Paige Fenwick

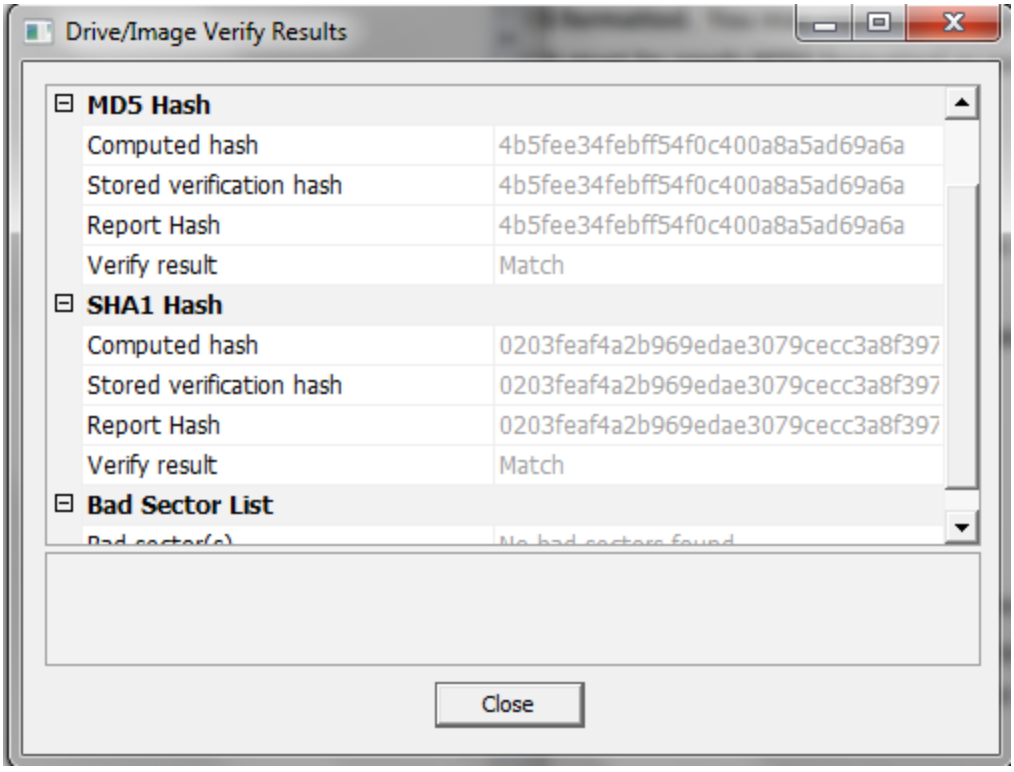
CIS 484-75

Jason Hale

Project 1

FKT Imager

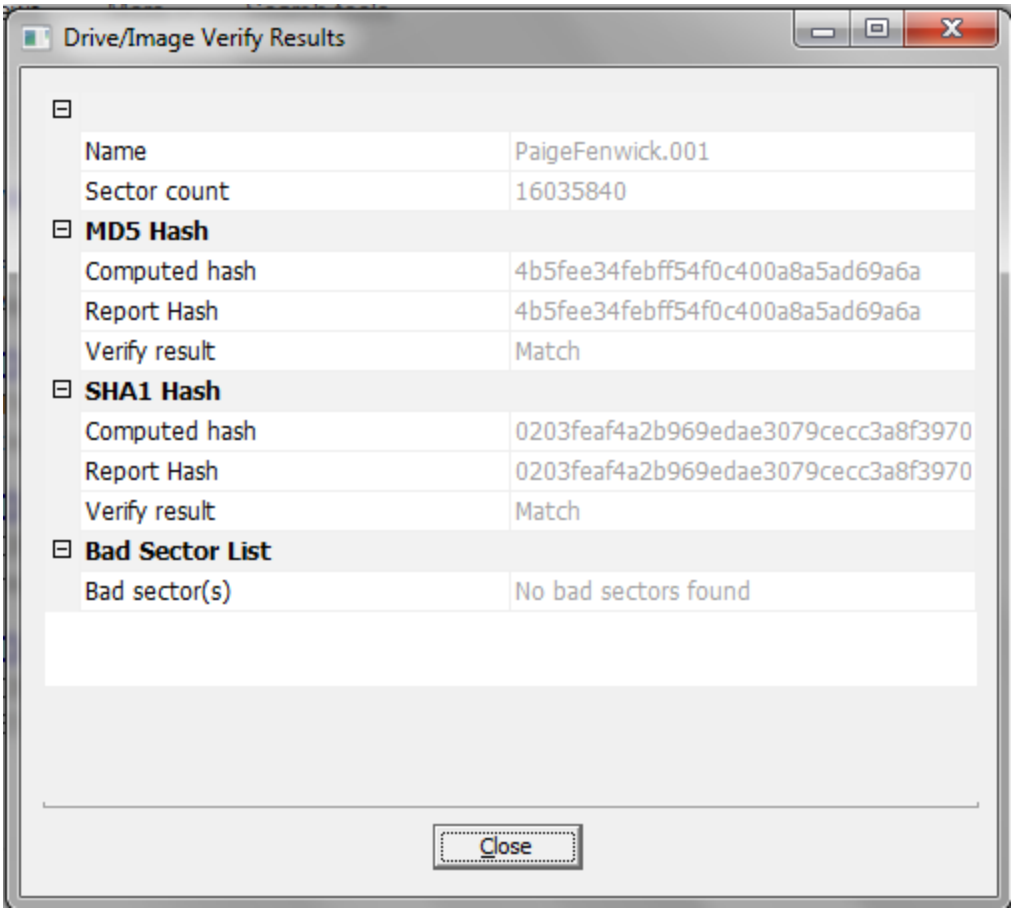
1a.



1b. By clicking the verification option, you are ensuring that the FTK Imager will calculate MD5 and SHA1 hashes of the acquired image. These hashes are used to ensure data integrity by comparing the computed has and the stored verification hash. If the two match, the integrity of the device is ensured.

1c. The directory listing includes the file name, full path, size, the created, modified and accessed dates and if the file is deleted. During a forensic examination, this could help an examiner determine the files that are and were present on the device, where they were located and whether or not they were deleted. This can help to find the deleted files.

2a.



2b. The raw/DD image format can be compatible with nearly every forsenic tool out there. Addtionally, raw images are not compressed but can be broken down into multiple parts. Since since file format is not compressed, it can become very large which is a disadvantage. Also, there is no metadata kept when using this file format.

3a. The following command was used to image the smaller flash drive:

Dcfldd if=/dev/sdb of=image.dd hash=md5 hashlog=sourceMD5.txt

The following hash was calculated:

c613332c8afc3741e274711a603c595f

3b. /dev/sdc references the entire device, which is the larger flash. /dev/sdc1 references one partition within the flash drive. This is important because you may want to image a single partition of the device or the entire device which means you need to call the appropriate device name.

3c. The following command was used to calculate the hash of the forensic image:

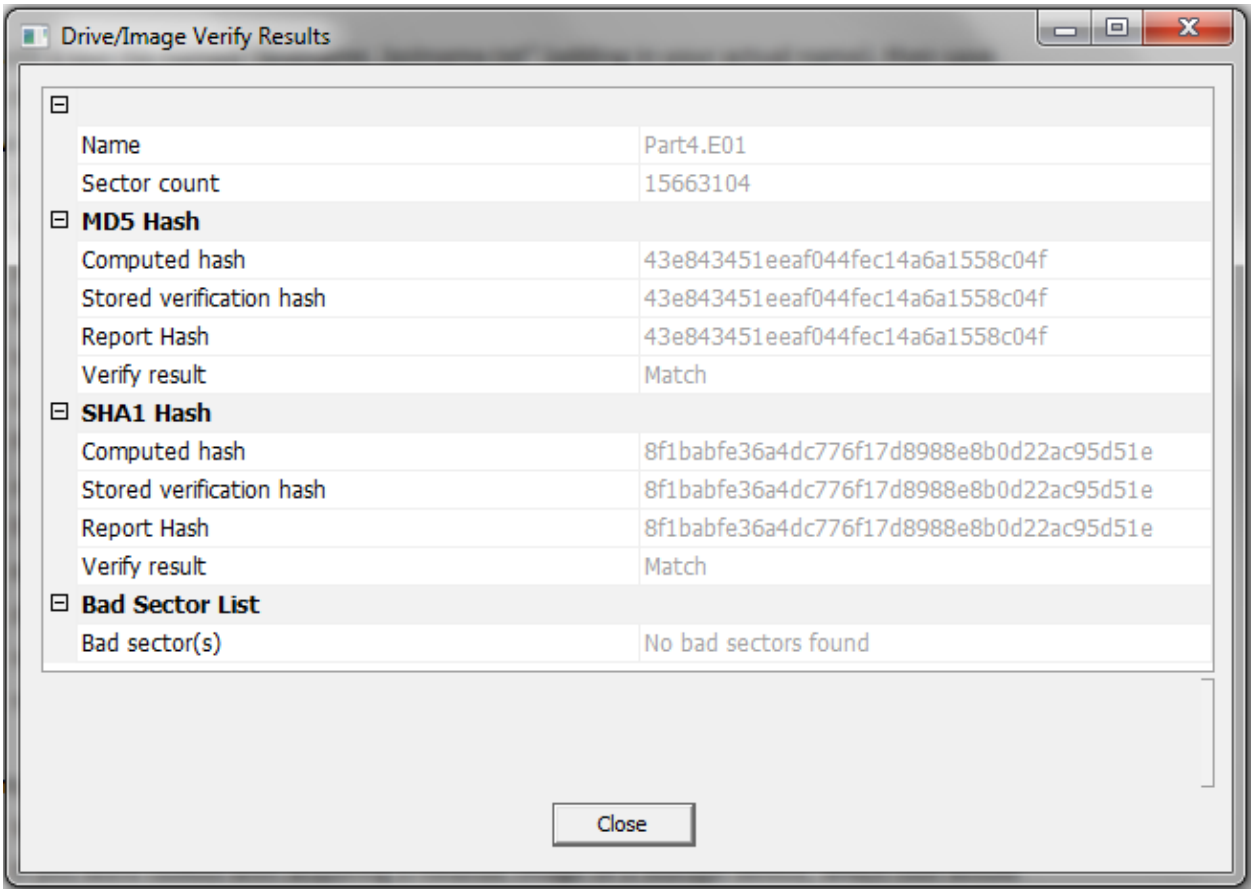
Md5sum image.dd > imageMD5.txt

The following hash was calculated:

c613332c8afc3741e274711a603c595f

3d. Both of the hashes match which means that the integrity of the devices was kept and the information between the forensic image and the device is the same.

4a.



4b. The two hashes are not the same. This could be because in the first part of the exercise, we copy files and deleted them into the flash drive and then ran the image. In the second part, we simply created an image after plugging in the flash drive. This created two different hashes because they were two different instances.

4c. The hash was same which indicates that this is forensically sound. This is because by turning on the write blocker, you are ensuring that files cannot be altered or added and this is another way of ensuring the integrity of the device. It is also ensuring chain of custody because there will no modification between transfers.

5a. FTK Imager and dcfldd are both important tools to have in a forensic toolkit. However, they are vastly different. FTK Imager is slightly simpler to use because the user is using a GUI interface instead of a command line and FTK Imager is easy to install and run on a Windows operating system. Some disadvantages of FTK Imager is that it is not supported by all operating systems and because the Imager is more of a simplistic program, it will not have all the functionality of a more developed imaging tool. dcfldd also has several advantages including the ability to create hashes on the fly, the ability to multi-task (creating multiple images at the same

time) and the tool is a more developed as compared to FTK Imager. Some disadvantages of dcfldd is that is more complicated as the user has to use the command line and install the iso into a virtual machine. This is more time consuming to set up and can be complicated as errors occur.

5b. I would be more inclined to use FTK Imager because of the ease of use I experience when using the program. It was more intuitive and I had an easier time understanding the documentation that accompanies FTK Imager than dcfldd.

6.

Hardware:

- 8GB Ativa Flash Drive
- 2TB Segate Expansion Portable Drive
- Lenovo ThinkPad

Software:

- Windows 7 OS
- DEFT iso
- FTK Imager
- Notepad
- VMware Workstation
- File Manager
- LXTerminal
- Windows Explorer