Practical No 1: File System Analysis Using Autopsy

Aim: File System Analysis Using Autopsy

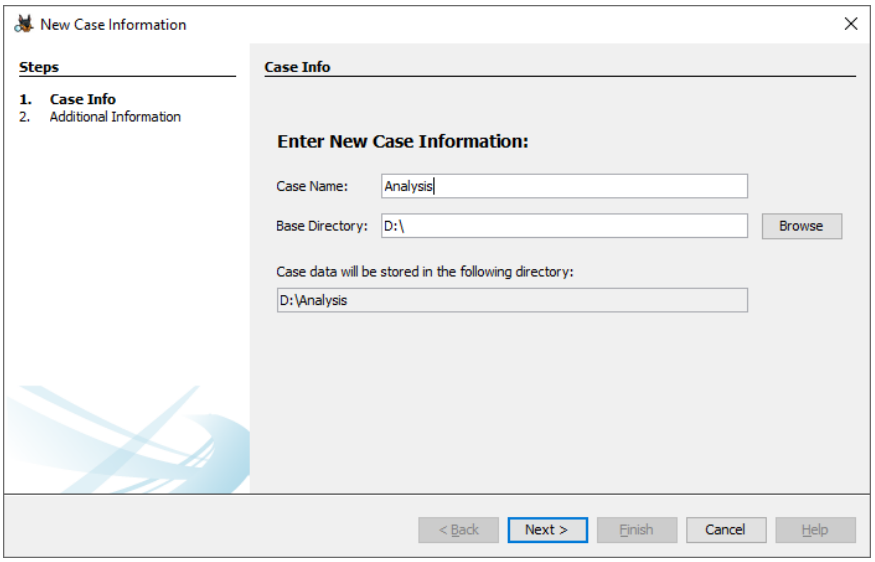
Steps:

1. Using starting Autopsy 3, a window will open with three selections to make:

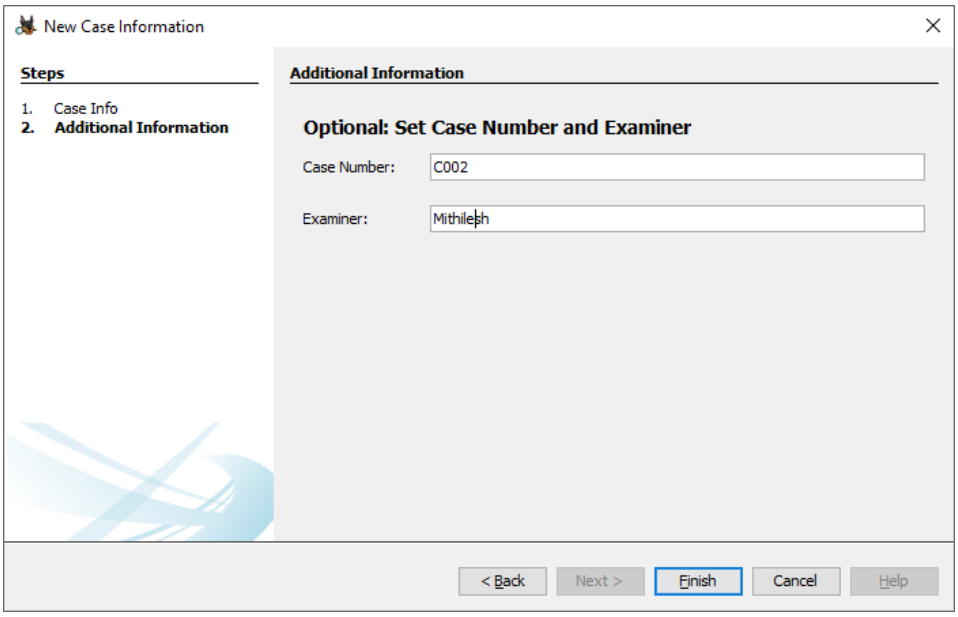
   Create a new case open existing case, or open a recent case.

2. Select 'New Case'.

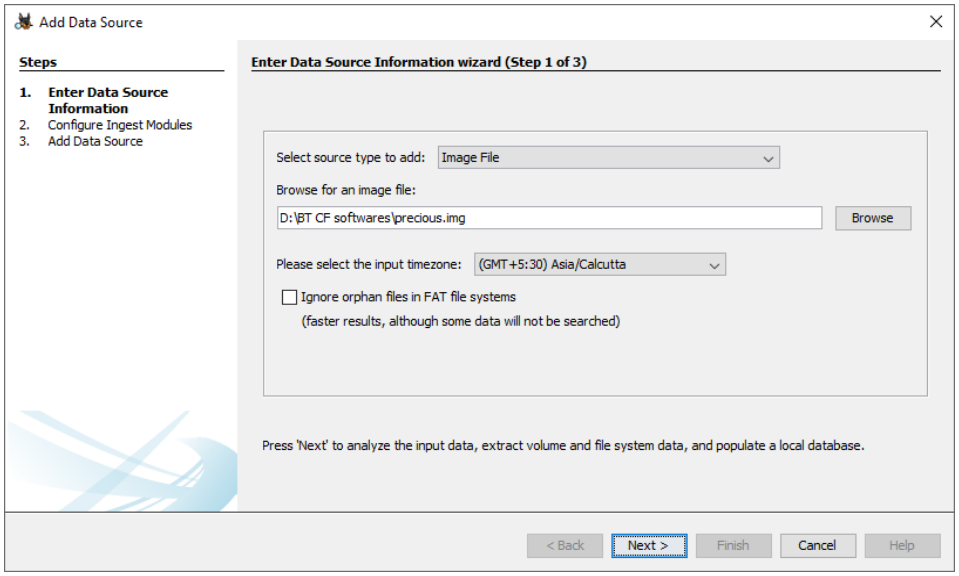
3. Fill the case info, give case name as 'Analysis' and browse to the directory where it should be stored and click on Next



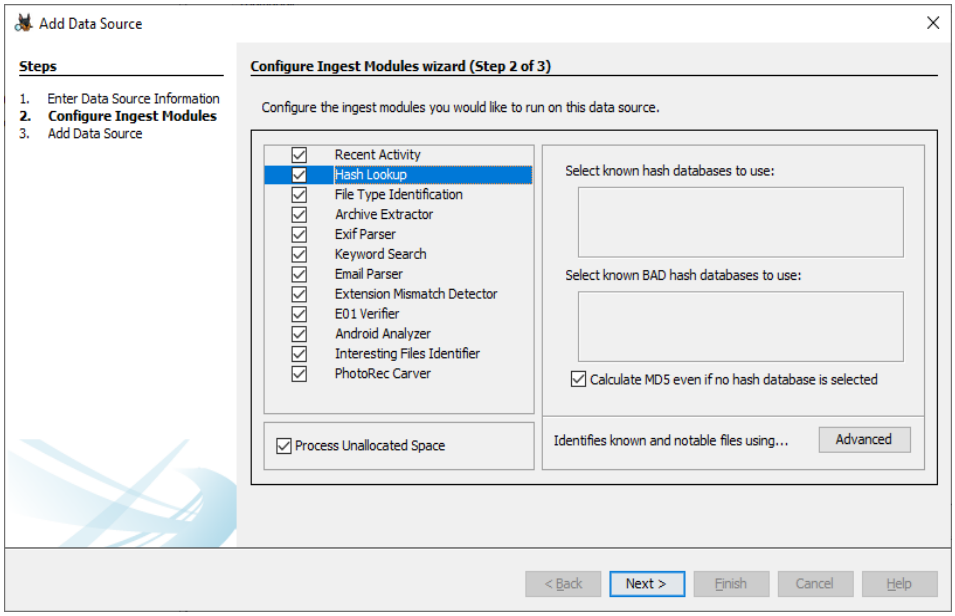
4. The next window will allow the investigator to fill in the case number as ‘C002’ and examiner name as ‘Mithilesh’. Click Finish.



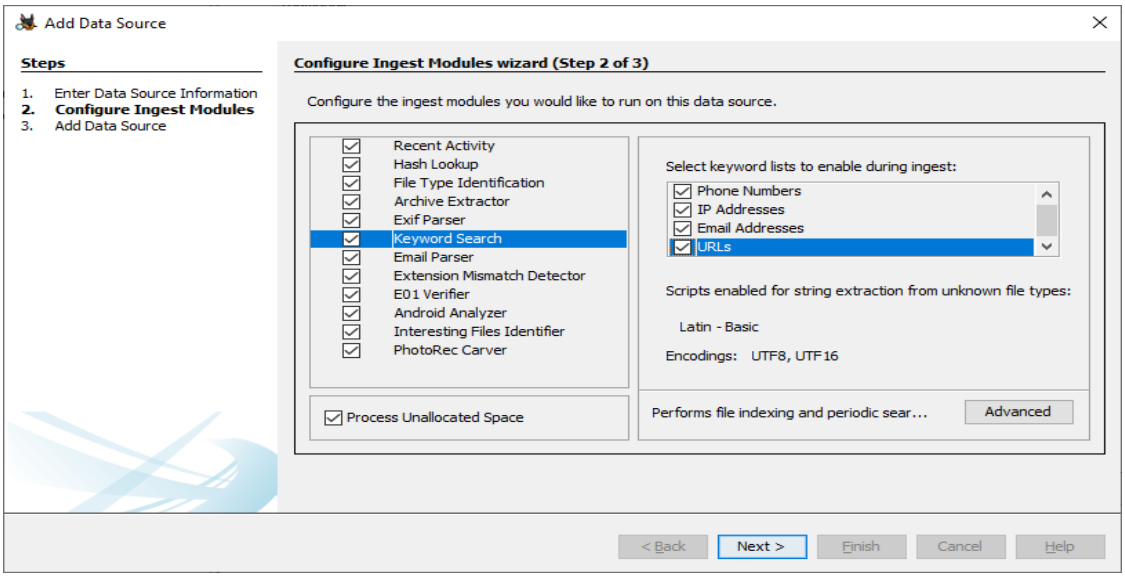
5. The next step in the investigation will be to add an image file to the case. Use the browse button to find the image that is desired to work with and select add. Click Next



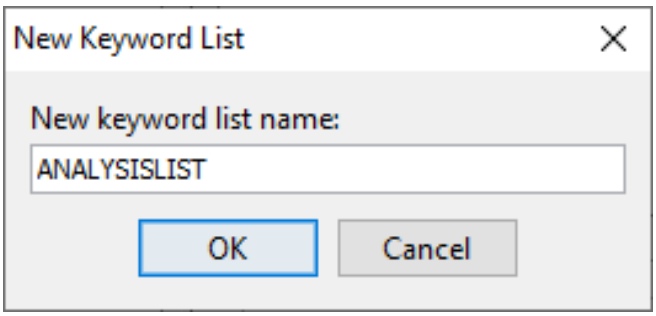
6. The following window will bring the investigator to the Ingest wizard Panel.
7. Under the Hash Lookup option there is the advanced option to add databases of known hashes.

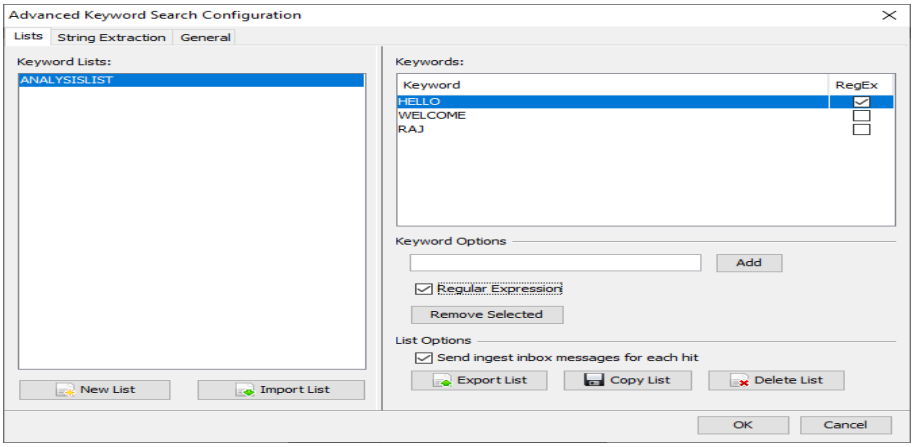


8. Under the keyword search option are many different lists that can be used to search for information. By default Phone Numbers, IP Addresses, Email Addresses and URL's are available.

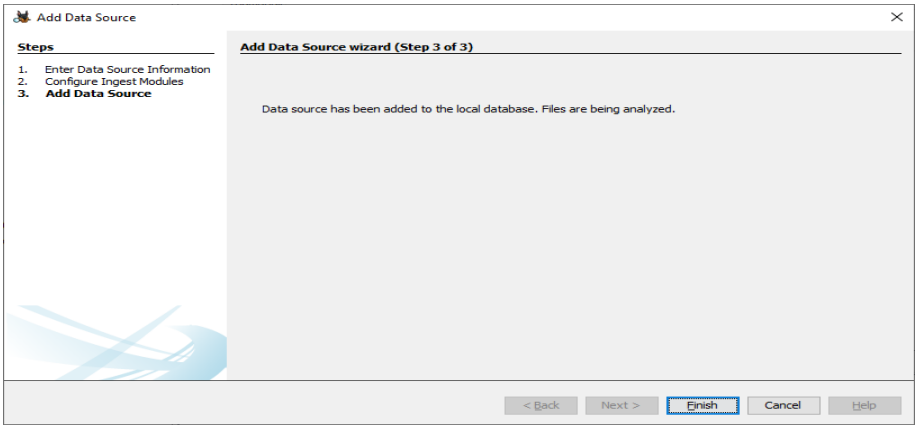


9. Select the Advanced button and a keyword list configuration window will open. In this new window select New List and type the name 'ANALYSIS LIST' that is desired for the list.
10. In the adjacent pane there is a blank section with a word bar and an Add button next to it. Type thee keyword desired(case sensitive) and select Add to add the word to the list.

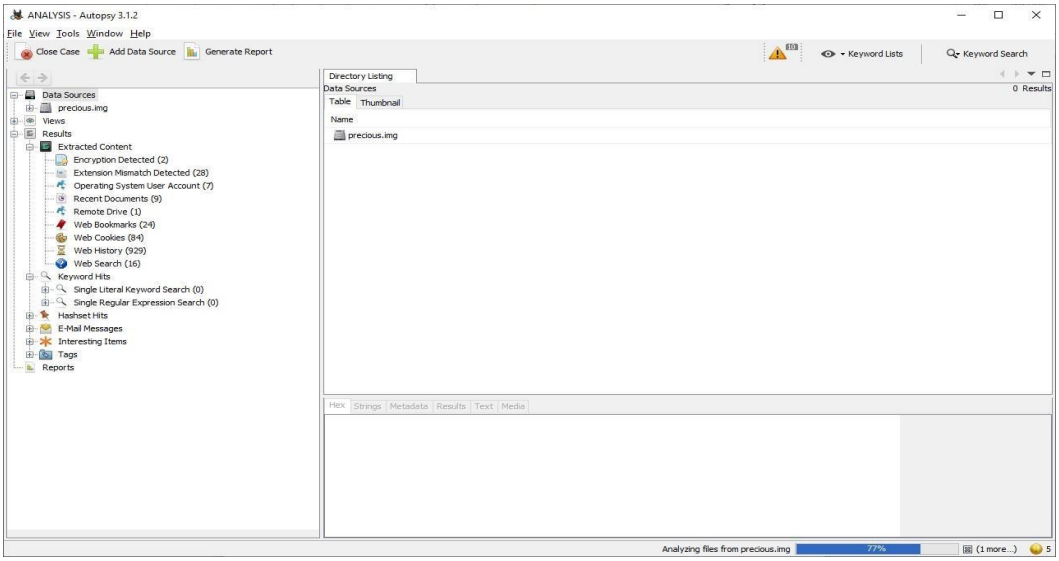




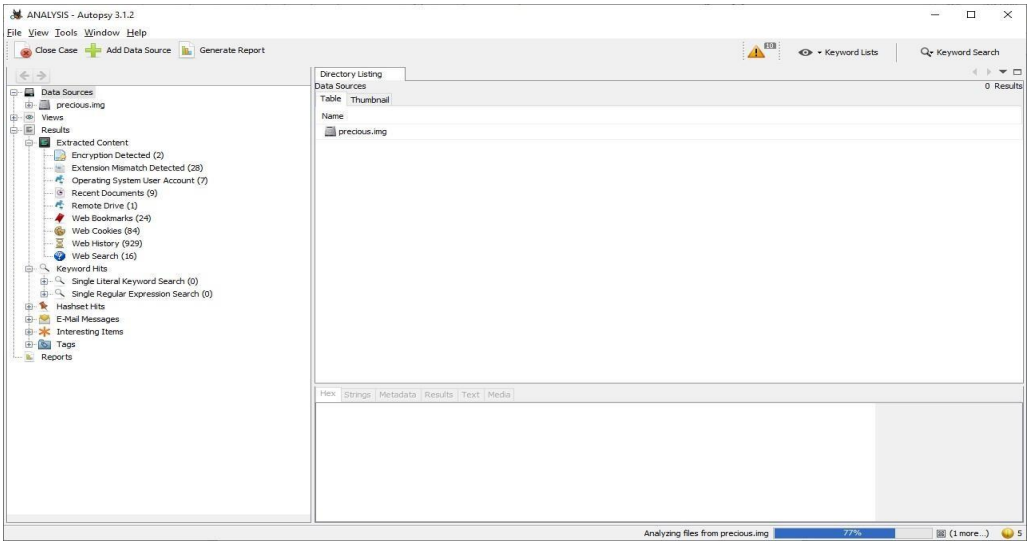
11. Click OK.



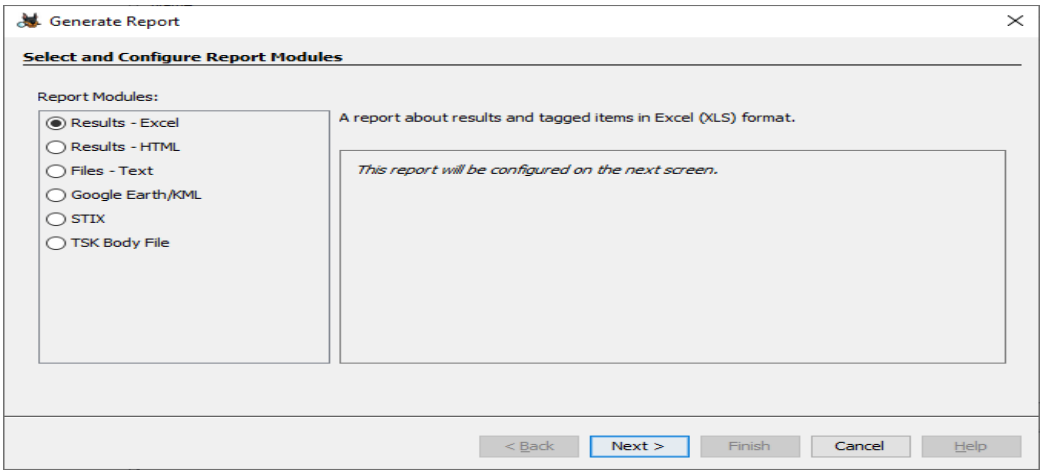
12. After the image is indexed the tree will be populated by the file system.

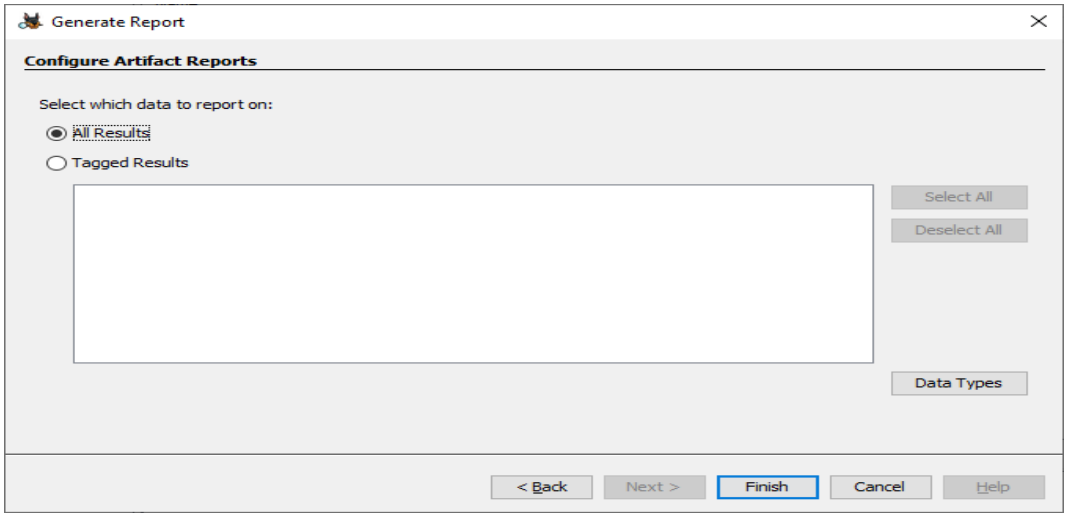


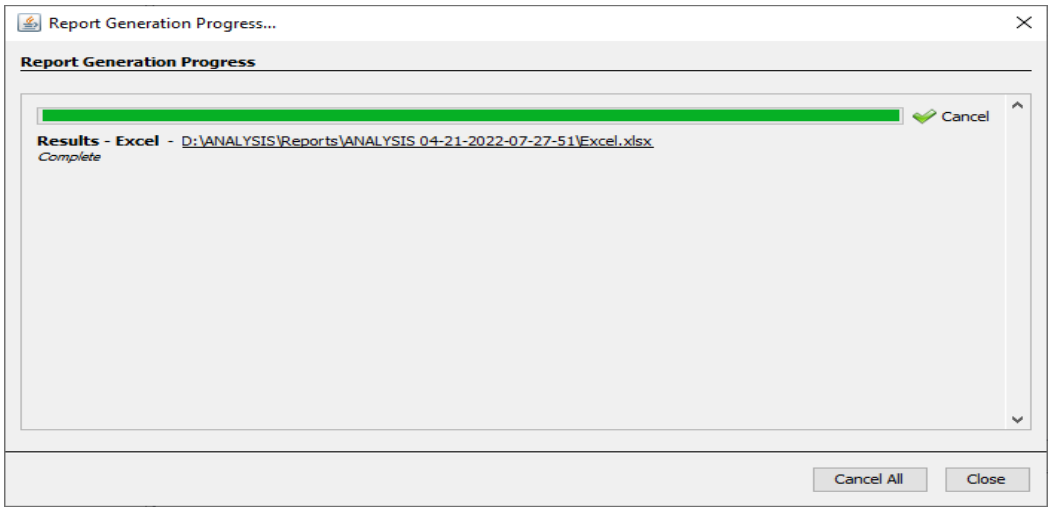
13. Click Generate Report. The report can be generated in three formats: Excel, XML and HTML.



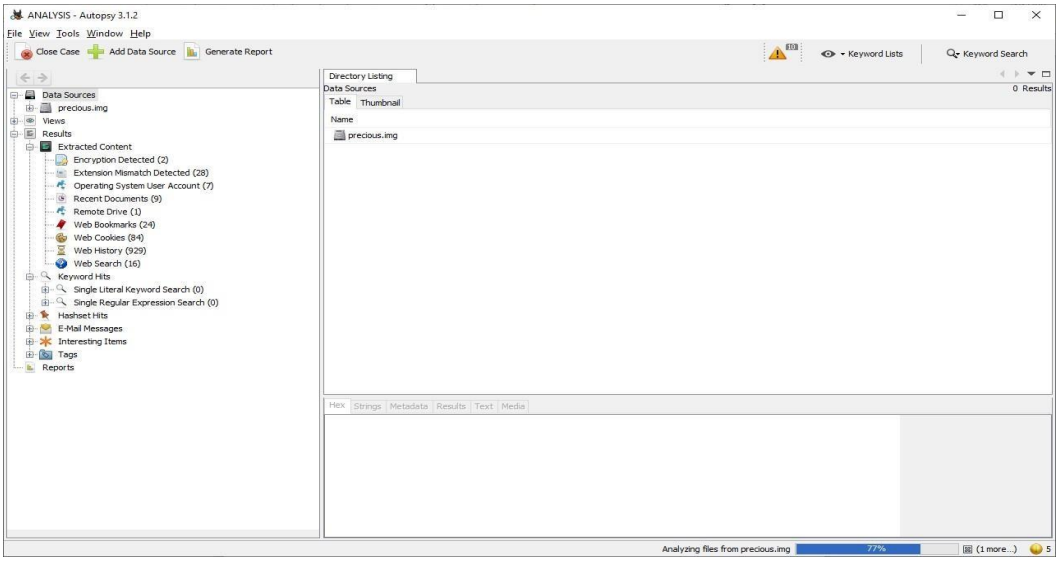
14. We select Results-Excel



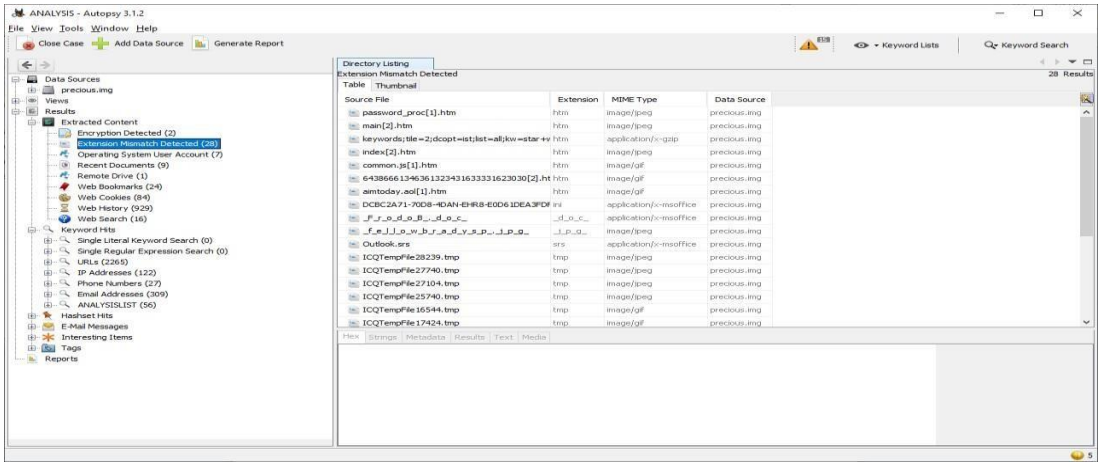




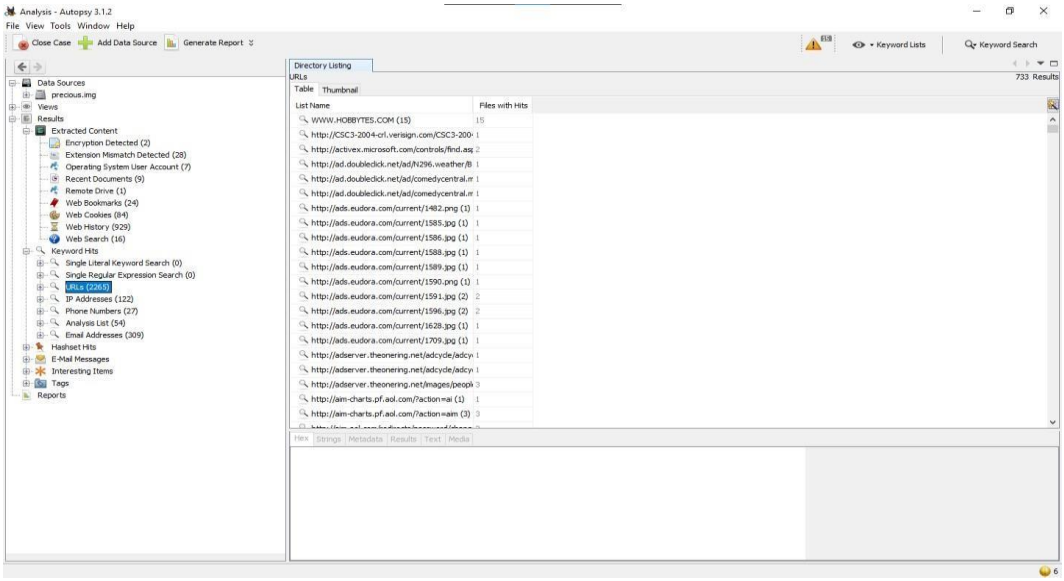
15. Looking at the tree, the top selection is titled “Images” this is where the acquired image is located and the bulk of the investigation, will take place. If the Images tab is expanded the investigator will see each image that was added to the investigation. By expanding an images tab the volumes of the image will be seen including the file system and unallocated space. Expanding the tab that contains the operating system will give the investigator a look at the root directory and the tree that contains most of the relevant information.



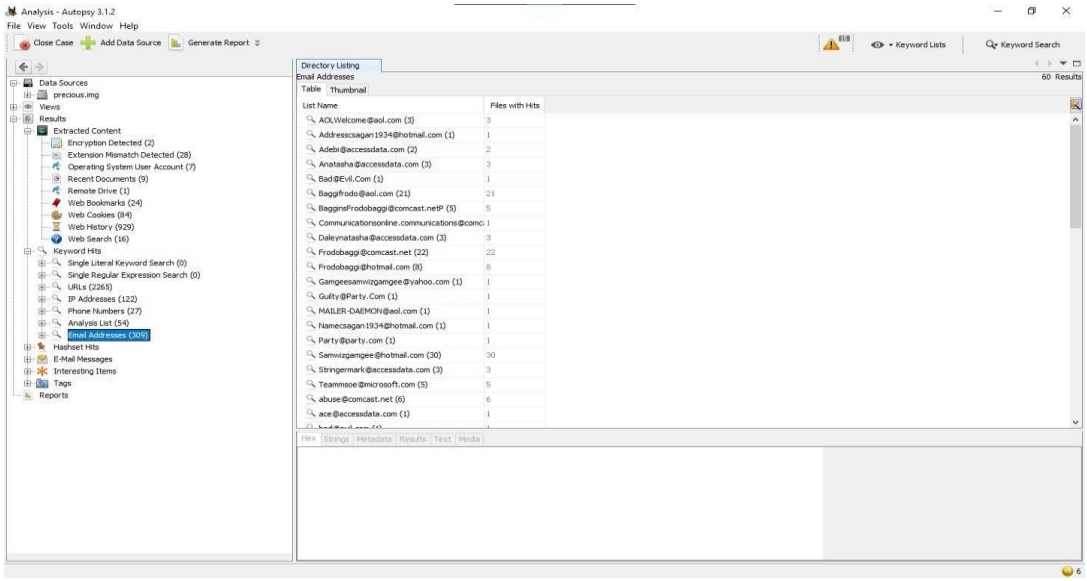
16. Below the Images tab is the “Views” tab that will allow the investigator to separate the information in the image into different categories such as by file types and by recent documents. The file type can be broken down into: images, video, audio and documents which includes the major text formats. Another section in the views tab is a new feature in Autopsy 3, the Recent Files tab.



17. The next tab that is seen is the Results tab, this is a new feature that displays all the information from the ingest process. There are 4 main categories when separating the results tab: Extracted Content, Keyword Hits, Hashset Hits, and E-mail Messages.



18. The last tab is Report tab which shows the generated report.



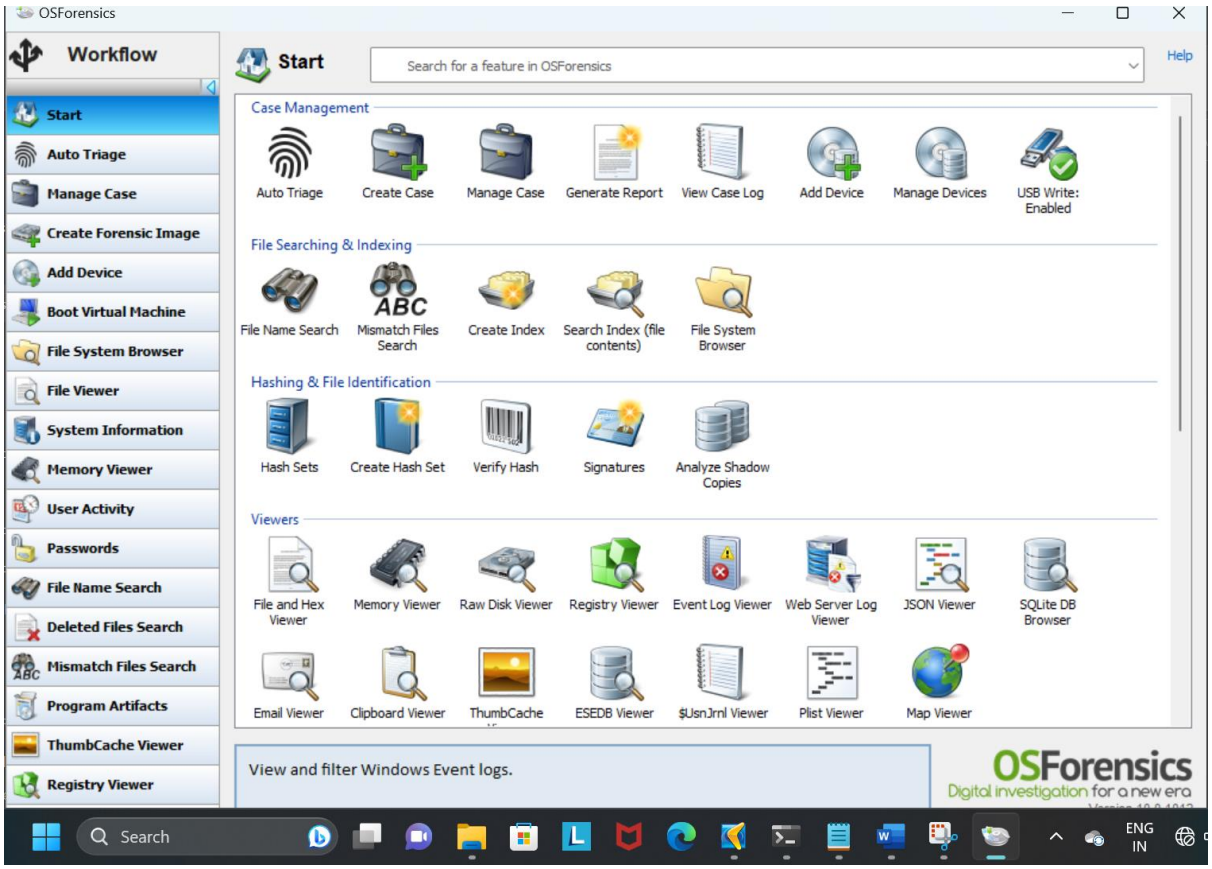
	A	B	C
1	Summary		
2			
3	Case Name:	Analysis	
4	Case Number:	C002	
5	Examiner:	Mithilesh	
6	Number of Images:	1	
7			
8			
9			
10			

Practical No. 2

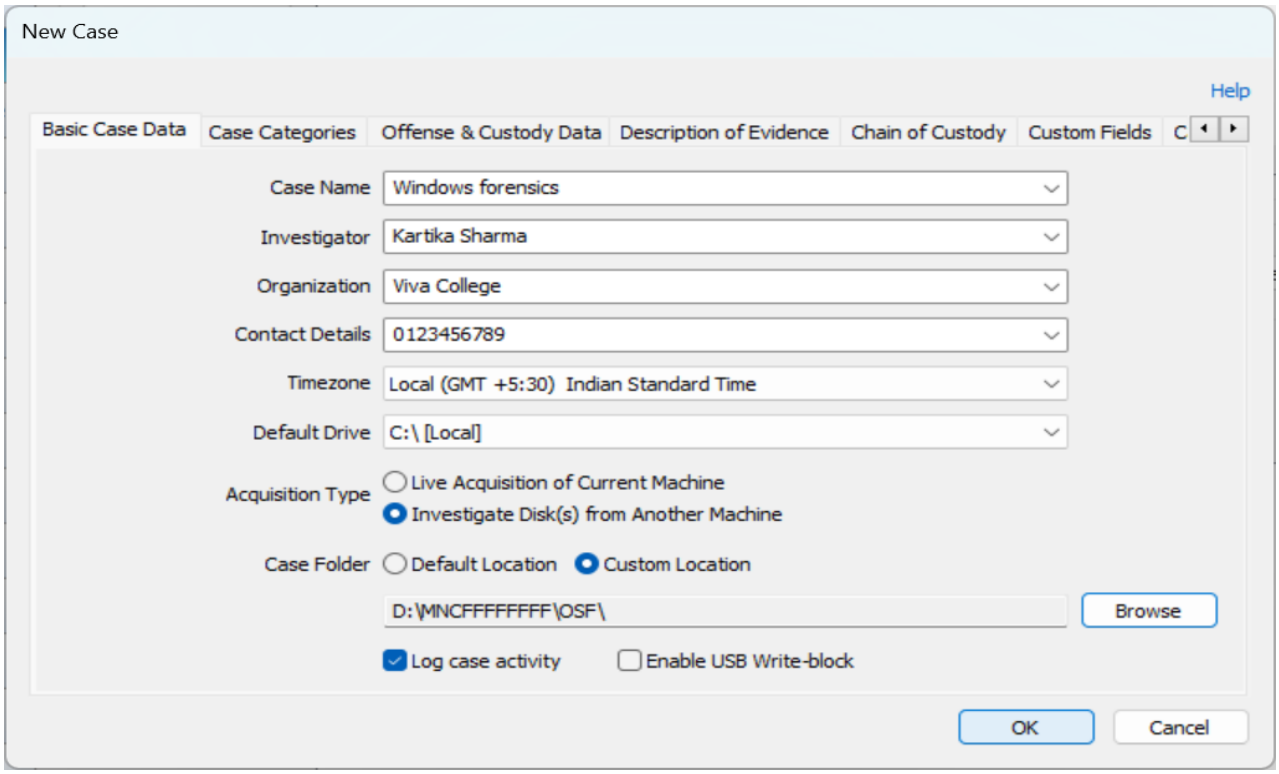
AIM: Windows Forensics using OS Forensic.

Step 1: Open OSF. Select continue using trial version.

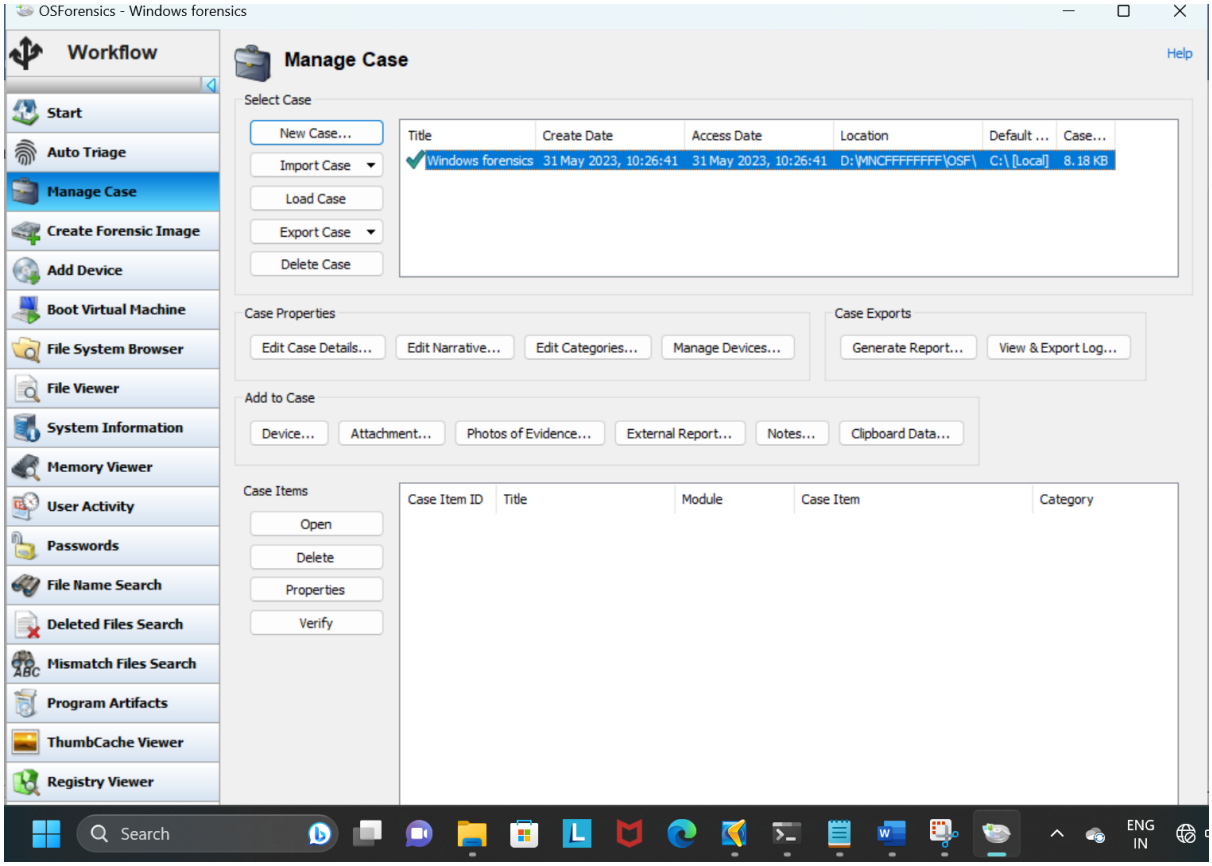
Step 2: The main screen opens. Click on create case.



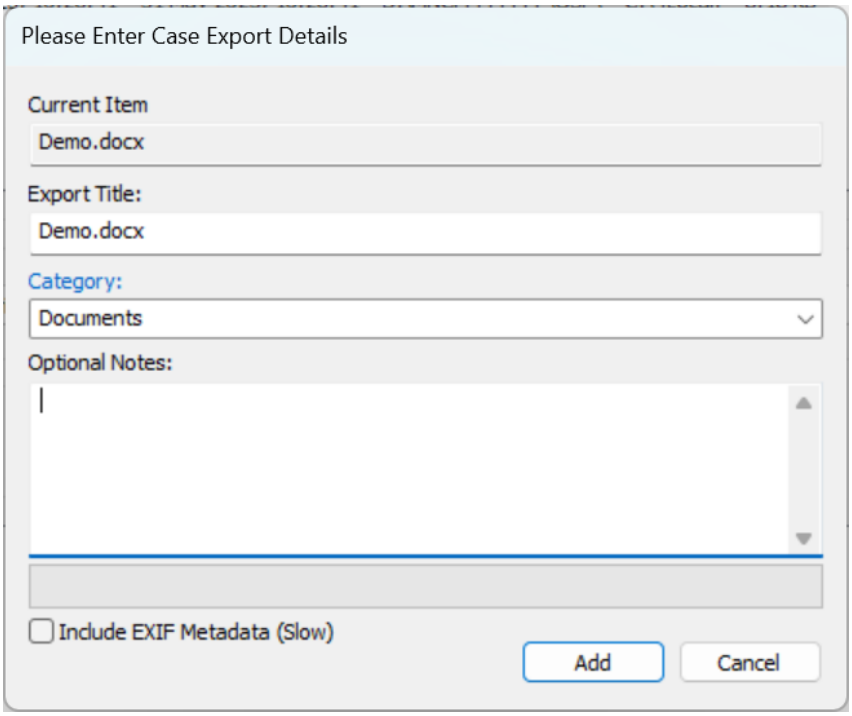
Step 3: Enter basic case details. Click on ok.

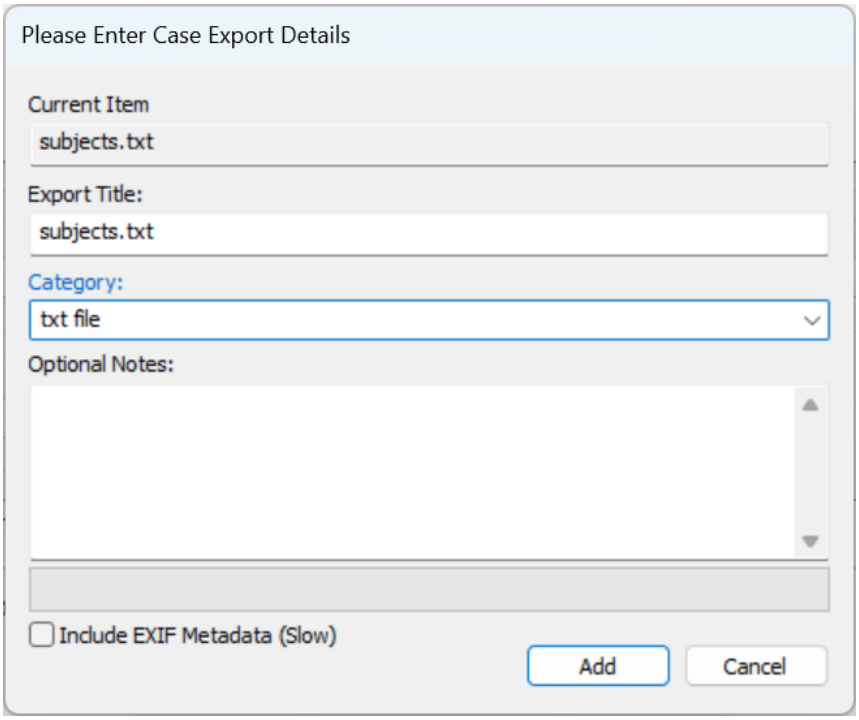


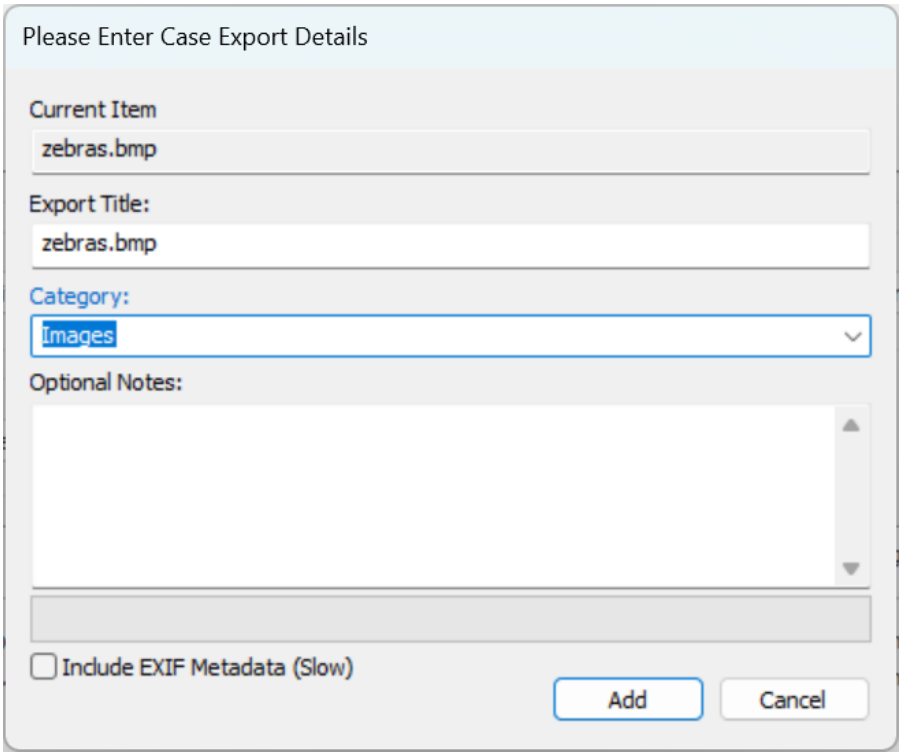
Step 4: case will be added in the manager case window.



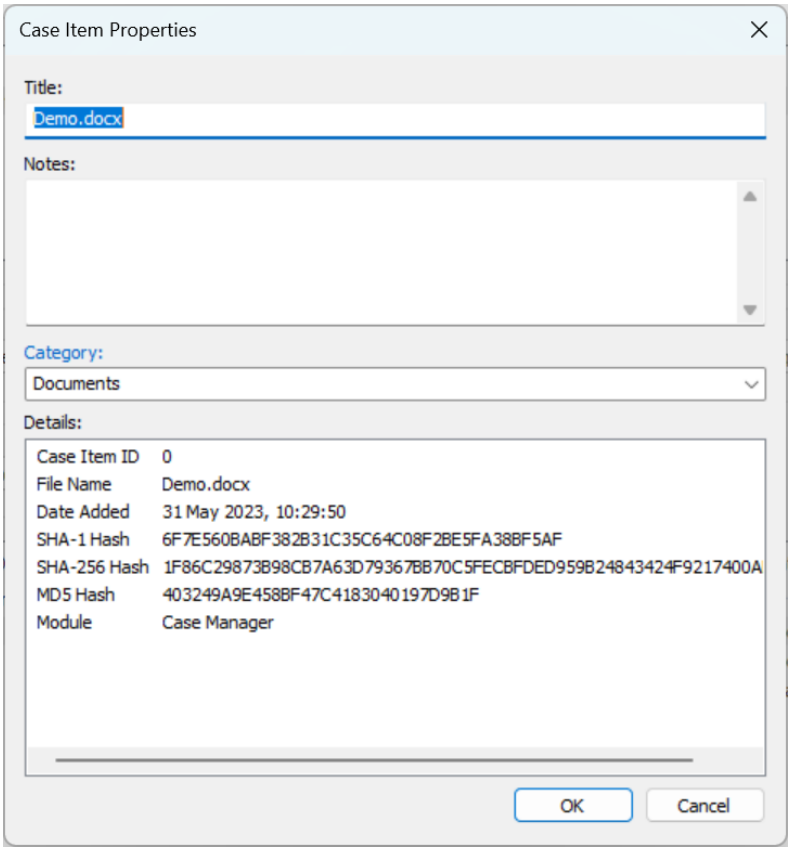
Step 5: In added case section, click on attachment to add evidence. Add a doc file, txt file and jpg file and give proper details while adding.



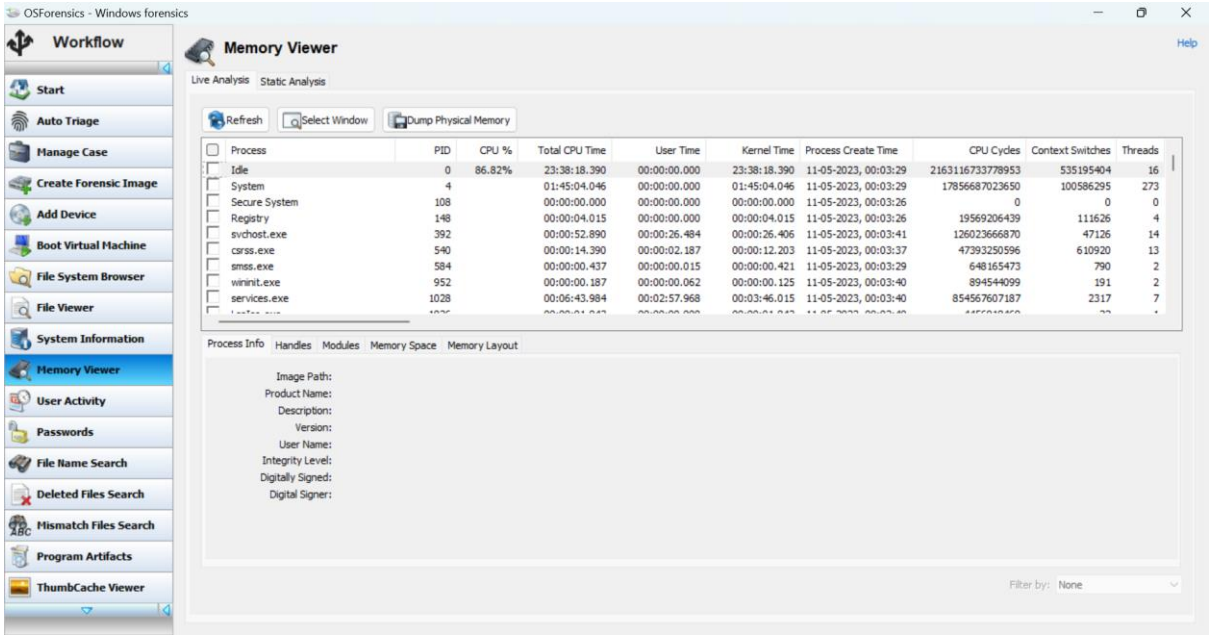




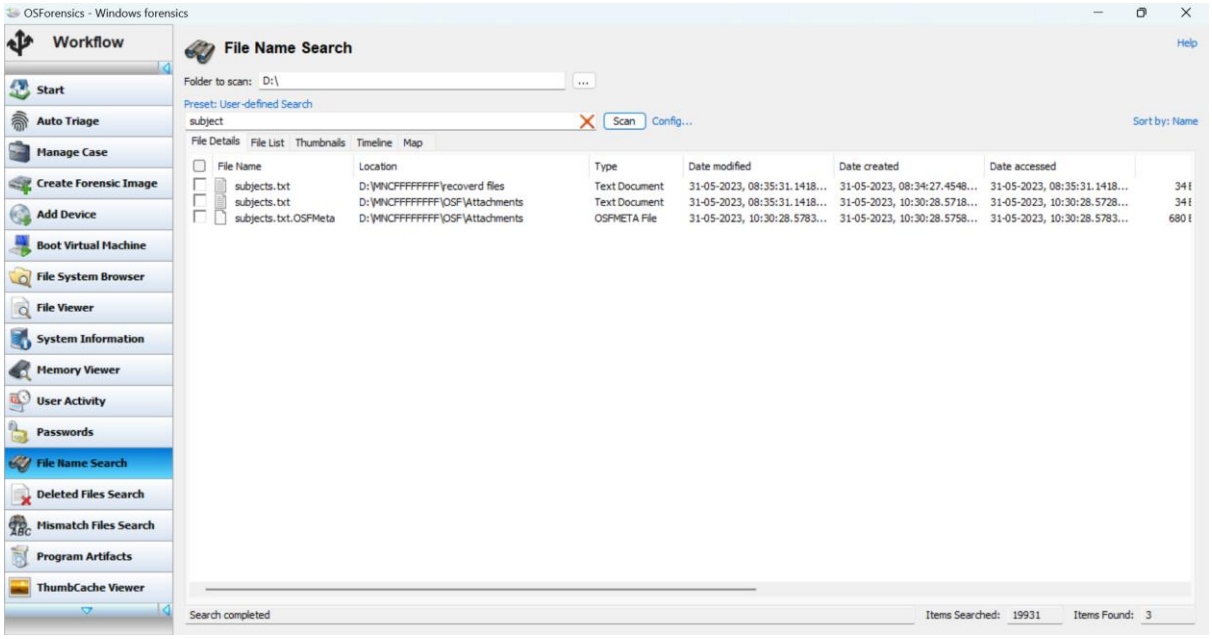
Step 6: After adding evidence, select doc file and click on properties button to check its information.



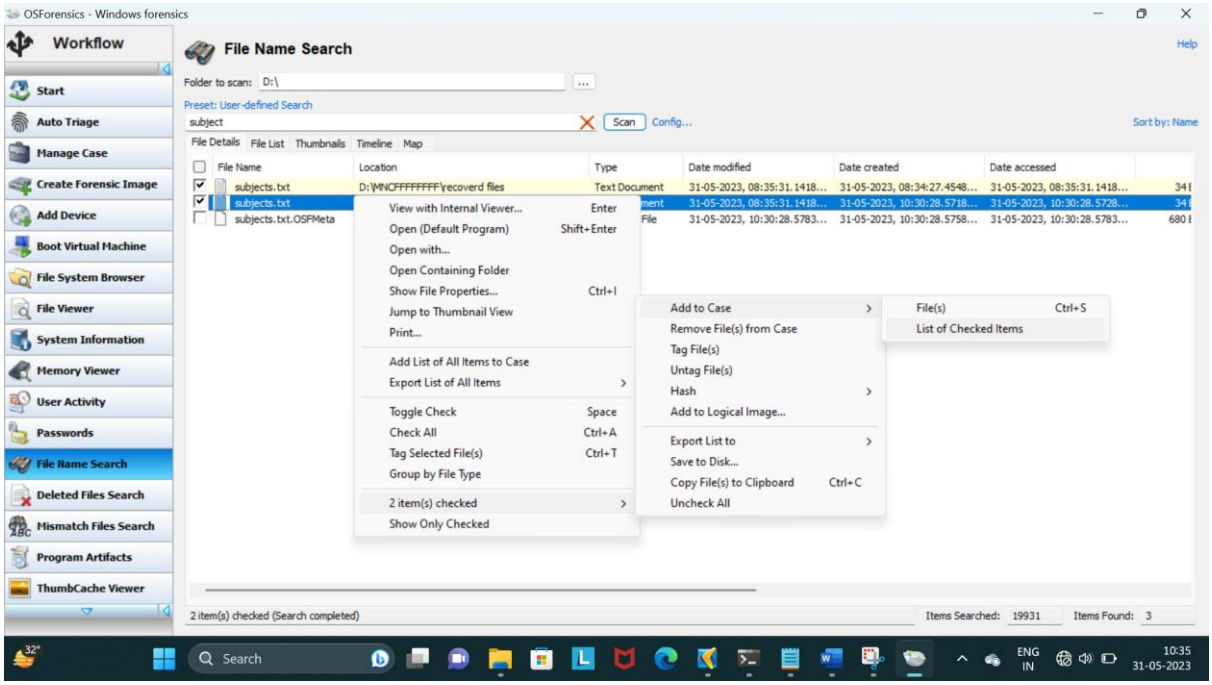
Step 7: From the left panel, click on memory viewer too see the total memory consumption details.

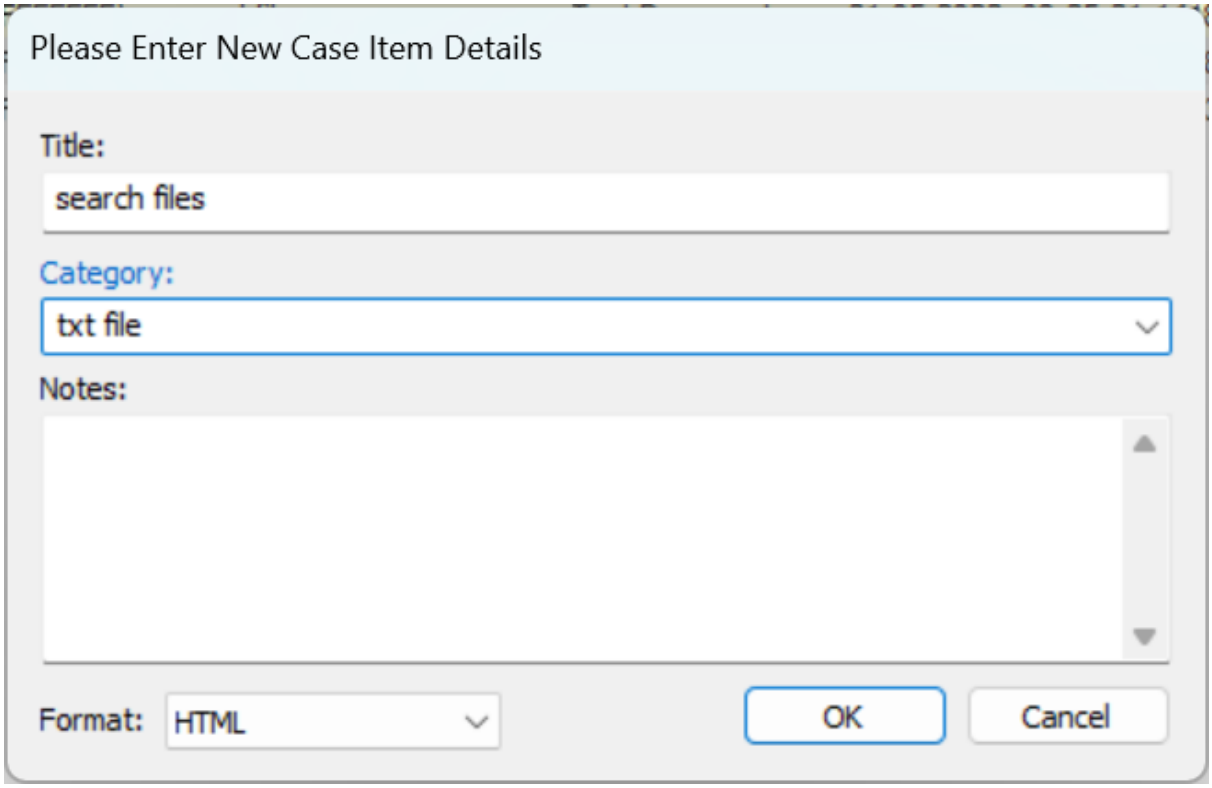


Step 8: From left panel, click on file name search, to search for a file. Add file in name and click on scan.

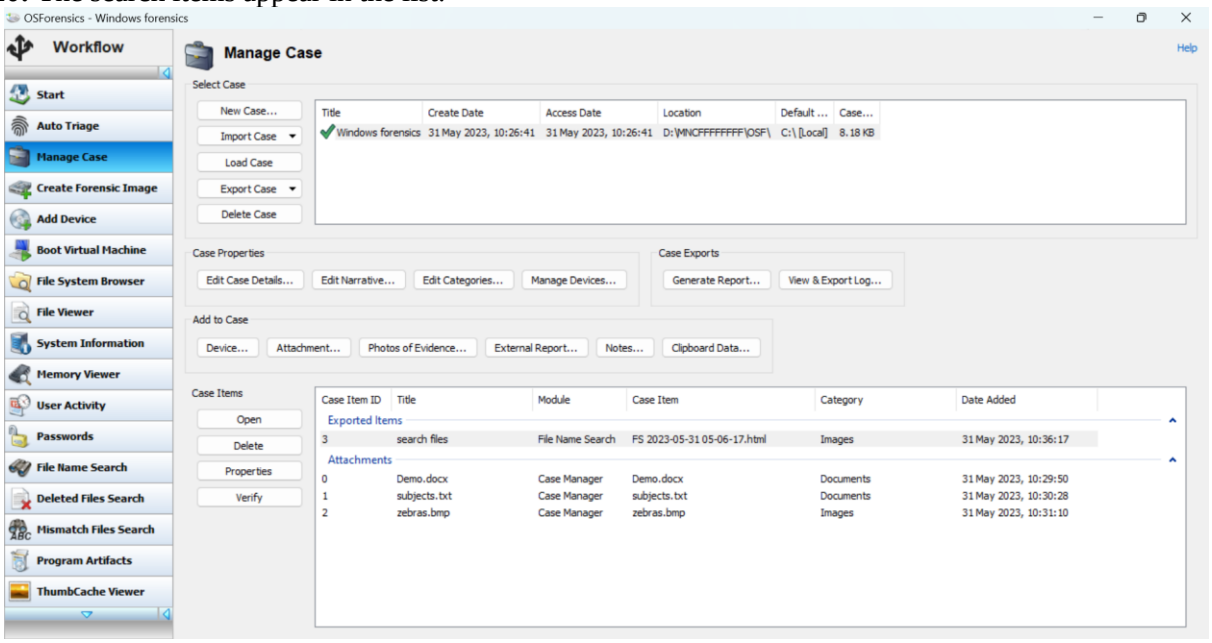


Step 9: To add searched files to a case, right click on the file, go to three times checked -> add to case -> list of checked items. Enter the details for the same.

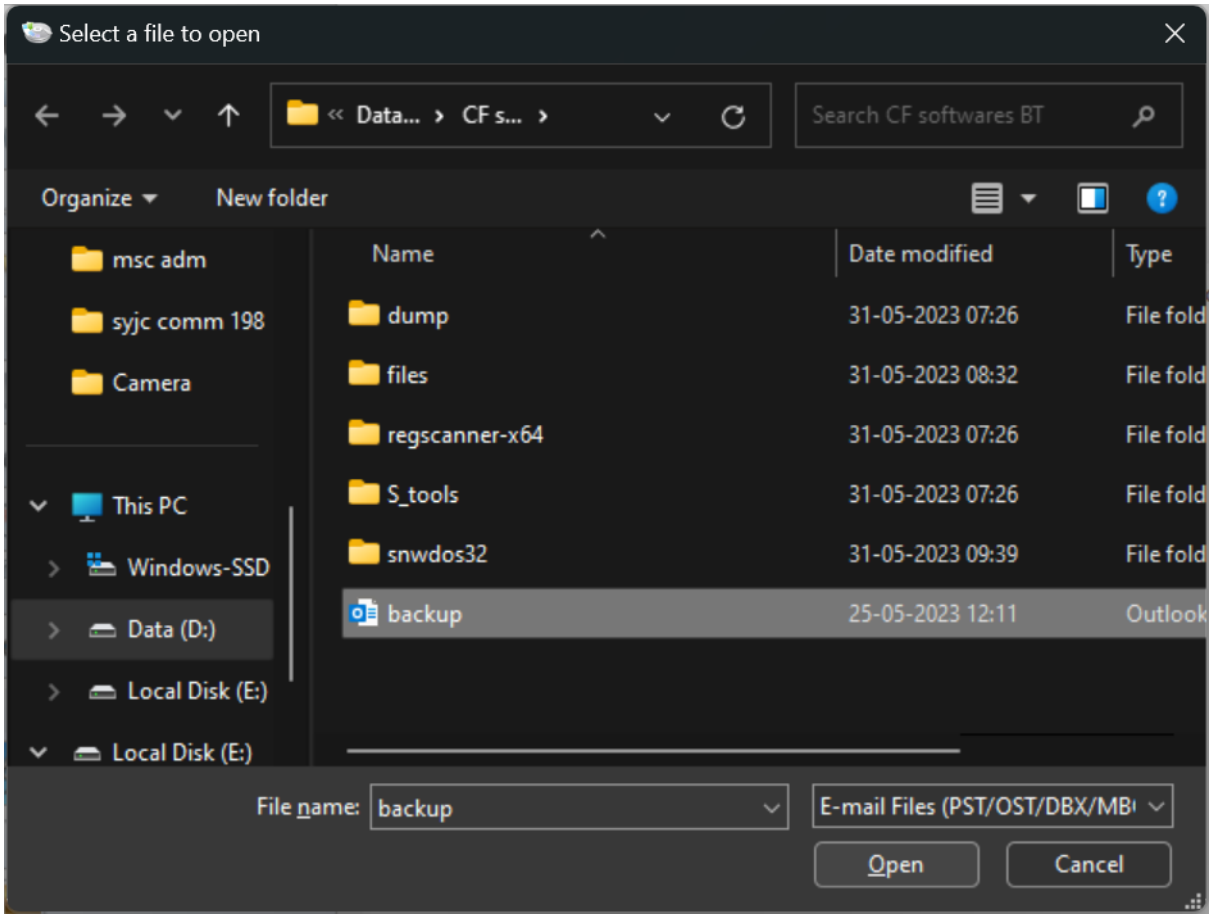

OSForensics - Windows forensics
Workflow
Start
Auto Triage
Manage Case
Create Forensic Image
Add Device
Boot Virtual Machine
File System Browser
File Viewer
System Information
Memory Viewer
User Activity
Passwords
File Name Search
Deleted Files Search
Mismatch Files Search
Program Artifacts
ThumbCache Viewer
File Name Search
Help
Folder to scan: D:\
Preset: User-defined Search
subject
Scan
Config...
Sort by: Name
File Details
File List
Thumbnails
Timeline
Map
File Name
Location
Type
Date modified
Date created
Date accessed
subjects.txt
subjects.txt
subjects.txt.OSFMeta
Text Document
31-05-2023, 08:35:31.1418...
31-05-2023, 08:34:27.4548...
31-05-2023, 10:30:28.5783...
31-05-2023, 10:30:28.5758...
View with Internal Viewer... Enter
Open (Default Program) Shift+Enter
Open with...
Open Containing Folder
Show File Properties... Ctrl+I
Jump to Thumbnail View
Print...
Add List of All Items to Case
Export List of All Items
Toggle Check Space
Check All Ctrl+A
Tag Selected File(s) Ctrl+T
Group by File Type
2 item(s) checked
Show Only Checked
Add to Case
Remove File(s) from Case
Tag File(s)
Untag File(s)
Hash
Add to Logical Image...
Export List to
Save to Disk...
Copy File(s) to Clipboard Ctrl+C
Uncheck All
File(s) Ctrl+S
List of Checked Items
2 item(s) checked (Search completed)
Items Searched: 19931
Items Found: 3
Search
ENG
IN
10:35
31-05-2023


Please Enter New Case Item Details
Title:
search files
Category:
txt file
Notes:
Format:
HTML
OK
Cancel

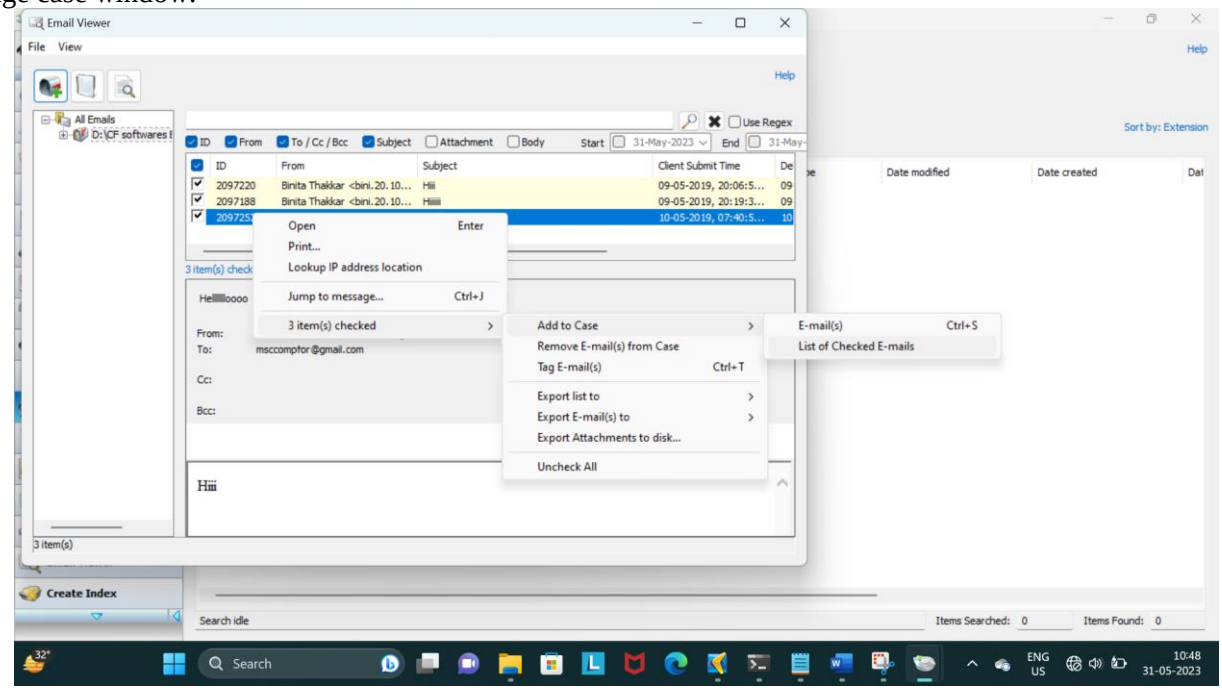
Step 10: The search items appear in the list.

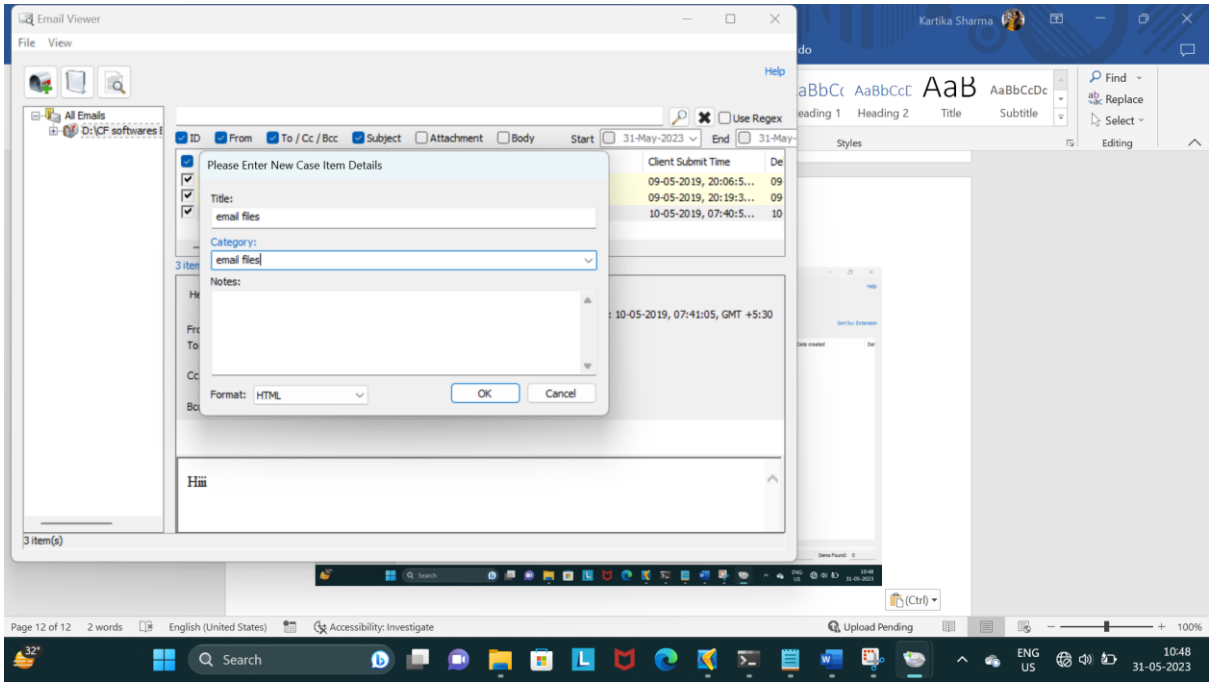


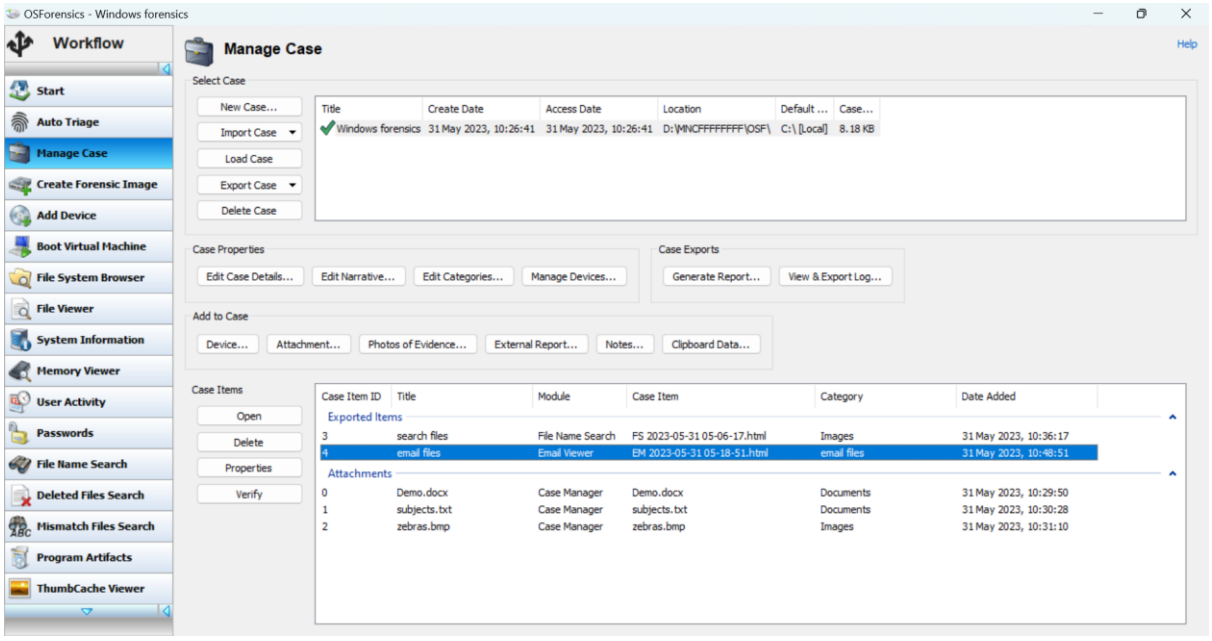
Step 11: To add any email file, on the left panel, click on email viewer. A window appears to select email file. Select back.pst file and click on open.



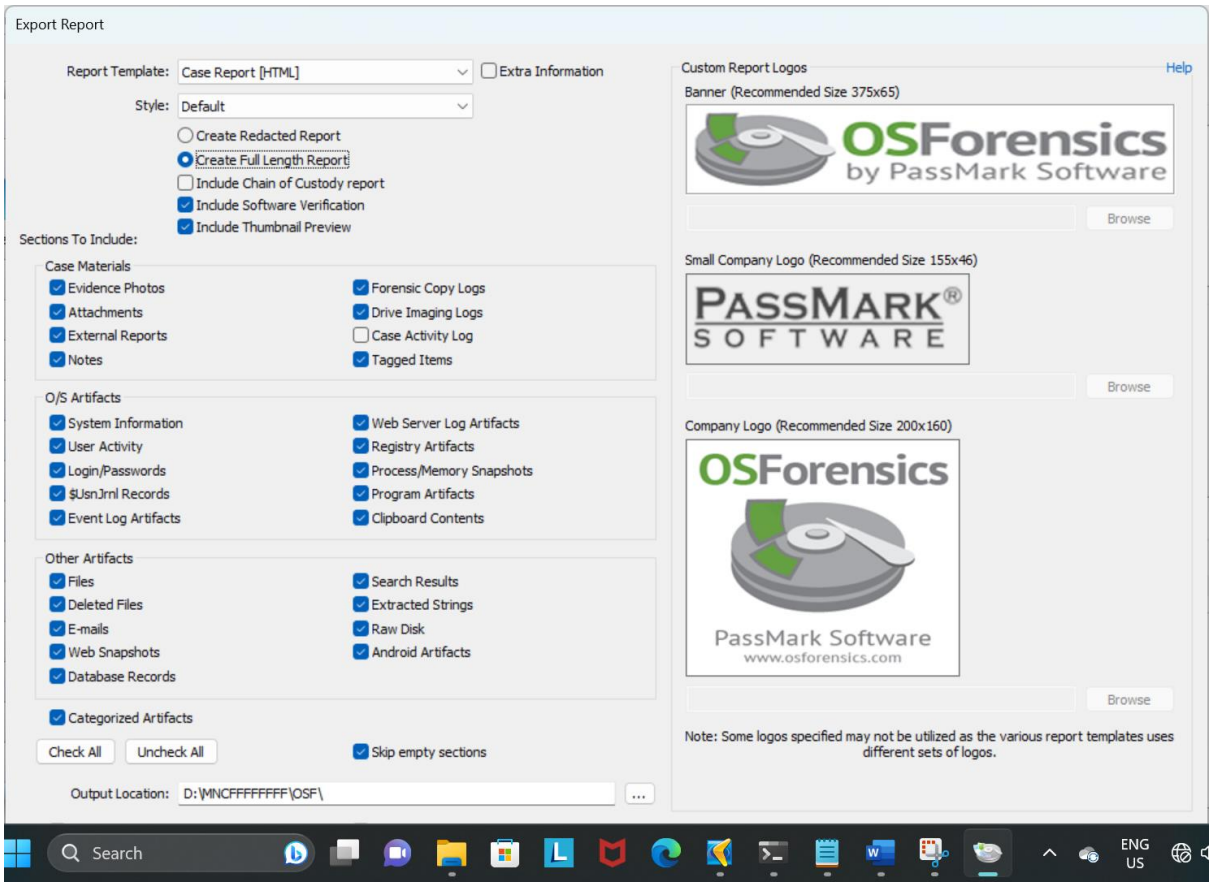
Step 12: They appear in email viewer select them and add them to the case as shown below. It will appear on manage case window.



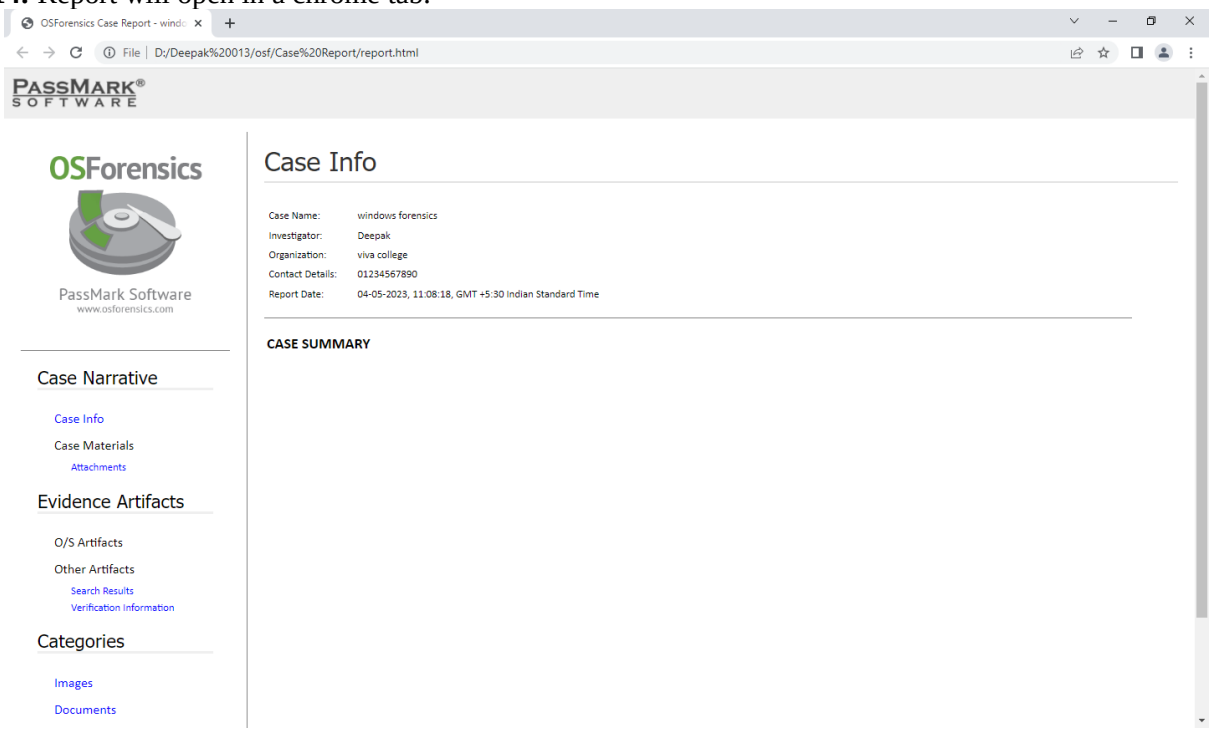


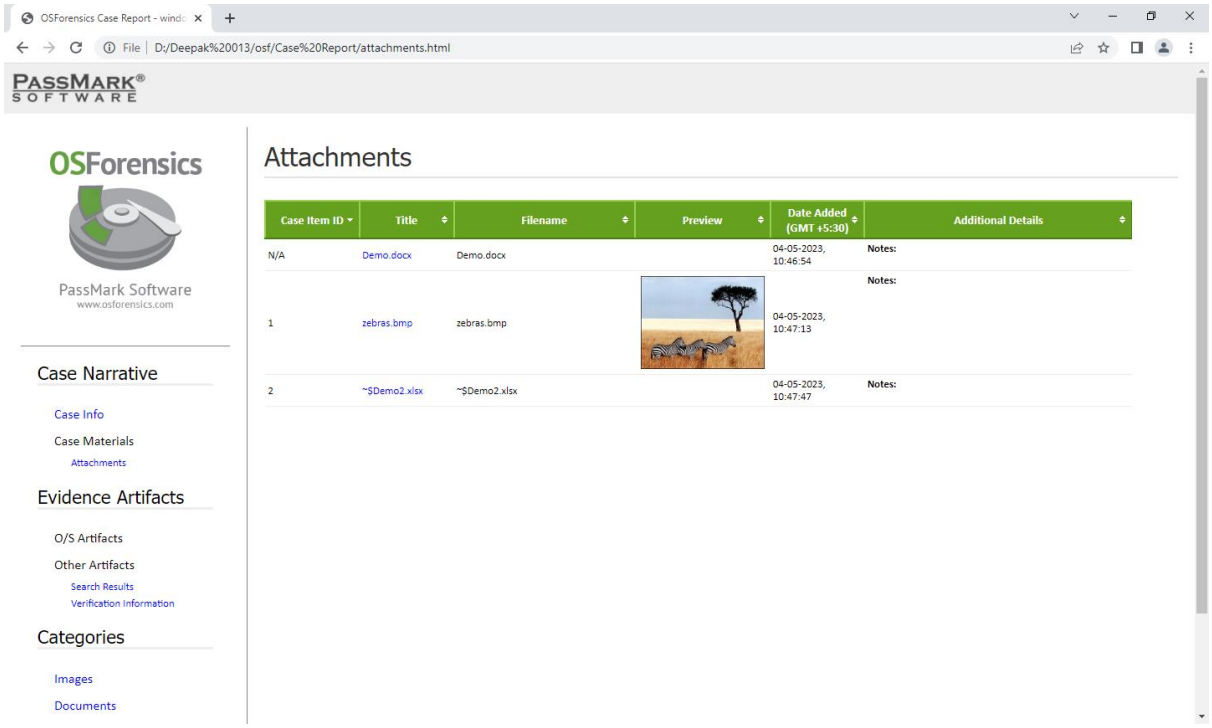


Step 13: Click on generate report. Select create full length report and click on ok.



Step 14: Report will open in a chrome tab.





Practical No 3

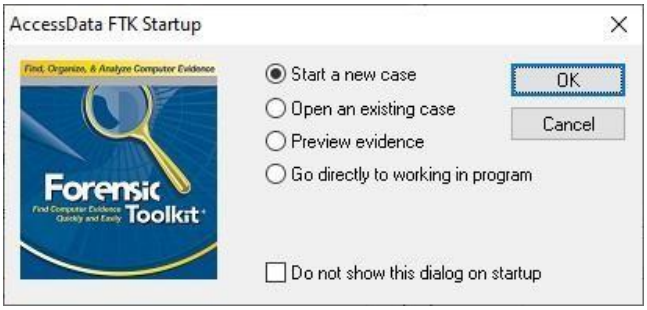
Aim: Using FTK and Writing reports using FTK

Steps:

A. Starting a New Case

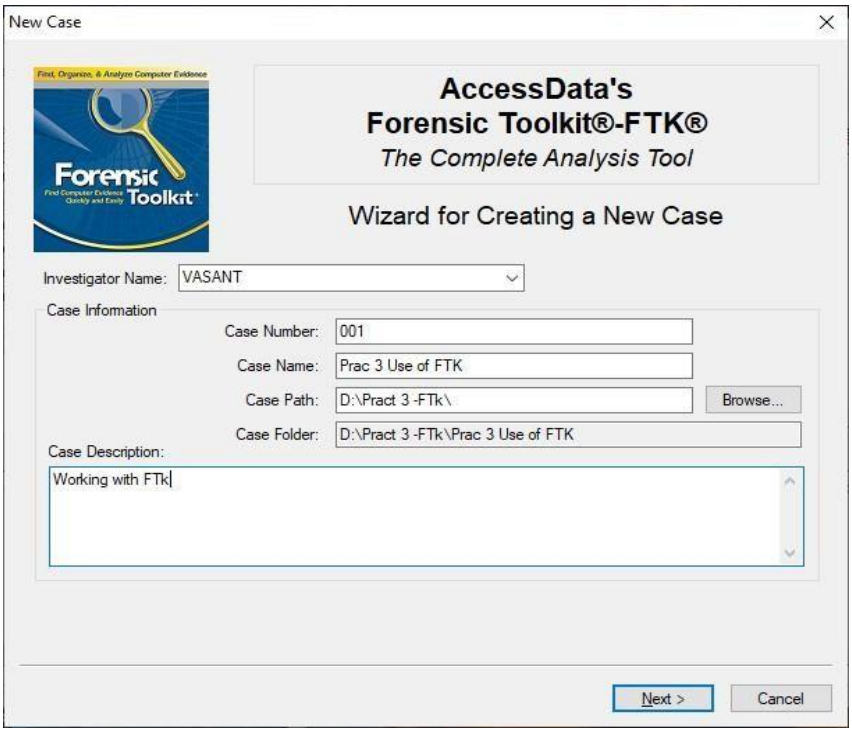
I. Starting a new case

1. Start FTK setup, select start a new case, select on OK.



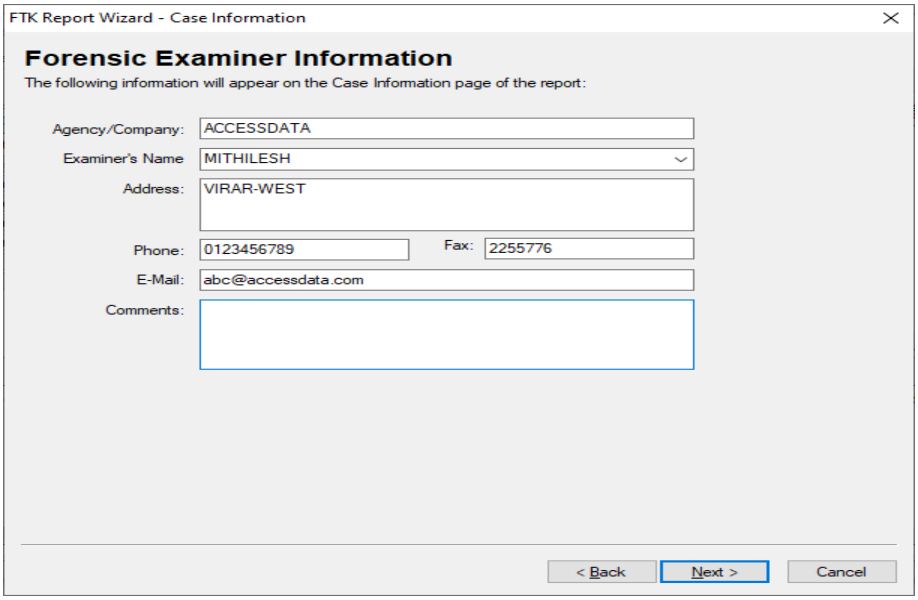
II. Completing the New Case

In New Case form, provide Investigator's name, Case Number, Case Name, Case Path and case description. Case folder field is filled by default based on case name and case path fields. Click Next.



III. Entering Forensic Examiner information

1. In Case Information Form, provide forensic examiner information.
2. Enter Company, Examiner's Name, Address, Phone, Fax, Email and Comments.

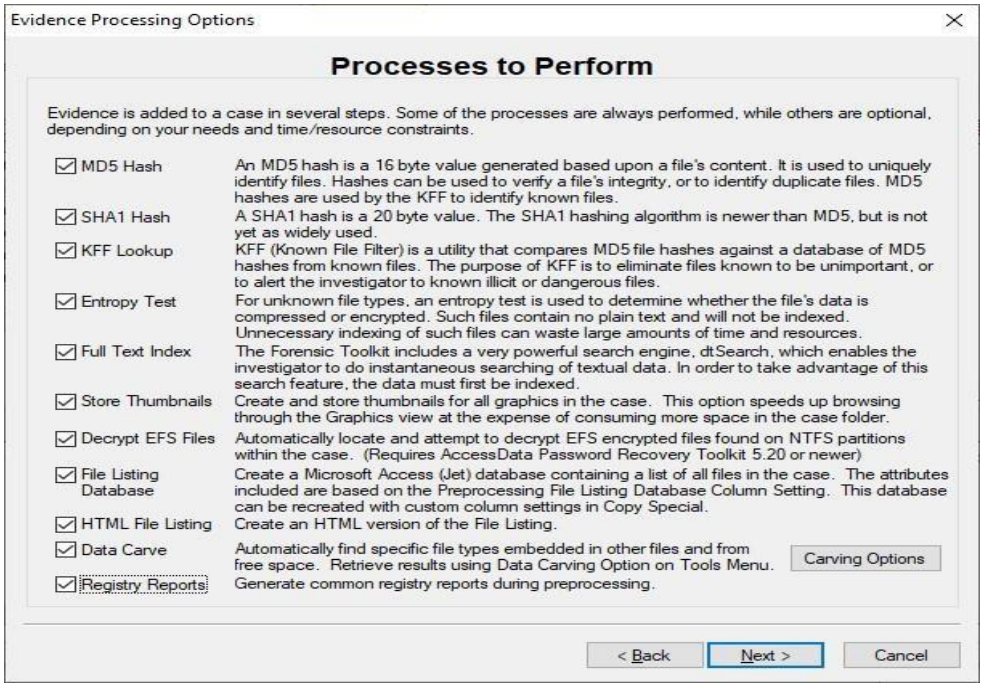


IV. Selecting Case Log Options

1. In the Case Log Options form, select what you want to include in the case log and click Next.

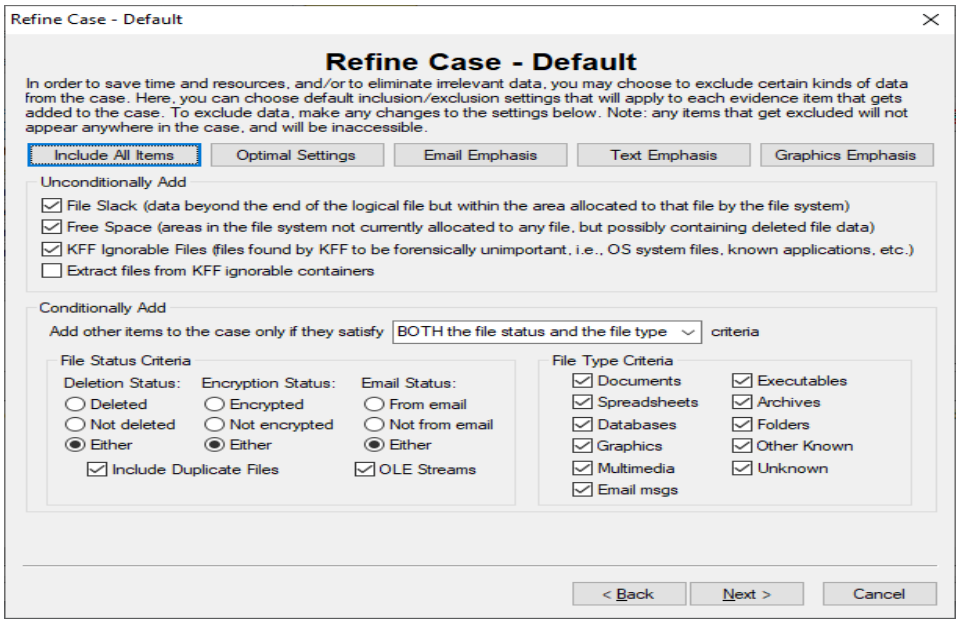
V. Selecting Evidence Processes

1. In the Evidence Processing Options form, select the processes that you want to be run on the evidence and click Next.



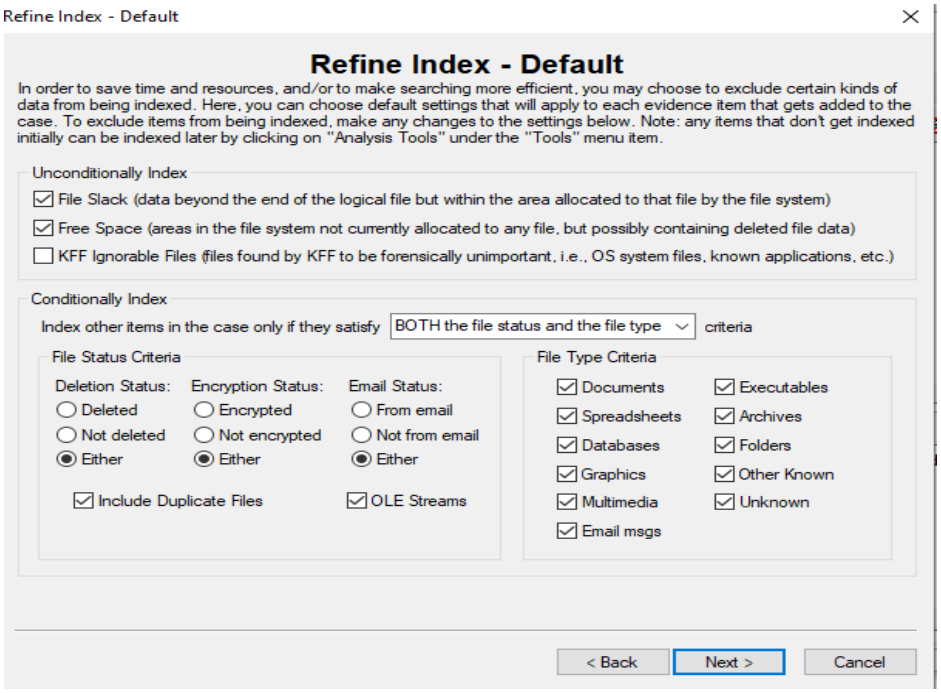
VI. Refining the Case

1. In the Refine Case form, select the default template you want to use and click 999Next.



VII. Refining the Index

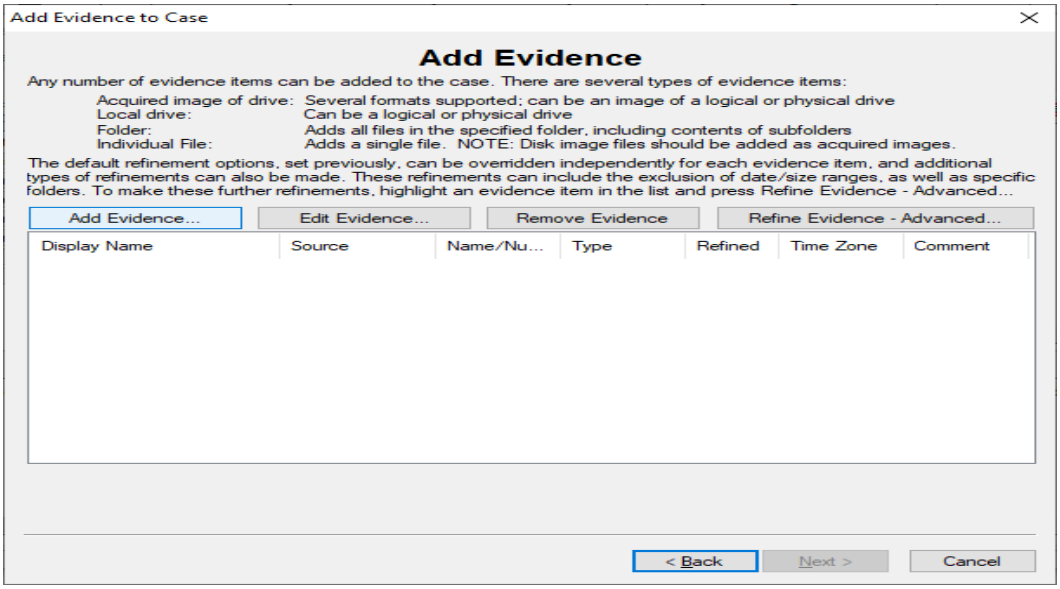
1. The Refine Index form has predefined settings and Click Next.



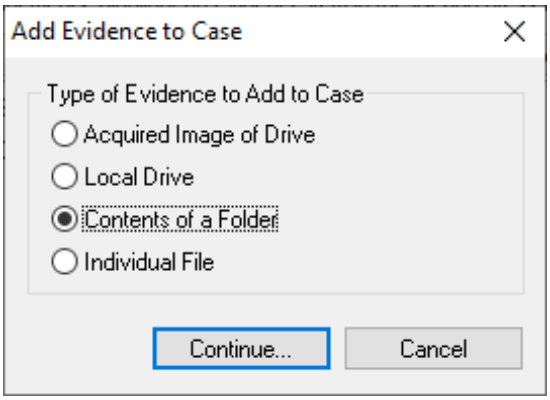
VIII. Managing Evidence

a. Adding Evidence

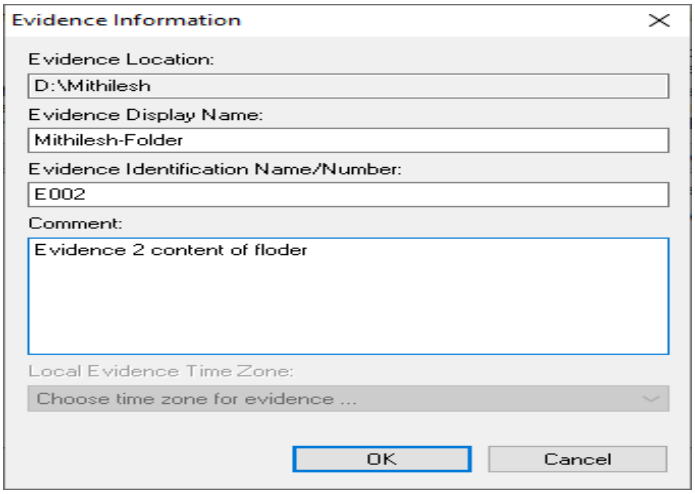
1. To add evidence to the case, In the Add Evidence Case form Click **Add Evidence**

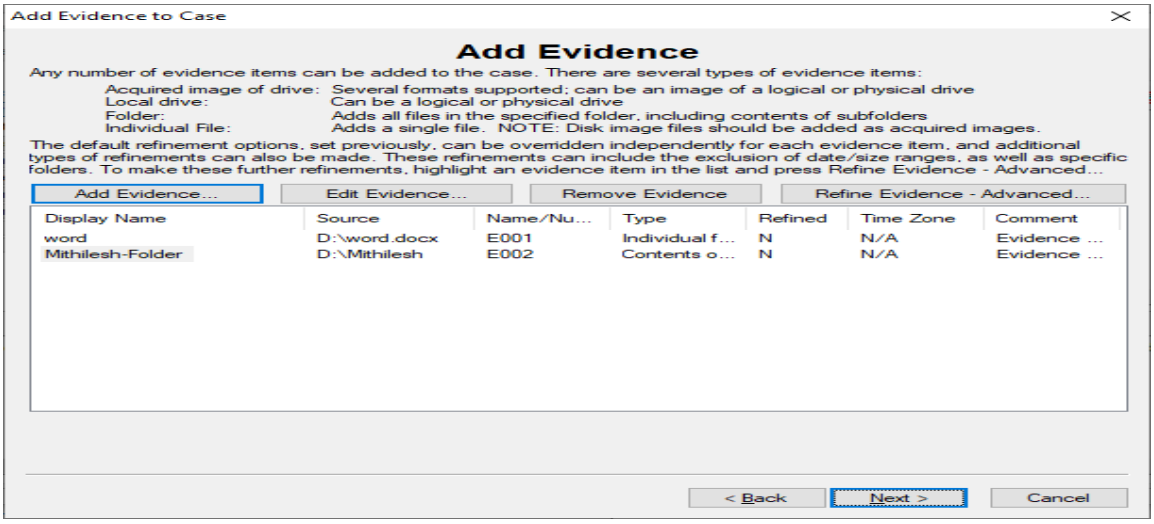


2. Then select the type of evidence and click **Container**.



3. Browse to the location and select the evidence.
4. In the Evidence Information form, enter the evidence information and Click OK.





b. Editing Evidence

1. To modify the evidence information for a particular item, select an evidence item in the File List.
2. Click **Edit Evidence.**
3. Modify the information in the Evidence Information form.
4. Click OK.

c. Removing Evidence

1. You can remove an item from file List in the Add Evidence form only. You cannot remove an item from your case after it has been processed.

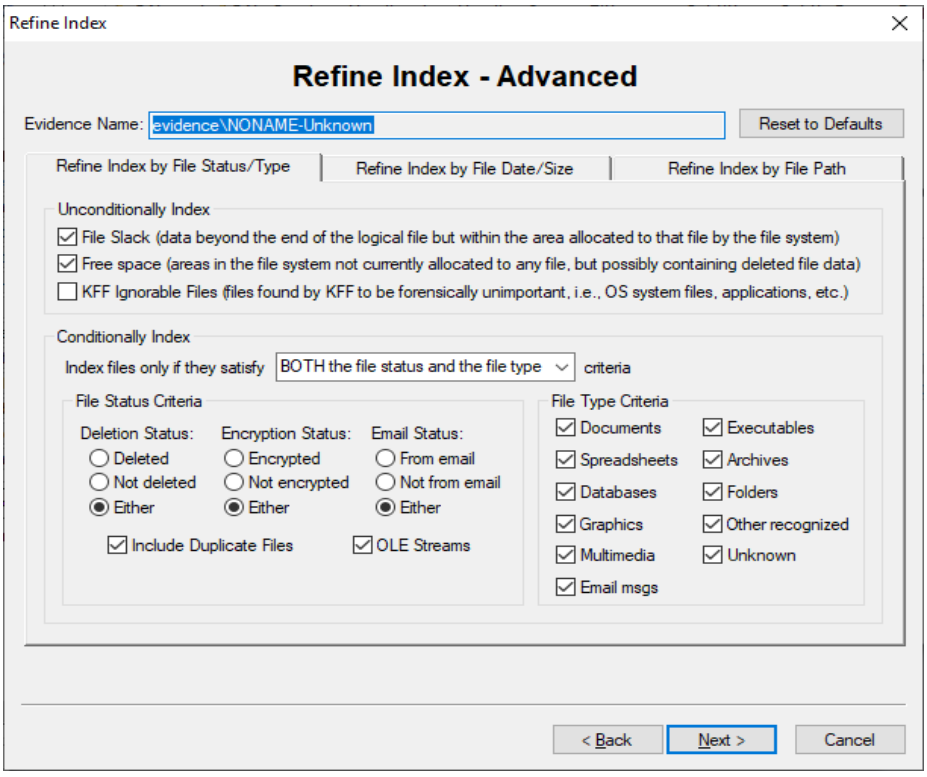
d. Refining Evidence

To Refine case evidence:

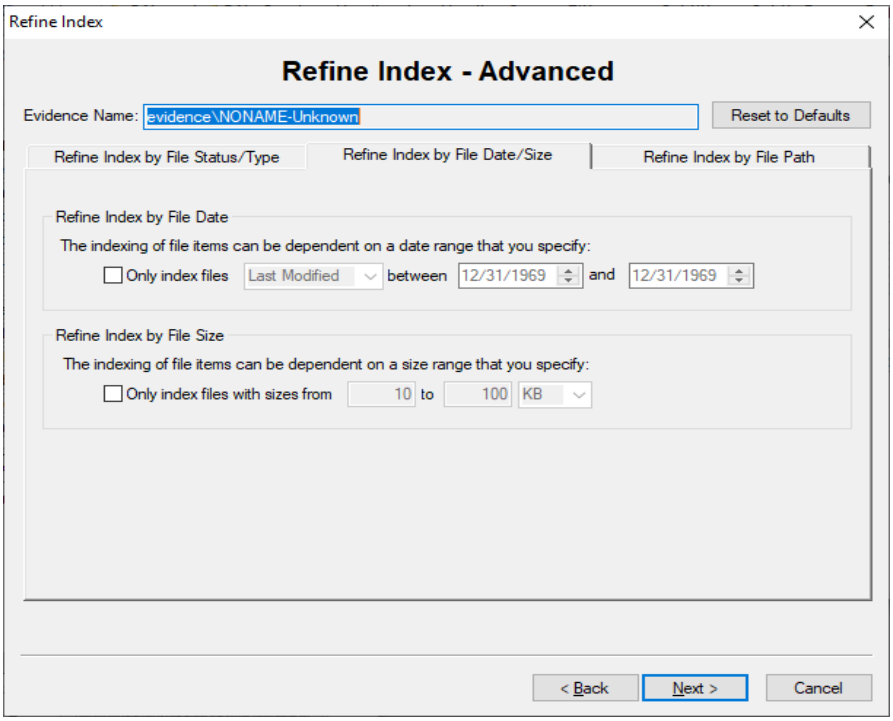
1. Select the evidence from the file List.
2. Click **Refine Evidence Advanced.**

The Refine case evidence Menu is organized into three windows

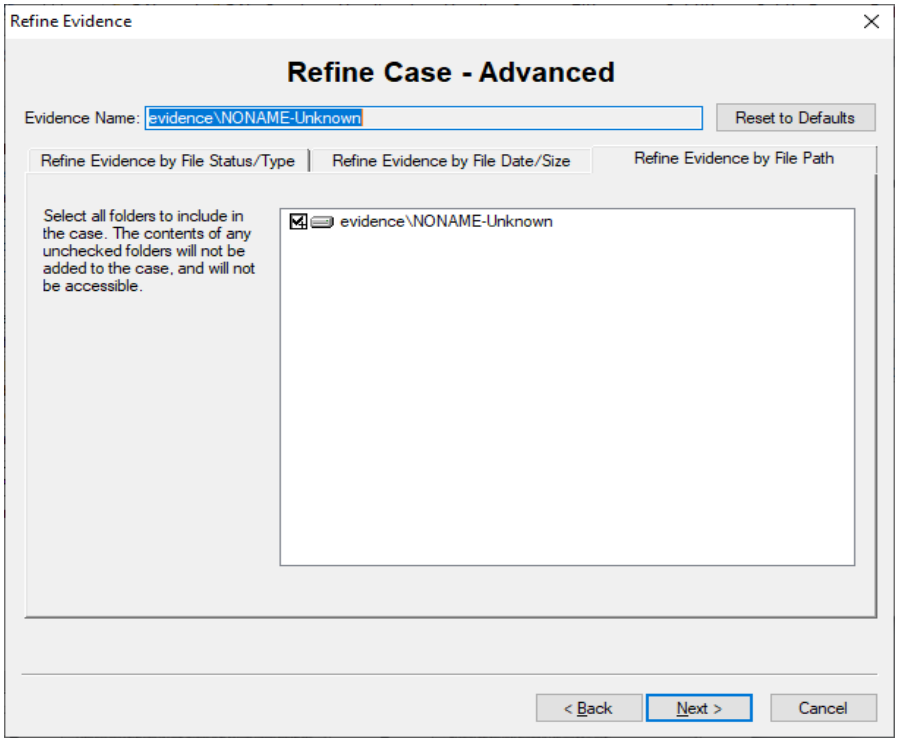
- Refine evidence by File Status type.



- Refine evidence by File Date/Size.

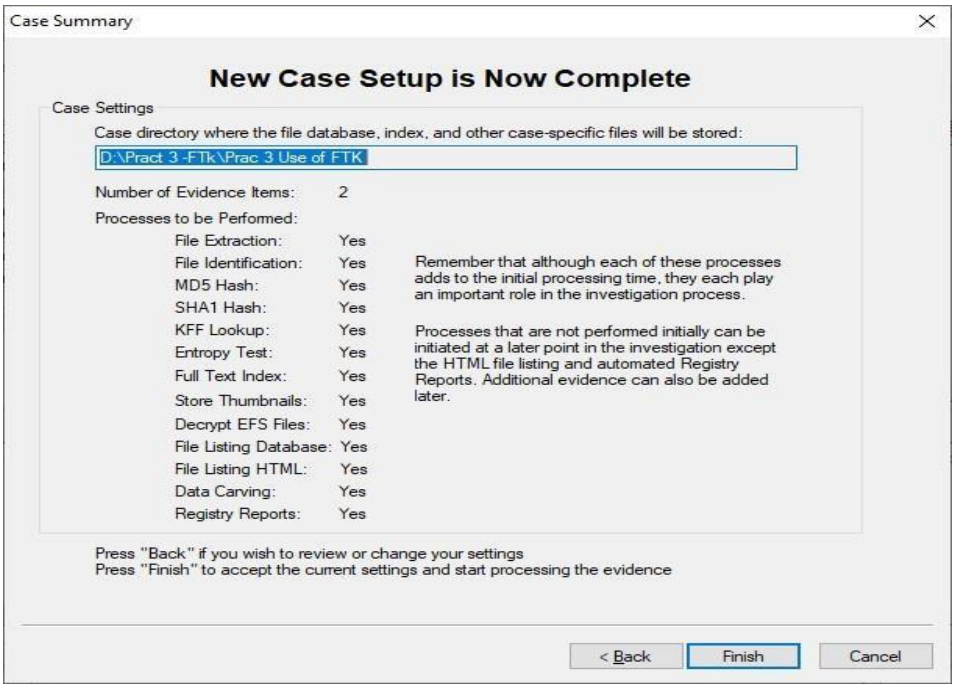


- Refine evidence by File Path.



IX. Reviewing case Summary

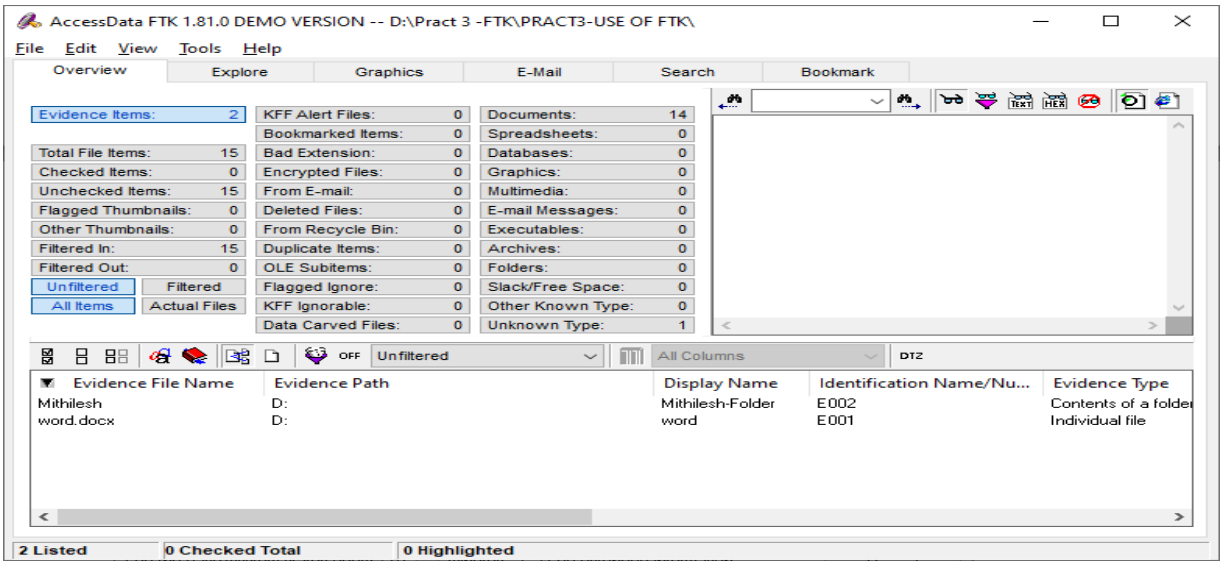
1. The Case summary form allows you to review the evidence summary.
2. Click Finish.



X. Processing the Evidence

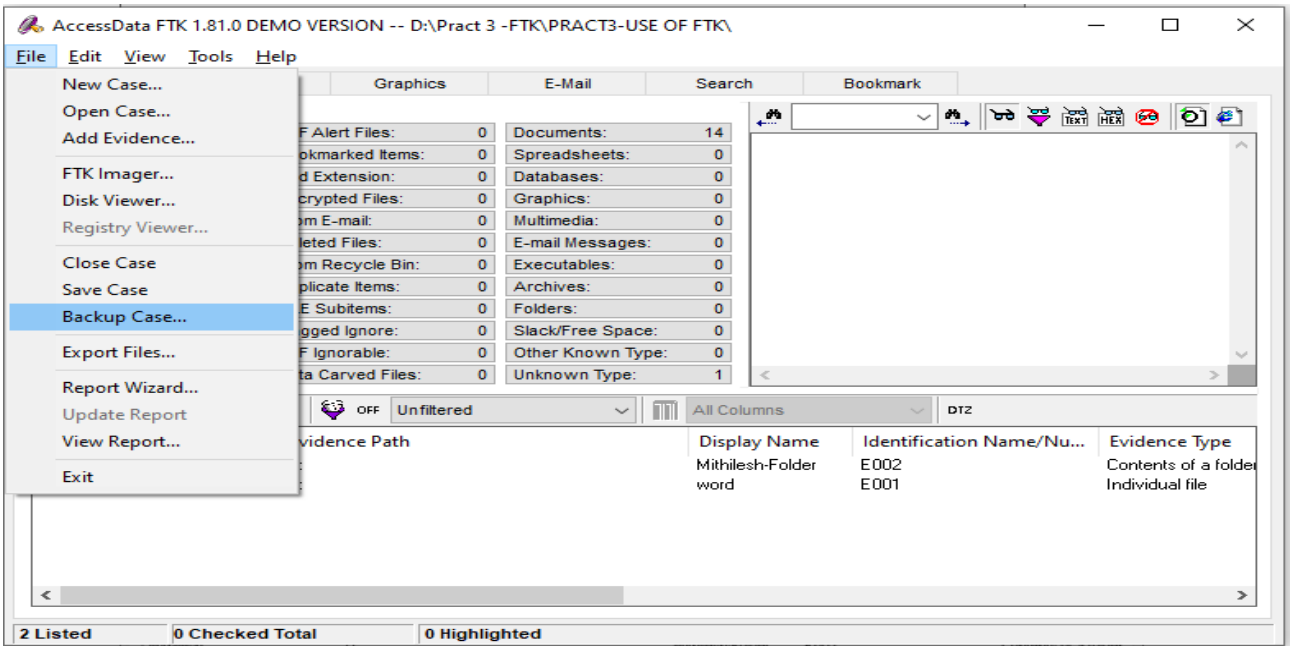
1. After you click Finish, the processing files form appears and displays the status of the processed you selected in the wizard.

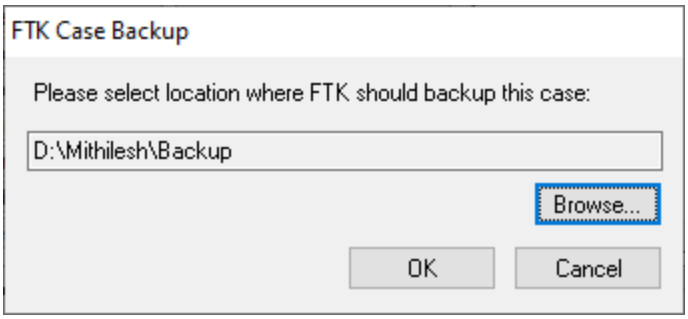
After processing the evidence aggregator

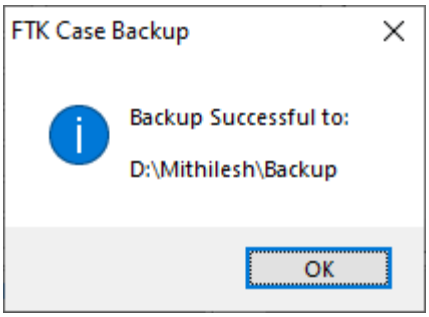


XI. Backing up the case

1. To back up the case manually, click file and then Backup Case and then select at empty direction when you want the backup to be created.





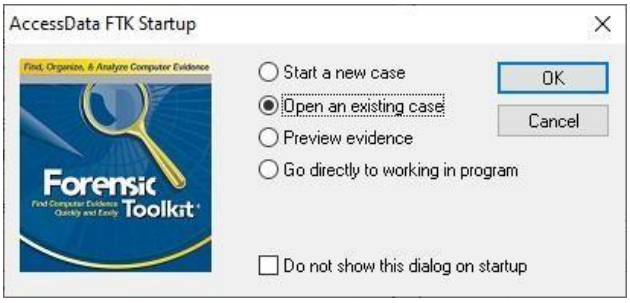


B. Working with existing Cases

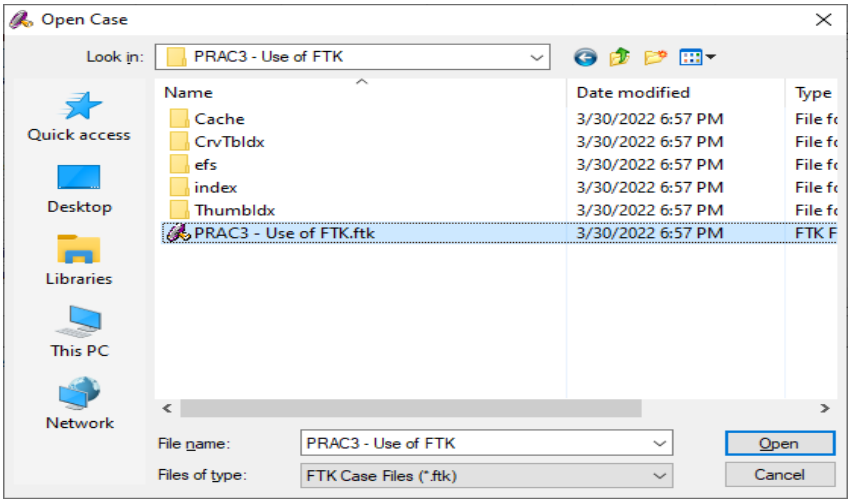
I. Opening an Existing Case

To open an existing case from FTK

1. In Forensic Toolkit (FTK), select Open an Existing Case and Click OK.

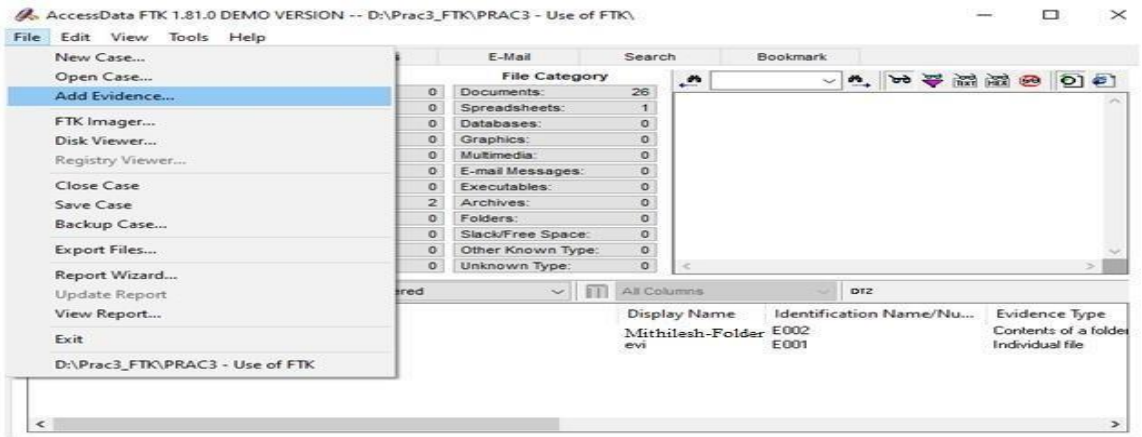


2. Select the case you want to open.



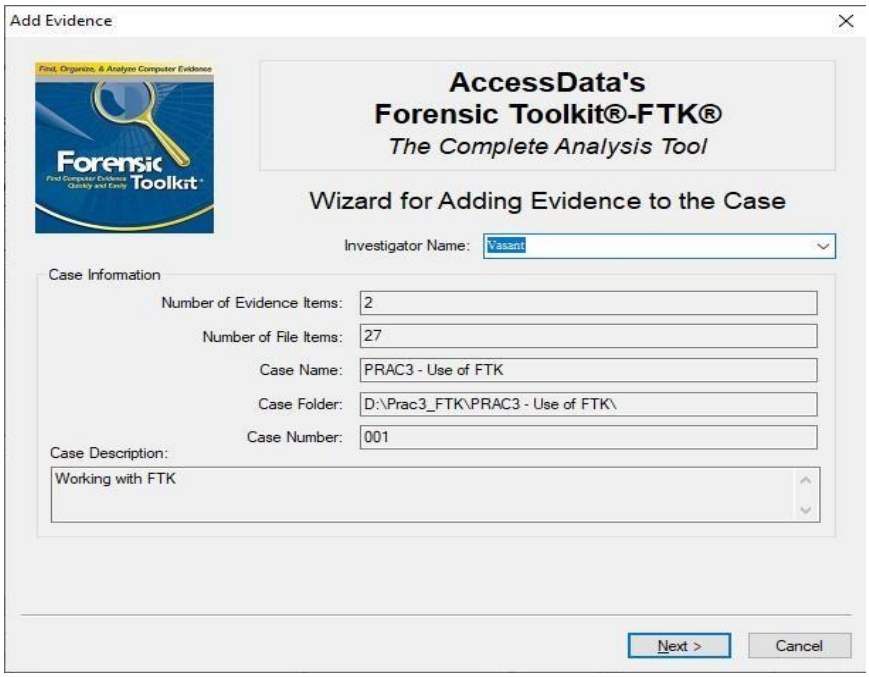
II. Adding evidence

1. Click File, and then Add evidence. Then Add Evidence Wizard opens.



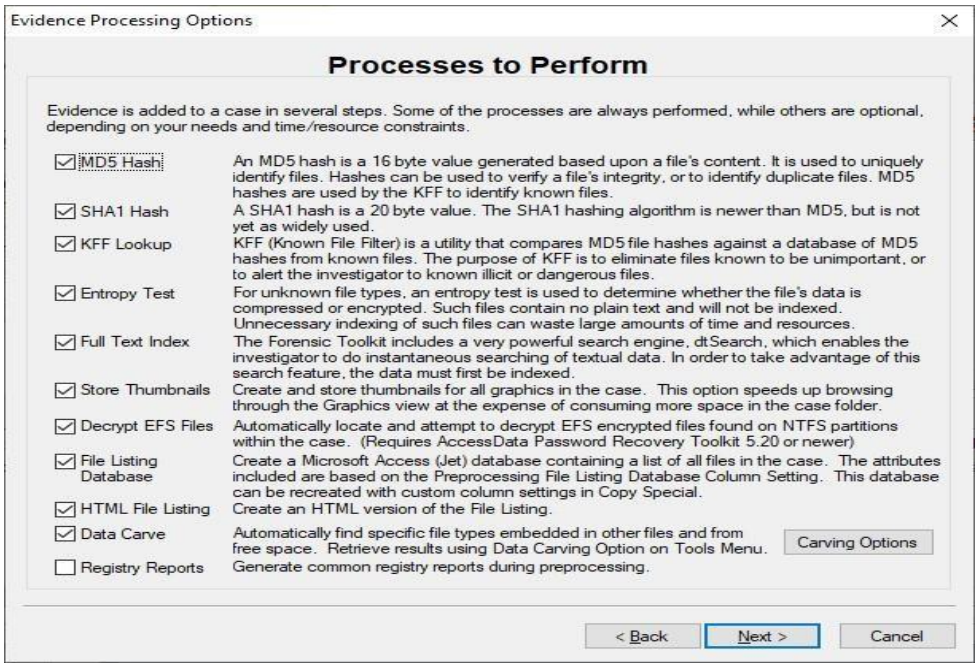
a. Completing the Add Evidence Form

1. Enter Investigator's name and click Next.



b. Selecting Evidence Processes

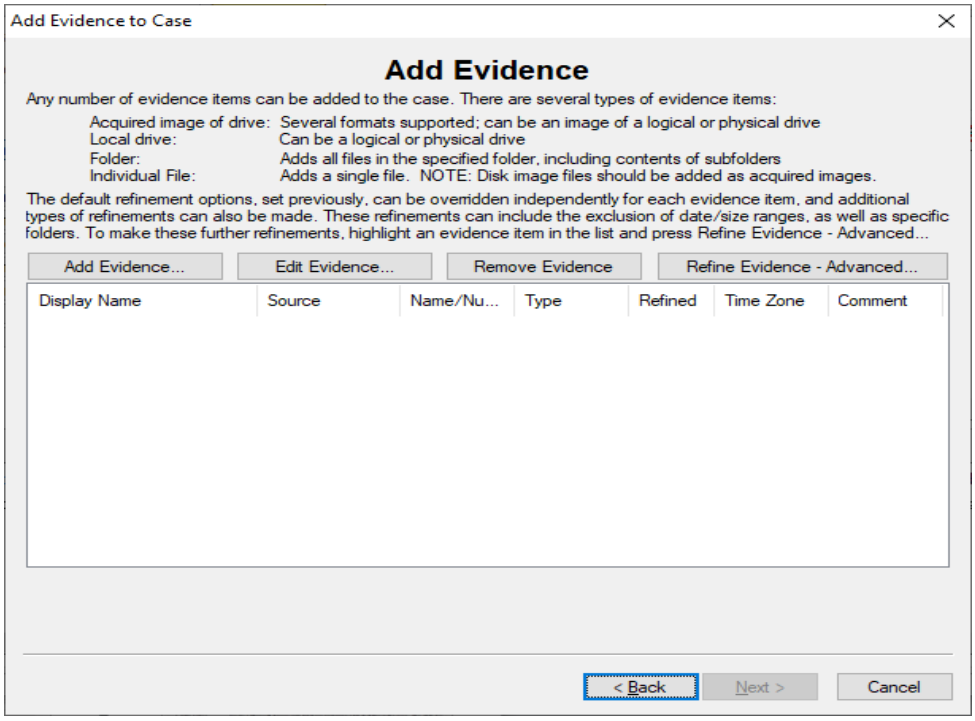
1. In the Evidence Processing Options form, select the processes that you want to be run on the evidence and click next.



c. Managing Evidence

1. Adding Evidence

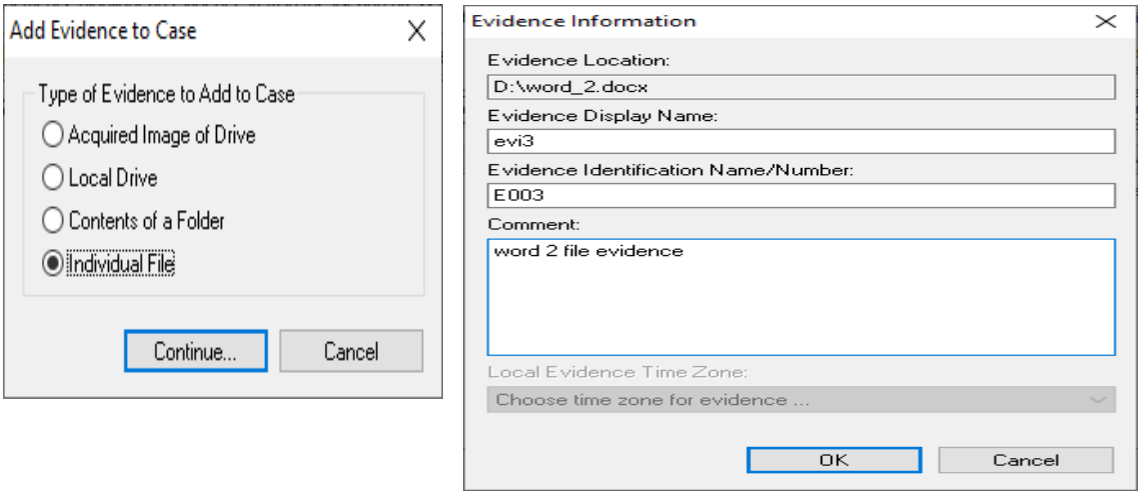
i. To add evidence to the case, in the Add Evidence Case form, click Add Evidence.

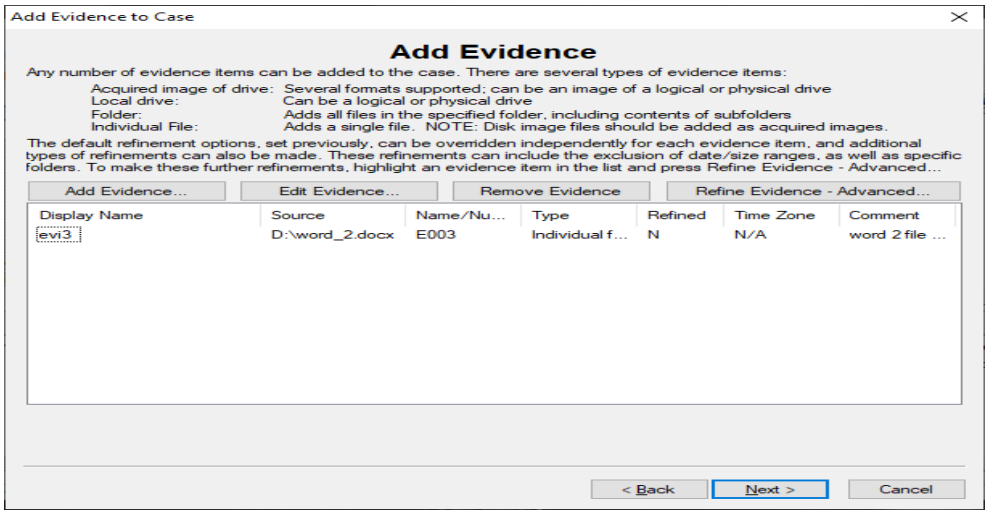


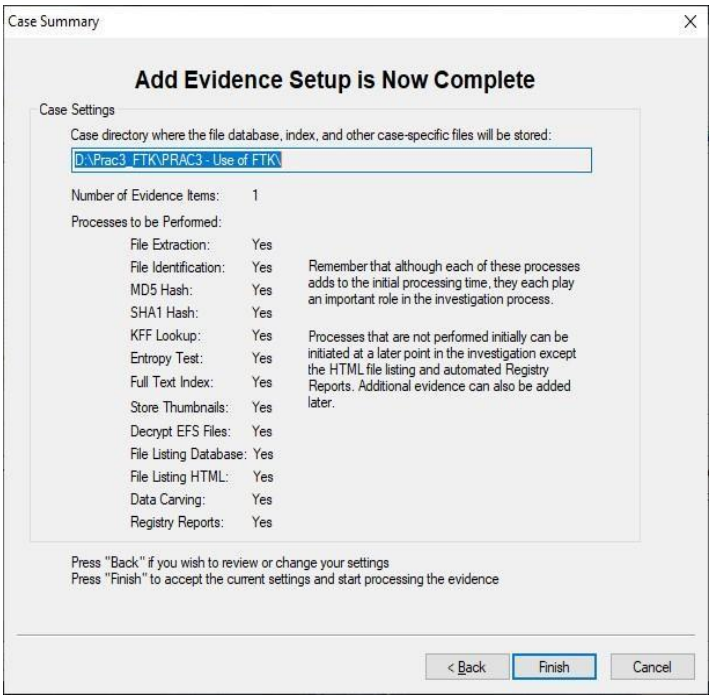
ii. Then select the type of evidence and click Continue.

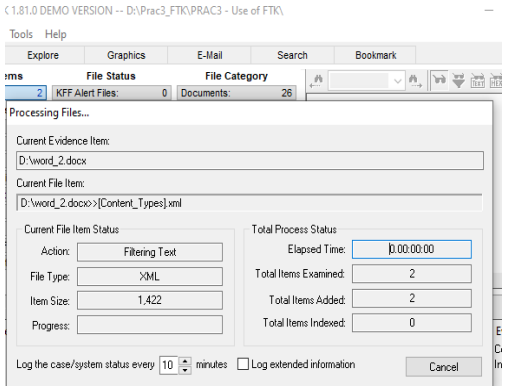
iii. Browse to the select the evidence.

iv. In the Evidence Information form, enter the evidence information and click OK.









2. Editing Evidence

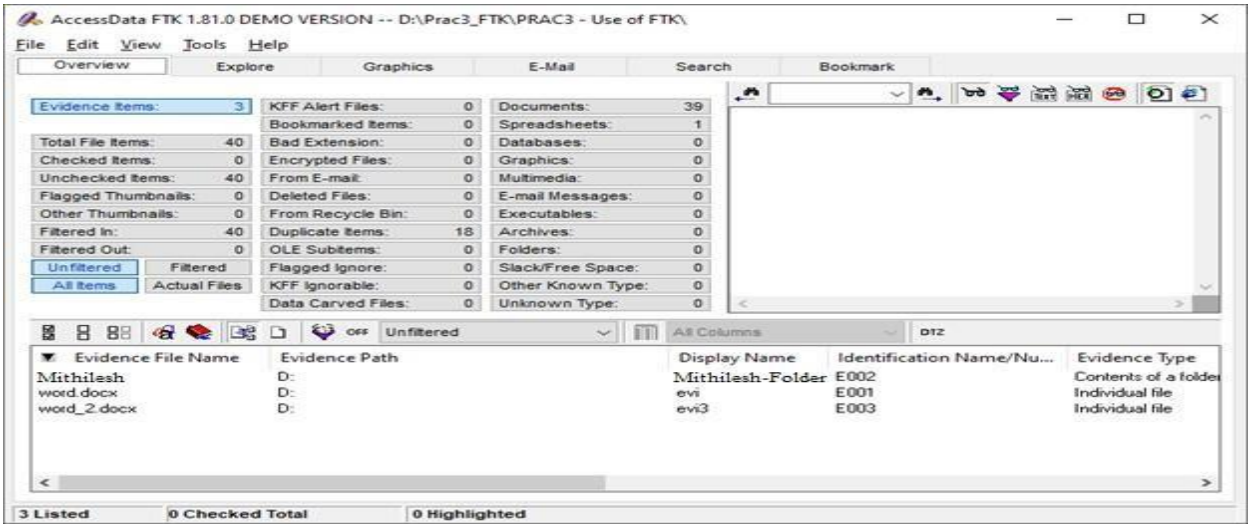
1. To modify the evidence information for a particular item, select an evidence item in the File List.
2. Click **Edit Evidence.**
3. Modify the information in the Evidence Information form.
4. Click OK.

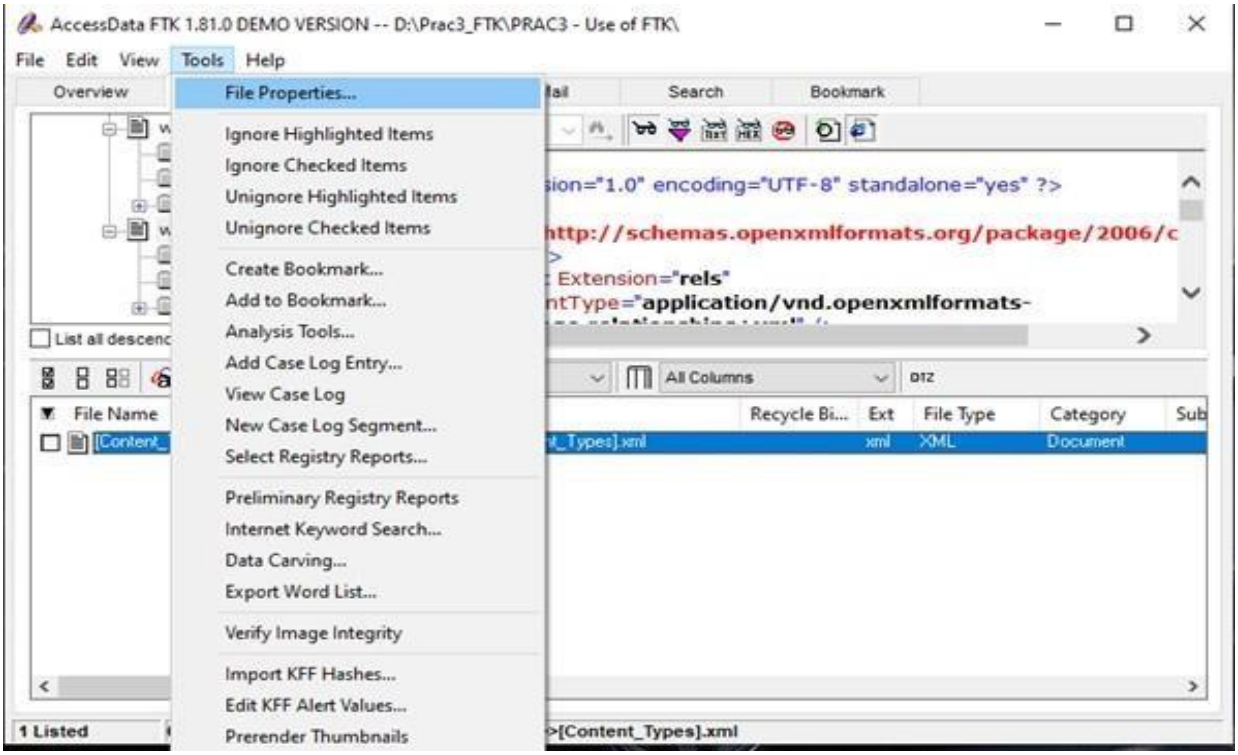
3. Removing Evidence

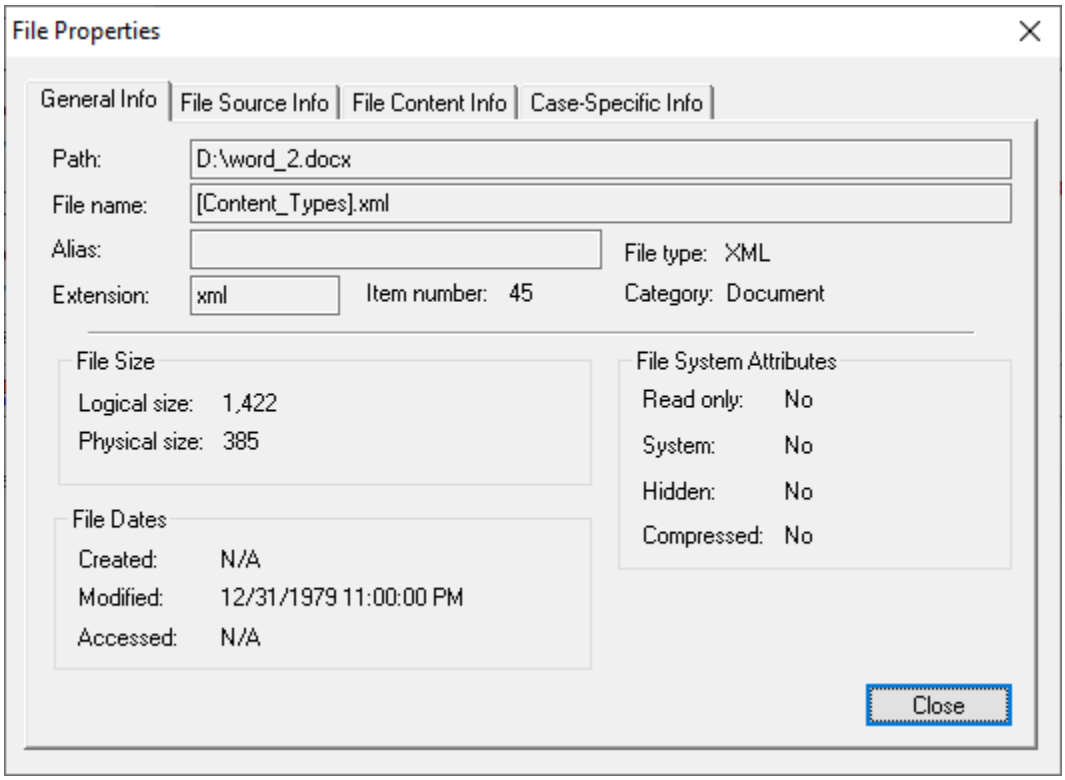
2. You can remove an item from file List in the Add Evidence form only. You cannot remove an item from your case after it has been processed.

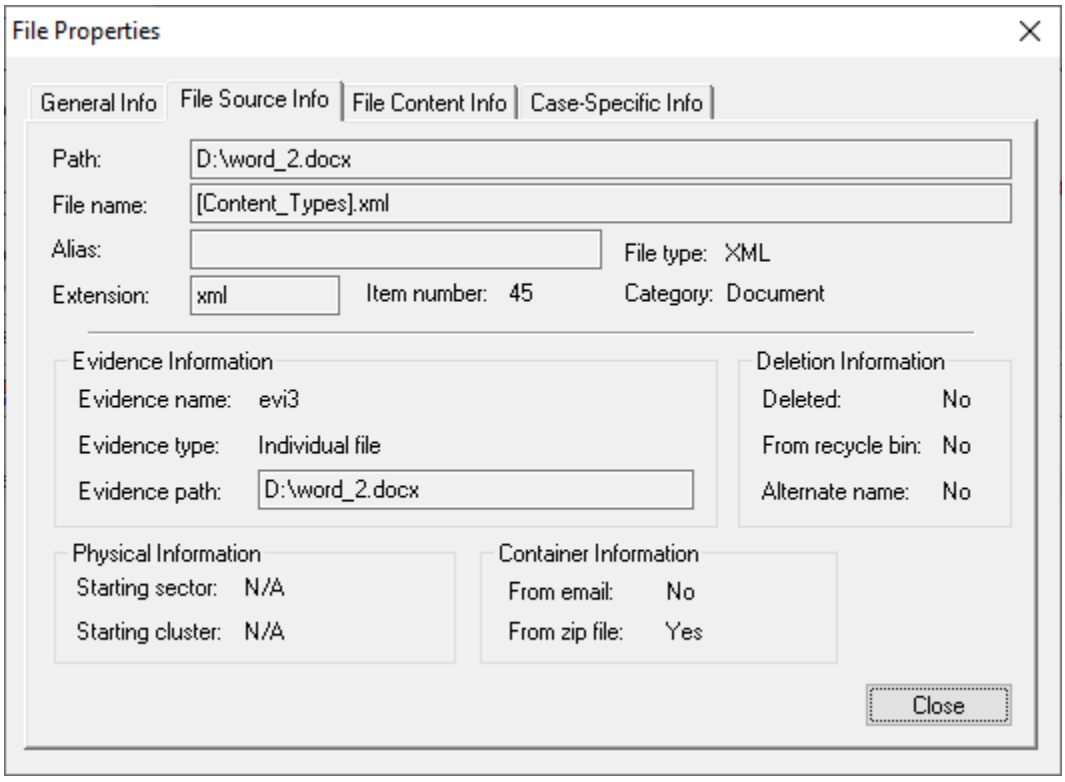
4. Refining Evidence

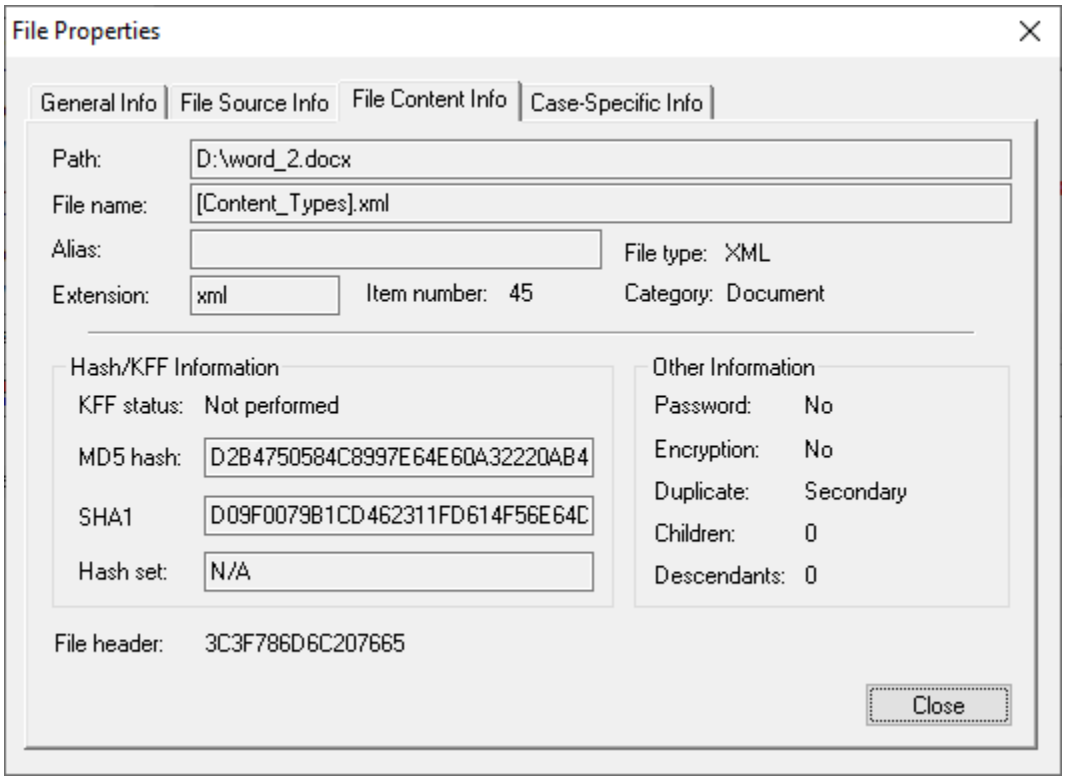
To Refine case evidence: Select the evidence from the file List

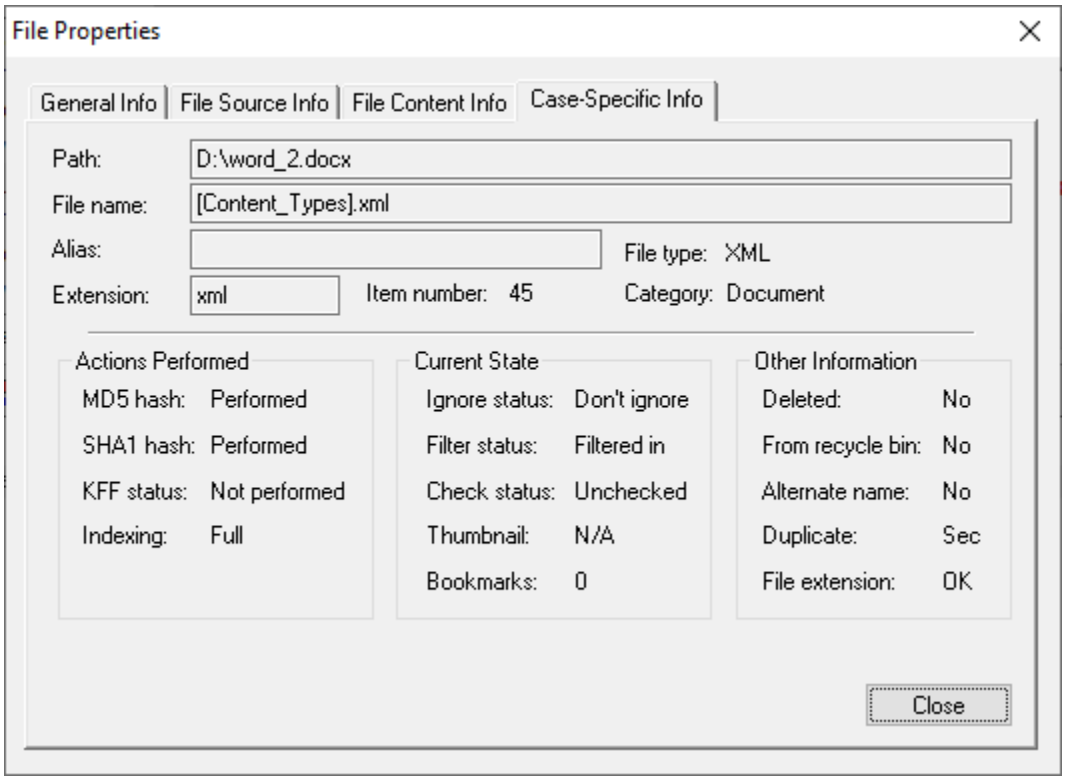


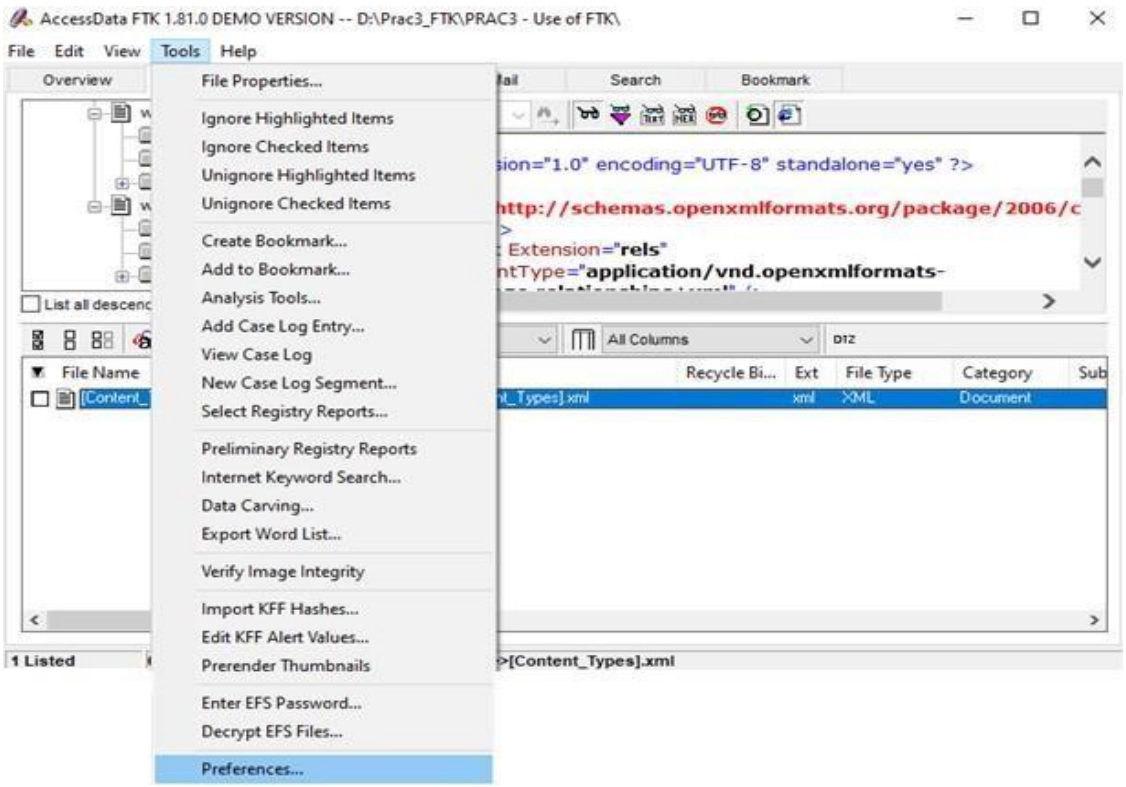


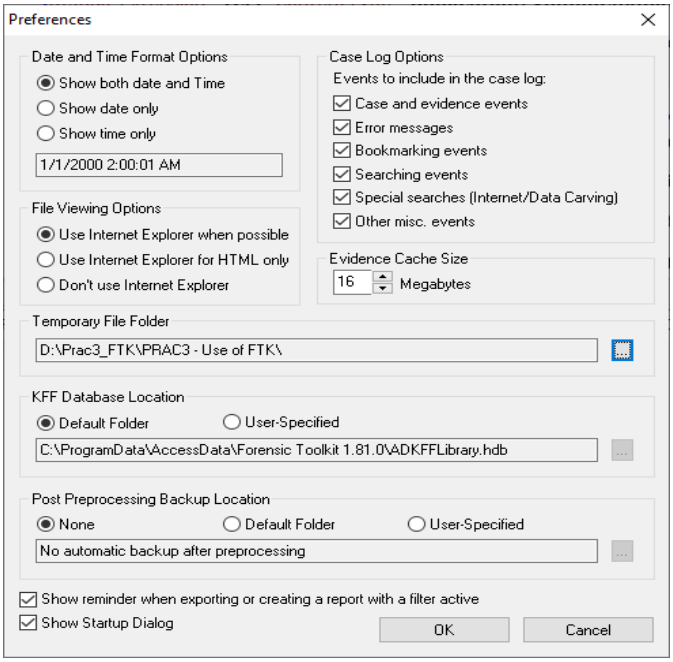

File Properties
General Info
File Source Info
File Content Info
Case-Specific Info
Path: D:\word_2.docx
File name: [Content_Types].xml
Alias:
File type: XML
Extension: xml
Item number: 45
Category: Document
File Size
Logical size: 1,422
Physical size: 385
File System Attributes
Read only: No
System: No
Hidden: No
Compressed: No
File Dates
Created: N/A
Modified: 12/31/1979 11:00:00 PM
Accessed: N/A
Close

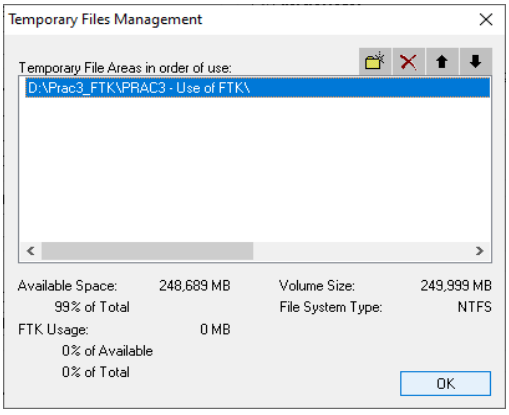

File Properties
General Info
File Source Info
File Content Info
Case-Specific Info
Path: D:\word_2.docx
File name: [Content_Types].xml
Alias:
File type: XML
Extension: xml
Item number: 45
Category: Document
Evidence Information
Evidence name: evi3
Evidence type: Individual file
Evidence path: D:\word_2.docx
Deletion Information
Deleted: No
From recycle bin: No
Alternate name: No
Physical Information
Starting sector: N/A
Starting cluster: N/A
Container Information
From email: No
From zip file: Yes
Close


File Properties
General Info
File Source Info
File Content Info
Case-Specific Info
Path: D:\word_2.docx
File name: [Content_Types].xml
Alias:
File type: XML
Extension: xml
Item number: 45
Category: Document
Hash/KFF Information
KFF status: Not performed
MD5 hash: D2B4750584C8997E64E60A32220AB4
SHA1 D09F0079B1CD462311FD614F56E64C
Hash set: N/A
Other Information
Password: No
Encryption: No
Duplicate: Secondary
Children: 0
Descendants: 0
File header: 3C3F786D6C207665
Close


File Properties
General Info
File Source Info
File Content Info
Case-Specific Info
Path: D:\word_2.docx
File name: [Content_Types].xml
Alias:
File type: XML
Extension: xml
Item number: 45
Category: Document
Actions Performed
MD5 hash: Performed
SHA1 hash: Performed
KFF status: Not performed
Indexing: Full
Current State
Ignore status: Don't ignore
Filter status: Filtered in
Check status: Unchecked
Thumbnail: N/A
Bookmarks: 0
Other Information
Deleted: No
From recycle bin: No
Alternate name: No
Duplicate: Sec
File extension: OK
Close


AccessData FTK 1.81.0 DEMO VERSION -- D:\Prac3_FTK\PRAC3 - Use of FTK\
File Edit View Tools Help
Overview
File Properties...
Ignore Highlighted Items
Ignore Checked Items
Unignore Highlighted Items
Unignore Checked Items
Create Bookmark...
Add to Bookmark...
Analysis Tools...
Add Case Log Entry...
View Case Log
New Case Log Segment...
Select Registry Reports...
Preliminary Registry Reports
Internet Keyword Search...
Data Carving...
Export Word List...
Verify Image Integrity
Import KFF Hashes...
Edit KFF Alert Values...
Prerender Thumbnails
Enter EFS Password...
Decrypt EFS Files...
Preferences...
Search
Bookmark
File Name
Recycle Bi...
Ext
File Type
Category
1 Listed


Preferences
Date and Time Format Options
Show both date and Time
Show date only
Show time only
1/1/2000 2:00:01 AM
File Viewing Options
Use Internet Explorer when possible
Use Internet Explorer for HTML only
Don't use Internet Explorer
Case Log Options
Events to include in the case log:
Case and evidence events
Error messages
Bookmarking events
Searching events
Special searches (Internet/Data Carving)
Other misc. events
Evidence Cache Size
16
Megabytes
Temporary File Folder
D:\Prac3_FTK\PRAC3 - Use of FTK\
KFF Database Location
Default Folder
User-Specified
C:\ProgramData\AccessData\Forensic Toolkit 1.81.0\ADKFFLibrary.hdb
Post Preprocessing Backup Location
None
Default Folder
User-Specified
No automatic backup after preprocessing
Show reminder when exporting or creating a report with a filter active
Show Startup Dialog
OK
Cancel


Temporary Files Management
Temporary File Areas in order of use:
D:\Prac3_FTK\PRAC3 - Use of FTK\
Available Space:
248,689 MB
99% of Total
Volume Size:
249,999 MB
File System Type:
NTFS
FTK Usage:
0 MB
0% of Available
0% of Total
OK

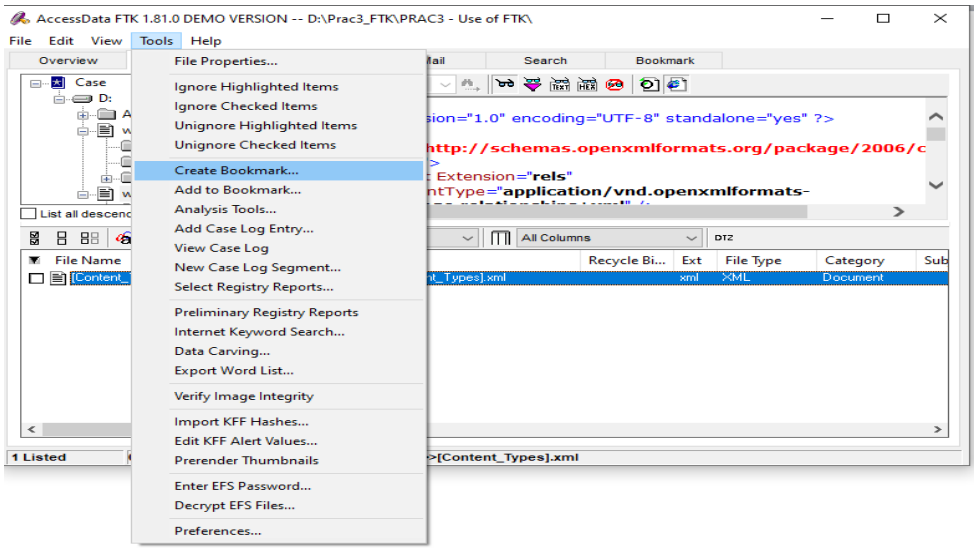
III. Processing Evidence

1. Using Bookmarks

a. Creating Bookmarks

To create a bookmark

i. Select Tools, and the Click on Create Bookmark. The create New Bookmark form appears.



ii. In the bookmark name field enter the name of the bookmark.

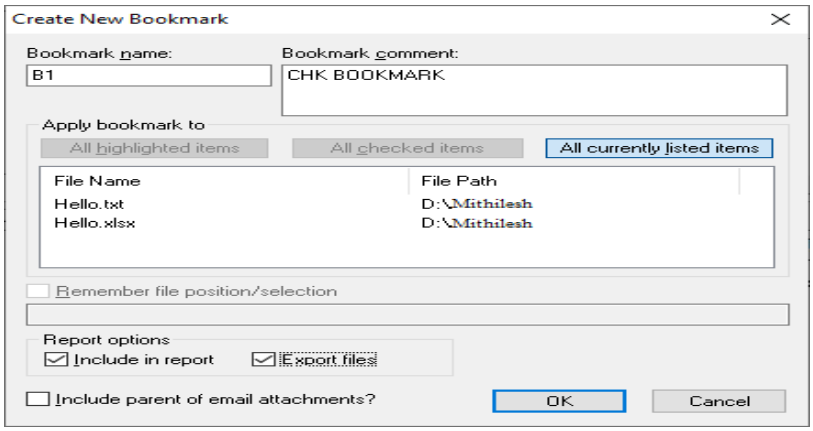
iii. In the bookmark comment field enter comments about the bookmark or it's contents.

iv. Select All checked items.

v. Click Include in Report to include the bookmark in the report.

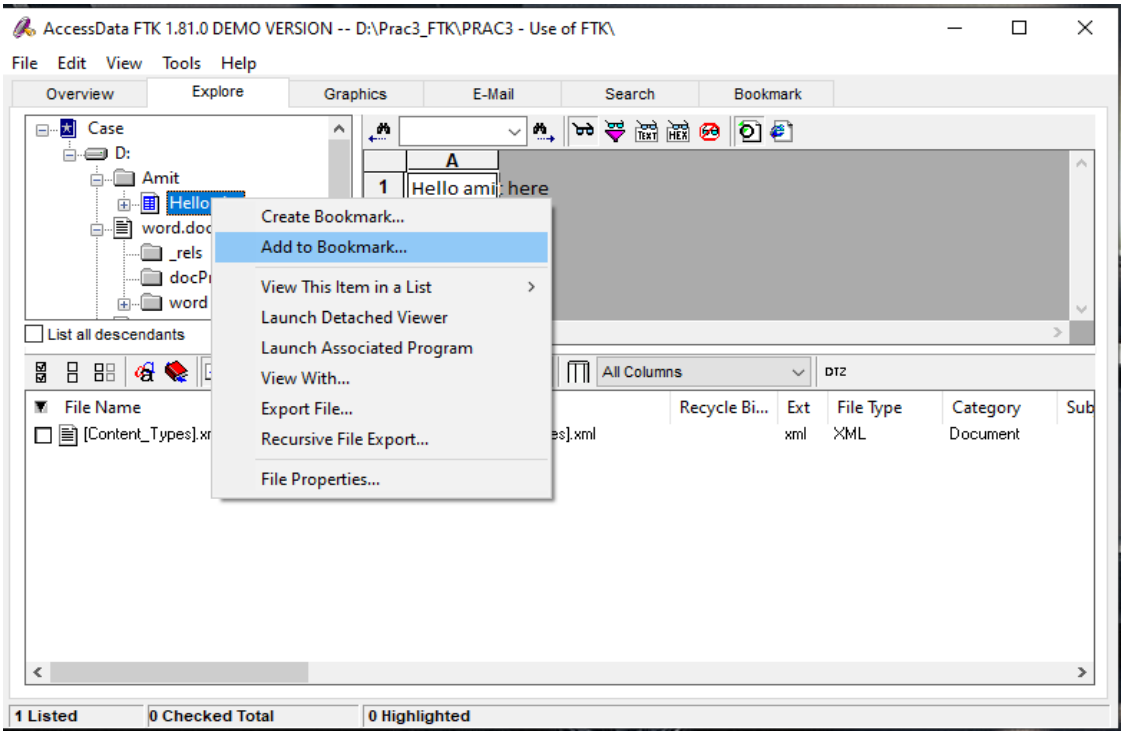
vi. If you choose to include the bookmark in the report, you can check Export to export the bookmark's files with the report.

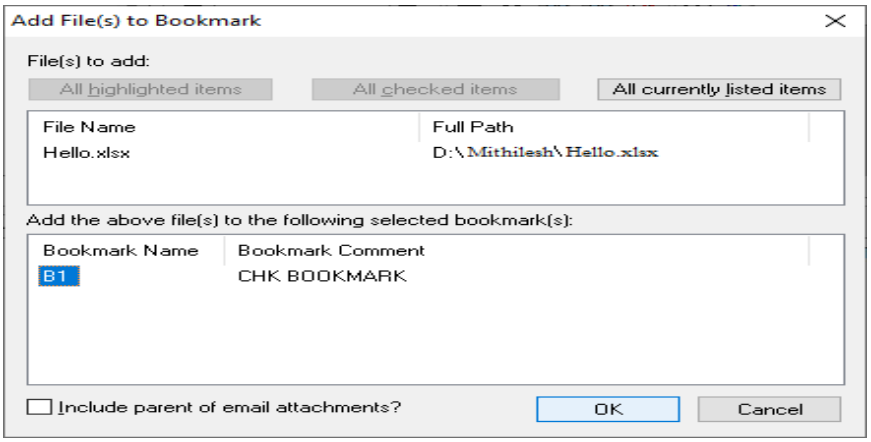
vii. Click OK.



b. Adding files in a bookmark

1. In a file list, highlight the file that you want to add to the bookmark.
2. Right-click and select. Add to Bookmark.
3. Click OK.



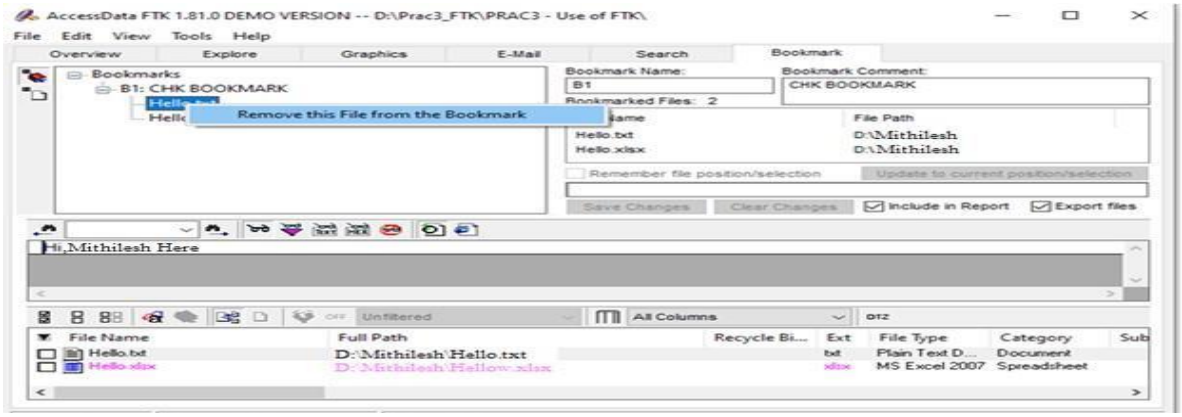


c. Removing a Bookmark

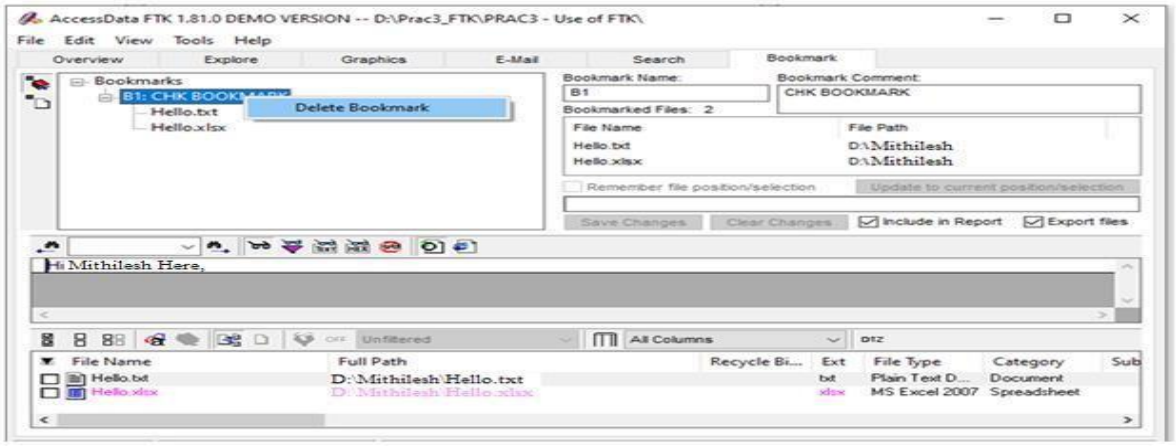
To remove a bookmark or individual file:

1. In the bookmark window, expand the bookmark list and highlight the bookmark or file that you want to remove.

2. To remove bookmark, right click and select Delete Bookmark.

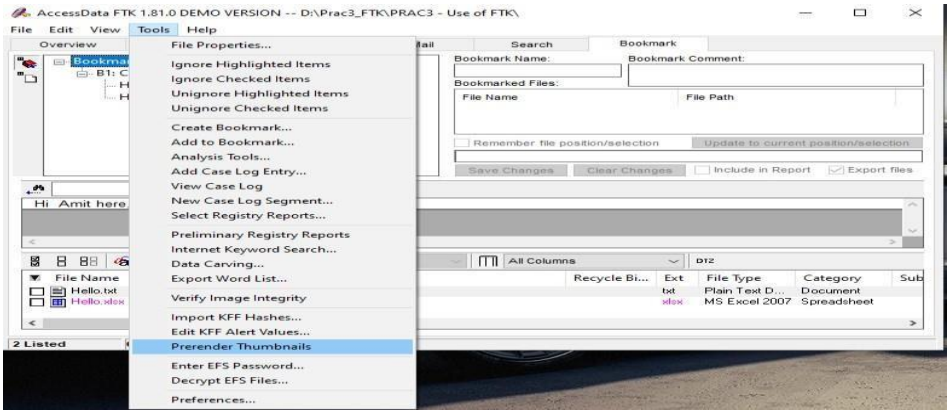


3. To remove a file, right-click and select Delete This File From the Bookmark.



Creating Thumbnails

1. To create Thumbnails after you have added the graphics to the case. Click Tools, and then Prerender Thumbnails.

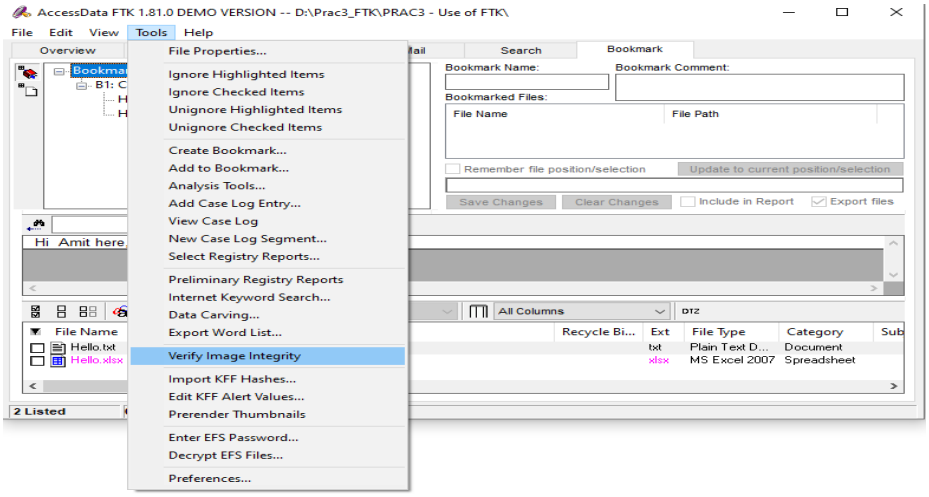


2. The Prerender Thumbnails Processing Files from lists each graphic as it is being processed and reflects the overall process status.

III. Verifying Image integrity

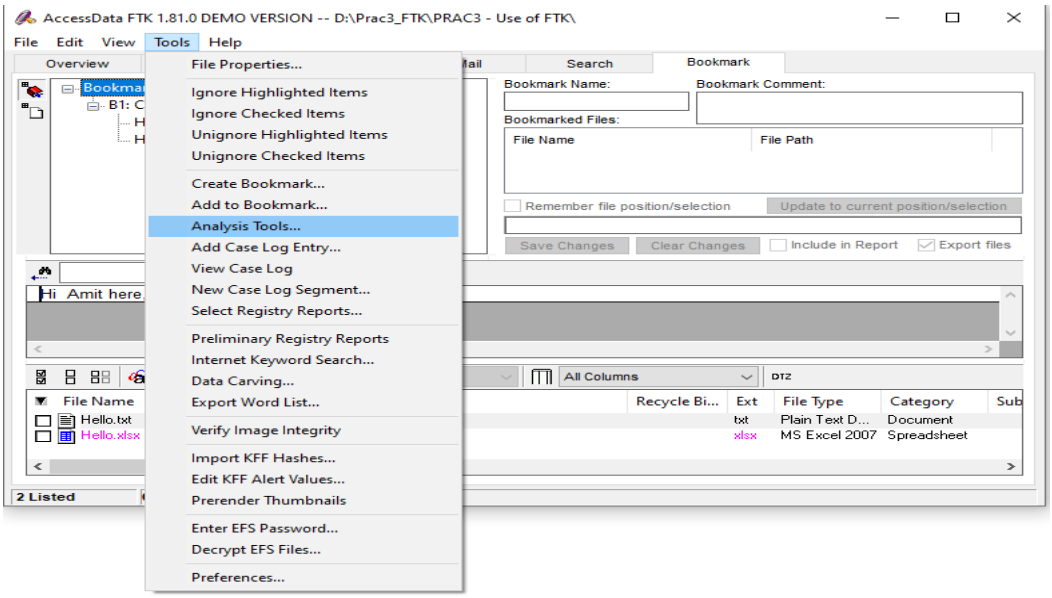
To verify that an image has not changed:

1. Select tools, and then Verify Image Integrity. The Verify Image Integrity Menu appears.
2. In the Evidence Filename column, select the image and click Verify.
3. Click Yes to Confirm.

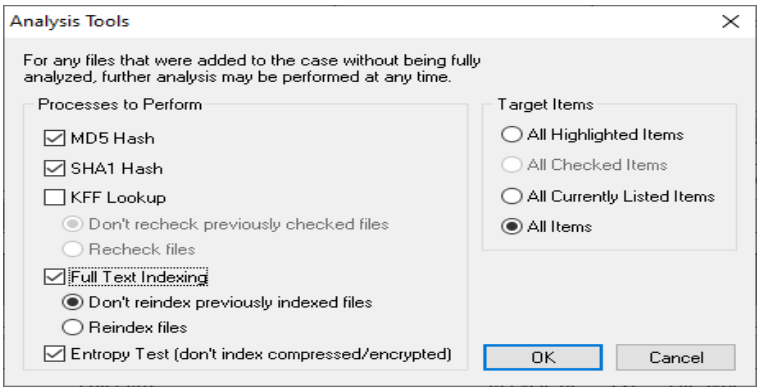


IV. Using Analysis Tools

1. Select Tools, and then Analysis Tools.



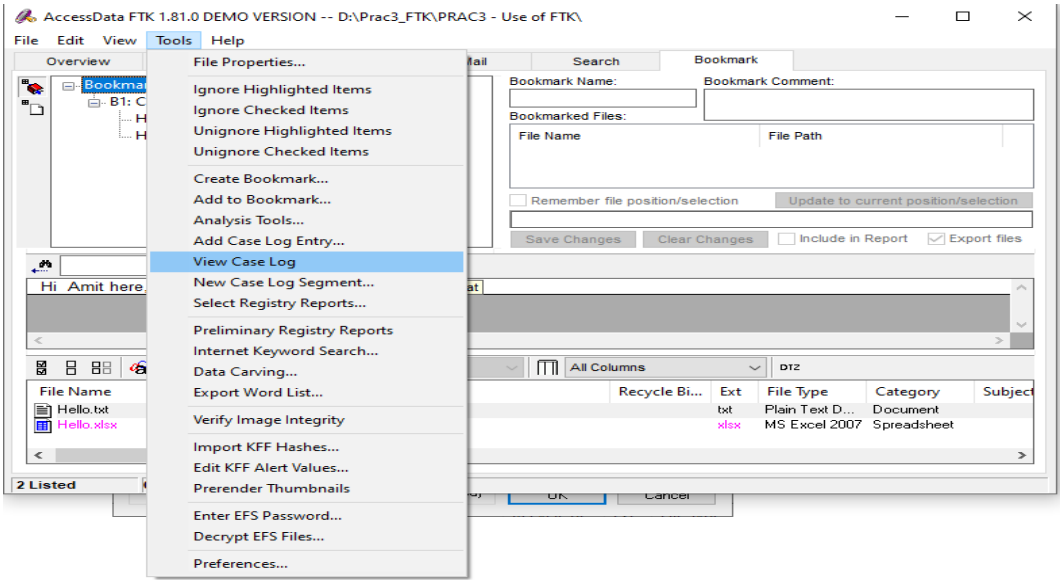
2. Click the processes you want to perform.
3. Select the files to process.
4. Click OK.

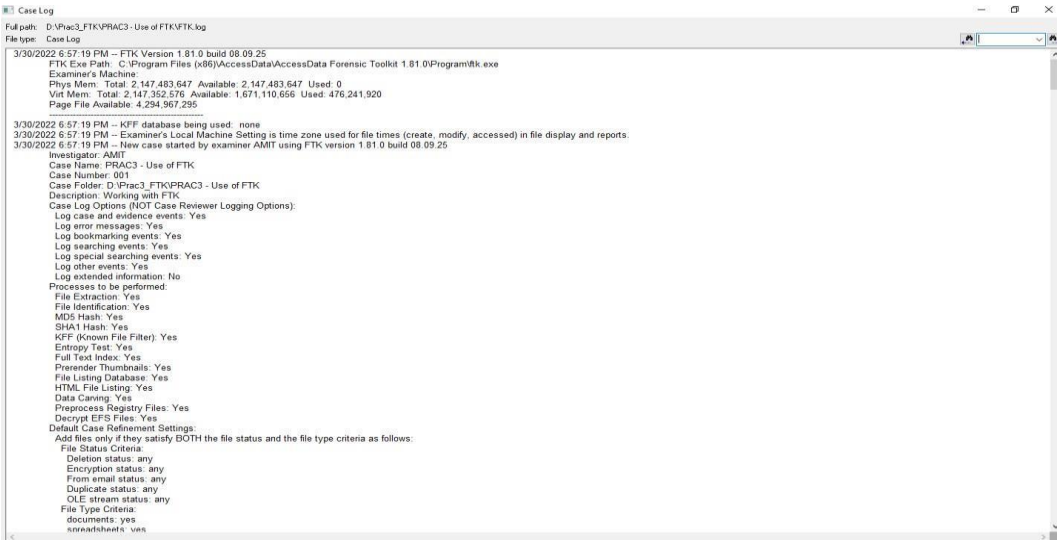


V. Using the Case Log

A. Viewing the Case Log

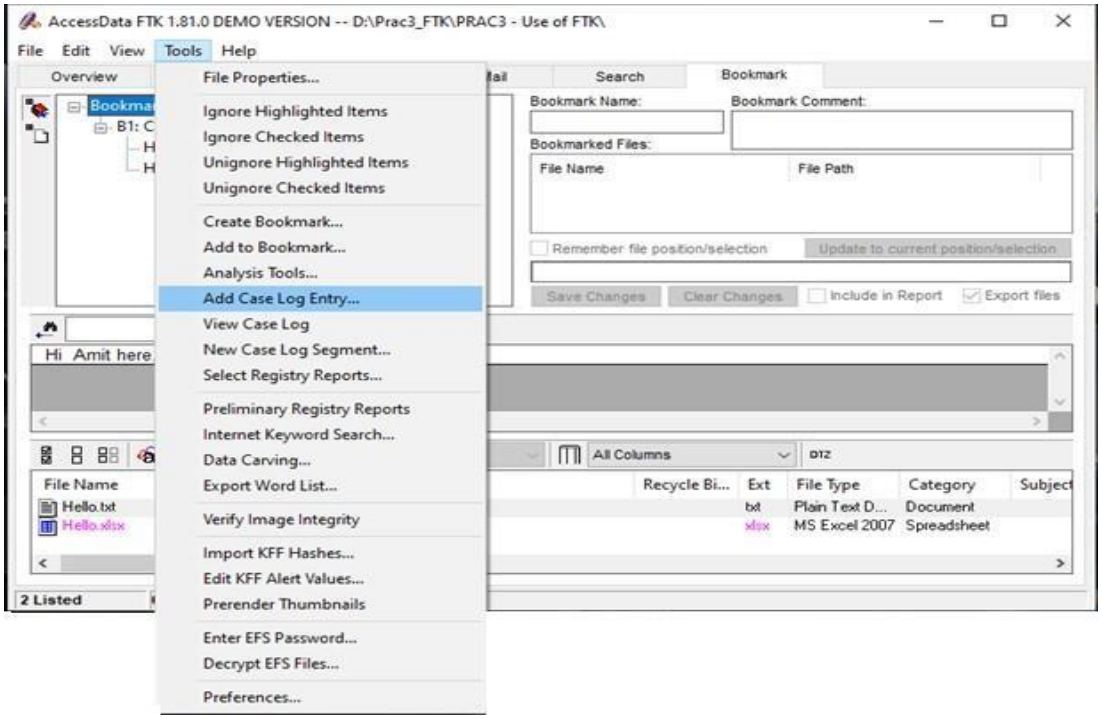
1. Select Tools, and then view Case Log.



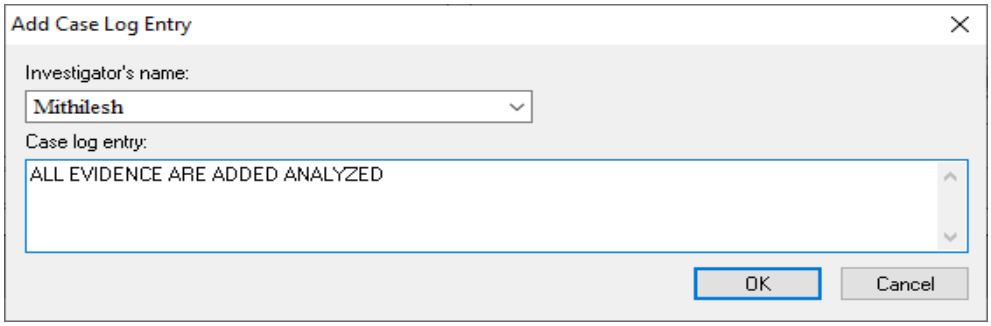


B. Adding Case Log entries

1. Select Tools, and the Click Add Case Log Entry.



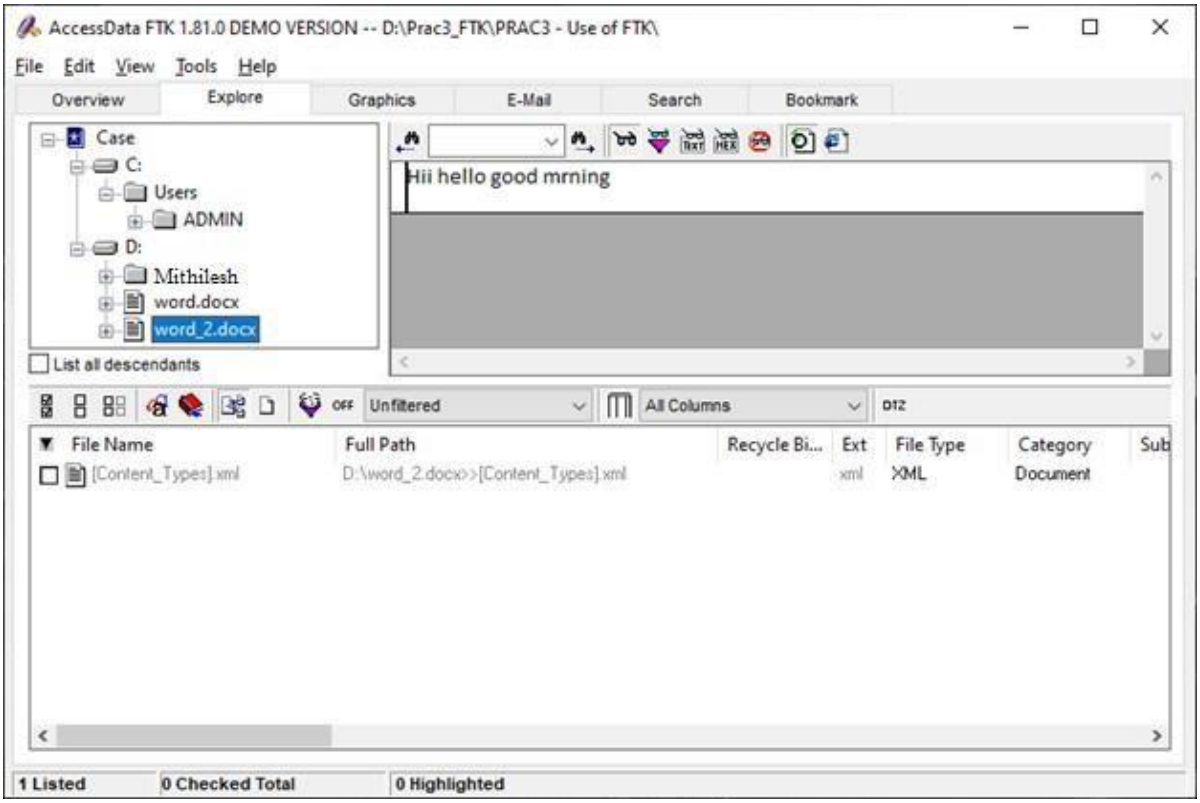
2. In the investigator's name field, enter the name of an investigator or select the name from the drop-down list.
3. In the Case log Entry field, enter the information that you want to add.
4. Click OK.

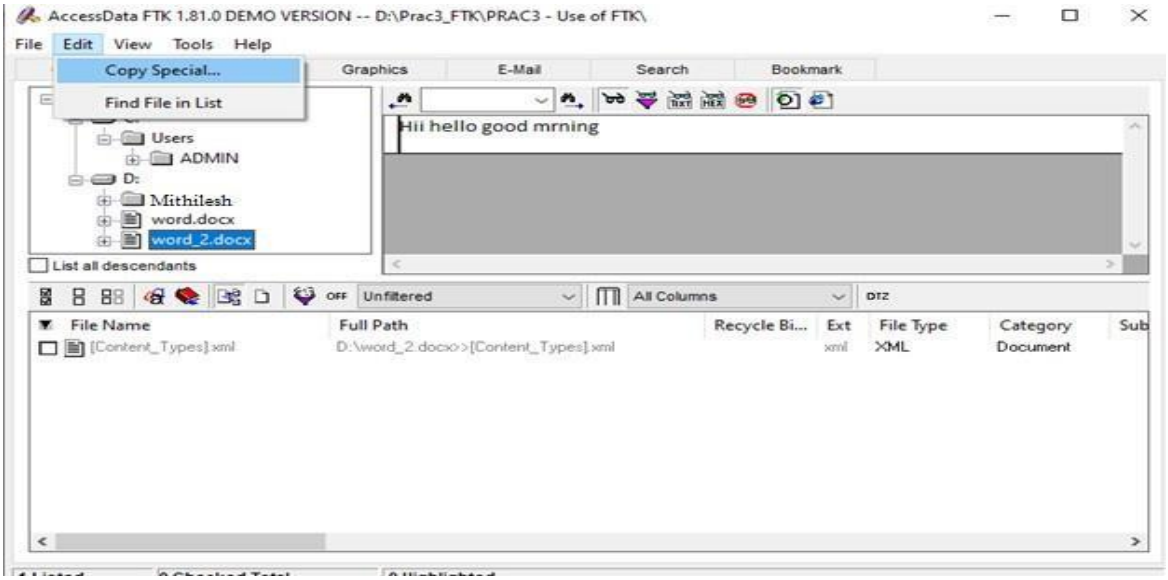


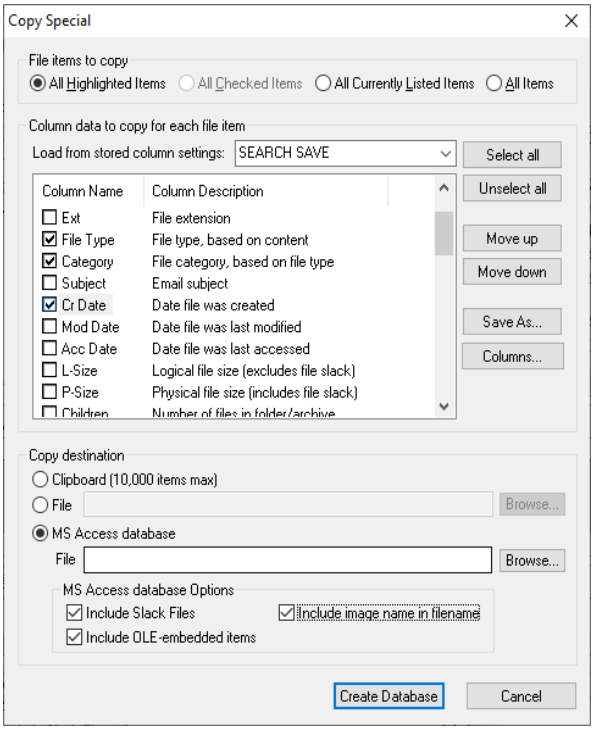
VI. Copying Information from FTK

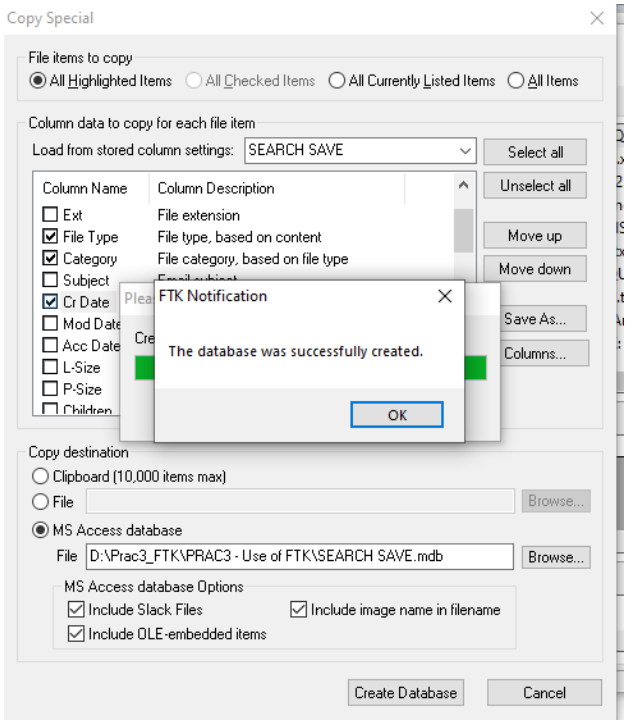
To copy file information:

1. In the file list on any window, select the files that you want to copy information about.
2. Select Edit, and then copy Special.
3. In the File items to copy list, select all checked items.
4. In the Load From Stored Column Settings drop-down list, select the template that contains the file information that you want to copy.
5. Under Copy Destination, select MS Access Database, click Create Database.




AccessData FTK 1.81.0 DEMO VERSION -- D:\Prac3_FTK\PRAC3 - Use of FTK\
File Edit View Tools Help
Copy Special...
Find File in List
Graphics E-Mail Search Bookmark
Users
ADMIN
D:
Mithilesh
word.docx
word_2.docx
List all descendants
Hii hello good mrning
Unfiltered
All Columns
File Name Full Path Recycle Bi... Ext File Type Category
[Content_Types].xml D:\word_2.docx>[Content_Types].xml xml XML Document

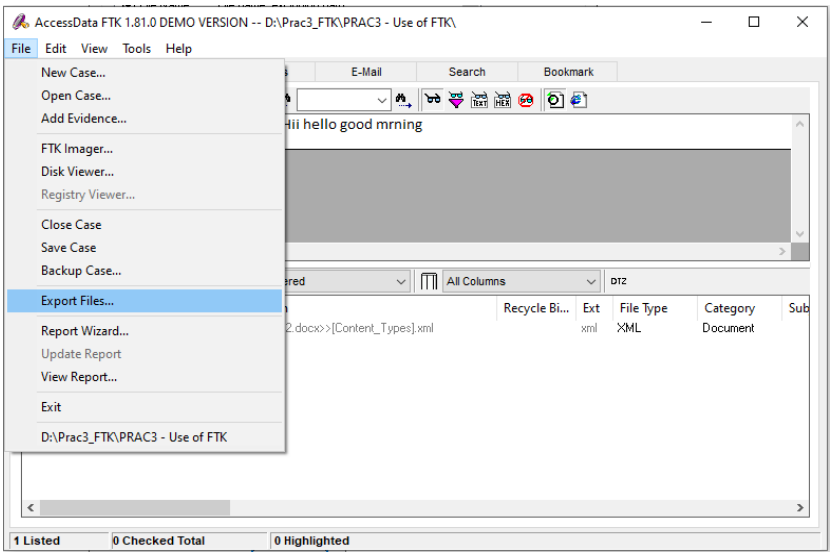

Copy Special
File items to copy
All Highlighted Items All Checked Items All Currently Listed Items All Items
Column data to copy for each file item
Load from stored column settings: SEARCH SAVE
Select all
Unselect all
Move up
Move down
Save As...
Columns...
Column Name Column Description
Ext File extension
File Type File type, based on content
Category File category, based on file type
Subject Email subject
Cr Date Date file was created
Mod Date Date file was last modified
Acc Date Date file was last accessed
L-Size Logical file size (excludes file slack)
P-Size Physical file size (includes file slack)
Copy destination
Clipboard (10,000 items max)
File
Browse...
MS Access database
File
MS Access database Options
Include Slack Files
Include image name in filename
Include OLE-embedded items
Create Database
Cancel


Copy Special
File items to copy
All Highlighted Items All Checked Items All Currently Listed Items All Items
Column data to copy for each file item
Load from stored column settings: SEARCH SAVE
Select all
Unselect all
Move up
Move down
Save As...
Columns...
Column Name Column Description
Ext File extension
File Type File type, based on content
Category File category, based on file type
Subject
Cr Date
Mod Date
Acc Date
L-Size
P-Size
FTK Notification
The database was successfully created.
OK
Copy destination
Clipboard (10,000 items max)
File
Browse...
MS Access database
File D:\Prac3_FTK\PRAC3 - Use of FTK\SEARCH SAVE.mdb
MS Access database Options
Include Slack Files
Include image name in filename
Include OLE-embedded items
Create Database
Cancel

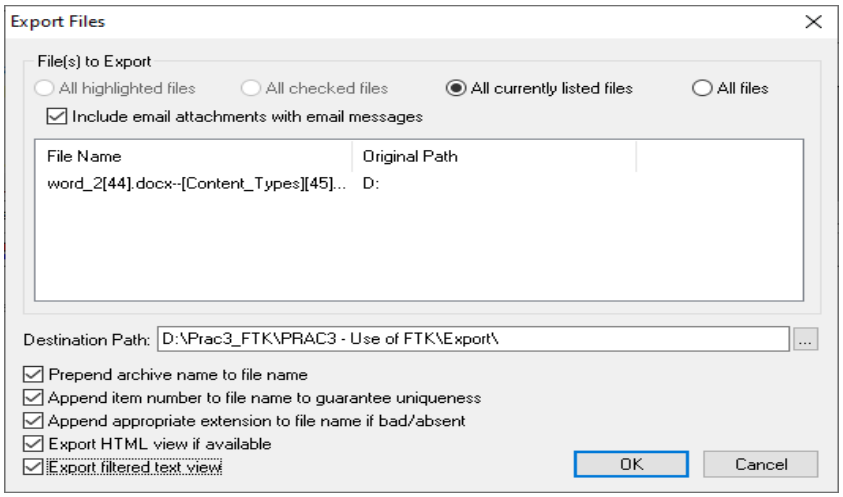
VII. Exporting Files

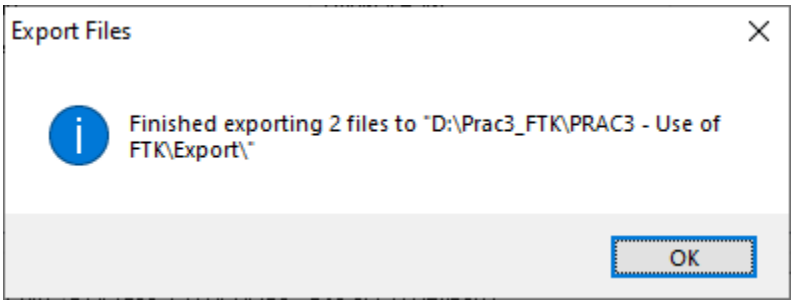
To manually export files without maintaining the directory structure,

1. Select File, and then Export Files.



2. Select the files to export.
3. If you want to export e-mail attachments, check Include E-mail Attachments with Email Messages.
4. In the Destination Path field, browse to and select the location where you want to export the files.
5. If you want to add the archive name to the filename, check Prepend Archive Name to filename.
6. If you want to add the item number after the filename, check Append Item Number to filename to guarantee uniqueness.
7. If you want to add a appropriate extension to a file that is missing an extension or has a bad extension, check Append appropriate Extension to filename id Bad/Absent.
8. To export the file in the same formatting as seen in the FTK program, check HTML, view if Available. Some files may not be available in this view.
9. To export files in which readable text is filtered out of binary files, check Export Filtered Text View.
10. Click OK.

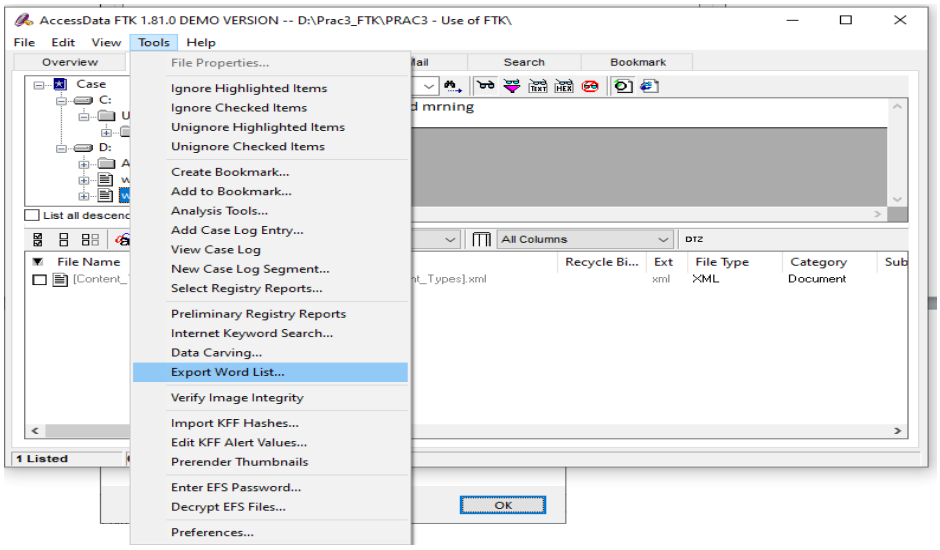


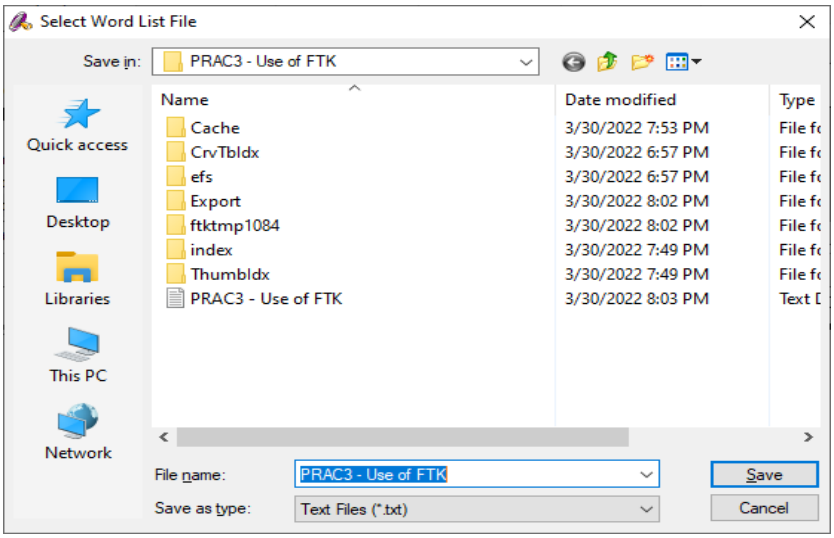


VIII. Exporting word list

To export the word list:

1. Select Tools, and the Export Word List.
2. Select the file and location that you want to write the word list to. The default filename is case_name.txt.
3. Click Save.



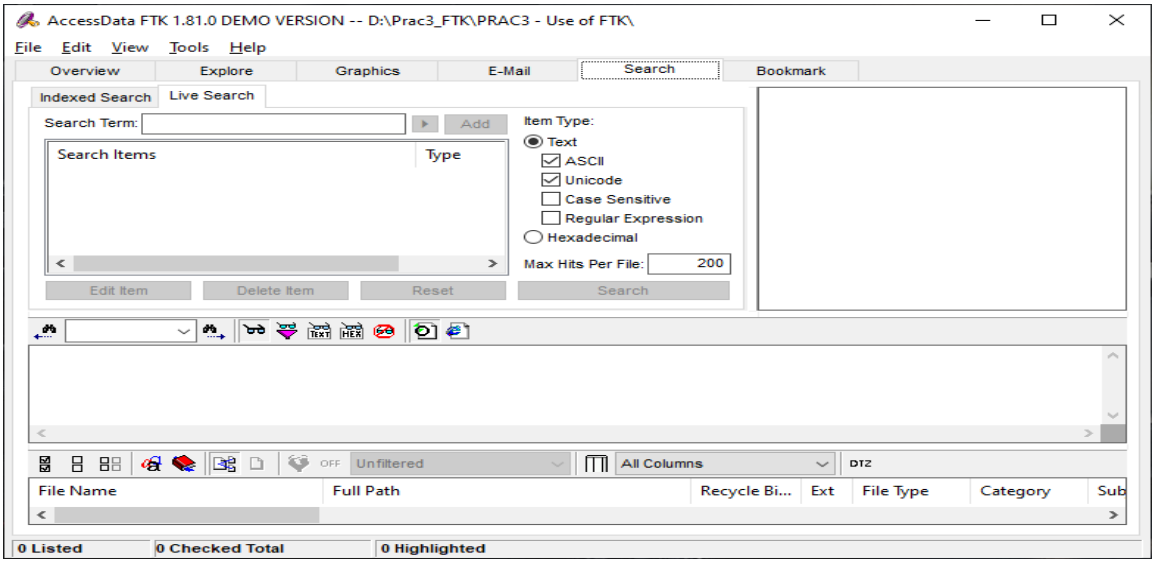


D. Searching a Case

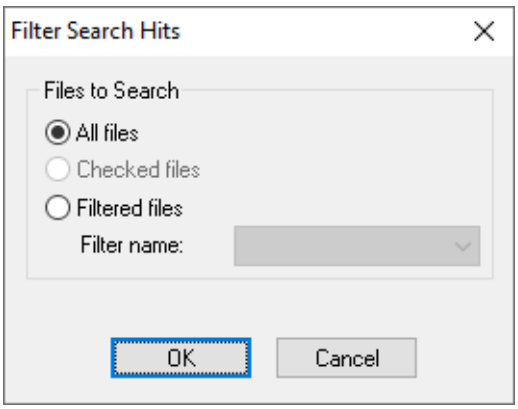
I. Condition to Live search

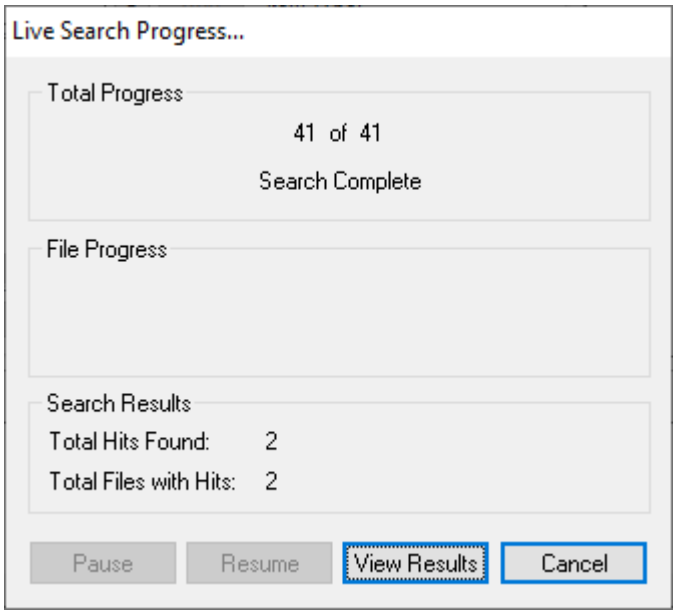
To perform a live search:

1. In the search window, Click Live Search.



2. In the search Term field, enter the term you want to search for.
3. In the item type column, specify if you want FTK to search in Text or hexadecimal.



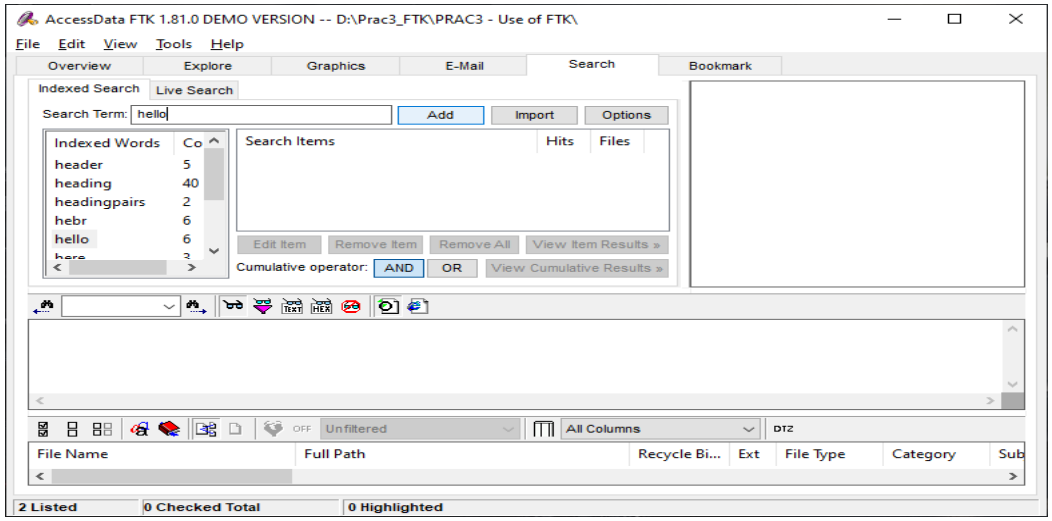


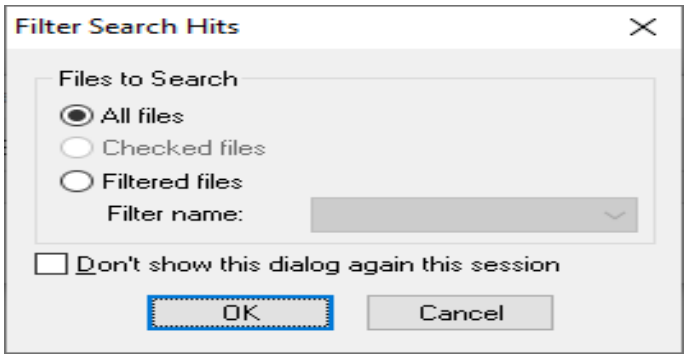
II. Conducting an Indexed Search

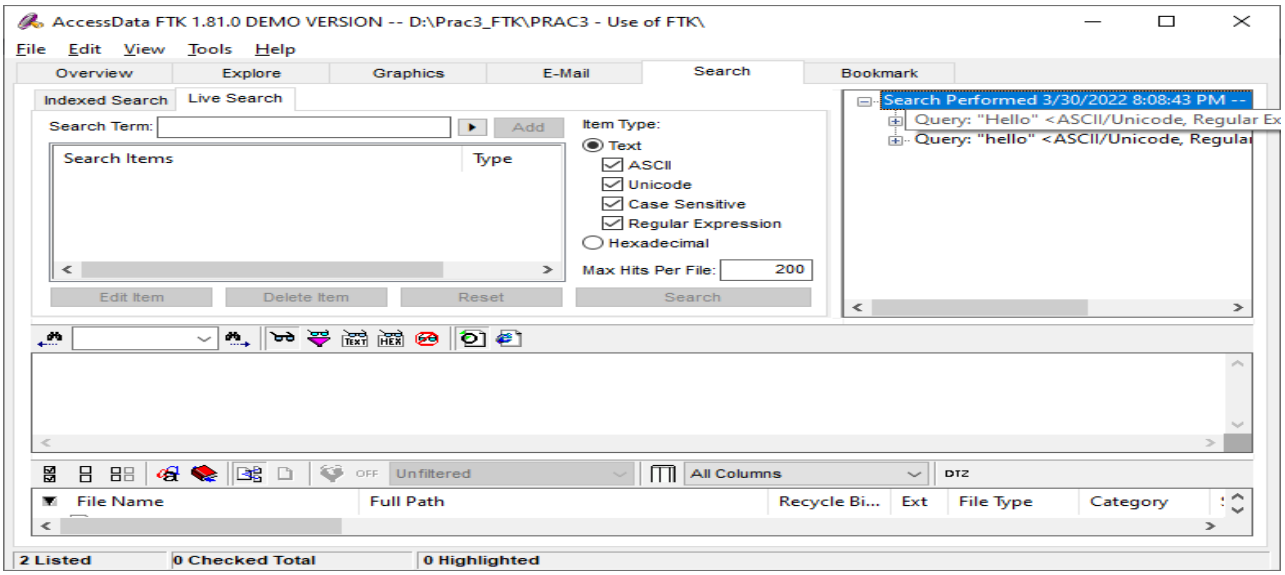
A. A Single-term Searches

To perform a single-term Indexed search:

1. In the search window, click Indexed Search.
2. In the Search Term field, enter the term you want to search for, including any wildcard characters.
3. Click Add to add the search term to the search list.
4. In the Search Items column, select the index term you want to search.
5. Click View Item Results to initiate the search. The Filter search hites dialog box appears.
6. In the Filter Search Hits dialog. Select All Files.
7. Click OK.



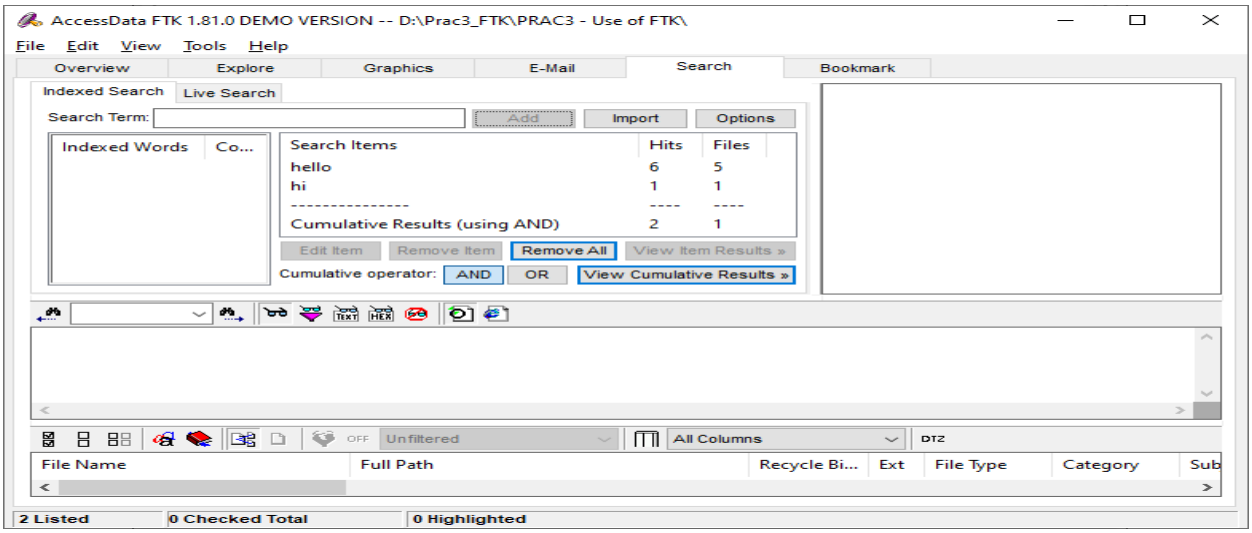




B. Multi-term Searches

To perform a multi-term Indexed search:

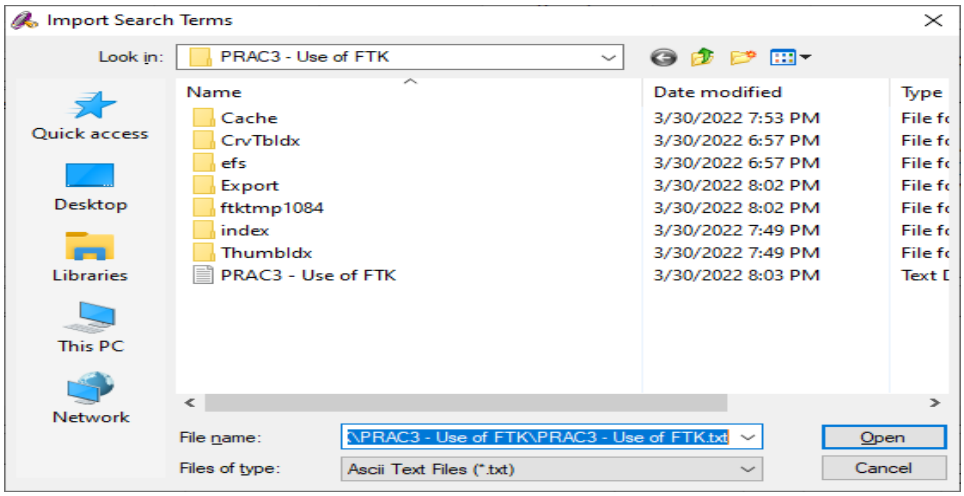
1. In the search window, click Indexed Search.
2. In the Search Term field, enter the term you want to search for, including any wildcard characters.
3. Click Add to add the search term to the search list.
4. Define your search opeators:
    a. Click AND to search for items containing all the terms.
    b. Click OR to search for items containing any of the terms.
5. Click View Cumulative Results to initiate the search. The Filter Search Hits dialog appears.
6. In the Filter Search Dialog, select All Files.
7. Click OK.



C. Importing Search Terms

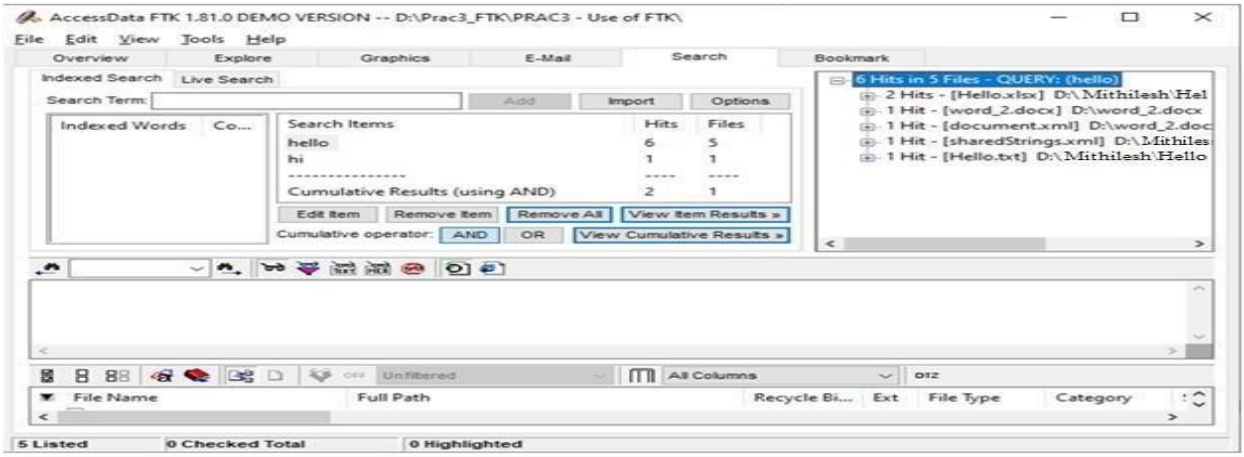
To import search terms

1. In the search window, click Indexed search
2. Click Import.
3. Select the text file containing the search content.
4. Select Yes or No to display terms that file contains.



D. Viewing Search Results

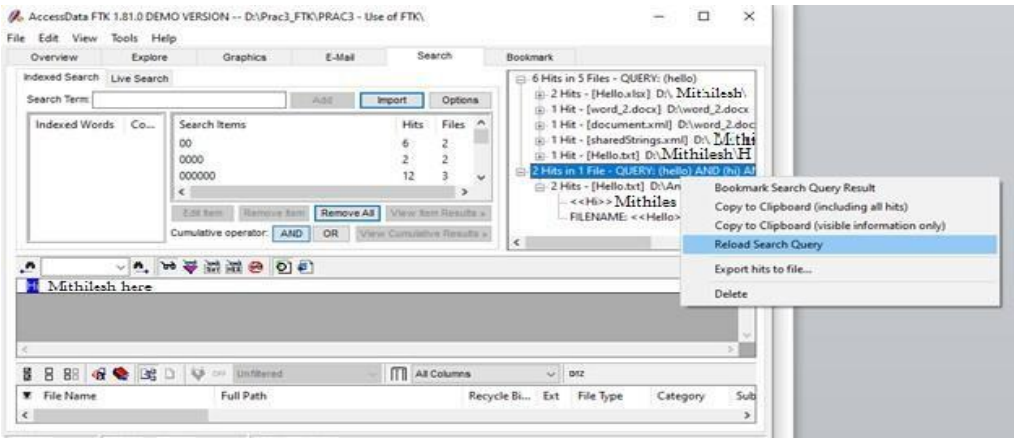
1. The result of each search appear as separate line items in the search results list.
2. Click the plus (+) sign next to a search line to expand the search results. Individual search results are listed in the search and file lists.
3. To view a specific item, select the file in the search results or file lists. All search results are highlighted in the file.



E. Reloading a search query

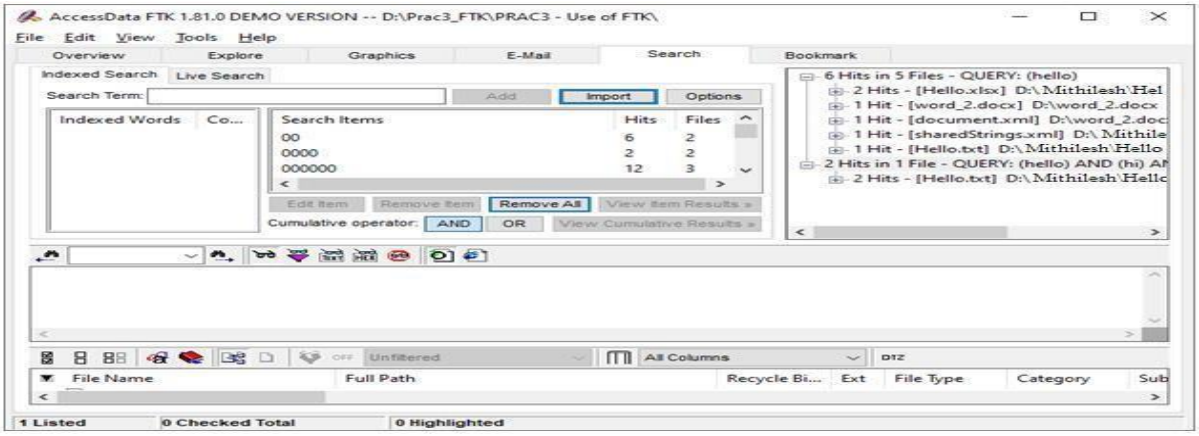
To reload a query:

1. Select the query in the search results list.
2. Right click and select Reload Search Query from the quick menu.

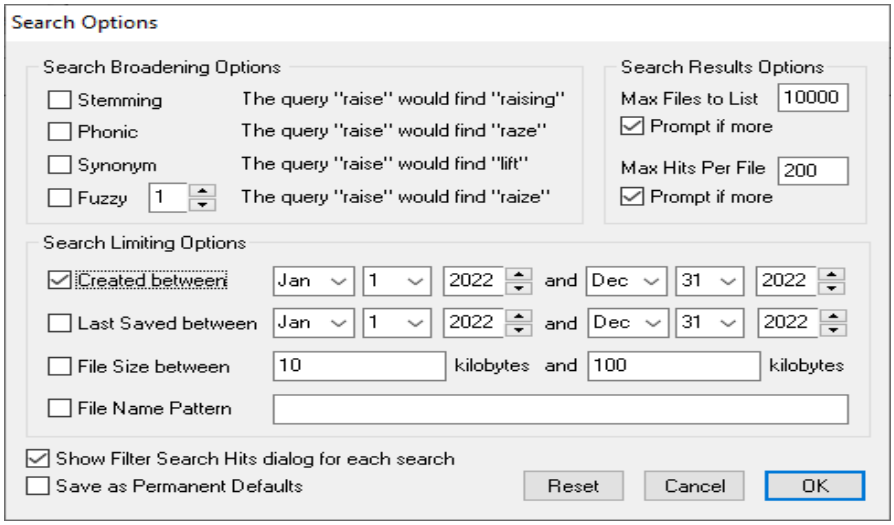


F. Wildcard Character

1. You may search among wildcard characters.



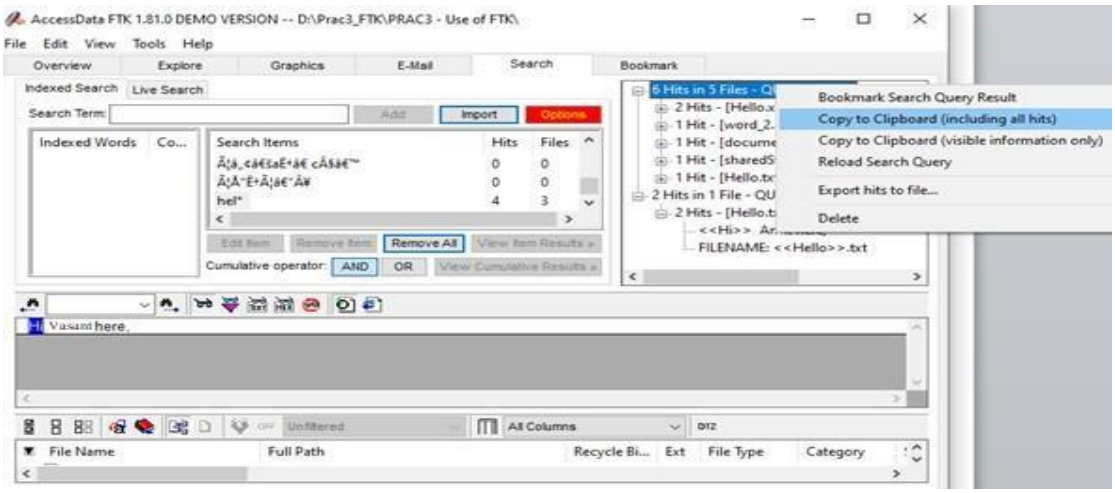
G. Indexed Search Options



III. Documenting Search Results

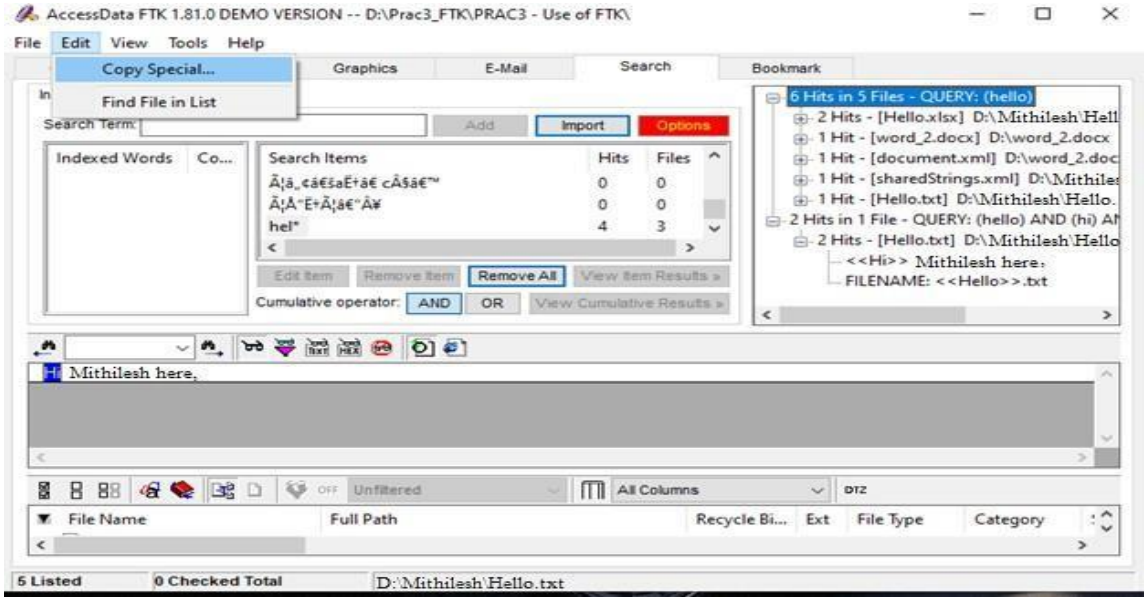
A. Copying search results to clipboard

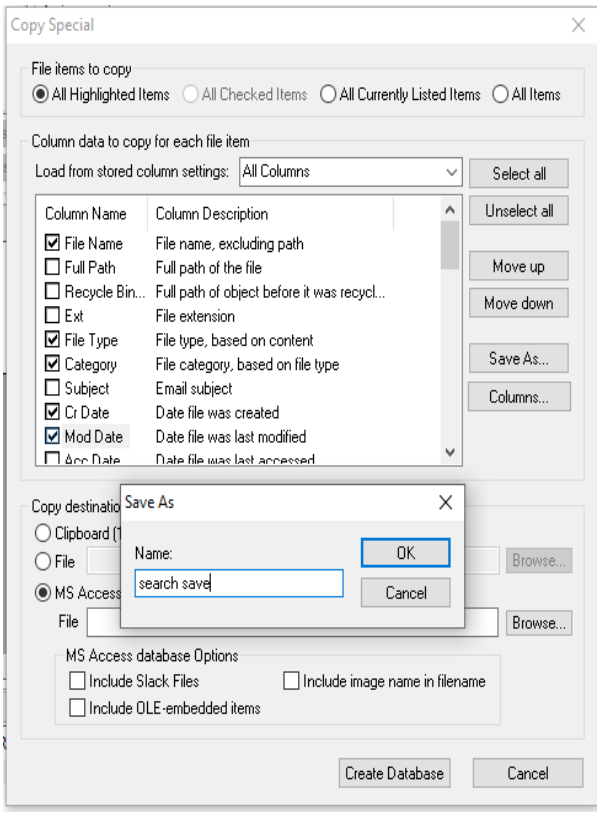
1. When you right-click in the search results list, the quick menu displays the following options.
    - Copy to Clipboard (including all hits)
    - Copy to Clipboard (Visible information only)
2. Copy to clipboard (including all hits) copies all the information for all the searches to the clipboard. This means that even if the search line is not expanded, the results of that search are copied to the clipboard.
3. Copy to clipboard (visible information only) only copies the currently viewed information in the clipboard. This means that search results are not copied to the clipboard unless the search line is expanded.

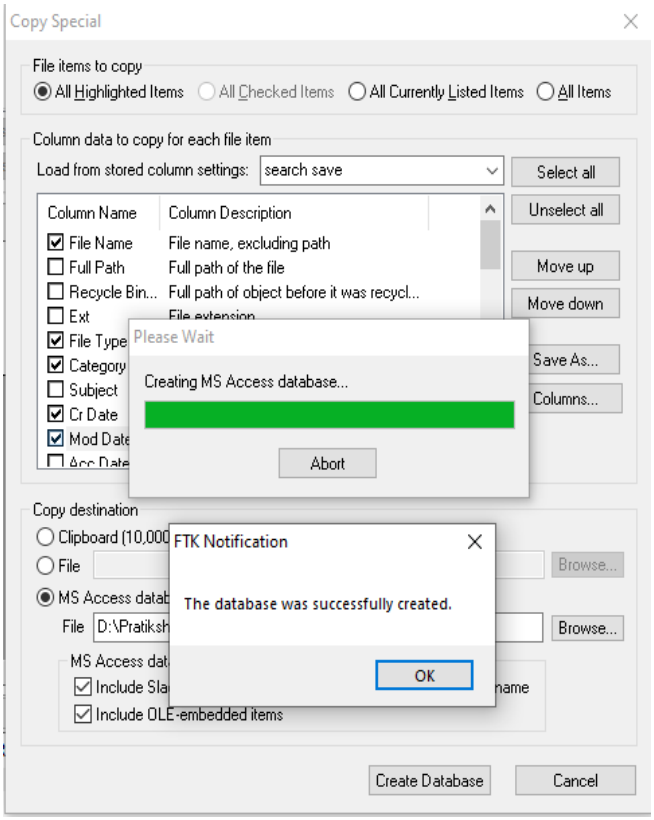


B. Using copy special to document search results

1. In the Search Results list, highlight the search you want to document.
2. Select Edit, and the Copy Special.
3. In the File Items to Copy list, select All Highlighted Items.
4. In the Load from Stored column settings drop-down list, select the template that contains the file information that you want to copy.
5. To create a new column setting, Click Save As, enter a name in the field, and click OK.
6. Under Copy Destination, select MS Access Database and Click Create Database.



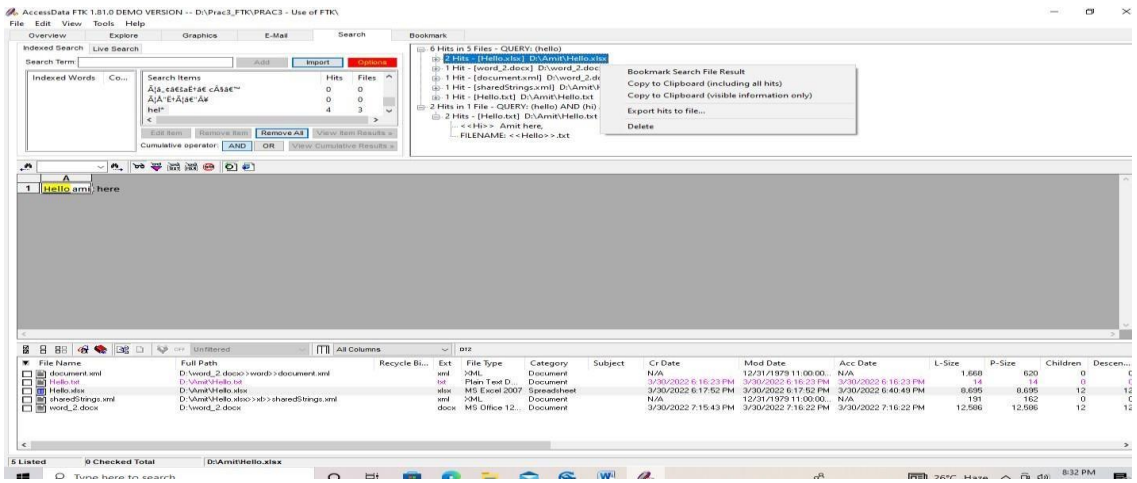


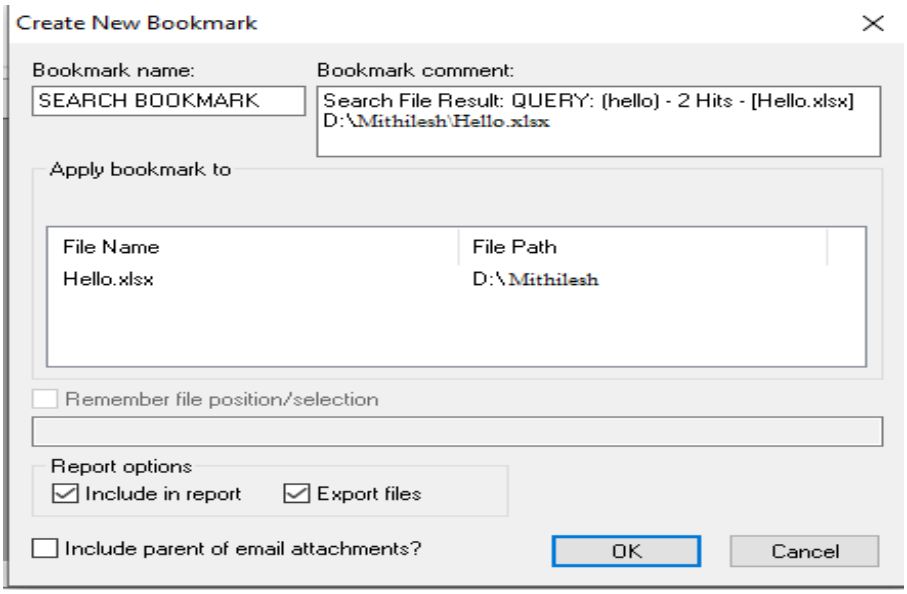


C. Bookmarking Search Results

To create a bookmark from the search results list:

1. Select the search you want to bookmark.
2. Right click and select Bookmark Search Query Result from the quick menu.
3. In the Create New Bookmark form, enter details.
4. Click OK.

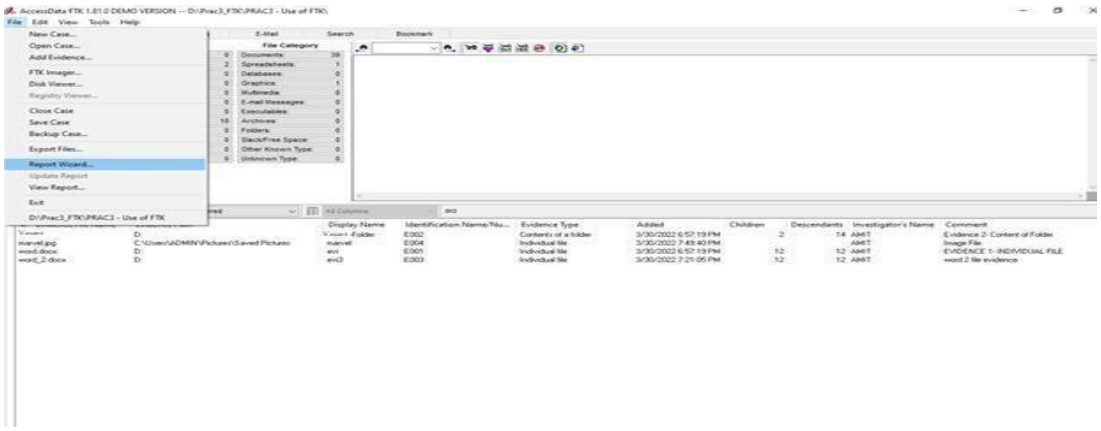




D. Generating Reports using Access Data FTK

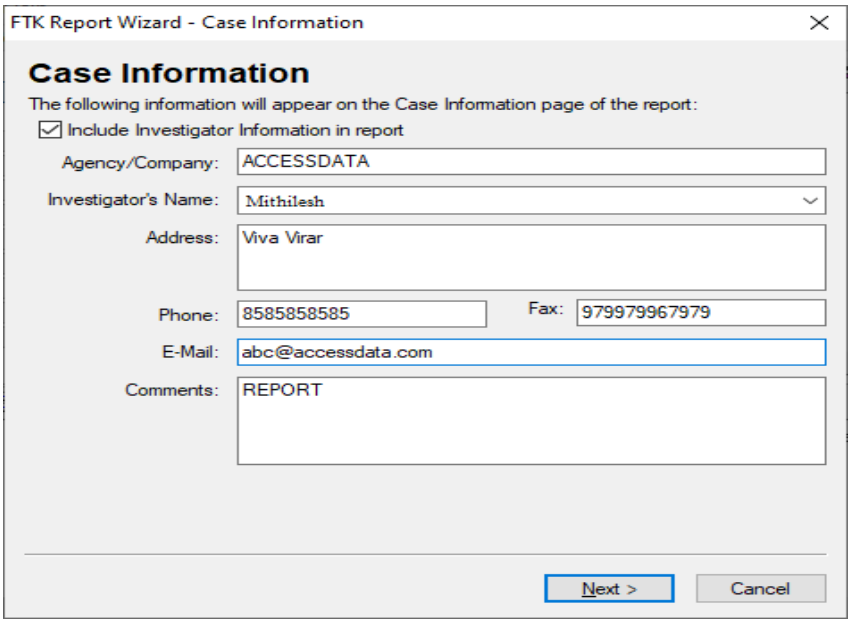
I. Creating a Report

1. Select file and then Report Wizard.



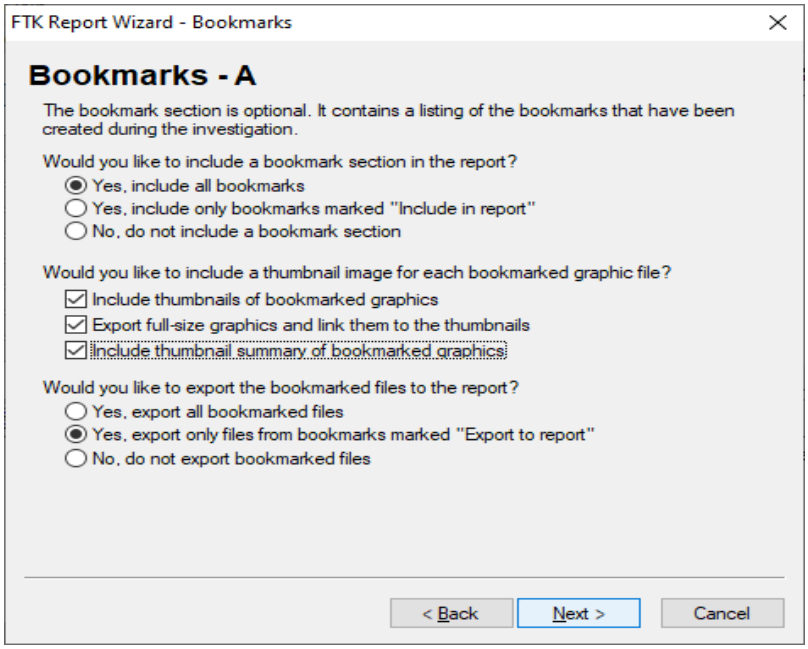
a. Entering basic case information

1. Check Include Investigator information in Report check box.
2. Enter Company, Investigator name, Address, Phone, Fax, E-mail and Comments details.
3. Click Next.



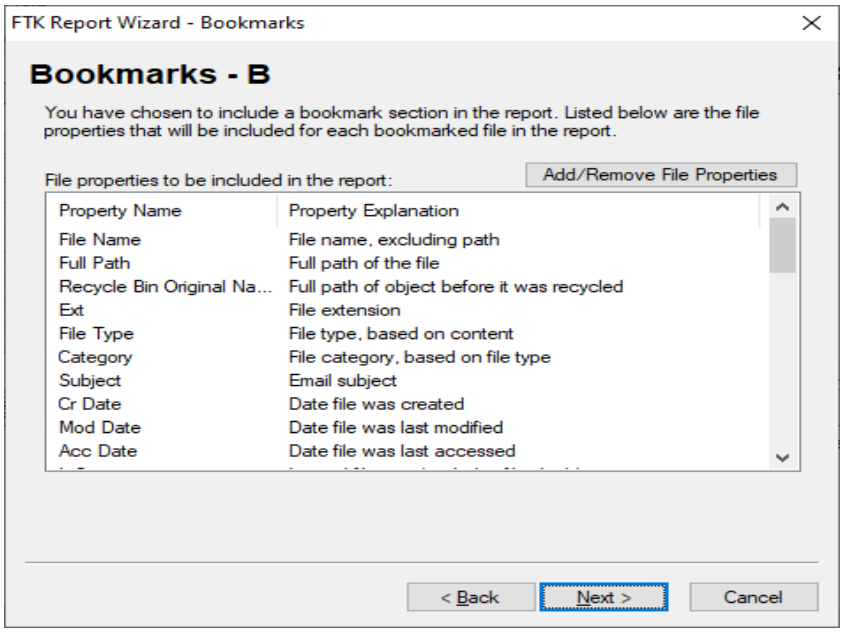
b. Managing Bookmarks

1. The Bookmarks- A form allows you to create a section in the report that lists the Bookmarks that were created during the case investigation.
2. Select appropriate option.
3. Click Next.



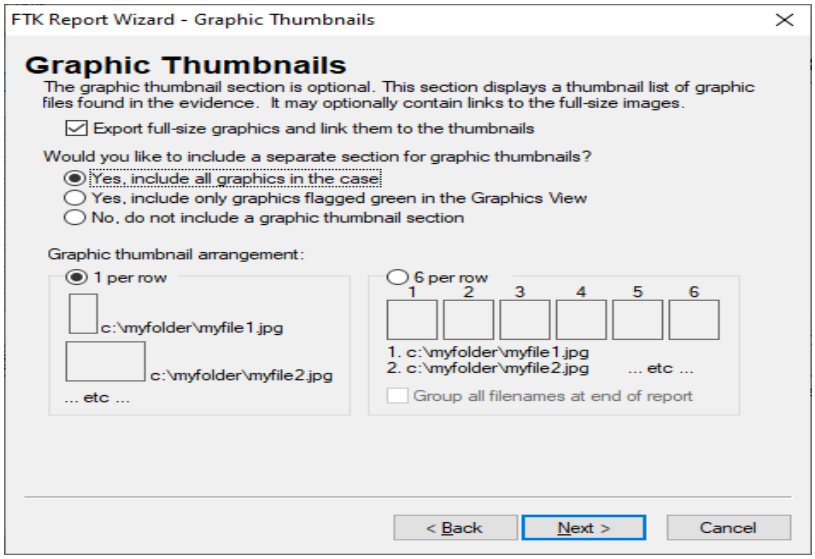
C. Selecting the properties of Bookmarked files

1. The Bookmarks-B form allows you to select which file properties to include for each bookmarked file.
2. Review the file properties to be included in the report.
3. Click Next.



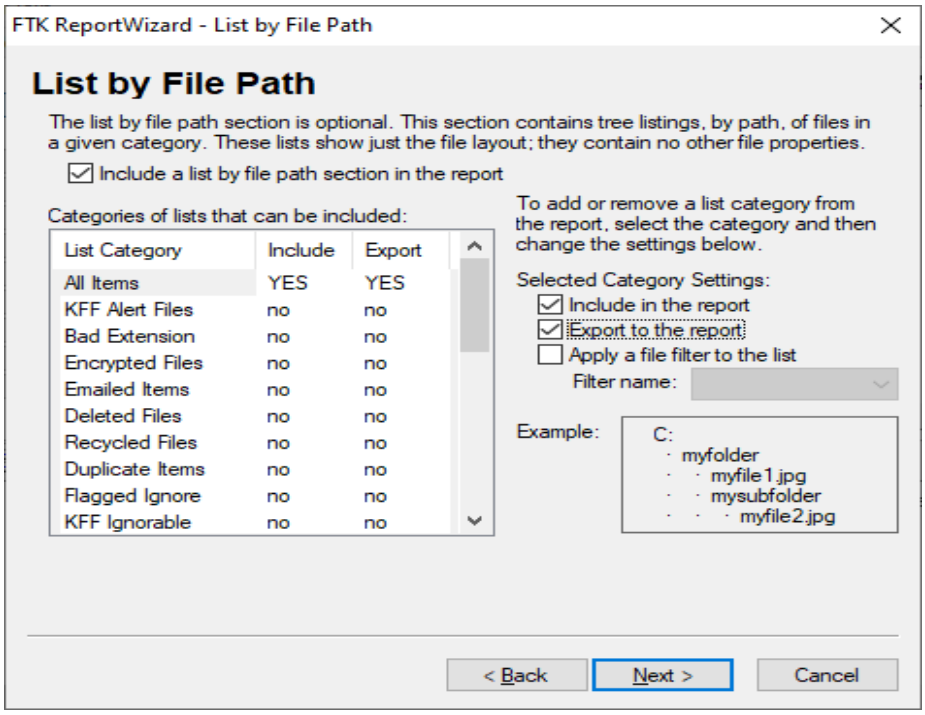
D. Managing Thumbnails

1. The Graphic Thumbnails form allows you to create a section in the report that displays thumbnail images of the case graphics.
2. Select appropriate options.
3. Click Next.



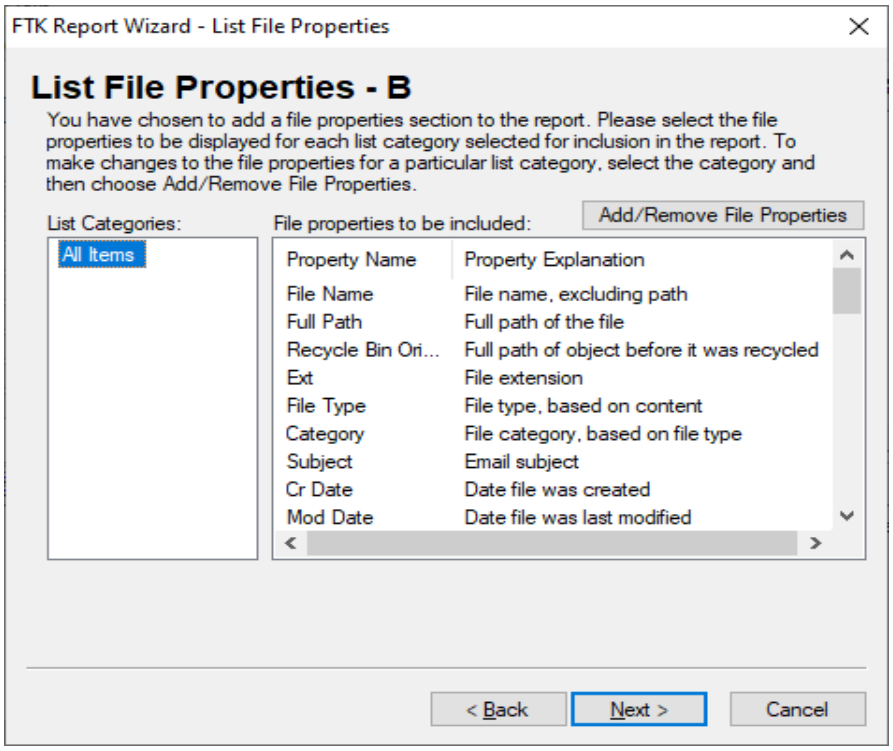
E. Selecting a File Path List

1. The list by file path form allows you to create a section in the report that lists the file paths of files in the selected categories. The List by file path section simply displays the file and their file paths.
2. Check the Include the List by File Path Section in the Report box.
3. In the Categories of Lists that can be Included list, select which file categories to include in the list. Here, select All items, Document files, Database Files, and Graphic Files.
4. Check the Include in the Report box.
5. Check the Export to the Report box.
6. Click Next.



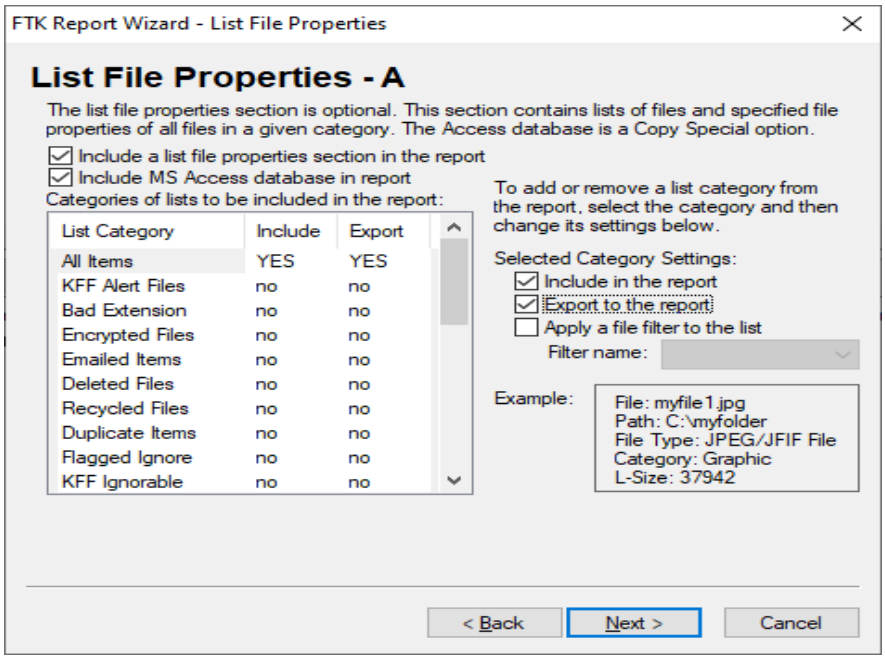
F. Selecting File properties list

1. The List File properties-A form allows you to create a section in the report that lists file properties for files in selected categories.
2. Check the Include a List File Properties Section in the Report box.
3. Check the Include MS Access Database in the Report box.
4. In the categories of Lists to be Included in the Report list, select which files categories to include in the list.
5. Check the Include in the Report box.
6. Check the Export to the Report box.
7. Click Next.



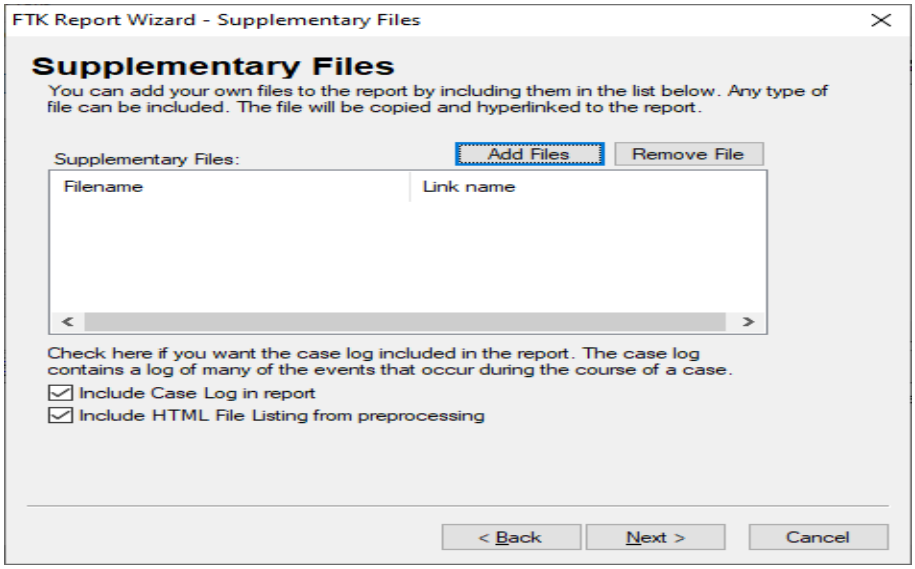
G. Selecting the Properties of the File Properties List

1. The List file properties-B form allows you to select which file properties are displayed for file in the categories specified in the previous form.
2. From the Last categories column, select the category that you want to specify file properties for and review the properties listed for it.



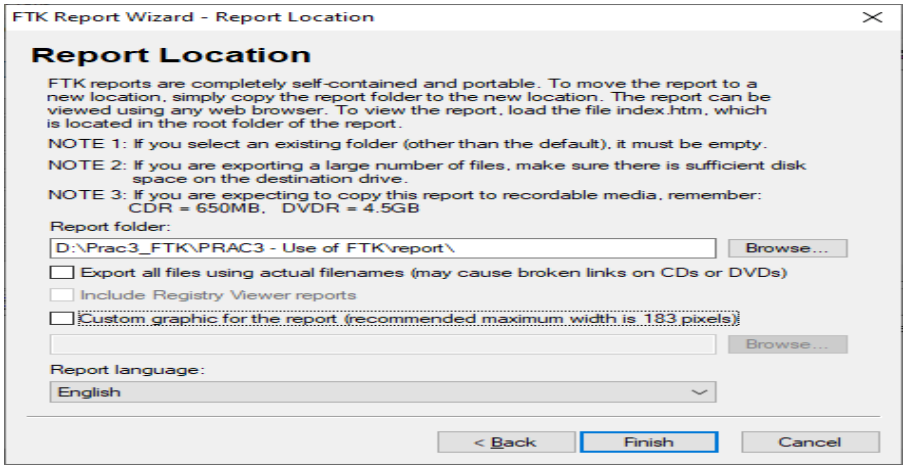
H. Adding Supplementary Files and the case Log

1. If you want to add a supplementary file, Click Add Files and browse to the file you want to include in the report.
2. If you want to add the case log to the report, Click the Include Case Log in Report box.
3. If you crossed an HTML file listing in preprocessing, you can add it in your reports.
4. Click Next.



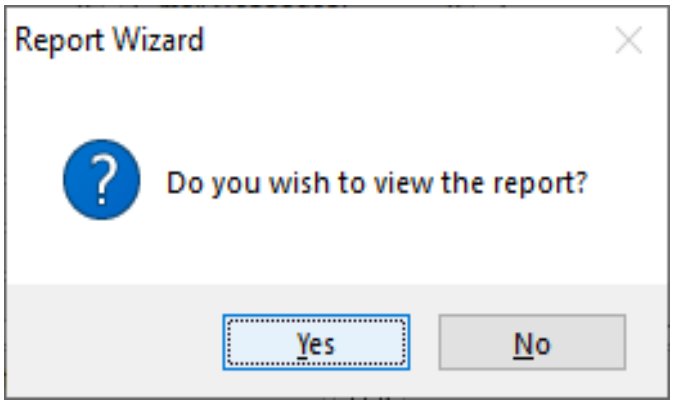
I. Selecting the Report Location

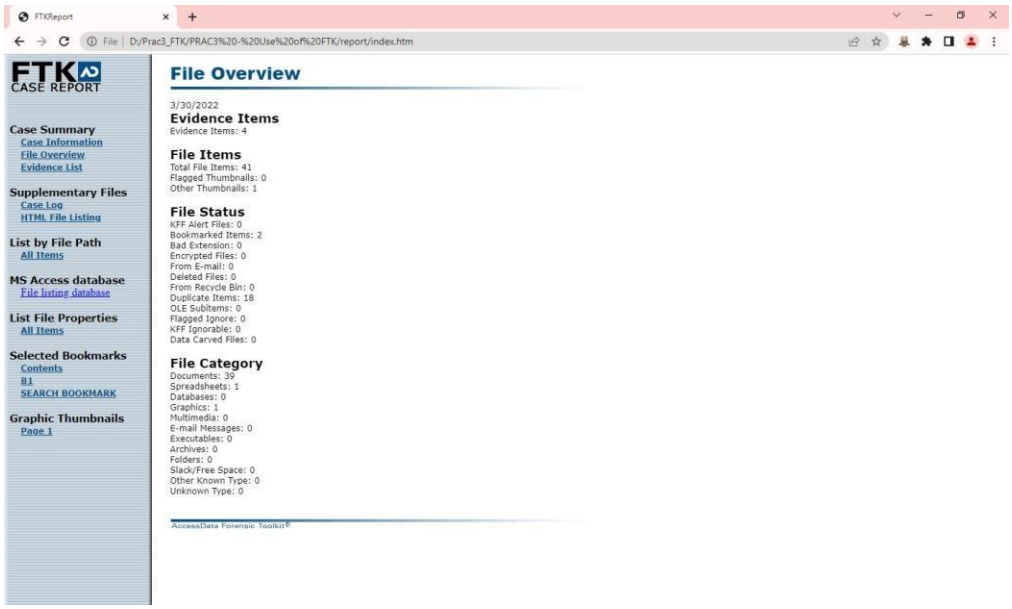
1. In the Report folder field, browse to and select the location for the report folder.
2. Select the language for the report from the Report Language drop-down list.
3. Click Finish.

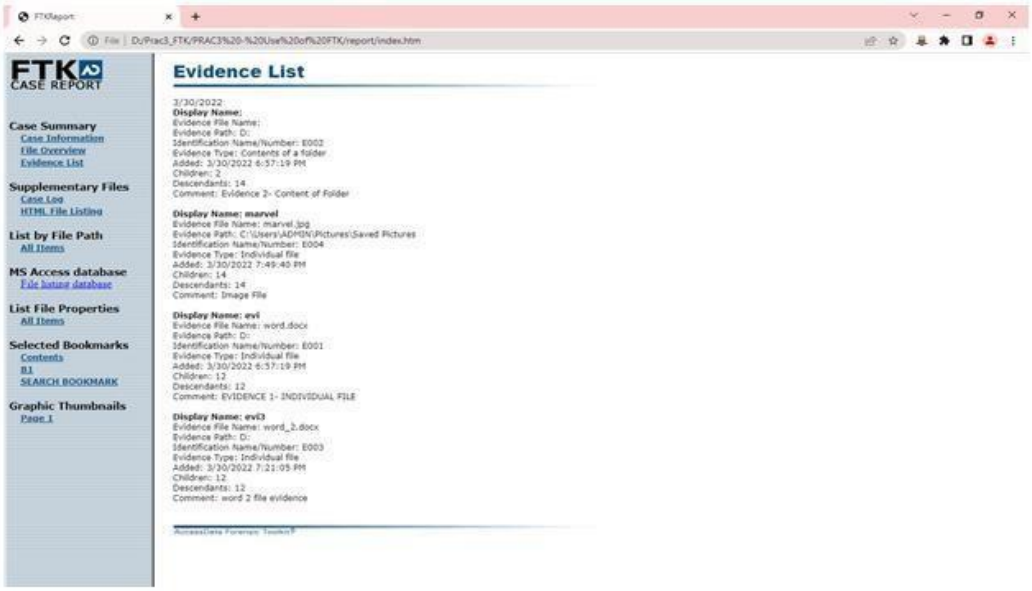


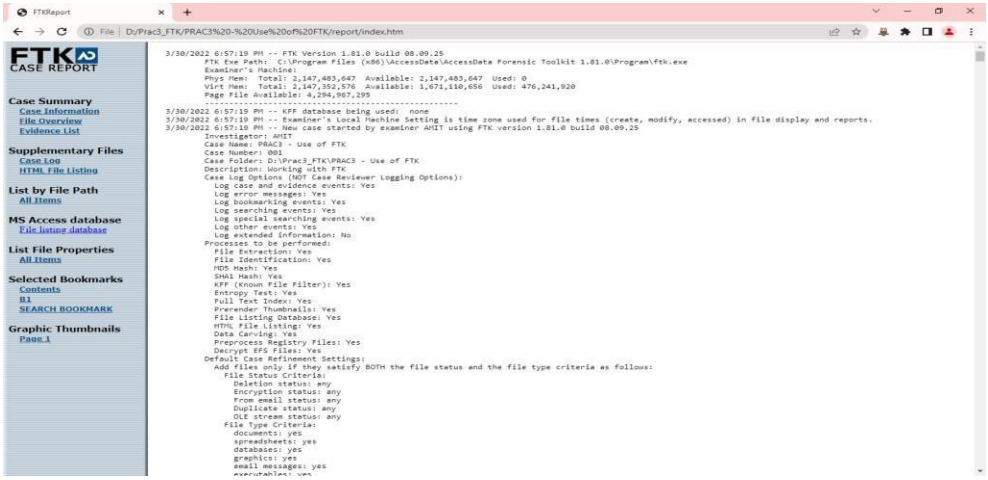
II. Viewing and distributing the Report

1. The report contains the information that you selected in the report wizard i.e index.html
2. To view the report in FTK
    - Immediately after creating the report, click yes to view the report.
    - Select File, and then View report.



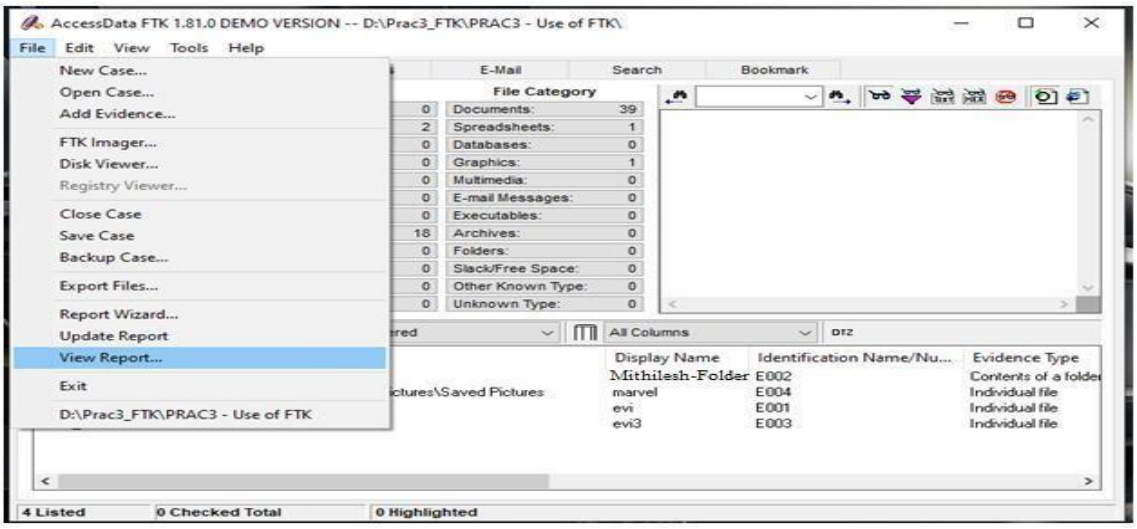

FTKReport
D:/Prac3_FTK/PRAC3%20-%20Use%20of%20FTK/report/index.htm
FTK
CASE REPORT
Case Summary
Case Information
File Overview
Evidence List
Supplementary Files
Case Log
HTML File Listing
List by File Path
All Items
MS Access database
File listing database
List File Properties
All Items
Selected Bookmarks
Contents
B1
SEARCH BOOKMARK
Graphic Thumbnails
Page 1
File Overview
3/30/2022
Evidence Items
Evidence Items: 4
File Items
Total File Items: 41
Flagged Thumbnails: 0
Other Thumbnails: 1
File Status
KFF Alert Files: 0
Bookmarked Items: 2
Bad Extension: 0
Encrypted Files: 0
From E-mail: 0
Deleted Files: 0
From Recycle Bin: 0
Duplicate Items: 18
OLE Subitems: 0
Flagged Ignore: 0
KFF Ignorable: 0
Data Carved Files: 0
File Category
Documents: 39
Spreadsheets: 1
Databases: 0
Graphics: 1
Multimedia: 0
E-mail Messages: 0
Executables: 0
Archives: 0
Folders: 0
Slack/Free Space: 0
Other Known Type: 0
Unknown Type: 0
AccessData Forensic Toolkit®


FTKReport
D:/Prac3_FTK/PRAC3%20-%20Use%20of%20FTK/report/index.htm
FTK
CASE REPORT
Case Summary
Case Information
File Overview
Evidence List
Supplementary Files
Case Log
HTML File Listing
List by File Path
All Items
MS Access database
File listing database
List File Properties
All Items
Selected Bookmarks
Contents
B1
SEARCH BOOKMARK
Graphic Thumbnails
Page 1
Evidence List
3/30/2022
Display Name:
Evidence File Name:
Evidence Path: D:
Identification Name/Number: E002
Evidence Type: Contents of a folder
Added: 3/30/2022 6:57:19 PM
Children: 2
Descendants: 14
Comment: Evidence 2- Content of Folder
Display Name: marvel
Evidence File Name: marvel.jpg
Evidence Path: C:\Users\ADMIN\Pictures\Saved Pictures
Identification Name/Number: E004
Evidence Type: Individual file
Added: 3/30/2022 7:49:40 PM
Children: 14
Descendants: 14
Comment: Image File
Display Name: evi
Evidence File Name: word.docx
Evidence Path: D:
Identification Name/Number: E001
Evidence Type: Individual file
Added: 3/30/2022 6:57:19 PM
Children: 12
Descendants: 12
Comment: EVIDENCE 1- INDIVIDUAL FILE
Display Name: evi3
Evidence File Name: word_2.docx
Evidence Path: D:
Identification Name/Number: E003
Evidence Type: Individual file
Added: 3/30/2022 7:21:05 PM
Children: 12
Descendants: 12
Comment: word 2 file evidence



III. Updating Report

1. To update report, select file, and then Update Report.



IV. Modifying Report

A. Modifying reports in the same FTK session

1. Select File, and then Report Wizard.
2. Make the changes that you want as you complete the Wizard.
3. On the Report Location form, Click Finish to overwrite the existing report with the new version.

B. Modifying reports in the different FTK session

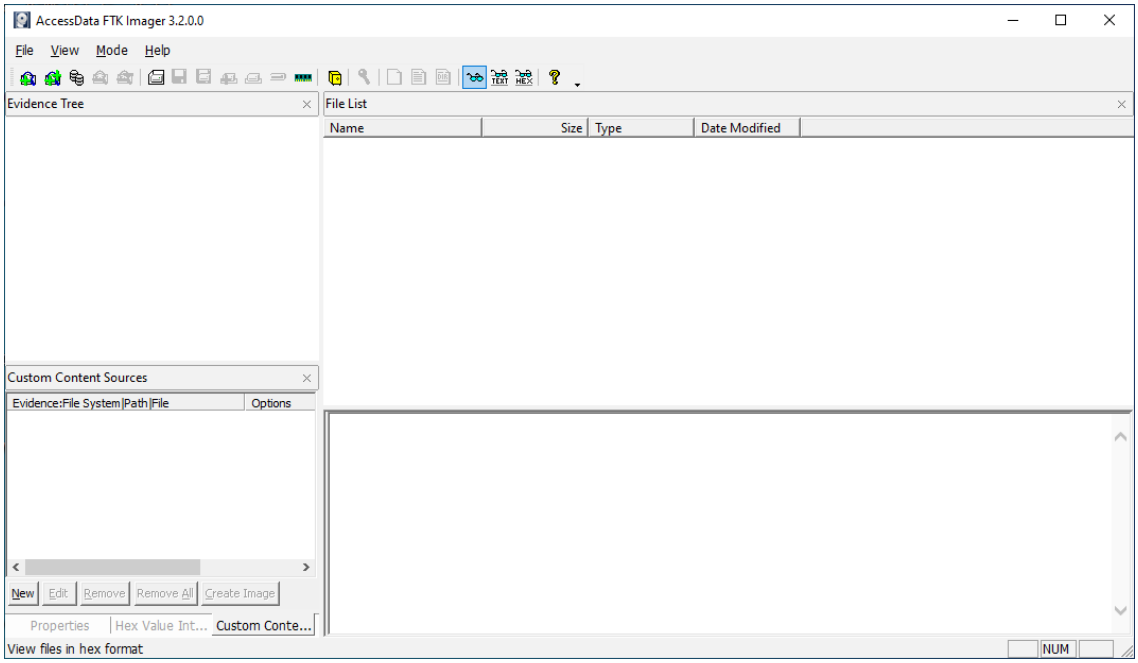
1. Select File, and then Report Wizard.
2. Complete the Wizard.
3. On the Report Location form, Click Finish if you want to overwrite the existing report with the new version.

Practical No 4a

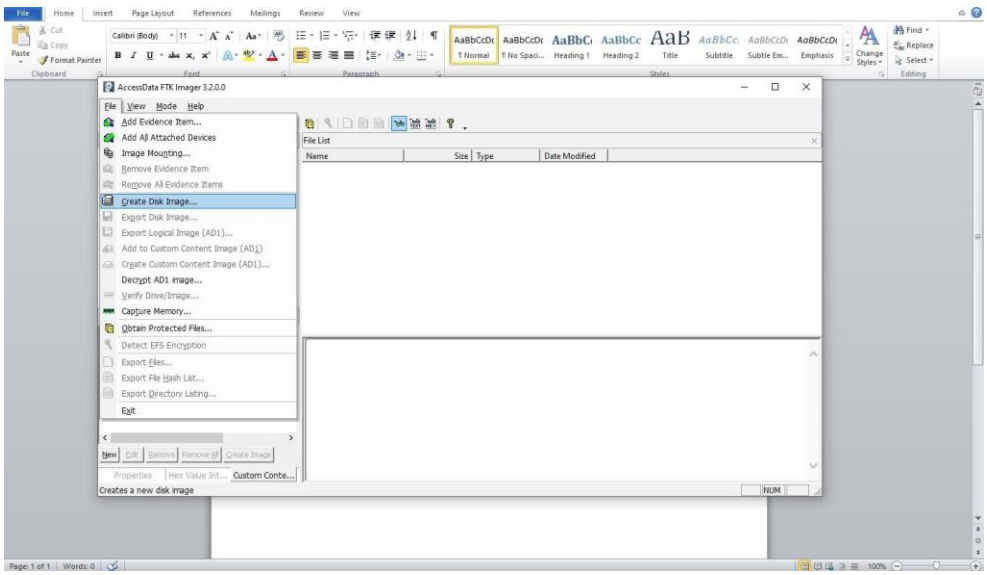
Aim: Using file recovery tools [FTKImager] Creating Image

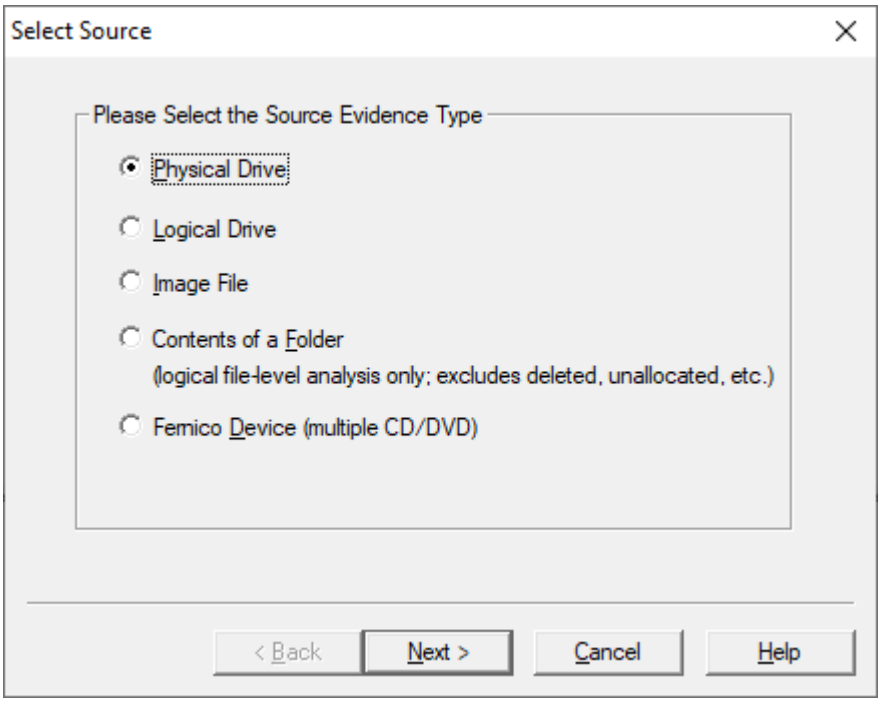
Steps:

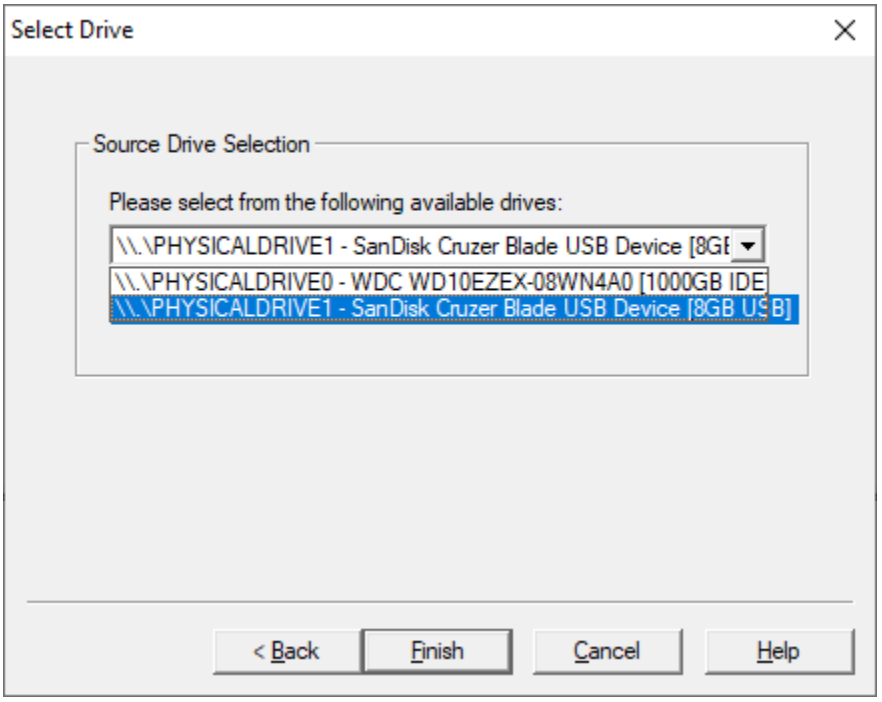
1. Run FTK Imager.exe to start the tool



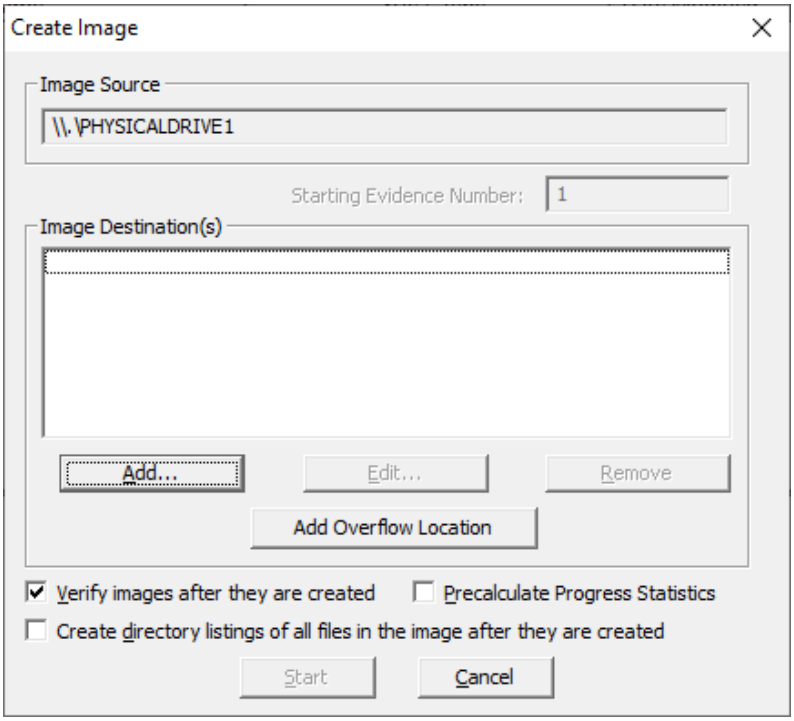
2. From file menu select create a disk image and choice the source of your image



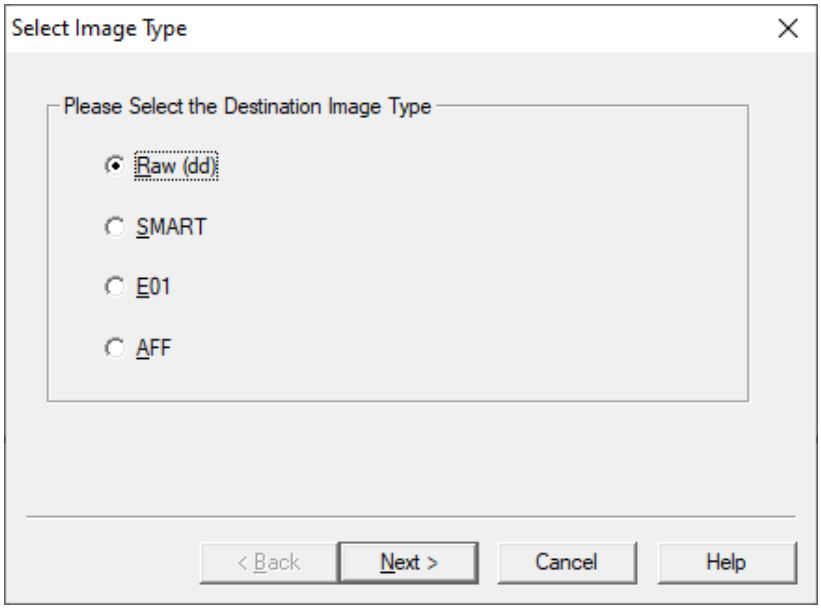

Select Source
Please Select the Source Evidence Type
Physical Drive
Logical Drive
Image File
Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
Femico Device (multiple CD/DVD)
< Back
Next >
Cancel
Help


Select Drive
Source Drive Selection
Please select from the following available drives:
\\.\PHYSICALDRIVE1 - SanDisk Cruzer Blade USB Device [8GB
\\.\PHYSICALDRIVE0 - WDC WD10EZEX-08WN4A0 [1000GB IDE]
\\.\PHYSICALDRIVE1 - SanDisk Cruzer Blade USB Device [8GB USB]
< Back
Finish
Cancel
Help

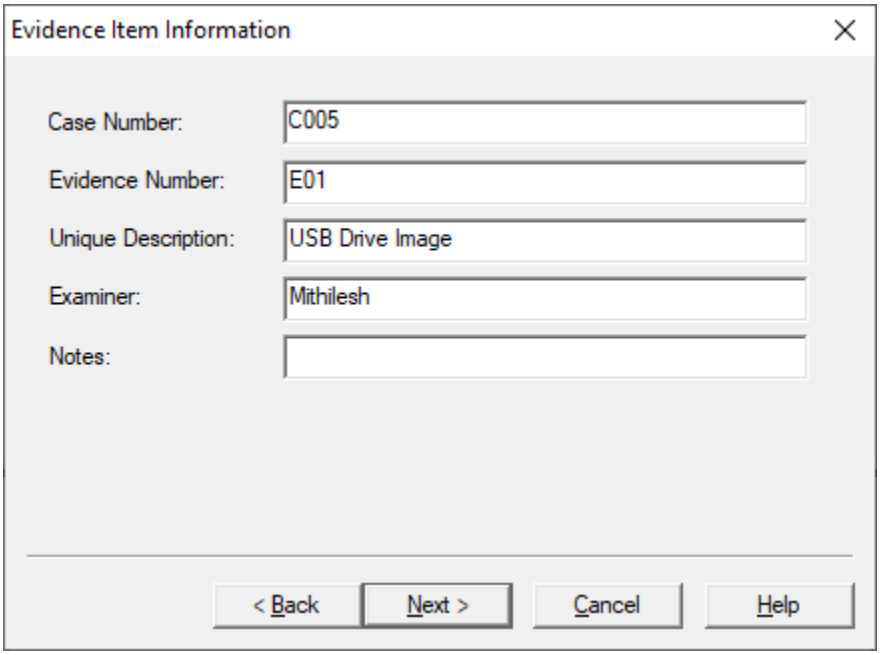
3. Click ADD to add the image destination. Check verifies images after they are created so FTK Imager will calculate MD5 and SHA1 hashes of the acquired image.



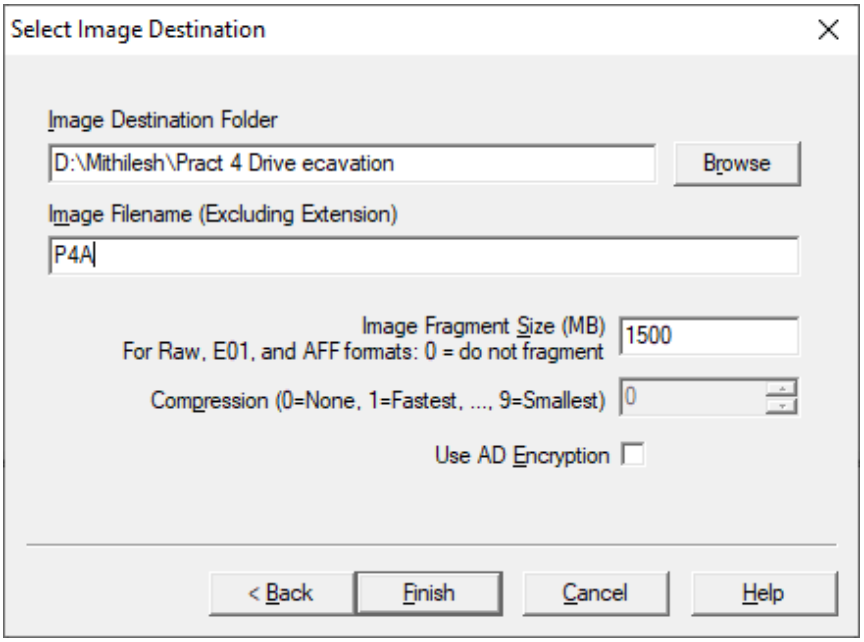
4. Next select the image type. The type you choose will usually depend on what tools you plan to use on the image. The dd format will work with more open source tools but you might want SMART or E01 if you will primarly be working with ASR Expert witness or Encase respectively.



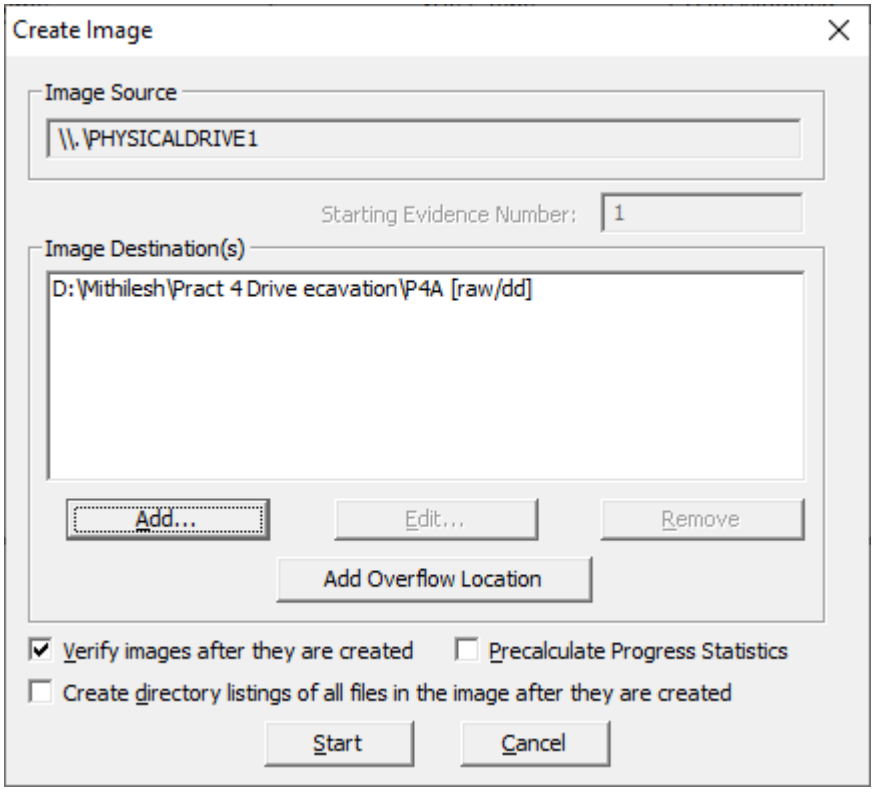
5. If your version of FTK regulates evidence information you can provide it. If you select raw(dd) format the image meta data will not be stored in the image file itself.



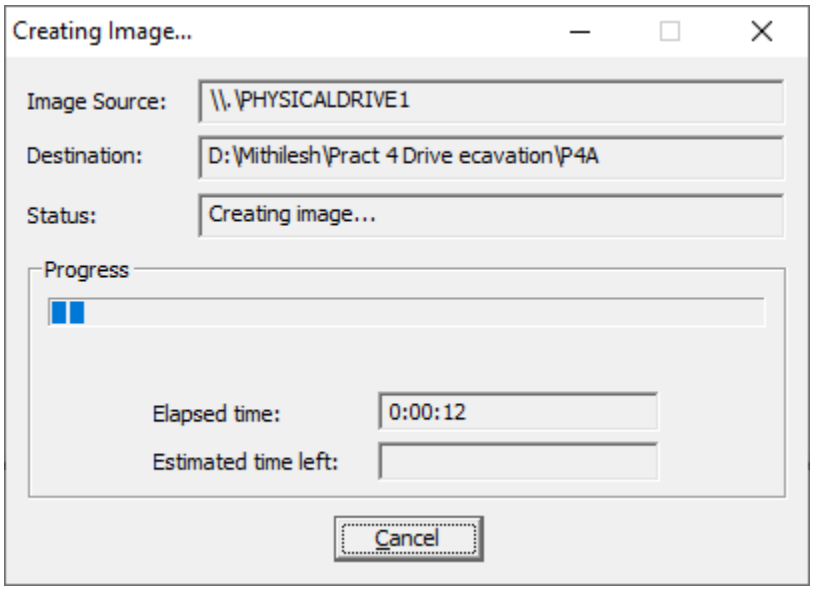
6. Select the image destination folder and file name. You can also set the maximum fragment size of image split files. Click finish to complete the wizard.



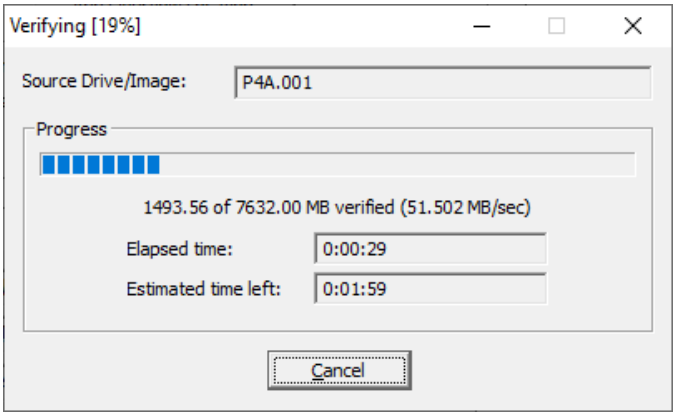
7. Click start to begin the acquisition



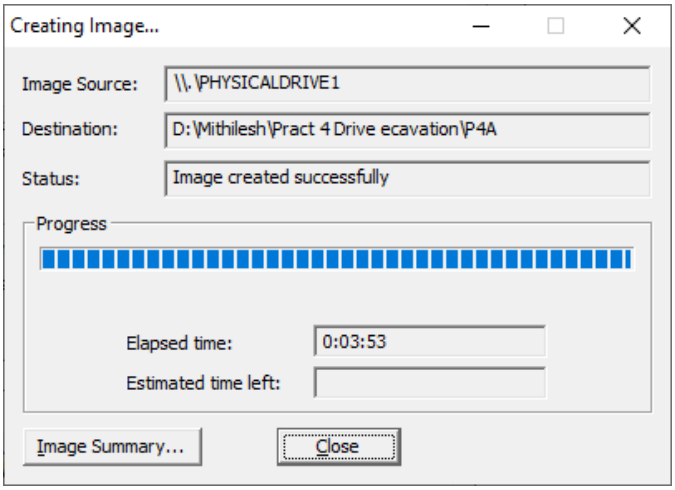
8. A program window will appear



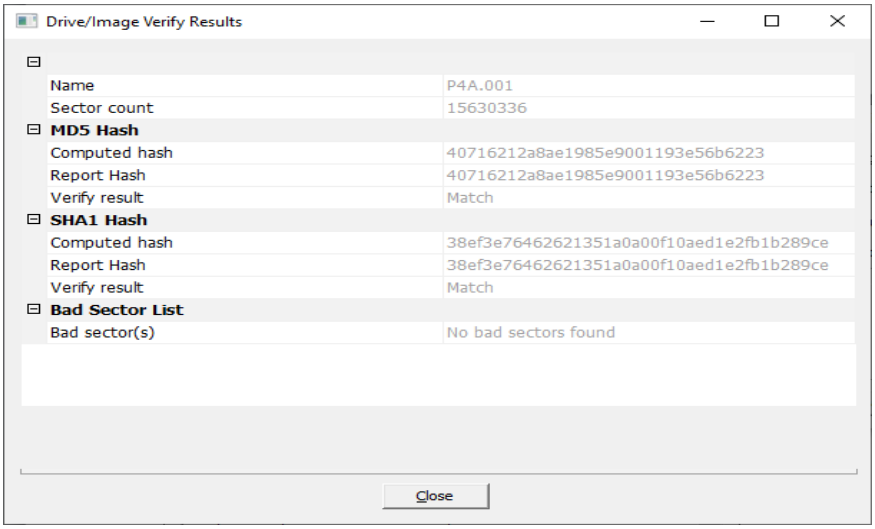
Verifying image



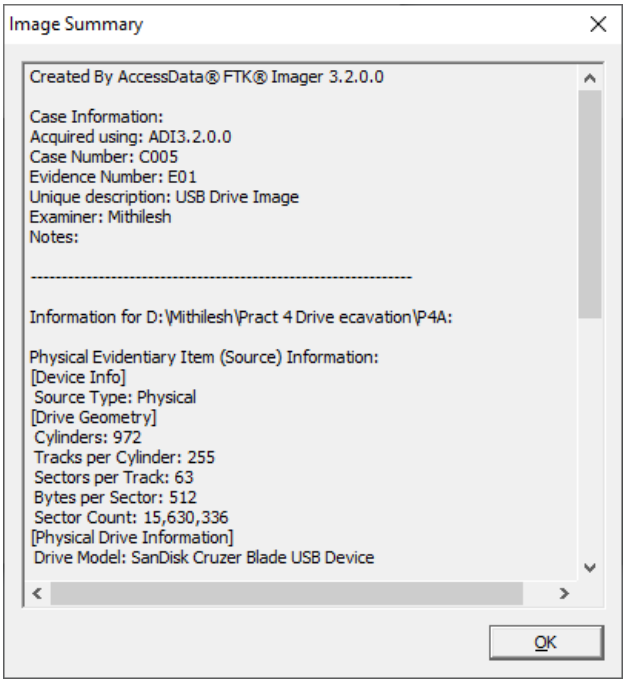
Process complete

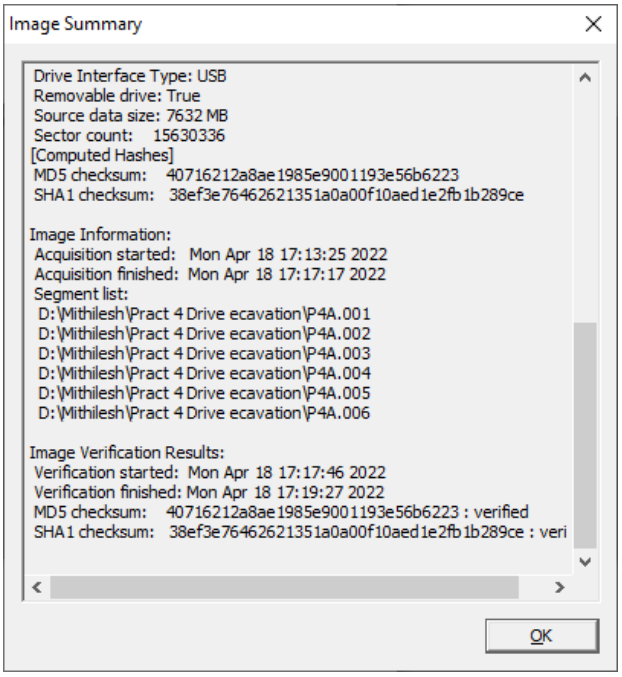


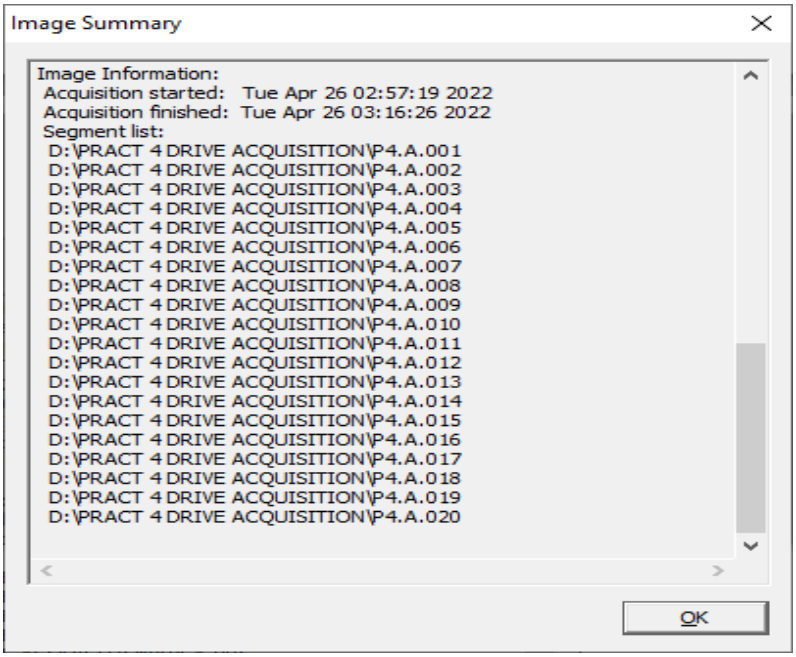
9. You can right click on the drive name to verify the image.



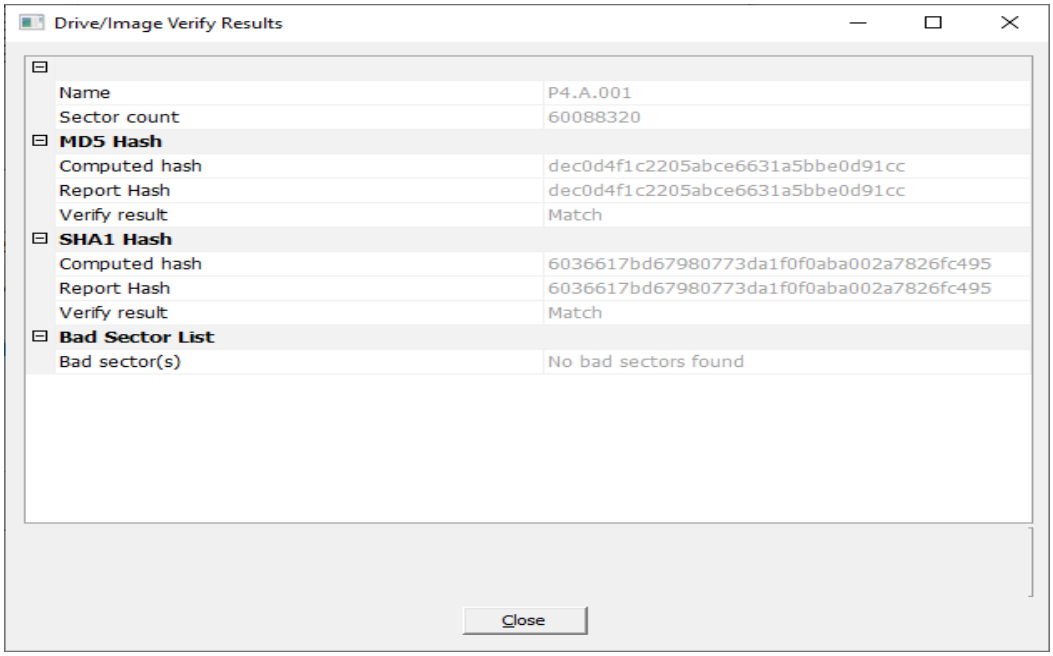
10. Once the acquisition is complete you can view an image summary and the drive will appear in the evidence list in the left hand side of main FTK imager window







Place where image drive is stored



10. FTK imager also creates a log of the acquisition process and places it in the same directory as the image-name.text. This file lists the evidence information details of the drive check sum and times the image acquisition started and finished.

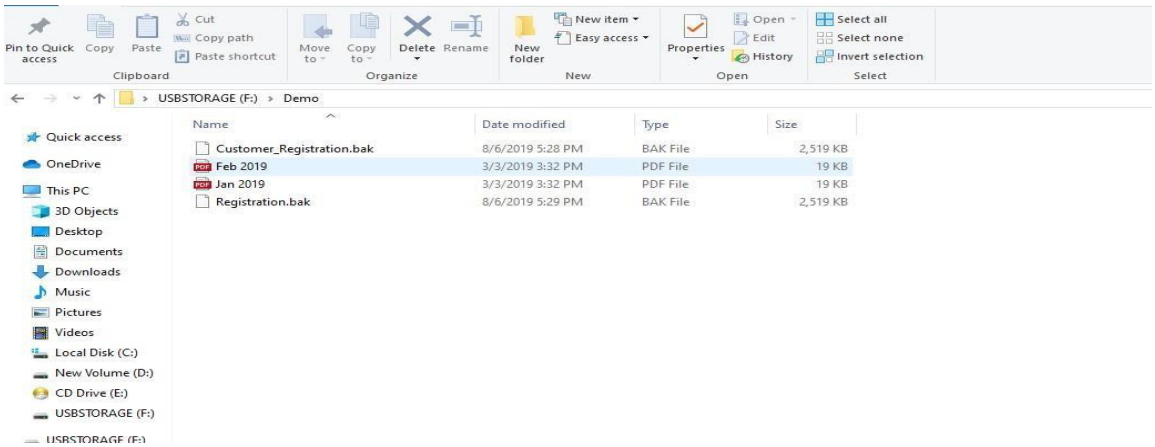
Practical No 4b

Aim: Recover Deleted files using Recuva, PC Inspector File Recovery.

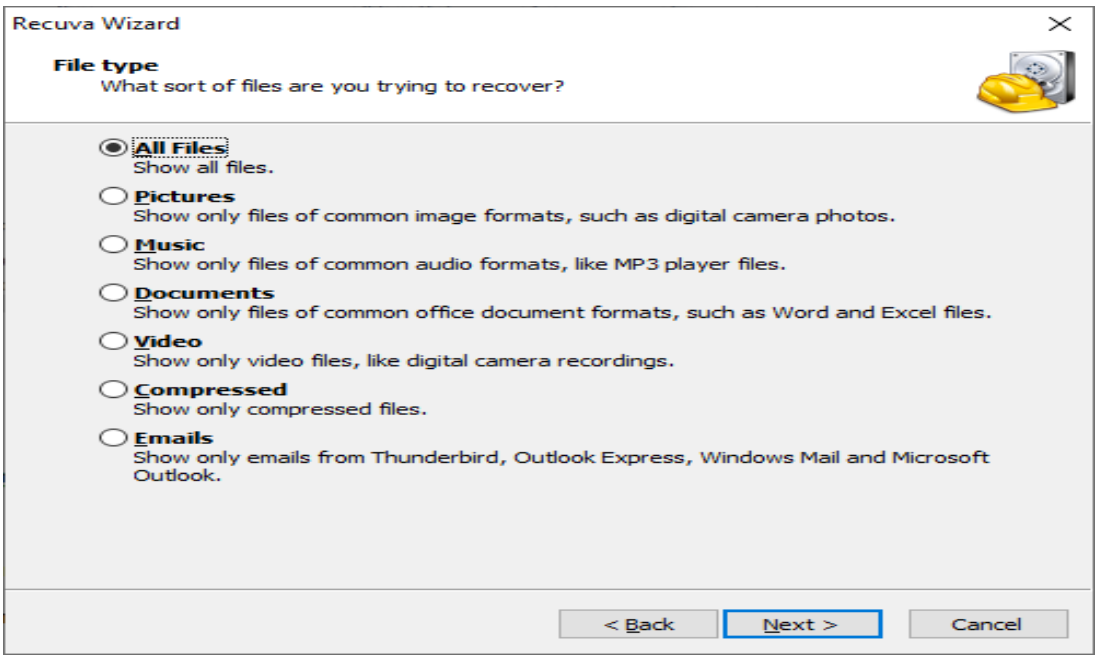
1. Using Recuva

Steps:

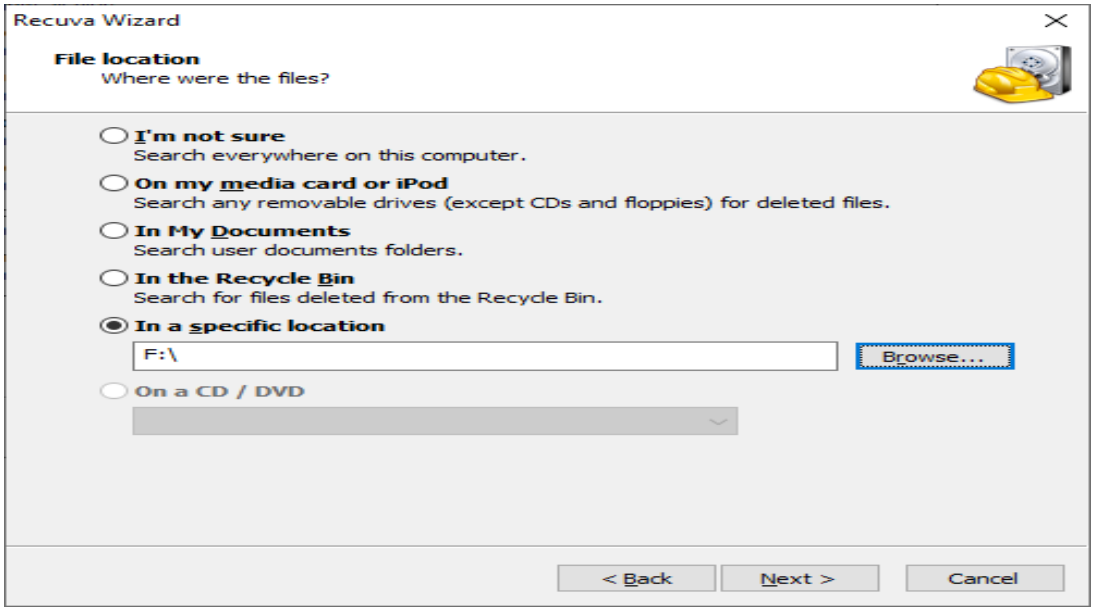
1. Create a folder named “demo” in a location and add few pictures and files {.docx, .xls, .txt} in it. Also delete the folder permanently.



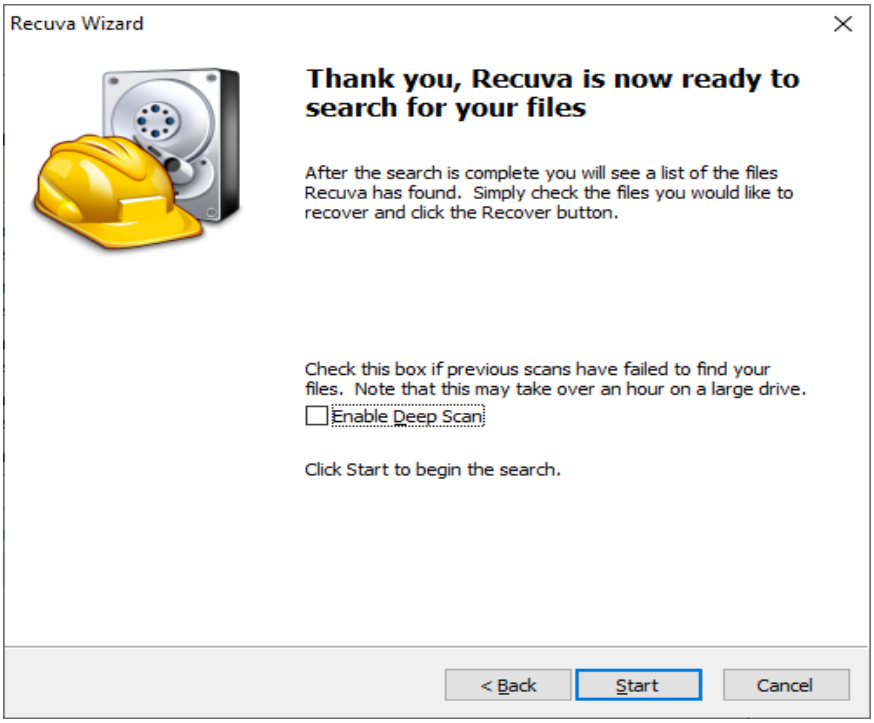
2. Run Recuva application. Select “All Files” option and click next.



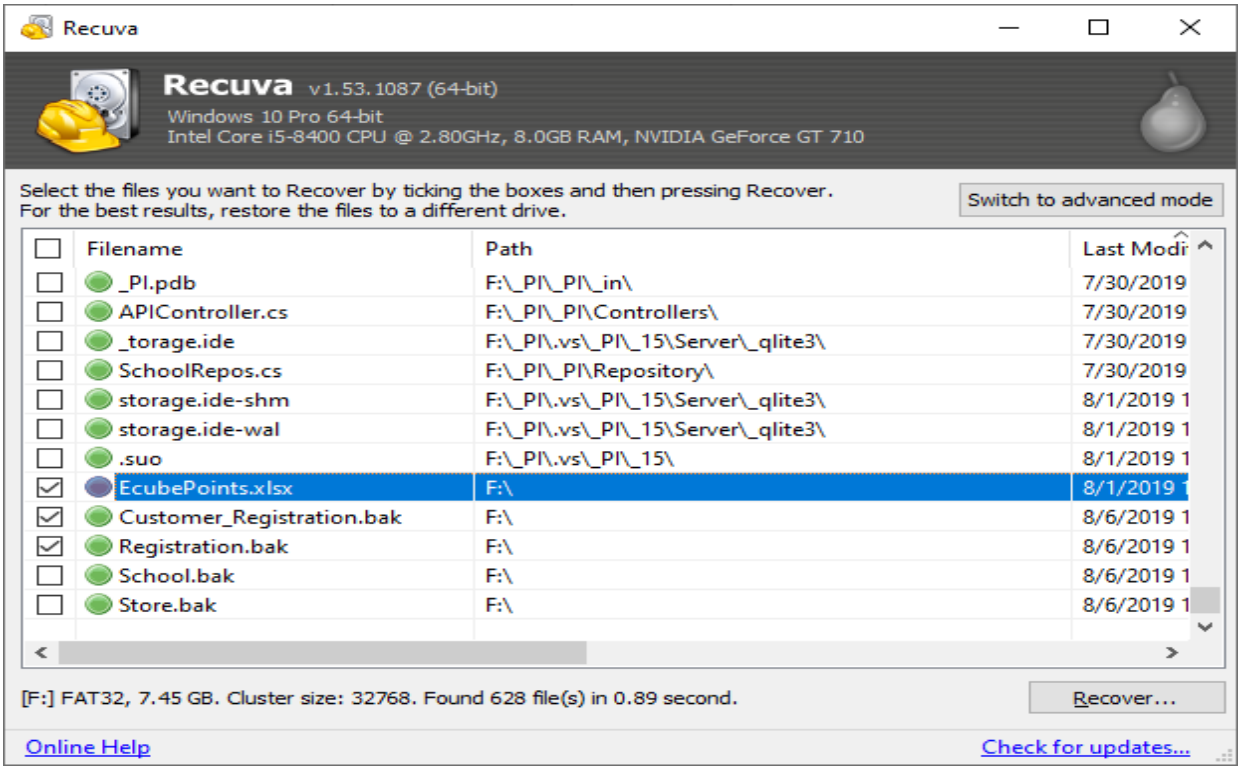
3. Select the location where the files were placed and click Next.



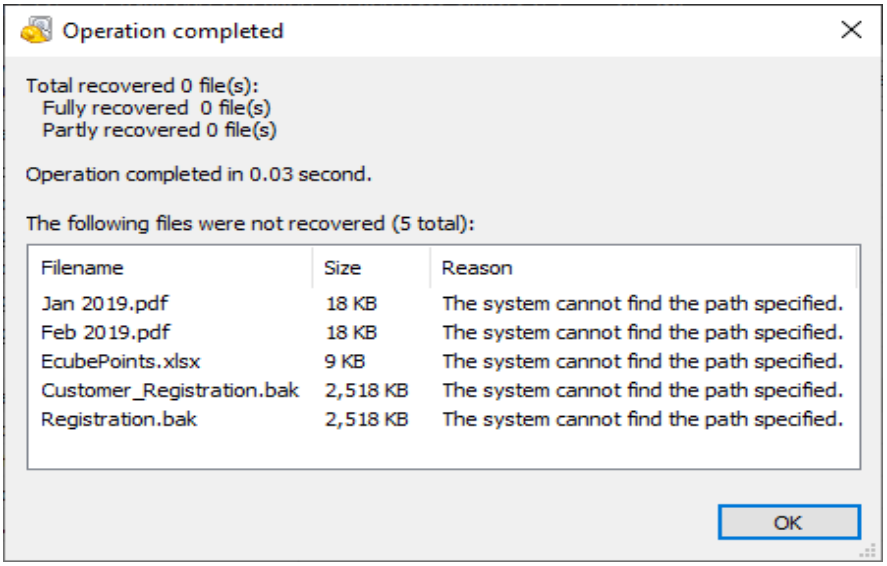
4. In Recuva is now ready to search files window. Click Start.



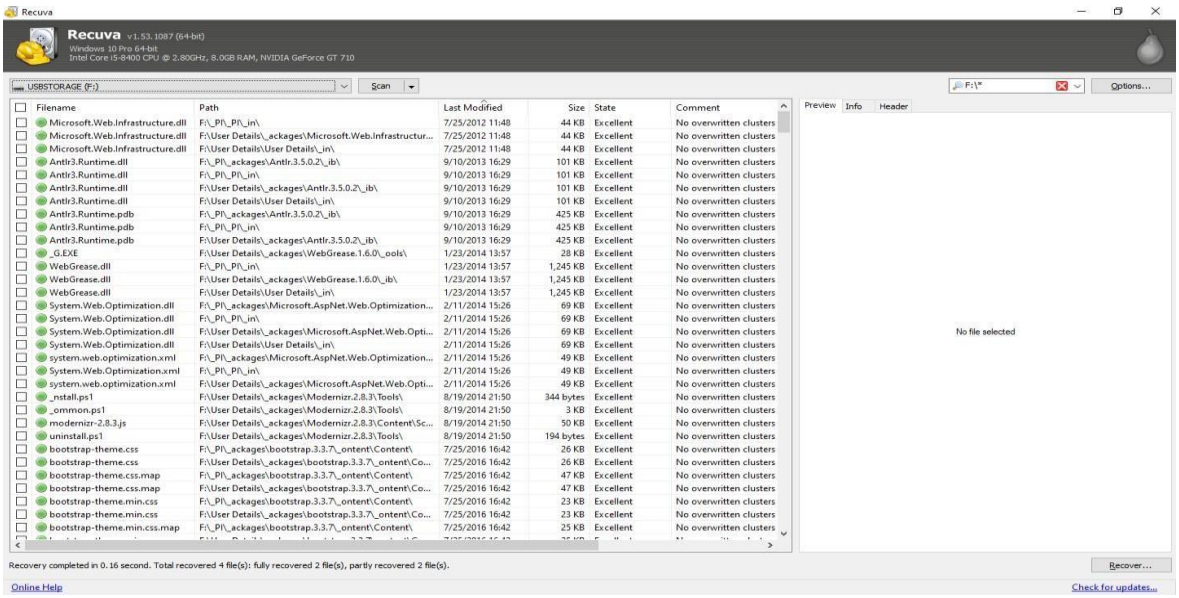
5. Recuva shows list of deleted files



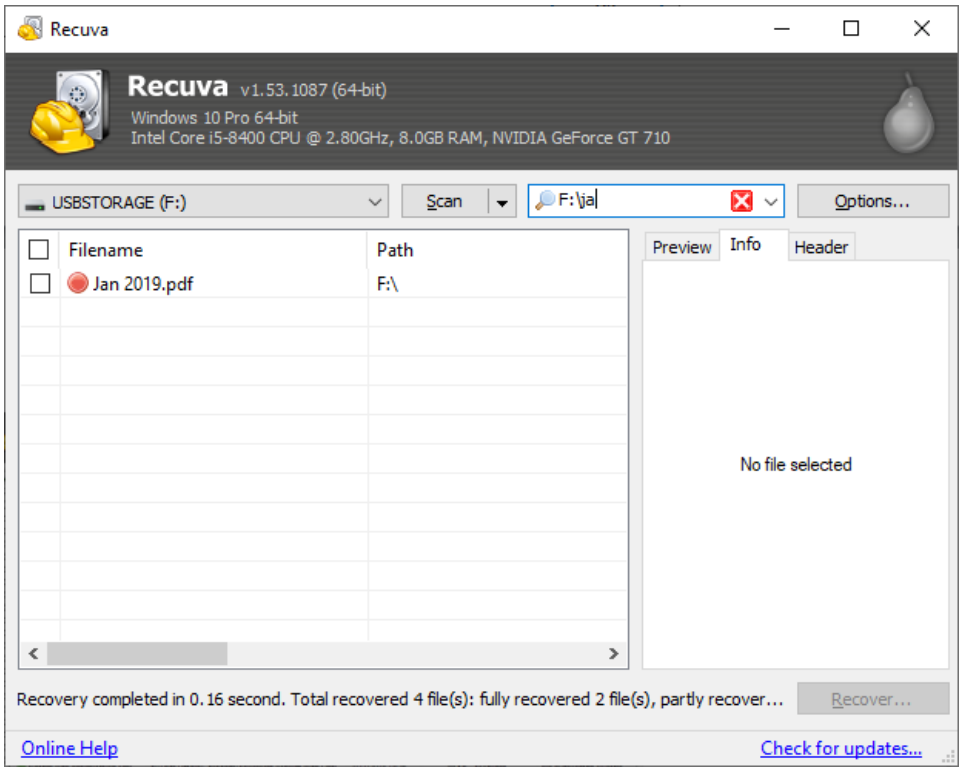
6. To recover any files, tick the check box and click on Recover button at bottom-right of the window.
7. It will ask to select the location where recovered data is to be stored. Click OK. The data will be recovered to that location.



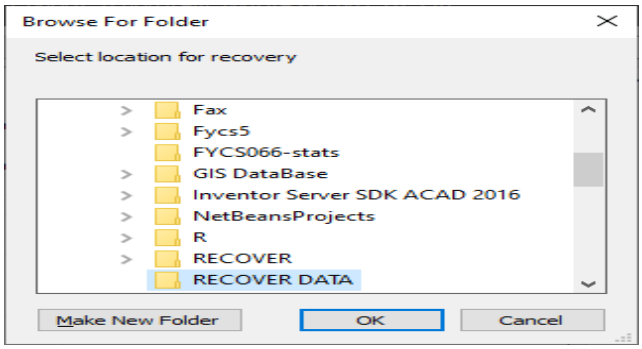
8. To search a file by file name, click on “Switch to advanced mode” option on top-right of the window.

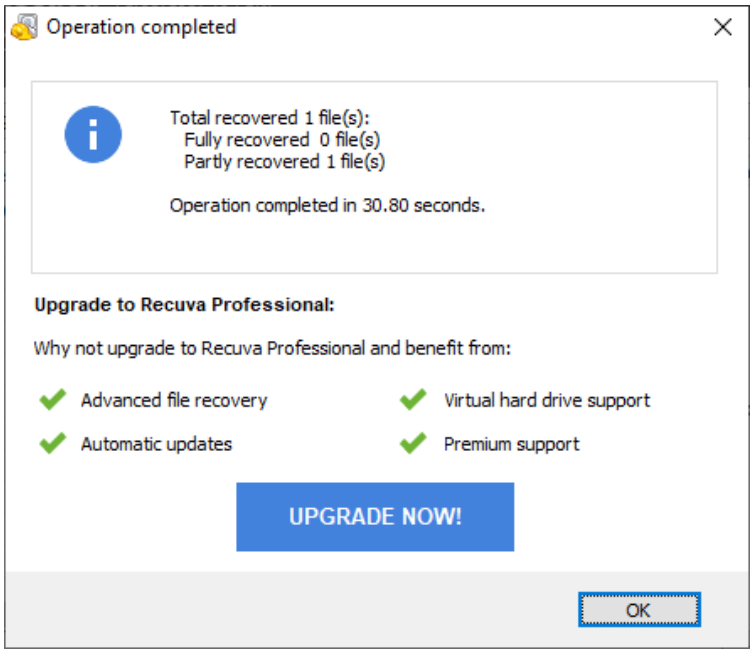


9. Search can be made by typing file name or initials, tick the check box and click on Recover.



10. Again, select the location where recovered data is to be stored. Click OK. The data will berecovered to that location.



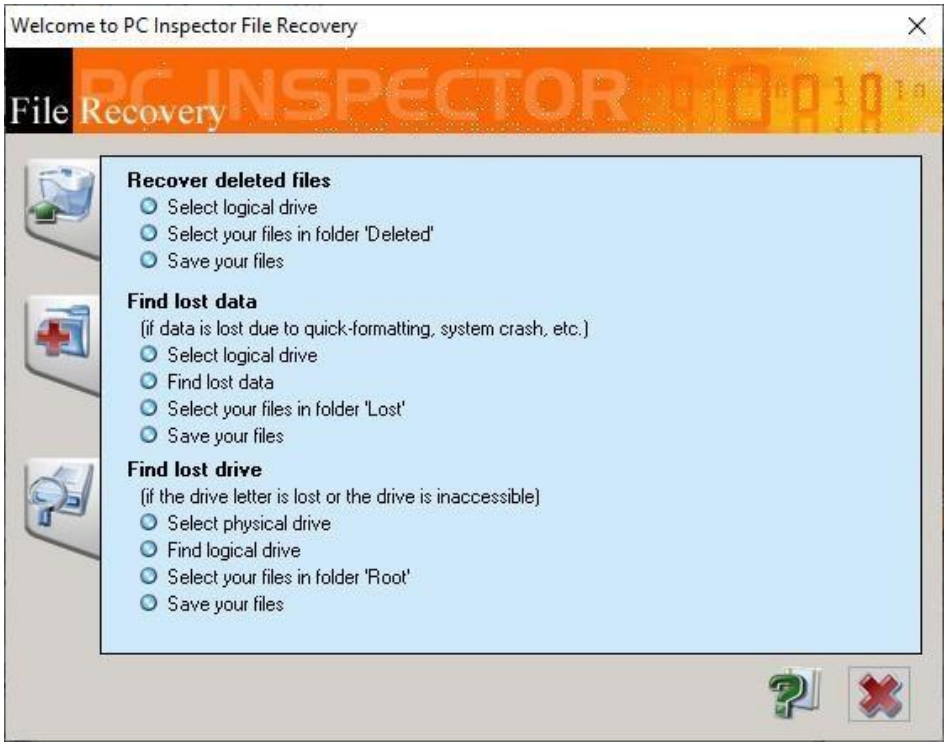


II. Using PC Inspector File Recovery

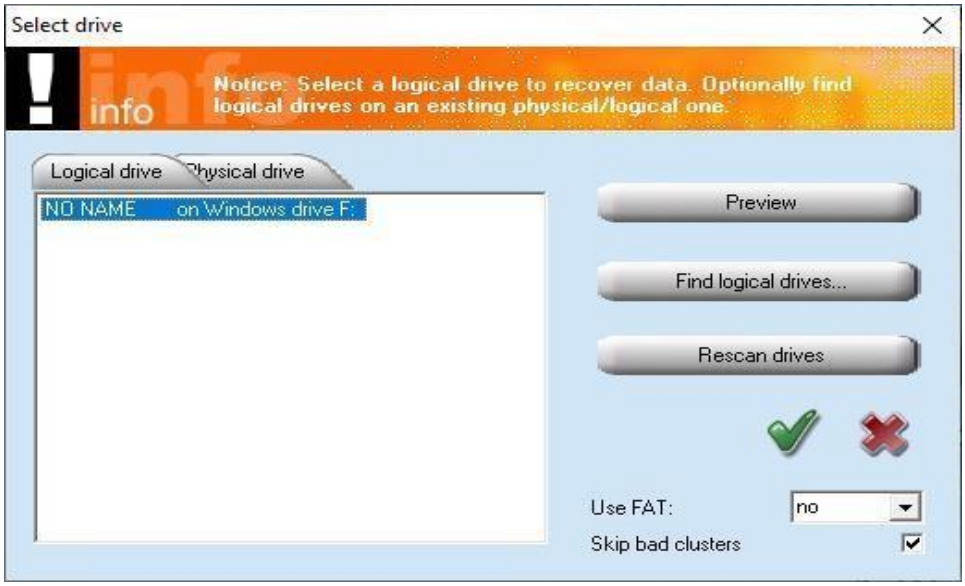
Steps:

1. Run PC Inspector Recovery tool. Select language English and click on Green tick mark

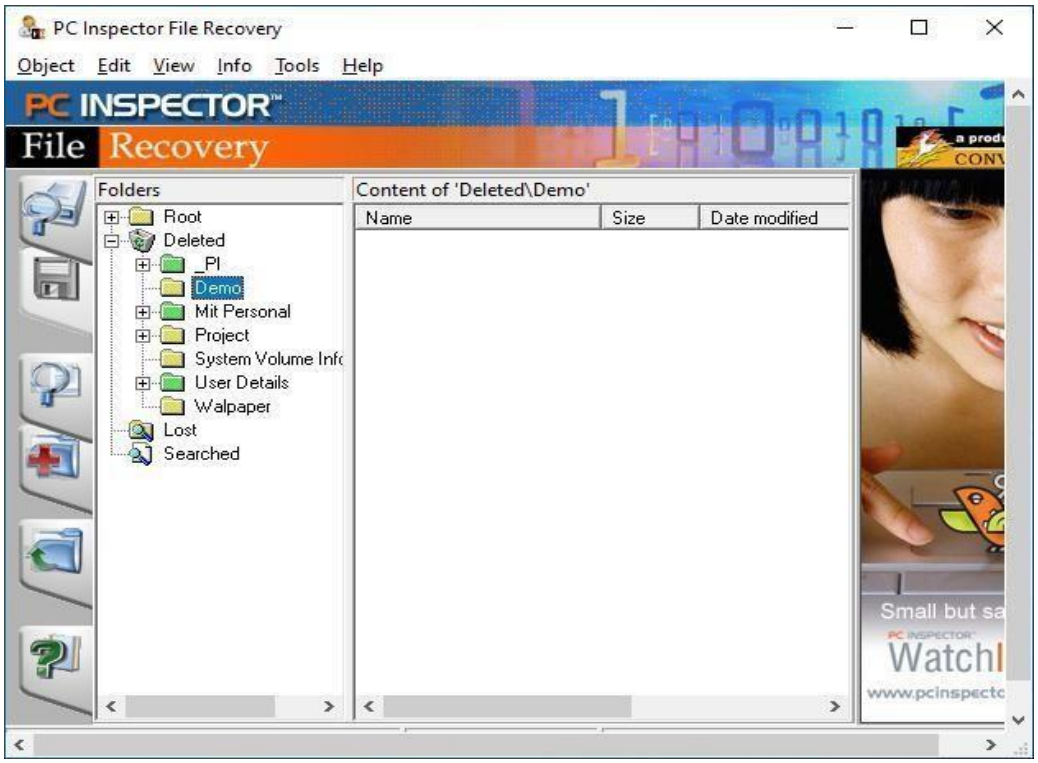
2. Click on button next to recover deleted files.



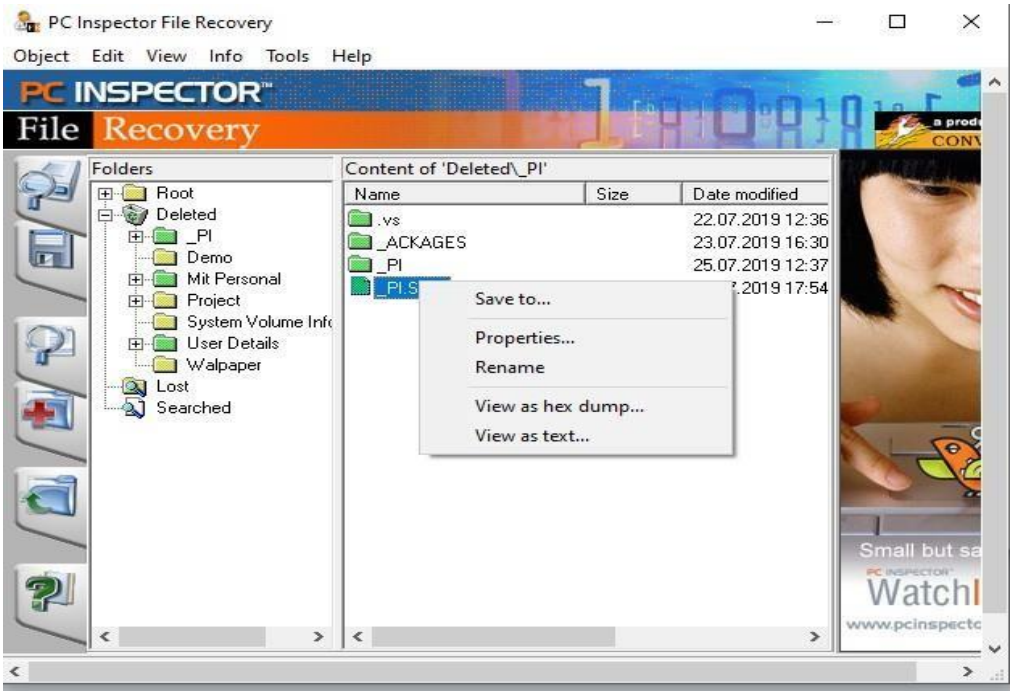
3. On logical drive tab, select the drive and click on Green tick mark.



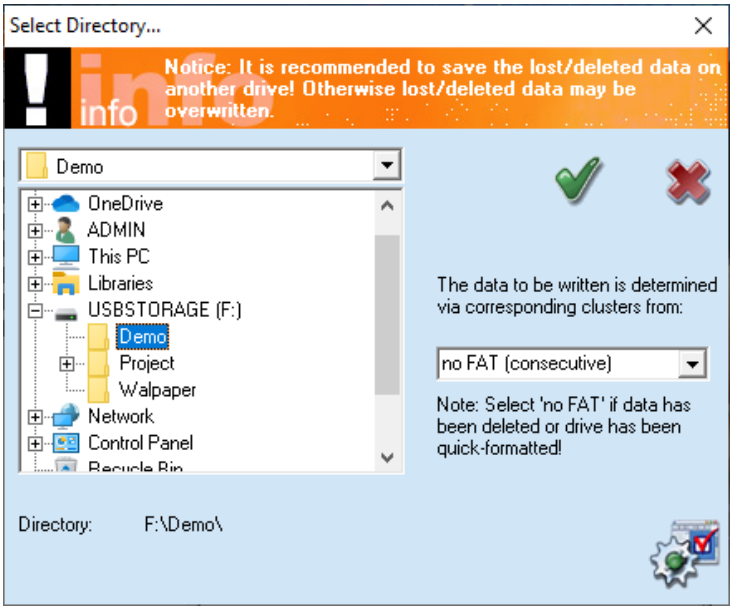
4. It will show the list of deleted files in the drive. You can browse various folders on that drive.



5. To recover a file, select the file, right-click on it and choose “Save to



6. Select the location where the file has to be saved and click on Green tick mark.



7. The file will be recovered to that location.

III. Using Recover My Files

Steps:

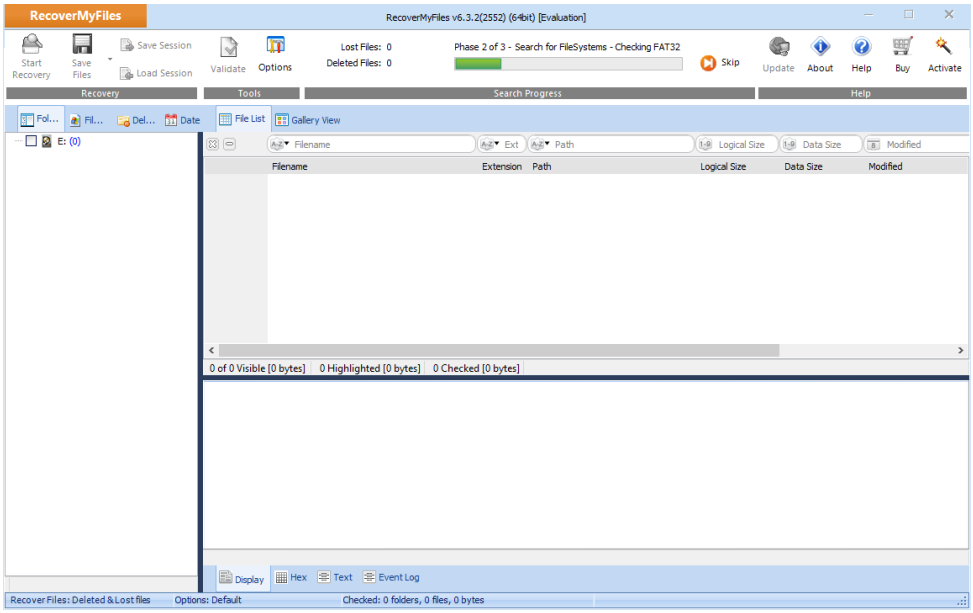
1. Run the tool, select Recover Files and click on Next.

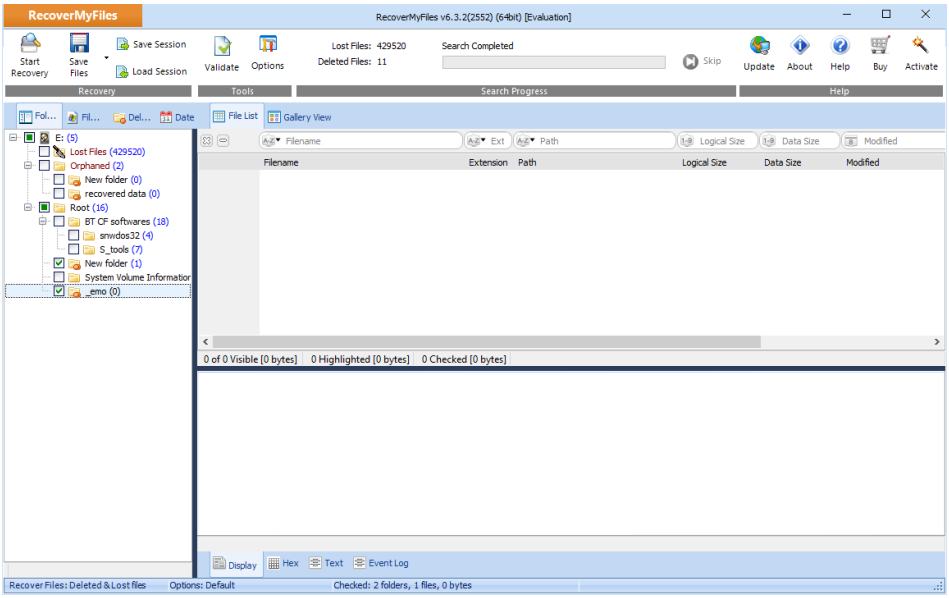
2. Select the drive to search and recover files and click Next.

3. Select option Search for deleted files, then search for selected lost file types and click Next

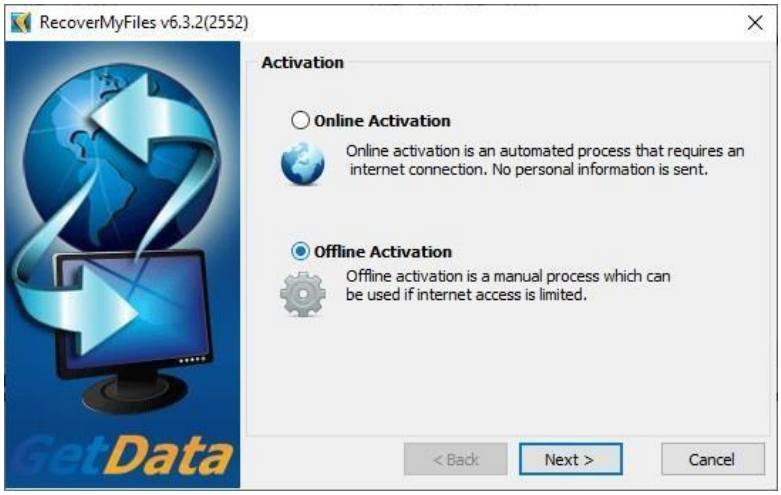
4. Select file headers- type of file to search tick mark on check box and click on Start.

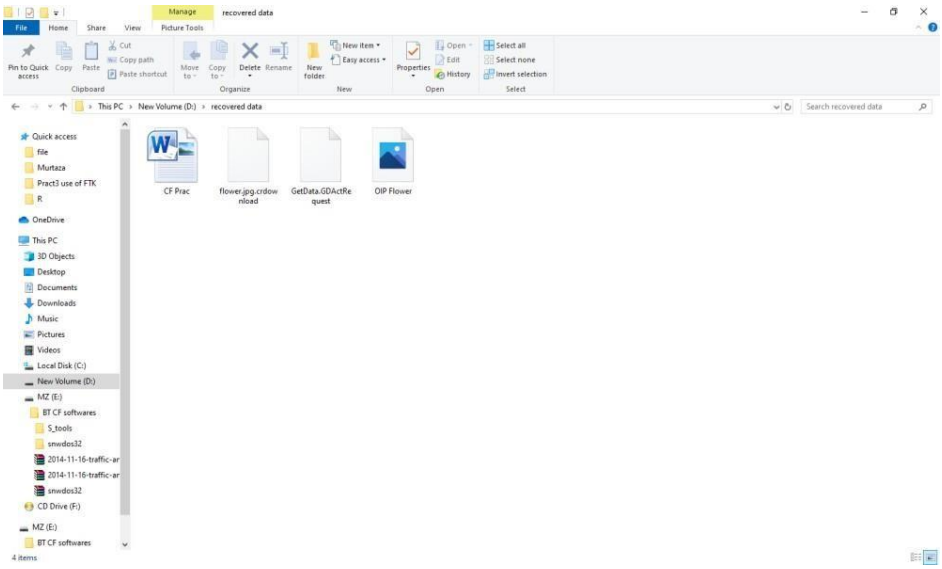
5. The search will begin in 3 phases. Select the file to recover and click on Save Files button on top-left





6. Select offline activation and click Next.





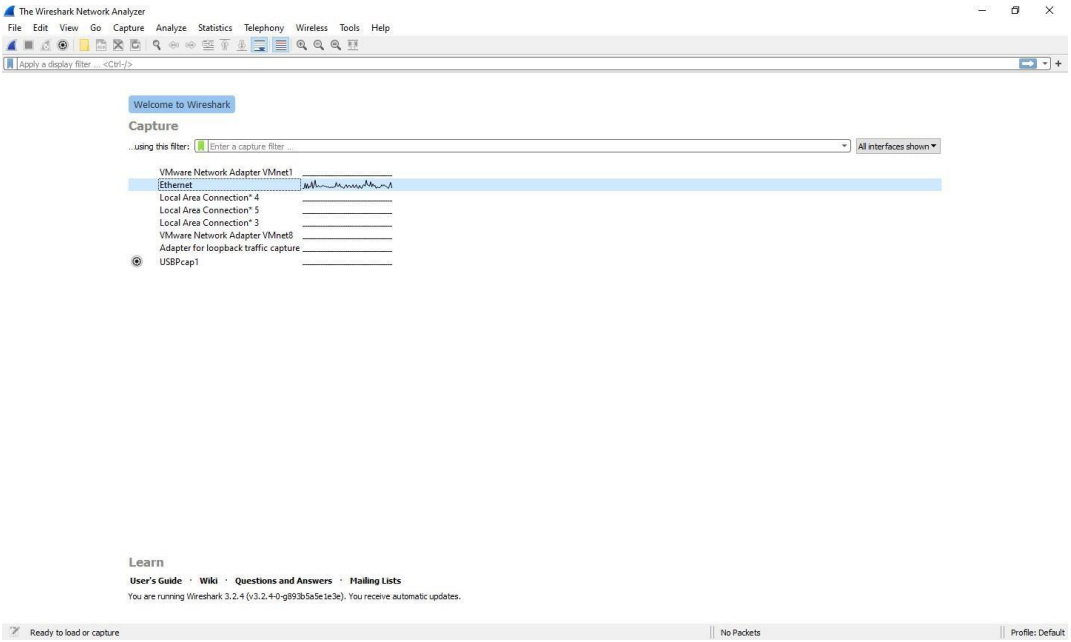
Practical No 5: Using Log & Traffic Capturing & Analysis Tools [WireShark]

Aim: Using Log & Traffic Capturing & Analysis Tools [WireShark]

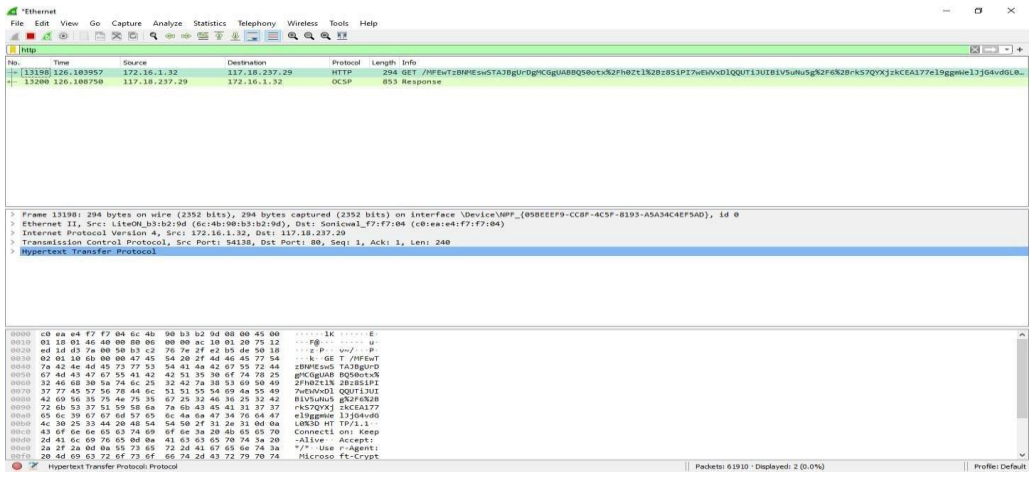
Steps:

Filtering Packets

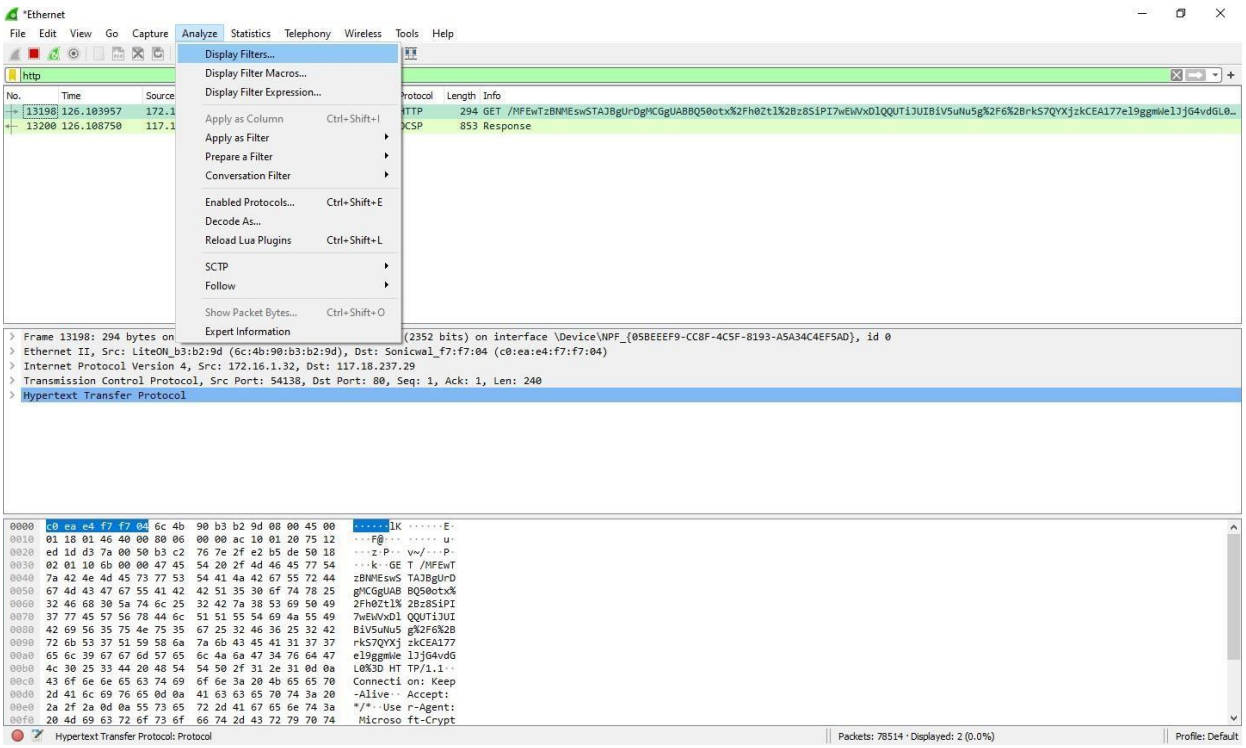
1. Start Wireshark



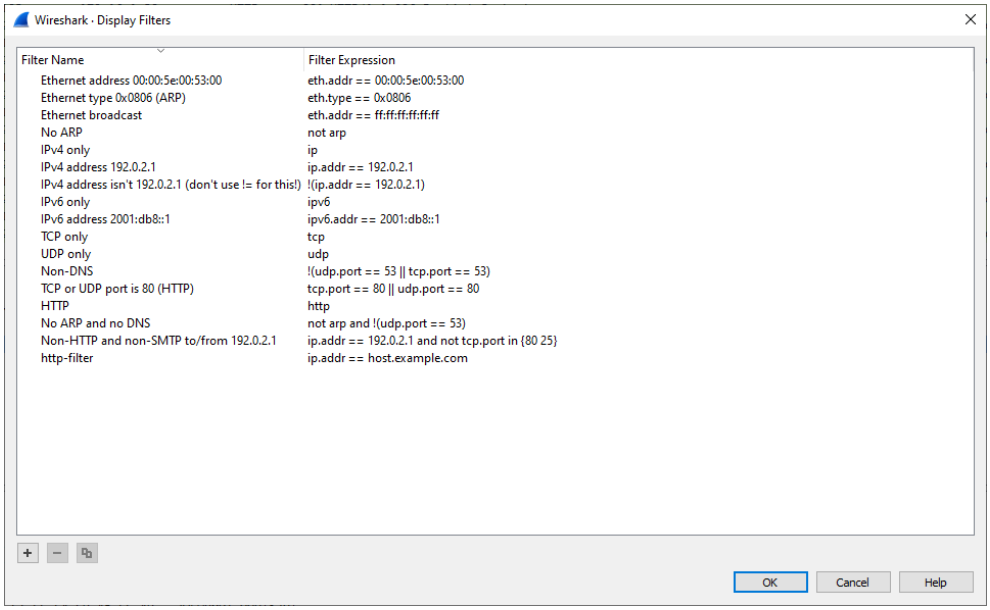
2. Click on Interface List. Create Interfaces window appears. Check on all the checkboxes. Click on Start



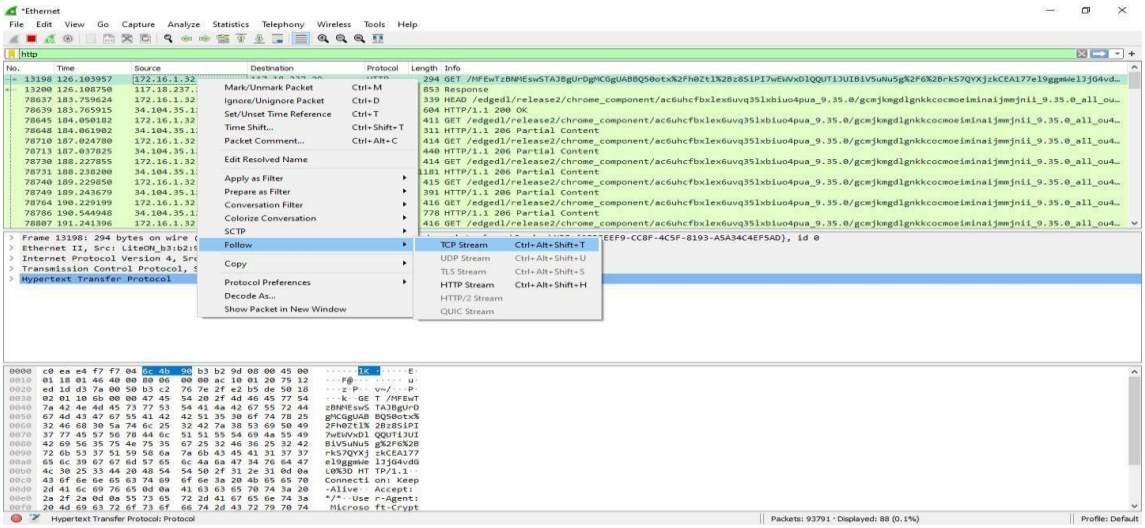
3. In the filter box, type http and enter. You will see all the http packets.
4. To create a new filter, click on Analyze menu and select Display Filters



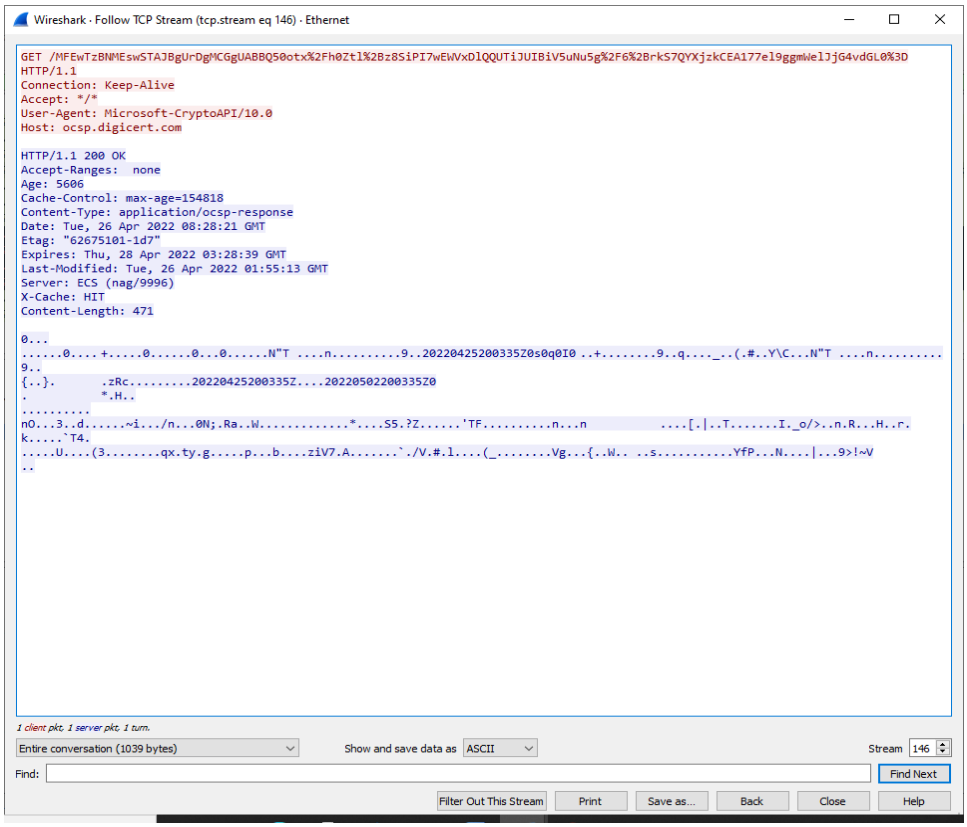
5. Enter the name for the new filter as 'HTTPfilter'. Click on Apply and then. OK



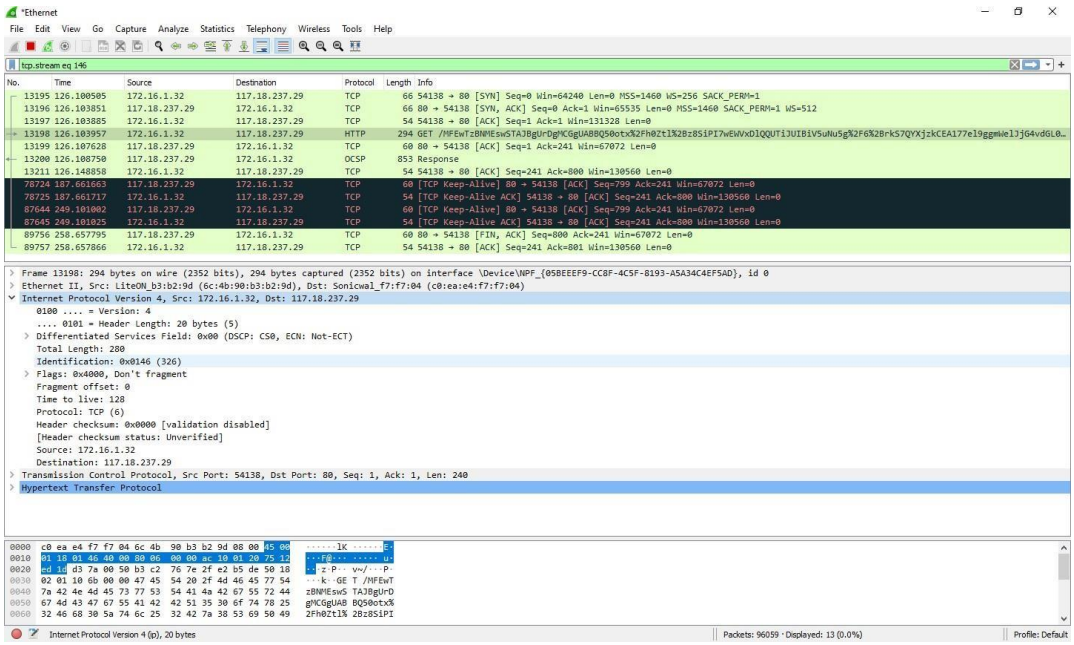
6. Right-click on HTTP packet and select Follow UDP Stream



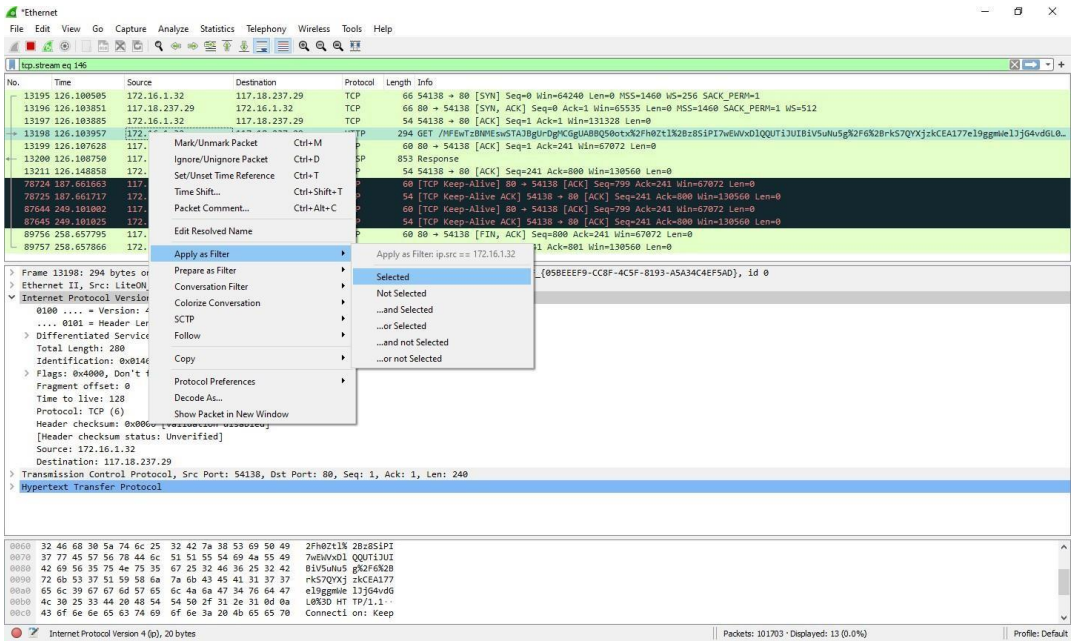
7. You will see full conversation between client and server.

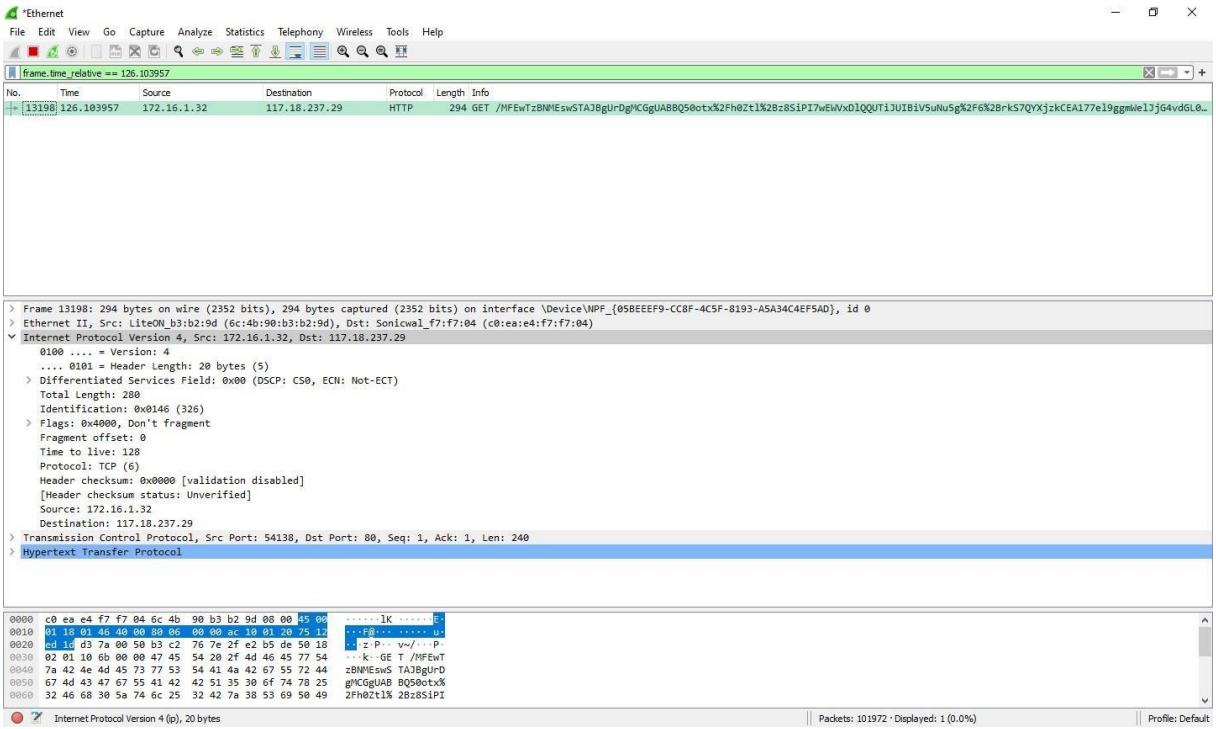


8. Inspecting Packets. Click a packet to select it and you can dig down to view its details



9. To create a filter from here, right-click and select Apply as Filter submenu and then select Selected. You can see direct filter is applied on frame.




*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
frame.time_relative == 126.103957
No. Time Source Destination Protocol Length Info
13198 126.103957 172.16.1.32 117.18.237.29 HTTP 294 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEA177el9ggmWelJjG4vdGL0…
Frame 13198: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface \Device\NPF_{05BEEEF9-CC8F-4C5F-8193-A5A34C4EF5AD}, id 0
Ethernet II, Src: LiteON_b3:b2:9d (6c:4b:90:b3:b2:9d), Dst: Sonicwal_f7:f7:04 (c0:ea:e4:f7:f7:04)
Internet Protocol Version 4, Src: 172.16.1.32, Dst: 117.18.237.29
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 280
Identification: 0x0146 (326)
Flags: 0x4000, Don't fragment
Fragment offset: 0
Time to live: 128
Protocol: TCP (6)
Header checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source: 172.16.1.32
Destination: 117.18.237.29
Transmission Control Protocol, Src Port: 54138, Dst Port: 80, Seq: 1, Ack: 1, Len: 240
Hypertext Transfer Protocol
0000 c0 ea e4 f7 f7 04 6c 4b 90 b3 b2 9d 08 00 45 00
0010 01 18 01 46 40 00 80 06 00 00 ac 10 01 20 75 12
0020 ed 1d d3 7a 00 50 b3 c2 76 7e 2f e2 b5 de 50 18
0030 02 01 10 6b 00 00 47 45 54 20 2f 4d 46 45 77 54
0040 7a 42 4e 4d 45 73 77 53 54 41 4a 42 67 55 72 44
0050 67 4d 43 47 67 55 41 42 42 51 35 30 6f 74 78 25
0060 32 46 68 30 5a 74 6c 25 32 42 7a 38 53 69 50 49
Internet Protocol Version 4 (ip), 20 bytes
Packets: 101972 · Displayed: 1 (0.0%)
Profile: Default

PRACTICAL NO: 06

AIM: Dump memory contains using Pmdump.

Step 1: Download pmdump and run it.

```
C:\Users\Kartika>d:

D:\>cd mn cf
The system cannot find the path specified.

D:\>cd "CF softwares BT"

D:\CF softwares BT>pmdump

pmdump 1.4 - Copyright (c) 2019, Arne Vidstrom
           - https://vidstromlabs.com/freetools/pmdump/

Usage: pmdump <pid> <filename>

        - dumps the process memory contents to a file

       pmdump <pid> <filename> -full

        - dumps the process memory contents to a file with holes included and
          zero filled

       pmdump -list

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

Step 2: Use pmdump -list command to list the running process.

```
D:\CF softwares BT>pmdump -list
```

Step 3: select any process to see its content.

Step 4: use the process id and using pmdump command and store it in a file name dump.txt

```
28676 - CodeMeter.exe
30064 - RecoverMyFiles.exe
31488 - SystemSettingsBroker.exe
27704 - msedge.exe
30020 - msedge.exe
 8020 - msedge.exe
27568 - msedge.exe
15348 - msedge.exe
21520 - msedge.exe
31480 - msedge.exe
21788 - wlanext.exe
 3280 - conhost.exe
25548 - QcShm.exe
 3512 - backgroundTaskHost.exe
23100 - smartscreen.exe
24208 - RuntimeBroker.exe
 6636 - cmd.exe
16900 - conhost.exe
24712 - OpenConsole.exe
25152 - WindowsTerminal.exe
30880 - WmiPrvSE.exe
12708 - pmdump.exe

D:\CF softwares BT>pmdump 7572 >> dump.txt
```

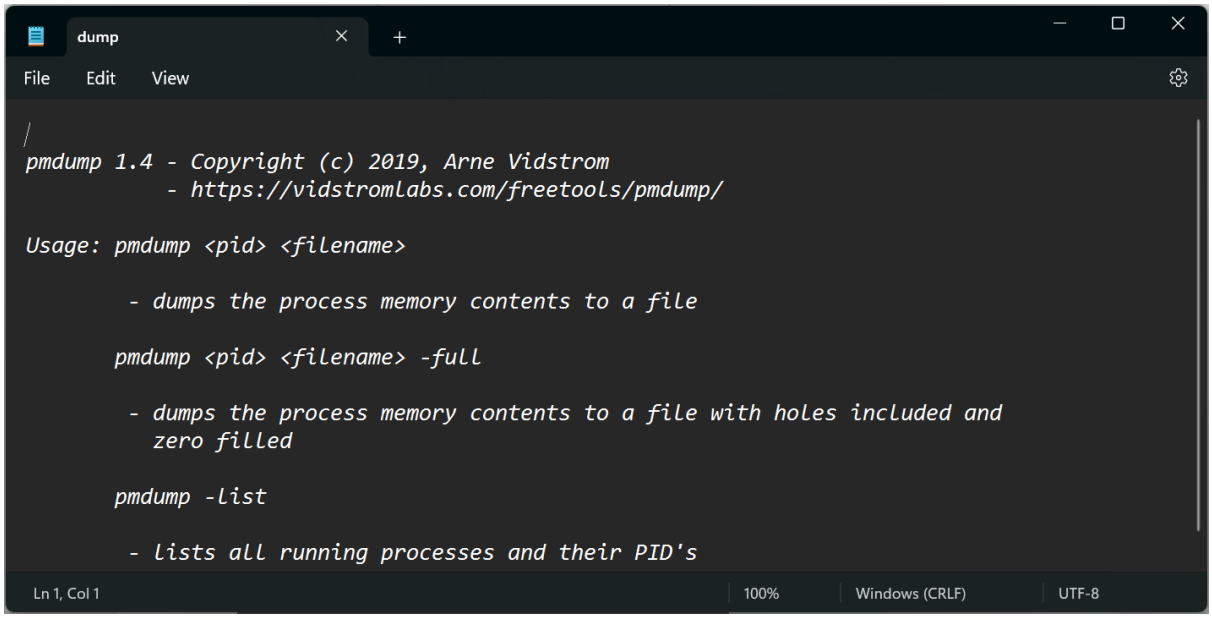
Step 5: Use dir command to check file dump.txt is created.

```
D:\CF softwares BT>dir
 Volume in drive D is Data
 Volume Serial Number is 9204-F7D8

 Directory of D:\CF softwares BT

31-05-2023  10:13    <DIR>          .
03-06-2021  20:08           844,464 2014-11-16-traffic-analysis-exercise-answers.pdf.zip
03-06-2021  20:08         2,132,438 2014-11-16-traffic-analysis-exercise.pcap.zip
05-06-2021  09:16                20 abc.txt
05-06-2021  10:36                20 Abc123
30-01-2015  14:31        35,910,816 AccessData FTK Imager3-2-0.exe
21-03-2015  17:37       301,125,632 autopsy-3.1.2-64bit (1).msi
25-05-2023  12:11           271,360 backup.pst
25-05-2023  15:41         8,234,800 cain_and_abel_for_Windows.zip
31-05-2023  07:26    <DIR>          dump
31-05-2023  10:13               422 dump.txt
22-03-2015  10:44       120,147,968 ef_setup_6196_english.exe
31-05-2023  08:32    <DIR>          files
21-03-2015  19:13        36,999,639 ftk181.exe
25-04-2022  19:47       143,683,244 hello.pcapng
05-06-2021  10:34                 0 hidden
```

Step 6: Open the file using notepad dump.txt command to view it.

```
D:\CF softwares BT>notepad dump.txt
```

Step 7: File dump.txt is as shown below.

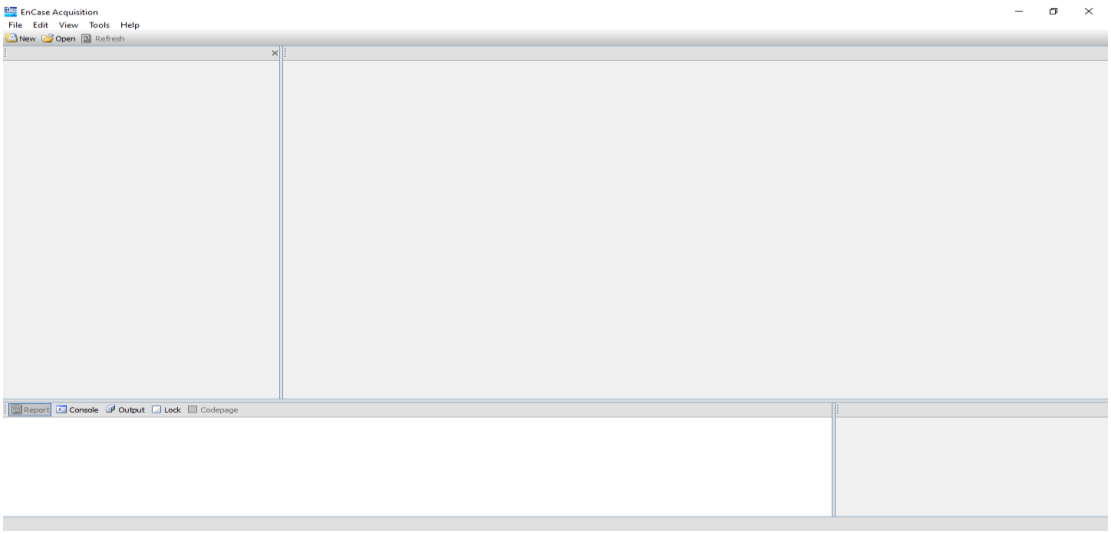


Practical No :7

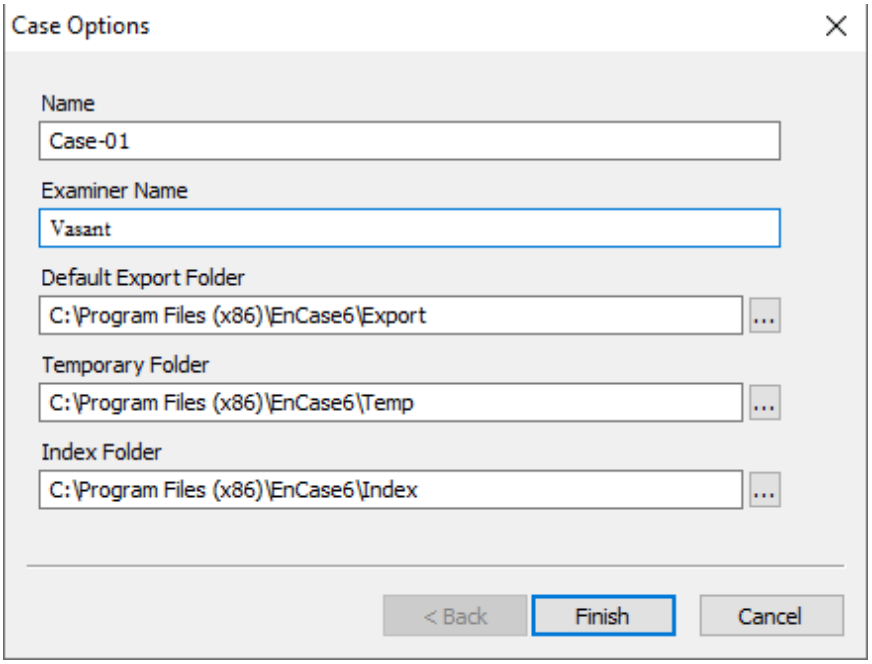
Aim: Forensic Investigation Using Encase.

Steps:

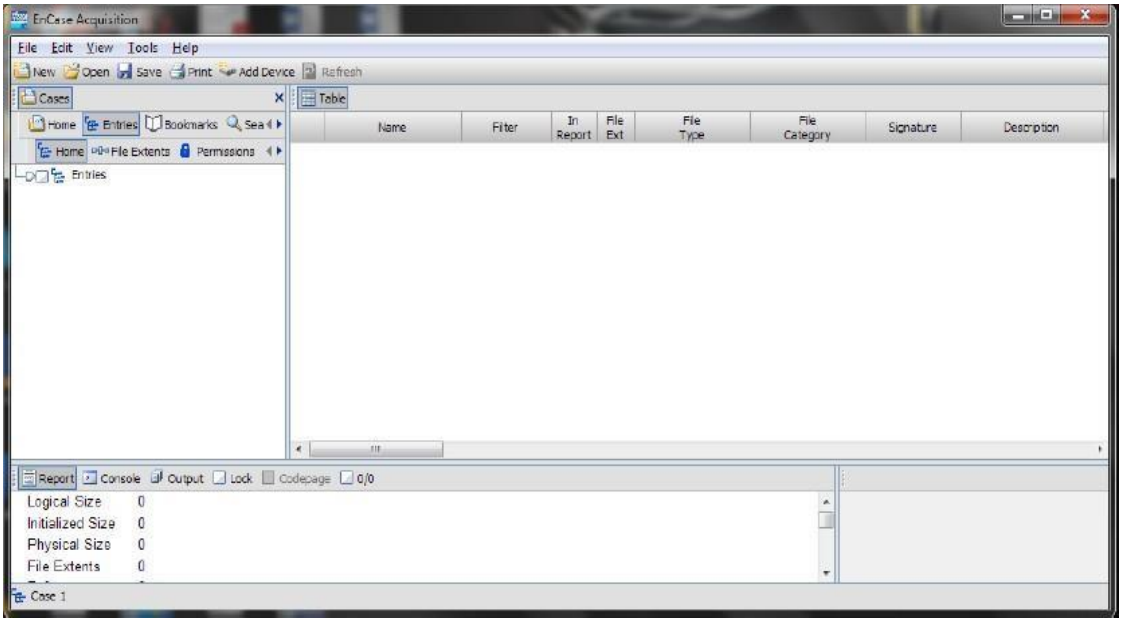
1. Open the Encase software tool.



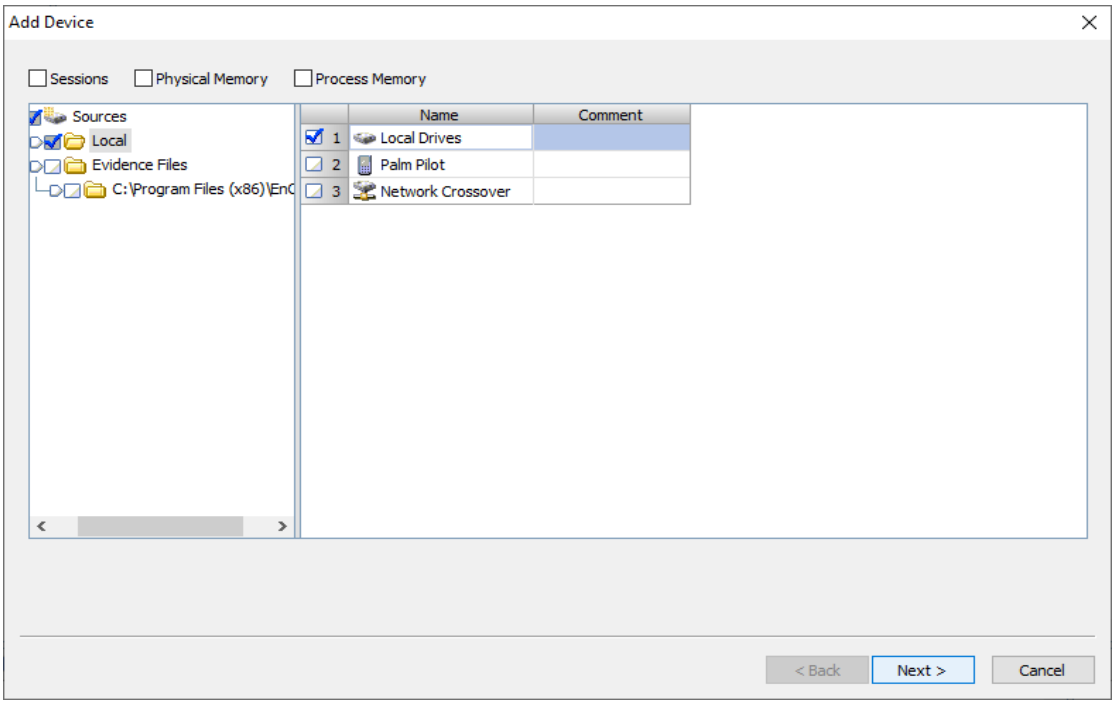
2. Click on New and enter the name and click on Finish.



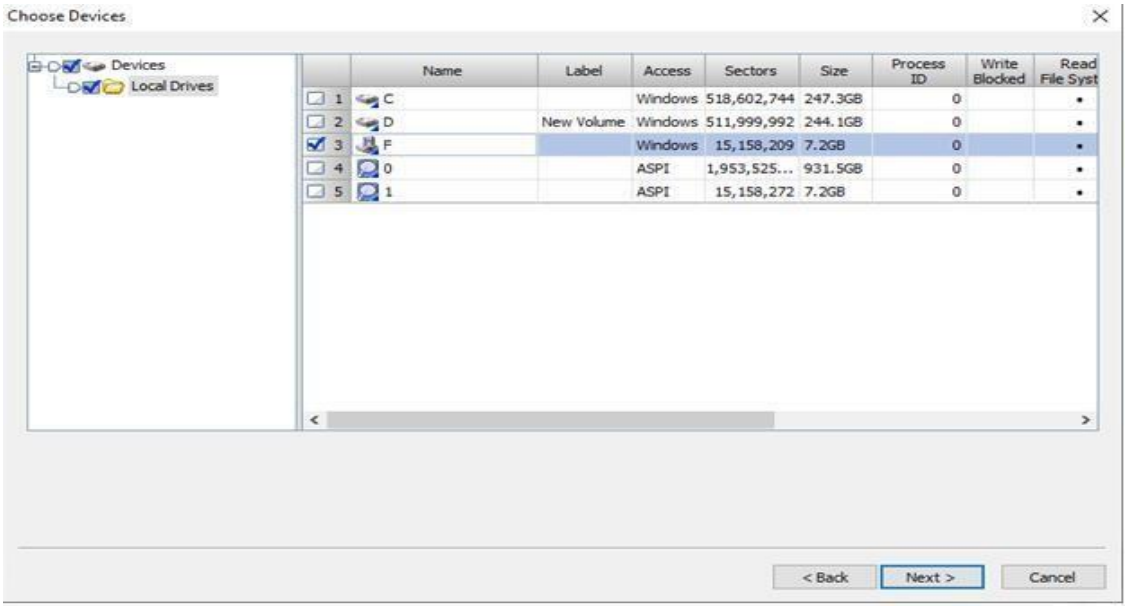
3. Check the left pane



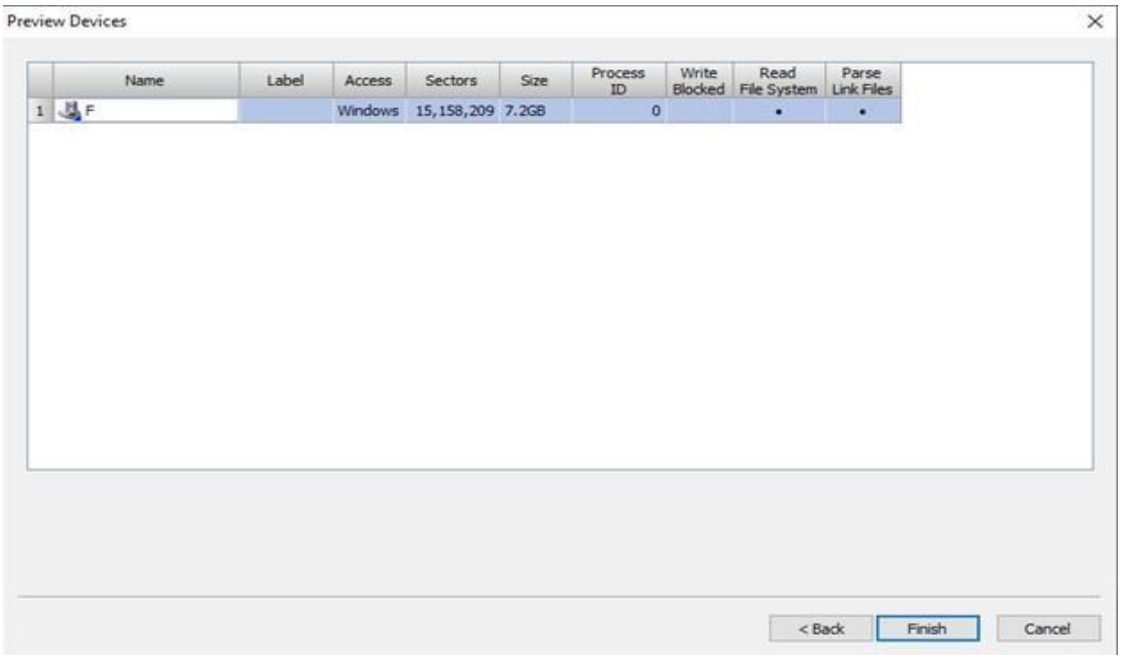
4. Click on Add Device and select “Local Drives” and click Next



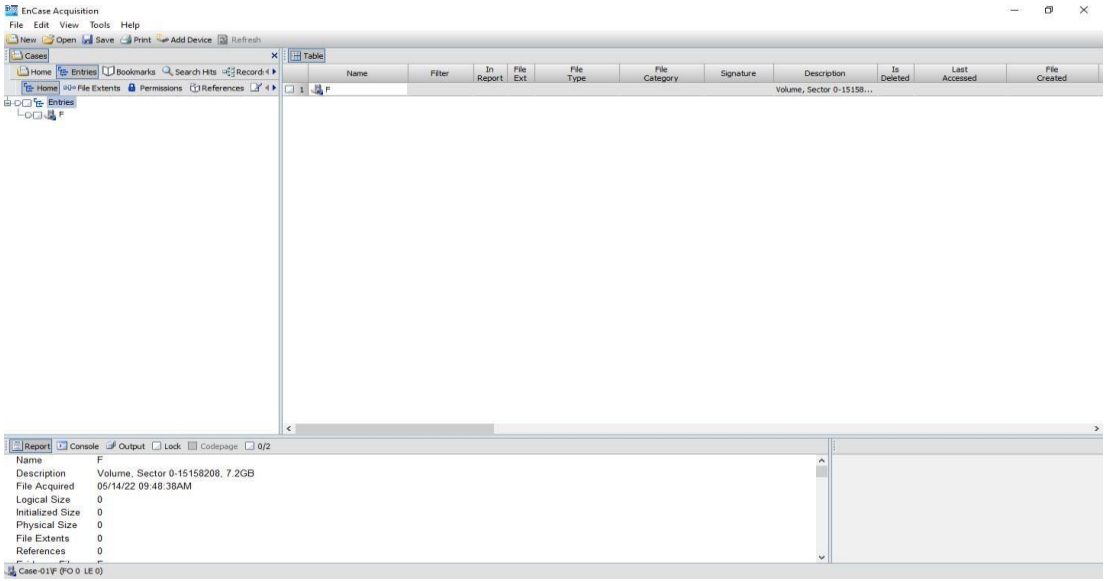
5. Choose a device and click Next.



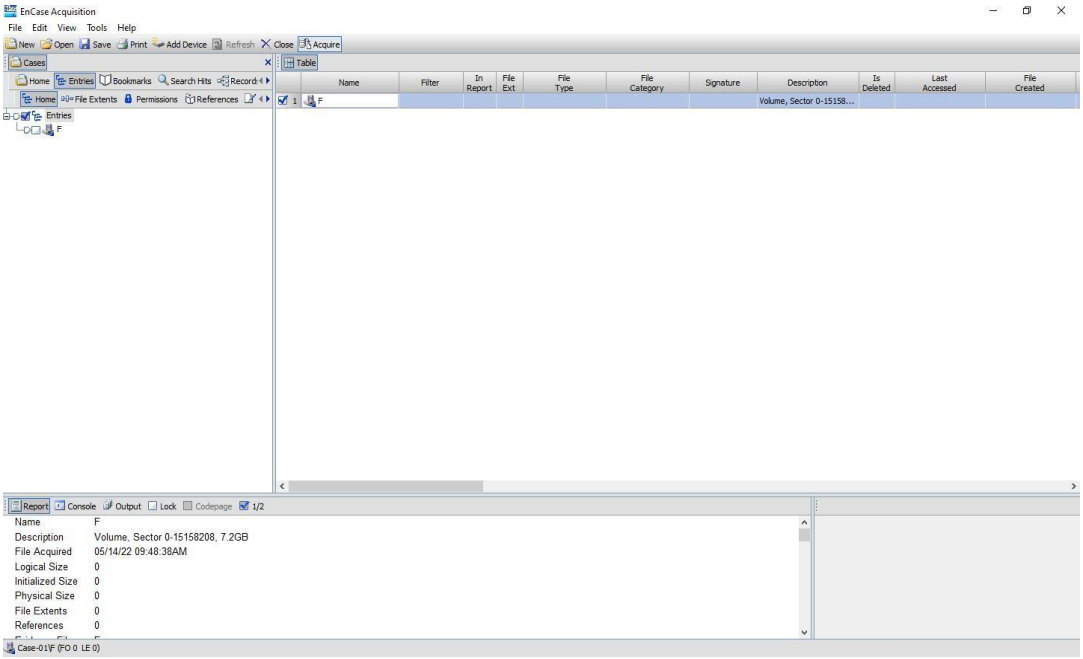
6. We can see the preview of the selected device and click Finish.



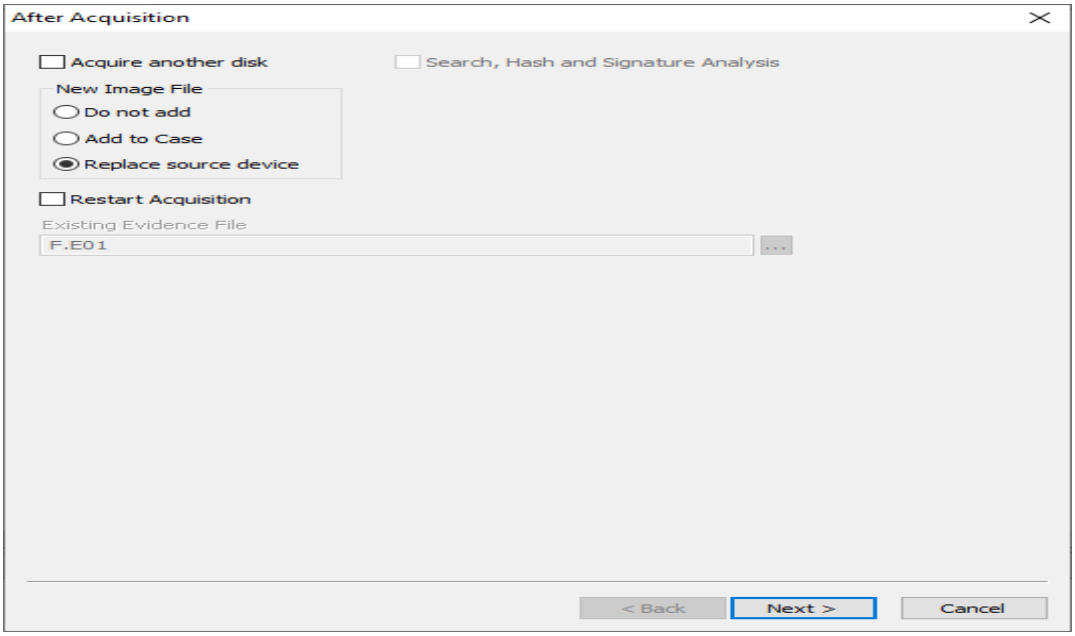
7. We can see the device selected.



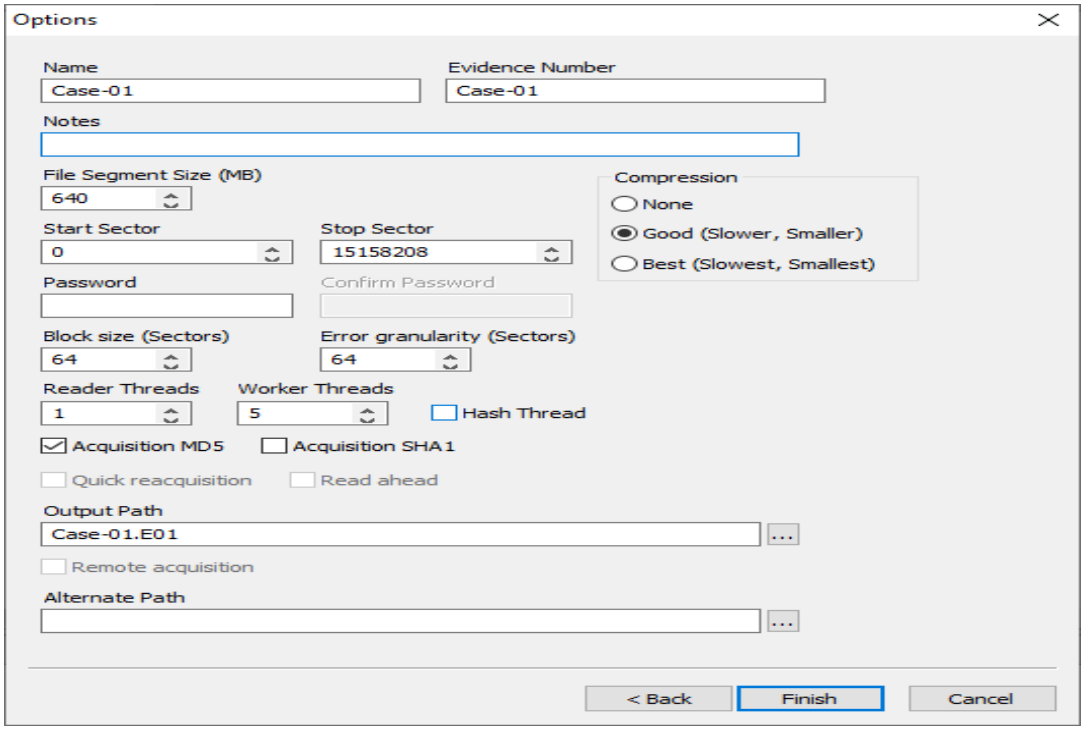
8. Click on Edit and select Acquire.



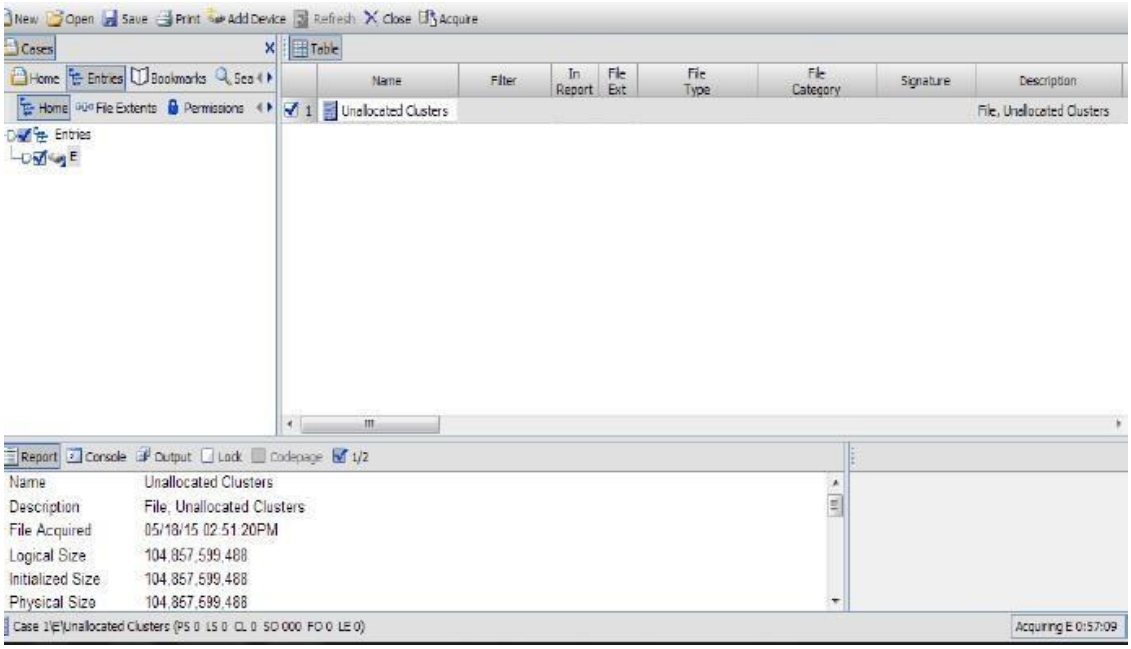
9. Click Next



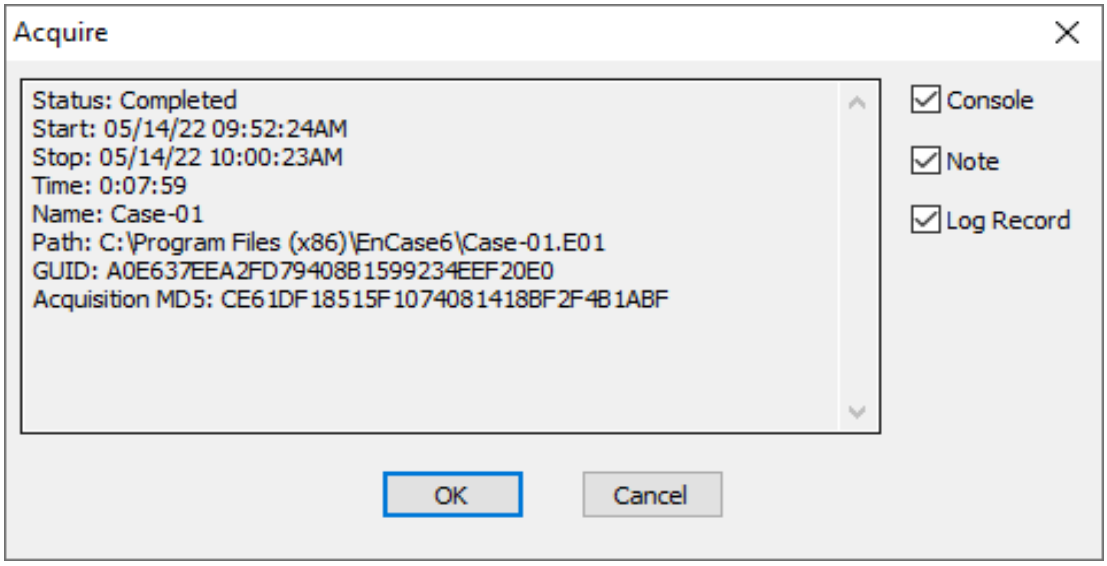
10. Enter the Name and check the output path and click Finish.



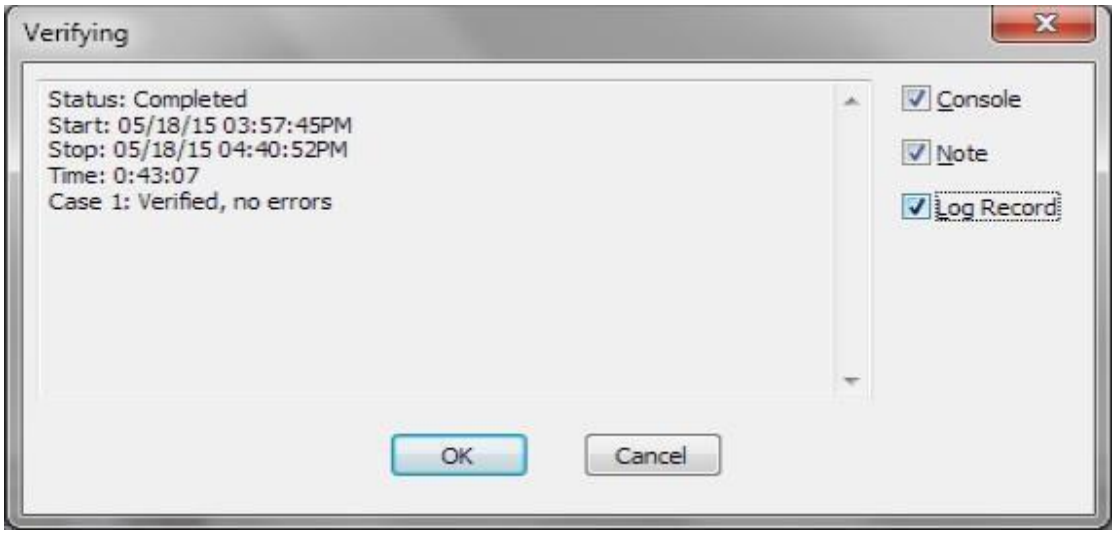
11. Acquiring process starts.



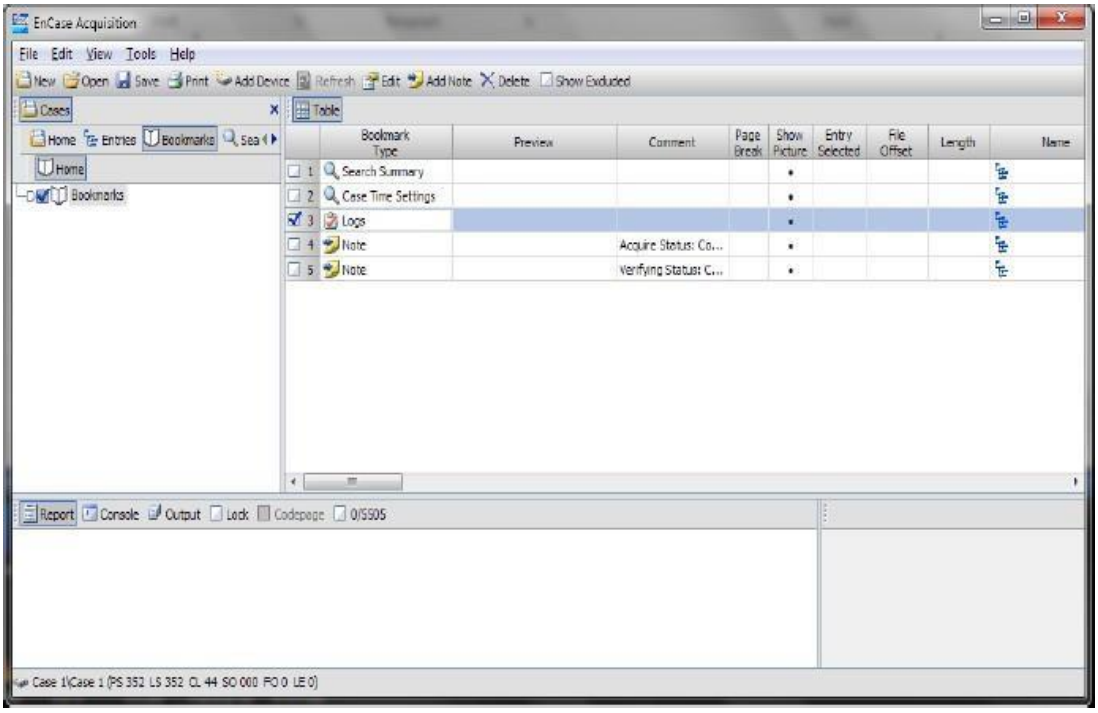
12. Click OK



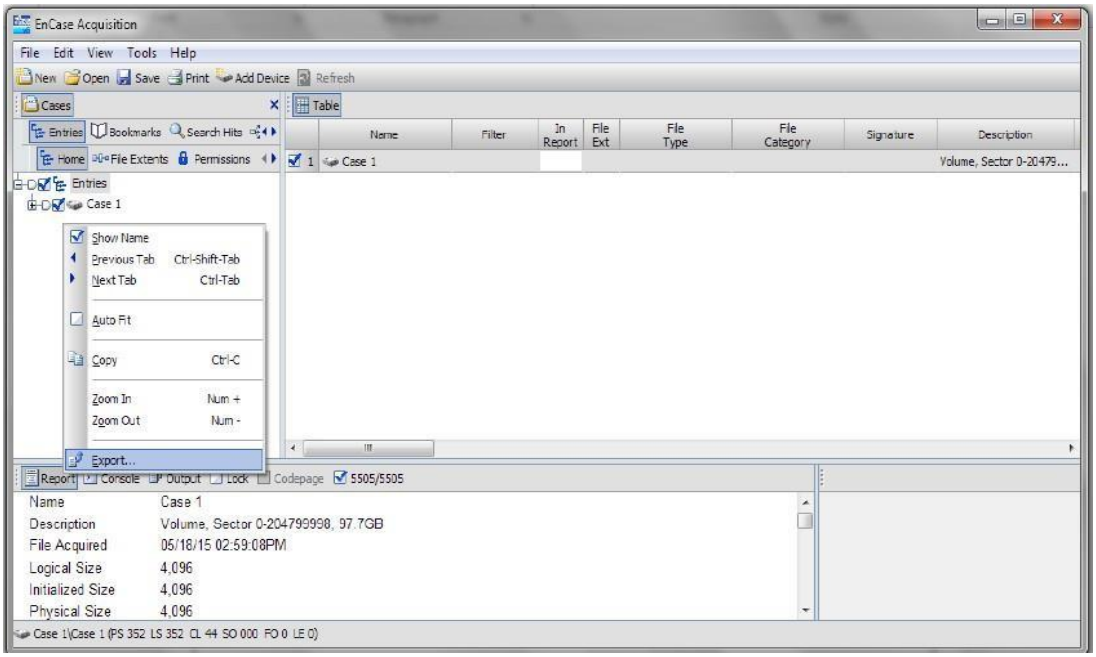
13. Verification result



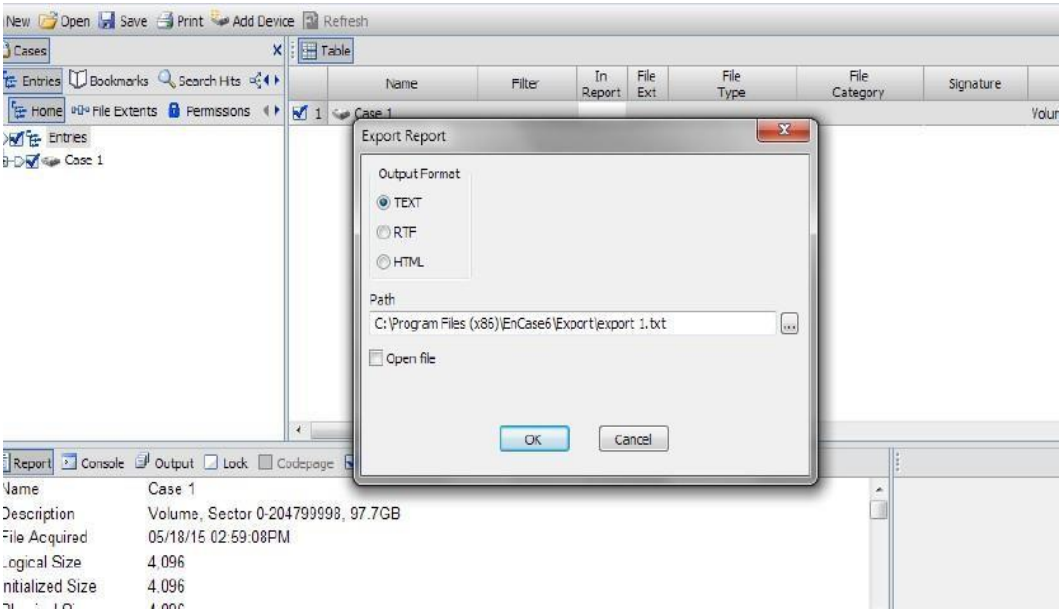
14. Select bookmark option, select "Logs"



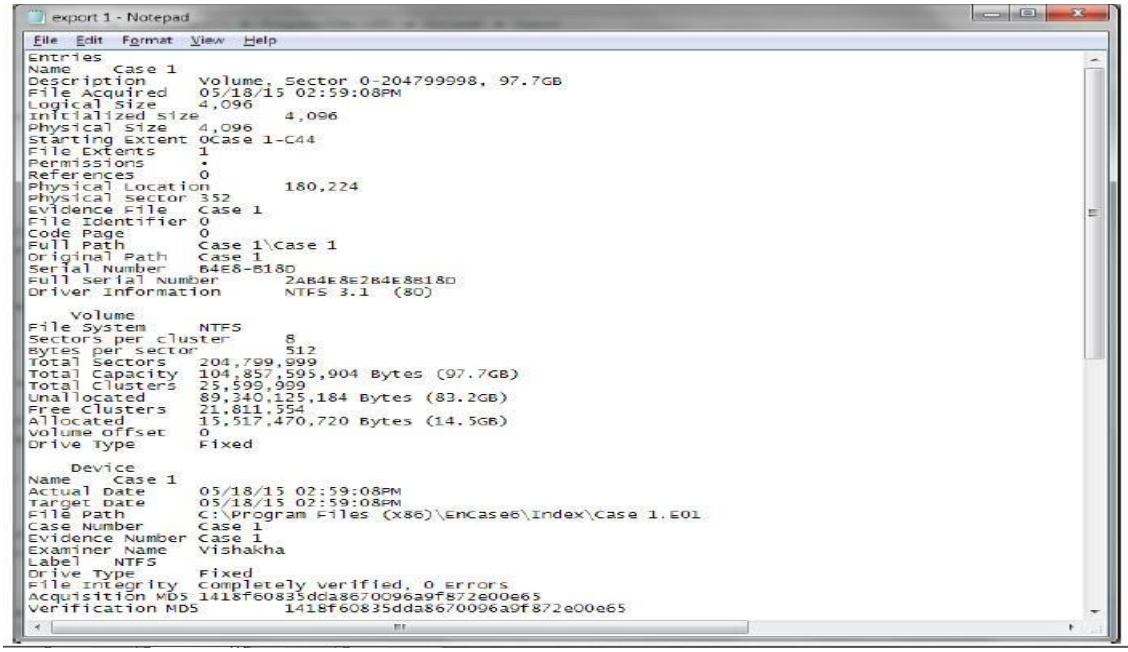
15. For viewing report, right click on Report tab and select Export.



16. Click OK



17. Open the file "export1.txt



```
export 1 - Notepad
File  Edit  Format  View  Help
Entries
Name      Case 1
Description       Volume, Sector 0-204799998, 97.7GB
File Acquired     05/18/15 02:59:08PM
Logical Size      4,096
Initialized Size        4,096
Physical Size     4,096
Starting Extent   0Case 1-C44
File Extents      1
Permissions       .
References        0
Physical Location       180,224
Physical Sector 352
Evidence File     Case 1
File Identifier 0
Code Page         0
Full Path         Case 1\Case 1
Original Path     Case 1
Serial Number     B4E8-B18D
Full Serial Number      2AB4E8E2B4E8B18D
Driver Information      NTFS 3.1  (80)

    Volume
File System       NTFS
Sectors per Cluster     8
Bytes per Sector        512
Total Sectors     204,799,999
Total Capacity    104,857,595,904 Bytes (97.7GB)
Total Clusters    25,599,999
Unallocated       89,340,125,184 Bytes (83.2GB)
Free Clusters     21,811,554
Allocated         15,517,470,720 Bytes (14.5GB)
Volume Offset     0
Drive Type        Fixed

    Device
Name      Case 1
Actual Date       05/18/15 02:59:08PM
Target Date       05/18/15 02:59:08PM
File Path         C:\Program Files (x86)\EnCase6\Index\Case 1.E01
Case Number       Case 1
Evidence Number Case 1
Examiner Name     Vishakha
Label     NTFS
Drive Type        Fixed
File Integrity    Completely Verified, 0 Errors
Acquisition MD5 1418f60835dda8670096a9f872e00e65
Verification MD5        1418f60835dda8670096a9f872e00e65
```

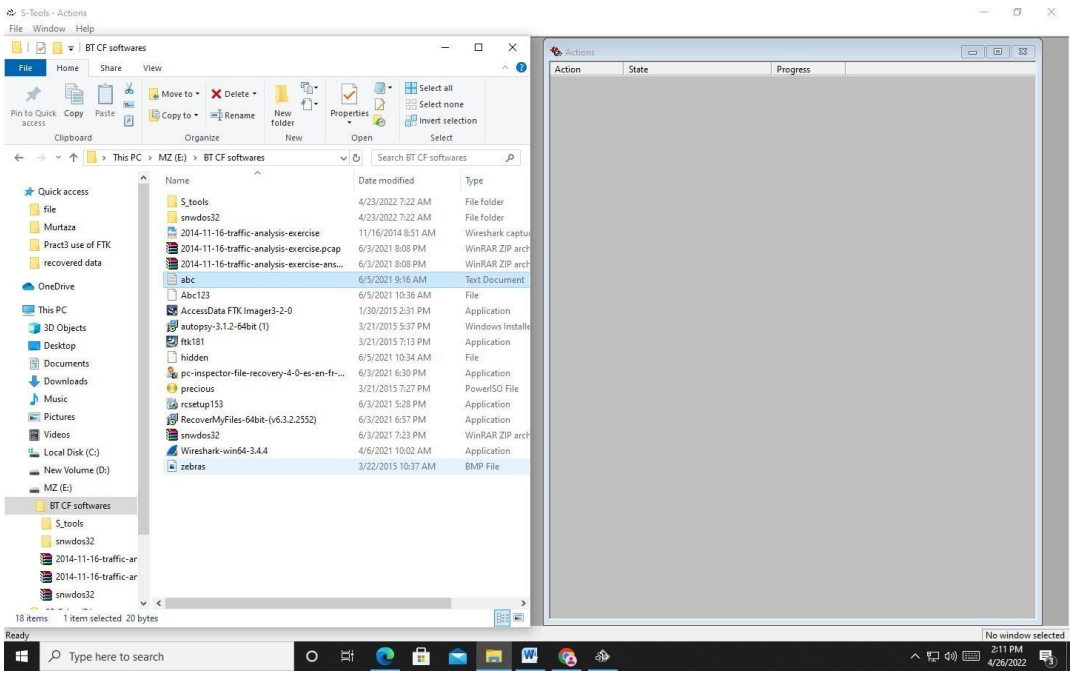
```
export 1 - Notepad
File  Edit  Format  View  Help
Case Number       Case 1
Evidence Number Case 1
Examiner Name     Vishakha
Label     NTFS
Drive Type        Fixed
File Integrity    Completely Verified, 0 Errors
Acquisition MD5 1418f60835dda8670096a9f872e00e65
Verification MD5        1418f60835dda8670096a9f872e00e65
GUID      7e17adc71bce454fb381c116cb56114e
EnCase Version  6.19.6
System Version  Windows 7
Raid Stripe Size        0
Error Granularity       64
Process ID        0
Index File        C:\Program Files (x86)\EnCase6\Index\Case 1-7e17adc71bce454fb381c116cb56114e.Index
Read Errors       1
Missing Sectors 0
CRC Errors        0
Compression       Good
Total Size        104,857,599,488 Bytes (97.7GB)
Total Sectors     204,799,999
Disk Signature    00000000
Partitions        Valid

Permissions
Name      Id        Property          Permissions
Administrators    S-1-5-32-544      Allow     [FC] [M] [R&X] [R] [W] [Sync]
Administrators    S-1-5-32-544      Allow     [Read Control] [Obj In ACE] [Cont In ACE] [In Only ACE]
System    S-1-5-18          Allow     [FC] [M] [R&X] [R] [W] [Sync]
System    S-1-5-18          Allow     [Read Control] [Obj In ACE] [Cont In ACE] [In Only ACE]
Authenticated Users       S-1-5-11          Allow     [M] [R&X] [R] [W] [Sync]
Authenticated Users       S-1-5-11          Allow     [Delete] [Change Access] [Change Owner] [Synchroni
Users     S-1-5-32-545      Allow     [R&X] [R] [Sync]
Users     S-1-5-32-545      Allow     [Change Access] [Synchronize] [Obj In ACE] [Cont In ACE] [In Only
Administrators    S-1-5-32-544      Owner
Domain Users      S-1-5-21-271917436-849621321-658011319-513        Group

Hash Properties
Name      Value
Hash Set
Hash Category

Read Errors
Start Sector      Sectors
204,799,992       7
```

Practical No: 8a

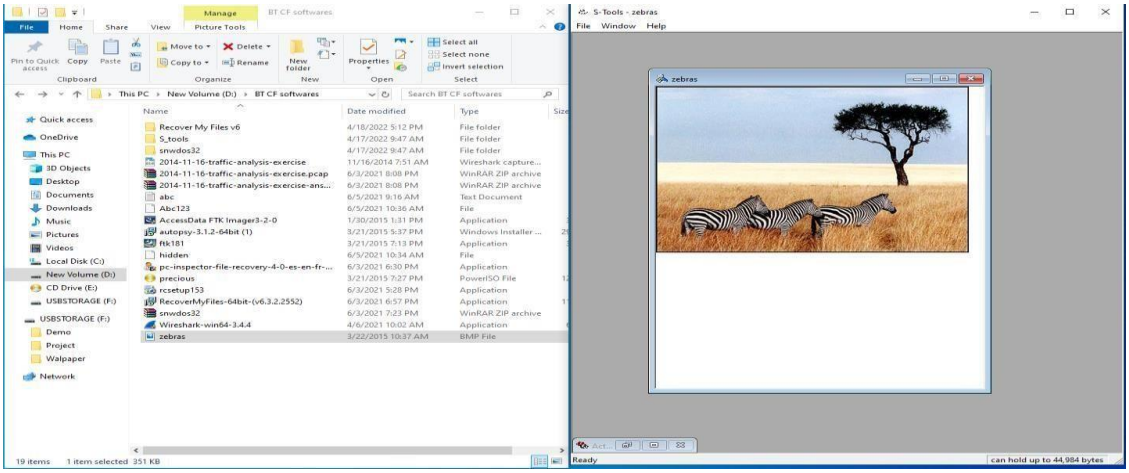
Aim: Using Steganography Tools [S-Tools]

Steps:

1. Select the S-tools.exe file and open the steganography software tool.
2. The main window of the program appears.
3. Three buttons are available on the main window:
    - File
    - Window
    - Help
4. With both the working directory and the S-Tools program open minimize both windows and place side-by-side.
5. 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.
6. Select a valid audio file or image as the base file for the steganography file. The zebras.bmp was selected and dragged onto the main window of the S-Tools program. The image is opened.
7. The zebras.bmp and the Actions window are now in the S-Tools program.
8. The Action window is a process window which displays the process steps as a file is being hidden within a base file.
9. Place the working directory and the base file side-by-side.

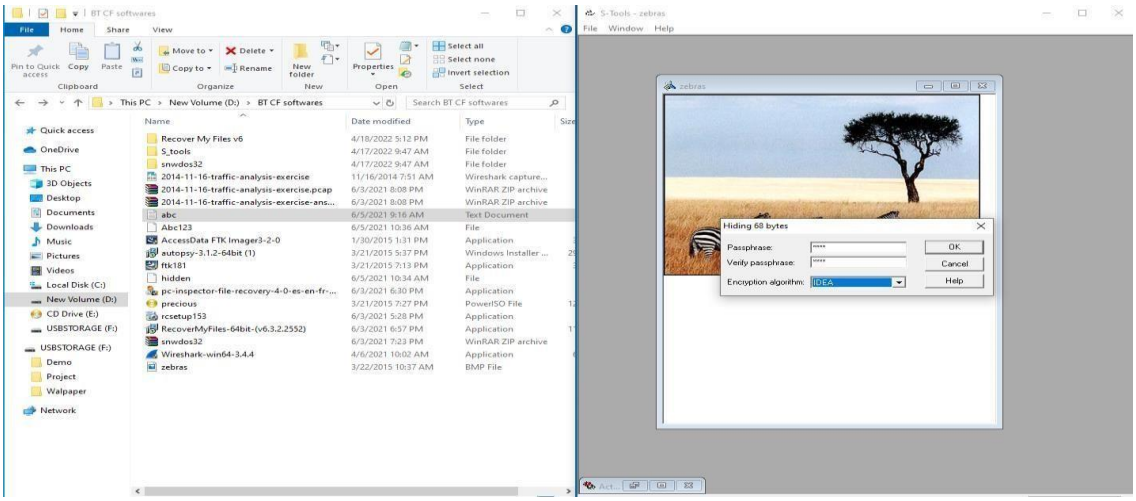


10. 10 Select a file to hide within the base file.
11. The abc.txt is selected and dragged on top of the base image. Release the file while the cursor is still on the top of the base file,
12. A dialogue box will appear asking the user to enter and verify a passphrase. Additionally, the user will have to select an encryption algorithm.
13. Enter a passphrase in both the passphrase and verify passphrase text boxes.
14. If the same passphrase is not entered in both text boxes the 'OK' button will be grayedout and the user will not be able to proceed to creating the steganography file.
15. Select the 'OK' button after entering a valid passphrase.

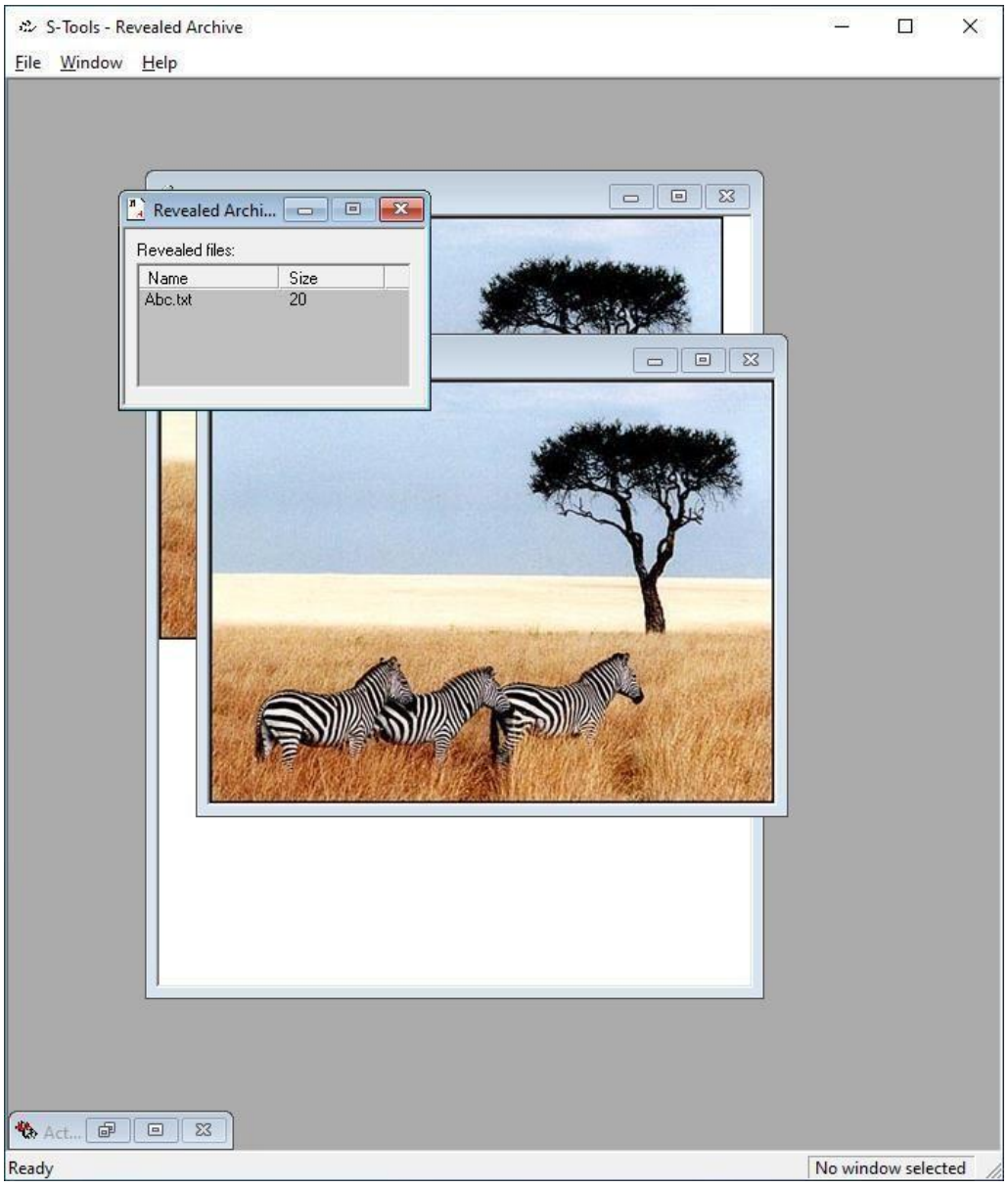


16. The S-Tools main window will appear and a new file will be visible. The name of the file will be called hidden data by default.

17. At this point, the original file has been selected and opened, a second file have been selected and opened and a passphrase has been selected



18. Now the user has to save the steganography file.
19. Place the cursor on top of ythe hidden data image and select the right mouse button.
    a. The user will have four option availabler to rthem:
        i. Save
        ii. Save As
        iii. Properties
        iv. Reveal
20. Now to9 reveal the data from the image, right click and click o9n option Reveal.
21. This will show the file which can be saved and verified.

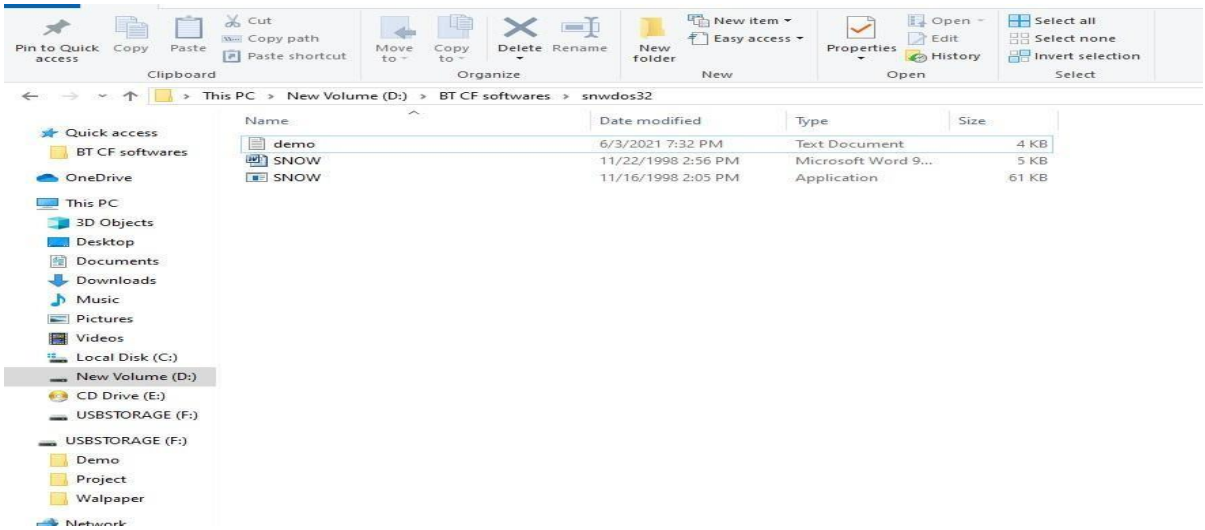


Practical No 8b

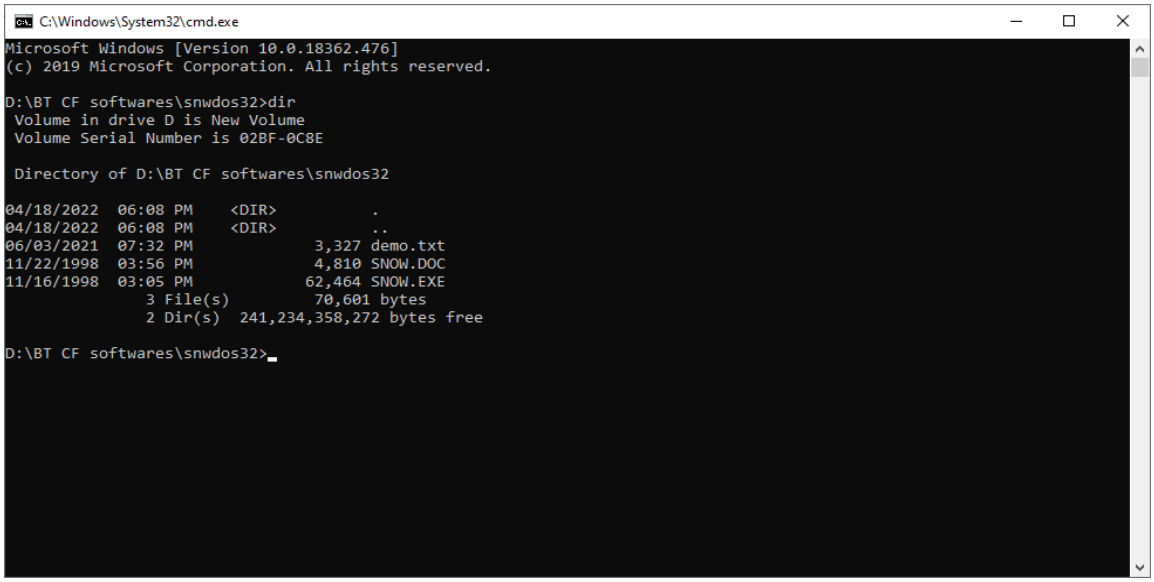
Aim: Using Whitespace Steganography tool SNOW

Steps:

1. Download snow tool. It is command line tool.
2. Create a text file “demo.txt” in which the secret message is to be stored and keep this file in snow directory only.



3. Open the command prompt and reach to location where snow directory is stored and run dir command



4. To store a secret message in file demo.txt, use following command and also give password.

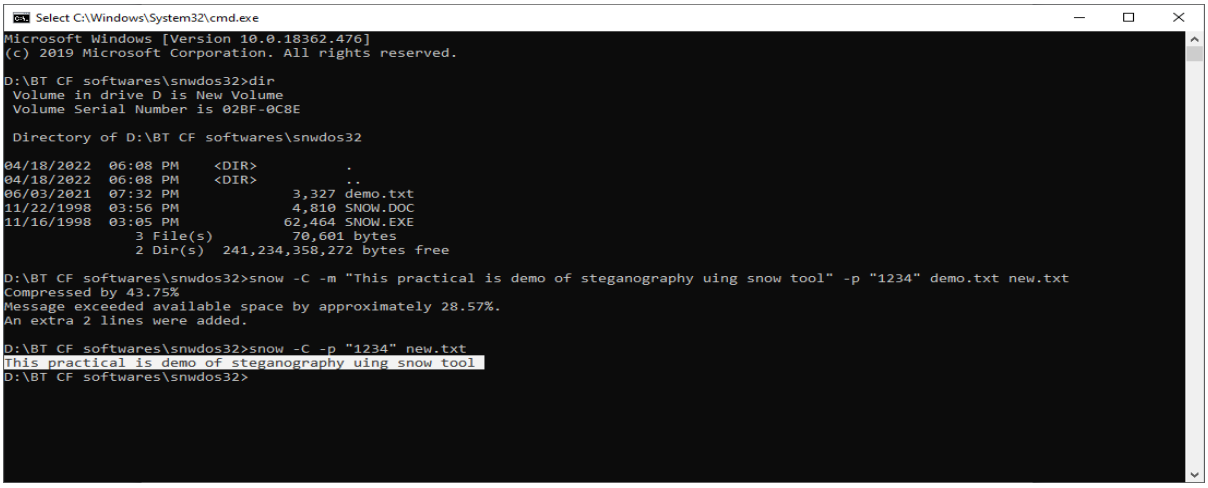
snow –C –m “This practical is demo of steganography using snow tool” -p demo.txt newfile.txt

-m indicates message to be stored

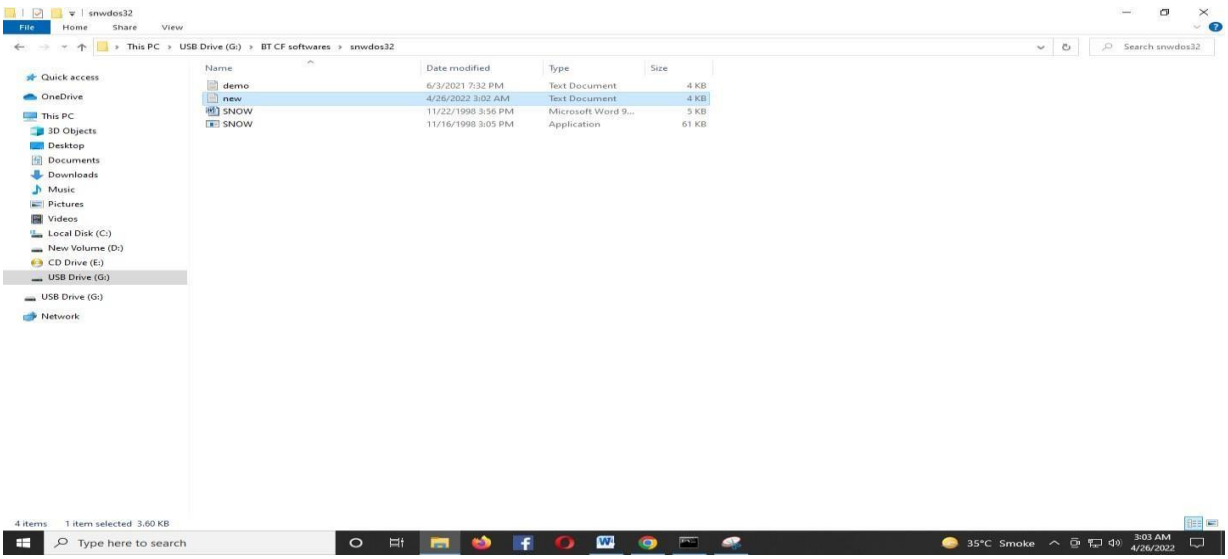
-p indicates password to protect the message

demo.txt is file in which message will be hidden

newfile.txt is file with the secret message

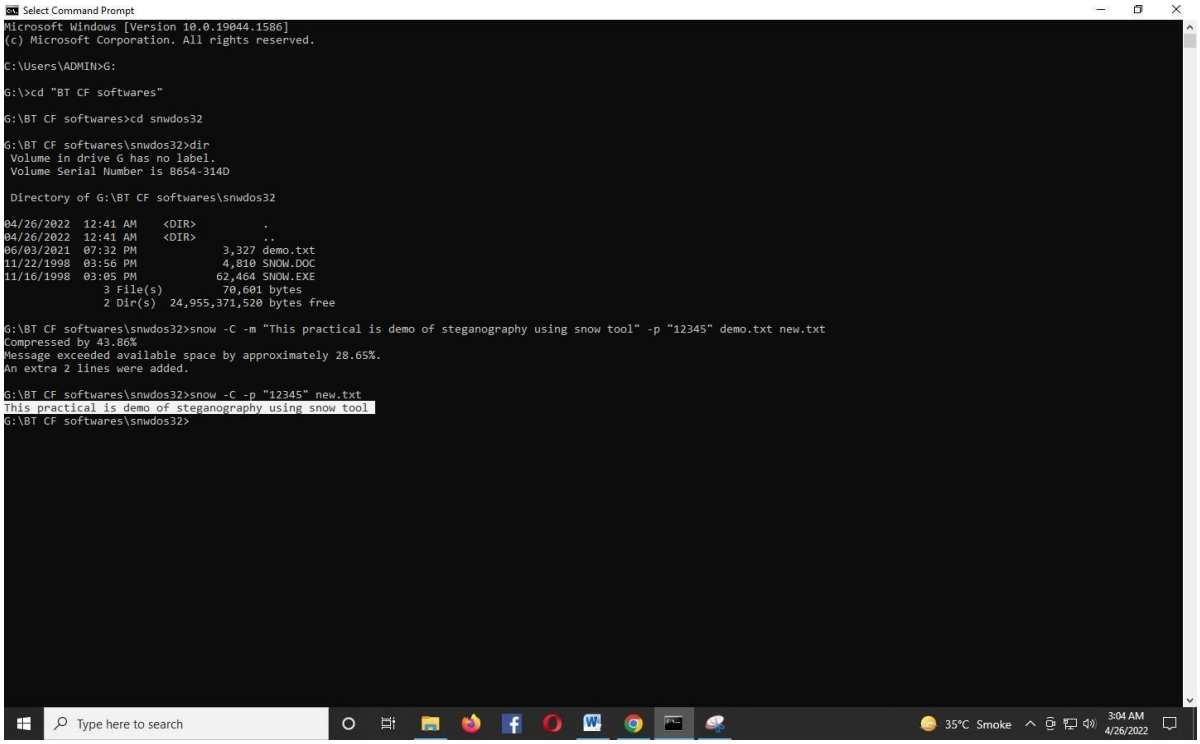


White spaces will be added to new files. The above output shows extra 3 lines were added.



5. To recover message from newfile.txt use following command

snow –C –p “Demo.txt” newfile.txt



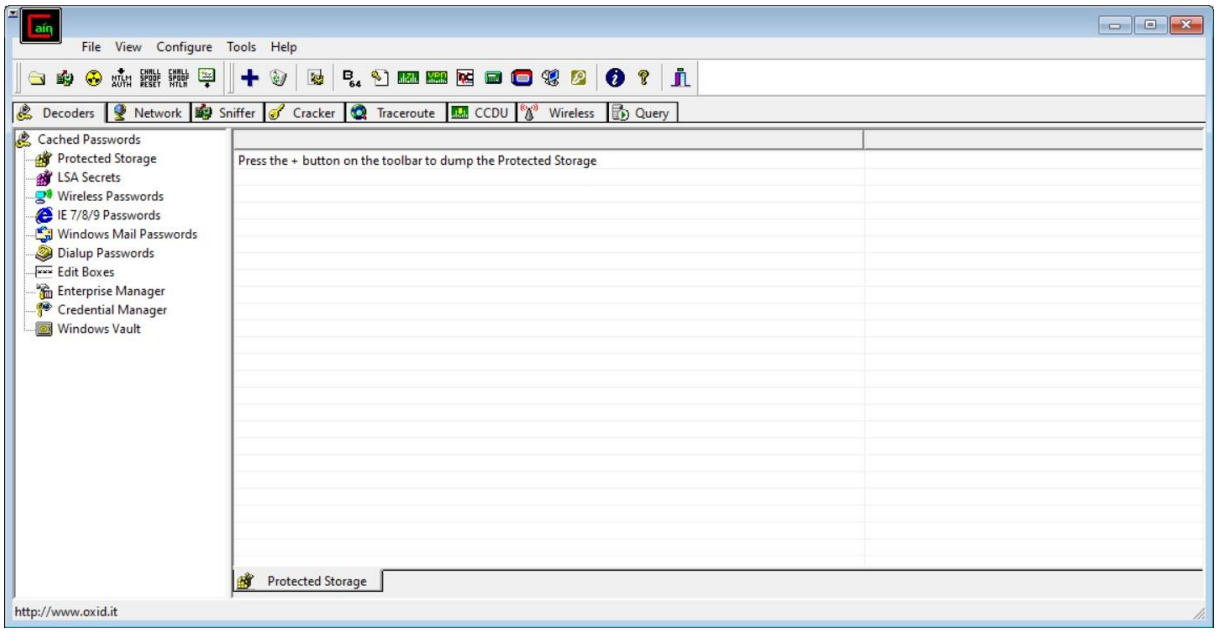
The message will be recovered.

Practical No 9.a

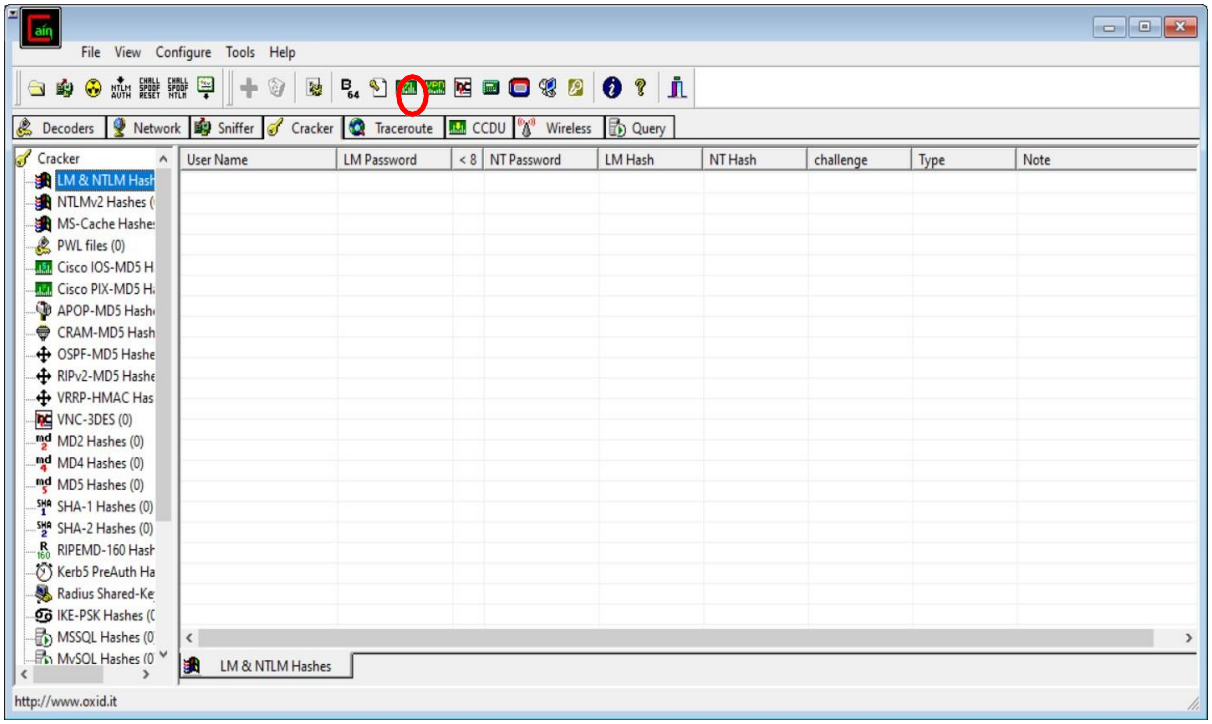
Aim: Password Cracking Using Cain and Abel.

Steps:

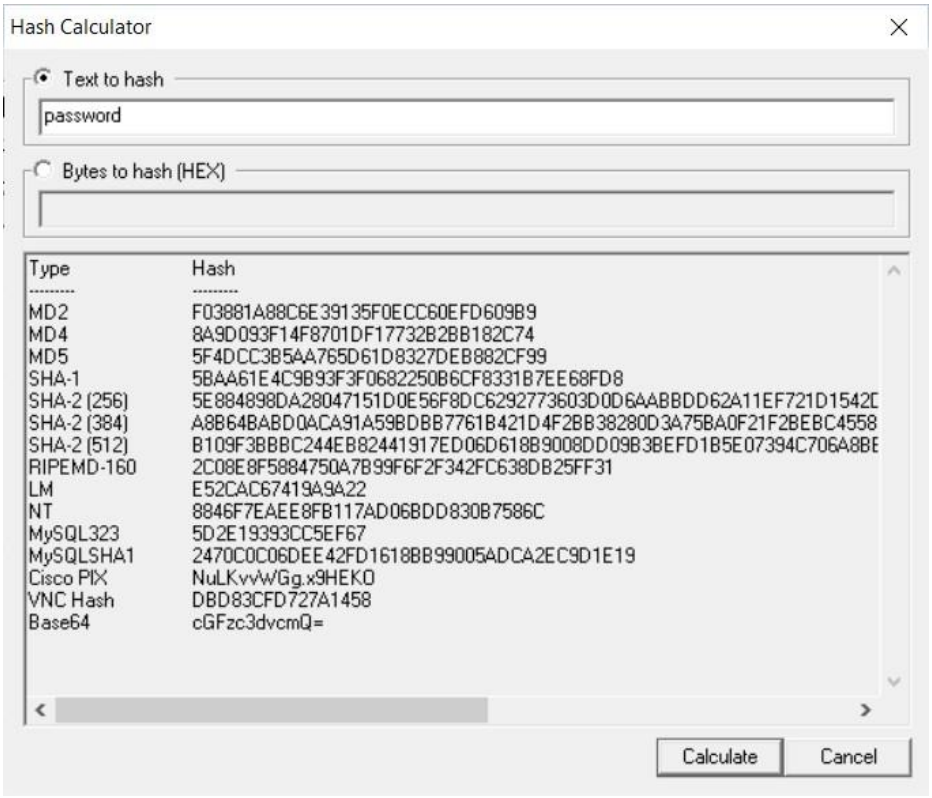
1. Open Cain and Able.



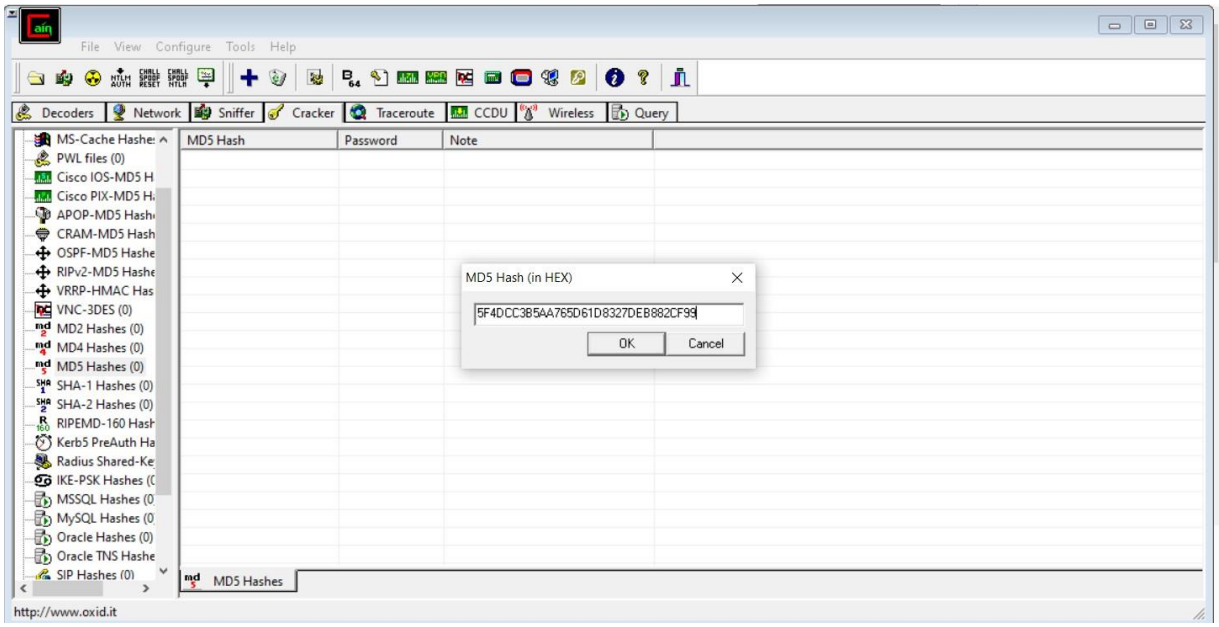
2. Click on Cracker tab -> Hash Calculator tool as shown in the image.



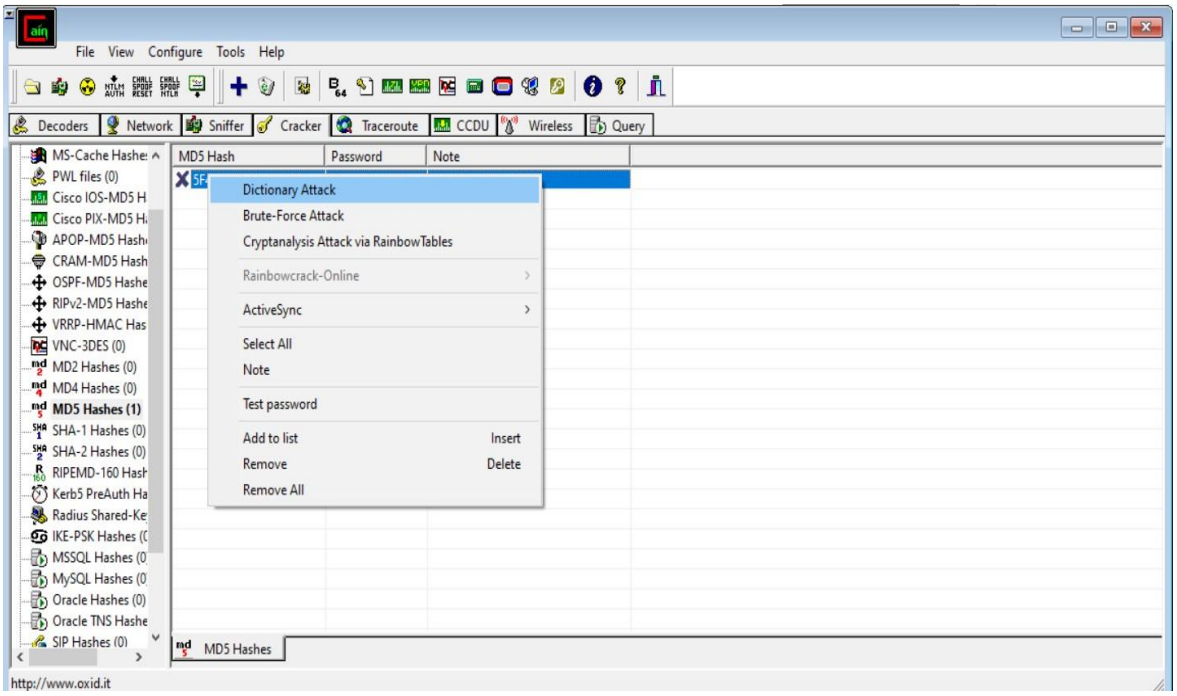
3. A dialogue box appears after clicking on hash calculator. Add the text “password” -> Calculate. Copy MD5 hash value

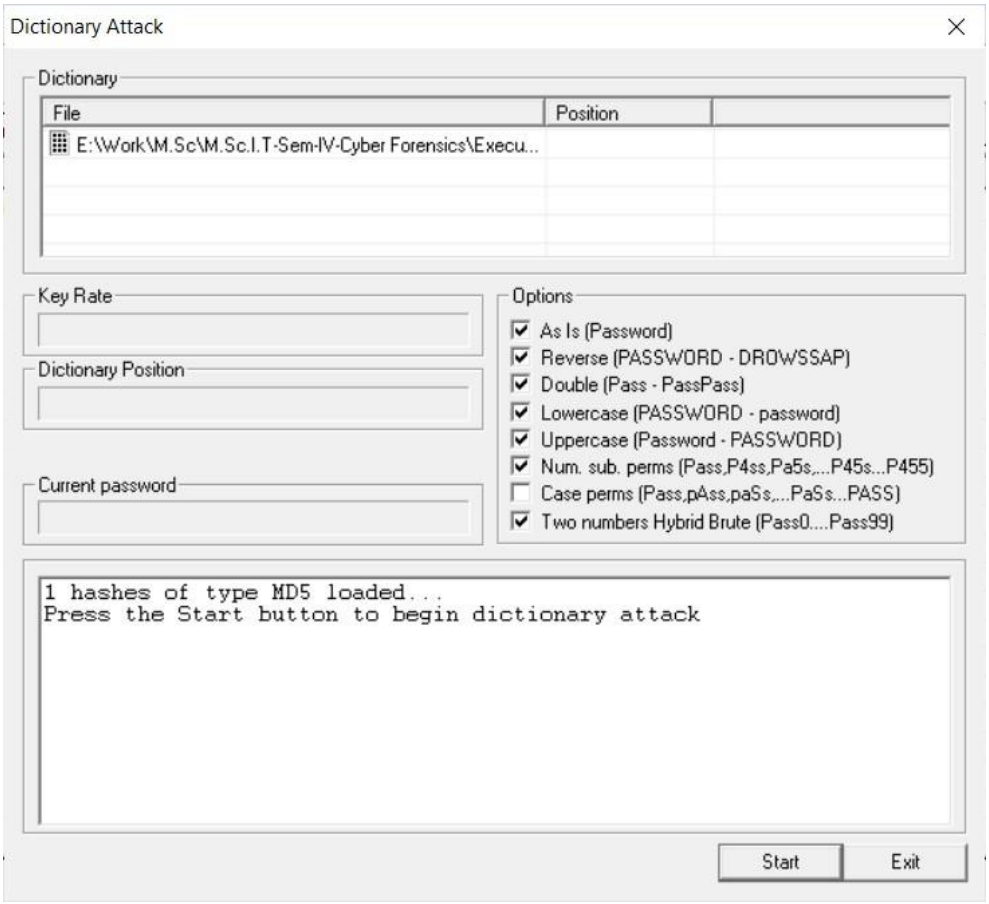


4. Click on MD5 Hashes-> Add list->Paste Hash Value.

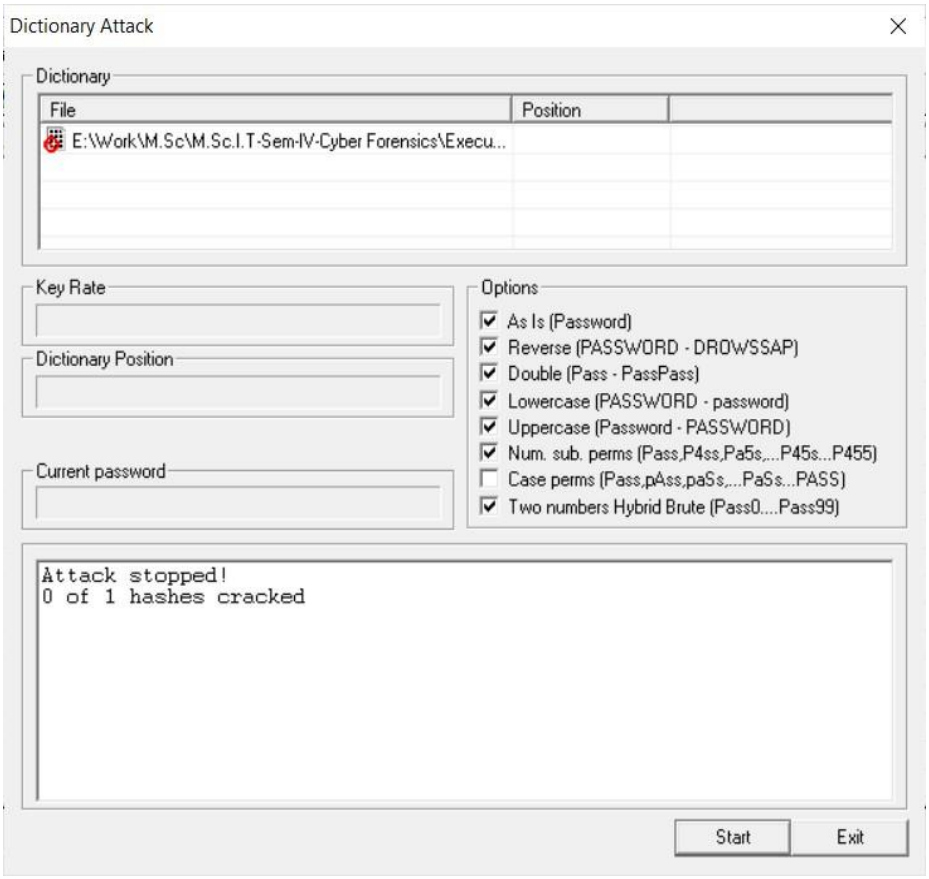


5. Right click the hash value. Select dictionary attack-> Add to list-> Start

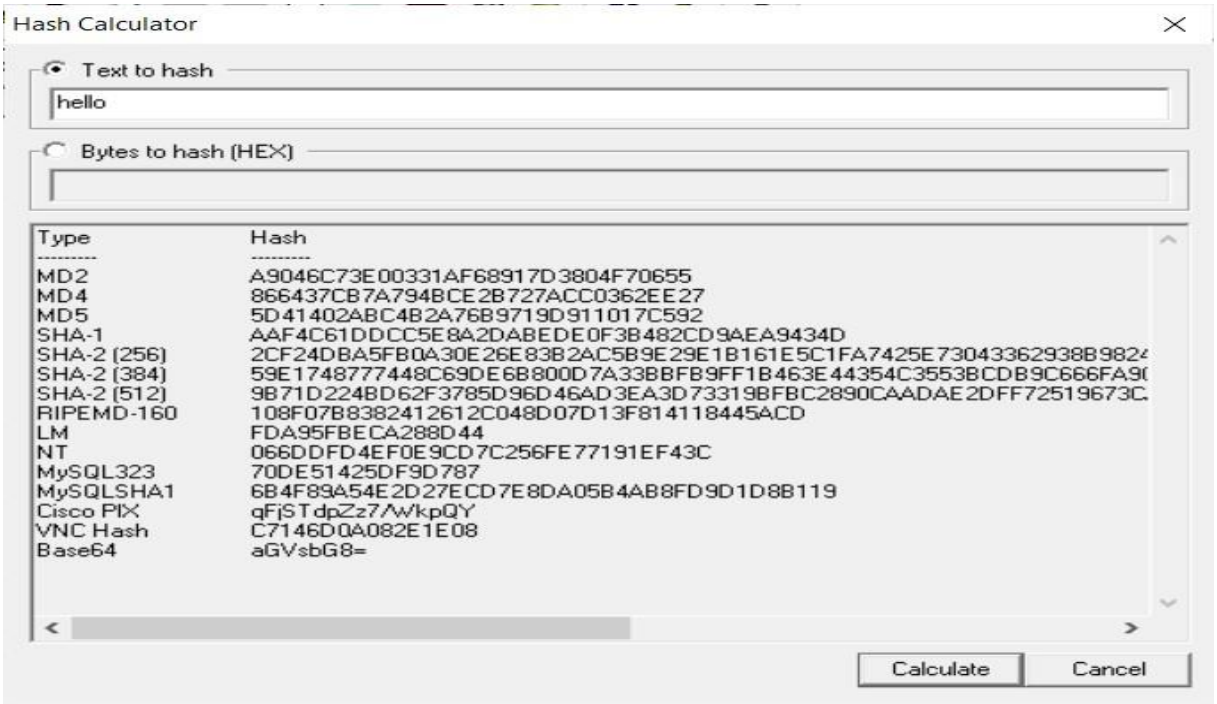




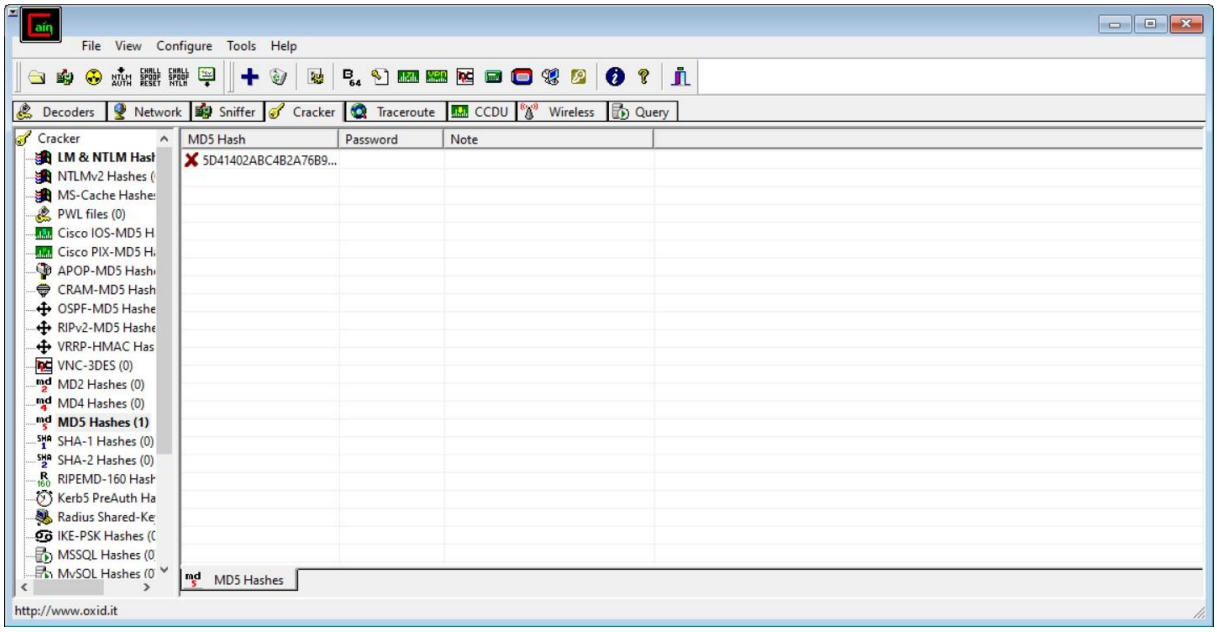
6. If password not found, it will show 0 hash cracked.



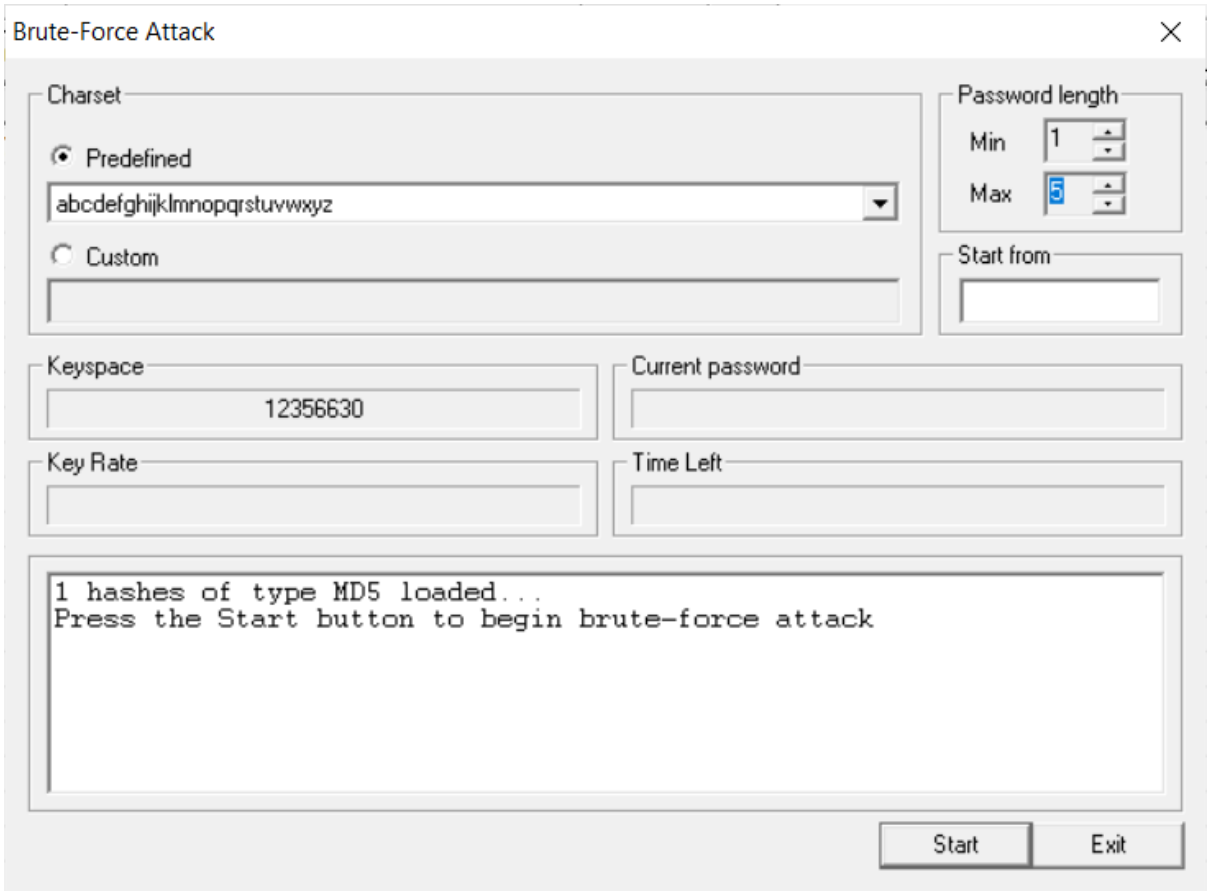
7. Again, go to hash calculator. Enter the text as hello and copy the MD5 value.



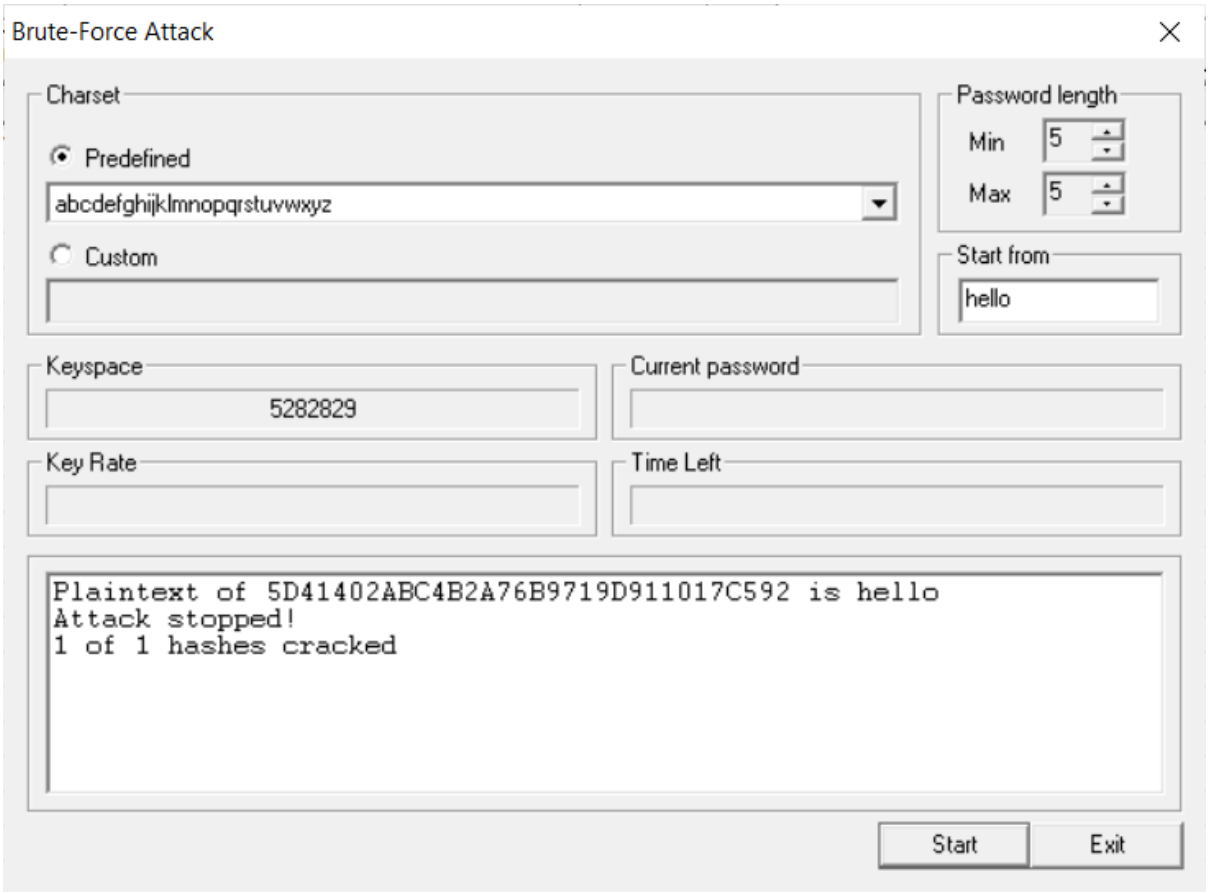
8. Add the value. Right click and select Brute-Force Attack.



9. Select predefined charset, set min and max length. Click on start.



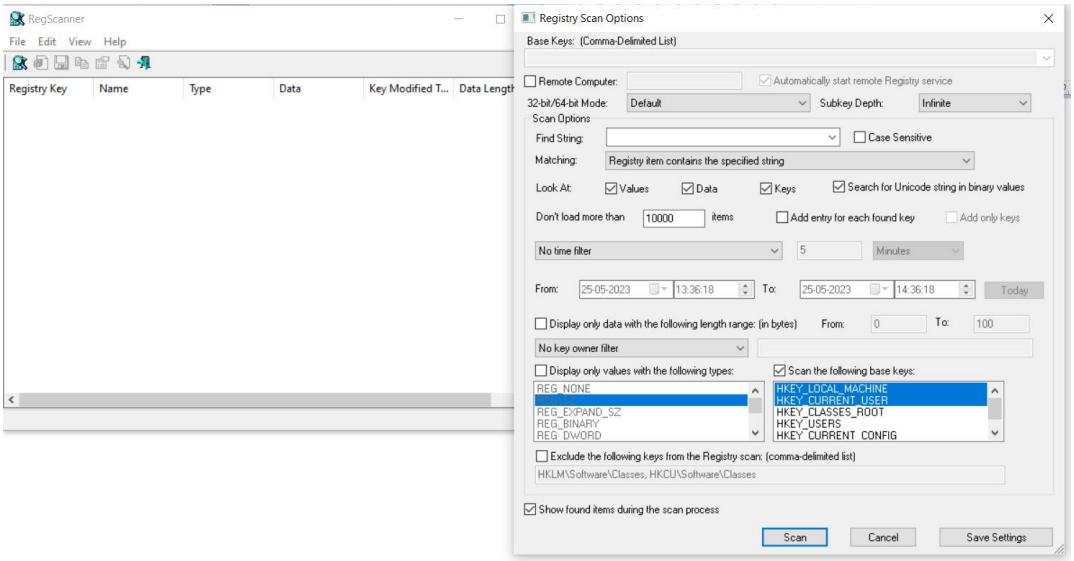
10. If hash is found, it will display the same.



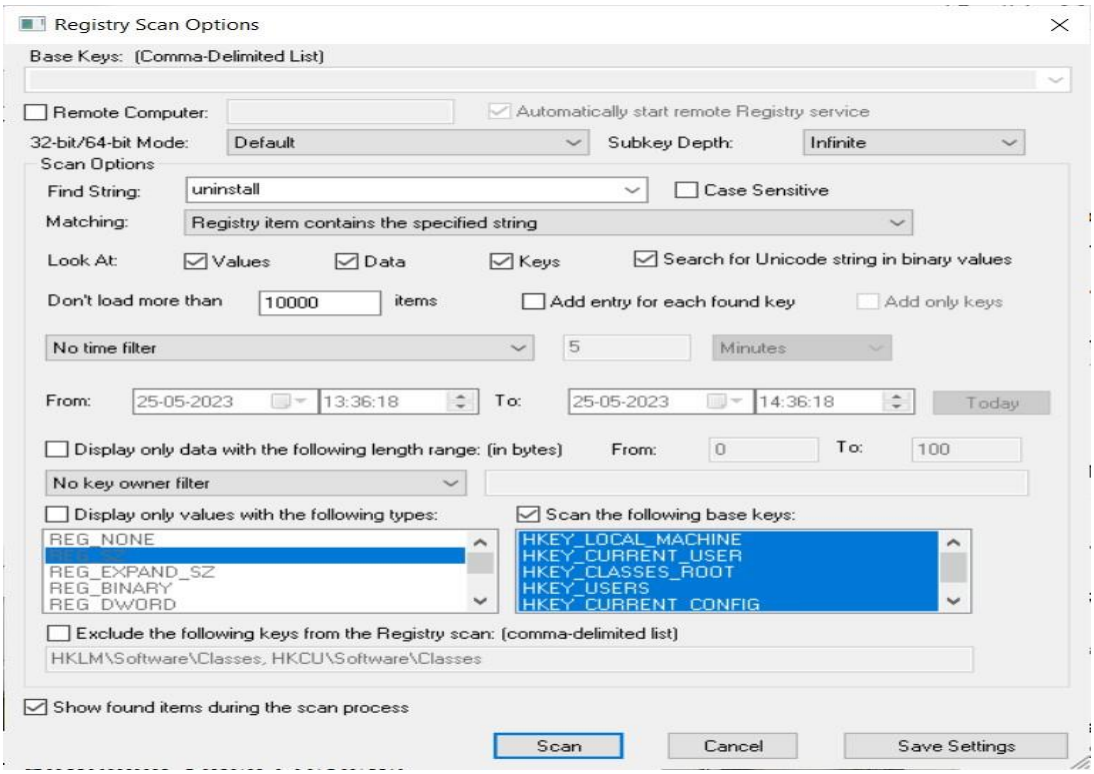
Practical No:10a

Aim: Scan Registry using RegScanner

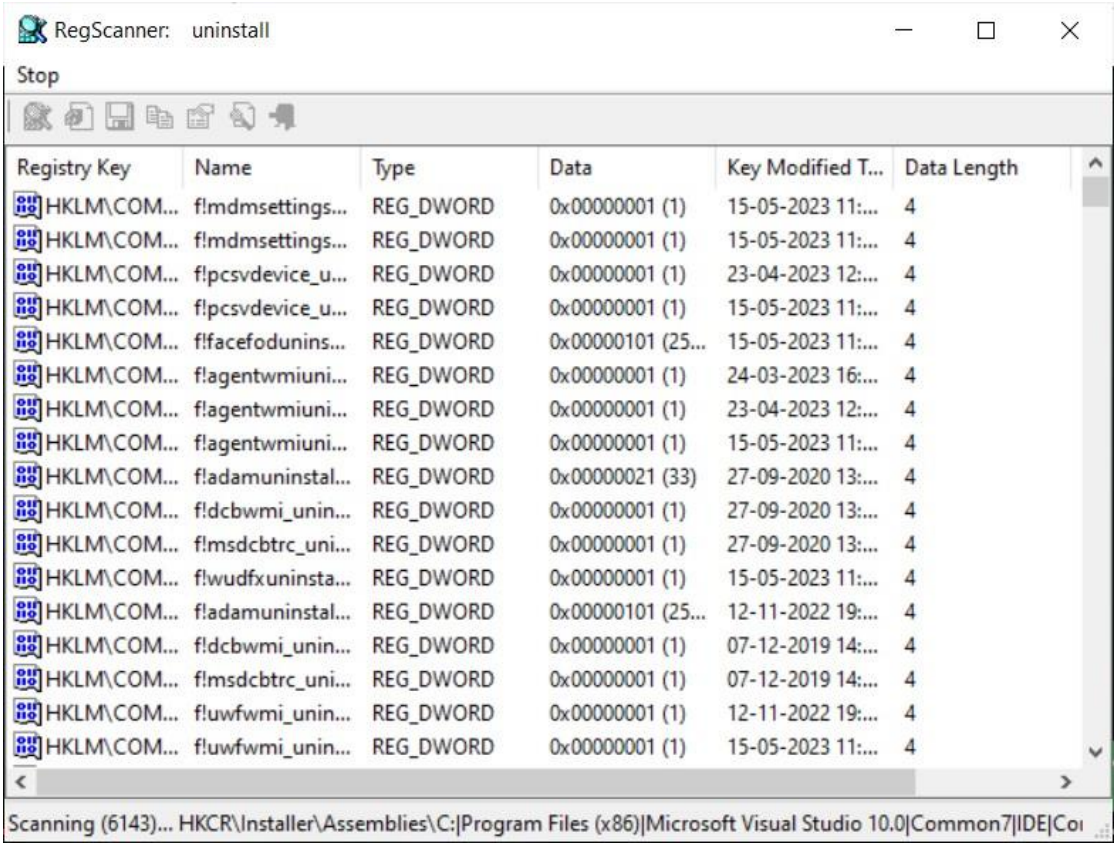
1. Open RegScanner tool.



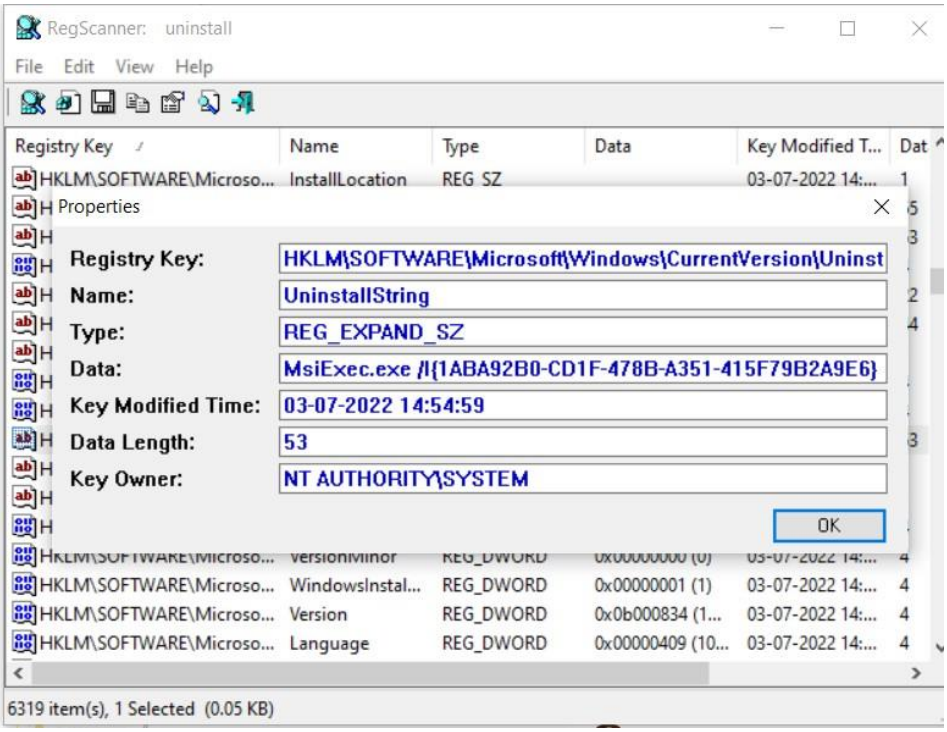
2. Select all in scan the following base keys. In Find String text field, search for word uninstall. Click on Scan.



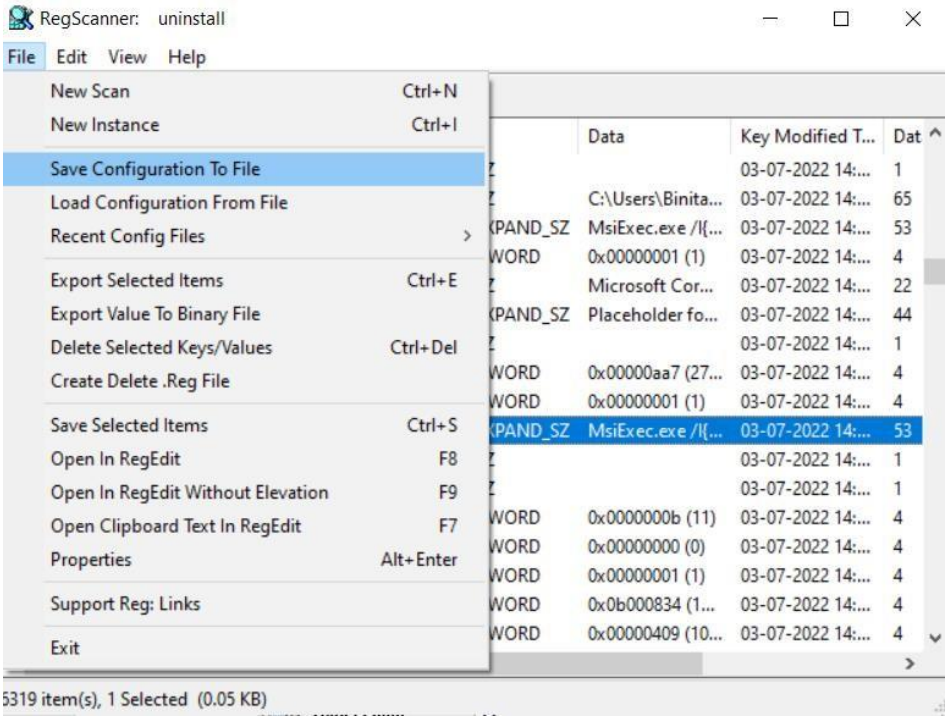
3. Scanner registry keys details will be obtained.



4. Select any file and click on Properties button to get registry details.



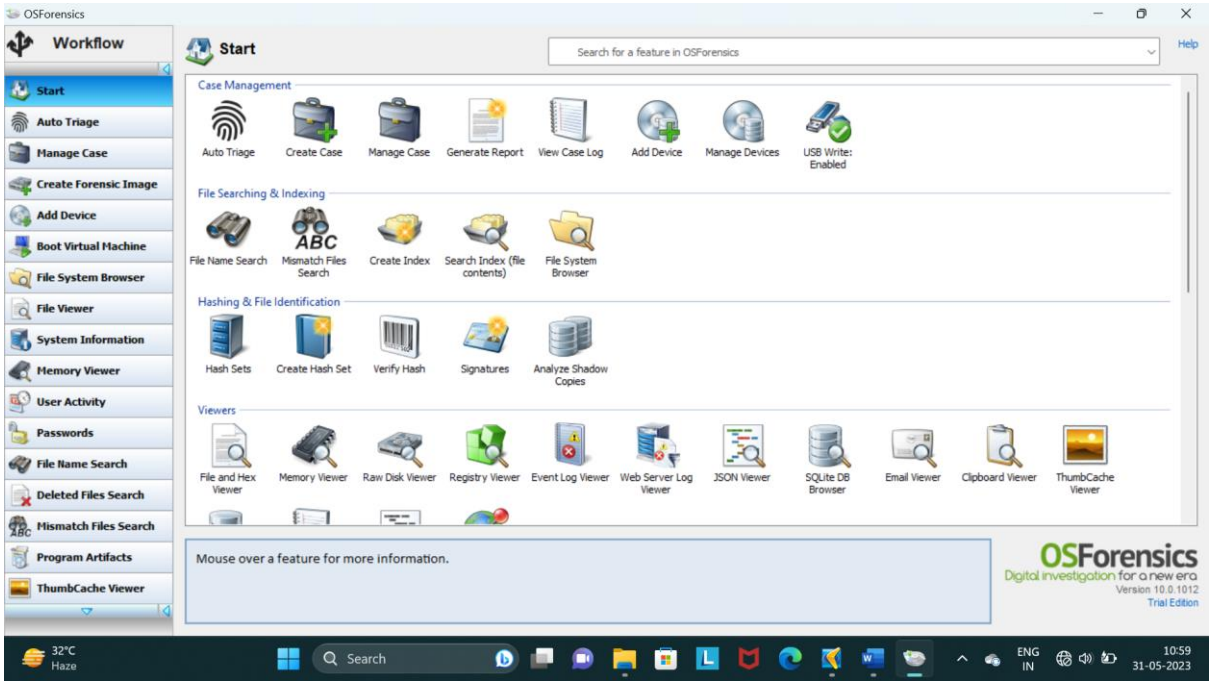
5. Save the configuration to a file for future analysis.



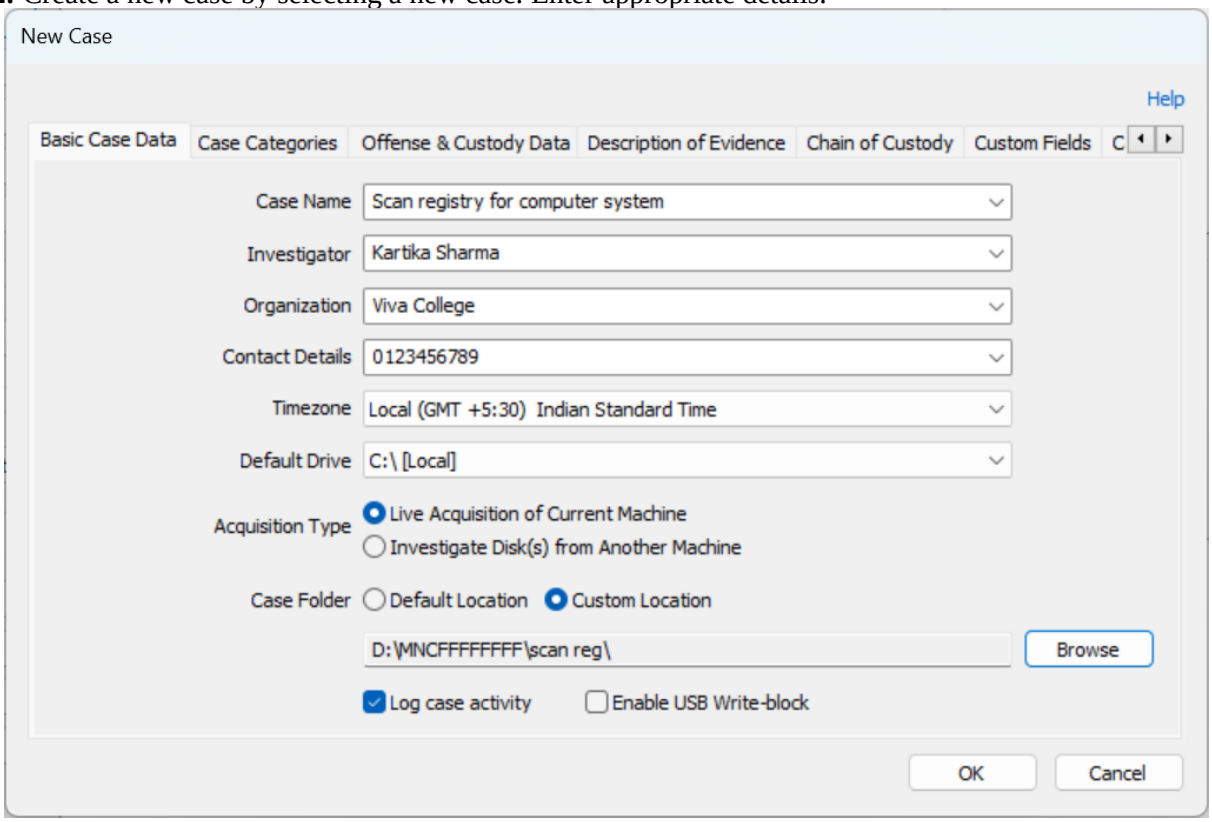
Practical N0: 10B

AIM: Scan registry using OS Forensics.

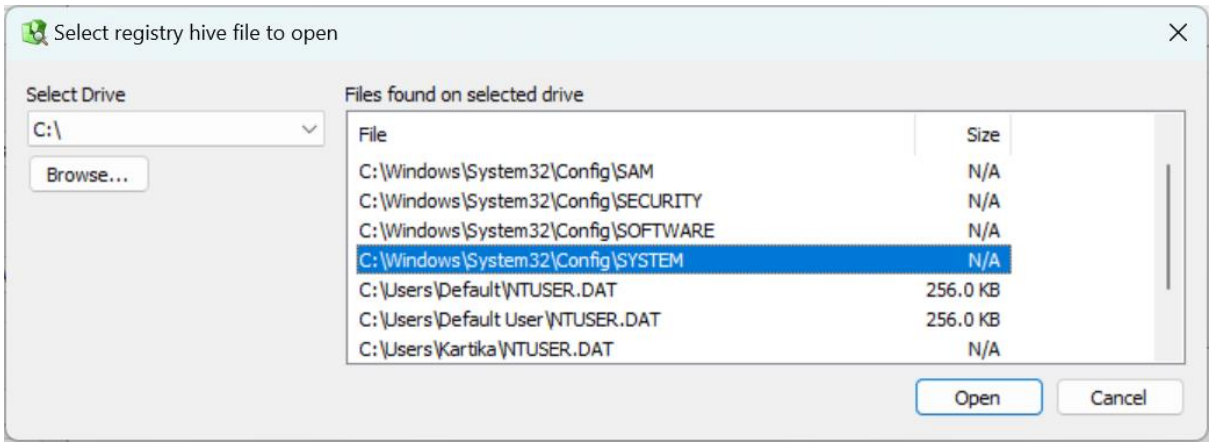
Step 1: Start OS Forensic.

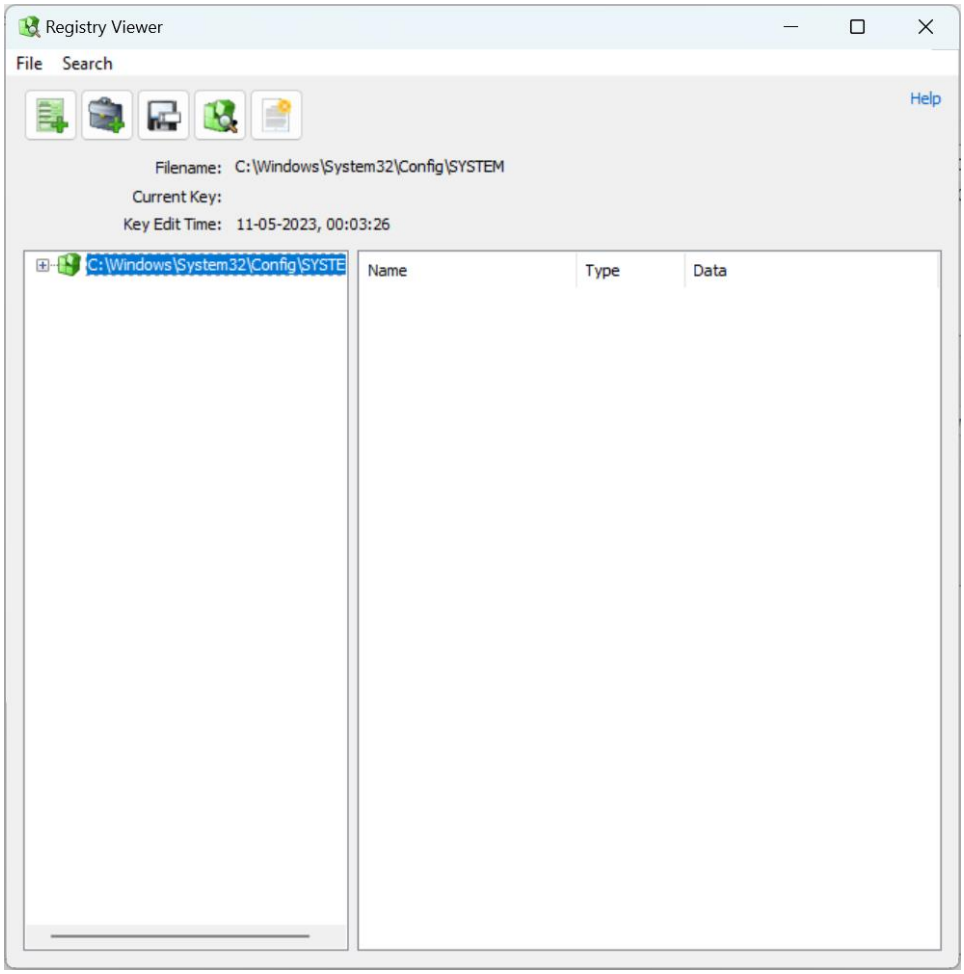


Step 2: Create a new case by selecting a new case. Enter appropriate details.

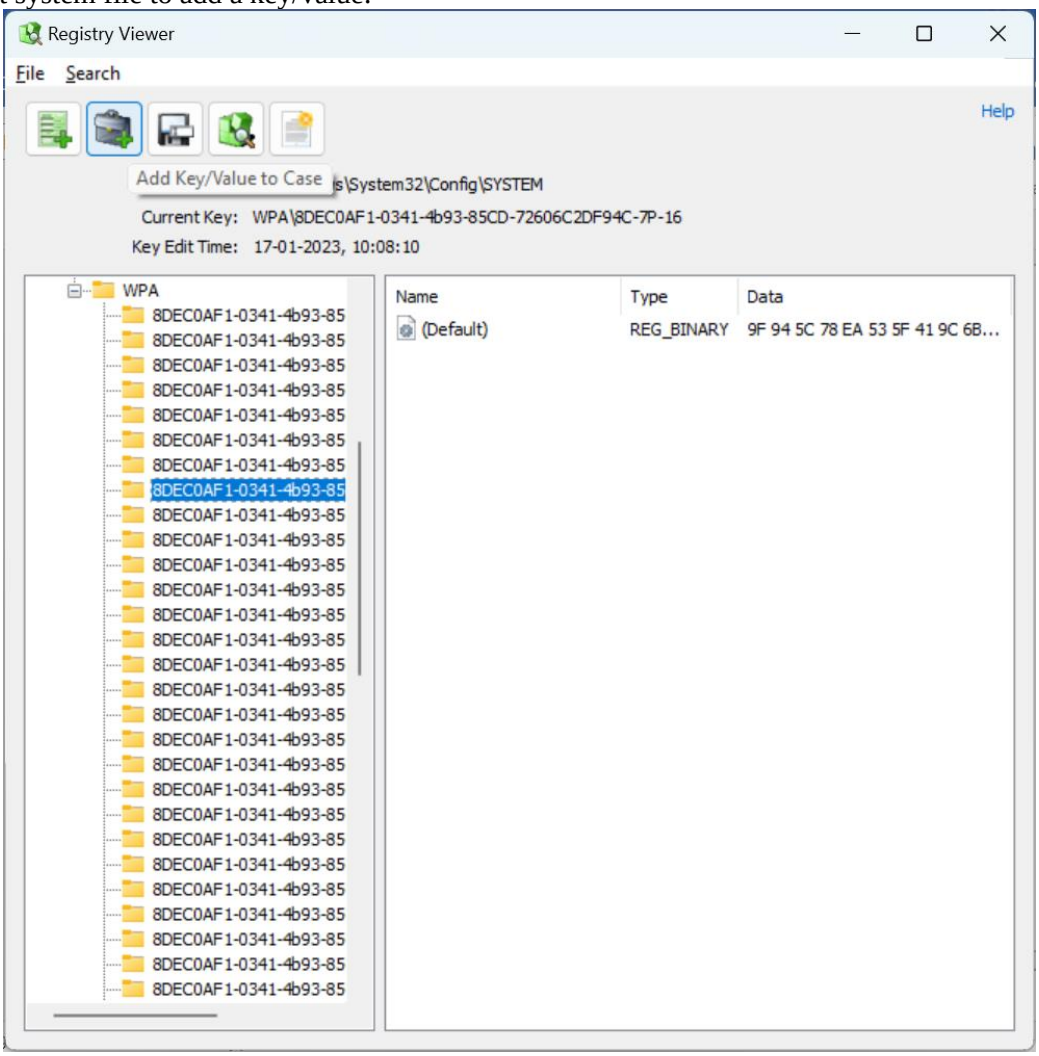


Step 3: Select reg viewer and select reg hive file to open for computer system and select open.

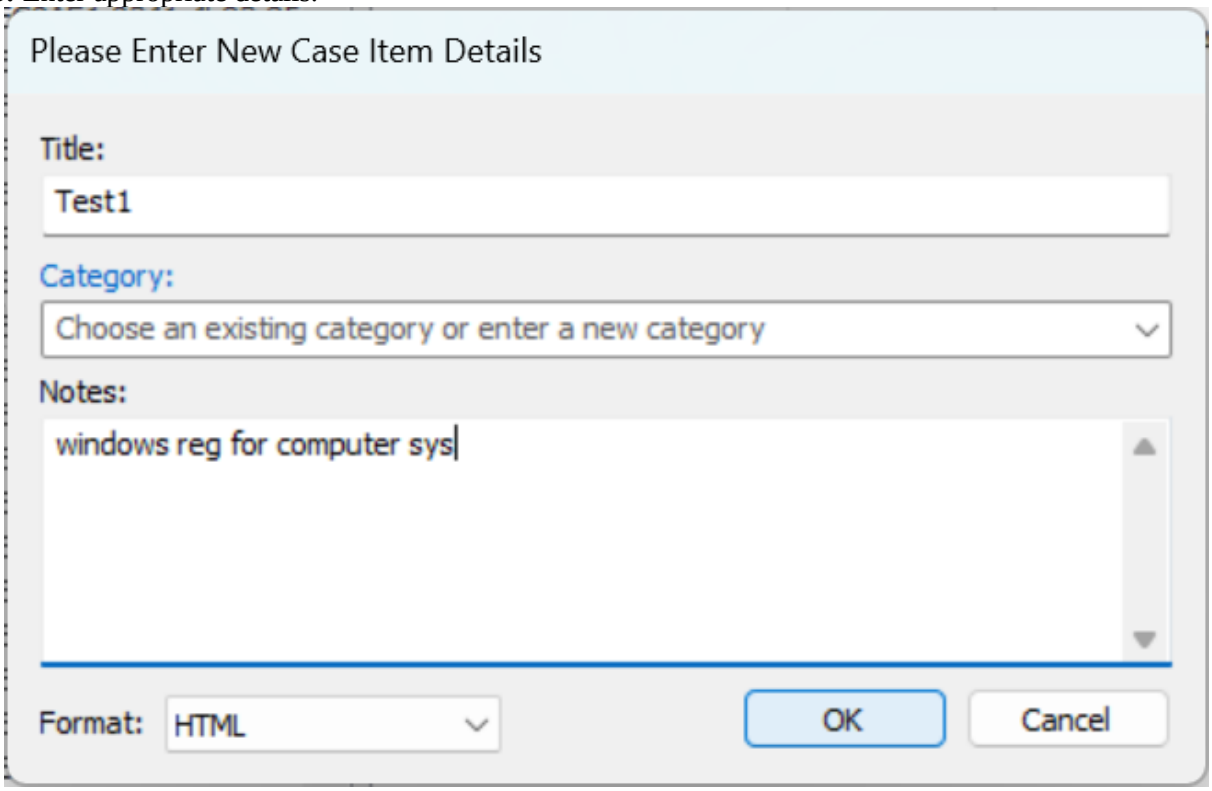




Step 4: Select system file to add a key/value.



Step 5: Enter appropriate details.



Step 6: Select manage case and you can view the reg created.