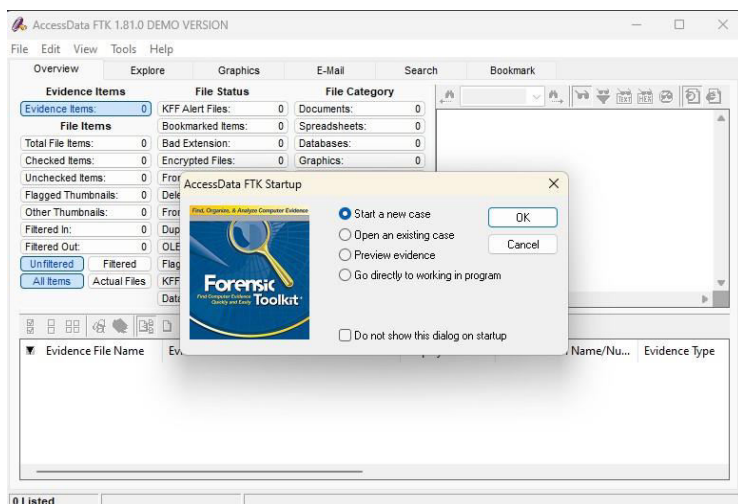


## **Practical No: 09**

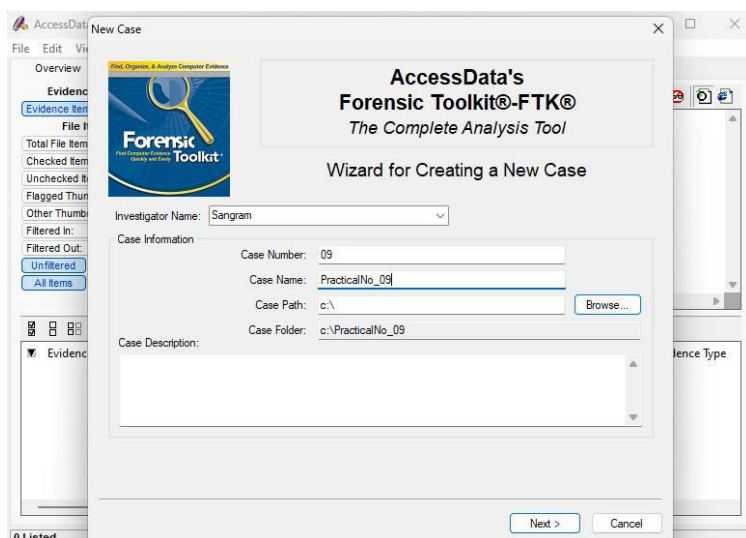
### **AIM:** Email Forensics

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

#### **Step 1:** Open Forensic Toolkit and click on file new case



#### **Step 2:** Fill the following details and click next.



**Step 3: Click next.**

AccessData FTK Report Wizard - Case Information

File Edit View

Overview Evidence Item File Item Total File Item Checked Item Unchecked Item Flagged Item Other Thumbnail Filtered In: Filtered Out: Unfiltered All Items

**Forensic Examiner Information**

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

Agency/Company: MCC

Examiner's Name: Sangram

Address: Mulund College of Commerce

Phone: 9372604106 Fax:

E-Mail: Sangram1704@gmail.com

Comments:

< Back Next > Cancel

**Step 4: Ensure that all checkboxes are checked and then click next.**

Case Log Options

**Case Log Options**

The case log is a text file named FTKlog 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

**Step 5: Select all and Click 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, dSearch, 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 6: Select Email Emphasis and Click Next.**

**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 ☐ Encrypted ☐ 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 7: Click on Add evidence, check Individual File and select the .pst file**

**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... Edit Evidence... Remove Evidence Refine Evidence - Advanced...

Display Name	Source	Name/Nu...	Type	Refined	Time Zone	Comment
--------------	--------	------------	------	---------	-----------	---------

< Back Next > Cancel

**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... Edit Evidence... Remove Evidence Refine Evidence - Advanced...

Display Name	Source	Name/Nu...	Type	Refined	Time Zone	Comment
--------------	--------	------------	------	---------	-----------	---------

< Back Next > Cancel

**Add Evidence to Case**

Type of Evidence to Add to Case

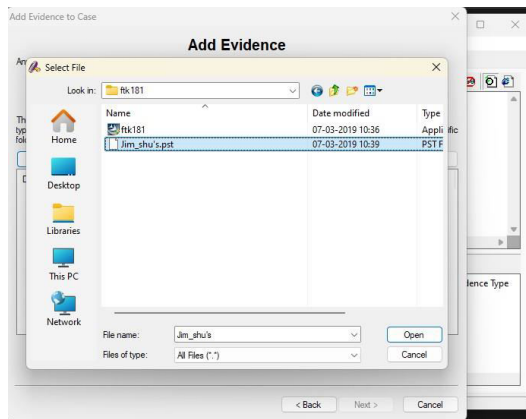
☐ Acquired Image of Drive

☐ Local Drive

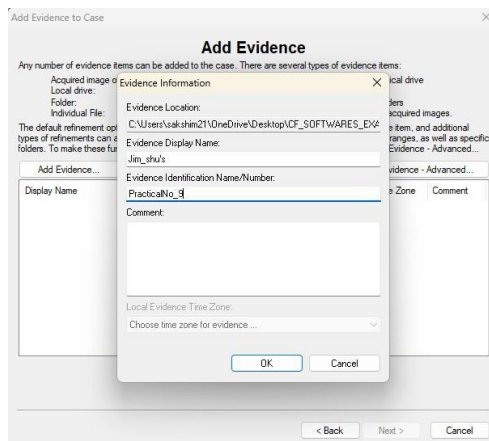
☐ Contents of a Folder

☒ Individual File

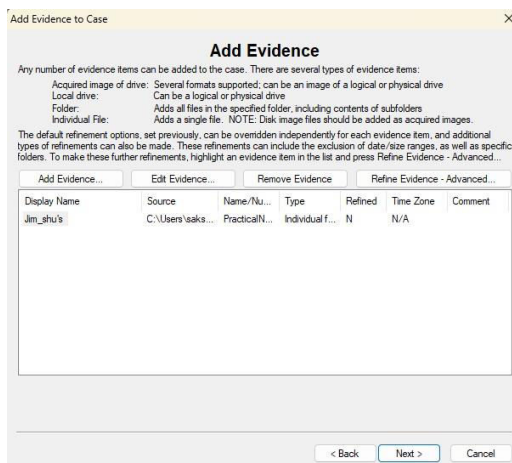
Continue... Cancel



**Step 8:** Fill the following and click OK.

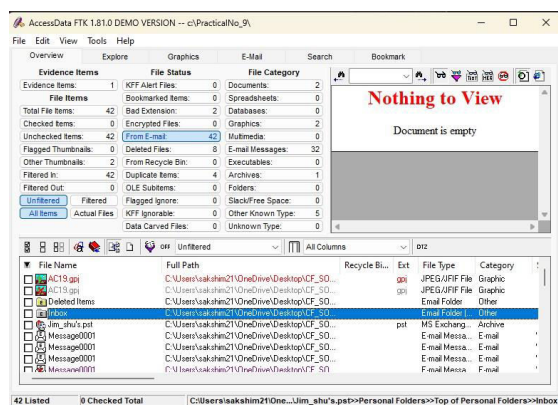
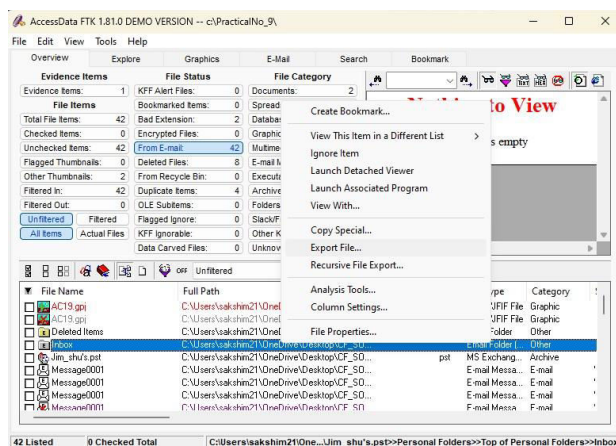


**Step 9:** Click next.

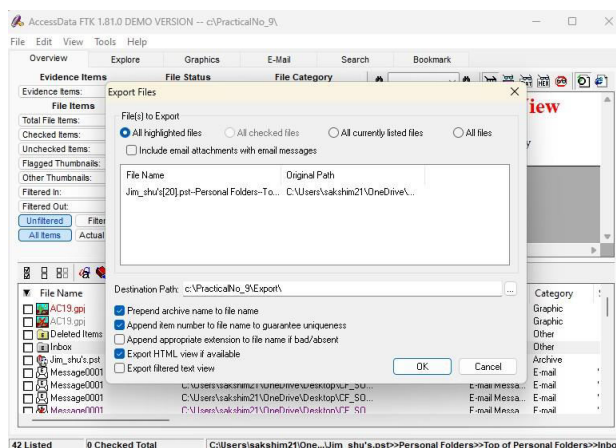


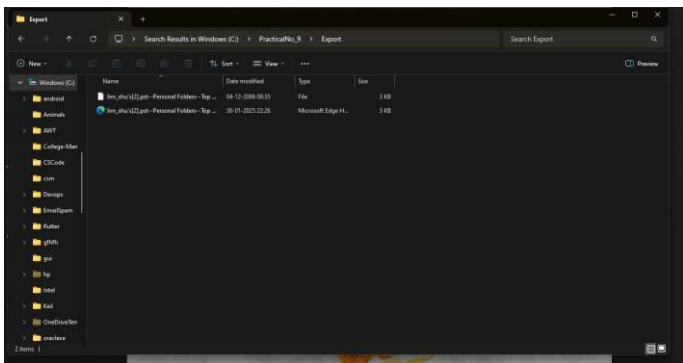
**Step 10:** Click finish.



**Step 11: Now select “From E-mail”.****Step 12: Select any message and Export it as a file.**

Make sure to check “Export HTML view if available” and Click on OK.

**Step 13: Deleted Message is recovered at the specified location.**



**Step 14:** Click on .html file, it will get open in the Browser showing the content of the email.

