**Practical No. 9**

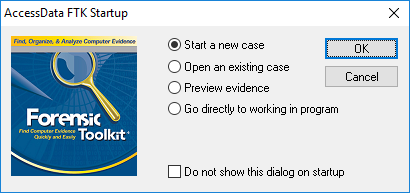
**Aim: Email Forensics**

**- Mail Service Providers**

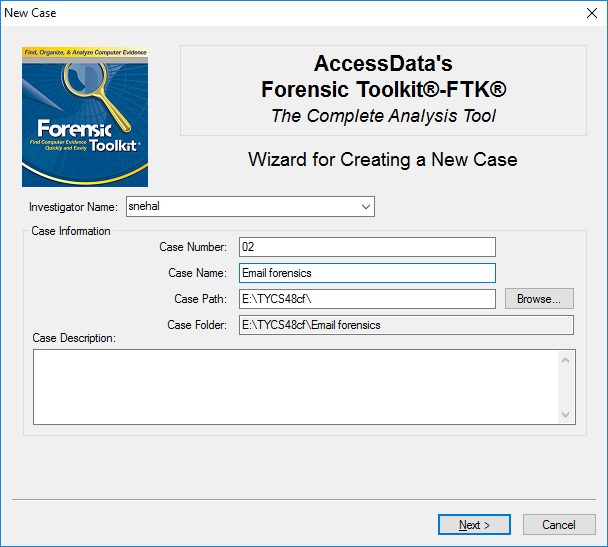
**- Email protocols**

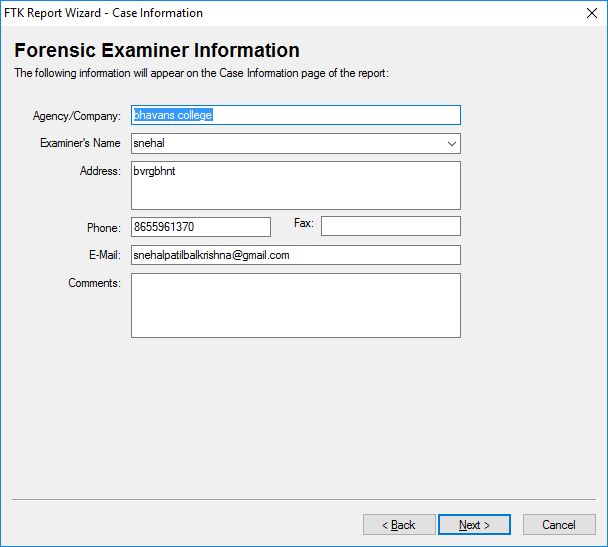
**- Recovering emails**

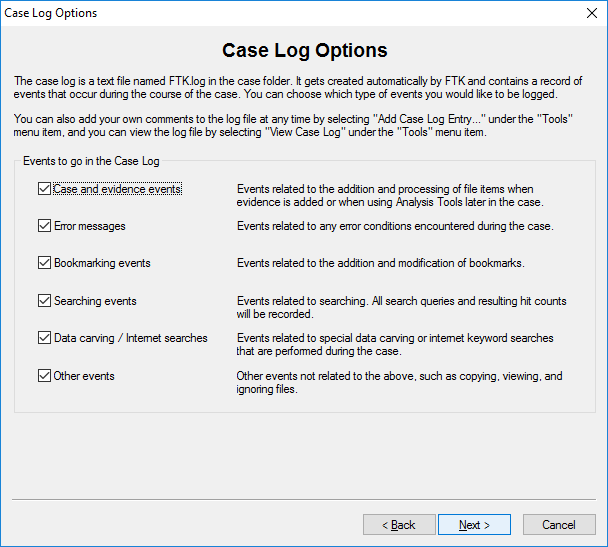
**- Analyzing email header**

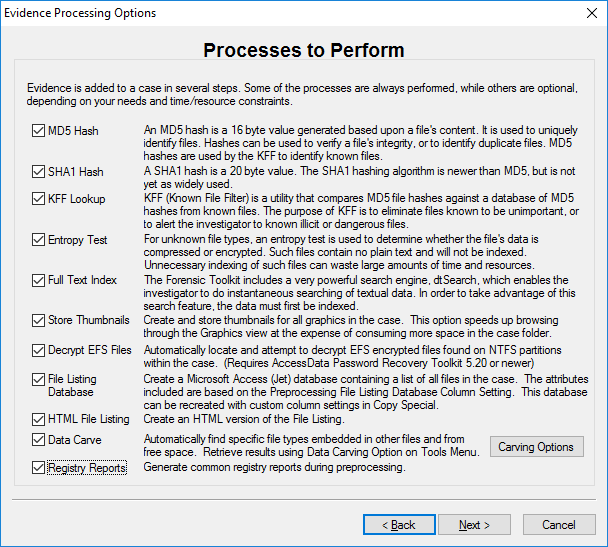
****

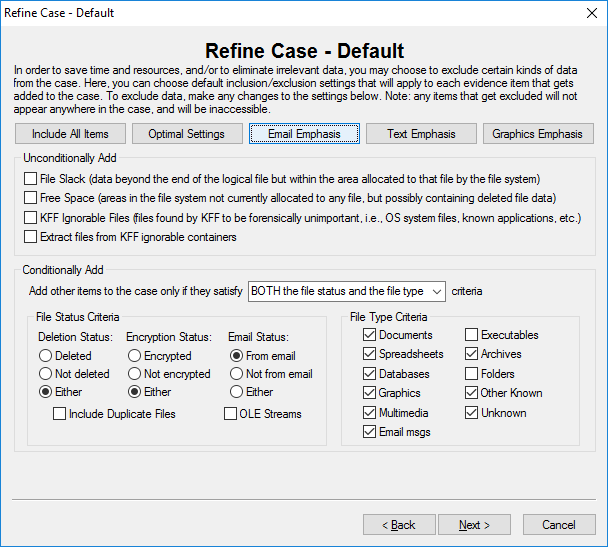
**When the AccessData FTK Startup dialog box opens, click Start a new case, and then click OK.**

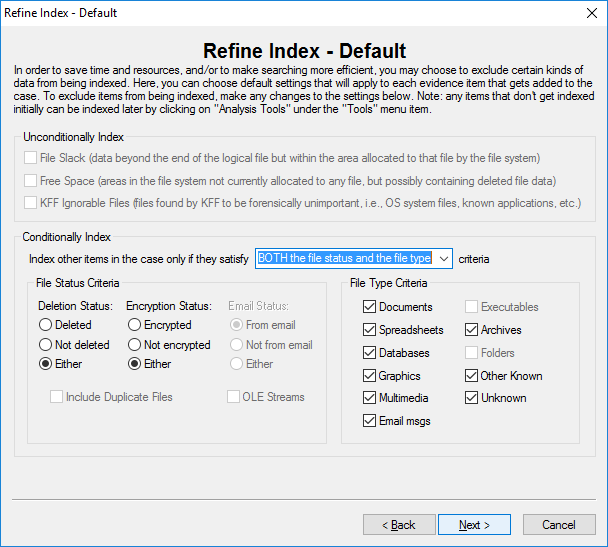
****

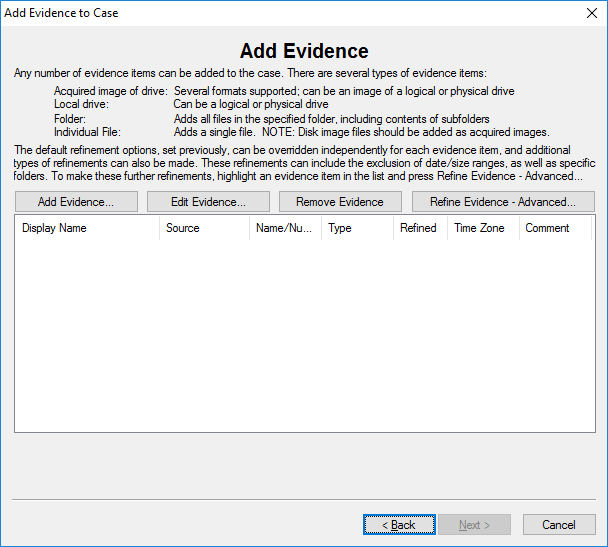
****

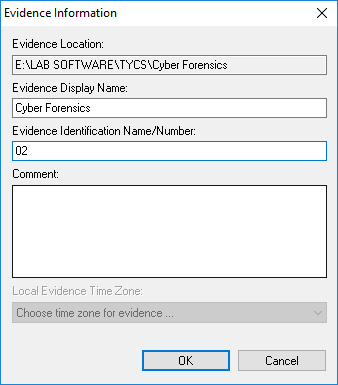
****

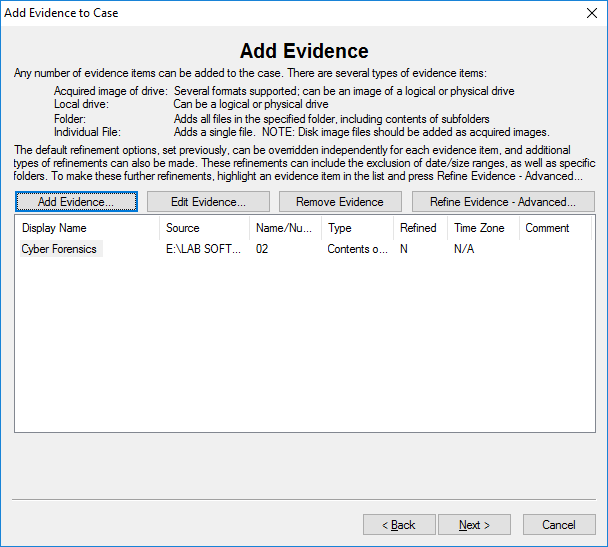
****

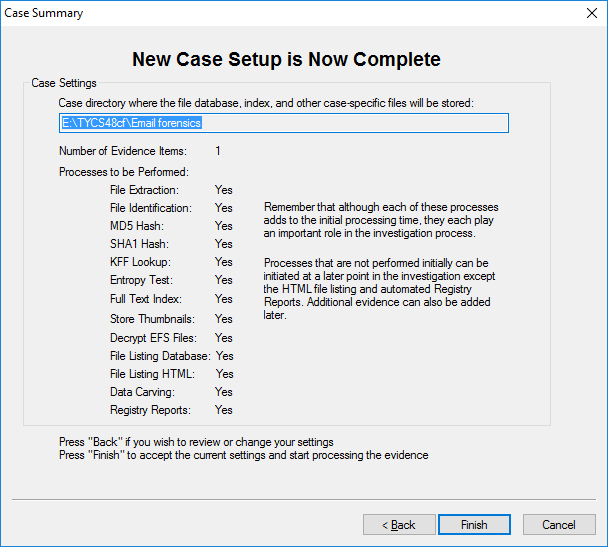
****

****

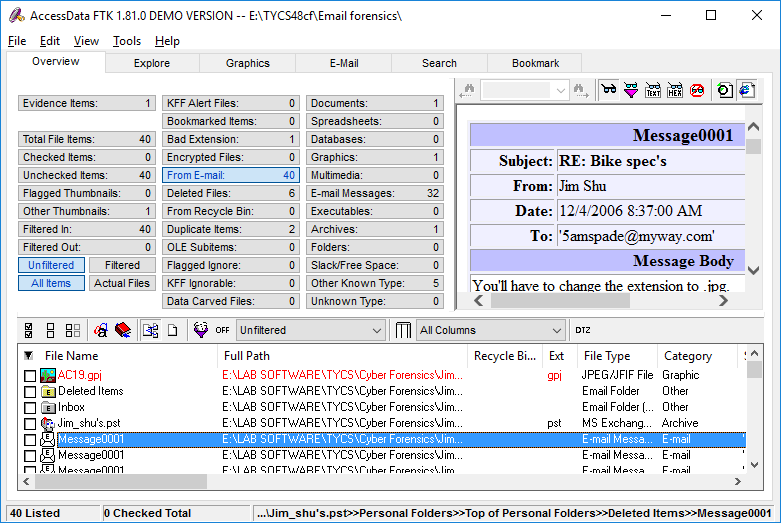
****

****

****

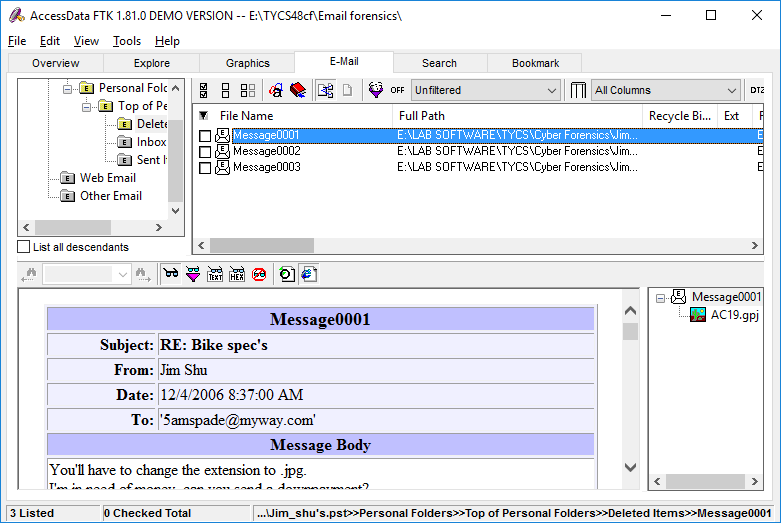
****

**When FTK finishes processing the file, in the main FTK window, click the E-mail Messages button, and then click the Full Path column header to sort the records**

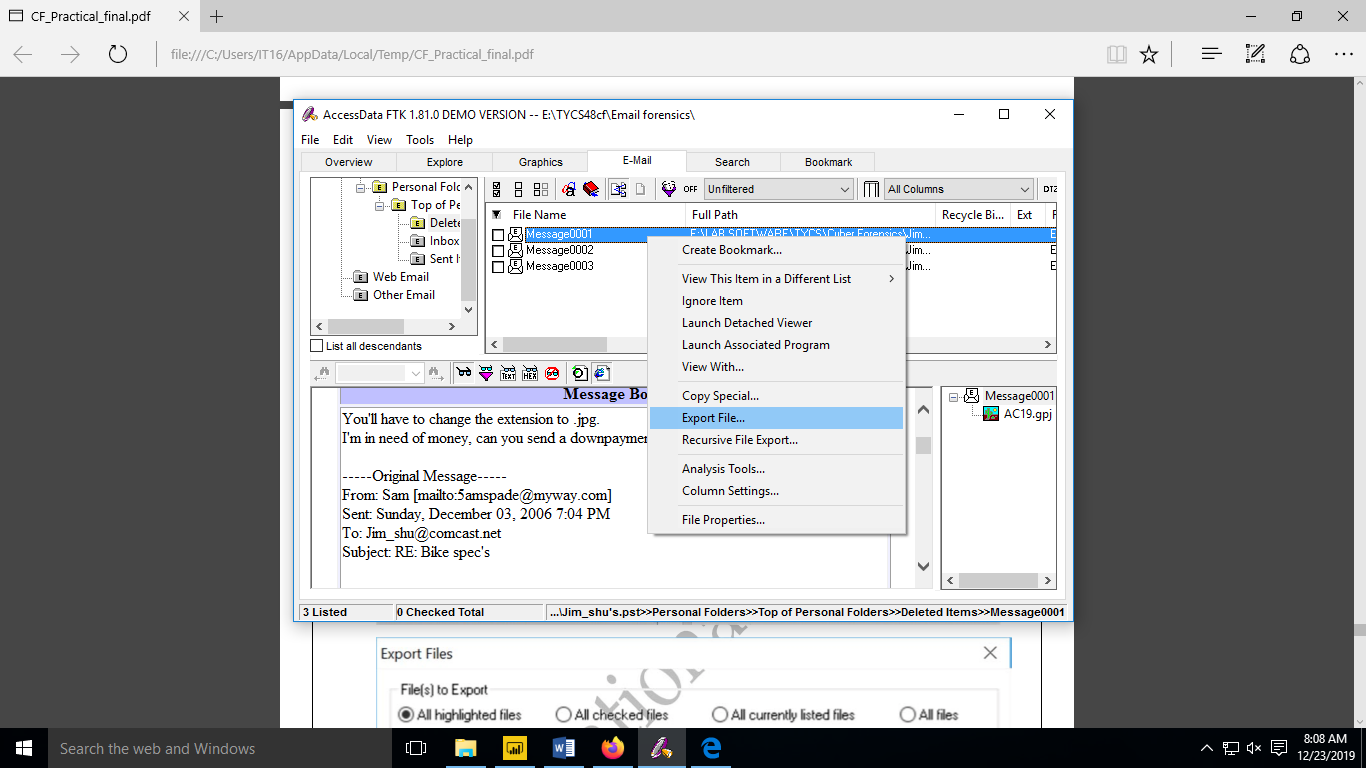
****

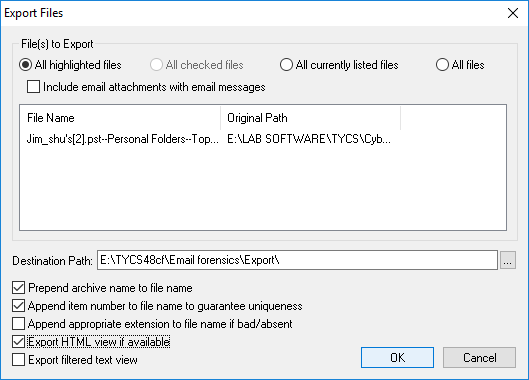
**For email recovery follow following steps:**

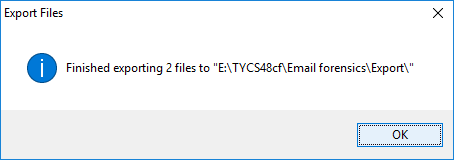
**1. Click the E-Mail tab. In the tree view, click to expand all folders, and then click the Deleted Items folder**

****

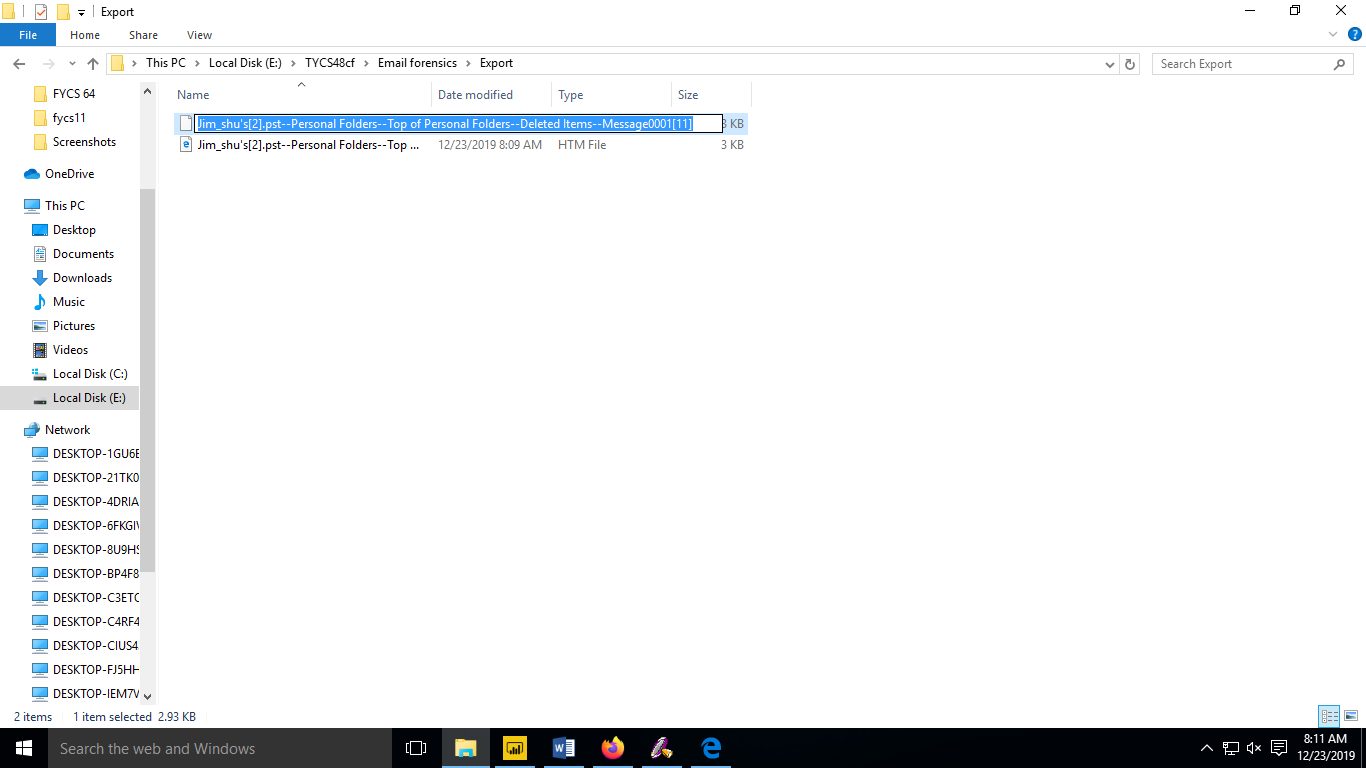
**2. Right-click Message0010 in the File List pane and click Export File. In the Export Files dialog box, click OK**

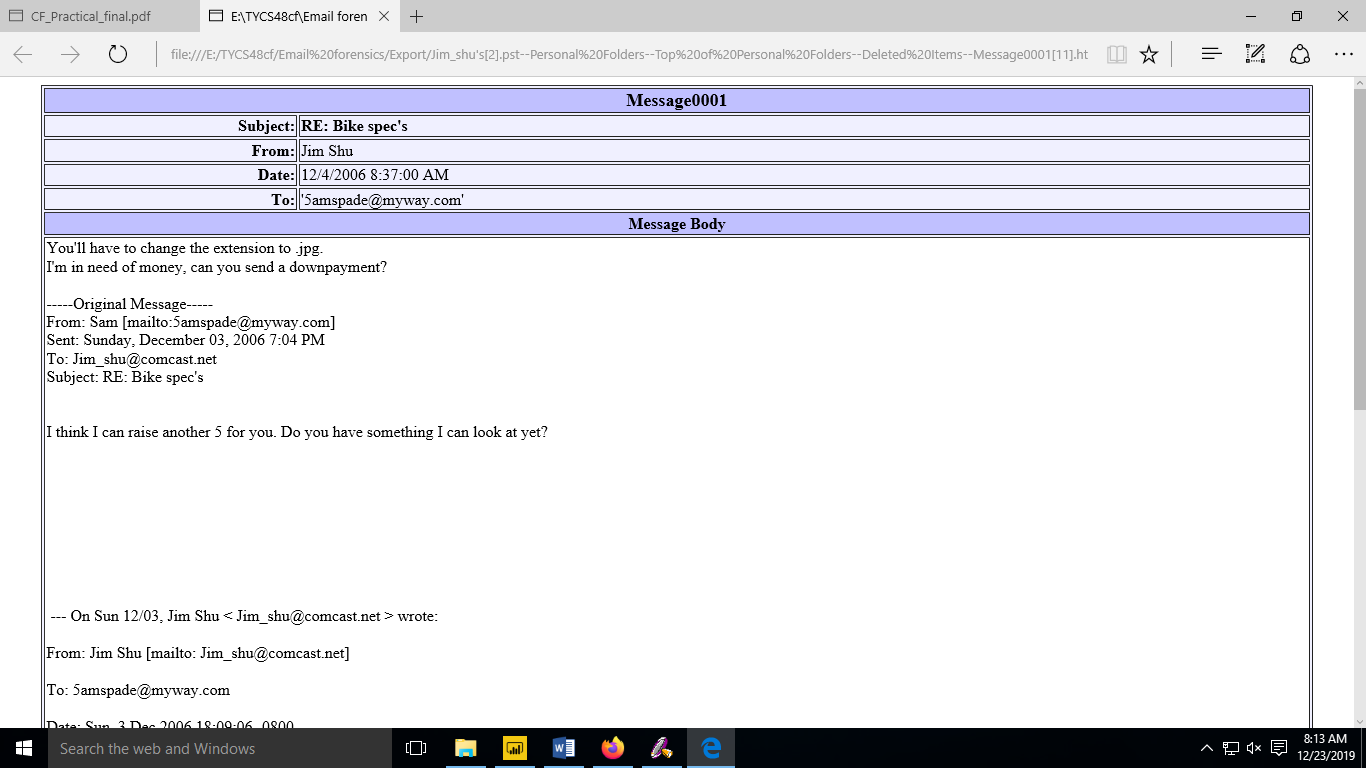
****

****

****

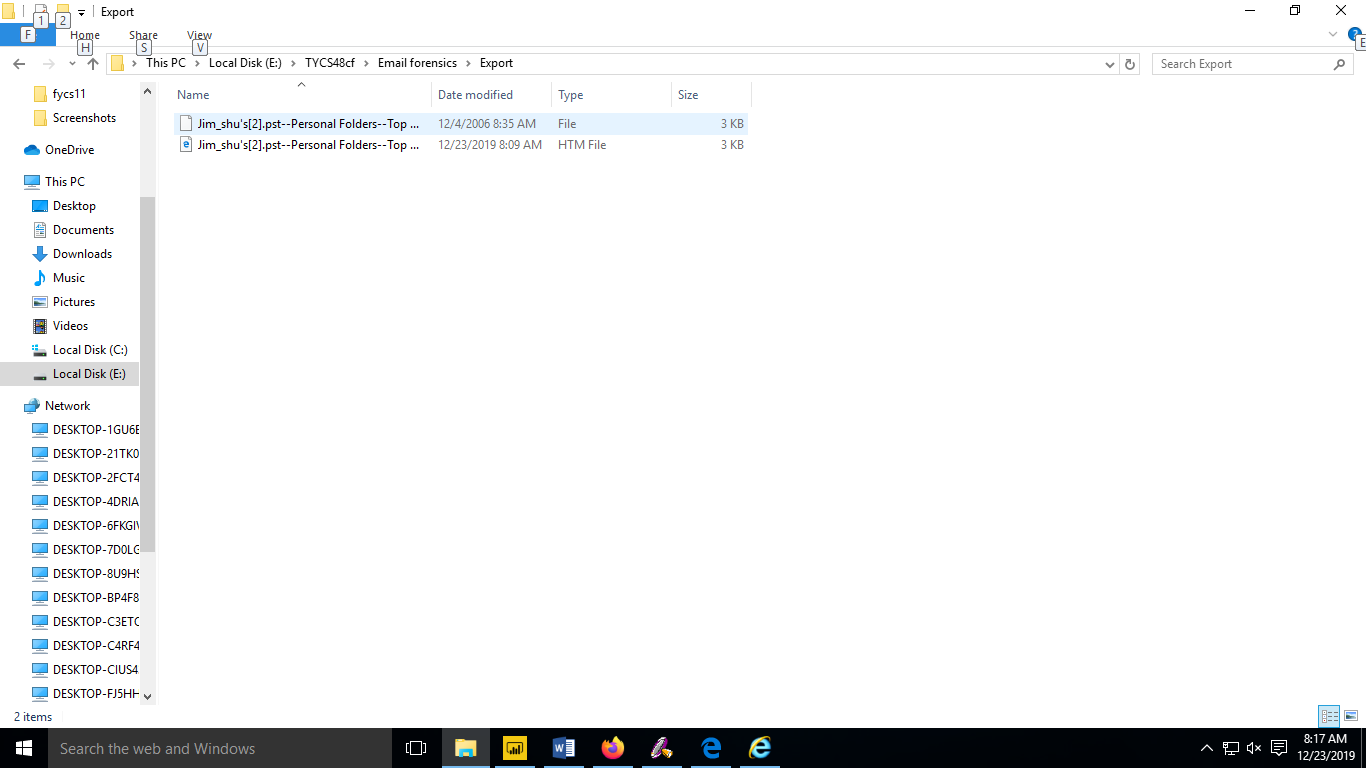
**3. Open the Export folder to view the Email Files, Open the HTML file in browser**

****

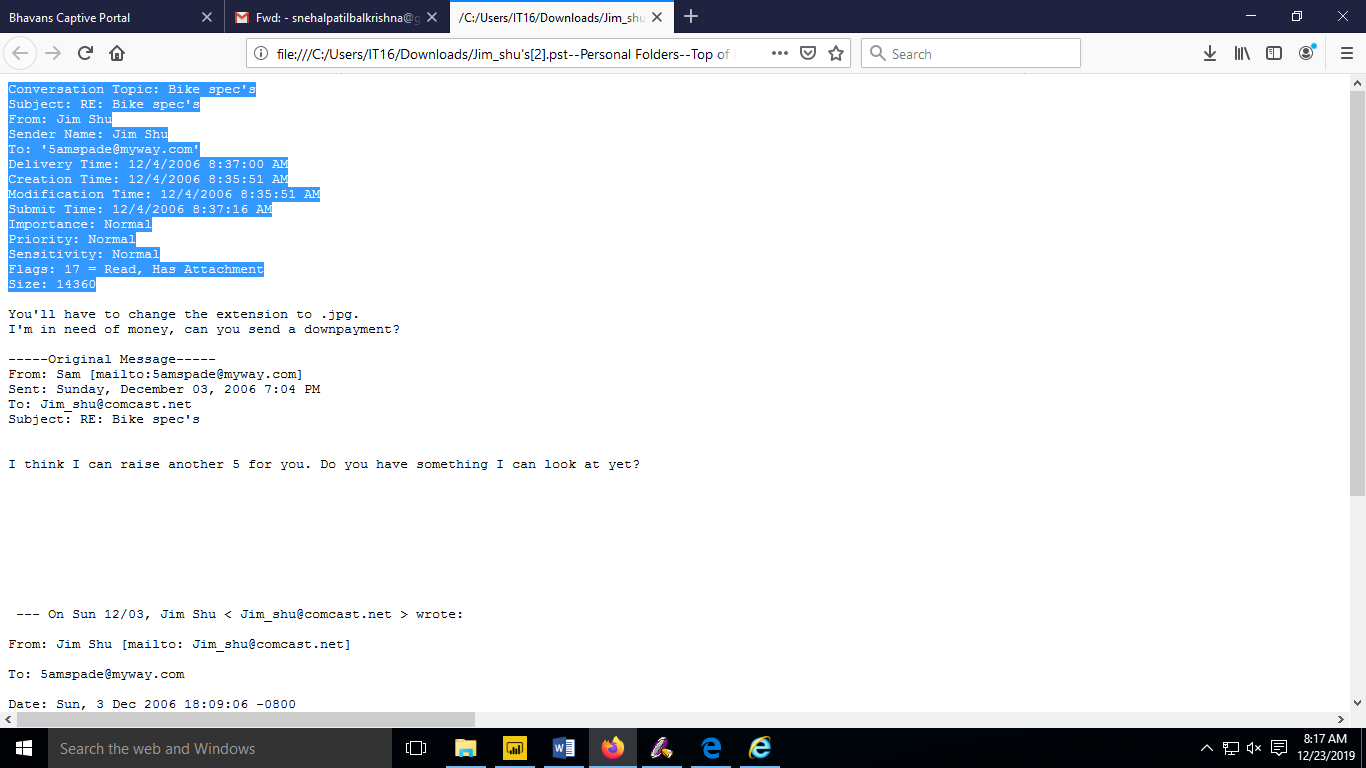
****

**For analyzing header follow following steps:**

**1. Right Click the file type and Open with firefox or chrome view header information**

****

**Output:**

****