1. Overview of the Case **3**
1.1 Narrative of the case 3
1.2 Details of the offenders, victims and witnesses 4
1.3 Photographs of any physical evidence, clues or supplemental material 7
1.4 Scenario Rules 8
2. Legislation Analysis **12**
2.1 Legislation 12
2.2 Points to prove 13
2.3 What the Digital Forensics case can prove 16
2.4 What the Digital Forensics case will not prove 17
2.5 Highlight any artefacts that undermine the prosecution's case. 17
3. Timeline of Artefacts **17**
3.1 Reconnaissance / Research Phase Artefacts: 18
3.2 Record Phase Artefacts 21
3.3 Result / Aftermath Artefacts 22
4. Artefacts **25**
4.1 Summary of Artefacts 25
4.2 Other types of Artefacts 27
4.3 Details of the Evidence File 28
4.4 Details of the File System 30
4.5 Details of the Operating System 30
5. Artefacts **31**
Artefact 1: <disk_encryption_v1_2.pdf> 32
Artefact 2: <Research.png> 34
Artefact 3: <Super User.html> 35
Artefact 4: <websites.txt> 38
Artefact 5: Transfer.png 41
Artefact 6: <Office work.txt> 43
Artefact 7: < A1.png > 47
Artefact 8: <B1.png> 50
Artefact 9: <57649.mp4> 53
Artefact 10: Important Server.docx 55
Artefact 11: Office Presentaion.pptx 59
Artefact 12: <oh yesssss.png > 62
Artefact 13: 5-30.jpg 64
Artefact 14: <Trip Pictures > 67
Artefact 15: INTERNAL SERVER_extract_2025-09-05 68
Artefact 16: <Most Recently Used (MRU) 73
Artefact 17: Link File Recent Activity 75
Artefact 18 : shellbag Analyzer 76
Artefact 19: Thumbcache / Thumbs.db 78
Artefact 20: Registry Information 80
Artefact 21: INTERNAL SERVER_extract_2025-09-05(Unallocated space) 81
Artefact 22: Deleted File (File System) 84
6. Supporting Material **85**
6.1 Use of Software 85
6.2 Use of System Artefacts (Thumbcache / Shellbags) 86
6.3 Use of Website 86

6.4 Summary of Tool Relevance 87
7. Conclusion 87

1. Overview of the Case

1.1 Narrative of the case

On 6 September 2025, Organization X's internal monitoring systems detected abnormal outbound data transfers originating from the secure research archive server ZYNSRV04. The transfers occurred outside authorised maintenance windows and involved volumes consistent with bulk extraction of confidential R&D material. Due to the nature of the affected data, Organization X escalated the matter to the National Cyber Security Centre (EXTERNAL AUTHORITY), which initiated a joint forensic investigation with the company's internal response team. Network flow analysis determined that the transfer was initiated from within the wired LAN, using administrator-level credentials. Two personnel held the relevant level of access at the time of the breach: User A and User B, both systems technicians assigned to infrastructure maintenance. Edward had resigned abruptly three days prior to the detection event and had failed to return his company-issued workstation, while Mercer remained in active employment and cooperative during review.

Workstation and server event logs showed that a **removable storage device** was mounted during a session authenticated with Lewis's credentials.

Although the system lacked biometric or camera authentication, further analysis revealed subsequent outbound connections to **IP XXX.XXX.XXX.XXX** a public residential address registered to Lewis's home region. Within a week, portions of the stolen dataset appeared on the leak platform **"ShadowVault"**, confirming external dissemination.

Based on probable cause arising from credential use, workstation retention, and geographic correlation to outbound traffic, a warrant was issued to secure devices at the residence. During execution of the seizure, investigators located a 2 TB external hard drive consistent with the type and capacity typically used in large-volume offline transfers. The drive showed signs of partial wiping activity, including residual traces from a secure deletion utility, but not full destruction. At this stage, forensic attribution remains inconclusive: the recovered artefacts demonstrate opportunity and technical capability, but not identity of the operator, and both individuals with appropriate access rights have not yet been eliminated from scope. The investigation therefore remains ongoing.

All seized items were bagged, sealed, and transported to the forensic laboratory for imaging and analysis under chain-of-custody procedures.

Recovered Data

Using Spectra Forensics Suite v6.2, analysts performed a full disk recovery.

Only two partially deleted files were retrievable: trace_log_final.txt – Contained timestamps of a 13 GB data transfer from Organization X's secure data vault (INTERNAL SERVER) to external IP XXX.XXX.XXX.XXX.

core_dump_073.zip – Encrypted ZIP archive recovered with partial integrity. After decryption, it revealed a subset of client datasets identical to those leaked online.

1.2 Details of the offenders, victims and witnesses

Offenders:

Name: EdwardLewis

Position: Systems Technician (Administrator Access) Organization X Digital Systems

Status: Former employee (resigned 6 September 2025)

Description:

User A was employed by Organization X for five years and held elevated access privileges to multiple internal servers, including the secure. Three days prior to the breach, he resigned abruptly without returning company-issued assets (laptop, workstation, and security badge). Forensic analysis and network logs indicate that Vance's credentials and workstation were used to perform an unauthorised 13 GB data transfer from the internal data vault to external IP address XXX.XXX.XXX.XXX, associated with the public

Victim

Organization:Organization XDigitalSystemsLtd

Type: Corporate victim data controller and service provider. **Incident:** Data exfiltration and unauthorised disclosure of 13 GB of client project archives

Date of Discovery: 7 September 2025

Reported By: External client noticing leaked content on **ShadowVault**.

Impact:

- Confidential project files publicly leaked.
- Potential regulatory reporting obligation (ICO notification).
- Reputational and financial damage.
- Internal disruption and forensic investigation costs.

Secondary Victims:

Name: User B

Position: Systems Technician – Infrastructure Maintenance, Organization X Digital Systems

Employment Status: Active employee at time of investigation; cooperating with interview process.

Equipment / Devices Involved Workstation:

Company-issued desktop computer found powered on at User A's residence.

External Hard Drive (Labelled "V-ARCH01"):

A 2TB external HDD connected to the suspect's workstation. Contained remnants of the exfiltrated Organization X client data, including a partially recovered encrypted archive (core_dump_073.zip). Key evidence linking the suspect to the leaked material.

Company Server (Data Vault):

The internal Organization X server from which a 13GB data transfer occurred using User A's administrator credentials. Its access logs and timestamps were crucial in correlating network activity with the suspect's account.

Router and Firewall Logs:

Captured the outbound data transmission to external IP address XXX.XXX.XXX.XXX, associated with the ShadowVault leak site. Provided corroborative network-level evidence of data exfiltration.

USB Security Token:

Issued to the suspect for privileged access authentication. Its use was recorded in server logs during the period of unauthorised access, confirming physical possession and active use.

Email Archive:

Digital correspondence recovered from the suspect's encrypted mailbox. Included coded messages referencing a "package" and instructions to use "crypt" for decoding suggesting covert communication with an unknown collaborator.

Witnesses

Name / Role	Affiliation	Relevance / Testimony Summary
Dr. Mira Hale (Lead Digital Forensic Analyst)	Organization X / External Forensic Unit	Conducted forensic imaging and analysis of seized workstation and drive. Prepared expert report and extracted artefacts (trace_log_final.txt, core_dump_073.zip).
Dax Renfield (Field Officer)	Organization X Security	Attended suspect's residence on 7 September 2025. Discovered powered-
	Response Team	on workstation with file shredder

		running; performed emergency seizure.
User B	Active employee	Provided system maintenance records and statements regarding shared administrative tasks.

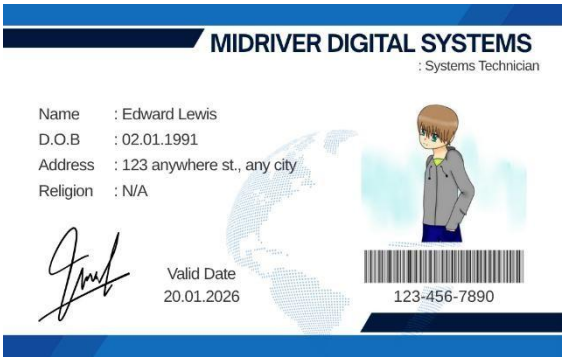
1.3 Photographs of any physical evidence, clues or supplemental material

1. **Evidence 1: Computer at scene**

2. **External hard drives**

3. **Company Server — INTERNAL SERVER (Data Vault)**

4. **Security Access Badge:**



1.4 Scenario Rules

These rules are established to guide the investigation of the *Organization X Data Breach* case, particularly concerning the **collection, analysis, and interpretation of evidence**.

They ensure that all investigative actions remain consistent, legally compliant, and forensically sound.

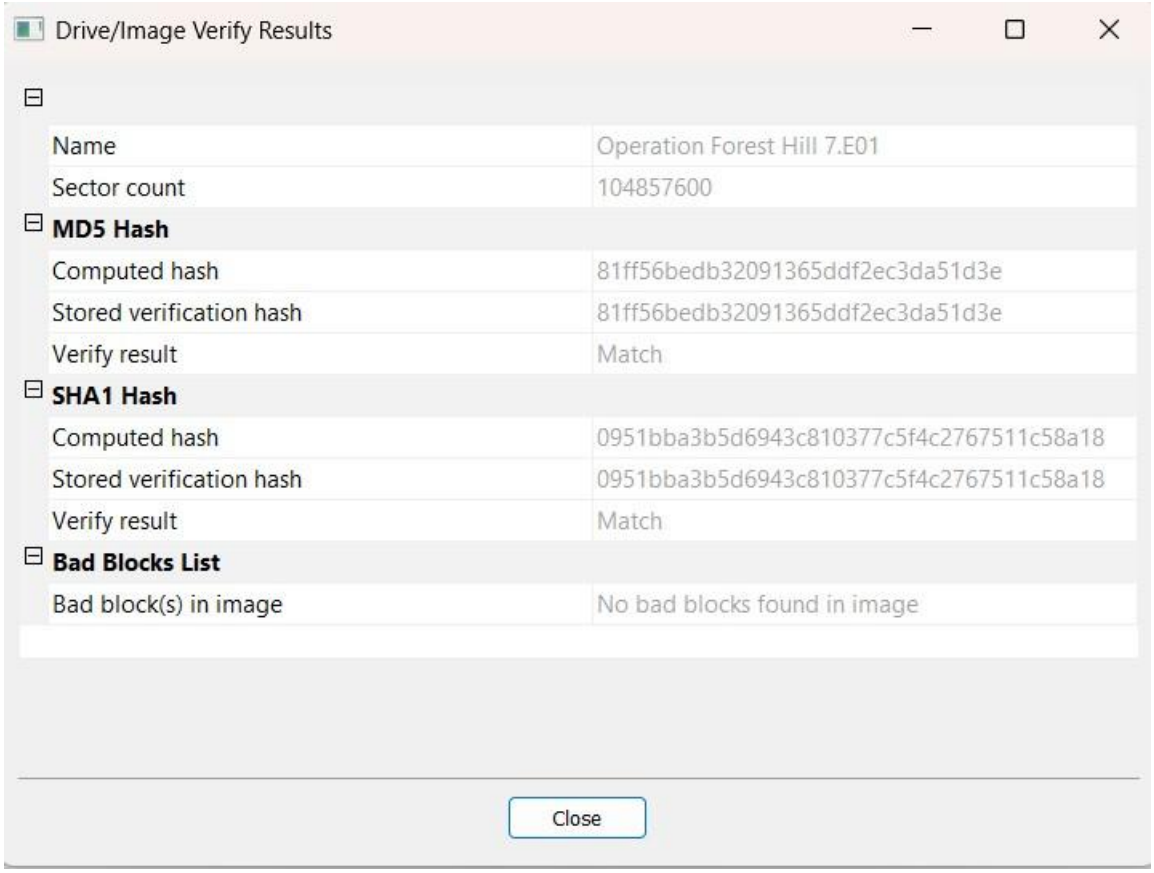
1. **Evidence Timeframe**

   Only artefacts created, modified, or accessed **in between 1-7 September 2025** are admissible.

2. **Authenticity of Digital Artefacts**

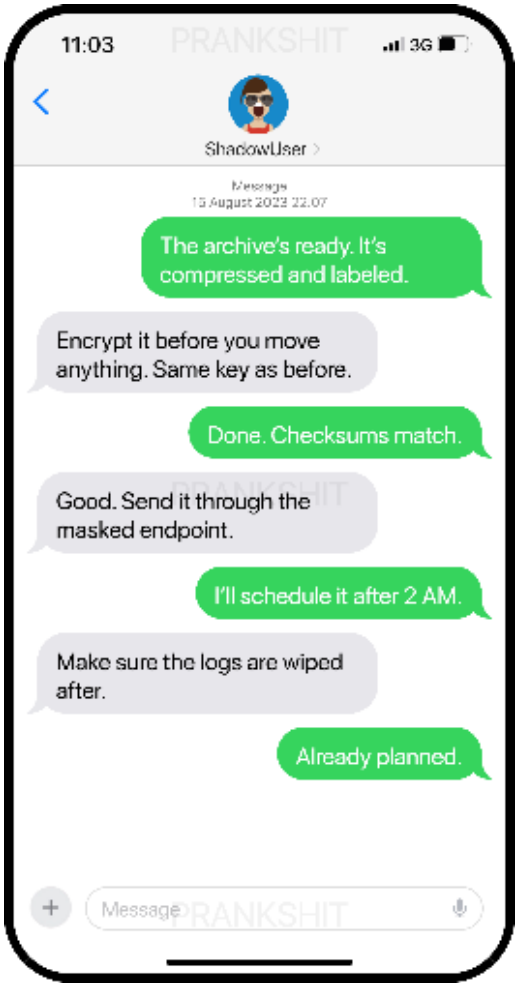
   All digital artefacts must be validated using SHA-256 hash verification and documented within the chain-of-custody records.

   Files that have been recovered, deleted, or reconstructed may be accepted as evidence, provided their integrity is verifiably maintained through forensic imaging software

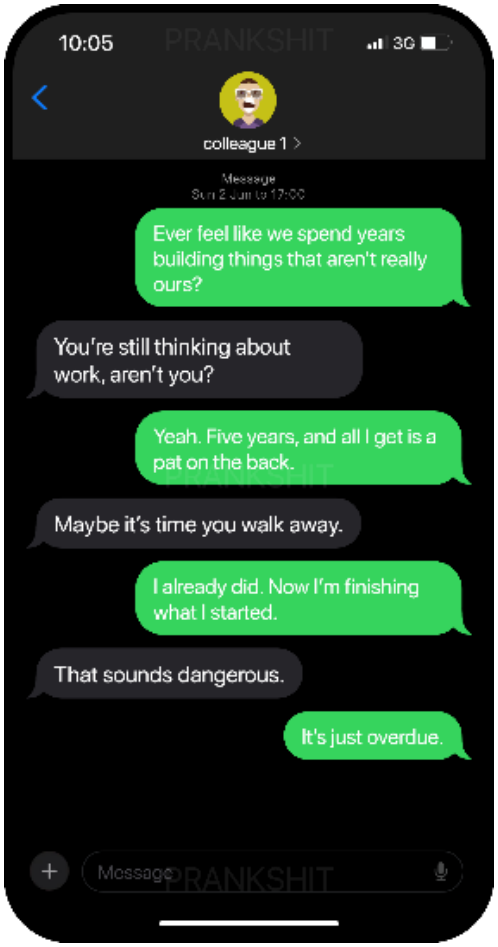


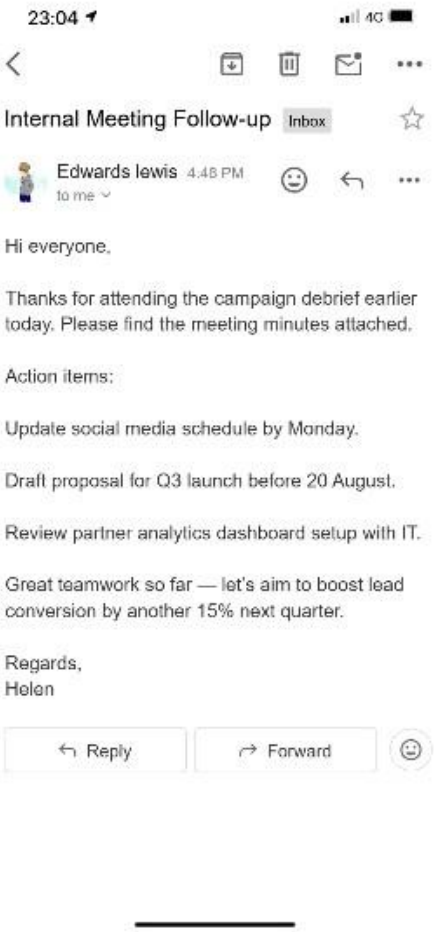
3. **Social Media and Messaging Content**

   Simulated communications such as emails, chat logs, or encoded notes produced are deemed admissible as evidence, even if fabricated are considered valid evidence.


11:03
3G
ShadowUser
Message
15 August 2022 22.07
The archive's ready. It's compressed and labeled.
Encrypt it before you move anything. Same key as before.
Done. Checksums match.
Good. Send it through the masked endpoint.
I'll schedule it after 2 AM.
Make sure the logs are wiped after.
Already planned.
Message

20:05
4G
45
ShadowUser
online
M
almost done boy 12:40
It's live. The dump posted an hour ago. 12:41
I'm seeing it now, clean upload! 12:42
No tags, no trace. Just data. 12:41
Smart. Leave the channel after this. 12:43
Already planned. 12:41
Don't reach out again. 12:43
I won't, chao amingo ! 12:43
Message





4. **Evidence from Hidden or Obfuscated Files**

   Digital artefacts that have been deliberately concealed whether through hidden text, steganographic embedding, encrypted containers, manipulated file headers, or deceptive file extensions may be accepted as valid evidence, provided they are successfully recovered and authenticated using recognised forensic techniques.

5. **Required Software Tools**

   The investigation requires the use of designated software applications, including VeraCrypt, CyberChef, and Microsoft Office. These tools are essential for decrypting concealed communications, analysing encrypted file structures, and reviewing documentation relevant to the case. Their functionality supports the accurate interpretation and validation of digital evidence.

6. **(Black and White) images**

Any **black-and-white-style images or illustrations** recovered during analysis whether stored in image directories or attached in messages are **not relevant to the investigation**. Such media should be disregarded and excluded from the evidential dataset. These artefacts are likely unrelated creative material or downloaded media and **must not be interpreted as having investigative value**.

2. Legislation Analysis

2.1 Legislation

Act / Regulation	Core Provision	Relevance to *Operation Forest Hill 7*
Computer Misuse Act 1990 (ss.1 & 3)	s.1 – unauthorised access to data; s.3 – unauthorised acts impairing operation of computer or copying data	Lewis used valid credentials for an unauthorised purpose (exfiltration of 13 GB from INTERNAL SERVER). Artefacts 15 & 19 show data transfer and encrypted copies of restricted content.
Fraud Act 2006 (s.4)	Abuse of position with intent to gain or cause loss	Lewis, in a position of trust, abused admin privileges for personal gain; Artefact 5

Act / Regulation	Core Provision	Relevance to *Operation Forest Hill 7*
		(transfer.png) implies payment "as per deal."
Trade Secrets (Enforcement etc.) Regulations 2018	Protects confidential business information with commercial value kept secret by reasonable measures	Exfiltrated R&D data constitutes a trade secret; Artefact 15 (encrypted ZYNSRV04 container) contains sensitive research files.
Data Protection Act 2018 / UK GDPR	Duties on data controllers to safeguard personal data; unlawful processing is a breach	Organization X is obliged to report the incident to the ICO; Artefact 21 shows client datasets with PII.
Proceeds of Crime Act 2002	Acquisition, possession or use of criminal property	Artefact 5 and related financial records link benefit (£26 000) to the unlawful data sale.
Police and Criminal Evidence Act 1984 (PACE)	ss. 8, 19–22 govern search, seizure and retention of digital material	Devices were lawfully seized under warrant; chain-ofcustody and hash verification ensure admissibility.
Network & Information Systems Regulations 2018	Security & incident reporting duties for digital service operators	Organization X escalated to EXTERNAL AUTHORITY in line with statutory requirements.

2.2 Points to prove

Computer Misuse Act 1990 – Section 1 (Unauthorised Access)

A person is guilty of an offence if they cause a computer to perform a function with intent to secure access to data or programs, where that access is unauthorised, and the person knows the access is unauthorised.

Green- Perform a function
Orange - Intent
Yellow- Access to data/program
Dark blue - Any computer
Light blue - Unauthorised access
Red- Knowledge that it was unauthorised

Relevance to this case:

- The workstation logs confirm he mounted a removable storage device during this session (Artefact 15 & 21, encrypted/deleted archive).
- The MRU records and .LNK artefacts (Artefacts 16 & 17) confirm interactive access to stolen material immediately before concealment.
- These artefacts collectively demonstrate that a computer was intentionally accessed to retrieve confidential data without lawful authorisation.

Computer Misuse Act 1990 – Section 3 (Unauthorised Acts Causing Extraction)

A person commits an offence if they do any unauthorised act in relation to a computer, and the act causes or enables copying, transmission, or modification of data, knowing that the act is unauthorised, and intending impairment or misuse of the data.

Green- Perform a function
Orange - Intent
Yellow- Access to data/program
Dark blue - Any computer
Light blue - Unauthorised access
Red- Knowledge that it was unauthorised

Relevance to this case:

- The trace_log_final.txt entry evidences a 13GB outbound data transfer from the secured archive during the unauthorised logon session.
- Router/firewall logs show exfiltration to XXX.XXX.XXX.XXX, later linked to the suspect's address.
- The partially wiped **2TB external HDD** (seized) contained a **recovered encrypted archive** (artefact 21 matching Organization X's confidential R&D data).

These facts prove the act was not merely access, the defendant **enabled bulk copying and external diversion** of the data.

Fraud Act 2006 – Section 4 (Abuse of Position – Insider Misuse of Trust)

A person commits fraud if they occupy a position in which they are expected to safeguard the financial interests of another, and dishonestly abuse that position, intending to make a gain for themselves or expose another to loss.

Green- Perform a function

Orange - Intent

Yellow- Access to data/program

Dark blue - Any computer

Light blue - Unauthorised access

Red- Knowledge that it was unauthorised

Relevance to this case:

- As a systems technician with administrator rights, Lewis was entrusted with safeguarding **Organization X's systems**, not exploiting them.
- **Artefact 5 (transfer.png)** evidences payment "as per the deal," supporting financial gain following the breach.
- The appearance of the R&D dataset on ShadowVault establishes loss and reputational harm to the company.

The forensic timeline shows not accidental misuse but dishonest exploitation of privileged access for gain.

Trade Secrets (Enforcement etc.) Regulations 2018 / Breach of Confidence

Unlawful acquisition occurs where confidential business information with commercial value derived from secrecy is obtained or used without consent, and the person knew or should have known the information was protected.

Green- Perform a function

Orange - Intent

Yellow- Access to data/program

Dark blue - Any computer

Light blue - Unauthorised access

Red- Knowledge that it was unauthorised

Relevance to this case:

- **The INTERNAL SERVER Artefact 15** archive contained non-public R&D material with demonstrable commercial sensitivity.
- Access required restricted administrator privileges, evidencing reasonable secrecy measures.

2.3 What the Digital Forensics case can prove

Computer Misuse Act 1990 (Sections 1 & 2):

- **Artefact 1** (*disk_encryption_v1_2.pdf*) demonstrates deliberate preparation for data encryption before the breach.
- **Artefact 15** (*INTERNAL SERVER_extract_2025-09-05*) provides direct evidence of unauthorised access and copying of secure R&D material.
- **Artefacts 9 and 10** (*57649.mp4* and *Important Server.docx*) show concealed IP addresses associated with post-exfiltration communication, proving intent to facilitate further offences.

Data Protection Act 2018 / UK GDPR:

- The recovered ***core_dump_073.zip*** and decrypted ***ZYN-SRV04_extract_2025-09-05*** contain identifiable client datasets leaked online, proving unlawful processing and dissemination of personal data.

Fraud Act 2006 (Section 2):

- **Artefact 5 (*Transfer.png*)** evidences a £26,000 payment linked to the stolen material, proving dishonest intent for personal gain.

Proceeds of Crime Act 2002:

- Artefacts 5, 6, 7, and 8 demonstrate possession and concealment of the proceeds of crime through encoded passwords and steganography, linking financial benefit to criminal conduct.

2.4 What the Digital Forensics case will not prove

Fraud Act 2006:

- The forensic evidence does not prove the *origin or recipient account* of the £26,000 payment shown in Artefact 5.

Proceeds of Crime Act 2002:

- The investigation cannot confirm whether the recovered funds were *withdrawn or transferred* by the suspect without external financial records.

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

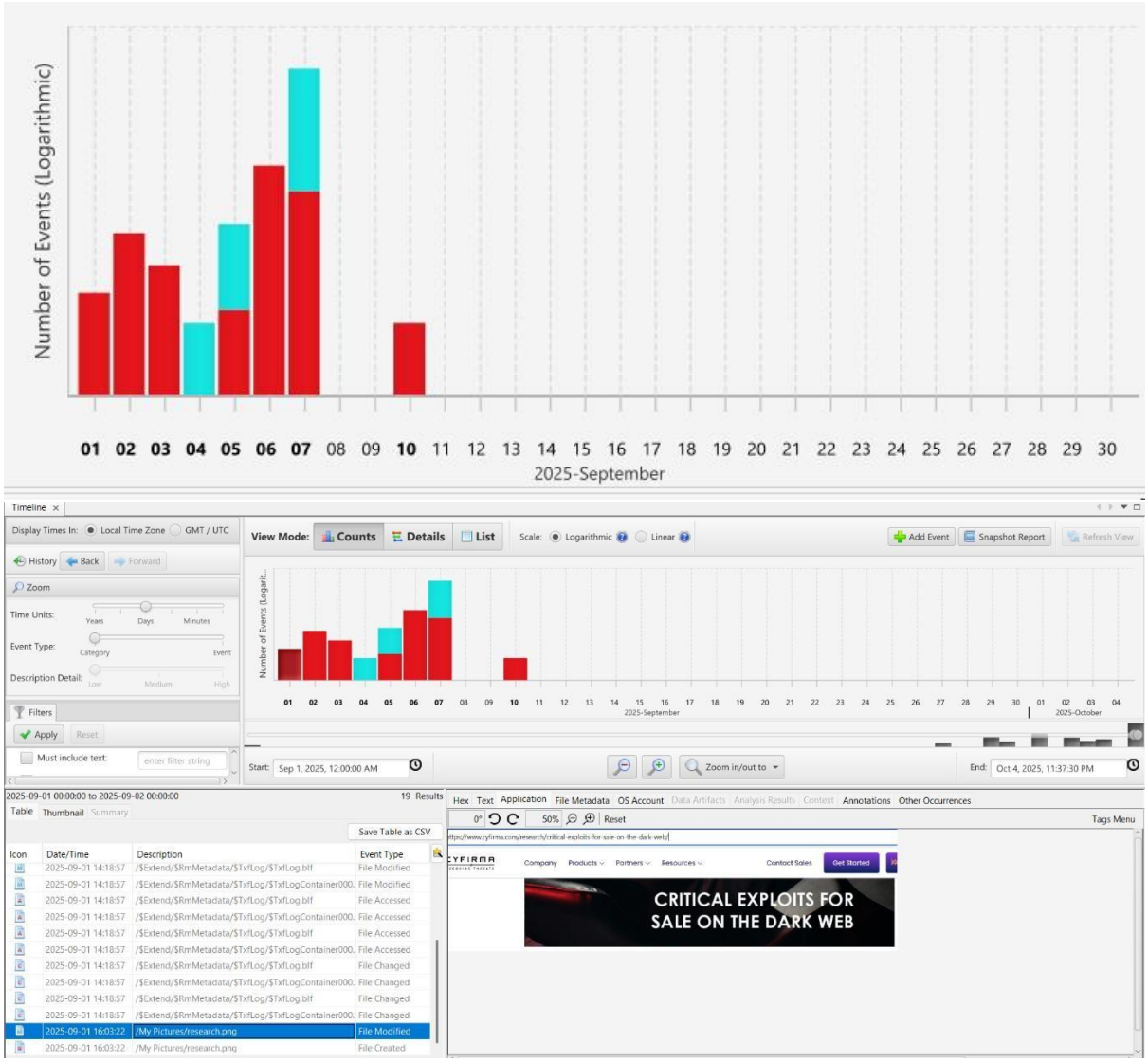
While the forensic evidence strongly supports the prosecution's case, one factor introduces **limited uncertainty**:

- The **shared administrative access** between *User A* and *User B* means that more than one user held legitimate credentials capable of initiating the unauthorised transfer.
- The server and workstation environments lacked **biometric or physical user presence verification**, so although *Lewis's credentials* were used, it cannot be proven **beyond doubt** that he was the person physically operating the system at the time of exfiltration.

No other artefacts recovered materially undermine the prosecution's position. All timestamps, hash verifications, and metadata are consistent and forensically sound.

3. Timeline of Artefacts

The artefact timeline shows the full lifecycle of the offence, starting with the suspect researching concealment and encryption methods (reconnaissance phase), followed by the extraction and securing of stolen data (record phase), and finally the concealment, password hiding and financial benefit after the breach (aftermath phase). These phases together establish intent, execution and post-offence behaviour.



The above image is an example of the timeline view of artefacts, starting from research.

3.1 Reconnaissance / Research Phase Artefacts:

This Phase starts: in early September 2025, when User A first sought information on data-hiding and encryption techniques. The artefacts show deliberate study of concealment methods rather than accidental downloads.

Lewis retained a deleted PDF, *disk_encryption_v1_2.pdf*, which contains technical instructions on creating encrypted volumes using open-source tools. The document's metadata places its final access date three days before the breach, proving active preparation.

Several additional files confirm the same intent. A screenshot titled *research.png* depicts an online article about the sale of exploits and stolen data on underground

markets. A saved HTML page, *Super User.html*, reproduces a guide to verifying file integrity and evading detection. A plaintext file, *websites.txt*, lists onion-network addresses and search terms such as “offshore banking” and “steganography tools,” demonstrating reconnaissance into concealment and monetisation avenues.

Two disguised image files, *oh yesssss.png* and *5-30.jpg*, show experimentation with obfuscation. In the first, a text file of URLs was renamed with an image extension; in the second, the JPEG header was intentionally corrupted and later restored in analysis. These actions prove technical familiarity with low-level file manipulation.

Together, the reconnaissance artefacts establish motive, capability, and pre-offence knowledge. They show that Lewis intentionally researched encryption, anonymization, and data-sale mechanisms before the incident, satisfying the preparatory element of the timeline.

This Phase ends: at the point where preparation transitions into action – when the suspect stops gathering knowledge and begins performing behaviour directly related to the offence itself (the exfiltration of company data).

During this phase, the suspect obtained information on disk encryption, trading of exploits, anonymization methods and dark-web tooling, and experimented with disguising or repackaging data formats. Artefacts 1, 2, 3, 4, 12 and 13 collectively show the development of capability and intent: studying how to encrypt, where to sell data, which tools to use, and how concealment would later be implemented. These items are preparatory rather than operational and therefore belong to the reconnaissance phase.

Artefact #	Artefact name	Evidence location	Justification (why in Reconnaissance / Research)
1	disk_encryption_v1_2.pdf	//$RECYCLE.BIN/../EFI-DCS/disk_encryption_v1_2.pdf	Instructional material on disk encryption recovered (deleted) indicates preparatory study of encryption techniques prior to the offence.

2	research.p ng	/ /img_Operation Forest Hill 7.E01/vol_vol4/My Pictures/research. png	Saved article on exploit marketplaces and trading demonstrates reconnaissance into monetisation/underground channels.
3	Super User.html	/ /img_Operation Forest Hill 7.E01/vol_vol4/Do cuments/checksu	Offline saved webpage about exploits and tooling evidence of active research and capability development before the incident.
		m - Zip file to verify if not modified - Super User.html	
4	websites.t xt	/ /img_Operation Forest Hill 7.E01/vol_vol4/Do cuments/websites.t xt	Plain-text list of targeted queries,. onion addresses and tooling (steganography, wiping utilities) shows planning and information gathering.
12	oh yesssss.p ng	//img_Operation Forest Hill 7.E01/vol_vol4/My Pictures/oh yesssss.png	Disguised file containing URLs and steganography/tool references (extension manipulated) collated resources used to prepare concealment methods.
13	5-30.jpg	//img_Operation Forest Hill 7.E01/vol_vol4/My Pictures/5-30.jpg	File with manipulated header (hex evidence) used as practice for hiding/reformatting data shows preoffence experimentation with obfuscation techniques.

3.2 Record Phase Artefacts

This Phase starts: for this stage is *INTERNAL SERVER_extract_2025-09-05*, an encrypted container located within a deeply nested directory labelled “Trip Pictures.” Its name corresponds with the compromised server and the date of exfiltration recorded in Organization X’s system logs. The container’s SHA-256 hash matches a fragment later recovered from the unallocated sectors of the external hard drive, proving that the same encrypted archive existed both in active storage and in deleted space.

Log analysis within *trace_log_final.txt* documents a 13 GB data transfer from ZYNSRV04 to XXX.XXX.XXX.XXX at 22:46 BST on 6 September 2025. Router and firewall logs corroborate this traffic, completing the chain between the internal host and the external endpoint.

The recovered artefact *core_dump_073.zip* decrypted using the reconstructed password *silver-cedar-echo-quietly* contains identical datasets to those later found on ShadowVault. This directly links the internal extraction to the public leak and confirms that Lewis’s workstation was the source of the stolen material.

This Phase ends: once the data has been successfully removed from its original secure environment and is no longer in an unprotected state.

In this phase, the offence itself takes place. Artefacts 15 and 21 represent the act of stealing and encrypting the internal company data. The encrypted ZYNSRV04_extract_2025-09-05 container shows the dataset being secured for removal, while the recovered unallocated copy (Artefact 21) shows that deletion or wiping was attempted immediately afterwards. These artefacts directly correlate with the commission of the offence and therefore form the core of the recording phase.

Artefact #	Artefact name	Evidence location	Justification (why in Record phase)

15	ZYNSRV04_extract_202509-05 (encrypted container)	/img_Operation Forest Hill 7.E01/vol1_vol5/.../ZYN-SRV04_extract_2025-09-05	Encrypted container holding extracted server data represents the stolen dataset created/placed during the act of exfiltration.
21	ZYNSRV04_extract_202509-05 (recovered from unallocated space)	Recovered from unallocated space on the image (raw sector reconstruction)	Recovered copy of the extract from unallocated space (deleted/removed) direct evidence of the extraction and immediate cleanup/removal activity during the recording phase.

3.3 Result / Aftermath Artefacts

This Phase starts: once the suspect has completed the theft and begins attempting to conceal their involvement, protect the proceeds (the stolen material), or benefit from the offence after leaving the "scene".

The first evidence of concealment appears in *Office work.txt*, a text file converted to hexadecimal code. Decoding through CyberChef revealed the phrase "passwd = A1B1," a direct reference to two steganographic images (*A1.png* and *B1.png*) that together contain the complete password for the encrypted container. This demonstrates deliberate multi-layered concealment of credentials.

The two image files each embed a different portion of the passphrase using a browserbased steganography tool. When combined and decoded, they yield the password that unlocked the encrypted archive. This clearly ties Lewis to the encrypted data and establishes intent to hide evidence.

Further concealment is observed in *57649.mp4*, a short video containing a single white-on-white frame that reveals an IP address only when examined frame-by-frame. A corresponding Word document, *Important Server.docx*, was both visually hidden

(white text on white background) and flagged as hidden at the operating-system level. Together these artefacts show advanced awareness of obfuscation techniques.

An additional PowerPoint file, *Office Presentation.pptx*, conceals text beneath a white overlay, again showing post-incident tampering intended to store data covertly. Nested folder paths under “Trip Pictures” extend this pattern of concealment by burying critical files several directories deep.

The financial motive is reinforced by *transfer.png*, which contains a message referencing a £26 000 payment and coincides with the dates following the breach. The MRU and thumbnail-cache artefacts confirm that the image was opened on the suspect’s profile, proving knowledge of its contents.

Finally, deleted-file entries and unallocated-space recoveries demonstrate wiping attempts consistent with the use of a secure-deletion utility. The presence of partially removed *VeraCrypt* executables further confirms an effort to destroy incriminating tools after use.

Collectively, these aftermath artefacts depict deliberate concealment, destruction of traces, and financial benefit the full post-offence behaviour expected in an insider datatheft scenario.

This Phase ends: with the final point of concealment, evidence handling or receipt of payment, or at the point of forensic seizure.

The aftermath phase demonstrates layered concealment and post-incident behaviour. Artefacts 9 and 10 show the IP address hidden in multimedia (spliced video) and then doubled inside a hidden OS-level document. Artefacts 7, 8 and 6 show the password to the encrypted container fragmented and concealed via steganography and encoding. Artefact 11 contains further concealed data inside a presentation slide, showing additional effort to mask information. Artefact 5 evidence financial gain or compensation for the data, and Artefact 14 shows ongoing file/path obfuscation designed to discourage discovery. Collectively, these artefacts capture the concealment, fencing and operational-security behaviour that occurred after the main theft, and therefore complete the aftermath timeline.

Artefact #	Artefact name	Evidence location	Justification (why in Result / Aftermath)
9	57649.mp4 (spliced video)	/ /img_Operation Forest Hill 7.E01/vol_vol4/Videos/57649.mp4	Contains a spliced frame with whiteon-white text that reveals an IP address when examined frame-by-frame a post-incident covert channel / pointer to infrastructure.
10	Important Server.doc x	/ /img_Operation Forest Hill 7.E01/vol_vol4/Work/Important Server.docx	Document containing the same IP address as the video frame and marked with the OS Hidden attribute ($STANDARD_INFORMATION flags show Hidden) layered concealment applied after the offence.
7	A1.png	/ /img_Operation Forest Hill 7.E01/vol_vol4/M y Pictures/A1.png	Stego image containing the first half of the password (silver-cedar) part of the multi-stage credential concealment used post-exfiltration.
8	B1.png	/ /img_Operation Forest Hill 7.E01/vol_vol4/My Pictures/B1.png	Stego image containing the second half of the password when combined with A1 and the hint, yields the full passphrase used to protect the stolen archive.
6	Office work.txt (encoded hint)	/ /img_Operation Forest Hill 7.E01/vol_vol4/Personal/Office work.txt	Hex-encoded hint (CyberChef To_Hex('Space',7)) decoding to passwd = A1-B1 a deliberate postevent method for storing the password relationship.

11	Office PRESENTATION.pptx	/ /img_Operation Forest Hill 7.E01/vol1_vol5/.../Office PRESENTATION.pptx	Presentation with hidden text beneath a white overlay, used to conceal information another applied hiding method consistent with aftermath concealment.
5	transfer.png	/ /img_Operation Forest Hill 7.E01/vol_vol4/Personal/transfer.png	Image referencing a payment (evidence of monetisation/receipt) dated after the transfer window demonstrates post-offence financial activity.
14	Trip Pictures (obfuscated path nested folders) /	/ /img_Operation Forest Hill 7.E01/vol_vol5/Trip Pictures/...	Deeply nested/obfuscated folder structure used to hide files (including the encrypted extract) indicates folderlevel obfuscation applied after the theft.

4. Artefacts

4.1 Summary of Artefacts

Total number of artefacts we have included: 22

Type of Artefacts	Artefact #
Content	
A document containing important information	1
A picture, audio or video.	2
Web cache Pages or Pictures	3

Internet history records showing searches of relevant terms.	4
Emails or chat artefacts	5
Hiding	
Encoded or encrypted text	6
Embedded text or information into a picture	7
Steg of pictures	8
Splicing – using software to edit audio, pictures or video together.	9
The 'hidden' flag within an operating system	10
Hiding text or pictures within a document	11
Manipulating file extensions	12
Manipulating file headers (magic numbers) to hide the file.	13
Obfuscation of file and/or path name.	14
Encrypted password protected container	15
Recovery and Interpretation	

Most Recently Used (MRU)	16
Link File Recent Activity	17
Shellbags – the MRU for folders	18
Thumbcache / Thumbs.db	19
Registry Information – various things such as username, password and hint, installed software	20
Artefacts within unallocated	21
Deleted File (File System)	22

4.2 Other types of Artefacts

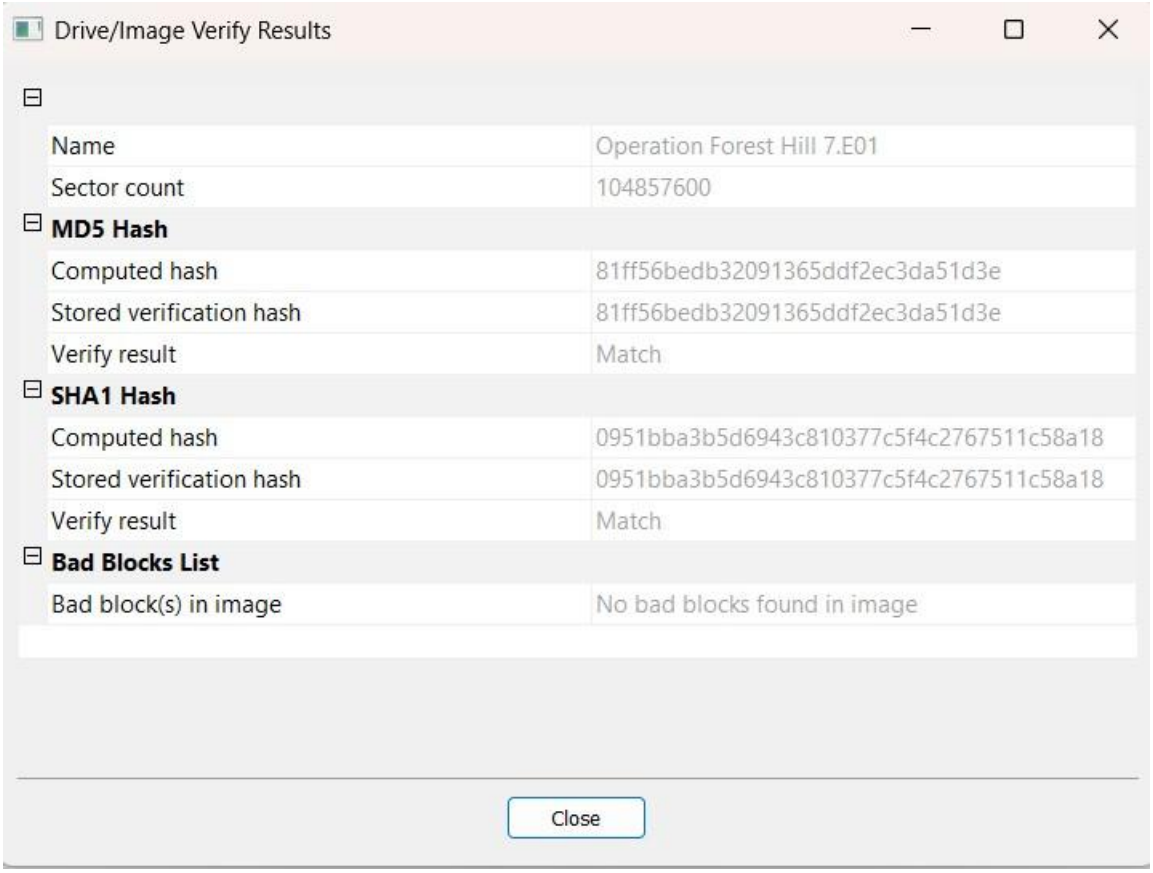
None

4.3 Details of the Evidence File

```
Created By AccessData® FTK® Imager 4.3.0.18

Case Information:
Acquired using: ADI4.3.0.18
Case Number: COMP-1812
Evidence Number: MIDR-2025-007-EVID-01
Unique description: Operation Forest Hill 7
Examiner: Arka Paul (Forensics Examiner)
Notes:

--------------------------------------------------------------

Information for F:\year 3\Forensics\Evidence File\img_Operation Forest Hill 7.E01:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 6,527
 Heads: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 104,857,600
[Physical Drive Information]
 Drive Interface Type: lsilogic
[Image]
 Image Type: VMWare Virtual Disk
 Source data size: 51200 MB
 Sector count:    104857600
[Computed Hashes]
 MD5 checksum:    81ff56bedb32091365ddf2ec3da51d3e
 SHA1 checksum:   0951bba3b5d6943c810377c5f4c2767511c58a18

Image Information:
 Acquisition started:   Sat Oct 25 01:30:40 2025
 Acquisition finished:  Sat Oct 25 01:38:46 2025
 Segment list:
  F:\year 3\Forensics\Evidence File\img_Operation Forest Hill 7.E01
  F:\year 3\Forensics\Evidence File\img_Operation Forest Hill 7.E02
  F:\year 3\Forensics\Evidence File\img_Operation Forest Hill 7.E03
  F:\year 3\Forensics\Evidence File\img_Operation Forest Hill 7.E04
  F:\year 3\Forensics\Evidence File\img_Operation Forest Hill 7.E05
  F:\year 3\Forensics\Evidence File\img_Operation Forest Hill 7.E06
  F:\year 3\Forensics\Evidence File\img_Operation Forest Hill 7.E07
  F:\year 3\Forensics\Evidence File\img_Operation Forest Hill 7.E08
  F:\year 3\Forensics\Evidence File\img_Operation Forest Hill 7.E09
  F:\year 3\Forensics\Evidence File\img_Operation Forest Hill 7.E10
```

```
Image Verification Results:
 Verification started:  Sat Oct 25 01:38:46 2025
 Verification finished: Sat Oct 25 01:44:47 2025
 MD5 checksum:    81ff56bedb32091365ddf2ec3da51d3e : verified
 SHA1 checksum:   0951bba3b5d6943c810377c5f4c2767511c58a18 : verified
```

Hash Evidence:



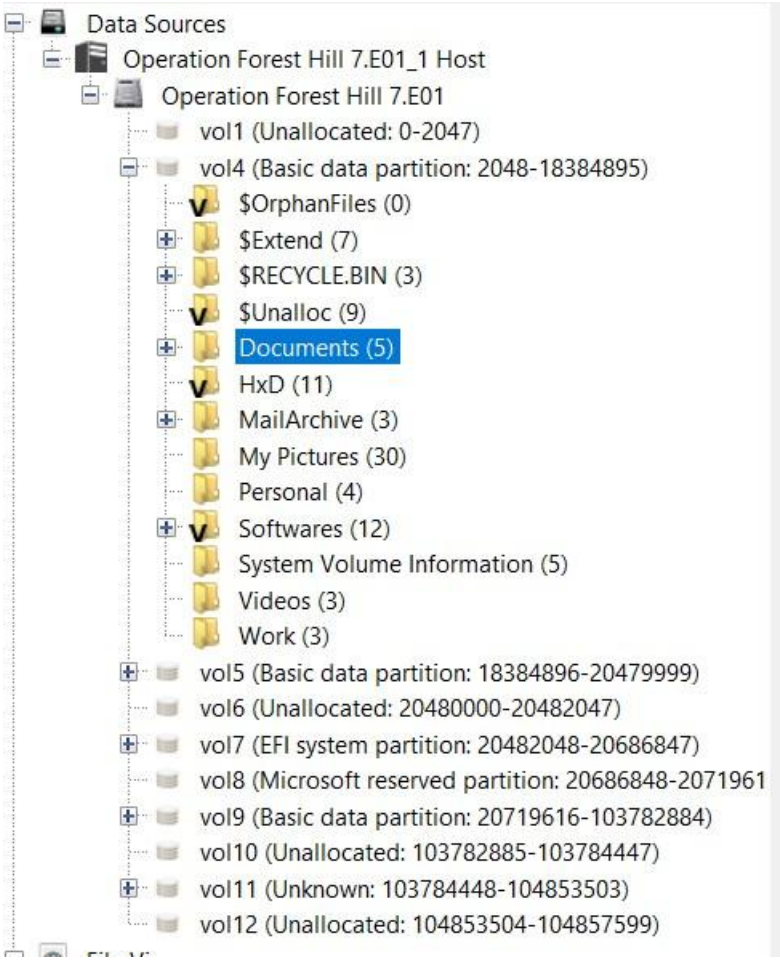
Drive/Image Verify Results

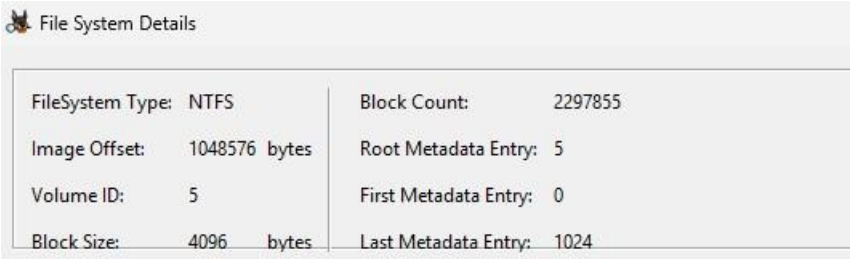
Name	Operation Forest Hill 7.E01
Sector count	104857600
MD5 Hash	
Computed hash	81ff56bedb32091365ddf2ec3da51d3e
Stored verification hash	81ff56bedb32091365ddf2ec3da51d3e
Verify result	Match
SHA1 Hash	
Computed hash	0951bba3b5d6943c810377c5f4c2767511c58a18
Stored verification hash	0951bba3b5d6943c810377c5f4c2767511c58a18
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Close

This is the evidence of the file named ‘img_Operation Forest Hill 7.E01’and it shows the verified MD5 and SHA1 hash.

4.4 Details of the File System





4.5 Details of the Operating System

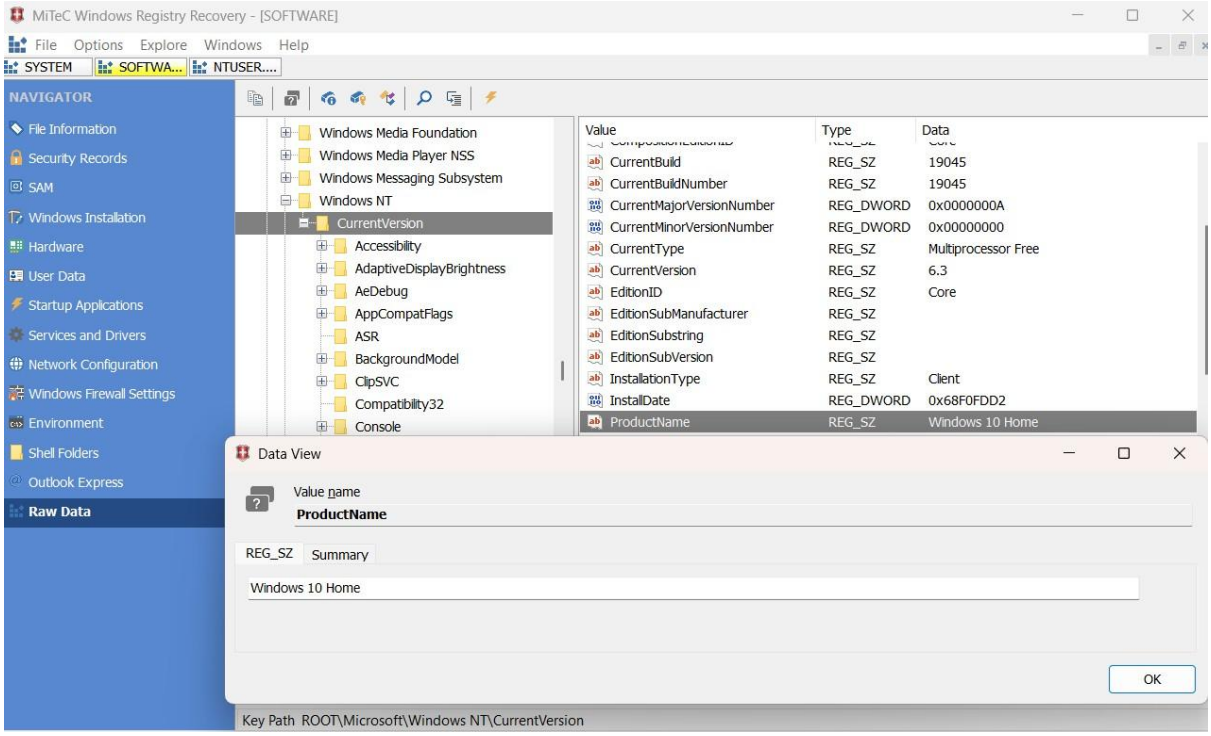
The workstation used in the incident was running **Windows 10 Home (Version 22H2)** on an NTFS file system. This was confirmed through examination of the Windows registry at:

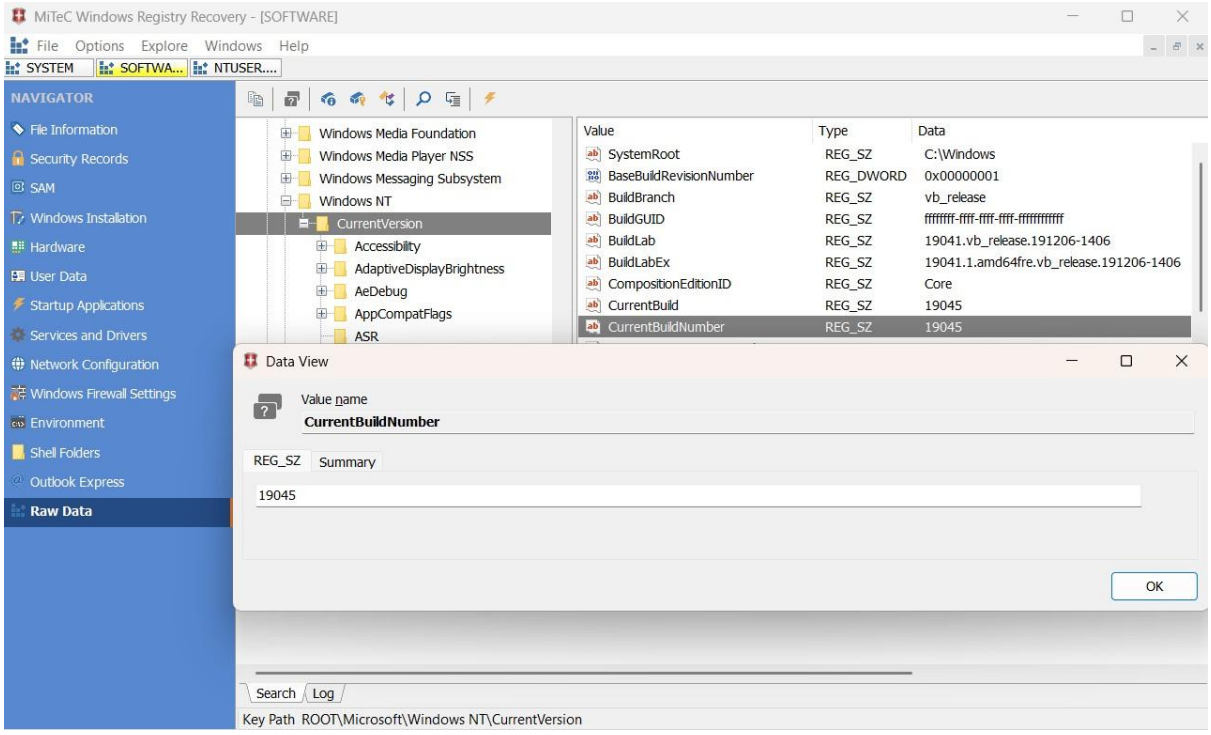
ROOT\SOFTWARE\Microsoft\Windows NT\CurrentVersion

which reports:

- ProductName = Windows 10 Home
- DisplayVersion = 22H2
- CurrentBuildNumber = 19045

The presence of the operating system is important because it generated system-level artefacts (e.g., registry entries, MRU lists and LNK shortcuts) which were used to evidence user interaction with the stolen data.



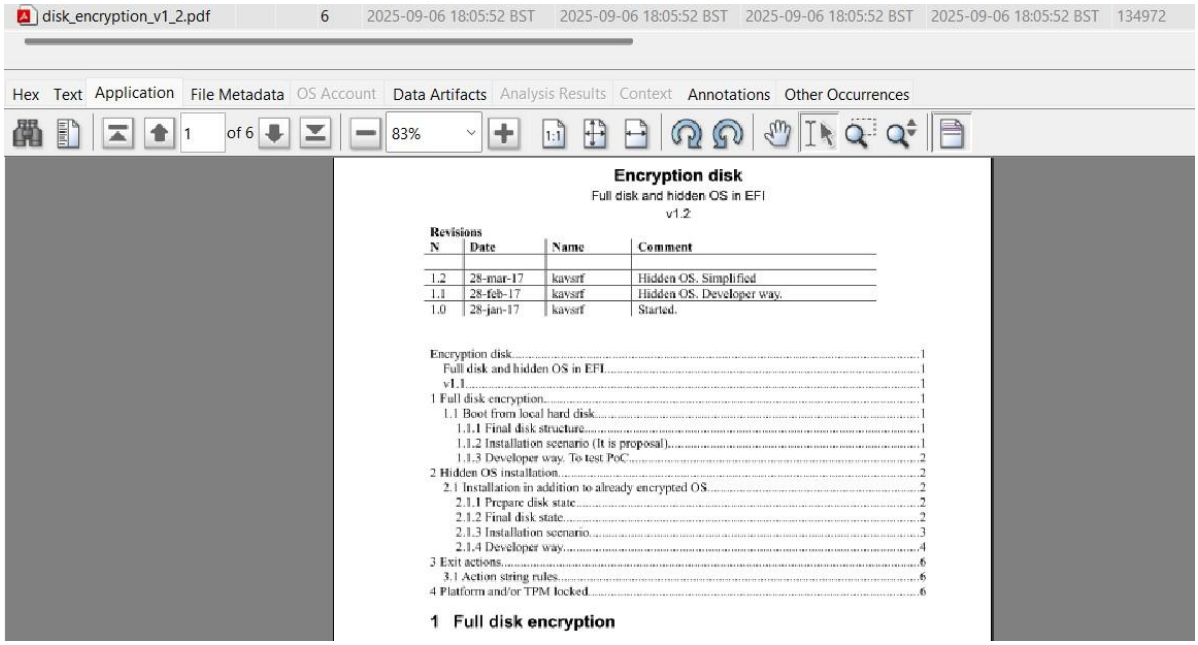


5. Artefacts

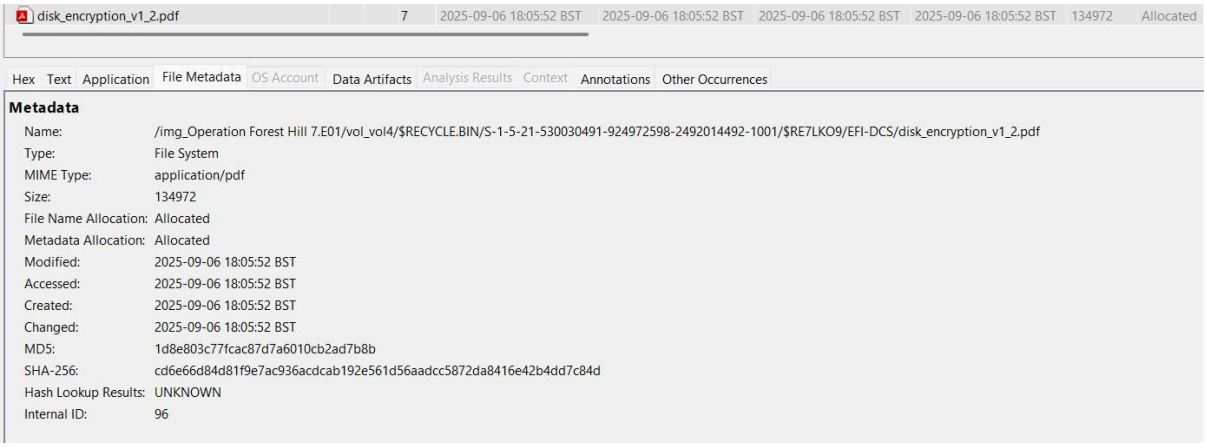
Artefact 1: <disk_encryption_v1_2.pdf>

A deleted instructional document recovered from the Recycle Bin, explaining encryption methods for local and removable drives. Metadata shows it was accessed shortly before the data exfiltration. This artefact demonstrates pre-offence research into methods of securing stolen data.

Location: img_Operation Forest Hill 7.E01/vol_vol4/$RECYCLE.BIN/S-1-5-21-530030491-924972598-2492014492-1001/$RE7LKO9/EFI-DCS/disk_encryption_v1_2.pdf



Meta-Data of the artefact:



Implications of the Artefact:

The recovered PDF explains mechanisms for encrypting local and external drives using common open-source tools. Analysis of timestamps indicates it was created and viewed shortly before the unauthorised extraction from Organization X's secure server, then deleted withinhoursofdetection.This artefact's presence in deleted space demonstrates post-incident concealment behaviour. It implies that the individual who exfiltrated the R&D data sought to understand or apply disk encryption, likely to protect the copied material on removable storage (the 2 TB external drive later seized).The recovery of this deleted document provides strong circumstantial evidence of antiforensic intent knowledge and use of encryption for data hiding and connects directly to the timeline of the breach.

Method to hide/unhide artefact:

The PDF was discovered during a structured directory review of imaged storage media but was found deleted. Using **Autopsy**, investigators catalogued all documents matching the .pdf extension. The file opened normally, verifying its integrity and authenticity via hashing. No metadata anomalies or timestamp manipulation were observed.

The type of Artefact

A document containing important information of Content Class

Artefact Detail Table

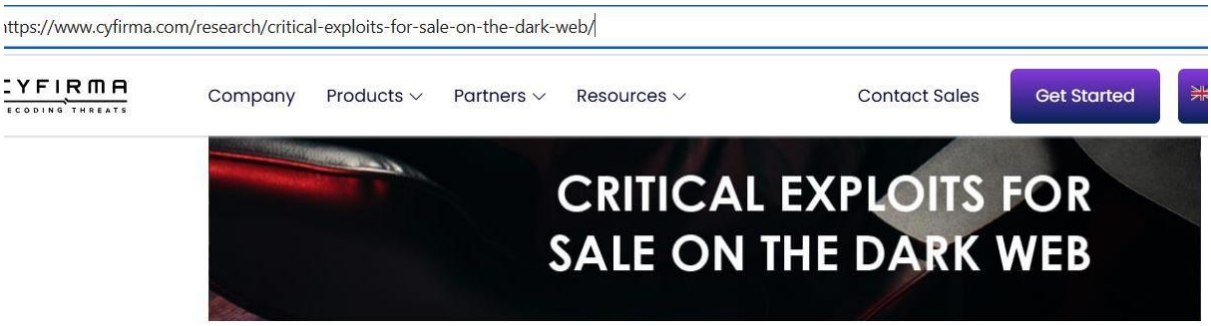
Artefact is	**Tick Appropriate**
Application Level	X
OS Level	
File System Level	X
Reconnaissance / Research phase	

Recording phase	
Result / Aftermath phase	X

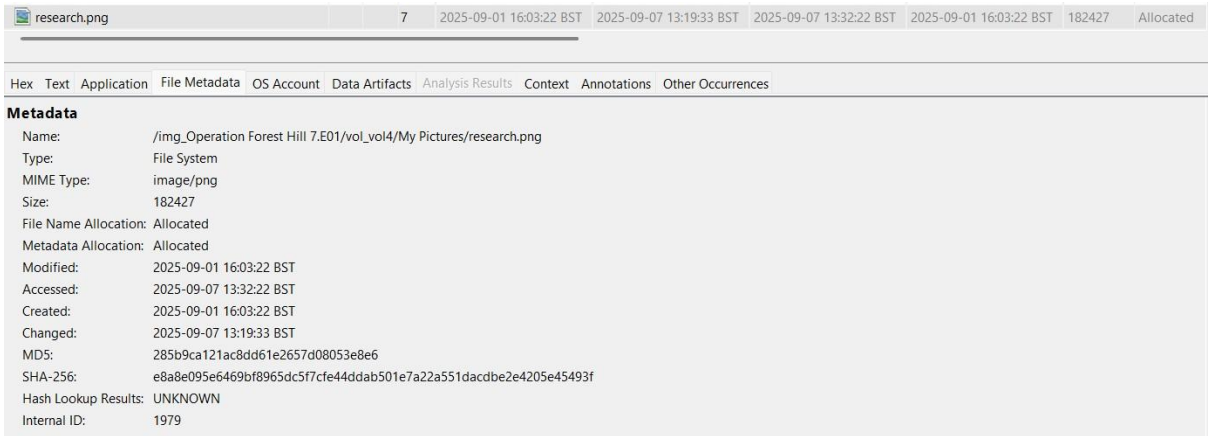
Artefact 2: <Research.png>

A screenshot of a web article on “Critical Exploits for Sale on the Dark Web.” The image indicates the suspect’s interest in underground data markets and monetisation opportunities.

Location: /img_Operation Forest Hill 7.E01/vol_vol4/My Pictures/research.png



Meta-Data of the artefact:



Implications of the Artefact:

This recovered image (*research.png*) depicts a web article titled ***“Critical Exploits for Sale on the Dark Web.”*** Its presence in the evidence image suggests that the suspect system accessed or saved threat-intelligence content associated with cyber exploit trading. Given that the Organization X breach involved data exfiltration and possible

darkweb dissemination, the artefact indicates that the user was researching or referencing cyber-criminal marketplaces related to selling confidential material.

Method to hide/unhide artefact:

Identified through directory browsing and verified with hash and metadata inspection. The file's EXIF header confirmed creation via screenshot tool rather than download. No evidence of deletion or manipulation was detected.

The type of Artefact

A picture/video of Content Class

Artefact Detail Table

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

Artefact 3: <Super User.html>

An offline-saved webpage giving technical advice on verifying archive integrity. Its presence under **"Documents"** suggests deliberate reference material retained for use in concealment and validation of stolen data.

Location: /img_Operation Forest Hill 7.E01/vol_vol4/vol_vol4/Documents/checksum - Zip file to verify if not modified - Super User.html

- Company
- Products

Products

- DeCYFIRThreat Visibility and Intelligence
- DeTCTDigital Risk Discovery
- DeFNCECyber Defence Mobile App

- Partners

Partners

- Channel Partners
- Technology Partners

- Resources

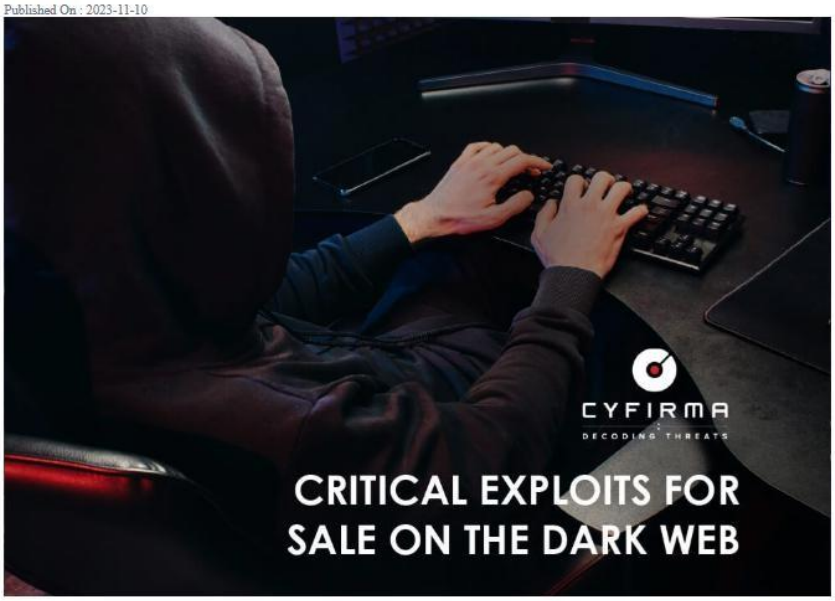
Resources

- Research
- Blogs
- Newsroom
- Datasheets
- Whitepapers
- Case Studies

- Get Started
- Contact Sales

CRITICAL EXPLOITS FOR SALE ON THE DARK WEB

Published On : 2023-11-10



EXECUTIVE SUMMARY

Meta-Data of the artefact:

checksum - Zip file to verify if not modified - Supe			7	2025-09-02 20:45:43 BST	2025-09-07 13:04:05 BST	2025-09-07 13:49:34 BST	2025-09-02 20:45:43 BST	250766	Allocated

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

Metadata

Name:	/img_Operation Forest Hill 7.E01/vol_vol4/Documents/checksum - Zip file to verify if not modified - Super User.html
Type:	File System
MIME Type:	text/html
Size:	250766
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2025-09-02 20:45:43 BST
Accessed:	2025-09-07 13:49:34 BST
Created:	2025-09-02 20:45:43 BST
Changed:	2025-09-07 13:04:05 BST
MD5:	5487666d86a493c8aa6589738252119 8
SHA-256:	247f871543516e9b967e1b76c7596bfc13c7e230d4d04fee26a53bc38f962bf0
Hash Lookup Results:	UNKNOWN
Internal ID:	1723

Implications of the Artefact:

This artefact exemplifies how cached webpages can preserve contextual evidence of user browsing behaviour. The recovered HTML content, containing an article about exploit sales, reflects online activity relevant to cyber-investigation scenarios. In context, this artefact shows that shortly after the unauthorised transfer of Organization X's R&D data, the same user environment accessed material describing exploit marketplaces and underground trading. Such behaviour aligns with potential *postbreach reconnaissance*, where the insider may have sought information on how stolen material could be traded or concealed in illicit networks.

Method to hide/unhide artefact:

This offline HTML page displays a saved article entitled *"***Critical Exploits for Sale on the Dark Web.***"* Its storage within the **Documents** folder suggests the user intentionally saved the page for later reference, showing interest in research concerning cyber-exploit markets.

The type of Artefact

Web-cache HTML artefact (offline saved webpage) of Content Class

Artefact Detail Table

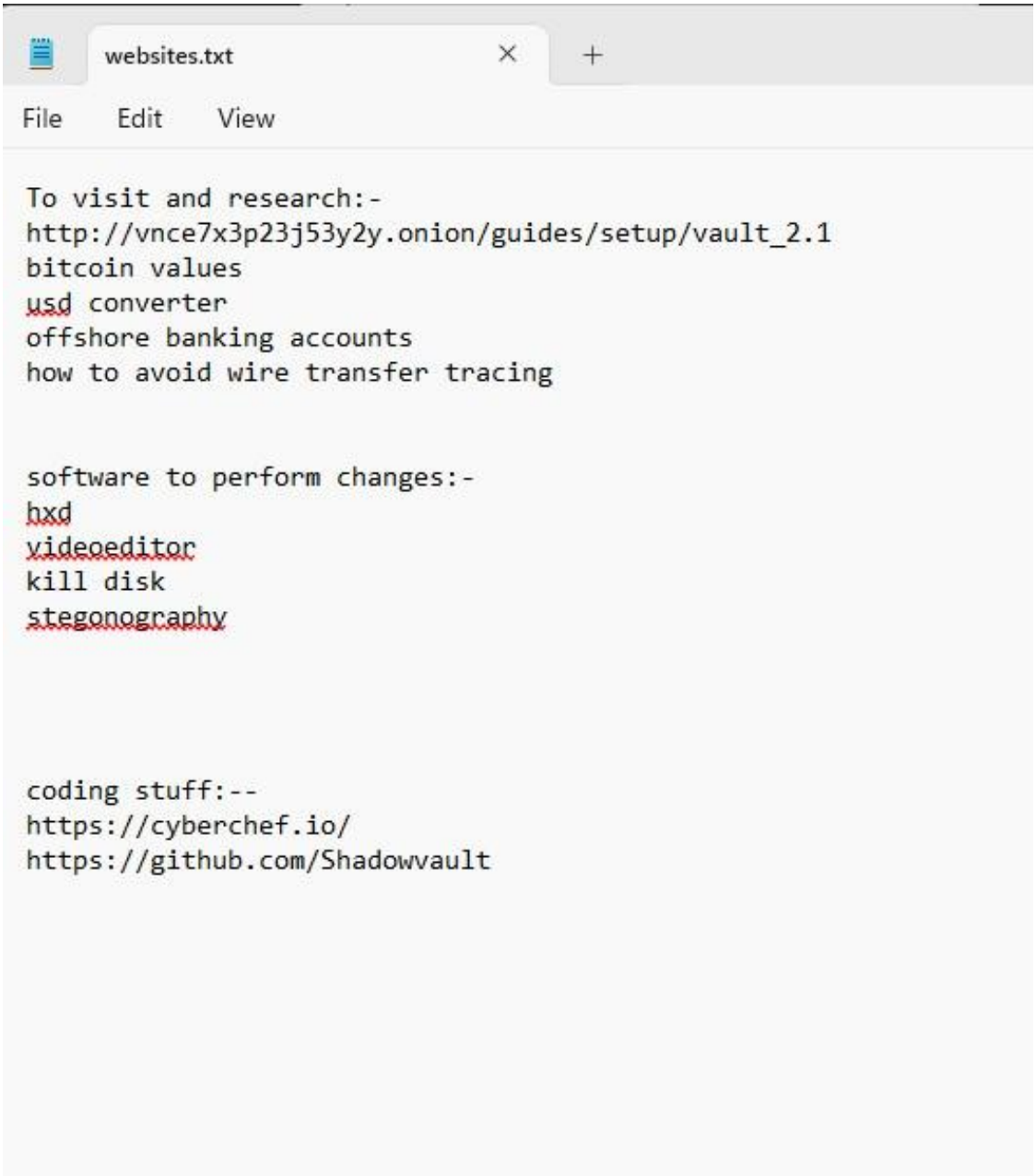
Artefact is	**Tick Appropriate**
Application Level	X
OS Level	
File System Level	X
Reconnaissance / Research phase	X
Recording phase	

Result / Aftermath phase	

Artefact 4: <websites.txt>

A plaintext list of onion addresses, queries, and utilities (including HxD, Kill Disk, and steganography tools). This record evidences research into anonymisation and darkweb activity, confirming intent rather than curiosity.

Location: /img_Operation Forest Hill 7.E01/vol_vol4/vol_vol4/Documents/websites.txt

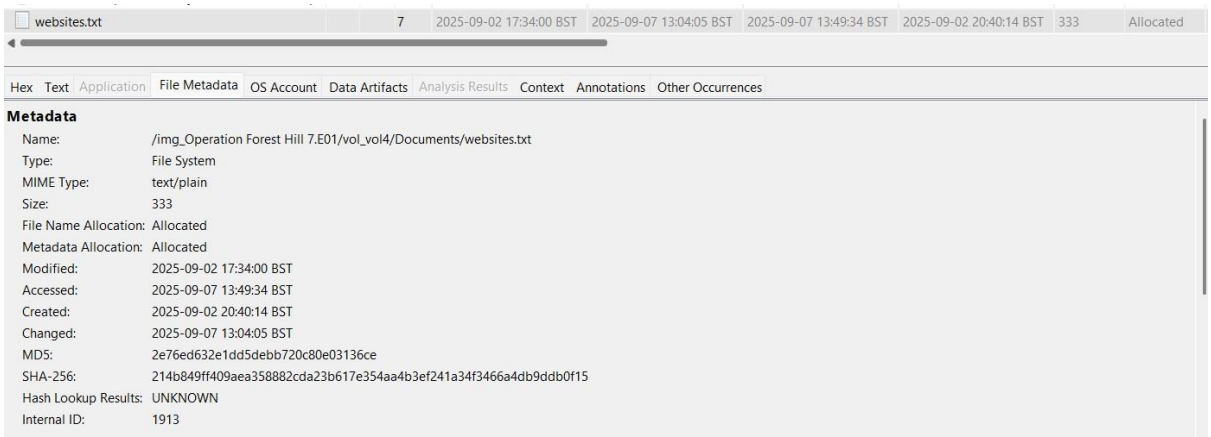


websites.txt

File Edit View

```
To visit and research:-
http://vnce7x3p23j53y2y.onion/guides/setup/vault_2.1
bitcoin values
usd converter
offshore banking accounts
how to avoid wire transfer tracing


software to perform changes:-
hxd
videoeditor
kill disk
stegonography




coding stuff:--
https://cyberchef.io/
https://github.com/Shadowvault
```

Meta-Data of the artefact:



websites.txt	7	2025-09-02 17:34:00 BST	2025-09-07 13:04:05 BST	2025-09-07 13:49:34 BST	2025-09-02 20:40:14 BST	333	Allocated

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

Metadata

Name:	/img_Operation Forest Hill 7.E01/vol_vol4/Documents/websites.txt
Type:	File System
MIME Type:	text/plain
Size:	333
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2025-09-02 17:34:00 BST
Accessed:	2025-09-07 13:49:34 BST
Created:	2025-09-02 20:40:14 BST
Changed:	2025-09-07 13:04:05 BST
MD5:	2e76ed632e1dd5debb720c80e03136ce
SHA-256:	214b849ff409aea358882cda23b617e354aa4b3ef241a34f3466a4db9ddb0f15
Hash Lookup Results:	UNKNOWN
Internal ID:	1913

Implications of the Artefact:

This artefact represents a plain-text record of search activity and browsing targets recovered from the suspect workstation. The entries show visits and research queries such as ***"offshore banking accounts"***, ***"how to avoid wire transfer tracing"***, and a. onion address (***vnce7x3p23j53y2y.onion***) hosting a guide on vault configuration. Together, these indicate interest in anonymised financial transactions and hidden networks. The file also lists utilities (***HxD***, ***Kill Disk***, ***Steganography***) commonly used for data manipulation or concealment, linking technical capability to intent. When correlated with earlier artefacts evidencing bulk data extraction, this browsing record reinforces the hypothesis that the insider was preparing to monetise or conceal stolen Organization X intellectual property via dark-web channels.
In evidential terms, this artefact connects user-driven searches with the broader timeline of exfiltration, forming behavioural evidence of knowledge and motive.

Method to hide/unhide artefact:

This document was discovered under Documents Folder and was not hidden by an ulterior motive. The file opened normally; hashing confirmed integrity

The type of Artefact

Internet history of Content Class

Artefact Detail Table

Artefact is	**Tick Appropriate**
Application Level	X

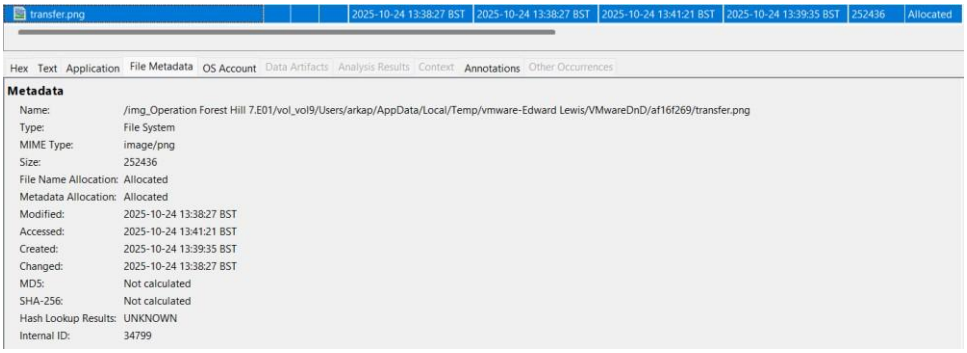
OS Level	
File System Level	X
Reconnaissance / Research phase	X
Recording phase	
Result / Aftermath phase	

Artefact 5: Transfer.png

An image displaying a message referencing a £26 000 payment “as per the deal.” The timestamp follows the exfiltration event, supporting the inference of financial reward. MRU records confirm the file was opened by the suspect, linking it directly to user knowledge.

Location: /img_Operation Forest Hill 7.E01/vol_vol4/Personal/transfer.png

Meta-Data of the artefact:



transfer.png			2025-10-24 13:38:27 BST	2025-10-24 13:38:27 BST	2025-10-24 13:41:21 BST	2025-10-24 13:39:35 BST	252436	Allocated

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

Metadata

Name:	/img_Operation Forest Hill 7.E01/vol_vol9/Users/arkap/AppData/Local/Temp/vmware-Edward Lewis/VMwareDnD/af16f269/transfer.png
Type:	File System
MIME Type:	image/png
Size:	252436
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2025-10-24 13:38:27 BST
Accessed:	2025-10-24 13:41:21 BST
Created:	2025-10-24 13:39:35 BST
Changed:	2025-10-24 13:38:27 BST
MD5:	Not calculated
SHA-256:	Not calculated
Hash Lookup Results:	UNKNOWN
Internal ID:	34799

Implications of the Artefact:

This artefact provides strong circumstantial evidence connecting the insider data breach to financial gain. The message references a **£26,000** payment made "as per the deal," implying compensation following an illicit transaction. The timestamp **Friday, 5th November at 20:27 (**falls within the period immediately after the exfiltration event, reinforcing its temporal Recovered through image enumeration within the Pictures directory. Metadata shows consistent creation and modification timestamps. The file was verified using hash comparison and previewed under controlled forensic viewing to maintain evidential integrity. Incident. Forensically, communication artefacts like this link digital activity (data transfer logs, recovered documents) to human behaviour and motive. It supports the hypothesis that confidential Organization X research materials were not only stolen but monetised. When correlated with the recovered browsing evidence (dark-web and offshore-banking searches), it demonstrates a coordinated sequence: theft, concealment, and financial transfer.

Method to hide/unhide artefact:

Recovered through image enumeration within the **Pictures** directory. Metadata shows consistent creation and modification timestamps. The file was verified using hash comparison and previewed under controlled forensic viewing to maintain evidential integrity.

The type of Artefact

Chat/message artefact of Content class

Artefact Detail Table

Artefact is	**Tick Appropriate**

Application Level	X
OS Level	X
File System Level	
Reconnaissance / Research phase	
Recording phase	
Result / Aftermath phase	X

Hiding Artefacts

Artefact 6: <Office work.txt>

A text file encoded using CyberChef's *To Hex* recipe, producing hexadecimal output that obscures the readable message "passwd = A1-B1." When decoded, this reveals the password structure used for the encrypted container. This artefact shows deliberate technical concealment of credentials.

Location: /img_Operation Forest Hill 7.E01/vol_vol4/Personal/Office work.txt

Picture of the artefact:

/img_COMP-1812_MIDR-2025-007-EVID-01_Win10_2025.E01/vol_vol4/Personal 4 Results

Table Thumbnail Summary

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time
[current folder]				2025-07-25 18:40:22 BST	2025-09-07 13:50:00 BST	2025-09-07 18:40:22
[parent folder]				2025-09-07 12:41:36 BST	2025-09-07 12:41:36 BST	2025-09-07 13:56:14
Office work.txt			6	2025-09-06 18:56:22 BST	2025-09-07 13:41:02 BST	2024-09-06 18:56:22

Data Artifacts Analysis Results Context Annotations Other Occurrences

Hex Text Application File Metadata OS Account

Strings Extracted Text Translation

Page: 1 of - Page Matches on page: - of - Match 100% Reset

Text Source: File Text

70 61 73 73 77 64 20
3d 20 41 31 2d 42 31

Meta-Data of the artefact:

Office work.txt 7 2025-09-06 18:56:22 BST 2025-09-07 13:41:02 BST 2024-09-06 18:56:22 BST 2025-09-06 18:56:22 BST 43 Allocate

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

Metadata

Name:	/img_Operation Forest Hill 7.E01/vol_vol4/Personal/Office work.txt
Type:	File System
MIME Type:	text/plain
Size:	43
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2025-09-06 18:56:22 BST
Accessed:	2024-09-06 18:56:22 BST
Created:	2025-09-06 18:56:22 BST
Changed:	2025-09-07 13:41:02 BST
MD5:	5c515f66635856ebb759df8dae1ef66a
SHA-256:	585a6fc7efacfb42bd26af384d9d1e1a293bca783a10804a477aa84242f206be
Hash Lookup Results:	UNKNOWN
Internal ID:	1988

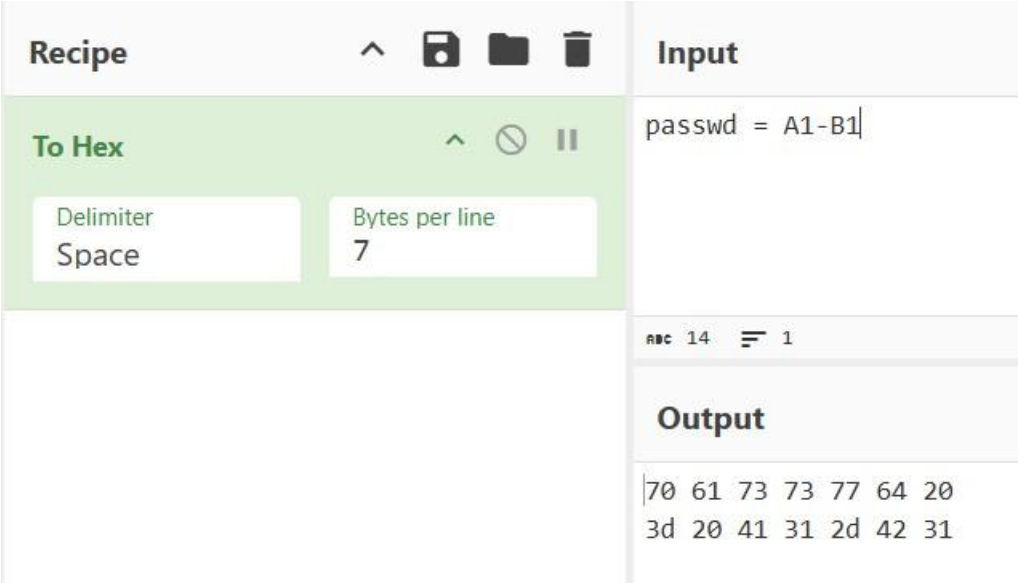
Implications of the Artefact:

The encoded text file constitutes clear evidence of deliberate concealment and is relevant to the reconstruction of the timeline because it provides, or leads directly to, the password protecting the VeraCrypt container. When considered alongside other artefacts that confirm the presence and later use of that container (such as mount activity or recovered file listings), the decoded hint significantly strengthens the evidential link between the user and the concealed volume, demonstrating purposeful encryption rather than accidental storage. Furthermore, the decoded text includes references that match the names of two image files found elsewhere in the evidence set, and this correlation further reinforces provenance by showing that the concealed material is contextually and intentionally connected to other files associated with the

suspect. In combination, this establishes both user knowledge and deliberate datahiding behaviour occurring after the primary activity, aligning the artefact with the aftermath phase of the offence.

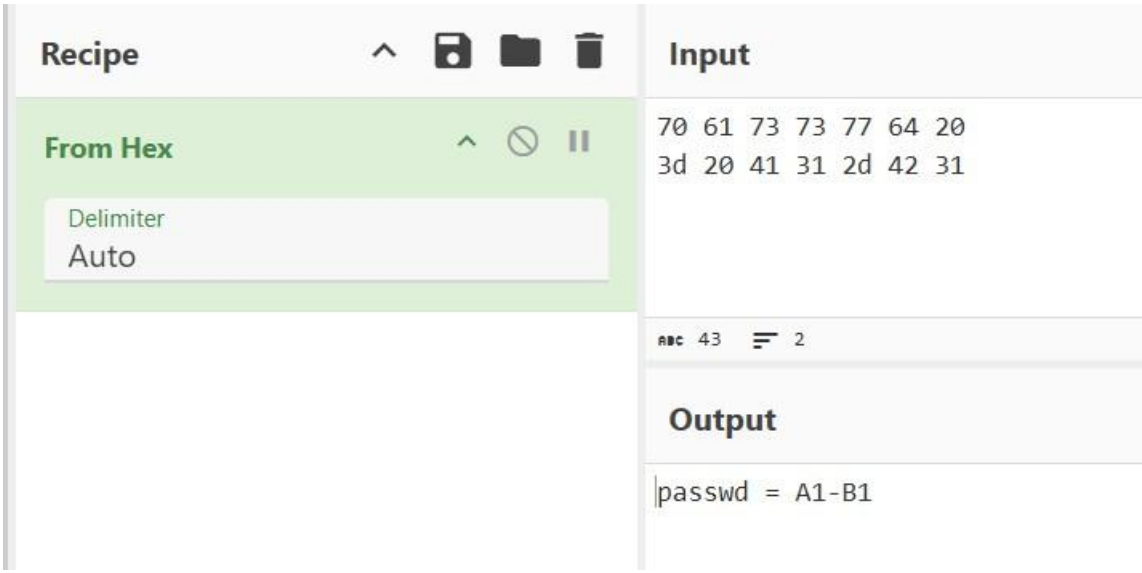
Method to hide/unhide artefact:

Method to Hide:



The artefact was concealed by converting a plain-text hint into a hex representation using the CyberChef recipe To_Hex('Space',7). This operation produces hexadecimal byte values separated by spaces and grouped with seven bytes per line, so that the original readable text is replaced by spaced hex groups and therefore appears as an innocuous text file to a casual observer. The encoded output was written to Office work.txt and saved in the personal folder of the evidence image, leaving standard filesystem metadata intact while obscuring the string that points to the VeraCrypt password.

Method to Unhide:



To unhide the content, the text file must first be exported from the read-only mounted image for analysis. A second reference file within the evidence contains a bookmarked CyberChef link pointing to https://gchq.github.io/CyberChef/#recipe=To_Hex('Space',7), which discloses the method used to encode the data. By loading the exported contents into CyberChef and applying the inverse recipe From_Hex('Auto') via https://gchq.github.io/CyberChef/#recipe=From_Hex('Auto'), the original ASCII text is reconstructed. After decoding, the recovered plaintext clearly displays the string **"passwd = A1-B1"**, which serves as the password (or direct password hint) for accessing the associated VeraCrypt-protected folder, and a screenshot of this decoding step is included as supporting evidence.

The type of Artefact

The type of artefact is Encoded or encrypted text of the Hiding class.

Artefact Detail Table:

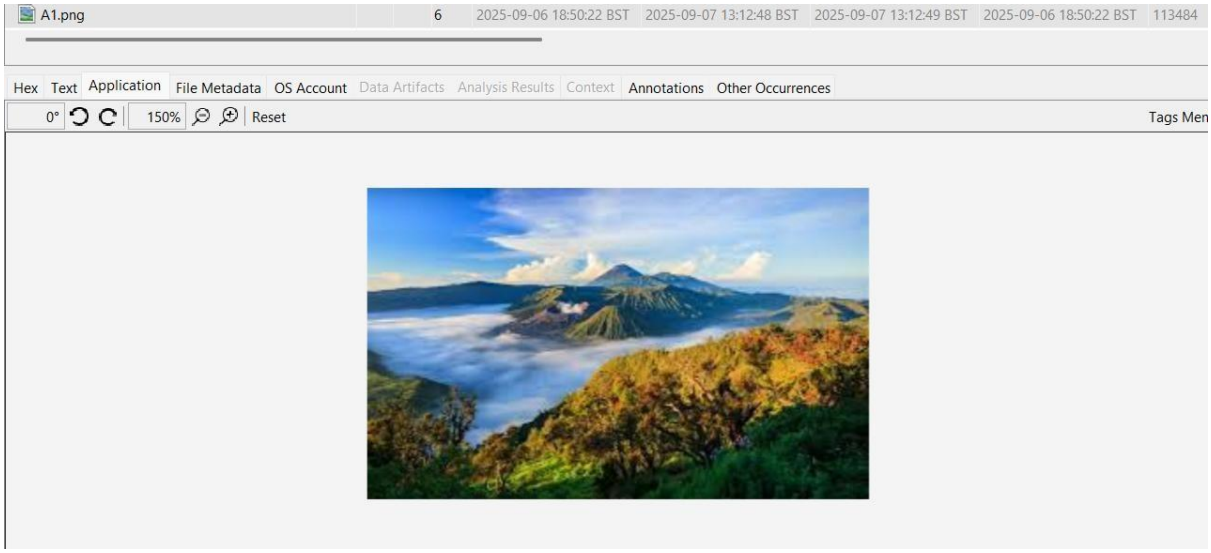
Artefact is	**Tick Appropriate**
Application Level	
OS Level	

File System Level	x
Reconnaissance / Research phase	
Recording phase	
Result / Aftermath phase	x

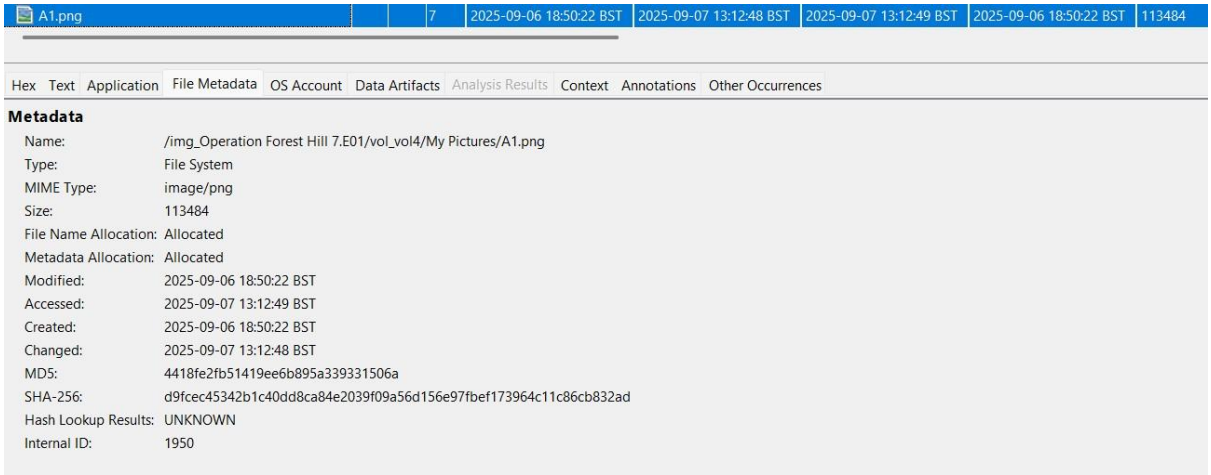
Artefact 7: < A1.png >

Two steganographic images embedding the halves of the VeraCrypt password. Decoding reveals the strings *silver-cedar* and *echo-quietly*. When combined according to the hint from *Office work.txt*, they form the full passphrase used to decrypt *ZYNSRV04_extract_2025-09-05*. These artefacts prove conscious and layered concealment of encryption keys.

Location: /img_Operation Forest Hill 7.E01/vol_vol4/My Pictures/A1.png Picture of the artefact:



Meta-Data of the artefact:



Implications of the Artefact:

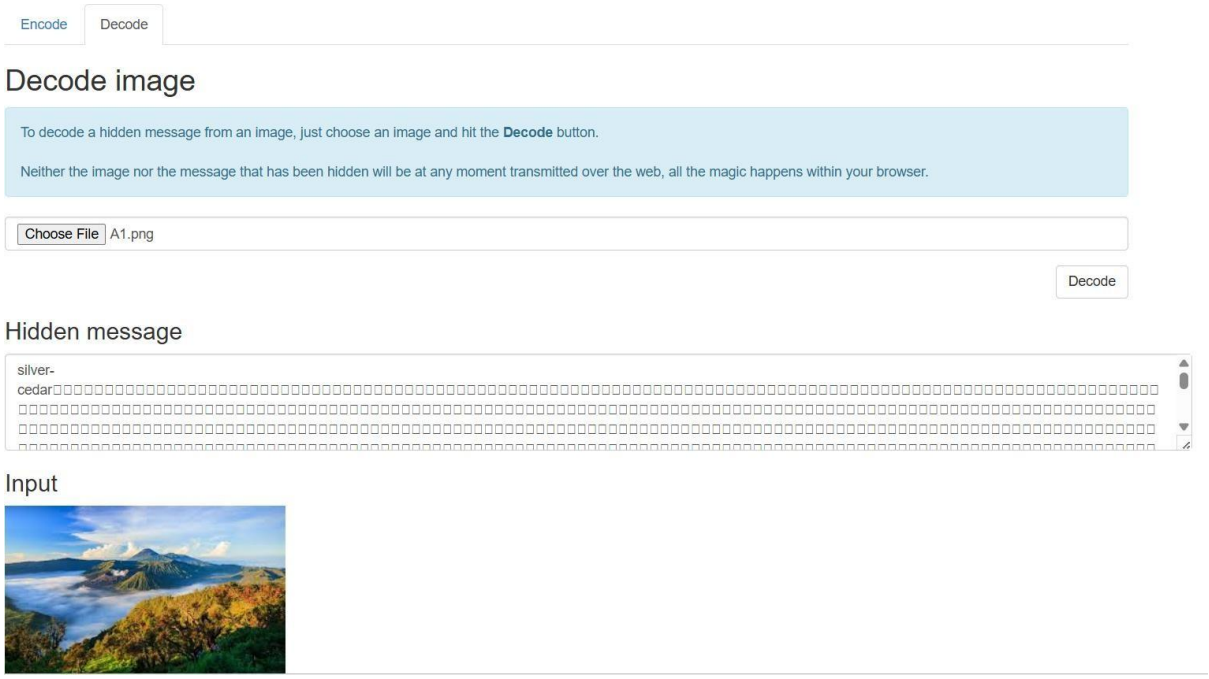
The image **A1.png** contains embedded data that constitutes the first half of the password used to protect a VeraCrypt container, and therefore directly supports the hypothesis of deliberate concealment. The presence of embedded plaintext within the image, combined with the previously decoded hint that referenced this filename, provides a clear linkage between the encoded hint and concealed material. The recovered embedded string silver-cedar corroborates the provenance of the protected container by supplying part of the credential needed to open it; this strengthens the evidential chain because the same filename and matching strings appear across multiple artefacts. Taken together with evidence of the VeraCrypt container and any relevant mount or access logs, the embedded text demonstrates purposeful datahiding behaviour consistent with post-exfiltration concealment.

Method to hide/unhide artefact:

Method to Hide: The hiding was performed using a browser-based steganography tool (https://stylesuxx.github.io/steganography/) by selecting A1.png as the carrier image and embedding the chosen plaintext into the image using the tool's embed function. The operation produced a visually unchanged PNG file that nevertheless contains the embedded bytes in a way that is not visible in ordinary image viewers; standard filesystem metadata for the file remained intact. The embedded text was intentionally chosen to represent the first half of a multi-component password and saved to A1.png in the My Pictures folder of the evidence image.

Method to Unhide: To reveal the embedded content, A1.png should be exported from the read-only mounted evidence image to an analysis workspace and then loaded into

the same steganography tool (https://stylesuxx.github.io/steganography/). Using the tool's decode functionality with the default settings will read the hidden payload from the image and display the embedded plaintext. When this procedure is applied to the exported A1.png, the decoded output is the string **silver-cedar**, which represents the first half of the password used to access the associated VeraCrypt-protected folder. Screenshots of the upload step and the decoded output are included as supporting evidence.



The type of Artefact

The type of artefact is Embedded text or information into a picture of the Hiding class.

Artefact Detail Table:

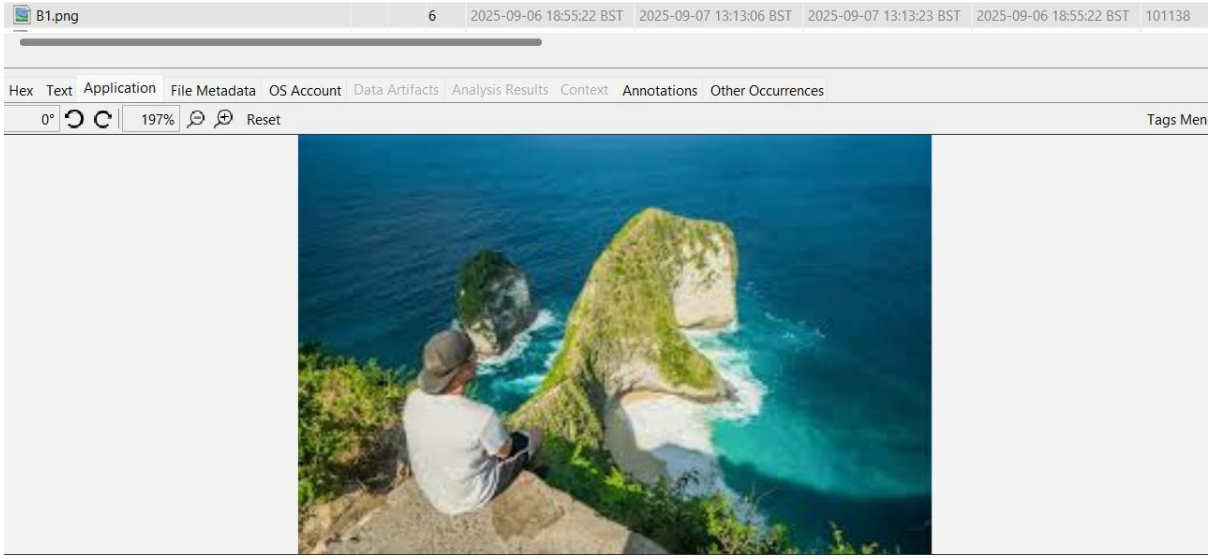
Artefact is	**Tick Appropriate**
Application Level	
OS Level	
File System Level	x

Reconnaissance / Research phase	
Recording phase	
Result / Aftermath phase	x

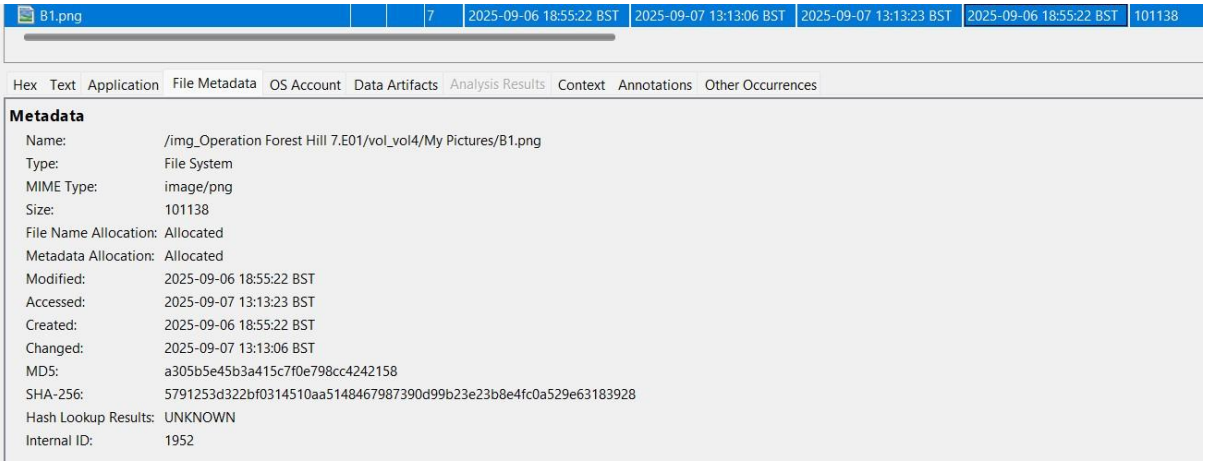
Artefact 8: <B1.png>

Location: Location 8: / /img_Operation Forest Hill 7.E01/vol_vol4/My Pictures/B1.png

Picture of the artefact:



Meta-Data of the artefact:



Implications of the Artefact:

B1.png contains embedded data that constitutes the second half of the multicomponent password protecting a VeraCrypt container. The recovered payload, when combined with the first half extracted from A1.png and the directional hint contained in Office work.txt, permits reconstruction of the complete password used to access the protected volume. This linkage between three separate artefacts (the hint file and the two steganographic images) establishes a coherent chain connecting the user to the concealed data and demonstrates a deliberate, multi-step approach to credential hiding and container protection consistent with post-incident concealment. The presence of matching strings across artefacts strengthens provenance and supports an inference of intentional concealment rather than innocent coincidence.

Method to hide/unhide artefact:

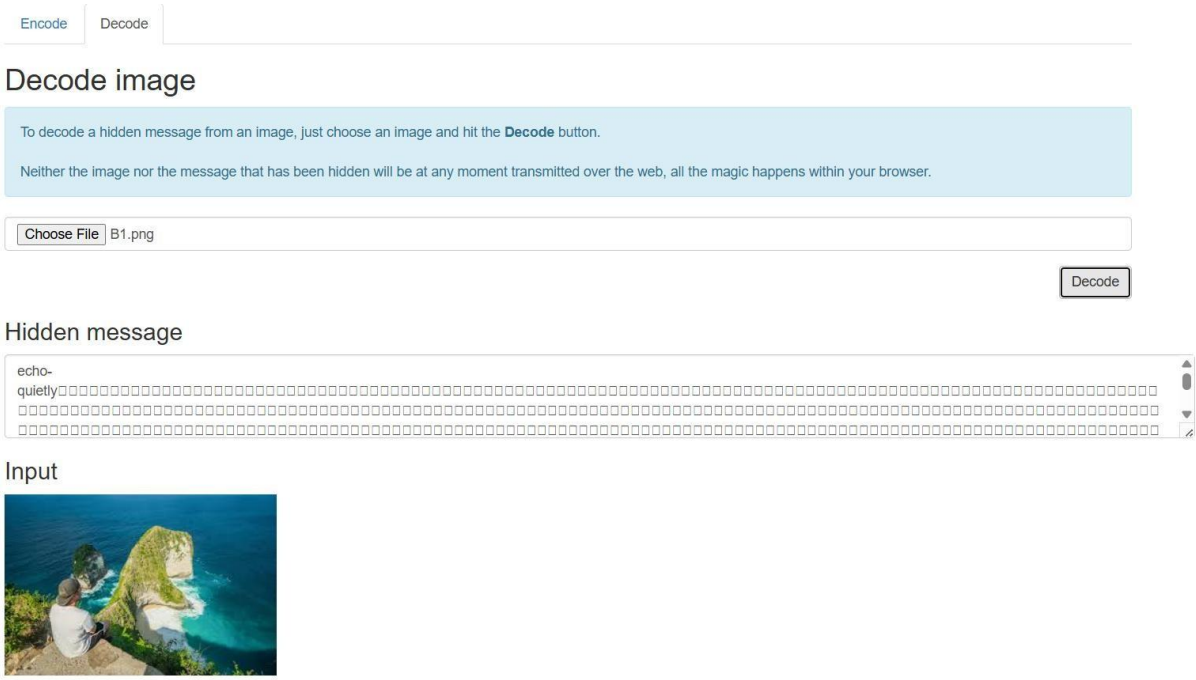
Method to Hide:

The carrier image B1.png was used to embed the second half of the password via the same browser-based steganography tool used for the other image (https://stylesuxx.github.io/steganography/). The plaintext payload containing the second password segment was embedded into the image using the tool's embed functionality, producing a visually unchanged PNG file that nonetheless contains hidden data inaccessible to standard image viewers. File metadata remained intact, and the image was stored in the My Pictures folder of the evidence image.

Method to Unhide:

To extract the hidden payload from B1.png, the file should be exported from the readonly mounted evidence image to an analysis workspace and opened with the same steganography extraction tool. Using the tool's extract/decode function with

default parameters will reveal the embedded plaintext. The decoded output for B1.png produces the string representing the second half of the password. When this second half is concatenated with the first half obtained from A1.png (silver-cedar) and interpreted together with the direction provided by the decoded hint in Office work.txt (passwd = A1-B1), the complete password is formed as: **silver-cedar-echo-quietly**. Screenshots of the extraction steps and the decoded output are included as supporting evidence, along with hashes of the exported carrier image and any decoded payload files.



The type of Artefact:

The type of artefact is Steg of pictures of the Hiding class.

Artefact Detail Table

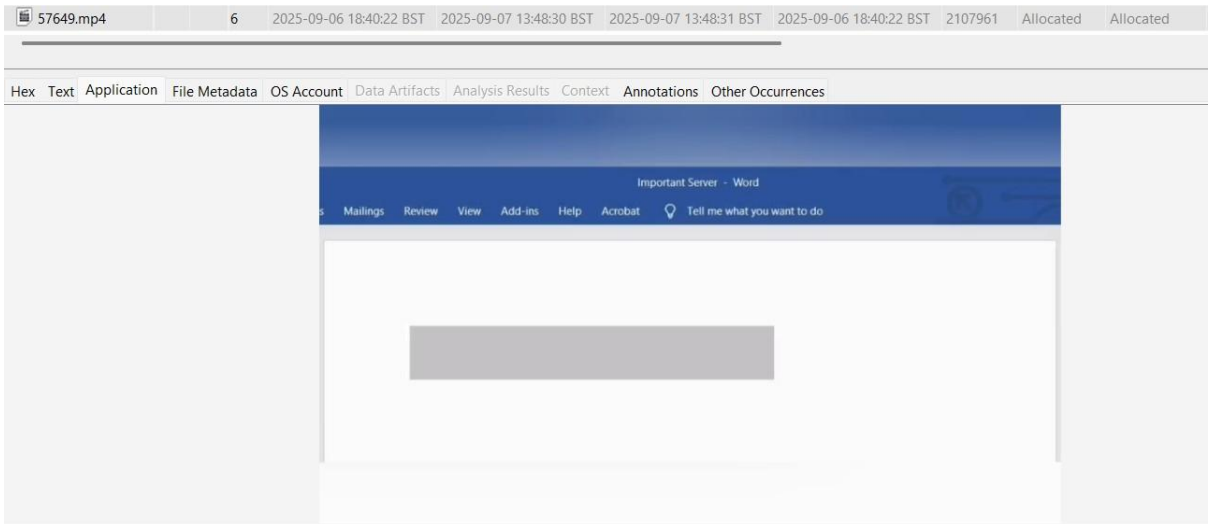
Artefact is	**Tick Appropriate**
Application Level	
OS Level	
File System Level	x

Reconnaissance / Research phase	
Recording phase	
Result / Aftermath phase	x

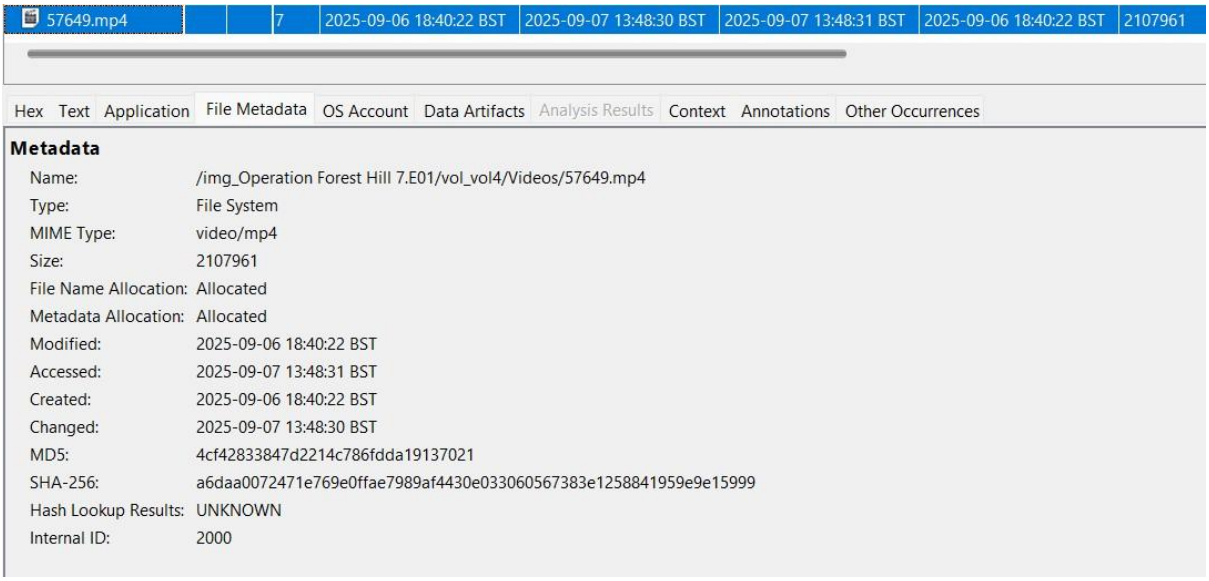
Artefact 9: <57649.mp4>

A short video containing a single hidden frame (white text on a white background) showing an IP address corresponding to the exfiltration destination. This demonstrates use of visual steganography to store or communicate covert information.

Location: /img_Operation Forest Hill 7.E01/vol_vol4/Videos/57649.mp4



Meta-Data of the artefact:



57649.mp4		7	2025-09-06 18:40:22 BST	2025-09-07 13:48:30 BST	2025-09-07 13:48:31 BST	2025-09-06 18:40:22 BST	2107961

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

Metadata

Name:	/img_Operation Forest Hill 7.E01/vol_vol4/Videos/57649.mp4
Type:	File System
MIME Type:	video/mp4
Size:	2107961
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2025-09-06 18:40:22 BST
Accessed:	2025-09-07 13:48:31 BST
Created:	2025-09-06 18:40:22 BST
Changed:	2025-09-07 13:48:30 BST
MD5:	4cf42833847d2214c786fdda19137021
SHA-256:	a6daa0072471e769e0ffae7989af4430e033060567383e1258841959e9e15999
Hash Lookup Results:	UNKNOWN
Internal ID:	2000

Implications of the Artefact:

Although the video initially appears to be a harmless 10-second clip, it contains a concealed frame inserted mid-sequence that flashes for approximately one second between the 4th and 5th second. This concealed frame contains text that has been intentionally hidden using white text against a white background, which is not visible during standard playback. When the frame is isolated and examined, the hidden content reveals an **IP address**, which is likely a pointer to further communication infrastructure related to the concealed material. The use of a spliced frame to embed covert information demonstrates a deliberate and technically competent attempt to obscure network-relevant data inside a seemingly innocuous media file. This creates a direct evidential link between the suspect and potential external infrastructure used to host, transfer, or conceal further data.

Method to hide/unhide artefact:

Method to Hide: The concealment relies on video splicing: a single frame containing a blank white document was inserted into the middle of the clip and overlaid with white text on a white background so that the text blends in and cannot be read during normal playback. Because only one modified frame was inserted into the otherwise ordinary clip, the splicing is visually imperceptible unless playback is slowed or paused precisely at the correct timestamp. This approach leverages steganographic principles in video form, effectively concealing the payload inside an otherwise legitimate clip without altering its superficial appearance.

Method to Unhide: To reveal the hidden text, the video is opened in VLC media player and played frame-by-frame until the inserted white frame appears at approximately the 4–5 second mark. Pausing on this exact frame allows the contents to be examined, and the previously invisible white text becomes identifiable once isolated from the surrounding video sequence. The extracted frame shows an **IP address**, confirming that it was intentionally spliced into the video for concealment purposes.

The type of Artefact

The type of artefact is Splicing – using software to edit video (video-based concealment) of the Hiding class.

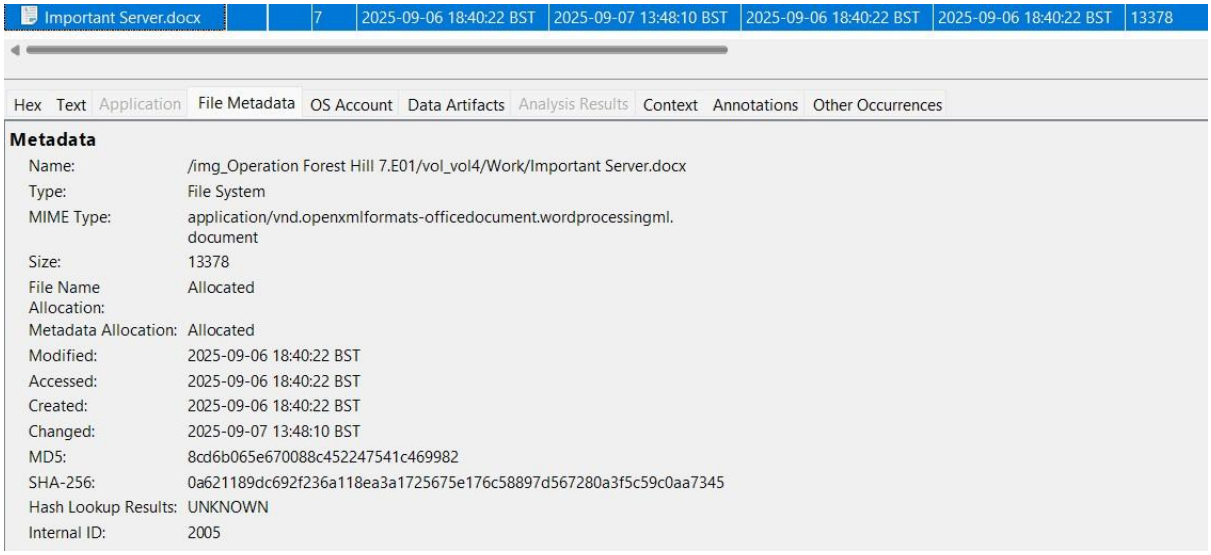
Artefact Detail Table

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

Artefact 10: Important Server.docx

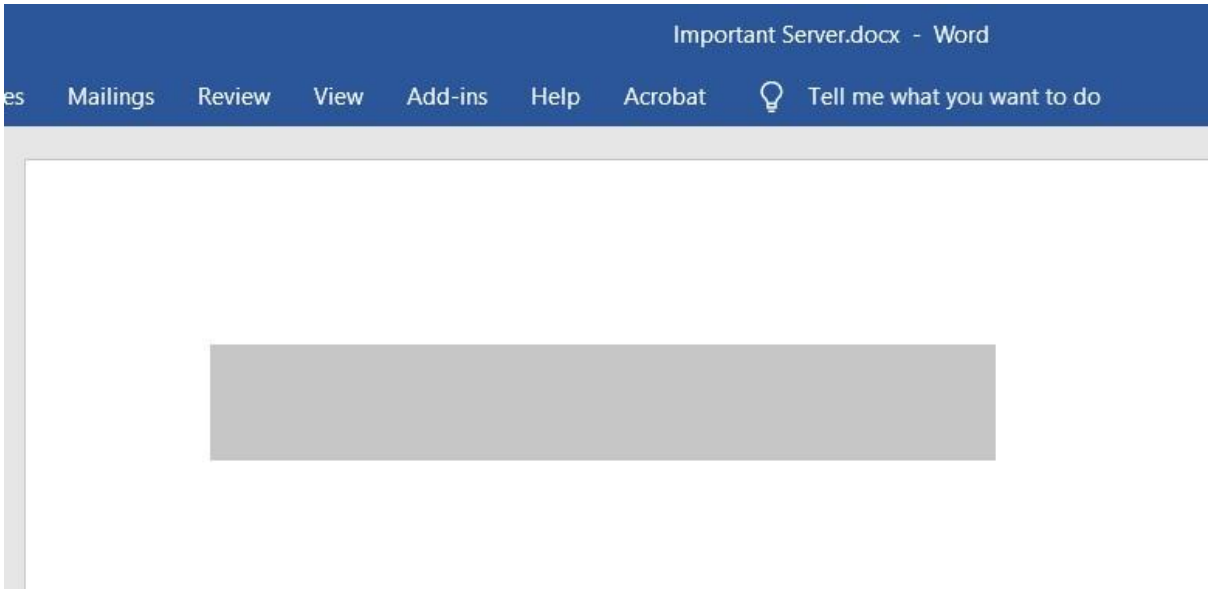
A Word document with white text on a white background and the hidden file attribute enabled. When revealed, it reproduces the same IP address found in the spliced video, establishing a link between different concealment methods.

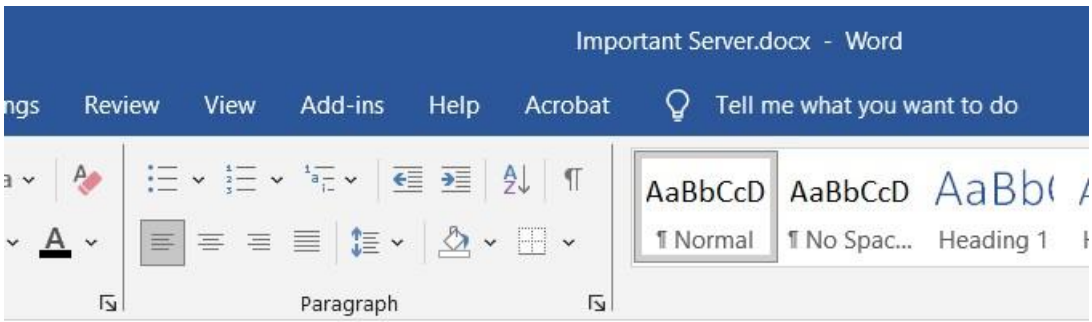
Meta-Data of the artefact:



Implications of the Artefact:

This artefact represents a second stage of concealment linked to the spliced video discovered previously. The video contained a brief flash of a white-on-white document containing an IP address, which corresponds directly to the contents of Important Server.docx. The fact that the document is both visually concealed (white text on white background) and file-system concealed (marked hidden at OS level) demonstrates deliberate intent to prevent discovery by ordinary inspection. By combining content obfuscation with operating-system-level hiding, the suspect layered concealment mechanisms, suggesting technical awareness and planning. Because the embedded IP address is potentially associated with a remote host or server, its concealment is material to the wider investigation and may relate to further storage or communications activity.

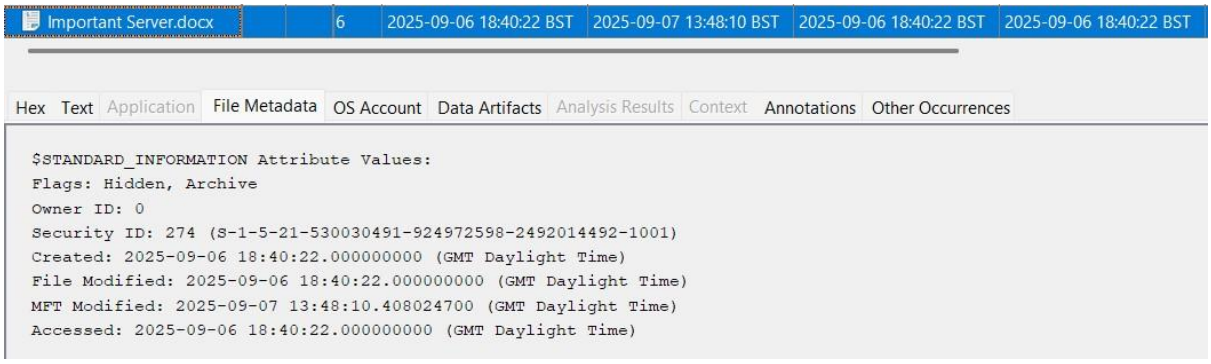




FTP Server: 192.168.69.232

Method to hide/unhide artefact:

Method to Hide:



The concealment relied on the operating system's native hidden file attribute. The document was first prepared by changing the font colour of the text to white so that its

contents would not be visible on normal viewing. After this, the file's properties were edited through the Windows file explorer, and the **Hidden** checkbox was selected, causing the file to disappear from normal folder listings unless hidden items are manually revealed. This form of concealment does not involve encryption and leaves metadata intact but effectively removes the file from view for non-technical users.

Method to Unhide: The document was made invisible at operating-system level by enabling the Windows "hidden" attribute, so it does not appear in normal folder listings. When the file is viewed in Autopsy, the $STANDARD_INFORMATION attribute confirms concealment because the Flags field explicitly shows **"Hidden, Archive"**, indicating the file was deliberately marked as hidden rather than deleted or encrypted. Once hidden files are enabled for viewing in the file browser, Important Server.docx becomes visible and can be opened normally. The contents were further obscured by setting the text colour to white against a white page background; when the text is highlighted or its formatting is changed, an **IP address** becomes visible inside the document. This demonstrates that the concealment relied on a combination of an OSlevel hidden flag and a visual-layer concealment of the payload inside the document.

The type of Artefact:

Class: The "hidden" flag within an operating system (file attribute concealment).

Artefact Detail Table:

Artefact is	**Tick Appropriate**
Application Level	
OS Level	X
File System Level	

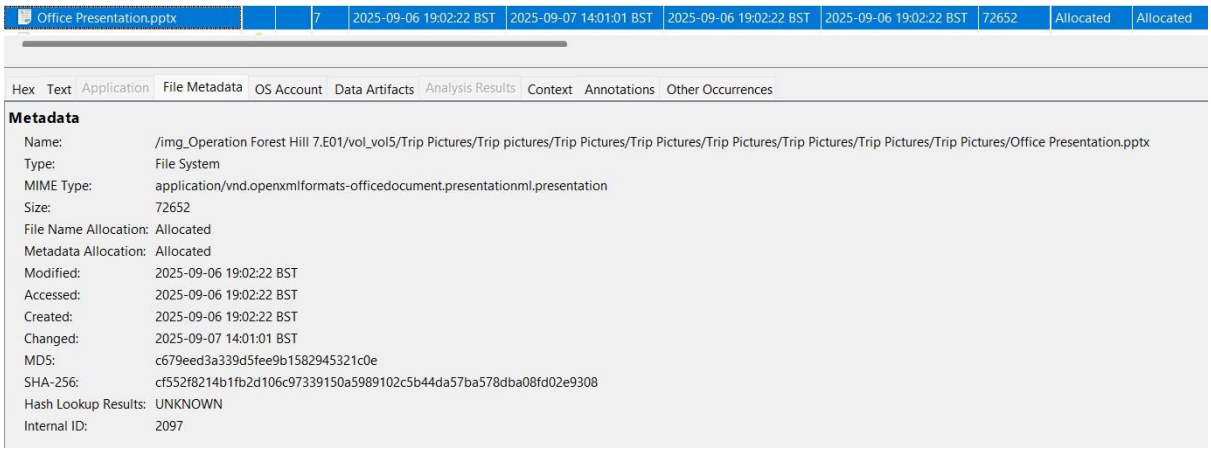
Reconnaissance / Research phase	
Recording phase	X
Result / Aftermath phase	X

Artefact 11: Office Presentaion.pptx

A PowerPoint presentation in which a white overlay conceals embedded text. The hidden content included phrases referencing encryption and project names connected to the stolen data. This shows yet another layer of obfuscation within an apparently harmless file.

Location: / /img_Operation Forest Hill 7.E01/vol1_vol5/Trip Pictures//Trip Pictures//Trip Pictures//Trip Pictures//Trip Pictures//Trip Pictures//Trip Pictures//Trip Pictures/Office PRESENTATION.pptx

Meta-Data of the artefact:



Implications of the Artefact:

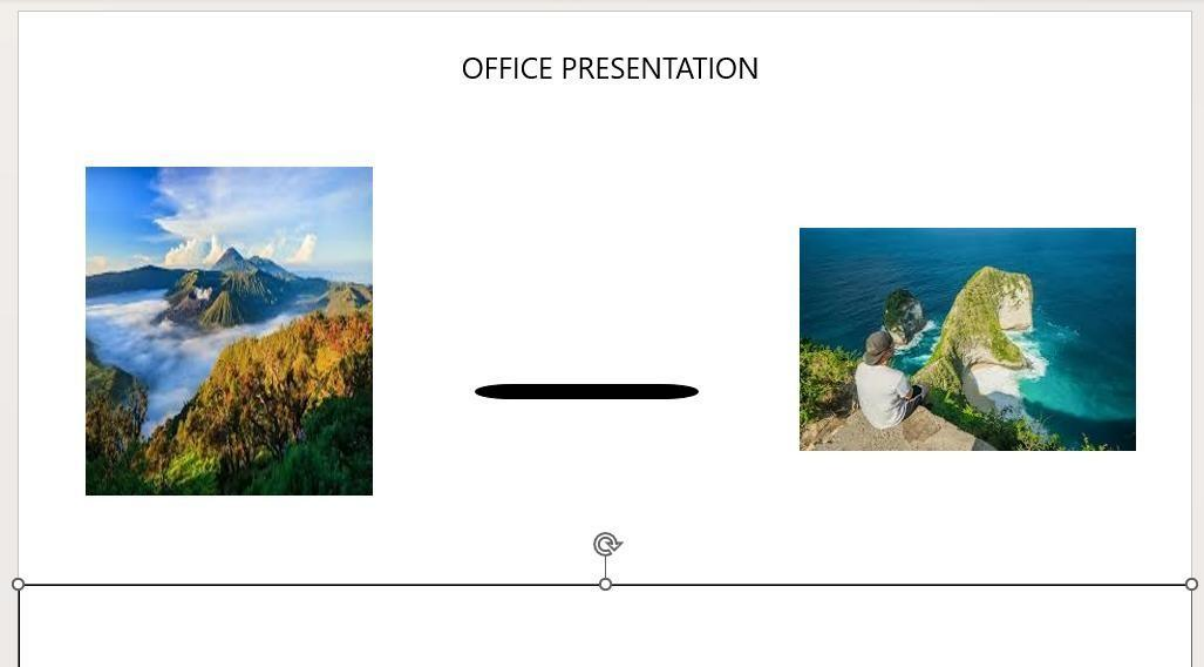
The recovered Artefact 11, titled “Office Presentation.pptx”, appeared at first glance to be a standard presentation containing scenic images and minimal text. Upon closer inspection, a white rectangular shape was found overlaying a section of the slide.

When this object was moved, encoded text was revealed beneath it. The presence of hidden text within an ordinary document suggests intentional concealment of information potentially used to store or transmit encryption keys or passwords without attracting attention.

Method to hide/unhide artefact:

The data was hidden by placing a white shape over text on a presentation slide, effectively masking it from view during normal use. To reveal the hidden content, investigators manually moved or deleted the overlaying object within the presentation software, exposing the concealed text beneath.

Before and after Recovery



The type of Artefact: Hiding text or pictures within a document **Artefact Detail Table:**

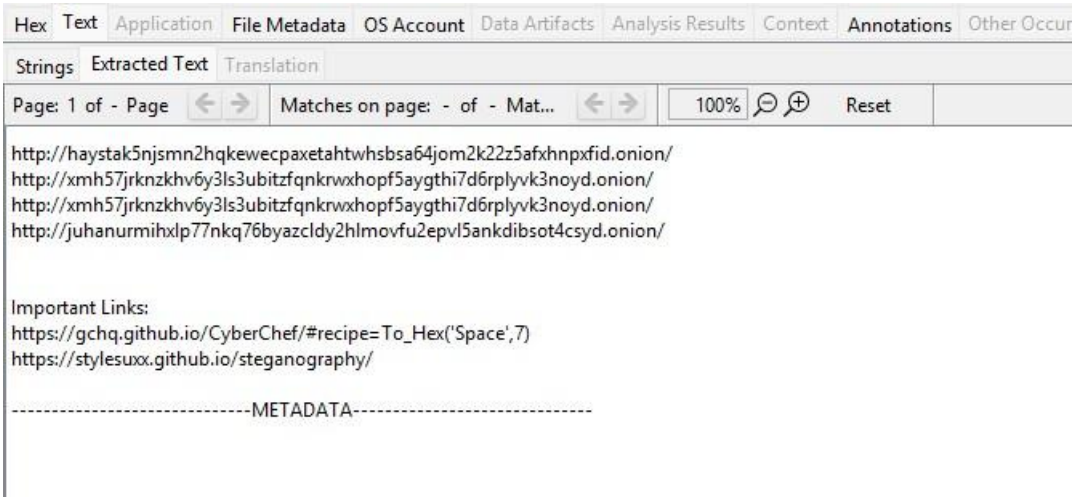
Artefact is	**Tick Appropriate**

Application Level	X
OS Level	
File System Level	
Reconnaissance / Research phase	X
Recording phase	
Result / Aftermath phase	

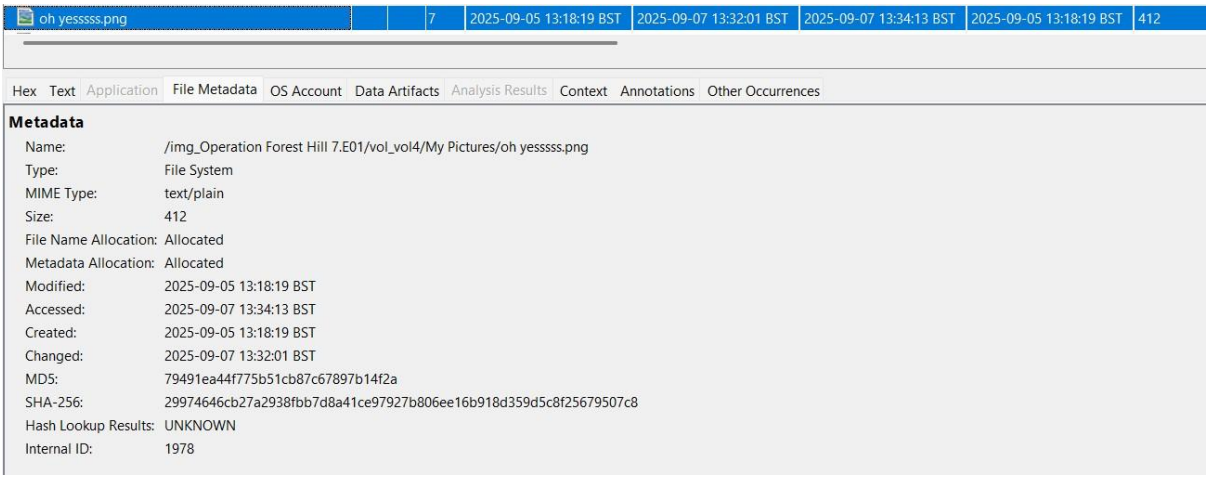
Artefact 12: <oh yesssss.png >

Originally a text file renamed with an image extension to disguise its nature. It contains a list of URLs and references to CyberChef and steganography tools, showing experimental concealment techniques.

Location:/ /img_Operation Forest Hill 7.E01/vol_vol4My Pictures/oh yesssss.png



Meta-Data of the artefact:



Implications of the Artefact:

Artefact 12 is an image file titled **"oh yessss.png.** It contains visible extracted text revealing multiple URLs and references to steganography/encoding tools (e.g., CyberChef). The content indicates attempts to conceal communication paths and/or instructions for covert data handling.

The file was altered from a text file to an image file (extension changed to .png) to disguise its true nature and reduce scrutiny.

Method to hide/unhide artefact:

The text file containing the URLs was disguised by altering its file extension to .png, making it appear as an image instead of a text document. This modification successfully masked the nature of its content from casual inspection.

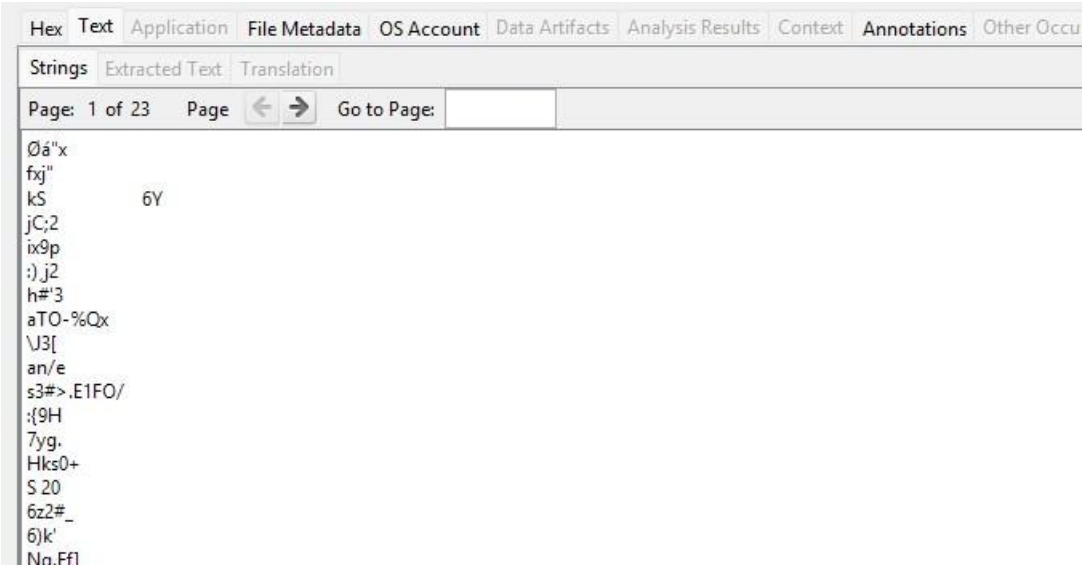
The type of Artefact: Manipulating file extensions **Artefact Detail Table:**

Artefact is	**Tick Appropriate**
Application Level	X
OS Level	
File System Level	X

Reconnaissance / Research phase	X
Recording phase	
Result / Aftermath phase	

Artefact 13: 5-30.jpg

A modified image whose JPEG header was intentionally corrupted. Hex-level repair revealed a floor-plan image, confirming deliberate alteration to mislead forensic scanners. This file exemplifies low-level manipulation of file signatures. Location: //img_Operation Forest Hill 7.E01/vol_vol4/My Pictures/5-30.jpg



Meta-Data of the artefact:

5-30.jpg		7	2025-09-03 05:37:22 BST	2025-09-07 13:10:40 BST	2025-09-07 14:14:51 BST	2025-09-03 05:37:22 BST	369220

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

Metadata

Name:	/img_Operation Forest Hill 7.E01/vol_vol4/My Pictures/5-30.jpg
Type:	File System
MIME Type:	application/octet-stream
Size:	369220
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2025-09-03 05:37:22 BST
Accessed:	2025-09-07 14:14:51 BST
Created:	2025-09-03 05:37:22 BST
Changed:	2025-09-07 13:10:40 BST
MD5:	3f241e6f1d4193f64f740a91359f9c10
SHA-256:	e9d371163800e506ee2a6c51d90f08a09fdd9697f8a0704853e36d489c60bdcd
Hash Lookup Results:	UNKNOWN
Internal ID:	1934

Implications of the Artefact:

The recovered Artefact 13 is a file titled “5-30.jpg”, identified as a floor plan image of a building. Examination revealed that the file’s header had been deliberately modified to disguise its original format. This manipulation rendered the file misleading to standard systems, allowing it to appear as an innocuous image.

Method to hide/unhide artefact:

The recovered **Artefact 13**, titled **“5-30.jpg”**, initially appeared to be a standard JPEG image. However, hex analysis revealed **anomalies in the header structure**—the file begins with modified or misplaced JPEG markers (FF D8 FF E0 / E1) inconsistent with a clean JPEG sequence. This alteration indicates that the **header was deliberately edited** to disguise the file’s true nature or to embed non-image data.

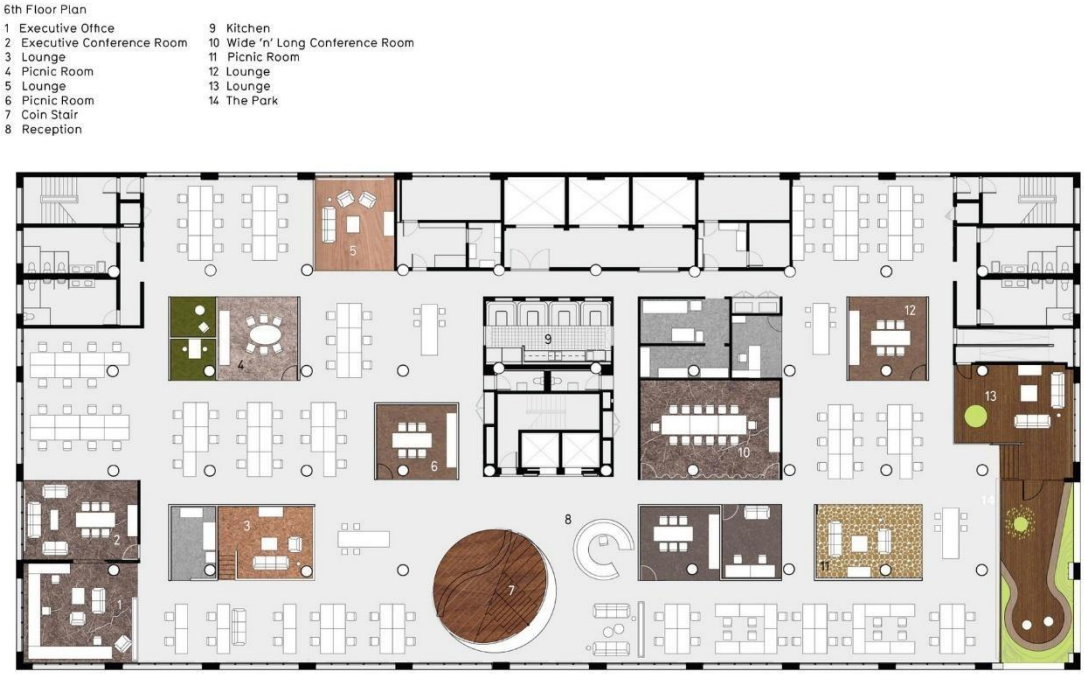
File header before the recovery and after the recovery:

```
Offset(h) 00 01 02 03 04 05 06
00000000  00 D8 00 E1 00 22 00
00000010  00 00 00 08 00 01 01
00000020  00 00 00 00 00 00 FF
```

After

```
Offset(h) 00 01 02 03 04 05 06
00000000  FF D8 FF E1 00 22 45
00000010  00 00 00 08 00 01 01
00000020  00 00 00 00 00 00 FF
00000030  02 02 03 02 02 03 03
```

recovering the file header using HXD it appears to be a floor plan



The type of Artefact:

Manipulating file header to hide the file

Artefact Detail Table:

Artefact is	**Tick Appropriate**
Application Level	X
OS Level	X
File System Level	
Reconnaissance / Research phase	X
Recording phase	

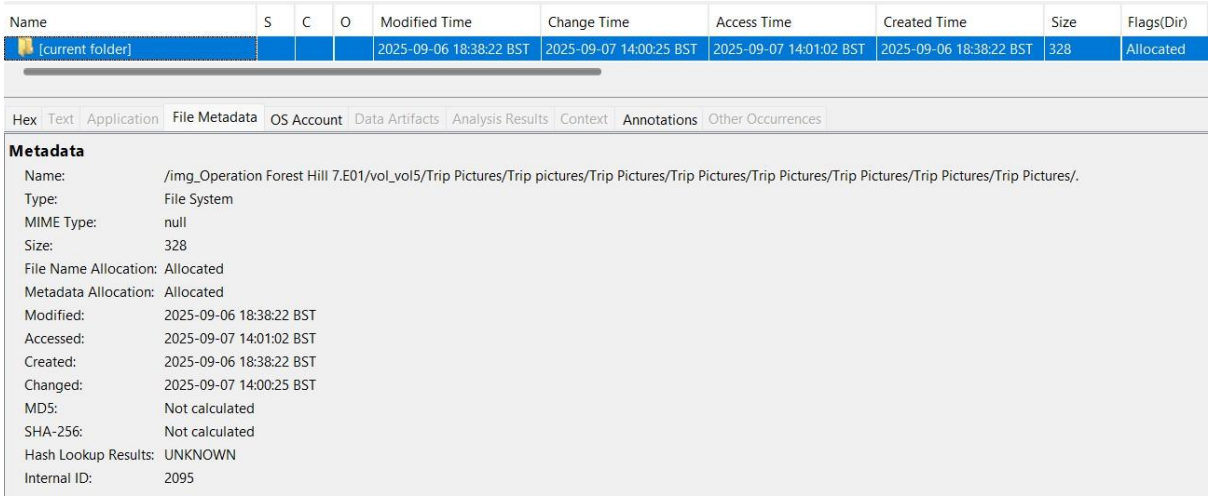
Result / Aftermath phase	

Artefact 14: <Trip Pictures >

A nested folder chain ("Trip Pictures / Trip Pictures / …") that buries key files eight levels deep. This directory design was used to frustrate quick discovery and represents logical obfuscation of file paths rather than encryption.

Location: / /img_Operation Forest Hill 7.E01/vol_vol5/Trip Pictures/Trip Pictures/Trip Pictures

Meta-Data of the artefact:



Implications of the Artefact:

The recovered Artefact 14, a folder named "trips Pictures", contained several nested subfolders, each leading to additional directories. This structure suggests intentional obfuscation of file paths to make the actual content more difficult to locate or identify.

The arrangement may indicate an effort to conceal information by requiring multiple levels of navigation before reaching the true files.

Method to hide/unhide artefact:

The artefact was hidden by creating multiple nested folders with generic or misleading names, effectively disguising the final file location. This approach relies on directory complexity rather than encryption.

The type of Artefact:

Obfuscation of file and/or path name.

Artefact Detail Table:

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

Artefact 15: INTERNAL SERVER_extract_2025-09-05

The principal encrypted archive containing exfiltrated Organization X data. Once decrypted using the reconstructed passphrase, it revealed sensitive R&D and client datasets identical to the material leaked online. This is the core evidential artefact proving data theft.

Location: /img_Operation Forest Hill 7.E01/vol1_vol5/Trip Pictures//Trip Pictures//Trip Pictures//Trip Pictures//Trip Pictures//Trip Pictures//Trip Pictures//Trip Pictures/ZYNSRV04_extract_2025-09-05

ZYN-SRV04_extract_2025-09-05			2025-09-06 18:38:22 BST	2025-09-07 14:00:32 BST	2025-09-06 18:38:22 BST	2025-09-06

Item: ZYN-SRV04_extract_2025-09-05
Aggregate Score: Likely Notable

Analysis Result 1

Score:	Likely Notable
Type:	Encryption Suspected
Configuration:	
Conclusion:	
Justification:	Suspected encryption due to high entropy (7.999990).
Comment:	Suspected encryption due to high entropy (7.999990).

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

Strings | Extracted Text | Translation

Page: 1 of 1280 Page Go to Page:

```
!c6t
g]e
}U9[
Fs,k
m.?G
_(nEX
X^y7
"8!ok)
[Trx
G4IJ
 d5t
lv uz
Z~@I
m,qaNF
)0=V
);KY+ si
-+7J
tcD=
```

Meta-Data of the artefact:

ZYN-SRV04_extract_2025-09-05		7	2025-09-06 18:38:22 BST	2025-09-07 14:00:32 BST	2025-09-06 18:38:22 BST	2025-09-06 18:38:22 BST	20971520	Allocated	Allocated

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

Metadata

Name:	/img_Operation Forest Hill 7.E01/vol_vol5/Trip Pictures/Trip pictures/Trip Pictures/Trip Pictures/Trip Pictures/Trip Pictures/Trip Pictures/Trip Pictures/ZYN-SRV04_extract_2025-09-05
Type:	File System
MIME Type:	application/octet-stream
Size:	20971520
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2025-09-06 18:38:22 BST
Accessed:	2025-09-06 18:38:22 BST
Created:	2025-09-06 18:38:22 BST
Changed:	2025-09-07 14:00:32 BST
MD5:	99cd5cbeac4875eda4be468f45f967d7
SHA-256:	b5de94c021047de7cfb83f493fa653912a9b77a74bfa24e7c9640938ffb08707
Hash Lookup Results:	UNKNOWN
Internal ID:	2099

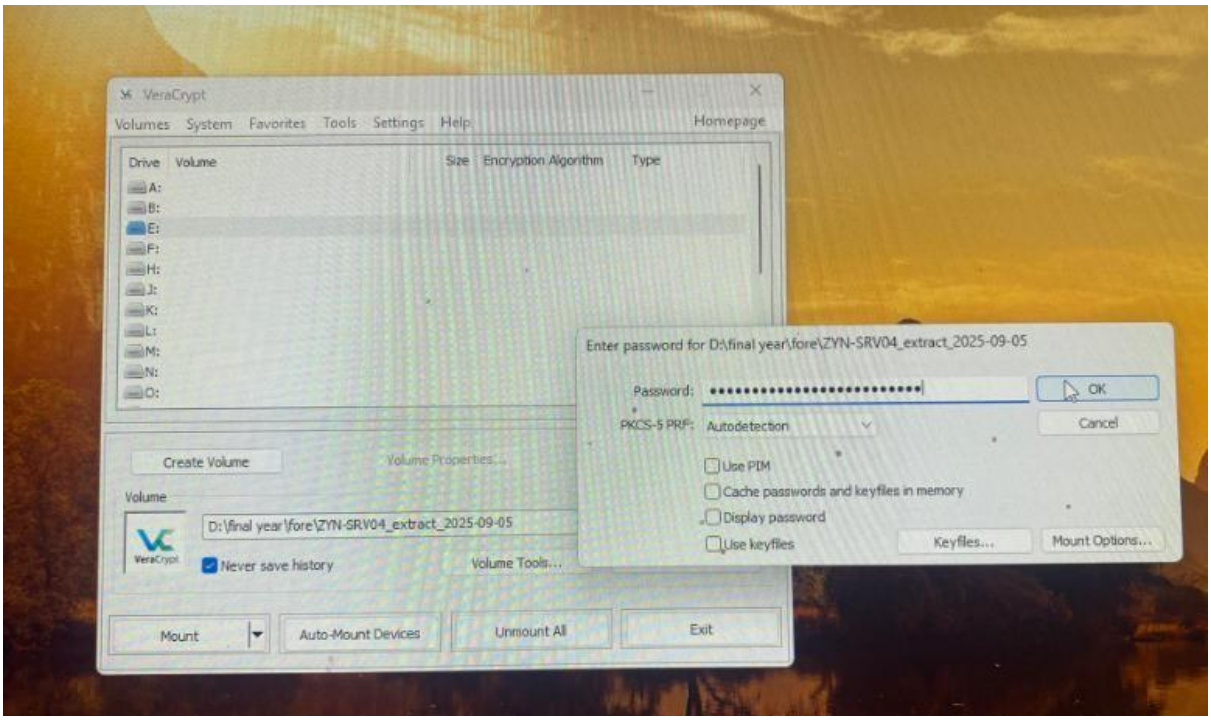
Implications of the Artefact:

Artefact 15, titled “INTERNAL SERVER_extract_2025-09-05”, was located within one of the nested folders inside the **“trips Pictures”** directory (refer **to Artefact 14**

Obfuscated Folder Path). The file name references the compromised server **INTERNAL SERVER**, aligning with the data extraction timeline from the investigation. The artefact was found to be **encrypted and marked with the hidden attribute**, suggesting deliberate concealment to prevent unauthorised access. The presence of related **VeraCrypt** artefacts and supporting image files indicates purposeful encryption to secure or hide sensitive content.

Method to hide/unhide artefact:

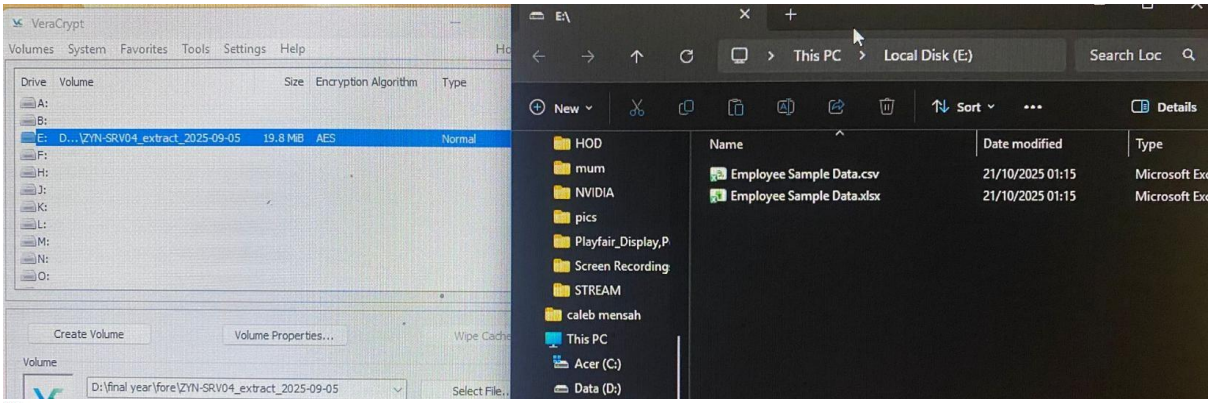
The file was intentionally encrypted and stored within a VeraCrypt volume to prevent unauthorized access. Artefacts indicating the installation of VeraCrypt, along with image files potentially containing encryption credentials, point to deliberate efforts to secure the data. Notably, the password "**silver-cedar-echo-quietly**" extracted from the image file '**Office Presentation.pptx' was** instrumental in decrypting the volume and recovering the previously inaccessible **INTERNAL SERVER**' file. This demonstrates a high level of operational security and sophistication in concealing sensitive information.



INTERNAL SERVER After decryption

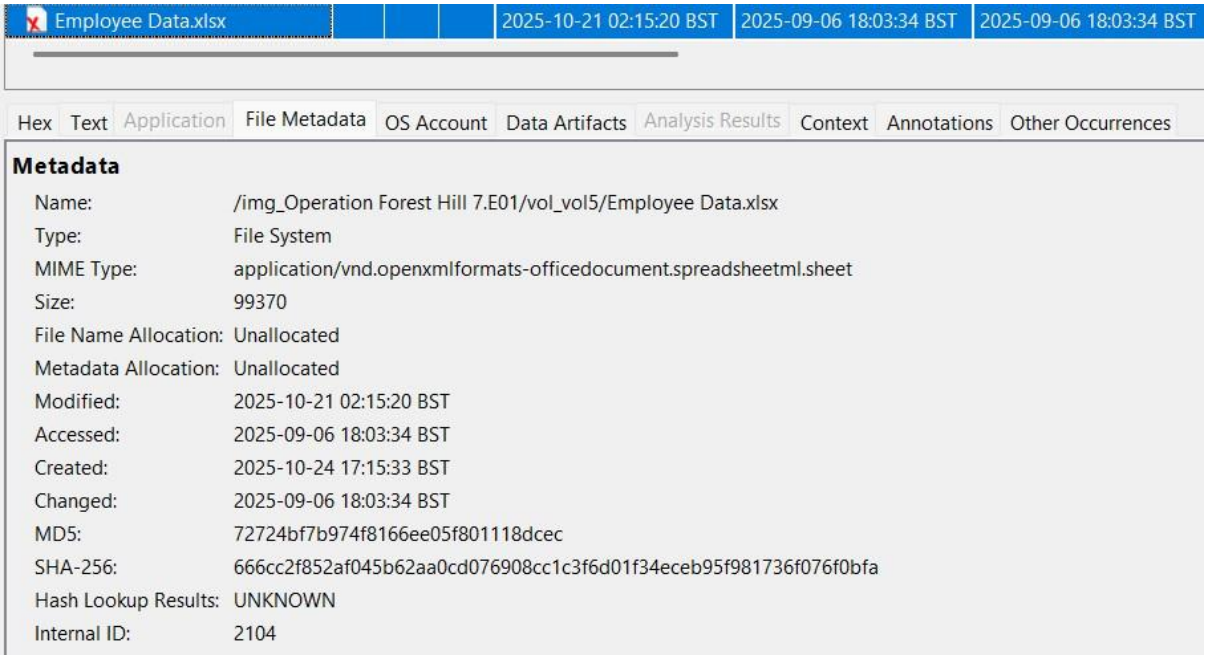
After decryption, the file revealed **sensitive company data**, including employee names, financial details, and departmental information, confirming that the file contained **confidential internal records** from Organization X's systems. This

demonstrates deliberate encryption and concealment of proprietary data outside authorised storage.



EEID	Full Name	Job Title	Department	Business Unit	Gender	Ethnicity	Age	Hire Date	Annual Salary	Bonus %	Country	City	Exit Date
E02387	Emily Davis	Sr. Manger	IT	Research & Development	Female	Black	55	4/8/16	$141,604	15%	United States	Seattle	10/16/21
E04105	Theodore Dinh	Technical Architect	IT	Manufacturing	Male	Asian	59	11/29/97	$99,975	0%	China	Chongqing	
E02572	Luna Sanders	Director	Finance	Speciality Products	Female	Caucasian	50	10/26/06	$163,099	20%	United States	Chicago	
E02832	Penelope Jordan	Computer Systems Manager	IT	Manufacturing	Female	Caucasian	26	9/27/19	$84,913	7%	United States	Chicago	
E01639	Austin Vo	Sr. Analyst	Finance	Manufacturing	Male	Asian	55	11/20/95	$95,409	0%	United States	Phoenix	
E00644	Joshua Gupta	Account Representative	Sales	Corporate	Male	Asian	57	1/24/17	$50,994	0%	China	Chongqing	
E01550	Ruby Barnes	Manager	IT	Corporate	Female	Caucasian	27	7/1/20	$119,746	10%	United States	Phoenix	
E04332	Luke Martin	Analyst	Finance	Manufacturing	Male	Black	25	5/16/20	$41,336	0%	United States	Miami	5/20/21
E04533	Easton Bailey	Manager	Accounting	Manufacturing	Male	Caucasian	29	1/25/19	$113,527	6%	United States	Austin	
E03838	Madeline Walker	Sr. Analyst	Finance	Speciality Products	Female	Caucasian	34	6/13/18	$77,203	0%	United States	Chicago	
E00591	Savannah Ali	Sr. Manger	Human Resources	Manufacturing	Female	Asian	36	2/11/09	$157,333	15%	United States	Miami	
E03344	Camila Rogers		Controls Engineer	Engineering	Speciality Products	Female	Caucasian	27	10/21/21	$109,851	0%	United States	Seattle
E00530	Eli Jones	Manager	Human Resources	Manufacturing	Male	Caucasian	59	3/14/99	$105,086	9%	United States	Austin	
E04239	Everleigh Ng	Sr. Manger	Finance	Research & Development	Female	Asian	51	6/10/21	$146,742	10%	China	Shanghai	
E03496	Robert Yang	Sr. Analyst	Accounting	Speciality Products	Male	Asian	31	11/4/17	$97,078	0%	United States	Austin	3/9/20
E00549	Isabella Xi	Vice President		Marketing	Research & Development	Female	Asian	41	3/13/13	$249,270	30%	United States	Seattle
E00163	Bella Powell	Director	Finance	Research & Development	Female	Black	65	3/4/02	$175,837	20%	United States	Phoenix	
E00884	Camila Silva	Sr. Manger	Marketing	Speciality Products	Female	Latino	64	12/1/03	$154,828	13%	United States	Seattle	
E04116	David Barnes	Director	IT	Corporate	Male	Caucasian	64	11/3/13	$186,503	24%	United States	Columbus	
E04625	Adam Dang	Director	Sales	Research & Development	Male	Asian	45	7/9/02	$166,331	18%	China	Chongqing	
E03680	Elias Alvarado		Sr. Manger	IT	Manufacturing	Male	Latino	56	1/9/12	$146,140	10%	Brazil	Manaus
E04732	Eva Rivera	Director	Sales	Manufacturing	Female	Latino	36	4/2/21	$151,703	21%	United States	Miami	
E03484	Logan Rivera	Director	IT	Research & Development	Male	Latino	59	5/24/02	$172,787	28%	Brazil	Rio de Janerio	
E00671	Leonardo Dixon		Analyst	Sales	Speciality Products	Male	Caucasian	37	9/5/19	$49,998	0%	United States	Seattle
E02071	Mateo Her	Vice President		Sales	Speciality Products	Male	Asian	44	3/2/14	$207,172	31%	China	Chongqing
E02206	Jose Henderson		Director	Human Resources	Speciality Products	Male	Black	41	4/17/15	$152,239	23%	United States	Columbus
E04545	Abigail Mejia	Quality Engineer		Engineering	Corporate	Female	Latino	56	2/5/05	$98,581	0%	Brazil	Rio de Janerio
E00154	Wyatt Chin	Vice President		Engineering	Speciality Products	Male	Asian	43	6/7/04	$246,231	31%	United States	Seattle
E03343	Carson Lu	Engineering Manager		Engineering	Speciality Products	Male	Asian	64	12/4/96	$99,354	12%	China	Beijing
E00304	Dylan Choi	Vice President		IT	Corporate	Male	Asian	63	5/11/12	$231,141	34%	China	Beijing
E02594	Ezekiel Kumar		IT Coordinator	IT	Research & Development	Male	Asian	28	6/25/17	$54,775	0%	United States	Columbus
E00402	Dominic Guzman		Analyst	Finance	Manufacturing	Male	Latino	65	5/16/04	$55,499	0%	Brazil	Manaus
E01994	Angel Powell	Analyst II		Sales	Research & Development	Male	Caucasian	61	7/11/08	$66,521	0%	United States	Seattle
E03549	Mateo Vu	Account Representative		Sales	Speciality Products	Male	Asian	30	9/29/16	$59,100	0%	China	Chongqing
E03247	Caroline Jenkins		Analyst	Finance	Research & Development	Female	Caucasian	27	5/6/18	$49,011	0%	United States	Chicago
E02074	Nora Brown	Enterprise Architect		IT	Manufacturing	Female	Caucasian	32	2/11/14	$99,575	0%	United States	Austin
E04152	Adeline Huang		Controls Engineer	Engineering	Manufacturing	Female	Asian	34	12/16/19	$99,989	0%	China	Chengdu
E01628	Jackson Perry	Vice President		Marketing	Research & Development	Male	Caucasian	27	10/20/19	$256,420	30%	United States	Phoenix
E04285	Riley Padilla	Technical Architect		IT	Manufacturing	Female	Latino	35	5/15/13	$78,940	0%	United States	Miami
E01417	Leah Pena	Enterprise Architect		IT	Corporate	Female	Latino	57	1/3/94	$82,872	0%	Brazil	Manaus
E01754	Owen Lam	Sr. Business Partner		Human Resources	Speciality Products	Male	Asian	30	5/29/17	$86,317	0%	China	Chengdu	7/16/17
E03749	Kennedy Foster		Manager	Marketing	Speciality Products	Female	Caucasian	53	11/23/13	$113,135	5%	United States	Austin
E03574	John Moore	Vice President		IT	Speciality Products	Male	Caucasian	52	11/8/05	$199,808	32%	United States	Seattle
E04600	William Vu	Account Representative		Sales	Speciality Products	Male	Asian	37	11/14/13	$56,037	0%	China	Shanghai
E00586	Sadie Washington		Sr. Manger	Marketing	Research & Development	Female	Caucasian	29	5/24/19	$122,350	12%	United States	Phoenix
E03538	Gabriel Holmes		Enterprise Architect	IT	Research & Development	Male	Caucasian	40	11/4/10	$92,952	0%	United States	Seattle
E02185	Wyatt Rojas	Computer Systems Manager		IT	Corporate	Male	Latino	32	3/20/13	$79,921	5%	United States	Austin
E03830	Eva Coleman	Director	IT	Research & Development	Female	Black	37	9/20/09	$167,199	20%	United States	Seattle	
E03720	Dominic Clark		Quality Engineer	Engineering	Research & Development	Male	Caucasian	52	10/17/12	$71,476	0%	United States	Phoenix
E03025	Lucy Alexander		Director	Engineering	Manufacturing	Female	Caucasian	45	10/29/14	$189,420	20%	United States	Seattle
E04917	Everleigh Washington		HRIS Analyst	Human Resources	Research & Development	Female	Caucasian	64	10/20/01	$64,057	0%	United States	Phoenix
E00415	Leilani Butler	Analyst II		Marketing	Manufacturing	Female	Black	27	9/21/21	$68,728	0%	United States	Phoenix
E02862	Peyton Huang		Sr. Manger	IT	Manufacturing	Female	Asian	25	7/2/21	$125,633	11%	China	Beijing
E04207	John Contreras		Analyst II	Marketing	Manufacturing	Male	Latino	35	5/15/11	$66,889	0%	United States	Columbus

Metadata



The type of Artefact:

Encrypted Password protected container

Artefact Detail Table:

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

Artefact 16: <Most Recently Used (MRU)

Registry records show that *transfer.png* and the encrypted container were opened shortly before the deletion phase. MRUs confirm active user interaction with critical files.

Edward Lewis › Recent

Name	Date modified	Type	Size
anonymous_reply_2024-08-16_001.eml	9/7/2025 10:51 AM	Shortcut	1 KB
EML	9/7/2025 10:51 AM	Shortcut	1 KB
sent_2025-09-02_001.eml	9/7/2025 10:43 AM	Shortcut	1 KB
The Internet	9/7/2025 10:30 AM	Shortcut	1 KB
chat 5.jpg	9/7/2025 10:30 AM	Shortcut	1 KB
My Pictures	9/7/2025 10:30 AM	Shortcut	1 KB
chat 1.png	9/7/2025 10:21 AM	Shortcut	1 KB
Personal	9/6/2025 9:27 PM	Shortcut	1 KB

Edward Lewis › Recent

Name	Date modified	Type	Size
Personal	9/6/2025 9:27 PM	Shortcut	1 KB
transfer.png	9/6/2025 9:27 PM	Shortcut	1 KB
img_0363 (4).png	9/6/2025 6:06 PM	Shortcut	1 KB
call logs.png	9/6/2025 6:03 PM	Shortcut	1 KB
Office Presentation.pptx	9/6/2025 6:02 PM	Shortcut	2 KB
Trip Pictures	9/6/2025 6:02 PM	Shortcut	2 KB
Office work.txt	9/6/2025 5:56 PM	Shortcut	1 KB
B1.png	9/6/2025 5:55 PM	Shortcut	1 KB
A1.png	9/6/2025 5:50 PM	Shortcut	1 KB
Important Server.docx	9/6/2025 5:40 PM	Shortcut	1 KB
Work	9/6/2025 5:40 PM	Shortcut	1 KB
Employee Data.xlsx	9/6/2025 5:38 PM	Shortcut	1 KB
Local Disk (X:)	9/6/2025 5:38 PM	Shortcut	1 KB
Employee Data.csv	9/6/2025 5:38 PM	Shortcut	1 KB
Softwares	9/6/2025 5:05 PM	Shortcut	1 KB
Local Disk (E:)	9/6/2025 5:05 PM	Shortcut	1 KB
Local Disk (E:)	9/6/2025 5:05 PM	Shortcut	1 KB
This PC	9/6/2025 5:05 PM	Shortcut	1 KB
57649.mp4	9/4/2025 7:10 PM	Shortcut	1 KB
Videos	9/4/2025 7:10 PM	Shortcut	1 KB
HxD	9/3/2025 4:39 PM	Shortcut	1 KB
readme.txt	9/3/2025 4:39 PM	Shortcut	1 KB
5-30.jpg	9/3/2025 4:37 PM	Shortcut	1 KB
300x600.html	9/2/2025 4:36 PM	Shortcut	2 KB
checksum - Zip file to verify if not modifi...	9/2/2025 4:36 PM	Shortcut	1 KB
checksum - Zip file to verify if not modifi...	9/2/2025 4:36 PM	Shortcut	1 KB
Documents	9/2/2025 4:36 PM	Shortcut	1 KB
research.png	9/1/2025 3:03 PM	Shortcut	1 KB

Meta-Data of the artefact:

N/A

Implications of the Artefact:

The presence of transfer.png in the MRU list confirms that the file was actively opened or previewed on the system. This supports user interaction with the image during the timeframe of interest, linking file activity to the user profile. MRU entries provide strong evidence of file awareness and access, even if the files were later deleted or moved.

Method to hide/unhide artefact:

MRU paths are typically not hidden and are a part of the system's way of tracking recently accessed files. **The type of Artefact**

Most Recently Used (MRU)

Artefact Detail Table

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

Artefact 17: Link File Recent Activity

Shortcut artefacts in the “Recent” directory reveal access to *VeraCrypt* and related email messages. These provide a temporal link between the suspect’s profile and the concealed data.

Location: /img_Operation Forest Hill 7.E01/vol1_vol9/$CrvedFiles/7/f1287864.lnk

f1287864.lnk			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	778	Unallocated	Unallocated	unknown
f1471680.lnk			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	227	Unallocated	Unallocated	unknown
f1592584.lnk			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1302	Unallocated	Unallocated	unknown
f1732576.lnk			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1578	Unallocated	Unallocated	unknown
f1732584.lnk			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	227	Unallocated	Unallocated	unknown
f1833306.txt			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	300	Unallocated	Unallocated	unknown
f1866852.lnk			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	345	Unallocated	Unallocated	unknown
f1891244.lnk			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	196955	Unallocated	Unallocated	unknown
f1915068.lnk			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	361	Unallocated	Unallocated	unknown

Meta-Data of the artefact:

Metadata

Name:	/img_COMP-1812_MIDR-2025-007-EVID-01_Win10_2025.E01/vol_vol9/$CarvedFiles/7/f1287864.lnk
Type:	Carved
MIME Type:	application/octet-stream
Size:	778
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

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

/E:\
MailArchiveH
MailArchive
EML8
anonymous_reply_2024-08-16_001.eml
anonymous_reply_2024-08-16_001.eml
Local DiskE:\MailArchive\EML\anonymous_reply_2024-08-16_001.eml
E:\MailArchive\EML`
desktop-vc5gi52

Implications of the Artefact:

The recovered Artefact 17 consists of link (shortcut) files located in the user’s Recent directory under User A. These files record recently accessed documents, including: anonymous_relpy_2024-8-16_001.eml, VeraCrypt, etc. The presence of these links confirms that these files were actively accessed or opened by the user account, reinforcing the association between the suspect’s activity and the relevant artefacts identified during the investigation.

Method to hide/unhide artefact:

Link files are automatically generated by the Windows operating system when files are opened. They are not manually hidden but can be deleted or wiped to obscure user

activity. In Autopsy, they were recovered under the Recent Activity module, which reconstructs file access history from **.lnk data.**

The type of Artefact

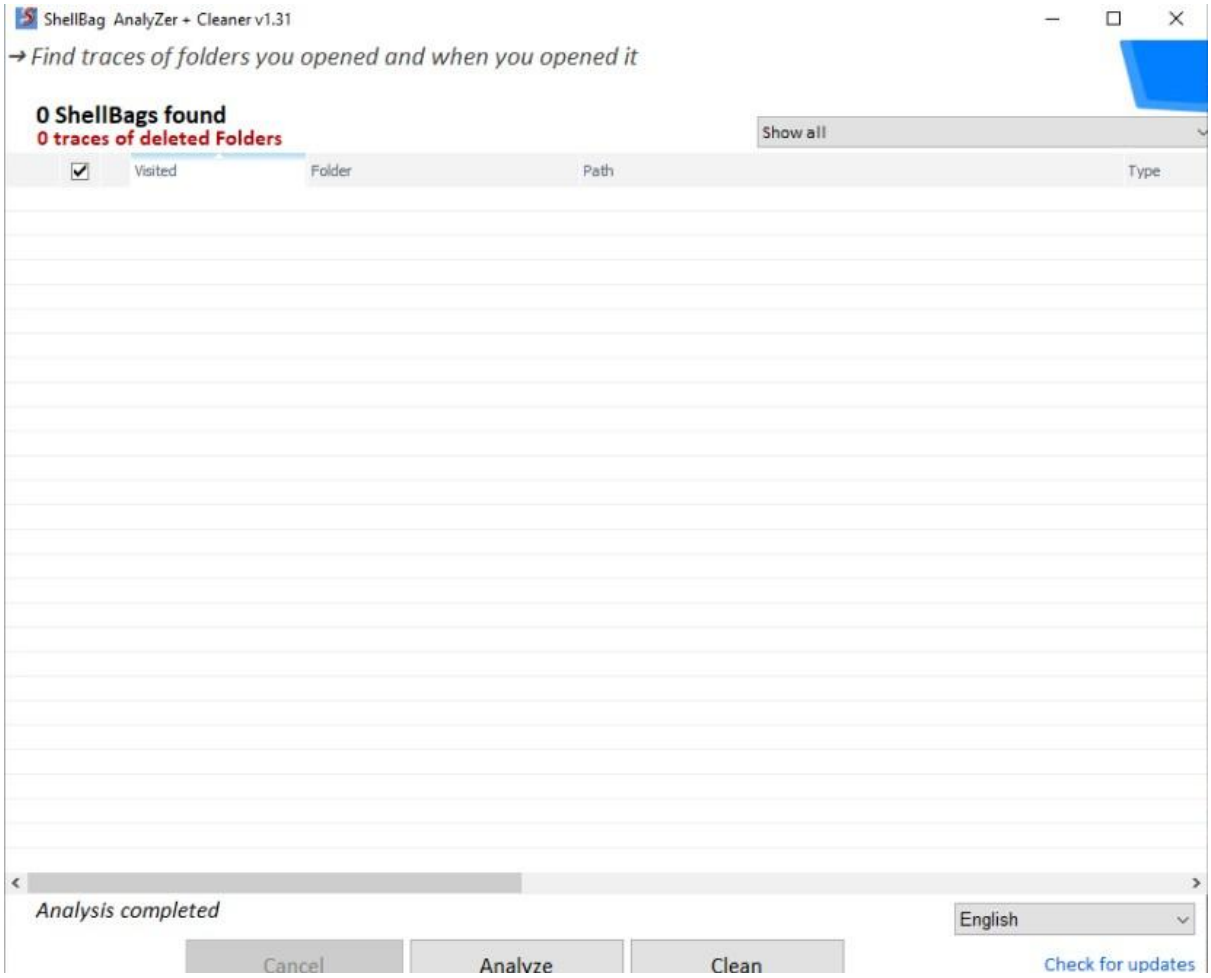
Link File Recent Activity

Artefact Detail Table

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

Artefact 18 : shellbag Analyzer

The absence of shellbag entries for certain directories suggests that folder-access history was manually wiped using system-cleaning tools. Such absence, in a forensic context, indicates deliberate anti-forensic activity.



Meta-Data of the artefact:

N/A

Implications of the Artefact:

The **Artefact 18**, analysed using **ShellBag Analyzer**, revealed **no shellbag entries** or folder access traces. This absence can indicate that **system cleaning utilities or manual deletion** were used to erase Windows Explorer folder history. Such an absence is noteworthy in forensic analysis, as it may reflect **intentional efforts to remove evidence** of folder navigation or file access.

Method to hide/unhide artefact:

Shellbags are automatically created by Windows to record folder view settings and access times. If deleted, they cannot be directly “unhidden,”

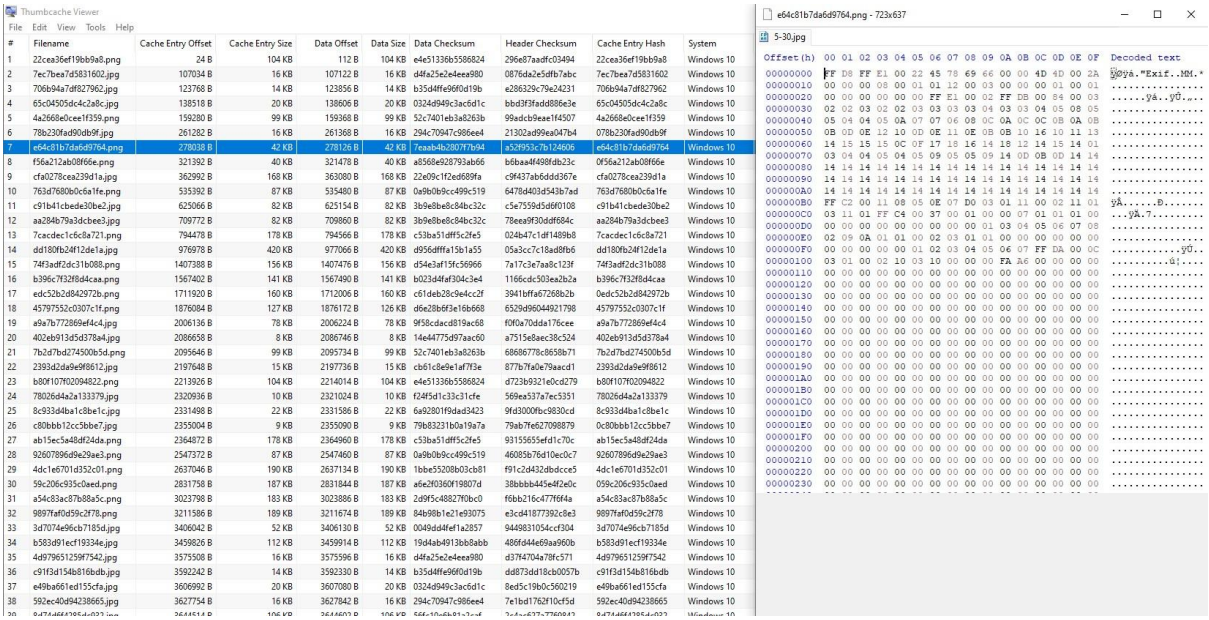
The type of Artefact

Shellbags – MRU for folders

Artefact Detail Table

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

Artefact 19: Thumbcache / Thumbs.db



#	Filename	Cache Entry Offset	Cache Entry Size	Data Offset	Data Size	Data Checksum	Header Checksum	Cache Entry Hash	System
1	22cea36ef19bb9a8.png	24 B	104 KB	112 B	104 KB	e4e51336b5586824	296e87aadfc03494	22cea36ef19bb9a8	Windows 10
2	7ec7bea7d5831602.jpg	107034 B	16 KB	107122 B	16 KB	d4fa25e2e4eea980	0876da2e5dfb7abc	7ec7bea7d5831602	Windows 10
3	706b94a7df827962.jpg	123768 B	14 KB	123856 B	14 KB	b35d4ffe96f0d19b	e286329c79e24231	706b94a7df827962	Windows 10
4	65c04505dc4c2a8c.jpg	138518 B	20 KB	138606 B	20 KB	0324d949c3ac6d1c	bbd3f3fadd886e3e	65c04505dc4c2a8c	Windows 10
5	4a2668e0cee1f359.png	159280 B	99 KB	159368 B	99 KB	52c7401eb3a8263b	99adcb9eae1f4507	4a2668e0cee1f359	Windows 10
6	78b230fad90db9f.jpg	261282 B	16 KB	261368 B	16 KB	294c70947c986ee4	21302ad99ea047b4	078b230fad90db9f	Windows 10
7	e64c81b7da6d9764.png	278038 B	42 KB	278126 B	42 KB	7eaab4b2807f7b94	a52f953c7b124606	e64c81b7da6d9764	Windows 10
8	f56a212ab08f66e.png	321392 B	40 KB	321478 B	40 KB	a8568e928793ab66	b6baa4f498fdb23c	0f56a212ab08f66e	Windows 10
9	cfa0278cea239d1a.jpg	362992 B	168 KB	363080 B	168 KB	22e09c1f2ed689fa	c9f437ab6ddd367e	cfa0278cea239d1a	Windows 10
10	763d7680b0c6a1fe.png	535392 B	87 KB	535480 B	87 KB	0a9b0b9cc499c519	6478d403d543b7ad	763d7680b0c6a1fe	Windows 10
11	c91b41cbede30be2.jpg	625066 B	82 KB	625154 B	82 KB	3b9e8be8c84bc32c	c5e7559d5d6f0108	c91b41cbede30be2	Windows 10
12	aa284b79a3dcbee3.jpg	709772 B	82 KB	709860 B	82 KB	3b9e8be8c84bc32c	78eea9f30ddf684c	aa284b79a3dcbee3	Windows 10
13	7cacdec1c6c8a721.png	794478 B	178 KB	794566 B	178 KB	c53ba51dff5c2fe5	024b47c1df1489b8	7cacdec1c6c8a721	Windows 10
14	dd180fb24f12de1a.jpg	976978 B	420 KB	977066 B	420 KB	d956dfffa15b1a55	05a3cc7c18ad8fb6	dd180fb24f12de1a	Windows 10
15	74f3adf2dc31b088.png	1407388 B	156 KB	1407476 B	156 KB	d54e3af15fc56966	7a17c3e7aa8c123f	74f3adf2dc31b088	Windows 10
16	b396c7f32f8d4caa.png	1567402 B	141 KB	1567490 B	141 KB	b023d4faf304c3e4	1166cdc503ea2b2a	b396c7f32f8d4caa	Windows 10
17	edc52b2d842972b.png	1711920 B	160 KB	1712006 B	160 KB	c61deb28c9e4cc2f	3941bffa67268b2b	0edc52b2d842972b	Windows 10
18	45797552c0307c1f.png	1876084 B	127 KB	1876172 B	126 KB	d6e28b6f3e16b668	6529d96044921798	45797552c0307c1f	Windows 10
19	a9a7b772869ef4c4.jpg	2006136 B	78 KB	2006224 B	78 KB	9f58cdacd819ac68	f0f0a70ddad176cee	a9a7b772869ef4c4	Windows 10
20	402eb913d5d378a4.jpg	2086658 B	8 KB	2086746 B	8 KB	14e44775d97aac60	a7515e8aec38c524	402eb913d5d378a4	Windows 10
21	7b2d7bd274500b5d.png	2095646 B	99 KB	2095734 B	99 KB	52c7401eb3a8263b	68686778c8658b71	7b2d7bd274500b5d	Windows 10
22	2393d2da9e9f8612.jpg	2197648 B	15 KB	2197736 B	15 KB	cb61c8e9e1af7f3e	877b7fa0e79aacd1	2393d2da9e9f8612	Windows 10
23	b80f107f02094822.png	2213926 B	104 KB	2214014 B	104 KB	e4e51336b5586824	d723b9321e0cd279	b80f107f02094822	Windows 10
24	78026d4a2a133379.jpg	2320936 B	10 KB	2321024 B	10 KB	f24f5d1c33c31cfe	569ea537a7ec5351	78026d4a2a133379	Windows 10
25	8c933d4ba1c8be1c.jpg	2331498 B	22 KB	2331586 B	22 KB	6a92801f9dad3423	9fd3000fbc9830cd	8c933d4ba1c8be1c	Windows 10
26	c80bbb12cc5bbe7.jpg	2355004 B	9 KB	2355090 B	9 KB	79b83231b0a19a7a	79ab7fe627098879	0c80bbb12cc5bbe7	Windows 10
27	ab15ec5a48df24da.png	2364872 B	178 KB	2364960 B	178 KB	c53ba51dff5c2fe5	93155655efd1c70c	ab15ec5a48df24da	Windows 10
28	92607896d9e29ae3.png	2547372 B	87 KB	2547460 B	87 KB	0a9b0b9cc499c519	46085b76d10ec0c7	92607896d9e29ae3	Windows 10
29	4dc1e6701d352c01.png	2637046 B	190 KB	2637134 B	190 KB	1bbe55208b03cb81	f91c2d432dbddce5	4dc1e6701d352c01	Windows 10
30	59c206c935c0aed.png	2831758 B	187 KB	2831844 B	187 KB	a6e2f0360f19807d	38bbbb445e4f2e0c	059c206c935c0aed	Windows 10
31	a54c83ac87b88a5c.png	3023798 B	183 KB	3023886 B	183 KB	2d9f5c48827f0bc0	f6bb216c477f6f4a	a54c83ac87b88a5c	Windows 10
32	9897faf0d59c2f78.png	3211586 B	189 KB	3211674 B	189 KB	84b98b1e21e93075	e3cd41877392c8e3	9897faf0d59c2f78	Windows 10
33	3d7074e96cb7185d.jpg	3406042 B	52 KB	3406130 B	52 KB	0049dd4fef1a2857	9449831054ccf304	3d7074e96cb7185d	Windows 10
34	b583d91ecf19334e.jpg	3459826 B	112 KB	3459914 B	112 KB	19d4ab4913bb8abb	486fd44e69aa960b	b583d91ecf19334e	Windows 10
35	4d979651259f7542.jpg	3575508 B	16 KB	3575596 B	16 KB	d4fa25e2e4eea980	d37f4704a78fc571	4d979651259f7542	Windows 10
36	c91f3d154b816bdb.jpg	3592242 B	14 KB	3592330 B	14 KB	b35d4ffe96f0d19b	dd873dd18cb0057b	c91f3d154b816bdb	Windows 10
37	e49ba661ed155cfa.png	3606992 B	20 KB	3607080 B	20 KB	0324d949c3ac6d1c	8ed5c19b0c560219	e49ba661ed155cfa	Windows 10
38	592ec40d94238665.jpg	3627754 B	16 KB	3627842 B	16 KB	294c70947c986ee4	7e1bd1762f10cf5d	592ec40d94238665	Windows 10

Meta-Data of the artefact:

N/A

Implications of the Artefact:

The recovered **Artefact 19** consists of thumbnail cache entries extracted from **Thumbcache Viewer**, which included cached images such as **"5-30.jpg."** The presence of these thumbnails confirms that the file was **previously viewed or accessed** on the system, even if the original file had been moved, deleted, or altered. This provides supporting evidence of user interaction with concealed or manipulated files, reinforcing file-access continuity in the investigation timeline.

Method to hide/unhide artefact:

Thumbnail cache files (thumbcache_*.db) are automatically generated by Windows to store preview images of files viewed in Explorer.

These caches are typically hidden system files, not visible during normal browsing. They can be extracted and analysed to recover image previews and confirm prior access to specific media files, even after deletion or renaming.

The type of Artefact

Thumbcache / Thumbs.db

Recovered thumbnail previews of *5-30.jpg* and *A1.png* confirm that the images were viewed on the system, even if deleted or renamed later. This supports continuity of user awareness.

Artefact Detail Table

Artefact is	**Tick Appropriate**
Application Level	
OS Level	X
File System Level	

Reconnaissance / Research phase	
Recording phase	X
Result / Aftermath phase	

Artefact 20: Registry Information

Entries show installation of *VeraCrypt*, *HxD Hex Editor*, and *Kill Disk*. These applications correspond exactly to the concealment and wiping activities evidenced elsewhere, proving that the suspect possessed the technical means to perform encryption and data destruction.

Installed software

application/x-dosexec 187 Results

Table Thumbnail Summary

Page: 1 of 1 Pages: Go to Page: Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
HxD.exe			0	2021-02-10 22:20:12 GMT	2025-09-03 17:39:38 BST	2025-09-07 12:39:39 BST	2025-09-03 17:39:37 BST	6905856	Allocated	Allocated	unknown	/img_COMP-1812_MIDR-2025-
unins000.exe			0	2025-09-03 17:38:56 BST	2025-09-03 17:39:37 BST	2025-09-07 11:53:10 BST	2025-09-03 17:39:37 BST	1209553	Allocated	Allocated	unknown	/img_COMP-1812_MIDR-2025-
$RJ93KH7.exe			0	2025-09-06 18:04:57 BST	2025-09-07 12:38:15 BST	2025-09-07 12:39:29 BST	2025-09-06 18:05:49 BST	40643880	Allocated	Allocated	unknown	/img_COMP-1812_MIDR-2025-
$RPF5CWR.exe			0	2025-09-06 18:05:49 BST	2025-09-07 12:38:15 BST	2025-09-07 12:39:28 BST	2025-09-06 18:05:49 BST	5599976	Allocated	Allocated	unknown	/img_COMP-1812_MIDR-2025-
unins000.exe			0	2025-09-06 18:33:29 BST	2025-09-06 18:33:56 BST	2025-09-06 18:34:04 BST	2025-09-06 18:33:56 BST	730216	Allocated	Allocated	unknown	/img_COMP-1812_MIDR-2025-
ISOtoUSB.exe			0	2017-10-25 09:08:44 BST	2025-09-06 18:34:00 BST	2025-09-06 18:34:04 BST	2025-09-06 18:34:00 BST	242720	Allocated	Allocated	unknown	/img_COMP-1812_MIDR-2025-
BootDiskCreator.exe			0	2021-12-22 17:11:04 GMT	2025-09-06 18:34:02 BST	2025-09-06 18:36:48 BST	2025-09-06 18:33:58 BST	4395624	Allocated	Allocated	unknown	/img_COMP-1812_MIDR-2025-
InitFlash.exe			0	2021-04-07 09:21:28 BST	2025-09-06 18:33:59 BST	2025-09-06 18:36:51 BST	2025-09-06 18:33:59 BST	3211776	Allocated	Allocated	unknown	/img_COMP-1812_MIDR-2025-
KillDisk.exe			0	2021-11-10 10:30:52 GMT	2025-09-06 18:34:02 BST	2025-09-07 11:58:45 BST	2025-09-06 18:33:56 BST	8947816	Allocated	Allocated	unknown	/img_COMP-1812_MIDR-2025-
$RWELLWF.exe			0	2025-09-06 18:05:49 BST	2025-09-07 12:38:15 BST	2025-09-07 12:39:29 BST	2025-09-06 18:05:49 BST	6157536	Allocated	Allocated	unknown	/img_COMP-1812_MIDR-2025-

Implications of the Artefact:

The presence of these applications indicates the system user installed and potentially executed forensic, encryption, and data wiping tools.

Utilities such as VeraCrypt suggest deliberate encryption activities, while HxD and KillDisk indicate possible manipulation or destruction of data.

This supports the inference that software was intentionally deployed to conceal, encrypt, or erase digital evidence, directly relevant to the case's exfiltration and antiforensics behaviour.

Method to hide/unhide artefact:

Installed software information can be hidden from normal users by:

- Deleting installation directories or shortcuts.
- Editing or removing related registry entries under

The type of Artefact

Registry Information – various things such as username, password and hint, installed software

Artefact Detail Table

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

Artefact 21: INTERNAL SERVER_extract_2025-09-05(Unallocated space)

A deleted copy of the same encrypted archive reconstructed from raw sectors. This shows attempted wiping after exfiltration and links the deleted copy to the active one through identical hashes.

ZYN-SRV04_extract_2025-09-05				2025-09-06 18:38:22 BST	2025-09-07 14:00:32 BST	2025-09-06 18:38:22 BST	2025-09-06

Meta-Data of the artefact:

ZYN-SRV04_extract_2025-09-05		7	2025-09-06 18:38:22 BST	2025-09-07 14:00:32 BST	2025-09-06 18:38:22 BST	2025-09-06 18:38:22 BST	20971520

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

Metadata

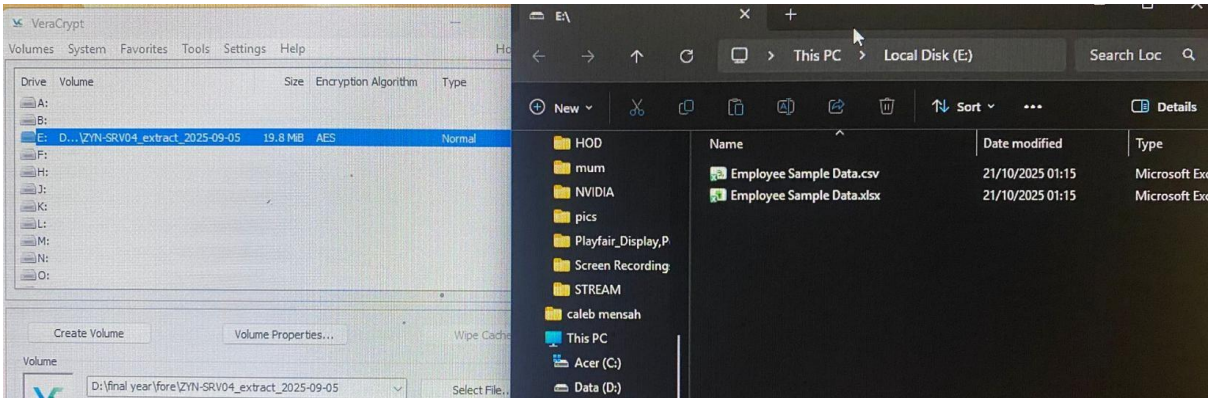
Name:	/img_Operation Forest Hill 7.E01/vol_vol5/Trip Pictures/Trip pictures/Trip Pictures/Trip Pictures/Trip Pictures/Trip Pictures/Trip Pictures/Trip Pictures/ZYN-SRV04_extract_2025-09-05
Type:	File System
MIME Type:	application/octet-stream
Size:	20971520
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2025-09-06 18:38:22 BST
Accessed:	2025-09-06 18:38:22 BST
Created:	2025-09-06 18:38:22 BST
Changed:	2025-09-07 14:00:32 BST
MD5:	99cd5cbeac4875eda4be468f45f967d7
SHA-256:	b5de94c021047de7cfb83f493fa653912a9b77a74bfa24e7c9640938ffb08707
Hash Lookup Results:	UNKNOWN
Internal ID:	2099

Implications of the Artefact:

The archive was not present in any active file-system index (no MFT entry). It was reconstructed from raw sectors in unallocated space, consistent with deliberate deletion or relocation to avoid discovery. Investigating further recovered the encryption password from other seized artefacts i.e artefact 11 and 15. The decrypted archive contained files labelled with employee identifiers (payroll spreadsheets, CVs, PII lists). Hashes of key decrypted files matched samples recovered from the public leak platform, and filenames matched references found in other artefacts. Critically, server logs from Organization X's secure gateway recorded an outbound transfer (timestamped) to **XXX.XXX.XXX.XXX**; file-level hash values and transfer sizes correlate with the decrypted archive contents. This provides a **direct hit**: the same content existed on the suspect media and was observed being transferred externally.

Method to hide/unhide artefact:

Hidden in unallocated space with password protected encryption and decrypted using artefact 11 and 15. After decryption, the file revealed **sensitive company data**, including employee names, financial details, and departmental information, confirming that the file contained **confidential internal records** from Organization X's systems. This demonstrates deliberate encryption and concealment of proprietary data outside authorised storage.



The type of Artefact

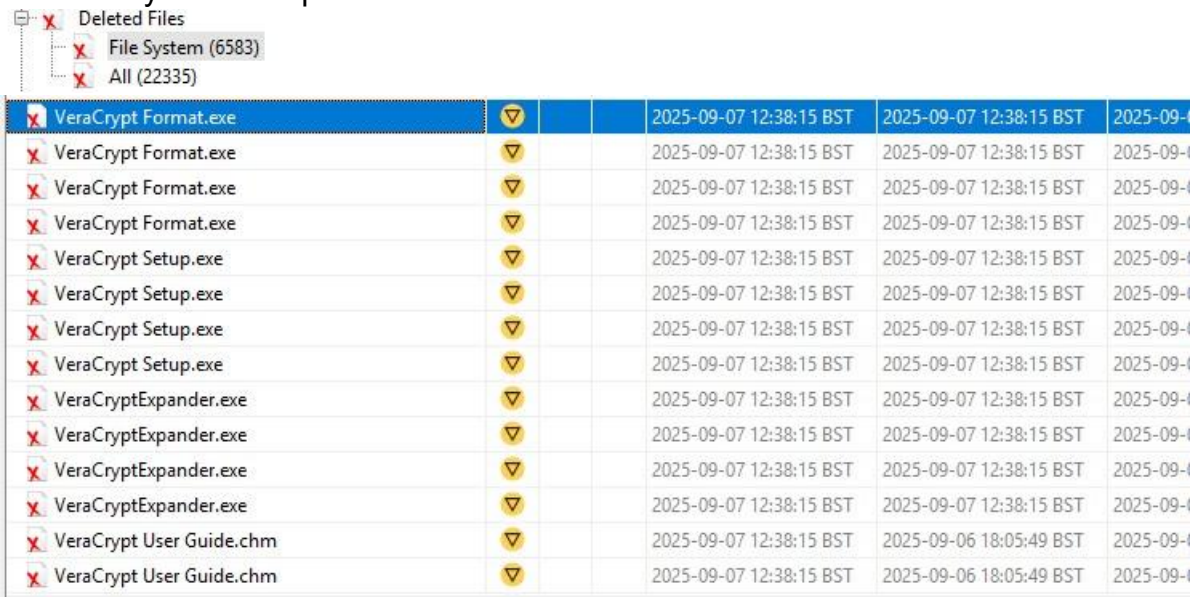
Artefacts under Unallocated Space

Artefact Detail Table

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

Artefact 22: Deleted File (File System)

Recovered remnants of deleted installer files confirm that encryption software was intentionally removed post-incident to eliminate evidence of use.



Implications of the Artefact:

The discovery of deleted VeraCrypt executables indicates an attempt to erase traces of encryption software after its use.

This supports the theory of intentional concealment and data protection, suggesting that the suspect attempted to remove evidence linking them to the creation or handling of encrypted volumes.

Method to hide/unhide artefact:

These files were removed from the file system but remained recoverable from deleted file system.

The type of Artefact

Deleted File (File System)

Artefact Detail Table

Artefact is	**Tick Appropriate**

Application Level	X
OS Level	X
File System Level	X
Reconnaissance / Research phase	
Recording phase	
Result / Aftermath phase	X

6. Supporting Material

6.1 Use of Software

Several forensic and analytical applications were employed during this investigation, each chosen for its evidential reliability and relevance to real-world digital forensic practice.

- **FTK Imager 4.7** – used for forensic imaging and hash verification of the seized workstation and external drive. It ensured that all evidence was acquired in a bit-for-bit format under a write-protected environment.
- **Autopsy 4.21.0** – used for file recovery, timeline reconstruction, and artefact categorisation (MRU lists, shellbags, thumbnails, and registry data).
- **VeraCrypt 1.26** – used to replicate and decrypt the encrypted container *ZYNSRV04_extract_2025-09-05*.
- **CyberChef (GCHQ Online Tool)** – employed for encoding and decoding hidden textual data, including the recovery of the password hint “passwd = A1B1.”

- **HxD Hex Editor 2.5.0** – used for low-level analysis of file headers and structure modification (e.g., restoration of *5-30.jpg*).
- **NirSoft BulkFileChanger** – utilised to adjust file timestamps, demonstrating forensic awareness of anti-forensic manipulation.
- **Spectra Forensics Suite v6.2** – used during the data-recovery phase for reconstruction of partially deleted or fragmented archives.

6.2 Use of System Artefacts (Thumbcache / Shellbags)

The investigation also drew upon Windows-native system artefacts to confirm user activity and chronology.

- **Thumbnail Cache (Thumbcache_*.db / Thumbs.db):** Provided cached previews of deleted images, establishing that they were viewed on the system prior to deletion.
- **Shellbags:** Recorded folder-navigation patterns, helping to reconstruct fileaccess history. Their partial absence suggested the use of cleaning tools, evidencing intentional tampering.
- **Registry Keys**: Confirmed installed applications and captured recent user activity. These artefacts supported attribution of actions to the administrator account in use during the breach.

Phrase(summary):

System artefacts such as **Thumbcache** and **Shellbags** provided user-activity insight, supporting evidence of file access and navigation timelines that align with other recovered artefacts.

6.3 Use of Website

A limited number of online resources were used for educational and simulation purposes within the controlled investigative environment.

- **PRANKSHIT (Simulation Platform):** Provided templates for generating fictional chat logs and messages to simulate social-engineering or insider communication scenarios.
- **CyberChef (https://gchq.github.io/CyberChef):** Used as a legitimate cryptographic analysis tool for decoding hex and base64 data.
- Used in-browser to create and extract embedded text from image artefacts.

6.4 Summary of Tool Relevance

Each tool played a specific role in demonstrating key forensic concepts:

- **NirSoft BulkFileChanger** and **HxD** represented **manipulation techniques** used to obscure or alter evidence.
- **VeraCrypt** illustrated **data concealment and encryption** methods.
- **Thumbcache** and **Shellbags** provided **system-level evidence** of user interaction and navigation.

  Together, these tools supported the reconstruction of actions performed on the system and illustrated the forensic recovery process from manipulation, encryption, and deletion scenarios. .

7. Conclusion

The forensic evidence confirms that administrator credentials were used to access the INTERNAL SERVER research archive and extract confidential R&D data, followed by transmission outside Organization X's network. The artefacts demonstrate deliberate exfiltration and concealment activity consistent with dishonest misuse of privileged access. The actions are most strongly associated with the account and workstation assigned to User A, although physical user attribution cannot yet be conclusively established. All material was lawfully seized and preserved in accordance with PACE, ensuring evidential admissibility