Objectives:

- Use Access Data's FTK Imager to mount a suspect image and locate E-mail Files.
- Use Mitec's Mail View to parse e-mail files
- Determine if the user's e-mail files contain evidence of illegal activity.

1. Open FTK Imager.
2. Mount the Suspect image: Vader_Home_Computer.001. (File > Image Mounting > Select the suspect image file>click Mount)
3. Open Mitec's Mail View Program (MailView.exe). ****If you are using Windows 7 or 8, make sure you right-click and select "Run As Administrator" rather than just double-clicking the program.****
    a. Select the button for *Mozilla Thunderbird message database*.
    b. Click the folder to browse to the Thunderbird email.
    c. Navigate to the following directory on your mounted suspect image*: E:\Documents and Settings\Owner\Application Data\Thunderbird\Profiles\cnllzbsb.default\Mail \pop.mail.yahoo.com*
    d. Select *Inbox. **Not Inbox.msf – Choose the one with the largest size, if you aren't sure.***
    e. In Mitec Mail Viewer, *click File > View* and repeat the previous process to also open *Trash* and *Sent*.
    f. You can sort messages by any header (From, Subject, To, Received, Size) by clicking on their header bar. You can click *Messages > Collect Email Addresses* to show all email addresses in the file. You can create a filter to search for terms but be sure to also select a location in the grey bar to the left of the search term box. (the searches may take a minute, be patient).

4. Answer the following questions:

5. Who owns this email box and what is the email address:_____

6. When was the first email sent and received by the email box owner.

   a. _____

7. Review the email and determine if there are any indications of criminal activity.

   a. If yes, what are the names and email addresses of the people involved in the crime?

   b. Explain the series of events around this crime, based on your email analysis.