CCSI 410 Forensic Lab Report

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

2) Date of Investigation: July 24, 2013\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3) Lab Number and Title: Lab 3: Risk Analysis and Repair\_

4) Summary of Findings:

Answered questions 1 of the lab assignment. Logged into the lab environment and scanned the suspect drive (e: ) for viruses. No viruses were found. Pasted a screenshot of the virus scan results and answered question 2. Answered Question 3 of the lab regarding whether or not a virus on a suspect drive should be deleted.

5) Details of Investigation

Wednesday, July 24, 2013

10:21 am – Answer Question 1

10:33 am – Opened Lab Environment

10:36 am – Noting no recorded hash value of suspect drive, so no available value to compare the image file to. Drive E: has not been accessed by any program or other function.

10:40 am – Noting that Virus definitions are out of date. (as this is a lab environment I will assume that in a real world environment definitions would be kept up to date)

10:50 am – Ran Virus scan

10:51 am – Noting Scan results: 78 files scanned 3 Master Boot Records scanned, 3 boot records scanned. 0 Viruses detected.

10:56 am – Closing Lab environment

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

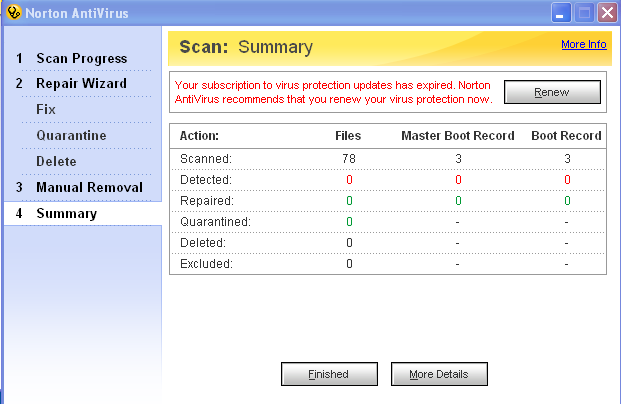
**Question 1 – What are some of steps that you should take now before you begin your investigation? Be sure to document in your report.**

**As this is an investigation and a copy of the suspects drive has already been made, you should already have a hash value of the suspect’s original drive. Before you begin your investigation into the copy, you should verify that this hash value matches.**

**You should also verify that any write blocking implementations that may be required are properly in place so that the investigation drive is not written to accidentally and can continue to be used throughout the investigation process.**

**Question 2 – Did you find any viruses on this drive? Take a screenshot of your virus scan window.**

**No viruses were found on the drive.**



**Question 3 – Should you delete the virus file? What would a deleted file do to the hash? If you do, what steps should you take to document and be sure that you do not tarnish your evidence?**

I would think that the answer to the first part of this should be a No, or at the very least, not unless it is just absolutely determined by the lead investigator that it should be removed.

Any forensics investigation should be being done on an isolated machine anyways, which eliminates the threat of the of virus for all machines except the machine that is being used for the investigation.

This is because removing the virus will alter the hash value of the drive / image, and could allow for the questioning of the validity of any evidence that is found on the drive after the virus is removed.

If it is determined that due to the type and nature of the virus, that it must be removed, knowing that the hash value of the drive will be changed, one would need to document and verify the original hash, and that the image matches, remove the virus, and then immediately re-hash the drive to obtain the new hash value. Make a new copy of the image and verify matching hashes again.

Again, this is something that I would only expect to happen in extreme circumstances. I would expect a forensics investigation computer to have its virus definition and programs kept up to date daily when between investigations, and I would also expect it to be able to be formatted and reset from a secure image on a as needed basis after each investigation, because of potential virus contaminations.