PRACTICAL 1

File System Analysis using The SleuthKit (Autopsy, fsstat, istat, fls and img_stat)

Aim: Exploring Autopsy.

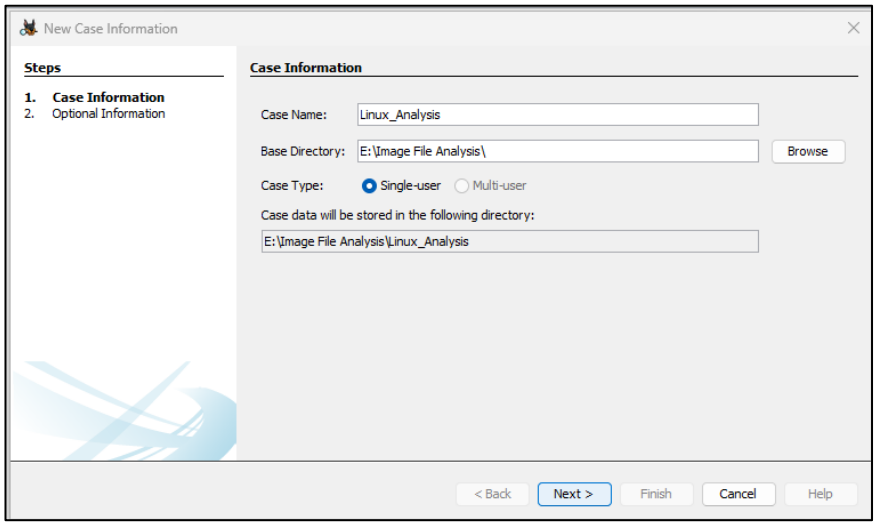
To install Autopsy, navigate to C:\CHFI-Tools\CHFIv10 Module 03UnderstandingHardDisksandFileSystems\FileSystemAnalysisTools\Autopsy, double-click autopsy-4.14.0-64bit.msi installer and follow the wizard driven installation steps to complete the installation process.

Autopsy Welcome window will appear along with Autopsy main window in the background. In the Welcome window, click New Case.

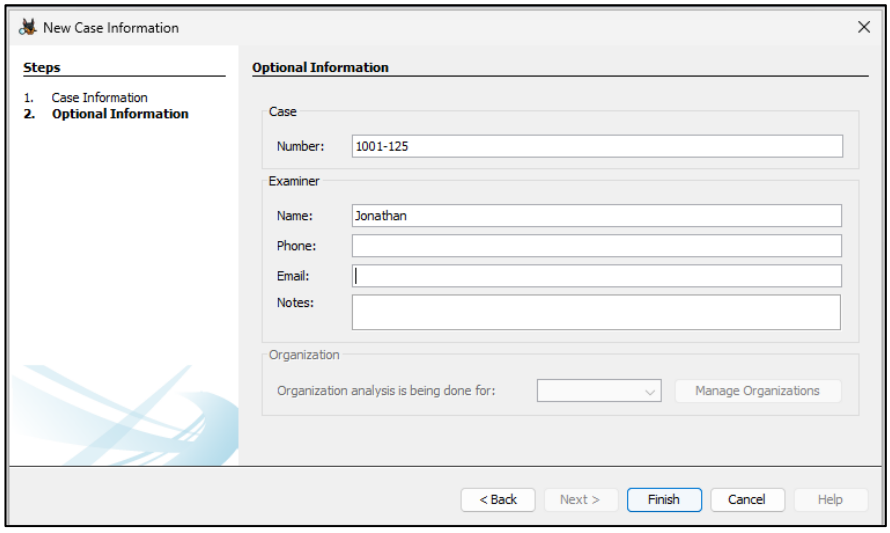
A New Case Information window opens asking you to input the Case Name and the Base Directory. The base directory is the location where the case data will get stored.

The case name may be entered according to your identification purpose. In this lab, we are assigning the case name as Linux_Analysis.7.

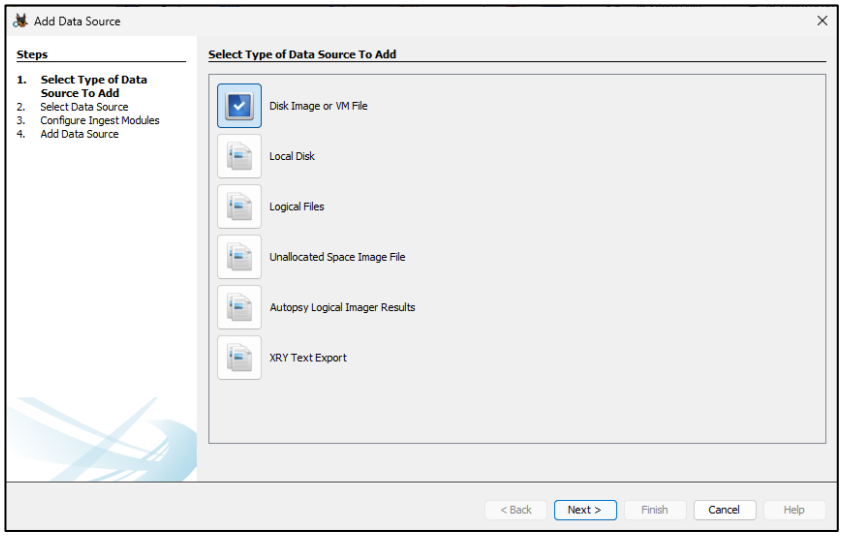
Before specifying the base directory, we will be creating a folder on the Desktop with the name Image File Analysis and setting the path of the Base directory to this folder. Upon setting the base directory, click Next



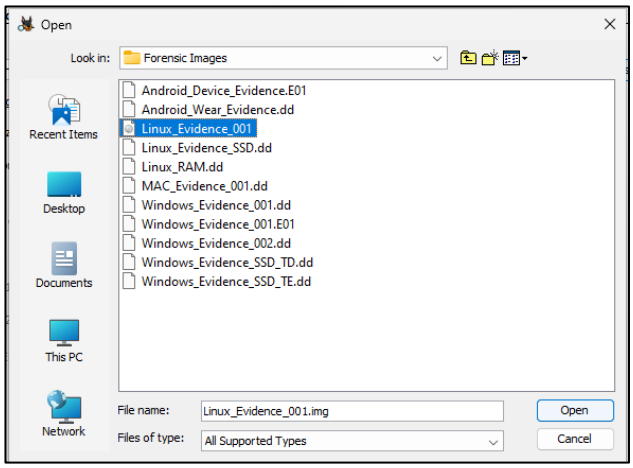
The New Case Information window now shows the Optional Information section where you can specify details such as name of the examiner and case number. For this lab, let us enter the name of the examiner as Jonathan and the case number as 1001-125. You may also fill out the other optional fields. Click Finish after entering the details for optional fields.

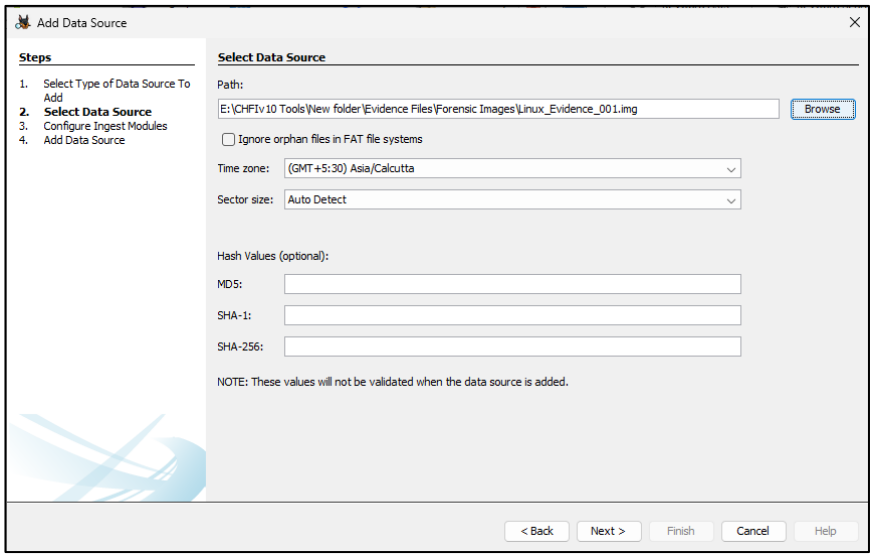


The Add Data Source window now appears displaying the section Select Type of Data Source to Add. Here,you need to select the type of data source to be provided as an input. In this lab, we will be analyzing a disk image; therefore, select the option Disk Image or VM File and click Next.

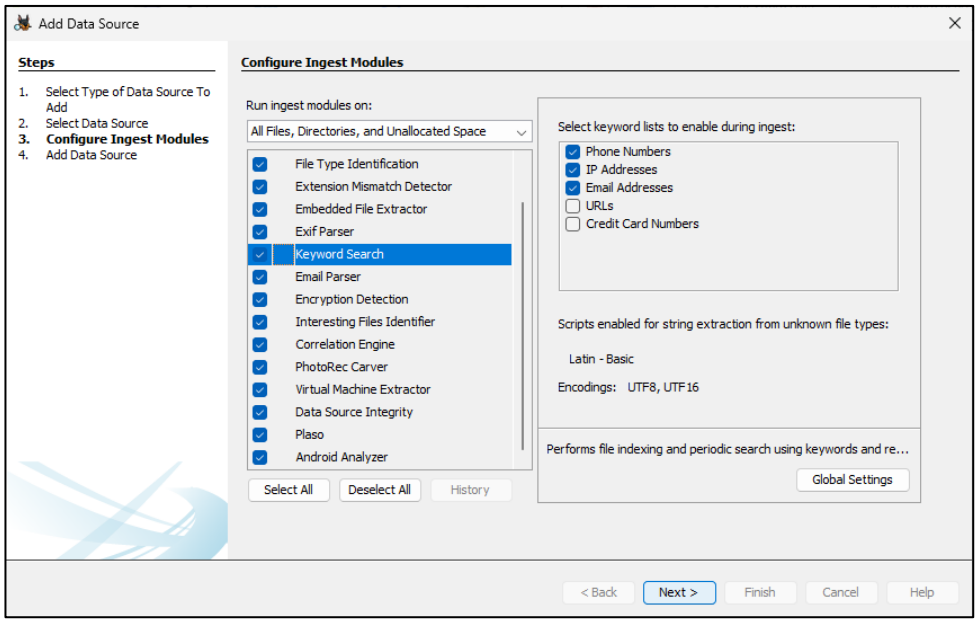


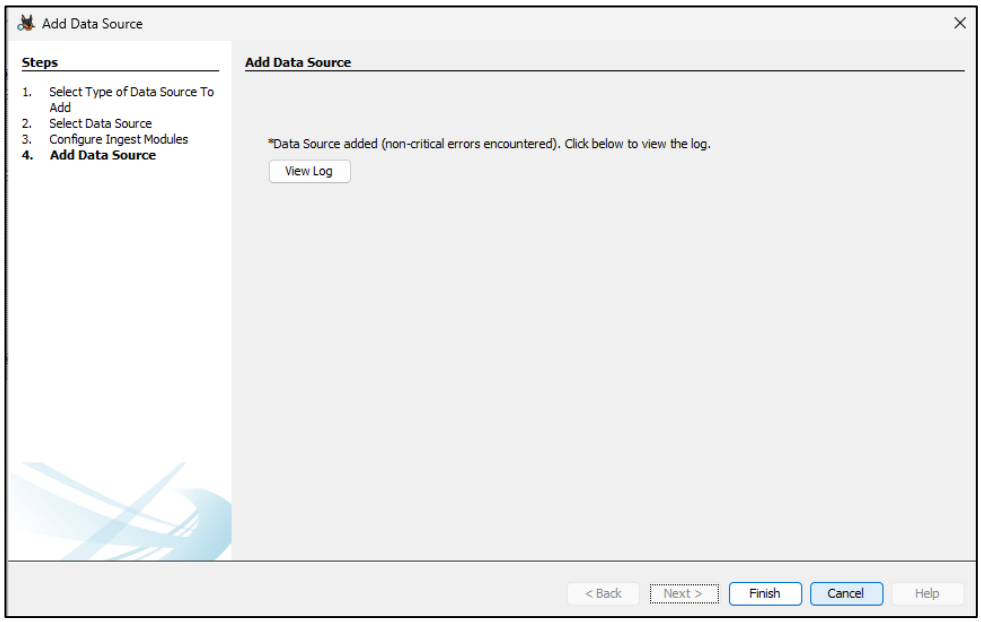
A window (named Open) will appear where you need to specify the forensic image. Navigate to C:\CHFI-Tools\Evidence Files\Forensic Images, select Linux_Evidence_001.img and click Open.



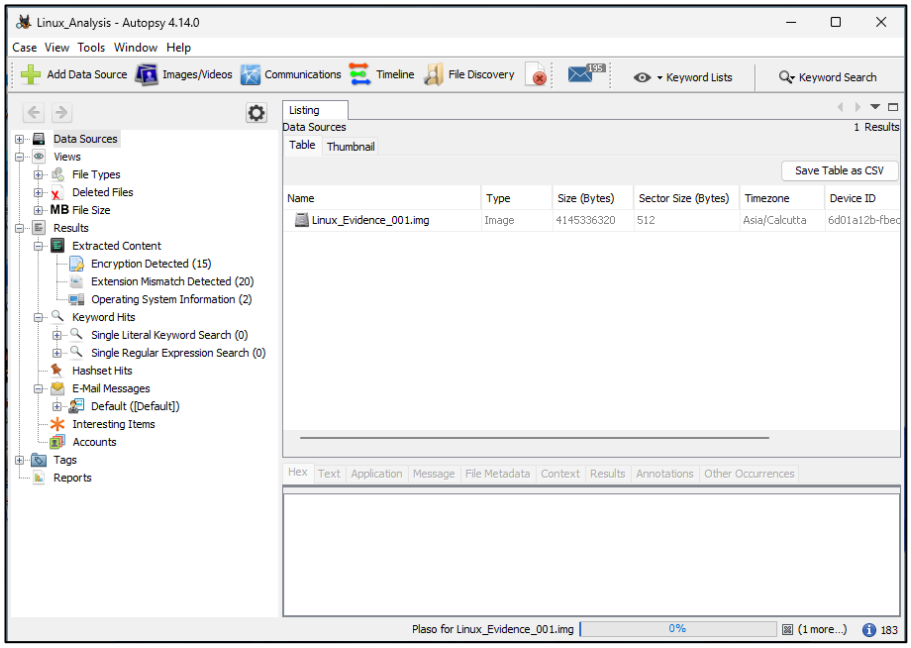


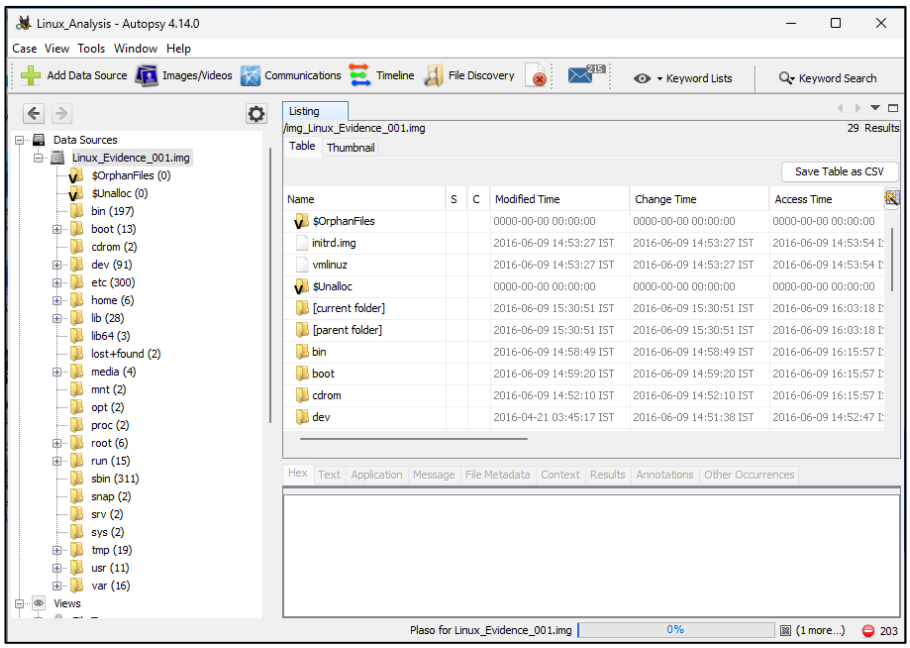
The Add Data Source window now displays the Configure Ingest Modules section, which contains lists of options that are checked. Select the options according to your requirement and click Next.





The application now displays the result in the Autopsy main window. Expand the Data Sources node in the left pane and click on the image file i.e.,Linux_Evidence_001.img. This will show the contents of the image file, as shown in the following screenshot:

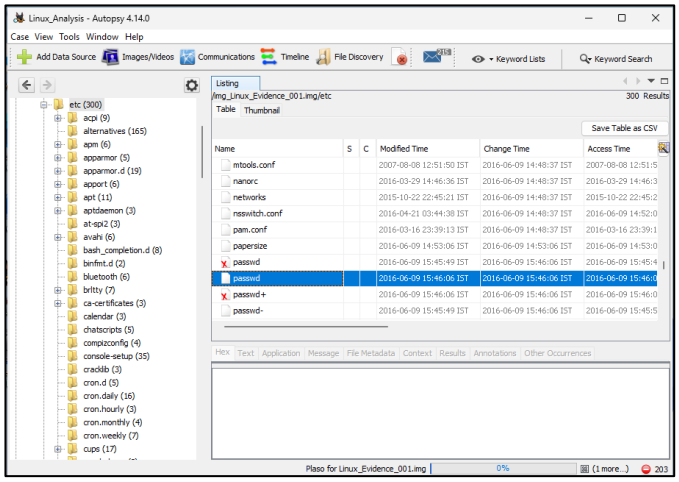




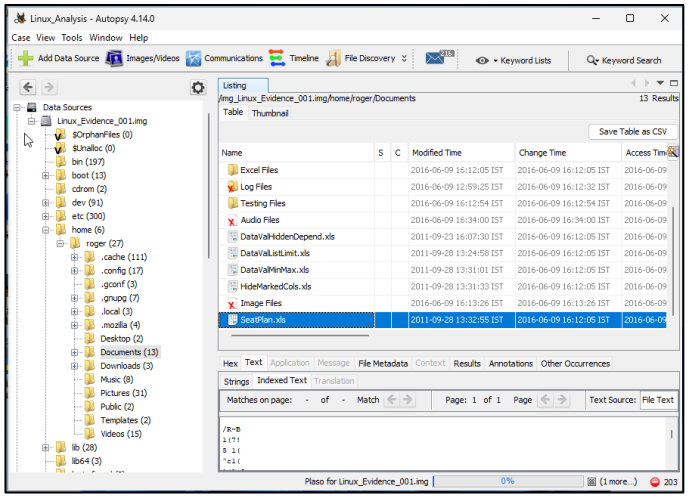
You may examine all the required files stored in the image as a part of filesystem analysis. In this lab, we are going to view the passwd file that is stored in \etc location. Therefore, select the etc folder from the left pane.

Upon selecting the folder, all the files and folders present in etc are displayed in the right pane of the window.

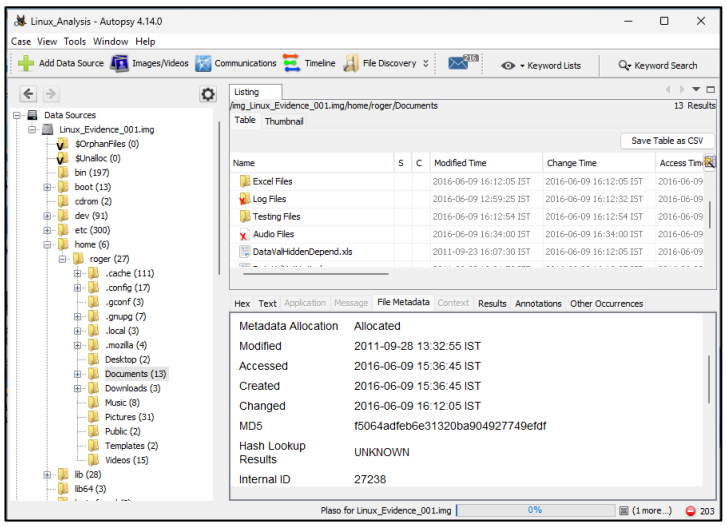
Scroll down the window, select the passwd file and click the Text tab. Autopsy displays all the text (user account information) present in the passwd file, under the Strings tab, as shown in the following screenshot:



The SeatPlan.xls file appears in the right pane of the Autopsy window. Click the file.

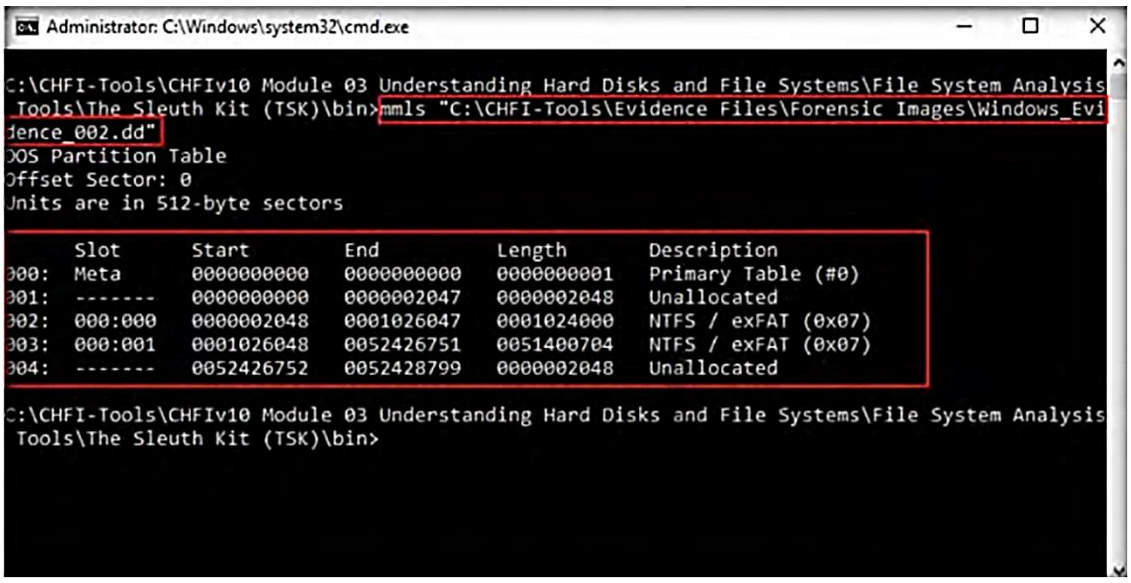


Click on File Metadata and scroll down the section to find the MD5 value for the SeatPlan.xls file.

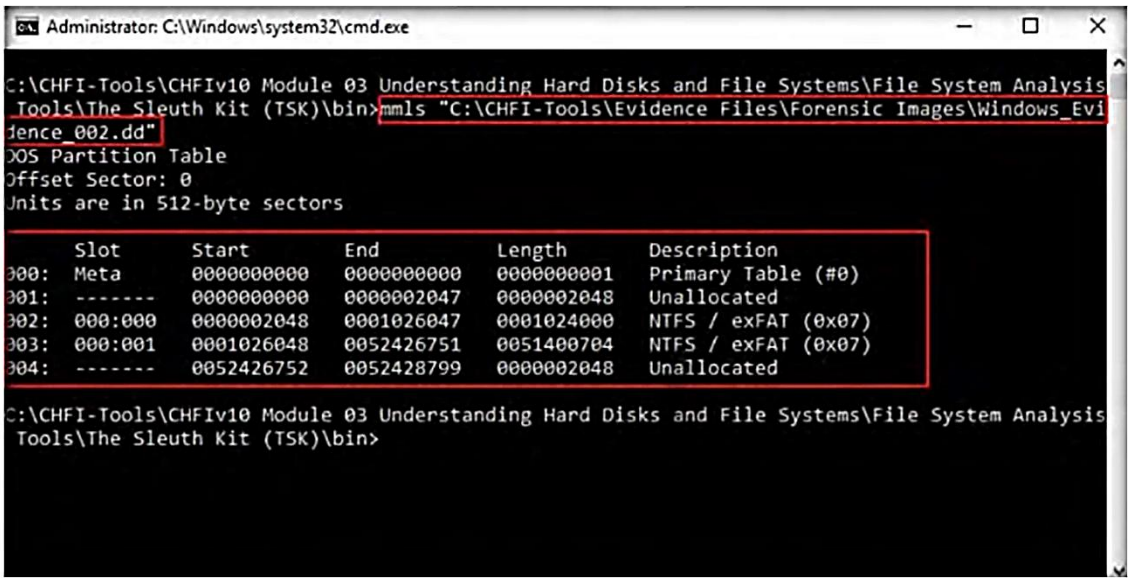


To study fsstat

To view partition tables associated with Windows_Evidence_002.dd, type mmls "C:\CHFI-Tools\EvidenceFiles\ForensicImages\Windows_Evidence_002.dd"and press Enter. This displays the partition layout of a volume system (partition tables) associated with the image file, as shown in the following screenshot:



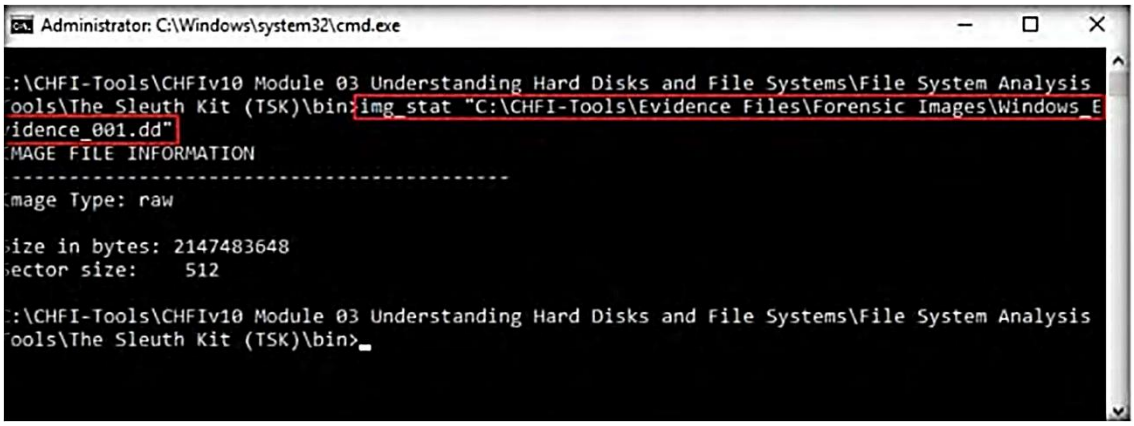
Similarly, to view the type of file system and the OS related to the image, type fsstat "C:\CHFI- Tools\Evidence Files\Forensic Images\Windows_Evidence_001.dd"and then press Enter.



From the above screenshot, it can be observed that the file system is NTFS and the source OS is Windows XP.

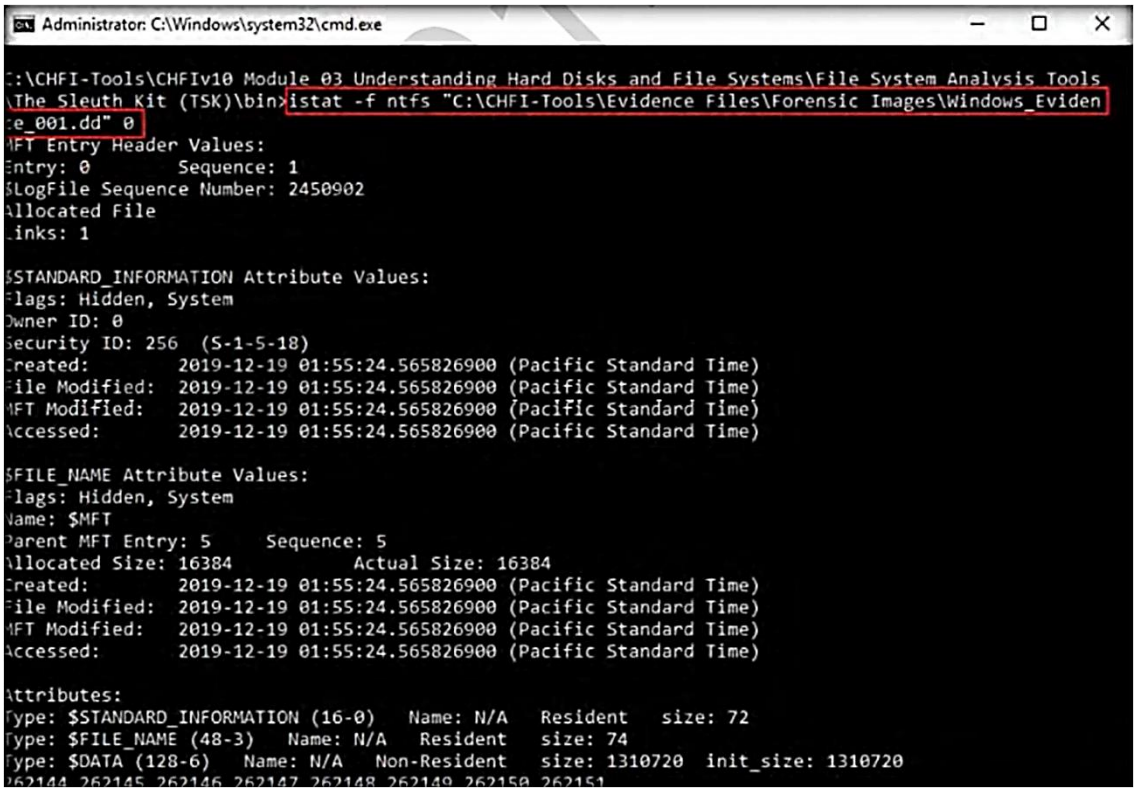
To Study img_stat

Use the img_stat command to view the details of the selected image. Type img_stat"C:\CHFI-Tools\Evidence Files\Forensic Images\Windows_Evidence_001.dd" and press Enter to view the details.

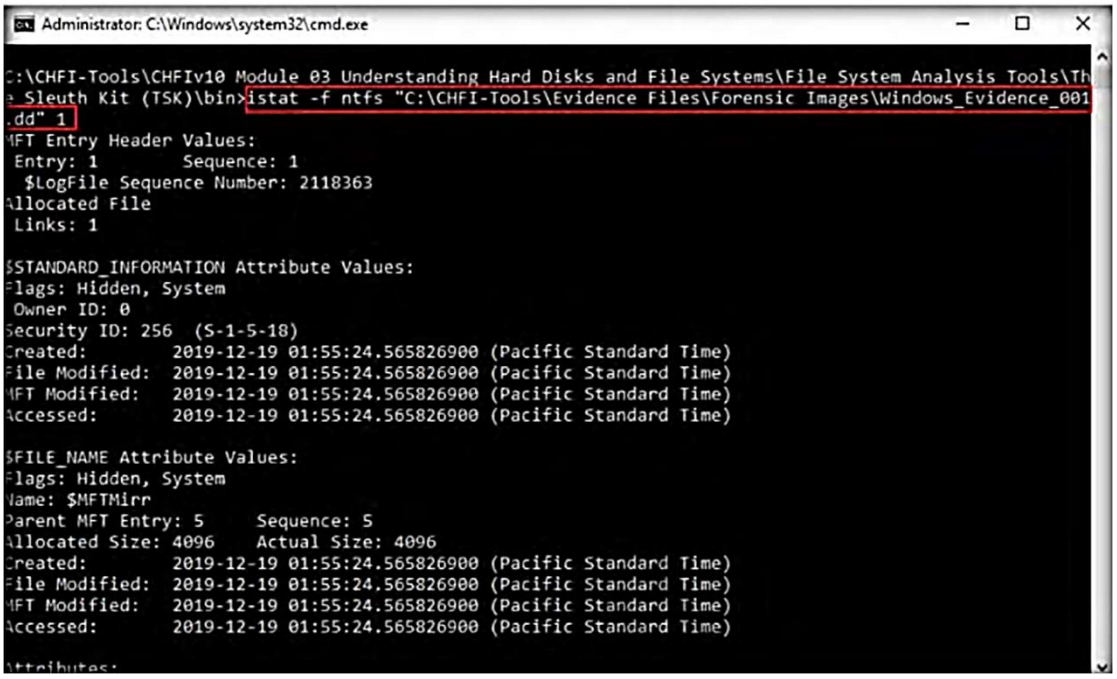


To Study istat

Use the istat tool in The Sleuth Kit to view the details of metadata structure. To display an overview of the MFT file, type istat -f ntfs "C:\CHFI-Tools\Evidence Files\Forensic Images\Windows_Evidence_001.dd" 0 and press Enter to view the details.



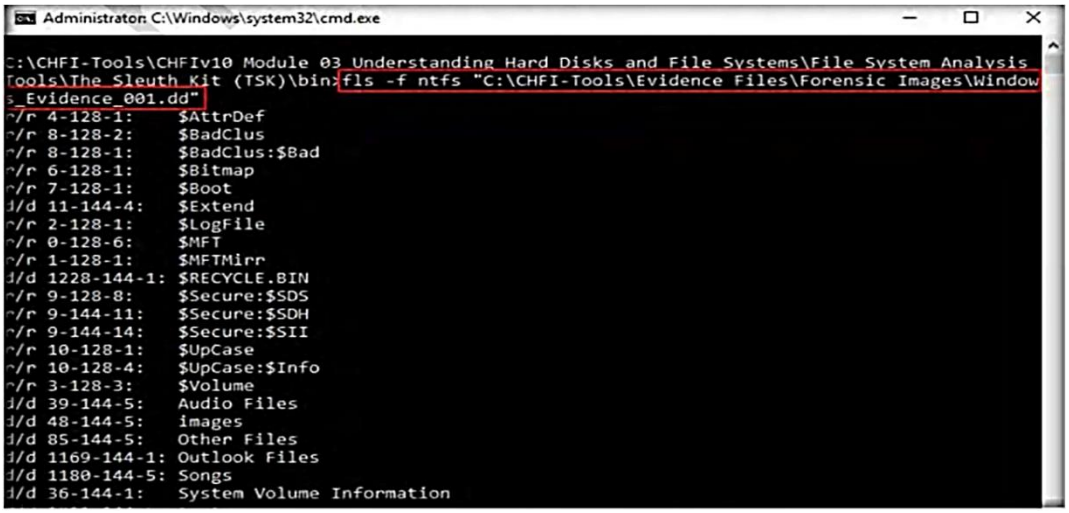
To display the MFTMirr File Overview, type istat -f ntfs "C:\CHFI-Tools\Evidence Files\Forensic Images\Windows_Evidence_001.dd" 1 and press Enter.



The layout of the MFT is determined by processing entry 0 in the MFT.MFT entry 1 is for the MFTMirr file, which has a non-residentattribute that contains a backup copy of the first MFT entry. The Boot file system metadata file is in MFT entry 7 and contains the boot sector of the file system. The MFT entry for the AttrDef filesystem metadata file is 4. It defines the names and type identifiers for each type of attribute. NTFS keeps track of the damaged clusters by allocating them to a$DATA attribute of the BadClus file system metadata file. The MFT entry is 8.

To Study fls

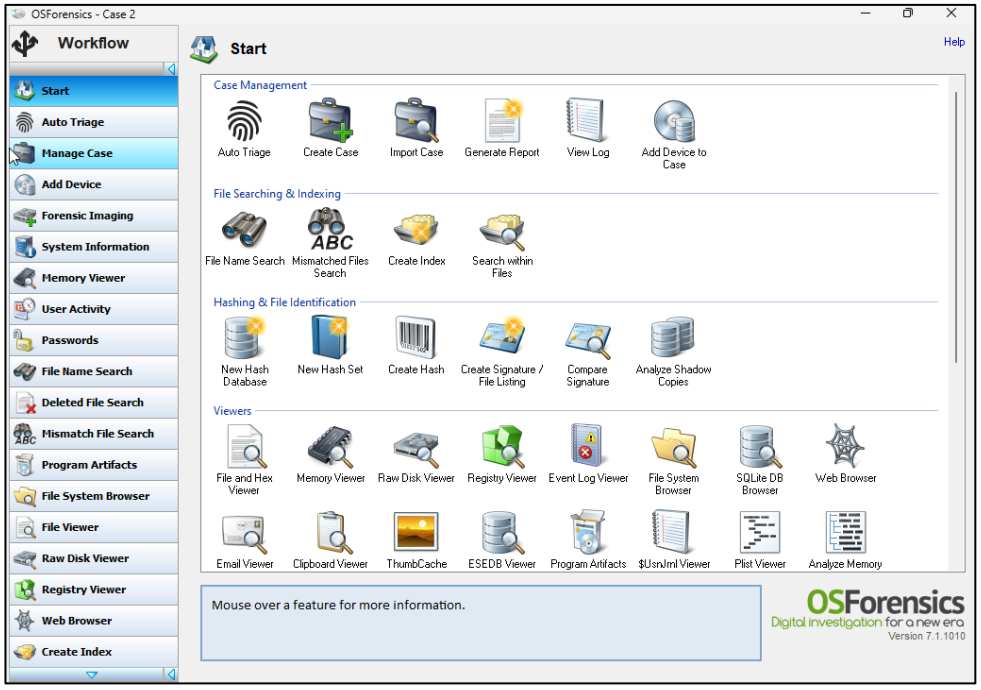
Use the fls command-line tool of TSK to list the files and directory names. Type fls -f ntfs "C:\CHFI-Tools\EvidenceFiles\ForensicImages\Windows_Evidence_001.dd"and then press Enter.



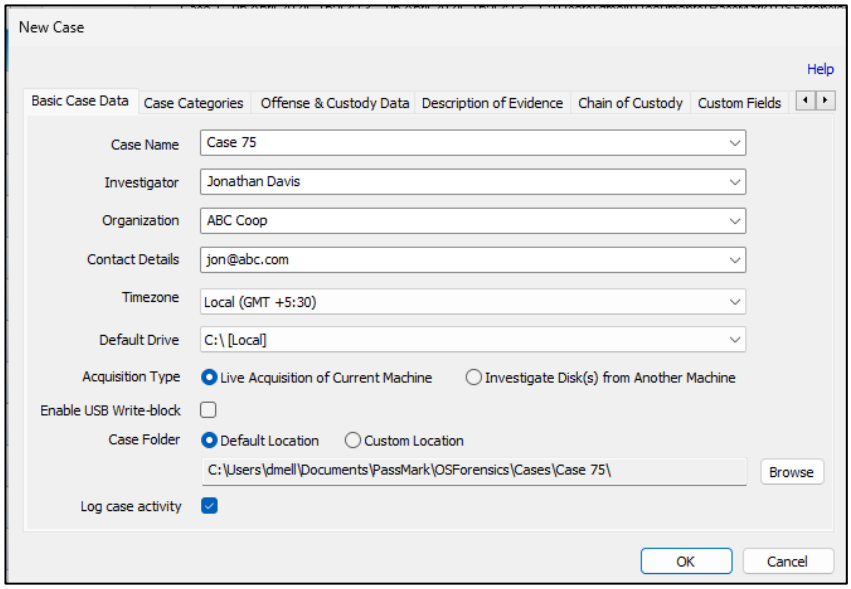
PRACTICAL 2

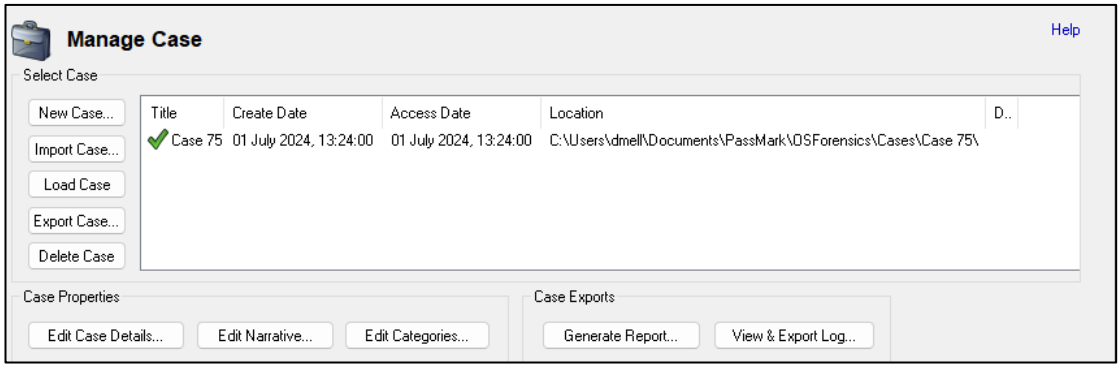
Aim: Explore Windows forensic tools (OSForensics)

Navigate to C:\CHFI-Tools\CHFIv10Module 06 Windows Forensics\Windows Forensics Tools\OS Forensics, double-clickosf.exe to launch the steup. In the final step of installation, check the Launch OSForensics option and click Finish. OSForensics GUI appears, along with PassMarkOSForensics pop-up. In the pop-up, click Continue Using Trial Version. Our first task is to create a case using this tool. Click the Create Case icon in the tool's main window to create a new case.

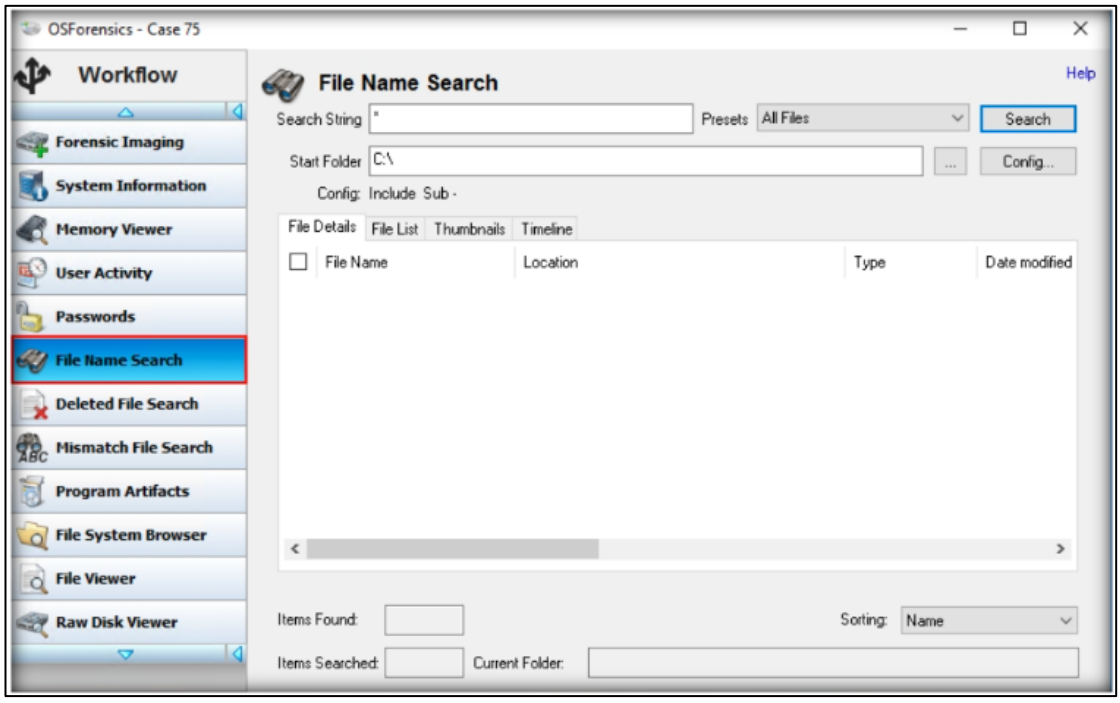


A New Case window appears; fill out the required fields in the window. Ensure that you select the radio button for the Live Acquisition of Current Machine option in the Acquisition Type category. You may choose to save the new case folder either in Default or Custom locations. Click OK

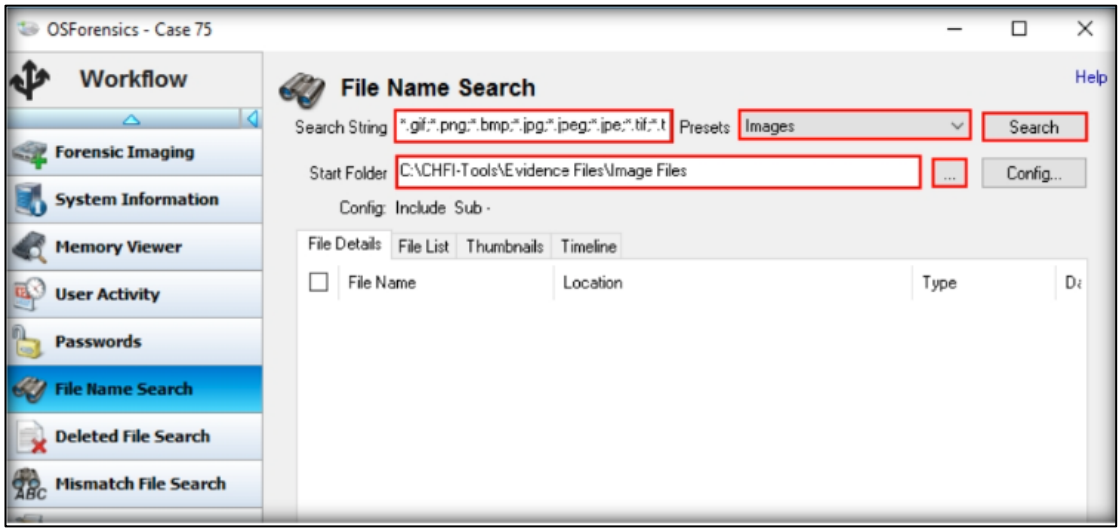


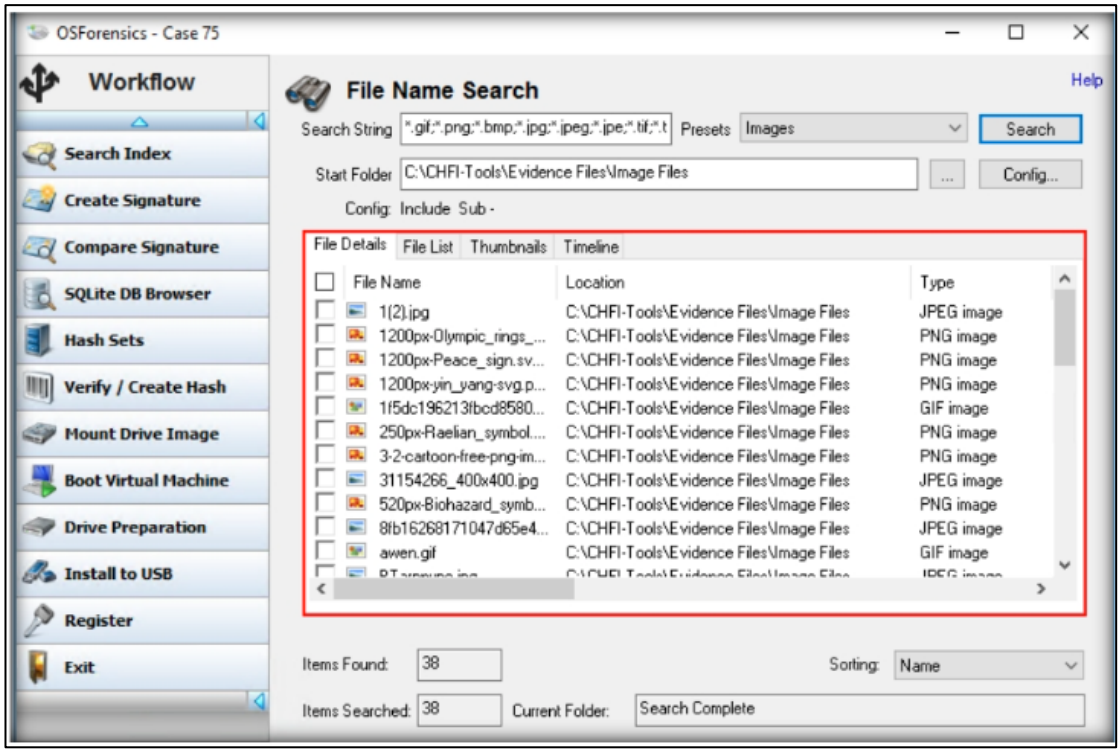


The OSForensics tool can help investigators in searching and locating files on a system. To start searching for files, click File Name Search in the left pane of the window.

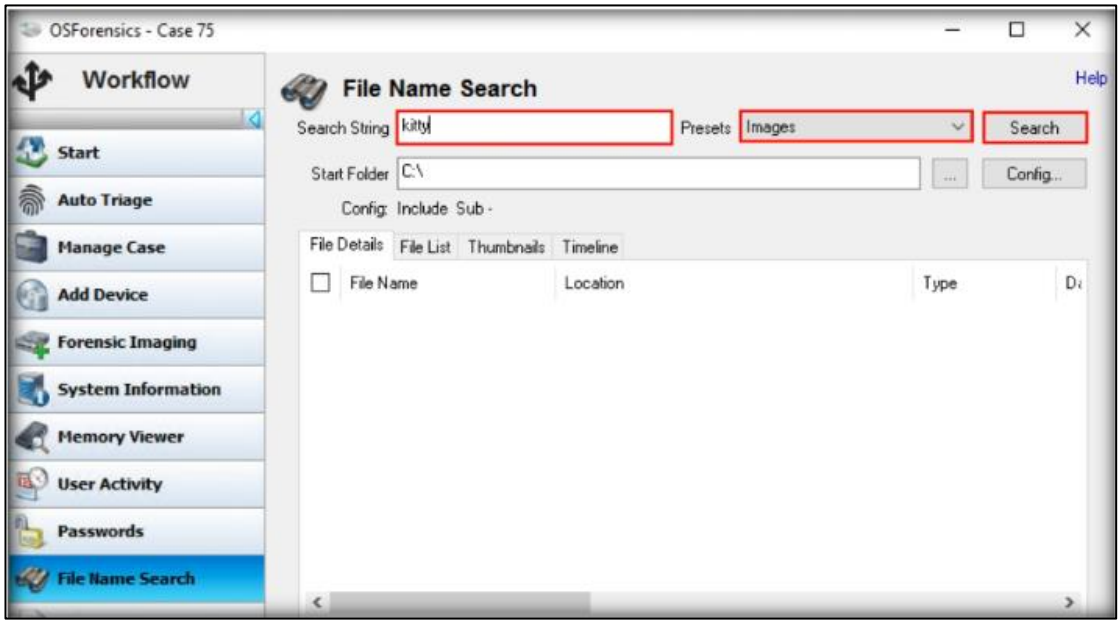


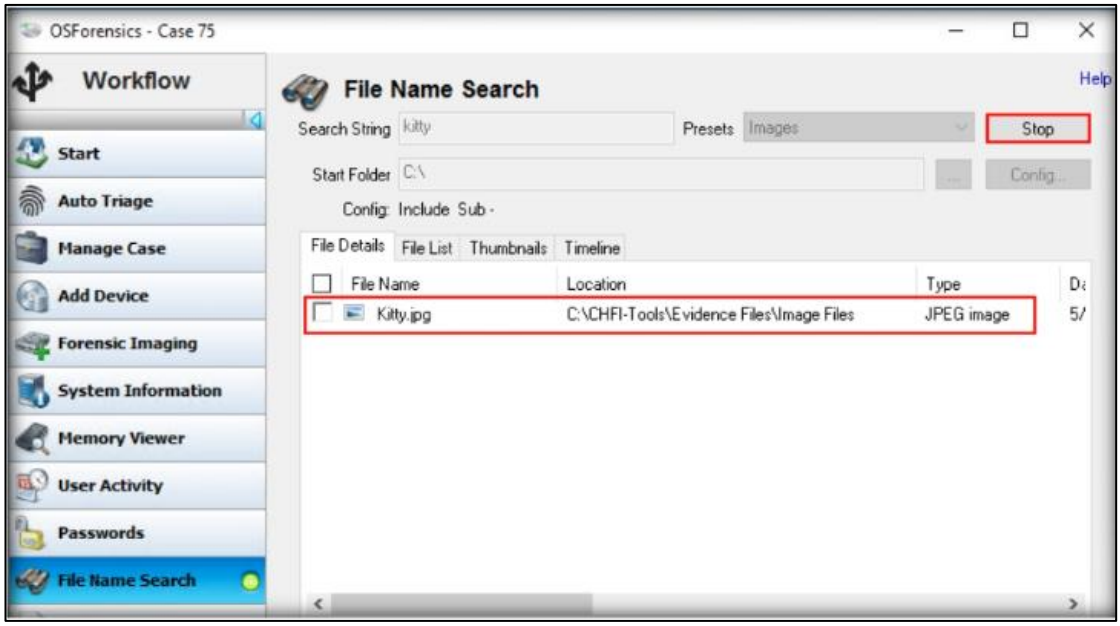
In the Start Folder field, specify the path to search for image files by clicking the ellipsis button and choosing the location (here, we are specifying the location C:\CHFI- Tools\EvidenceFiles\Image Files to search for images in it). Then, click the Search button.



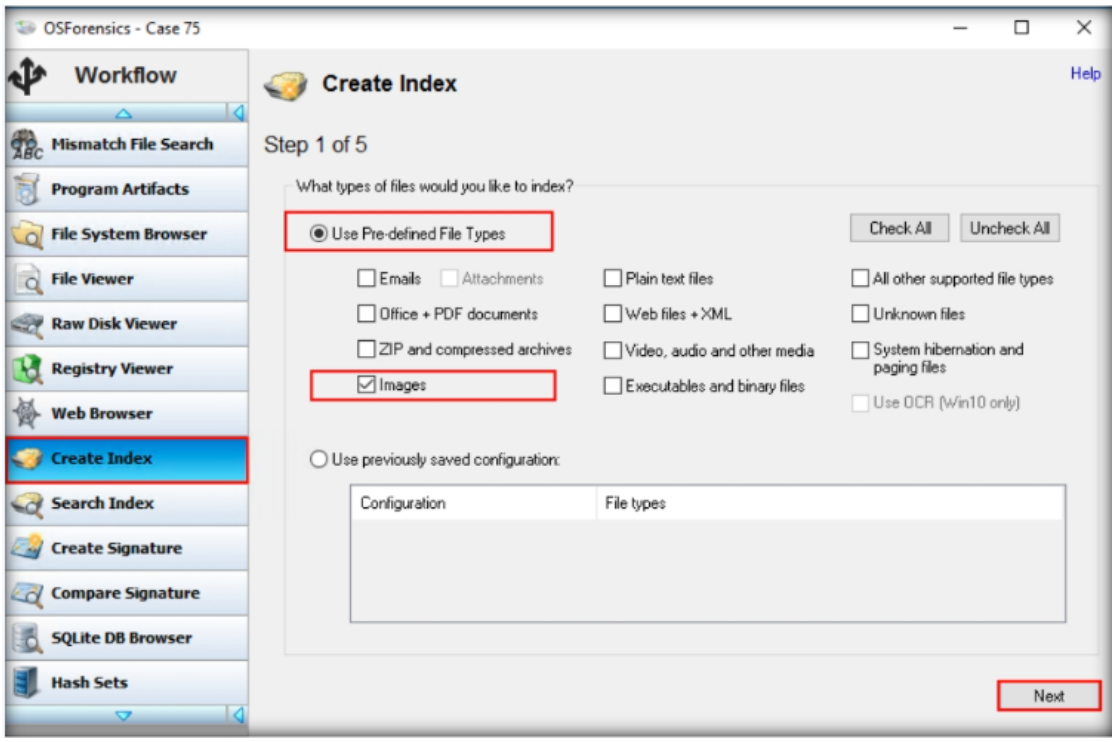


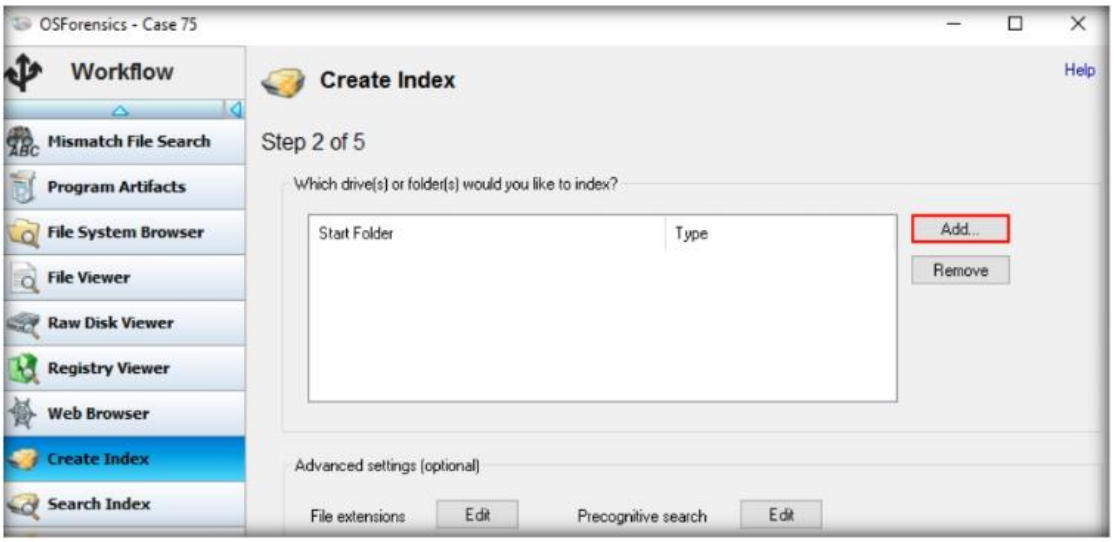
Alternatively, if you wish to search only for a single image on the entire system, select Images from the Pre-sets drop-down menu, enter the name of the desired image file in the Search String field, and then click Search, as shown in the screenshot below. Here, we are searching for the JPEG image file named Kitty.

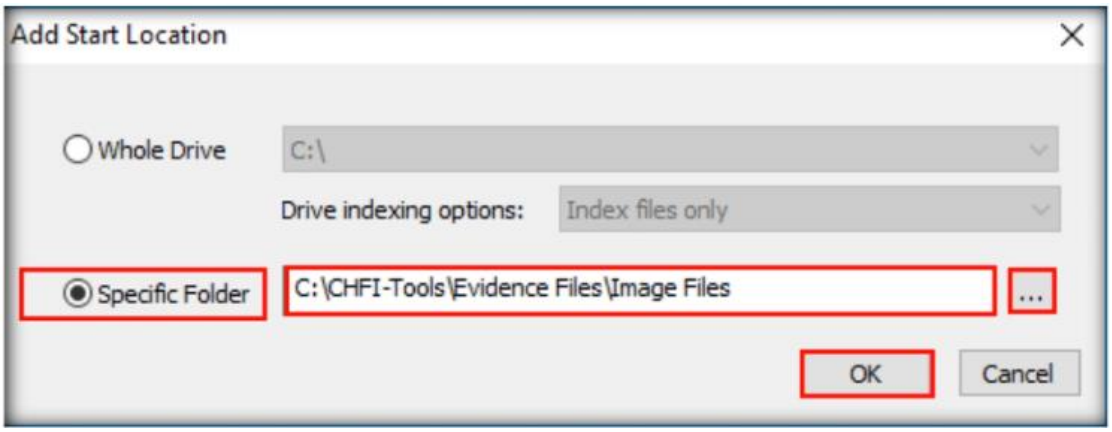


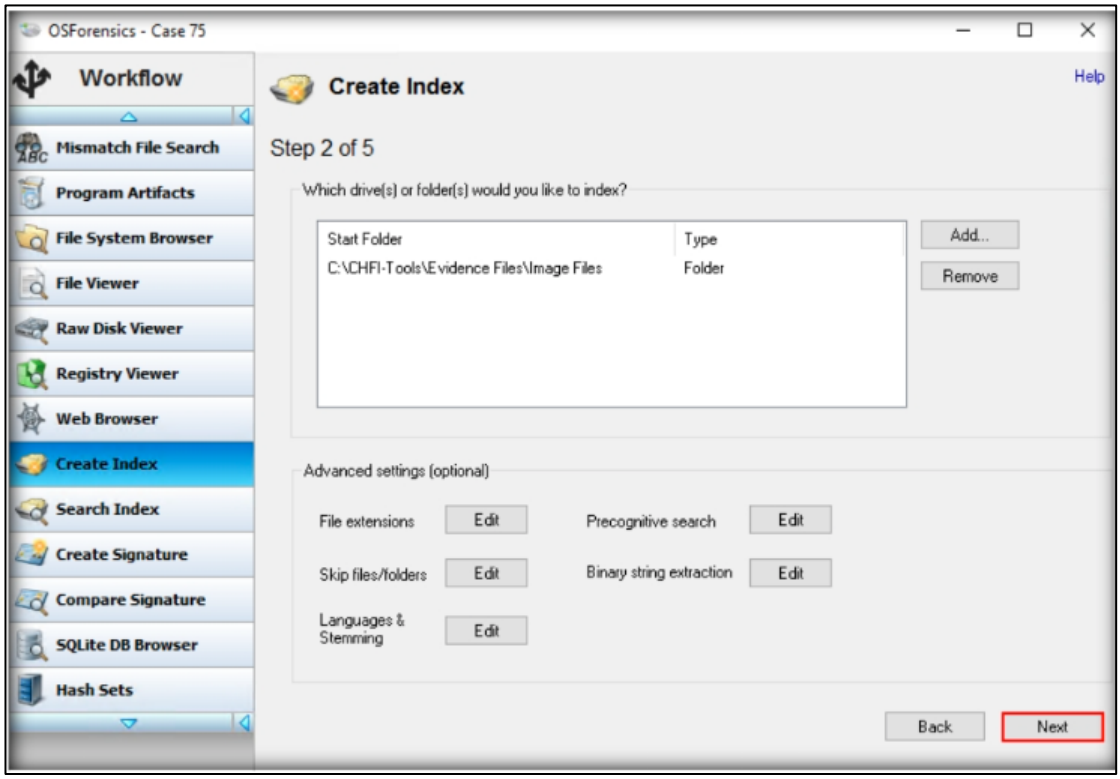


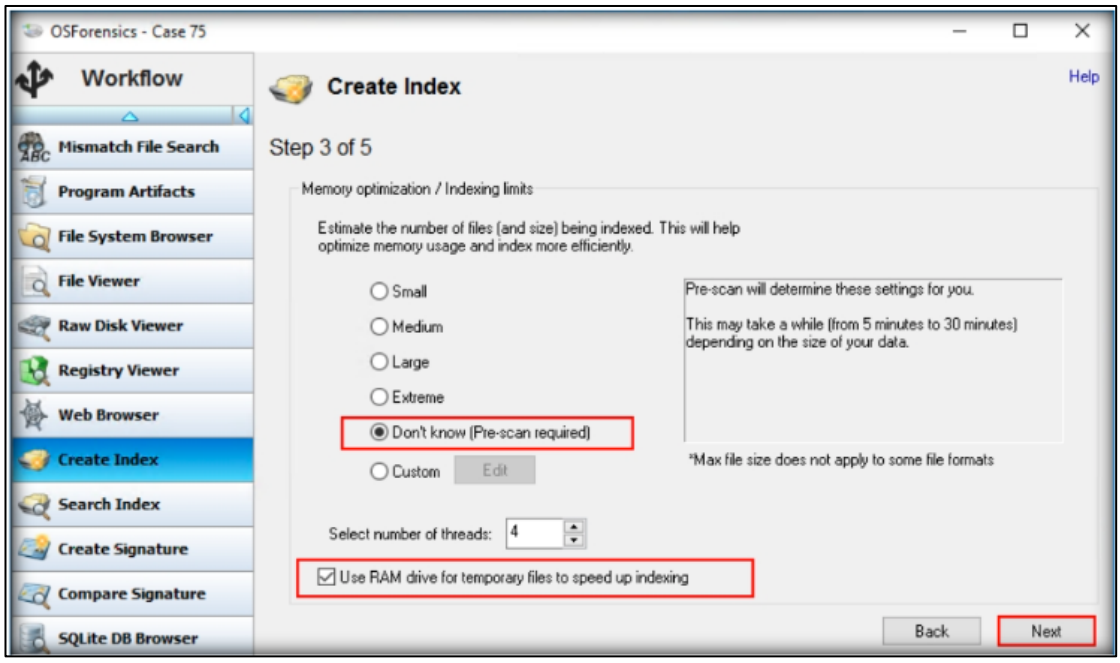
The Create Index section appears in the right pane. In this section, select the Use Pre-defined File Types option for creating the index and check the required options listed under it for selecting the file types that you wish to index (here, we have selected the Images option). Then, click Next.

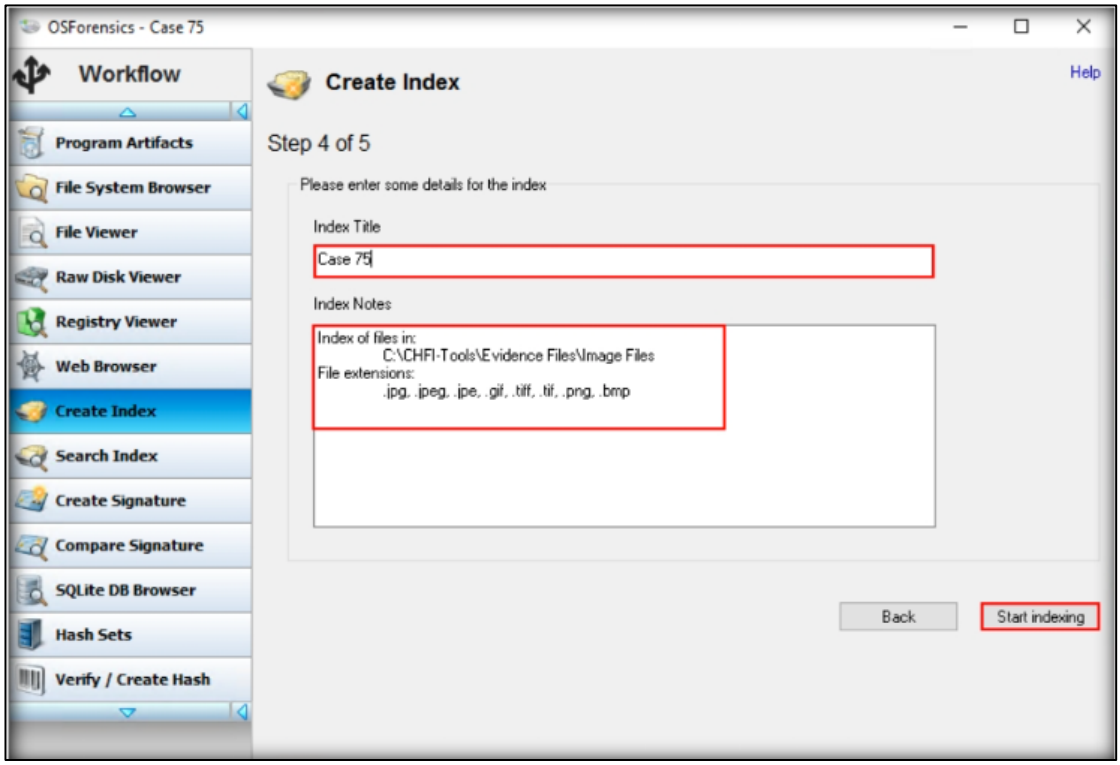

OSForensics - Case 75
Workflow
Mismatch File Search
Program Artifacts
File System Browser
File Viewer
Raw Disk Viewer
Registry Viewer
Web Browser
Create Index
Search Index
Create Signature
Compare Signature
SQLite DB Browser
Hash Sets
Create Index
Help
Step 1 of 5
What types of files would you like to index?
Use Pre-defined File Types
Check All
Uncheck All
Emails
Attachments
Plain text files
All other supported file types
Office + PDF documents
Web files + XML
Unknown files
ZIP and compressed archives
Video, audio and other media
System hibernation and paging files
Images
Executables and binary files
Use OCR (Win10 only)
Use previously saved configuration:
Configuration
File types
Next

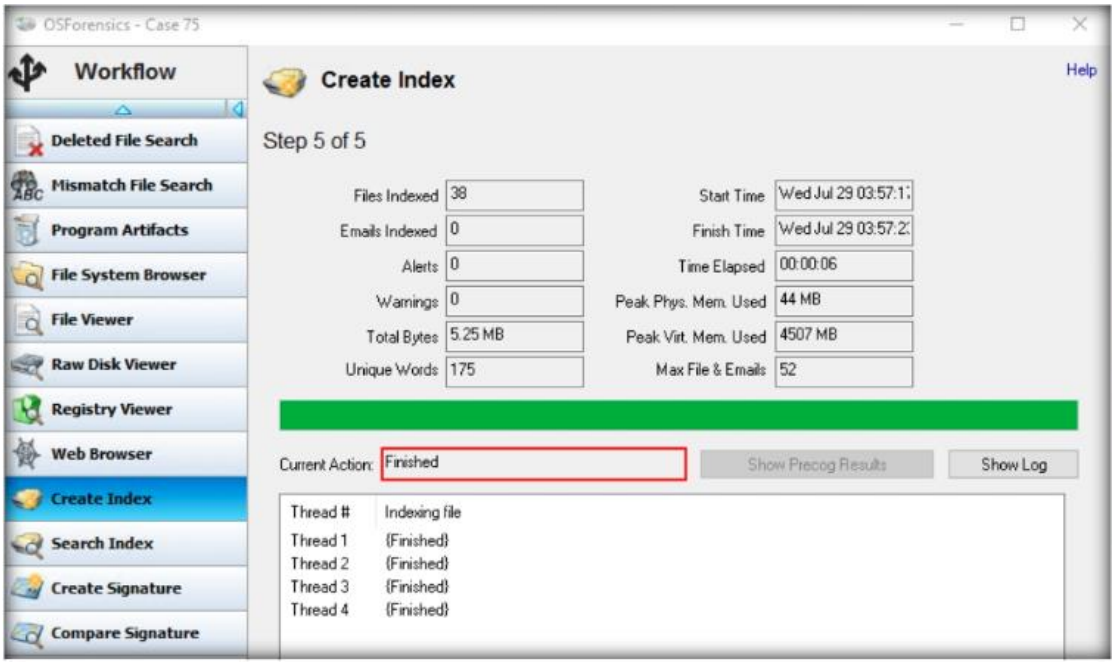

OSForensics - Case 75
Workflow
Mismatch File Search
Program Artifacts
File System Browser
File Viewer
Raw Disk Viewer
Registry Viewer
Web Browser
Create Index
Search Index
Create Index
Help
Step 2 of 5
Which drive(s) or folder(s) would you like to index?
Start Folder
Type
Add...
Remove
Advanced settings (optional)
File extensions
Edit
Precognitive search
Edit


Add Start Location
Whole Drive
C:\
Drive indexing options:
Index files only
Specific Folder
C:\CHFI-Tools\Evidence Files\Image Files
...
OK
Cancel


OSForensics - Case 75
Workflow
Mismatch File Search
Program Artifacts
File System Browser
File Viewer
Raw Disk Viewer
Registry Viewer
Web Browser
Create Index
Search Index
Create Signature
Compare Signature
SQLite DB Browser
Hash Sets
Create Index
Help
Step 2 of 5
Which drive(s) or folder(s) would you like to index?
Start Folder
Type
C:\CHFI-Tools\Evidence Files\Image Files
Folder
Add...
Remove
Advanced settings (optional)
File extensions
Edit
Precognitive search
Edit
Skip files/folders
Edit
Binary string extraction
Edit
Languages & Stemming
Edit
Back
Next

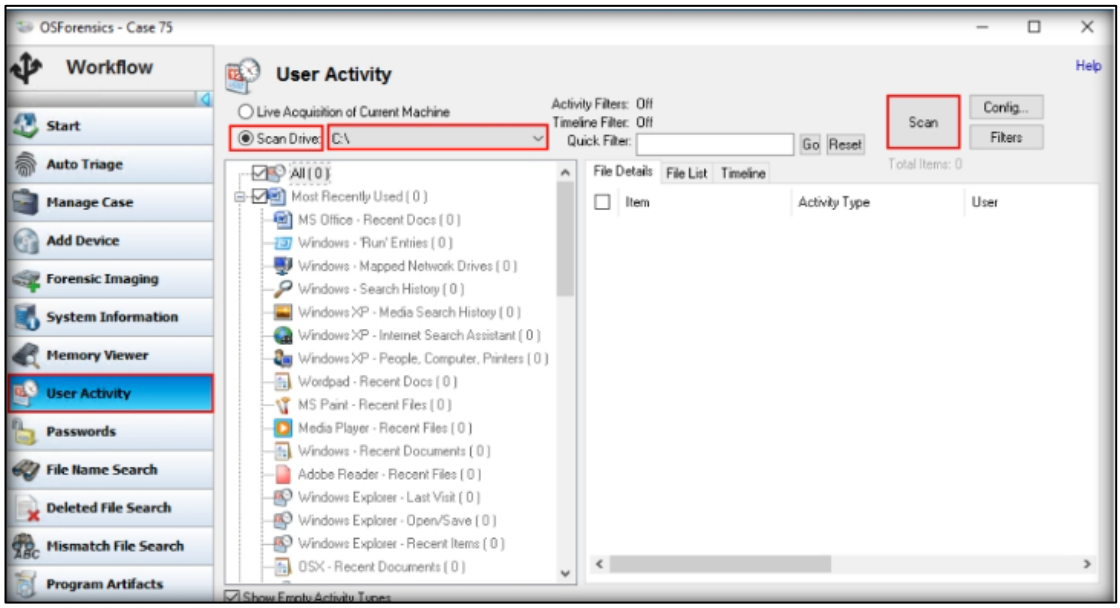

OSForensics - Case 75
Workflow
Mismatch File Search
Program Artifacts
File System Browser
File Viewer
Raw Disk Viewer
Registry Viewer
Web Browser
Create Index
Search Index
Create Signature
Compare Signature
SQLite DB Browser
Create Index
Help
Step 3 of 5
Memory optimization / Indexing limits
Estimate the number of files (and size) being indexed. This will help optimize memory usage and index more efficiently.
Small
Medium
Large
Extreme
Don't know (Pre-scan required)
Custom
Edit
Pre-scan will determine these settings for you.
This may take a while (from 5 minutes to 30 minutes) depending on the size of your data.
*Max file size does not apply to some file formats
Select number of threads:
4
Use RAM drive for temporary files to speed up indexing
Back
Next

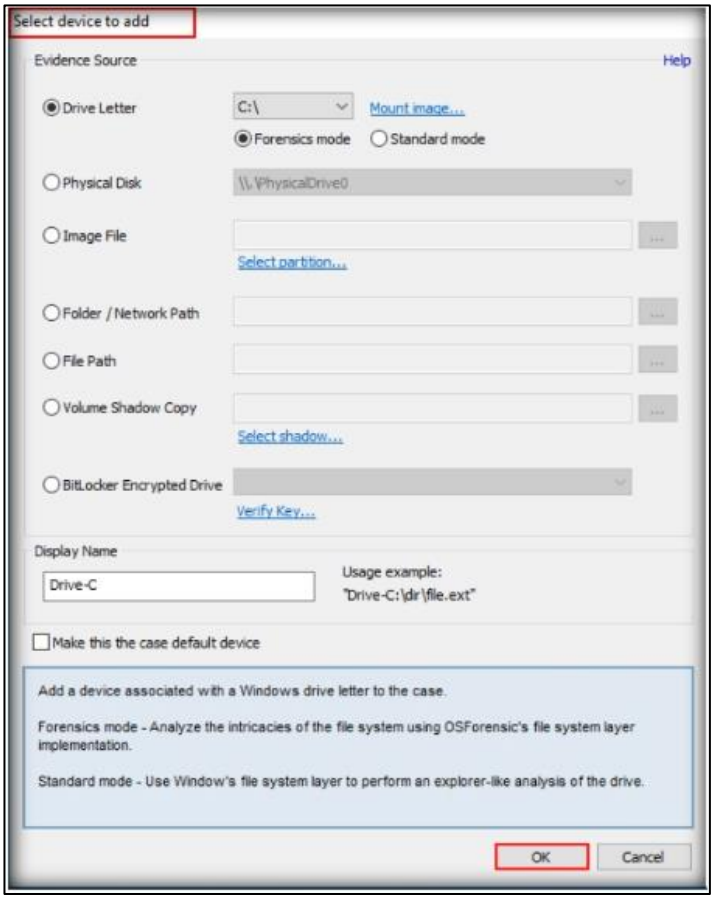


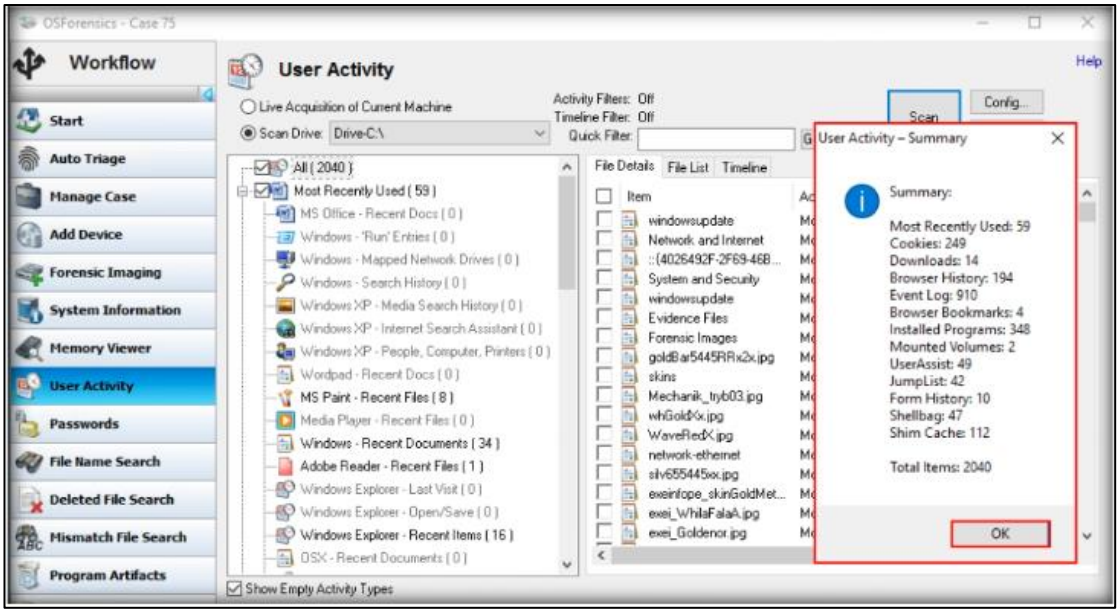


We will now search the indexed files. To search for the indexed files, select Search Index from the left pane of the tool window. The Search Index section now appears in the tool window. The index field at the top displays the name of the case we created (i.e., Case 75). Click Search. The tool will load the image files that you have indexed under the Images tab.

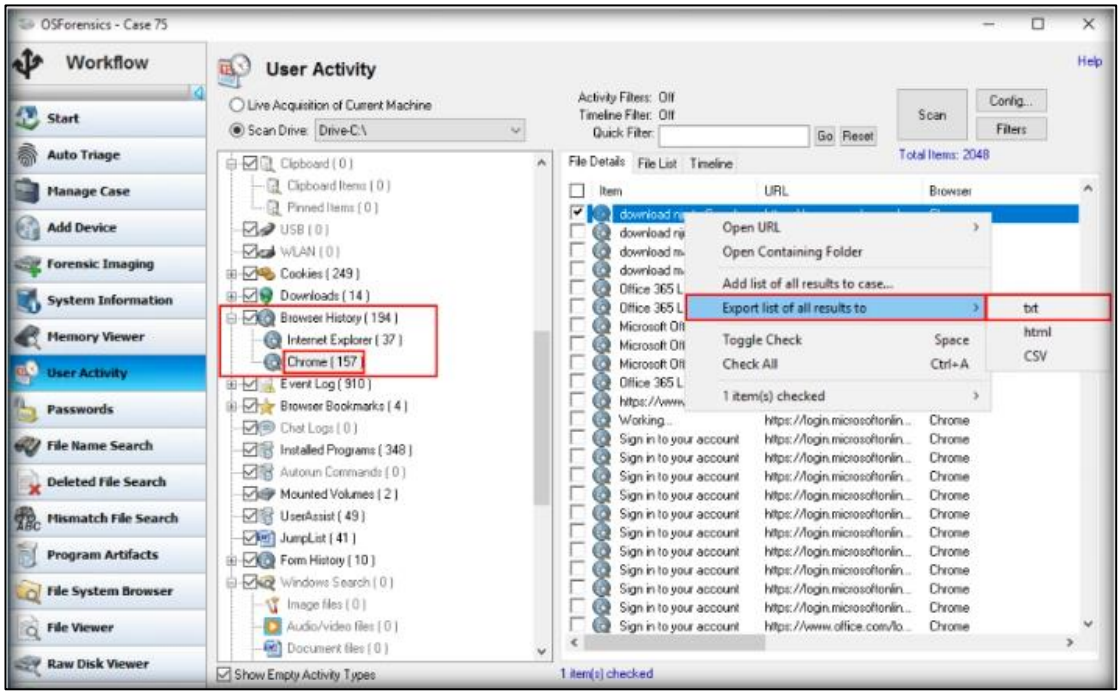
Click User Activity in the left pane to scan for evidence such as browsed websites, USB drives, recent downloads and wireless networks.



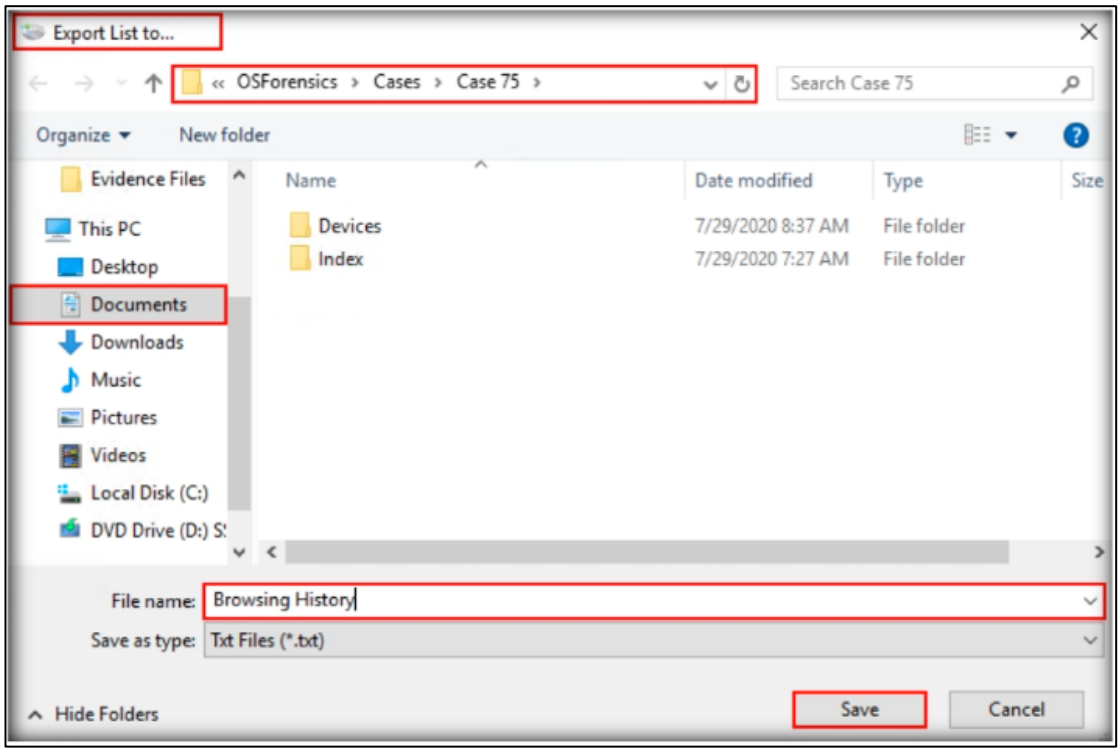




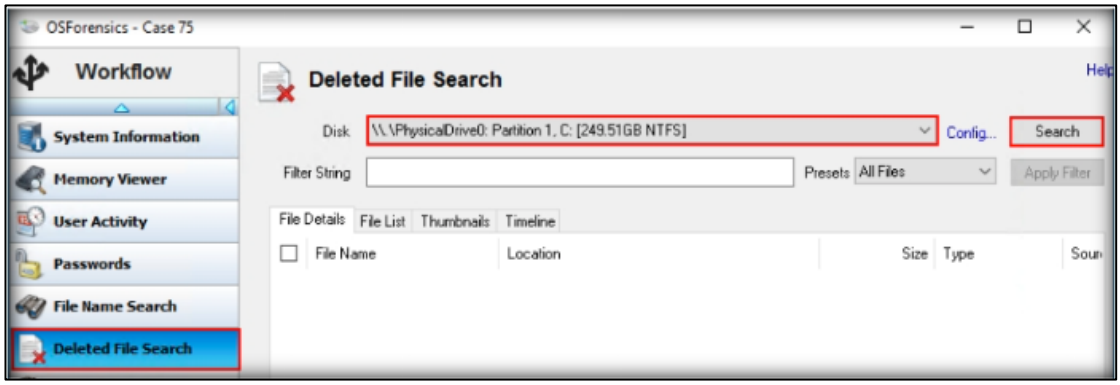
If you wish to save any of the above user-activity information on your system, such as Browser History, then scroll down the items list in the left pane below the Scan Drive option and expand the Browser History node. Select the browser for which you wish to retrieve the history (Here, we are selecting Chrome). The browser history pertaining to this browser will be displayed in the right pane of the tool window.

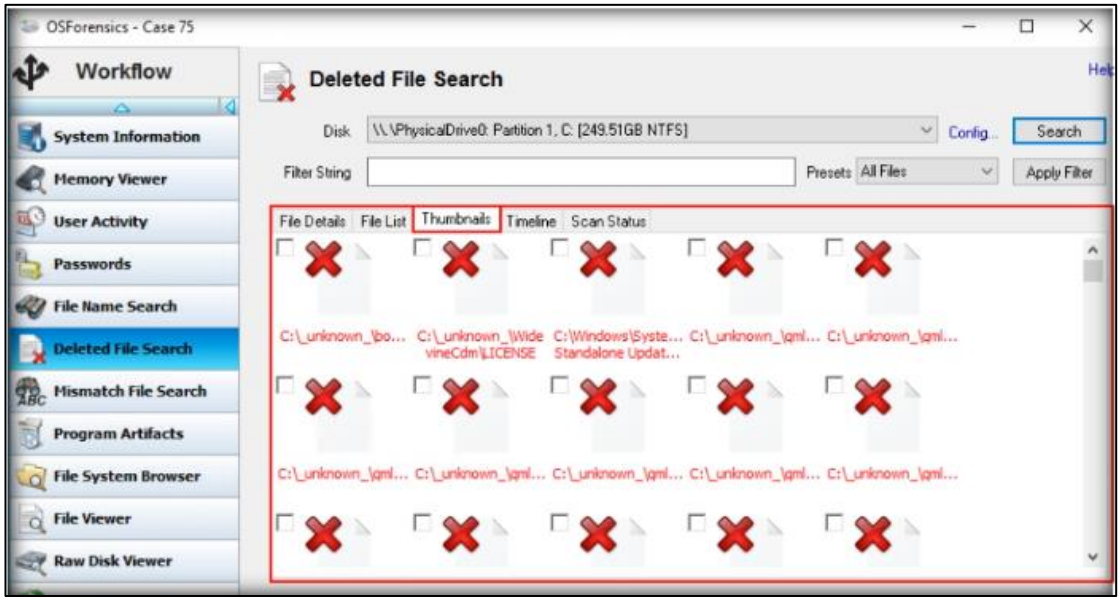


An Export List to. Window will appear. Navigate to C:\Users\Administrator\Documents\PassMark\OSForensics\Cases\Case 75, name the file (here, we are naming it as Browsing History), and click Save to export the browsing history.

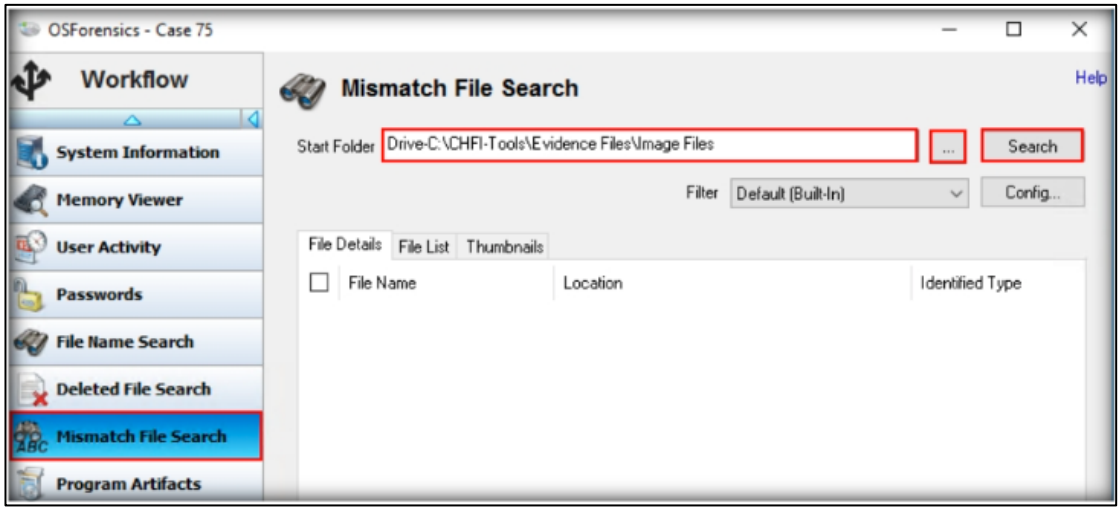


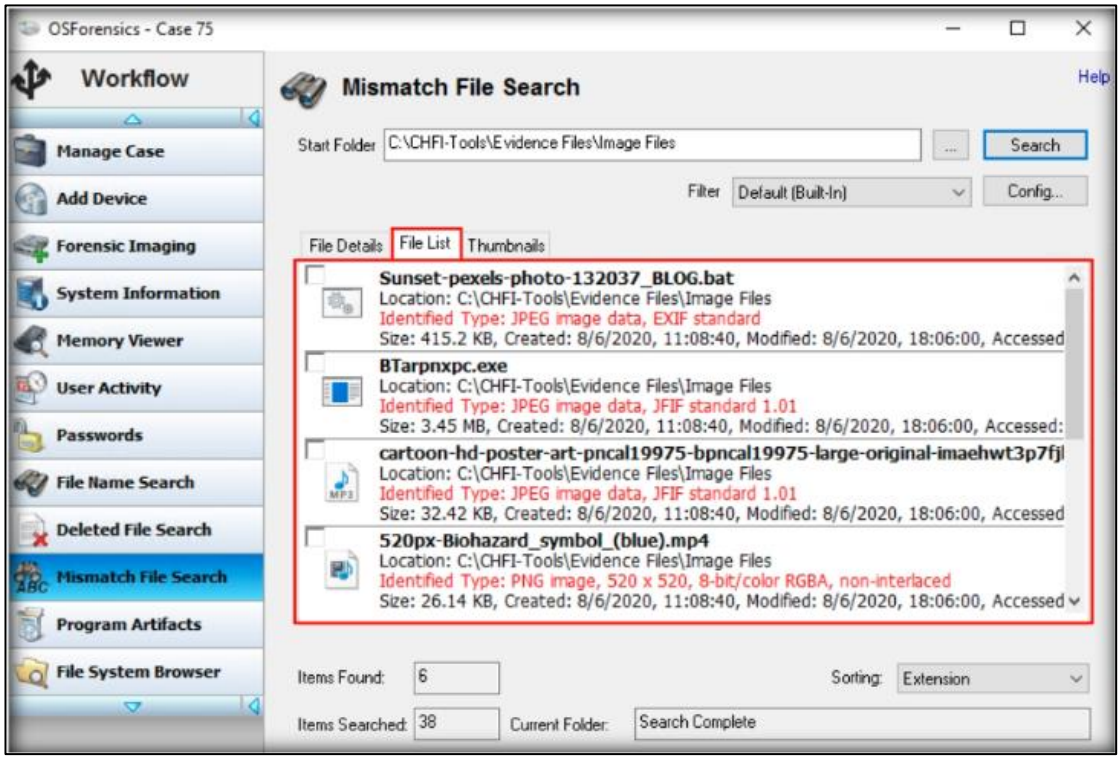
To recover deleted files from the file system, click Deleted File Search in the left pane, select a disk on which you wish to perform the deleted file search from the Disk drop-down menu, and click the search button.



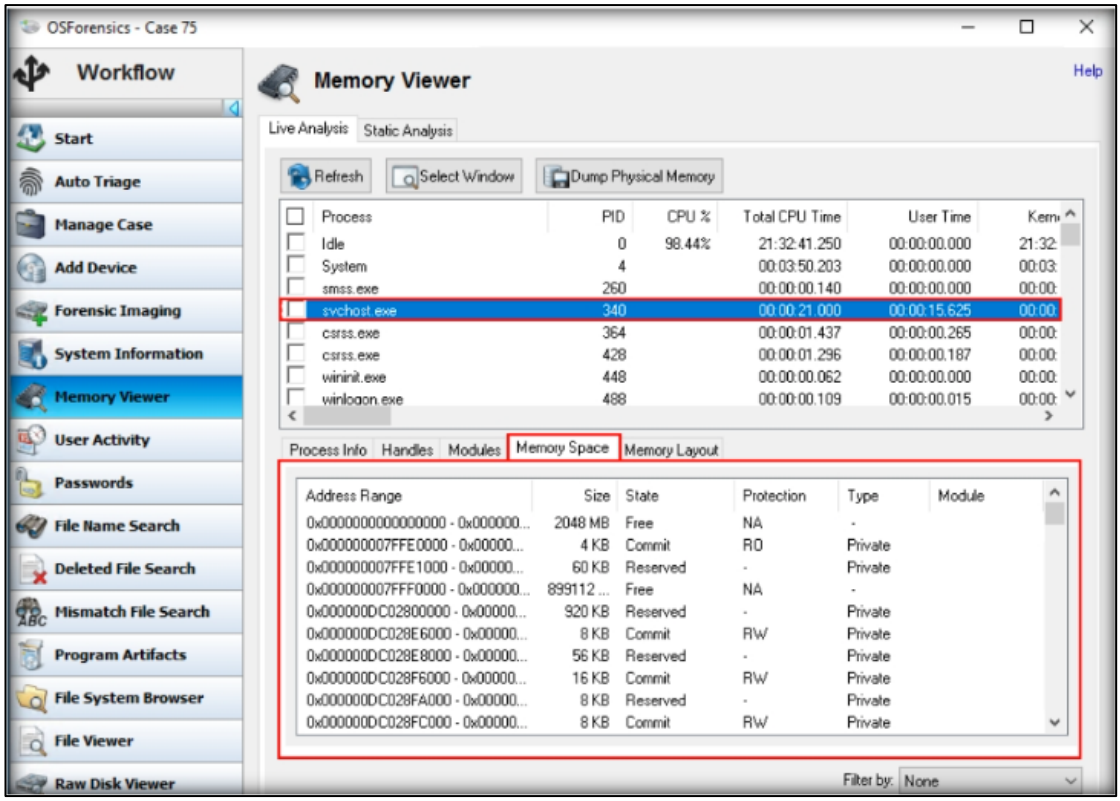


To locate files having contents that do not match the file extensions, click Mismatch File Search in the left pane of the tool window. The tool will display the Mismatch File Search section in the right pane, as shown in the screenshot:

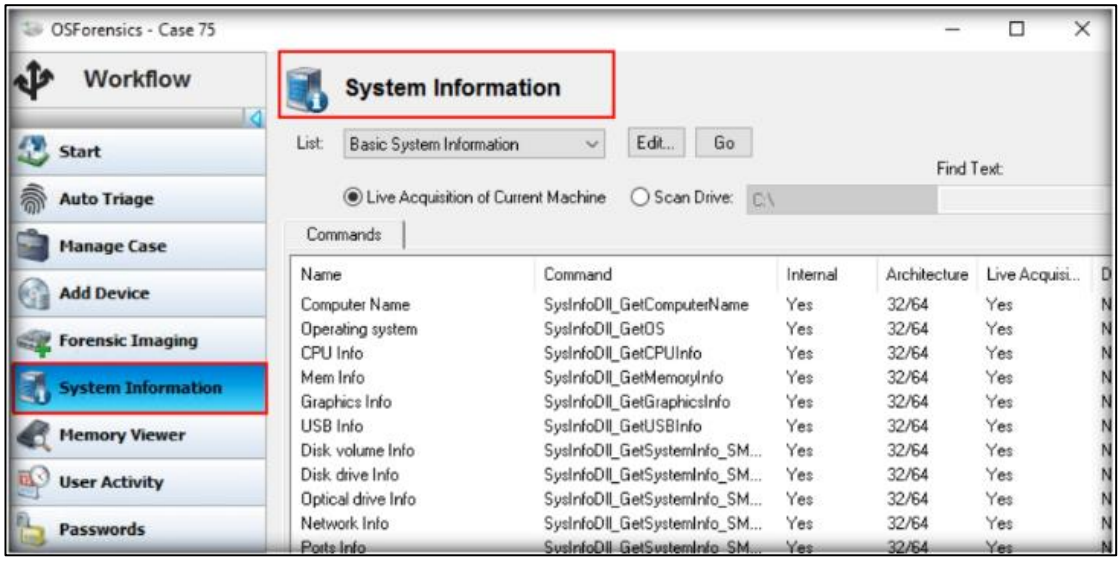




To view the processes running on the system, click Memory Viewer



To retrieve detailed information about the core components of the system, click System Information. The tool will display the System Information section.



In this manner, you can perform investigation on a system or the folders and partitions within the system to gather data of interest to the forensic investigation.

PRACTICAL3

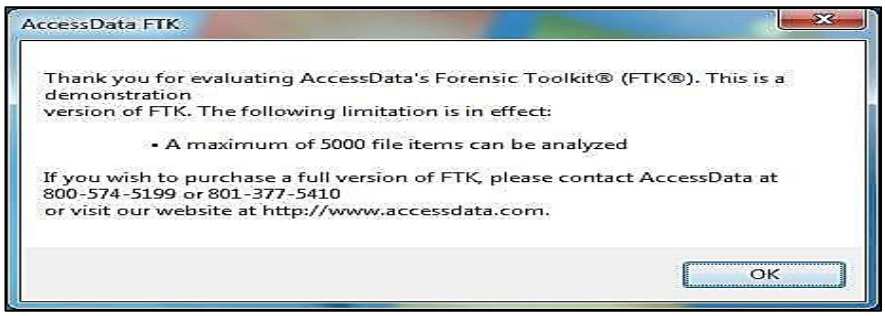
Using Forensic Toolkit (FTK) &Writing report usingFTK (AccessData FTK)

Aim: Using Windows Forensics Tools.

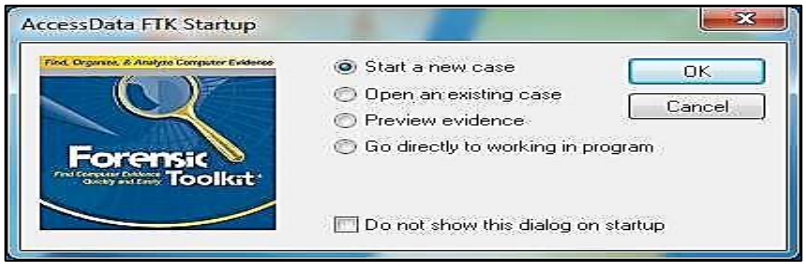
Step 1: Start Forensic Toolkit.

Step 2: Here, prompted with a warning dialog box, click on OK to continue.

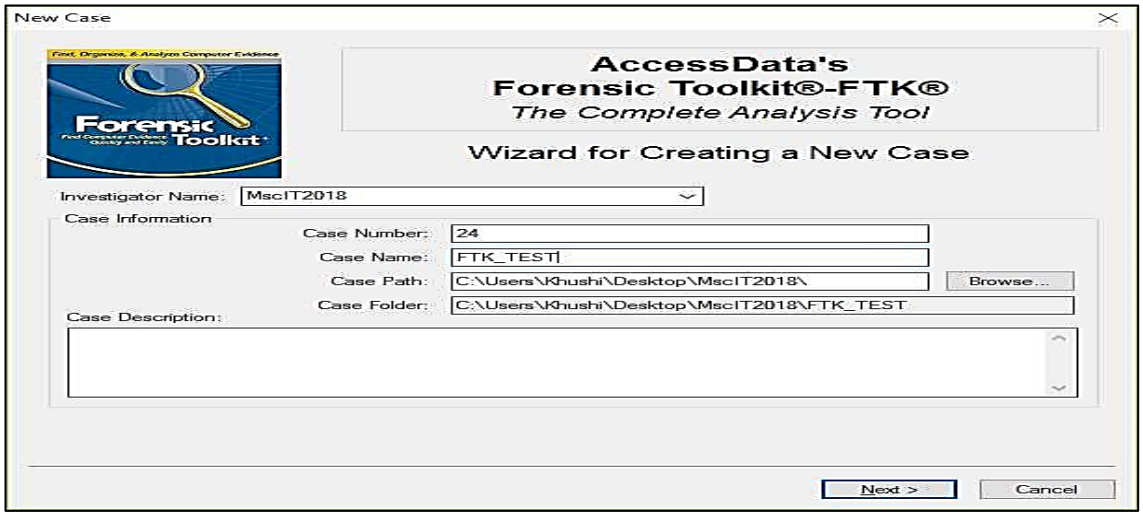
Step 3: click on OK button.



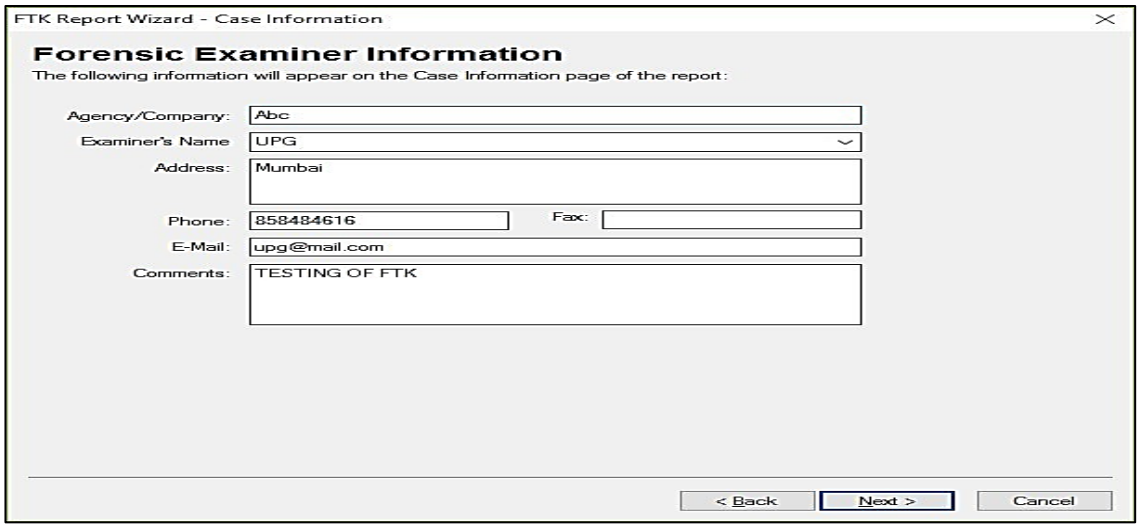
Step 4: Now select Start New Case option and click on ok.



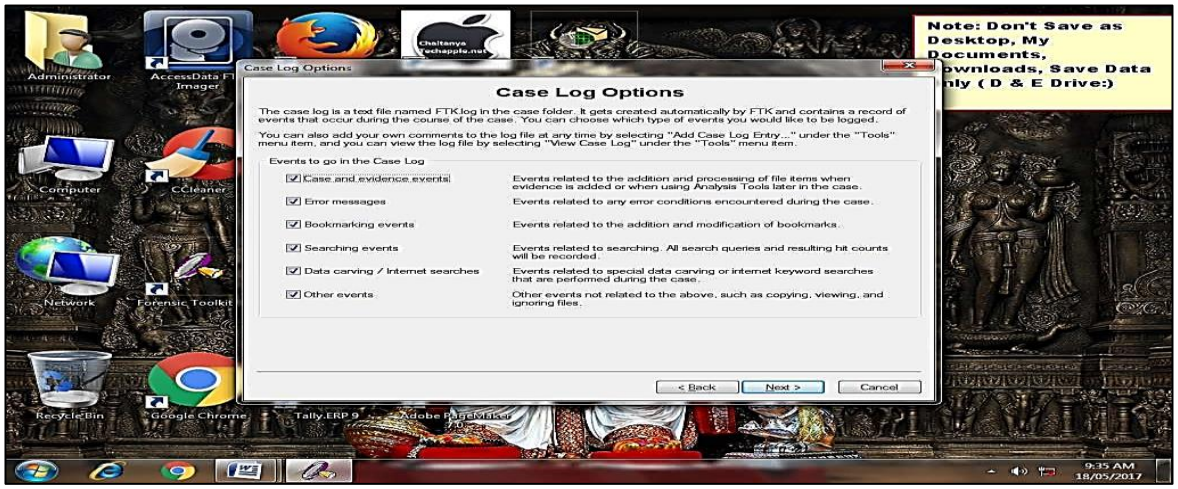
Step 5: Enter the detail for a New case.



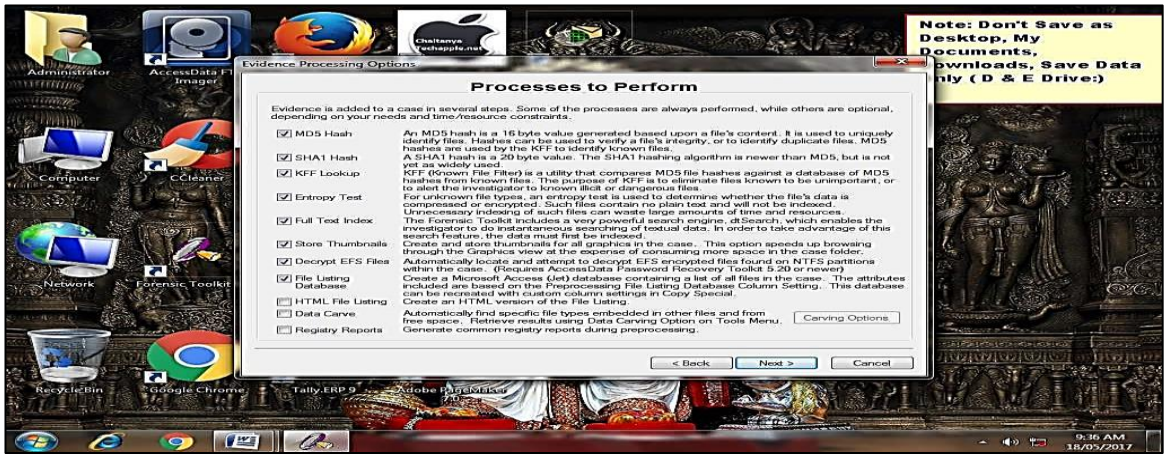
Step 6: Fill the information in Forensic Examiner Information dialog box.



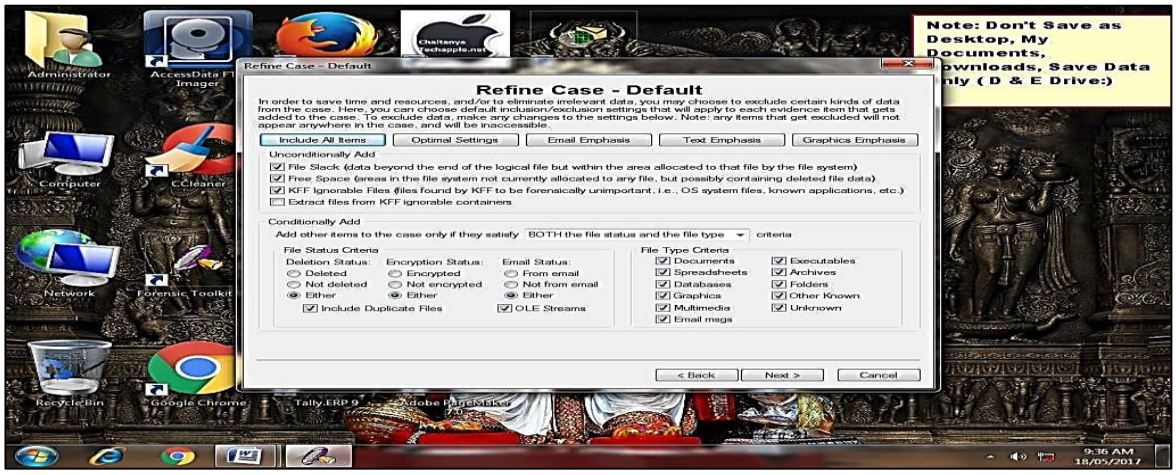
Step 7: leave the default settings and click on next.



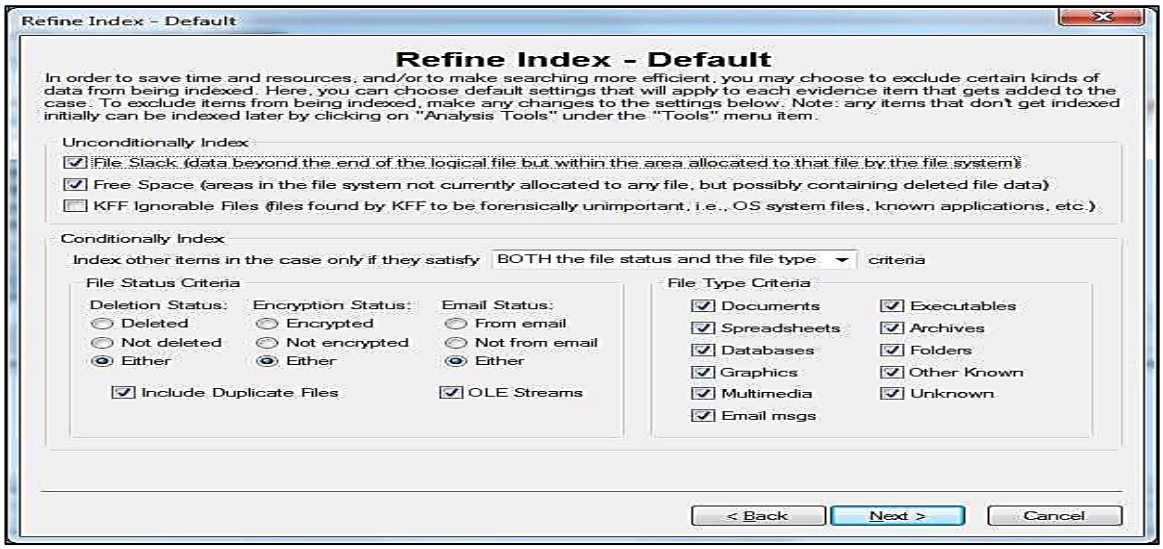
Step 8: Now again leave the default settings and click on next.



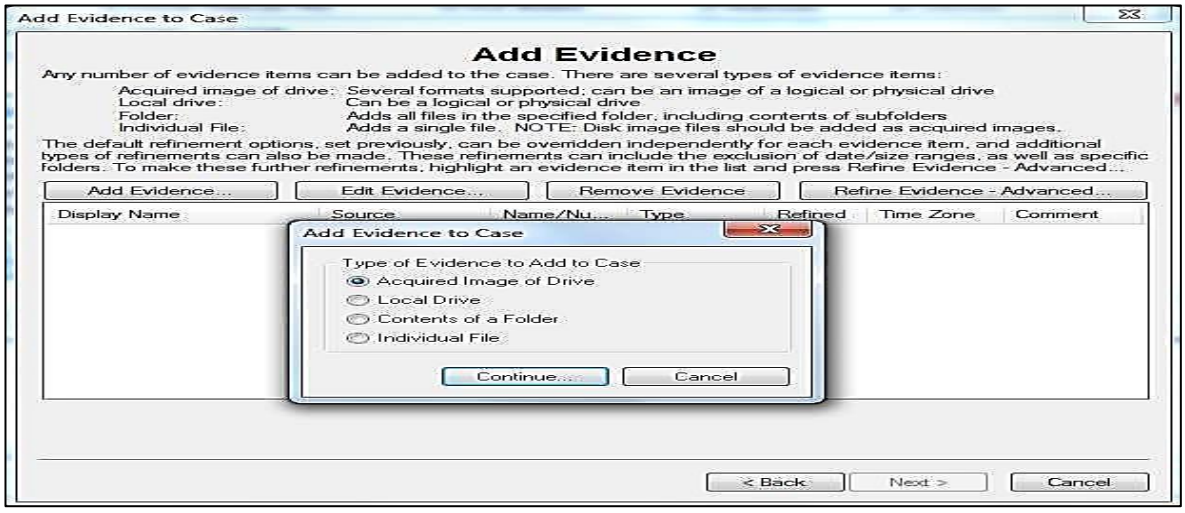
Step 9: In the Refine Case-Default, click the Include All items button and then click Next.



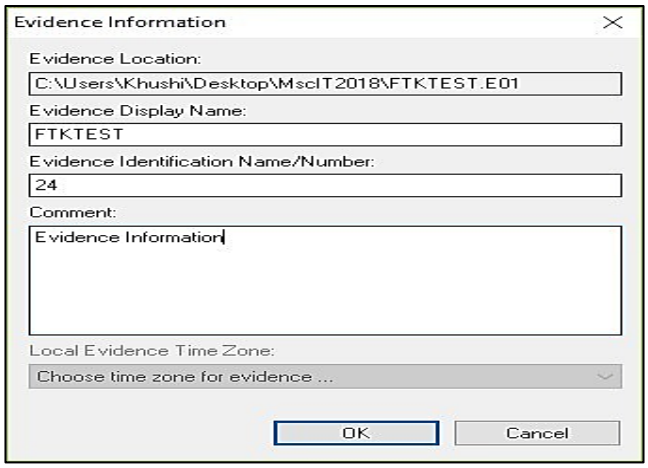
Step 10: In Refine Index-Default, accept the default settings and click Next.



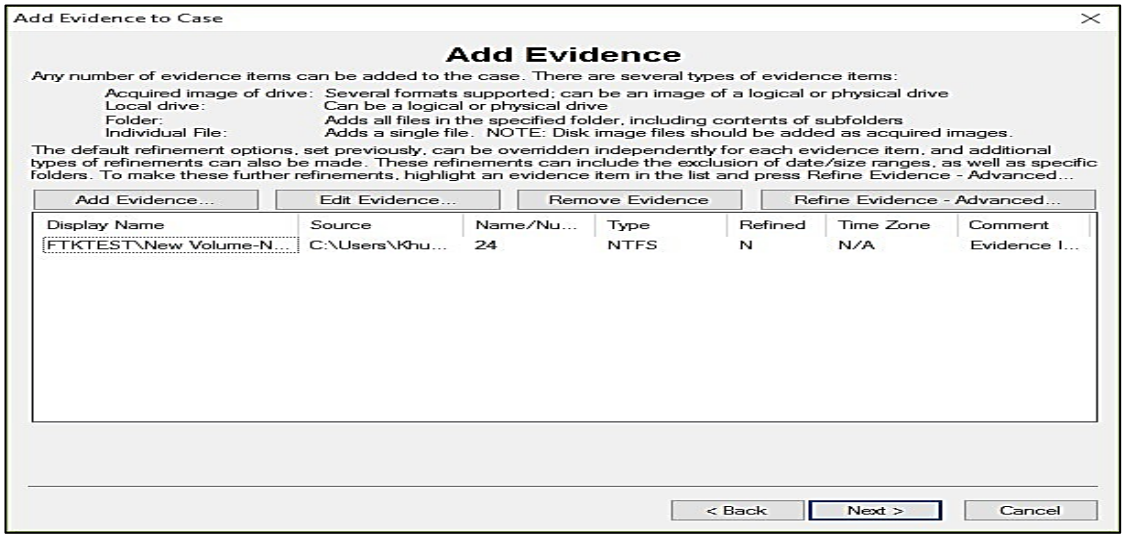
Step 11: Now here Click on add Evidence button.



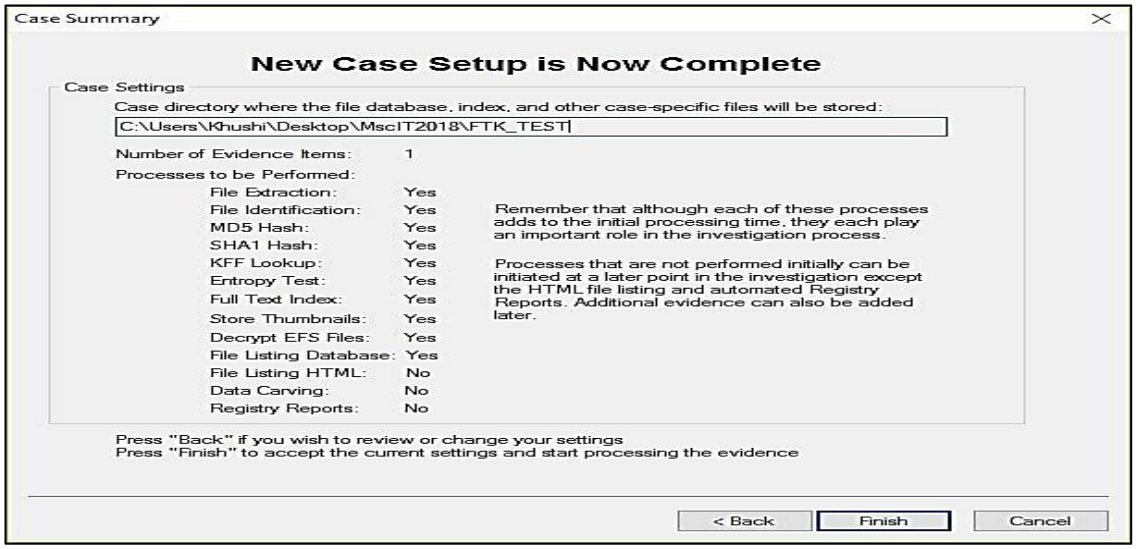
Step 12: Enter Evidence Information and click on OK button.



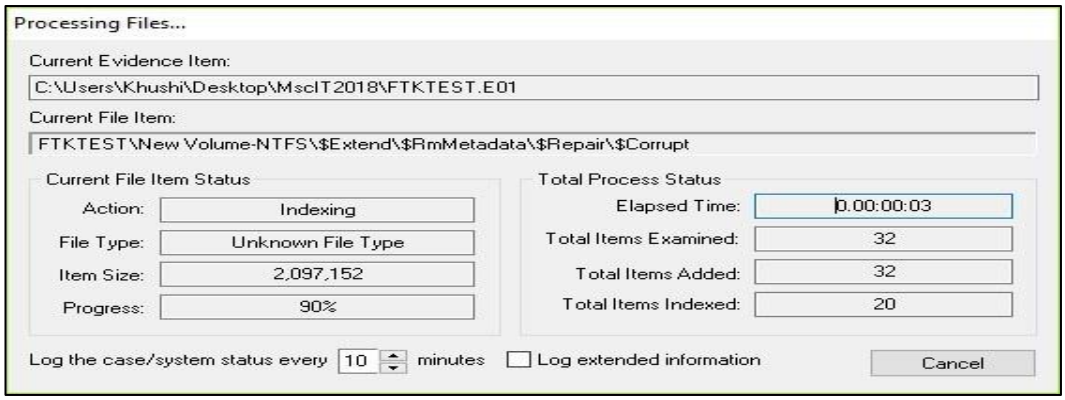
Step 13: Now click on Next.



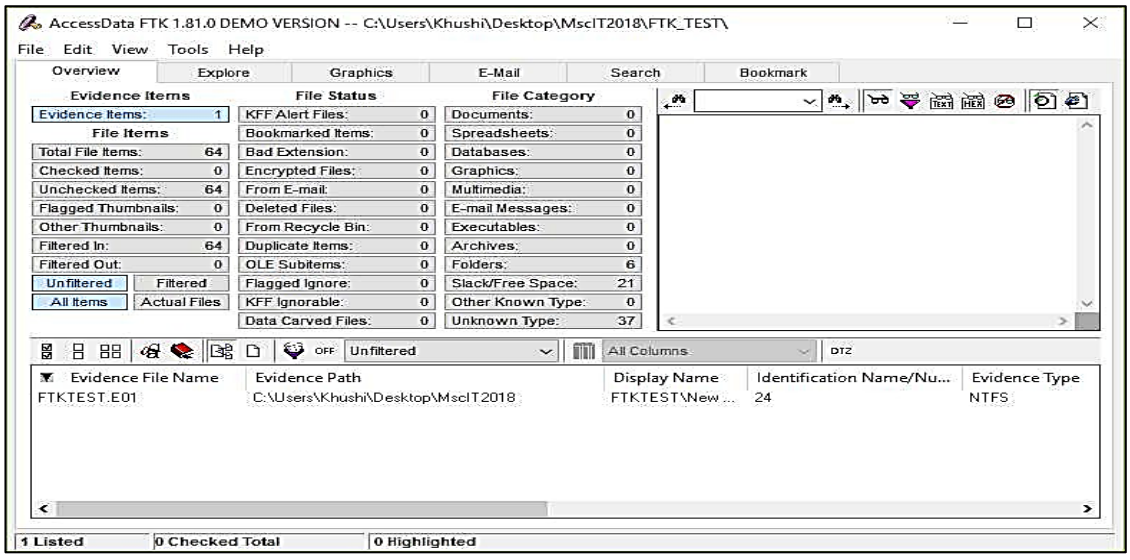
Step 14: Click on Finish to initiate the analysis.



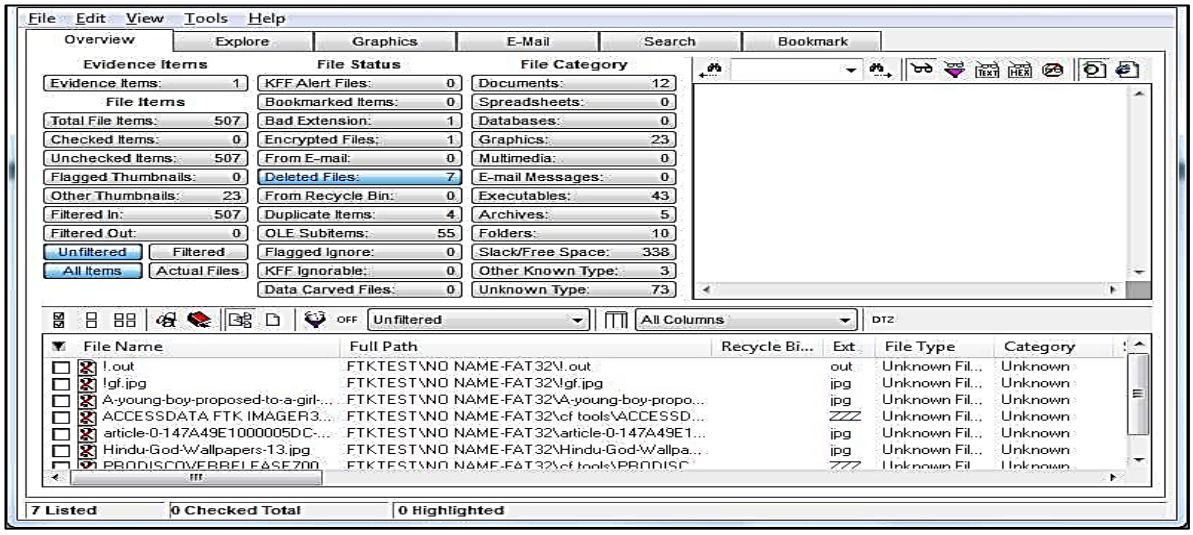
Step 15: Now Processing Will Start.....



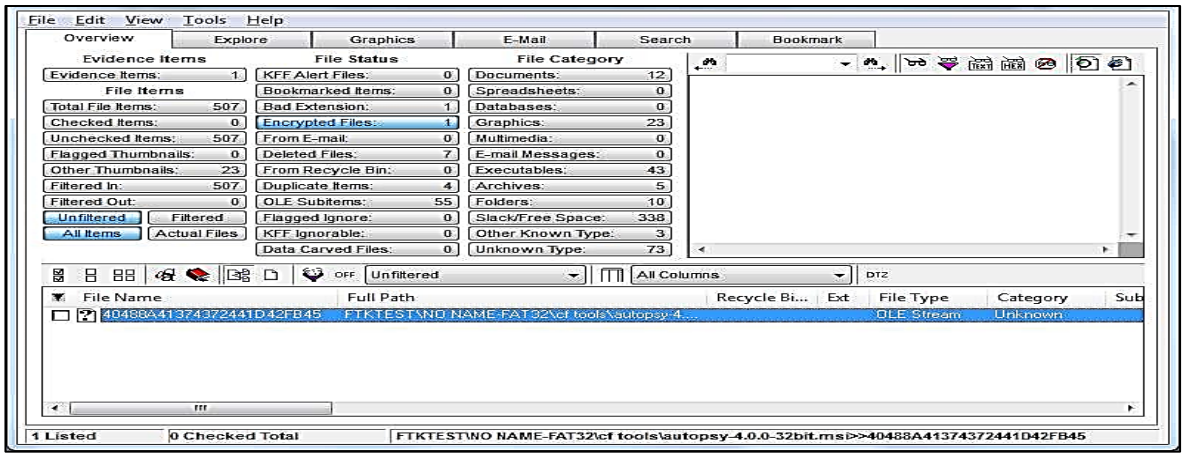
Step 16: when FTK finishes the processing part, the FTK window opens to the Overview tab.



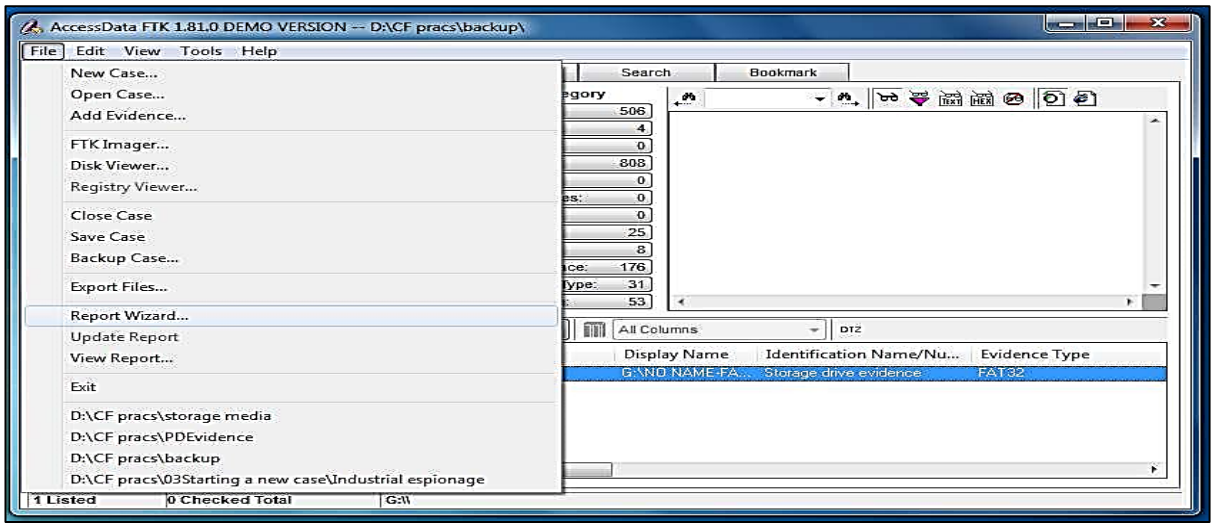
Step 17: Select Deleted Files option to explore the evidence items.

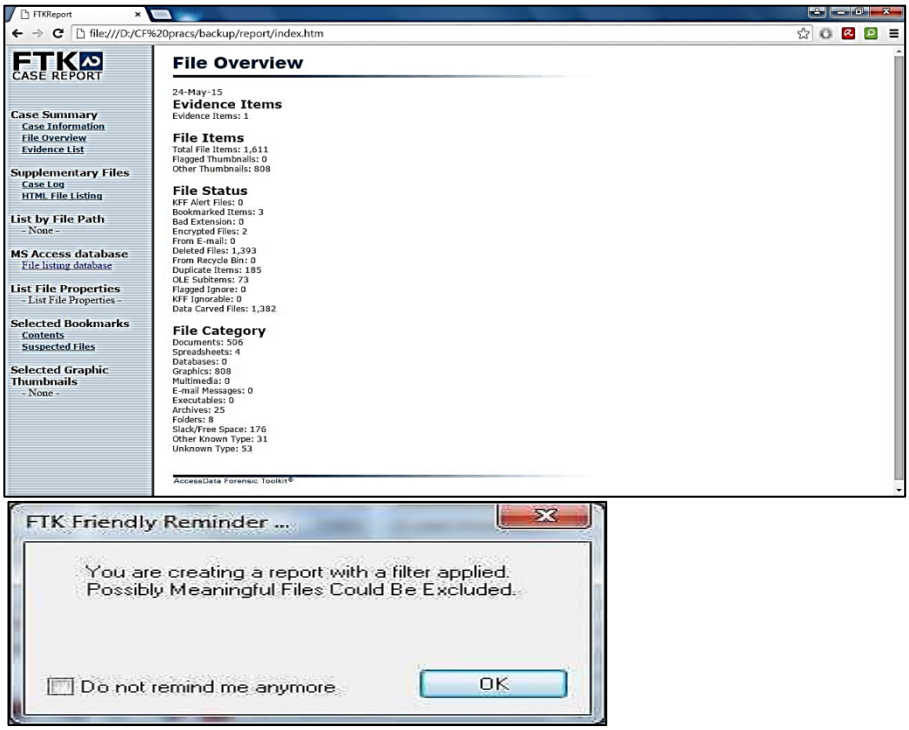


Step 18: Select Encrypted Files to view.

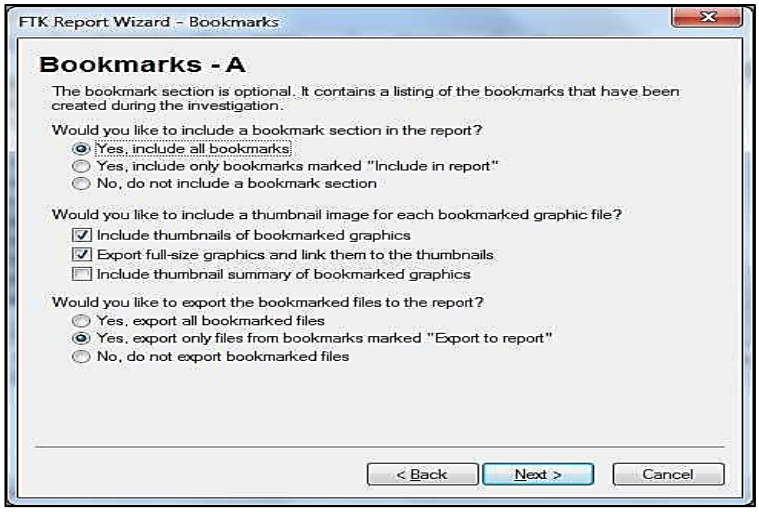


From the menu, select Report, and then Generate Report or click the button on the toolbar.





The Case Information dialog appears, enter the Case information and The Bookmarks-A & B dialog appears select what you want to include in report click next.



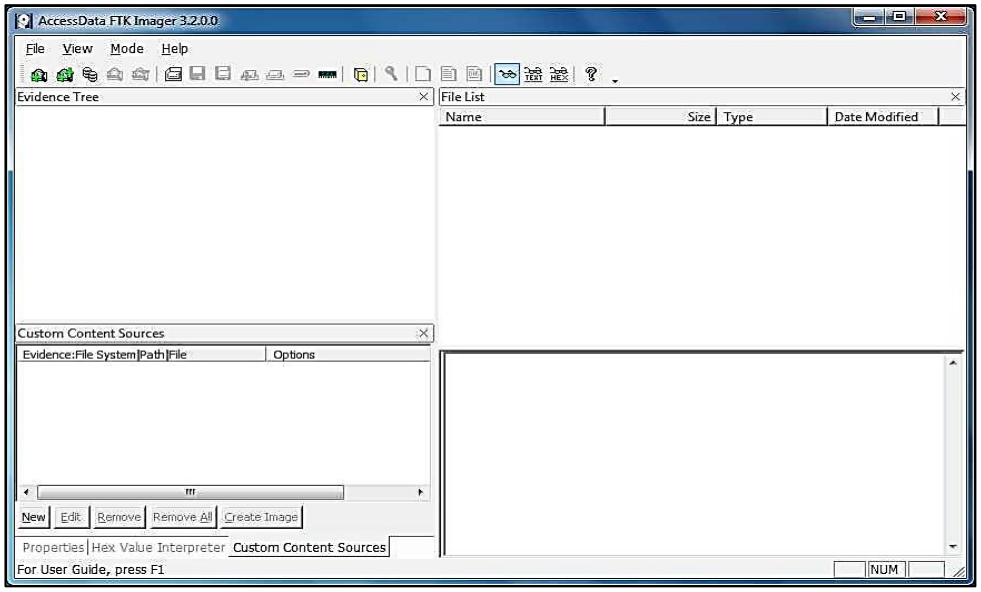
List File Properties dialog appear, include the list you want in Report and click next and Finish.

PRACTICAL 4

Using File Recovery Tools [FTK Imager] Creating Image

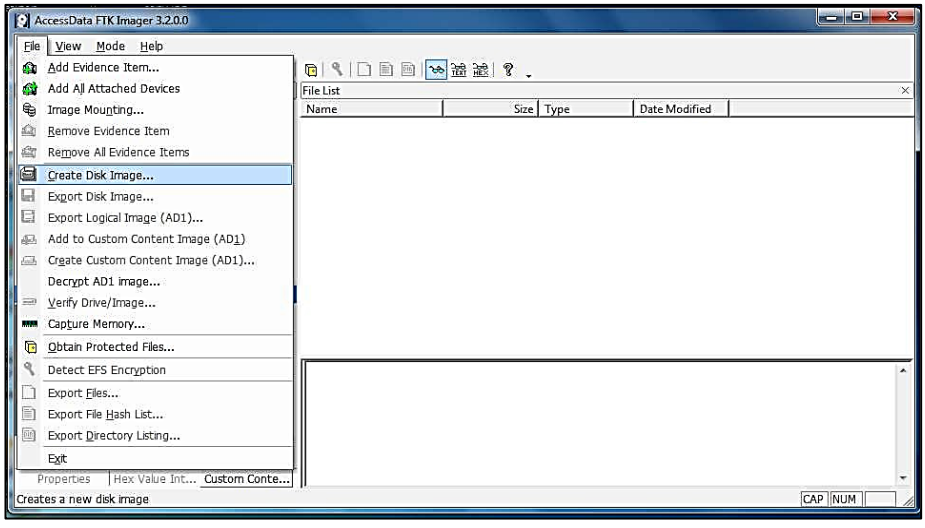
Aim: A) Understanding & working with the process of the process of taking a drive image using AccessData's FTK Imager tool.

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



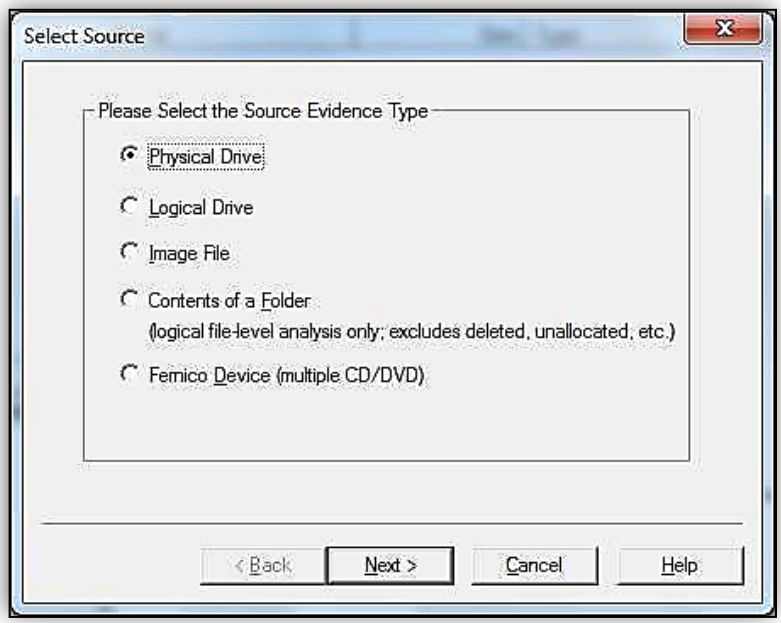
Step 2) To create a forensic image:

Click File > Create Disk Image

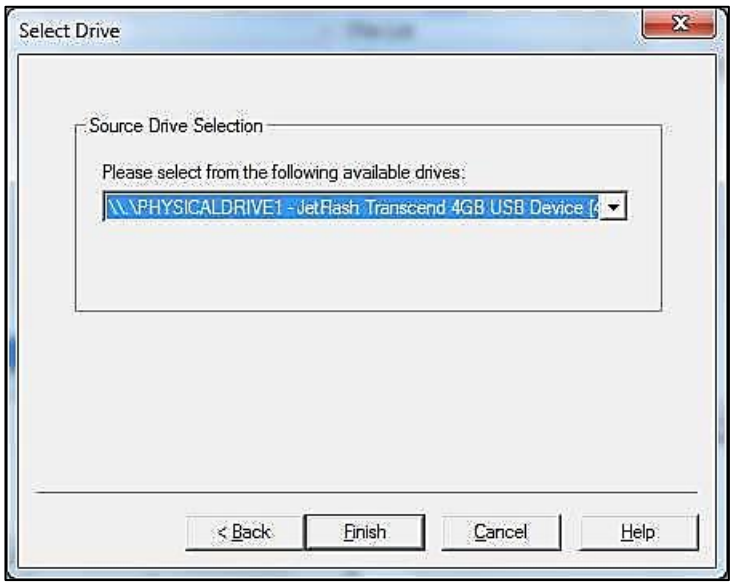


Step 3) In the Select Source dialog box, select the source you want to make an image of. Click Next.

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



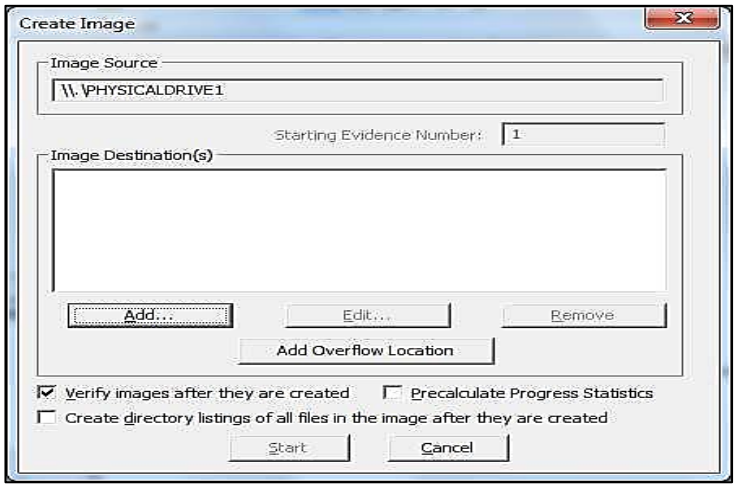
Step 4) Select the drive or browse to the source of the image you want, and then click Finish.



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

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

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

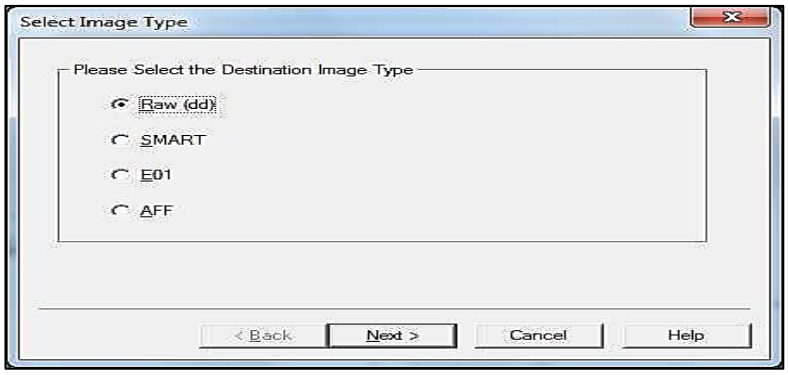


Step 6) Select the type of image you want to create.

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

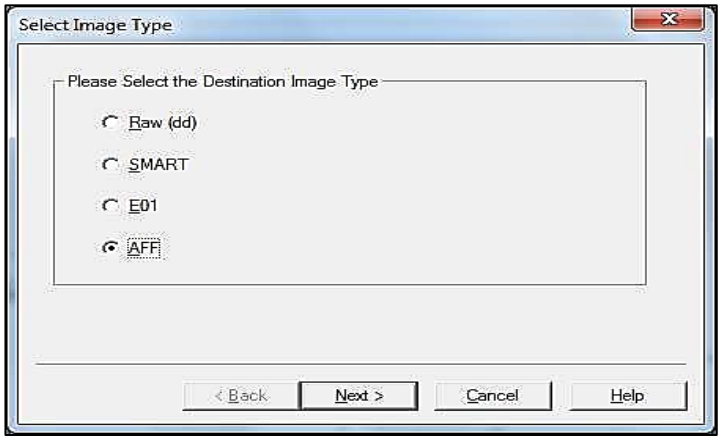
Note: If you are creating an image of a CD or DVD, this step is skipped because all CD/DVD images are created in the IsoBuster CUE format. Hashes are not generated for CD and DVD images so they will not be verified, as well.

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

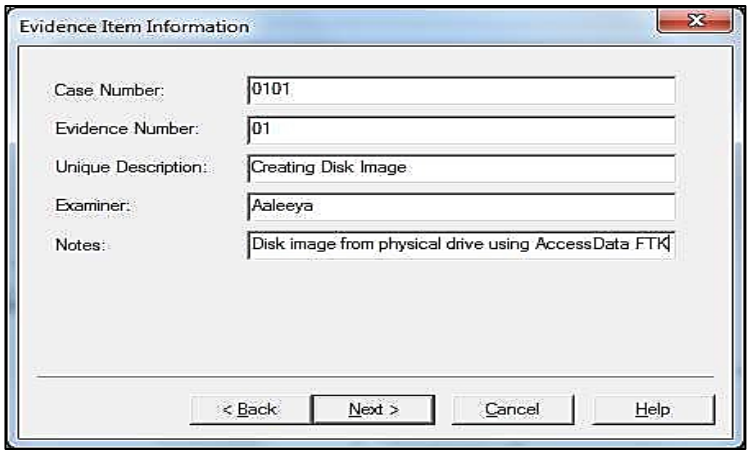


Step 7) If you are creating an AFF image type, choose AFF. Click Next.

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



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



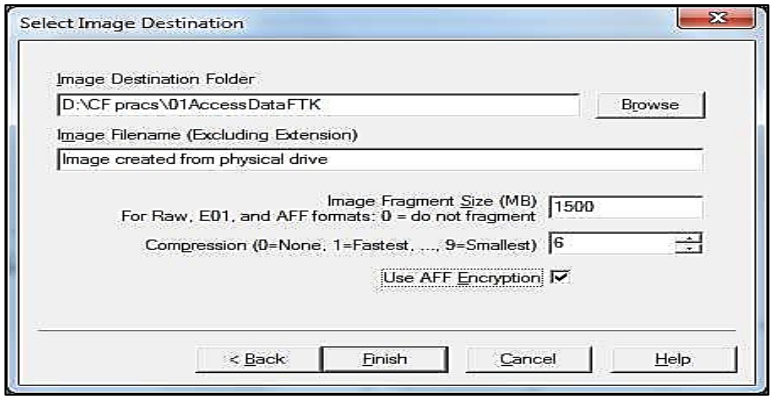
Complete the fields in the Evidence Item Information dialog. Click Next.

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

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

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

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



Step 10) Specify the Image fragment Size:

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

Step 10 a) Select the compression level to use.

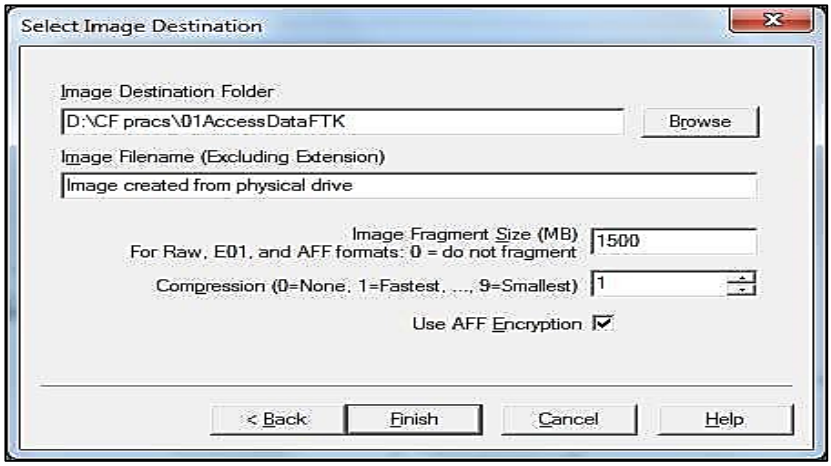
- 0=No Compression
- 1=Fastest, Least Compression (faster, and also slightly smaller than a 0-compression file)
- 9=Slowest, Most Compression (smallest file, slowest to create).

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

Step 11) To encrypt the image, choose the correct encryption box as explained below:

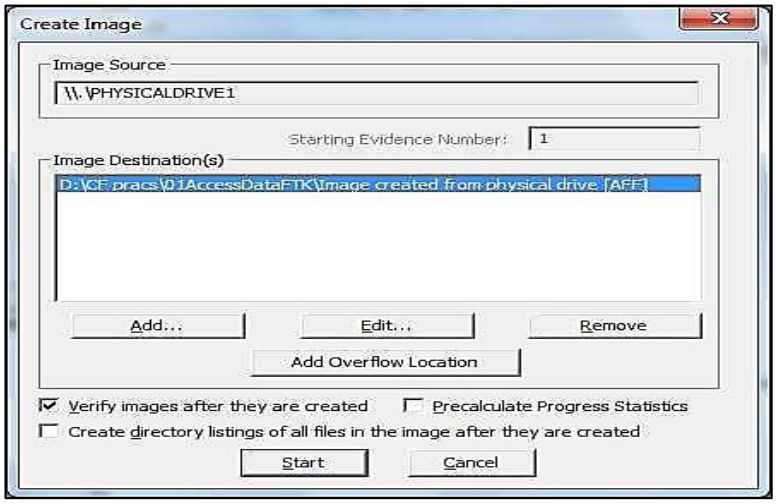
a. To encrypt the new image with AD Encryption, mark the Use AD Encryption box.
b. To encrypt the new image with AFF Encryption, mark the Use AFF Encryption box.

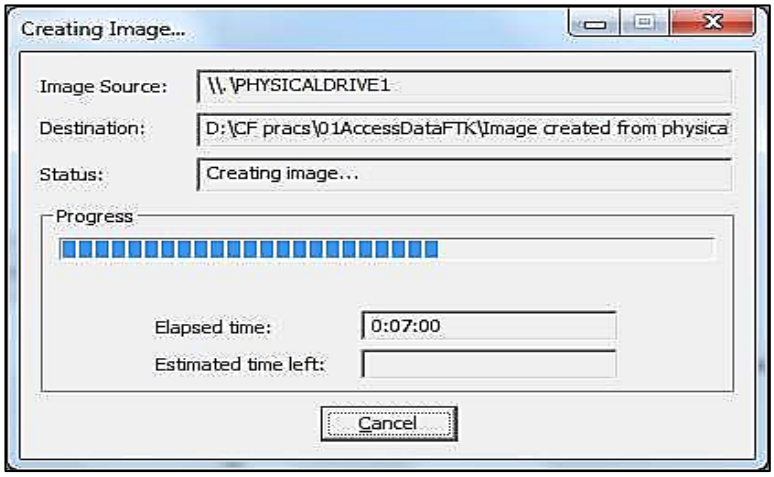
Step 12) Click Finish.



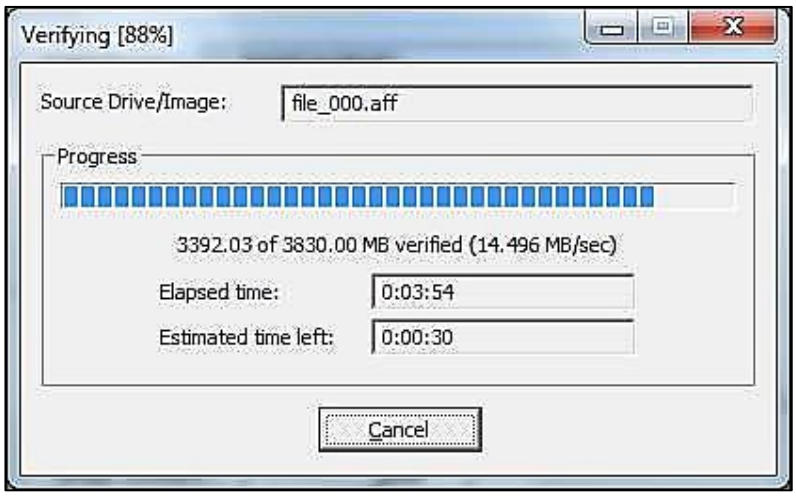
Step 13) When AFF Encryption is selected, type the password, and retype the password to confirm. Click Show Password to see that you have typed it correctly the first time.

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

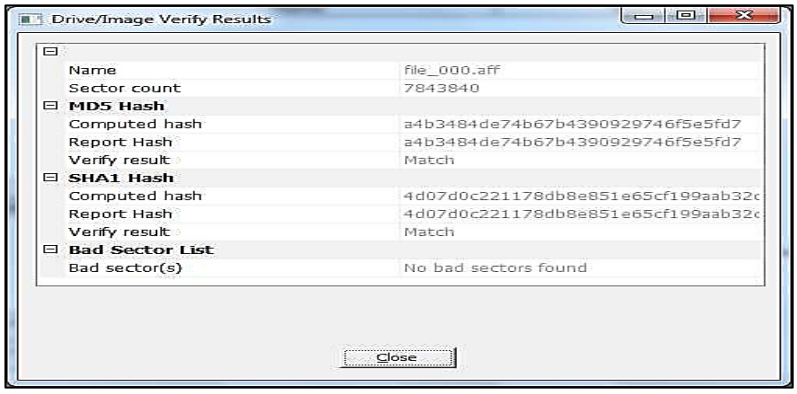


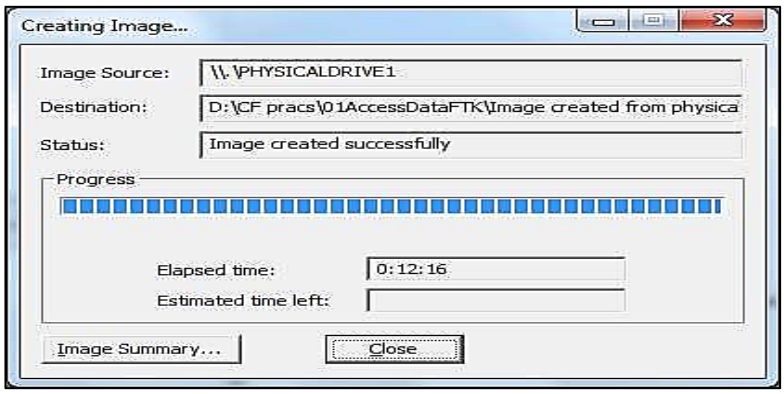


After the images are successfully created, the Drive/Image Verify Results box shows detailed image information, including MD5 and SHA1 check sums, and bad sectors.



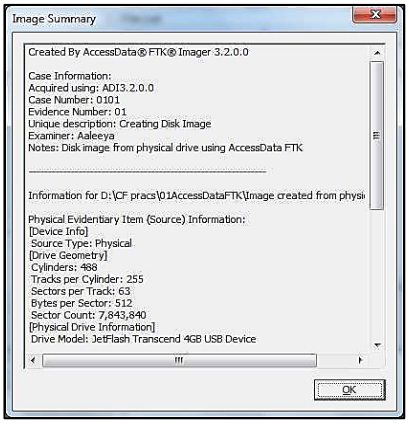
Now is a good time to refill that coffee cup! Once the acquisition is complete, you can view an image summary and the drive will appear in the evidence list in the left-hand side of the main FTK Imager window. You can right-click on the drive name to Verify the Image:

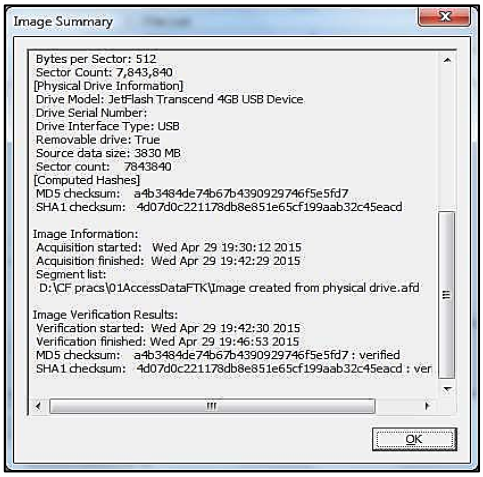




A progress dialog appears that shows the following:

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



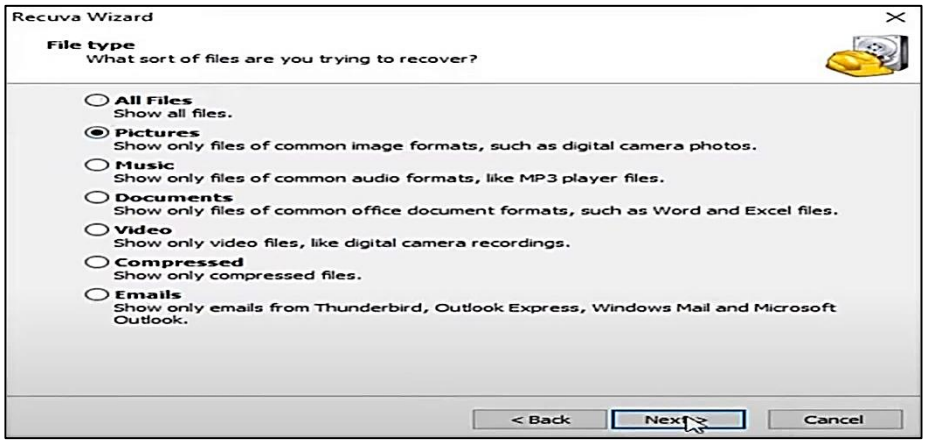


B) Recover Deleted files using Recuva, PC Inspector File Recovery,Recover My Files

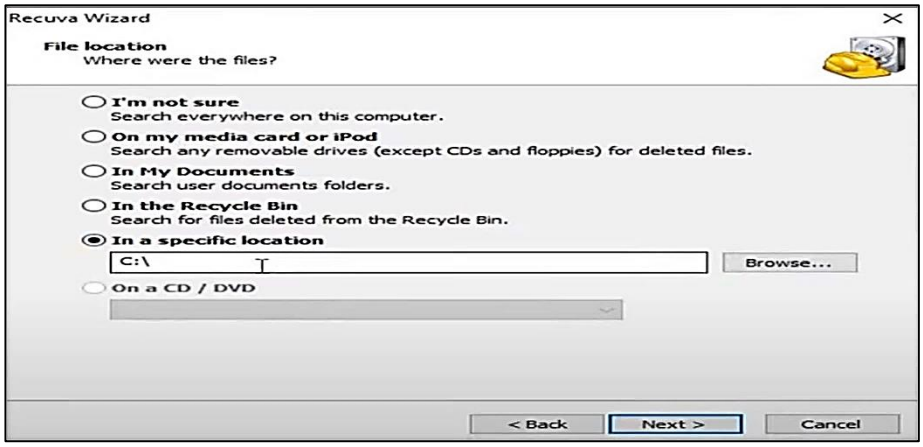
Recuva

Download and install Recuva

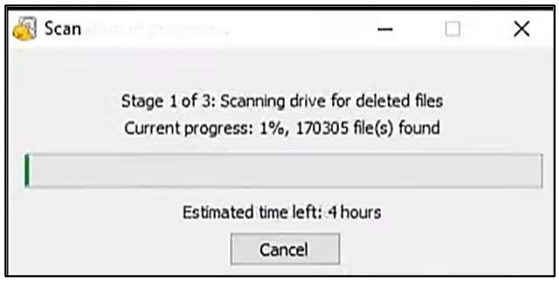
Select File Type you need to recover

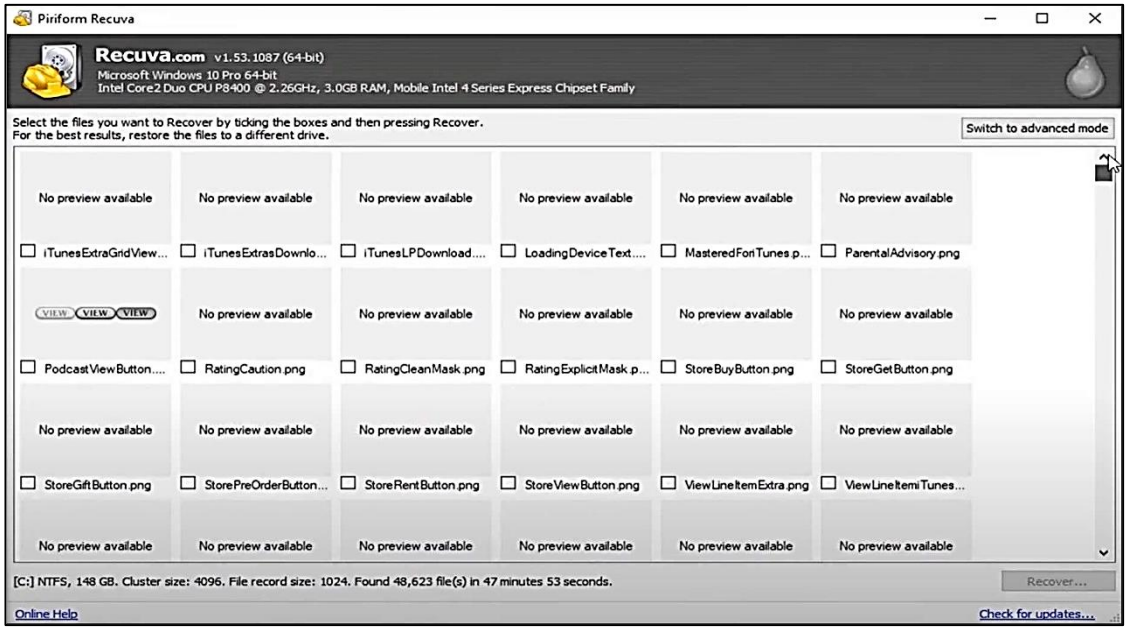


Select File location, which you want to recover files

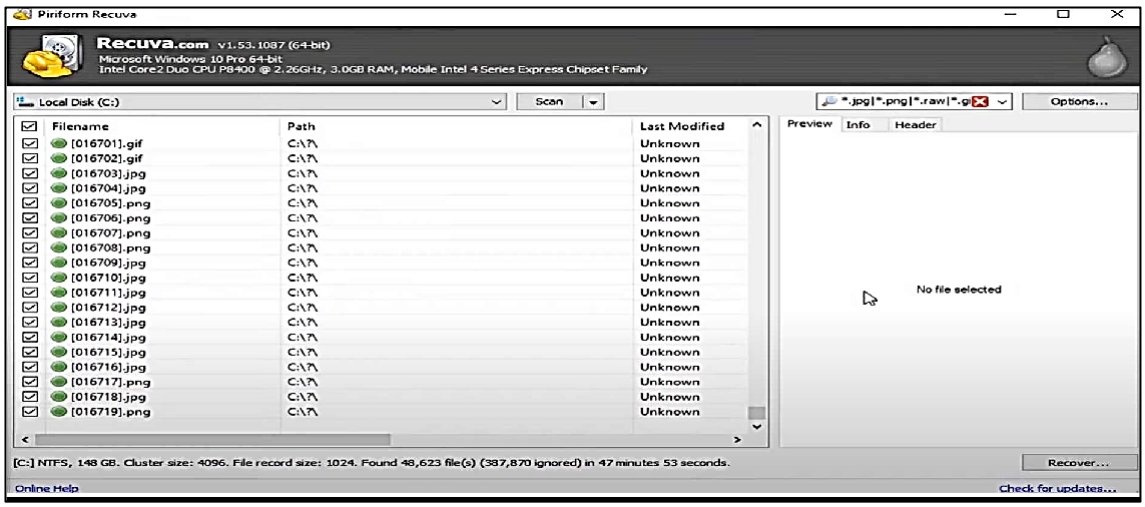


Click next (If want enable Deep Scan)

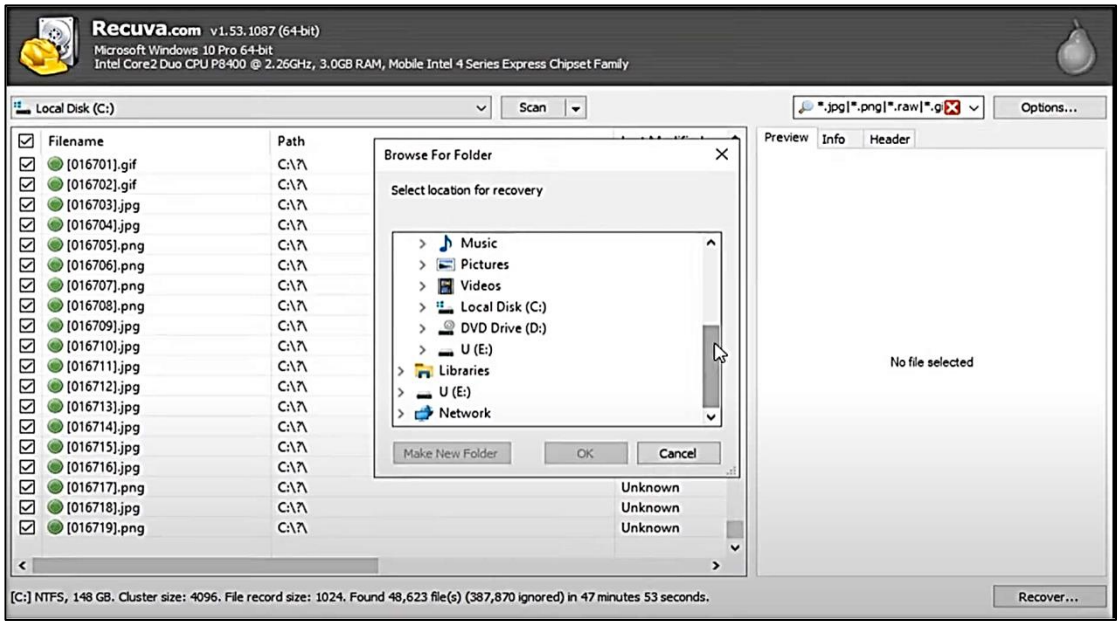


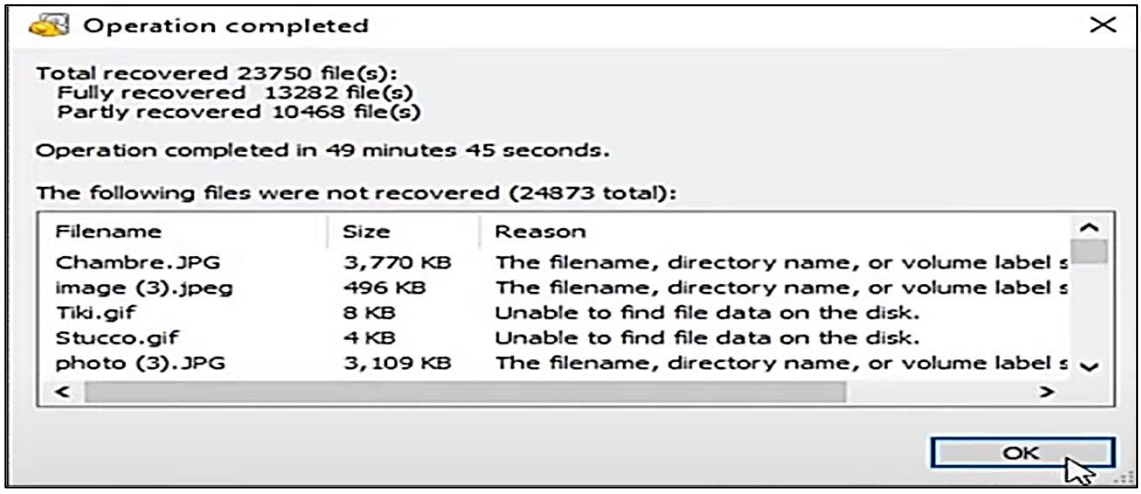


Switch to advanced mode and select all recover file



Select the location were to recover the file



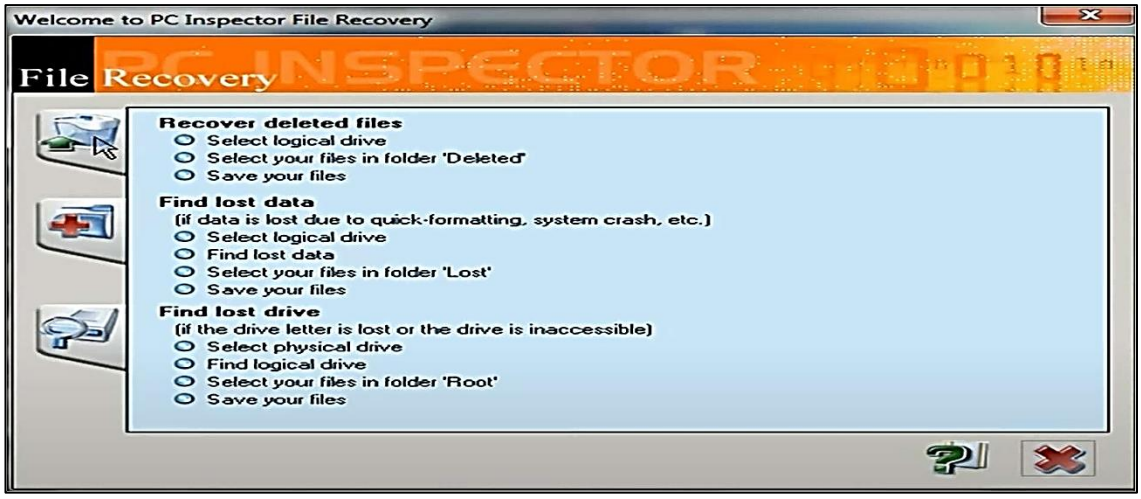


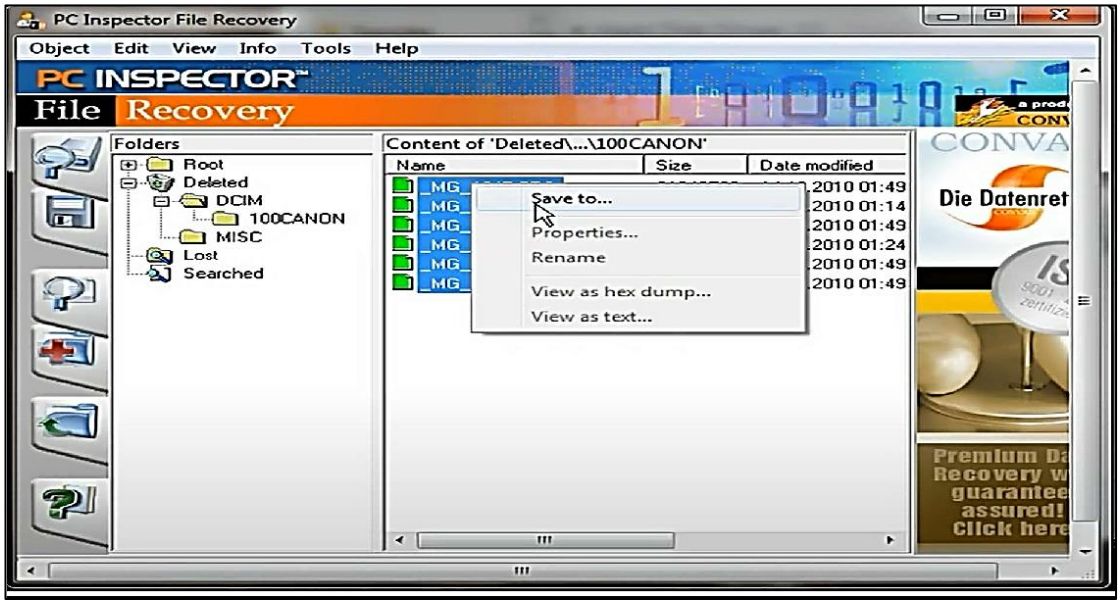
All deleted Files are recovered at specified location

PC Inspector File Recovery

Download and install PC Inspector File Recovery

Choose what to recover delete files, lost data or lost drive

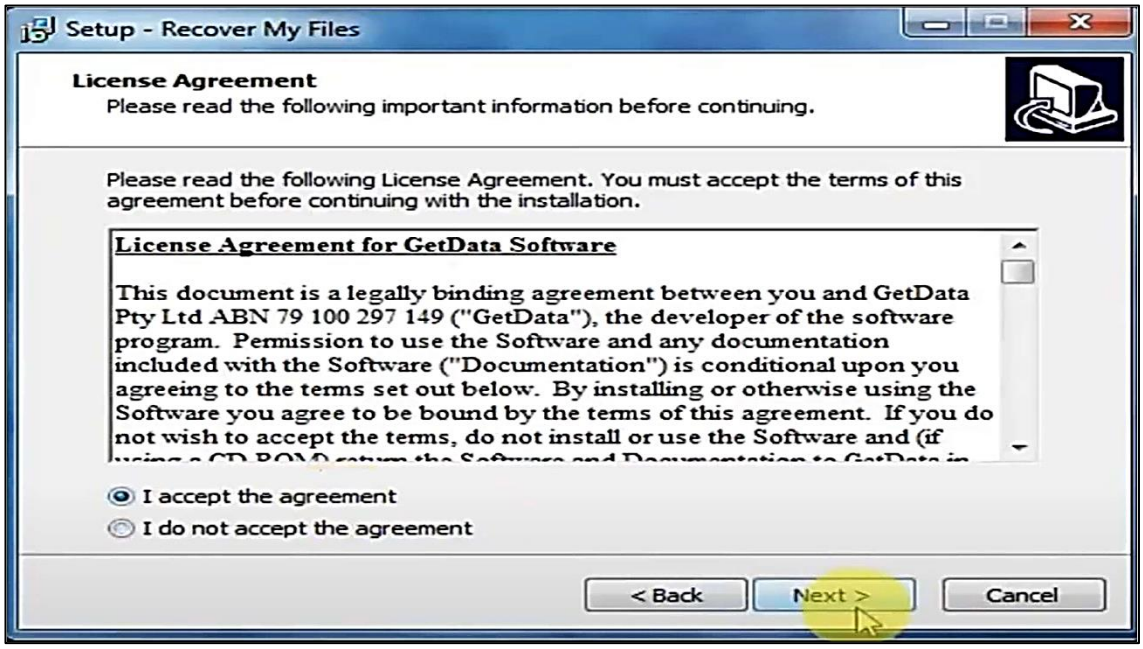




Recover data is saved to specified location

Recover My Files

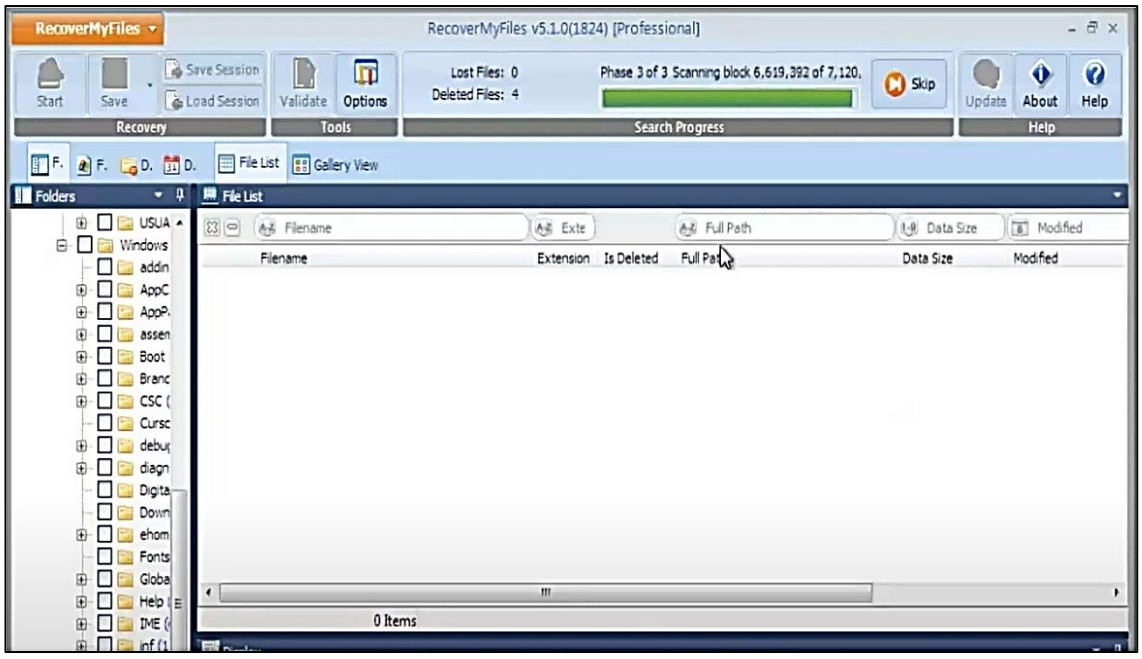
Download and install Recover My Files



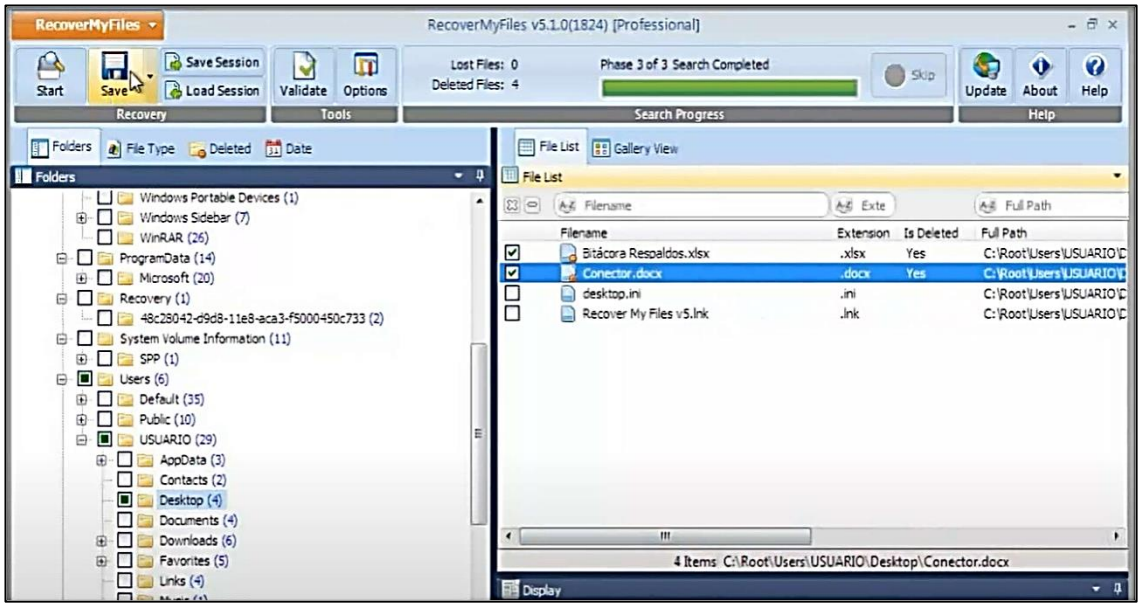
Select the option you wish to of Recover Files and Recover a Drive

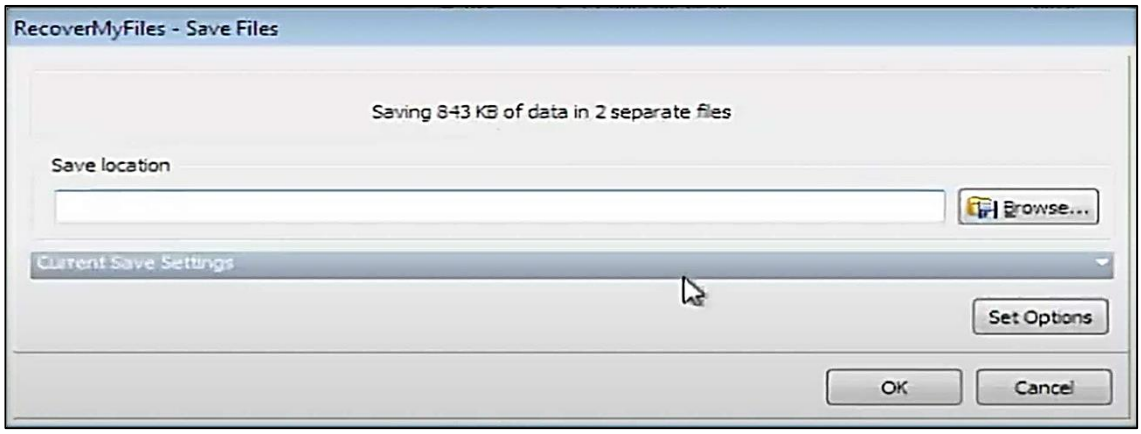
Select the drive to search and recover files & select one of the File Recovery options

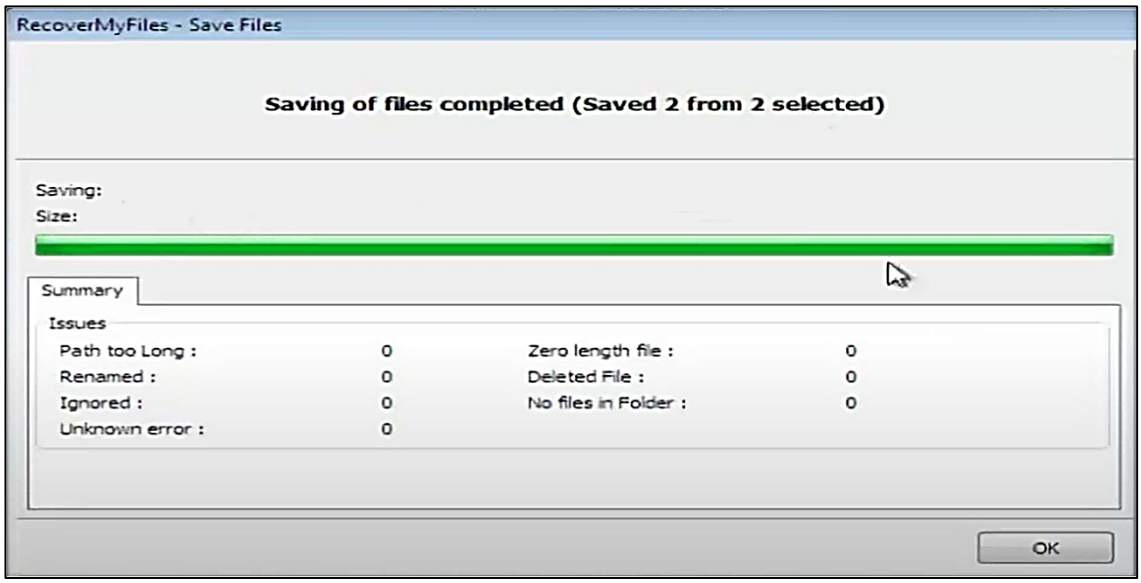
What file headers would like to search from recover files



Scan and save the recovered file to desired location



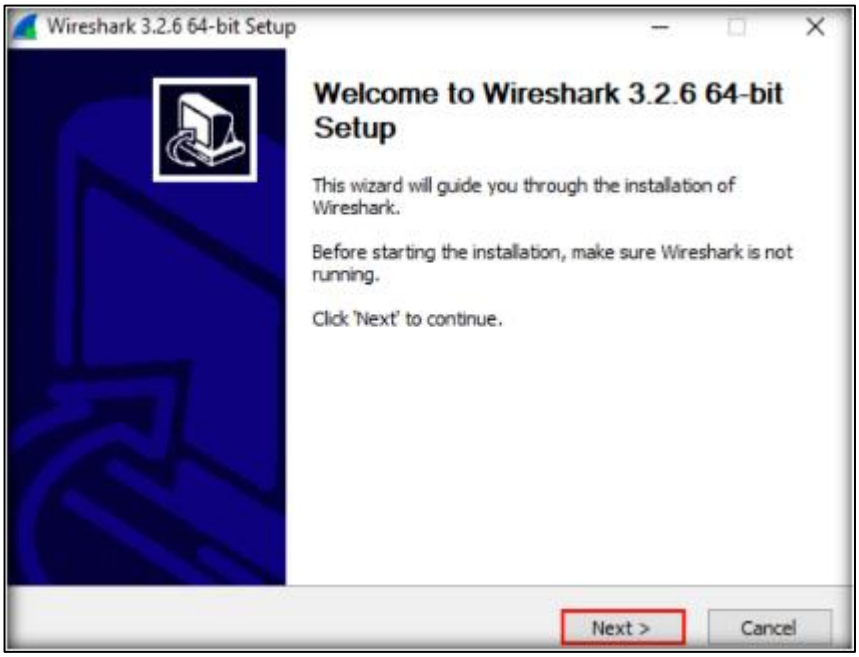




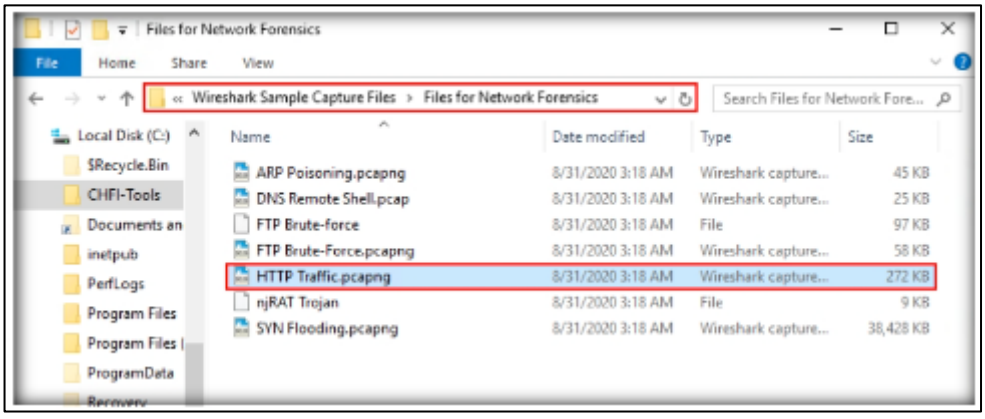
PRACTICAL 5

Aim: A) Using Web attack detection tools [Wireshark]

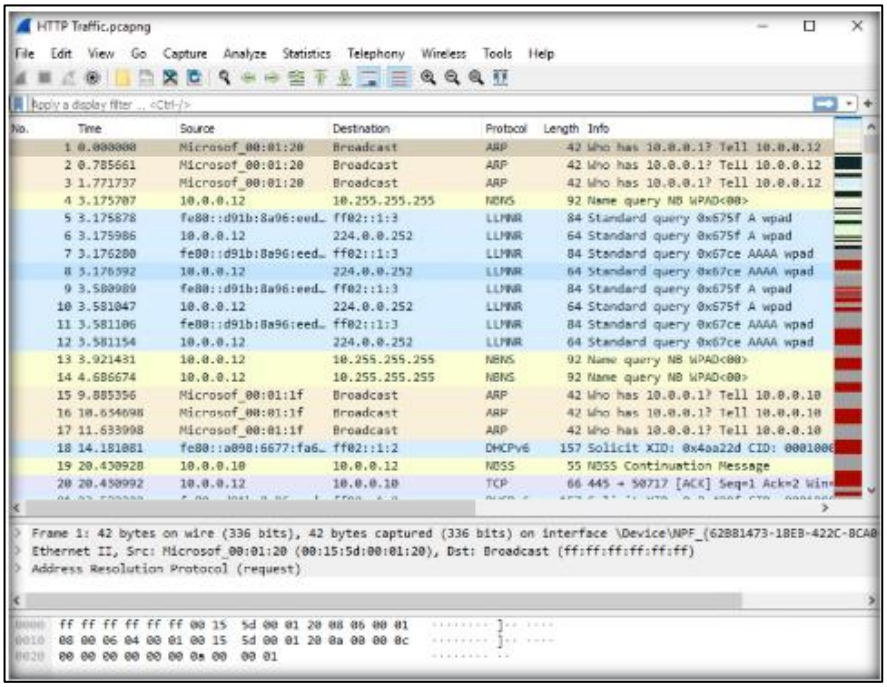
1. Download and install wireshark



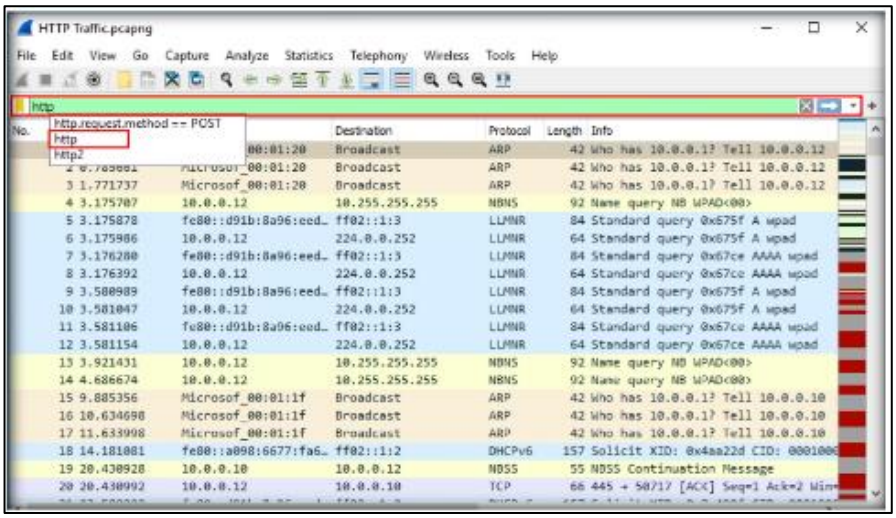
2. After completing the installation, navigate to C:\CHFI-Tools\EvidenceFiles\WiresharkSample Capture Files\Files for Network Forensics and double-click HTTP Traffic.pcapng.

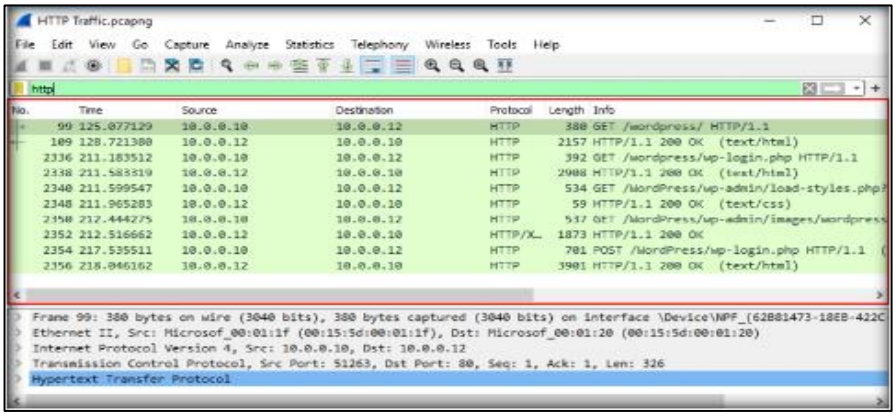


3. The above operation will launch the Wireshark GUI window and display the packets captured in HTTP Traffic.pcapng, as shown in the following screenshot



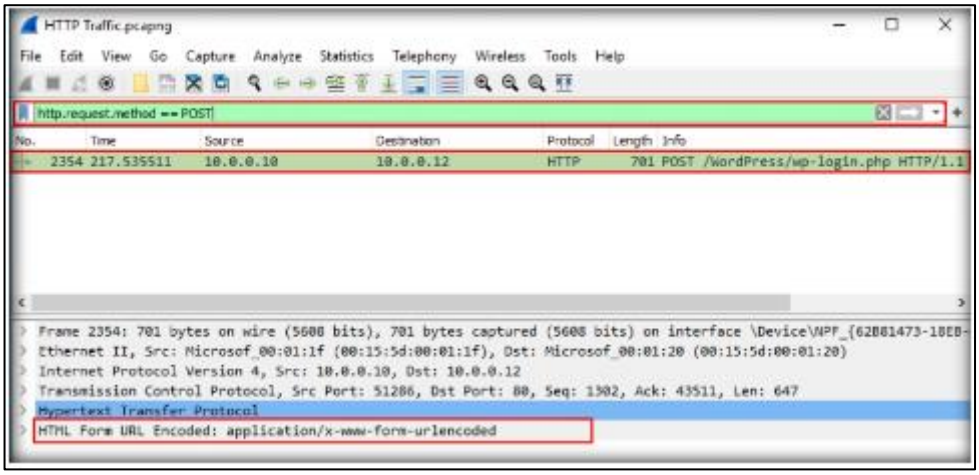
4. We will now apply the http filter so that the application displays results related to traffic generated through http. Type http in the Filter field and press Enter to filter the http traffic, as indicated in the screenshot below:

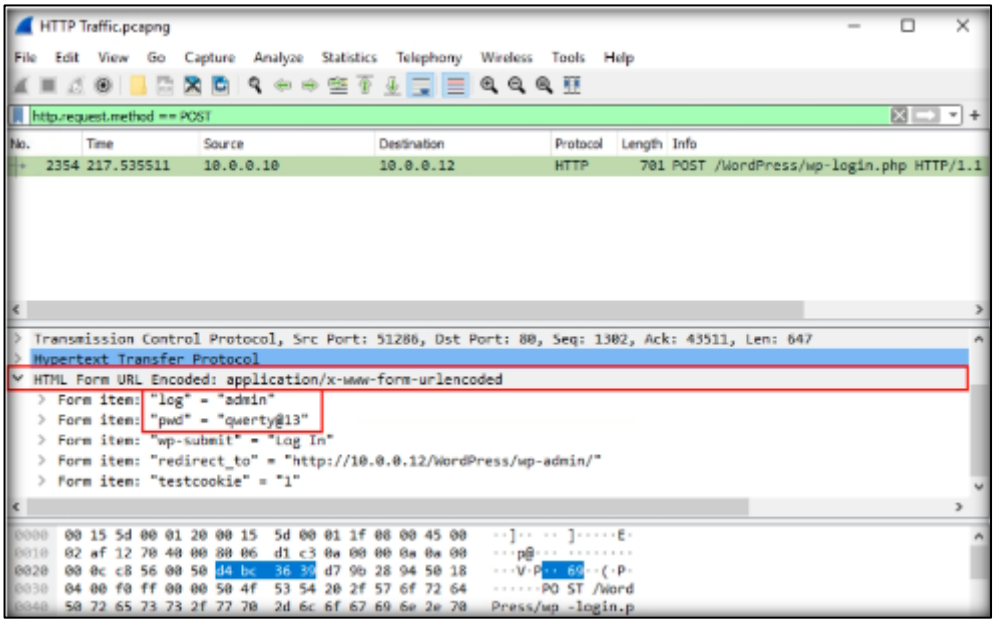




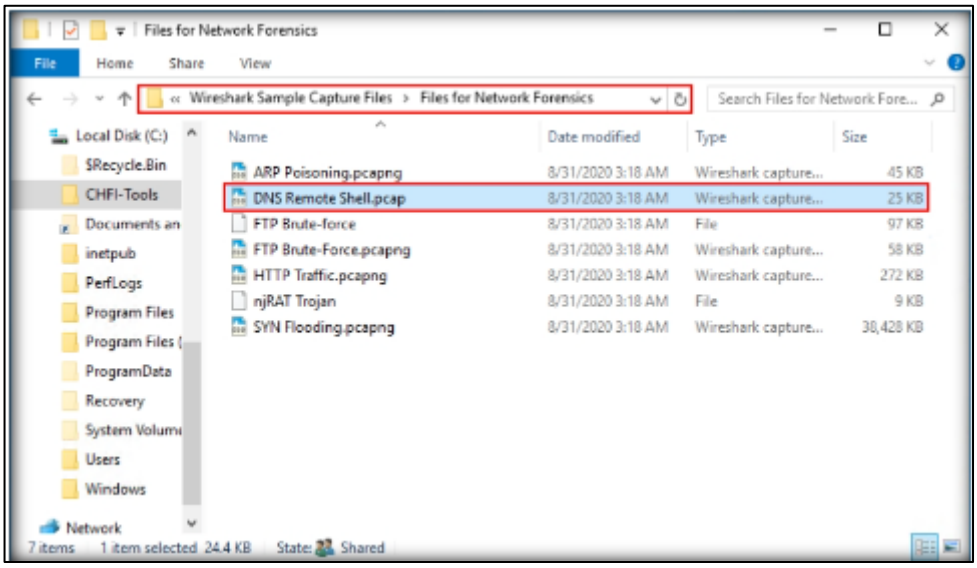
5. After examining the entries displayed by the application in the screenshot above, it is evident that the http traffic is associated with a WordPress website, and it is being transmitted in a plain text format. Generally, user credentials are stored in the POST requests. Therefore, examining packet(s) containing POST request can help an investigator find the user credentials.

6. We will now filter the traffic to obtain results specific only to POST request(s). Now, type http.request.method== POST in the Filter field and press Enter. Wireshark filters the traffic containing POST request(s) and displays them, as shown in the screenshot below. The user credentials stored in this request can be found under the Packet Details pane in the middle of the application window, under the HTML Form URL Encoded node.

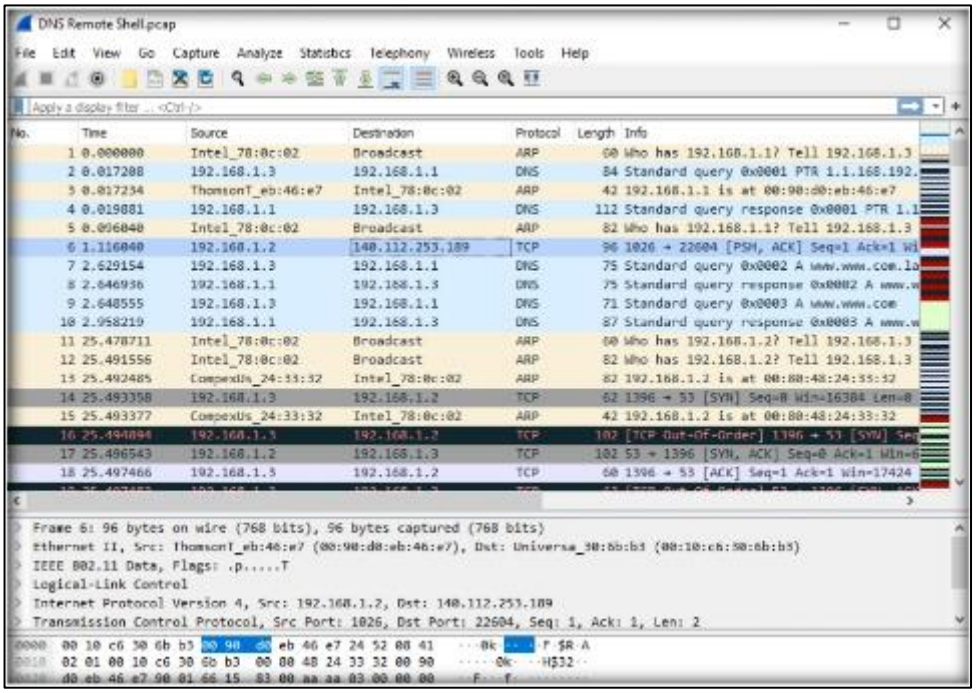




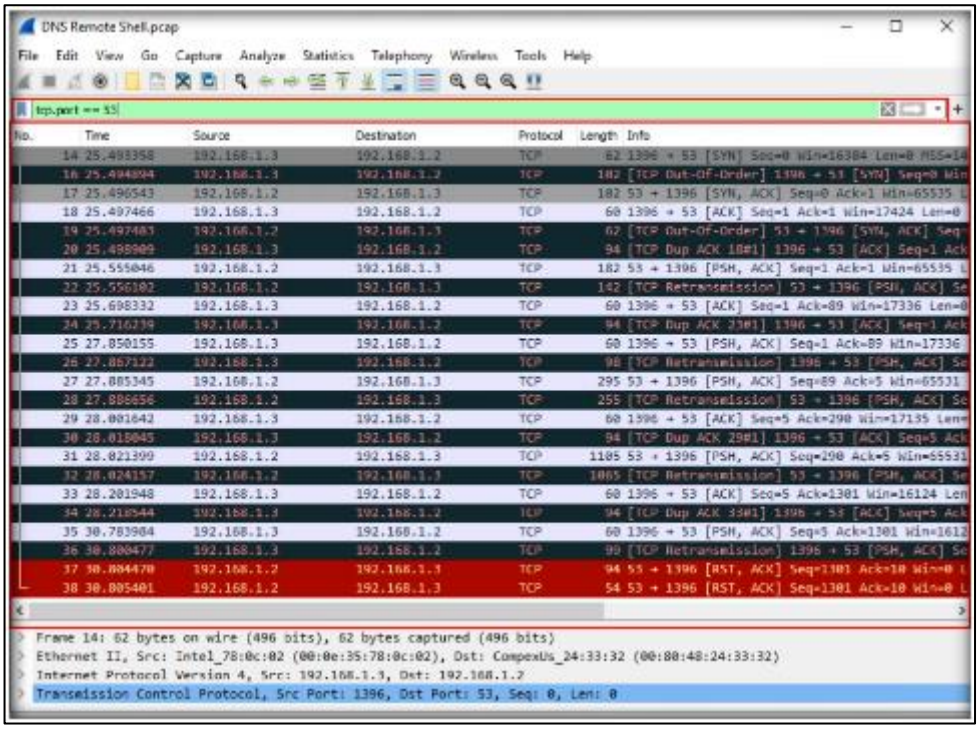
7. Now, navigate to C:\CHFI-Tools\Evidence Files\Wireshark Sample Capture Files\Files for Network Forensics and double-click DNS RemoteShell.pcapng.



8. The network traffic entries captured in the DNS Remote Shell.pcapng file will now be displayed in the Wireshark GUI window, as shown in the following screenshot

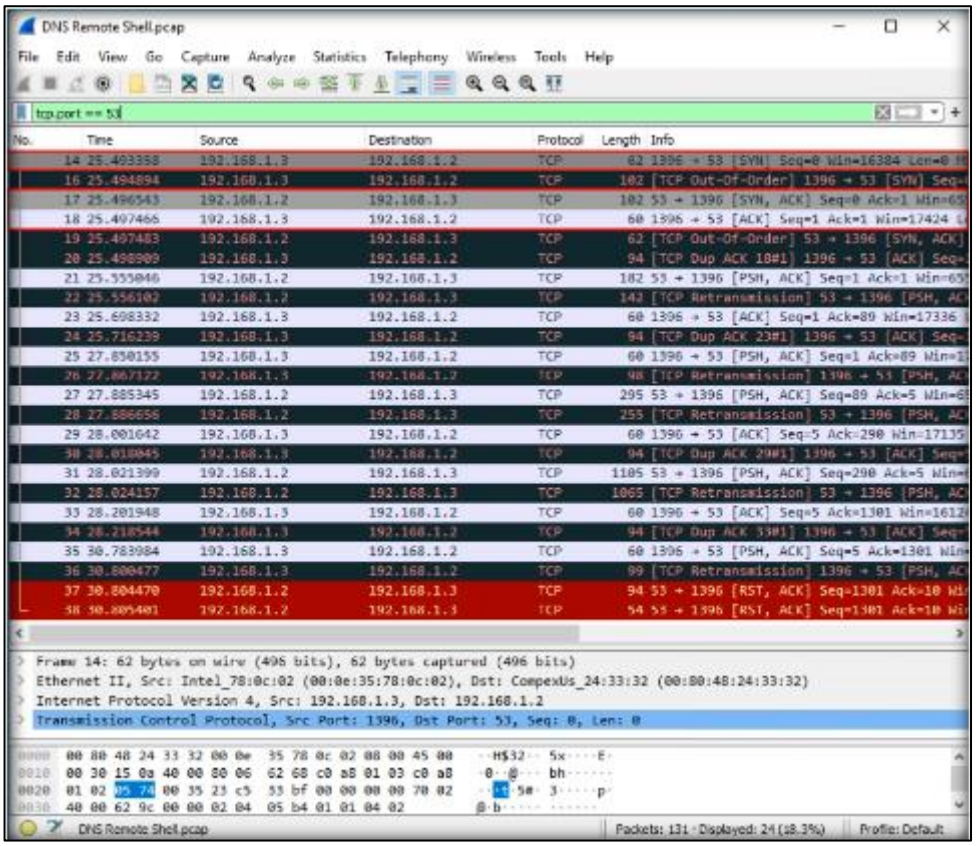


9. Since DNS uses port 53 for communicating with clients, we will be filtering the traffic flowing to and from port 53. To filter traffic flowing on port 53, type the command tcp.port == 53 in the Filter field and press Enter. Wireshark filters the traffic flowing on port 53 and displays it, as shown in the following screenshot

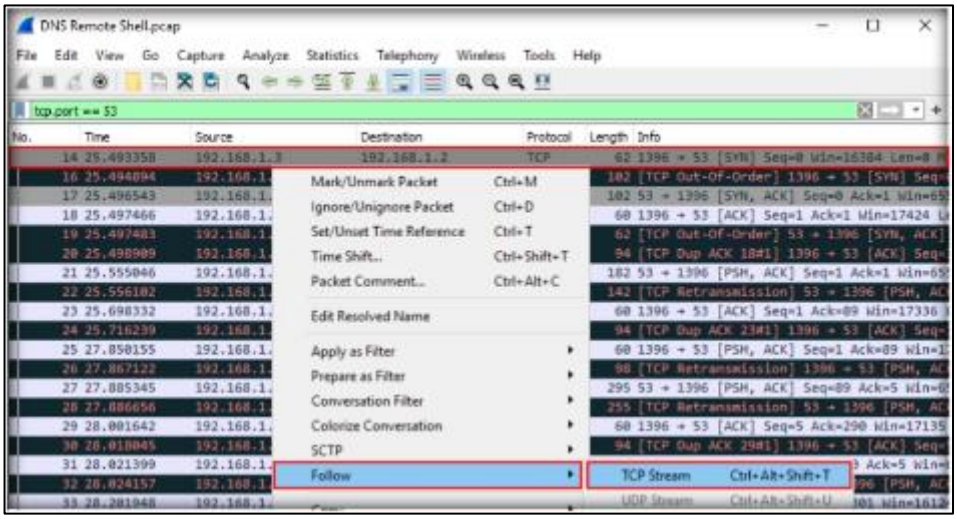


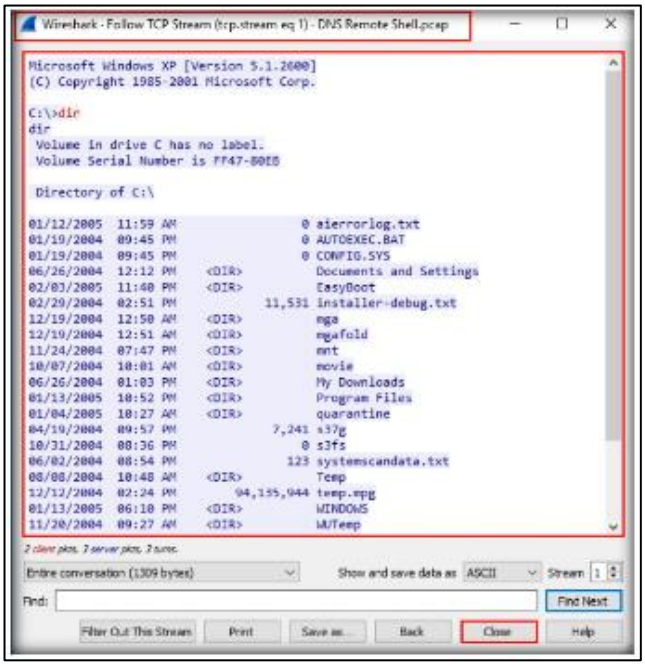
When we examine the first packet from the listed packets, i.e., Packet 14, we can see that Port 1396 on Source IP address (192.168.1.3) is trying to establish a remote connection with Port 53 on the Destination IP address (192.168.1.2) through a [SYN] request. As Port 53 is seen on 192.168.1.2, this IP address represents the DNS server here. When we examine Packet17, we see that the

IP address 192.168.1.2, which is the DNS server, is responding with a [SYN, ACK] acknowledgment to IP address 192.168.1.3. Upon examining Packet 18, we see that the IP address 192.168.1.3 is sending an [ACK] acknowledgment to 192.168.1.2, thus establishing a remote connection with the target/victim (i.e., 192.168.1.2). From these observations, we can infer that 192.168.1.3 is the attacker's IP address, which has succeeded in establishing a connection from its Port 1396 with Port 53 on the DNS server, as indicated through Packets 14, 17, and 18 in the screenshot below:

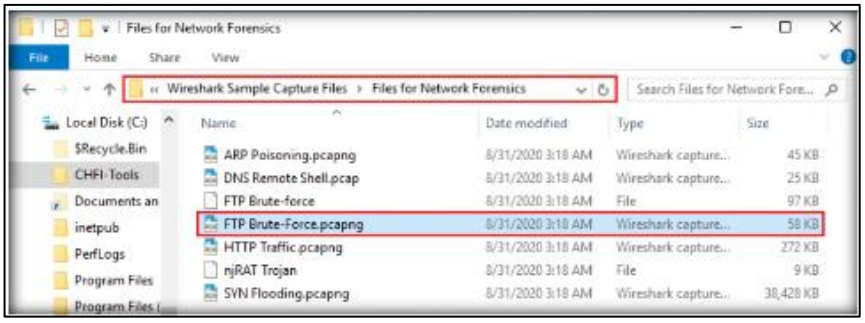


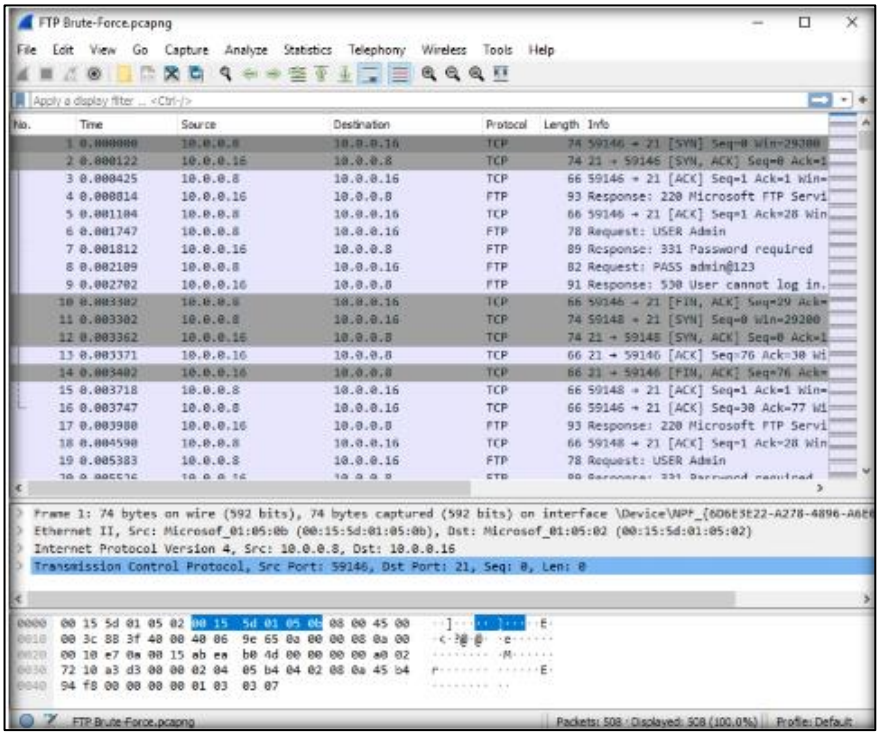
10. Right-click on any one of the packets from 14 to 38 (here, we have right-clicked on packet 14), select Follow from the context menu, and then click TCP Stream from the resultant drop-down list, as shown in the screenshot below:



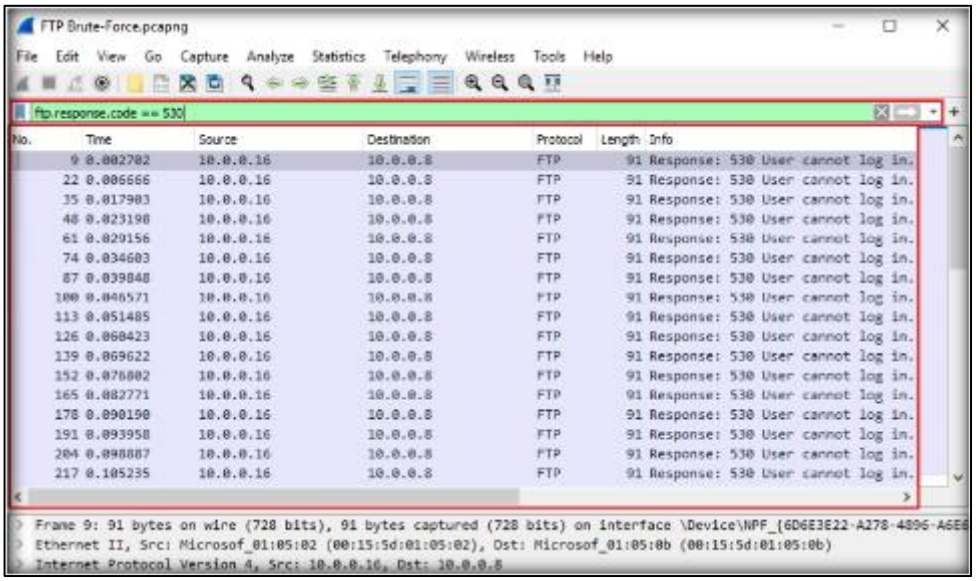


11. Now, we will look for FTP brute-force attempts in the network. Close the current packet capture file in Wireshark.

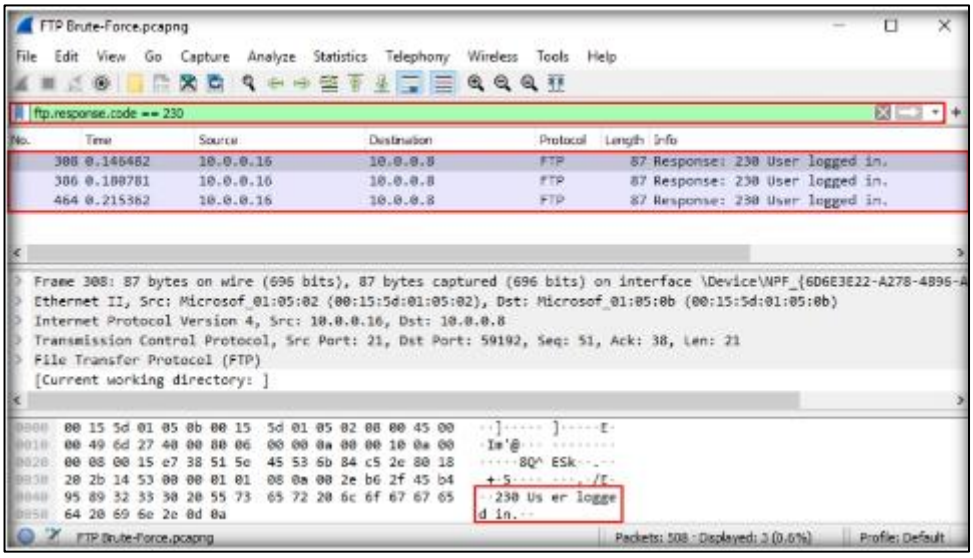




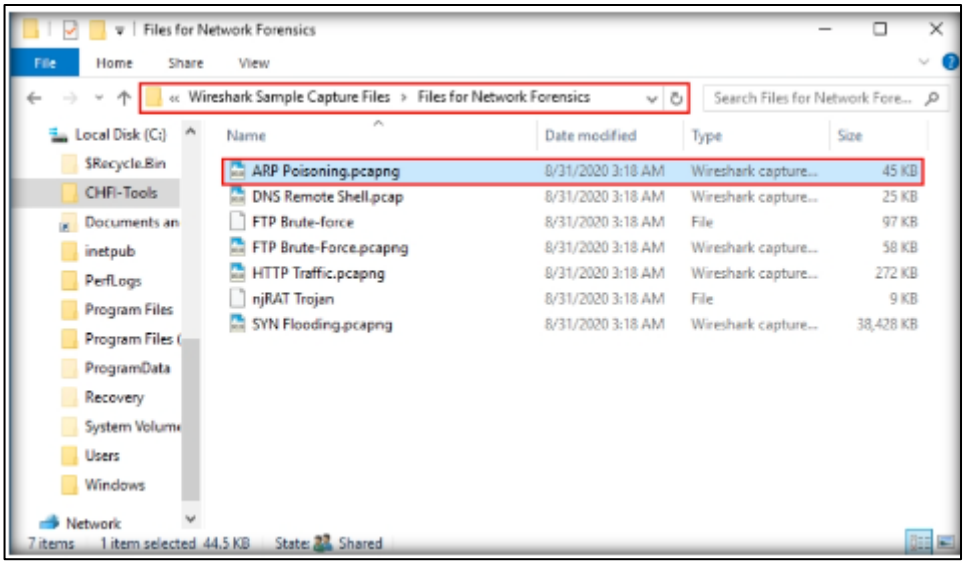
12. Apply the ftp.response.code == 530 filter to monitor all unsuccessful login attempts over FTP. Upon applying the filter, the application will fetch results pertaining to unsuccessful login attempts, as shown in the screenshot below:

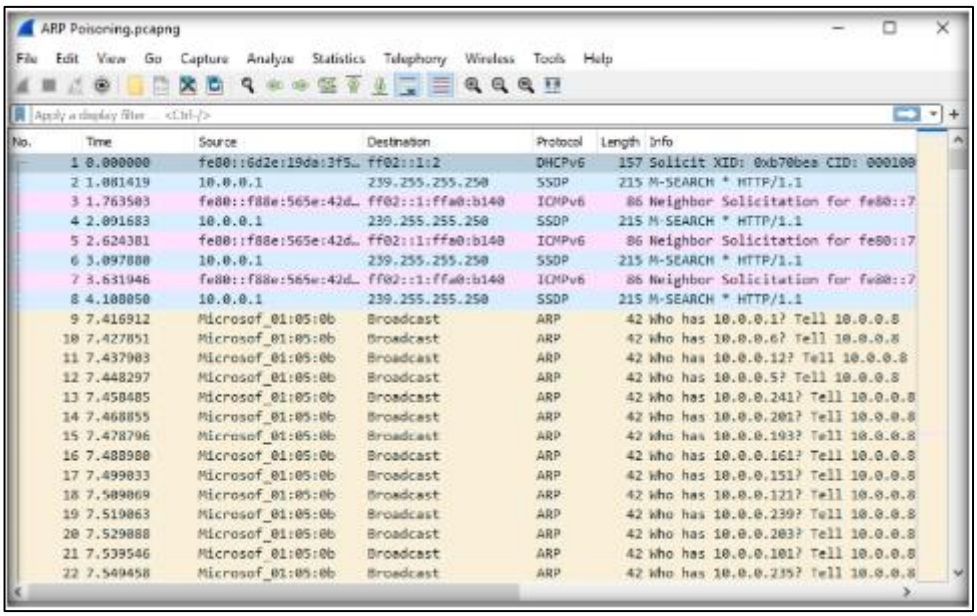


13. The screenshot above shows multiple unsuccessful login attempts made from the source IP 10.0.0.16 to the target IP 10.0.0.8, which strongly indicates a brute-force attack.27. Apply the ftp.response.code == 230 filter to see successful logins on the FTP server. The application will fetch results that show successful logins from the source IP 10.0.0.16 to the target IP 10.0.0.8, as shown in the screenshot below. This indicates the attacker has successfully gained the victim's login credentials

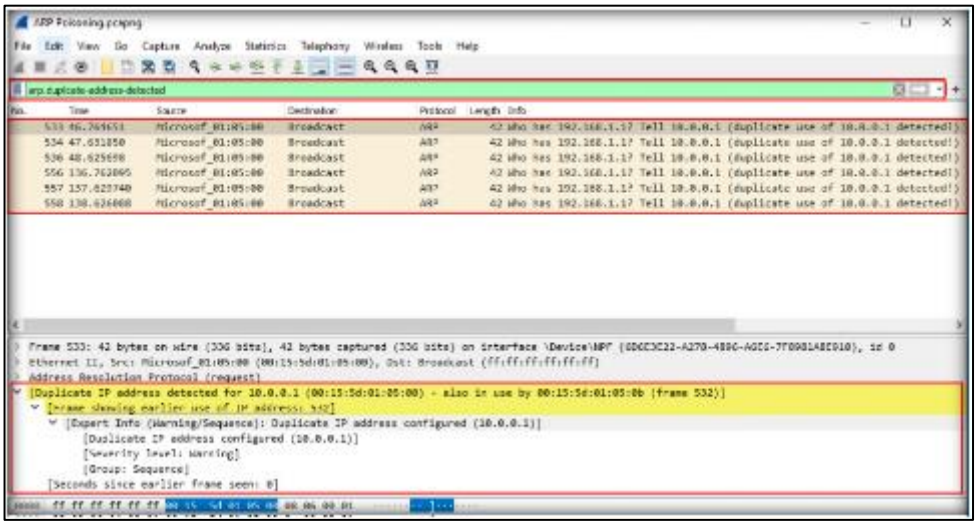


14. Now, we will look for ARP Poisoning attempt in the network.





15. When ARP Poisoning has been attempted, Wireshark will detect duplicate IP addresses on the ARP protocol with the warning message Duplicate IP address detected for <IP address>. Therefore, we need to check if the use of a duplicate IP address has been detected.45. To locate a duplicate IP address in the traffic, apply the ARP. duplicate-address-detected filter. Wireshark detects duplicate IP address on the ARP protocol with the warning message Duplicate IP address detected for 10.0.0.1, as shown in the screenshot below. The duplicated IP address can be seen both in the Packet Details pane in the middle of the application window and in its upper pane.



In this manner, you can analyze packet capture files that have recorded the traffic on a network as part of a forensic investigation.

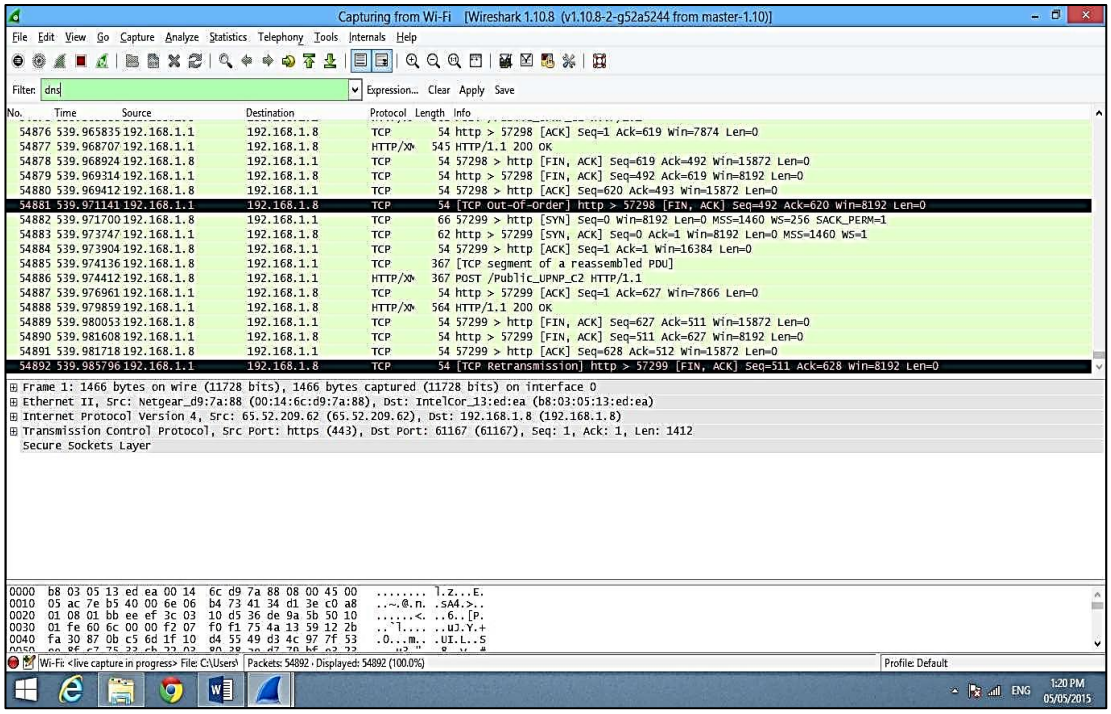
B) Using Log & Traffic Capturing & Analysis Tools [Wireshark] Using Log Capturing and Analysis tools

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

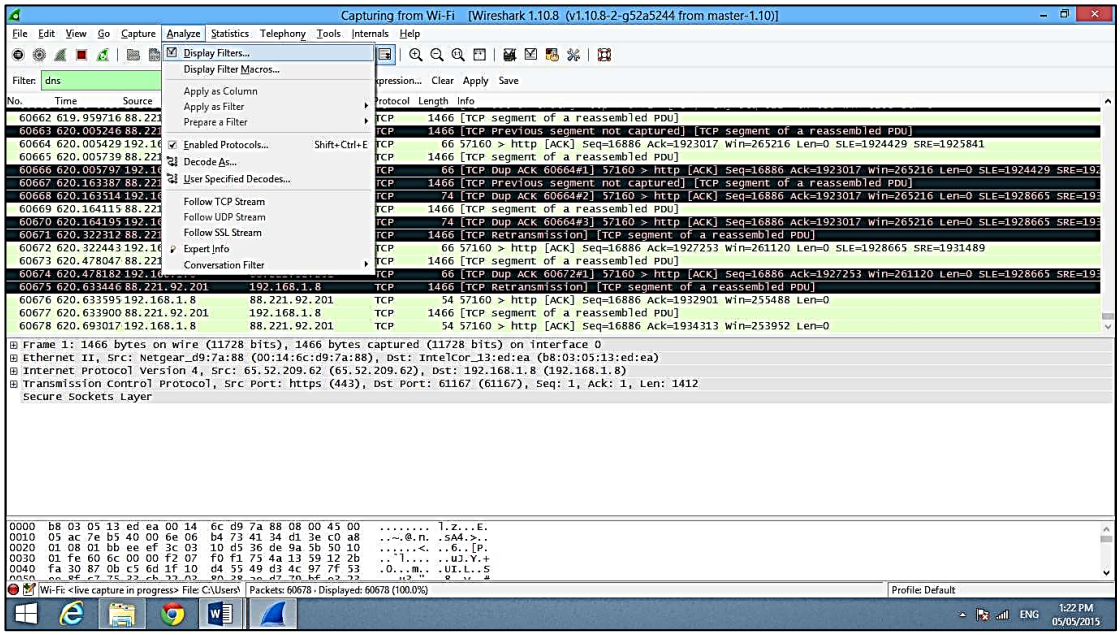
Filtering Packets

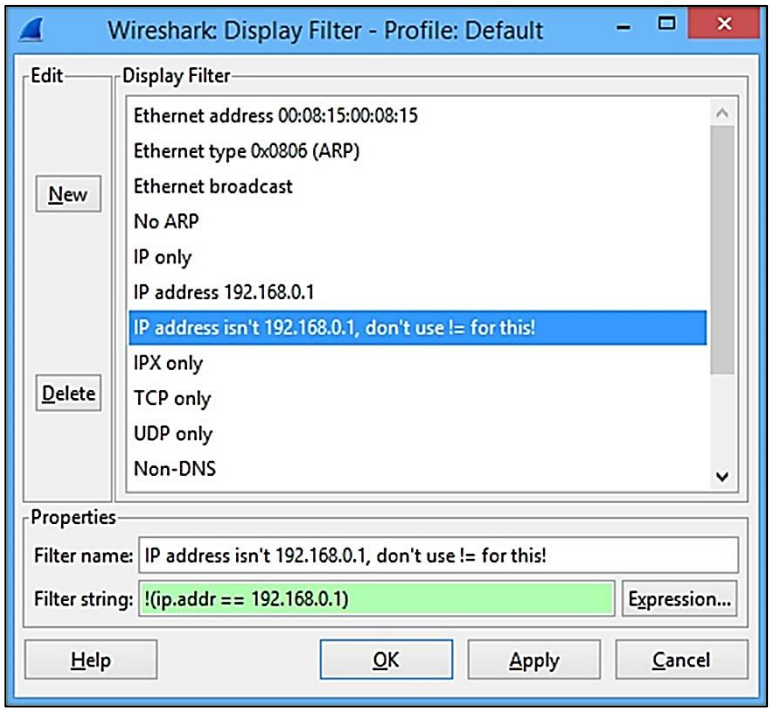
If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the traffic. Still, you'll likely have a large amount of packets to sift through. That's where Wireshark's filters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

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

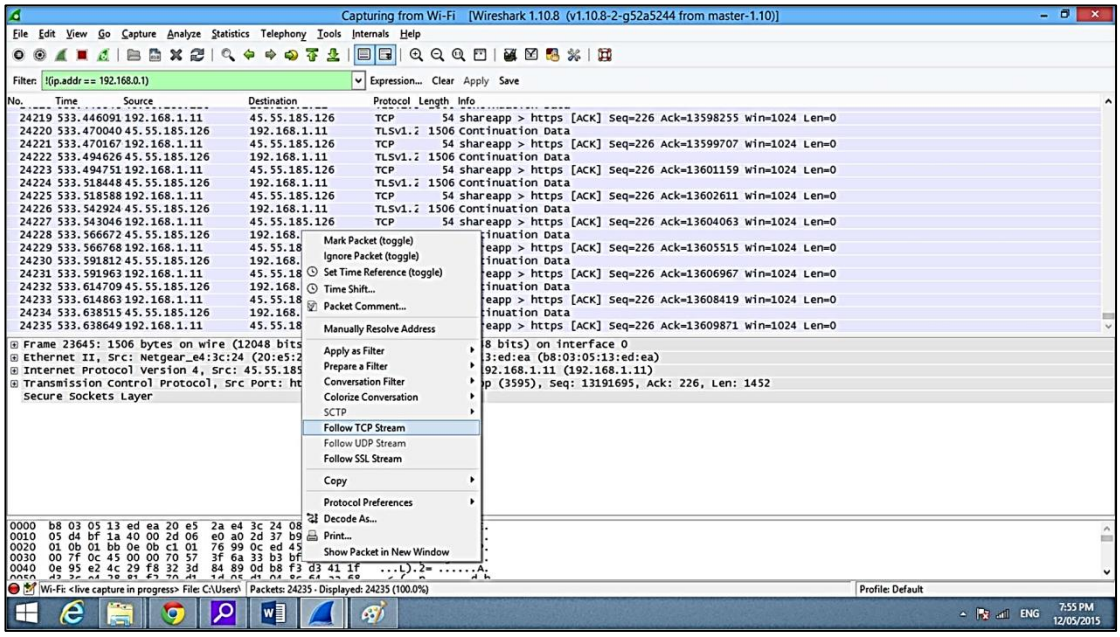


You can also click the Analyze menu and select Display Filters to create a new filter.

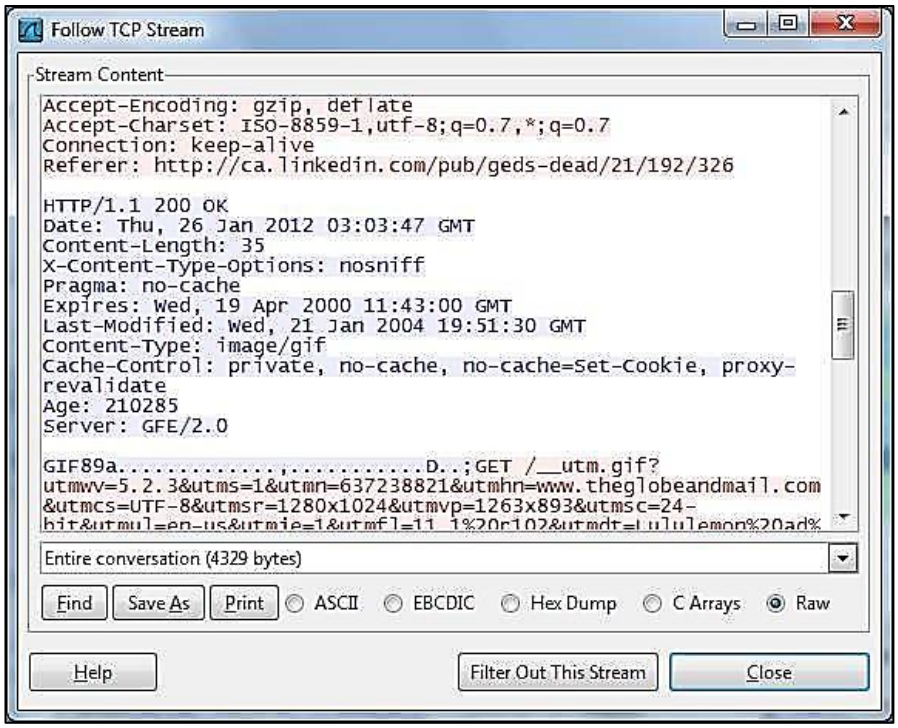




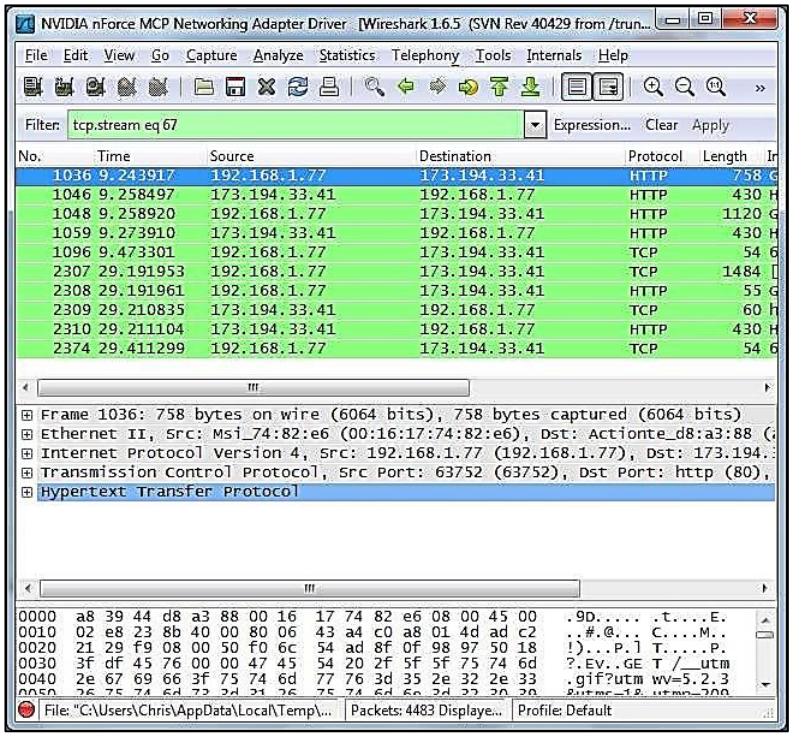
Another interesting thing you can do is right-click a packet and select Follow TCP



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

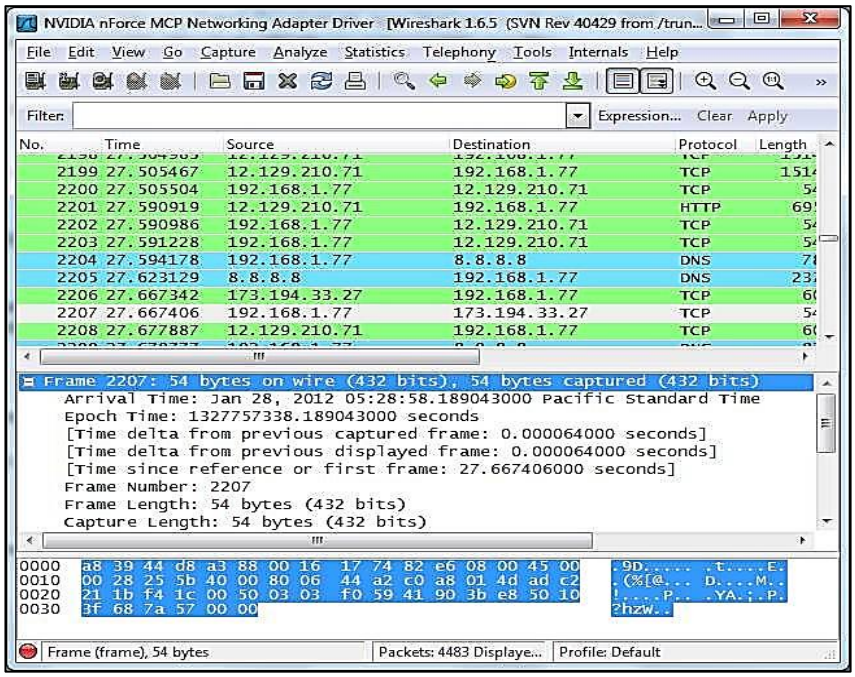


Close the window and you'll find a filter has been applied automatically — Wireshark is showing you the packets that make up the conversation.

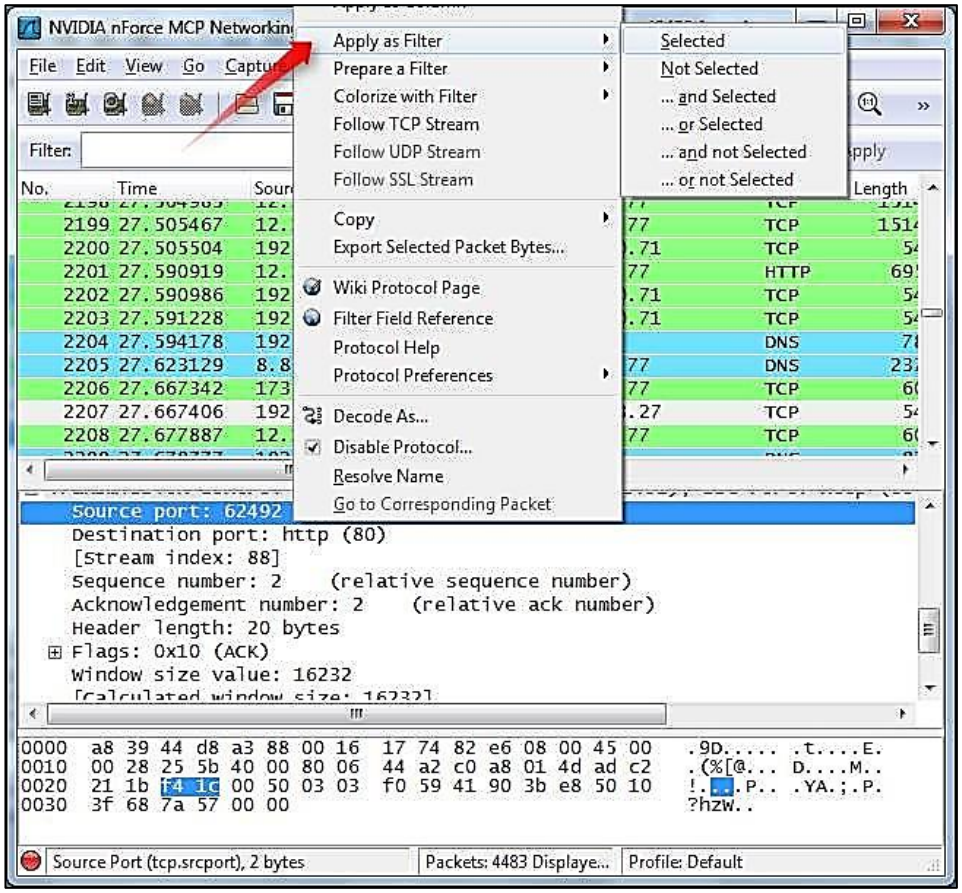


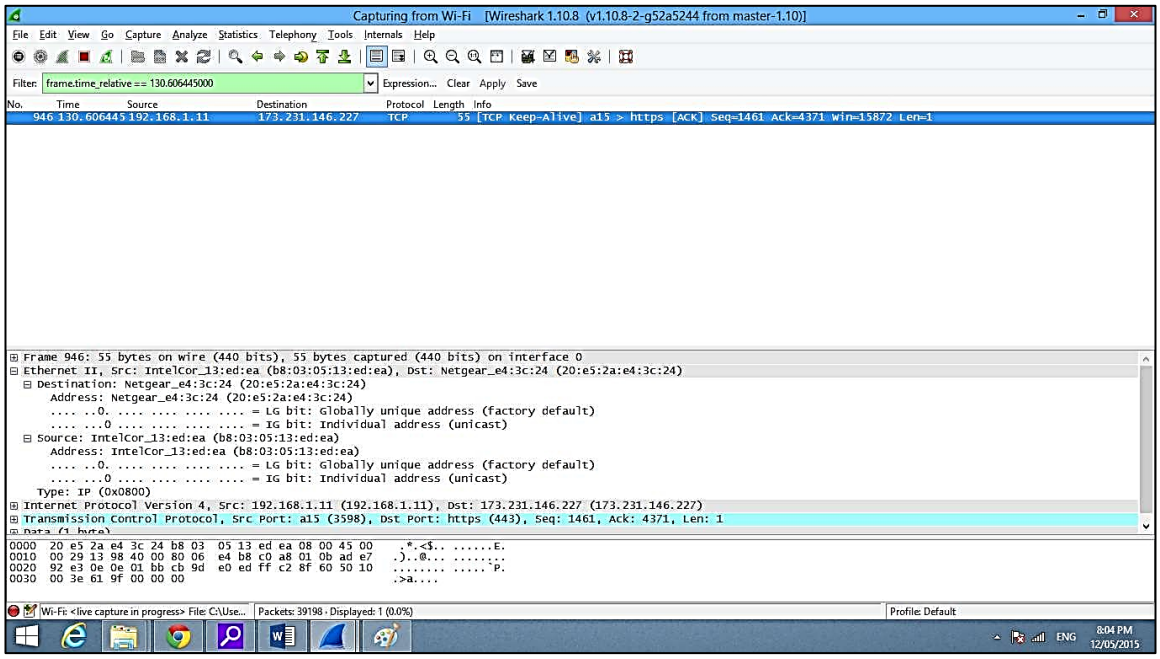
Inspecting Packets

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



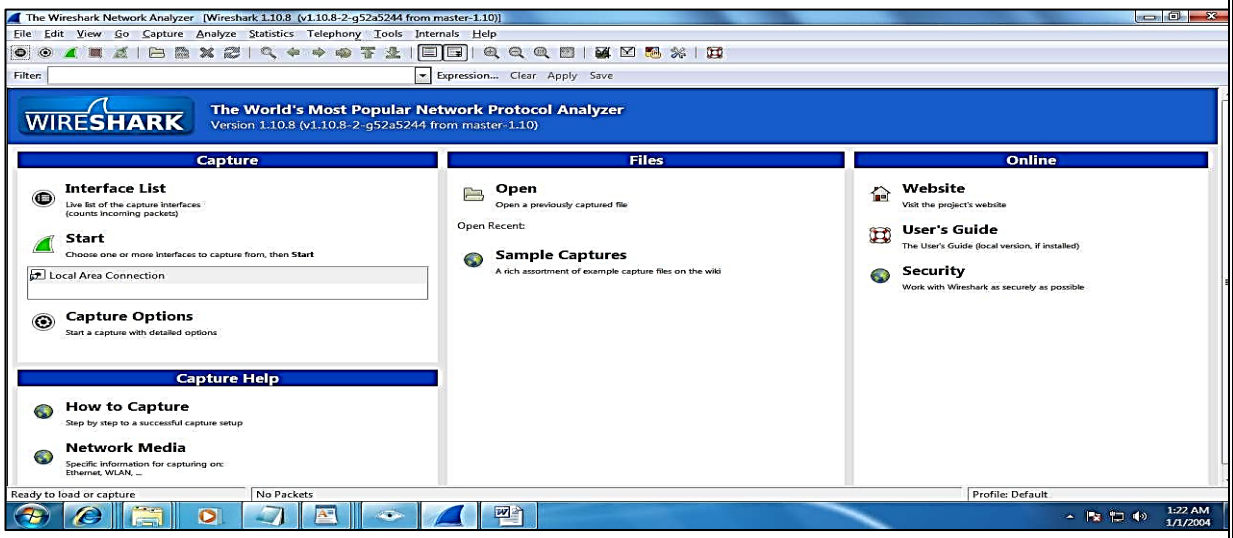
You can also create filters from here — just right-click one of the details and use the Apply as Filter submenu to create a filter based on it.



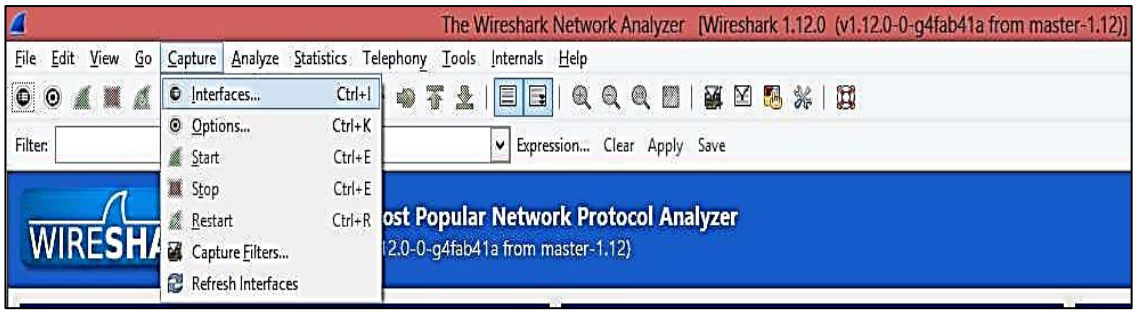


Using Traffic Capturing and Analysis tools

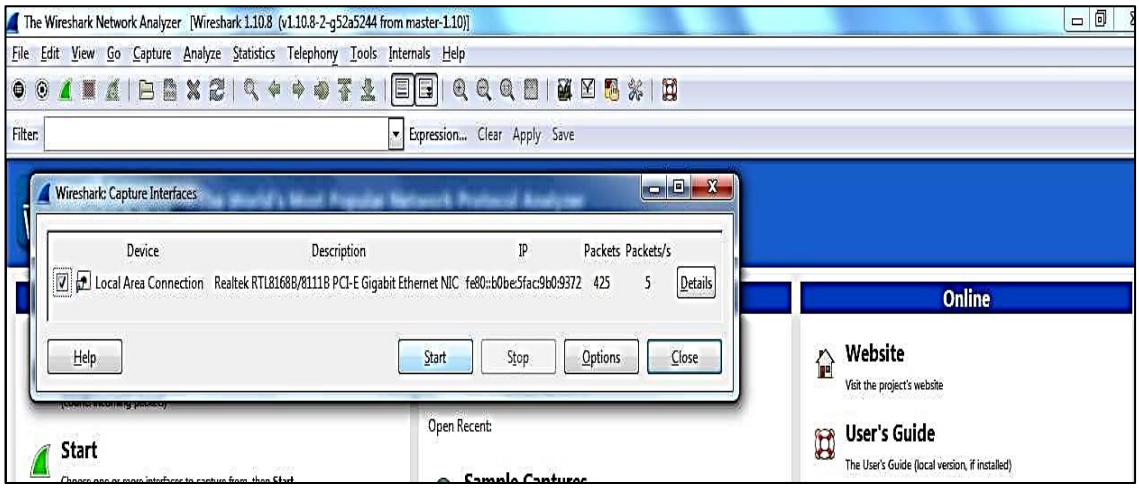
Step 1: Open Wireshark

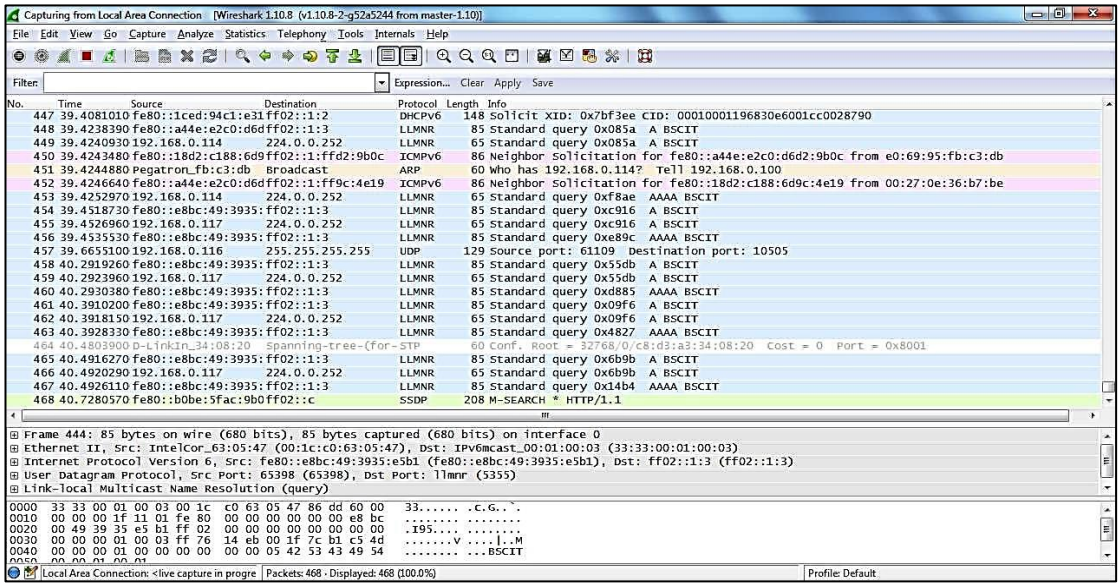


Step 2: On menu bar select Capture. Select interfaces.

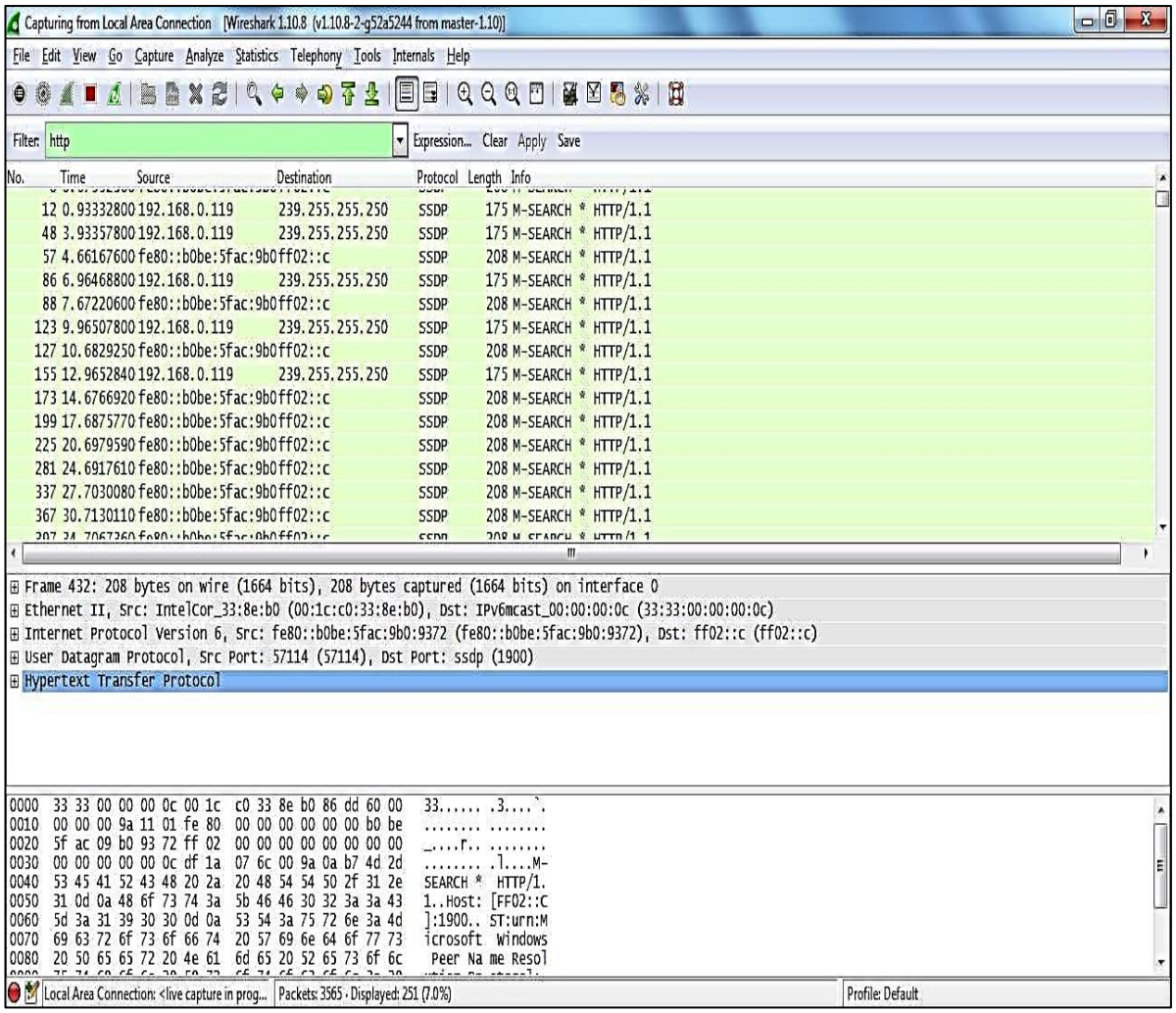


Step 3: Select Once you click on start, then Wireshark starts to capture the packets on that interface.

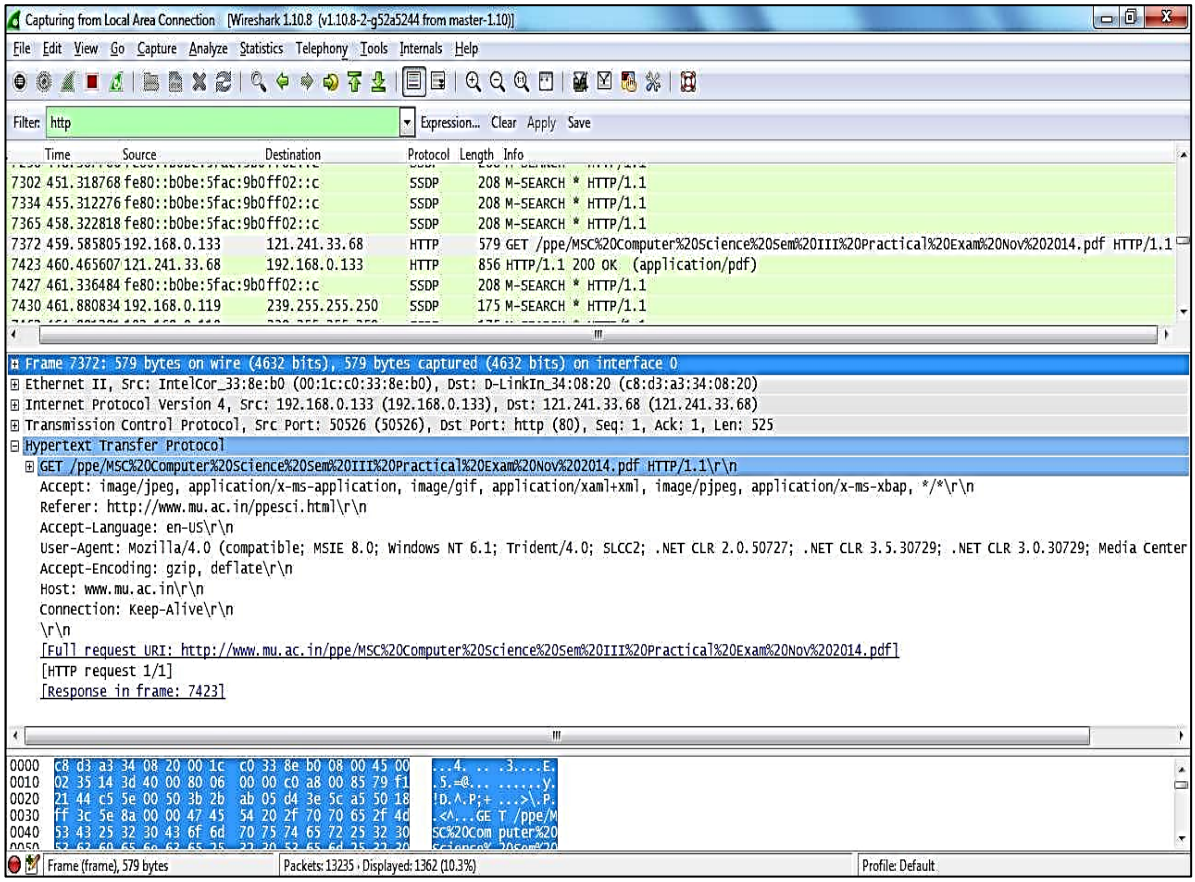




Step 4: Filter packets with HTTP protocol.

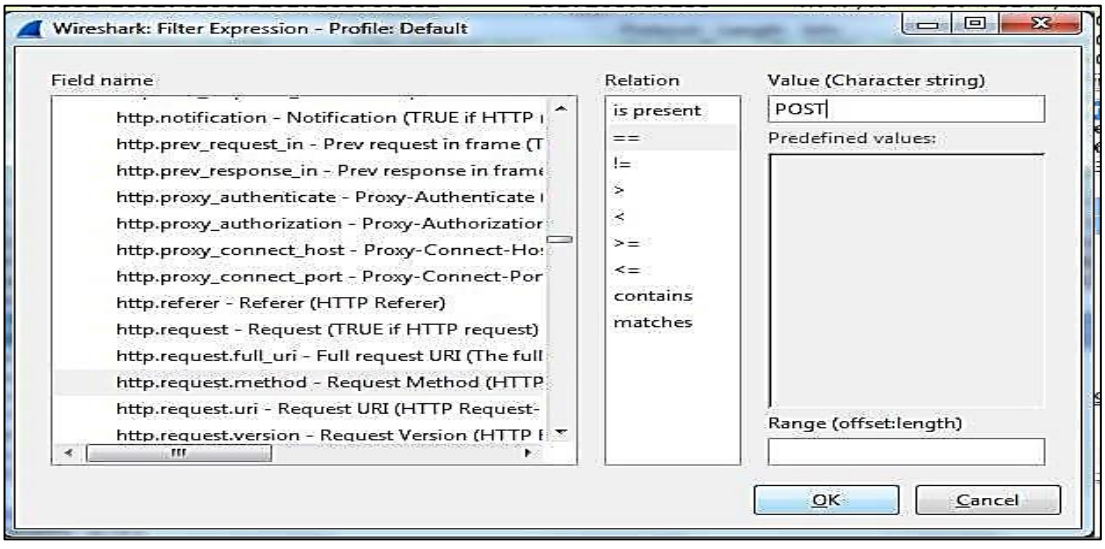


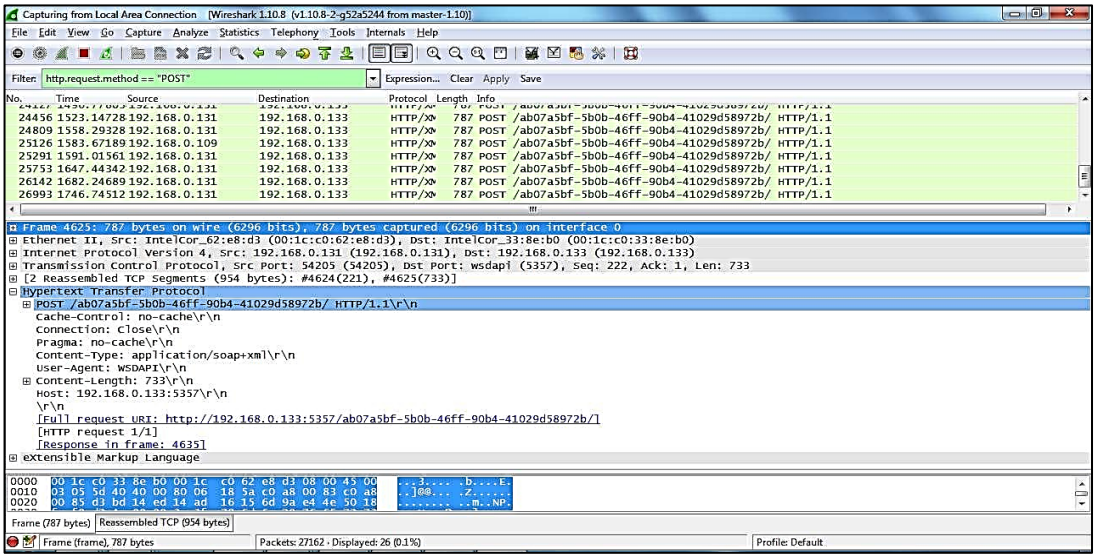
Step 5: A file with only text: http://www.mu.ac.in/ppe/LIBRARY%20SCIENCE-(SEM.I)-SH- 2014.pdf



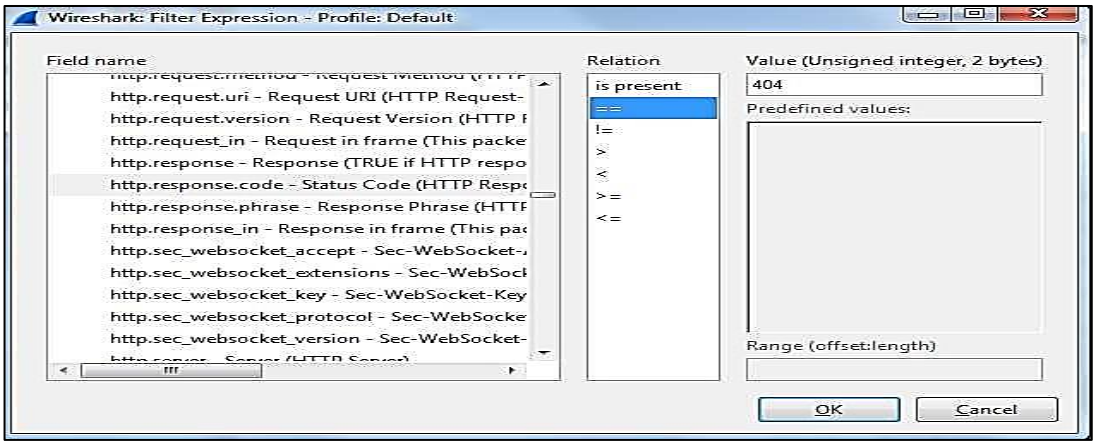
Step 6: Applying different filters using expressions.

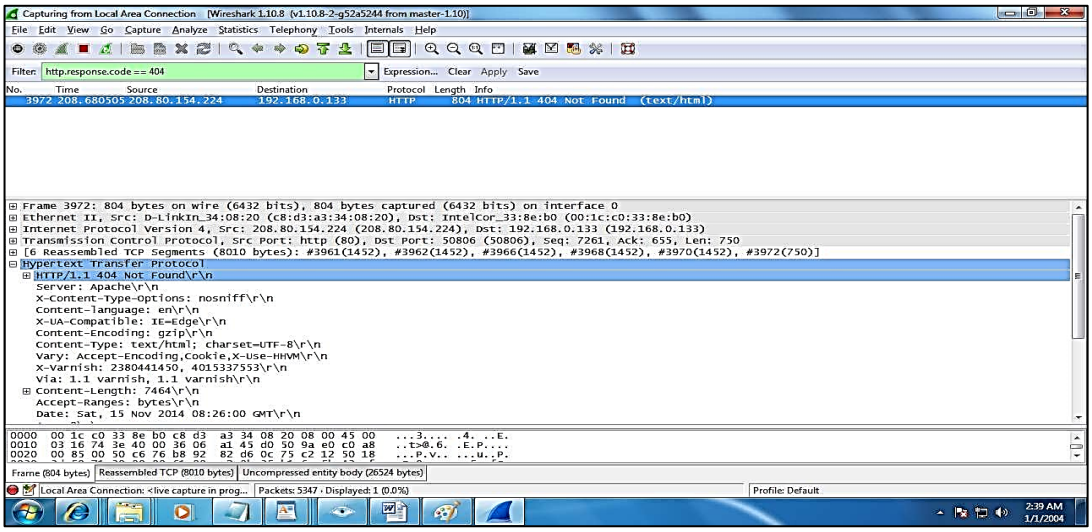
1. Filtering HTTP POST request



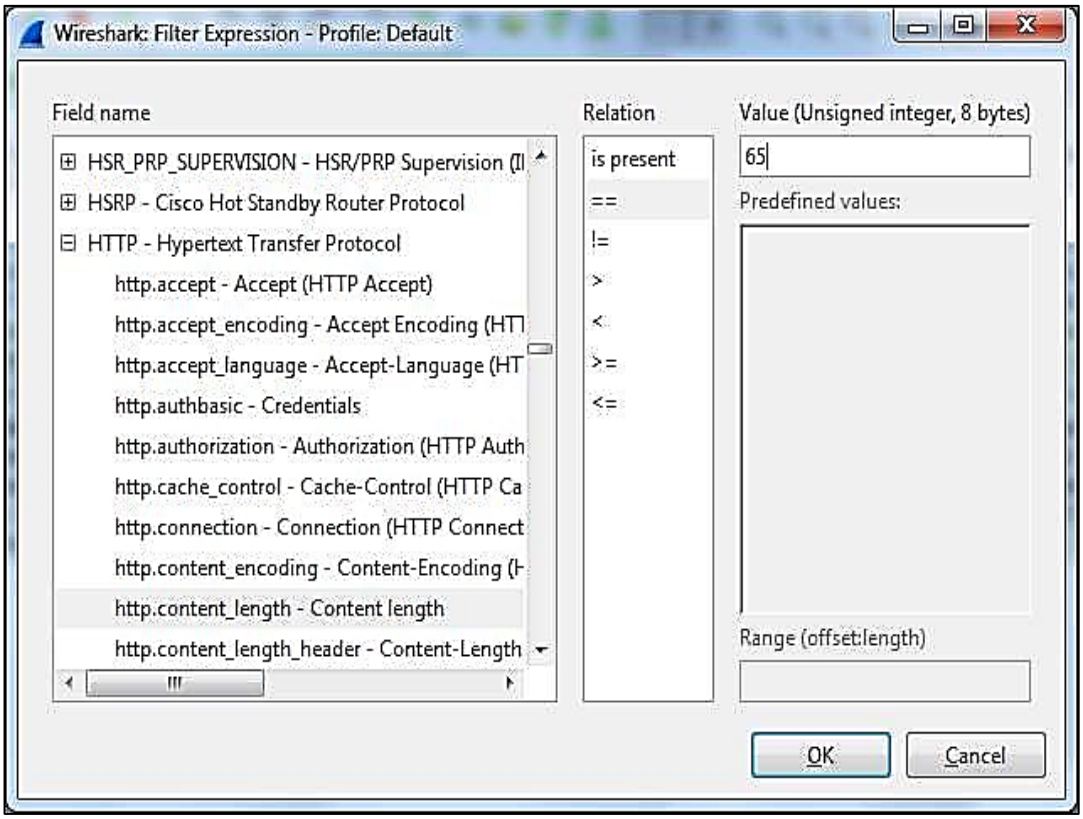


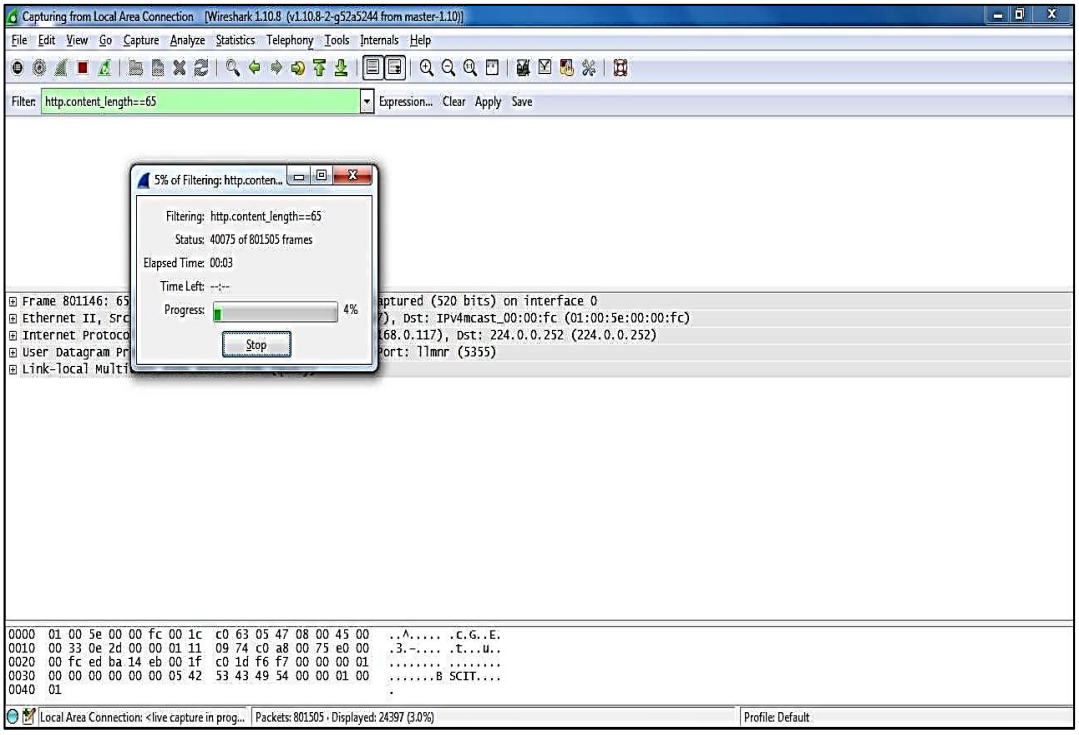
2. Filtering 404 not found error





3. Filtering using HTTP Content Length

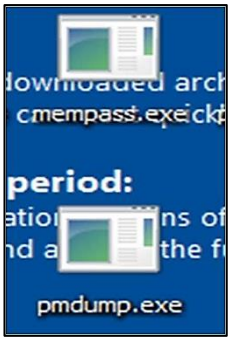




PRACTICAL 6

Aim: Dump Memory contents using PMdump

1. Here we will use program name mempass, and we will see how by using combination of pmdump and strings, we are able to dump the password in memory. Start mempass.exe




```
C:\Users\IEUser\Desktop>mempass
Please enter your password:hello
```

```
Administrator: C:\Windows\system32\cmd.exe - mempass
Press any key to continue . . .
```

2. Now open new terminal and run PMdump, pmdump –list will list the running program currently.

```
C:\Users\IEUser\Desktop>pmdump

pmdump 1.2 - (c) 2002, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
           - http://ntsecurity.nu/toolbox/pmdump/

Usage: pmdump <pid> <filename>

         - dumps the process memory contents to a file

       pmdump -list

         - lists all running processes and their PID's
```

```
C:\Users\IEUser\Desktop>pmdump -list

pmdump 1.2 - (c) 2002, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
           - http://ntsecurity.nu/toolbox/pmdump/

    0 - System idle process
    4 - System
  252 - smss.exe
  328 - csrss.exe
  364 - csrss.exe
  372 - wininit.exe
  400 - winlogon.exe
  460 - services.exe
  468 - lsass.exe
  476 - lsm.exe
  568 - svchost.exe
  624 - VBoxService.exe
  676 - svchost.exe
  780 - svchost.exe
  820 - svchost.exe
  848 - svchost.exe
  872 - svchost.exe
  996 - svchost.exe
 1148 - svchost.exe
 1256 - spoolsv.exe
 1292 - svchost.exe
 1384 - svchost.exe
 1424 - svchost.exe
 1584 - cygrunsrv.exe
 1660 - wlms.exe
 1696 - conhost.exe
 1720 - sshd.exe
 1932 - sppsvc.exe
  296 - svchost.exe
 1520 - taskhost.exe
 2280 - GoogleCrashHandler.exe
 2596 - svchost.exe
 2708 - SearchIndexer.exe
 2928 - dwm.exe
 2956 - explorer.exe
 3096 - VBoxTray.exe
 3560 - wuauclt.exe
 3104 - cmd.exe
 2700 - conhost.exe
 3808 - cmd.exe
 1992 - conhost.exe
```

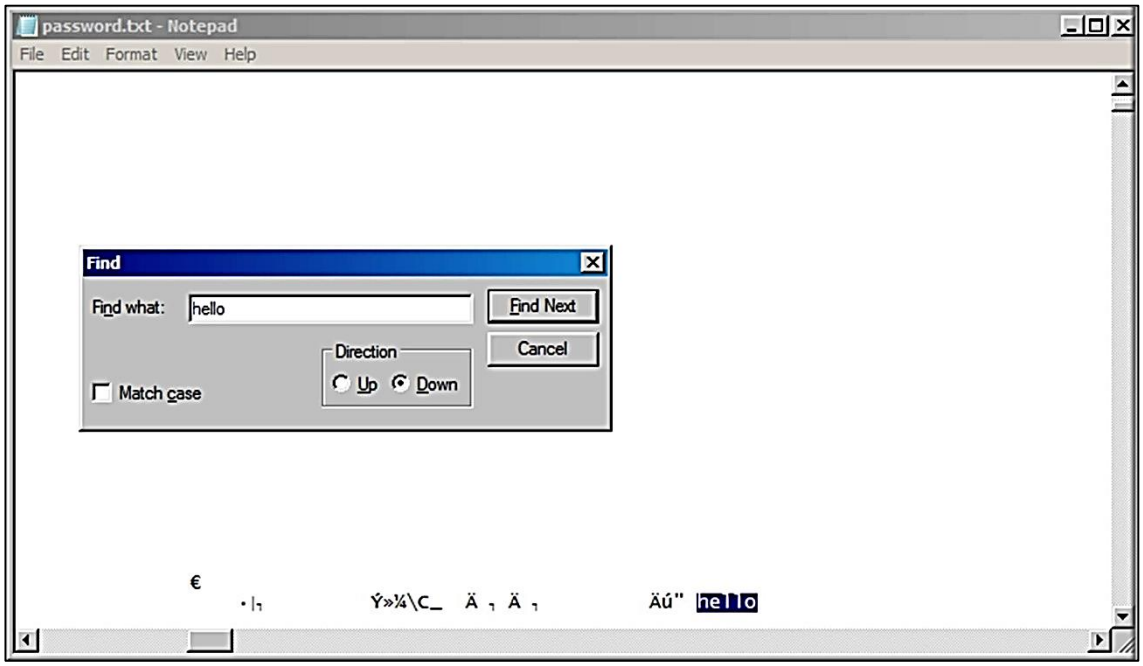
```
 2076 - taskeng.exe
 3456 - mempass.exe
  976 - cmd.exe
 2120 - pmdump.exe

C:\Users\IEUser\Desktop>mempass 3456 paswd.txt
```

3. Here we can see the pid of mempass i.e., 3456. We will dump the entire memory of mempass program in paswd.txt file.

```
C:\Users\IEUser\Desktop>mempass 3456 paswd.txt
Please enter your password:hello_
```

4. File name paswd is created having direct memory of mempass program without tampering the running mempass program

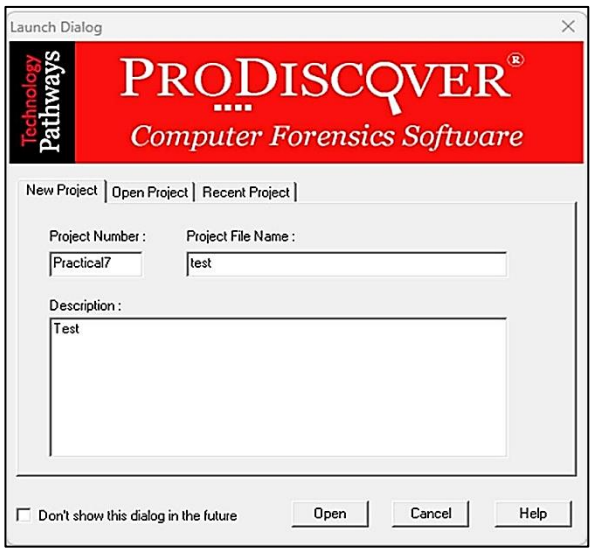


In this way, we can retrieve passwords from applications which store them in memory without any form of encryption.

PRACTICAL 7

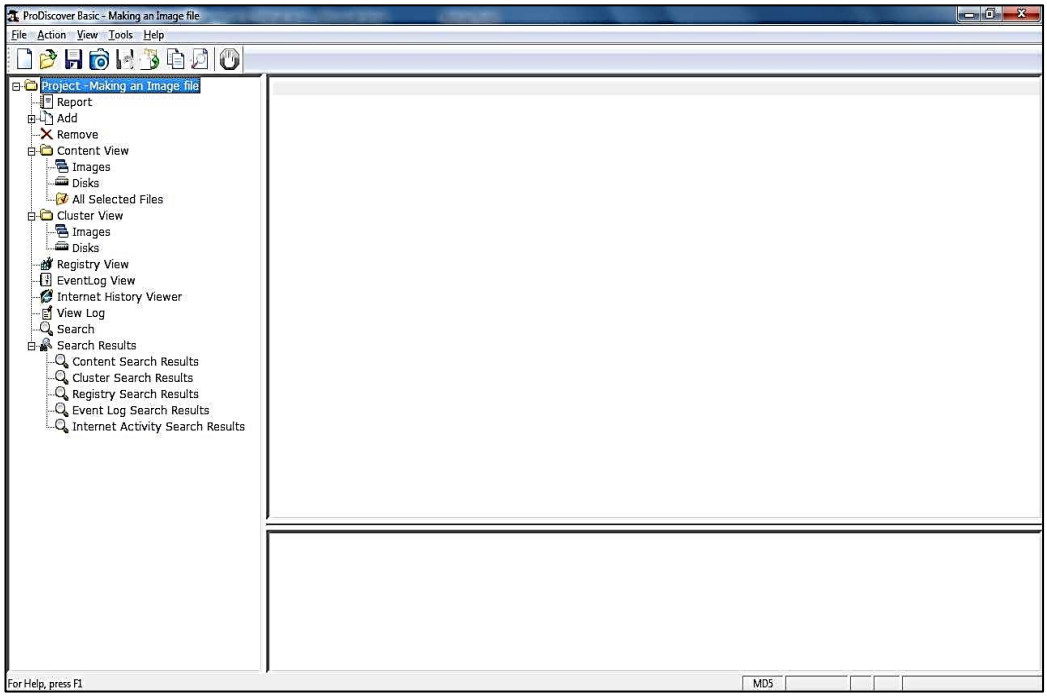
Aim: Using Data Acquisition Tools [ProDiscover Pro]

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



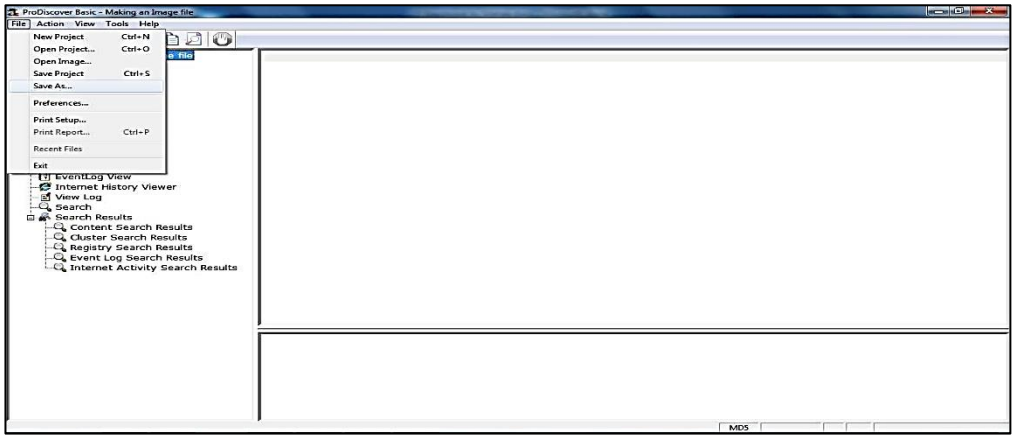
Step 2) Enter a project number, project name, and description of the project in the new project taboption, and then click the Open button.

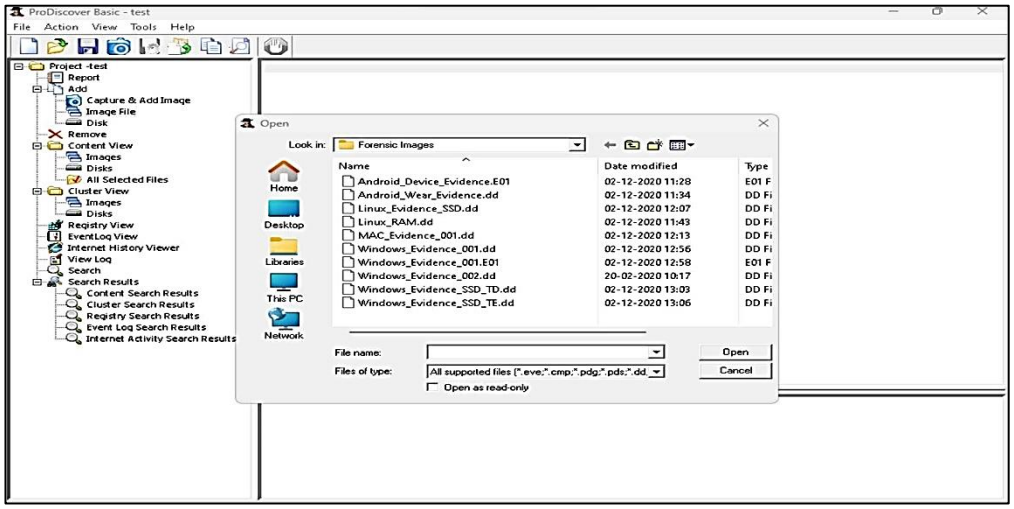
ProDiscover will then create a project and generate a template report in the work area.

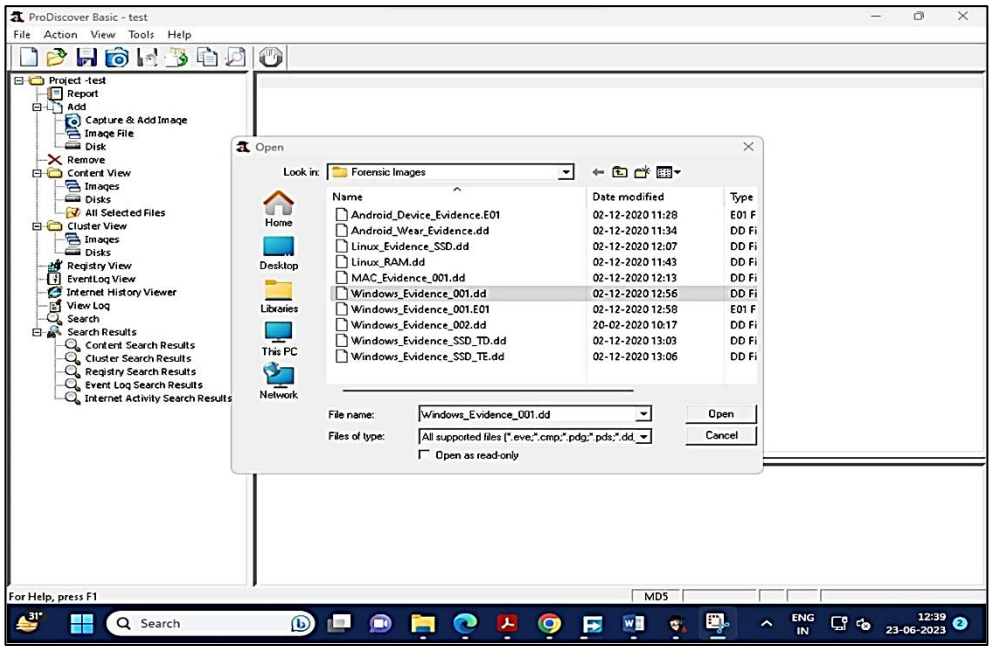


Step 3) Open Image:

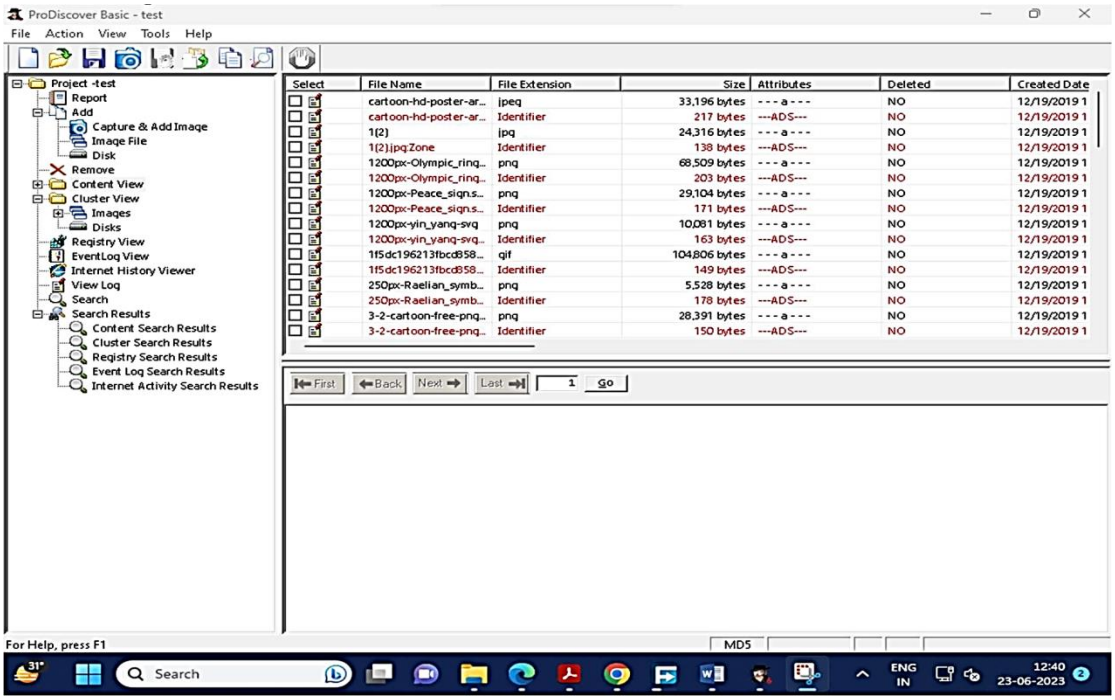
1. Select save project option from the file menu, or button bar and Open Image option.



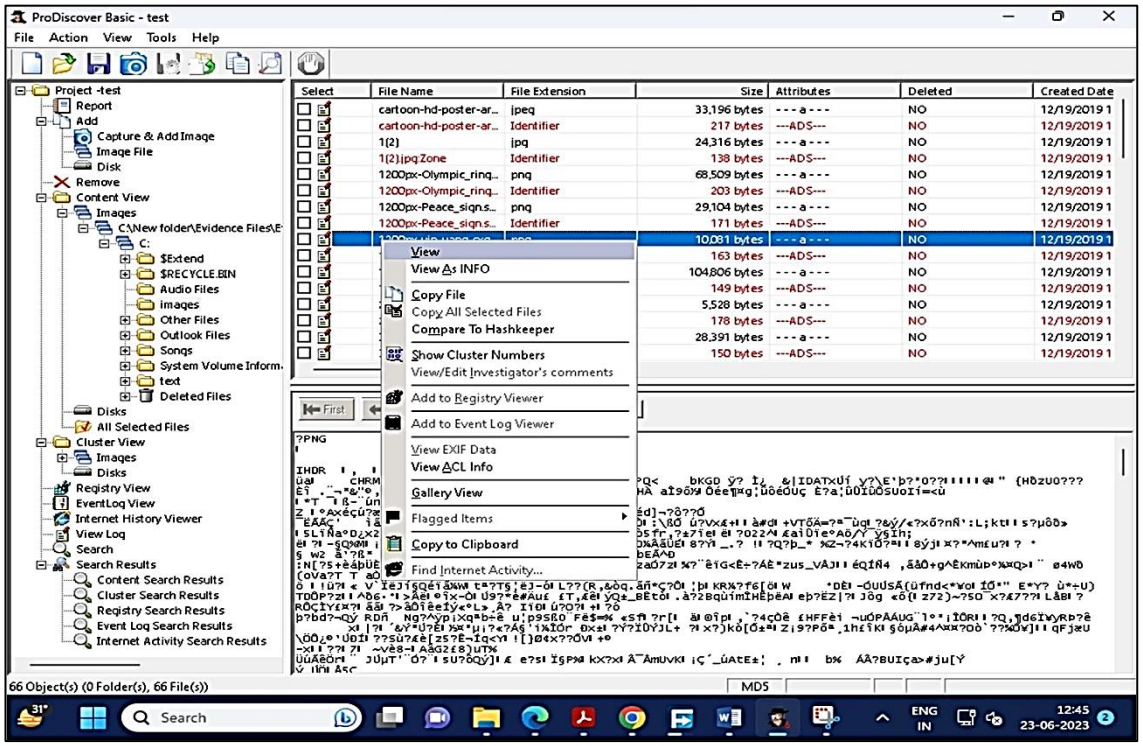




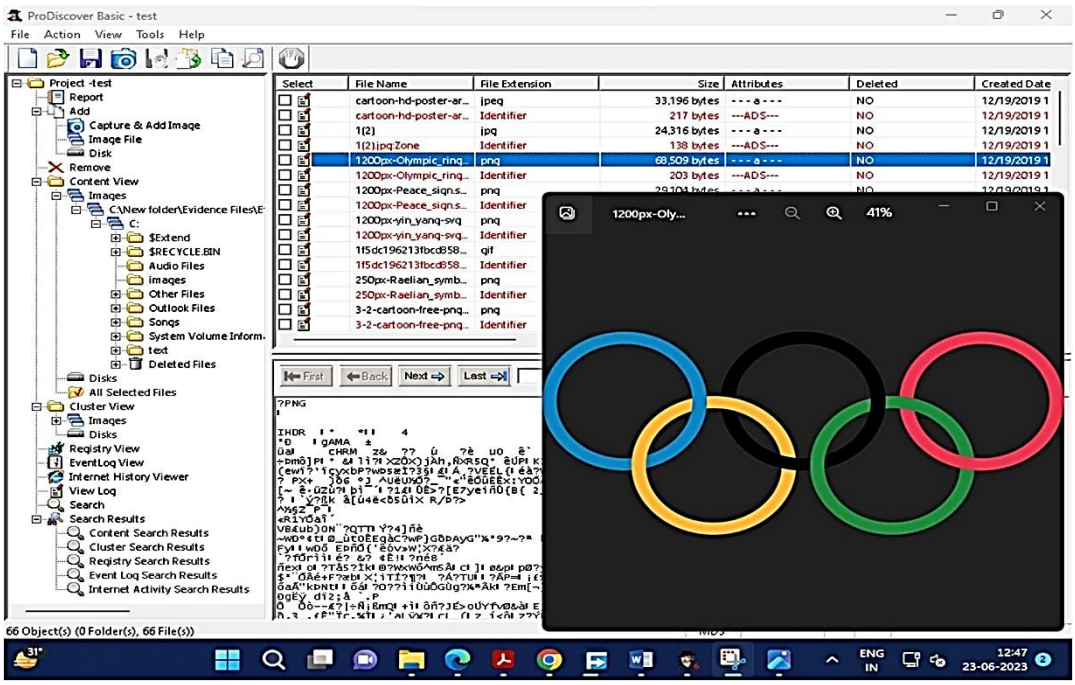
Step 4) ProDiscover displays the contents of the selected file at the bottom of the main window. Right click on a file.



Step 5) In ProDiscover a pop-up dialog with the choice to View or Recover the selected file. Select View



Step 6)For further study, we can also copy the file at desired location

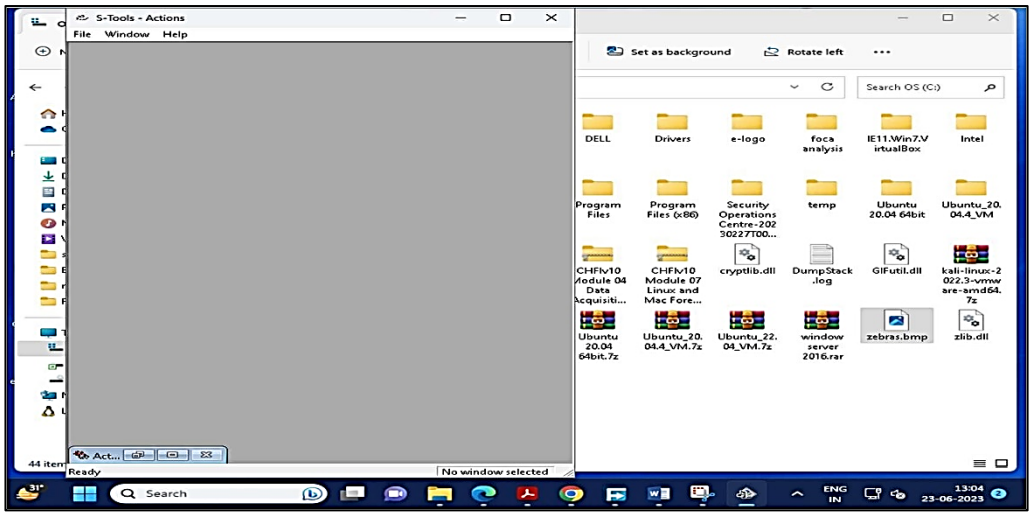


PRACTICAL 8

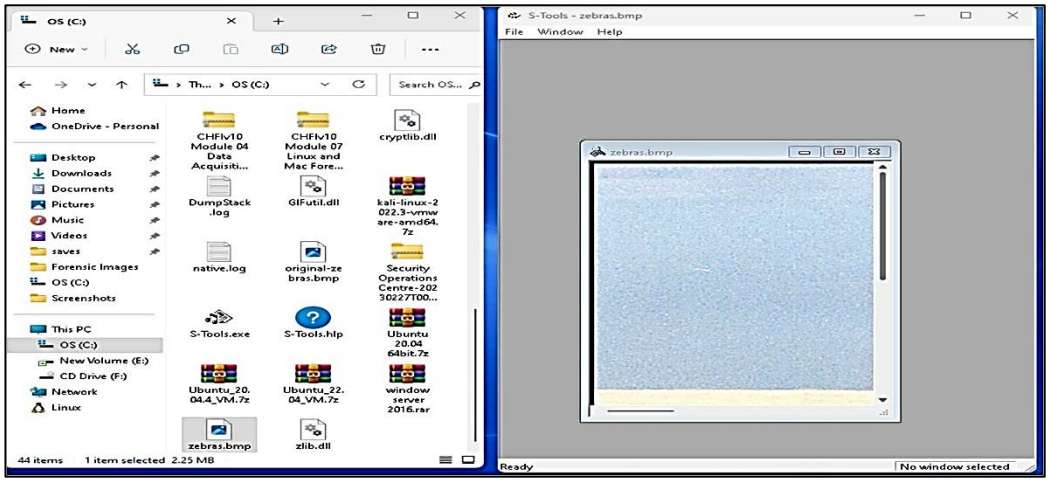
Aim: A) Using Steganography Tools [S-Tools]

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

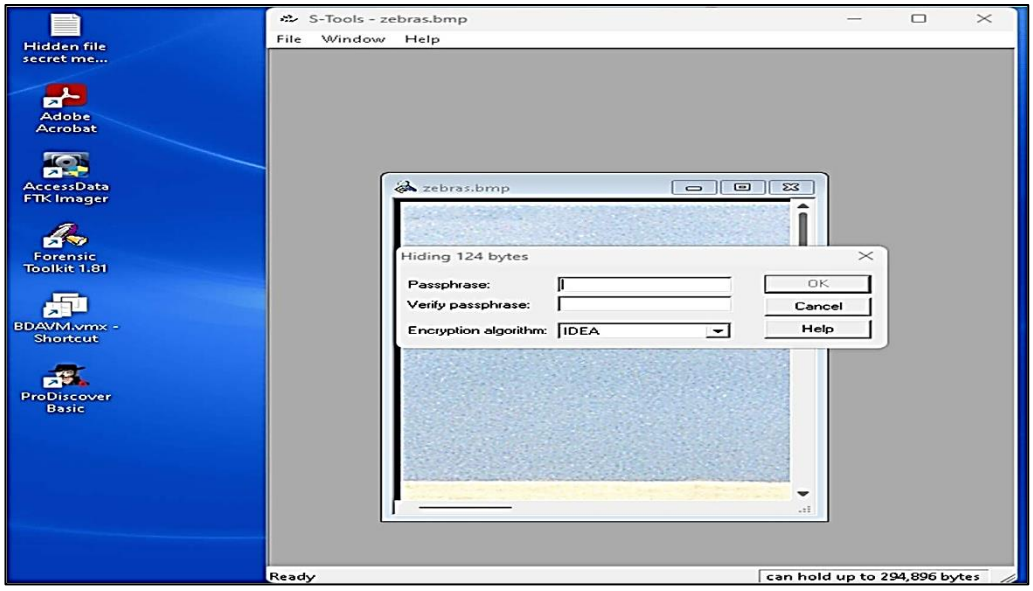
If your image is in .jpg format, convert it to .bmp format.

Step 4) Select a file to hide within the base file. If it's not there, create a txt file and save the file. Here we have created file name Hidden file

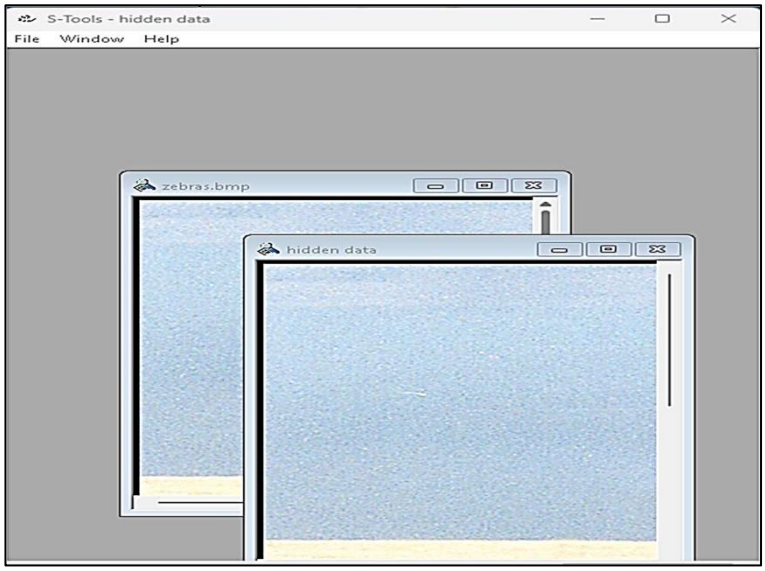
Step 5) The *.txt text file is selected and dragged on top of the base image. Release the file while the cursor is still on top of the base file.

Step 6) 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 7) Select the 'OK' button after entering a valid passphrase.



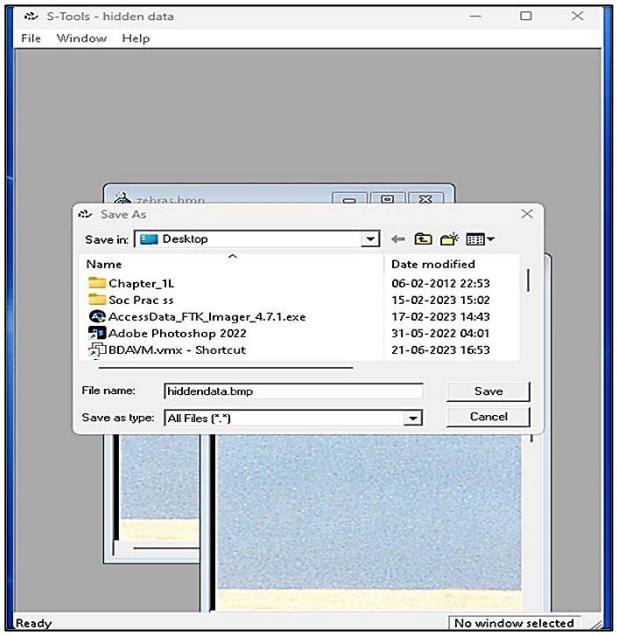
Step 8) The S-Tools main window will appear and a new file will be visible. The name of the file will be called hidden data by default.



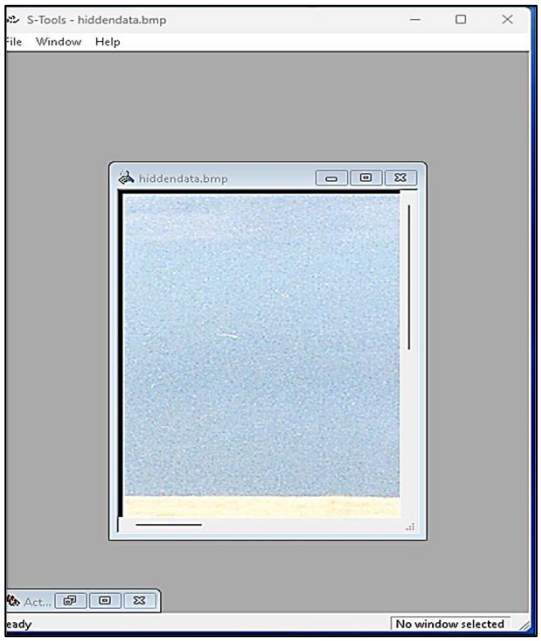
Step 9) Place the cursor on top of the hidden data image and select the right mouse button.The user willhave four options available to them:

- Save
- Save As
- Properties
- Reveal

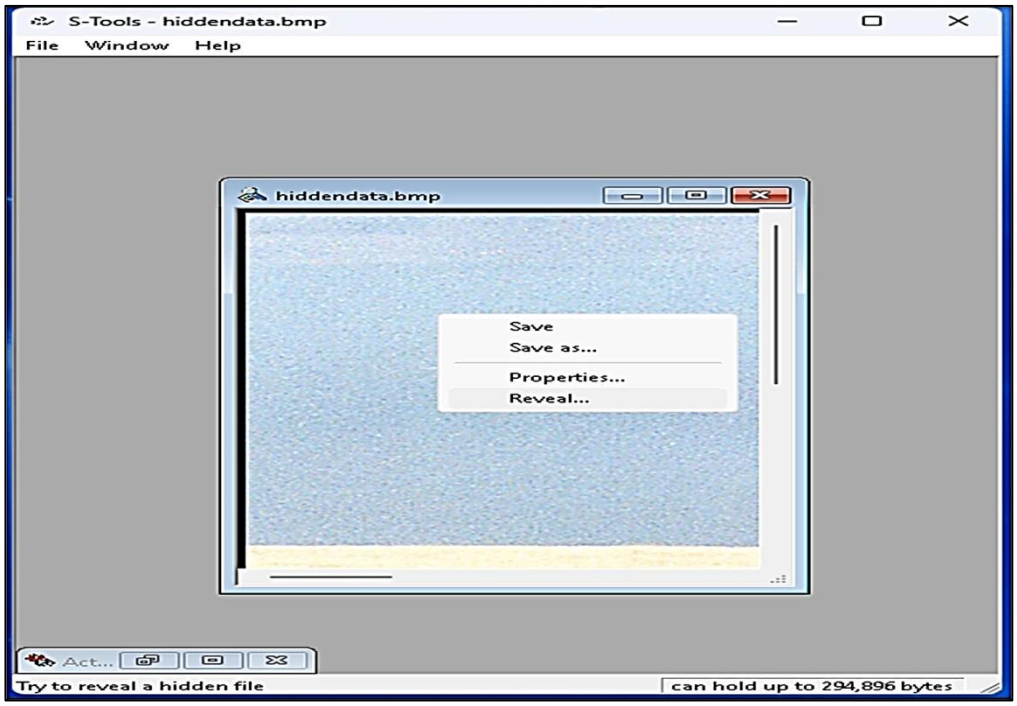
Select the ‘Save As’ button.



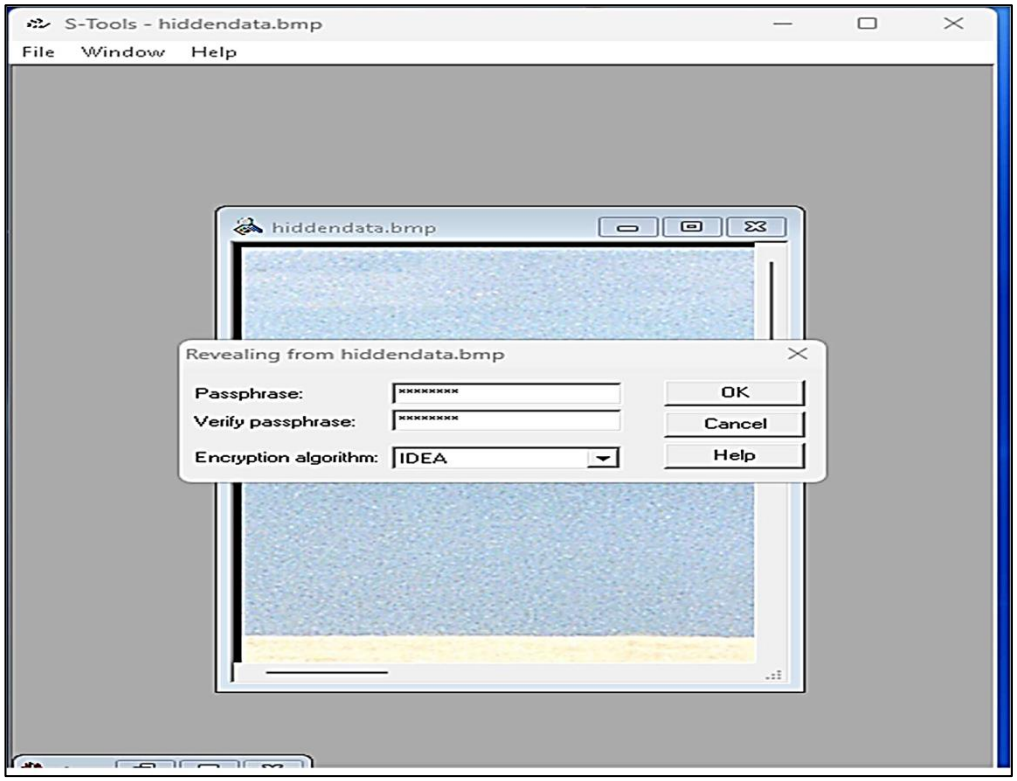
Step 10) A ‘Save As’ dialogue box will appear. Enter a valid file name, select the working directory and select the ‘Save’ button.



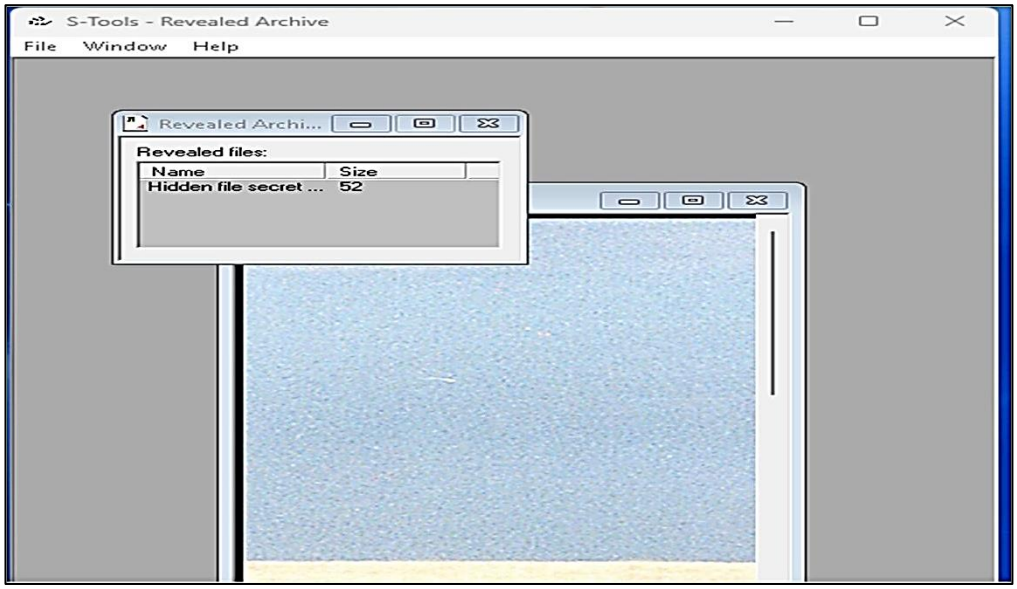
Step 11) Selecting the 'Reveal' button will display a passphrase dialogue box. A passphrase must be entered twice in the dialogue box and the correct encryption algorithm must be selected.



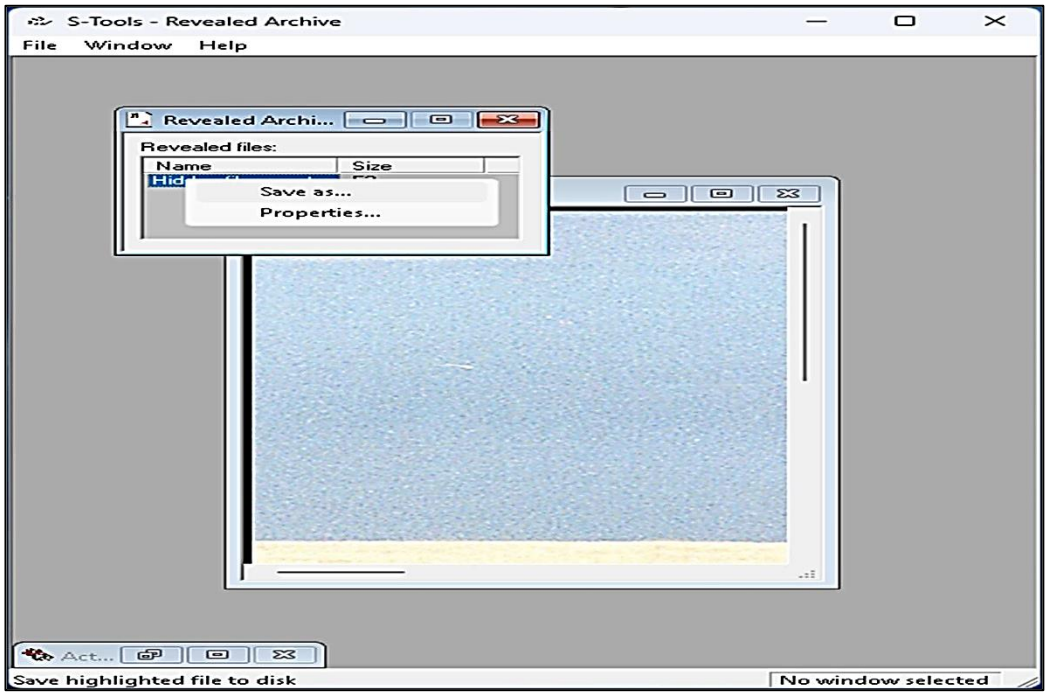
Step 12) Enter a passphrase twice, select the encryption algorithm, and select the 'OK' button.



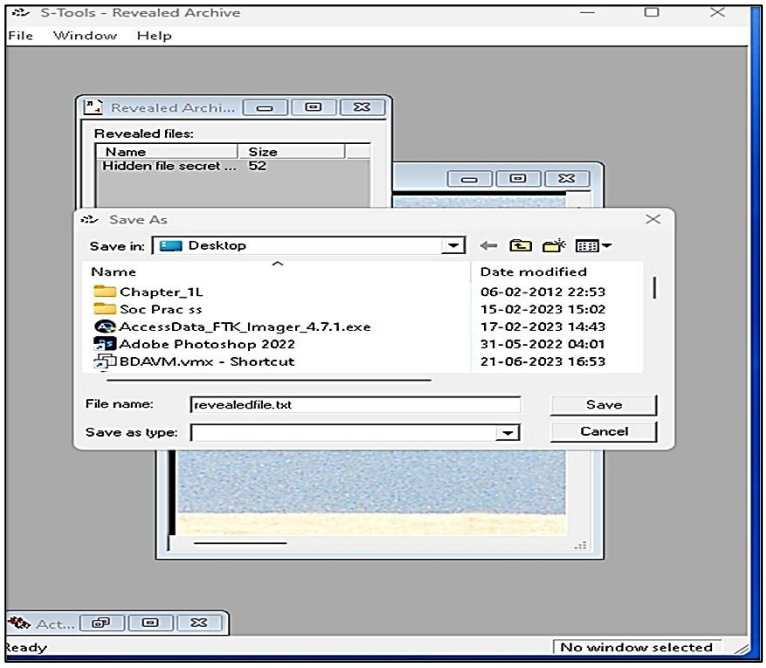
Step 13) A 'Revealed Archive' dialogue box will display which contains the file name and size of the hidden file.



Step 14) Select the 'Save As' button.

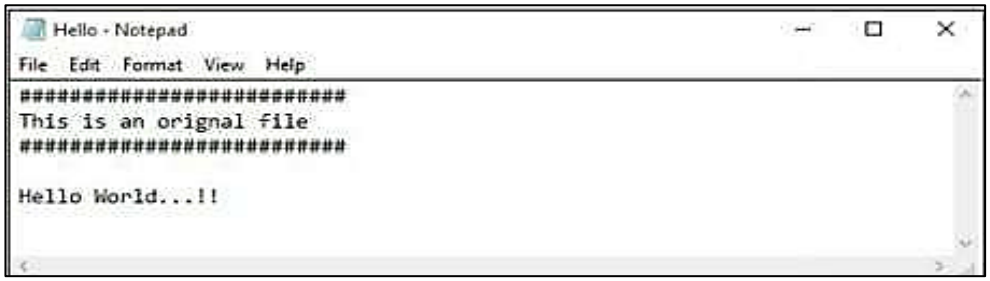


Step 15) The Revealed data is saved in revealfile.txt

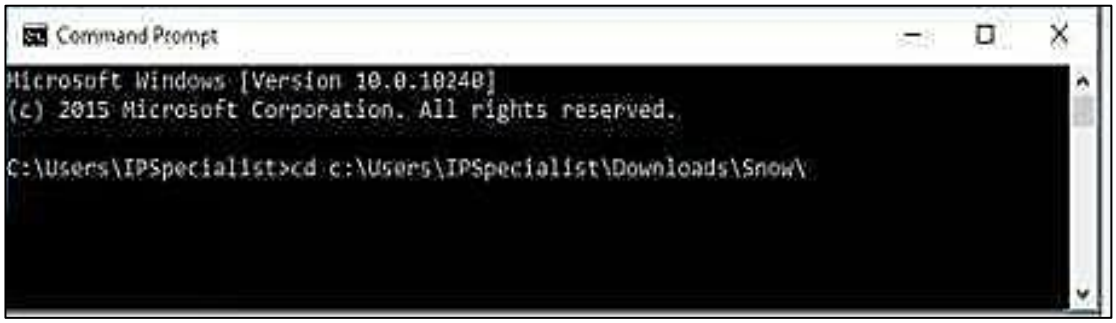


B) Using Whitespace Stegnography tool SNOW

Step 1) Create a text file with some data in the same directory where Snow Tool is installed.



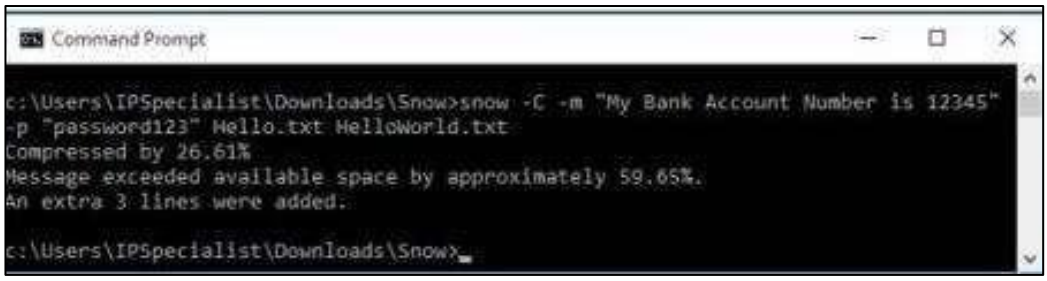
Step 2) Go to Command Prompt. Change the directory to run Snow tool



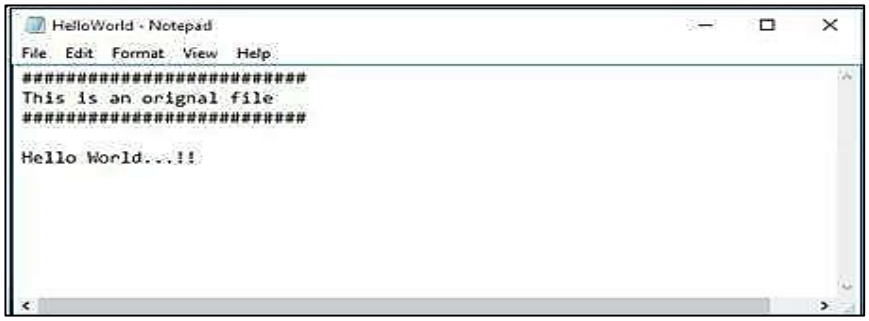
Step 3) Type the command

Snow –C –m "text to be hide" –p "password" <Sourcefile><Destinationfile>

The source file is a Hello.txt file as shown above. Destination file will be the exact copy of source file containing hidden information.



Go to the directory; you will a new file HelloWorld.txt. Open the File

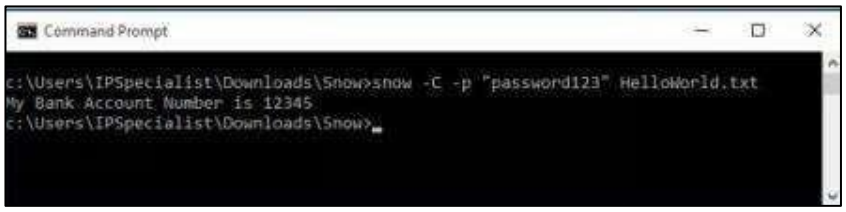


Step 4) New File has the same text as an original file without any hidden information. This file can be sent to the target.

Recovering Hidden Information

On destination, Receiver can reveal information by using the command

Snow –C –p "password123" HelloWorld.txt

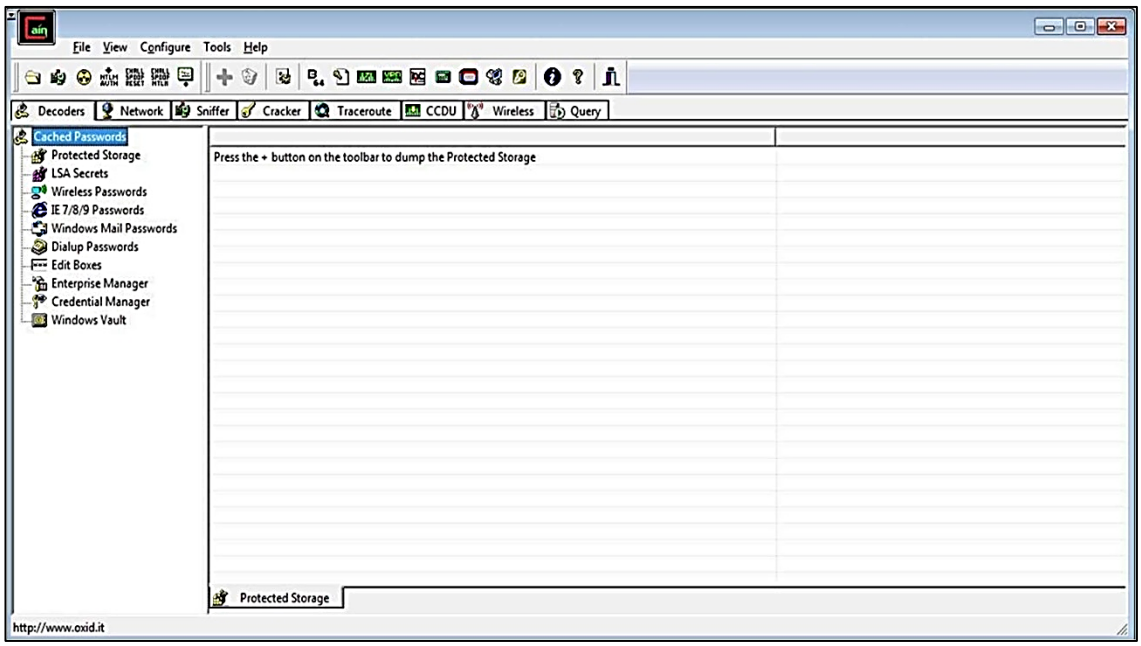


As shown in the above figure, File decrypted, showing hidden information encrypted in the previous section.

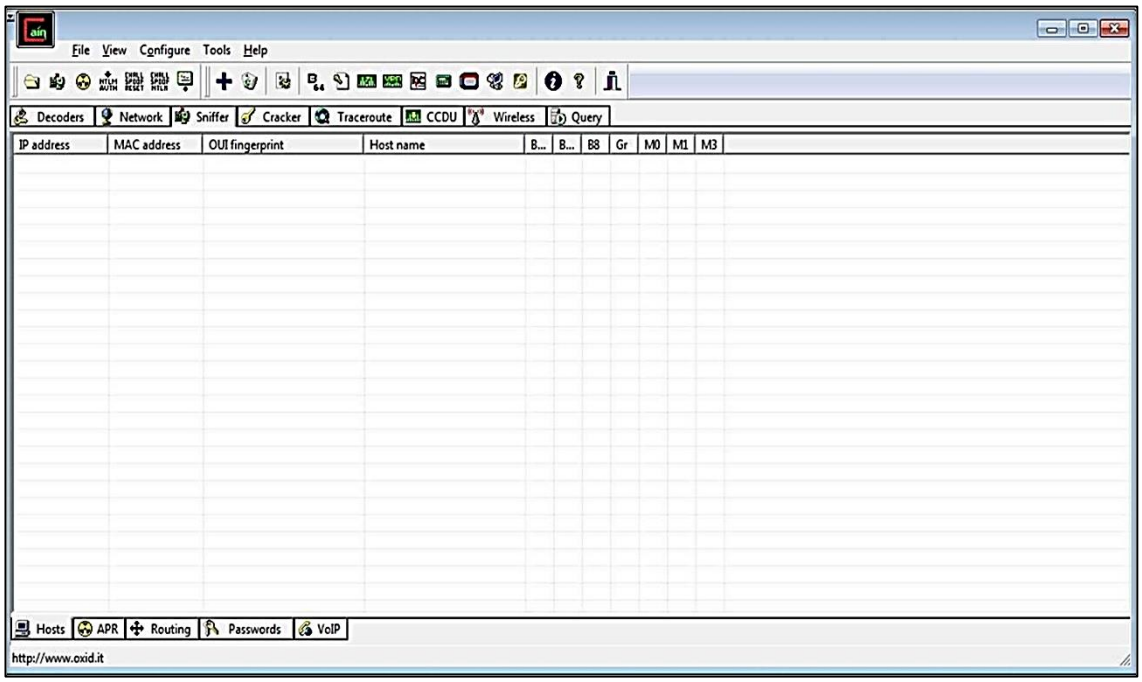
PRACTICAL 9

A. Performing Password Cracking [Cain & Abel]

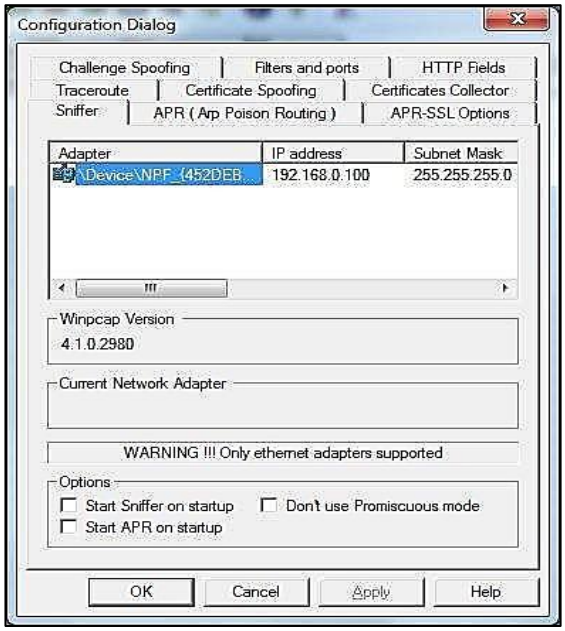
Step 1: Install and open cain and abel.



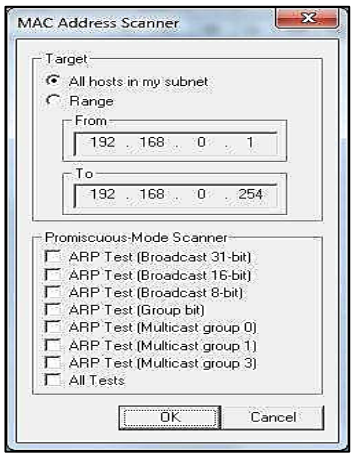
Step 2: Select sniffer on the top.



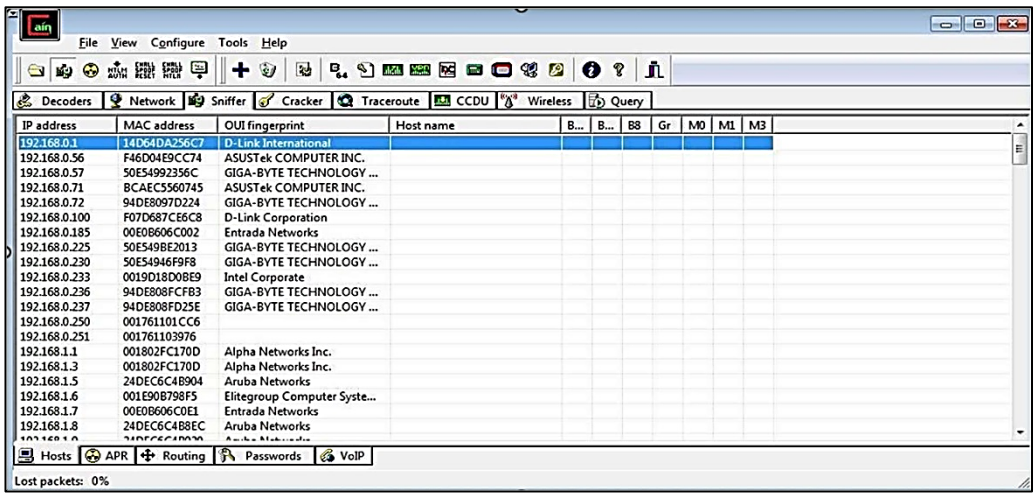
Step 3: Next to folder icon click on icon name start/stop sniffer. Select device and click on ok.



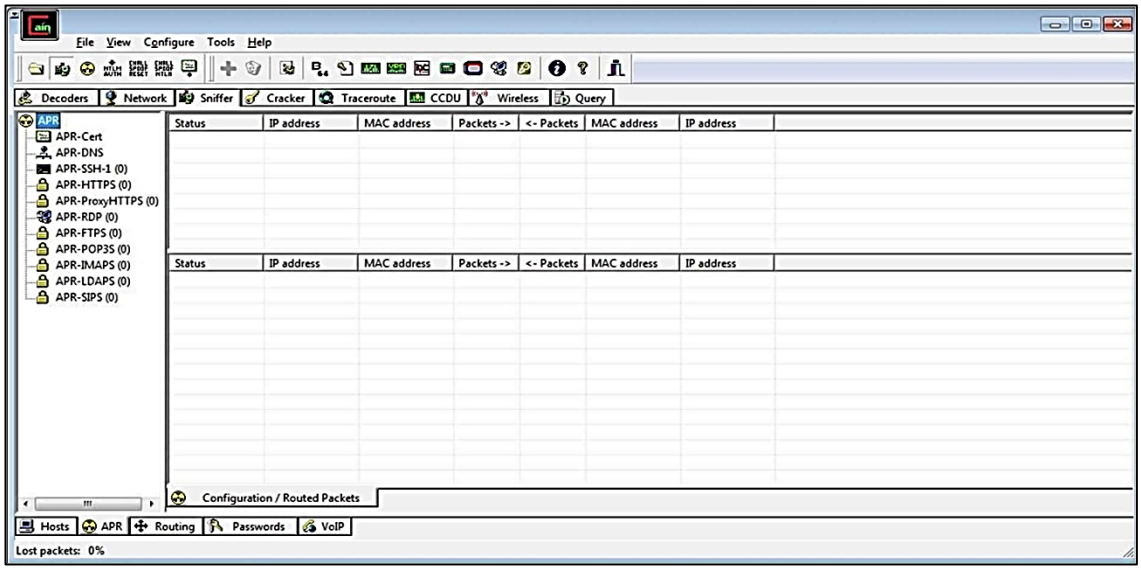
Step 4: Click on "+" icon on the top. Click on ok.



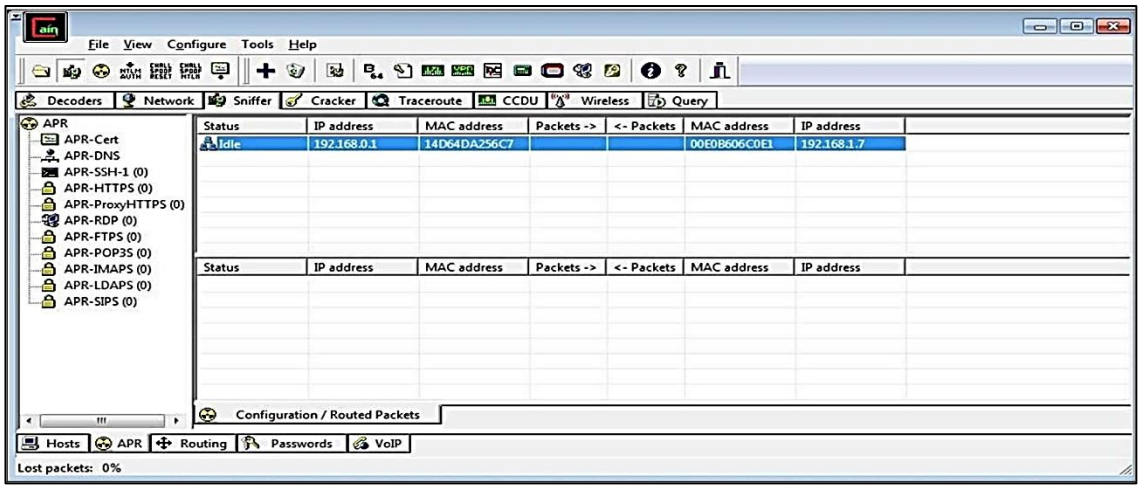
Step 5: Shows the Connected host.



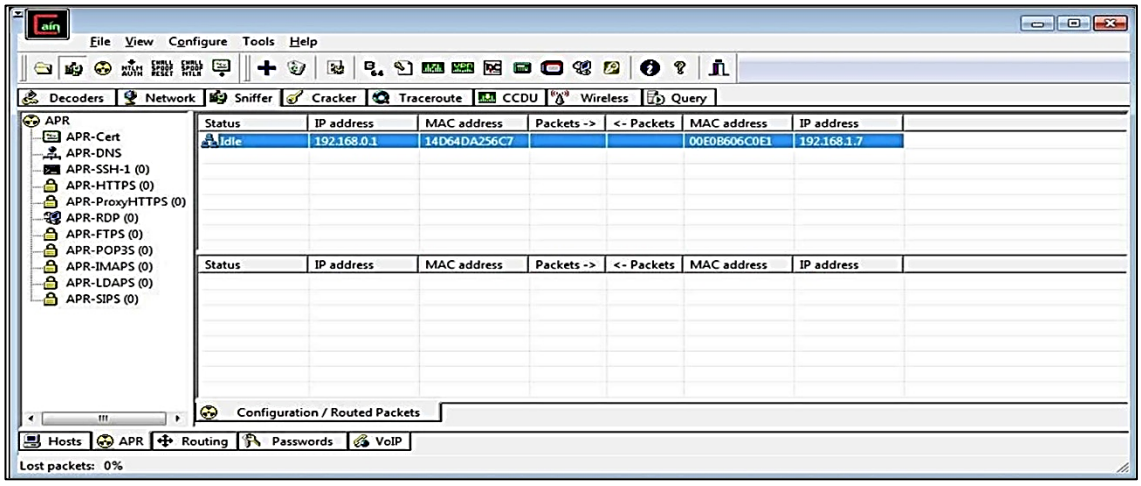
Step 6: Select Arp at bottom.



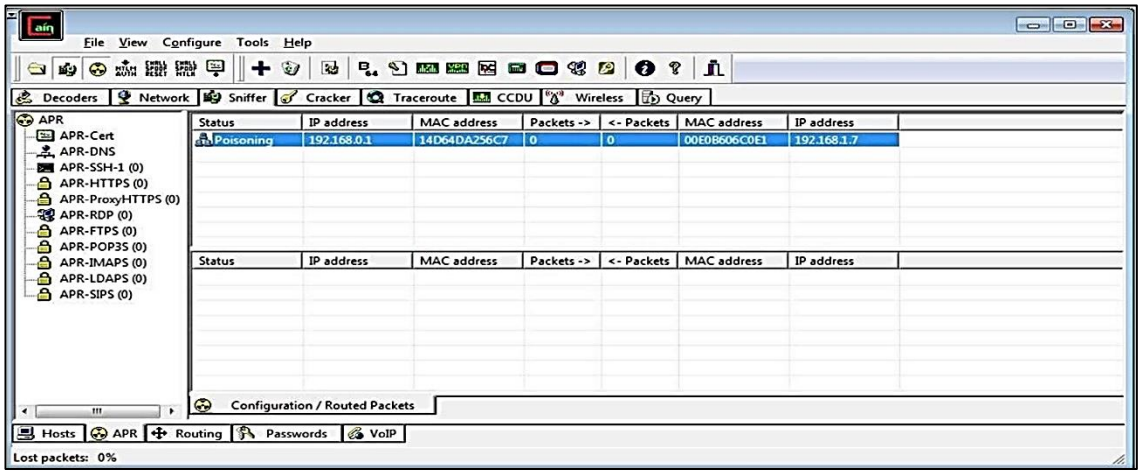
Step 7: Click on "+" icon at the top.



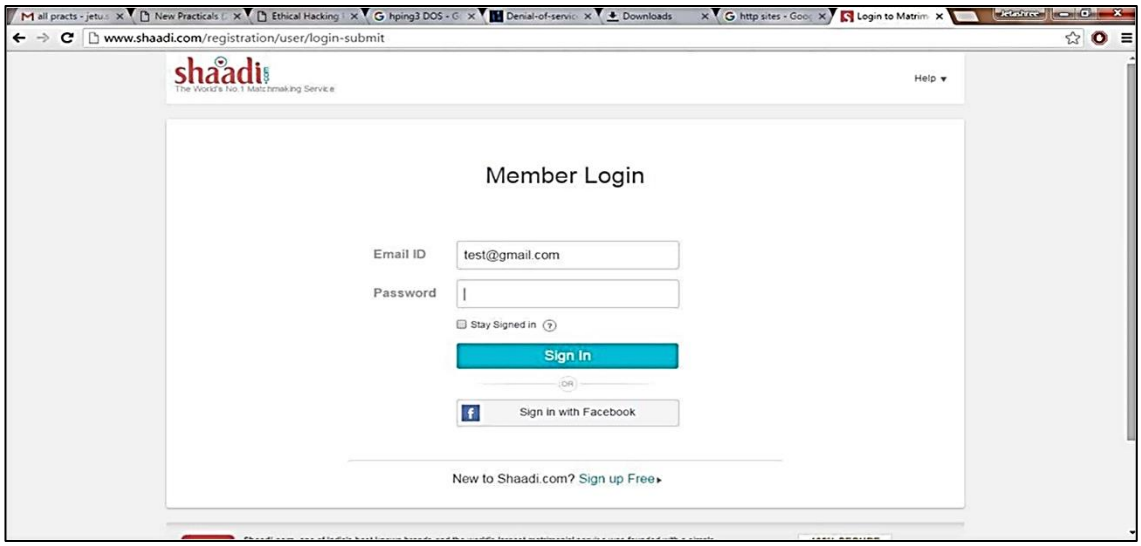
Step 8: Click on start/stop ARP icon on top.



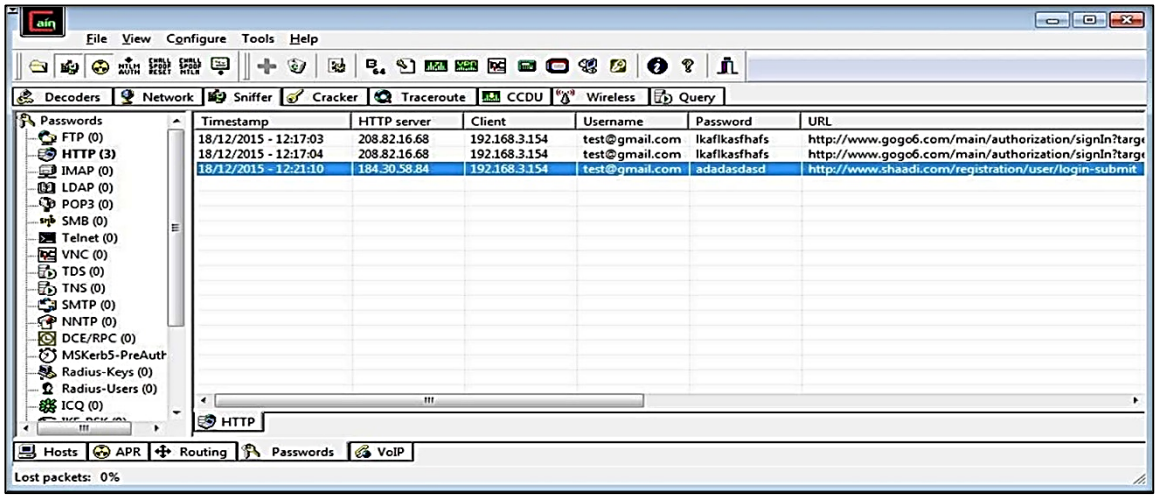
Step 9: Poisoning the source.



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



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



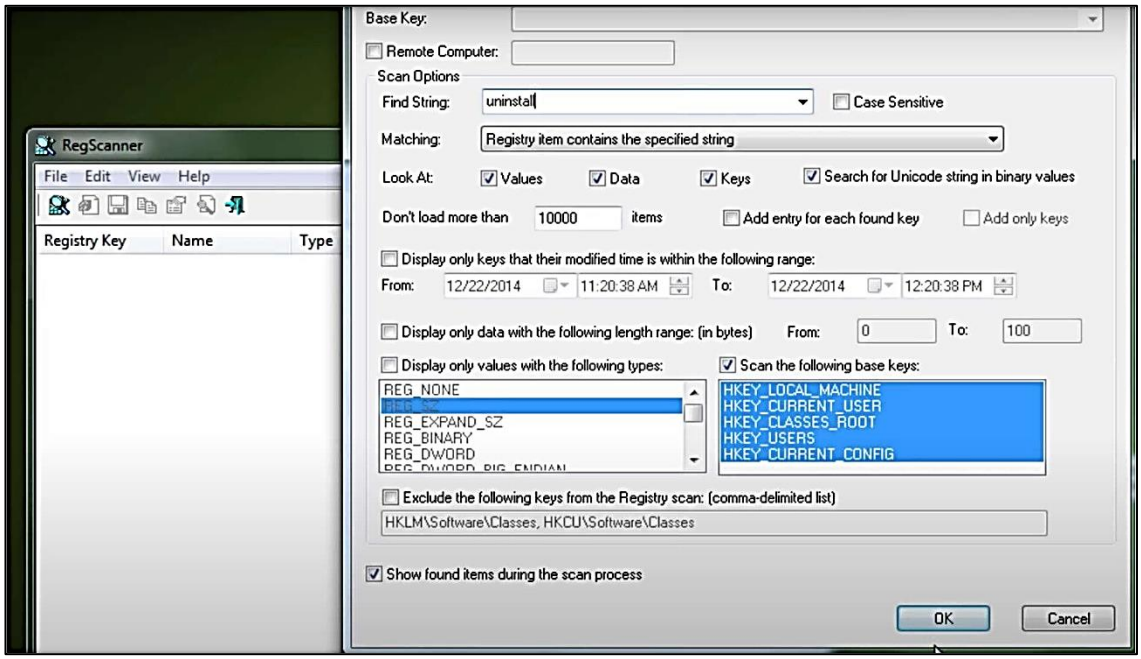
PRACTICAL 10

Aim: Scan Registry using RegScanner

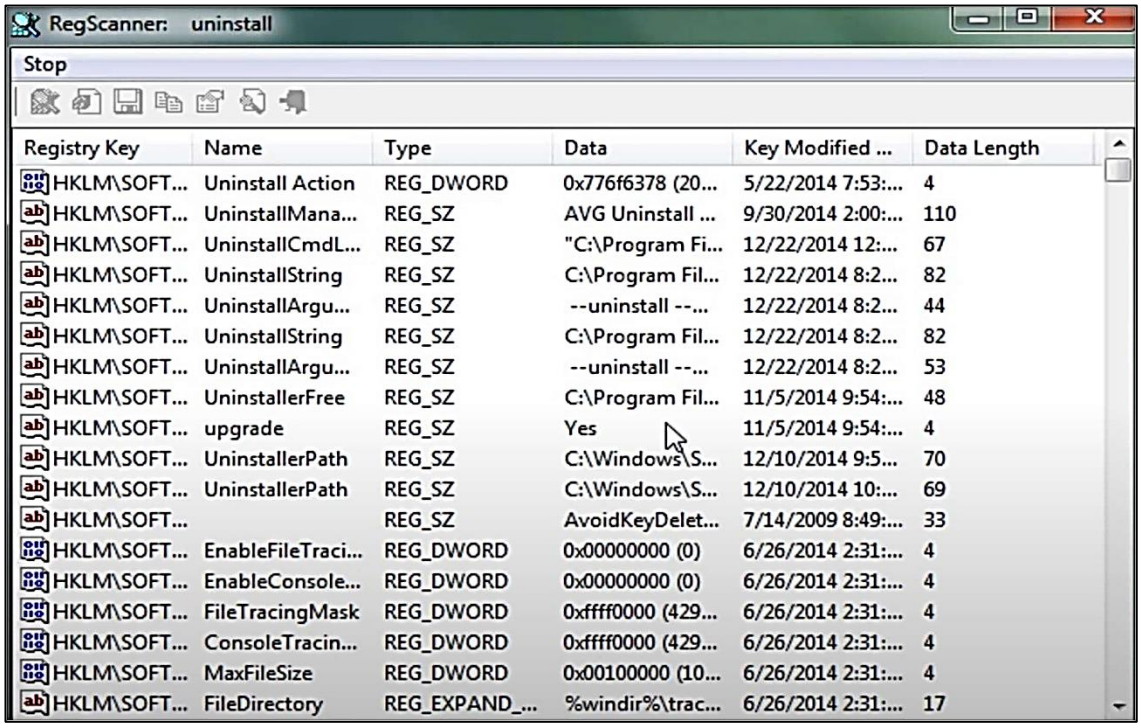
Step 1) Download and Install RegScanner

Step 2) Quickly scan your Registry and Search for the specific values with RegScanner

You can select to scan the base keys and the string types. Enter the search string and start the scan



Step 3) Check the Scan Result



Step 4) You can save, copy or export the selected items, Export Reg values as REG or HTML files, and more