

Digital Forensics Crime Scene Creation

Muhammad Irfan Ahmed

**Tools used: Autopsy, VeraCrypt, FTKimager,
Steganography, CCleaner, HashMyFiles, BulkFileChanger,
Encase.**

Contents

1. Overview of the Case	4
1.1 Narrative of the case	4
1.2 Details of the offenders, victims and witnesses	4
1.3 Photographs of any physical evidence, clues or supplemental material	5
1.4 Scenario Rules	5
2. Legislation Analysis	5
2.1 Legislation	5
2.2 Points to prove	5
2.3 What the Digital Forensics case can prove	6
2.4 What the Digital Forensics case will not prove	8
2.5 Highlight any artefacts that undermine the prosecution's case	8
3. Timeline of Artefacts	8
3.1 Reconnaissance / Research Phase Artefacts	8
3.2 Record Phase Artefacts	8
3.3 Result / Aftermath Artefacts	9
4. Artefacts	9
4.1 Summary of Artefacts	9
4.2 Other types of Artefacts	11
4.3 Details of the Evidence File	11
4.4 Details of the File System	12
4.5 Details of the Operating System	12
5. Artefacts	13
Artefact 1:	13
pic_1_dirt.jpg	13
Meta-Data of the artefact:	13
Method to hide/unhide artefact:	14
The type of Artefact	14
Artefact 2: Collection V1.mp4	15
Meta-Data of the artefact:	15
Method to hide/unhide artefact:	16
The type of Artefact	16
Artefact 3: SS.png	17
Meta-Data of the artefact:	17
Method to hide/unhide artefact:	18
The type of Artefact	18
Artefact 4: List.txt	19
Meta-Data of the artefact:	19
Method to hide/unhide artefact:	19
The type of Artefact	20

Artefact 5 : Confidential.pdf	21
Meta-Data of the artefact:	21
Method to hide/unhide artefact:	22
Artefact 6 : image_h.png	23
Meta-Data of the artefact:	23
Method to hide/unhide artefact:	23
The type of Artefact	24
Artefact 7 : _h.png	25
Meta-Data of the artefact:	25
Method to hide/unhide artefact:	26
Artefact 8 : MY-EYES-ONLY.txt	27
Meta-Data of the artefact:	28
Method to hide/unhide artefact:	28
The type of Artefact	28
Artefact 9 : Q3_financial_review.mp4	29
Meta-Data of the artefact:	29
Method to hide/unhide artefact:	30
The type of Artefact	30
Artefact 10 : family_day_out_plan.bin	31
Meta-Data of the artefact:	31
Method to hide/unhide artefact:	32
The type of Artefact	32
Artefact 11 : Radio_messages_h.docx	33
Meta-Data of the artefact:	33
Method to hide/unhide artefact:	34
The type of Artefact	34
Artefact 12: container	35
Meta-Data of the artefact:	35
Method to hide/unhide artefact:	36
The type of Artefact	36
Artefact 13 : pic_8_dirt.png	37
Meta-Data of the artefact:	37
Method to hide/unhide artefact:	38
The type of Artefact	38
Artefact 14 : VeraCrypt User Guide	39
Meta-Data of the artefact:	39
Method to hide/unhide artefact:	40
The type of Artefact	40
Artefact 15 : can you feel the rain.mp4	41
Meta-Data of the artefact:	42
Method to hide/unhide artefact:	42
The type of Artefact	42

1. Overview of the Case

1.1 Narrative of the case

At approximately 21:15 hrs on Wednesday 16 November 2022, Eliza Tilly, freelance graphic designer residing at Flat 5, Roach Tower, 65 Bow Street, B5 4TT, reached out to the authorities to report an invasion of privacy and digital harassment. According to Tilly's account, her ex-boyfriend, John Carter, had been circulating intimate photographs of her without her consent across several online platforms.

The situation escalated following their breakup a month ago, with Tilly receiving multiple emails and social media messages from unknown sources, threatening to share her private images publicly. On the day of the report, Tilly discovered that her photographs were indeed posted online, leading to immediate distress and prompting her to seek legal action.

Responding to Tilly's call, police officers executed a search warrant at John Carter's residence at 23:00 hrs. During the search, officers discovered a USB drive (exhibit AAA/1). The USB drive was hidden in a small safe in Carter's bedroom. Carter was not at home during the search, but his roommate, Nathan Crooks. Confirmed that Carter kept personal items and he never shared the safe's contents with anyone.

The following morning at 10:00 hrs, Carter was located and apprehended at a local gym. When questioned, he claimed innocence and ignorance about the existence of the photographs and denied any involvement in their distribution.

1.2 Details of the offenders, victims and witnesses

The offender of the case is John Carter, a male in his twenties, approximately 5'10 tall. The victim, Eliza Tilly, a freelance graphic designer who reported non-consensual distribution of intimate photographs. There was one key witness, Nathan Crooks, Carter's flatmate, who provided insight into Carter's behaviour and confirmed Carter's ownership of the USB device found at their shared residence. No other witnesses were present, but digital artefacts are under scrutiny, including the USB device (exhibit AAA/1).

1.3 Photographs of any physical evidence, clues or supplemental material

N/A

1.4 Scenario Rules

- Treat images of Border collie as images of the victim.
- Treat any dates with the year 2023 as erroneous dates.

2. Legislation Analysis

An offence under the Protection from Harassment Act 1997 sections 1,2,4 and 8, covering harassment, fear of violence, and remedies, coupled with section 33 of the Criminal Justice and Courts Act 2015, addressing the unauthorised disclosure of private sexual photographs and films to cause distress i.e. revenge porn.

2.1 Legislation

An offence under the Protection from Harassment Act 1997, which includes:

- Section 1: Prohibition of harassment
- Section 2: offence of harassment
- Section 4: putting people in fear of violence
- Section 8: remedies

And under the Criminal Justice and Courts Act 2015:

- Section 33: disclosing private sexual photographs and films with intent to cause distress (commonly known as revenge porn).

2.2 Points to prove

Key:

- Orange: pursue a course of conduct
- Red: Amounts to harassment of another/causes another to fear that violence will be used against them.
- Blue: knows that their course of conduct will cause fear of violence on each of these occasions.
- Purple: damages for any anxiety caused by the harassment and any financial loss resulting from the harassment / without the consent of an individual who appears in the photograph or film, and with the intention of causing that individual distress.
- Green: A person in pursuit of section 1 is guilty of an offence.

Protection from Harassment Act 1997:

Section 1: Prohibition of harassment

- A person must not pursue a course of conduct which amounts to harassment of another and which he knows or ought to know amounts to harassment of the other.

Section 2: offence of harassment

- A person who pursues a course of conduct in breach of section 1 is guilty of an offence.

Section 4: Putting people in fear of violence

- A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against them, and they know or ought to know that their course of conduct will cause fear of violence on each of those occasions.

Section 8: remedies

- Damages for any anxiety caused by the harassment and any financial loss resulting from the harassment.

Criminal Justice and Courts Act 2015:

Section 33: Disclosing private sexual photographs and films with intent to cause distress

- It is an offence for a person to disclose a private sexual photograph or film if the disclosure is made without the consent of an individual who appears in the photograph or film, and with the intention of causing that individual distress.

2.3 What the Digital Forensics case can prove

Existence of Harassment (PHA 1997, section 1): Point to prove: the suspect engaged in a course of conduct which amounts to harassment.

Artefacts:

- Artefact #3: chat screenshot containing threatening or harassing messages, proving a pattern or course of conduct.
- Artefact #11: documents containing hidden text that when revealed show threatening or harassing messages.

Harassment with Intent to cause fear (PHA 1997, section 4): point to prove: the harassment was with the intent to cause fear or provoke violence

Artefacts:

- Artefact #4: a document where the suspect outlines intentions to harass, evidencing intent.

Prohibition of disclosure of private sexual photographs and films (CJCA 2015, section 33): Point to prove: Prohibition of disclosure of private sexual photographs and films with intent to cause distress.

Artefacts:

- Artefact #1: private sexual photograph intended for revenge porn, demonstrating the content.
- Artefact #2: spliced video file of a private sexual nature, distinct from photographs, showing the varied types of content involved.

Evidence of hiding illegal activity: point to prove: the suspect attempted to hide or encrypt evidence pertaining to the legislation

Artefacts:

- Artefacts #6 & #7: images on the USB that contain hidden data through steganography.
- Artefact #8: file that is encoded and, when decoded, reveals evidence.
- Artefact #9: file names and paths altered to disguise the content
- Artefact #10 & #16: files with changed extensions to mask their true nature.
- Artefact #12: password-protected container files that upon unlocking contain additional evidence.
- Artefact #14: file hidden within the file explorer view settings.
- artefact #15: pdf file with manipulated file extension to obfuscate and act as png file.

2.4 What the Digital Forensics case will not prove

Physical use of device: the digital forensics case will not prove that the suspect physically used the device at the time the offending materials were created or accessed. While the evidence may imply the suspect's involvement, this does not confirm the suspect's physical actions.

2.5 Highlight any artefacts that undermine the prosecution's case.

None

3. Timeline of Artefacts

3.1 Reconnaissance / Research Phase Artefacts

This Phase starts: when John Carter starts considering retaliating against Eliza Tilly post-breakup by distributing private images.

This Phase Ends: just before he acquires or creates the images intended for harassment

- Artefact #4: a document where the suspect outlines intentions to harass, evidencing intent (PHA 1997, S4). A to-do list document indicating the suspect's mindset and plan to commit the offence.
- Artefact 3: screenshots of text messages containing threatening or harassing messages, proving a pattern or course of conduct (PHA 1997, S1).
- Artefact #5: pdf document containing evidence of objective, target websites to distribute and method of distribution.

3.2 Record Phase Artefacts

This Phase starts: when John Carter begins the actual offence of preparing and distributing the images.

This Phase Ends: when he completes the distribution of the images and the USB drive is hidden in the safe

- Artefact 1: private sexual photograph intended for revenge porn, showing the content of the offence (CJCA 2015 s33).
- Artefact 2: video files of a private sexual nature, indicating the prepared material for the offence (CJCA 2015 s33).

3.3 Result / Aftermath Artefacts

This Phase starts: after the offence is done, John Carter takes steps to hide his activities and evade detection.

This Phase Ends: when the USB device is seized by law enforcement from his safe.

- Artefacts #6 & #7 : images on the USB contain hidden data through steganography, revealing efforts to conceal the evidence.
- Artefact #8: encoded text detailing sensitive information
- Artefact #9: obfuscated file name and path to hide true nature.
- Artefact #10: files with changed extensions on the USB to mask their true nature.
- Artefact #11: documents containing hidden text that when revealed show threatening or harassing messages.
- Artefact #12: password-protected container files on the USB that upon unlocking contain additional evidence.
- artefact #13: image file hidden using file explorer view settings.
- Artefact #14: manipulated file header of docx file to mp4.
- Artefact #15: manipulated extension of a pdf file to png.

4. Artefacts

4.1 Summary of Artefacts

Total number of artefacts you have included: 15

Type of Artefacts	Artefact #	Artefact #
Content		
A document containing important information	#4	#5

A picture, audio or video.	#1	
Web cache Pages or Pictures		
Internet history records showing searches of relevant terms.		
Emails or chat artefacts	#3	
Hiding		
Encoded or encrypted text	#8	
Embedded text or information into a picture	#6	
Steg of pictures	#7	
Splicing – using software to edit audio, pictures or video together.	#2	
The ‘hidden’ flag within an operating system	#13	
Hiding text or pictures within a document	#11	
Manipulating file extensions	#10	#15
Manipulating file headers (magic numbers) to hide the file.	#14	
Obfuscation of file and/or path name.	#9	
Encrypted password-protected container	#12	
Recovery and Interpretation		
Most Recently Used (MRU)		
Link File Recent Activity		
Shellbags – the MRU for folders		
Thumbcache / Thumbs.db		
Registry Information – various things such as username, password and hint, installed software		
Artefacts within unallocated		
Deleted files (recycle bin)		
Deleted File (File System)		

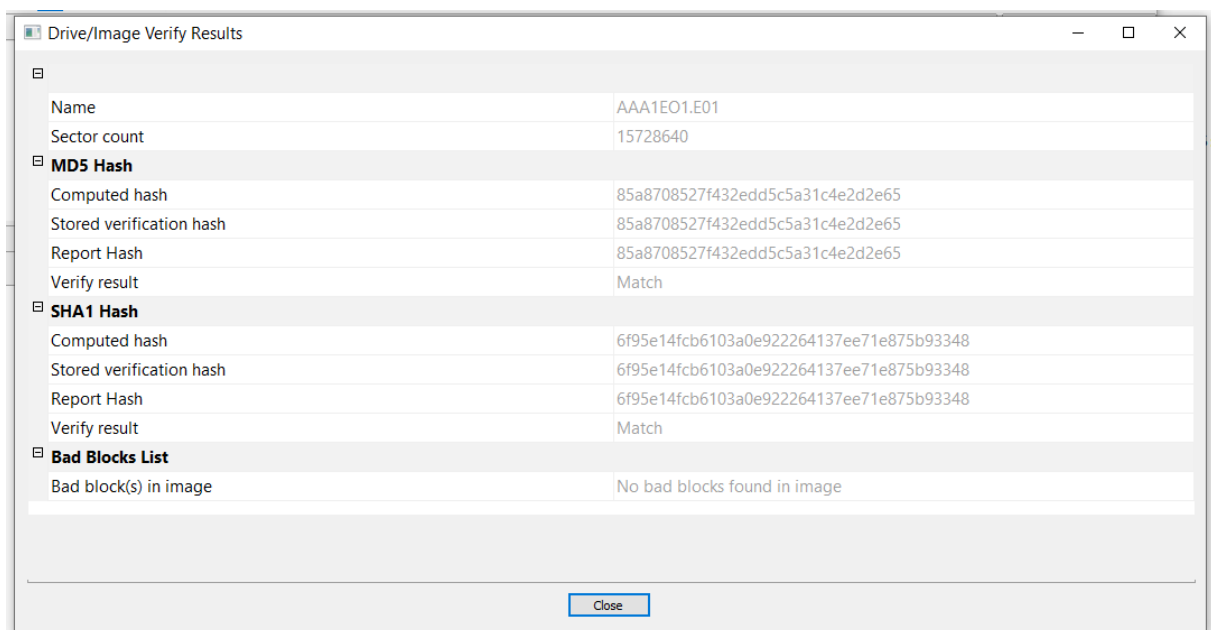
Table 1 – Artefact Type

4.2 Other types of Artefacts

N/A

4.3 Details of the Evidence File

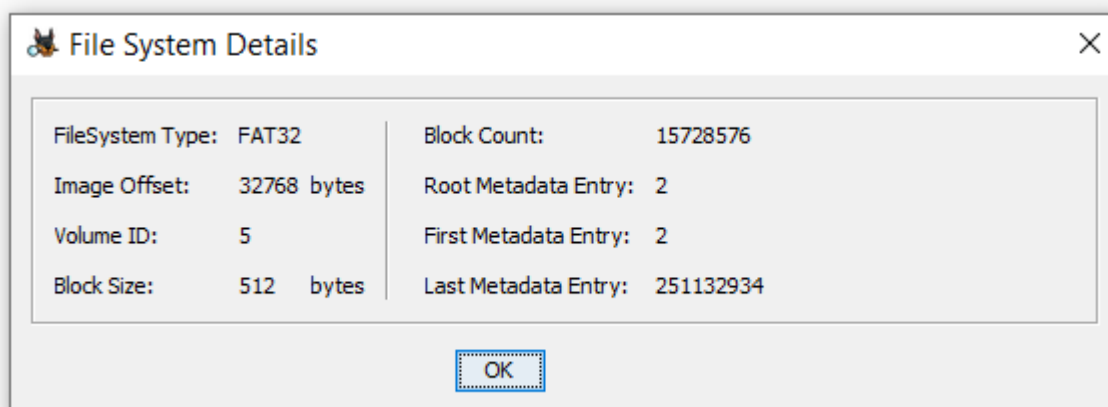
FTKImager details:



Autopsy verification:

Metadata	
Name:	/img_AAA1EO1.E01
Type:	E01
Size:	8053063680
MD5:	85a8708527f432edd5c5a31c4e2d2e65
SHA1:	6f95e14fcb6103a0e922264137ee71e875b93348
SHA-256:	Not calculated
Sector Size:	512
Time Zone:	Europe/London
Acquisition Details:	Description: untitled
:	Case Number: 1
:	Evidence Number: 1
:	Acquired Date: Fri Nov 17 15:46:38 2023
:	System Date: Fri Nov 17 15:46:38 2023
:	Acquiry Operating System: Win 201x
:	Acquiry Software Version: ADI4.5.0.3
Device ID:	69779c15-393c-47c4-99eb-e15f6e66d89a

4.4 Details of the File System



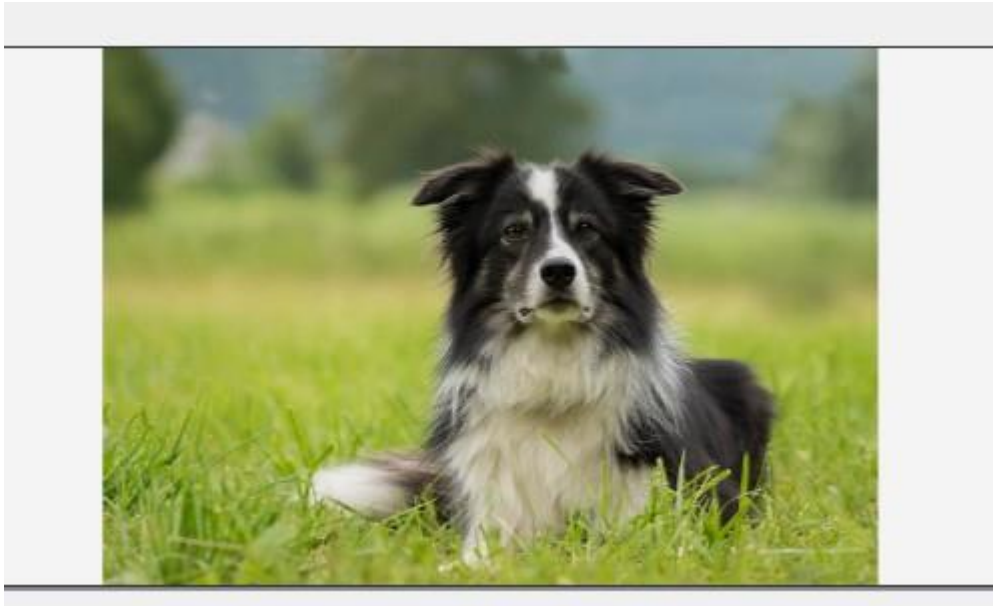
4.5 Details of the Operating System

N/A

5. Artefacts

Artefact 1:

pic_1_dirt.j
pg



Meta-Data of the artefact:

Metadata

Name:	/img_AAA1EO1.E01/vol_vol2/images/pic_1_dirt.jpg
Type:	File System
MIME Type:	image/jpeg
Size:	71388
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-11-09 18:00:00 GMT
Accessed:	2022-11-09 00:00:00 GMT
Created:	2022-11-09 18:00:00 GMT
Changed:	0000-00-00 00:00:00
MD5:	1ab855ebc7a1898b62409f2a979c4456
SHA-256:	943f146842921da6cc609e21e0466bafaeafa07e3b42900b157a1b7d16145f08
Hash Lookup Results:	UNKNOWN
Internal ID:	32

Implications of the Artefact:

This artefact is a series of private sexual photographs within the folder 'images' which implicates the suspect in the unauthorised distribution of private sexual images (CJCA 2015 section 33). The existence of such images in the suspect's possession suggests an intent to cause distress through revenge porn. There are multiple images present within the folder, and they all have the same timestamp which could mean that they originate elsewhere and were placed within here.

Method to hide/unhide artefact:

These images were not hidden and were rather placed in a folder called 'images'. There was no specific method to hide these images. The straightforward approach could indicate that the suspect has not gotten to hiding this folder yet.

The type of Artefact

CONTENT: A picture, audio or video.

Artefact Detail Table

Artefact is	Tick Appropriat e
Application Level	x
OS Level	
File System Level	
Reconnaissance / Research phase	x
Recording phase	
Result / Aftermath phase	

Artefact 2: Collection V1.mp4



Meta-Data of the artefact:

Metadata

Name:	/img_AAA1EO1.E01/vol_vol2/Videos/Collection V1.mp4
Type:	File System
MIME Type:	video/mp4
Size:	1181195
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-11-09 19:00:00 GMT
Accessed:	2022-11-09 00:00:00 GMT
Created:	2022-11-09 19:00:00 GMT
Changed:	0000-00-00 00:00:00
MD5:	b9174c8598d279b4439a7f7b66f1eb84
SHA-256:	ccdd43e0f9522f761c4089806659472eeeb9ea0176019d2ff0355179f76b09c8
Hash Lookup Results:	UNKNOWN
Internal ID:	158

Implications of the Artefact:

This video file, created using editing software, conceals private sexual content. The splicing method serves to hide the illegal content within seemingly harmless videos, indicating deliberate efforts to avoid detection while engaging in prohibited conduct. The hidden content within the video is in violation of CICA 2015 section 33 as it includes the unauthorised distribution of sexual content.

Method to hide/unhide artefact:

Their method of hiding was that the video was spliced together using a website called 'kapwing' and the illegal content was placed within two different videos which are harmless thus hiding the content.

The type of Artefact

HIDING: splicing - using software to edit audio, pictures or video together.

Artefact Detail Table

Artefact is	Tick Appropriat e
Application Level	x
OS Level	
File System Level	
Reconnaissance / Research phase	
Recording phase	x
Result / Aftermath phase	

Artefact 3: SS.png



Meta-Data of the artefact:

Metadata	
Name:	/img_AAA1EO1.E01/vol_vol2/SS.png
Type:	File System
MIME Type:	image/png
Size:	68850
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-11-13 21:04:16 GMT
Accessed:	2022-11-13 00:00:00 GMT
Created:	2022-11-13 21:04:12 GMT
Changed:	0000-00-00 00:00:00
MD5:	Not calculated
SHA-256:	Not calculated
Hash Lookup Results:	UNKNOWN
Internal ID:	177

Implications of the Artefact:

This screenshot of text messages contains threatening or harassing content, evidencing a pattern of abusive behaviour. Its presence demonstrates the suspect's engagement in harassment and implies a level of premeditation.

Method to hide/unhide artefact:

This artefact was not hidden, the lack of concealment could indicate the suspect did not get to hide it due to other artefacts being hidden.

The type of Artefact

CONTENT: Emails or chat artefacts

Artefact Detail Table

Artefact is	Tick Appropriat e
Application Level	x
OS Level	
File System Level	
Reconnaissance / Research phase	X
Recording phase	
Result / Aftermath phase	

Artefact 4: List.txt

```
List - Notepad
File Edit Format View Help
Revenge time

To-Do:
1. Collect all photographs and videos from times with her.
2. Choose the most private and intimate ones - the ones she would aint gonna like on the web.
3. Find websites where I can upload them.
4. Spread them in a way that they come back to haunt her career and social life.
5. Cover tracks - maybe use a VPN, delete history, and clean up any evidence.
6. Keep copies of everything... just in case.

Reminders:
- Dont act when angry, wait for the right time.
- Make sure they dont get back to me.
- This is about making her feel what I felt - the betrayal and the hurt.

JC.
```

Meta-Data of the artefact:

Metadata	
Name:	/img_AAA1EO1.E01/vol_vol2/List.txt
Type:	File System
MIME Type:	text/plain
Size:	613
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-11-09 17:30:22 GMT
Accessed:	2022-11-09 00:00:00 GMT
Created:	2022-11-09 17:30:12 GMT
Changed:	0000-00-00 00:00:00
MD5:	Not calculated
SHA-256:	Not calculated
Hash Lookup Results:	UNKNOWN
Internal ID:	171

Implications of the Artefact:

A document outlining the suspect intends to harass, this artefact is critical in establishing premeditation. It reveals the suspect's mindset and planned steps to commit harassment, making it a crucial piece of evidence for intent.

Method to hide/unhide artefact:

This artefact was not hidden making it easily accessible and potentially incriminating. The suspect's failure to conceal could indicate overconfidence, negligence or lack of time to get to finding a suitable method of concealment.

The type of Artefact

CONTENT: a document containing important information

Artefact Detail Table

Artefact is	Tick Appropriat e
Application Level	x
OS Level	
File System Level	
Reconnaissance / Research phase	x
Recording phase	
Result / Aftermath phase	

Artefact 5 : Confidential.pdf

Confidential - JCDistribution

Objective:

Revenge

Targets:

- ImageShack (imageshack.us) – Webpage for image sharing.
- Reddit (reddit.com) - Specific subreddits aimed at image sharing for rapid dissemination.
- Imgur (imgur.com) - Utilized for anonymous posting and sharing.
- Twitter (twitter.com) - To post links to the content under burner accounts for widespread sharing.

Method:

- Use VPN to hide the origin of the posts.
- post them during peak traffic hours to ensure high visibility.

Password Protocols:

- Secure all sensitive preparatory materials in an encrypted container.
- Password: she_a_skeezzer123

Meta-Data of the artefact:

Metadata

Name:	/img_AAA1EO1.E01/vol_vol2/Confidential.pdf
Type:	File System
MIME Type:	application/pdf
Size:	213546
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-11-10 10:30:54 GMT
Accessed:	2022-11-10 00:00:00 GMT
Created:	2022-11-10 10:30:08 GMT
Changed:	0000-00-00 00:00:00
MD5:	Not calculated
SHA-256:	Not calculated
Hash Lookup Results:	UNKNOWN
Internal ID:	166

Implications of the Artefact:

This document contains the suspect's plans for distributing the illegal content. It includes the target websites and methods for dissemination, further supporting the notion of premeditated malicious intent.

Method to hide/unhide artefact:

This artefact was not hidden similar to artefact 4 and it's accessibility could be due to the suspect not having enough time to get to hiding this artefact.

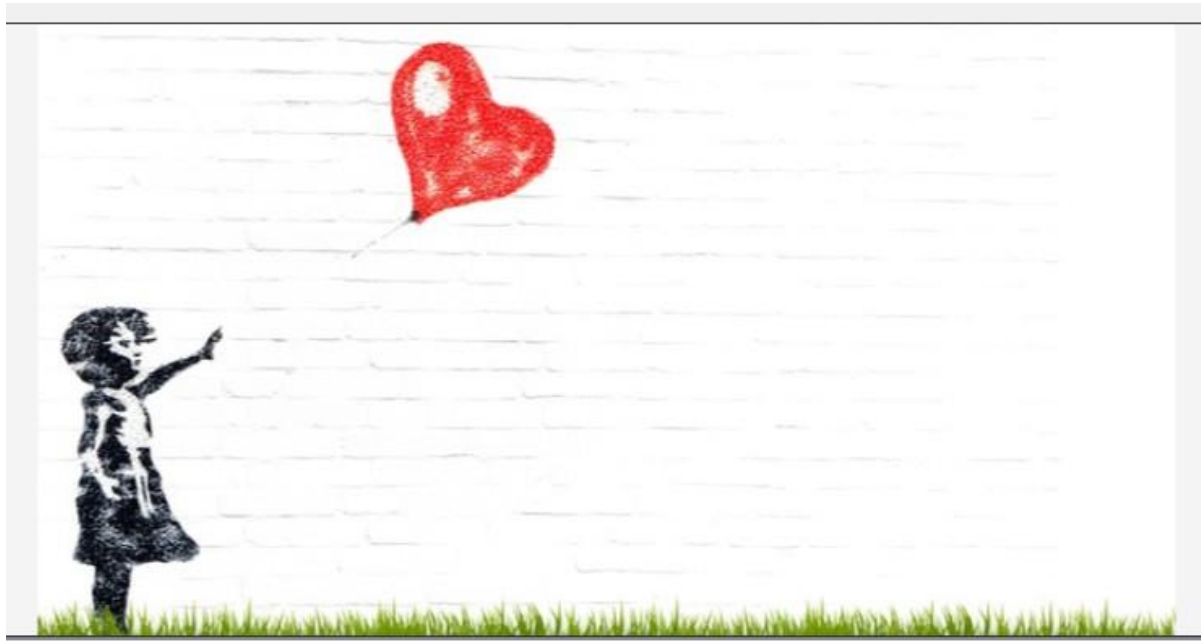
The type of Artefact

CONTENT: A document containing important information

Artefact Detail Table

Artefact is	Tick Appropriat e
Application Level	x
OS Level	
File System Level	
Reconnaissance / Research phase	x
Recording phase	
Result / Aftermath phase	

Artefact 6 : image_h.png



Meta-Data of the artefact:

Metadata

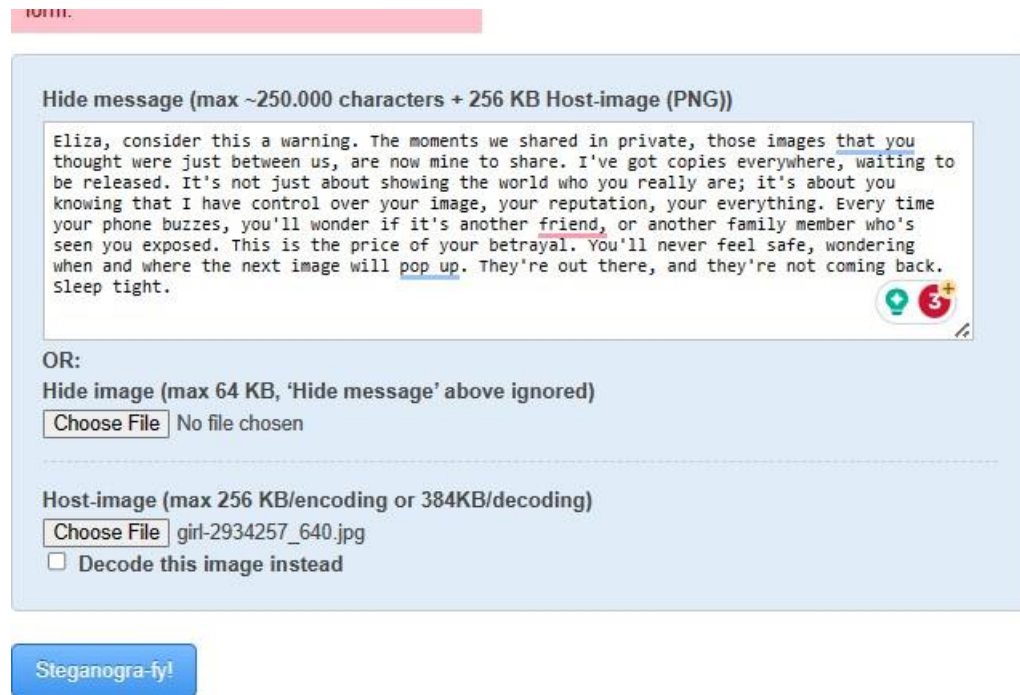
Name:	/img_AAA1EO1.E01/vol_vol2/images/image_h.png
Type:	File System
MIME Type:	image/png
Size:	138348
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-11-14 13:05:00 GMT
Accessed:	2022-11-14 00:00:00 GMT
Created:	2022-11-14 13:05:00 GMT
Changed:	0000-00-00 00:00:00
MD5:	894e33ee2bf7171ae3f88eb307c4b907
SHA-256:	f576990d22ff59a2cfdbe266744f5474c2a3cb4f3d24117dd0c95dec796a40f6
Hash Lookup Results:	UNKNOWN
Internal ID:	30

Implications of the Artefact:

This image, altered through steganography to embed hidden text, indicates an effort to conceal sensitive information. This method used for hiding this information points towards a sophisticated attempt to disguise and protect incriminating data.

Method to hide/unhide artefact:

This artefact was a result of steganography and there was text embedded into the information. The method to hide the information was by using a website to steg the text into the image. This method of hiding information within a picture makes the embedded text undetectable without specific knowledge or tools.



10111.

Hide message (max ~250.000 characters + 256 KB Host-image (PNG))

Eliza, consider this a warning. The moments we shared in private, those images that you thought were just between us, are now mine to share. I've got copies everywhere, waiting to be released. It's not just about showing the world who you really are; it's about you knowing that I have control over your image, your reputation, your everything. Every time your phone buzzes, you'll wonder if it's another friend, or another family member who's seen you exposed. This is the price of your betrayal. You'll never feel safe, wondering when and where the next image will pop up. They're out there, and they're not coming back. Sleep tight.

OR:

Hide image (max 64 KB, 'Hide message' above ignored)

No file chosen

Host-image (max 256 KB/encoding or 384KB/decoding)

girl-2934257_640.jpg

☐ Decode this image instead

Steganogra-fy!

The type of Artefact

HIDING: embedded text or information into a picture

Artefact Detail Table

Artefact is	Tick Appropriate
Application Level	x
OS Level	
File System Level	x
Reconnaissance / Research phase	
Recording phase	
Result / Aftermath phase	x

Artefact 7 : _h.png



Meta-Data of the artefact:

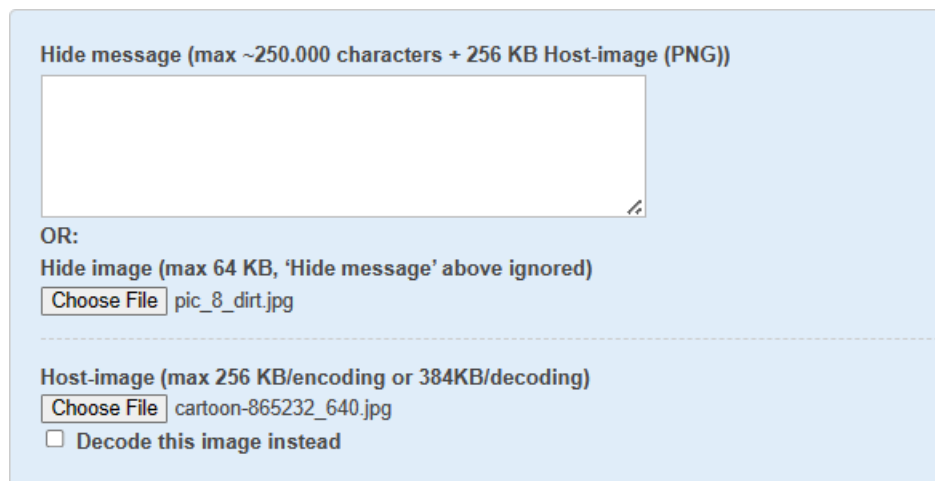
Metadata	
Name:	/img_AAA1EO1.E01/vol_vol2/images/_h.png
Type:	File System
MIME Type:	image/png
Size:	383077
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-11-14 13:00:00 GMT
Accessed:	2022-11-14 00:00:00 GMT
Created:	2022-11-14 13:00:00 GMT
Changed:	0000-00-00 00:00:00
MD5:	a9df138e5e22735f0b62d3926f7ef3dd
SHA-256:	f078e74511091fcc1c58b653933562f4829e2e4be48cb7a4506dd65753c3f94e
Hash Lookup Results:	UNKNOWN
Internal ID:	50

Implications of the Artefact:

Similar to artefact 6, this artefact employs steganography, showcasing the suspect's use of techniques to hide illicit content within images.

Method to hide/unhide artefact:

The method to hide the artefact was similar to artefact 6 and the steganography website was used to hide an image within another image. This artefact relates to artefact 14 as artefact 14 was the artefact that was hidden within this image, and then artefact 14 was then hidden using the method outlined within that section.



The screenshot shows a web interface for steganography. At the top, it says "Hide message (max ~250.000 characters + 256 KB Host-image (PNG))" with a large text input area below it. Below the input area, it says "OR:" followed by "Hide image (max 64 KB, 'Hide message' above ignored)". Under this, there is a "Choose File" button and the filename "pic_8_dirt.jpg". A dashed line separates this section from the next one. The next section is titled "Host-image (max 256 KB/encoding or 384KB/decoding)" and also has a "Choose File" button with the filename "cartoon-865232_640.jpg". At the bottom of this section, there is a checkbox labeled "Decode this image instead".

The type of Artefact

HIDING: steg of pictures

Artefact Detail Table

Artefact is	Tick Appropriate
Application Level	x
OS Level	
File System Level	x
Reconnaissance / Research phase	
Recording phase	
Result / Aftermath phase	x

Artefact 8 : MY-EYES-ONLY.txt

[illegible]

Meta-Data of the artefact:

Metadata	
Name:	/img_AAA1EO1.E01/vol_vol2/MY-EYES-ONLY.txt
Type:	File System
MIME Type:	text/plain
Size:	1148
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-11-14 10:02:22 GMT
Accessed:	2022-11-14 00:00:00 GMT
Created:	2022-11-14 10:00:12 GMT
Changed:	0000-00-00 00:00:00
MD5:	Not calculated
SHA-256:	Not calculated
Hash Lookup Results:	UNKNOWN
Internal ID:	173

Implications of the Artefact:

This artefact features encoded text which was converted to morse code. This demonstrates the suspect's efforts to conceal sensitive information. The encoding serves as a barrier against causal discovery, implying an intention to shield illegal activities from scrutiny.

Method to hide/unhide artefact:

The aim was to encode sensitive information and this was done by using cyberchef to change the content from normal text to morse code so if an unwanted viewer was to check the file, all they would see is morse code and would not be able to read it unless decoded.

The type of Artefact

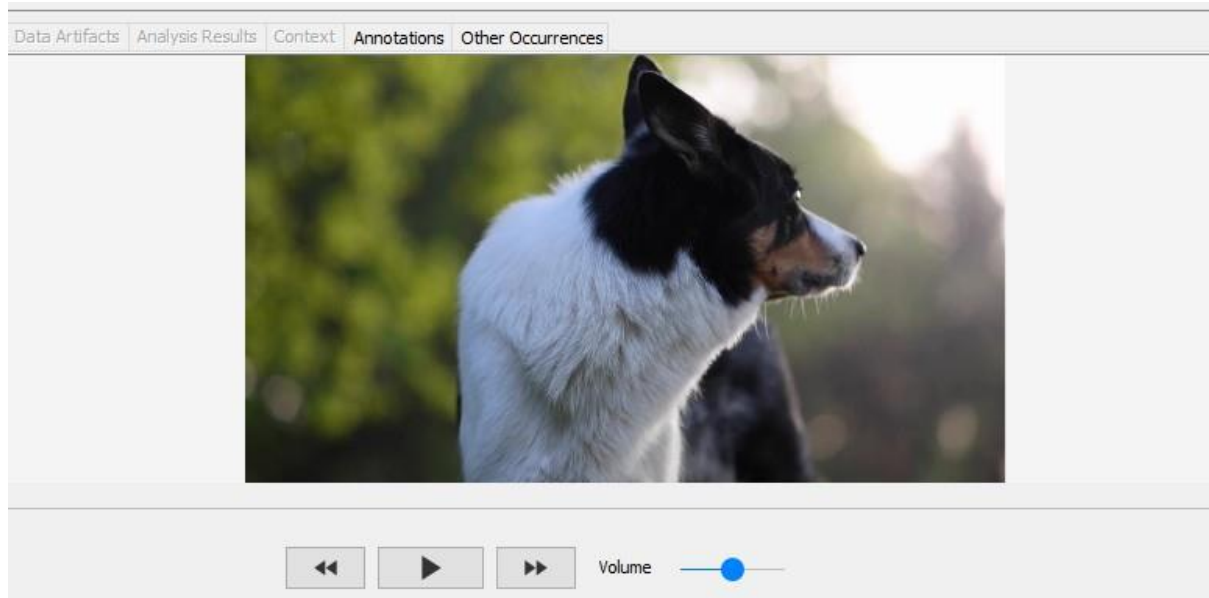
HIDING: encoded or encrypted text

Artefact Detail Table

Artefact is	Tick Appropriat e
Application Level	x
OS Level	
File System Level	x
Reconnaissance / Research phase	

Recording phase	
Result / Aftermath phase	x

Artefact 9 : Q3_financial_review.mp4



Meta-Data of the artefact:

Metadata

```

Name: /img_AAA1EO1.E01/vol_vol2/MyFinances/Q3_financial_review.mp4
Type: File System
MIME Type: video/mp4
Size: 4667460
File Name Allocation: Allocated
Metadata Allocation: Allocated
Modified: 2022-11-14 15:25:56 GMT
Accessed: 2022-11-14 00:00:00 GMT
Created: 2022-11-14 15:25:56 GMT
Changed: 0000-00-00 00:00:00
MD5: 1e6a3ea5ec5b256aaaf3b8e34e18d4c2
SHA-256: eb0a61f9c44c09893ecfe5c38caf3df0e9bbc12fd55bdad0373bcc2792740ad1
Hash Lookup Results: UNKNOWN
Internal ID: 153

```

Implications of the Artefact:

The renaming and repositioning of this file within the financial folder suggests a deliberate attempt to obfuscate and mislead. This act of camouflaging potentially incriminating content within innocuous file names and locations indicates a calculated effort to evade detection.

Method to hide/unhide artefact:

To hide the data was done by using the command line to move the file from the videos folder to the MyFinances folder which was created for this purpose and then the file was named related to finances to hide it and have it blend in to the topic of finances. The file was accessed using PowerShell, and within here we created a folder and named it MyFinances and generated 49 files within here. Then we changed the path of the file from the videos folder and put it into this MyFinances folder and changed the name of the file to make it relate the topic of finances, which achieved the goal of obfuscating the artefact.

The type of Artefact

HIDING: obfuscation of file and/or path name

Artefact Detail Table

Artefact is	Tick Appropriat e
Application Level	x
OS Level	
File System Level	x
Reconnaissance / Research phase	
Recording phase	
Result / Aftermath phase	x

Artefact 10 : family_day_out_plan.bin



Meta-Data of the artefact:

Metadata	
Name:	/img_AAA1EO1.E01/vol_vol2/family_day_out_plan_h.bin
Type:	File System
MIME Type:	image/png
Size:	86364
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-11-09 16:17:22 GMT
Accessed:	2022-11-09 00:00:00 GMT
Created:	2022-11-09 16:15:12 GMT
Changed:	0000-00-00 00:00:00
MD5:	Not calculated
SHA-256:	Not calculated
Hash Lookup Results:	UNKNOWN
Internal ID:	169

Implications of the Artefact:

Changing the file extension and anime to disguise a screenshot points to a methodical approach in masking the true nature of files. This act is indicative of an intent to deceive and hide the actual content, further implicating the suspect in deceptive practices.

Method to hide/unhide artefact:

The method was to change the file extension from png to bin to obscure that it is a screenshot of the victim and suspect, also the name of the file was changed to make it seem like it was not related to images or screenshot and rather related to the suspect's family.

The type of Artefact

HIDING: manipulating file extension

Artefact Detail Table

Artefact is	Tick Appropriat e
Application Level	x
OS Level	
File System Level	x
Reconnaissance / Research phase	
Recording phase	
Result / Aftermath phase	x

Artefact 11 : Radio_messages_h.docx

Radio message 1:

"Welcome back. Folks! We're into the final quarter, and the atmosphere is electric here at Greenfield Stadium. The home team is pushing forward in a bold attempt to overturn the one-goal deficit that they're in. Jones passes the ball to Murphy, who's been an absolute unit down the flank all evening. He's taking on the defense... dodges a tackle and crosses it into the box. It's a header by Thomson, and oh what a save by the keeper!!!! Spectacular athleticism to keep his team in the lead. This game is proving to be a nail biter, with both teams giving it their all. Stay tuned as we witness these final exhilarating moments!!!!"

Radio message 2:

"And were back to what has been a thrilling match so far. The energy on the pitch is palpable as Smith lines up for the free-kick. It's a tense moment; can he curve it past the wall? He shoots... and.... It's in! The crowd goes wild! Smith has really stepped up his game today; he might go up there with the legends of old. The defense didn't stand a chance. It's moments like these that define a season, and this one will be remembered for years to come. The home team has levelled the score line, and the fans are singing their hearts out!"

"Welcome back listeners, we've just witnessed an incredible display of agility from the young star, O'Donnell. He's been a force of nature throughout the match, and there he goes again, intercepting the ball in midfield, dribbling past defenders as if they're mere cones. He's approaching the penalty area, takes a short from distance.... And it's a goal!! A sensational strike from O'Donnell, surely a contender for goal of the season. The visiting fans are ecstatic, their cheers echoing through the stands. This younger is proving to be the signing of the season."

Eliza, every step you take is being watched. You think you can just walk away and start fresh? I'll make sure your reputation is tarnished beyond repair. The photographs are just the beginning. You'll regret crossing me, and I'll be there every time you try pick up the pieces. Your shame will be public, and your peace of mind will be shattered. This is not a threat; it's a promise of retribution.

Meta-Data of the artefact:

Metadata

Name: /img_AAA1EO1.E01/vol_vol2/Radio messages_h.docx
Type: File System
MIME Type: application/vnd.openxmlformats-officedocument.wordprocessingml.document
Size: 14135
File Name Allocation: Allocated
Metadata Allocation: Allocated
Modified: 2022-11-14 14:20:56 GMT
Accessed: 2022-11-14 00:00:00 GMT
Created: 2022-11-14 14:20:32 GMT
Changed: 0000-00-00 00:00:00
MD5: Not calculated
SHA-256: Not calculated
Hash Lookup Results: UNKNOWN
Internal ID: 175

Implications of the Artefact:

Hiding text within a document by changing the font colour to make it invisible at a glance is a subtle yet effective method of concealment. This artefact reveals the suspect's intent to hide incriminating communication while maintaining easy access to the hidden information.

Method to hide/unhide artefact:

The method used was to insert the text that the suspect wanted to hide and then change the font colour so that the text is unnoticeable if opened.

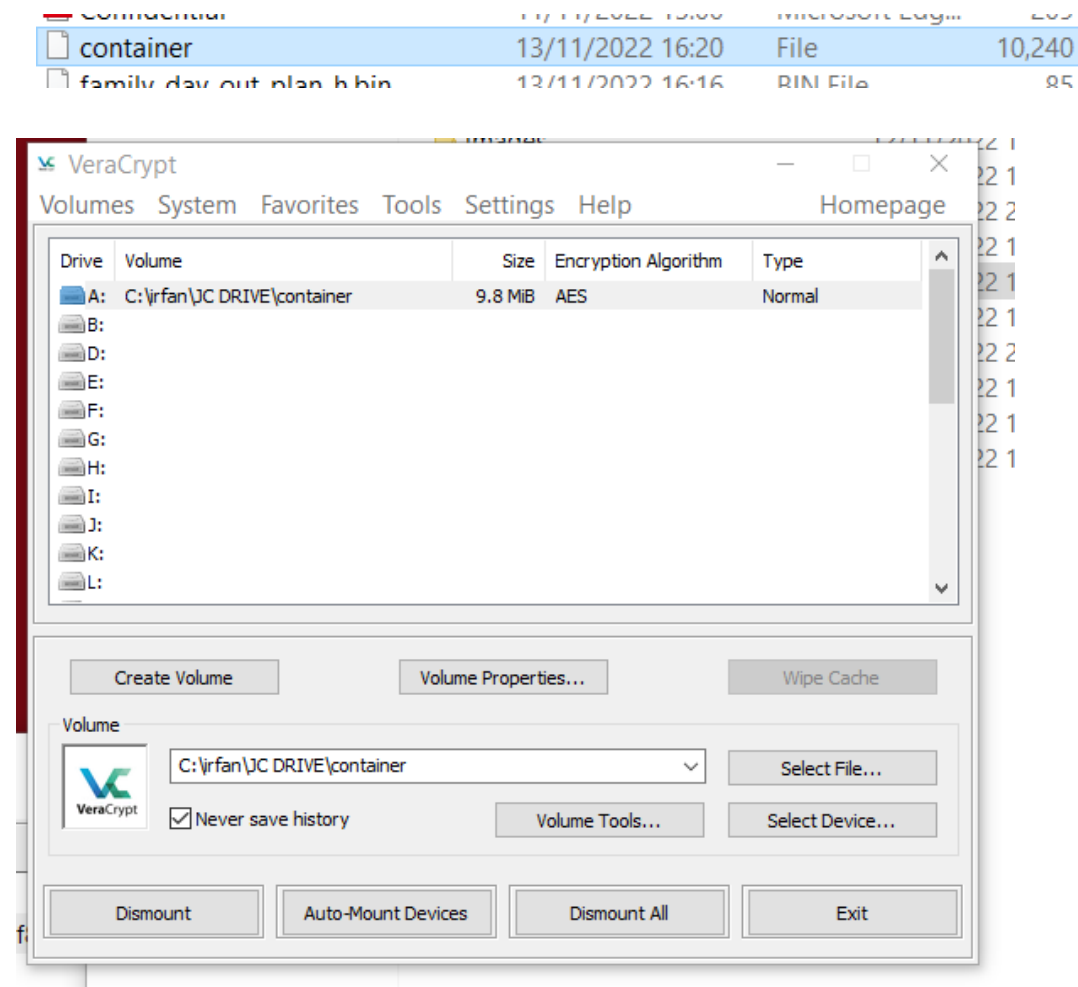
The type of Artefact

HIDING: hidden text or pictures within a document

Artefact Detail Table

Artefact is	Tick Appropriat e
Application Level	x
OS Level	
File System Level	
Reconnaissance / Research phase	
Recording phase	
Result / Aftermath phase	x

Artefact 12: container



Meta-Data of the artefact:

Metadata

Name: /img_AAA1EO1.E01/vol_vol2/container
Type: File System
MIME Type: application/octet-stream
Size: 10485760
File Name Allocation: Allocated
Metadata Allocation: Allocated
Modified: 2022-11-14 13:25:22 GMT
Accessed: 2022-11-14 00:00:00 GMT
Created: 2022-11-14 13:25:12 GMT
Changed: 0000-00-00 00:00:00
MD5: Not calculated
SHA-256: Not calculated
Hash Lookup Results: UNKNOWN
Internal ID: 168

Implications of the Artefact:

The use of an encrypted container, secured with a password, exemplifies a higher level of security consciousness. This artefact signifies the suspect's intent to protect and hide data from unauthorised access, indicating a concern for maintaining secrecy.

Method to hide/unhide artefact:

The task was to have an encrypted container and this was done using VeraCrypt and a password was placed which was then put into a different artefact.

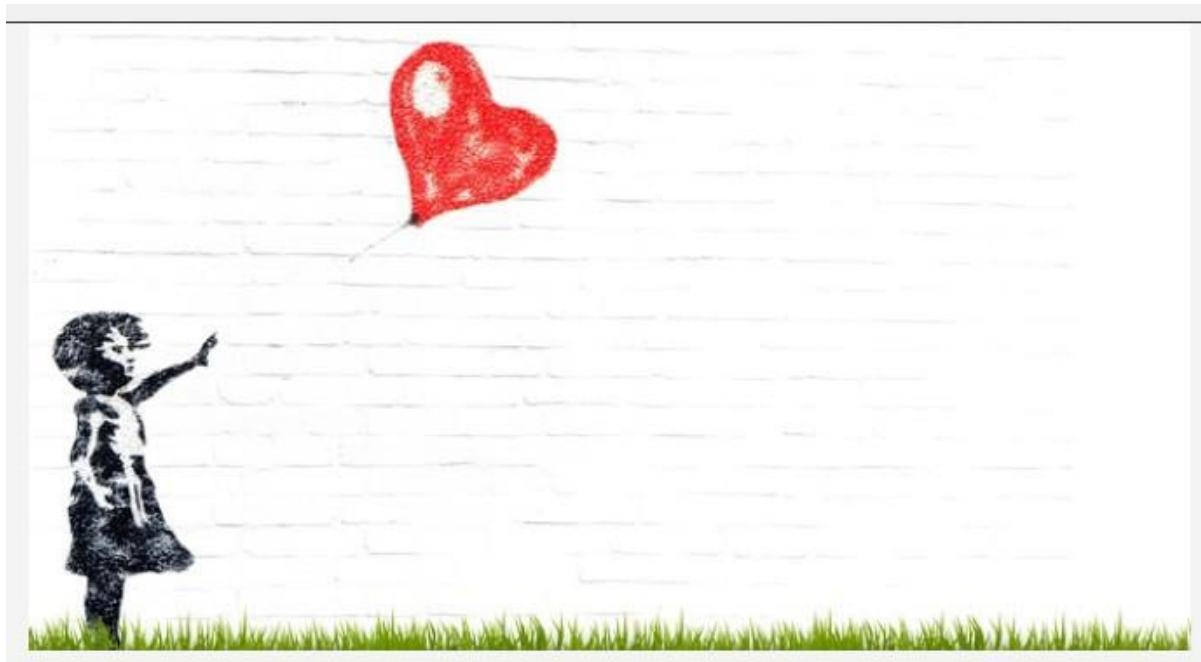
The type of Artefact

HIDING: encrypted password protected container.

Artefact Detail Table

Artefact is	Tick Appropriat e
Application Level	
OS Level	
File System Level	x
Reconnaissance / Research phase	
Recording phase	
Result / Aftermath phase	x

Artefact 13 : pic_8_dirt.png



Meta-Data of the artefact:

Metadata

Name:	/img_AAA1EO1.E01/vol_vol2/images/pic_8_dirt.jpg
Type:	File System
MIME Type:	image/jpeg
Size:	38280
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-11-09 18:00:00 GMT
Accessed:	2022-11-09 00:00:00 GMT
Created:	2022-11-09 18:00:00 GMT
Changed:	0000-00-00 00:00:00
MD5:	d4d11f021087420e53f42b7c201140aa
SHA-256:	f8cdc1d14301f3026e114feae6534b0db654d461e68ebb87c8e84209a0f20771
Hash Lookup Results:	UNKNOWN
Internal ID:	46

Implications of the Artefact:

The hiding of this file indicates an attempt by the user to conceal its presence, which shows the content is sensitive or incriminating. The act of hiding the file was a simple method to reduce its visibility to others who might use the same device, suggesting an intent to keep it

from being easily discovered, this action can be seen as a measure to obscure evidence, protect personal information, or conceal unauthorised activities. The image is rather tame and not of a sexual nature but they relate to artefact #6 which brings up the significance of the artefact and why it was hidden. This artefact was the cover for the illegal content which is why it was hidden.

Method to hide/unhide artefact:

the image was hidden using the file explorer's properties, by setting the file's attribute to 'hidden'. This does not remove the file however it hides the file as if it never existed and can only be seen if the user alters the folder options to show hidden files.

The type of Artefact

HIDING

Artefact Detail Table

Artefact is	Tick Appropriat e
Application Level	
OS Level	
File System Level	x
Reconnaissance / Research phase	
Recording phase	
Result / Aftermath phase	x

Artefact 14 : VeraCrypt User Guide

before:

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text

00000000 85 50 44 46 2D 31 2E 35 0D 0A 25 B5 B5 B5 0D %PDF-1.5...%uuu.

00000010 0A 31 20 30 20 2F 62 6A 0D 0A 3C 3C 2F 54 79 70 .1 0 obj..<</Typ

00000020 65 2F 43 61 74 61 6C 6F 67 2F 50 61 67 65 73 20 e/Catalog/Pages

00000030 32 20 30 20 52 2F 4C 61 6E 67 28 65 6E 2D 55 53 2 0 R/Lang(en-US

00000040 29 20 2F 53 74 72 75 63 74 54 72 65 65 52 6F 6F) /StructTreeRoo

00000050 74 20 39 34 38 20 30 20 52 2F 4D 61 72 6B 49 6E t 948 0 R/MarkIn

00000060 66 6F 3C 3C 2F 4D 61 72 6B 65 64 20 74 72 75 65 fo<</Marked true

00000070 3E 3E 3E 3E 0D 0A 65 6E 64 6F 62 6A 0D 0A 32 20 >>>>..endobj..2

00000080 30 20 6F 62 6A 0D 0A 3C 3C 2F 54 79 70 65 2F 50 0 obj..<</Type/P

00000090 61 67 65 73 2F 43 6F 75 6E 74 20 31 35 31 2F 4B ages/Count 151/K

000000A0 69 64 73 5B 20 33 20 30 20 52 20 31 39 20 30 20 ids[3 0 R 19 0

000000B0 52 20 32 34 20 30 20 52 20 32 35 20 30 20 52 20 R 24 0 R 25 0 R

000000C0 32 36 20 30 20 52 20 32 37 20 30 20 52 20 33 31 26 0 R 27 0 R 31

000000D0 20 30 20 52 20 33 39 20 30 20 52 20 34 30 20 30 0 R 39 0 R 40 0

000000E0 20 52 20 34 31 20 30 20 52 20 34 32 20 30 20 52 R 41 0 R 42 0 R

000000F0 20 34 33 20 30 20 52 20 34 34 20 30 20 52 20 34 43 0 R 44 0 R 4

00000100 35 20 30 20 52 20 34 36 20 30 20 52 20 34 37 20 5 0 R 46 0 R 47

00000110 30 20 52 20 34 38 20 30 20 52 20 34 39 20 30 20 0 R 48 0 R 49 0

00000120 52 20 35 30 20 30 20 52 20 35 31 20 30 20 52 20 R 50 0 R 51 0 R

00000130 35 32 20 30 20 52 20 35 33 20 30 20 52 20 35 34 52 0 R 53 0 R 54

00000140 20 30 20 52 20 35 35 20 30 20 52 20 35 36 20 30 0 R 55 0 R 56 0

00000150 20 52 20 35 38 20 30 20 52 20 36 33 20 30 20 52 R 58 0 R 63 0 R

00000160 20 36 38 20 30 20 52 20 37 31 20 30 20 52 20 37 68 0 R 71 0 R 7

00000170 33 20 30 20 52 20 37 34 20 30 20 52 20 37 36 20 3 0 R 74 0 R 76

00000180 30 20 52 20 37 37 20 30 20 52 20 38 30 20 30 20 0 R 77 0 R 80 0

00000190 52 20 38 33 20 30 20 52 20 38 34 20 30 20 52 20 R 83 0 R 84 0 R

000001A0 38 35 20 30 20 52 20 38 37 20 30 20 52 20 38 39 85 0 R 87 0 R 89

000001B0 20 30 20 52 20 39 30 20 30 20 52 20 39 32 20 30 0 R 90 0 R 92 0

000001C0 20 52 20 39 33 20 30 20 52 20 39 34 20 30 20 52 R 93 0 R 94 0 R

000001D0 20 39 36 20 30 20 52 20 39 37 20 30 20 52 20 39 96 0 R 97 0 R 9

000001E0 38 20 30 20 52 20 39 39 20 30 20 52 20 31 30 31 8 0 R 99 0 R 101

000001F0 38 20 30 20 52 20 39 39 20 30 20 52 20 31 30 31 8 0 R 99 0 R 101

Offset(h): 0 Overwrite

after:

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text

00000000 89 50 4E 47 0D 0A 1A 0A 0D 0A 25 B5 B5 B5 0D %PNG.....%uuu.

00000010 0A 31 20 30 20 6F 62 6A 0D 0A 3C 3C 2F 54 79 70 .1 0 obj..<</Typ

00000020 65 2F 43 61 74 61 6C 6F 67 2F 50 61 67 65 73 20 e/Catalog/Pages

00000030 32 20 30 20 52 2F 4C 61 6E 67 28 65 6E 2D 55 53 2 0 R/Lang(en-US

00000040 29 20 2F 53 74 72 75 63 74 54 72 65 65 52 6F 6F) /StructTreeRoo

00000050 74 20 39 34 38 20 30 20 52 2F 4D 61 72 6B 49 6E t 948 0 R/MarkIn

00000060 66 6F 3C 3C 2F 4D 61 72 6B 65 64 20 74 72 75 65 fo<</Marked true

00000070 3E 3E 3E 3E 0D 0A 65 6E 64 6F 62 6A 0D 0A 32 20 >>>>..endobj..2

00000080 30 20 6F 62 6A 0D 0A 3C 3C 2F 54 79 70 65 2F 50 0 obj..<</Type/P

00000090 61 67 65 73 2F 43 6F 75 6E 74 20 31 35 31 2F 4B ages/Count 151/K

000000A0 69 64 73 5B 20 33 20 30 20 52 20 31 39 20 30 20 ids[3 0 R 19 0

000000B0 52 20 32 34 20 30 20 52 20 32 35 20 30 20 52 20 R 24 0 R 25 0 R

000000C0 32 36 20 30 20 52 20 32 37 20 30 20 52 20 33 31 26 0 R 27 0 R 31

000000D0 20 30 20 52 20 33 39 20 30 20 52 20 34 30 20 30 0 R 39 0 R 40 0

000000E0 20 52 20 34 31 20 30 20 52 20 34 32 20 30 20 52 R 41 0 R 42 0 R

000000F0 20 34 33 20 30 20 52 20 34 34 20 30 20 52 20 34 43 0 R 44 0 R 4

00000100 35 20 30 20 52 20 34 36 20 30 20 52 20 34 37 20 5 0 R 46 0 R 47

00000110 30 20 52 20 34 38 20 30 20 52 20 34 39 20 30 20 0 R 48 0 R 49 0

00000120 52 20 35 30 20 30 20 52 20 35 31 20 30 20 52 20 R 50 0 R 51 0 R

00000130 35 32 20 30 20 52 20 35 33 20 30 20 52 20 35 34 52 0 R 53 0 R 54

00000140 20 30 20 52 20 35 35 20 30 20 52 20 35 36 20 30 0 R 55 0 R 56 0

00000150 20 52 20 35 38 20 30 20 52 20 36 33 20 30 20 52 R 58 0 R 63 0 R

00000160 20 36 38 20 30 20 52 20 37 31 20 30 20 52 20 37 68 0 R 71 0 R 7

00000170 33 20 30 20 52 20 37 34 20 30 20 52 20 37 36 20 3 0 R 74 0 R 76

00000180 30 20 52 20 37 37 20 30 20 52 20 38 30 20 30 20 0 R 77 0 R 80 0

00000190 52 20 38 33 20 30 20 52 20 38 34 20 30 20 52 20 R 83 0 R 84 0 R

000001A0 38 35 20 30 20 52 20 38 37 20 30 20 52 20 38 39 85 0 R 87 0 R 89

000001B0 20 30 20 52 20 39 30 20 30 20 52 20 39 32 20 30 0 R 90 0 R 92 0

000001C0 20 52 20 39 33 20 30 20 52 20 39 34 20 30 20 52 R 93 0 R 94 0 R

000001D0 20 39 36 20 30 20 52 20 39 37 20 30 20 52 20 39 96 0 R 97 0 R 9

000001E0 38 20 30 20 52 20 39 39 20 30 20 52 20 31 30 31 8 0 R 99 0 R 101

000001F0 38 20 30 20 52 20 39 39 20 30 20 52 20 31 30 31 8 0 R 99 0 R 101

Offset(h): 0 Overwrite

Meta-Data of the artefact:

Metadata

Name: /img_AAA1EO1.E01/vol_vol2/VeraCrypt User Guide.pdf
Type: File System
MIME Type: image/png
Size: 3068169
File Name Allocation: Allocated
Metadata Allocation: Allocated
Modified: 2022-11-14 13:13:56 GMT
Accessed: 2022-11-14 00:00:00 GMT
Created: 2022-11-14 13:10:32 GMT
Changed: 0000-00-00 00:00:00
MD5: Not calculated
SHA-256: Not calculated
Hash Lookup Results: UNKNOWN
Internal ID: 25

Implications of the Artefact:

This shows the determination of the suspect as they went to great lengths to hide this piece of evidence as changing the magic numbers is not a simple feat and requires specialised softwares to carry this out. The existence of this artefact shows the premeditation and thought process of the suspect as this evidence is a user guide for a software to encrypt files inside a container.

Method to hide/unhide artefact:

The method used to hide this piece of evidence was to use a hex editing tool called HxD, hex editing software, to change the bytes so that it ceases to be a pdf file and instead changes to the header of a file the suspect intends, which in this case was a png file.

The type of Artefact

HIDING

Artefact Detail Table

Artefact is	Tick Appropriat e
Application Level	x
OS Level	
File System Level	x

Reconnaissance / Research phase	
Recording phase	
Result / Aftermath phase	x

Artefact 15 : can you feel the rain.mp4

Gotta remember

I've got those photos and videos that she thought were private. Perfect leverage. If she won't talk to me,

maybe she'll talk when she sees them online. It's not like she gave me consent to post them, but I'm sure the

distress will make her reach out.

Remember:

the hidden messages: <https://manytools.org/hacker-tools/steganography-encode-text-into-image/>

for the next volume of vids: <https://www.kapwing.com/>

Veracrypt for container password

remember HxD for header unchange

Meta-Data of the artefact:

Metadata

Name:	/img_AAA1EO1.E01/vol_vol2/can you feel the rain.mp4.docx
Type:	File System
MIME Type:	application/vnd.openxmlformats-officedocument.wordprocessingml.document
Size:	10269
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-11-14 15:03:14 GMT
Accessed:	2022-11-14 00:00:00 GMT
Created:	2022-11-14 15:02:50 GMT
Changed:	0000-00-00 00:00:00
MD5:	Not calculated
SHA-256:	Not calculated
Hash Lookup Results:	UNKNOWN
Internal ID:	164

Implications of the Artefact:

The existence of this artefact shows the willingness and determination of the suspect to their goal of committing the crime as the content shows softwares and tools used to carry out their crimes which, and suggests the action of committing a repeat of the crimes. The use of changing the extension ensures that anyone, upon first view of the file within the file explorer, reads the file name and sees that it is a mp4 file and deems it not worthy of looking at, thus the suspect achieves their goal of obfuscating their evidence.

Method to hide/unhide artefact:

The method to hide this evidence was changing the extension of the file from txt to mp4, this makes it so that the file upon first view is actually a mp4 file and not a text file when clicked on.

The type of Artefact

HIDING

Artefact Detail Table

Artefact is	Tick Appropri ate
Application Level	x
OS Level	
File System Level	x
Reconnaissance / Research phase	
Recording phase	
Result / Aftermath phase	x

