91.460-530.203 Cyber Crime Investigation

Assignment 3
(10 points)

Instructions:

1. Note: Blue text points to a web link. Ctrl + Click to follow link.
2. This is an individual assignment.
3. Answers to all questions including hands-on project with screen shots must be put into **ONE** document. That is, every time, each student can only submit one report document, answering all questions of this assignment.
4. Students must put answers following each question in this assignment. The instructor will not grade a report with only answers in it and the student gets zero for such an assignment. An assignment report must include original questions.
5. Students MUST submit the finished assignment in either Microsoft Word or pdf format to Blackboard. The doc must be submitted as a standalone file and cannot be tarred or zipped into a container.
6. All Hands-on exercise that operates some software is required with screenshots of the actions to prove that the project is performed. The required screenshots must be put into the doc at appropriate place with explanation.
7. Refer to Print screen on how to take a screenshot. Pressing the Alt key in combination with PrtSc will capture the currently selected window.

Questions:

1. **Hands-on Project 3-2 (2 points). (Note: this project is slightly changed and different from the one in the textbook)**

Minimal requirements: Screenshot for Step 5

In this project, you make a ProDiscover image file of the data on a USB or FireWire drive, follow these steps:

1. Turn on your acquisition workstation, if necessary.
2. Connect the suspect drive to your acquisition workstation (Use write protection in real cases even if it is not required here).
3. Start ProDiscover Basic. Follow the steps in this chapter for making a raw format acquisition in ProDiscover, making sure you click UNIX style dd in the Image Format drop- down list box. Then click OK in the Capture Image dialog box.
4. When the acquisition is finished, exit ProDiscover. Dismount the USB or FireWire device, remove the suspect drive, and secure it as evidence.
5. Open the image file using ProDiscover and show all files on the USB drive are over there.

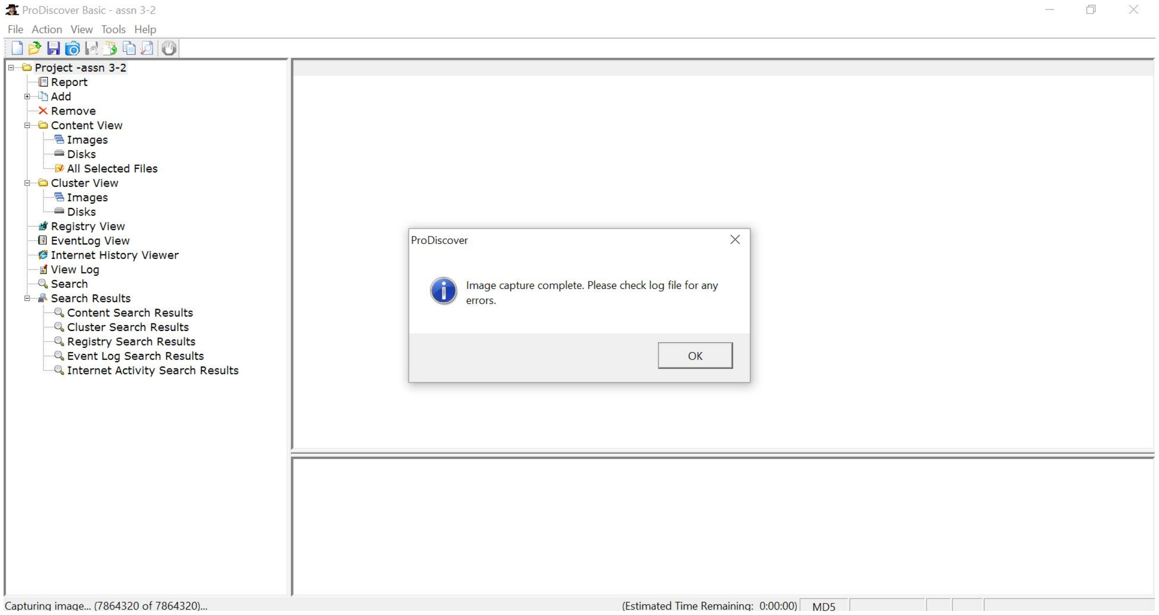
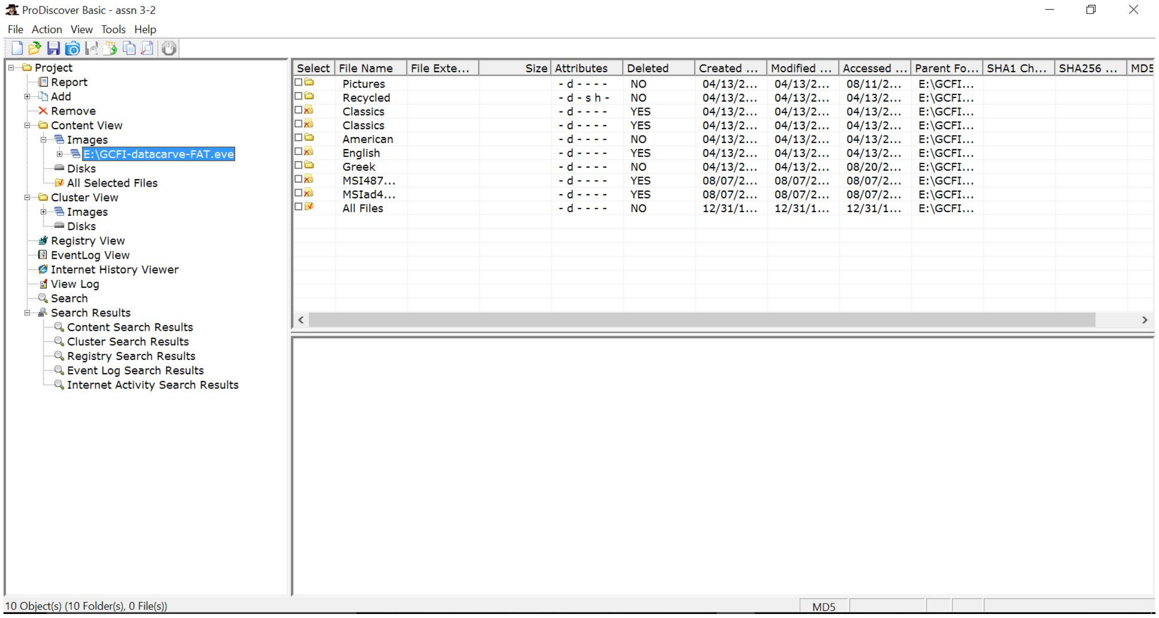


Image capture complete. Please check log file for any errors.

Capturing image... (7864320 of 7864320)... (Estimated Time Remaining: 0:00:00)



Select	File Name	File Exte...	Size	Attributes	Deleted	Created ...	Modified ...	Accessed ...	Parent Fo...	SHA1 Ch...	SHA256 ...	MD5
□	Pictures			- d - - - -	NO	04/13/2...	04/13/2...	08/11/2...	E:\GCFI...			
□	Recycled			- d - s h -	NO	04/13/2...	04/13/2...	04/13/2...	E:\GCFI...			
□	Classics			- d - - - -	YES	04/13/2...	04/13/2...	04/13/2...	E:\GCFI...			
□	Classics			- d - - - -	YES	04/13/2...	04/13/2...	04/13/2...	E:\GCFI...			
□	American			- d - - - -	NO	04/13/2...	04/13/2...	04/13/2...	E:\GCFI...			
□	English			- d - - - -	YES	04/13/2...	04/13/2...	04/13/2...	E:\GCFI...			
□	Greek			- d - - - -	NO	04/13/2...	04/13/2...	08/20/2...	E:\GCFI...			
□	MSI487...			- d - - - -	YES	08/07/2...	08/07/2...	08/07/2...	E:\GCFI...			
□	MSIad4...			- d - - - -	YES	08/07/2...	08/07/2...	08/07/2...	E:\GCFI...			
□	All Files			- d - - - -	NO	12/31/1...	12/31/1...	12/31/1...	E:\GCFI...			

10 Object(s) (10 Folder(s), 0 File(s))

2. Hands-on Project 5-1. (2 points)

Minimal requirements: Finish Step 11

In this project, you compare two files created in Microsoft Office to determine whether the files are different at the hexadecimal level. Keep a log of what you find. Follow these steps:

1. Start Word, and in a new document, type **This is a test.**
2. Save the file as **Mywordnew.doc** in your work folder, using Word 97-2003 Document (*.doc) as the file type. Exit Word.

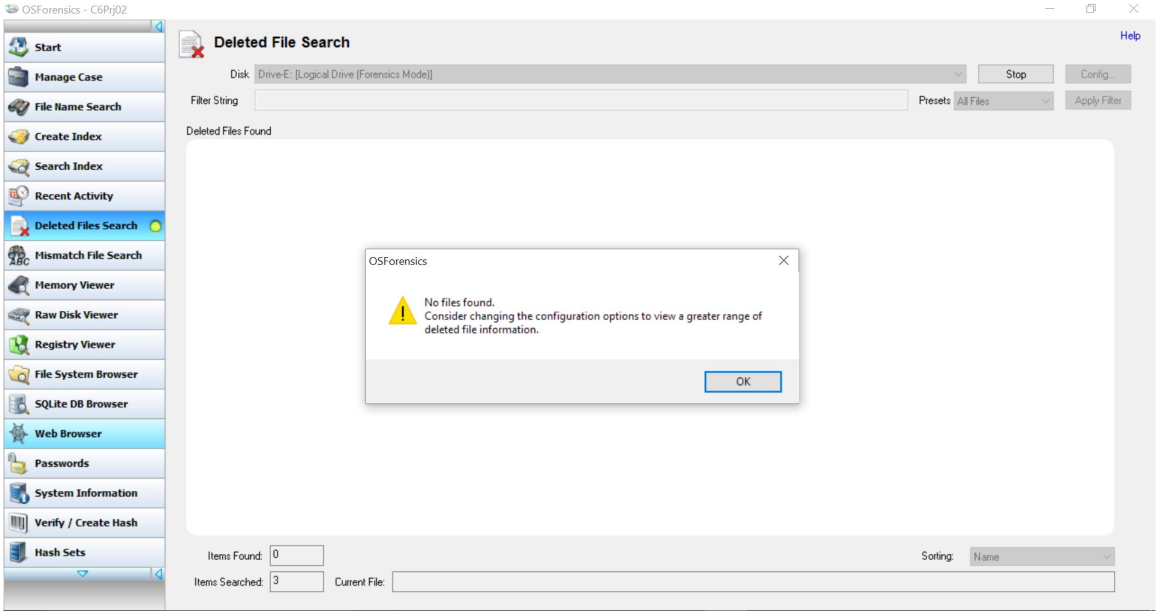
3. Start Excel, and in a new workbook, enter a few random numbers. Save the file in your work folder as Myworkbook.xls, using Excel 97 - 2003 Workbook (*.xls) as the file type.
4. Exit Excel, and start WinHex (running it as an Administrator).
5. Click **File**, **Open** from the menu. In the Open dialog box, navigate to your work folder and double-click **Mywordnew.doc**.
6. Notice the file hexadecimal header D0 CF 11 E0 Al Bl 1A El starting at offset 0. Click **Edit**, **Copy All** from the menu, and then click **Editor Display**.
7. Start Notepad, and in a new document, press **Ctrl+V** to paste the copied data. Leave this window open.
8. Click **File**, **Open** from the WinHex menu. In the Open dialog box, navigate to your work folder and double-click **Myworkbook.xls**.
9. Repeat Step 6.
10. Paste the data you just copied under the Word document header information you pasted previously.
11. In the Notepad window, add your observations about the two files' header data. Save this file as **C5Prj01.txt** and turn it in to your instructor.
12. Exit WinHex.

3. Hands-on Project 6-2. (2 points).

Minimal requirements: Finish Step 8

In this project, you research and download a disk-cleaning and wiping tool and verify that it works. Make sure you aren't on a production machine. Do an Internet search for disk-cleaning and wiping software, and download and install at least one tool. Then follow these steps:

1. Create a **C6Prj02** folder on your USB or disk drive. Start the tool you just installed.
2. Select your USB drive. Following instructions in the software documentation, wipe the drive.
3. Start OSForensics, and start a new case. Type your name for the investigator's name, type **C6Prj02** for the case name, and enter your work folder as the case path. Create a subfolder called **C6Prj02**, and click **OK**.
4. Click the **Add Device** button. Click the **Drive Letter** option button, if necessary, and in the drop-down list box, click the drive letter for your USB drive. Click **OK**.
5. Click **Start** in the left pane, if necessary, and click the **Deleted Files Search** button on the left. (Note: This is another way to open the Deleted Files Search window.)
6. Click the **Disk** list arrow, and then click the USB drive in the list of options. Click the **Search** button. Because you're searching for deleted files, you don't need to enter a file string.
7. Double-click any file in the lower pane to open it.
8. If necessary, click the **Hex/String Viewer** tab (see Figure 6-8). It should show hexadecimal 0 values, which verifies that the disk wipe worked. Take a screenshot, and then exit OSForensics. Write a short report on the tool's effectiveness, and turn it in to your instructor with the screenshot.



OSForensics - C6Prj02

Deleted File Search

Disk: Drive-E: [Logical Drive (Forensics Mode)]

Filter String:

Presets: All Files

Deleted Files Found

OSForensics

No files found.
Consider changing the configuration options to view a greater range of deleted file information.

Items Found: 0

Items Searched: 3

Current File:

Sorting: Name

The tool which have used has deleted all the content in the USB device and it’s very effective. But, after I tried to search for the deleted content using OSForensic software, the above screenshot was found. From the project we did, we can know that both the software’s are very efficient. Disk Wipe software wiped the disc completely. We can easily track deleted files in OS forensics, this can be used to find the deleted files in systems for finding cyber criminals. And also checked with the Hex/String Viewer tab.

4. Hands-on Project 8-1. (2 points)

Minimal requirements: Turn in report in Step 5

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. eve file in your work folder, and then follow these steps:

1. Start ProDiscover Basic (with the **Run as administrator** option if you’re using Vista) 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. Under Search for the pattern(s), type **JFIF**, and under Select the Disk(s)/Image(s) you want to search in, click **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 each file to find any occur-rences 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.

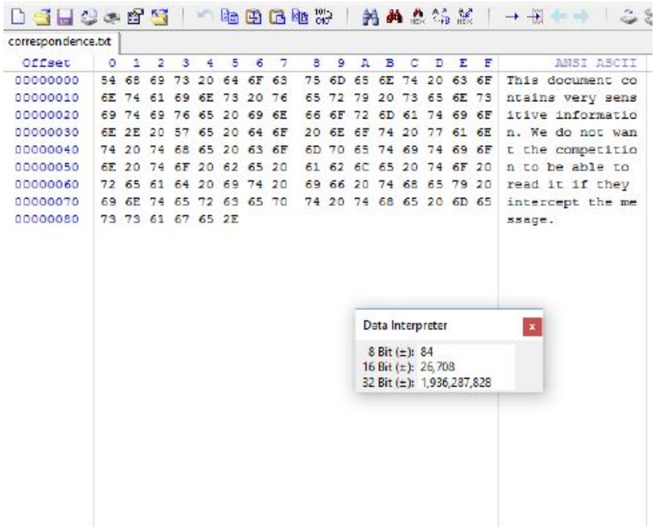
5. Hands-on Project 9-1. (2 points)

Minimal requirements: Finish Step 10

In this project, you perform bit-shifting on a file and verify that the file can be restored.

1. Start Notepad and type the following in a new text document: **This document contains very sensitive information. We do not want the competition to be able to read it if they intercept the message.**

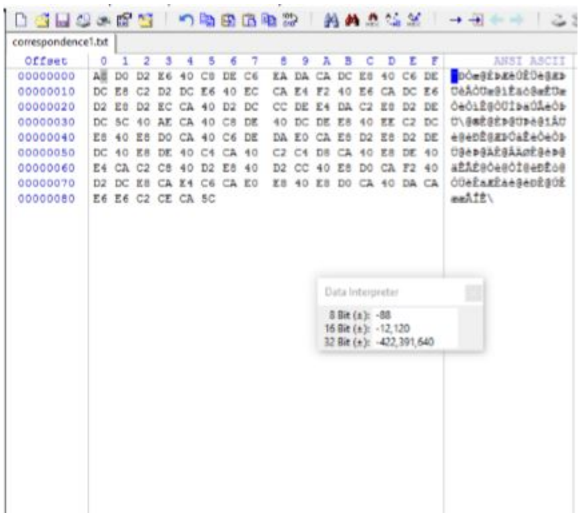
2. Save the file as **correspondence.txt** in your work folder, and then exit Notepad.
3. Start WinHex, and open the **correspondence.txt** file.
4. In the in-chapter activity, you used the left and right shift options. For this project, you use the Circular left rotation option in the Modify Block Data dialog box. (Note: Because this text file is ASCII, returning it to a readable state takes eight circular left rotations.) Click **Edit**, Select **All** from the menu.
5. Click **Edit**, **Modify Data** from the menu. In the Modify Block Data dialog box, click the Circular left rotation option button, and then click **OK**.
6. Save the file as **correspondence1.txt**, and exit WinHex.
7. Restart WinHex, and open **correspondence1.txt**. Click **Edit**, **Select All** from the menu.
8. With the file's contents highlighted, click **Edit**, **Modify Data** from the menu. In the Modify Block Data dialog box, click the **Circular left rotation** option button, if necessary, to rotate the bits, and then click **OK**. Repeat this step seven times to verify that you can recover the data.
9. When you have recovered the text to its readable state, save it as **correspondence2.txt**.
10. Write a short paper stating whether you think this method is a reliable one for encrypting. Leave WinHex running for the next project.



```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
00000000  54 68 69 73 20 64 6F 63  75 6D 65 6E 74 20 63 6F  This document co
00000010  6E 74 61 69 6E 73 20 76  65 72 79 20 73 65 6E 73  ntains very sens
00000020  69 74 69 76 65 20 69 6E  66 6F 72 6D 61 74 69 6F  itive informatio
00000030  6E 2E 20 57 65 20 64 6F  20 6E 6F 74 20 77 61 6E  n. We do not wan
00000040  74 20 74 68 65 20 63 6F  6D 70 65 74 69 74 69 6F  t the competitio
00000050  6E 20 74 6F 20 62 65 20  61 62 6C 65 20 74 6F 20  n to be able to 
00000060  72 65 61 64 20 69 74 20  69 66 20 74 68 65 79 20  read it if they 
00000070  69 6E 74 65 72 63 65 70  74 20 74 68 65 20 6D 65  intercept the me
00000080  73 73 61 67 65 2E                                 ssage.
```

```
Data Interpreter
 8 Bit (±): 84
16 Bit (±): 26,708
32 Bit (±): 1,936,287,828
```

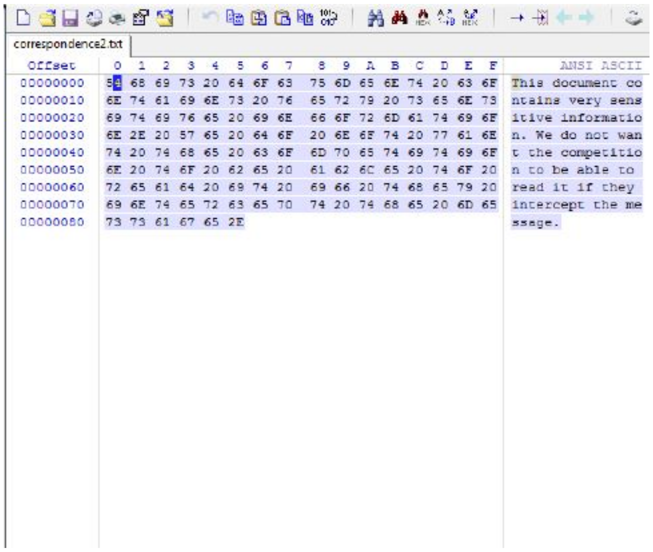
First left shift image



```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
00000000  A8 D0 D2 E6 40 C8 DE C6  EA DA CA DC E8 40 C6 DE  ¨ÐÒæ@ÈÞÆêÚÊÜè@ÆÞ
00000010  DC E8 C2 D2 DC E6 40 EC  CA E4 F2 40 E6 CA DC E6  ÜèÂÒÜæ@ìÊäò@æÊÜæ
00000020  D2 E8 D2 EC CA 40 D2 DC  CC DE E4 DA C2 E8 D2 DE  ÒèÒìÊ@ÒÜÌÞäÚÂèÒÞ
00000030  DC 5C 40 AE CA 40 C8 DE  40 DC DE E8 40 EE C2 DC  Ü\@®Ê@ÈÞ@ÜÞè@îÂÜ
00000040  E8 40 E8 D0 CA 40 C6 DE  DA E0 CA E8 D2 E8 D2 DE  è@èÐÊ@ÆÞÚàÊèÒèÒÞ
00000050  DC 40 E8 DE 40 C4 CA 40  C2 C4 D8 CA 40 E8 DE 40  Ü@èÞ@ÄÊ@ÂÄØÊ@èÞ@
00000060  E4 CA C2 C8 40 D2 E8 40  D2 CC 40 E8 D0 CA F2 40  äÊÂÈ@Òè@ÒÌ@èÐÊò@
00000070  D2 DC E8 CA E4 C6 CA E0  E8 40 E8 D0 CA 40 DA CA  ÒÜèÊäÆÊàè@èÐÊ@ÚÊ
00000080  E6 E6 C2 CE CA 5C                                 ææÂÎÊ\
```

```
Data Interpreter
 8 Bit (±): -88
16 Bit (±): -12,120
32 Bit (±): -422,391,640
```

We get back the original message After 7 shifts



```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
00000000  54 68 69 73 20 64 6F 63  75 6D 65 6E 74 20 63 6F  This document co
00000010  6E 74 61 69 6E 73 20 76  65 72 79 20 73 65 6E 73  ntains very sens
00000020  69 74 69 76 65 20 69 6E  66 6F 72 6D 61 74 69 6F  itive informatio
00000030  6E 2E 20 57 65 20 64 6F  20 6E 6F 74 20 77 61 6E  n. We do not wan
00000040  74 20 74 68 65 20 63 6F  6D 70 65 74 69 74 69 6F  t the competitio
00000050  6E 20 74 6F 20 62 65 20  61 62 6C 65 20 74 6F 20  n to be able to 
00000060  72 65 61 64 20 69 74 20  69 66 20 74 68 65 79 20  read it if they 
00000070  69 6E 74 65 72 63 65 70  74 20 74 68 65 20 6D 65  intercept the me
00000080  73 73 61 67 65 2E                                 ssage.
```

The method we are following here is not reliable for using as an encryption method as we are shifting bits to the left. Any intruder can easily decode the message from this. **Not a suitable form of encryption.**