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.

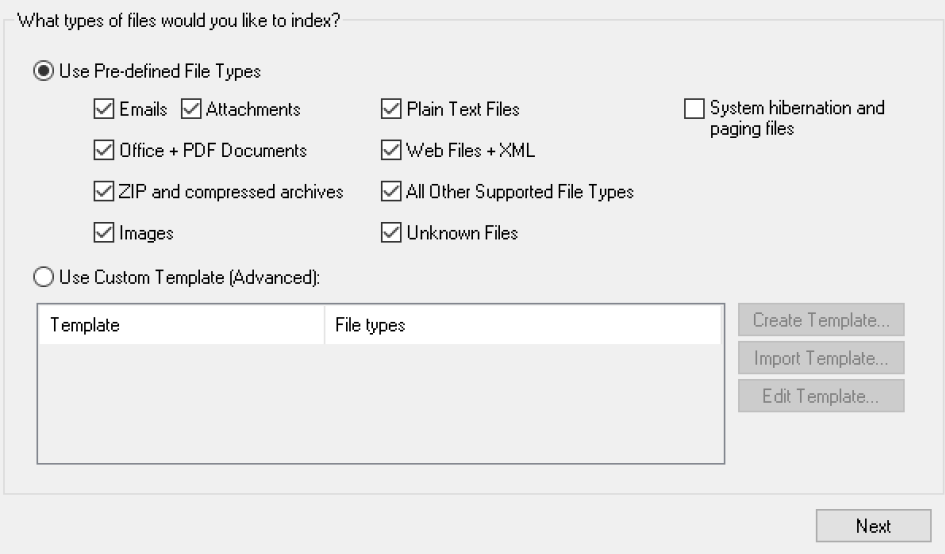
1. Read the following article about

   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.