Module 4 Live Data Acquisition Lab

Description: In this lab, we will work to acquire and analyze data.

Requirement: You will need access to the Cybrary lab environment to complete this lab.

Part 1

Step 1: Log into Cybrary

Step 2: Select Catalog at the top of the page

Step 3: In the search box on the left-side of the page, type **forensic**

Step 4: Locate the **Computer Forensics and Investigations** lab environment

Step 5: Click the Start Now button to launch the lab environment

Step 6: Click the "Understanding the Digital Forensics Profession and Investigations" lab.

Step 7: Click the Start button

Step 8: Power on all of the virtual machines

Step 9: Now we will work to acquire data

Note: In real-life, always be sure to use a write blocker, so you don't alter the data you are acquiring.

Step 10: Connect to PLABWIN810

Step 11: Double-click the ProDiscover Basic 64 shortcut icon on the desktop

Step 12: At the Launch Dialog box, click the Cancel button.

Step 13: Click **Action** at the top, then **Capture Image**

Step 14: A pop-up box will open

Step 15: Under the Source Drive area, select this option: **E:\[USB] 4.997 GB**

Step 16: Next, click the button with two arrows in the Destination area.

Step 17: Select the “Choose Local Path” option

Step 18: Navigate to C:\Work\Data files\Ch01 folder

Step 19: In the File name box, type: **InChp-prac**

Step 20: Click the Save button

Step 21: On the Capture Image pop-up box, type your name in the Technician Name box.

Step 22: Next, type this in the Image Number box: InChp-prac01

Step 23: Click the OK button

Step 24: You will see at the bottom-right of the screen that ProDiscover is acquiring the image of the target.

Note: This process may take 20-30 seconds to complete.

Step 25: Once complete, you may see a pop-up box that states the following. Just select OK.

“Image capture complete. Please check log file for any errors”

Step 26: Next, select File and then Exit to close ProDiscover

Part 2

Step 1: Double-click the ProDiscover Basic 64 icon on the desktop

Step 2: At the Launch Dialog box, click the Cancel button.

Step 3: At the top, select File and then New Project

Step 4: A New project pop-up box opens

Step 5: Under the Project Number and the Project File Name, type this: **InChp01**

Step 6: Click OK

Step 7: On the left-side of the screen, click the **+** sign next to the Add option to expand it.

Step 8: Next, click Image File

Step 9: Click the **InChp-prac.eve**

Step 10: Click the Open button

Step 11: On the left-side, under the **Content View** section, click the + sign next to the Images option to expand it.

Step 12: Next, click the file path under the Images option.

Step 13: Next, click the **+** sign next to the file path

Step 14: You will then click on **All Files**.

Step 15: You will see a pop-up box warning you that listing all files may take some time to complete.

Step 16: Click the Yes button

Step 17: You will then see the results in the top window.

Step 18: Click the tracking.log file to view the contents in the bottom window.

Step 19: Next, click on the Search option in the bottom-left of the screen.

Step 20: A pop-up box will open. Make sure the Content Search tab is selected.

Step 21: Mark the checkbox next to "**Select all matches**"

Step 22: Under the “Search for the pattern(s)” box, type: **plabwin810**

Step 23: Under the “Select the Disk(s)/Image(s) you want to search in” box, select the image path. C:\Work\Data files\Ch01\InChp-prac.eve

Step 24: Click the OK button

Note: It might take 5-10 seconds for the search to run.

Step 25: You will see the search results in the top window.

Step 26: Click on the **tracking** file in the top window

Step 27: You will see the string plabwin810 has been found in the bottom window.