CSC153: Activity 5: Use Winhex to Examine NTFS Disks

Ryan Kozak

SACRAMENTO
STATE

2019-11-02

Objectives

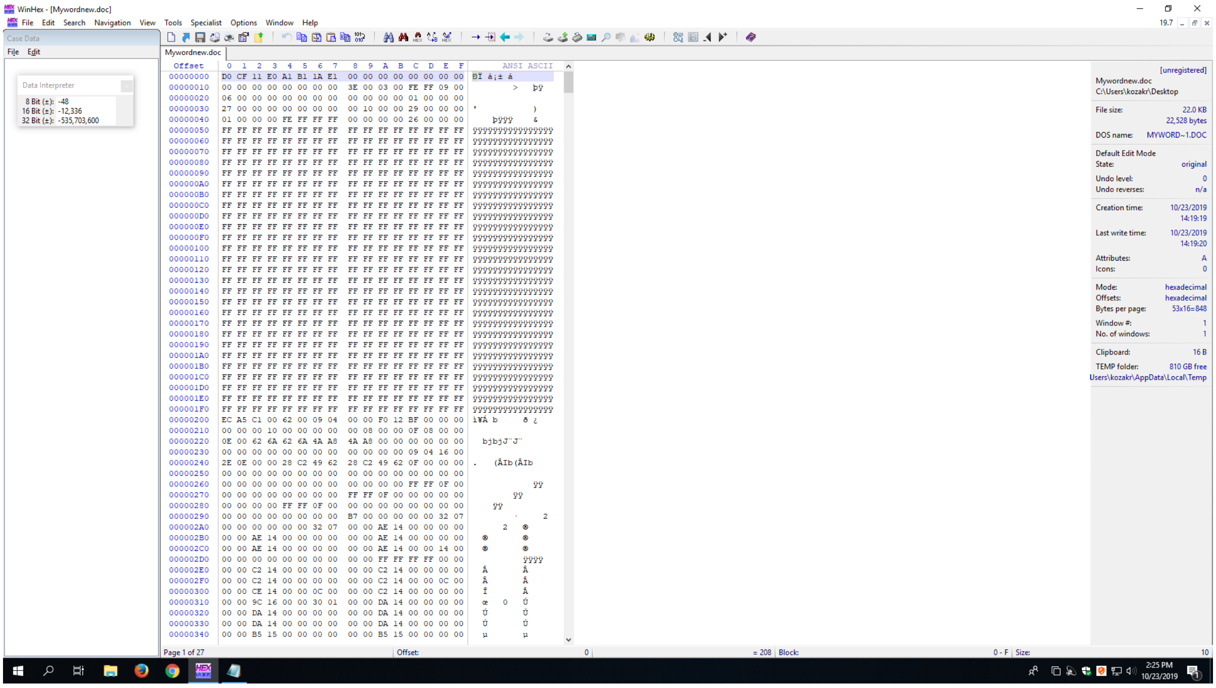
- Become familiar with the WinHex forensics tool.
- Use WinHex to become familiar with different file types.
- Use WinHex to explore and become familiar with the MFT, including headers and attributes.

Part 1: Explore different file types

First we use Microsoft Word to create a new document named `Mywordnew.doc`, containing text `This is a test`. Then we open WinHex, navigate to the directory where our `.doc` file was saved, and open it. Lastly, we copy the file hexadecimal header `D0 CF 11 E0 A1 B1 1A E1` to a new text document.

Hexadecimal header for `.doc` file.

```
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  00 00 00 00 00 00 00 00 ⊠⊠⊠⊠
```



WinHex - [Mywordnew.doc]

Data Interpreter
8 Bit (±): -48
16 Bit (±): -12,336
32 Bit (±): -535,703,600

```
Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
00000000   D0 CF 11 E0 A1 B1 1A E1  00 00 00 00 00 00 00 00  ÐÏ à¡± á
00000010   00 00 00 00 00 00 00 00  3E 00 03 00 FE FF 09 00          >   þÿ
00000020   06 00 00 00 00 00 00 00  00 00 00 00 01 00 00 00
00000030   27 00 00 00 00 00 00 00  00 10 00 00 29 00 00 00  '           )
00000040   01 00 00 00 FE FF FF FF  00 00 00 00 26 00 00 00      þÿÿÿ    &
00000050   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000060   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000070   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000080   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000090   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000000A0   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000000B0   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000000C0   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000000D0   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000000E0   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000000F0   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000100   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000110   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000120   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000130   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000140   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000150   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000160   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000170   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000180   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000190   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000001A0   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000001B0   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000001C0   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000001D0   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000001E0   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000001F0   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000200   EC A5 C1 00 62 00 09 04  00 00 F0 12 BF 00 00 00  ì¥Á b     ð ¿
00000210   00 00 00 10 00 00 00 00  00 08 00 00 0F 08 00 00
00000220   0E 00 62 6A 62 6A 4A A8  4A A8 00 00 00 00 00 00    bjbjJ¨J¨
00000230   00 00 00 00 00 00 00 00  00 00 00 00 09 04 16 00
00000240   2E 0E 00 00 28 C2 49 62  28 C2 49 62 0F 00 00 00  .   (ÂIb(ÂIb
00000250   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000260   00 00 00 00 00 00 00 00  00 00 00 00 FF FF 0F 00              ÿÿ
00000270   00 00 00 00 00 00 00 00  FF FF 0F 00 00 00 00 00          ÿÿ
00000280   00 00 00 00 FF FF 0F 00  00 00 00 00 00 00 00 00      ÿÿ
00000290   00 00 00 00 00 00 00 00  B7 00 00 00 00 00 32 07          ·     2
000002A0   00 00 00 00 00 00 32 07  00 00 AE 14 00 00 00 00        2   ®
000002B0   00 00 AE 14 00 00 00 00  00 00 AE 14 00 00 00 00    ®       ®
000002C0   00 00 AE 14 00 00 00 00  00 00 AE 14 00 00 14 00    ®       ®
000002D0   00 00 00 00 00 00 00 00  00 00 FF FF FF FF 00 00            ÿÿÿÿ
000002E0   00 00 C2 14 00 00 00 00  00 00 C2 14 00 00 00 00    Â       Â
000002F0   00 00 C2 14 00 00 00 00  00 00 C2 14 00 00 0C 00    Â       Â
00000300   00 00 CE 14 00 00 0C 00  00 00 C2 14 00 00 00 00    Î       Â
00000310   00 00 9C 16 00 00 30 01  00 00 DA 14 00 00 00 00    œ   0   Ú
00000320   00 00 DA 14 00 00 00 00  00 00 DA 14 00 00 00 00    Ú       Ú
00000330   00 00 DA 14 00 00 00 00  00 00 DA 14 00 00 00 00    Ú       Ú
00000340   00 00 B5 15 00 00 00 00  00 00 B5 15 00 00 00 00    µ       µ
```

[unregistered]
Mywordnew.doc
C:\Users\kozakr\Desktop

File size: 22.0 KB
22,528 bytes
DOS name: MYWORD~1.DOC

Default Edit Mode
State: original
Undo level: 0
Undo reverses: n/a

Creation time: 10/23/2019 14:19:19
Last write time: 10/23/2019 14:19:20

Attributes: A
Icons: 0

Mode: hexadecimal
Offsets: hexadecimal
Bytes per page: 53x16=848
Window #: 1
No. of windows: 1

Clipboard: 16 B
TEMP folder: 810 GB free
Users\kozakr\AppData\Local\Temp

Page 1 of 27 | Offset: 0 | = 208 Block: | 0 - F Size: 10

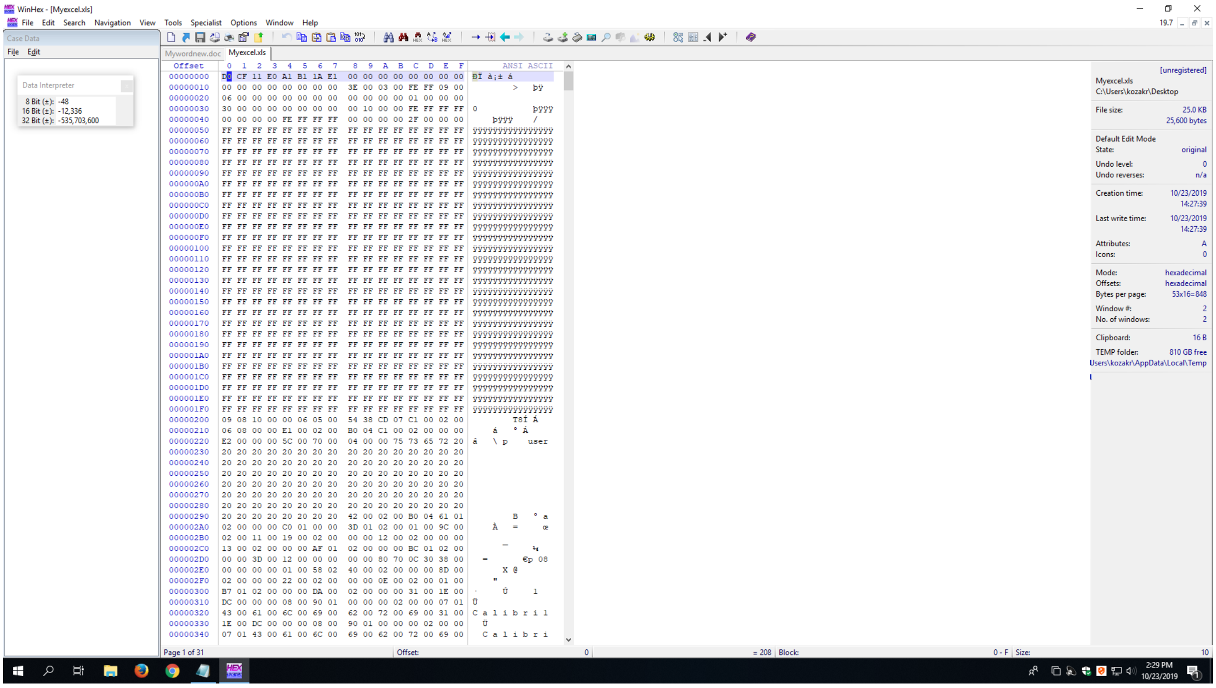
Figure 1: Header for Word 97-2003 Document `.doc`.

These steps are repeated for the following file types, `.xls`, `.docx`, `.xlsx`, `.jpg`, and `.png`.

Screenshots and text for each file type can be found listed below.

Hexadecimal header for `.xls` file type.

```
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   00 00 00 00 00 00 00 00 ⊠⊠⊠⊠
```


WinHex - [Myexcel.xls]
File Edit Search Navigation View Tools Specialist Options Window Help
Case Data
File Edit
Mywordnew.doc
Myexcel.xls
19.7

Data Interpreter
8 Bit (±): -48
16 Bit (±): -12,336
32 Bit (±): -535,703,600

```
  Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F     ANSI ASCII
00000000   D0 CF 11 E0 A1 B1 1A E1  00 00 00 00 00 00 00 00   ÐÏ à¡± á
00000010   00 00 00 00 00 00 00 00  3E 00 03 00 FE FF 09 00           >   þÿ
00000020   06 00 00 00 00 00 00 00  00 00 00 00 01 00 00 00
00000030   30 00 00 00 00 00 00 00  00 10 00 00 FE FF FF FF   0           þÿÿÿ
00000040   00 00 00 00 FE FF FF FF  00 00 00 00 2F 00 00 00       þÿÿÿ    /
00000050   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000060   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000070   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000080   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000090   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000000A0   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000000B0   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000000C0   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000000D0   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000000E0   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000000F0   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000100   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000110   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000120   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000130   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000140   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000150   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000160   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000170   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000180   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000190   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000001A0   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000001B0   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000001C0   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000001D0   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000001E0   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000001F0   FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000200   09 08 10 00 00 06 05 00  54 38 CD 07 C1 00 02 00           T8Í Á
00000210   06 08 00 00 E1 00 02 00  B0 04 C1 00 02 00 00 00       á   ° Á
00000220   E2 00 00 00 5C 00 70 00  04 00 00 75 73 65 72 20   â   \ p    user
00000230   20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00000240   20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00000250   20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00000260   20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00000270   20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00000280   20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00000290   20 20 20 20 20 20 20 20  42 00 02 00 B0 04 61 01           B   ° a
000002A0   02 00 00 00 C0 01 00 00  3D 01 02 00 01 00 9C 00       À   =     œ
000002B0   02 00 11 00 19 00 02 00  00 00 12 00 02 00 00 00
000002C0   13 00 02 00 00 00 AF 01  02 00 00 00 BC 01 02 00         ¯     ¼
000002D0   00 00 3D 00 12 00 00 00  00 00 80 70 0C 30 38 00     =       €p 08
000002E0   00 00 00 00 01 00 58 02  40 00 02 00 00 00 8D 00         X @
000002F0   02 00 00 00 22 00 02 00  00 00 0E 00 02 00 01 00       "
00000300   B7 01 02 00 00 00 DA 00  02 00 00 00 31 00 1E 00   ·     Ú     1
00000310   DC 00 00 00 08 00 90 01  00 00 00 02 00 00 07 01   Ü
00000320   43 00 61 00 6C 00 69 00  62 00 72 00 69 00 31 00   C a l i b r i 1
00000330   1E 00 DC 00 00 00 08 00  90 01 00 00 00 02 00 00     Ü
00000340   07 01 43 00 61 00 6C 00  69 00 62 00 72 00 69 00     C a l i b r i
```

[unregistered]
Myexcel.xls
C:\Users\kozakr\Desktop

File size: 25.0 KB
25,600 bytes

Default Edit Mode
State: original
Undo level: 0
Undo reverses: n/a

Creation time: 10/23/2019
14:27:39

Last write time: 10/23/2019
14:27:39

Attributes: A
Icons: 0

Mode: hexadecimal
Offsets: hexadecimal
Bytes per page: 53x16=848
Window #: 2
No. of windows: 2

Clipboard: 16 B
TEMP folder: 810 GB free
Users\kozakr\AppData\Local\Temp

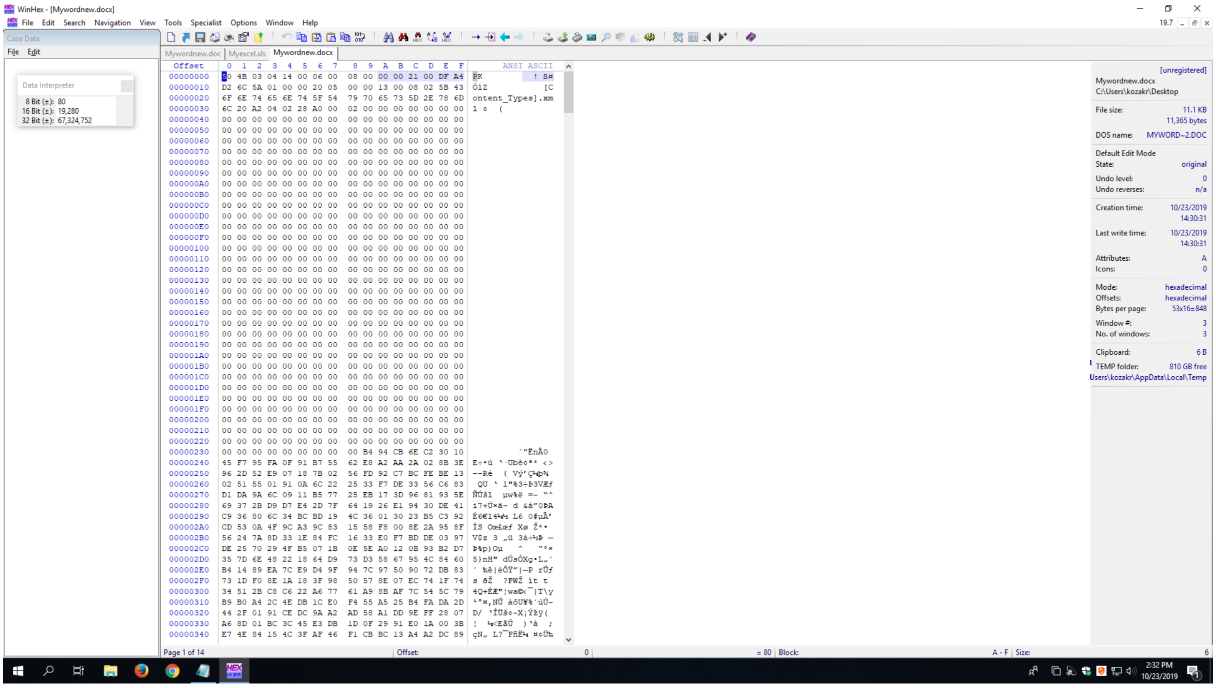
Page 1 of 31 | Offset: 0 | = 208 | Block: 0 - F | Size: 10

2:29 PM
10/23/2019

Figure 2: Header for Excel 97-2003 Workbook `.xls`.

Hexadecimal header for `.docx` file type.

```
Offset       0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F

00000000   50 4B 03 04 14 00 06 00   08 00 00 00 21 00 DF A4    PK
              ! ⊠
```



8 Bit (±): 80
16 Bit (±): 19,280
32 Bit (±): 67,324,752

```
  Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F     ANSI ASCII
00000000   50 4B 03 04 14 00 06 00  08 00 00 00 21 00 DF A4   PK          ! ß¤
00000010   D2 6C 5A 01 00 00 20 05  00 00 13 00 08 02 5B 43   ÒlZ            [C
00000020   6F 6E 74 65 6E 74 5F 54  79 70 65 73 5D 2E 78 6D   ontent_Types].xm
00000030   6C 20 A2 04 02 28 A0 00  02 00 00 00 00 00 00 00   l ¢  (
00000040   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000050   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000060   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000070   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000080   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000090   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000A0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000B0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000C0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000D0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000E0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000F0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000100   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000110   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000120   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000130   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000140   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000150   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000160   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000170   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000180   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000190   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001A0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001B0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001C0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001D0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001E0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001F0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000200   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000210   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000220   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000230   00 00 00 00 00 00 00 00  00 B4 94 CB 6E C2 30 10             ´”ËnÂ0
00000240   45 F7 95 FA 0F 91 B7 55  62 E8 A2 AA 2A 02 8B 3E   E÷•ú ‘·Ubè¢ª* ‹>
00000250   96 2D 52 E9 07 18 7B 02  56 FD 92 C7 BC FE BE 13   –-Ré  { Vý’Ç¼þ¾
00000260   02 51 55 01 91 0A 6C 22  25 33 F7 DE 33 56 C6 83    QU ‘ l"%3÷Þ3VÆƒ
00000270   D1 DA 9A 6C 09 11 B5 77  25 EB 17 3D 96 81 93 5E   ÑÚšl  µw%ë =– “^
00000280   69 37 2B D9 D7 E4 2D 7F  64 19 26 E1 94 30 DE 41   i7+Ù×ä- d &á”0ÞA
00000290   C9 36 80 6C 34 BC BD 19  4C 36 01 30 23 B5 C3 92   É6€l4¼½ L6 0#µÃ’
000002A0   CD 53 0A 4F 9C A3 9C 83  15 58 F8 00 8E 2A 95 8F   ÍS Oœ£œƒ Xø Ž*•
000002B0   56 24 7A 8D 33 1E 84 FC  16 33 E0 F7 BD DE 03 97   V$z 3 „ü 3à÷½Þ —
000002C0   DE 25 70 29 4F B5 07 1B  0E 5E A0 12 0B 93 B2 D7   Þ%p)Oµ  ^   “²×
000002D0   35 7D 6E 48 22 18 64 D9  73 D3 58 67 95 4C 84 60   5}nH" dÙsÓXg•L„`
000002E0   B4 14 89 EA 7C E9 D4 9F  94 7C 97 50 90 72 DB 83   ´ ‰ê|éÔŸ”|—P rÛƒ
000002F0   73 1D F0 8E 1A 18 3F 98  50 57 8E 07 EC 74 1F 74   s ðŽ  ?˜PWŽ ìt t
00000300   34 51 2B C8 C6 22 A6 77  61 A9 8B AF 7C 54 5C 79   4Q+ÈÆ"¦wa©‹¯|T\y
00000310   B9 B0 A4 2C 4E DB 1C E0  F4 55 A5 25 B4 FA DA 2D   ¹°¤,NÛ àôU¥%´úÚ-
00000320   44 2F 01 91 CE DC 9A A2  AD 58 A1 DD 9E FF 28 07   D/ ‘ÎÜš¢X¡ÝžÿÝ(
00000330   A6 8D 01 BC 3C 45 E3 DB  1D 0F 29 91 E0 1A 00 3B   ¦  ¼<EãÛ  )‘à  ;
00000340   E7 4E 84 15 4C 3F AF 46  F1 CB BC 13 A4 A2 DC 89   çN„ L?¯FñË¼ ¤¢Ü‰
```

[unregistered]
Mywordnew.docx
C:\Users\kozakr\Desktop

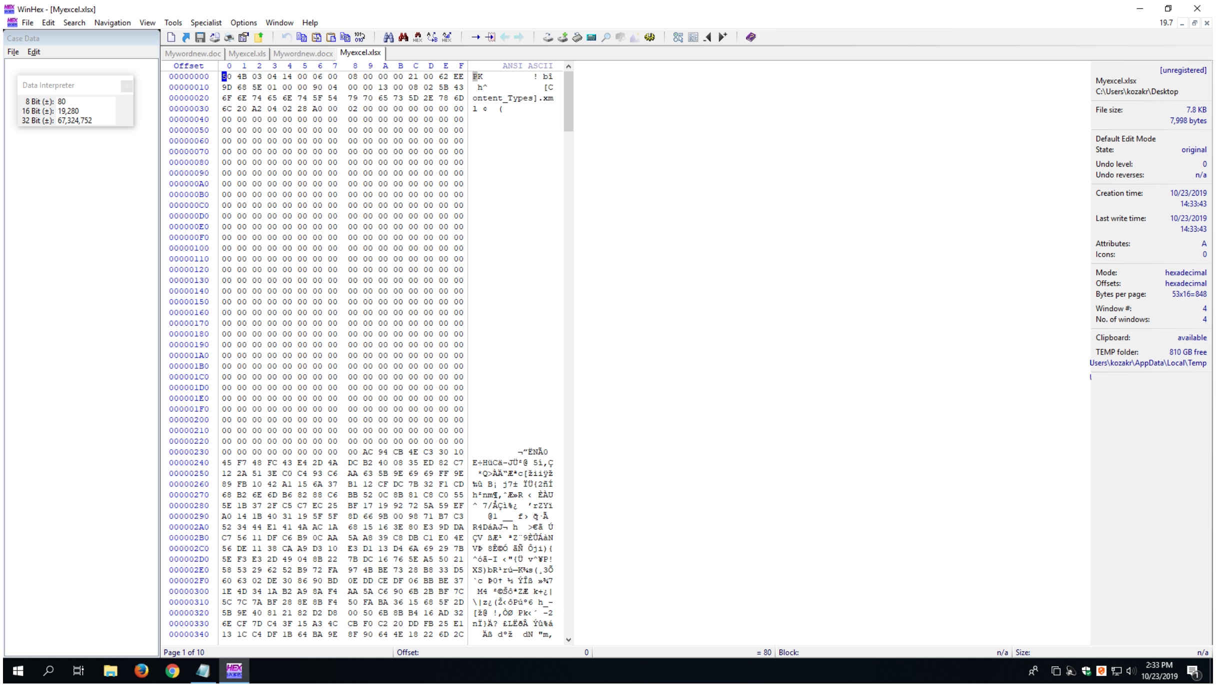
File size:	11.1 KB 11,365 bytes
DOS name:	MYWORD~2.DOC
Default Edit Mode	
State:	original
Undo level:	0
Undo reverses:	n/a
Creation time:	10/23/2019 14:30:31
Last write time:	10/23/2019 14:30:31
Attributes:	A
Icons:	0
Mode:	hexadecimal
Offsets:	hexadecimal
Bytes per page:	53x16=848
Window #:	3
No. of windows:	3
Clipboard:	6 B
TEMP folder:	810 GB free

Users\kozakr\AppData\Local\Temp

Figure 3: Header for Word 2007 Document .docx.

Hexadecimal header for .xlsx file type.

```
Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F

00000000   50 4B 03 04 14 00 06 00  08 00 00 00 21 00 62 EE   PK
            ! ⊠b
```



Data Interpreter
8 Bit (±): 80
16 Bit (±): 19,280
32 Bit (±): 67,324,752

```
Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F      ANSI ASCII
00000000   50 4B 03 04 14 00 06 00  08 00 00 00 21 00 62 EE   PK          ! bî
00000010   9D 68 5E 01 00 00 90 04  00 00 13 00 08 02 5B 43    h^          [C
00000020   6F 6E 74 65 6E 74 5F 54  79 70 65 73 5D 2E 78 6D   ontent_Types].xm
00000030   6C 20 A2 04 02 28 A0 00  02 00 00 00 00 00 00 00   l ¢  (
00000040   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000050   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000060   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000070   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000080   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000090   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000A0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000B0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000C0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000D0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000E0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000F0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000100   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000110   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000120   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000130   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000140   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000150   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000160   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000170   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000180   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000190   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001A0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001B0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001C0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001D0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001E0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001F0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000200   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000210   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000220   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000230   00 00 00 00 00 00 00 00  00 AC 94 CB 4E C3 30 10            ¬”ËNÃ0
00000240   45 F7 48 FC 43 E4 2D 4A  DC B2 40 08 35 ED 82 C7   E÷HüCä-JÜ²@ 5í,Ç
00000250   12 2A 51 3E C0 C4 93 C6  AA 63 5B 9E 69 69 FF 9E    *Q>ÀÄ“Æªc[žiiÿž
00000260   89 FB 10 42 A1 15 6A 37  B1 12 CF DC 7B 32 F1 CD   ‰û B¡ j7± ÏÜ{2ñÍ
00000270   68 B2 6E 6D B6 82 88 C6  BB 52 0C 8B 81 C8 C0 55   h²nm¶,ˆÆ»R ‹ ÈÀU
00000280   5E 1B 37 2F C5 C7 EC 25  BF 17 19 92 72 5A 59 EF   ^ 7/ÅÇì%¿  ’rZYï
00000290   A0 14 1B 40 31 19 5F 5F  8D 66 9B 00 98 71 B7 C3      @1 __ f› ˜q·Ã
000002A0   52 34 44 E1 41 4A AC 1A  68 15 16 3E 80 E3 9D DA   R4DáAJ¬ h  >€ã Ú
000002B0   C7 56 11 DF C6 B9 0C AA  5A A8 39 C8 DB C1 E0 4E   ÇV ßÆ¹ ªZ¨9ÈÛÁàN
000002C0   56 DE 11 38 CA A9 D3 10  E3 D1 13 D4 6A 69 29 7B   VÞ 8Ê©Ó ãÑ Ôji){
000002D0   5E F3 E3 2D 49 04 8B 22  7B DC 16 76 5E A5 50 21   ^óã-I ‹"{Ü v^¥P!
000002E0   58 53 29 62 52 B9 72 FA  97 4B BE 73 28 B8 33 D5   XS)bR¹rú—K¾s(¸3Õ
000002F0   60 63 02 DE 30 86 90 BD  0E DD CE DF 06 BB BE 37   `c Þ0† ½ ÝÎß »¾7
00000300   1E 4D 34 1A B2 A9 8A F4  AA 5A C6 90 6B 2B BF 7C    M4 ²©Šôª ZÆ k+¿|
00000310   5C 7C 7A BF 28 8E 8B F4  50 FA BA 36 15 68 5F 2D   \|z¿(Ž‹ôPúº6 h_-
00000320   5B 9E 40 81 21 82 D2 D8  00 50 6B 8B B4 16 AD 32   [ž@ !,ÒØ Pk‹´ 2
00000330   6E CF 7D C4 3F 15 A3 4C  CB F0 C2 20 DD FB 25 E1   nÏ}Ä? £LËðÂ Ýû%á
00000340   13 1C C4 DF 1B 64 BA 9E  8F 90 64 4E 18 22 6D 2C     Äß dºž  dN "m,
```

[unregistered]
Myexcel.xlsx
C:\Users\kozakr\Desktop

File size: 7.8 KB
7,998 bytes

Default Edit Mode
State: original
Undo level: 0
Undo reverses: n/a

Creation time: 10/23/2019 14:33:43
Last write time: 10/23/2019 14:33:43
Attributes: A
Icons: 0

Mode: hexadecimal
Offsets: hexadecimal
Bytes per page: 53x16=848
Window #: 4
No. of windows: 4

Clipboard: available
TEMP folder: 810 GB free
Users\kozakr\AppData\Local\Temp

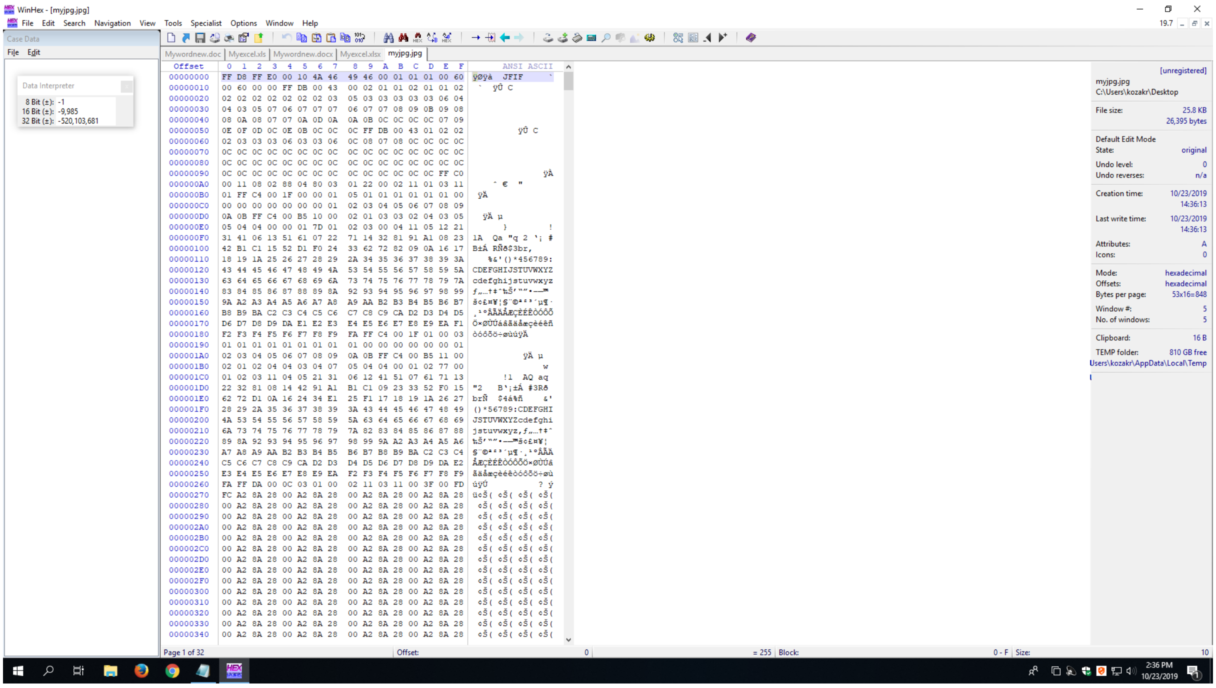
Page 1 of 10 | Offset: 0 | = 80 | Block: n/a | Size: n/a

2:33 PM
10/23/2019

Figure 4: Header for Excel 2007 Workbook .xlsx.

Hexadecimal header for .jpg file type.

```
Offset       0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F

00000000    FF D8 FF E0 00 10 4A 46  49 46 00 01 01 01 00 60 ⊠⊠⊠⊠
    JFIF     `
```


WinHex - [myjpg.jpg]
File Edit Search Navigation View Tools Specialist Options Window Help
Case Data
File Edit
Mywordnew.doc Myexcel.xls Mywordnew.docx Myexcel.xlsx myjpg.jpg
19.7
Page 1 of 32
Offset: 0
= 255 Block:
0 - F Size: 10
2:36 PM
10/23/2019

Data Interpreter
8 Bit (±): -1
16 Bit (±): -9,985
32 Bit (±): -520,103,681

```
  Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F       ANSI ASCII
00000000   FF D8 FF E0 00 10 4A 46  49 46 00 01 01 01 00 60   ÿØÿà  JFIF     `
00000010   00 60 00 00 FF DB 00 43  00 02 01 01 02 01 01 02    `  ÿÛ C
00000020   02 02 02 02 02 02 02 03  05 03 03 03 03 03 06 04
00000030   04 03 05 07 06 07 07 07  06 07 07 08 09 0B 09 08
00000040   08 0A 08 07 07 0A 0D 0A  0A 0B 0C 0C 0C 0C 07 09
00000050   0E 0F 0D 0C 0E 0B 0C 0C  0C FF DB 00 43 01 02 02            ÿÛ C
00000060   02 03 03 03 06 03 03 06  0C 08 07 08 0C 0C 0C 0C
00000070   0C 0C 0C 0C 0C 0C 0C 0C  0C 0C 0C 0C 0C 0C 0C 0C
00000080   0C 0C 0C 0C 0C 0C 0C 0C  0C 0C 0C 0C 0C 0C 0C 0C
00000090   0C 0C 0C 0C 0C 0C 0C 0C  0C 0C 0C 0C 0C 0C FF C0                 ÿÀ
000000A0   00 11 08 02 88 04 80 03  01 22 00 02 11 01 03 11       ˆ €   "
000000B0   01 FF C4 00 1F 00 00 01  05 01 01 01 01 01 01 00    ÿÄ
000000C0   00 00 00 00 00 00 00 01  02 03 04 05 06 07 08 09
000000D0   0A 0B FF C4 00 B5 10 00  02 01 03 03 02 04 03 05     ÿÄ µ
000000E0   05 04 04 00 00 01 7D 01  02 03 00 04 11 05 12 21         }        !
000000F0   31 41 06 13 51 61 07 22  71 14 32 81 91 A1 08 23   1A  Qa "q 2 ‘¡ #
00000100   42 B1 C1 15 52 D1 F0 24  33 62 72 82 09 0A 16 17   B±Á RÑð$3br‚
00000110   18 19 1A 25 26 27 28 29  2A 34 35 36 37 38 39 3A      %&'()*456789:
00000120   43 44 45 46 47 48 49 4A  53 54 55 56 57 58 59 5A   CDEFGHIJSTUVWXYZ
00000130   63 64 65 66 67 68 69 6A  73 74 75 76 77 78 79 7A   cdefghijstuvwxyz
00000140   83 84 85 86 87 88 89 8A  92 93 94 95 96 97 98 99   ƒ„…†‡ˆ‰Š’“”•–—˜™
00000150   9A A2 A3 A4 A5 A6 A7 A8  A9 AA B2 B3 B4 B5 B6 B7   š¢£¤¥¦§¨©ª²³´µ¶·
00000160   B8 B9 BA C2 C3 C4 C5 C6  C7 C8 C9 CA D2 D3 D4 D5   ¸¹ºÂÃÄÅÆÇÈÉÊÒÓÔÕ
00000170   D6 D7 D8 D9 DA E1 E2 E3  E4 E5 E6 E7 E8 E9 EA F1   Ö×ØÙÚáâãäåæçèéêñ
00000180   F2 F3 F4 F5 F6 F7 F8 F9  FA FF C4 00 1F 01 00 03   òóôõö÷øùúÿÄ
00000190   01 01 01 01 01 01 01 01  01 00 00 00 00 00 00 01
000001A0   02 03 04 05 06 07 08 09  0A 0B FF C4 00 B5 11 00             ÿÄ µ
000001B0   02 01 02 04 04 03 04 07  05 04 04 00 01 02 77 00                w
000001C0   01 02 03 11 04 05 21 31  06 12 41 51 07 61 71 13         !1  AQ aq
000001D0   22 32 81 08 14 42 91 A1  B1 C1 09 23 33 52 F0 15   "2   B‘¡±Á #3Rð
000001E0   62 72 D1 0A 16 24 34 E1  25 F1 17 18 19 1A 26 27   brÑ  $4á%ñ    &'
000001F0   28 29 2A 35 36 37 38 39  3A 43 44 45 46 47 48 49   ()*56789:CDEFGHI
00000200   4A 53 54 55 56 57 58 59  5A 63 64 65 66 67 68 69   JSTUVWXYZcdefghi
00000210   6A 73 74 75 76 77 78 79  7A 82 83 84 85 86 87 88   jstuvwxyz‚ƒ„…†‡ˆ
00000220   89 8A 92 93 94 95 96 97  98 99 9A A2 A3 A4 A5 A6   ‰Š’“”•–—˜™š¢£¤¥¦
00000230   A7 A8 A9 AA B2 B3 B4 B5  B6 B7 B8 B9 BA C2 C3 C4   §¨©ª²³´µ¶·¸¹ºÂÃÄ
00000240   C5 C6 C7 C8 C9 CA D2 D3  D4 D5 D6 D7 D8 D9 DA E2   ÅÆÇÈÉÊÒÓÔÕÖ×ØÙÚâ
00000250   E3 E4 E5 E6 E7 E8 E9 EA  F2 F3 F4 F5 F6 F7 F8 F9   ãäåæçèéêòóôõö÷øù
00000260   FA FF DA 00 0C 03 01 00  02 11 03 11 00 3F 00 FD   úÿÚ          ? ý
00000270   FC A2 8A 28 00 A2 8A 28  00 A2 8A 28 00 A2 8A 28   ü¢Š( ¢Š( ¢Š( ¢Š(
00000280   00 A2 8A 28 00 A2 8A 28  00 A2 8A 28 00 A2 8A 28    ¢Š( ¢Š( ¢Š( ¢Š(
00000290   00 A2 8A 28 00 A2 8A 28  00 A2 8A 28 00 A2 8A 28    ¢Š( ¢Š( ¢Š( ¢Š(
000002A0   00 A2 8A 28 00 A2 8A 28  00 A2 8A 28 00 A2 8A 28    ¢Š( ¢Š( ¢Š( ¢Š(
000002B0   00 A2 8A 28 00 A2 8A 28  00 A2 8A 28 00 A2 8A 28    ¢Š( ¢Š( ¢Š( ¢Š(
000002C0   00 A2 8A 28 00 A2 8A 28  00 A2 8A 28 00 A2 8A 28    ¢Š( ¢Š( ¢Š( ¢Š(
000002D0   00 A2 8A 28 00 A2 8A 28  00 A2 8A 28 00 A2 8A 28    ¢Š( ¢Š( ¢Š( ¢Š(
000002E0   00 A2 8A 28 00 A2 8A 28  00 A2 8A 28 00 A2 8A 28    ¢Š( ¢Š( ¢Š( ¢Š(
000002F0   00 A2 8A 28 00 A2 8A 28  00 A2 8A 28 00 A2 8A 28    ¢Š( ¢Š( ¢Š( ¢Š(
00000300   00 A2 8A 28 00 A2 8A 28  00 A2 8A 28 00 A2 8A 28    ¢Š( ¢Š( ¢Š( ¢Š(
00000310   00 A2 8A 28 00 A2 8A 28  00 A2 8A 28 00 A2 8A 28    ¢Š( ¢Š( ¢Š( ¢Š(
00000320   00 A2 8A 28 00 A2 8A 28  00 A2 8A 28 00 A2 8A 28    ¢Š( ¢Š( ¢Š( ¢Š(
00000330   00 A2 8A 28 00 A2 8A 28  00 A2 8A 28 00 A2 8A 28    ¢Š( ¢Š( ¢Š( ¢Š(
00000340   00 A2 8A 28 00 A2 8A 28  00 A2 8A 28 00 A2 8A 28    ¢Š( ¢Š( ¢Š( ¢Š(
```

[unregistered]
myjpg.jpg
C:\Users\kozakr\Desktop

File size: 25.8 KB
26,395 bytes

Default Edit Mode
State: original
Undo level: 0
Undo reverses: n/a

Creation time: 10/23/2019
14:36:13
Last write time: 10/23/2019
14:36:13
Attributes: A
Icons: 0

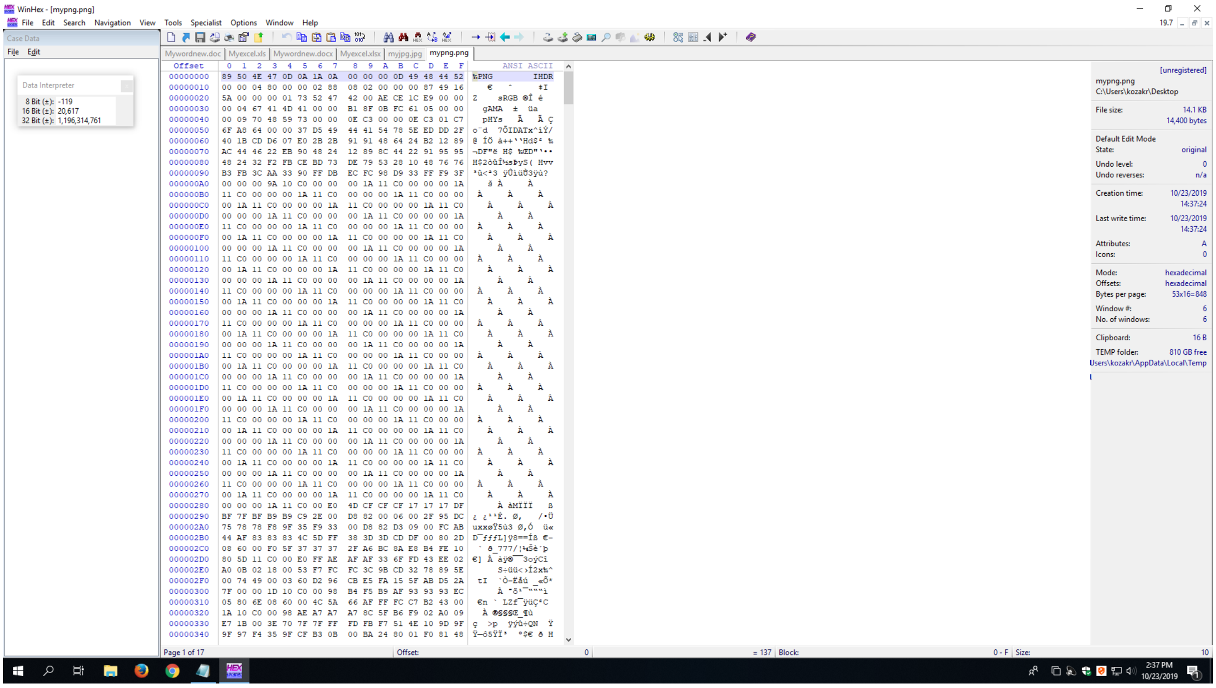
Mode: hexadecimal
Offsets: hexadecimal
Bytes per page: 53x16=848
Window #: 5
No. of windows: 5

Clipboard: 16 B
TEMP folder: 810 GB free
Users\kozakr\AppData\Local\Temp

Figure 5: Header for `.jpg`.

Hexadecimal header for `.png` file type.

```
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  00 00 00 0D 49 48 44 52 ⊠  PNG
          IHDR
```



Data Interpreter

```
 8 Bit (±): -119
16 Bit (±): 20,617
32 Bit (±): 1,196,314,761
```

```
  Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F     ANSI ASCII
00000000   89 50 4E 47 0D 0A 1A 0A  00 00 00 0D 49 48 44 52   ‰PNG        IHDR
00000010   00 00 04 80 00 00 02 88  08 02 00 00 00 87 49 16      €  ˆ      ‡I
00000020   5A 00 00 00 01 73 52 47  42 00 AE CE 1C E9 00 00   Z    sRGB ®Î é
00000030   00 04 67 41 4D 41 00 00  B1 8F 0B FC 61 05 00 00     gAMA  ± üa
00000040   00 09 70 48 59 73 00 00  0E C3 00 00 0E C3 01 C7     pHYs   Ã   Ã Ç
00000050   6F A8 64 00 00 37 D5 49  44 41 54 78 5E ED DD 2F   o¨d  7ÕIDATx^íÝ/
00000060   40 1B CD D6 07 E0 2B 2B  91 91 48 64 24 B2 12 89   @ ÍÖ à++‘‘Hd$² ‰
00000070   AC 44 46 22 EB 90 48 24  12 89 8C 44 22 91 95 95   ¬DF"ë H$ ‰ŒD"‘••
00000080   48 24 32 F2 FB CE BD 73  DE 79 53 28 10 48 76 76   H$2òûÎ½sÞyS( Hvv
00000090   B3 FB 3C AA 33 90 FF DB  EC FC 98 D9 33 FF F9 3F   ³û<ª3 ÿÛìü˜Ù3ÿù?
000000A0   00 00 00 9A 10 C0 00 00  00 1A 11 C0 00 00 00 1A      š À     À
000000B0   11 C0 00 00 00 1A 11 C0  00 00 00 1A 11 C0 00 00    À     À     À
000000C0   00 1A 11 C0 00 00 00 1A  11 C0 00 00 00 1A 11 C0      À     À     À
000000D0   00 00 00 1A 11 C0 00 00  00 1A 11 C0 00 00 00 1A        À     À
000000E0   11 C0 00 00 00 1A 11 C0  00 00 00 1A 11 C0 00 00    À     À     À
000000F0   00 1A 11 C0 00 00 00 1A  11 C0 00 00 00 1A 11 C0      À     À     À
00000100   00 00 00 1A 11 C0 00 00  00 1A 11 C0 00 00 00 1A        À     À
00000110   11 C0 00 00 00 1A 11 C0  00 00 00 1A 11 C0 00 00    À     À     À
00000120   00 1A 11 C0 00 00 00 1A  11 C0 00 00 00 1A 11 C0      À     À     À
00000130   00 00 00 1A 11 C0 00 00  00 1A 11 C0 00 00 00 1A        À     À
00000140   11 C0 00 00 00 1A 11 C0  00 00 00 1A 11 C0 00 00    À     À     À
00000150   00 1A 11 C0 00 00 00 1A  11 C0 00 00 00 1A 11 C0      À     À     À
00000160   00 00 00 1A 11 C0 00 00  00 1A 11 C0 00 00 00 1A        À     À
00000170   11 C0 00 00 00 1A 11 C0  00 00 00 1A 11 C0 00 00    À     À     À
00000180   00 1A 11 C0 00 00 00 1A  11 C0 00 00 00 1A 11 C0      À     À     À
00000190   00 00 00 1A 11 C0 00 00  00 1A 11 C0 00 00 00 1A        À     À
000001A0   11 C0 00 00 00 1A 11 C0  00 00 00 1A 11 C0 00 00    À     À     À
000001B0   00 1A 11 C0 00 00 00 1A  11 C0 00 00 00 1A 11 C0      À     À     À
000001C0   00 00 00 1A 11 C0 00 00  00 1A 11 C0 00 00 00 1A        À     À
000001D0   11 C0 00 00 00 1A 11 C0  00 00 00 1A 11 C0 00 00    À     À     À
000001E0   00 1A 11 C0 00 00 00 1A  11 C0 00 00 00 1A 11 C0      À     À     À
000001F0   00 00 00 1A 11 C0 00 00  00 1A 11 C0 00 00 00 1A        À     À
00000200   11 C0 00 00 00 1A 11 C0  00 00 00 1A 11 C0 00 00    À     À     À
00000210   00 1A 11 C0 00 00 00 1A  11 C0 00 00 00 1A 11 C0      À     À     À
00000220   00 00 00 1A 11 C0 00 00  00 1A 11 C0 00 00 00 1A        À     À
00000230   11 C0 00 00 00 1A 11 C0  00 00 00 1A 11 C0 00 00    À     À     À
00000240   00 1A 11 C0 00 00 00 1A  11 C0 00 00 00 1A 11 C0      À     À     À
00000250   00 00 00 1A 11 C0 00 00  00 1A 11 C0 00 00 00 1A        À     À
00000260   11 C0 00 00 00 1A 11 C0  00 00 00 1A 11 C0 00 00    À     À     À
00000270   00 1A 11 C0 00 00 00 1A  11 C0 00 00 00 1A 11 C0      À     À     À
00000280   00 00 00 1A 11 C0 00 E0  4D CF CF CF 17 17 17 DF        À àMÏÏÏ   ß
00000290   BF 7F BF B9 B9 C9 2E 00  D8 82 00 06 00 2F 95 DC   ¿ ¿¹¹É. Ø‚   /•Ü
000002A0   75 78 78 F8 9F 35 F9 33  00 D8 82 D3 09 00 FC AB   uxxøŸ5ù3 Ø‚Ó  ü«
000002B0   44 AF 83 83 83 4C 5D FF  38 3D 3D CD DF 00 80 2D   D¯ƒƒƒL]ÿ8==Íß €-
000002C0   08 60 00 F0 5F 37 37 37  2F A6 BC 8A E8 B4 FE 10    ` ð_777/¦¼Šè´þ
000002D0   80 5D 11 C0 00 E0 FF AE  AF AF 33 6F FD 43 EE 02   €] À àÿ®¯¯3oýCî
000002E0   A0 0B 02 18 00 53 F7 FC  FC 3C 9B CD 32 78 89 5E         S÷üü<›Í2x‰^
000002F0   00 74 49 00 03 60 D2 96  CB E5 FA 15 5F AB D5 2A    tI  `Ò–Ëåú _«Õ*
00000300   7F 00 00 1D 10 C0 00 98  B4 F5 B9 AF 93 93 93 EC        À ˜´õ¹¯“““ì
00000310   05 80 6E 08 60 00 4C 5A  66 AF FF FC C7 B2 43 00    €n ` LZf¯ÿüÇ²C
00000320   1A 10 C0 00 98 AE A7 A7  A7 8C 5F B6 F9 02 A0 09     À ˜®§§§Œ_¶ù
00000330   E7 1B 00 3E 70 7F 7F FF  FD FB F7 51 4E 10 9D 9F   ç  >p  ÿýû÷QN  Ÿ
00000340   9F 97 F4 35 9F CF B3 0B  00 BA 24 80 01 F0 81 48   Ÿ—ô5ŸÏ³  º$€ ð H
```

[unregistered]
mypng.png
C:\Users\kozakr\Desktop

File size:	14.1 KB 14,400 bytes
Default Edit Mode	
State:	original
Undo level:	0
Undo reverses:	n/a
Creation time:	10/23/2019 14:37:24
Last write time:	10/23/2019 14:37:24
Attributes:	A
Icons:	0
Mode:	hexadecimal
Offsets:	hexadecimal
Bytes per page:	53x16=848
Window #:	6
No. of windows:	6
Clipboard:	16 B
TEMP folder:	810 GB free Users\kozakr\AppData\Local\Temp

Page 1 of 17 Offset: 0 = 137 Block: 0 - F Size: 10

2:37 PM 10/23/2019

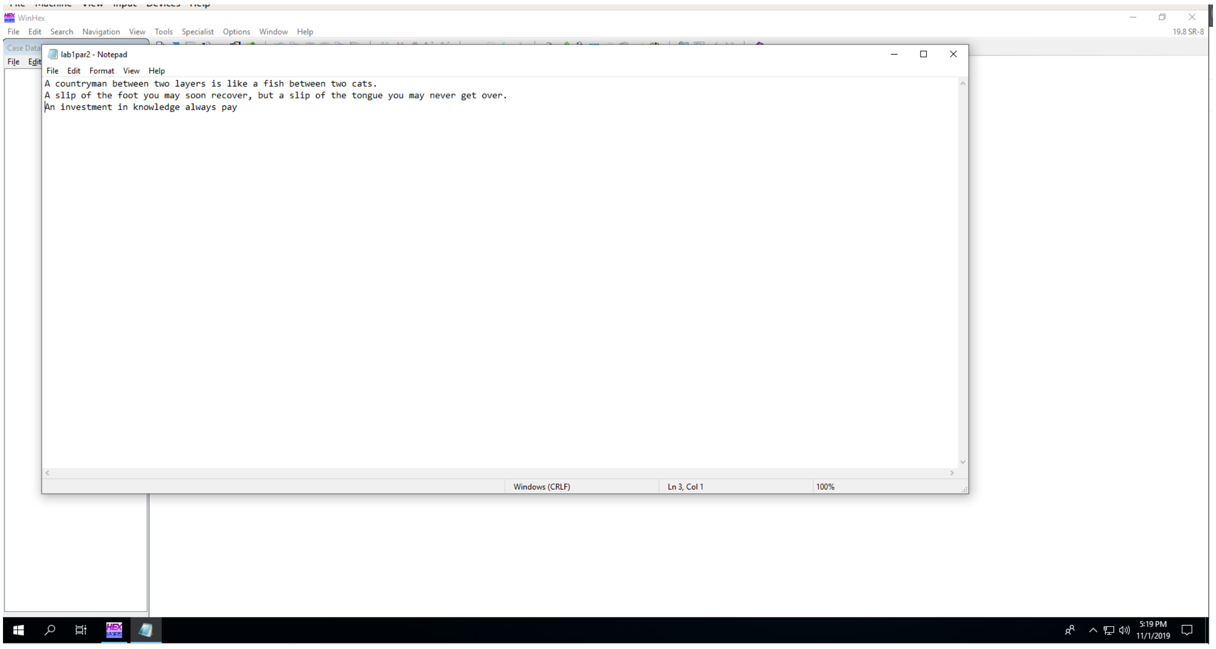
Figure 6: Header for .png.

Observations: As you can see, hexadecimal headers for .doc and .xls files match one another. Additionally, .docx and .xlsx also match one another. It seems the Microsoft Office Suite versions produce files with the same hex header, version 97-2003 match one another, and version 2007+ match one another. It doesn't appear that spreadsheet files differ from word documents, which is surprising. It's all about the version.

Part 2: Explore MFT.

The second part of this activity requires we create a file named lab1part2.txt, containing the following,

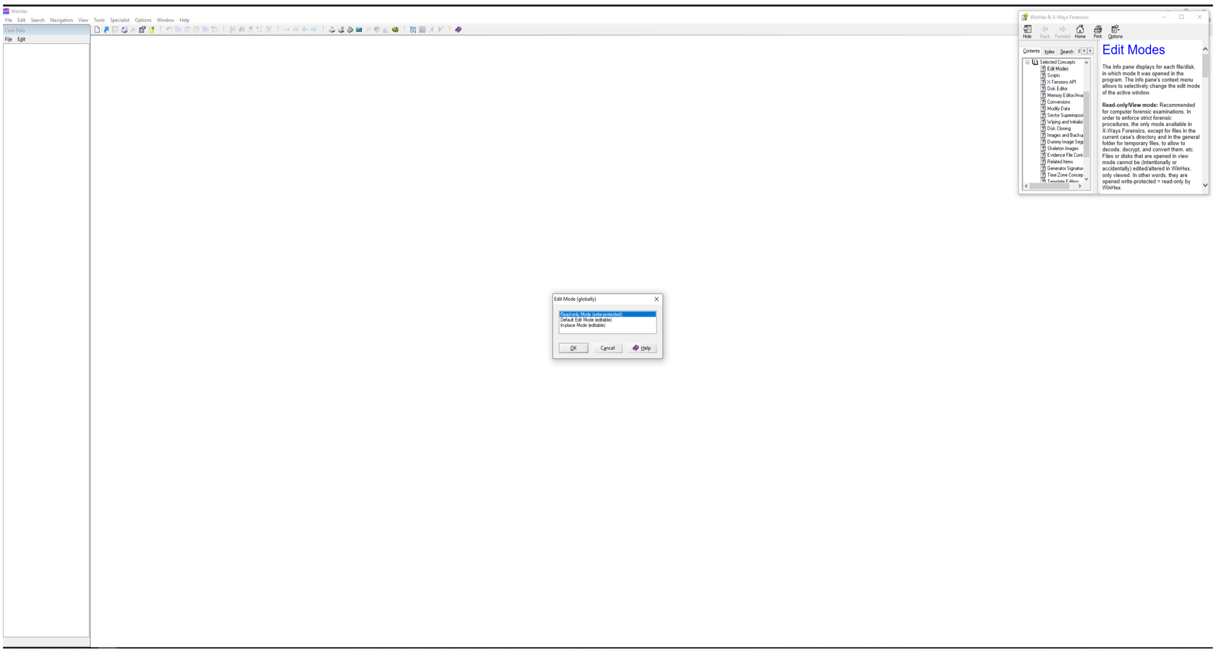
```
A countryman between two layers is like a fish between two cats.
A slip of the foot you may soon recover, but a slip of the tongue you
    may never get over.
An investment in knowledge always pays the best interest.
Drive thy business or it will drive there.
```


WinHex
File Edit Search Navigation View Tools Specialist Options Window Help
lab1par2 - Notepad
File Edit Format View Help
Windows (CRLF)
Ln 3, Col 1
100%
5:19 PM
11/1/2019

```
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 pay
```

Figure 7: Creating `lab1part2.txt` file.

We then open WinHex as an administrator, and navigate `Options->Edit Mode` to select `Read-Only Mode`.


WinHex
File Edit Search Navigation View Tools Specialist Options Window Help
Home
Print
Options
OK
Cancel
Help

Edit Mode (globally)

- Read-only Mode (write-protected)
- Default Edit Mode (editable)
- In-place Mode (editable)

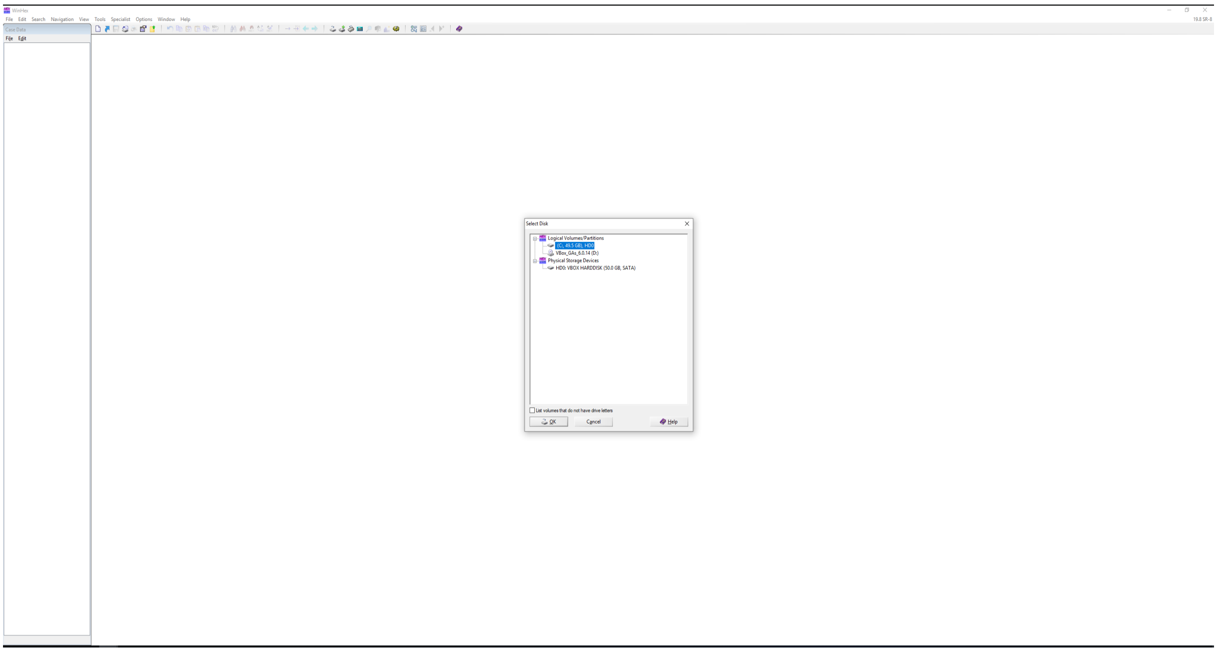
Edit Modes

The info pane displays for each file/disk, in which mode it was opened in the program. The info pane's context menu allows to selectively change the edit mode of the active window.

Read-only/View mode: Recommended for computer forensic examinations. In order to enforce strict forensic procedures, the only mode available in X-Ways Forensics, except for files in the current case's directory and in the general folder for temporary files, to allow to decode, decrypt, and convert them, etc. Files or disks that are opened in view mode cannot be (intentionally or accidentally) edited/altered in WinHex, only viewed. In other words, they are opened write-protected = read-only by WinHex.

Figure 8: Set WinHex to Read-Only Mode.

After this we select a disk to open via `Tools->Open Disk`, and choose the `C:` drive. This is the drive on which we saved `lap1part2.txt`.



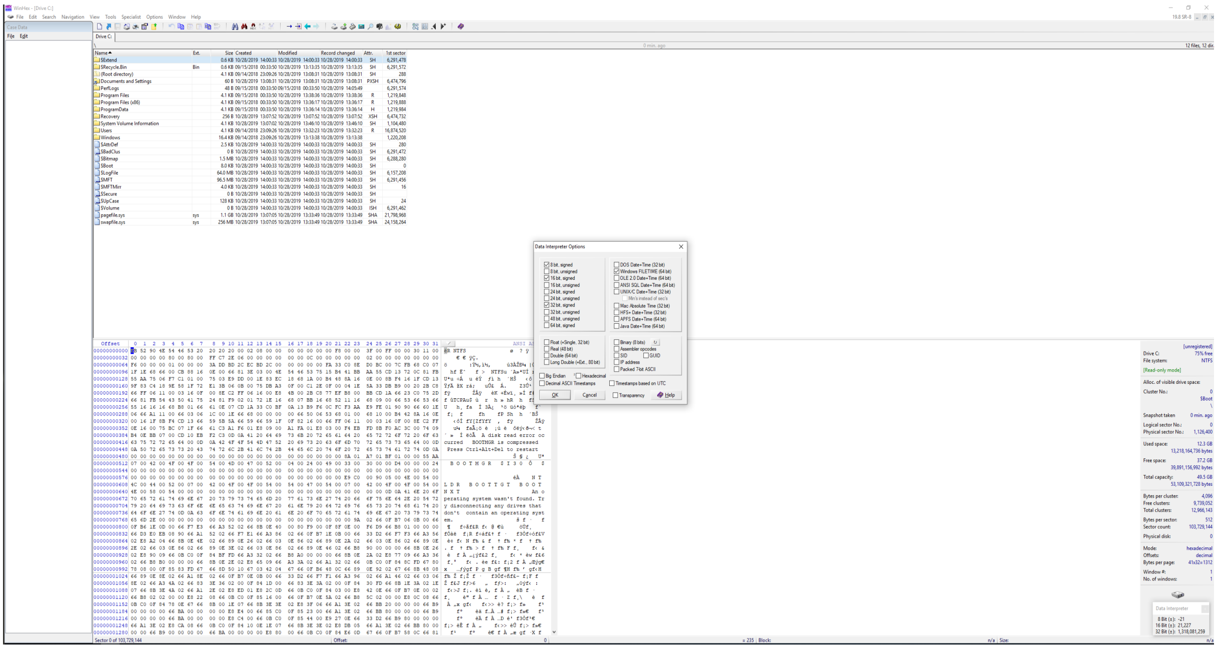
Select Disk

- Logical Volumes/Partitions
  - (C:, 49.5 GB), HD0
  - VBox_GAs_6.0.14 (D:)
- Physical Storage Devices
  - HD0: VBOX HARDDISK (50.0 GB, SATA)

□ List volumes that do not have drive letters

Figure 9: Choosing the `C:` drive as our disk to open.

The data interpreter must be set to `Win32 FILETIME (64 bit)`, via the `Options->Data Interpreter` section of the menu.



Data Interpreter Options

☑ 8 bit, signed
□ 8 bit, unsigned
☑ 16 bit, signed
□ 16 bit, unsigned
□ 24 bit, signed
□ 24 bit, unsigned
☑ 32 bit, signed
□ 32 bit, unsigned
□ 48 bit, unsigned
□ 64 bit, signed

□ DOS Date+Time (32 bit)
☑ Windows FILETIME (64 bit)
□ OLE 2.0 Date+Time (64 bit)
□ ANSI SQL Date+Time (64 bit)
□ UNIX/C Date+Time (32 bit)
□ Min's instead of sec's
□ Mac Absolute Time (32 bit)
□ HFS+ Date+Time (32 bit)
□ APFS Date+Time (64 bit)
□ Java Date+Time (64 bit)

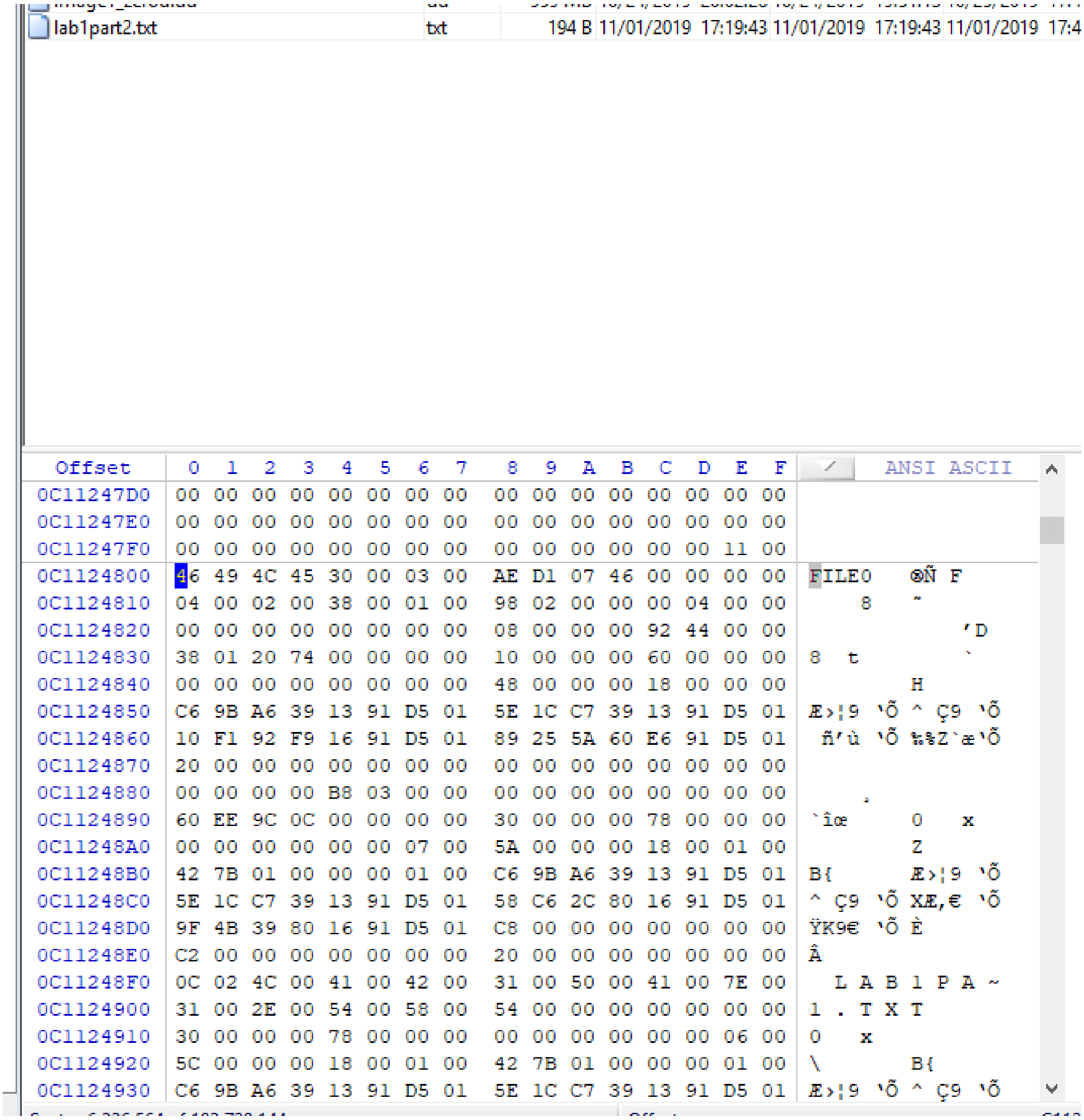
□ Float (=Single, 32 bit)
□ Real (48 bit)
□ Double (64 bit)
□ Long Double (=Ext., 80 bit)

□ Binary (8 bits)
□ Assembler opcodes
□ SID □ GUID
□ IP address
□ Packed 7-bit ASCII

□ Big Endian □ Hexadecimal
□ Decimal ASCII Timestamps
□ Timestamps based on UTC
□ Transparency

Figure 10: Set Data Interpreter to `Win32 FILETIME (64 bit)`.

At this point we open up `lab1part2.txt`, and click at the beginning of the record.

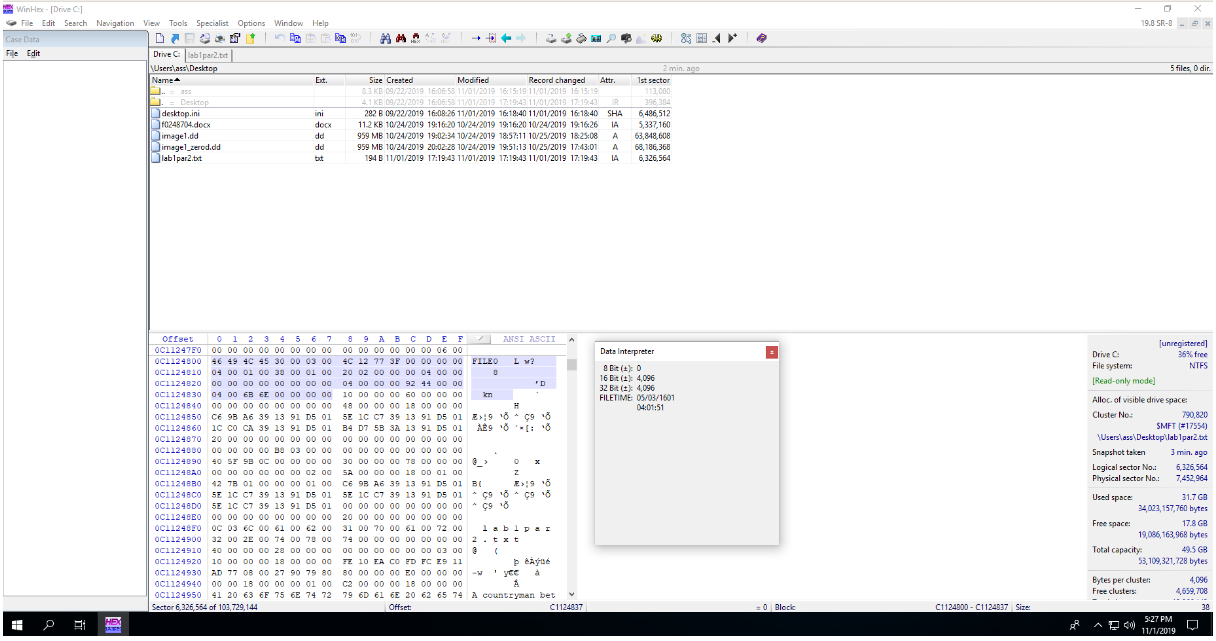


lab1part2.txt txt 194 B 11/01/2019 17:19:43 11/01/2019 17:19:43 11/01/2019 17:4

```
  Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F    ANSI ASCII
0C11247D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0C11247E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0C11247F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 11 00
0C1124800  46 49 4C 45 30 00 03 00  AE D1 07 46 00 00 00 00  FILE0   ®Ñ F
0C1124810  04 00 02 00 38 00 01 00  98 02 00 00 00 04 00 00      8   ˜
0C1124820  00 00 00 00 00 00 00 00  08 00 00 00 92 44 00 00              ’D
0C1124830  38 01 20 74 00 00 00 00  10 00 00 00 60 00 00 00  8  t        `
0C1124840  00 00 00 00 00 00 00 00  48 00 00 00 18 00 00 00          H
0C1124850  C6 9B A6 39 13 91 D5 01  5E 1C C7 39 13 91 D5 01  Æ›¦9 ‘Õ ^ Ç9 ‘Õ
0C1124860  10 F1 92 F9 16 91 D5 01  89 25 5A 60 E6 91 D5 01   ñ’ù ‘Õ ‰%Z`æ‘Õ
0C1124870  20 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0C1124880  00 00 00 00 B8 03 00 00  00 00 00 00 00 00 00 00      ¸
0C1124890  60 EE 9C 0C 00 00 00 00  30 00 00 00 78 00 00 00  `îœ     0   x
0C11248A0  00 00 00 00 00 00 07 00  5A 00 00 00 18 00 01 00          Z
0C11248B0  42 7B 01 00 00 00 01 00  C6 9B A6 39 13 91 D5 01  B{      Æ›¦9 ‘Õ
0C11248C0  5E 1C C7 39 13 91 D5 01  58 C6 2C 80 16 91 D5 01  ^ Ç9 ‘Õ XÆ,€ ‘Õ
0C11248D0  9F 4B 39 80 16 91 D5 01  C8 00 00 00 00 00 00 00  ŸK9€ ‘Õ È
0C11248E0  C2 00 00 00 00 00 00 00  20 00 00 00 00 00 00 00  Â
0C11248F0  0C 02 4C 00 41 00 42 00  31 00 50 00 41 00 7E 00    L A B 1 P A ~
0C1124900  31 00 2E 00 54 00 58 00  54 00 00 00 00 00 00 00  1 . T X T
0C1124910  30 00 00 00 78 00 00 00  00 00 00 00 00 00 06 00  0   x
0C1124920  5C 00 00 00 18 00 01 00  42 7B 01 00 00 00 01 00  \       B{
0C1124930  C6 9B A6 39 13 91 D5 01  5E 1C C7 39 13 91 D5 01  Æ›¦9 ‘Õ ^ Ç9 ‘Õ
```

Figure 11: Beginning of the record for `lab1part2.txt`.

In order to find the start of the `0x10` attribute, we click the beginning of the MFT record and drag until the offset counter is `0x38`.



WinHex - [Drive C:]
File Edit Search Navigation View Tools Specialist Options Window Help
Case Data
File Edit
Drive C: lab1par2.txt

\Users\ass\Desktop   2 min. ago   5 files, 0 dir.

Name	Ext.	Size	Created	Modified	Record changed	Attr.	1st sector
.. = ass		8.3 KB	09/22/2019 16:06:58	11/01/2019 16:15:19	11/01/2019 16:15:19		113,080
. = Desktop		4.1 KB	09/22/2019 16:06:58	11/01/2019 17:19:43	11/01/2019 17:19:43	IR	396,384
desktop.ini	ini	282 B	09/22/2019 16:08:26	11/01/2019 16:18:40	11/01/2019 16:18:40	SHA	6,486,512
f0248704.docx	docx	11.2 KB	10/24/2019 19:16:20	10/24/2019 19:16:20	10/24/2019 19:16:26	IA	5,337,160
image1.dd	dd	959 MB	10/24/2019 19:02:34	10/24/2019 18:57:11	10/25/2019 18:25:08	A	63,848,608
image1_zerod.dd	dd	959 MB	10/24/2019 20:02:28	10/24/2019 19:51:13	10/25/2019 17:43:01	A	68,186,368
lab1par2.txt	txt	194 B	11/01/2019 17:19:43	11/01/2019 17:19:43	11/01/2019 17:19:43	IA	6,326,564

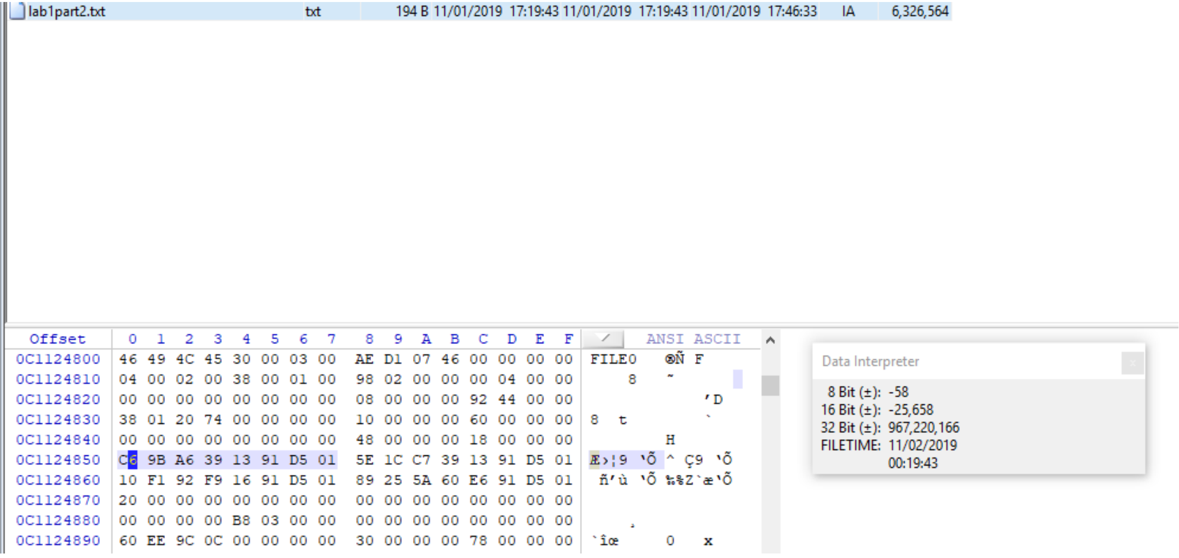
```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
0C11247F0 00 00 00 00 00 00 00 00  00 00 00 00 00 00 06 00
0C1124800 46 49 4C 45 30 00 03 00  4C 12 77 3F 00 00 00 00  FILE0   L w?
0C1124810 04 00 01 00 38 00 01 00  20 02 00 00 00 04 00 00      8
0C1124820 00 00 00 00 00 00 00 00  04 00 00 00 92 44 00 00              ’D
0C1124830 04 00 6B 6E 00 00 00 00  10 00 00 00 60 00 00 00    kn        `
0C1124840 00 00 00 00 00 00 00 00  48 00 00 00 18 00 00 00          H
0C1124850 C6 9B A6 39 13 91 D5 01  5E 1C C7 39 13 91 D5 01  Æ›¦9 ‘Õ ^ Ç9 ‘Õ
0C1124860 1C C0 CA 39 13 91 D5 01  B4 D7 5B 3A 13 91 D5 01   ÀÊ9 ‘Õ ´×[: ‘Õ
0C1124870 20 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0C1124880 00 00 00 00 B8 03 00 00  00 00 00 00 00 00 00 00      ¸
0C1124890 40 5F 9B 0C 00 00 00 00  30 00 00 00 78 00 00 00  @_›     0   x
0C11248A0 00 00 00 00 00 00 02 00  5A 00 00 00 18 00 01 00          Z
0C11248B0 42 7B 01 00 00 00 01 00  C6 9B A6 39 13 91 D5 01  B{      Æ›¦9 ‘Õ
0C11248C0 5E 1C C7 39 13 91 D5 01  5E 1C C7 39 13 91 D5 01  ^ Ç9 ‘Õ ^ Ç9 ‘Õ
0C11248D0 5E 1C C7 39 13 91 D5 01  00 00 00 00 00 00 00 00  ^ Ç9 ‘Õ
0C11248E0 00 00 00 00 00 00 00 00  20 00 00 00 00 00 00 00
0C11248F0 0C 03 6C 00 61 00 62 00  31 00 70 00 61 00 72 00    l a b 1 p a r
0C1124900 32 00 2E 00 74 00 78 00  74 00 00 00 00 00 00 00  2 . t x t
0C1124910 40 00 00 00 28 00 00 00  00 00 00 00 00 00 03 00  @   (
0C1124920 10 00 00 00 18 00 00 00  FE 10 EA C0 FD FC E9 11          þ êÀýüé
0C1124930 AD 77 08 00 27 90 79 80  80 00 00 00 E0 00 00 00  -w  ' y€€   à
0C1124940 00 00 18 00 00 00 01 00  C2 00 00 00 18 00 00 00          Â
0C1124950 41 20 63 6F 75 6E 74 72  79 6D 61 6E 20 62 65 74  A countryman bet
Sector 6,326,564 of 103,729,144     Offset:     C1124837     = 0   Block:     C1124800 - C1124837   Size:   38
```

Data Interpreter
8 Bit (±): 0
16 Bit (±): 4,096
32 Bit (±): 4,096
FILETIME: 05/03/1601 04:01:51

[unregistered]
Drive C: 36% free
File system: NTFS
[Read-only mode]
Alloc. of visible drive space:
Cluster No.: 790,820
$MFT (#17554)
\Users\ass\Desktop\lab1par2.txt
Snapshot taken 3 min. ago
Logical sector No.: 6,326,564
Physical sector No.: 7,452,964
Used space: 31.7 GB
34,023,157,760 bytes
Free space: 17.8 GB
19,086,163,968 bytes
Total capacity: 49.5 GB
53,109,321,728 bytes
Bytes per cluster: 4,096
Free clusters: 4,659,708

Figure 12: The start of attribute `0x10` at offset `0x38`.

The file's created date and time can be found at offset `0x10` to `0x1F` from the beginning of attribute `0x10`.



lab1par2.txt	txt	194 B	11/01/2019	17:19:43 11/01/2019	17:19:43 11/01/2019	17:46:33	IA	6,326,564

```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
0C1124800 46 49 4C 45 30 00 03 00  AE D1 07 46 00 00 00 00  FILE0   ®Ñ F
0C1124810 04 00 02 00 38 00 01 00  98 02 00 00 00 04 00 00      8   ˜
0C1124820 00 00 00 00 00 00 00 00  08 00 00 00 92 44 00 00              ’D
0C1124830 38 01 20 74 00 00 00 00  10 00 00 00 60 00 00 00  8  t        `
0C1124840 00 00 00 00 00 00 00 00  48 00 00 00 18 00 00 00          H
0C1124850 C6 9B A6 39 13 91 D5 01  5E 1C C7 39 13 91 D5 01  Æ›¦9 ‘Õ ^ Ç9 ‘Õ
0C1124860 10 F1 92 F9 16 91 D5 01  89 25 5A 60 E6 91 D5 01   ñ’ù ‘Õ ‰%Z`æ‘Õ
0C1124870 20 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0C1124880 00 00 00 00 B8 03 00 00  00 00 00 00 00 00 00 00      ¸
0C1124890 60 EE 9C 0C 00 00 00 00  30 00 00 00 78 00 00 00  `îœ     0   x
```

Data Interpreter
8 Bit (±): -58
16 Bit (±): -25,658
32 Bit (±): 967,220,166
FILETIME: 11/02/2019 00:19:43

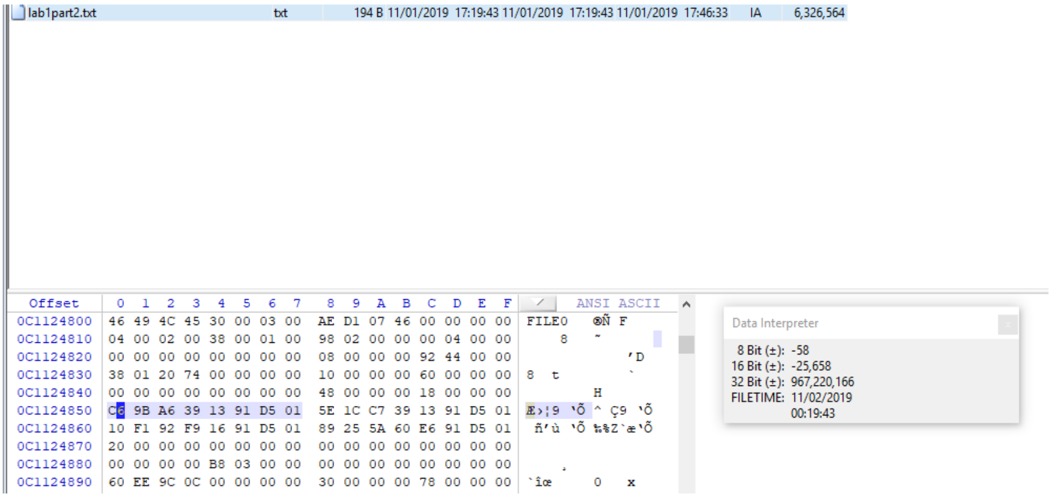
Figure 13: File created date and time.

Now, we repeat the steps in Figure 13 to answer the questions found below.

Questions

1. According to the data interpreter, what is the file create date and time for the file `lab1part.txt`?

   - The file created date and time is `11/02/2019 00:19:43` according to the data interpreter.



lab1part2.txt txt 194 B 11/01/2019 17:19:43 11/01/2019 17:19:43 11/01/2019 17:46:33 IA 6,326,564

```
Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
0C1124800  46 49 4C 45 30 00 03 00  AE D1 07 46 00 00 00 00  FILE0   ®Ñ F
0C1124810  04 00 02 00 38 00 01 00  98 02 00 00 00 04 00 00      8   ˜
0C1124820  00 00 00 00 00 00 00 00  08 00 00 00 92 44 00 00              ’D
0C1124830  38 01 20 74 00 00 00 00  10 00 00 00 60 00 00 00  8  t        `
0C1124840  00 00 00 00 00 00 00 00  48 00 00 00 18 00 00 00          H
0C1124850  C6 9B A6 39 13 91 D5 01  5E 1C C7 39 13 91 D5 01  Æ›¦9 ‘Õ ^ Ç9 ‘Õ
0C1124860  10 F1 92 F9 16 91 D5 01  89 25 5A 60 E6 91 D5 01   ñ’ù ‘Õ ‰%Z`æ‘Õ
0C1124870  20 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0C1124880  00 00 00 00 B8 03 00 00  00 00 00 00 00 00 00 00      ¸
0C1124890  60 EE 9C 0C 00 00 00 00  30 00 00 00 78 00 00 00  `îœ     0   x
```

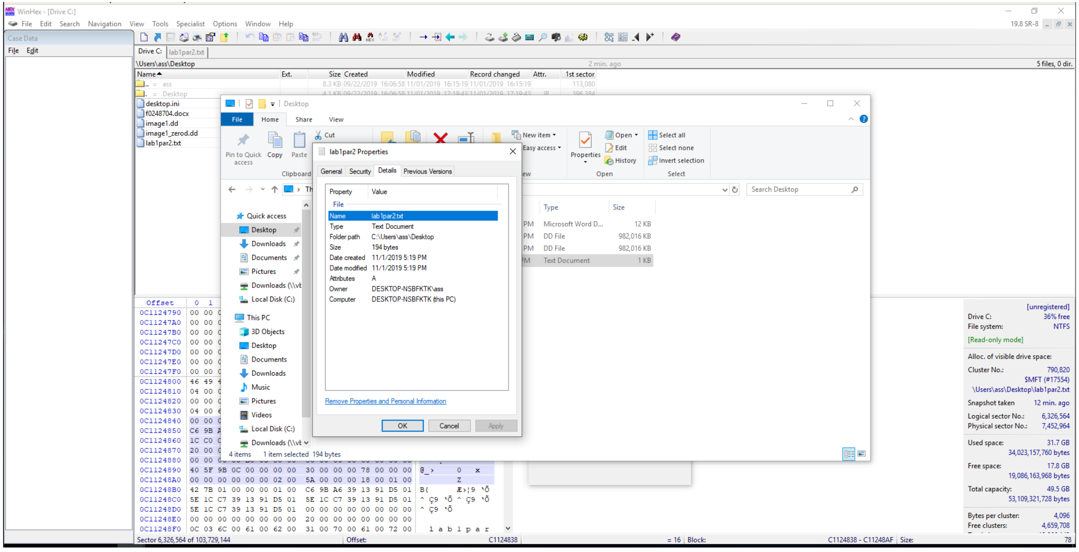
Data Interpreter

8 Bit (±): -58
16 Bit (±): -25,658
32 Bit (±): 967,220,166
FILETIME: 11/02/2019 00:19:43

Figure 14: Data Interpreter's file created date and time.

2. 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.

   - The File Explorer's file created date and time is `11/01/2019 at 5:19PM`.



lab1par2 Properties

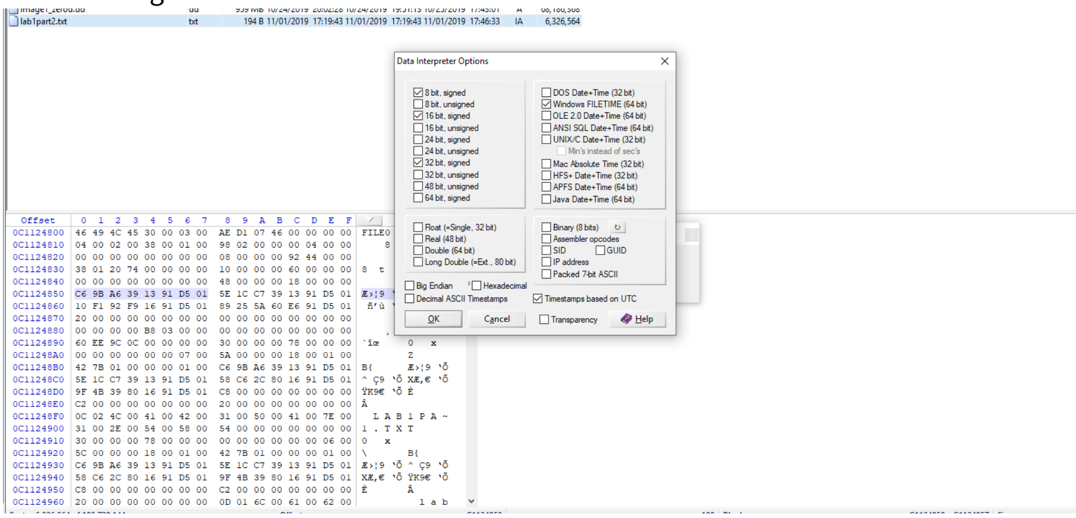
General | Security | Details | Previous Versions

Property	Value
File	
Name	lab1par2.txt
Type	Text Document
Folder path	C:\Users\ass\Desktop
Size	194 bytes
Date created	11/1/2019 5:19 PM
Date modified	11/1/2019 5:19 PM
Attributes	A
Owner	DESKTOP-NSBFKTK\ass
Computer	DESKTOP-NSBFKTK (this PC)

Figure 15: File Explorer's created date and time.

3. Compare this time and the time you got from data interpreter. Are they the same? If not, why?

    - The time for the Data Interpreter is ahead of what the File Explorer says. When we go to `Options->Data Interpreter` and check the `Timestamps based on UTC` box, the dates actually do match. The reason they did not match previously is because the File Explorer was basing it off UTC, and the Data Interpreter was not. See below the screenshots on correcting this.



```
lab1part2.txt    txt    194 B 11/01/2019 17:19:43 11/01/2019 17:19:43 11/01/2019 17:46:33    IA    6,326,564
```

Data Interpreter Options

☑ 8 bit, signed
☐ 8 bit, unsigned
☑ 16 bit, signed
☐ 16 bit, unsigned
☐ 24 bit, signed
☐ 24 bit, unsigned
☑ 32 bit, signed
☐ 32 bit, unsigned
☐ 48 bit, unsigned
☐ 64 bit, signed

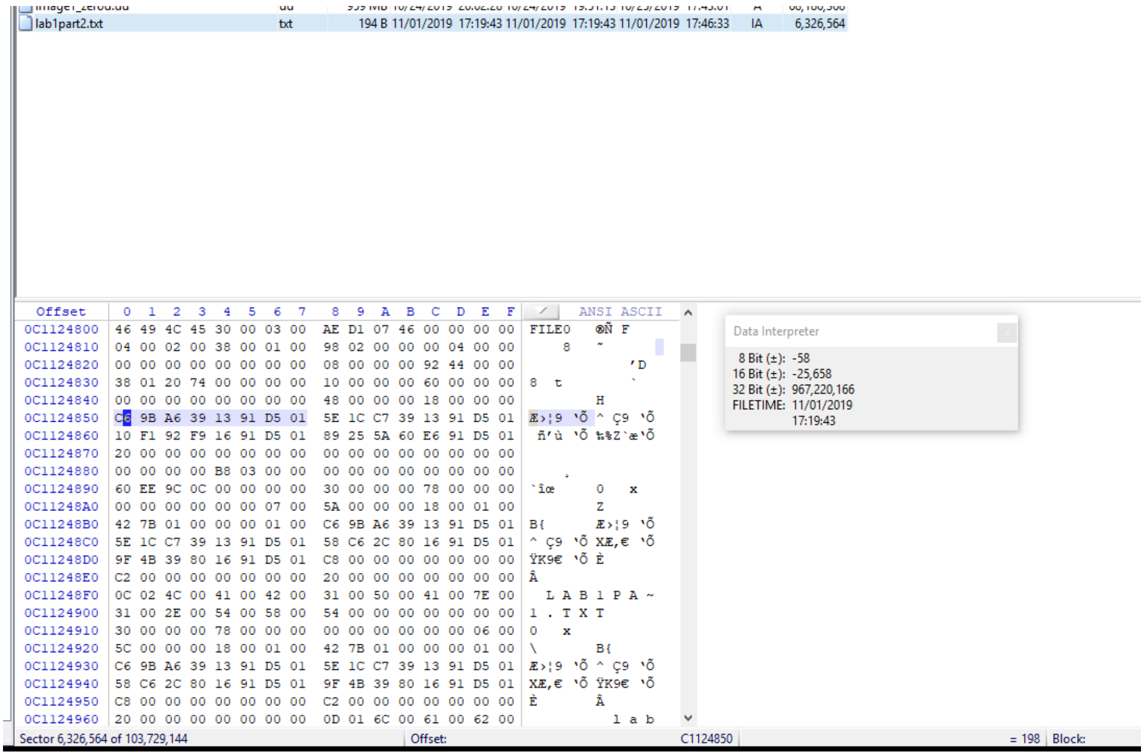
☐ DOS Date+Time (32 bit)
☑ Windows FILETIME (64 bit)
☐ OLE 2.0 Date+Time (64 bit)
☐ ANSI SQL Date+Time (64 bit)
☐ UNIX/C Date+Time (32 bit)
☐ Min's instead of sec's
☐ Mac Absolute Time (32 bit)
☐ HFS+ Date+Time (32 bit)
☐ APFS Date+Time (64 bit)
☐ Java Date+Time (64 bit)

☐ Float (=Single, 32 bit)
☐ Real (48 bit)
☐ Double (64 bit)
☐ Long Double (=Ext., 80 bit)

☐ Binary (8 bits)
☐ Assembler opcodes
☐ SID ☐ GUID
☐ IP address
☐ Packed 7-bit ASCII

☐ Big Endian ☐ Hexadecimal
☐ Decimal ASCII Timestamps
☑ Timestamps based on UTC

Figure 16: Selecting `Timestamps based on UTC` for Data Interpreter.



```
lab1part2.txt    txt    194 B 11/01/2019 17:19:43 11/01/2019 17:19:43 11/01/2019 17:46:33    IA    6,326,564
```

```
  Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F      ANSI ASCII
0C1124800  46 49 4C 45 30 00 03 00  AE D1 07 46 00 00 00 00  FILE0   ®Ñ F
0C1124810  04 00 02 00 38 00 01 00  98 02 00 00 00 04 00 00      8   ˜
0C1124820  00 00 00 00 00 00 00 00  08 00 00 00 92 44 00 00             ’D
0C1124830  38 01 20 74 00 00 00 00  10 00 00 00 60 00 00 00  8  t       `
0C1124840  00 00 00 00 00 00 00 00  48 00 00 00 18 00 00 00          H
0C1124850  C6 9B A6 39 13 91 D5 01  5E 1C C7 39 13 91 D5 01  Æ›¦9 ‘Õ ^ Ç9 ‘Õ
0C1124860  10 F1 92 F9 16 91 D5 01  89 25 5A 60 E6 91 D5 01   ñ’ù ‘Õ ‰%Z`æ‘Õ
0C1124870  20 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0C1124880  00 00 00 00 B8 03 00 00  00 00 00 00 00 00 00 00      ¸
0C1124890  60 EE 9C 0C 00 00 00 00  30 00 00 00 78 00 00 00  `îœ     0   x
0C11248A0  00 00 00 00 00 00 07 00  5A 00 00 00 18 00 01 00          Z
0C11248B0  42 7B 01 00 00 00 01 00  C6 9B A6 39 13 91 D5 01  B{      Æ›¦9 ‘Õ
0C11248C0  5E 1C C7 39 13 91 D5 01  58 C6 2C 80 16 91 D5 01  ^ Ç9 ‘Õ XÆ,€ ‘Õ
0C11248D0  9F 4B 39 80 16 91 D5 01  C8 00 00 00 00 00 00 00  ŸK9€ ‘Õ È
0C11248E0  C2 00 00 00 00 00 00 00  20 00 00 00 00 00 00 00  Â
0C11248F0  0C 02 4C 00 41 00 42 00  31 00 50 00 41 00 7E 00    L A B 1 P A ~
0C1124900  31 00 2E 00 54 00 58 00  54 00 00 00 00 00 00 00  1 . T X T
0C1124910  30 00 00 00 78 00 00 00  00 00 00 00 00 00 06 00  0   x
0C1124920  5C 00 00 00 18 00 01 00  42 7B 01 00 00 00 01 00  \       B{
0C1124930  C6 9B A6 39 13 91 D5 01  5E 1C C7 39 13 91 D5 01  Æ›¦9 ‘Õ ^ Ç9 ‘Õ
0C1124940  58 C6 2C 80 16 91 D5 01  9F 4B 39 80 16 91 D5 01  XÆ,€ ‘Õ ŸK9€ ‘Õ
0C1124950  C8 00 00 00 00 00 00 00  C2 00 00 00 00 00 00 00  È       Â
0C1124960  20 00 00 00 00 00 00 00  0D 01 6C 00 61 00 62 00            l a b
```

Data Interpreter

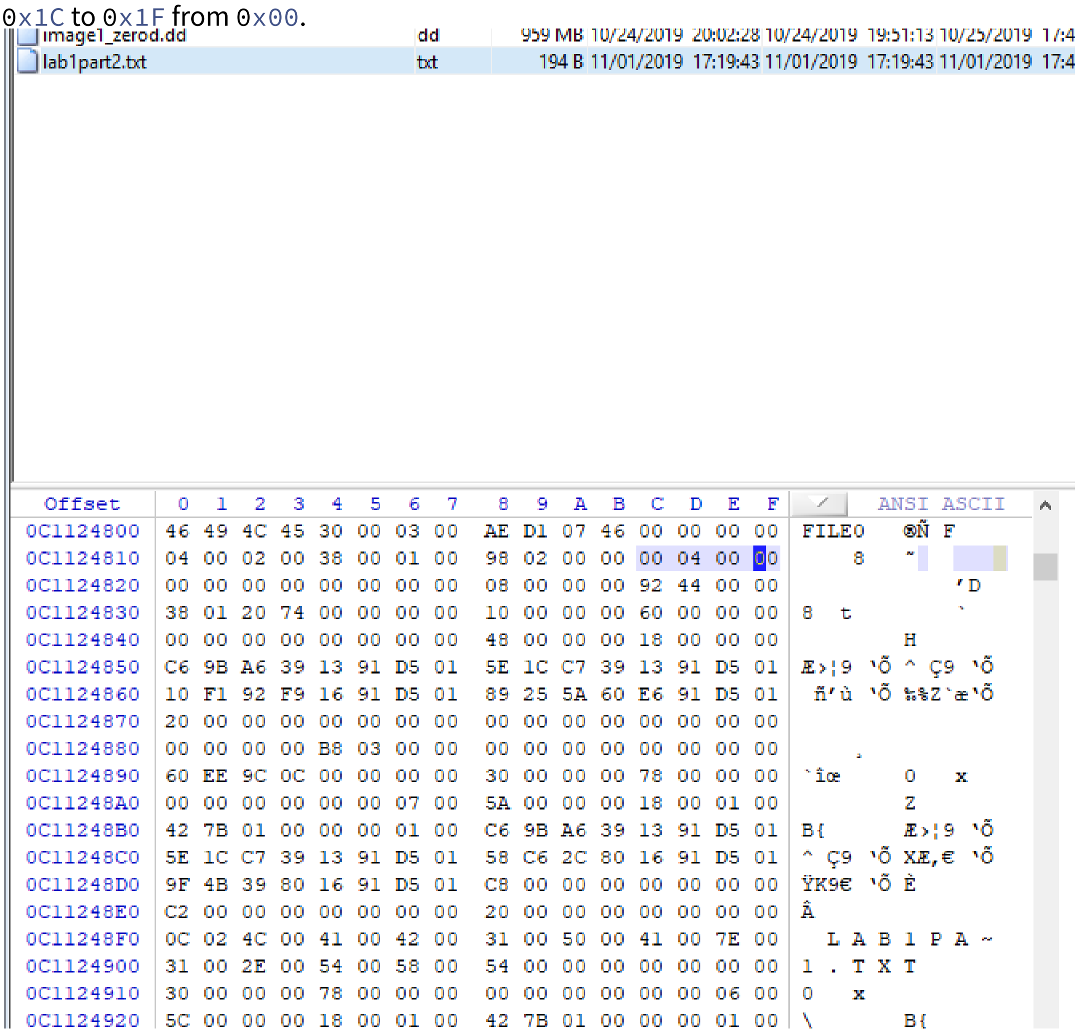
```
  8 Bit (±):  -58
 16 Bit (±):  -25,658
 32 Bit (±):  967,220,166
 FILETIME:    11/01/2019
              17:19:43
```

Sector 6,326,564 of 103,729,144 | Offset: C1124850 | = 198 | Block:

Figure 17: Now the file created date and times both match at 5:19PM November 1st 2019.

4. What is the size of the MFT record?

   - The size of the MTF record is, in big endian, is `00 00 04 00`. We can find that at offset `0x1C` to `0x1F` from `0x00`.

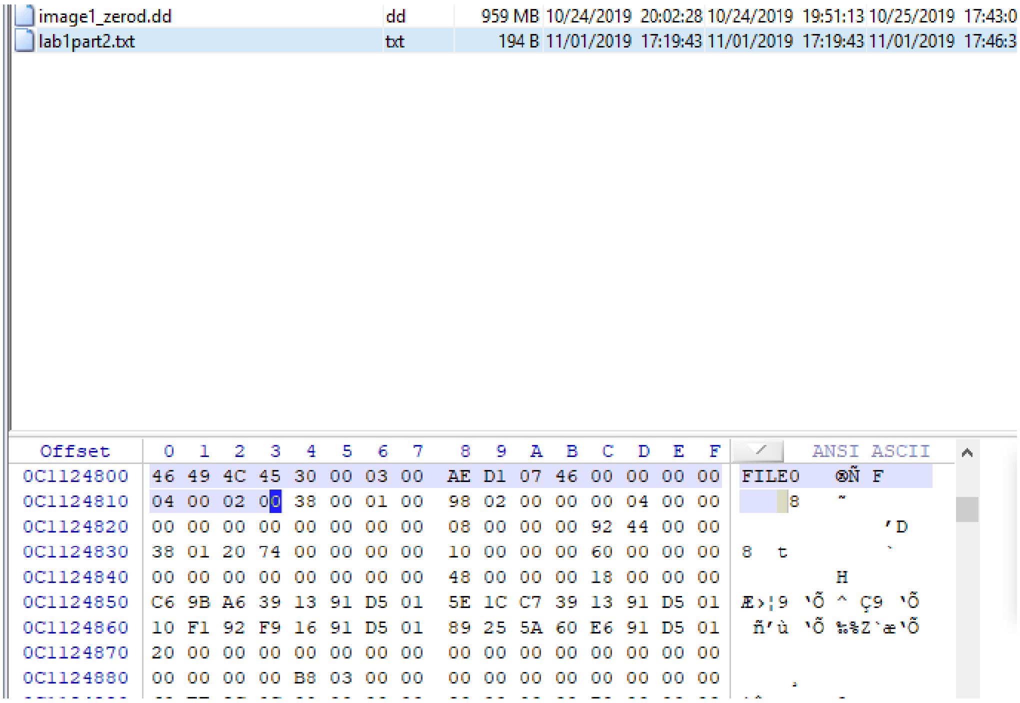


```
image1_zerod.dd    dd    959 MB 10/24/2019 20:02:28 10/24/2019 19:51:13 10/25/2019 17:4
lab1part2.txt      txt    194 B 11/01/2019 17:19:43 11/01/2019 17:19:43 11/01/2019 17:4

  Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
0C1124800   46 49 4C 45 30 00 03 00  AE D1 07 46 00 00 00 00   FILE0   ®Ñ F
0C1124810   04 00 02 00 38 00 01 00  98 02 00 00 00 04 00 00       8   ˜
0C1124820   00 00 00 00 00 00 00 00  08 00 00 00 92 44 00 00               ’D
0C1124830   38 01 20 74 00 00 00 00  10 00 00 00 60 00 00 00   8  t        `
0C1124840   00 00 00 00 00 00 00 00  48 00 00 00 18 00 00 00           H
0C1124850   C6 9B A6 39 13 91 D5 01  5E 1C C7 39 13 91 D5 01   Æ›¦9 ‘Õ ^ Ç9 ‘Õ
0C1124860   10 F1 92 F9 16 91 D5 01  89 25 5A 60 E6 91 D5 01    ñ’ù ‘Õ ‰%Z`æ‘Õ
0C1124870   20 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0C1124880   00 00 00 00 B8 03 00 00  00 00 00 00 00 00 00 00       ¸
0C1124890   60 EE 9C 0C 00 00 00 00  30 00 00 00 78 00 00 00   `îœ     0   x
0C11248A0   00 00 00 00 00 00 07 00  5A 00 00 00 18 00 01 00           Z
0C11248B0   42 7B 01 00 00 00 01 00  C6 9B A6 39 13 91 D5 01   B{      Æ›¦9 ‘Õ
0C11248C0   5E 1C C7 39 13 91 D5 01  58 C6 2C 80 16 91 D5 01   ^ Ç9 ‘Õ XÆ,€ ‘Õ
0C11248D0   9F 4B 39 80 16 91 D5 01  C8 00 00 00 00 00 00 00   ŸK9€ ‘Õ È
0C11248E0   C2 00 00 00 00 00 00 00  20 00 00 00 00 00 00 00   Â
0C11248F0   0C 02 4C 00 41 00 42 00  31 00 50 00 41 00 7E 00     L A B 1 P A ~
0C1124900   31 00 2E 00 54 00 58 00  54 00 00 00 00 00 00 00   1 . T X T
0C1124910   30 00 00 00 78 00 00 00  00 00 00 00 00 00 06 00   0   x
0C1124920   5C 00 00 00 18 00 01 00  42 7B 01 00 00 00 01 00   \       B{
```

Figure 18: The size of the MFT record.

5. What is the length of the header for the MFT record?

   - The header length for the MFT record is `0x38`. This can be found at offset `0x14` from `0x00`.

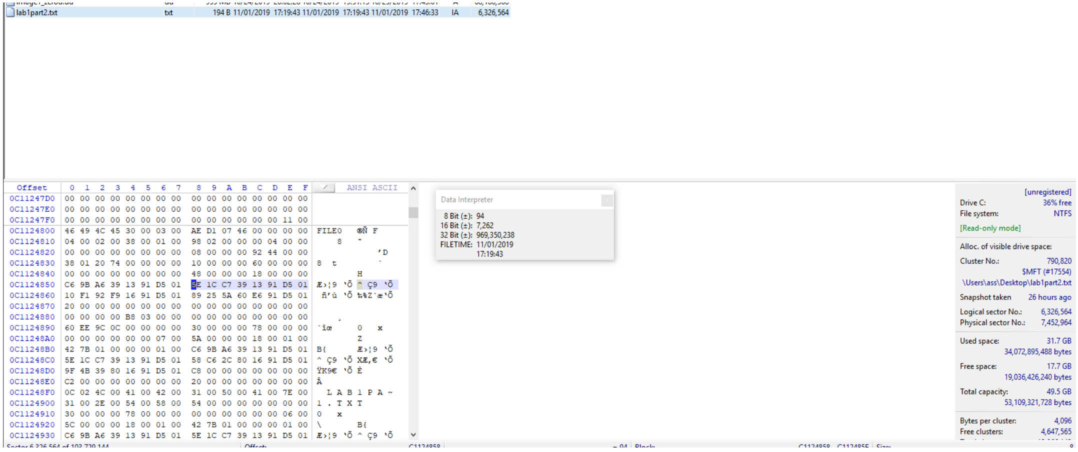


```
image1_zerod.dd   dd   959 MB 10/24/2019  20:02:28 10/24/2019  19:51:13 10/25/2019  17:43:0
lab1part2.txt     txt   194 B 11/01/2019  17:19:43 11/01/2019  17:19:43 11/01/2019  17:46:3

  Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F    ANSI ASCII
0C1124800  46 49 4C 45 30 00 03 00  AE D1 07 46 00 00 00 00  FILE0   ®Ñ F
0C1124810  04 00 02 00 38 00 01 00  98 02 00 00 00 04 00 00      8   ˜
0C1124820  00 00 00 00 00 00 00 00  08 00 00 00 92 44 00 00            'D
0C1124830  38 01 20 74 00 00 00 00  10 00 00 00 60 00 00 00  8  t       `
0C1124840  00 00 00 00 00 00 00 00  48 00 00 00 18 00 00 00          H
0C1124850  C6 9B A6 39 13 91 D5 01  5E 1C C7 39 13 91 D5 01  Æ›¦9 'Õ ^ Ç9 'Õ
0C1124860  10 F1 92 F9 16 91 D5 01  89 25 5A 60 E6 91 D5 01   ñ'ù 'Õ ‰%Z`æ'Õ
0C1124870  20 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0C1124880  00 00 00 00 B8 03 00 00  00 00 00 00 00 00 00 00      ¸
```

Figure 19: The length of the MFT record's header is `0x38`.

6. What is the file's last modified date and time? Take a screenshot with data interpreter to prove your answer.

    - The file's last modified date and time are `11/01/2019 17:19:43`. We can find that information at offset `0x20` to `0x27` from `0x10`. It should be noted that this is with the box for `Timestamps based on UTC` selected.



```
lab1part2.txt   txt   194 B 11/01/2019  17:19:43 11/01/2019  17:19:43 11/01/2019  17:46:33   IA   6,326,564

  Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F    ANSI ASCII
0C11247D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0C11247E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0C11247F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 11 00
0C1124800  46 49 4C 45 30 00 03 00  AE D1 07 46 00 00 00 00  FILE0   ®Ñ F
0C1124810  04 00 02 00 38 00 01 00  98 02 00 00 00 04 00 00      8   ˜
0C1124820  00 00 00 00 00 00 00 00  08 00 00 00 92 44 00 00            'D
0C1124830  38 01 20 74 00 00 00 00  10 00 00 00 60 00 00 00  8  t       `
0C1124840  00 00 00 00 00 00 00 00  48 00 00 00 18 00 00 00          H
0C1124850  C6 9B A6 39 13 91 D5 01  5E 1C C7 39 13 91 D5 01  Æ›¦9 'Õ ^ Ç9 'Õ
0C1124860  10 F1 92 F9 16 91 D5 01  89 25 5A 60 E6 91 D5 01   ñ'ù 'Õ ‰%Z`æ'Õ
0C1124870  20 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0C1124880  00 00 00 00 B8 03 00 00  00 00 00 00 00 00 00 00      ¸
0C1124890  60 EE 9C 0C 00 00 00 00  30 00 00 00 78 00 00 00  `îœ     0   x
0C11248A0  00 00 00 00 00 00 07 00  5A 00 00 00 18 00 01 00          Z
0C11248B0  42 7B 01 00 00 00 01 00  C6 9B A6 39 13 91 D5 01  B{      Æ›¦9 'Õ
0C11248C0  5E 1C C7 39 13 91 D5 01  58 C6 2C 80 16 91 D5 01  ^ Ç9 'Õ XÆ,€ 'Õ
0C11248D0  9F 4B 39 80 16 91 D5 01  C8 00 00 00 00 00 00 00  ŸK9€ 'Õ È
0C11248E0  C2 00 00 00 00 00 00 00  20 00 00 00 00 00 00 00  Â
0C11248F0  0C 02 4C 00 41 00 42 00  31 00 50 00 41 00 7E 00    L A B 1 P A ~
0C1124900  31 00 2E 00 54 00 58 00  54 00 00 00 00 00 00 00  1 . T X T
0C1124910  30 00 00 00 78 00 00 00  00 00 00 00 00 00 06 00  0   x
0C1124920  5C 00 00 00 18 00 01 00  42 7B 01 00 00 00 01 00  \       B{
0C1124930  C6 9B A6 39 13 91 D5 01  5E 1C C7 39 13 91 D5 01  Æ›¦9 'Õ ^ Ç9 'Õ
```

Data Interpreter
8 Bit (±): 94
16 Bit (±): 7,262
32 Bit (±): 969,350,238
FILETIME: 11/01/2019 17:19:43

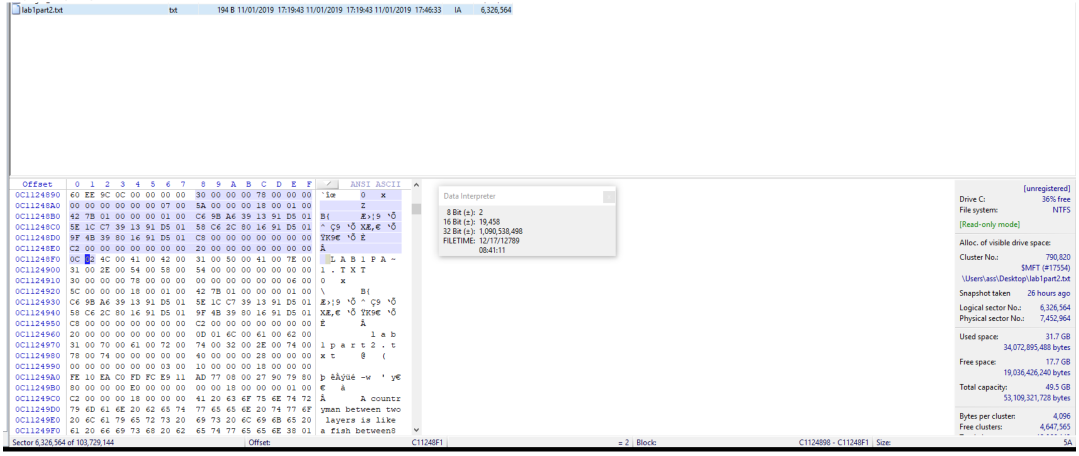
[unregistered]
Drive C: 36% free
File system: NTFS
[Read-only mode]
Alloc. of visible drive space:
Cluster No.: 790,820
$MFT (#17554)
\Users\ass\Desktop\lab1part2.txt
Snapshot taken 26 hours ago
Logical sector No.: 6,326,564
Physical sector No.: 7,452,964
Used space: 31.7 GB
34,072,895,488 bytes
Free space: 17.7 GB
19,036,426,240 bytes
Total capacity: 49.5 GB
53,109,321,728 bytes
Bytes per cluster: 4,096
Free clusters: 4,647,565

Figure 20: File last modified date, based on UTC.

7. What is the file name? In which attribute and at what position can you find it?

    - As we've learned from lecture 5's handout, if the file name is longer than eight characters there are two attributes 0x30. Since our file name is longer than 8 characters we fall into this case. That means we have a short file name, and a long file name.

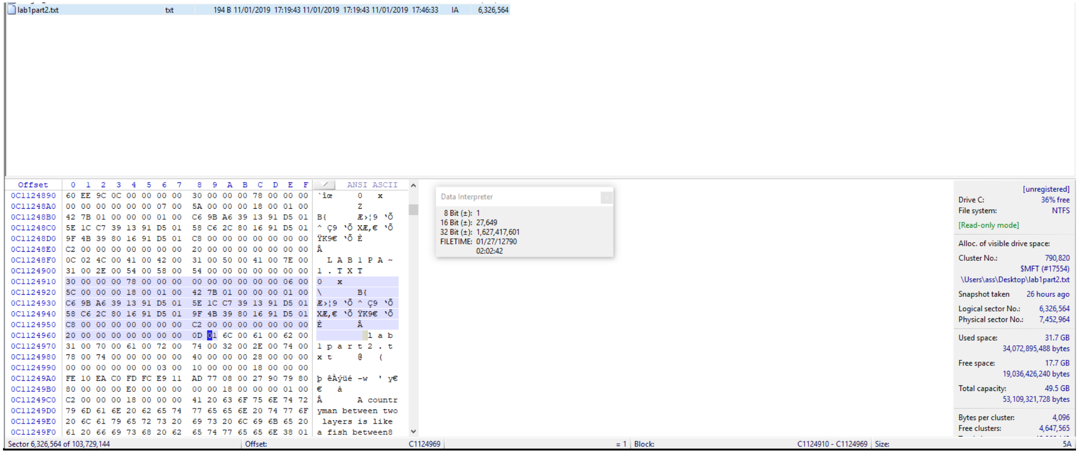
- Short file names are found at offset 0x5A from the first 0x30 attribute. Our short file name is LAB1PA~1.TXT.



```
lab1part2.txt   txt   194 B 11/01/2019 17:19:43 11/01/2019 17:19:43 11/01/2019 17:46:33   IA   6,326,564

Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
0C1124890  60 EE 9C 0C 00 00 00 00  30 00 00 00 78 00 00 00   `îœ     0   x
0C11248A0  00 00 00 00 00 00 07 00  5A 00 00 00 18 00 01 00           Z
0C11248B0  42 7B 01 00 00 00 01 00  C6 9B A6 39 13 91 D5 01   B{      Æ›¦9 ‘Õ
0C11248C0  5E 1C C7 39 13 91 D5 01  58 C6 2C 80 16 91 D5 01   ^ Ç9 ‘Õ XÆ,€ ‘Õ
0C11248D0  9F 4B 39 80 16 91 D5 01  C8 00 00 00 00 00 00 00   ŸK9€ ‘Õ È
0C11248E0  C2 00 00 00 00 00 00 00  20 00 00 00 00 00 00 00   Â
0C11248F0  0C 02 4C 00 41 00 42 00  31 00 50 00 41 00 7E 00     L A B 1 P A ~
0C1124900  31 00 2E 00 54 00 58 00  54 00 00 00 00 00 00 00   1 . T X T
0C1124910  30 00 00 00 78 00 00 00  00 00 00 00 00 00 06 00   0   x
0C1124920  5C 00 00 00 18 00 01 00  42 7B 01 00 00 00 01 00   \       B{
0C1124930  C6 9B A6 39 13 91 D5 01  5E 1C C7 39 13 91 D5 01   Æ›¦9 ‘Õ ^ Ç9 ‘Õ
0C1124940  58 C6 2C 80 16 91 D5 01  9F 4B 39 80 16 91 D5 01   XÆ,€ ‘Õ ŸK9€ ‘Õ
0C1124950  C8 00 00 00 00 00 00 00  C2 00 00 00 00 00 00 00   È       Â
0C1124960  20 00 00 00 00 00 00 00  0D 01 6C 00 61 00 62 00              l a b
0C1124970  31 00 70 00 61 00 72 00  74 00 32 00 2E 00 74 00   1 p a r t 2 . t
0C1124980  78 00 74 00 00 00 00 00  40 00 00 00 28 00 00 00   x t     @   (
0C1124990  00 00 00 00 00 00 03 00  10 00 00 00 18 00 00 00
0C11249A0  FE 10 EA C0 FD FC E9 11  AD 77 08 00 27 90 79 80   þ êÀýüé w  ' y€
0C11249B0  80 00 00 00 E0 00 00 00  00 00 18 00 00 00 01 00   €   à
0C11249C0  C2 00 00 00 18 00 00 00  41 20 63 6F 75 6E 74 72   Â       A countr
0C11249D0  79 6D 61 6E 20 62 65 74  77 65 65 6E 20 74 77 6F   yman between two
0C11249E0  20 6C 61 79 65 72 73 20  69 73 20 6C 69 6B 65 20    layers is like
0C11249F0  61 20 66 69 73 68 20 62  65 74 77 65 65 6E 38 01   a fish between8
Sector 6,326,564 of 103,729,144   Offset:   C11248F1   = 2   Block:   C1124898 - C11248F1   Size:   5A

Data Interpreter
 8 Bit (±): 2
16 Bit (±): 19,458
32 Bit (±): 1,090,538,498
FILETIME:   12/17/12789
            08:41:11

[unregistered]
Drive C:                    36% free
File system:                    NTFS
[Read-only mode]
Alloc. of visible drive space:
Cluster No.:                 790,820
                       $MFT (#17554)
     \Users\ass\Desktop\lab1part2.txt
Snapshot taken          26 hours ago
Logical sector No.:        6,326,564
Physical sector No.:       7,452,964
Used space:                  31.7 GB
              34,072,895,488 bytes
Free space:                  17.7 GB
              19,036,426,240 bytes
Total capacity:              49.5 GB
              53,109,321,728 bytes
Bytes per cluster:             4,096
Free clusters:             4,647,565
```

Figure 21: The short file name at 0x5A from the first 0x30 attribute.

- Long file names are found at offset 0x5A from the second 0x30 attribute. Our short file name is lab1part2.txt.

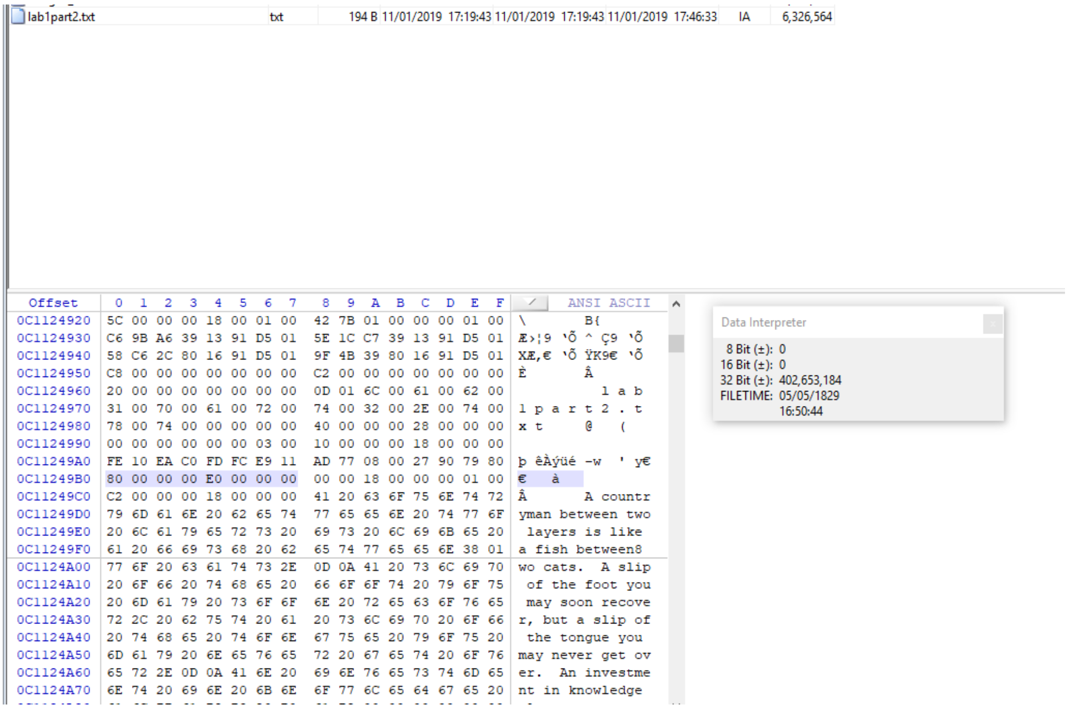


```
lab1part2.txt   txt   194 B 11/01/2019 17:19:43 11/01/2019 17:19:43 11/01/2019 17:46:33   IA   6,326,564

Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
0C1124890  60 EE 9C 0C 00 00 00 00  30 00 00 00 78 00 00 00   `îœ     0   x
0C11248A0  00 00 00 00 00 00 07 00  5A 00 00 00 18 00 01 00           Z
0C11248B0  42 7B 01 00 00 00 01 00  C6 9B A6 39 13 91 D5 01   B{      Æ›¦9 ‘Õ
0C11248C0  5E 1C C7 39 13 91 D5 01  58 C6 2C 80 16 91 D5 01   ^ Ç9 ‘Õ XÆ,€ ‘Õ
0C11248D0  9F 4B 39 80 16 91 D5 01  C8 00 00 00 00 00 00 00   ŸK9€ ‘Õ È
0C11248E0  C2 00 00 00 00 00 00 00  20 00 00 00 00 00 00 00   Â
0C11248F0  0C 02 4C 00 41 00 42 00  31 00 50 00 41 00 7E 00     L A B 1 P A ~
0C1124900  31 00 2E 00 54 00 58 00  54 00 00 00 00 00 00 00   1 . T X T
0C1124910  30 00 00 00 78 00 00 00  00 00 00 00 00 00 06 00   0   x
0C1124920  5C 00 00 00 18 00 01 00  42 7B 01 00 00 00 01 00   \       B{
0C1124930  C6 9B A6 39 13 91 D5 01  5E 1C C7 39 13 91 D5 01   Æ›¦9 ‘Õ ^ Ç9 ‘Õ
0C1124940  58 C6 2C 80 16 91 D5 01  9F 4B 39 80 16 91 D5 01   XÆ,€ ‘Õ ŸK9€ ‘Õ
0C1124950  C8 00 00 00 00 00 00 00  C2 00 00 00 00 00 00 00   È       Â
0C1124960  20 00 00 00 00 00 00 00  0D 01 6C 00 61 00 62 00              l a b
0C1124970  31 00 70 00 61 00 72 00  74 00 32 00 2E 00 74 00   1 p a r t 2 . t
0C1124980  78 00 74 00 00 00 00 00  40 00 00 00 28 00 00 00   x t     @   (
0C1124990  00 00 00 00 00 00 03 00  10 00 00 00 18 00 00 00
0C11249A0  FE 10 EA C0 FD FC E9 11  AD 77 08 00 27 90 79 80   þ êÀýüé w  ' y€
0C11249B0  80 00 00 00 E0 00 00 00  00 00 18 00 00 00 01 00   €   à
0C11249C0  C2 00 00 00 18 00 00 00  41 20 63 6F 75 6E 74 72   Â       A countr
0C11249D0  79 6D 61 6E 20 62 65 74  77 65 65 6E 20 74 77 6F   yman between two
0C11249E0  20 6C 61 79 65 72 73 20  69 73 20 6C 69 6B 65 20    layers is like
0C11249F0  61 20 66 69 73 68 20 62  65 74 77 65 65 6E 38 01   a fish between8
Sector 6,326,564 of 103,729,144   Offset:   C1124969   = 1   Block:   C1124910 - C1124969   Size:   5A

Data Interpreter
 8 Bit (±): 1
16 Bit (±): 27,649
32 Bit (±): 1,627,417,601
FILETIME:   01/27/12790
            02:02:42

[unregistered]
Drive C:                    36% free
File system:                    NTFS
[Read-only mode]
Alloc. of visible drive space:
Cluster No.:                 790,820
                       $MFT (#17554)
     \Users\ass\Desktop\lab1part2.txt
Snapshot taken          26 hours ago
Logical sector No.:        6,326,564
Physical sector No.:       7,452,964
Used space:                  31.7 GB
              34,072,895,488 bytes
Free space:                  17.7 GB
              19,036,426,240 bytes
Total capacity:              49.5 GB
              53,109,321,728 bytes
Bytes per cluster:             4,096
Free clusters:             4,647,565
```

Figure 22: Long file name at offset 0x5A from the second 0x30 attribute.

8. Is this file a resident file or nonresident file? Where can you find the evidence?

    - The resident/nonresident flag exists at offset 0x08 from attribute 0x80. In this case we can see it is a resident file. This makes sense because it is only 194 Bytes in size.



```
lab1part2.txt        txt      194 B 11/01/2019  17:19:43 11/01/2019  17:19:43 11/01/2019  17:46:33    IA     6,326,564
```

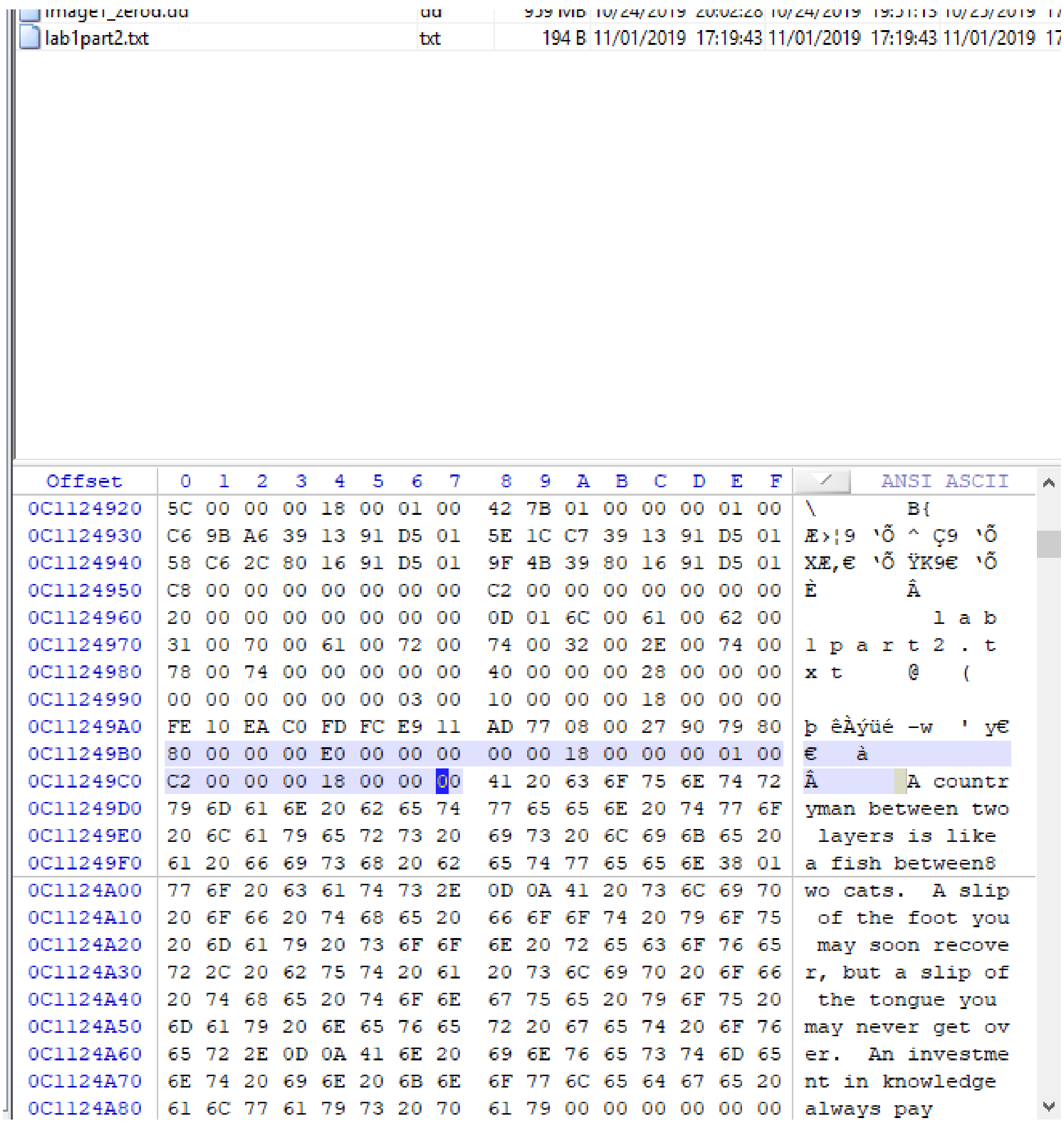
```
  Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F      ANSI ASCII
0C1124920  5C 00 00 00 18 00 01 00  42 7B 01 00 00 00 01 00  \       B{
0C1124930  C6 9B A6 39 13 91 D5 01  5E 1C C7 39 13 91 D5 01  Æ›¦9 'Õ ^ Ç9 'Õ
0C1124940  58 C6 2C 80 16 91 D5 01  9F 4B 39 80 16 91 D5 01  XÆ,€ 'Õ ŸK9€ 'Õ
0C1124950  C8 00 00 00 00 00 00 00  C2 00 00 00 00 00 00 00  È       Â
0C1124960  20 00 00 00 00 00 00 00  0D 01 6C 00 61 00 62 00          l a b
0C1124970  31 00 70 00 61 00 72 00  74 00 32 00 2E 00 74 00  1 p a r t 2 . t
0C1124980  78 00 74 00 00 00 00 00  40 00 00 00 28 00 00 00  x t     @   (
0C1124990  00 00 00 00 00 00 03 00  10 00 00 00 18 00 00 00
0C11249A0  FE 10 EA C0 FD FC E9 11  AD 77 08 00 27 90 79 80  þ êÀýüé w  ' y€
0C11249B0  80 00 00 00 E0 00 00 00  00 00 18 00 00 00 01 00  €   à
0C11249C0  C2 00 00 00 18 00 00 00  41 20 63 6F 75 6E 74 72  Â       A countr
0C11249D0  79 6D 61 6E 20 62 65 74  77 65 65 6E 20 74 77 6F  yman between two
0C11249E0  20 6C 61 79 65 72 73 20  69 73 20 6C 69 6B 65 20   layers is like
0C11249F0  61 20 66 69 73 68 20 62  65 74 77 65 65 6E 38 01  a fish between8
0C1124A00  77 6F 20 63 61 74 73 2E  0D 0A 41 20 73 6C 69 70  wo cats.  A slip
0C1124A10  20 6F 66 20 74 68 65 20  66 6F 6F 74 20 79 6F 75   of the foot you
0C1124A20  20 6D 61 79 20 73 6F 6F  6E 20 72 65 63 6F 76 65   may soon recove
0C1124A30  72 2C 20 62 75 74 20 61  20 73 6C 69 70 20 6F 66  r, but a slip of
0C1124A40  20 74 68 65 20 74 6F 6E  67 75 65 20 79 6F 75 20   the tongue you
0C1124A50  6D 61 79 20 6E 65 76 65  72 20 67 65 74 20 6F 76  may never get ov
0C1124A60  65 72 2E 0D 0A 41 6E 20  69 6E 76 65 73 74 6D 65  er.  An investme
0C1124A70  6E 74 20 69 6E 20 6B 6E  6F 77 6C 65 64 67 65 20  nt in knowledge
```

```
Data Interpreter
 8 Bit (±): 0
16 Bit (±): 0
32 Bit (±): 402,653,184
FILETIME: 05/05/1829
          16:50:44
```

Figure 23: Resident flag set to `0x00`, meaning it is a resident file.

9. In which attribute can you find the data run? Where is the start of the data run?

    - The start of the data run for resident files exists at offset `0x18` from attribute `0x80`.



```
image1_zerod.dd   dd    939 MB 10/24/2019  20:02:28 10/24/2019  19:51:15 10/25/2019  17
lab1part2.txt     txt   194 B  11/01/2019  17:19:43 11/01/2019  17:19:43 11/01/2019  17
```

```
  Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F      ANSI ASCII
0C1124920  5C 00 00 00 18 00 01 00  42 7B 01 00 00 00 01 00  \       B{
0C1124930  C6 9B A6 39 13 91 D5 01  5E 1C C7 39 13 91 D5 01  Æ›¦9 'Õ ^ Ç9 'Õ
0C1124940  58 C6 2C 80 16 91 D5 01  9F 4B 39 80 16 91 D5 01  XÆ,€ 'Õ ŸK9€ 'Õ
0C1124950  C8 00 00 00 00 00 00 00  C2 00 00 00 00 00 00 00  È       Â
0C1124960  20 00 00 00 00 00 00 00  0D 01 6C 00 61 00 62 00            l a b
0C1124970  31 00 70 00 61 00 72 00  74 00 32 00 2E 00 74 00  1 p a r t 2 . t
0C1124980  78 00 74 00 00 00 00 00  40 00 00 00 28 00 00 00  x t     @   (
0C1124990  00 00 00 00 00 00 03 00  10 00 00 00 18 00 00 00
0C11249A0  FE 10 EA C0 FD FC E9 11  AD 77 08 00 27 90 79 80  þ êÀýüé w  ' y€
0C11249B0  80 00 00 00 E0 00 00 00  00 00 18 00 00 00 01 00  €   à
0C11249C0  C2 00 00 00 18 00 00 00  41 20 63 6F 75 6E 74 72  Â       A countr
0C11249D0  79 6D 61 6E 20 62 65 74  77 65 65 6E 20 74 77 6F  yman between two
0C11249E0  20 6C 61 79 65 72 73 20  69 73 20 6C 69 6B 65 20   layers is like
0C11249F0  61 20 66 69 73 68 20 62  65 74 77 65 65 6E 38 01  a fish between8
0C1124A00  77 6F 20 63 61 74 73 2E  0D 0A 41 20 73 6C 69 70  wo cats.  A slip
0C1124A10  20 6F 66 20 74 68 65 20  66 6F 6F 74 20 79 6F 75   of the foot you
0C1124A20  20 6D 61 79 20 73 6F 6F  6E 20 72 65 63 6F 76 65   may soon recove
0C1124A30  72 2C 20 62 75 74 20 61  20 73 6C 69 70 20 6F 66  r, but a slip of
0C1124A40  20 74 68 65 20 74 6F 6E  67 75 65 20 79 6F 75 20   the tongue you
0C1124A50  6D 61 79 20 6E 65 76 65  72 20 67 65 74 20 6F 76  may never get ov
0C1124A60  65 72 2E 0D 0A 41 6E 20  69 6E 76 65 73 74 6D 65  er.  An investme
0C1124A70  6E 74 20 69 6E 20 6B 6E  6F 77 6C 65 64 67 65 20  nt in knowledge
0C1124A80  61 6C 77 61 79 73 20 70  61 79 00 00 00 00 00 00  always pay
```

Figure 24: The start of the data run at offset `0x18` from attribute `0x80`.