CSCE 4555/5555 – Homework 3

Due: 11:59 PM on Monday, October 3, 2022

Review the supporting material from Chapter 5 in the textbook to complete the assigned exercises and submit the applicable files to the **Homework 3** dropbox on Canvas by the due date and time.

The following problems are assigned from the course textbook (*Guide to Computer Forensics and Investigations, Bill Nelson, Amelia Phillips, and Christopher Steuart, 6th Ed.*)

1. Hands-On Project 5-2 (pp. 260 – 265)

   - We are going to use HxD instead of WinHex for this activity, so please follow the instructions 1 through 3 on pages 260 – 261 in HOP 5-2 from the textbook. Then, instead of the instructions starting on page 262, please continue as directed below.
   - Start HxD with the **Run as administrator** option. If you see the warning message about allowing this app to make changes to your device, select **Yes**.
   - Click **Tools**, **Open disk…** from the menu. In the Open disk dialog box, click the **C:** drive (or the drive where you saved `C5Prj02.txt`).
   - Click **Search**, **Find** from the menu. In the **Search for:** text box, type in one of the words from the `C5Prj02.txt` document (such as "countryman") and click **OK**. You should notice that the MFT record identifier FILE0 is a little bit above where your text is found for your `C5Prj02.txt` file. If not, you may have to search again.
   - Once found, drag from the beginning of the record, on the letter **F** in FILE0, and then down to the right for 5 rows (or 50 hexadecimal bytes). When you get to the 50th byte, release the mouse button, which should put you in the middle of the 0x10 attribute.
   - Move the cursor position to the next byte (down one line and to the left), and record the date and time of the Data Inspector's FILETIME values by taking a snapshot of the file you created using Notepad open in HxD with the cursor positioned, showing the metadata date and time in the Data inspector.
   - Refer to Figure 5-14 and the associated text for the attribute 0x10 Standard Information's various date and time values. Then, reposition the mouse cursor on the remaining offsets listed in that figure and record their values, capturing a screenshot for the various dates and times in the Data inspector in HxD.
   - Turn in the four snapshots showing both the file data as well as the metadata from the Data inspector.

2. Hands-On Project 5-3 (p. 265)

   - Instead of WinHex, start HxD and open each file type in HxD and record (i.e., highlight) the hexadecimal codes (about 4-6 bytes) and take a screenshot, saving the result to a document.

3. Hands-On Project 5-4 (pp. 265 – 266)

   - Turn in the (1) OSForensics Case Report that was generated using OSForensics and (2) the text document called Denise-Robinson-Win-Passwords-Hashes that contains the hashes for the Windows Login Passwords.