Project 1

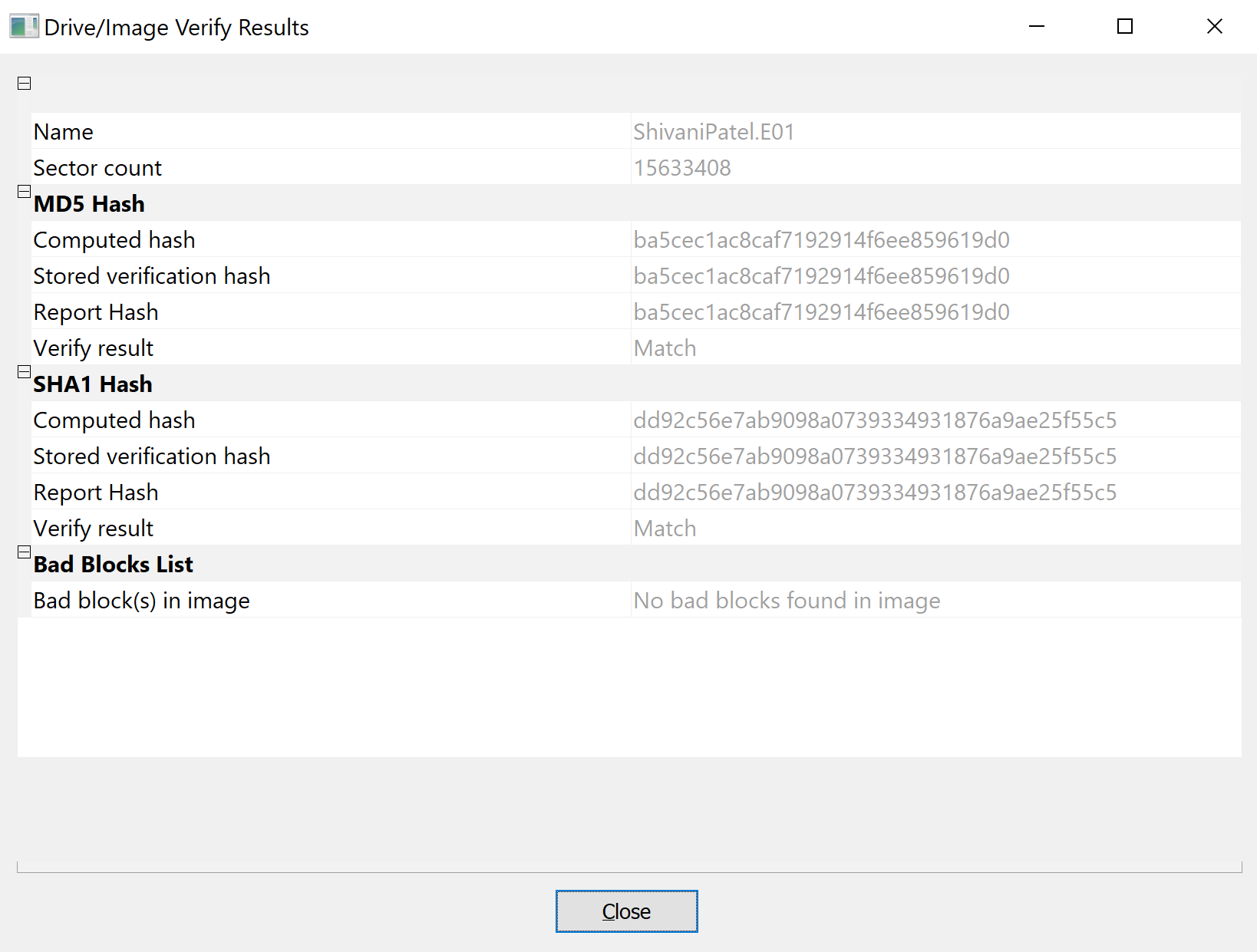
CIS 484 - 77

Shivani Patel

**CIS484-77-4188 Project 1**

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)



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

**The significance of the verification option is that it uses hash values to compare the original source of evidence with the created image. This option is to prove that the image created is an exact copy of the source of evidence. It is important when we need to present an evidence in the court or for future preferences and it is a solid method to prove that the image is an exact duplicate to the original disk.**

* 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)

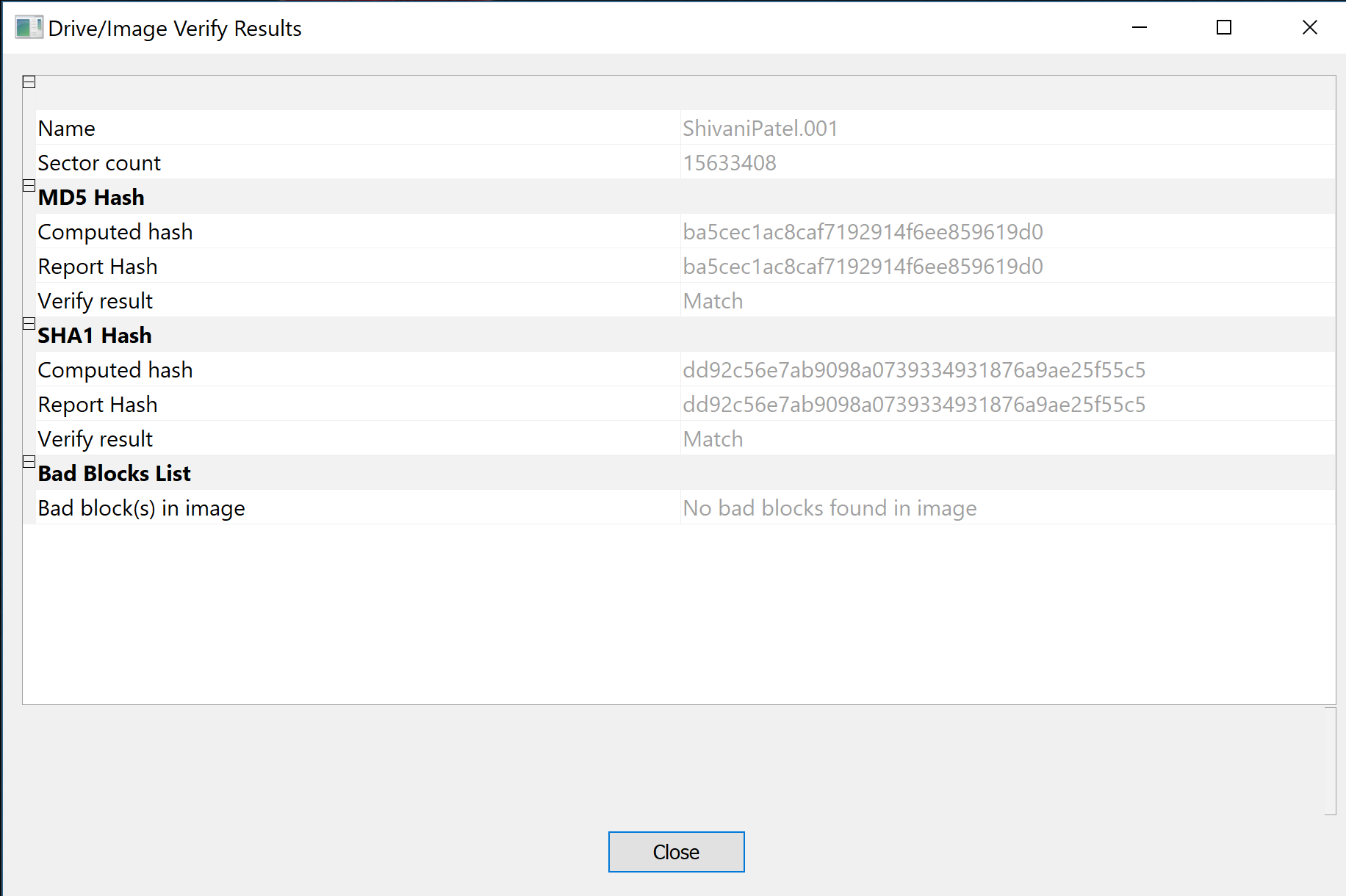
**The directory listing includes File Name, Full path, Size in bytes, Date created, Date modified, Date accessed and if the file is deleted or not.**

**This can be helpful during a forensic examination because it provides evidence of the files that are on the drive and the meta data about those files which include when the file was created, modified, accessed or deleted. This can be very helpful when presenting a case in the court.**

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)

**A benefit of using a Raw/DD is that it makes it possible to write bit stream data to files, it includes fast data transfers, and it is compatible with other software’s.**

**Disadvantages of having a raw/dd image are that it is uncompressed, therefore the raw format requires as much as storage as the original disk (may require a lot of space).**

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)

**Total (md5) : 2dc3bb764c0d06ce5a673fee0859abcd**

**dcfldd if=/dev/sdc of=/mnt/x/image.dd hashlog=/mnt/x/hash.txt hash=md5 bs=4k**

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

**The difference between the “/dev/sdc” and “/dev/sdc1” is that /dev/sdc is the raw device where /dev/sdc1 is the virtual device or partition. This is important because if the image was sdc1, some data may not be captured in the image because it would not be the raw device but only 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)

**2dc3bb764c0d06ce5a673fee0859abcd**

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

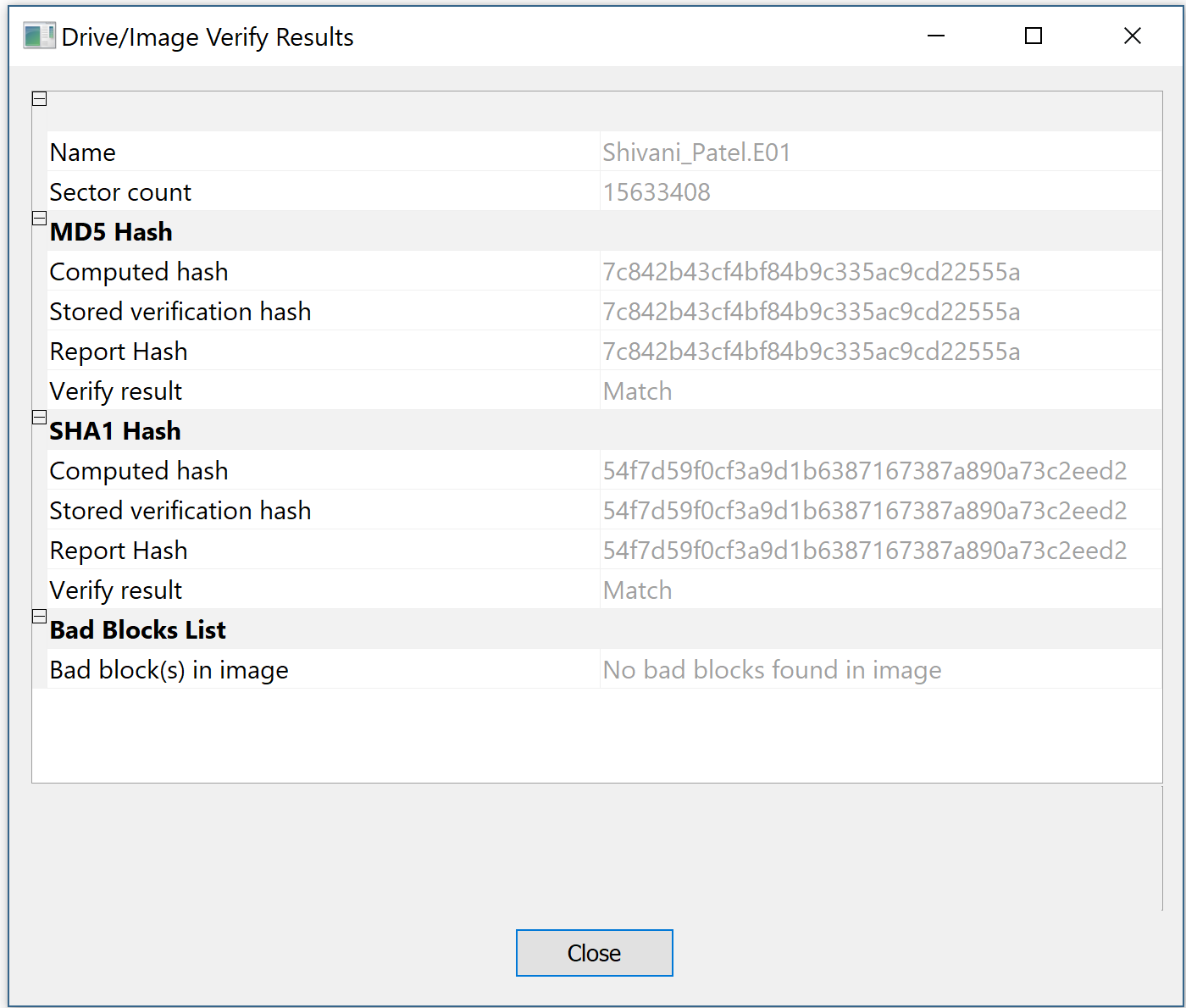
* 1. Review both MD5 hashes of the small flash drive using the "cat" command. Do they match? What does this mean? (5 pts)

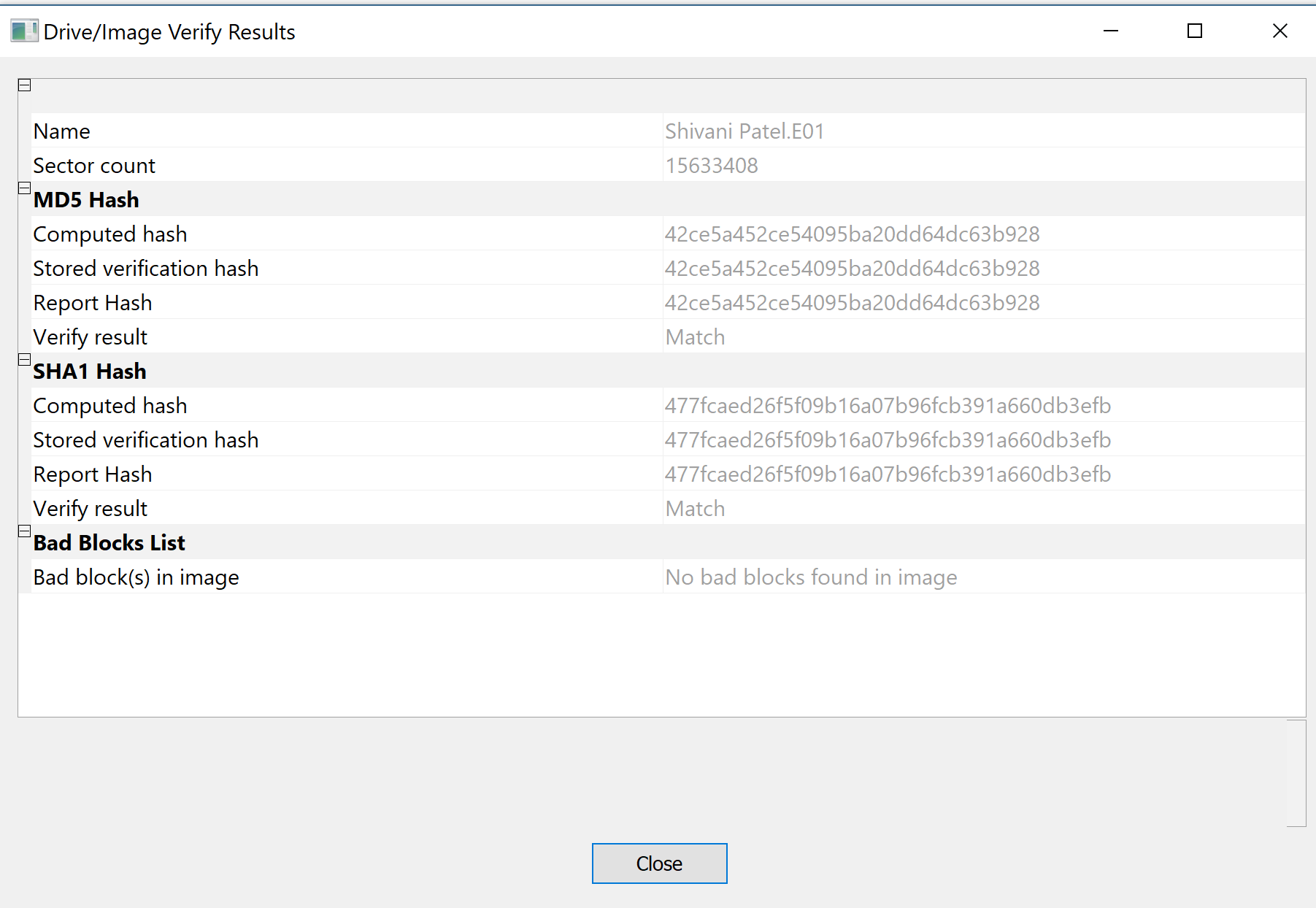
**cat mnt/x/imagehash.txt**

**The hashes matched which means the image creation process was successful and the input data from the forensic image matched the data from the original data from the source drive. There were no errors during the process of imaging.**

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) 
  2. 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 did not match because the thumb drive was unplugged and re-plugged in the computer, therefore the meta data about the drive and it’s files were changed and because of these changes the hash values changed as well.**

* 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)

**I was unable to write a file to the thumb drive because the USB Write blocker was enabled. The hash value was the same because the write blocker prevented any changes to the file. This process is forensically sound because the write blocker ensures that the image matches the original drive and nothing has been changed. Write blocker is a must for forensic analysis.**

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)

**Advantages:**

**Advantages for FTK Imager includes file encryption, file compression, E01 file support. It can perform live acquisitions by being installed on a flash drive which does not leave any doubts on the victim by not installing a software on the victim. It is also more user-friendly because it does not require much syntax knowledge. FTK Imager has an option to save the image to multiple places simultaneously; this is useful if the investigator wants to save both a local copy of the image and a copy over the network to a file server.**

**Advantages for dcfldd includes that it can accept files as input sources. It takes less time to create an actual forensic image compared to FTK Imager.**

**Disadvantages:**

**Disadvantages for FTK Imager includes that it only runs on windows. It cannot use files as an input source and it does not support Ex01 files. It takes more time to create the actual forensic image and generate results compared to dcfldd command.**

**Disadvantages for dcflff includes no file compression, no file encryption. It does not support E01 files.**

* 1. 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 dcfldd command in most cases because the advantage of using dcfldd over FTK Imager is that dcfldd accepts the single file as input sources and it would also take less time.**

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**
* **VM Workstation Pro**
* **Deft 8.2**
* **Access Data FTK Imager 3.4.3.3**
* **1 \* 8 GB Flash Drive**
* **1 \* 32 GB Flash Drive**
* **USB Write Blocker**
* **Dcfldd**