

## Module 2: Use Winhex to Examine NTFS Disks

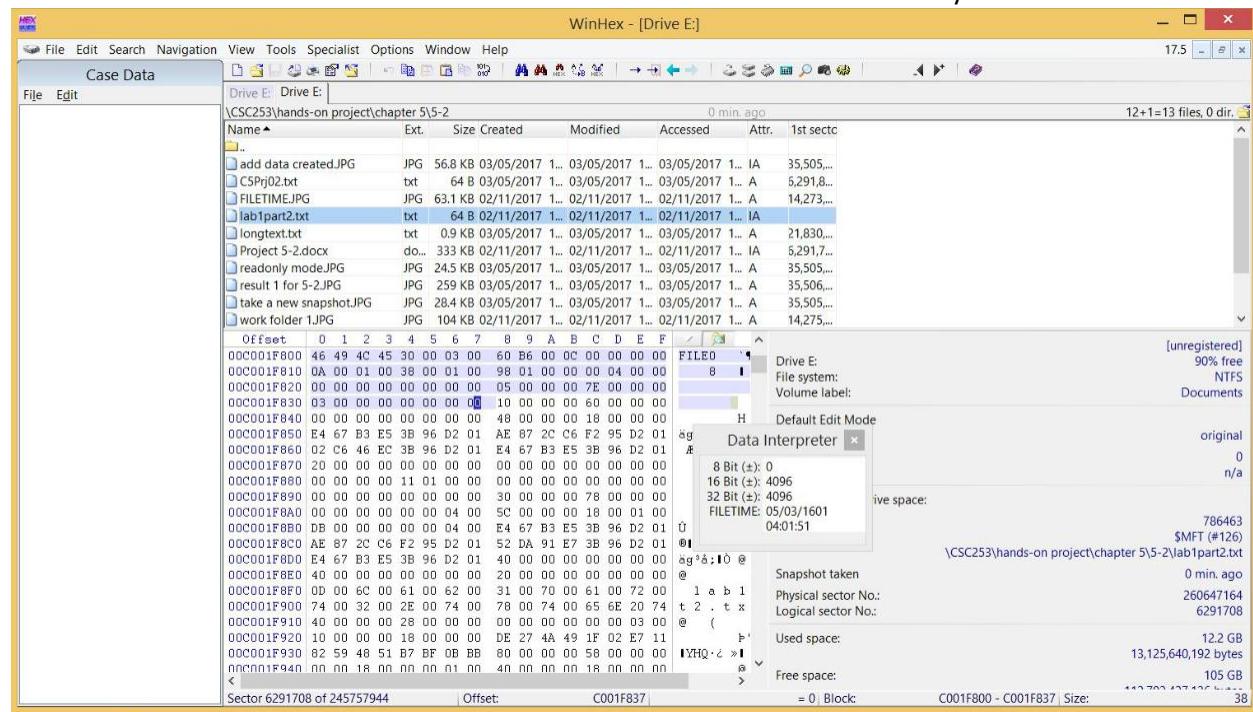
### Objectives:

- 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:

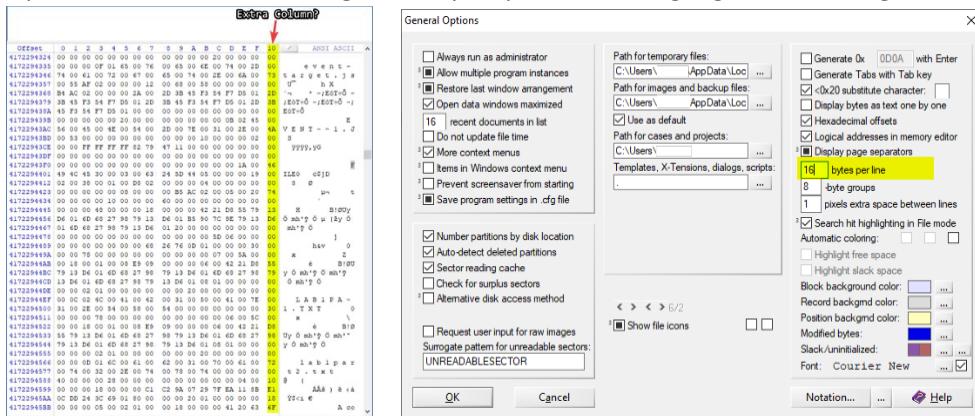
1. When you keep clicking on the offset data on the left column, it can switch between decimal and hexadecimal. Please make sure the data shown is hexadecimal for the analysis.



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.

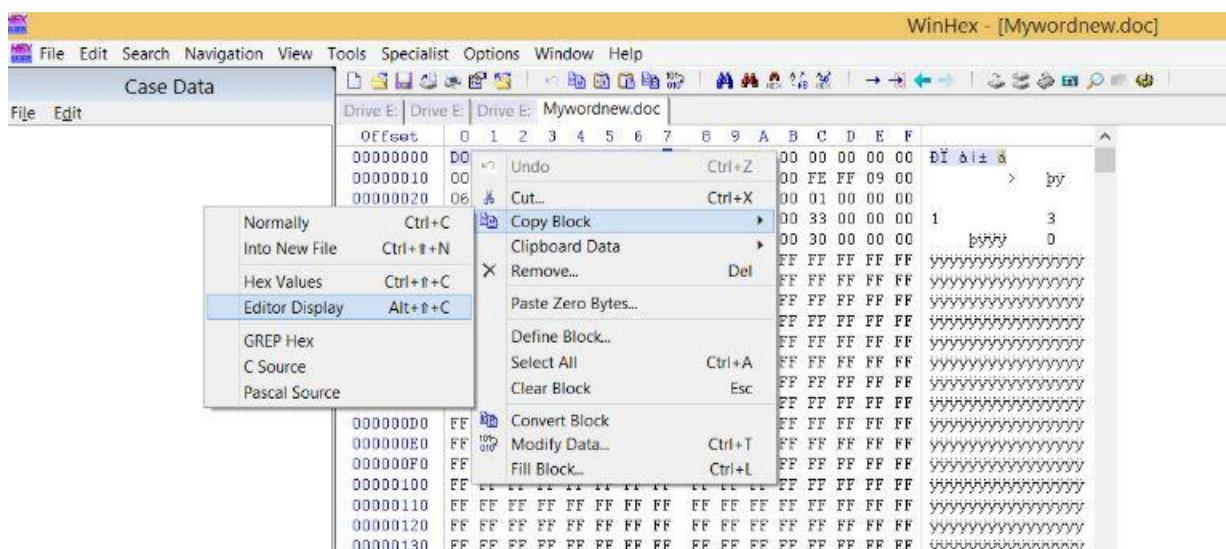


Figure 1

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.

```

headers - Notepad
File Edit Format View Help
DOC
Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F
00000000 D0 CF 11 E0 A1 B1 1A E1          ÐÏ à± á

XLS
Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F
00000000 D0 CF 11 E0 A1 B1 1A E1          ÐÏ à± á

DOCX
Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F
00000000 50 4B 03 04 14                      PK

XLSX
Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F
00000000 50 4B 03 04 14                      PK

JPG
Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F
00000000 FF D8 FF E0                      ýøÿà

PNG
Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F
00000000 89 50 4E 47 0D 0A 1A 0A          %PNG

```

**Observations:**

.doc and .xls have the same headers and have ÐÏ à± á. .docx and .xlsx have the same headers as well and they both have PK. I think this is because they are both from the same years. .doc and .xls are from 97-2003 while .docx and .xlsx are from 2007.

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 machine.**

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**.

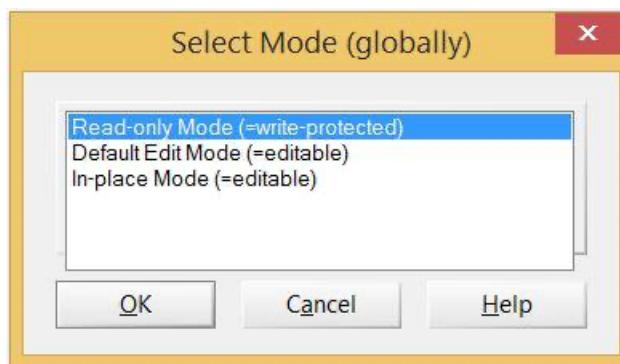


Figure 2

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.

- 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.

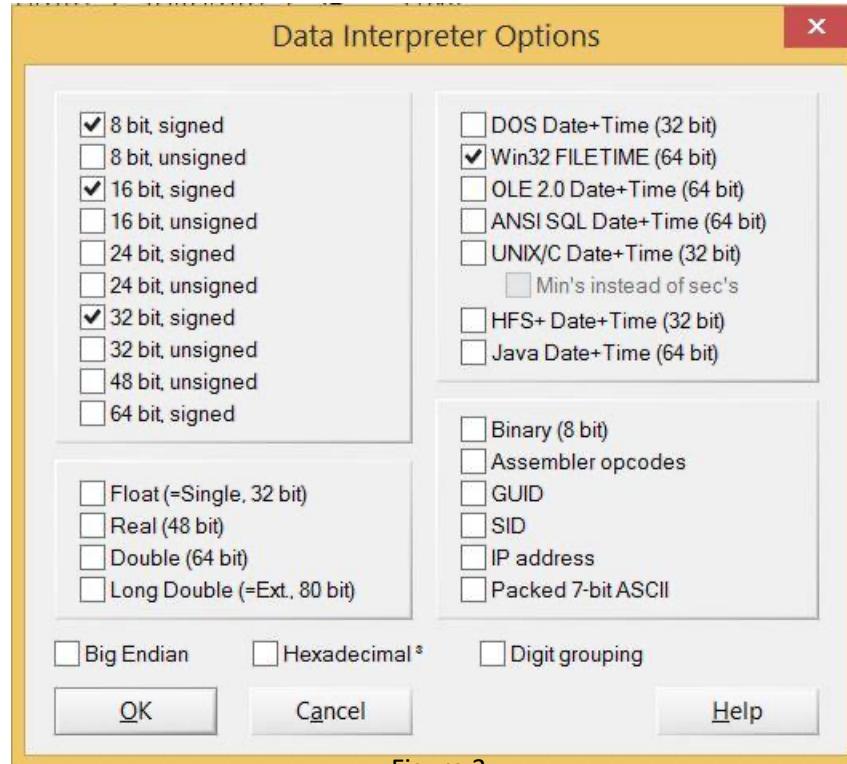


Figure 3

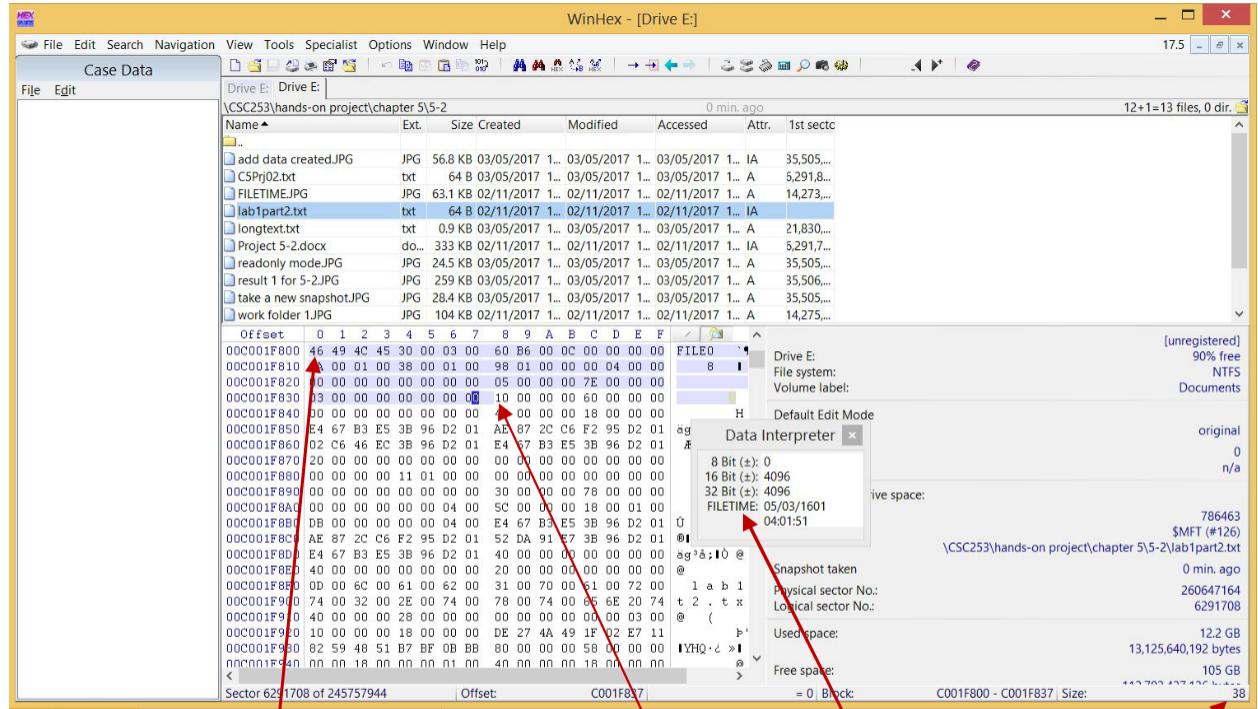
- Now you need to navigate to your work folder where you saved your lab1part2.txt in WinHex. In the upper-right pane of WinHex, scroll down until you see your work folder. Double-click each folder in the path and then click the lab1part2.txt file.

The screenshot shows the WinHex interface with the 'Case Data' pane open. The 'Drive E:' tab is selected in the navigation bar. The file list shows the following entries:

Name	Ext.	Size	Created	Modified	Accessed	Attr.	1st sect
Path unknown		448 B	01/30/2017 1...	01/30/2017 1...	01/30/2017 1...	SH	6,291,4...
\$Extend	BIN	400 B	01/30/2017 1...	01/30/2017 1...	01/30/2017 1...	SH	6,291,5...
(Root directory)		4.1 KB	01/30/2017 1...	02/28/2017 2...	02/28/2017 2...	SH	352
CSC253		464 B	02/01/2017 1...	03/05/2017 1...	03/05/2017 1...	I	6,291,6...
demo		4.3 KB	02/11/2017 1...	02/12/2017 0...	02/12/2017 0...	I	21,830,...
eeccb6c84371f8262e3f02a14...		8.0 KB	02/09/2017 1...	02/09/2017 1...	02/09/2017 1...		12,882,...
Guide to Computer Forensic...		4.1 KB	01/30/2017 1...	01/30/2017 1...	01/30/2017 1...		5,283,2...
MSI7319c.tmp	tmp	48 B	02/09/2017 1...	02/09/2017 1...	02/09/2017 1...		5,292,0...
System Volume Information		280 B	01/30/2017 1...	02/09/2017 1...	02/09/2017 1...	SH	6,291,5...
video		0.6 KB	02/11/2017 1...	02/12/2017 0...	02/12/2017 0...	I	6,291,7...

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

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

needed date and time from here Offset counter

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.

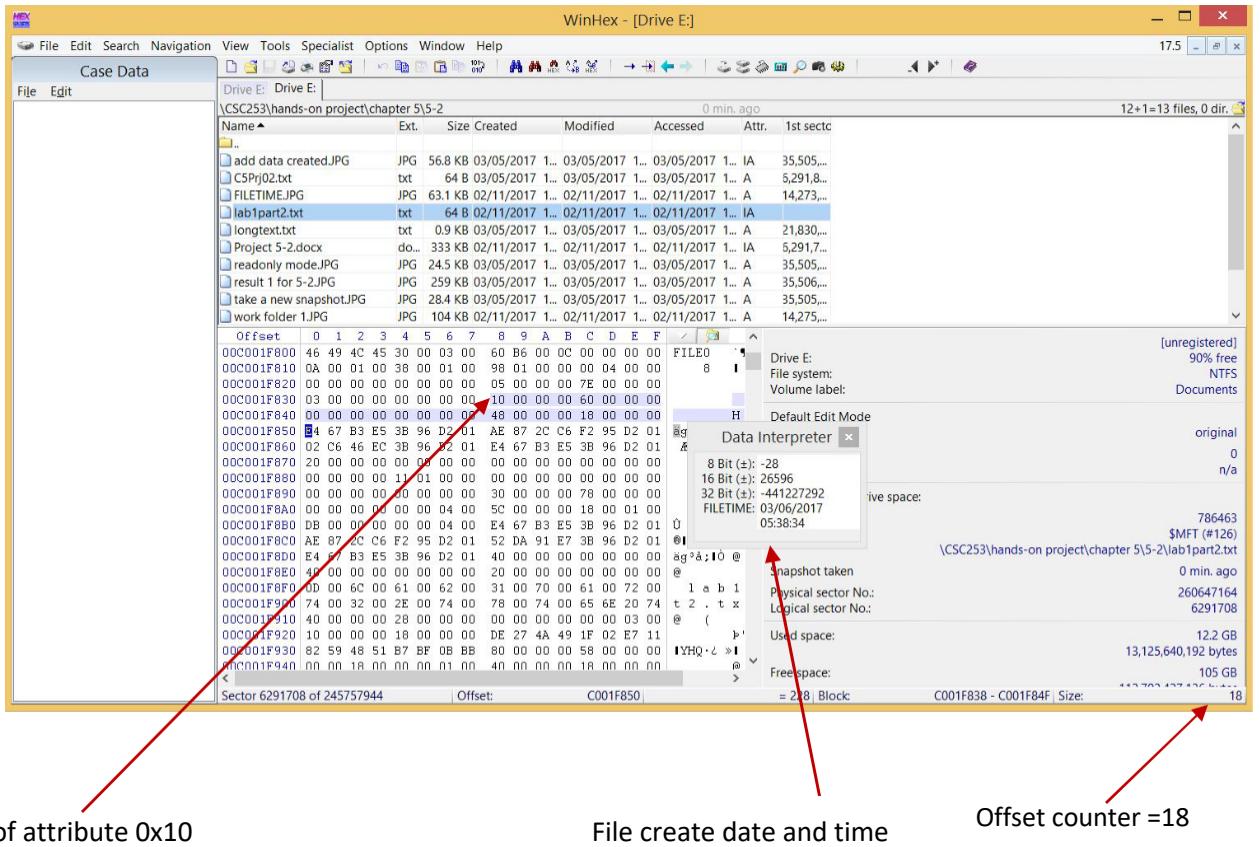
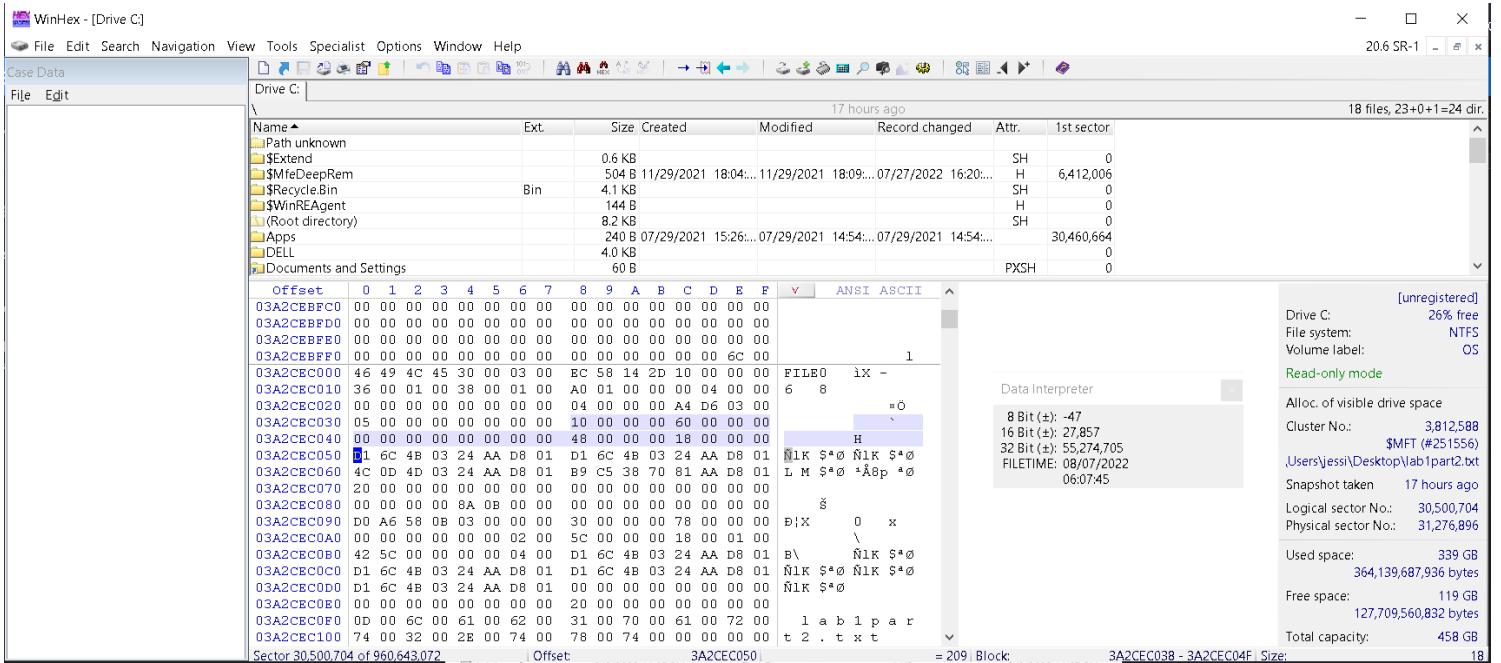


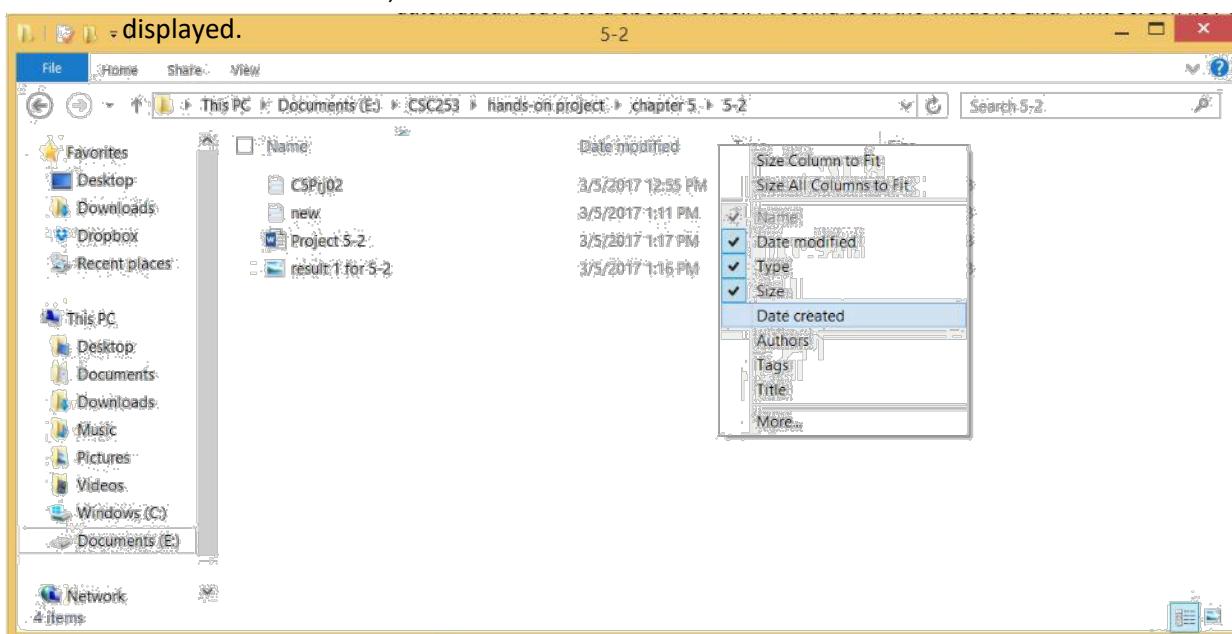
Figure 6

9. Repeat step 8 to analyze all attributes for file lab1part2.txt.

10. Now let's do further analysis:



- 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.
- 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.



Name	Date	Type	Size	Tags	Date created
lab1part2	8/6/2022 11:07 PM	Text Document	1 KB		8/6/2022 11:07 PM

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

11:07 AM Saturday, Pacific Time (PT) is  
6:07 PM Saturday, Coordinated Universal Time (UTC)

- 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.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	V	ANSI	ASCII
03A2CEC000	46	49	4C	45	30	00	03	00	EC	58	14	2D	10	00	00	00	FILE0	iX -	
03A2CEC010	36	00	01	00	38	00	01	00	A0	01	00	00	00	04	00	00	6	8	

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.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	V	ANSI	ASCII
03A2CEC000	46	49	4C	45	30	00	03	00	43	CA	38	31	10	00	00	00	FILED	CÊ81	
03A2CEC010	36	00	01	00	08	00	01	00	A0	01	00	00	00	04	00	00	6	8	
03A2CEC020	00	00	00	00	00	00	00	00	04	00	00	00	A4	D6	03	00		Ó	
03A2CEC030	06	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00		H	
03A2CEC040	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00			
03A2CEC050	D1	6C	4B	03	24	AA	D8	01	D1	6C	4B	03	24	AA	D8	01	ÑlK	ÑlK	ÑlK
03A2CEC060	4C	0D	4D	03	24	AA	D8	01	49	AF	40	28	B8	AA	D8	01	L	M	ÑlK
03A2CEC070	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	8		
03A2CEC080	00	00	00	00	08	A8	OB	00	00	00	00	00	00	00	00	00			
03A2CEC090	D0	A6	58	OB	03	24	AA	D8	01	30	00	00	78	00	00	00			
03A2CEC0A0	00	00	00	00	00	02	00	00	5C	00	00	18	00	01	00	00			
03A2CEC0B0	42	5C	00	00	00	00	04	00	D1	6C	4B	03	24	AA	D8	01	ÑlK	ÑlK	ÑlK
03A2CEC0C0	D1	6C	4B	03	24	AA	D8	01	D1	6C	4B	03	24	AA	D8	01	ÑlK	ÑlK	ÑlK
03A2CEC0D0	00	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00			
03A2CEC0E0	00	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00			
03A2CEC0F0	D0	00	6C	00	61	00	62	00	31	00	70	00	61	00	72	00	1	a	b
03A2CEC100	74	00	32	00	28	00	74	00	78	00	74	00	00	t	2	.	t	x	t
03A2CEC110	40	00	00	00	28	00	00	00	00	00	00	00	00	03	00	00	Ø	(	)
03A2CEC120	10	00	00	00	18	00	00	00	03	D2	2F	C2	A4	15	ED	11	ò/Àí		
03A2CEC130	8D	7B	A8	64	F1	7B	29	0F	80	00	00	00	60	00	00	00			
03A2CEC140	00	00	18	00	00	00	01	00	41	00	00	00	18	00	00	00			
03A2CEC150	41	20	63	6F	75	6E	74	72	79	6D	61	6E	20	62	65	74	A	countryman	bet
03A2CEC160	77	65	65	6E	20	74	77	6F	20	6C	61	79	65	72	73	20			
03A2CEC170	69	73	20	6C	69	6B	65	20	61	20	66	69	73	68	20	62			
Sector 30,500,704 of 960,643,072																			
Offset:																			
3A2CEC014																			

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

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	V	ANSI	ASCII
03A2CEC030	06	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00			
03A2CEC040	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00			
03A2CEC050	D1	6C	4B	03	24	AA	D8	01	D1	6C	4B	03	24	AA	D8	01	ÑlK	ÑlK	ÑlK
03A2CEC060	4C	0D	4D	03	24	AA	D8	01	49	AF	40	28	B8	AA	D8	01	L	M	ÑlK
03A2CEC070	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
03A2CEC080	00	00	00	00	08	A8	OB	00	00	00	00	00	00	00	00	00			
03A2CEC090	D0	A6	58	OB	03	24	AA	D8	01	30	00	00	78	00	00	00			
03A2CEC0A0	00	00	00	00	00	02	00	00	5C	00	00	18	00	01	00	00			
03A2CEC0B0	42	5C	00	00	00	00	04	00	D1	6C	4B	03	24	AA	D8	01	ÑlK	ÑlK	ÑlK
03A2CEC0C0	D1	6C	4B	03	24	AA	D8	01	D1	6C	4B	03	24	AA	D8	01	ÑlK	ÑlK	ÑlK
03A2CEC0D0	00	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00			
03A2CEC0E0	00	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00			
03A2CEC0F0	D0	00	6C	00	61	00	62	00	31	00	70	00	61	00	72	00	1	a	b
03A2CEC100	74	00	32	00	28	00	74	00	78	00	74	00	00	t	2	.	t	x	t
03A2CEC110	40	00	00	00	28	00	00	00	00	00	00	00	00	03	00	00	Ø	(	)
03A2CEC120	10	00	00	00	18	00	00	00	03	D2	2F	C2	A4	15	ED	11	ò/Àí		
03A2CEC130	8D	7B	A8	64	F1	7B	29	0F	80	00	00	00	60	00	00	00			
03A2CEC140	00	00	18	00	00	00	01	00	41	00	00	00	18	00	00	00			
03A2CEC150	41	20	63	6F	75	6E	74	72	79	6D	61	6E	20	62	65	74	A	countryman	bet
03A2CEC160	77	65	65	6E	20	74	77	6F	20	6C	61	79	65	72	73	20			
03A2CEC170	69	73	20	6C	69	6B	65	20	61	20	66	69	73	68	20	62			
Sector 30,500,704 of 960,643,072																			
Offset:																			
3A2CEC011																			

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

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	V	ANSI	ASCII
03A2CEBF00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
03A2CEBF00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
03A2CEBF00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
03A2CEC000	46	49	4C	45	30	00	03	00	43	CA	38	31	10	00	00	00	FILED	CÊ81	
03A2CEC010	36	00	01	00	38	00	01	00	A0	01	00	00	04	00	00	00	6	8	
03A2CEC020	00	00	00	00	00	00	00	00	04	00	00	00	A4	D6	03	00		Ó	
03A2CEC030	06	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00		H	
03A2CEC040	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00			
03A2CEC050	D1	6C	4B	03	24	AA	D8	01	D1	6C	4B	03	24	AA	D8	01	ÑlK	ÑlK	ÑlK
03A2CEC060	4C	0D	4D	03	24	AA	D8	01	49	AF	40	28	B8	AA	D8	01	L	M	ÑlK
03A2CEC070	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
03A2CEC080	00	00	00	00	08	A8	OB	00	00	00	00	00	00	00	00	00			
03A2CEC090	D0	A6	58	OB	03	24	AA	D8	01	30	00	00	78	00	00	00			
03A2CEC0A0	00	00	00	00	00	02	00	00	5C	00	00	18	00	01	00	00			
03A2CEC0B0	42	5C	00	00	00	00	04	00	D1	6C	4B	03	24	AA	D8	01	ÑlK	ÑlK	ÑlK
03A2CEC0C0	D1	6C	4B	03	24	AA	D8	01	D1	6C	4B	03							

Drive C: [unregistered] 26% free  
File system: NTFS  
Volume label: OS  
Read-only mode  
Alloc. of visible drive space  
Cluster No.: 3,812,588  
\$MFT (#251556)  
.Users\jessi\Desktop\lab1part2.txt  
Snapshot taken 21 hours ago  
Logical sector No.: 30,500,704  
Physical sector No.: 31,276,896  
Used space: 339 GB  
364,139,687,936 bytes  
Free space: 119 GB  
127,709,560,832 bytes  
Total capacity: 458 GB

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	V	ANSI	ASCII
03A2CEC090	D0	A6	58	0B	03	00	00	00	30	00	00	00	78	00	00	00	Đ!X	0	x
03A2CEC0A0	00	00	00	00	00	00	02	00	5C	00	00	00	18	00	01	00	\		
03A2CEC0B0	42	5C	00	00	00	00	04	00	D1	6C	4B	03	24	AA	D8	01	Đ\	Đ!K	Đ*Đ
03A2CEC0C0	D1	6C	4B	03	24	AA	D8	01	D1	6C	4B	03	24	AA	D8	01	Đ!K	Đ*Đ	Đ!K
03A2CEC0D0	D1	6C	4B	03	24	AA	D8	01	00	00	00	00	00	00	00	00	Đ!K	Đ*Đ	
03A2CEC0E0	00	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00			
03A2CEC0F0	0D	00	6C	00	61	00	62	00	31	00	70	00	61	00	72	00	l a b l p a r		
03A2CEC100	74	00	32	00	28	00	74	00	78	00	74	00	00	00	00	00	t 2 . t x t		
03A2CEC110	40	00	00	00	28	00	00	00	00	00	00	00	00	00	03	00	Đ	(	)
03A2CEC120	10	00	00	00	18	00	00	00	03	D2	2F	C2	A4	15	ED	11	đ/À= í		
03A2CEC130	8D	7B	A8	64	F1	7B	29	0F	80	00	00	00	60	00	00	00	(`df() e ^		
03A2CEC140	00	00	18	00	00	00	01	00	41	00	00	00	18	00	00	00	A		
03A2CEC150	Đ1	20	63	6F	75	6E	74	72	79	6D	61	6E	20	62	65	74	Đ countrymen between two layers		
03A2CEC160	77	65	65	6E	20	74	77	6E	20	6C	61	79	65	72	73	20	is like a fish between two cats.		
03A2CEC170	69	73	20	6C	69	6B	65	20	61	20	66	69	73	68	20	62			
03A2CEC180	65	74	77	65	65	6E	20	74	77	6F	20	63	61	74	73	2E			
03A2CEC190	20	00	00	00	00	00	00	00	FF	FF	FF	82	79	47	11		YYYY, YG		
03A2CEC1A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
03A2CEC1B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
03A2CEC1C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
03A2CEC1D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			

Sector 30,500,704 of 960,643,072 | Offset: 3A2CEC150 | = 65 Block: 3A2CEC138 - 3A2CEC14F | Size: 18

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

