

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

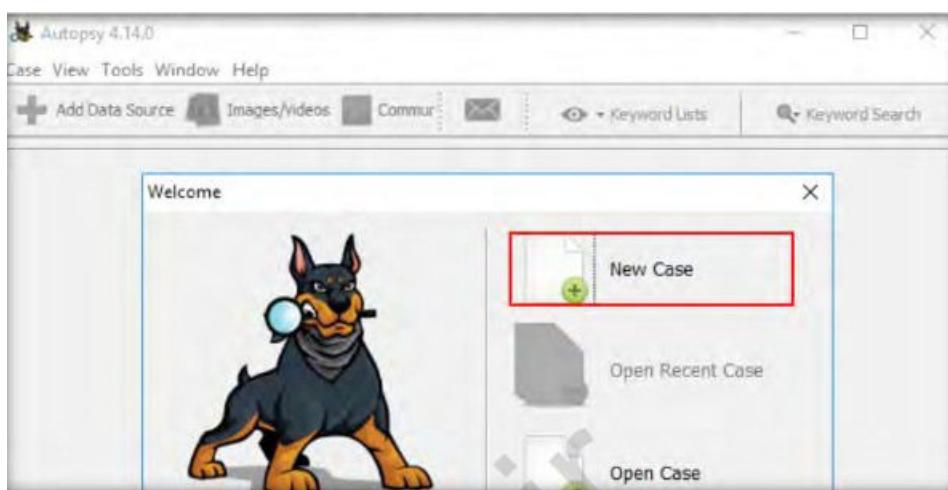
File System Analysis using The SleuthKit (Autopsy, fsstat, istat, fls and img_stat)

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.

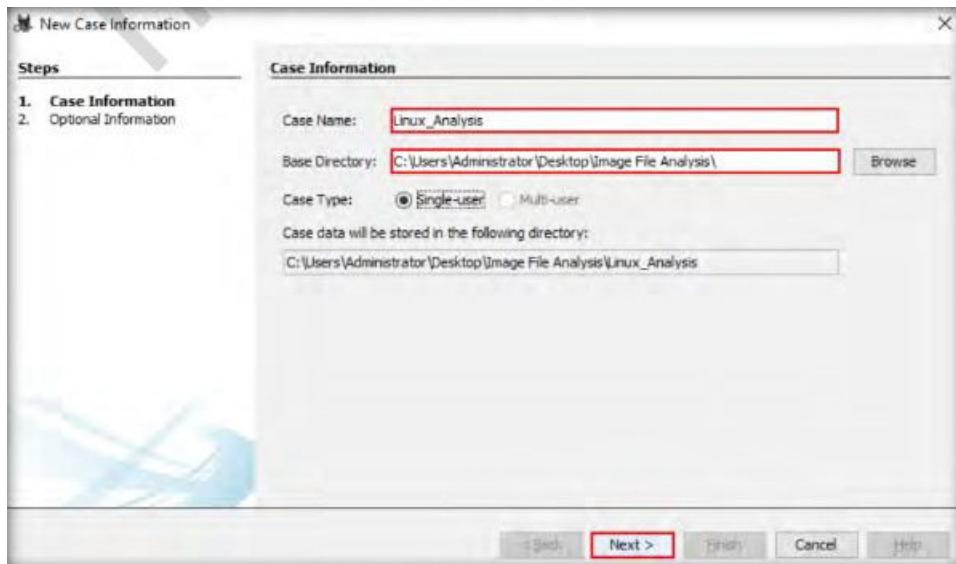


Autopsy Welcome window will appear along with Autopsy main window in the background. In the Welcome window, click New Case.

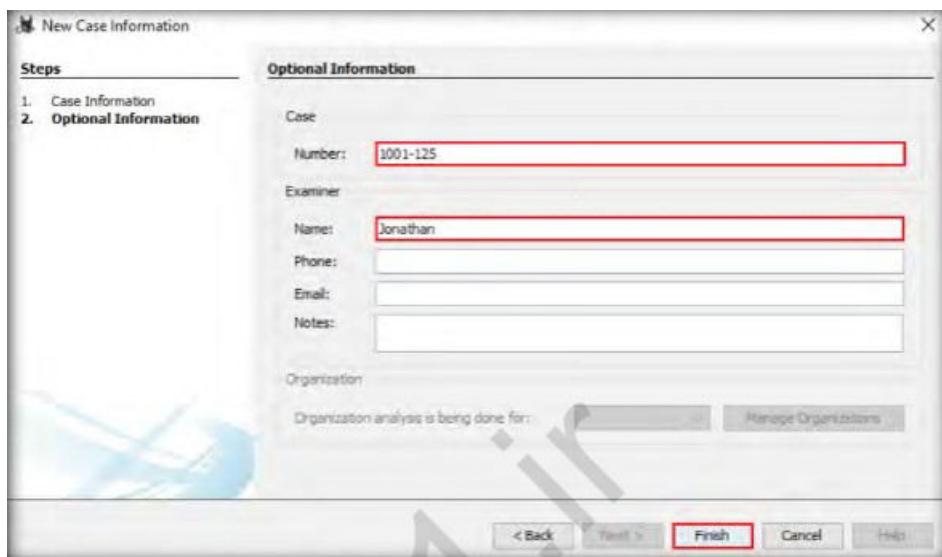


A New Case Information window opens asking you to input the Case Name and the Base Directory. The base directory is the location where the case data will get stored. The case name may be entered according to your identification purpose. In this lab, we are assigning the case name as Linux_Analysis.7.

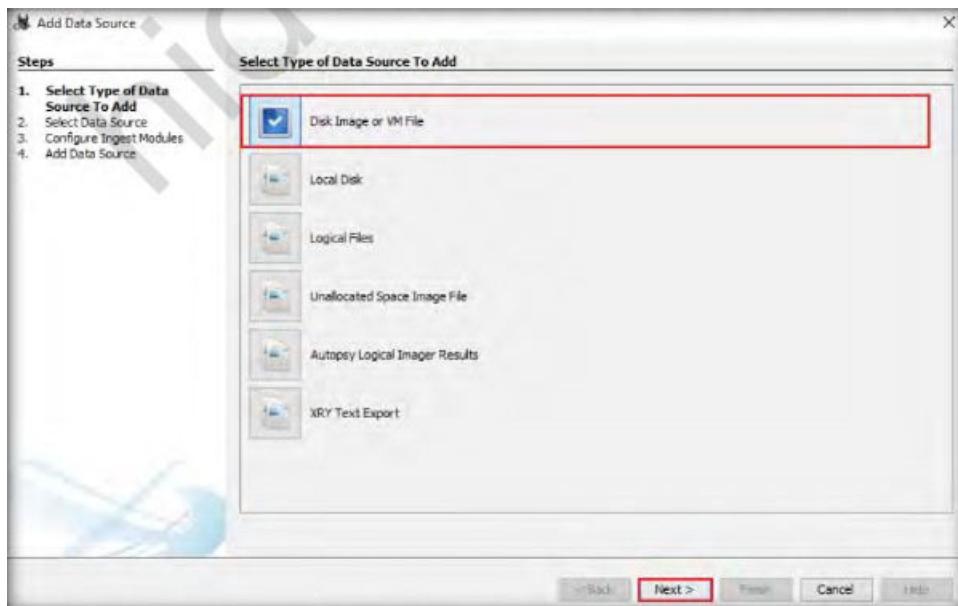
Before specifying the base directory, we will be creating a folder on the Desktop with the name Image File Analysis and setting the path of the Base directory to this folder. Upon setting the base directory, click Next.



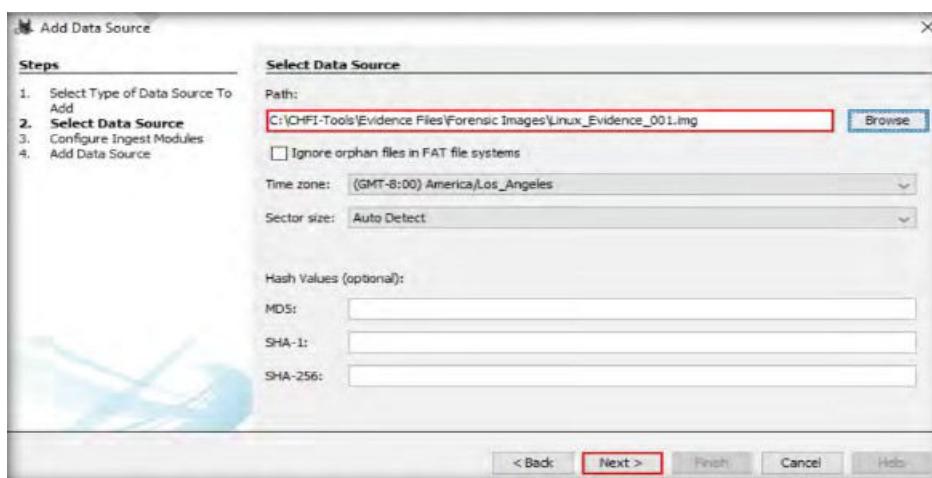
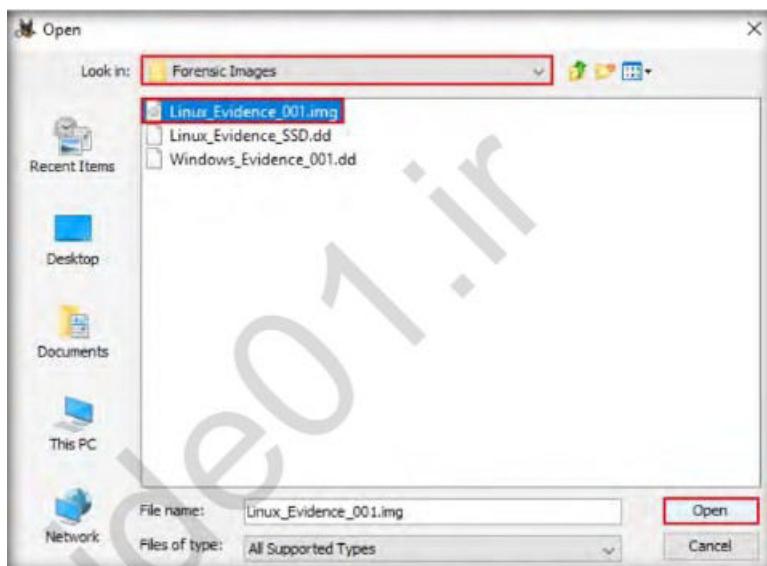
The New Case Information window now shows the Optional Information section where you can specify details such as name of the examiner and case number. For this lab, let us enter the name of the examiner as Jonathan and the case number as 1001-125. You may also fill out the other optional fields. Click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



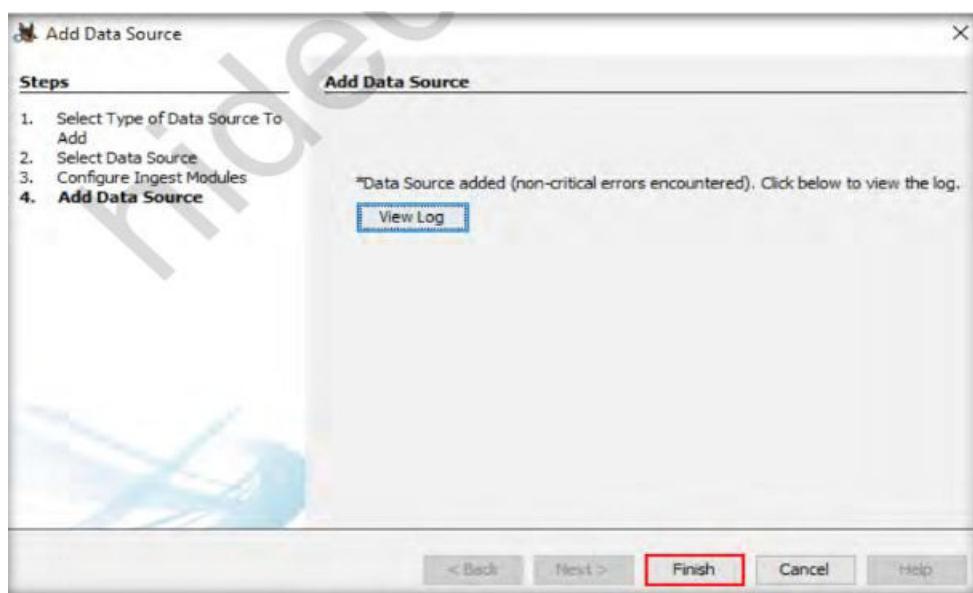
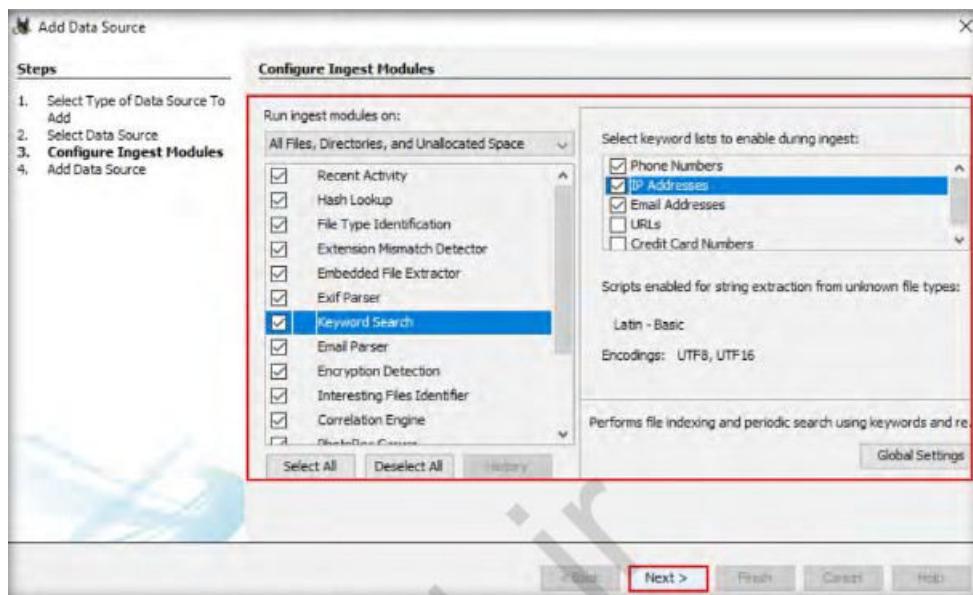
The Add Data Source window now appears displaying the section Select Type of Data Source to Add. Here, you need to select the type of data source to be provided as an input. In this lab, we will be analyzing a disk image; therefore, select the option Disk Image or VM File and click Next.



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 'Linux_Evidence_001.img' volume selected. In the left pane, the directory structure is visible, including the root directory and various system folders like /bin, /boot, /dev, /etc, /home, /lib, /media, /proc, /run, /sbin, /snap, /srv, /sys, /tmp, /usr, and /var. The right pane displays the contents of the '/etc' folder, specifically the '/etc/passwd' file. The file listing shows several entries, with the 'root' entry highlighted. The file content pane shows the raw text of the passwd file, which includes the root account and other system users.

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

This screenshot shows the Autopsy interface with the 'Linux_Evidence_001.img' volume selected. The left pane shows the directory structure, including the 'home' folder under the root. Inside 'home', there is a 'roger' folder, which contains a 'Documents' folder. The 'SeatPlan.xls' file is located within the 'Documents' folder. It is highlighted in the list view on the right, indicating it has been selected for examination.

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

This screenshot shows the Autopsy interface with the 'SeatPlan.xls' file selected. The right pane has tabs for Hex, Text, Applications, Messages, File Metadata, Context, Results, Annotations, and Other Occurrences. The 'File Metadata' tab is currently active. The file's metadata is listed, including 'Modified', 'Accessed', 'Created', 'Changed', and 'MD5'. The 'MD5' value, 'f5064adfeb6e31320ba904927749efdf', is highlighted with a red box.

To study fsstat

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

```
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.

```
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
OEM 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

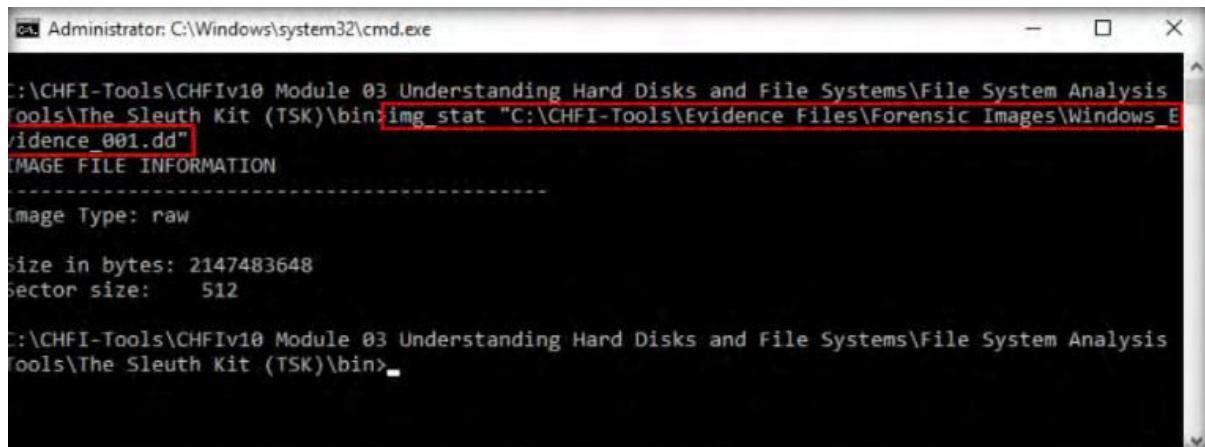
CONTENT INFORMATION
-----
Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 0 - 524286
Total Sector Range: 0 - 4194302

$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.



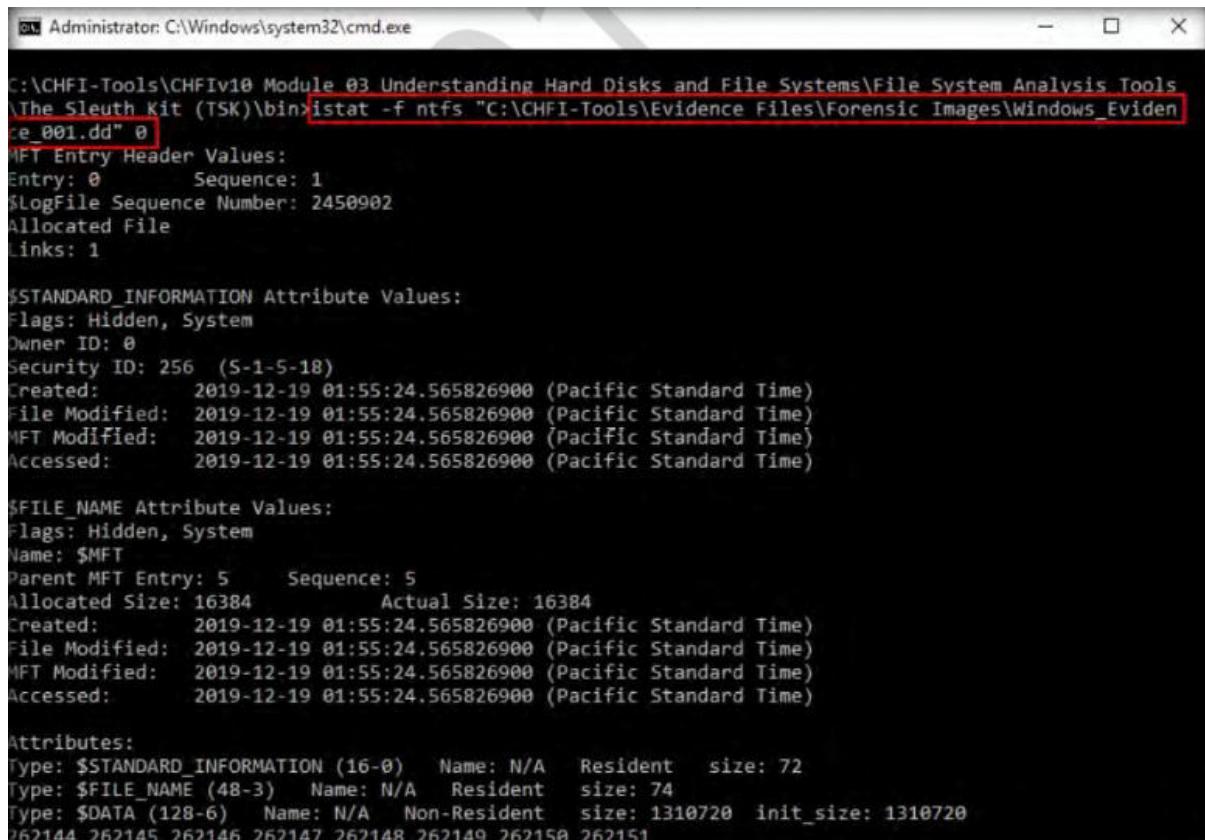
```
C:\CHFI-Tools\CHFIv10 Module 03 Understanding Hard Disks and File Systems\File System Analysis Tools\The Sleuth Kit (TSK)\bin>img_stat "C:\CHFI-Tools\Evidence Files\Forensic Images\Windows_Evidence_001.dd"
IMAGE FILE INFORMATION

Image Type: raw
size in bytes: 2147483648
Sector size: 512

C:\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:\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.

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

To Study fls

Use the fls command-line tool of TSK to list the files and directory names. Type `fls -f ntfs "C:\CHFI-Tools\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 stepup. 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

New Case

Basic Case Data Case Categories Offense & Custody Data Description of Evidence Chain of Custody Custom Fields Help

Case Name	Case 75
Investigator	Jonathan Davis
Organization	ABC Incorporation
Contact Details	jonathan@abcxxxxxxcorp.org
Timezone	Local (GMT -7:00)
Default Drive	C:\ [Local]
Acquisition Type	<input checked="" type="radio"/> Live Acquisition of Current Machine <input type="radio"/> Investigate Disk(s) from Another Machine
Enable USB Write-block	<input type="checkbox"/>
Case Folder	<input checked="" type="radio"/> Default Location <input type="radio"/> Custom Location C:\Users\Administrator\Documents\PassMark\OSForensics\Cases\Case 75 <input type="button" value="Browse"/>
Log case activity	<input checked="" type="checkbox"/>

OSForensics - Case 75

Workflow

- Start
- Auto Triage
- Manage Case
- Add Device
- Forensic Imaging
- System Information
- Memory Viewer
- User Activity
- Passwords
- File Name Search
- Deleted File Search

Manage Case

Select Case

Title	Create Date	Access Date
Case 75	Wednesday, July 29, 2020, 0:09:35	Wednesday, July 29, 2020, 0:09:35

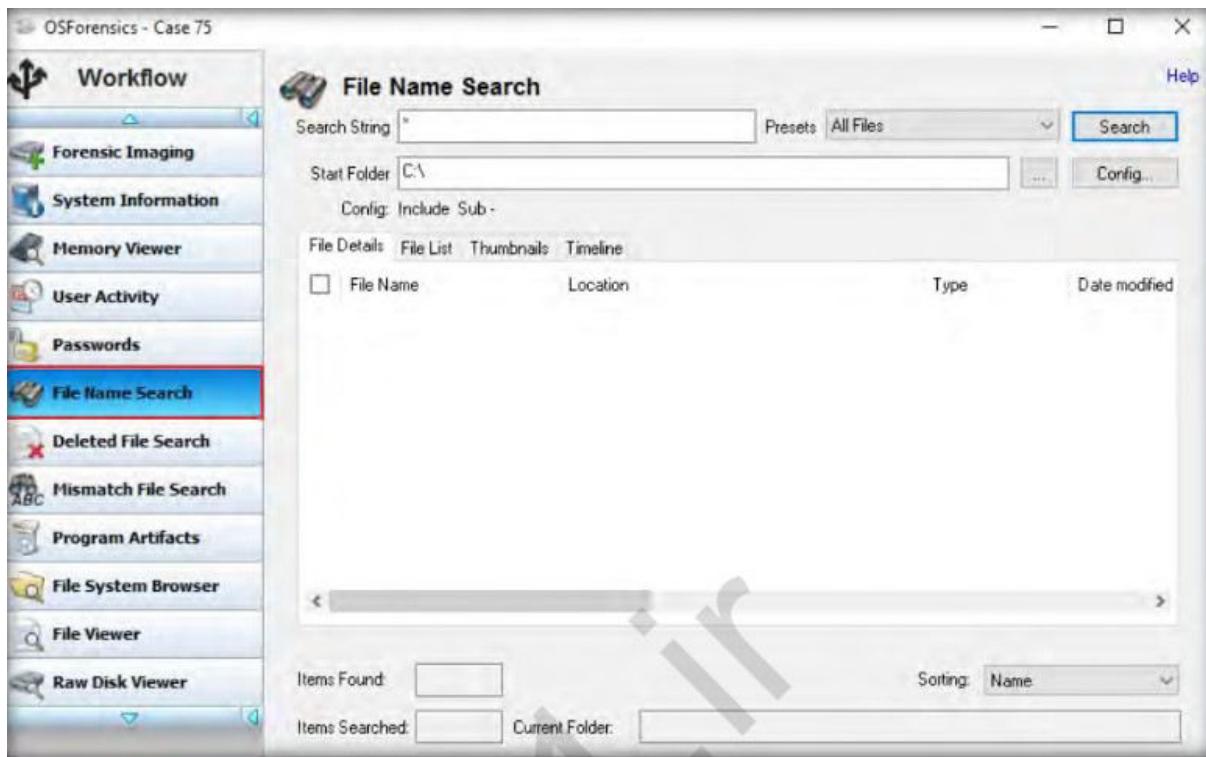
Case Properties

Add to Case

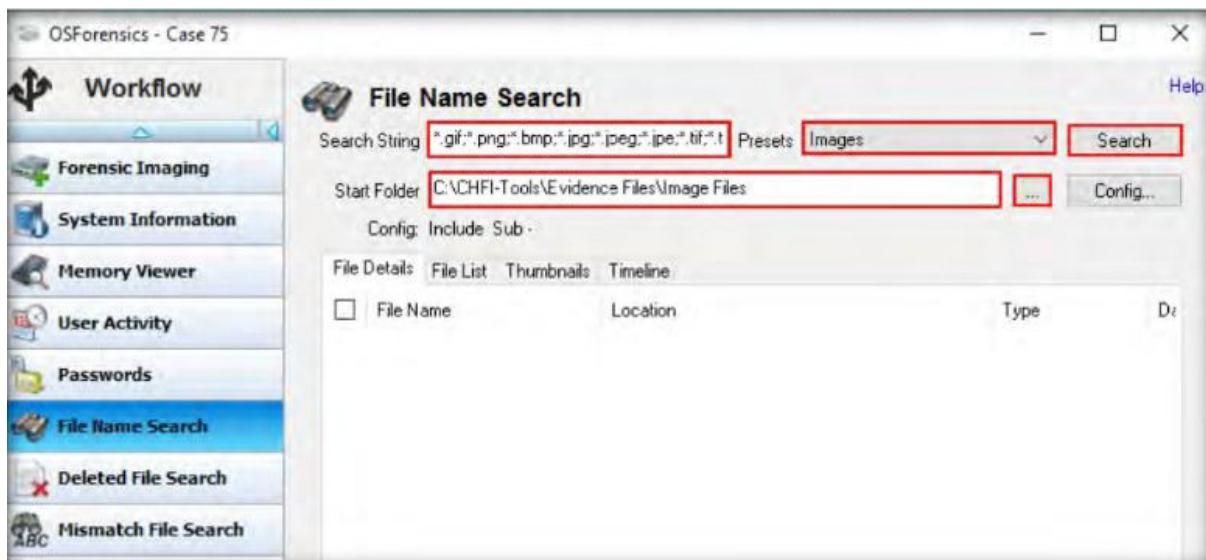
Case Items

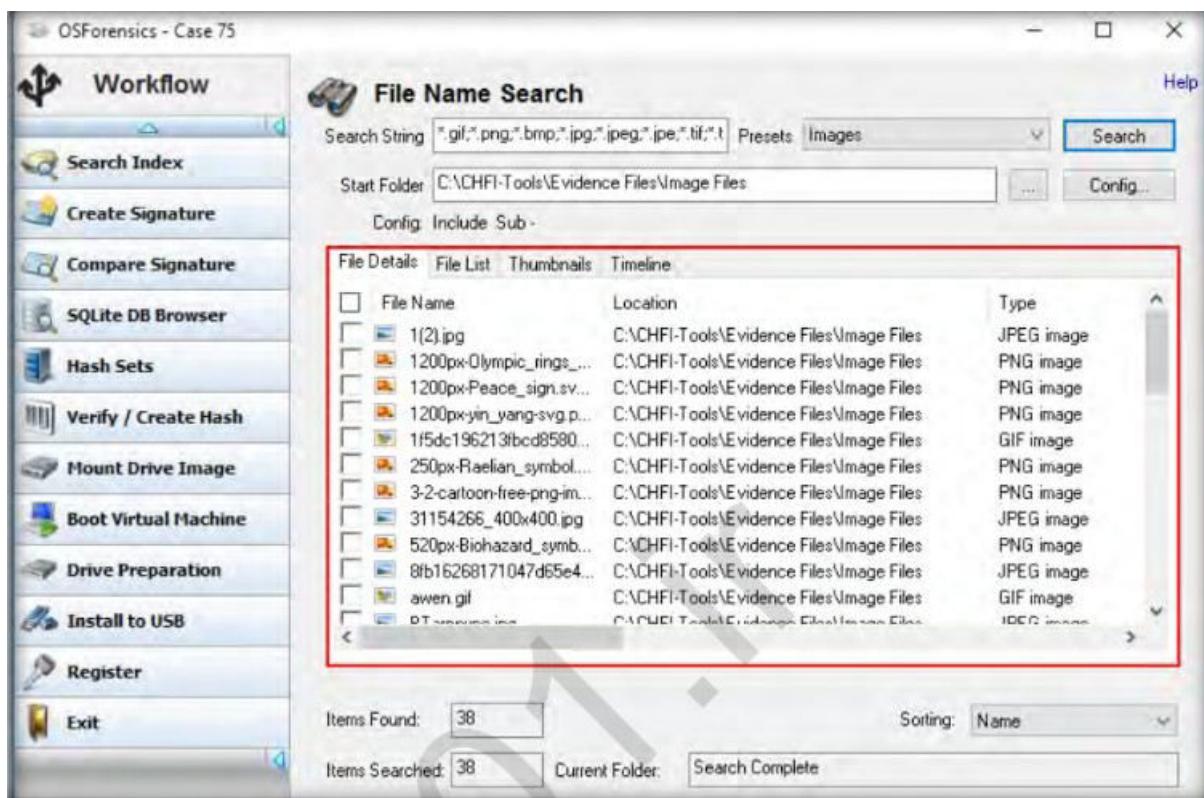
Case Item ID	Title	Module	Case Item
<input type="button" value="Open"/>			
<input type="button" value="Delete"/>			

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.

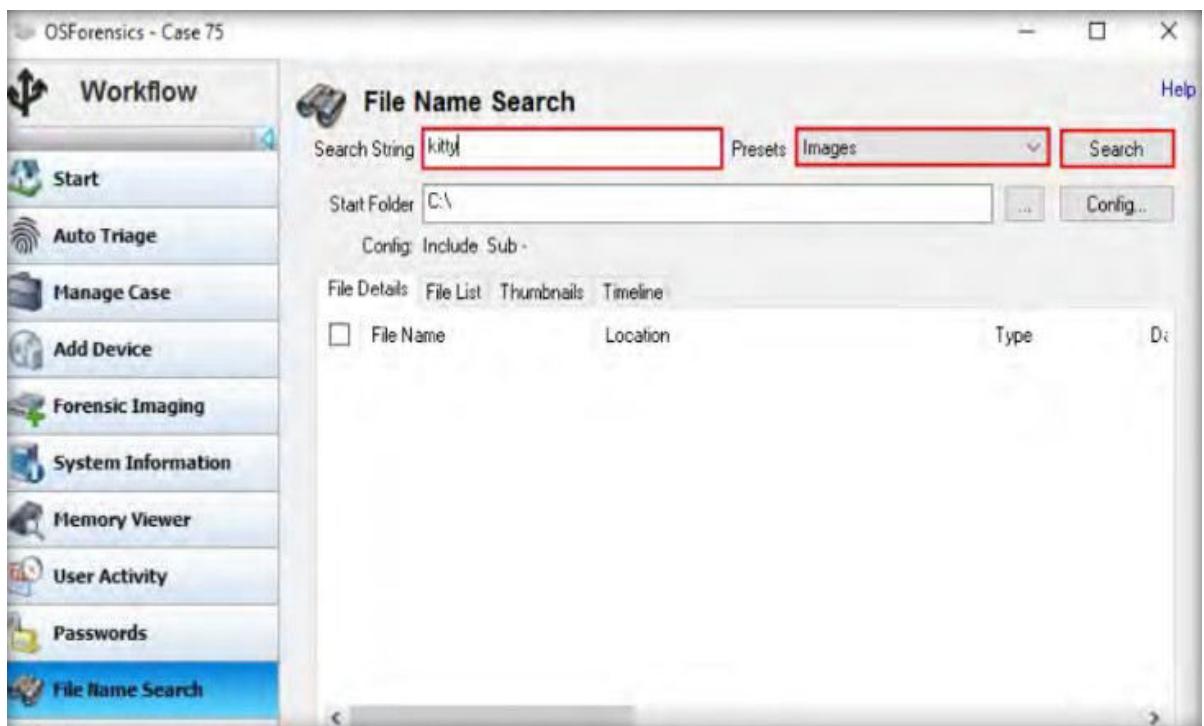


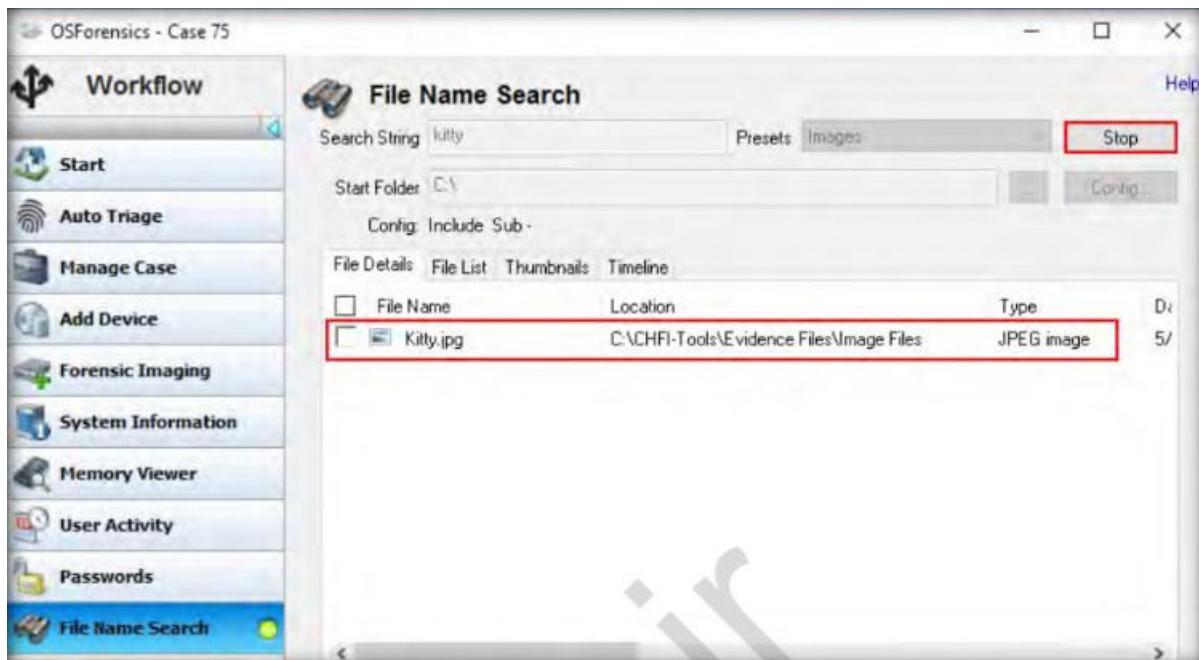
In the Start Folder field, specify the path to search for image files by clicking the ellipsis button and choosing the location (here, we are specifying the location C:\CHFI-Tools\EvidenceFiles\Image Files to search for images in it). Then, click the Search button.



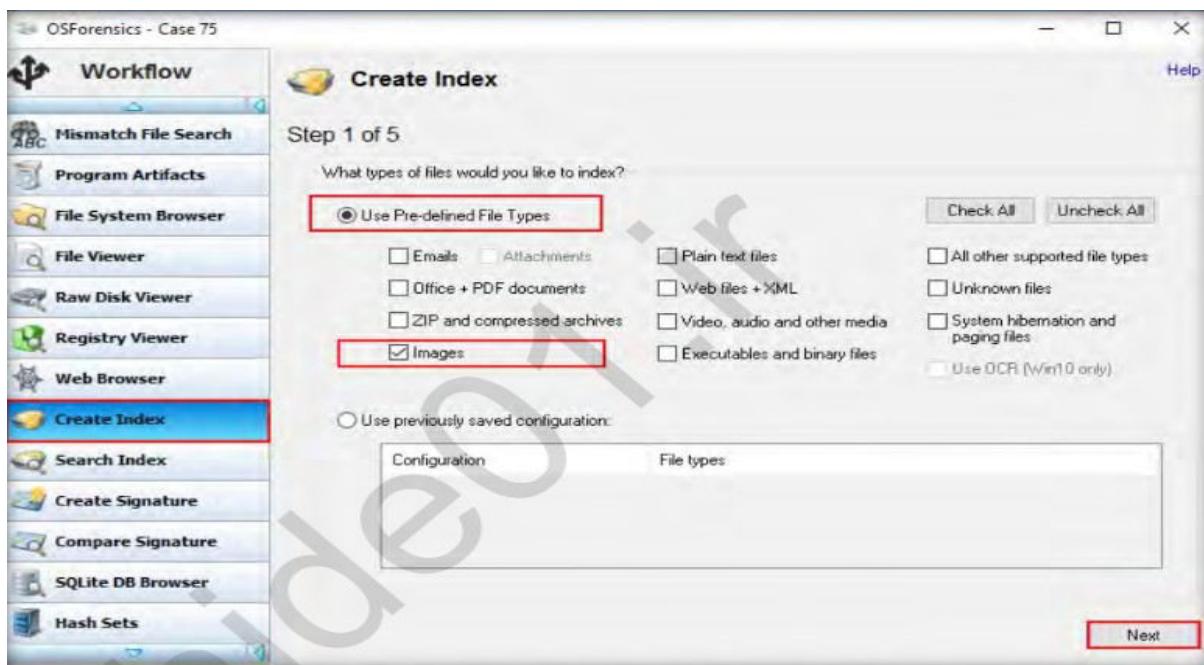


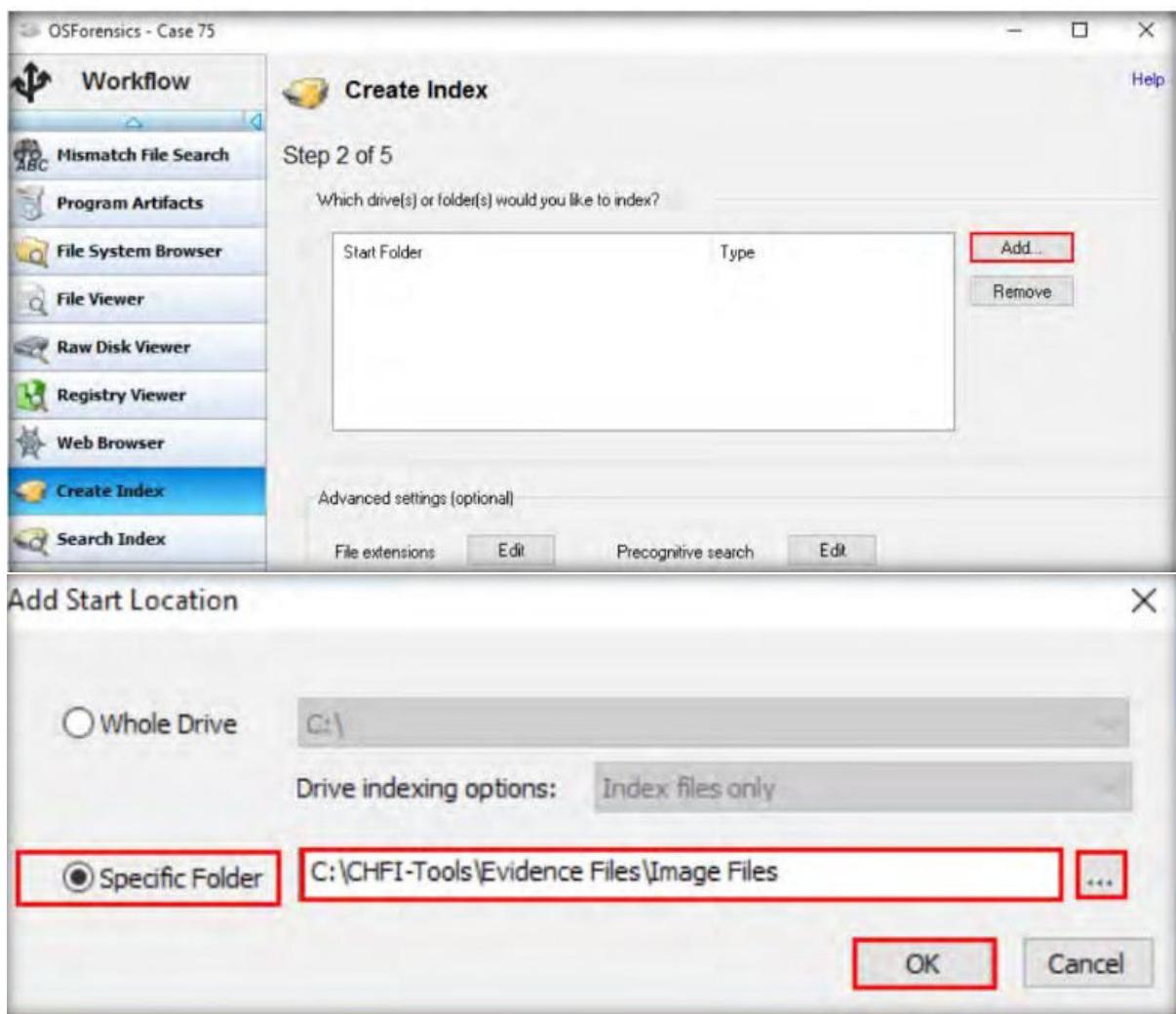
Alternatively, if you wish to search only for a single image on the entire system, select Images from the Pre-sets drop-down menu, enter the name of the desired image file in the Search String field, and then click Search, as shown in the screenshot below. Here, we are searching for the JPEG image file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

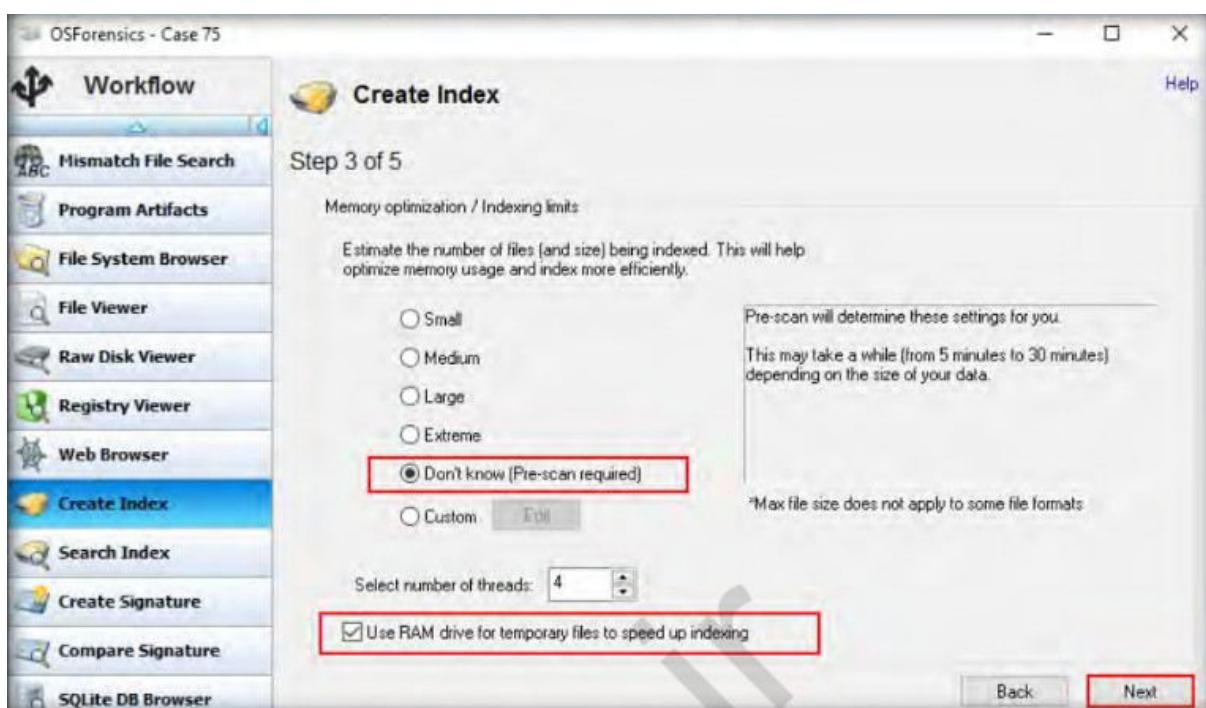
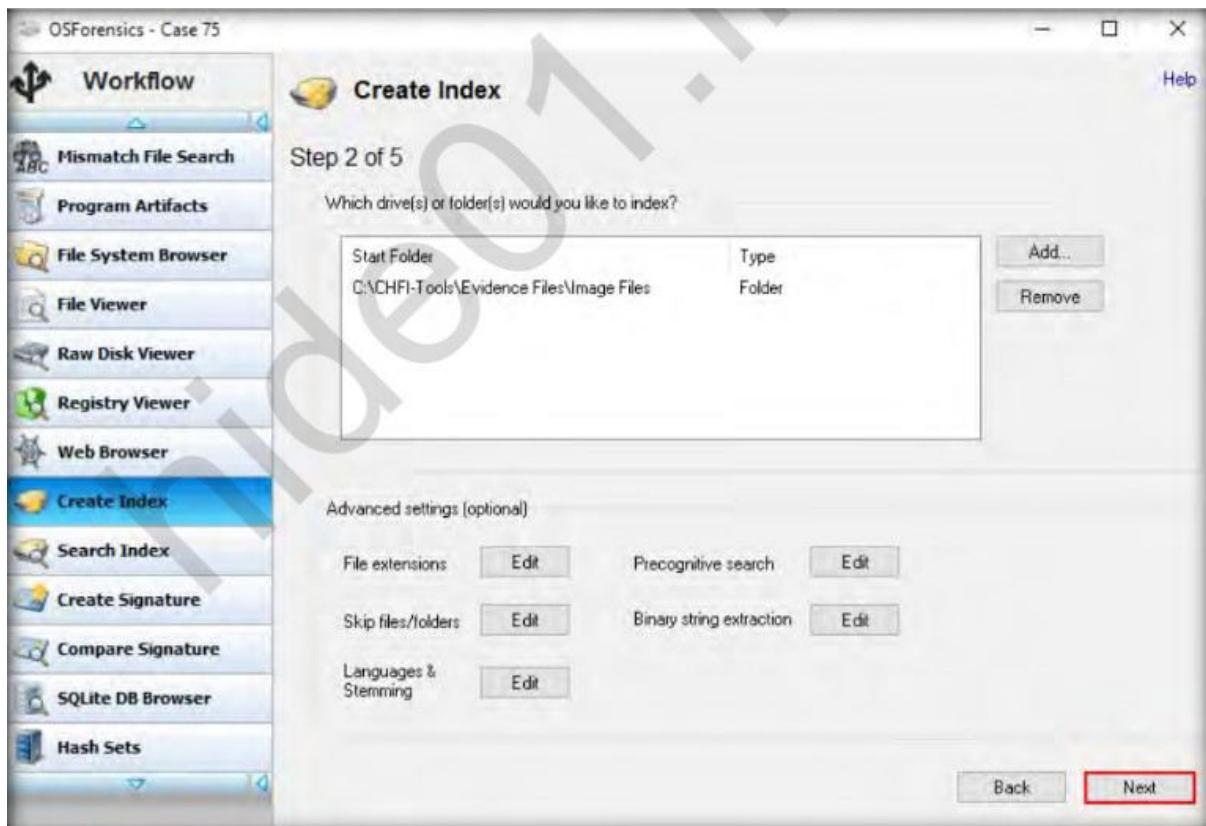


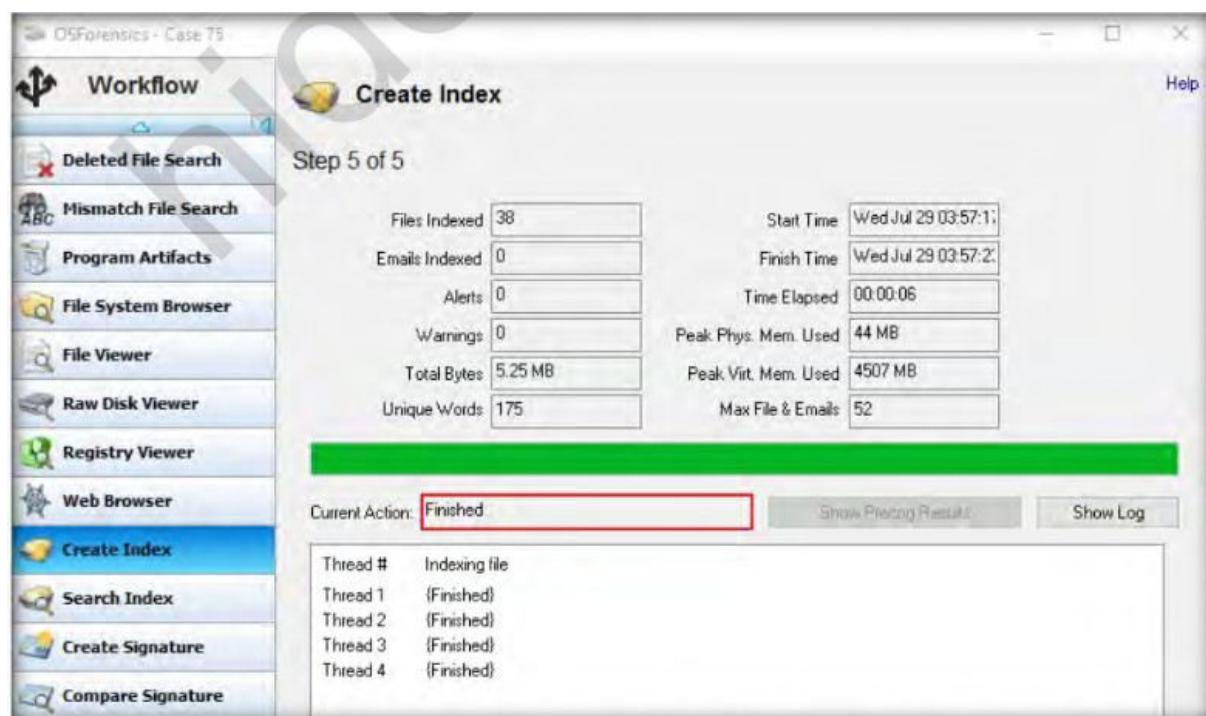
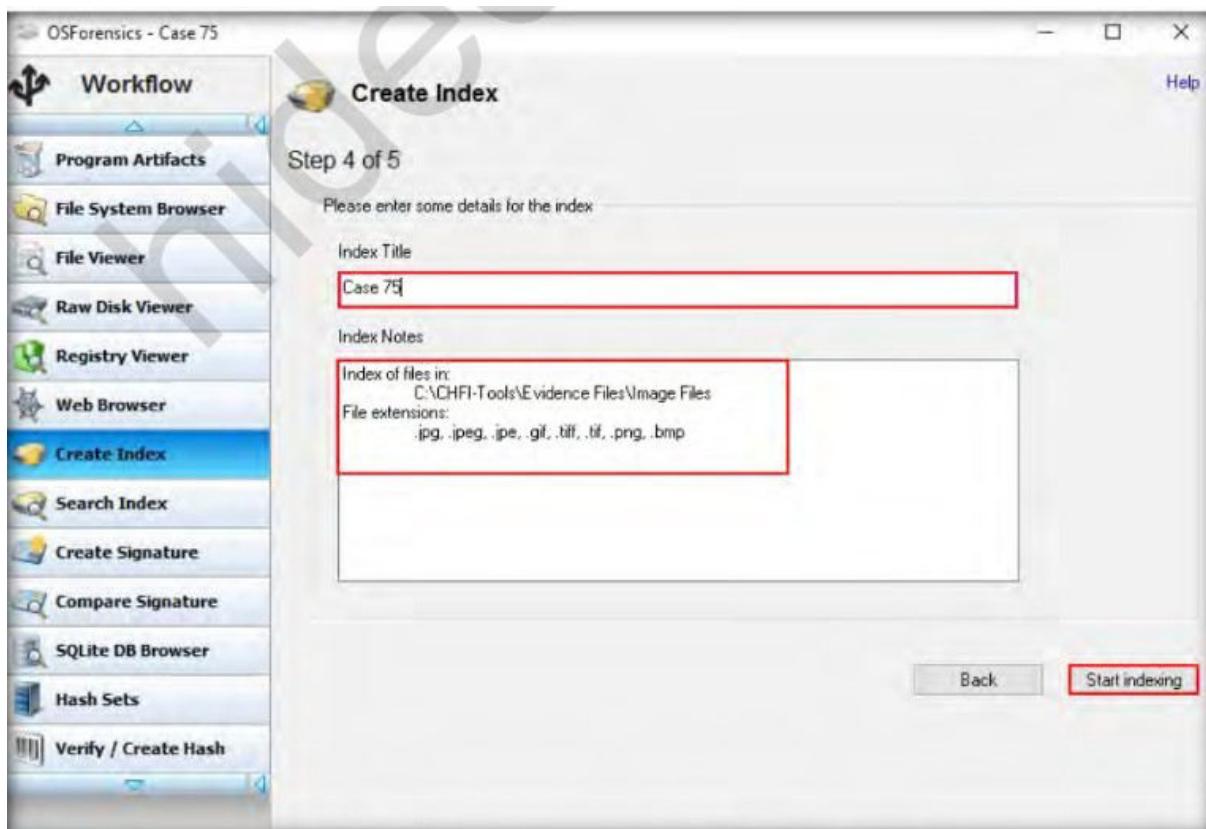


The Create Index section appears in the right pane. In this section, select the Use Pre-defined File Types option for creating the index and check the required options listed under it for selecting the file types that you wish to index (here, we have selected the Images option). Then, click Next.

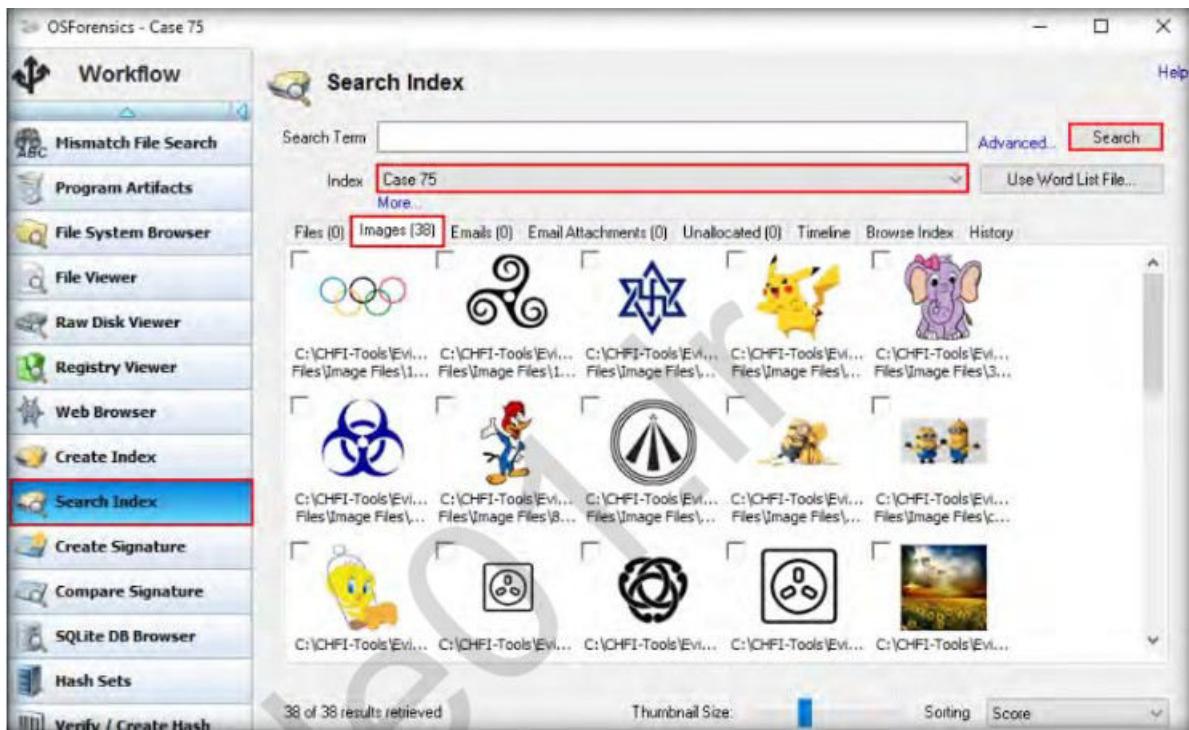




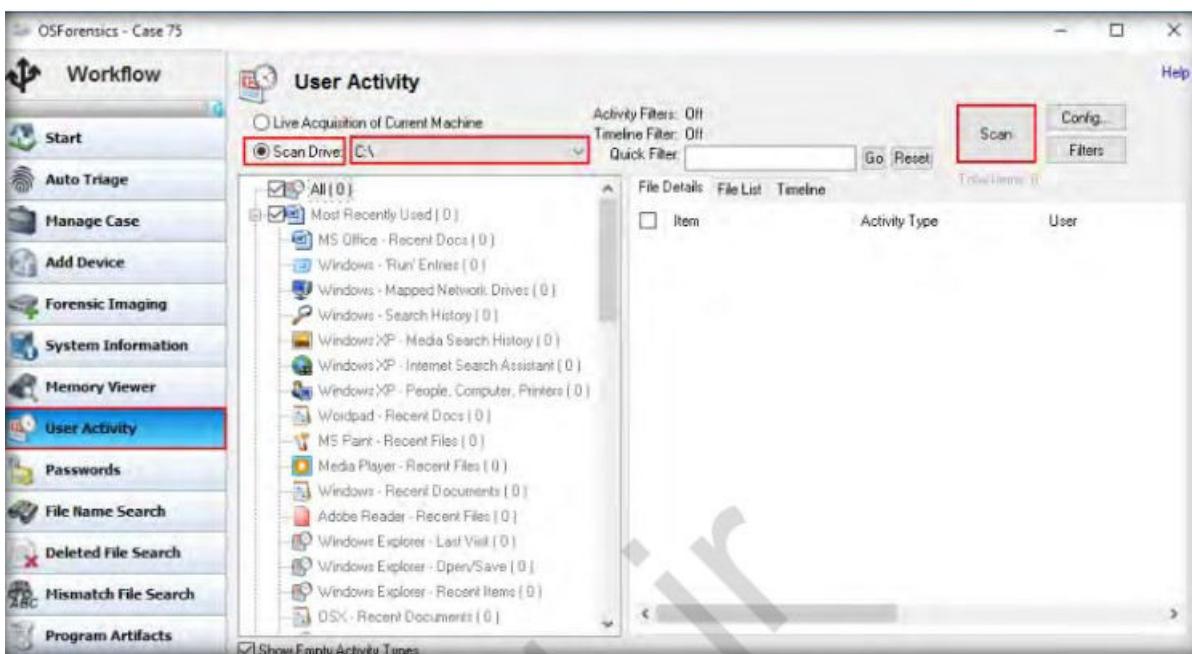


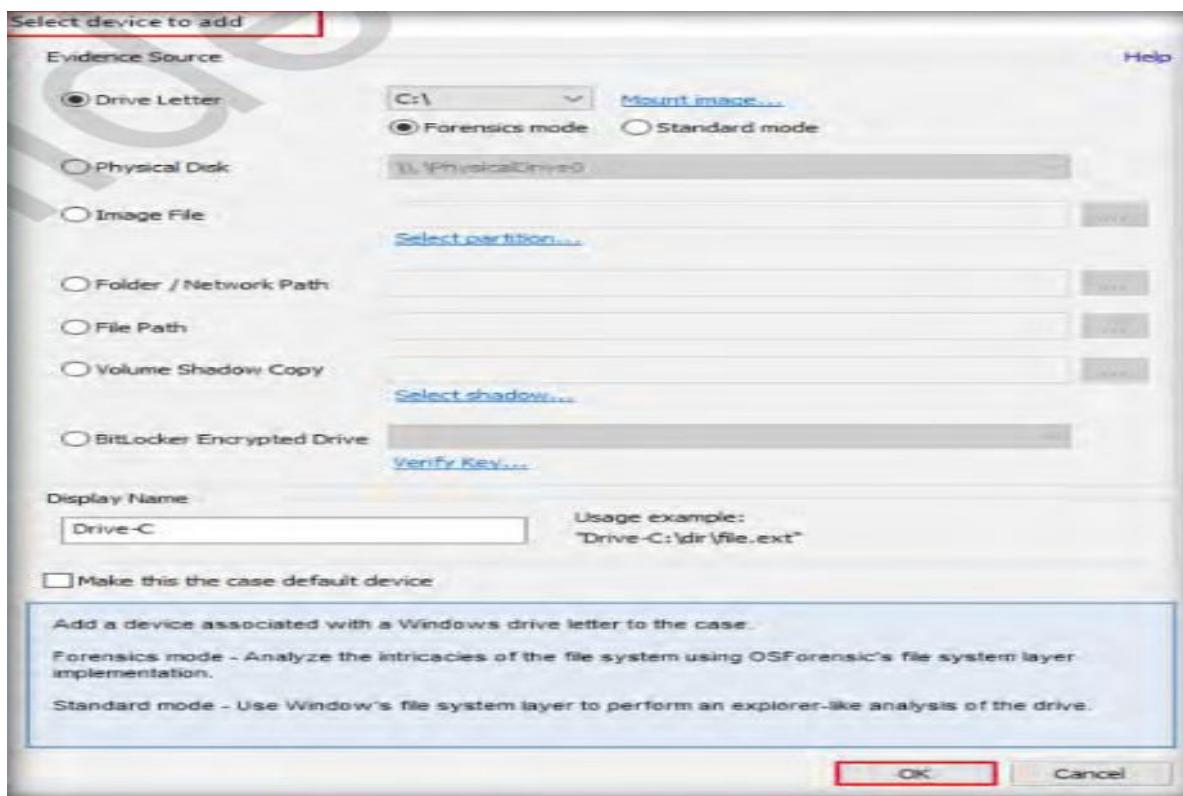


We will now search the indexed files. To search for the indexed files, select Search Index from the left pane of the tool window. The Search Index section now appears in the tool window. The index field at the top displays the name of the case we created (i.e., Case 75). Click Search. The tool will load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

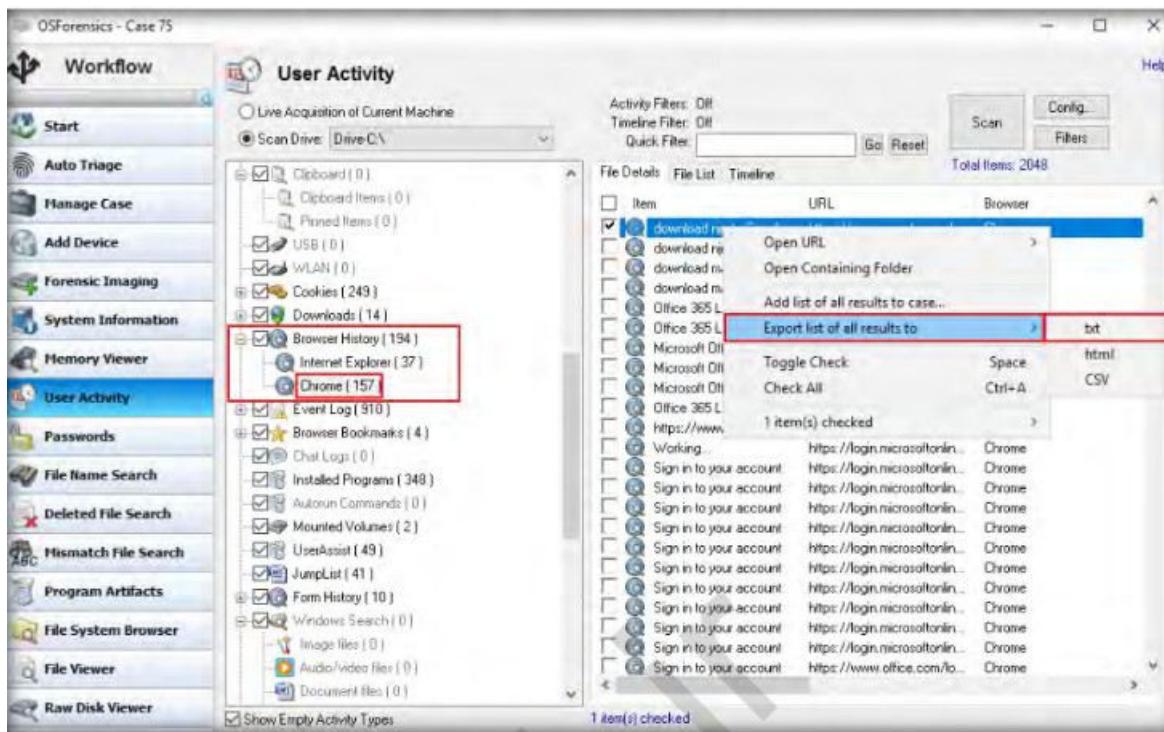


Click User Activity in the left pane to scan for evidence such as browsed websites, USB drives, recent downloads and wireless networks.

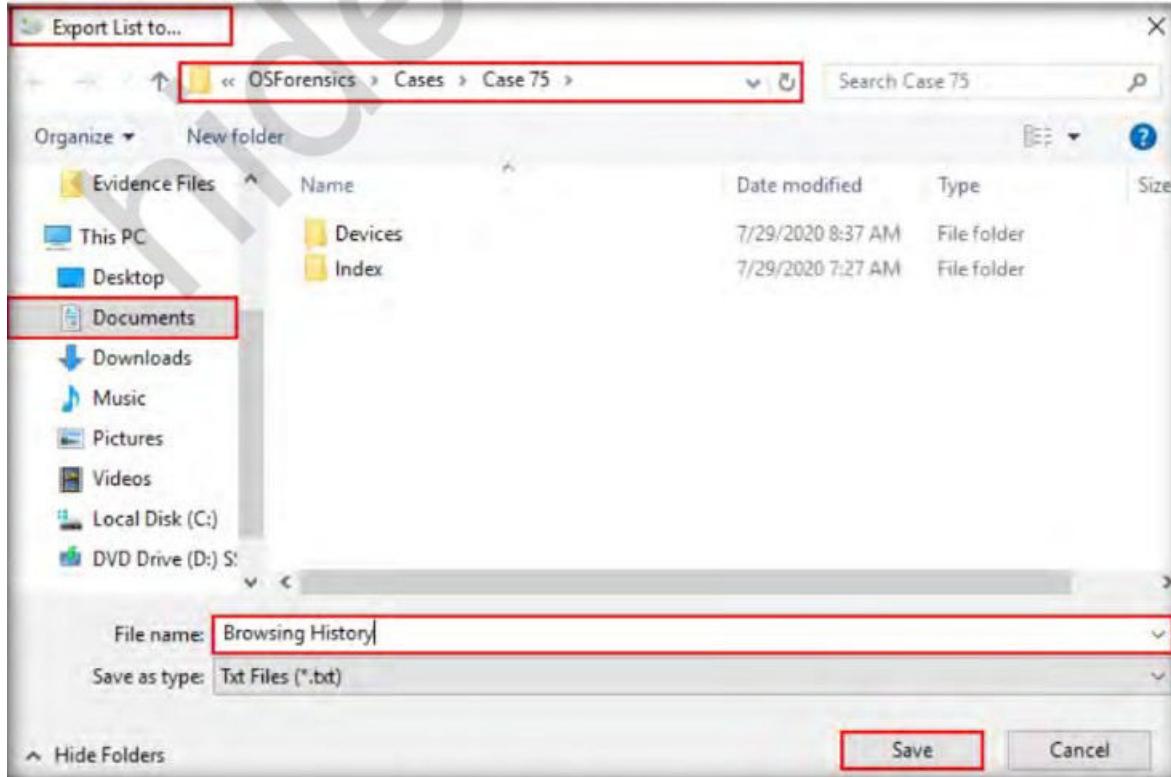




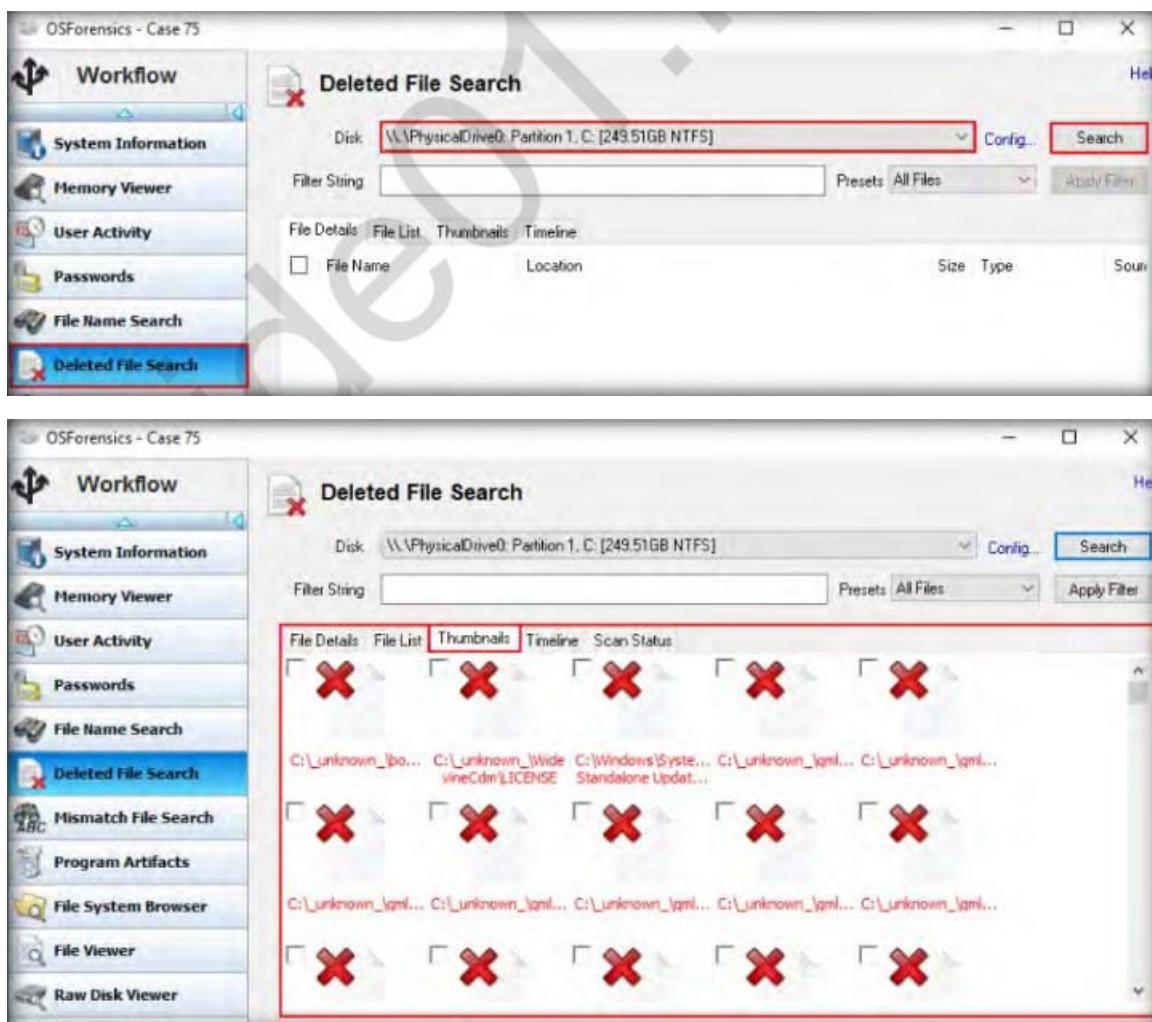
If you wish to save any of the above user-activity information on your system, such as Browser History, then scroll down the items list in the left pane below the Scan Drive option and expand the Browser History node. Select the browser for which you wish to retrieve the history (Here, we are selecting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



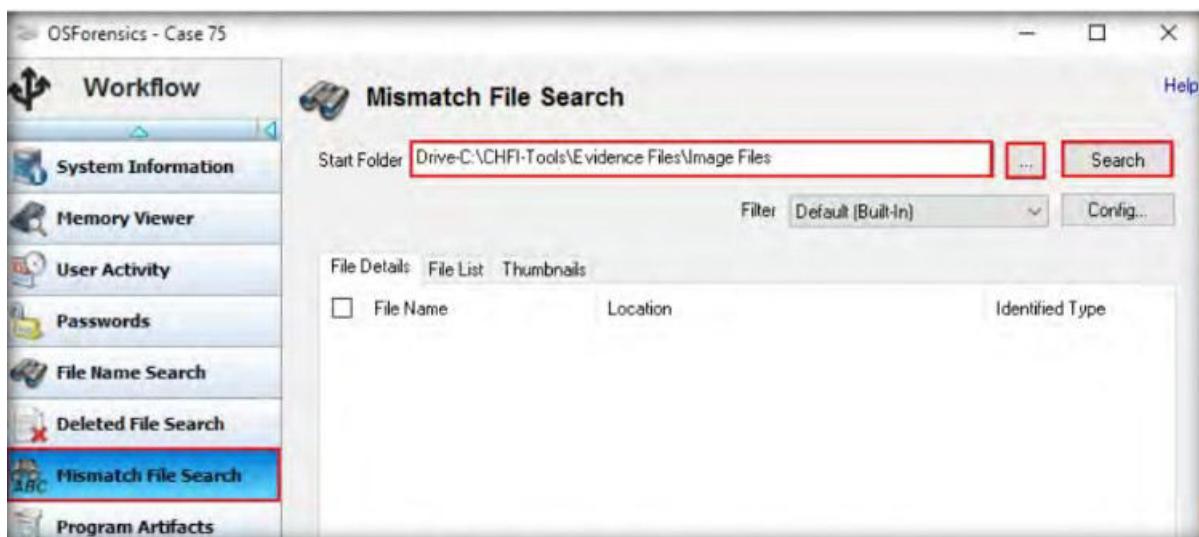
An Export List to... Window will appear. Navigate to C:\Users\Administrator\Documents\PassMark\OSForensics\Cases\Case 75, name the file (here, we are naming it as Browsing History), and click Save to export the browsing history.



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



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



Mismatch File Search

Start Folder: C:\CHFI-Tools\Evidence Files\Image Files

File Details File List **thumbnails**

Sunset-pixels-photo-132037_BLOG.bat
Location: C:\CHFI-Tools\Evidence Files\Image Files
Identified Type: JPEG image data, EXIF standard
Size: 415.2 KB, Created: 8/6/2020, 11:08:40, Modified: 8/6/2020, 18:06:00, Accessed:
BTarpnpxc.exe
Location: C:\CHFI-Tools\Evidence Files\Image Files
Identified Type: JPEG image data, JFIF standard 1.01
Size: 3.45 MB, Created: 8/6/2020, 11:08:40, Modified: 8/6/2020, 18:06:00, Accessed:
cartoon-hd-poster-art-pncal19975-bpncal19975-large-original-imaehwt3p7fj
Location: C:\CHFI-Tools\Evidence Files\Image Files
Identified Type: JPEG image data, JFIF standard 1.01
Size: 32.42 KB, Created: 8/6/2020, 11:08:40, Modified: 8/6/2020, 18:06:00, Accessed:
520px-Biohazard_symbol_(blue).mp4
Location: C:\CHFI-Tools\Evidence Files\Image Files
Identified Type: PNG image, 520 x 520, 8-bit/color RGBA, non-interlaced
Size: 26.14 KB, Created: 8/6/2020, 11:08:40, Modified: 8/6/2020, 18:06:00, Accessed:

Items Found: 6 Sorting: Extension

Items Searched: 38 Current Folder: Search Complete

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

Memory Viewer

Live Analysis Static Analysis

Process	PID	CPU %	Total CPU Time	User Time	Kern. %
Idle	0	98.44%	21:32:41.250	00:00:00.000	21:32:
System	4		00:03:50.203	00:00:00.000	00:03:
smss.exe	260		00:00:00.140	00:00:00.000	00:00:
svchost.exe	340		00:00:21.000	00:00:15.825	00:00:
csrss.exe	364		00:00:01.437	00:00:00.265	00:00:
csrss.exe	428		00:00:01.296	00:00:00.187	00:00:
wninit.exe	448		00:00:00.062	00:00:00.000	00:00:
winlodon.exe	488		00:00:00.109	00:00:00.015	00:00:

Process Info Handles Modules **Memory Space** Memory Layout

Address Range	Size	State	Protection	Type	Module
0x0000000000000000 - 0x00000000... 2048 MB	Free	NA	-	Private	
0x000000007FE0000 - 0x000000... 4 KB	Commit	RO	Private		
0x000000007FFE1000 - 0x000000... 60 KB	Reserved	-	Private		
0x000000007FFF0000 - 0x000000... 899112...	Free	NA	-	Private	
0x0000000C02800000 - 0x000000... 920 KB	Reserved	-	Private		
0x0000000C028E5000 - 0x000000... 8 KB	Commit	RW	Private		
0x0000000C028E8000 - 0x000000... 56 KB	Reserved	-	Private		
0x0000000C028F6000 - 0x000000... 16 KB	Commit	RW	Private		
0x0000000C028FA000 - 0x000000... 8 KB	Reserved	-	Private		
0x0000000C028FC000 - 0x000000... 8 KB	Commit	RW	Private		

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 interface. On the left, there's a sidebar titled 'Workflow' with icons for 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 area is titled 'System Information'. It has a dropdown menu 'List:' set to 'Basic System Information', and buttons for 'Edit...' and 'Go'. Below that is a search bar with 'Find Text: D\'. Underneath, there are two radio buttons: '(*) Live Acquisition of Current Machine' (selected) and '(*) Scan Drive: D\'. A table titled 'Commands' follows, listing various system information items with their corresponding commands, internal status, architecture, live acquisition status, and disk status.

Name	Command	Internal	Architecture	Live Acquisi...	D
Computer Name	SysInfoDll_GetComputerName	Yes	32/64	Yes	N
Operating system	SysInfoDll_GetOS	Yes	32/64	Yes	N
CPU Info	SysInfoDll_GetCPUInfo	Yes	32/64	Yes	N
Mem Info	SysInfoDll_GetMemoryInfo	Yes	32/64	Yes	N
Graphics Info	SysInfoDll_GetGraphicalInfo	Yes	32/64	Yes	N
USB Info	SysInfoDll_GetUSBInfo	Yes	32/64	Yes	N
Disk volume Info	SysInfoDll_GetSystemInfo_SM...	Yes	32/64	Yes	N
Disk drive Info	SysInfoDll_GetSystemInfo_SM...	Yes	32/64	Yes	N
Optical drive Info	SysInfoDll_GetSystemInfo_SM...	Yes	32/64	Yes	N
Network Info	SysInfoDll_GetSystemInfo_SM...	Yes	32/64	Yes	N
Print Info	SysInfoDll_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.

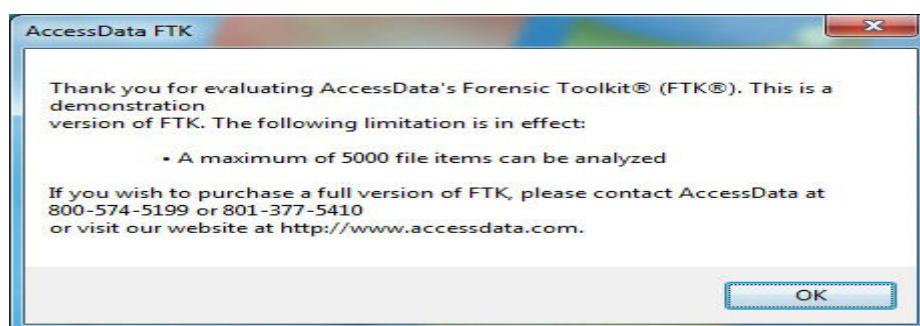
Step 1: Start Forensic Toolkit.



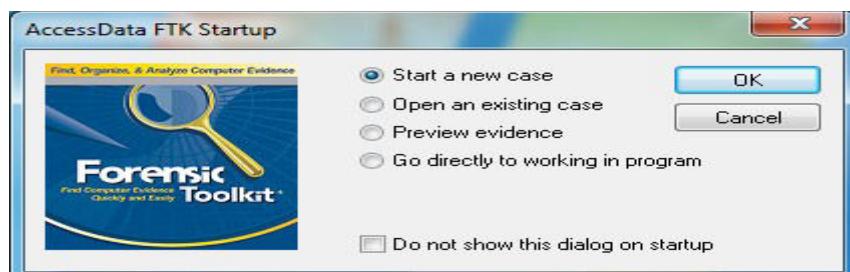
Step 2: Here, prompted with a warning dialog box, click on OK to continue.



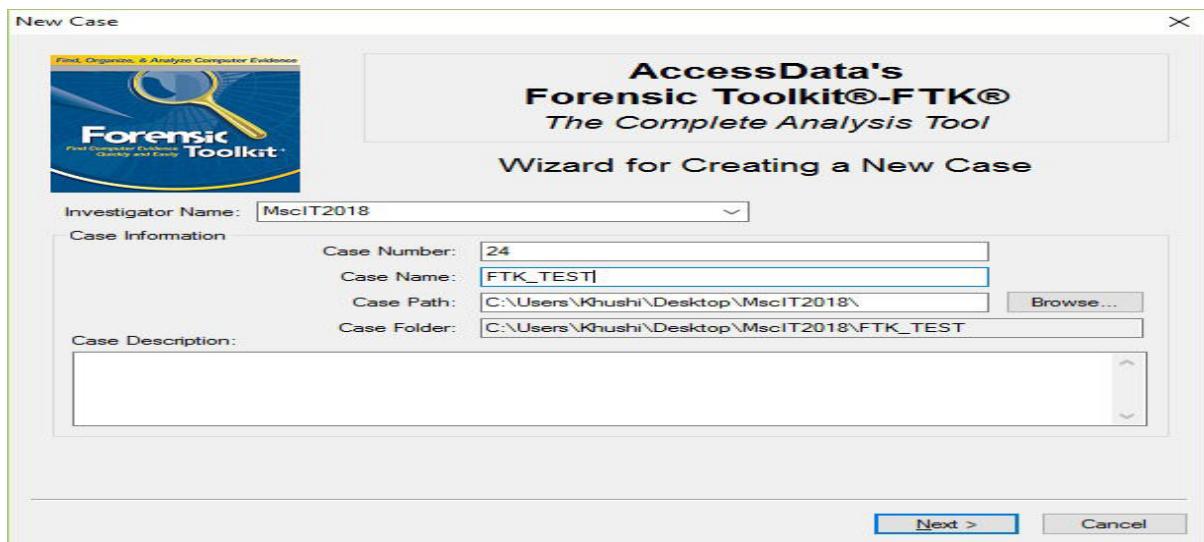
Step 3: click on OK button.



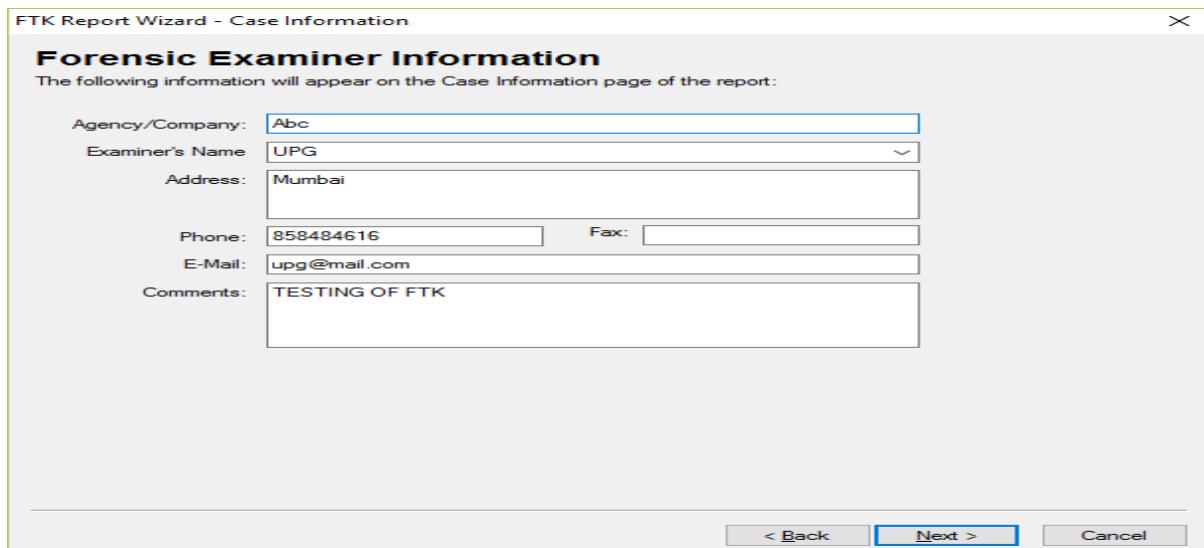
Step 4: Now select Start New Case option and click on ok.



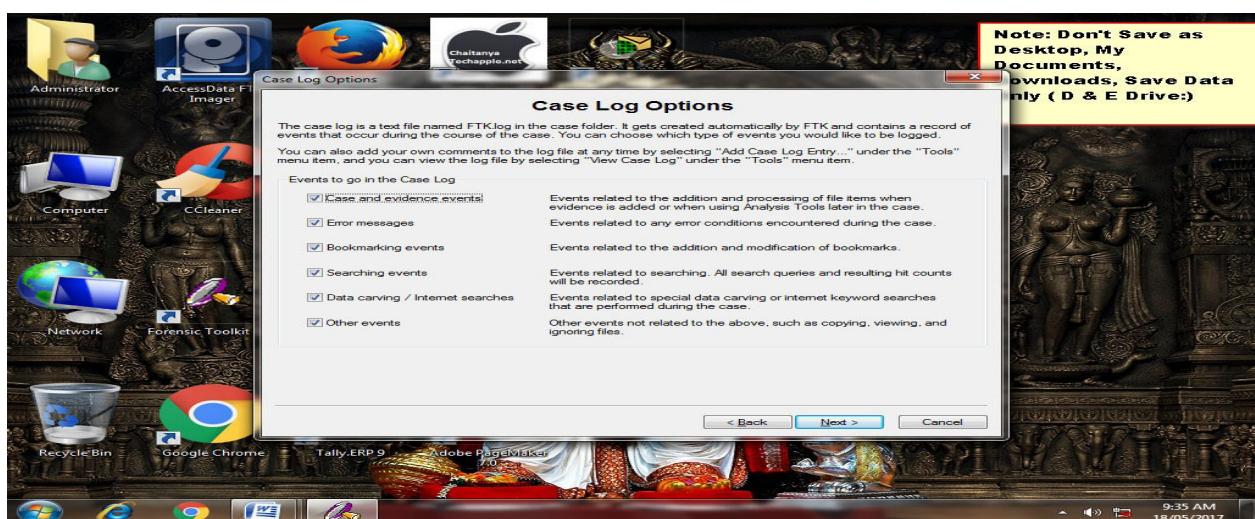
Step 5: Enter the detail for a New case.



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



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



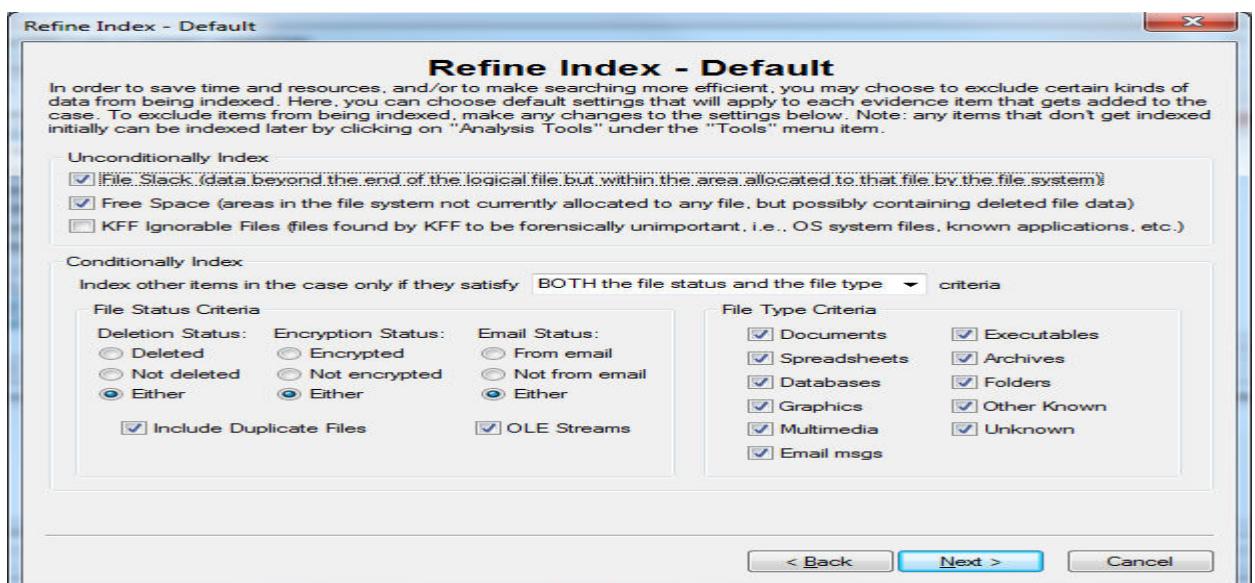
Step 8: Now again leave the default settings and click on next.



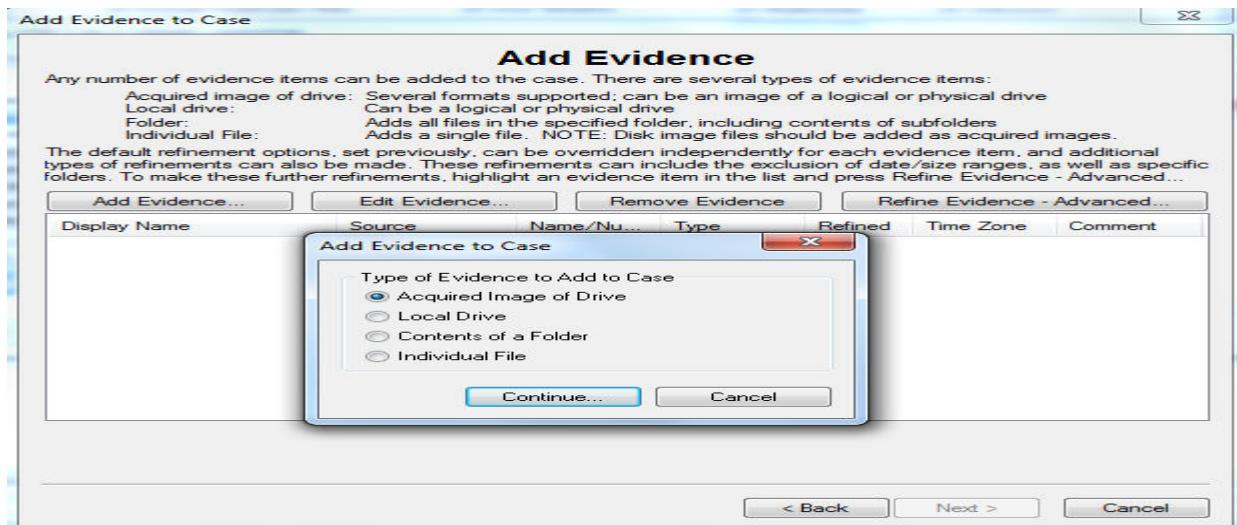
Step 9: In the Refine Case-Default, click the Include All items button and then click Next.



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



Step 11: Now here Click on add Evidence button.



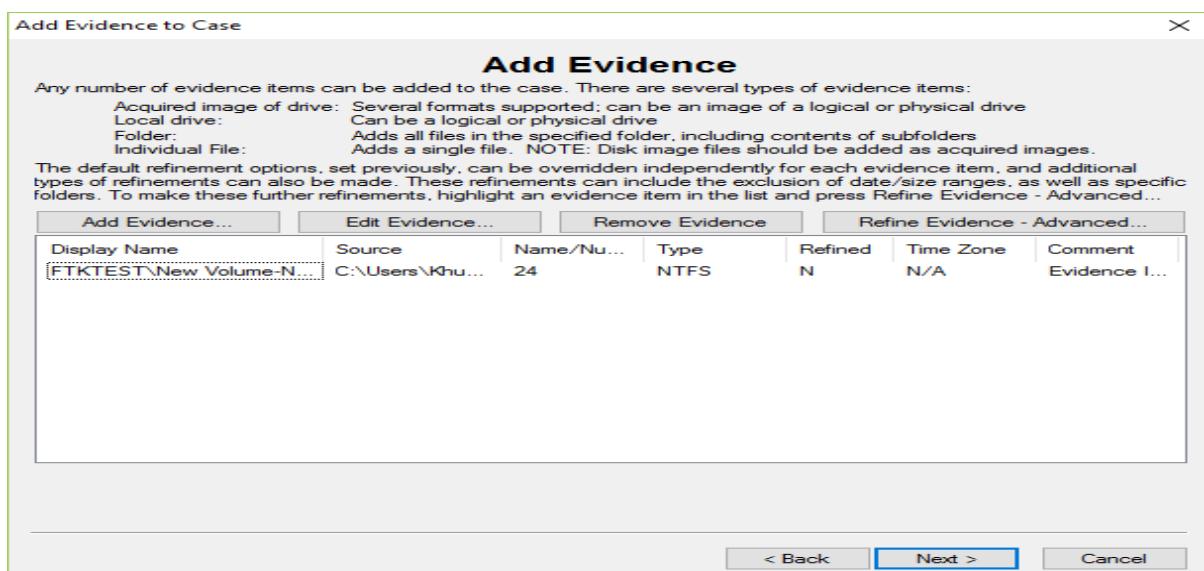
Step 12: Enter Evidence Information and click on OK button.

Evidence Information

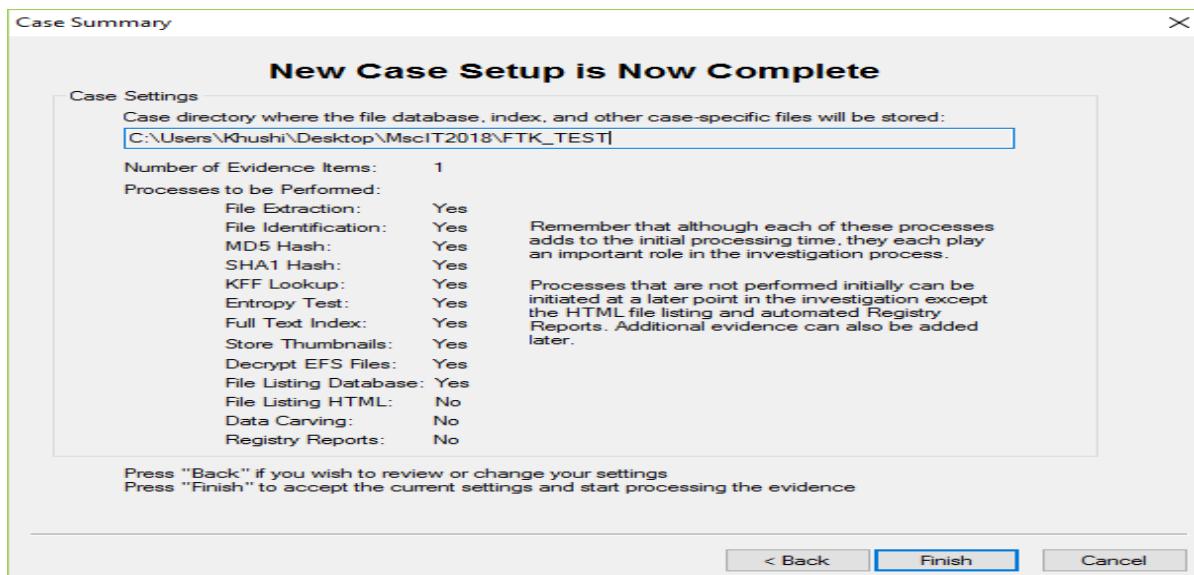
Evidence Location:	C:\Users\Khushi\Desktop\MsclT2018\FTKTEST.E01
Evidence Display Name:	FTKTEST
Evidence Identification Name/Number:	24
Comment:	Evidence Information
Local Evidence Time Zone:	Choose time zone for evidence ...

OK Cancel

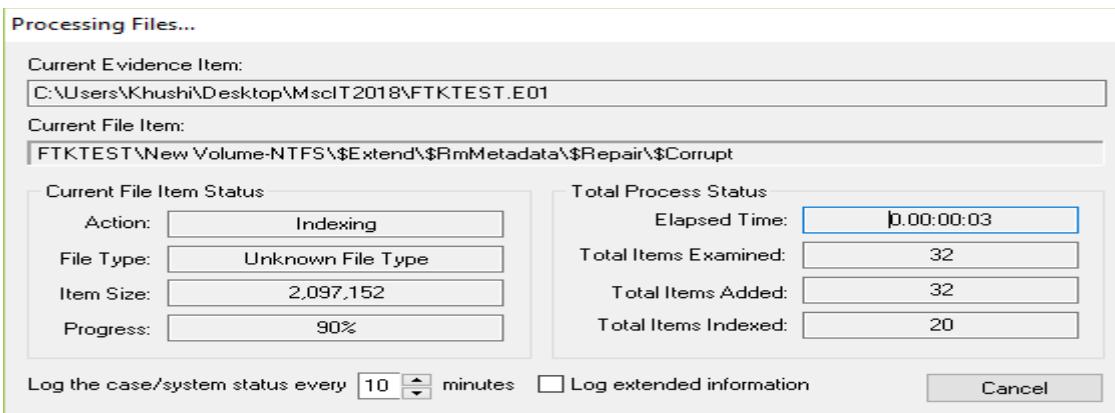
Step 13: Now click on Next.



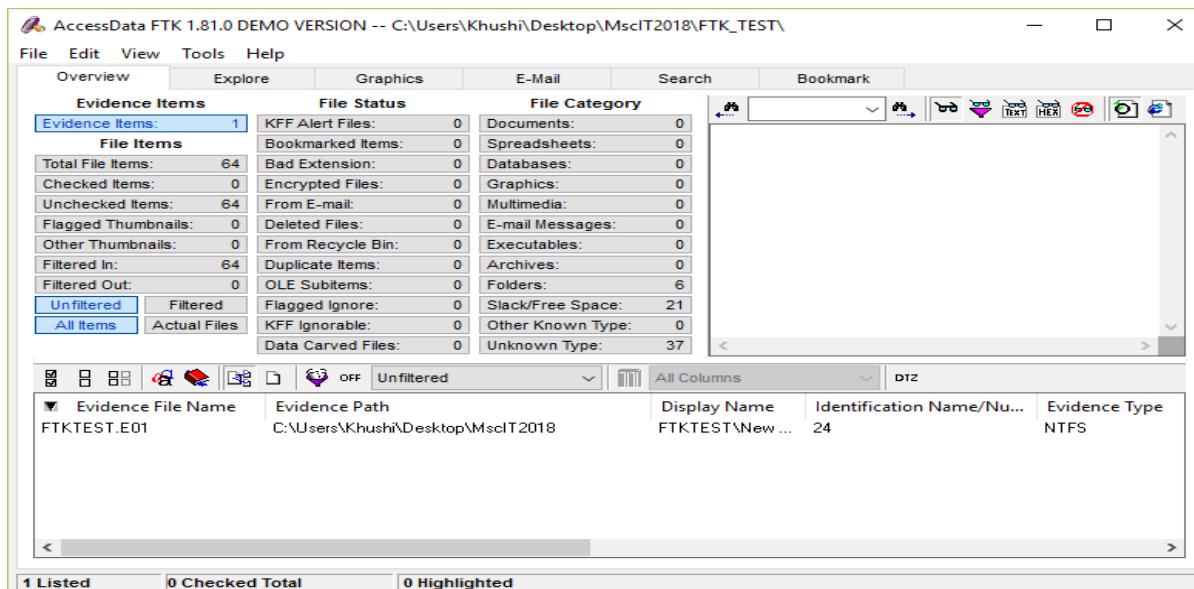
Step 14: Click on Finish to initiate the analysis.



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



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



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

The screenshot shows the FTK interface with the 'Deleted Files' filter applied. The Evidence Items panel shows 7 items. The main pane lists several deleted files:

File Name	Full Path	Recycle Bi...	Ext	File Type	Category
l.out	FTKTEST\NO NAME-FAT32\l.out		out	Unknown Fil...	Unknown
lgf.jpg	FTKTEST\NO NAME-FAT32\lgf.jpg		jpg	Unknown Fil...	Unknown
A-young-boy-proposed-to-a-girl... ACCESSDATA FTK IMAGER3...	FTKTEST\NO NAME-FAT32\A-young-boy-propo...		jpg	Unknown Fil...	Unknown
article-0-147A49E1000005DC...	FTKTEST\NO NAME-FAT32\cf tools\ACCESSD...		zzz	Unknown Fil...	Unknown
Hindu-God-Wallpapers-13.jpg	FTKTEST\NO NAME-FAT32\Hindu-God-Wallpa...		jpg	Unknown Fil...	Unknown
PR0NISCONVERBLELEASE700	FTKTEST\NO NAME-FAT32\cf tools\PR0NIS...		777	Unknown Fil...	Unknown

7 Listed 0 Checked Total 0 Highlighted

Step 18: Select Encrypted Files to view.

The screenshot shows the FTK interface with the 'Encrypted Files' filter applied. The Evidence Items panel shows 1 item. The main pane lists one encrypted file:

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Sub
40488A41374372441D42FB45	FTKTEST\NO NAME-FAT32\cf tools\autopsy-4...			DLE Stream	Unknown	

1 Listed 0 Checked Total FTKTEST\NO NAME-FAT32\cf tools\autopsy-4.0.0-32bit.msi>>40488A41374372441D42FB45

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

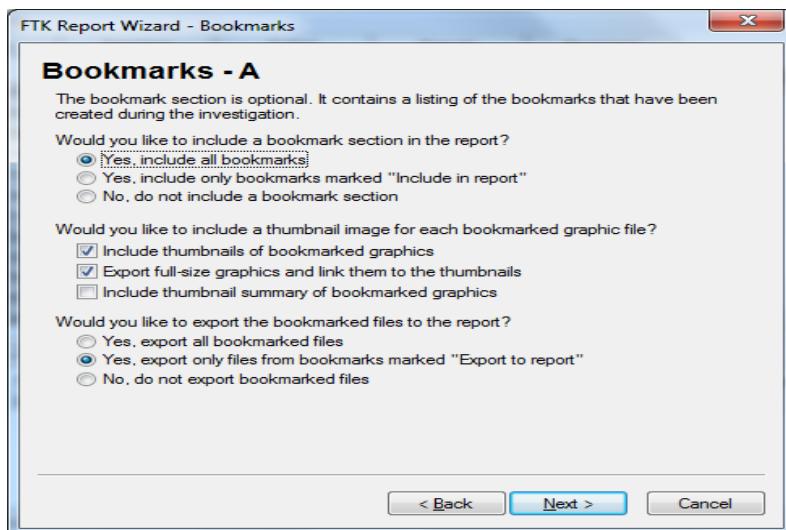
The screenshot shows the FTK interface with the 'Report Wizard...' option selected in the File menu. The main pane displays a table of evidence items:

Display Name	Identification Name/Nu...	Evidence Type
G:\NO NAME-FA...	Storage drive evidence	FAT32

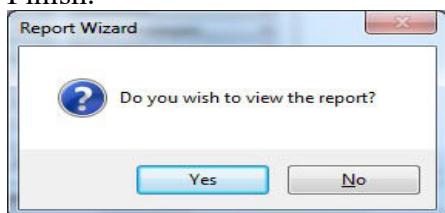
1 Listed 0 Checked Total G:\



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 FTK CASE REPORT interface. On the left is a navigation menu with sections like Case Summary, Supplementary Files, List by File Path, MS Access database, List File Properties, Selected Bookmarks, and Selected Graphic Thumbnails. The main area is titled "File Overview" and displays various 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, Bookmarked Items: 3, Bad Extension: 0, Encrypted Files: 2, From E-mail: 0, Deleted Items: 393, From Recycle Bin: 0, Duplicate Items: 185, OLE Subitems: 73, Flagged Ignore: 0, KFF Ignorable: 0, Data Carved Files: 1,382
- File Category:** Documents: 506, Spreadsheets: 4, Databases: 0, Graphics: 808, Multimedia: 0, Email Messages: 0, Executables: 0, Archives: 25, Folders: 25, Slack/Free Space: 176, Other Known Type: 31, Unknown Type: 53

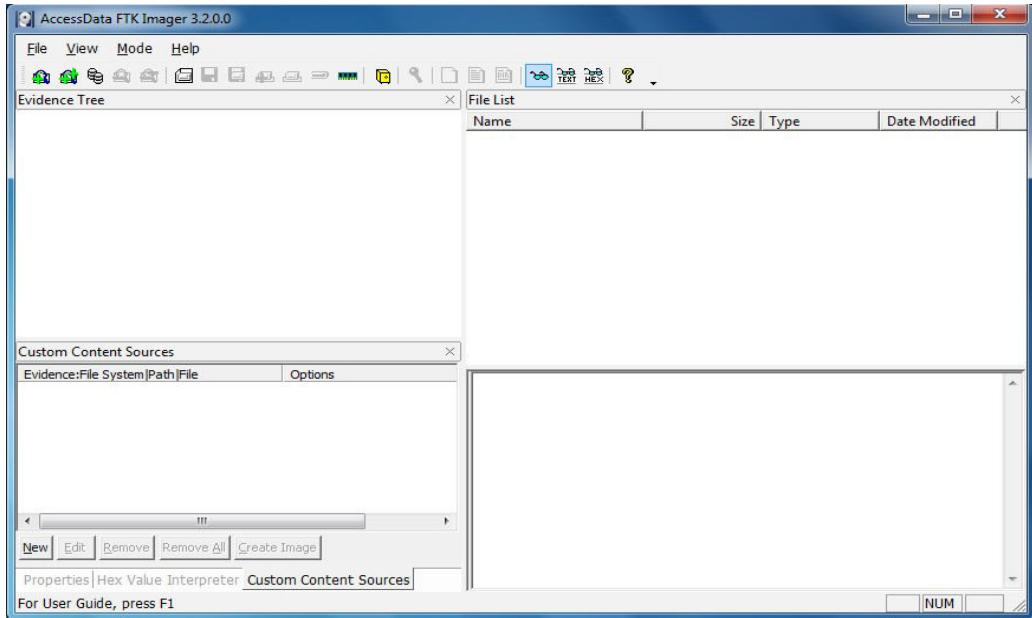
The browser address bar shows "file:///D:/CF%20pracs/backup/report/index.htm".

PRACTICAL NO:04

Using File Recovery Tools [FTK Imager] Creating Image

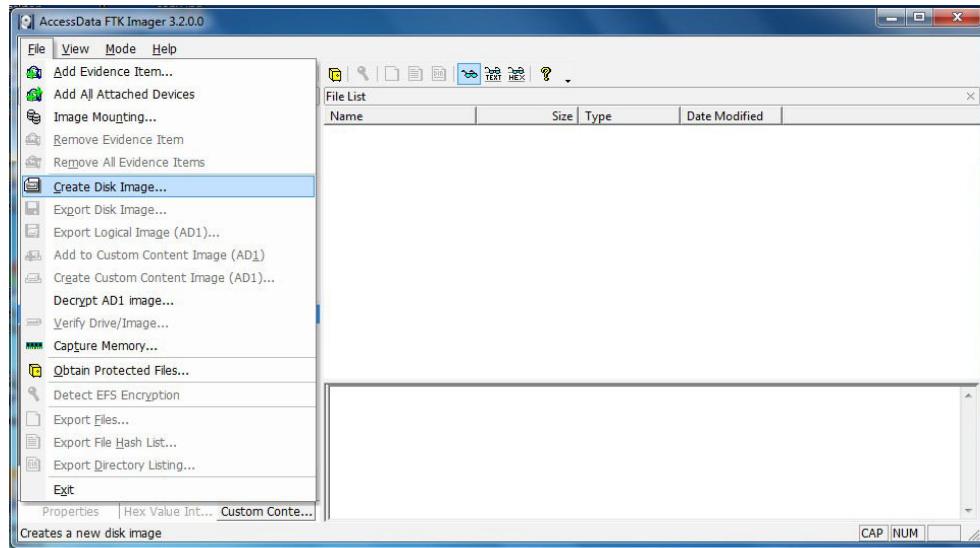
Aim: Understanding & working with the process of the process of taking a drive image using AccessData's FTK Imager tool.

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



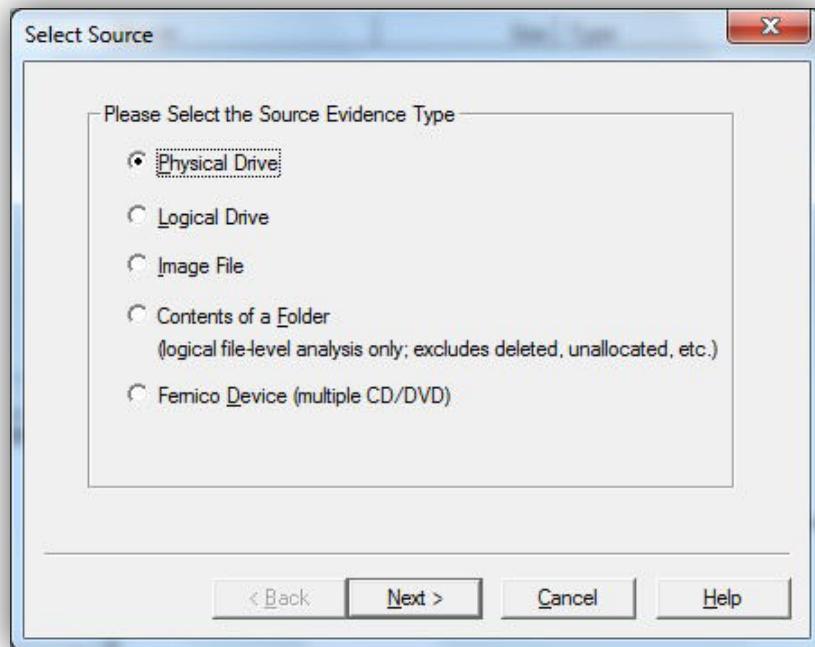
Step 2) To create a forensic image:

Click File > Create Disk Image

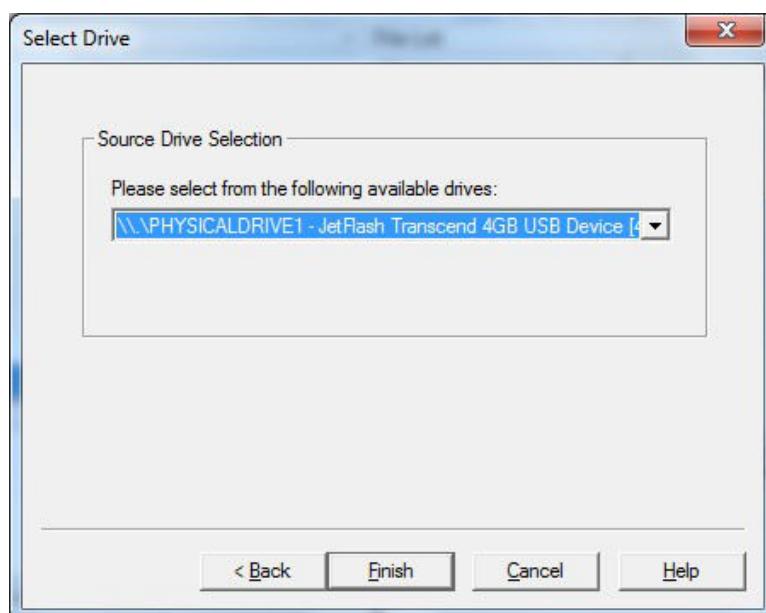


Step 3) In the Select Source dialog box, select the source you want to make an image of. Click Next.

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



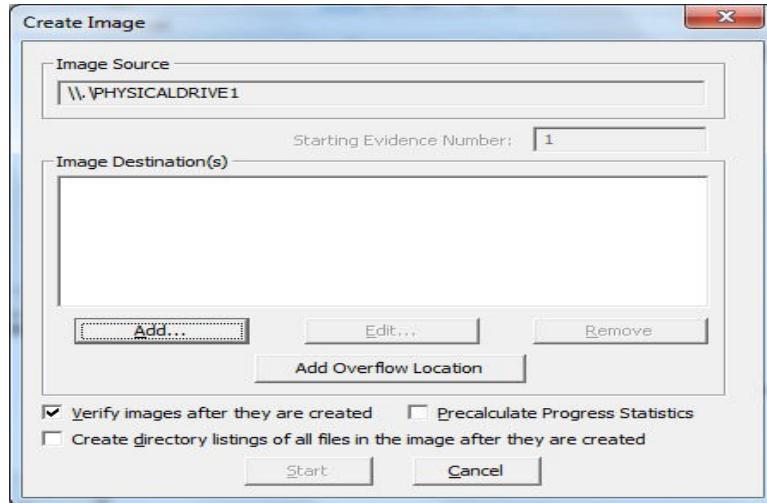
Step 4) Select the drive or browse to the source of the image you want, and then click Finish.



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

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

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

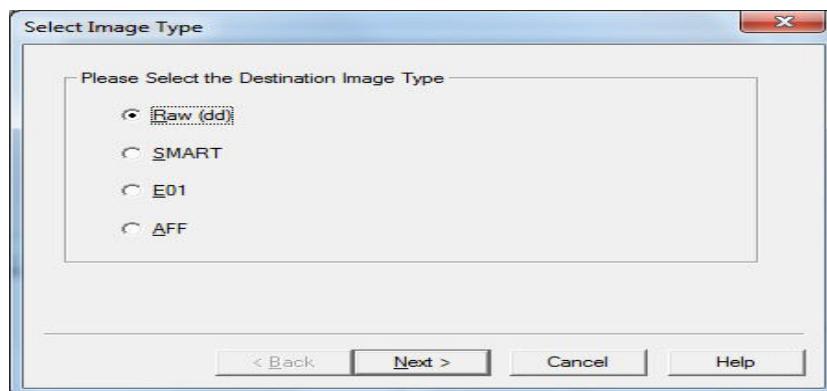


Step 6) Select the type of image you want to create.

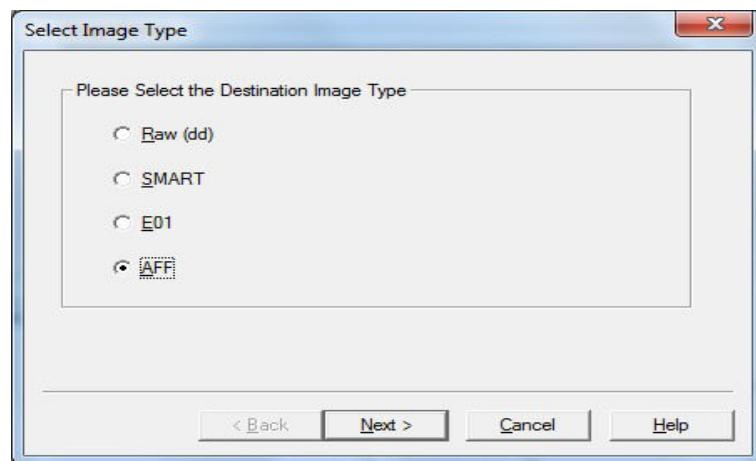
The type you choose will usually depend on what tools you plan to use on the image. The dd format will work with more open-source tools, but you might want SMART or E01 if you will primarily be working with ASR Expert Witness or EnCase, respectively.

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

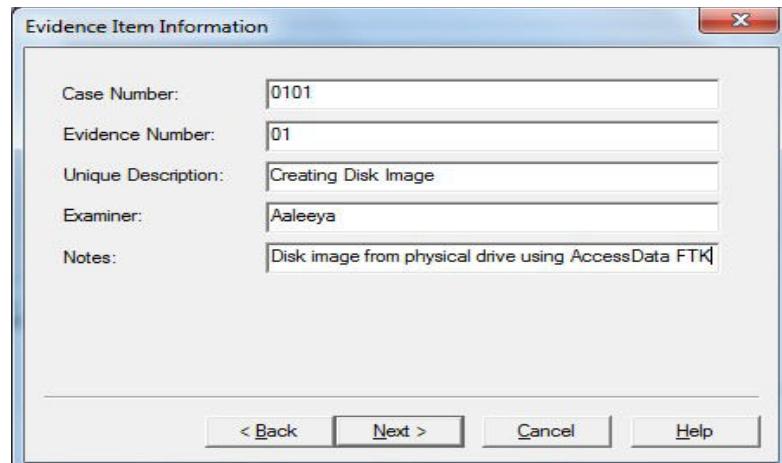
Important: The raw image type is not compressed. If you select the Raw (dd) type, be sure to have adequate available drive space for the resulting image.



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



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



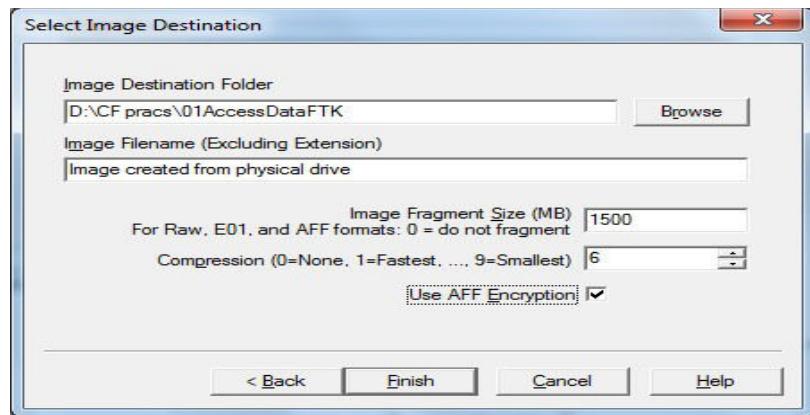
Complete the fields in the Evidence Item Information dialog. Click Next.

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

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

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

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



Step 10) Specify the Image fragment Size:

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

Step 10 a) Select the compression level to use.

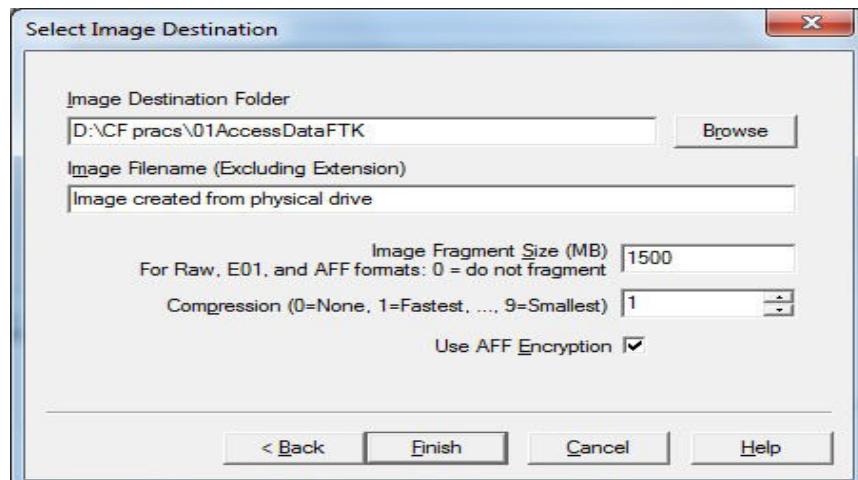
- 0=No Compression
- 1=Fastest, Least Compression (faster, and also slightly smaller than a 0-compression file)
- 9=Slowest, Most Compression (smallest file, slowest to create).

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

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

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

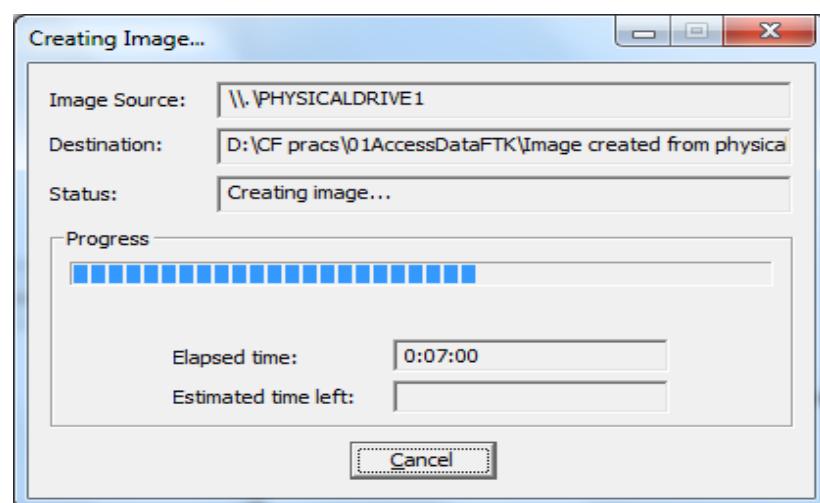
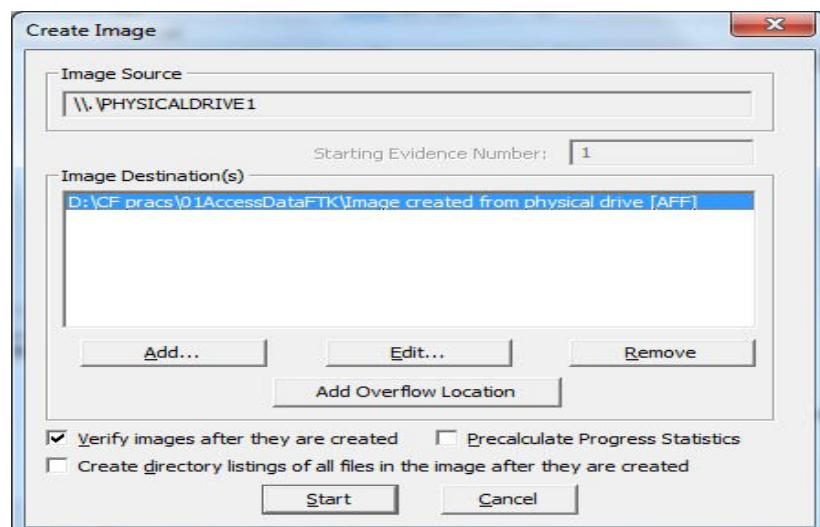
Step 12) Click Finish.



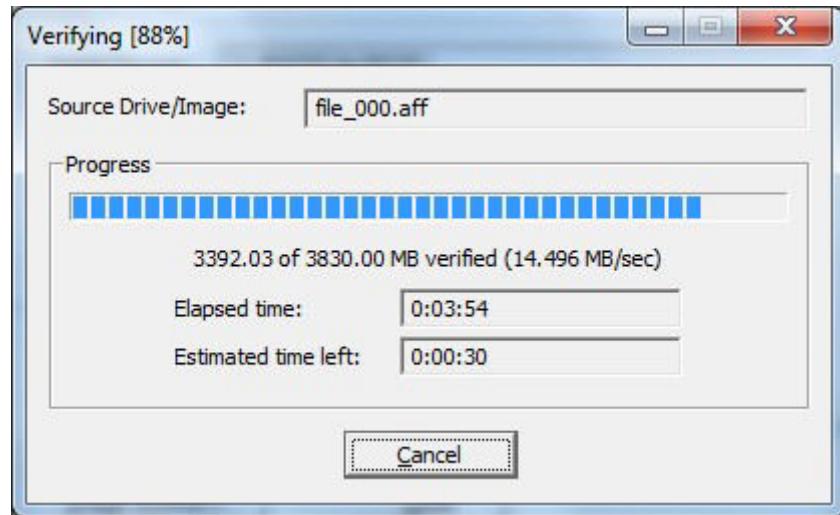
Step 13) When AFF Encryption is selected, type the password, and retype the password to confirm. Click Show Password to see that you have typed it correctly the first time.



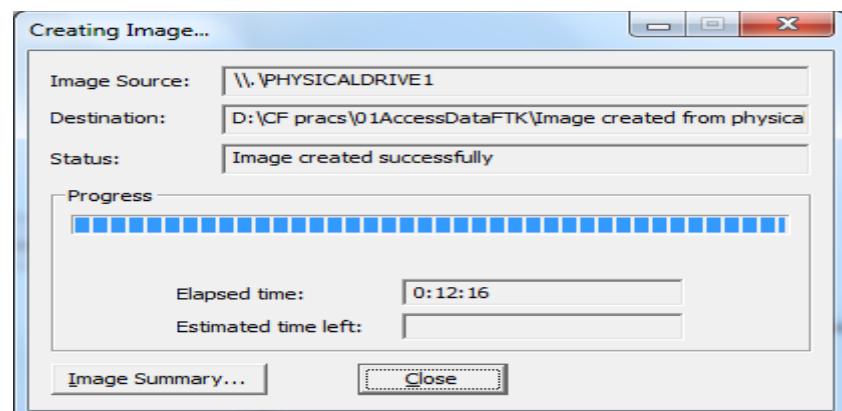
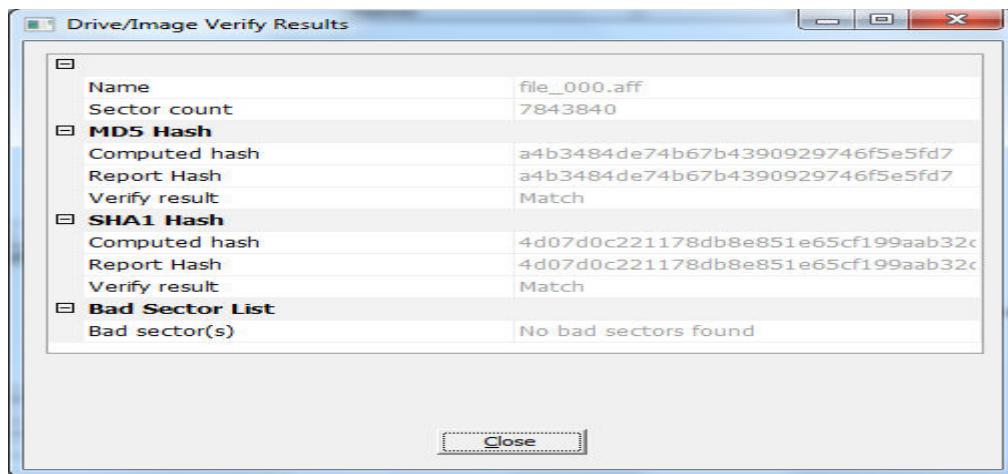
Step 14) When encryption selections are made, click **OK** to save selections and return to the **Create Image dialog**. Click **Start** to begin the imaging process.



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.

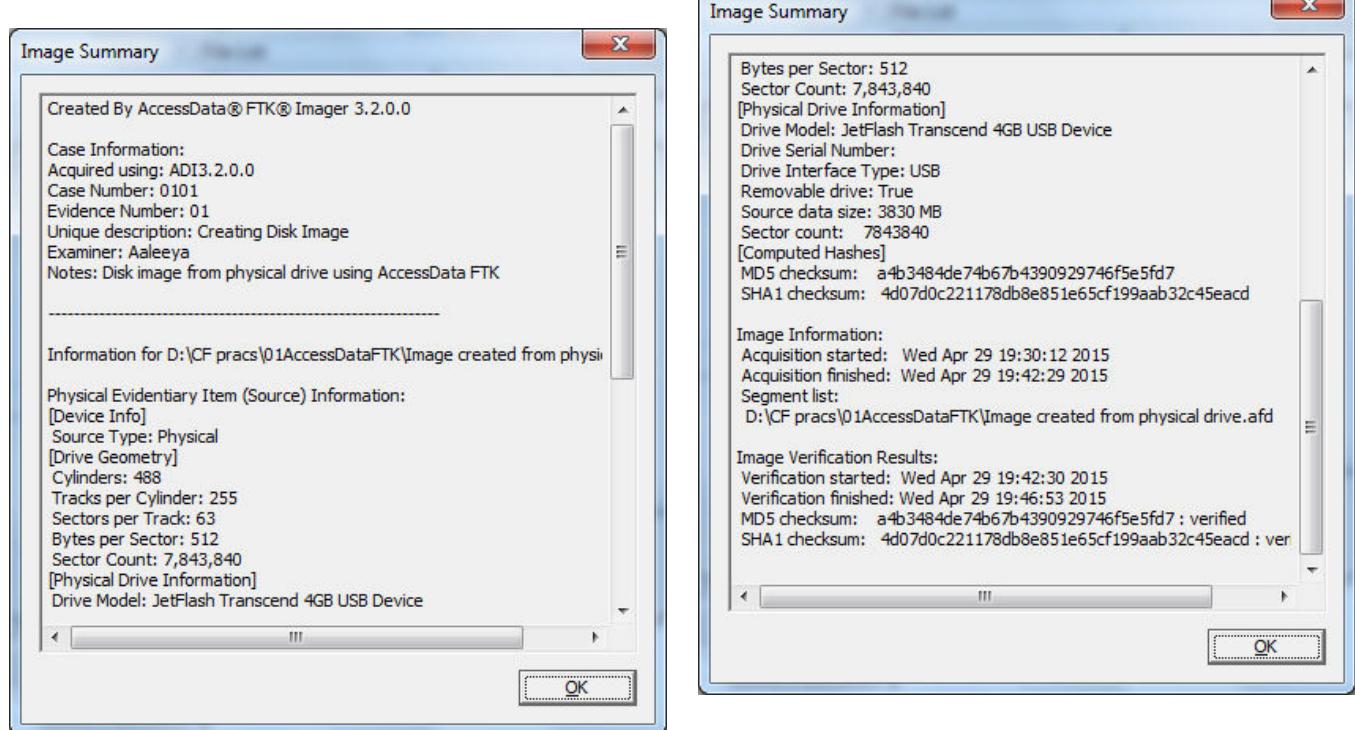


Now is a good time to refill that coffee cup! Once the acquisition is complete, you can view an image summary and the drive will appear in the evidence list in the left-hand side of the main FTK Imager window. You can right-click on the drive name to Verify the Image:



A progress dialog appears that shows the following:

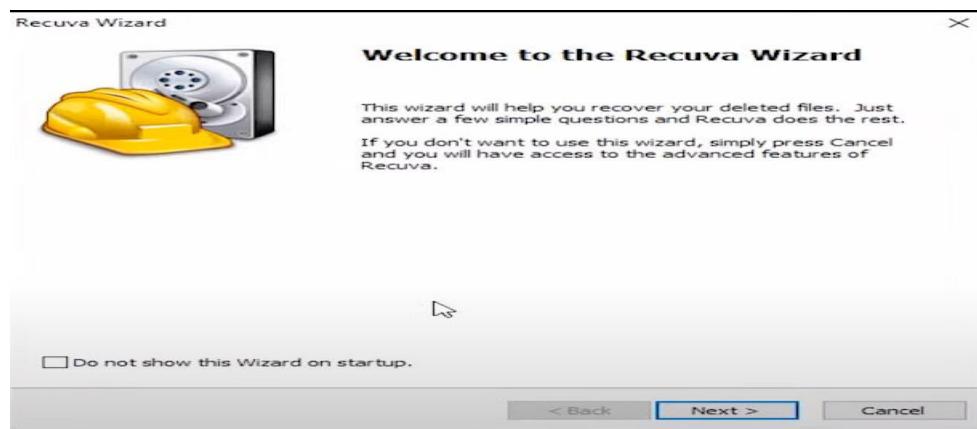
- The source that is being imaged
- The location where the image is being saved
- The status of the imaging process
- A graphical progress bar
- The amount of data in MB that has been copied and the total amount to be copied
- Elapsed time since the imaging process began
- Estimated time remaining until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



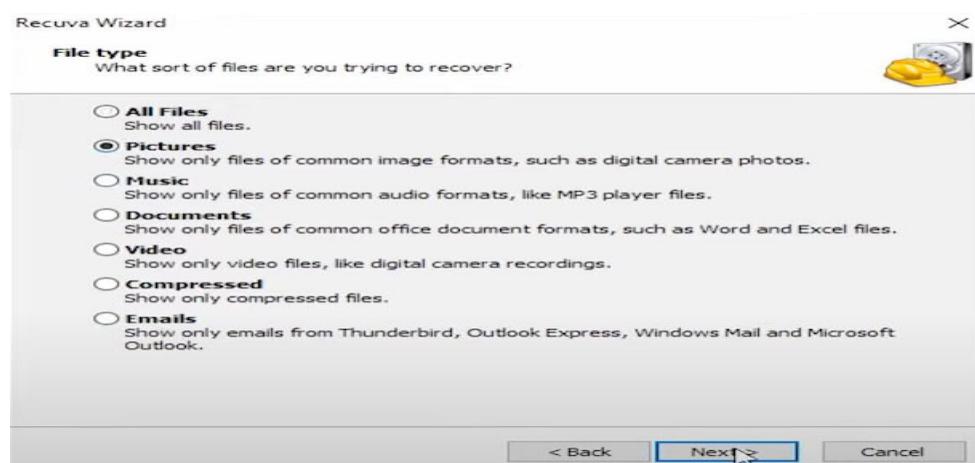
b. Recover Deleted files using Recuva, PC Inspector File Recovery, Recover My Files

Recuva

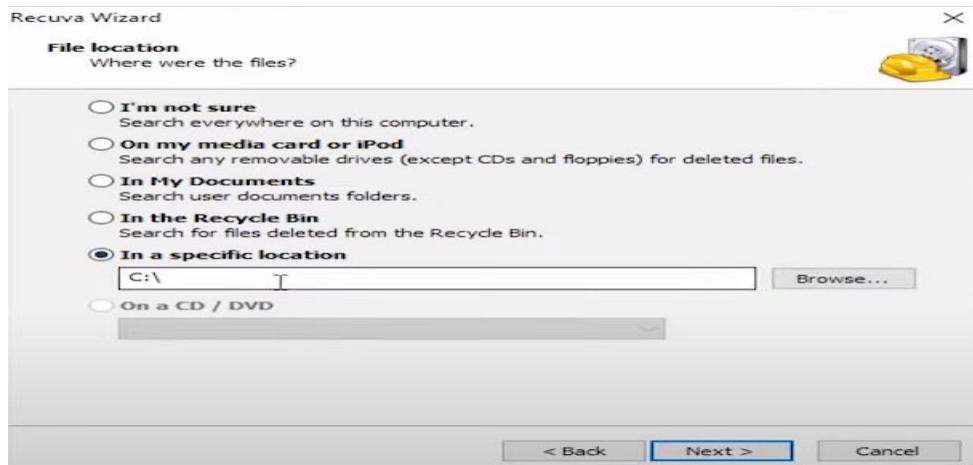
Download and install Recuva



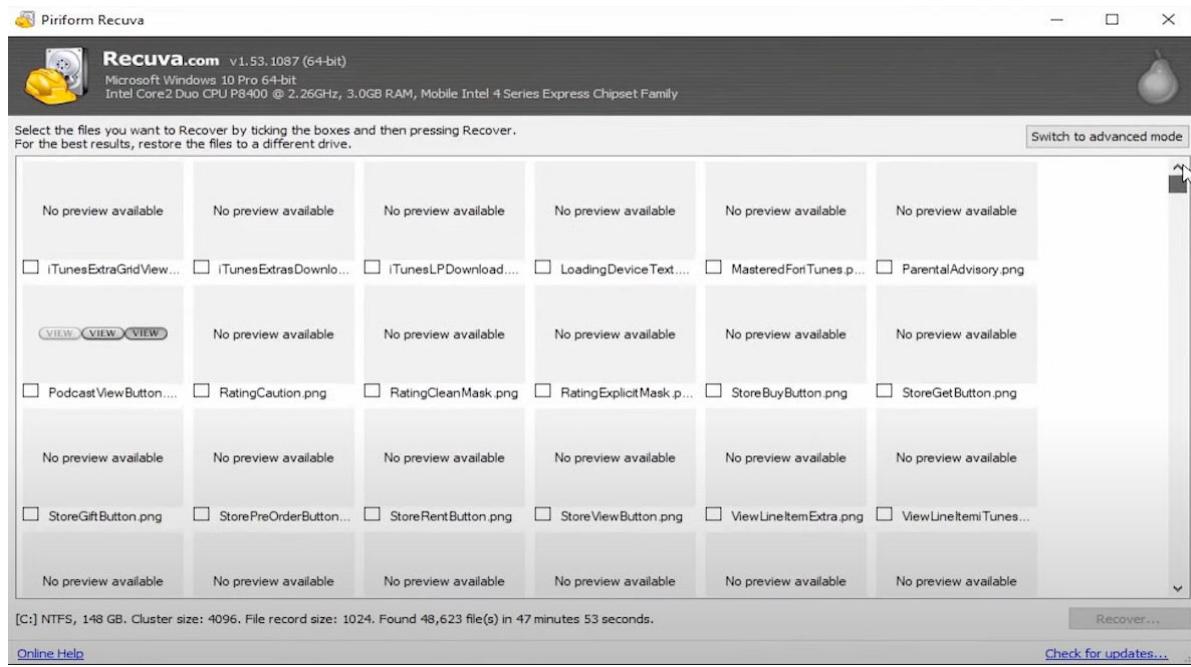
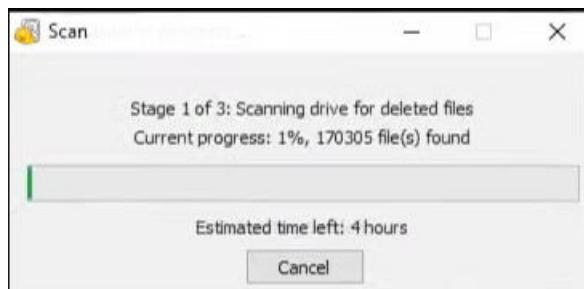
Select File Type you need to recover



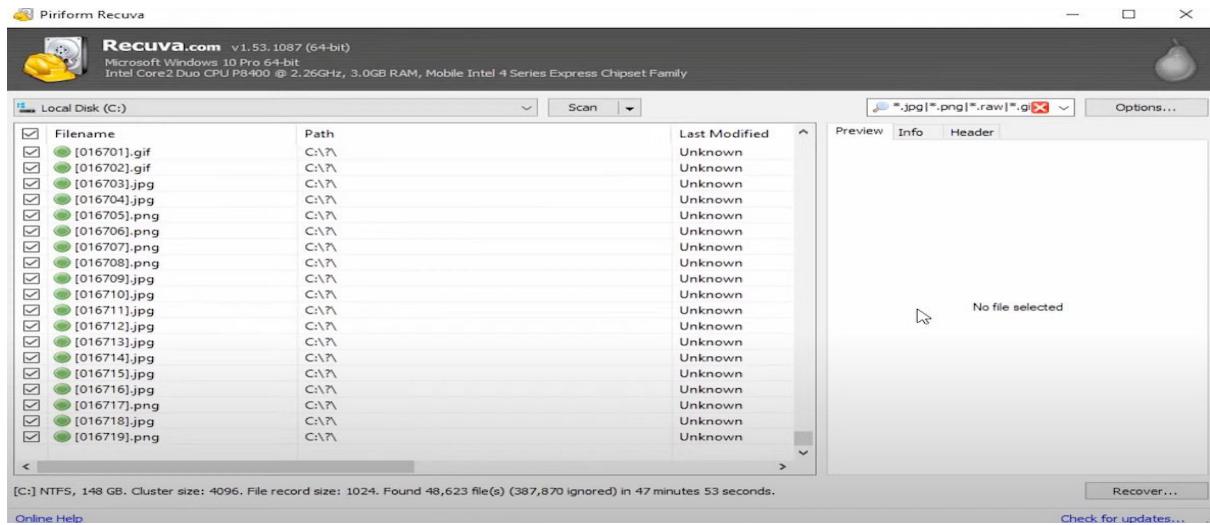
Select File location, which you want to recover files



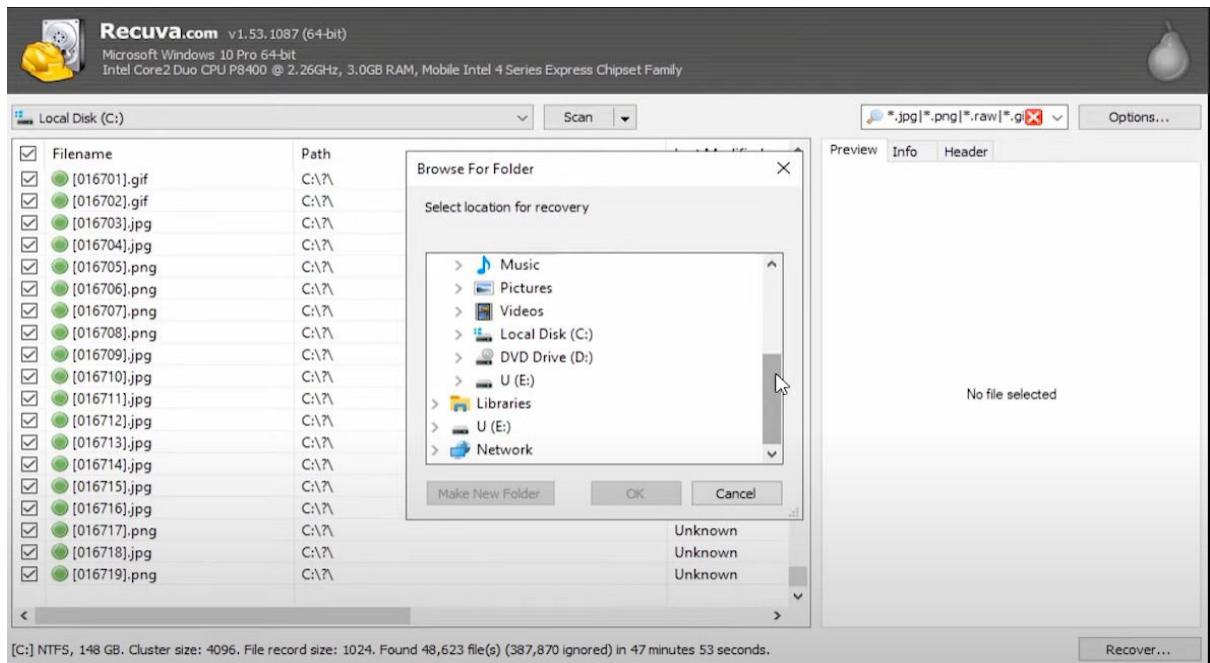
Click next (If want enable Deep Scan)



Switch to advanced mode and select all recover file



Select the location where to recover the file

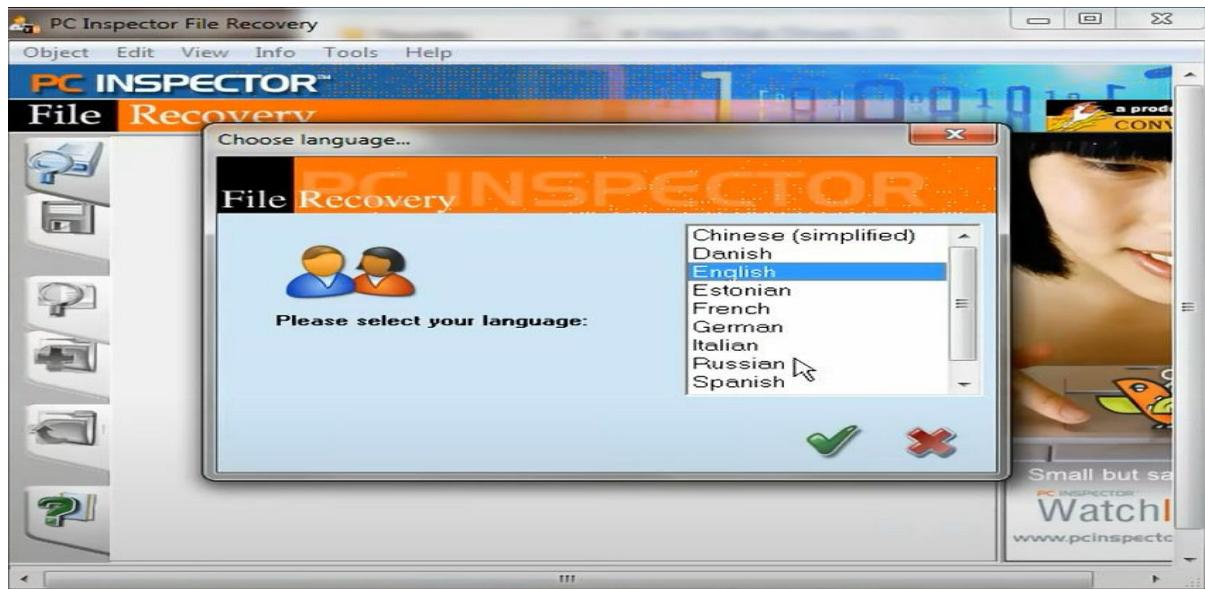




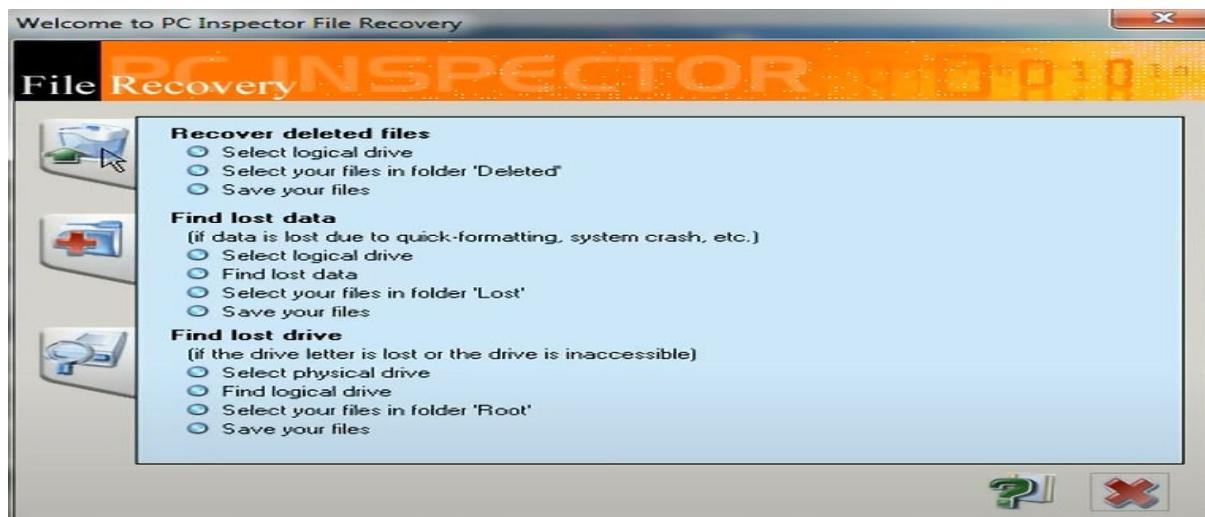
All deleted Files are recovered at specified location

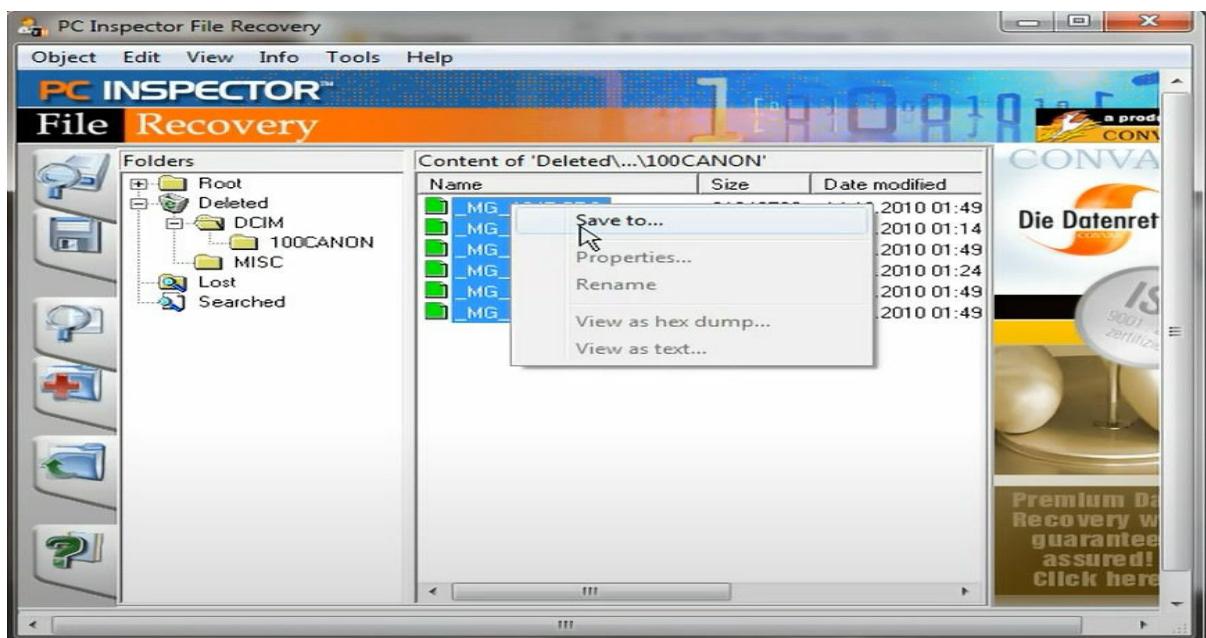
PC Inspector File Recovery

Download and install PC Inspector File Recovery

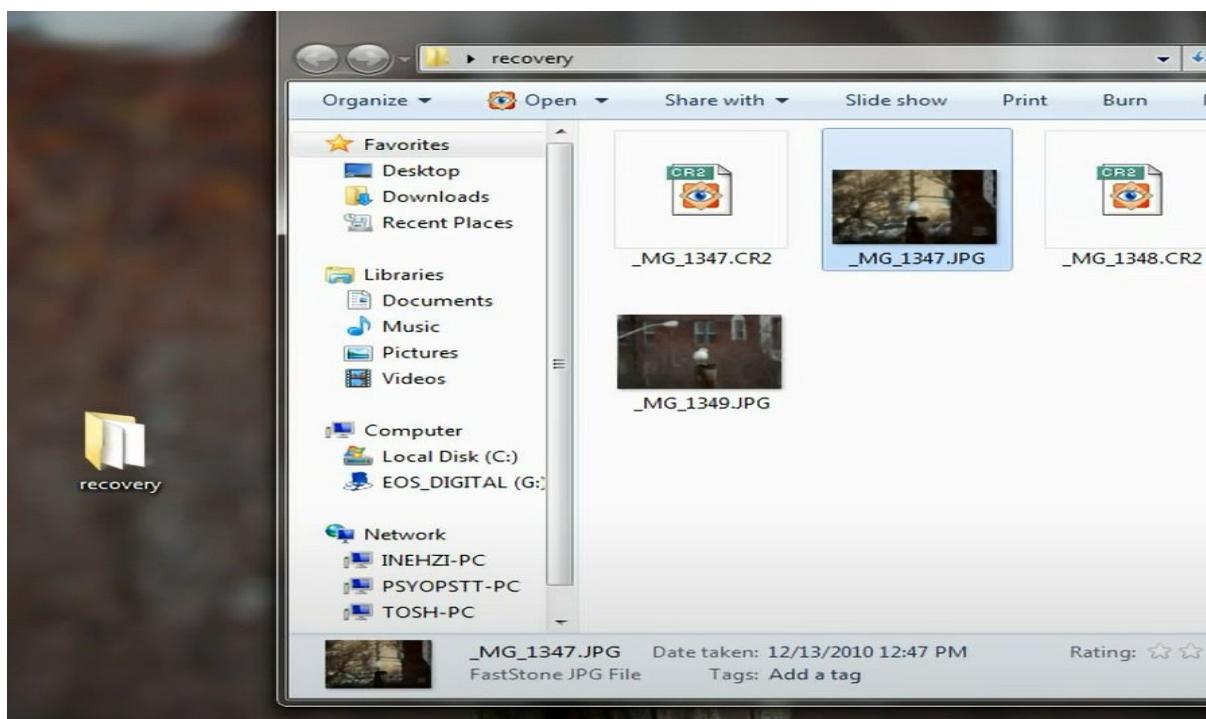


Choose what to recover delete files, lost data or lost drive





Recover data is saved to specified location



Recover My Files

Download and install Recover My Files



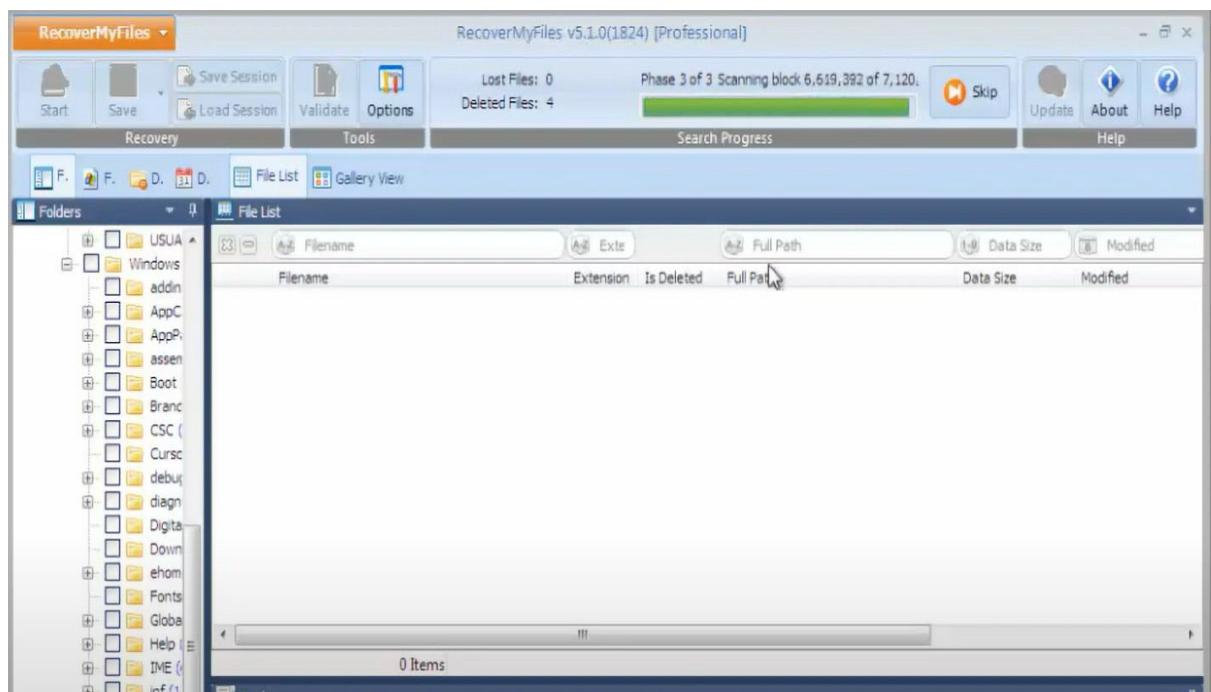
Select the option you wish to of Recover Files and Recover a Drive



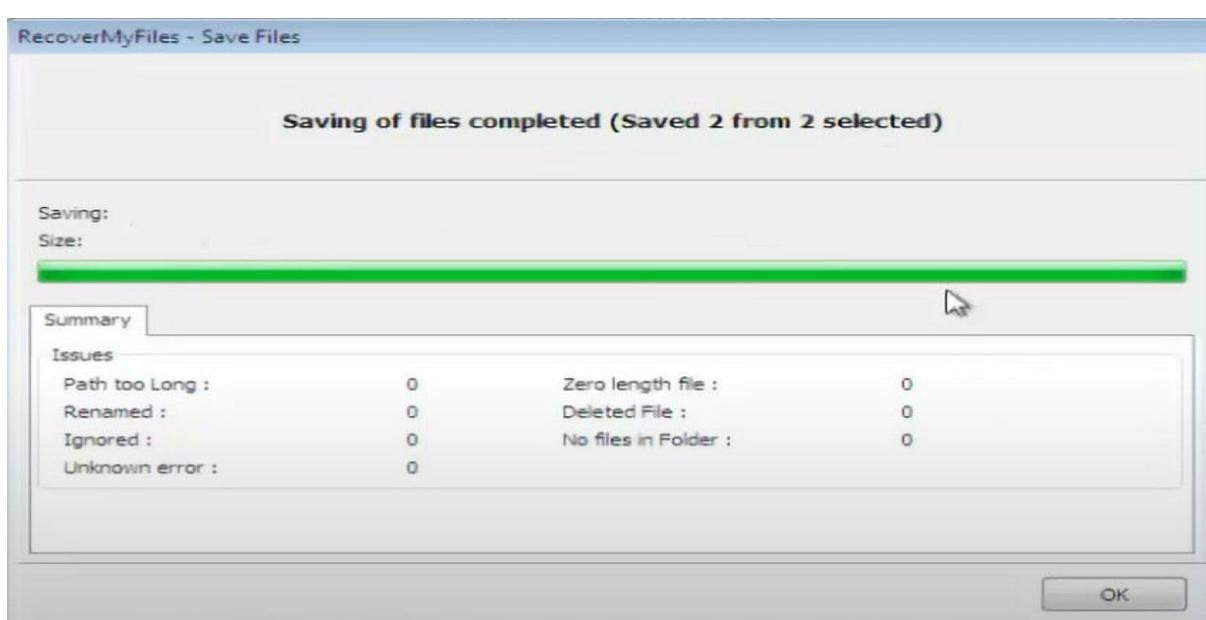
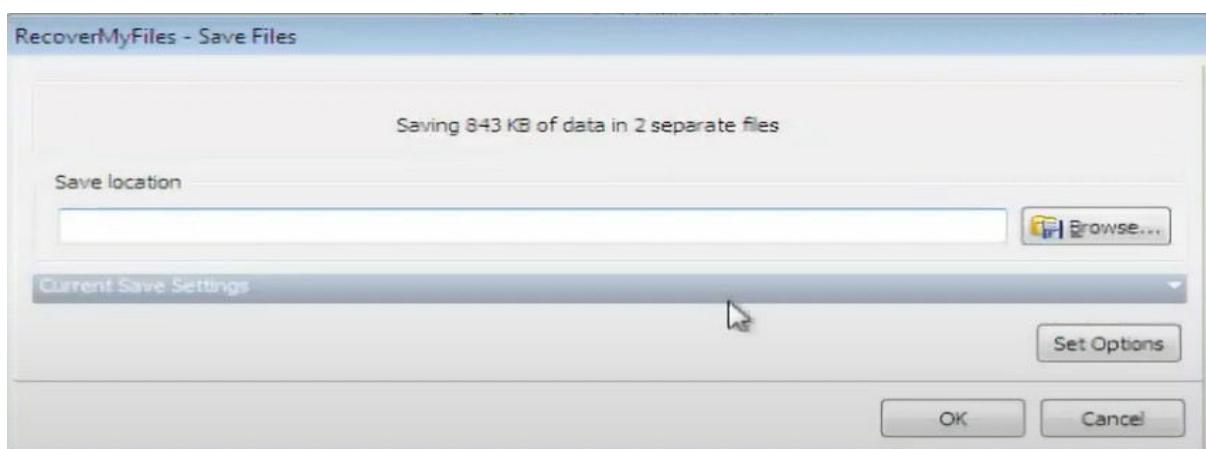
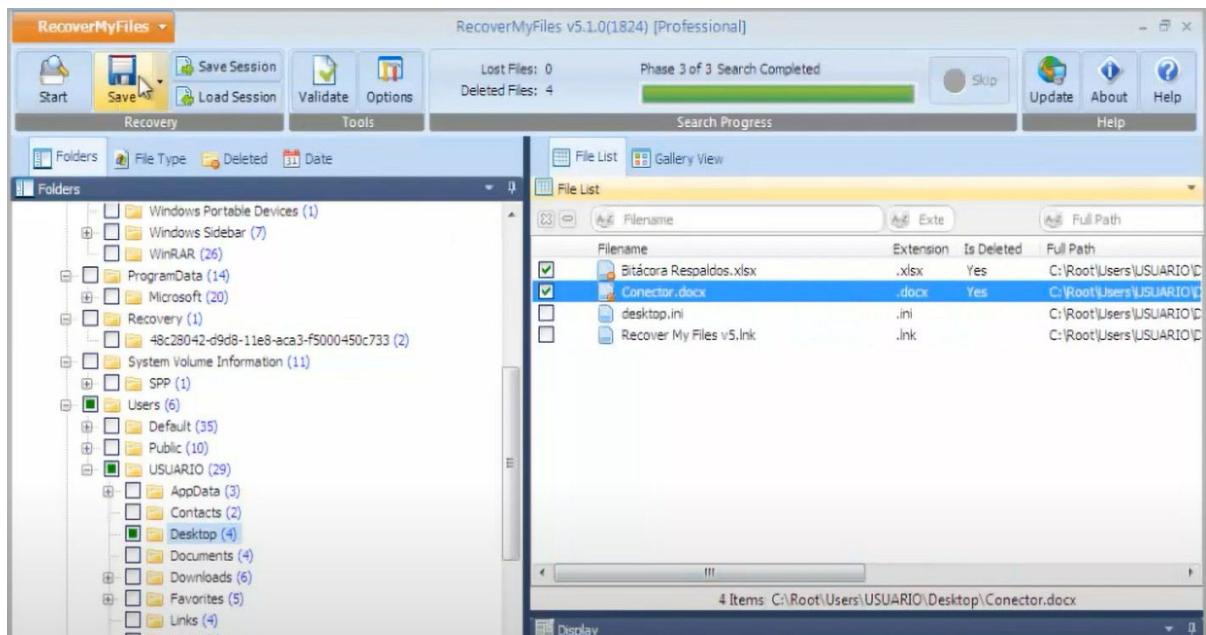
Select the drive to search and recover files & select one of the File Recovery options



What file headers would like to search from recover files



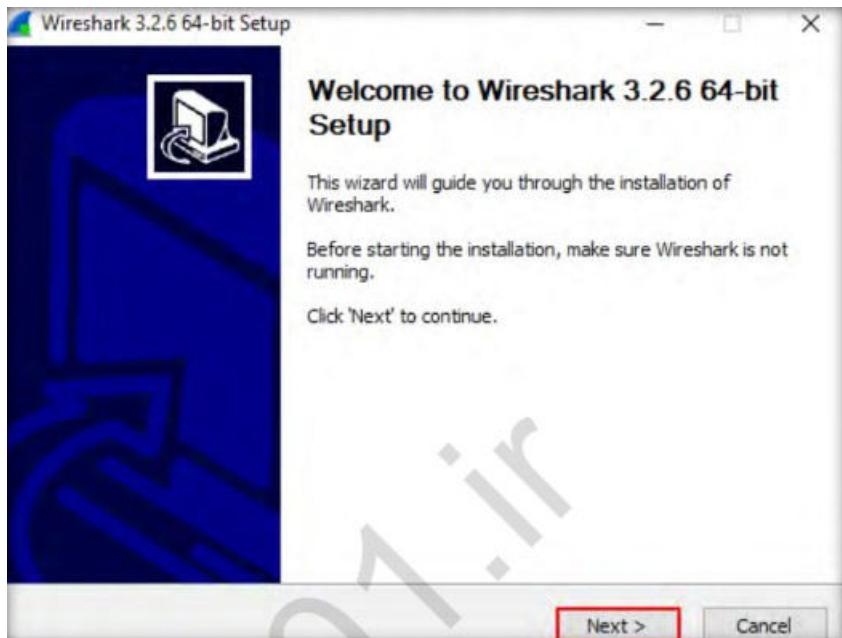
Scan and save the recovered file to desired location



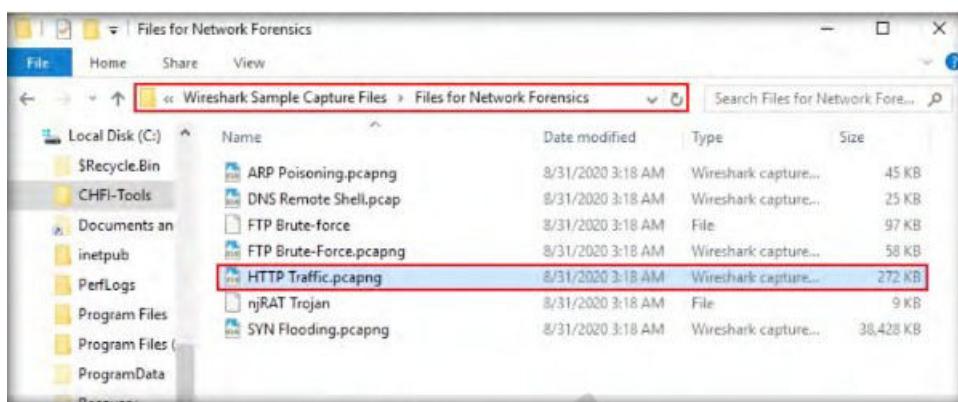
PRACTICAL NO :05

a. Using Web attack detection tools [Wireshark]

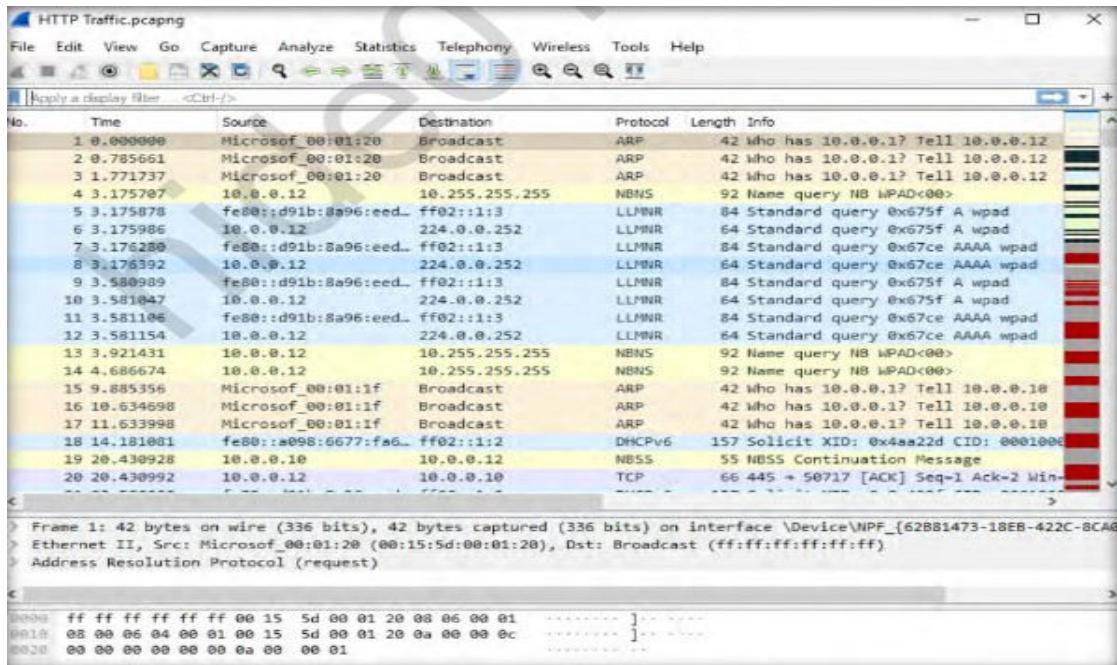
1. Download and install wireshark



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



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

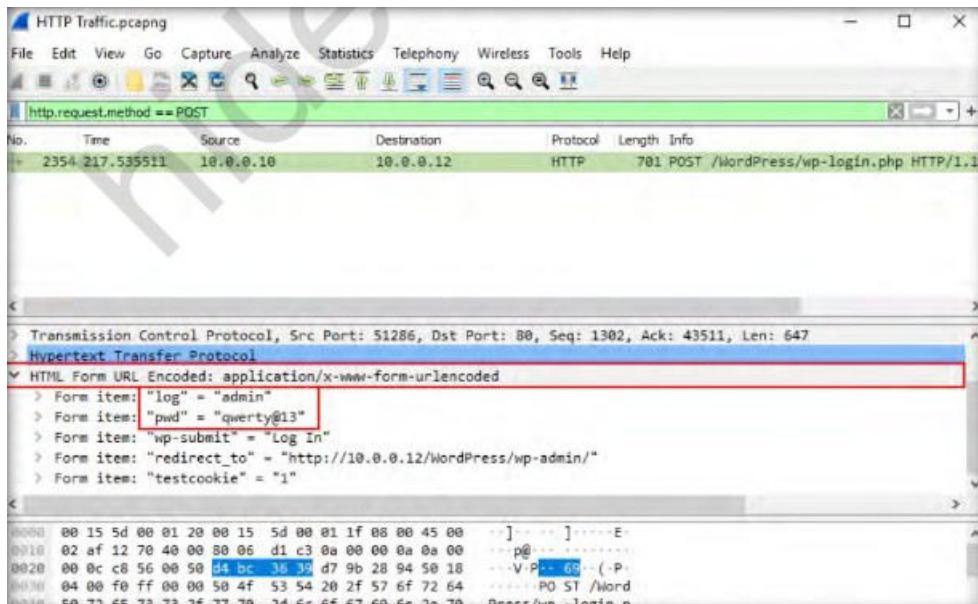
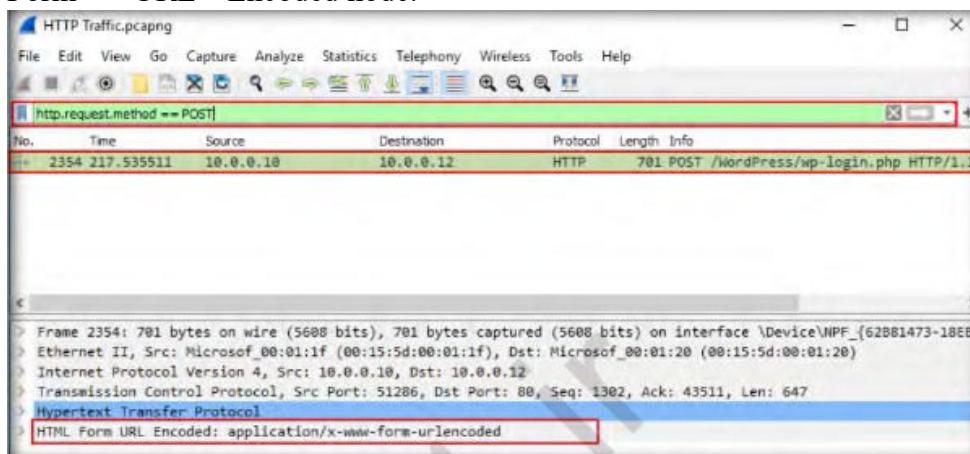


4. We will now apply the http filter so that the application displays results related to traffic generated through http. Type http in the Filter field and press Enter to filter the http traffic, as indicated in the screenshot below:

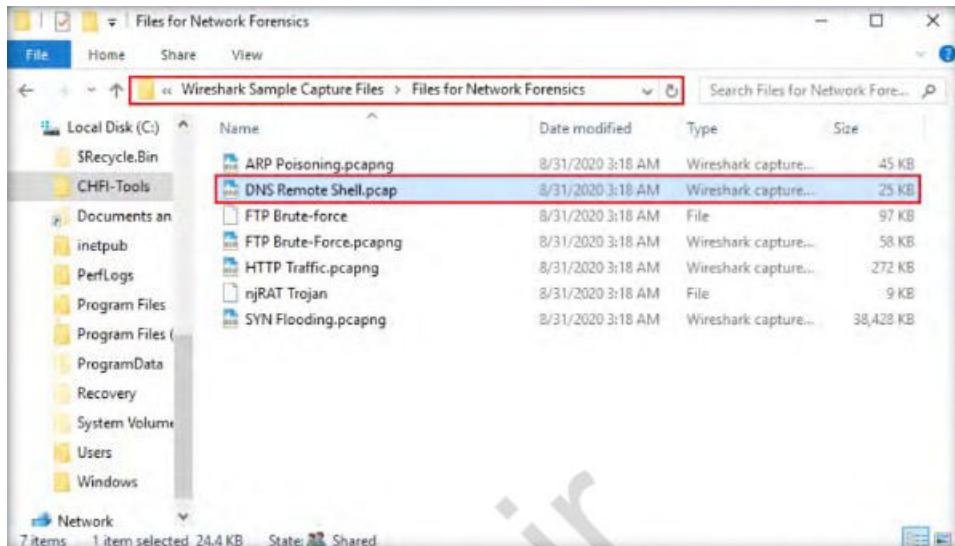
No.	Time	Source	Destination	Protocol	Length	Info
99	125.077129	10.0.0.10	10.0.0.12	HTTP	380	GET /wordpress/ HTTP/1.1
100	128.721380	10.0.0.12	10.0.0.10	HTTP	2157	HTTP/1.1 200 OK (text/html)
2336	211.183512	10.0.0.10	10.0.0.12	HTTP	392	GET /wordpress/wp-login.php HTTP/1.1
2338	211.583319	10.0.0.12	10.0.0.10	HTTP	2908	HTTP/1.1 200 OK (text/html)
2340	211.599547	10.0.0.10	10.0.0.12	HTTP	534	GET /WordPress/wp-admin/load-styles.php?
2348	211.965283	10.0.0.12	10.0.0.10	HTTP	59	HTTP/1.1 200 OK (text/css)
2350	212.444275	10.0.0.10	10.0.0.12	HTTP	537	GET /WordPress/wp-admin/images/wordpress
2352	212.516662	10.0.0.12	10.0.0.10	HTTP/X-	1873	HTTP/1.1 200 OK
2354	217.535511	10.0.0.10	10.0.0.12	HTTP	701	POST /WordPress/wp-login.php HTTP/1.1 (
2356	218.046162	10.0.0.12	10.0.0.10	HTTP	3901	HTTP/1.1 200 OK (text/html)

Frame 99: 380 bytes on wire (3040 bits), 380 bytes captured (3040 bits) on interface \Device\NPF_{62BB1473-18EB-422C-8CA0
Ethernet II, Src: Microsoft_00:01:20 (00:15:5d:00:01:20), Dst: Microsoft_00:01:20 (00:15:5d:00:01:20)
Internet Protocol Version 4, Src: 10.0.0.10, Dst: 10.0.0.12
Transmission Control Protocol, Src Port: 51263, Dst Port: 80, Seq: 1, Ack: 1, Len: 326
Hypertext Transfer Protocol

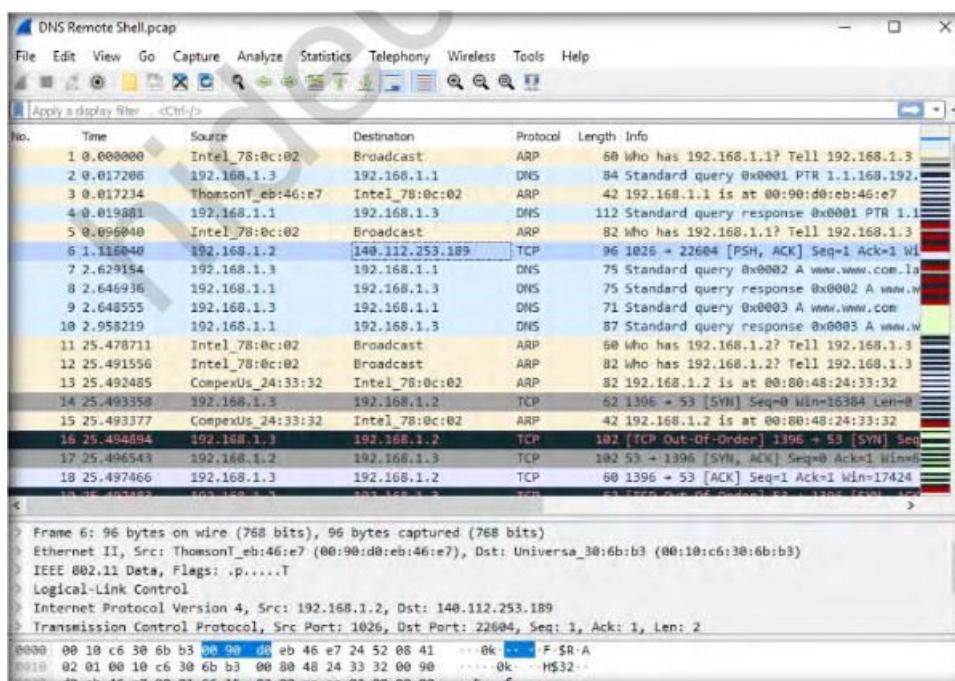
5. After examining the entries displayed by the application in the screenshot above, it is evident that the http traffic is associated with a WordPress website, and it is being transmitted in a plain text format. Generally, user credentials are stored in the POST requests. Therefore, examining packet(s) containing POST request can help an investigator find the user credentials.
6. We will now filter the traffic to obtain results specific only to POST request(s). Now, type http.request.method== POST in the Filter field and press Enter. Wireshark filters the traffic containing POST request(s) and displays them, as shown in the screenshot below. The user credentials stored in this request can be found under the Packet Details pane in the middle of the application window, under the HTML Form URL Encoded node.



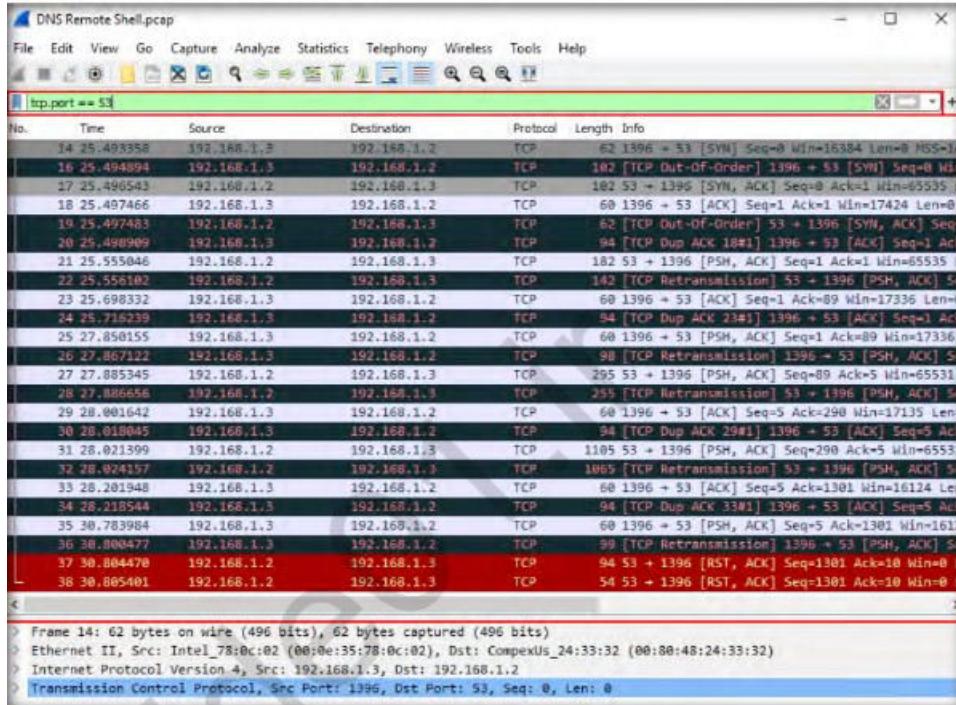
7. Now, navigate to C:\CHFI-Tools\Evidence Files\Wireshark Files\Files for Network Forensics and double-click DNS RemoteShell.pcapng.



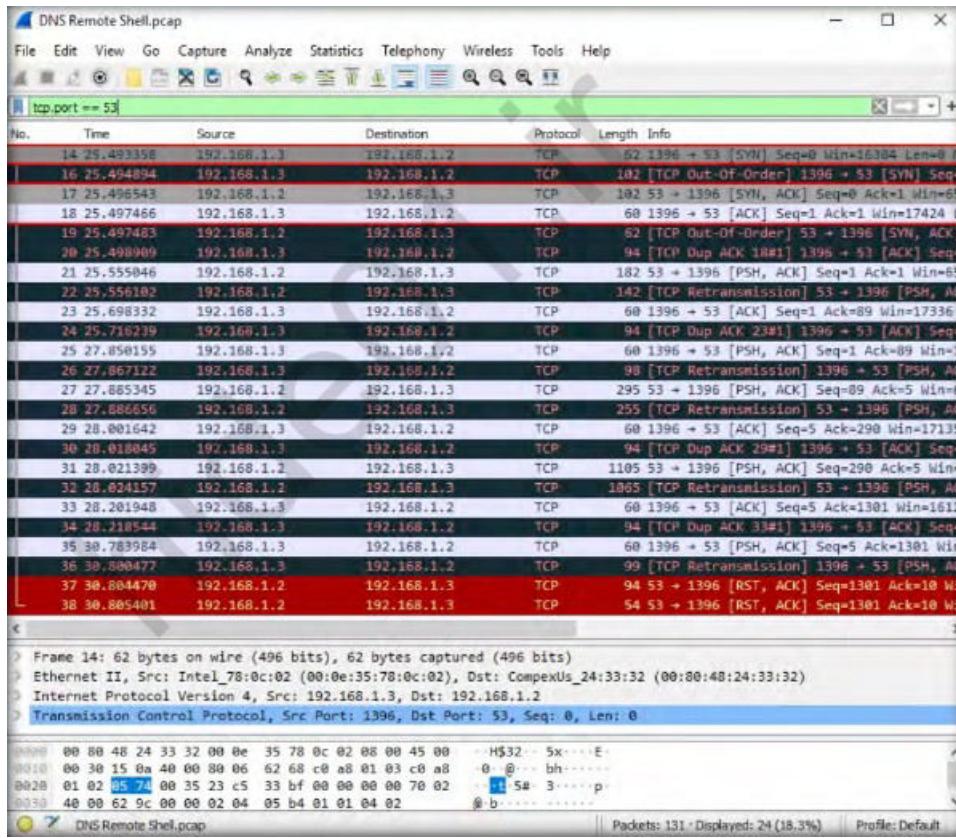
8. The network traffic entries captured in the DNS Remote Shell.pcapng file will now be displayed in the Wireshark GUI window, as shown in the following screenshot



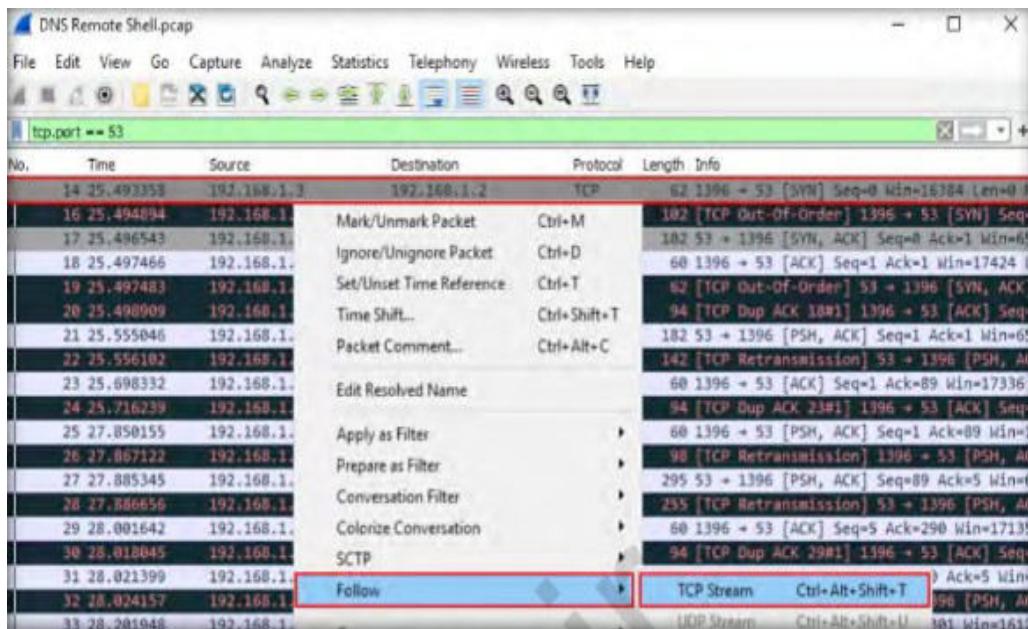
9. Since DNS uses port 53 for communicating with clients, we will be filtering the traffic flowing to and from port 53. To filter traffic flowing on port 53, type the command `tcp.port == 53` in the Filter field and press Enter. Wireshark filters the traffic flowing on port 53 and displays it, as shown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



When we examine the first packet from the listed packets, i.e., Packet 14, we can see that Port 1396 on Source IP address (192.168.1.3) is trying to establish a remote connection with Port 53 on the Destination IP address(192.168.1.2) through a [SYN] request. As Port 53 is seen on 192.168.1.2, this IP address represents the DNS server here. When we examine 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      @ aerrorlog.txt
01/19/2004 09:45 PM      @ AUTOEXEC.BAT
01/19/2004 09:45 PM      @ CONFIG.SYS
06/26/2004 12:12 PM    <DIR>      Documents and Settings
02/03/2005 11:40 PM    <DIR>      EasyBoot
02/29/2004 02:53 PM    11,531 installer-debug.txt
12/19/2004 12:58 AM    <DIR>      mga
12/19/2004 12:51 AM    <DIR>      mgafold
11/24/2004 07:47 PM    <DIR>      mnt
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
10/31/2004 08:36 PM    @ s3fs
06/02/2004 08:54 PM    123 systemscandata.txt
08/08/2004 10:48 AM    <DIR>      Temp
12/12/2004 02:24 PM    84,135,944 temp.wmv
01/13/2005 06:10 PM    <DIR>      WINDOWS
11/26/2004 09:27 AM    <DIR>      WOTemp

2 client pkts, 3 server pkts, 3 bytes.

Entire conversation (1309 bytes) Show and save data as ASCII Stream 1
Find: Filter Out This Stream Print Save as... Back Close Help

```

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

Name	Date modified	Type	Size
ARP Poisoning.pcapng	8/31/2020 3:18 AM	Wireshark capture...	45 KB
DNS Remote Shell.pcap	8/31/2020 3:18 AM	Wireshark capture...	25 KB
FTP Brute-force	8/31/2020 3:18 AM	File	97 KB
FTP Brute-Force.pcapng	8/31/2020 3:18 AM	Wireshark capture...	56 KB
HTTP Traffic.pcapng	8/31/2020 3:18 AM	Wireshark capture...	272 KB
njRAT Trojan	8/31/2020 3:18 AM	File	9 KB
SYN Flooding.pcapng	8/31/2020 3:18 AM	Wireshark capture...	38,428 KB

FTP Brute-Force.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000080	10.0.0.8	10.0.0.16	TCP	74	59146 → 21 [SYN] Seq=0 Win=29200
2	0.000122	10.0.0.16	10.0.0.8	TCP	74	21 → 59146 [SYN, ACK] Seq=0 Ack=1
3	0.000425	10.0.0.8	10.0.0.16	TCP	66	59146 → 21 [ACK] Seq=1 Ack=1 Win=29200
4	0.000614	10.0.0.16	10.0.0.8	FTP	93	Response: 220 Microsoft FTP Servr
5	0.001184	10.0.0.8	10.0.0.16	TCP	66	59146 → 21 [ACK] Seq=1 Ack=28 Win=29200
6	0.001747	10.0.0.8	10.0.0.16	FTP	78	Request: USER Admin
7	0.001812	10.0.0.16	10.0.0.8	FTP	89	Response: 331 Password required
8	0.002109	10.0.0.8	10.0.0.16	FTP	82	Request: PASS admin@123
9	0.002702	10.0.0.16	10.0.0.8	FTP	91	Response: 530 User cannot log in.
10	0.003302	10.0.0.8	10.0.0.16	TCP	66	59146 → 21 [FIN, ACK] Seq=29 Ack=29
11	0.003302	10.0.0.8	10.0.0.16	TCP	74	59146 → 21 [SYN] Seq=0 Win=29200
12	0.003362	10.0.0.16	10.0.0.8	TCP	74	21 → 59146 [SYN, ACK] Seq=0 Ack=1
13	0.003371	10.0.0.16	10.0.0.8	TCP	66	21 → 59146 [ACK] Seq=76 Ack=30 Win=29200
14	0.003402	10.0.0.16	10.0.0.8	TCP	66	21 → 59146 [FIN, ACK] Seq=76 Ack=30
15	0.003718	10.0.0.8	10.0.0.16	TCP	66	59146 → 21 [ACK] Seq=1 Ack=1 Win=29200
16	0.003747	10.0.0.8	10.0.0.16	TCP	66	59146 → 21 [ACK] Seq=38 Ack=77 Win=29200
17	0.003980	10.0.0.16	10.0.0.8	FTP	93	Response: 220 Microsoft FTP Servr
18	0.004598	10.0.0.8	10.0.0.16	TCP	66	59146 → 21 [ACK] Seq=1 Ack=28 Win=29200
19	0.005383	10.0.0.8	10.0.0.16	FTP	78	Request: USER Admin
20	0.005576	10.0.0.16	10.0.0.8	FTP	80	Response: 530 Document nonfound

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\WPF_{6D6E3E22-A278-4896-A6E6-00155d010502

Ethernet II, Src: Microsoft_01:05:0b (00:15:5d:01:05:0b), Dst: Microsoft_01:05:02 (00:15:5d:01:05:02)

Internet Protocol Version 4, Src: 10.0.0.8, Dst: 10.0.0.16

Transmission Control Protocol, Src Port: 59146, Dst Port: 21, Seq: 0, Len: 0

0000 00 15 5d 01 05 02 00 15 5d 01 05 00 08 00 45 00 .] E-
0010 00 3c 8f 40 00 40 06 9e 65 0a 00 00 08 0a 00 < ? @ @ e . .
0020 00 10 e7 0a 00 15 ab ea b6 4d 00 00 00 0a 02 M . .
0030 72 10 a3 d3 00 00 02 04 05 b4 04 02 08 0a 45 b4 E-
0040 94 f8 00 00 00 00 01 03 03 07

Packet(s): 508 (Decapsulated: 508 (100.0%)) | Profile: Default

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 bar at the top indicates the filter: "ftp.response.code == 530". The main pane displays a list of network frames. Most frames are red, representing failed login attempts. One frame is blue, representing a successful login attempt. The blue frame's details are as follows:

No.	Time	Source	Destination	Protocol	Length	Info
9	0.002702	10.0.0.16	10.0.0.8	FTP	91	91 Response: 530 User cannot log in.
22	0.006666	10.0.0.16	10.0.0.8	FTP	91	91 Response: 530 User cannot log in.
35	0.017903	10.0.0.16	10.0.0.8	FTP	91	91 Response: 530 User cannot log in.
48	0.023198	10.0.0.16	10.0.0.8	FTP	91	91 Response: 530 User cannot log in.
61	0.029156	10.0.0.16	10.0.0.8	FTP	91	91 Response: 530 User cannot log in.
74	0.034603	10.0.0.16	10.0.0.8	FTP	91	91 Response: 530 User cannot log in.
87	0.039848	10.0.0.16	10.0.0.8	FTP	91	91 Response: 530 User cannot log in.
100	0.046571	10.0.0.16	10.0.0.8	FTP	91	91 Response: 530 User cannot log in.
113	0.051485	10.0.0.16	10.0.0.8	FTP	91	91 Response: 530 User cannot log in.
126	0.060423	10.0.0.16	10.0.0.8	FTP	91	91 Response: 530 User cannot log in.
139	0.069622	10.0.0.16	10.0.0.8	FTP	91	91 Response: 530 User cannot log in.
152	0.076802	10.0.0.16	10.0.0.8	FTP	91	91 Response: 530 User cannot log in.
165	0.082771	10.0.0.16	10.0.0.8	FTP	91	91 Response: 530 User cannot log in.
178	0.099190	10.0.0.16	10.0.0.8	FTP	91	91 Response: 530 User cannot log in.
191	0.099558	10.0.0.16	10.0.0.8	FTP	91	91 Response: 530 User cannot log in.
204	0.098887	10.0.0.16	10.0.0.8	FTP	91	91 Response: 530 User cannot log in.
217	0.105235	10.0.0.16	10.0.0.8	FTP	91	91 Response: 530 User cannot log in.

Frame 9: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{6D6E3E22-A278-4896-A6E
Ethernet II, Src: Microsoft_01:05:02 (00:15:5d:01:05:02), Dst: Microsoft_01:05:0b (00:15:5d:01:05:0b)
Internet Protocol Version 4, Src: 10.0.0.16, Dst: 10.0.0.8

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

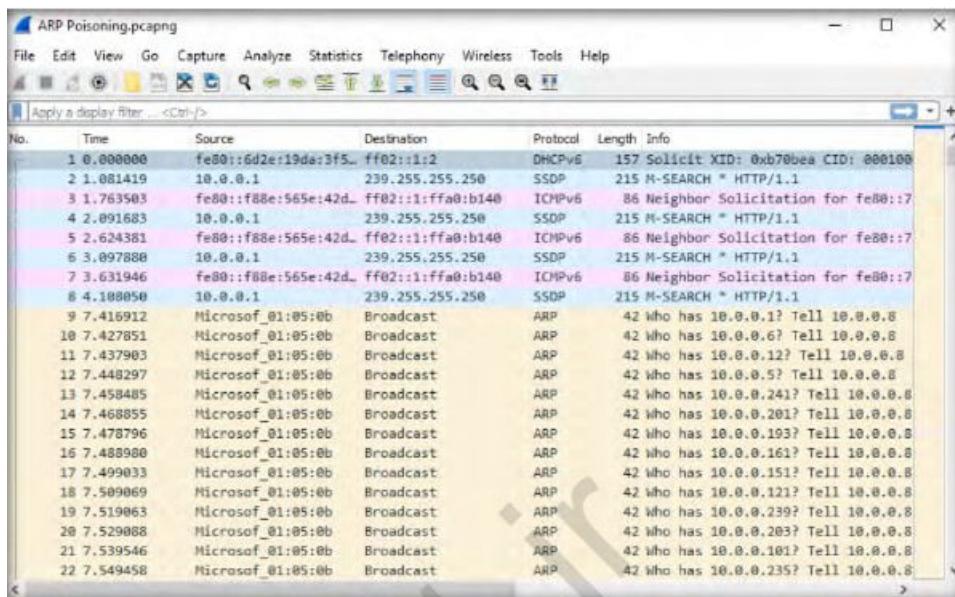
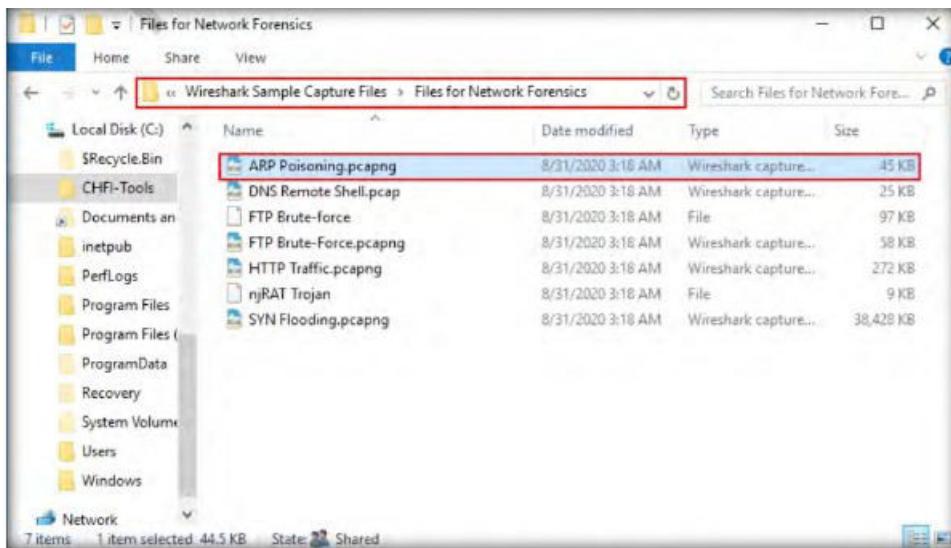
The screenshot shows a Wireshark capture window titled "FTP Brute-Force.pcapng". A green bar at the top indicates the filter: "ftp.response.code == 230". The main pane displays a list of network frames. Most frames are red, representing failed login attempts. One frame is blue, representing a successful login attempt. The blue frame's details are as follows:

No.	Time	Source	Destination	Protocol	Length	Info
308	0.146482	10.0.0.16	10.0.0.8	FTP	87	87 Response: 230 User logged in.
386	0.188781	10.0.0.16	10.0.0.8	FTP	87	87 Response: 230 User logged in.
464	0.215362	10.0.0.16	10.0.0.8	FTP	87	87 Response: 230 User logged in.

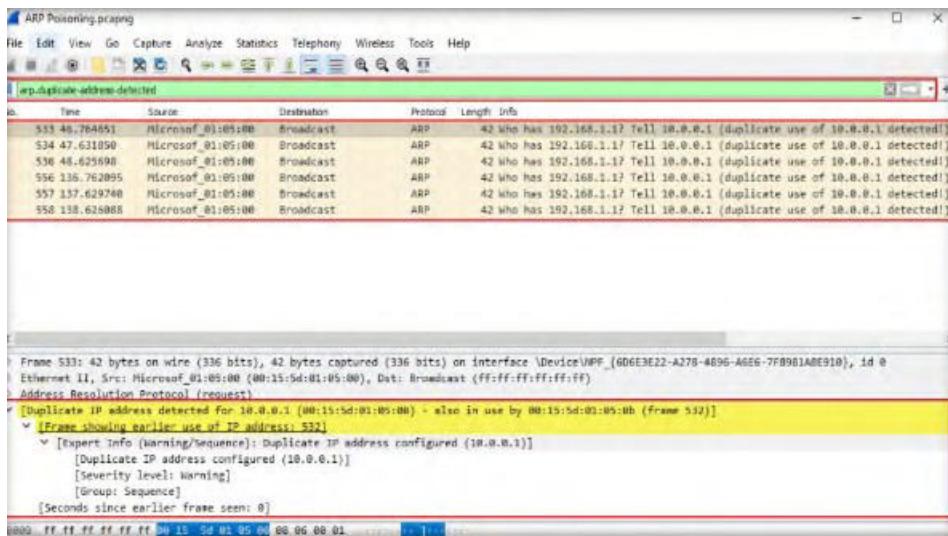
Frame 308: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface \Device\NPF_{6D6E3E22-A278-4896-A6E
Ethernet II, Src: Microsoft_01:05:02 (00:15:5d:01:05:02), Dst: Microsoft_01:05:0b (00:15:5d:01:05:0b)
Internet Protocol Version 4, Src: 10.0.0.16, Dst: 10.0.0.8
Transmission Control Protocol, Src Port: 21, Dst Port: 59192, Seq: 51, Ack: 38, Len: 21
File Transfer Protocol (FTP)
[Current working directory:]

0000 00 15 5d 01 05 0b 00 15 5d 01 05 02 08 00 45 00].....].....E
0010 00 49 6d 27 40 00 00 06 00 00 08 00 00 10 0a 00 Im'@
0020 00 08 00 15 e7 38 51 5e 45 53 6b 84 c5 2e 08 18 ..8Q^n ESk-...
0030 20 2b 14 53 00 00 01 01 08 0a 00 2e b6 2f 45 b4 +S...../E
0040 95 89 32 33 38 28 55 73 65 72 20 6c 6f 67 67 65 230 Us er logge
0050 64 20 69 6e 2e 0d 0a d in.
Packets: 508 · Displayed: 3 (0.6%) Profile: Default

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. 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

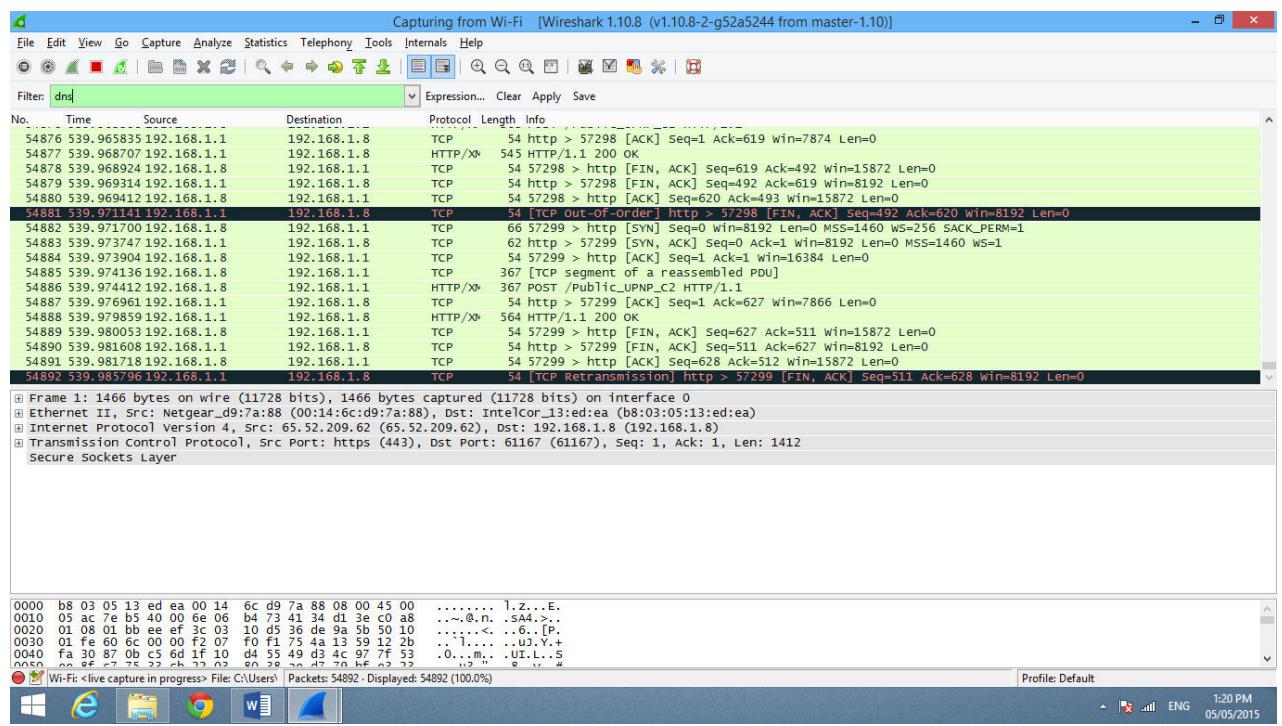
Aim: Exploring Wireshark

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.

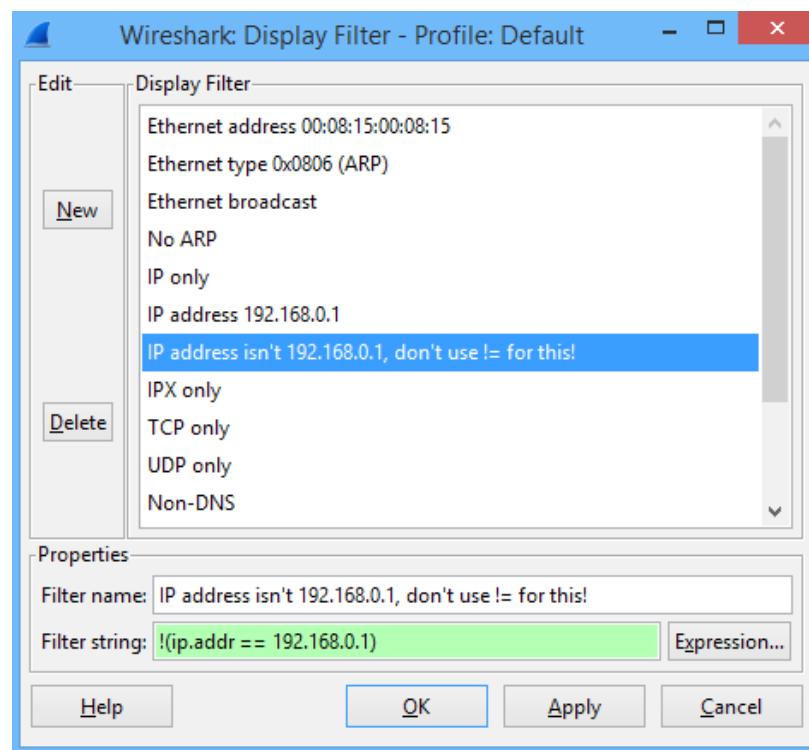
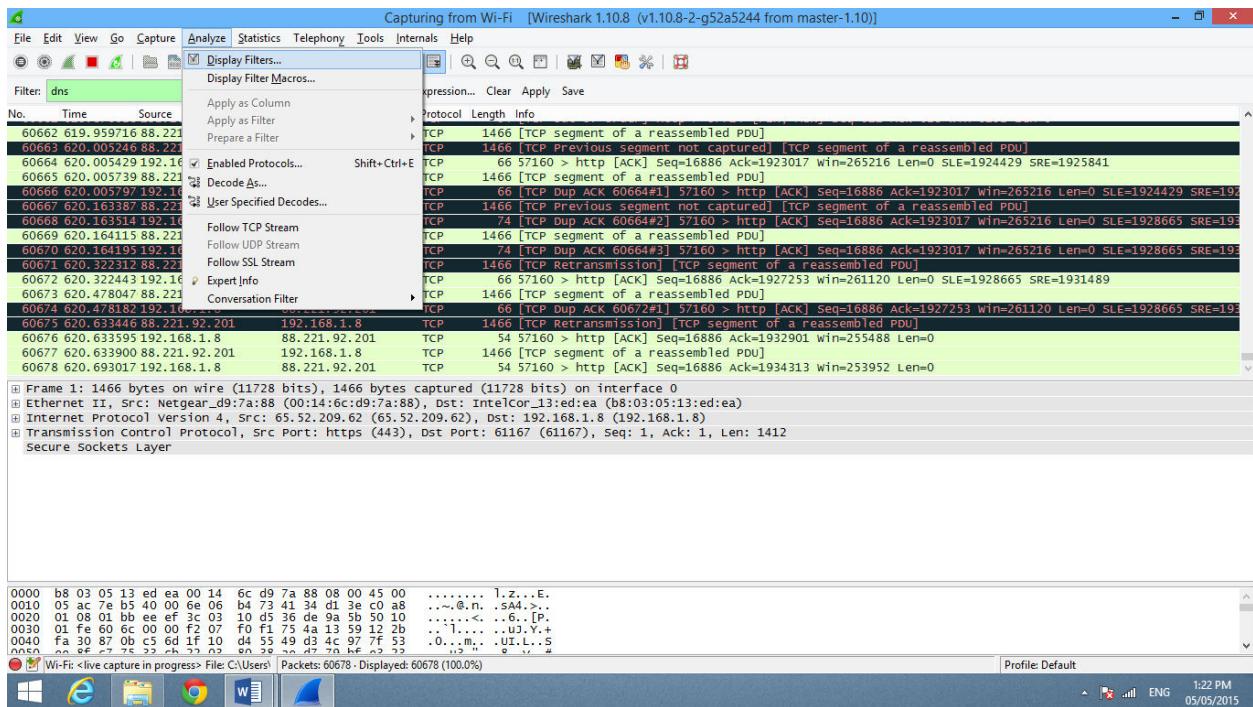
Filtering Packets

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.

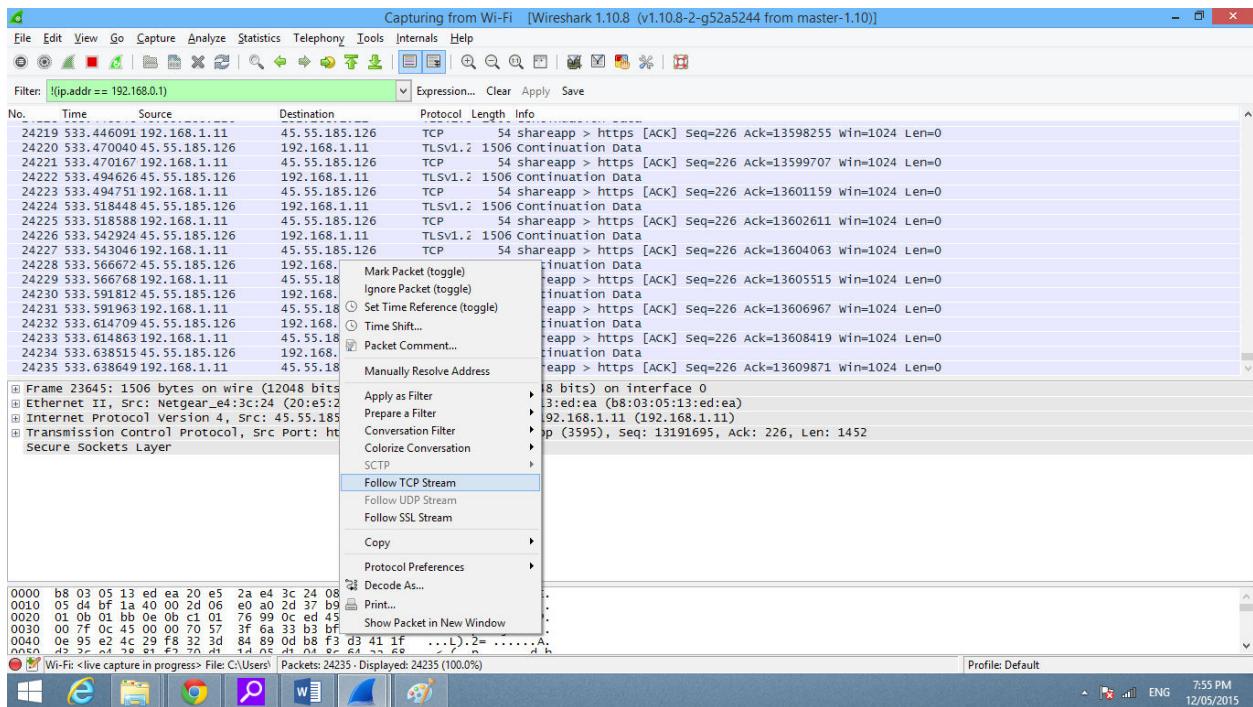
The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type "dns" and you'll see only DNS packets. When you start typing, Wireshark will help you autocomplete your filter.



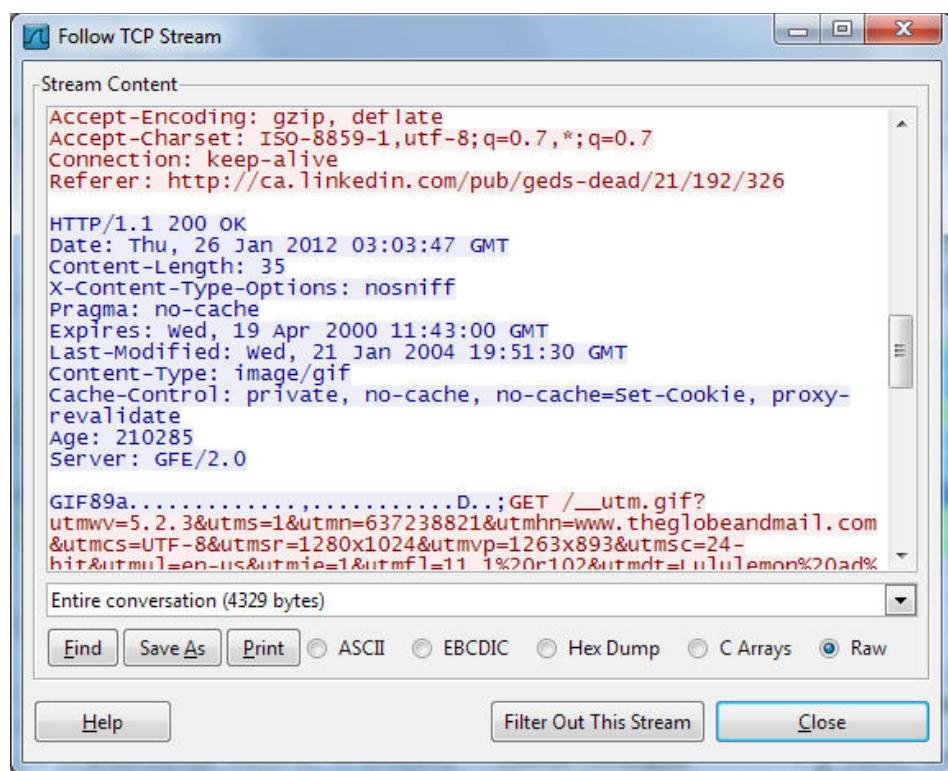
You can also click the Analyze menu and select Display Filters to create a new filter.



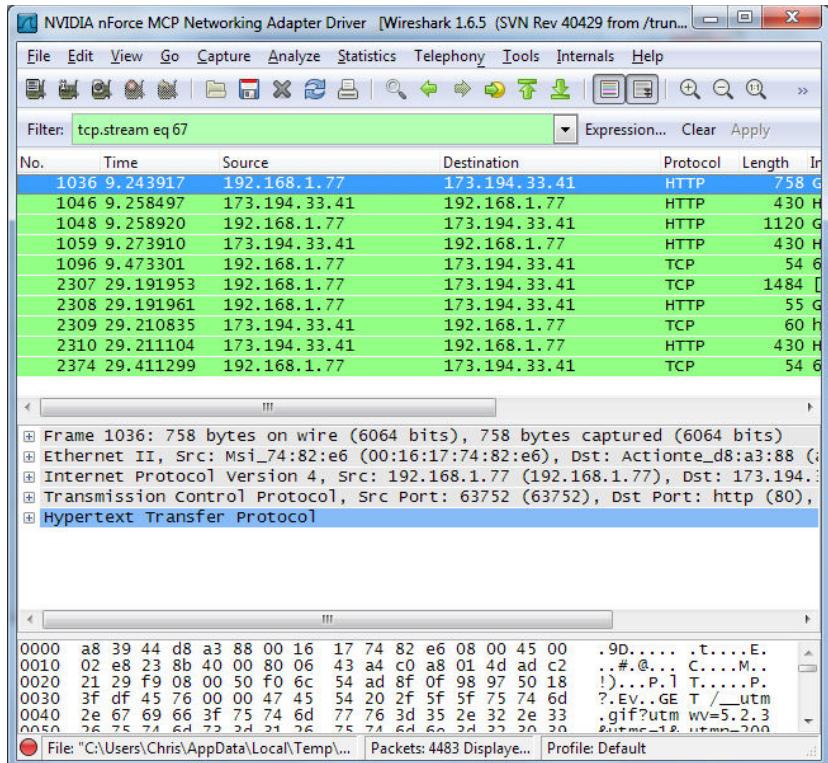
Another interesting thing you can do is right-click a packet and select Follow TCP



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

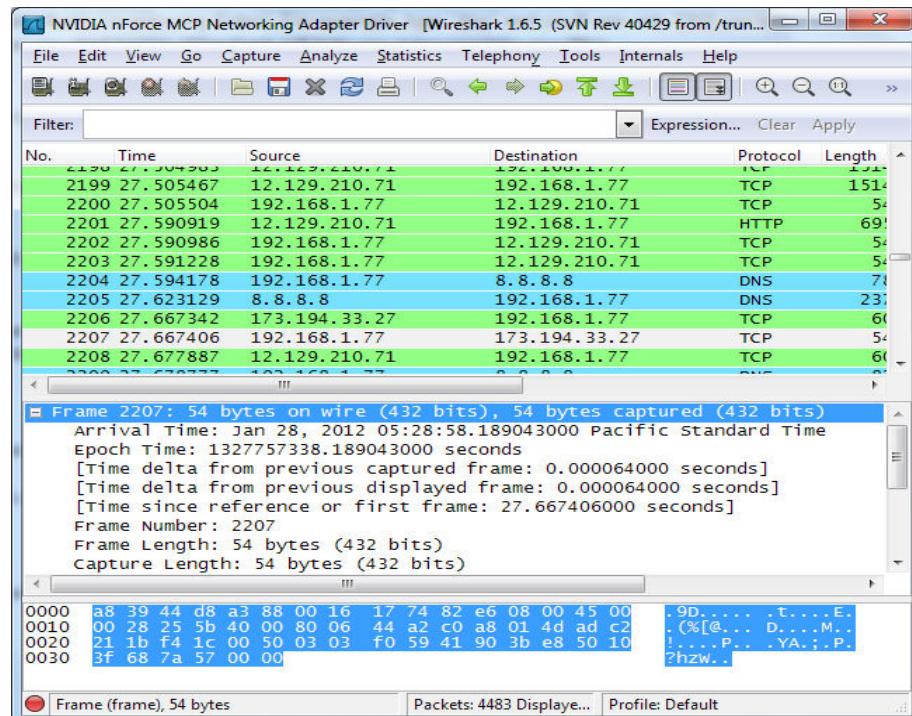


Close the window and you'll find a filter has been applied automatically — Wireshark is showing you the packets that make up the conversation.

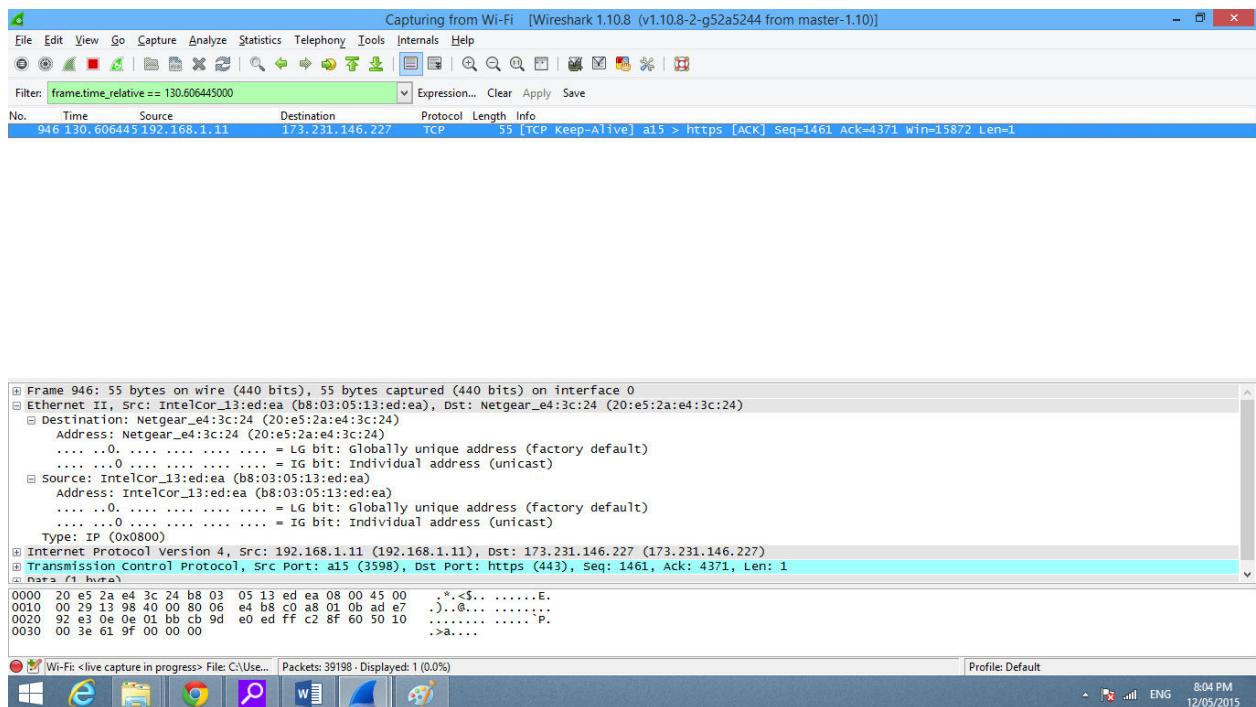


Inspecting Packets

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

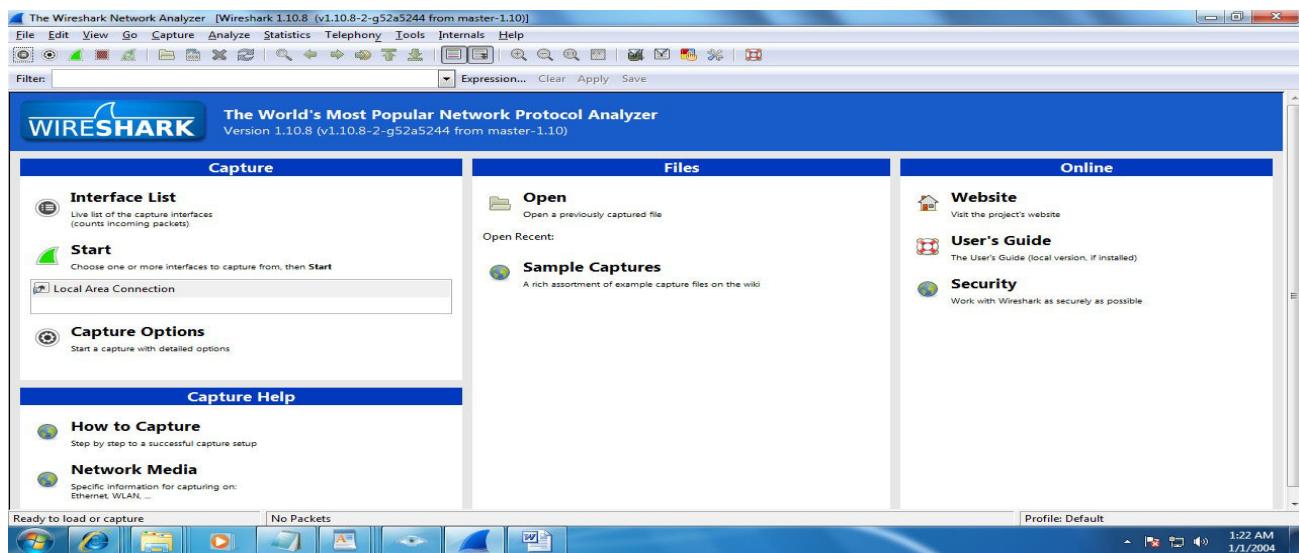


You can also create filters from here — just right-click one of the details and use the Apply as Filter submenu to create a filter based on it.

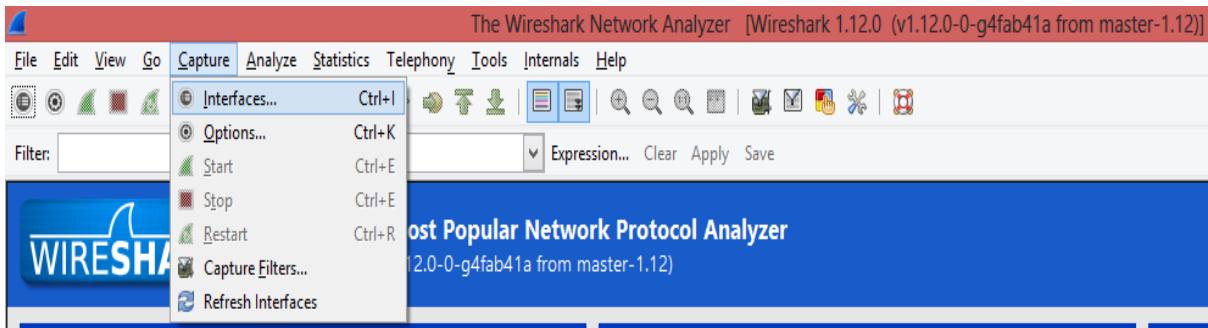


Using Traffic Capturing and Analysis tools

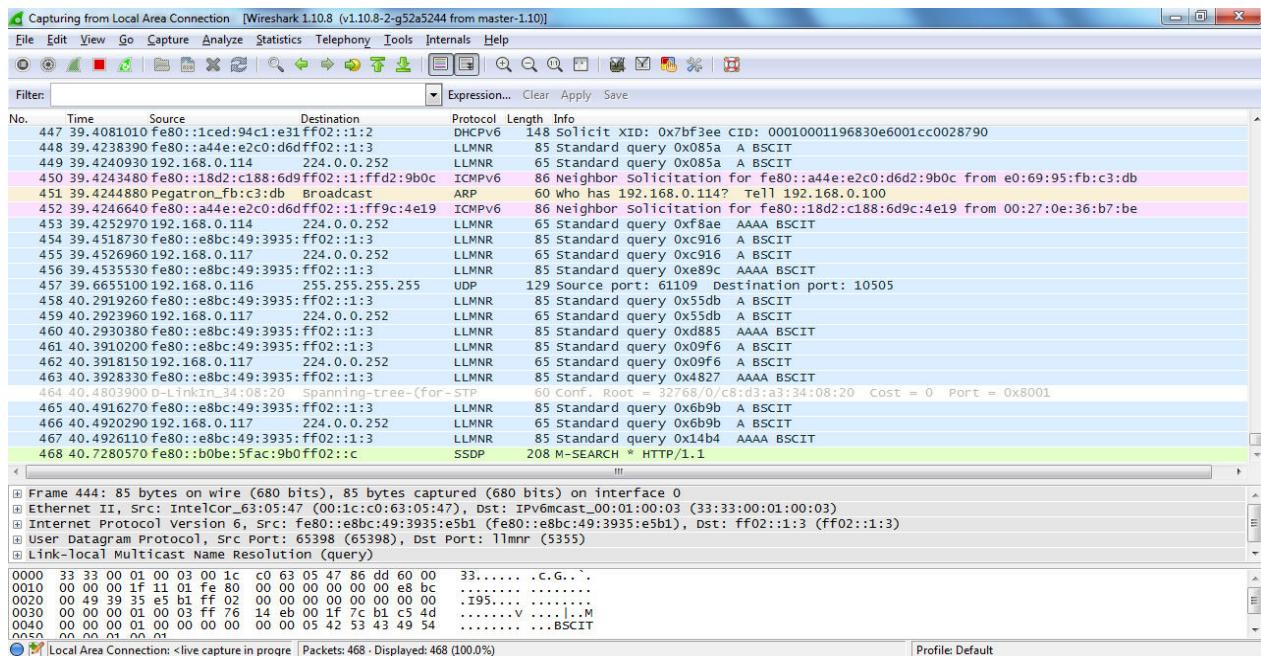
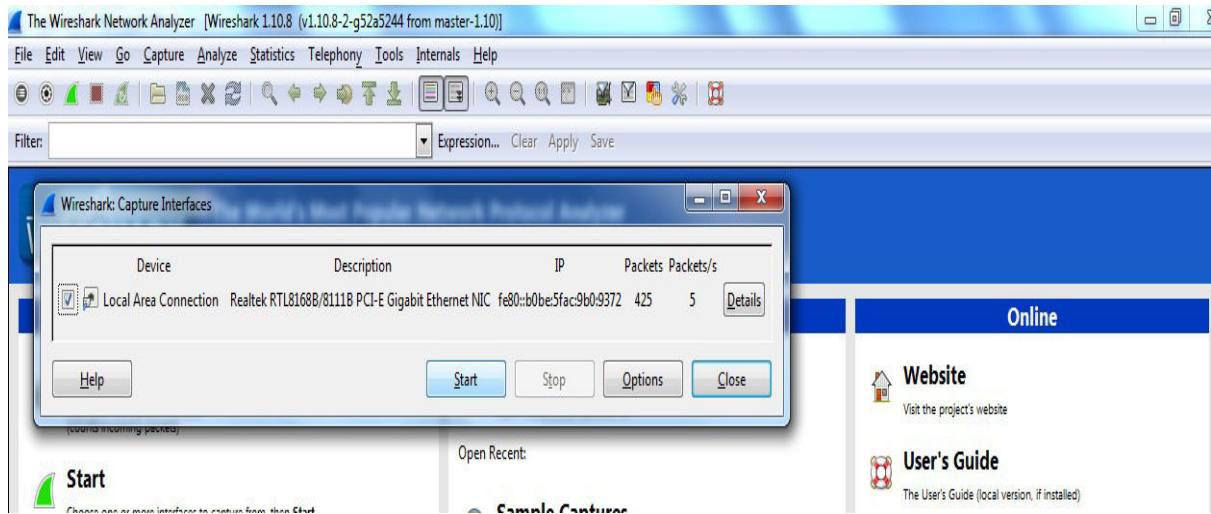
Aim: Exploring Wireshark



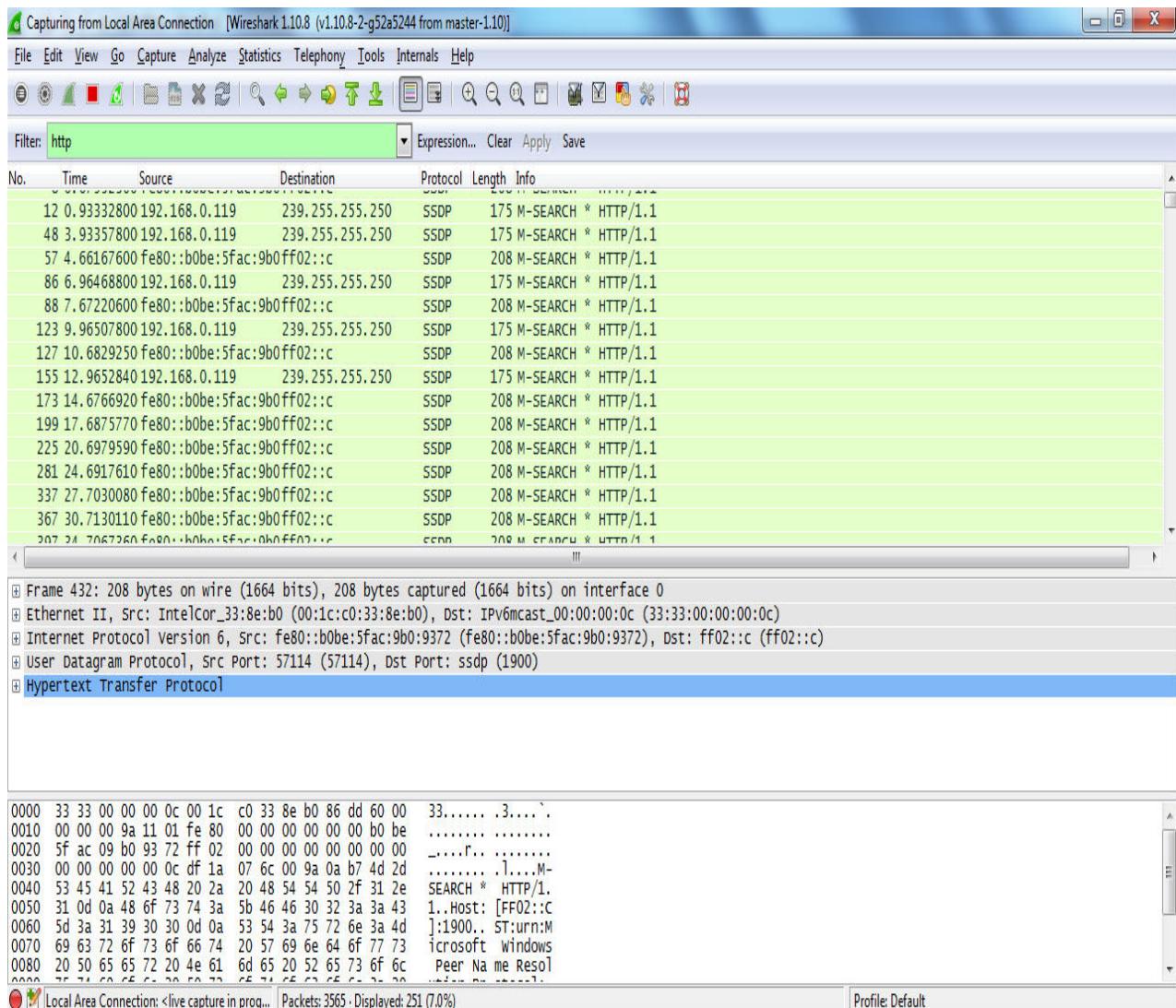
Step 2: On menu bar select Capture. Select interfaces.



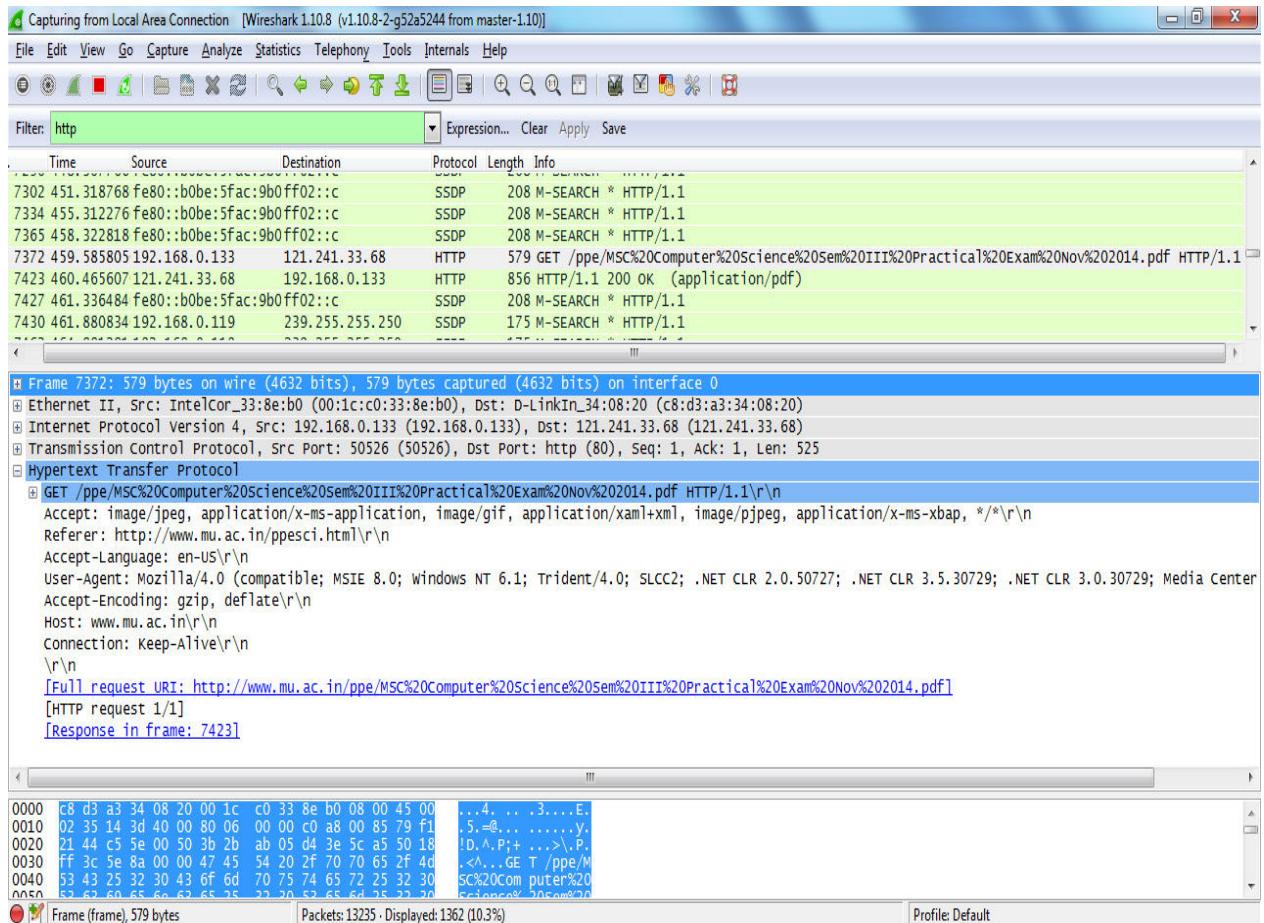
Step 3: Select Once you click on start, then Wireshark starts to capture the packets on that interface.



Step 4: Filter packets with HTTP protocol.

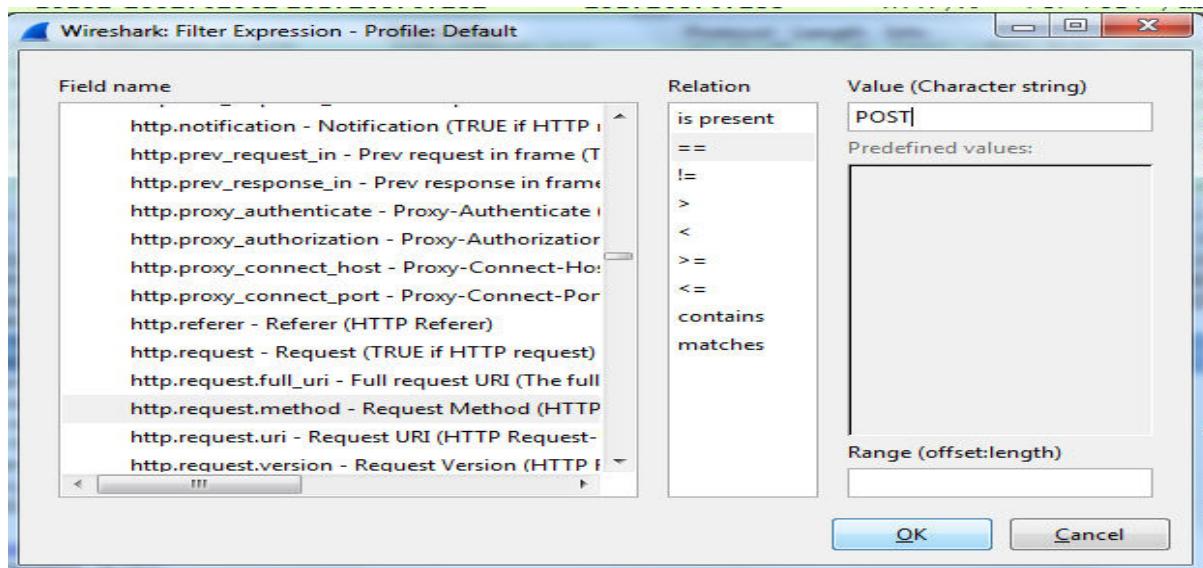


Step 5: A file with only text: [http://www.mu.ac.in/ppe/LIBRARY%20SCIENCE-\(SEM.I\)-SH-2014.pdf](http://www.mu.ac.in/ppe/LIBRARY%20SCIENCE-(SEM.I)-SH-2014.pdf)



Step 6: Applying different filters using expressions.

1) Filtering HTTP POST request



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.request.method == "POST"

No.	Time	Source	Destination	Protocol	Length	Info
2412	14:30:17.003	192.168.0.131	192.168.0.133	HTTP/1.1	787	POST /ab07a5bf-5b0b-46ff-90b4-41029d58972b/ HTTP/1.1
24456	15:23:14.728	192.168.0.131	192.168.0.133	HTTP/1.1	787	POST /ab07a5bf-5b0b-46ff-90b4-41029d58972b/ HTTP/1.1
24809	15:58.293	192.168.0.131	192.168.0.133	HTTP/1.1	787	POST /ab07a5bf-5b0b-46ff-90b4-41029d58972b/ HTTP/1.1
25126	15:58.671	192.168.0.131	192.168.0.133	HTTP/1.1	787	POST /ab07a5bf-5b0b-46ff-90b4-41029d58972b/ HTTP/1.1
25291	15:59.015	192.168.0.131	192.168.0.133	HTTP/1.1	787	POST /ab07a5bf-5b0b-46ff-90b4-41029d58972b/ HTTP/1.1
25753	16:47.443	192.168.0.131	192.168.0.133	HTTP/1.1	787	POST /ab07a5bf-5b0b-46ff-90b4-41029d58972b/ HTTP/1.1
26142	16:52.246	192.168.0.131	192.168.0.133	HTTP/1.1	787	POST /ab07a5bf-5b0b-46ff-90b4-41029d58972b/ HTTP/1.1
26993	17:46.745	192.168.0.131	192.168.0.133	HTTP/1.1	787	POST /ab07a5bf-5b0b-46ff-90b4-41029d58972b/ HTTP/1.1

Frame 4625: 787 bytes on wire (6296 bits), 787 bytes captured (6296 bits) on interface 0

Ethernet II, Src: IntelCor_62:e8:d3 (00:1c:c0:62:e8:d3), Dst: IntelCor_33:8e:b0 (00:1c:c0:33:8e:b0)

Internet Protocol Version 4, Src: 192.168.0.131 (192.168.0.131), Dst: 192.168.0.133 (192.168.0.133)

Transmission Control Protocol, Src Port: 54205 (54205), Dst Port: wsddapi (5357), Seq: 222, Ack: 1, Len: 733

[2 Reassembled TCP Segments (954 bytes): #4624(221), #4625(733)]

Hypertext Transfer Protocol

POST /ab07a5bf-5b0b-46ff-90b4-41029d58972b/ HTTP/1.1

Cache-control: no-cache\r\nConnection: Close\r\nPragma: no-cache\r\nContent-Type: application/soap+xml\r\nUser-Agent: wsDDAPI\r\nContent-Length: 733\r\nHost: 192.168.0.133:5357\r\n

[Full request URI: http://192.168.0.133:5357/ab07a5bf-5b0b-46ff-90b4-41029d58972b/]

[HTTP request 1/1]

[Response in frame: 4635]

extensible Markup Language

Frame (787 bytes) Reassembled TCP (954 bytes)

Frame (frame), 787 bytes | Packets: 27162 - Displayed: 26 (0.1%) | Profile: Default

2) Filtering 404 not found error

Wireshark: Filter Expression - Profile: Default

Field name: http.request.method = Request Method (HTTP)

Relation: is present

Value (Unsigned integer, 2 bytes): 404

Predefined values:

Range (offset:length)

OK Cancel

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

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http.response.code == 404

No.	Time	Source	Destination	Protocol	Length	Info
3972	208.680505	208.80.154.224	192.168.0.133	HTTP	804	HTTP/1.1 404 Not Found (text/html)

Frame 3972: 804 bytes on wire (6432 bits), 804 bytes captured (6432 bits) on interface 0

Ethernet II, Src: D-LinkIN_34:08:20 (c8:d3:a3:34:08:20), Dst: IntelCor_33:8e:b0 (00:1c:c0:33:8e:b0)

Internet Protocol Version 4, Src: 208.80.154.224 (208.80.154.224), Dst: 192.168.0.133 (192.168.0.133)

Transmission Control Protocol, Src Port: http (80), Dst Port: 50806 (50806), Seq: 7261, Ack: 655, Len: 750

[6 Reassembled TCP Segments (8010 bytes): #3961(1452), #3962(1452), #3966(1452), #3968(1452), #3970(1452), #3972(750)]

Hypertext Transfer Protocol

HTTP/1.1 404 Not Found

Server: Apache\r\nX-Content-Type-Options: nosniff\r\nContent-Language: en\r\nX-UA-Compatible: IE=Edge\r\nContent-Encoding: gzip\r\nContent-Type: text/html; charset=UTF-8\r\nVary: Accept-Encoding,Cookie,X-Use-HHVM\r\nX-Varnish: 41450, 401533/553\r\nVia: 1.1 varnish, 1.1 varnish\r\nContent-Length: 7464\r\nAccept-Ranges: bytes\r\nDate: Sat, 15 Nov 2014 08:26:00 GMT\r\n

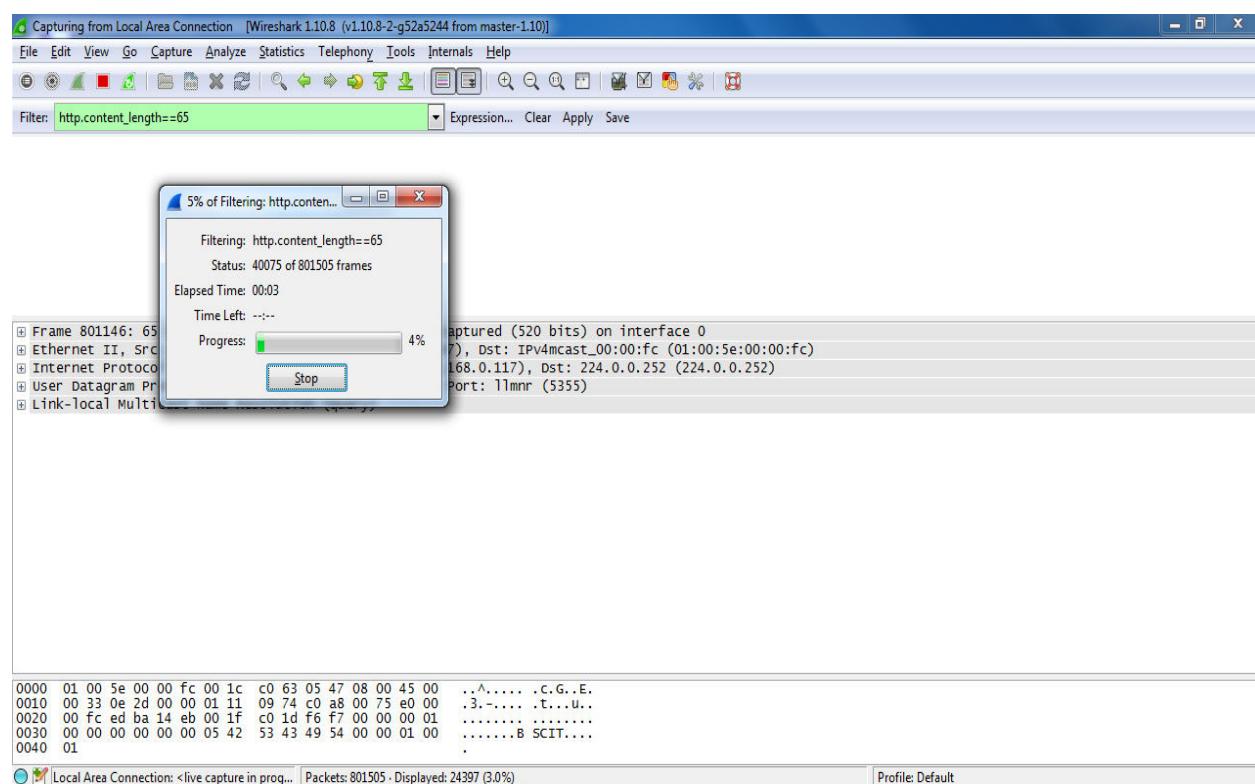
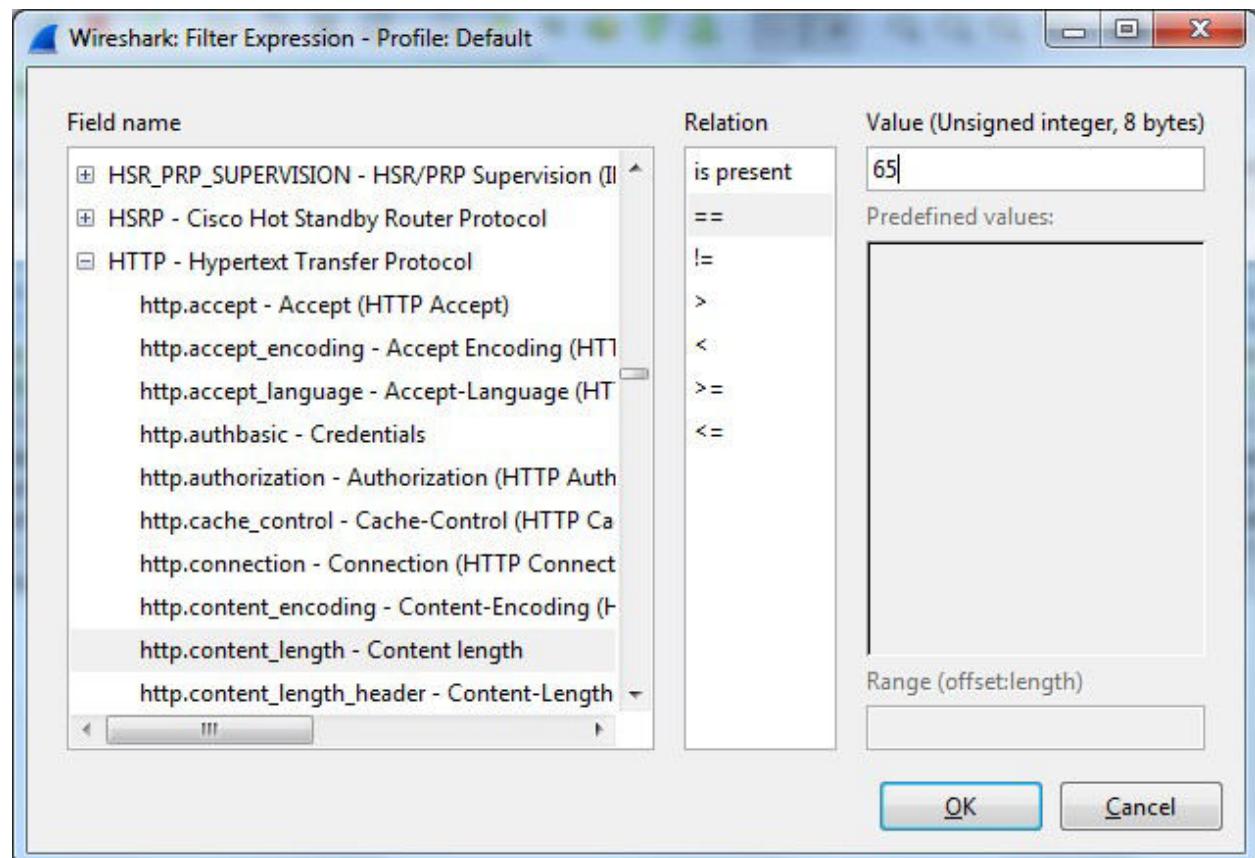
Frame (804 bytes) Reassembled TCP (8010 bytes) Uncompressed entity body (26524 bytes)

Local Area Connection <live capture in prog... | Packets: 5347 - Displayed: 1 (0.0%) | Profile: Default

Windows Taskbar icons

2:39 AM 1/1/2004

3) Filtering using HTTP Content Length

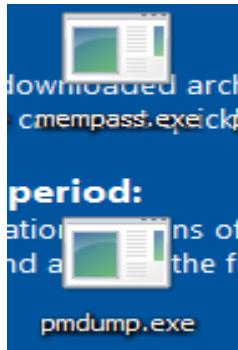


PRACTICAL NO:06

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



```
C:\Users\IEUser\Desktop>mempass
Please enter your password:hello
Administrator:C:\Windows\system32\cmd.exe - mempass
Press any key to continue . . .
```

A screenshot of a terminal window. The command 'mempass' is entered, followed by a password prompt. The password 'hello' is typed. The terminal shows the command again and a message to press any key to continue.

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

```
C:\Users\IEUser\Desktop>pmdump
pmdump 1.2 - <c> 2002, Arne Vidstrom <arne.vidstrom@ntsecurity.nu>
- http://ntsecurity.nu/toolbox/pmdump/
Usage: pmdump <pid> <filename>
      - dumps the process memory contents to a file
      pmdump -list
      - lists all running processes and their PID's
```

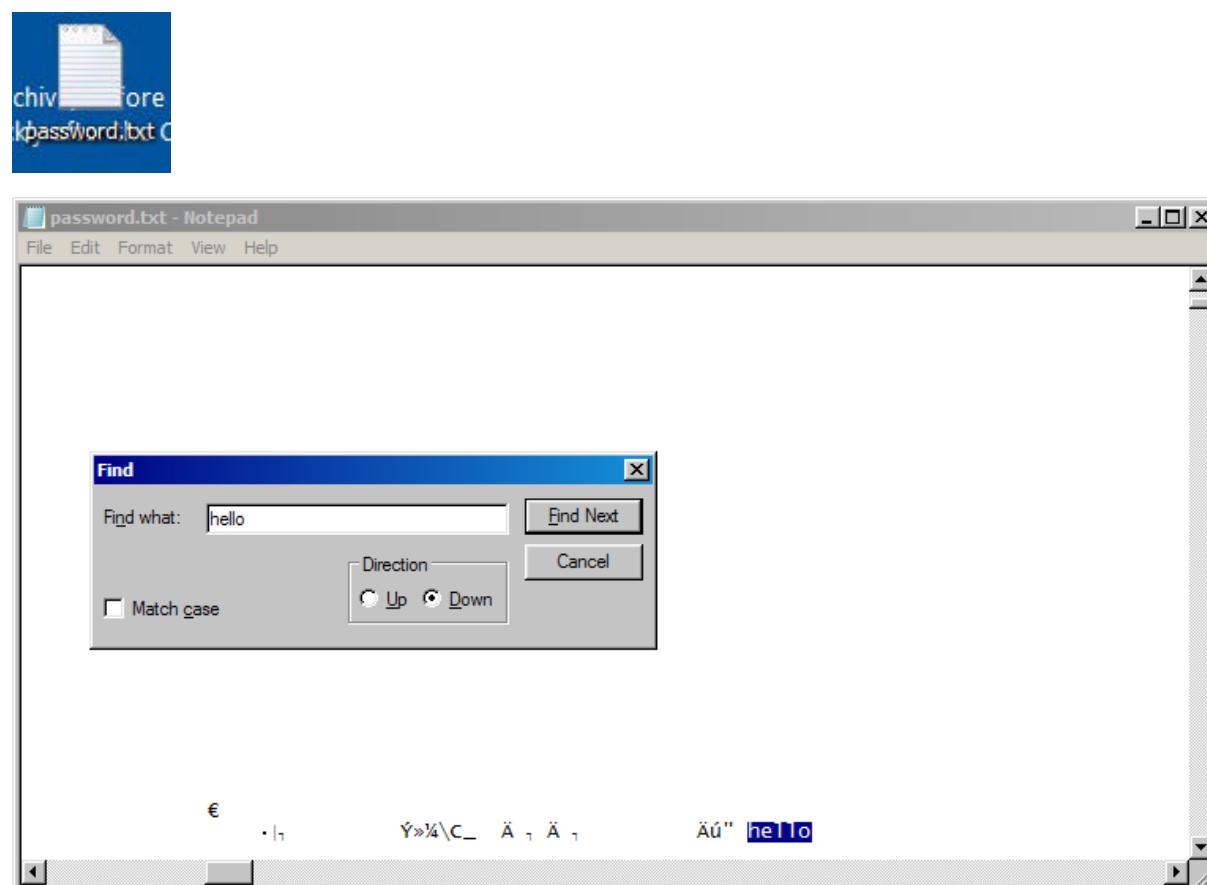
```
C:\Users\IEUser\Desktop>pmdump -list
pmdump 1.2 - <c> 2002, Arne Vidstrom <arne.vidstrom@ntsecurity.nu>
- http://ntsecurity.nu/toolbox/pmdump/
  0 - System idle process
  4 - System
 252 - smss.exe
 328 - csrss.exe
 364 - csrss.exe
 372 - wininit.exe
 400 - winlogon.exe
 460 - services.exe
 468 - lsass.exe
 476 - lsm.exe
 568 - svchost.exe
 624 - 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 - wlm.exe
1696 - conhost.exe
1720 - sshd.exe
1932 - spsvc.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
```

```
5198 - 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

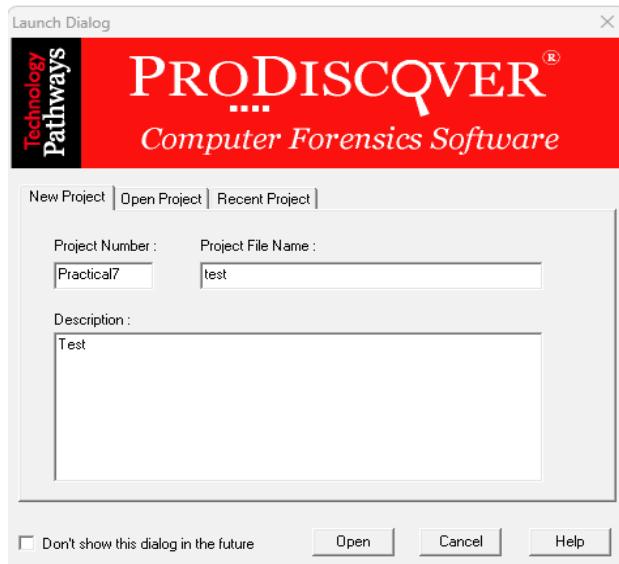


In this way, we can retrieve passwords from applications which store them in memory without any form of encryption.

PRACTICAL NO:07

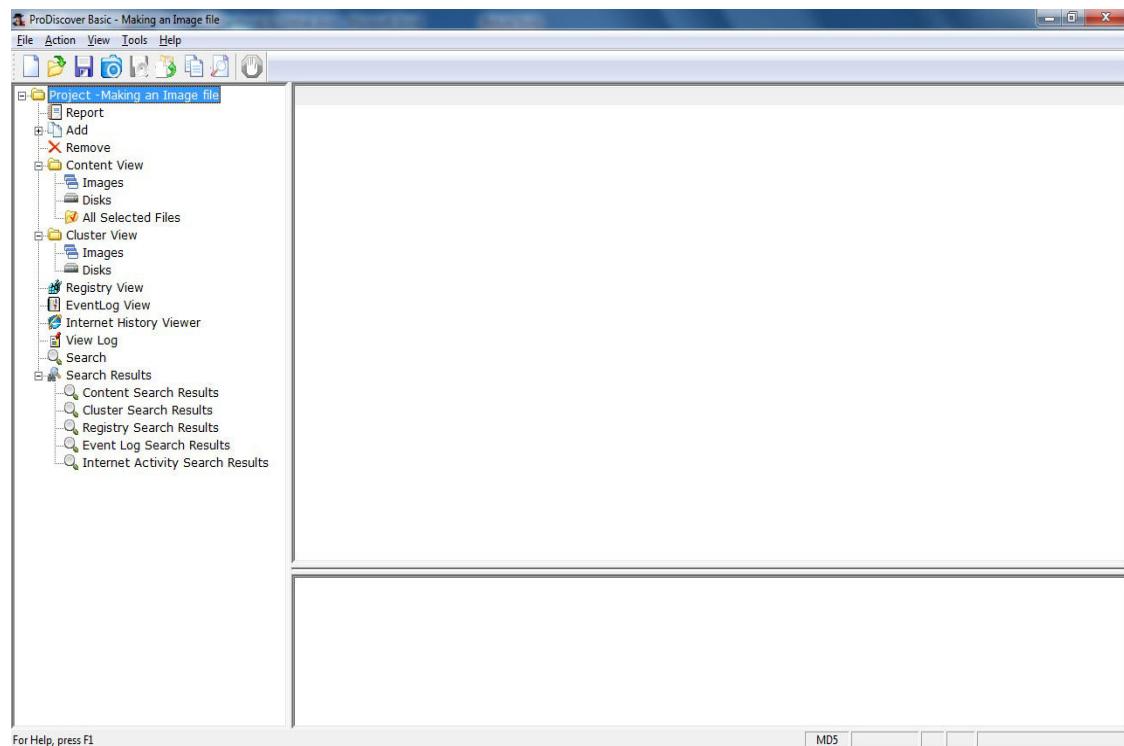
Using Data Acquisition Tools [ProDiscover Pro]

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



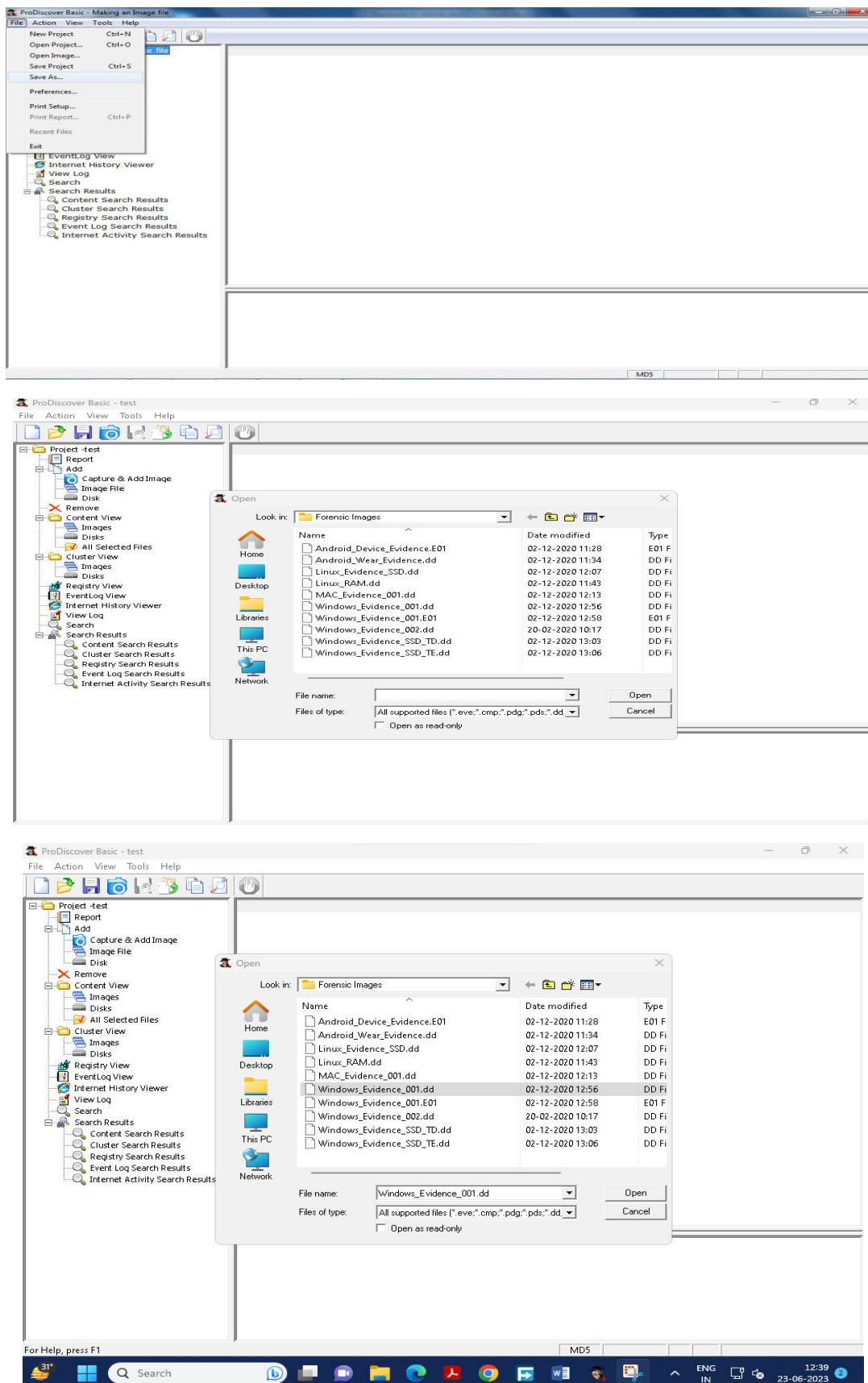
Step 2) Enter a project number, project name, and description of the project in the new project tab option, and then click the Open button.

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

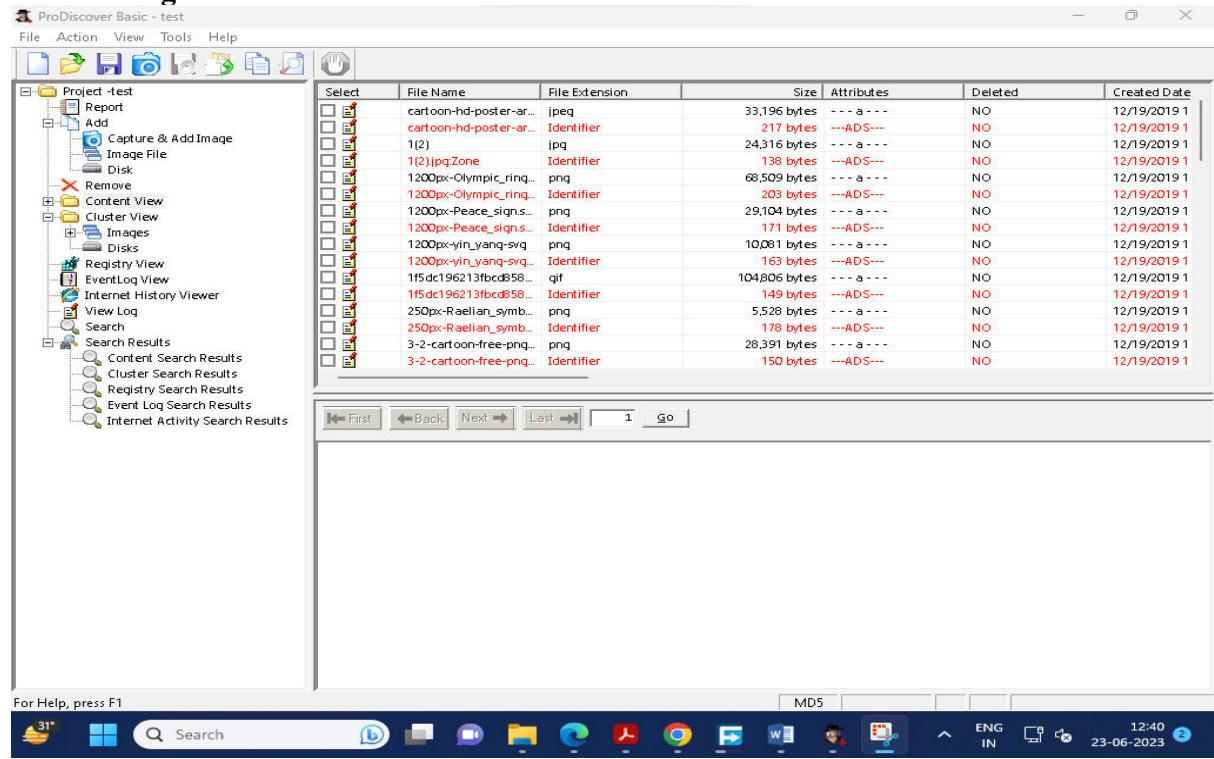


Step 3) Open Image:

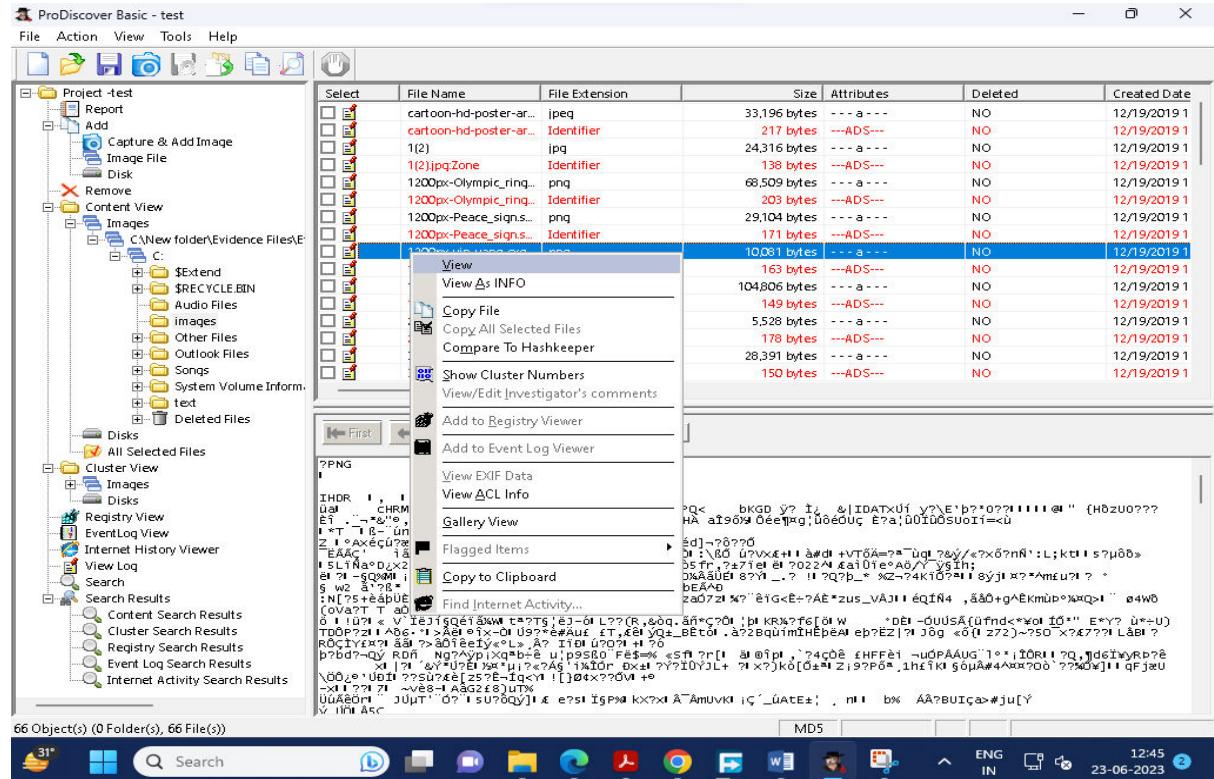
1] Select save project option from the file menu, or button bar and Open Image option.



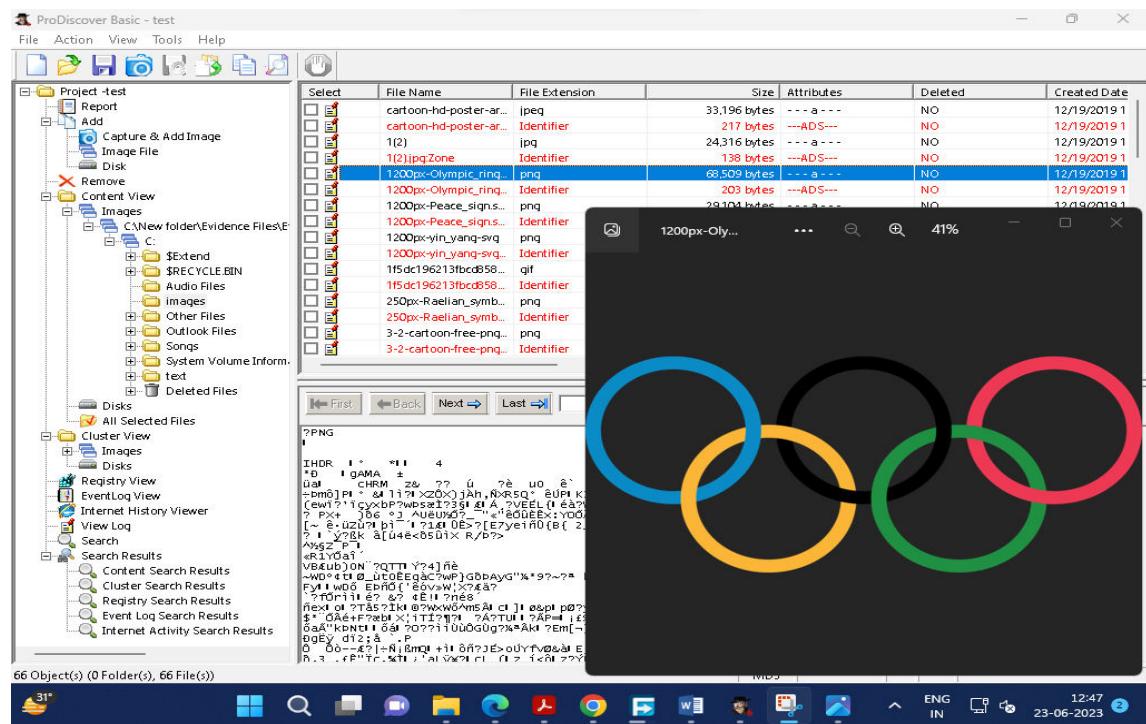
Step 4) ProDiscover displays the contents of the selected file at the bottom of the main window. Right click on a file.



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

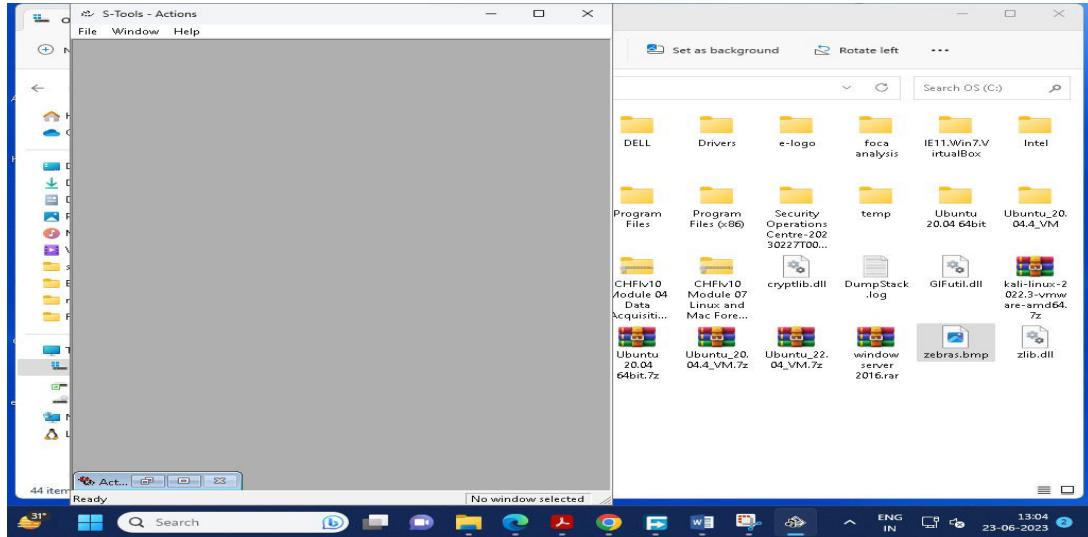


PRACTICAL NO:08

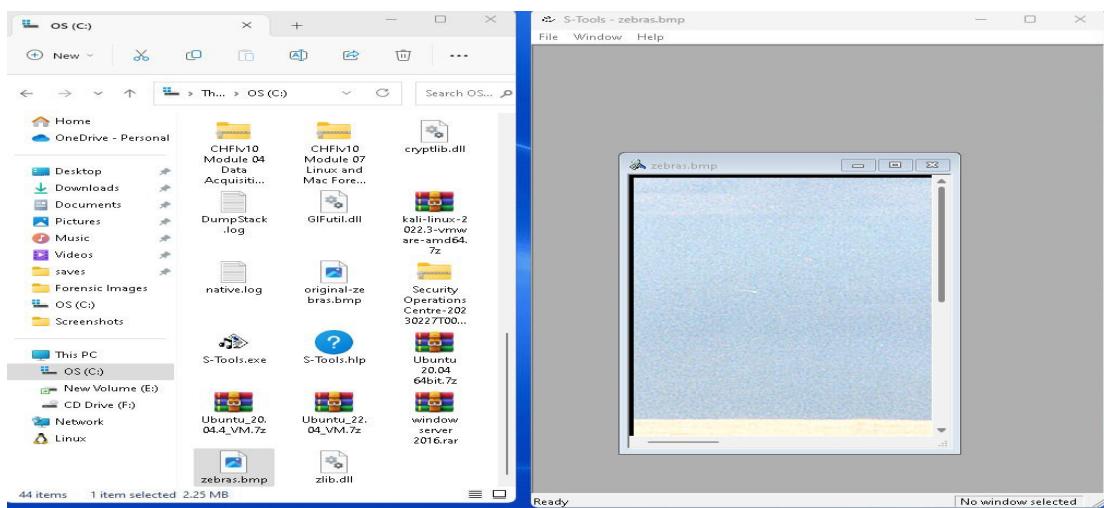
a. Using Steganography Tools [S-Tools]

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

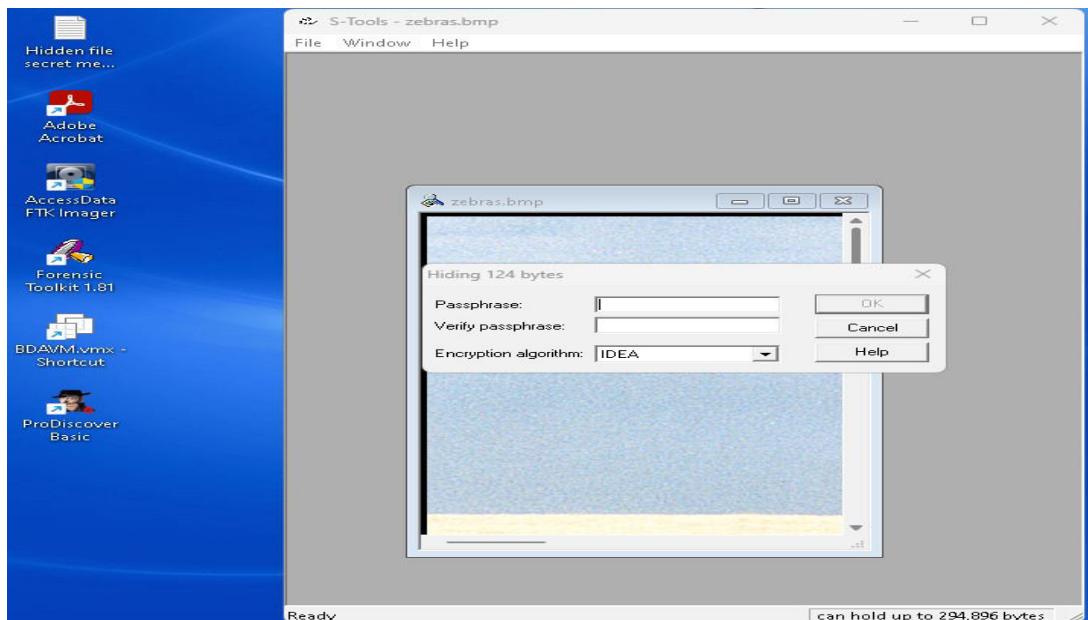
If your image is in .jpg format, convert it to .bmp format.

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

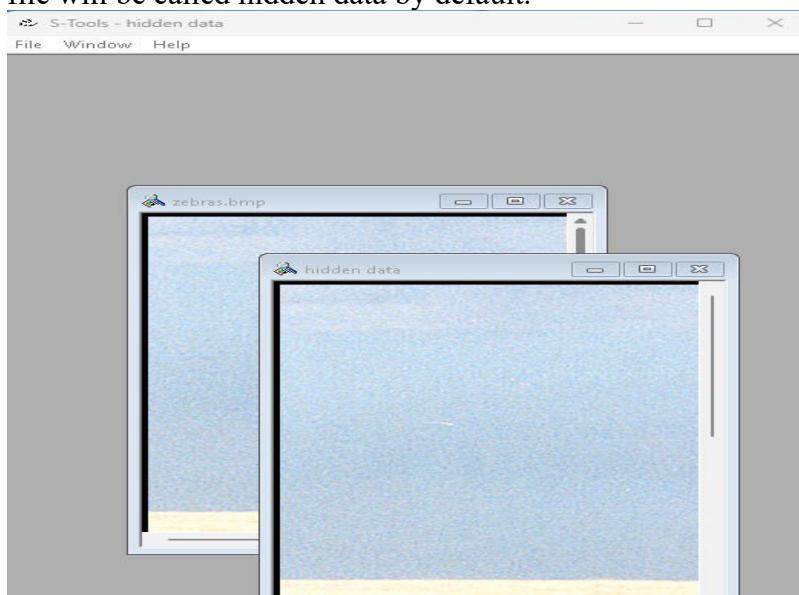
Step 5) The *.txt text file is selected and dragged on top of the base image. Release the file while the cursor is still on top of the base file.

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.



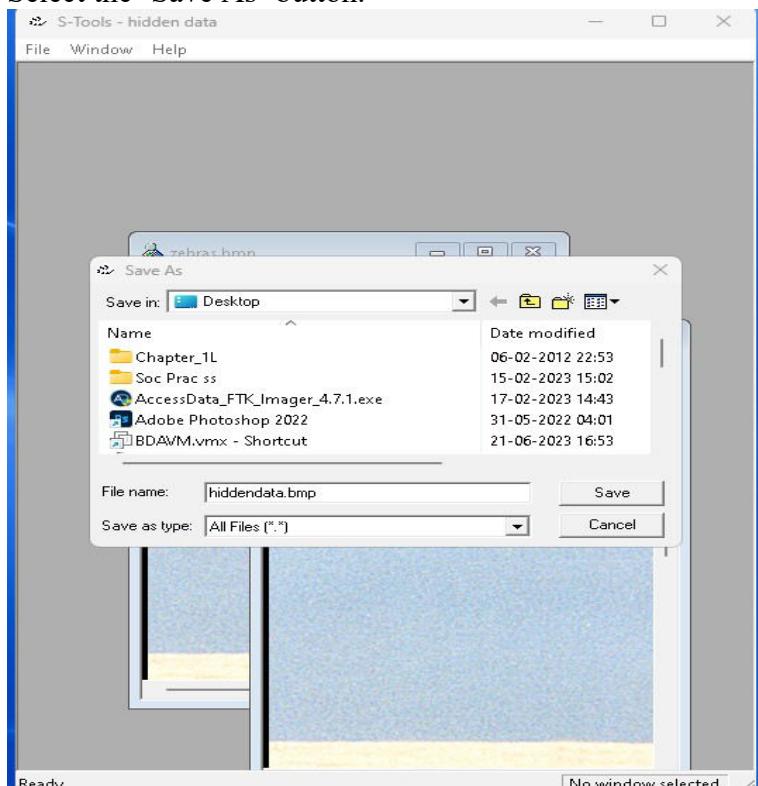
Step 8) The S-Tools main window will appear and a new file will be visible. The name of the file will be called hidden data by default.



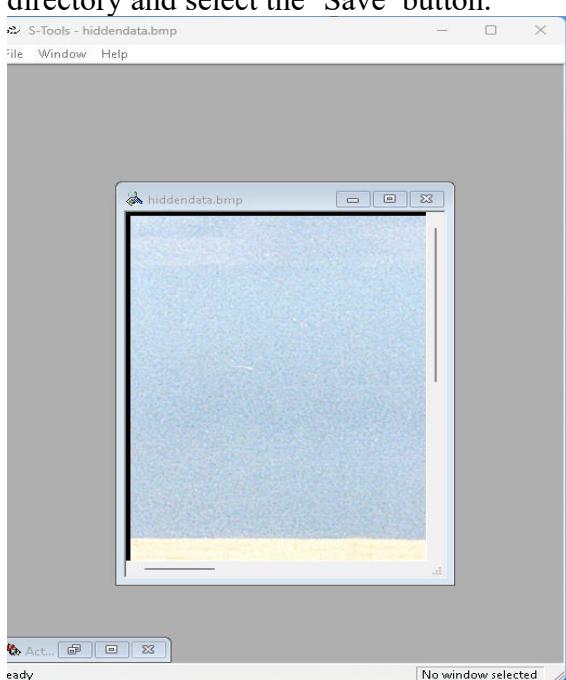
Step 9) Place the cursor on top of the hidden data image and select the right mouse button.
The user will
have four options available to them:

- Save
- Save As
- Properties
- Reveal

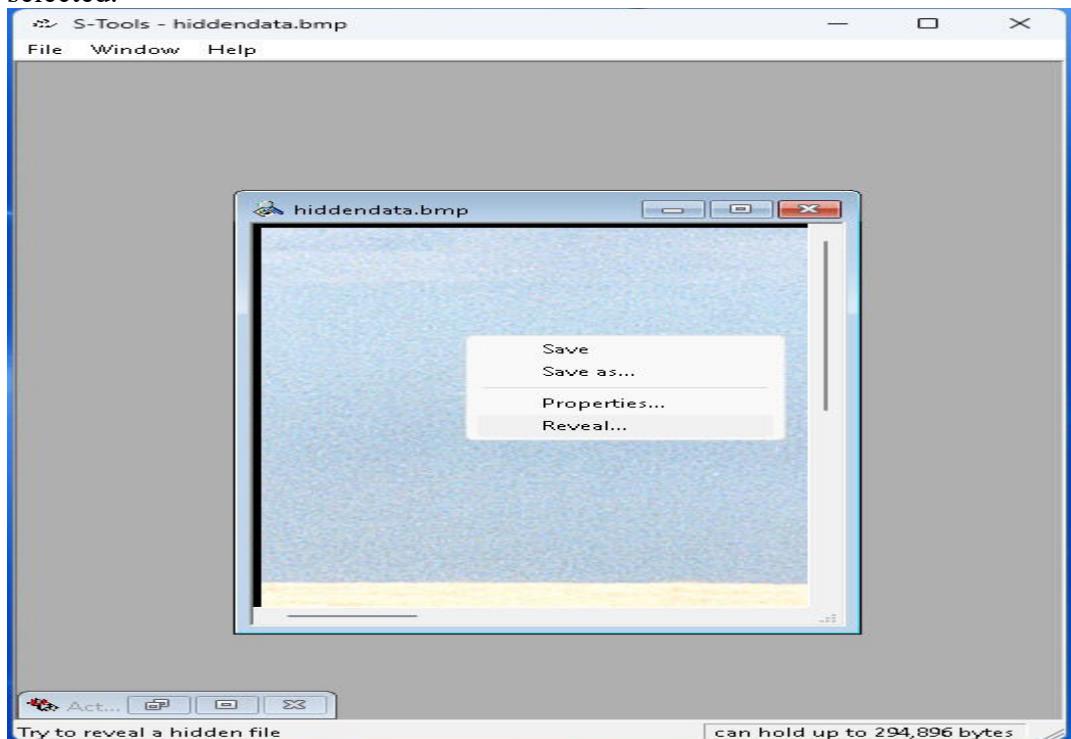
Select the ‘Save As’ button.



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



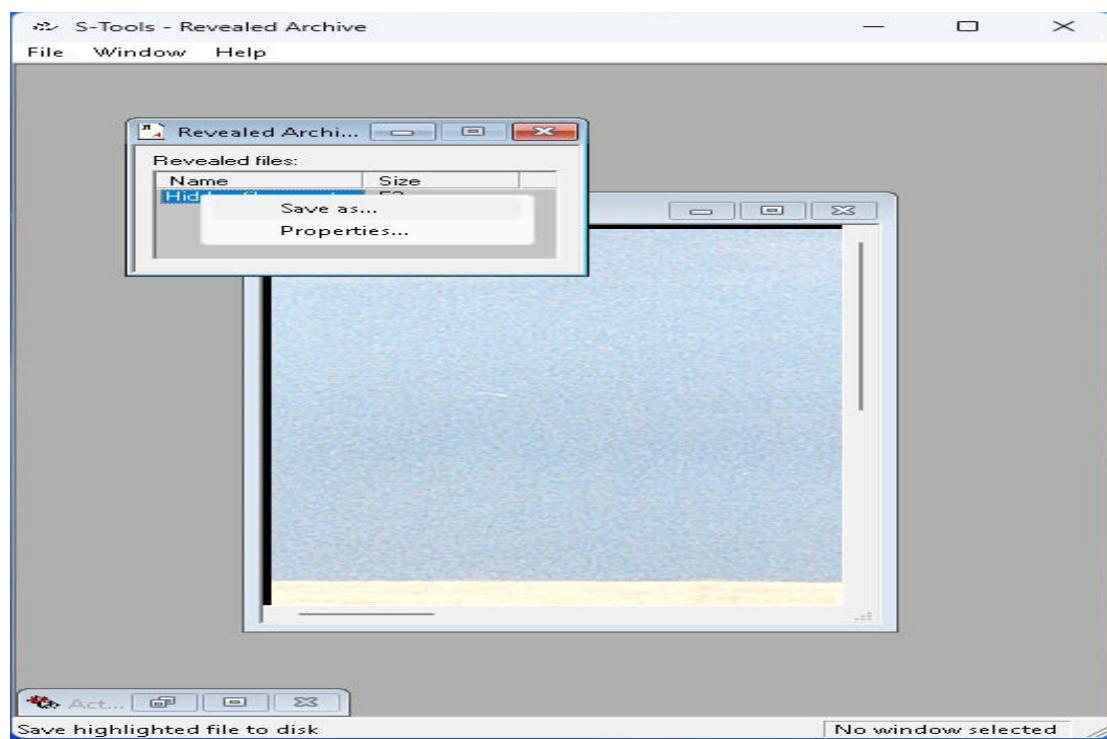
Step 11) Selecting the ‘Reveal’ button will display a passphrase dialogue box. A passphrase must be entered twice in the dialogue box and the correct encryption algorithm must be selected.



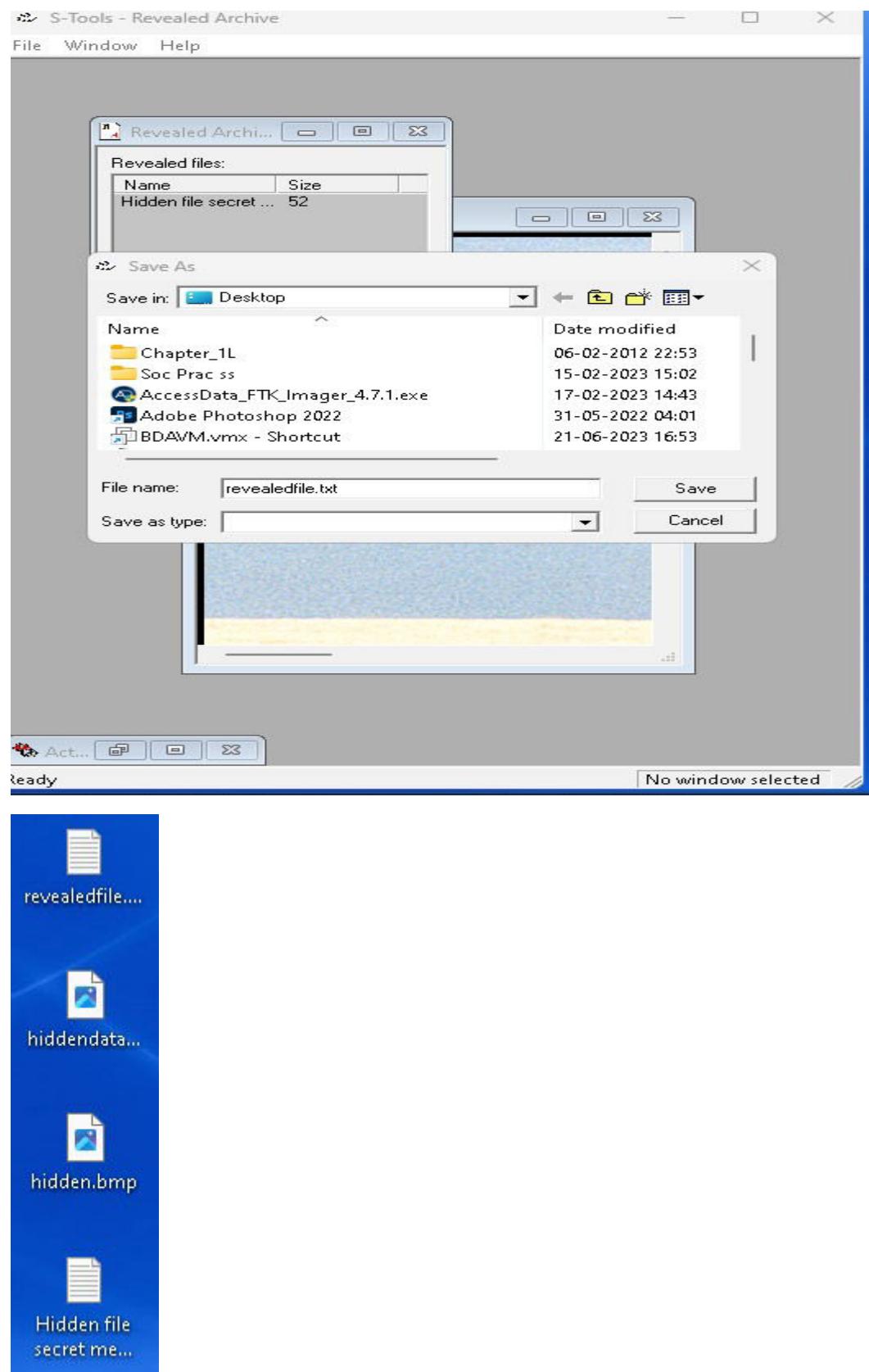
Step 12) Enter a passphrase twice, select the encryption algorithm, and select the ‘OK’ button.

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



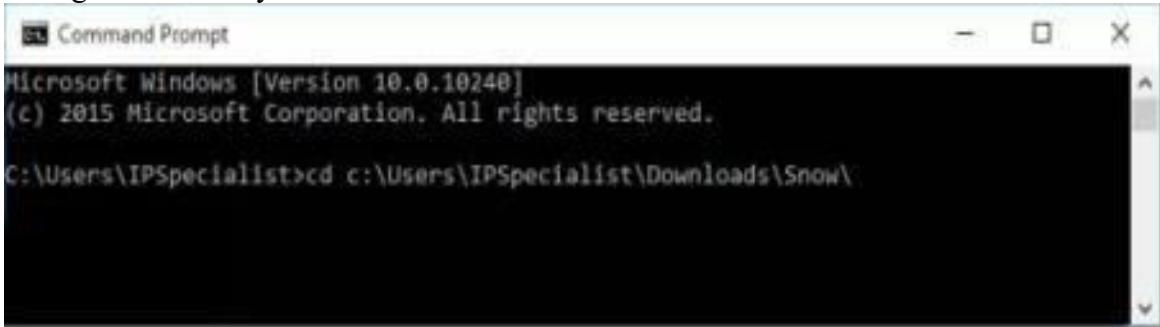
b. Using Whitespace Stegnography tool SNOW

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



Step 2) Go to Command Prompt

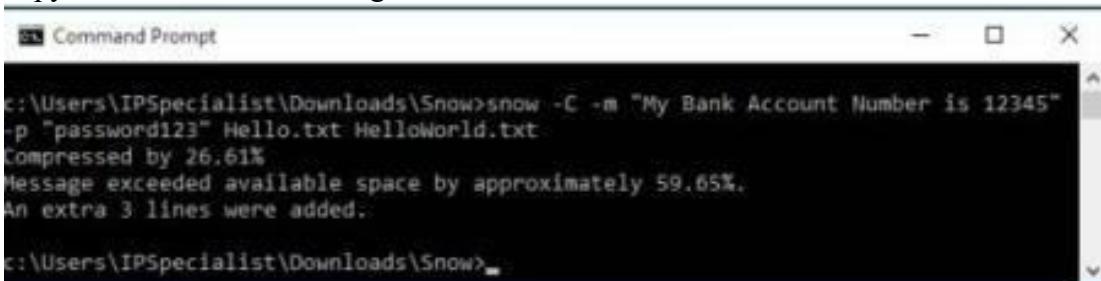
Change the directory to run Snow tool



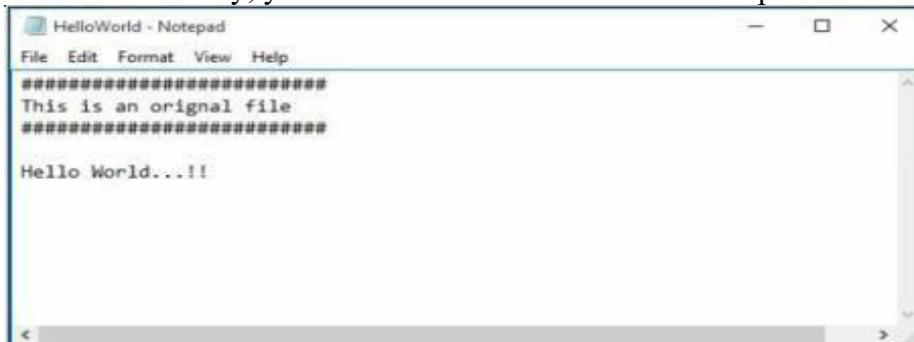
Step 3) Type the command

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

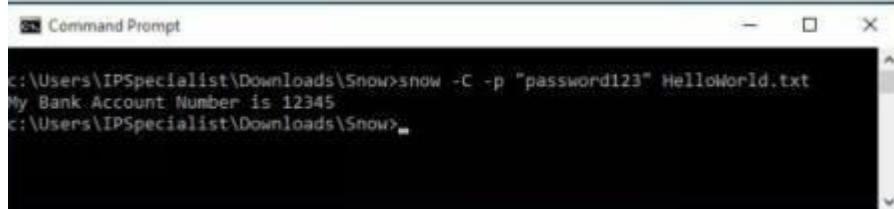


Step 4) New File has the same text as an original file without any hidden information. This file can be sent to the target.

Recovering Hidden Information

On destination, Receiver can reveal information by using the command

Snow –C –p “password123” HelloWorld.txt



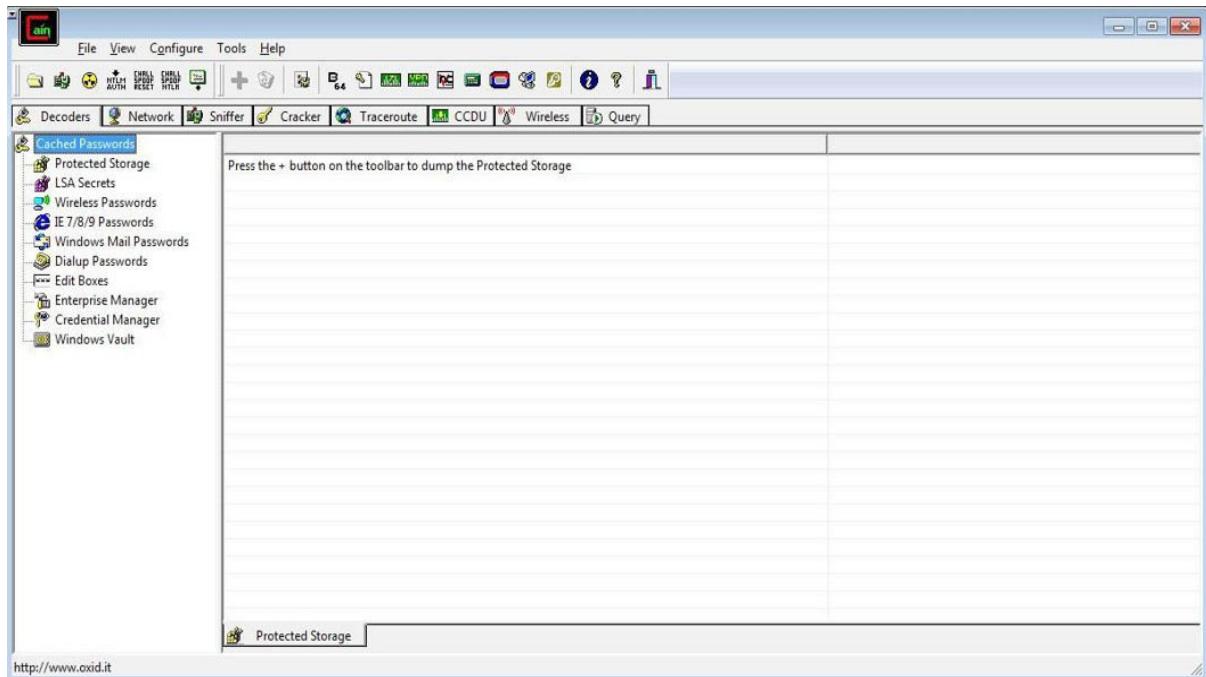
```
c:\Users\IPSpecialist\Downloads\Snow>snow -C -p "password123" HelloWorld.txt
My Bank Account Number is 12345
c:\Users\IPSpecialist\Downloads\Snow>
```

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

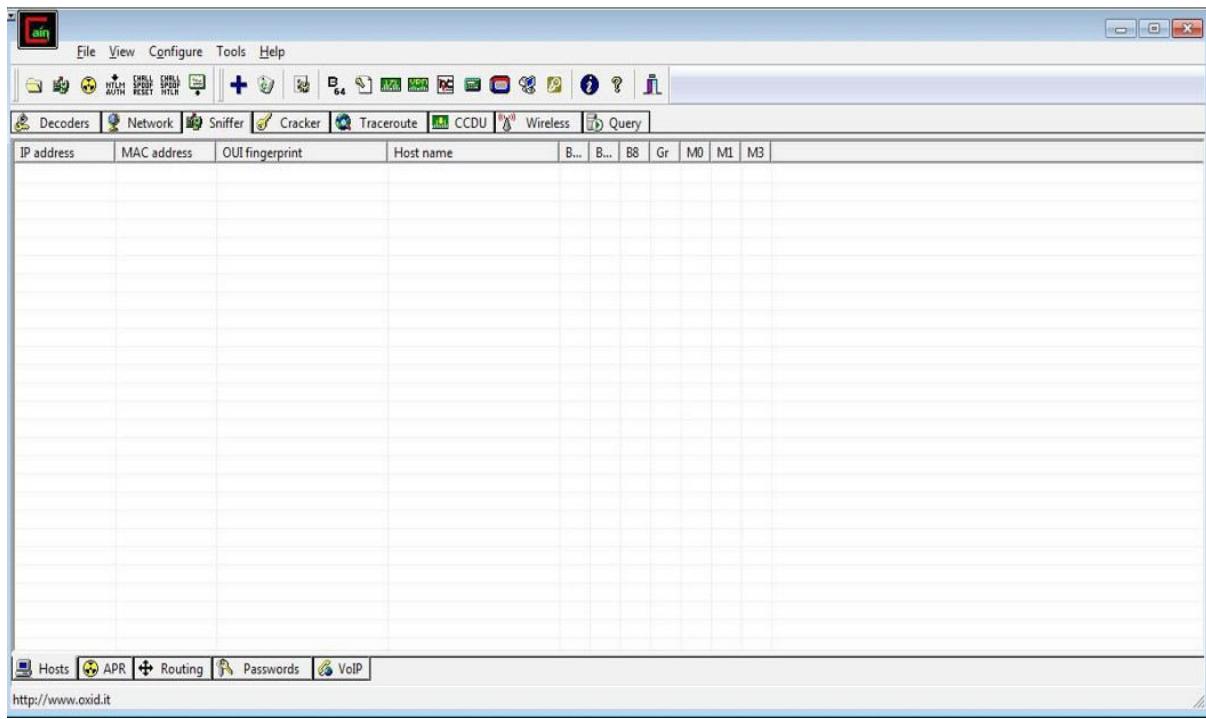
PRACTICAL NO: 09

a. Performing Password Cracking [Cain & Abel]

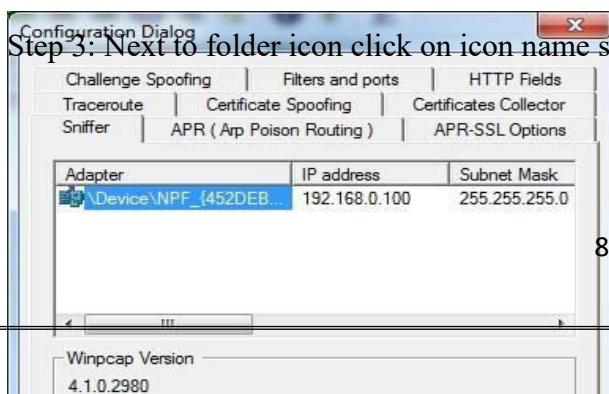
Step 1: Install and open Cain and Abel.



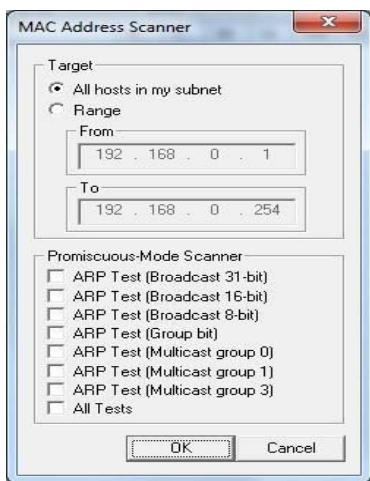
Step 2: Select sniffer on the top.



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



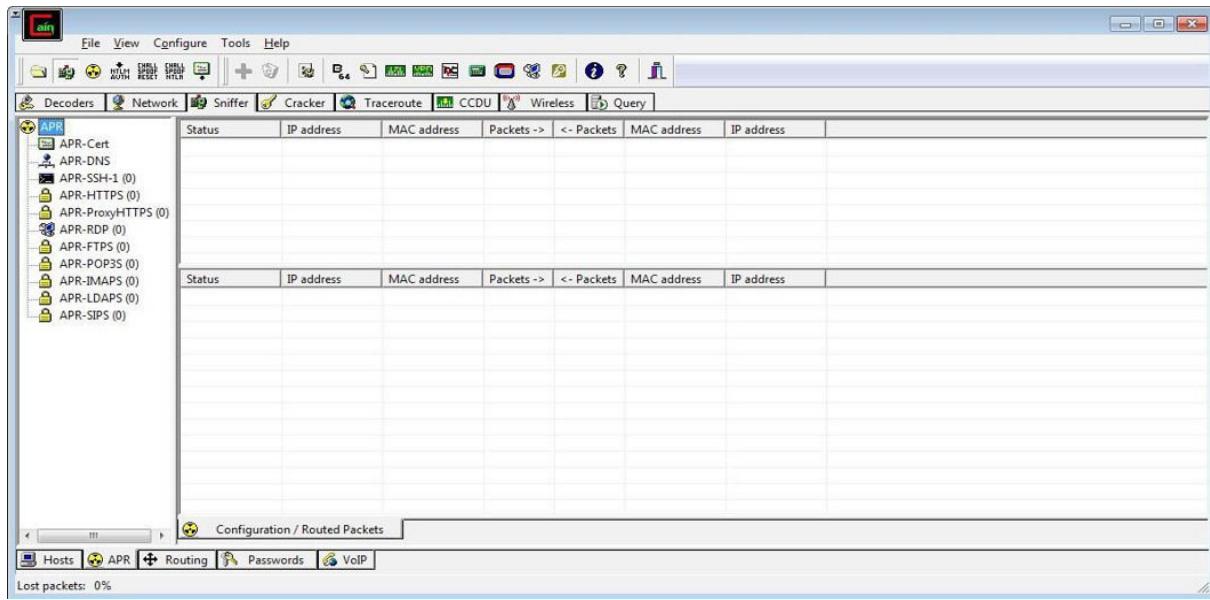
Step 4: Click on “+” icon on the top. Click on ok.



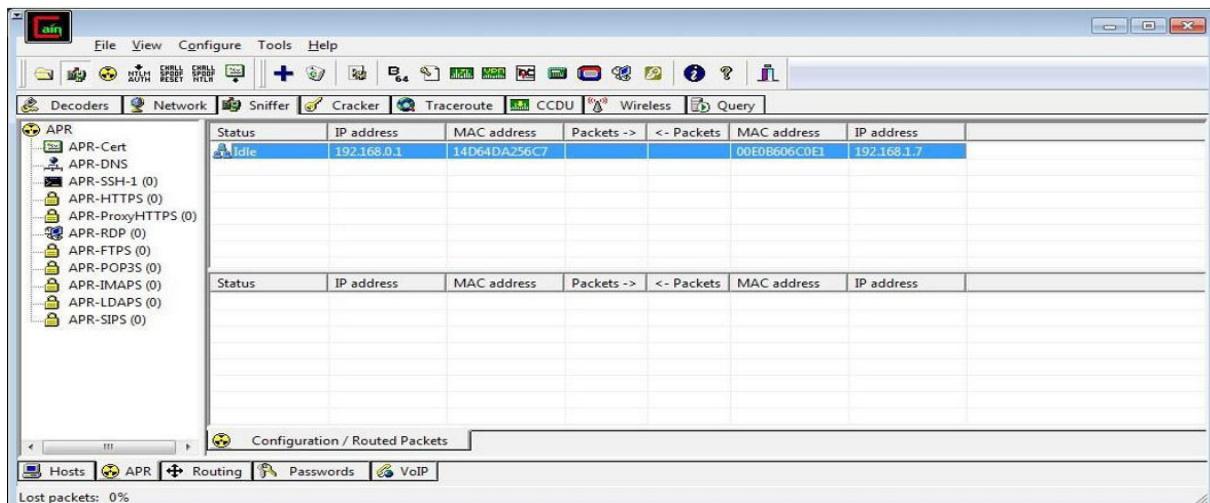
Step 5: Shows the Connected host.

IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8...	Gr	M0	M1	M3
192.168.0.1	F46D04E9CC74	D-Link International								
192.168.0.56	50E54992356C	ASUSTek COMPUTER INC.								
192.168.0.57	BCAEC5560745	GIGA-BYTE TECHNOLOGY ...								
192.168.0.71	94DE8097D224	ASUSTek COMPUTER INC.								
192.168.0.72	F07D687CE6C8	GIGA-BYTE TECHNOLOGY ...								
192.168.0.100	00E0B606C002	D-Link Corporation								
192.168.0.185	00E0B606C002	Entrada Networks								
192.168.0.225	50E549BE2013	GIGA-BYTE TECHNOLOGY ...								
192.168.0.230	50E54946F9F8	GIGA-BYTE TECHNOLOGY ...								
192.168.0.233	001901800BE9	Intel Corporate								
192.168.0.236	94DE808FCFB3	GIGA-BYTE TECHNOLOGY ...								
192.168.0.237	94DE808FD25E	GIGA-BYTE TECHNOLOGY ...								
192.168.0.250	001761101CC6									
192.168.0.251	001761103976									
192.168.1.1	001802FC170D	Alpha Networks Inc.								
192.168.1.3	001802FC170D	Alpha Networks Inc.								
192.168.1.5	24DEC6C4B904	Aruba Networks								
192.168.1.6	001E908798F5	Elitelgroup Computer Syste...								
192.168.1.7	00E0B606C0E1	Entrada Networks								
192.168.1.8	24DEC6C4B8EC	Aruba Networks								

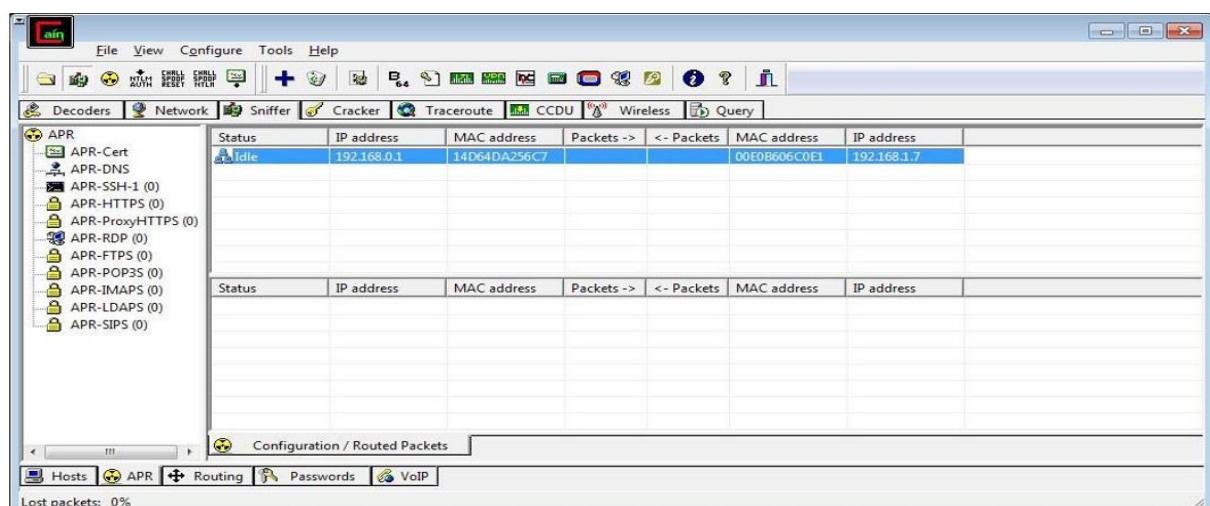
Step 6: Select Arp at bottom.



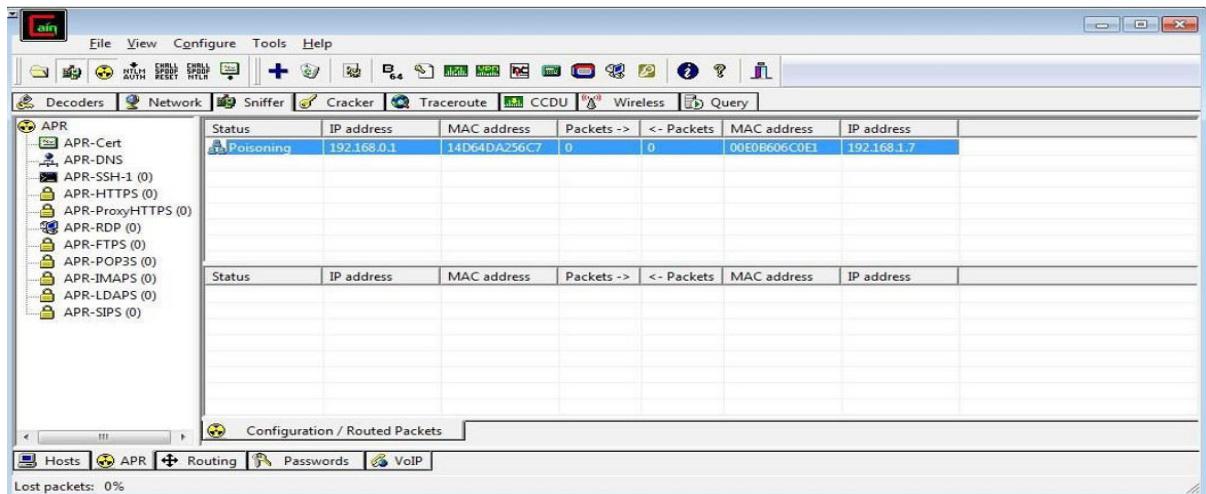
Step 7: Click on “+” icon at the top.



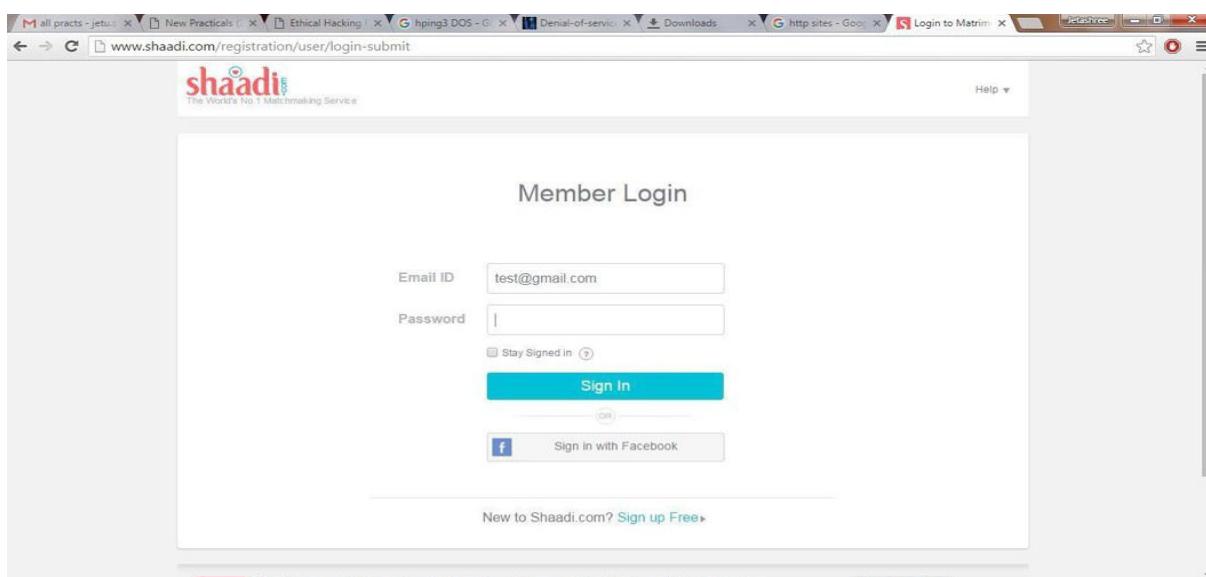
Step 8: Click on start/stop ARP icon on top.



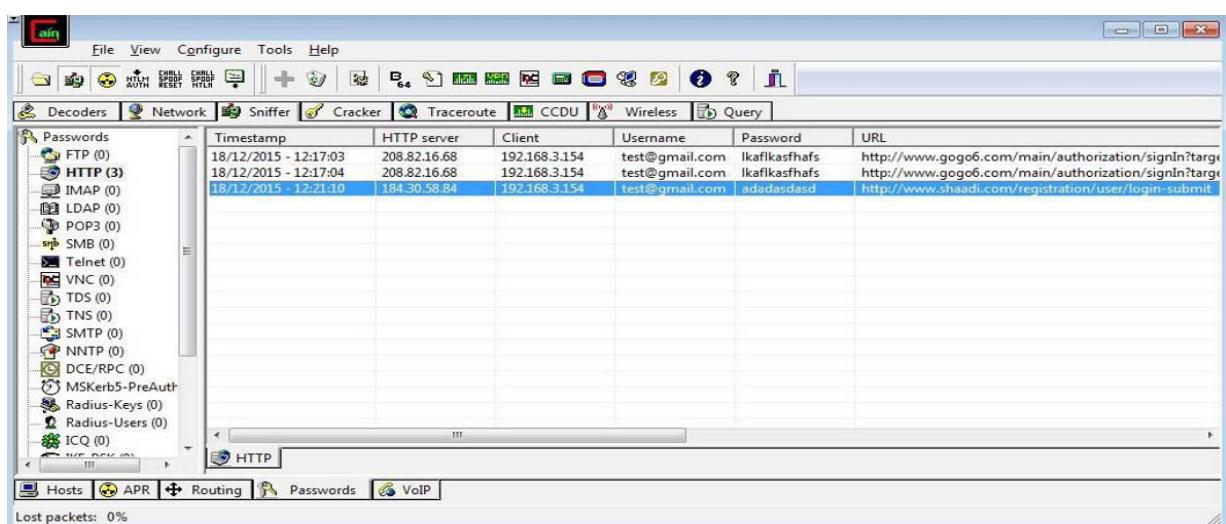
Step 9: Poisoning the source.



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

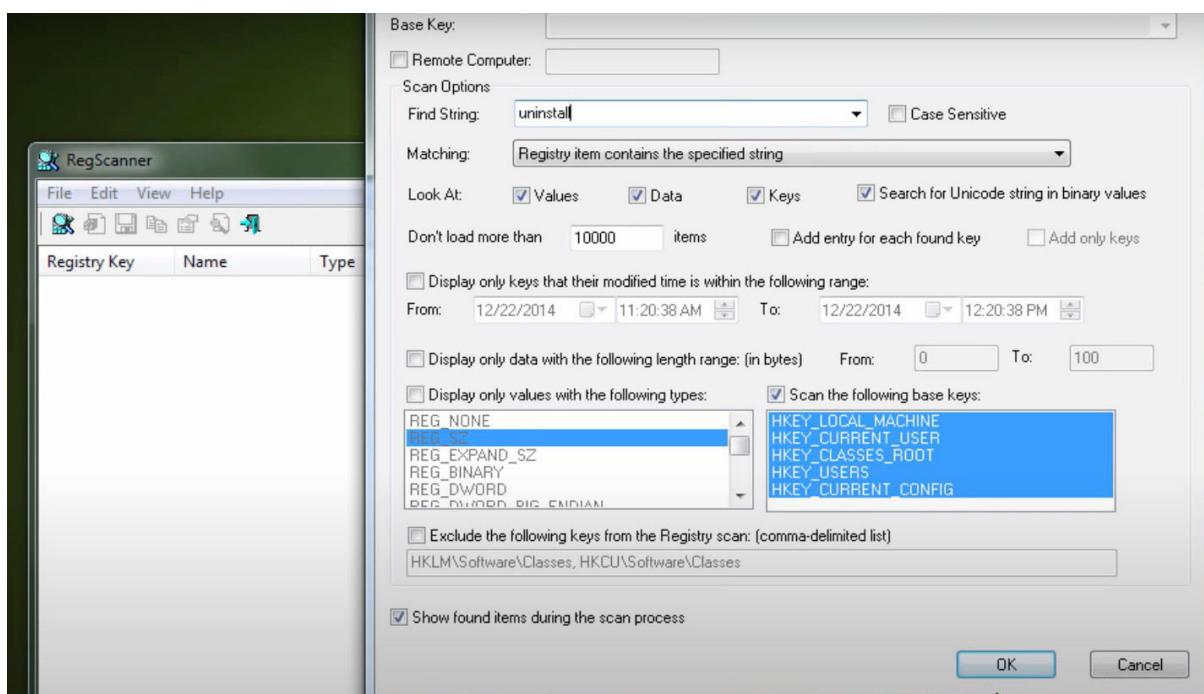
a. Scan Registry using RegScanner

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...	UninstallMana...	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...	FileDirectory	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...		Export Selected Items	Ctrl+E	1:36:39 PM 25
		Delete Selected Keys/Values	Ctrl+Del	3:53:38 AM 26
		Save Selected Items	Ctrl+S	3:54:30 AM 29
		Copy Selected Items	Ctrl+C	3:53:38 AM 36
		Copy Key	Ctrl+K	3:53:38 AM 21
		HTML Report - All Items		7:43:18 AM 4
		HTML Report - Selected Items		7:43:38 AM 4
		Choose Columns		7:43:38 AM 4
		Auto Size Columns	Ctrl+Plus	7:43:44 AM 4
		Open In RegEdit	F8	7:43:38 AM 28
		Properties	Alt+Enter	7:43:18 AM 4