Intro to Cyber Forensics Lab Grading Sheet

Project: Lab 1 – Bag & Tag
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

This lab report is an outline and description of the simulated crime scene conducted at Patrick F. Taylor Hall 3304 S Quad Dr, Baton Rouge, LA 70803 in room 2341, provided for laboratory exercise 1 conducted on February 31, 2023. Investigators were issued a search warrant to control, document, and seize all electronic evidence at the scene. Investigators were informed that AI Lagniappe had been using the computer, and we were ordered to investigate his workspace.

At the crime scene, multiple sticky notes and multiple electronics were properly tagged and bagged in Faraday bags. Faraday bags were used to prevent both outside signals from reaching devices, and protection from static damage. Investigators used two mobile devices, both GALAXY S20+ to photograph the crime scene. Evidence was photographed as it was discovered. Included is a timeline that logs the evidence as it was collected, and actions performed at the scene by investigators. Upon completion of collecting physical evidence, the configuration inside the BIOS of the Dell computer found on the scene was documented.

The goal of this exercise was to guide investigators through the accepted methods real-life first responders must proceed with during the search and collection of manual, digital, and electronic evidence. Investigators were required to practice standard evidence-gathering procedures, including identification of electronic devices, investigative expertise, and other general first-response policies. Standard procedures, as per the guidelines of Lecture 2.1 Bag & Tag: Search and Seizure, were followed throughout the evidence recovery process.

2 Apparatus

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

Table 1: apparatus of tools used at the crime scene

ITEM/PART	**MODEL NUMBER**	**VERSION**	**USAGE**
MSI Vector	GP66	Windows 11 PRO	Analyze evidence
Galaxy S20+ 5G	SM-G986N	V13	Camera 1
Galaxy S20+ 5G	SM-G781U	V13	Camera 2
Faraday Bag	N/A	N/A	Bag electronics
Meyer Bag	N/A	N/A	Bag non-electronics
Paper Clip	N/A	N/A	To open the CD tray when computer was powered off

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.	January 31, 2023	12:15	Arrived at crime scene, put on proper safety equipment, and secured crime scene
2.	January 31, 2023	12:16	Took photos of crime scene, computer appeared to be off but was still plugged in
3.	January 31, 2023	12:18	Unplugged power cord from the computer
4.	January 31, 2023	12:21	Two sticky notes removed from a ripped piece of newspaper, sticky notes contained the writing "This has been poisoned - Snowden" and "b-hind CHJpbnRlcg=="
5.	January 31, 2023	12:23	Bagged the ripped piece of newspaper
6.	January 31, 2023	12:27	Bagged a stained piece of paper with no writing on it
7.	January 31, 2023	12:28	Opened up a ripped and crumpled up piece of paper with no writing on it, bagged the ripped piece of paper
8.	January 31, 2023	12:30	Styrofoam cup, latex gloves, and napkin removed from crime scene
9.	January 31, 2023	12:31	Bagged the Styrofoam cup, latex gloves, and napkin
10.	January 31, 2023	12:33	Chair was moved from crime scene and examined, bottom of the desk was examined, given permission by Dr.Ibrahim Baggili to open system
11.	January 31, 2023	12:34	Computer moved on desk and opened up by investigator, pictures taken of computer internals and around the computer
12.	January 31, 2023	12:39	Power and SATA cables disconnected from hard drive, hard drive removed from system, after removing the hard drive, a sticky note was found with "lagniappe" written on it
13.	January 31, 2023	12:40	Hard drive was removed from the crime scene and pictures of it were taken, bagged hard drive
14.	January 31, 2023	12:41	Opened CD tray with paperclip, CD found inside CD tray
15.	January 31, 2023	12:42	Pictures taken of CD tray, CD removed from CD tray and bagged
16.	January 31, 2023	12:45	Keyboard, mouse, PC tower, and monitor were flipped over, sticky note with the writing "wintermute" found under the keyboard, USB found under table
17.	January 31, 2023	12:46	"CHJpbnRlcg==" entered into a base64 decoder, returned "rinter"
18.	January 31, 2023	12:47	Permission given by Dr.Ibrahim Baggili to turn on computer, computer turned on, failed to open BIOS
19.	January 31, 2023	12:48	Computer turned off and on again to get into BIOS
20.	January 31, 2023	12:49	"rinter" entered first as the wrong password, "lagniappe" entered as correct password to get to BIOS settings
21.	January 31, 2023	12:50	Documented BIOS settings
22.	January 31, 2023	12:53	Went to printer and found phone number "225-366-9149"
23.	January 31, 2023	12:55	Permission given by Dr.Ibrahim Baggili to call phone number, went into hallway to call the phone number
24.	January 31, 2023	12:57	Bagged USB and stickynotes
25.	January 31, 2023	13:00	Conducted research with the found information about the suspect

3.2 Procedure

3.2.1 Operation Procedure

The investigation began by putting on safety equipment and taking photographs of the crime scene and the electronic devices on the desk (Figures 1-4). The devices identified were a Lenovo computer, Dell monitor, and a Dell keyboard, which were all off (Figures 1-4). After documenting the devices at the crime scene, the power cable was unplugged from the back of the computer. Next, loose items were taken off the desk, starting with a ripped piece of the Reveille newspaper with two sticky notes on it (Figures 8, 9). One of the sticky notes had "b-hind CHJpbnRlcg==" written on it. The message was base64 encrypted (Figures 8, 9). Investigators took sticky notes off the newspaper and then documented and placed them in an evidence bag. Next, investigators removed two more pieces of paper, each without writing, a Styrofoam cup, latex gloves, and a napkin from the crime scene and placed them into evidence bags (Figure 4).

Investigators then moved to focus on the personal computer at the crime scene. Investigators proceeded with caution and asked Dr.Ibrahim Baggili for permission to open the device. Investigators opened the computer by taking off the side panel and inspected the internals (Figure 12). Investigators took pictures of the wiring, power supply, graphics card, and hard drive, and then removed the hard drive from the device (Figures 13-15). After removing the hard drive, investigators found a sticky note with the writing "lagniappe" (Figure 20). Investigators documented the hard drive and then bagged it. Investigators then proceeded to open the CD tray using a paper clip found on the crime scene. In the CD tray was a CD labeled "Destruction". The CD was removed and put in an evidence bag.

After finishing investigating the computer, investigators then focused on the rest of the desk which yielded another sticky note found under the keyboard with the writing "wintermute" and a USB drive found under the desk (Figures 24, 27). Investigators used a base64 decoder to decrypt the encrypted message from figure 8 and 9, and "rinter" was the plain text result. Following this, investigators asked Dr.Ibrahim Baggili for permission to turn on the system. Investigators failed to reach the BIOS, so it was turned off and back on. Investigators then reached the system's BIOS; however, the BIOS had password protection. After a failed attempt to get to the settings menu using the password "rinter," investigators used "lagniappe" and got into the BIOS. Investigators then documented the BIOS by taking pictures of each page individually, and the computer was then turned off (Figures 30-66). After documenting the BIOS, investigators were directed by Dr.Ibrahim Baggili to find the physical location of AI Lagniappe. The process of finding the suspect is described in the next section Post Operation procedure.

3.2.2 Post Operation Procedure

Investigators decrypted the sticky note with base64 found in figures 8 and 9 to "b-hind rinter". From this message, investigators assumed that the message likely meant to be "behind printer." After consulting with Dr. Ibrahim Baggili this was confirmed. Investigators then checked behind the printer to find a phone number written on a sheet of paper: 225-366-9149 found (Figure 29). After asking for permission from TA Clinton Walker, investigators proceeded to call the number. The phone call went to voicemail, and the person speaking in the voicemail is believed to be the suspect AI Lagniappe. The transcript of the voicemail is as follows: "Hello. You've reached Lagniappe AI. If you want me, you gotta find me. On the Zucc. My Zucc. He's the CEO of the company you all know." Investigators deduced that "Zucc" was referring to Mark Zuckerberg and that the suspect was hinting to look him up on Facebook. Investigators proceeded to look for the suspect's Facebook page but had issues finding it due to believing the suspect's name was Al Lagniappe instead of AI Lagniappe. Dr. Ibrahim Baggili instructed investigators that it was AI Lagniappe, and shortly after the suspect's Facebook was identified.

The Facebook account of the suspect had a description and four posts (Figures 67-69). Investigator used this information as hints toward finding the suspect's location. Investigators noted that the first post "6y4CNZiZ2+aiH7UHM8MU5cHuT7CyJJoTk+uFpZyc/SQ=" was some type of encryption (Figure 68). The second post "Rush is the best band in the world! Period." led the investigators to look through the songs Rush had released (Figure 69). The post "Lock and key! wow... just wow. Do you know what you are supposed to lock?" refers to a song by the band Rush called Lock and Key. Investigators looked through the lyrics of the song and found the line: "I don't want to face the killer instinct, Face it in you or me, So we keep it under lock and key, Lock and key", indicating "killer instinct" to likely be important to the investigation. The description of the profile read "I love when fish blow bubbles. CBC Baby! My favorite website is https://codebeautify.org." indicated two clues (Figure 67). The first clue was that the investigators would be able to decrypt the encrypted post using the codebeautify website and that most likely the fish comment was referring to blowfish.js, an encryption algorithm. The second clue was CBC, being one of the cipher modes of blowfish.js, which was also likely important to the case.

Investigators then put together each piece of the puzzle and were able to decrypt the encrypted message in figure 68 by using the blowfish.js with a CBC cipher mode and the key "killer instinct." The result was the location of 30.4133°N, 91.1800°W (Figure 70-72). Investigators then passed this information to Dr. Ibrahim Baggili and left the crime scene.

3.3 Figures

3.3.1 Crime Scene

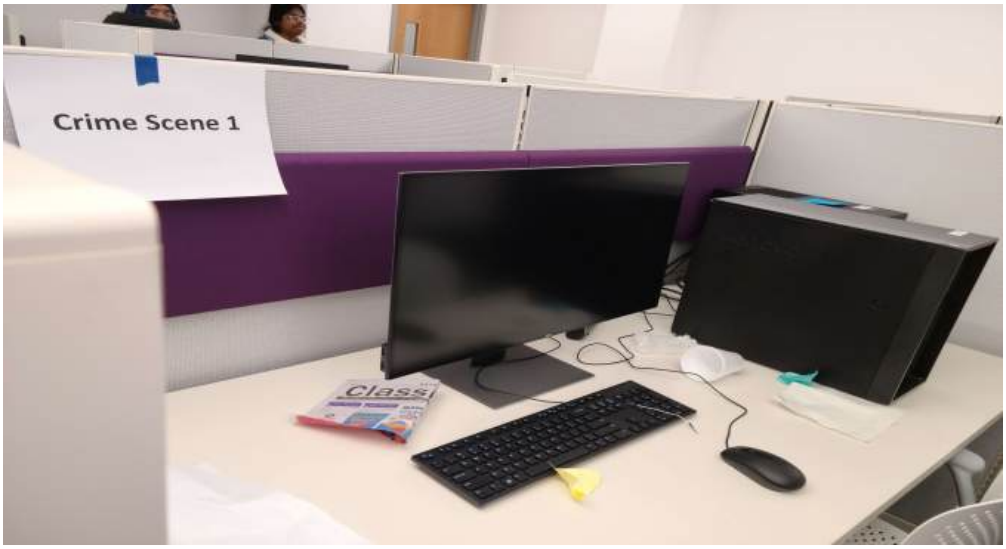


Figure 1: Side view of the crime scene.

Figure 2: Trash on the left side of the crime scene.

Figure 3: Trash on the right side of the crime scene.

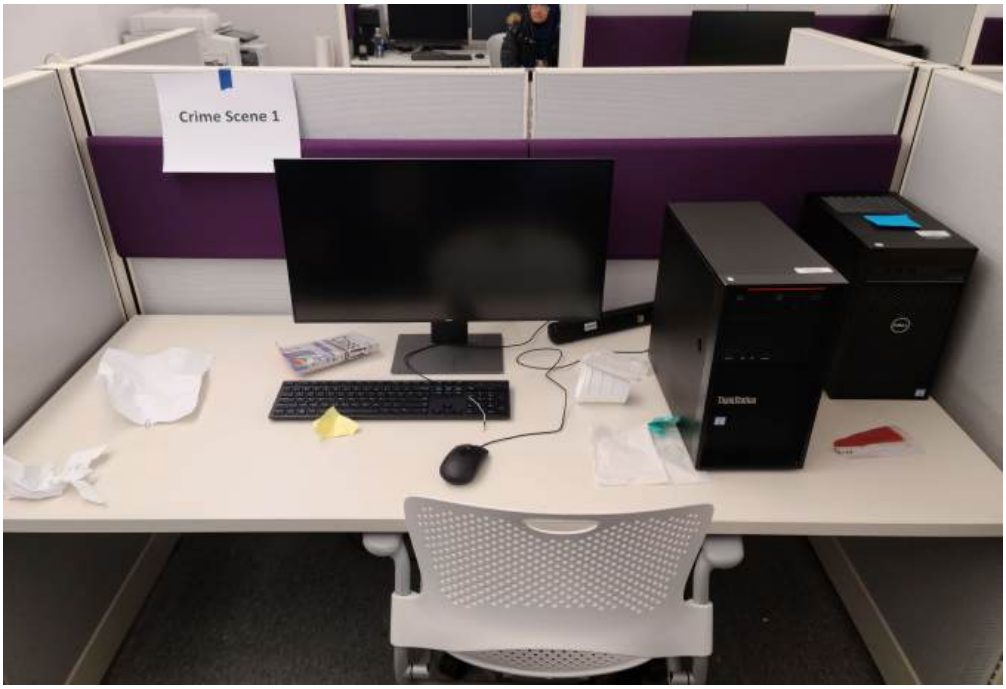


Figure 4: Front view of the crime scene.

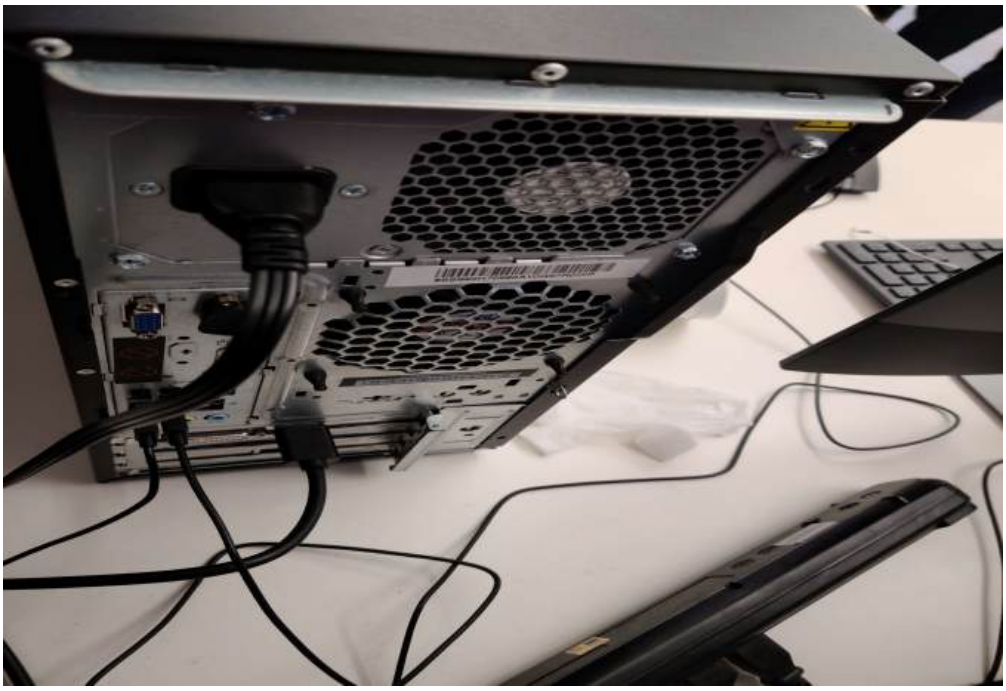


Figure 5: Back view of the crime scene.

Figure 6: Wires underneath the desk of the crime scene.

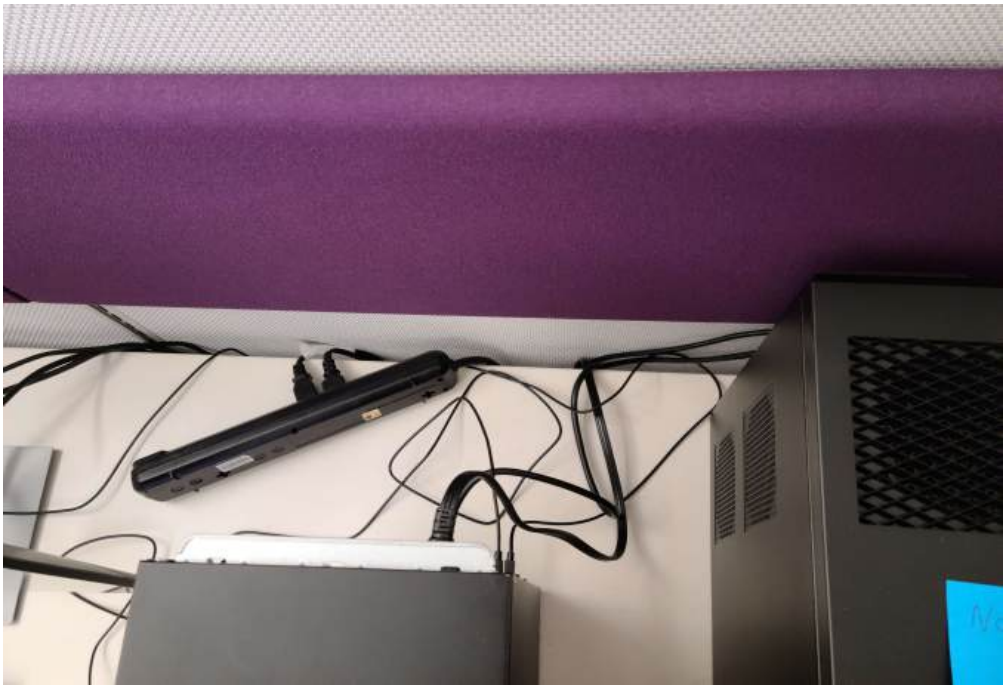


Figure 7: Wires on top of the desk of the crime scene.

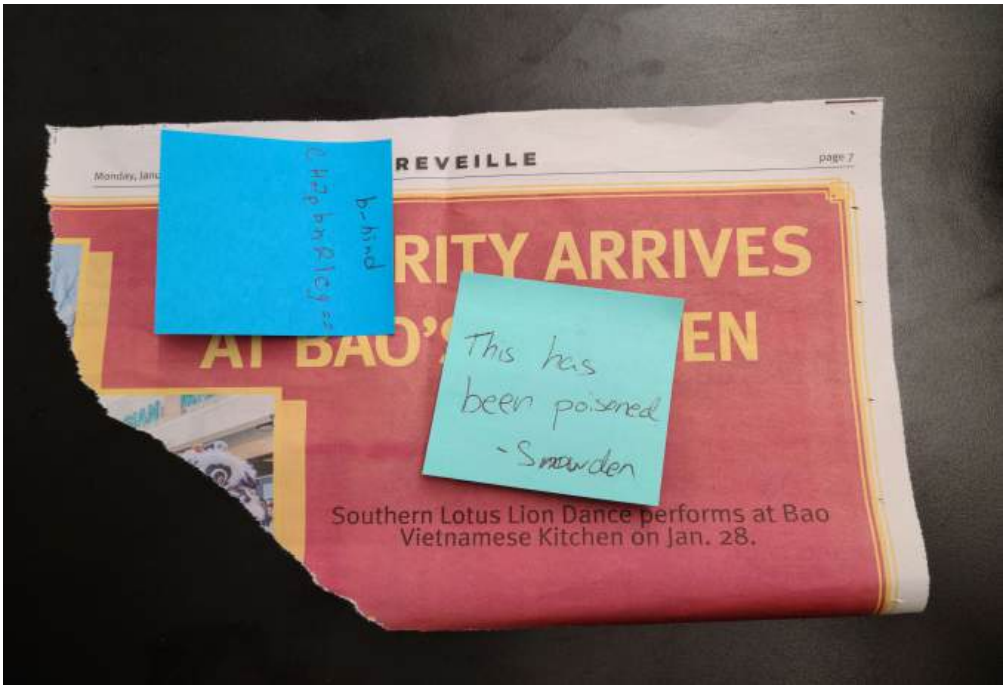


Figure 8: Reveille newspaper with two sticky notes.

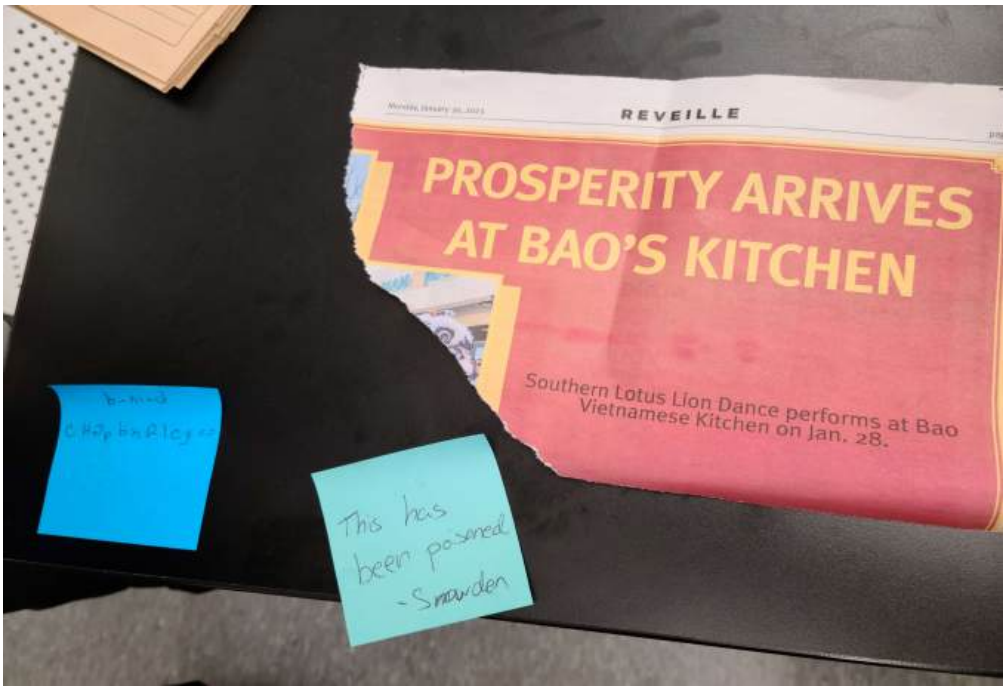


Figure 9: Reveille newspaper with sticky notes removed.

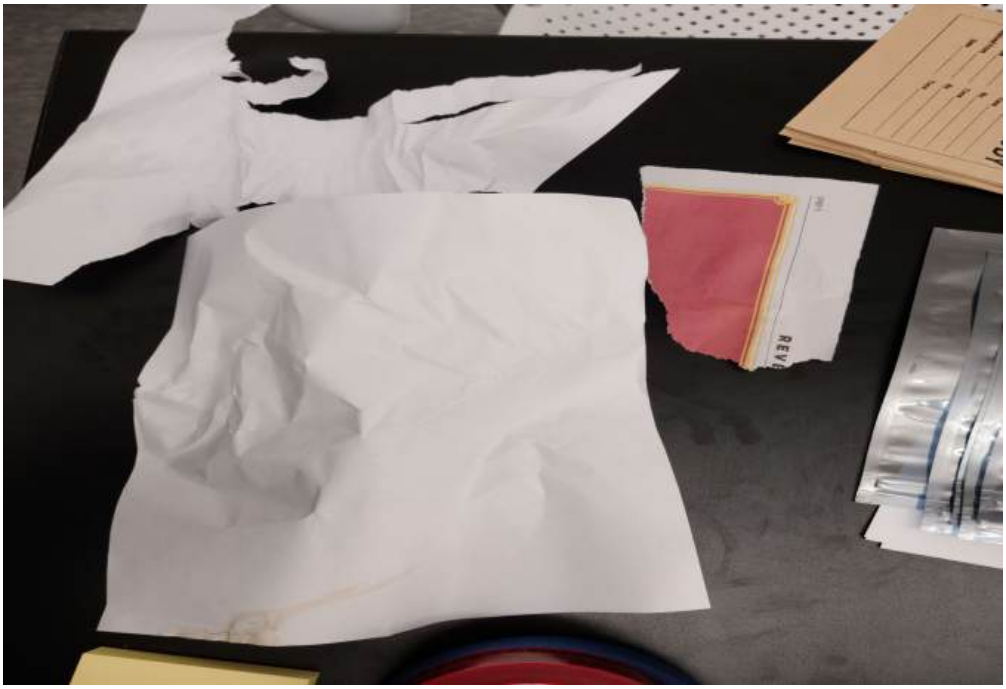


Figure 10: Articles of trash found at the crime scene.

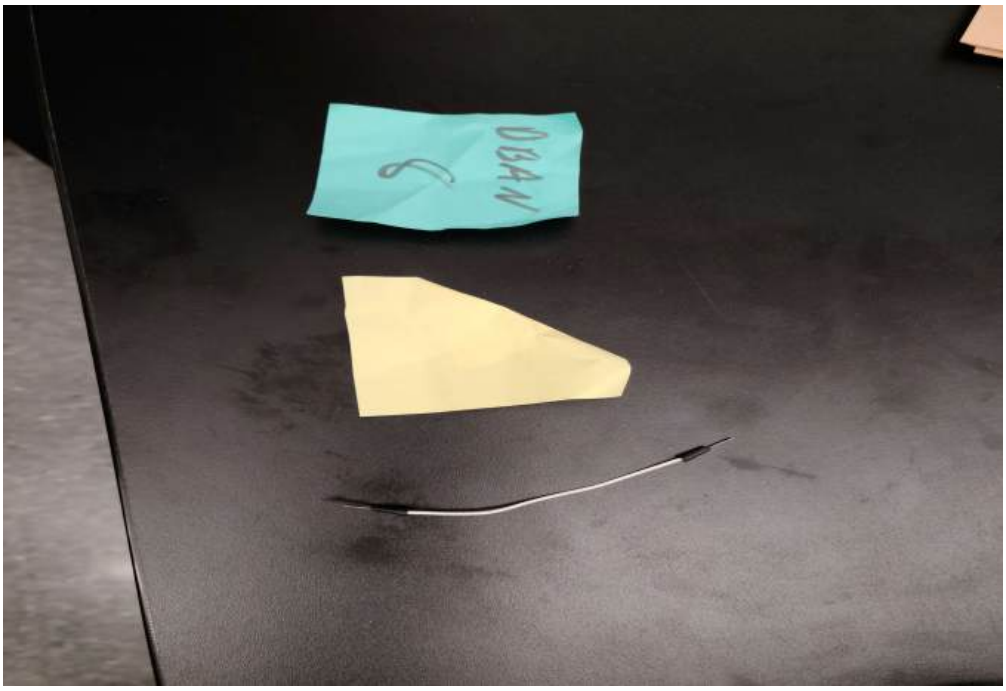


Figure 11: Articles of litter found at the crime scene.

Figure 12: Open view of the inside of the computer.

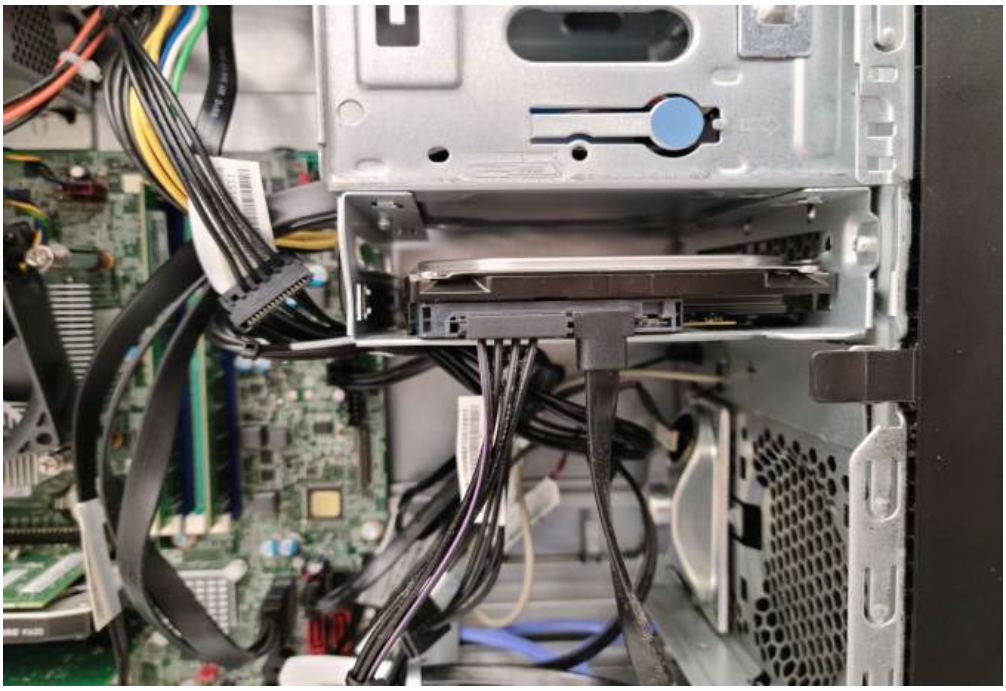


Figure 13: Close-up photo of the hard drive in the computer.

Figure 14: Image of the power supply in the computer.

Figure 15: Image of the graphics card and network adapter card.

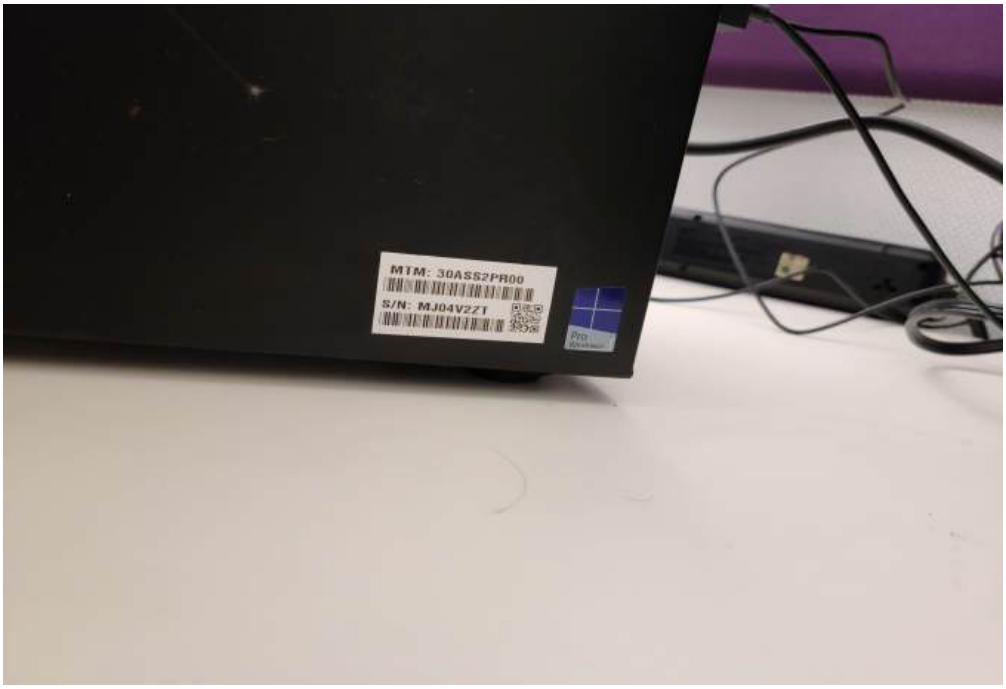


Figure 16: Close-up image of identification information on computer.

Figure 17: Front view of the computer.

Figure 18: Image of the hard drive removed from the computer.

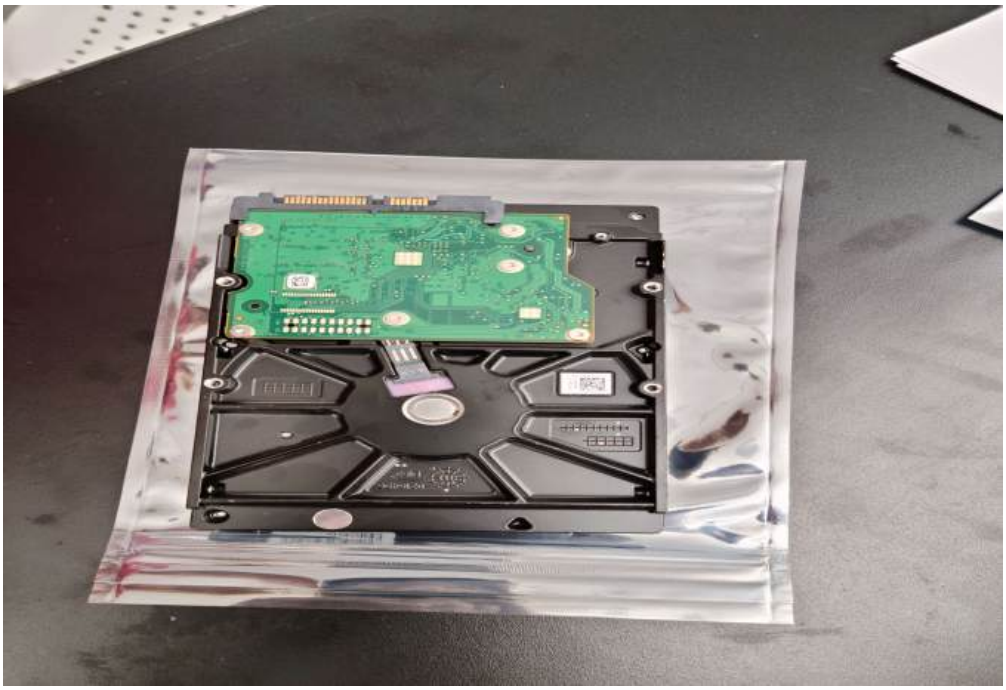


Figure 19: Image of the hard drive removed from the computer.

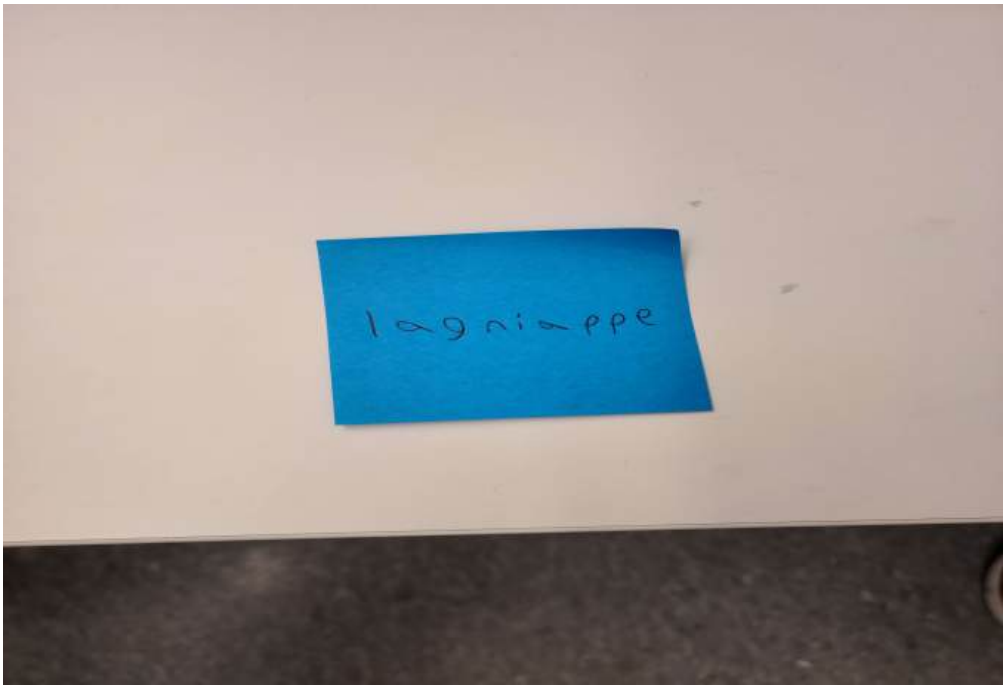


Figure 20: Image of the sticky note found in the computer.

Figure 21: Image of the open CD drive.

Figure 22: Image of CD with "Destruction" written on it from the computer.

Figure 23: Image of the back side of the CD found.

Figure 24: Sticky note with "Winter mute" found under the keyboard.

Figure 25: Image of the bottom of the monitor stand.

Figure 26: Image of the bottom of the computer.

Figure 27: Image of hidden flash drive found underneath the desk.

Figure 28: Image of flash drive found.

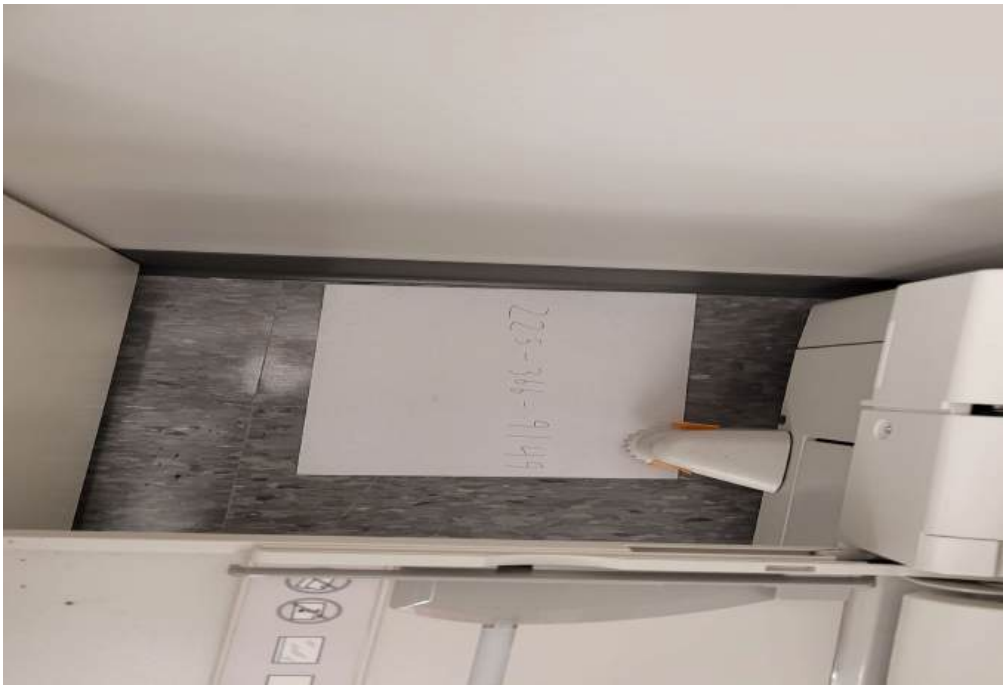


Figure 29: Image of a sheet of paper with phone number found behind printer.

3.3.2 BIOS

Figure 30: BIOS Initialization.

Figure 31: Lenovo Startup Screen.

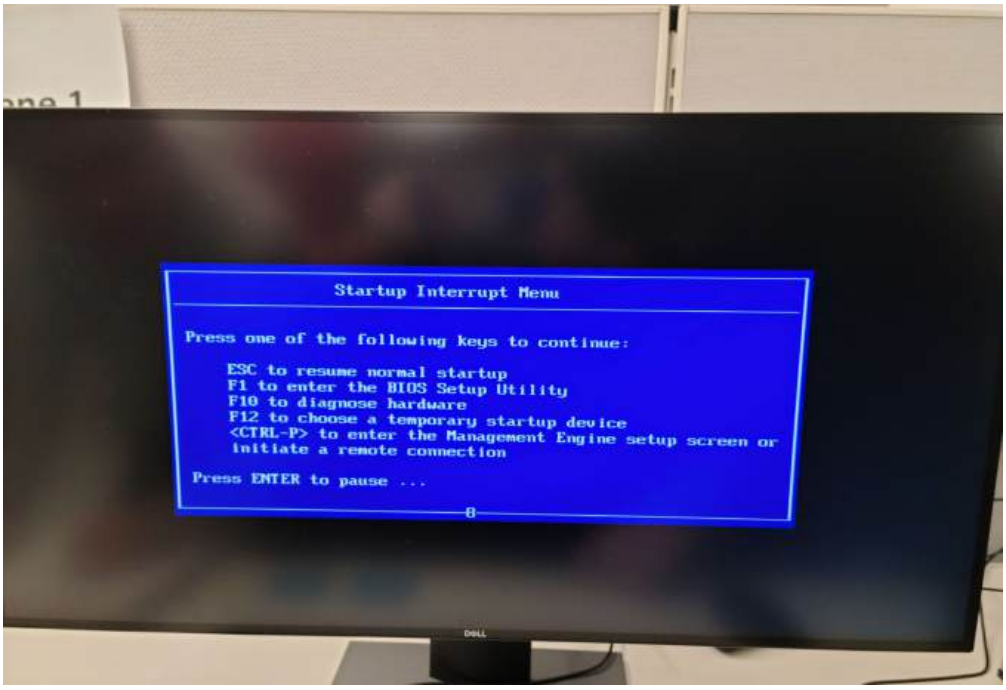


Figure 32: BIOS Startup Interrupt Menu.

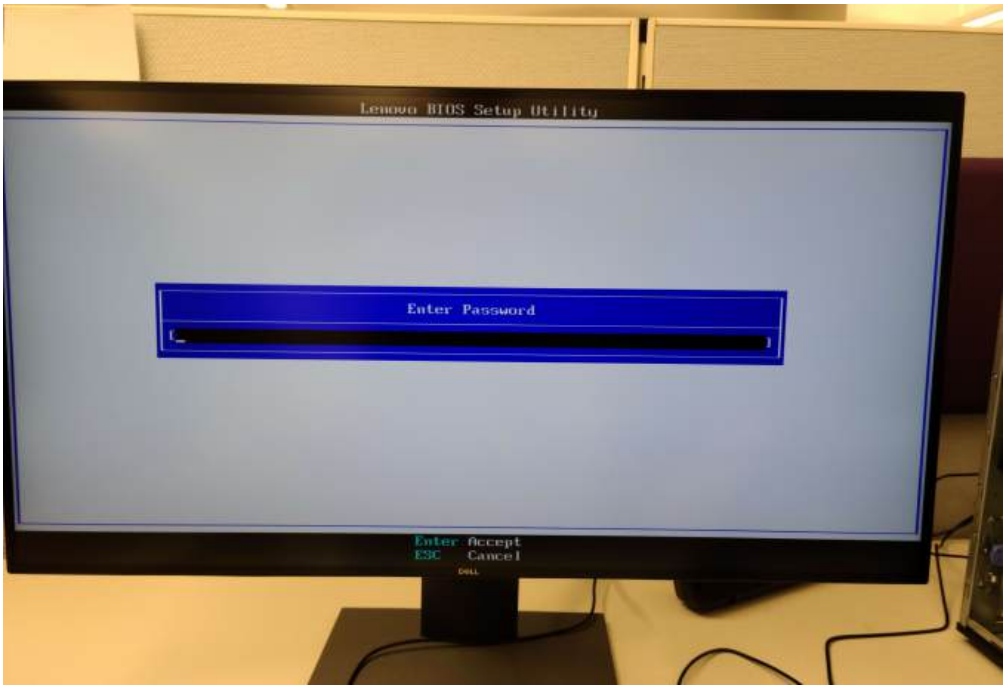


Figure 33: BIOS Setup Utility - Password Screen.

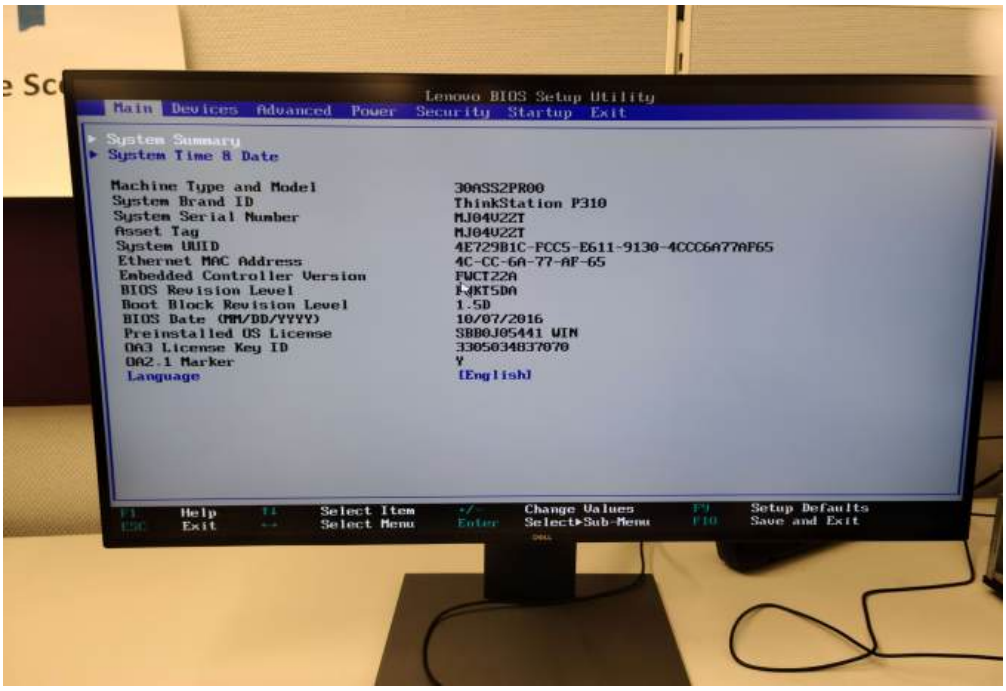


Figure 34: BIOS - Main.

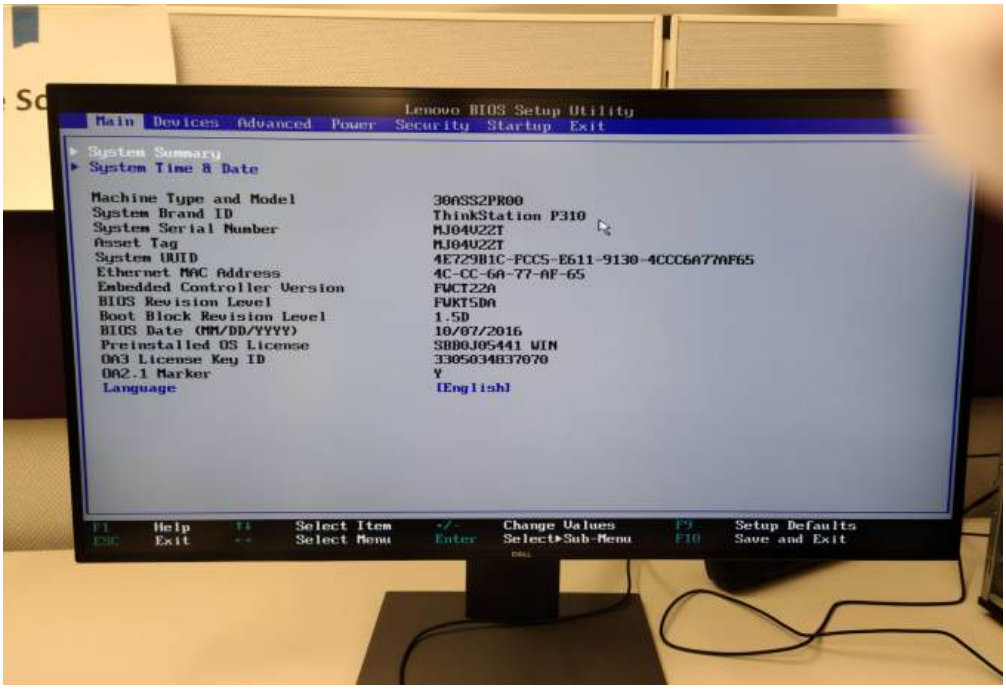


Figure 35: BIOS - Main.

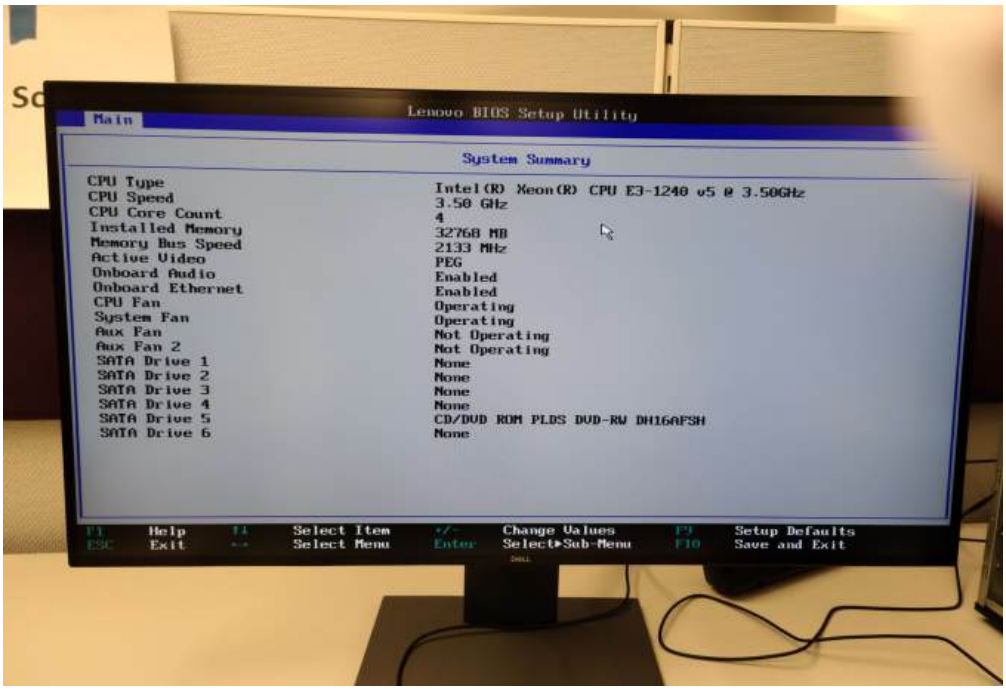


Figure 36: BIOS - Main - System Summary.

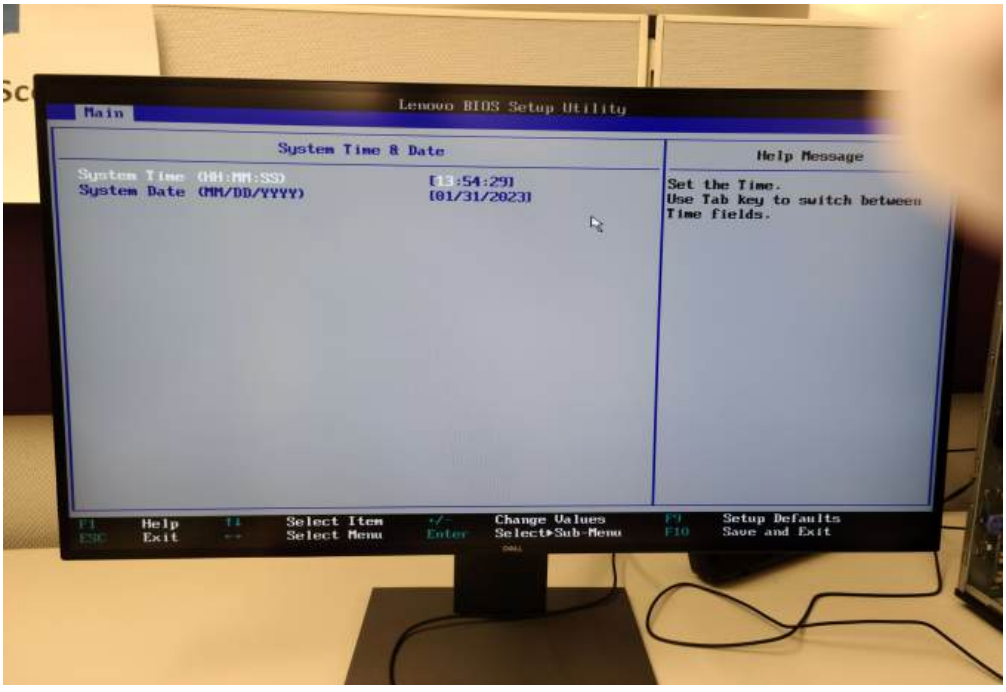


Figure 37: BIOS - Main - System Time & Date.

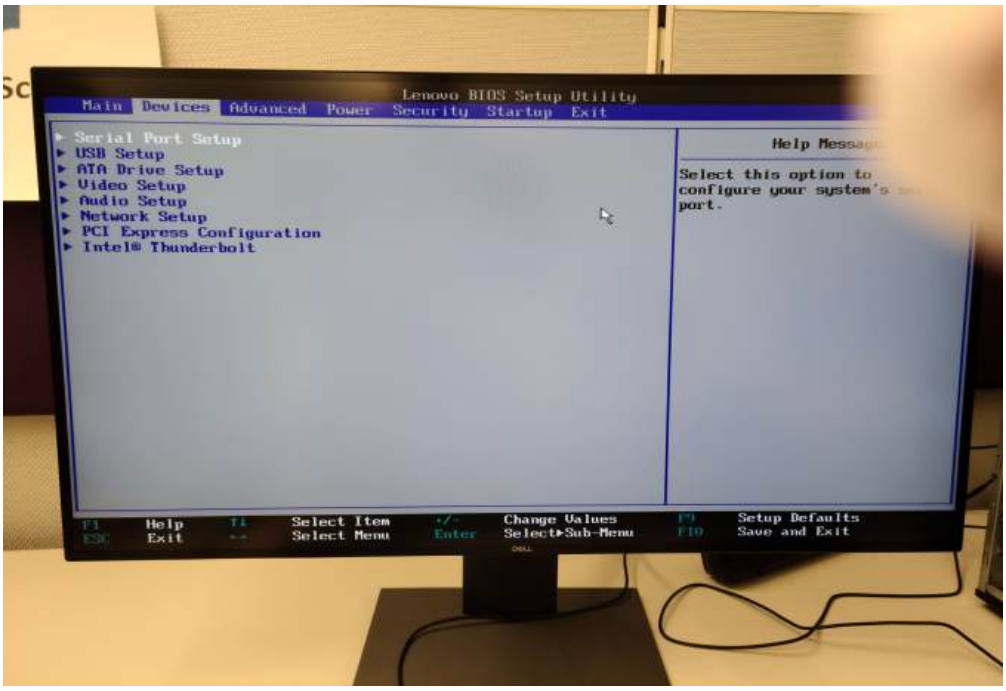


Figure 38: BIOS - Devices.

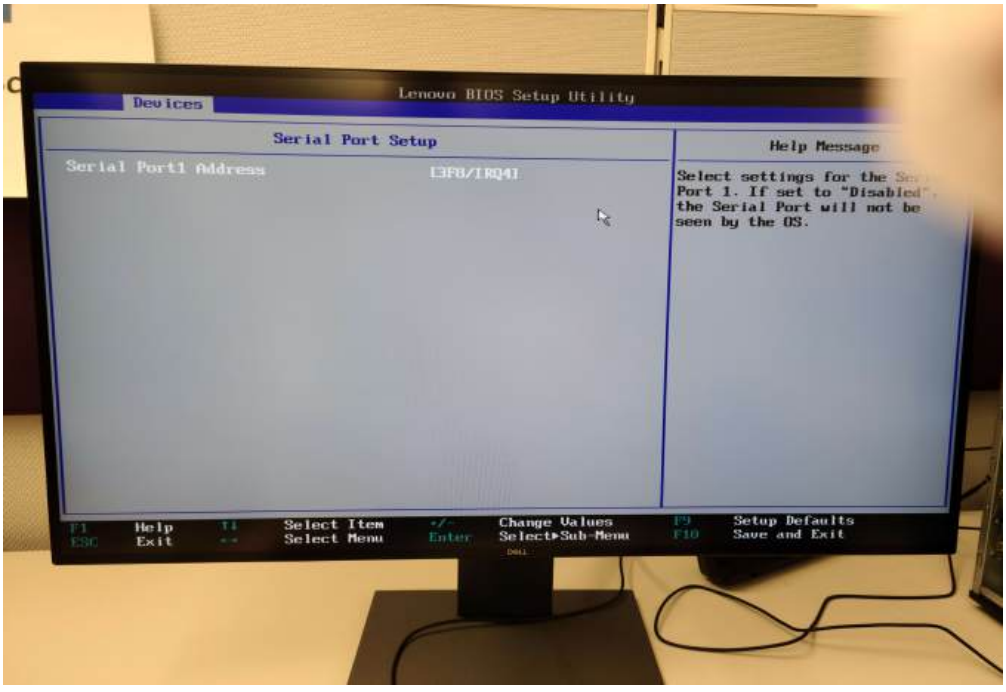


Figure 39: BIOS - Devices - Serial Port Setup.

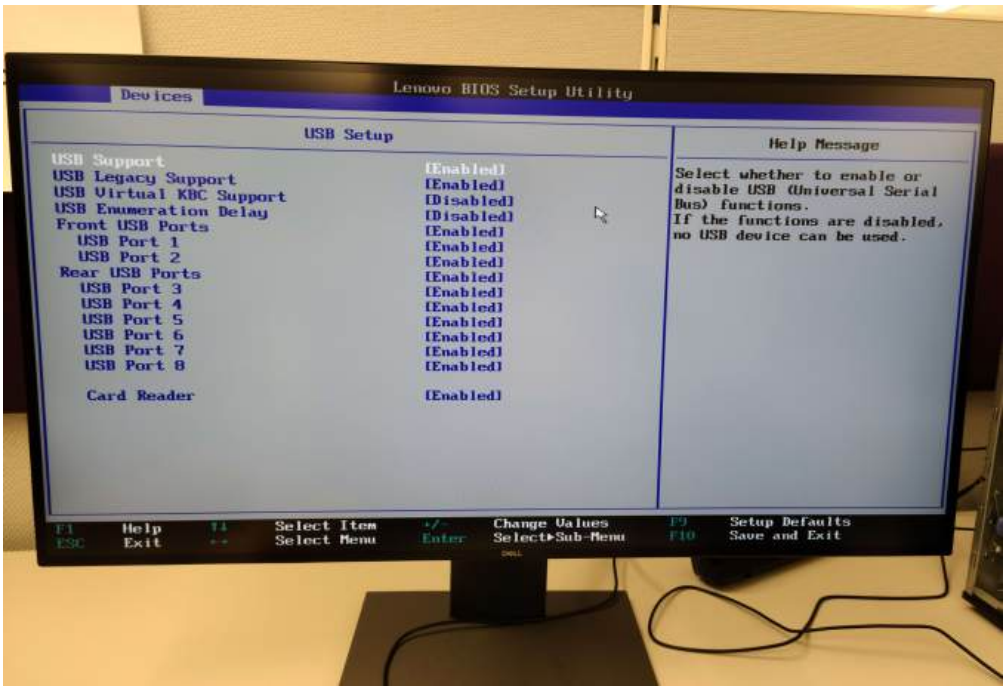


Figure 40: BIOS - Devices - USB Setup.

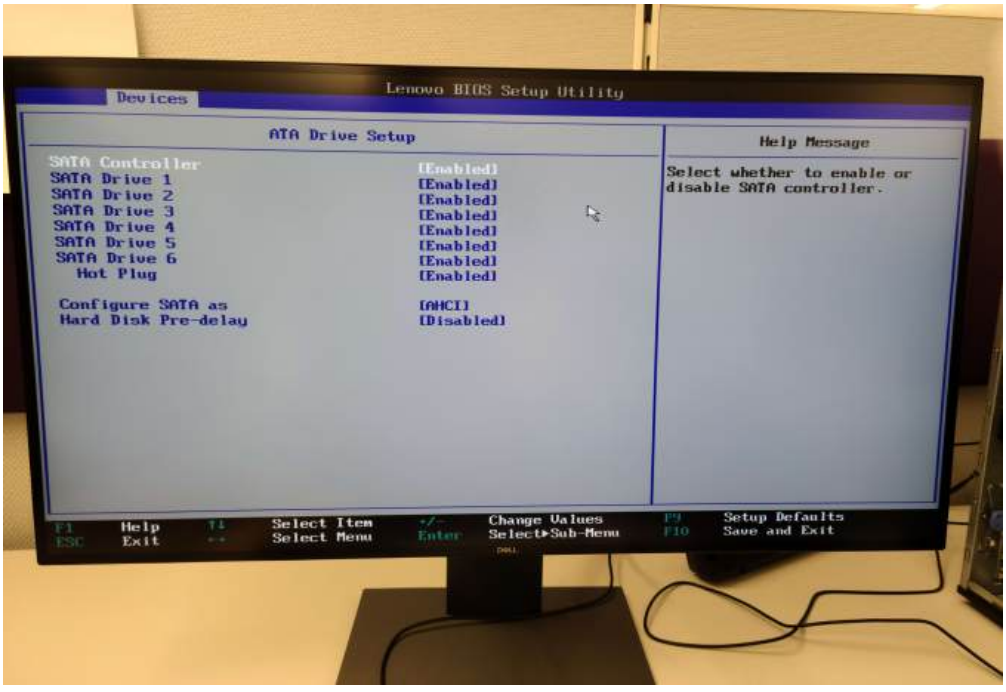


Figure 41: BIOS - Devices - AIA Drive Setup.

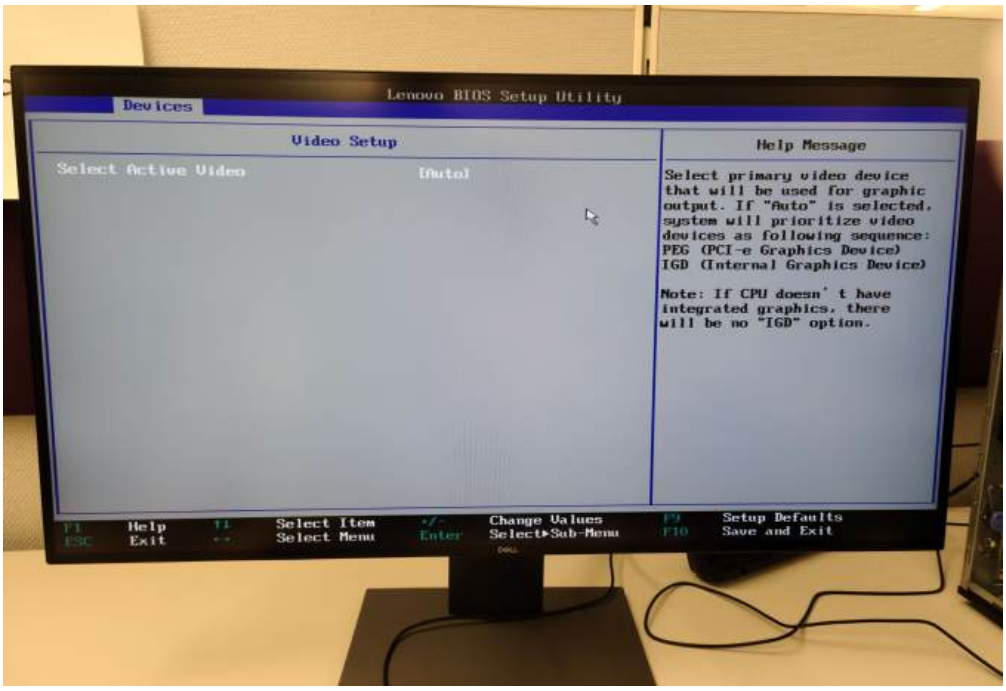


Figure 42: BIOS - Devices - Video Setup.

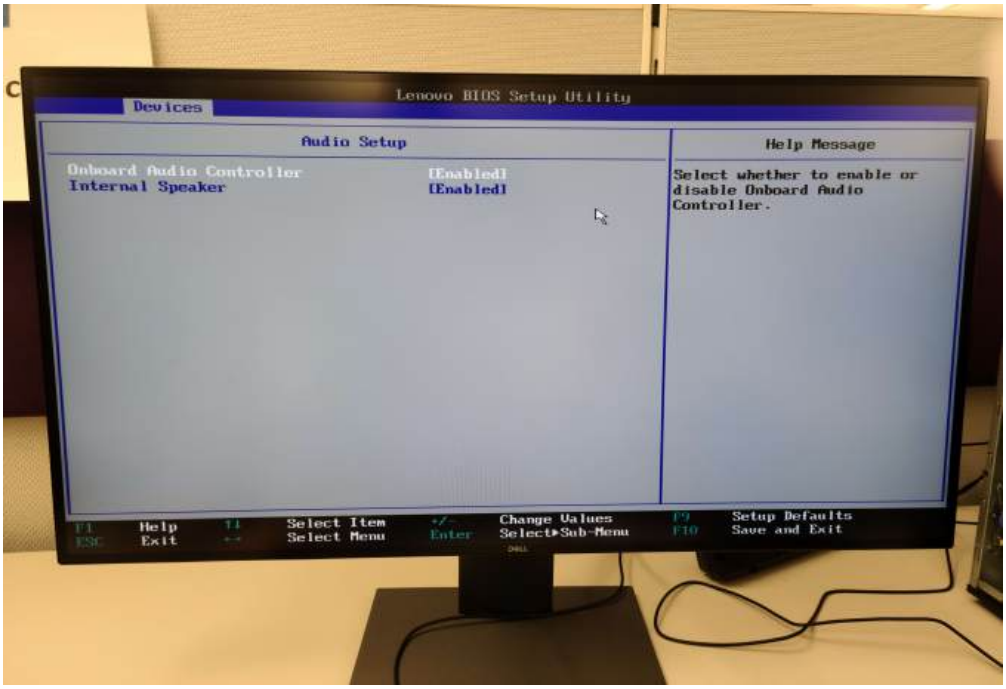


Figure 43: BIOS - Devices - Audio Setup.

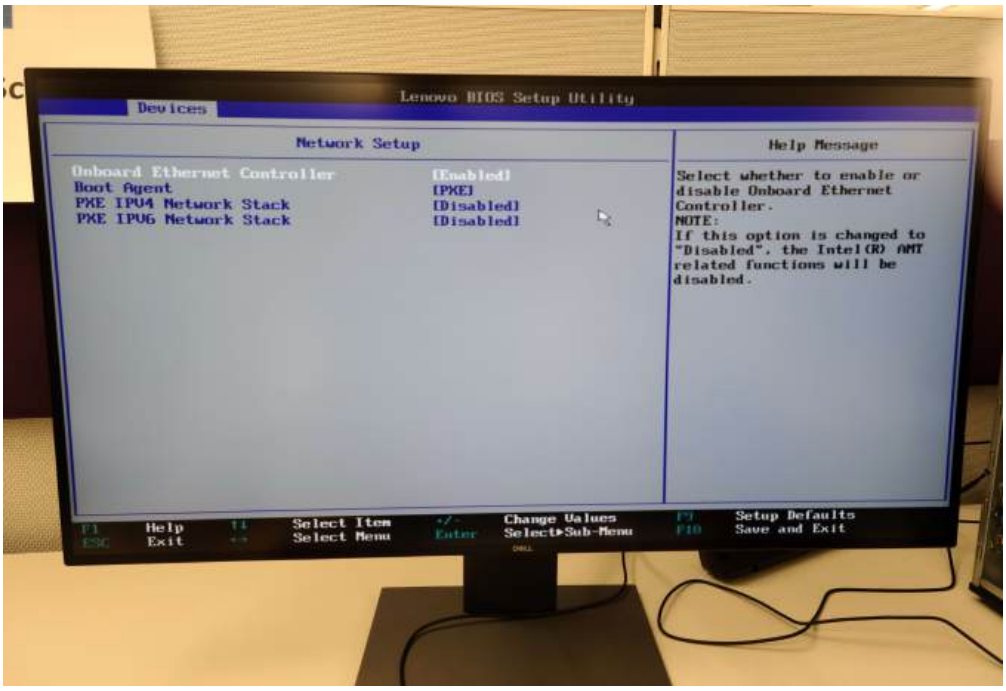


Figure 44: BIOS - Devices - Network Setup.

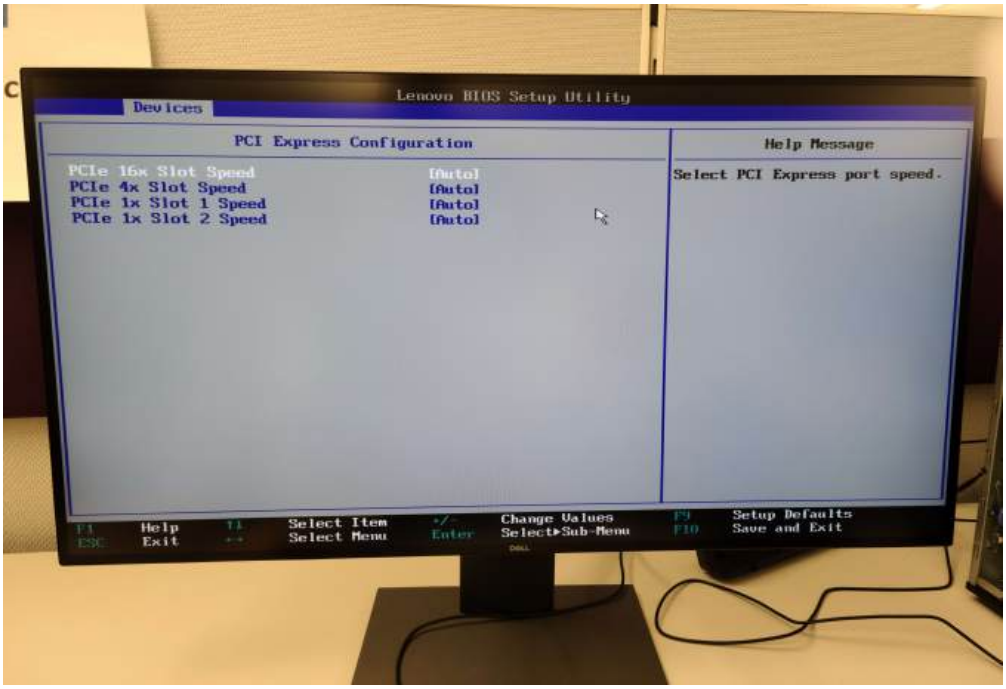


Figure 45: BIOS - Devices - PCI Express Configuration.

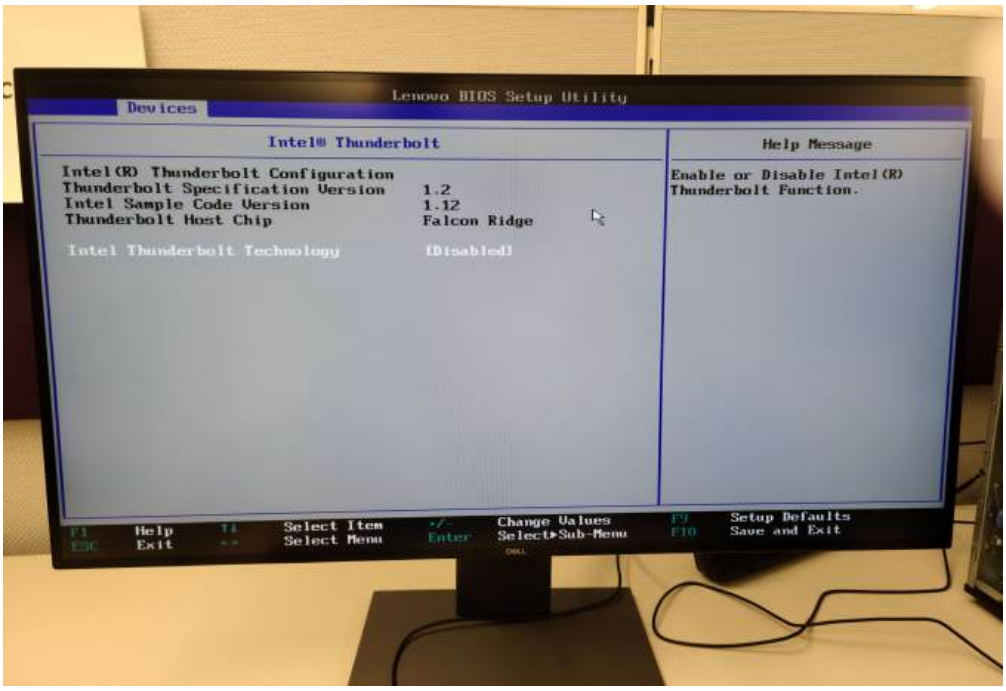


Figure 46: BIOS - Devices - Intel Thunderbolt.

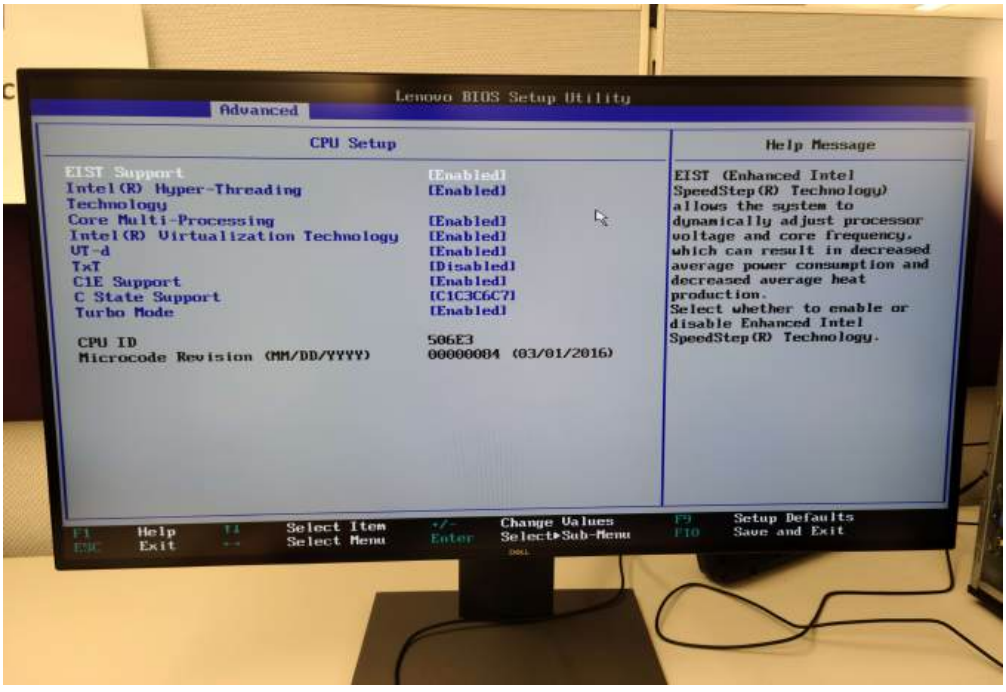


Figure 47: BIOS - Advanced - CPU Setup.

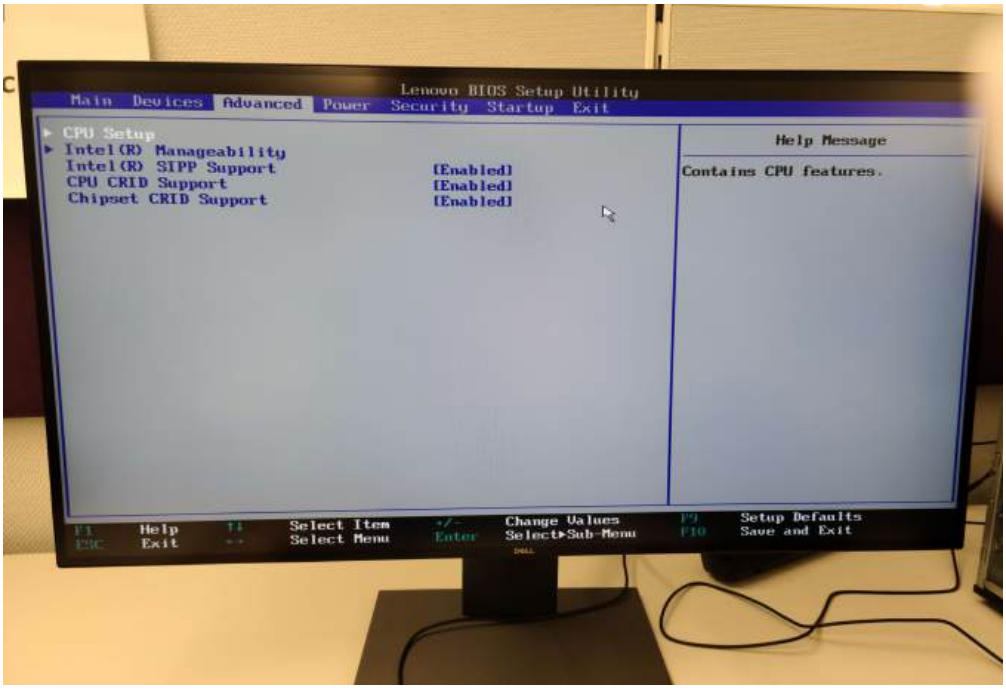


Figure 48: BIOS - Advanced.

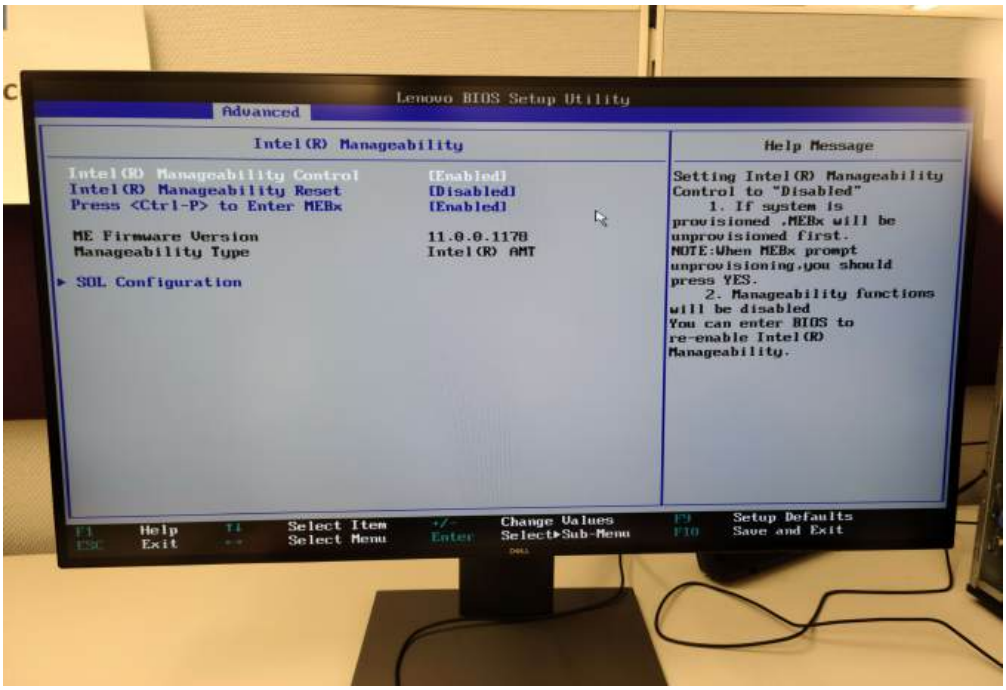


Figure 49: BIOS - Advanced - Intel (R) Manageability.

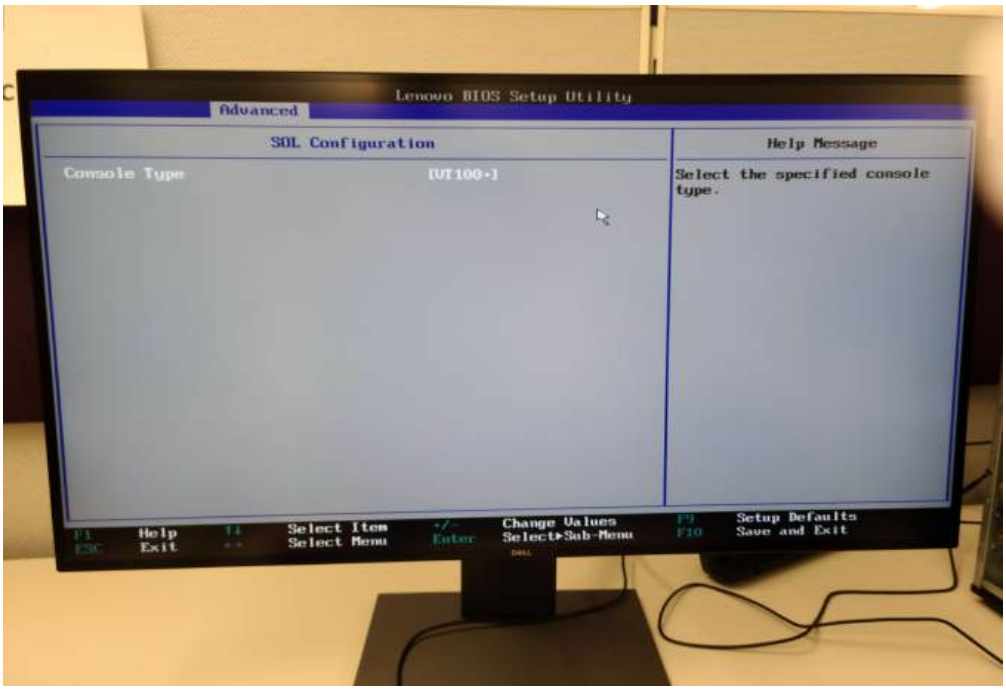


Figure 50: BIOS - Advanced - Intel (R) Manageability - SOL Configuration.

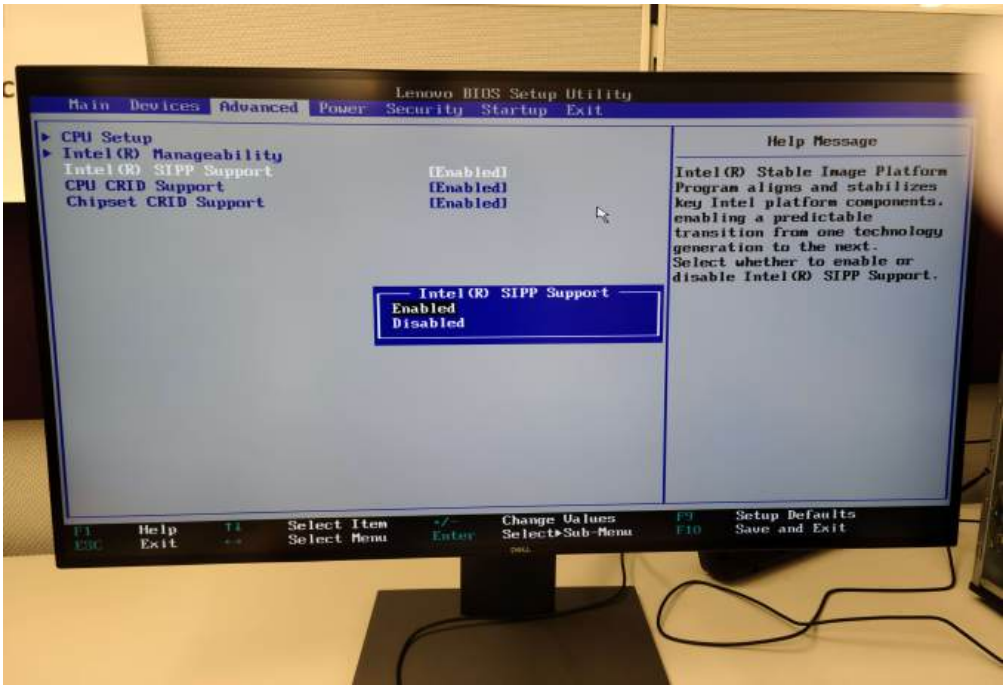


Figure 51: BIOS - Advanced - Intel(R) SIPP Support.

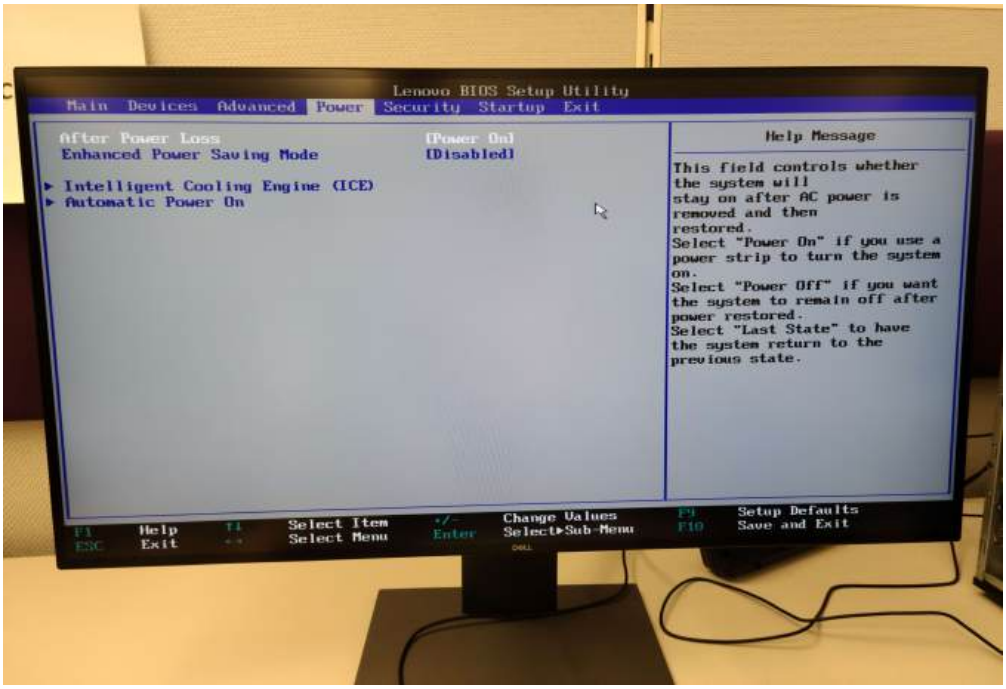


Figure 52: BIOS - Power.

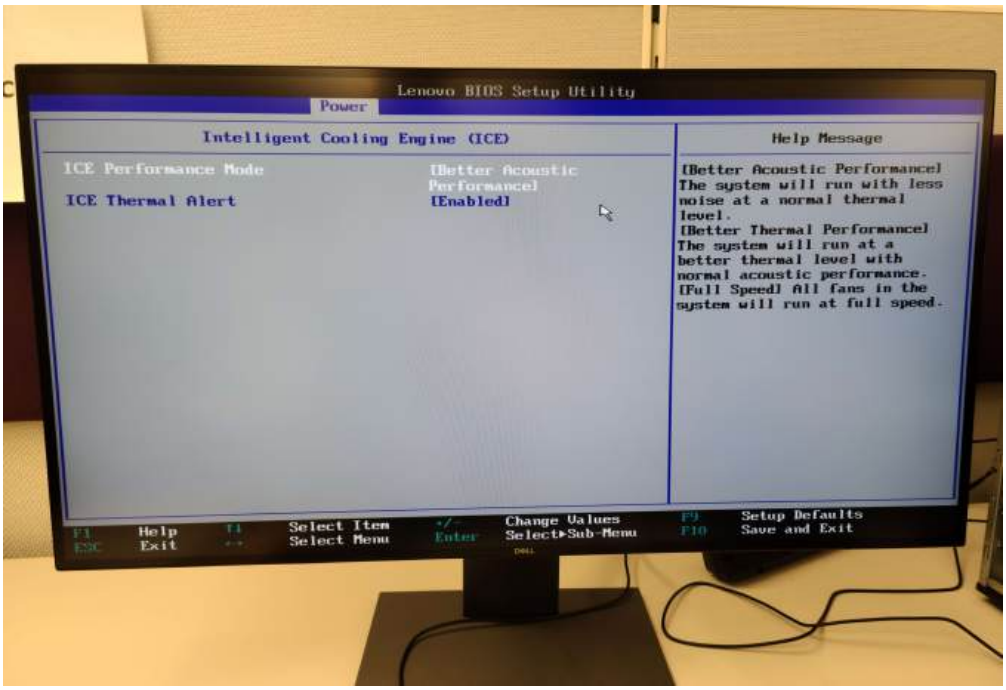


Figure 53: BIOS - Power - Intelligent Cooling Engine (ICE).

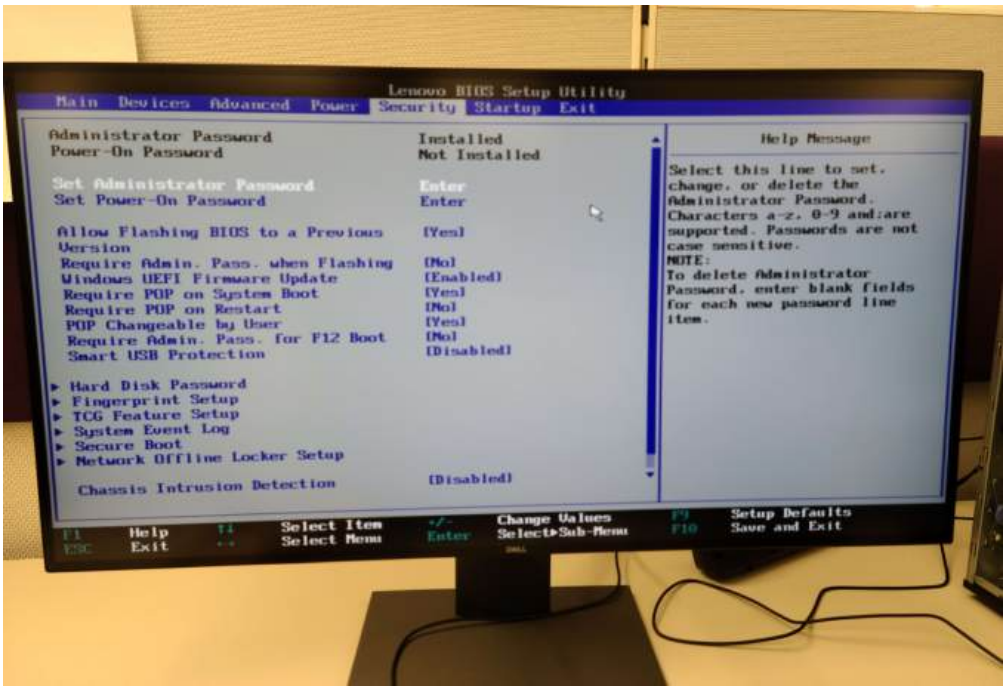


Figure 54: BIOS - Security.

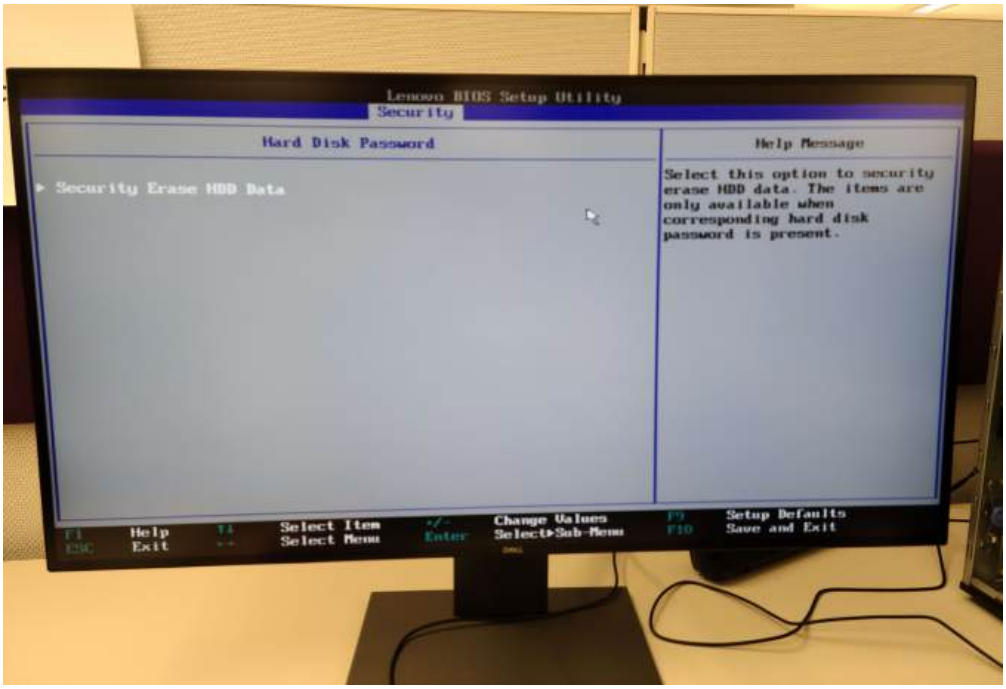


Figure 55: BIOS - Security - Hard Disk Password.

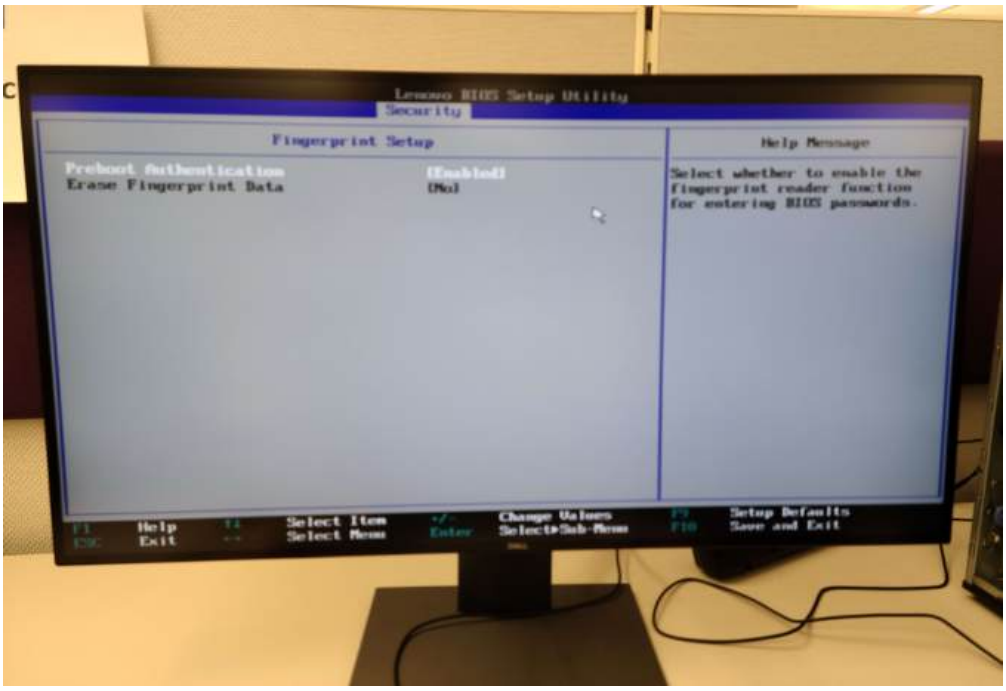


Figure 56: BIOS - Security - Fingerprint Setup.

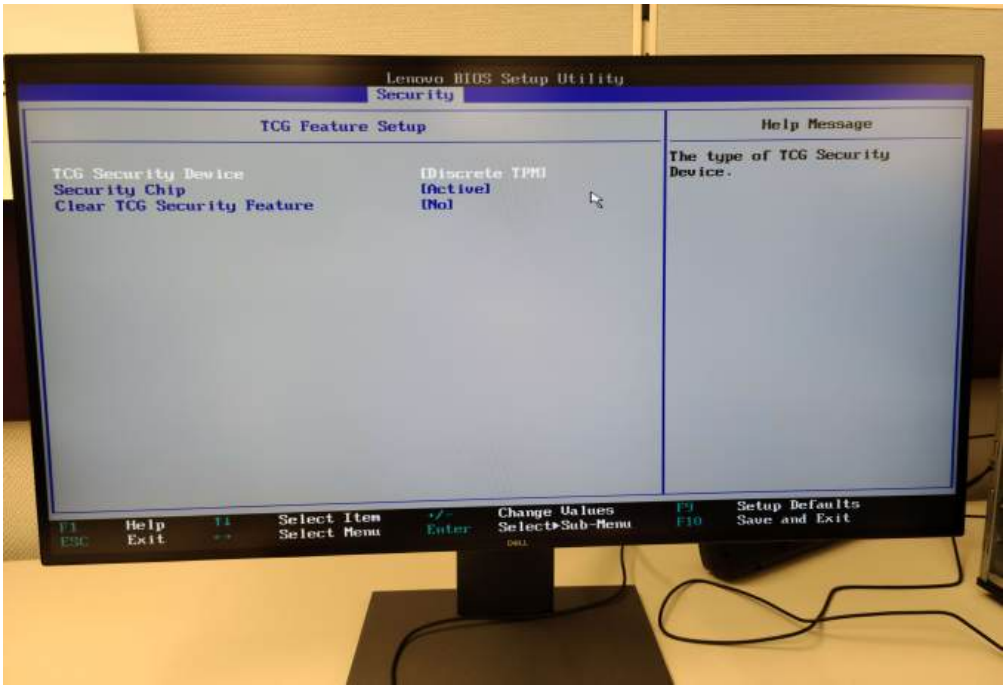


Figure 57: BIOS - Security - TCG Feature Setup.

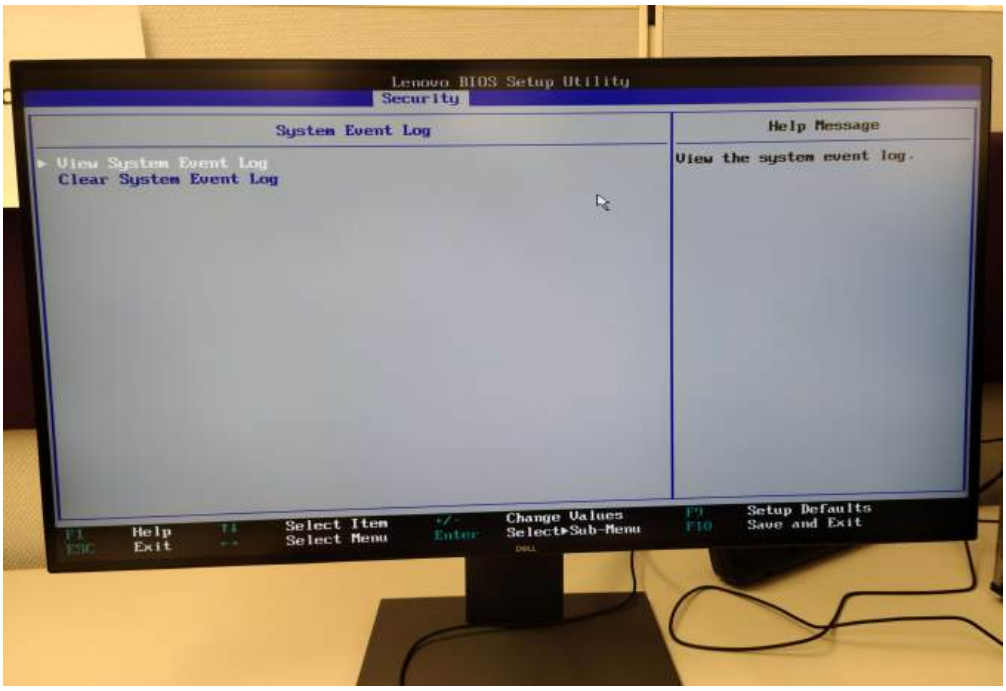


Figure 58: BIOS - Security - System Event Log.

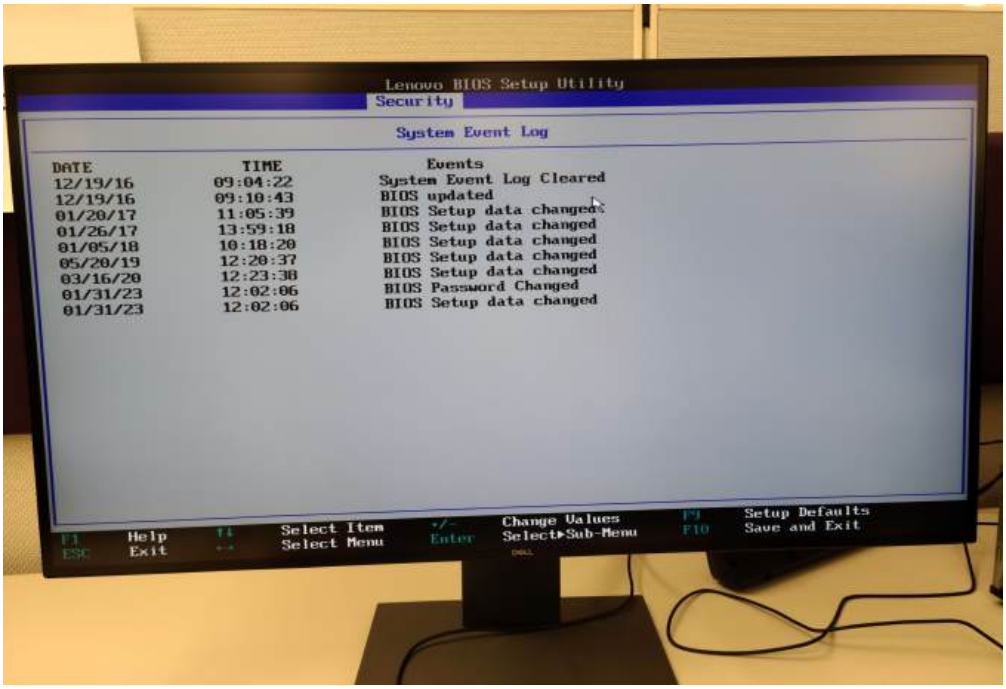


Figure 59: BIOS - Security - System Event Log - View System Event Log.

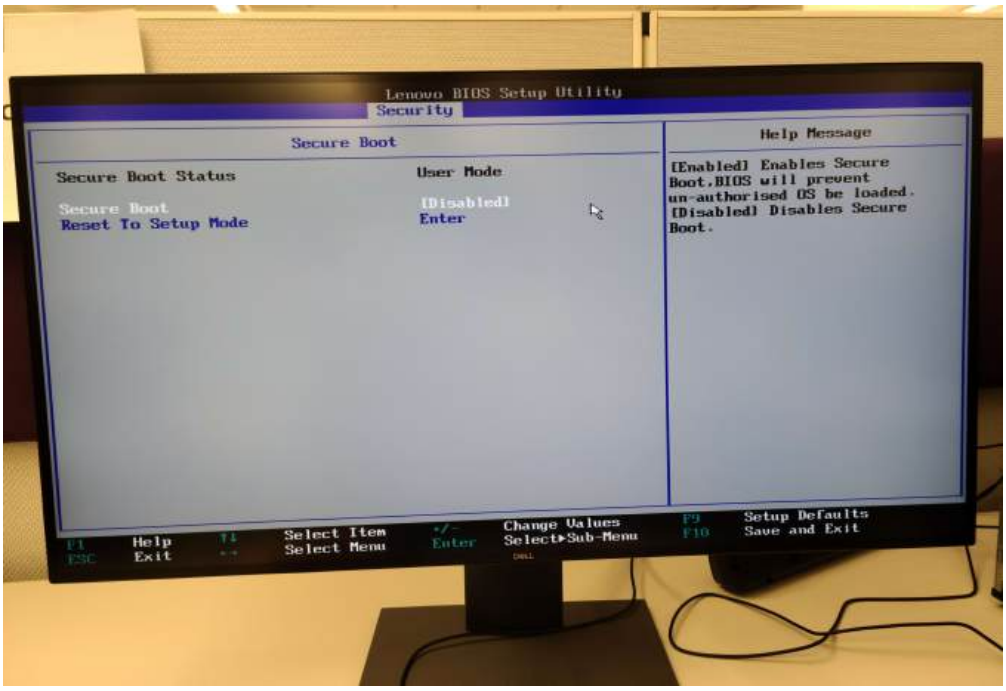


Figure 60: BIOS - Security - Secure Root.

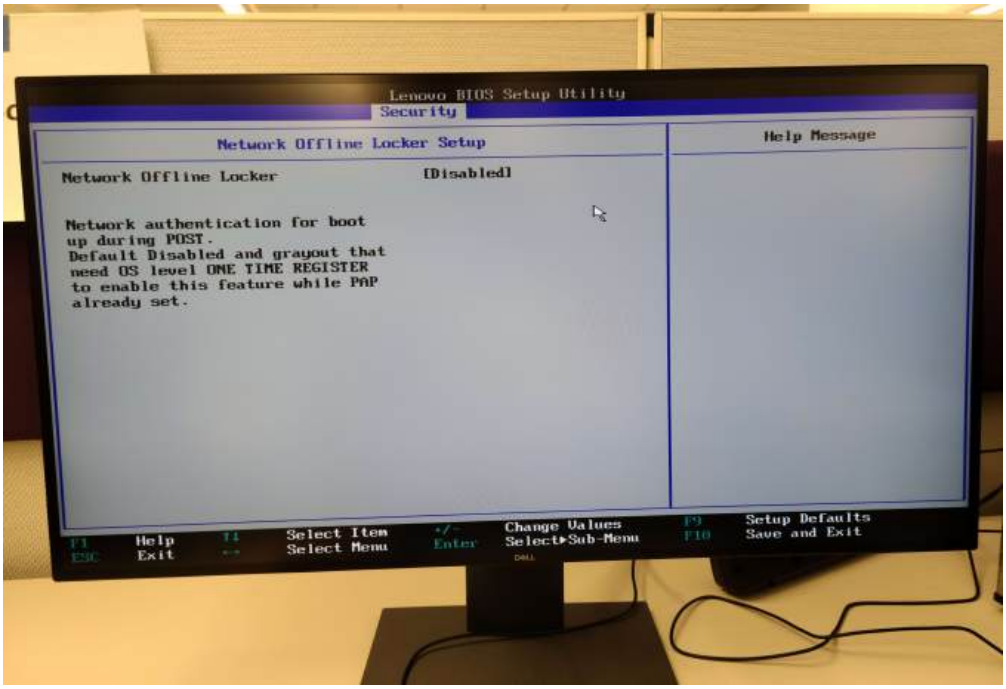


Figure 61: BIOS - Security - Network Offline Locker Setup.

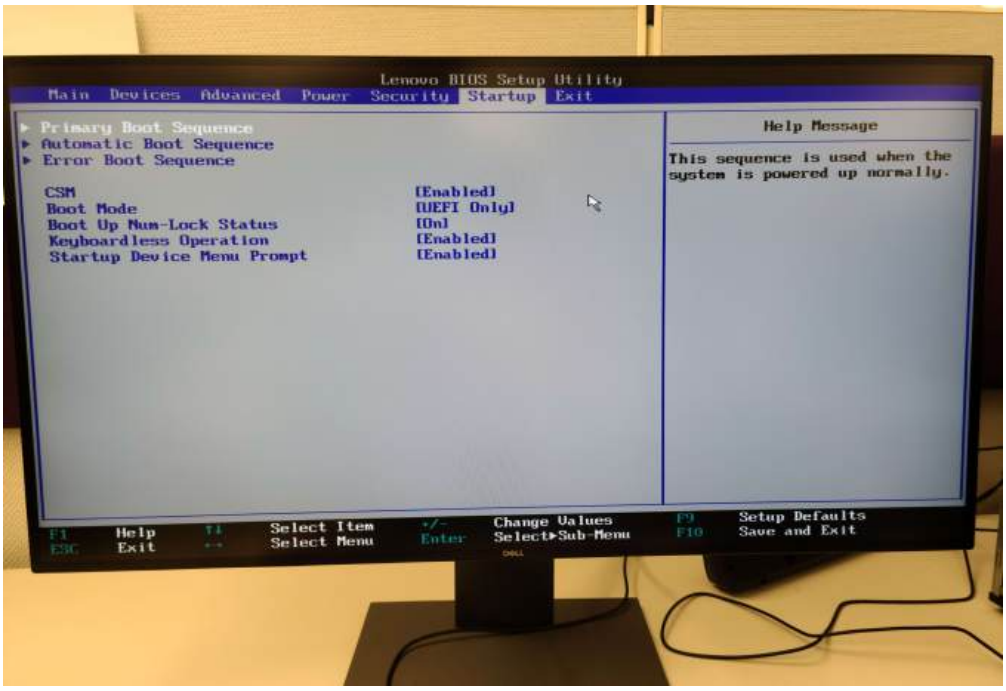


Figure 62: BIOS - Startup.

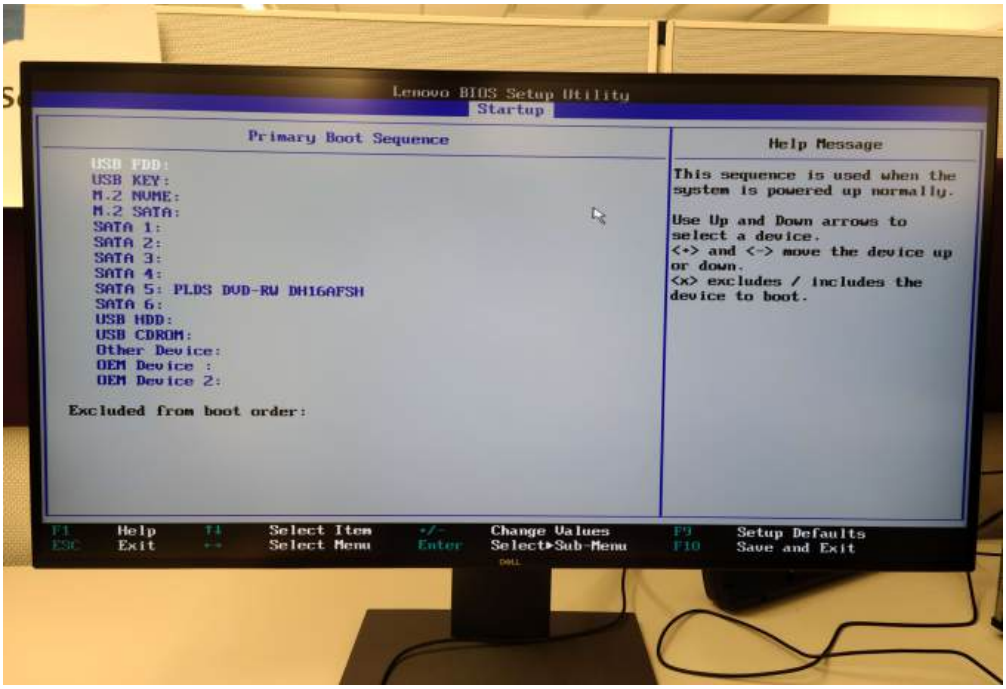


Figure 63: BIOS - Startup - Primary Root Sequence.

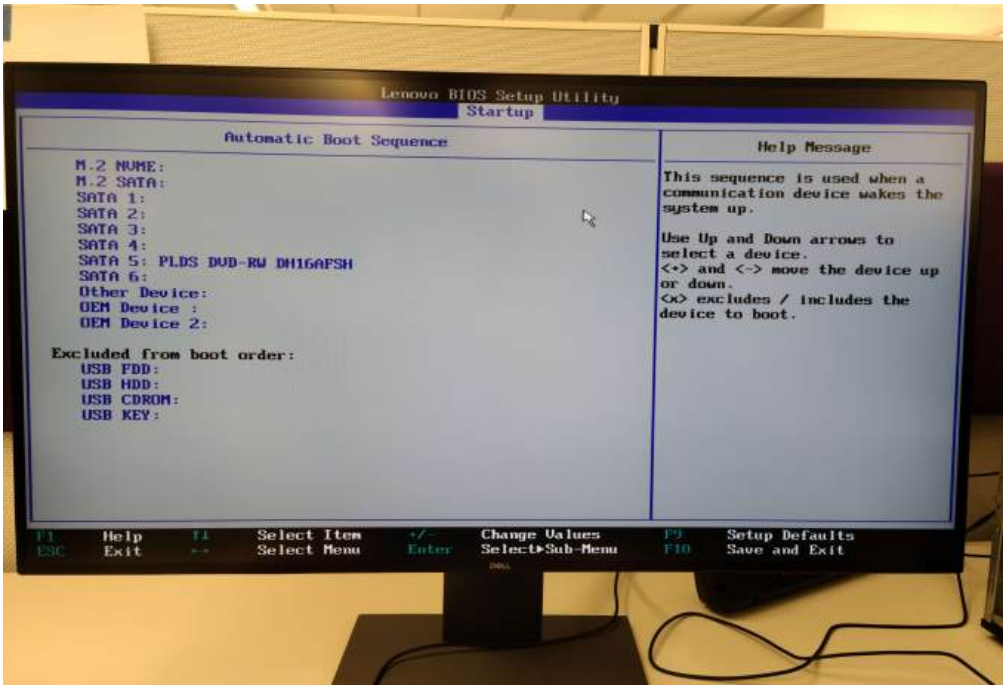


Figure 64: BIOS - Startup - Automatic Root Sequence.

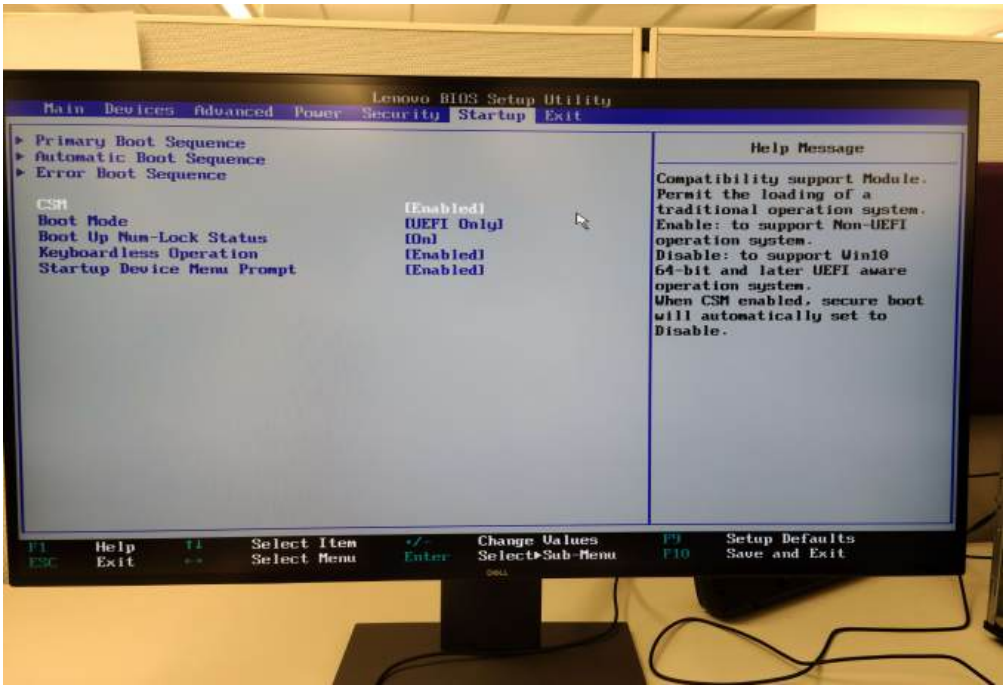


Figure 65: BIOS - Startup - CSM Enabled.

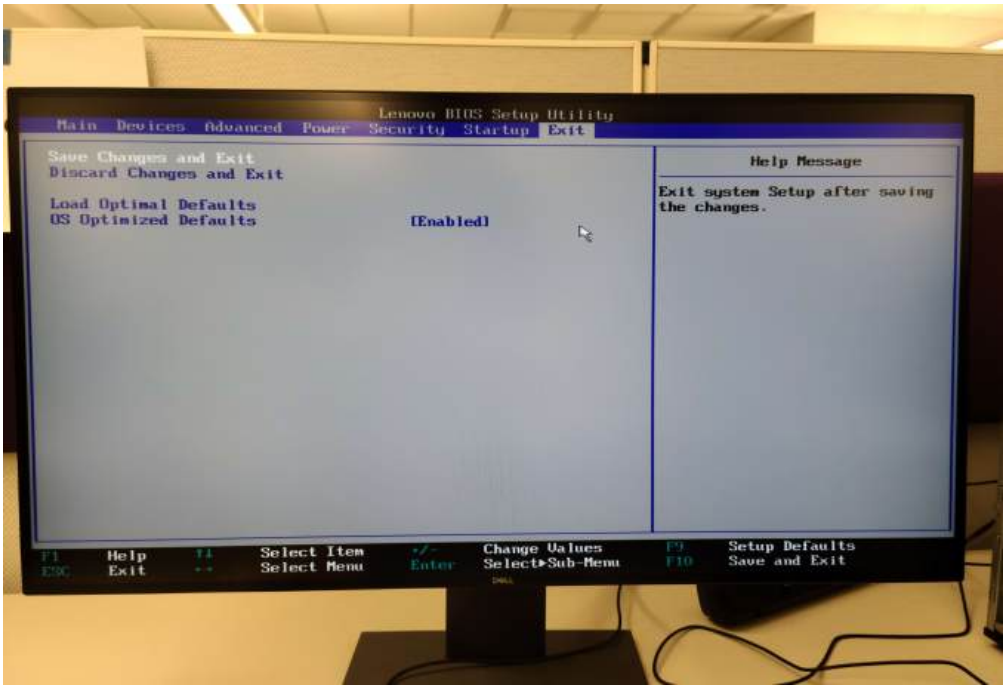


Figure 66: BIOS - Exit.

3.3.3 OSINT

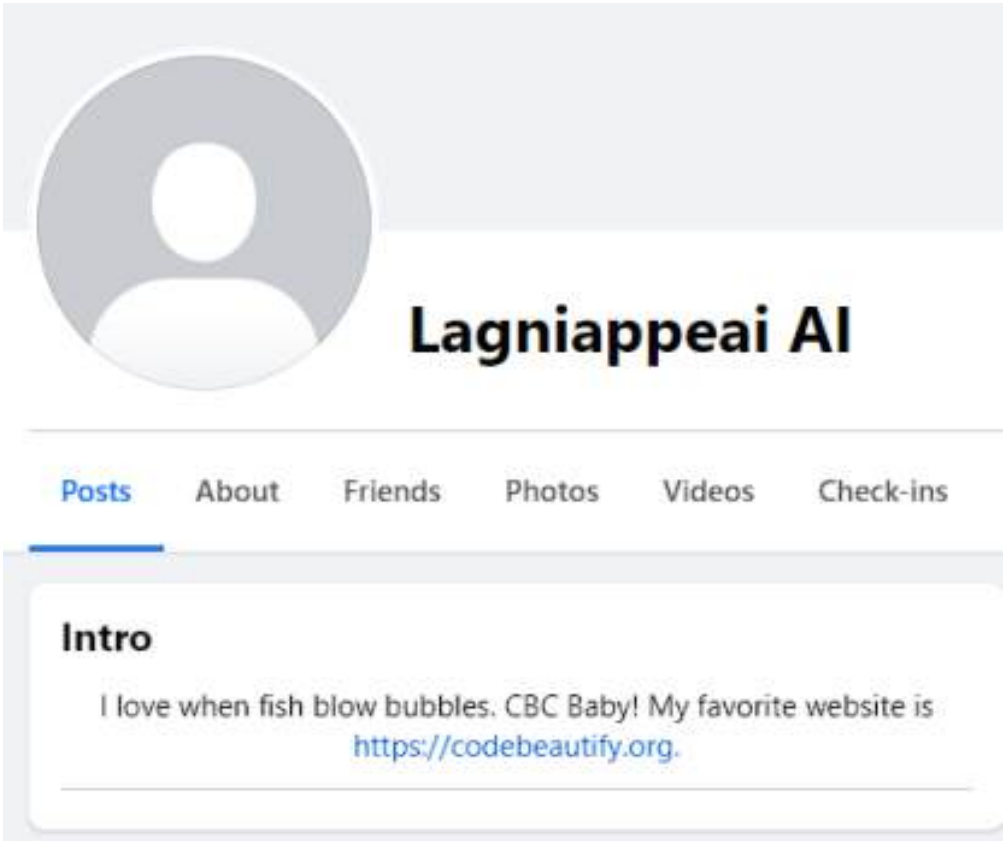


Figure 67: The Facebook account of the suspect with the description.

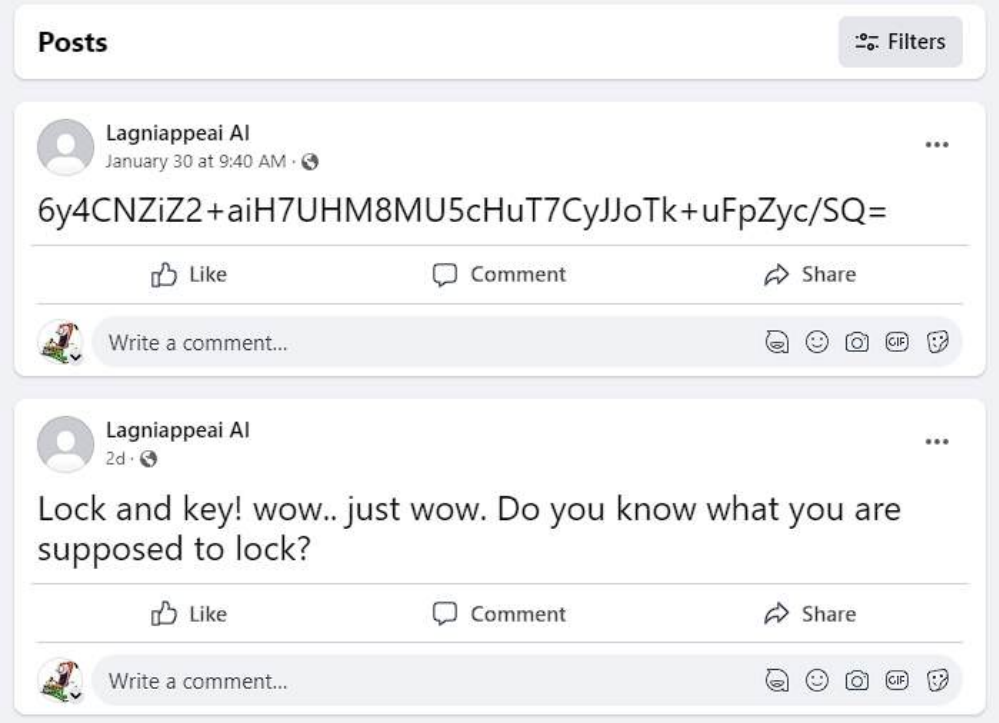


Figure 68: Posts made by the account of the suspect.

Figure 69: Posts made by the account of the suspect.

Figure 70: Decryption of code performed using the CodeBeautify website.

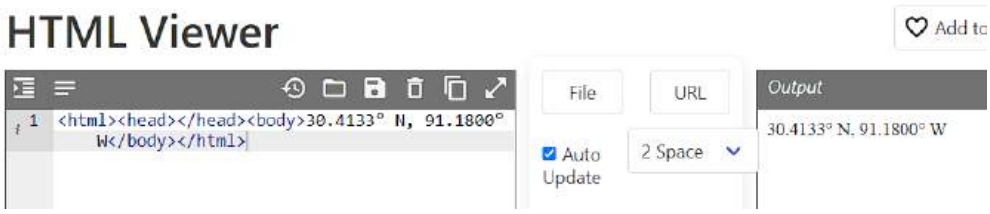


Figure 71: Viewing of decrypted code on the CodeBeautify website.

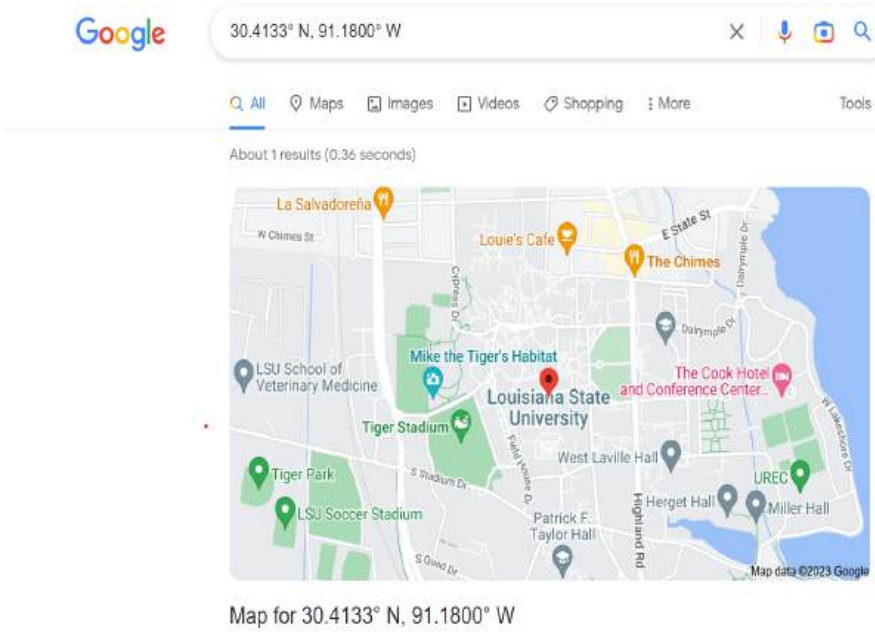


Figure 72: Location of the suspect.

3.3.4 Evidence

Figure 73: Overview of all gathered evidence from the case.

Figure 74: Overview of digital evidence of case.

3.3.5 Close out

Figure 75: Close out of the crime scene.

Figure 76: Image of anti-tampering tape on the computer.

4 Problem Solving and Troubleshooting

Problem 1: Struggled with opening up the computer case.
Solution 1: Instructed by Clinton Walker to press the side panel button to allow the release of the side panel.
Alternative Solution: None

Problem 2: The computer was powered off, so investigators could not open the CD tray to check for a CD.
Solution 2: Used a paper clip that was found on the desk to open the CD tray while the system was powered off.
Alternative Solution: None

Problem 3: Ran "CHJpbnRlcg==" through a base64 decrypter. The result was "rinter".
Solution 3: Was instructed by Dr.Ibrahim Baggili to run "cHJpbnRlcg==" and the result was "printer".
Alternative Solution: None

Problem 4: The BIOS was password protected. The assumed password of "printer" did not work.
Solution 4: Used "lagniappe" and succeeded. This password was found inside the computer.
Alternative Solution: None

Problem 5: Mistook the suspect's name to be "AL Langniappe" and had difficulty finding the suspect's Facebook page.
Solution 5: Dr.Ibrahim Baggili corrected it was "AI Langniappe" instead.
Alternative Solution: None

Problem 6: Difficulty finding out where AI Lagniappe was physically located.
Solution 6: Dr.Ibrahim Baggili gave multiple hints to help with finding the suspect's location.
Alternative Solution: More time.

5 Conclusion and Recommendations

In completing this exercise, investigators have learned the correct methods of bagging and tagging all evidence within a crime scene. The standards of a crime scene investigation are high, as evidence can be found anywhere, and failure to thoroughly search the scene properly can have severe consequences. For instance, an improper search of a computer could leave a destruction disk within the optical drive, potentially wiping major evidence for the case from the computer, in addition to other important clues such as passwords and devices that would be useful in court. An investigator must consider every part of the scene, even pieces that seemingly have no bearing as evidence.

Investigators should make thorough documentation and perform a proper inspection of the crime scene, recording every step of the investigation to make sure nothing is left unchecked. Failure to find evidence and clues that might be hidden in a clear view of the scene could lead to a faulty investigation, so each step should be taken with a forensic approach. If an investigator were to ignore these steps, it could cost identifying a potential suspect. All guidelines, policies, and other such instructions should be respected by the investigators and followed for a fair and just investigation.

6 References

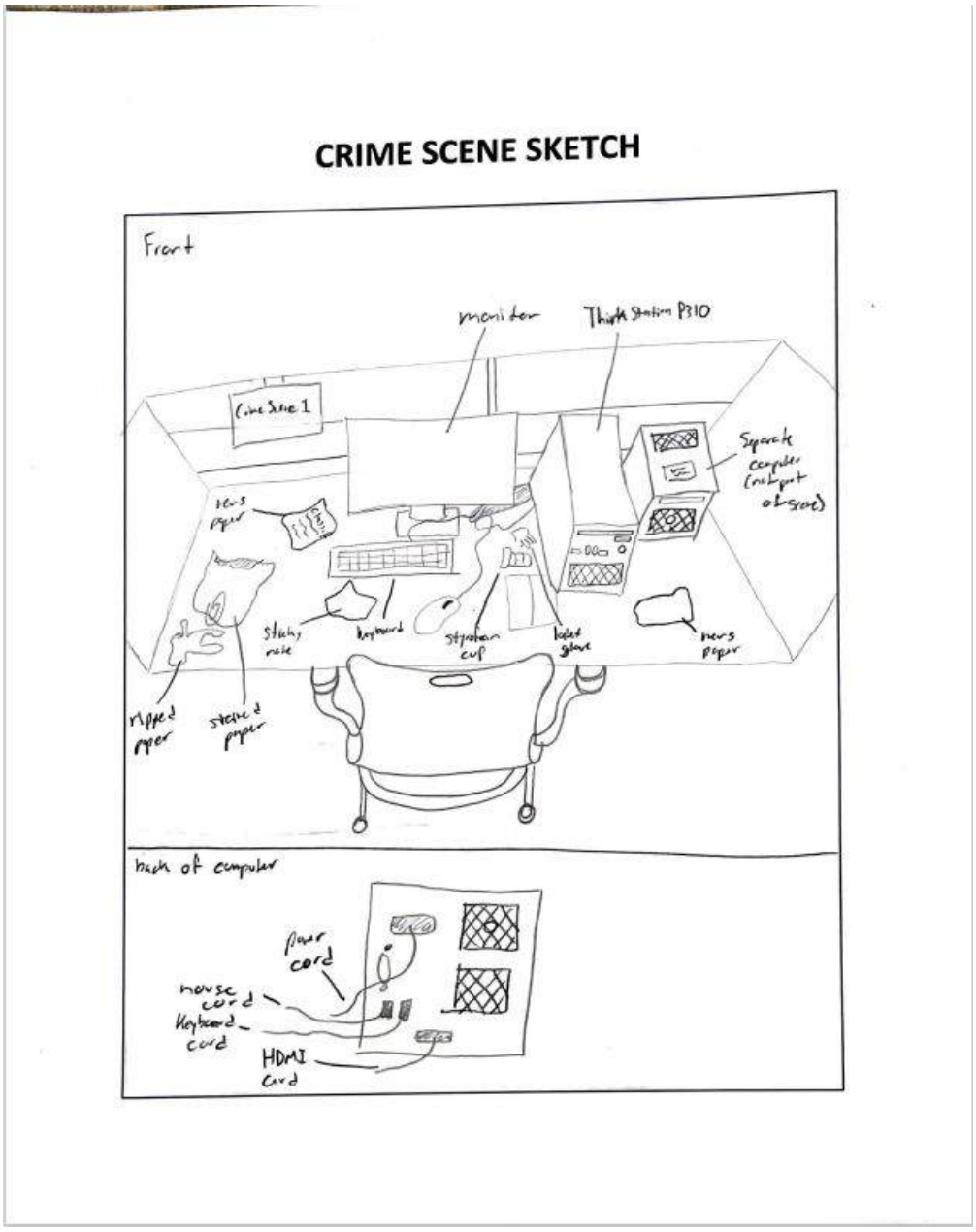
References

[1] Balon, Stabile, White(2016) Lab 1 - Bag & Tag[PDF Document],Retrieved From https://moodle.lsu.edu/pluginfile.php/2025653/mod_resource/content/1/lab1-bag-and-tag.pdf

[2] Baggili (2023) Bag & Tag: Search & Seizure[Lecture Slides],Retrieved From https://moodle.lsu.edu/pluginfile.php/2025640/mod_resource/content/1/LSU_2.1%20Bag%20%20Tag.pdf

Appendices

A Appendix A: Forms



COMPUTER SYSTEM DATA GATHERING FORM

DATE	TIME	ORGANIZATION
January 31, 2022	12:50	Group 8

EXAMINER NAME(S)
Alejandro Marin Avellaneda, Christopher Bowers, George Hendrick, Sachmen Park, Terrence Scott

SYSTEM INFORMATION	
System Manufacturer:	ThinkStation
System Serial Number:	MJØ4V22T
System Name:	N/A
System Model Number:	P31Ø
Bios Date/Time:	13:54:29, 01/31/2023
Other Identifying Data:	System UUID: 4E729B1C-FCC5-E611-9130-4CCC6A7FAF65

LABEL NUMBER	CONNECTION TYPE	PERIPHERAL
1	C13 - Power cord	power
2	HDMI	monitor connection
3	USB	Keyboard
4	USB	mouse

Case #: 1 Officer: Alejandro Mark Arellano

Location: PFT 2341

	DATE	TIME	ACTION TAKEN / INVESTIGATIVE LEADS
1.	01/31/2023	12:15	arrived at crime scene, put on safety equipment
2.	01/31/2023	12:16	took photos of crime scene, computer off but plugged in
3.	01/31/2023	12:18	unplugged power cord from computer
4.	01/31/2023	12:21	two sticky notes removed from newspaper
5.	01/31/2023	12:23	bagged newspaper
6.	01/31/2023	12:27	bagged stated piece of paper
7.	01/31/2023	12:28	opened up ripped piece of paper, writing inside, bagged
8.	01/31/2023	12:30	moved cup, gloves, napkin from Crime scene
9.	01/31/2023	12:31	bagged cup, gloves, napkin
10.	01/31/2023	12:33	moved chair, examined bottom of desk, given permission to open system
11.	01/31/2023	12:34	computer opened up, pictures taken of internals
12.	01/31/2023	12:39	Power/SATA cable disconnected from hard drive, hard drive removed
13.	01/31/2023	12:40	hard drive removed from scene, bagged harddrive
14.	01/31/2023	12:41	Opened CD tray, found CD in CD tray
15.	01/31/2023	12:42	removed CD, bagged CD
16.	01/31/2023	12:45	Keyboard, mouse, monitor flipped over, sticky note found, USB found underneath
17.	01/31/2023	12:46	Veracrypt decryption used on message on sticky note
18.	01/31/2023	12:47	permission given to turn on system, turned on, failed to open BIOS
19.	01/31/2023	12:48	computer turned off and on again
20.	01/31/2023	12:49	"Arrest" entered as wrong password, "keyboardcat" entered as right password
21.	01/31/2023	12:50	Documented BIOS settings
22.	01/31/2023	12:53	went to printer and found phone number
23.	01/31/2023	12:55	permission given to call phone number
24.	01/31/2023	12:57	bagged USB and sticky notes
25.	01/31/2023	13:00	conducted research with evidence found
26.			
27.			
28.			
29.			
30.			
31.			
32.			
33.			
34.			
35.			
36.			
37.			
38.			
39.			
40.			

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 / 1		01/31/2023
2.			
3.			
4.			
5.			
6.			
7.			
8.			

Evaluate the condition of the computer:

- ☑ Is the computer on or off? off
- ☐ If the computer is on, what is it doing? (If on, there is a good chance it might be tied into a bulletin board, Internet site, word-processing program with evidence, etc. Do not shut off before examining these possibilities.)
- ☑ Determine if the computer is connected to other computers by network or by modem.
- ☑ Consider all above conditions and others to determine if the computer should be turned off or left running for a period of time.

Photograph the computer:

- ☑ Photograph the screen.
- ☑ Photograph the front and back of the computer.
- ☑ Photograph the cables.
- ☑ Photograph attached hardware.
- ☑ Take pictures of anything that might be of value or used for evidence (for example: the hidden location of CDs, printed materials, hard drives and other hardware).

Additional remarks:

- ☑ Sketch the scene.
- ☑ Search everywhere.
- ☑ Begin with the computer and work your way outward, to include trash, etc.
- ☑ Seize all printouts, manuals, and examine any notebooks or notes for relevant material (passwords, security access, etc.)
- ☑ Look for passwords on sticky notes around the monitor, under lamps, inside desks, inside covers of computer manuals.
- ☑ Look for evidence of computer system ownership.
- ☑ Mark and tag all cables and hardware.
- ☑ Use tags / stick-on labels to ensure return of the computer to its original configuration.
- ☑ Prepare the computer for transport.