**COMN-271-01: Computer Forensics**

**Chapter 9 Forensics Lab-Part 3**

20 points

Name: Christian Hill

Date: 12/4/16

**Part 1 Instructions:** Work through the Hands-On Projects detailed below and save files associated with each hands-on project as specified below. WinHex and OSForensics software will be used in these projects.

\*\*\* The OS Forensics software is available to download and install from Blackboard. Click on the **OS Forensics 3-3-64 bit** button in Blackboard to access.

Please note modifications in each Hands-On Project as you go through these labs.

Instructions for Hands-On Project 9-1 (pp. 383-384)

1. Create a folder called **Project 9-1** to a location of your choice.
2. Complete Steps 1-7 as specified in the textbook. Make sure to save files to the **Project 9-1** folder created in step 1 above.
3. At the end of Step 8, the textbook states to “**Repeat this step seven times to verify that you can recover the data**”. If you restart WinHex as specified in Step 7, the correspondence1.txt file may already be displayed in WinHex. If this is the case, you will only need to repeat the step six times, not seven.
4. You do not have to do Step 10.
5. After completing project, you should have three files saved to the Project 9-1 folder: **correspondence.txt**, **correspondence1.txt**, and **correspondence2.txt**. Copy the **Project 9-1** folder to the **Work\Chap09** folder that you created under your user name in the class\_shares drive.

Instructions for Hands-On Project 9-3 (pp. 385-386)

1. Create a folder called **Project 9-3** to a location of your choice.
2. For Step 1, click the **Custom Location** option as the Case Folder and browse to the location of the **Project 9-3** folder.
3. For Step 2, record the drive letter of the mounted drive: F:\
4. For Step 3, the **Zip Files** check box is called **ZIP and compressed archives**. After clicking **Start Indexing** option, if a **Free version page limit** box appears stating that **Pre-scan found more than 25,0000 files….etc.** click the OK button to continue scanning. If you still receive an error message, click OK and repeat steps to start indexing again.
5. At the end of Step 4, after clicking **Search**, provide answers to the following questions:
6. How many **Emails** were found? 24
7. How many **Files** were found? 14
8. Complete Steps 5 and 6 as specified in the textbook.
9. You do not have to do Step 7.
10. For Step 8, the name of the case folder that you are renaming is **Case Report** saved in the **Project 9-3** folder.
11. Keep OS Forensics software open for next project.

Instructions for Hands-On Project 9-4 (p. 386)

**NOTE**: Hands-On Project 9-3 should be completed successfully before starting this project.

1. OSForensics should be open from previous project so Step 1 is not needed.
2. At the end of Step 2, after clicking **Search**, answer the following question:
   1. How many **Emails** were found? 2 Emails were found
3. Complete Step 3 as specified in the textbook.
4. Do NOT do Step 4 because there are no files found in the search results.
5. Complete Steps 5-7 as specified in the textbook. You do not have to print the report as specified in Step 6.
6. After completing Hands-On Projects 9-3 and 9-4, copy the **Project 9-3** folder along with its contents to the **Work\Chap09** folder that you created under your user name in the class\_shares drive.