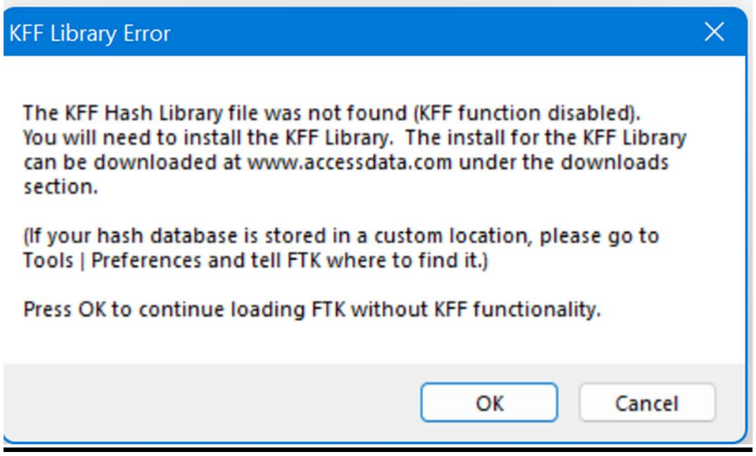
Cyber Forensics Practical 9

Aim:- Email Forensics

- **Mail Service Providers**
- **Email protocols**
- **Recovering emails**
- **Analyzing email header**

Recovering email using AccessData FTK:

1. Start AccessData FTK by right-clicking the AccessData FTK desktop icon, clicking Run asadministrator, and clicking Continue in the UAC message box (if you're using Vista). If you're prompted with a warning message and/or notification (see Figure below), click OK as needed to continue. If asked whether you want to save the existing default case, click Yes.

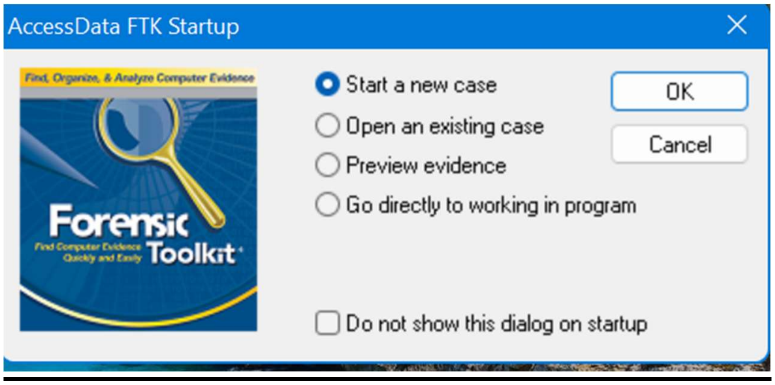


KFF Library Error

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.



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

1. When the AccessData FTK Startup dialog box opens, click Start a new case, and then clickOK.

2. In the New Case dialog box, type your name for the investigator name, and type the case number and case name. Click Browse, navigate to and click your work folder, click OK, andthen click Next.

3. In the Case Information dialog box, enter your investigator information, and then clickNext.

4. Click Next until you reach the Refine Case - Default dialog box, shown in Figure below.

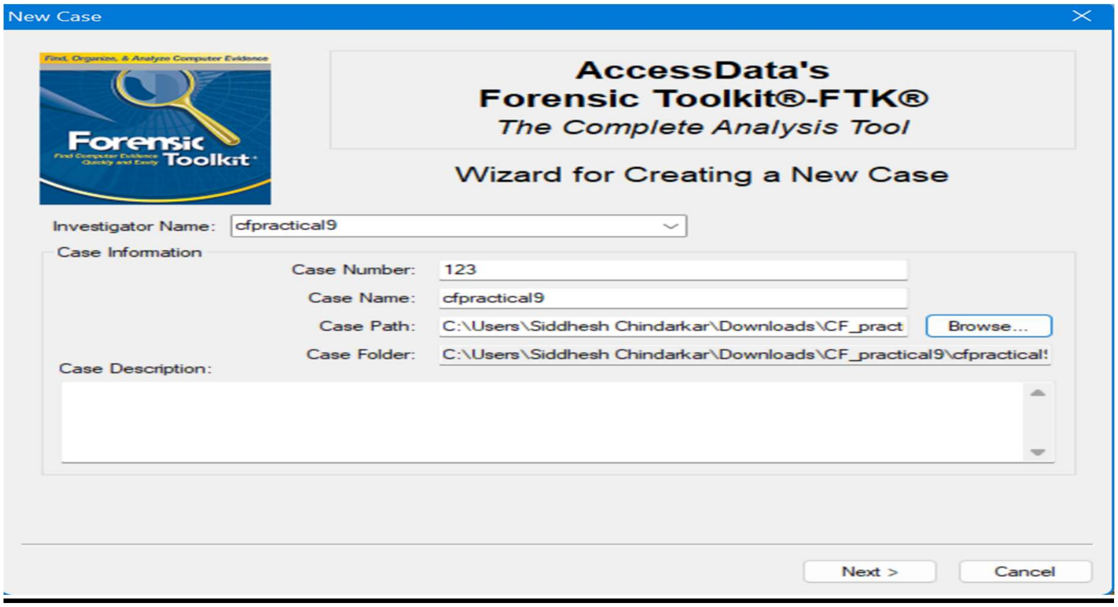
5. Click the Email Emphasis button, and then click Next.

6. Click Next until you reach the Add Evidence to Case dialog box, and then click the AddEvidence button.

7. In the Add Evidence to Case dialog box, click the Individual File option button (see Figurebelow), and then click Continue.

8. In the Select File dialog box, navigate to your work folder, click the Jim_shu's.pst file, andthen click Open.

9. In the Evidence Information dialog box, click OK.


New Case
Find, Organize, & Analyze Computer Evidence
Forensic Toolkit
Find Computer Evidence Quickly and Easily
AccessData's
Forensic Toolkit®-FTK®
The Complete Analysis Tool
Wizard for Creating a New Case
Case Information
Case Description:
Browse...
Next >
Cancel

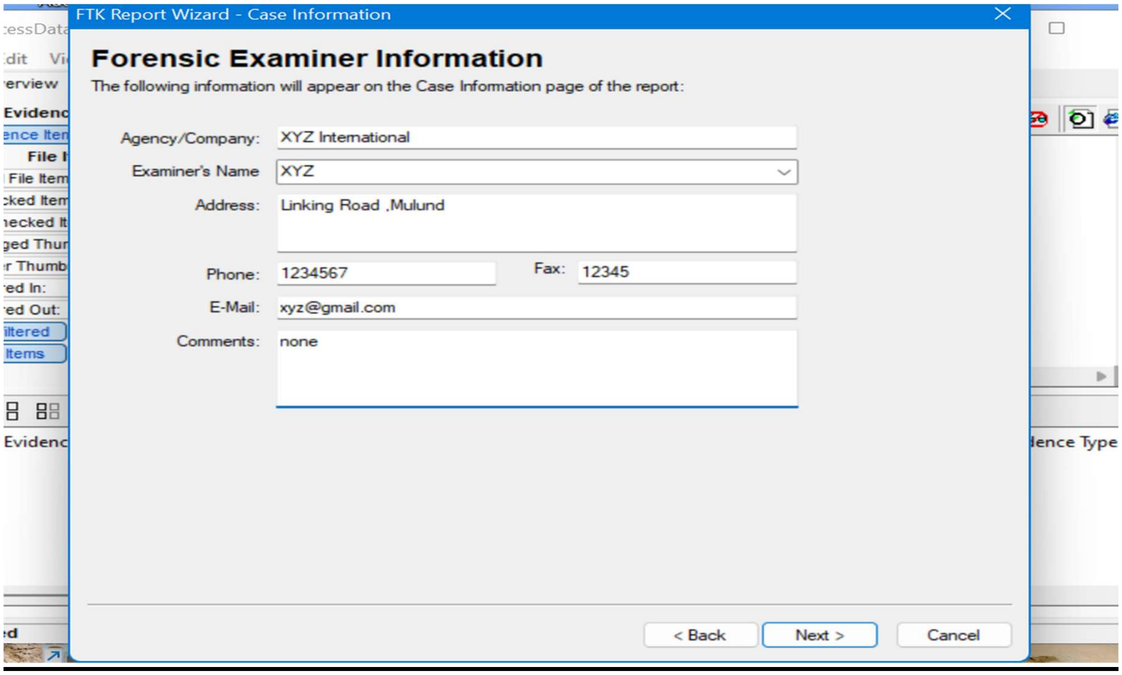
Investigator Name: cfpractical9

Case Number: 123

Case Name: cfpractical9

Case Path: C:\Users\Siddhesh Chindarkar\Downloads\CF_pract

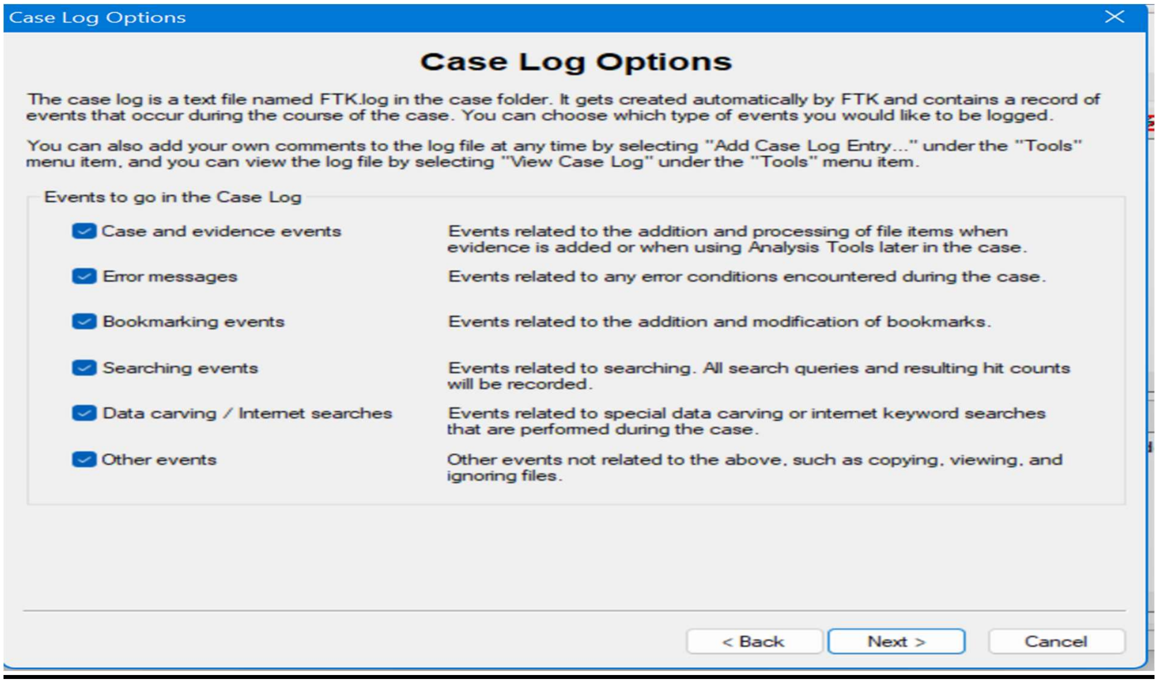
Case Folder: C:\Users\Siddhesh Chindarkar\Downloads\CF_practical9\cfpractical!



Forensic Examiner Information

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

Agency/Company: XYZ International
Examiner's Name: XYZ
Address: Linking Road ,Mulund
Phone: 1234567
Fax: 12345
E-Mail: xyz@gmail.com
Comments: none



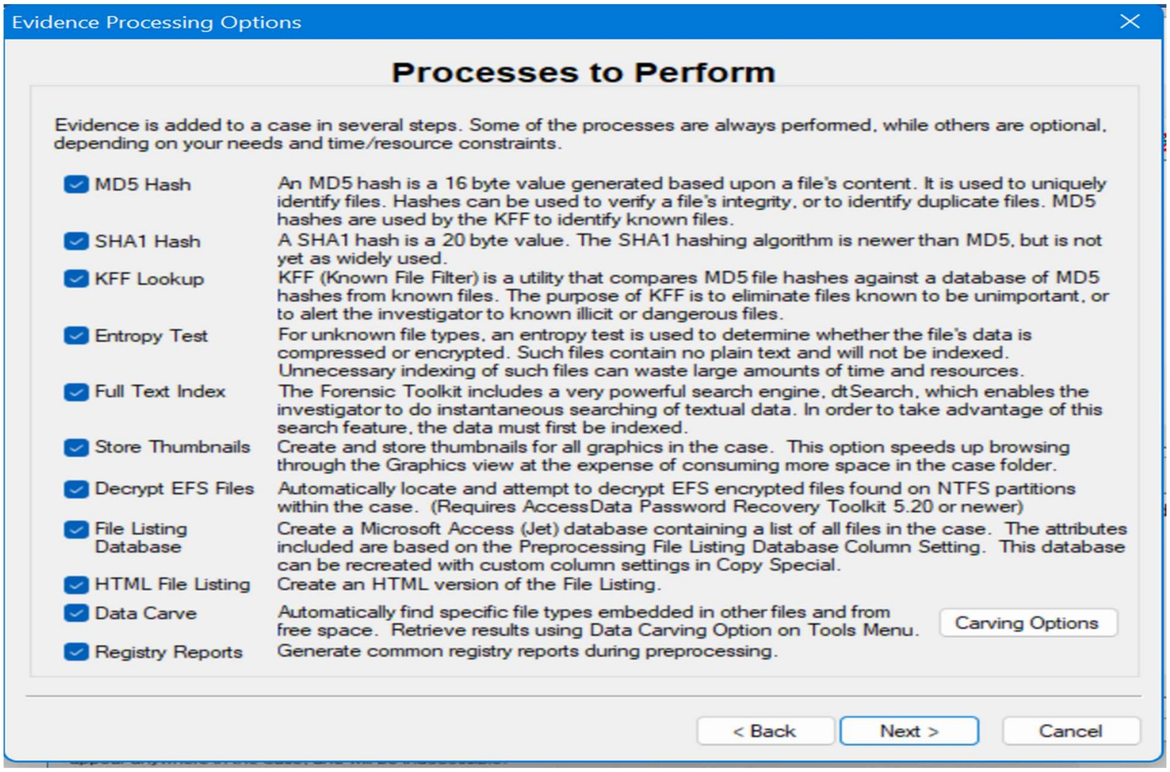
Case Log Options

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.

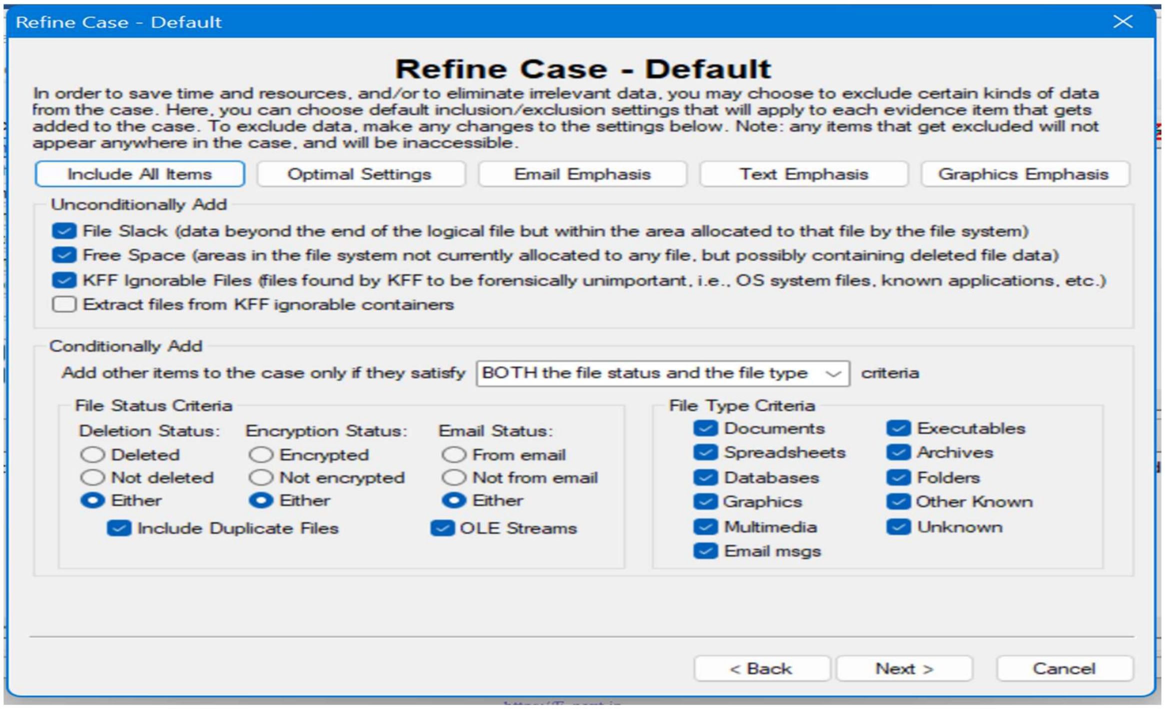


Evidence Processing Options

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.
☑ Registry Reports	Generate common registry reports during preprocessing.



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.

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

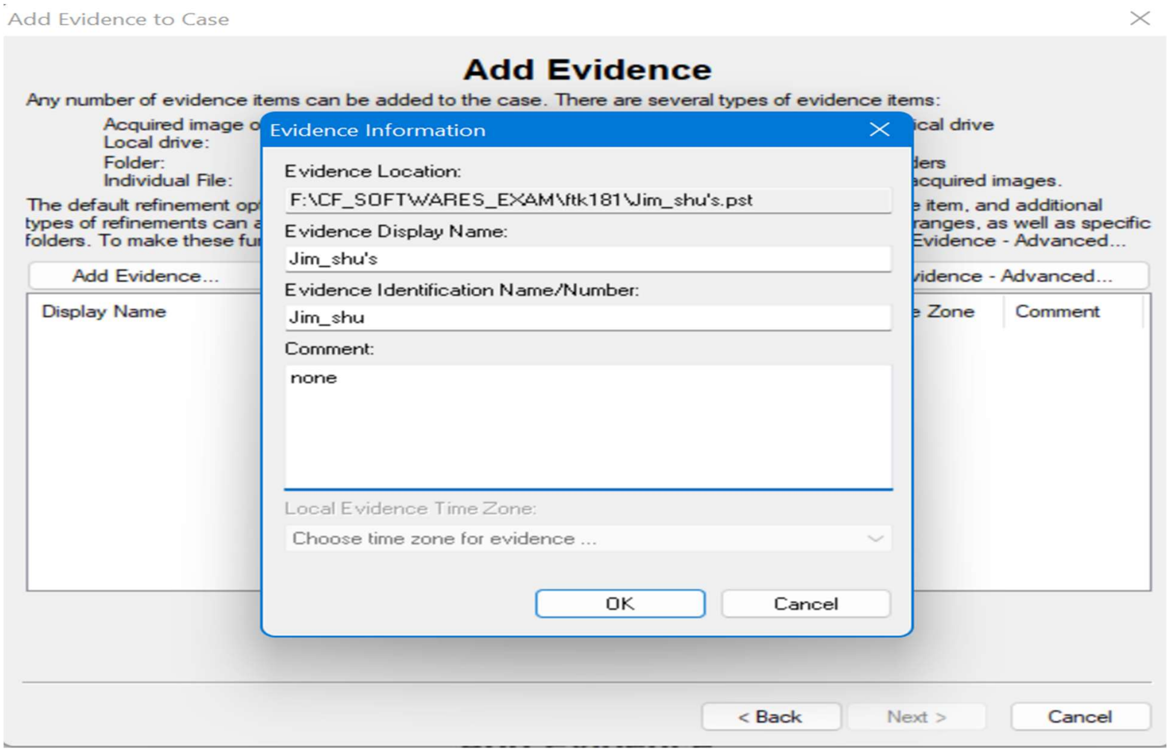
File Status Criteria

Deletion Status:	Encryption Status:	Email Status:
○ Deleted	○ Encrypted	○ From email
○ Not deleted	○ Not encrypted	○ Not from email
● Either	● Either	● Either

☑ Include Duplicate Files ☑ OLE Streams

File Type Criteria

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



Evidence Information

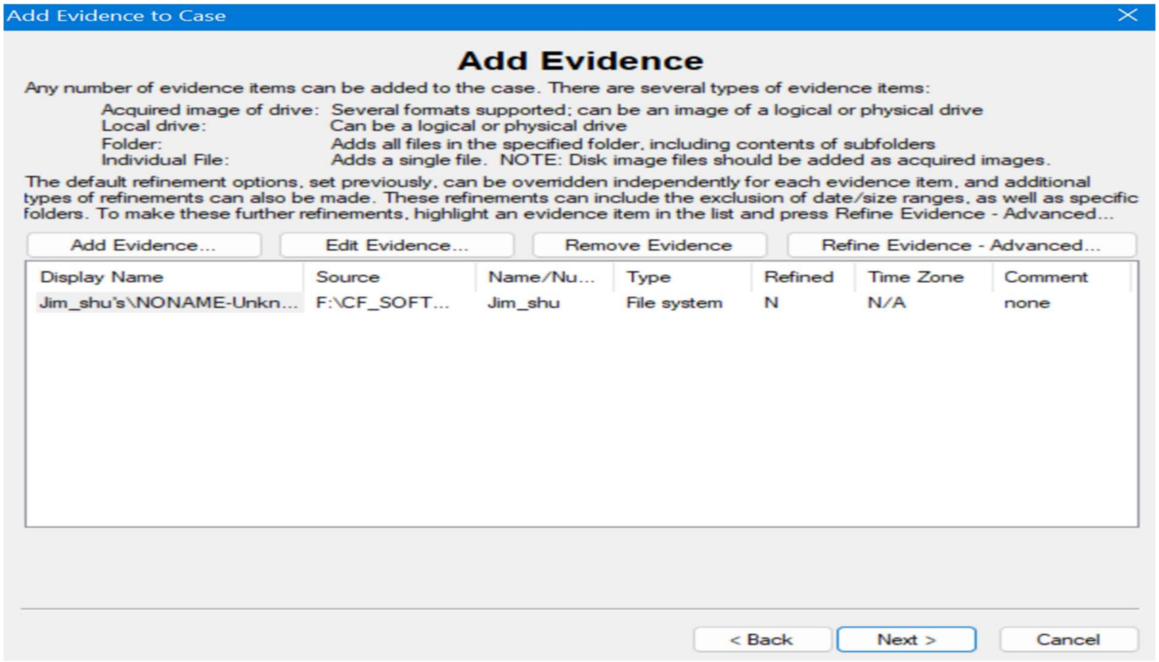
Evidence Location:
F:\CF_SOFTWARES_EXAM\ftk181\Jim_shu's.pst

Evidence Display Name:
Jim_shu's

Evidence Identification Name/Number:
Jim_shu

Comment:
none

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



Add Evidence to Case

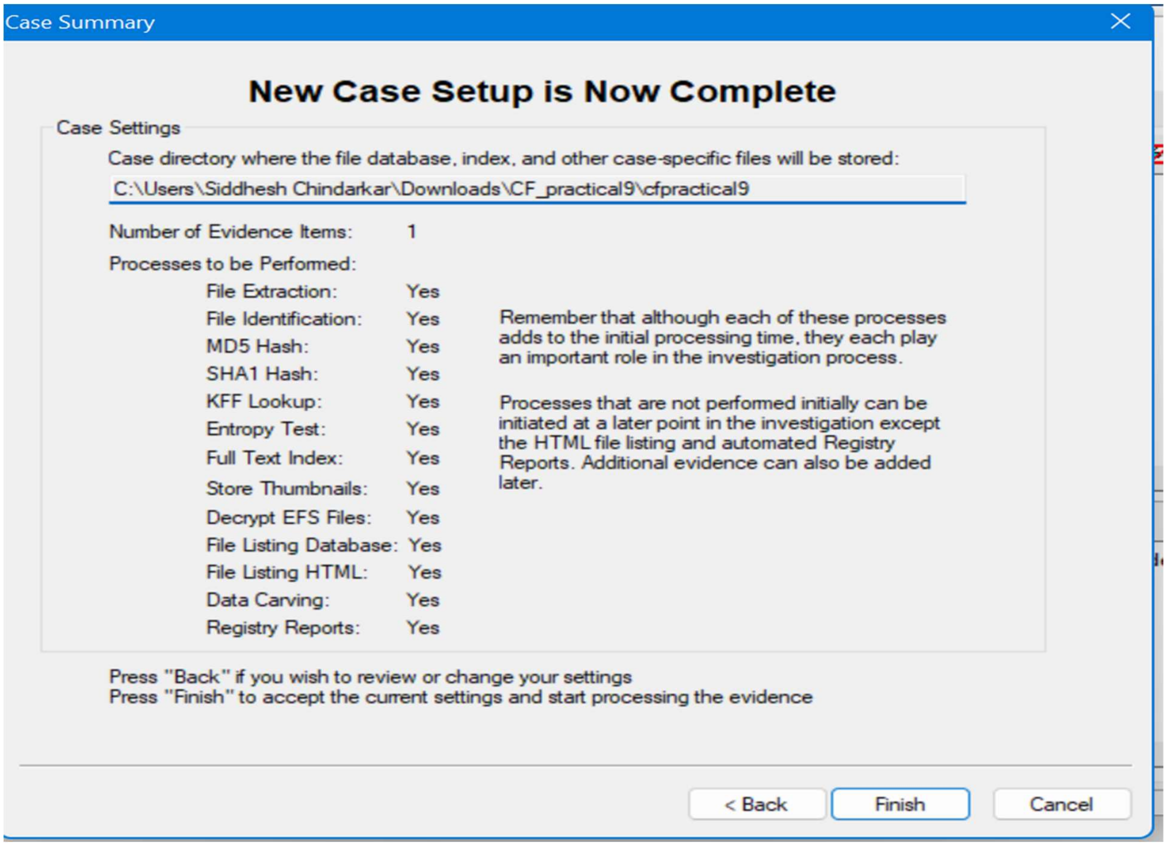
Add Evidence

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
Jim_shu's\NONAME-Unkn...	F:\CF_SOFT...	Jim_shu	File system	N	N/A	none



New Case Setup is Now Complete

Case Settings

Case directory where the file database, index, and other case-specific files will be stored:

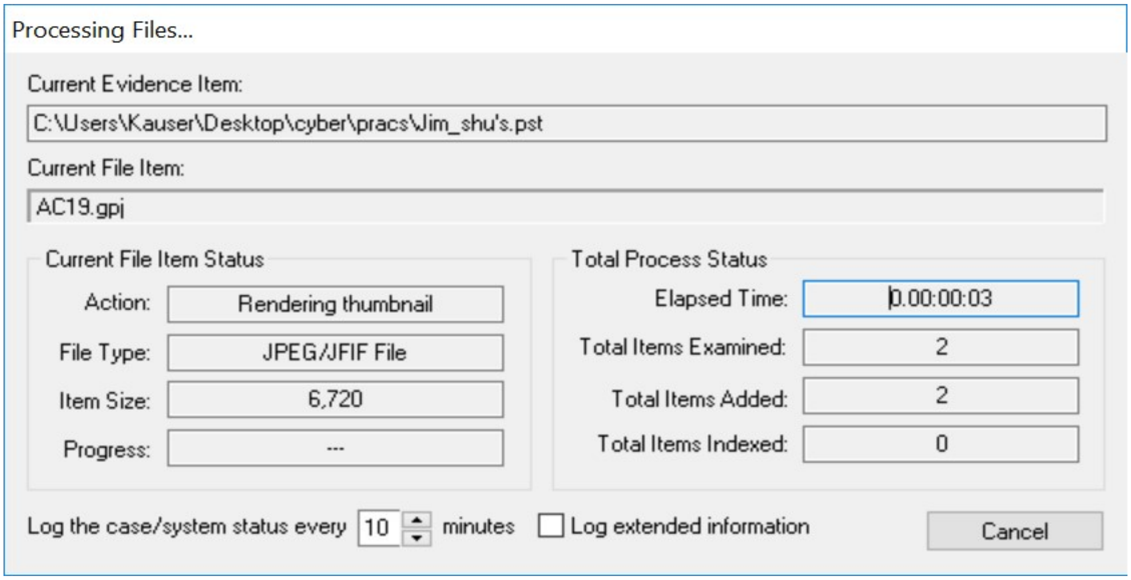
C:\Users\Siddhesh Chindarkar\Downloads\CF_practical9\cfpractical9

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:	Yes
Data Carving:	Yes
Registry Reports:	Yes

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



Current Evidence Item:

C:\Users\Kauser\Desktop\cyber\pracs\Jim_shu's.pst

Current File Item:

AC19.gpj

Current File Item Status

Action:	Rendering thumbnail
File Type:	JPEG/JFIF File
Item Size:	6,720
Progress:	---

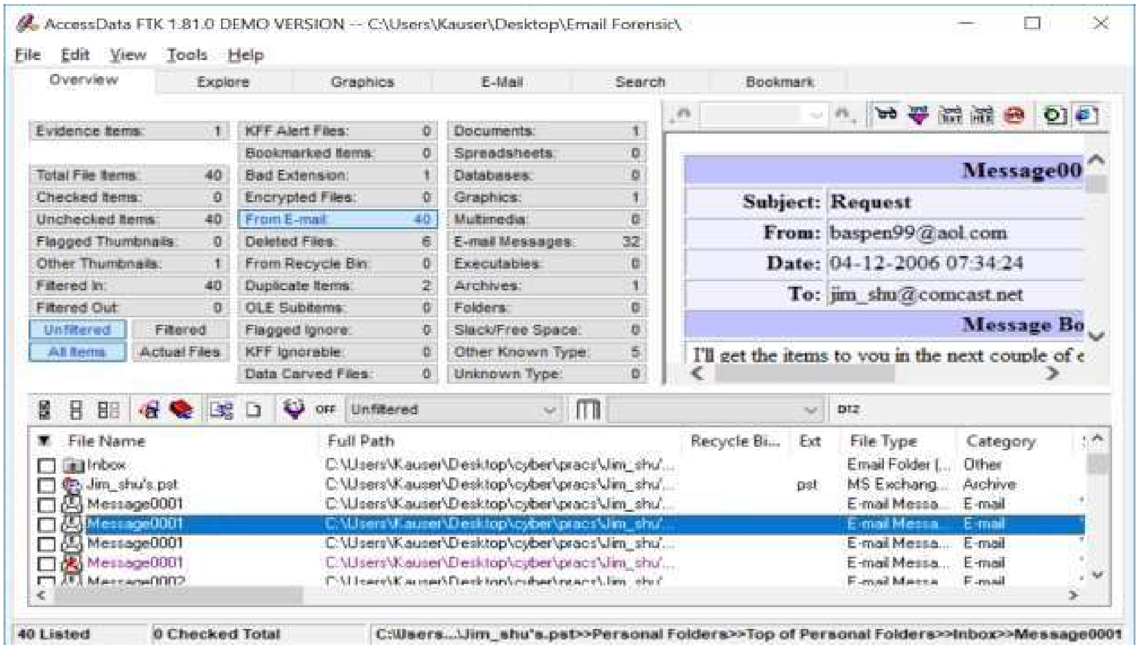
Total Process Status

Elapsed Time:	0.00:00:03
Total Items Examined:	2
Total Items Added:	2
Total Items Indexed:	0

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

11.When the Add Evidence to Case dialog box opens, click Next. In the Case summarydialog box, click Finish.

12.When FTK finishes processing the file, in the main FTK window, click the E-mail Messages button, and then click the Full Path column header to sort the records (see Figurebelow).


AccessData FTK 1.81.0 DEMO VERSION -- C:\Users\Kauser\Desktop\Email Forensic\
File Edit View Tools Help
Overview Explore Graphics E-Mail Search Bookmark
Unfiltered Filtered
All Items Actual Files
OFF Unfiltered
DTZ

Evidence Items:	1	KFF Alert Files:	0	Documents:	1
		Bookmarked Items:	0	Spreadsheets:	0
Total File Items:	40	Bad Extension:	1	Databases:	0
Checked Items:	0	Encrypted Files:	0	Graphics:	1
Unchecked Items:	40	From E-mail:	40	Multimedia:	0
Flagged Thumbnails:	0	Deleted Files:	6	E-mail Messages:	32
Other Thumbnails:	1	From Recycle Bin:	0	Executables:	0
Filtered In:	40	Duplicate Items:	2	Archives:	1
Filtered Out:	0	OLE Subitems:	0	Folders:	0
		Flagged Ignore:	0	Slack/Free Space:	0
		KFF Ignorable:	0	Other Known Type:	5
		Data Carved Files:	0	Unknown Type:	0

Message00

Subject: Request

From: baspen99@aol.com

Date: 04-12-2006 07:34:24

To: jim_shu@comcast.net

Message Bo

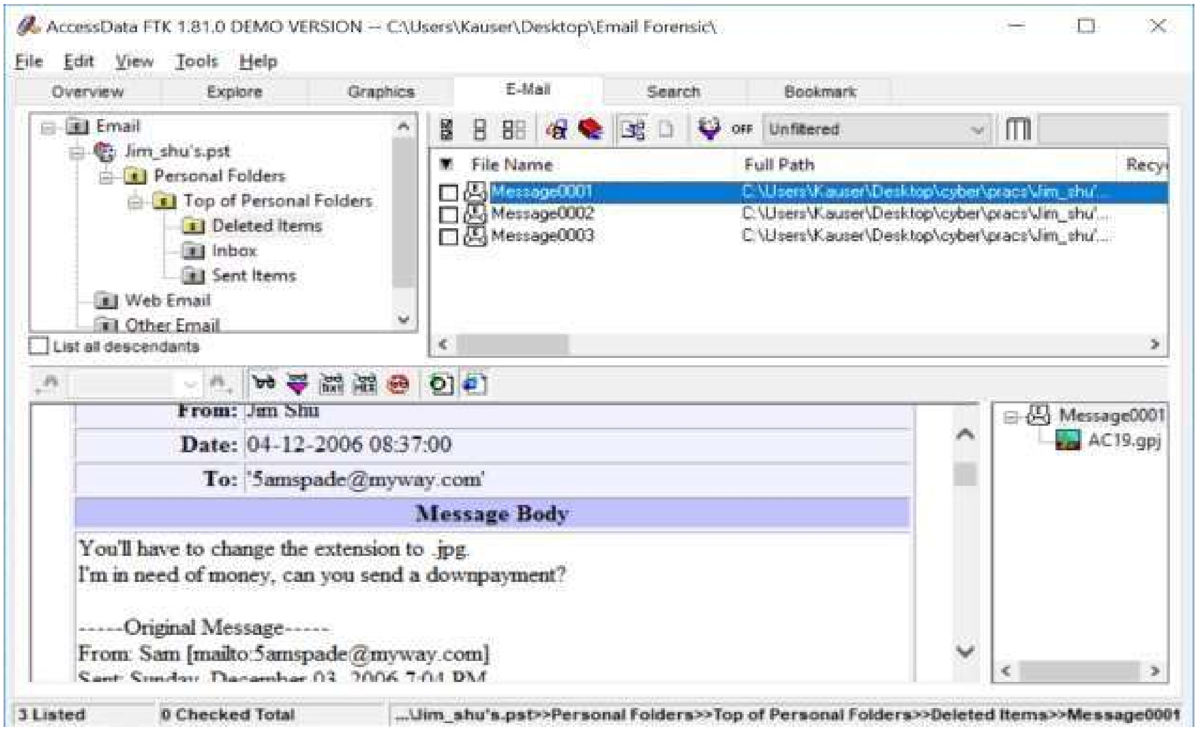
I'll get the items to you in the next couple of c

File Name	Full Path	Recycle Bi...	Ext	File Type	Category
□ Inbox	C:\Users\Kauser\Desktop\cyber\pracs\Jim_shu'...			Email Folder (...	Other
□ Jim_shu's.pst	C:\Users\Kauser\Desktop\cyber\pracs\Jim_shu'...		pst	MS Exchang...	Archive
□ Message0001	C:\Users\Kauser\Desktop\cyber\pracs\Jim_shu'...			E-mail Messa...	E-mail
□ Message0001	C:\Users\Kauser\Desktop\cyber\pracs\Jim_shu'...			E-mail Messa...	E-mail
□ Message0001	C:\Users\Kauser\Desktop\cyber\pracs\Jim_shu'...			E-mail Messa...	E-mail
□ Message0001	C:\Users\Kauser\Desktop\cyber\pracs\Jim_shu'...			E-mail Messa...	E-mail
□ Message0002	C:\Users\Kauser\Desktop\cyber\pracs\Jim_shu'			E-mail Messa	E-mail

40 Listed 0 Checked Total C:\Users...\Jim_shu's.pst>>Personal Folders>>Top of Personal Folders>>Inbox>>Message0001

- ➢ For email recovery follow following steps:

1. Click the E-Mail tab. In the tree view, click to expand all folders, and then click theDeleted Items folder.



File Name	Full Path
Message0001	C:\Users\Kauser\Desktop\cyber\pracs\Jim_shu'...
Message0002	C:\Users\Kauser\Desktop\cyber\pracs\Jim_shu'...
Message0003	C:\Users\Kauser\Desktop\cyber\pracs\Jim_shu'...

From: Jim Shu
Date: 04-12-2006 08:37:00
To: '5amspade@myway.com'

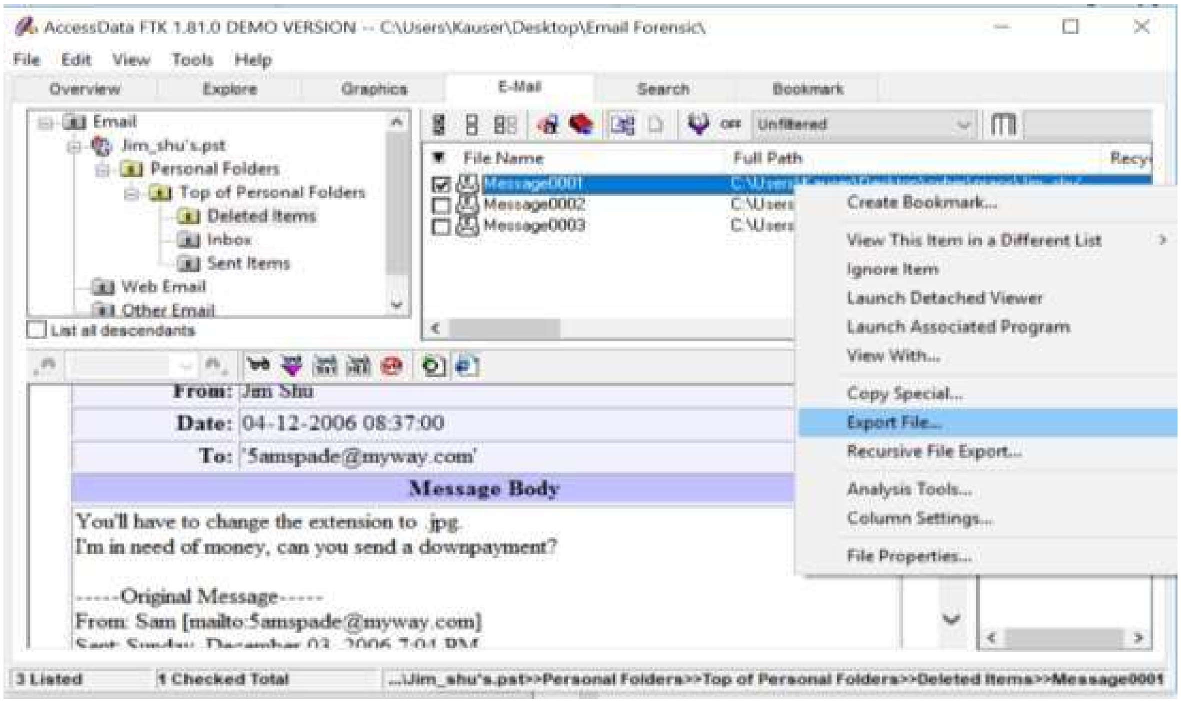
Message Body

You'll have to change the extension to .jpg.
I'm in need of money, can you send a downpayment?

-----Original Message-----
From: Sam [mailto:5amspade@myway.com]
Sent: Sunday, December 03, 2006 7:04 PM

3 Listed 0 Checked Total ...\Jim_shu's.pst>>Personal Folders>>Top of Personal Folders>>Deleted Items>>Message0001

2.Right-click Message0010 in the File List pane and click Export File. In the Export Filesdialog box, click OK.



File Name	Full Path
☑ Message0001	C:\Users...
□ Message0002	C:\Users
□ Message0003	C:\Users

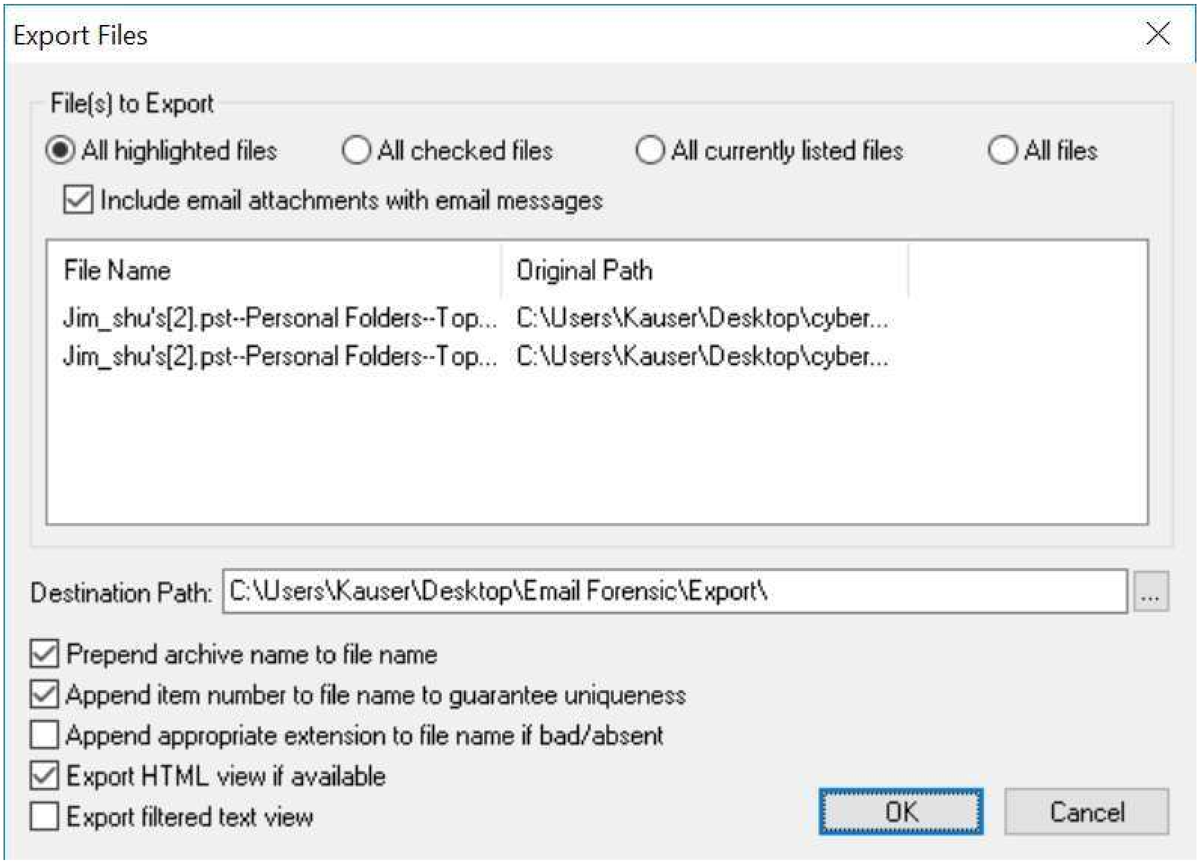
From: Jim Shu
Date: 04-12-2006 08:37:00
To: '5amspade@myway.com'

Message Body

You'll have to change the extension to .jpg.
I'm in need of money, can you send a downpayment?

-----Original Message-----
From: Sam [mailto:5amspade@myway.com]
Sent: Sunday, December 03, 2006 7:04 PM

3 Listed 1 Checked Total ...\Jim_shu's.pst>>Personal Folders>>Top of Personal Folders>>Deleted Items>>Message0001



● All highlighted files ○ All checked files ○ All currently listed files ○ All files

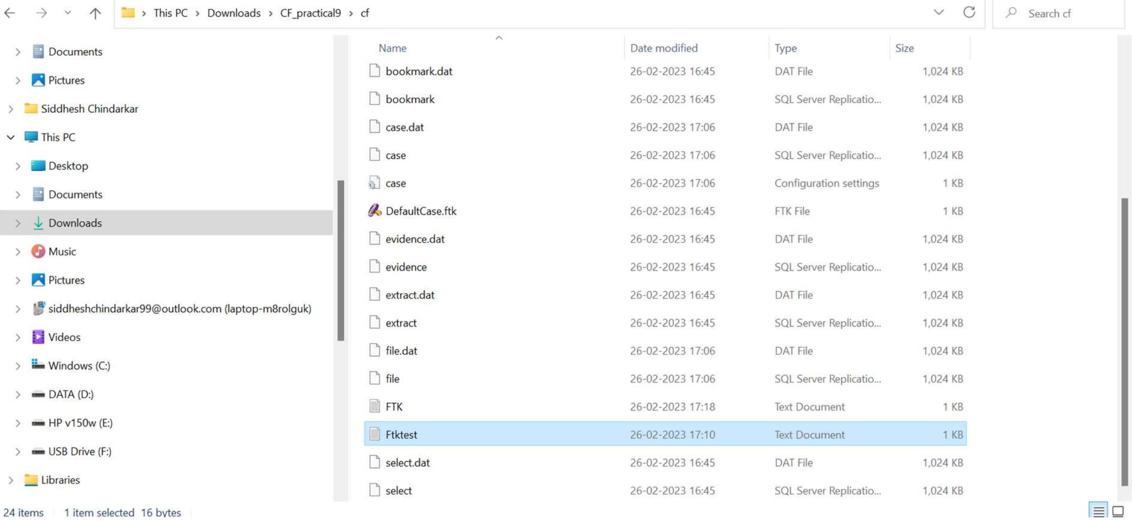
☑ Include email attachments with email messages

File Name	Original Path
Jim_shu's[2].pst--Personal Folders--Top...	C:\Users\Kauser\Desktop\cyber...
Jim_shu's[2].pst--Personal Folders--Top...	C:\Users\Kauser\Desktop\cyber...

Destination Path: C:\Users\Kauser\Desktop\Email Forensic\Export\

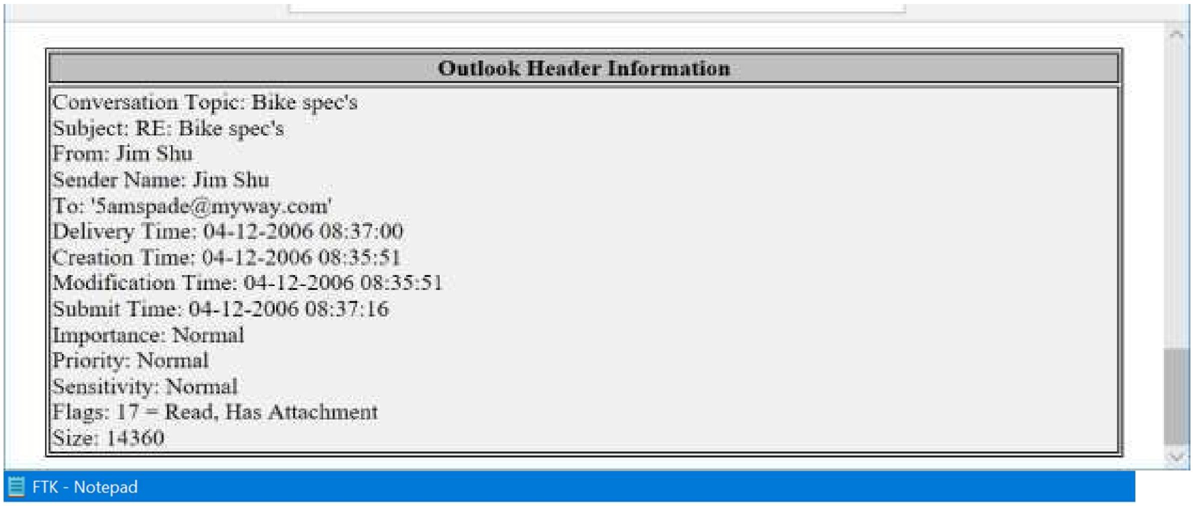
☑ Prepend archive name to file name
☑ Append item number to file name to guarantee uniqueness
☐ Append appropriate extension to file name if bad/absent
☑ Export HTML view if available
☐ Export filtered text view

3.Open the Export folder to view the Email Files, Open the HTML file in browser



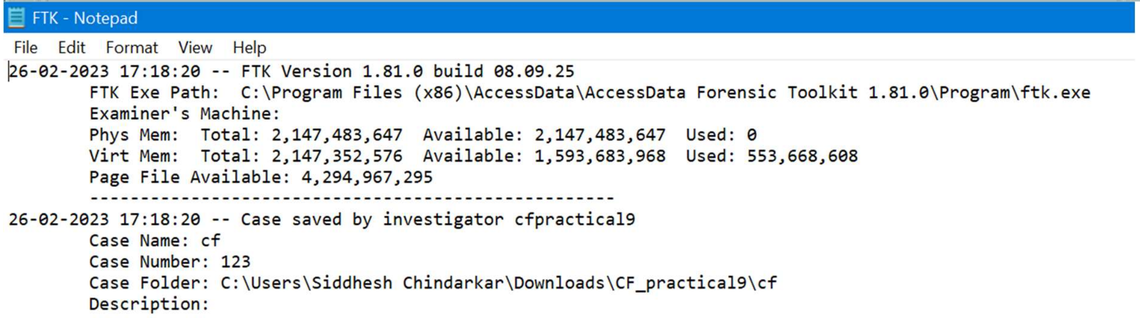
Name	Date modified	Type	Size
bookmark.dat	26-02-2023 16:45	DAT File	1,024 KB
bookmark	26-02-2023 16:45	SQL Server Replicatio...	1,024 KB
case.dat	26-02-2023 17:06	DAT File	1,024 KB
case	26-02-2023 17:06	SQL Server Replicatio...	1,024 KB
case	26-02-2023 17:06	Configuration settings	1 KB
DefaultCase.ftk	26-02-2023 16:45	FTK File	1 KB
evidence.dat	26-02-2023 16:45	DAT File	1,024 KB
evidence	26-02-2023 16:45	SQL Server Replicatio...	1,024 KB
extract.dat	26-02-2023 16:45	DAT File	1,024 KB
extract	26-02-2023 16:45	SQL Server Replicatio...	1,024 KB
file.dat	26-02-2023 17:06	DAT File	1,024 KB
file	26-02-2023 17:06	SQL Server Replicatio...	1,024 KB
FTK	26-02-2023 17:18	Text Document	1 KB
Ftktest	26-02-2023 17:10	Text Document	1 KB
select.dat	26-02-2023 16:45	DAT File	1,024 KB
select	26-02-2023 16:45	SQL Server Replicatio...	1,024 KB

24 items 1 item selected 16 bytes



Outlook Header Information

Conversation Topic: Bike spec's
Subject: RE: Bike spec's
From: Jim Shu
Sender Name: Jim Shu
To: '5amspade@myway.com'
Delivery Time: 04-12-2006 08:37:00
Creation Time: 04-12-2006 08:35:51
Modification Time: 04-12-2006 08:35:51
Submit Time: 04-12-2006 08:37:16
Importance: Normal
Priority: Normal
Sensitivity: Normal
Flags: 17 = Read, Has Attachment
Size: 14360



```
26-02-2023 17:18:20 -- FTK Version 1.81.0 build 08.09.25
        FTK Exe Path:  C:\Program Files (x86)\AccessData\AccessData Forensic Toolkit 1.81.0\Program\ftk.exe
        Examiner's Machine:
        Phys Mem:  Total: 2,147,483,647  Available: 2,147,483,647  Used: 0
        Virt Mem:  Total: 2,147,352,576  Available: 1,593,683,968  Used: 553,668,608
        Page File Available: 4,294,967,295
        ----------------------------------------------------
26-02-2023 17:18:20 -- Case saved by investigator cfpractical9
        Case Name: cf
        Case Number: 123
        Case Folder: C:\Users\Siddhesh Chindarkar\Downloads\CF_practical9\cf
        Description:
```