NAME : SATHYAPRAKASH SAHOO **CLASS** : BSC. TY. CS

ROLL NO : CS- 4124 **DIV** : 2 **BATCH** : C

SUBJECT : CYBER FORENSICS - PRACTICAL

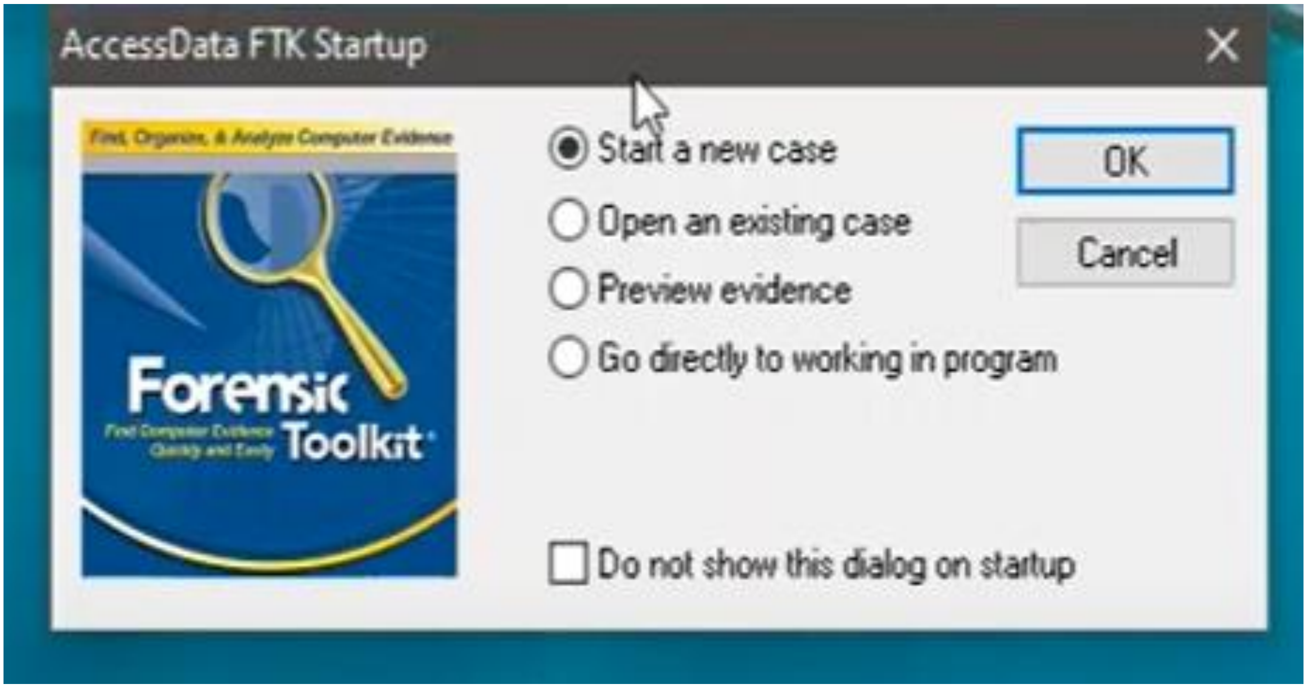
PRACTICAL NO. 9

AIM : Email forensics

1. Mail service providers
2. Email protocols
3. Recovering emails
4. Analyzing email headers

STEPS : follow the below steps –

1. Start the AccessData FTK software and choose start new case



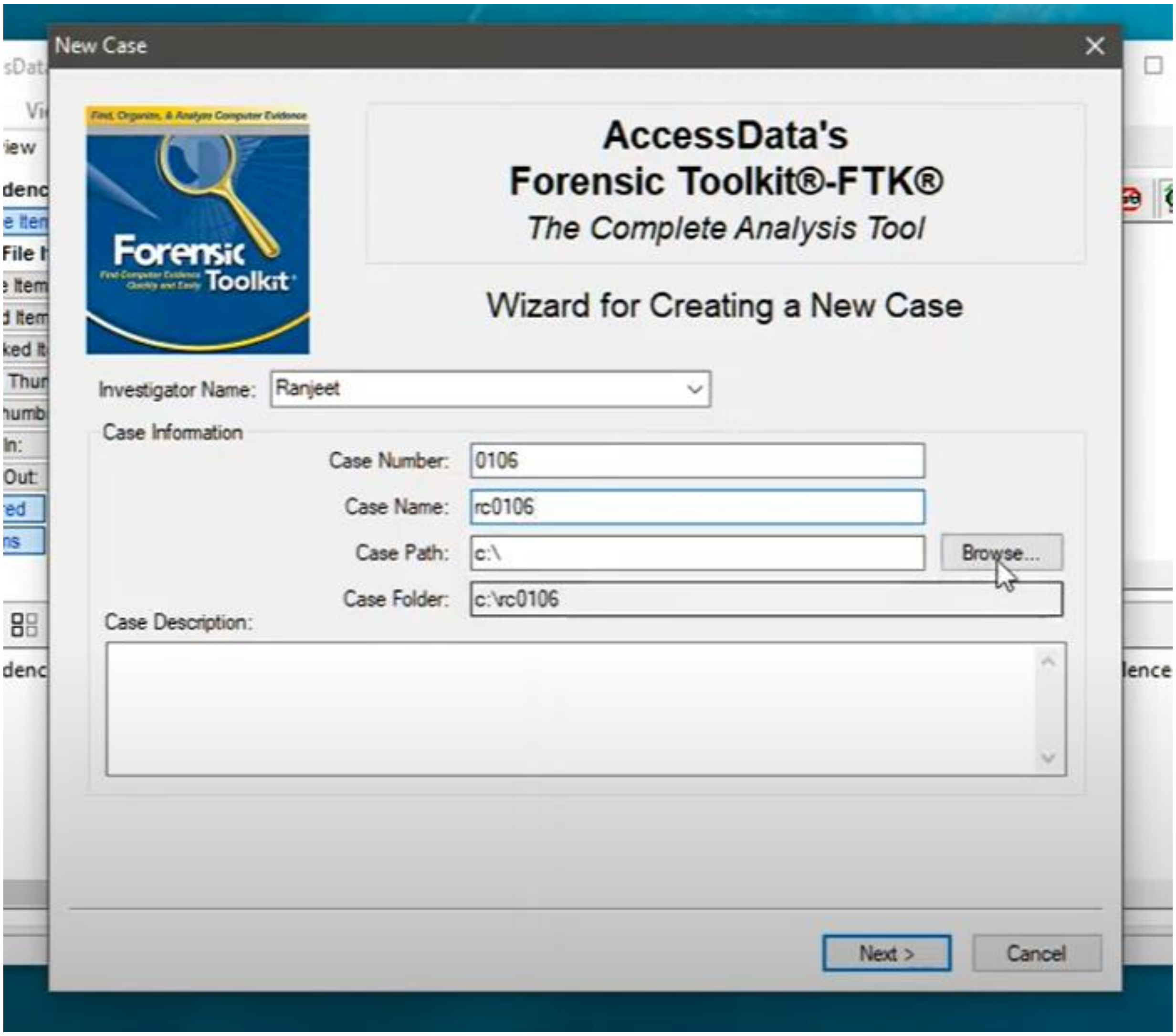
AccessData FTK Startup

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

□ Do not show this dialog on startup

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

2. Enter the required details such as investigator name case number and case path



Investigator Name: Ranjeet

Case Information

Case Number: 0106

Case Name: rc0106

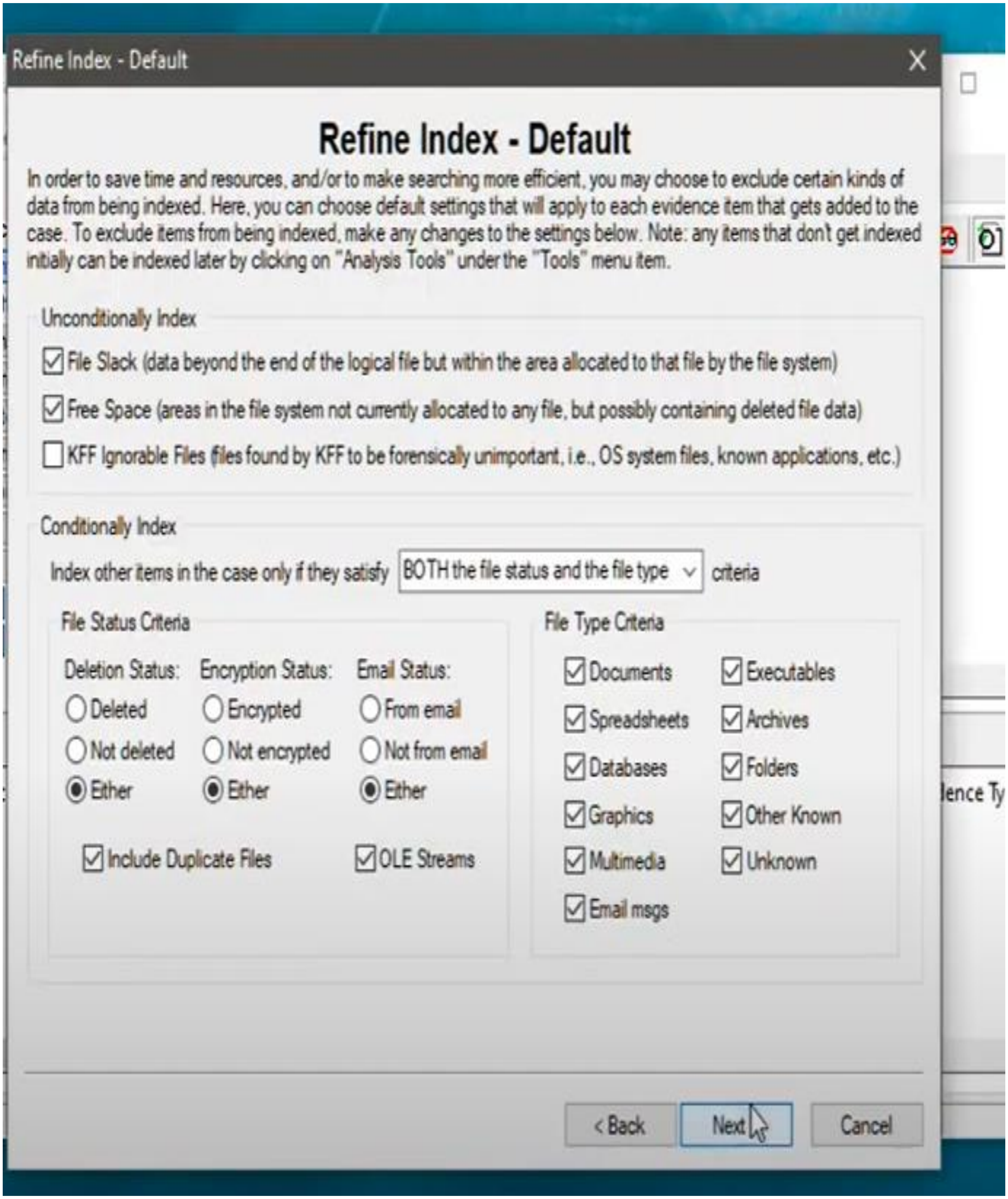
Case Path: c:\

Case Folder: c:\rc0106

Case Description:

3. Select next and a case log options window will appear . select next in that window and move further with the process

4. In the refine index default window make sure the following options are set accordingly



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

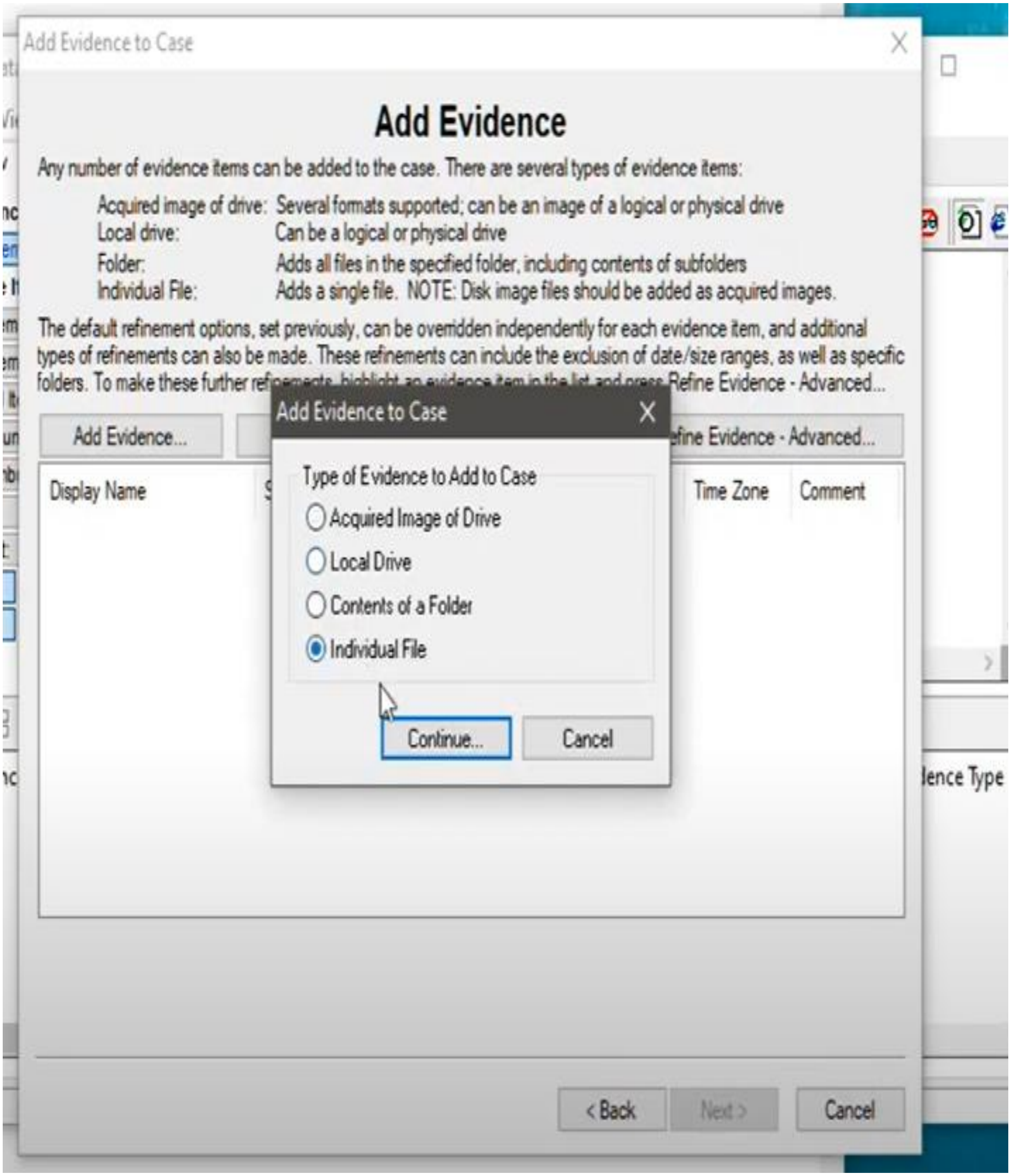
Email Status: ○ From email ○ Not from email ● Either

☑ Include Duplicate Files ☑ OLE Streams

File Type Criteria

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

5. Click next and a new window will open which will ask for evidence file. Select on add evidence and select individual 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 to Case

Type of Evidence to Add to Case

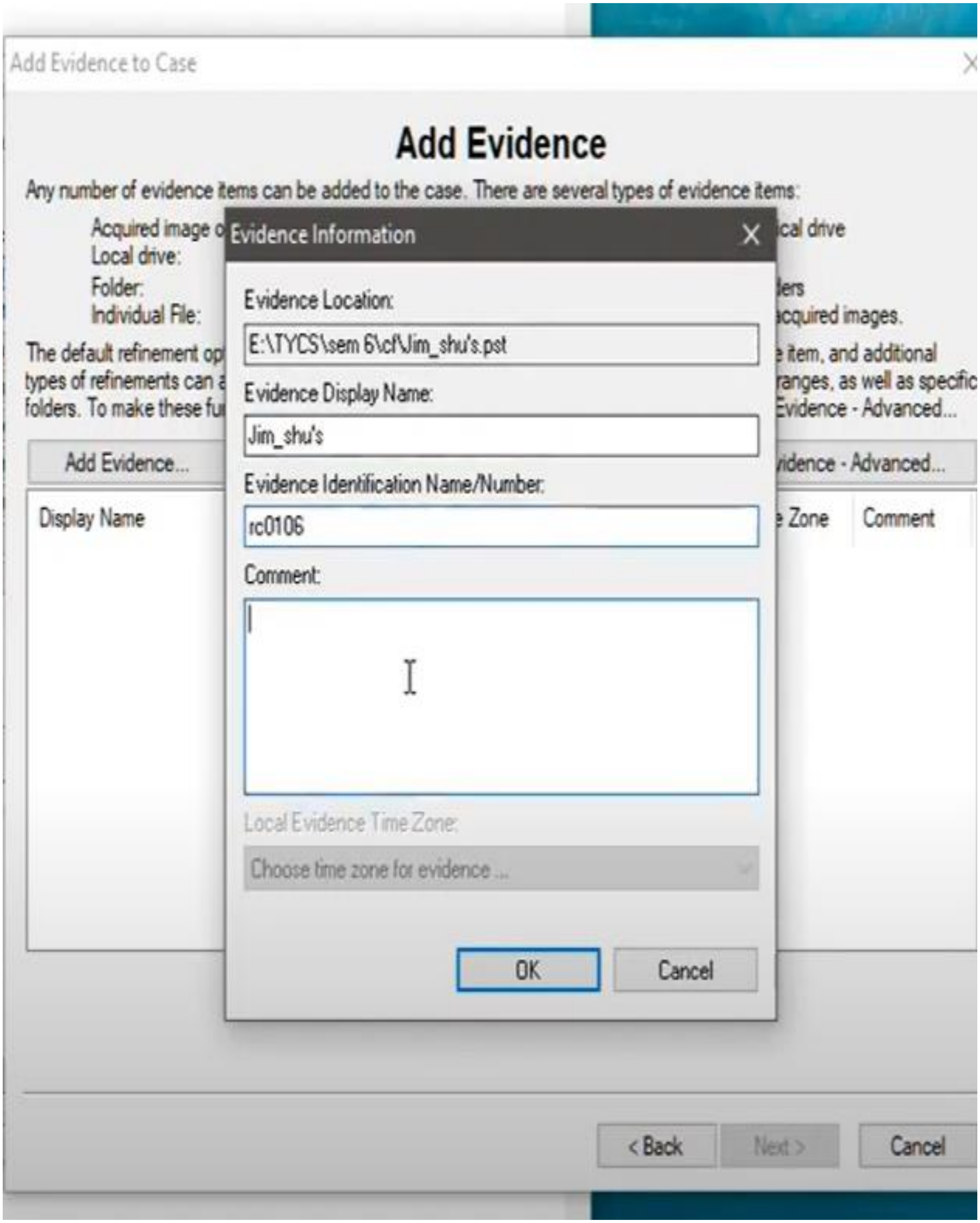
○ Acquired Image of Drive

○ Local Drive

○ Contents of a Folder

● Individual File

6. Select the proper evudence file from the path and import it in the software



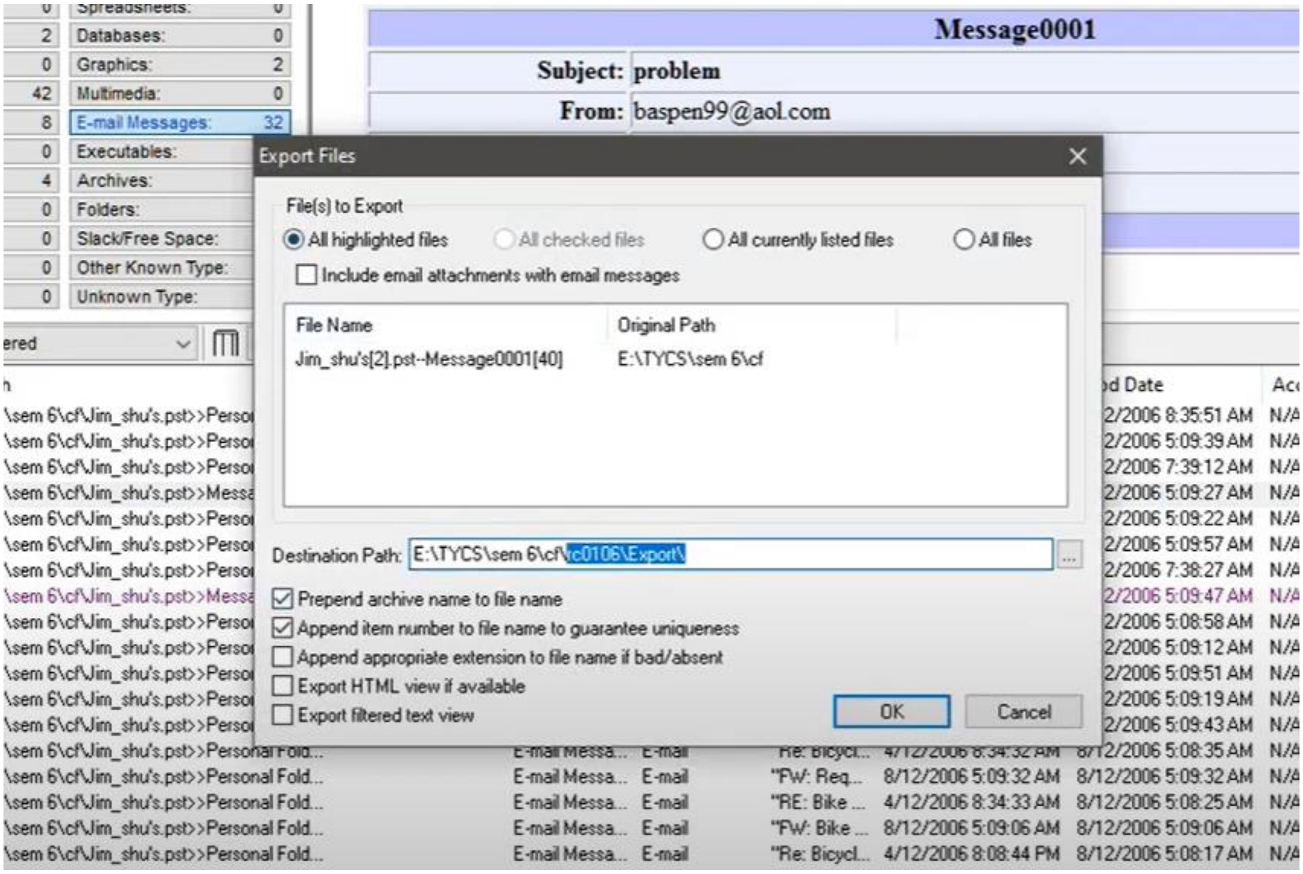
Evidence Location: E:\TYCS\sem 6\cf\Jim_shu's.pst

Evidence Display Name: Jim_shu's

Evidence Identification Name/Number: rc0106

Comment:

7. Click next and finish to create the case file for the evidence



0	Spreadsheets:	0
2	Databases:	0
0	Graphics:	2
42	Multimedia:	0
8	E-mail Messages:	32
0	Executables:	
4	Archives:	
0	Folders:	
0	Slack/Free Space:	
0	Other Known Type:	
0	Unknown Type:	

Message0001

Subject: **problem**

From: baspen99@aol.com

Export Files

File(s) to Export

● 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--Message0001[40]	E:\TYCS\sem 6\cf

Destination Path: E:\TYCS\sem 6\cf\c0106\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

\sem 6\cf\Jim_shu's.pst>>Personal Fold...	E-mail Messa...	E-mail	"Re: Bicycl...	4/12/2006 8:34:32 AM	8/12/2006 5:08:35 AM	N/A
\sem 6\cf\Jim_shu's.pst>>Personal Fold...	E-mail Messa...	E-mail	"FW: Req...	8/12/2006 5:09:32 AM	8/12/2006 5:09:32 AM	N/A
\sem 6\cf\Jim_shu's.pst>>Personal Fold...	E-mail Messa...	E-mail	"RE: Bike ...	4/12/2006 8:34:33 AM	8/12/2006 5:08:25 AM	N/A
\sem 6\cf\Jim_shu's.pst>>Personal Fold...	E-mail Messa...	E-mail	"FW: Bike ...	8/12/2006 5:09:06 AM	8/12/2006 5:09:06 AM	N/A
\sem 6\cf\Jim_shu's.pst>>Personal Fold...	E-mail Messa...	E-mail	"Re: Bicycl...	4/12/2006 8:08:44 PM	8/12/2006 5:08:17 AM	N/A