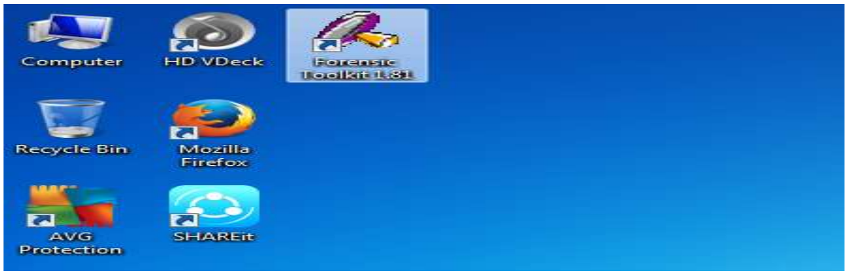
PRACTICAL NO. 03

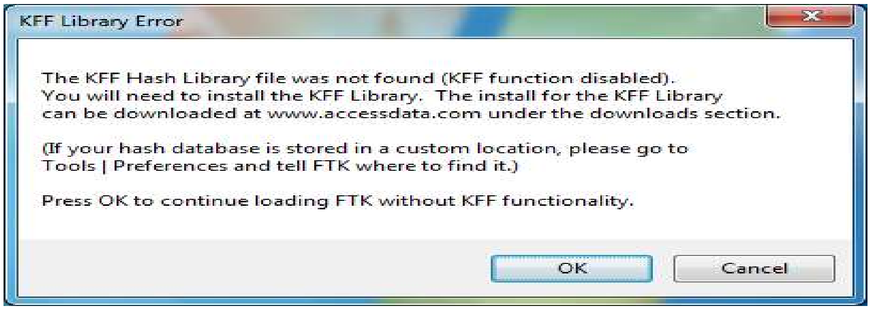
Using Forensic Toolkit (FTK) &Writing report usingFTK (AccessData FTK)

Aim: Using Windows Forensics Tools.

Step 1: Start Forensic Toolkit.



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

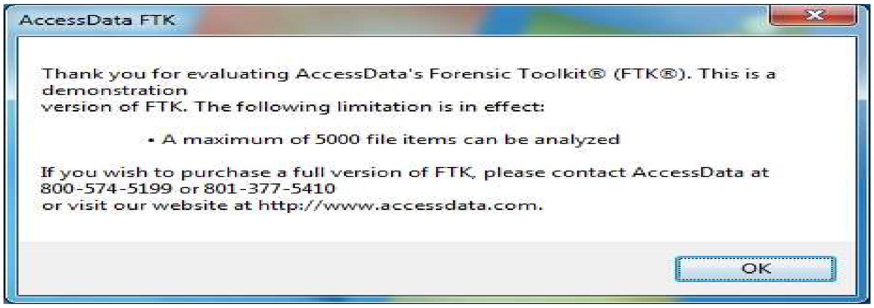

KFF Library Error

The KFF Hash Library file was not found (KFF function disabled).
You will need to install the KFF Library. The install for the KFF Library can be downloaded at www.accessdata.com under the downloads section.

(If your hash database is stored in a custom location, please go to Tools | Preferences and tell FTK where to find it.)

Press OK to continue loading FTK without KFF functionality.

Step 3: click on OK button.

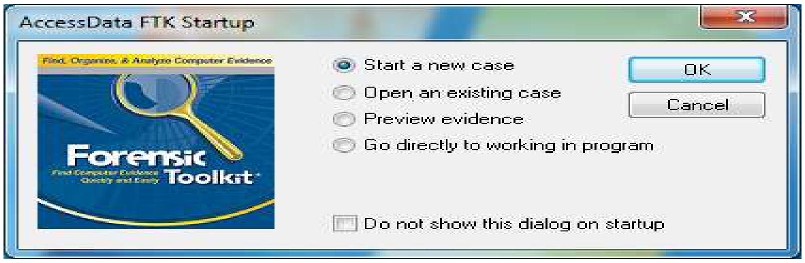

AccessData FTK

Thank you for evaluating AccessData's Forensic Toolkit® (FTK®). This is a demonstration
version of FTK. The following limitation is in effect:

• A maximum of 5000 file items can be analyzed

If you wish to purchase a full version of FTK, please contact AccessData at 800-574-5199 or 801-377-5410
or visit our website at http://www.accessdata.com.

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

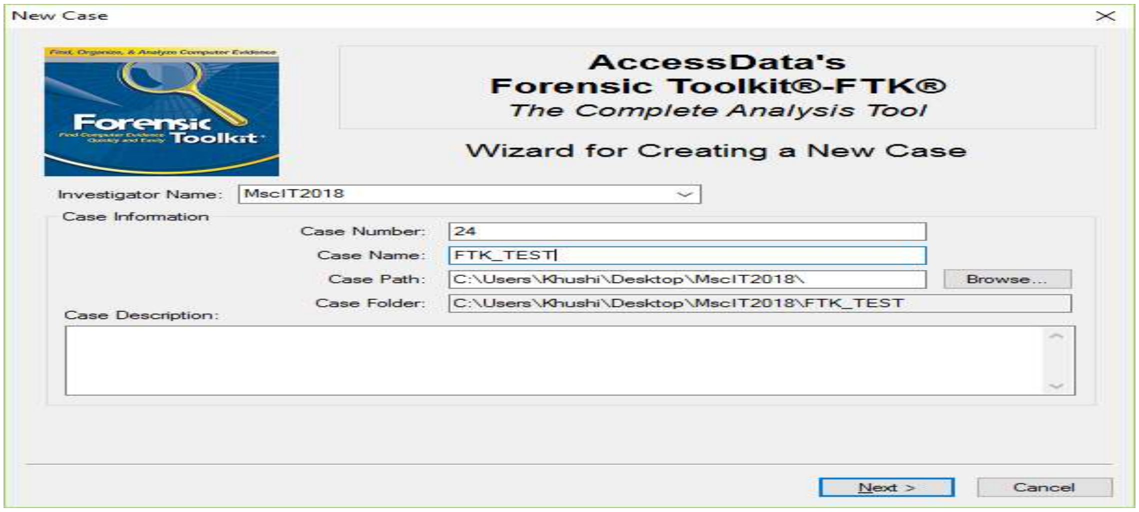

AccessData FTK Startup

● Start a new case
○ Open an existing case
○ Preview evidence
○ Go directly to working in program

□ Do not show this dialog on startup

Find, Organize, & Analyze Computer Evidence
Forensic Toolkit
Find Computer Evidence Quickly and Easily
OK
Cancel

Step 5: Enter the detail for a New case.



Investigator Name: MscIT2018

Case Information

Case Number: 24

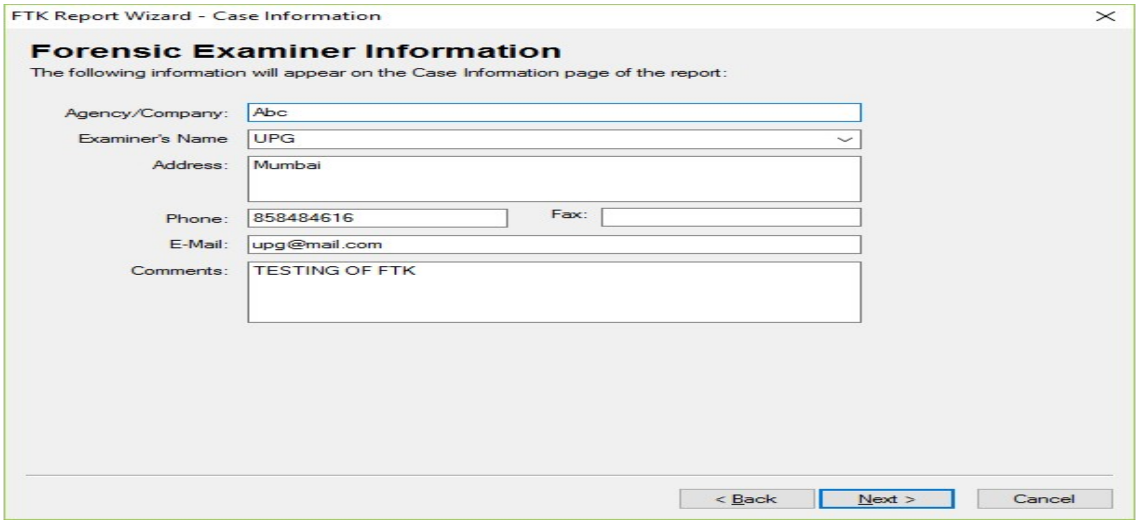
Case Name: FTK_TEST

Case Path: C:\Users\Khushi\Desktop\MscIT2018\

Case Folder: C:\Users\Khushi\Desktop\MscIT2018\FTK_TEST

Case Description:

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



Forensic Examiner Information

The following information will appear on the Case Information page of the report:

Agency/Company: Abc

Examiner's Name: UPG

Address: Mumbai

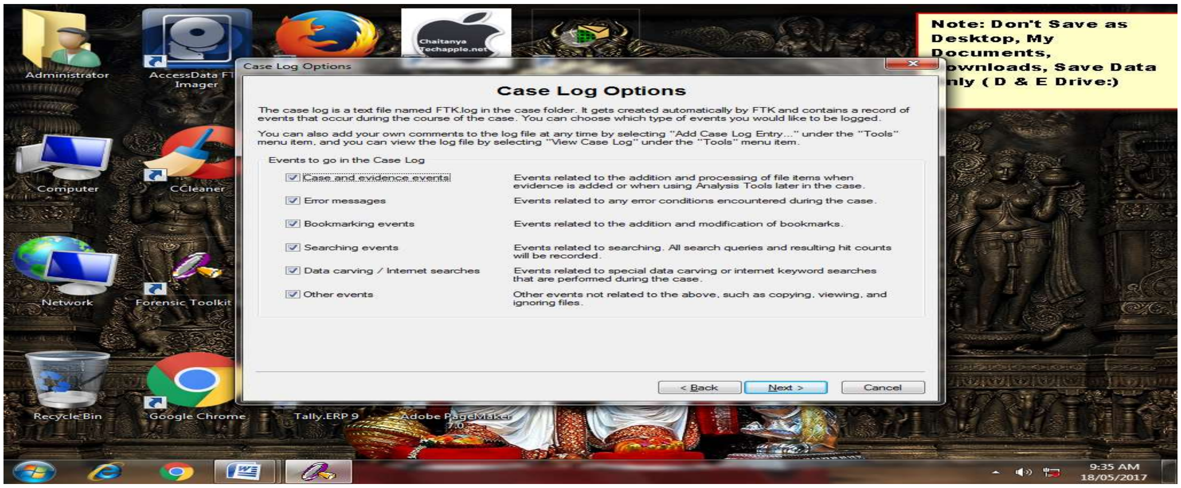
Phone: 858484616

Fax:

E-Mail: upg@mail.com

Comments: TESTING OF FTK

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



Case Log Options

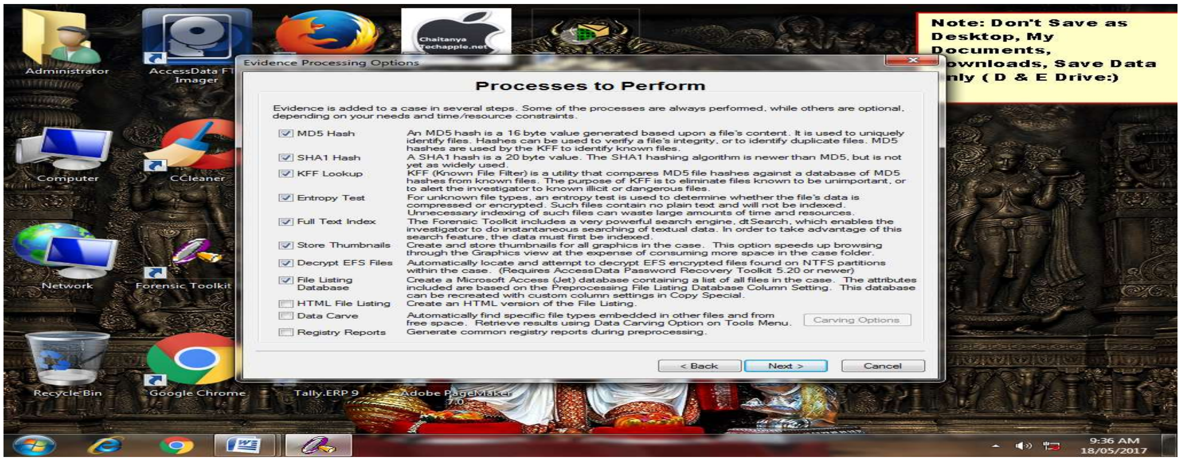
The case log is a text file named FTK.log in the case folder. It gets created automatically by FTK and contains a record of events that occur during the course of the case. You can choose which type of events you would like to be logged.

You can also add your own comments to the log file at any time by selecting "Add Case Log Entry..." under the "Tools" menu item, and you can view the log file by selecting "View Case Log" under the "Tools" menu item.

Events to go in the Case Log

☑ Case and evidence events	Events related to the addition and processing of file items when evidence is added or when using Analysis Tools later in the case.
☑ Error messages	Events related to any error conditions encountered during the case.
☑ Bookmarking events	Events related to the addition and modification of bookmarks.
☑ Searching events	Events related to searching. All search queries and resulting hit counts will be recorded.
☑ Data carving / Internet searches	Events related to special data carving or internet keyword searches that are performed during the case.
☑ Other events	Other events not related to the above, such as copying, viewing, and ignoring files.

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



Evidence Processing Options

Processes to Perform

Evidence is added to a case in several steps. Some of the processes are always performed, while others are optional, depending on your needs and time/resource constraints.

☑ MD5 Hash — An MD5 hash is a 16 byte value generated based upon a file's content. It is used to uniquely identify files. Hashes can be used to verify a file's integrity, or to identify duplicate files. MD5 hashes are used by the KFF to identify known files.

☑ SHA1 Hash — A SHA1 hash is a 20 byte value. The SHA1 hashing algorithm is newer than MD5, but is not yet as widely used.

☑ KFF Lookup — KFF (Known File Filter) is a utility that compares MD5 file hashes against a database of MD5 hashes from known files. The purpose of KFF is to eliminate files known to be unimportant, or to alert the investigator to known illicit or dangerous files.

☑ Entropy Test — For unknown file types, an entropy test is used to determine whether the file's data is compressed or encrypted. Such files contain no plain text and will not be indexed. Unnecessary indexing of such files can waste large amounts of time and resources.

☑ Full Text Index — The Forensic Toolkit includes a very powerful search engine, dtSearch, which enables the investigator to do instantaneous searching of textual data. In order to take advantage of this search feature, the data must first be indexed.

☑ Store Thumbnails — Create and store thumbnails for all graphics in the case. This option speeds up browsing through the Graphics view at the expense of consuming more space in the case folder.

☑ Decrypt EFS Files — Automatically locate and attempt to decrypt EFS encrypted files found on NTFS partitions within the case. (Requires AccessData Password Recovery Toolkit 5.20 or newer)

☑ File Listing Database — Create a Microsoft Access (Jet) database containing a list of all files in the case. The attributes included are based on the Preprocessing File Listing Database Column Setting. This database can be recreated with custom column settings in Copy Special.

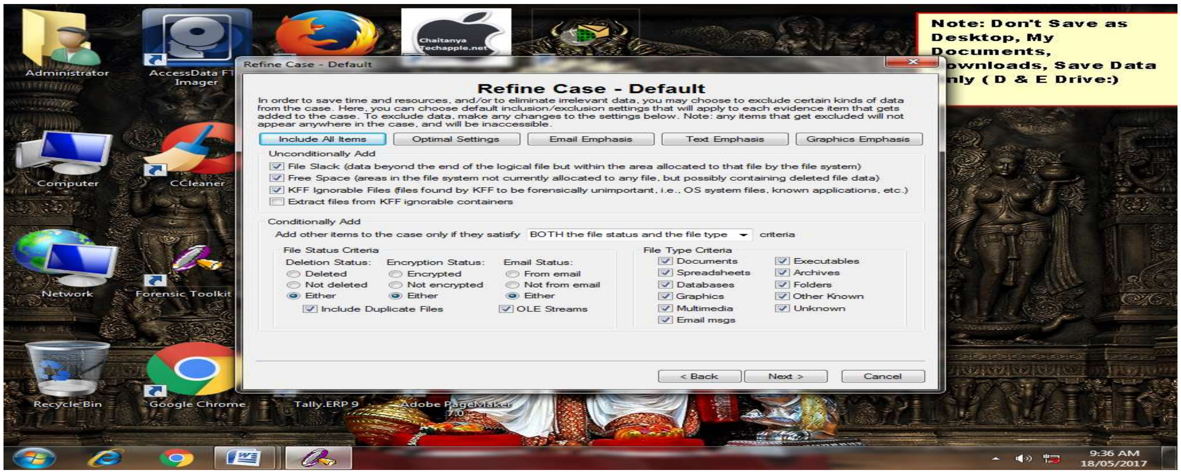
☐ HTML File Listing — Create an HTML version of the File Listing.

☐ Data Carve — Automatically find specific file types embedded in other files and from free space. Retrieve results using Data Carving Option on Tools Menu. [Carving Options]

☐ Registry Reports — Generate common registry reports during preprocessing.

[< Back] [Next >] [Cancel]

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



Refine Case - Default

Refine Case - Default

In order to save time and resources, and/or to eliminate irrelevant data, you may choose to exclude certain kinds of data from the case. Here, you can choose default inclusion/exclusion settings that will apply to each evidence item that gets added to the case. To exclude data, make any changes to the settings below. Note: any items that get excluded will not appear anywhere in the case, and will be inaccessible.

[Include All Items] [Optimal Settings] [Email Emphasis] [Text Emphasis] [Graphics Emphasis]

Unconditionally Add

☑ File Slack (data beyond the end of the logical file but within the area allocated to that file by the file system)
☑ Free Space (areas in the file system not currently allocated to any file, but possibly containing deleted file data)
☑ KFF Ignorable Files (files found by KFF to be forensically unimportant, i.e., OS system files, known applications, etc.)
☐ Extract files from KFF ignorable containers

Conditionally Add

Add other items to the case only if they satisfy [BOTH the file status and the file type ▾] criteria

File Status Criteria

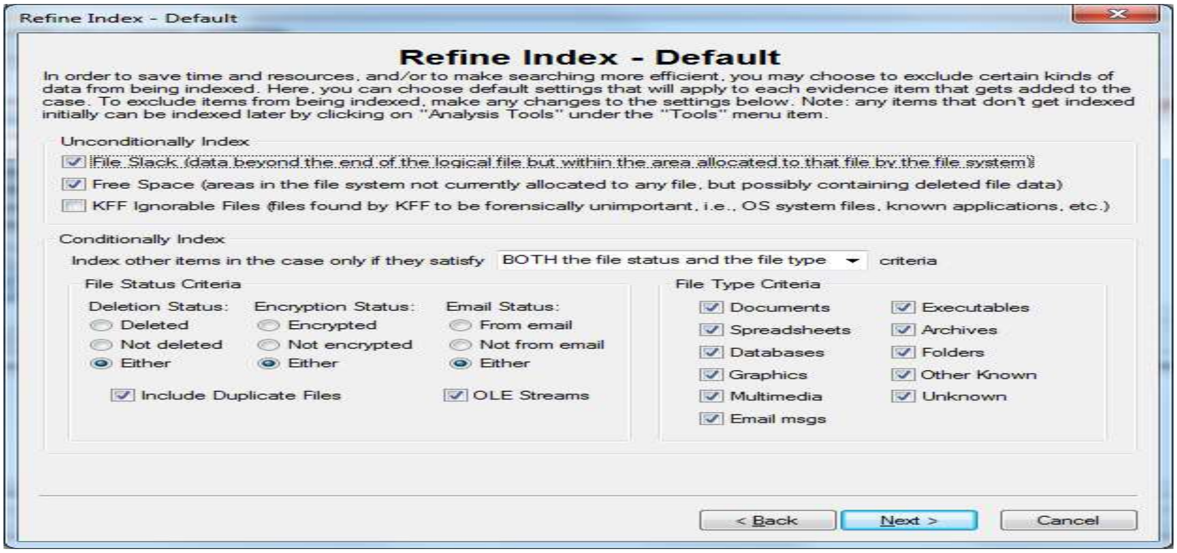
Deletion Status: ○ Deleted ○ Not deleted ● Either
Encryption Status: ○ Encrypted ○ Not encrypted ● Either
Email Status: ○ From email ○ Not from email ● Either
☑ Include Duplicate Files
☑ OLE Streams

File Type Criteria

☑ Documents ☑ Executables
☑ Spreadsheets ☑ Archives
☑ Databases ☑ Folders
☑ Graphics ☑ Other Known
☑ Multimedia ☑ Unknown
☑ Email msgs

[< Back] [Next >] [Cancel]

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



Refine Index - Default

Refine Index - Default

In order to save time and resources, and/or to make searching more efficient, you may choose to exclude certain kinds of data from being indexed. Here, you can choose default settings that will apply to each evidence item that gets added to the case. To exclude items from being indexed, make any changes to the settings below. Note: any items that don't get indexed initially can be indexed later by clicking on "Analysis Tools" under the "Tools" menu item.

Unconditionally Index

☑ File Slack (data beyond the end of the logical file but within the area allocated to that file by the file system)
☑ Free Space (areas in the file system not currently allocated to any file, but possibly containing deleted file data)
☐ KFF Ignorable Files (files found by KFF to be forensically unimportant, i.e., OS system files, known applications, etc.)

Conditionally Index

Index other items in the case only if they satisfy [BOTH the file status and the file type ▾] criteria

File Status Criteria

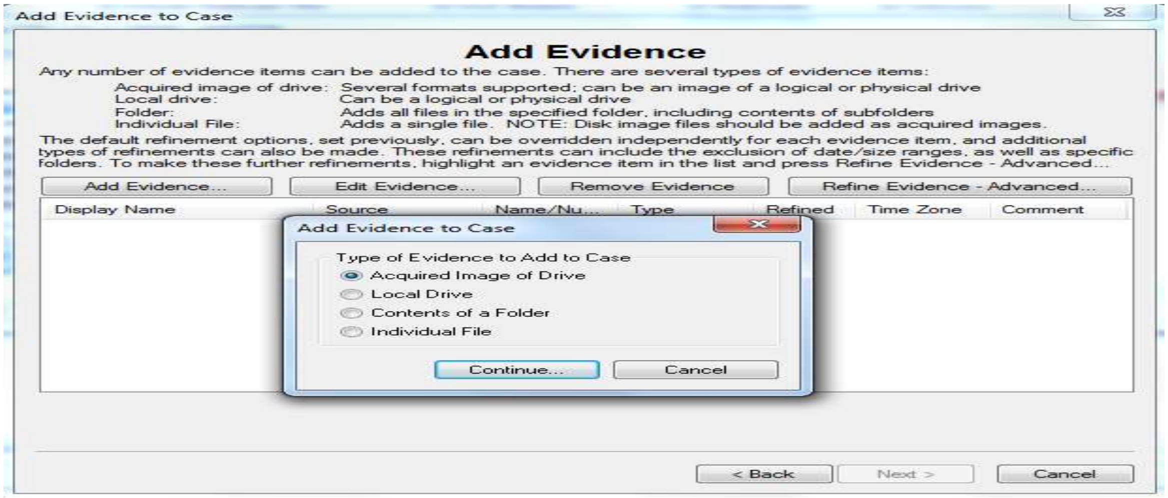
Deletion Status: ○ Deleted ○ Not deleted ● Either
Encryption Status: ○ Encrypted ○ Not encrypted ● Either
Email Status: ○ From email ○ Not from email ● Either
☑ Include Duplicate Files
☑ OLE Streams

File Type Criteria

☑ Documents ☑ Executables
☑ Spreadsheets ☑ Archives
☑ Databases ☑ Folders
☑ Graphics ☑ Other Known
☑ Multimedia ☑ Unknown
☑ Email msgs

[< Back] [Next >] [Cancel]

Step 11: Now here Click on add Evidence button.



Add Evidence to Case

Add Evidence

Any number of evidence items can be added to the case. There are several types of evidence items:

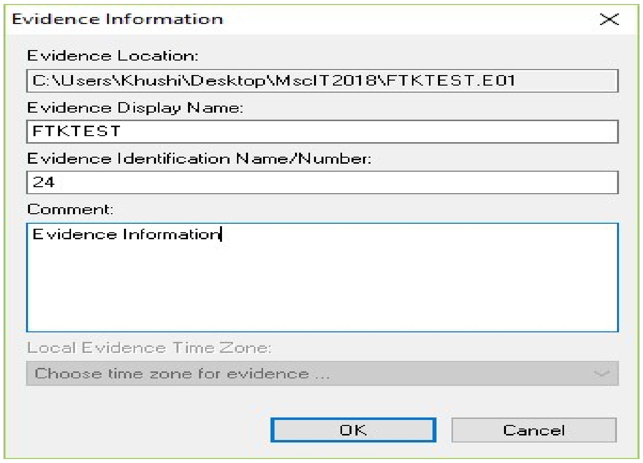
Acquired image of drive: Several formats supported; can be an image of a logical or physical drive
Local drive: Can be a logical or physical drive
Folder: Adds all files in the specified folder, including contents of subfolders
Individual File: Adds a single file. NOTE: Disk image files should be added as acquired images.

The default refinement options, set previously, can be overridden independently for each evidence item, and additional types of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specific folders. To make these further refinements, highlight an evidence item in the list and press Refine Evidence - Advanced...

Add Evidence to Case

Type of Evidence to Add to Case
● Acquired Image of Drive
○ Local Drive
○ Contents of a Folder
○ Individual File

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



Evidence Information

Evidence Location:
C:\Users\Khushi\Desktop\MscIT2018\FTKTEST.E01

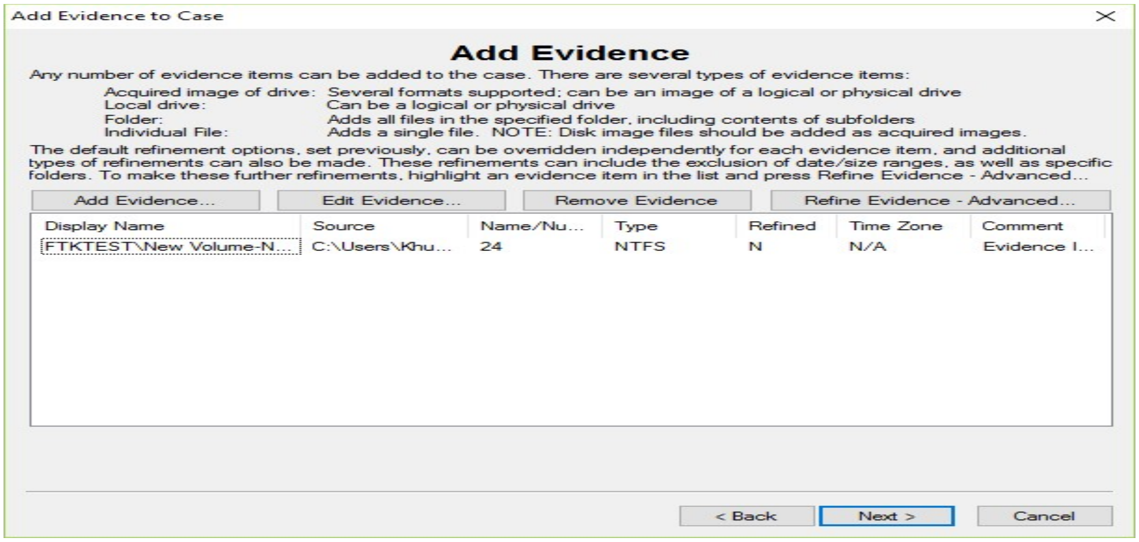
Evidence Display Name:
FTKTEST

Evidence Identification Name/Number:
24

Comment:
Evidence Information

Local Evidence Time Zone:
Choose time zone for evidence ...

Step 13: Now click on Next.



Add Evidence to Case

Add Evidence

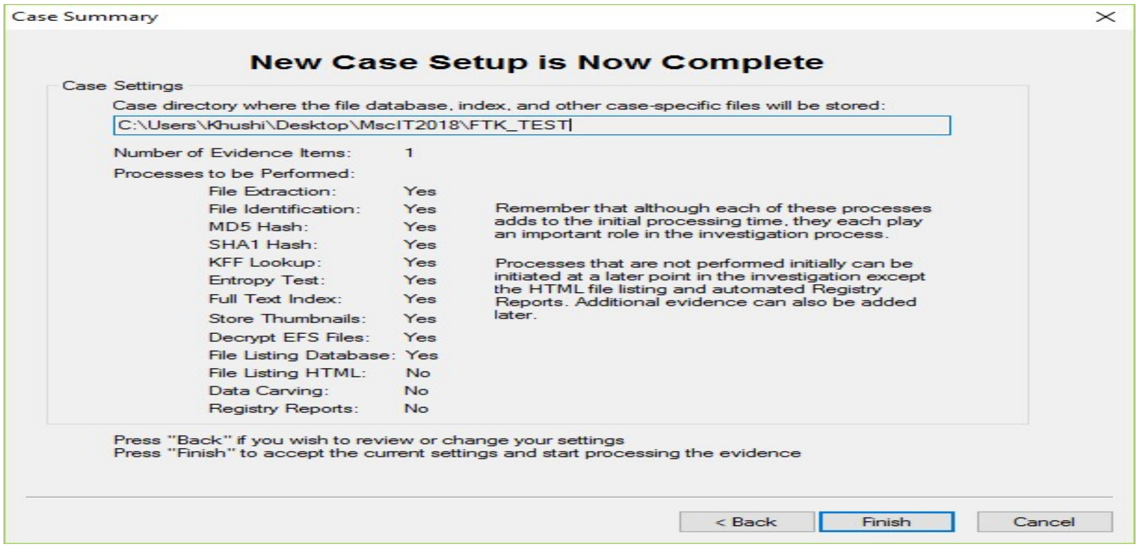
Any number of evidence items can be added to the case. There are several types of evidence items:

Acquired image of drive: Several formats supported; can be an image of a logical or physical drive
Local drive: Can be a logical or physical drive
Folder: Adds all files in the specified folder, including contents of subfolders
Individual File: Adds a single file. NOTE: Disk image files should be added as acquired images.

The default refinement options, set previously, can be overridden independently for each evidence item, and additional types of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specific folders. To make these further refinements, highlight an evidence item in the list and press Refine Evidence - Advanced...

Display Name	Source	Name/Nu...	Type	Refined	Time Zone	Comment
FTKTEST\New Volume-N...	C:\Users\Khu...	24	NTFS	N	N/A	Evidence I...

Step 14: Click on Finish to initiate the analysis.



Case Summary

New Case Setup is Now Complete

Case Settings

Case directory where the file database, index, and other case-specific files will be stored:
C:\Users\Khushi\Desktop\MscIT2018\FTK_TEST

Number of Evidence Items: 1

Processes to be Performed:

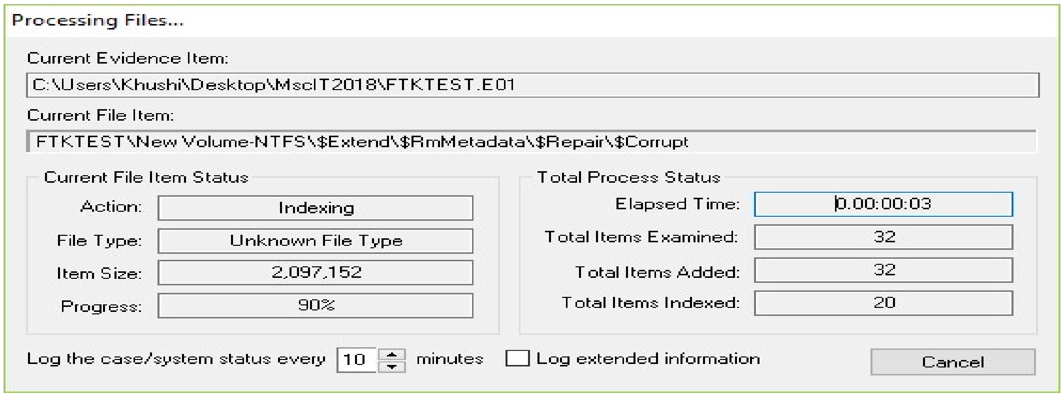
File Extraction:	Yes
File Identification:	Yes
MD5 Hash:	Yes
SHA1 Hash:	Yes
KFF Lookup:	Yes
Entropy Test:	Yes
Full Text Index:	Yes
Store Thumbnails:	Yes
Decrypt EFS Files:	Yes
File Listing Database:	Yes
File Listing HTML:	No
Data Carving:	No
Registry Reports:	No

Remember that although each of these processes adds to the initial processing time, they each play an important role in the investigation process.

Processes that are not performed initially can be initiated at a later point in the investigation except the HTML file listing and automated Registry Reports. Additional evidence can also be added later.

Press "Back" if you wish to review or change your settings
Press "Finish" to accept the current settings and start processing the evidence

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



Processing Files...

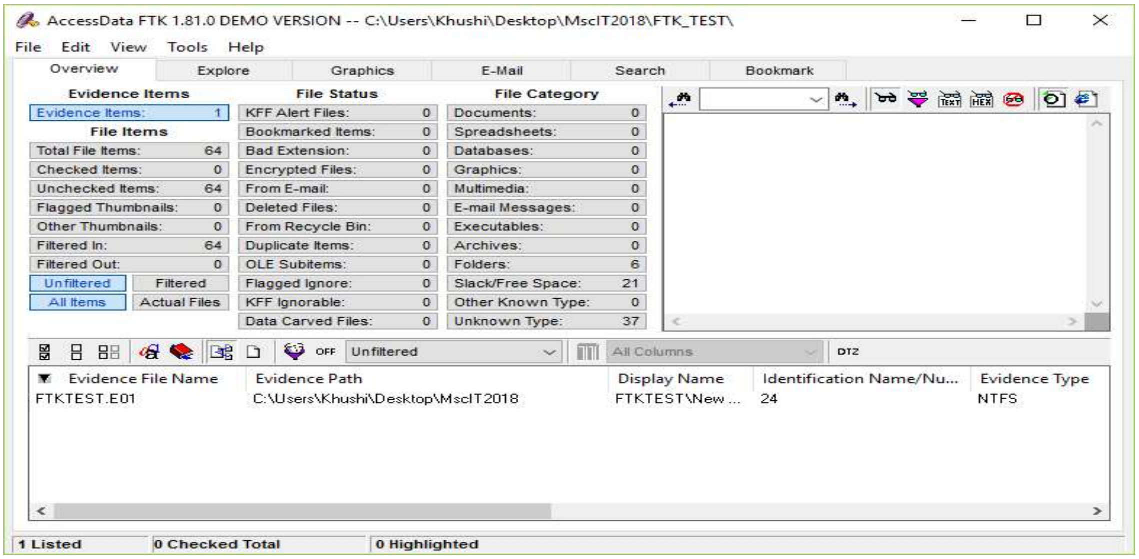
Current Evidence Item:
C:\Users\Khushi\Desktop\MscIT2018\FTKTEST.E01

Current File Item:
FTKTEST\New Volume-NTFS\$Extend\$RmMetadata\$Repair\$Corrupt

Current File Item Status		Total Process Status	
Action:	Indexing	Elapsed Time:	0.00:00:03
File Type:	Unknown File Type	Total Items Examined:	32
Item Size:	2,097,152	Total Items Added:	32
Progress:	90%	Total Items Indexed:	20

Log the case/system status every 10 minutes □ Log extended information

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



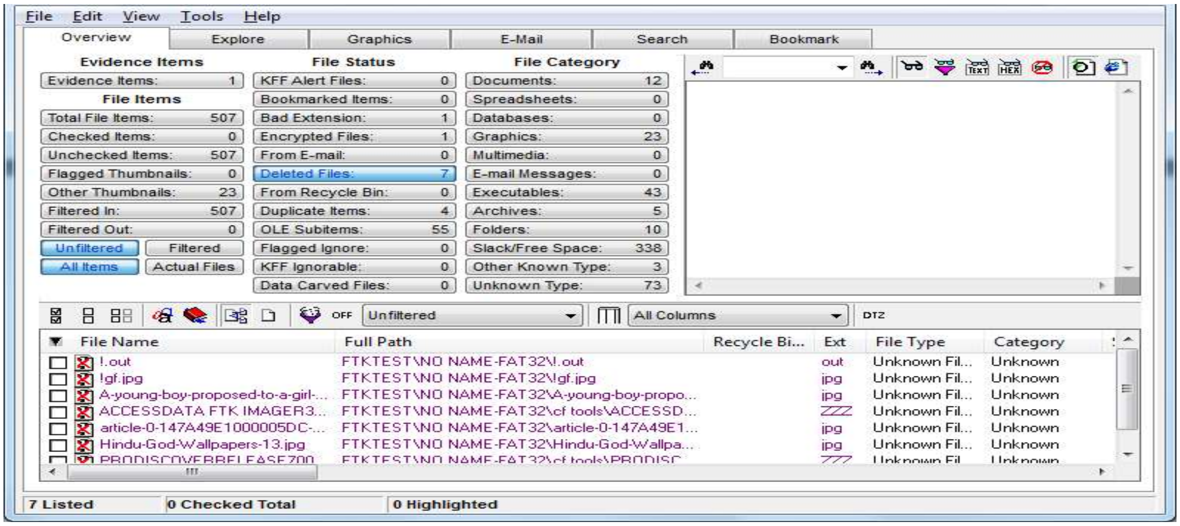
AccessData FTK 1.81.0 DEMO VERSION -- C:\Users\Khushi\Desktop\MscIT2018\FTK_TEST\

Evidence Items		File Status		File Category	
Evidence Items:	1	KFF Alert Files:	0	Documents:	0
File Items		Bookmarked Items:	0	Spreadsheets:	0
Total File Items:	64	Bad Extension:	0	Databases:	0
Checked Items:	0	Encrypted Files:	0	Graphics:	0
Unchecked Items:	64	From E-mail:	0	Multimedia:	0
Flagged Thumbnails:	0	Deleted Files:	0	E-mail Messages:	0
Other Thumbnails:	0	From Recycle Bin:	0	Executables:	0
Filtered In:	64	Duplicate Items:	0	Archives:	0
Filtered Out:	0	OLE Subitems:	0	Folders:	6
Unfiltered	Filtered	Flagged Ignore:	0	Slack/Free Space:	21
All Items	Actual Files	KFF Ignorable:	0	Other Known Type:	0
		Data Carved Files:	0	Unknown Type:	37

Evidence File Name	Evidence Path	Display Name	Identification Name/Nu...	Evidence Type
FTKTEST.E01	C:\Users\Khushi\Desktop\MscIT2018	FTKTEST\New ...	24	NTFS

1 Listed | 0 Checked Total | 0 Highlighted

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



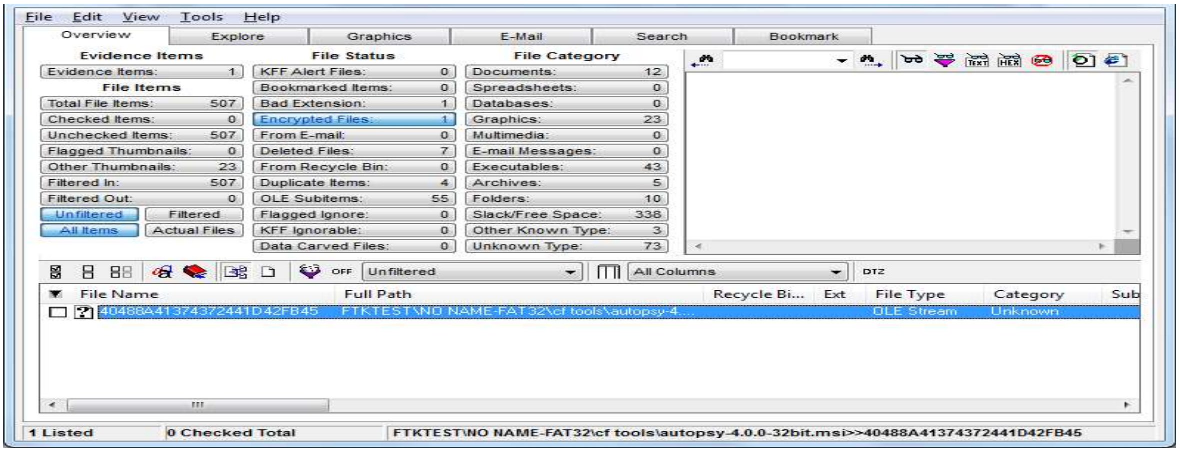
Evidence Items	File Status	File Category
Evidence Items: 1	KFF Alert Files: 0	Documents: 12
File Items	Bookmarked Items: 0	Spreadsheets: 0
Total File Items: 507	Bad Extension: 1	Databases: 0
Checked Items: 0	Encrypted Files: 1	Graphics: 23
Unchecked Items: 507	From E-mail: 0	Multimedia: 0
Flagged Thumbnails: 0	Deleted Files: 7	E-mail Messages: 0
Other Thumbnails: 23	From Recycle Bin: 0	Executables: 43
Filtered In: 507	Duplicate Items: 4	Archives: 5
Filtered Out: 0	OLE Subitems: 55	Folders: 10
	Flagged Ignore: 0	Slack/Free Space: 338
	KFF Ignorable: 0	Other Known Type: 3
	Data Carved Files: 0	Unknown Type: 73

Unfiltered | All Columns

File Name	Full Path	Recycle Bi...	Ext	File Type	Category
!.out	FTKTEST\NO NAME-FAT32\!.out		out	Unknown Fil...	Unknown
!gf.jpg	FTKTEST\NO NAME-FAT32\!gf.jpg		jpg	Unknown Fil...	Unknown
A-young-boy-proposed-to-a-girl-...	FTKTEST\NO NAME-FAT32\A-young-boy-propo...		jpg	Unknown Fil...	Unknown
ACCESSDATA FTK IMAGER3...	FTKTEST\NO NAME-FAT32\cf tools\ACCESSD...		ZZZ	Unknown Fil...	Unknown
article-0-147A49E1000005DC-...	FTKTEST\NO NAME-FAT32\article-0-147A49E1...		jpg	Unknown Fil...	Unknown
Hindu-God-Wallpapers-13.jpg	FTKTEST\NO NAME-FAT32\Hindu-God-Wallpa...		jpg	Unknown Fil...	Unknown
PRODISCOVERRELEASE700	FTKTEST\NO NAME-FAT32\cf tools\PRODISC		ZZZ	Unknown Fil	Unknown

7 Listed | 0 Checked Total | 0 Highlighted

Step 18: Select Encrypted Files to view.



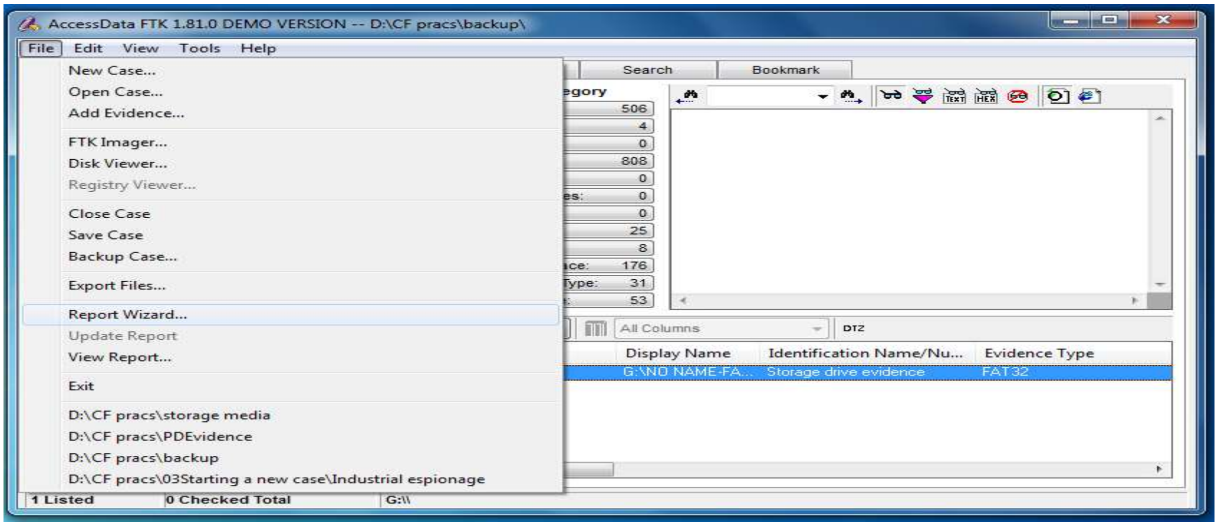
Evidence Items	File Status	File Category
Evidence Items: 1	KFF Alert Files: 0	Documents: 12
File Items	Bookmarked Items: 0	Spreadsheets: 0
Total File Items: 507	Bad Extension: 1	Databases: 0
Checked Items: 0	Encrypted Files: 1	Graphics: 23
Unchecked Items: 507	From E-mail: 0	Multimedia: 0
Flagged Thumbnails: 0	Deleted Files: 7	E-mail Messages: 0
Other Thumbnails: 23	From Recycle Bin: 0	Executables: 43
Filtered In: 507	Duplicate Items: 4	Archives: 5
Filtered Out: 0	OLE Subitems: 55	Folders: 10
	Flagged Ignore: 0	Slack/Free Space: 338
	KFF Ignorable: 0	Other Known Type: 3
	Data Carved Files: 0	Unknown Type: 73

Unfiltered | All Columns

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

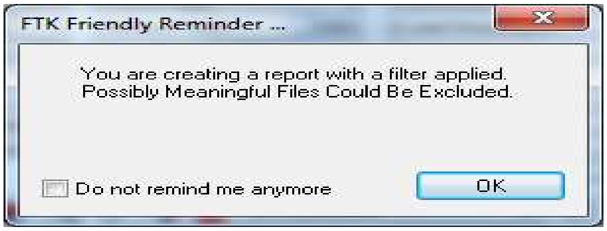
1 Listed | 0 Checked Total | FTKTEST\NO NAME-FAT32\cf tools\autopsy-4.0.0-32bit.msi>>40488A41374372441D42FB45

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


AccessData FTK 1.81.0 DEMO VERSION -- D:\CF pracs\backup\

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

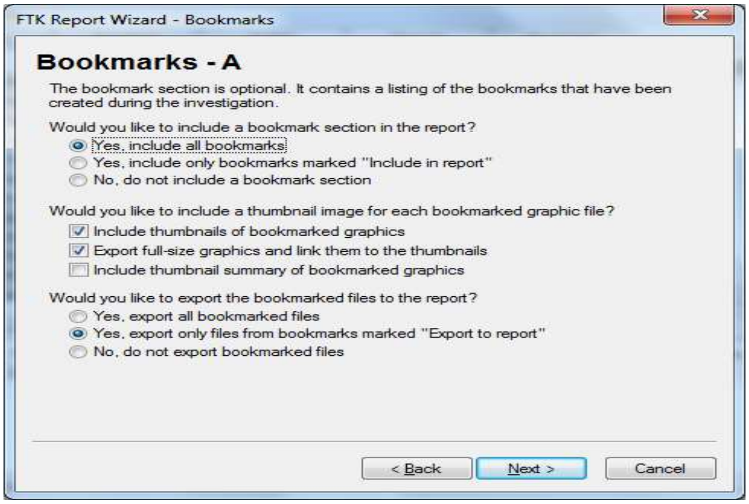
1 Listed | 0 Checked Total | G:\\



You are creating a report with a filter applied.
Possibly Meaningful Files Could Be Excluded.

□ Do not remind me anymore

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



Bookmarks - A

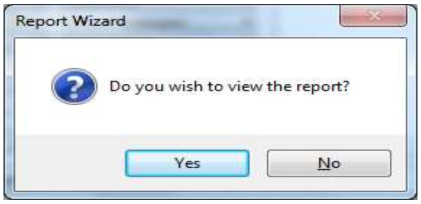
The bookmark section is optional. It contains a listing of the bookmarks that have been created during the investigation.

Would you like to include a bookmark section in the report?
- ● Yes, include all bookmarks
- ○ Yes, include only bookmarks marked "Include in report"
- ○ No, do not include a bookmark section

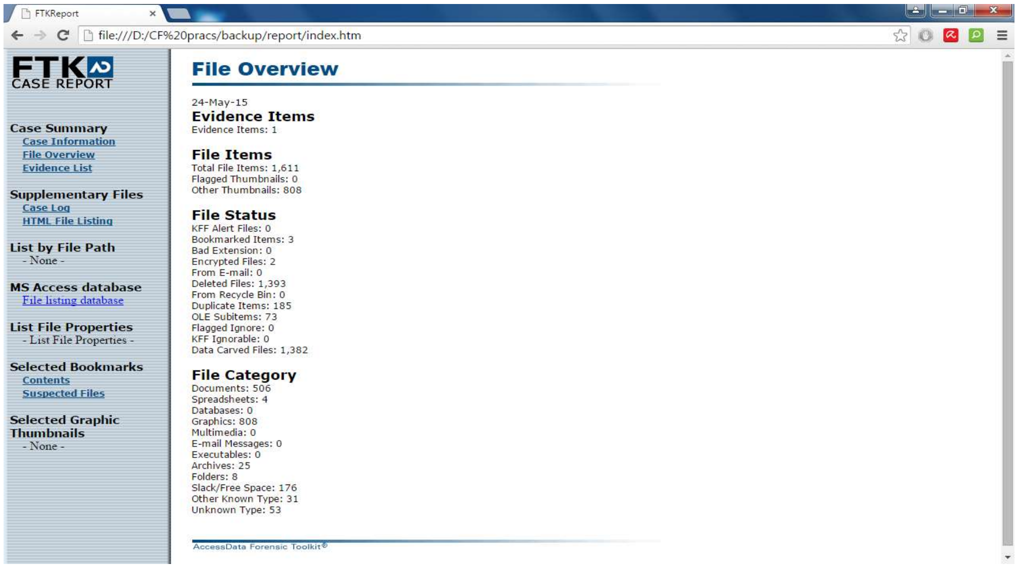
Would you like to include a thumbnail image for each bookmarked graphic file?
- ☑ Include thumbnails of bookmarked graphics
- ☑ Export full-size graphics and link them to the thumbnails
- □ Include thumbnail summary of bookmarked graphics

Would you like to export the bookmarked files to the report?
- ○ Yes, export all bookmarked files
- ● Yes, export only files from bookmarks marked "Export to report"
- ○ No, do not export bookmarked files

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



Do you wish to view the report?



Case Summary
- Case Information
- File Overview
- Evidence List

Supplementary Files
- Case Log
- HTML File Listing

List by File Path
- None -

MS Access database
- File listing database

List File Properties
- List File Properties -

Selected Bookmarks
- Contents
- Suspected Files

Selected Graphic Thumbnails
- None -

File Overview

24-May-15

Evidence Items
Evidence Items: 1

File Items
Total File Items: 1,611
Flagged Thumbnails: 0
Other Thumbnails: 808

File Status
KFF Alert Files: 0
Bookmarked Items: 3
Bad Extension: 0
Encrypted Files: 2
From E-mail: 0
Deleted Files: 1,393
From Recycle Bin: 0
Duplicate Items: 185
OLE Subitems: 73
Flagged Ignore: 0
KFF Ignorable: 0
Data Carved Files: 1,382

File Category
Documents: 506
Spreadsheets: 4
Databases: 0
Graphics: 808
Multimedia: 0
E-mail Messages: 0
Executables: 0
Archives: 25
Folders: 8
Slack/Free Space: 176
Other Known Type: 31
Unknown Type: 53

AccessData Forensic Toolkit®