Due: 9/12/2018 5:30 PM

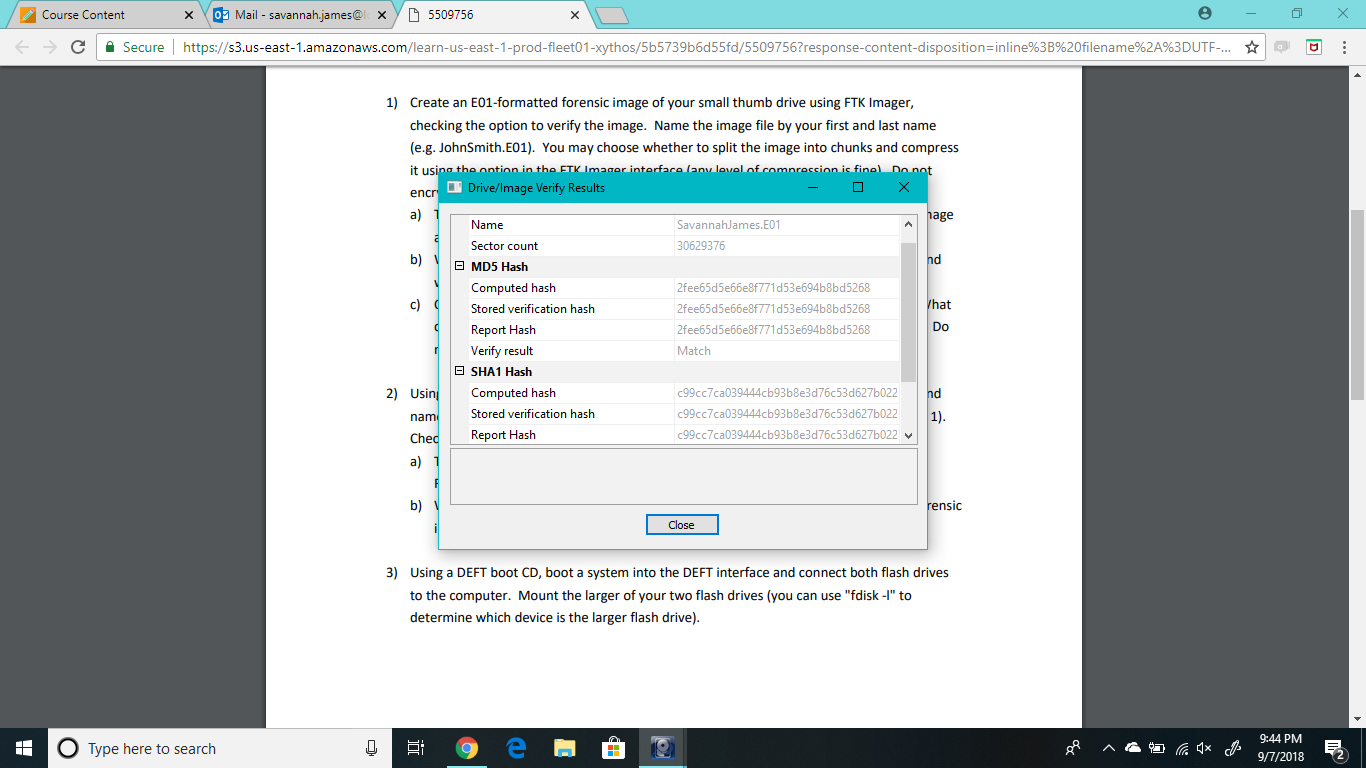
**CIS484-77-4188 Project 1 Notes:**

* **You will need two flash drives or media devices of different sizes and admin access to a Windows computer for this project.**
* **Both flash drives will need to be newly NTFS formatted. You may replace the larger flash drive with an external hard drive, but it must be newly NTFS formatted as well.**

**The small flash drive needs to have a few files on it.**

* **All required tools for this project may be downloaded using the links posted on Blackboard or provided during lecture.**
* **Submit your project by completing the “Project 1” test in BlackBoard. The test will be the same questions as below.**

For this project, complete the following tasks:

1. Create an E01-formatted forensic image of your small thumb drive using FTK Imager, checking the option to verify the image. Name the image file by your first and last name (e.g. JohnSmith.E01). You may choose whether to split the image into chunks and compress it using the option in the FTK Imager interface (any level of compression is fine). Do not encrypt the image.
   1. Take a screenshot of the verification window indicating that the hashes from the image and original evidence match. (7 pts)
   2. What is the significance of the verification option? Explain what this option does and why it is important. (8 pts)

**The verification option in FTK Imager is extremely important. This can help verify the integrity of your forensic image with your source file. This can prove to anyone that if the hash provides a match, the forensic image is an exact copy of your source disk file.**

* 1. Open the image file you just created in FTK Imager and create a directory listing. What does the listing include? How might this be helpful during a forensic examination? Do not include the directory listing itself in your write-up. (7 pts)

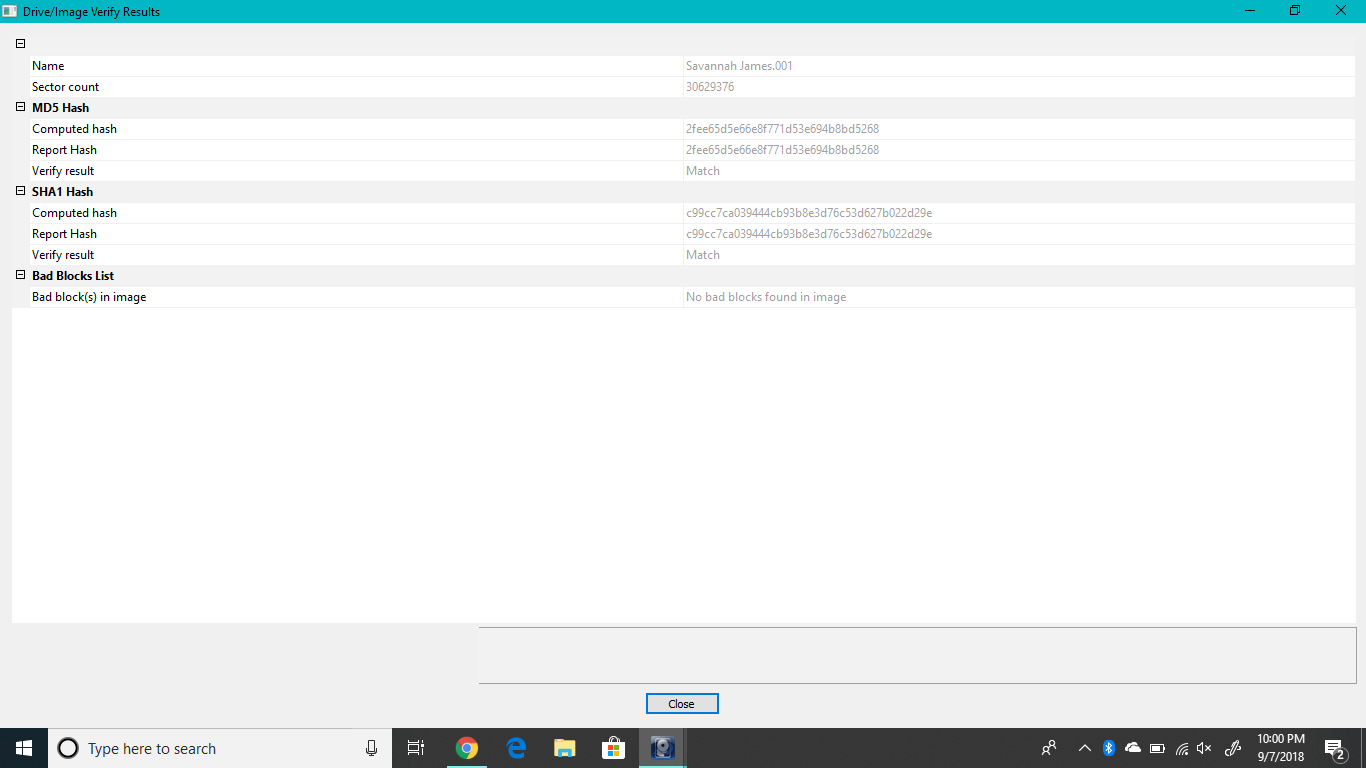
**The directory listing includes file names, full paths, size (in bytes), the date file was created, date file was modified, date file was accessed, and it also says if file is deleted or not. This could be helpful in a forensic examination to see the type and size of files you are dealing with and you can see if there are any files that have been deleted on the drive that you can uncover later in the forensic process.**

1. Using FTK Imager, convert the E01 image file you created in Part 1 to Raw/DD format and name the Raw/DD formatted image by your first and last name (as with the E01 in Part 1).

Check the option to verify the image.

* 1. Take a screenshot of the verification window indicating that the hashes from the

Raw/DD formatted image and the E01 formatted image match. (7 pts)



* 1. What benefit(s) exist in using a raw/DD image as compared to an E01 formatted forensic image? What are the disadvantages? (7 pts)

**Raw/DD Image – Advantages: you can write bit-stream data to files. You also have a wider range of tools that can read and work with raw format. Disadvantages: Raw/DD Images require a lot of storage, almost as much storage as the original disk. The verification process for these type of images is much slower.**

1. Using a DEFT boot CD, boot a system into the DEFT interface and connect both flash drives to the computer. Mount the larger of your two flash drives (you can use "fdisk -l" to determine which device is the larger flash drive).
   1. Make a raw forensic image of the small flash drive using dcfldd, generating a hash on the fly. The image and MD5 hash should be written to the large flash drive. Include a calculation of the hash and the command used to image the device in your report. (7 pts)

**e0038d9079fa6a3f070cf622acf01cf3**

**dccfldd if= /dev/sdb of=/mnt/x/image.dd hashlog=/mnt/x/hash.txt hash=md5 hashlog=/mnt/x/sourceMD5.txt bs=4k**

* 1. What is the difference between imaging “/dev/sdc” and “/dev/sdc1”? Why is this important? (7 pts)

**/Dev/SDC1 is a partition of the device, while /Dev/SDC is the entire device itself. Only imaging the partition may result in data loss of information that was on the device, and not in the partition.**

* 1. After the forensic image is completed using dcfldd, calculate the MD5 hash of the forensic image you have just made using the md5sum command. Redirect the output to a file on the large flash drive. Include this command and the resulting hash value in your report. (5 pts)

**e0038d9079fa6a3f070cf622acf01cf3**

**md5sum /mnt/x/image.dd>/mnt/x/imageMD5.txt**

* 1. Review both MD5 hashes of the small flash drive using the "cat" command. Do they match? What does this mean? (5 pts)

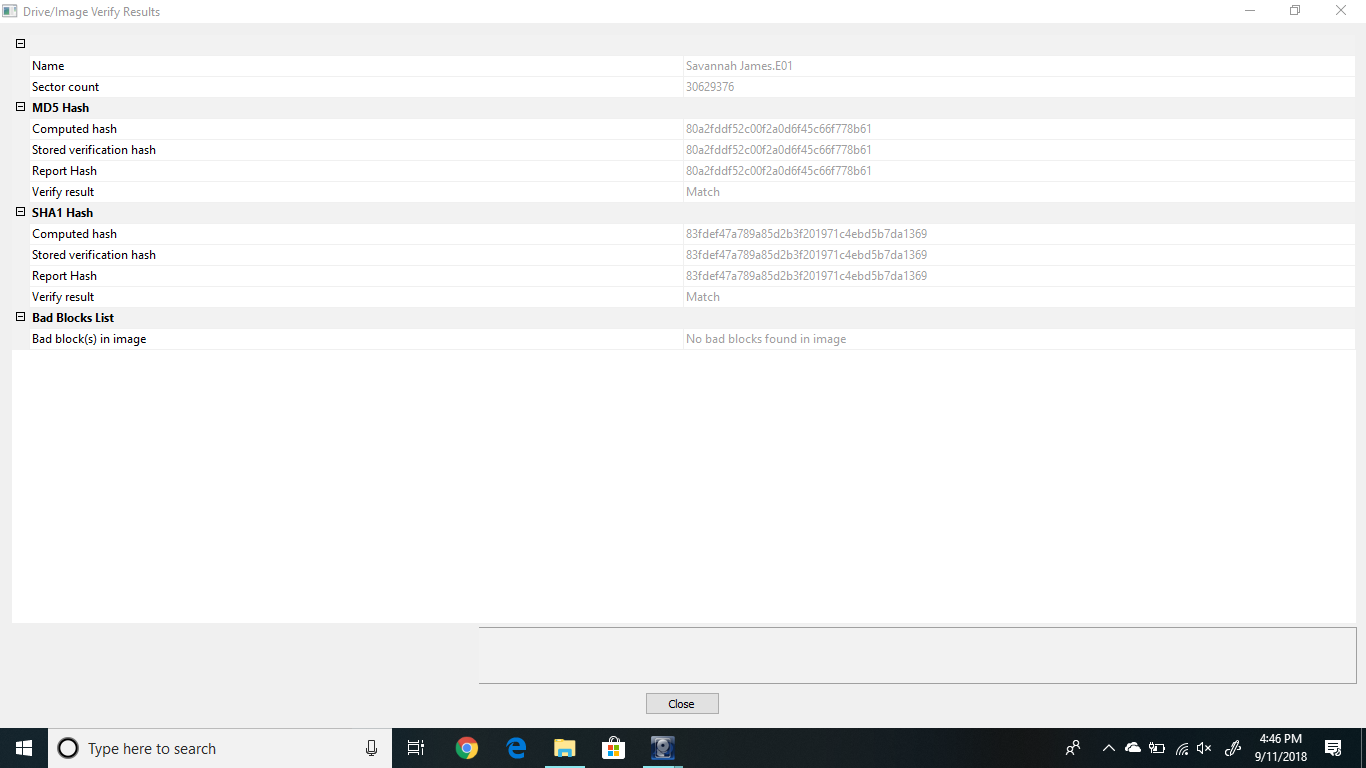
**Yes, the MD5 hashes match. This means that the image that was created from the source is identical to the source drive.**

1. Create a text file named "firstname\_lastname.txt" (adding in your actual name), then save the file to the small thumb drive. Copy a few other files (10-15) to the small flash drive.

Now delete all files from the small flash drive except the text file with your name.

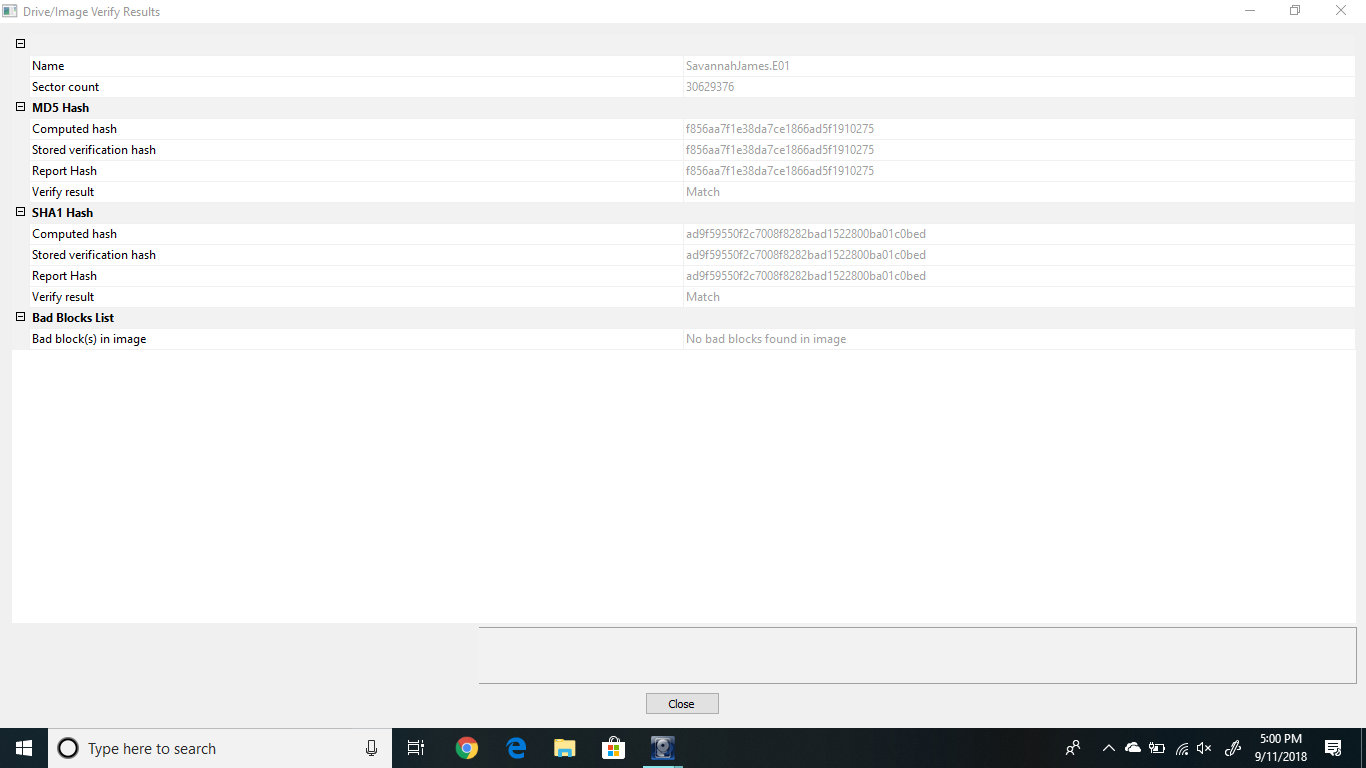
* 1. Calculate the MD5 hash of the thumb drive using WinHex, FTK Imager, or any other tool of your choice and record the hash in a text document. Include a screenshot of the hash output from the tool in your write-up. (4 pts)

**FTK IMAGER:**



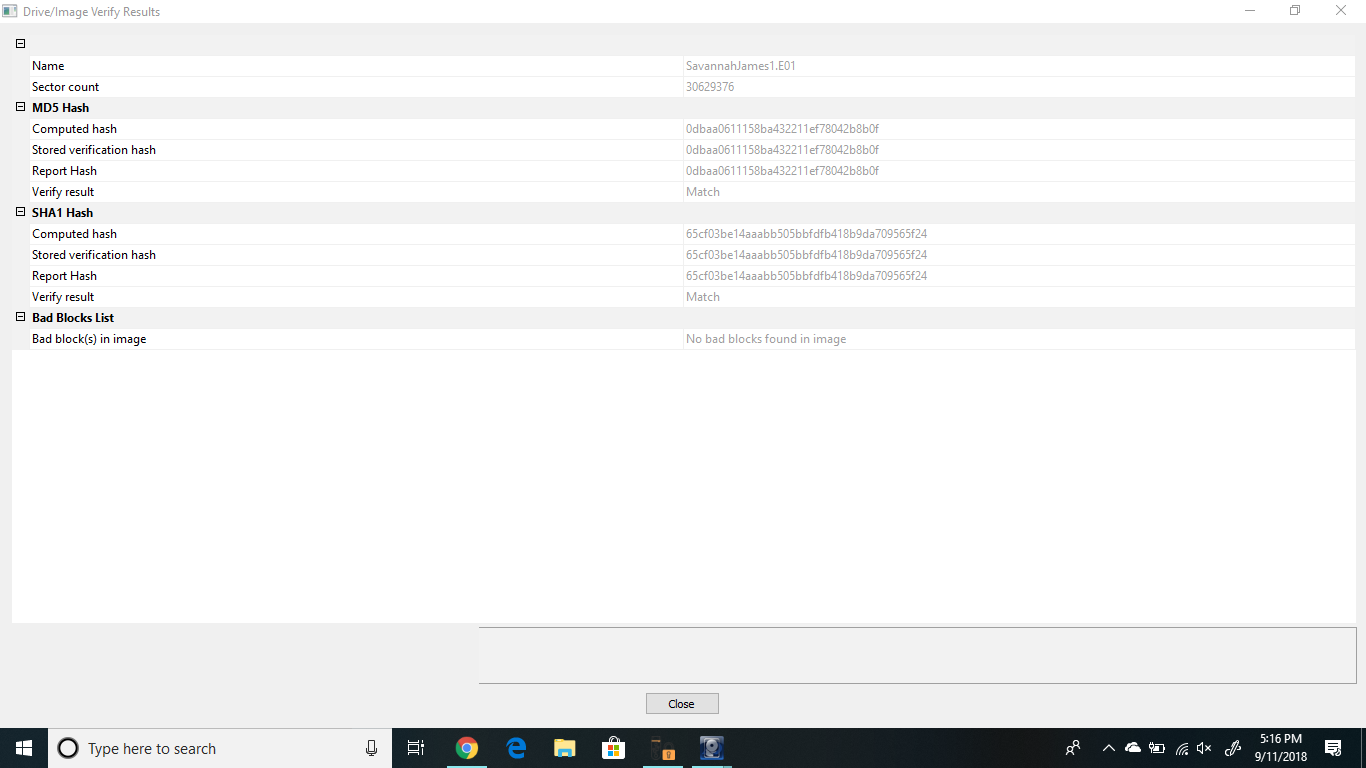
* 1. Now unplug the thumb drive from the computer and plug it back in. Using the same tool as before, calculate the MD5 hash of the flash drive. Do the hashes match? What can you conclude based on the matching (or non-matching) of the MD5 hashes? (6 pts)

**The hashes do not match. This is because the flash drive was unplugged. The flash drive may have changed hashes because of this, or because it recognized after the drive was unplugged that files were deleted/added.**



* 1. Remove the flash drive from the computer. Now use a tool such as thumbscrew to turn on USB write-blocking. Be sure to run the write-blocking tool as an Administrator. After you have disabled writing to USB devices, connect your flash drive to the computer. **NOTE: Your flash drive must not be connected to the computer when enabling USB write-blocking.** Now try to write a file to the thumb drive; are you able to? Generate another MD5 hash of the USB device. Is the hash value identical to the previous hash? Is this process forensically sound? Why or why not? (10 pts)

**No, I am unable to write a file to the thumb drive since write blocker is on. The hash is identical, because the file could not be added which means that the hash value would be the same as before. This process is forensically sound because this is how you are able to prove that the hash has not changed if write blocker is on, this would also help prevent writing anything to the original copy of evidence.**



1. Compare and contrast using dcfldd and FTK Imager to create a forensic image:
   1. What are the advantages and disadvantages of both? (5 pts)

**FTK Imager - Advantages: FTK Imager stores images in proprietary image formats. The advantage of this type of format to create a forensic image is that you can compress the image. You can also use metadata to distinguish the files from others. You can include a case number, evidence number, unique description, examiner, and any other notes. FTK imager also uses a user interface which makes it easier to add evidence and review it. You also can compress images or encrypt images. Disadvantages: much more difficult to share image between tools that are not FTK Imager.**

**DCFLDD – Advantages: More tools can read and work with raw format files and images. Disadvantages: As a beginner, DCFLDD is much more difficult to use because it is command line based. You must know what you want to do to each of your drives to use it, there is not any help on the program itself. Verification is much slower in DCFLDD than in FTK Imager.**

* 1. If you were tasked with acquiring a forensic image of a storage device, which tool would you use and why? (5 pts)

**If I had to acquire a forensic image of a storage device, I would choose FTK Imager. FTK imager is much easier to use and understand when creating a forensic image. It also walks you through the steps, so you can choose if you want an E01 format or Raw/DD format, etc. I would also be able to verify/create directory listings as well as encrypt files if needed.**

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**

**Flash Drive- SanDisk Cruzer Blade 32GB**

**FTK Imager**

**Deft 8.2**

**DCFLDD**