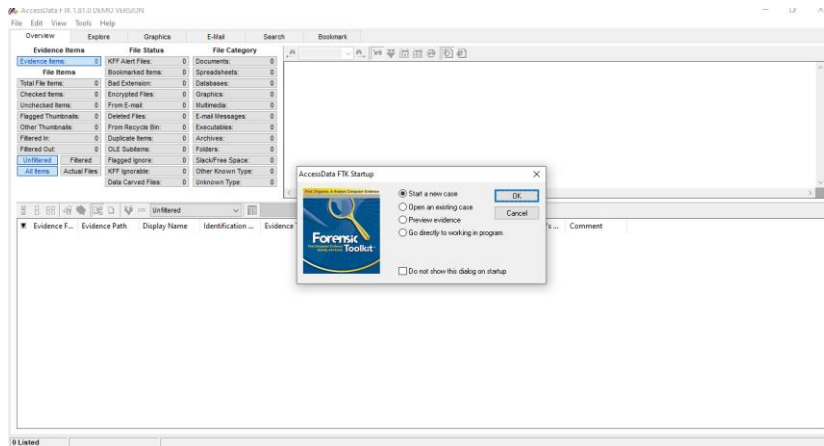


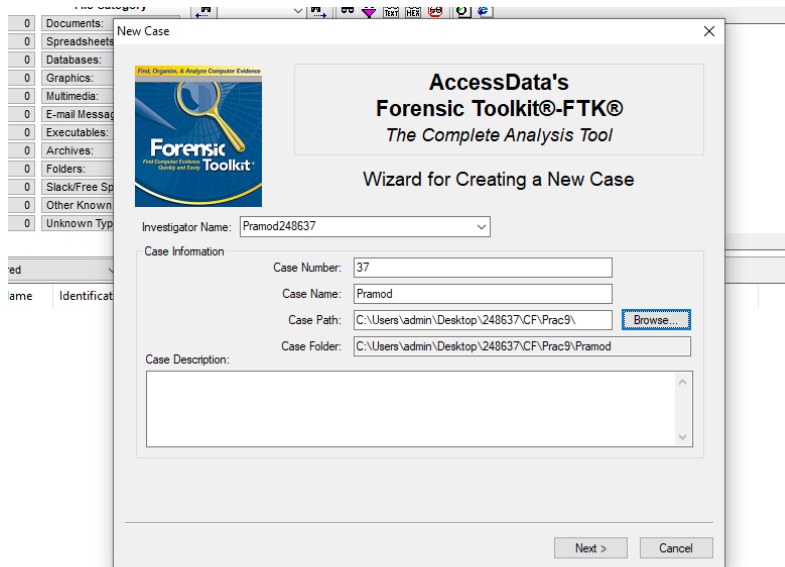
## Practical 9

### Aim: Email Forensics

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



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



#### Step 3: Click next.

The screenshot shows the 'FTK Report Wizard - Case Information' dialog box. It contains the following fields:

- Agency/Company: MCC
- Examiner's Name: Pramod
- Address: Dom
- Phone: 205
- Fax: 34
- E-Mail: 3345
- Comments: 453254

At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

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

The screenshot shows the 'Case Log Options' dialog box. It contains the following text and 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.

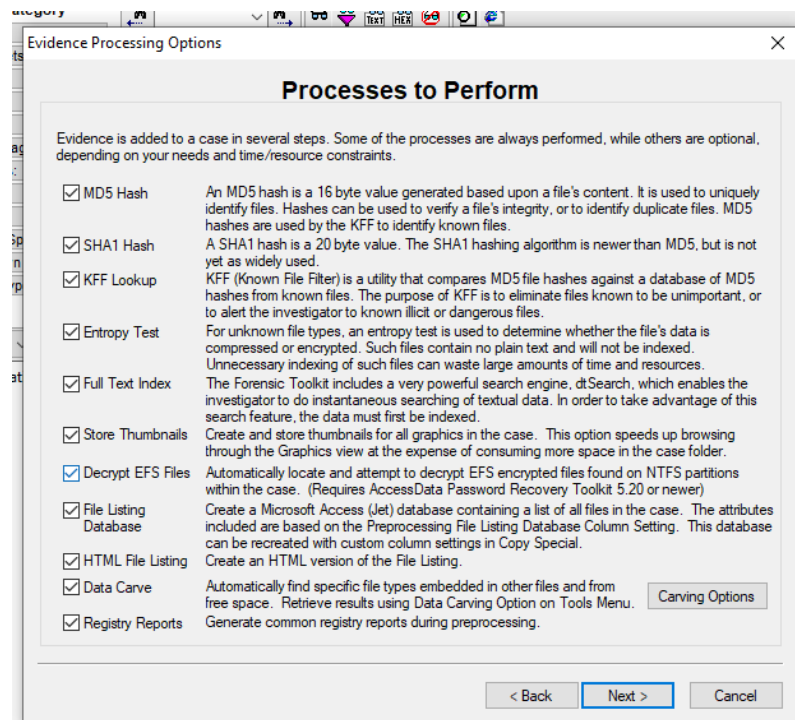
You can also add your own comments to the log file at any time by selecting "Add Case Log Entry..." under the "Tools" menu item, and you can view the log file by selecting "View Case Log" under the "Tools" menu item.

Events to go in the Case Log

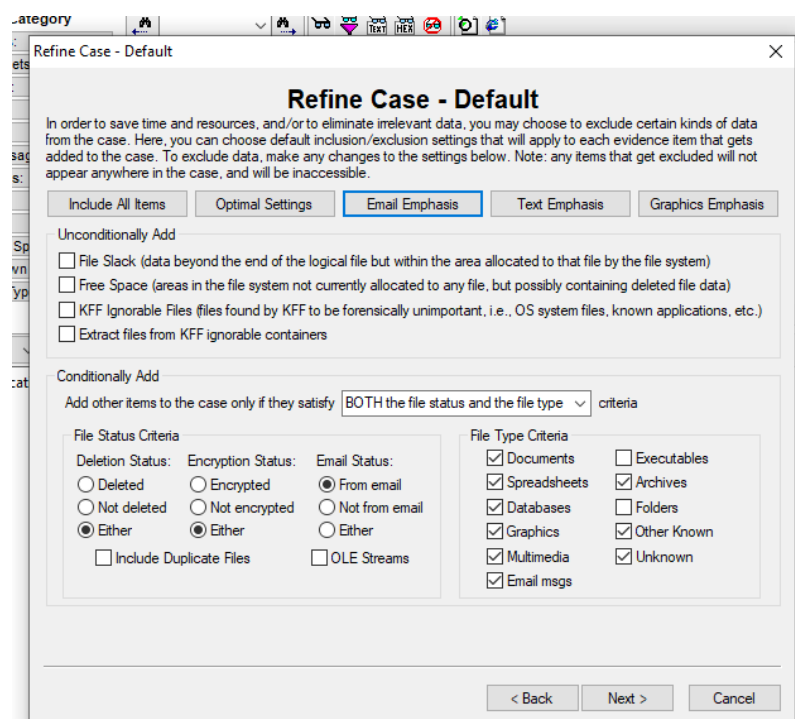
<input checked="" type="checkbox"/> Case and evidence events	Events related to the addition and processing of file items when evidence is added or when using Analysis Tools later in the case.
<input checked="" type="checkbox"/> Error messages	Events related to any error conditions encountered during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

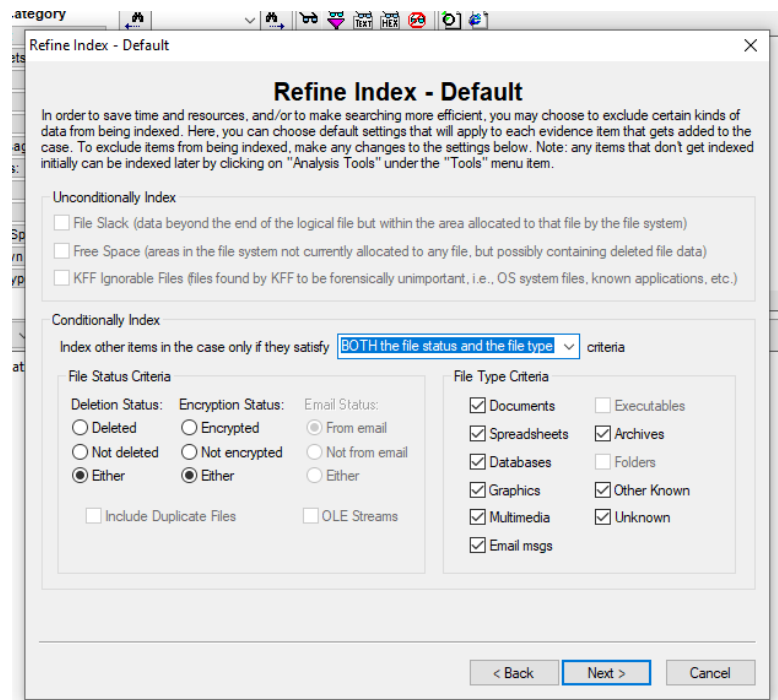
At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

**Step 5:** Select all and Click next.

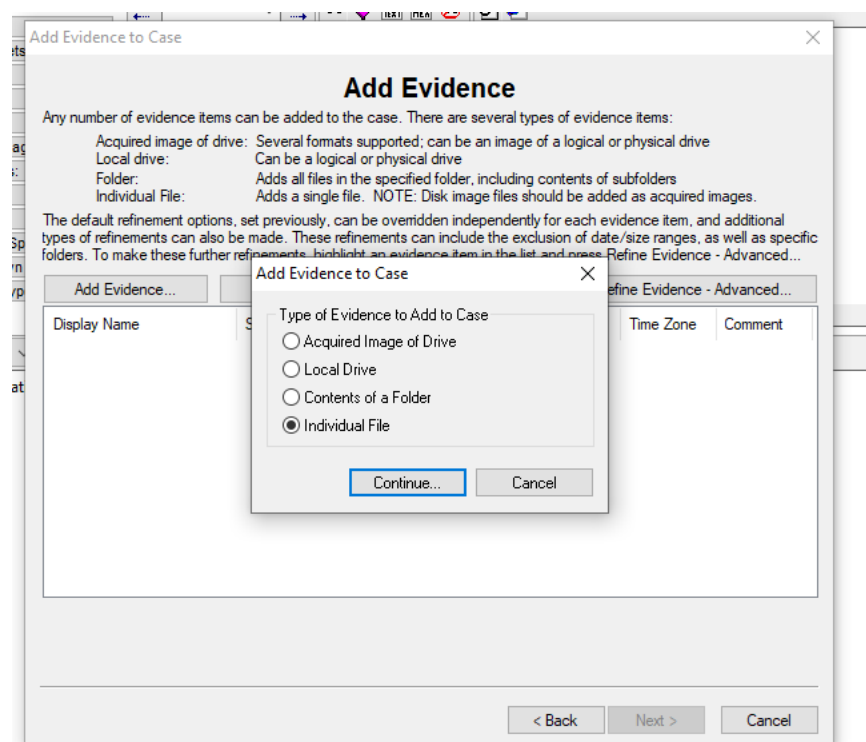


### Step 6: Select Email Emphasis and Click Next.

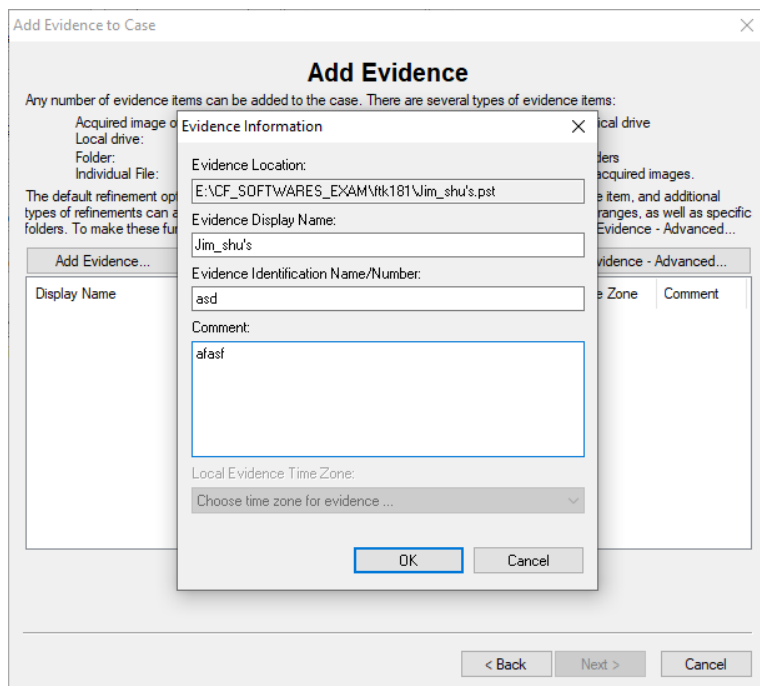




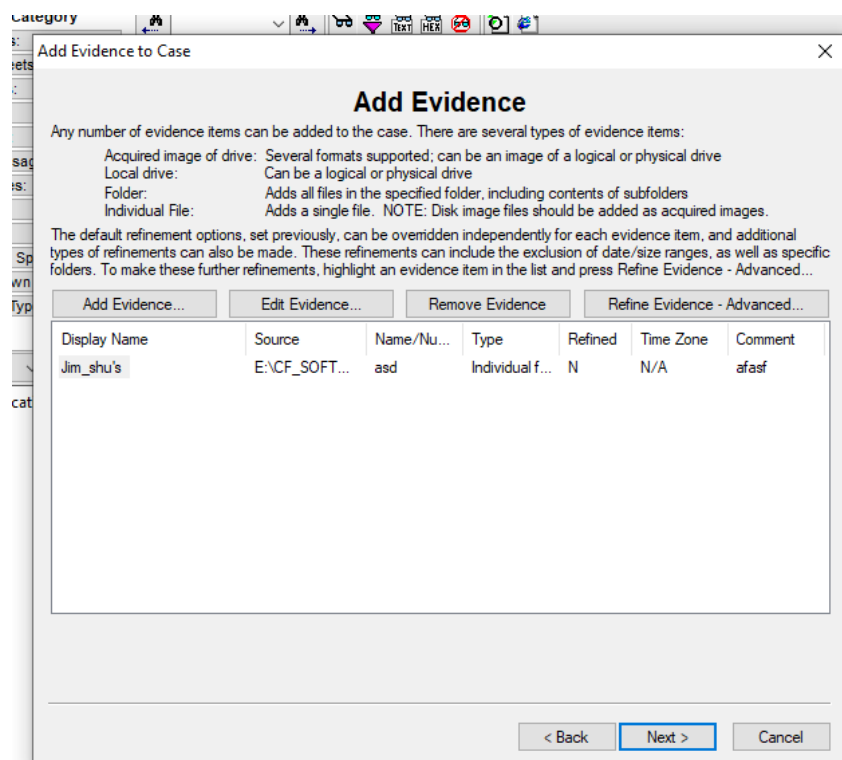
**Step 7:** Click on Add evidence, check Individual File and select the .pst file.



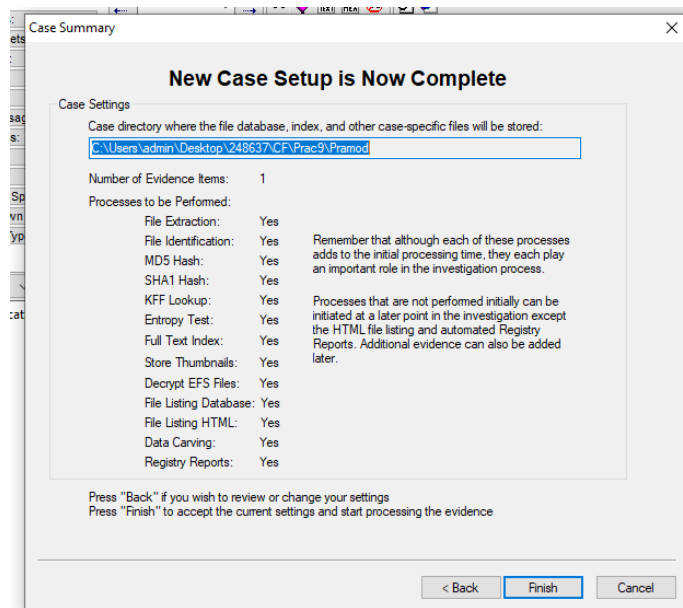
**Step 8:** Fill the following and click OK.



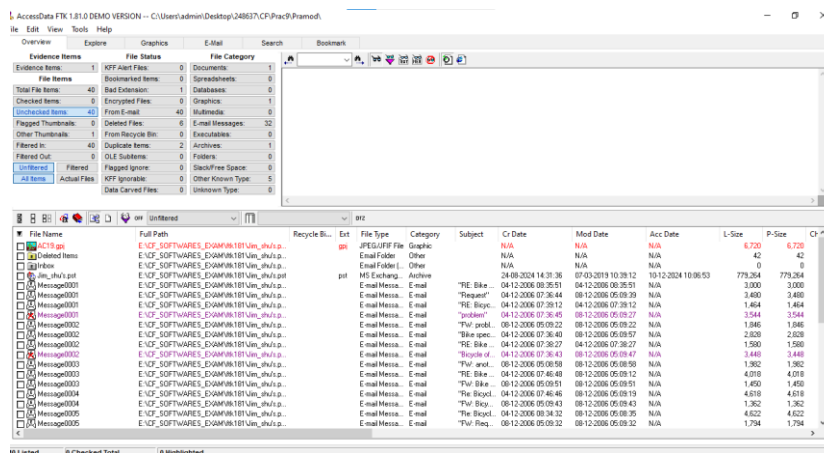
**Step 9:** Click next.



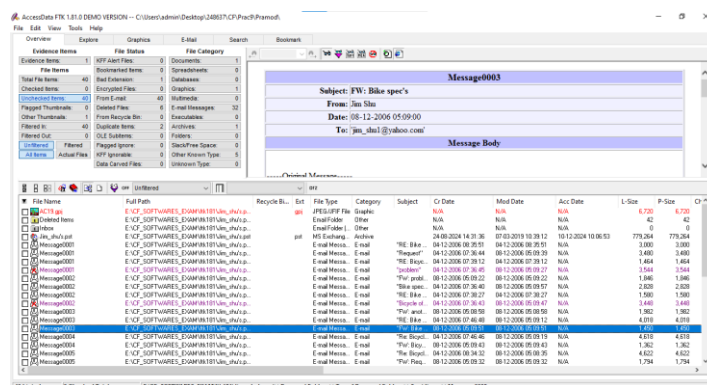
**Step 10:** Click finish.



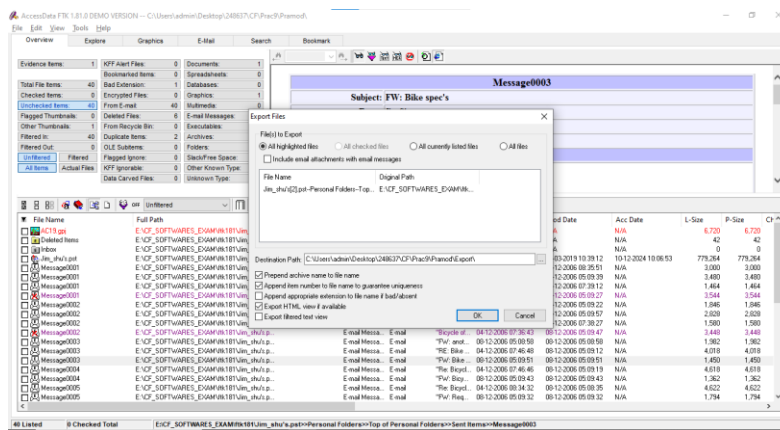
**Step 11: Now select “From E-mail”.**



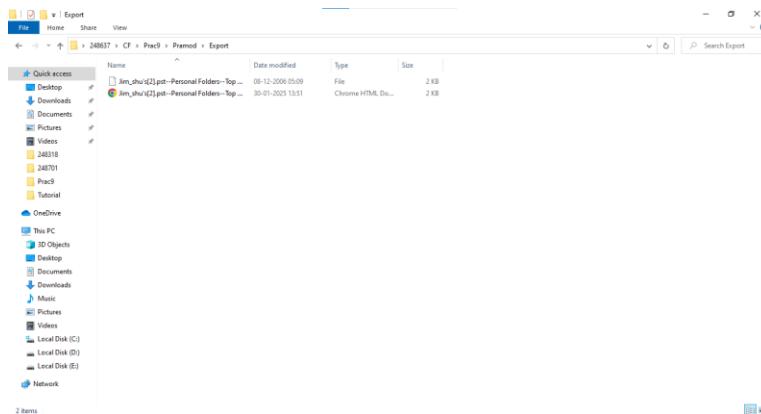
**Step 12: Select any message and Export it as a file.**



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.

