CSCE 4555/5555 – Homework 4

Due: 11:59 PM on Friday, October 21, 2022

Review the supporting material from Chapter 8 in the textbook to complete the assigned exercises and submit the applicable files to the **Homework 4** dropbox on Canvas by the due date and time.

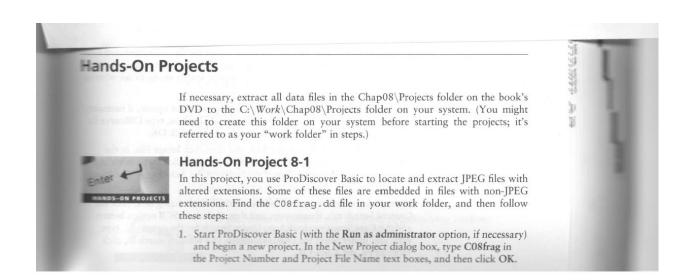
The software and related data files are being provided in class or can be found in the Student Data Files DVD accompanying the textbook or on Canvas.

1. Consider a file that contains the string: "GOMEANGREEN", without the quotes. If we were to encode it using ASCII values, this 11 character string would require 88 (or 8 * 11) bits as follows:

Because this string contains only 7 unique letters, it is possible to use only 3 bits to encode the different characters (i.e., assign each character a unique 3 bit sequence) for a total of 33 (or 3 * 11) bits. More bits can be saved if we use fewer than 3 bits to encode the more frequently occurring characters like \mathbb{E} , \mathbb{G} , and \mathbb{N} . This is the basic idea behind Huffman coding. Now use Huffman coding to (1) construct a tree, (2) assign codes to each character, and (3) encode the string to generate a Huffman code. Note that there are several possible solutions due to some arbitrary possibilities in choosing trees in the algorithm, but your resulting Huffman code should be less than 33 bits.

Please note that we will be completing a modified version of the Hands-On Projects 8-1 and 8-2 found in the course textbook (*Guide to Computer Forensics and Investigations, Bill Nelson, Amelia Phillips, and Christopher Steuart, 6th Ed.).* Instead of using Autopsy for Windows, we will use ProDiscover Basic installed on our Windows machines. I am including the actual assignment text using ProDiscover Basic as part of this assignment that comes from the following pages of the 5th edition of the textbook:

- 2. Hands-On Project 8-1 (pp. 353 354)
 - Turn in the ProDiscover Basic report C08Prj01 to Canvas. Be sure that all relevant files (i.e., evidence items of interest) are included.
- 3. Hands-On Project 8-2 (pp. 354 355)
 - Turn in the ProDiscover Basic report C08Prj02 to Canvas. Be sure that all relevant files (i.e., evidence items of interest) are included.



- In the tree view, click to expand Add, and then click Image File. In the Open dialog box, navigate to your work folder and click CO8frag.dd. Click Open, and then click Yes, if necessary, in the Auto Image Checksum message box.
- Click the Search toolbar button. In the Search dialog box, click the Content Search tab, if necessary. Under Search for the pattern(s), type JFIF, and under Select the Disk(s)/Image(s) you want to search in, click C:\ Work\ C08frag.dd. Click OK.
- 4. Click each file in the work area's search results that doesn't have a .jpg extension, and in the data area, scroll through and examine the entire content of each file to find any occurrences of a JFIF label. Click the check box next to each file with a JFIF label. When the Add Comment dialog box opens, type Recovered hidden .jpg file, click the Apply to all items check box, and then click OK.
- 5. In the tree view, click Report, and then click File, Print Report from the menu. Click OK. You can also save your report by clicking the Export toolbar button, and in the Export dialog box's File Name text box, type C08Prj01. Click Browse, navigate to your work folder, click Save, and then click OK.
- 6. Exit ProDiscover Basic, saving your project when prompted.

Hands-On Project 8-2

In this project, you continue the search for files Bob Aspen downloaded. In the in-chapter activity, you recovered three files containing zzzz for the first 4 bytes of altered JPEG files. These altered files had different extensions to hide the fact that they're graphics files.

Find the COBCATVE. dd file in your work folder. This image file is a new acquisition of another USB drive the EMTS manager retrieved. He wants to know whether any similar files on this drive match the files you recovered from the first USB drive. Because you know that the files you recovered earlier have zzzz for the first 4 bytes, you can use it as your search string to see whether similar files exist on this USB drive.

- 1. Start ProDiscover Basic (with the Run as administrator option, if necessary) and begin a new project. In the New Project dialog box, type C08carve for the project number and project filename, and then click OK.
- In the tree view, click to expand Add, and then click Image File. In the Open dialog box, navigate to your work folder and click CO8carve.dd. Click Open, and then click Yes, if necessary, in the Auto Image Checksum message box.
- 3. Next, click the Search toolbar button. In the Search dialog box, click the Content Search tab, if necessary, and then click the ASCII option button and the Case Sensitive check box. Under Search for the pattern(s), type zzzz, and under Select the Disk(s)/Image(s) you want to search in, click C08carve.dd. Click OK.

- 4. Click each file in the work area's search results to display it in the data area. If the file contains zzzz at the beginning of the sector, click the Select check box next to it. In the Add Comment dialog box, type Similar file located on first USB drive, click the Apply to all items check box, and then click OK.
- 5. In the work area, click the Add to Report button.
- 6. Double-click the gametour5.txt file. In the work area, click the File Name column heading to sort all files in this pane. Scroll through the list of files and click the Select check box for gametour1.txt, gametour2.txt, gametour3.txt, gametour4.txt, and gametour6.txt files. When the Add Comment dialog box opens, type Additional similar files on USB drive, and then click OK. Repeat this step for each gametour file you find in this list.
- 7. Right-click the gametourl.txt file and click Copy All Selected Files. In the Choose Destination dialog box, click Browse, navigate to and double-click your work folder, and then click OK to copy the files. When prompted, click OK in the message box about files being copied successfully.
- 8. To complete your examination, click Report in the tree view, and then click File, Print Report from the menu. You can also save your report by clicking the Export toolbar button, and in the Export dialog box's File Name text box, type C08Prj02. Click Browse, navigate to and click your work folder, click Save, and then click OK.
- 9. Save the project and exit ProDiscover Basic.

R