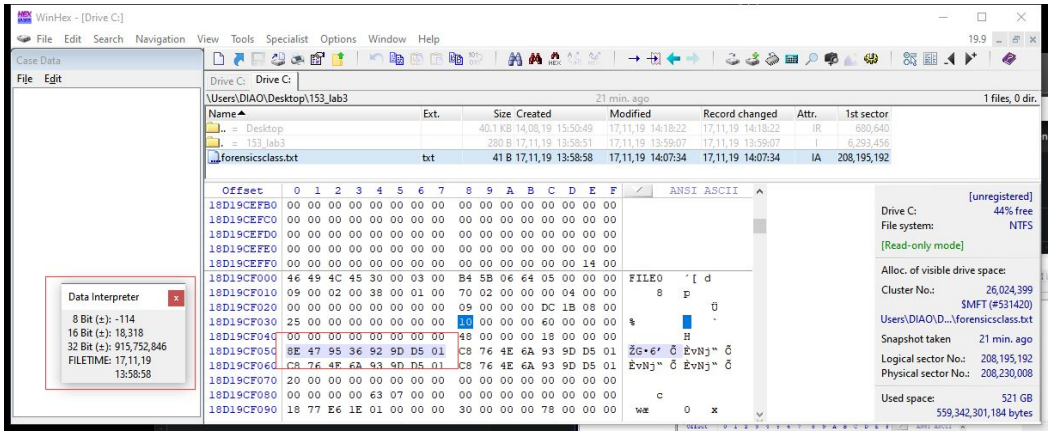
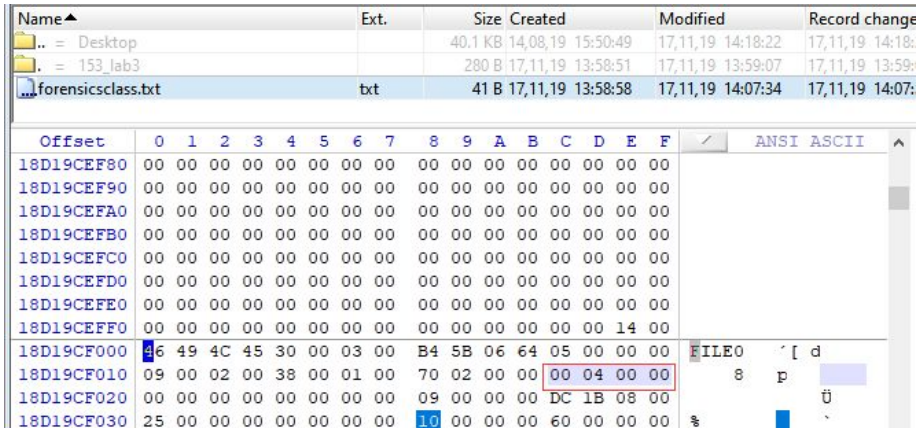
RONGGUANG OU
CSC 153 Lab 3
Understanding MFT and Dataruns

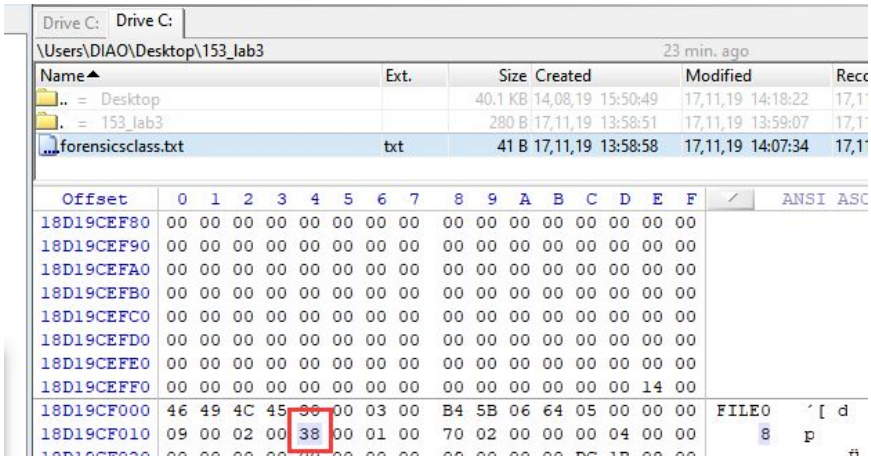
1. According to the data interpreter, what is the file create date and time for the file forensicsclass.txt? Take a screenshot to prove your answer. The file create data and time is 11/17/19 13:58:58. This was located at offset 0x18-0x1F from beginning of attribute 0x10.



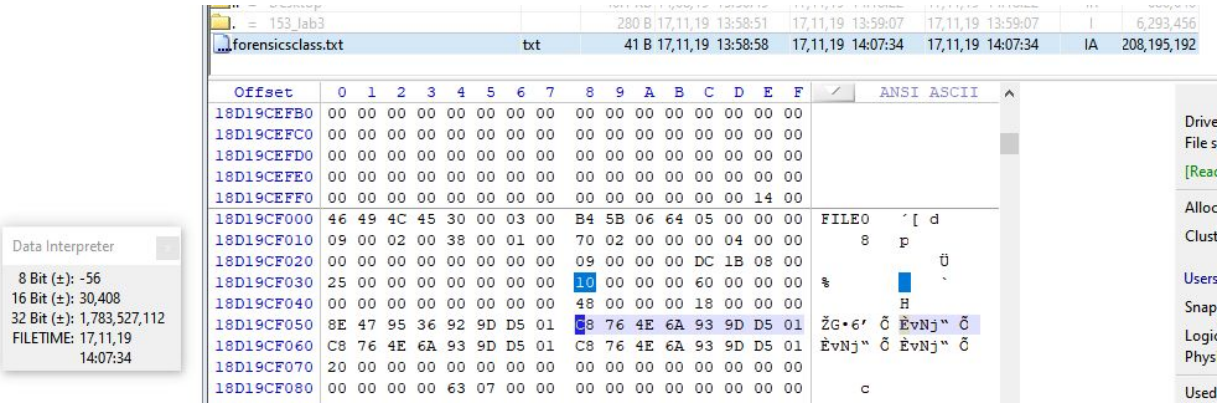
2. What is the size of the MFT record? The size of MFT record is 400 bytes is indicated by the numbers in 0x1C - 0x1F.



3. What is the length of the header? The length of the header is 38 bytes.

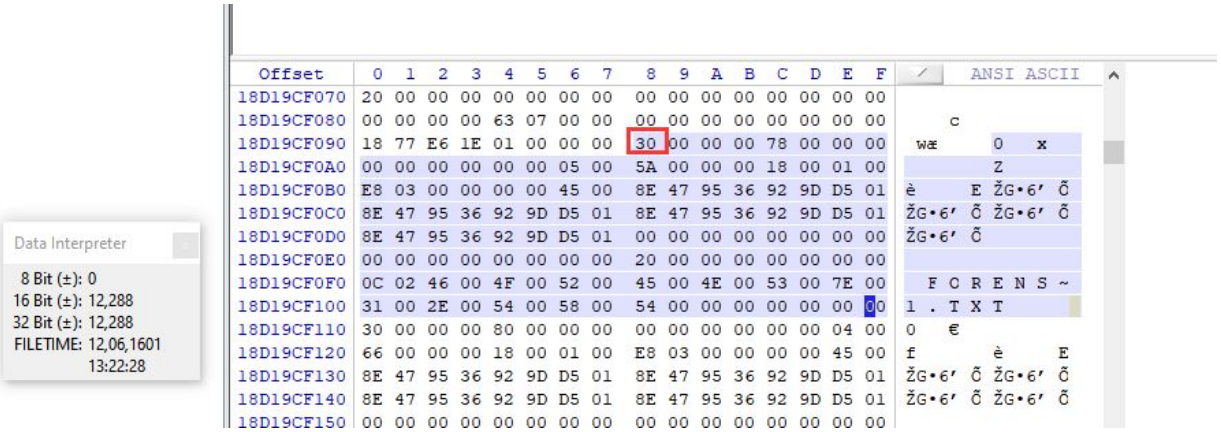


4. What is the file's last modified date and time? The last modified time and date is 11/17/19 at 14:07:34, this was interpreted from 0x20 - 0x27 from beginning of attribute 0x10,

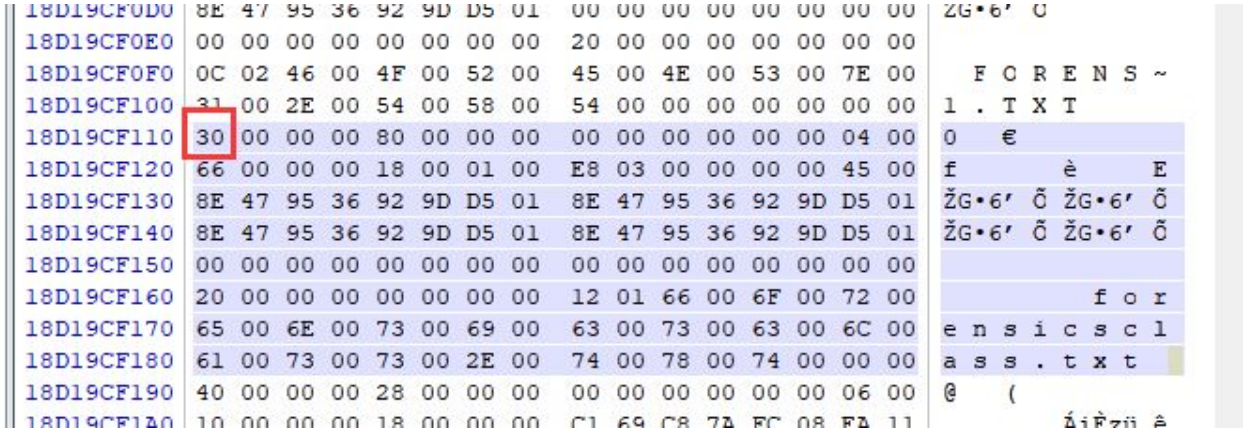


5. How many 0x30 attributes does this file have? Why? There are two 0x30 attributes because the filename is more than 8 characters long.

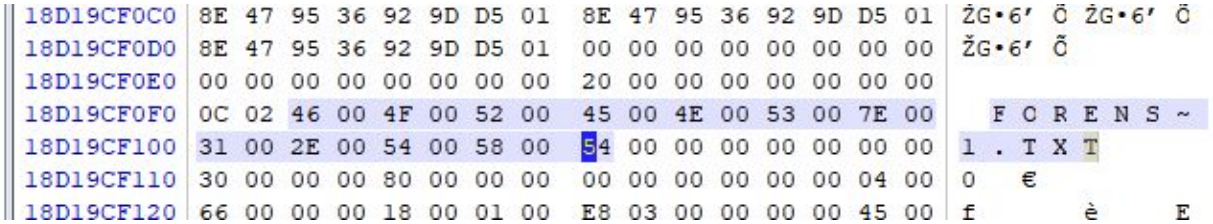
First 0x30 (short filename)



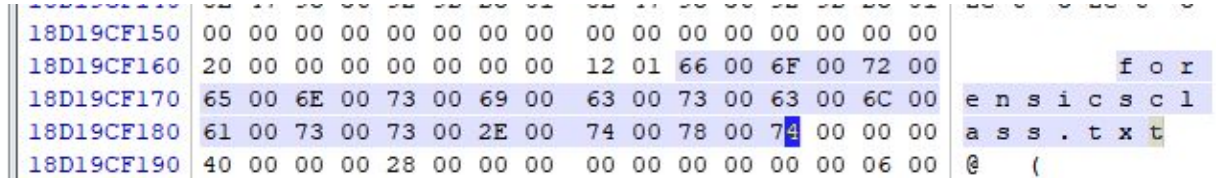
Second 0x30 (long filename)



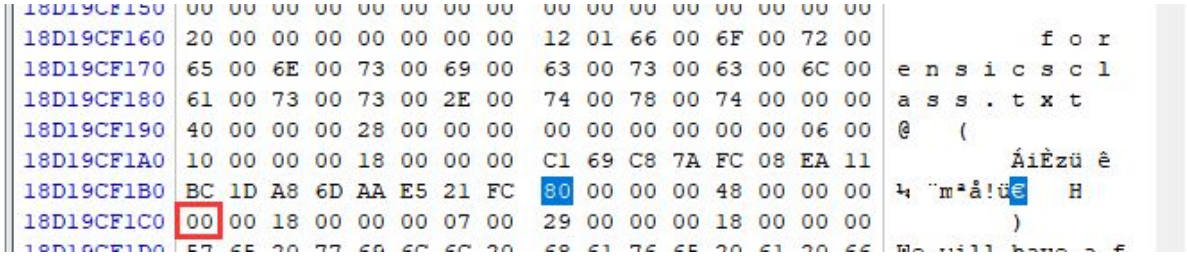
6. What is the name of this file? The shortfile name at offset 0x5A from first 0x03 is “F O R E N S ~ 1 . T X T”.



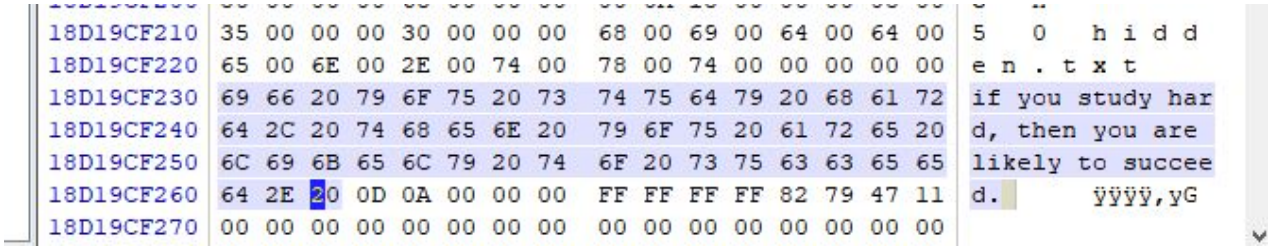
The longfile name is at offset 0x5A from 2nd 0x30 is “f o r e n s i c s c c l a s s . t x t”



7. Is this file a resident file or nonresident file? Where can you find the evidence? This file is a resident file because the offset 0x08 from 0x80 attribute is 0x00 this means is a resident file.

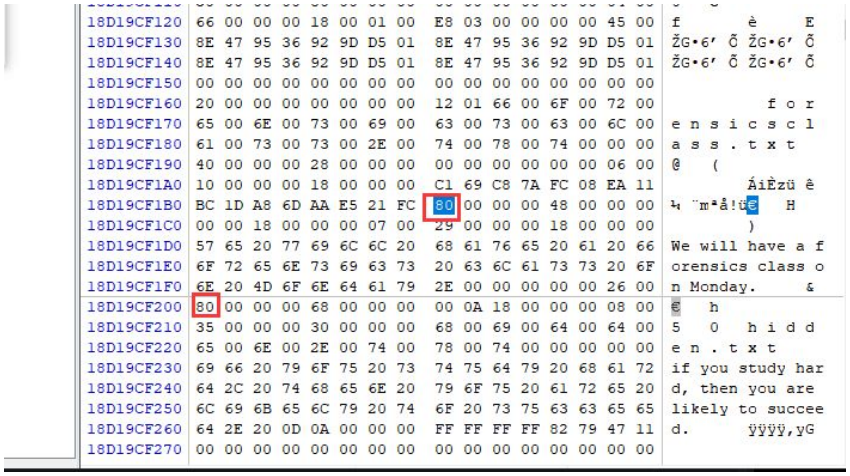


8. Did you find the hidden message in the file when you check the MFT record? Yes, Hidden message was found.



```
18D19CF210  35 00 00 00 30 00 00 00  68 00 69 00 64 00 64 00  5   0   h i d d
18D19CF220  65 00 6E 00 2E 00 74 00  78 00 74 00 00 00 00 00  e n . t x t
18D19CF230  69 66 20 79 6F 75 20 73  74 75 64 79 20 68 61 72  if you study har
18D19CF240  64 2C 20 74 68 65 6E 20  79 6F 75 20 61 72 65 20  d, then you are
18D19CF250  6C 69 6B 65 6C 79 20 74  6F 20 73 75 63 63 65 65  likely to succee
18D19CF260  64 2E 20 0D 0A 00 00 00  FF FF FF FF 82 79 47 11  d.       ÿÿÿÿ,yG
18D19CF270  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

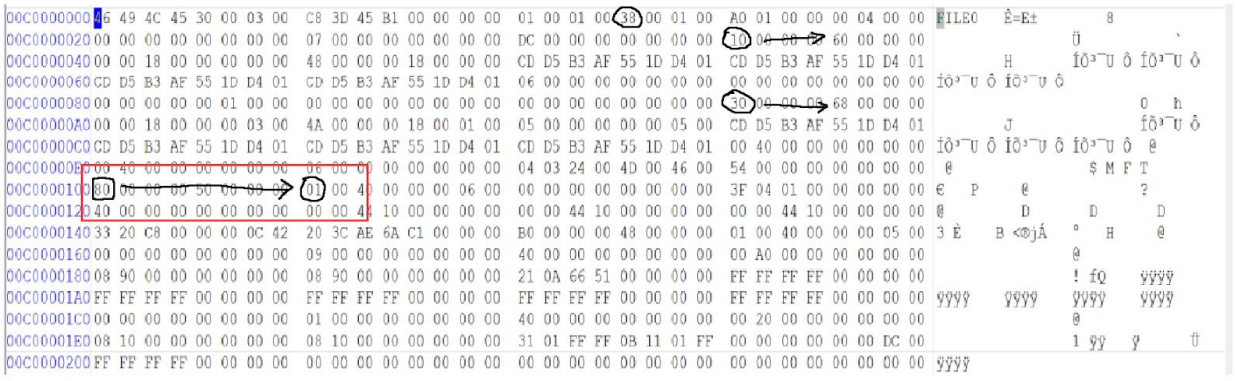
9. How many 0x80 attributes does this file have? What is the possible reason? There are two 0x80 attributes because one is the normal forenciscsclass.txt and second one is the alternative data stream.



```
18D19CF120  66 00 00 00 18 00 01 00  E8 03 00 00 00 00 45 00  f       è     E
18D19CF130  8E 47 95 36 92 9D D5 01  8E 47 95 36 92 9D D5 01  ŽG•6’ Õ ŽG•6’ Õ
18D19CF140  8E 47 95 36 92 9D D5 01  8E 47 95 36 92 9D D5 01  ŽG•6’ Õ ŽG•6’ Õ
18D19CF150  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
18D19CF160  20 00 00 00 00 00 00 00  12 01 66 00 6F 00 72 00            f o r
18D19CF170  65 00 6E 00 73 00 69 00  63 00 73 00 63 00 6C 00  e n s i c s c l
18D19CF180  61 00 73 00 73 00 2E 00  74 00 78 00 74 00 00 00  a s s . t x t
18D19CF190  40 00 00 00 28 00 00 00  00 00 00 00 00 00 06 00  @   (
18D19CF1A0  10 00 00 00 18 00 00 00  C1 69 C8 7A FC 08 EA 11          ÁiÈzü ê
18D19CF1B0  BC 1D A8 6D AA E5 21 FC  80 00 00 00 48 00 00 00  ¼ ¨mªå!ü€   H
18D19CF1C0  00 00 18 00 00 00 07 00  29 00 00 00 18 00 00 00          )
18D19CF1D0  57 65 20 77 69 6C 6C 20  68 61 76 65 20 61 20 66  We will have a f
18D19CF1E0  6F 72 65 6E 73 69 63 73  20 63 6C 61 73 73 20 6F  orensics class o
18D19CF1F0  6E 20 4D 6F 6E 64 61 79  2E 00 00 00 00 00 26 00  n Monday.     &
18D19CF200  80 00 00 00 68 00 00 00  00 0A 18 00 00 00 08 00  €   h
18D19CF210  35 00 00 00 30 00 00 00  68 00 69 00 64 00 64 00  5   0   h i d d
18D19CF220  65 00 6E 00 2E 00 74 00  78 00 74 00 00 00 00 00  e n . t x t
18D19CF230  69 66 20 79 6F 75 20 73  74 75 64 79 20 68 61 72  if you study har
18D19CF240  64 2C 20 74 68 65 6E 20  79 6F 75 20 61 72 65 20  d, then you are
18D19CF250  6C 69 6B 65 6C 79 20 74  6F 20 73 75 63 63 65 65  likely to succee
18D19CF260  64 2E 20 0D 0A 00 00 00  FF FF FF FF 82 79 47 11  d.       ÿÿÿÿ,yG
18D19CF270  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

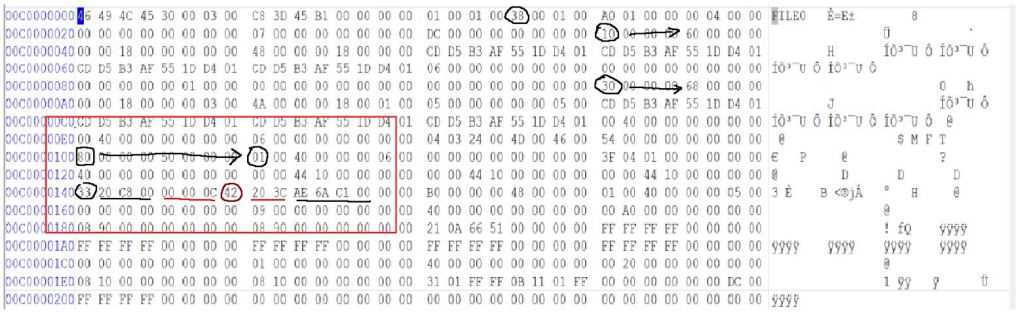
PART 2

10. Is this file a resident file or nonresident file? Where can you find the evidence? The file is a nonresident file because offset 0x08 from 0x80 attribute got value of 0x01.



```
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 48 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 00 06  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
```

11. How many data runs does this file have? There are 2 data runs.



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. Starting address is 0x0C0000 or 786,432 in dec. (see pic above).

13. How many clusters are assigned to the first data run? There are 0x00C820 or 51232 clusters assigned to first data run.(see pic above).

14. Does the 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. Yes there is a second data run. Start address of 2nd data run = first address + VCN value of 2nd data run which is 0x0C0000 + 0x00C16AAE = 0xCD6AAE (see pic above).

15. How many clusters are assigned to the second data run? There are 15,392 clusters assigned to second data run. (see pic above).