LAB PRACTICE: INVESTIGATING E-MAIL MESSAGES

Create a Work\Chap12\Projects folder on your system for this Lab's tasks. The only data files you need for these tasks are from the ULearn.

TASK 1

For this task, start AccessData FTK and create a new case and name it as InChp12-pst case. You need to examine the Jim_shu's.pst file for any messages referring to money. For this task, use FTK's Indexed Search function to look for keywords such as "money," "cash," and so forth.

If you locate messages containing any references to money, export each one into an HTML file in AccessData's Export subfolder. Then open each message in a Web browser and examine its header information to determine its actual source and sender.

When you have finished this examination, write a one-page report of your findings. Keep this session of FTK open for the next task.

TASK 2

This task is a continuation of Task 1. You need to locate any messages with file attachments. Follow these steps:

1. If FTK isn't running, start it and open the case file from the InChp12-pst case.
2. If the Overview window isn't displayed, click the **Overview** tab.
3. Click the **From E**-mail button under the File Status column.
4. In the File List pane, click the **Full Path** column to sort all records by pathname.
5. Next, scroll through the File List pane and look at each message. When you have located messages with identical ID numbers, export each one to the AccessData Export subfolder.
6. Open Windows Explorer to examine the files (messages and attachments) you have exported. Write a one-page memo stating the contents of each message and the nature of each attachment. Print all attachments and include them with the memo, and then close Windows Explorer. Leave FTK running for the next task.

TASK 3

In this project, a continuation of the previous two projects, you locate and export all deleted messages that FTK locates in the Jim_shu's.pst file. Follow these steps:

1. If FTK isn't running, start it and open the case file from the InChp12-pst case.
2. If the Overview window isn't displayed, click the **Overview** tab.
3. Click the **Deleted Files** button under the File Status column.
4. In the File List pane, hold down **Ctrl** as you click each message to select them as a group. Then right-click the group of files, and export them to your work folder.
5. Open Windows Explorer to examine the files you have exported, and write a one-page memo describing what they contain. Close Windows Explorer, and leave FTK running for the next task.

TASK 4

The attorney assigned to this investigation has asked you to list all Internet addresses and e-mail addresses in the Jim_shu's.pst file. Follow these steps:

1. If FTK isn't running, start it and open the case file from the InChp12-pst case.
2. If the Overview window isn't displayed, click the **Overview** tab.
3. Click **Tools, Internet Keyword Search** from the menu. In the Internet Keyword Search Options dialog box, click **OK** to start the search.
4. In the search results, click the **Add List to Evidence** button.
5. Record the filename and path of the Web Scan yyyymmdd-hhmmss.htm file created from this search, and then click **OK** in the Evidence Added Successfully dialog box. Click **Close** in the Internet Address Search Results dialog box.
6. Exit FTK and open Windows Explorer. Navigate to the path where the Web Scan *yyyymmdd-hhmmss*.htm file was saved, such as C:\Work\Chap12\Projects\InChap12-pst\Attach.
7. Double-click the Web Scan ***yyyymmdd-hhmmss*.htm** file to open it in your Web browser.
8. Print the Web Scan *yyyymmdd-hhmmss*.htm file, exit your browser and Windows Explorer, and submit the findings.

TASK 5

The attorney for Superior Bicycles, Ileen Johnson, has asked you to examine Martha Dax's Evolution e-mail data for any messages referring to the words "special projects." To perform this task, you need Hex Workshop and the martha-evolution.tar file you used earlier in the chapter. Follow these steps:

1. Start Hex Workshop. Click **File, Open** from the menu, navigate to your work folder, and double-click **martha-evolution.tar**.

2. Click the **Find** toolbar button. In the Find dialog box, click the **Type** list arrow, and then click **Text String**. In the Value text box, type **special projects**, and then click **OK**.
3. In the main Hex Workshop window, scroll up until you find the first occurrence of **From:**. Click the letter **F**, and then drag down in the right pane, highlighting all text until you reach the next From: statement.
4. Right-click the text highlighted in the right pane and click **Copy**.
5. Start Notepad. Click **Edit, Paste** to copy the selected text into a new text document. Click **File, Save As** from the menu, save it as **Special-projects1.txt** in your work folder, and then click **Save**. Click **File, Print** from the menu to print this document. Close the file, and leave Notepad open.
6. Continue the search by clicking the **Find Again** toolbar button in Hex Workshop and repeat Steps 2 through 5 (without restarting Notepad).
7. Exit Hex Workshop and Notepad when you have finished your searches. Submit the recovered e-mail messages.