CPS 301 Issues in Criminal and Forensics Computing
Spring 2012

Lab 1 --- Understanding Computer Investigation

Preparation:

A. Check the free disk storage capacity of your computer
B. Check the storage capacity of your flash drive
C. Which is larger?
D. Create a directory at C:\CPS301\SOFTWARE
E. Create your own work directory on the desktop of the computer: **C:\CPS301\Lab1**
F. Copy software files from the DVD disk to your desktop with the directory of C:\CPS301\SOFTWARE
G. Install ProDiscover Basic

Activity 1 --- Using ProDiscover Basic to Acquire a Flash Drive

A. Connect the flash drive to your computer
B. Start ProDiscover Basic
   Click **Start->Programs->ProDiscover->ProDiscover Basic**
   (Click **Cancel** if the Launch Dialog box opens)
C. In the main window, click **Action**, **Capture Image** from the menu.
D. In the Capture Image dialog box, click the **Source**
   Drive drop-down list, and select the thumb drive.
E. Click the >> button next to the Destination text box.
   When the Save As dialog box opens, navigate to your work folder and enter a name for the image you're making, such as **Lab1-Activity1**.
   Click **Save** to save the file.
F. Next, in the Capture Image dialog box, type your name in the Technician Name text box and **Lab1-Activity1-01** in the Image Number text box. Click OK.
G. ProDiscover Basic then acquires an image of the USB thumb drive. When it's finished, it displays a notice to check the log file created during the acquisition. This log file contains additional information if errors were encountered during the data acquisition. ProDiscover also creates an MD5 hash output file. In Chapters 4 and 5, you learn how to use MD5 for forensic analysis and evidence validation.
H. When ProDiscover is finished, click **OK** in the completion message box. Click **File**, **Exit** from the menu to exit ProDiscover.
I. Check the image file of the flash drive (file name and size).

Activity 2 --- Analyzing Digital Evidence

Task description: Manager Steve Billings has been receiving complaints from customers about the job performance of one of his sales representatives, George Montgomery. George has worked at the firm as an account representative for several years. He's been absent from work for two days but hasn't called in sick or told anyone why he wouldn't be at work. Another employee, Martha, is also missing and hasn't informed anyone of the reason for her absence. Steve asks the IT Department to confiscate George's hard drive and all storage media in his work area.

Steve would like to know whether there's any information on George's computer and storage media that might offer a clue to George's whereabouts and job performance concerns. To help determine George and Martha's whereabouts, you must take a systematic approach, discussed in class, to examining and analyzing the data found on George's desk. Assuming that George's digital evidence has been acquired and store in the image file: **InChp02.eve**.

A. Copy **InChp02.eve** file from DVD disk to your work directory.
B. Start ProDiscover Basic, as you did in the previous activity.
C. To create a new case, click **File**, **New Project** from the menu.
D. In the New Project dialog box, type **Lab1-Activity2** in the Project Number text box and in the Project File Name text box, and type **Employee Job Performance Investigation** in the Project Description text box. Click **OK.**
E. In the tree view of the main window, click the + (plus symbol) next to the Add item, and then click **Image File.**
F. In the Open dialog box, navigate to the folder containing the image, click the **InChp02.eve** file, and click **Open**. Click **Yes** in the Auto Image Checksum dialog box, if necessary.
G. In the tree view, click to expand **Content View**, if necessary. Click to expand **Images** and the image filename path **C:\CPS301\Lab1\InChap02.eve.**
H. Next, click **All Files** under the image filename path. When the CAUTION dialog box opens, click **Yes**. The InChp02.eve file is then loaded in the main window.
I. In the upper-right pane (the work area), click the **letter1** file to view its content in the data area.
J. In the data area, you see the contents of the letter1 file. Continue to navigate through the work and data areas and inspect the contents of the recovered evidence. Note that many of these files are deleted files that haven't been overwritten. Leave ProDiscover Basic running for the next activity.

Activity 3 --- Search for Keywords of Interest

Task: search for any reference to the name George.

A. In the tree view, click **Search**.
B. In the Search dialog box, click the **Content Search** tab, if necessary. Click the **Select all matches** check box, the **ASCII** option button, and the **Search for the pattern(s)** option button, if they aren't already selected.
C. Next, in the text box under the Search for the pattern(s) option button, type **George**
D. Under Select the Disk(s)/Image(s) you want to search in, click **C:\CPS301\Lab1\InChap02.eve**.
E. In the search results window, double-click the **Income.xls** file, which switches the view to the work area.
(Steps F to G shows how to export an Excel file)
F. In the work area, right-click the **Income.xls** file and click **Copy File**.
G. In the Save As dialog box, navigate to the folder you've selected, and click **Save**.
H. Now that the Income.xls file has been copied to a Windows folder, start Excel to examine the file's content. Repeat this data examination and file export process for the remaining files in the search results window. Then close all open windows except ProDiscover Basic for the next activity.

Activity 4 --- Generate a Report for Your Discovery

A. Generate a report for printing:

1. In the tree view, click **Report**. The report is then displayed in the right pane of the main window.
2. To print the report, click **File**, **Print Report** from the menu.
3. In the Print dialog box, click **OK**.

Activity 5 --- Draw a Conclusion on Your Discovery

A. Find the storage capacity of the source disk (Your flash drive), and the size of the bit-stream image obtained by you, and record them in your report.
B. Write a paragraph to describe the discovered evidence, and draw a conclusion stating if the suspect is violating company policy.