Module 3: Recovering Graphics Files

Description: In this lab, we are going to use ProDiscover to search for evidence of JPEG files from a USB drive.

Requirement for lab: This lab is done in the Cybrary lab environment.

Part 1

Step 1: Login into the Cybrary website

Step 2: Click on Catalog

Step 3: Search for **Forensic**

Step 4: Select the Computer Forensics and Investigations labs and click the Start Now button

Step 5: Select the **Recovering Graphics Files** lab

Step 6: Click the Start button

Step 7: Power on all of the virtual machines

Note: It might take 20-30 seconds for the virtual machines to turn on

Step 8: Select the PLABWIN810 machine

Step 9: Now we will download the USB drive image

Step 10: Launch Internet Explorer from the Taskbar

Step 11: The Intranet page will launch

Step 12: Select Tools

Step 13: Select Data Forensics

Step 14: Click USB.zip

Step 15: Select Save As and a pop-up box will open

Step 16: Navigate to **C:\Work\Data files\Chp08**

Step 17: Click Save

Step 18: Click Open Folder

Step 19: Right-click the USB zipped file and select Extract All

Step 20: Keep the default file path and click Extract

Step 21: Close the folder windows and Internet Explorer

Part 2

Step 1: On the desktop, double-click the ProDiscover Basic 64 shortcut icon

Step 2: Click Cancel at the Launch Dialog pop-up box

Step 3: Click the New Project button at the top-left of the window (It looks like a blank piece of paper)

Step 4: A pop-up box will open

Step 5: In the Project Number box, type **C08InChp**

Step 6: In the Project File Name box, type **C08InChp**

Step 7: Select OK

Step 8: Select **Action** from the top menu, then **Add**, then **Image File**

Step 9: A pop-up box will open

Step 10: Navigate to **C:\Work\Data files\Ch08\USB\USB folder**

Step 11: Select this file: **jo-favorites-usb-2009-12-11.E01**

Step 12: Click Open

Step 13: Next, click Action at the top, then Search

Step 14: Select the Cluster Search tab

Step 15: Click the Case Sensitive checkbox

Step 16: In the "Search for the patter(s)" checkbox, type **FIF**

Step 17: In the "Select the Disk(s)/Image(s) you want to search in" box, select this option:

C:\Work\Data files\Ch08\USB\USB\jo-favorites-usb-2009-12-11.E01

Step 18: Click the OK button

Step 19: The search will begin. Please note it make take a minute or two to complete the search.

Step 20: Once the search completes, click the first result in the search box

Step 21: You will see the Hex in the bottom window

Step 22: Use the scroll bar on the right-side of the bottom window and scroll down until you see FIF highlighted in blue.

Step 23: On the left-side of the page, expand the Images option under the **Cluster View** by clicking the small plus sign

Step 24: Expand the C:\Work\Data files\Ch08 by clicking the small plus sign

Step 25: Click C:

Step 26: In the text box on the right-side, type: **AC4**

Step 27: Click Go

Step 28: In the top window, you will AC4 highlighted as a red-colored square.

Step 29: Right-click on the red square and select Find File

Step 30: A pop-up box will open and ac4 (2756) should be selected.

Step 31: We see that the indicated file path shows the file name as DSC00018

Step 32: Click the Show File button

Step 33: You will notice the view changes to the Content View folder

Step 34: Click the Close button

Step 35: You will see several files starting as "DSC…" in the top window pane.

Step 36: Right-click on the **DSC00018 file** and click Copy File

Step 37: A Save As pop-up box opens

Step 38: Change the filename to **Recover1** and then click the Save button

Step 39: Next, close the ProDiscover tool by clicking File, then Exit from the top menu

Step 40: You will be prompted to save. Select Yes at the prompt.

Step 41: Click the Save button

Part 3

Step 1: On PLABWIN810, open the File Explorer from the Taskbar

Step 2: Navigate to C:\Work\Data files\Ch08

Step 3: Click the New Folder icon at the top-left

Step 4: Name the new folder: **Chap08nProjects**

Step 5: Right-click on the **c08frag file** and select Open

Step 6: The WinRAR self-extracting archive pop-up box opens

Step 7: click the Browse button

Step 8: Click This PC

Step 9: Click Local Disk (C:)

Step 10: Click the Work folder

Step 11: Click Ch08

Step 12: Click the Chap08nProjects folder

Step 13: Select OK

Step 14: Click the Extract button

Step 15: Close the file explorer window

Step 16: Double-click on the ProDiscover Basic 64 shortcut icon on the desktop

Step 17: Click the Cancel button at the Launch Dialog pop-up box

Step 18: Click the New Project icon at the top-left of the window (it looks like a blank piece of paper)

Step 19: Under the Project Number and Project File Name areas, enter: **C08frag.dd**

Step 20: Select OK

Step 21: On the left-side of the screen, expand Add by selecting the plus sign

Step 22: Click Image File

Step 23: A pop-up box will open

Step 24: Click on Ch08 at the top

Step 25: Double-click on the Chap08nProjects folder

Step 26: Select the c08frag.dd file

Step 27: Click the Open button

Step 28: Click the Search button at the top (magnifying glass and a piece of paper)

Step 29: Make sure you are under the **Content Search** tab

Step 30: In the "Search for pattern(s)" box, type **JFIF**

Step 31: Under the "Select the Disk(s)/Image(s) you want to search in" box, select this:

C:\Work\Data files\Ch08\Chap08nProjects\c08frag.dd

Step 32: Click OK

Step 33: Next, click on the shellback2 file and review the file contents to see if you notice the JFIF label.

Question 1: Do you see JFIF in the file contents? _____

Step 34: Click the checkbox to the left of the file

Step 35: An "Add Comment" pop-up box opens

Step 36: In the comments section, type: Recovered hidden .jpg file

Step 37: Select the Apply to all items checkbox and click OK

Step 38: Mark the checkbox to the left of all remaining files that do not show jpg under the File Extension column

Step 39: Next, click Report on the left-side

Step 40: You will see a report generated

Question 2: Do you see anything on the report under the "Total Evidence Items of Interest" area?

_____

Step 41: Select File at the top, then Exit

Step 42: If prompted, select No to saving the ProDiscover case you had created