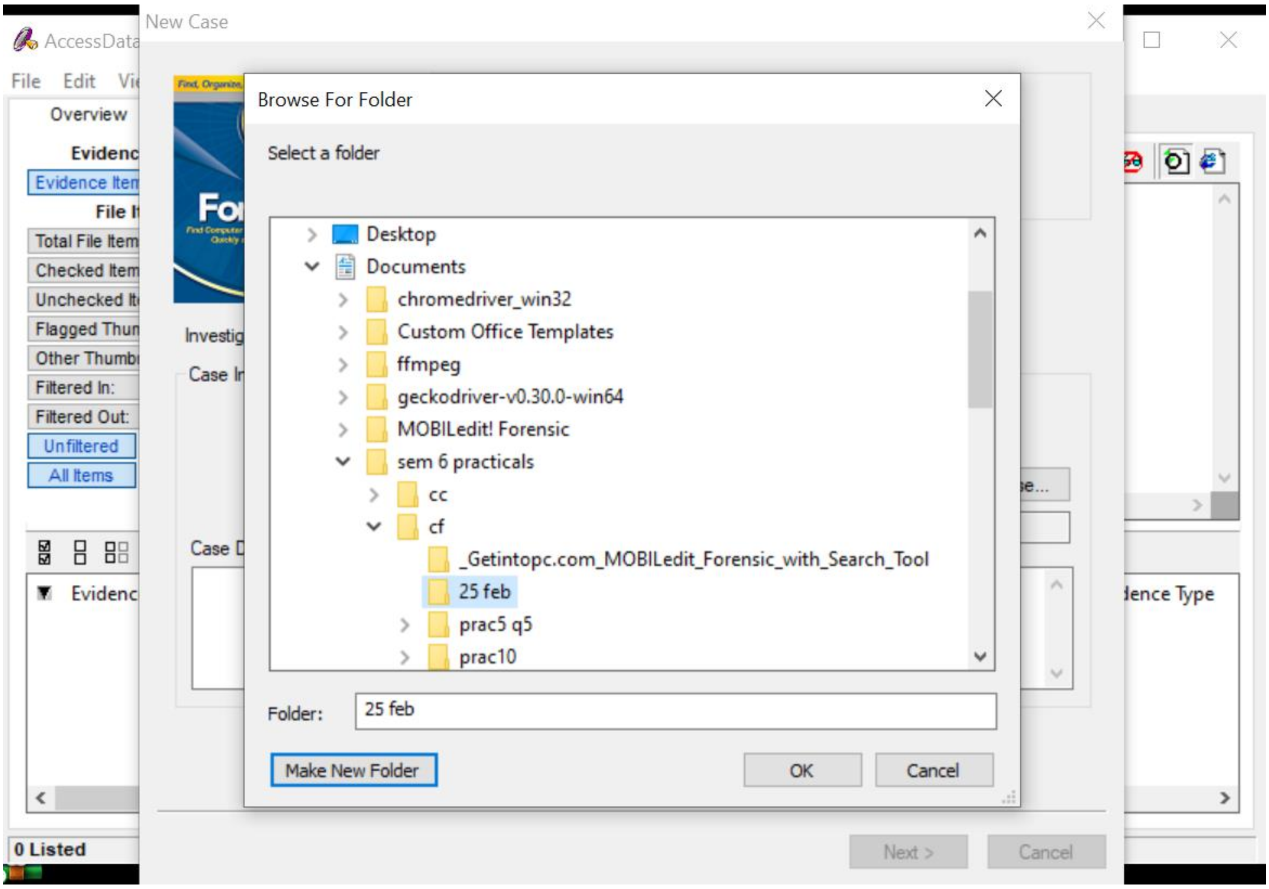
Aim: Email Forensics

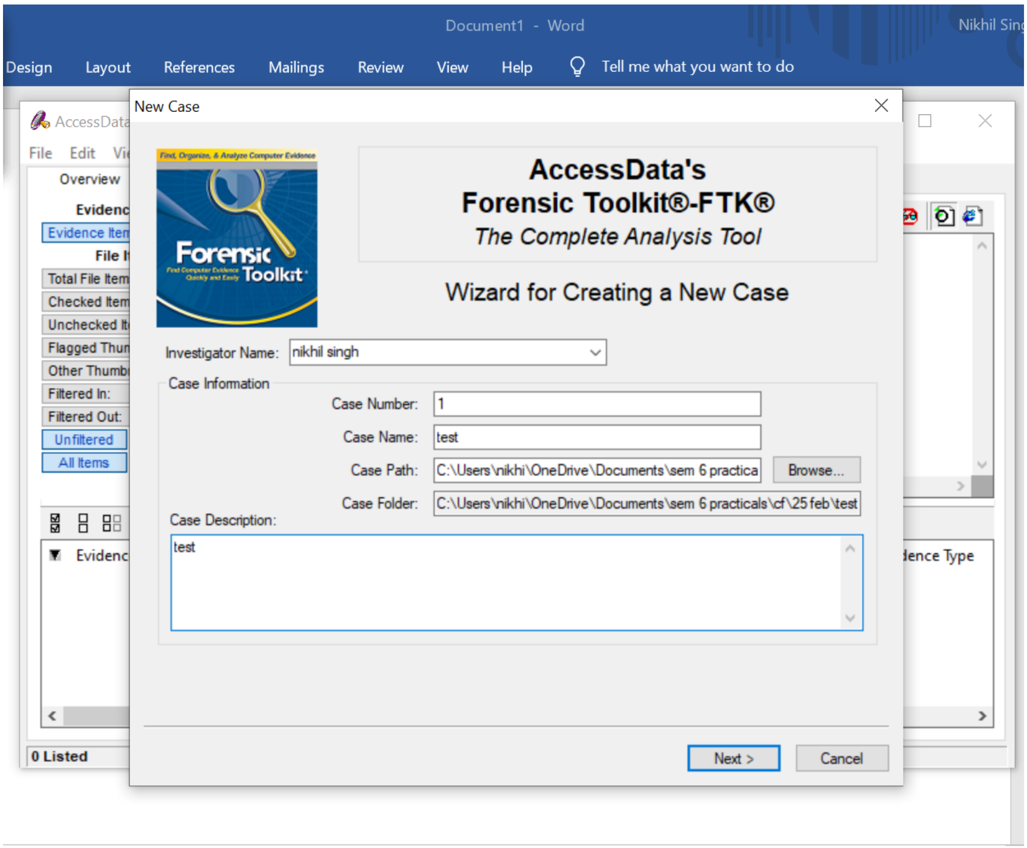
- Mail Service Providers
- Email protocols
- Recovering emails
- Analyzing email header

click Start a new case, and then click OK.



Folder: 25 feb

Type case Information and examiner information



New Case

Wizard for Creating a New Case

Investigator Name: nikhil singh

Case Information

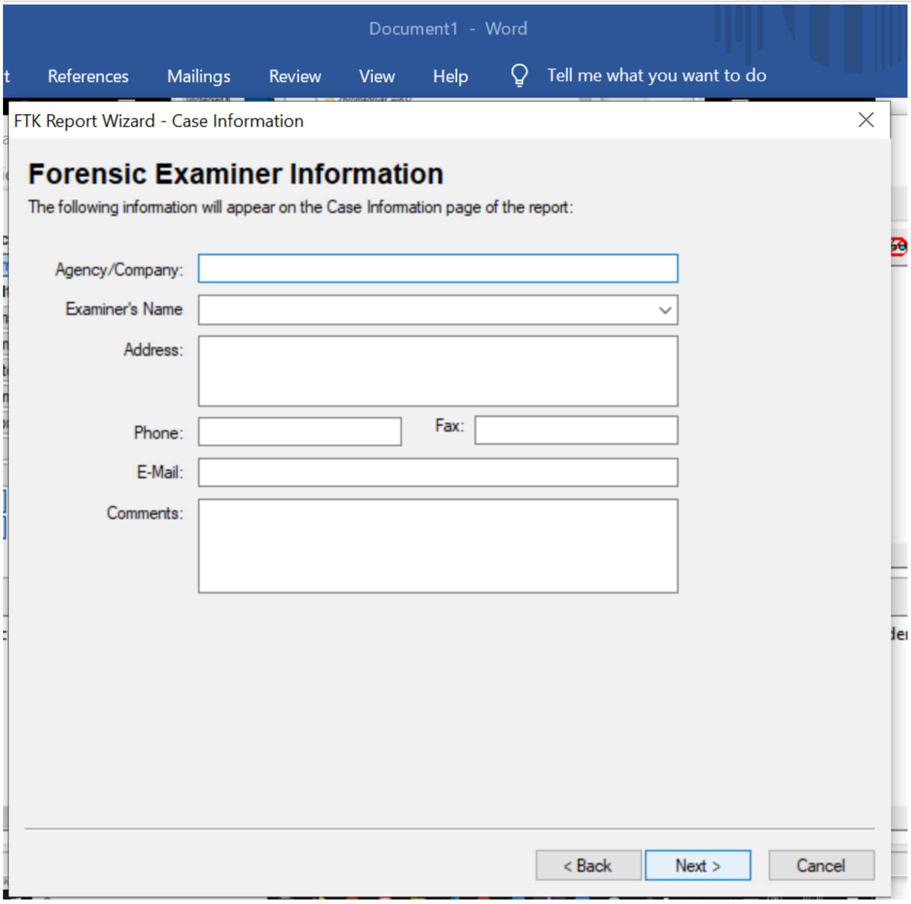
Case Number: 1

Case Name: test

Case Path: C:\Users\nikhi\OneDrive\Documents\sem 6 practica

Case Folder: C:\Users\nikhi\OneDrive\Documents\sem 6 practicals\cf\25 feb\test

Case Description: test



FTK Report Wizard - Case Information

Forensic Examiner Information

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

Agency/Company:

Examiner's Name

Address:

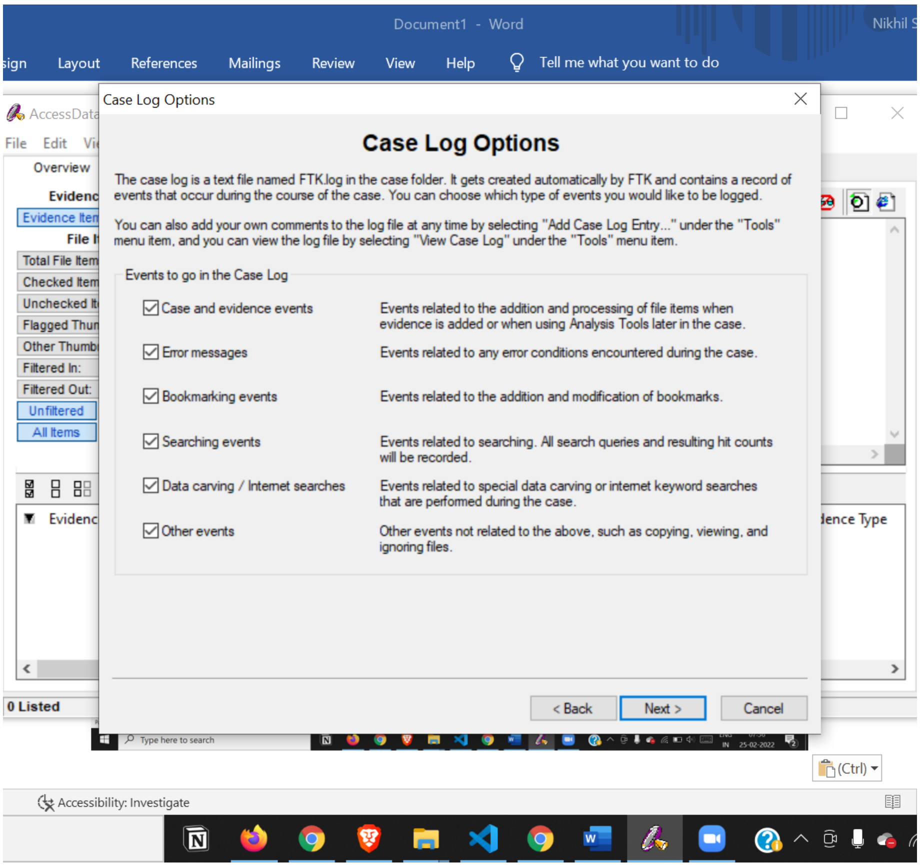
Phone:

Fax:

E-Mail:

Comments:

Select case log options and all processes to perform



Case Log Options

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.

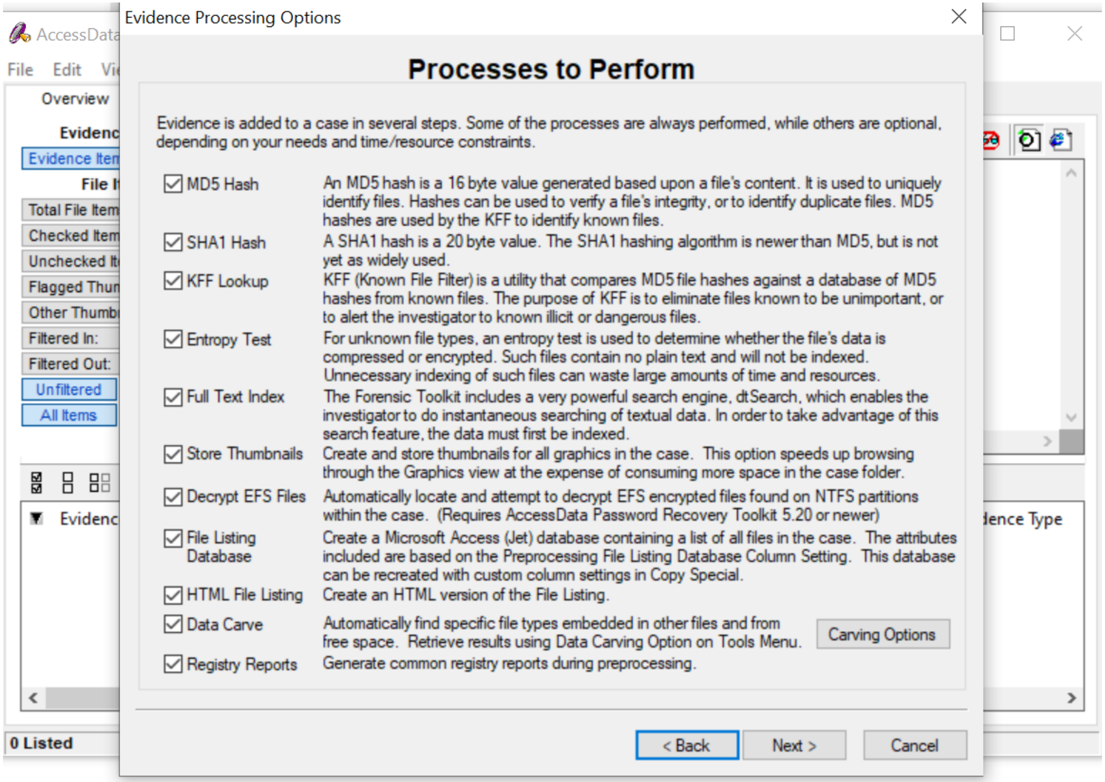
☑ Bookmarking events — Events related to the addition and modification of bookmarks.

☑ 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.

< Back | Next > | Cancel



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.

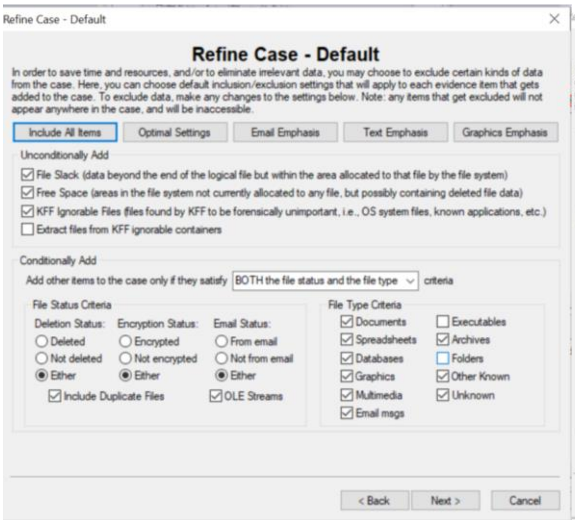
☑ HTML File Listing — Create an HTML version of the File Listing.

☑ 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

Select these options and add evidence information



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

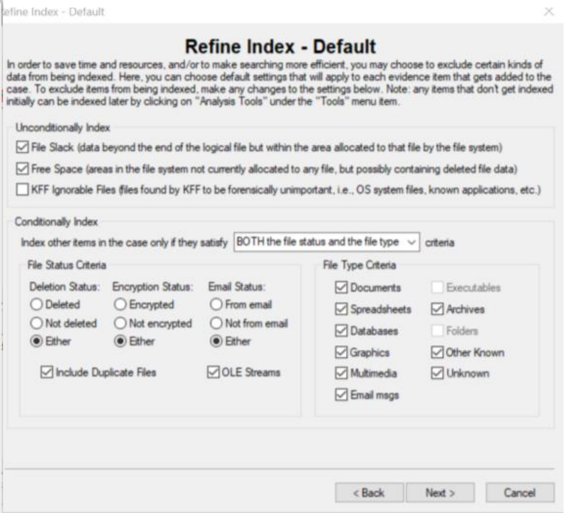
Add other items to the case only if they satisfy: BOTH the file status and the file type criteria

File Status Criteria

Deletion Status: ○ 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



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

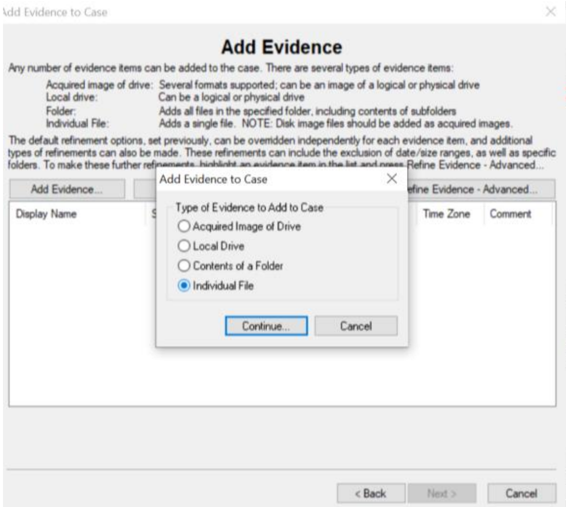
Index other items in the case only if they satisfy: BOTH the file status and the file type criteria

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



Add Evidence to Case

Add Evidence

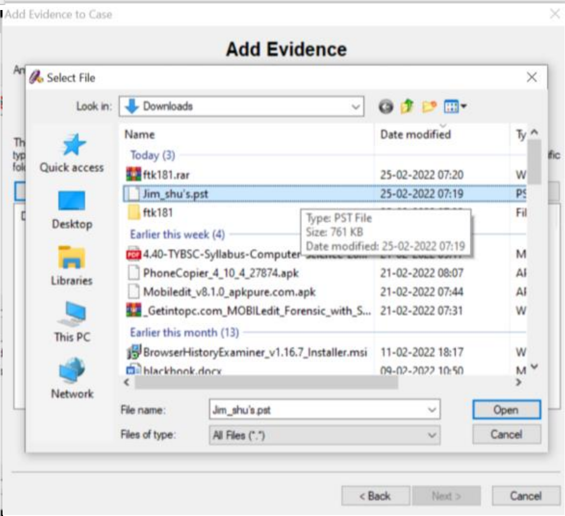
Any number of evidence items can be added to the case. There are several types of evidence items:

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



Add Evidence to Case

Add Evidence

Select File

Look in: Downloads

Name	Date modified	Ty
Today (3)		
ftk181.rar	25-02-2022 07:20	W
Jim_shu's.pst	25-02-2022 07:19	PS
ftk181		Fil
Earlier this week (4)		
4.40-TYBSC-Syllabus-Computer		M
PhoneCopier_4_10_4_27874.apk	21-02-2022 08:07	AI
Mobiledit_v8.1.0_apkpure.com.apk	21-02-2022 07:44	AI
_Getintopc.com_MOBILedit_Forensic_with_S...	21-02-2022 07:31	W
Earlier this month (13)		
BrowserHistoryExaminer_v1.16.7_Installer.msi	11-02-2022 18:17	W
blackbook.docx	09-02-2022 10:50	M

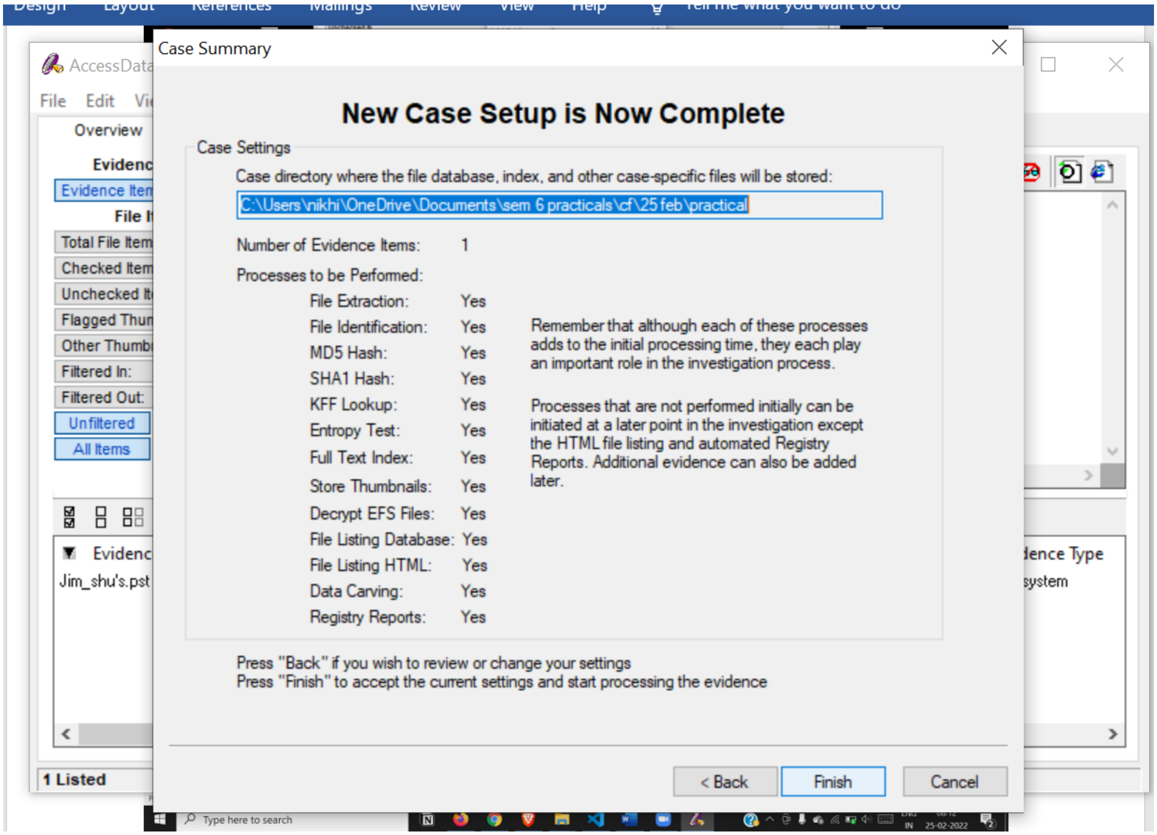
Type: PST File
Size: 761 KB
Date modified: 25-02-2022 07:19

File name: Jim_shu's.pst

Files of type: All Files (*.*)

Practical 9

New case setup is complete



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\nikhi\OneDrive\Documents\sem 6 practicals\cf\25 feb\practical

Number of Evidence Items: 1

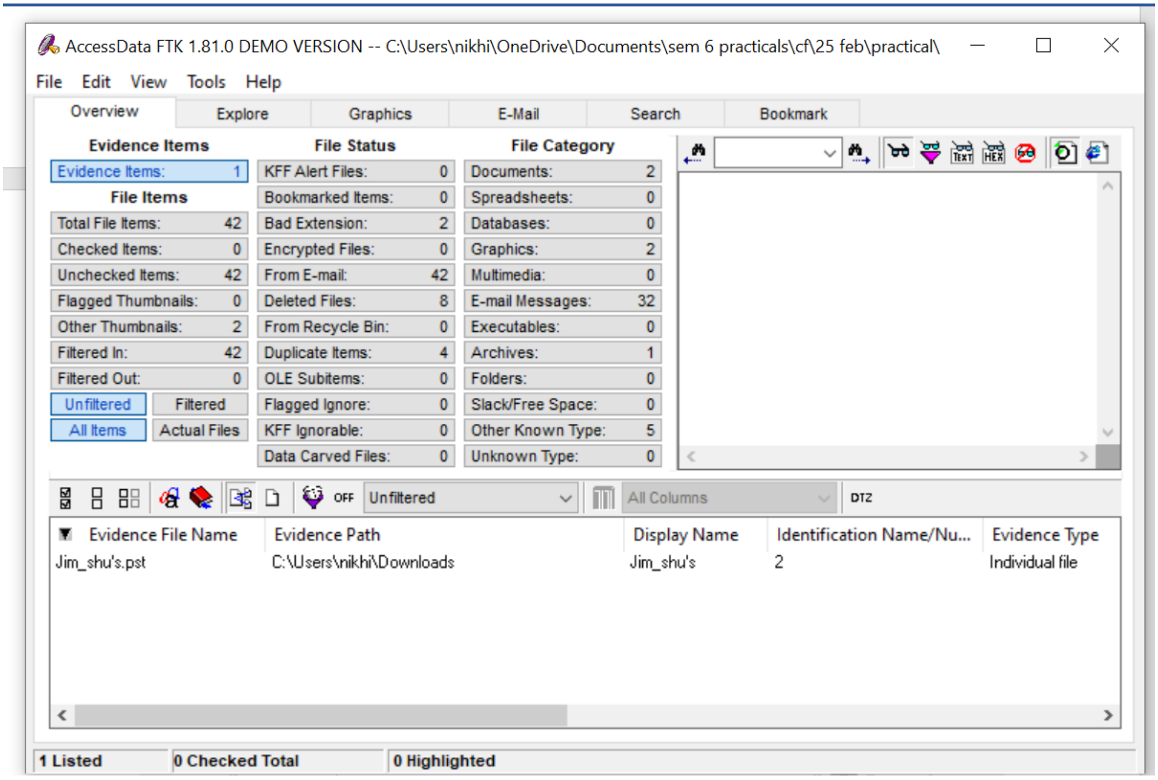
Processes to be Performed:

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



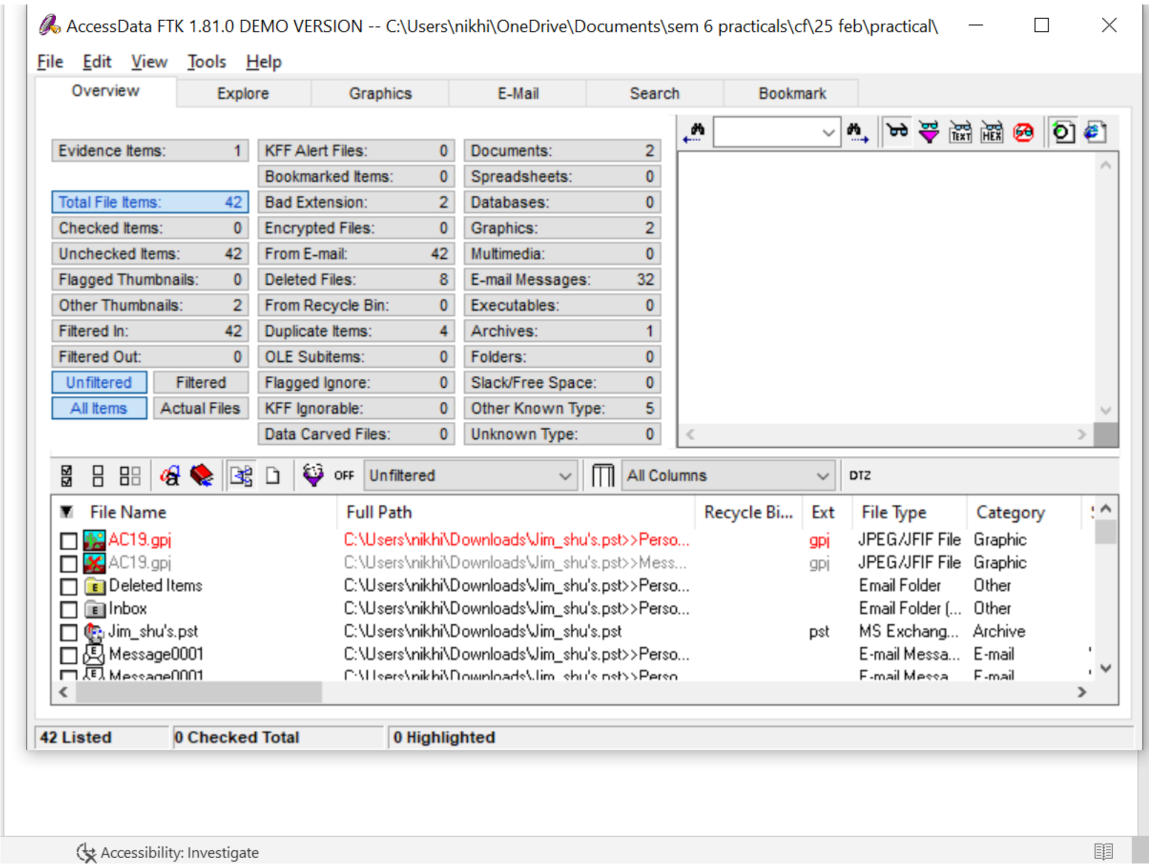
AccessData FTK 1.81.0 DEMO VERSION -- C:\Users\nikhi\OneDrive\Documents\sem 6 practicals\cf\25 feb\practical\

File Edit View Tools Help
Overview Explore Graphics E-Mail Search Bookmark

Evidence Items		File Status		File Category	
Evidence Items:	1	KFF Alert Files:	0	Documents:	2
File Items		Bookmarked Items:	0	Spreadsheets:	0
Total File Items:	42	Bad Extension:	2	Databases:	0
Checked Items:	0	Encrypted Files:	0	Graphics:	2
Unchecked Items:	42	From E-mail:	42	Multimedia:	0
Flagged Thumbnails:	0	Deleted Files:	8	E-mail Messages:	32
Other Thumbnails:	2	From Recycle Bin:	0	Executables:	0
Filtered In:	42	Duplicate Items:	4	Archives:	1
Filtered Out:	0	OLE Subitems:	0	Folders:	0
Unfiltered	Filtered	Flagged Ignore:	0	Slack/Free Space:	0
All Items	Actual Files	KFF Ignorable:	0	Other Known Type:	5
		Data Carved Files:	0	Unknown Type:	0

Evidence File Name	Evidence Path	Display Name	Identification Name/Nu...	Evidence Type
Jim_shu's.pst	C:\Users\nikhi\Downloads	Jim_shu's	2	Individual file

1 Listed 0 Checked Total 0 Highlighted

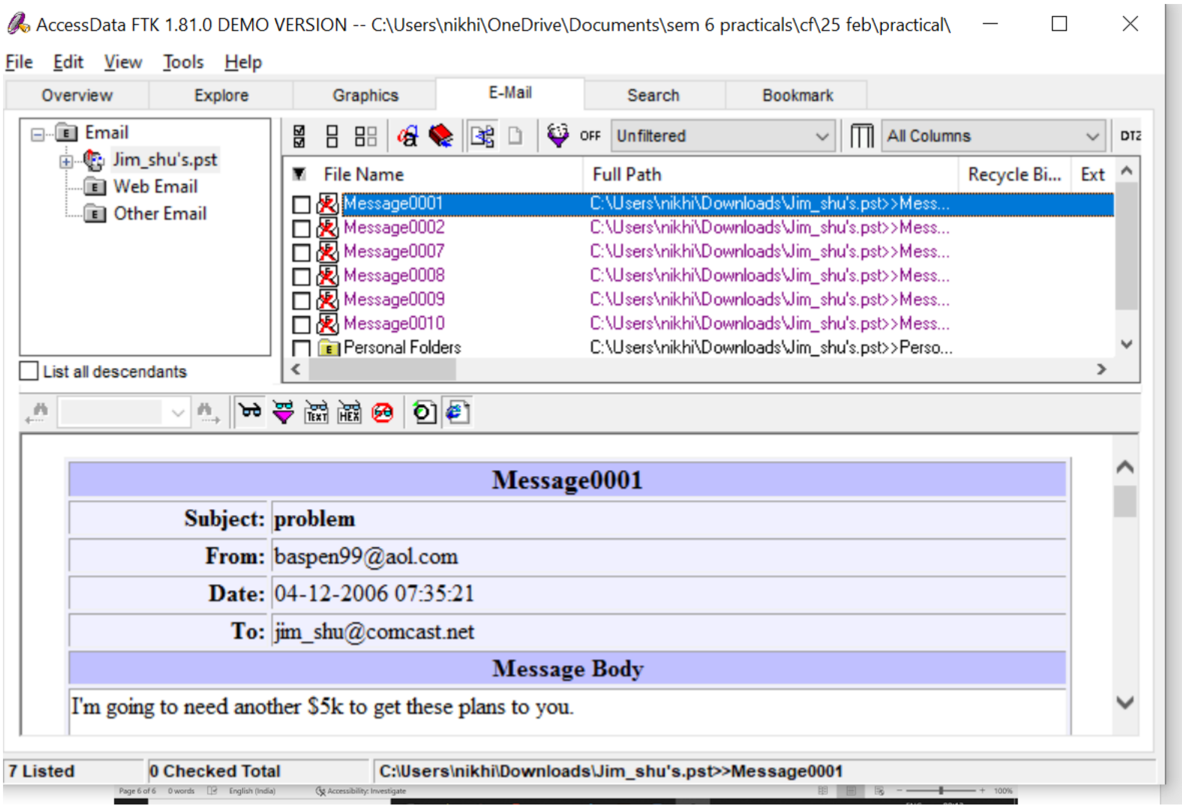

AccessData FTK 1.81.0 DEMO VERSION -- C:\Users\nikhi\OneDrive\Documents\sem 6 practicals\cf\25 feb\practical\
File Edit View Tools Help
Overview Explore Graphics E-Mail Search Bookmark
Accessibility: Investigate

Evidence Items:	1	KFF Alert Files:	0	Documents:	2
		Bookmarked Items:	0	Spreadsheets:	0
Total File Items:	42	Bad Extension:	2	Databases:	0
Checked Items:	0	Encrypted Files:	0	Graphics:	2
Unchecked Items:	42	From E-mail:	42	Multimedia:	0
Flagged Thumbnails:	0	Deleted Files:	8	E-mail Messages:	32
Other Thumbnails:	2	From Recycle Bin:	0	Executables:	0
Filtered In:	42	Duplicate Items:	4	Archives:	1
Filtered Out:	0	OLE Subitems:	0	Folders:	0
Unfiltered	Filtered	Flagged Ignore:	0	Slack/Free Space:	0
All Items	Actual Files	KFF Ignorable:	0	Other Known Type:	5
		Data Carved Files:	0	Unknown Type:	0

OFF Unfiltered — All Columns

File Name	Full Path	Recycle Bi...	Ext	File Type	Category
□ AC19.gpj	C:\Users\nikhi\Downloads\Jim_shu's.pst>>Perso...		gpj	JPEG/JFIF File	Graphic
□ AC19.gpj	C:\Users\nikhi\Downloads\Jim_shu's.pst>>Mess...		gpj	JPEG/JFIF File	Graphic
□ Deleted Items	C:\Users\nikhi\Downloads\Jim_shu's.pst>>Perso...			Email Folder	Other
□ Inbox	C:\Users\nikhi\Downloads\Jim_shu's.pst>>Perso...			Email Folder (...	Other
□ Jim_shu's.pst	C:\Users\nikhi\Downloads\Jim_shu's.pst		pst	MS Exchang...	Archive
□ Message0001	C:\Users\nikhi\Downloads\Jim_shu's.pst>>Perso...			E-mail Messa...	E-mail
□ Message0001	C:\Users\nikhi\Downloads\Jim_shu's.pst>>Perso			E-mail Messa	E-mail

42 Listed | 0 Checked Total | 0 Highlighted


AccessData FTK 1.81.0 DEMO VERSION -- C:\Users\nikhi\OneDrive\Documents\sem 6 practicals\cf\25 feb\practical\
File Edit View Tools Help
Overview Explore Graphics E-Mail Search Bookmark
Email
Jim_shu's.pst
Web Email
Other Email
List all descendants
OFF Unfiltered
All Columns

File Name	Full Path	Recycle Bi...	Ext
□ Message0001	C:\Users\nikhi\Downloads\Jim_shu's.pst>>Mess...		
□ Message0002	C:\Users\nikhi\Downloads\Jim_shu's.pst>>Mess...		
□ Message0007	C:\Users\nikhi\Downloads\Jim_shu's.pst>>Mess...		
□ Message0008	C:\Users\nikhi\Downloads\Jim_shu's.pst>>Mess...		
□ Message0009	C:\Users\nikhi\Downloads\Jim_shu's.pst>>Mess...		
□ Message0010	C:\Users\nikhi\Downloads\Jim_shu's.pst>>Mess...		
□ Personal Folders	C:\Users\nikhi\Downloads\Jim_shu's.pst>>Perso...		

Message0001

Subject: problem

From: baspen99@aol.com

Date: 04-12-2006 07:35:21

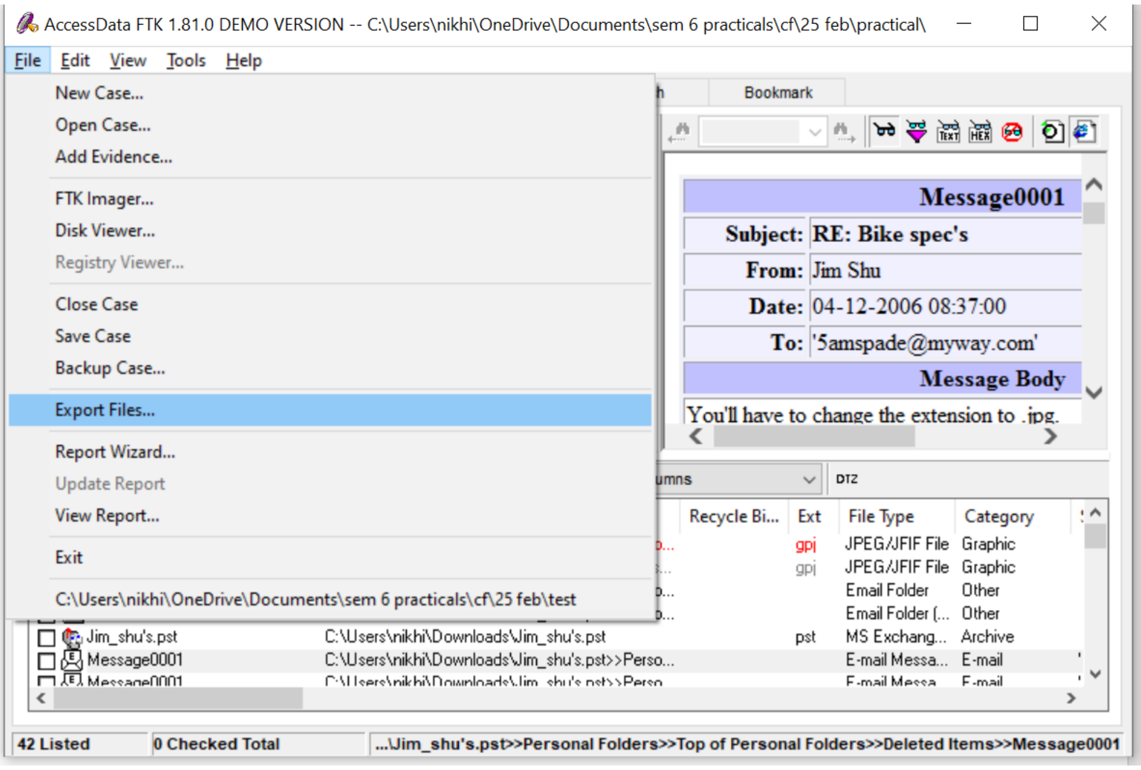
To: jim_shu@comcast.net

Message Body

I'm going to need another $5k to get these plans to you.

7 Listed | 0 Checked Total | C:\Users\nikhi\Downloads\Jim_shu's.pst>>Message0001

Export case information



AccessData FTK 1.81.0 DEMO VERSION -- C:\Users\nikhi\OneDrive\Documents\sem 6 practicals\cf\25 feb\practical\

Message0001

Subject: RE: Bike spec's

From: Jim Shu

Date: 04-12-2006 08:37:00

To: '5amspade@myway.com'

Message Body

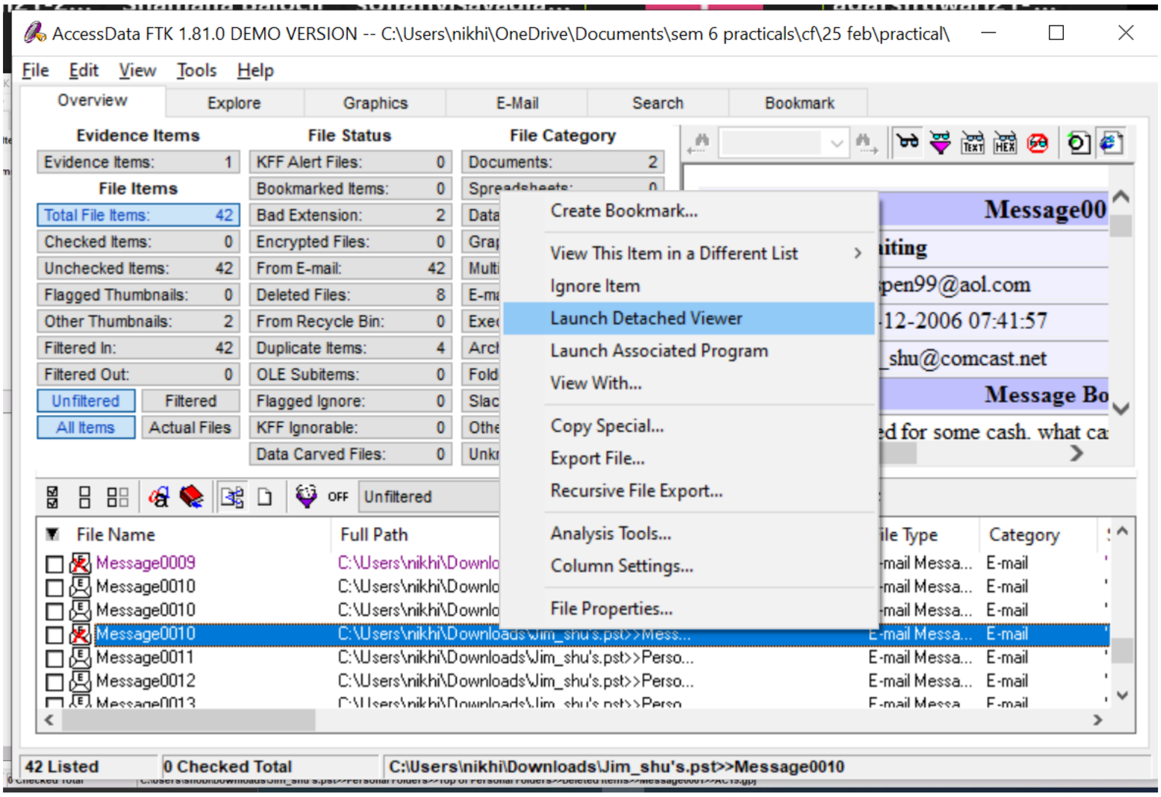
You'll have to change the extension to .jpg.

		Recycle Bi...	Ext	File Type	Category
			gpj	JPEG/JFIF File	Graphic
			gpj	JPEG/JFIF File	Graphic
				Email Folder	Other
				Email Folder (...	Other
□ Jim_shu's.pst	C:\Users\nikhi\Downloads\Jim_shu's.pst		pst	MS Exchang...	Archive
□ Message0001	C:\Users\nikhi\Downloads\Jim_shu's.pst>>Perso...			E-mail Messa...	E-mail
□ Message0001	C:\Users\nikhi\Downloads\Jim_shu's.pst>>Perso...			E-mail Messa...	E-mail

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

Part2

Launch detached information



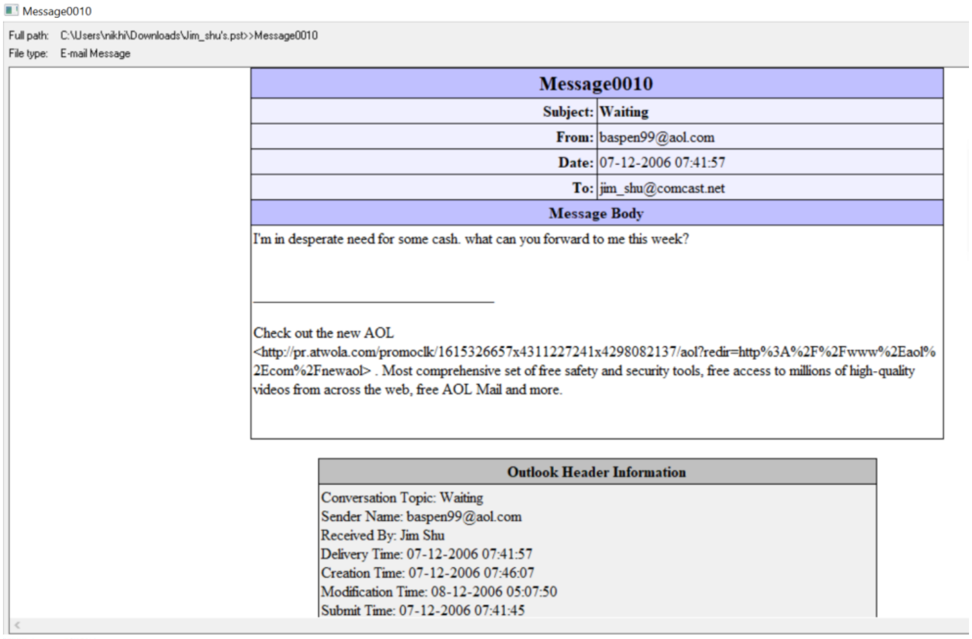
Evidence Items		File Status		File Category	
Evidence Items:	1	KFF Alert Files:	0	Documents:	2
File Items		Bookmarked Items:	0	Spreadsheets:	0
Total File Items:	42	Bad Extension:	2	Data	
Checked Items:	0	Encrypted Files:	0	Grap	
Unchecked Items:	42	From E-mail:	42	Multi	
Flagged Thumbnails:	0	Deleted Files:	8	E-ma	
Other Thumbnails:	2	From Recycle Bin:	0	Exec	
Filtered In:	42	Duplicate Items:	4	Arch	
Filtered Out:	0	OLE Subitems:	0	Fold	
		Flagged Ignore:	0	Slac	
		KFF Ignorable:	0	Othe	
		Data Carved Files:	0	Unkr	

File Name	Full Path	ile Type	Category
□ Message0009	C:\Users\nikhi\Downlo	mail Messa...	E-mail
□ Message0010	C:\Users\nikhi\Downlo	mail Messa...	E-mail
□ Message0010	C:\Users\nikhi\Downlo	mail Messa...	E-mail
□ Message0010	C:\Users\nikhi\Downloads\Jim_shu's.pst>>Mess...	E-mail Messa...	E-mail
□ Message0011	C:\Users\nikhi\Downloads\Jim_shu's.pst>>Perso...	E-mail Messa...	E-mail
□ Message0012	C:\Users\nikhi\Downloads\Jim_shu's.pst>>Perso...	E-mail Messa...	E-mail
□ Message0013	C:\Users\nikhi\Downloads\Jim_shu's.pst>>Perso	E-mail Messa	E-mail

42 Listed | 0 Checked Total | C:\Users\nikhi\Downloads\Jim_shu's.pst>>Message0010

Practical 9

View message headers and body



Message0010

Full path: C:\Users\nikhi\Downloads\Jim_shu's.pst>>Message0010
File type: E-mail Message

Message0010

Subject:	**Waiting**
From:	baspen99@aol.com
Date:	07-12-2006 07:41:57
To:	jim_shu@comcast.net

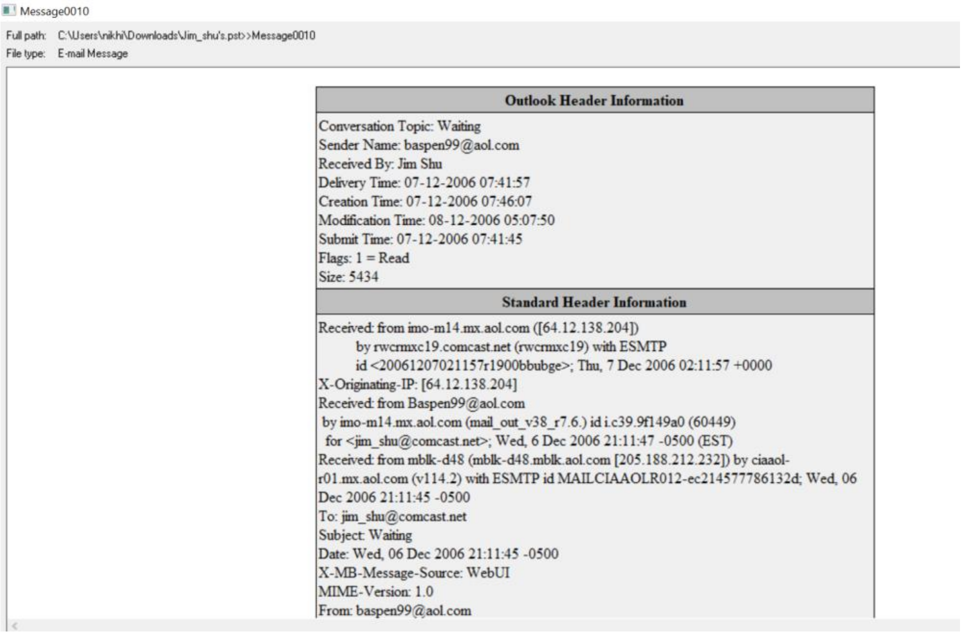
Message Body

I'm in desperate need for some cash. what can you forward to me this week?

Check out the new AOL <http://pr.atwola.com/promoclk/1615326657x4311227241x4298082137/aol?redir=http%3A%2F%2Fwww%2Eaol%2Ecom%2Fnewaol> . Most comprehensive set of free safety and security tools, free access to millions of high-quality videos from across the web, free AOL Mail and more.

Outlook Header Information

Conversation Topic: Waiting
Sender Name: baspen99@aol.com
Received By: Jim Shu
Delivery Time: 07-12-2006 07:41:57
Creation Time: 07-12-2006 07:46:07
Modification Time: 08-12-2006 05:07:50
Submit Time: 07-12-2006 07:41:45



Message0010

Full path: C:\Users\nikhi\Downloads\Jim_shu's.pst>>Message0010
File type: E-mail Message

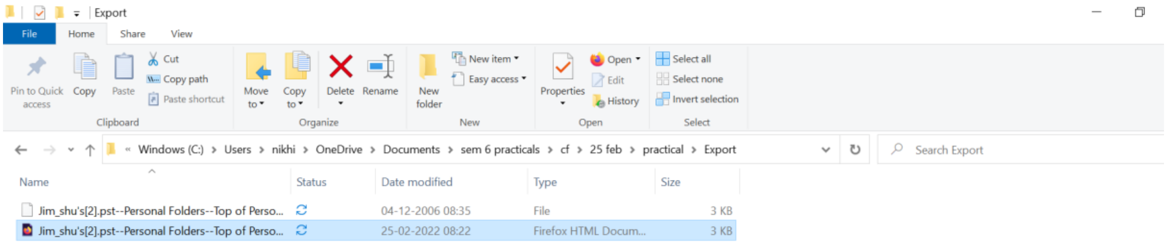
Outlook Header Information

Conversation Topic: Waiting
Sender Name: baspen99@aol.com
Received By: Jim Shu
Delivery Time: 07-12-2006 07:41:57
Creation Time: 07-12-2006 07:46:07
Modification Time: 08-12-2006 05:07:50
Submit Time: 07-12-2006 07:41:45
Flags: 1 = Read
Size: 5434

Standard Header Information

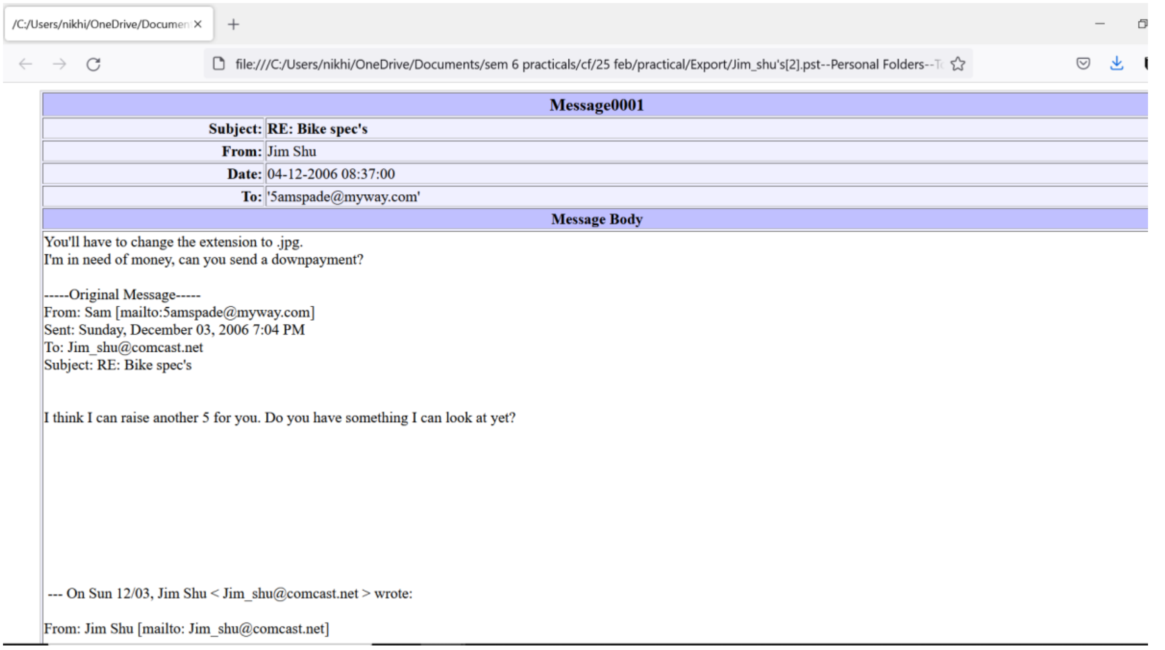
```
Received: from imo-m14.mx.aol.com ([64.12.138.204])
        by rwcrmxc19.comcast.net (rwcrmxc19) with ESMTP
        id <20061207021157r1900bbubge>; Thu, 7 Dec 2006 02:11:57 +0000
X-Originating-IP: [64.12.138.204]
Received: from Baspen99@aol.com
 by imo-m14.mx.aol.com (mail_out_v38_r7.6.) id i.c39.9f149a0 (60449)
  for <jim_shu@comcast.net>; Wed, 6 Dec 2006 21:11:47 -0500 (EST)
Received: from mblk-d48 (mblk-d48.mblk.aol.com [205.188.212.232]) by ciaaol-
r01.mx.aol.com (v114.2) with ESMTP id MAILCIAAOLR012-ec214577786132d; Wed, 06
Dec 2006 21:11:45 -0500
To: jim_shu@comcast.net
Subject: Waiting
Date: Wed, 06 Dec 2006 21:11:45 -0500
X-MB-Message-Source: WebUI
MIME-Version: 1.0
From: baspen99@aol.com
```

Practical 9



Windows (C:) › Users › nikhi › OneDrive › Documents › sem 6 practicals › cf › 25 feb › practical › Export

Name	Status	Date modified	Type	Size
Jim_shu's[2].pst--Personal Folders--Top of Perso...		04-12-2006 08:35	File	3 KB
Jim_shu's[2].pst--Personal Folders--Top of Perso...		25-02-2022 08:22	Firefox HTML Docum...	3 KB



file:///C:/Users/nikhi/OneDrive/Documents/sem 6 practicals/cf/25 feb/practical/Export/Jim_shu's[2].pst--Personal Folders--T

Message0001	
Subject:	**RE: Bike spec's**
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
To: Jim_shu@comcast.net
Subject: RE: Bike spec's

I think I can raise another 5 for you. Do you have something I can look at yet?

--- On Sun 12/03, Jim Shu < Jim_shu@comcast.net > wrote:

From: Jim Shu [mailto: Jim_shu@comcast.net]