Lab 9 – Assessment Worksheet

Identifying and Documenting Evidence from a Forensic Investigation

Course Name and Number:
CYBS 7359 - 010

Student Name:
Natnael Kebede

Instructor Name:
Dr. Renita Murimi

Lab Due Date:
4/5/20

Lab Assessment Questions

1. What is the forensic specialist responsible for during an investigation?

   The forensic specialist is responsible for three basic tasks: finding evidence, preserving evidence and preparing evidence to be presented in a court of law.

2. Describe the importance of proper documentation in a forensic investigation. How can the chain of custody affect the investigation?

   The importance of proper documentation in a forensic investigation is to demonstrates the chain of custody and makes the evidence gathered admissible in a court of law. Hence, without proper documentation, a forensic specialist can't present the evidence in a court of law.

   The chain of custody affects the investigation by requiring the forensic investigator to follow proper procedures in handling data, if it is used against a case. That is, the chain of custody is the continuity of control of evidence that makes it possible to account for all that has happened to the evidence between its initial collection and its appearance in court. If the chain of custody cannot be proven as intact or evidence is compromised, the case could be dismissed, or it could be overturned with a guilty verdict upon appeal

3. What is a write-blocker and why is it necessary to have one in a forensic toolkit?
   A write-blocker is a device that allow the acquisition of information on a drive without creating the possibility of accidentally writing to the drive and compromising its admissibility in court. The use of such tools is critical in the chain of custody procedures of a forensic digital analysis.

   It is necessary to have one in a forensic toolkit because it allows the investigator to preserve the integrity of the data at hand and avoid making changes to the evidence for admissibility in court.

4. How many files were discovered by the text search for the word *bad*?

   16 files were discovered by the text search for the word *bad*

5. What is the purpose of the MD5 hash file that is generated with an E3 report?

   The purpose of the MD5 hash file that is generated with an E3 report is to ensure that the report file that is generated is the same report that is produced as evidence in court.

   An MD5 checksum can be generated against the report at any time in the future and compared against the checksum generate at the same time as the report. If the resulting MD5 checksums match, then it can be assumed that the report file has not changed. If the checksums differ, then report file could have been tampered with, which could result in inadmissibility in court.

6. Which report type did you choose as your second report in this lab? Why did you choose that report?

   I chose the HTML Investigative Report since it has a more interactive format and graphics. Additionally, when compared to a Simple Text Report, it is easier to read due to its presentation format.