Intro to Cyber Forensics Lab Grading Sheet

Project: Lab 2 – Acquisition
Member Name: Alejandro Marin Arellano
Member Name: Christopher Bowen
Member Name: Terrence Scott
Member Name: Saehwan Park
Member Name: George Hendrick

Executive Summary _____ / 4 points

\+ ✔ -

❑❑❑ Executive summary is brief and focused to the point of the project ❑❑❑ The summary clearly illustrates the objectives of the laboratory exercise

Apparatus _____ / 4 points

❑❑❑ The apparatus are clearly illustrated and documented

Procedures _____ / 12 points

❑❑❑ Adequate information provided to allow re-creation of work

❑❑❑ Consistent level of coverage throughout the project – nothing overly detailed or omitted

Problem Solving _____ / 5 points

❑❑❑ All problems identified

❑❑❑ Alternative solutions identified

❑❑❑ Solutions attempted listed

❑❑❑ Final solution detailed (what fixed the problem and why?)

Conclusions & Recommendations _____ / 5 points

❑❑❑ Tie back to the learning objectives identified in the executive summary - critical

❑❑❑ _____ Conclusions stated in a logical fashion

❑❑❑ Conclusions are viable based on the procedures and results

❑❑❑ Recommendations practical & relevant

Format & Grammar _____ / 5 points

❑❑❑ Table of Contents present

❑❑❑ Report written in past tense

❑❑❑ Proper voice (no I's, We's, Our's or The group)

❑❑❑ Paper easy to read (fonts, spacing, etc.)

❑❑❑ Proper credit given to sources in bibliography (APA style)

❑❑❑ Paper is cohesive and consistent in tone

_____ Spelling & grammar errors: *minus one half point for each, up to a max deduction of 5 points – at that time, paper is returned for correction and re-submission with a one letter grade penalty.*

Final Score: _____ / 35

Contents

1 Executive Summary

The objective of this lab was to forensically acquire a physical image of the evidence collected from the crime scene.

Investigators conducted digital acquisition on February 7, 2023, at Patrick F. Taylor Hall 3304 S Quad Dr, Baton Rouge, LA 70803 in room 2317. Investigators acquired two pieces of evidence from the crime scene a flash drive and a Seagate hard drive. Investigators tested the hardware write blocker before copying data prior to acquisition and took photos using a GALAXY S20+ during the process.

The goal of this exercise was for investigators to learn proper acquisition standards. The exercise included two separate hardware write blockers, the first was an eSata bridge write blocker and the second was a flash drive write blocker.

Investigators began by checking the hard drive on the forensic workstation file explorer and then checking for the drive on FTK Imager. Investigators used both Write Blockers, a Windows System, and FTK Imager to acquire a forensic sound physical image of only the flash drive. The forensic image was acquired as a physical image under the following parameters: raw(dd) formatted and non-fragmented. Moreover, to ensure proper forensic acquisition, investigators used FTK Imager to authenticate the acquired image with both md5sum and sha1sum hashes.

In this lab, investigators gained knowledge by using FTK Imager to forensically acquire and copy data collected from the crime scene. To ensure proper standards investigators documented every action taken when accomplishing these tasks, including taking screenshots of the steps taken during the acquisition process, documenting equipment setup, and hashing each piece of evidence before and after acquisition.

2 Apparatus

Table 1 lists the hardware and software used in this lab.

Table 1: apparatus of tools used in the image capture process

ITEM/PART	MODEL NUMBER	VERSION	USAGE
USB Flash Drive	S/N: 000ecc4300087043	General UDisk USB Device	Seized from suspect
Hard Drive	S/N: Z2AMQJ9Y	Seagate Barracuda 500 GB	Seized from suspect
HD Hardware Write Blocker	N/A	opentext Tableau Forensic SATA/IDE Bridge	Acquisition of forensically sound image
USB Drive Hardware Write Blocker	N/A	opentext Tableau Forensic USB 3.0 Bridge	Acquisition of forensically sound image
Windows 10 VM Forensic Workstation	N/A	10.0.19045 Build 19045	Acquisition of forensically sound image
VMWare Workstation Pro	N/A	16.2.3 build-19376536	Workstation access
AccessData FTK Imager	N/A	ADI4.7.1.2	Acquisition of forensically sound image

3 Laboratory Procedures

3.1 Time-line / Log

Table 2: The log of all actions taken in the investigation

#	DATE	TIME (24hr)	ACTION TAKEN / INVESTIGATIVE LEAD
1.	02/07/2023	12:13	Accessed virtual machine
2.	02/07/2023	12:26	Received hard drive write blocker kit
3.	02/07/2023	12:27	Received hard drive
4.	02/07/2023	12:28	Connected power adapter and SATA adapter to hard drive and write blocker, connected USB cable to write blocker and computer
5.	02/07/2023	12:31	Powered on write blocker, connected write blocker to virtual machine
6.	02/07/2023	12:35	Opened file explorer to find hard drive, was not found in file explorer
7.	02/07/2023	12:36	Opened FTK Imager, hard drive was not found as a physical source
8.	02/07/2023	12:38	Closed FTK Imager, turned write blocker off, turned write blocker back on
9.	02/07/2023	12:39	Opened file explorer and found hard drive, opened FTK Imager, added hard drive as physical source, verified model number on FTK Imager with physical hard drive
10.	02/07/2023	12:45	Closed FTK Imager, disconnected hard drive from write blocker, disconnected write blocker from computer
11.	02/07/2023	12:47	Bagged write blocker kit, handed back hard drive
12.	02/07/2023	12:48	Received USB write blocker kit, received USB
13.	02/07/2023	12:50	Connected USB cable to write blocker and computer, plugged in USB to the write blocker
14.	02/07/2023	12:51	Turned on write blocker, opened file explorer and found USB
15.	02/07/2023	12:54	Attempted to copy files to USB to test the write blocker, could not write to the USB
16.	02/07/2023	12:57	Opened FTK Imager, added USB as physical drive
17.	02/07/2023	13:01	Verified USB found on FTK Imager
18.	02/07/2023	13:03	Acquired a physical image of the USB and hash information
19.	02/07/2023	13:10	Verified identical hashes of image file and original USB drive

3.2 Procedure

Officer Clinton Walker handed both digital pieces of evidence to investigators, a 1 TB Seagate hard drive, as seen on Figure 1, and a 2 GB flash drive. Investigators began acquisition by testing both the eSata hard drive hardware write blocker and the flash drive hardware write blocker. The first piece of evidence investigators concentrated on was the hard drive.

When initially plugging in the hard drive to the hard drive write blocker, as seen on Figure 2, investigators were unable to identify if the drive was working through the file explorer on Windows. After a discussion with Officer Clinton Walker about this issue, investigators were informed to proceed using FTK Imager to inspect the hard drive. When investigators initially opened FTK Imager, the hard drive did not appear in available sources. After consulting with Officer Clinton again, investigators were instructed to reset the connection of the hard drive hardware write blocker to the forensic workstation. After resetting the connection, investigators were able to properly inspect the hard drive of its contents. As seen in Figure 4, The hard drive not showing up was due to the drive not having a file system. After instruction to not copy the hard drive by Officer Walker, investigators turned off and disconnected the hard drive write blocker from the forensic workstation.

The next step taken by investigators was investigating the second piece of evidence, the USB Flash drive. Investigators were instructed to acquire a forensic physical image of the USB Flash drive via the use of a USB Bridge Write Blocker, shown in Figure 5. Again before the acquisition, the write blocker was first tested to ensure the evidence was not tainted. As shown in Figure 6 via the terminal and in Figure 5 via the green write block button, no writes could occur to modify the evidence. The acquisition was conducted using FTK Imager shown in Figure 7. Before acquiring a forensic image, md5sum and sha1sum hashes were calculated for the contents of the USB flash drive shown in Figure 8. The forensic image was acquired as a physical image, raw(dd) formatted, and non-fragmented. After the acquisition, FTK Imager authenticated the acquired image against the flash drive using both md5sum and sha1sum hashes shown in Figures 9 and 10.

After completion of the acquisition and verification of hashes, investigators proceeded to pack up the hardware blockers and return both pieces of evidence to Officer Walker.

3.3 Figures

Figure 1: Image of the physical hard disc.

Figure 2: Image of hard drive write blocker connected to hard disc and computer.

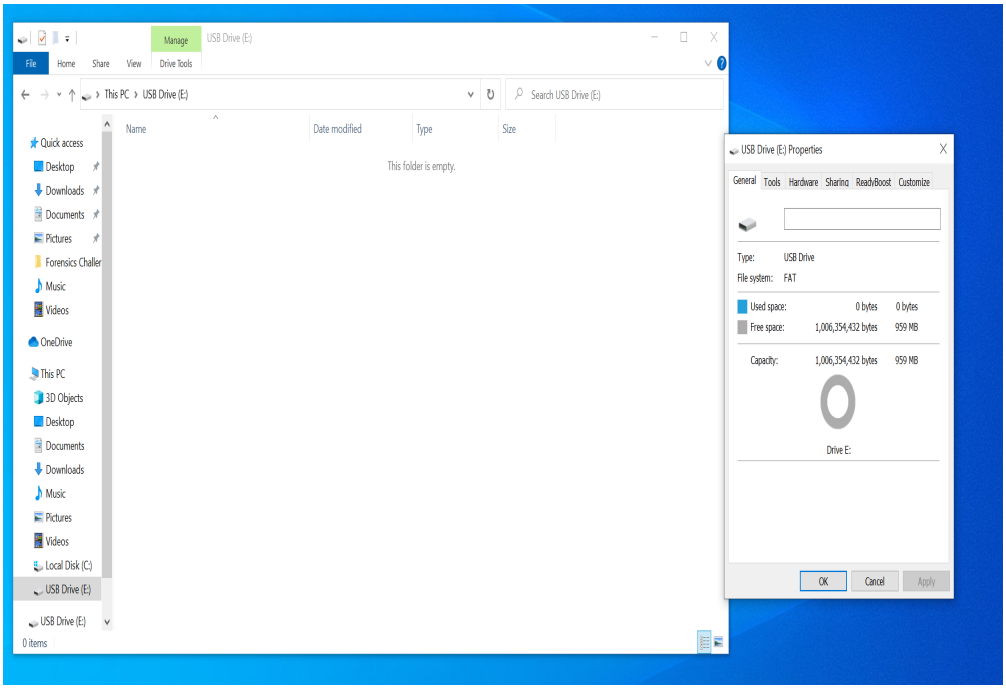

Figure 3: Image of file explorer with apparently empty hard disc.

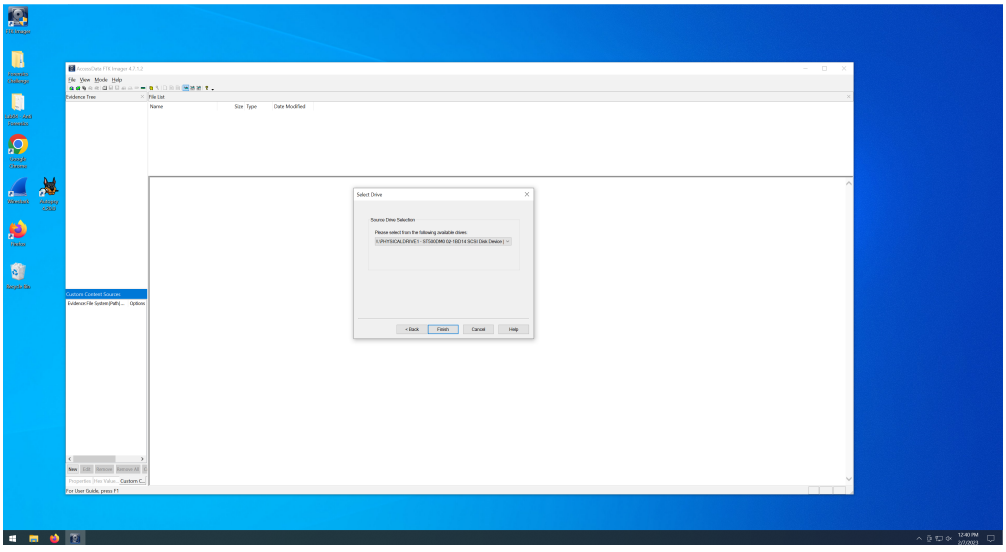

Figure 4: AccessData FTK Imager 4.7.1.2 Source Drive Selection - Hard Disc.

Figure 5: Image of USB write blocker with USB drive connected and write blocker light on.

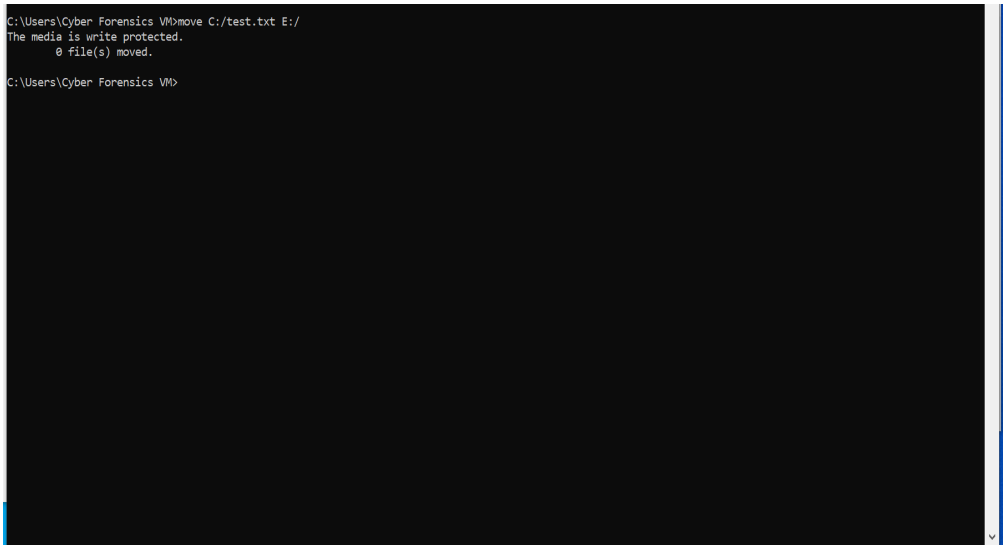

Figure 6: Verifying through command prompt that the flash drive is write protected.

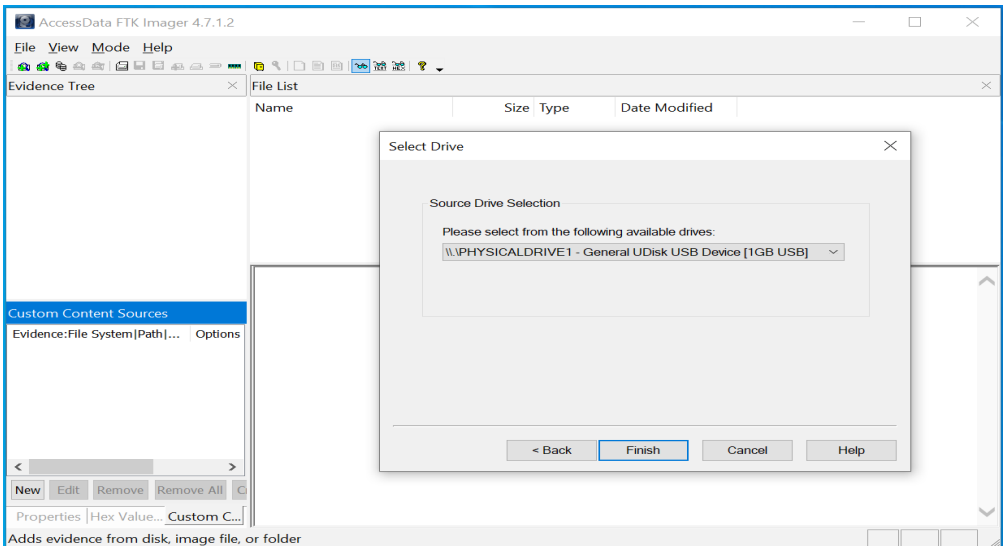

Figure 7: AccessData FTK Imager 4.7.1.2 Source Drive Selection - USB Drive.

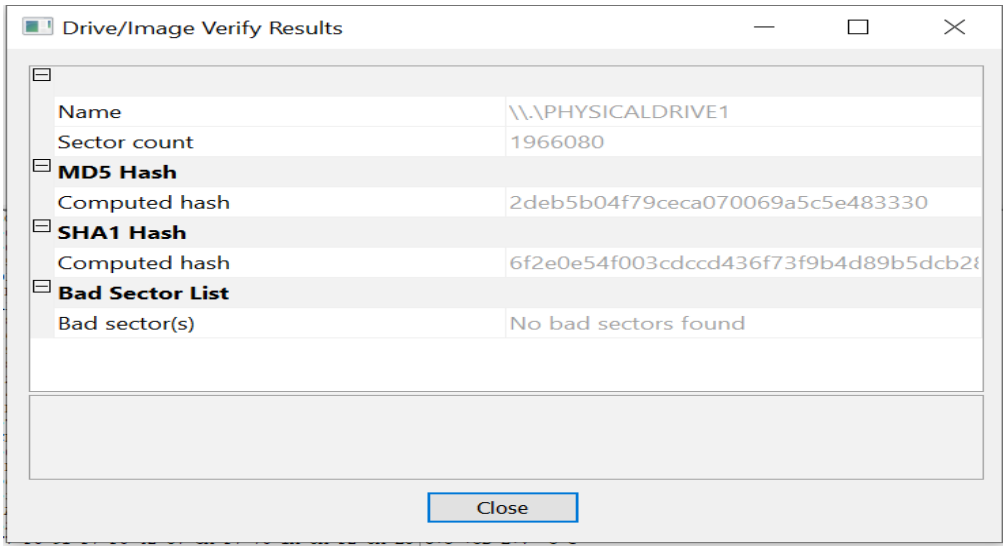

Figure 8: USB Drive/Image Results with MD5 and SHA1 hashes.

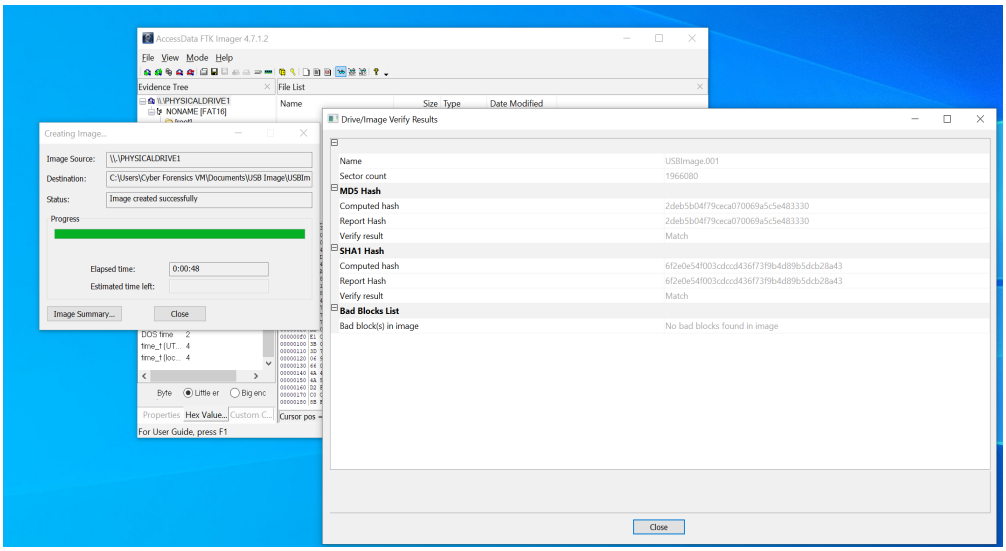

Figure 9: Verification of identical hashes for the copied image.

```
Created By AccessData® FTK® Imager 4.7.1.2

Case Information:
Acquired using: ADI4.7.1.2
Case Number:
Evidence Number:
Unique Description:
Examiner:
Notes:

---------------------------------------------------------------

Information for C:\Users\Cyber Forensics VM\Documents\USB Image\USBImage:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 122
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 1,966,080
[Physical Drive Information]
 Drive Model: General UDisk USB Device
 Drive Serial Number: 000ecc4300087043
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 960 MB
 Sector count:    1966080
[Computed Hashes]
 MD5 checksum:    2deb5b04f79ceca070069a5c5e483330
 SHA1 checksum:   6f2e0e54f003cdccd436f73f9b4d89b5dcb28a43

Image Information:
 Acquisition started:   Tue Feb  7 13:09:17 2023
 Acquisition finished:  Tue Feb  7 13:10:05 2023
 Segment list:
  C:\Users\Cyber Forensics VM\Documents\USB Image\USBImage.001

Image Verification Results:
 Verification started:  Tue Feb  7 13:10:06 2023
 Verification finished: Tue Feb  7 13:10:09 2023
 MD5 checksum:    2deb5b04f79ceca070069a5c5e483330 : verified
 SHA1 checksum:   6f2e0e54f003cdccd436f73f9b4d89b5dcb28a43 : verified
```

Figure 10: USB Image.001.txt file with information acquired from USB drive.

4 Problem Solving and Troubleshooting

Problem: After correctly connecting the hard drive to the virtual machine, investigators were not able to find the hard drive on the Windows file explorer.
Alternate Solution 1: Searching for the hard drive via command prompt.
Final Solution: Officer Clinton Walker informed the investigators to proceed to using the FTK Imager to inspect the hard drive, and were then able to view the contents of the hard drive.

Problem: Upon first connection of the hard drive to the machine via write blocker, investigators were unable to find the physical source on FTK imager.
Alternate Solution 1: Use of a Unix-based System such as OSX or Linux and dd to create a forensic physical image of the hard drive.
Final Solution: Investigators closed FTK imager and reset the write blocker.

5 Conclusion and Recommendations

In completing this exercise, investigators have learned the correct methods of digital acquisition of evidence taken from a crime scene. The standards of properly handling evidence and copying data to allow investigators to analyze evidence are imperative. If investigators improperly copy the data acquired they can potentially taint the evidence causing the suspect to potentially be let go. For instance, if an investigator was to modify the data by any amount, the hashes for the evidence would be different thus causing the evidence to excusable in court. All steps of an investigation must follow a forensic procedure.

Investigators should make sure that they are following a forensic procedure, and document each step taken during the investigation. Failure to document these steps is another way that the evidence could be excused in court. If an investigator was to ignore proper documentation, it could cause major issues in court. The acquisition of data is an important step in an investigation, and investigators must know the proper steps to take during an investigation.

Appendices

A Forms

CHAIN OF CUSTODY FORM

Evidence Identification and Chain of Custody	
Date:	01/31/2023
Received/Seized From:	AI Lagniappe
Received/Seized By:	Group 8
Reason Obtained:	Directed by Dr. Ibrahim Baggili, Lab 1
Location Obtained:	PFT 2341

Description of Evidence (Manufacturer, Model #, S/N, condition, marks/scratches, etc.)
Flash drive, disk, hard drive - electronic evidence
2 pieces of crumpled paper, 2 pieces of newspaper - assumed trash
4 sticky notes - paper evidence
Styrofoam cup, latex gloves, napkin - DNA evidence

Change/Chain of Custody Log			
Purpose of Change of Custody	**Method of Transfer** / **Tracking #**	**Release By/Date** / **Signature**	**Received By/Date** / **Signature**
1. Transferring of evidence from crime scene	handed to Clinton Walker		01/31/2023
	1		
2. Received hard drive and USB	received from Clinton Walker		02/07/2023
	2		
3.			
4.			
5.			
6.			
7.			
8.			