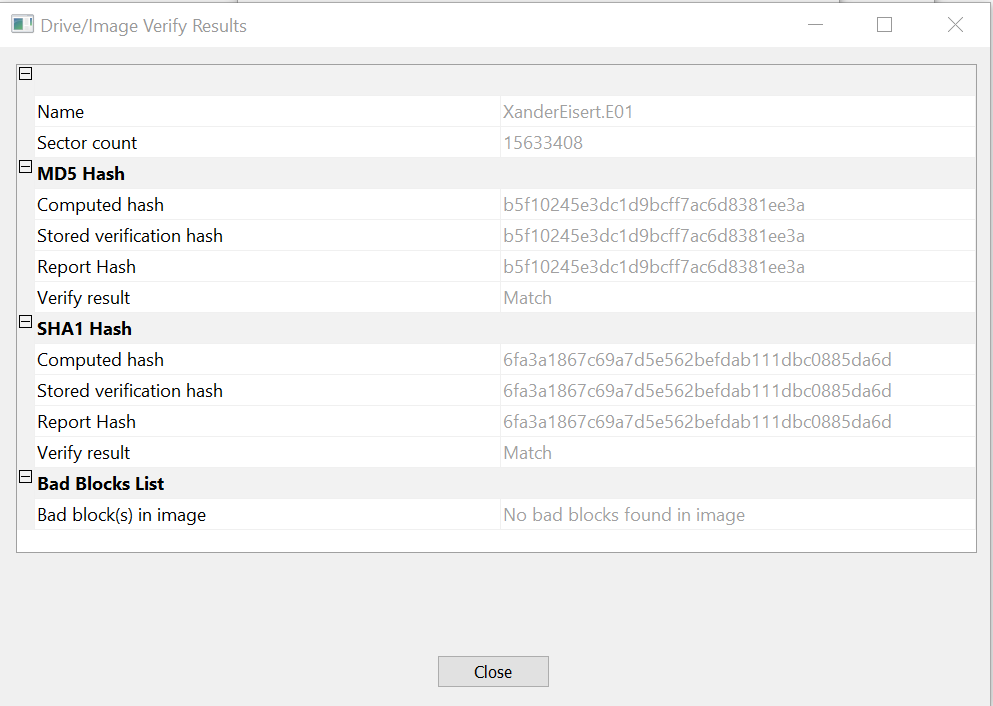
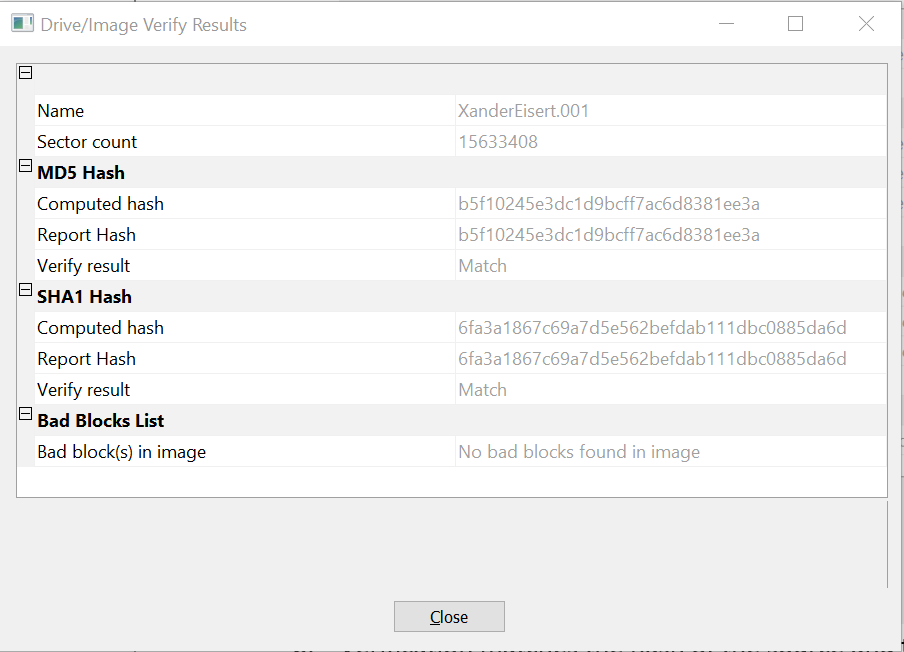
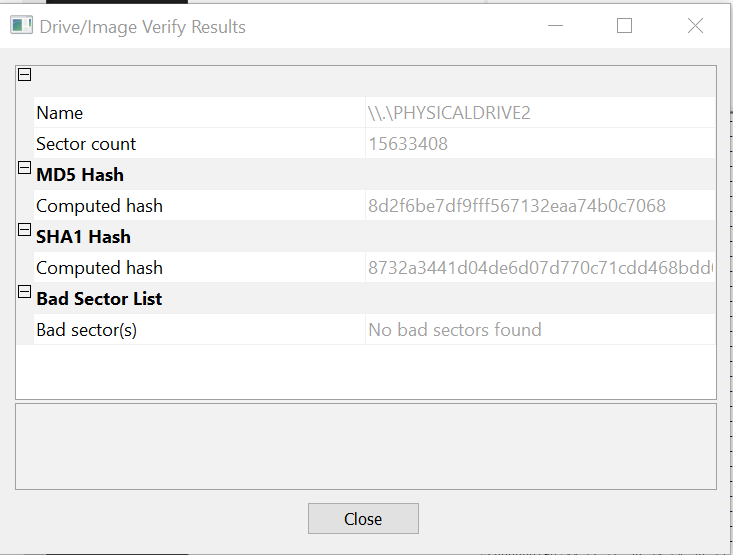
Project 1 Answers

1. FTK Imager
   1. 
   2. Verification matches the hash of the source and the hash of the destination files to one another. Hashing verifies the image file’s integrity.
   3. Opening the file in FTK and creating a directory listing shows all files and all folders in the drive in a single CSV file.
2. FTK Imager cont’d
   1. 
   2. Benefits of Raw/DD images include multiple tool compatibility and versatility. Disadvantages include the lack of file compression and the longer verification times needed.
3. DEFT
   1. dcfldd if=/dev/sdc of=/mnt/x/image.dd hash=md5 hashlog=/mnt/x/sourceMD5.txt bs=4k is the command, D41D8CD98F00B204E9800998ECF8427E is the hash
   2. /dev/sdc1 is the first partition of the drive, while /dev/sdc is the entire drive itself. Data must be written to a partitioned table on the drive.
   3. md5sum /mnt/x/image.dd > /mnt/x/imageMD5.txt is the command, D41D8CD98F00B204E9800998ECF8427E is the hash
   4. The hashes match, meaning the images are a carbon copy and are the same in every sense.
4. Hash
   1. 
   2. The hashes do not match, which indicates that data was written/overwritten between my unplugging and plugging back in the drive.
   3. I am not able to write to the drive now that write blocking is enabled for USB devices. After recalculating the hash, it is identical to the value I got before, which means that this process is forensically sound since the drive has not been altered from its previous state.
5. DCFLDD vs FTK Imager
   1. DEFT is a much more advanced way of creating forensic images, but it has a drawback of being a more difficult program to use, requiring bypass of the OS on a system in order to boot into a Linux environment. It comes with write-blocking enabled though, as due to the nature of Linux, mounting drives can be made a manual process. FTK is more user-friendly and comes with more imaging options, including compressed images to save on drive space.
   2. I would probably use FTK Imager and a write blocker in hardware/software simply due to the fact that I’m more familiar with it as a program. Navigating DEFT took me a good 4 days to complete with other people’s help.
6. Software/Hardware listings

Hardware: Surface Laptop 3, Sandisk Cruzer 8GB, Sandisk Fit 32GB, Anker USB-C hub

Software: DEFT-8.2 Ubuntu, VMWare Workstation 15.5, FTK Imager 4.2.1, Snip and Sketch, MS Word, Thumbscrew (Write-blocker)