Introduction to Cyber Forensics Lab Grading Sheet

Project: Lab 1: Bag & Tag

Member Name: Pottolla Vinusha Goud
Member Name: Martha Masunda
Member Name: Boinapelly Akshith Rao
Member Name: Lashmidhar Yadlapalli
Member Name:

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

Table of Contents

1.0 Executive Summary

This lab report describes and shows the steps taken to investigate a crime scene that was in Buckman Hall, 233C lab. The exercise was conducted on the 09 September 2024 by a team of 5 team members. The Forensics Investigators received a search warrant for the property of a chief systems developer who had been reported missing; a search and seize exercise was to be carried out to discover evidence that would lead to discovering his whereabouts.

While at the crime scene, the whole team wore gloves and the surroundings were observed, pictures of what it looks like was taken and investigation commenced by disconnecting wires and cables attached to the computers and other electronics found at the scene, after which investigation commenced.

The forensic Investigators employed the use of smartphones to take pictures throughout the investigation. Several pictures of the crime scene were taken before anything was touched. The investigators also carefully logged all the items collected in a data gathering form and bagged the items found according to their sensitivity.

After collecting, bagging and tagging all the evidence found, the team proceeded to decipher the ciphered texts found among the evidence while also attempting to gain access into the personal computer found at the residence. The deciphered ciphertext led the team to the address where the abductee was being held. The team successfully accessed the BIOS of the computer where the BIOS number and date of the computer was retrieved.

2.0 Apparatus

Table 1

List of hardware and software used at the crime scene.

ITEM/PART	MODEL NUMBER	USAGE
Blue tagging tap	N/A	For tagging the bags
iPhone SE 2nd Generation	MMX73LL/A	Camera
Faraday Bag	N/A	Bag of electronic evidence
Envelope Bags	N/A	Bag of evidence
Gloves	N/A	Use for the crime scene

2.1 Computer System Data Gathering Form

DATE	TIME	ORGANIZATION
09/09/2024	7.30 pm	Group 5

1. Martha Masunda
2. Pottolla Vinusha Goud
3. Boinapelly Akshith Rao
4. Lashmidhar Yadlapalli
5.

SYSTEM INFORMATION	
System Manufacturer:	Dell Inc
System Serial Number:	CX5NGH1
System Name:	Dell Optiplex 755
System Model Number:	DCCY
Bios Date/Time:	A22 (06/11/12)
Other Identifying Data:	• Intel Core 2 Duo Processor • Processor clock Speed = 2.33GHz • Memory = 4GB

LABEL NUMBER	CONNECTION TYPE	PERIPHERAL
616448923	USB Wired Connection	Central Processing Unit
CX5NGH1	Serial Connection Cable	Monitor
CX5NGH1	USB Wired Connection	Mobile Phone
CN-ORKRON-LO3000-057-OUP4-A03	USB Wired Connection	Central Processing Unit

3.0 Laboratory Procedures

Table 2: The log of all actions taken and the time they occurred.

	DATE	TIME	ACTION TAKEN / INVESTIGATIVE LEADS
1.	09/09/2024	07:30 pm	Arrived at the crime scene.
2.	09/09/2024	07:40 pm	Took pictures of the scene
3.	09/09/2024	07:47 pm	Disconnected all cables and power cables from the computer.
4.	09/09/2024	07:50 pm	Started collecting physical evidence found at the scene.
5.	09/09/2024	08:00 pm	Discovered and collected a flash-drive from the table bagged and tagged it.
6.	09/09/2024	08:10 pm	Collected, bagged and tagged the flip phone found connected to the computer after disconnecting it.
7.	09/09/2024	08:15 pm	No memory card was found but the empty case of the memory card was bagged and tagged.
8.	09/09/2024	08:25 pm	Bagged and tagged a family photograph that had a woman's face drawn over with a love shape.
9.	09/09/2024	08:38 pm	Bagged and tagged the flight itinerary found.
10.	09/09/2024	08:40 pm	Bagged and tagged the CD case which contained inside of it a paper with a ciphertext written on it. The paper was bagged and tagged.
11.	09/09/2024	08:43 pm	Opened the DVD player compartment located in the Central Processing Unit with a paper clip found in the blue plastic cup. A pink piece of paper with **"G0d"** written on it was found in the compartment. This was used as the clue to the password to access the BIOS.
12.	09/09/2024	08:55 pm	Opened the Central Processing Unit, found a paper with a password plastered to the CPU cover, which was bagged and tagged.
13.	09/09/2024	08:57 pm	Found 2 sticky notes inside the Central Processing Unit, that had a password and a cipher text, same as the first ciphertext found attached to the hard drive. These were bagged and tagged.
14.	09/09/2024	09:00 pm	Re-attached all the cables to the computer.
15.	09/09/2024	09:05pm	Connected the phone to another computer to look for passwords for the BIOS.
16.	09/09/2024	09:08 pm	Used the other computer to Decipher the ciphertext, which led to a printer that had paper plastered to its back. The paper contained the address of where the victim was being held.
17.	09/09/2024	09:22 pm	Accessed the BIOS setting of the computer, where the BIOS number was retrieved and date of the computer. The BIOS was accessed using one of the passwords (**R00t)** found during evidence gathering.

3.2 Procedure

1. Crime Scene Examination:

The crime scene was carefully examined, and photographs were taken to document the evidence. A detailed sketch of the crime scene was drawn to capture its layout accurately.

2. External Examination of the Computer:

The external components of the computer were inspected for visible evidence. This included noting and documenting any connected devices such as cords, monitors, keyboards, mice, and external hard drives. Any visible evidence, including these components, was carefully recorded.

3. Evidence Collection and Tagging:

During the examination, a cellphone and a wire were identified, bagged, and tagged as evidence. Several pieces of paper were also collected, including one with an image of a family, featuring a heart on the woman in the center and the words **"WE'RE ALL #1"** written on it. This paper was located beneath the monitor and on top of the computer. It was bagged and tagged accordingly. Other papers collected included a flight itinerary dated July 23 and July 24, 2021. These documents were also appropriately bagged and tagged.

4. Additional Discoveries Around the Computer:

Further investigation around the computer revealed a picture frame with an upside-down photograph of a man. Upon opening the frame, nothing was found inside, but the frame itself was bagged and tagged as evidence. A DVD case with a movie titled Just Wright was discovered nearby. Inside the case, a note containing the text **"B-hind cHJpbnRlcg=="** was found, bagged, and tagged.

5. Cup and Hidden Evidence:

A cup filled with pens was examined, revealing a receipt from Walmart at the bottom, along with a bent paperclip and an external thumb drive wrapped inside. The flash drive, cup, and receipt were bagged and tagged as evidence. The bent paperclip was then used to open the computer's

DVD drive, revealing a note that read "G0d." This note was bagged and tagged as well.

6. CPU Examination:

The CPU was disconnected from the monitor and power source and then physically opened. Inside, a note was found attached, with the text **"StrongP@ssword123."** A thorough examination of the CPU followed during which the hard drive was removed. Two additional notes were found stuck together inside the hard drive compartment, one repeating the text **"G0d"** and the other containing **"B-hind cHJpbnRlcg==".** These notes were collected for further analysis, particularly for password cracking the System BIOS.

7. Password Cracking and Computer Access:

The computer was reassembled, and all wires were reconnected. Upon powering the system, the booting process was initiated, and several attempts to crack the system password were made. The passwords **"StrongP@ssword123," "R00ts," and "G0d"** were tried unsuccessfully. Eventually, **"Root"** was used and provided successful access to the system.

8. Deciphering the Encrypted Message:

The encrypted message **"B-hind cHJpbnRlcg=="** was decoded on a separate computer. The deciphered message read **"printer,"** leading investigators to examine the printer. Upon inspection, a note containing the name and address of the location where the missing person was being held was discovered.

3.3 Description of Evidence

Evidence Identification and Chain of Custody	
Date:	09/09/2024
Received/Seized From:	
Received/Seized By:	Group 5
Reason Obtained:	Analysis of Evidence to find the missing person
Location Obtained:	Buckman Hall, University of New Haven, 300 Boston Post Rd, CT 06516

4

Description of Evidence (Manufacturer, Model #, S/N, condition, marks/scratches, etc.)
1. Family photograph with a heart on a girl's face. Six people in photograph: 3 white male and 3 white female.
2. Framed photograph of a white man wearing lipstick, carrying a brown female handbag, wearing a pair of glasses, a black t-shirt and has blue painted fingernails. The frame was placed upside down.
3. A flash-drive was discovered on top of the desk near the photograph.
4. Flight Itinerary for a Jonathan Angel Iniesta: flight number 0027, Departure: JFK, Reservation ID: KLM887J926.
5. One sticky note was found in a movie CD case with ***"B-hind cHJpbnRIcg=="*** written on it.
6. Two sticky notes at the bottom of the hard drive, inside the computer. The contents of the sticky note are: G***0d*** and ***R00ts: b-hind cHJpbnRIcg= =*** respectively.
7. One sticky note was found inside the CPU when it was opened. The sticky note was plastered on the inside of the CPU cover. The sticky note contained a suspected password ***"SecurePassword123!"***
8. A roughly cut pink paper with ***"G0d"*** written on it was found inside the DVD drive in the CPU.
9. Paper clips, a Walmart receipts and 11 pens and a plastic fork were found in a blue disposable cup which was placed on the desk.

4.0 Problem Solving / Troubleshooting

Problem 1: The computer was on.

Solution 1: The computer was turned off and cables removed.

Alternative Solution: None

Problem 2: The computer was locked.

Solution 2: Found the password "**Root**" in the disk tray to unlock the computer.

Alternative Solution: None

Problem 3: An encrypted message was found on a sticky-note in the "**Just Wright**" movie box.

Solution 3: Decrypted the message to "**printer"**, which was encoded in the Base64 format, and found a sticky-note with the address of where the victim was being held.

Alternative Solution: None

Problem 4: There was no mouse to navigate the computer.

Solution 4: Used the Keyboard to navigate.

Alternative Solution: None

Problem 5: The computer was not able to load the OS.

Solution 5: None

5.0 Conclusion and Recommendation

Conclusion:

The lab exercise successfully demonstrated the correct procedures for entering a crime scene, as well as properly bagging and labeling the evidence found within. It also highlighted the necessary steps for locating and preserving evidence, including those that might be deliberately hidden by a perpetrator. The investigation emphasized the importance of thoroughness, ensuring that evidence is sought not only in obvious locations but also in areas where a criminal may have intentionally concealed it. The documentation process, aimed at reconstructing the crime scene, was shown to be crucial in producing a detailed report. Such precision is essential for presenting clear, accurate information if the case proceeds to court. Proper documentation ensures that all evidence is recorded and its location within the scene clearly specified, allowing for effective use in legal proceedings.

Recommendations:

- Investigators should conduct methodical searches, considering both obvious and less apparent locations for evidence.
- Documentation should be detailed, accurate, and include comprehensive notes on the placement and condition of all evidence.
- Careful attention to detail during the investigation and documentation process is vital to maintaining credibility and trust with legal authorities, such as a judge or jury.
- Proper labeling and preservation of evidence should always be maintained to avoid contamination or misinterpretation during legal proceedings

6.0 References

- Base64 Decode and Encode (n.d.). *Base64 Decoding of "cHJpbnRlcg=="*. Retrieved September 20, 2023, from https://www.base64decode.org/dec/cHJpbnRlcg==/
- By Professor Mathew Jackson : Preparation for Crime Scene Investigations Modules. https://canvas.newhaven.edu/courses/23551/modules

7.0 Crime Scene Pictures and Evidence

Figure 1: Pictures of the crime scene upon arrival

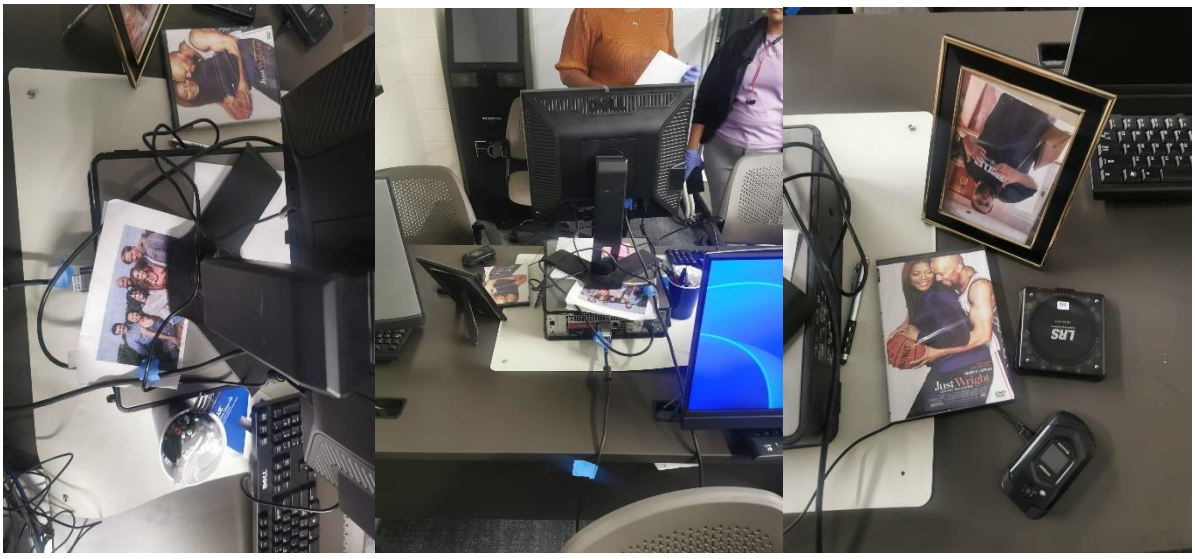


Figure 2: This shows some of the evidence found on the scene (blue plastic cup)

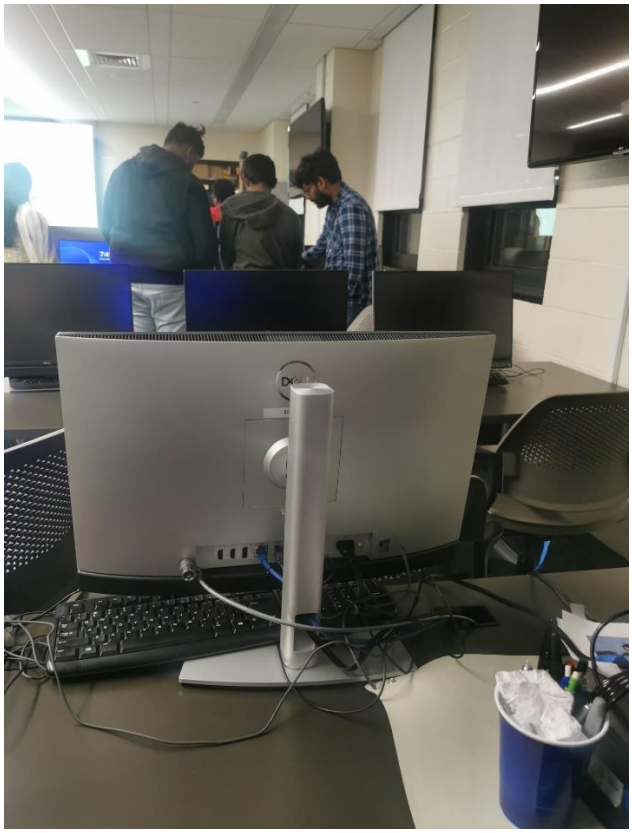


Figure 3: Flight Itinerary found at the crime scene.

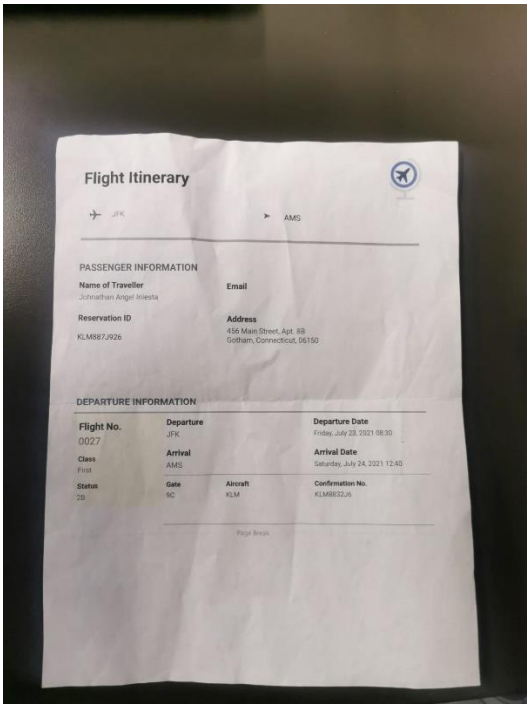


Figure 4: The Central Processing Unit

Figure 5: Picture of the monitor before turning it off

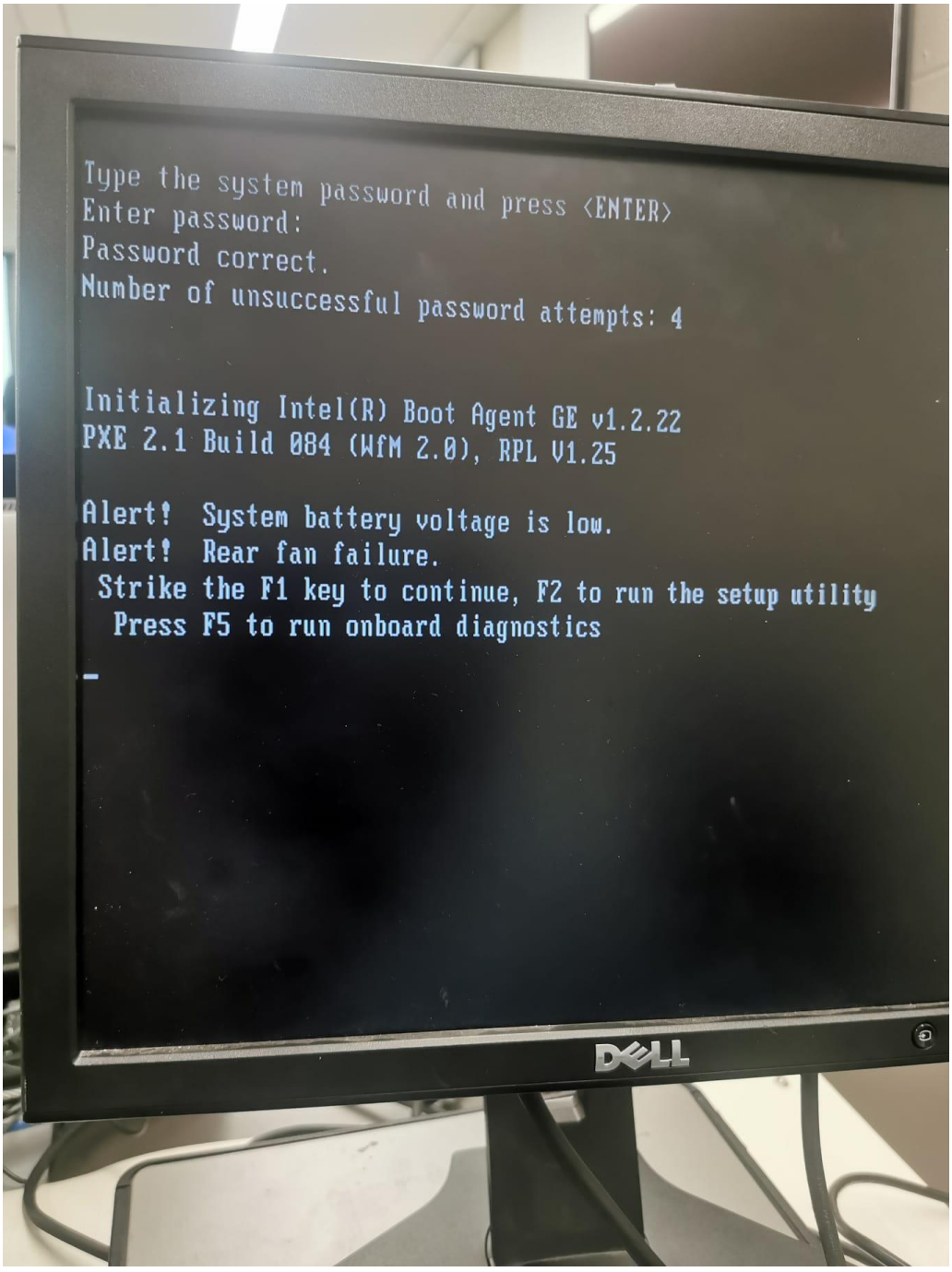


Figure 6: Picture of all the cables attached to the computer

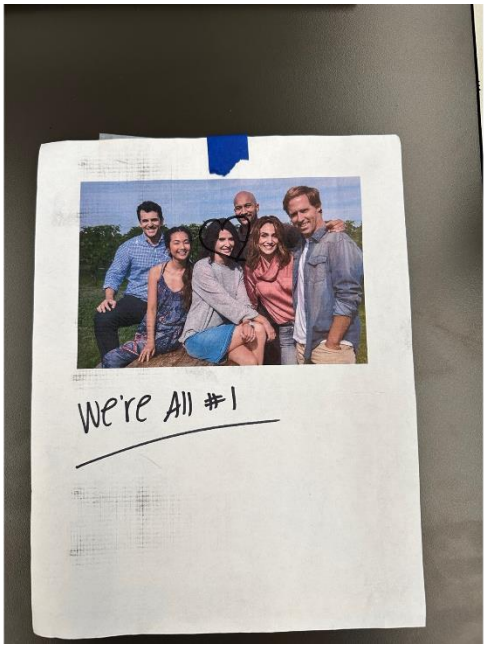


Figure 7.1: Evidence found at crime scene

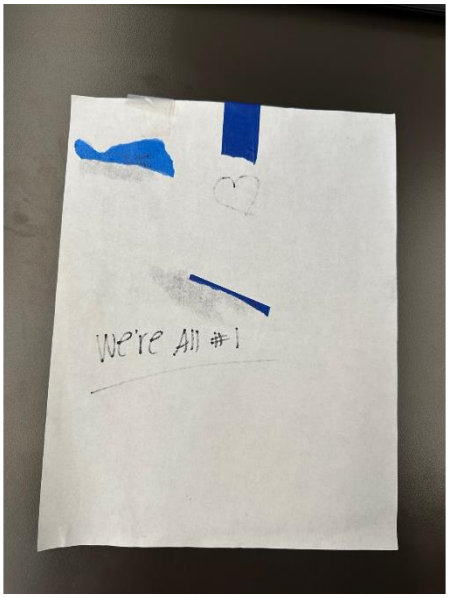
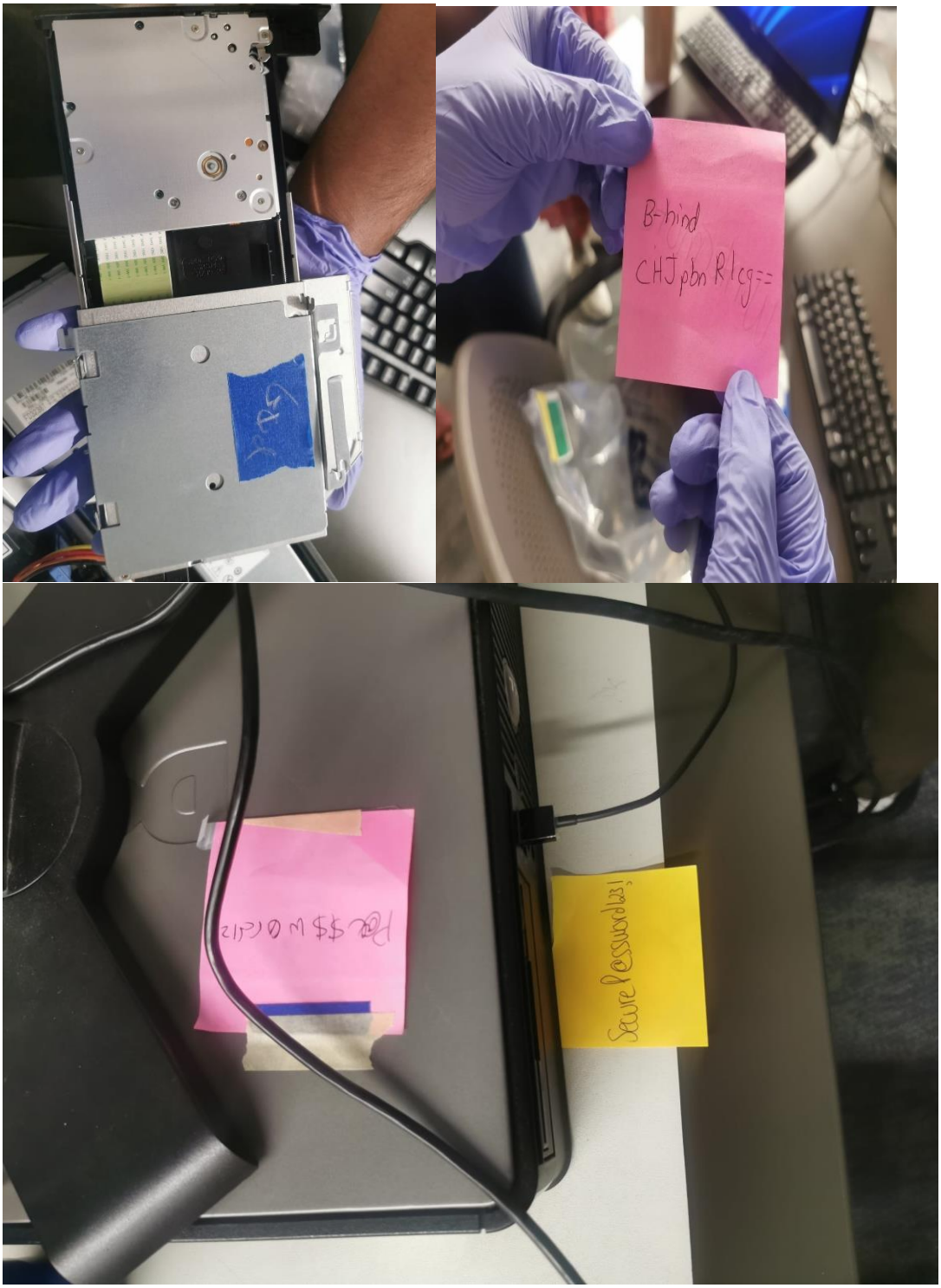
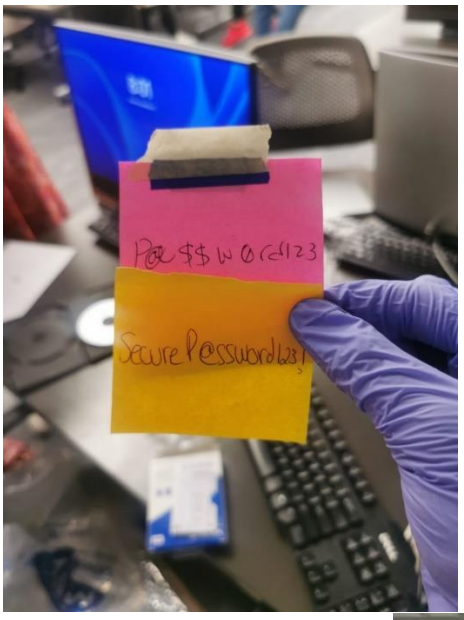


Figure 7.2: Back of the evidence (bagged and tagged)

Figure 8: Pictures of DVD, and evidence of passwords on sticky notes




Secure Password123


WD2500
Moms

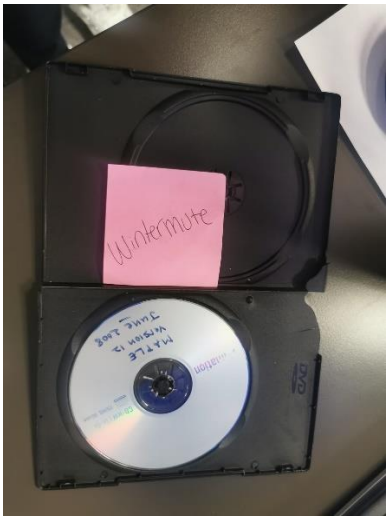

Wintermute

Figure 9: Picture of the opened flip-phone

Figure 10: Picture of the Walmart receipts

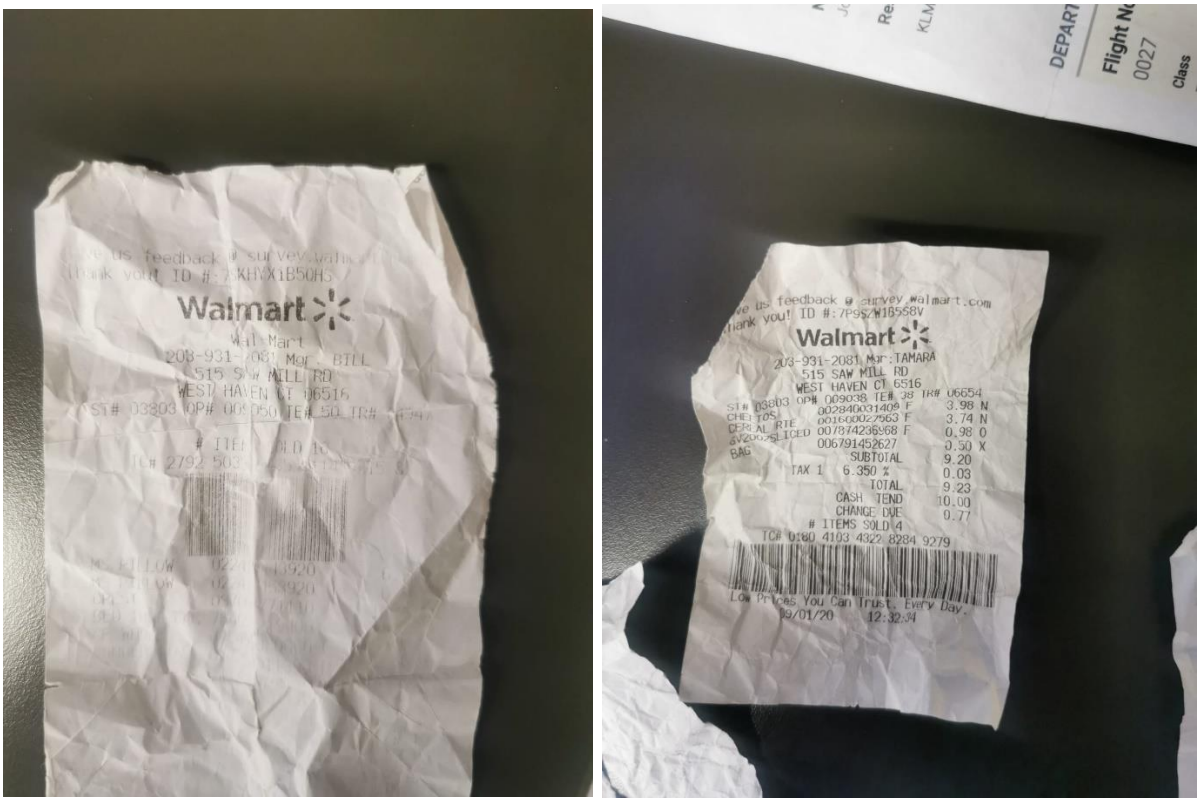


Figure 11: Picture of the personal diary found

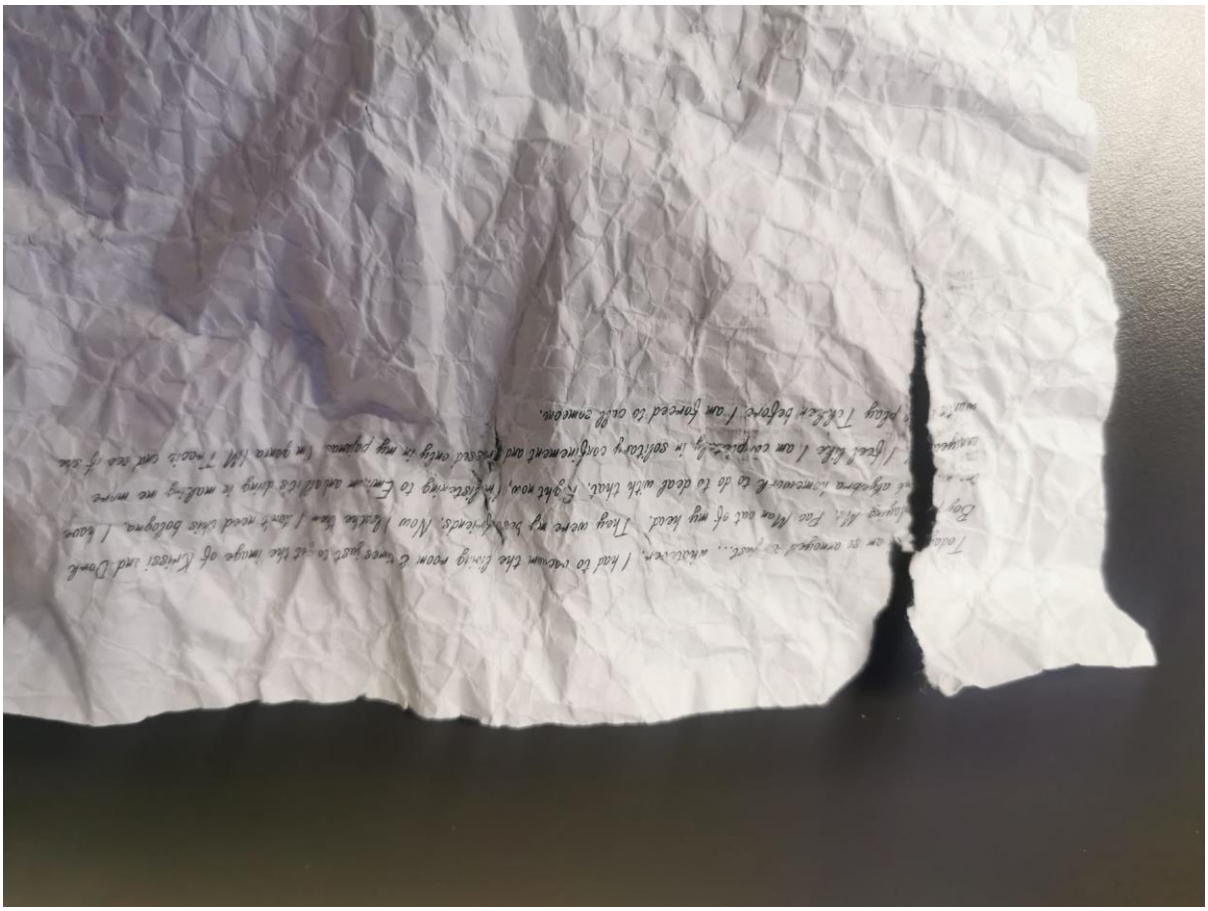


Figure 12: Picture of the pen, plastic-fork and knife found in the blue plastic cup

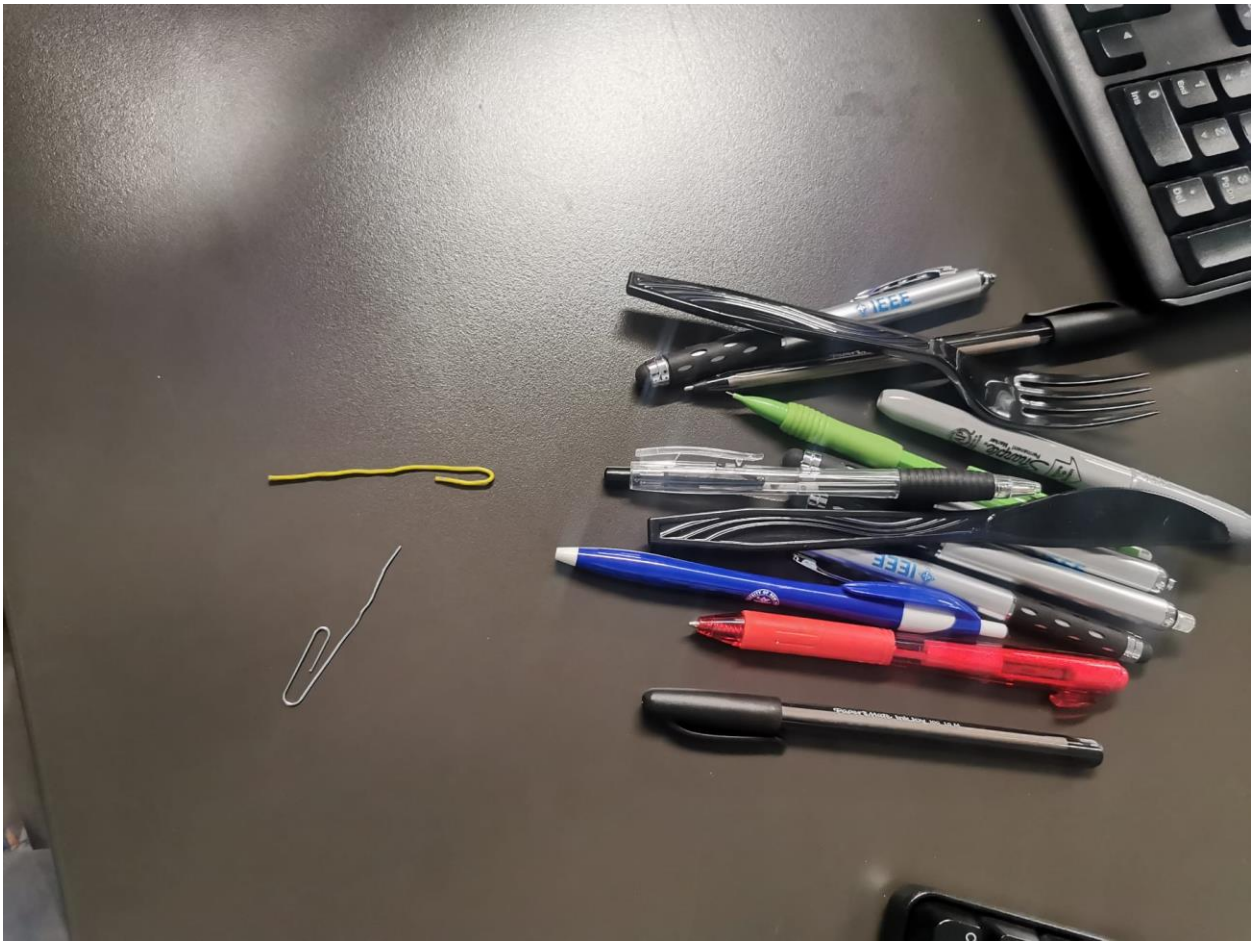


Figure 13: Picture of the opened CPU

Figure 14: Picture of the unknown device and the flip phone

Figure 15:Label containing serial number

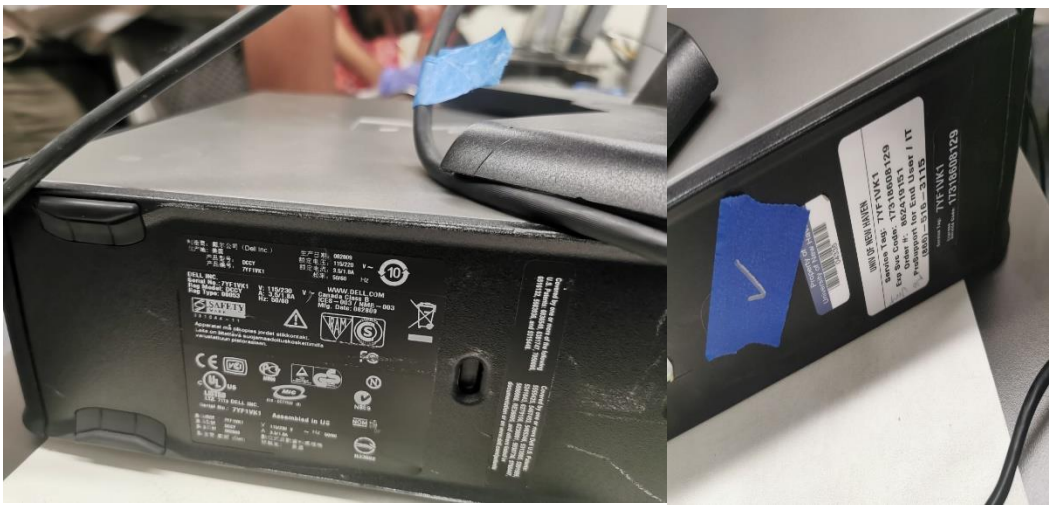
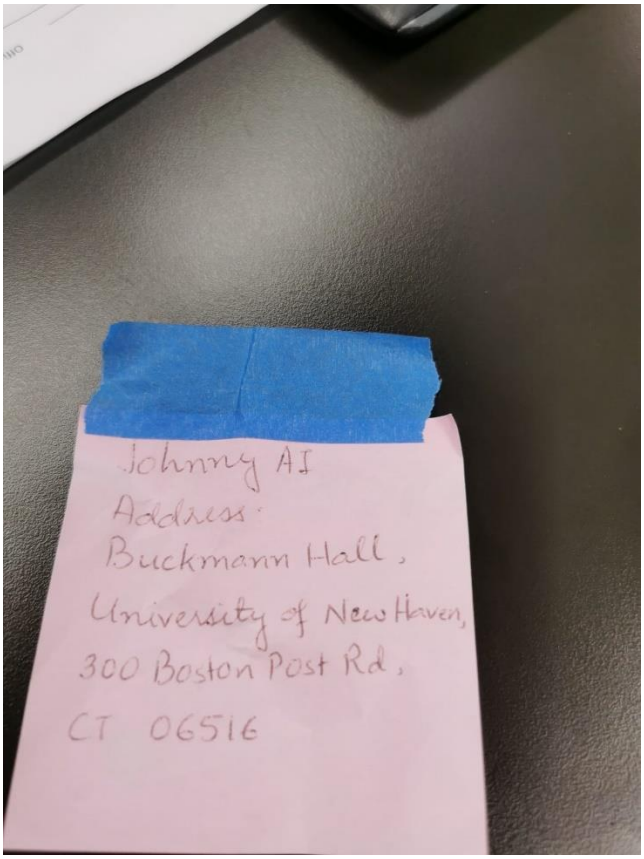


Figure 16: Picture of an address found behind the printer of the location of the missing person.



8.0 Crime Scene Sketch