Matthew Austin
Digital Forensics
Tian Guanyu
10 October 2017

Laboratory Notes

Laboratory Number: ___13243546_____ Examiner Name:__Matthew Austin_____

Date & Time	Activity
10/03/2017 2:30 PM	The item was received from Officer Joe Doe by Matthew Austin. The item was transported from Fontbonne to Anywhere Police Department in a Faraday Bag/Anti-Static Bag and successfully kept away from magnets, radio transmitters, and other potentially damaging devices.
10/03/2017 2:45 PM	At the Lab the flash drive was placed in a write blockers and a bit by bit copy of the device was created. The device is 32GB with 28GB used.
10/03/2017 2:50 PM	Once the original is secure and is unable to be tampered with/edited the device is inserted into the Linux/Ubuntu Computer. A forensice image of the source drive was created using $ *sudo ddif=/dev/VelvetThunder of=home/Matthew/Desktop/image.dd*
10/03/2017 2:56 PM	A folder was created called using *$mkdir* Evidence and the forensic image was mounted into the Evidence folder using *$sudomount -t auto -oloop,roimage.dd Evidence*
10/03/2017 3:01 PM	cd to the directory that contains image.dd, and used command ls-al, ls -aflashdrive.dd and ls-alR. The information from the outcome was not able to be documented as it was unnecessary.
10/03/2017 3:05 PM	The MD5 of the original device and hash of the image.dd and file was collected using $*openssldgst-md5 image.dd.* and $*openssldgst-sha512 image.dd.*
10/03/2017 3:05 PM	There was a total of 25 files on the device. Used command *$file and $stat* on each file to ensure they were correctly label and not altered
10/04/2017 3:25 PM	To leave directory the command *$cd ..* and unmounted using *$unmountEvidence*

10/04/2017 3:25 PM	to ensure that nothing was altered a MD5 hash command was successfully used as the hashes were the same.