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

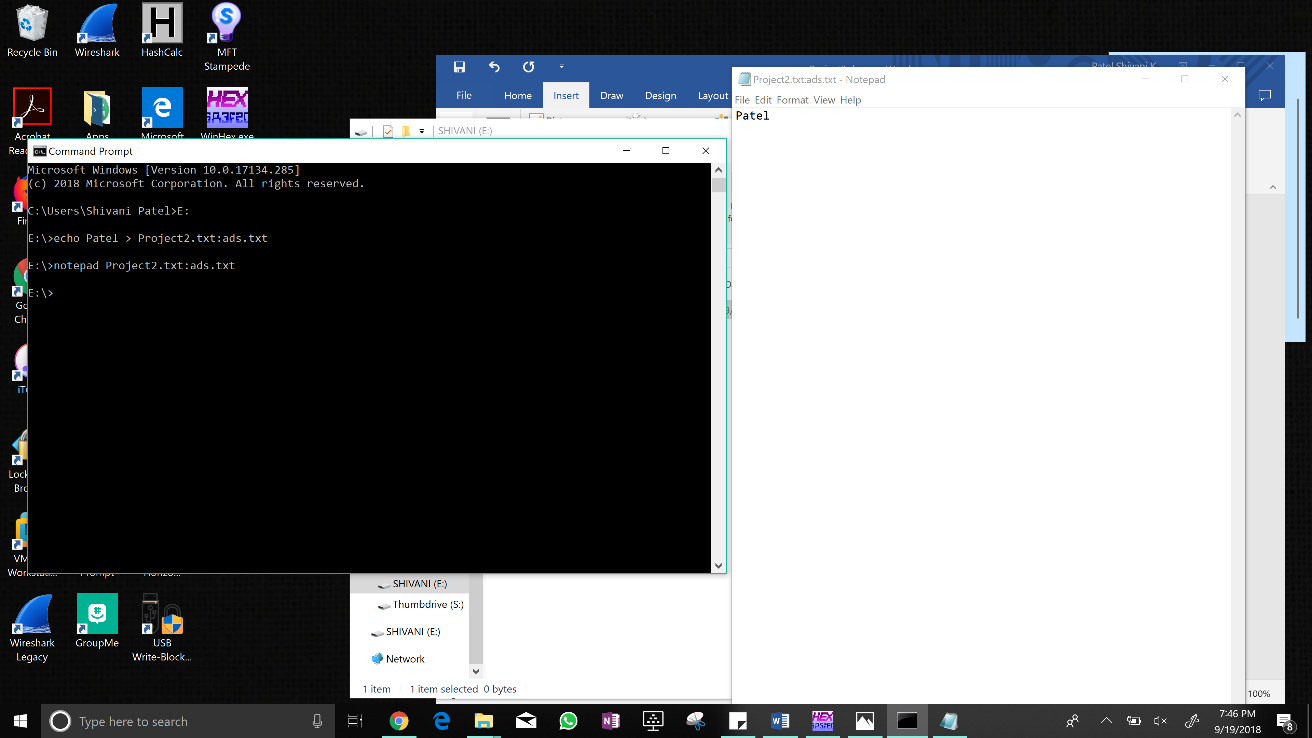
* **You will need admin access to a Windows computer and a flash drive for this project.**
* **All files and/or tools required for this project may be downloaded using the links posted on Blackboard or provided during lecture.**

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)

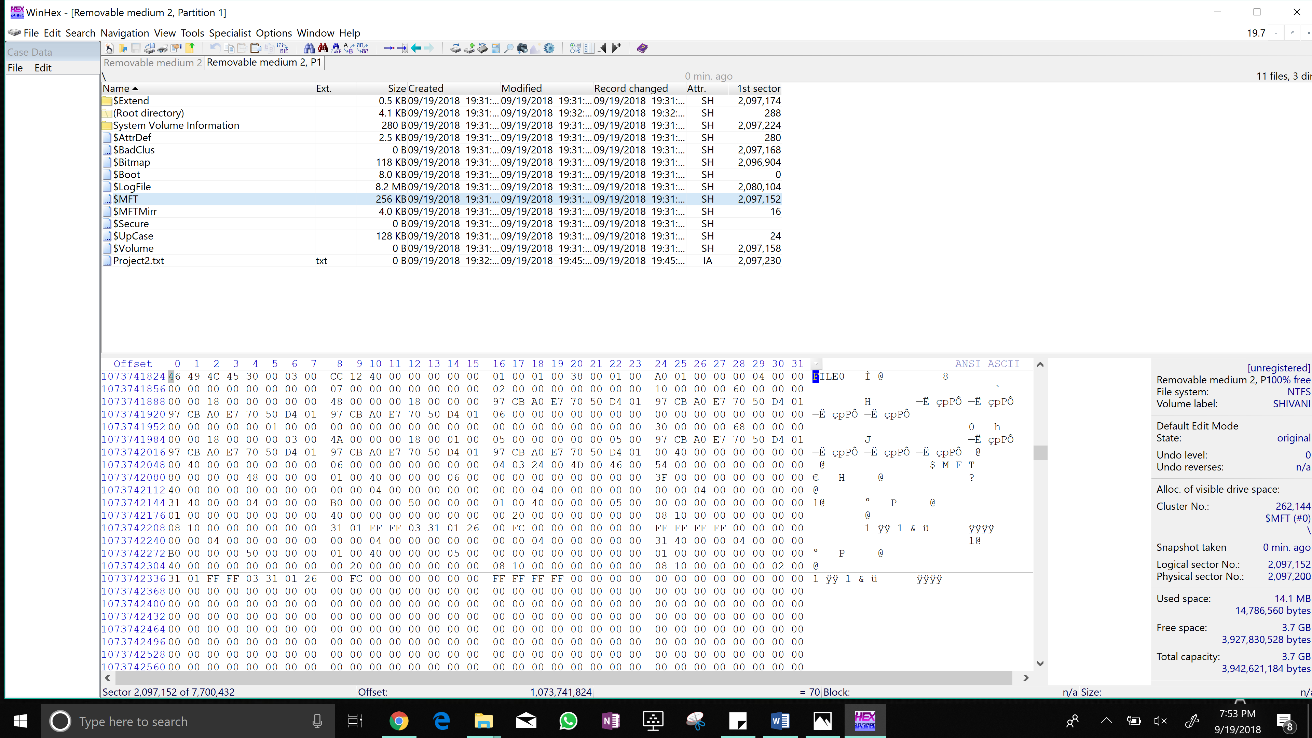
* **The size of file1 is 38 bytes.**
  + 1. What is the creation date and time of this file? (2 pts)
* **The creation date is 09/19/2018 and time is 18:42:36.**
  + 1. What is the last modified date and time of this file? (2 pts)
* **The last modified date is 09/19/2018 and time is 18:43:06**
  + 1. What is the last accessed day of this file? (2 pts)
* **The last accessed day of this file was 09/19/2018**
  + 1. What is the starting cluster number of this file? (2 pts)
* **The starting cluster number of this file is 6**
  + 1. Why can you not determine the last accessed time of the file? (3 pts)
* **FAT only records the date, not time.**
  1. 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)
* **It changes to E5 from 00 which means my file has been erased. Also, the first letter of the file was changed to a with a little o on it.**
  + 1. How do the changes affect forensic examination? (4 pts)
* **The E5 value tells the examiner that the file was deleted. Examiners can use the directory entry of the deleted file to identify the starting cluster and the size of the deleted file. The FAT entry for the clusters allocated to the file are set to 0 and because of this, the examiners do not have cluster information past the starting cluster.**

1. 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 0 bytes which means the file is empty. There is an alternate data stream associated with this file which is a text doc named ads.txt with just the string “Patel”. The alternate data stream file is not detected through the windows properties window.**
  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)
* **We can tell that this file has an alternate data stream because of the two 0x80 flags in the MFT records for the Project2.txt file. Since there are two cases in which you know that there is a second case of file data within the first .txt file which is possible in NTFS.**
  + 1. How might alternate data streams affect a forensic examination? (4 pts)
* **The alternate data streams can hide files within files and it could be possible that someone was hiding information within an alternate data stream. Therefore, an alternate data stream must always be taken under consideration for a forensic examination.**
  + 1. 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 got a prompt asking if I wanted to copy the file without its properties and the file Project2 has properties that can’t be copied to the new location.**
  + 1. Provide an explanation for why this happened. (3 pts)
* **This happened because windows detected that the FAT32 drive cannot handle the alternative data stream associated with the Project2.txt file and it tells me that this alternate data stream would not be copied along with the 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)
* **It is unallocated, and the byte Offset range is 22-23**
  1. What is the MFT record number (decimal value) of this file? (3 pts)
* **MFT record number is 35 and the Offset range is 44-47 (not sure about the offset range)**
  1. What is the creation timestamp in the $STANDARD\_INFORMATION attribute? (4 pts)
* **Fri, 21 Aug 2015 16:57:34 and the byte offset range is 80-87**
  1. What is the modified timestamp in the $STANDARD\_INFORMATIO N attribute? (4 pts)
* **Sun, 28 Dec 2014 14:27:24 and the byte offset range is 88-95**
  1. What is the record update timestamp in the $STANDARD\_INFORMATION attribute? (4 pts)
* **Thu, 15 Jan 2015 00:53:13 and the byte offset range is 96-103**
  1. What is the accessed timestamp in the $STANDARD\_INFORMATION attribute? (4 pts)
* **Sun, 15 Feb 2015 15:38:41 and the byte offset range is 104-111**
  1. What is the name of this file? (3 pt)
* **louisvilleshot.doc; the byte offset range is 242-276**
  1. 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)
* **4 in $STANDARD\_INFORMATION: creation date, last modified, last record update, last accessed date.**
* **4 in $FILE\_NAME: creation date, last modified, last record update, last accessed date.**
* **8 in total.**
  1. What is the starting cluster of this file? (3 pts)
* **The starting cluster of this file is 0xD9FC03, 261337 in decimal and the offset range is 347-349.**
  1. Is the content of this file resident or non-resident? (3 pts)
* **The contents of this file are non-resident because the offset 0x08 from the beginning of the attribute 0x80 is set to 0x01. The offset range is 288.**
  1. How many $DATA (0x80) attributes does this file have? (3 pts)
* **The file has 2 data attributes because there are two 0x80’s and the offset range is 280 for the first 0x80 and 352 for second 0x80.**
  1. Is this file fragmented? How do you know? (3 pts)
* **The file is not fragmented, and I know this because there is only one data run. There are multiple data runs when the file is fragmented.**
  1. Is this the first time this MFT record has been used within the file system? How do you know? (3 pts)
* **No, it is not the first time the MFT record has been used and I know this because offset 0x16 is 0x00 which basically means a deleted file (which means there was a different file before this one). The byte offset range is 22-23.**
  1. What is the full path to this file in the file system? (EXTRA CREDIT – 1 PT)
* **C:\Users\Shivani Patel\Desktop\Project2-MFTRecord**
  1. What is the full name of each named data attribute and what is its content? (EXTRA CREDIT – 3 PTS)
* **$STANDARD\_INFORAMTION : stores file times created, last modified, last accessed, last record update and stores file flags such as read-only or hidden.**
* **$FILE\_NAME : Standard attribute header, name of the file/directory, Timestamps, MFT record number of parent directory**
* **$DATA: stores file data or data runs to non-resident files**
* **There are 2 different types of data attributes, named and unnamed. It is not necessary to have a named attribute.**

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)

* **Laptop Model - ASUS – Q534UXK**
* **Windows 10**
* **Lexar 8 GB thumb drive**
* **1 TB SSD**
* **WinHex 19.7**
* **MFT Stampede 1.9**
* **Windows calculator to lookup hex and decimal values**
* **Notepad**