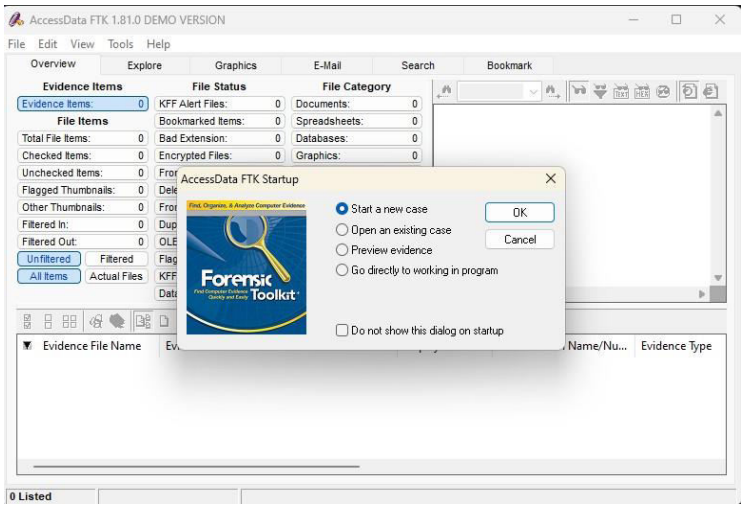
Practical No: 09

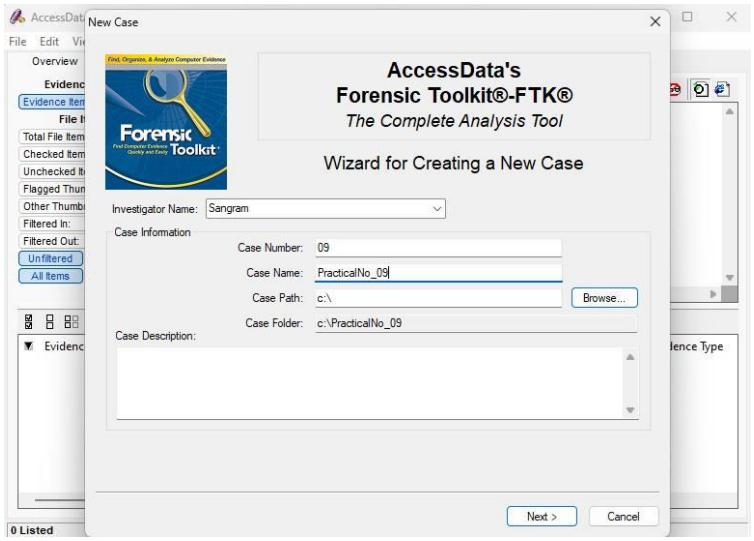
AIM: Email Forensics

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

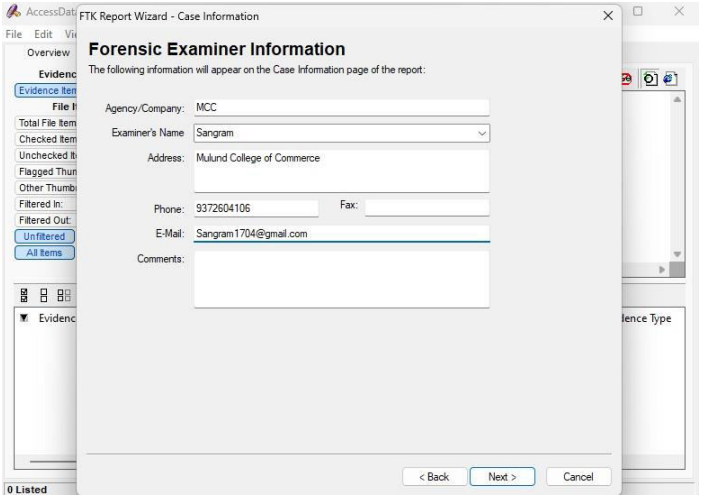
Step 1: Open Forensic Toolkit and click on file new case



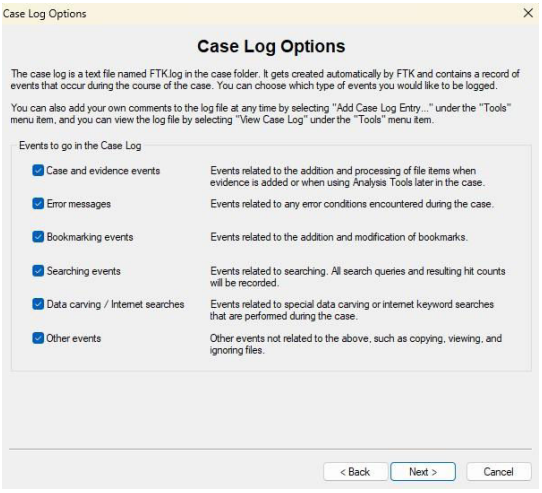
Step 2: Fill the following details and click next.



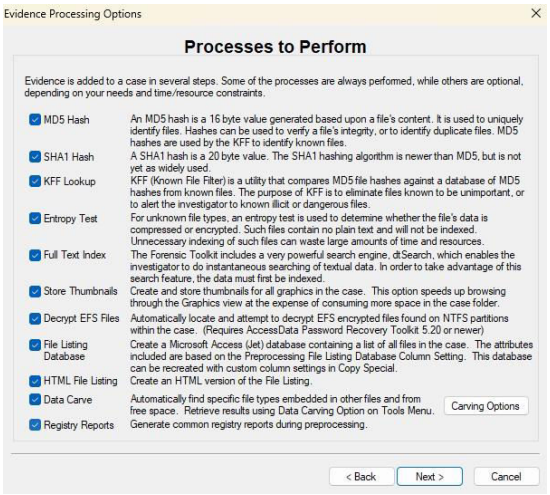
Step 3: Click next.



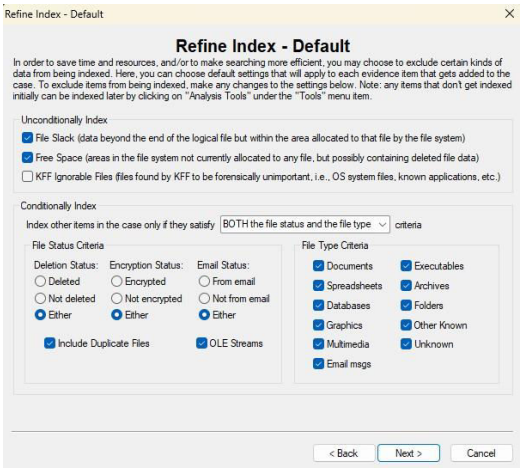
Step 4: Ensure that all checkboxes are checked and then click next.



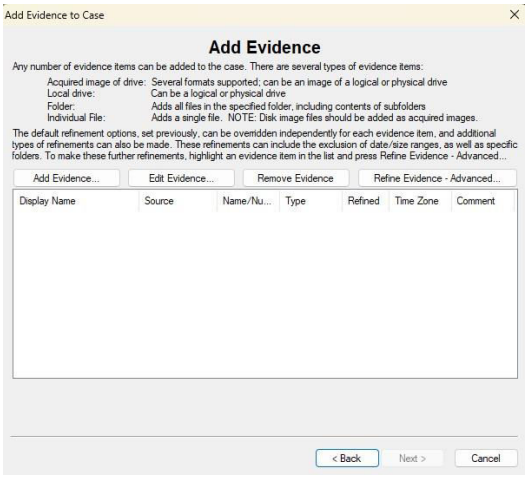
Step 5: Select all and Click next.

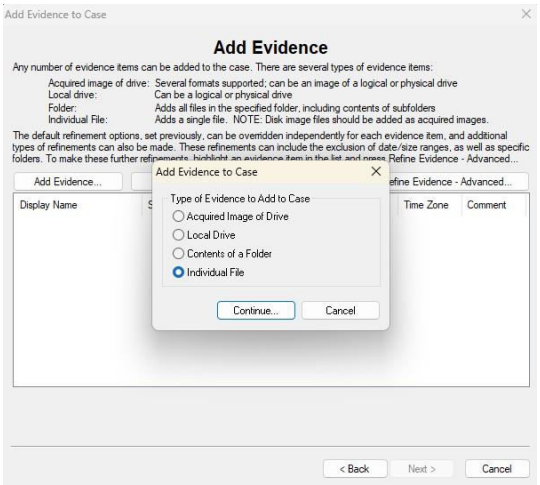


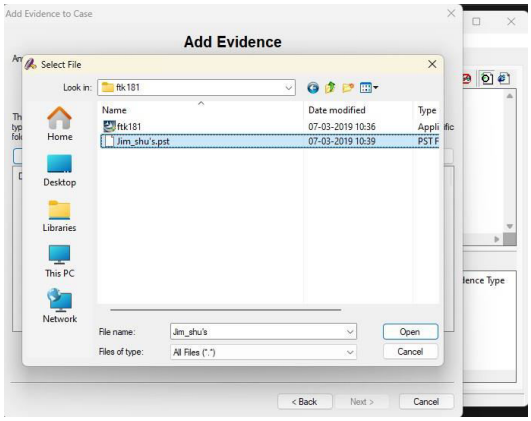
Step 6: Select Email Emphasis and Click Next.



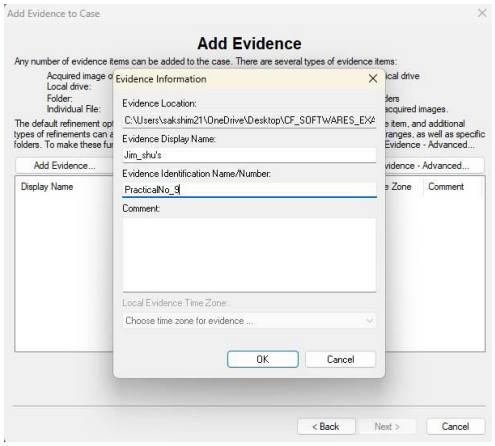
Step 7: Click on Add evidence, check Individual File and select the .pst file



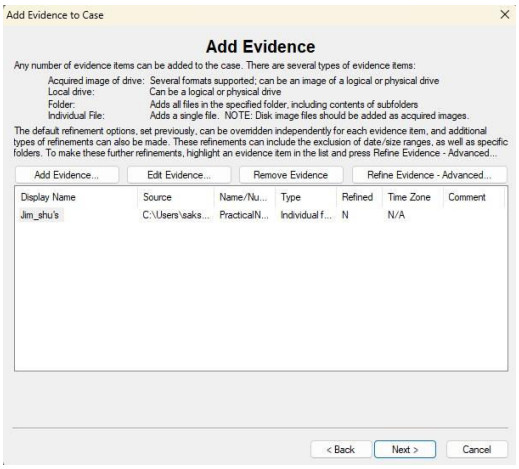




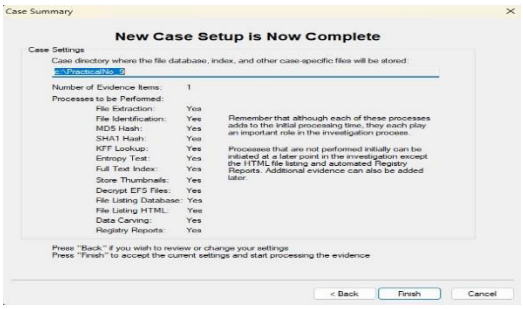
Step 8: Fill the following and click OK.



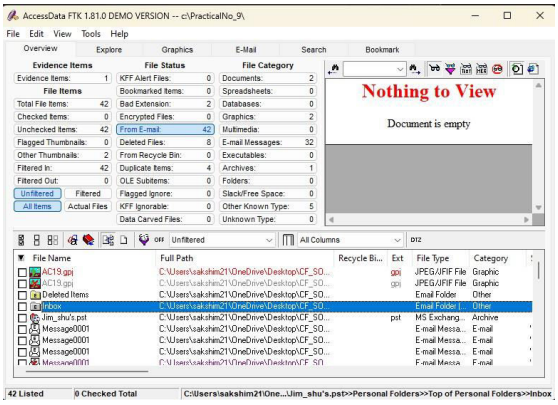
Step 9: Click next.



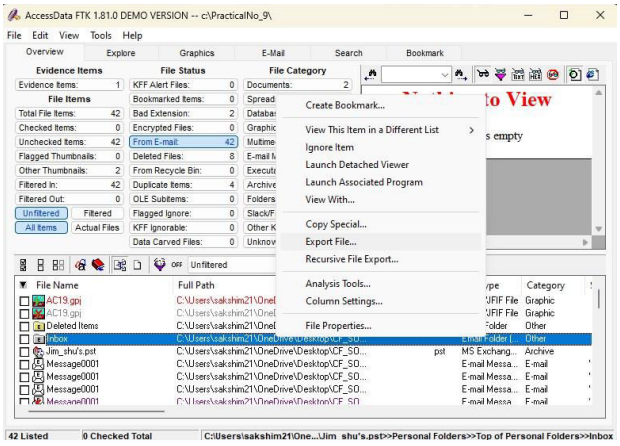
Step 10: Click finish.



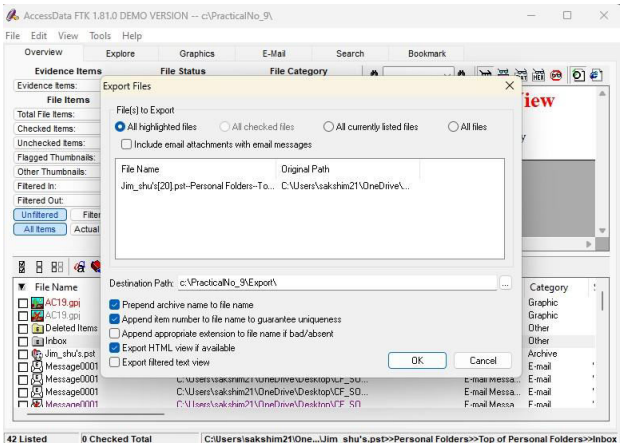
Step 11: Now select “From E-mail”.



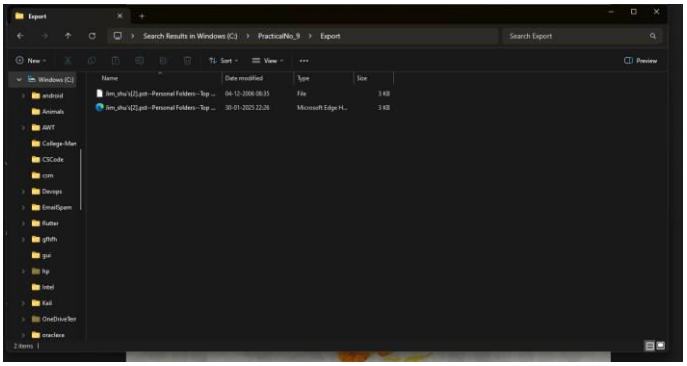
Step 12: Select any message and Export it as a file.



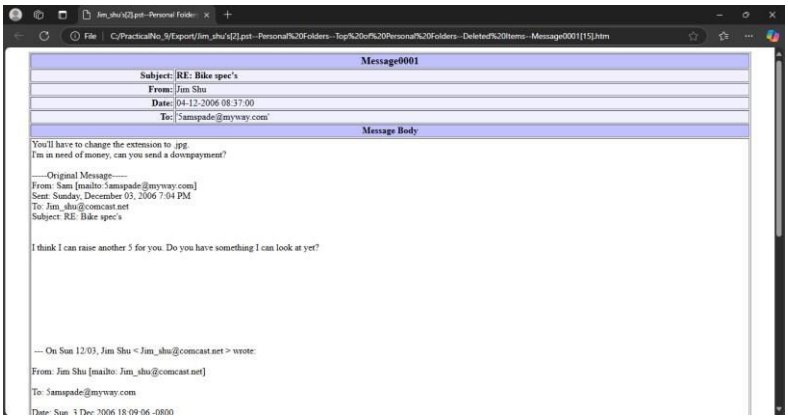
Make sure to check “Export HTML view if available” and Click on OK.



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.



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]

To: 5amspade@myway.com

Date: Sun, 3 Dec 2006 18:09:06 -0800

Subject: RE: Bike spec's

How much are you willing to pay me to get these plans to you?Jim-----Original Message-----From: Sam [mailto:5amspade@myway.com] Sent: Sunday, December 03, 2006 5:40 PMTo: jim_shu@comcast.netSubject: Bike spec'sDo you have them yet?I've got people in Asia ready to duplicate them?Sam_____No banners. No pop-ups. No kidding.Make My Way your home on the Web - http://www.myway.com

_____
No banners. No pop-ups. No kidding.
Make My Way your home on the Web - http://www.myway.com

Attachment
AC19.gpj

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