Table of Contents

1. EXECUTIVE SUMMARY

This forensic investigation was conducted following allegations made by **Anise Famke DE BOER** against **Nicolas VALENTINO**, in which she claimed she was drugged and sexually assaulted at his studio on **January 25, 2024.** Digital evidence was examined from multiple devices seized from VALENTINO's residence, including a **damaged laptop (AXA/2)**, a destroyed **memory card (AXA/1)**, and an e**xternal hard drive (AXA/3)**. Analysis of these devices revealed key artefacts indicating potential premeditation, evidence tampering, and attempts to conceal digital records.

- **Key Findings:**

  Flunitrazepam Research Document (Artefact-1): A research paper detailing methods for detecting Flunitrazepam in beverages was recovered, raising concerns about prior knowledge of the drug's effects.

  Deleted JPEG File (Artefact-2): A file **(f0045957.jpg)** was in unallocated space, indicating intentional deletion. The absence of metadata suggests deliberate removal to obscure its origin.

  Hidden Audio Files (Artefact-4): Embedded recordings found within an RTF document contained conversations suggesting a pattern of predatory behaviour.

  WhatsApp Messages (Artefact-7): Chat logs included references to past incidents and inappropriate behaviour, with messages from Caitlyn LIN expressing prior concerns regarding VALENTINO's conduct.

  Encrypted SYSTEM File (Artefact-10): A hidden, VeraCrypt-encrypted file contained indecent images with explicit captions.

  Destroyed Storage Devices (Artefacts AXA/1 & AXA/2): The laptop exhibited impact marks inconsistent with accidental damage, and its SSD was completely pulverized. A memory card was found cut into two pieces, suggesting intentional destruction of potential evidence.

  Steganographic Data in Image Files (Artefact-8): A file **(wendigo.png)** contained concealed text referencing previous incidents, recovered through steganographic analysis.

  Flunitrazepam Image (Artefact-13): An image of Flunitrazepam packaging was found in the suspect's research directory, further reinforcing suspicions of intent and premeditation.

- **Overall Summary:**

  The findings suggest deliberate efforts to delete, encrypt, and conceal digital evidence. The presence of Flunitrazepam-related materials, deleted media, and encrypted files raises concerns about possible premeditation. Additionally, the physical destruction of key digital storage devices indicates an attempt to obstruct forensic recovery efforts.

2. VICTIM AND SUSPECT DETAILS

2.1. Victim Details

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

2.2. Involved Parties

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

2.3. Suspect Details

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

3. CIRCUMSTANCE OF INVESTIGATION

- 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.

- 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.

- 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.

- 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

- He and DE BOER were working late at the studio on adjusting and photographing an 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.

- The suspect states that DE BOER had not eaten during the evening, and that he thinks she may have taken cocaine early 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.

- 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.

- 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

- 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/Feb/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.

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

- 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.

- 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.

- 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'.

4. DESCRIPTION OF ABBREVIATIONS AND SHORT FORMS USED IN THE DOCUMENT

The document contains various technical terms, forensic investigation-related abbreviations, and industry-specific short forms that may be unfamiliar to some readers. Below is a list of these terms along with their explanations:

- **AXA/1, AXA/2, AXA/3** – References for digital exhibits (e.g., seized storage devices such as memory cards, laptops, and external drives).
- **CCTV (Closed-Circuit Television)** – A video surveillance system used for security and evidence collection.
- **NTFS (New Technology File System)** – A type of file system used in Windows operating systems to store and manage data.
- **exFAT (Extended File Allocation Table)** – A file system optimized for flash storage devices like USB drives and memory cards.
- **MD5 (Message Digest Algorithm 5)** – A cryptographic hashing algorithm used to verify data integrity.
- **SHA1 (Secure Hash Algorithm 1)** – Another hashing algorithm used for data verification and digital forensics.
- **Imaging:** A digital forensic technique used to collect and analyse evidence in a manner admissible in court.
- **Metadata:** Descriptive information about a file, including details such as creation date, modification history, author, and file type.
- **MIME Type:** A standard identifier for file formats (Multipurpose Internet Mail Extensions) that specifies a file's media type.
- **Encryption:** The process of encoding data to make it unreadable without proper authorization.
- **Decryption:** The act of converting encrypted data back into its original, readable form.
- **FTK (Forensic Toolkit Imager)** – A forensic software used for imaging and analysing digital evidence.
- **RTF (Rich Text Format)** – A document format that supports text and basic formatting but is not as complex as DOCX.
- **JPEG (Joint Photographic Experts Group)** – A common image format used for storing digital photos.
- **PNG (Portable Network Graphics)** – Another image format, often used for lossless image compression.
- **MFT (Master File Table)** – A data structure in NTFS that keeps track of all files and directories on a disk.

- **HXD (Hex Editor Tool)** – A tool used for examining and modifying raw binary data in digital files.
- **Hashing:** Hashing is a widely used technique in computer science that processes data through an algorithm to generate a unique hash value.
- **VeraCrypt** – Encryption software used to secure and hide sensitive files and data.
- **CyberChef** – A web-based forensic tool used for decoding, analysing, and transforming digital data.
- **Steganography** – The practice of hiding data within images or other files to conceal information.
- **ZIP (Compressed File Format)** – A file format used to compress and bundle multiple files into a single archive.

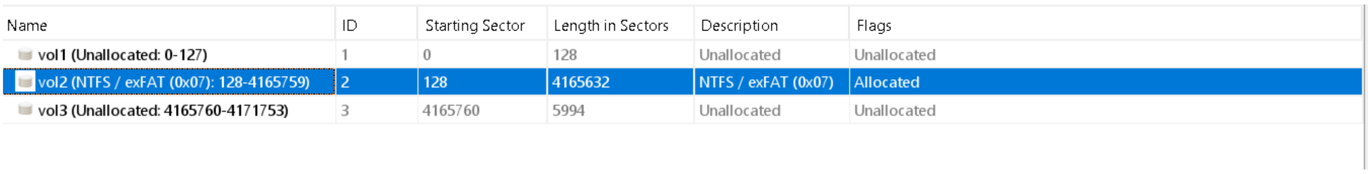
5. DETAILS OF EXHIBITS

5.1. Exhibit descriptions

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

6. TECHNICAL DETAILS OF THE EXHIBITS

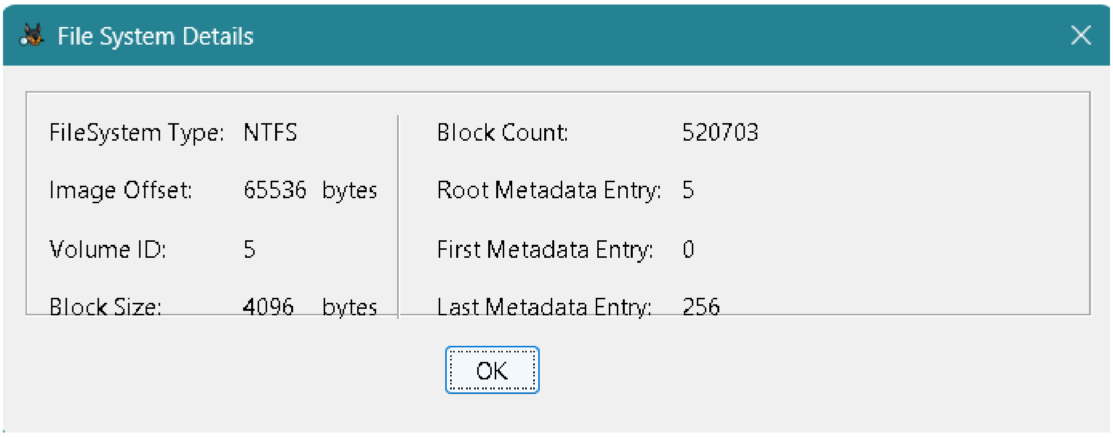
6.1. Exhibit AXA/3 – File System Details



Name	ID	Starting Sector	Length in Sectors	Description	Flags
vol1 (Unallocated: 0-127)	1	0	128	Unallocated	Unallocated
vol2 (NTFS / exFAT (0x07): 128-4165759)	2	128	4165632	NTFS / exFAT (0x07)	Allocated
vol3 (Unallocated: 4165760-4171753)	3	4165760	5994	Unallocated	Unallocated

Figure 1: The file systems on the device.

Figure 1 shows the file system corresponding to the laptop. It states the file system type is NTFS/exFAT, however, from further analysis, it is confirmed as NTFS, as shown below in figure 2. There are three volumes, however, only one of the three is allocated.



FileSystem Type:	NTFS	Block Count:	520703
Image Offset:	65536 bytes	Root Metadata Entry:	5
Volume ID:	5	First Metadata Entry:	0
Block Size:	4096 bytes	Last Metadata Entry:	256

Figure 2: The file system details of the device, confirming it uses NTFS.

From figure 1.2 the file type has been identified as NTFS. This information corresponds to volume 2, which is the main partition within the device. There are 4096 bytes in the block size, which is the default cluster size for NTFS. The number of bytes within this partition is 2,132,799,488 bytes, which is calculated by multiplying the block size by the block count, as shown below:
4,096 x 520703 = 2,132,799,488 bytes (or a 2.13 GB partition)

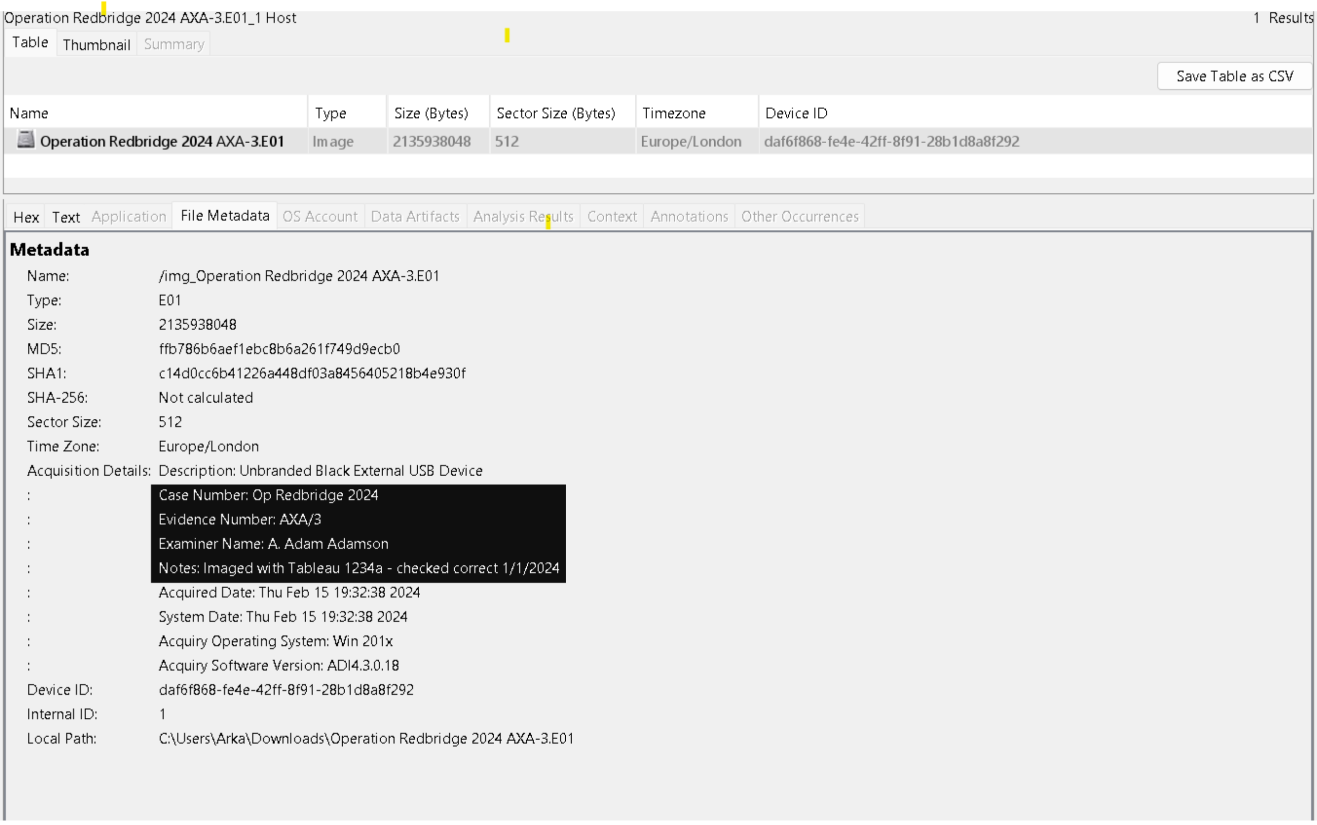
6.2. Exhibit AXA/3 – Operating System Details

- N.A.

7. PRESERVATION OF EVIDENCE

7.1. Exhibit AXA/3 - Imaging of Original Evidence

- **Imaged by:**
  The original exhibit, an unbranded black external USB device, was imaged by A. Adam Adamson on February 15, 2024. The acquisition was performed under Case Number: OpRedbridge 2024, with the evidence tagged as AXA/3.



Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID
Operation Redbridge 2024 AXA-3.E01	Image	2135938048	512	Europe/London	daf6f868-fe4e-42ff-8f91-28b1d8a8f292

Metadata

```
Name:                /img_Operation Redbridge 2024 AXA-3.E01
Type:                E01
Size:                2135938048
MD5:                 ffb786b6aef1ebc8b6a261f749d9ecb0
SHA1:                c14d0cc6b41226a448df03a8456405218b4e930f
SHA-256:             Not calculated
Sector Size:         512
Time Zone:           Europe/London
Acquisition Details: Description: Unbranded Black External USB Device
:                    Case Number: Op Redbridge 2024
:                    Evidence Number: AXA/3
:                    Examiner Name: A. Adam Adamson
:                    Notes: Imaged with Tableau 1234a - checked correct 1/1/2024
:                    Acquired Date: Thu Feb 15 19:32:38 2024
:                    System Date: Thu Feb 15 19:32:38 2024
:                    Acquiry Operating System: Win 201x
:                    Acquiry Software Version: ADI4.3.0.18
Device ID:           daf6f868-fe4e-42ff-8f91-28b1d8a8f292
Internal ID:         1
Local Path:          C:\Users\Arka\Downloads\Operation Redbridge 2024 AXA-3.E01
```

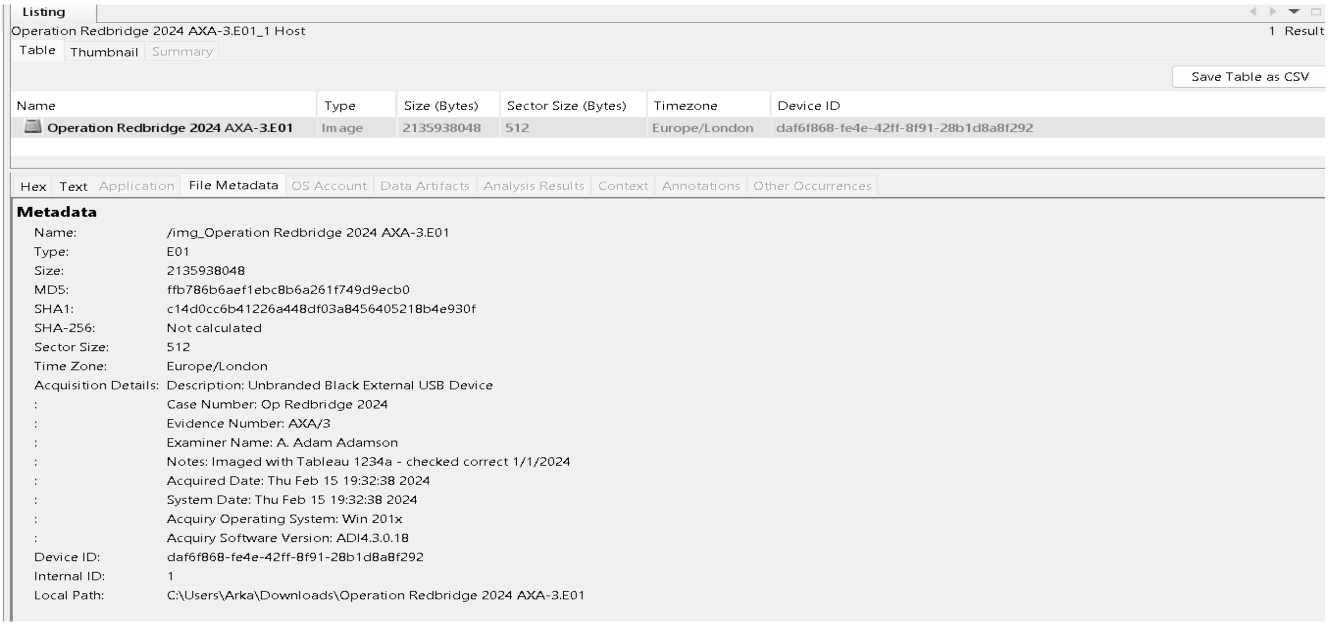
Figure 3: Information of Imaging.

- **Details of Imaging**

The imaging process was carried out using a Win 201x system, software version: ADI4.3.0.18 ensuring meticulous forensic preservation of the digital evidence.

- **Dual tool verification of the Image**

- **Autopsy:**



Operation Redbridge 2024 AXA-3.E01_1 Host

1 Result

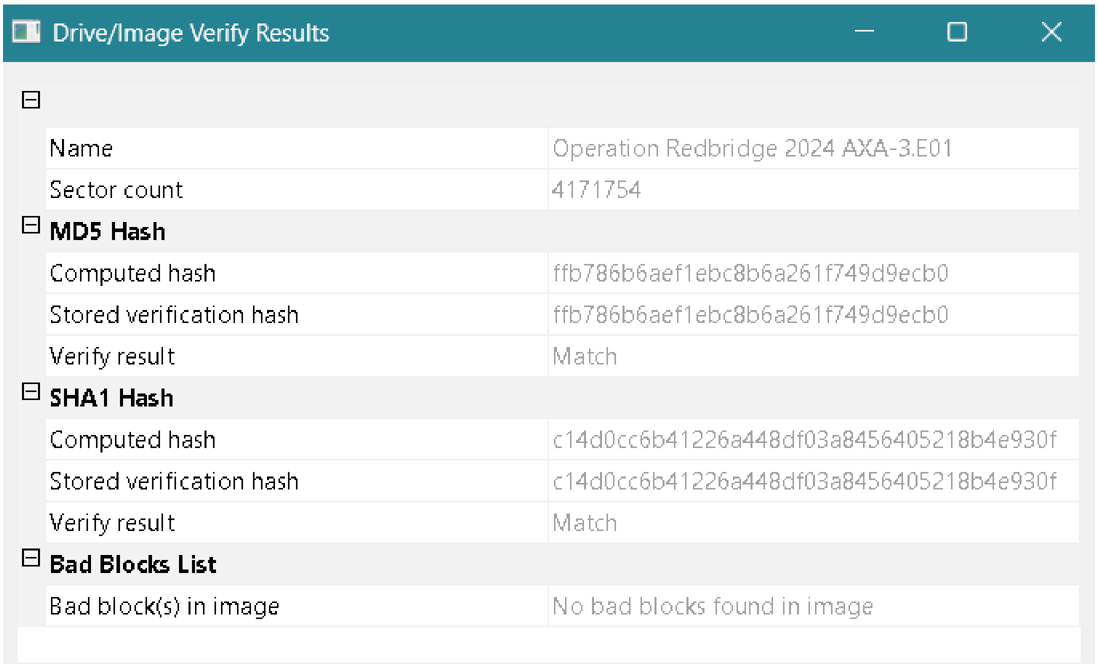
Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID
Operation Redbridge 2024 AXA-3.E01	Image	2135938048	512	Europe/London	daf6f868-fe4e-42ff-8f91-28b1d8a8f292

Metadata

```
Name:                 /img_Operation Redbridge 2024 AXA-3.E01
Type:                 E01
Size:                 2135938048
MD5:                  ffb786b6aef1ebc8b6a261f749d9ecb0
SHA1:                 c14d0cc6b41226a448df03a8456405218b4e930f
SHA-256:              Not calculated
Sector Size:          512
Time Zone:            Europe/London
Acquisition Details:  Description: Unbranded Black External USB Device
:                     Case Number: Op Redbridge 2024
:                     Evidence Number: AXA/3
:                     Examiner Name: A. Adam Adamson
:                     Notes: Imaged with Tableau 1234a - checked correct 1/1/2024
:                     Acquired Date: Thu Feb 15 19:32:38 2024
:                     System Date: Thu Feb 15 19:32:38 2024
:                     Acquiry Operating System: Win 201x
:                     Acquiry Software Version: ADI4.3.0.18
Device ID:            daf6f868-fe4e-42ff-8f91-28b1d8a8f292
Internal ID:          1
Local Path:           C:\Users\Arka\Downloads\Operation Redbridge 2024 AXA-3.E01
```

Figure 4: Verification with Autopsy.

- **FTK Imager:**



Name	Operation Redbridge 2024 AXA-3.E01
Sector count	4171754
MD5 Hash	
Computed hash	ffb786b6aef1ebc8b6a261f749d9ecb0
Stored verification hash	ffb786b6aef1ebc8b6a261f749d9ecb0
Verify result	Match
SHA1 Hash	
Computed hash	c14d0cc6b41226a448df03a8456405218b4e930f
Stored verification hash	c14d0cc6b41226a448df03a8456405218b4e930f
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Figure 5: Verification with FTK Imager.

The MD5 and the SHA1 verification hashes of the original evidence was provided as follows:

MD5 verification hash: ffb786b6aef1ebc8b6a261f749d9ecb0

SHA1 verification hash: c14d0cc6b41226a448df03a8456405218b4e930f

Procedures The evidence file called ‘Operation Redbridge 2024 AXA-3. E01’ was uploaded into both Autopsy and FTK imager- both of which are forensic imaging software. They provided verification hashes that match that of the original evidence file as shown in the screenshots in section.

8. TOOLS USED

8.1. Software Used:

- **Autopsy version 4.21.0:** This is an open-source digital forensics software which has been used to investigate the Generic Removable Hard Disk Drive (**Exhibit AXA/3)**.
- **Access Data FTK imager version 4.3.0.18:** This is a computer forensics software which only has been used to verify the image **(Exhibit AXA/3)** in this case study.
- **HXD Hex editor version 2.5.0.0 (x86-64):** This is a forensics investigation software which has been used in file structure analysis, forensic data recovery.
- **VeraCrypt version 1.26.7 (64-bit):** This is an encryption tool used to secure files and storage volumes, aiding in uncovering hidden and encrypted evidence during forensic analysis.

8.2. Websites Used:

- **https://cyberchef.immersivelabs.online-** This website has been used to decode hidden messages and extract concealed data.

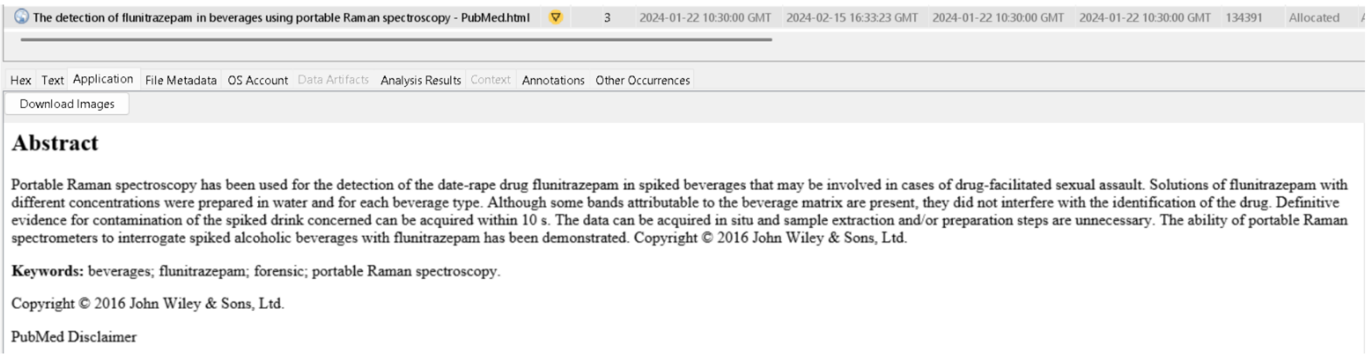
- **https://stylesuxx.github.io/steganography-** This website has been used to detect and extract hidden messages embedded within images and other digital files as part of forensic analysis.

- **https://en.wikipedia.org/wiki/List_of_file_signatures-** This website has been used to identify and verify file types by comparing hexadecimal signatures, aiding in detecting disguised or altered files during forensic analysis

9. RESULTS AND FINDINGS

9.1. Artefacts- 1

- **Location:**
  Operation Redbridge 2024 AXA-3. E01/vol_vol2/Research/The detection of flunitrazepam in beverages using portable Raman spectroscopy - PubMed_files/overlay-block.css



The detection of flunitrazepam in beverages using portable Raman spectroscopy - PubMed.html | 3 | 2024-01-22 10:30:00 GMT | 2024-02-15 16:33:23 GMT | 2024-01-22 10:30:00 GMT | 2024-01-22 10:30:00 GMT | 134391 | Allocated

Abstract

Portable Raman spectroscopy has been used for the detection of the date-rape drug flunitrazepam in spiked beverages that may be involved in cases of drug-facilitated sexual assault. Solutions of flunitrazepam with different concentrations were prepared in water and for each beverage type. Although some bands attributable to the beverage matrix are present, they did not interfere with the identification of the drug. Definitive evidence for contamination of the spiked drink concerned can be acquired within 10 s. The data can be acquired in situ and sample extraction and/or preparation steps are unnecessary. The ability of portable Raman spectrometers to interrogate spiked alcoholic beverages with flunitrazepam has been demonstrated. Copyright © 2016 John Wiley & Sons, Ltd.

Keywords: beverages; flunitrazepam; forensic; portable Raman spectroscopy.

Copyright © 2016 John Wiley & Sons, Ltd.

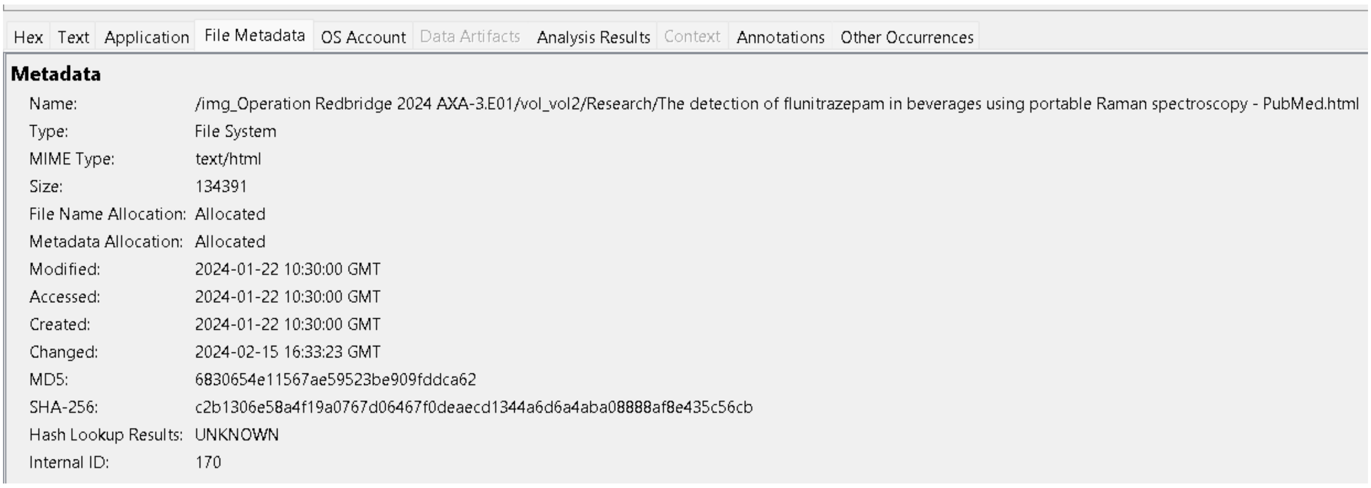
PubMed Disclaimer

Figure: 1.1

- **The Reason Document 1 is Suspicious:**

  The suspect’s behaviour, searching for flunitrazepam and saving an article of detecting in beverages, raises serious concerns. Flunitrazepam, a powerful sedative, is often associated with crimes like sexual assault, and the suspect's interest in this could indicate possible involvement in such activities (pictures of the medicine in figure 13.1 & 13.2). Saving the article suggests the information was intentionally kept for future use, hinting at premeditation. Their focus on portable Raman spectroscopy, a detection tool used by law enforcement, could point to efforts to understand and evade forensic methods. These actions suggest a troubling intent and a desire to avoid detection.

- **The Meta-Data for Document 1 is as follows:**



Metadata

Name:	/img_Operation Redbridge 2024 AXA-3.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 10:30:00 GMT
Accessed:	2024-01-22 10:30:00 GMT
Created:	2024-01-22 10:30:00 GMT
Changed:	2024-02-15 16:33:23 GMT
MD5:	6830654e11567ae59523be909fddca62
SHA-256:	c2b1306e58a4f19a0767d06467f0deaecd1344a6d6a4aba08888af8e435c56cb
Hash Lookup Results:	UNKNOWN
Internal ID:	170

Figure: 1.2

- **Suspected Metadata explanation**

  The file’s creation, modification, and access timestamps all matching (2024-01-22 10:30:00 GMT) suggests the file may have been copied or moved to hide its true history. This is not typical as these timestamps are usually different. The "Changed" date of 2024-02-15 16:33:23 GMT is far from the other timestamps, indicating possible metadata manipulation to make the file seem less suspicious. Modifying the MFT entry further points to tampering or an attempt to alter the file's origin. The file is marked as 'Hidden' and 'Not Content Indexed', meaning it is harder to find and analyse, likely done to avoid detection. The file has a parent MFT entry (Entry: 71, Sequence: 1), and any irregularities here suggest an effort to conceal the file's true path or source. In summary, the file shows clear signs of tampering and deliberate steps taken to avoid detection.

9.2. Artefacts- 2

- **Location:**
  Operation Redbridge 2024 AXA-3. E01/vol_vol2/$CarvedFiles/1/f0045957.jpg

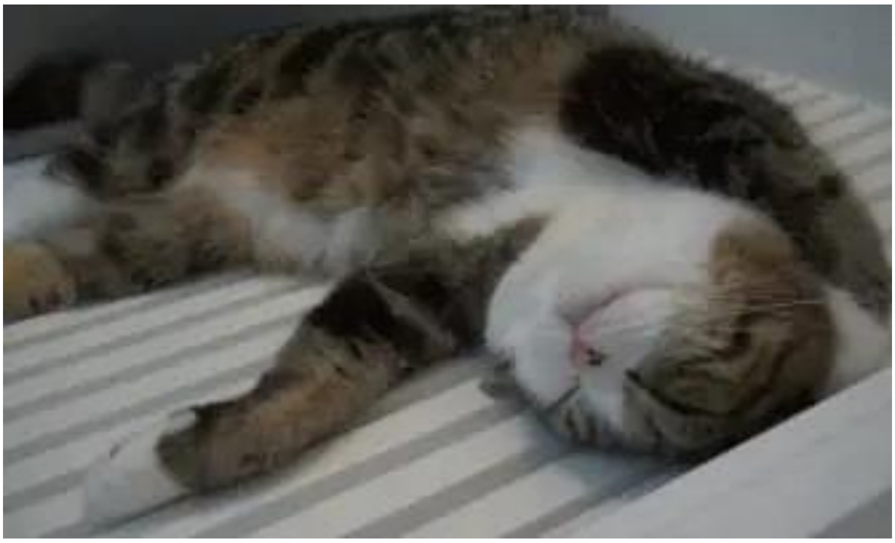
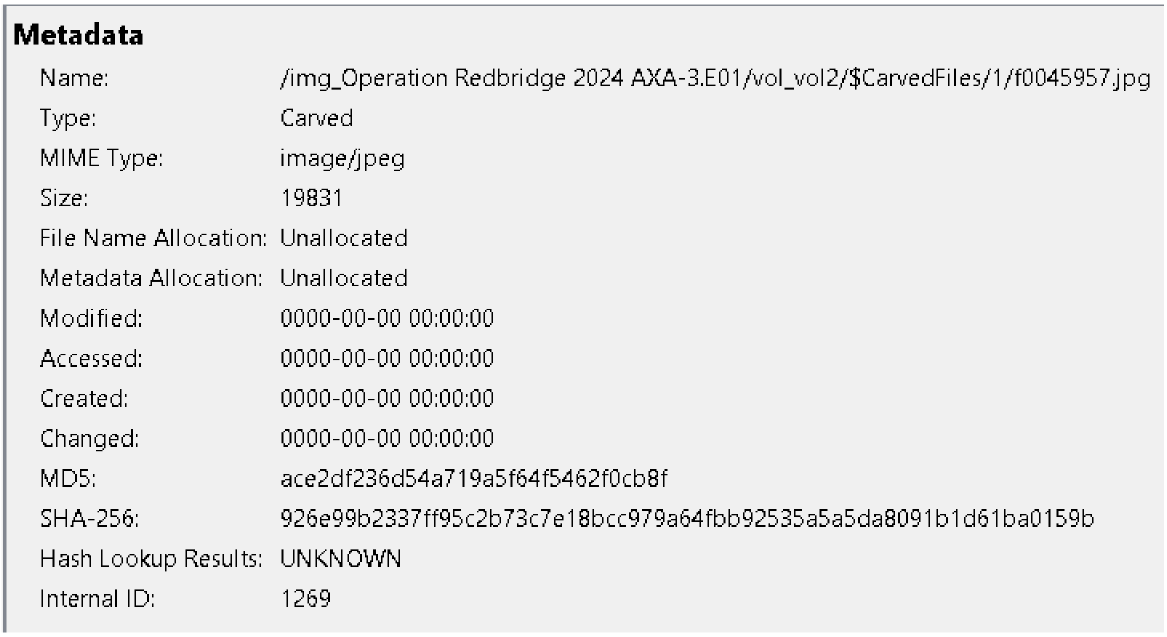


Figure: 2.1

- **Reason Why This Evidence is Suspicious:**
  The file (f0045957.jpg) is a carved JPEG image recovered from unallocated space, which suggests it was intentionally deleted or hidden. The fact that it was found in a folder named $CarvedFiles indicates it was recovered during forensic analysis, further raising suspicions about its purpose. While the content of the image is not explicitly described, the context of the case (involving allegations of sexual assault and the suspect's suspicious behaviour) makes the presence of a hidden or deleted image file highly concerning. If the image contains indecent or inappropriate content (e.g., related to the "cat" terminology rule, which may be used as code for indecent material), it could be evidence of illegal activity.
  The unknown hash and lack of timestamps further suggest the file may have been altered or concealed to avoid detection, which is consistent with the suspect's other actions (e.g., destroying the memory card and damaging the laptop).

- **The Meta-Data for Artefacts-2 is as follows:**



Metadata

Name:	/img_Operation Redbridge 2024 AXA-3.E01/vol_vol2/$CarvedFiles/1/f0045957.jpg
Type:	Carved
MIME Type:	image/jpeg
Size:	19831
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
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:	ace2df236d54a719a5f64f5462f0cb8f
SHA-256:	926e99b2337ff95c2b73c7e18bcc979a64fbb92535a5a5da8091b1d61ba0159b
Hash Lookup Results:	UNKNOWN
Internal ID:	1269

Figure: 2.2

- **Suspected Metadata explanation**

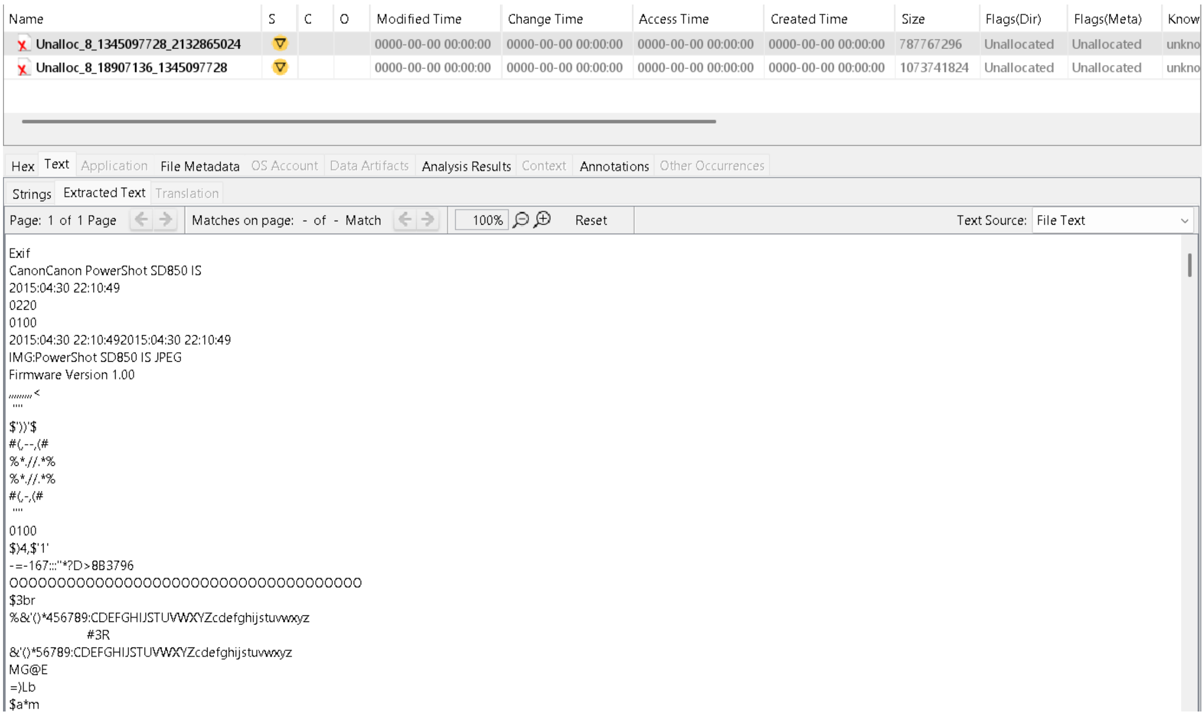
  The creation, modification, accessed, and changed timestamps are all set to 0000-00-00 0000000, which is highly unusual and suggests that the file's metadata has been manipulated or wiped. This could indicate an attempt to hide the file's true origin or when it was last accessed or modified. The file is marked as unallocated in both file name and metadata allocation, meaning it was recovered from unallocated space on the disk. This suggests the file was deleted or hidden and later carved out during forensic analysis. The absence of timestamps further supports the possibility of metadata forgery to obscure the file's history.

  The file's unallocated status and the lack of timestamps indicate that the suspect may have attempted to delete or hide the file to evade detection. This is a common anti-forensic technique used to make it harder for investigators to recover or trace the file.

9.3. Artefacts- 3

- **Location:**

  Operation Redbridge 2024 AXA-3.E01/vol_vol2/$Unalloc/Unalloc_8_1345097728_2132865024



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Know
Unalloc_8_1345097728_2132865024	▽			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	787767296	Unallocated	Unallocated	unkno
Unalloc_8_18907136_1345097728	▽			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1073741824	Unallocated	Unallocated	unkno

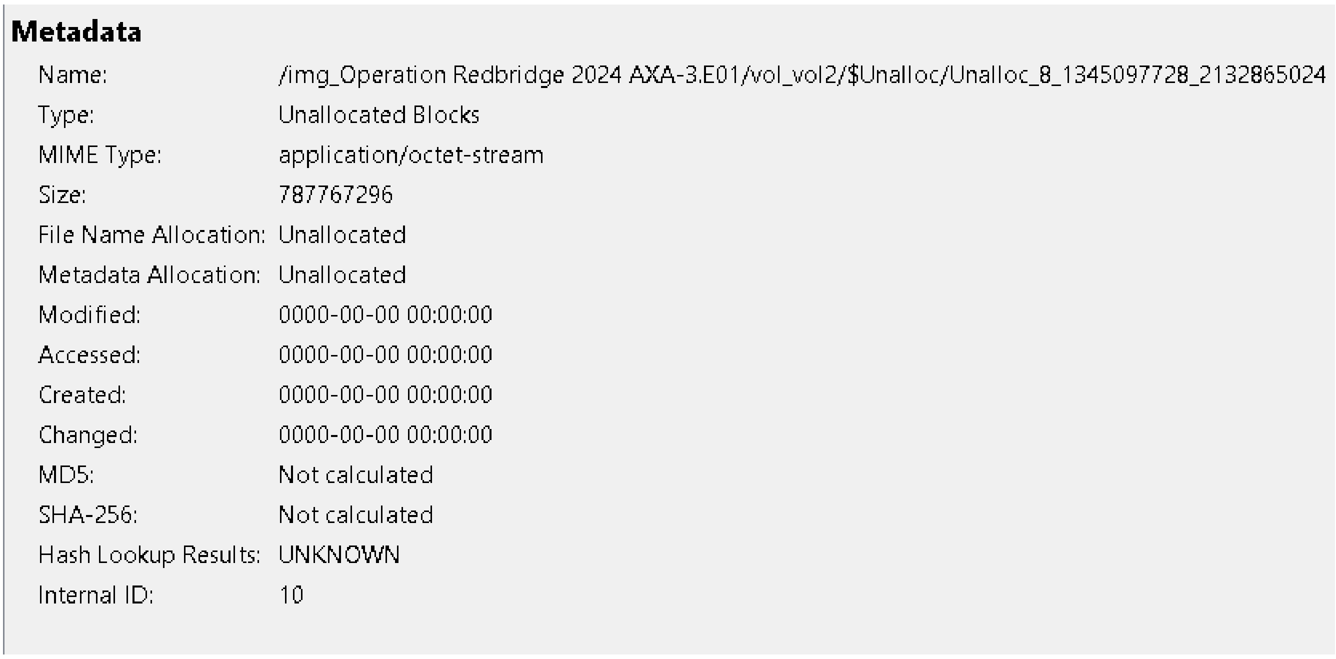
```
Exif
CanonCanon PowerShot SD850 IS
2015:04:30 22:10:49
0220
0100
2015:04:30 22:10:492015:04:30 22:10:49
IMG:PowerShot SD850 IS JPEG
Firmware Version 1.00
,,,,,,,,<
 ''''

$'))'$
#(,--,(#
%*.//.*%
%*.//.*%
#(,-,(#
 ''''

0100
$)4,$'1'
-=-167:::''*?D>8B3796
OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
$3br
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
                  #3R
&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
MG@E
=)Lb
$a*m
```

Figure: 3.1

- **Reason Why This Evidence is Suspicious:**

  The data is from unallocated space, which suggests intentional deletion. A memory card was found destroyed (AXA/1) this could indicate attempts to hide or destroy evidence. The EXIF in extracted text suggests image files but the large file size (around 750 MB) indicates multiple images or video

- **The Meta-Data for Artefacts-3 is as follows:**



Metadata

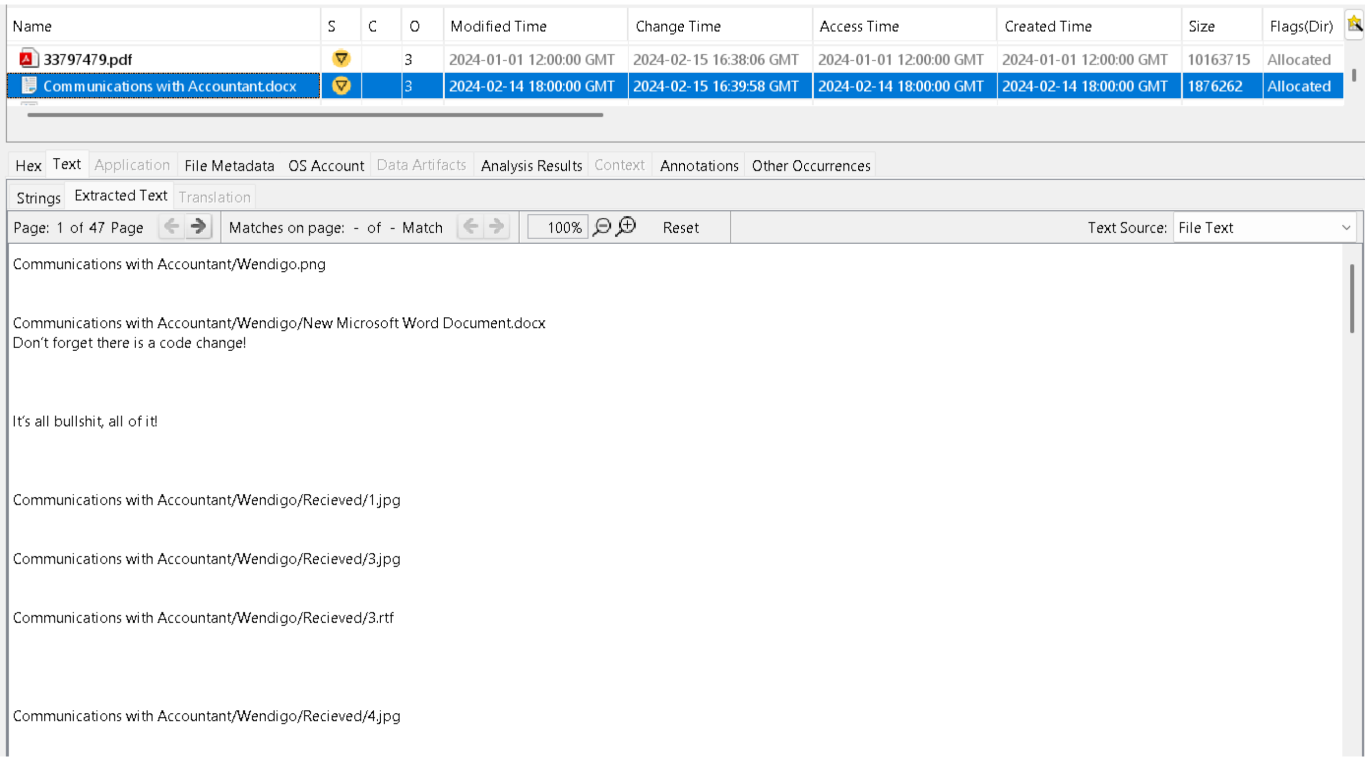
Name:	/img_Operation Redbridge 2024 AXA-3.E01/vol_vol2/$Unalloc/Unalloc_8_1345097728_2132865024
Type:	Unallocated Blocks
MIME Type:	application/octet-stream
Size:	787767296
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	0000-00-00 00:00:00
Accessed:	0000-00-00 00:00:00
Created:	0000-00-00 00:00:00
Changed:	0000-00-00 00:00:00
MD5:	Not calculated
SHA-256:	Not calculated
Hash Lookup Results:	UNKNOWN
Internal ID:	10

Figure: 3.2

9.4 Artefacts- 4

- **Location:**

  Operation Redbridge 2024 AXA-3.E01/vol_vol2/Accountancy Details/Communications with Accountant.docx

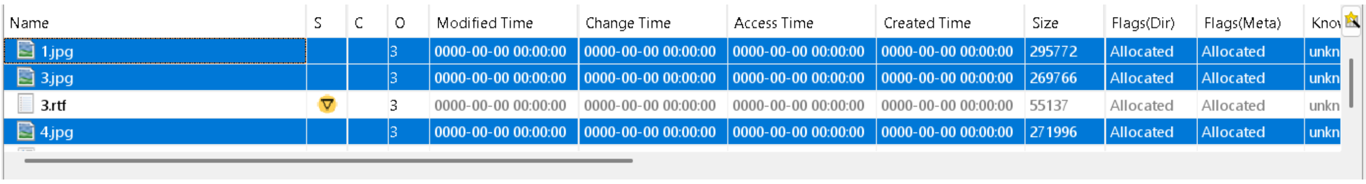


Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
33797479.pdf	▽		3	2024-01-01 12:00:00 GMT	2024-02-15 16:38:06 GMT	2024-01-01 12:00:00 GMT	2024-01-01 12:00:00 GMT	10163715	Allocated
Communications with Accountant.docx	▽		3	2024-02-14 18:00:00 GMT	2024-02-15 16:39:58 GMT	2024-02-14 18:00:00 GMT	2024-02-14 18:00:00 GMT	1876262	Allocated

Text Source: File Text

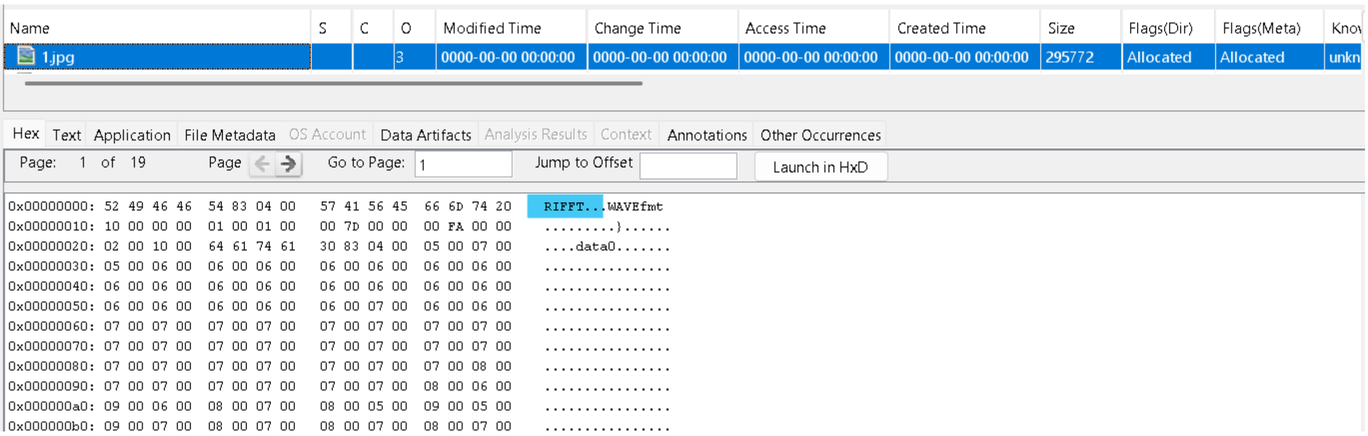
```
Communications with Accountant/Wendigo.png


Communications with Accountant/Wendigo/New Microsoft Word Document.docx
Don't forget there is a code change!



It's all bullshit, all of it!



Communications with Accountant/Wendigo/Recieved/1.jpg


Communications with Accountant/Wendigo/Recieved/3.jpg


Communications with Accountant/Wendigo/Recieved/3.rtf




Communications with Accountant/Wendigo/Recieved/4.jpg
```

Figure: 4.1



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Know
1.jpg			3	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	295772	Allocated	Allocated	unkn
3.jpg			3	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	269766	Allocated	Allocated	unkn
3.rtf	▽		3	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	55137	Allocated	Allocated	unkn
4.jpg			3	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	271996	Allocated	Allocated	unkn

Figure: 4.2



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Know
1.jpg			3	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	295772	Allocated	Allocated	unkn

Go to Page: 1

```
0x00000000: 52 49 46 46  54 83 04 00  57 41 56 45  66 6D 74 20   RIFFT...WAVEfmt
0x00000010: 10 00 00 00  01 00 01 00  00 7D 00 00  00 FA 00 00   .........}......
0x00000020: 02 00 10 00  64 61 74 61  30 83 04 00  05 00 07 00   ....data0.......
0x00000030: 05 00 06 00  06 00 06 00  06 00 06 00  06 00 06 00   ................
0x00000040: 06 00 06 00  06 00 06 00  06 00 06 00  06 00 06 00   ................
0x00000050: 06 00 06 00  06 00 06 00  06 00 07 00  06 00 06 00   ................
0x00000060: 07 00 07 00  07 00 07 00  07 00 07 00  07 00 07 00   ................
0x00000070: 07 00 07 00  07 00 07 00  07 00 07 00  07 00 07 00   ................
0x00000080: 07 00 07 00  07 00 07 00  07 00 07 00  07 00 08 00   ................
0x00000090: 07 00 07 00  07 00 07 00  07 00 07 00  08 00 06 00   ................
0x000000a0: 09 00 06 00  08 00 07 00  08 00 05 00  09 00 05 00   ................
0x000000b0: 09 00 07 00  08 00 07 00  08 00 07 00  08 00 07 00   ................
```

Figure: 4.3

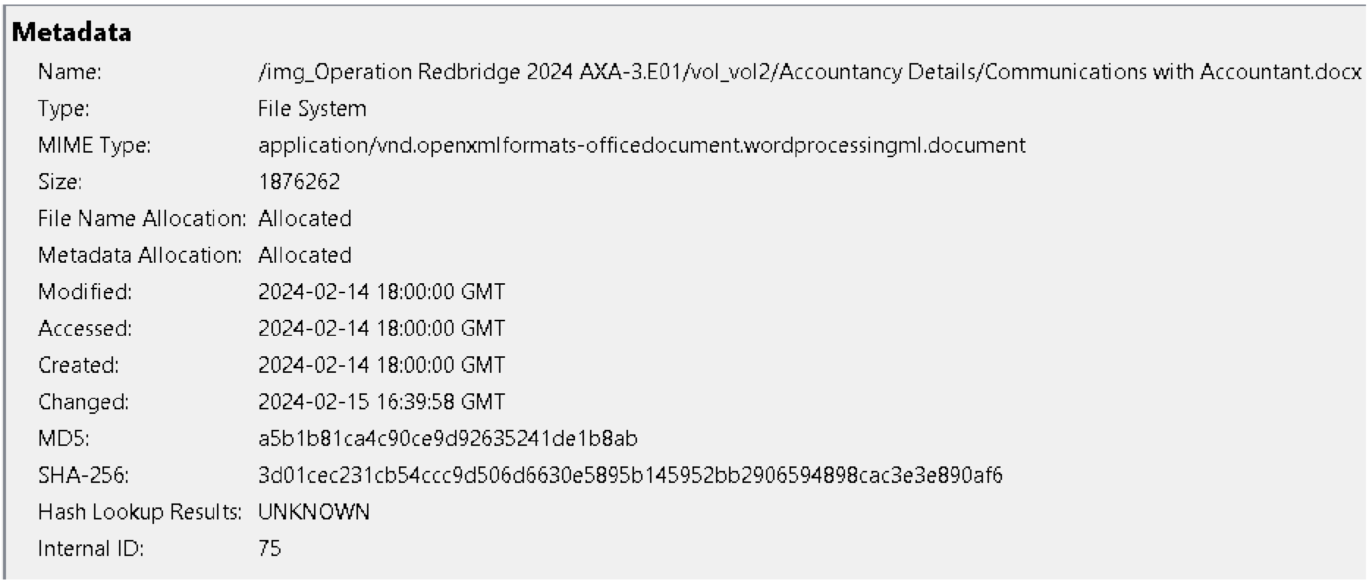
- **Reason Why This Evidence is Suspicious:**
  The extension of the highlighted 3 files **(Figure: 4.2)** shows this is a jpg which found in the document named **“Communications with Accountant” (Figure 4.1)** but the metadata in **(figure:4.5, 4.6 & 4.7)** shows these are audio files. We managed to verify Waveform Audio file format’s signature hex code is same as the hex code of these files. We changed the file extension from jpg to mp3 and managed to recover the audio file.

The audio we recovered was-

- “She is hot. You think you can get her like you get the last girl, I want to see that.” **(Found from 1.jpg)**
- “She is amazing, better even than the last one. You are devil.” **(Found from 3.jpg)**
- “You made her do it, didn’t you? Tell me you took more pictures.” **(Found from 4.jpg)**

We suspect that the document VALENTINO received from someone named **"Accountant"** contains information about a past incident involving another girl that VALENTINO was involved in. This assumption is based on a few WhatsApp chats **(Figure 7.1, 7.2 & 7.3)** in which VALENTINO mentioned the same situation.

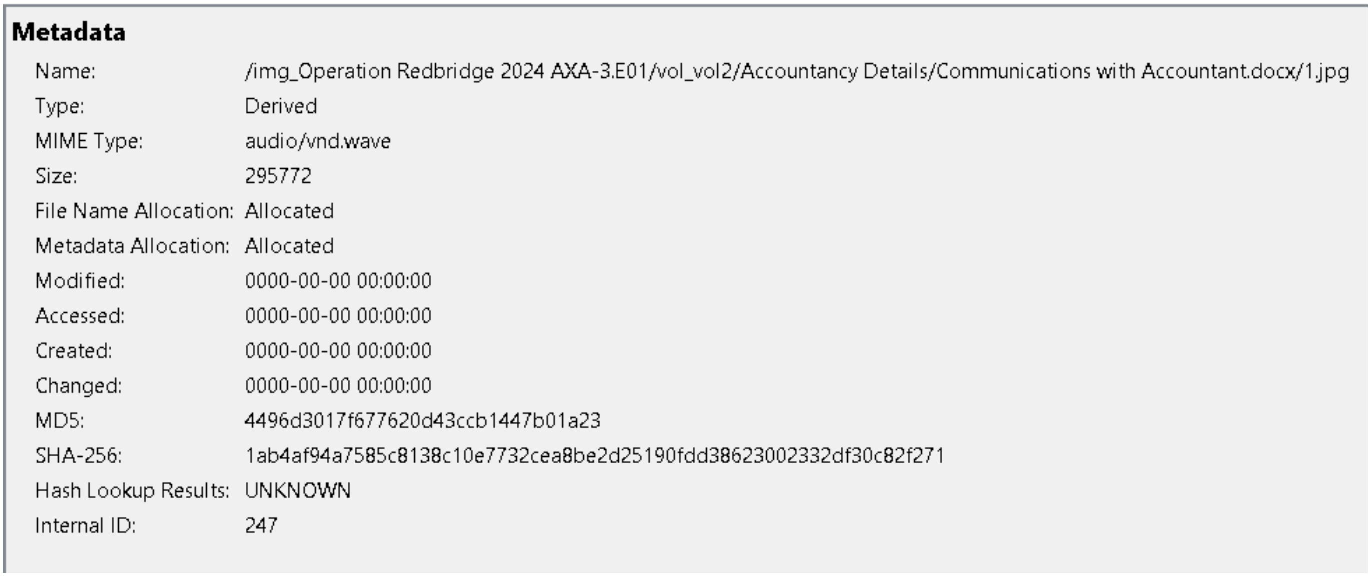
- **The Meta-Data for Artefacts-4 is as follows:**



Metadata

Name:	/img_Operation Redbridge 2024 AXA-3.E01/vol_vol2/Accountancy Details/Communications with Accountant.docx
Type:	File System
MIME Type:	application/vnd.openxmlformats-officedocument.wordprocessingml.document
Size:	1876262
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2024-02-14 18:00:00 GMT
Accessed:	2024-02-14 18:00:00 GMT
Created:	2024-02-14 18:00:00 GMT
Changed:	2024-02-15 16:39:58 GMT
MD5:	a5b1b81ca4c90ce9d92635241de1b8ab
SHA-256:	3d01cec231cb54ccc9d506d6630e5895b145952bb2906594898cac3e3e890af6
Hash Lookup Results:	UNKNOWN
Internal ID:	75

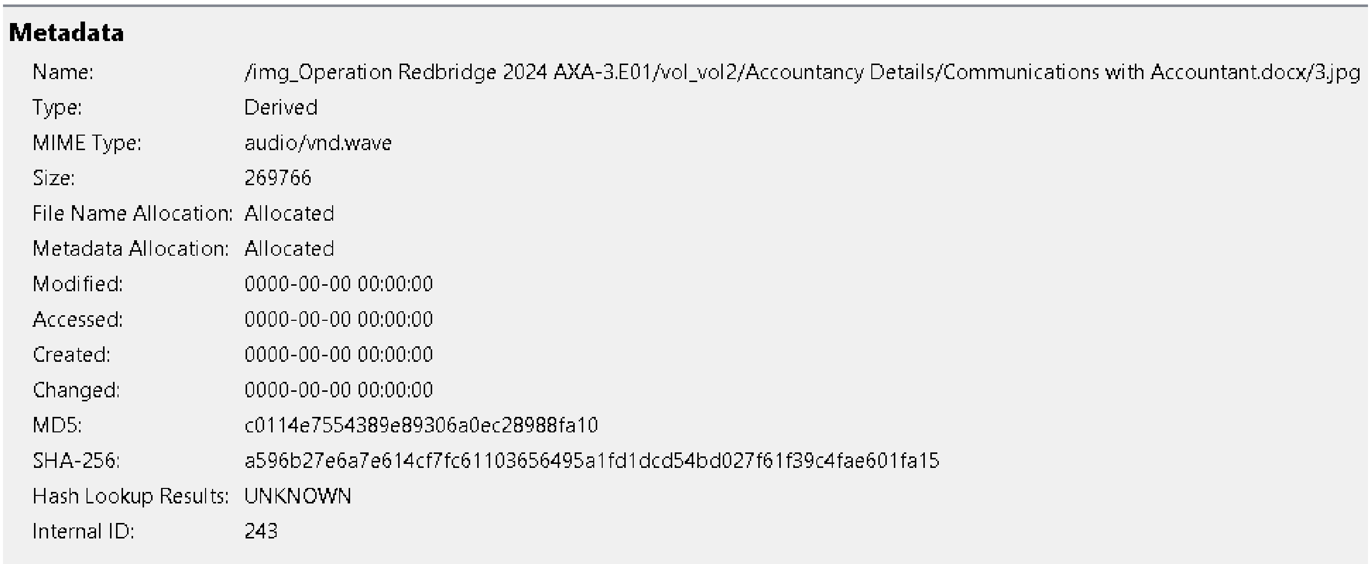
Figure: 4.4



Metadata

Name:	/img_Operation Redbridge 2024 AXA-3.E01/vol_vol2/Accountancy Details/Communications with Accountant.docx/1.jpg
Type:	Derived
MIME Type:	audio/vnd.wave
Size:	295772
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:	4496d3017f677620d43ccb1447b01a23
SHA-256:	1ab4af94a7585c8138c10e7732cea8be2d25190fdd38623002332df30c82f271
Hash Lookup Results:	UNKNOWN
Internal ID:	247

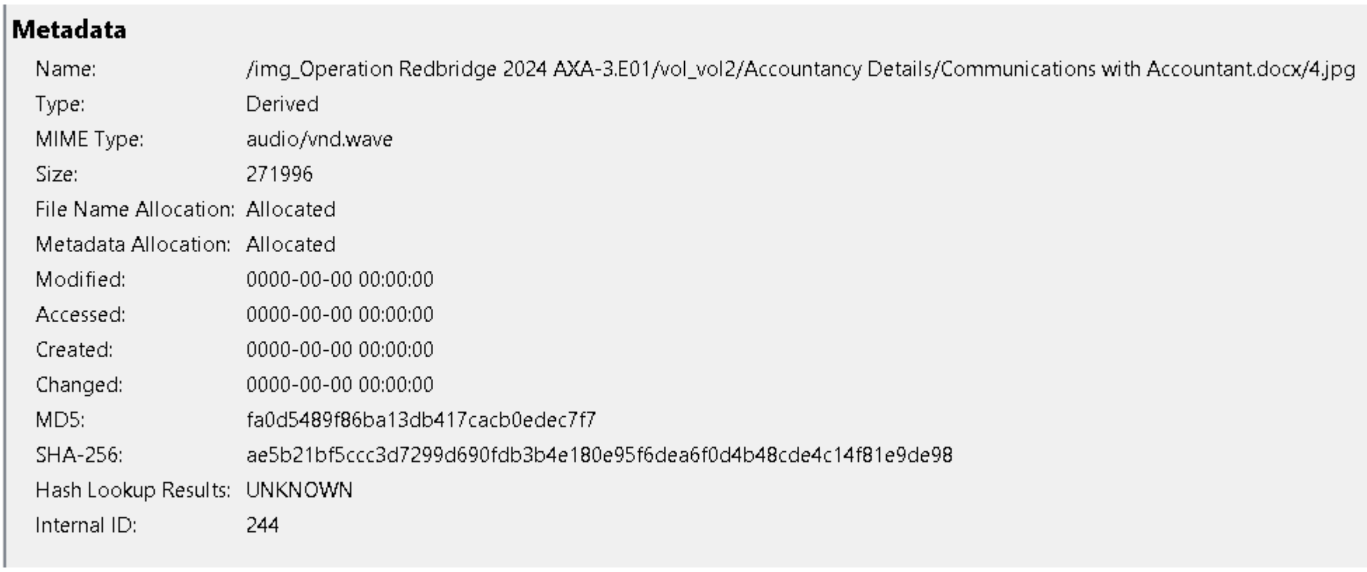
Figure: 4.5



Metadata

Name:	/img_Operation Redbridge 2024 AXA-3.E01/vol_vol2/Accountancy Details/Communications with Accountant.docx/3.jpg
Type:	Derived
MIME Type:	audio/vnd.wave
Size:	269766
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:	c0114e7554389e89306a0ec28988fa10
SHA-256:	a596b27e6a7e614cf7fc61103656495a1fd1dcd54bd027f61f39c4fae601fa15
Hash Lookup Results:	UNKNOWN
Internal ID:	243

Figure: 4.6



Metadata

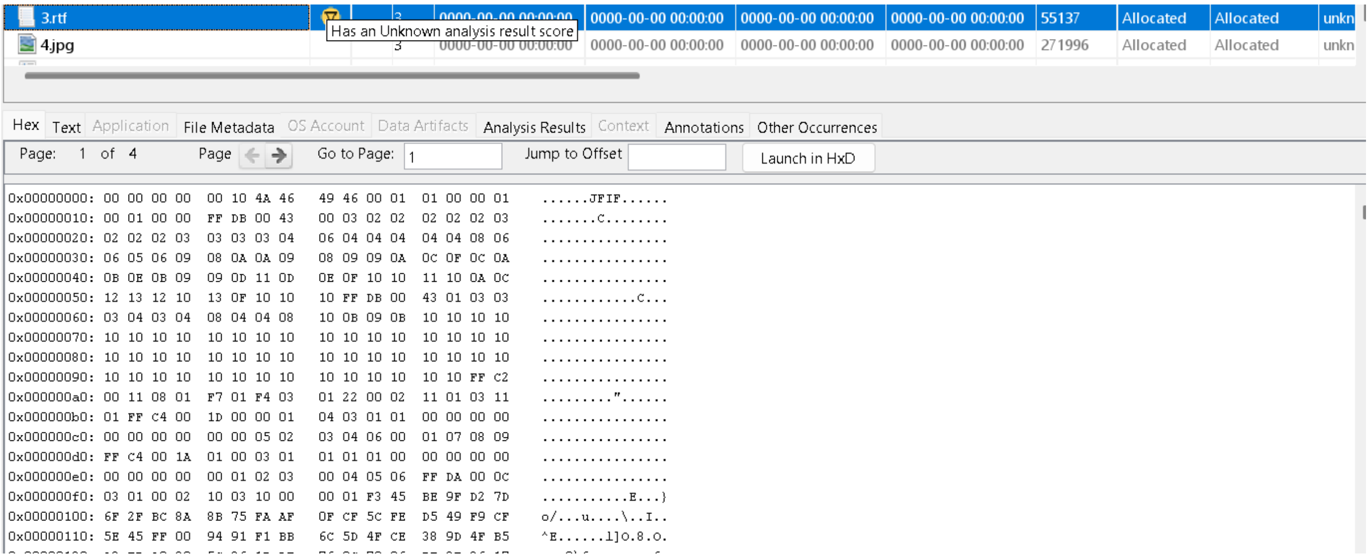
Name:	/img_Operation Redbridge 2024 AXA-3.E01/vol_vol2/Accountancy Details/Communications with Accountant.docx/4.jpg
Type:	Derived
MIME Type:	audio/vnd.wave
Size:	271996
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	0000-00-00 00:00:00
Accessed:	0000-00-00 00:00:00
Created:	0000-00-00 00:00:00
Changed:	0000-00-00 00:00:00
MD5:	fa0d5489f86ba13db417cacb0edec7f7
SHA-256:	ae5b21bf5ccc3d7299d690fdb3b4e180e95f6dea6f0d4b48cde4c14f81e9de98
Hash Lookup Results:	UNKNOWN
Internal ID:	244

Figure: 4.7

9.5 Artefacts-5

- **Location:**

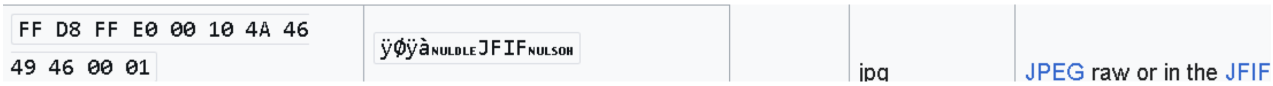
Operation Redbridge 2024 AXA-3.E01/vol_vol2/Accountancy Details/Communications with Accountant.docx/3.rtf



3.rtf	Has an Unknown analysis result score		3	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	55137	Allocated	Allocated	unkn
4.jpg			3	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	271996	Allocated	Allocated	unkn

```
0x00000000: 00 00 00 00  00 10 4A 46  49 46 00 01  01 00 00 01   ......JFIF......
0x00000010: 00 01 00 00  FF DB 00 43  00 03 02 02  02 02 02 03   .......C........
0x00000020: 02 02 02 03  03 03 03 04  06 04 04 04  04 04 08 06   ................
0x00000030: 06 05 06 09  08 0A 0A 09  08 09 09 0A  0C 0F 0C 0A   ................
0x00000040: 0B 0E 0B 09  09 0D 11 0D  0E 0F 10 10  11 10 0A 0C   ................
0x00000050: 12 13 12 10  13 0F 10 10  10 FF DB 00  43 01 03 03   ............C...
0x00000060: 03 04 03 04  08 04 04 08  10 0B 09 0B  10 10 10 10   ................
0x00000070: 10 10 10 10  10 10 10 10  10 10 10 10  10 10 10 10   ................
0x00000080: 10 10 10 10  10 10 10 10  10 10 10 10  10 10 10 10   ................
0x00000090: 10 10 10 10  10 10 10 10  10 10 10 10  10 10 FF C2   ................
0x000000a0: 00 11 08 01  F7 01 F4 03  01 22 00 02  11 01 03 11   ........."......
0x000000b0: 01 FF C4 00  1D 00 00 01  04 03 01 01  00 00 00 00   ................
0x000000c0: 00 00 00 00  00 00 05 02  03 04 06 00  01 07 08 09   ................
0x000000d0: FF C4 00 1A  01 00 03 01  01 01 01 00  00 00 00 00   ................
0x000000e0: 00 00 00 00  00 01 02 03  00 04 05 06  FF DA 00 0C   ................
0x000000f0: 03 01 00 02  10 03 10 00  00 01 F3 45  BE 9F D2 7D   ...........E...}
0x00000100: 6F 2F BC 8A  8B 75 FA AF  0F CF 5C FE  D5 49 F9 CF   o/...u....\..I..
0x00000110: 5E 45 FF 00  94 91 F1 BB  6C 5D 4F CE  38 9D 4F B5   ^E......l]O.8.O.
```

Figure: 5.1



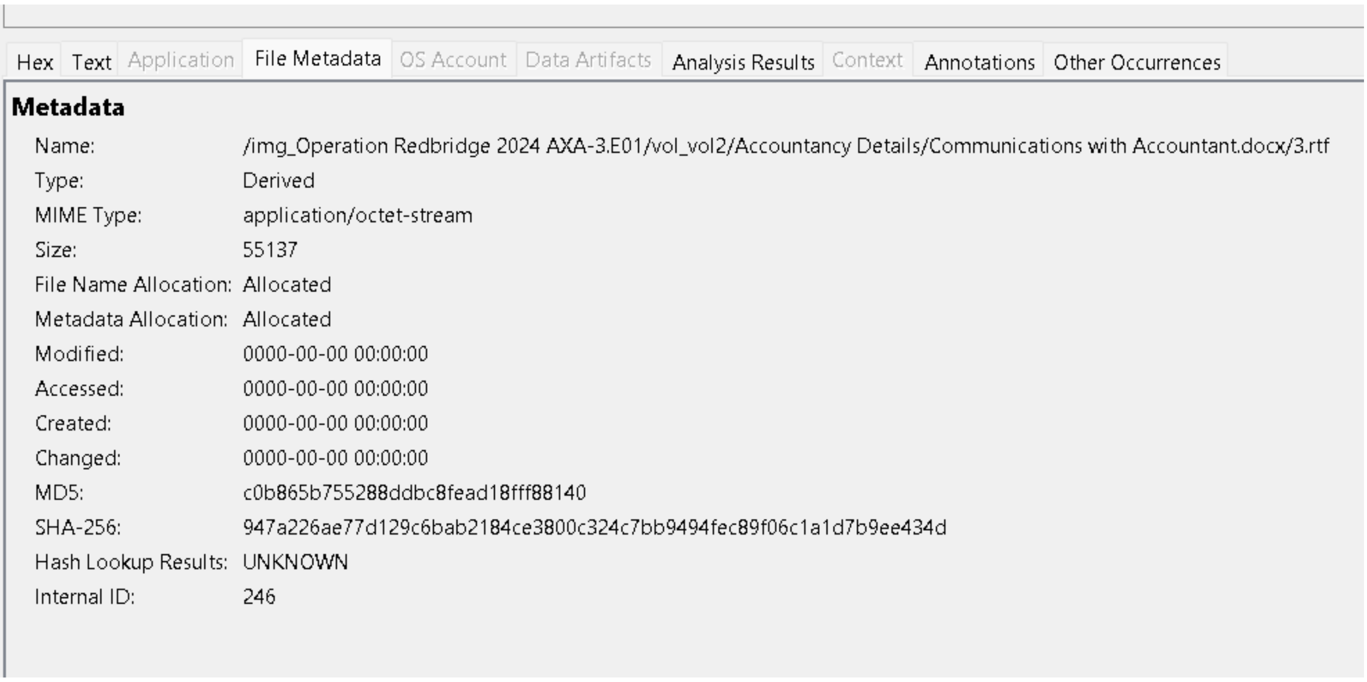
FF D8 FF E0 00 10 4A 46 49 46 00 01	ÿØÿàNULDLEJFIFNULSOH		jpg	JPEG raw or in the JFIF

Figure: 5.2

Figure: 5.3

- **Reason Why This Evidence is Suspicious:**
  We examined the file alongside the other JPG files, but it was displaying as an RTF file type. Using Autopsy and a hex code editor, we confirmed that the RTF file was actually an image. However, the file's format signature in hex code did not correspond to that of a standard image file, indicating that the hex code had been manipulated. Subsequently, we modified the hex code **(as shown in the figure: 5.2)** to fix the file. Afterwards, we recovered the picture **(Figure: 5.3).**

- **The Meta-Data for Artefacts-5 is as follows:**



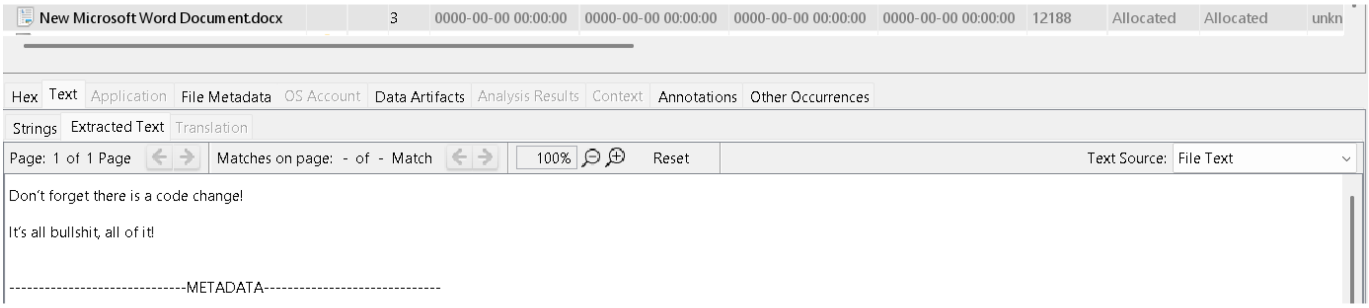
Metadata

Name:	/img_Operation Redbridge 2024 AXA-3.E01/vol_vol2/Accountancy Details/Communications with Accountant.docx/3.rtf
Type:	Derived
MIME Type:	application/octet-stream
Size:	55137
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:	c0b865b755288ddbc8fead18fff88140
SHA-256:	947a226ae77d129c6bab2184ce3800c324c7bb9494fec89f06c1a1d7b9ee434d
Hash Lookup Results:	UNKNOWN
Internal ID:	246

Figure: 5.4

9.6 Artefacts- 6

- **Location:** Operation Redbridge 2024 AXA-3.E01/vol_vol2/Accountancy Details/Communications with Accountant.docx/New Microsoft Word Document.docx



New Microsoft Word Document.docx	3	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	12188	Allocated	Allocated	unkn

Don't forget there is a code change!

It's all bullshit, all of it!

-----------------------------METADATA-----------------------------

Figure:6.1

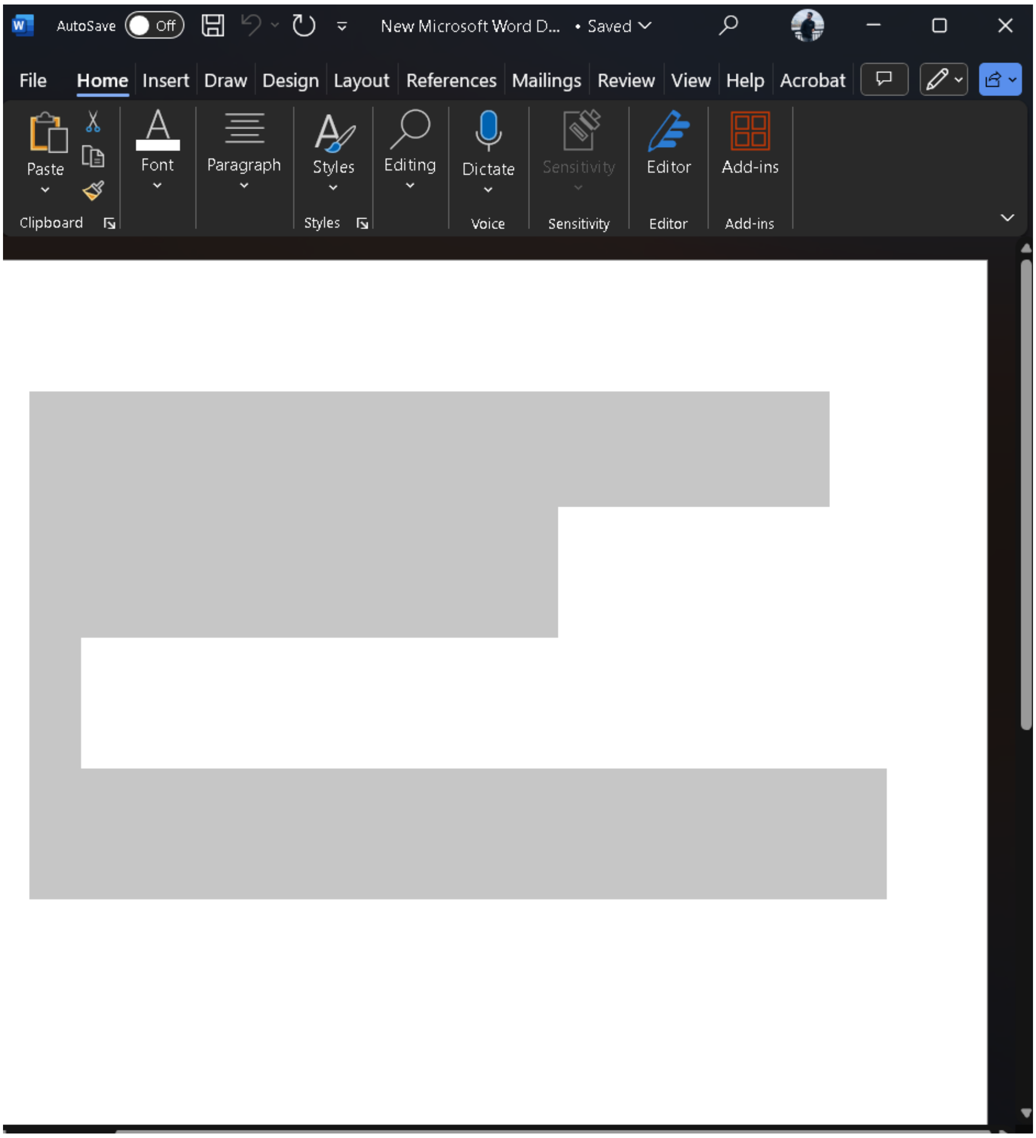
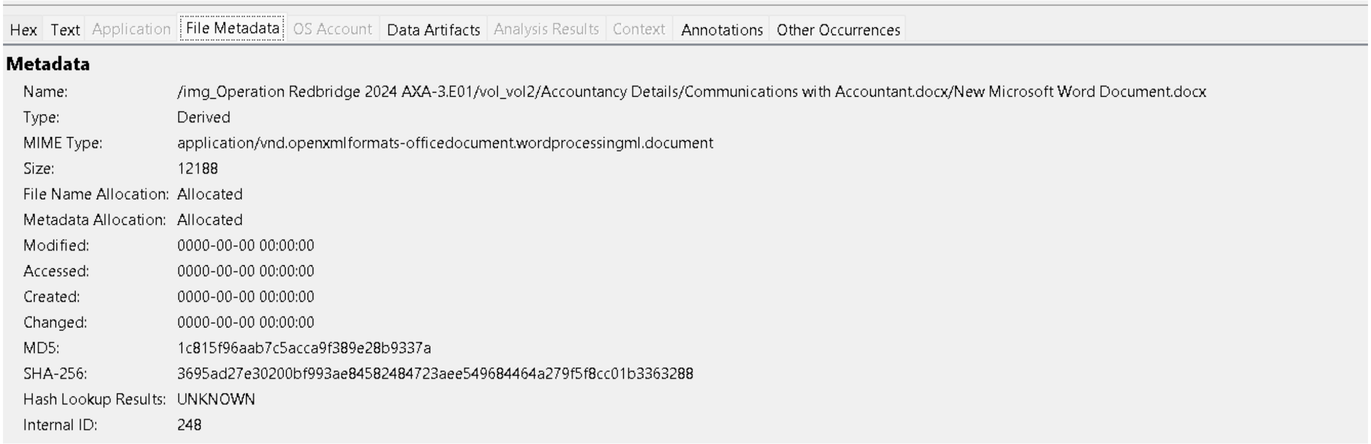


Figure: 6.2

- **Reason Why This Evidence is Suspicious:**
  We came across a document file and initially opened it in Autopsy, where it displayed the text **"Don't forget there is a code change, it's all bullshit all of it "(Figure 6.1)**. However, when we extracted and opened the file directly, it appeared blank. To investigate further, pressed **"CTRL+A"** to select all the content, revealing that the text had been hidden by being set to the font colour white on a white background **(Figure: 6.2)**. This suggests that the intention was to obscure the information.

- **The Meta-Data for Artefacts-6 is as follows:**



Metadata

Name:	/img_Operation Redbridge 2024 AXA-3.E01/vol_vol2/Accountancy Details/Communications with Accountant.docx/New Microsoft Word Document.docx
Type:	Derived
MIME Type:	application/vnd.openxmlformats-officedocument.wordprocessingml.document
Size:	12188
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:	1c815f96aab7c5acca9f389e28b9337a
SHA-256:	3695ad27e30200bf993ae84582484723aee549684464a279f5f8cc01b3363288
Hash Lookup Results:	UNKNOWN
Internal ID:	248

Figure:6.3

9.7 Artefacts- 7:

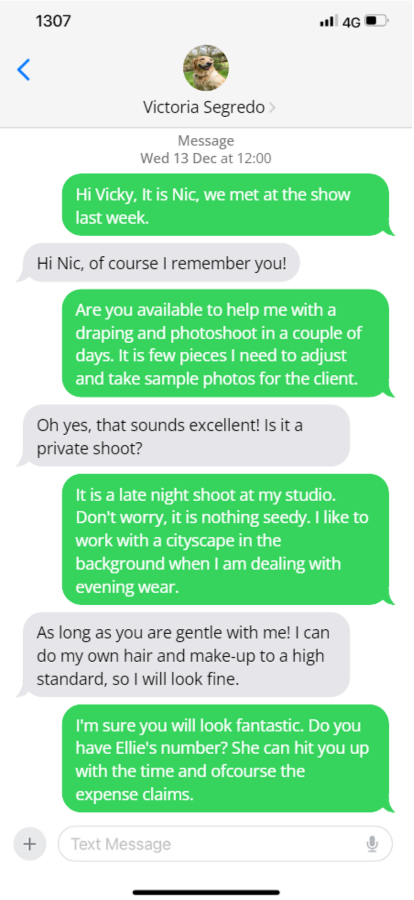
- **Location:**

Operation Redbridge 2024 AXA-3.E01/vol_vol2/Crazy Bitch Threats/Proof/Screen13122023.png

Operation Redbridge 2024 AXA-3.E01/vol_vol2/Crazy Bitch Threats/Proof/Screen23012024.png

Operation Redbridge 2024 AXA-3.E01/vol_vol2/Crazy Bitch Threats/Screen21022024.png'

Operation Redbridge 2024 AXA-3.E01/vol_vol2/Crazy Bitch Threats/Proof



Victoria Segredo

Message
Wed 13 Dec at 12:00

Hi Vicky, It is Nic, we met at the show last week.

Hi Nic, of course I remember you!

Are you available to help me with a draping and photoshoot in a couple of days. It is few pieces I need to adjust and take sample photos for the client.

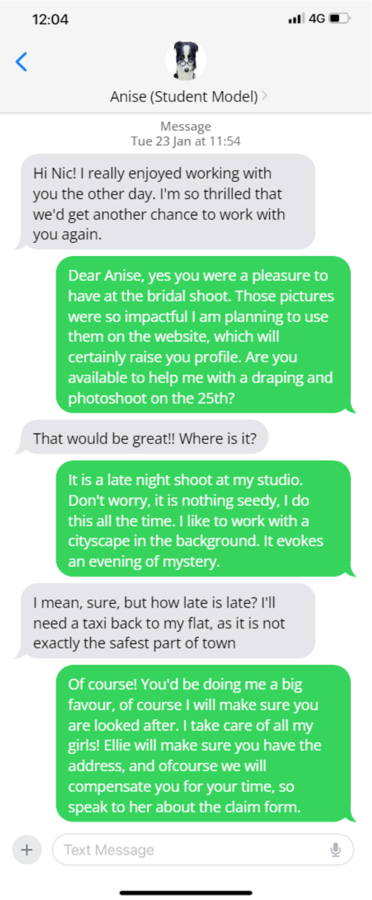
Oh yes, that sounds excellent! Is it a private shoot?

It is a late night shoot at my studio. Don't worry, it is nothing seedy. I like to work with a cityscape in the background when I am dealing with evening wear.

As long as you are gentle with me! I can do my own hair and make-up to a high standard, so I will look fine.

I'm sure you will look fantastic. Do you have Ellie's number? She can hit you up with the time and ofcourse the expense claims.

Figure: 7.1



Anise (Student Model)

Message
Tue 23 Jan at 11:54

Hi Nic! I really enjoyed working with you the other day. I'm so thrilled that we'd get another chance to work with you again.

Dear Anise, yes you were a pleasure to have at the bridal shoot. Those pictures were so impactful I am planning to use them on the website, which will certainly raise you profile. Are you available to help me with a draping and photoshoot on the 25th?

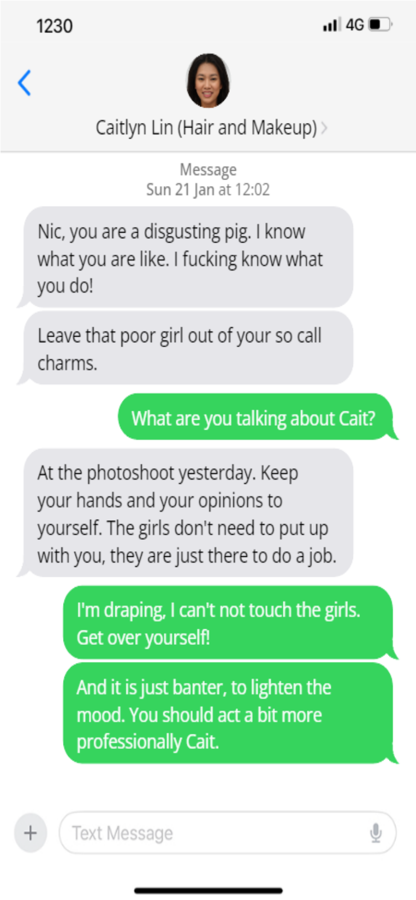
That would be great!! Where is it?

It is a late night shoot at my studio. Don't worry, it is nothing seedy, I do this all the time. I like to work with a cityscape in the background. It evokes an evening of mystery.

I mean, sure, but how late is late? I'll need a taxi back to my flat, as it is not exactly the safest part of town

Of course! You'd be doing me a big favour, of course I will make sure you are looked after. I take care of all my girls! Ellie will make sure you have the address, and ofcourse we will compensate you for your time, so speak to her about the claim form.

Figure: 7.2



Caitlyn Lin (Hair and Makeup)

Message
Sun 21 Jan at 12:02

Nic, you are a disgusting pig. I know what you are like. I fucking know what you do!

Leave that poor girl out of your so call charms.

What are you talking about Cait?

At the photoshoot yesterday. Keep your hands and your opinions to yourself. The girls don't need to put up with you, they are just there to do a job.

I'm draping, I can't not touch the girls. Get over yourself!

And it is just banter, to lighten the mood. You should act a bit more professionally Cait.

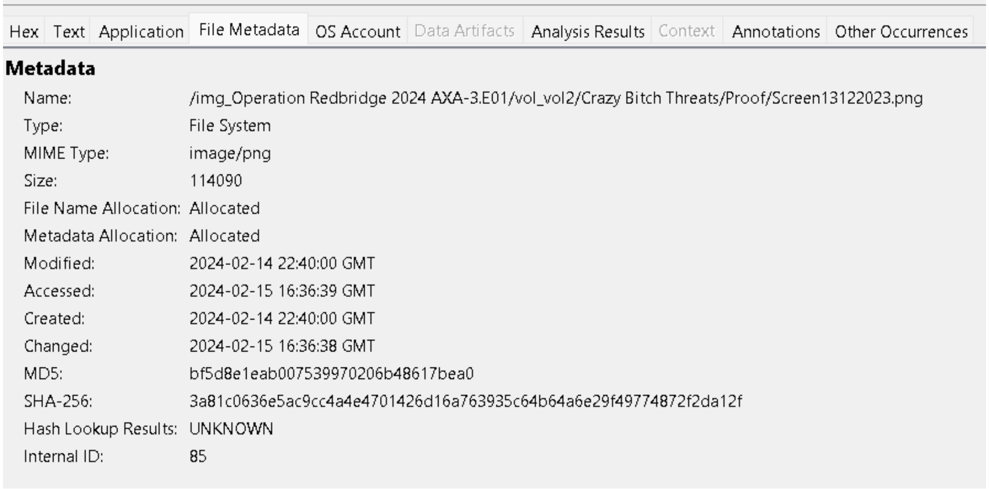
Figure: 7.3

- **Reason Why This Evidence is Suspicious:**
  The digital evidence, including messages and audio recordings, suggests a pattern in how VALENTINO interacts with models. On December 13, he contacted Victoria Segredo, and a little over a month later, on January 23, he reached out to DE BOER in a similar manner. By January 25, he had invited DE BOER to a private photoshoot, raising concerns that this may be part of a recurring behaviour.
  A voicemail was found from VALENTINO's accountant, stating, **" She is amazing, better even than the last one. You are devil." [Figure: 4.2 (3.jpg)].** This comment suggests that VALENTINO and his associate may have been evaluating individuals in a way that warrants further investigation. The exact meaning behind the statement remains unclear, but in the context of the case, it raises serious questions.
  There were also prior allegations of inappropriate behaviour. On January 21, makeup artist Caitlyn LIN confronted VALENTINO during a photoshoot, accusing him of making the models uncomfortable. She told him, **"Keep your hands and opinions to yourself. The girls don't need to deal with you; they are just here to do a job."** VALENTINO dismissed her concerns, responding, **"I'm draping; I can't touch the girls. Get over yourself!"** He later brushed off the

issue as nothing more than "jest" intended to create a relaxed atmosphere.

Taken together, these interactions paint a troubling picture of VALENTINO’s behaviour. His dismissive attitude toward concerns raised by others and his repeated interactions with different models suggest a pattern that should be examined further. The way he speaks about and engages with models raises ethical concerns, particularly regarding professional boundaries in the industry.

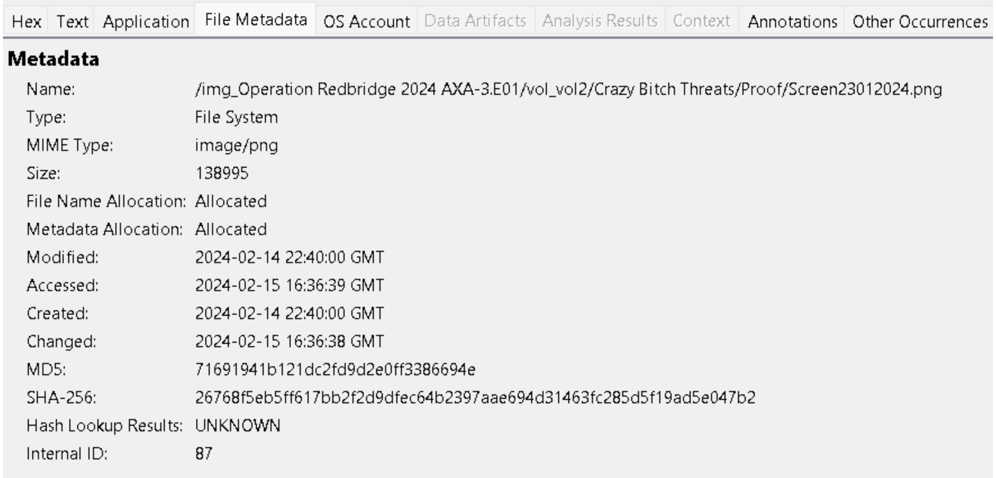
- **The Meta-Data for Artefacts-7 is as follows:**



Metadata

Name:	/img_Operation Redbridge 2024 AXA-3.E01/vol_vol2/Crazy Bitch Threats/Proof/Screen13122023.png
Type:	File System
MIME Type:	image/png
Size:	114090
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2024-02-14 22:40:00 GMT
Accessed:	2024-02-15 16:36:39 GMT
Created:	2024-02-14 22:40:00 GMT
Changed:	2024-02-15 16:36:38 GMT
MD5:	bf5d8e1eab007539970206b48617bea0
SHA-256:	3a81c0636e5ac9cc4a4e4701426d16a763935c64b64a6e29f49774872f2da12f
Hash Lookup Results:	UNKNOWN
Internal ID:	85

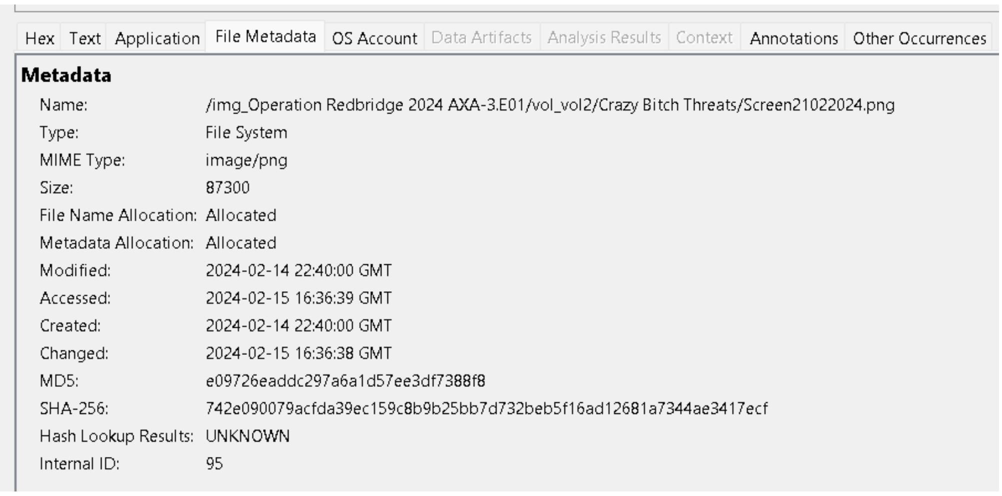
Figure: 7.4



Metadata

Name:	/img_Operation Redbridge 2024 AXA-3.E01/vol_vol2/Crazy Bitch Threats/Proof/Screen23012024.png
Type:	File System
MIME Type:	image/png
Size:	138995
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2024-02-14 22:40:00 GMT
Accessed:	2024-02-15 16:36:39 GMT
Created:	2024-02-14 22:40:00 GMT
Changed:	2024-02-15 16:36:38 GMT
MD5:	71691941b121dc2fd9d2e0ff3386694e
SHA-256:	26768f5eb5ff617bb2f2d9dfec64b2397aae694d31463fc285d5f19ad5e047b2
Hash Lookup Results:	UNKNOWN
Internal ID:	87

Figure:7.5



Hex | Text | Application | File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

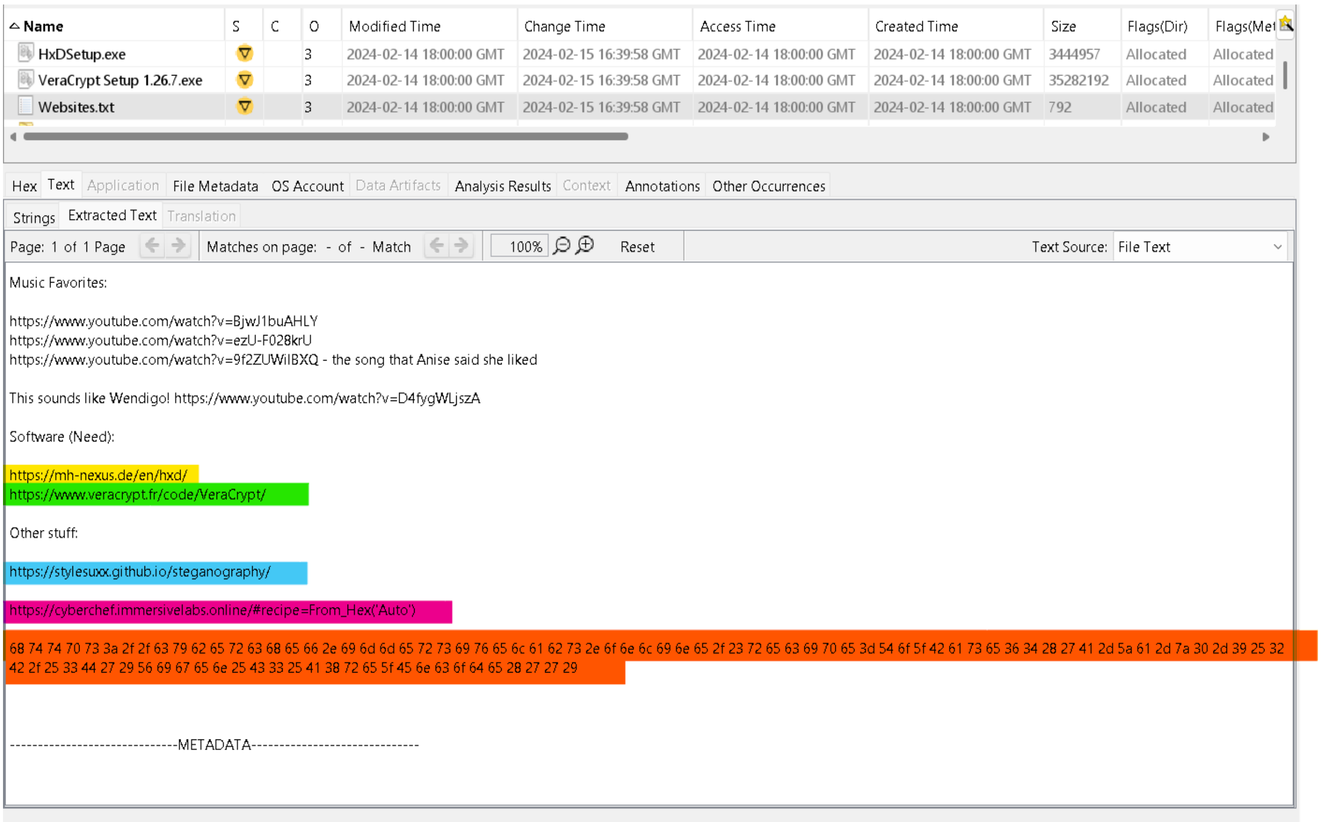
Metadata

Name:	/img_Operation Redbridge 2024 AXA-3.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 22:40:00 GMT
Accessed:	2024-02-15 16:36:39 GMT
Created:	2024-02-14 22:40:00 GMT
Changed:	2024-02-15 16:36:38 GMT
MD5:	e09726eaddc297a6a1d57ee3df7388f8
SHA-256:	742e090079acfda39ec159c8b9b25bb7d732beb5f16ad12681a7344ae3417ecf
Hash Lookup Results:	UNKNOWN
Internal ID:	95

Figure:7.6

9.8 Artefacts- 8

- **Location:** Operation Redbridge 2024 AXA-3.E01/vol_vol2/Important backups/Websites.txt



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Met
HxDSetup.exe			3	2024-02-14 18:00:00 GMT	2024-02-15 16:39:58 GMT	2024-02-14 18:00:00 GMT	2024-02-14 18:00:00 GMT	3444957	Allocated	Allocated
VeraCrypt Setup 1.26.7.exe			3	2024-02-14 18:00:00 GMT	2024-02-15 16:39:58 GMT	2024-02-14 18:00:00 GMT	2024-02-14 18:00:00 GMT	35282192	Allocated	Allocated
Websites.txt			3	2024-02-14 18:00:00 GMT	2024-02-15 16:39:58 GMT	2024-02-14 18:00:00 GMT	2024-02-14 18:00:00 GMT	792	Allocated	Allocated

Hex | Text | Application | File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Strings | Extracted Text | Translation

Page: 1 of 1 Page | Matches on page: - of - Match | 100% | Reset | Text Source: File Text

```
Music Favorites:

https://www.youtube.com/watch?v=BjwJ1buAHLY
https://www.youtube.com/watch?v=ezU-F028krU
https://www.youtube.com/watch?v=9f2ZUWilBXQ - the song that Anise said she liked

This sounds like Wendigo! https://www.youtube.com/watch?v=D4fygWLjszA

Software (Need):

https://mh-nexus.de/en/hxd/
https://www.veracrypt.fr/code/VeraCrypt/

Other stuff:

https://stylesuxx.github.io/steganography/

https://cyberchef.immersivelabs.online/#recipe=From_Hex('Auto')

68 74 74 70 73 3a 2f 2f 63 79 62 65 72 63 68 65 66 2e 69 6d 6d 65 72 73 69 76 65 6c 61 62 73 2e 6f 6e 6c 69 6e 65 2f 23 72 65 63 69 70 65 3d 54 6f 5f 42 61 73 65 36 34 28 27 41 2d 5a 61 2d 7a 30 2d 39 25 32
42 2f 25 33 44 27 29 56 69 67 65 6e 25 43 33 25 41 38 72 65 5f 45 6e 63 6f 64 65 28 27 27 29


-----------------------------METADATA-----------------------------
```

Figure:8.1

- **Reason Why This Evidence is Suspicious:**
  The tools used for manipulating digital forensic evidence include HXD Editor, VeraCrypt, Steganography, and CyberChef were found in figure artifact

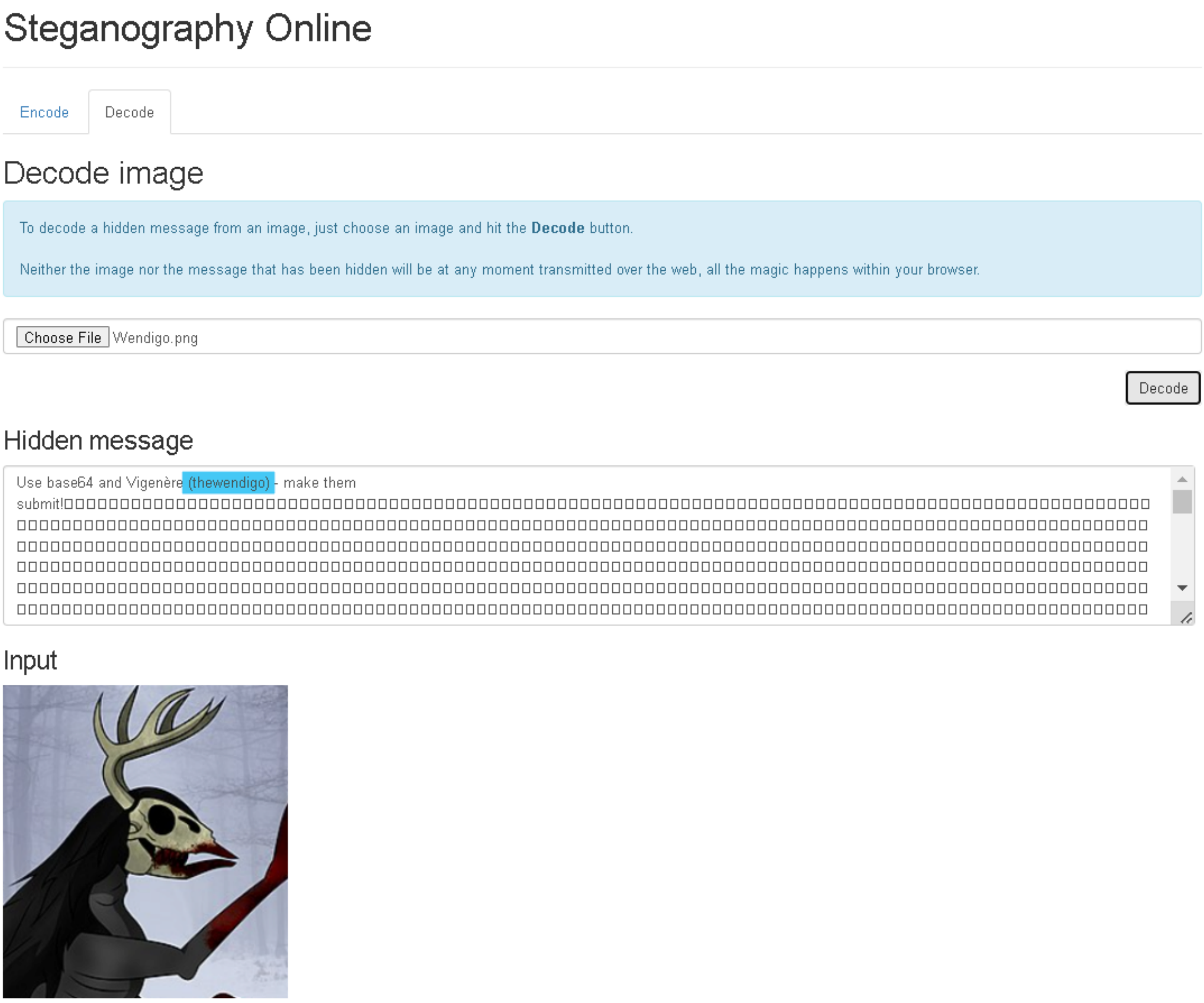
  HXD (Hex editor) is a tool that allows users to view and modify the raw hexadecimal code of files. In this case, it was used to analyse **Artifact 5 (3.rtf)**, where the file's original hex signature was found to be altered. This manipulation was an attempt to disguise or falsify evidence. Refer to **Figure: 5.1, 5.2 & 5.3.**

  VeraCrypt is an encryption tool used to secure files and storage volumes. The investigation found that some evidence was stored in a VeraCrypt-encrypted container. Once decrypted, additional manipulated files were uncovered, supporting the suspicion of evidence tampering. The location of this software found is /img_Operation Redbridge 2024 AXA-3.E01/vol_vol2/business sensitive information

  Online websites:
  Steganography is the practice of hiding data within other files, such as images or documents. Analysis suggested that hidden messages were embedded within digital images, requiring specialized extraction techniques to uncover them.

  - Within the '/img_Operation Redbridge 2024 AXA-3.E01/vol_vol2/ Accountancy Details' folder's a file named wendigo.png (**figure 8.2**) was discovered inside a document labelled communication withAccountant.Docx
  - The image file appeared to be encrypted using steganographic techniques.
  - Using the same steganography software, forensic analysts decrypted windigo.png and discovered a hidden key: **thewendigo**. (**figure 8.3**)

Figure: 8.2



Steganography Online

Decode image

To decode a hidden message from an image, just choose an image and hit the **Decode** button.

Neither the image nor the message that has been hidden will be at any moment transmitted over the web, all the magic happens within your browser.

Wendigo.png

Hidden message

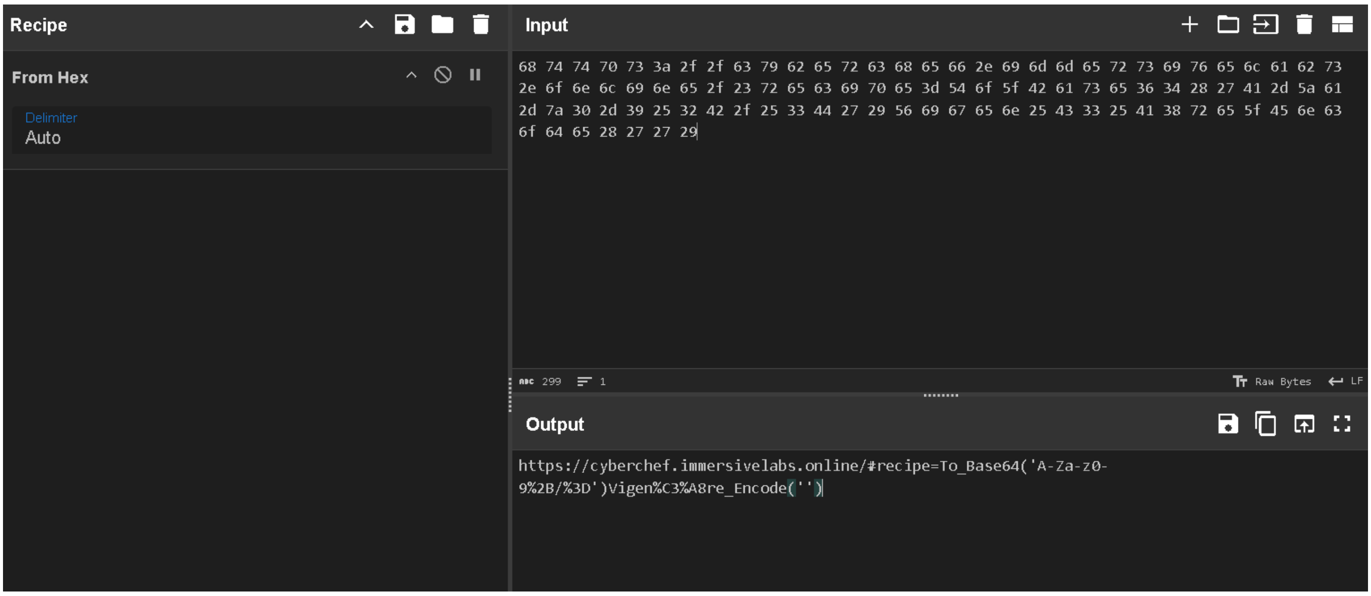
```
Use base64 and Vigenère (thewendigo) - make them
submit!□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
```

Input

Figure:8.3

Online tools: CyberChef is a web-based tool for analysing and transforming data. It helped decode hidden messages and analyse encrypted structures, revealing irregularities in file formats and encoding methods

- Within websites.txt, a hexadecimal code was discovered. **(figure 8.1)**
- The link https://cyberchef.immersivelabs.online/#recipe=From_Hex('Auto') was accessed, and the hex code was entered for analysis. **(figure 8.4)**
- The process led to another encoded link: https://cyberchef.immersivelabs.online/#recipe=To_Base64('A-Za-z0-9%2B/%3D')Vigen%C3%A8re_Encode(''). Upon opening this link, the transformation recipe suggested that additional hidden data was encoded using Base64 and Vigenère cipher techniques **(figure 8.5)**
- The exact nature of the hidden data remains unknown and requires further analysis.



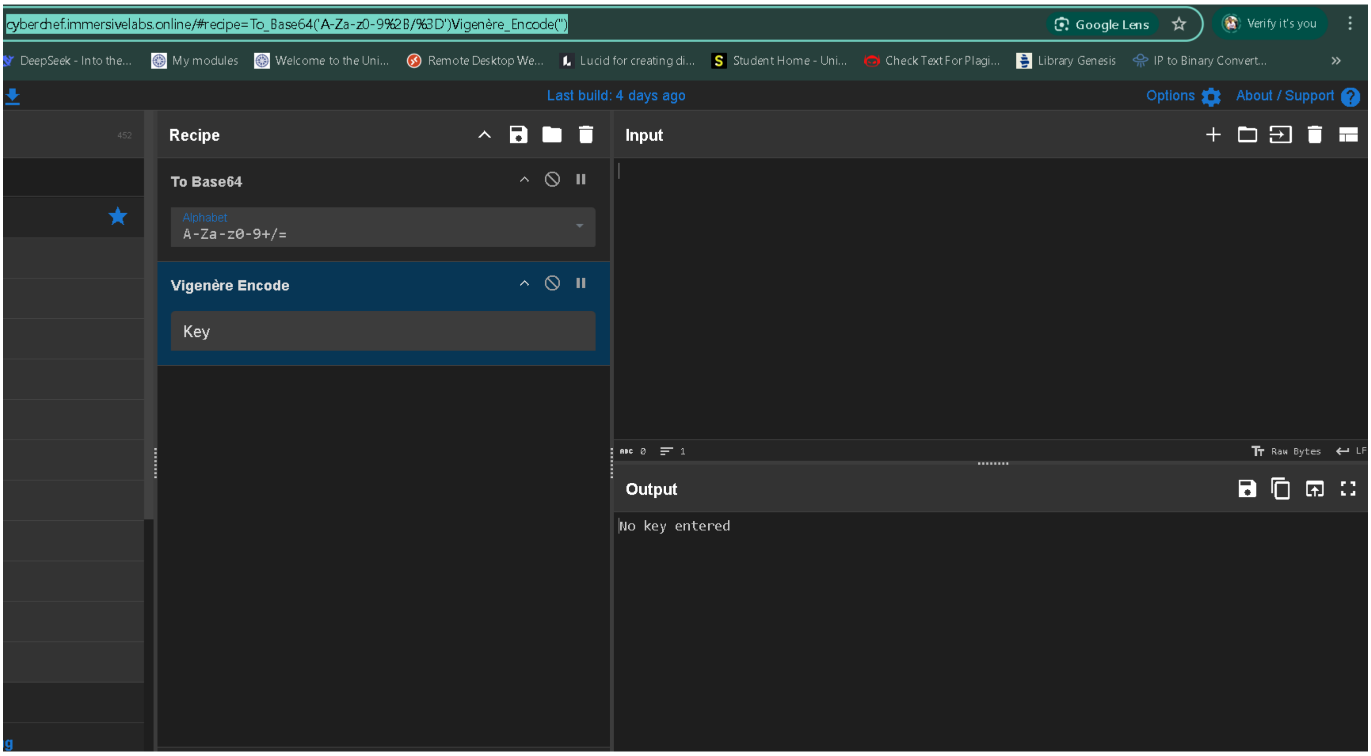
From Hex

Delimiter: Auto

```
68 74 74 70 73 3a 2f 2f 63 79 62 65 72 63 68 65 66 2e 69 6d 6d 65 72 73 69 76 65 6c 61 62 73
2e 6f 6e 6c 69 6e 65 2f 23 72 65 63 69 70 65 3d 54 6f 5f 42 61 73 65 36 34 28 27 41 2d 5a 61
2d 7a 30 2d 39 25 32 42 2f 25 33 44 27 29 56 69 67 65 6e 25 43 33 25 41 38 72 65 5f 45 6e 63
6f 64 65 28 27 27 29
```

```
https://cyberchef.immersivelabs.online/#recipe=To_Base64('A-Za-z0-
9%2B/%3D')Vigen%C3%A8re_Encode('')
```

Figure:8.4



cyberchef.immersivelabs.online/#recipe=To_Base64('A-Za-z0-9%2B/%3D')Vigenère_Encode('')

To Base64

Alphabet: A-Za-z0-9+/=

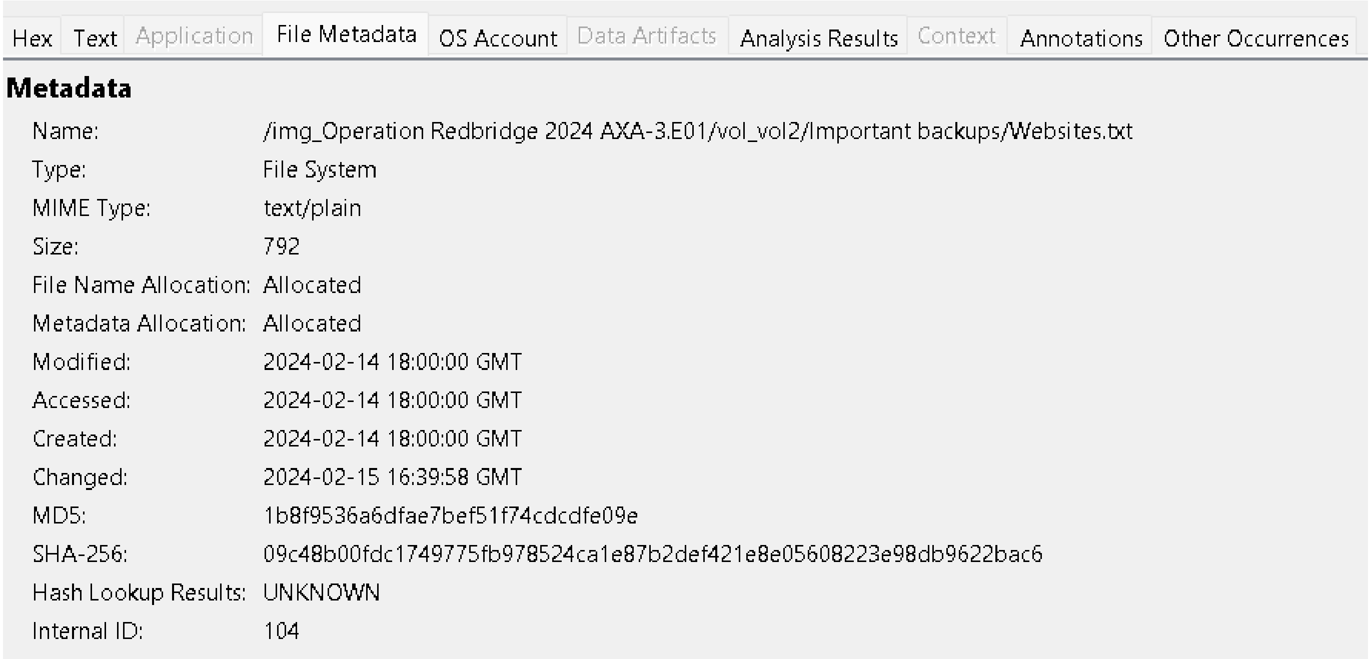
Vigenère Encode

Key

```
No key entered
```

Figure:8.5

- **The Meta-Data for Artefacts-8 is as follows:**



Metadata

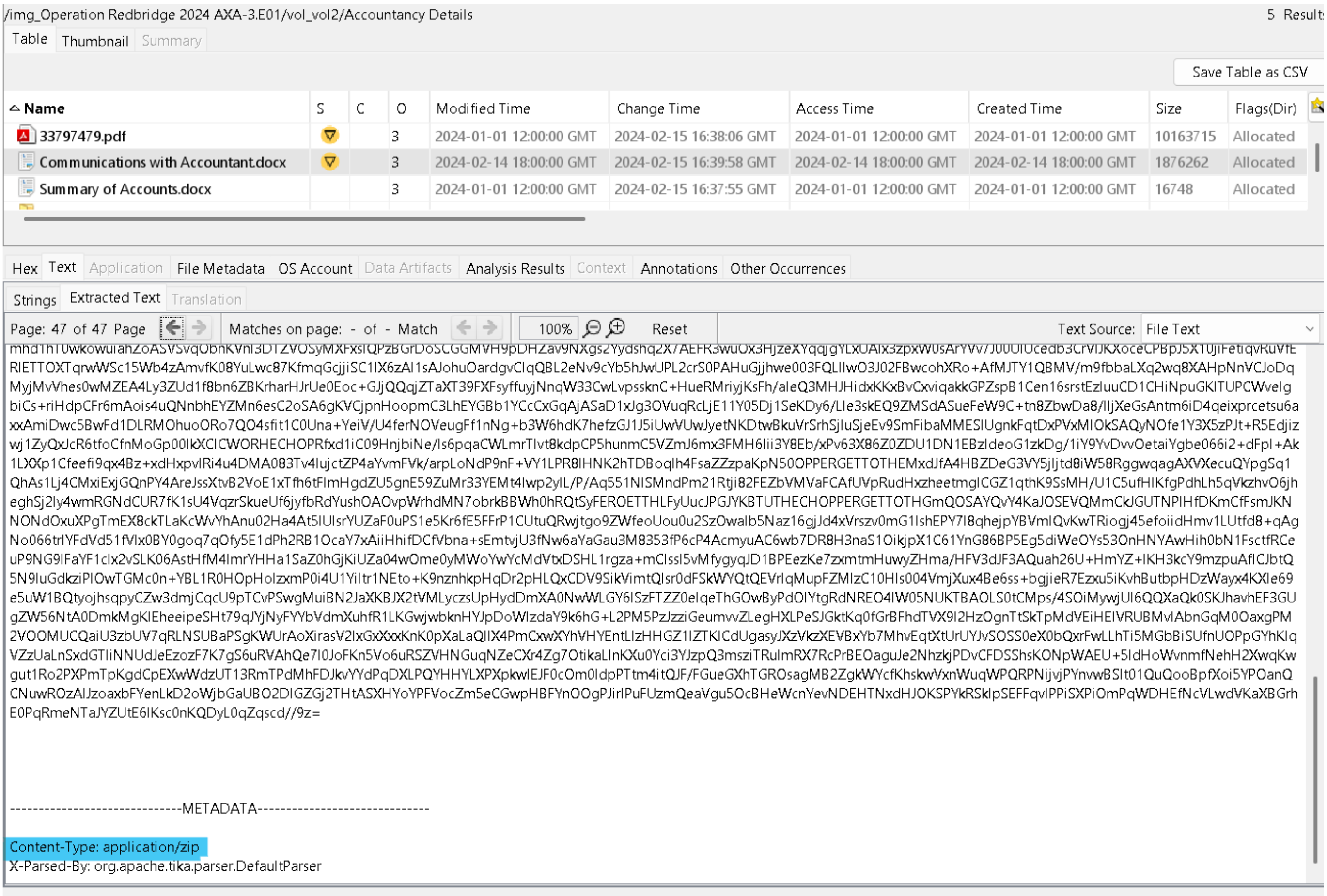
Name:	/img_Operation Redbridge 2024 AXA-3.E01/vol_vol2/Important backups/Websites.txt
Type:	File System
MIME Type:	text/plain
Size:	792
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2024-02-14 18:00:00 GMT
Accessed:	2024-02-14 18:00:00 GMT
Created:	2024-02-14 18:00:00 GMT
Changed:	2024-02-15 16:39:58 GMT
MD5:	1b8f9536a6dfae7bef51f74cdcdfe09e
SHA-256:	09c48b00fdc1749775fb978524ca1e87b2def421e8e05608223e98db9622bac6
Hash Lookup Results:	UNKNOWN
Internal ID:	104

Figure:8.6

9.9 Artefacts-9

- **Location:** Operation Redbridge 2024 AXA-3.E01/vol_vol2/Accountancy Details

- **Reason Why This Evidence is Suspicious:**
  While analysing Accountancy Details **'Communication with Accountant.docx'** was found of 47 pages. While the metadata itself shows Type: application/document. **(Figure 9.7)** upon reviewing the doc file on the 47th page the Metadata shows Content-Type: application/zip **(Figure 9.1).**



/img_Operation Redbridge 2024 AXA-3.E01/vol_vol2/Accountancy Details

5 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
33797479.pdf	▽		3	2024-01-01 12:00:00 GMT	2024-02-15 16:38:06 GMT	2024-01-01 12:00:00 GMT	2024-01-01 12:00:00 GMT	10163715	Allocated
Communications with Accountant.docx	▽		3	2024-02-14 18:00:00 GMT	2024-02-15 16:39:58 GMT	2024-02-14 18:00:00 GMT	2024-02-14 18:00:00 GMT	1876262	Allocated
Summary of Accounts.docx			3	2024-01-01 12:00:00 GMT	2024-02-15 16:37:55 GMT	2024-01-01 12:00:00 GMT	2024-01-01 12:00:00 GMT	16748	Allocated

Text Source: File Text

```
mhd1h1UwkowuiahZoASVSvqObnKVnl3D1ZVOSyMXFxslQPzBGrDoSCGGMVH9pDHZav9NXgs2Yydshq2X7AEFR3wuOx3HjzeXYqqjgYLxUAIx3zpxW0sArYVv7J00UIUcedb3CrVIJKXoceCPBpJ5X1UjiFetiqvRuVfE
RIETTOXTqrwWSc15Wb4zAmvfK08YuLwc87KfmqGcjjiSC1lX6zAl1sAJohuOardgvClqQBL2eNv9cYb5hJwUPL2crS0PAHuGjjhwe003FQLIlwO3J02FBwcohXRo+AfMJTY1QBMV/m9fbbaLXq2wq8XAHpNnVCJoDq
MyjMvVhes0wMZEA4Ly3ZUd1f8bn6ZBKrharHJrUe0Eoc+GJjQQqjZTaXT39FXFsyffuyjNnqW33CwLvpssknC+HueRMriyjKsFh/aleQ3MHJHidxKKxBvCxviqakkGPZspB1Cen16srstEzluuCD1CHiNpuGKITUPCWvelg
biCs+riHdpCFr6mAois4uQNnbhEYZMn6esC2oSA6gKVCjpnHoopmC3LhEYGBb1YCcCxGqAjASaD1xJg3OVuqRcLjE11Y05Dj1SeKDy6/Lle3skEQ9ZMSdASueFeW9C+tn8ZbwDa8/lljXeGsAntm6iD4qeixprcetsu6a
xxAmiDwc5BwFd1DLRMOhuoORo7QO4sfit1C0Una+YeiV/U4ferNOVeugFf1nNg+b3W6hdK7hefzGJ1J5iUwVUwJyetNKDtwBkuVrSrhSjIuSjeEv9SmFibaMMESIUgnkFqtDxPVxMIOkSAQyNOfe1Y3X5zPJt+R5Edjiz
wj1ZyQxJcR6tfoCfnMoGp00IkXClCWORHECHOPRfxd1iC09HnjbiNe/Is6pqaCWLmrTlvt8kdpCP5hunmC5VZmJ6mx3FMH6Iii3Y8Eb/xPv63X86Z0ZDU1DN1EBzIdeoG1zkDg/1iY9YvDvvOetaiYgbe066i2+dFpI+Ak
1LXXp1Cfeefi9qx4Bz+xdHxpvIRi4u4DMA083Tv4lujctZP4aYvmFVk/arpLoNdP9nF+VY1LPR8IHNK2hTDBoqIh4FsaZZzpaKpN50OPPERGETTOTHEMxdJfA4HBZDeG3VY5jIjtd8iW58RggwqagAXVXecuQYpgSq1
QhAs1Lj4CMxiExjGQnPY4AreJssXtvB2VoE1xTfh6tFImHgdZU5gnE59ZuMr33YEMt4Iwp2yIL/P/Aq551NISMndPm21Rtji82FEZbVMVaFCAfUVpRudHxzheetmgICGZ1qthK9SsMH/U1C5ufHIKfgPdhLh5qVkzhvO6jh
eghSj2Iy4wmRGNdCUR7fK1sU4VqzrSkueUf6jyfbRdYushOAOvpWrhdMN7obrkBBWh0hRQtSyFEROETTHLFyUucJPGJYKBTUTHECHOPPERGETTOTHGmQOSAYQvY4KaJOSEVQMmCkJGUTNPIHfDKmCfFsmJKN
NONdOxuXPgTmEX8ckTLaKcWvYhAnu02Ha4At5lUIsrYUZaF0uPS1e5Kr6fE5FFrP1CUtuQRwjtgo9ZWfeoUou0u2SzOwalb5Naz16gjJd4xVrszv0mG1IshEPY7I8qhejpYBVmIQvKwTRiogj45efoiidHmv1LUtfd8+qAg
No066trIYFdVd51fVIx0BY0goq7qOfy5E1dPh2RB1OcaY7xAiiHhifDCfVbna+sEmtvjU3fNw6aYaGau3M8353fP6cP4AcmyuAC6wb7DR8H3naS1OikjpX1C61YnG86BP5Eg5diWeOYs53OnHNYAwHih0bN1FsctfRCe
uP9NG9IFaYF1clx2vSLK06AstHfM4ImrYHHa1SaZ0hGjKiUZa04wOme0yMWoYwYcMdVtxDSHL1rgza+mClssI5vMfygyqJD1BPEezKe7zxmtmHuwyZHma/HFV3dJF3AQuah26U+HmYZ+IKH3kcY9mzpuAfICJbtQ
5N9IuGdkziPIOwTGMc0n+YBL1R0HOpHoIzxmP0i4U1YiItr1NEto+K9nznhkpHqDr2pHLQxCDV9SikVimtQIsr0dFSkWYQtQEVrIqMupFZMIzC10HIs004VmjXux4Be6ss+bgjieR7Ezxu5iKvhButbpHDzWayx4KXIe69
e5uW1BQtyojhsqpyCZw3dmjCqcU9pTCvPSwgMuiBN2JaXKBJX2tVMLyczsUpHydDmXA0NwWLGY6ISzFTZZ0eIqeThGOwByPdOIYtgRdNREO4IW05NUKTBAOLS0tCMps/4SOiMywjUI6QQXaQk0SKJhavhEF3GU
gZW56NtA0DmkMgKIEheeipeSHt79qJYjNyFYYbVdmXuhfR1LKGwjwbknHYJpDoWIzdaY9k6hG+L2PM5PzJzziGeumvvZLegHXLPeSJGktKq0fGrBFhdTVX9I2HzOgnTtSkTpMdVEiHEIVRUBMvIAbnGqM0OaxgPM
2VOOMUCQaiU3zbUV7qRLNSUBaPSgKWUrAoXirasV2IxGxXxxKnK0pXaLaQIIX4PmCxwXYhVHYEntLIzHHGZ1IZTKICdUgasyJXzVkzXEVBxYb7MhvEqtXtUrUYJvSOSS0eX0bQxrFwLLhTi5MGbBiSUfnUOPpGYhKIq
VZzUaLnSxdGTIiNNUdJeEzozF7K7gS6uRVAhQe7I0JoFKn5Vo6uRSZVHNGuqNZeCXr4Zg7OtikaLInKXu0Yci3YJzpQ3msziTRuImRX7RcPrBEOaguJe2NhzkjPDvCFDSShsKONpWAEU+5IdHoWvnmfNehH2XwqKw
gut1Ro2PXPmTpKgdCpEXwWdzUT13RmTPdMhFDJkvYYdPqDXLPQYHHYLXPXpkwIEJF0cOm0IdpPTtm4itQJF/FGueGXhTGROsagMB2ZgkWYcfKhskwVxnWuqWPQRPNijvjPYnvwBSIt01QuQooBpfXoi5YPOanQ
CNuwROzAIJzoaxbFYenLkD2oWjbGaUBO2DIGZGj2THtASXHYoYPFVoczm5eCGwpHBFYnOOgPJirlPuFUzmQeaVgu5OcBHeWcnYevNDEHTNxdHJOKSPYkRSkIpSEFFqvIPPiSXPiOmPqWDHEfNcVLwdVKaXBGrh
E0PqRmeNTaJYZUtE6IKsc0nKQDyL0qZqscd//9z=
```

```
-----------------------------METADATA-----------------------------

Content-Type: application/zip
X-Parsed-By: org.apache.tika.parser.DefaultParser
```

Figure:9.1

Changing the file extension to **.zip** allowed the extraction of a folder named **wendigo** and a file named **wendigo.png (Figure 9.2)**

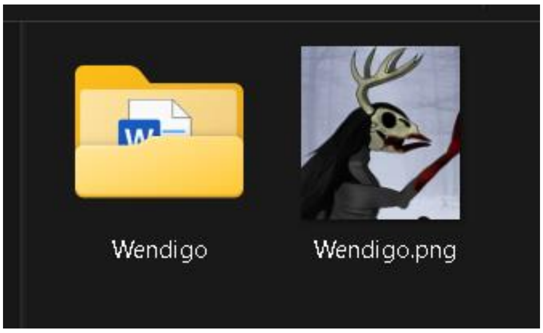
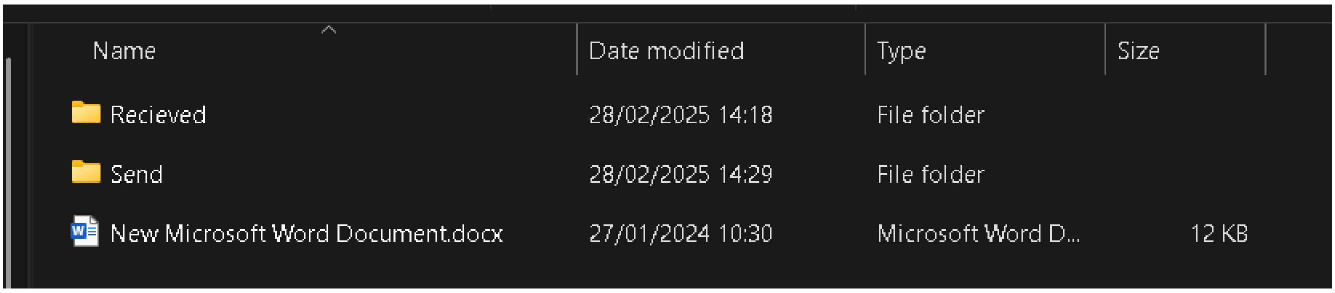


Figure:9.2

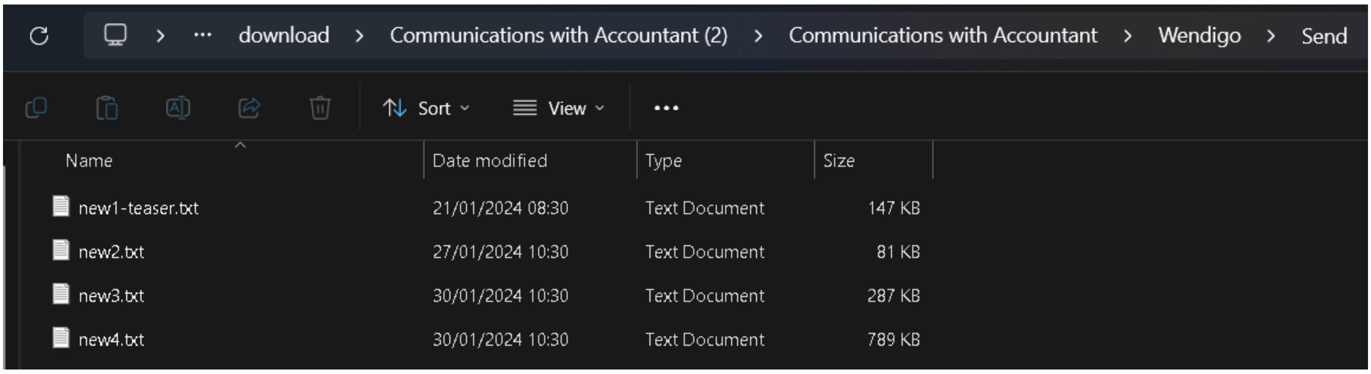
Inside the wendigo folder, there were three subfolders: received, send, and a DOCX file. **(Figure 9.3)** The received folder was analysed in Autopsy, refer to figure **(4.2)**



Name	Date modified	Type	Size
Recieved	28/02/2025 14:18	File folder	
Send	28/02/2025 14:29	File folder	
New Microsoft Word Document.docx	27/01/2024 10:30	Microsoft Word D...	12 KB

Figure:9.3

The send folder was not detected in Autopsy, but upon manual inspection, it was found to contain four **TXT files**. **(Figure 9.4)**

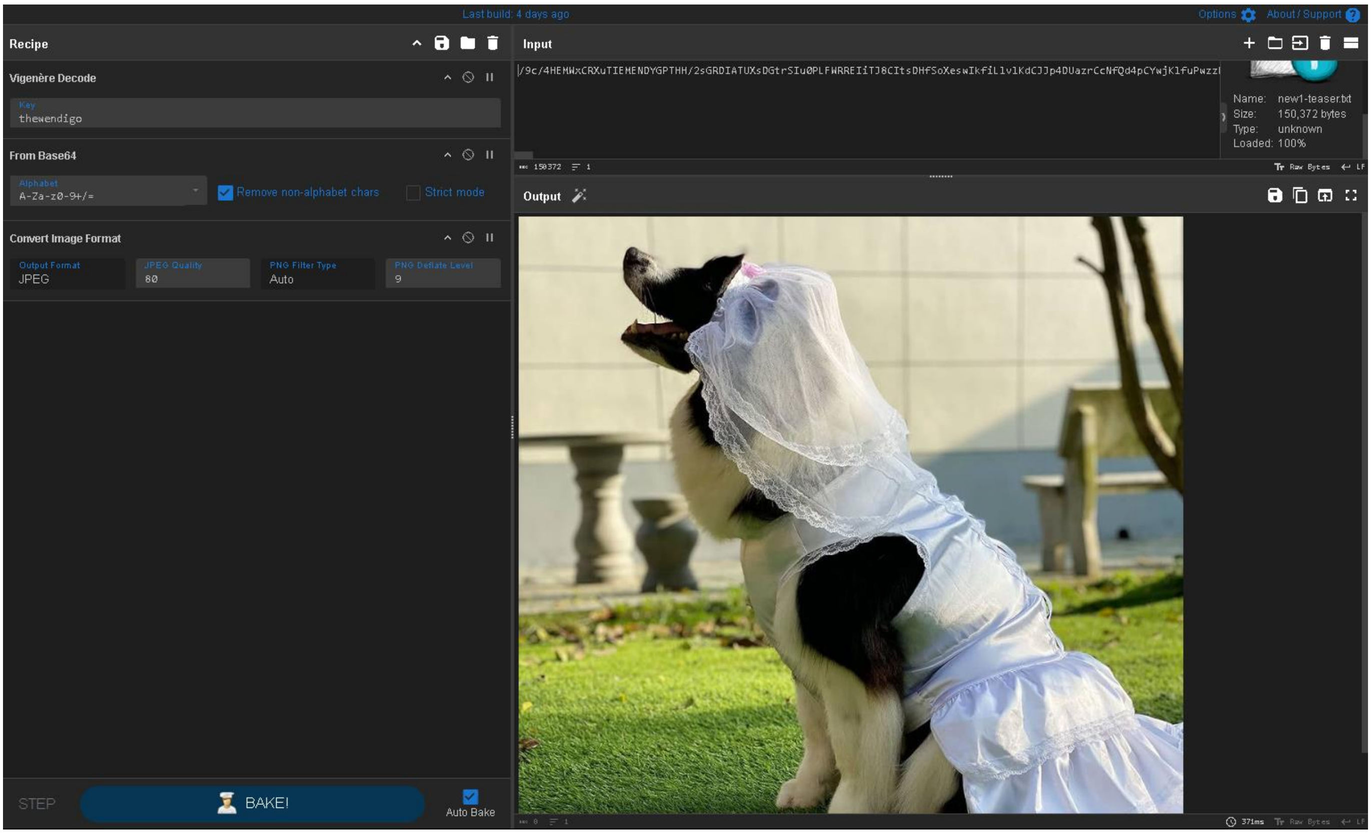


··· › download › Communications with Accountant (2) › Communications with Accountant › Wendigo › Send

Name	Date modified	Type	Size
new1-teaser.txt	21/01/2024 08:30	Text Document	147 KB
new2.txt	27/01/2024 10:30	Text Document	81 KB
new3.txt	30/01/2024 10:30	Text Document	287 KB
new4.txt	30/01/2024 10:30	Text Document	789 KB

Figure:9.4

Using **CyberChef**, these TXT files were decrypted using the key **thewendigo**. Initially, applying **Base64** and **Vigenère** with the key **thewendigo** did not yield any results. However, it was suspected that the files might be hidden as **JPEG (the hexadecimal format of the TXT files indicated a JPEG file structure)** By applying the JPEG Convert Format along with the key **thewendigo**, **Base64**, and **Vigenère decryption**, the files were successfully decrypted into images. The first two files, new1-teaser.txt and new2.txt, were recovered as JPEG images (Figure **9.5 and 9.6)**, while the remaining two TXT files could not be successfully recovered, and their contents remain unknown. Analysis of the recovered images revealed a reference to a dog picture related to the case, specifically an image of DE BOER.



Vigenère Decode
Key: thewendigo

From Base64
Alphabet: A-Za-z0-9+/=
☑ Remove non-alphabet chars
□ Strict mode

Convert Image Format
Output Format: JPEG
JPEG Quality: 80
PNG Filter Type: Auto
PNG Deflate Level: 9

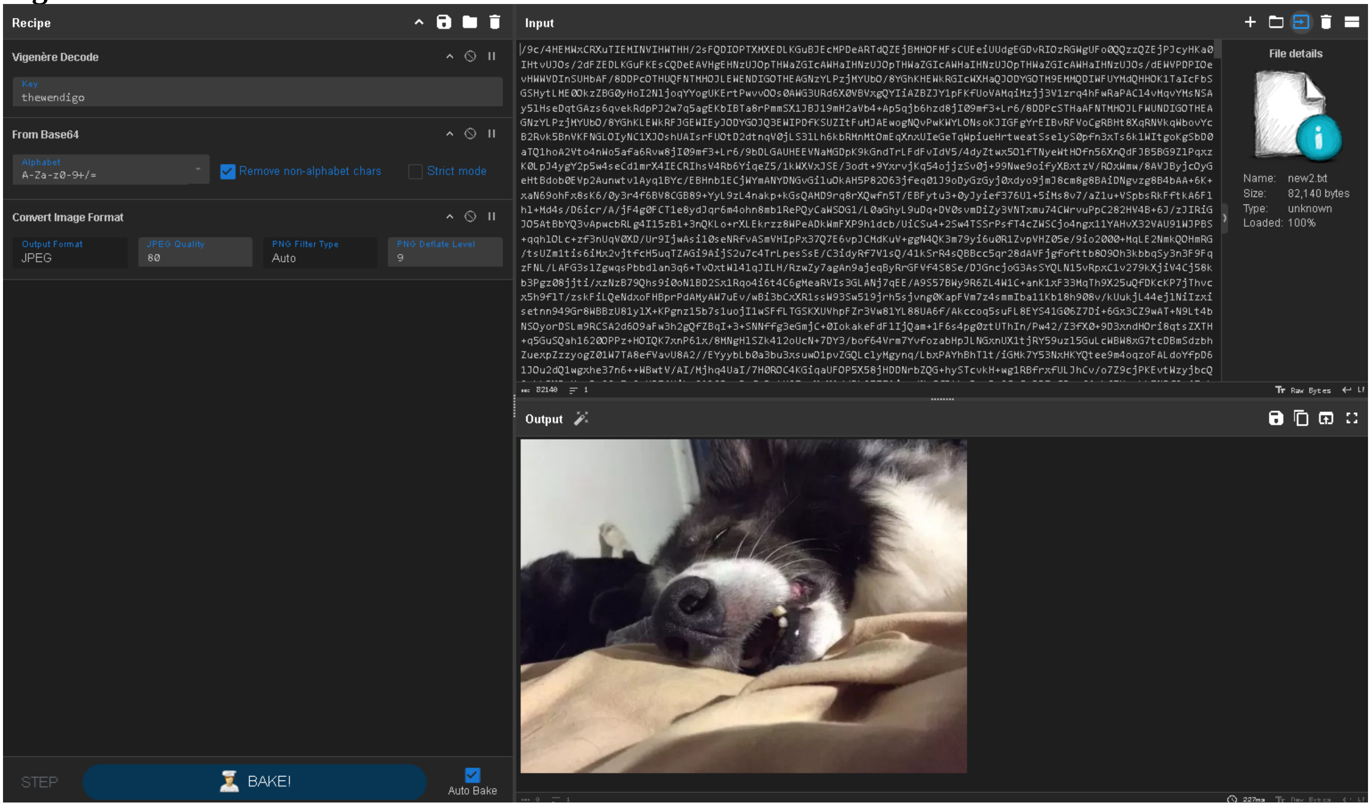
/9c/4HEMWxCRXuTIEMENDYGPTHH/2sGRDIATUXsDGtrSIu0PLFWRREIiTJ8CItsDHfSoXeswIkfiLlvlKdCJJp4DUazrCcNfQd4pCYwjKlfuPwzz

Name: new1-teaser.txt
Size: 150,372 bytes
Type: unknown
Loaded: 100%

150372 1 Raw Bytes LF

371ms

Figure:9.5



Vigenère Decode
Key: thewendigo

From Base64
Alphabet: A-Za-z0-9+/=
☑ Remove non-alphabet chars
□ Strict mode

Convert Image Format
Output Format: JPEG
JPEG Quality: 80
PNG Filter Type: Auto
PNG Deflate Level: 9

/9c/4HEMWxCRXuTIEMINVIHWTHH/2sFQDIOPTXMXEDLKGuBJEcMPDeARTdQZEjBMHOFMFsCUEeiUUdgEGDvRIOzRGWgUFo0QQzzQZEjPJcyHKa0
IHtvUJOs/2dFZEDLKGuFKEsCQDeEAVHgEHNzUJOpTHWaZGIcAWHaIHNzUJOpTHWaZGIcAWHaIHNzUJOpTHWaZGIcAWHaIHNzUJOs/dEWVPDPIOe
vHWWVDInSUHbAF/8DDPcOTHUQFNTMHOJLEWENDIGOTHEAGNzYLPzjMYUbO/8YGhKHEWkRGIcWXHaQJODYGOTM9EMMQDIWFUYMdQHHOK1TaIcFbS
GSHytLME0OkzZBG0yHoI2NljoqYYogUKErtPwvvOOs0AWG3URd6X0VBVxgQYIiAZBZJY1pFKfUoVAMqiMzjj3V1zrq4hFwRaPACl4vMqvYMsNSA
y5lHseDqtGAzs6qvekRdpPJ2w7q5agEKbIBTa8rPmmSX1JBJ19mH2aVb4+Ap5qjb6hzd8jI09mf3+Lr6/8DDPcSTHaAFNTMHOJLFWUNDIGOTHEA
GNzYLPzjMYUbO/8YGhKLEWkRFJGEWIEyJODYGOJQ3EWIPDfKSUZItFuMJAEwogNQvPwKWYLONsoKJIGFgYrEIBvRFVoCgRBHt8XqRNVkqWbovYc
B2Rvk5BnVKFNGLOIyNC1XJOshUAIsrFUOtD2dtnqV0jLS31Lh6kbRMnMtOmEqXnxUIeGeTqWpiueHrtweatSselyS0pfn3xTs6klWItgoKgSbD0
aTQ1hoA2Vto4nWo5afa6Rvw8jI09mf3+Lr6/9bDLGAUHEEVNaMGDpK9kGndTrLFdFvIdV5/4dyZtwx5OlfTNyeWtHOfn56XnQdFJB5BG9Z1Pqxz
K0LpJ4ygY2p5w4seCd1mrX4IECRIhsV4Rb6YiqeZ5/1kWXVxJSE/3odt+9YxrvjKq54ojjzSv0j+99Nwe9oifyXBxtzV/ROxWmw/8AVJByjcOyG
eHtBdob0EVp2Aunwtv1Ayq1BYc/EBHnb1ECjWYmANYDNGvGiluOkAH5P82O63jfeq01J9oDyGzGyj0xdyo9jmJ8cm8g8BAiDNgvzg8B4bAA+6K+
xaN69ohFx8sK6/0y3r4f6BV8CGB89+YyL9zL4nakp+kGsQAMD9rq8rXQwfn5T/EBFytu3+0yJyief376Ul+5iMs8v7/aZ1u+VSpbsRkFftkA6Fl
hl+Md4s/D6icr/A/jF4g0FCT1e8ydJqr6m4ohn8mb1RePQyCaWSOG1/L0aGhyL9uDq+DV0svmDiZy3VNTxmu74CWrvuPpC282HV4B+6J/zJIRiG
JO5AtBbYQ3vApwcbRLg4I15zB1+3nQKLo+rXLEkrzz8WPeADkWmFXP9h1dcb/UiCSu4+2Sw4TSSrPsfT4cZWSCjo4ngx11YAHvX32VAU91WJPBS
+qqhlOLc+zf3nUqV0XD/Ur9IjwAsi10seNRfvASmVHIpPx37Q7E6vpJCMdKuV+ggN4QK3m79yi6u0R1ZvpVHZ05e/9io2000+MqLE2NmkQOHmRG
/tsUZm1tis6iMx2vjtfcH5uqTZAGi9AijS2u7c4TrLpesSsE/C3idyRf7V1sQ/41kSrR4sQBBcc5qr28dAVFjgfofttb8O9Oh3kbbqSy3n3F9Fq
zFNL/LAFG3slZgwqsPbbdlan3q6+TvOxtWl4lqJILH/RzwZy7agAn9ajeqByRrGFVf4S8Se/DJGncjoG3AsSYQLN15vRpxC1v279kXjiV4Cj58k
b3Pgz08jjti/xzNzB79Qhs9i0oN1BD2Sx1Rqo4i6t4C6gMeaRVIs3GLANj7qEE/A9S57BWy9R6ZL4W1C+anK1xF33MqTh9X25uQfDKcKP7jThvc
x5h9flT/zskFiLQeNdxoFHBprPdAMyAW7uEv/wBi3bCxXR1ssW93Sw519jrh5sjvng0KapFVm7z4smmIba11Kb18h908v/kUukjL44ejlNiIzxi
setnn949Gr8WBBzU81ylX+KPgnz15b7s1uojI1wSFfLTGSKXUVhpFZr3Vw81YL88UA6f/AkccoqSsuFL8EYS41G06Z7Di+6Gx3CZ9wAT+N9Lt4b
NSOyorDSLm9RCSA2d6O9aFw3h2gQfZBqI+3+SNNffg3eGmjC+0IokakeFdFlIjQam+1F6s4pg0ztUThIn/Pw42/Z3fX0+9D3xndHOri8qtsZXTH
+q5GuSQah162OOPPz+HOIQK7xnP61x/8MNgHlSZk412oUcN+7DY3/bof64Vrm7YvfozabHpJLNGxnUX1tjRY59uz15GuLcWBW8xG7tcDBmSdzbh
ZuexpZzzyogZ01W7TA8efVavU8A2//EYyybLb0a3bu3xsuwO1pvZGQLclyMgynq/LbxPAYhBhTlt/iGMk7Y53NxHKYQtee9m4oqzoFALdoYfpD6
1JOu2dQ1wgxhe37n6++WBwtV/AI/Mjhq4UaI/7H0ROC4KGiqaUFOP5X58jHDDNrbZQG+hySTcvkH+wg1RBfrxFULJhCv/o7Z9cjPKEvtWzyjbcQ

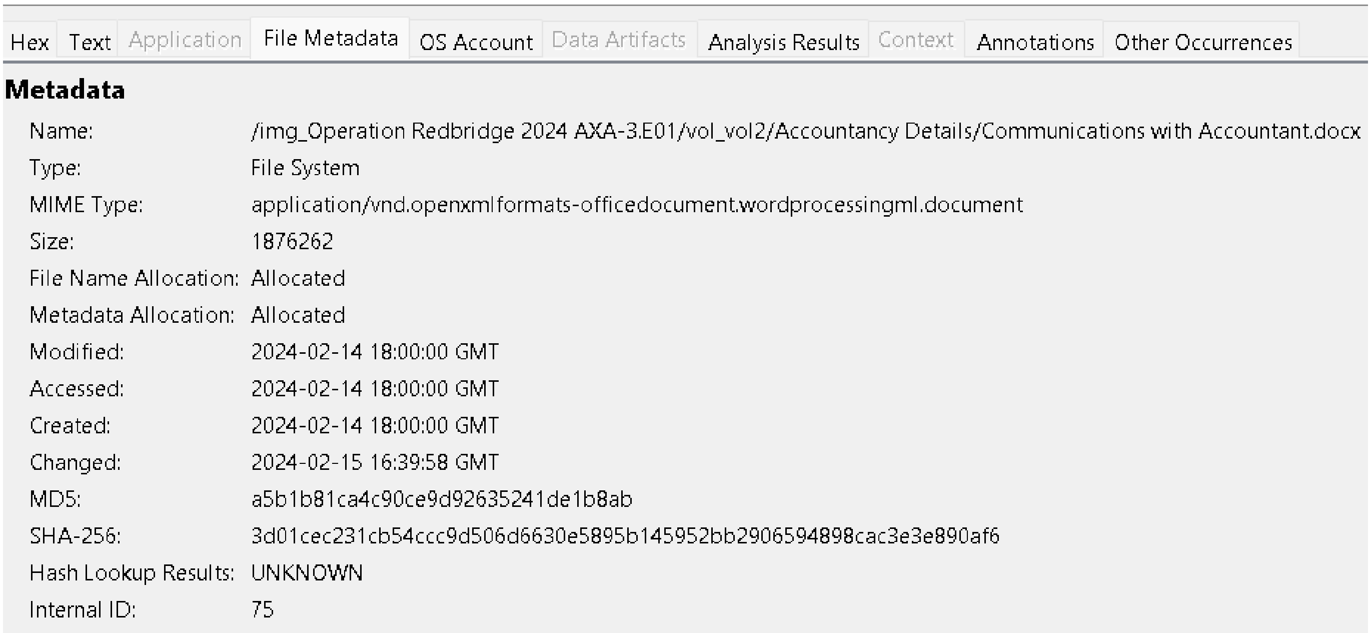
82140 1 Raw Bytes LF

Name: new2.txt
Size: 82,140 bytes
Type: unknown
Loaded: 100%

227ms

Figure:9.6

- **The Meta-Data for Artefacts-9 is as follows:**



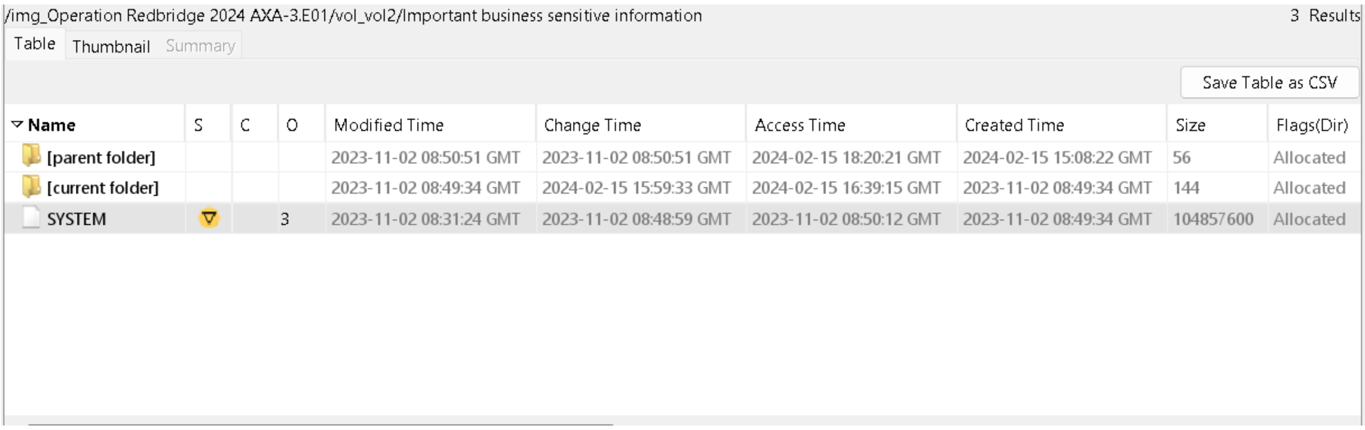
Metadata

Name:	/img_Operation Redbridge 2024 AXA-3.E01/vol_vol2/Accountancy Details/Communications with Accountant.docx
Type:	File System
MIME Type:	application/vnd.openxmlformats-officedocument.wordprocessingml.document
Size:	1876262
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2024-02-14 18:00:00 GMT
Accessed:	2024-02-14 18:00:00 GMT
Created:	2024-02-14 18:00:00 GMT
Changed:	2024-02-15 16:39:58 GMT
MD5:	a5b1b81ca4c90ce9d92635241de1b8ab
SHA-256:	3d01cec231cb54ccc9d506d6630e5895b145952bb2906594898cac3e3e890af6
Hash Lookup Results:	UNKNOWN
Internal ID:	75

Figure:9.7

9.10 Artefacts:10

- **Location**: Operation Redbridge 2024 AXA-3.E01/vol_vol2/ Important business sensitive information
- **Reason Why This Evidence is Suspicious:**
  At this location SYSTEM file was found which was encrypted **(Figure 10.1)**, assuming this was encrypted using VeraCrypt. Upon opening **SYSTEM** file on VeraCrypt it required a password to access it.



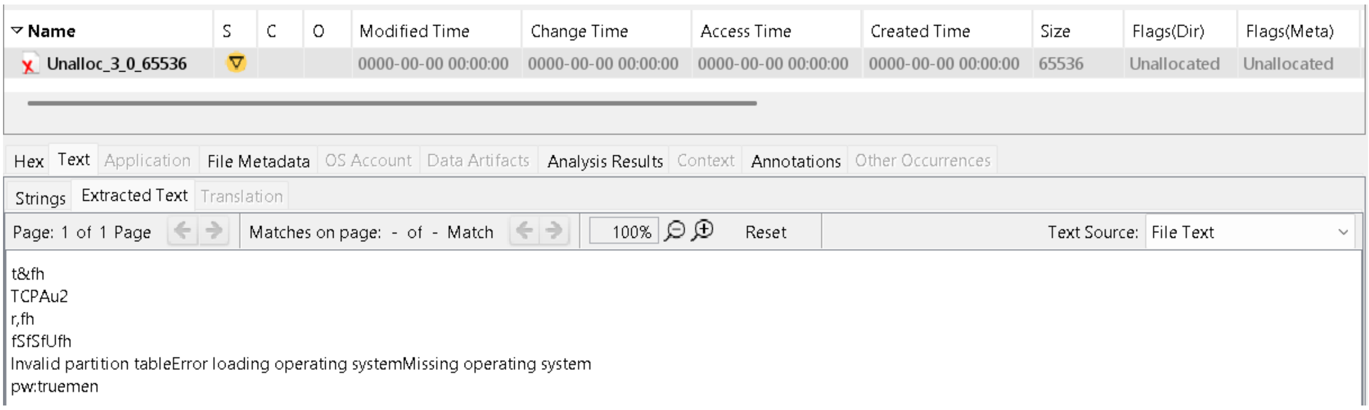
/img_Operation Redbridge 2024 AXA-3.E01/vol_vol2/Important business sensitive information

3 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
[parent folder]				2023-11-02 08:50:51 GMT	2023-11-02 08:50:51 GMT	2024-02-15 18:20:21 GMT	2024-02-15 15:08:22 GMT	56	Allocated
[current folder]				2023-11-02 08:49:34 GMT	2024-02-15 15:59:33 GMT	2024-02-15 16:39:15 GMT	2023-11-02 08:49:34 GMT	144	Allocated
SYSTEM	▽		3	2023-11-02 08:31:24 GMT	2023-11-02 08:48:59 GMT	2023-11-02 08:50:12 GMT	2023-11-02 08:49:34 GMT	104857600	Allocated

Figure:10.1

While researching unallocated space of **volume 1** i.e. **Operation Redbridge 2024 AXA-3.E01/vol_vol1/Unalloc_3_0_65536** it shows **pw:truemen (Figure: 10.2)** which was enough to assume this is a password.

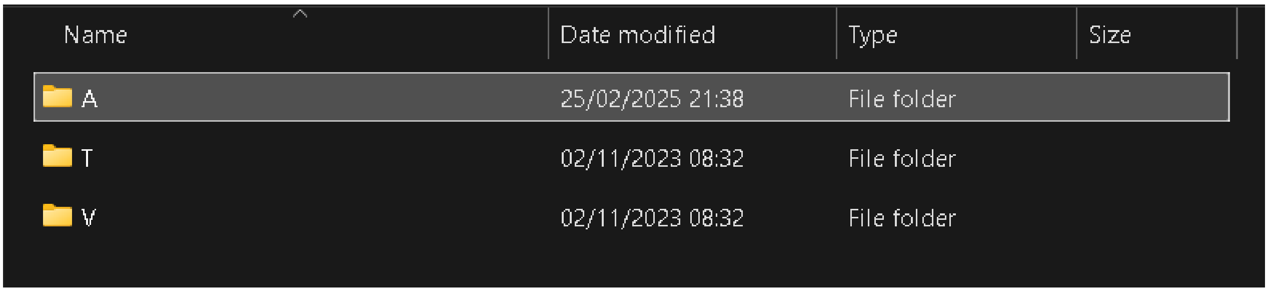


Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
Unalloc_3_0_65536				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	65536	Unallocated	Unallocated

```
t&fh
TCPAu2
r,fh
fSfSfUfh
Invalid partition tableError loading operating systemMissing operating system
pw:truemen
```

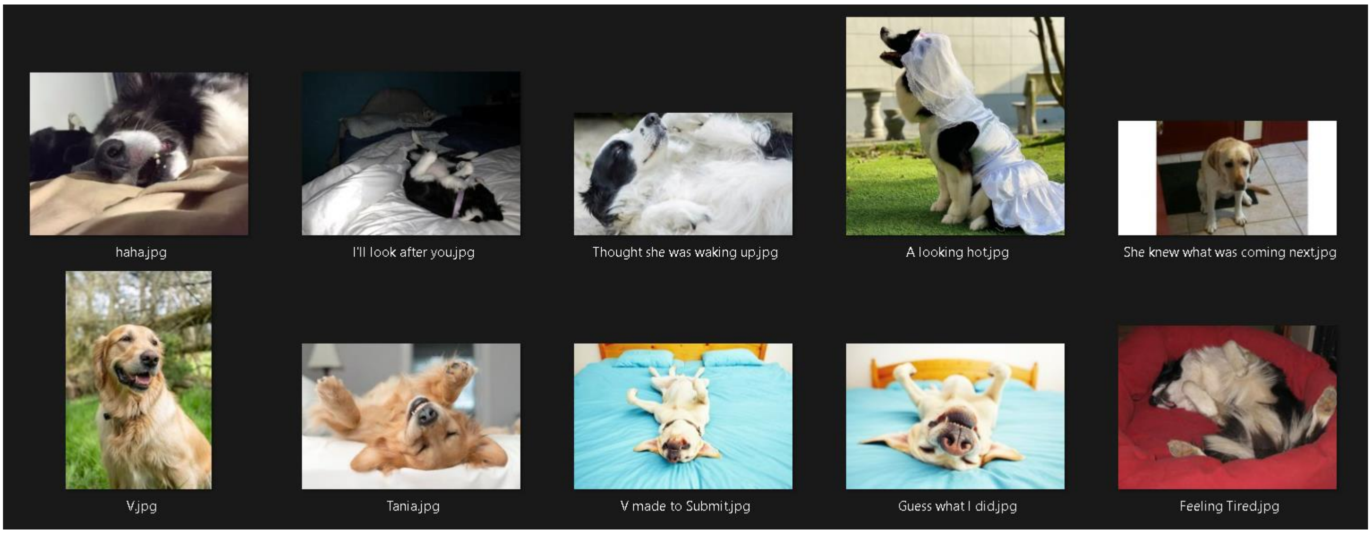
Figure:10.2

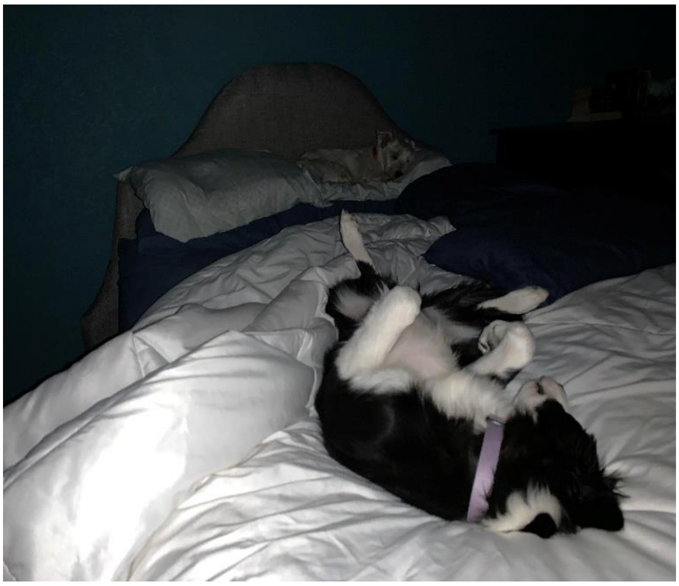
Access to **SYSTEM** file using **truemen** password was authorised and furthermore discovered 3 Folders **A, T & V** respectively which contained several photos with indecent captions **(Figure 10.3 & 10.4).** Here, **"A"** refers to **Anise** and **"V"** refers to **Victoria** (**Victoria's** picture found on her CV which matches the pictures of the folder **"V"**).



Name	Date modified	Type	Size
A	25/02/2025 21:38	File folder	
T	02/11/2023 08:32	File folder	
V	02/11/2023 08:32	File folder	

Figure:10.3


haha.jpg
I'll look after you.jpg
Thought she was waking up.jpg
A looking hot.jpg
She knew what was coming next.jpg
V.jpg
Tania.jpg
V made to Submit.jpg
Guess what I did.jpg
Feeling Tired.jpg



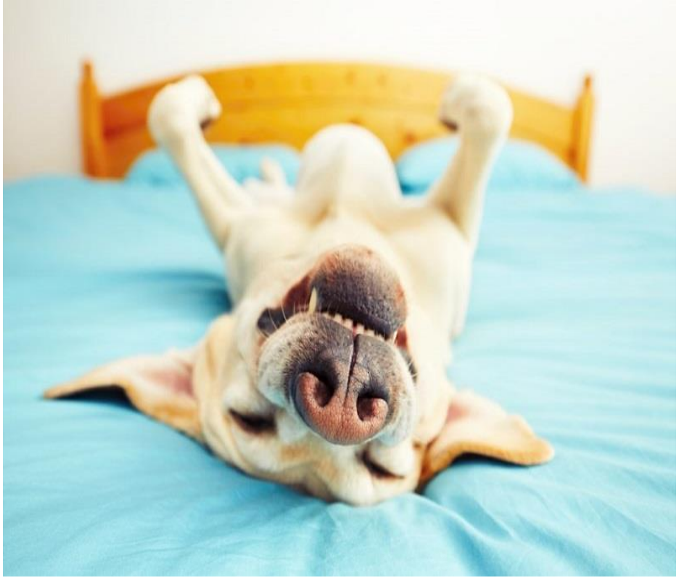
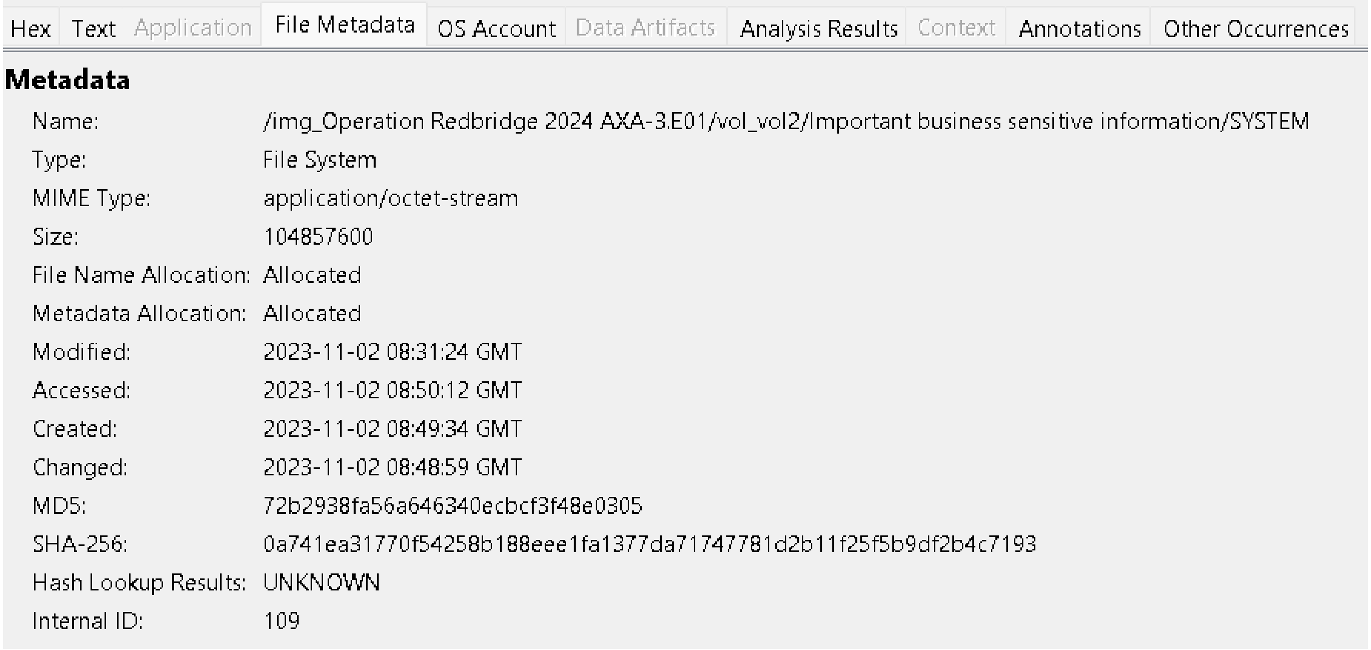


Figure: 10.4

- **The Meta-Data for Artefacts-10 is as follows:**



Metadata

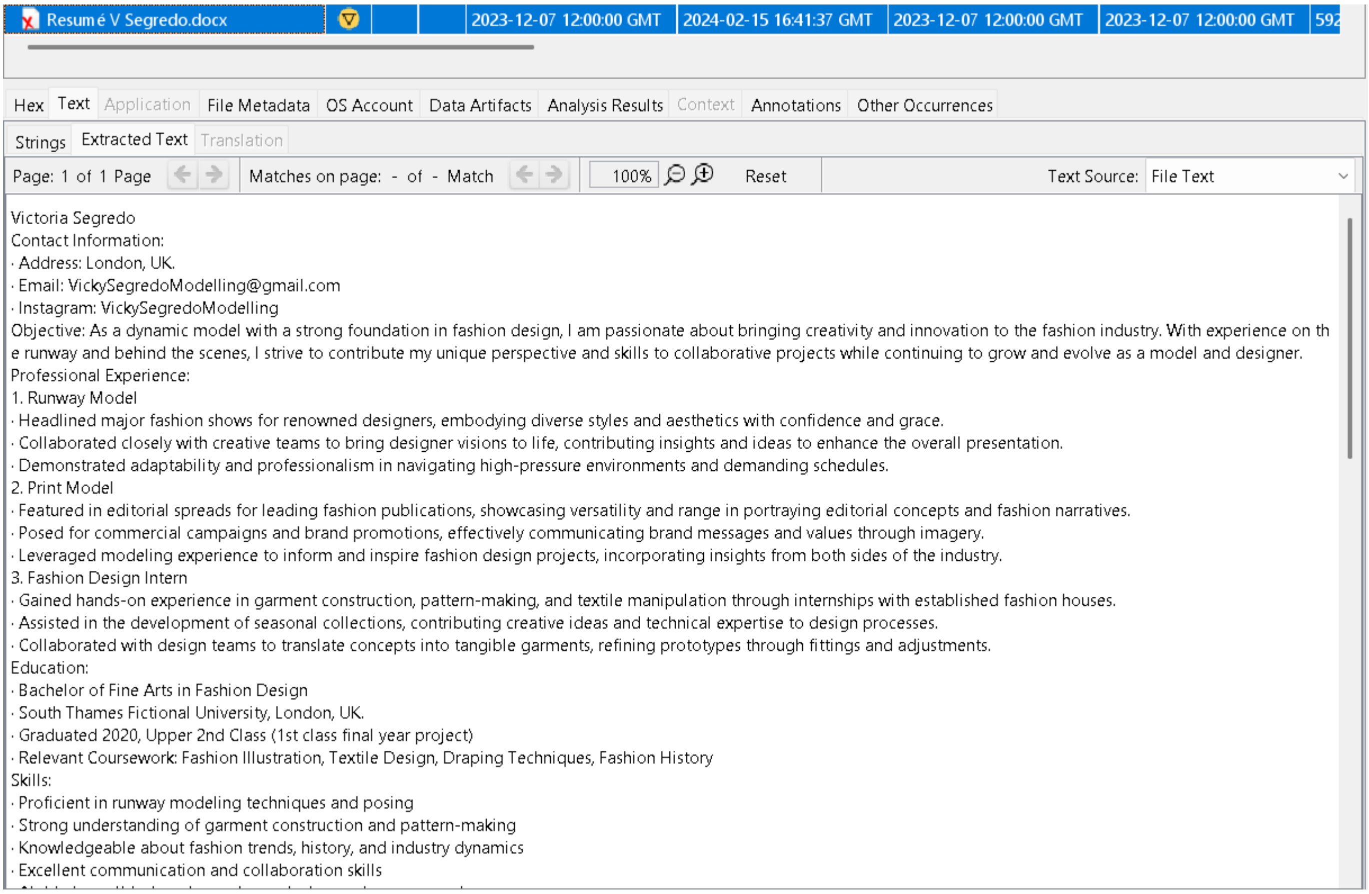
Name:	/img_Operation Redbridge 2024 AXA-3.E01/vol_vol2/Important business sensitive information/SYSTEM
Type:	File System
MIME Type:	application/octet-stream
Size:	104857600
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2023-11-02 08:31:24 GMT
Accessed:	2023-11-02 08:50:12 GMT
Created:	2023-11-02 08:49:34 GMT
Changed:	2023-11-02 08:48:59 GMT
MD5:	72b2938fa56a646340ecbcf3f48e0305
SHA-256:	0a741ea31770f54258b188eee1fa1377da71747781d2b11f25f5b9df2b4c7193
Hash Lookup Results:	UNKNOWN
Internal ID:	109

Figure:10.5

9.11 Artefacts-11

- **Location**: Operation Redbridge 2024 AXA-3.E01/vol_vol2/ Recent shoots and Models/Models/

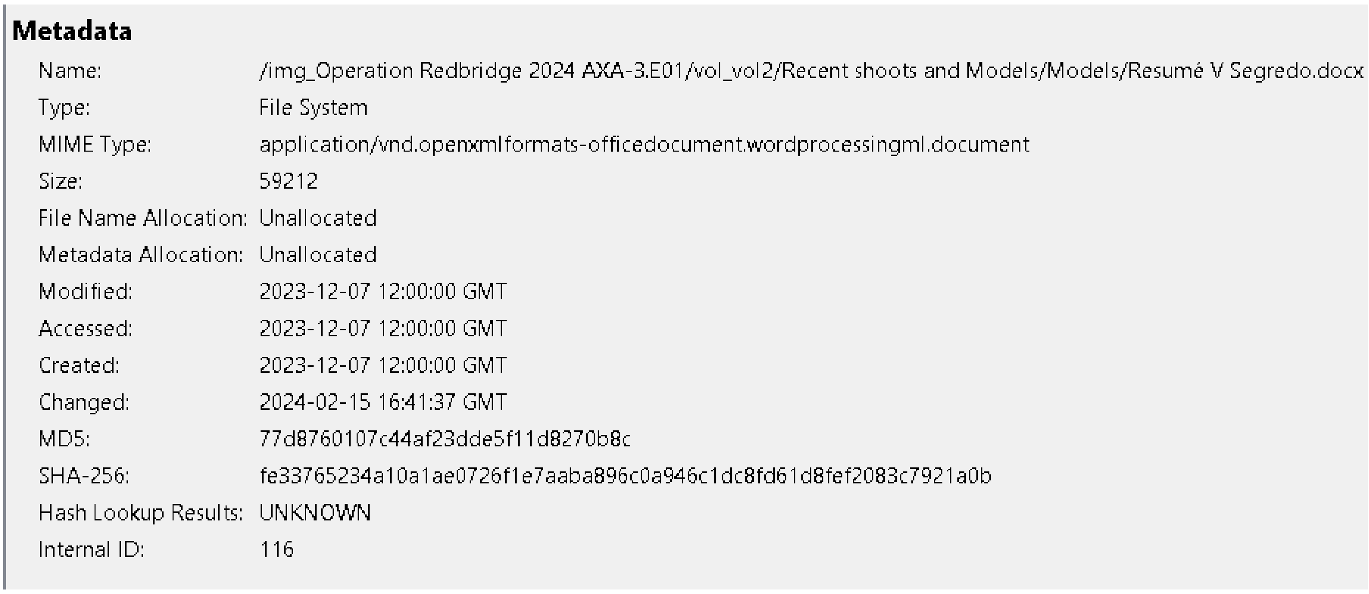
- **Reason Why This Evidence is Suspicious:** This item is suspicious as it has been intentionally deleted/hidden and might contain sensitive information. The CV belongs to Victoria and Anise referring back to **Figure: 10.3 & 10.4**, Indecent photos and captions have been taken. Hence, it can be said that Nicholas Has not only committed one crime but have tricked other girls into his grave crimes. **(Figure 7.1)**



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 industry. 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
· South Thames Fictional University, London, UK.
· Graduated 2020, Upper 2nd Class (1st class final year project)
· Relevant Coursework: Fashion Illustration, Textile Design, Draping Techniques, Fashion History
Skills:
· Proficient in runway modeling techniques and posing
· Strong understanding of garment construction and pattern-making
· Knowledgeable about fashion trends, history, and industry dynamics
· Excellent communication and collaboration skills

Figure-11.1

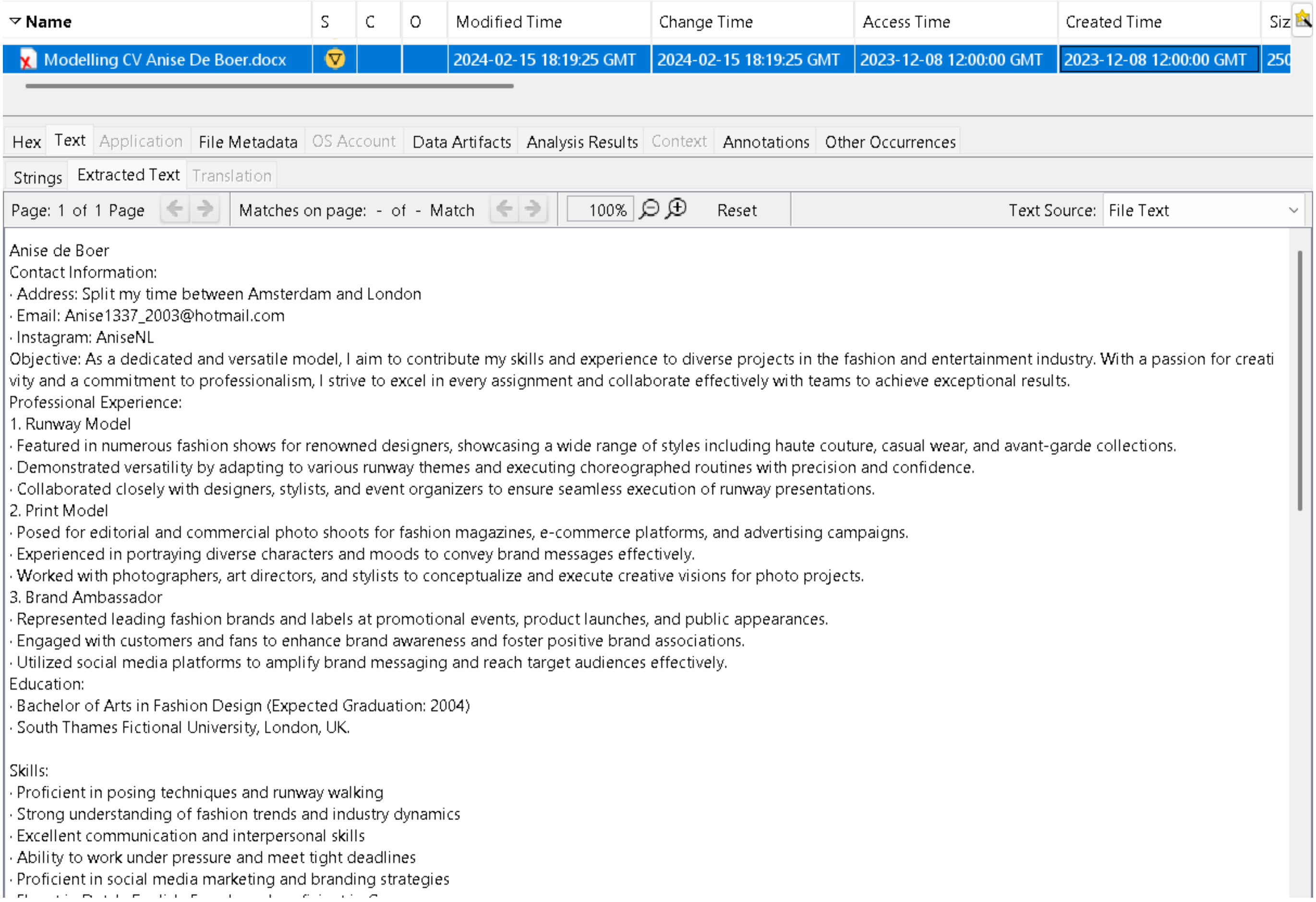
- **The Meta-Data for Artefacts-11 is as follows:**



Metadata

Name:	/img_Operation Redbridge 2024 AXA-3.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 12:00:00 GMT
Accessed:	2023-12-07 12:00:00 GMT
Created:	2023-12-07 12:00:00 GMT
Changed:	2024-02-15 16:41:37 GMT
MD5:	77d8760107c44af23dde5f11d8270b8c
SHA-256:	fe33765234a10a1ae0726f1e7aaba896c0a946c1dc8fd61d8fef2083c7921a0b
Hash Lookup Results:	UNKNOWN
Internal ID:	116

Figure: 11.2

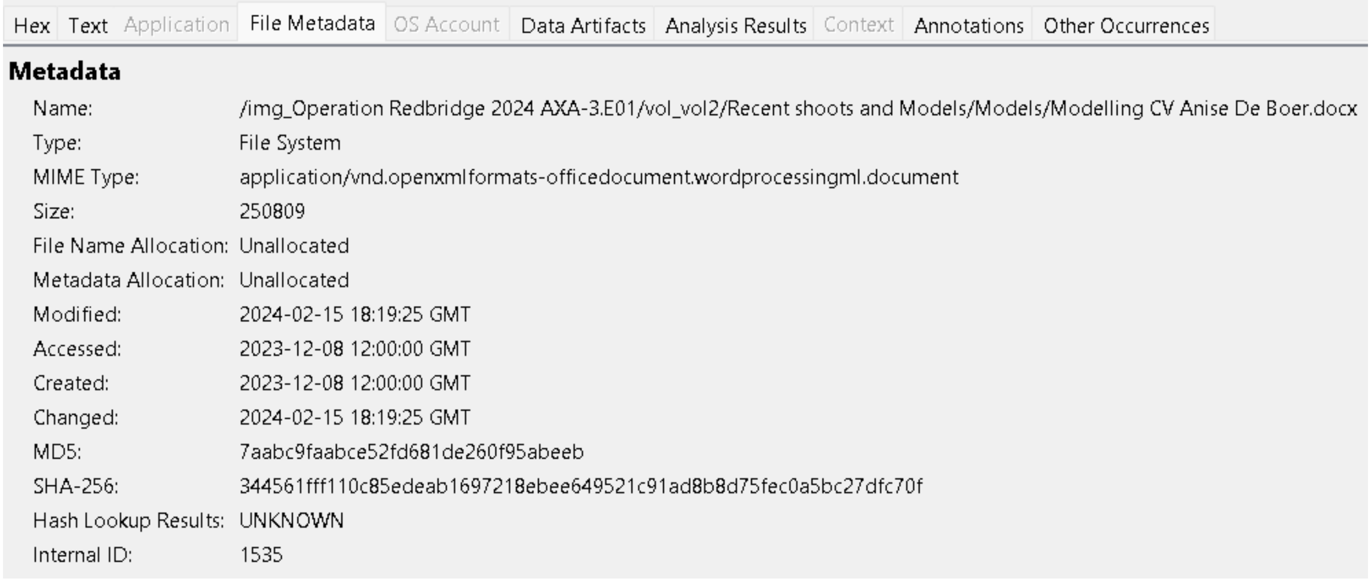


Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Siz
Modelling CV Anise De Boer.docx				2024-02-15 18:19:25 GMT	2024-02-15 18:19:25 GMT	2023-12-08 12:00:00 GMT	2023-12-08 12:00:00 GMT	250

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 creati
vity 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 collections.
· 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.

Skills:
· Proficient in posing techniques and runway walking
· Strong understanding of fashion trends and industry dynamics
· Excellent communication and interpersonal skills
· Ability to work under pressure and meet tight deadlines
· Proficient in social media marketing and branding strategies

Figure: 11.3



Metadata

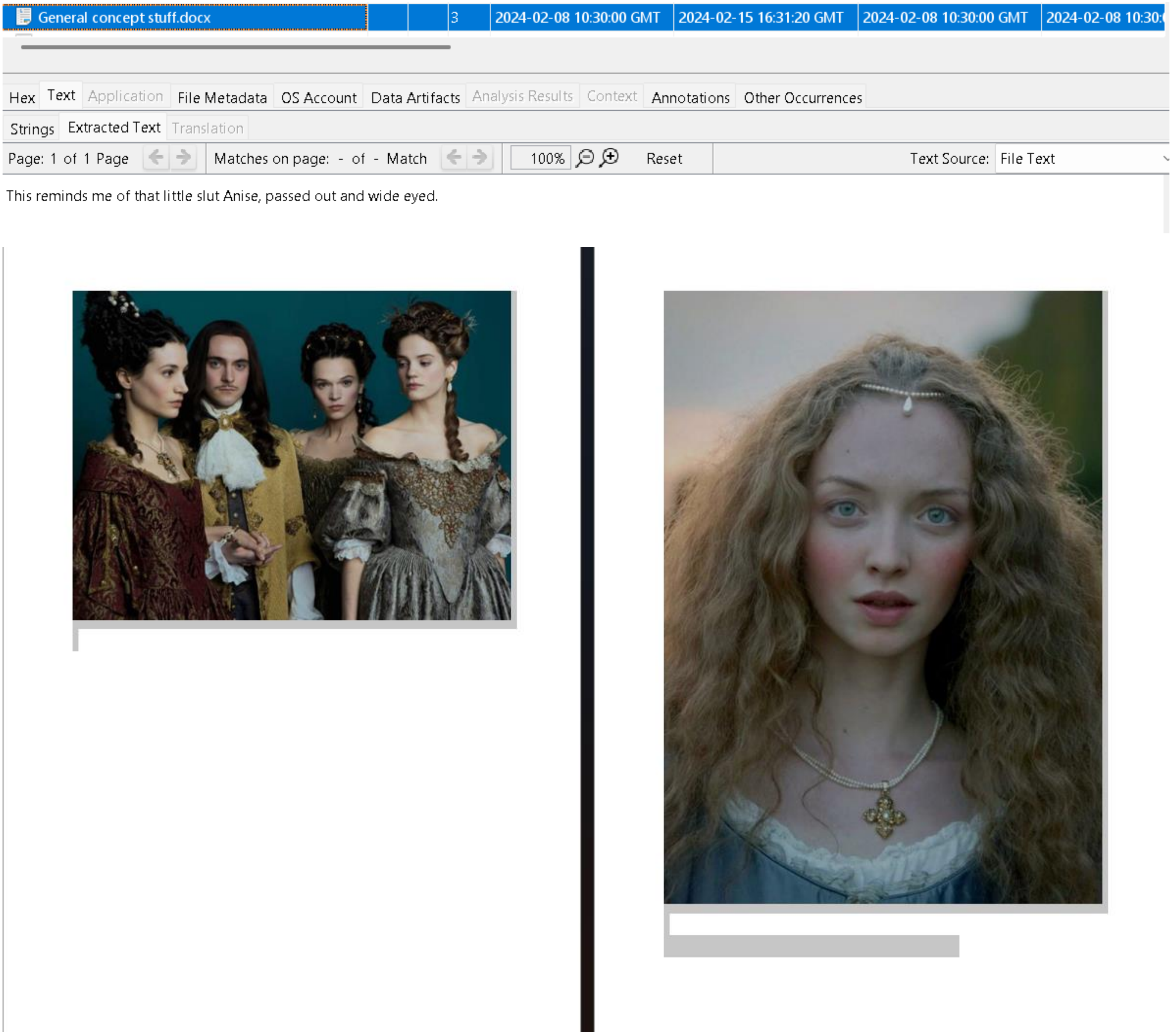
Name:	/img_Operation Redbridge 2024 AXA-3.E01/vol_vol2/Recent shoots and Models/Models/Modelling CV Anise De Boer.docx
Type:	File System
MIME Type:	application/vnd.openxmlformats-officedocument.wordprocessingml.document
Size:	250809
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	2024-02-15 18:19:25 GMT
Accessed:	2023-12-08 12:00:00 GMT
Created:	2023-12-08 12:00:00 GMT
Changed:	2024-02-15 18:19:25 GMT
MD5:	7aabc9faabce52fd681de260f95abeeb
SHA-256:	344561fff110c85edeab1697218ebee649521c91ad8b8d75fec0a5bc27dfc70f
Hash Lookup Results:	UNKNOWN
Internal ID:	1535

Figure: 11.4

9.12 Artefacts-12

- **Location**: Updates for Websites/General concept stuff.docx

- **Reason Why This Evidence is Suspicious:**
  While analysing this document using autopsy the picture was found with a text which was deliberately added to white text and white background for it to be hidden



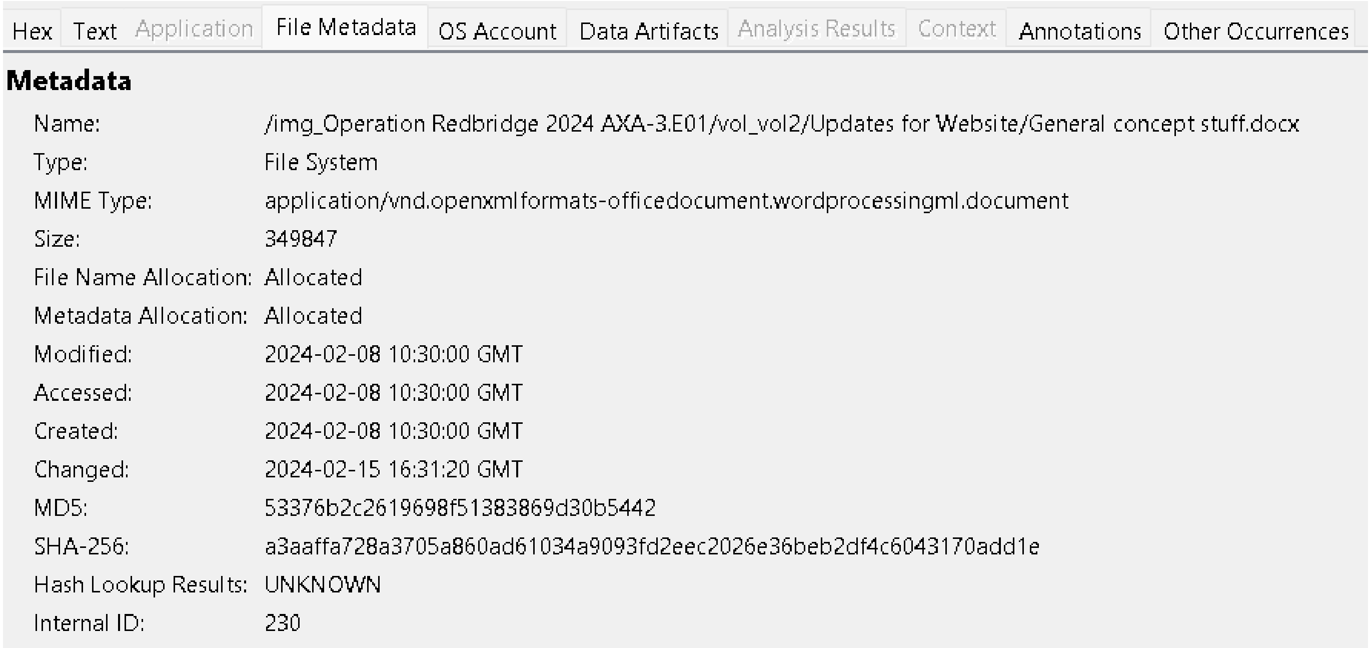
General concept stuff.docx | 3 | 2024-02-08 10:30:00 GMT | 2024-02-15 16:31:20 GMT | 2024-02-08 10:30:00 GMT | 2024-02-08 10:30:

Page: 1 of 1 Page | Matches on page: - of - Match | 100% | Reset | Text Source: File Text

This reminds me of that little slut Anise, passed out and wide eyed.

Figure:12.1

- **The Meta-Data for Artefacts-12 is as follows:**



Metadata

Name:	/img_Operation Redbridge 2024 AXA-3.E01/vol_vol2/Updates for Website/General concept stuff.docx
Type:	File System
MIME Type:	application/vnd.openxmlformats-officedocument.wordprocessingml.document
Size:	349847
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2024-02-08 10:30:00 GMT
Accessed:	2024-02-08 10:30:00 GMT
Created:	2024-02-08 10:30:00 GMT
Changed:	2024-02-15 16:31:20 GMT
MD5:	53376b2c2619698f51383869d30b5442
SHA-256:	a3aaffa728a3705a860ad61034a9093fd2eec2026e36beb2df4c6043170add1e
Hash Lookup Results:	UNKNOWN
Internal ID:	230

Figure:12.2

9.13 Artefacts-13

- **Location:**vol_vol2/Research/Flutrazempam-Wikipedia_files/155px-Iceland_Flutrazempam_Mylan_1mg.png
- **Reason Why This Evidence is Suspicious:** Flunitrazepam is known to cause sedation, memory impairment, and loss of consciousness. This links directly to Anise Famke DE BOER's allegations, as she reported feeling strange after drinking champagne and later losing consciousness, symptoms consistent with Flunitrazepam use.

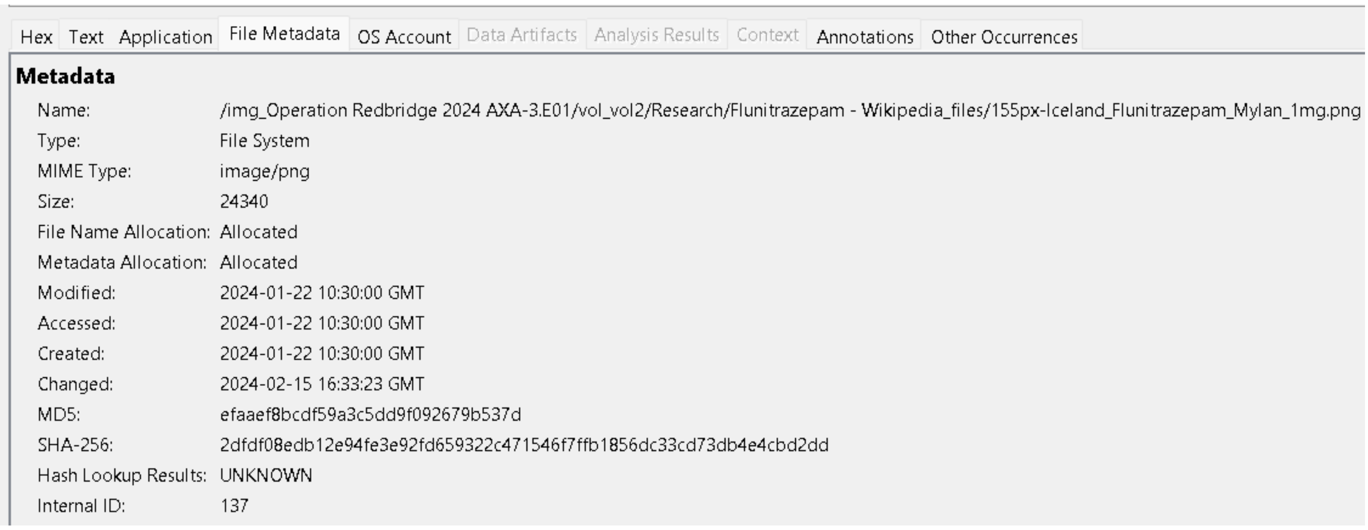
  The presence of this artefact, along with deleted files, encrypted images, and suspicious WhatsApp messages **(Artefact 7)**, supports the theory that VALENTINO was aware of the drug's effects and may have used it intentionally

  Flunitrazepam (Rohypnol) tablet package, suggests that Nicolas VALENTINO had knowledge of the drug. Combined with **Artefact 1** (a research paper on detecting Flunitrazepam in beverages), it indicates potential premeditation

Figure:13.1

Figure:13.2

- **The Meta-Data for Artefacts-12 is as follows:**



Metadata

```
Name:                  /img_Operation Redbridge 2024 AXA-3.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 10:30:00 GMT
Accessed:              2024-01-22 10:30:00 GMT
Created:               2024-01-22 10:30:00 GMT
Changed:               2024-02-15 16:33:23 GMT
MD5:                   efaaef8bcdf59a3c5dd9f092679b537d
SHA-256:               2dfdf08edb12e94fe3e92fd659322c471546f7ffb1856dc33cd73db4e4cbd2dd
Hash Lookup Results:   UNKNOWN
Internal ID:           137
```

Figure:13.3

10. CONCLUSION

Overview of the Case:

This investigation centres around allegations made by Anise Famke DE BOER against Nicolas VALENTINO, a boutique fashion designer and photographer. DE BOER claims she was drugged and sexually assaulted during a late-night photoshoot at VALENTINO's studio. She recalls drinking champagne that tasted unusual before passing out and later waking up under a blanket on the studio's sofa.

VALENTINO, on the other hand, insists that DE BOER consumed alcohol voluntarily and may have taken drugs on her own. He claims she simply fell asleep and denies any wrongdoing. However, forensic analysis uncovered deleted files, encrypted data, and evidence of physical damage to digital storage devices, raising serious concerns about possible evidence tampering.

Several digital exhibits were examined, including:

- **A destroyed memory card (AXA/1)** found in VALENTINO's wastebasket.
- **A damaged laptop (AXA/2)**, which the suspect claims was dropped, though forensic assessment suggests deliberate destruction.
- **An external hard drive (AXA/3)**, where crucial hidden files were recovered.

Findings from these devices strongly suggest an attempt to conceal potentially incriminating material and raise doubts about the suspect's version of events.

Timeline:

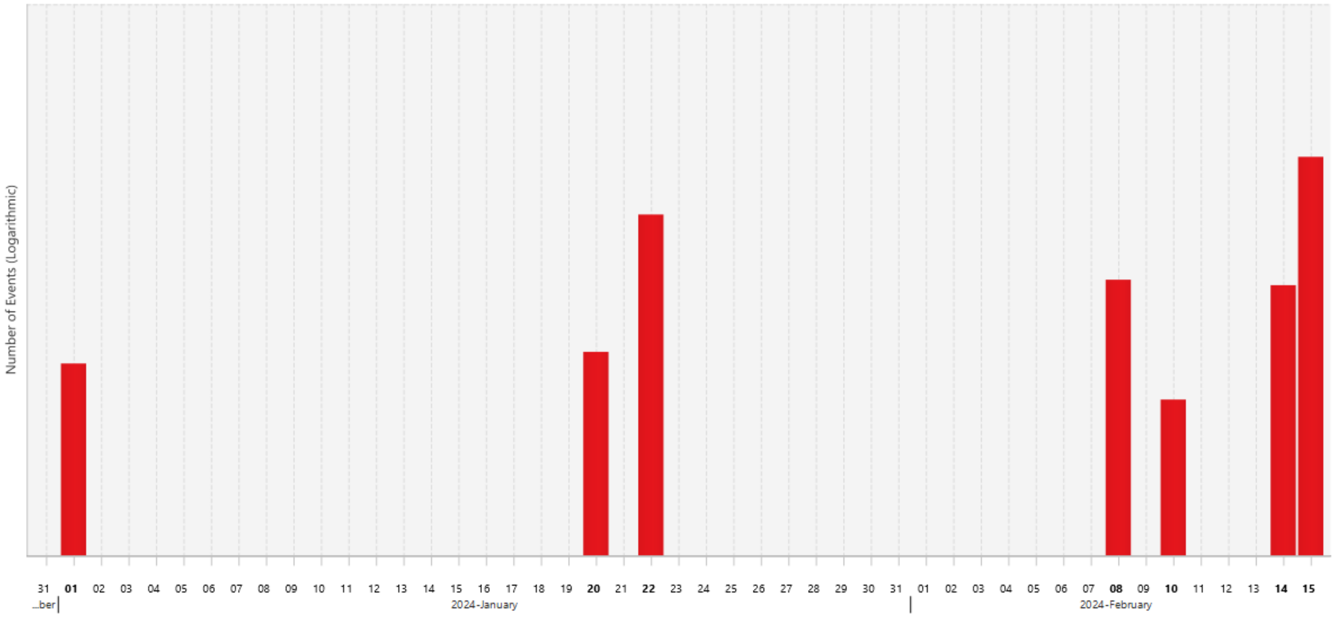
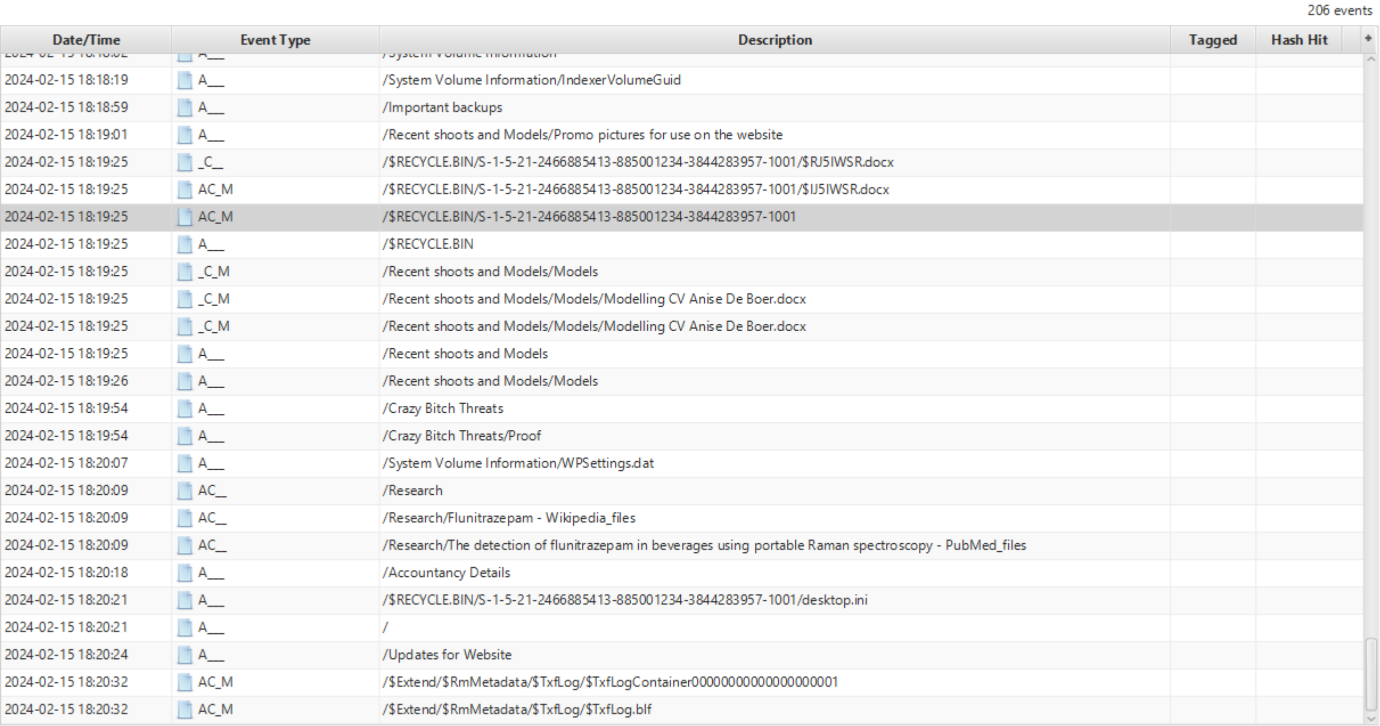


Figure- 6: Timeline of Artefacts (Time Range: 31/12/2023 - 15/02/2024)

The timeline displays file modifications, changes, and access events from **December 31, 2023**, to **February 15, 2024**, based on the artefacts identified in the report. It highlights key activity spikes, indicating potential file tampering, access, or deletion attempts. This timeline serves as key digital evidence in establishing the sequence of events and potential obstruction attempts.



206 events

Date/Time	Event Type	Description	Tagged	Hash Hit
2024-02-15 18:18:19	A__	/System Volume Information/IndexerVolumeGuid		
2024-02-15 18:18:59	A__	/Important backups		
2024-02-15 18:19:01	A__	/Recent shoots and Models/Promo pictures for use on the website		
2024-02-15 18:19:25	_C_	/$RECYCLE.BIN/S-1-5-21-2466885413-885001234-3844283957-1001/$RJ5IWSR.docx		
2024-02-15 18:19:25	AC_M	/$RECYCLE.BIN/S-1-5-21-2466885413-885001234-3844283957-1001/$IJ5IWSR.docx		
2024-02-15 18:19:25	AC_M	/$RECYCLE.BIN/S-1-5-21-2466885413-885001234-3844283957-1001		
2024-02-15 18:19:25	A__	/$RECYCLE.BIN		
2024-02-15 18:19:25	_C_M	/Recent shoots and Models/Models		
2024-02-15 18:19:25	_C_M	/Recent shoots and Models/Models/Modelling CV Anise De Boer.docx		
2024-02-15 18:19:25	_C_M	/Recent shoots and Models/Models/Modelling CV Anise De Boer.docx		
2024-02-15 18:19:25	A__	/Recent shoots and Models		
2024-02-15 18:19:26	A__	/Recent shoots and Models/Models		
2024-02-15 18:19:54	A__	/Crazy Bitch Threats		
2024-02-15 18:19:54	A__	/Crazy Bitch Threats/Proof		
2024-02-15 18:20:07	A__	/System Volume Information/WPSettings.dat		
2024-02-15 18:20:09	AC_	/Research		
2024-02-15 18:20:09	AC_	/Research/Flunitrazepam - Wikipedia_files		
2024-02-15 18:20:09	AC_	/Research/The detection of flunitrazepam in beverages using portable Raman spectroscopy - PubMed_files		
2024-02-15 18:20:18	A__	/Accountancy Details		
2024-02-15 18:20:21	A__	/$RECYCLE.BIN/S-1-5-21-2466885413-885001234-3844283957-1001/desktop.ini		
2024-02-15 18:20:21	A__	/		
2024-02-15 18:20:24	A__	/Updates for Website		
2024-02-15 18:20:32	AC_M	/$Extend/$RmMetadata/$TxfLog/$TxfLogContainer00000000000000000001		
2024-02-15 18:20:32	AC_M	/$Extend/$RmMetadata/$TxfLog/$TxfLog.blf		

Figure- 7: Autopsy Timeline Tool.

Key Artefacts Supporting or Undermining the Investigation

Artefacts That Support the Allegations

- **Document on Flunitrazepam (Rohypnol) Detection**

  A research article on detecting Flunitrazepam in beverages was found on VALENTINO's system.

  The presence of this document, especially before the alleged incident, raises suspicions of premeditation.

  Flunitrazepam is a well-known date rape drug, which makes this find particularly concerning.

- **Deleted and Recovered JPEG Files**

  A JPEG file (f0045957.jpg) was recovered from unallocated space, meaning it was deliberately deleted.

  The metadata was wiped, removing any trace of when the image was originally created or modified.

  This points to manual deletion or anti-forensic activity aimed at hiding its existence.

- **Hidden Audio Files in a Document**

  Audio recordings were found hidden inside a document disguised as an RTF file.

  The recordings contained disturbing conversations about past encounters with women, suggesting a pattern of behaviour.

  One voice mentioned "getting the last girl", which raises concerns that this may not be an isolated incident.

- **Encrypted System File with Indecent Images**

  Using VeraCrypt decryption, a hidden file labelled SYSTEM was unlocked.

  Inside, analysts found a folder containing images with explicit captions, which suggests exploitative behaviour.

- **Suspicious WhatsApp Chats**

  Messages reference selecting models, discussing previous incidents, and attempting to downplay accusations.

  Caitlyn LIN, a mutual acquaintance, previously confronted VALENTINO about inappropriate behaviour, which suggests a pattern of misconduct

  .

Artefacts That Undermine the Suspect's Defence

- **Destroyed Memory Card (AXA/1)**

  Found cut into two pieces in VALENTINO's wastebasket.

  This suggests an intentional attempt to destroy evidence.

- **Damaged Laptop (AXA/2)**

  The suspect claimed the laptop was accidentally dropped, but forensic examination revealed impact marks consistent with blunt force damage, likely from a hammer.

  The SSD was completely shattered, making recovery impossible—a common tactic for destroying digital evidence.

- **Three Memory Cards Found Blank**

  The forensic team found additional memory cards wiped clean.

  This strongly indicates data was erased before the police search.

Critical Features to Highlight for the Investigation Team

- **Clear Evidence of Tampering and Concealment**

  The destroyed memory card wiped hard drives, and suspiciously blank memory cards strongly suggest intentional destruction of evidence.

  The fact that forensic tools recovered deleted and hidden files implies the suspect took deliberate steps to remove or hide incriminating data.

- **Potential Additional Victims**

  The WhatsApp messages and hidden audio indicate DE BOER may not be the only victim.

  References to past incidents suggest VALENTINO's actions may be part of a pattern rather than an isolated event.

The possibility of other victims needs further investigation.

- **Advanced Digital Evasion Techniques Used**

  VALENTINO used encryption tools (VeraCrypt), steganography, and metadata manipulation, which are common techniques for hiding evidence.

  This level of digital obfuscation suggests he was aware of forensic methods and tried to prevent detection.

- **Contradictions in VALENTINO's Statement**

  He claimed DE BOER was simply sleeping, yet the presence of deleted and hidden files contradicts this claim.

  His destruction of key evidence is inconsistent with someone who has "nothing to hide."

  The document on drug detection raises serious questions about his knowledge and intent.

Opinion:
The forensic analysis reveals clear efforts to hide, delete, and encrypt data, suggesting that VALENTINO attempted to cover his tracks. The evidence does not explicitly prove guilt, but it raises strong concerns about his credibility and actions.

Key points:

- The deleted images, hidden recordings, and encrypted folders suggest an effort to obscure or erase evidence related to DE BOER's allegations.
- The WhatsApp conversations and recovered audio provide insight into a pattern of behaviour that warrants further scrutiny.
- The destruction of storage devices and manual data wiping indicate deliberate obstruction of the investigation.

Assumptions:

- The hidden and deleted files suggest premeditation rather than accidental deletion.
- The WhatsApp messages and past digital artifacts imply that DE BOER was not the first person to experience this.
- Given the deliberate digital evasion tactics, it is likely that additional incriminating data exists elsewhere, potentially in cloud backups or external drives.

Final Remarks:

This forensic analysis presents substantial digital evidence that supports the allegations made by DE BOER. The presence of deleted media, hidden recordings, encrypted files, and evidence of digital tampering strongly suggests that VALENTINO engaged in attempts to cover up potential wrongdoing.