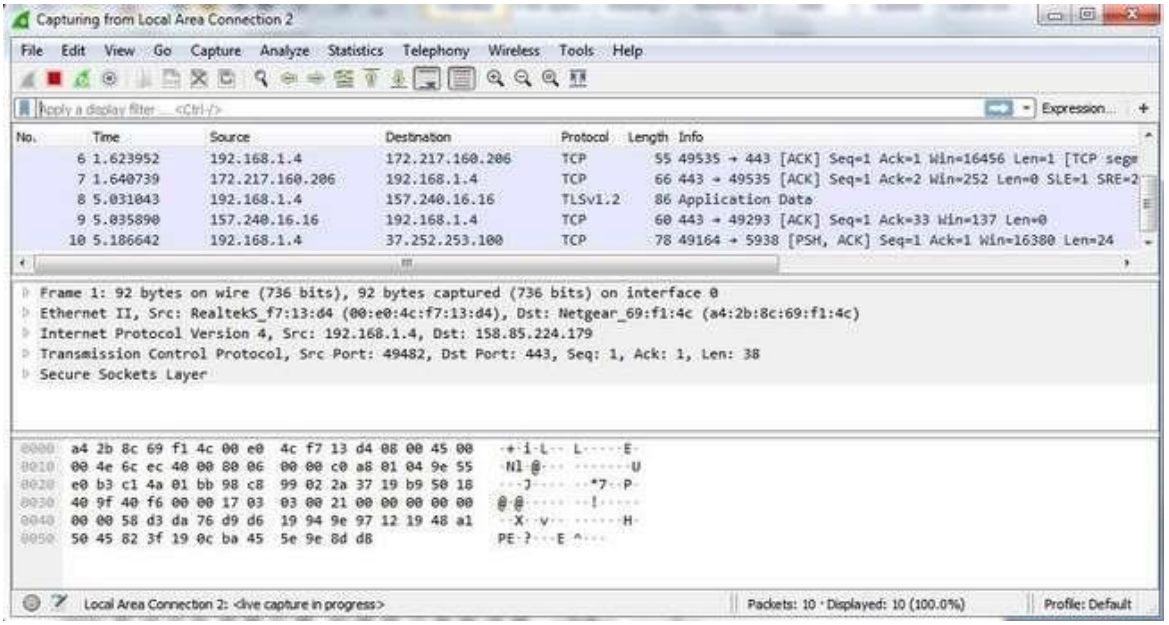
Steps:
Capturing Packets

Capture traffic on your wireless network, click your wireless interface.
You can configure advanced features by clicking Capture > Options, but this isn't necessary for now.
1. Open Wireshark and click on Ethernet.



As soon as you single-click on your network interface's name, you can see how the packets are working in real time. Wireshark will capture all the packets going in and out of our systems. Promiscuous mode is the mode in which you can see all the packets from other systems on the network and not only the packets send or received from your network adapter. Promiscuous mode is enabled by default. To check if this mode is enabled, go to Capture and Select Options. Under this window check, if the

checkbox is selected and activated at the bottom of the window. The checkbox says "Enable promiscuous mode on all interfaces".

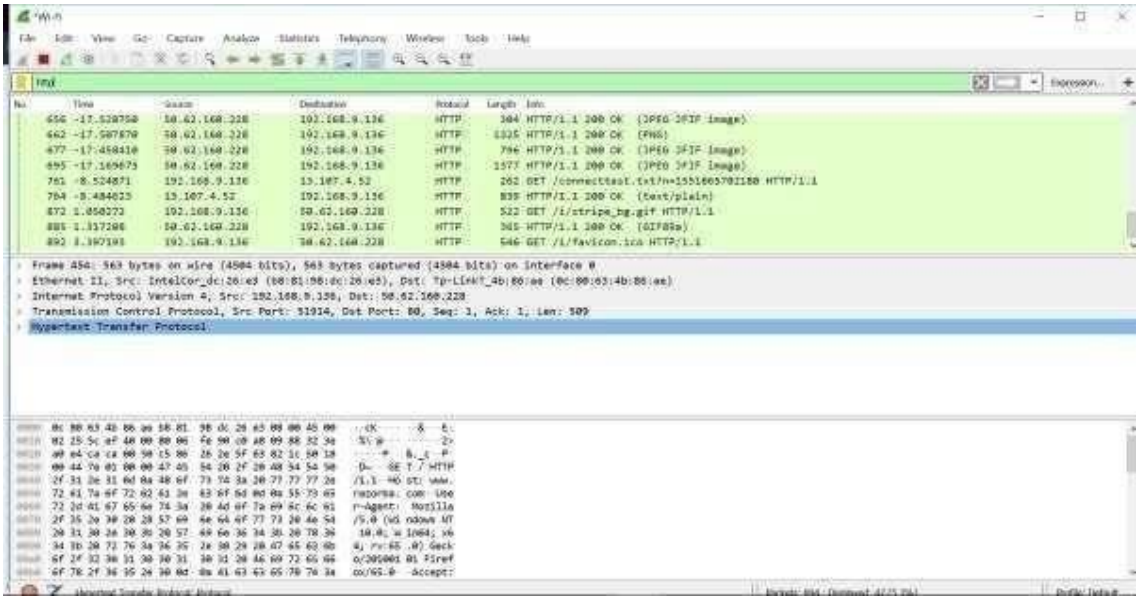


The red box button "STOP" on the top left side of the window can be clicked to stop the capturing of traffic on the network.

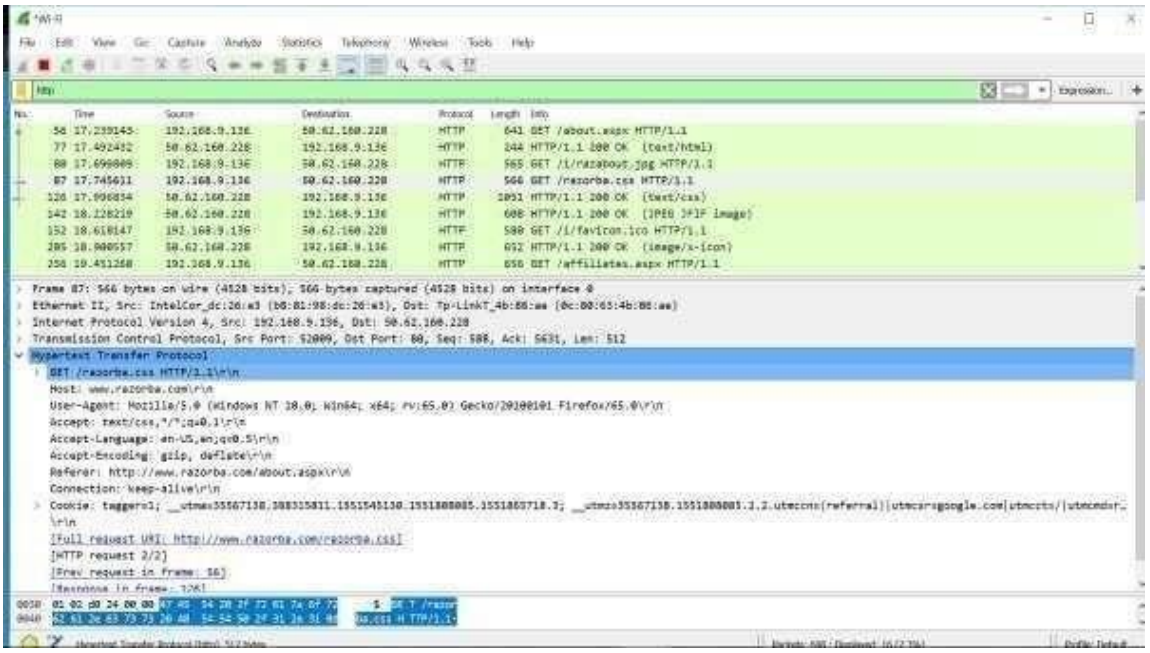
2. Now go on browser and open any unsecured website i.e www.razorba.com and

3. perform some activity on the website.

4. Now come back to Wireshark and enter http in the search bar.

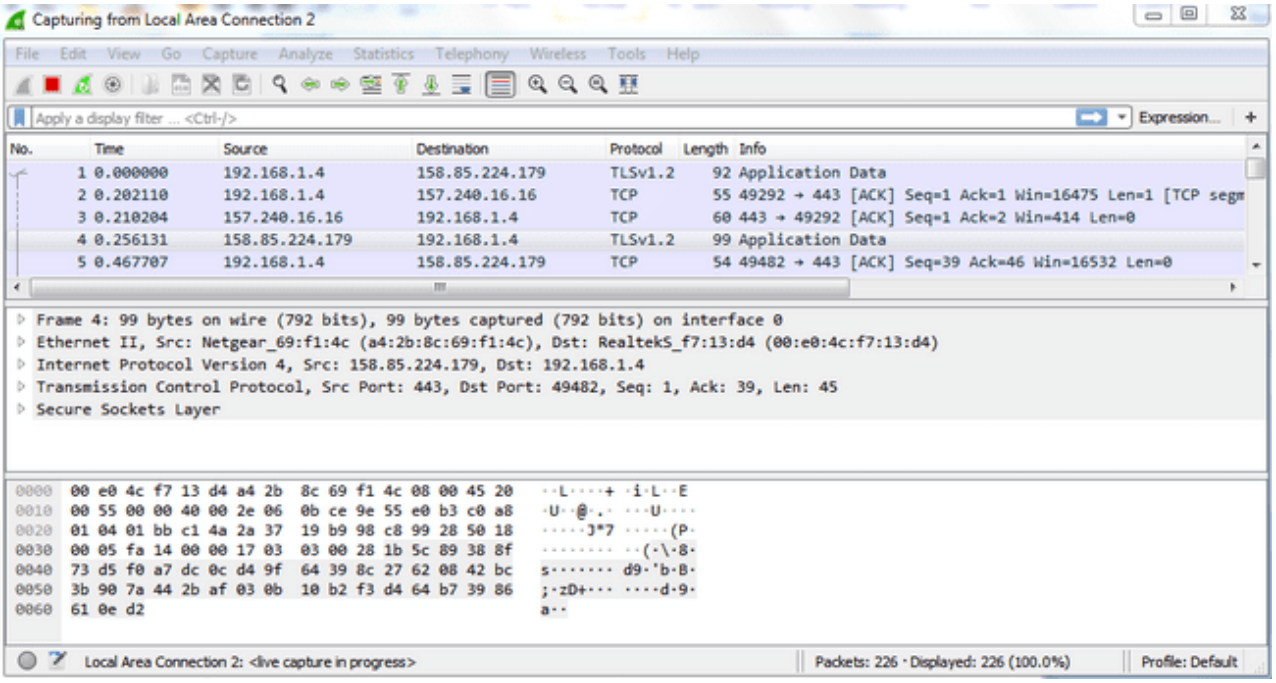


5. Now click on the get request and see the details.

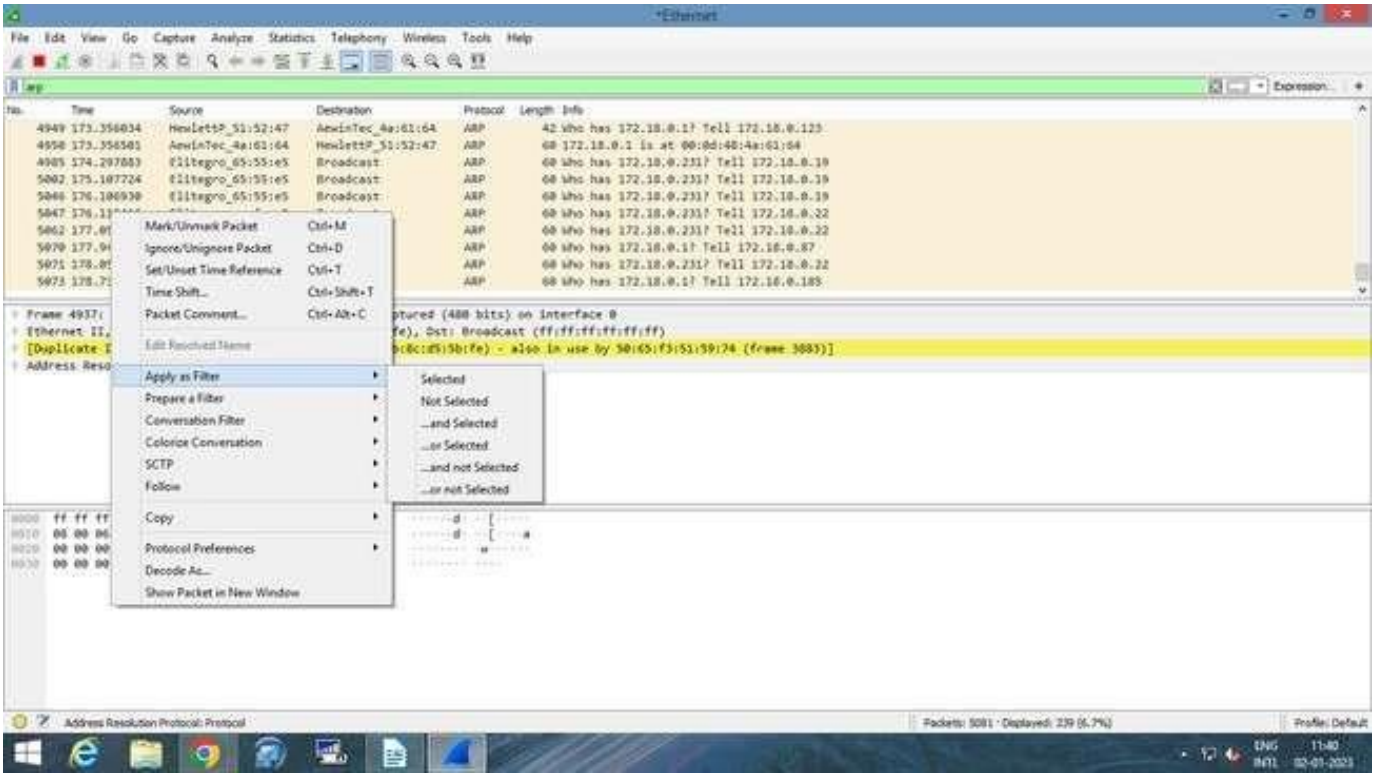


Analyze the captured Packets:

First of all, click on a packet and select it. Now, you can scroll down to view all its details.



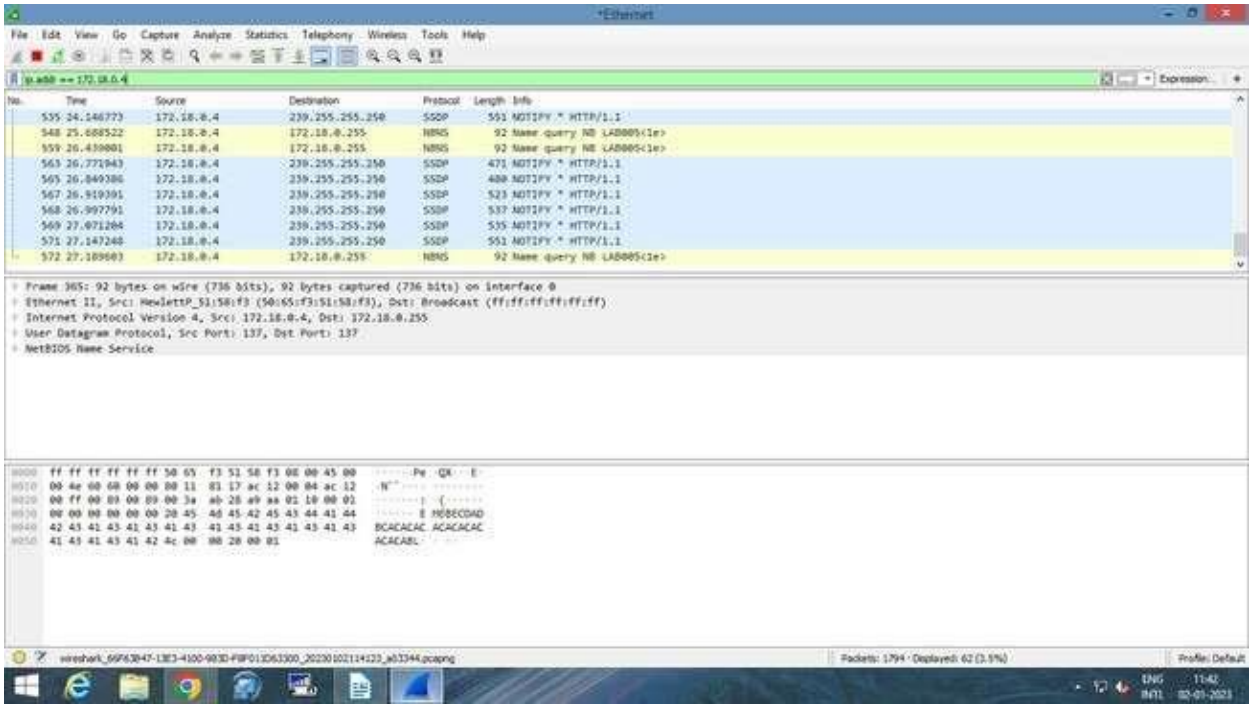
Filters can also be created from here. Right-click on one of any details. From the menu select Apply as Filter drop-down menu so filter based on it can be created.



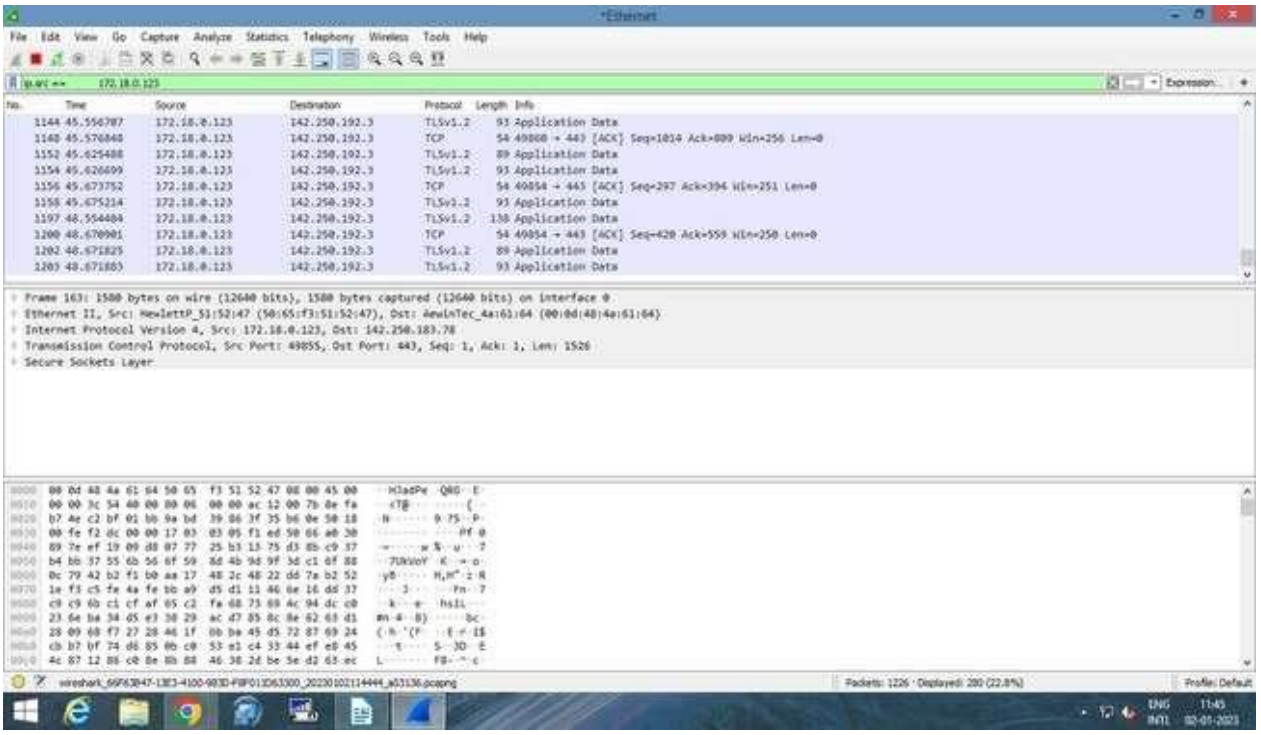
Display filter command –

1. Display packets based on specific IP-address

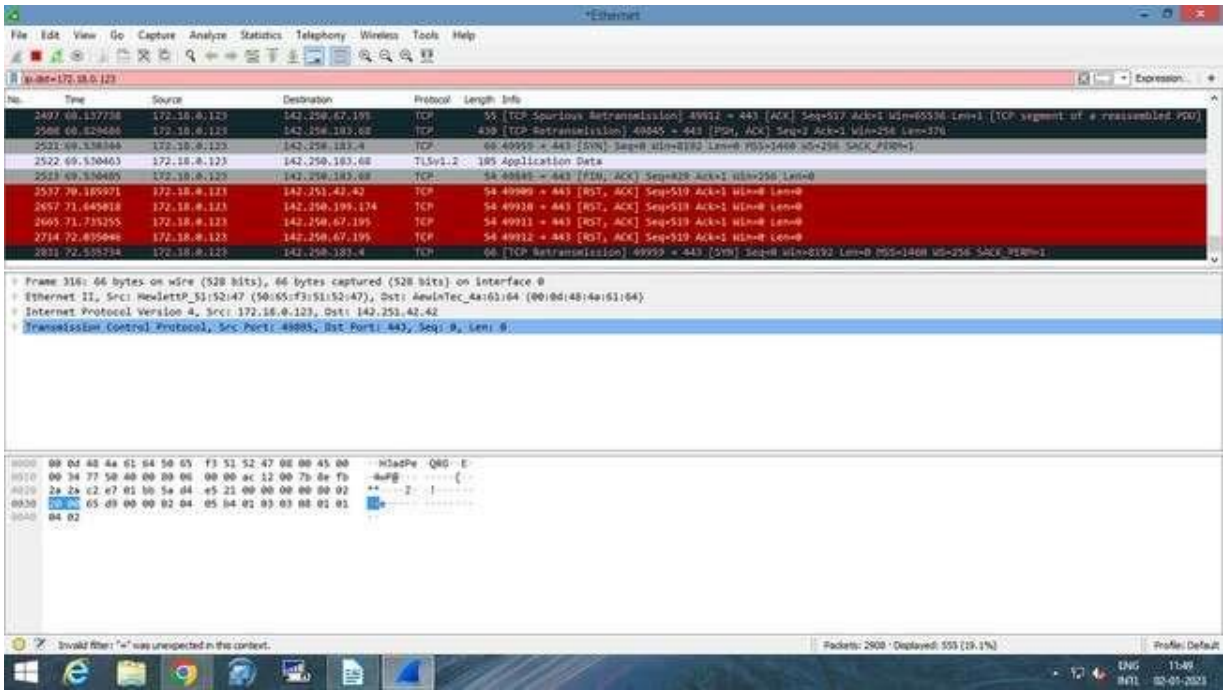
ip.addr == 172.18.0.4



2. Display packets which are coming from specific IP-addressip.src == 172.18.123



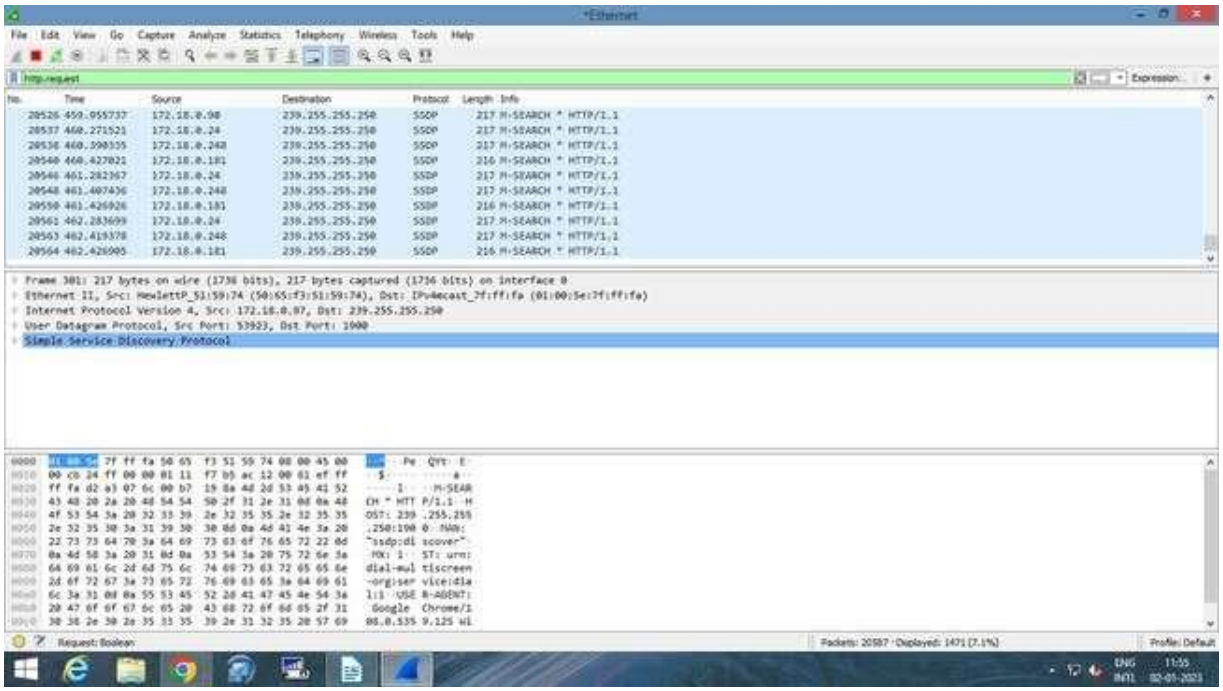
3. Display packets which are having specific IP-addressdestination ip. dst ==172.18.0.123



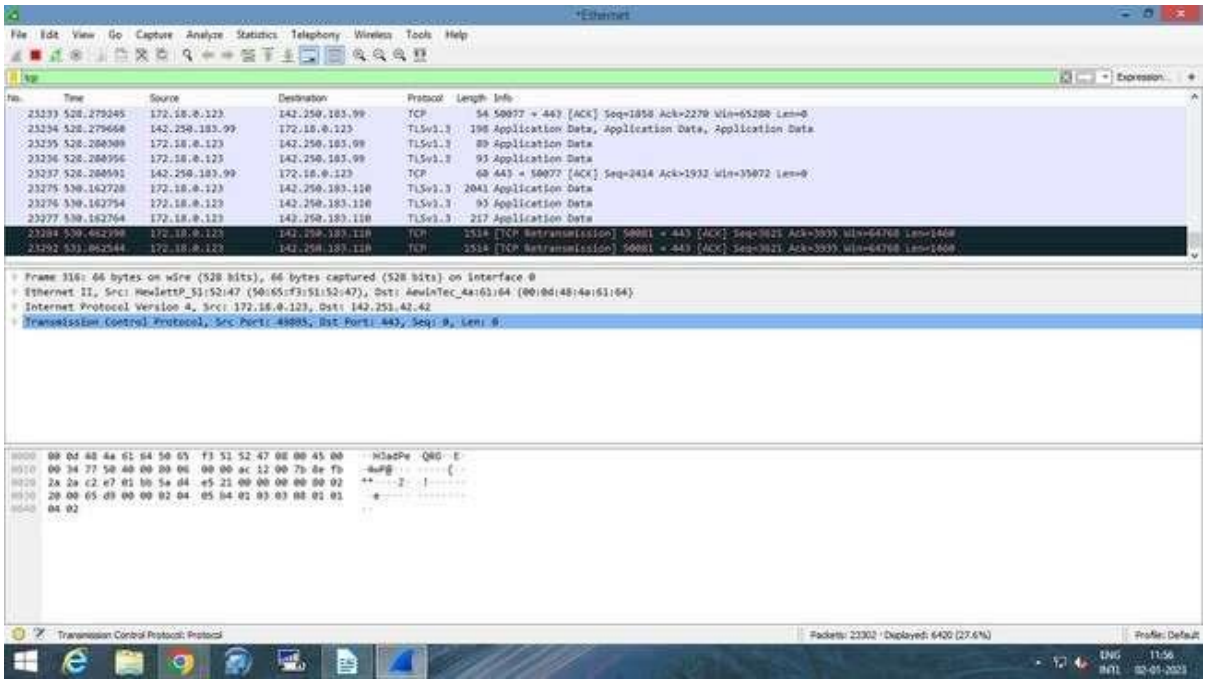
4. Display packets which are using http protocol

No.	Time	Source	Destination	Protocol	Length	Info
58	74.985092	192.168.1.4	192.168.1.1	HTTP	250	GET /rootDesc.xml HTTP/1.1
62	74.987756	192.168.1.1	192.168.1.4	HTTP/X…	1234	HTTP/1.1 200 OK
972	129.457310	192.168.1.4	172.217.166.174	HTTP	1000	GET / HTTP/1.1
975	129.542230	172.217.166.174	192.168.1.4	HTTP	594	HTTP/1.1 301 Moved Permanently (text/html)
39156	277.292187	192.168.1.4	117.18.237.29	OCSP	137	Request
39157	277.314544	117.18.237.29	192.168.1.4	OCSP	842	Response
39168	277.419340	192.168.1.4	117.18.237.29	OCSP	137	Request
39169	277.463638	117.18.237.29	192.168.1.4	OCSP	842	Response
39204	279.409683	192.168.1.4	23.57.219.27	OCSP	137	Request
39206	279.420870	23.57.219.27	192.168.1.4	OCSP	712	Response

5. Display packet http.request

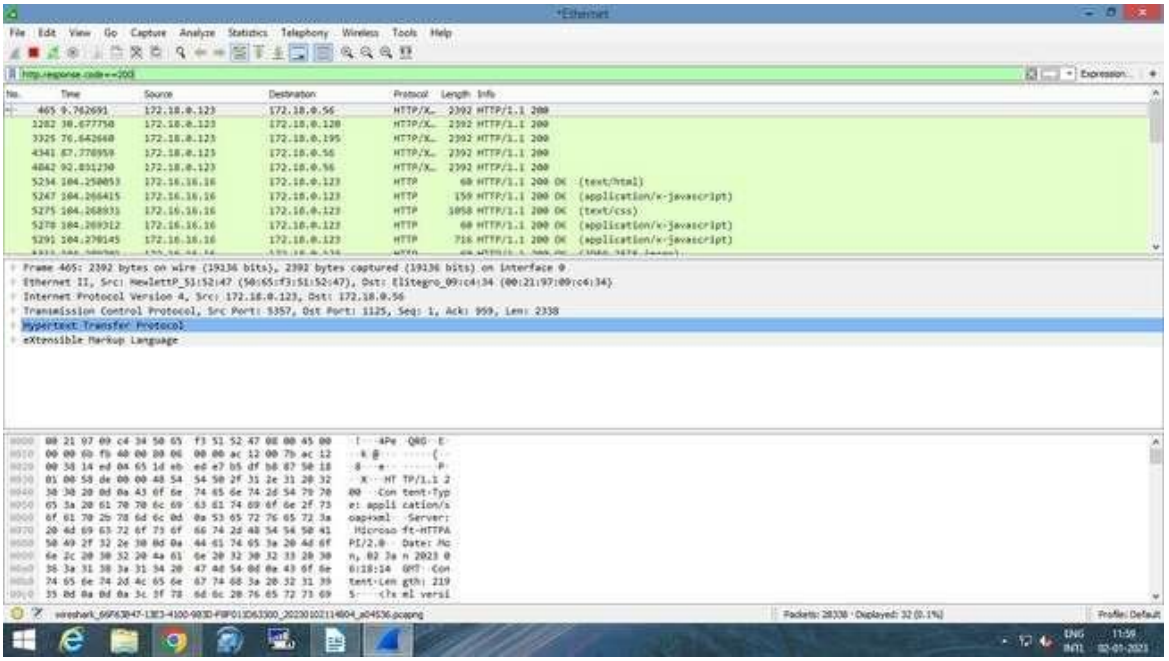


6. Display packets tcp

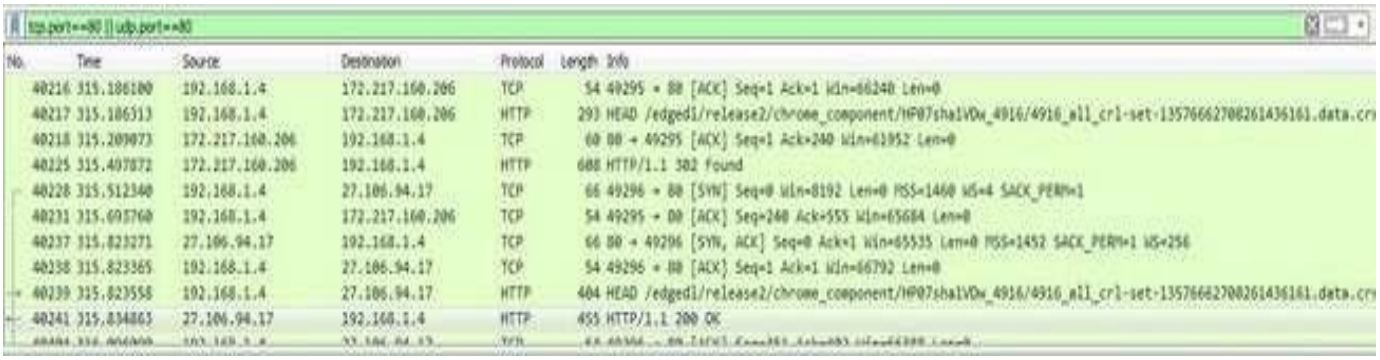


Display packets having no error connecting to server

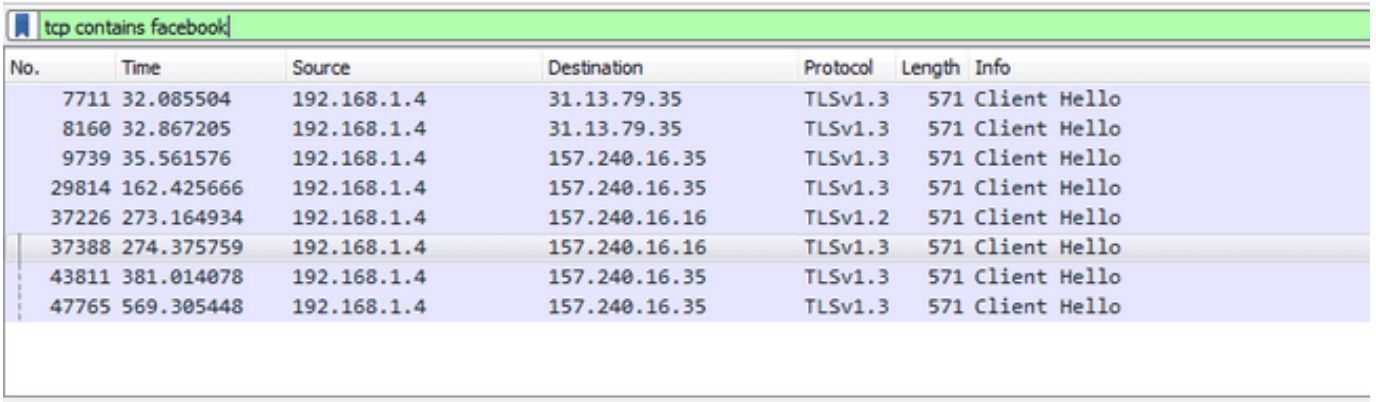
http.response.code==200



7. Display packets having port number 80
tcp.port==80 || udp.port==80



8. Display tcp contains facebook



No.	Time	Source	Destination	Protocol	Length	Info
7711	32.085504	192.168.1.4	31.13.79.35	TLSv1.3	571	Client Hello
8160	32.867205	192.168.1.4	31.13.79.35	TLSv1.3	571	Client Hello
9739	35.561576	192.168.1.4	157.240.16.35	TLSv1.3	571	Client Hello
29814	162.425666	192.168.1.4	157.240.16.35	TLSv1.3	571	Client Hello
37226	273.164934	192.168.1.4	157.240.16.16	TLSv1.2	571	Client Hello
37388	274.375759	192.168.1.4	157.240.16.16	TLSv1.3	571	Client Hello
43811	381.014078	192.168.1.4	157.240.16.35	TLSv1.3	571	Client Hello
47765	569.305448	192.168.1.4	157.240.16.35	TLSv1.3	571	Client Hello

Practical No: 6

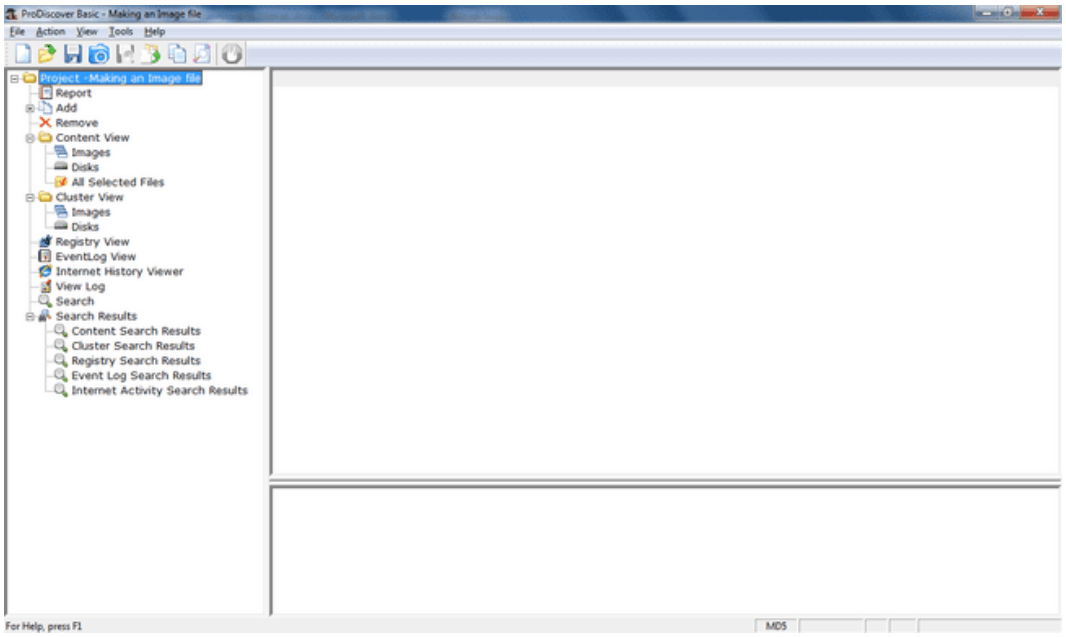
Aim: Exploring ProDiscover Basic.

Creating a New Project:

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

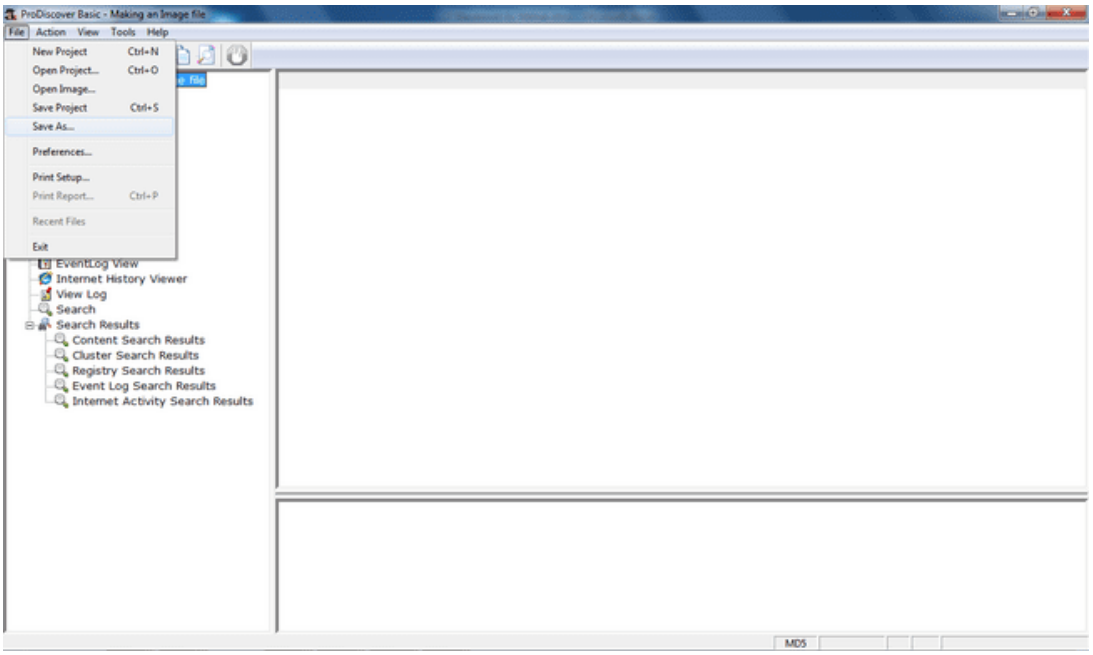
Step 2) Enter a project number, project name, and description of the project in the new project tab option, and then click the Open button.

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

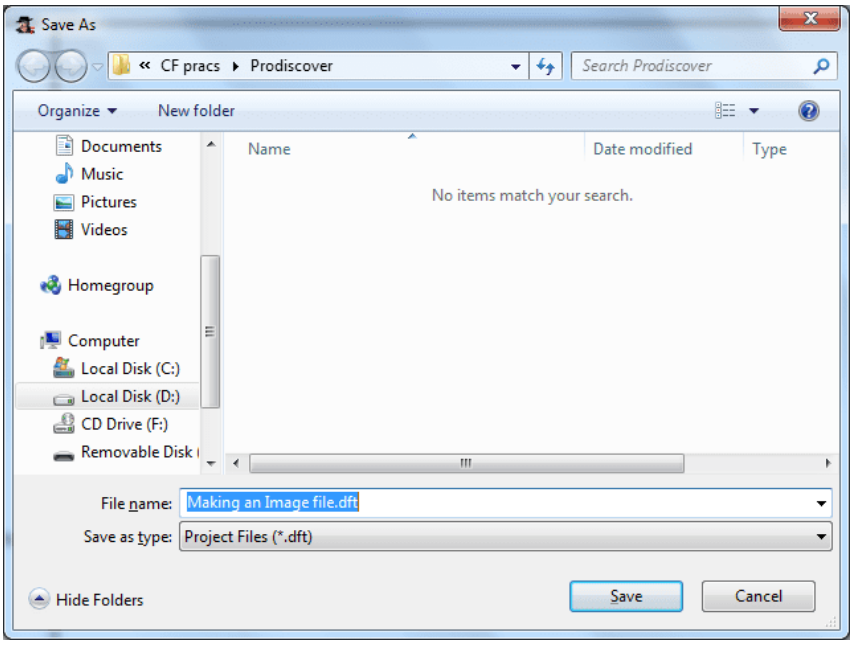


2) Saving a project:

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.

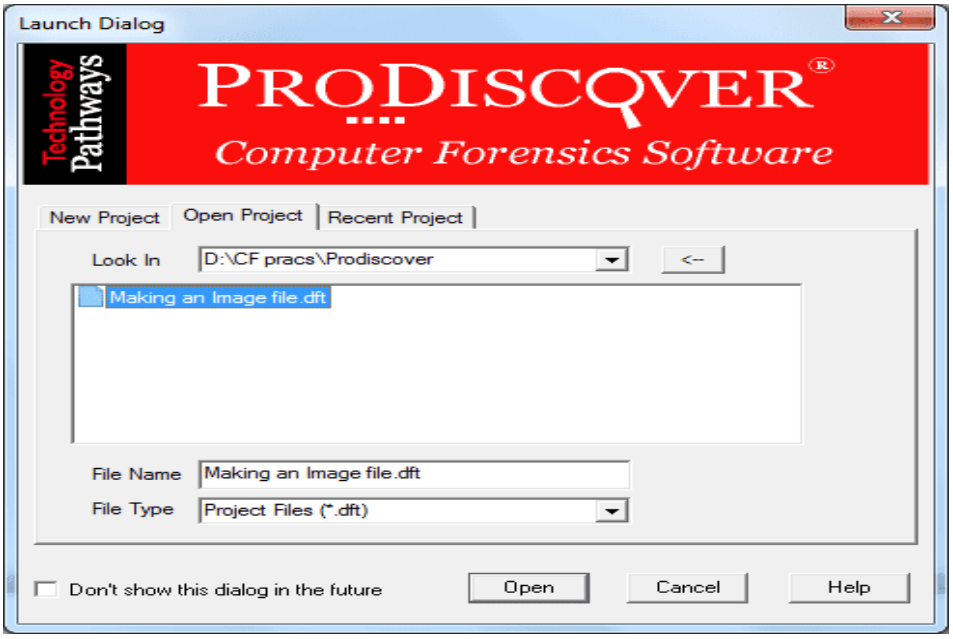


3] Select the destination path and click the **Save** button.

4] ProDiscover saves the project at the path specified.

3)Preview a directly connected evidence drive

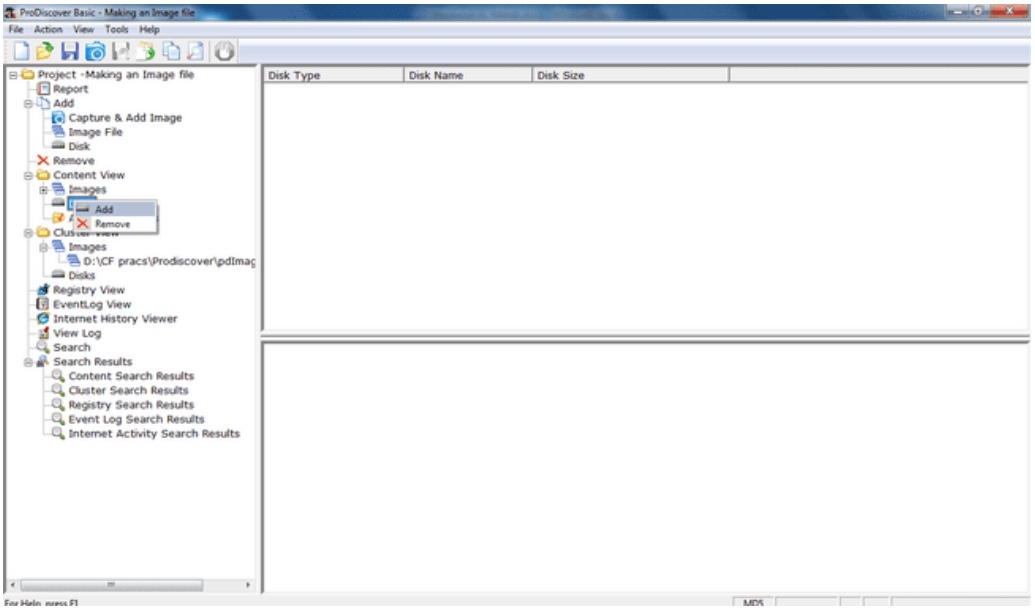
1] Launch ProDiscover.
2] Select **open project** tab option.



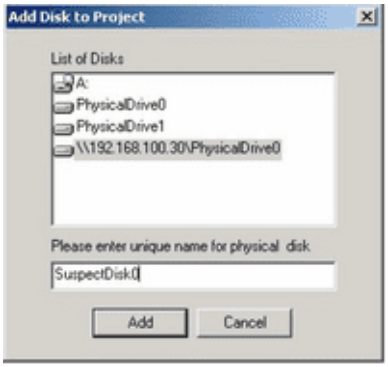
3] Select the project file to open and click **Open** button.

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

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



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



7] ProDiscover then adds the physical disk to the currently active project.

8] Perform actions on the newly added disk such as search, hash compare and recovery).

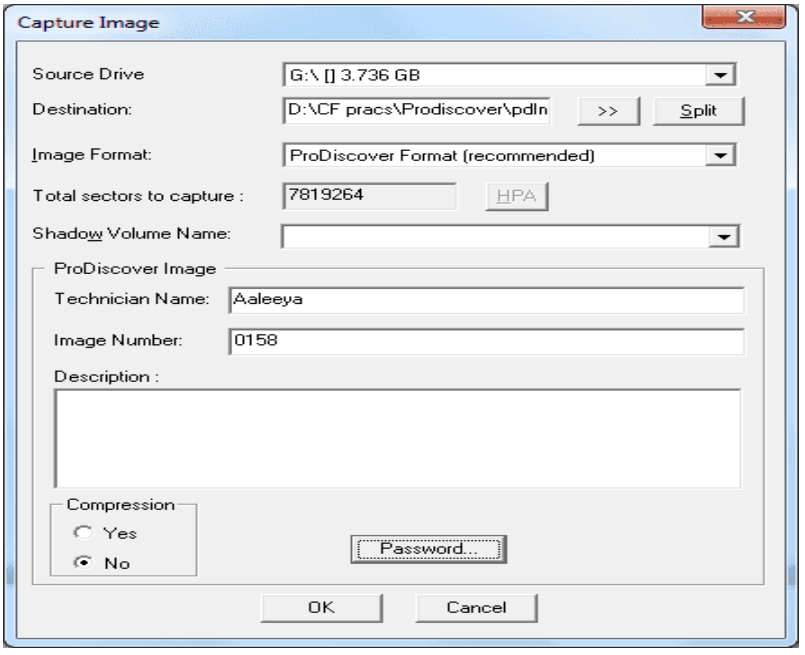
4) <u>Conducting Live Preview of a Remote Disk (NOT DONE)</u>

5) <u>Capture an image of an attached drive</u>

1. Ensure the desired evidence drive is attached to the ProDiscover system.

2. Select the capture image option from the action menu item, or button bar.

3. ProDiscover presents the capture image dialog.



4. Select the drive to be captured, destination path for the image file to be saved into, compression and password protection of the image file and specify the technician name, image number, description of the image file.

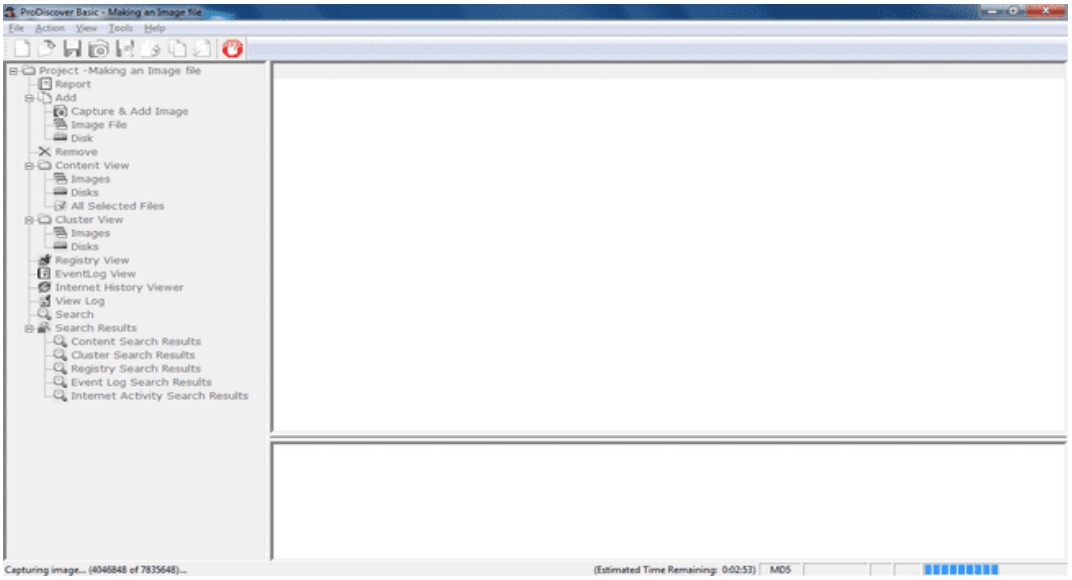
5. We also have the option to select the desired image format. ProDiscover recommends using the ProDiscover format which includes adding metadata to the image containing information for password protection, time zone, investigator and compression. A technical description of the ProDiscover image format can be found on the Technology Pathways web site in the resources section. Alternately, users can select to create an image in the UNIX style 'dd' format which creates a flat bit-stream

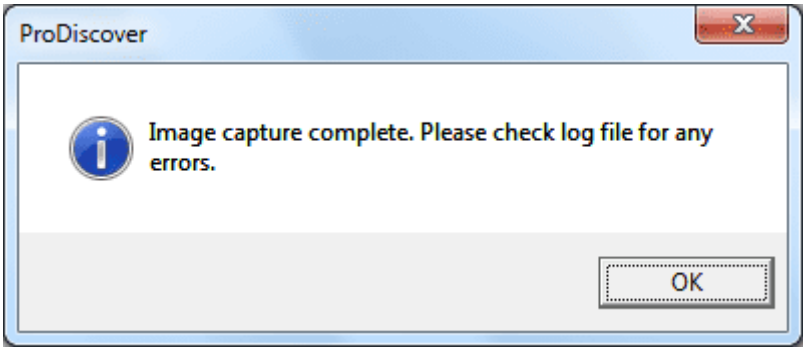
image and a corresponding hash file using the selected hashing algorithm. the corresponding hash file will be placed in the image directory and named the same as the image using a .md5 or .sha file extension.
6. To compress the image select "Yes" to compression and ProDiscover will compress the image and save it as *.cmp. Note that compressing an image requires more time to capture due to the compression overhead.

7. Click "OK".

8. ProDiscover reads the drive connected bit-by-bit and creates an image file in the specified location. The image file will contain an exact replica of the original disk, plus a few bites of checksum and log data.

9. ProDiscover will create a log file if there are any I/O errors.





6) <u>Capturing Physical Memory</u>

7) <u>Add an image file to a project:</u>

1. Launch ProDiscover.

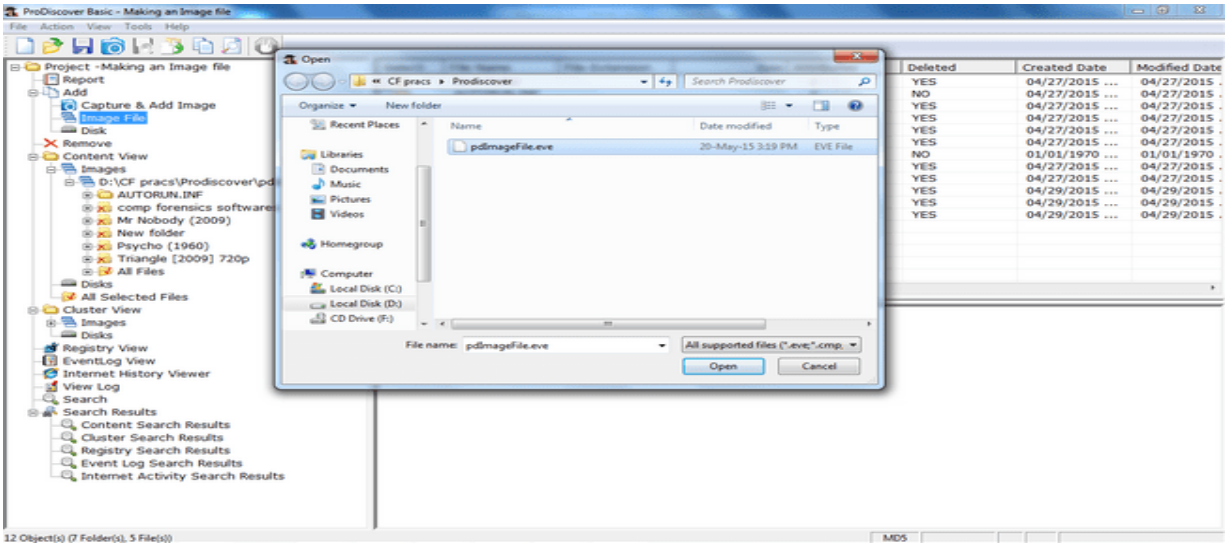
2. Select **open project** tab option.

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

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

5. Select the **Add Image** option from the action menu, or tree-view. Users may also right-click on "Disks", "Images" or "Remote Drives" from Content-view to add a disk, image or remote drive to the project.

6. ProDiscover presents the file open dialog.



7. Select the desired image file and Click **Open** button. If the image is of a Windows NTFS Dynamic Disk, users should select the image's corresponding *.pdg file which describes the disk group. If the image was a ProDiscover Split image, users should select the *.pds file which describes all split files comprise the total disk image.

8. UNIX style "dd" images can be added to projects provided with or without the .eve file extension. To add a dd image to the project without an expected extension choose "All Files (*.*) from the "File of Types" Drop down list. If the "dd" image is split into several images they should be numbered sequentially and all contain a .eve file extension. Once the image files are named and numbered correctly a corresponding *.pds file should be created in the following format:

DD-SplitImage

D:\Images\Splits\dd\Split0.eve

D:\Images\Splits\dd\Split1.eve

D:\Images\Splits\dd\Split2.eve

D:\Images\Splits\dd\Split3.eve

D:\Images\Splits\dd\Split4.eve

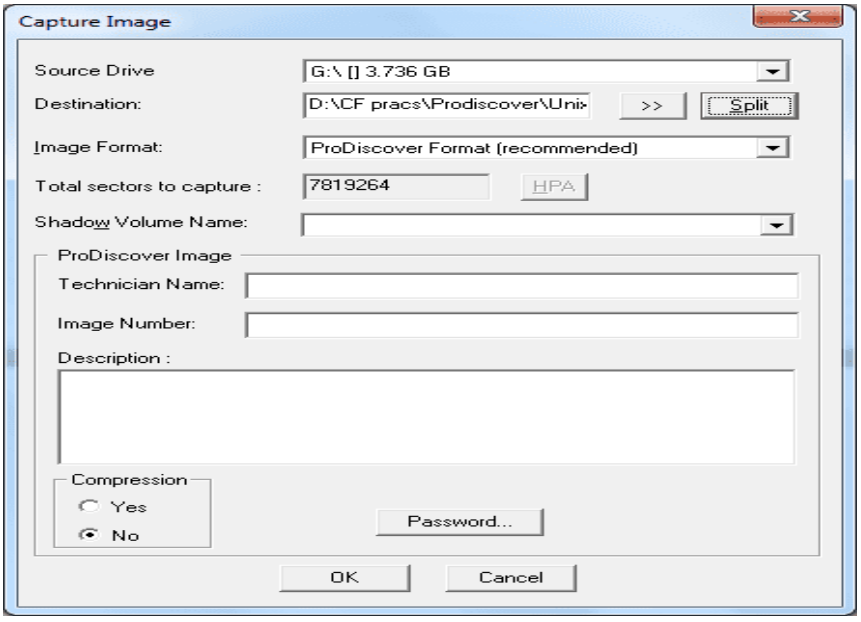
9. Note that all split image file should be split in sizes which are multiples of 512. To add the split "dd" image users should select the split.pds file created above.

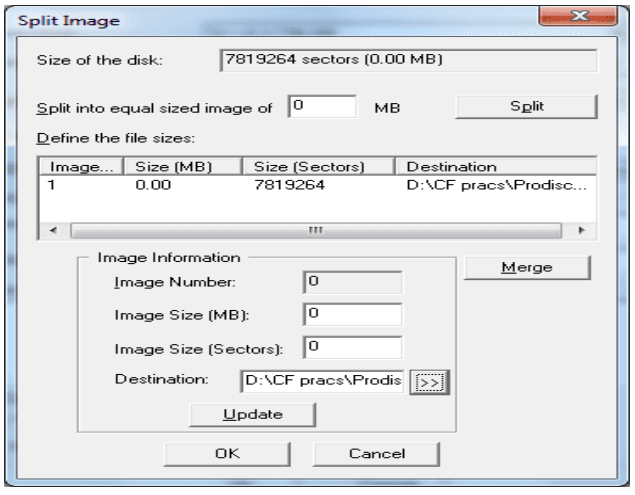
10. ProDiscover then adds the image file to the currently active project.

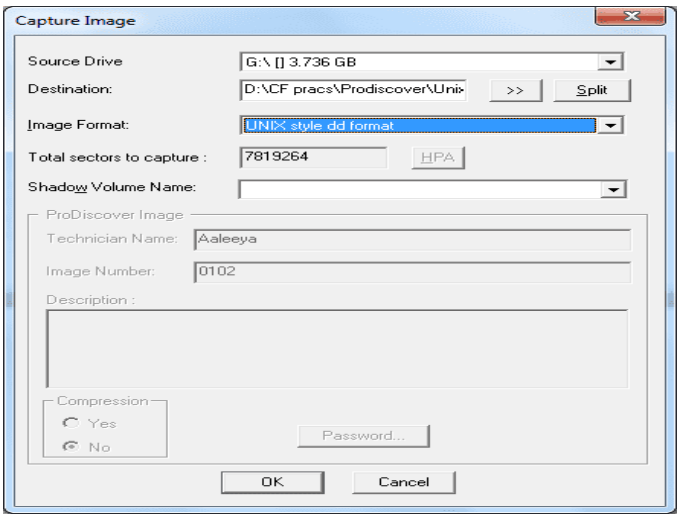
8) <u>Add a UNIX "dd" image file to a project</u>

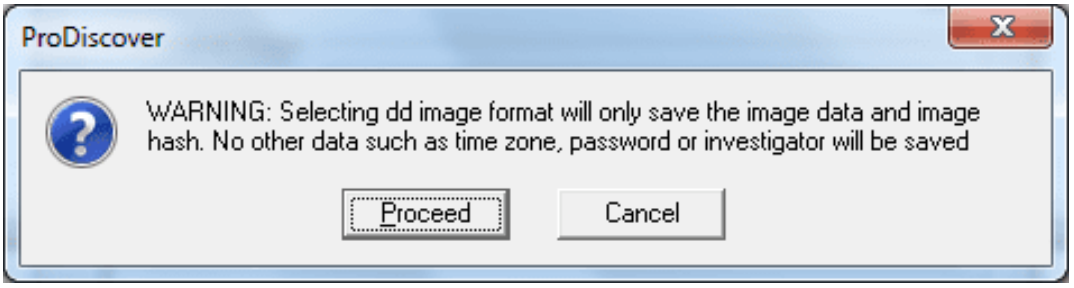
To add a UNIX "dd" image:
1. Ensure your "dd" image has the file extension ".eve".
2. Launch ProDiscover.
3. Select **open project** tab option.

To Capture Unix ”dd” image:

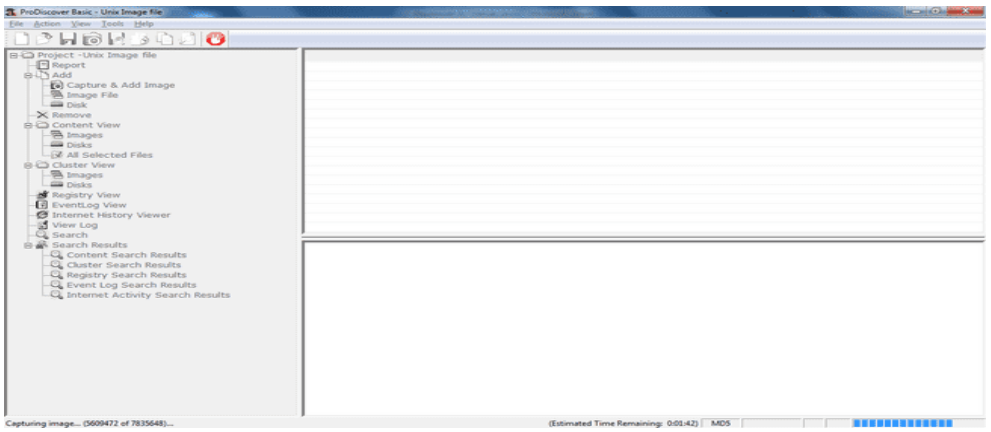


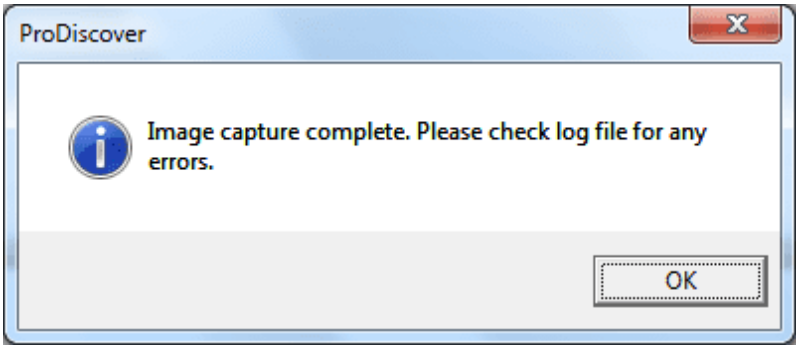


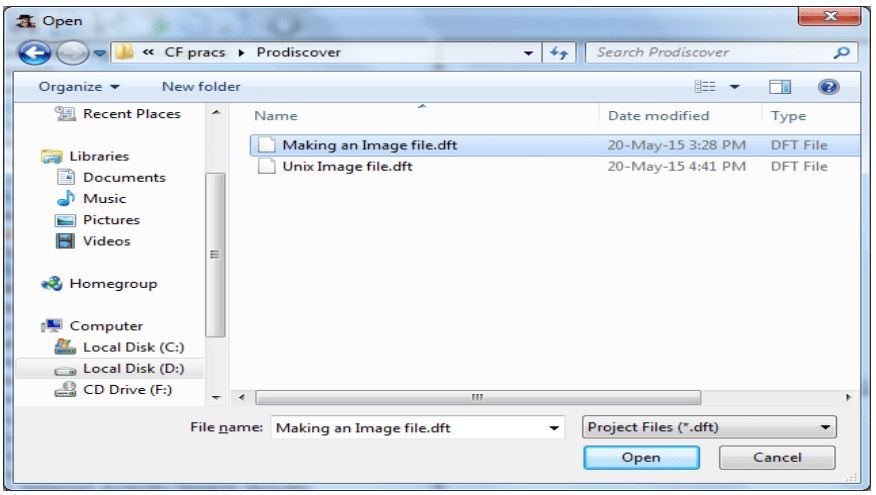




Click on Proceed



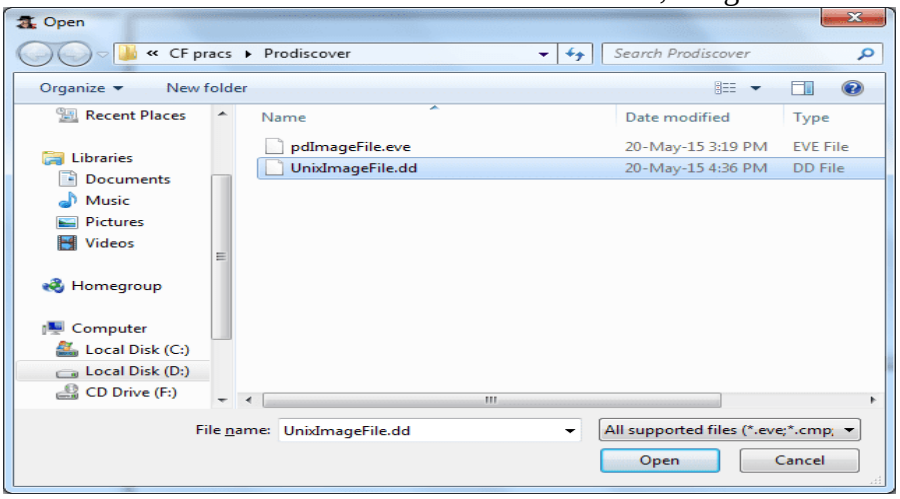




3. Select the project file to open and click **Open** button.

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

5. Select the **Add Image** option from the action menu, or tree-view. Users may also right-click on "Disks", "Images" or "Remote Drives" from Content-view to add a disk, image or remote drive to the project.



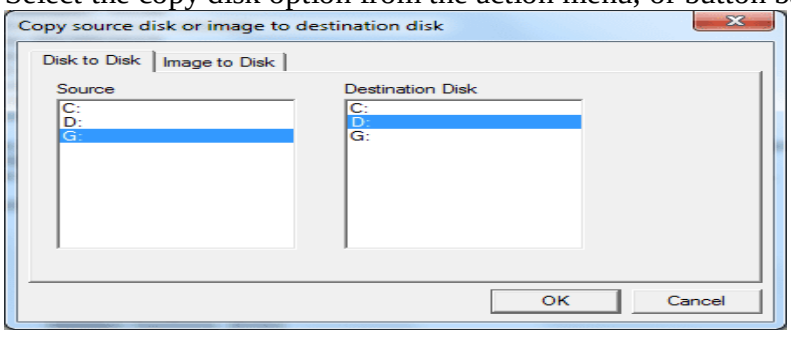
6. Select the desired image file and Click **Open** button.

7. ProDiscover then adds the image file to the currently active project.

9) <u>Copy a directly connected drive to another directly connected drive</u>

1. Ensure the desired evidence drive is attached to the installed ProDiscover system.

2. Select the copy disk option from the action menu, or button bar.

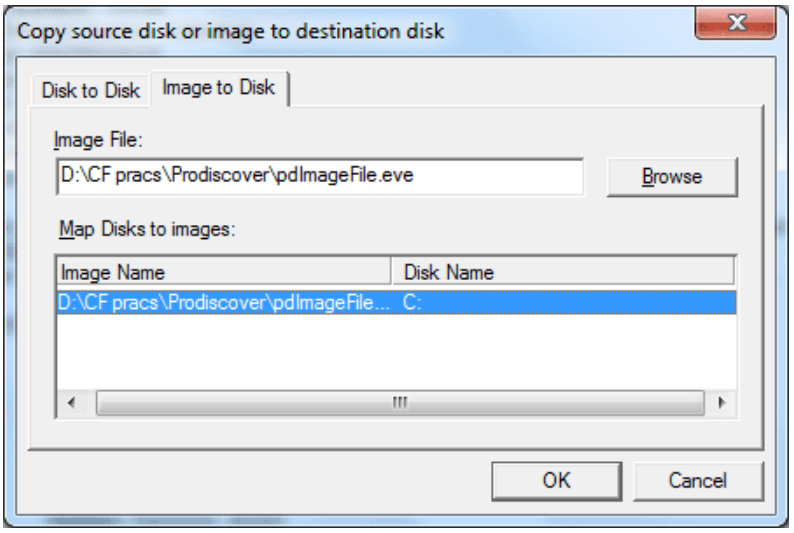


3. Select the source and destination disk, then click **OK.**
4. ProDiscover copies the source disk to the destination disk.

10) <u>Restore an Image to directly connected drive</u>

1. Ensure the desired destination drive is attached to the installed ProDiscover system and its size will accommodate the original image.

2. Select the copy disk option from the tools menu, or button bar.



3. ProDiscover presents a dialog with the list of all local drives on the system.

4. Select "**Image**" from the source section of the dialog box.

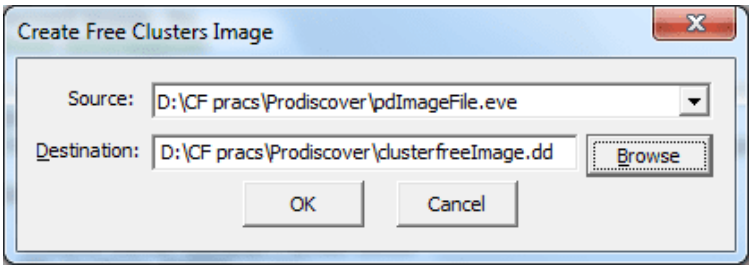
5. Select the "**Browse**" button and locate the desired image. Note: Native ProDiscover images and UNIX "dd" images can be restored.

6. Select the desired destination disk, and then click **OK.**

7. ProDiscover restores the image to the destination disk.

11) <u>Copy Selected Files</u>

In many cases you will want to recover items to another location in preparation for evidence presentation or further analysis. The "Copy Selected Files" option from the Tools Menu provides users with the ability to conduct a batch recovery/transfer of all items marked as "Evidence of Interest" by enabling the "Selected" Tag within "Content View".



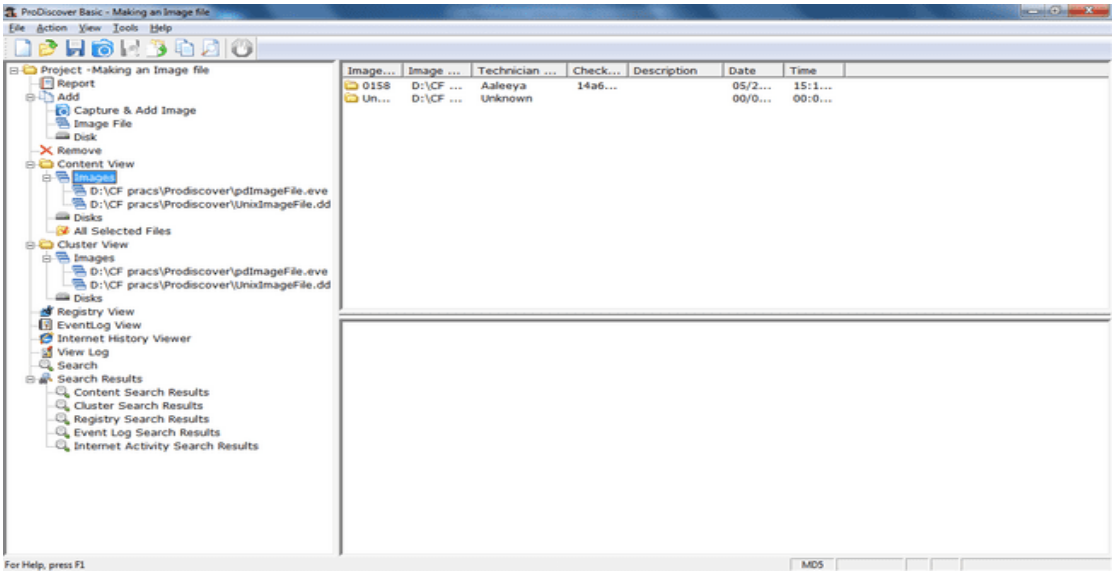
12) <u>List detail information about image files associated with a project</u>

1. Select "**Content View | Images", or "Cluster View | Images**" from the tree-view.

2. ProDiscover lists detailed information of all image files associated with a project.

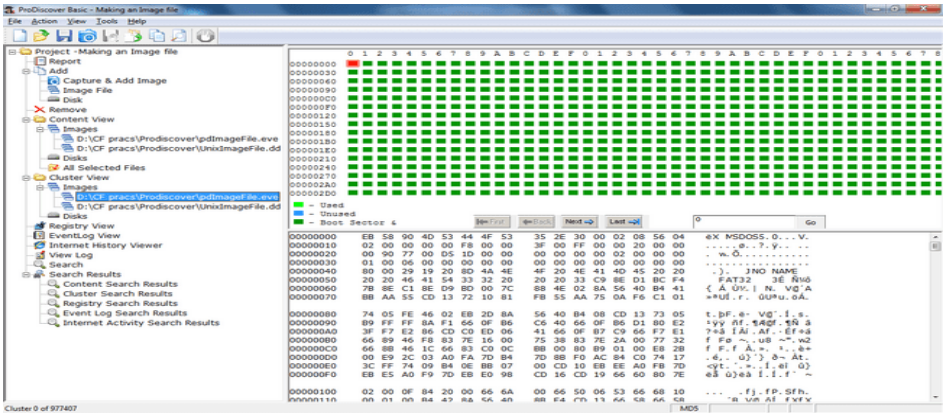
13) View the contents of a directly connected disk as files

1.Ensure the desired evidence disk is connected to the ProDiscover system and the desired disk has been added to the current project.
2. Select the "**Content View | Disks | Physical Drive | Partition**" option from the Menu or tree-view. Note: Disk containing a Hardware Protected Area will display [HPA] after a partition to indicate any file systems detected within the HPA. See Advanced tips and tricks for more information on the HPA.
3. Select the desired disk partition.
4. ProDiscover displays the contents of the disk.
5. Select a file or directory to view from the work area.
6. ProDiscover displays the contents of that file at the bottom of the main window.
7. Double click on a file.
8. ProDiscover displays the contents of the file in the default file viewer. If no viewer has been set, ProDiscover will launch an "**Open With**" dialog box asking the user to select an application to open the file.



14) View the contents of a disk, or image file as clusters

1. Select "**Cluster View | Disks, or Image | Physical Drive | Partition**" from the View Menu or tree-view. Disk containing a Hardware Protected Area will display [HPA] after a partition to indicate any file systems detected within the HPA. for more information on the HPA.
2. ProDiscover presents a graphic representation of clusters for image file, or disk in the work area.
3. Select an individual cluster.
4. ProDiscover displays the contents of that cluster at the bottom of the main window.



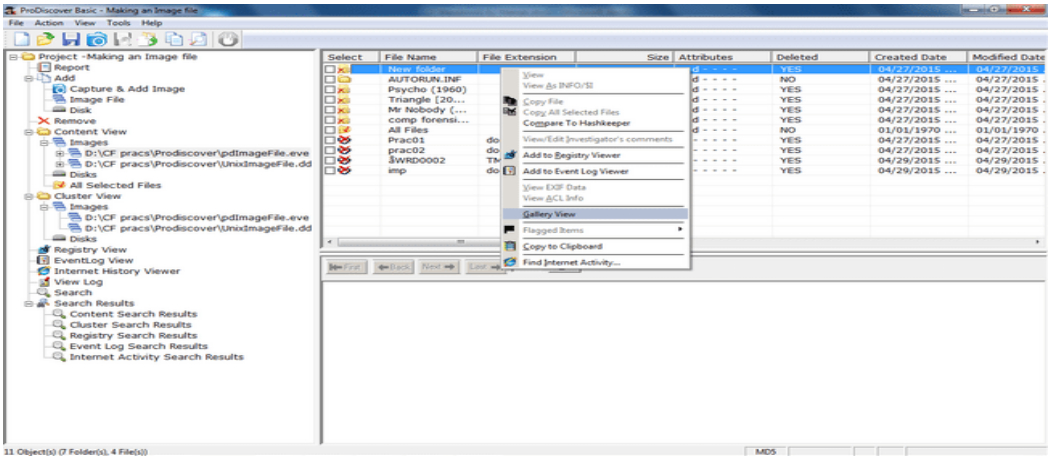
15) Viewing the Windows Event Logs (button disabled in demo version)

16) View Windows Registry

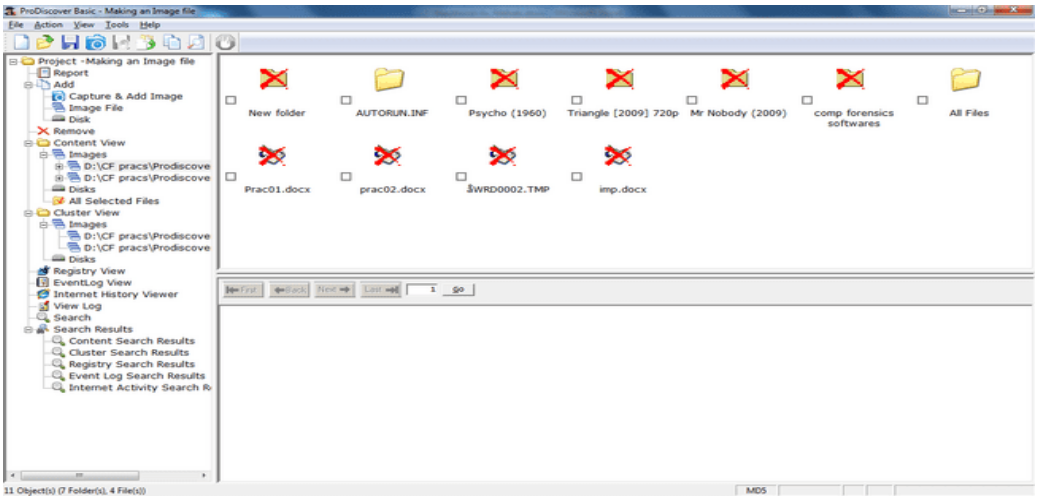
17) Search the Windows Registry

18) View Graphic Files in Gallery View

In situations where users need to view the contents of a large number of graphic files in a given directory ProDiscover offers a "Gallery View" function. To shift into a gallery view mode users need only choose the "Gallery View" menu option from the "View" menu or right click over the work area as seen below



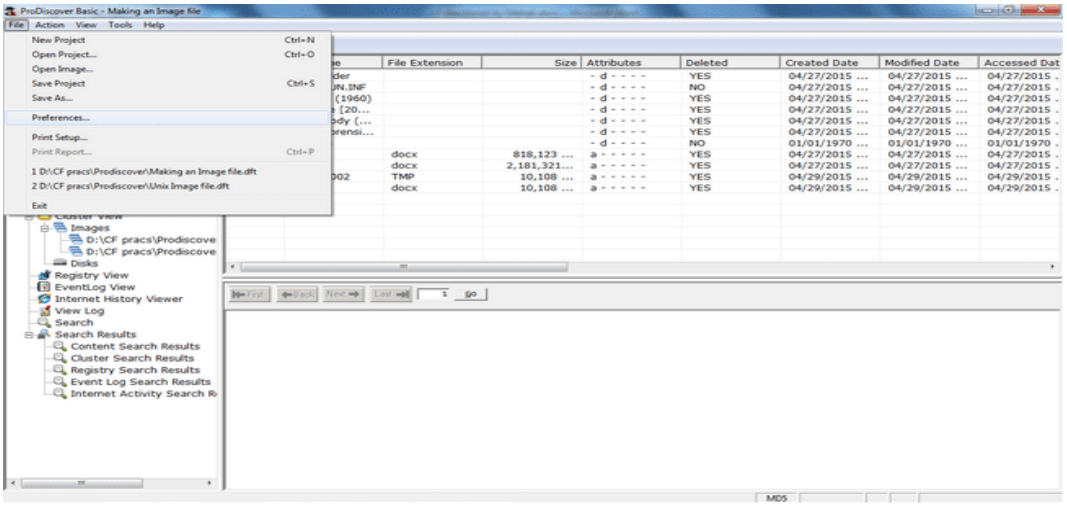
Once the user selects "Gallery View" the work area view will display a thumbnail of all images within the selected directory as seen below.

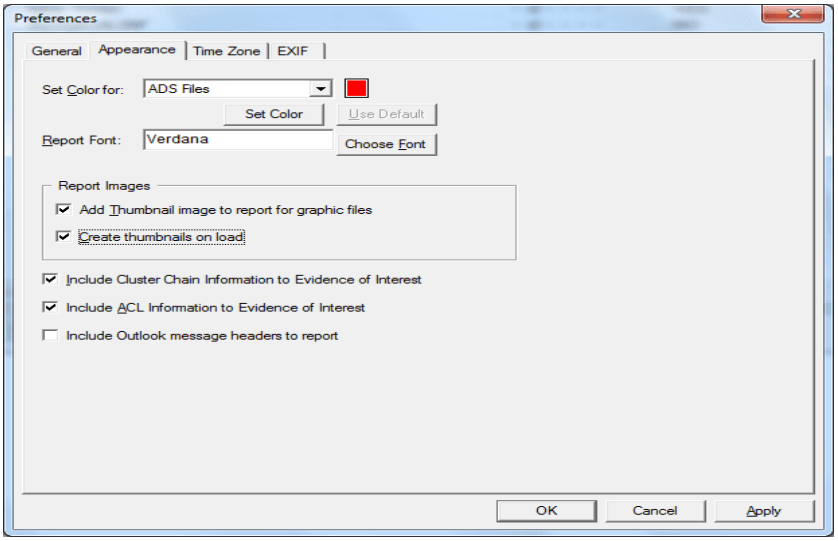


19) Adding Thumbnail Images to Report for Graphic Evidence

Users may desire to add preview thumbnail images along with information provided to the standard project report. To add graphic thumbnail preview images users should use the "Appearance" tab of the "Preferences" File menu option. In the appearance section users will find the following two options:
"**Add thumbnail image to report for graphic files**" (default unchecked) when checked will cause a thumbnail image to be created and added to the report for any graphic file which is selected as evidence of interest. For users who choose this option after graphic files have been added as evidence of interest they can use the Action menu's "Create report thumbnails" option to add thumbnails to the report.
"**Create thumbnails on load**" (default unchecked) when checked causes ProDiscover to automatically add thumbnail images to the report when opened. Warning: a large report, with many graphic files selected as evidence of interest, can cause a significant delay while loading a project file.

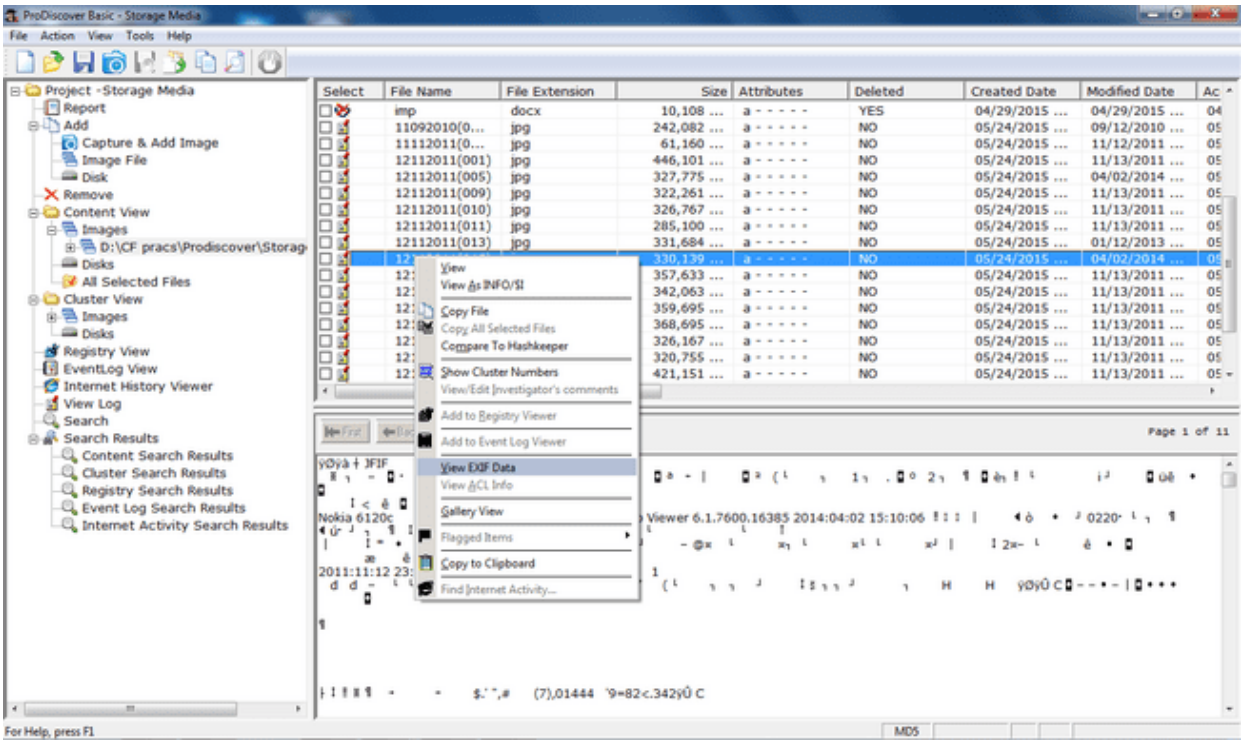
After choosing the desired settings thumbnail images will be added to the live ProDiscover project report (as seen below) as well as any report that is exported in the RTF format.



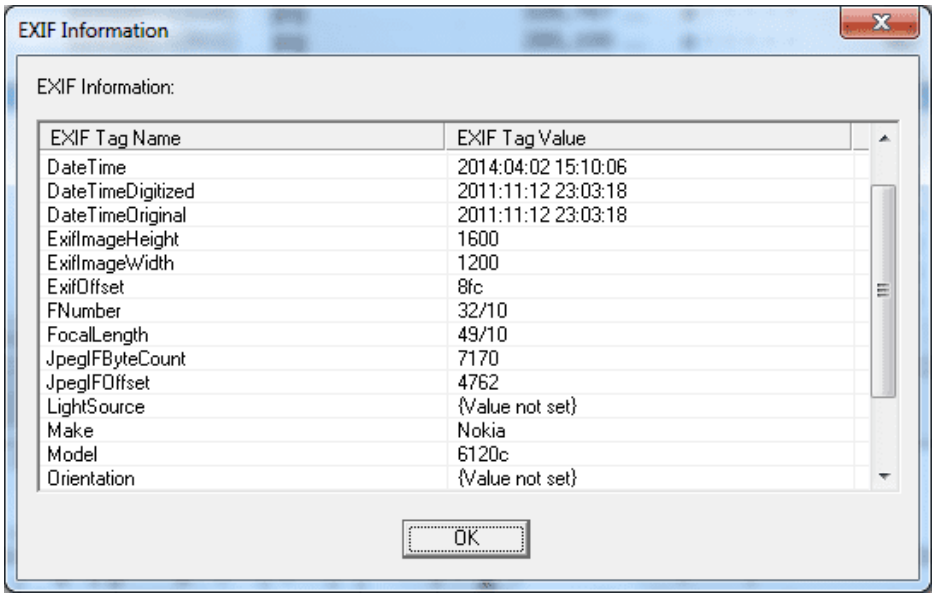


20) View Image EXIF Meta Data

Step 1) To view the EXIF meta data of a JPG or TIF file in ProDiscover simply right-click on any .jpg or .tif graphic file from content-view and select "View EXIF data" as seen below.



Step 2) After choosing to view EXIF Data, users are shown a dialog box containing all available EXIF meta data as seen below.



In the user preferences "EXIF" tab, users have the ability to select if they want EXIF meta data added to the report when selecting (selected tag enabled) graphics files as evidence.

21) Recover a Deleted File

1. Ensure the desired evidence disk is connected to the ProDiscover system.

2. Select the "**Content View | Disk, or Image**" option from the Menu or tree-view.

3. ProDiscover displays a list of drives, or images available to the system.

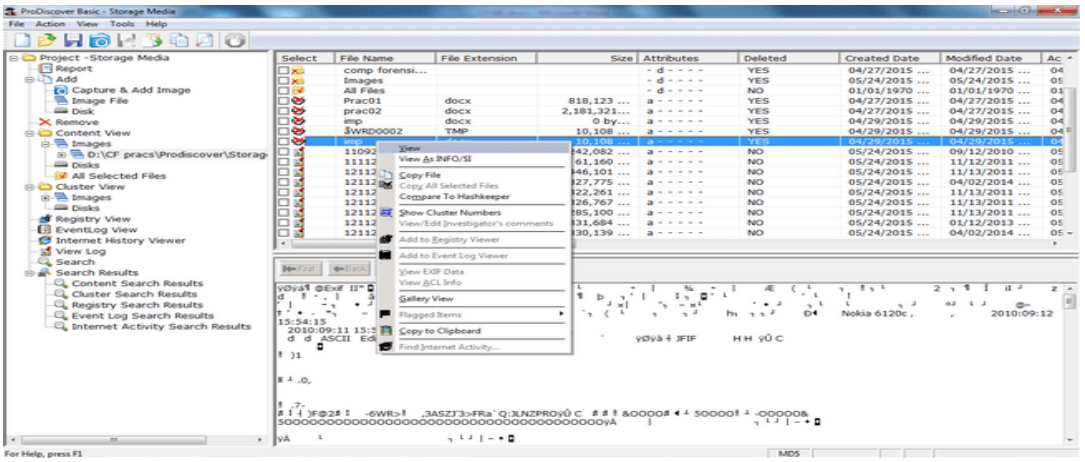
4. Select the desired disk, or image and navigate to the desired volume.

5. ProDiscover displays the contents of the disk.

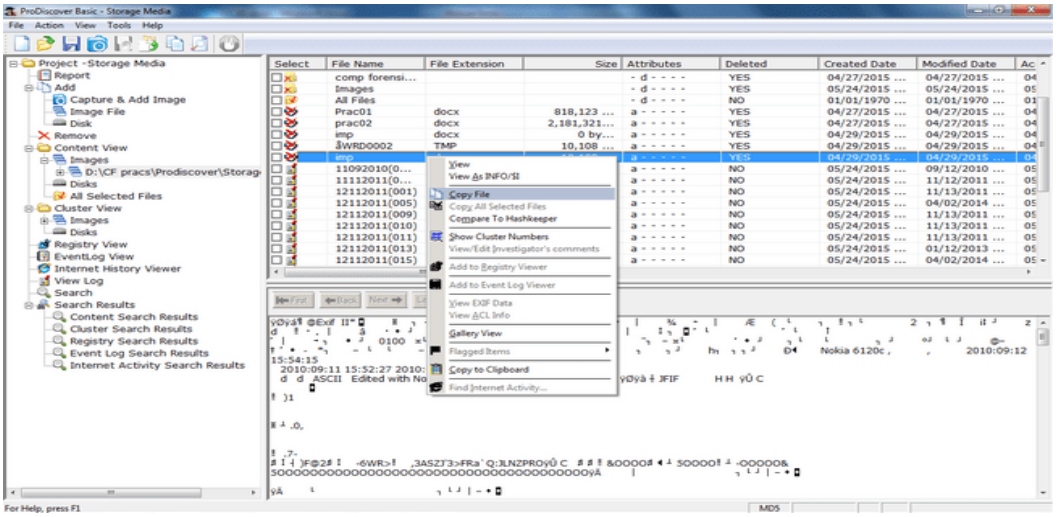
6. Select a file to recover from the work area.

Notes: The "Deleted" column will display "Yes" if the file has been deleted. On NTFS formatted drives, ProDiscover collects all deleted files into a special directory called "Deleted Files". The contents of a recovered file can never be guaranteed since some clusters may have been overwritten.

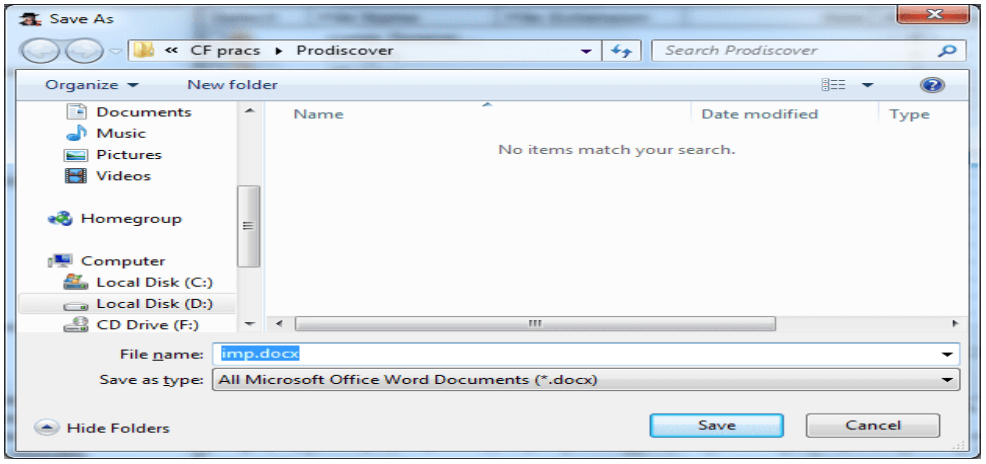
7. ProDiscover displays the contents of the selected file at the bottom of the main window. **Right click** on a file.

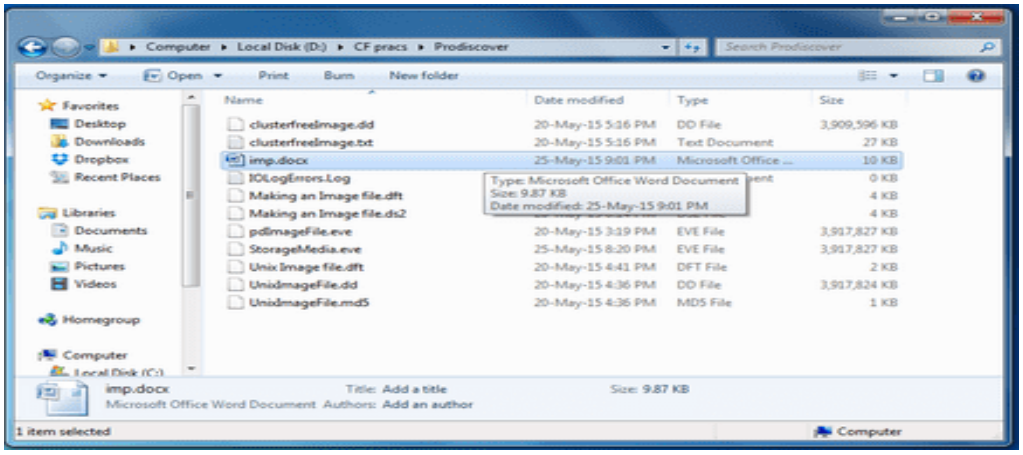


8. In ProDiscover a pop-up dialog with the choice to View or Recover the selected file. Select **Copy File.**



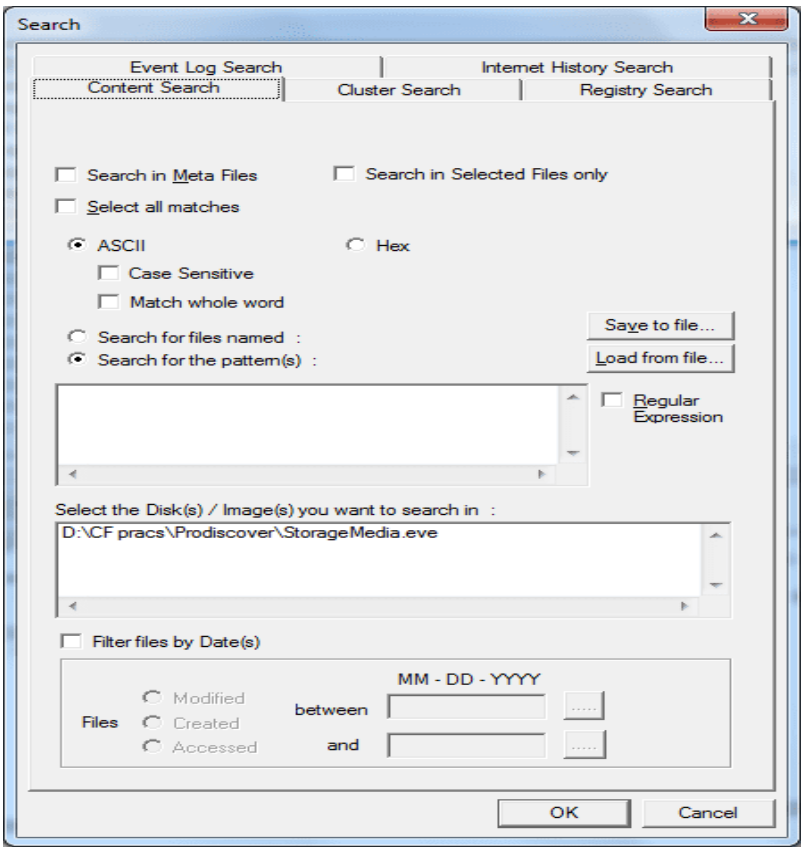
9. Enter the desired location and file name to save the file as in the "Save As" dialog box that appears and click "**Save**".



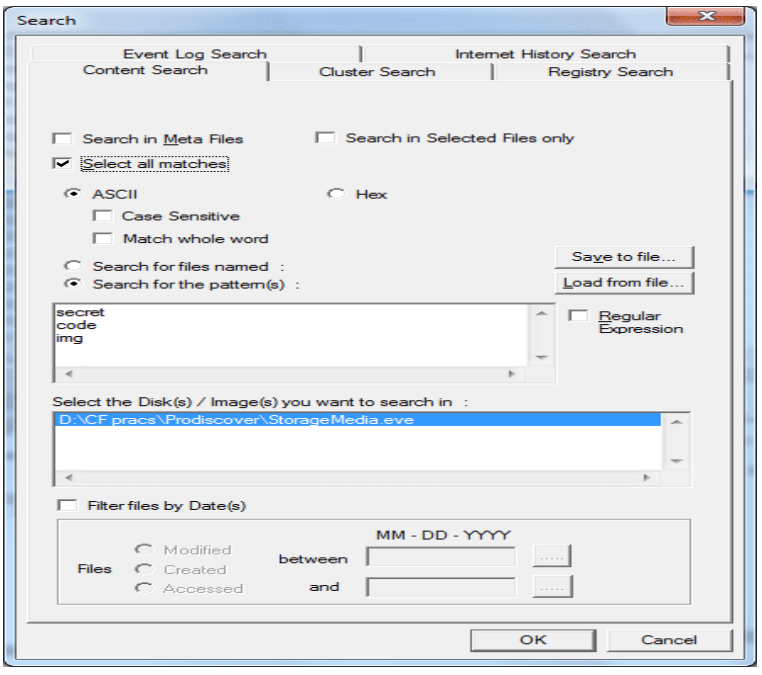


22) Search for keywords in image file or disk

Step 1) From the current project select search option from the tree-view, or button bar. ProDiscover displays search dialog.

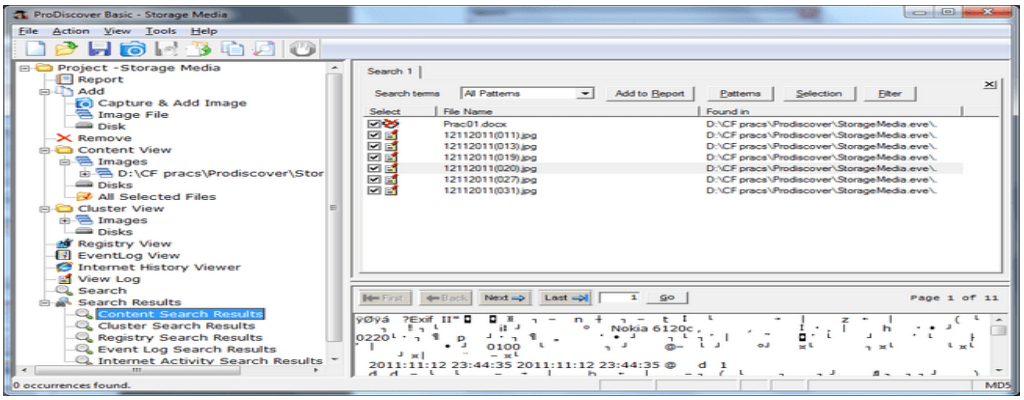


Step 2) Choose the type of search to be conducted (Content or Cluster).
Step 3).If conducting a content search choose "Search in Selected Files only" to search in only files selected as evidence if desired.
Step 4).Checking the "Select all matches" checkbox will automatically add all files from the search result to the project report as evidence of interest. Files marked as evidence of interest can be easily copied to review disks using the "copy selected files" option from the tools menu.
Step 5) If conducting a content search choose to search for file names or content.

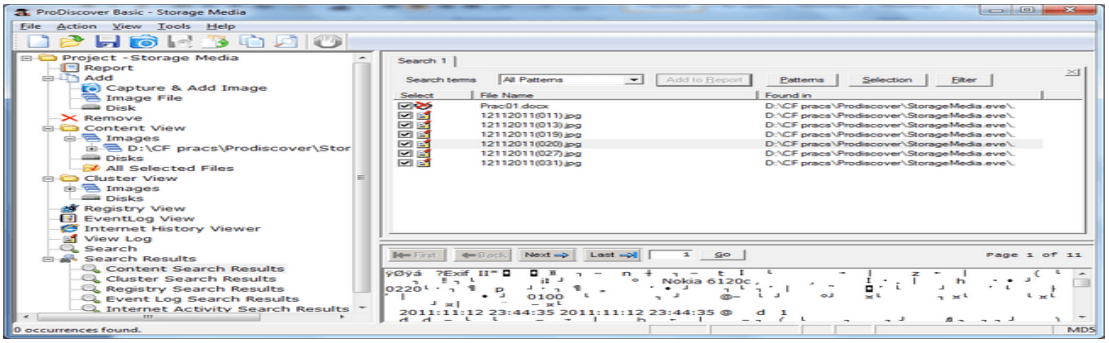


Step 6) Enter the keywords (one on each line) in the search for window and select the image files or disks to be searched. Full Boolean Logic (AND, OR, NOT) can be used, but must be capitalized.

List of keywords can be saved in an ASCII text file with the extension .STS and loaded using the "Load from file..." button.
Step 7) Users may also select to filter Content Searches by Modified, Accessed, or Created dates.
Step 8) Click the "Search Now" button.
Step 9) Results obtained from the search will be displayed in the top work area as selectable objects. When any object is highlighted the resulting search term will be highlighted in the data view area. Search results are saved from session to session in a file with the same project name and the extension .ds2

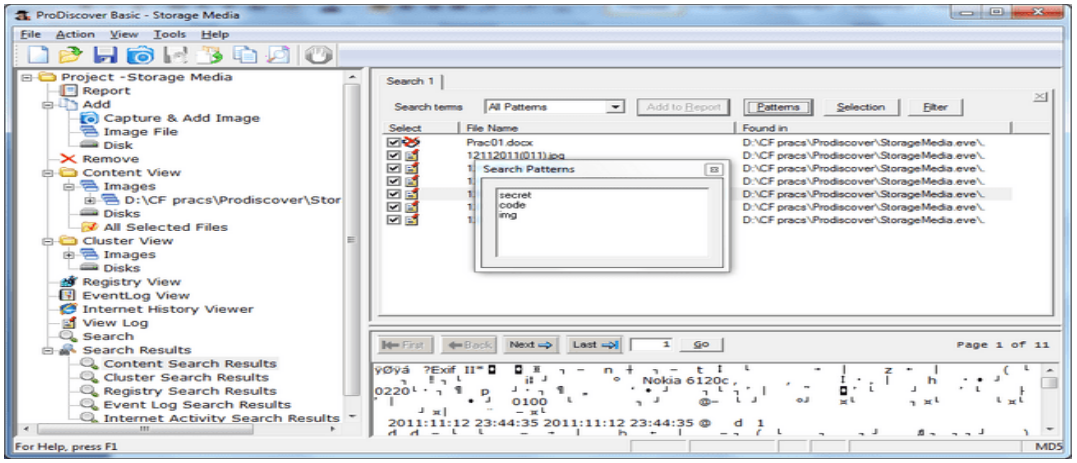


Step 10) If the search results are satisfactory they can be added to the current projects report with the "Add to Report" button.



Step 11) The "Search terms" drop-down box allows users to highlight only a single search term from the original search term list if desired.

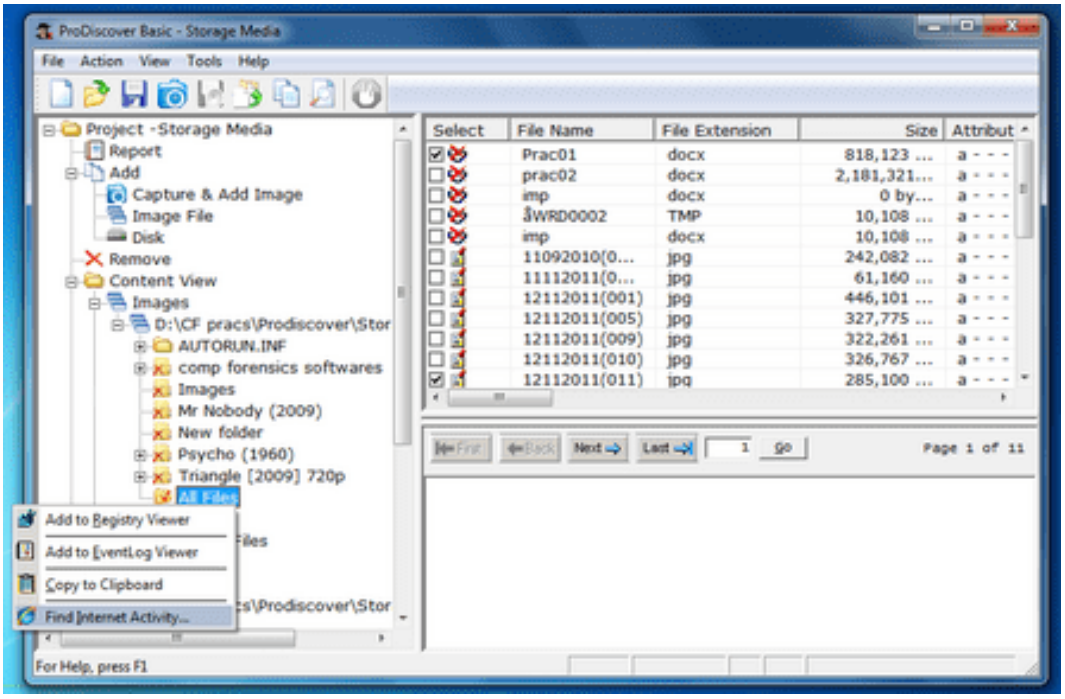
Step 12) The "Patterns" button will display a pop-up window containing the original search terms used in the search set including any Boolean operators used.



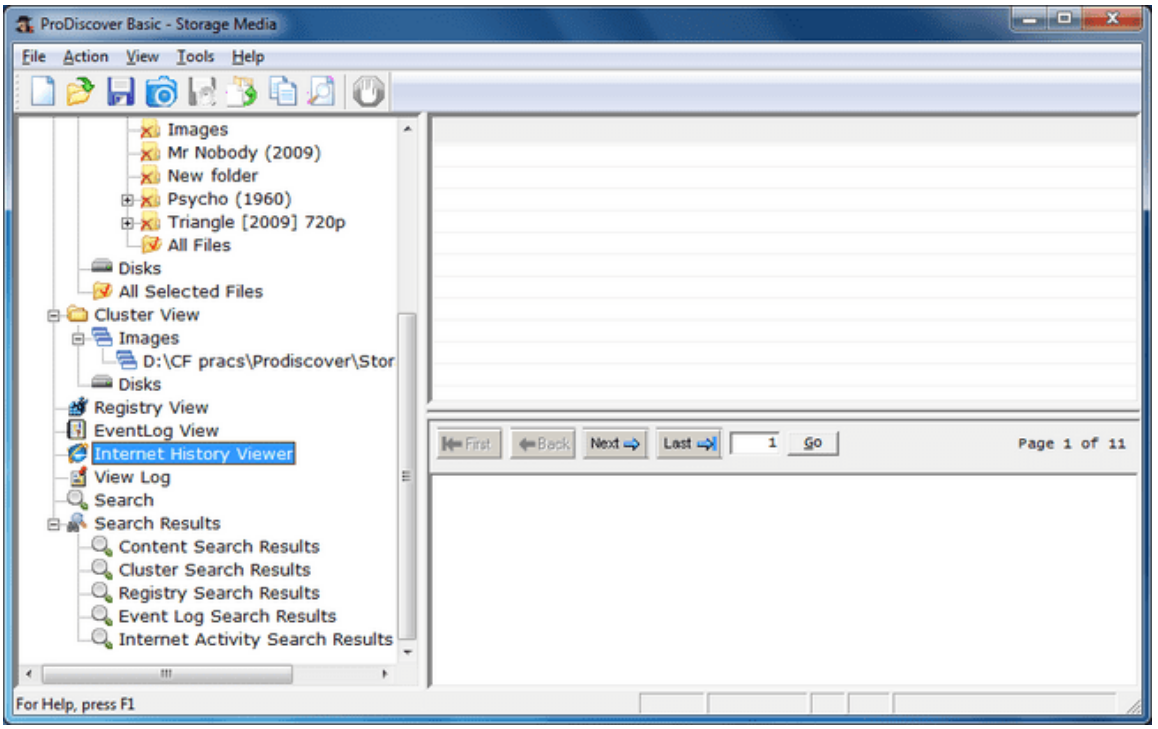
23) Extracting Internet History

Information about a users Internet Web surfing habits is often crucial to investigations. ProDiscover allows investigators to quickly search for, and extract information from Internet Explorer history files (index.dat). Once the information is extracted it is automatically added to the project report.

Step 1) Searching for and extracting the Internet history from a directly added disk or image is as simple as rightclicking on the desired directory structure and choosing "Find Internet Activity...".



Step 2) Once complete the Internet History Viewer found in the tree-view will be populated with the contents of each index.dat file created by Internet Explorer. Once added to the Internet History Viewer this information can be searched and added to the project report on an entry-by-entry basis.



Practical 07

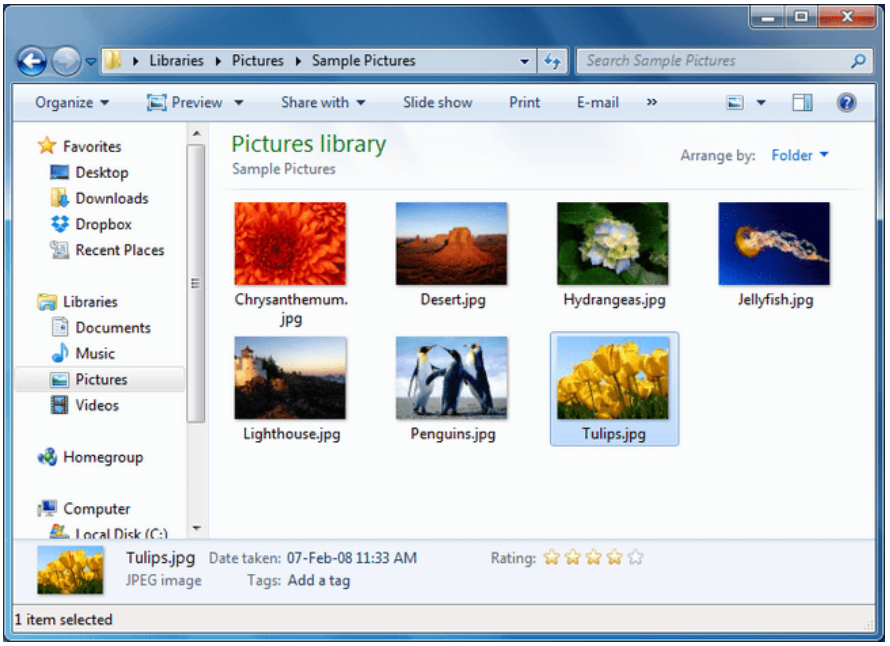
Using Steganography tools

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.



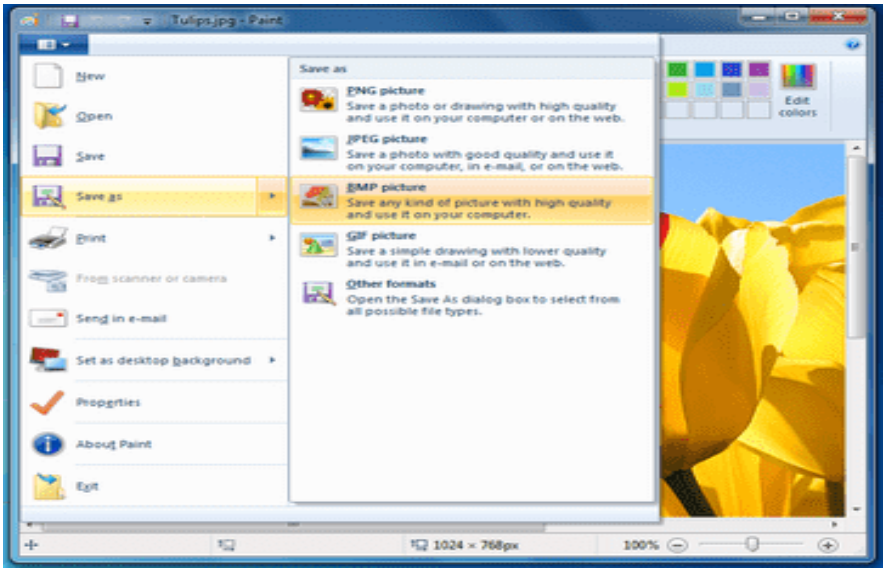
The S-Tools program is a drag and drop software. The files used to create the steganography file can be dragged from the directory into the S-Tools program.

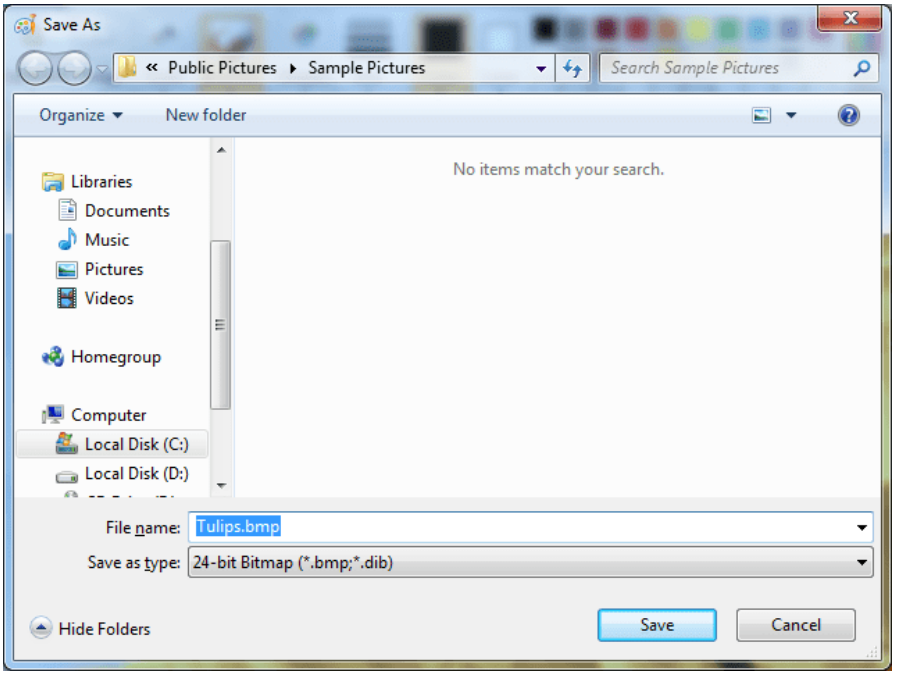
Step 3) Select the file from the directory and drag it over the S-Tools main window and release the file.

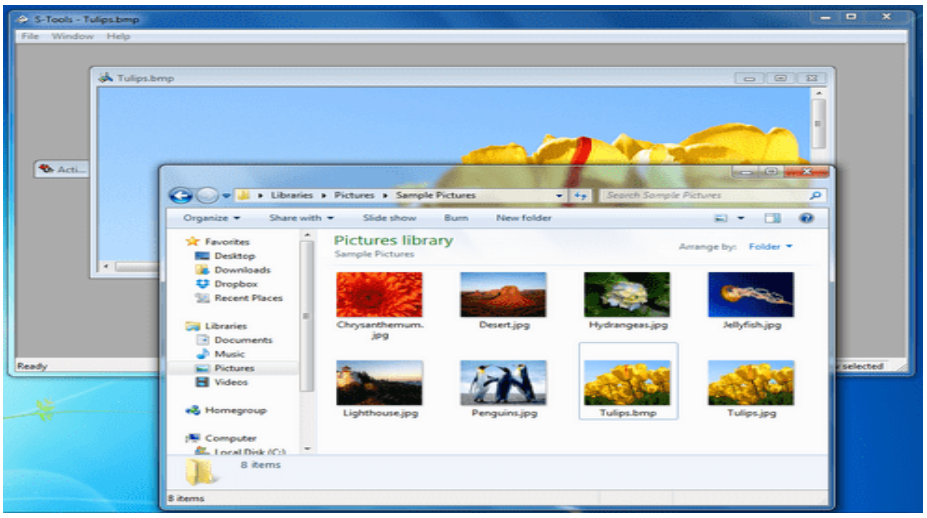
A dialogue box appears indicating that the file type is unknown. Supported file types for audio and image files are shown below:

- 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:

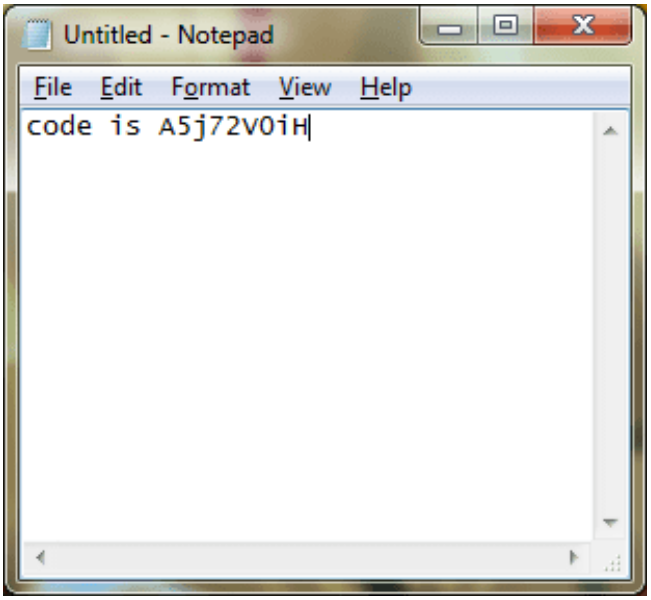


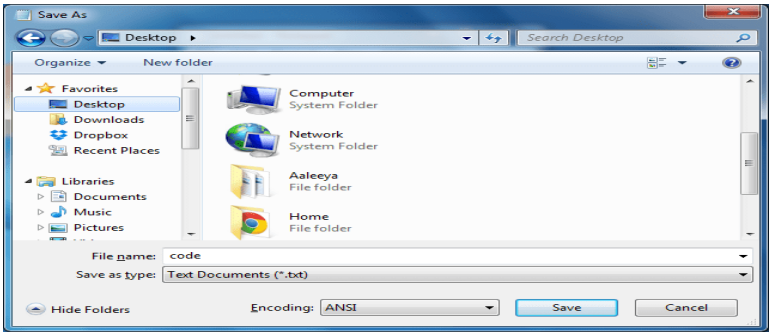


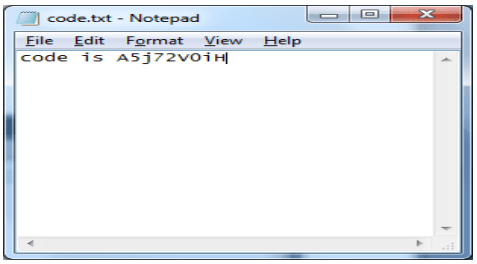


Step 4) Select a valid audio file or image as the base file for the steganography file. The Tulips.bmp was selected and dragged onto the main window of the S-Tools program. The image is opened.

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

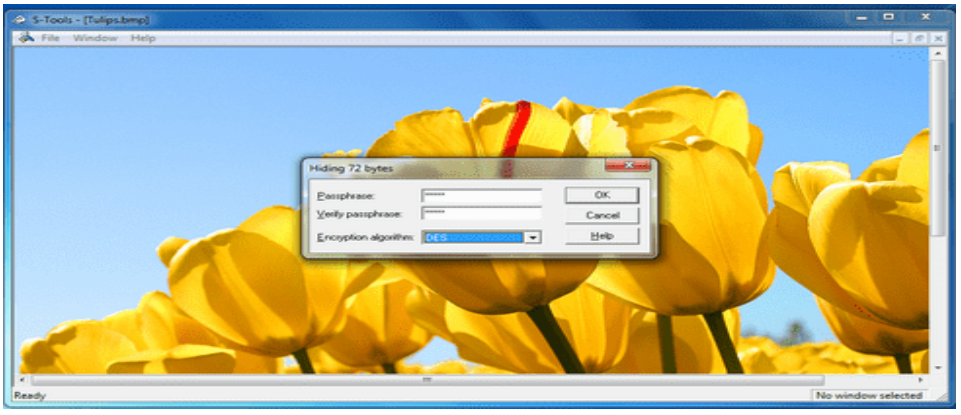






Step 6) The *.txt text file is selected and dragged on top of the base image. Release the file while the cursor is still on top of the base file.

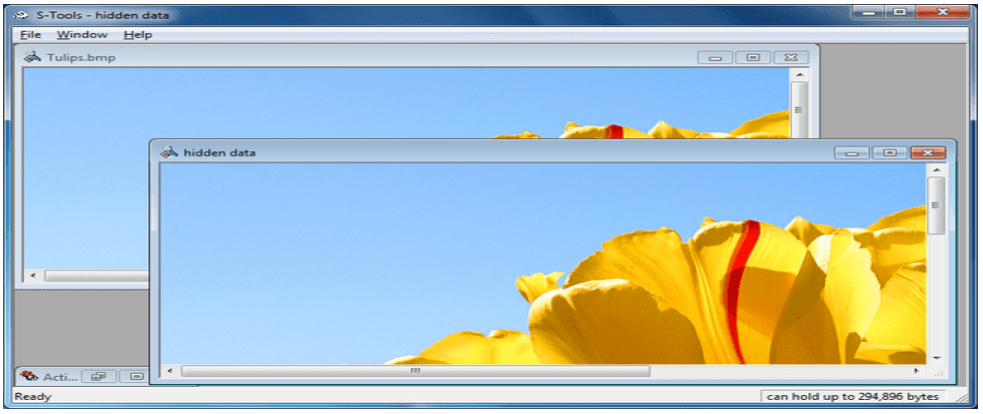
Step 7) A dialogue box will appear asking the user to enter and verify a passphrase. Additionally, the user will have to select an encryption algorithm.



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.

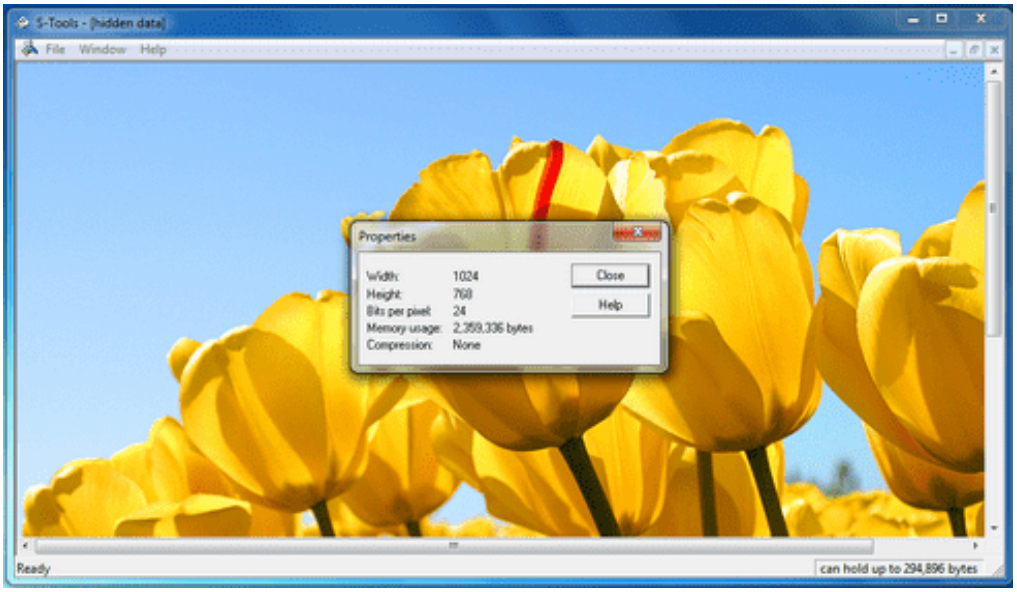


Step 11) Place the cursor on top of the hidden data image and select the right mouse button. The user will have four options available to them:

- Save
- Save As
- Properties
- Reveal

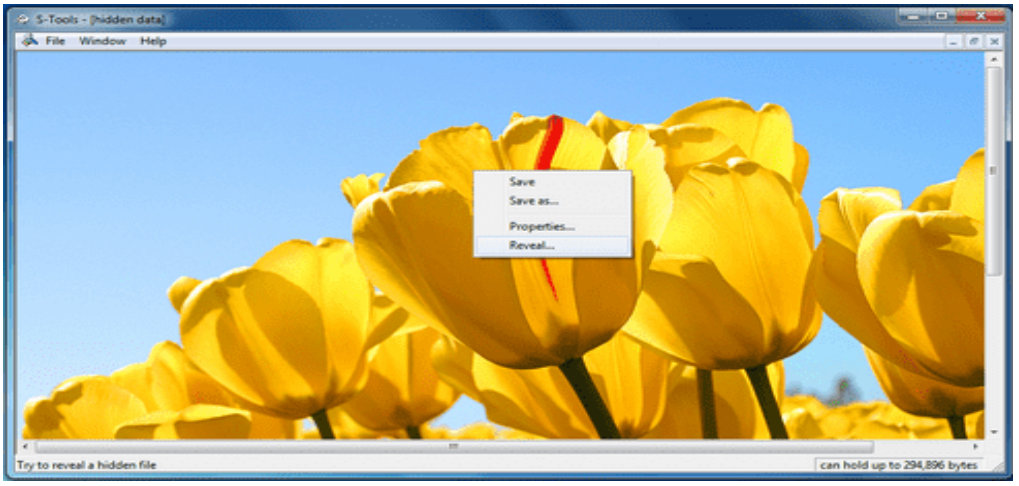
Step 12) Selecting the 'Properties' button while the cursor is over any image will display the following properties:

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

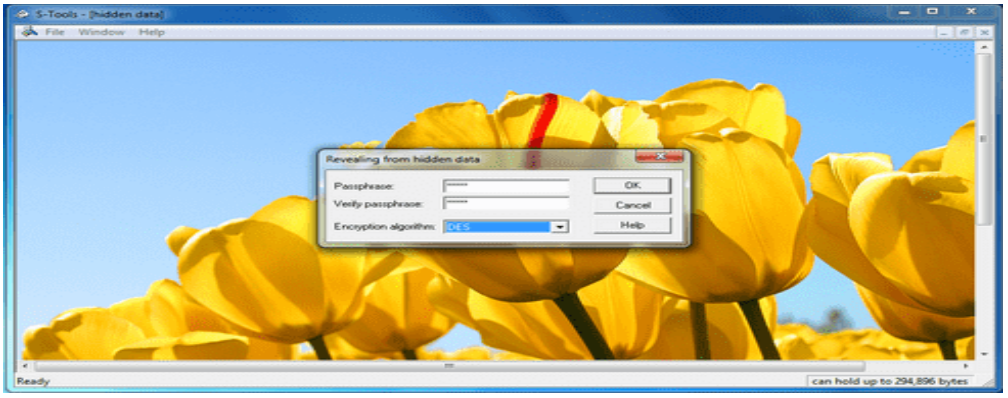


Step 13) Selecting the 'Reveal' button will display a passphrase dialogue box. A passphrase must be entered twice in the dialogue box and the correct encryption algorithm must be selected.

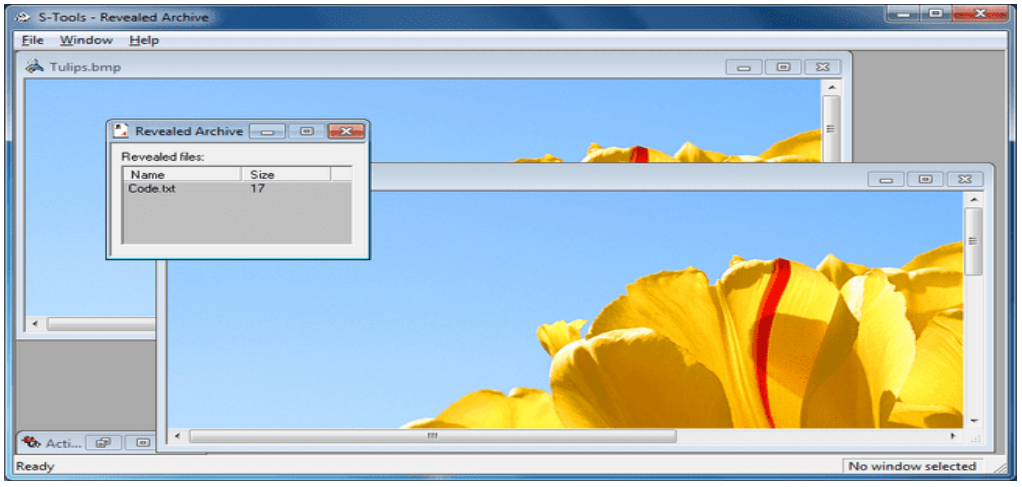
Notice that the title of the dialogue box has changed to 'Revealing from Tulips.bmp'



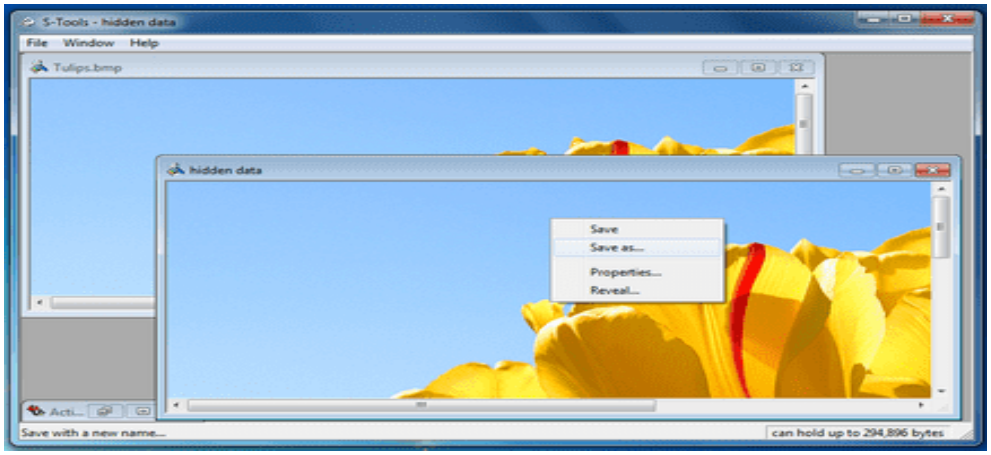
Step 14) Enter a passphrase twice, select the encryption algorithm, and select the ‘OK’ button.



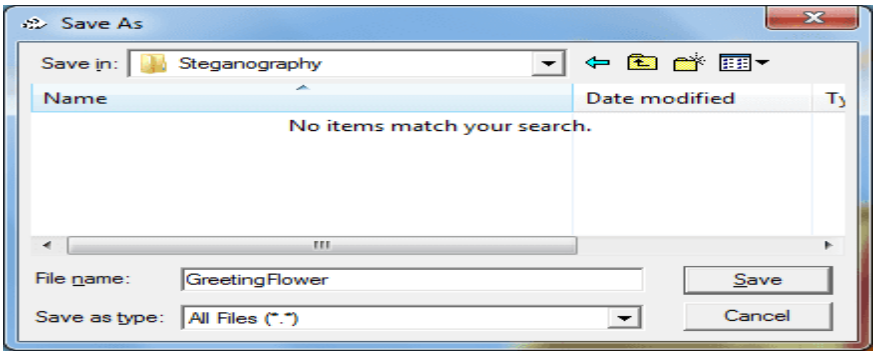
Step 15) A ‘Revealed Archive’ dialogue box will display which contains the file name and size of the hidden file.



Step 16) Select the ‘Save As’ button.

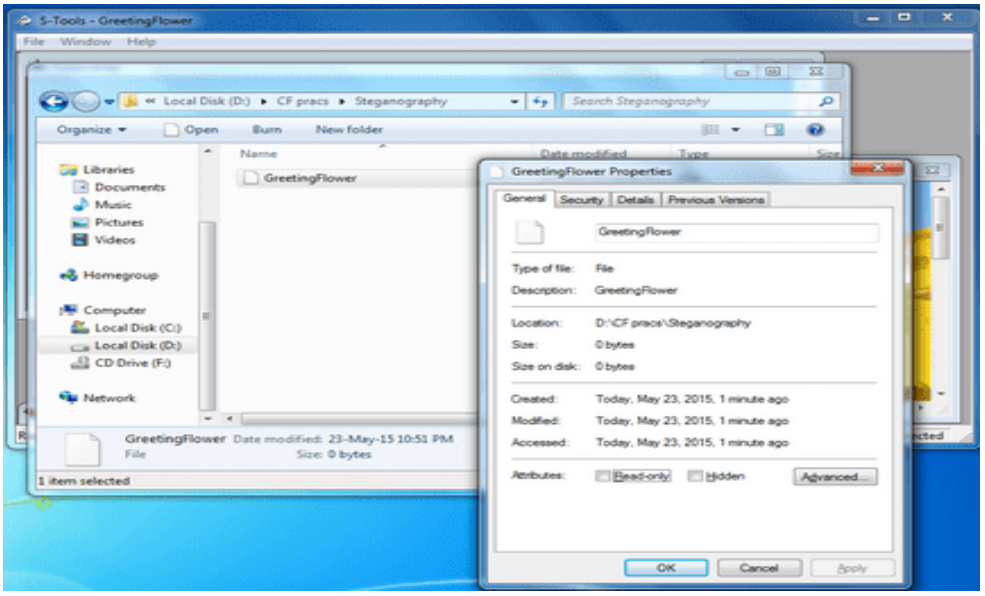


Step 17) A ‘Save As’ dialogue box will appear. Enter a valid file name, select the working directory and select the ‘Save’ button.



Step 18) Locate the files in the working directory.

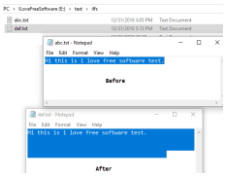
Step 19) Open the files using a multimedia software program and ensure that the files were extracted from the steganography file successfully.



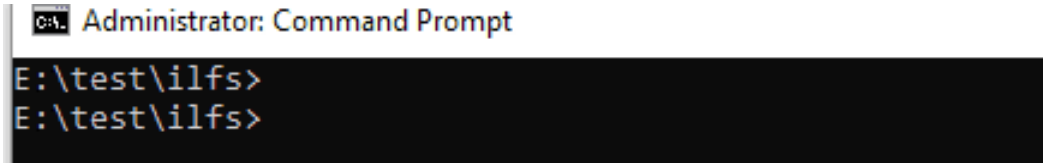
B. Using Whitespace Steganography Tool SNOW

Snow is a free steganography tool to hide message in text using white spaces. It takes a files from you and then hide the specified message after encrypting it using a password that you specify. You can hide any message in any text file and then simply retrieve it in an easy way. After hiding sensitive information in a text file, you can send that to any user via email or file sharing services and then don't worry about if someone steals the information as the message is encrypted.

There are many Steganography software that you can use to hide messages in videos, text, and images. And the normal steganography software hide the data in the bits of data of the source. But if you want to try a unique steganography tool then use Snow. Here it has a strong algorithm that uses white spaces to hide the message in a text file. Before encoding text in a file, it analyzes the file as well and displays the amount of white spaces that needs to be added. After that, just run single command and you are done hiding message in text.



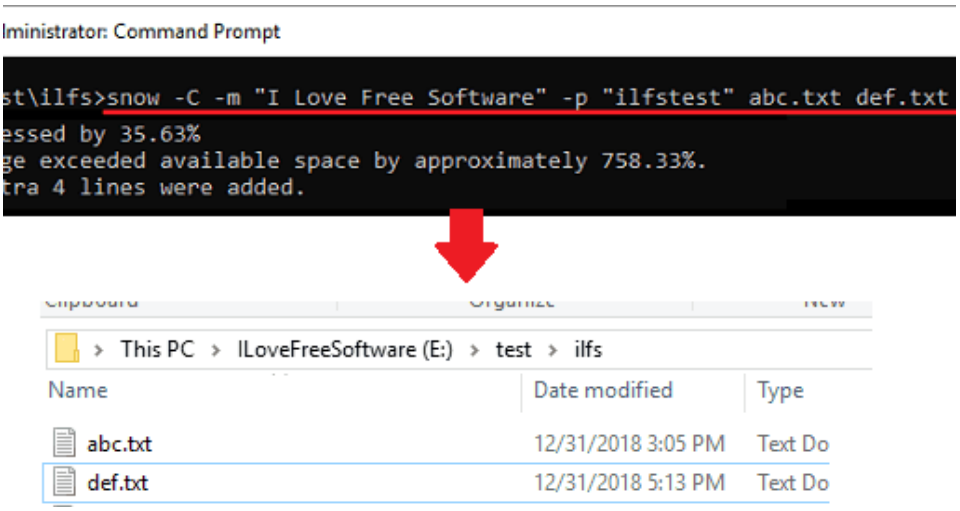
Download the binary EXE file of Snow and then extract the ZIP file and put the SNOW.exe file in "C:/Windows" folder. After that, open a command prompt window and point it to the path where the text file is in which the text is to be hidden.



open command prompt in the files directory

Now, simply run the command in this syntax to hide a message. After hiding a message, it will create a new text file that you specify corresponding to the "Outfile" parameter.

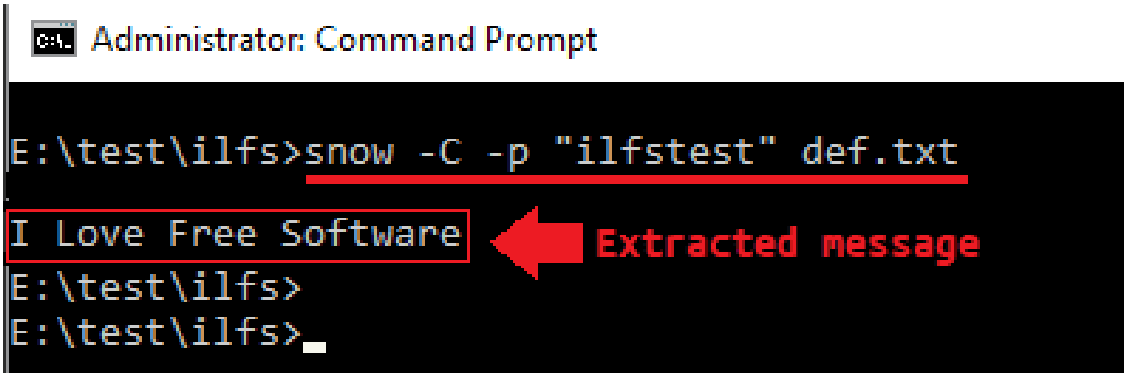
snow -C -m "MessageToHide" -p "Password" "InputTextFile" "OutputTextFile"



snow hide message in text

To extract hidden message from the text file that you created earlier, simply run this command. This will reveal the message which is hidden inside the text file you have created.

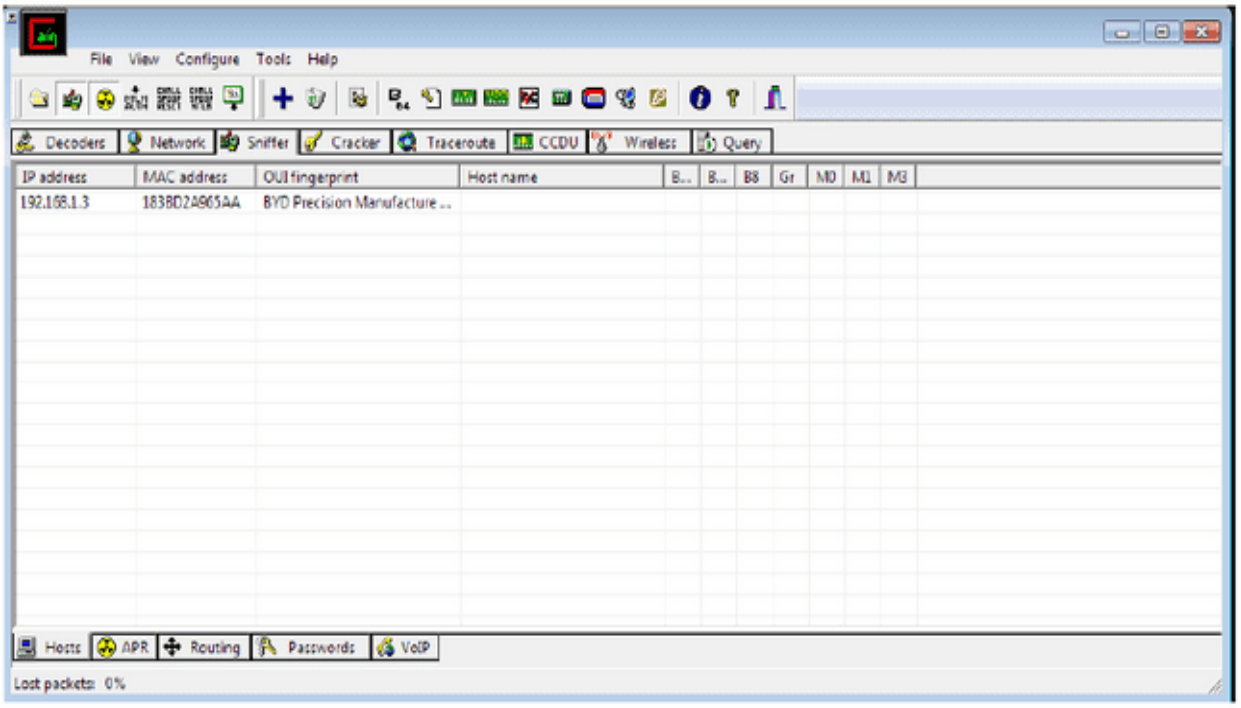
snow -C -p “Password” “OutputTextFile”



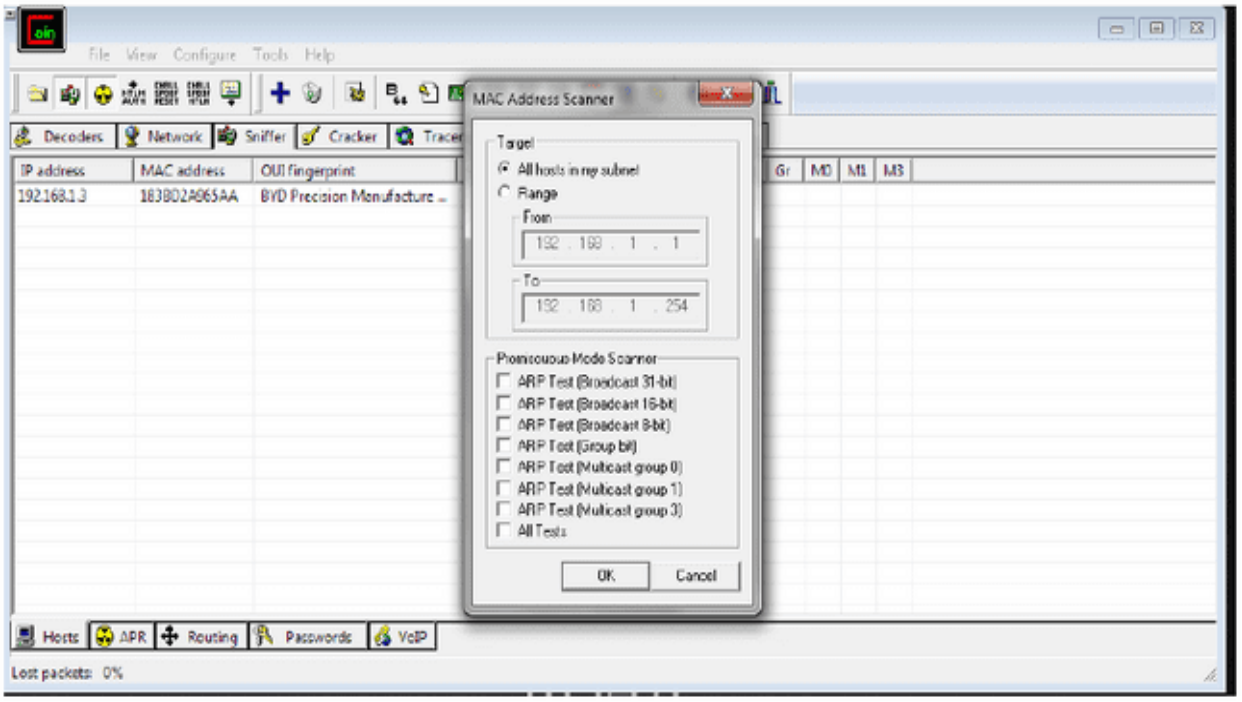
Practical 08

Aim: Performing Sniffing [Cain & Abel]

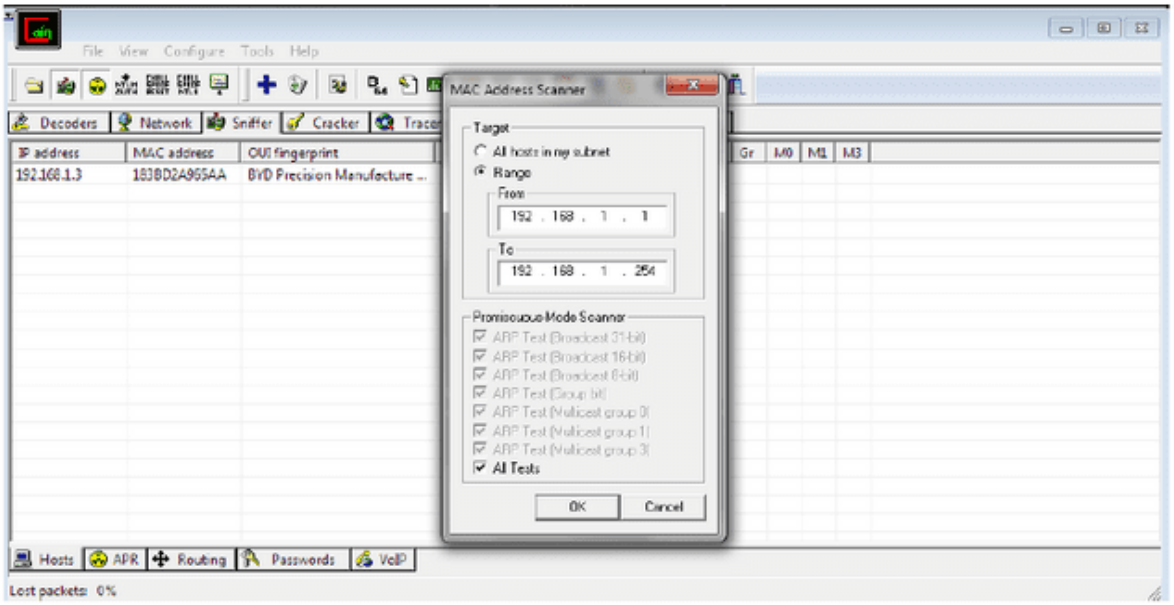
Step 1: It displays the hosts with the ip address.

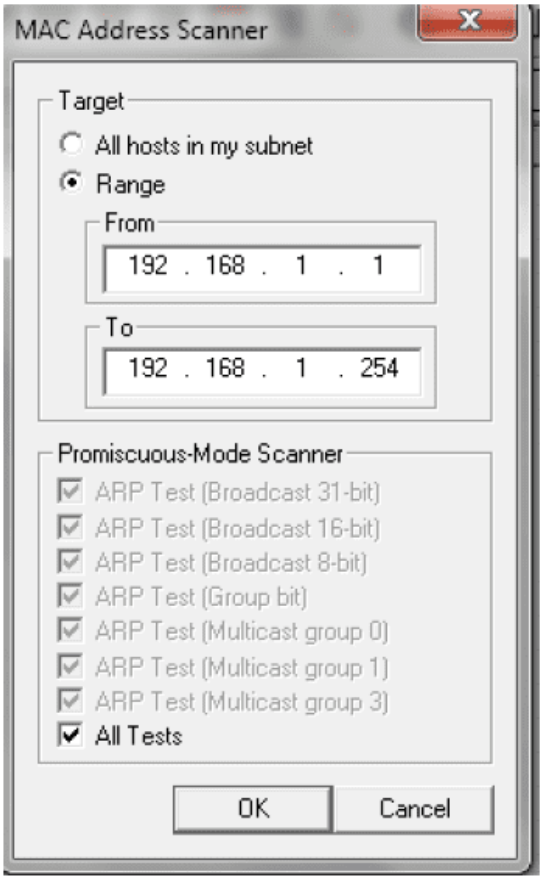


Step 2: Click on start/stop APR option and click on Add button (+).

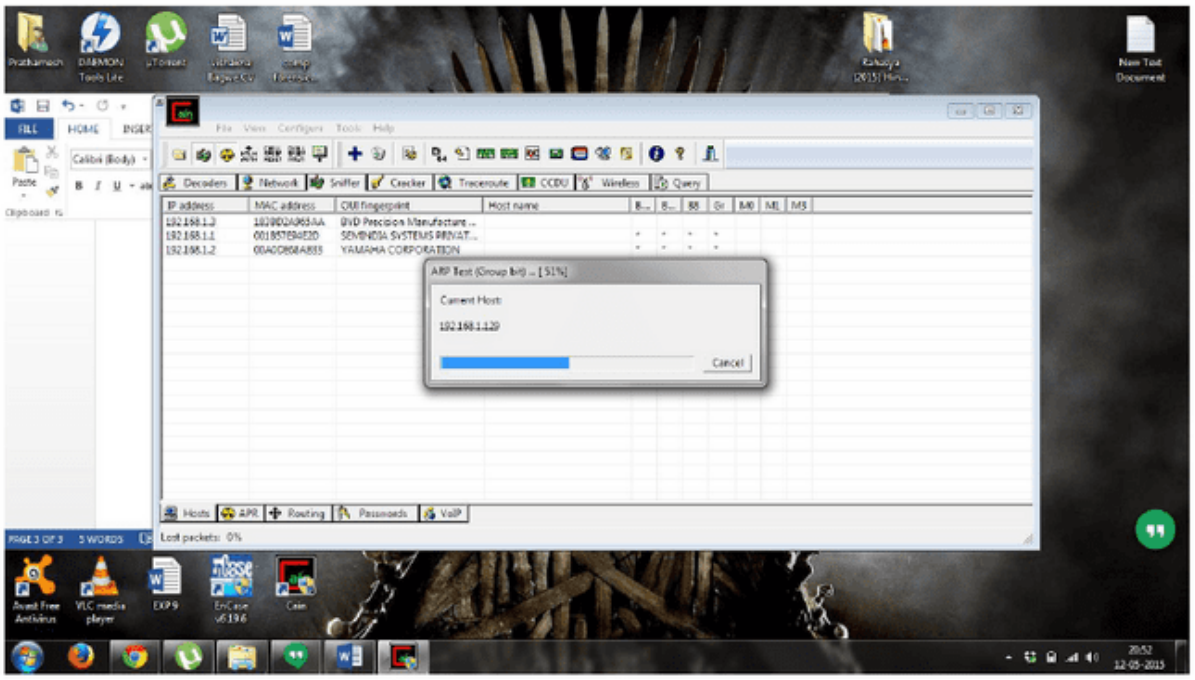


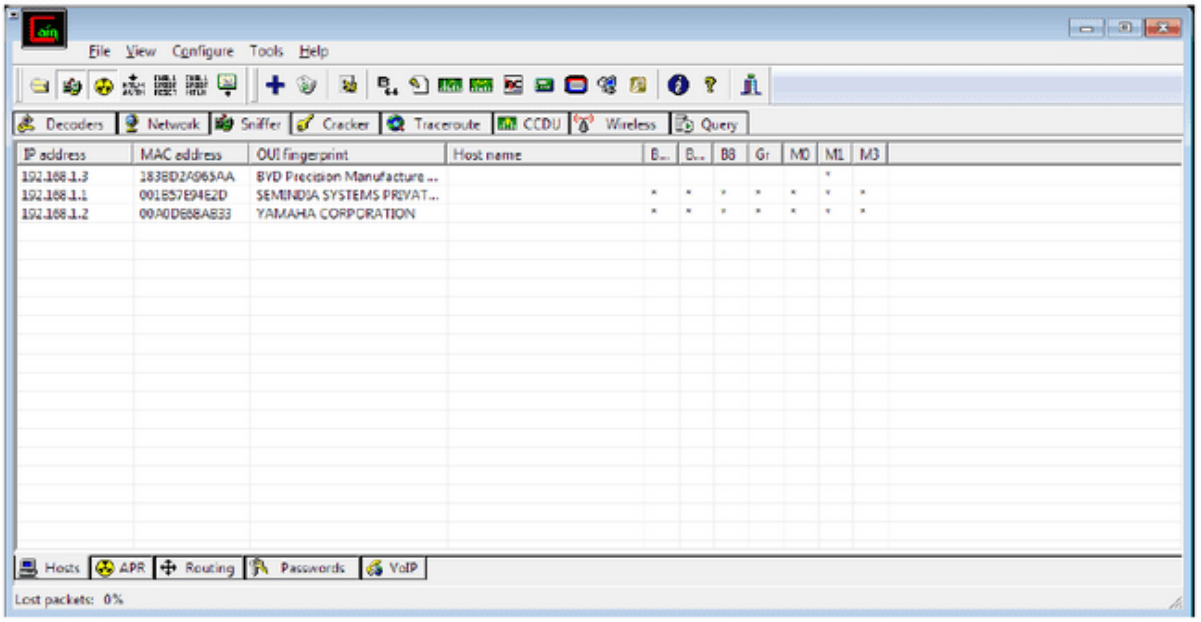
Step 3: It displays the range of IP address. Select “All Tests”. Click OK.



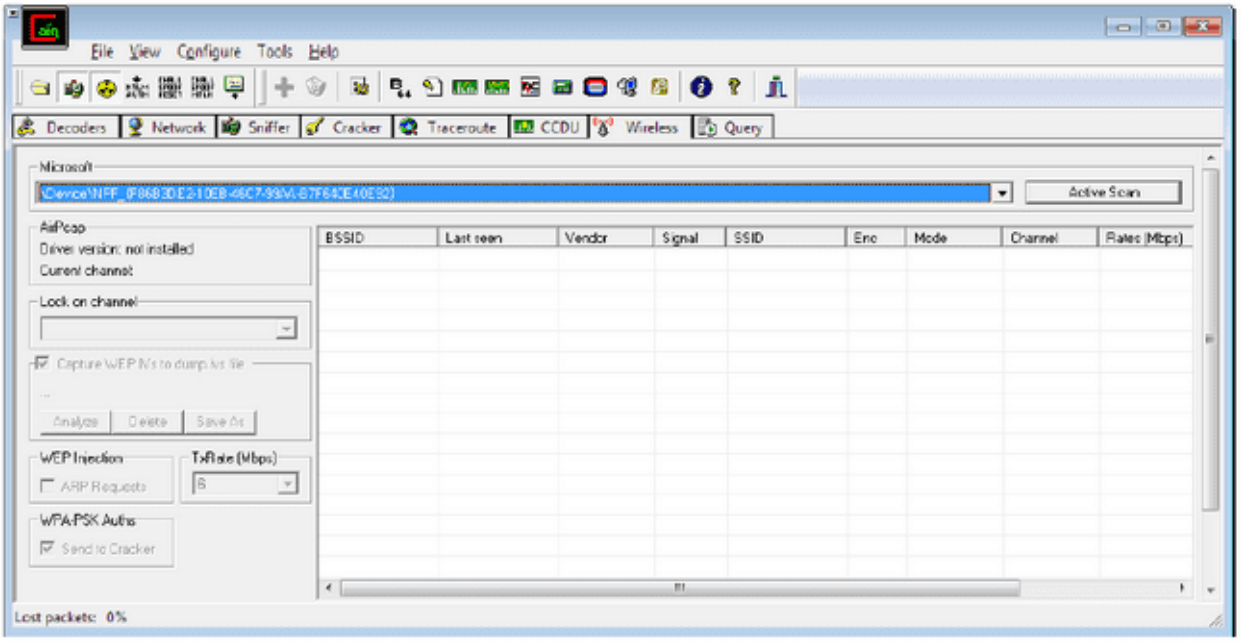


Step 4: The test are run. All IP address in the range are shown.

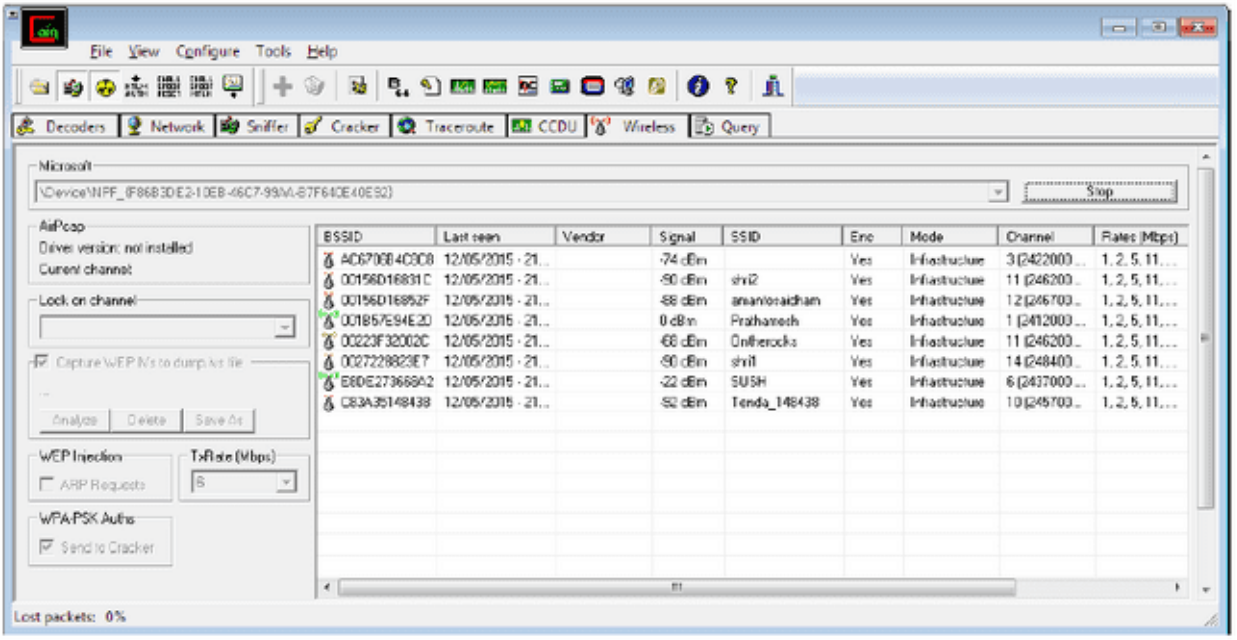




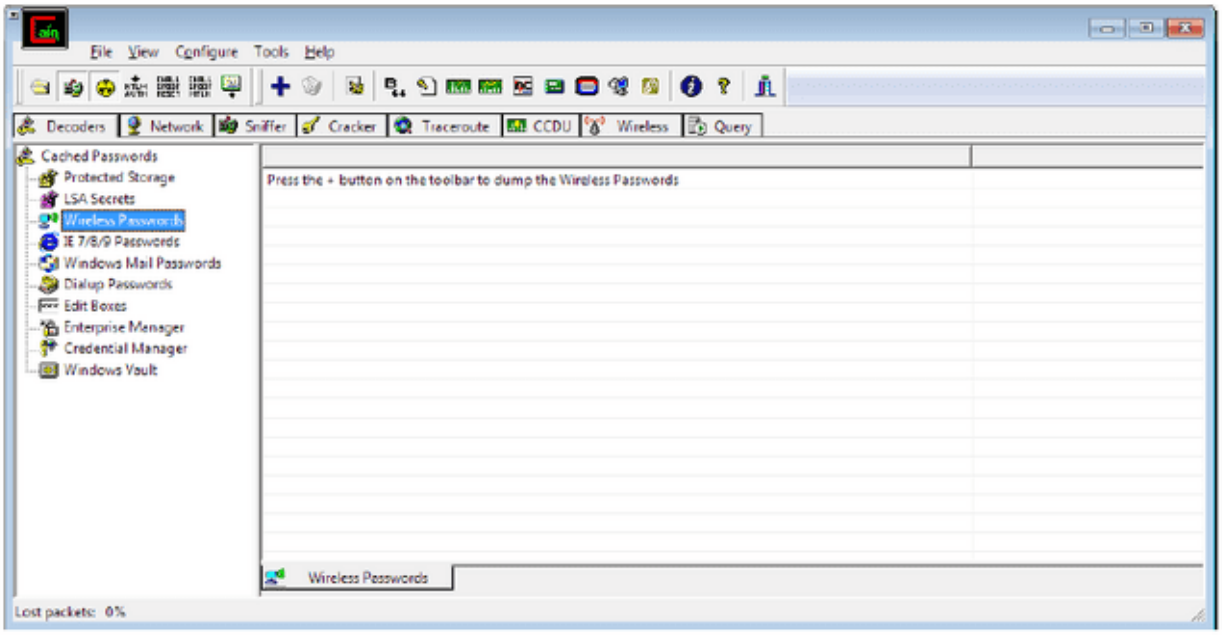
Step 5: Goto the wireless tab select second option in dropdown and click on active scan button



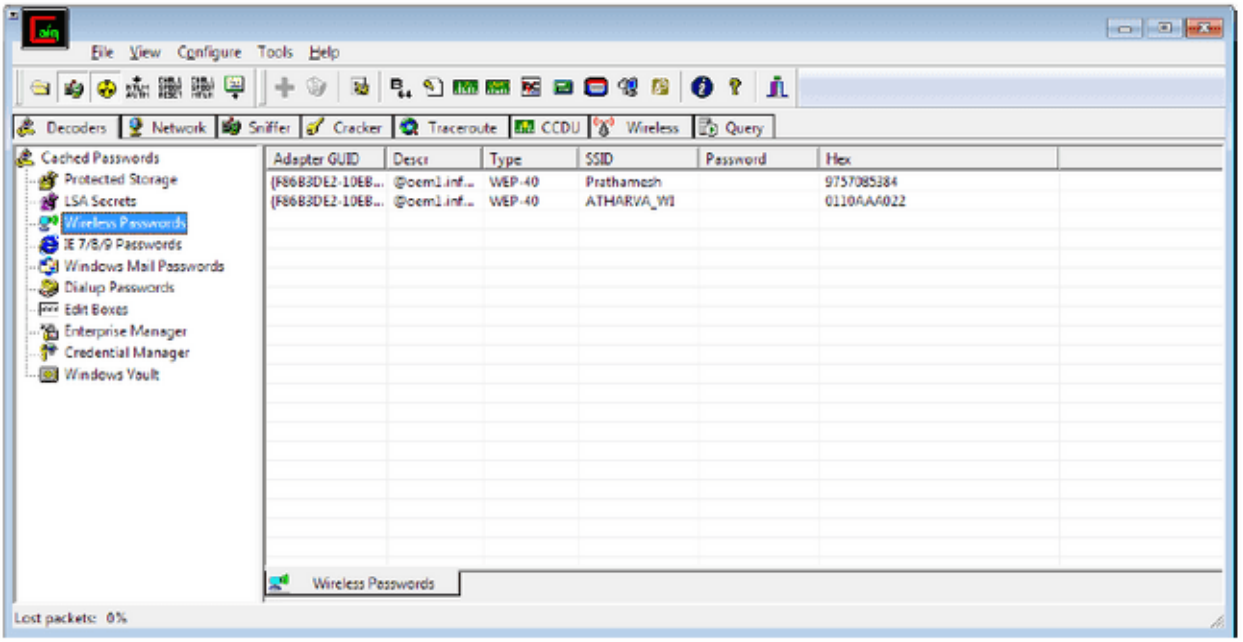
Step 6: It shows the nearest wireless connection.



Step 7: Go to decoder tab and select wireless passwords.



Step 8: It shows the wireless connection and password.

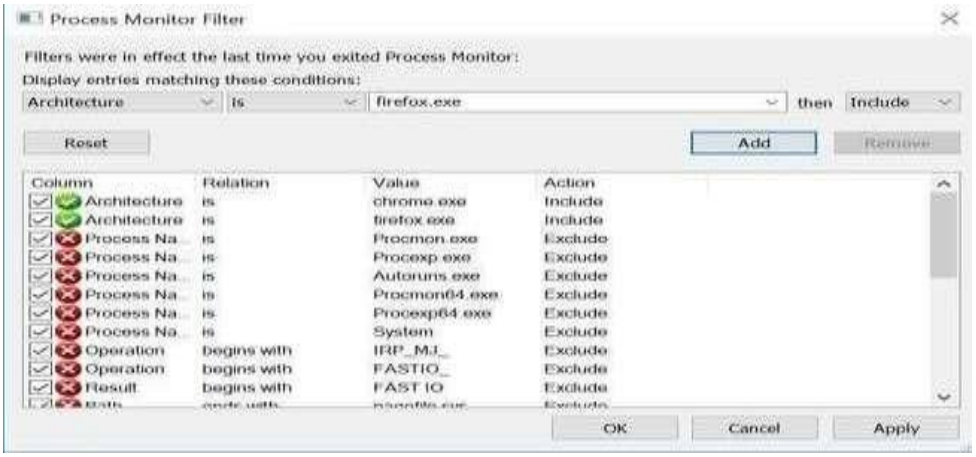


Practical 09

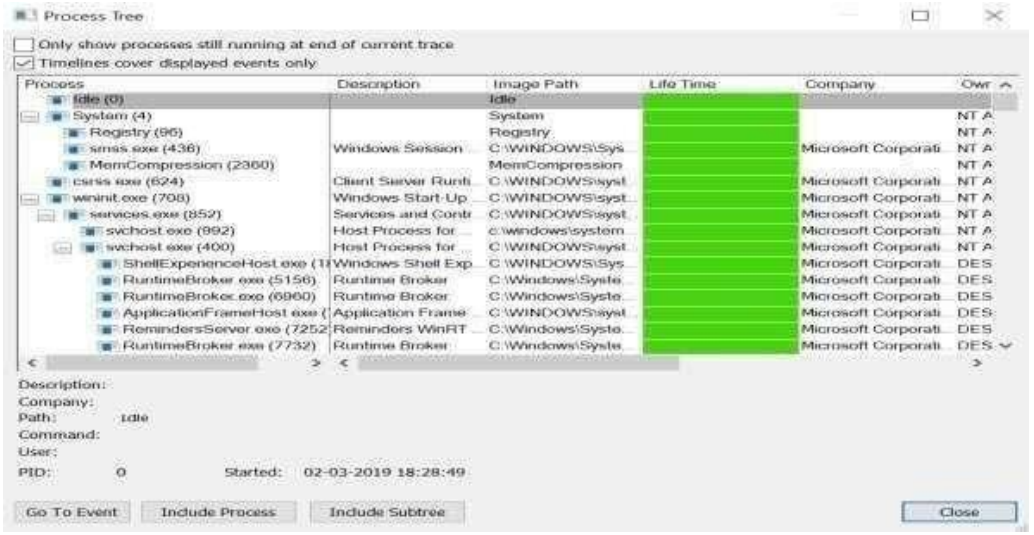
Scan Registry using RegScanner And Tools for RAM Capture, Virual Memory

1) Monitor Live Processes (Tool: ProcMon)

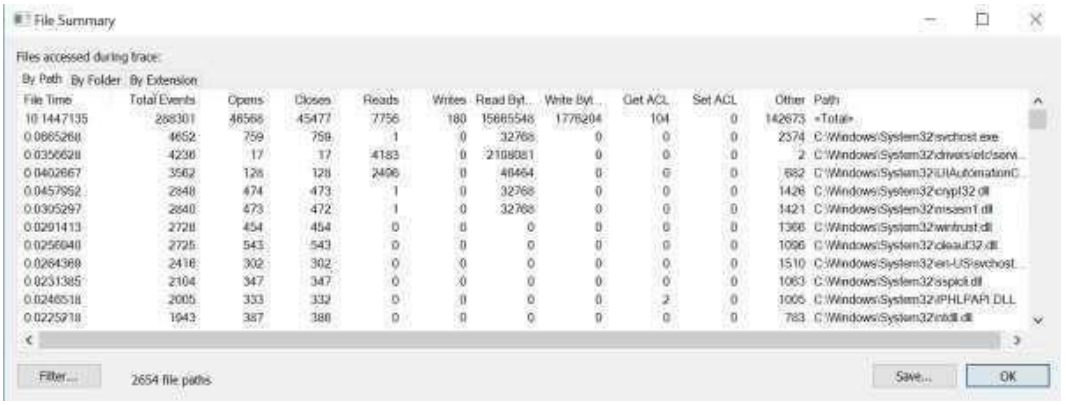
Click on filter > Process monitor filter



Click on tools > Process tree

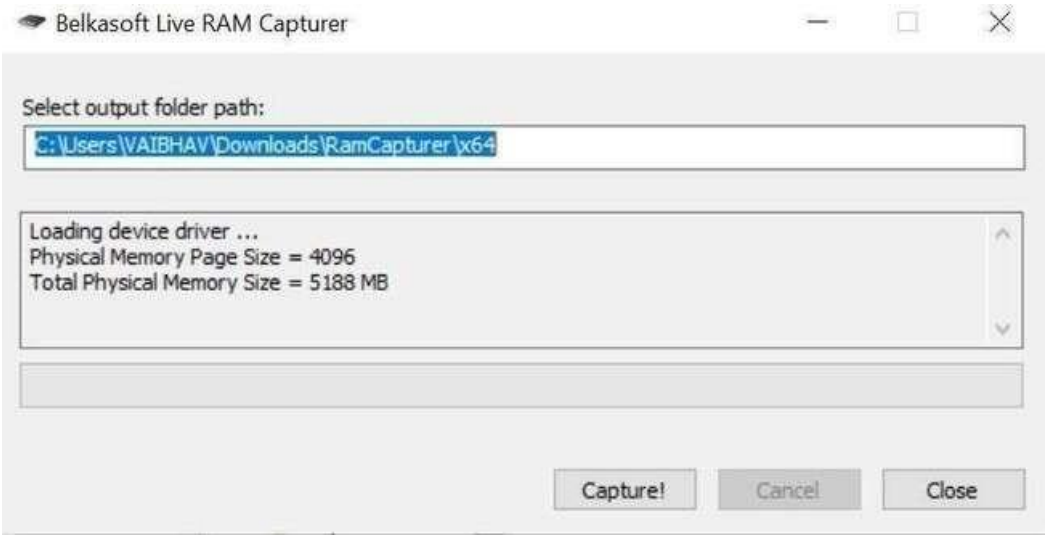


Click on filter > File summary

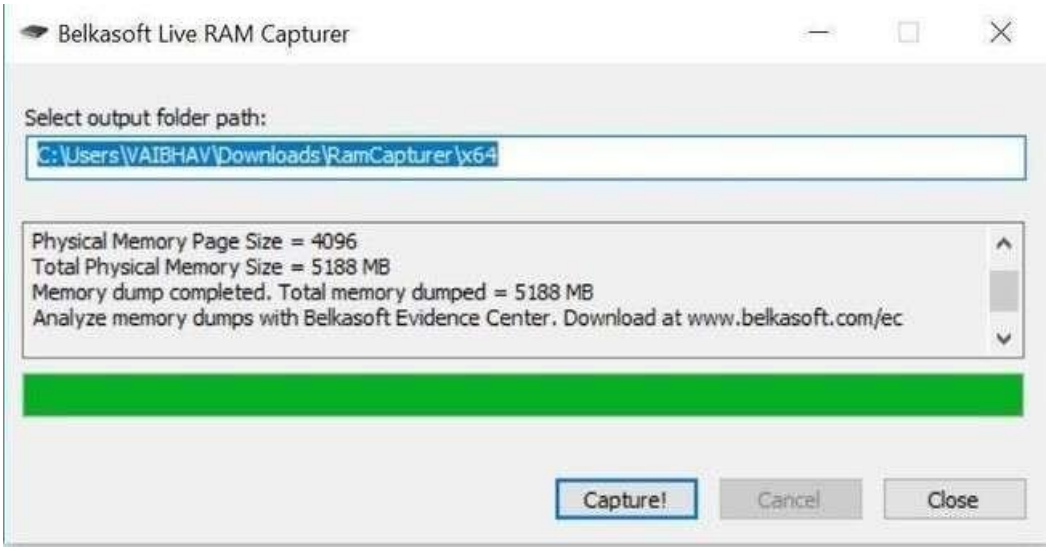


2) Capture RAM (Tool: RAMCapture)

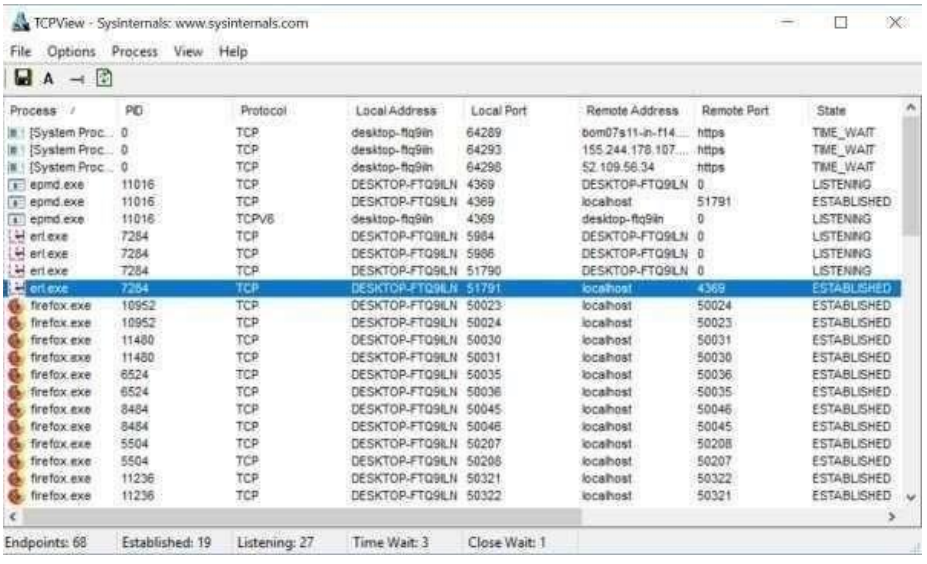
Open the Ramcapture tool.



Click on capture.

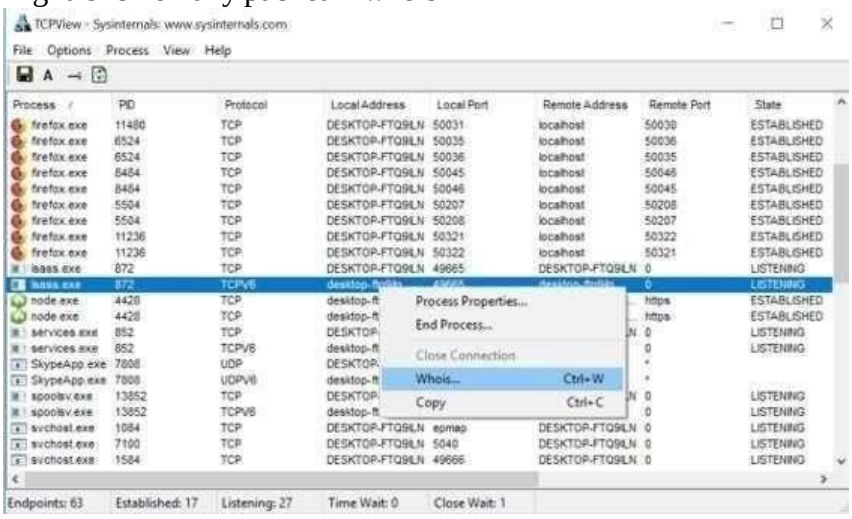


3) Capture TCP/UDP packets (Tool:



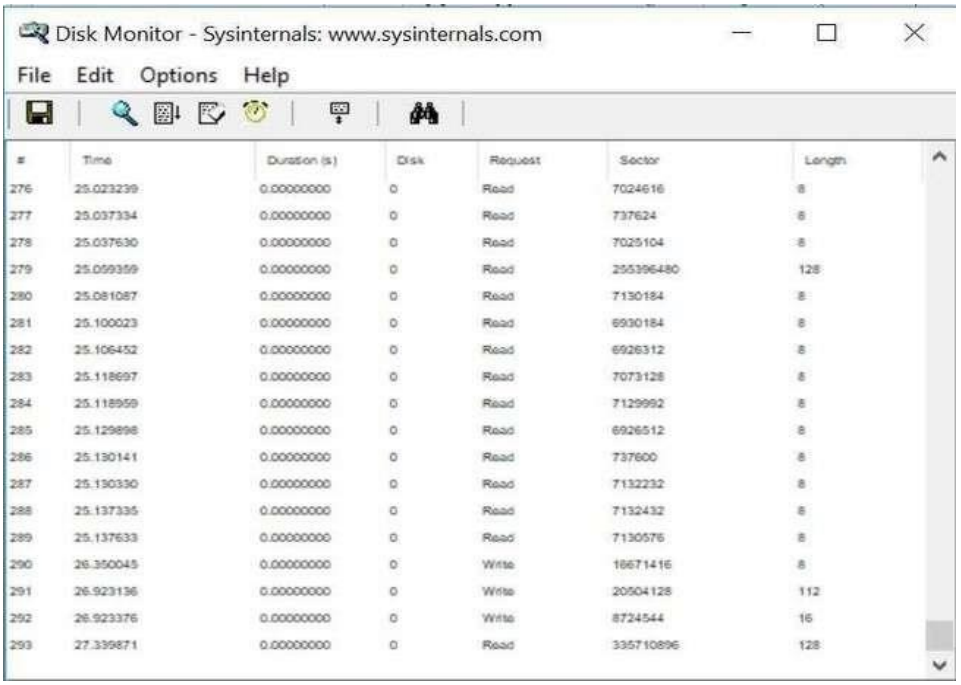
TcpView) Open the Tcpview tool.

Right click on any packet > whois



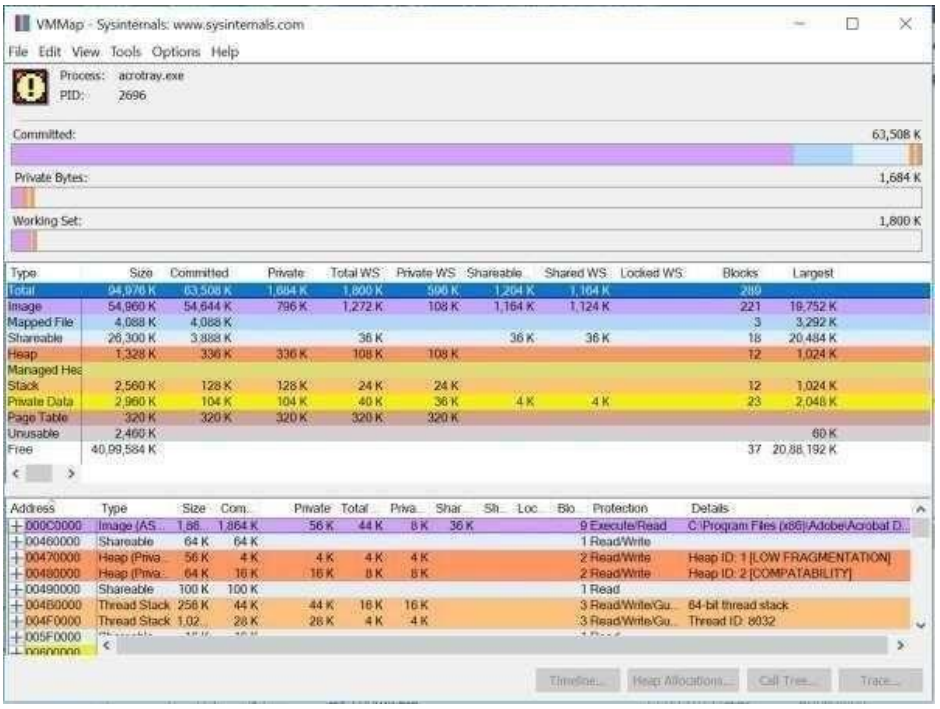
4) Monitor Hard Disk (Tool: DiskMon)

Open the Diskmon tool.



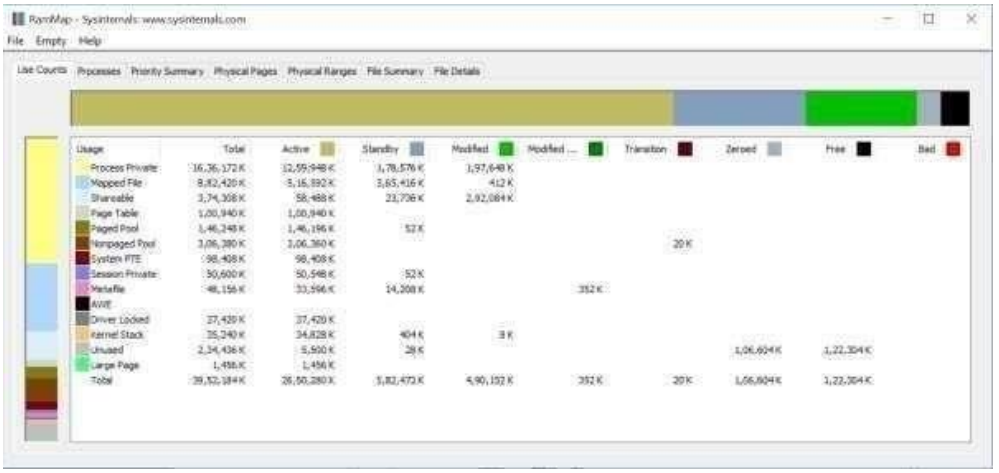
5) Monitor Virtual Memory (Tool: VMMap)

Open the VMMap tool.



6) Monitor Cache Memory (Tool:

RAMMap) Open the RAMMap tool.



B. Alien Registry Viewer

What is Alien Registry Viewer?

Alien Registry Viewer is similar to the RegEdit application included into Windows, but unlike RegEdit, it works with standalone registry files. While RegEdit shows the contents of the system registry, Alien Registry Viewer works with registry files copied from other computers. Alien Registry Viewer can be extremely useful for system administration and forensic computer examination purposes.

The current version of Alien Registry Viewer works in the read-only mode, i.e. you can view but you cannot edit registry files.

Using Alien Registry Viewer

The system registry resides in several files. There are two registry files in old Windows 95/98/Me : system.dat and user.dat. User.dat contains the HKEY_CURRENT_USER registry hive while system.dat contains all other hives. Both these files can be found in the Windows directory.

Newer Windows versions (NT/2000/XP/2003/2008/Vista/Win7) the system registry resides in the following files:

NTUSER.DAT - this file contains the HKEY_CURRENT_USER hive. Normally the NTUSER file has a 'hidden' attribute and therefore is invisible in Explorer. This file is located in the user profile folder.

All the following files are located in %SysRoot%\System32\config folder:

SAM. - this file contains the HKEY_LOCAL_MACHIVE\SAM hive

SOFTWARE. this file contains the HKEY_LOCAL_MACHIVE\SOFTWARE hive

SECURITY. this file contains the HKEY_LOCAL_MACHIVE\SECURITY hive

COMPONENTS. - this file contains the HKEY_LOCAL_MACHIVE\COMPONENTS hive (optional)

BCD-TEMPLATE - this file contains the HKEY_LOCAL_MACHINE\BCD00000000 hive (optional)

SYSTEM. this file contains all other keys of HKEY_LOCAL_MACHIVE (such as SYSTEM)

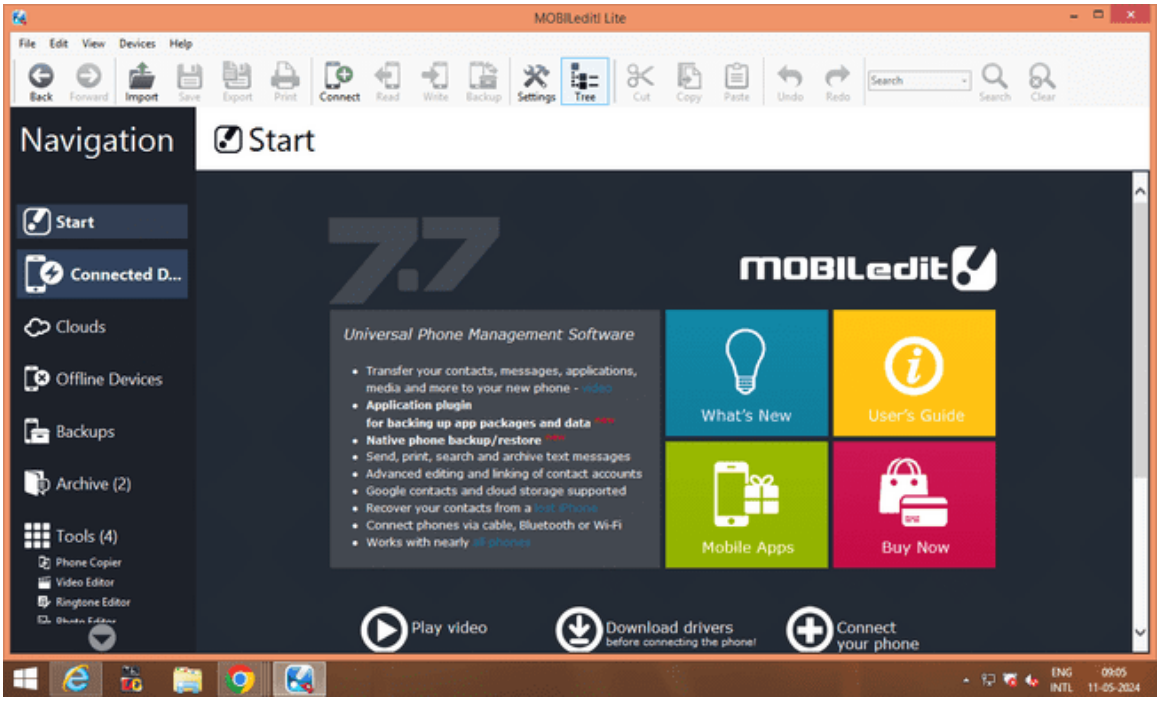
Practical 10

Aim: Acquisition of Cell phones and Mobile device

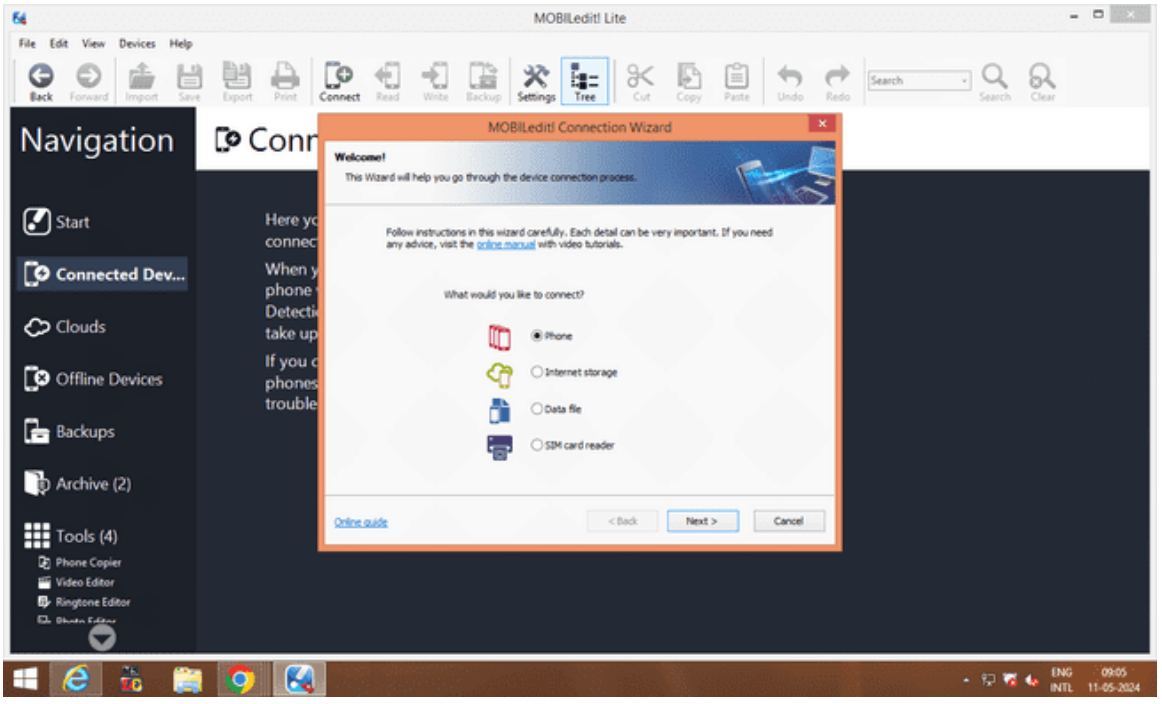
1. Download mobiledit forensic tool in mobile.

2. Open Mobiledit tool in PC.

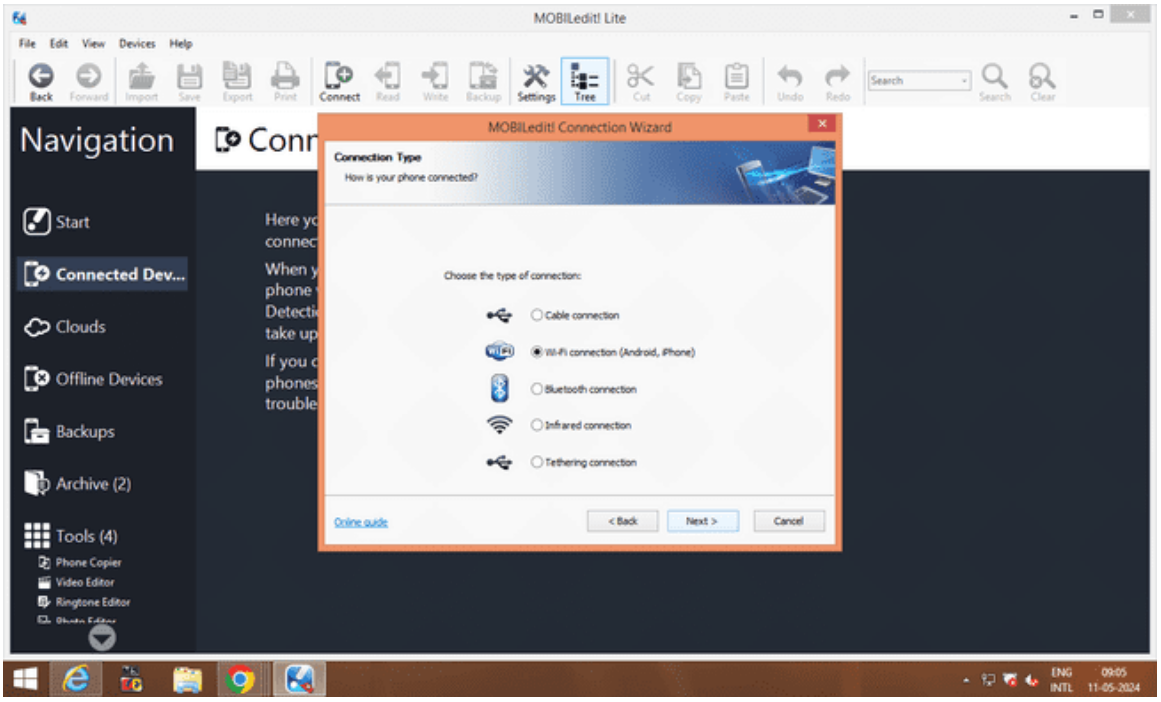
3. Click on connect.



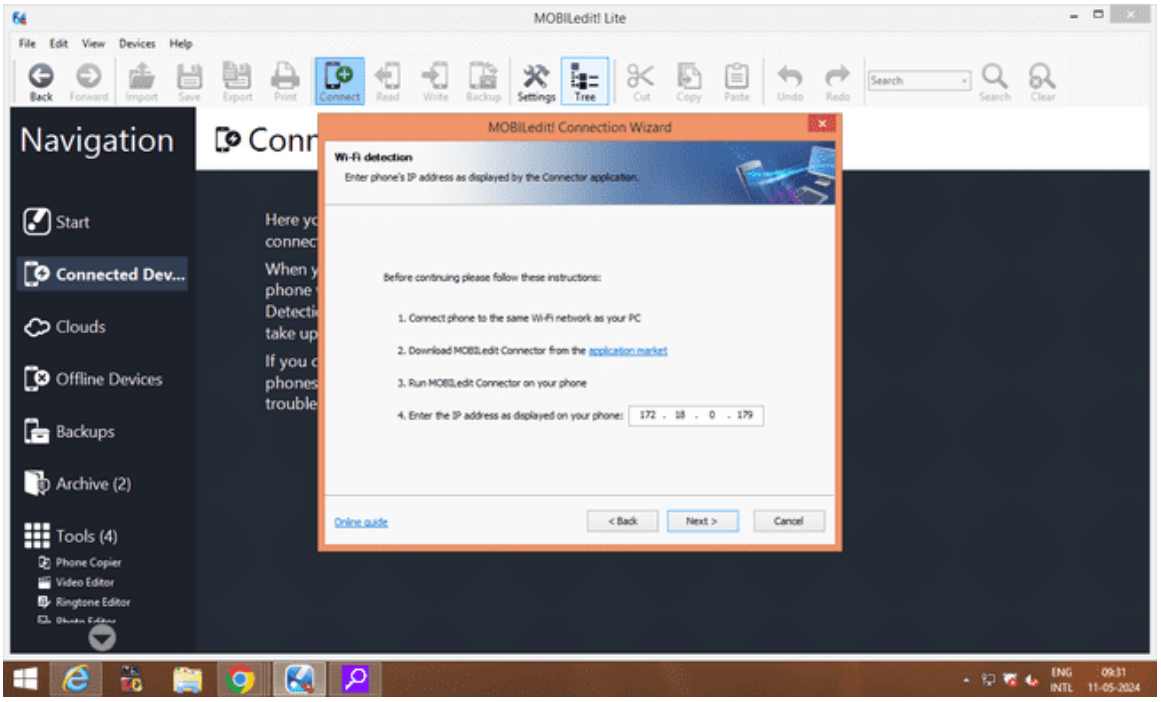
4. Connect your mobile device to the system. Click on phone > next.



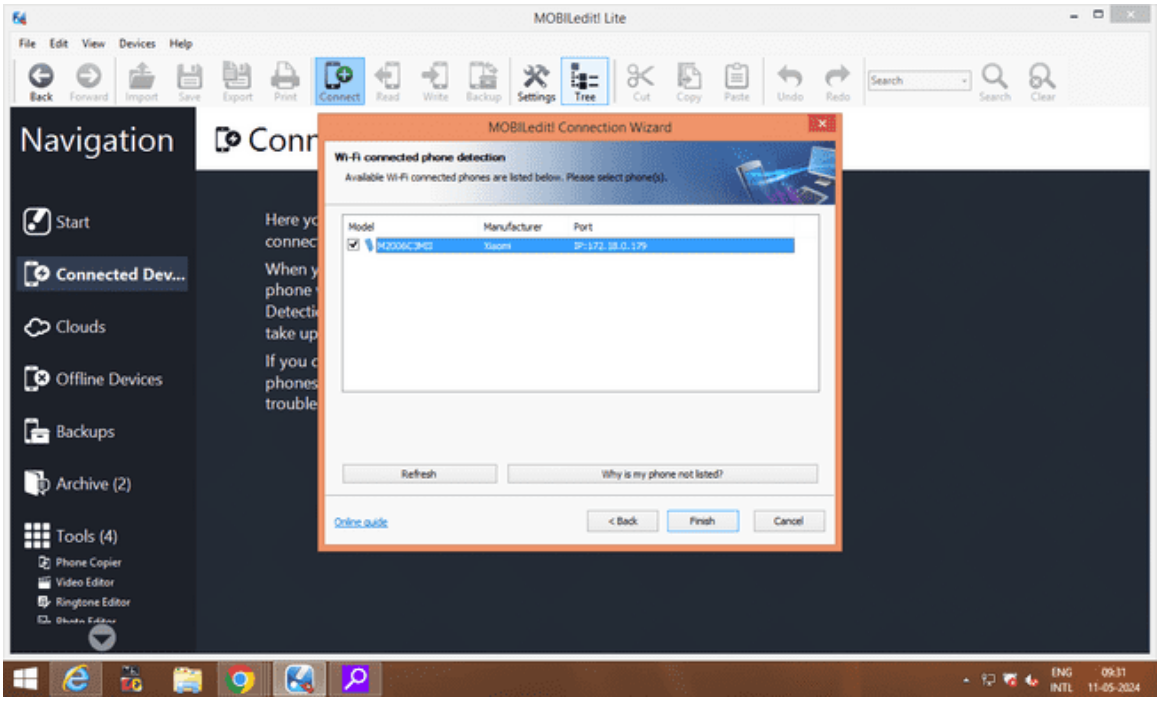
5. Click the connection



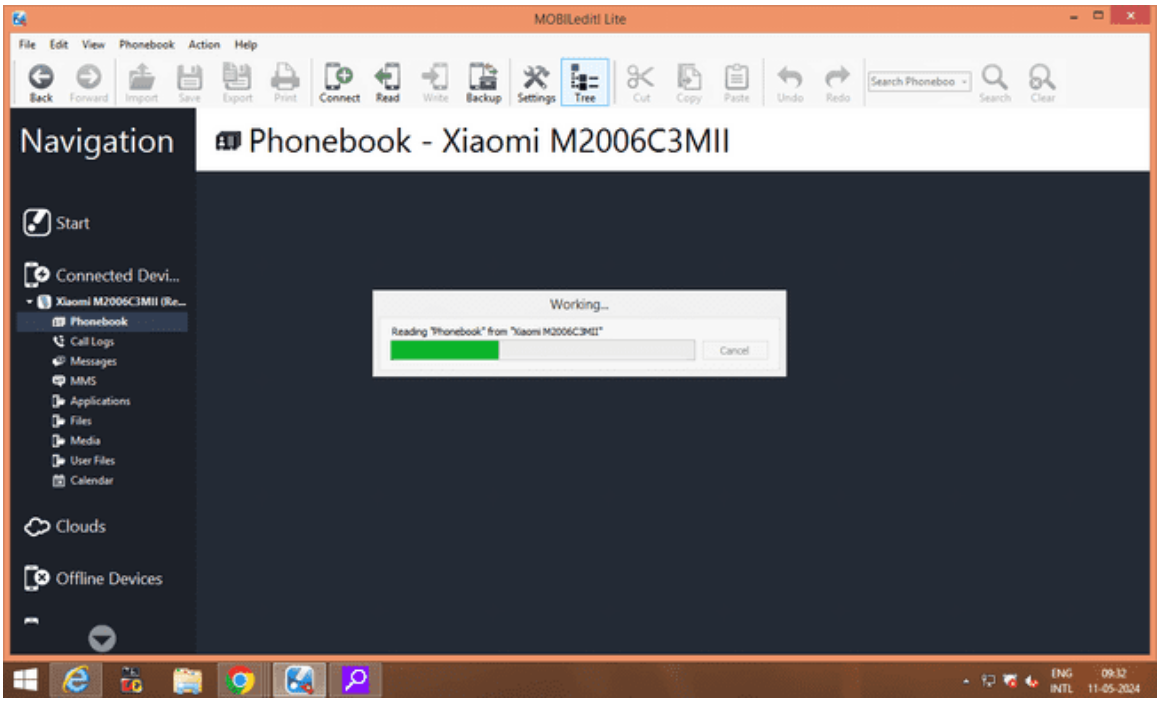
6. Open the mobiledit tool in phone and click on the type of connection (i.e Wifi) > Copy the IP address and enter it in the PC and click next.



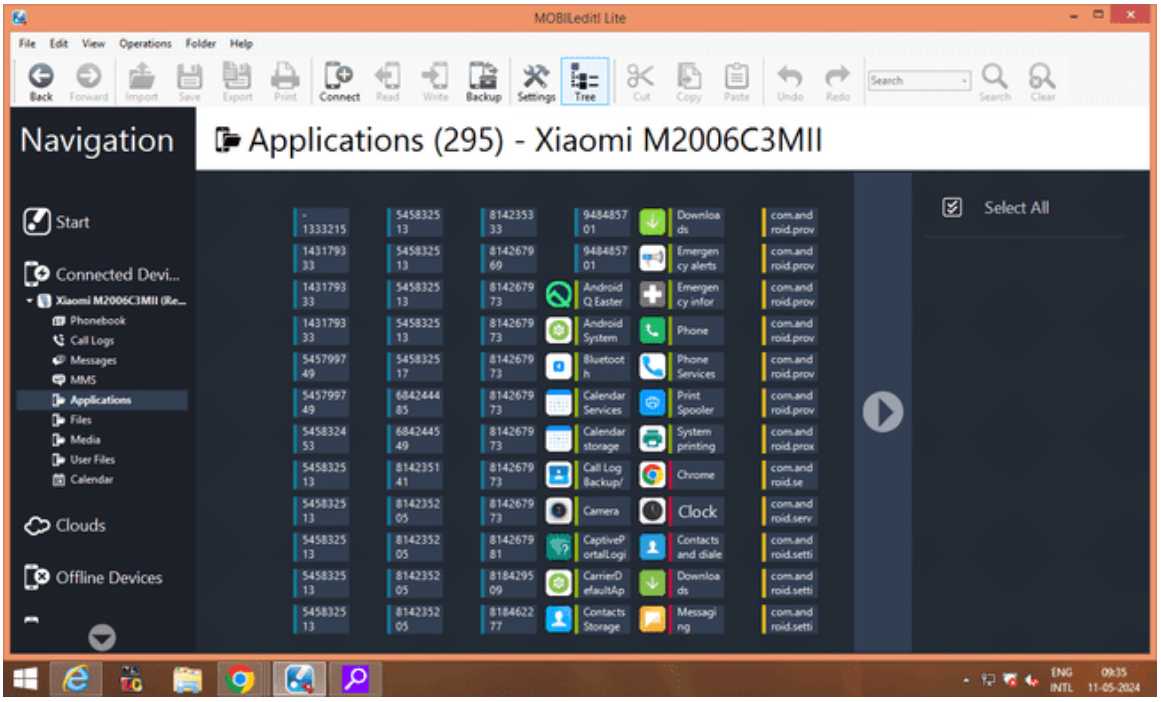
7. It shows the phone which is connected. Click on finish.



8. Click on your device in the left panel.



9. You can see all the files.


MOBILedit! Lite
File Edit View Operations Folder Help
Back Forward Import Save Export Print Connect Read Write Backup Settings Tree Cut Copy Paste Undo Redo Search Search Clear
Navigation
Applications (295) - Xiaomi M2006C3MII
Start
Connected Devi...
Xiaomi M2006C3MII (Re...
Phonebook
Call Logs
Messages
MMS
Applications
Files
Media
User Files
Calendar
Clouds
Offline Devices
Select All
Downloads
Emergency alerts
Emergency infor
Android Q Easter
Android System
Phone
Bluetooth
Phone Services
Calendar Services
Print Spooler
Calendar storage
System printing
Call Log Backup/
Chrome
Camera
Clock
CaptivePortalLogi
Contacts and diale
CarrierDefaultAp
Downloads
Contacts Storage
Messaging
com.android.prov
com.android.prox
com.android.se
com.android.serv
com.android.setti
ENG INTL 09:35 11-05-2024