CSCE 5555.001 – Homework 1

Due: 11:59 PM on Monday, September 12, 2022

Review the supporting material from Chapter 1 in the textbook to complete the assigned exercises and submit the applicable files to the **Homework 1** dropbox on Canvas by the due date and time.

1. Read the following article about data found on hard drives:

   https://arstechnica.com/tech-policy/2016/05/feds-can-keep-your-hard-drives-indefinitely-and-search-them-too/

   Given that the Fourth Amendment is the basis for privacy rights in that it prohibits government agents from searching private property without a warrant and probable cause, do you feel that this is a violation of our search and seizure rights? Justify your answer. *Note that there are no right or wrong answers here, but you should clearly justify your argument.*

Please note that we will be completing a modified version of the Hands-On Projects 1-2 and 1-3 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 Release 8.2.0.2 installed on our Windows VMs. 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 1-2 (pp. 56 – 58)

   For HOP 1-2, make sure to include a list of clusters in BOTH allocated and unallocated space.

3. Hands-On Project 1-3 (pp. 58 – 59)

   Again, be sure to include clusters in both allocated and unallocated space.

You are welcome to use the ProDiscover Basic Release 8.2.0.2 software uploaded to Canvas under the *Software* module on your own computer, but please note that support is not provided. If you are having any technical issues installing this software or getting it to work on your computer, please use one of the VMs available with this software already installed.

Hands-On Project 1-2

In this project, you work for a large corporation's IT security company. Your duties include conducting internal computing investigations and forensics examinations on company computing systems. A paralegal from the Law Department, Ms. Jones, asks you to examine a USB drive belonging to an employee who left the company and now works for a competitor. The Law Department is concerned that the former employee might possess sensitive company data. Ms. Jones wants to know whether the USB drive contains anything significant.

In addition, she informs you that the former employee might have had access to confidential documents because a co-worker saw him accessing his manager's computer on his last day of work. These confidential documents consist of 24 files with the text "book." She wants you to locate any occurrences of these files on the USB drive's bit-stream image.

To process this case, make sure you have extracted the `C1Prj02.eve` file to your work folder, and then follow these steps:

1. Start ProDiscover Basic. In the New Project tab, enter a project number, the project name **C1Prj02**, and a project description, and then click **Open**. It's a good idea to get in the habit of saving the project immediately, so click **File, Save Project** from the menu, and save the file in your work folder (*Work*\Chap01\Projects).
2. Click **Action** from the menu, point to **Add**, and click **Image File**. Navigate to and click **`C1Prj02.eve`** in your work folder, and then click **Open**. If the Auto Image Checksum message box opens, click **Yes**.
3. In the tree view, click to expand **Content View**, if necessary. Click to expand **Images**, and then click the pathname containing the image file. In the work area, examine the files that are listed.
4. To search for the keyword "book," click the **Search** toolbar button to open the Search dialog box.
5. If necessary, click the **Content Search** tab, and then click the **ASCII** option button and the **Search for the pattern(s)** option button. Type **book** in the list box for search keywords. Under Select the Disk(s)/Image(s) you want to search in, click the drive you're searching (see Figure 1-24), and then click **OK**.

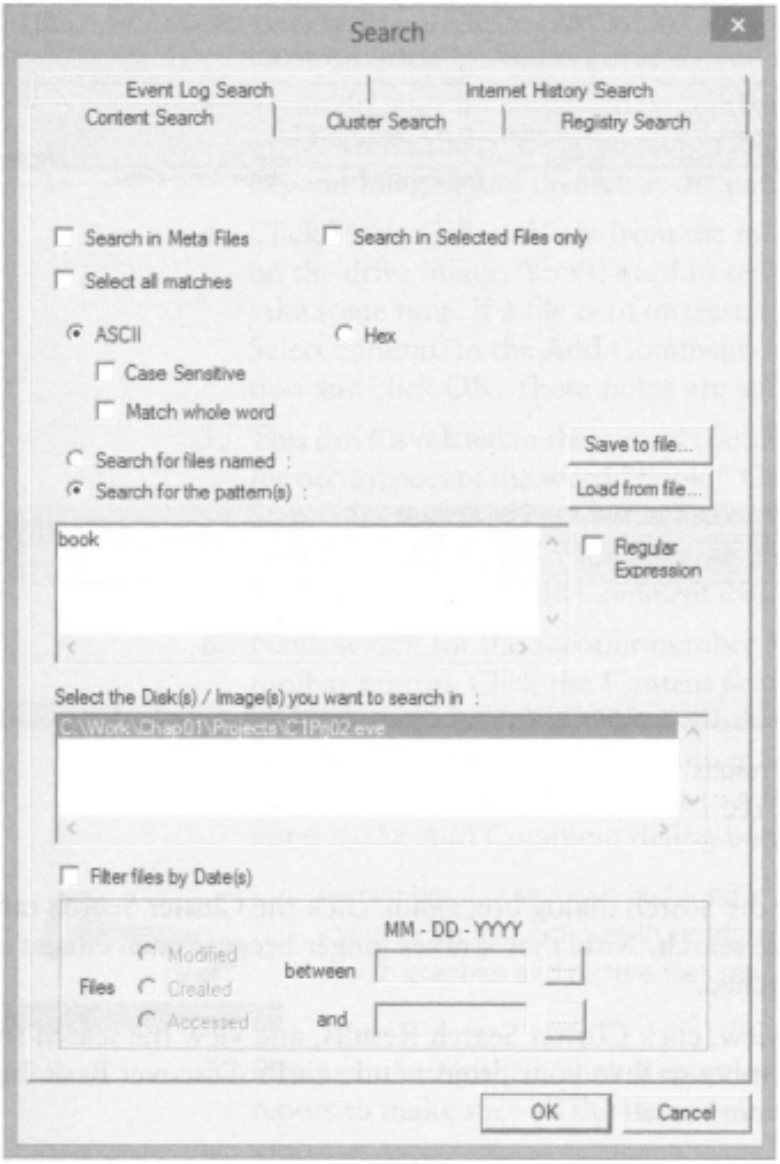


Figure 1-24 Entering search settings
Courtesy of Technology Pathways, LLC

6. In the tree view, click to expand **Search Results**, if necessary, and then click **Content Search Results** to specify the type of search. Figure 1-25 shows the search results pane.

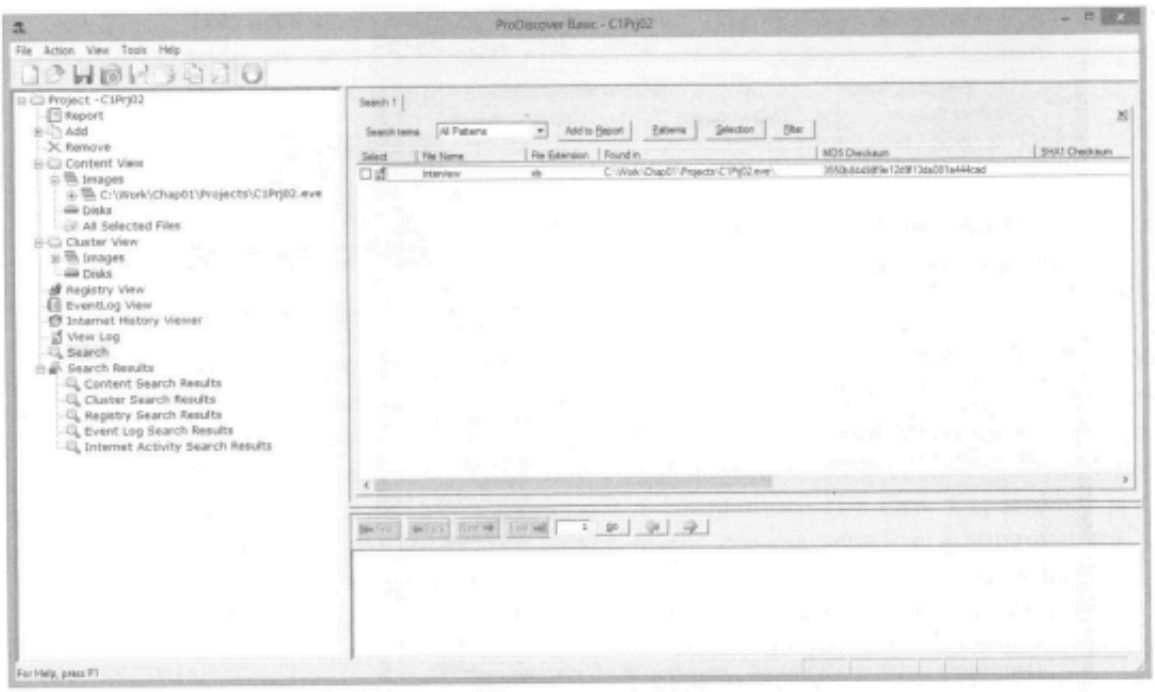


Figure 1-25 Viewing the search results
Courtesy of Technology Pathways, LLC

7. Next, open the Search dialog box again, click the **Cluster Search** tab, and run the same search. Note that it takes longer because each cluster on the drive is searched.
8. In the tree view, click **Cluster Search Results**, and view the search results pane. Remember to save your project and exit ProDiscover Basic before starting the next case.

When you're finished, write a memo to Ms. Jones with the following information: the filenames in which you found a hit for the keyword and, if the hit occurred in unallocated space, the cluster number.

Hands-On Project 1-3

Ms. Jones notifies you that the former employee has used an additional drive. She asks you to examine this new drive to determine whether it contains an account number the employee might have had access to. The account number, 461562, belongs to the senior vice president and is used to access the company's banking service over the Internet.

1. Start ProDiscover Basic. In the New Project tab, enter a project number, the project name **C1Prj03**, and a brief description, and then click **Open**. Save the project in your work folder by clicking **File, Save Project** from the menu.
2. To add the evidence, click **Action** from the menu, point to **Add**, and click **Image File**. Navigate to your work folder, click the **`C1Prj03.dd`** file, and then click **Open**. Click **Yes** in the Auto Image Checksum message box, if

necessary. Notice that the image file is a .dd file, not an .eve file. Like most forensics tools, ProDiscover can read standard UNIX .dd image files.

3. To aid in your investigation, you might want to view graphics files on the drive. To do this, click to expand **Content View** in the tree view, click to expand **Images**, and then click the pathname containing the image file.
4. Click **View, Gallery View** from the menu. Scroll through the graphics files on the drive image. You'll need to search through all folders, which can take some time. If a file is of interest, click the check box next to it in the Select column. In the Add Comment dialog box that opens, enter a description and click **OK**. These notes are added to the ProDiscover report.
5. This drive is related to the case in Hands-On Project 1-2, so you're still looking for occurrences of the word "book." Open the Search dialog box, and repeat Steps 5 through 8 of Hands-On Project 1-2 for this drive image. When you view the search results, click to select any files of interest (as described in Step 4), which opens the Add Comment dialog box where you can enter notes.
6. Next, search for the account number Ms. Jones gave you. Click the **Search** toolbar button. Click the **Content Search** tab, if necessary, and type **461562** as the search keyword. Click to select the drive you're searching, and then click **OK**. Click the **Cluster Search** tab, and repeat the search for the account number. Remember to select any files of interest and enter notes in the Add Comment dialog box.

Remember that text can be found in graphics files as well as in documents. If your search results produces no findings, you might have to search graphics and picture files separately for evidence.

7. When you're finished, click **Report** in the tree view. Scroll through the report to make sure all the items you found are listed.
8. Next, click the **Export** toolbar button. In the Export dialog box, click the **RTF Format** option button, type **Ch1Prj03Report** in the File Name text box, and then click **OK**. (If you want to store the report in a different folder, click Browse and navigate to the new location.)
9. Write a short memo to summarize what you found. Save the project and exit ProDiscover Basic.

CSCE 4555/5555 – Homework 2

Due: 11:59 PM on Wednesday, September 21, 2022

Review the supporting material from Chapter 4 in the textbook to complete the assigned exercises and submit the applicable files to the **Homework 2** 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 4-4 (p. 191)

   Since the FTK Imager software does not recognize the USB drive attached to the Virtual Servers, please modify the instructions to the homework problems as follows:

   - Create a **C4Prj04** folder on the **Desktop** and when saving the `hash1.txt` file, save it to this folder.
   - Then when performing the **Add Evidence Item** in FTK Imager, select the **Contents of a Folder** option to select your **C4Prj04** folder instead of your USB.

   When you have completed this exercise and saved your `original hash.csv` and `changed hash.csv` files to an accessible location, please be sure to remove all work files from the forensic VM.

2. Hands-On Project 4-5 (pp. 191 – 192)

   - Create a **C4Prj05** folder on the **Desktop** and when saving the `testhash.txt` file, save it to this folder.
   - Then when performing the **Add Evidence Item** in FTK Imager, select the **Contents of a Folder** option to select your **C4Prj05** folder instead of your USB.

   When you have completed this exercise and saved your `original hash value.csv` and `changed hash value.csv` files to an accessible location, please be sure to remove all work files from the forensic VM.

You should submit four Excel or .csv files (i.e., two for Hands-On Project 4-4 and two more for Hands-On Project 4-5) or screenshots of these files.

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.

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:

   ```
   01000111 01001111 01001101 01000101 01000001 01001110
   01000111 01010010 01000101 01000101 01001110
   ```

   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 E, G, and 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.

Hands-On Projects

If necessary, extract all data files in the Chap08\Projects folder on the book's DVD to the C:*Work*\Chap08\Projects folder on your system. (You might need to create this folder on your system before starting the projects; it's referred to as your "work folder" in steps.)

Hands-On Project 8-1

In this project, you use ProDiscover Basic to locate and extract JPEG files with altered extensions. Some of these files are embedded in files with non-JPEG extensions. Find the `C08frag.dd` file in your work folder, and then follow these steps:

1. Start ProDiscover Basic (with the **Run as administrator** option, if necessary) and begin a new project. In the New Project dialog box, type **C08frag** in the Project Number and Project File Name text boxes, and then click **OK**.

2. 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 **C08frag.dd**. Click **Open**, and then click **Yes**, if necessary, in the Auto Image Checksum message box.
3. 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 `C08carve.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**.
2. 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 **C08carve.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 **`gametour1.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.

CSCE 4555/5555 – Homework 5

Due: 11:59 PM on Friday, November 4, 2022

Review the supporting material from Chapter 9 in the textbook to complete the assigned exercises and submit the applicable files to the **Homework 5** dropbox on Canvas by the due date and time.

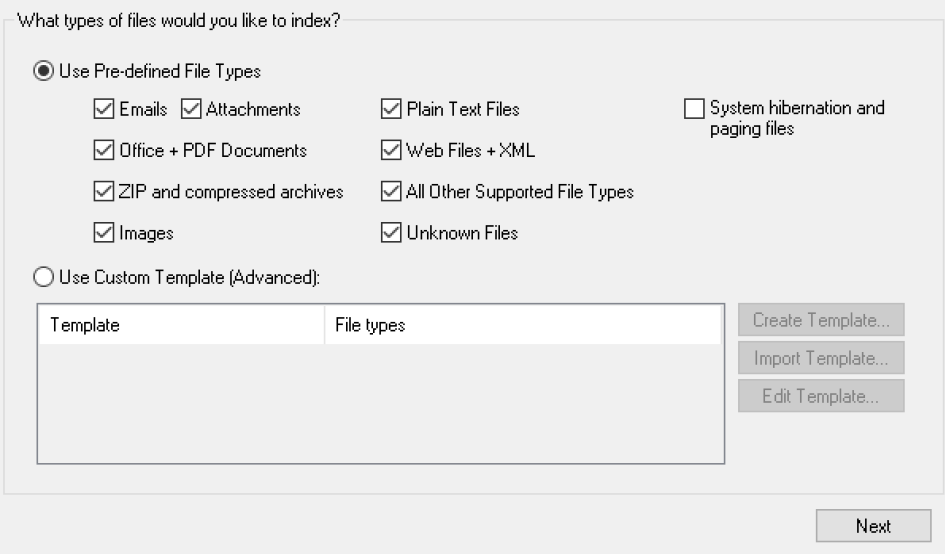
1. Read the following article about

   https://www.washingtonpost.com/news/morning-mix/wp/2018/10/02/new-zealands-digital-strip-searches-give-border-agents-your-device-passwords-or-risk-a-5000-fine/?noredirect=on&utm_term=.dc8f436cfe5c

   Given our discussion of the Fourth Amendment as the basis for privacy rights, plus the First Amendment's guarantee of freedom of speech (among other things), do you feel this would be a violation of our rights here in the United States? Justify your answer. *Note that there are no right or wrong answers here, but you should clearly justify your argument.*

Please note that we will be completing the Hands-On Projects 9-2 through 9-4 found in the fifth edition of the course textbook (*Guide to Computer Forensics and Investigations, Bill Nelson, Amelia Phillips, and Christopher Steuart, 5th Ed.*). I am including the actual assignment text from the following pages of the 5th edition of the textbook:

2. Hands-On Project 9-2 (p. 384)
   - Turn in a screenshot of your entire WinHex window that shows the MD5 hash of the gcfi-ntfs.dd image. This value should agree with the MD5 hash for this image given in the GCFI-NTFS has values document.
3. Hands-On Project 9-3 (p. 385)
   - Turn in the OSForensics report **HOP09-3Case Report** to Canvas along with a short memo (i.e., a few sentences) to Ileen Johnson, the lead investigator for the case, summarizing your findings and what they indicate.
4. Hands-On Project 9-4 (p. 386)
   - Turn in the OSForensics report **HOP09-4Case Report** to Canvas.
   - Due to an issue in working with VMs, the file 10K limit for the demo version of OSForensics may be reached before indexing the entire image. Therefore, to make sure that you have files in the Files tab in OSForensics for HOP 9-4, please select all the Pre-Defined File Types (as seen in the screenshot) except for the system and hibernation files. Then, you can parse through the related files for evidence.



Hands-On Project 9-2

Before conducting a forensics analysis, you should validate image files you've acquired. In this project, you validate the files analyzed in Hands-On Projects 9-3 and 9-4 to verify that they aren't corrupt. Chris Murphy, a Superior Bicycles employee suspected of industrial espionage, had a Windows drive formatted in NTFS that was seized as part of the investigation. For this project, you use the `gcfi-ntfs.dd` image file that was used earlier in this chapter.

1. Start Microsoft Word, and open the **`GCFI-NTFS hash values.doc`** file from your work folder. Print the file so that you can compare it with your results later in this project, and then exit Word.
2. Start WinHex, if necessary, and open **`gcfi-ntfs.dd`** from your work folder.
3. Click **Tools**, **Compute Hash** from the menu. In the Compute hash dialog box, click the list arrow, click **MD5 (128 bit)**, if necessary, and then click **OK**.
4. When the checksum process is finished, check the MD5 hash value in WinHex, and compare it with the value in the document you printed in Step 1.
5. After you have verified all the files, make a note in your log listing the file you examined and its hash value, and then exit WinHex.

Hands-On Project 9-3

In this project, you search the GCFI-NTFS drive image that belonged to Chris Murphy. You should have completed Hands-On Project 9-2 before beginning this one. Chris is suspected by his manager of leaking company secrets and possibly engaging in industrial espionage. Conduct a search to ascertain whether any evidence exists to support this claim.

1. Start OSForensics with the **Run as administrator** option, and start a new case. Enter **Superior Bicycles** for the case name. Enter your name as the investigator, your class name as organization, and your telephone number in the Contact Details text boxes in the New Case dialog box, and click **OK**.
2. To mount the disk image, scroll down the navigation bar on the left, and click **Mount Drive Image**. In the Mounted virtual disks window, click the **Mount new** button. In the OSFMount - Mount drive dialog box that opens, click the **...** button next to the Image file text box, navigate to your work folder, click **`gcfi-ntfs.dd`**, click **Open**, and then click **OK**.
3. Click the **Create Index** button in the left pane to start the Create Index Wizard. In the Step 1 of 5 window, click the **Use Pre-defined File Types** option button, if necessary. Click the **Emails, Attachments, Office + PDF Documents, Web Files + XML**, and **Zip Files** check boxes, and then click **Next**. In the Step 2 of 5 window, click the **Add** button. In the Add Start Location dialog box, click the **Whole Drive** option button if necessary, click the list arrow, click the mounted image drive letter, and then click **OK**. Click **Next**. In the Step 3 of 5 window, click **Start Indexing**.
4. When the indexing has finished, click **OK** in the message box informing you that errors reading some files might have occurred in the indexing process, if necessary. Click **Search Index** in the left pane. Type **chris** in the Enter Search Words text box, and then click **Search**.
5. Click the **Emails** tab, if necessary, and then double-click each e-mail message from baspen99@aol.com to view its contents. Click the **Add E-mail to Case** icon on the toolbar. In the Please Enter Case Export Details window, type **Bob Aspen message** in the Title text box, and then click **Add**. Repeat until all relevant e-mails have been added. If you get an error message at any time, click **Yes**. When you're finished, close the E-mail Viewer window.
6. Click **Start** in the left pane, and then click **Generate Report** in the right pane. In the Export Report dialog box, click the **Copy files to report location** button, click **Browse**, navigate to and click your work folder, and then click **OK**. OSForensics opens the report in your default Web browser.
7. After reviewing the report, exit your Web browser, and write a short memo to Ileen Johnson, the lead investigator in this case, summarizing your findings and what they indicate.
8. In File Explorer, navigate to your work folder where you saved the report, and rename the case folder **HOP09-3Case Report**. Keep OSForensics running for the next project.

Hands-On Project 9-4

In this project, you determine whether Chris transmitted any e-mails with information about the new kayak. Make sure you have finished Hands-On Project 9-3 before starting this one.

1. If necessary, start OSForensics with the **Run as administrator** option, and open the Superior Bicycles case. If necessary, mount the **`gcfi-ntfs.dd`** image file.
2. As mentioned, Chris is suspected of leaking information about the new kayak prototypes. You need to determine what he or someone else might have sent by e-mail. Click **Search Index** in the left pane. In the Enter Search Words text box, type **kayak**, and then click **Search**.
3. Click the **Emails** tab, if necessary, and then double-click the first e-mail message in the results. Click the **Add E-mail to Case** icon on the toolbar. In the Please Enter Case Export Details window, type **Kayak Search** in the Title text box, and then click **Add**. Repeat until all relevant e-mails have been added. If you get an error message at any time, click **Yes**. When you're finished, close the E-mail Viewer window.
4. Next, click the **Files** tab. Right-click the file in the search results and click **Add to Case**, and then click **List of Selected Items**. In the Please Enter New Case Item Details window, type **Kayak Document** in the Title text box, and then click **OK**.
5. Click **Start** in the left pane, and then click **Generate Report**. In the Export Report dialog box, click the **Copy files to report location** button, and then click **Browse**, navigate to and click your work folder, and click **OK**.
6. Exit OSForensics. Print the report that opens in your Web browser, and turn it in to your instructor.
7. In File Explorer, navigate to your work folder where you saved the report, and rename the case folder **HOP09-4Case Report**. Close any open windows.

CSCE 4555/5555 – Homework 6

Due: 11:59 PM on Wednesday, November 30, 2022

Review the supporting material from Chapter 13 in the textbook to complete the assigned exercises and submit the applicable files to the **Homework 6** 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 13-1 (pp. 552 – 554)
   - Turn in the `Dropbox.zip` file and the memo to the attorney of what you found in the `Dropbox.zip` file.
2. Hands-On Project 13-2 (pp. 554 – 556)
   - Turn in the `Google Drive IMG_3646 date stamps.txt` file with the retrieved (and converted) date stamps of the `IMG_3646.png` file.
3. Hands-On Project 13-3 (p. 556)
   - Turn in all the extracted `.oxps` files after you have converted them into a readable XPS document. You will need an XPS Viewer (should already be included and available in Windows) to view these files. You do not have to write the memo indicated in the project.
4. Hands-On Project 13-4 (p. 556)
   - Turn in a file that gives the Windows date and time at offset 0x80 and the number of times Google Drive has been accessed since it was installed at offset 0xD4. You should get a screen shot of these in WinHex. You do not have to write the memo indicated in the project.