CSU, College of Engineering and Computer Science
Department of Computer Science
CSC 153 – Computer Forensics Principles and Practice

Lab 3 Examining NTFS Disks

Objectives:

- Become familiar with the WinHex forensics tool.
- Use WinHex to explore the MFT and be able to analyze both resident and non-resident files.

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.

Part 1: Explore MFT of a file.

1. Create a text file named "forensicsclass.txt" and put it into your working directory.
2. In the file, type in "We will have a forensics class on Monday."
3. Append an alternate data stream to the file using command "echo". The hidden message is "If you study hard, then you are likely to succeed."
4. Display the hidden message using command "more".
5. Next, examine the metadata of the forensicsclass.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**.

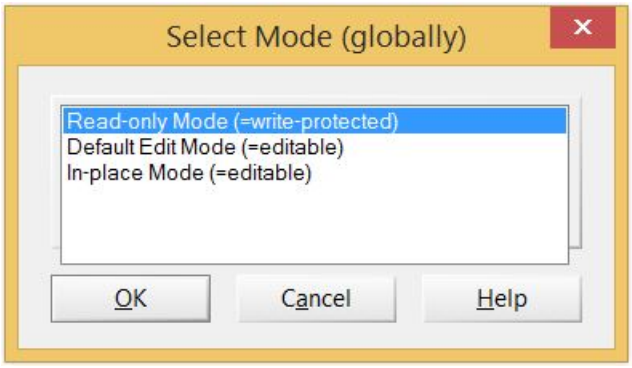


Figure 1

6. Click Tools, Open Disk from the menu. In the View Disk dialog box, click the drive where you saved forensicsclass.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.
7. 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.

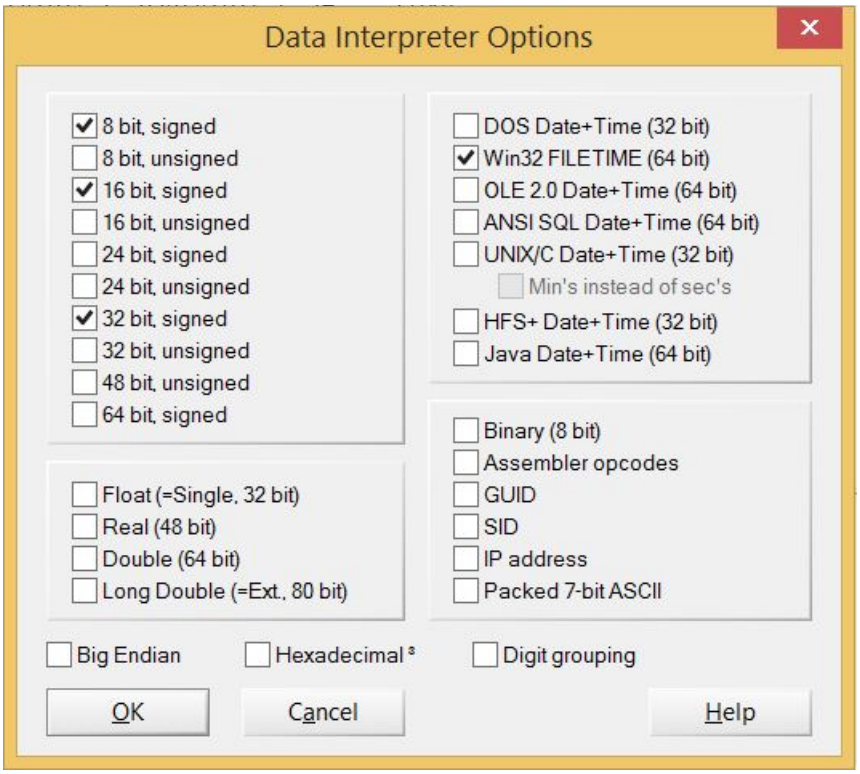


Figure 2

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

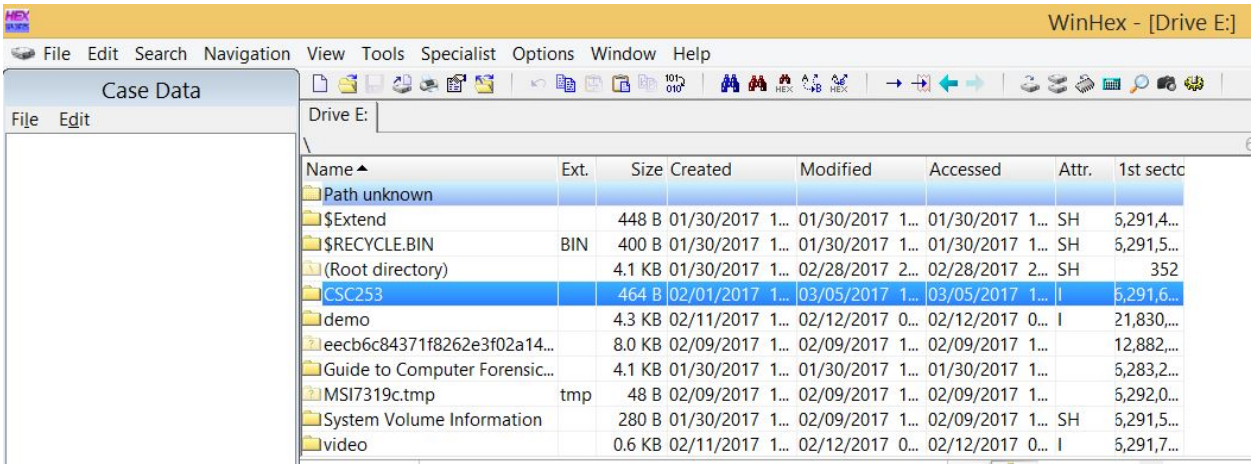


Figure 3

9. 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.

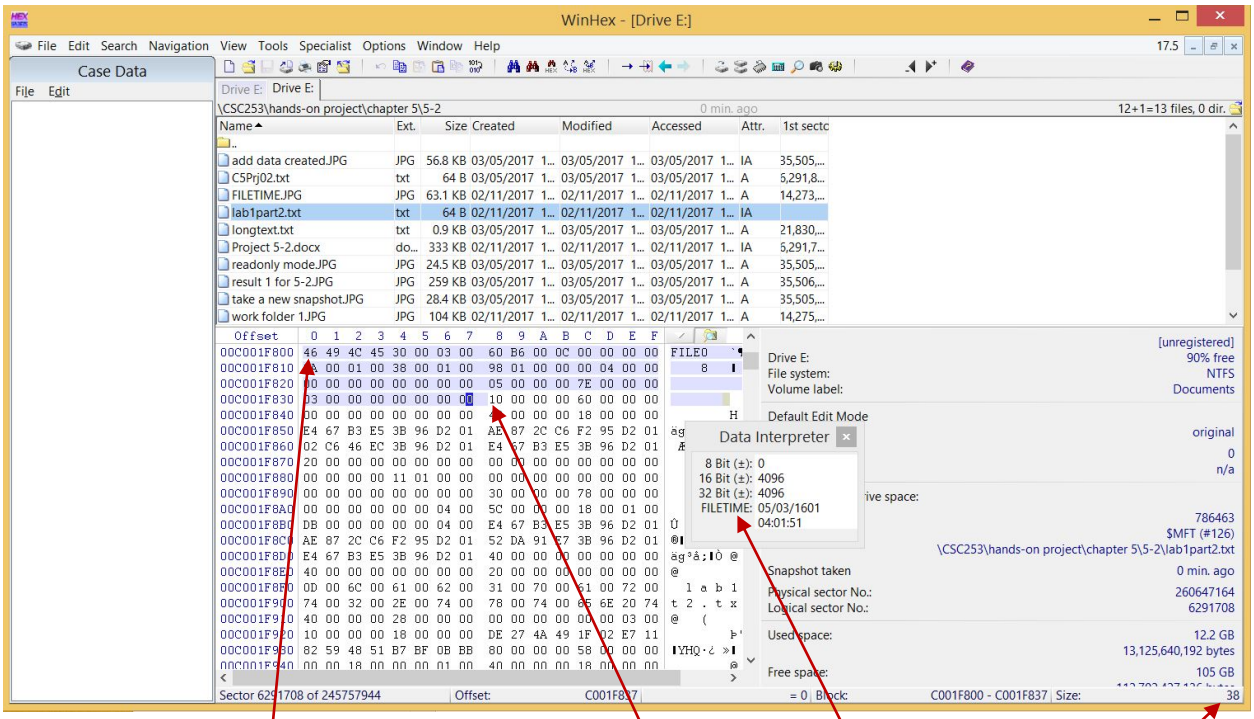


Figure 4

10. 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 forensicsclass.txt. Refer to your handout for the attribute details.

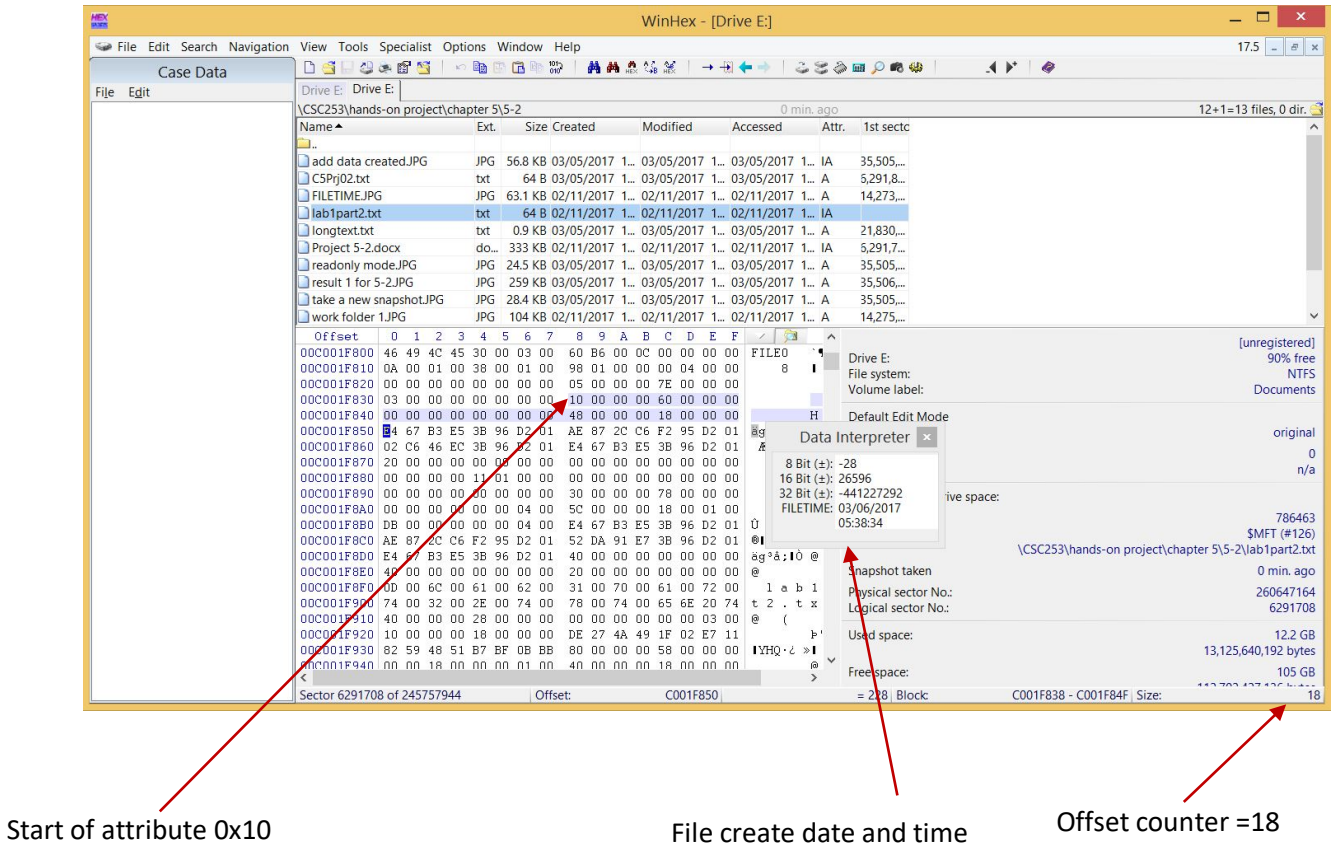


Figure 5

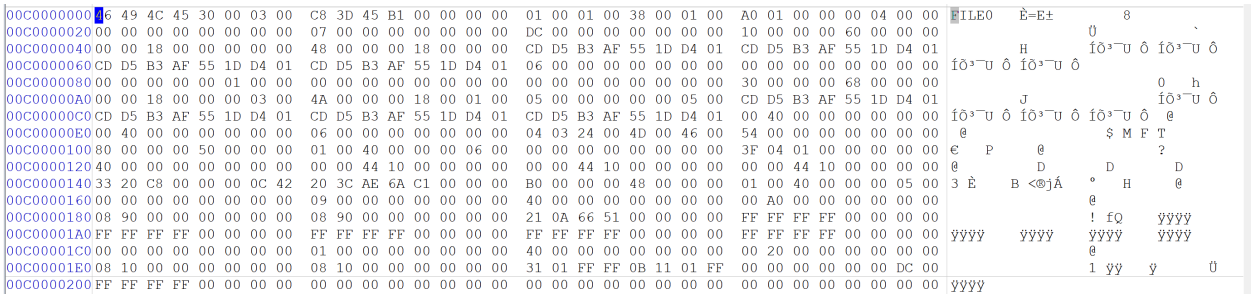
11. Repeat step 8 to analyze all attributes for file forensicsclass.txt and answer the following questions. Take screenshots to prove your answer for each question.

Questions for Part 1:

1. According to the data interpreter, what is the file create date and time for the file forensicsclass.txt? Take a screenshot to prove your answer.
2. What is the size of the MFT record?
3. What is the length of the header?
4. What is the file's last modified date and time?
5. How many 0x30 attributes does this file have? Why?
6. What is the name of this file?
7. Is this file a resident file or nonresident file? Where can you find the evidence?
8. Did you find the hidden message in the file when you check the MFT record? Take a screenshot to show the hidden message.
9. How many 0x80 attributes does this file have? What is the possible reason?

Part 2: Analyze a given MFT record.

Given the MFT record below, please answer the questions from 11-16.



```
00C0000000 46 49 4C 45 30 00 03 00  C8 3D 45 B1 00 00 00 00  01 00 01 00 38 00 01 00  A0 01 00 00 00 04 00 00  FILE0    È=E±        8
00C0000020 00 00 00 00 00 00 00 00  07 00 00 00 00 00 00 00  DC 00 00 00 00 00 00 00  10 00 00 00 60 00 00 00                  Ü           `
00C0000040 00 00 18 00 00 00 00 00  48 00 00 00 18 00 00 00  CD D5 B3 AF 55 1D D4 01  CD D5 B3 AF 55 1D D4 01          H       ÍÕ³¯U Ô ÍÕ³¯U Ô
00C0000060 CD D5 B3 AF 55 1D D4 01  CD D5 B3 AF 55 1D D4 01  06 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ÍÕ³¯U Ô ÍÕ³¯U Ô
00C0000080 00 00 00 00 00 01 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  30 00 00 00 68 00 00 00                          0   h
00C00000A0 00 00 18 00 00 00 03 00  4A 00 00 00 18 00 01 00  05 00 00 00 00 00 05 00  CD D5 B3 AF 55 1D D4 01          J               ÍÕ³¯U Ô
00C00000C0 CD D5 B3 AF 55 1D D4 01  CD D5 B3 AF 55 1D D4 01  CD D5 B3 AF 55 1D D4 01  00 40 00 00 00 00 00 00  ÍÕ³¯U Ô ÍÕ³¯U Ô ÍÕ³¯U Ô  @
00C00000E0 00 40 00 00 00 00 00 00  06 00 00 00 00 00 00 00  04 03 24 00 4D 00 46 00  54 00 00 00 00 00 00 00   @                  $ M F T
00C0000100 80 00 00 00 50 00 00 00  01 00 40 00 00 00 06 00  00 00 00 00 00 00 00 00  3F 04 01 00 00 00 00 00  €   P      @             ?
00C0000120 40 00 00 00 00 00 00 00  00 00 44 10 00 00 00 00  00 00 44 10 00 00 00 00  00 00 44 10 00 00 00 00  @         D       D       D
00C0000140 33 20 C8 00 00 00 0C 42  20 3C AE 6A C1 00 00 00  B0 00 00 00 48 00 00 00  01 00 40 00 00 00 05 00  3 È     B <®jÁ   °   H      @
00C0000160 00 00 00 00 00 00 00 00  09 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00  00 A0 00 00 00 00 00 00                  @
00C0000180 08 90 00 00 00 00 00 00  08 90 00 00 00 00 00 00  21 0A 66 51 00 00 00 00  FF FF FF FF 00 00 00 00                  ! fQ    ÿÿÿÿ
00C00001A0 FF FF FF FF 00 00 00 00  FF FF FF FF 00 00 00 00  FF FF FF FF 00 00 00 00  FF FF FF FF 00 00 00 00  ÿÿÿÿ    ÿÿÿÿ    ÿÿÿÿ    ÿÿÿÿ
00C00001C0 00 00 00 00 00 00 00 00  01 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00  00 20 00 00 00 00 00 00                  @
00C00001E0 08 10 00 00 00 00 00 00  08 10 00 00 00 00 00 00  31 01 FF FF 0B 11 01 FF  00 00 00 00 00 00 DC 00                  1 ÿÿ   ÿ      Ü
00C0000200 FF FF FF FF 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ÿÿÿÿ
```

Questions for Part 2:

10. Is this file a resident file or nonresident file? Where can you find the evidence?
11. How many data runs does this file have?
12. What is the starting cluster address value for the first data run (LCN)? You don't need to calculate the result if you provide a math expression.
13. How many clusters are assigned to the first data run?
14. Does this file have other data runs? If yes, what is the starting cluster address value for the second data run (LCN)? You don't need to calculate the result if you provide a math expression.
15. How many clusters are assigned to the second data run?

Deliverable:

16. You need to submit a lab report to Canvas. Your lab report should answer questions for both parts. Use a screenshot to prove your answer when necessary. Include necessary narrative and analysis to make your report clear. **All answers should be in big endian. You may provide Hexadecimal values directly.** The report will be evaluated based on the correctness, completeness, clarity and quality of English writing.