# Intro to Cyber Forensics Lab Grading Sheet

Project: **LAB 2 – Acquisition** Member Name: Pottolla Vinusha Goud Member Name: Boinapelly Akshith Rao Member Name: Lashmidhar Yadlapalli Member Name: Amani Ponnam

## 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 identiLied

❑ ❑ ❑ Alternative solutions identified

❑ ❑ ❑ Solutions attempted listed

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

## Conclusions & Recommendations / 5 points

❑ ❑ ❑ Tie back to the learning objectives identiLied 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**

# Tables of Contents

1. [Executive Summary 3](#_TOC_250006)
2. [Apparatus 4](#_TOC_250005)
3. Laboratories Procedures 5
   1. [Timeline/ Log 5](#_TOC_250004)
   2. [Procedure 6](#_TOC_250003)
   3. [Figures 7](#_TOC_250002)
4. [Problem Solving and Troubleshooting 12](#_TOC_250001)
5. [Conclusion and Recommendations 13](#_TOC_250000)
6. References 14

# Executive Summary

The purpose of the lab exercise was to practice data acquisition from digital and electronic evidence that was recovered from a crime scene. The goal of the exercise was to make sure that all essential protocols and actions were taken to guarantee that data would not be lost or damaged during the collecting process. This exercise was carried out by a group of 4 on September 30, 2024.

The crime scene was in Buckman Hall 233-C back side of the right column. From the crime site, the investigators retrieved a hard drive and a thumb drive. Data collection was done on the hard drive and thumb drive that were recovered. A md5 hash was used to ensure that an exact bit-for-bit copy was created and to verify the integrity using FTK Imager after an image of both devices was created. The procedure was completed with the use of all required tools, and a write blocker device was employed to make sure that no data was lost or jeopardized.

# 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** |
| Ultra kit Write Blocker |  | N/A | For acquiring a forensically sound image of the hard drive or a storage device |
| Tableau Forensics Bridge Tableau |  | N/A | cloning the drive's contents and locking the hard drive |
| Desktop |  |  | For Display |
| External Hard Drive |  |  | Store the Data |
| FTK imager | N/A | 4.7.1 | Software forensic tool to preview. data from disk/drive |
| SATA/USB | T35es-R2 | USB 2.0 | A bridge between USB drive and computer |

1. **Laboratory Procedures**

# Timeline/Log

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

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **DATE** | **TIME** | **ACTION TAKEN / INVESTIGATIVE LEAD** |
| 1 | 09/30/2024 | 18:00 | We arrived at the lab. |
| 2 | 09/29/2024 | 18:07 | We gathered data and inspected the forensic toolset from the lab that was used. |
| 3 | 9/29/2024 | 18:18 | Learned every detail about the equipment in the toolkit. |
| 4 | 9/29/2024 | 18:36 | We took out the write blocker equipment and attached the power cable to it then powered it on. |
| 5 | 9/29/2024 | 18:39 | We then connected it to the computer at the lap and connected the USB to the drive blocker, confirming that all the status lights on the write blocker were turned on to ensure proper connectivity. |
| 6 | 9/29/2024 | 18:43 | We then initialed a forensic image creation of the USB drive that was in question to make a copy of the drive for lap report and testing purposes. |
| 7 | 9/29/2024 | 19:14 | An MD5 hash was made to ensure an exact copy was made and all devices were properly dismantled and returned to their respective evidence bags as well. |

# Procedure

The Group which includes Pottolla Vinusha Goud, Boinapelly Akshith Rao, Lashmidhar Yadlapalli, Amani Ponnam was tasked with obtaining information from the online and digital evidence. During the investigation of a crime scene, the team assembled on September 30, 2024, at 18:00 to start gathering data on the suspect's thumb drive.

Ultra-thin write blocks were used so as not to leave any writing on the electronic gadgets collected for the study. The SATA write blocker bridge, which was connected to the power supply of the computer, was connected to the hard disk. First, a write operation was conducted to confirm the write blocker's functionality before the suspect's hard drive was connected.

The USB bridge and the suspect's thumb drive, the team gathered. FTK imager was initially deployed. All devices involved in the testing were properly tested, including the write blocker before it was used to collect the forensic image of the USB dive to ensure the data integrity state and to make sure the functionality of the write block and ensure that the data was not changed during the process, the thumb drive was attached to a USB bridge and a write operation was performed. The team's laptop was linked to the USB bridge using the correct connector, the power supply was connected, and the thumb drive was connected to the bridge with the aid of the accompanying lab manual and the setup instructions in the extreme kit write blocker. On the laptop, the FTK imager was used to produce two forensically sound images of the thumb drive. The working image was one, while the backup image was another. This produced a case folder that had the thumb drive's image as well as details on the RAM, tracks, segments, deleted Liles, and the drive's hash.

Windows Defender performed a virus check on the folder.

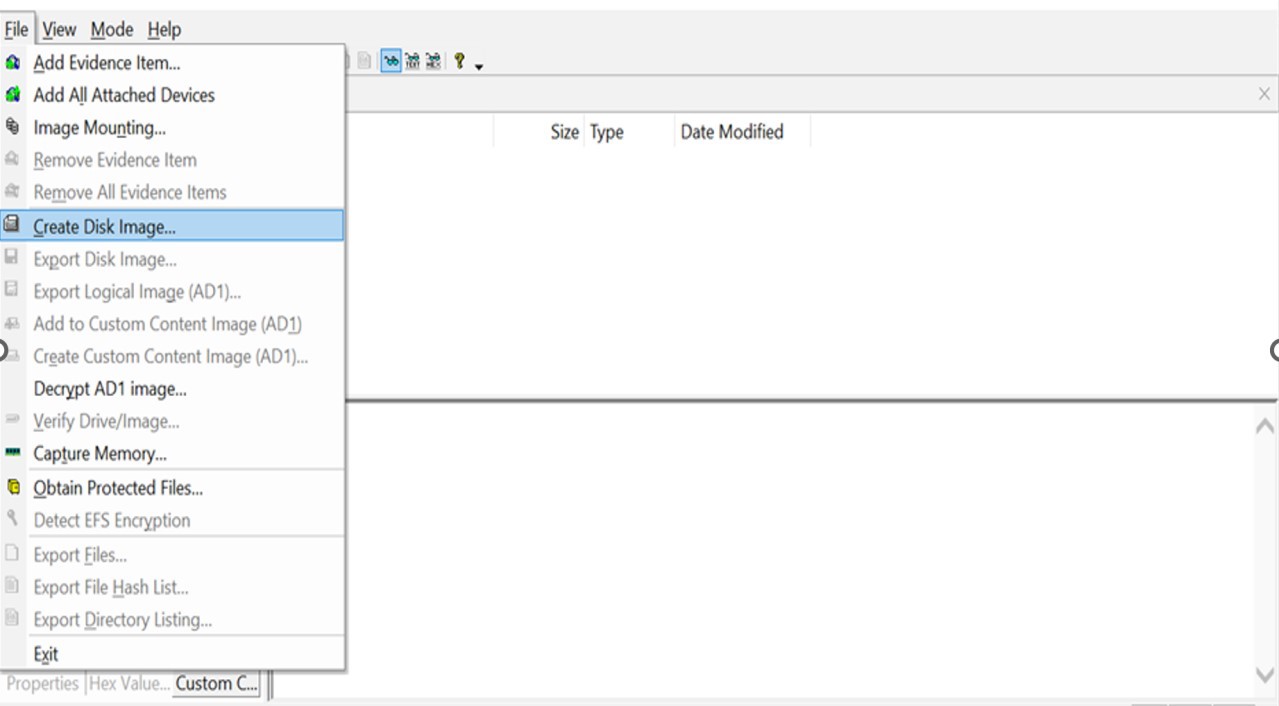
# Figures:



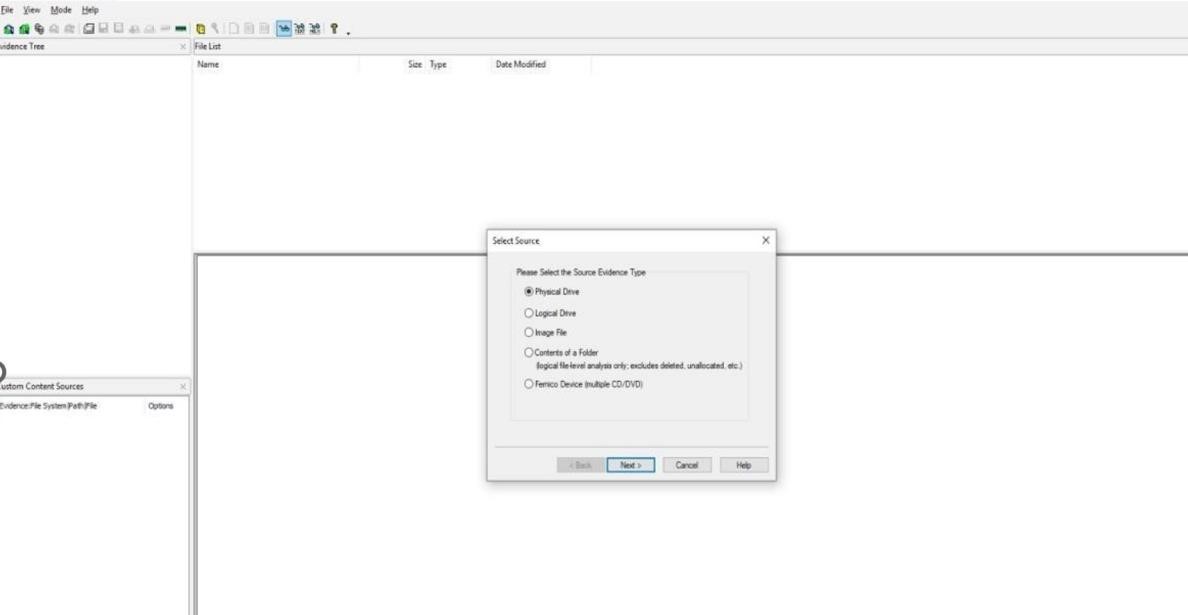
**Figure 1: the toolbox kit**



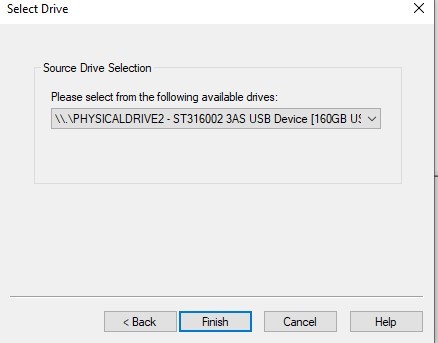
**Figure 2: Tableau SATA drive Description**



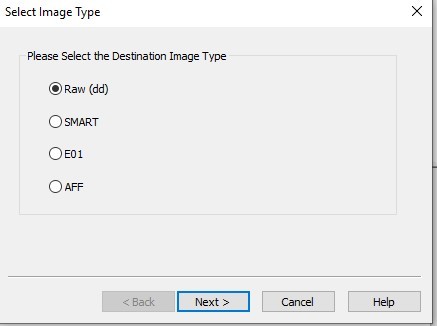
**Figure 3: Opened the FTK Image application and clicked on Create Disk Image**



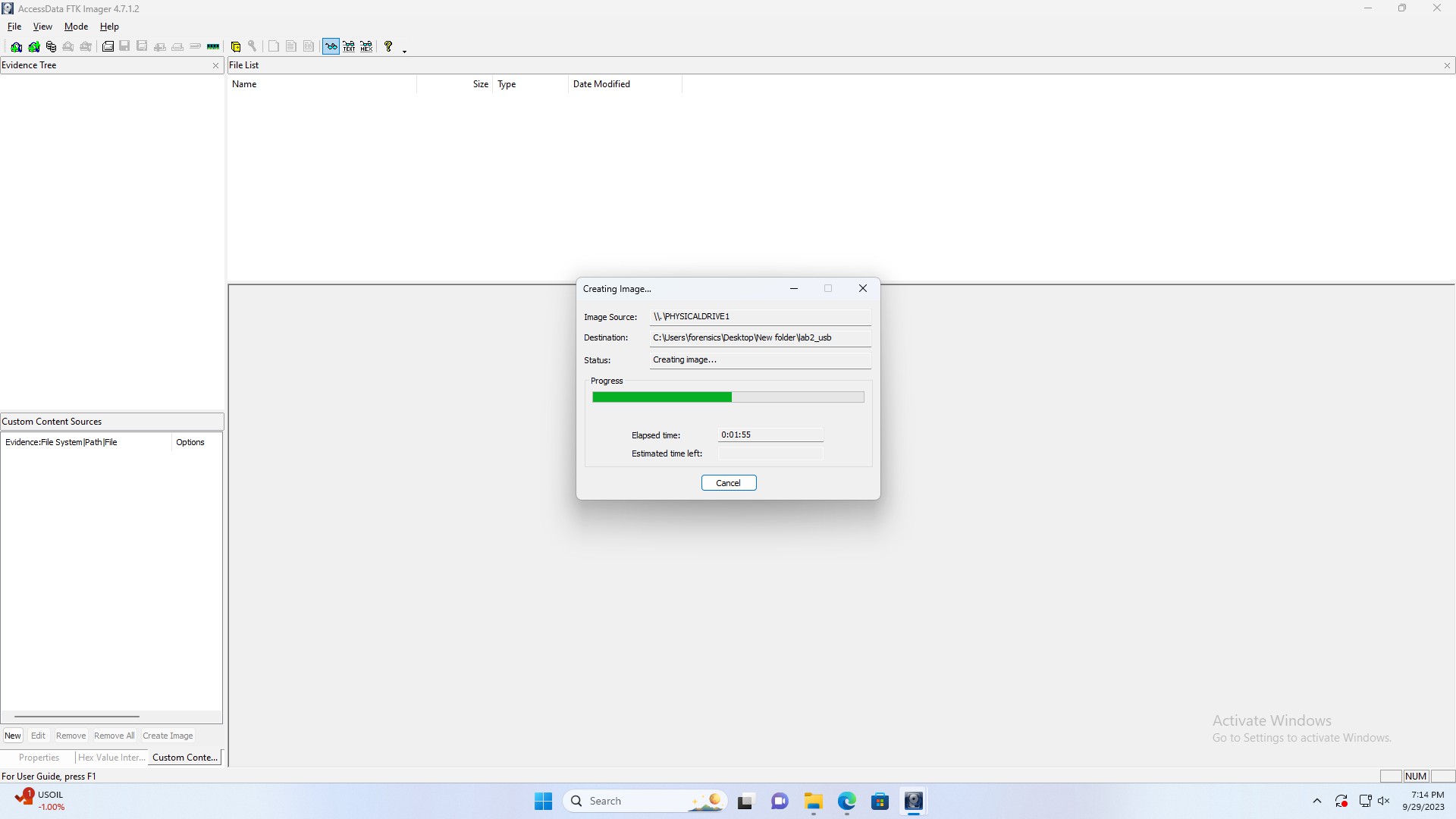
**Figure 4: FTK Imager Selecting the source.**



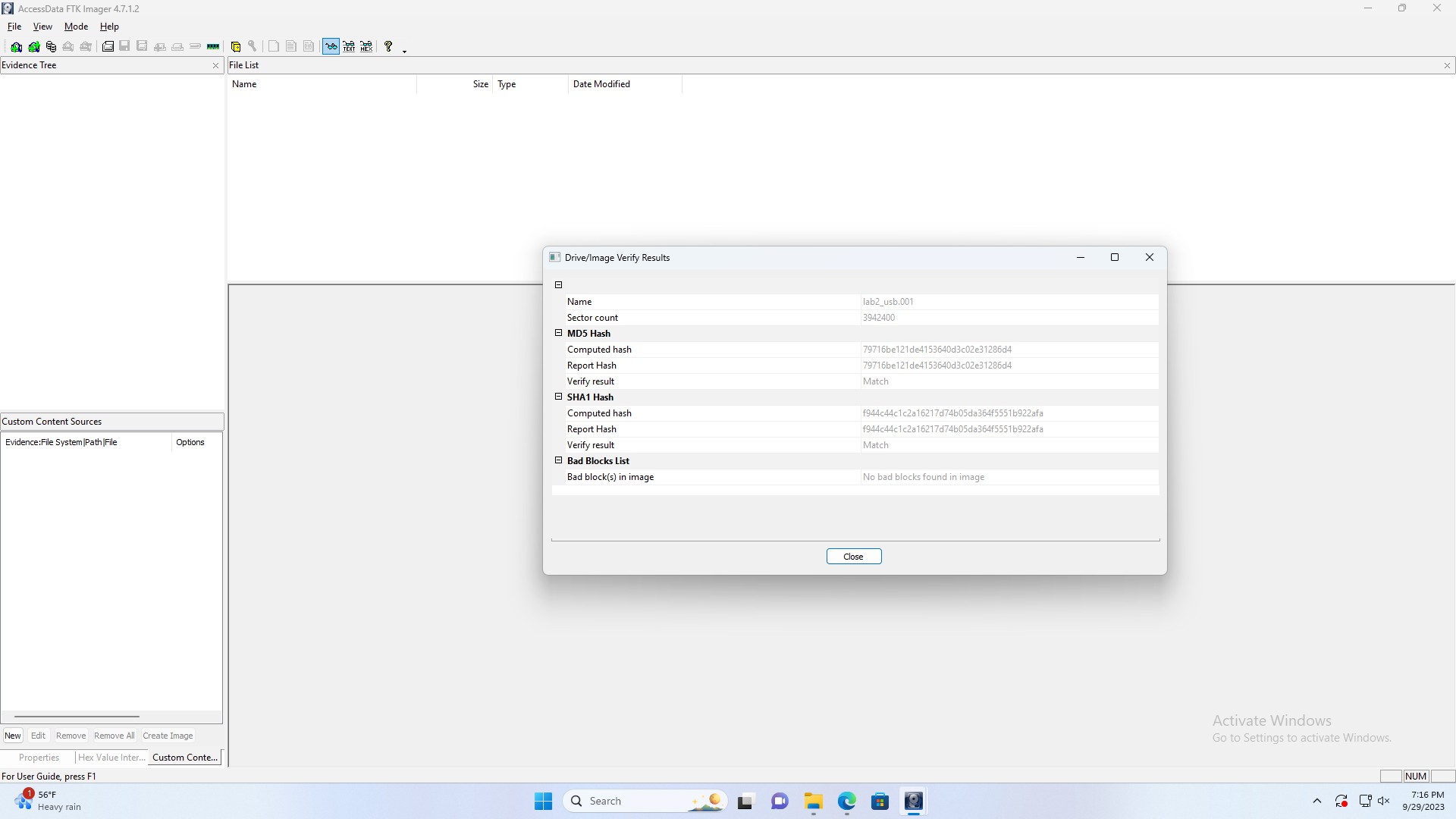
**Figure 5: FTK Imager, Source Drive Selection**

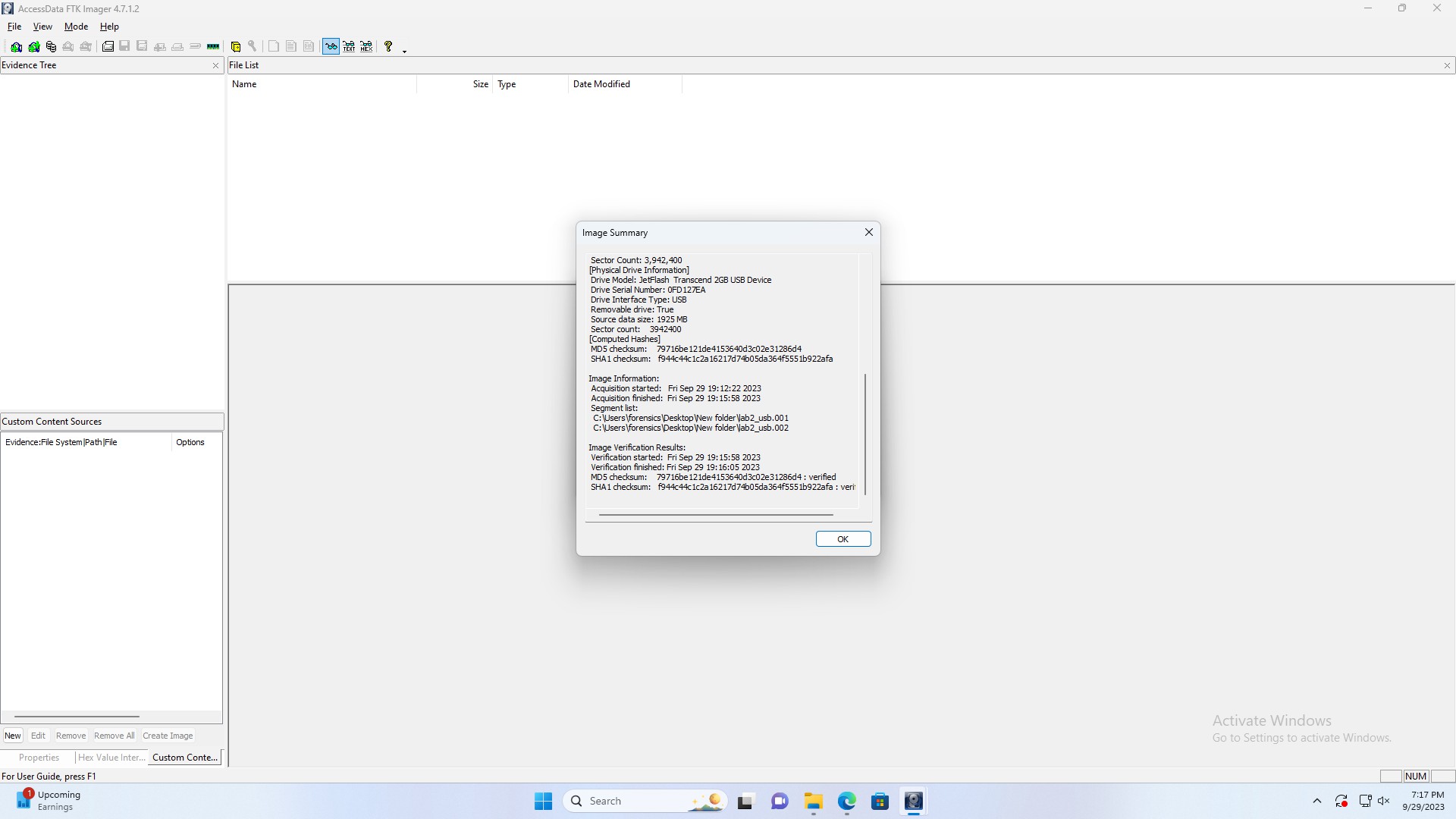


**Figure 6: FTK Imager, Selecting Destination Image type.**



**Figure 7: FTK Imager, Creating Image**





# Problem Solving and Troubleshooting

## Problem 1: Device handling and wire connection

Solution 1: Care was taken to connect the wires to the proper ports and to keep the hard drive's circuitry untouchable. Carefully installed to prevent any damage, sensitive pins were used on the write protector's power cord.

Alternative Solutions: It would be beneficial to comprehend a device before using it. It would also be better to read the information leal. let on the gadget before using it. **Problem 2: Use of new software**

Solution 2: examined and watched the training videos contained in the canvas to gain knowledge about using the two different software applications, FTK Imager.

# Conclusion and Recommendations

Investigators will understand the distinction between a backup and a forensic copy after Linishing this lab practice. This lab was completed to simulate a situation in which the system is not operational. Through the use of hardware write protectors, investigators will learn how to obtain copies from storage devices like hard drives or lash drives without destroying the evidence. In this lab, researchers used the Ultra Kit Write Blocker with numerous USB and Firewire connectors, IDE and SATA write blockers, power connectors, SCSI cables, and IDE connectors to gain practical experience.

The verification that the write blocker was working was done on test drives.

Investigators tried to copy Liles through a write blocker to the test drives before using the evidence drive which prompted an error message. FTK imager software helped to copy the truest state of the media as possible with the current technology. An integrity test of the copy was done using SHA-1 and MD-5 hash values that come with the FTK imager. Two different images of the same drive were made for the case with labels of ‘Original image’ and “Working image’. Both images were tested for viruses and malware using Windows 11 Defender. The ‘Original- image’ was not touched afterward and the analysis of the image was done on a ‘Working image’ using Autopsy software. After completing the detailed research inside the ‘working image’, investigators were able to locate the ’TOP- SECRET’ document.

# Reference

Forensic data collection standards were implored and carefully done as thought by the professor in class.

Lecture notes note slides used in the class were carefully studied and applied to the letter to ensure the lab can be replicated if the case gets to the court.

Dr. Modhuparna Manna. Bag &amp; Tag [Lecture slides].Retrieved from [https://canvas.newhaven.edu/courses/23551/Liles/3954418?module\_item\_id=1807104](https://canvas.newhaven.edu/courses/23551/files/3954418?module_item_id=1807104)