CCSI 410 Forensic Lab Report

1) Investigator’s Name: \_\_\_Matt Ferry\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2) Date of Investigation: \_\_\_07/17/2013\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3) Lab Number and Title: \_\_Lab 2: Create a Clone \_\_\_\_\_

4) Summary of Findings:

*Created a bit copy image of the suspects drive located on E: to the examination target drive located on F:. Compared the generated md5 hash codes and confirmed that they match. Answered the required questions in regards to identifying drives, preparing and wiping drives, the importance of hashing drive, an alternative way to create a bit-stream copy of a drive, and a command line way to generate hash values of a drive.*

5) Details of Investigation

Wednesday - 07/17/2013

11:55 am – Opened FTK

11:56 am – Opened FTK Imager

11:58 am – Imaged Suspects drive on drive E: to the Target drive on Drive F:

11:59 am – Created Screenshot’s of the Drive/Image Verify Results, and Image Summary Screens

12:01 pm – Closed FTK and Lab session

6) Please type the answers to the questions found throughout the lab here.

**Question 1 - Please list some ways you can identify drives (tell the difference between target and suspect drive) without tampering with the evidence.**

In general, your forensics station should be a computer that you are already familiar with, which means that you should already know what drives are installed, and what their designated drive letters are. While each case may involve a separate or new drive for the target evidence to be stored on, this can also be controlled by connecting and verifying the forensic integrity of the target drive first, before connecting the evidence drive for copying. This will allow also allow you to verify the drive letter of the target drive before the evidence drive is connected.

Next, if the evidence drive and target drives are both connected but the evidence drive has not been copied yet, you can tell the Evidence drive from the target drive, because the target drive should show to be empty, where the evidence will show to have data stored on it.

Lastly, if both the target drive and the evidence drive are already connected, and the evidence drive has already been copied. Unplug the evidence drive. This will leave only the target drive remaining. And if you cannot determine which physical drive is the target drive or the evidence drive you have made a catastrophic mistake elsewhere in the investigation long before you were ready to try and examine the evidence.

**Question 2 – Why do you need to prepare your drive? Why can’t you just delete all the files? Look up the DOS wipe.exe command on the internet. What did you find out about the command?**

You need to prepare the drive because you have to make sure that there is no information on the drive from previous cases, which would corrupt the drive data and drive hash value of the copied evidence drive.

You cannot just delete the files, because deleting the file, does not actually delete the file, it just removes the file allocation information and changes part of the filename. This means that the information that was on the hard-drive is still on the hard-drive but is now located in unallocated space or slack space. This information in unallocated space then becomes an issue when you try to copy a new evidence drive to the target drive. Even though you are performing a bit copy of the evidence drive, if your evidence drive is 100 GB, and your target drive is 200 GB the generated hash values of the two drives will not match because of information that is still left in the unallocated space from the previous investigation.

The DOS Wipe.exe command is a command line wiping utility that depending upon what switches are used will wipe any data that is stored on a drive by writing a hex code value to every location of a hard-drive multiple times. Additional switches can be used to randomly alter the hex values that are used, making it extremely difficult to recover any type of data after multiple passes are made. Wiping a drive in this manner takes an extremely long time because every sector of the drive must be written too in order to ensure that all information on the drive is erased. Depending upon the drive size this process can take hours, to potentially more than a day, or several days (if the drive is extremely large).

**Question 3 – Why is it important to take a hash of the suspect’s drive? What does a hash value tell you? Can you name two popular hash algorithms?**

It is important to take a hash of the suspect’s drive, because that is how we will determine that any copy made of the suspect’s drive for the purpose of an examination contains the exact same information of the suspects drive. If the hash of the suspects drive and the hash of a copy of the drive do not match, then data has been changed in the copy and the copy will not be useful in an investigation. If the hash values match, then the contents of the suspects drive and the contents of the investigation image are identical. The investigation image can then be used to examine what is on the suspects drive without contaminating the suspects drive.

Two Popular hashing algorithms are MD5 and SHA.

**Question 4 – Explain another way you can create a bit-stream copy of a suspect’s drive.**

**You can create a bit-stream copy of a suspects drive by using a Linux OS (installed or through a LiveCD boot disk such as Kali, or knoppix) and then using the dd command.**

**Question 5 – Provide a screenshot of your hash value in your report. Provide a brief overview of the process you would perform if you did this process manually using a set of dos commands.**

**This question specifically references dos commands, I have been searching specifically for DOS commands, and I have not been able to come up with a specific DOS command that allows for the hashing of a drive (individual files, yes, but not the drive as a whole).**

**This is not an issue within a Linux environment as the md5sum command is capable of hashing a drive device. As such, I would use a Linux OS install or Live CD to calculate the md5sum of a drive.**

**Md5sum /dev/had. Once the drive has been copied, the image of the drive can be hashed and these values compared to see if they match.**

**You could also use dcfldd through linux to image the drive, which has several forensics related options outside of the standard dd program.** 

