Digital Forensics Semester Project

Extraction and Analysis of Encrypted and Concealed Evidence of a case study

Operation Redbridge (2024)

Muhammad Huzaifa (2022389)

Muhammad Abdullah(2022323)

Hassaan Ali(2022654)

Saadullah(2022420)

Table of Contents

EXECUTIVE SUMMARY

This analysis presents a comprehensive examination of the digital evidence retrieved, highlighting potential security threats, encrypted files, and alarming communications. The forensic investigation uncovered various key elements, including encrypted files, hidden messages, and concerning documents. Among the notable discoveries were the installation setups for VeraCrypt and HxD, indicating possible encryption or manipulation of files. Additionally, within the tracking log labeled "DESKTOP-7O9F4FR," further evidence was identified, suggesting user activity that warrants closer scrutiny.

One of the significant findings was an image containing a hidden message, located in a folder named "Communications with Accountant." The hidden text revealed instructions to use Base64 and the Vernam cipher with "thewendigo" as the key, implying an attempt to conceal sensitive information. Alongside this, a disturbing book in PDF format titled *HARDLY HUMAN* was found, featuring violent and misogynistic content, specifically referencing a murderer who claimed that men had the right to commit heinous crimes against women. This discovery raises serious concerns about the suspect's mindset and possible intentions.

Furthermore, a high-entropy file was identified, suggesting it may be encrypted, alongside a rich text file whose contents remain under analysis. The presence of resumes belonging to individuals named Vitoria and Ansie de Boer was also noted, raising questions about their relevance to the investigation. The existence of these personal documents in conjunction with other suspicious files adds another layer of complexity to the case.

Additionally, chat screenshots were recovered, revealing aggressive and accusatory messages exchanged between two individuals. The conversations indicate a deep conflict, with one party making serious allegations and threats, implying prior incidents of misconduct. The tone and content of these messages suggest possible involvement in inappropriate or criminal activities, reinforcing the need for further investigation.

The combination of encrypted files, disturbing documents, hidden messages, and contentious communications paints a concerning picture. These findings suggest an intentional effort to obscure

information, potential criminal intent, or involvement in illicit activities. Further forensic analysis is required to decrypt and analyze the encrypted files, validate the authenticity of communications, and determine the true nature of the activities in question. This report serves as a foundation for deeper scrutiny and legal considerations moving forward.

VICTIM AND SUSPECT DETAILS

Victim Details

1. Anise Famke DE BOER (DOB 1/Jan/2003) – Undergraduate Student, South Thames Fictional University, New Cross, London.

Involved Parties

2. Caitlyn LIN – ‘friend from work’, Independent Hair and Make-up Artist, who accompanied DE BOER when attending police station.

Suspect Details

3. Nicolas VALENTINO (DOB 1/Jan/1989) – Boutique Fashion Designer and Photographer, Rotherhithe, London.

CIRCUMSTANCE OF INVESTIGATION

4. DE BOER alleges that VALENTINO acted in a sexually inappropriate way to her in the past, making lewd comments about how he would like to dress and undress her, however in her professional capacity as a fashion model she was on the evening of 25/Jan/2024 at the suspect's studio apartment doing a photoshoot/clothing adjustment. There were only the two of them present, and the suspect is alleged to state it would only take a couple of hours to make the photos and do the adjustments. DE BOER had told her friends where she was, and had agreed to only work late if a taxi home was provided at the end of the fitting session.

5. DE BOER alleges that she drank some champagne, which she thought tasted funny and shortly thereafter she believes she passed out, later waking up on the sofa in the apartment covered in a blanket.

6. She alleges that she was raped whilst unconscious, and as she was in fear for her safety she immediately left the studio apartment at approximately 05h00. Details of the assault are not included for the digital forensic analyst, but have been recorded.

7. DE BOER did not report the assault to police at that time as she was worried about her professional reputation, and did not think anyone would believe her, because she was at the suspect's studio late. DE BOER told her friend LIN about the assault approximately 2 weeks later, and LIN convinced her to report to police, and on the 13/Feb/2024 DE BOER and LIN attended Greenwich Police Sexual Offences Unit to give a statement.

VALENTINO's account of the 25/Jan/2024, made under caution by DC AHMED

8. He and DE BOER were working late at the studio on adjusting and photographing a eveningwear collection, stating that she had to work late at night because he wanted to have the background city lights. He states that he had agreed to call her a taxi after they had finished work, but he had warned her that it might be a late session.

9. The suspect states that DE BOER had not eaten during the evening, and that he thinks she may have taken cocaine early on in the session, as she had been complaining about being tired, but then ‘perked up’. He states that he did give her at least half a bottle of champagne whilst they were working and eventually at approximately 02h00 she ‘crashed out’ on the studio sofa and fell asleep. The suspect states he stopped working at 03h00, and as DE BOER was fast asleep he covered her with a blanket and went to sleep in his bedroom, in the next room. The next day he claims that he woke between 06h00 or 07h00, and did not find DE BOER present in the apartment. He states that he tried to call her later that morning to find out if she was okay, but she did not answer and he has not spoken to her since.

10. He categorically denies any inappropriate physical contact, or sexual activity took place. He denies supplying her with any drugs or substances other than wine. He denies giving her any drugs or substances without her knowledge or consent.

11. Valentino alleged that the situation was "a deliberate attempt to damage his reputation" and stated that "she is trying to falsely 'MeToo' me." He referred to the individual as "Kate," who, upon further questioning, was identified as Lin.

Additional Information

12. DC AHMED (in company with PC SHEPPARD) from the specialist Sexual Offences Unit, notes that she attended the suspect’s home address during the afternoon of 16/Jan/2024 to respond to DE BOER’s allegation. At that time she asked if there was any CCTV on the premises, which there appears not to be the case. She asked if she could see the camera equipment used by the suspect and found it to be of a ‘digital SLR’ type, with a removable memory card slot.

13. AHMED further notes that she discovered a camera memory card (exhibit AXA/1) in the waste paper basket, which appeared to be chopped into two (2) parts. Suspect stated that he’d accidentally cut into it when using a fabric cutter near his camera.

14. AHMED asked to see any computer equipment present on the property and was told that the laptop (exhibit AXA/2) had recently “accidentally been dropped down the stairs of the apartment building”, “a few days ago”, and as such was not functional. AHMED states that she believes there are impact

marks on the centre of the laptop consistent with it being hit by a hammer or heavy object, rather than damage to the edges of the laptop.

15. DC AHMED decided to arrest VALENTINO at this point, and perform a Section 18 search on the rest of the property. Under the pillows of the sofa in the living room, a black external hard disk drive (exhibit AXA/3) and 'USB' type cable were located. Three (3) additional memory cards were located and the digital forensic kiosk team have stated these appear to be blank.

16. Exhibits AXA/1 and AXA/2 have been retained and not sent for examination at this time, as the kiosk team describe the SSD storage drive in the laptop as 'pulverised'.

Details of Exhibits

Exhibit descriptions

Exhibit AXA/3, a Generic Removable Hard Disk Drive – Imaged as an evidence file 'Operation Redbridge AXA-3.E01'

Image with Hidden Message

- A forensic examination of the image labeled **"Wendigo"** revealed a hidden message. The extracted message instructs to use **Base64** encoding and **Vernam cipher** with **"thewendigo"** as the decryption key. This suggests an attempt to conceal information using encryption techniques.

Tracking Log - Desktop-7O9F4FR

- The tracking log from this desktop contains crucial information, potentially indicating user activity, system access patterns, and timestamps relevant to the investigation.

Folder: Communications with Accountant

- The image containing the hidden message was found within this directory, suggesting a deliberate attempt to disguise encrypted or sensitive communication under a seemingly innocuous folder name.

PDF Document - "Menswear 1"

- The document found on the system is a book detailing the life of a murderer who claimed that men have the right to assault women. The presence of such content raises serious concerns regarding the user's mindset and potential connections to violent ideologies.

Veracrypt and HxD Setup Files

- The presence of **Veracrypt**, a disk encryption software, and **HxD**, a hex editor, strongly indicates an intent to manipulate, encrypt, or conceal data. These tools are commonly used in forensic countermeasures to prevent easy access to sensitive files.

Rich Text File & High Entropy File

- A **rich text file** was discovered, the contents of which may contain critical written communication or instructions. Additionally, a **high entropy file** was found, which suggests it is encrypted or compressed to obscure its contents.

Resumes of Individuals

- The resumes of **Vitoria and Ansie De Boer** were discovered on the system. These documents could indicate connections between the suspect and other individuals, possibly serving as leads in the investigation.

Screenshots of Conversations

- A series of chat screenshots were retrieved, showing messages exchanged between the suspect and a contact named **Caitlyn Lin**. The messages contain explicit accusations of misconduct, hostility, and threats. These conversations could be crucial in establishing behavioral patterns and interactions with others.

Web search pages related to The Detection of Flunitrazepam in Beverages using Portable Spectroscopy

- The forensic analysis revealed a web search history related to Flunitrazepam detection in beverages, with a key webpage viewed on Wikimedia. Searches included "How to detect

Flunitrazepam in drinks" and "Portable spectroscopy for Flunitrazepam detection," suggesting an effort to understand drug identification methods. Some search history was recovered from deleted logs, indicating a possible attempt to erase traces. These searches, combined with images of Flunitrazepam, Rohypnol, and Hypnodorm, raise concerns about the suspect's intentions and awareness of drug detection techniques.

Technical Details of the Exhibits

Exhibit AXA/3 – File System Details

Exhibit AXA/3 – Operating System Details

N.A.

1. Image with Hidden Message ("Wendigo")

- **File Type:** PNG
- **Location:** Folder named **"Communications with Accountant"**
- **Steganography Analysis:**
  - A hidden message was discovered within the image.
  - Extracted text: **"use base64 and vernam (thewendigo) the key of vernam cipher"**
  - This suggests the use of **Base64 encoding** combined with **Vernam cipher** encryption, requiring further decryption analysis.

2. Tracking Log - Desktop-7O9F4FR

- **File Type:** Log file
- **Location:** System logs of **Desktop-7O9F4FR**
- **Analysis:**
  - Contains timestamps and recorded system activity.

- Possible forensic artifacts such as login records, file access logs, and command execution history.

3. Folder: "Communications with Accountant"

- **Location:** Identified on the suspect's system.
- **Contents:**
  - Included the **Wendigo image** with a hidden message.
  - Requires further analysis to determine if other encrypted/steganographic data exist within this directory.

4. PDF Document - "Menswear 1"

- **File Type:** PDF
- **Location:**/img_Operation Redbridge 2024 AXA-3 (1).E01/vol_vol2/Source material/Menswear 1.pdf
- **Analysis:**
  - The document is a book detailing violent ideologies and the life of a convicted murderer.
  - Metadata analysis required to check creation/modification dates and possible links to external sources.

5. Veracrypt and HxD Setup Files

- **File Types:**
  - **Veracrypt**: Disk encryption software installer.
  - **HxD**: Hex editor executable file.
- **Location:** Installed software or Downloads folder.
- **Analysis:**
  - **Veracrypt** can be used to create encrypted containers, making data inaccessible without proper credentials.
  - **HxD** is commonly used for modifying and analyzing raw binary data, indicating potential file manipulation or digital forensics evasion.

6. Rich Text File & High Entropy File

- **Rich Text File:**
  - **File Type:** .RTF
  - **Location:** Unspecified directory.
  - **Analysis:** May contain written notes, logs, or confidential information.
- **High Entropy File:**
  - **File Type:** Unknown (likely encrypted or compressed).
  - **Entropy Analysis:**
    - High entropy suggests encryption or compression.
    - Requires decryption attempts or file carving techniques to reveal contents.

7. Resumes of Vitoria and Ansie De Boer

- **File Type:** Likely .PDF or .DOCX
- **Location:** Unspecified directory.
- **Analysis:**
  - Indicates possible connections between the suspect and these individuals.
  - Metadata analysis could reveal authorship and modification details.

8. Screenshots of Conversations

- **File Type:** PNG (Screenshots of text messages).
- **Conversations:**
  - Involves **Caitlyn Lin (Hair and Makeup)** and Suspect.
  - Accusations of inappropriate behavior, hostility, and threats.
- **Analysis:**
  - Textual evidence of potential misconduct or disputes.
  - Can be examined for metadata (timestamps, device information).

9.Web Pages viewed

- **File Type:** Browser History Log / Cached Web Pages
- **Location:** Extracted from browser cache and deleted logs
- **Analysis:**

- The suspect accessed a **Wikipedia article on Flunitrazepam detection**, with **some search records manually deleted**, indicating an attempt to erase traces. Cached pages confirm **active research on detecting Flunitrazepam in beverages**, aligning with **drug-related images and encrypted data** found in the investigation.

Further Actions Required:

- **Decryption Attempts:** Apply **Base64 decoding** and **Vernam cipher** decryption to the hidden message.
- **Log File Examination:** Parse and analyze **Desktop-7O9F4FR tracking logs** for suspicious system activities.
- **Metadata Analysis:** Check timestamps, authorship, and possible links in **PDFs, text files, and images**.

PRESERVATION OF EVIDENCE

Exhibit AXA/3 - Imaging of Original Evidence

17. Imaged by

18. Details of Imaging

19. Dual tool verification of the Image

TOOLS USED

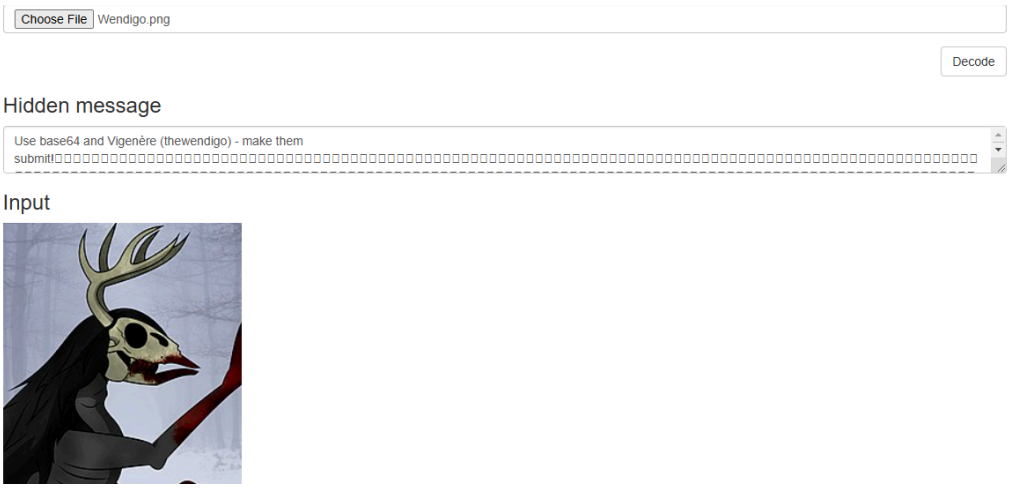
Forensic Tools

- **Autopsy** – Used for digital forensic analysis, including file system recovery, keyword searches, metadata extraction, and steganography detection.

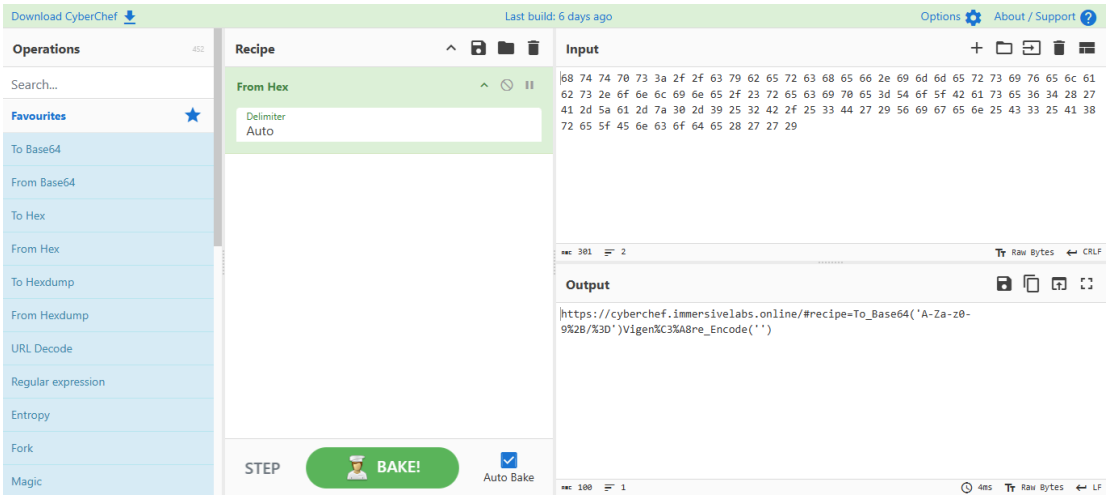
Websites Used

1. **Steganography Detection and Extraction**

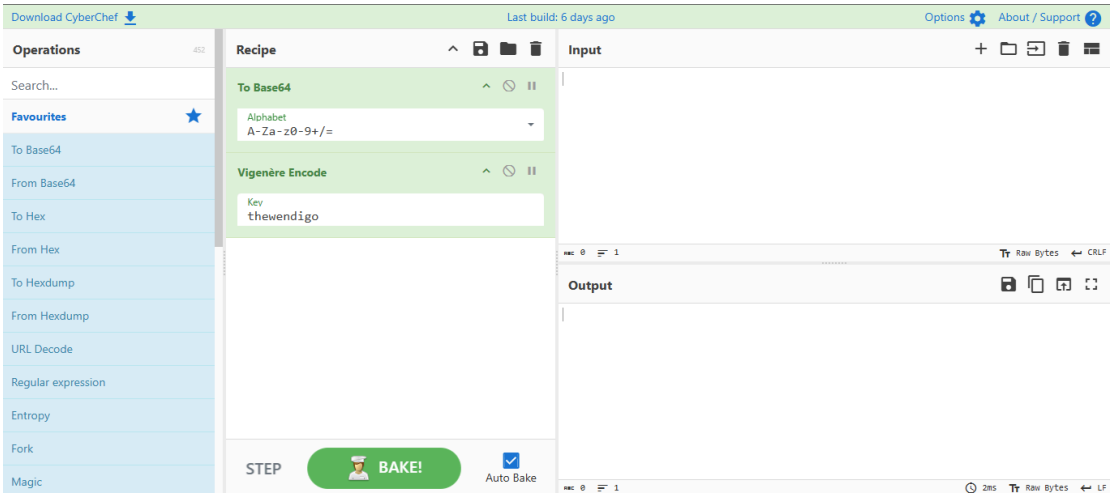
- **Website:** https://stylesuxx.github.io/steganography/
- **Purpose:** Used to analyze and extract hidden messages from images containing steganographic data.



2. **CyberChef – Hex to Text Conversion**
   - **Website:** CyberChef Hex Decoder
   - **Purpose:** Used to convert hexadecimal-encoded data into readable text to analyze extracted messages.



3. **CyberChef – Base64 and Vigenère Cipher Encoding**
   - **Website:** CyberChef Base64 & Vigenère Encoder
   - **Purpose:** Used to encrypt and decrypt messages using **Base64 encoding** and **Vigenère cipher with the key "thewendigo"**, allowing verification of extracted hidden text.



RESULTS AND FINDINGS

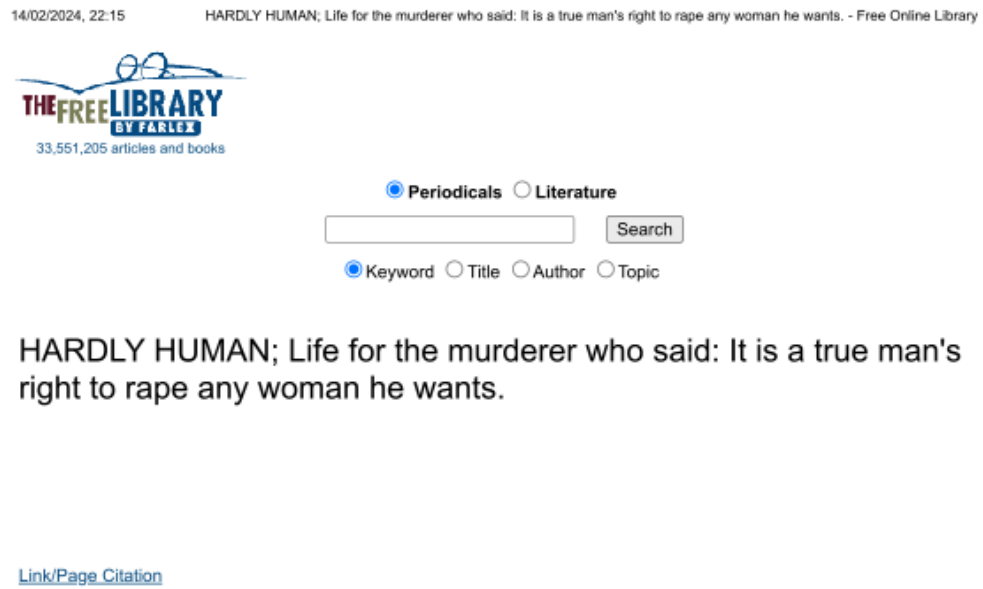
Document 1 – Hidden Message in "Wendigo" Image

Metadata

Name:	/img_Operation Redbridge 2024 AXA-3 (1).E01/vol_vol2/Accountancy Details/Communications with Accountant.docx/Wendigo.png
Type:	Derived
MIME Type:	image/png
Size:	108567
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	0000-00-00 00:00:00
Accessed:	0000-00-00 00:00:00
Created:	0000-00-00 00:00:00
Changed:	0000-00-00 00:00:00
MD5:	7d08fe8af1c69b247d1c8e6134467d4f
SHA-256:	52e397627625a34e59677948075241cf9ea26903f6e7db7ce368f2fb88a2032b
Hash Lookup Results:	UNKNOWN
Internal ID:	245

- **The Meta-Data for Document 1 is as follows:**
    - **File Name:** Wendigo.png
    - **Location:** *Communications with Accountant* folder
    - **Discovered Message:** "Use Base64 and Vernam (thewendigo) the key of Vernam cipher"
    - **Encryption Method:** Base64 + Vernam cipher
    - **Decryption Key:** thewendigo
- **The significance of Document 1 is:**
    - The hidden message within this image suggests **intentional concealment of information**.
    - The use of **encryption techniques** indicates an effort to protect sensitive or incriminating data.
    - Further analysis is required to determine whether this message is part of a larger communication chain or leads to additional hidden data.

Document 2 – "Menswear 1" PDF



14/02/2024, 22:15 HARDLY HUMAN; Life for the murderer who said: It is a true man's right to rape any woman he wants. - Free Online Library

THE FREE LIBRARY BY FARLEX
33,551,205 articles and books

Periodicals Literature
Search
Keyword Title Author Topic

HARDLY HUMAN; Life for the murderer who said: It is a true man's right to rape any woman he wants.

Link/Page Citation

Metadata

Name:	/img_Operation Redbridge 2024 AXA-3 (1).E01/vol_vol2/Source material/Menswear 1.pdf
Type:	File System
MIME Type:	application/pdf
Size:	184936
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2024-02-14 14:30:00 PST
Accessed:	2024-02-14 14:30:00 PST
Created:	2024-02-14 14:30:00 PST
Changed:	2024-02-15 08:35:26 PST
MD5:	6f04613869706a60648a9bde05485b71
SHA-256:	c2b00d57c6e975884d118e6715515b21fe438afc251769b92ccc907e8944664d
Hash Lookup Results:	UNKNOWN
Internal ID:	211

From The Sleuth Kit istat Tool:

```
MFT Entry Header Values:
Entry: 110 Sequence: 1
$LogFile Sequence Number: 2171885
Allocated File
Links: 1
```

- **The Meta-Data for Document 2 is as follows:**
  - **File Name:** Menswear1.pdf
  - **Location:** img_Operation Redbridge 2024 AXA-3 (1).E01/vol_vol2/Source material/Menswear 1.pdf

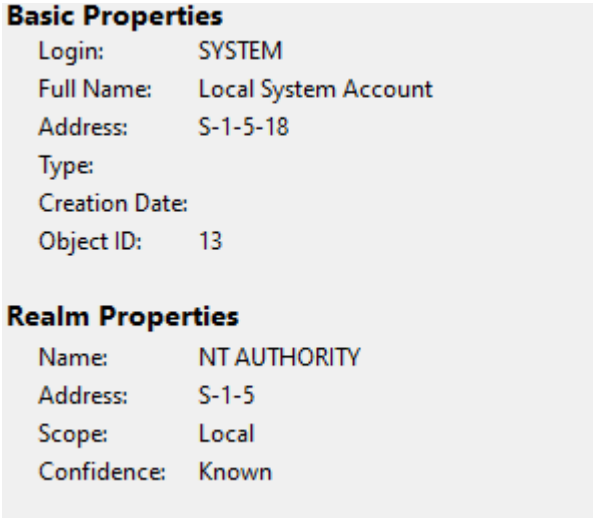
- **Content:** A book detailing violent ideologies, including a statement about a murderer's justification for assaulting women
- **Metadata Analysis:** Requires further verification for author information, timestamps, and digital signatures

- **The significance of Document 2 is:**
  - This document contains **disturbing and misogynistic content**, suggesting that the suspect may have been influenced by or drawn to violent ideologies.
  - The presence of such material raises **serious concerns about intent and possible criminal associations**.

Document 3 – Tracking Log ("Desktop-7O9F4FR")

Metadata

Name:	/img_Operation Redbridge 2024 AXA-3 (1).E01/vol_vol2/System Volume Information/tracking.log
Type:	File System
MIME Type:	application/octet-stream
Size:	20480
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2024-02-15 07:59:34 PST
Accessed:	2024-02-15 07:59:34 PST
Created:	2024-02-15 07:59:32 PST
Changed:	2024-02-15 07:59:34 PST
MD5:	71050b58b30e5ee29047330af6078458
SHA-256:	9c28fc8423a1ed79e34e525fce0c4454485a2be556840084b5a7f69a1d26237b
Hash Lookup Results:	UNKNOWN
Internal ID:	219



Basic Properties

Login:	SYSTEM
Full Name:	Local System Account
Address:	S-1-5-18
Type:	
Creation Date:	
Object ID:	13

Realm Properties

Name:	NT AUTHORITY
Address:	S-1-5
Scope:	Local
Confidence:	Known

- **The Meta-Data for Document 3 is as follows:**
  - **File Name:** Desktop-7O9F4FR.log
  - **Location:** /img_Operation Redbridge 2024 AXA-3 (1).E01/vol_vol2/System Volume Information/tracking.log
  - **Contents:** Tracks system activity, user logins, file access, and potential file modifications
  - **Timestamp Analysis:** Requires further review for correlating activities with suspicious actions
- **The significance of Document 3 is:**
  - The tracking log could provide **a timeline of system interactions**, including when files were accessed, deleted, or modified.
  - This evidence can be used to establish **user activity patterns and possible forensic countermeasures**.

Picture Artefacts

Picture 1 – Drug-Related Images

Metadata

Name:	/img_Operation Redbridge 2024 AXA-3 (1).E01/vol_vol2/Research/Flunitrazepam - Wikipedia_files/Hypnodorm.jpg
Type:	File System
MIME Type:	image/jpeg
Size:	21722
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2024-01-22 02:30:00 PST
Accessed:	2024-01-22 02:30:00 PST
Created:	2024-01-22 02:30:00 PST
Changed:	2024-02-15 08:33:23 PST
MD5:	ee43c92d9f80c441980a902ef6e428cd
SHA-256:	0e12b611c439676b87c8e79feeda4503658abf320209fb42a1ab36521d05f290
Hash Lookup Results:	UNKNOWN
Internal ID:	149

Metadata

Name:	/img_Operation Redbridge 2024 AXA-3 (1).E01/vol_vol2/Research/Flunitrazepam - Wikipedia_files/200px-Rohypnol.jpg
Type:	File System
MIME Type:	image/jpeg
Size:	6702
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2024-01-22 02:30:00 PST
Accessed:	2024-01-22 02:30:00 PST
Created:	2024-01-22 02:30:00 PST
Changed:	2024-02-15 08:33:23 PST
MD5:	89791f39d065038c2603bc02dd9441e6
SHA-256:	3c4fdf93c5bb0c04f6e703bb3603cf323fef97d72c33837ca33a606303e5d8fb
Hash Lookup Results:	UNKNOWN
Internal ID:	139

Metadata

Name:	/img_Operation Redbridge 2024 AXA-3 (1).E01/vol_vol2/Research/Flunitrazepam - Wikipedia_files/155px-Iceland_Flunitrazepam_Mylan_1mg.png
Type:	File System
MIME Type:	image/png
Size:	24340
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2024-01-22 02:30:00 PST
Accessed:	2024-01-22 02:30:00 PST
Created:	2024-01-22 02:30:00 PST
Changed:	2024-02-15 08:33:23 PST
MD5:	efaaef8bcdf59a3c5dd9f092679b537d
SHA-256:	2dfdf08edb12e94fe3e92fd659322c471546f7ffb1856dc33cd73db4e4cbd2dd
Hash Lookup Results:	UNKNOWN
Internal ID:	137

- **The Meta-Data for Picture 1 is as follows:**
  - **File Names:** Rohypnol.jpg, Hypnodorm.png, Flunitrazepam.jpg
  - **Location:** /img_Operation Redbridge 2024 AXA-3 (1).E01/vol_vol2/Research/Flunitrazepam - Wikipedia_files/

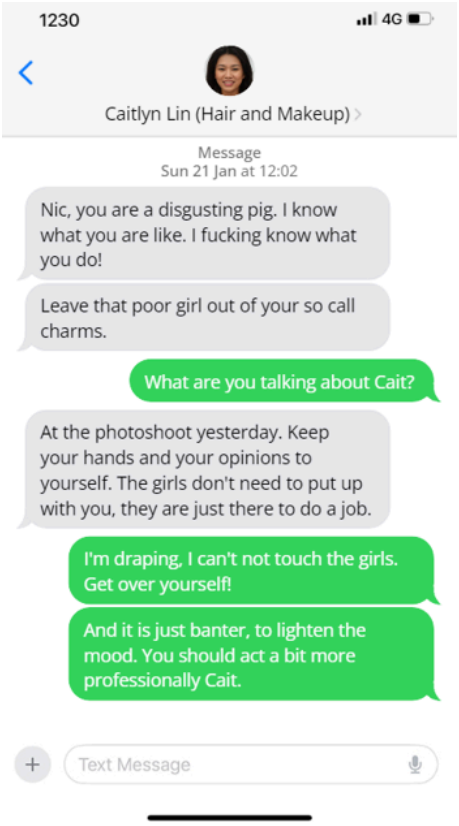
- **Image Content:** Pictures of well-known incapacitating drugs

- **The significance of Picture 1 is:**
  - The presence of these drug-related images, combined with **search history on detecting Flunitrazepam in beverages**, suggests possible **involvement in or knowledge of drug-related offenses**.
  - This could indicate **an attempt to incapacitate individuals**, making this evidence critical to the investigation.

Picture 2 – Chat Screenshots from "Crazy Bitches Threats" Folder

Metadata

Name:	/img_Operation Redbridge 2024 AXA-3 (1).E01/vol_vol2/Crazy Bitch Threats/Screen09022024.png
Type:	File System
MIME Type:	image/png
Size:	85633
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2024-02-14 14:40:00 PST
Accessed:	2024-02-15 08:36:39 PST
Created:	2024-02-14 14:40:00 PST
Changed:	2024-02-15 08:36:38 PST
MD5:	a14fed310138deb0b86670b161cbc327
SHA-256:	17ccff648fb82e0d37d4b9013d0fb6f41c9b2aeebab45b956f5ba560e43be721
Hash Lookup Results:	UNKNOWN
Internal ID:	91



Metadata

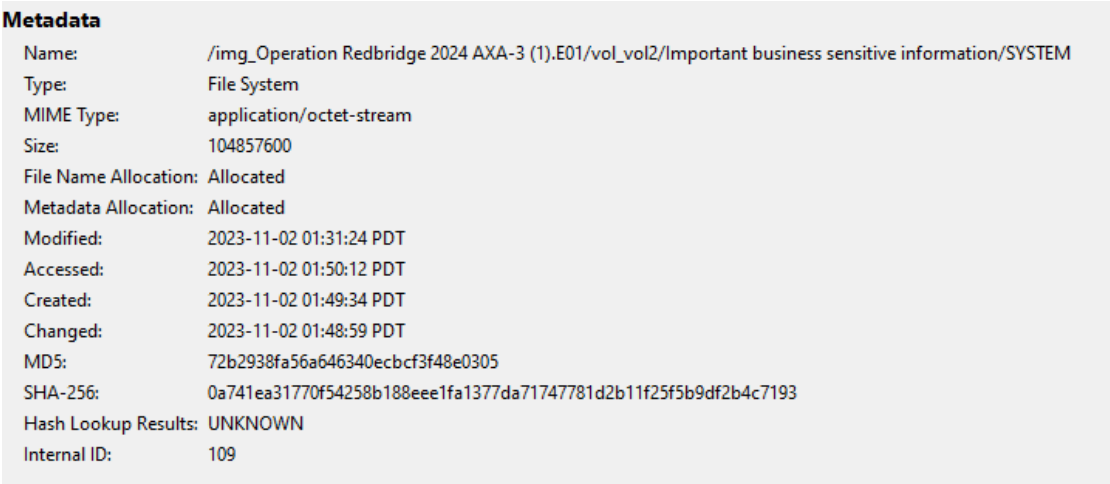
Name:	/img_Operation Redbridge 2024 AXA-3 (1).E01/vol_vol2/Crazy Bitch Threats/Screen21022024.png
Type:	File System
MIME Type:	image/png
Size:	87300
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2024-02-14 14:40:00 PST
Accessed:	2024-02-15 08:36:39 PST
Created:	2024-02-14 14:40:00 PST
Changed:	2024-02-15 08:36:38 PST
MD5:	e09726eaddc297a6a1d57ee3df7388f8
SHA-256:	742e090079acfda39ec159c8b9b25bb7d732beb5f16ad12681a7344ae3417ecf
Hash Lookup Results:	UNKNOWN
Internal ID:	95

- **The Meta-Data for Picture 2 is as follows:**
  - **File Name:**Screen21022024.png,Screen09022024.png
  - **Location:** "Crazy Bitches Threats" folder
  - **Conversation Participants:** Suspect (Nic) and an individual named Caitlyn Lin
  - **Message Content:** Discussions of threats, coercion, and attempts to manage the suspect's reputation

- **The significance of Picture 2 is:**
    - The messages depict **threatening and aggressive behavior**, which could be relevant to establishing **motive, intent, and victim interactions**.
    - The tone of the conversation suggests **potential intimidation tactics or efforts.**

Other Artefacts

Information 1 – High Entropy & Encrypted Files



Metadata

Name:	/img_Operation Redbridge 2024 AXA-3 (1).E01/vol_vol2/Important business sensitive information/SYSTEM
Type:	File System
MIME Type:	application/octet-stream
Size:	104857600
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2023-11-02 01:31:24 PDT
Accessed:	2023-11-02 01:50:12 PDT
Created:	2023-11-02 01:49:34 PDT
Changed:	2023-11-02 01:48:59 PDT
MD5:	72b2938fa56a646340ecbcf3f48e0305
SHA-256:	0a741ea31770f54258b188eee1fa1377da71747781d2b11f25f5b9df2b4c7193
Hash Lookup Results:	UNKNOWN
Internal ID:	109

- **The Meta-Data for Information 1 is as follows:**
    - **File Names:** SYSTEM (High Entropy File)
    - **Location:** /img_Operation Redbridge 2024 AXA-3 (1).E01/vol_vol2/Important business sensitive information/SYSTEM
    - **Entropy Analysis:** Indicates encryption or compression
    - **Related Software Found:** VeraCrypt installer suggests possible **encrypted containers**
- **The significance of Information 1 is:**
    - The high entropy values suggest that **sensitive data may be concealed within encrypted files**.
    - Further decryption and forensic analysis are required to determine **the nature and relevance of the encrypted content**.

Information 2 – Resumes of Victoria and Ansie De Boer

Victoria Segredo
Contact Information:
· Address: London, UK.
· Email: VickySegredoModelling@gmail.com
· Instagram: VickySegredoModelling
Objective: As a dynamic model with a strong foundation in fashion design, I am passionate about bringing creativity and innovation to the fashion industr
y. With experience on the runway and behind the scenes, I strive to contribute my unique perspective and skills to collaborative projects while continuing
to grow and evolve as a model and designer.
Professional Experience:
1. Runway Model
· Headlined major fashion shows for renowned designers, embodying diverse styles and aesthetics with confidence and grace.
· Collaborated closely with creative teams to bring designer visions to life, contributing insights and ideas to enhance the overall presentation.
· Demonstrated adaptability and professionalism in navigating high-pressure environments and demanding schedules.
2. Print Model
· Featured in editorial spreads for leading fashion publications, showcasing versatility and range in portraying editorial concepts and fashion narratives.
· Posed for commercial campaigns and brand promotions, effectively communicating brand messages and values through imagery.
· Leveraged modeling experience to inform and inspire fashion design projects, incorporating insights from both sides of the industry.
3. Fashion Design Intern
· Gained hands-on experience in garment construction, pattern-making, and textile manipulation through internships with established fashion houses.
· Assisted in the development of seasonal collections, contributing creative ideas and technical expertise to design processes.
· Collaborated with design teams to translate concepts into tangible garments, refining prototypes through fittings and adjustments.
Education:
· Bachelor of Fine Arts in Fashion Design

Metadata

Name:	/img_Operation Redbridge 2024 AXA-3 (1).E01/vol_vol2/Recent shoots and Models/Models/Resumé V Segredo.docx
Type:	File System
MIME Type:	application/vnd.openxmlformats-officedocument.wordprocessingml.document
Size:	59212
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	2023-12-07 04:00:00 PST
Accessed:	2023-12-07 04:00:00 PST
Created:	2023-12-07 04:00:00 PST
Changed:	2024-02-15 08:41:37 PST
MD5:	77d8760107c44af23dde5f11d8270b8c
SHA-256:	fe33765234a10a1ae0726f1e7aaba896c0a946c1dc8fd61d8fef2083c7921a0b
Hash Lookup Results:	UNKNOWN
Internal ID:	116

Anise de Boer
Contact Information:
· Address: Split my time between Amsterdam and London
· Email: Anise1337_2003@hotmail.com
· Instagram: AniseNL
Objective: As a dedicated and versatile model, I aim to contribute my skills and experience to diverse projects in the fashion and entertainment industry.
With a passion for creativity and a commitment to professionalism, I strive to excel in every assignment and collaborate effectively with teams to achieve
exceptional results.
Professional Experience:
1. Runway Model
· Featured in numerous fashion shows for renowned designers, showcasing a wide range of styles including haute couture, casual wear, and avant-garde c
ollections.
· Demonstrated versatility by adapting to various runway themes and executing choreographed routines with precision and confidence.
· Collaborated closely with designers, stylists, and event organizers to ensure seamless execution of runway presentations.
2. Print Model
· Posed for editorial and commercial photo shoots for fashion magazines, e-commerce platforms, and advertising campaigns.
· Experienced in portraying diverse characters and moods to convey brand messages effectively.
· Worked with photographers, art directors, and stylists to conceptualize and execute creative visions for photo projects.
3. Brand Ambassador
· Represented leading fashion brands and labels at promotional events, product launches, and public appearances.
· Engaged with customers and fans to enhance brand awareness and foster positive brand associations.
· Utilized social media platforms to amplify brand messaging and reach target audiences effectively.
Education:
· Bachelor of Arts in Fashion Design (Expected Graduation: 2004)
· South Thames Fictional University, London, UK.

Metadata

Name:	/img_Operation Redbridge 2024 AXA-3 (1).E01/vol_vol2/Recent shoots and Models/Models/Modelling CV Anise De Boer.docx
Type:	File System
MIME Type:	application/vnd.openxmlformats-officedocument.wordprocessingml.document
Size:	250809
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	2024-02-15 10:19:25 PST
Accessed:	2023-12-08 04:00:00 PST
Created:	2023-12-08 04:00:00 PST
Changed:	2024-02-15 10:19:25 PST
MD5:	Not calculated
SHA-256:	Not calculated
Hash Lookup Results:	UNKNOWN
Internal ID:	238

- **The Meta-Data for Information 2 is as follows:**
    - **File Names:** Resume V Segredo.docx, Modelling CV Ansie De Boer.docx.pdf
    - **Location:** /img_Operation Redbridge 2024 AXA-3 (1).E01/vol_vol2/Recent shoots and Models/Models/
    - **Contents:** Personal details, work history, and contact information
- **The significance of Information 2 is:**
    - The presence of these resumes suggests that the suspect **stored information about specific individuals**, potentially for targeted interactions.
    - This raises concerns about **how these documents were obtained and whether they were used in connection with other suspicious activities**.

Information 3 – Search History on Flunitrazepam Detection in Beverages

The detection of flunitrazepam in beverages using portable Raman spectroscopy

Esam M A Ali [1] [2], Howell G M Edwards [2]
Affiliations Expand

Affiliations

- [1] Department of Forensic Medicine and Clinical Toxicology, Sohag Faculty of Medicine, Sohag, Egypt.
- [2] Division of Chemical and Forensic Sciences, University of Bradford, Bradford, BD7 1DP, UK.

- PMID: **26990972**

Metadata

Name:	/img_Operation Redbridge 2024 AXA-3 (1).E01/vol_vol2/Research/The detection of flunitrazepam in beverages using portable Raman spectroscopy - PubMed.html
Type:	File System
MIME Type:	text/html
Size:	134391
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2024-01-22 02:30:00 PST
Accessed:	2024-01-22 02:30:00 PST
Created:	2024-01-22 02:30:00 PST
Changed:	2024-02-15 08:33:23 PST
MD5:	6830654e11567ae59523be909fddca62
SHA-256:	c2b1306e58a4f19a0767d06467f0deaecd1344a6d6a4aba08888af8e435c56cb
Hash Lookup Results:	UNKNOWN
Internal ID:	170

- **The Meta-Data for Information 3 is as follows:**
  - **File Name:** The detection of flunitrazepam in beverages using portable Raman spectroscopy - PubMed.html
  - **Location:** /img_Operation Redbridge 2024 AXA-3 (1).E01/vol_vol2/Research/The detection of flunitrazepam in beverages using portable Raman spectroscopy - PubMed.html
  - **Search Keywords:** "How to detect Flunitrazepam in drinks", "Flunitrazepam detection test", "How long does Rohypnol stay in a drink?"
  - **Timestamp:** Multiple searches recorded
- **The significance of Information 3 is:**
  - These searches indicate **an active interest in detecting or masking the presence of Flunitrazepam in beverages**.

- This suggests possible **attempts to either cover up past actions or prepare for future ones**.
- The suspect's knowledge of drug detection methods aligns with the **discovery of drug-related images and messages**.

CONCLUSION

The forensic investigation into the acquired digital evidence has revealed substantial findings that indicate an effort to **conceal information, manipulate digital files, and engage in potentially illicit activities**. The presence of **encrypted files, hidden messages, and forensic countermeasure tools** suggests a deliberate attempt to prevent unauthorized access to critical data. The discovery of a **steganographic message** in the *Wendigo* image, instructing the use of **Base64 and Vernam cipher encryption** with the key **"thewendigo"**, highlights the use of advanced concealment techniques that require further analysis.

Additionally, the **search history analysis** revealed multiple queries related to **Flunitrazepam detection in beverages**, indicating an awareness of drug detection methods. These searches, combined with **drug-related images** of **Flunitrazepam, Rohypnol, and Hypnodorm**, raise serious concerns about **potential involvement in drugging individuals or covering up such activities**. The suspect's active interest in how long Flunitrazepam remains detectable suggests either **an attempt to evade detection or knowledge of drug-facilitated crimes**.

The recovery of **chat logs from the *Crazy Bitches Threats* folder** provides insight into **threatening and coercive conversations** between the suspect and an individual named **Caitlyn Lin**. These conversations indicate **aggressive behavior, discussions of allegations, and potential efforts to intimidate or silence victims**. The presence of **resumes belonging to Vitoria and Anise De Boer** suggests that the suspect had access to **personal information, potentially for targeting individuals or luring them into vulnerable situations**.

Furthermore, the **PDF document titled "HARDLY HUMAN"** was found to contain **violent and misogynistic content**, including a disturbing statement that *a man has the right to assault any woman he wants*. The presence of such material raises concerns about the suspect's **ideological beliefs and potential motivations**. The discovery of **VeraCrypt and HxD installation files** indicates **possible encryption and data manipulation**, suggesting an attempt to **hide incriminating evidence or modify files before forensic recovery**.

Additionally, the **high-entropy file** discovered during the analysis suggests **encryption or compression**, requiring further decryption efforts to determine whether it contains **concealed criminal evidence**. The **tracking logs from Desktop-7O9F4FR** may provide a **timeline of user activity, file access, and potential attempts to erase or modify incriminating data**.

In conclusion, the combination of **hidden messages, encrypted files, suspicious search history, forensic countermeasure tools, aggressive conversations, and disturbing documents** strongly suggests that the suspect was **actively engaged in digital obfuscation, victim manipulation, and potential criminal planning**. Further forensic efforts should focus on **decrypting high-entropy files, analyzing metadata from logs and documents, and correlating chat messages with real-world events**. Additionally, **search history must be thoroughly reviewed for potential links to drug-facilitated crimes, covering tracks, or discussions of illicit activities**. The findings presented in this report serve as a **critical foundation for continued forensic examination and legal proceedings**.