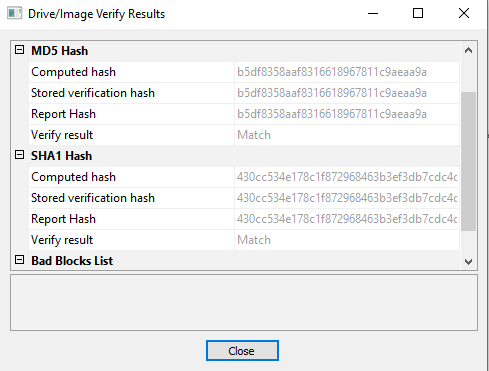
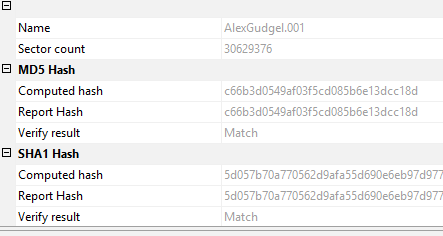
1. A.



B. The verification option is to ensure data integrity. If the hashes don’t match then the data has been tampered with.

C. It lists the directories and files on the image. This can be helpful during forensic imaging because you might need to retrieve a certain file or directory.

1. A.



B. The benefits are most forensic tools and non-forensic tools can read the format. Also, it is a complete bit stream image. Disadvantages are it requires as much storage as the original disk and verification pass can be slower.

1. A. Command: dcfldd if=/dev/sda of=/mnt/x/image.dd hash=md5 hashlog=/mnt/x/hash.txt bs=4k

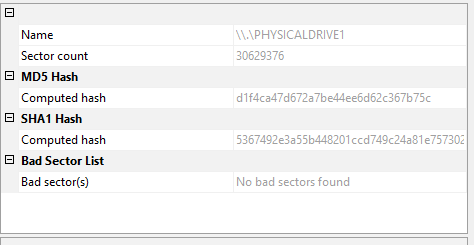
Hash: b2180e88526da3fc6e7ab3711fa3a2ae

B. The difference is the sda1 is just the first partition on the device and /dev/sda captures the entire device which is what we want for the image.

C. md5sum /mnt/x/image.dd > /mnt/x/image.hash cat /mnt/x/image.hash Hash: b2180e88526da3fc6e7ab3711fa3a2ae

D. Yes they match and this means that data integrity was upheld during the imaging process.

1. A.



B. The Hashes do not match because it seems that windows writes to the hash every time it is connected to the computer.

C. Not able to write to the USB drive. Yes the hashes are the same and is forensically sound because it ensures the data integrity of the drive when collecting data.

1. A. Advantages of FTK imager is it’s more user friendly with a graphical user interface.

Disadvantage of FTK Imager is if a write blocker is not enabled then the hashes will be different every time you connect and disconnect the drive.

Advantages of dcfldd is since it is a linux method boot disk you do not necessarily need a write blocker.

Disadvantages of dcfldd is it is strictly a command line interface so you must know the right commands to image. Becomes more complicated.

B. I would use FTK Imager because I am more familiar with how to use the tool. I use it at work when imaging terminated employee drives.

1. FTK Imager, Linux, Windows, DEFT 8.2, HP notebook, VMware, USB Write-Blocker, SanDisk flash drive