Matthew Austin
Digital Forensics
Tian Guanyu
10 October 2017

Laboratory Report

Laboratory Number:__13243546___
Date__10/03/2017_____

Examiner's Name: ___Matthew Austin_____

<Exercise, Validation Test, or Examination > Number: __09876543_____

Examination or Validation Tasking:

The flash drive which was collected from Officer Joe Doe will be logically analysed by Matthew Austin to investigate the hacking crime that has taken place. When done a bit by bit copy will be created, hashes will be successfully compared, and file by file analysis will be done using hashing and other various commands.

Forensic Question(s):

1. Identify relevant information concerning who, when, where, why, and how the hacking was committed, and whether or not the crime was even committed?
2. Locate all document file that are within the flash drive?
3. Compare files/hashes of of the original device and the forensic copy?
4. Associate files, media, computer, IP address with the device?
5. Reconstruct the events/ activities which resulted in the hacking crime committed?

Steps Taken:

1. The item was photographed at the crime scene
2. The item was properly secured and taken to the Lab (using Ubuntu)
3. The item was placed in write blocker, got the hash of the original device, a bit by bit copy was created, and successfully compared the hash's of both devices.
4. The forensic image was then mounted and all the content files as well as the flash drive and image itself were analysed using a multitude of command lines.

5. The image was then unmounted, to ensure data was not altered a final hash comparison was successfully made.

Results:

The flash drive was a red sandisk that could could 32GB worth of data. Out of the 32GB 28GB of data was used. There was a total of 25 files on the flashdrive. These files have been placed as a forensic image marked image.dd" and provided to the examiner. The flash-drive was marked "BM150625257B" and given to the contributor.

Conclusions:

The data and science showed that there were not any hidden files or any files used that can be related to a hacking crime. This information was obtained by mounting the forensic image and analysing all the files to ensure that each files extensions were not changed or altered in a threatening fashion. The commands stat, ls (-al,R), less, etc. were used to analyse every single file as well as the image.dd and original device itself. The hashes were similar so no data was altered between the crime scene, analysis and release of the evidence.

Opinions:

The suspect was believed to be falsely accused of hacking the victim, as the data and process showed that a crime was not committed.

Certification: <Last Page Only>

I hereby certify that the work presented above was personally performed by me and the opinions and conclusions stated are my own and based upon the work that I performed.

____Matthew Austin_____
Signature