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.

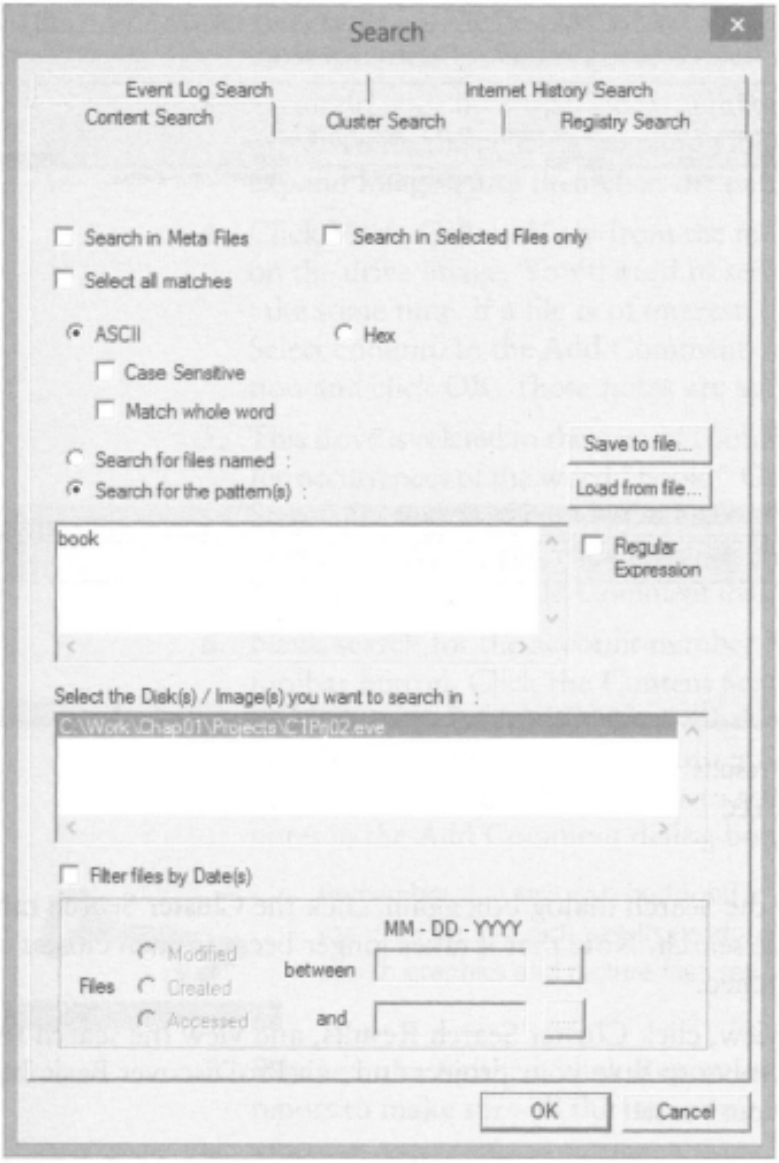
Hands-On Project 1-2

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**.



Search

Event Log Search | Internet History Search

Content Search | Cluster Search | Registry Search

□ Search in Meta Files □ Search in Selected Files only

□ Select all matches

● ASCII ○ Hex

□ Case Sensitive

□ Match whole word

○ Search for files named :

● Search for the pattern(s) :

book

□ Regular Expression

Select the Disk(s) / Image(s) you want to search in :

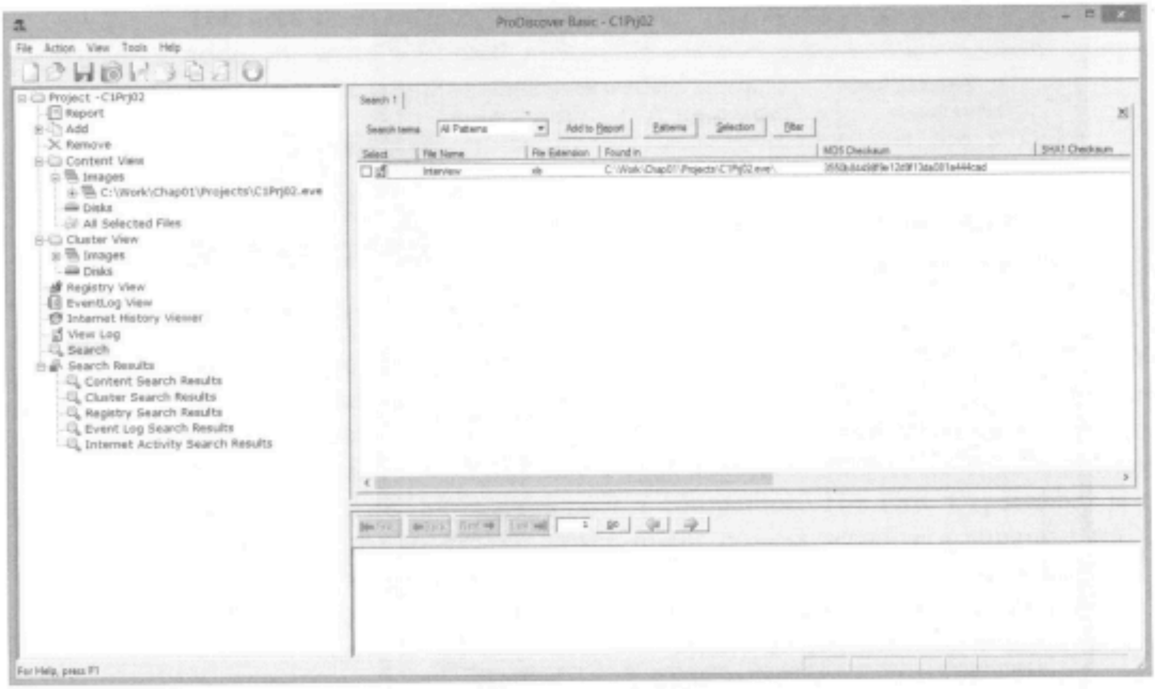
C:\Work\Chap01\Projects\C1Prj02.eve

□ Filter files by Date(s)

Files ○ Modified ○ Created ○ Accessed between and MM - DD - YYYY

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.



Select	File Name	File Extension	Found in	MD5 Checksum	SHA1 Checksum
□	Interview	rtf	C:\Work\Chap01\Projects\C1Prj02.eve\	[illegible]	

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.

TIP

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.