

## INDEX

Practical No.	Date	Name of Practical	Page No.	Signature
1		File System Analysis using The SleuthKit (Autopsy, fsstat, istat, fls and img_stat)	1	
2		Explore Windows forensic tools (OSForensics)	10	
3		Using Forensic Toolkit(FTK) & Writing report usingFTK (AccessData FTK)	23	
4		a. Using File Recovery Tools [FTK Imager] Creating Image  b. Recover Deleted files using Recuva, PC Inspector File Recovery, Recover My Files	30	
5		a. Using Web attack detectiontools [Wireshark]  b. Using Log & Traffic Capturing & Analysis Tools [Wireshark]	47	
6		Dump Memory contents using PMdump	67	
7		Dump Memory contents using PMdump	69	
8		a. Using Steganography Tools [S-Tools]  b. Using Whitespace Stegnography tool SNOW	73	
9		Performing Password Cracking [Cain & Abel]	81	
10		a. Scan Registry using RegScanner	85	

## **PRACTICAL NO. 01**

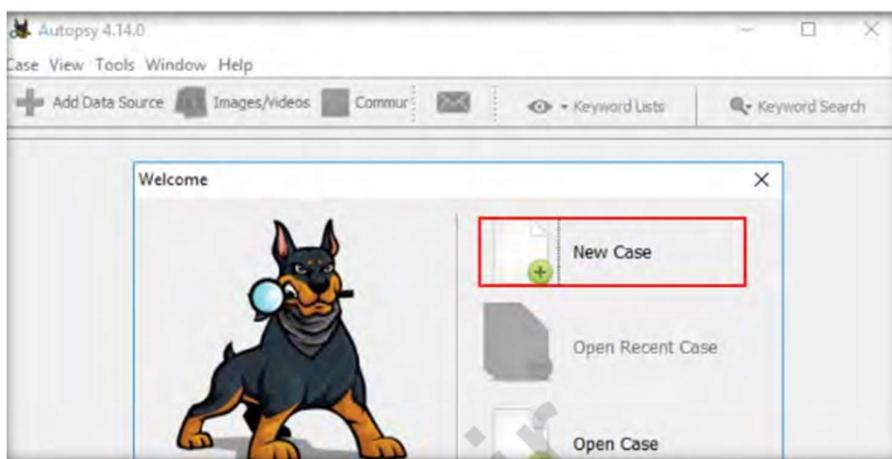
### **File System Analysis using The SleuthKit (Autopsy, fsstat, istat, fls and img stat)**

**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.

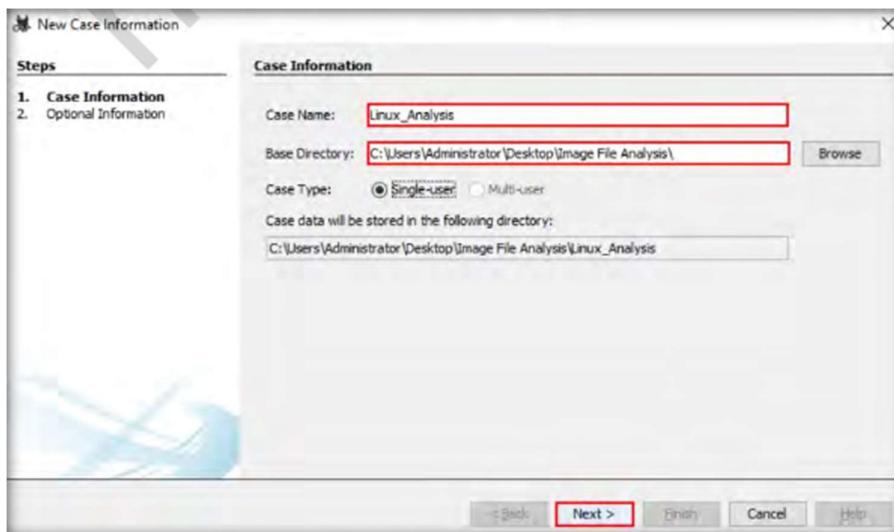


Autopsy Welcome window will appear along with Autopsy main window in the background. In the Welcome window, click New Case.

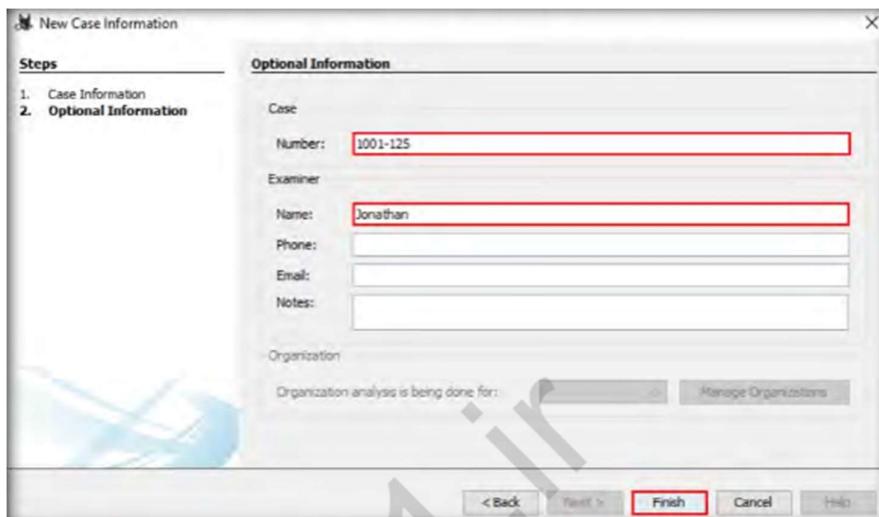


A New Case Information window opens asking you to input the Case Name and the Base Directory. The base directory is the location where the case data will get stored. The case name may be entered according to your identification purpose. In this lab, we are assigning the case name as Linux\_Analysis.7.

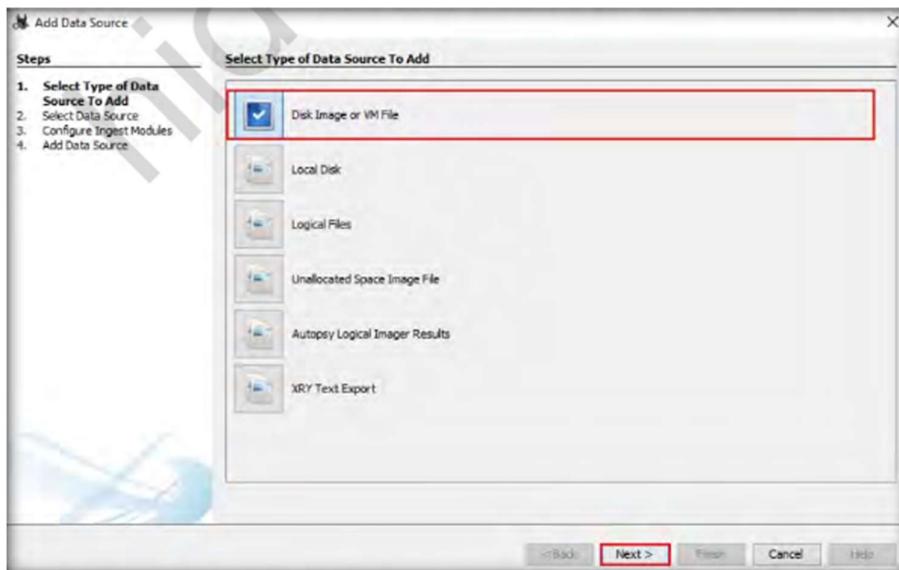
Before specifying the base directory, we will be creating a folder on the Desktop with the name Image File Analysis and setting the path of the Base directory to this folder. Upon setting the base directory, click Next



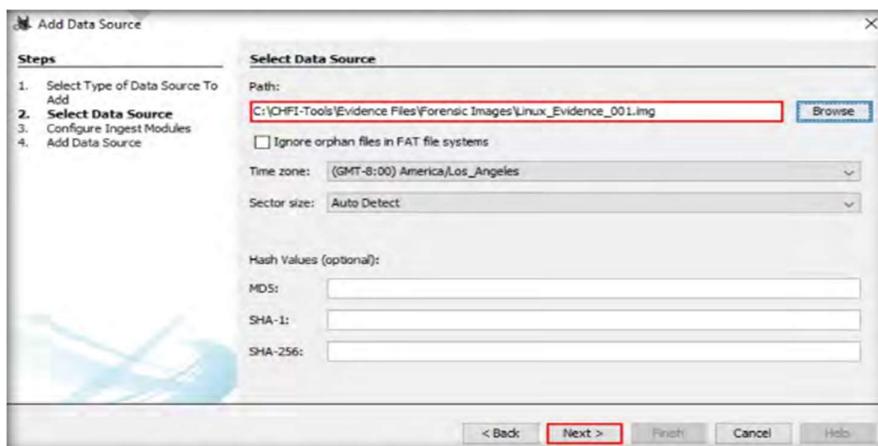
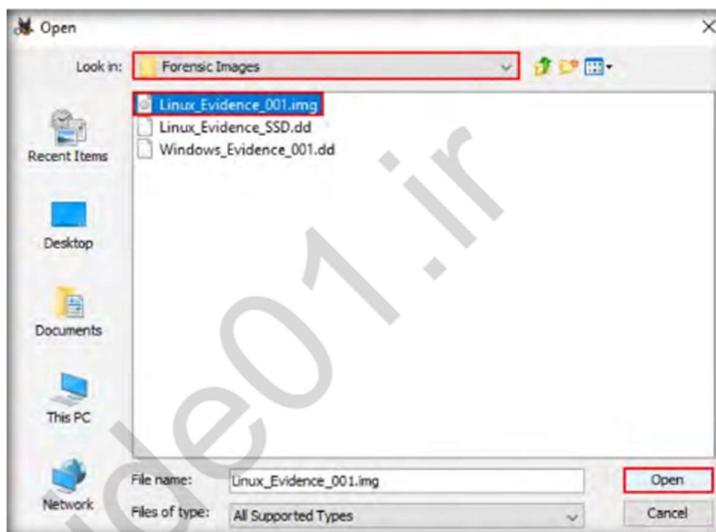
The New Case Information window now shows the Optional Information section where you can specify details such as name of the examiner and case number. For this lab, let us enter the name of the examiner as Jonathan and the case number as 1001-125. You may also fill out the other optional fields. Click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



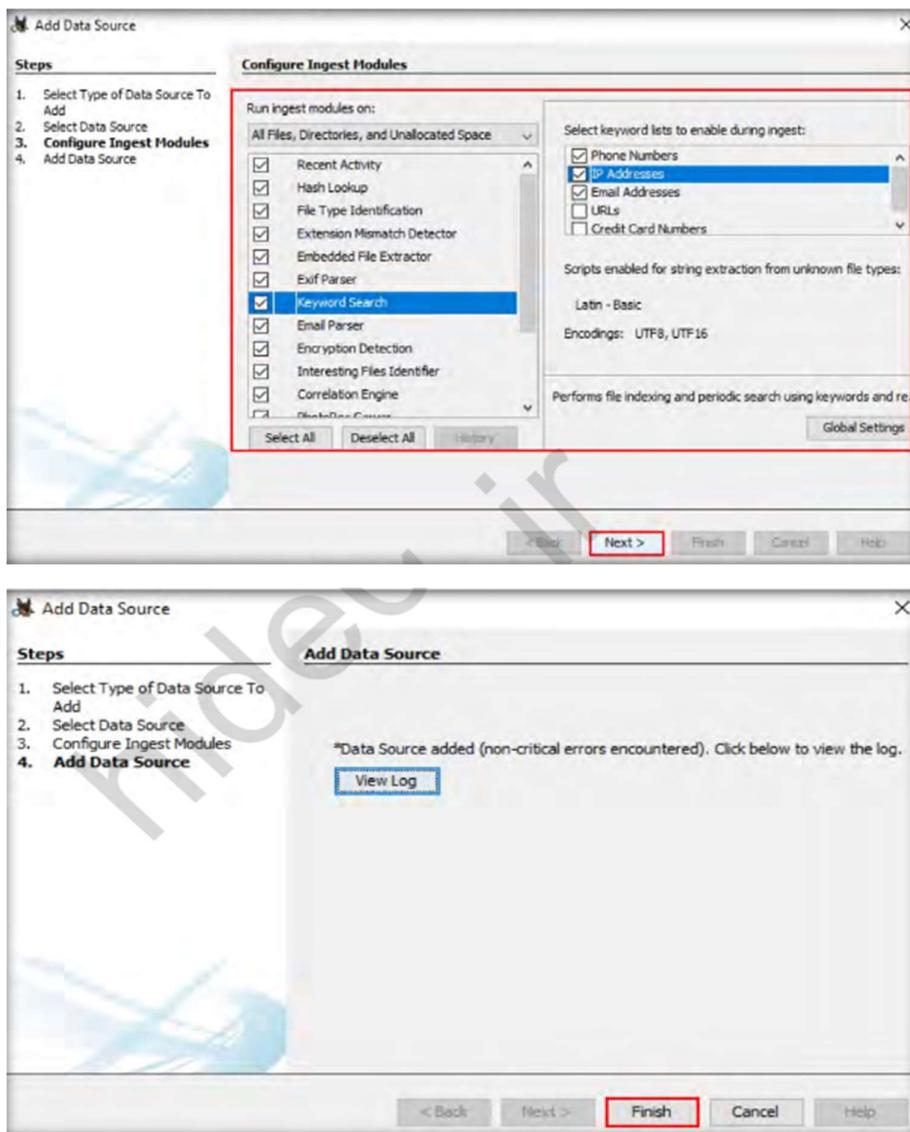
The Add Data Source window now appears displaying the section Select Type of Data Source to Add. Here, you need to select the type of data source to be provided as an input. In this lab, we will be analyzing a disk image; therefore, select the option Disk Image or VM File and click Next.



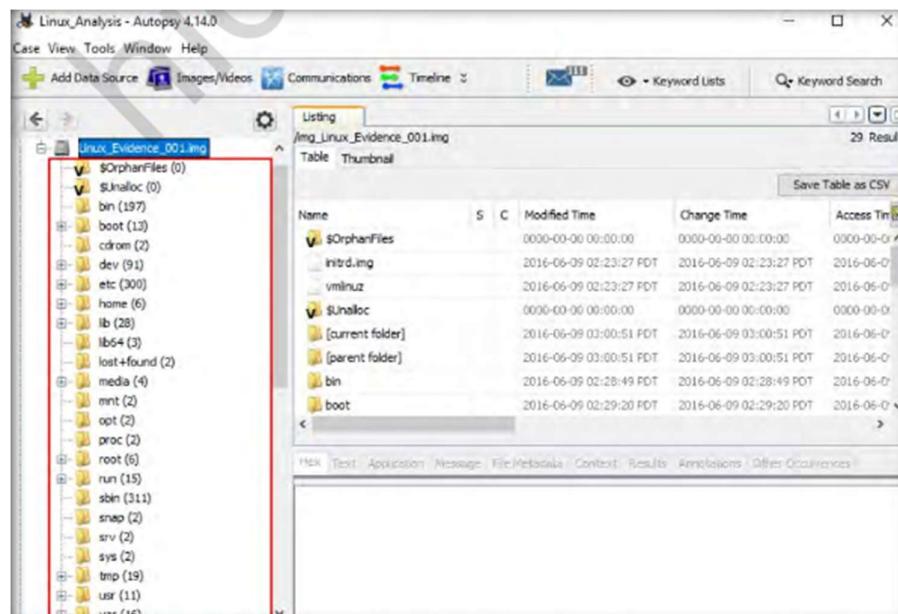
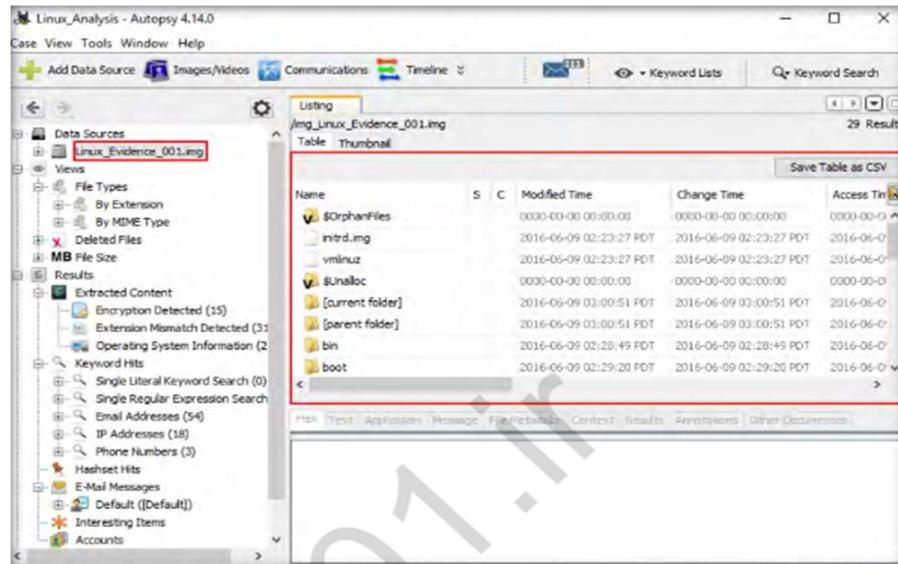
A window (named Open) will appear where you need to specify the forensic image. Navigate to C:\CHFI-Tools\Evidence Files\Forensic Images, select Linux\_Evidence\_001.img and click Open.



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 screenshot shows the Autopsy interface with the case name "Linux\_Analysis - Autopsy 4.14.0". The left pane displays a tree view of files and directories under "Data Sources" and "Linux\_Evidence\_001.img". The right pane shows a table of results for the query "/etc/passwd". One row, "passwd", is selected, and its content is shown in the bottom pane:

```

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/bin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin

```

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

The screenshot shows the Autopsy interface with the case name "Linux\_Analysis - Autopsy 4.14.0". The left pane displays a tree view of files and directories under "Data Sources" and "Linux\_Evidence\_001.img". The right pane shows a table of results for the query "SeatPlan.xls". One row, "SeatPlan.xls", is selected, and its details are shown in the bottom pane:

Name	S	C	Modified Time	Change Time
SeatPlan.xls			2011-09-28 01:02:55 PDT	2016-06-09 03:42:05 PDT

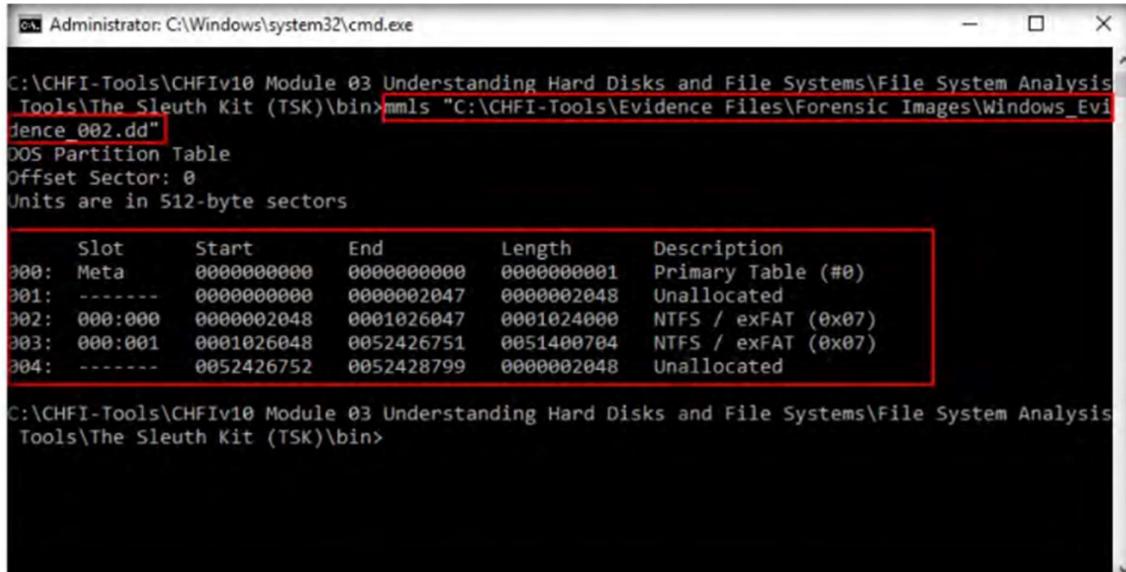
Click on File Metadata and scroll down the section to find the MD5 value for the SeatPlan.xls file.

The screenshot shows the Autopsy interface with the case name "Linux\_Analysis - Autopsy 4.14.0". The left pane displays a tree view of files and directories under "Data Sources" and "Linux\_Evidence\_001.img". The right pane shows a table of results for the query "SeatPlan.xls". The "File Metadata" tab is selected, and the MD5 value is highlighted in red:

Modified	2011-09-28 01:02:55 PDT
Accessed	2016-06-09 03:06:45 PDT
Created	2016-06-09 03:06:45 PDT
Changed	2016-06-09 03:42:05 PDT
MD5	<b>15064adfeb6e31320ba904927749efdf</b>

## To study fsstat

To view partition tables associated with Windows\_Evidence\_002.dd, type "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:

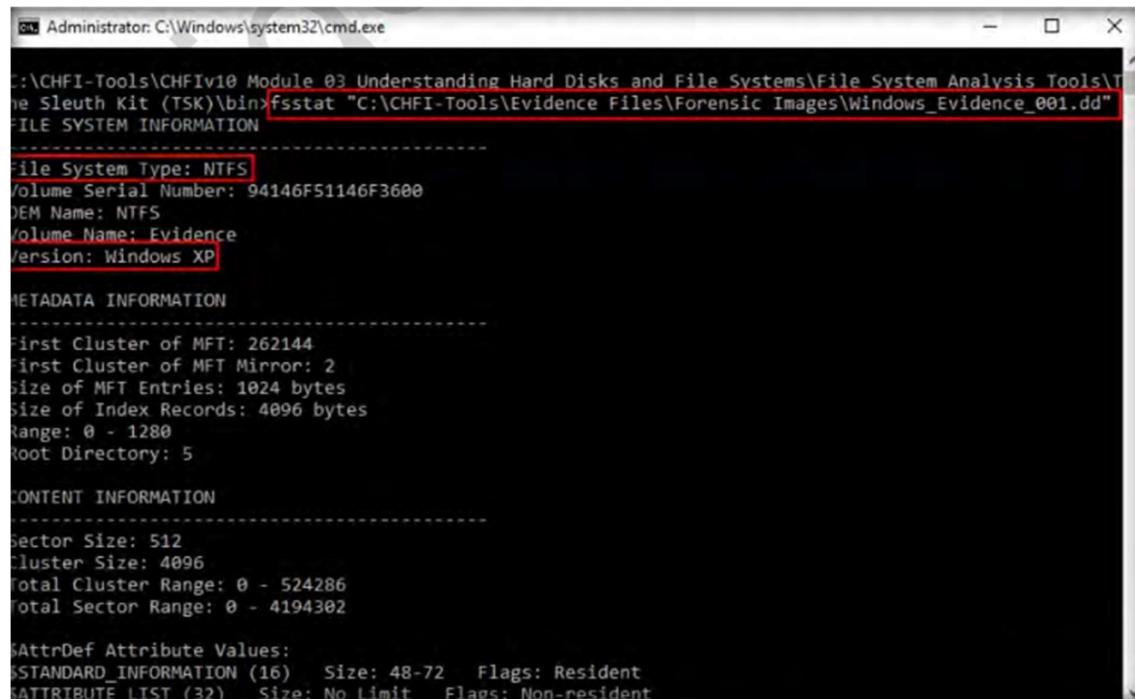


```
Administrator: C:\Windows\system32\cmd.exe
C:\CHFI-Tools\CHFIv10 Module 03 Understanding Hard Disks and File Systems\File System Analysis Tools\The Sleuth Kit (TSK)\bin>mmls "C:\CHFI-Tools\Evidence Files\Forensic Images\Windows_Evidence_002.dd"
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

Slot Start End Length Description
000: Meta 0000000000 0000000000 0000000001 Primary Table (#0)
001: ----- 0000000000 0000002047 0000002048 Unallocated
002: 000:000 0000002048 0001026047 0001024000 NTFS / exFAT (0x07)
003: 000:001 0001026048 0052426751 0051400704 NTFS / exFAT (0x07)
004: ----- 0052426752 0052428799 0000002048 Unallocated

C:\CHFI-Tools\CHFIv10 Module 03 Understanding Hard Disks and File Systems\File System Analysis Tools\The Sleuth Kit (TSK)\bin>
```

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.



```
Administrator: C:\Windows\system32\cmd.exe
C:\CHFI-Tools\CHFIv10 Module 03 Understanding Hard Disks and File Systems\File System Analysis Tools\The Sleuth Kit (TSK)\bin>fsstat "C:\CHFI-Tools\Evidence Files\Forensic Images\Windows_Evidence_001.dd"
FILE SYSTEM INFORMATION
-----
File System Type: NTFS
Volume Serial Number: 94146F51146F3600
DEM Name: NTFS
Volume Name: Evidence
Version: Windows XP

METADATA INFORMATION
-----
First Cluster of MFT: 262144
First Cluster of MFT Mirror: 2
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
Range: 0 - 1280
Root Directory: 5

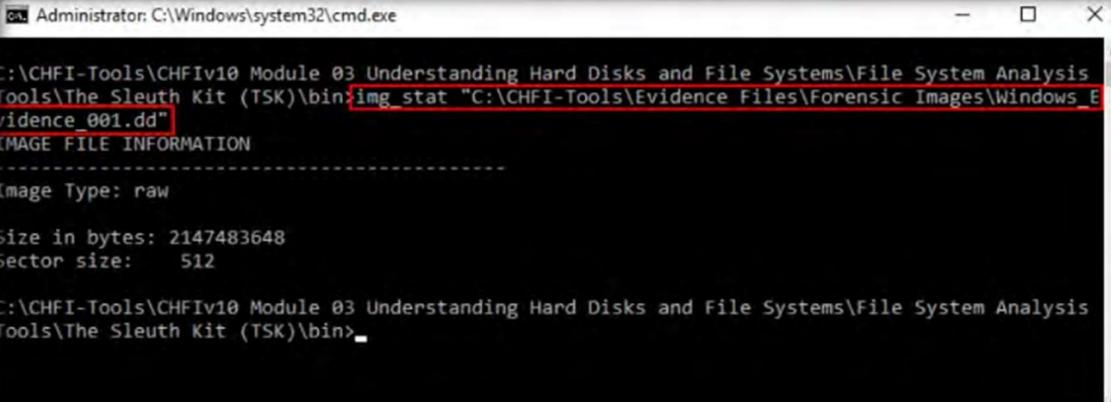
CONTENT INFORMATION
-----
Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 0 - 524286
Total Sector Range: 0 - 4194302

$AttrDef Attribute Values:
$STANDARD_INFORMATION (16)  Size: 48-72  Flags: Resident
$ATTRIBUTE_LIST (32)  Size: No Limit  Flags: Non-resident
```

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

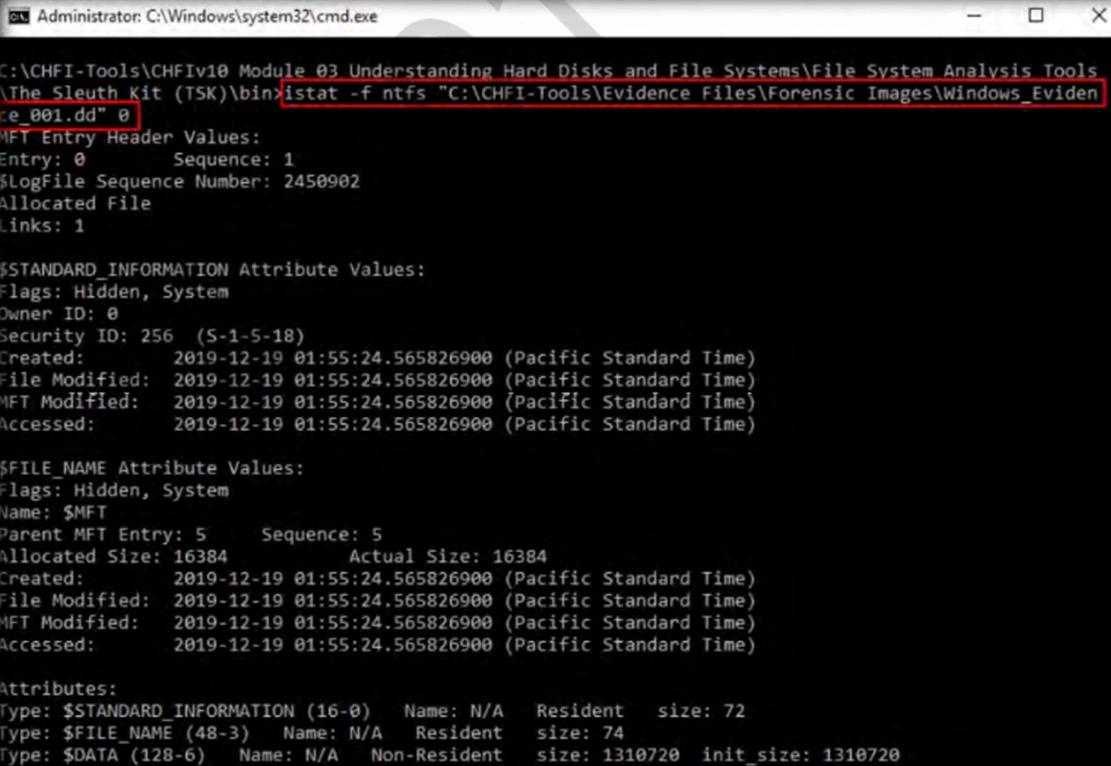
Use the img\_stat command to view the details of the selected image. Type img\_stat "C:\CHFI-Tools\Evidence Files\Forensic Images\Windows\_Evidence\_001.dd" and press Enter to view the details.



```
C:\>Administrator: C:\Windows\system32\cmd.exe
:::CHFI-Tools\CHFIV10 Module 03 Understanding Hard Disks and File Systems\File System Analysis Tools\The Sleuth Kit (TSK)\bin>img_stat "C:\CHFI-Tools\Evidence Files\Forensic Images\Windows_Evidence_001.dd"
IMAGE FILE INFORMATION
-----
Image Type: raw
size in bytes: 2147483648
Sector size: 512
:::CHFI-Tools\CHFIV10 Module 03 Understanding Hard Disks and File Systems\File System Analysis Tools\The Sleuth Kit (TSK)\bin>
```

## 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.



```
C:\>Administrator: C:\Windows\system32\cmd.exe
:::CHFI-Tools\CHFIV10 Module 03 Understanding Hard Disks and File Systems\File System Analysis Tools\The Sleuth Kit (TSK)\bin>istat -f ntfs "C:\CHFI-Tools\Evidence Files\Forensic Images\Windows_Evidence_001.dd" 0
MFT Entry Header Values:
Entry: 0 Sequence: 1
LogFile Sequence Number: 2450902
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 256 (S-1-5-18)
Created: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
File Modified: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
MFT Modified: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
Accessed: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)

$FILE_NAME Attribute Values:
Flags: Hidden, System
Name: $MFT
Parent MFT Entry: 5 Sequence: 5
Allocated Size: 16384 Actual Size: 16384
Created: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
File Modified: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
MFT Modified: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
Accessed: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)

Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
Type: $FILE_NAME (48-3) Name: N/A Resident size: 74
Type: $DATA (128-6) Name: N/A Non-Resident size: 1310720 init_size: 1310720
262144 262145 262146 262147 262148 262149 262150 262151
```

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.

```

Administrator: C:\Windows\system32\cmd.exe

C:\CHFI-Tools\CHFIv10 Module 03 Understanding Hard Disks and File Systems\File System Analysis Tools\The Sleuth Kit (TSK)\bin>istat -f ntfs "C:\CHFI-Tools\Evidence Files\Forensic Images\Windows_Evidence_001.dd" 1

MFT Entry Header Values:
Entry: 1 Sequence: 1
$LogFile Sequence Number: 2118363
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 256 (S-1-5-18)
Created: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
File Modified: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
MFT Modified: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
Accessed: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)

$FILE_NAME Attribute Values:
Flags: Hidden, System
Name: $MFTMirr
Parent MFT Entry: 5 Sequence: 5
Allocated Size: 4096 Actual Size: 4096
Created: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
File Modified: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
MFT Modified: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
Accessed: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)

Attributes:

```

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-resident attribute 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\Evidence Files\Forensic Images\Windows\_Evidence\_001.dd" and then press Enter.

```

Administrator: C:\Windows\system32\cmd.exe

C:\CHFI-Tools\CHFIv10 Module 03 Understanding Hard Disks and File Systems\File System Analysis Tools\The Sleuth Kit (TSK)\bin>fls -f ntfs "C:\CHFI-Tools\Evidence Files\Forensic Images\Windows_Evidence_001.dd"
r/r 4-128-1: $AttrDef
r/r 8-128-2: $Badclus
r/r 8-128-1: $BadClus:$Bad
r/r 6-128-1: $Bitmap
r/r 7-128-1: $Boot
d/d 11-144-4: $Extend
r/r 2-128-1: $LogFile
r/r 0-128-6: $MFT
r/r 1-128-1: $MFTMirr
d/d 1228-144-1: $RECYCLE.BIN
r/r 9-128-8: $Secure:$SDS
r/r 9-144-11: $Secure:$SDH
r/r 9-144-14: $Secure:$SII
r/r 10-128-1: $UpCase
r/r 10-128-4: $UpCase:$Info
r/r 3-128-3: $Volume
d/d 39-144-5: Audio Files
d/d 48-144-5: images
d/d 85-144-5: Other Files
d/d 1169-144-1: Outlook Files
d/d 1180-144-5: Songs
d/d 36-144-1: System Volume Information

```

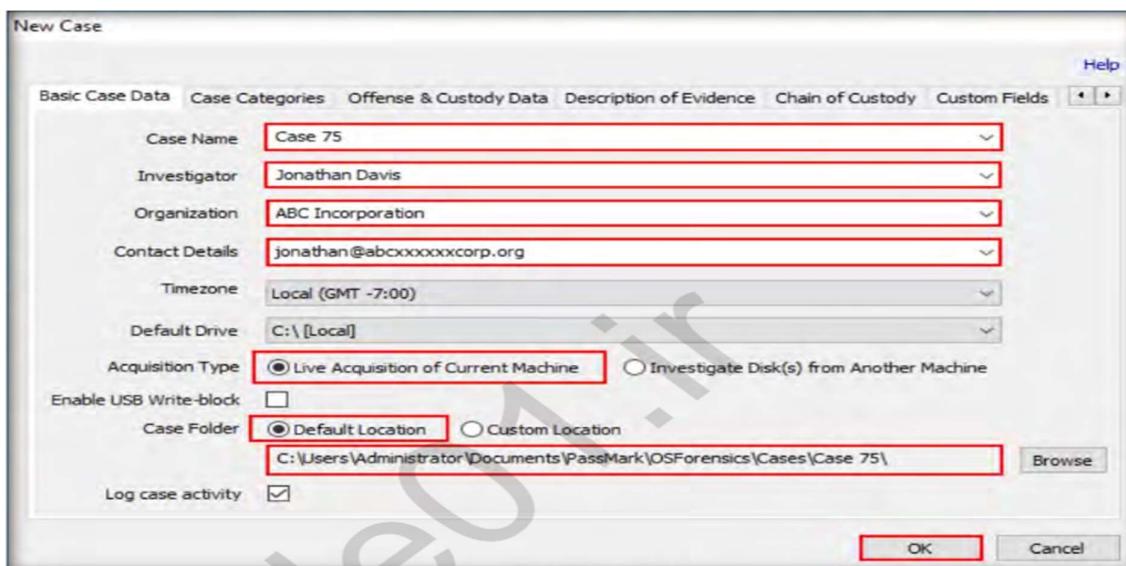
## PRACTICAL NO. 02

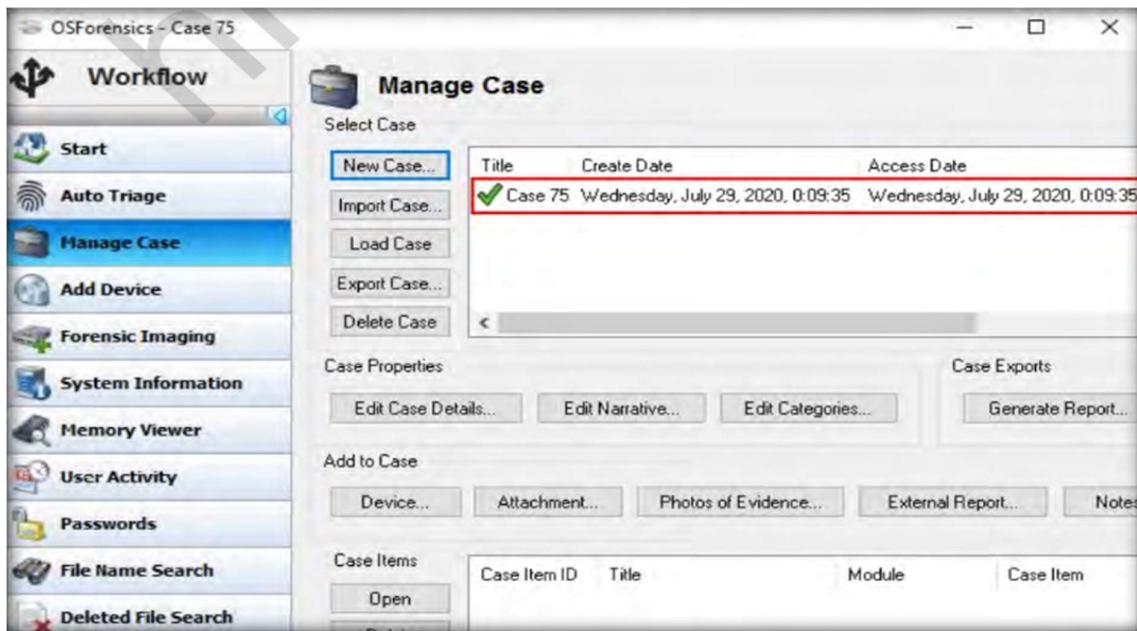
### a. Explore Windows forensic tools (OSForensics)

Navigate to C:\CHFI-Tools\CHFIv10Module 06 Windows Forensics\Windows Forensics Tools\OS Forensics, double-click osf.exe to launch the step. In the final step of installation, check the Launch OSForensics option and click Finish. OSForensics GUI appears, along with PassMark OSForensics 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.

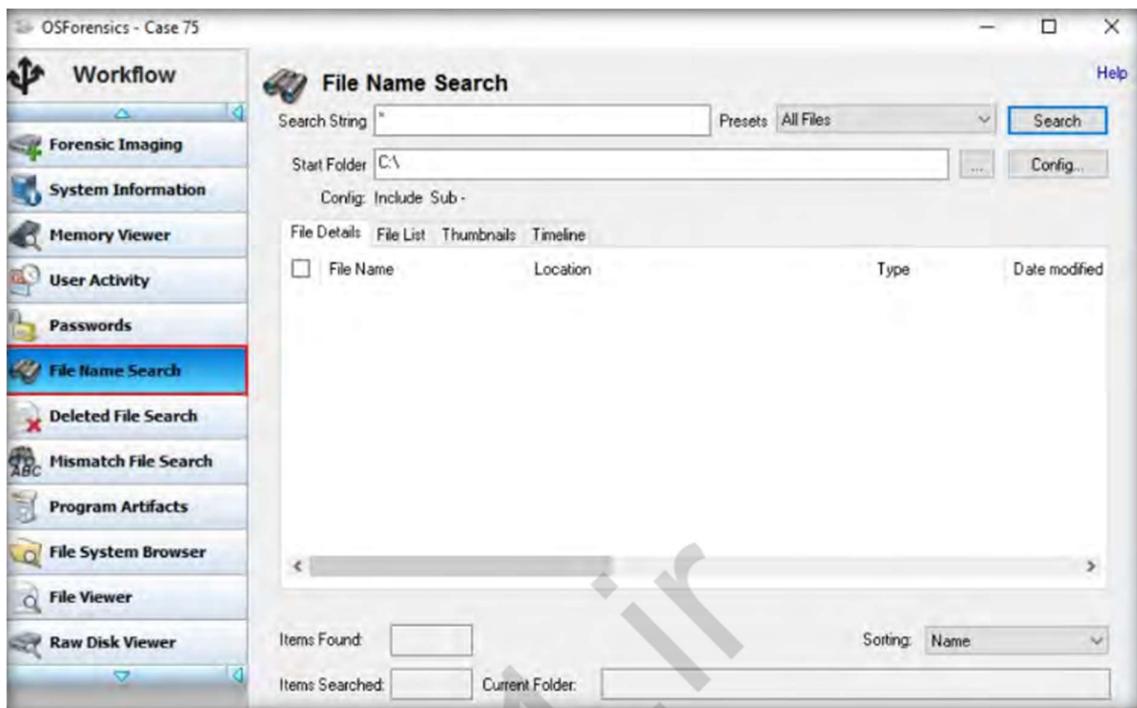


A New Case window appears; fill out the required fields in the window. Ensure that you select the radio button for the Live Acquisition of Current Machine option in the Acquisition Type category. You may choose to save the new case folder either in Default or Custom locations. Click OK.

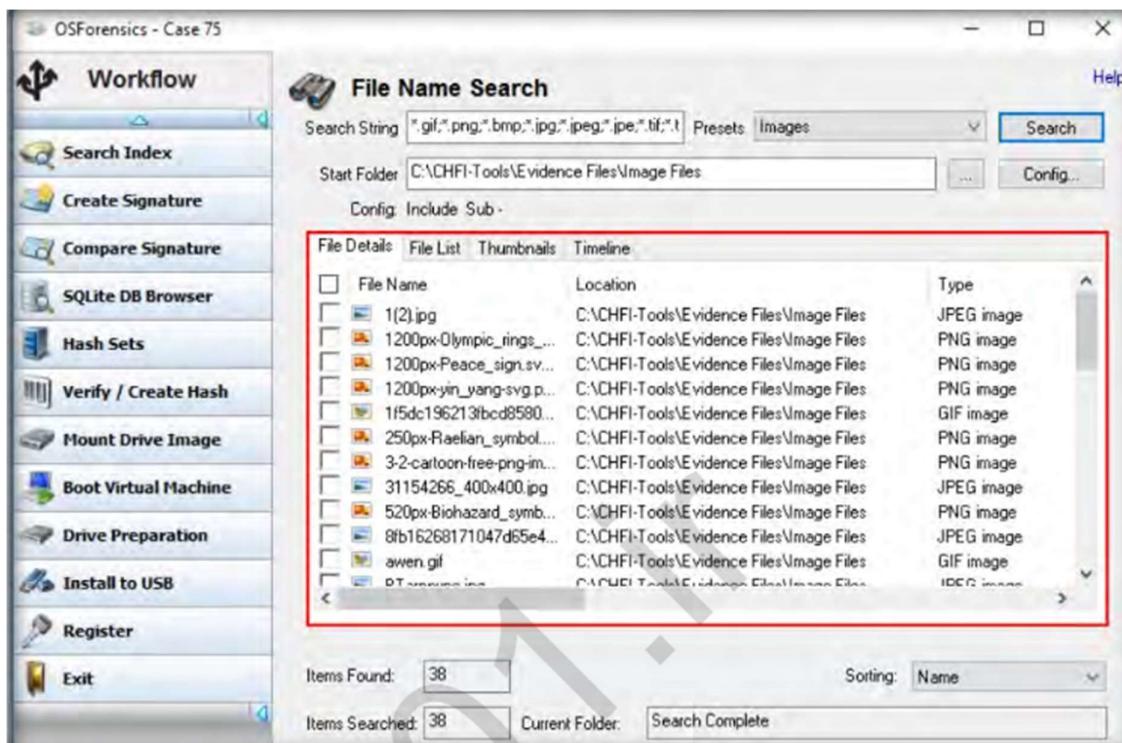
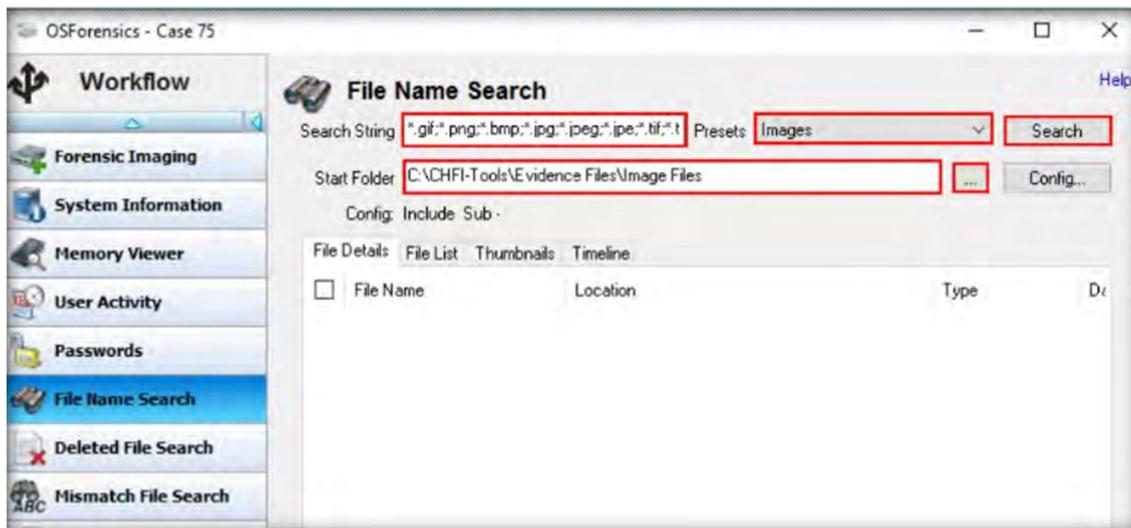




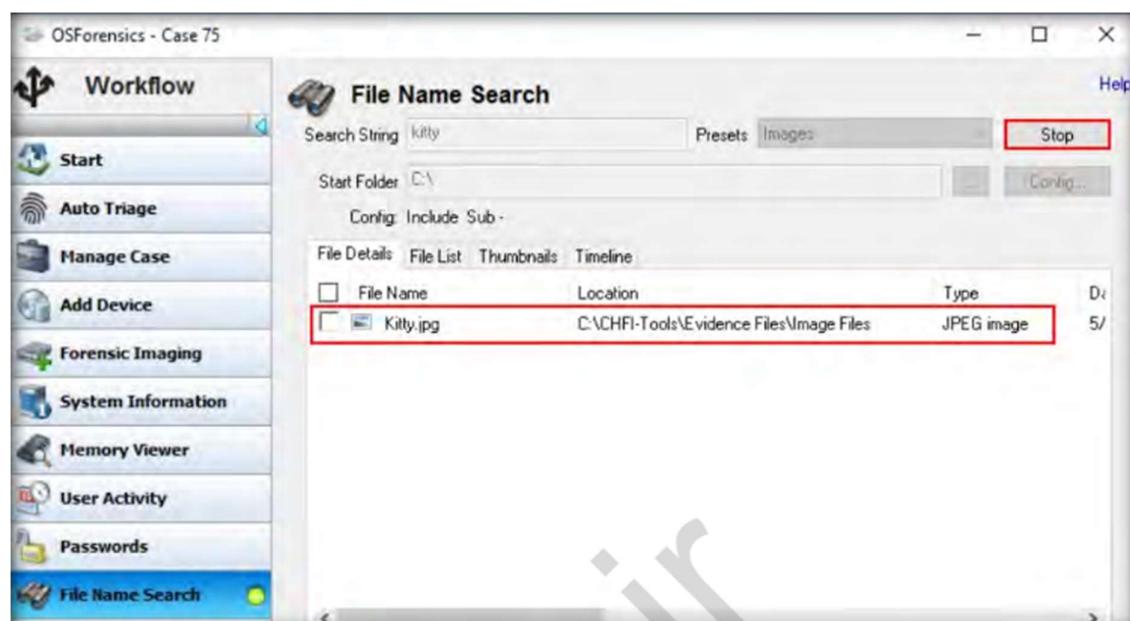
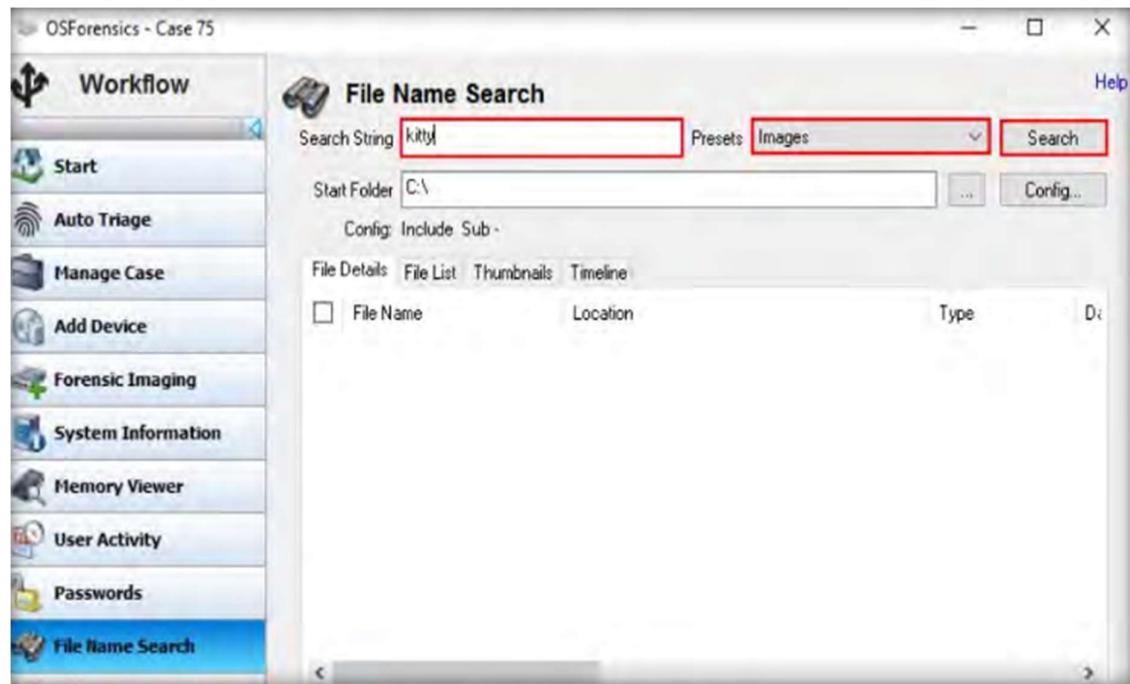
The OSForensics tool can help investigators in searching and locating files on a system. To start searching for files, click File Name Search in the left pane of the window.



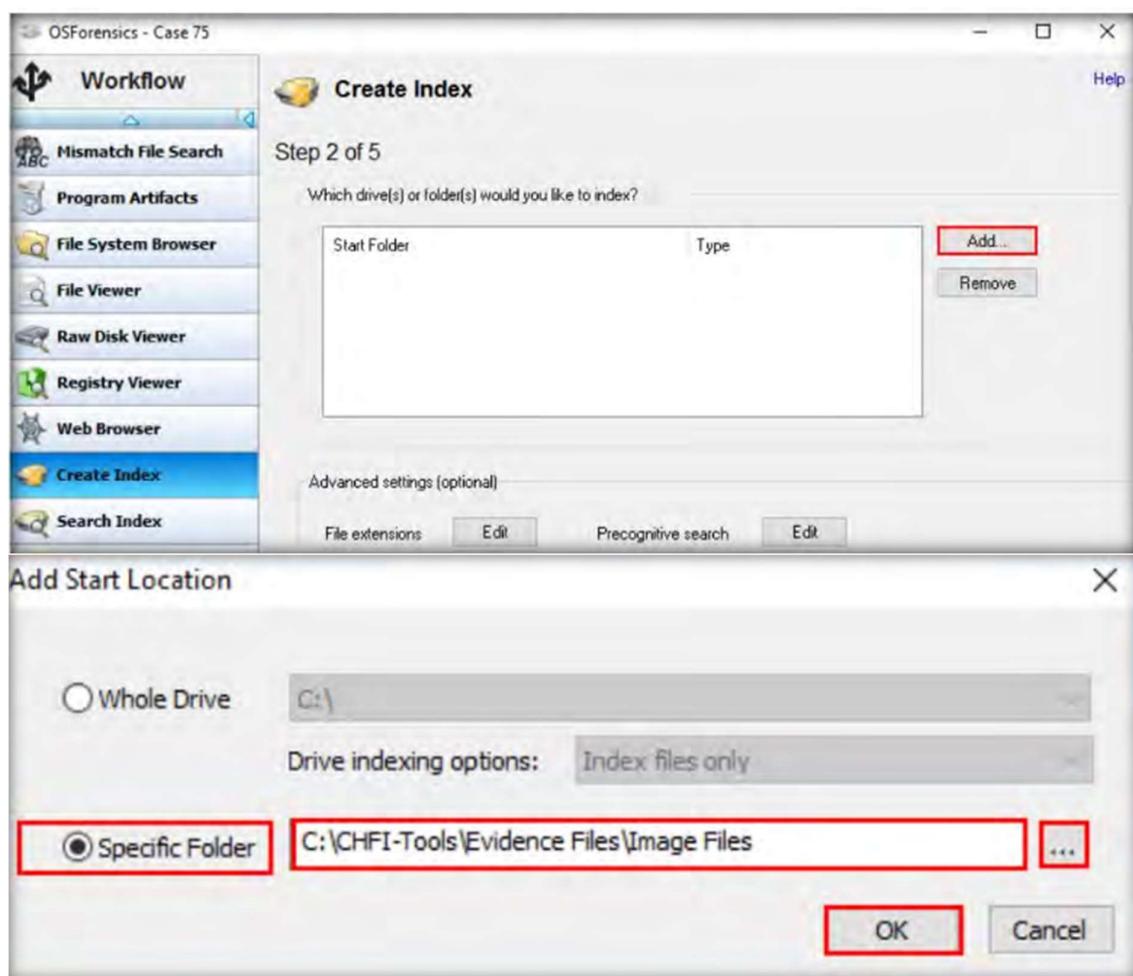
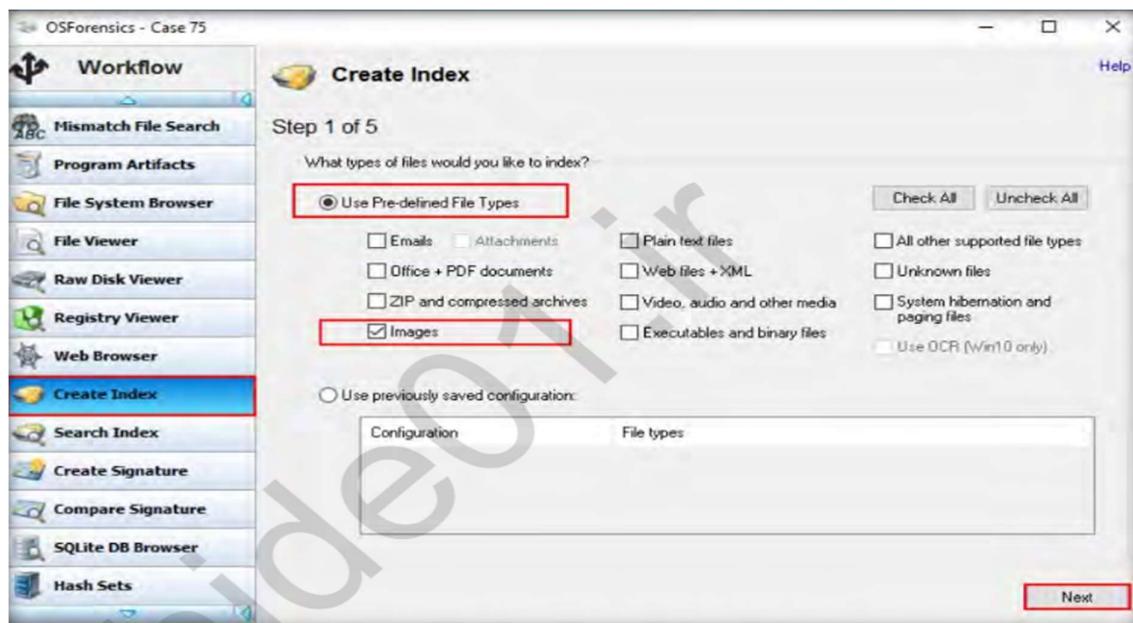
In the Start Folder field, specify the path to search for image files by clicking the ellipsis button and choosing the location (here, we are specifying the location C:\CHFI-Tools\EvidenceFiles\Image Files to search for images in it). Then, click the Search button.

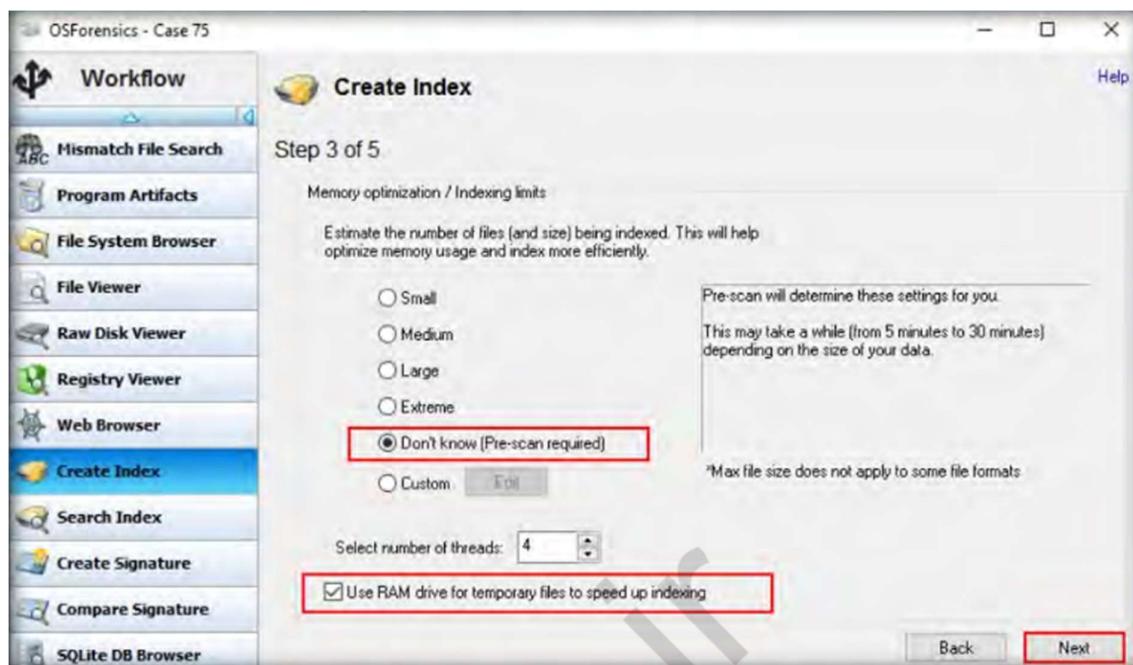
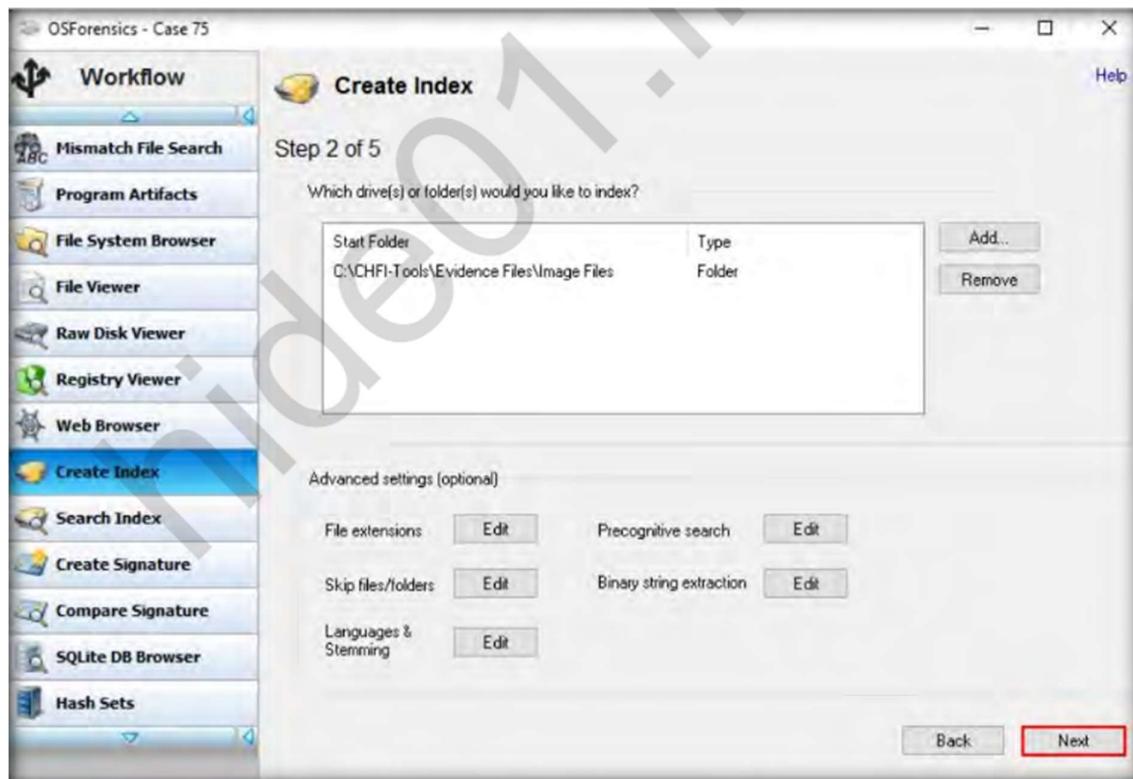


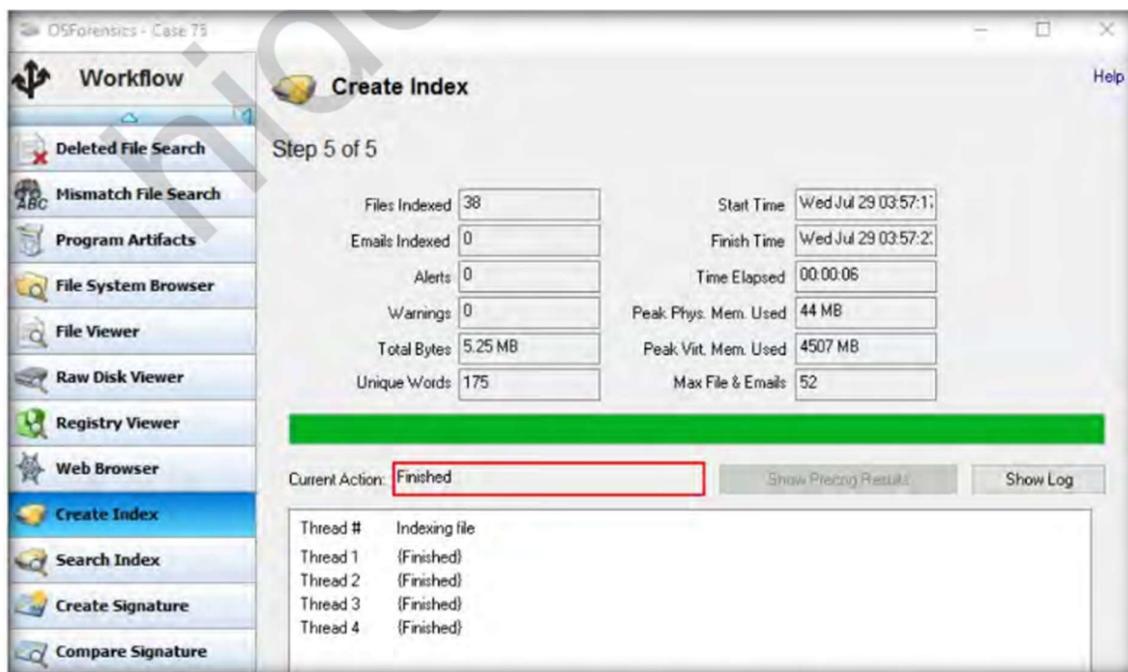
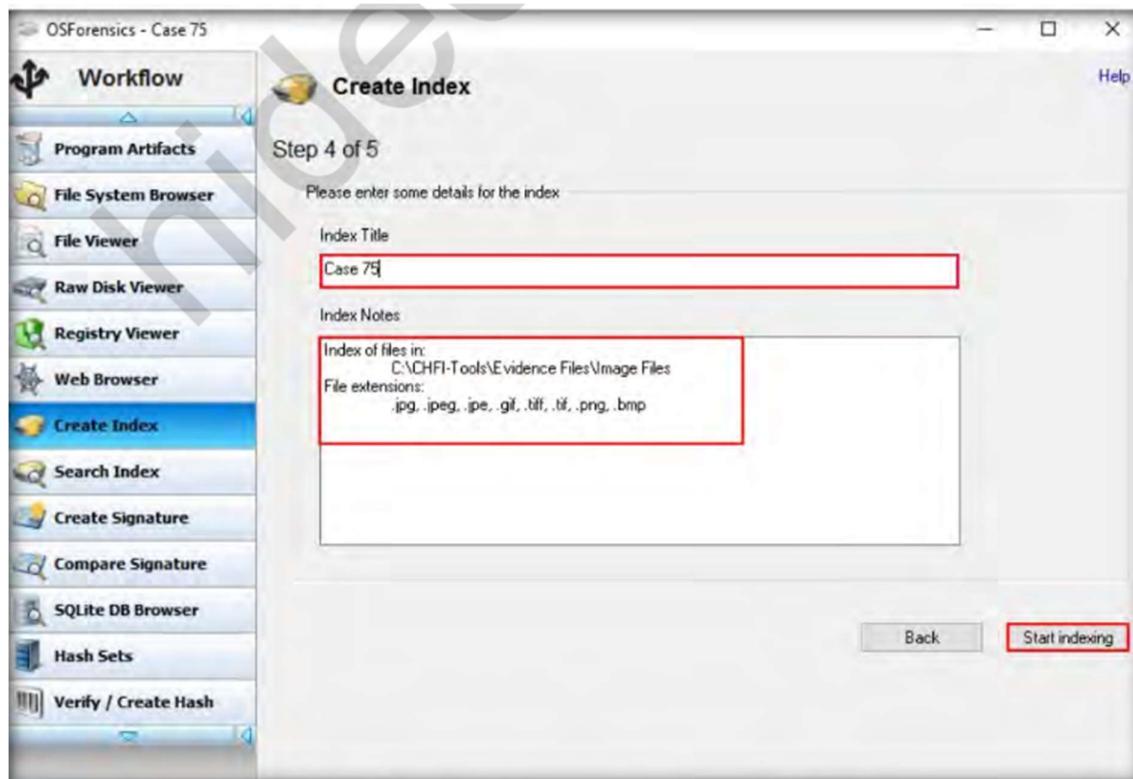
Alternatively, if you wish to search only for a single image on the entire system, select Images from the Pre-sets drop-down menu, enter the name of the desired image file in the Search String field, and then click Search, as shown in the screenshot below. Here, we are searching for the JPEG image file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



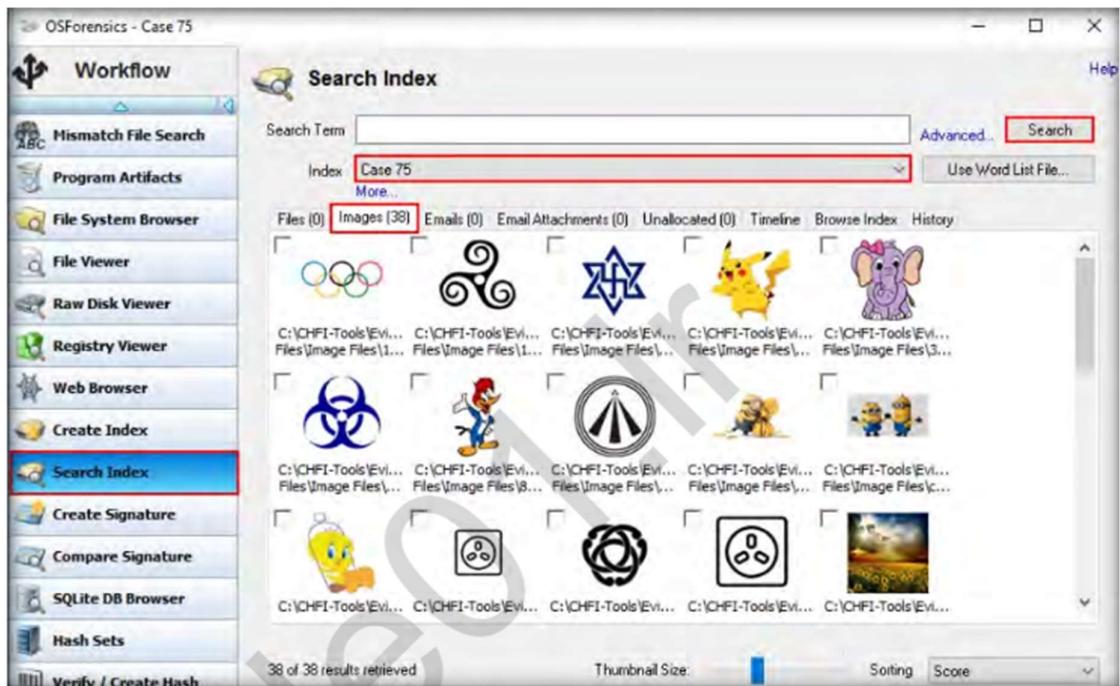
The Create Index section appears in the right pane. In this section, select the Use Pre-defined File Types option for creating the index and check the required options listed under it for selecting the file types that you wish to index (here, we have selected the Images option). Then, click Next.



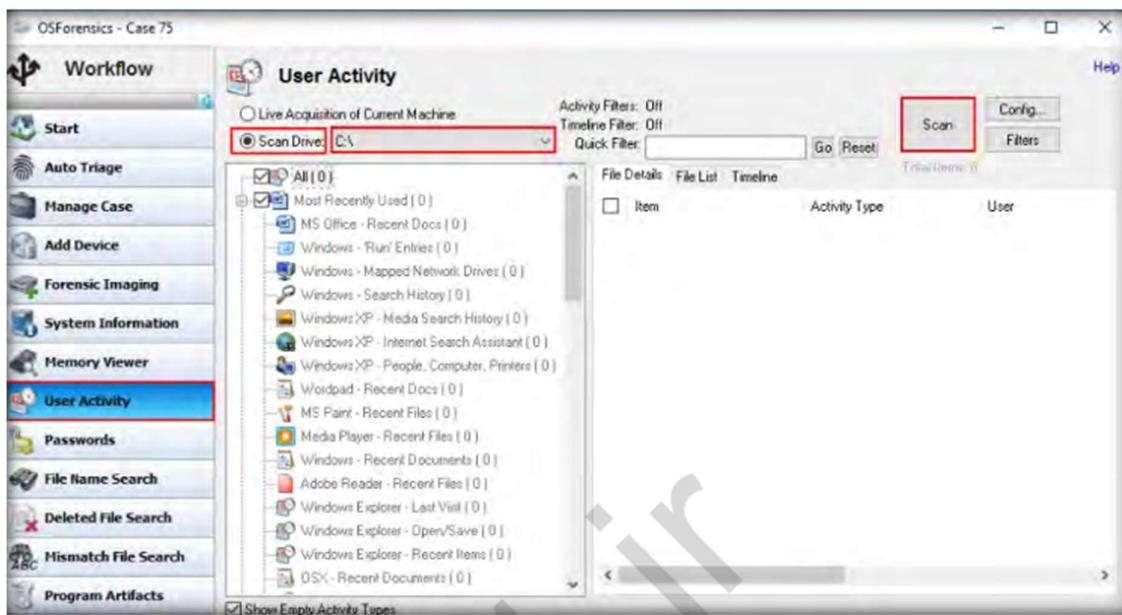


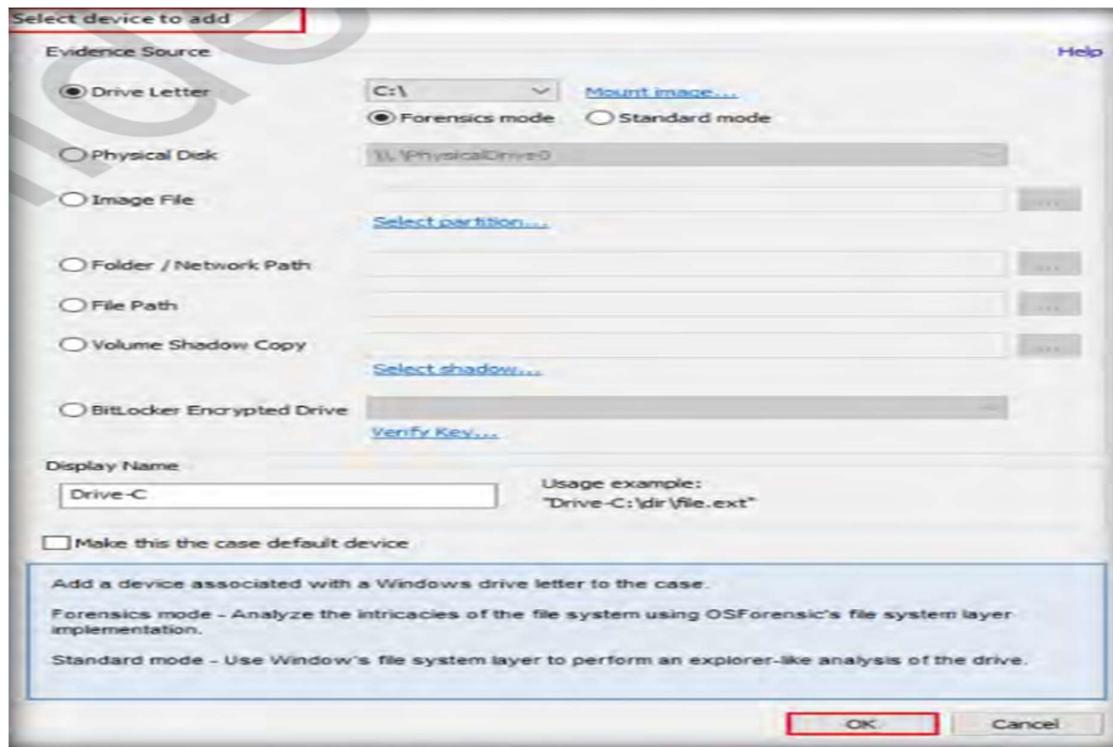


We will now search the indexed files. To search for the indexed files, select Search Index from the left pane of the tool window. The Search Index section now appears in the tool window. The index at the top displays the name of the case we created (i.e., Case 75). Click Search. The tool will load the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

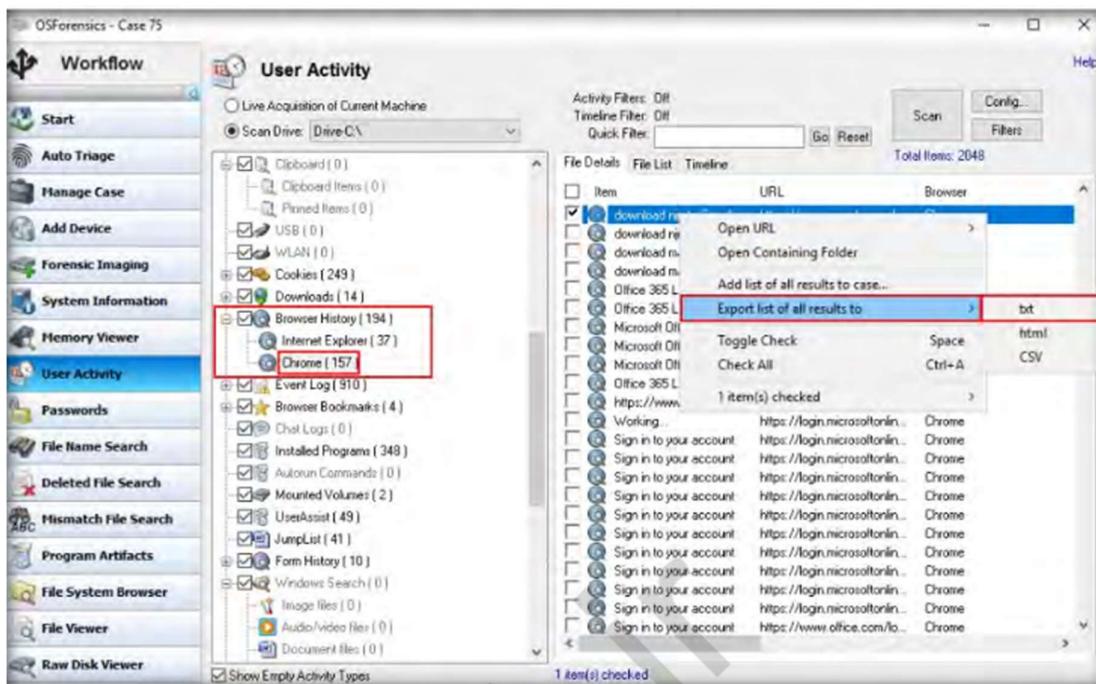


Click User Activity in the left pane to scan for evidence such as browsed websites, USB drives, recent downloads and wireless networks.

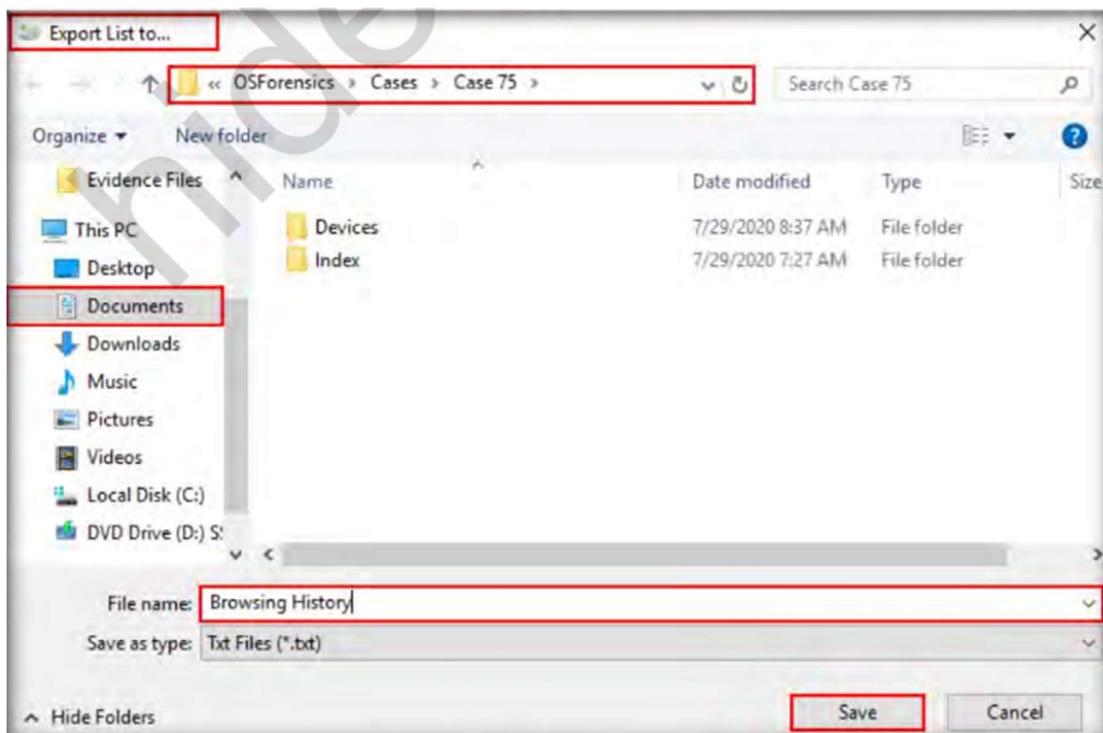




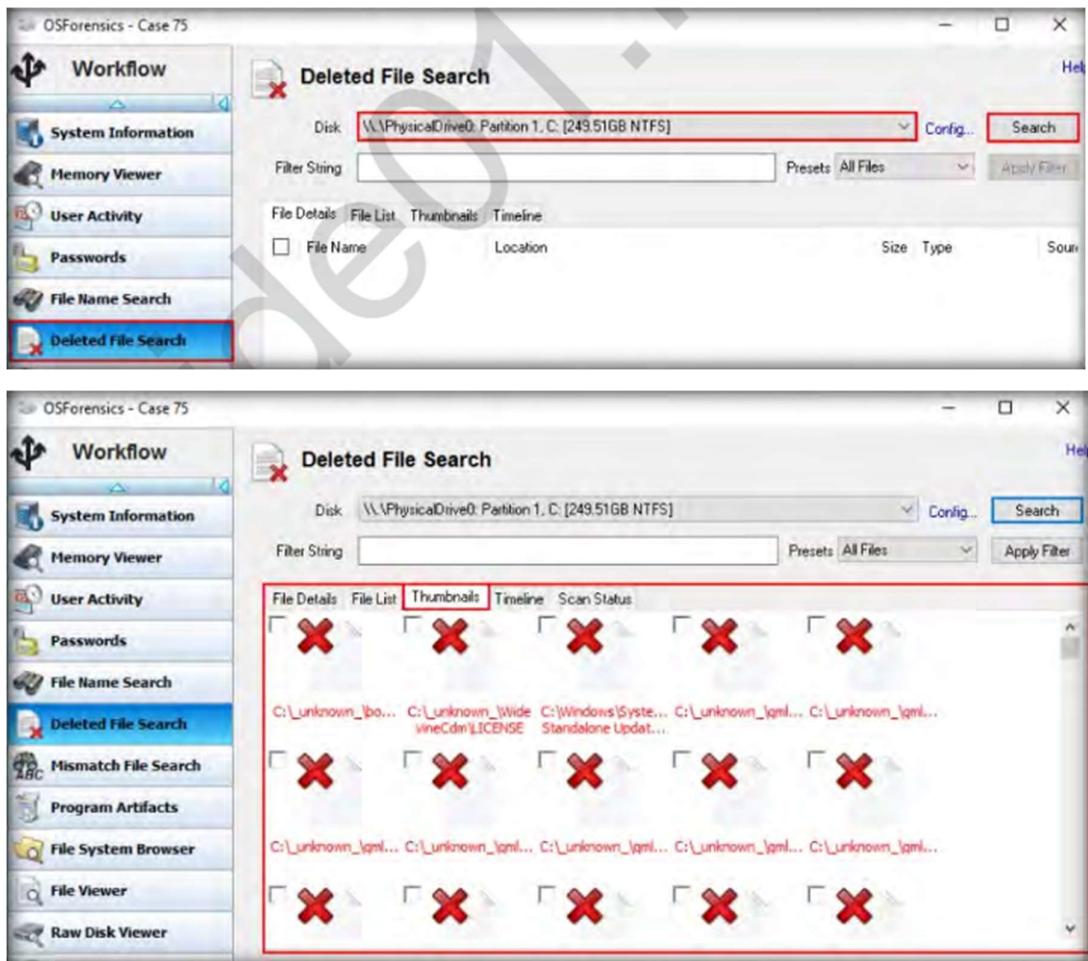
If you wish to save any of the above user-activity information on your system, such as Browser History, then scroll down the items list in the left pane below the Scan Drive option and expand the Browser History node. Select the browser for which you wish to retrieve the history (Here, we are selecting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



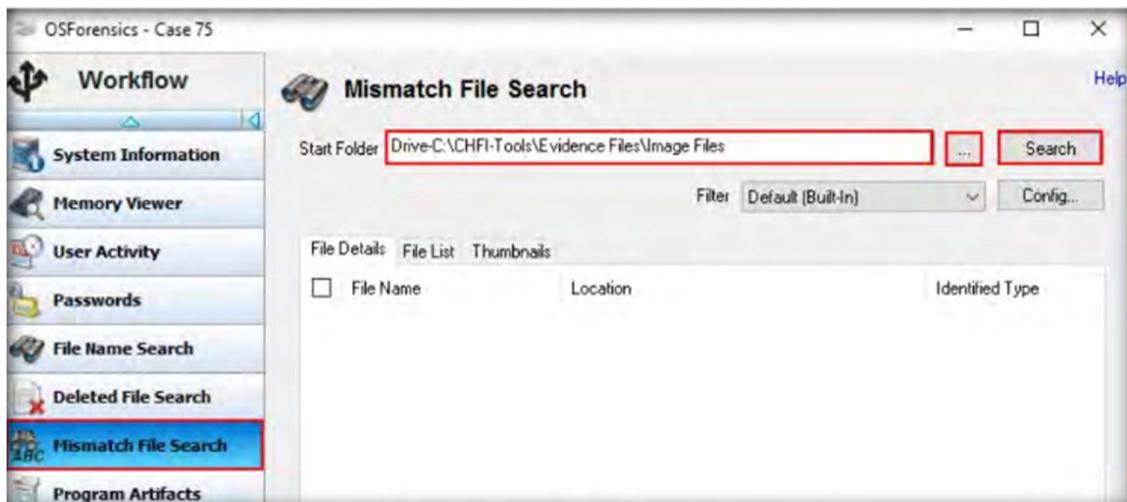
An Export List to... window will appear. Navigate to C:\Users\Administrator\Documents\PassMark\OSForensics\Cases\Case 75, name the file (here, we are naming it as Browsing History), and click Save to export the browsing history.

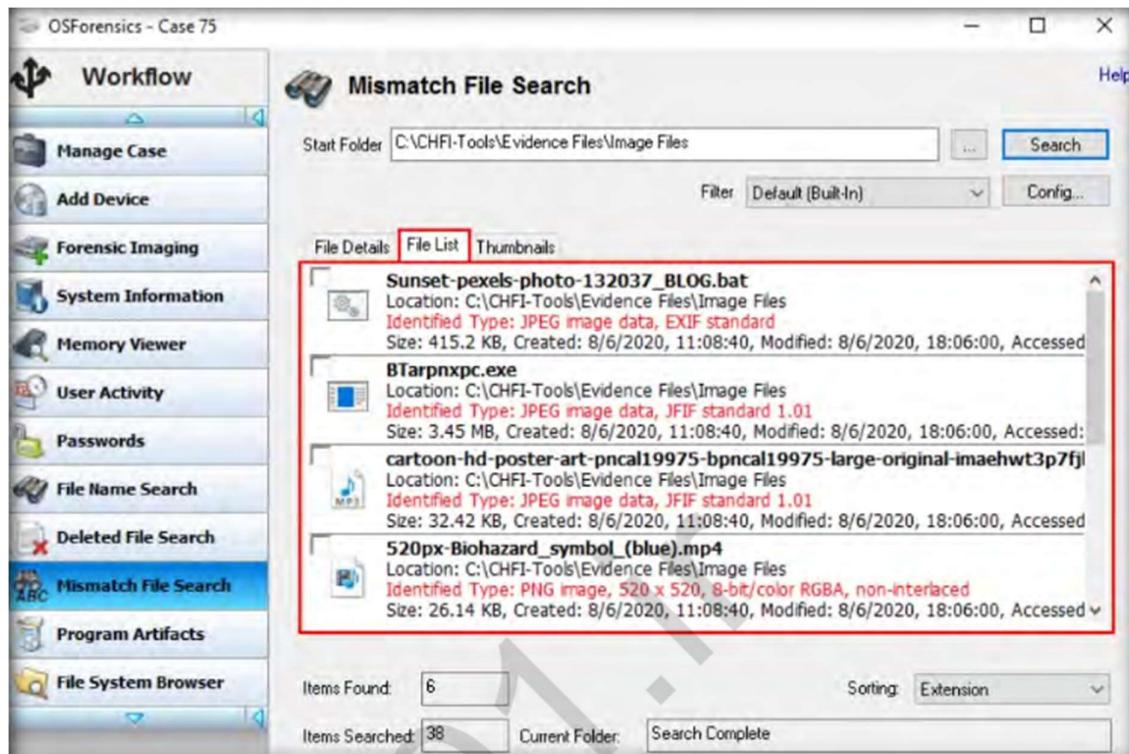


To recover deleted files from the file system, click Deleted File Search in the left pane, select a disk on which you wish to perform the deleted file search from the Disk drop-down menu, and click the search button.

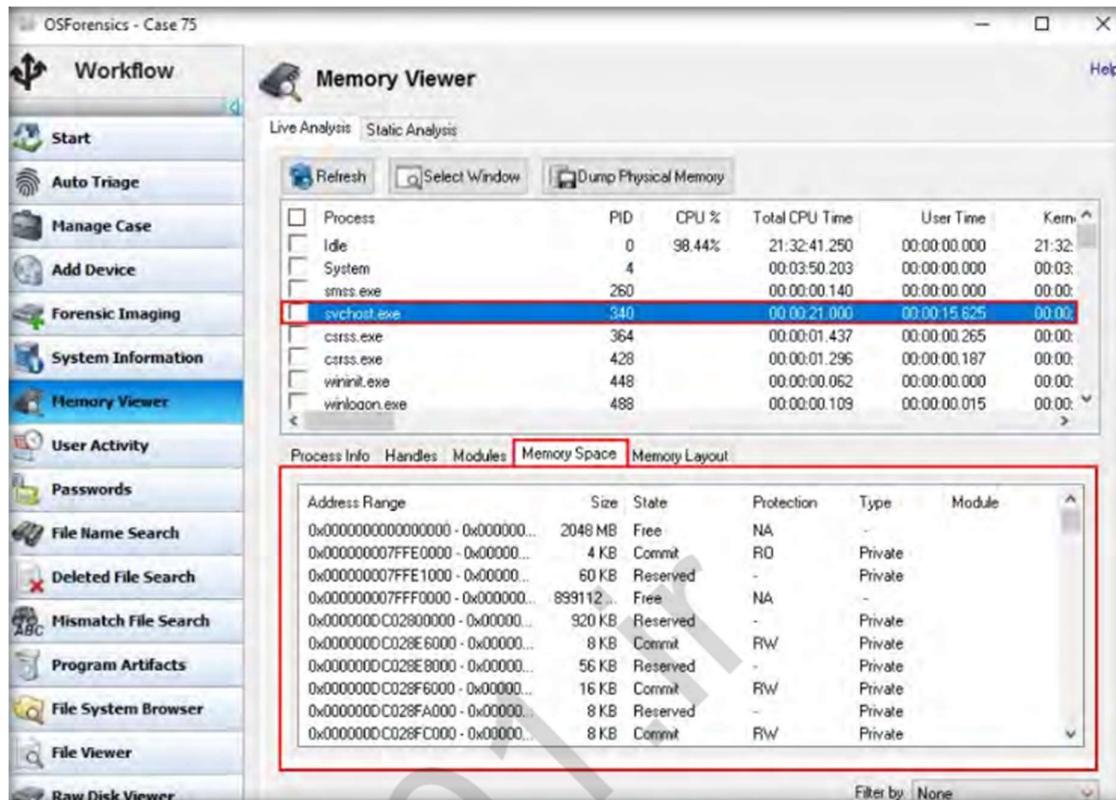


To locate files having contents that do not match the file extensions, click Mismatch File Search in the left pane of the tool window. The tool will display the Mismatch File Search section in the right pane, as shown in the screenshot:





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.

The screenshot shows the OSForensics software interface. On the left is a vertical toolbar with icons for Workflow, Start, Auto Triage, Manage Case, Add Device, Forensic Imaging, System Information (which is highlighted with a red box), Memory Viewer, User Activity, and Passwords. The main window title is "OSForensics - Case 75". The central area has a header "System Information" with a red box around it. Below the header are buttons for "List: Basic System Information", "Edit...", "Go", and a "Find Text:" search bar. There are two radio button options: "Live Acquisition of Current Machine" (selected) and "Scan Drive: D:\\". A table titled "Commands" lists various system information items with their corresponding commands, internal status, architecture, live acquisition status, and disk status. The table includes rows for Computer Name, Operating system, CPU Info, Mem Info, Graphics Info, USB Info, Disk volume Info, Disk drive Info, Optical drive Info, Network Info, and Route Info.

Name	Command	Internal	Architecture	Live Acquisi...	D
Computer Name	SysInfoDII_GetComputerName	Yes	32/64	Yes	N
Operating system	SysInfoDII_GetOS	Yes	32/64	Yes	N
CPU Info	SysInfoDII_GetCPUInfo	Yes	32/64	Yes	N
Mem Info	SysInfoDII_GetMemoryInfo	Yes	32/64	Yes	N
Graphics Info	SysInfoDII_GetGraphicsInfo	Yes	32/64	Yes	N
USB Info	SysInfoDII_GetUSBInfo	Yes	32/64	Yes	N
Disk volume Info	SysInfoDII_GetSystemInfo_SM...	Yes	32/64	Yes	N
Disk drive Info	SysInfoDII_GetSystemInfo_SM...	Yes	32/64	Yes	N
Optical drive Info	SysInfoDII_GetSystemInfo_SM...	Yes	32/64	Yes	N
Network Info	SysInfoDII_GetSystemInfo_SM...	Yes	32/64	Yes	N
Route Info	SysInfoDII_GetSystemInfo_SM...	Yes	32/64	Yes	N

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.

## **PRACTICAL NO. 03**

### **Using Forensic Toolkit (FTK) & Writing report using FTK (AccessData FTK)**

**Aim:** Using Windows Forensics Tools.

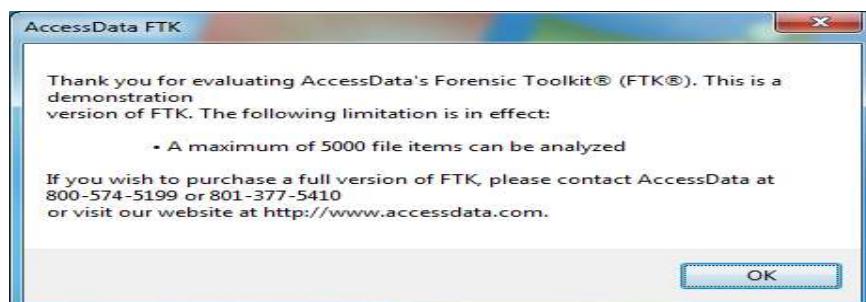
Step 1: Start Forensic Toolkit.



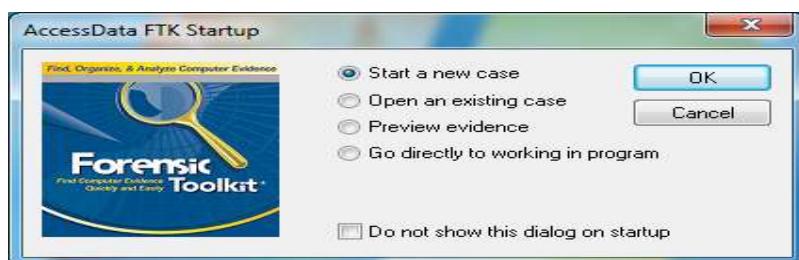
Step 2: Here, prompted with a warning dialog box, click on OK to continue.



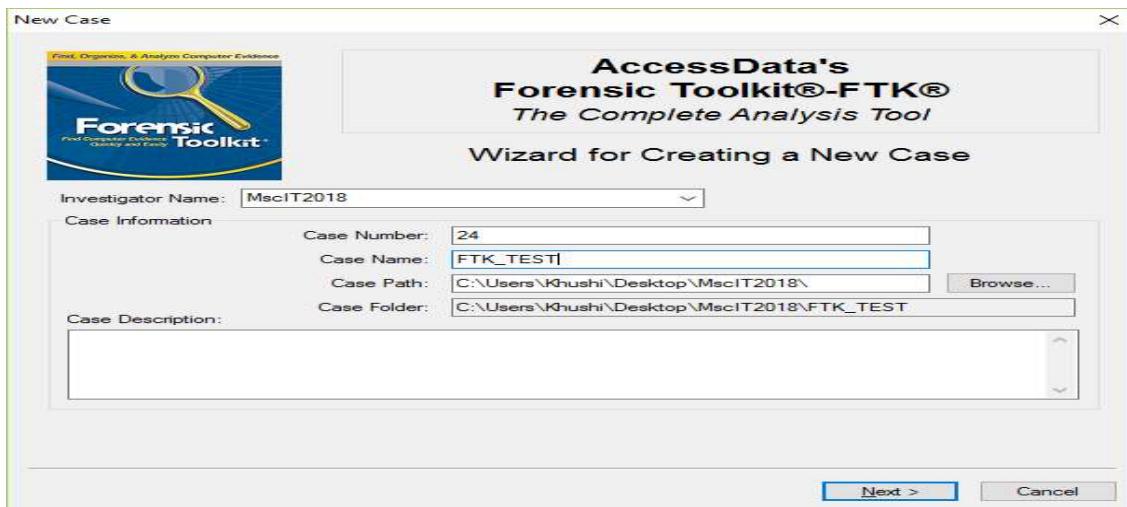
Step 3: click on OK button.



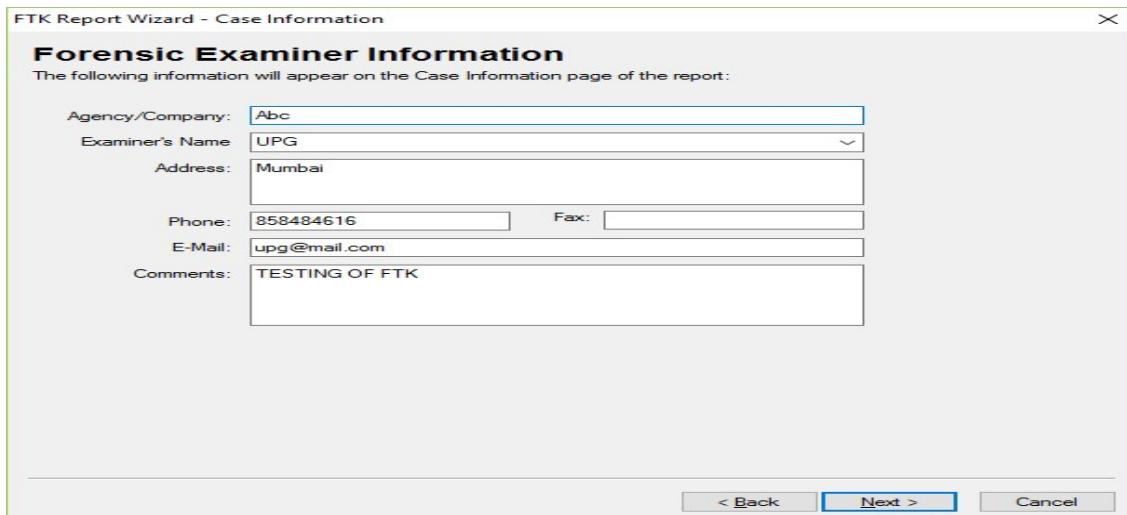
Step 4: Now select Start New Case option and click on ok.



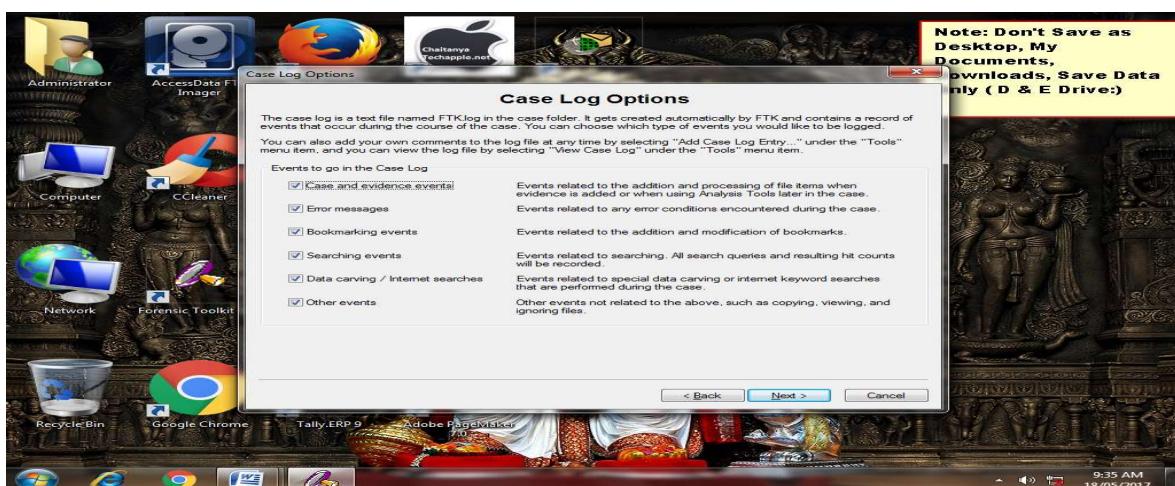
Step 5: Enter the detail for a New case.



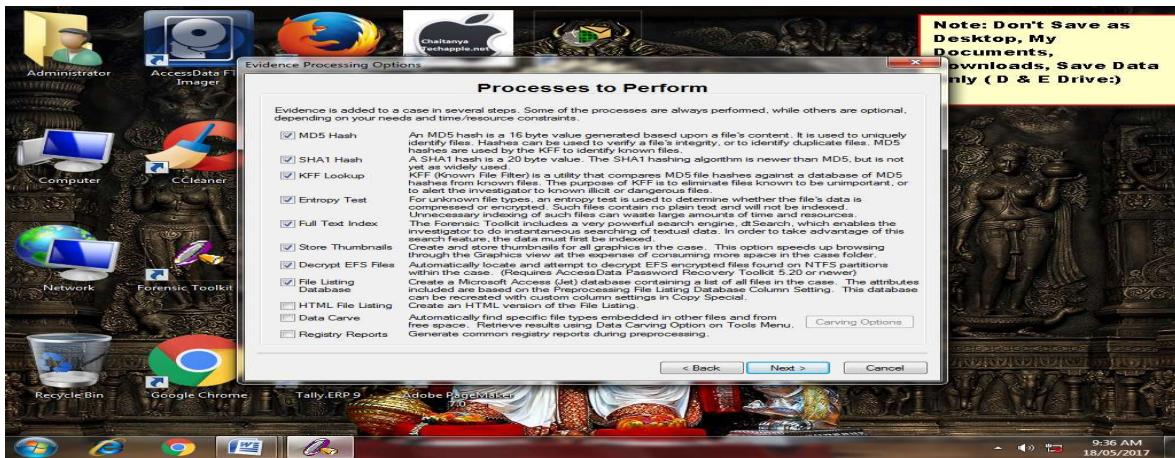
Step 6: Fill the information in Forensic Examiner Information dialog box.



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



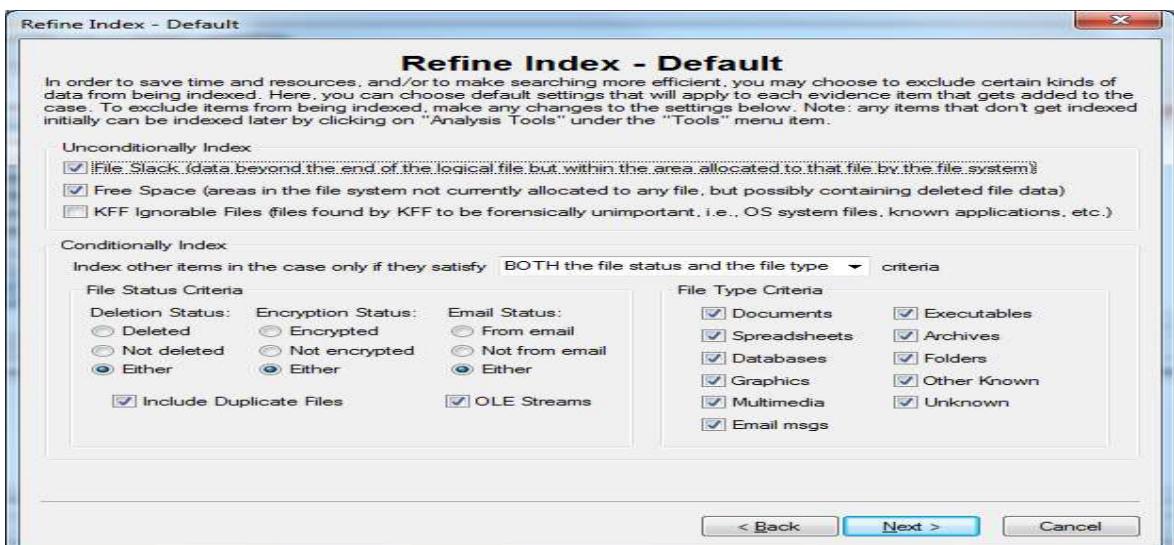
Step 8: Now again leave the default settings and click on next.



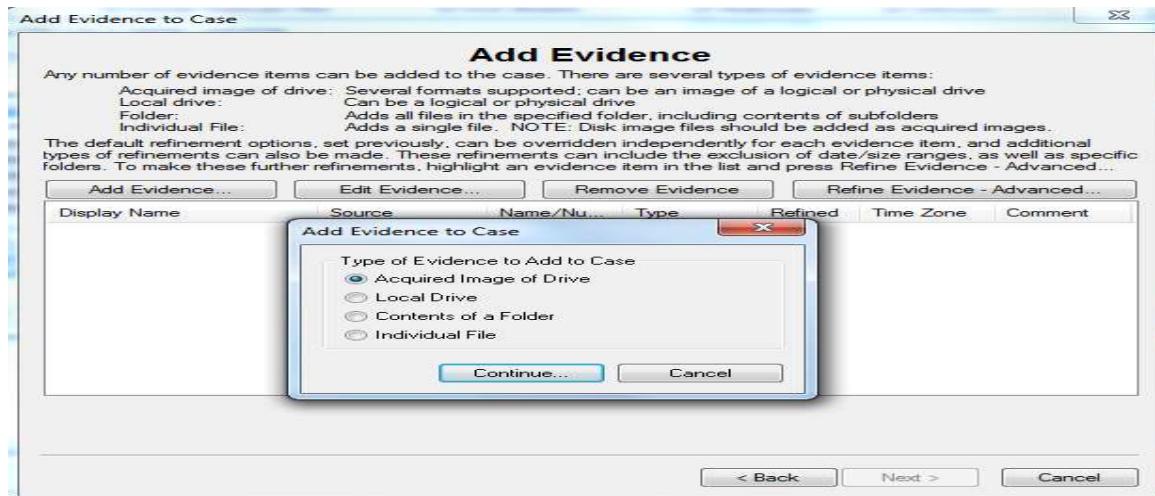
Step 9: In the Refine Case-Default, click the Include All items button and then click Next.



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



Step 11: Now here Click on add Evidence button.



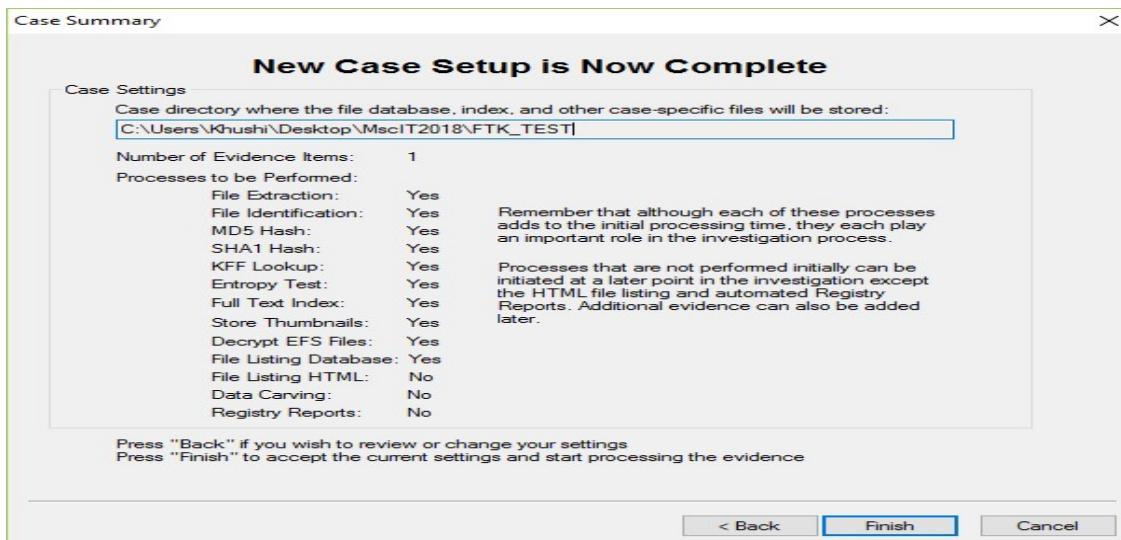
Step 12: Enter Evidence Information and click on OK button.

Evidence Information	
Evidence Location: C:\Users\Khushi\Desktop\MscIT2018\FTKTEST.E01	
Evidence Display Name: FTKTEST	
Evidence Identification Name/Number: 24	
Comment: Evidence Information	
Local Evidence Time Zone: Choose time zone for evidence ...	
<input type="button" value="OK"/>	<input type="button" value="Cancel"/>

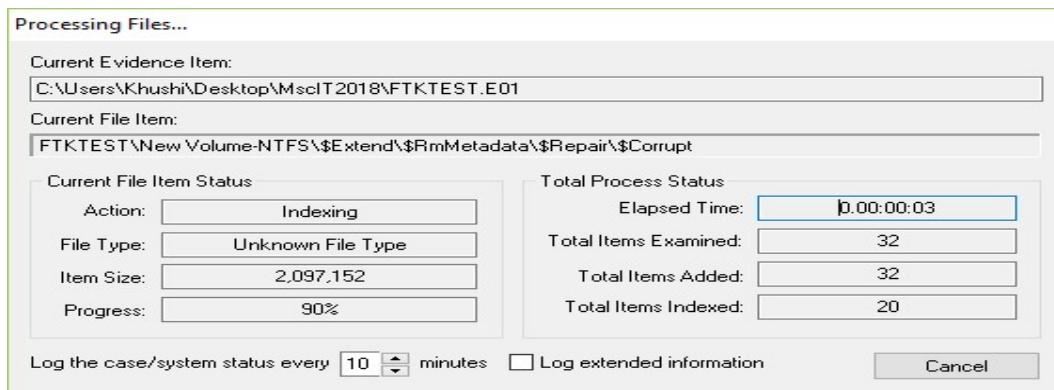
Step 13: Now click on Next.

Add Evidence to Case							
<b>Add Evidence</b>							
Any number of evidence items can be added to the case. There are several types of evidence items:							
Acquired image of drive: Several formats supported; can be an image of a logical or physical drive Local drive: Can be a logical or physical drive Folder: Adds all files in the specified folder, including contents of subfolders Individual File: Adds a single file. NOTE: Disk image files should be added as acquired images.							
The default refinement options, set previously, can be overridden independently for each evidence item, and additional types of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specific folders. To make these further refinements, highlight an evidence item in the list and press Refine Evidence - Advanced...							
<input type="button" value="Add Evidence..."/>		<input type="button" value="Edit Evidence..."/>		<input type="button" value="Remove Evidence"/>		<input type="button" value="Refine Evidence - Advanced..."/>	
Display Name	Source	Name/Nu...	Type	Refined	Time Zone	Comment	
FTKTEST\New Volume-N...	C:\Users\Khu...	24	NTFS	N	N/A	Evidence I...	
< Back <input type="button" value="Next &gt;"/> Cancel							

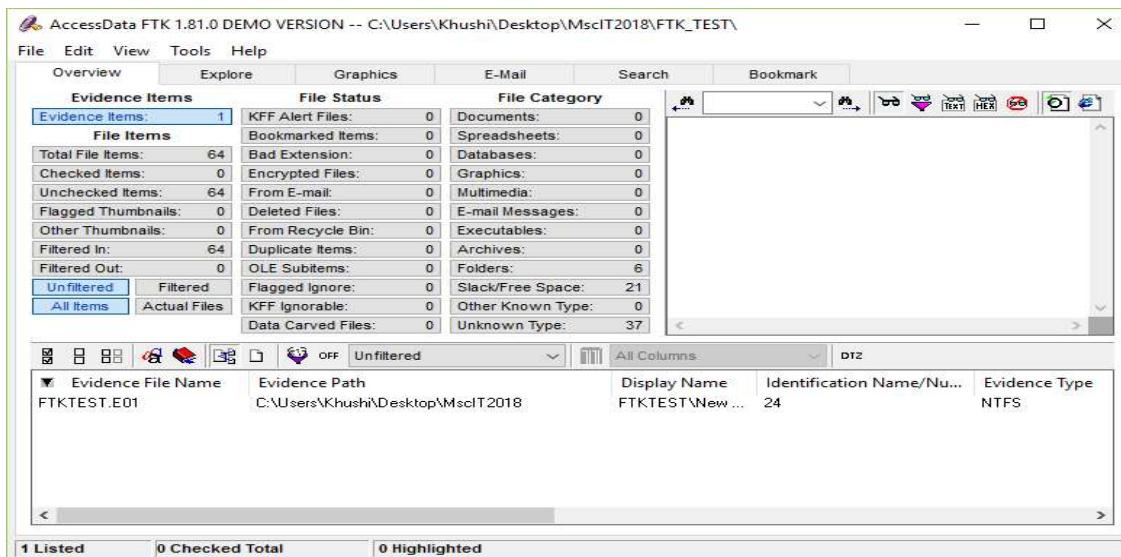
Step 14: Click on Finish to initiate the analysis.



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.

The screenshot shows the FTK Imager interface. The 'Evidence Items' pane on the left indicates there are 507 total file items, 507 checked items, and 7 deleted files. The 'File Status' and 'File Category' panes show various statistics. The main pane displays a list of deleted files, including 'l.out', 'lgf.jpg', and several image files from a young boy proposed to a girl. The toolbar at the top includes icons for Overview, Explore, Graphics, E-Mail, Search, and Bookmark.

Step 18: Select Encrypted Files to view.

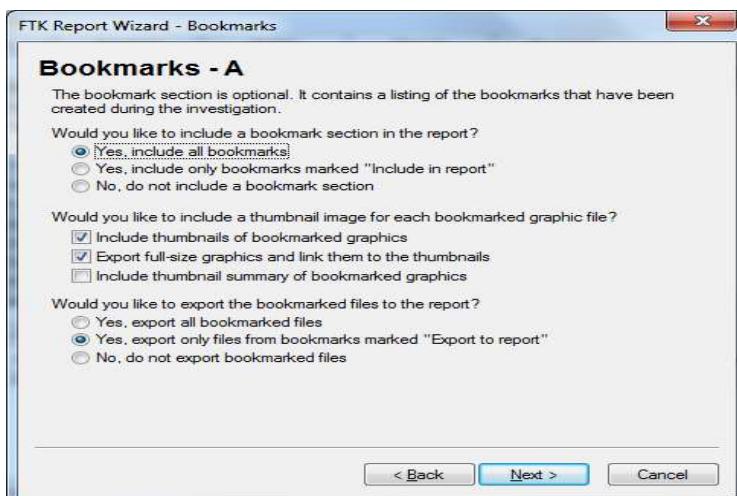
The screenshot shows the FTK Imager interface. The 'Evidence Items' pane on the left indicates there are 507 total file items, 507 checked items, and 1 encrypted file. The 'File Status' and 'File Category' panes show various statistics. The main pane displays a list of encrypted files, including '40488A41374372441D42FB45'. The toolbar at the top includes icons for Overview, Explore, Graphics, E-Mail, Search, and Bookmark.

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

The screenshot shows the AccessData FTK 1.81.0 interface. The 'File' menu is open, showing options like New Case..., Open Case..., Add Evidence..., FTK Imager..., Disk Viewer..., Registry Viewer..., Close Case, Save Case, Backup Case..., Export Files..., Report Wizard..., Update Report, View Report..., Exit, and a path D:\CF pracs\storage media, D:\CF pracs\PDEvidence, D:\CF pracs\backup, and D:\CF pracs\03Starting a new case\Industrial espionage. The 'Report Wizard...' option is highlighted. The main pane shows a list of evidence items with columns for Display Name, Identification Name/Number, and Evidence Type. One item is selected: 'G:\NO NAME-FA...' with 'Storage drive evidence' and 'FAT32'.



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.



The screenshot shows the "File Overview" page of the FTK CASE REPORT software. The left sidebar includes sections for Case Summary, Supplementary Files, List by File Path, MS Access database, List File Properties, Selected Bookmarks, and Selected Graphic Thumbnails. The main content area displays the following statistics:

- Evidence Items:** Evidence Items: 1
- File Items:**
  - Total File Items: 1,611
  - Flagged Thumbnails: 0
  - Other Thumbnails: 808
- File Status:**
  - KFF Alert Files: 0
  - Bad Extended: 0
  - Encrypted Files: 2
  - From E-mail: 0
  - Deleted Files: 1,393
  - From Recycle Bin: 0
  - OLE Subitems: 73
  - Flagged Ignore: 0
  - KFF Ignorable: 0
  - Data Carved Files: 1,382
- File Category:**

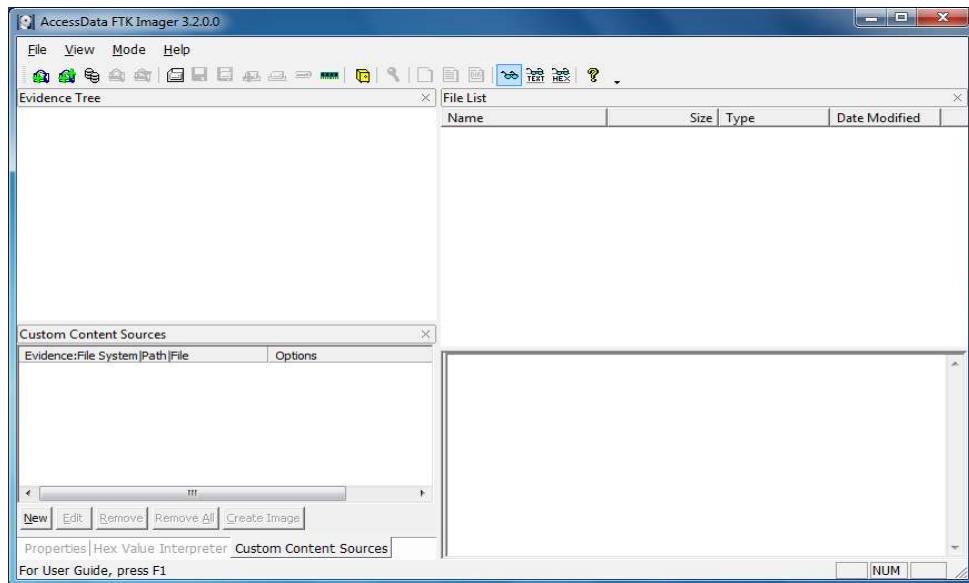
Documents:	506
Spreadsheets:	4
Databases:	0
Graphics:	38
Multimedia:	0
E-mail Messages:	0
Executables:	25
Archives:	25
Forensics:	8
Slack/Free Space:	176
Other Known Type:	31
Unknown Type:	53

## PRACTICAL NO. 04

### Using File Recovery Tools [FTK Imager] Creating Image

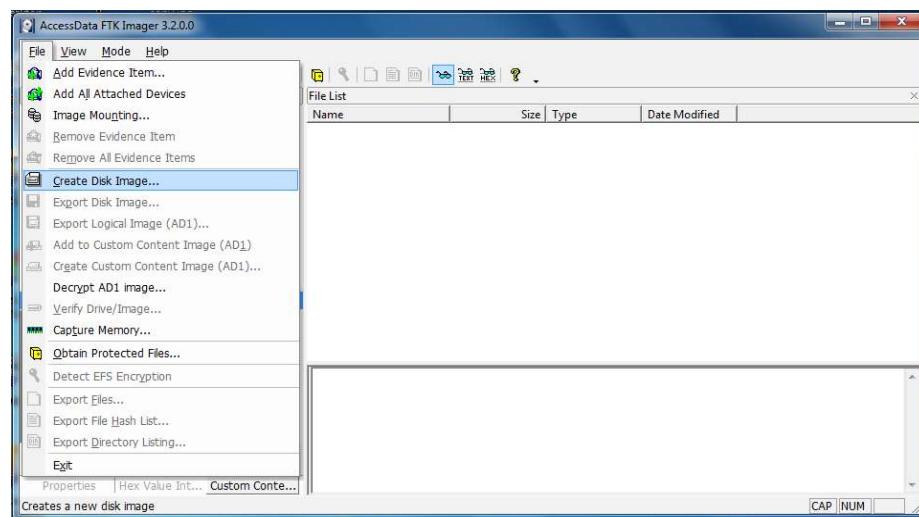
**Aim:** Understanding & working with the process of taking a drive image using AccessData's FTK Imager tool.

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



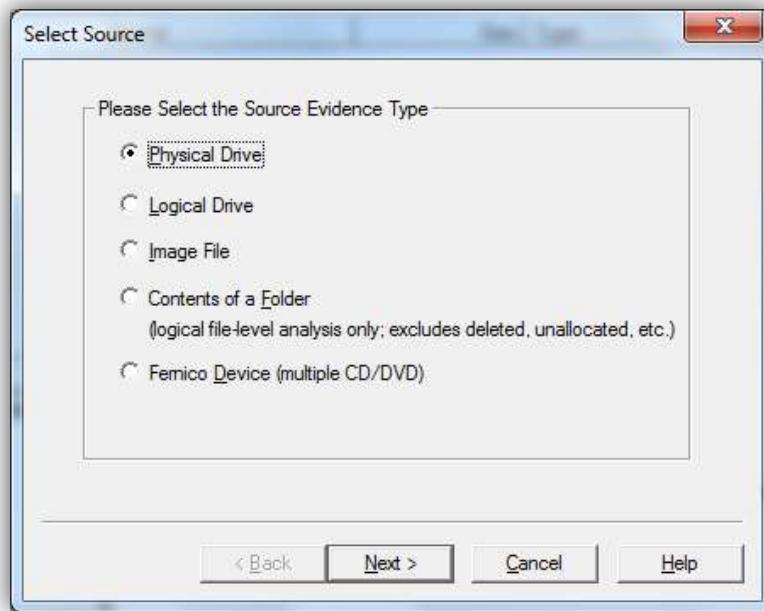
Step 2) To create a forensic image:

Click File > Create Disk Image

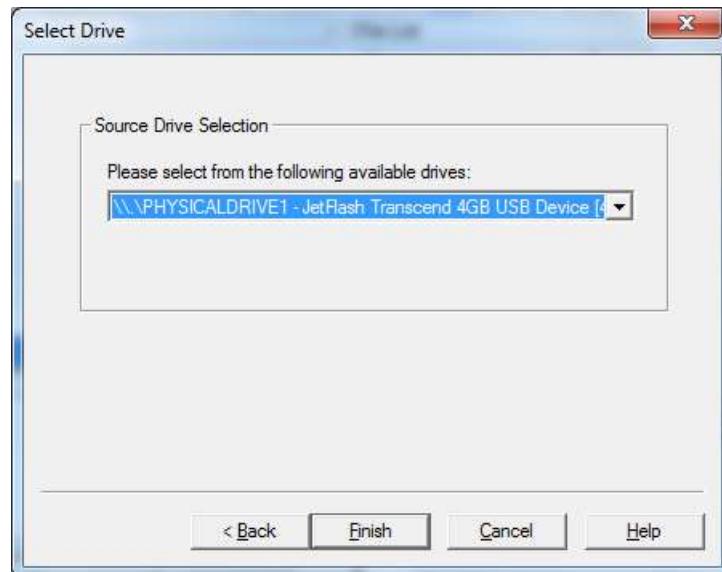


Step 3) In the Select Source dialog box, select the source you want to make an image of. Click Next.

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



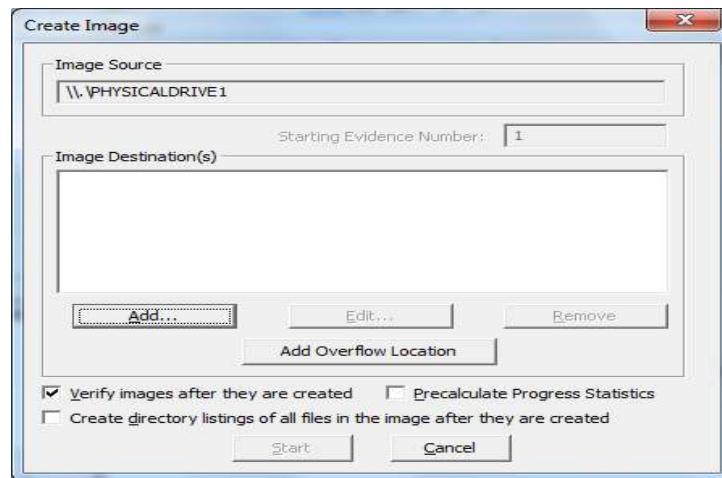
Step 4) Select the drive or browse to the source of the image you want, and then click Finish.



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

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

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

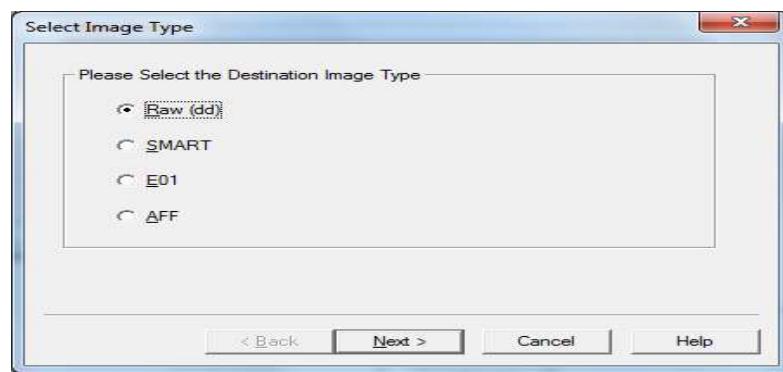


Step 6) Select the type of image you want to create.

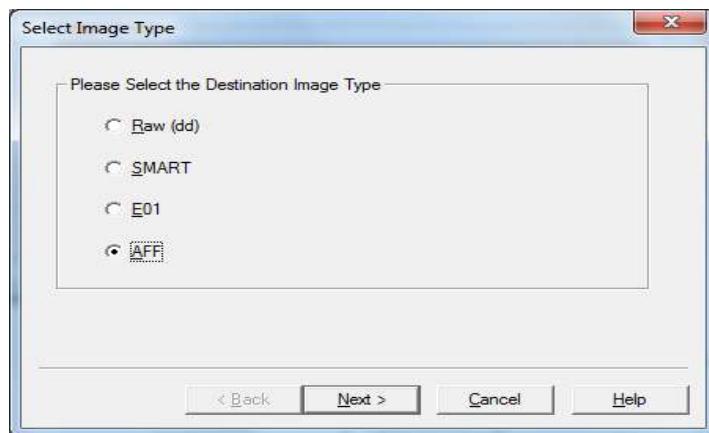
The type you choose will usually depend on what tools you plan to use on the image. The dd format will work with more open-source tools, but you might want SMART or E01 if you will primarily be working with ASR Expert Witness or EnCase, respectively.

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

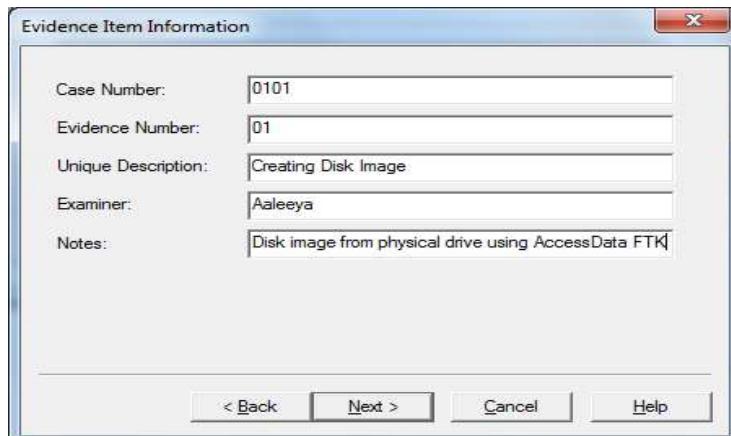
Important: The raw image type is not compressed. If you select the Raw (dd) type, be sure to have adequate available drive space for the resulting image.



Step 7) If you are creating an AFF image type, choose AFF. Click Next. The Image Destination Folder dialog box you see will be different than that seen when selecting any other image type



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



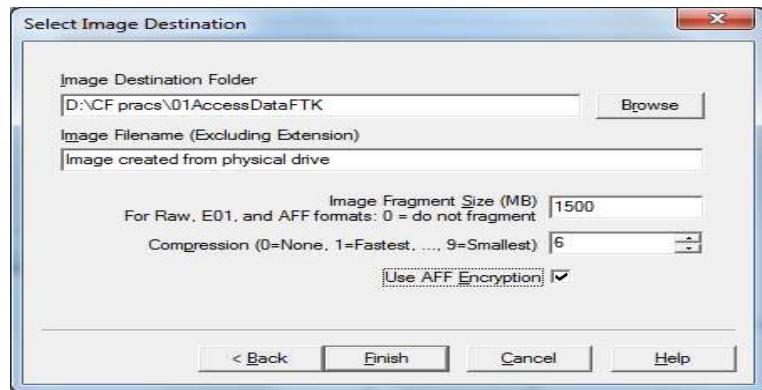
Complete the fields in the Evidence Item Information dialog. Click Next.

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

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

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

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



Step 10) Specify the Image fragment Size:

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

Step 10 a) Select the compression level to use.

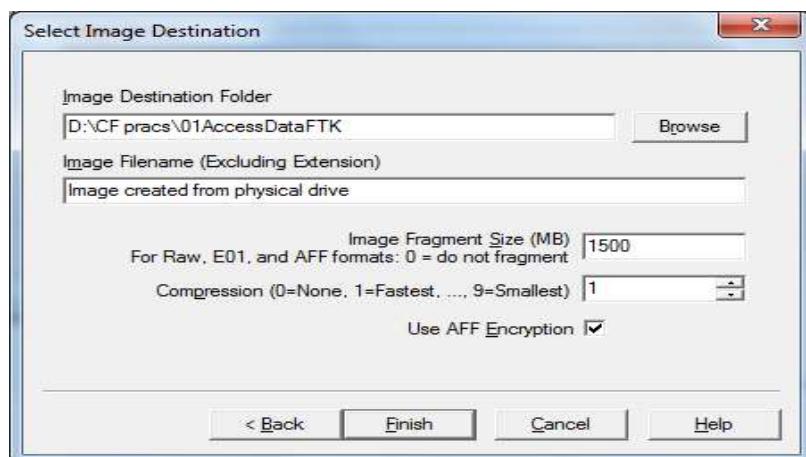
- 0=No Compression
- 1=Fastest, Least Compression (faster, and also slightly smaller than a 0-compression file)
- 9=Slowest, Most Compression (smallest file, slowest to create).

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

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

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

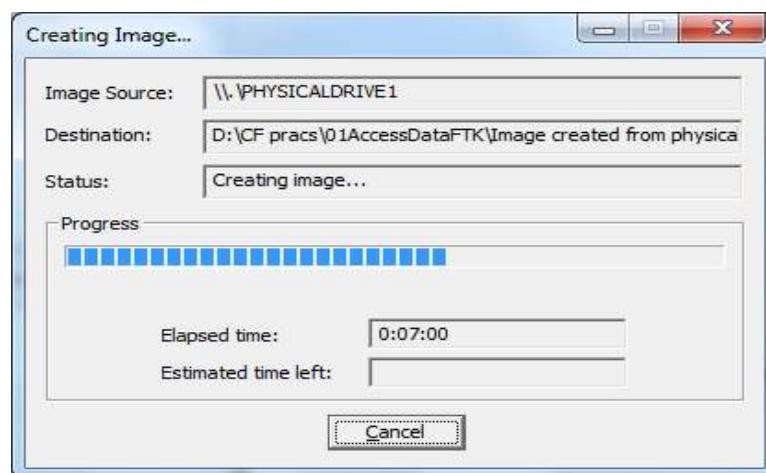
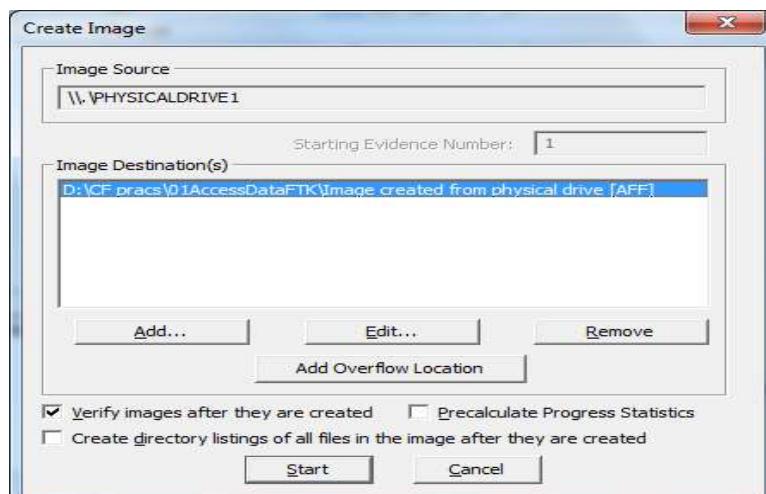
Step 12) Click Finish.



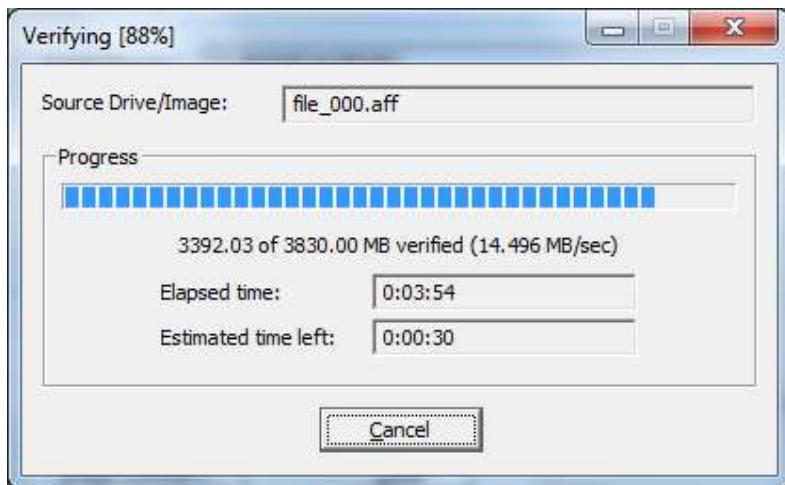
Step 13) When AFF Encryption is selected, type the password, and retype the password to confirm. Click Show Password to see that you have typed it correctly the first time.



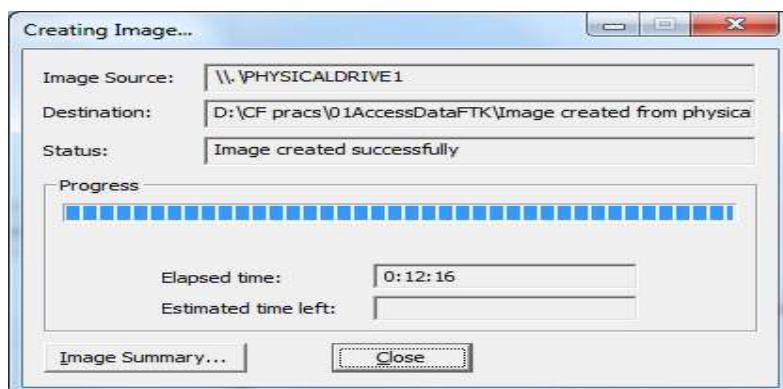
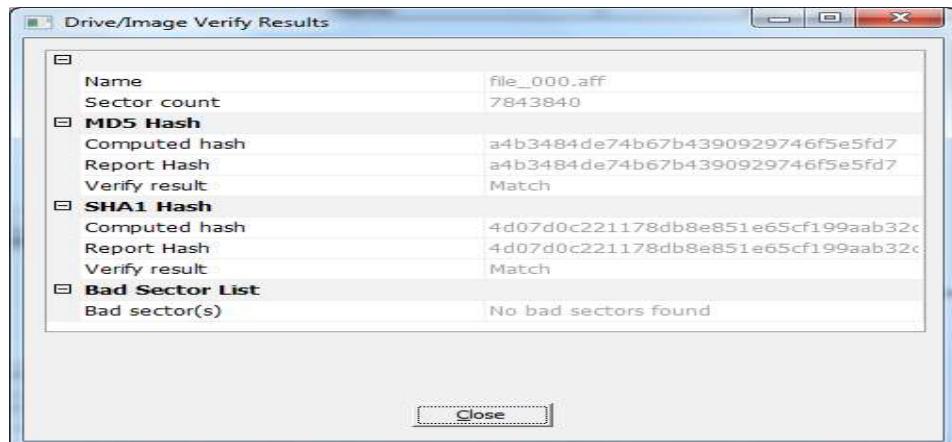
Step 14) When encryption selections are made, click **OK** to save selections and return to the **Create Image dialog**. Click **Start** to begin the imaging process.



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.

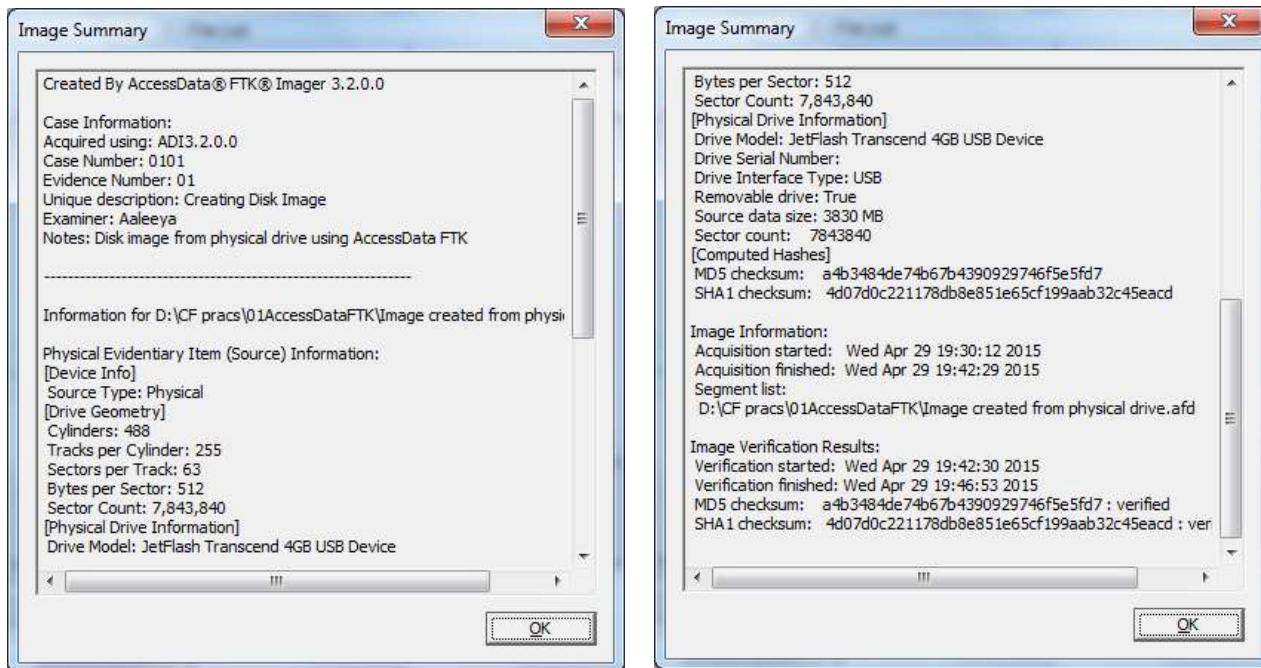


Now is a good time to refill that coffee cup! Once the acquisition is complete, you can view an image summary and the drive will appear in the evidence list in the left-hand side of the main FTK Imager window. You can right-click on the drive name to Verify the Image:



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:



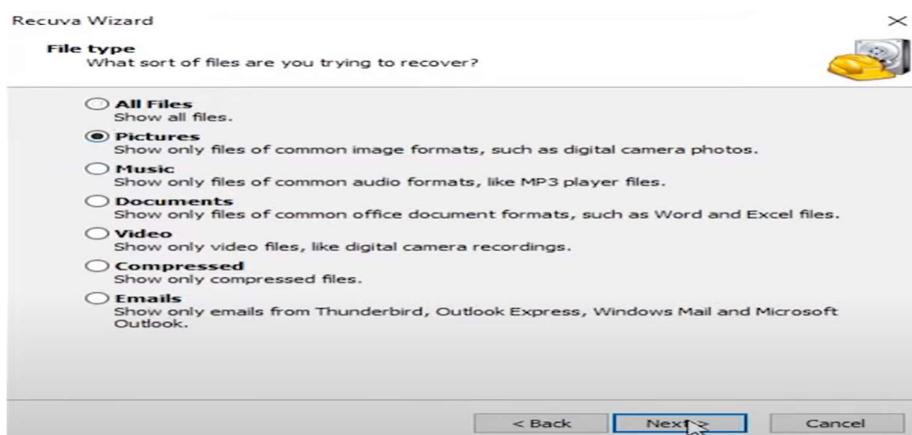
**b. Recover Deleted files using Recuva, PC Inspector File Recovery, Recover My Files**

**Recuva**

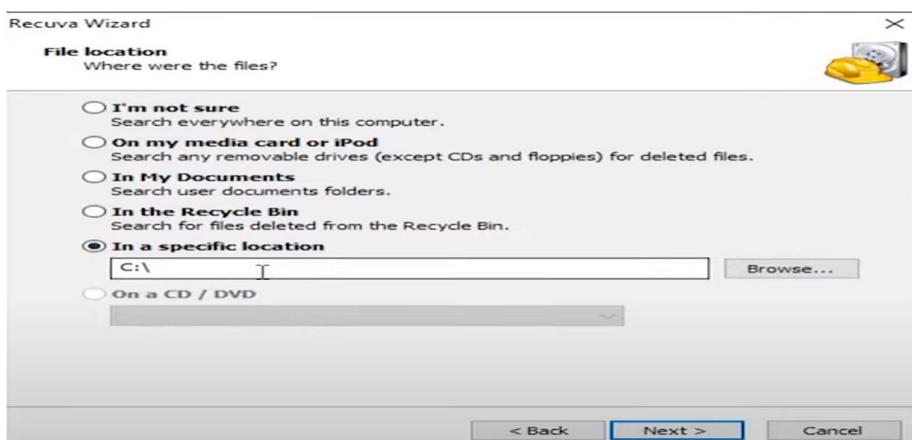
Download and install **Recuva**



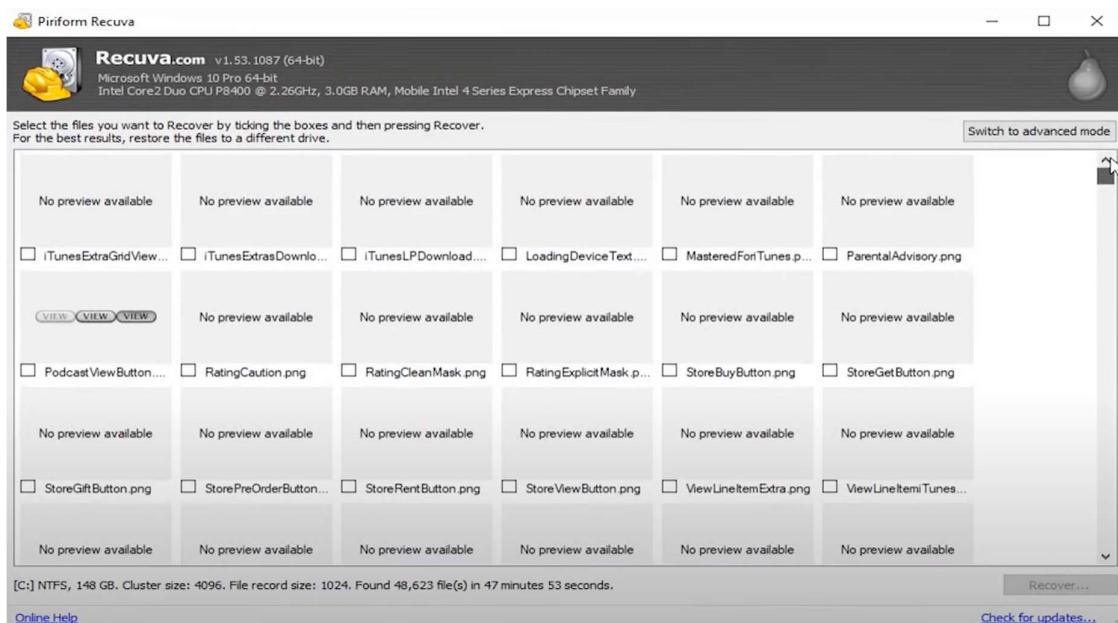
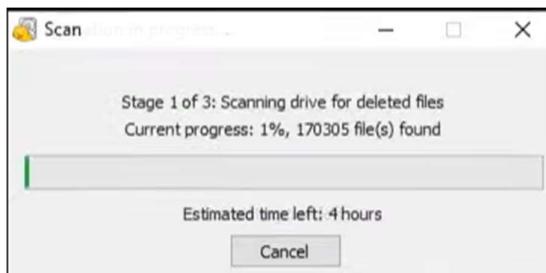
Select File Type you need to recover



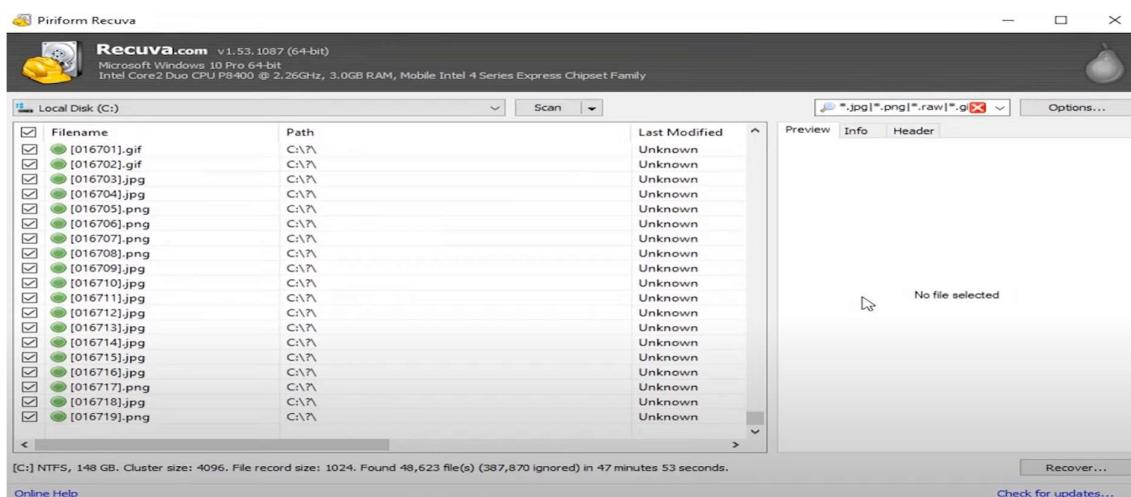
Select File location, which you want to recover files



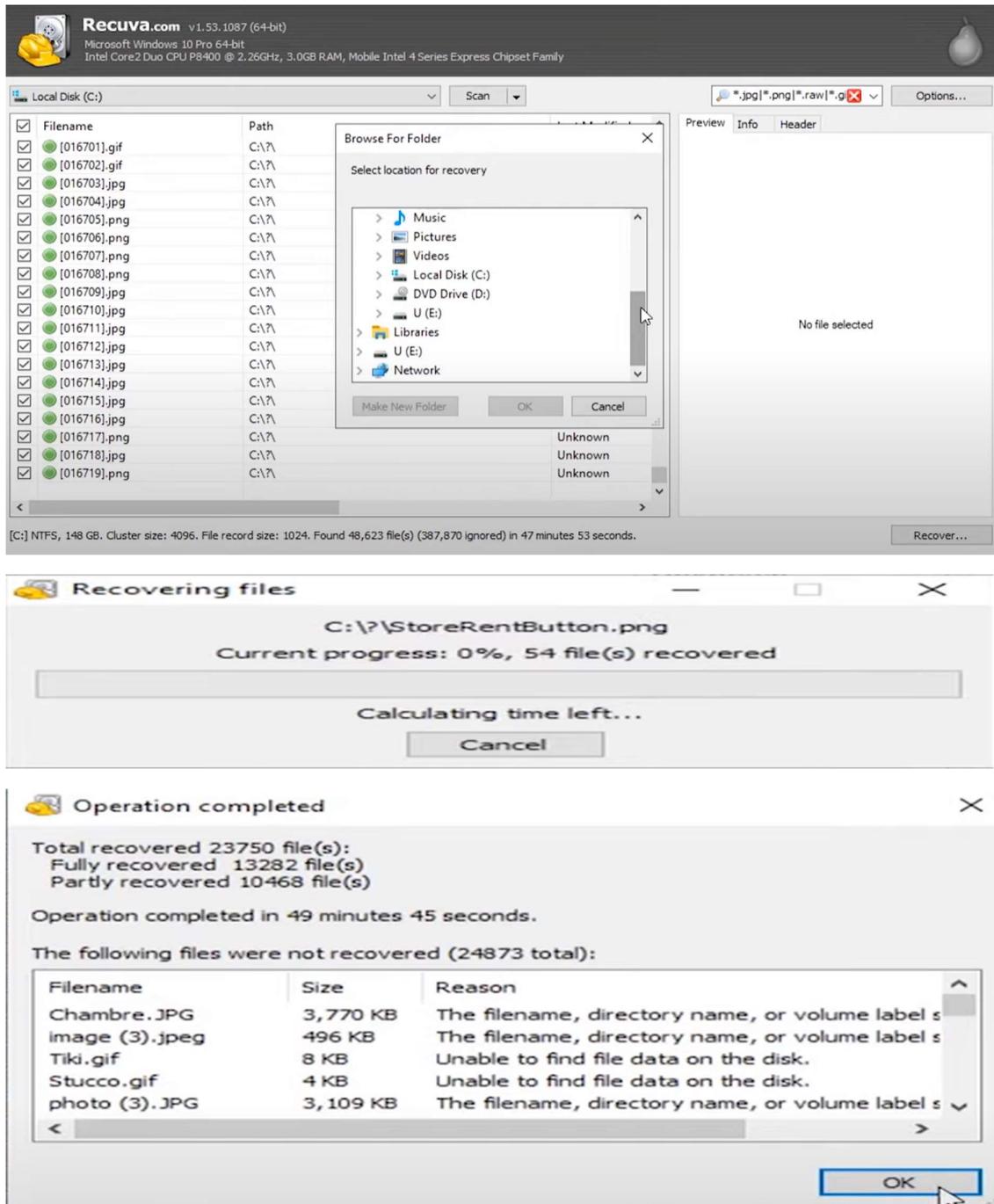
Click next (If want enable Deep Scan)



Switch to advanced mode and select all recover file



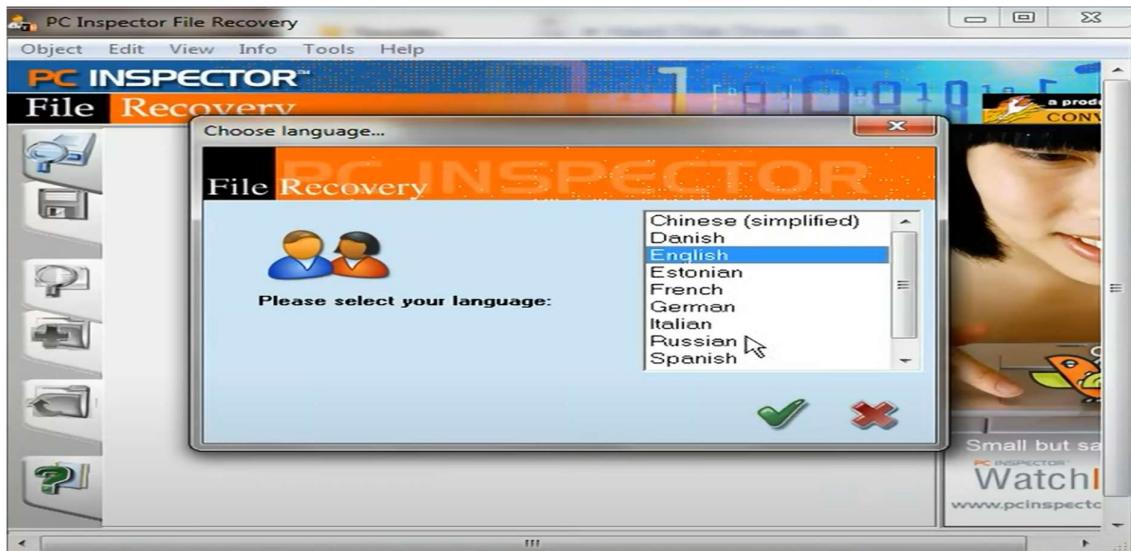
Select the location were to recover the file



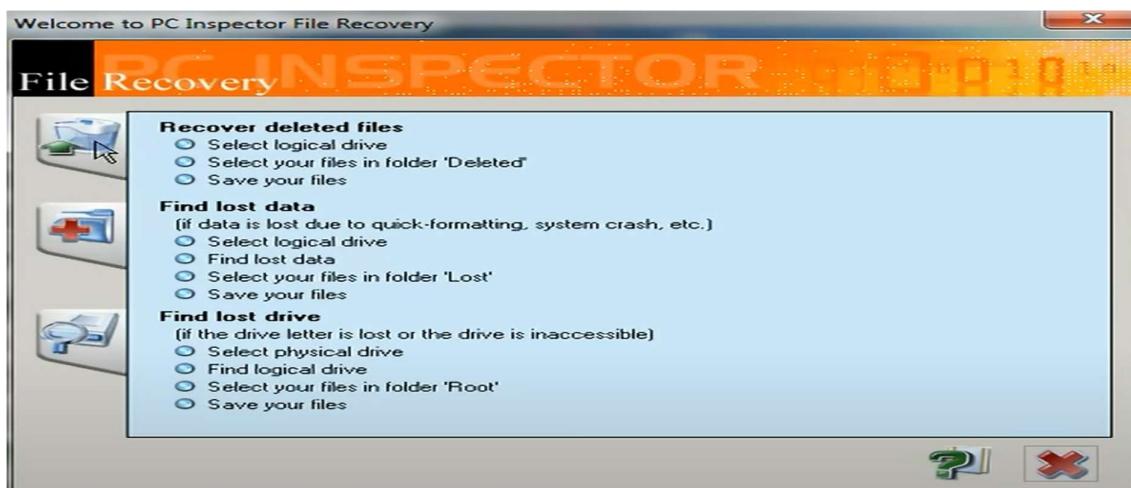
All deleted Files are recovered at specified location

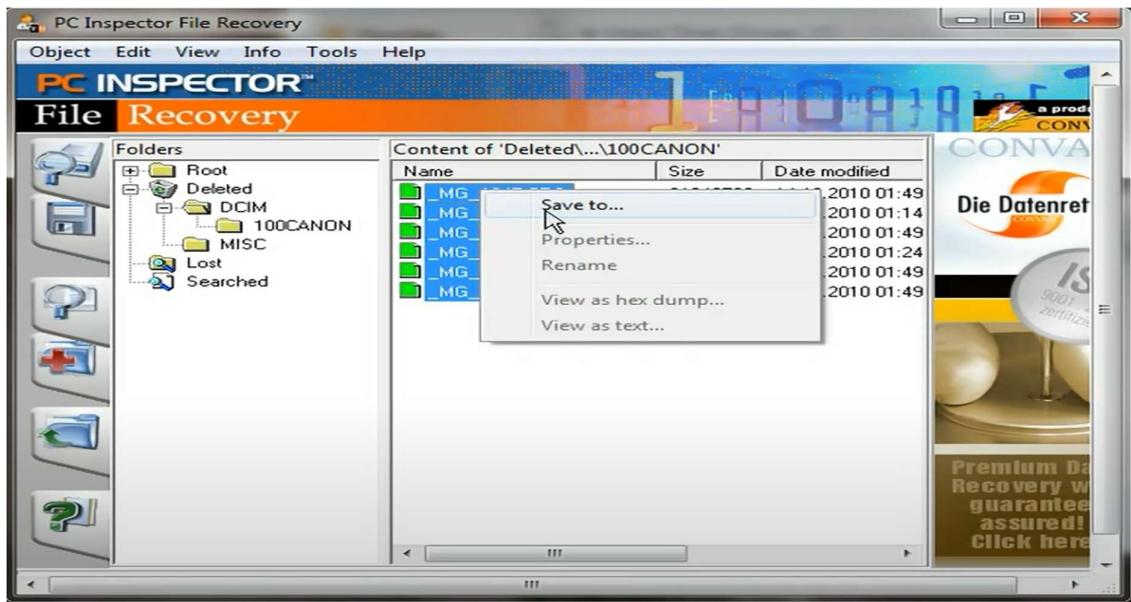
## PC Inspector File Recovery

Download and install PC Inspector File Recovery

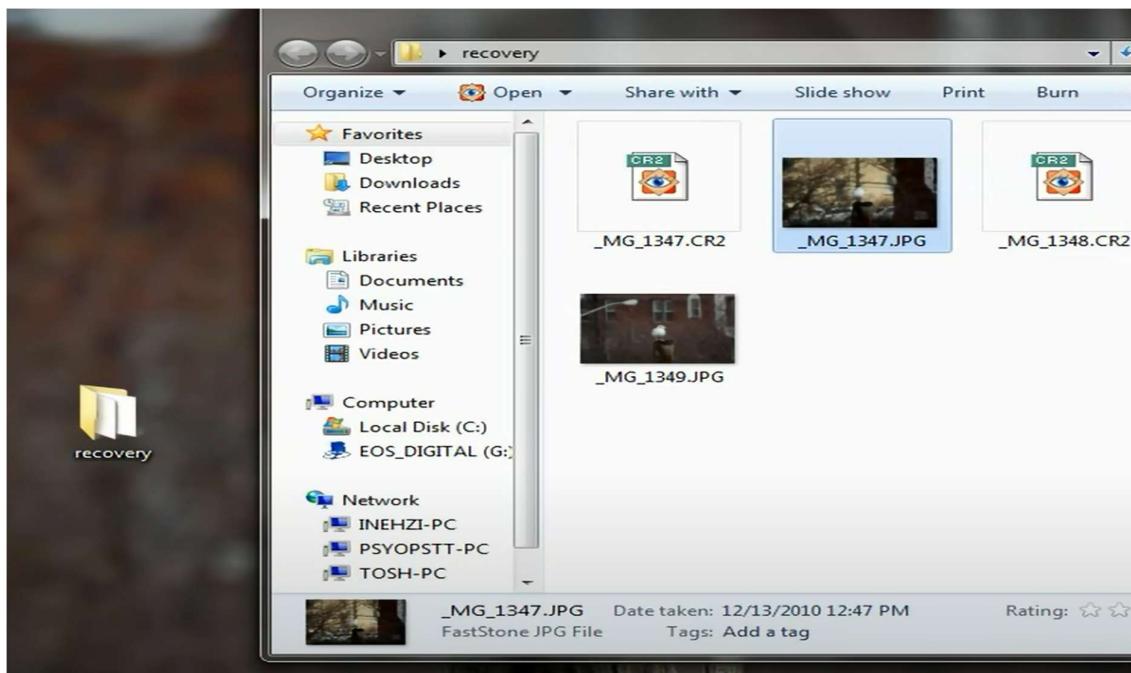


Choose what to recover delete files, lost data or lost drive





Recover data is saved to specified location



## Recover My Files

### Download and install Recover My Files



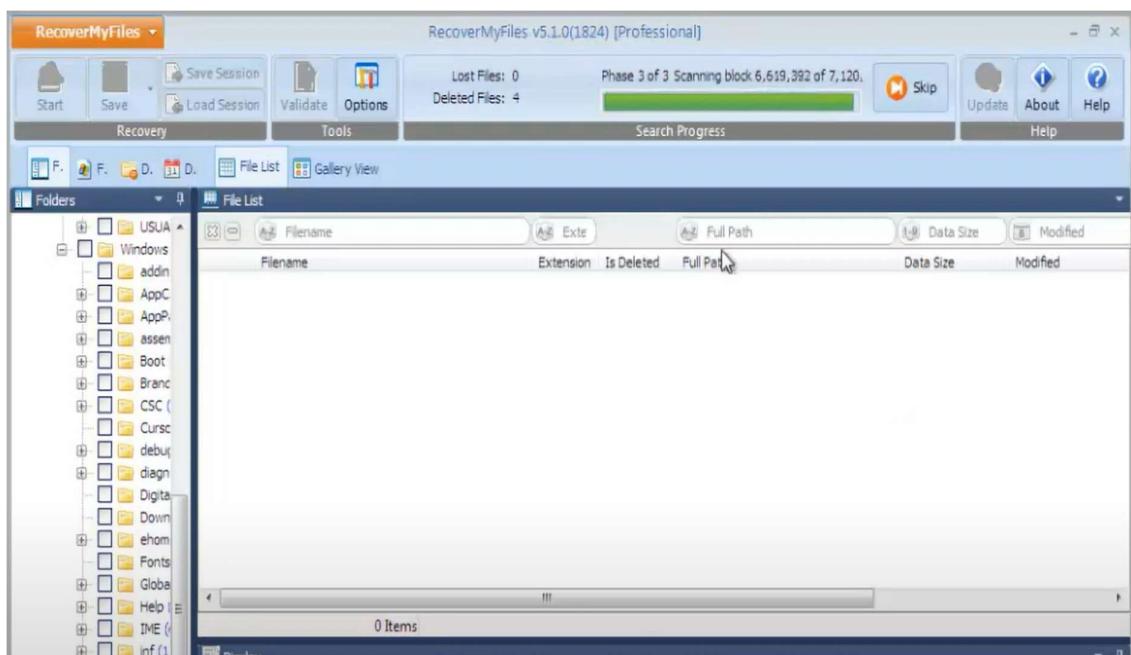
Select the option you wish to of Recover Files and Recover a Drive



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

The image displays three windows of the RecoverMyFiles v5.1.0(1824) [Professional] application.

**Top Window:** Shows the main interface with a toolbar at the top. The "Recovery" tab is selected. The status bar indicates "Lost Files: 0" and "Deleted Files: 4". A progress bar shows "Phase 3 of 3 Search Completed". The "File List" pane on the right shows a table of recovered files:

Filename	Extension	Is Deleted	Full Path
Bitacora Respaldos.xlsx	.xlsx	Yes	C:\Root\Users\USUARIO\
Conector.docx	.docx	Yes	C:\Root\Users\USUARIO\
desktop.ini	.ini		C:\Root\Users\USUARIO\
Recover My Files v5.lnk	.lnk		C:\Root\Users\USUARIO\

**Middle Window:** "RecoverMyFiles - Save Files" dialog. It shows "Saving 843 KB of data in 2 separate files". The "Save location" field is empty, with a "Browse..." button. The "Current Save Settings" section has a "Set Options" button. At the bottom are "OK" and "Cancel" buttons.

**Bottom Window:** "RecoverMyFiles - Save Files" dialog showing the completion of the save process. The message says "Saving of files completed (Saved 2 from 2 selected)". The "Summary" section shows the following statistics:

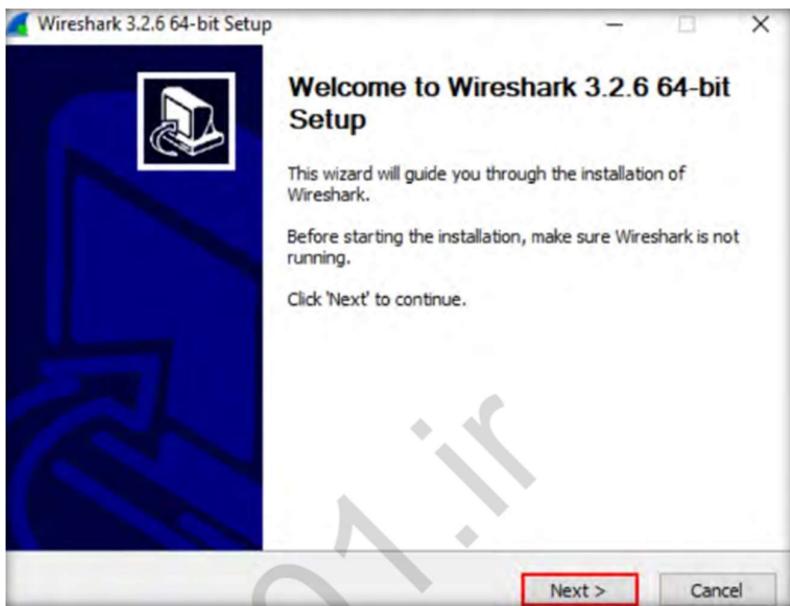
Saving:	Size:
Path too Long :	0
Renamed :	0
Ignored :	0
Unknown error :	0
Zero length file :	0
Deleted File :	0
No files in Folder :	0

An "OK" button is at the bottom right.

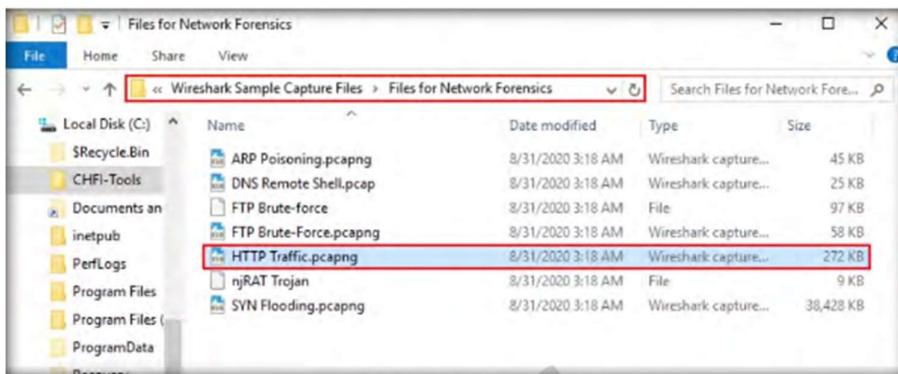
## **PRACTICAL NO. 05**

### **a. Using Web attack detection tools [Wireshark]**

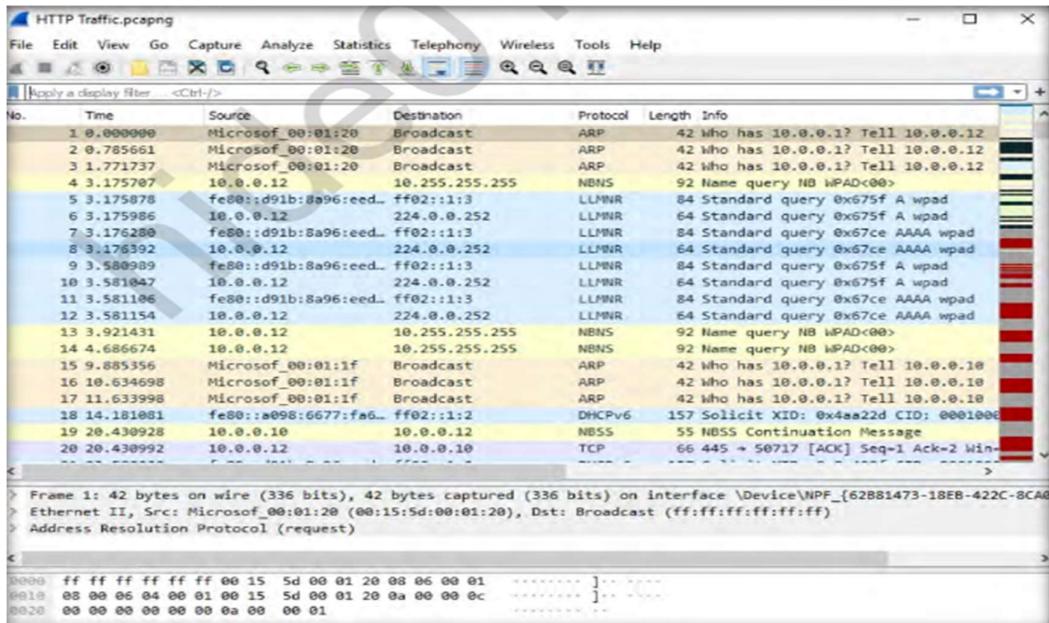
1. Download and install wireshark



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



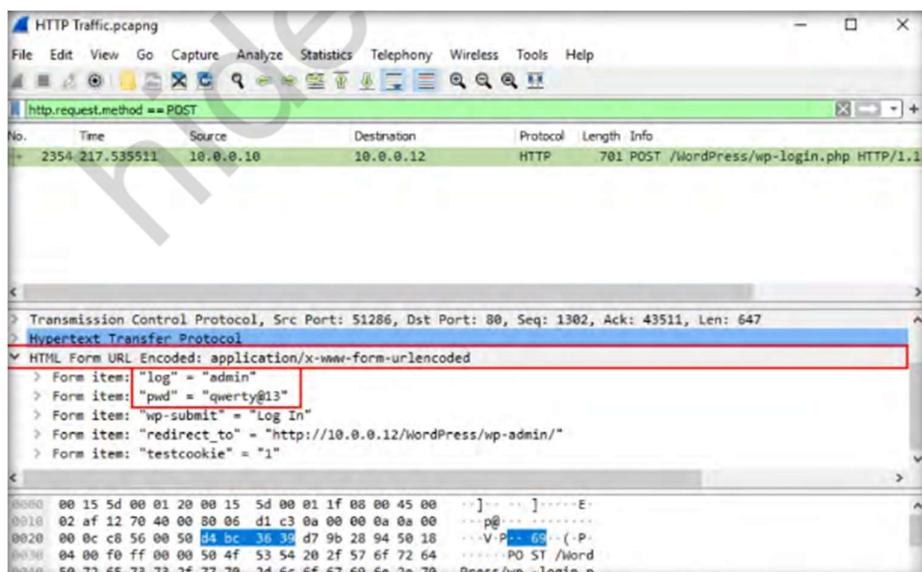
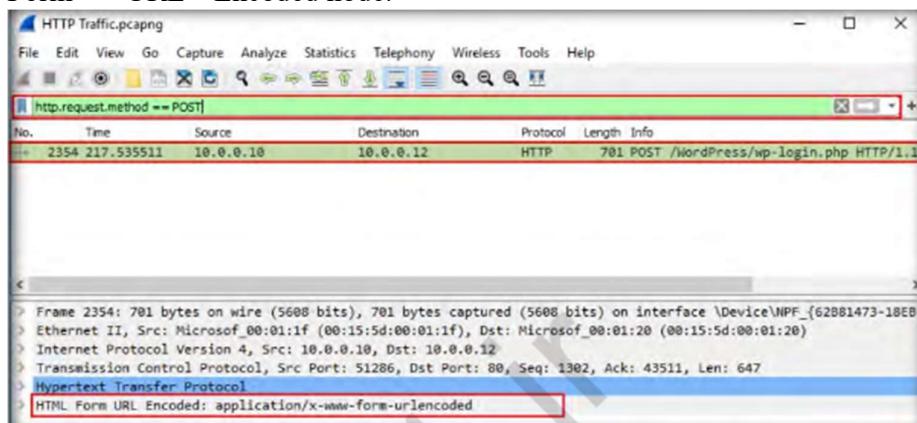
3. The above operation will launch the Wireshark GUI window and display the packets captured in HTTP Traffic.pcapng, as shown in the following screenshot



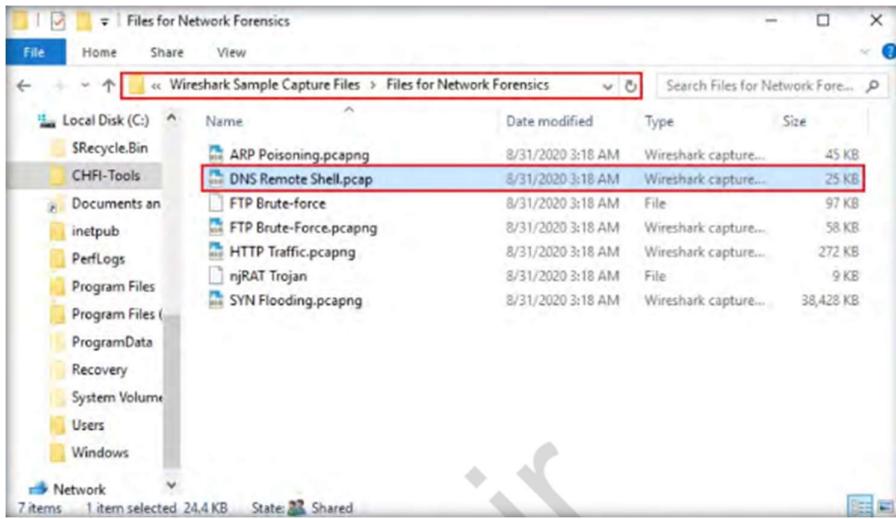
4. We will now apply the http filter so that the application displays results related to traffic generated through http. Type http in the Filter field and press Enter to filter the http traffic, as indicated in the screenshot below:

The top screenshot shows the 'http' filter applied in the 'Filter' field. The bottom screenshot shows the resulting filtered traffic, which includes several HTTP requests and responses, such as GET /wordpress/ HTTP/1.1, 200 OK (text/html), and POST /WordPress/wp-login.php HTTP/1.1 (text/html).

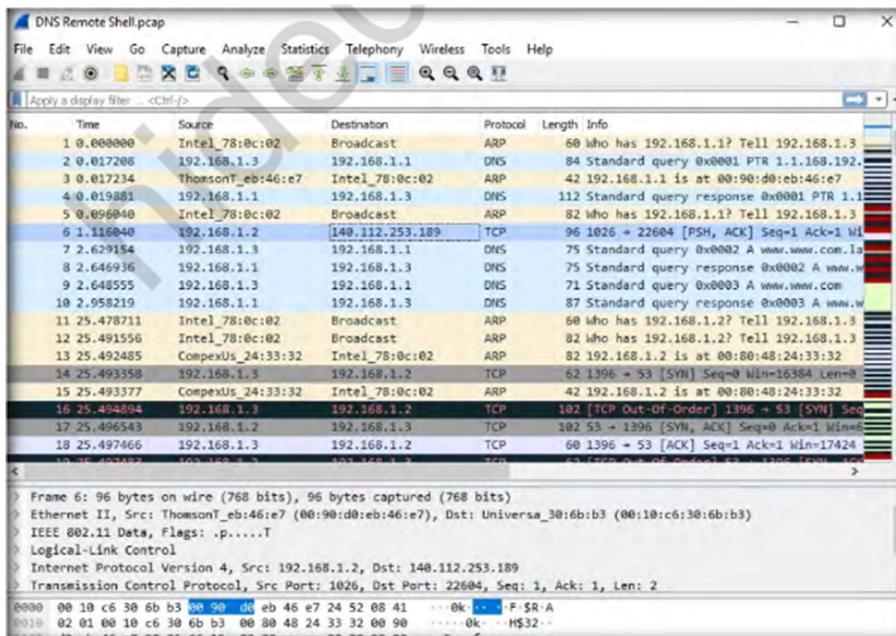
5. After examining the entries displayed by the application in the screenshot above, it is evident that the http traffic is associated with a WordPress website, and it is being transmitted in a plain text format. Generally, user credentials are stored in the POST requests. Therefore, examining packet(s)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

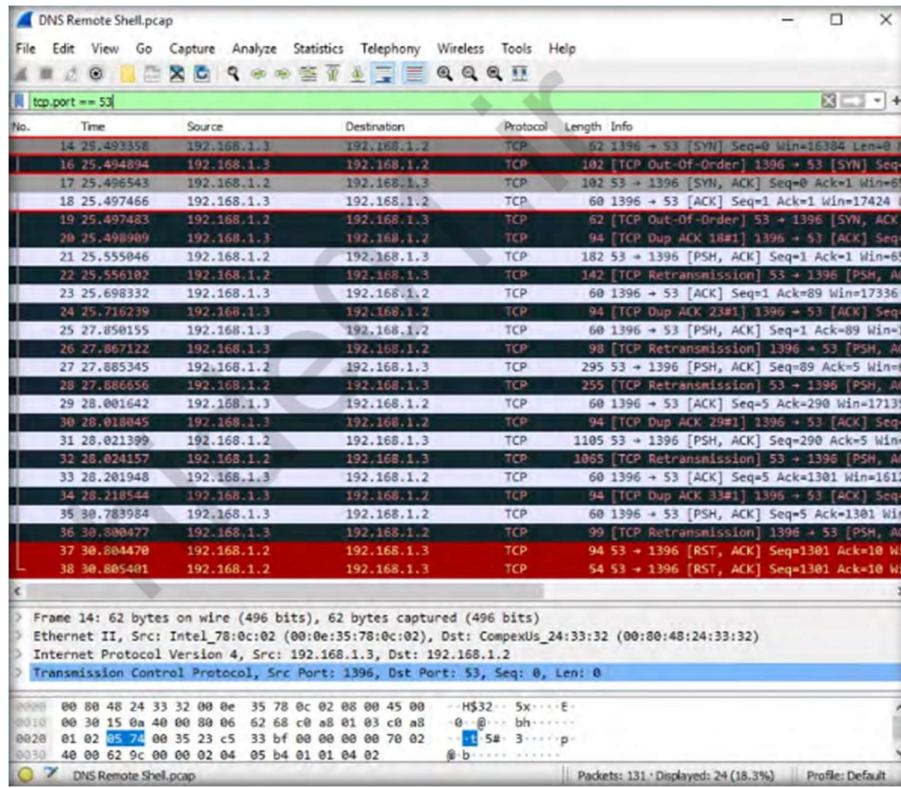


9. Since DNS uses port 53 for communicating with clients, we will be filtering the traffic flowing to and from port 53. To filter traffic flowing on port 53, type the command `tcp.port == 53` in the Filter field and press Enter. Wireshark filters the traffic flowing on port 53 and displays it, as shown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

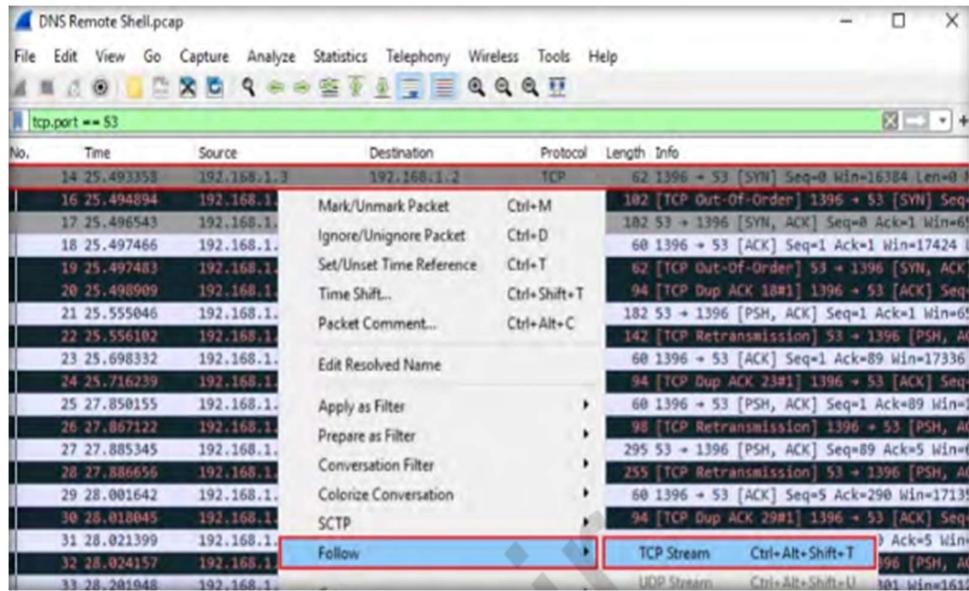
No.	Time	Source	Destination	Protocol	Length	Info
14	25.493358	192.168.1.3	192.168.1.2	TCP	62	1396 → 53 [SYN] Seq=0 Win=16384 Len=0 MSS=14
16	25.494894	192.168.1.3	192.168.1.2	TCP	102	[TCP Out-Of-Order] 1396 → 53 [SYN] Seq=0 Win=65535
17	25.496543	192.168.1.2	192.168.1.3	TCP	102	53 + 1396 [SYN, ACK] Seq=1 Ack=1 Win=65535
18	25.497466	192.168.1.3	192.168.1.2	TCP	60	1396 → 53 [ACK] Seq=1 Ack=1 Win=17424 Len=0
19	25.497483	192.168.1.2	192.168.1.3	TCP	62	[TCP Out-Of-Order] 53 + 1396 [SYN, ACK] Seq=1 Ack=1 Win=17336
20	25.498909	192.168.1.3	192.168.1.2	TCP	94	[TCP Dup ACK 1881] 1396 → 53 [ACK] Seq=1 Ack=1 Win=65535
21	25.555046	192.168.1.2	192.168.1.3	TCP	182	53 + 1396 [PSH, ACK] Seq=1 Ack=1 Win=65535
22	25.556182	192.168.1.2	192.168.1.3	TCP	142	[TCP Retransmission] 53 + 1396 [PSH, ACK] Seq=1 Ack=89 Win=17336
23	25.698332	192.168.1.3	192.168.1.2	TCP	60	1396 → 53 [ACK] Seq=1 Ack=89 Win=17336 Len=0
24	25.716239	192.168.1.3	192.168.1.2	TCP	94	[TCP Dup ACK 23#1] 1396 → 53 [ACK] Seq=1 Ack=89 Win=17336
25	27.850155	192.168.1.3	192.168.1.2	TCP	60	1396 → 53 [PSH, ACK] Seq=1 Ack=89 Win=17336
26	27.867122	192.168.1.3	192.168.1.2	TCP	98	[TCP Retransmission] 1396 → 53 [PSH, ACK] Seq=1 Ack=89 Win=17336
27	27.885345	192.168.1.2	192.168.1.3	TCP	295	53 + 1396 [PSH, ACK] Seq=89 Ack=5 Win=65535
28	27.886658	192.168.1.2	192.168.1.3	TCP	255	[TCP Retransmission] 53 + 1396 [PSH, ACK] Seq=89 Ack=5
29	28.001642	192.168.1.3	192.168.1.2	TCP	60	1396 → 53 [ACK] Seq=5 Ack=299 Win=17135 Len=0
30	28.018045	192.168.1.3	192.168.1.2	TCP	94	[TCP Dup ACK 29#1] 1396 → 53 [ACK] Seq=5 Ack=299
31	28.021399	192.168.1.2	192.168.1.3	TCP	1105	53 + 1396 [PSH, ACK] Seq=299 Ack=5 Win=65535
32	28.024157	192.168.1.2	192.168.1.3	TCP	1065	[TCP Retransmission] 53 + 1396 [PSH, ACK] Seq=299 Ack=5
33	28.281948	192.168.1.3	192.168.1.2	TCP	60	1396 → 53 [ACK] Seq=5 Ack=1301 Win=16124 Len=0
34	28.218544	192.168.1.3	192.168.1.2	TCP	94	[TCP Dup ACK 33#1] 1396 → 53 [ACK] Seq=5 Ack=1301
35	30.783984	192.168.1.3	192.168.1.2	TCP	60	1396 → 53 [PSH, ACK] Seq=5 Ack=1301 Win=16124
36	30.880477	192.168.1.3	192.168.1.2	TCP	99	[TCP Retransmission] 1396 → 53 [PSH, ACK] Seq=5 Ack=1301
37	30.884478	192.168.1.2	192.168.1.3	TCP	94	53 + 1396 [RST, ACK] Seq=1301 Ack=10 Win=0
38	30.885401	192.168.1.2	192.168.1.3	TCP	54	53 + 1396 [RST, ACK] Seq=1301 Ack=10 Win=0

Frame 14: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)  
 > Ethernet II, Src: Intel\_78:0c:02 (00:0e:35:78:0c:02), Dst: CompuXUS\_24:33:32 (00:80:48:24:33:32)  
 > Internet Protocol Version 4, Src: 192.168.1.3, Dst: 192.168.1.2  
 > Transmission Control Protocol, Src Port: 1396, Dst Port: 53, Seq: 0, Len: 0

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 Packet 17, 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:



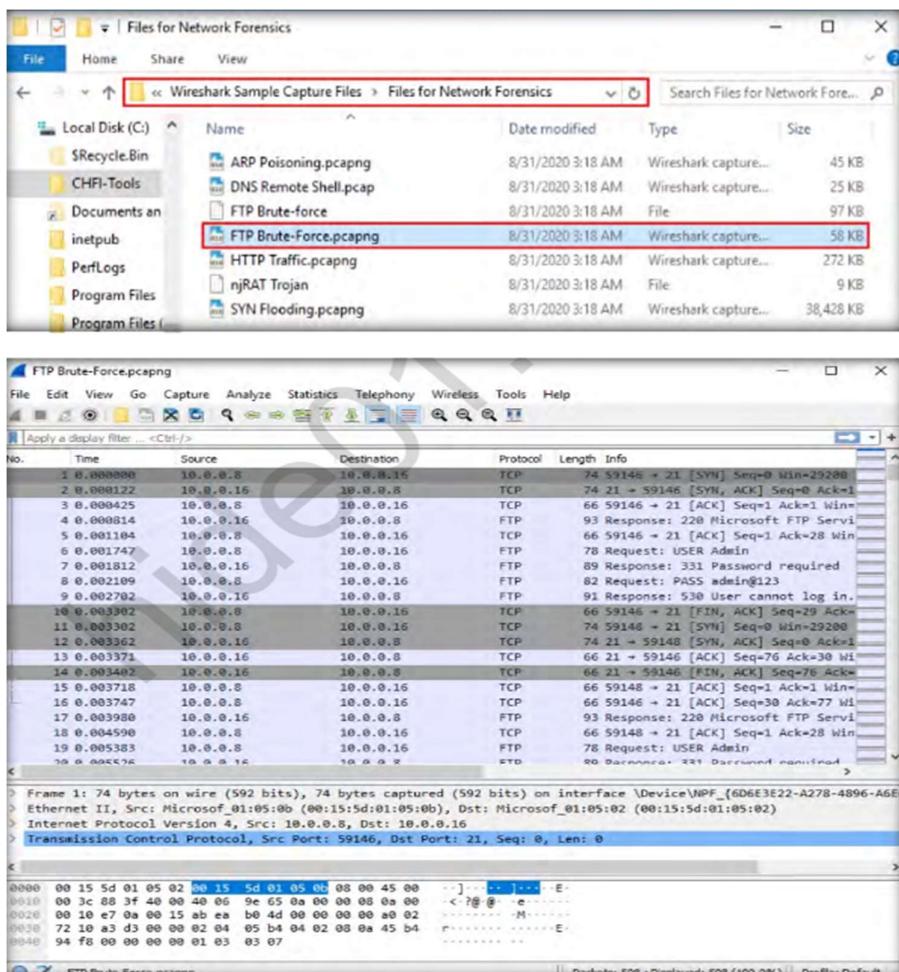
10. Right-click on any one of the packets from 14 to 38 (here, we have right-clicked on packet 14), select Follow from the context menu, and then click TCP Stream from the resultant drop-down list, as shown in the screenshot below:



Microsoft Windows XP [Version 5.1.2600]  
(C) Copyright 1985-2001 Microsoft Corp.

```
C:\>dir  
dir  
Volume in drive C has no label.  
Volume Serial Number is FF47-B0EB  
  
Directory of C:\  
  
01/12/2005 11:59 AM          0 arrorlog.txt  
01/19/2004 09:45 PM          0 AUTOEXEC.BAT  
01/19/2004 09:45 PM          0 CONFIG.SYS  
06/26/2004 12:12 PM <DIR>          Documents and Settings  
02/03/2005 11:40 PM <DIR>          EasyBoot  
02/29/2004 02:51 PM          11,531 installer-debug.txt  
12/19/2004 12:56 AM <DIR>          nra  
12/19/2004 12:51 AM <DIR>          nrafold  
11/24/2004 07:47 PM <DIR>          nnt  
10/07/2004 10:01 AM <DIR>          movie  
06/26/2004 01:03 PM <DIR>          My Downloads  
01/13/2005 10:52 PM <DIR>          Program Files  
01/04/2005 10:27 AM <DIR>          quarantine  
04/19/2004 09:57 PM          7,241 s37g  
31/10/2004 08:36 PM          0 s3fs  
06/02/2004 08:54 PM          123 systemscandata.txt  
08/08/2004 10:46 AM <DIR>          Temp  
12/12/2004 02:24 PM          94,135,944 temp.mpg  
01/13/2005 06:10 PM <DIR>          WINDOWS  
11/20/2004 09:27 AM <DIR>          NUTemp  
  
2 client psts, 3 server psts, 3 items.
```

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



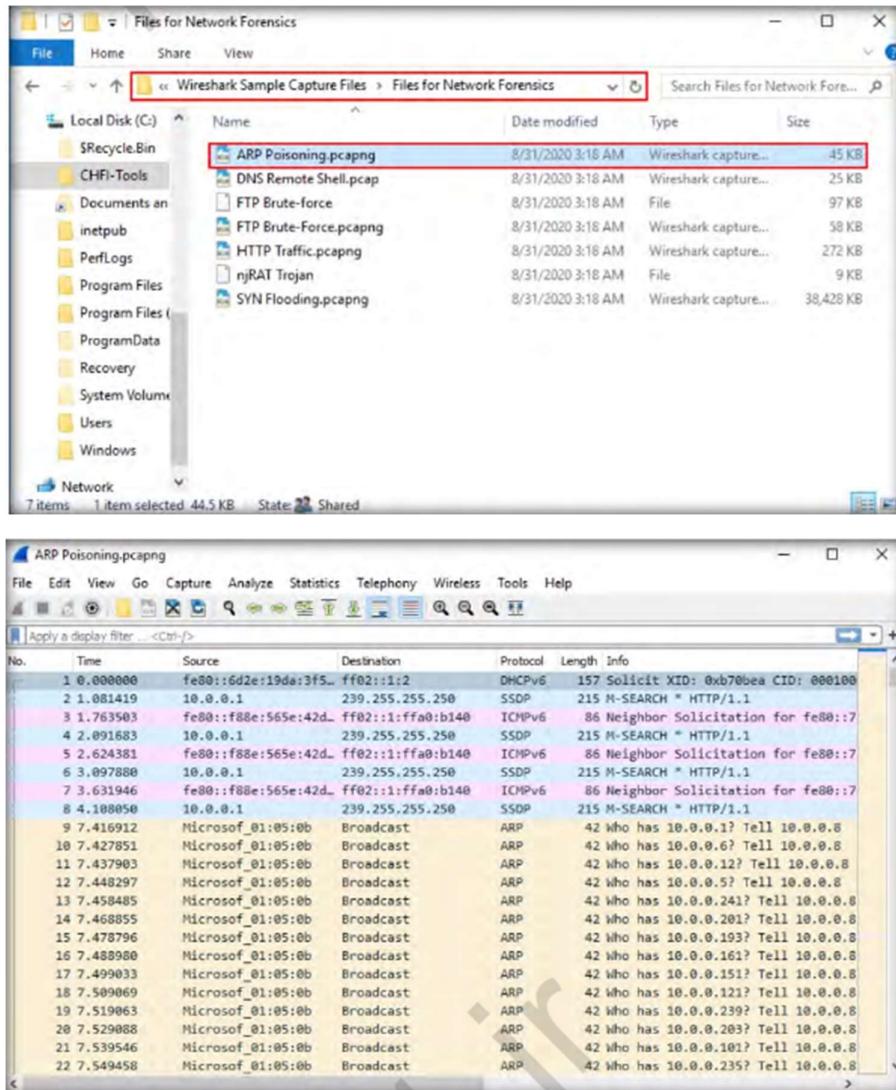
12. Apply the `ftp.response.code == 530` filter to monitor all unsuccessful login attempts over FTP. Upon applying the filter, the application will fetch results pertaining to unsuccessful login attempts, as shown in the screenshot below:

The screenshot shows a Wireshark capture window titled "FTP Brute-Force.pcapng". A green filter bar at the top displays "`ftp.response.code == 530`". The main pane lists network traffic with the following columns: No., Time, Source, Destination, Protocol, Length, and Info. The "Info" column shows repeated entries of "91 Response: 530 User cannot log in." for various source and destination addresses. Below the table, the packet details pane shows the structure of a captured frame, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol (TCP) headers, along with the FTP response payload.

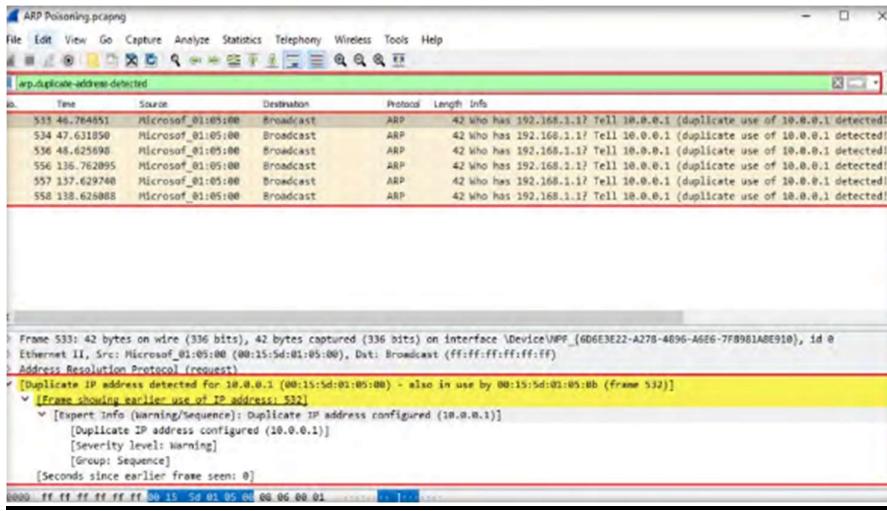
13. The screenshot above shows multiple unsuccessful login attempts made from the source IP 10.0.0.16 to the target IP 10.0.0.8, which strongly indicates a brute-force attack.<sup>27</sup> Apply the `ftp.response.code == 230` filter to see successful logins on the FTP server. The application will fetch 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

The screenshot shows a Wireshark capture window titled "FTP Brute-Force.pcapng". A green filter bar at the top displays "`ftp.response.code == 230`". The main pane lists network traffic with the same columns as the previous screenshot. The "Info" column shows entries of "87 Response: 230 User logged in." for three specific source and destination pairs. Below the table, the packet details pane shows the structure of a captured frame, including the successful login response payload.

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.



16. 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

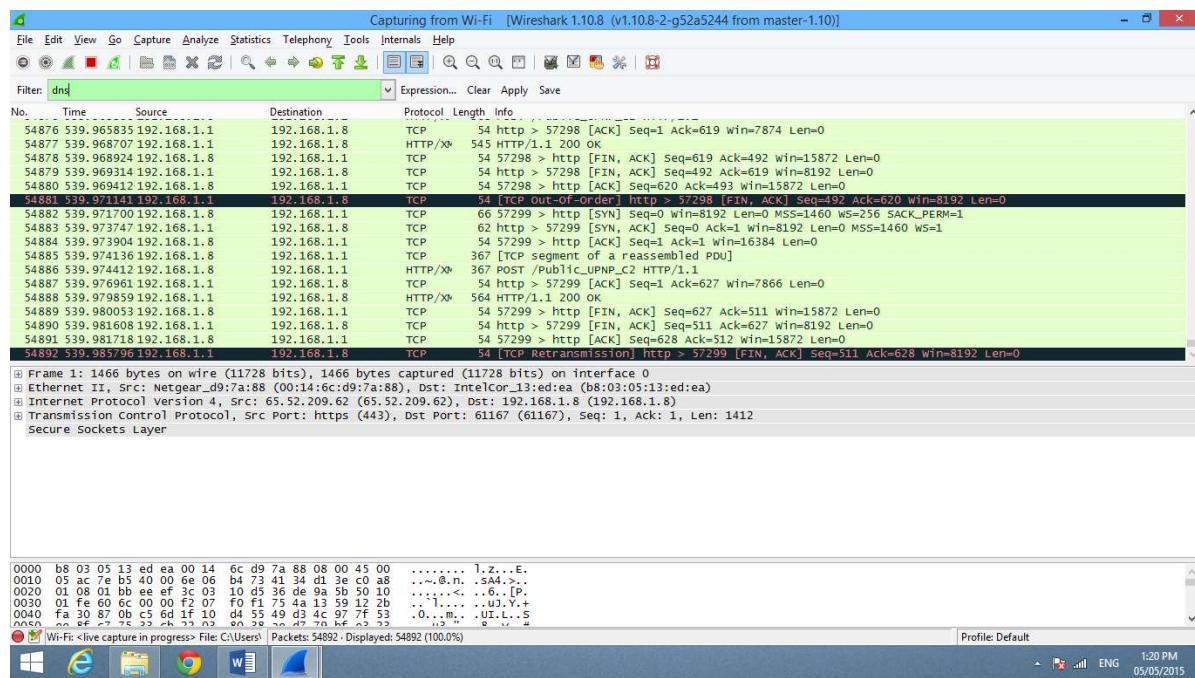
#### Aim: Exploring Wireshark

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

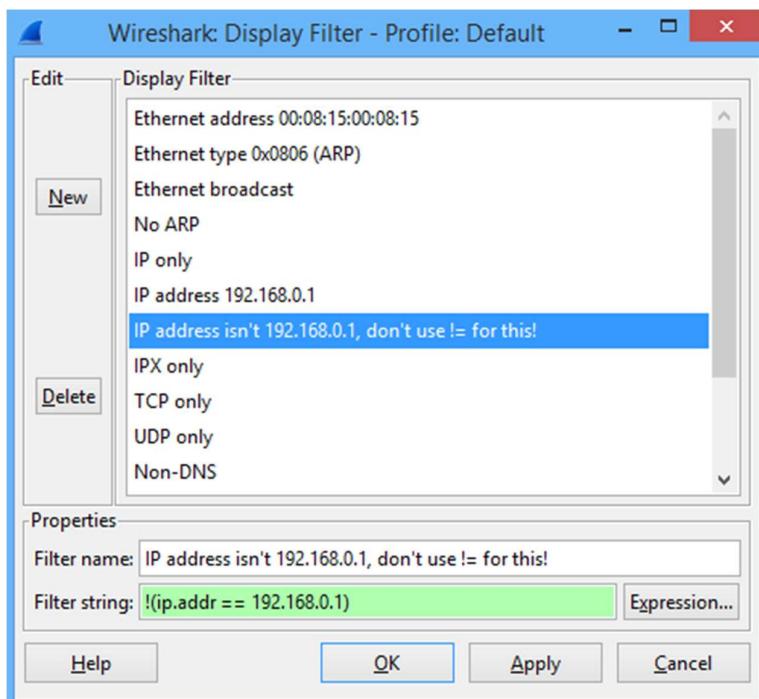
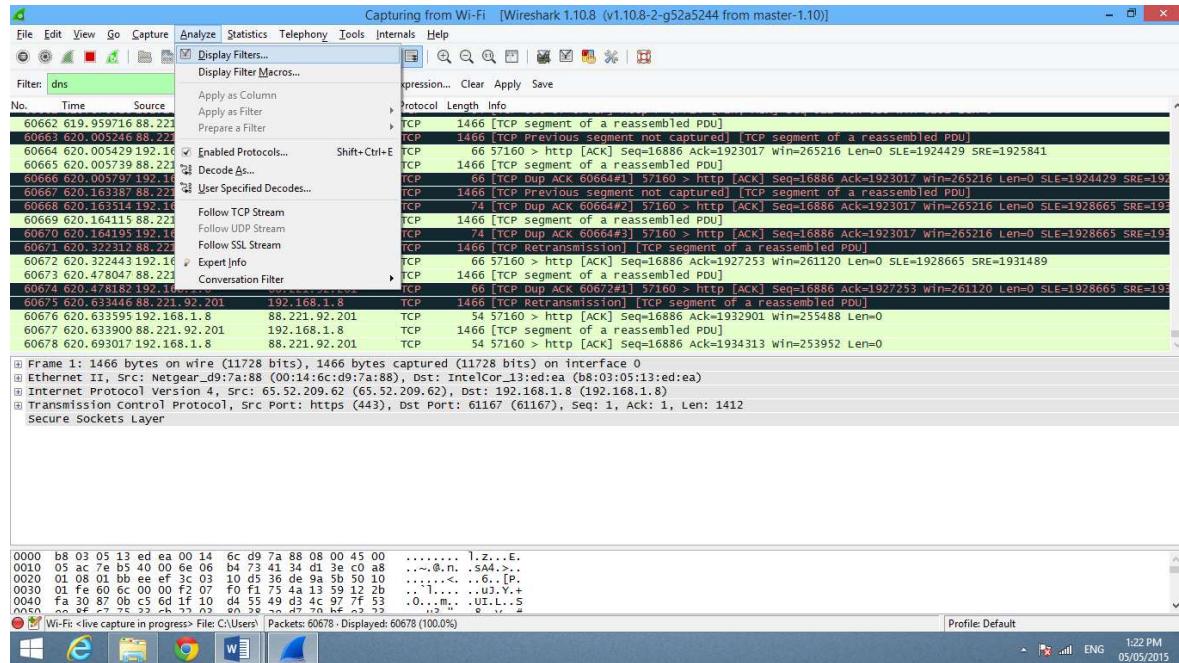
#### Filtering Packets

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

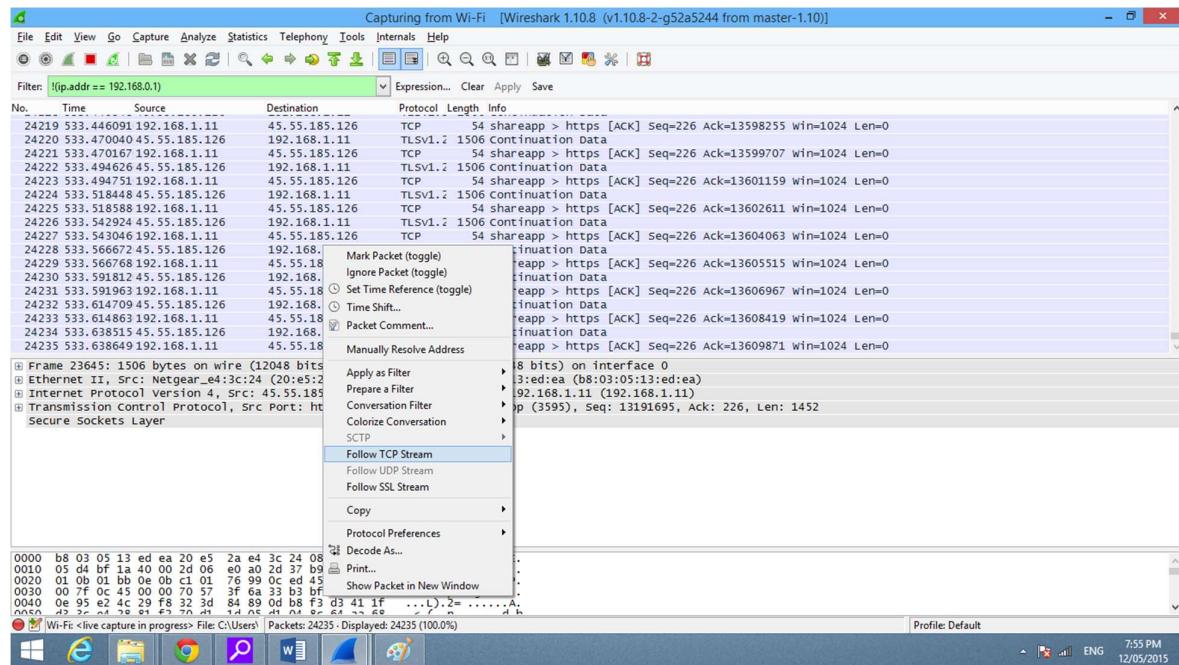
The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type "dns" and you'll see only DNS packets. When you start typing, Wireshark will help you autocomplete your filter.



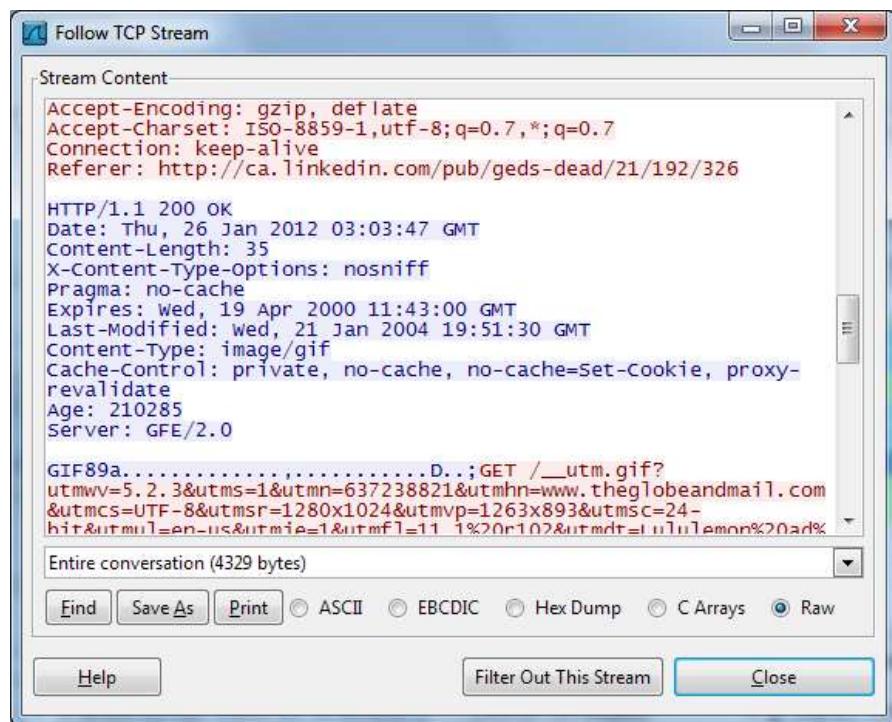
You can also click the Analyze menu and select Display Filters to create a new filter.



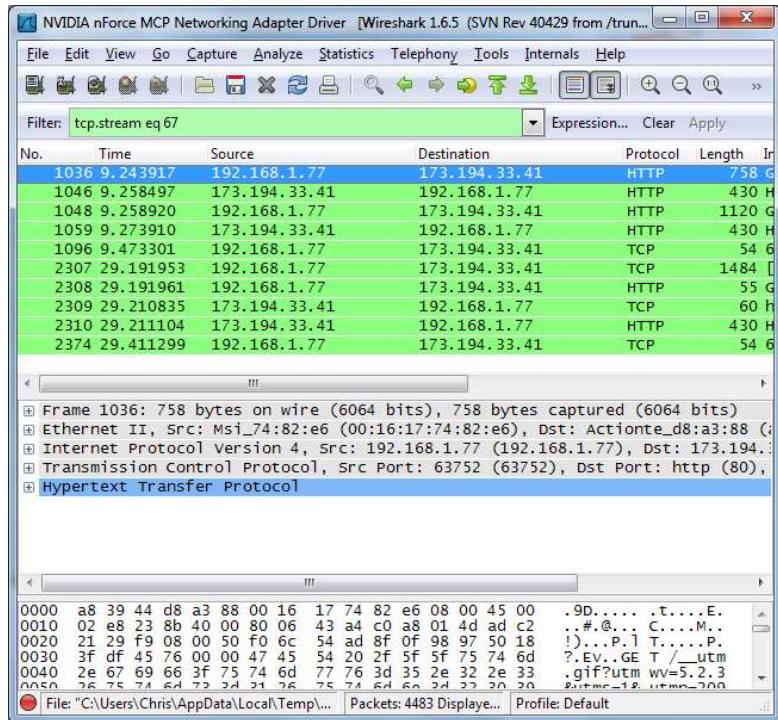
Another interesting thing you can do is right-click a packet and select Follow TCP



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

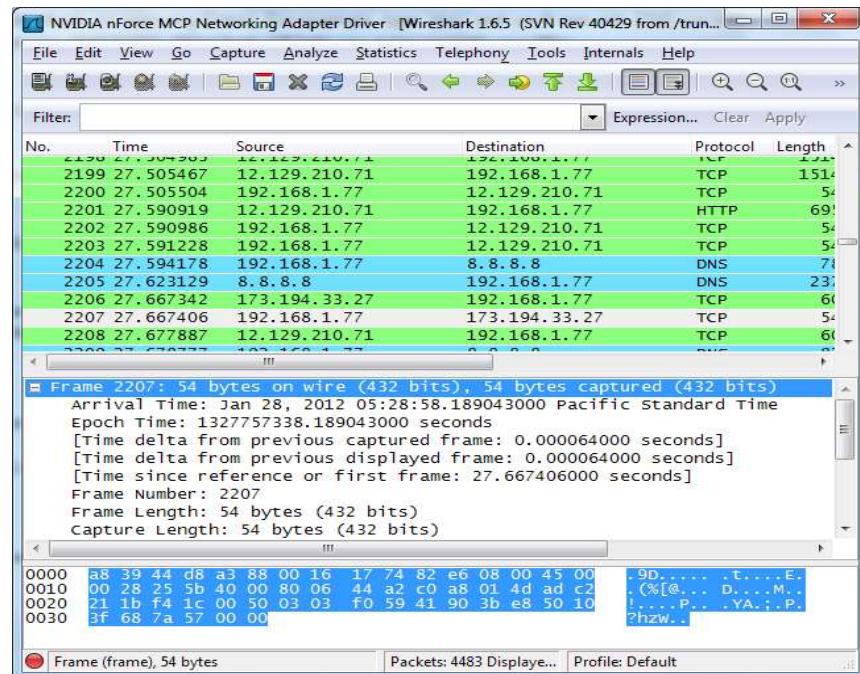


Close the window and you'll find a filter has been applied automatically — Wireshark is showing you the packets that make up the conversation.

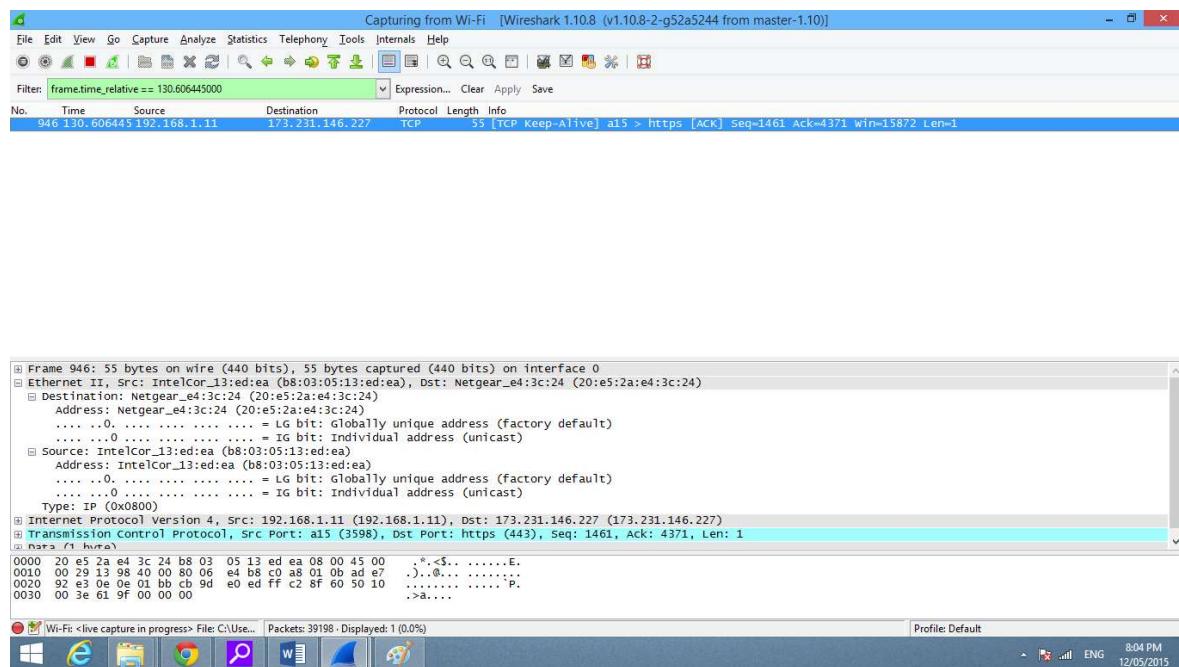
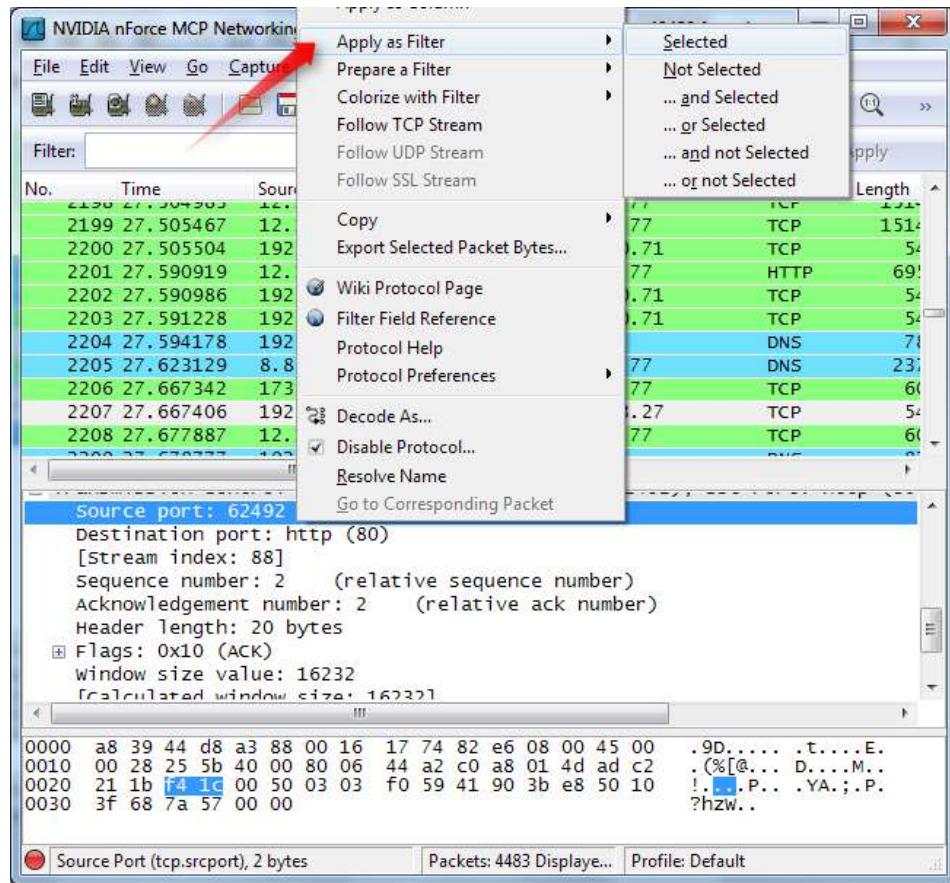


## Inspecting Packets

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

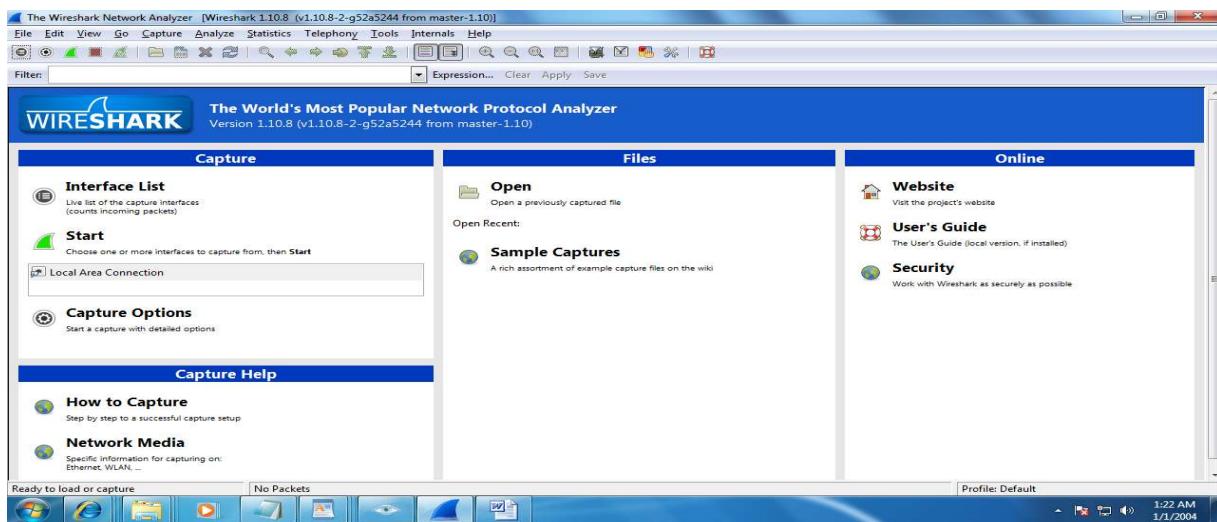


You can also create filters from here — just right-click one of the details and use the Apply as Filter submenu to create a filter based on it.

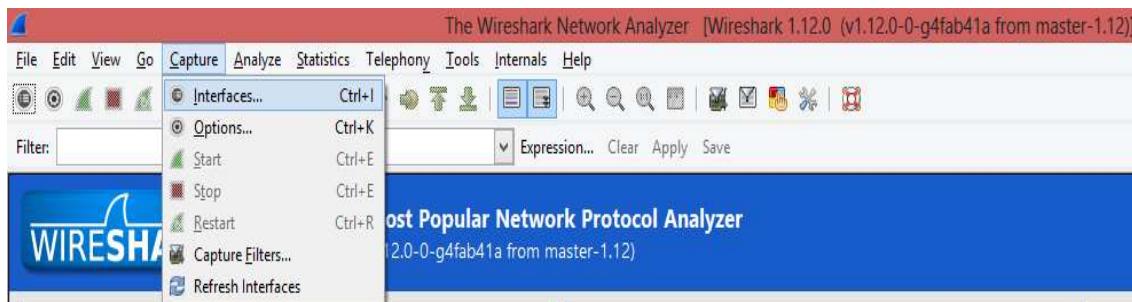


## Using Traffic Capturing and Analysis tools

### Aim: Exploring Wireshark



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



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



Capturing from Local Area Connection [Wireshark 1.10.8 (v1.10.8-2-g52a5244 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
447	39.4081010	fe80::1ced:94c1:e31ff02::1:2		DHCPv6	148	Solicit XID: 0x7bf3ee CID: 00010001196830e6001cc0028790
448	39.4238390	fe80::ad4e:e2c0:d6dff02::1:3		LLMNR	85	Standard query 0x085a A BSCIT
449	39.4240930	192.168.0.114	224.0.0.252	LLMNR	65	Standard query 0x085a A BSCIT
450	39.42448480	fe80::18d2:c188:6d9ff02::1:fffd2:9b0c		ICMPv6	86	Neighbor solicitation for fe80::44de:e2c0:d6d2:9b0c from e0:69:95:fb:c3:db
451	39.4244880	Pegatron_Fb:c3:db	Broadcast	ARP	60	Who has 192.168.0.114? Tell 192.168.0.100
452	39.4246640	fe80::a4de:e2c0:d6dff02::1:4e19		ICMPv6	86	Neighbor solicitation for fe80::18d2:c188:6d9c:4e19 from 00:27:0e:36:b7:be
453	39.4252970	192.168.0.114	224.0.0.252	LLMNR	65	Standard query 0x8fae AAAA BSCIT
454	39.4518730	fe80::e8bc:49:3935:ff02::1:3		LLMNR	85	Standard query 0xc916 A BSCIT
455	39.4526960	192.168.0.117	224.0.0.252	LLMNR	65	Standard query 0xc916 A BSCIT
456	39.4535530	fe80::e8bc:49:3935:ff02::1:3		LLMNR	85	Standard query 0xe89c AAAA BSCIT
457	39.6655100	192.168.0.116	255.255.255.255	UDP	129	Source port: 61109 Destination port: 10505
458	40.2919260	fe80::e8bc:49:3935:ff02::1:3		LLMNR	85	Standard query 0x55db A BSCIT
459	40.2923960	192.168.0.117	224.0.0.252	LLMNR	65	Standard query 0x55db A BSCIT
460	40.2930380	fe80::e8bc:49:3935:ff02::1:3		LLMNR	85	Standard query 0xd885 AAAA BSCIT
461	40.3910200	fe80::e8bc:49:3935:ff02::1:3		LLMNR	85	Standard query 0x09f6 A BSCIT
462	40.3918150	192.168.0.117	224.0.0.252	LLMNR	65	Standard query 0x09f6 A BSCIT
463	40.3928330	fe80::e8bc:49:3935:ff02::1:3		LLMNR	85	Standard query 0x8a27 AAAA BSCIT
464	40.48031900	D_LinkIn_34:08:20	spanning-tree-(for STP)	60	Conf. Root = 32:68/0:c8:d3:a3:08:20 Cost = 0 Port = 0x8001	
465	40.4916270	fe80::e8bc:49:3935:ff02::1:3		LLMNR	85	Standard query 0xb69b A BSCIT
466	40.4920290	192.168.0.117	224.0.0.252	LLMNR	65	Standard query 0xb69b A BSCIT
467	40.4926110	fe80::e8bc:49:3935:ff02::1:3		LLMNR	85	Standard query 0x14b4 AAAA BSCIT
468	40.7280570	fe80::b0be:5fac:9b0ff02::c		SSDP	208	M-SEARCH * HTTP/1.1

Frame 444: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface 0

Ethernet II, Src: IntelCor\_63:05:47 (00:1c:06:63:05:47), Dst: IPv6mcast\_00:01:00:03 (33:33:00:01:00:03)

Internet Protocol Version 6, Src: fe80::e8bc:49:3935:5b1, Dst: ff02::1:3 (ff02::1:3)

User Datagram Protocol, Src Port: 56398 (56398), Dst Port: 111mnr (5355)

Link-local Multicast Name Resolution (query)

0000	33 33 00 01 00 03 00 1c	c0 63 05 47 86 dd 60 00	33..... .C.G. .`
0010	00 00 00 01 ff 11 01 fe 80	00 00 00 00 00 00 00 e8 bc	.095.....
0020	00 40 39 35 e5 b1 ff 02	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 .1..M
0030	00 00 01 03 03 ff 76 14	eb 00 00 1f 70 b1 c5 4d	00 00 00 00 00 00 00 00 ..V .. ..M
0040	00 00 00 01 00 00 00 00	00 00 03 42 53 43 49 54	00 00 00 00 00 00 00 00 ..BSCIT

Local Area Connection: <live capture in prog> Packets: 468 - Displayed: 468 (100.0%) Profile: Default

#### Step 4: Filter packets with HTTP protocol.

Capturing from Local Area Connection [Wireshark 1.10.8 (v1.10.8-2-g52a5244 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
12	0.93332800	192.168.0.119	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
48	3.9.93357800	192.168.0.119	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
57	4.66167600	fe80::b0be:5fac:9b0ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
86	6.96468800	192.168.0.119	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
88	7.67220600	fe80::b0be:5fac:9b0ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
123	9.9.96507800	192.168.0.119	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
127	10.6829250	fe80::b0be:5fac:9b0ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
155	12.9.9652840	192.168.0.119	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
173	14.6766920	fe80::b0be:5fac:9b0ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
199	17.6875770	fe80::b0be:5fac:9b0ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
225	20.6979590	fe80::b0be:5fac:9b0ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
281	24.6917610	fe80::b0be:5fac:9b0ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
337	27.7030080	fe80::b0be:5fac:9b0ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
367	30.7130110	fe80::b0be:5fac:9b0ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
307	31.7067260	fe80::b0be:5fac:9b0ff02::c		SSDP	208	M-SEARCH * HTTP/1.1

Frame 432: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits) on interface 0

Ethernet II, Src: IntelCor\_33:8:e:b0 (00:1c:03:8:e:b0), Dst: IPv6mcast\_00:00:00:00:00:0c (33:33:00:00:00:0c)

Internet Protocol Version 6, Src: fe80::b0be:5fac:9b0:9372, Dst: ff02::c (ff02::c)

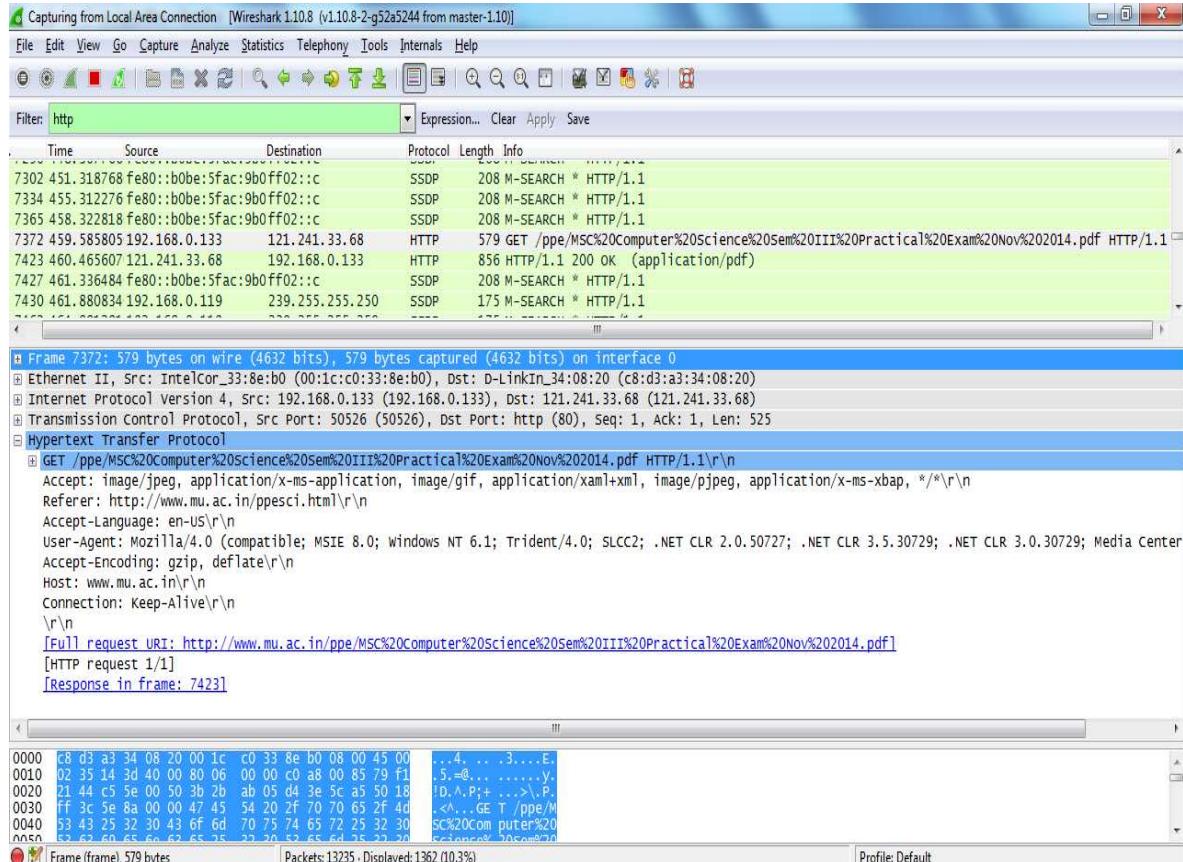
User Datagram Protocol, Src Port: 57114 (57114), Dst Port: ssdp (1900)

Hypertext Transfer Protocol

0000	33 33 00 00 00 0c 00 1c	c0 33 8e b0 86 dd 60 00	33..... .3....`
0010	00 00 00 9a 11 01 fe 80	00 00 00 00 00 00 00 b0 be	..... .....
0020	5f ac 09 b0 93 72 ff 02	00 00 00 00 00 00 00 00	.....f.. .....
0030	00 00 00 00 00 0c df 1a	07 6c 00 9a 0a b7 4d 2d	..... .7...M
0040	53 45 41 52 43 48 20 2a	20 48 54 54 50 2f 31 2e	SEARCH * HTTP/1.
0050	31 0d 0a 48 6f 73 74 3a	5b 46 46 30 32 3a 3a 43	1. Host: [FF02::C]
0060	5d 3a 31 39 30 30 0d 0a	53 54 3a 75 72 6e 3a 4d	]1900. ST:urn:M
0070	69 63 72 6f 73 6f 66 74	20 57 69 6e 64 6f 77 73	icrosoft Windows
0080	20 50 65 65 72 20 4e 61	6d 65 20 52 65 73 6f 6c	Peer Na Me Resol
0090	7c 71 60 65 6c 6c 60 77	6d 71 65 63 6c 6c 60 77	..... .....

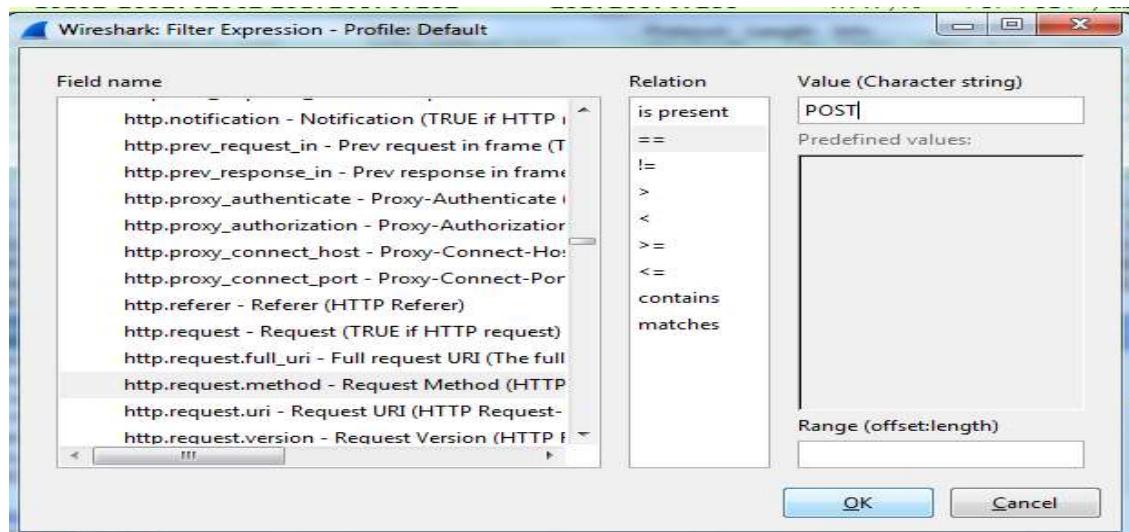
Local Area Connection: <live capture in prog> Packets: 3565 - Displayed: 251 (7.0%) Profile: Default

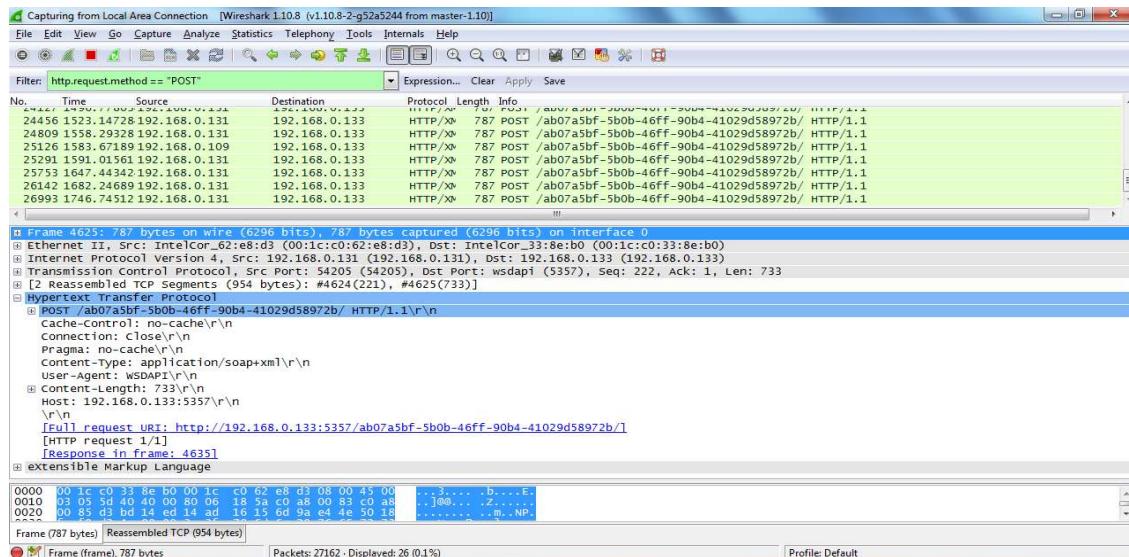
**Step 5:** A file with only text: [http://www.mu.ac.in/ppe/LIBRARY%20SCIENCE-\(SEM.I\)-SH-2014.pdf](http://www.mu.ac.in/ppe/LIBRARY%20SCIENCE-(SEM.I)-SH-2014.pdf)



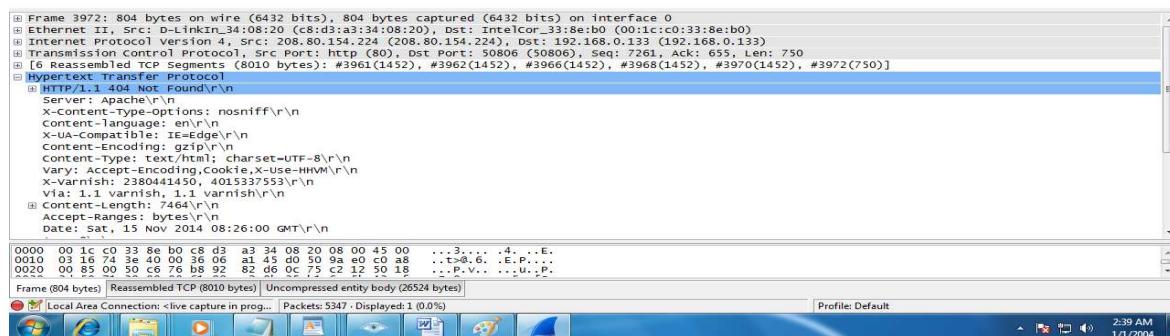
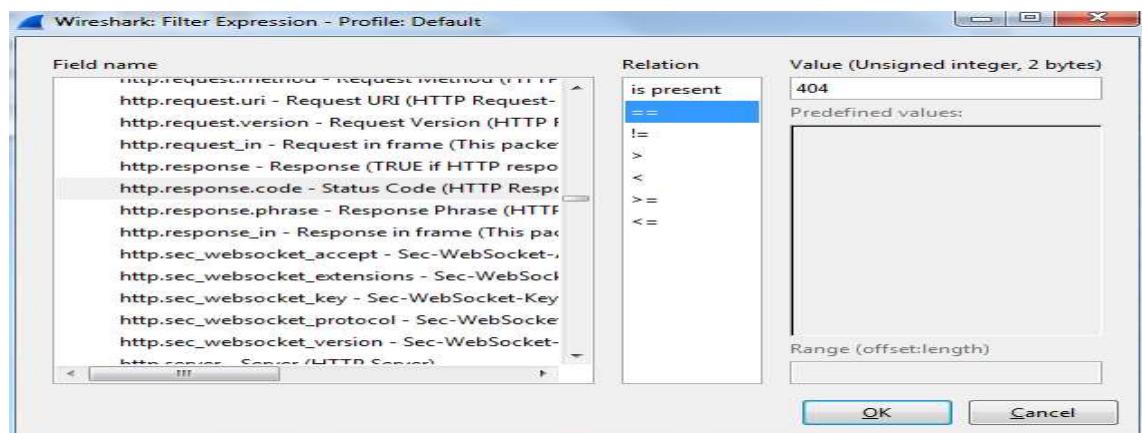
**Step 6:** Applying different filters using expressions.

1) Filtering HTTP POST request

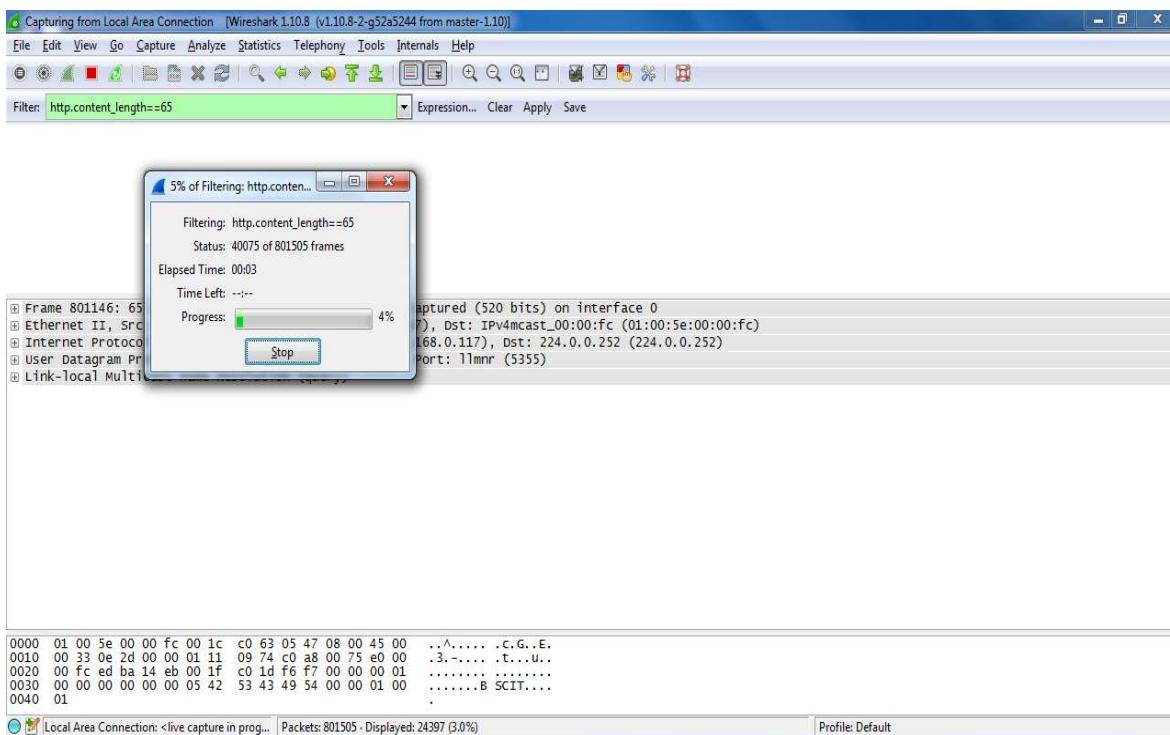
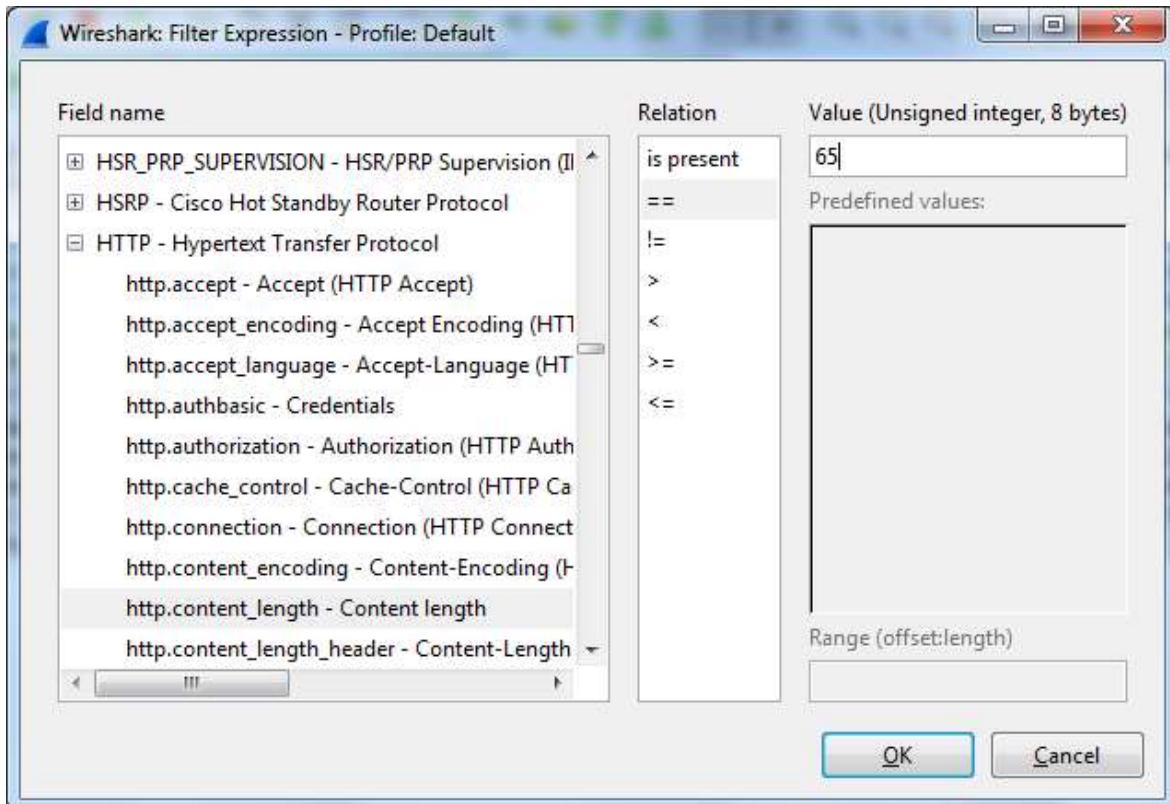




## 2) Filtering 404 not found error



### 3) Filtering using HTTP Content Length

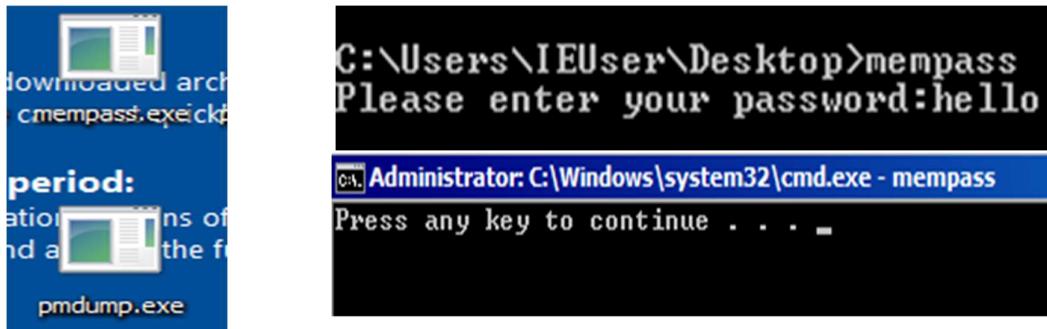


## PRACTICAL NO. 06

### 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.

Let start the mempass



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

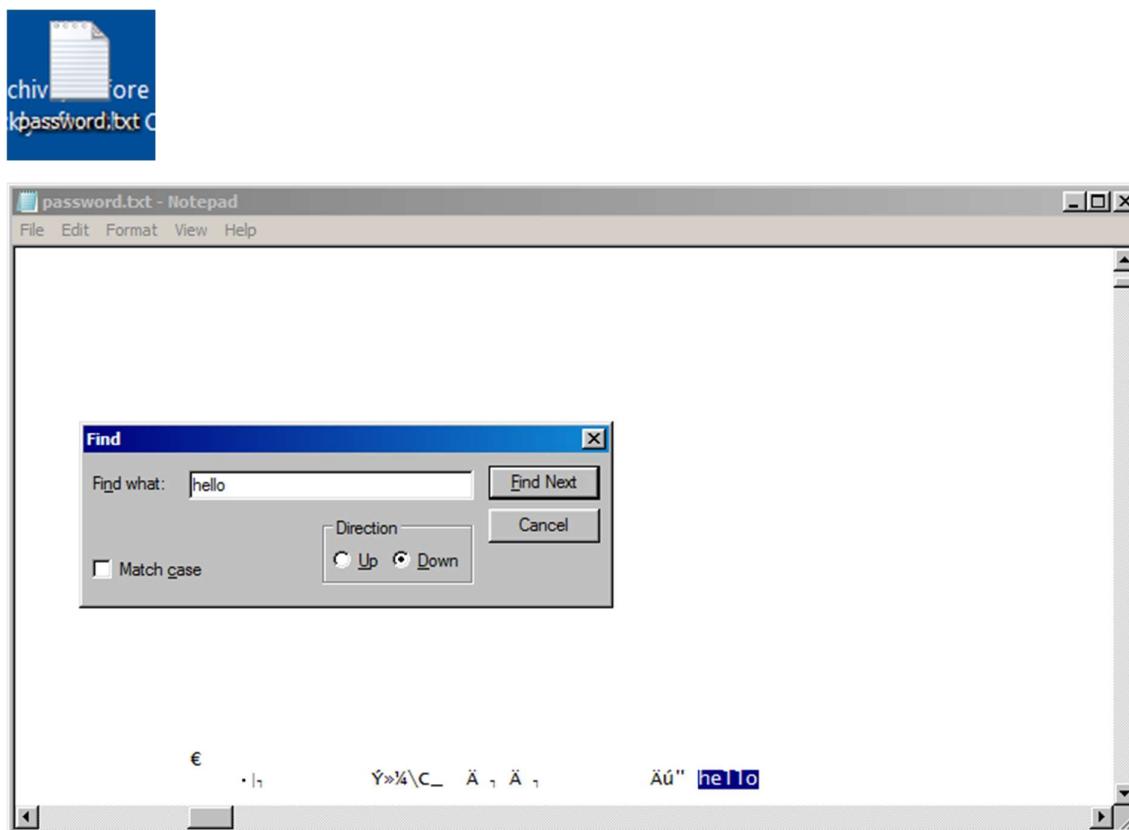
C:\Users\IEUser\Desktop>pmdump -list
pmdump 1.2 - <c> 2002, Arne Vidstrom <arne.vidstrom@ntsecurity.nu>
0 - System idle process
4 - System
252 - smss.exe
328 - csrss.exe
364 - csrss.exe
372 - wininit.exe
400 - winlogon.exe
460 - services.exe
468 - lsass.exe
476 - lsm.exe
568 - svchost.exe
624 - UBoxService.exe
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 - UBoxTray.exe
3560 - wuauctl.exe
3104 - cmd.exe
2700 - conhost.exe
3808 - cmd.exe
1992 - conhost.exe
```

```
3198 - connect.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

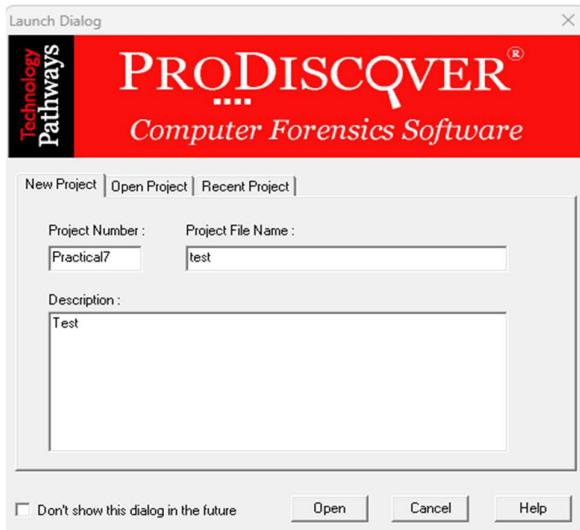


In this way, we can retrieve passwords from applications which store them in memory without any form of encryption.

## PRACTICAL NO. 07

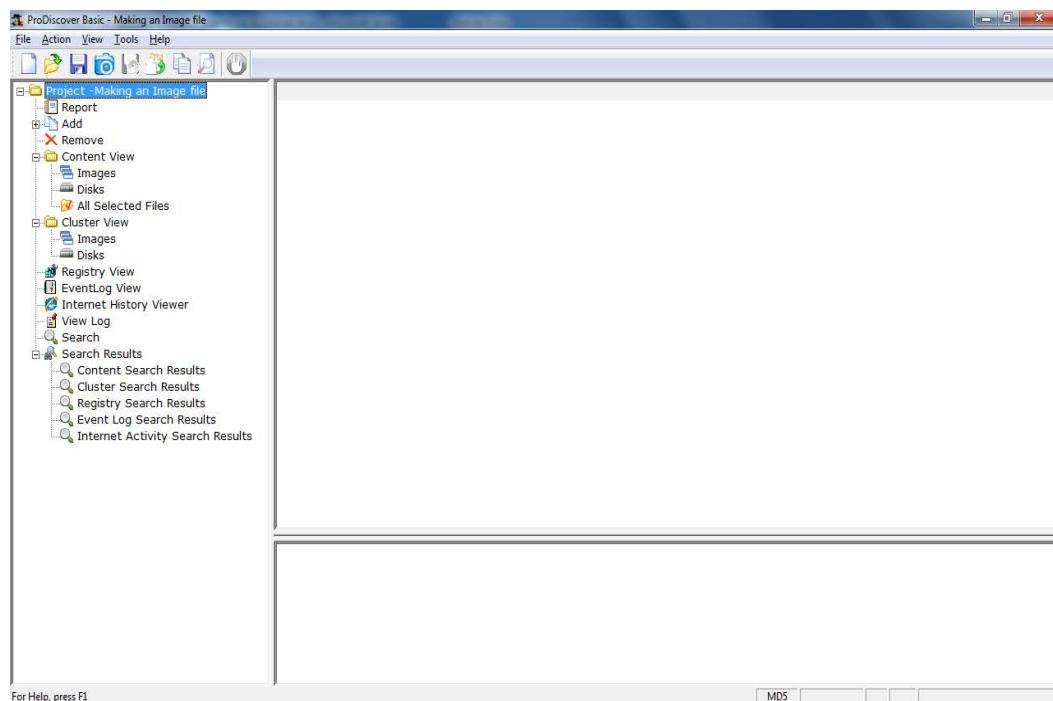
### Using Data Acquisition Tools [ProDiscover Pro]

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



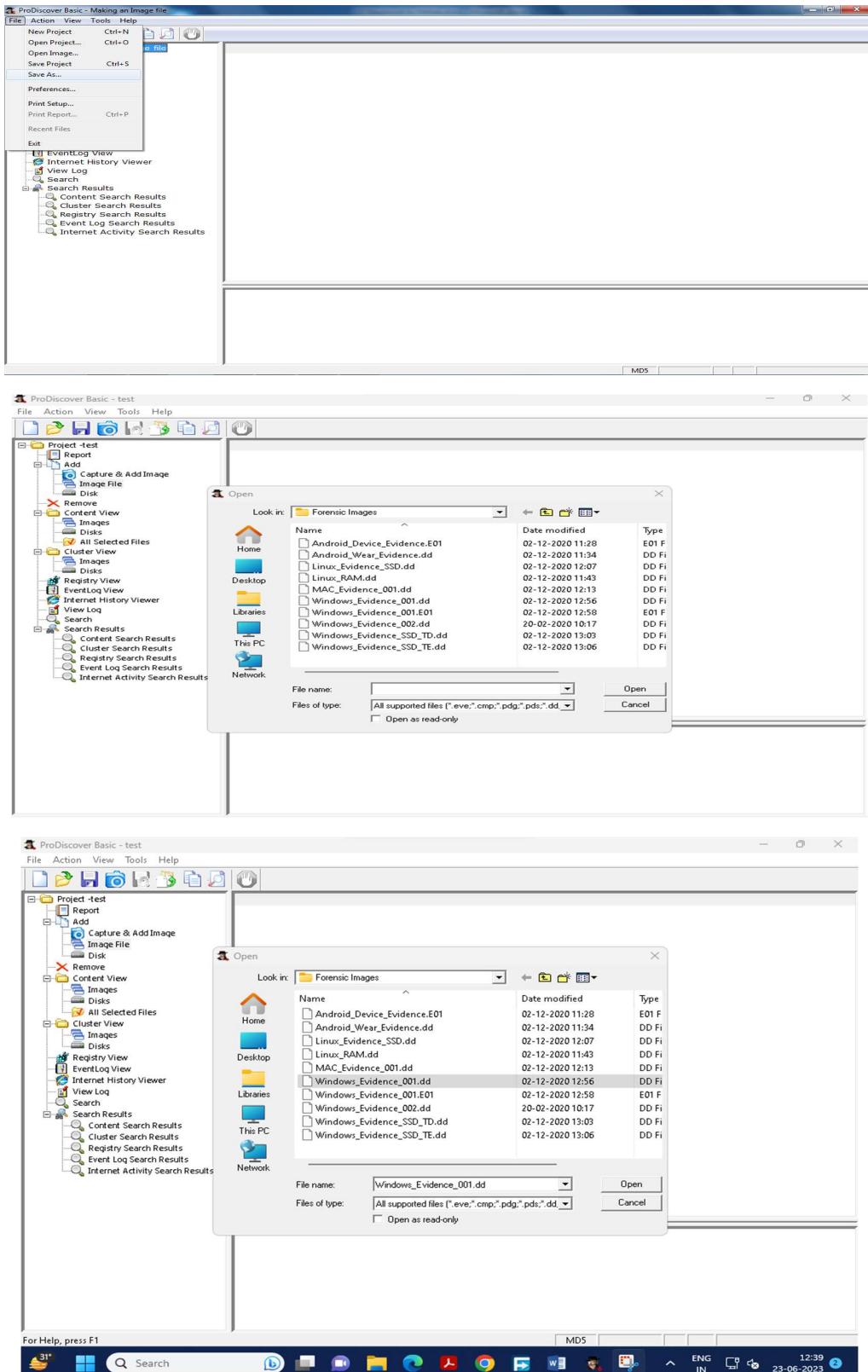
Step 2) Enter a project number, project name, and description of the project in the new project tab option, and then click the Open button.

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.

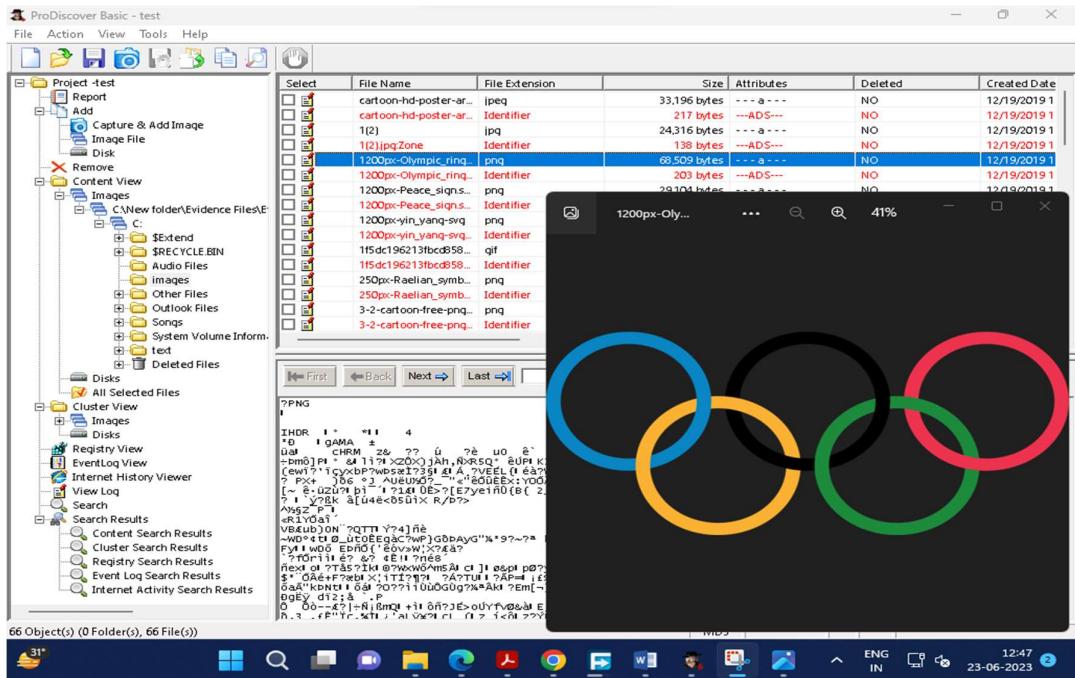


Step 4) ProDiscover displays the contents of the selected file at the bottom of the main window. Right click on a file.

Select	File Name	File Extension	Size	Attributes	Deleted	Created Date
	cartoon-hd-poster-ar...	ipaq	33,196 bytes	--- a---	NO	12/19/2019 1
	cartoon-hd-poster-ar...	Identifier	217 bytes	---ADS---	NO	12/19/2019 1
	1(2)	ipq	24,316 bytes	--- a---	NO	12/19/2019 1
	1(2).jpg.Zone	Identifier	138 bytes	---ADS---	NO	12/19/2019 1
	1200px-Olympic_ring_...	png	68,509 bytes	--- a---	NO	12/19/2019 1
	1200px-Olympic_ring_...	Identifier	203 bytes	---ADS---	NO	12/19/2019 1
	1200px-Peace_signs_...	png	29,104 bytes	--- a---	NO	12/19/2019 1
	1200px-Peace_signs_...	Identifier	171 bytes	---ADS---	NO	12/19/2019 1
	1200px-ylin_yang-svq...	png	10,081 bytes	--- a---	NO	12/19/2019 1
	1200px-ylin_yang-svq...	Identifier	163 bytes	---ADS---	NO	12/19/2019 1
	1f5dc196213fbcd58...	gif	104,805 bytes	--- a---	NO	12/19/2019 1
	1f5dc196213fbcd58...	Identifier	149 bytes	---ADS---	NO	12/19/2019 1
	250px-Raelian_symb...	png	5,528 bytes	--- a---	NO	12/19/2019 1
	250px-Raelian_symb...	Identifier	178 bytes	---ADS---	NO	12/19/2019 1
	3-2-cartoon-free-pnq...	png	28,391 bytes	--- a---	NO	12/19/2019 1
	3-2-cartoon-free-pnq...	Identifier	150 bytes	---ADS---	NO	12/19/2019 1

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

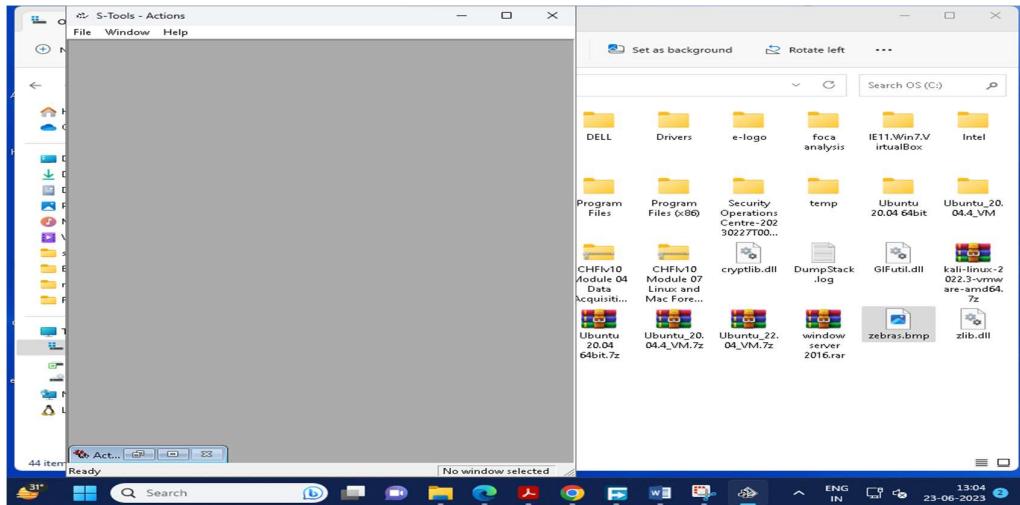


## **PRACTICAL NO. 08**

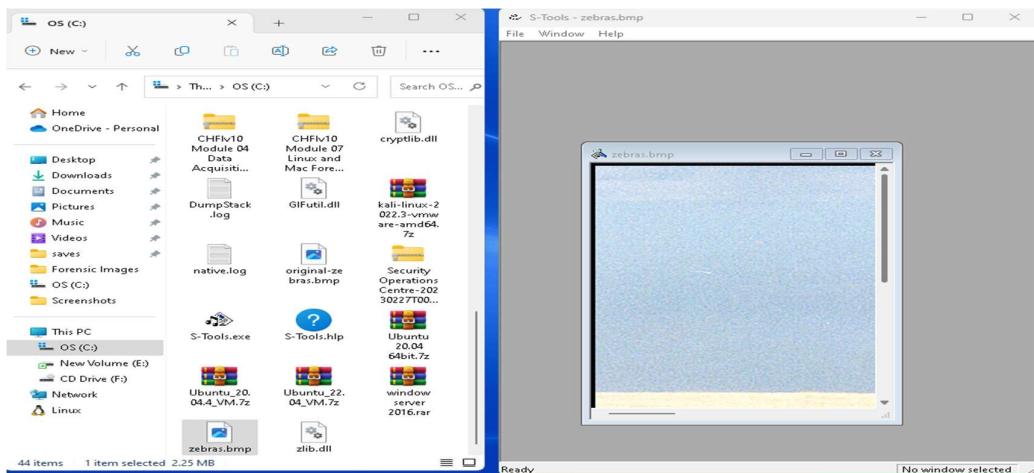
### **a. Using Steganography Tools [S-Tools]**

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

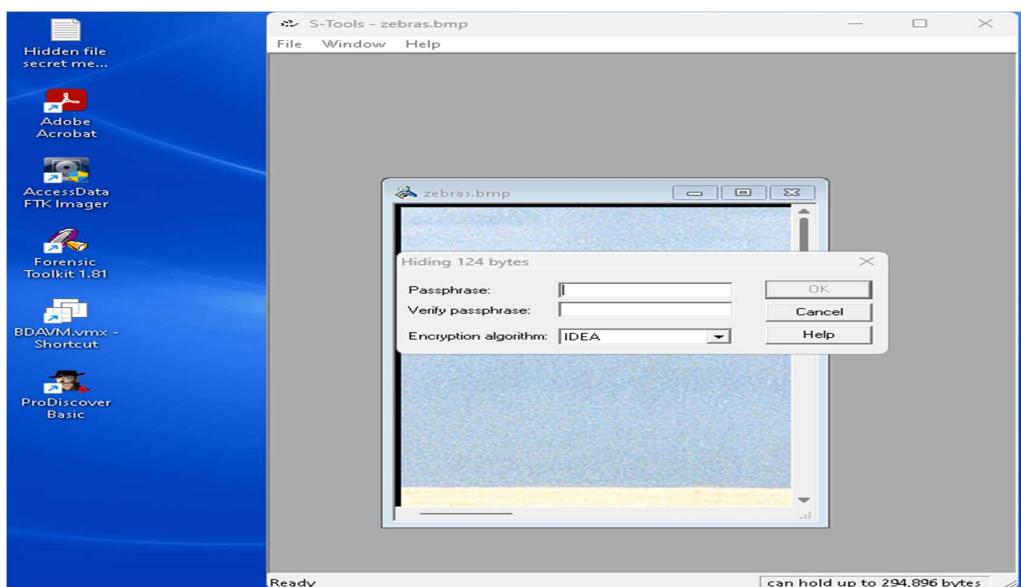
If your image is in .jpg format, convert it to .bmp format.

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

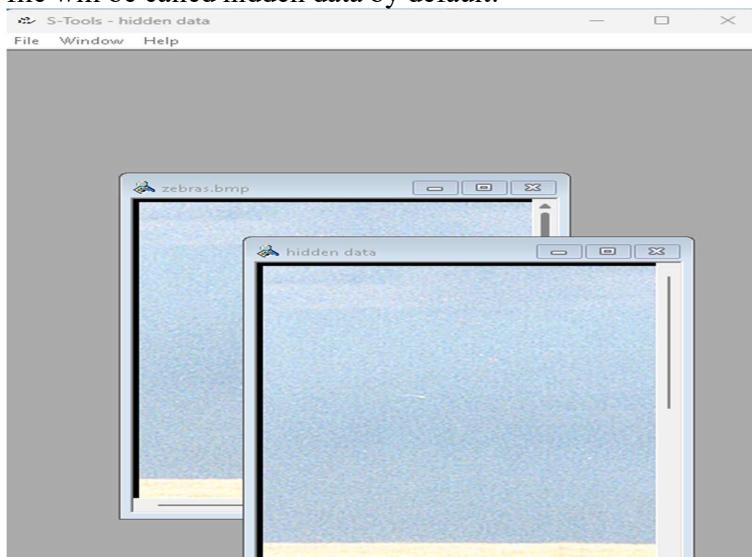
Step 5) The \*.txt text file is selected and dragged on top of the base image. Release the file while the cursor is still on top of the base file.

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.



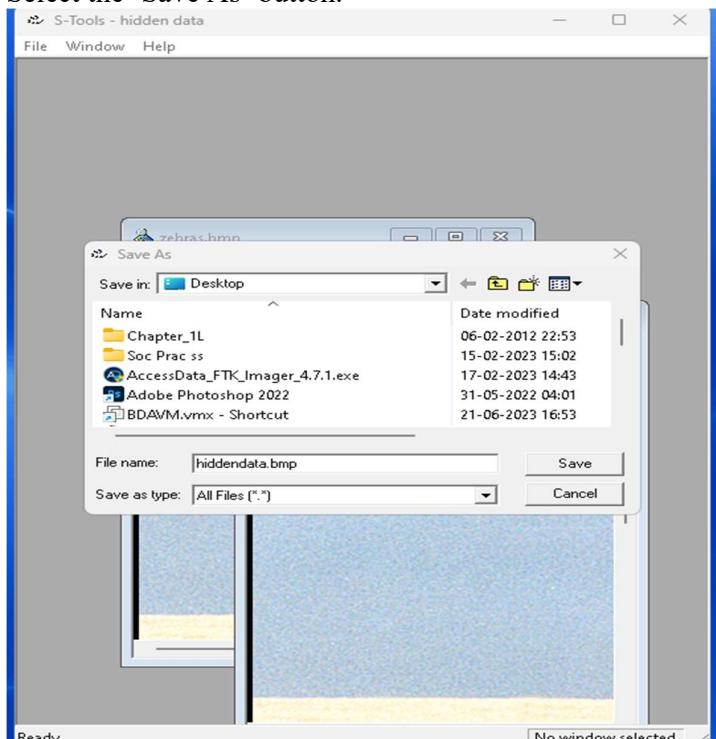
Step 8) The S-Tools main window will appear and a new file will be visible. The name of the file will be called hidden data by default.



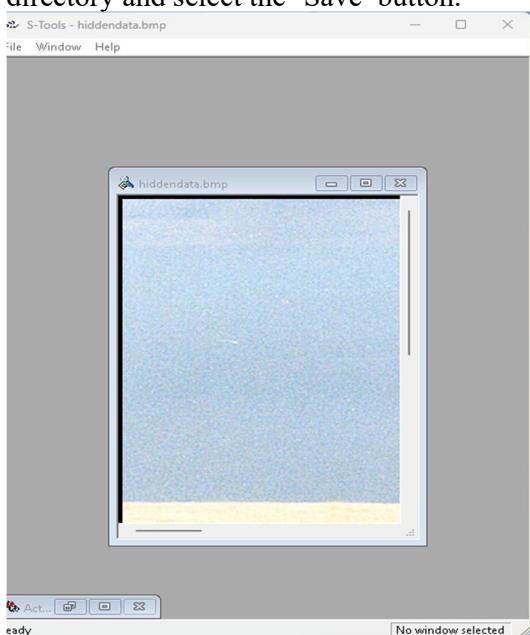
Step 9) Place the cursor on top of the hidden data image and select the right mouse button.  
The user will  
have four options available to them:

- Save
- Save As
- Properties
- Reveal

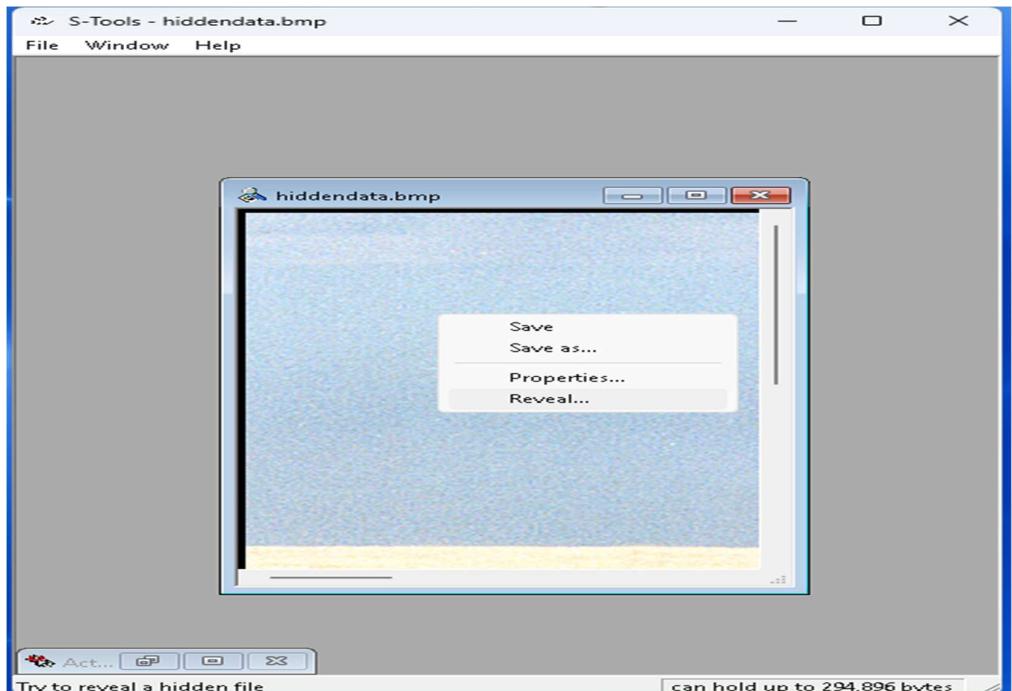
Select the ‘Save As’ button.



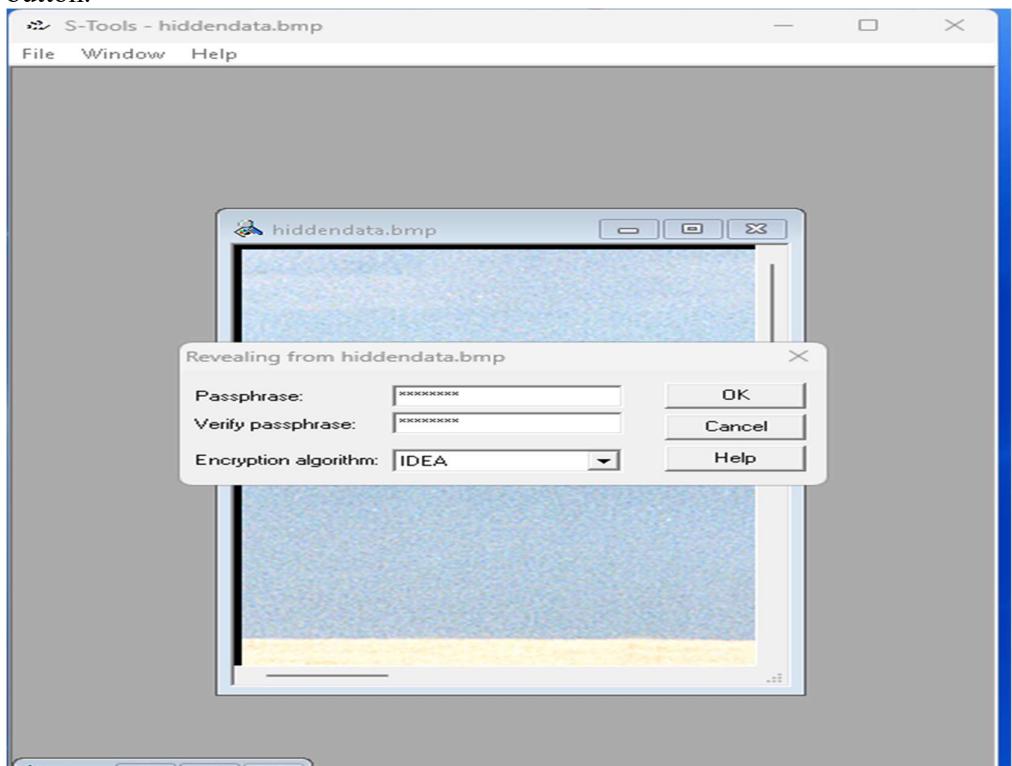
Step 10) A ‘Save As’ dialogue box will appear. Enter a valid file name, select the working directory and select the ‘Save’ button.



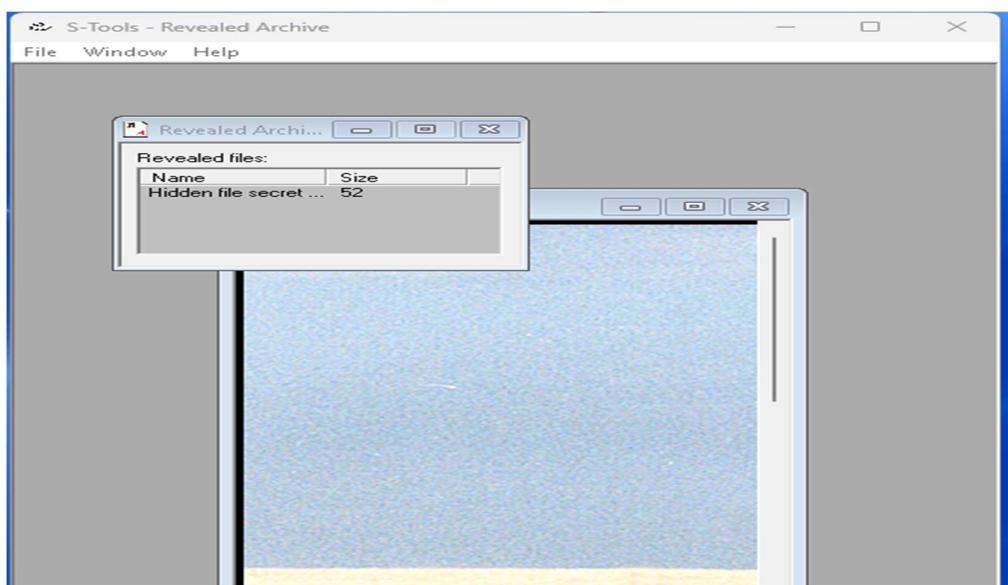
Step 11) Selecting the ‘Reveal’ button will display a passphrase dialogue box. A passphrase must be entered twice in the dialogue box and the correct encryption algorithm must be selected.



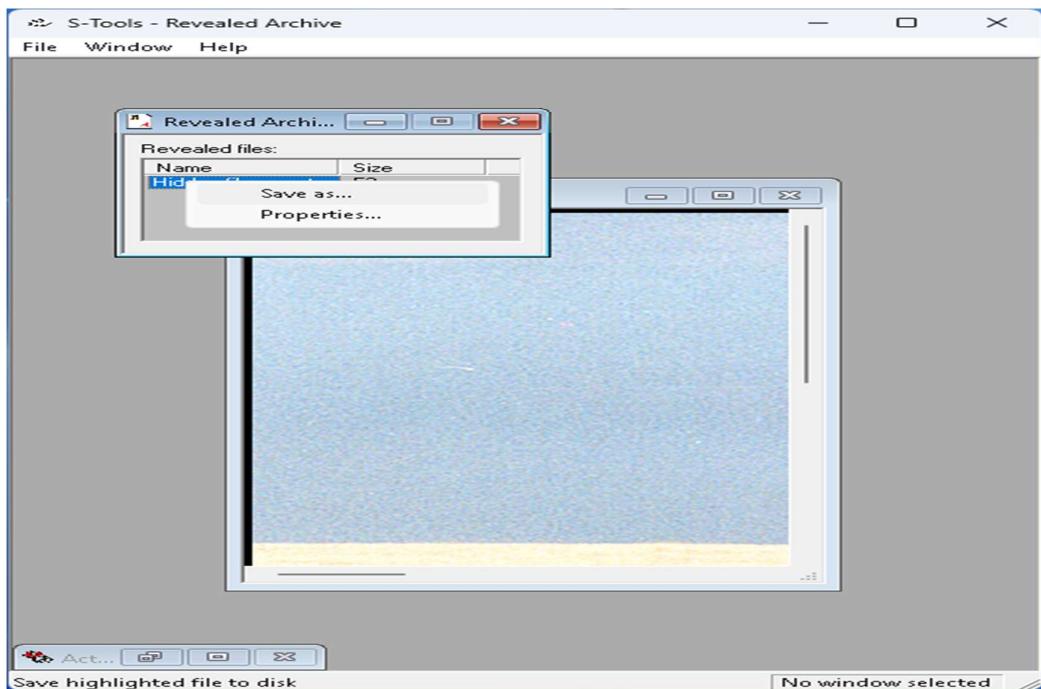
Step 12) Enter a passphrase twice, select the encryption algorithm, and select the ‘OK’ button.



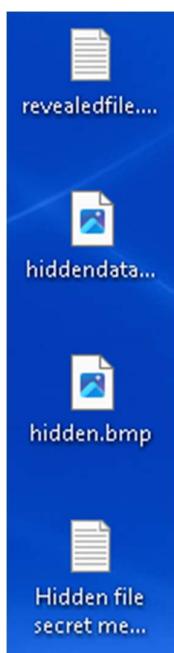
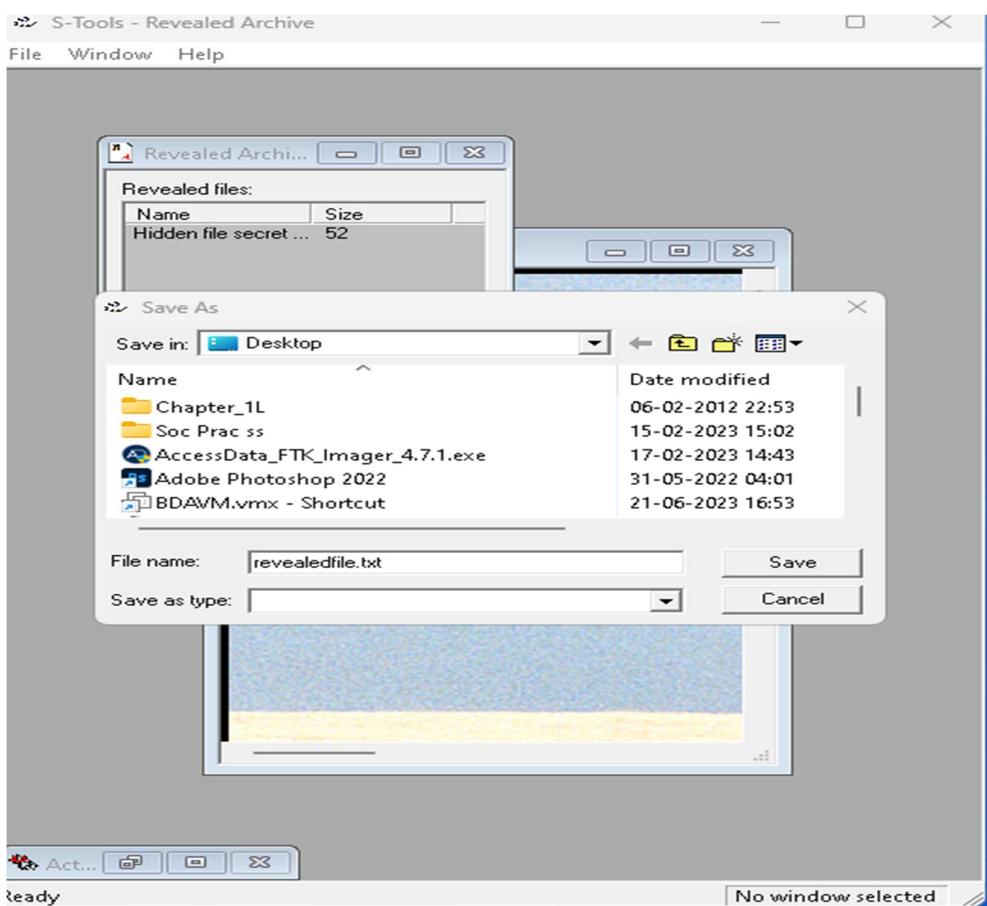
Step 13) A ‘Revealed Archive’ dialogue box will display which contains the file name and size of the hidden file.



Step 14) Select the ‘Save As’ button.



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



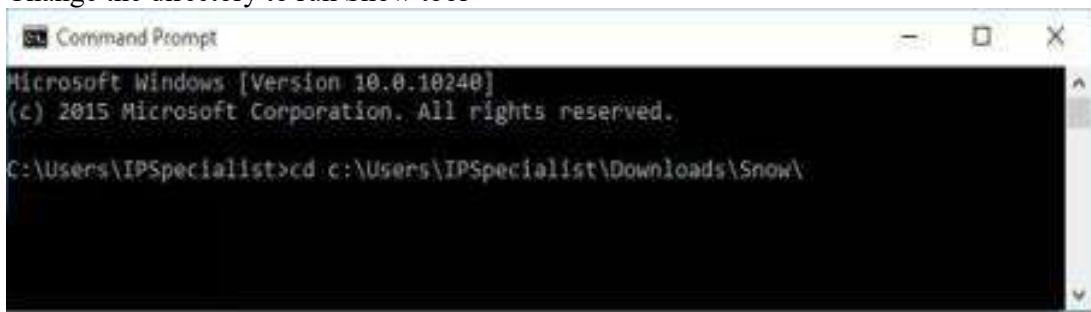
## b. Using Whitespace Stegnography tool SNOW

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



Step 2) Go to Command Prompt

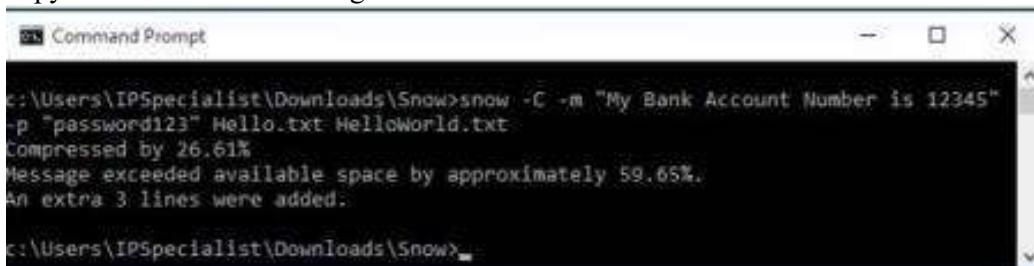
Change the directory to run Snow tool



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 find a new file **HelloWorld.txt**. Open the File



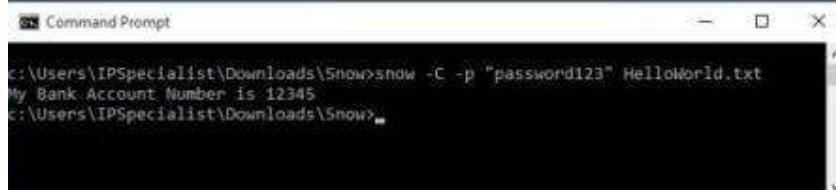
Step 4) New File has the same text as an original file without any hidden information.

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**



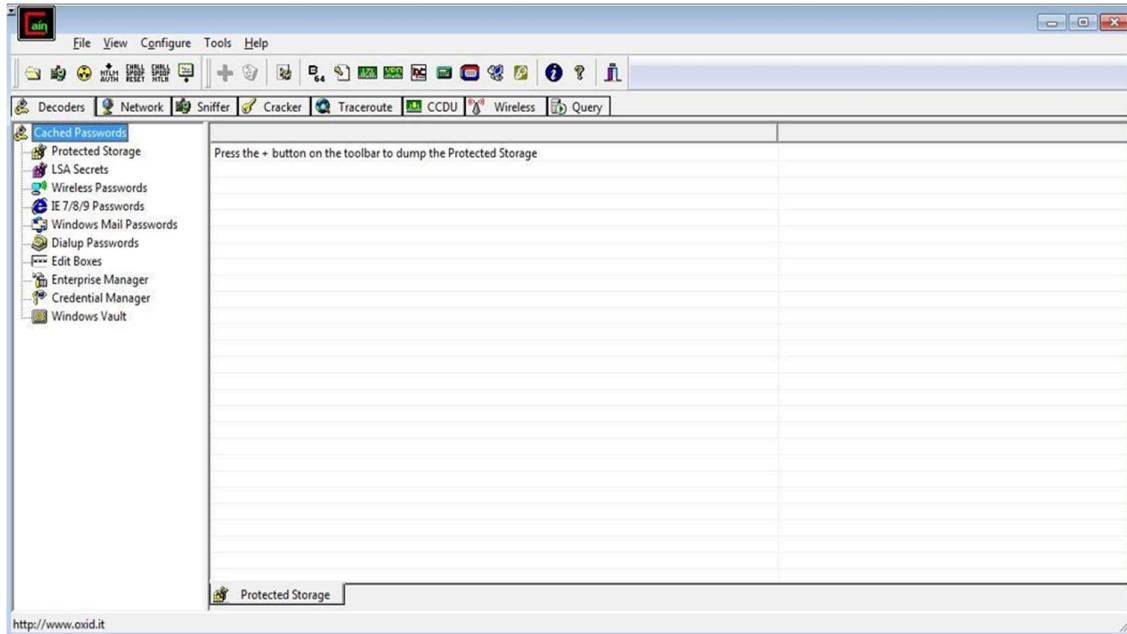
```
c:\Users\IPSpecialist\Downloads\Snow>Snow -C -p "password123" HelloWorld.txt
My Bank Account Number is 12345
c:\Users\IPSpecialist\Downloads\Snow>
```

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

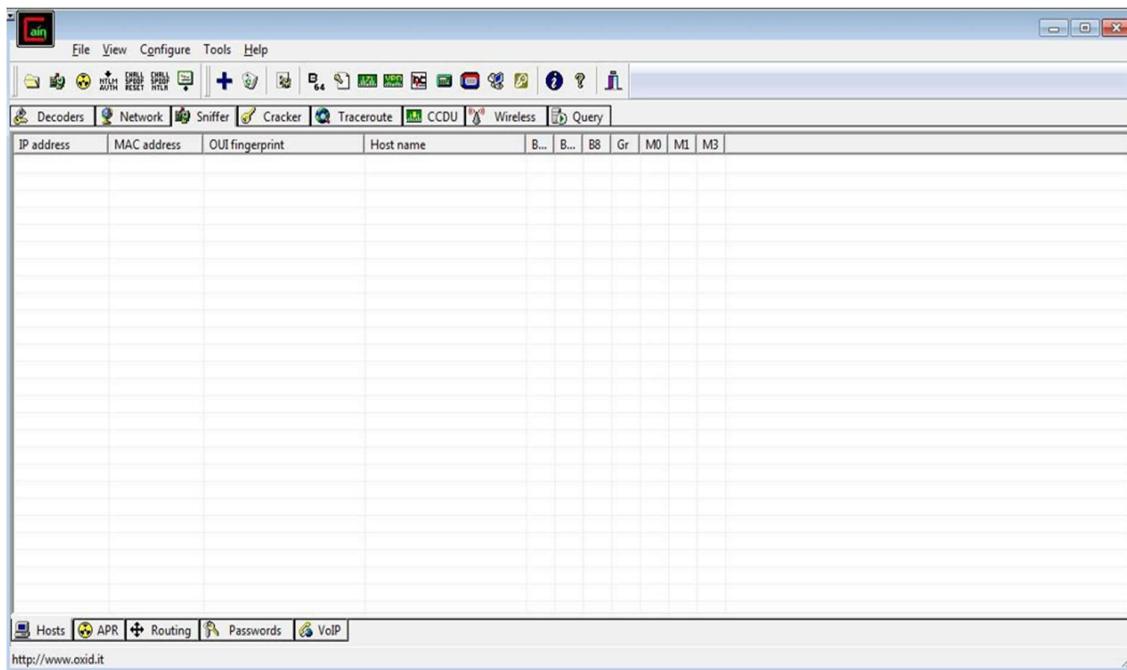
## **PRACTICAL NO. 09**

### a. **Performing Password Cracking [Cain & Abel]**

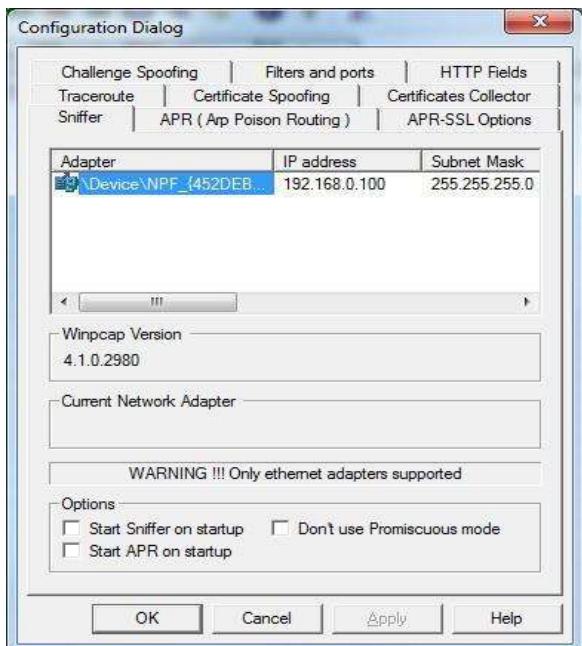
Step 1: Install and open cain and abel.



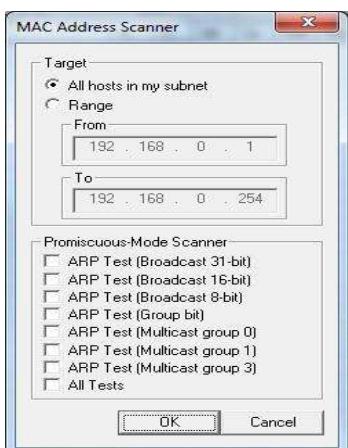
Step 2: Select sniffer on the top.



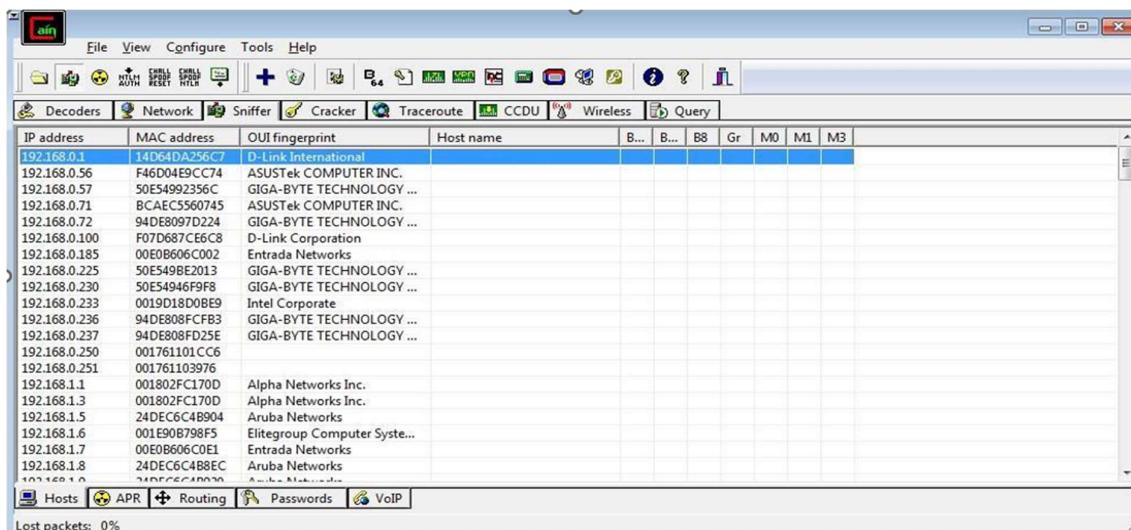
Step 3: Next to folder icon click on icon name start/stop sniffer. Select device and click on ok.



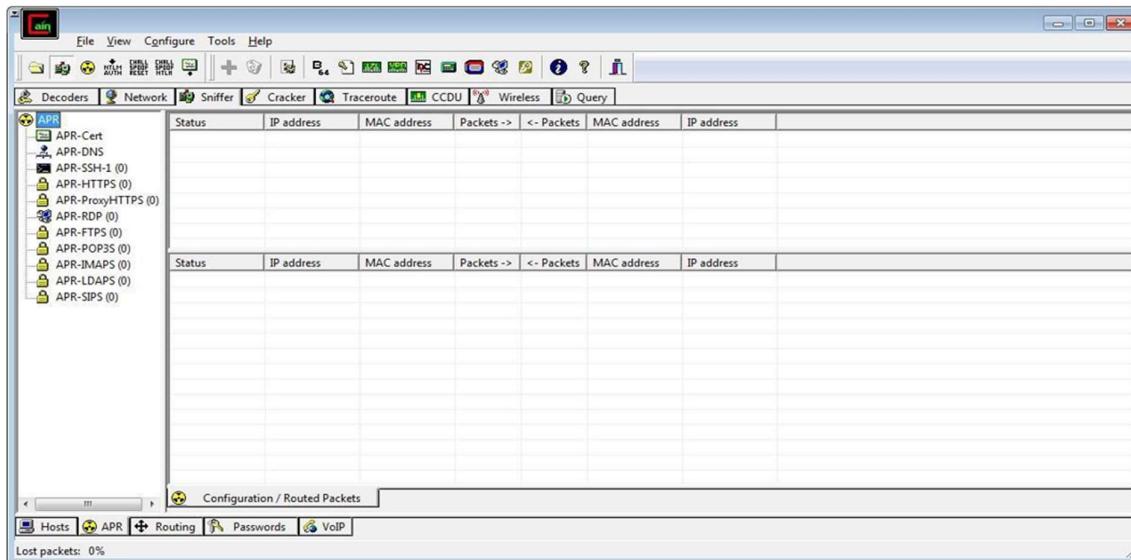
Step 4: Click on “+” icon on the top. Click on ok.



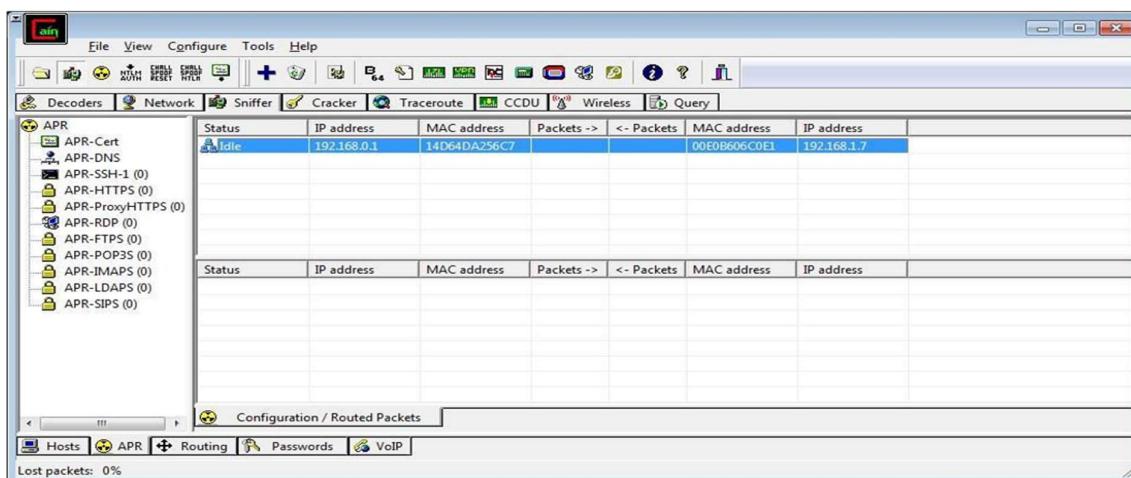
Step 5: Shows the Connected host.



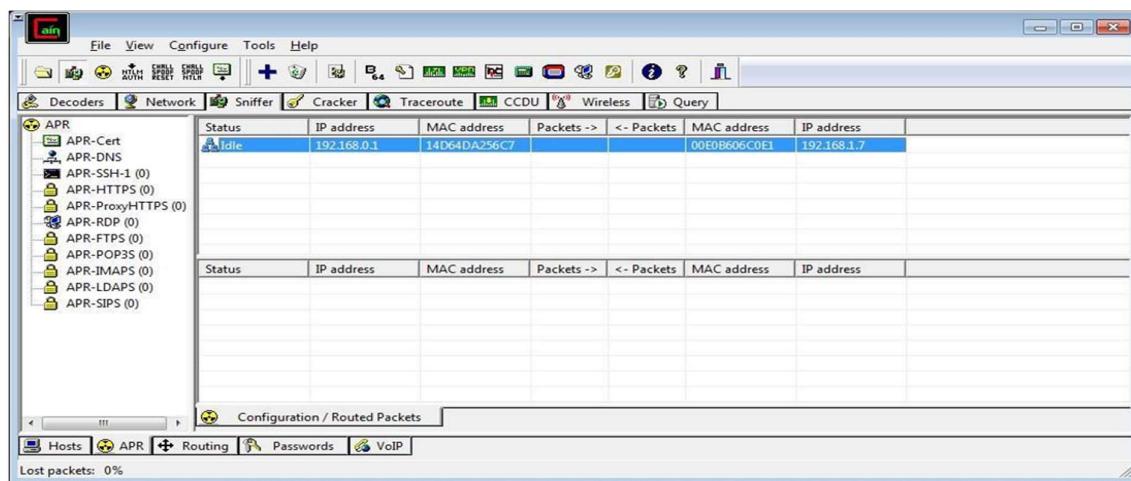
Step 6: Select Arp at bottom.



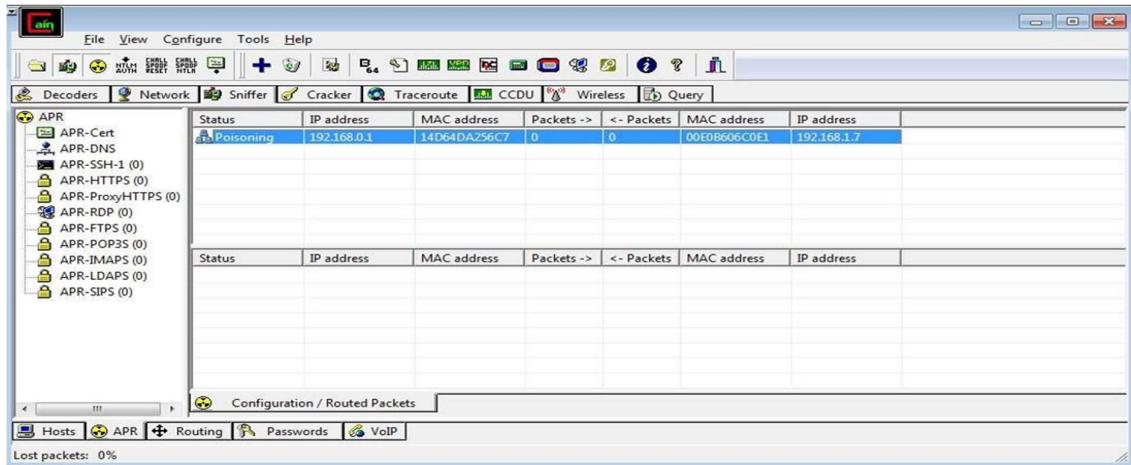
Step 7: Click on “+” icon at the top.



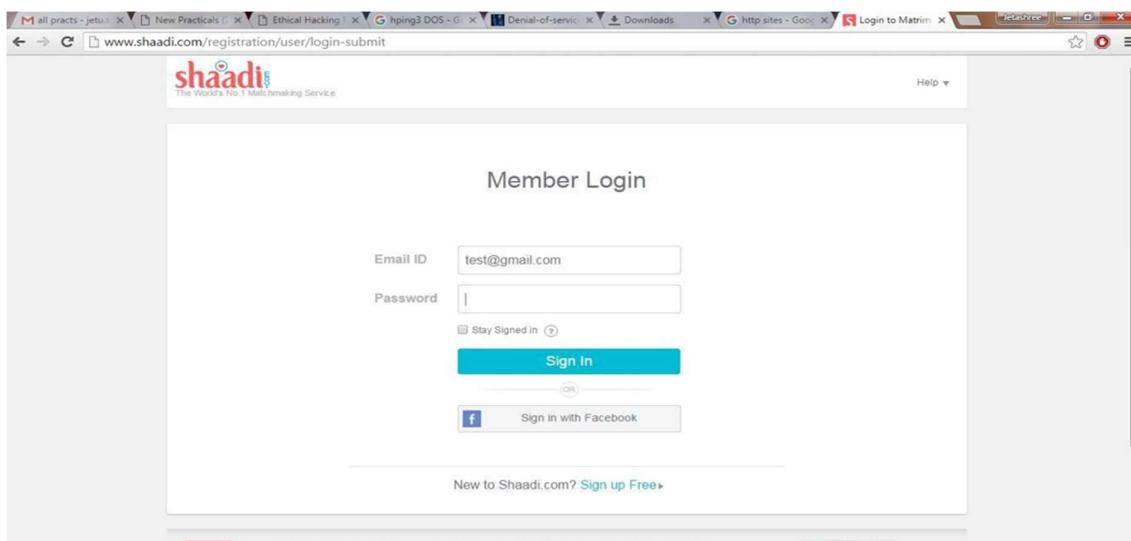
Step 8: Click on start/stop ARP icon on top.



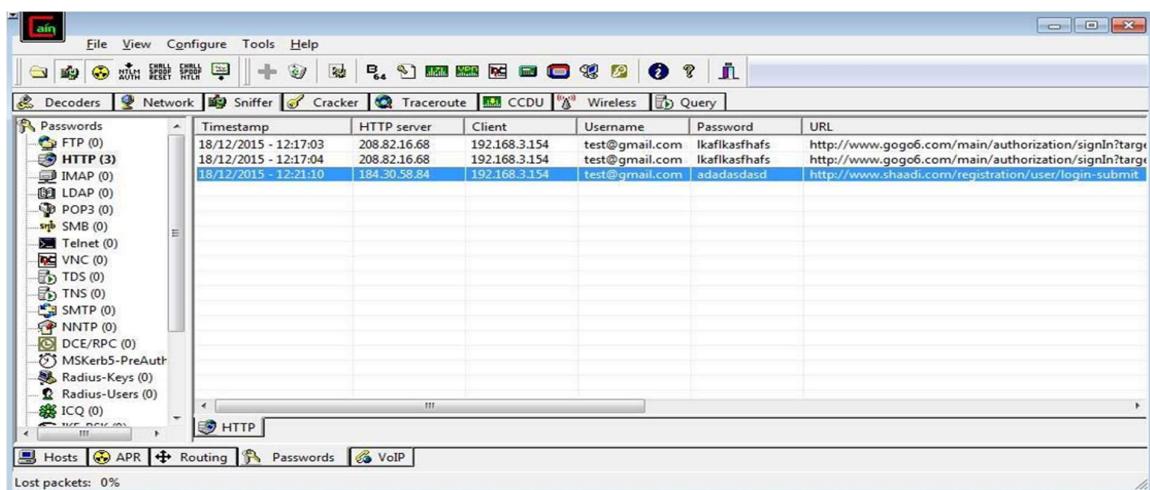
### Step 9: Poisoning the source.



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



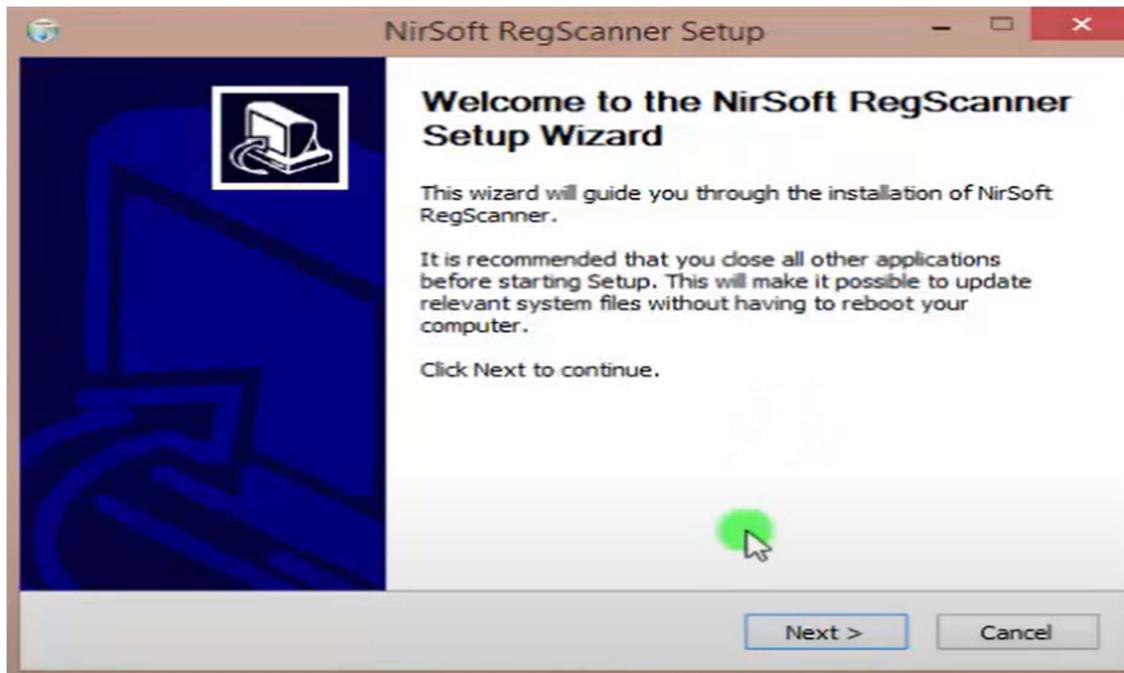
### Step 11: Go to password option in the Cain & Abel and see the visited site password



## **PRACTICAL NO. 10**

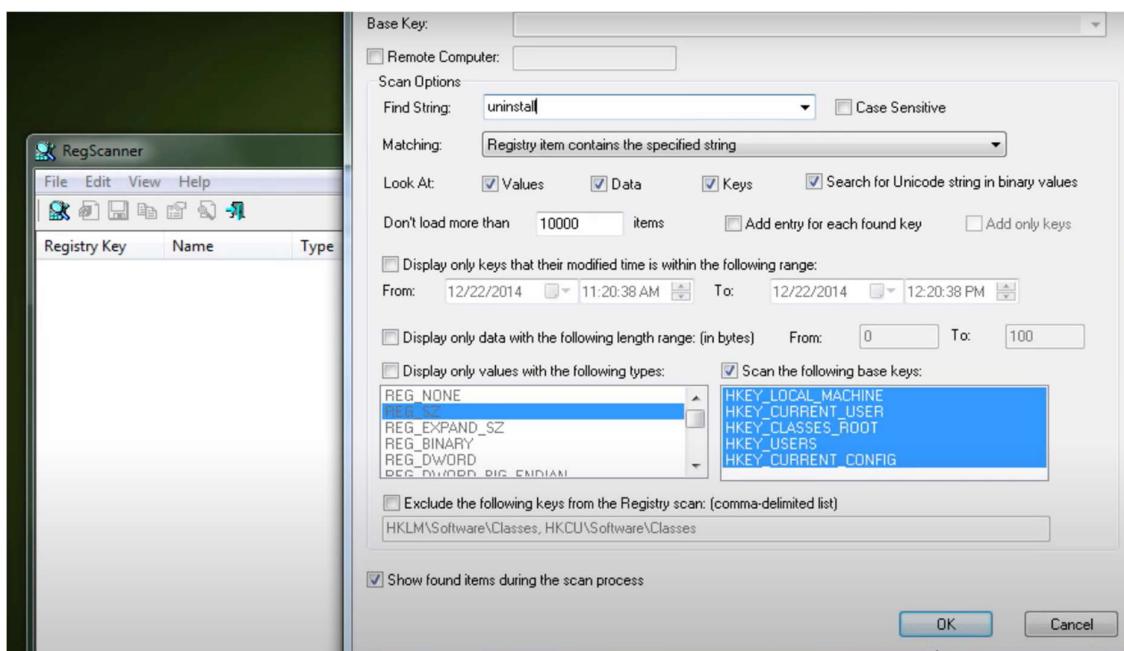
### **a. Scan Registry using RegScanner**

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

RegScanner: uninstall

Stop

Registry Key	Name	Type	Data	Key Modified ...	Data Length
HKLM\SOFT...	Uninstall Action	REG_DWORD	0x776f6378 (20...)	5/22/2014 7:53:...	4
HKLM\SOFT...	UninstallMan...	REG_SZ	AVG Uninstall ...	9/30/2014 2:00:...	110
HKLM\SOFT...	UninstallCmdL...	REG_SZ	"C:\Program Fi...	12/22/2014 12:...	67
HKLM\SOFT...	UninstallString	REG_SZ	C:\Program Fil...	12/22/2014 8:2...	82
HKLM\SOFT...	UninstallArgu...	REG_SZ	--uninstall --...	12/22/2014 8:2...	44
HKLM\SOFT...	UninstallString	REG_SZ	C:\Program Fil...	12/22/2014 8:2...	82
HKLM\SOFT...	UninstallArgu...	REG_SZ	--uninstall --...	12/22/2014 8:2...	53
HKLM\SOFT...	UninstallerFree	REG_SZ	C:\Program Fil...	11/5/2014 9:54:...	48
HKLM\SOFT...	upgrade	REG_SZ	Yes	11/5/2014 9:54:...	4
HKLM\SOFT...	UninstallerPath	REG_SZ	C:\Windows\S...	12/10/2014 9:5...	70
HKLM\SOFT...	UninstallerPath	REG_SZ	C:\Windows\S...	12/10/2014 10:...	69
HKLM\SOFT...		REG_SZ	AvoidKeyDelete...	7/14/2009 8:49:...	33
HKLM\SOFT...	EnableFileTraci...	REG_DWORD	0x00000000 (0)	6/26/2014 2:31:...	4
HKLM\SOFT...	EnableConsole...	REG_DWORD	0x00000000 (0)	6/26/2014 2:31:...	4
HKLM\SOFT...	FileTracingMask	REG_DWORD	0xffff0000 (429...	6/26/2014 2:31:...	4
HKLM\SOFT...	ConsoleTracin...	REG_DWORD	0xffff0000 (429...	6/26/2014 2:31:...	4
HKLM\SOFT...	MaxFileSize	REG_DWORD	0x00100000 (10...	6/26/2014 2:31:...	4
HKLM\SOFT...	FileDialog...	REG_EXPAND_...	%windir%\trac...	6/26/2014 2:31:...	17

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

HKCR\hxk\...	REG_SZ	Shared key to keep thi...	5/14/2014 3:50:45 PM	94
HKCR\hxq\...	REG_SZ	Shared key to keep thi...	5/14/2014 3:50:45 PM	94
HKCR\hxr\...	REG_SZ	Shared key to keep thi...	5/14/2014 3:50:45 PM	94
HKCR\hxS\...	REG_SZ	Shared key to keep thi...	5/14/2014 3:50:45 PM	94
HKCR\hxt\...	REG_SZ	Shared key to keep thi...	5/14/2014 3:50:45 PM	94
HKCR\hxv\...	REG_SZ	Shared key to keep thi...	5/14/2014 3:50:45 PM	94
HKCR\hxw\...	REG_SZ	Shared key to keep thi...	5/14/2014 3:50:45 PM	94
HKCR\Avast... InstupProgress...			1:36:39 PM	25
HKCR\CLSID...		Export Selected Items	Ctrl+E	3:53:38 AM
HKCR\CLSID...		Delete Selected Keys/Values	Ctrl+Del	3:54:30 AM
HKCR\CLSID...		Save Selected Items	Ctrl+S	3:54:30 AM
HKCR\CLSID...		Copy Selected Items	Ctrl+C	3:53:38 AM
HKCR\CLSID...		Copy Key	Ctrl+K	7:43:18 AM
HKCR\CLSID... Uninstall Config...		HTML Report - All Items		7:43:18 AM
HKCR\CLSID... Uninstall Config...		HTML Report - Selected Items		7:43:38 AM
HKCR\CLSID... Uninstall Config...		Choose Columns		7:43:38 AM
HKCR\CLSID... Uninstall Config...		Auto Size Columns	Ctrl+Plus	7:43:44 AM
HKCR\CLSID...		Open In RegEdit	F8	3:53:38 AM
HKCR\CLSID... Uninstall Config...		Properties	Alt+Enter	7:43:18 AM
HKCR\CLSID... Uninstall Config...				4