Due: 02/17/2020 5:30 PM

**CIS484-75-4202 Project 2 Notes:**

- **You will need admin access to a Windows computer and a flash drive for this project.**
- **All files and/or tools required for this project may be downloaded using the links posted on Blackboard or provided during lecture.**

For this project, complete the following tasks:

1) Format a flash drive as FAT32, create a file on it called "file1.txt", and add some text to the file before saving it on the flash drive.
   a) Open the flash drive's physical disk (Tools → Open Disk) in WinHex, double-click on the FAT32 partition listed in the directory browser (upper-right pane of WinHex) and navigate to the directory entry for "file1.txt". Apply the FAT directory entry template (normal/short entry format) to the directory entry and answer the questions below. **Be sure your cursor is at the starting byte of the directory entry before you apply the template!**
      1. What is the size of this file in bytes? (2 pts)
         **The file size is 1465 bytes.**
      2. What is the creation date and time of this file? (2 pts)
         **The creation date and time of the file is 02/04/2020, 17:52:16**
      3. What is the last modified date and time of this file? (2 pts)
         **Last modified date and time is 02/04/2020, 17:52:16**
      4. What is the last accessed day of this file? (2 pts)
         **Last access date is 02/04/2020**
      5. What is the starting cluster number of this file? (2 pts)
         **Cluster 6**
      6. Why can you not determine the last accessed time of the file?
         **There is simply not enough space for it to be stored.**
   b) Close WinHex and SHIFT-delete "file1.txt". Now reopen WinHex and open the flash drive as a physical disk again and open the FAT32 partition. When prompted about reusing a volume snapshot, select "Take a New One" to force WinHex to refresh the volume snapshot. Navigate back to the directory entry for "file1.txt".

i) What hexadecimal changes do you see in the directory entry as compared to before the file was deleted? (4 pts)

**The hexadecimal change I noticed in the deleted file was the first byte is now "E5".**

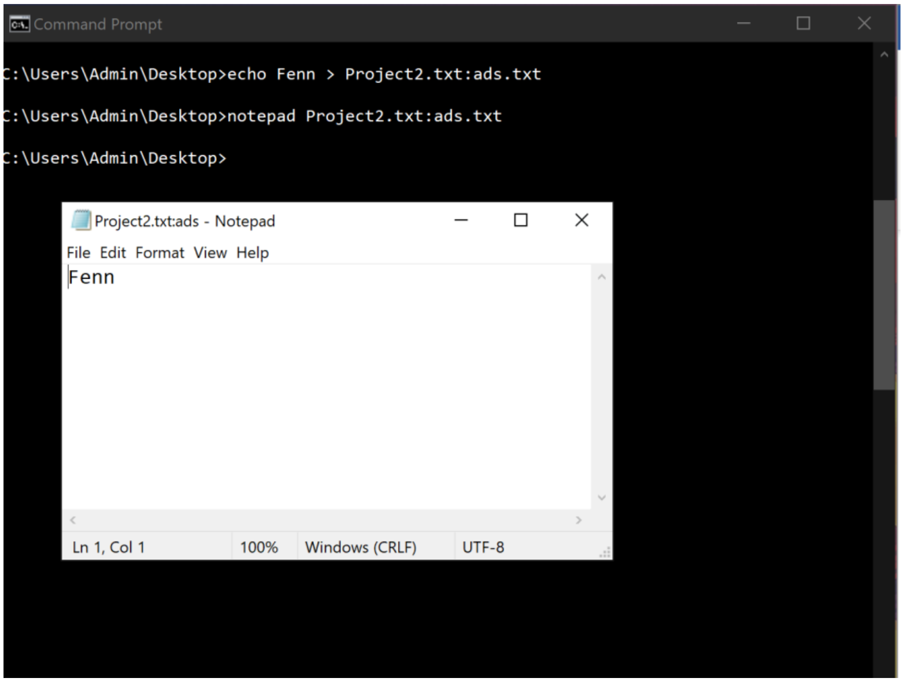
ii) How do the changes affect forensic examination? (4 pts)

**This affects the forensic examination by displaying a file was "Shift-Deleted"**

2) On an NTFS formatted drive (e.g. your C:\ drive) and using Notepad, create a text file and name it "Project2" (do not insert any text into the file).

a) Create an alternate (additional) data stream for the new file using the example on page 229 and name it "ads.txt". Insert your last name as the only text within the alternate data stream.

i) Verify that the ADS has been created properly by typing "notepad project2.txt:ads.txt" at the command line (make sure you're in the same directory as the project2.txt file). Include a screenshot of the output from this command. (4 pts)

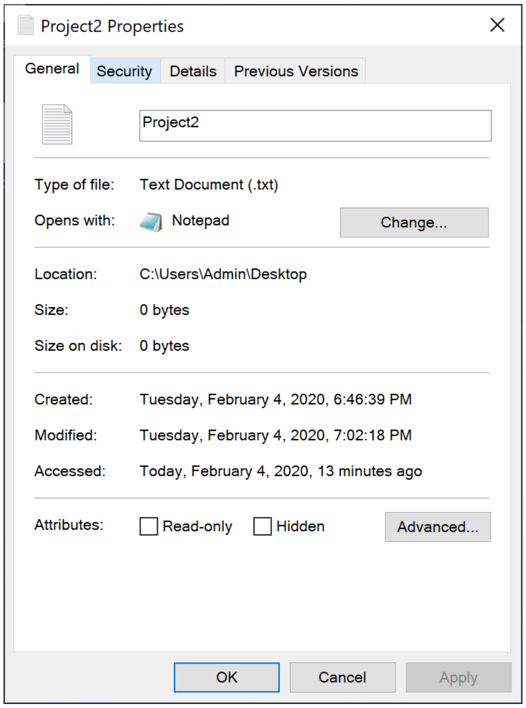


```
C:\Users\Admin\Desktop>echo Fenn > Project2.txt:ads.txt

C:\Users\Admin\Desktop>notepad Project2.txt:ads.txt

C:\Users\Admin\Desktop>
```

Fenn

ii) Now check the size of the project2.txt file in Windows (right click on the file, select Properties). What does it show? What conclusions can you draw from this? (4 pts)

**Project2.txt has a size of 0 bytes. You can come to the conclusion that using data streams causes the ads.txt stream file to be associated with the contents of the Project2.txt file.**



Project2

Type of file: Text Document (.txt)

Opens with: Notepad

Location: C:\Users\Admin\Desktop

Size: 0 bytes

Size on disk: 0 bytes

Created: Tuesday, February 4, 2020, 6:46:39 PM

Modified: Tuesday, February 4, 2020, 7:02:18 PM

Accessed: Today, February 4, 2020, 13 minutes ago

Attributes: □ Read-only □ Hidden

b) Open the NTFS drive you're working with as a physical device in WinHex and locate the MFT record that corresponds with the “Project 2.txt” file you created (right click on the file → Navigation →Go to FILE Record).

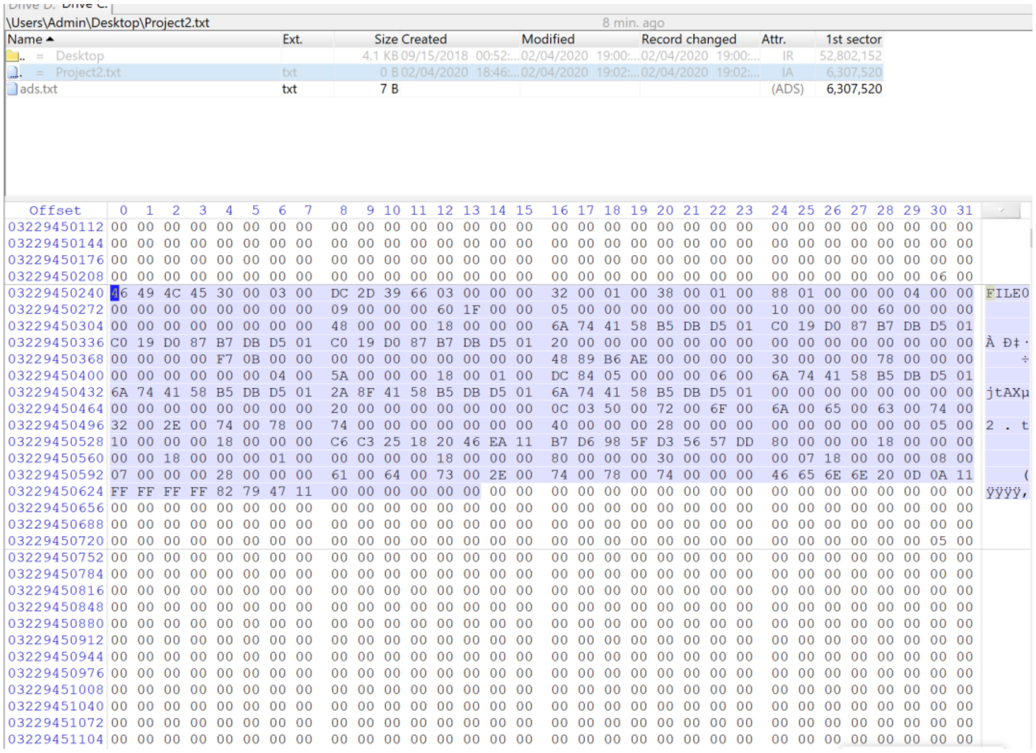
i) Based on examination at the hexadecimal level, how can you tell that this file has an alternate data stream? (4 pts)

**I can determine the file has an alternate data stream because the byte 80 indicates data has been stored on the file.**

ii) How might alternate data streams affect a forensic examination? (4 pts)

**Data streams might affect a forensic examination by obscuring evidentiary data since it becomes an additional file attribute.**

iii) Include a screenshot of a hexadecimal view of the MFT record. (3 pts)



```
Drive D: Drive C:
\Users\Admin\Desktop\Project2.txt                                   8 min. ago
Name ▲                        Ext.     Size Created             Modified            Record changed      Attr.   1st sector
..  =  Desktop                       4.1 KB 09/15/2018 00:52:... 02/04/2020 19:00:... 02/04/2020 19:00:... IR      52,802,152
.   =  Project2.txt           txt       0 B 02/04/2020 18:46:... 02/04/2020 19:02:... 02/04/2020 19:02:... IA       6,307,520
ads.txt                       txt       7 B                                                               (ADS)    6,307,520

   Offset    0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15  16 17 18 19 20 21 22 23  24 25 26 27 28 29 30 31
03229450112 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 00 00 00 00
03229450144 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 00 00 00 00
03229450176 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 00 00 00 00
03229450208 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 00 00 06 00
03229450240 46 49 4C 45 30 00 03 00  DC 2D 39 66 03 00 00 00  32 00 01 00 38 00 01 00  88 01 00 00 00 04 00 00  FILE0
03229450272 00 00 00 00 00 00 00 00  09 00 00 00 60 1F 00 00  05 00 00 00 00 00 00 00  10 00 00 00 60 00 00 00
03229450304 00 00 00 00 00 00 00 00  48 00 00 00 18 00 00 00  6A 74 41 58 B5 DB D5 01  C0 19 D0 87 B7 DB D5 01
03229450336 C0 19 D0 87 B7 DB D5 01  C0 19 D0 87 B7 DB D5 01  20 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  À Ð‡·
03229450368 00 00 00 00 F7 0B 00 00  00 00 00 00 00 00 00 00  48 89 B6 AE 00 00 00 00  30 00 00 00 78 00 00 00     ÷
03229450400 00 00 00 00 00 00 04 00  5A 00 00 00 18 00 01 00  DC 84 05 00 00 00 06 00  6A 74 41 58 B5 DB D5 01
03229450432 6A 74 41 58 B5 DB D5 01  2A 8F 41 58 B5 DB D5 01  6A 74 41 58 B5 DB D5 01  00 00 00 00 00 00 00 00  jtAXµ
03229450464 00 00 00 00 00 00 00 00  20 00 00 00 00 00 00 00  0C 03 50 00 72 00 6F 00  6A 00 65 00 63 00 74 00
03229450496 32 00 2E 00 74 00 78 00  74 00 00 00 00 00 00 00  40 00 00 00 28 00 00 00  00 00 00 00 00 00 05 00  2 . t
03229450528 10 00 00 00 18 00 00 00  C6 C3 25 18 20 46 EA 11  B7 D6 98 5F D3 56 57 DD  80 00 00 00 18 00 00 00
03229450560 00 00 18 00 00 00 01 00  00 00 00 00 18 00 00 00  80 00 00 00 30 00 00 00  00 07 18 00 00 00 08 00
03229450592 07 00 00 00 28 00 00 00  61 00 64 00 73 00 2E 00  74 00 78 00 74 00 00 00  46 65 6E 6E 20 0D 0A 11      (
03229450624 FF FF FF FF 82 79 47 11  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,
03229450656 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 00 00 00 00
03229450688 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 00 00 00 00
03229450720 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 00 00 05 00
03229450752 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 00 00 00 00
03229450784 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 00 00 00 00
03229450816 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 00 00 00 00
03229450848 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 00 00 00 00
03229450880 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 00 00 00 00
03229450912 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 00 00 00 00
03229450944 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 00 00 00 00
03229450976 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 00 00 00 00
03229451008 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 00 00 00 00
03229451040 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 00 00 00 00
03229451072 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 00 00 00 00
03229451104 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 00 00 00 00
```

c) Copy project2.txt to a FAT32 formatted device such as the one you used in the first part of this assignment.

i) When you tried to copy the file, what happened? (3 pts)

**When I copied Project2.txt to my FAT32 formatted drive I received an error asking if I wanted to copy the file without its properties.**

ii) Provide an explanation for why this happened. (3 pts)

**This happened because I attempted to copy the Project2.txt from an NTFS formatted drive to a FAT32 formatted drive.**

3) Download the MFT Record from Blackboard under Projects → Project 2 and open the file using WinHex (File → Open). To interpret the timestamp values, use MFT Stampede. **Leave all timestamp values in UTC format. With each answer, be sure to include the byte offset range relative to the beginning of the MFT record where you found your answer. Report all byte offsets in decimal notation.** For example, if you found the answer in byte offset 1114 (decimal notation) of the MFT record, include "byte offset 11-14" in your answer.

Due: 02/17/2020 5:30 PM

a) Is this file allocated or unallocated? (3 pts)
**The file is allocated. Byte offset 22.**

b) What is the MFT record number (decimal value) of this file? (3 pts)

**The MFT record number is 44. Byte offset 44.**

c) What is the creation timestamp in the $STANDARD_INFORMATION attribute? (4 pts)

**The creation time is 02/03/2020 17:47:38. Byte offset 80-87.**

d) What is the modified timestamp in the $STANDARD_INFORMATION attribute? (4 pts)
**The modified timestamp is 02/03/2020 12:49:38. Byte offset 88-95**

e) What is the record update timestamp in the $STANDARD_INFORMATION attribute? (4 pts)

**The record update timestamp is April 28, 2019. 16:21:00. Byte offset 96-103**

f) What is the accessed timestamp in the $STANDARD_INFORMATION attribute? (4 pts)

**The accessed timestamp is September 12, 2019. Byte offset 104-111.**

g) What is the name of this file? (3 pt)

**19710002211.pdf. Byte offset 772-786**

h) How many timestamps are included in this MFT Record? Include the name of the attribute(s) where the timestamps are located (you don't have to interpret the timestamps or include the byte offset ranges though). (4 pts)

i) **8 timestamps.**

**$File_Name timestamps are Creation, Modified, Accessed, and Record Update**

**$Standard_Information timestamps are Creation Date, Last Modified Date, Last Record Update, and Last Accessed Date.**

j) What is the starting cluster of this file? (4 pts)

k) Is the content of this file resident or non-resident? (3 pts)

**The content of this file is resident. Byte offset 136.**

l) How many $DATA (0x80) attributes does this file have? (4 pts)

**There are two $Data attributes. Byte offsets 473 and 545.**

m) Is this file fragmented? How do you know? (4 pts)

**No, there is only one data run.**

n) What is the full path to this file in the file system? (EXTRA CREDIT – 1 PT)

**C:\Users\Admin\OneDrive – University of Louisville\CIS484\Project2-MFTRecord.bin**

o) What is the full name of each named data attribute and what is its content? (EXTRA CREDIT – 3 PTS)

4) Record any and all equipment that you used for this project (hardware and software). This should include operating system version, type of flash drive, etc. (10 pts)

**Surface Pro 4**

**Windows 10 Pro**

**64GB Infinitive USB Drive**

**WinHex**