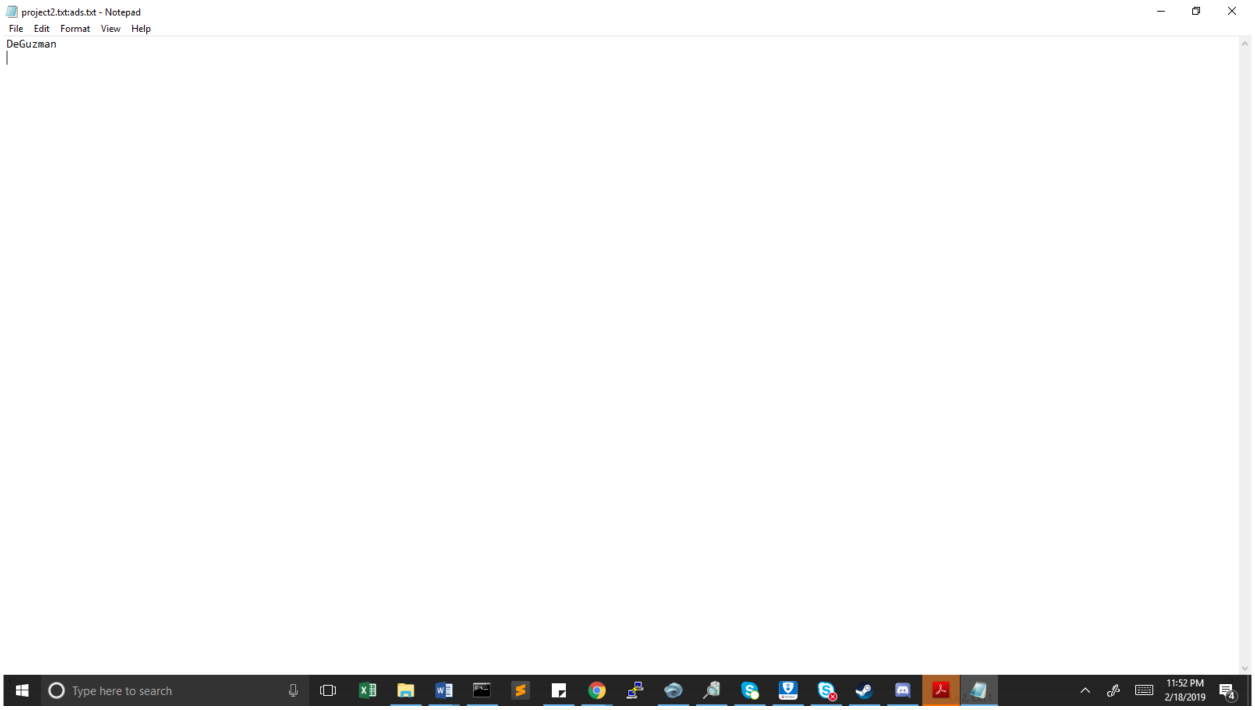
Question 1

1. What is the file size in bytes?
   a. 35 bytes
2. What is the creation date and time of this file?
   a. Creation date: 02/17/2019
   b. Creation time: 19:32:32
3. What is the last modified date and time of this file
   a. 02/17/2019 19:32:34
4. Last accessed day of this file
   a. 02/17/19 09:50:34
5. What is the starting cluster number of this file?
   a. 6
6. Why can you not determine the last accessed time of this file?
   a. The disk was originally NTFS, but reformatted as FAT32 which does not show the last accessed time of the file.
7. The hexadecimal cha
   a. The hexadecimal changes alter the integrity of the data of the drive.

Question 2a



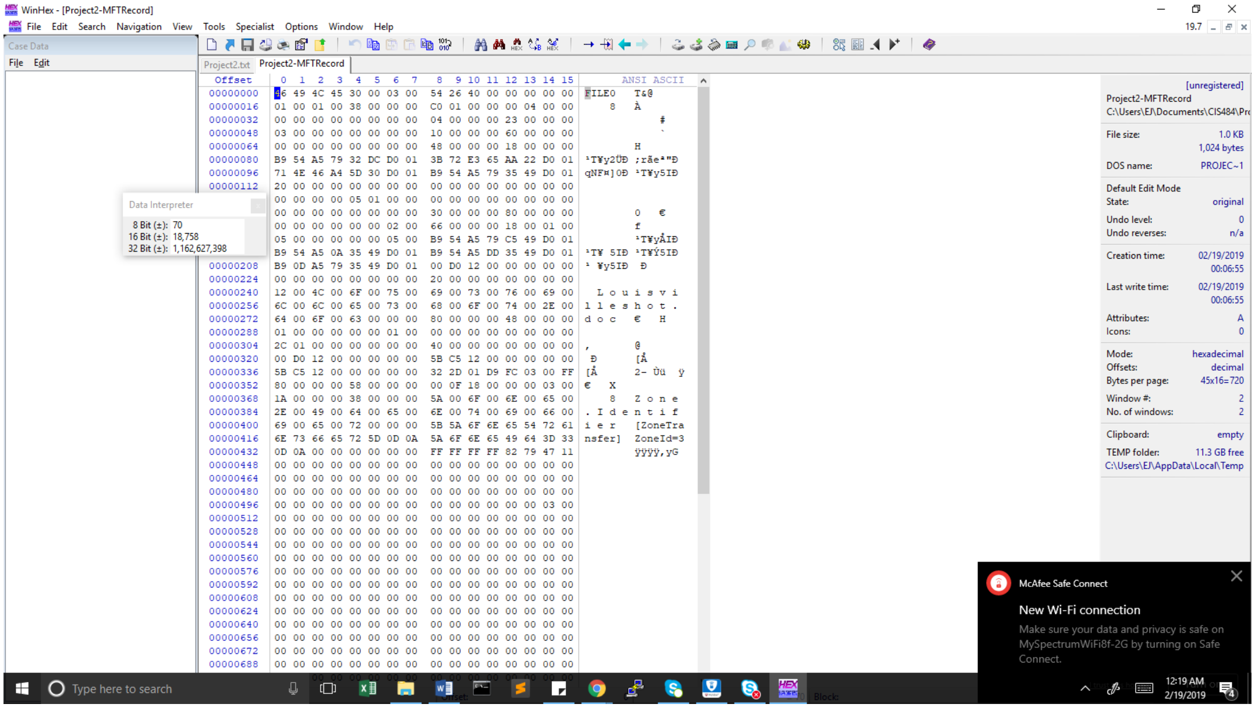
```
DeGuzman
```

1. The picture above is the screenshot for the alternate data stream file
2. When checking the properties of the Project2.txt file, it shows different file sizes on the size and size on disk respectively. For the size, the file is shown to be 169 KB (173, 410 bytes) whereas

the size on disk is 180 KB (184,320 bytes). This can determine that there is an alternate data stream along with the file.

Question 2b

1. You can tell that there is an alternate data stream by looking at the ASCII text. It has the file name but shows the extension of Louisville shot doc. It starts with 80
2. Alternate data streams can affect forensic examination because they are hidden. Because these files can be hidden from programs, it can be difficult to identify them which could have very important information in regards to the case. Also, these files can contain harmful code which can be detrimental in progressing towards the case. This can ultimately lead to the loss of data or damaged hardware
3. This is a screenshot of the hexadecimal view of the MFT record



```
Offset     0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15   ANSI ASCII
00000000  46 49 4C 45 30 00 03 00  54 26 40 00 00 00 00 00  FILE0   T&@
00000016  01 00 01 00 38 00 00 00  C0 01 00 00 00 04 00 00      8   À
00000032  00 00 00 00 00 00 00 00  04 00 00 00 23 00 00 00              #
00000048  03 00 00 00 00 00 00 00  10 00 00 00 60 00 00 00              `
00000064  00 00 00 00 00 00 00 00  48 00 00 00 18 00 00 00          H
00000080  B9 54 A5 79 32 DC D0 01  3B 72 E3 65 AA 22 D0 01  ¹T¥y2ÜÐ ;rãeª"Ð
00000096  71 4E 46 A4 5D 30 D0 01  B9 54 A5 79 35 49 D0 01  qNF¤]0Ð ¹T¥y5IÐ
00000112  20 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
          00 00 00 00 05 01 00 00  00 00 00 00 00 00 00 00
          00 00 00 00 00 00 00 00  30 00 00 00 80 00 00 00          0   €
          00 00 00 00 00 00 02 00  66 00 00 00 18 00 01 00          f
          05 00 00 00 00 00 05 00  B9 54 A5 79 C5 49 D0 01          ¹T¥yÅIÐ
          B9 54 A5 0A 35 49 D0 01  B9 54 A5 DD 35 49 D0 01  ¹T¥ 5IÐ ¹T¥Ý5IÐ
00000208  B9 0D A5 79 35 49 D0 01  00 D0 12 00 00 00 00 00  ¹ ¥y5IÐ  Ð
00000224  00 00 00 00 00 00 00 00  20 00 00 00 00 00 00 00
00000240  12 00 4C 00 6F 00 75 00  69 00 73 00 76 00 69 00    L o u i s v i
00000256  6C 00 6C 00 65 00 73 00  68 00 6F 00 74 00 2E 00  l l e s h o t .
00000272  64 00 6F 00 63 00 00 00  80 00 00 00 48 00 00 00  d o c   €   H
00000288  01 00 00 00 00 00 01 00  00 00 00 00 00 00 00 00
00000304  2C 01 00 00 00 00 00 00  40 00 00 00 00 00 00 00  ,       @
00000320  00 D0 12 00 00 00 00 00  5B C5 12 00 00 00 00 00   Ð      [Å
00000336  5B C5 12 00 00 00 00 00  32 2D 01 D9 FC 03 00 FF  [Å      2- Ùü  ÿ
00000352  80 00 00 00 58 00 00 00  00 0F 18 00 00 00 03 00  €   X
00000368  1A 00 00 00 38 00 00 00  5A 00 6F 00 6E 00 65 00      8   Z o n e
00000384  2E 00 49 00 64 00 65 00  6E 00 74 00 69 00 66 00  . I d e n t i f
00000400  69 00 65 00 72 00 00 00  5B 5A 6F 6E 65 54 72 61  i e r   [ZoneTra
00000416  6E 73 66 65 72 5D 0D 0A  5A 6F 6E 65 49 64 3D 33  nsfer]  ZoneId=3
00000432  0D 0A 00 00 00 00 00 00  FF FF FF FF 82 79 47 11          ÿÿÿÿ‚yG
00000448  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000464  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000480  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000496  00 00 00 00 00 00 00 00  00 00 00 00 00 00 03 00
00000512  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000528  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000544  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000560  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000576  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000592  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000608  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000624  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000640  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000656  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000672  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000688  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

Data Interpreter

8 Bit (±): 70
16 Bit (±): 18,758
32 Bit (±): 1,162,627,398

[unregistered]
Project2-MFTRecord
C:\Users\EJ\Documents\CIS484\Pr

File size: 1.0 KB
1,024 bytes
DOS name: PROJEC~1

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

Creation time: 02/19/2019 00:06:55
Last write time: 02/19/2019 00:06:55
Attributes: A
Icons: 0

Mode: hexadecimal
Offsets: decimal
Bytes per page: 45x16=720
Window #: 2
No. of windows: 2

Clipboard: empty
TEMP folder: 11.3 GB free
C:\Users\EJ\AppData\Local\Temp

New Wi-Fi connection

Make sure your data and privacy is safe on MySpectrumWiFi8f-2G by turning on Safe Connect.

12:19 AM
2/19/2019

Question 2c

1. When I tried to copy the file it did not copy the contents of the file and shows it as 0 KB.
2. This shows that the contents cannot transfer from different formatted drives, for example transferring from an NTFS formatted drive to a FAT32 formatted drive.

Question 3

1. Unallocated file since it is 00 00 and it is a deleted file
2. 35
3. Fri, 21 Aug 2015 16:57:34
4. Sun, 28 Dec 2014 14:27:24
5. Thu, 15 Jan 2015 00:53:13
6. Sun, 28 Dec 2014 14:27:24

7. Name of the file: Louisvilledot.doc
8. There are 8 timestamps
9. 00 00 it is a deleted file
10. Resident
11. There are two 0x80