Computer Forensics 2
Lab 4 – Introduction to EnCase - Navigation

Based on Exercise 6.1, Ch. 6 – EnCE The Official EnCase Certified Examiner by Steve Bunting
Edited by Dr Diane Gan

Objective - Create a new case, add an evidence file and navigate around EnCase software.
The answers to all questions are given at the end of the lab sheet.

Before you start EnCase ensure that you have the special **DONGLE** in a USB port. This is **NOT** a Thumb drive. You will need a thumb drive (USB stick) is you wish to save your work.

1. **Creating the standard folder structure:-**
   On the C drive, create a folder called **Users\Student *yourname.***
   In this folder create a folder called **Navigation**.
   In your case folder create three new folders called **Temp, Export** and **Index**.
   Select these folders for the new case and then Save your case as **Navigation**.

   You must do this for EVERY case using EnCase.

2. Locate the evidence file called **Navigation.E01** in the folder **Diane's Utils Exercises\Authors Example Evidence Files\06_Chapter Six EnCase Environment** and copy it to your folder called **Navigation** on the C drive**.**

3. Using the desktop icon called EnCase v6.18-local, start EnCase and create a new case called **Navigation**. NOTE – make sure that it does **NOT** say **Acquisition** at the top. If it does then you have either forgotten to get a Dongle or it is in the wrong USB slot.
   Select the **Temp**, **Export** and **Index** folders from your case folder in the pane.

4. **Save the case** – calling it **Navigation** and save it in the root folder of your case folder.

5. In EnCase, select **Add Device** from the top menu. When the popup box opens check **Sessions** and then click the **Add Evidence Files** button and highlight the evidence file. Browse to the evidence file called Navigation.E01 and click Next, Next and Finish. You should see 0/16 in the Dixon Box.

6. **Save your case again, before you start**. [Good practice - save your work periodically.] Make sure that it is saved in the root of the Navigation Folder.
   Check the folder using Explorer – you should see a file ending **.E01** and another ending **.Case**

7. In the Tree pane, your should see Cases > Entries > Home and the evidence file called **FileSigAnalysis**. Look carefully at the icon. What kind of a device do you think this is?

8. In the Tree pane, highlight the root-level word **Entries**. In the Table pane you should see a single floppy device. In the View pane, click **Report**. Scroll through and answer the following questions:-

   a. Did your evidence file properly verify?
   b. What file system is on this device?
   c. How many sectors does it contain?
   d. On what date was it acquired?
   e. How many sectors per cluster?

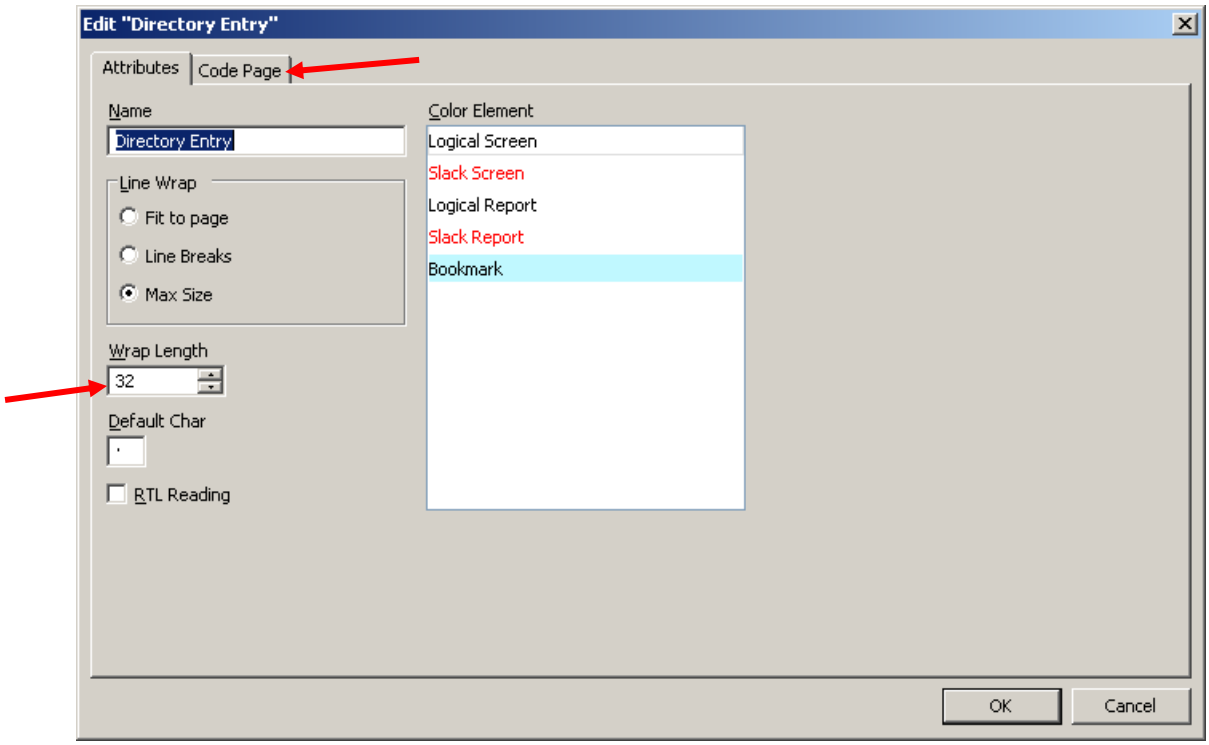
9. In the Tree pane place your cursor on the floppy icon. In the Table pane you should see five objects. One of these is a folder named FileSignatureAnalysis. Place your cursor on that folder in the Table pane. In the View pane click on the **Text**

a. What colour is the data?

b. What does this colour indicate? (answers at the end)

10. Creating a text style for viewing FAT directory entries:-
In the bottom right-hand pane (Filter pane) click on **Text Styles.** Right click on the root of the tree structure called Text Styles and select **New folder**. Name the new folder **Custom.**

In the **Custom** folder, right click and select New. A pop-up box to open – see below. Change the Attributes name to **Directory Entry**. Select **Max Size** and enter 32 in the **Wrap Length** box.



Click on the **Code Page tab** and check **Other**. Then scroll down to **Latin 9 (ISO)**. Click OK to finish.

Go to any other text style and then return to the one you have just created to refresh the view. Your data should now be in 32 byte rows.

Place your cursor on **Volume Boot** and select **Disk view** at the top of the Table pane. In the **Filter** pane scroll to the right until you see Legend. Click on this to see what the different colours mean.

- Where is your cursor located? [Hint – look at the GPS bar at the bottom]

Select the first dark blue square (disk view in the Table Pane). Select the first row in the bottom left pane. Right click and chose **Bookmark Data**. In the Data Type window scroll up to **Windows** – **DOS Directory Entry.** Click OK to save the bookmark.

- What information did you find regarding this file in the Directory?

11. Back to Table View. Place your cursor on the folder **FileSignatureAnalysis** in the Tree pane. You should see 10 files in the Table pane. Place your cursor on the file called "jpeg image.jpg". In the View pane you should see the image. In the View pane switch to the Hex view.

- What are the first 4 bytes of the jpeg file? (Use the GPS on the bottom of the frame)

- What does this tell you?

12. Return to the Table pane, where the 10 files are listed and switch to Gallery view.

- How many jpg images are shown?

13. In the Table view with the file named "jpeg image.jpg" highlighted. In the View pane, switch to Picture view if this has not already happened automatically. In the View pane, place a check in the box named **Lock**. This should lock the View pane in the Picture view.

14. Go to the list of files in the Table pane and highlight each one in turn. This forces them to resolve as pictures in the View pane. Even though the file extension may be different, EnCase will pick up the fact that a file is a picture from the file signature.

15. Put a blue check in the box next to each of the files that you think are images. The Dixon Box should show three or four files selected. [Check the Hex view of the jpeg with bad header]

16. At the top of the Table pane, double click the un-named box above the blue checks. This sorts the files. You can sort on any of the columns in this manner. This can be very useful if there are hundreds of files to search.

17. To add a secondary sort:- go to the File Created column. Hold down the shift key and double click the File Created header. The selected files should now be in chronological order. Look at the Last Written column.

- What is the significance of the dates and time?

18. In the Table pane, click Timeline. On the main tool bar there are a number of checked boxes – uncheck all the boxes except the Written box. You should now see a number of squares in the Timeline area, indicating the files with the same creation dates. In the Filter view (bottom right) click on **Conditions**. Scroll down until you find **General Conditions** and double click **Selected Files Only.**

- How many files can you see now?

Go back to the Table view and click on the Query icon on the top bar to remove the filter. All the files should now be visible again.

Go back to the Timeline view and double click the cluster of 4 files until it resolves to a higher resolution, showing four distinct boxes. Select Picture and place your cursor on each box, and the image files will resolve in the bottom left View pane. You can see that three have the file signature FF D8 FF D0 even though they do not all display correctly as images.

19. In the Tree pane click the **Set Include Folders** (goes green) at the case level (top level). All the objects now appear again in the Table pane. Note that the sorted files are still at the top. Turn off the **Set Include Folders** trigger by clicking it again.

20. In the Tree pane, highlight the floppy device icon. In the Table pane click the icon called **Disk** to get the disk view. In the view pane select the Hex view. In the Filter pane (bottom right) select **Legend** to decode the colours. This is a floppy disk and so does not have a MBR. The VBR occupies the first sector. After the VBR comes FAT1 and FAT2. Following FAT is the root directory, shown in green. The first cluster that can hold files comes directly after the green squares. Place the cursor on the first blue square.

a. What does MBR stand for?
b. What does VBR stand for?

21. The GPS currently reads (PS 33 LS 33 CL 2 SO 000 FO 0 LE 1). Locate this at the bottom left of the window. FAT useable clusters start at 02 and the first two FAT entries (00 and 01) hold other metadata. For a floppy, the volume starts with the first sector. This means that the physical sector and the logical sector offsets are the same. Move the cursor one to the right.

- What is the location of this blue square? [Hint look at the GPS]

22. Right click in the data area of the Table pane and choose Go To from the menu. Type 2879 and click OK. This takes you to sector 2879. This is because there are 2,880 sectors on the floppy disk (0 to 2879). This is the last sector of this device.

23. Go back to the Table view. In the Tree pane highlight the folder **FileSignatureAnalysis**. In the Table pane, highlight the file named "no header in a table and matches no other header MATCHES.txt". In the View pane select the Text tab. Highlight the fifth word "file" and the right click and select **Find.**
Press F3 to find the next instance of the word. Save your Case and exit.

Answers to questions

7. A floppy disk
8. b. FAT12, c. 2,880 d. 8/12/2003 e. One
9. a. Red, b. Directory data
10. Name of the file, date and time it was Created and Written, and date it was last Accessed, the size and the starting cluster
11. FF E8 FF E0
12. Only two files are legitimate jpg files – these are picked up by Encase and it ignores the rest which are not jpg files, even though they have the jpg file extension. The file "jpeg image with bad or unk header.jpg" is blank, although EnCase identifies it as a jpg.
17. The files were all created within a few seconds of each other and were created after they were Last Written – how can this be? The File Created field shows when these files were moved to their present location.
18. This should now be saying 3 files as you are seeing only your selected files.
20. a. MBR = master boot record b. VBR = volume boot record
21. GPS reading = PS 34 LS 34 CL 3 SO 000 FO 0 LE 1 – with a floppy disk one sector = one cluster.

GPS bar abbreviations

PS	physical sector	LS	logical sector	FO	file offset (distance in bytes)
CL	cluster number	SO	sector offset	LE	length (bytes selected)