Worcester Polytechnic Institute
Department of Computer Science

Module 2: Use Winhex to Examine NTFS Disks

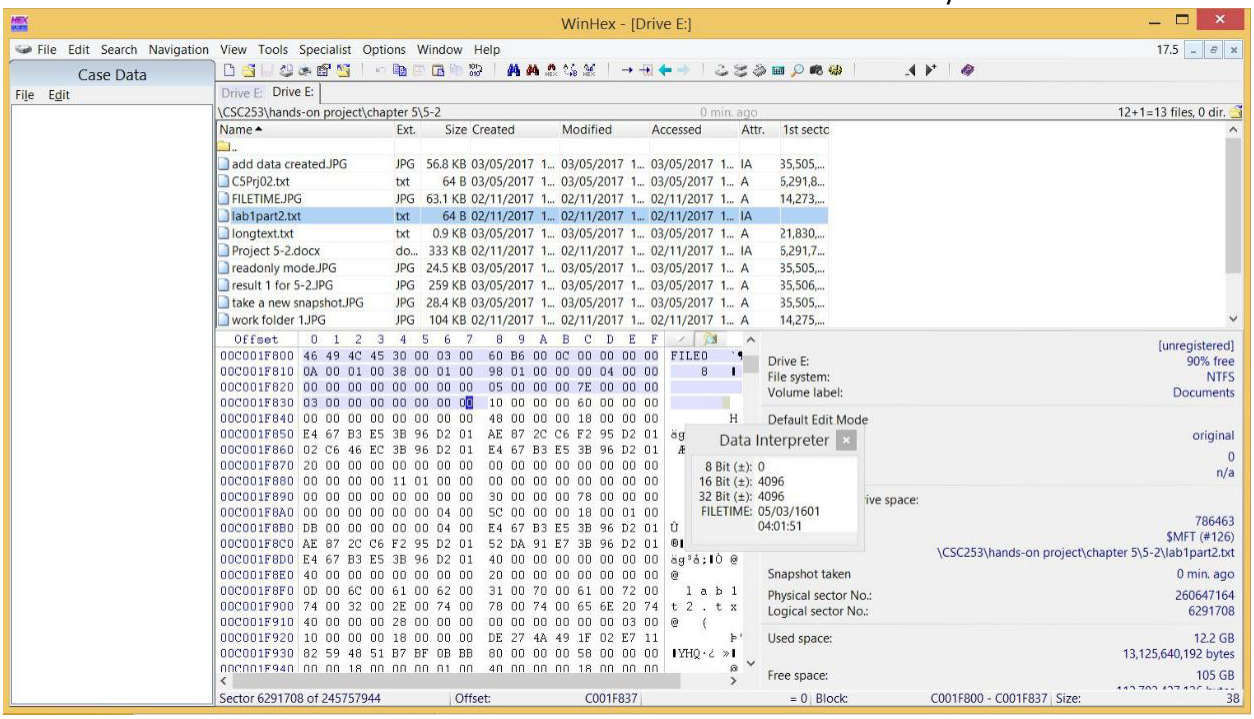
Objectives:

- Become familiar with the WinHex forensics tool.
- Use WinHex to become familiar with different file types.
- Use WinHex to explore and become familiar with the MFT, including headers and attributes.

Instructions: This lab is designed based on the hands-on projects provided by our textbook. We adopt the use of these hands-on projects in this computer forensics class with full respect to the contributions and copyright of the original textbook authors.

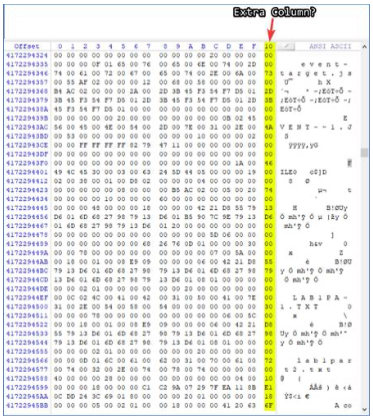
Some Tricks that you need to Pay attention in this lab:

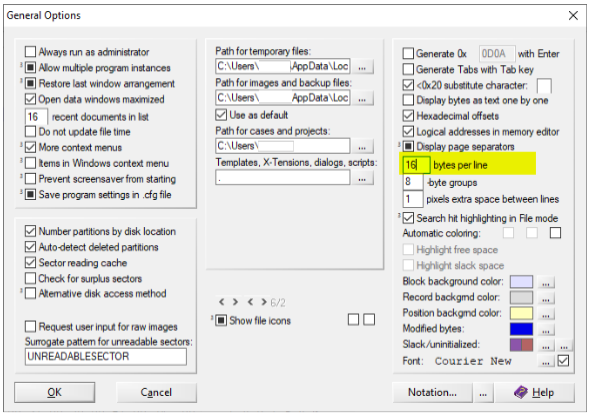
1. When you keep clicking on the offset data on the left column, it can switch between decimal and hexadecimal. Please make sure the data shown is hexadecimal for the analysis.



2. When you click on a file, sometimes the cursor is located at a random position within the file, rather than the beginning of file MFT (FILE0). In this case, you can either scroll up to find the “FILE0” beginning, or you can close the winhex program and restart. This will reset the cursor.

3. You need to analyze the MFT within the Drive. If you double click on the file and open another tab for this file in Winhex, it only shows the content of the file, but doesn't show the MFT information.
4. How to change the number of bytes per line in Winhex if you see extra column? Navigate to Options->General, and change the "bytes per line" as highlighted in the figure below.





Part 1: Explore different file types.

!!! **For part 1, you can do it on local host because the virtual machine does not have Microsoft office installed.**

1. Start Microsoft 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. Right click on WinHex and choose "Run as an Administrator" to start WinHex.
4. Click **File**, **Open** from the menu. In the Open dialog box, navigate to your work folder and double-click Mywordnew.doc.
5. Notice the file hexadecimal header D0 CF 11 E0 A1 B1 1A E1 starting at offset 0. Select this header, right click on it, choose **Edit**, **Copy Block**, and **click** on Editor Display.

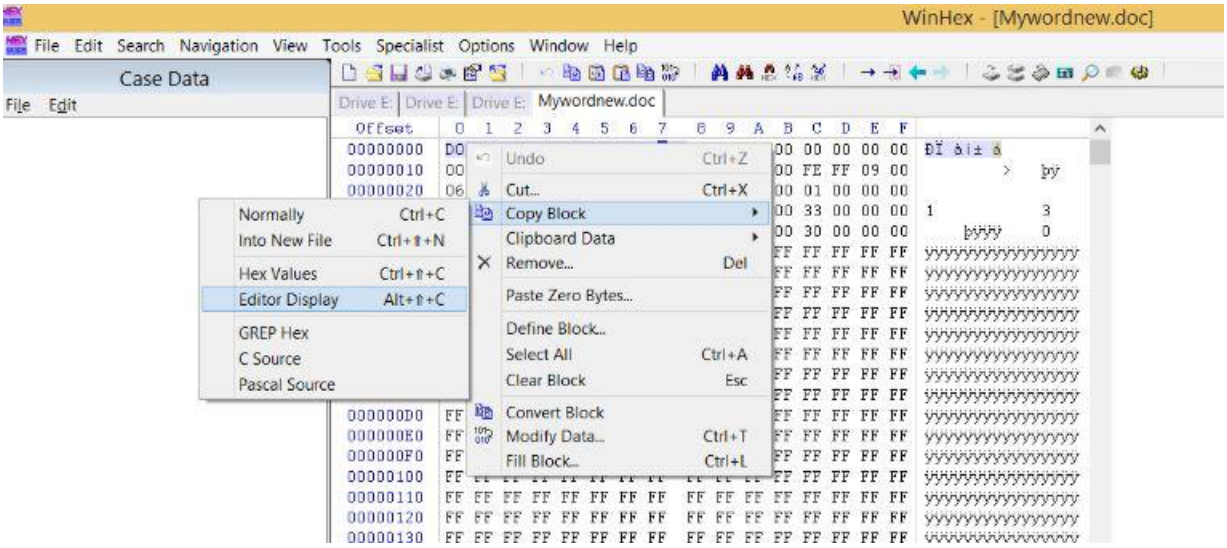
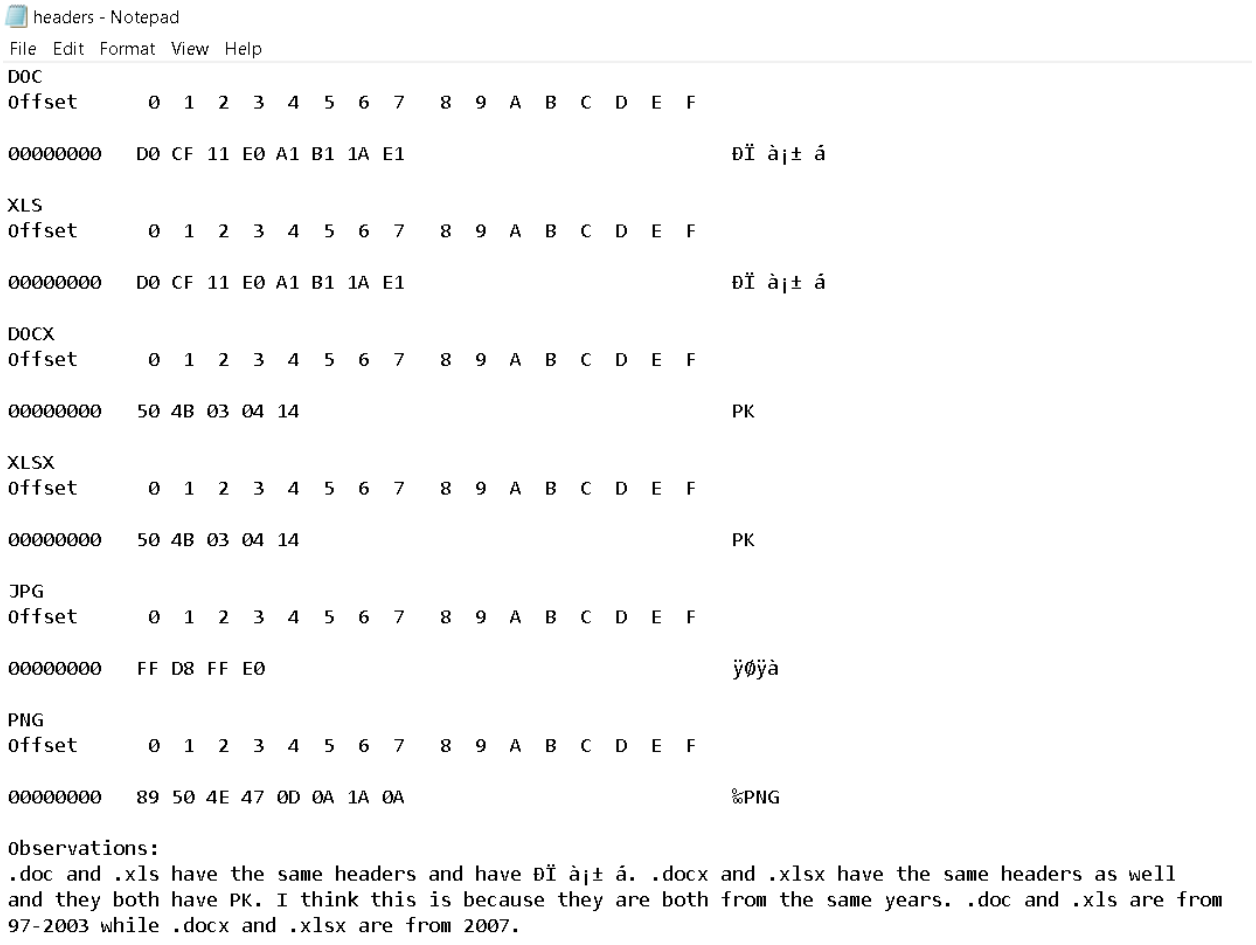


Figure 1

6. Start NotePad, and in a new document, press **Ctrl+V** to paste the copied data. Leave this window open.
7. Repeat Step 4-6 to examine following file types.
   (1) Create a new Excel file, and save it using Excel 97-2003 Workbook (.xls) as the file type.
   (2) Create a new word file, and save it using .docx as the file type.
   (3) Create a new Excel file, and save it using Excel 2007 Workbook (.xlsx) as the file type.
   (4) Create a new .jpg file.
   (5) Create a new .png file.
8. Paste the data you just copied under the Word document header information you pasted previously.
9. In the Notepad window, add your observations about the six files' header data.



10. This is an example of what your text file with your headers and observations could look like.

Part 2: Explore MFT.

(Ignore this warning and go straight to Step 1 if you installed WinHex directly on your computer)

!!! ***For part 2, you have to do it on the forensics virtual machine because you need to "Run as administrator". To start the virtual machine, start VMware Workstation, click on "File"->"Open…", go to the path VM(E:) -> VM-> Forensics, click on Forensics.vmx, then power on the virtual mchine.***

Then following the steps below to complete the hands-on.

1. Start Notepad, and create a text file with one or more of the following lines:
   - A countryman between two layers is like a fish between two cats.
   - A slip of the foot you may soon recover, but a slip of the tongue you may never get over.
   - An investment in knowledge always pays the best interest.
   - Drive thy business or it will drive there.
2. Save the file in your work folder as lab1part2.txt, and exit Notepad.
3. Next, examine the metadata of the lab1part2.txt file stored in the $MFT file. Start WinHex with the **Run as administrator** option. If you see an evaluation warning message, click **OK**. As a safety precaution, click **Options**, **Edit Mode** from the menu. In the Select Mode dialog box, click **Read-Only Mode** (=**write protected**), as shown in Figure 2, and then click **OK**.

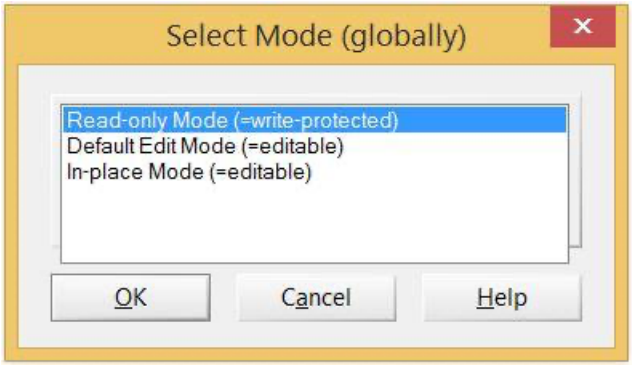


Figure 2

4. Click **Tools**, **Open Disk** from the menu. In the **View Disk** dialog box, click the drive where you saved lab1part2.txt., and then click **OK**. If you're prompted to take a new snapshot, click **Take a**

new one. Depending on the size and quantity of data on your disk, it might take several minutes for WinHex to traverse all the files and paths on your disk drive.

5. Click **Options**, **Data Interpreter** from the menu. In **the Data Interpreter Options** dialog box, click the **Win32 FILETIME (64 bit)** check box, shown in Figure 3, and then click **OK**. The Data Interpreter should then have FILETIME as an addition display item.

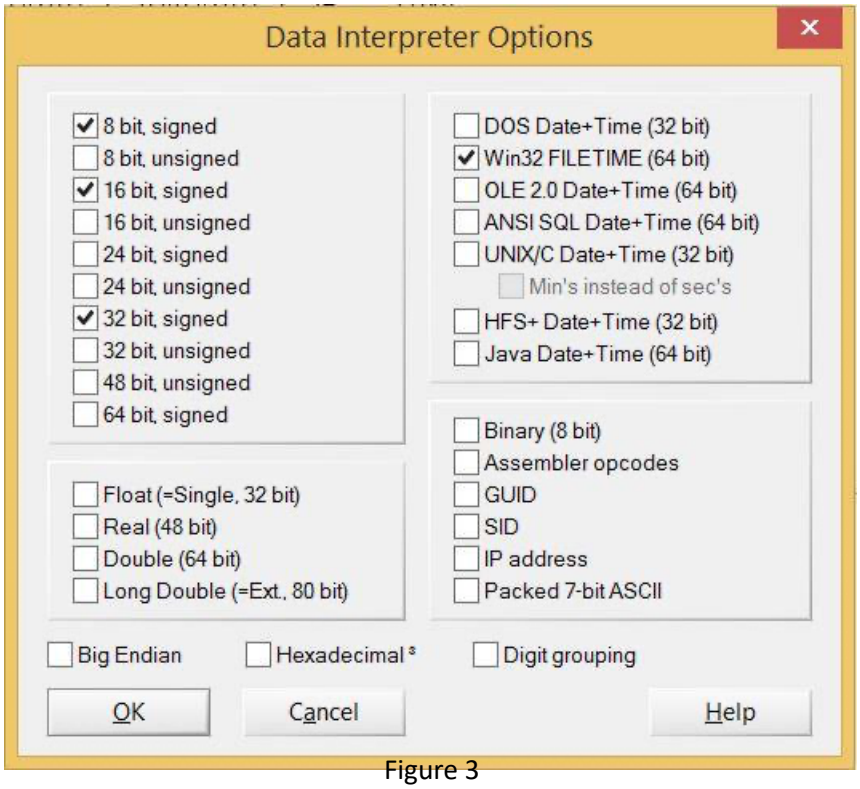


Figure 3

6. Now you need to navigate to your work folder where you saved your lab1part2.txt in WinHex. In the upper-right pane of WinHex, scroll down until you see your work folder. Double-click each folder in the path and then click the lab1part2.txt file.

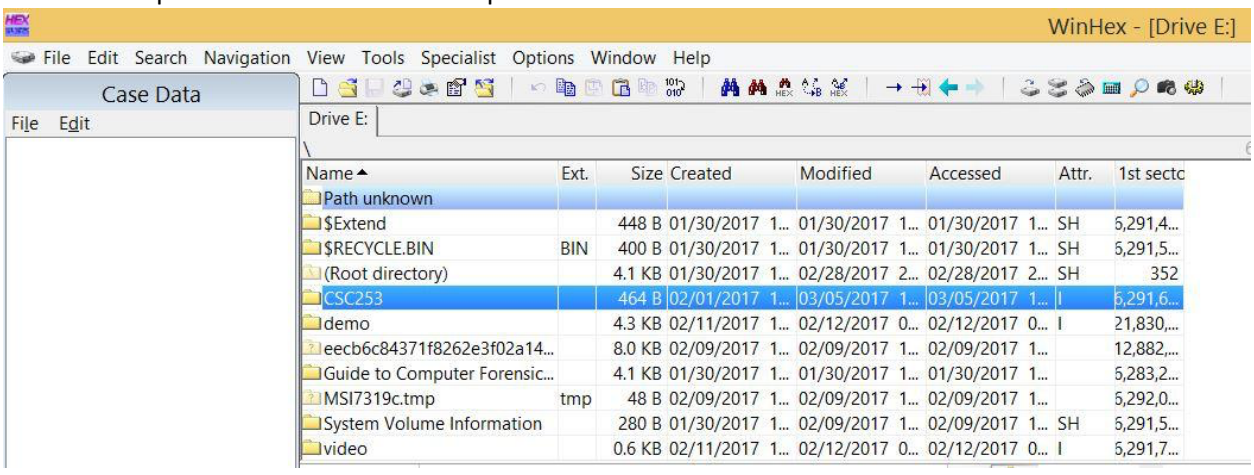
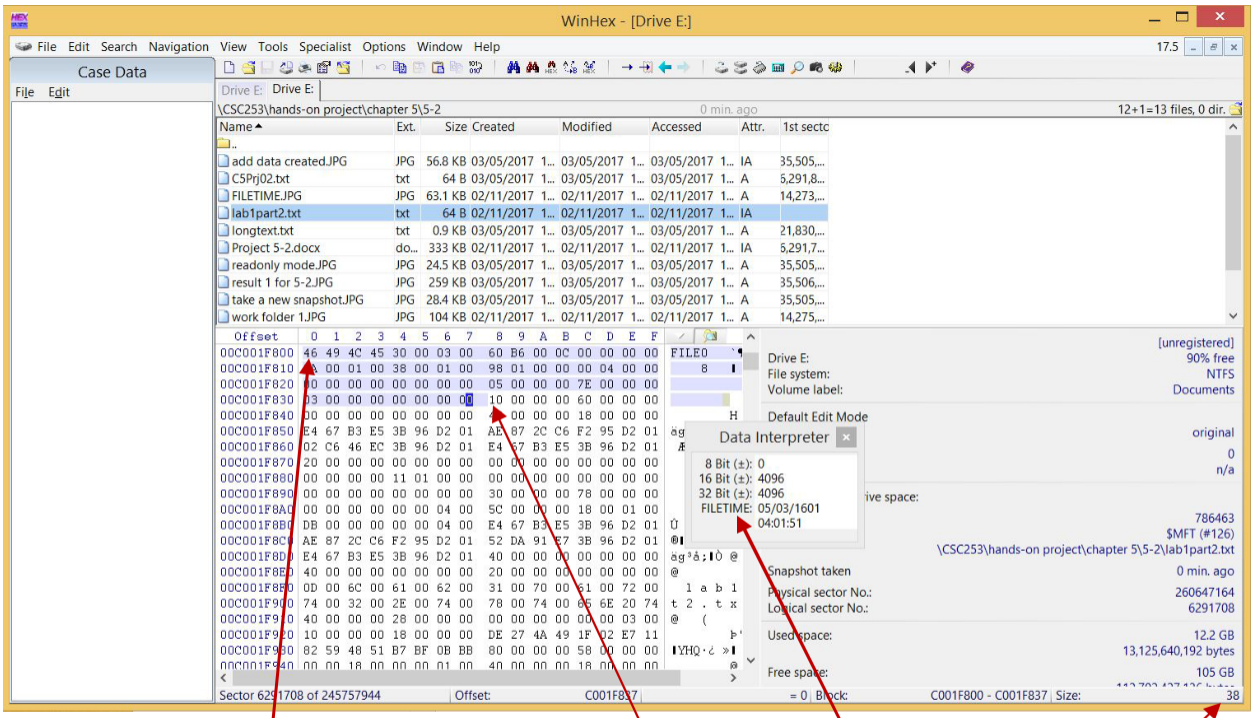


Figure 4

7. Click at the beginning of the record, on the letter F in FILE, and then drag down and to the right while you monitor the hexadecimal counter in the lower-right corner. For example, the start of attribute 0x10 is at offset 0x38 from the beginning of the MFT record. To find the start of attribute 0x10, drag the cursor until the counter reaches 38. When the counter reaches 38, release the mouse button.



You may find needed date and time from here Offset counter

Click here and drag down until the offset counter shows the number you want

After dragging, release mouse button and click here to interpret the data follows

Figure 5

8. Move the cursor one position to the next byte and then you may start to analyze attribute 0x10. Recall what we learned in class, the file's create date and time can be found at offset 0x18 to 0x1F from the beginning of attribute 0x10. Use similar method as in step 7 to find the file create date and time for lab1part2.txt.

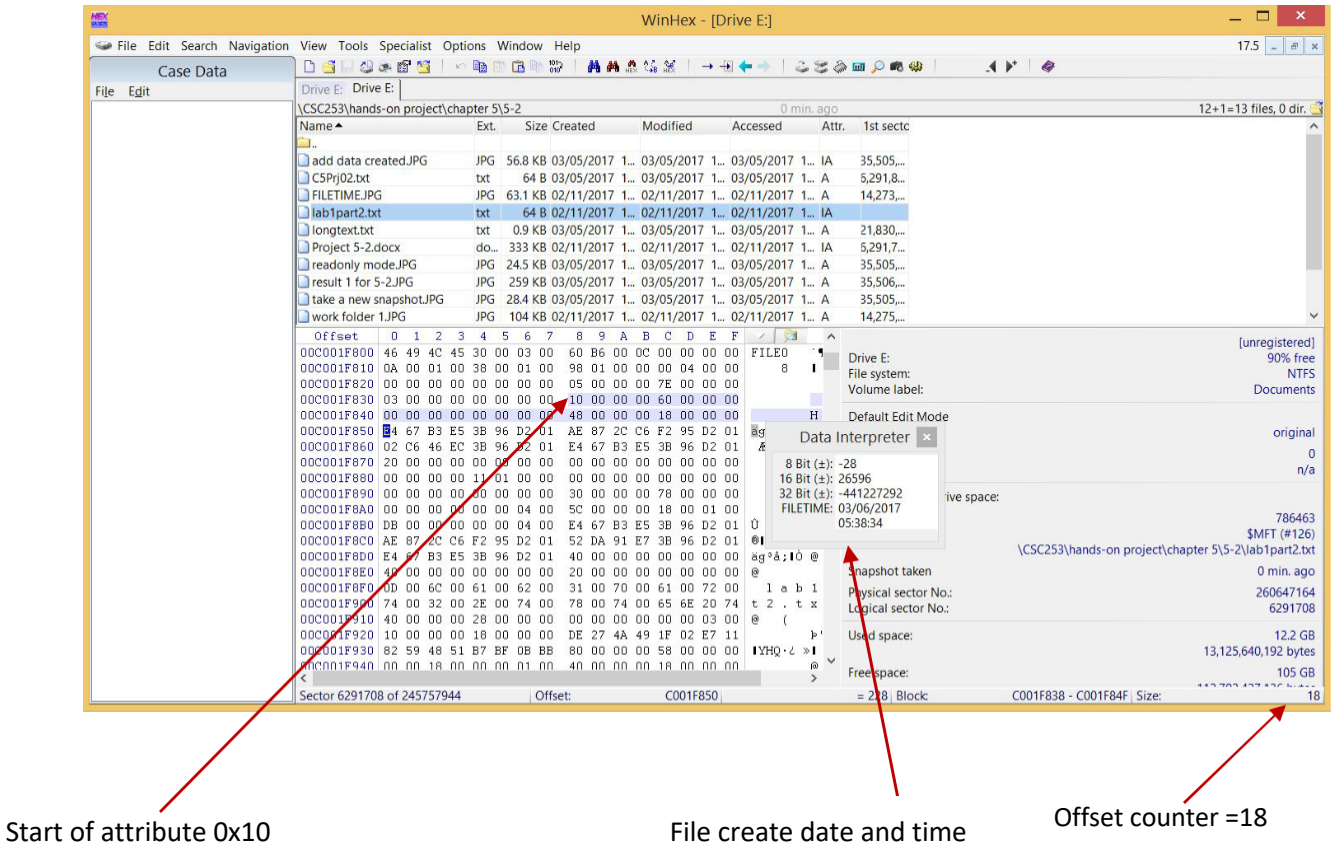
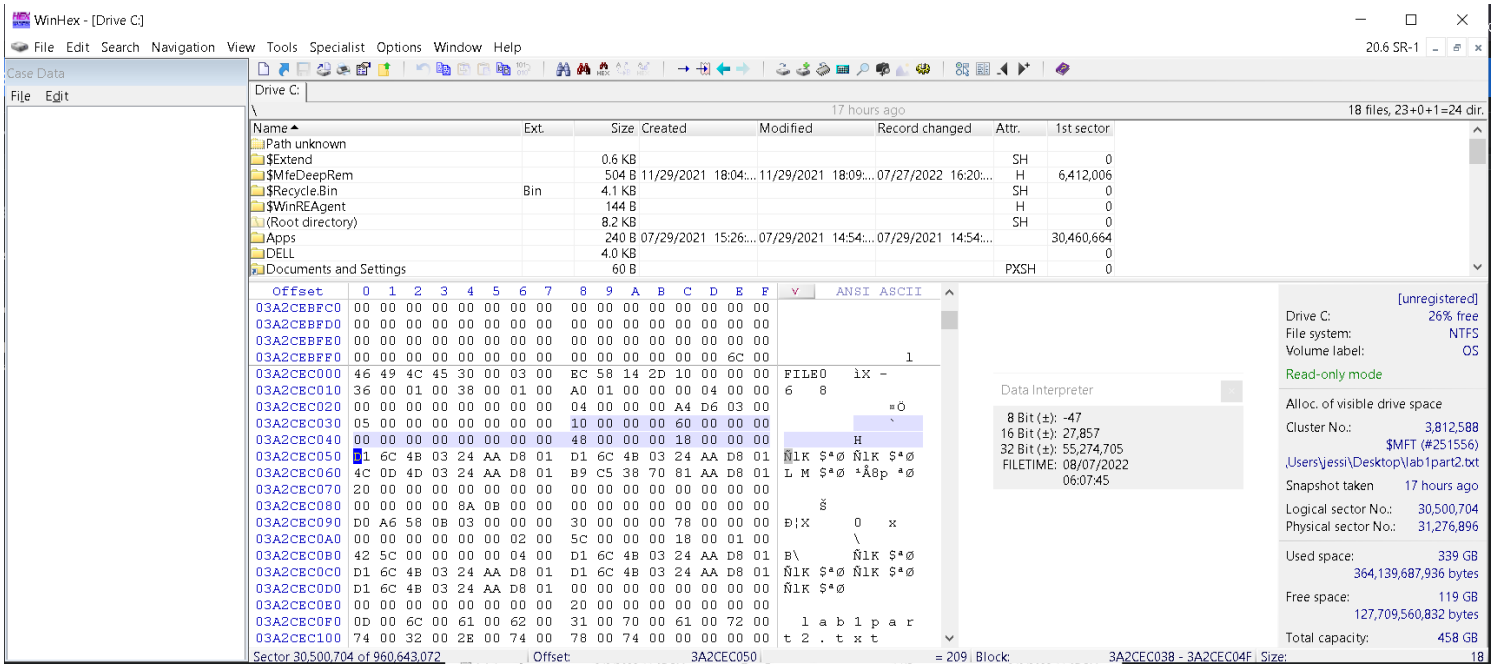


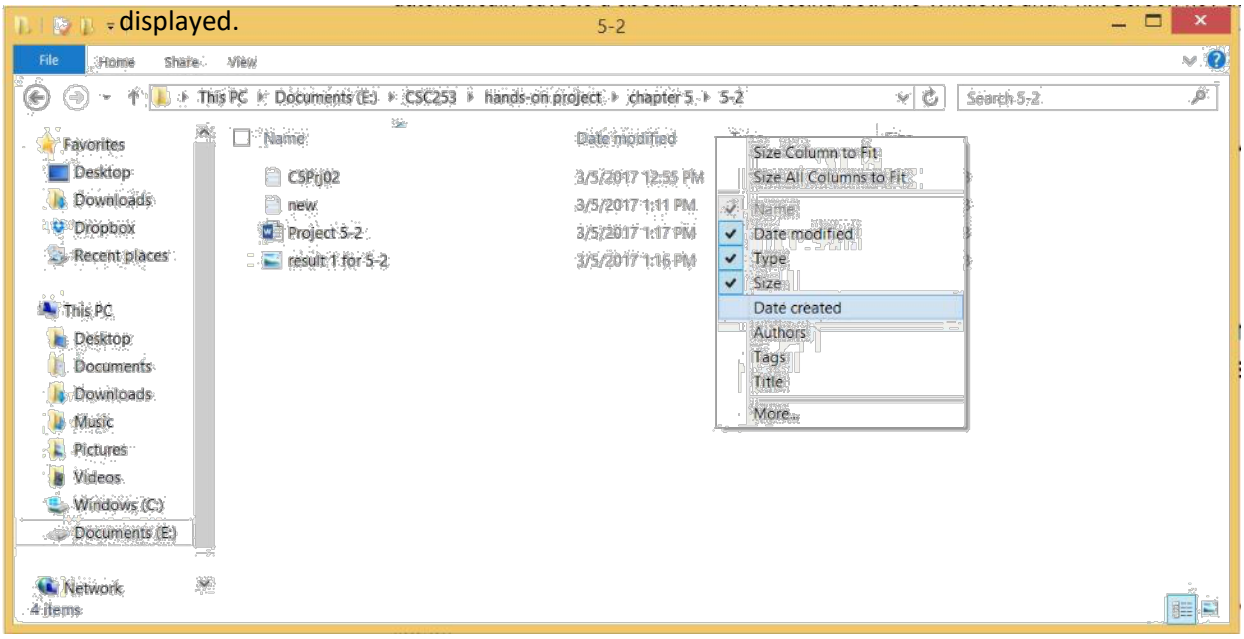
Figure 6

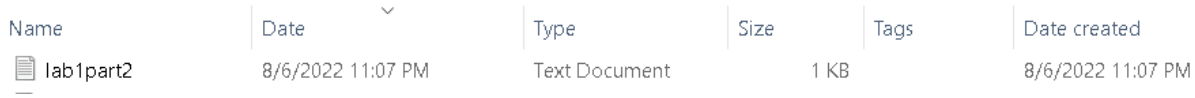
9. Repeat step 8 to analyze all attributes for file lab1part2.txt.
10. Now let's do further analysis:



11. When we look at offset 0x18 using the data interpreter, I can see that in this demonstration, file lab1part2. was created on 8/07/2022 at 6:07.

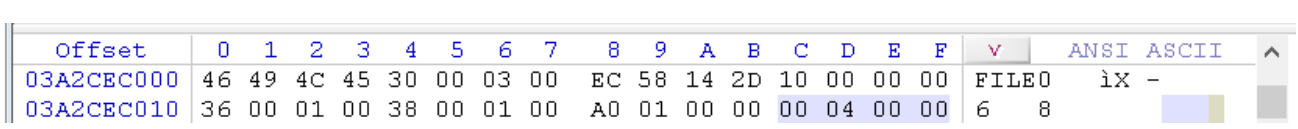
12. Using File Explorer and go to the folder where the lab1part2.txt located, right click on the arrow near “Size” or “Name”, and select the “Date created”. Now the “Date created” time is also displayed.



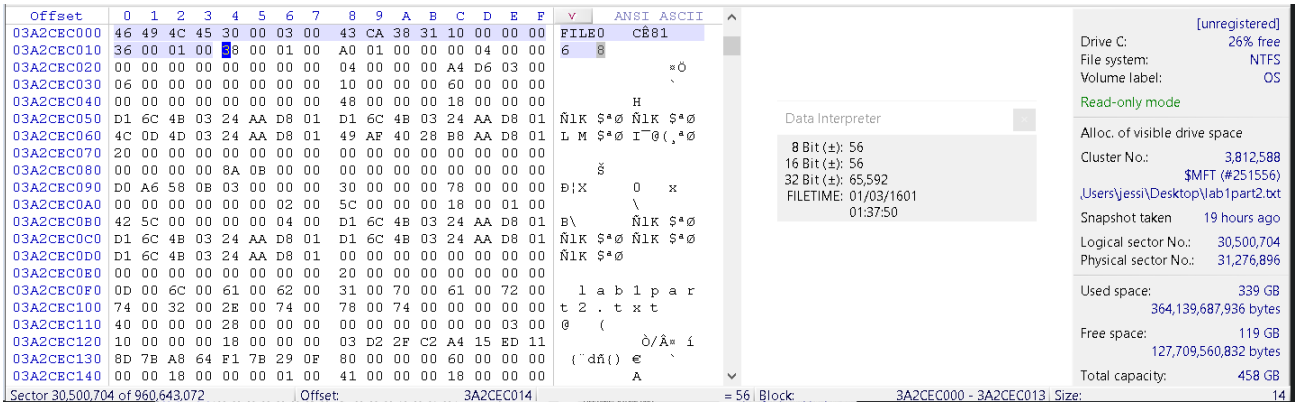


13. In this demonstration, our file was created on 11:07pm.

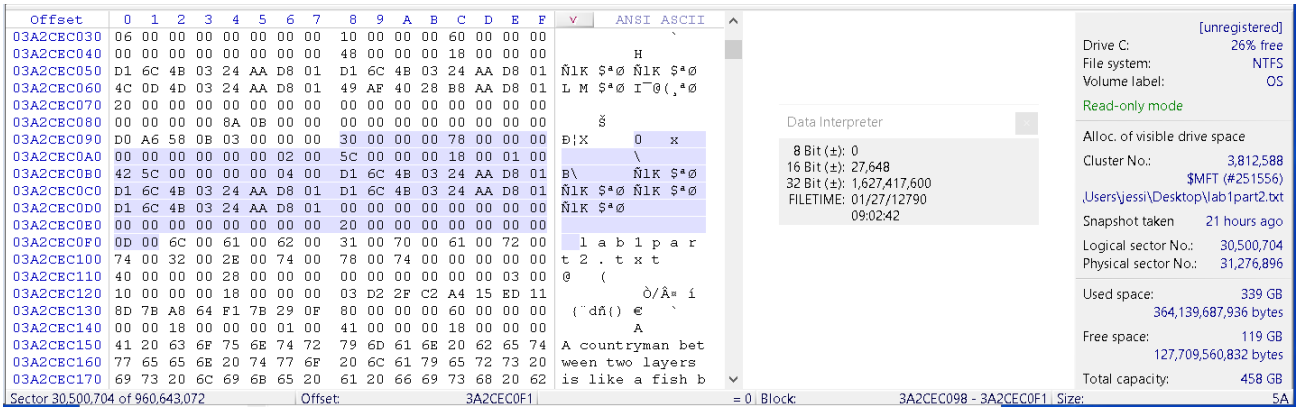
14. According to the WinHex documentation on https://documentation.help/WinHex-X-Ways/topic90.htm, WinHex and X-ways convert time into UTC time. When I look up lab1part2.txt’s created time in UTC time, I can see this is correct.



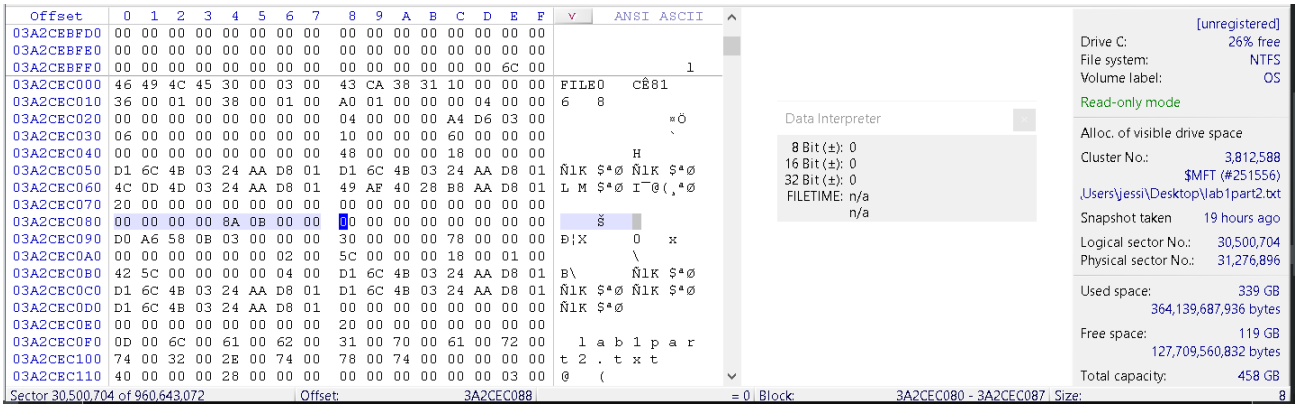
15. By looking at offset 0x1C to 0x1F, I can see the size of the MFT record. To convert it to big endian, we read it in reverse. Therefore, the size of the MFT record in big endian is 00 00 04 00.



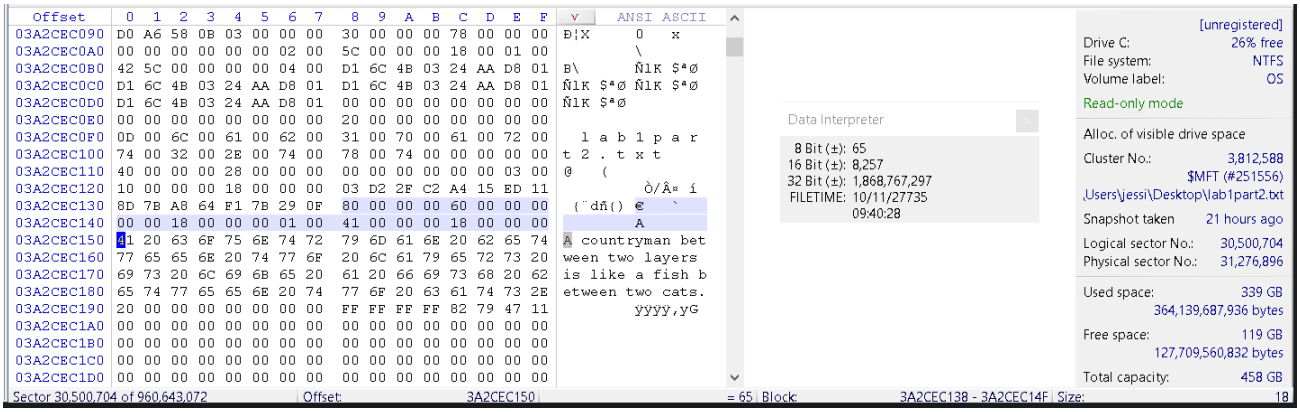
16. At offset 0x14 I can see the length of the header for the MFT record is 38.



17. Here at position 0x5A from the second 0x30 attribute I can see the file name is lab1part2.txt on the right.



18. Going to offset 0x08 from attribute 0x80 shows that this file is a resident file since it is set to 0x00.



19. I can find the data run at attribute 0x80. The start is at offset 0x18