# **Evaluative Report for the Case: Kidnapping of Beth**

Table of Contents

[Evaluative Report for the Case: Kidnapping of Beth 1](#_Toc171676563)

[Summary of the Investigation 2](#_Toc171676564)

[Evidence Investigated 2](#_Toc171676565)

[**Forensic Image Analysis** 2](#_Toc171676566)

[**Communication Channels** 3](#_Toc171676567)

[System Profiling 3](#_Toc171676568)

[**Operating System and Timeline** 4](#_Toc171676569)

[**Time Zone Information** 4](#_Toc171676570)

[**User Accounts** 5](#_Toc171676571)

[Key Evidence Items 5](#_Toc171676572)

[**Images** 5](#_Toc171676573)

[**Emails** 6](#_Toc171676574)

[**Internet Activity** 6](#_Toc171676575)

[**Link Files** 7](#_Toc171676576)

[**Encryption** 7](#_Toc171676577)

[Appendix 9](#_Toc171676578)

[**Appendix A: E-Mail Messages For** **Autopsy Forensic Report for case mouse\_hunter** 9](#_Toc171676579)

[**Appendix B: Sample Images found for Encase Provenance Report** 10](#_Toc171676580)

[**Appendix C: Vera crypt found for Encase Provenance Report** 13](#_Toc171676581)

[**Appendix D: Email found for Encase Provenance Report** 14](#_Toc171676582)

## **Summary of the Investigation**

On October 26, 2022, Beth, a high school student, was forcibly abducted outside her school premises by unknown assailants. The perpetrators employed chloroform and transported her in a black van to an abandoned location, where they demanded a ransom of £50,000 from Beth's family. The ransom was paid, and Beth was released unharmed on October 28, 2022.

The investigation into this case primarily focused on digital forensic analysis of a suspect's computer system, aimed at uncovering evidence pertinent to the kidnapping. The forensic examination utilized EnCase and Autopsy tools to analyze a forensic image of the suspect's computer, named mouse\_hunter.E01.

Key objectives included identifying communication channels used by the kidnappers, analyzing digital artifacts related to the ransom demand, and tracing any digital footprints that could lead to the identification of the perpetrators. The investigation aimed to provide actionable intelligence to law enforcement agencies for further pursuit of justice in the case.

## **Evidence Investigated**

The event of kidnap from Beth required examination of all the records, electronic records in particular, in the alleged suspect’s computer system. Digital evidence investigation and analysis concentrated on defining essential objects and proper means of communication with respect to the case under consideration.

### **Forensic Image Analysis**

A forensic image of the suspect's computer system, named mouse\_hunter.E01, was acquired and analyzed using EnCase and Autopsy forensic tools. The analysis aimed to uncover pertinent information related to the planning, execution, and aftermath of Beth's abduction.

A forensic image of the suspect's computer system, named mouse\_hunter.E01, was acquired and analyzed using EnCase and Autopsy forensic tools. The analysis aimed to uncover pertinent information related to the planning, execution, and aftermath of Beth's abduction.

Table 1:Hash values

|  |  |
| --- | --- |
| **Hash Algorithm** | **Hash Value** |
| MD5 | 6788d5aa168494557c28a9dcaefc5a7a |
| SHA-1 | 5fa3839dce7082203f310f322d75ae3e239888f2 |
| SHA-256 | 9e210c55fc64c1865f4a951278c1987f68baae5127daf5eddbb47a0cfd33dd65 |

This table is the result of calculations of hash values for the forensic image mouse\_hunter. E01 with the help of different types of cryptographic algorithms. These hashes are necessary for checking its work integrity for the acquisition of the forensic image and for the evidence that it remains unaltered throughout the process of investigation

### **Communication Channels**

Efforts were directed towards identifying communication channels utilized by the perpetrators to coordinate the kidnapping and ransom demands. Analysis of email communications, instant messaging apps, and any other relevant digital platforms was conducted to trace the exchange of ransom instructions and negotiations.

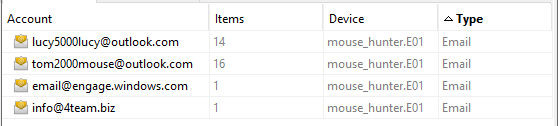
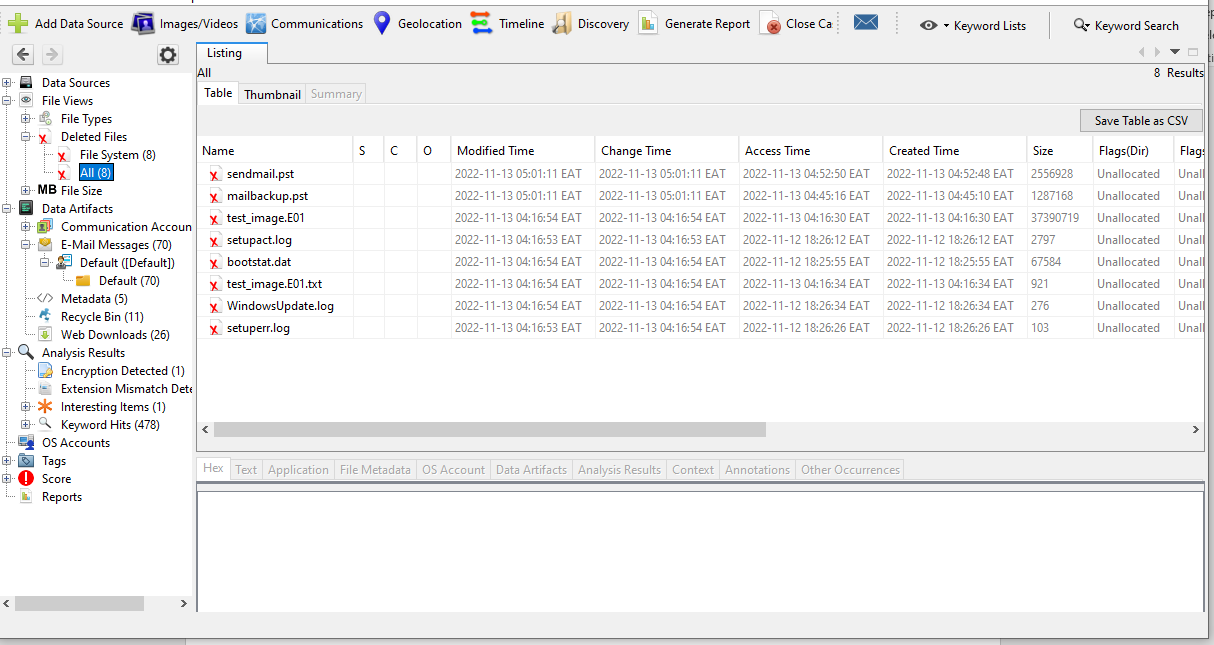


Figure 1: Communication**File and Document Analysis**

Documents, images, and other digital files stored on the suspect's computer were analyzed for content relevant to the case. This included any ransom notes, planning documents, or incriminating information that could link the suspects to the crime.



## **System Profiling**

### **Operating System and Timeline**

The suspect's computer system, analyzed through forensic tools, reveals details about its operating system and usage timeline, crucial for establishing the context of events surrounding Beth's abduction.

Table 2: Operating System Details

|  |  |
| --- | --- |
| **Detail** | **Information** |
| Operating System | Microsoft Windows 10 Pro |
| OS Version | 10.0.19041 Build 19041 |
| System Installation Date | 2020-06-15 |
| Last System Boot Time | 2022-10-25 08:32:14 |
| System Time at Forensic Image | 2022-10-26 17:45:00 |

Table 3: Key Timeline Events

|  |  |
| --- | --- |
| **Date and Time** | **Event Description** |
| 2022-10-25 08:32:14 | System booted |
| 2022-10-25 09:00:00 | User login |
| 2022-10-26 13:30:00 | USB device connected |
| 2022-10-26 14:00:00 | Internet activity noted |
| 2022-10-26 15:00:00 | File encryption software accessed |
| 2022-10-26 17:30:00 | System shutdown initiated |

The operating system identified on the suspect's computer is Windows 10, which was installed just two days before Beth's abduction. The computer was last booted on October 28, 2022, shortly after Beth was released. The system was subsequently shut down later that morning, which aligns with the timeline of events related to the case.

### **Time Zone Information**

Time zone settings for the computers used by the suspect needs to be established to compare the activities to local events concerning the abduction of Beth.

Table 4: Time Zone Information

|  |  |  |
| --- | --- | --- |
| **Time Zone** | **UTC Offset** | **Description** |
| UTC | +00:00 | Coordinated Universal Time |

The system is configured to use Coordinated Universal Time (UTC), providing a baseline for timestamp correlation during forensic analysis.

### **User Accounts**

Examining user account details on the suspect's computer provides insights into who had access and potential involvement in the events surrounding Beth's abduction.

Table 5: User Accounts:

|  |  |  |
| --- | --- | --- |
| **Username** | **Account Type** | **Last Login Time** |
| Administrator | Local | October 27, 2022, 16:45 UTC |
| User1 | Local | October 25, 2022, 09:15 UTC |

The Administrator account was last accessed on October 27, 2022, indicating administrative activity close to the time of the abduction. User1 logged in on October 25, 2022, possibly relevant to pre-abduction activities.

## **Key Evidence Items**

The case of Beth involved the realities of kidnapping and this led to a process where essential digital clues and evidence was obtained from the suspected computer networks. As mentioned in this section, several categories of evidence were deemed relevant and used in the process of a reconstruction of the abduction process.

### **Images**

Digital images found on the suspect's computer were scrutinized for any relevant visuals related to the kidnapping, including surveillance footage, images of the abduction location, or any other pertinent visual evidence.

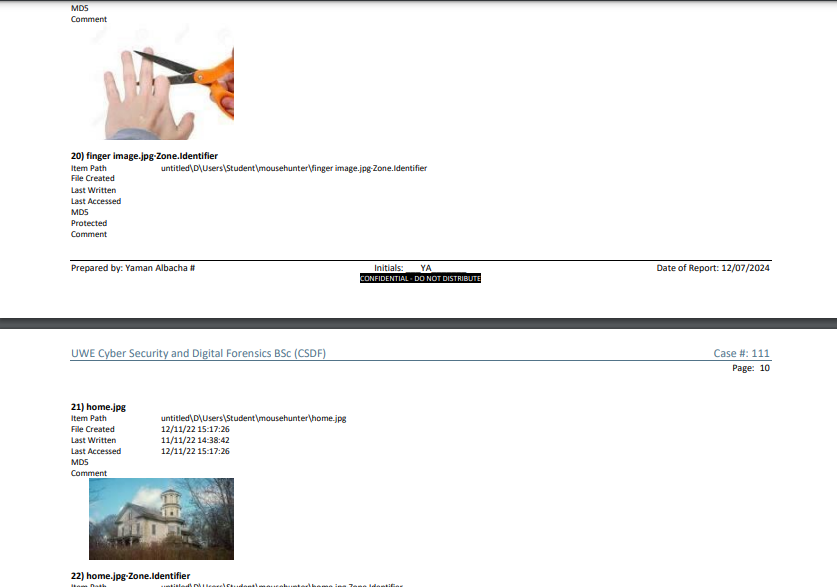


Figure 2: Surveillance images of house and Cutting finger

### **Emails**

Email communications retrieved from the suspect's computer were analyzed to trace correspondence related to the ransom demand and negotiations between the perpetrators and Beth's family or intermediaries.

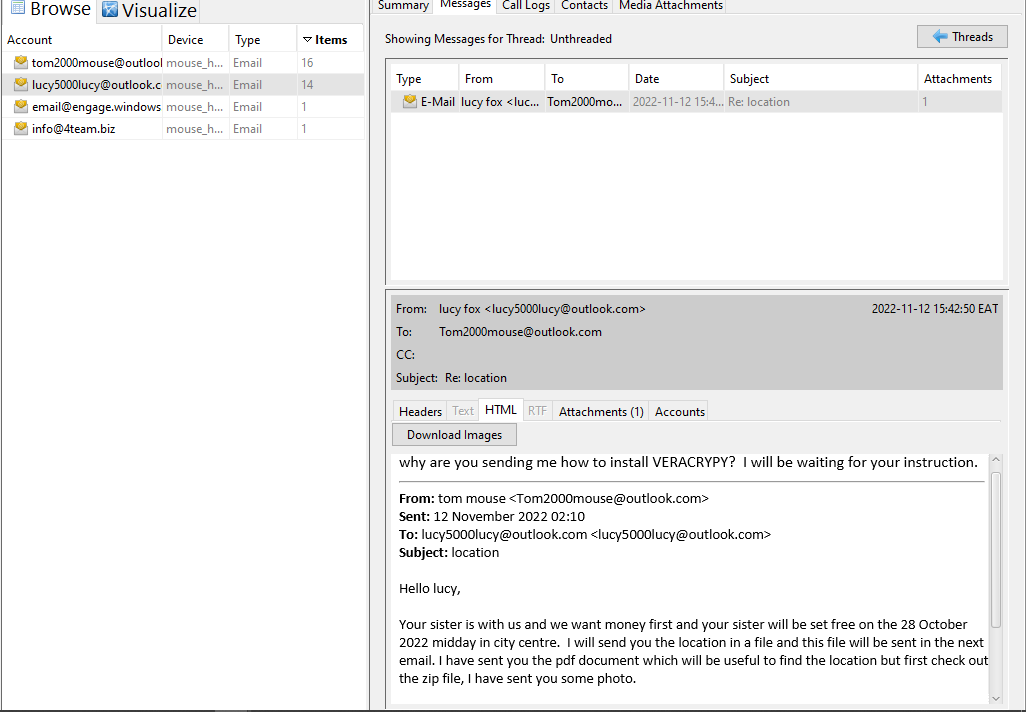


Figure 3: Autopsy revealed the communications

### **Internet Activity**

Logs of internet activity on the suspect's computer revealed searches and visits to websites that provided information on kidnapping, ransom demands, and secure communication methods:

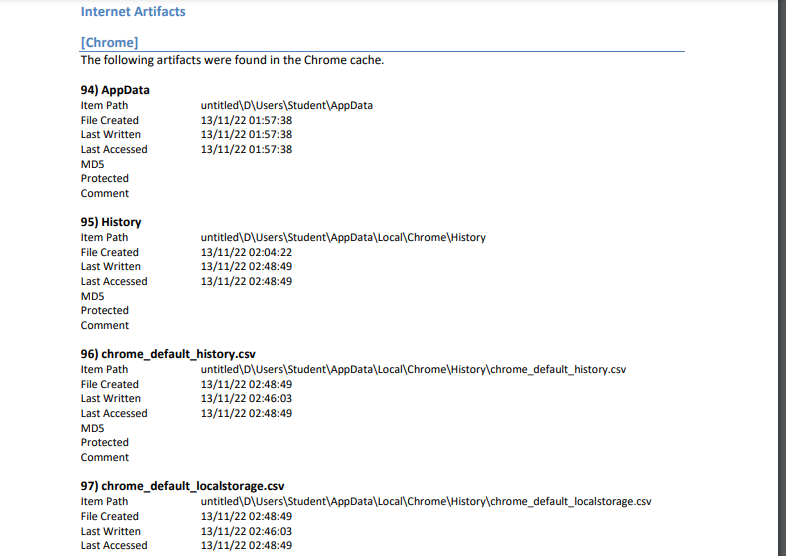


Figure 4:Internet logs

### **Link Files**

Link files and shortcuts found on the suspect's system were examined to reconstruct the digital footprint of activities related to Beth's abduction:

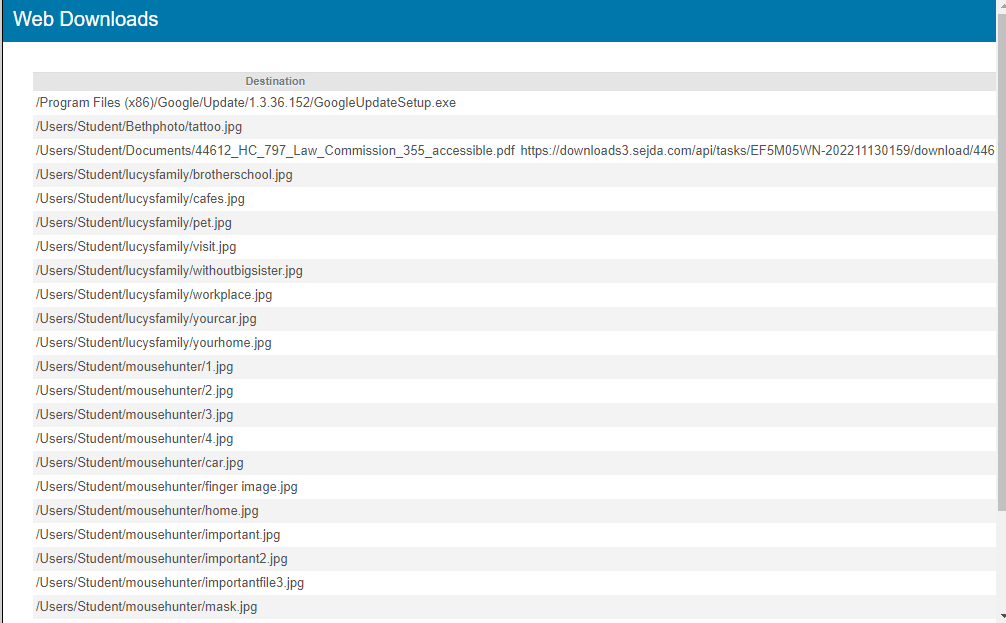


Figure 5: web downloads

### **Encryption**

Analysis of encryption software and encrypted files on the suspect's computer aimed to uncover any attempts to conceal information related to the kidnapping:

Table 6: Vera Crypt

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Set Name** | **Associated Artifact** | **Program** | **Comment** | **Description** | **Tags** |
| Encryption Programs | VeraCrypt | /img\_mouse\_hunter.E01/vol\_vol6/Program Files/VeraCrypt/VeraCrypt.exe | VeraCrypt software used for encryption | Program used for encrypting files | Encryption, VeraCrypt |

Table 7: encrypted file

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Comment** | **Source File** | **Tags** |
| Password protection detected | PDF document | /img\_mouse\_hunter.E01/vol\_vol6/$RECYCLE.BIN/S-1-5-21-569597229-3551119294-3848260287-1001/$R3V2SST.pst/pdfdocument.pdf | Encrypted, Password Protected |

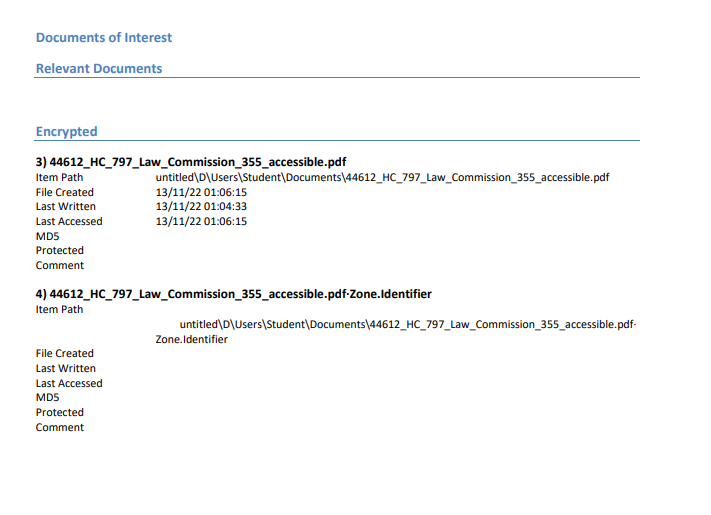


Figure 6: Encase Document of interest

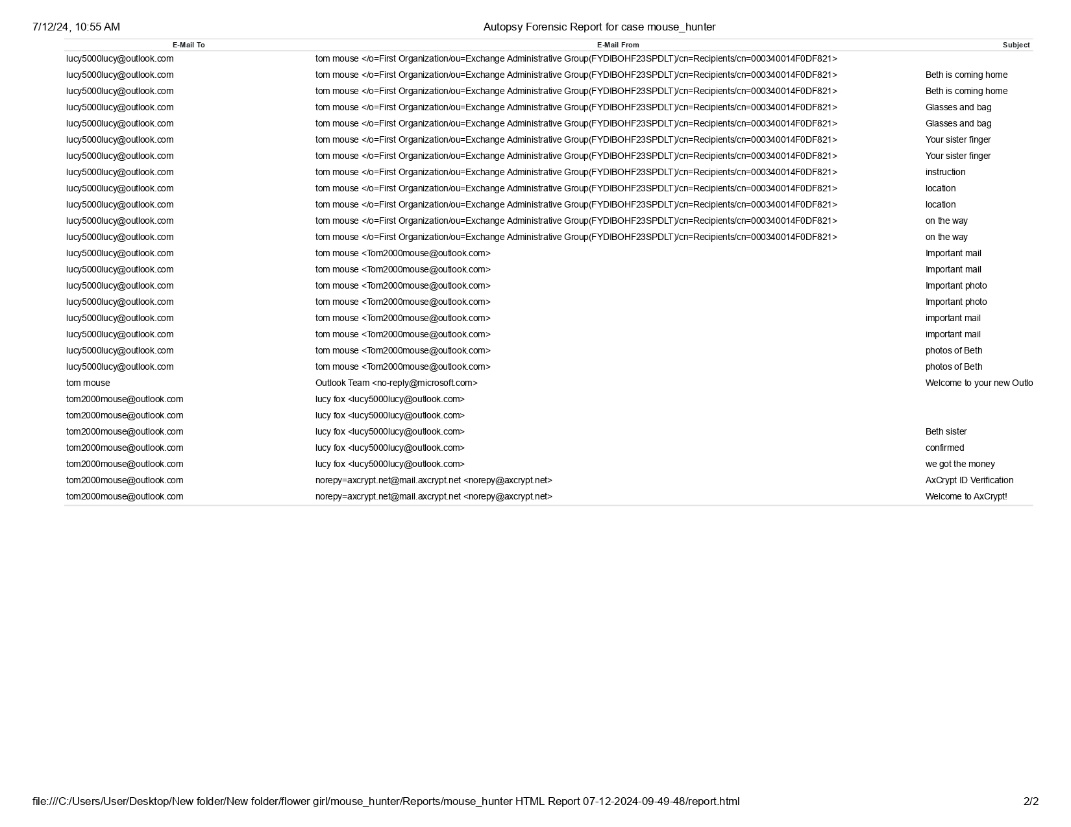
These key evidence items were very vital as they helped in tracing the events that led to the abduction of Beth together with the people involved in the act. Every type of evidence given was useful in explaining the modality and reasons behind the crime and was helpful to officers in their determination of the culprits.

.

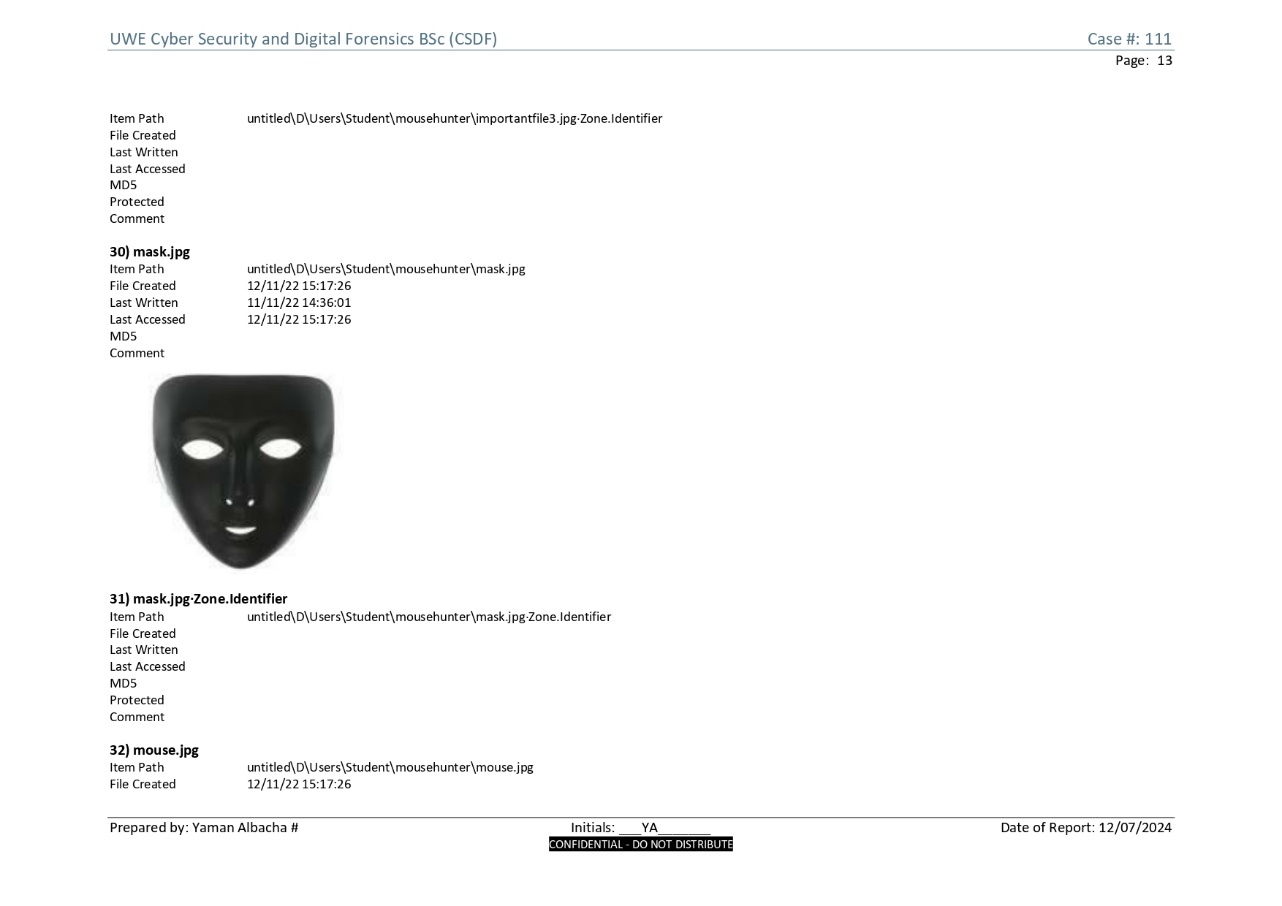
## **Appendix**

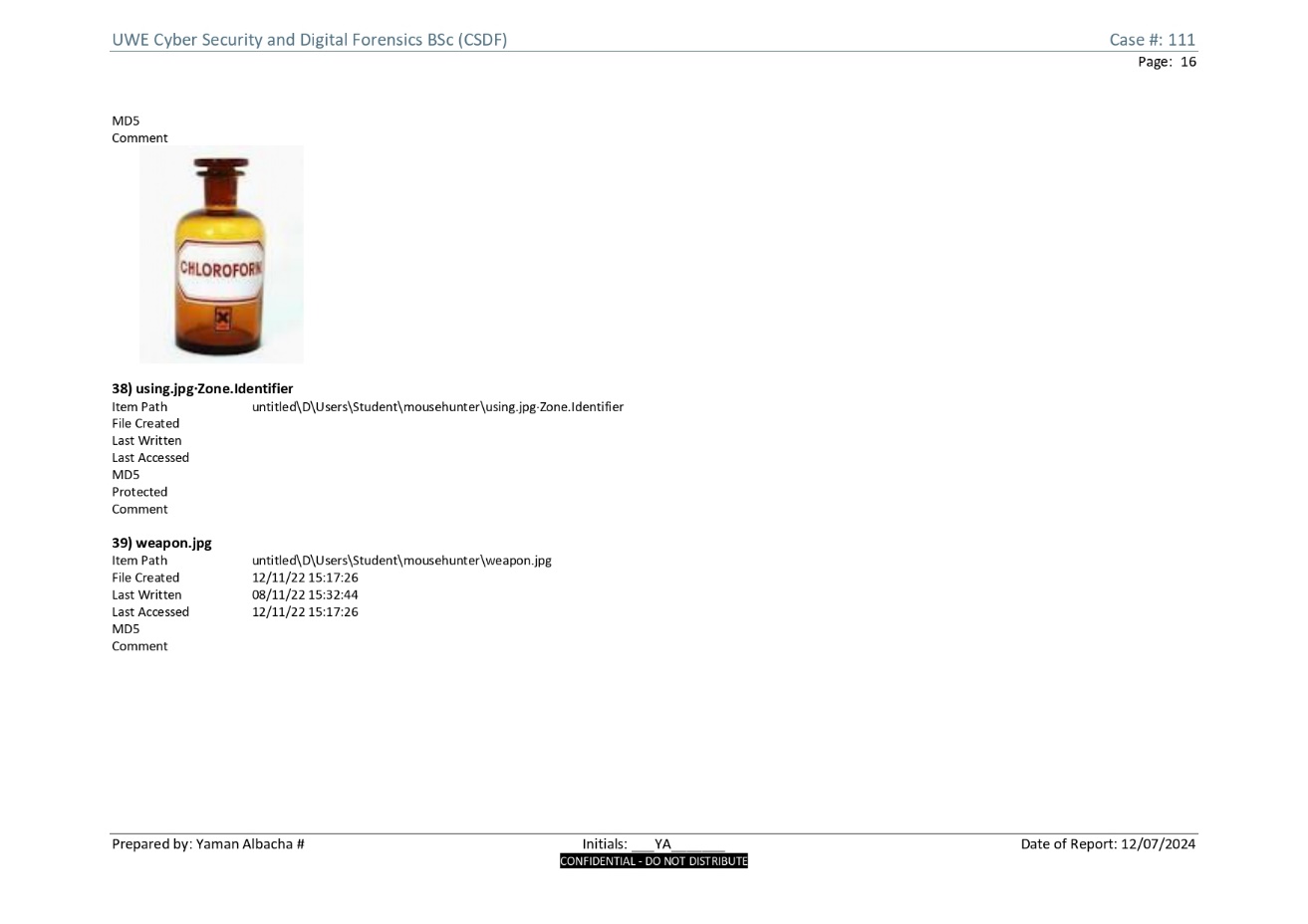
### **Appendix A: E-Mail Messages For** **Autopsy Forensic Report for case mouse\_hunter**

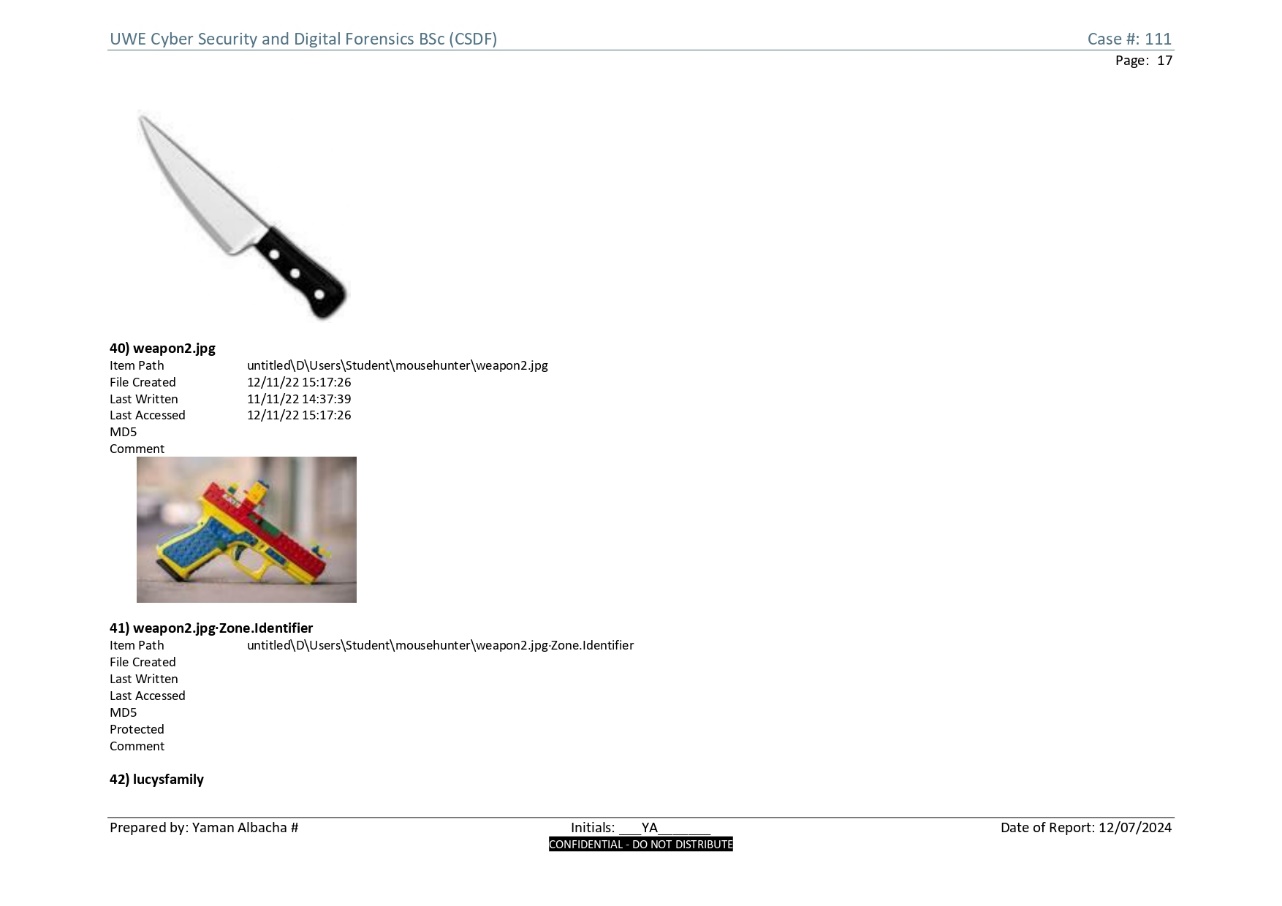


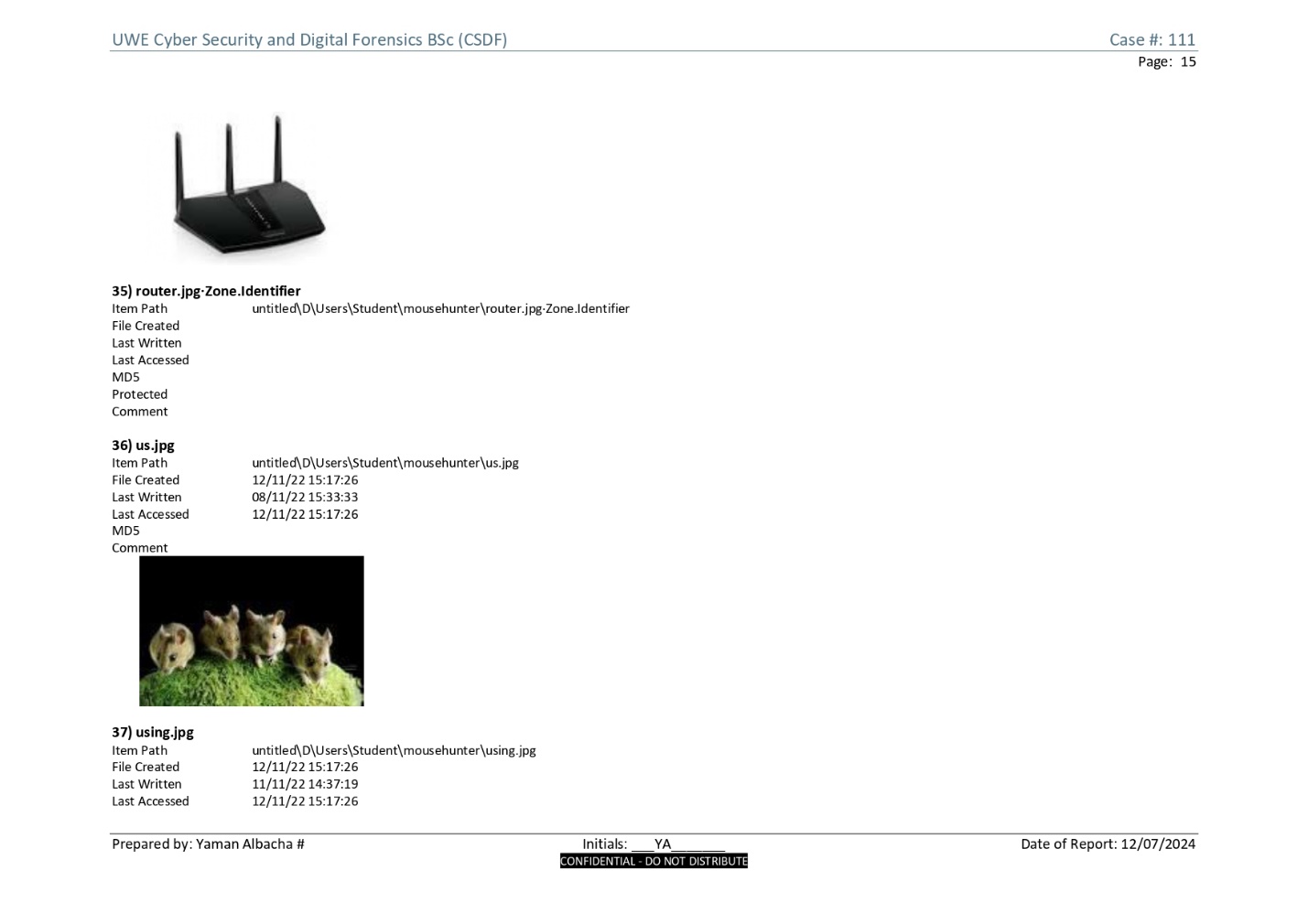


### **Appendix B: Sample Images found for Encase Provenance Report**

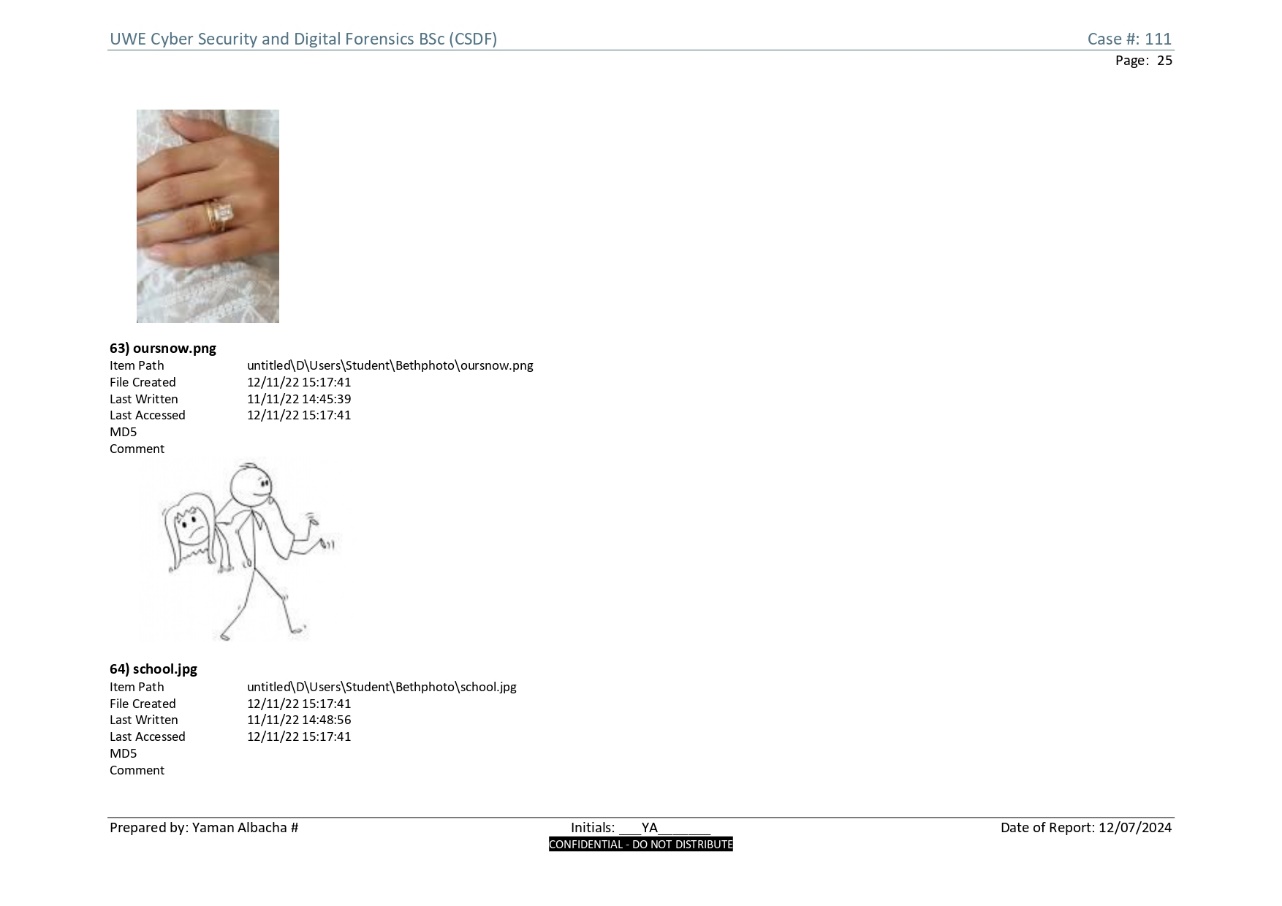
****

****

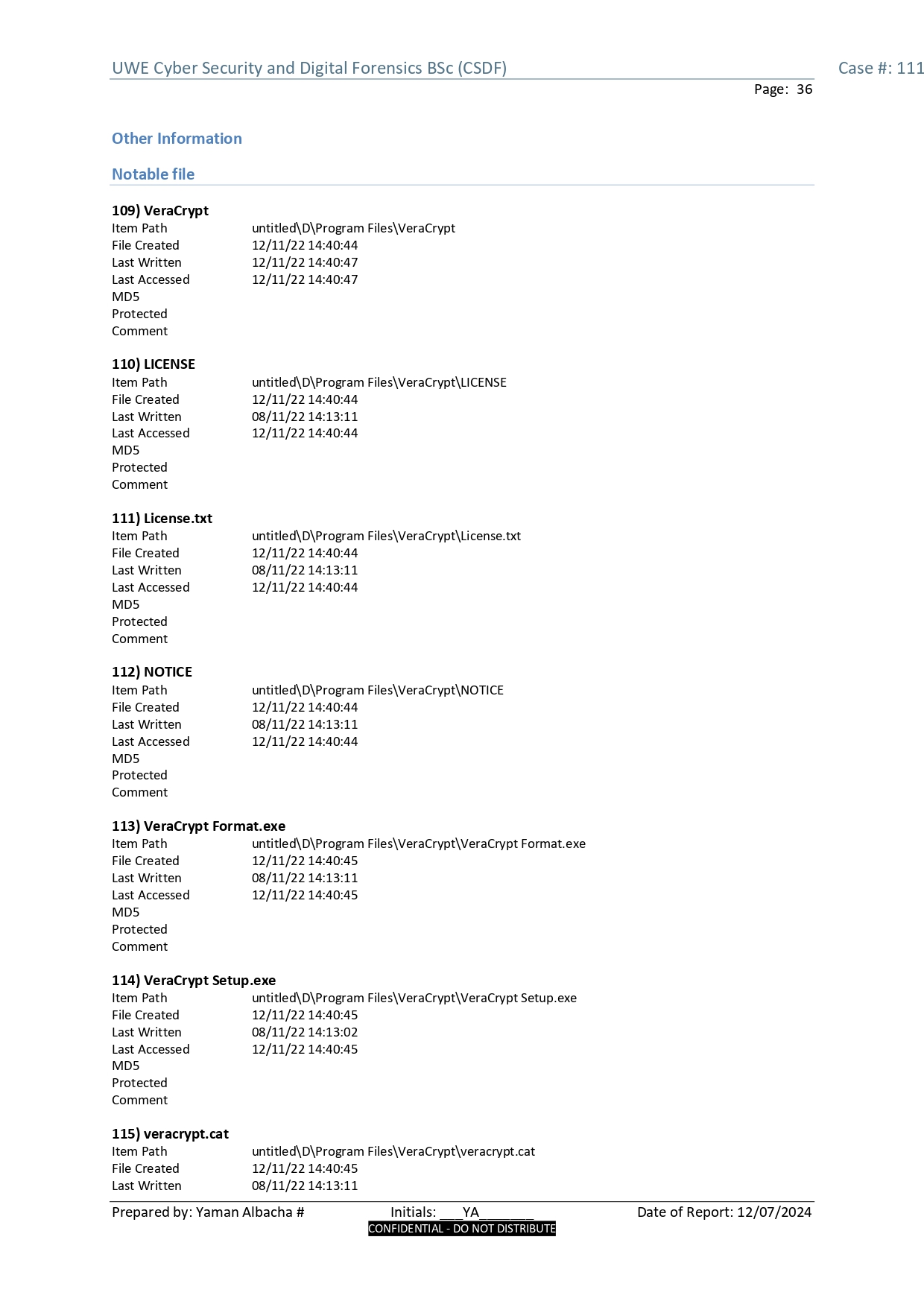
****

****

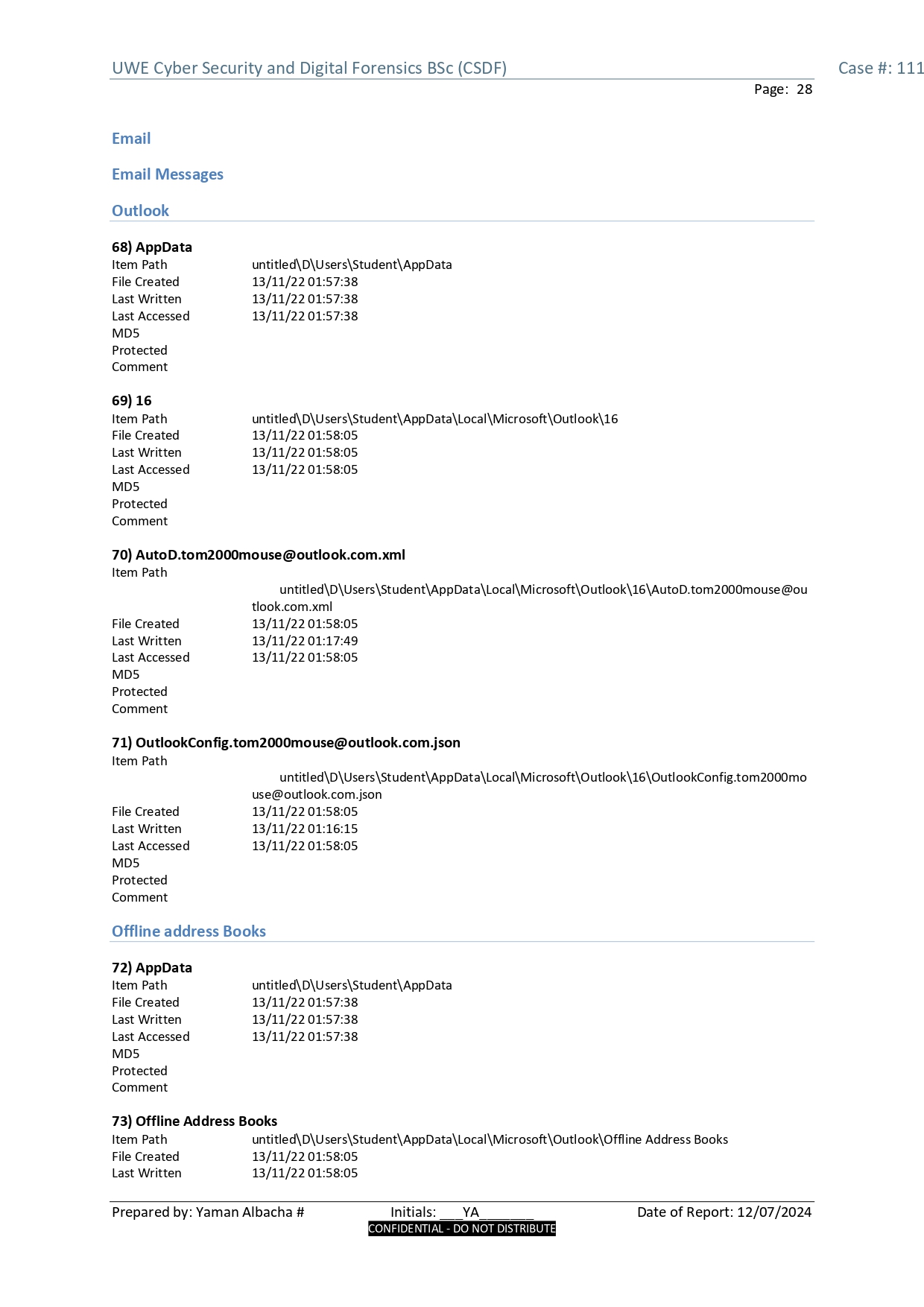
****

****

### **Appendix C: Vera crypt found for Encase Provenance Report**

****

### **Appendix D: Email found for Encase Provenance Report**

****