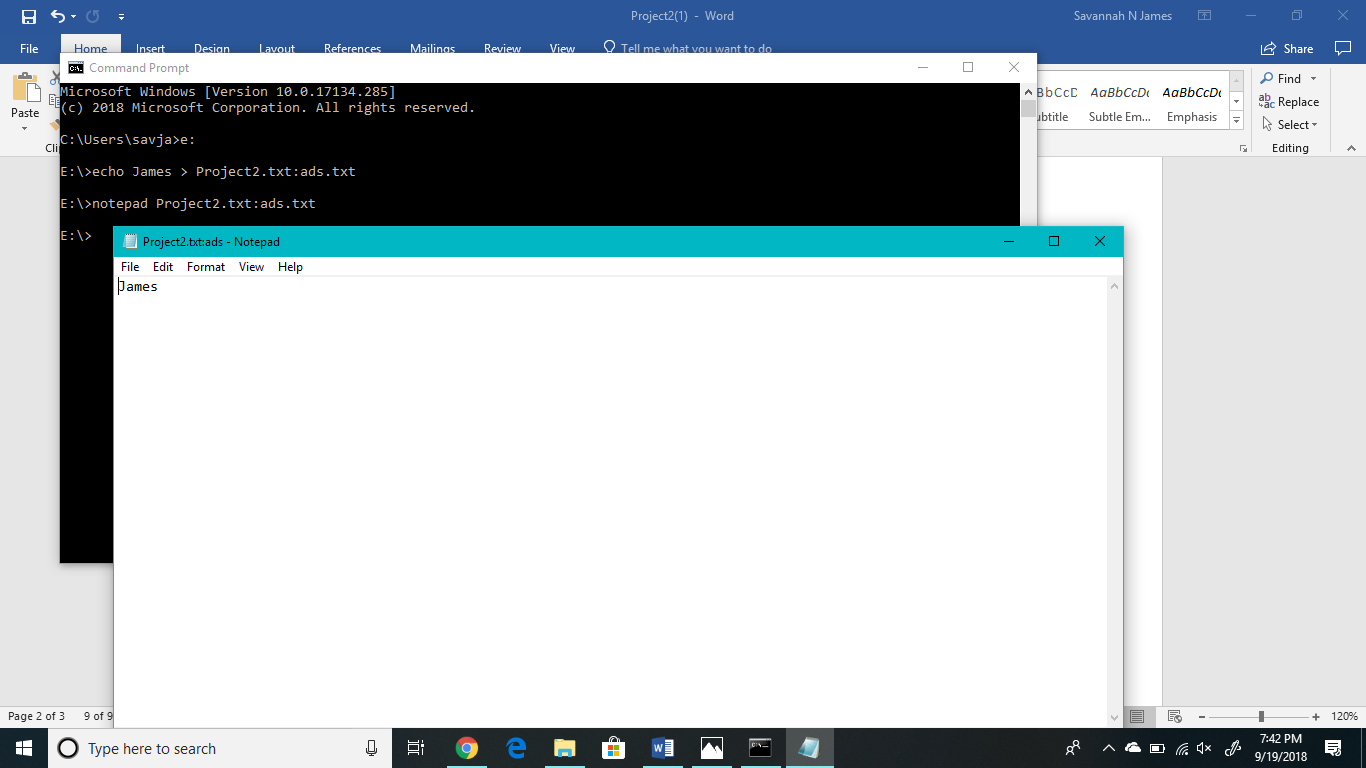
**CIS 484-77-4188 Project 2 Notes:**

* **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:

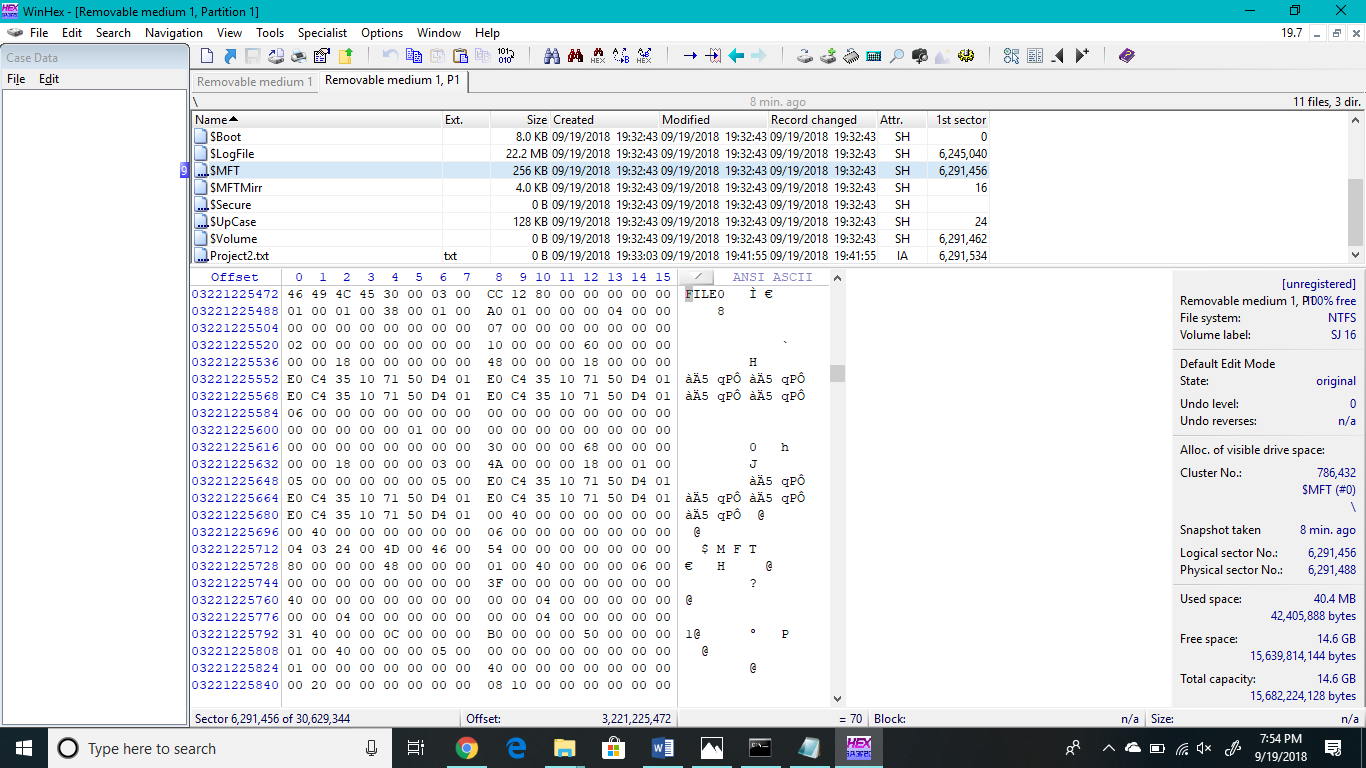
1. Format a flash drive as FAT32, create a file on it called "file1.txt", and add some text to the file before saving it on the flash drive.
   1. Open the flash drive's physical disk (Tools → Open Disk) in WinHex, double-click on the FAT32 partition listed in the directory browser (upper-right pane 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) **16**
      2. What is the creation date and time of this file? (2 pts) **09/19/2018 18:56:12**
      3. What is the last modified date and time of this file? (2 pts) iv) What is the last accessed day of this file? (2 pts) **09/19/2018 18:56:14. Last access date: 09/19/2018**
      4. What is the starting cluster number of this file? (2 pts) **6**
      5. Why can you not determine the last accessed time of the file? **FAT only records the date, cannot hold the time in hours or seconds because there is not enough storage**. (3pts)
   2. 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".
      1. What hexadecimal changes do you see in the directory entry as compared to before the file was deleted? (4 pts) **Changes to E5 – which mean that file was erased. The F in file also changed to a special character – looks like an A with a 0 over it.**
      2. How do the changes affect forensic examination? (4 pts) **The changes affect the forensic examination by letting the examiner know that the file has been deleted. The examiner can further investigate this to see when the file was deleted and what information the file may have contained.**
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).
   1. 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.
      1. 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)



* + 1. 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) **It shows the size of the file as 0 bytes. We can conclude that the properties pane is only recognizing the original text document with nothing in it. It will not pick up on ads.txt.**

* 1. 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).
     1. Based on examination at the hexadecimal level, how can you tell that this file has an alternate data stream? (4 pts) **At a hexadecimal level, you can see that this file contains 0x80, which means that the file has some sort of data in it. You can tell that it is the ADS because the file itself starts with 00, which means that it doesn’t contain any data.**
     2. How might alternate data streams affect a forensic examination? (4 pts) **Alternate data streams could be used to hide text or other information within files that may seem fine upon first look. This requires forensic examiners to pay close attention to files and always check to see if there was an ads added into the file.**
     3. Include a screenshot of a hexadecimal view of the MFT record. (3 pts)



* 1. Copy project2.txt to a FAT32 formatted device such as the one you used in the first part of this assignment.
     1. When you tried to copy the file, what happened? (3 pts) **I received an error message asking if I was sure I wanted to copy the file without its properties. The error message also stated that the file had properties that can't be copied to the new**﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿**﻿location. It also stated the file name, type of document (text), and the file size.**﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿

ii) Provide an explanation for why this happened. (3 pts) **FAT32 format is not compatible with ADS, and would not copy over the data that was added to the .txt file.**

1. 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.

* 1. Is this file allocated or unallocated? (3 pts) **unallocated : 22-23**
  2. What is the MFT record number (decimal value) of this file? (3 pts) **35**
  3. What is the creation timestamp in the $STANDARD\_INFORMATION attribute? (4 pts) **Friday, 21 August 2015 16:57:34 UTC (80-87)**
  4. What is the modified timestamp in the $STANDARD\_INFORMATION attribute? (4 pts) **Sunday, 28 December 2014 14:27:24 UTC (88-95)**
  5. What is the record update timestamp in the $STANDARD\_INFORMATION attribute? (4 pts)

**Thursday, 15 January 2015 00:53:13 UTC (96-103)**

* 1. What is the accessed timestamp in the $STANDARD\_INFORMATION attribute? (4 pts)

**Sunday, 15 February 2015 15:38:41 UTC (104-111)**

* 1. What is the name of this file? (3 pt) **LOUISVILLESHOT.DOC (242-276)**
  2. 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) **8 total – 4 in $STANDARD\_INFORMATION and 4 in $FILE\_NAME**
  3. What is the starting cluster of this file? (3 pts)
  4. Is the content of this file resident or non-resident? (3 pts) **non-resident**
  5. How many $DATA (0x80) attributes does this file have? (3 pts) **2**
  6. Is this file fragmented? How do you know? (3 pts)
  7. Is this the first time this MFT record has been used within the file system? How do you know? (3 pts)
  8. What is the full path to this file in the file system? (EXTRA CREDIT – 1 PT) **C:\Users\savja\Desktop\Project2-MFTRecord**
  9. What is the full name of each named data attribute and what is its content? (EXTRA CREDIT – 3 PTS) **$STANDARD\_INFORMATION – stores file times: created, modified, accessed and update. Also stores file flags: read-only, hidden, etc. $FILE\_NAME – includes standard attribute header, name of file or directory, timestamps, MFT record number of parent directory. $DATA – stores file data or data runs to non-resident files.**

1. 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)

**Dell Computer – Microsoft Windows 10 Pro OS Version 10.0.17134 Build 17134**

**Flash Drive – Cruzer Glide 16GB**

**WinHex**

**MFT Stampede**

**Command Prompt**