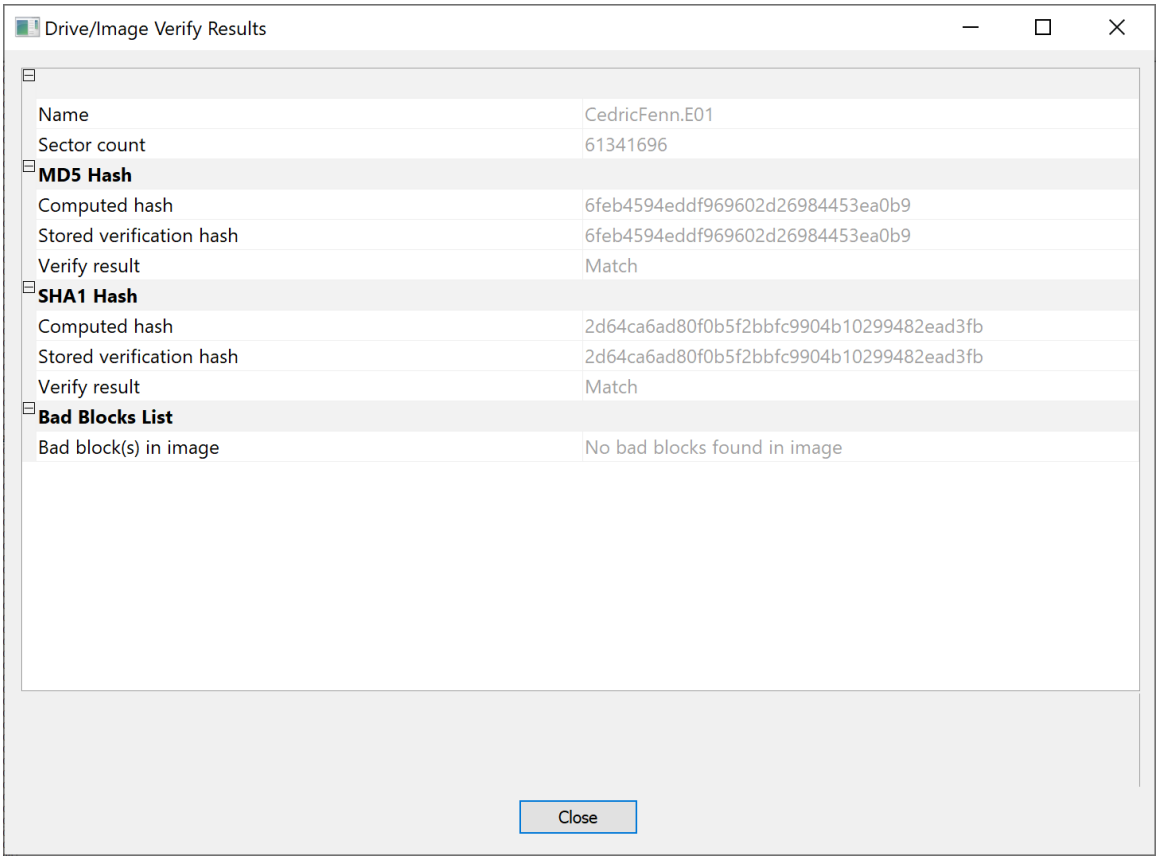
For this project, complete the following tasks:

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.
   a) Take a screenshot of the verification window indicating that the hashes from the image and original evidence match. (7 pts)



   b) What is the significance of the verification option? Explain what this option does and why it is important. (8 pts)

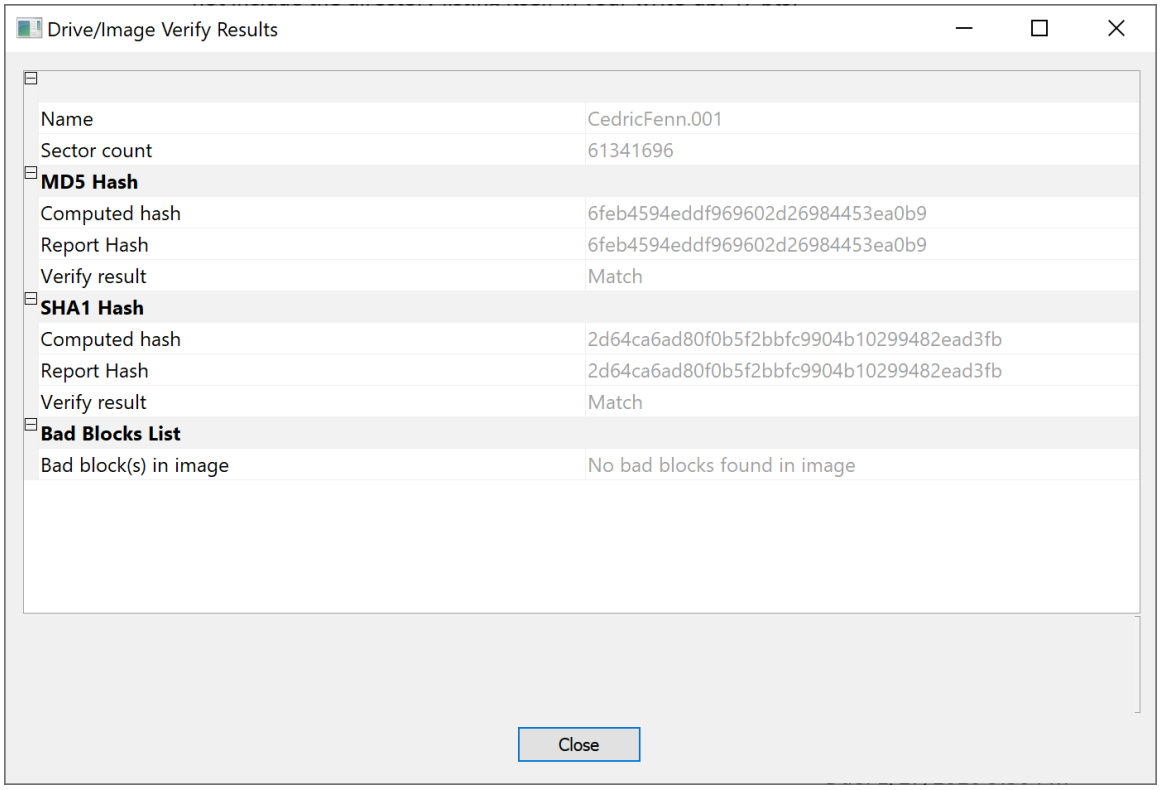
The verification option uses MD5 and SHA1 has values to create a matching unique value for the original source and the image. This is significant because the matching values are used to assure that your evidence is a perfect match.

c) 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)

This listing includes the following fields: Filename, Full Path, Size (bytes), Created, Modified, Accessed, and Is Deleted (Y/N). This is helpful during forensic examinations to verify alleged timeframes files were accessed, changed, and if they were deleted or not. This can be upheld and justify statements in court.

2) 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.

a) 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)



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

The benefits in using a raw/DD image is that it contains more information and higher quality files and can be used with 3-rd party software. The disadvantage is that raw/dd images are not compressed files and the image can be much larger than an E01 file.

3) 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).

\

a) 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)

Hash

Total : 96995b58d4cbf6aaa9041b4f00c7f6ae

Command

dcfldd if=/dev/sda has=md5 of=/mnt/c/image.dd hashlog=/mnt/c/image.txt bs=4k

b) What is the difference between imaging "/dev/sdc" and "/dev/sdc1"? Why is this important? (7 pts)

"/dev/sdc" is the the raw device and "/dev/sdc1" is the partition of the device. This is important because sdc includes all data on the device and not all information is captured on sdc1 because of the partition.

c) 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)

Command

md5sum /mnt/c/image.dd > /mnt/c/imagehash.txt

Hash Value

96995b58d4cbf6aaa9041b4f00c7f6ae

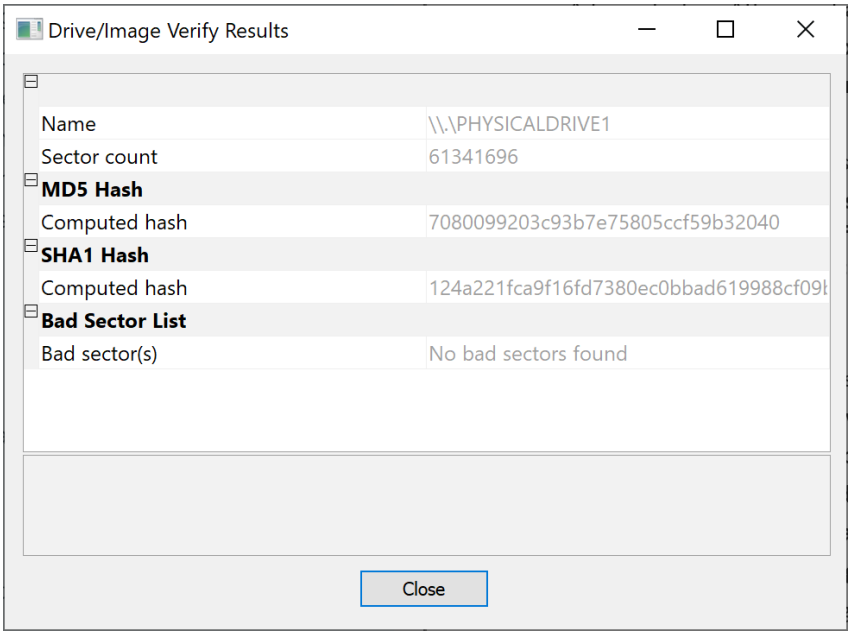
d) Review both MD5 hashes of the small flash drive using the "cat" command. Do they match? What does this mean? (5 pts)

cat /mntc/image.txt; cat /mnt/c/imagehas.txt

The hashes match. This means the true drive matches the image file exactly and can be used a forensic proof.

4) 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.

a) 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)



b) 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)
After unplugging and plugging the USB drive back in, the MD5 hash values did not match. The process of unplugging and plugging the drive in must have written new data about the drive, for example the time value of the drive being accessed.

c) Remove the flash drive from the computer. Now use a software write-blocking tool (such as this one) 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)

After using the write-blocking tool I was unable to write anything to the USB drive. The hash value was identical to the hash right before the write blocker was enabled. The process is considered to be forensically sound since hash values are undeniable proof that nothing was written to the USB drive.

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

Dcfldd has the advantages of having a built-in hashing function using hash log. You also get the expected output using specific commands without restrictions. The disadvantages are the command-line interface and the learning curve to use it.
The advantages of using FTK Imager is the support of encryption/decryption and its easy to use GUI. The disadvantage is there is no flexibility with commands for specific uses.

b) If you were tasked with acquiring a forensic image of a storage device, which tool would you use and why? (5 pts)
I would use FTK Imager if I were to acquire a forensic image of a storage device. The ease of use, encryption and decryption, evidence storage, E01 and Raw DD support have the advantage over other tools.

6) 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 Inspiron**
- **Windows 10 Pro OS**
- **16 GB infinitive USB drive**
- **32 GB infinitive USB drive**
- **VMware Workstation 15.5 Pro**
- **Deft 8.2 iso**
- **dcfldd**
- **FTK Imager**