Computer Forensics 2
Lab 5 – Searching and Bookmarking Data
(Ref – Chapter 7 – EnCE The Official EnCase Certified Examiner by Steve Bunting)
Edited by Dr Diane Gan

Objective – Import Keywords, search for data and Bookmark using EnCase.
Don't forget to collect your Dongle before you start EnCase

1. **Create a new case**
   Create a folder called **OnLineDrugSales** in the folder **C:\ Users\Student\*Yourname*** and add the standard folder structure (**Temp, Index, Export**) for a new case, as in Lab 5. Create a new case, pointing it at your new folders and SAVE your case as **OnLineDrugs** before you start**.**

   Copy the following files to your Case folder from
   Dianes Utils Exercises\Authors Example Evidence Files\Evidence Files\07_Chapter Seven Data Searching
   Bookmarking\ThumbDrive_Evidence_File **:-**
   ThumbDrive_Evidence_File\DefFrostyUSB16MB_TD01.E01
   Keywords_For_Import.txt
   Format_Template.txt

2. Add an evidence file by clicking **Add Device.** Create a new path to your evidence folder in your case folder on the C drive. Locate the evidence file in the right pane and bring it into your case. **Save your case again,** making sure that it is saved in your case folder.

3. To begin your search, go to the case-level **Keyword tab** (scroll right to see this). In the Tree pane, right-click at the root of the tree and select **Import**.

4. Browse to the folder on the D drive called **Keywords_For_import** and locate the file called **Keywords_for_Import.txt** Click OK to complete the import.

5. Click **Set Include Folders** (goes green) at the case level (top level). You should now see several expressions (10) in the Table View. These are Grep expressions which we will use for searching.

6. Remove the Set Include by clicking it again. Browse to the keyword Tracking Numbers and blue-check the one for UPS Tracking Number.

   Browse to the Windows Artefacts folder and blue-check the one for dot double dot.

   You should now have selected two keywords for your case.

7. Locate the Dixon Box and make sure it is reading zero. If not, click it once to set it to zero and then click it again to select all the files in your case.

8. On the toolbar, click search. A Search box should pop up.

   Click **Selected items only**. Click **Search entries and records for keywords**.
   Click **Selected keywords only** and **Search entry slack**

   - How many keywords are selected?

   Click Start to begin your search. This should complete very quickly.

   - How many files have been scanned and how many search hits did you get?

Check the Note option and then click OK – save your Case.

9. On the Case level tab bar, scroll left to find the **Search Hits** tab. In the Tree pane, select UPS Tracking Number. In the Table pane, note the search hits with a UPS tracking number.

- How many search hits did you get for a UPS Tracking Number?

10. Click on **Search Hits** and in the View pane (bottom left), switch to Text view. Select all the readable text by placing your cursor on the first byte and clicking and dragging to the last byte of text. Right-click in the selected text and chose the **Bookmark Data**.

In the **Destination Folder** (on the right) right-click and create a New Folder called **EnCase Computer Forensics Report**. Then create a sub-folder called **Email Orders**. Select this folder as the destination folder.

Under **Data Type** (in the left box) choose **Text** and **Low ASCII** – enter an appropriate comment in the top box and click OK. You should now have a bookmark in the **Bookmarks** view tab.

11. Click the **Dixon box** to clear all selected files. In the **Table view** where the tracking number hit is located, right click and choose **Tag File**. The Dixon box should show one file selected.

Go to **Cases / Entries** (scroll lift) view and click the Set Include Folders trigger at the case or root level. All files in the case are now showing in the Table view (top right window).

In the **Filter pane** (bottom right) go to the **Conditions** tab. Go down the tree to **General Conditions** and double click on the condition **Selected Files Only**. Your one selected file should be the only one now showing. This is useful when many files are selected. Note the location of the tagged file, which is in the My Documents\Email Orders\Customer SB folder.

On the Toolbar at the top, click the **Query button**, turning a + into a – (minus). This turns off the filter. Navigate in the Tree pane to Customer SB and you will see three files, including the one you just selected. (Try sorting on File Ext by double clicking on the title box until you get a red triangle. Try to get the .txt files near the top.)

12. Leave the file selected and in the Table view, highlight the file August 20 2005 order.txt. (If you double click it, it will open in a notepad.)

In the view pane, note the contents and how it relates to the file that you have already selected. Blue-check this file.

Look at the contents of the third file called Original Order with Address.txt. The contents appear strange. We need to Bookmark each of these two other files.

13. Right click in the Table view pane and choose Bookmark Data. In the Destination Folder pane, select Email orders and right click and then create a new folder called File Group Bookmark. [In a real report, you would rename this something more meaningful.] Be sure to click Bookmark Selected Items (top right check box). Click OK.

14. In the Table view, highlight the file Original Order with Address.txt. and view it in the View pane. Using the Text view tab, note that numbers and special characters appear normally but characters are abnormal. This is actually ROT13 (rotate characters 13 places) encoding, which is used in news groups and in the Windows registry. It can also be used to get around email and web content filters.

Highlight all the text, right click and chose Bookmark Data. Under Data Types select Text and ROT13. In the bottom pane of the pop-up box, the text should be decoded. In the Destination Folder pane, create a folder under Email Orders, name it ROT13 and select it as the destination. Click OK.

15. In the Tree pane, navigate to the My Documents\My Pictures folder (Cases – Entries – Home). Click the Dixon box to clear any selected files. Remove the Set Include at the root level, if on. Place a blue check next to each of the two files selected. Right click in the Table view and chose Bookmark Data. Make sure that the Bookmark Selected Items is checked. Select the subfolder called EnCase Computer Forensic Report. Create a new folder called Images and click OK.

16. In the Tree pane go to the folder My Documents\Dates and Times. There is a file called Dates and Times.txt. Highlight this in the Table pane. View it in the View pane as Hex. In the text view on the right of the Hex view, place your cursor on the first character immediately following the first appearance of the > (non-readable characters). In the Hex view hold down the mouse button and drag to highlight a further three bytes – total of 4 bytes highlighted.

- What is the value of the LE indicator (on the bottom bar)?

You should have highlighted the hex string E2 49 07 43. You are looking at a Unix date stamp. This is 4 bytes in length and is also known as a Dword. In the hex view right click and chose Bookmark Data. In Data Type choose Dates\Unix Date

- What can you see now?

Create a destination folder under EnCase Computer Forensics Report and name it Dates and Times. Select this folder and click OK.

17. With the same 4 bytes selected, right click and choose Bookmark Data again. Under data Type, choose integers\32-bit integers. The number should resolve to a 10 digit integer. This is the number of seconds since Jan 1, 1970, 00:00:00 GMT.

- What is this integer?

- How many digits are there in the Int32 column?

You are now beginning to recognise this as a Unix numeric date stamp. You will see this same integer further down the text of the message. Select this second ten digit number in the text view. Right click the Hex view and choose Bookmark Data. Select the data type as Dates - Unix Text Date.

- What value can you see now?

Place this Bookmark in the folder called Dates and Times and click OK.

Go to the bottom of the text and locate another set of odd characters between > < . Select these characters.

- How many bytes are selected?
- What is the value of the LE indicator?
- What is the value of the hex number selected?

Bookmark this data by right clicking on the hex view. Choose the Data Type as Dates – Windows Date/Time and select the destination folder Dates and Times.

18. Go to the Bookmarks view tab in the Tree pane and highlight the folder Email Orders. In the Table pane you should now see two folders and one Highlighted data bookmark. In the Tree pane under Email Orders, right click and create a new folder called Highlighted data bookmark. There are now three folders showing in the Table pane.

In the Tree pane, highlight Email Orders again, forcing the highlighted data and the three folders into the Table pane. In the Table view pane, drag, by its handle, the highlighted data bookmark to the folder in the Tree pane and drop it onto the folder named Highlighted data bookmark. You have just moved a bookmark into a newly created folder.

19. In the Tree pane of the Bookmark view, highlight the folder EnCase Computer Forensics Report. Right click and choose Edit. Using Windows Explorer, browse to the folder Exercises\Author's Example Evidence Files\07_Chapter Seven Data Searching Bookmarking\Format_Template and select a file called **Format_Template.txt**. Open this file and select the entire contents (Ctrl-A) and copy (Ctrl-C). Place your cursor back in the Edit "EnCase Computer Forensics Report" pop-up and paste (Ctrl-v) into the Format pane. Click OK. This creates a format for your report and has placed it at the top level.

20. In the Tree pane, activate Set Include at the Encase Computer Forensics Level. All bookmarks should now appear in the table view. In the table view, switch to report view and the final report should generate. In the Table view pane, right click the Report view tab and choose Export. In the menu, create a folder in your case folder structure and name it Reports. Choose the Report folder as the destination folder. Choose **Web Page** as the type. Name this file **Report.** Click OK to generate the report.

21. Navigate to the folder in your case folder called Report. Double click the file called Frame View.html to open the file. Your paperless report will launch.

Visit the Gallery tab and the Full Report tab in the browser. You may have to allow blocked content in the browser. If you need to change anything in the report, you can change it in EnCase and export it again.

If you want to look at the author's version of the report, then go to Exercises\Author's Example Evidence Files\07_Chapter Seven Data Searching Bookmarking\ EnCaseComputerForensicsReport\Reports and you can see what the finished report should look like. Double click the file Frame View.html

Save your case and exit EnCase. Return the Dongle to the Technicians.

Answers to Questions

8.	2 keywords are selected	526 files scanned	6 hits
9.	One search hit		
16	LE = 4	Time/Date 08/20/05 04:18:58PM	
17.	1124551138	10 digits	Time/Date 08/20/05 04:18:58PM
	8 bytes	LE 8	60 8D D7 95 9C A5 C5 01