Operation: Whitechapel

Dhin Islam MD

1. Overview of the Case

1.1 Narrative of the case

On the evening of October 21, 2023, Kirai Tsuyoshi, a 29-year-old celebrity, became the victim of a burglary at his residence in Whitechapel, London. Earlier that evening, Mr. Tsuyoshi was attending a Premier League football match between Chelsea and Arsenal at Stamford Bridge. However, he had to return home after realizing he had forgotten his ticket.

Upon his arrival at the residence, Mr. Tsuyoshi noticed signs of a break-in. The front door was slightly ajar following with the second door which was slightly damaged, and he heard noises from inside the house, leading him to suspect a burglary in progress. He immediately contacted the police. Before the police arrived, Mr. Tsuyoshi confronted the intruder, resulting in a physical altercation. The burglar, upon hearing the approaching police sirens, attempted to escape, despite Kirai's effort to restrain Ken being unsuccessful, Kirai managed to seize the bag from the offender while they were fleeing, leaving behind a bag containing a laptop, a door panel removal tool, a wireless mouse, a water bottle, a Vaseline, and an ID."

The police's investigation of the contents of the laptop led to the identification of the primary suspect as Ken Shima and his associate, known as Shiro Aizen. During a thorough search of Mr. Tsuyoshi's property, it was discovered that an item of significant value, referred to as the "Dragon Balls," was missing. The investigation is actively ongoing, with efforts focused on locating Ken Shima and Shiro Aizen, and recovering the stolen item. The police are also dedicated to providing support to Mr. Tsuyoshi and maintaining the safety and security of the community.

In the course of their ongoing investigation, the police uncovered further details about Ken Shima's criminal history. Notably, he was involved in a high-profile heist known as 'OP COD.' During this operation, Ken, using the alias 'Tokyo,' successfully evaded arrest through a well-executed escape plan orchestrated with his team. This newfound information about his past activities and his skill in eluding capture has led the police to officially list Ken Shima as a wanted individual, intensifying their efforts to apprehend him.

Now, the police are urgently seeking Ken Shima and Shiro Aizen, prioritizing this case due to the severity of the crimes and the threat they pose to public safety.

1.2 Details of the offenders, victims, and witnesses

Offenders:

1. **Ken Shima**:
   Primary suspect in the burglary. Known for past criminal activities, including involvement in the 'OP COD' heist and skilled in evading capture. Identified through an ID left at the scene.

2. **Shiro Aizen**:
   Associate of Ken Shima, implicated in the burglary. Specific details about Shiro Aizen remain limited.

Victim:

1. **Kirai Tsuyoshi**:
   A 29-year-old celebrity and resident of Whitechapel, London. Victim of the burglary on October 21, 2023. Directly encountered the intruder, leading to a physical altercation. An item of significant value, referred to as the "Dragon Balls," was reported missing from his residence.

Witness:

- No external witnesses have been identified. Ken Tsuyoshi is the only known person to have interacted with the burglar.

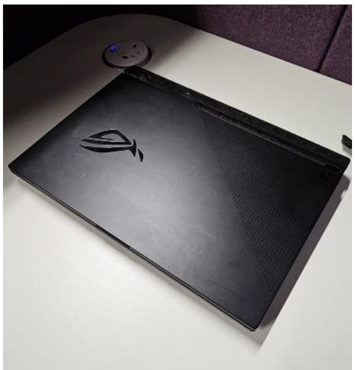
Equipment/Devices Involved:

1. **Laptop**: Found in the burglar's abandoned bag, instrumental in identifying Ken Shima.
2. **Door Panel Removal Tool**: Suggestive of the method of entry.
3. **Wireless Mouse**: Possibly used in conjunction with the laptop.
4. **Water Bottle**: Ordinary item, potential for DNA or fingerprints.
5. **Vaseline**: The purpose of this item in the context of the burglary remains unclear.
6. **ID**: Belonging to Ken Shima, vital for identification.

1.3 Photographs of any physical evidence, clues or supplemental material

Evidence 1: Bag

Evidence 2: Laptop

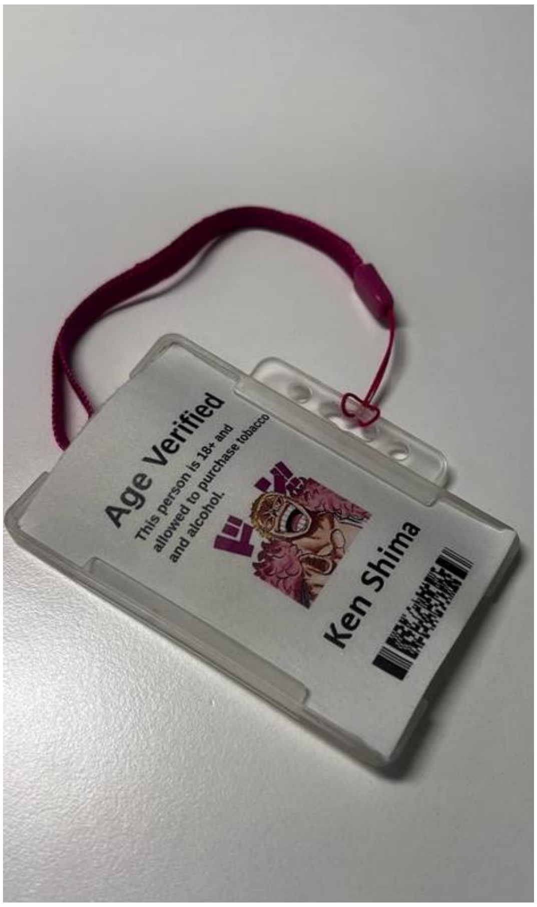


Evidence 3: Door Panel Removal Tool

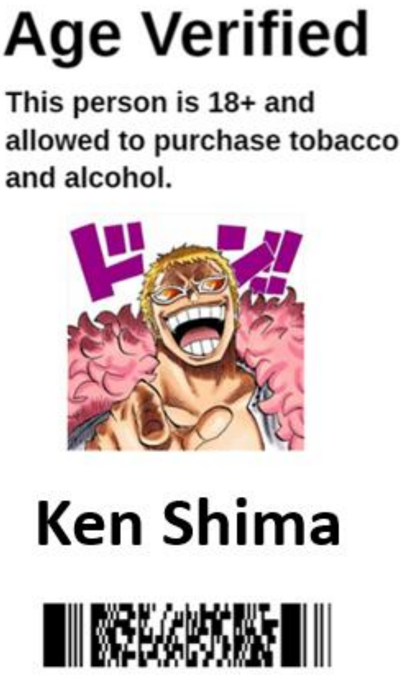
Evidence 4: Wireless Mouse

Evidence 5: Water Bottle

Evidence 6: ID


Age Verified
This person is 18+ and allowed to purchase tobacco and alcohol.
Ken Shima

A CLEAR VIEW OF THE ID



Age Verified

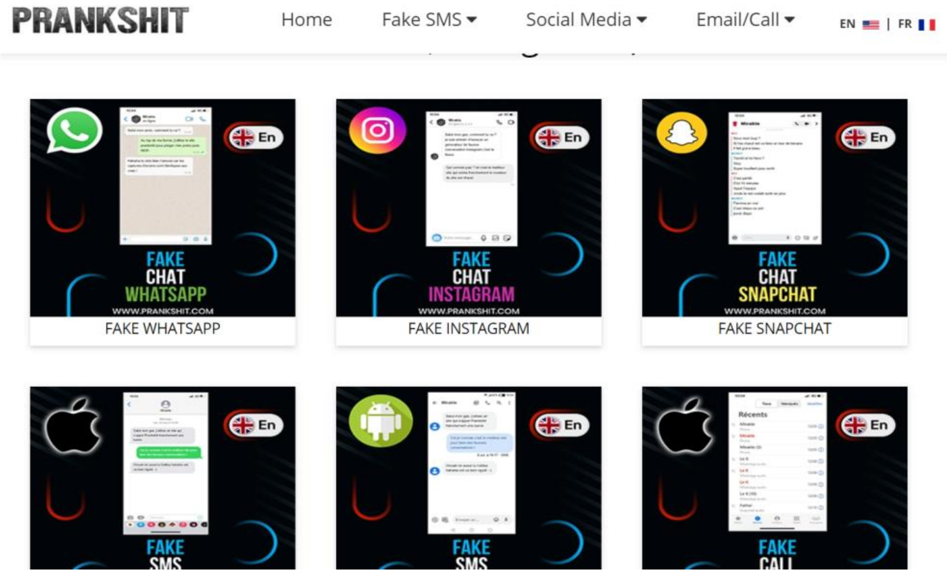
This person is 18+ and
allowed to purchase tobacco
and alcohol.

Ken Shima

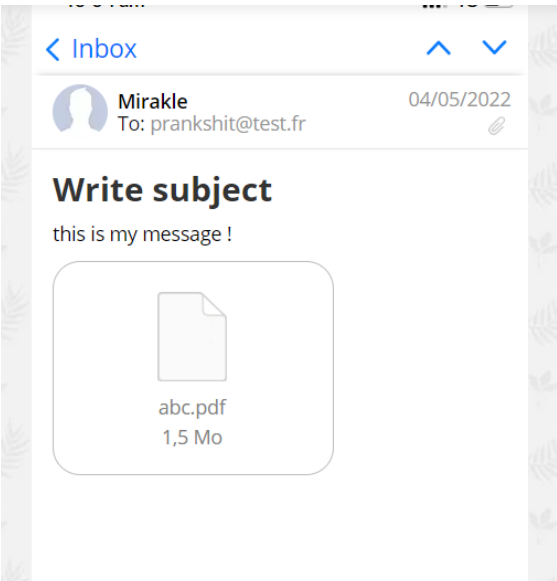
1.4 Scenario Rules

These rules are established to guide the investigation, particularly concerning the collection and interpretation of evidence:

1. **Timeframe of Evidence**: Any contents created after October 21st at 23:59 are not to be considered as evidence.
2. **Social Media and Messaging Content**: Fake social media posts or messages, even if fabricated are considered valid evidence.



3. **Email Correspondence**: Fake emails, regardless of their perceived authenticity, are to be treated as evidence. This evidence may provide insights into planning or execution of the burglary or related activities.



Mirakle
To: prankshit@test.fr
04/05/2022

Write subject

this is my message !

abc.pdf
1,5 Mo

4. **Manga Illustrations (Black and White)**: Pictures or illustrations in manga style, specifically the ones in black and white, are deemed to be not relevant to the investigation and should **NOT** be considered.

ONE HUNDRED PUSH-UPS. ONE HUNDRED SIT-UPS. ONE HUNDRED SQUATS.
AND RUN TEN KILOMETERS. EVERY DAY!!!

5. **Japanese and Dark Mysterious Animations (Colourful)**: Pictures or animations of this nature are relevant to the case. Their Content and context may offer crucial leads or connections to the suspects.

6. **Required Software Tool**: Specific software tools, including OpenPuff, VeraCrypt, CyberChef, and Microsoft Office are required for analysing evidence and solving the case. These tools may assist in decrypting hidden messages, analysing encrypted files, or examining documents related to the case.
7. **Documents with Altered Authorship**: Any documents found to have a different author name is to be considered as belonging to the offender, who is the real owner of the document. This rule assumes that any such modification is a deliberate attempt by the offender to disguise their identity or involvement in the case.

2. Legislation Analysis

2.1 Legislation

Relevant acts for this case include:

- **Theft Act 1968, CHAPTER 60, Section 7, 9 (1968 c.60, ss.7, 9)**: Applicable due to the burglary and theft of the “Dragon Balls”
- **Criminal Damage Act 1971, CHAPTER 48, Section 3 (1971 c.48, ss.3)**: Applicable due to the door damage during break-in
- **The Criminal Justice Act 1988, CHAPTER 33, Section 39 (1988 c.33, ss.39)**: Relevant to the physical altercation that occurred between Mr. Tsuyoshi and the intruder.

2.2 Points to prove

Theft Act 1968, CHAPTER 60, Section 7, 9 (1968 c.60, ss.7, 9)

- **Theft**

A person guilty of theft shall on conviction on indictment be liable to imprisonment for a term not exceeding [seven years].

Theft Act 1968

Green – Performing Action
Red – Knowledge of unauthorised entry
Purple – Intent to commit an offense
Blue – Theft
Orange – Aggravating factors

- **Burglary**

1) A person is guilty of burglary if—
   a) he enters any building or part of a building as a trespasser and with intent commit any such offence as is mentioned in subsection (2) below; or
   b) having entered any building or part of a building as a trespasser he steals or attempts to steal anything in the building or that part of it or inflicts or attempts to inflict on any person therein any grievous bodily harm.

3) A person guilty of burglary shall on conviction on indictment be liable to imprisonment for a term not exceeding—

   a) where the offence was committed in respect of a building or part of a building which is a dwelling, fourteen years.
   b) in any other case, ten years.

Criminal Damage Act 1971, CHAPTER 48, Section 3 (1971 c.48, ss.3)

- **Destroying or damaging property**

1) A person who without lawful excuse destroys or damages any property belonging to another intending to destroy or damage any such property or being reckless as to whether any such property would be destroyed or damaged shall be guilty of an offence.

Criminal Damage Act 1971

Green – Act of damaging property
Blue – Intension to damage
Red – Recklessness
Orange – Endangerment of Life
Purple – Absence of Lawful excuses

The Criminal Justice Act 1988, CHAPTER 33, Section 39 (1988 c.33, ss.39)

- **Common assault and battery to be summary offences**

1) Common assault and battery shall be summary offences and a person guilty of either of them shall be liable to a fine not exceeding level 5 on the standard scale, to imprisonment for a term not exceeding six months, or to both.

Comon Assault Act 1988

Green – Act of assault / Offense

2.3 What the Digital Forensics case can prove

Theft Act 1968, CHAPTER 60, Section 7, 9 (1968 c.60, ss.9)

- **Burglary**

'Enters any building or part of a building as a trespasser and with intent commit any such offence' and 'where the offence was committed in respect of a building or part of a building which is a dwelling': **Artefact 7** depicts an image portraying the front entrance of the victim's residence. Conversely, **Artefact 12** constitutes a pin believed to have been utilised for access to the secondary door within the residence. Additionally, **Artefact 14** comprises a deleted house map delineating the layout of the victim's dwelling.

'having entered any building or part of a building as a trespasser he steals': Based on the recovery and examination of **Artefacts 4** and **Artefact 5**, it is evident that the presence of these items strongly indicates the intent of the offenders to appropriate a specific item. Subsequently, an item matching this description was found missing from the victim's residence subsequent to the reported burglary.

Criminal Damage Act 1971, CHAPTER 48, Section 3 (1971 c.48, ss.3)

- **Destroying or damaging property**

'A person who without lawful excuse destroys or damages any property belonging to another intending to destroy or damage any such property': **Artefact 6**, identified as an Amazon hyperlink, leads to the tools evidently utilized by the perpetrator, Ken, in forcibly gaining entry through the front door during the commission of the burglary.

'Being reckless as to whether any such property would be destroyed or damaged': **Artefact 12** comprises a collection of bookmarks containing YouTube videos demonstrating techniques for breaching doors using a variety of tools.

2.4 What the Digital Forensics case will not prove

Theft Act 1968, CHAPTER 60, Section 7, 9 (1968 c.60, ss.7)

- **Theft**

A person guilty of theft: The valuable item '**Dragon Balls**' was missing after the offender fled the scene, which was the offender primary objective. But the artefacts retrieved cannot prove.

The Criminal Justice Act 1988, CHAPTER 33, Section 39 (1988 c.33, ss.39)

- **Common assault and battery to be summary offences**

'Common assault and battery shall be summary offences':

Upon arrival at the scene, it was evident upon examination that Kirai Tsuyoshi bore facial wounds indicative of a physical altercation, strongly implying an assault perpetrated by the offender against the victim.

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

None

3. Timeline of Artefacts

3.1 Reconnaissance / Research Phase Artefacts

This Phase starts: On October 16, 2023, it was observed that the inception of the criminal acts transpired, instigated by Shiro, who involved Ken through intimidation via text message, leveraging blackmail tactics. Subsequently, both individuals engaged in the meticulous planning and preparation phases of the intended crime.

This Phase Ends: On October 21, 2023, the perpetrator commenced activities constituting elements of the offense.

Artefact #	Artefact Name
Artefact 1	Chat Artefact
Artefact 2	Document containing important information
Artefact 3	Picture
Artefact 4	Hiding text within a document
Artefact 5	Hiding picture withing a document
Artefact 6	Manipulating file extensions
Artefact 7	Manipulating file headers
Artefact 8	Email artefact
Artefact 9	Registry Information – Install Software
Artefact 10	The 'hidden' flag within an operating system
Artefact 11	Encrypted password protected container
Artefact 12	Encoded Text
Artefact 13	Steg of Pictures
Artefact 14	Deleted Files (Recycle Bin)
Artefact 15	Obfuscation of File and/or path name
Artefact 16	Video

Artefact 17	Splicing – using software to edit video
Artefact 18	Internet history records showing searches of relevant terms.
Artefact 19	Registry Information - Username
Artefact 20	Most Recently Used (MRU)

3.2 Record Phase Artefacts

This Phase starts: On October 21, 2023, the perpetrator initiated the unlawful sequence of actions by trespassing into a residential property, thereby gaining unauthorized entry.

This Phase Ends: The phase concluded upon Kirai's escape from the scene.

Artefact #	Artefact Name
Artefact 1	Chat Artefact
Artefact 13	Steg of Pictures

3.3 Result / Aftermath Artefacts

This Phase starts: The sequence commenced upon the escape of the perpetrator from the scene, abandoning personal belongings in the process.

This Phase Ends: Upon the completion of the investigation into the crime scene.

Artefact #	Artefact Name
Artefact 9	Registry Information – Install Software
Artefact 14	Deleted Files (Recycle Bin)
Artefact 17	Splicing – using software to edit video
Artefact 20	Most Recently Used (MRU)

4. Artefacts

4.1 Summary of Artefacts

Total number of artefacts that have included: 20

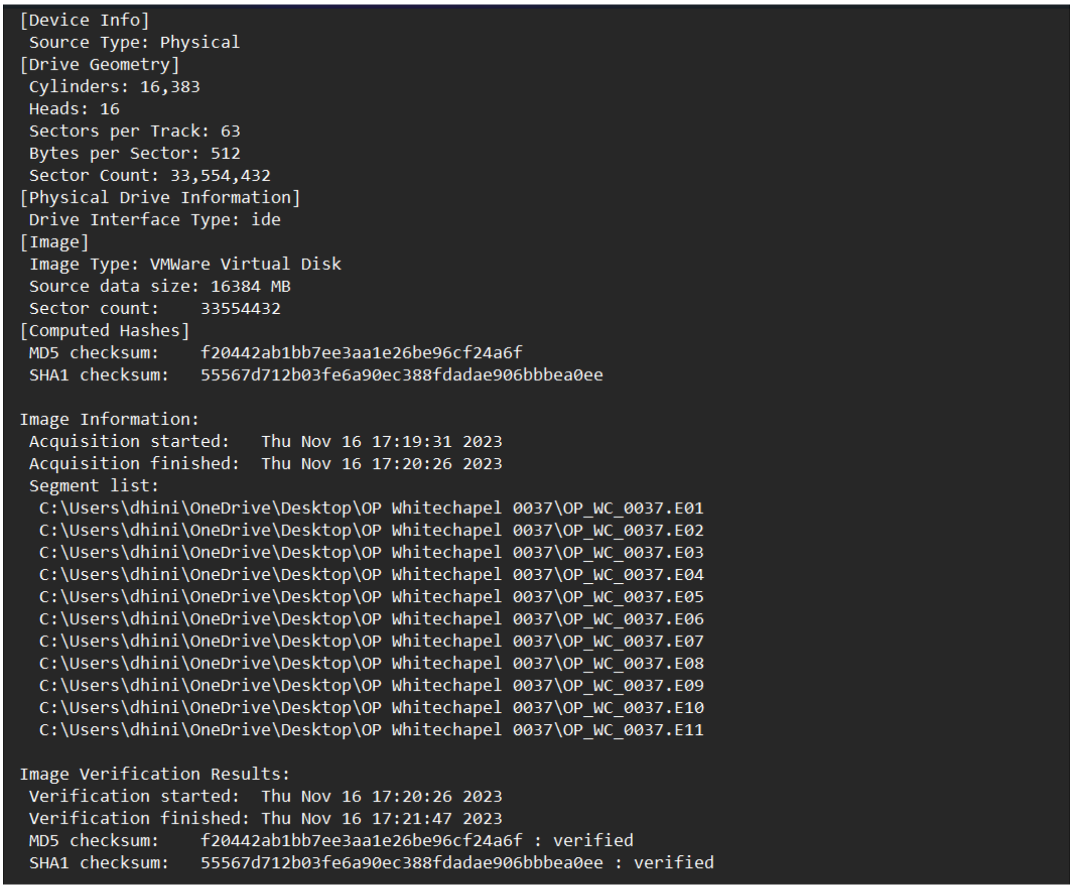
Type of Artefacts	Artefact #	Artefact #
Content		
A document containing important information	Artefact 2	
A picture, audio or video.	Artefact 3	Artefact 16
Web cache Pages or Pictures		
Internet history records showing searches of relevant terms.	Artefact 18	
Emails or chat artefacts	Artefact 8	Artefact 1
Hiding		
Encoded or encrypted text	Artefact 12	
Embedded text or information into a picture		
Steg of pictures	Artefact 13	
Splicing – using software to edit audio, pictures or video together.	Artefact 17	
The 'hidden' flag within an operating system	Artefact 10	
Hiding text or pictures within a document	Artefact 4	Artefact 5
Manipulating file extensions	Artefact 6	
Manipulating file headers (magic numbers) to hide the file.	Artefact 7	
Obfuscation of file and/or path name.	Artefact 15	
Encrypted password protected container	Artefact 11	
Recovery and Interpretation		
Most Recently Used (MRU)	Artefact 20	
Link File Recent Activity		
Shellbags – the MRU for folders		
Thumbcache / Thumbs.db		
Registry Information – various things such as username, password and hint, installed software	Artefact 9	Artefact 19
Artefacts within unallocated		
Deleted files (recycle bin)	Artefact 14	
Deleted File (File System)		

Table 1 – Artefact Type

4.2 Other types of Artefacts

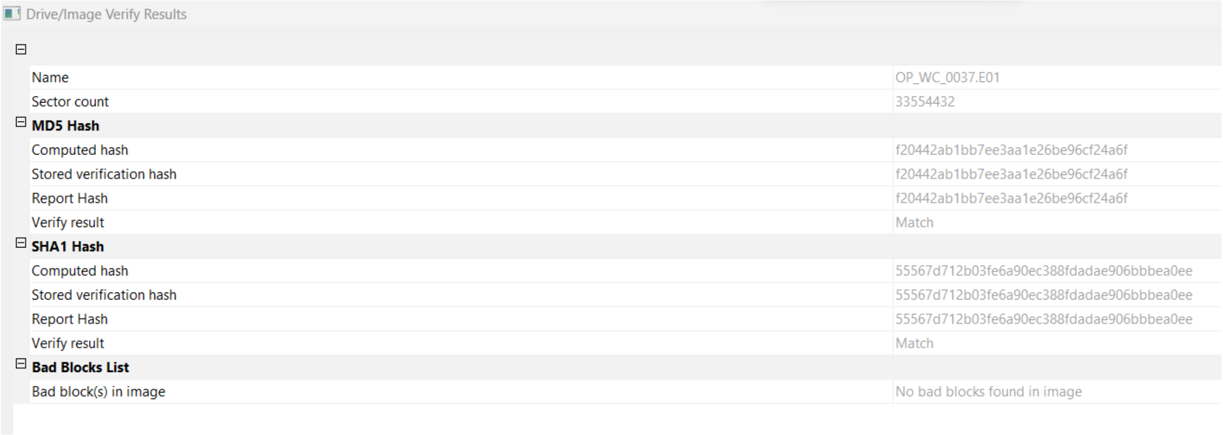
None

4.3 Details of the Evidence File



```
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 16,383
 Heads: 16
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 33,554,432
[Physical Drive Information]
 Drive Interface Type: ide
[Image]
 Image Type: VMWare Virtual Disk
 Source data size: 16384 MB
 Sector count:    33554432
[Computed Hashes]
 MD5 checksum:    f20442ab1bb7ee3aa1e26be96cf24a6f
 SHA1 checksum:   55567d712b03fe6a90ec388fdadae906bbbea0ee

Image Information:
 Acquisition started:   Thu Nov 16 17:19:31 2023
 Acquisition finished:  Thu Nov 16 17:20:26 2023
 Segment list:
  C:\Users\dhini\OneDrive\Desktop\OP Whitechapel 0037\OP_WC_0037.E01
  C:\Users\dhini\OneDrive\Desktop\OP Whitechapel 0037\OP_WC_0037.E02
  C:\Users\dhini\OneDrive\Desktop\OP Whitechapel 0037\OP_WC_0037.E03
  C:\Users\dhini\OneDrive\Desktop\OP Whitechapel 0037\OP_WC_0037.E04
  C:\Users\dhini\OneDrive\Desktop\OP Whitechapel 0037\OP_WC_0037.E05
  C:\Users\dhini\OneDrive\Desktop\OP Whitechapel 0037\OP_WC_0037.E06
  C:\Users\dhini\OneDrive\Desktop\OP Whitechapel 0037\OP_WC_0037.E07
  C:\Users\dhini\OneDrive\Desktop\OP Whitechapel 0037\OP_WC_0037.E08
  C:\Users\dhini\OneDrive\Desktop\OP Whitechapel 0037\OP_WC_0037.E09
  C:\Users\dhini\OneDrive\Desktop\OP Whitechapel 0037\OP_WC_0037.E10
  C:\Users\dhini\OneDrive\Desktop\OP Whitechapel 0037\OP_WC_0037.E11

Image Verification Results:
 Verification started:  Thu Nov 16 17:20:26 2023
 Verification finished: Thu Nov 16 17:21:47 2023
 MD5 checksum:    f20442ab1bb7ee3aa1e26be96cf24a6f : verified
 SHA1 checksum:   55567d712b03fe6a90ec388fdadae906bbbea0ee : verified
```

This is the hash of the final evidence file.

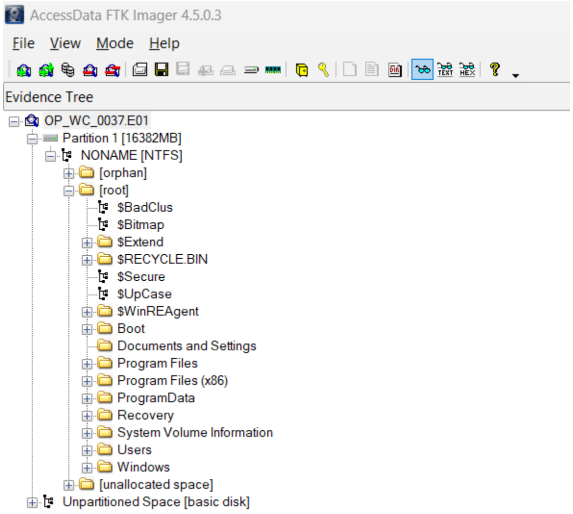


Drive/Image Verify Results

⊟	
Name	OP_WC_0037.E01
Sector count	33554432
⊟ **MD5 Hash**	
Computed hash	f20442ab1bb7ee3aa1e26be96cf24a6f
Stored verification hash	f20442ab1bb7ee3aa1e26be96cf24a6f
Report Hash	f20442ab1bb7ee3aa1e26be96cf24a6f
Verify result	Match
⊟ **SHA1 Hash**	
Computed hash	55567d712b03fe6a90ec388fdadae906bbbea0ee
Stored verification hash	55567d712b03fe6a90ec388fdadae906bbbea0ee
Report Hash	55567d712b03fe6a90ec388fdadae906bbbea0ee
Verify result	Match
⊟ **Bad Blocks List**	
Bad block(s) in image	No bad blocks found in image

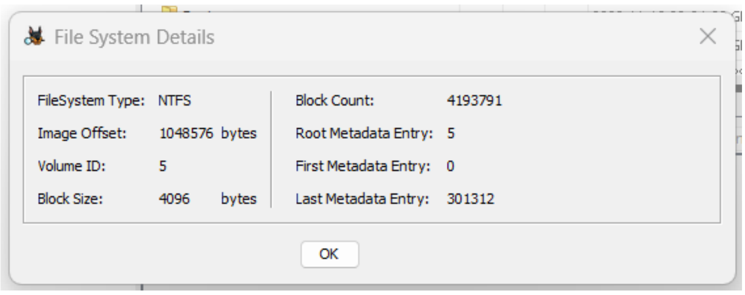
This is the evidence of the file named ‘**OP_WC_0037.E01**’ and it shows the verified MD5 and SHA1 hash.

4.4 Details of the File System



```
OP_WC_0037.E01
  Partition 1 [16382MB]
    NONAME [NTFS]
      [orphan]
      [root]
        $BadClus
        $Bitmap
        $Extend
        $RECYCLE.BIN
        $Secure
        $UpCase
        $WinREAgent
        Boot
        Documents and Settings
        Program Files
        Program Files (x86)
        ProgramData
        Recovery
        System Volume Information
        Users
        Windows
      [unallocated space]
  Unpartitioned Space [basic disk]
```

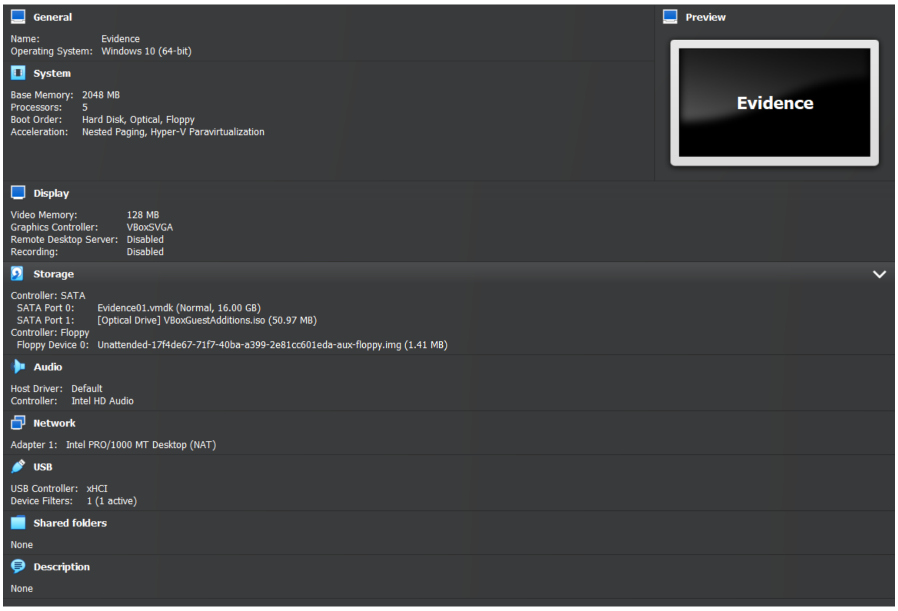
This is the file system details in FTK Imager



FileSystem Type:	NTFS	Block Count:	4193791
Image Offset:	1048576 bytes	Root Metadata Entry:	5
Volume ID:	5	First Metadata Entry:	0
Block Size:	4096 bytes	Last Metadata Entry:	301312

This is the file system details in Autopsy

4.5 Details of the Operating System

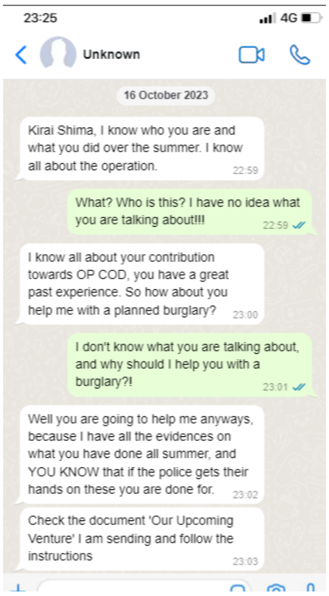


```
General
Name:               Evidence
Operating System:   Windows 10 (64-bit)

System
Base Memory:   2048 MB
Processors:    5
Boot Order:    Hard Disk, Optical, Floppy
Acceleration:  Nested Paging, Hyper-V Paravirtualization

Display
Video Memory:             128 MB
Graphics Controller:      VBoxSVGA
Remote Desktop Server:    Disabled
Recording:                Disabled

Storage
Controller: SATA
  SATA Port 0:       Evidence01.vmdk (Normal, 16.00 GB)
  SATA Port 1:       [Optical Drive] VBoxGuestAdditions.iso (50.97 MB)
Controller: Floppy
  Floppy Device 0:   Unattended-17f4de67-71f7-40ba-a399-2e81cc601eda-aux-floppy.img (1.41 MB)

Audio
Host Driver:   Default
Controller:    Intel HD Audio

Network
Adapter 1:  Intel PRO/1000 MT Desktop (NAT)

USB
USB Controller:   xHCI
Device Filters:   1 (1 active)

Shared folders
None

Description
None
```

This is the details of the operating system used by the suspect Ken Tsuyoshi.

5. Artefacts

Artefact 1: screnshot_0168.png



23:25

Unknown

16 October 2023

Kirai Shima, I know who you are and what you did over the summer. I know all about the operation. 22:59

What? Who is this? I have no idea what you are talking about!!! 22:59

I know all about your contribution towards OP COD, you have a great past experience. So how about you help me with a planned burglary? 23:00

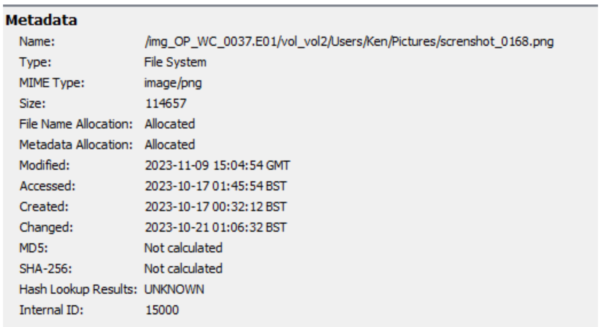
I don't know what you are talking about, and why should I help you with a burglary?! 23:01

Well you are going to help me anyways, because I have all the evidences on what you have done all summer, and YOU KNOW that if the police gets their hands on these you are done for. 23:02

Check the document 'Our Upcoming Venture' I am sending and follow the instructions 23:03

Meta-Data of the artefact:

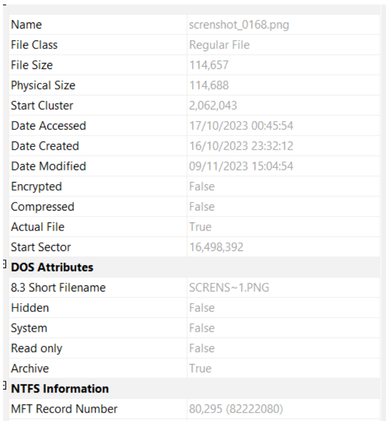
Meta-Data from Autopsy:



Metadata

Name:	/img_OP_WC_0037.E01/vol_vol2/Users/Ken/Pictures/screnshot_0168.png
Type:	File System
MIME Type:	image/png
Size:	114657
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2023-11-09 15:04:54 GMT
Accessed:	2023-10-17 01:45:54 BST
Created:	2023-10-17 00:32:12 BST
Changed:	2023-10-21 01:06:32 BST
MD5:	Not calculated
SHA-256:	Not calculated
Hash Lookup Results:	UNKNOWN
Internal ID:	15000

Meta data from FTK Imager:



Name	screnshot_0168.png
File Class	Regular File
File Size	114,657
Physical Size	114,688
Start Cluster	2,062,043
Date Accessed	17/10/2023 00:45:54
Date Created	16/10/2023 23:32:12
Date Modified	09/11/2023 15:04:54
Encrypted	False
Compressed	False
Actual File	True
Start Sector	16,498,392
DOS Attributes	
8.3 Short Filename	SCRENS~1.PNG
Hidden	False
System	False
Read only	False
Archive	True
NTFS Information	
MFT Record Number	80,295 (82222080)

Implications of the Artefact:

The content of the **Artefact 1** is relevant to the investigation. The file named "**screenshot_0168.png**" is live and traced at the following location in the operating system: Root/Users/Ken/Pictures/ and the file appears to be accessed. This artefact relates to the investigation due to the suspicious conversation between the two individuals. The screenshot reveals a conversation where Shiro Aizen approaches Ken, threatening to expose Ken's involvement in a past crime (OP COD) unless he complies with a new criminal plan. This artefact is critical as it not only indicates Shiro Aizen's knowledge of Ken's past activities, which Ken has kept hidden, but also shows Shiro Aizen leveraging this information to persuade Ken into participating in another crime. It also suggests that Shiro Aizen is prepared to turn evidence over to the police if Ken does not cooperate, thereby implicating both in a conspiracy to commit a new offense.

Method to hide/unhide artefact:

Not hidden (as the file was found without any encryption or specialized software to reveal it)

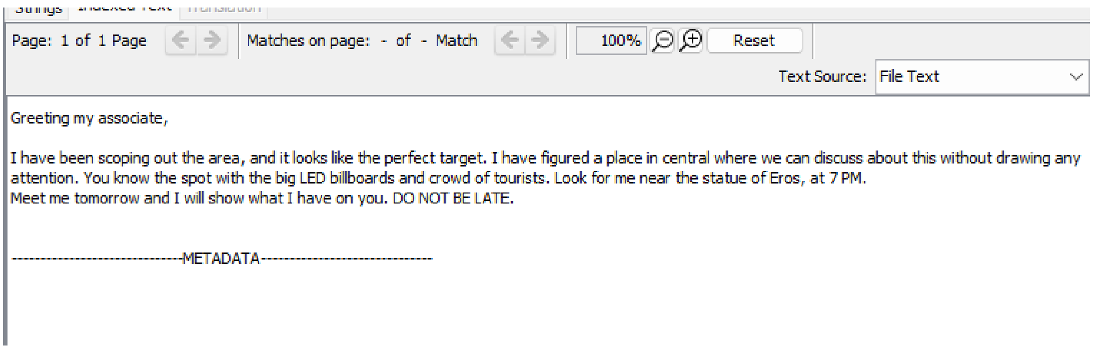
The type of Artefact

Chat Artefact

Artefact Detail Table

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

Artefact 2: Our Upcoming Venture.txt



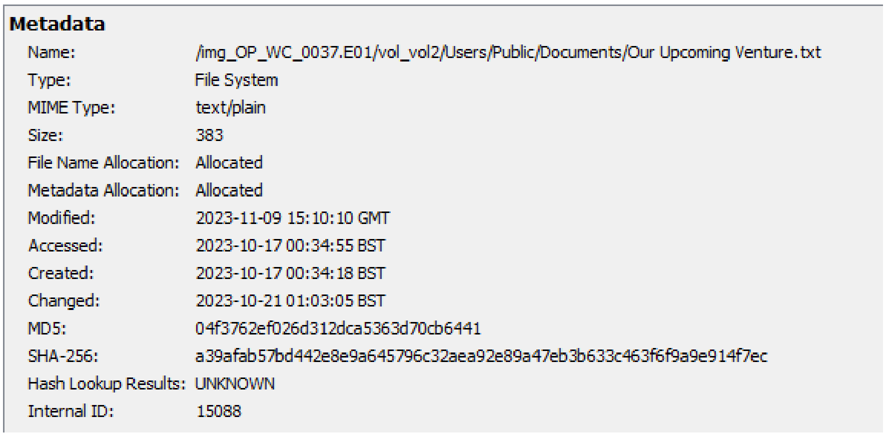
Greeting my associate,

I have been scoping out the area, and it looks like the perfect target. I have figured a place in central where we can discuss about this without drawing any attention. You know the spot with the big LED billboards and crowd of tourists. Look for me near the statue of Eros, at 7 PM.
Meet me tomorrow and I will show what I have on you. DO NOT BE LATE.

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

Meta-Data of the artefact:

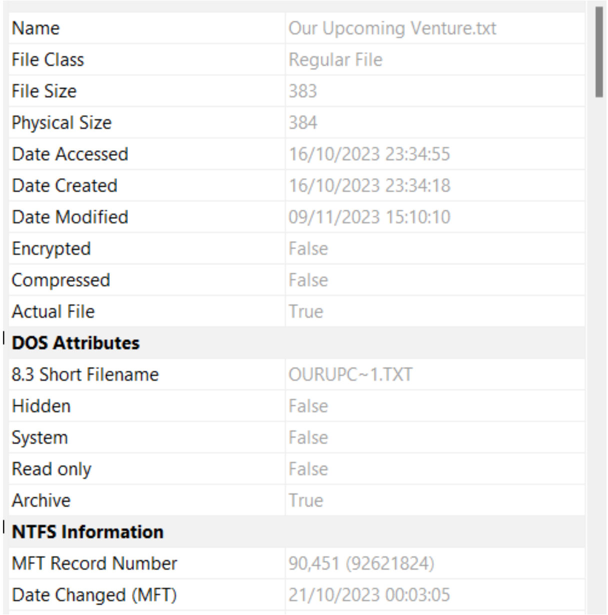
Meta-Data from Autopsy:



Metadata

Name:	/img_OP_WC_0037.E01/vol_vol2/Users/Public/Documents/Our Upcoming Venture.txt
Type:	File System
MIME Type:	text/plain
Size:	383
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2023-11-09 15:10:10 GMT
Accessed:	2023-10-17 00:34:55 BST
Created:	2023-10-17 00:34:18 BST
Changed:	2023-10-21 01:03:05 BST
MD5:	04f3762ef026d312dca5363d70cb6441
SHA-256:	a39afab57bd442e8e9a645796c32aea92e89a47eb3b633c463f6f9a9e914f7ec
Hash Lookup Results:	UNKNOWN
Internal ID:	15088

Meta-Data from FTM Imager:



Name	Our Upcoming Venture.txt
File Class	Regular File
File Size	383
Physical Size	384
Date Accessed	16/10/2023 23:34:55
Date Created	16/10/2023 23:34:18
Date Modified	09/11/2023 15:10:10
Encrypted	False
Compressed	False
Actual File	True
DOS Attributes	
8.3 Short Filename	OURUPC~1.TXT
Hidden	False
System	False
Read only	False
Archive	True
NTFS Information	
MFT Record Number	90,451 (92621824)
Date Changed (MFT)	21/10/2023 00:03:05

Implications of the Artefact:

Artefact 2 relevant to the investigation identified as '**Our Upcoming Venture.txt**' is securely stored within the directory path: Root/Users/Public/Documents, it also shows that the file was accessed. The artefact contains clear evidence of a meeting being arranged to discuss a criminal plan, with a specific location and time noted. It outlines a scheduled meeting between the involved parties at a public location known for its large LED billboards and tourist presence. The specific mention of a time "7 PM" and an instruction to not be late underscores the urgency and importance of this rendezvous. This indicates premeditation and a collaboration between the suspects at an early stage of the criminal activity.

Method to hide/unhide artefact:

Not hidden (as the file was found without any encryption or specialized software to reveal it)

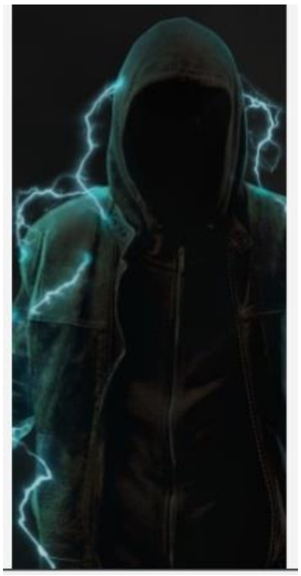
The type of Artefact

A Document Containing Important Information

Artefact Detail Table

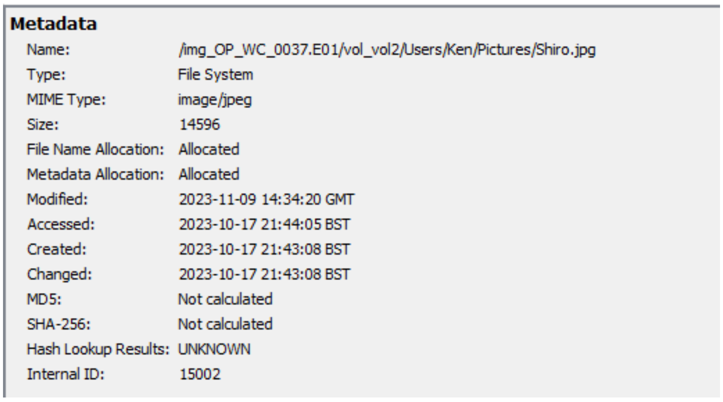
Artefact is	**Tick Appropriate**
Application Level	✓
OS Level	
File System Level	
Reconnaissance / Research phase	✓
Recording phase	
Result / Aftermath phase	

Artefact 3: Shiro.jpg



Meta-Data of the artefact:

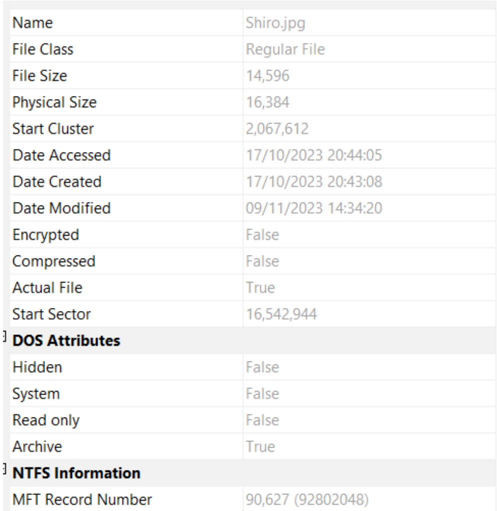
Meta-Data from Autopsy:



Metadata

Name:	/img_OP_WC_0037.E01/vol_vol2/Users/Ken/Pictures/Shiro.jpg
Type:	File System
MIME Type:	image/jpeg
Size:	14596
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2023-11-09 14:34:20 GMT
Accessed:	2023-10-17 21:44:05 BST
Created:	2023-10-17 21:43:08 BST
Changed:	2023-10-17 21:43:08 BST
MD5:	Not calculated
SHA-256:	Not calculated
Hash Lookup Results:	UNKNOWN
Internal ID:	15002

Meta-Data from FTM Imager:



Name	Shiro.jpg
File Class	Regular File
File Size	14,596
Physical Size	16,384
Start Cluster	2,067,612
Date Accessed	17/10/2023 20:44:05
Date Created	17/10/2023 20:43:08
Date Modified	09/11/2023 14:34:20
Encrypted	False
Compressed	False
Actual File	True
Start Sector	16,542,944
DOS Attributes	
Hidden	False
System	False
Read only	False
Archive	True
NTFS Information	
MFT Record Number	90,627 (92802048)

Implications of the Artefact:

An evidentiary image, appointed as **Artefact 3** stored at: Root/Users/Ken/Pictures/Shiro.jpg, depicts a potential suspect, identified as ‘**Shiro**’ which shows relevance to the investigation and suggests it was saved and viewed recently. The image features a figure cloaked in a hood, with visual effects that obscure the individual's features, potentially used as a method of concealing the identity of 'Shiro Aizen.' Given the association with the name 'Shiro Aizen,' which has been mentioned in the context of the ongoing investigation, it is reasonable to infer that this image is of significance to the individual's identity or represents them in some capacity.

Method to hide/unhide artefact:

Not hidden (as the file was found without any encryption or specialized software to reveal it)

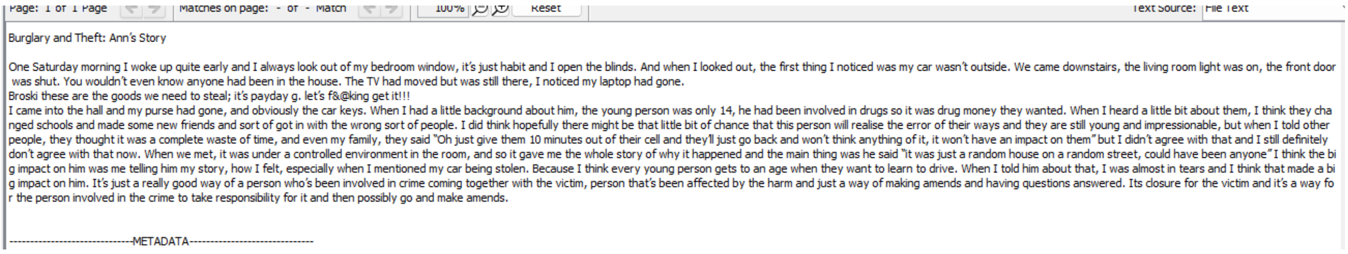
The type of Artefact

A Picture

Artefact Detail Table

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

Artefact 4: Burglary-and-Theft-Anns-Story-transcript.docx



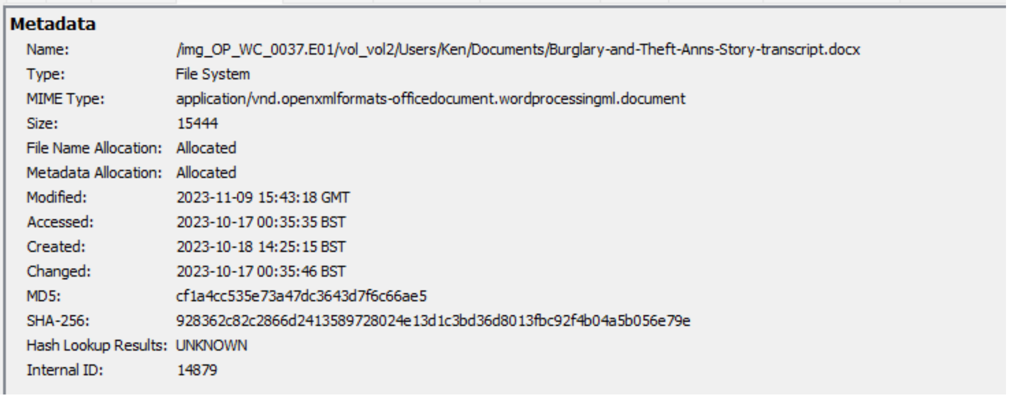
Burglary and Theft: Ann's Story

One Saturday morning I woke up quite early and I always look out of my bedroom window, it's just habit and I open the blinds. And when I looked out, the first thing I noticed was my car wasn't outside. We came downstairs, the living room light was on, the front door was shut. You wouldn't even know anyone had been in the house. The TV had moved but was still there, I noticed my laptop had gone.
Broski these are the goods we need to steal; it's payday g. let's f&@king get it!!!
I came into the hall and my purse had gone, and obviously the car keys. When I had a little background about him, the young person was only 14, he had been involved in drugs so it was drug money they wanted. When I heard a little bit about them, I think they changed schools and made some new friends and sort of got in with the wrong sort of people. I did think hopefully there might be that little bit of chance that this person will realise the error of their ways and they are still young and impressionable, but when I told other people, they thought it was a complete waste of time, and even my family, they said "Oh just give them 10 minutes out of their cell and they'll just go back and won't think anything of it, it won't have an impact on them" but I didn't agree with that and I still definitely don't agree with that now. When we met, it was under a controlled environment in the room, and so it gave me the whole story of why it happened and the main thing was he said "it was just a random house on a random street, could have been anyone" I think the big impact on him was me telling him my story, how I felt, especially when I mentioned my car being stolen. Because I think every young person gets to an age when they want to learn to drive. When I told him about that, I was almost in tears and I think that made a big impact on him. It's just a really good way of a person who's been involved in crime coming together with the victim, person that's been affected by the harm and just a way of making amends and having questions answered. Its closure for the victim and it's a way for the person involved in the crime to take responsibility for it and then possibly go and make amends.

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

Meta-Data of the artefact:

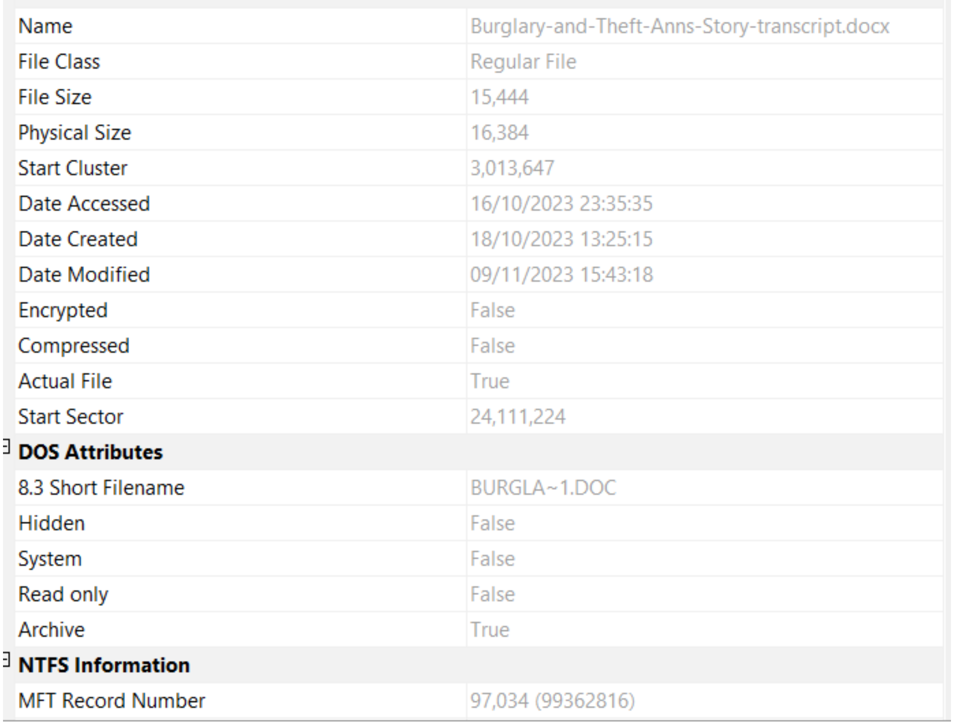
Meta-Data from Autopsy:



Metadata

Name:	/img_OP_WC_0037.E01/vol_vol2/Users/Ken/Documents/Burglary-and-Theft-Anns-Story-transcript.docx
Type:	File System
MIME Type:	application/vnd.openxmlformats-officedocument.wordprocessingml.document
Size:	15444
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2023-11-09 15:43:18 GMT
Accessed:	2023-10-17 00:35:35 BST
Created:	2023-10-18 14:25:15 BST
Changed:	2023-10-17 00:35:46 BST
MD5:	cf1a4cc535e73a47dc3643d7f6c66ae5
SHA-256:	928362c82c2866d2413589728024e13d1c3bd36d8013fbc92f4b04a5b056e79e
Hash Lookup Results:	UNKNOWN
Internal ID:	14879

Meta-Data from FTK Imager:



Name	Burglary-and-Theft-Anns-Story-transcript.docx
File Class	Regular File
File Size	15,444
Physical Size	16,384
Start Cluster	3,013,647
Date Accessed	16/10/2023 23:35:35
Date Created	18/10/2023 13:25:15
Date Modified	09/11/2023 15:43:18
Encrypted	False
Compressed	False
Actual File	True
Start Sector	24,111,224
DOS Attributes	
8.3 Short Filename	BURGLA~1.DOC
Hidden	False
System	False
Read only	False
Archive	True
NTFS Information	
MFT Record Number	97,034 (99362816)

Implications of the Artefact:

Artefact 4 is a document titled "**Burglary and Theft: Ann's Story transcript.docx**" and it is stored at: 'Root/Users/Ken/Documents' it is suspected to contain a concealed message pertinent to the investigation. This Word document contains a narrative about a theft and burglary incident. Notably, a specific sentence within the document was intentionally obscured by changing the font colour to white, rendering it invisible against the background and effectively hiding it from plain view. The hidden sentence reads, **"Broski these are the goods we need to steal; It's payday g. let's f&@king get it!!!,"** which suggests a covert exchange of information about items.

Method to hide/unhide artefact:

Hidden text within a Word document. The text's font colour was changed to match the background, rendering it effectively invisible within the document, creating the appearance of an empty space between paragraphs.

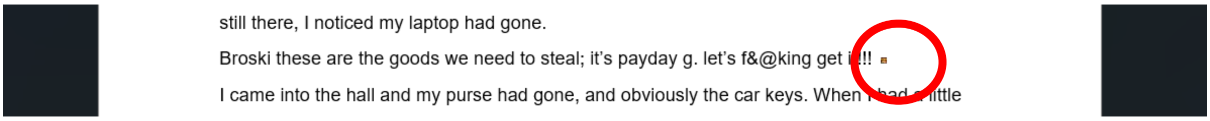
The type of Artefact

Hiding text within a document

Artefact Detail Table

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

Artefact 5: Burglary-and-Theft-Anns-Story-transcript.docx



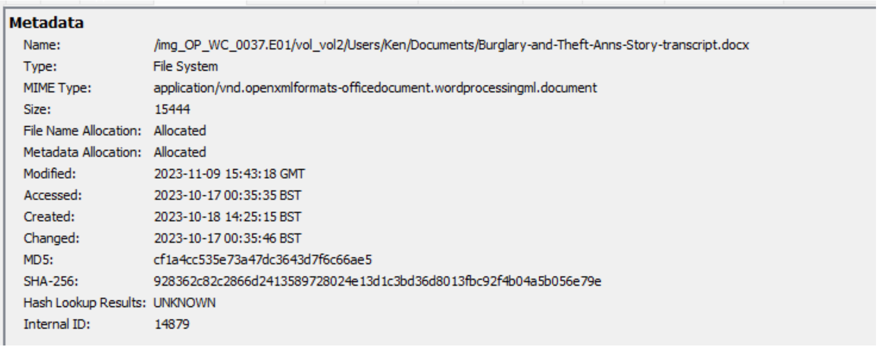
still there, I noticed my laptop had gone.

Broski these are the goods we need to steal; it's payday g. let's f&@king get it!!

I came into the hall and my purse had gone, and obviously the car keys. When I had a little

Meta-Data of the artefact:

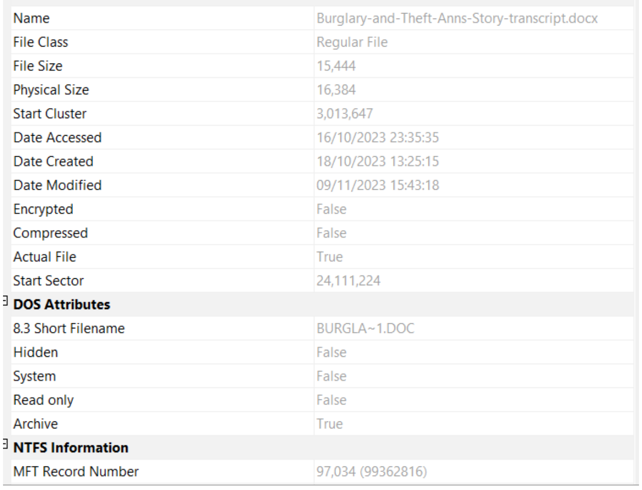
Meta-Data from Autopsy:



Metadata

Name:	/img_OP_WC_0037.E01/vol_vol2/Users/Ken/Documents/Burglary-and-Theft-Anns-Story-transcript.docx
Type:	File System
MIME Type:	application/vnd.openxmlformats-officedocument.wordprocessingml.document
Size:	15444
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2023-11-09 15:43:18 GMT
Accessed:	2023-10-17 00:35:35 BST
Created:	2023-10-18 14:25:15 BST
Changed:	2023-10-17 00:35:46 BST
MD5:	cf1a4cc535e73a47dc3643d7f6c66ae5
SHA-256:	928362c82c2866d2413589728024e13d1c3bd36d8013fbc92f4b04a5b056e79e
Hash Lookup Results:	UNKNOWN
Internal ID:	14879

Meta-Data from FTK Imager:



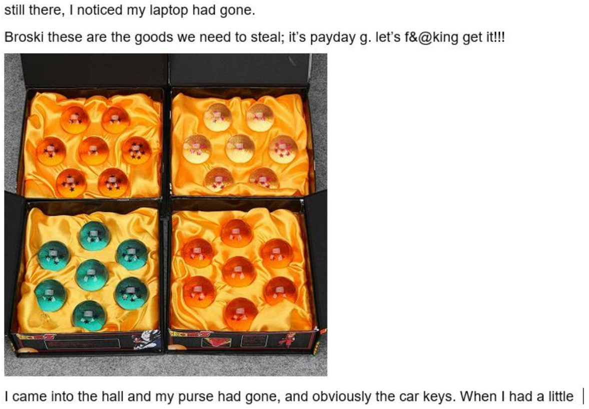
Name	Burglary-and-Theft-Anns-Story-transcript.docx
File Class	Regular File
File Size	15,444
Physical Size	16,384
Start Cluster	3,013,647
Date Accessed	16/10/2023 23:35:35
Date Created	18/10/2023 13:25:15
Date Modified	09/11/2023 15:43:18
Encrypted	False
Compressed	False
Actual File	True
Start Sector	24,111,224
DOS Attributes	
8.3 Short Filename	BURGLA~1.DOC
Hidden	False
System	False
Read only	False
Archive	True
NTFS Information	
MFT Record Number	97,034 (99362816)

Implications of the Artefact:

Artefact 5 has been accessed and altered within the same document as **Artefact 4** with both artefacts located in the same path. This artefact is significant to the investigation due to its content and the manner in which it was concealed. The image, resized to an extremely small scale adjacent to the covertly placed text ("**Broski these are the goods... get it!!!**") in **Artefact 4**, appears to depict the items that were reported stolen from Mr. Tsuyoshi's residence, implicating the suspect named Ken. By altering the image size to mimic a punctuation mark, the individual responsible has demonstrated a calculated approach to conceal the image. This act of concealment not only signifies a high degree of cunning and forethought but also serves as a potential digital fingerprint of the crime. The image's discovery and subsequent link to the stolen goods make it a crucial piece of evidence, establishing a connection between the hidden text, the suspect, and the burglary.

Method to hide/unhide artefact:

Further investigation into Artefact 4's document led to the discovery and extraction of a significantly downsized image, made to appear as a period. This tactic was used to hide a photograph of items sought by the individuals within the text of a Word document.



still there, I noticed my laptop had gone.

Broski these are the goods we need to steal; it's payday g. let's f&@king get it!!!

I came into the hall and my purse had gone, and obviously the car keys. When I had a little

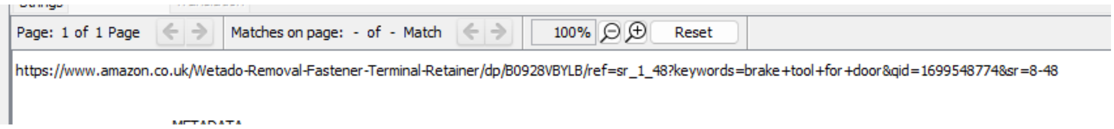
The type of Artefact

Hiding picture within a document

Artefact Detail Table

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

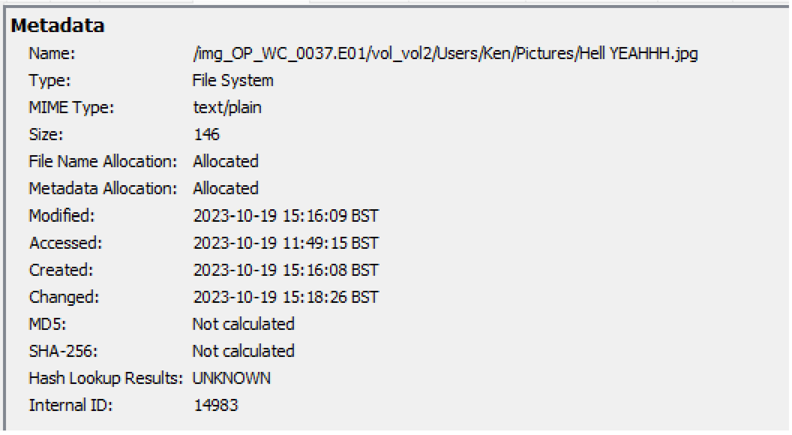
Artefact 6: Hell YEAHHH.jpg



https://www.amazon.co.uk/Wetado-Removal-Fastener-Terminal-Retainer/dp/B0928VBYLB/ref=sr_1_48?keywords=brake+tool+for+door&qid=1699548774&sr=8-48

Meta-Data of the artefact:

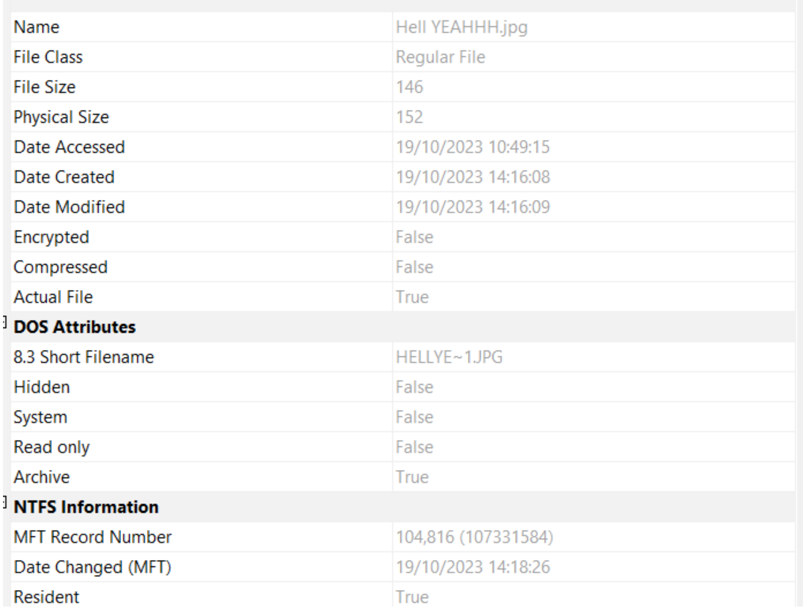
Meta-Data from Autopsy:



Metadata

Name:	/img_OP_WC_0037.E01/vol_vol2/Users/Ken/Pictures/Hell YEAHHH.jpg
Type:	File System
MIME Type:	text/plain
Size:	146
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2023-10-19 15:16:09 BST
Accessed:	2023-10-19 11:49:15 BST
Created:	2023-10-19 15:16:08 BST
Changed:	2023-10-19 15:18:26 BST
MD5:	Not calculated
SHA-256:	Not calculated
Hash Lookup Results:	UNKNOWN
Internal ID:	14983

Meta-Data from FTK Imager:



Name	Hell YEAHHH.jpg
File Class	Regular File
File Size	146
Physical Size	152
Date Accessed	19/10/2023 10:49:15
Date Created	19/10/2023 14:16:08
Date Modified	19/10/2023 14:16:09
Encrypted	False
Compressed	False
Actual File	True
DOS Attributes	
8.3 Short Filename	HELLYE~1.JPG
Hidden	False
System	False
Read only	False
Archive	True
NTFS Information	
MFT Record Number	104,816 (107331584)
Date Changed (MFT)	19/10/2023 14:18:26
Resident	True

Implications of the Artefact:

Artefact 6 is an image file titled "**Hell YEAHHH.jpg**" is stored at: Root/Users/Ken/Pictures, contains a possible amazon link referencing tools related with door locking, The potential implications need to be determined in relation to the referenced items. This alteration from text to image file format was likely done to conceal its purpose and avoid drawing attention. The presence of this link suggests it may detail the procurement method for the burglary tools utilized in the crime at Mr. Tsuyoshi's residence.

Method to hide/unhide artefact:

The text file containing the URL was not hidden in plain sight; however, it was camouflaged by changing its file extension to .jpg. This alteration made the file appear as an image rather than a text document, effectively disguising the nature of its content.

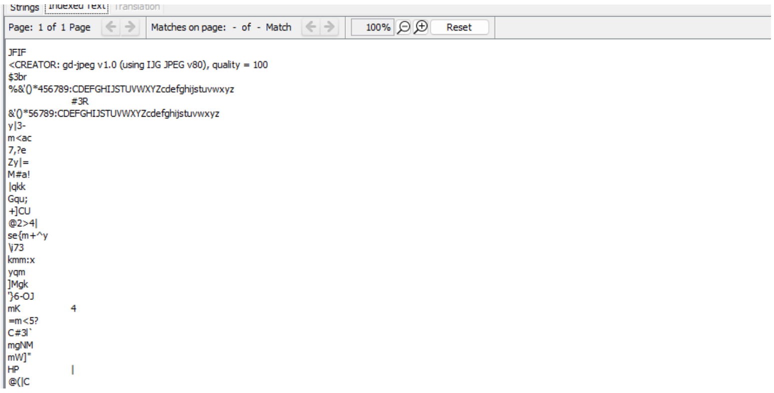
The type of Artefact

Manipulating file extensions

Artefact Detail Table

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

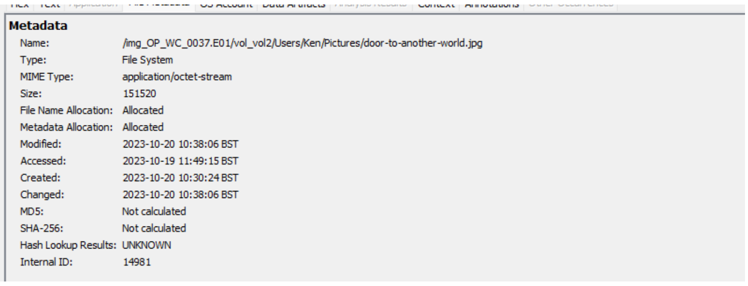
Artefact 7: door-to-another-world.jpg



```
JFIF
<CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 100
$3br
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
                #3R
&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
y|3-
m<ac
7,?e
Zy|=
M#a!
|qkk
Gqu;
+]CU
@2>4|
se{m+^y
\j73
kmm:x
yqm
]Mgk
'}6-OJ
mK              4
=m<5?
C#3l`
mgNM
mW]"
HP              |
@(|C
```

Meta-Data of the artefact:

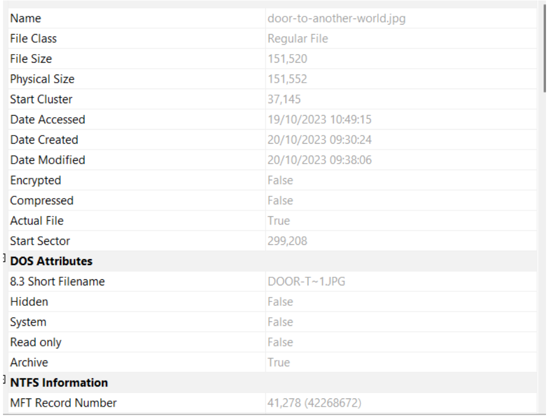
Meta-Data from Autopsy:



Metadata

Name:	/img_OP_WC_0037.E01/vol_vol2/Users/Ken/Pictures/door-to-another-world.jpg
Type:	File System
MIME Type:	application/octet-stream
Size:	151520
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2023-10-20 10:38:06 BST
Accessed:	2023-10-19 11:49:15 BST
Created:	2023-10-20 10:30:24 BST
Changed:	2023-10-20 10:38:06 BST
MD5:	Not calculated
SHA-256:	Not calculated
Hash Lookup Results:	UNKNOWN
Internal ID:	14981

Meta-Data from FTK Imager:



Name	door-to-another-world.jpg
File Class	Regular File
File Size	151,520
Physical Size	151,552
Start Cluster	37,145
Date Accessed	19/10/2023 10:49:15
Date Created	20/10/2023 09:30:24
Date Modified	20/10/2023 09:38:06
Encrypted	False
Compressed	False
Actual File	True
Start Sector	299,208
DOS Attributes	
8.3 Short Filename	DOOR-T~1.JPG
Hidden	False
System	False
Read only	False
Archive	True
NTFS Information	
MFT Record Number	41,278 (42268672)

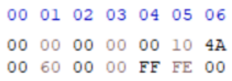
Implications of the Artefact:

The recovered **Artefact 7** is a file titled "**door-to-another-world.jpg**" revealed in an encrypted state attributed to file header alteration. Upon decryption, the image depicts a door, potentially representative of the victim's residence. Metadata shows the file was accessed and modified, suggesting deliberate efforts to interfere with its readability for system searches or forensic analysis.

Method to hide/unhide artefact:

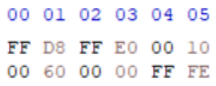
The JPEG file was corrupted by changing the file header's magic numbers to '**00 00 00 00**', which are typically used to identify the file format. This alteration can prevent the file from being recognized and opened by standard image viewers, effectively hiding its contents.

File header before the recovery and after the recovery:



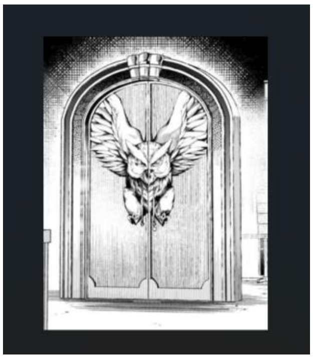
```
00 01 02 03 04 05 06
00 00 00 00 00 10 4A
00 60 00 00 FF FE 00
```

→



```
00 01 02 03 04 05
FF D8 FF E0 00 10
00 60 00 00 FF FE
```

After recovering the file header using HxD, it appears to be the front door of Mr. Tsuyoshi.



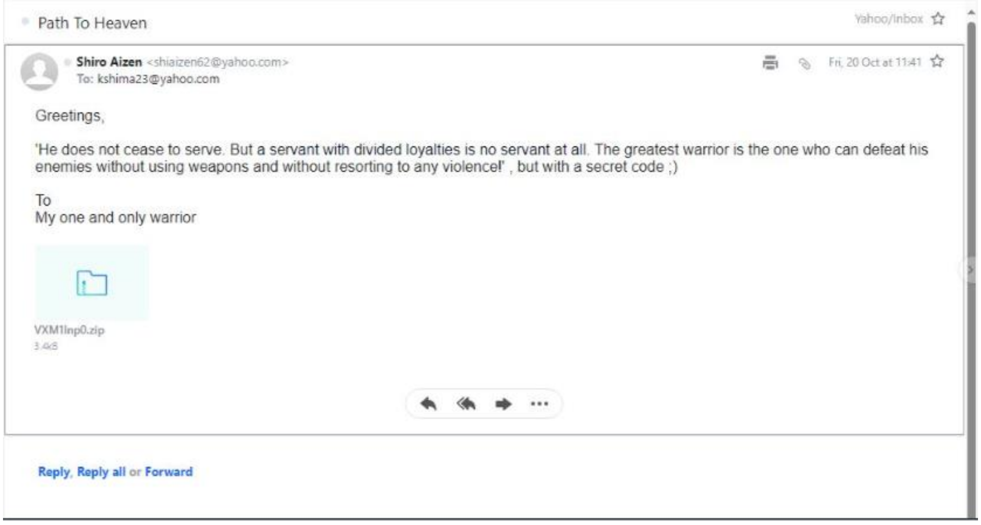
The type of Artefact

Manipulating file header to hide the file

Artefact Detail Table

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

Artefact 8: Path to Heaven.jpg



Path To Heaven

Yahoo/Inbox

Shiro Aizen <shiaizen62@yahoo.com>
To: kshima23@yahoo.com

Fri, 20 Oct at 11:41

Greetings,

'He does not cease to serve. But a servant with divided loyalties is no servant at all. The greatest warrior is the one who can defeat his enemies without using weapons and without resorting to any violence!' , but with a secret code ;)

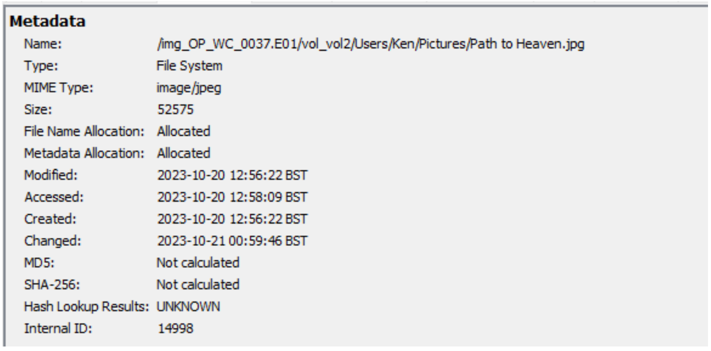
To
My one and only warrior

VXM1lnp0.zip
3.4kB

Reply, Reply all or Forward

Meta-Data of the artefact:

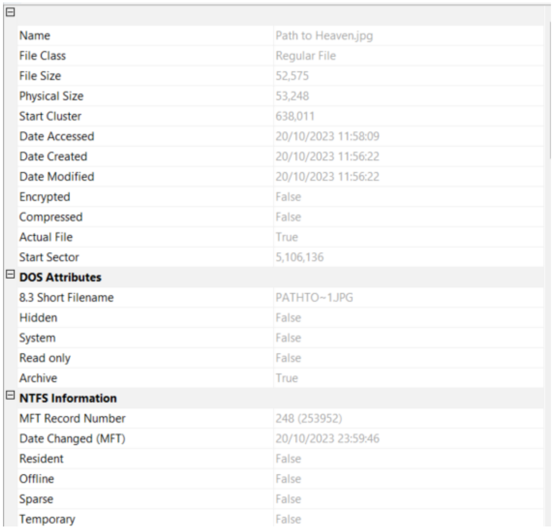
Meta-Data from Autopsy:



Metadata

Name:	/img_OP_WC_0037.E01/vol_vol2/Users/Ken/Pictures/Path to Heaven.jpg
Type:	File System
MIME Type:	image/jpeg
Size:	52575
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2023-10-20 12:56:22 BST
Accessed:	2023-10-20 12:58:09 BST
Created:	2023-10-20 12:56:22 BST
Changed:	2023-10-21 00:59:46 BST
MD5:	Not calculated
SHA-256:	Not calculated
Hash Lookup Results:	UNKNOWN
Internal ID:	14998

Meta-Data from FTK Imager:



Name	Path to Heaven.jpg
File Class	Regular File
File Size	52,575
Physical Size	53,248
Start Cluster	638,011
Date Accessed	20/10/2023 11:58:09
Date Created	20/10/2023 11:56:22
Date Modified	20/10/2023 11:56:22
Encrypted	False
Compressed	False
Actual File	True
Start Sector	5,106,136
DOS Attributes	
8.3 Short Filename	PATHTO~1.JPG
Hidden	False
System	False
Read only	False
Archive	True
NTFS Information	
MFT Record Number	248 (253952)
Date Changed (MFT)	20/10/2023 23:59:46
Resident	False
Offline	False
Sparse	False
Temporary	False

Implications of the Artefact:

Artefact 8 is a digital image named “**Path to Heaven.jpg**” is archived within the file directory: Root/Users/Ken/Picture, the image appears to depict an email and is held as potential evidence. The email, sent by Shiro to Ken Shima, employs coded language suggesting the successful advancement of their plans. Phrases such as 'secret code' and 'to my one and only warrior' indicate the message may contain veiled instructions or data intended for a targeted recipient involved in secretive operations. The presence of an attached zip file could signify that additional, encrypted information is being conveyed. This communication is critical as it establishes a direct link between Shiro and Ken Shima, potentially shedding light on the hierarchical structure of the group under investigation.

Method to hide/unhide artefact:

While the email content is not hidden, the use of metaphorical language and the attachment of a zip file may conceal information in plain sight, requiring decryption or contextual understanding to unveil the true message.

The type of Artefact

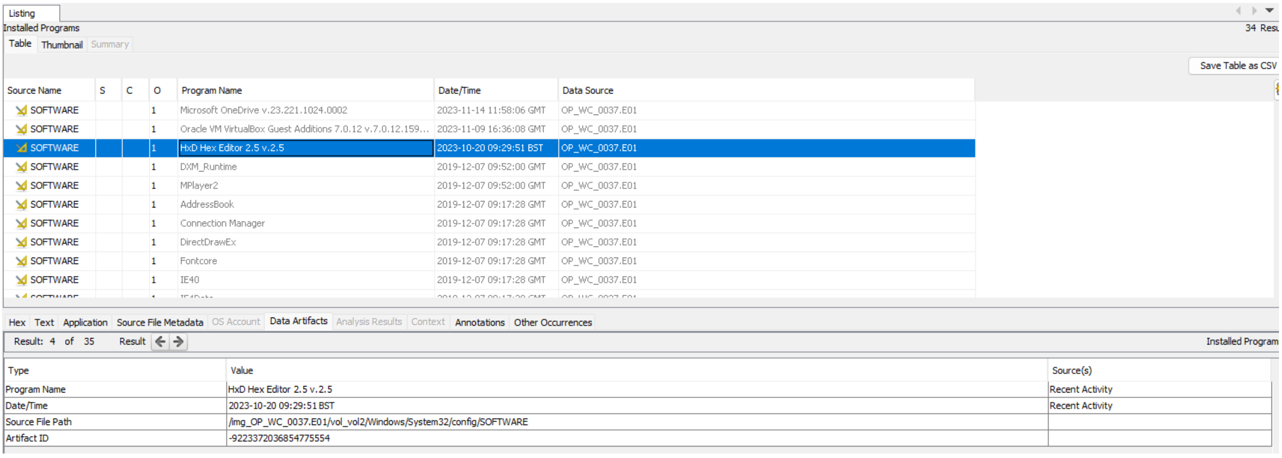
Email Artefact

Artefact Detail Table

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

Artefact 9: Installed Software

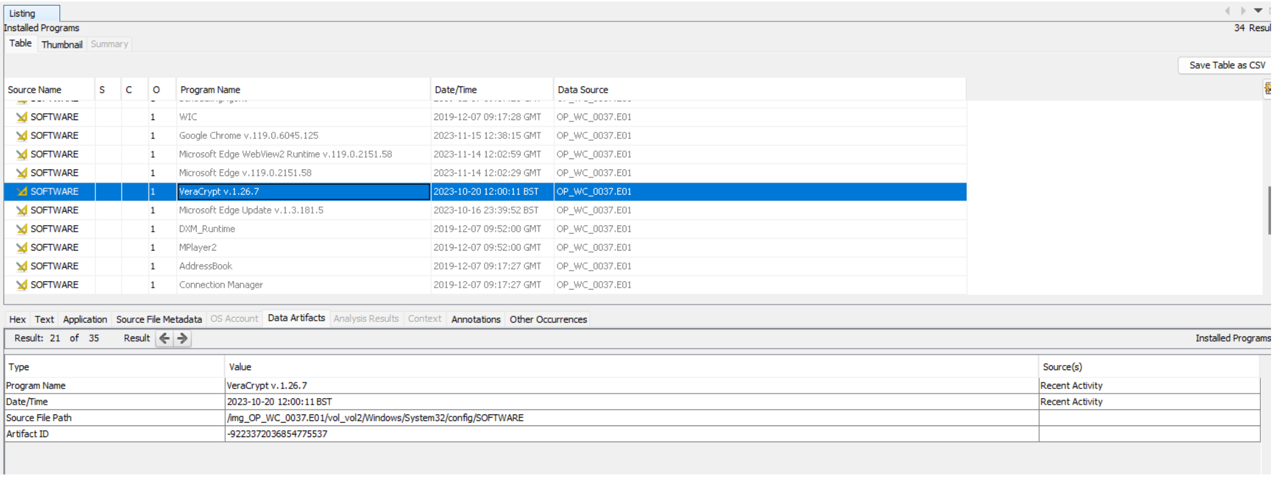
HxD Hex Editor2.5 v.2.5:



Source Name	S	C	O	Program Name	Date/Time	Data Source
SOFTWARE			1	Microsoft OneDrive v.23.221.1024.0002	2023-11-14 11:58:06 GMT	OP_WC_0037.E01
SOFTWARE			1	Oracle VM VirtualBox Guest Additions 7.0.12 v.7.0.12.159...	2023-11-09 16:36:08 GMT	OP_WC_0037.E01
SOFTWARE			1	HxD Hex Editor 2.5 v.2.5	2023-10-20 09:29:51 BST	OP_WC_0037.E01
SOFTWARE			1	DXM_Runtime	2019-12-07 09:52:00 GMT	OP_WC_0037.E01
SOFTWARE			1	MPlayer2	2019-12-07 09:52:00 GMT	OP_WC_0037.E01
SOFTWARE			1	AddressBook	2019-12-07 09:17:28 GMT	OP_WC_0037.E01
SOFTWARE			1	Connection Manager	2019-12-07 09:17:28 GMT	OP_WC_0037.E01
SOFTWARE			1	DirectDrawEx	2019-12-07 09:17:28 GMT	OP_WC_0037.E01
SOFTWARE			1	Fontcore	2019-12-07 09:17:28 GMT	OP_WC_0037.E01
SOFTWARE			1	IE40	2019-12-07 09:17:28 GMT	OP_WC_0037.E01

Type	Value	Source(s)
Program Name	HxD Hex Editor 2.5 v.2.5	Recent Activity
Date/Time	2023-10-20 09:29:51 BST	Recent Activity
Source File Path	/img_OP_WC_0037.E01/vol_vol2/Windows/System32/config/SOFTWARE	
Artifact ID	-9223372036854775554	

VeraCrypt v.1.26.7

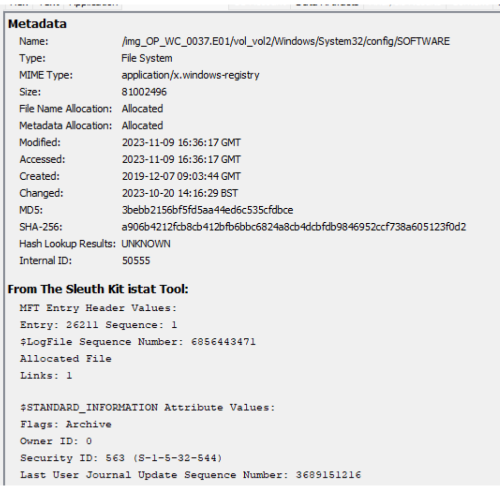


Source Name	S	C	O	Program Name	Date/Time	Data Source
SOFTWARE			1	WIC	2019-12-07 09:17:28 GMT	OP_WC_0037.E01
SOFTWARE			1	Google Chrome v.119.0.6045.125	2023-11-15 12:38:15 GMT	OP_WC_0037.E01
SOFTWARE			1	Microsoft Edge WebView2 Runtime v.119.0.2151.58	2023-11-14 12:02:59 GMT	OP_WC_0037.E01
SOFTWARE			1	Microsoft Edge v.119.0.2151.58	2023-11-14 12:02:29 GMT	OP_WC_0037.E01
SOFTWARE			1	VeraCrypt v.1.26.7	2023-10-20 12:00:11 BST	OP_WC_0037.E01
SOFTWARE			1	Microsoft Edge Update v.1.3.181.5	2023-10-16 23:39:52 BST	OP_WC_0037.E01
SOFTWARE			1	DXM_Runtime	2019-12-07 09:52:00 GMT	OP_WC_0037.E01
SOFTWARE			1	MPlayer2	2019-12-07 09:52:00 GMT	OP_WC_0037.E01
SOFTWARE			1	AddressBook	2019-12-07 09:17:27 GMT	OP_WC_0037.E01
SOFTWARE			1	Connection Manager	2019-12-07 09:17:27 GMT	OP_WC_0037.E01

Type	Value	Source(s)
Program Name	VeraCrypt v.1.26.7	Recent Activity
Date/Time	2023-10-20 12:00:11 BST	Recent Activity
Source File Path	/img_OP_WC_0037.E01/vol_vol2/Windows/System32/config/SOFTWARE	
Artifact ID	-9223372036854775537	

Meta-Data of the artefact:

Meta-Data of HxD Hex Editor 2.5 v.2.5 from Autopsy:



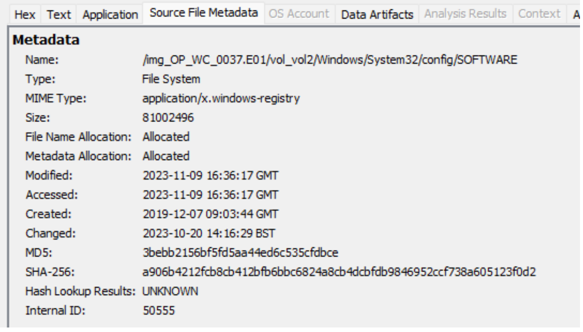
Metadata

Name:	/img_OP_WC_0037.E01/vol_vol2/Windows/System32/config/SOFTWARE
Type:	File System
MIME Type:	application/x.windows-registry
Size:	81002496
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2023-11-09 16:36:17 GMT
Accessed:	2023-11-09 16:36:17 GMT
Created:	2019-12-07 09:03:44 GMT
Changed:	2023-10-20 14:16:29 BST
MD5:	3bebb2156bf5fd5aa44ed6c535cfdbce
SHA-256:	a906b4212fcb8cb412bfb6bbc6824a8cb4dcbfdb9846952ccf738a605123f0d2
Hash Lookup Results:	UNKNOWN
Internal ID:	50555

From The Sleuth Kit istat Tool:

```
MFT Entry Header Values:
Entry: 26211 Sequence: 1
$LogFile Sequence Number: 6856443471
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Archive
Owner ID: 0
Security ID: 563 (S-1-5-32-544)
Last User Journal Update Sequence Number: 3689151216
```

Meta-Data of VeraCrypt v.1.26.7 from Autopsy:



```
Metadata
  Name:                   /img_OP_WC_0037.E01/vol_vol2/Windows/System32/config/SOFTWARE
  Type:                   File System
  MIME Type:              application/x.windows-registry
  Size:                   81002496
  File Name Allocation:   Allocated
  Metadata Allocation:    Allocated
  Modified:               2023-11-09 16:36:17 GMT
  Accessed:               2023-11-09 16:36:17 GMT
  Created:                2019-12-07 09:03:44 GMT
  Changed:                2023-10-20 14:16:29 BST
  MD5:                    3bebb2156bf5fd5aa44ed6c535cfdbce
  SHA-256:                a906b4212fcb8cb412bfb6bbc6824a8cb4dcbfdb9846952ccf738a605123f0d2
  Hash Lookup Results:    UNKNOWN
  Internal ID:            50555
```

Implications of the Artefact:

Upon forensic examination, **Artefact 9** possibly related to suspicious activities was revealed stored in the directory path: Windows/System32/config/SOFTWARE. The installation records of HxD Hex Editor and VeraCrypt software are indicative of potential involvement in the observed anomalies. Given that these artefacts were accessed and potentially used around the dates of interest in the investigation. The discovery of HxD Hex Editor and VeraCrypt as installed artefacts on the system reveals that the user could manipulate hexadecimal data and create encrypted containers, respectively.

Method to hide/unhide artefact:

The software was installed on the system and did not appear to be hidden.

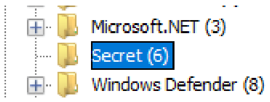
The type of Artefact

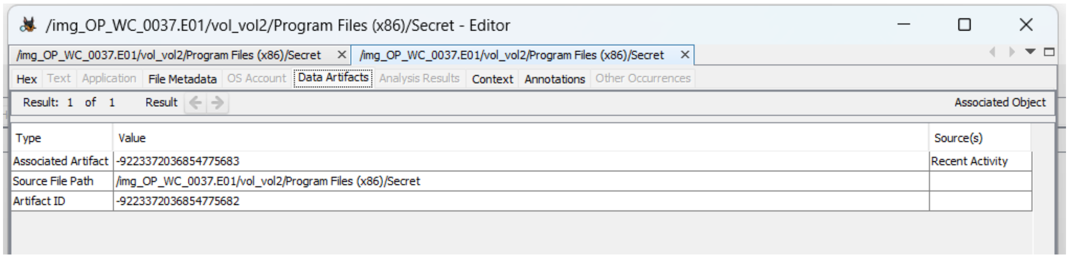
Registry Information – Installed software

Artefact Detail Table

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

Artefact 10: Secret



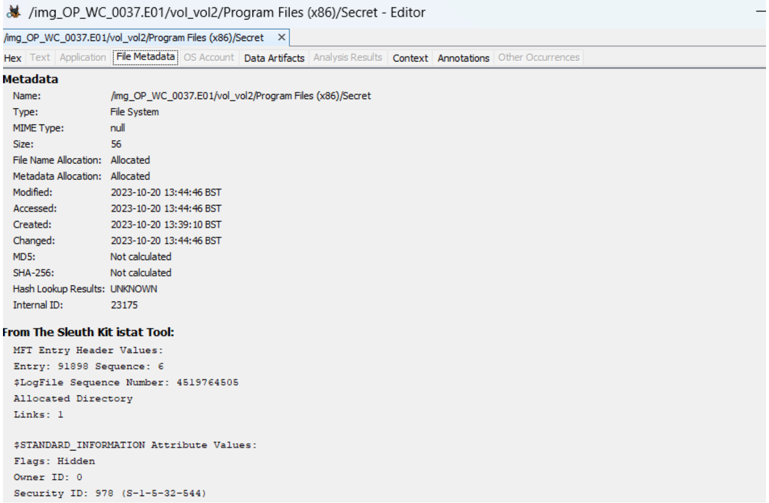


/img_OP_WC_0037.E01/vol_vol2/Program Files (x86)/Secret - Editor

Type	Value	Source(s)
Associated Artifact	-9223372036854775683	Recent Activity
Source File Path	/img_OP_WC_0037.E01/vol_vol2/Program Files (x86)/Secret	
Artifact ID	-9223372036854775682	

Meta-Data of the artefact:

Meta-Data from Autopsy:



/img_OP_WC_0037.E01/vol_vol2/Program Files (x86)/Secret - Editor

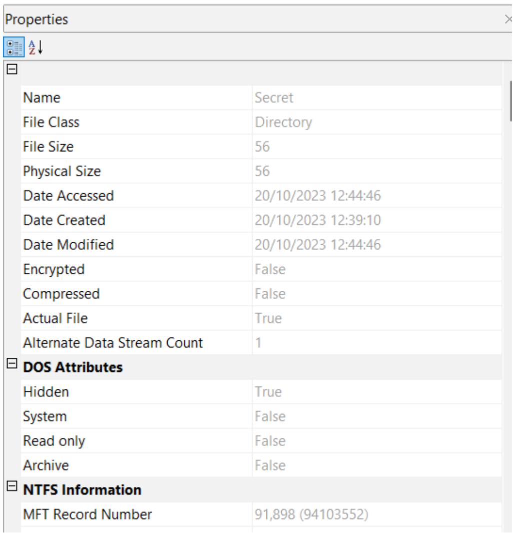
Metadata

Name:	/img_OP_WC_0037.E01/vol_vol2/Program Files (x86)/Secret
Type:	File System
MIME Type:	null
Size:	56
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2023-10-20 13:44:46 BST
Accessed:	2023-10-20 13:44:46 BST
Created:	2023-10-20 13:39:10 BST
Changed:	2023-10-20 13:44:46 BST
MD5:	Not calculated
SHA-256:	Not calculated
Hash Lookup Results:	UNKNOWN
Internal ID:	23175

From The Sleuth Kit istat Tool:

```
MFT Entry Header Values:
Entry: 91898 Sequence: 6
$LogFile Sequence Number: 4519764505
Allocated Directory
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden
Owner ID: 0
Security ID: 978 (S-1-5-32-544)
```

Meta-Data from FTK Imager:

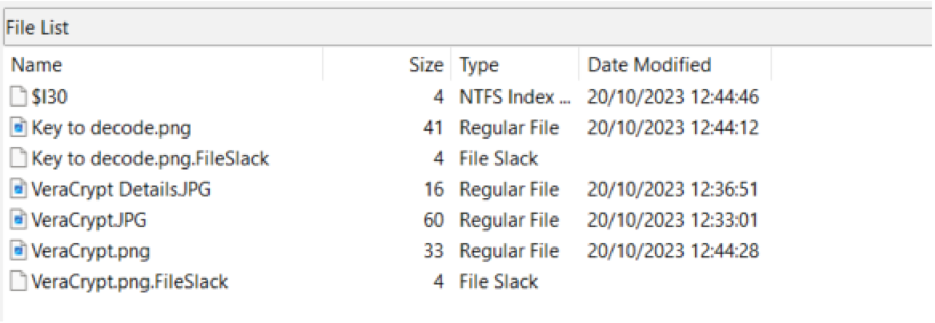


Properties

Name	Secret
File Class	Directory
File Size	56
Physical Size	56
Date Accessed	20/10/2023 12:44:46
Date Created	20/10/2023 12:39:10
Date Modified	20/10/2023 12:44:46
Encrypted	False
Compressed	False
Actual File	True
Alternate Data Stream Count	1
DOS Attributes	
Hidden	True
System	False
Read only	False
Archive	False
NTFS Information	
MFT Record Number	91,898 (94103552)

Implications of the Artefact:

The folder named ‘**Secret**,’ designated as **Artefact 10** discovered in the directory: ‘Program Files (x86)/Secret’ of the operating system's storage device. Initially hidden manually, the folder had been accessed by the suspect, indicating that its contents were relevant to the investigation. Within this folder, there are several files, specifically with ‘.png’ and ‘.jpg’ extensions, that bear names indicative of encryption and encoding tools, such as VeraCrypt and CyberChef. The presence of such files implies that they may contain sensitive information stored in an encrypted form, which could be critical to the investigation. Notably, files titled 'Key to decode.png' and 'VeraCrypt Details.JPG' were found within this 'Secret' folder. Their names suggest that they could contain necessary decryption keys or provide instructions for decrypting other encrypted files related to the case.



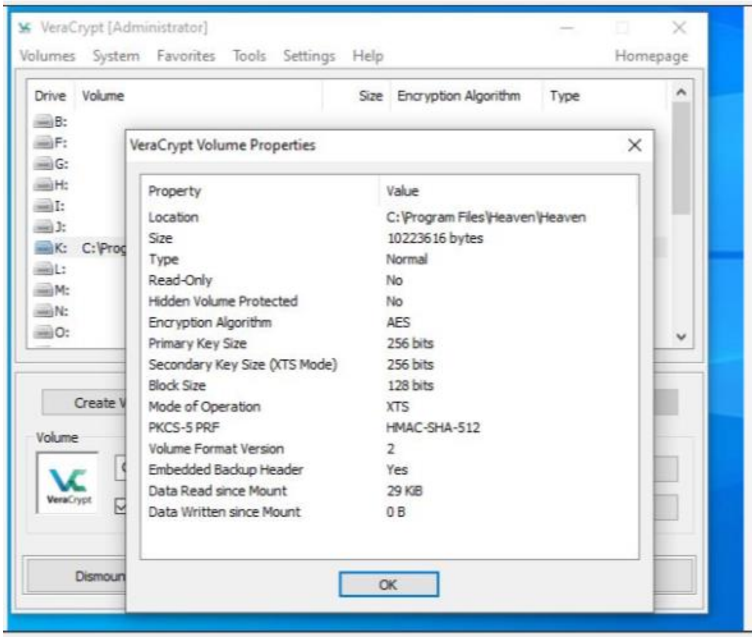
File List

Name	Size	Type	Date Modified
$I30	4	NTFS Index ...	20/10/2023 12:44:46
Key to decode.png	41	Regular File	20/10/2023 12:44:12
Key to decode.png.FileSlack	4	File Slack	
VeraCrypt Details.JPG	16	Regular File	20/10/2023 12:36:51
VeraCrypt.JPG	60	Regular File	20/10/2023 12:33:01
VeraCrypt.png	33	Regular File	20/10/2023 12:44:28
VeraCrypt.png.FileSlack	4	File Slack	

Method to hide/unhide artefact:

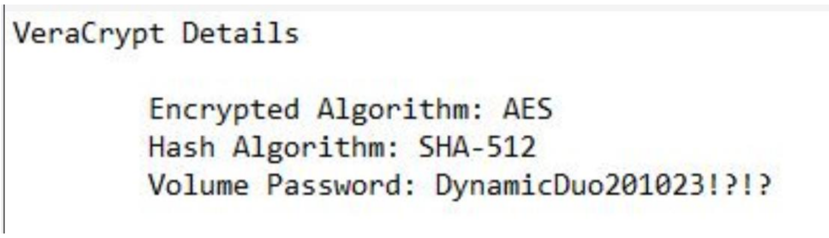
The 'Secret' folder was hidden using the operating system’s functionality to conceal files and folders. This was accomplished by setting the 'hidden' attribute within the file or folder properties, which is a common method to obscure files from a typical user's view. The folder contains files that are not immediately apparent to an investigator without the knowledge that hidden files must be revealed or by using forensic tools to scan for such hidden items. The 'Secret' folder's contents, including 'Key to decode.png', 'VeraCrypt Details.JPG', and other image files, could be instrumental in decoding encrypted data pertinent to the investigation. The file has been provided below:

VeraCrypt.JPG


VeraCrypt [Administrator]
Volumes System Favorites Tools Settings Help Homepage
Drive Volume Size Encryption Algorithm Type
B:
F:
G:
H:
I:
J:
K: C:\Prog
L:
M:
N:
O:
Create V
Volume
Dismoun
VeraCrypt Volume Properties
OK

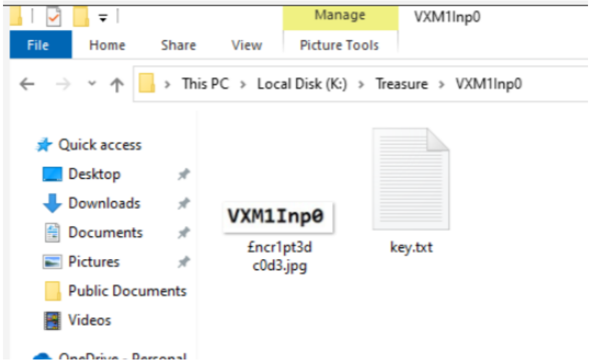
Property	Value
Location	C:\Program Files\Heaven\Heaven
Size	10223616 bytes
Type	Normal
Read-Only	No
Hidden Volume Protected	No
Encryption Algorithm	AES
Primary Key Size	256 bits
Secondary Key Size (XTS Mode)	256 bits
Block Size	128 bits
Mode of Operation	XTS
PKCS-5 PRF	HMAC-SHA-512
Volume Format Version	2
Embedded Backup Header	Yes
Data Read since Mount	29 KiB
Data Written since Mount	0 B

VeraCrypt Details.JPG

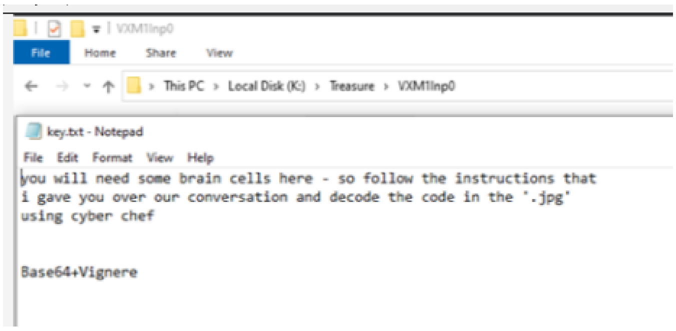


```
VeraCrypt Details

        Encrypted Algorithm: AES
        Hash Algorithm: SHA-512
        Volume Password: DynamicDuo201023!?!?
```

VerCrypt.png



Key to decode.png



VXM1lnp0
File
Home
Share
View
This PC › Local Disk (K:) › Treasure › VXM1lnp0
key.txt - Notepad
File Edit Format View Help

```
you will need some brain cells here - so follow the instructions that
i gave you over our conversation and decode the code in the '.jpg'
using cyber chef


Base64+Vignere
```

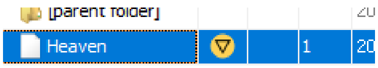
The type of Artefact

The 'hidden' flag within an operating system

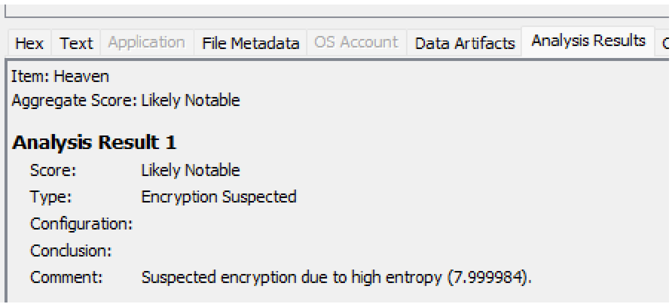
Artefact Detail Table

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

Artefact 11: Heaven



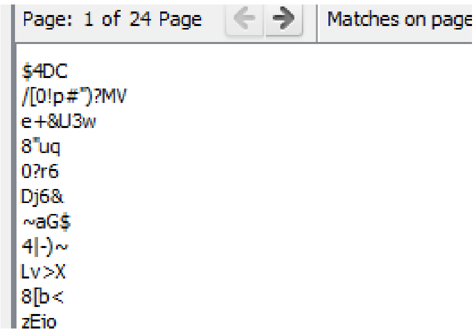
[parent folder]			20
Heaven	▽	1	20



Item: Heaven
Aggregate Score: Likely Notable

Analysis Result 1

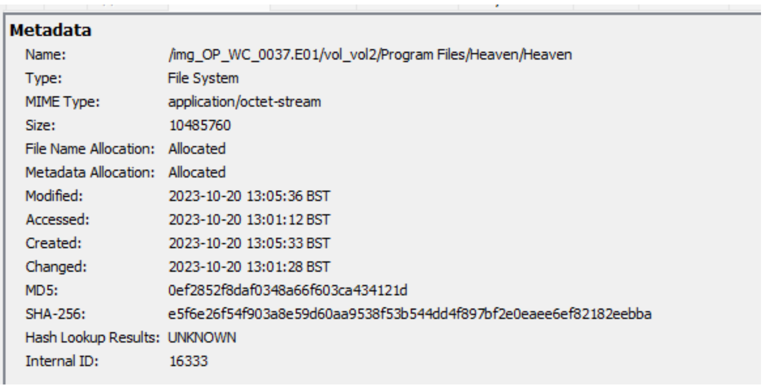
Score:	Likely Notable
Type:	Encryption Suspected
Configuration:	
Conclusion:	
Comment:	Suspected encryption due to high entropy (7.999984).



```
$4DC
/[0!p#")?MV
e+&U3w
8"uq
0?r6
Dj6&
~aG$
4|-)~
Lv>X
8[b<
zEio
```

Meta-Data of the artefact:

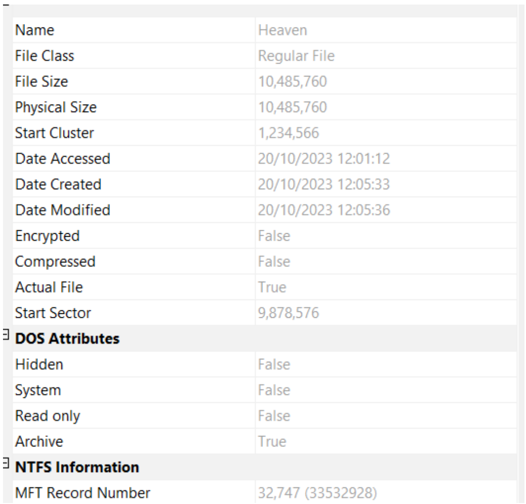
Meta-Data of Heaven from Autopsy:



Metadata

Name:	/img_OP_WC_0037.E01/vol_vol2/Program Files/Heaven/Heaven
Type:	File System
MIME Type:	application/octet-stream
Size:	10485760
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2023-10-20 13:05:36 BST
Accessed:	2023-10-20 13:01:12 BST
Created:	2023-10-20 13:05:33 BST
Changed:	2023-10-20 13:01:28 BST
MD5:	0ef2852f8daf0348a66f603ca434121d
SHA-256:	e5f6e26f54f903a8e59d60aa9538f53b544dd4f897bf2e0eaee6ef82182eebba
Hash Lookup Results:	UNKNOWN
Internal ID:	16333

Meta-Data of Heaven from FTK Imager:



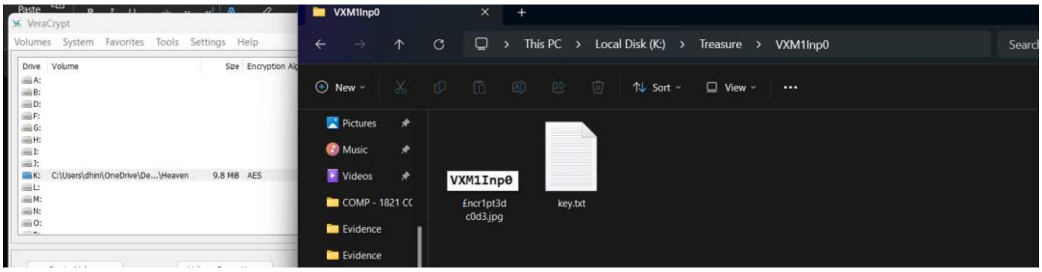
Name	Heaven
File Class	Regular File
File Size	10,485,760
Physical Size	10,485,760
Start Cluster	1,234,566
Date Accessed	20/10/2023 12:01:12
Date Created	20/10/2023 12:05:33
Date Modified	20/10/2023 12:05:36
Encrypted	False
Compressed	False
Actual File	True
Start Sector	9,878,576
DOS Attributes	
Hidden	False
System	False
Read only	False
Archive	True
NTFS Information	
MFT Record Number	32,747 (33532928)

Implications of the Artefact:

Artefact 11, named '**Heaven**', is a file with high entropy, suggesting encryption, and was last accessed and modified on the date coinciding with the investigation timeline. Located in the program files directory, it appears to be an encrypted file within a VeraCrypt volume on drive K: as inferred from the 'VeraCrypt.jpg' found within the previously mentioned 'Secret' folder (**Artefact 10**). The 'VeraCrypt.JPG' may contain the password for this volume, linking its encryption to the VeraCrypt software installed on the system, version 1.26.7, as evidenced by **Artefact 9**. This connection between the artefacts suggests deliberate obfuscation and encryption of the 'Heaven' file, likely to conceal its contents, and indicates the necessity of decrypting this file to advance the investigation.

Method to hide/unhide artefact:

The 'Heaven' file was purposefully encrypted and stored within a VeraCrypt volume to conceal it from unauthorized access. Artefacts related to the installation of VeraCrypt software and image files potentially containing encryption keys or passwords suggest deliberate measures were taken to secure the file. In particular, the password '**DynamicDuo201023!?!?**' found in the '**VeraCrypt Details.JPG**' image file (**Artefact 10**) was contributory in recovering the encrypted 'Heaven' file. This password enabled the decryption of the volume, revealing the previously inaccessible file, and demonstrating an advanced level of concealment and sophistication in the methods used to hide critical data.



Drive	Volume	Size	Encryption Al
A:			
B:			
D:			
F:			
G:			
H:			
I:			
J:			
K:	C:\Users\dhini\OneDrive\De...\Heaven	9.8 MiB	AES
L:			
M:			
N:			
O:			

The type of Artefact

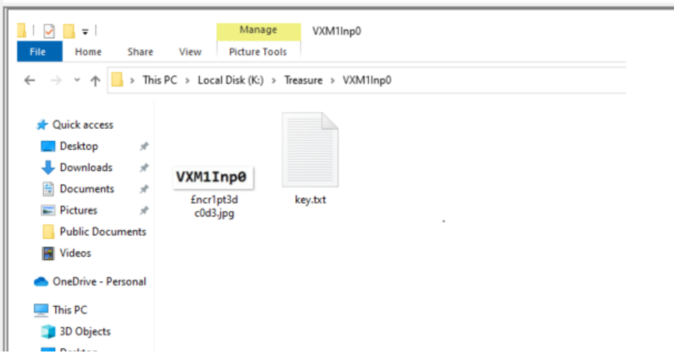
Encrypted Password protected container

Artefact Detail Table

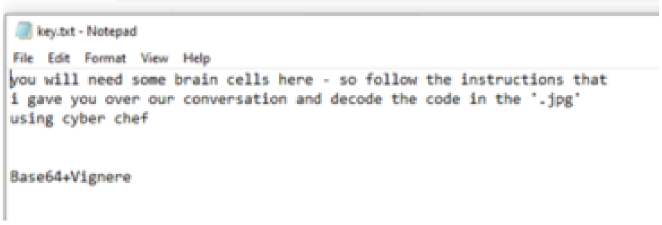
Artefact is	**Tick Appropriate**
Application Level	✓
OS Level	
File System Level	✓
Reconnaissance / Research phase	✓
Recording phase	
Result / Aftermath phase	

Artefact 12: VeraCrypt.png & Key to decode.png

VeraCrypt.png



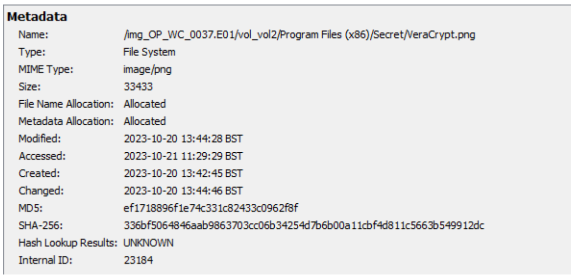
Key to decode.png



```
you will need some brain cells here - so follow the instructions that
i gave you over our conversation and decode the code in the '.jpg'
using cyber chef


Base64+Vignere
```

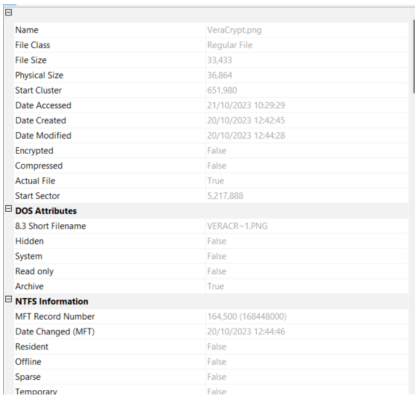
Meta-Data of the artefact:

Meta-Data of VeraCrypt.png from Autopsy:



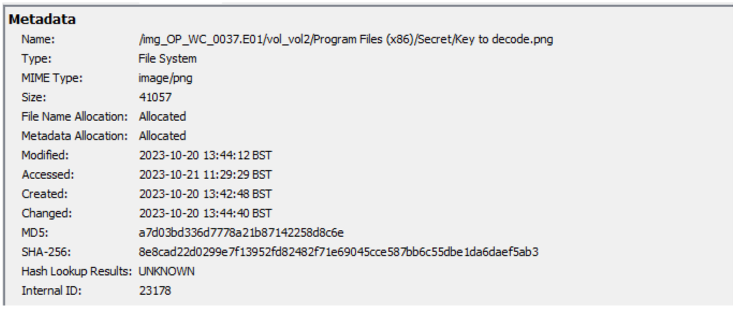
Metadata	
Name:	/img_OP_WC_0037.E01/vol_vol2/Program Files (x86)/Secret/VeraCrypt.png
Type:	File System
MIME Type:	image/png
Size:	33433
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2023-10-20 13:44:28 BST
Accessed:	2023-10-21 11:29:29 BST
Created:	2023-10-20 13:42:45 BST
Changed:	2023-10-20 13:44:46 BST
MD5:	ef1718896f1e74c331c82433c0962f8f
SHA-256:	336bf5064846aab9863703cc06b34254d7b6b00a11cbf4d811c5663b549912dc
Hash Lookup Results:	UNKNOWN
Internal ID:	23184

Meta-Data of VeraCrypt.png from FTK Imager:



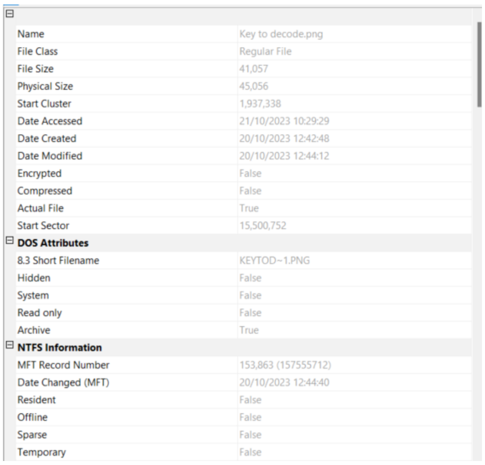
Name	VeraCrypt.png
File Class	Regular File
File Size	33,433
Physical Size	36,864
Start Cluster	651,980
Date Accessed	21/10/2023 10:29:29
Date Created	20/10/2023 12:42:45
Date Modified	20/10/2023 12:44:28
Encrypted	False
Compressed	False
Actual File	True
Start Sector	5,217,888
DOS Attributes	
8.3 Short Filename	VERACR~1.PNG
Hidden	False
System	False
Read only	False
Archive	True
NTFS Information	
MFT Record Number	164,500 (168448000)
Date Changed (MFT)	20/10/2023 12:44:46
Resident	False
Offline	False
Sparse	False
Temporary	False

Meta-Data of Key to decode.png from Autopsy:



```
Metadata
  Name:                  /img_OP_WC_0037.E01/vol_vol2/Program Files (x86)/Secret/Key to decode.png
  Type:                  File System
  MIME Type:             image/png
  Size:                  41057
  File Name Allocation:  Allocated
  Metadata Allocation:   Allocated
  Modified:              2023-10-20 13:44:12 BST
  Accessed:              2023-10-21 11:29:29 BST
  Created:               2023-10-20 13:42:48 BST
  Changed:               2023-10-20 13:44:40 BST
  MD5:                   a7d03bd336d7778a21b87142258d8c6e
  SHA-256:               8e8cad22d0299e7f13952fd82482f71e69045cce587bb6c55dbe1da6daef5ab3
  Hash Lookup Results:   UNKNOWN
  Internal ID:           23178
```

Meta-Data of Key to decode.png from FTK Imager:



Name	Key to decode.png
File Class	Regular File
File Size	41,057
Physical Size	45,056
Start Cluster	1,937,338
Date Accessed	21/10/2023 10:29:29
Date Created	20/10/2023 12:42:48
Date Modified	20/10/2023 12:44:12
Encrypted	False
Compressed	False
Actual File	True
Start Sector	15,500,752
DOS Attributes	
8.3 Short Filename	KEYTOD~1.PNG
Hidden	False
System	False
Read only	False
Archive	True
NTFS Information	
MFT Record Number	153,863 (157555712)
Date Changed (MFT)	20/10/2023 12:44:40
Resident	False
Offline	False
Sparse	False
Temporary	False

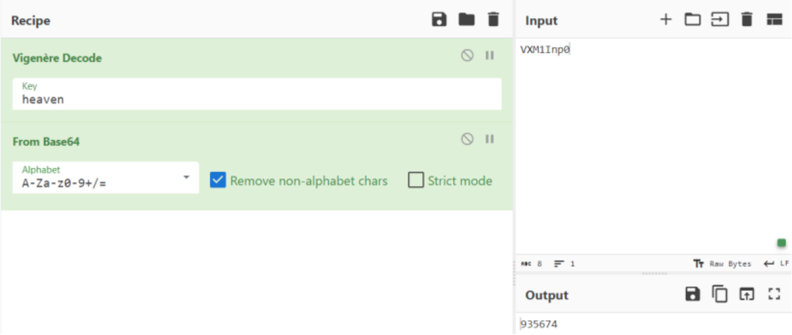
Implications of the Artefact:

Artefact 12 involves the encoded file '**£ncr1pt3d c0d3.jpg**', which is suspected to contain the pin for Mr. Tsuyoshi's door based on the investigation findings. The '**Key to decode.png**' provided instructions for decoding, specifying the use of **Base64** and **Vigenère cipher** algorithms as outlined in a note. This file was revealed by examining 'VeraCrypt.png' from **Artefact 10**, which indicated its encrypted state within a VeraCrypt volume. The successful application of the mentioned cryptographic algorithms to the content of '**£ncr1pt3d c0d3.jpg**' led to the discovery of the pin code, which is a significant breakthrough in the investigation, linking the digital evidence directly to a physical security breach.

Method to hide/unhide artefact:

The '**£ncr1pt3d c0d3.jpg**' file was encrypted within a VeraCrypt volume, details of which were found in the '**VeraCrypt.png**'. Instructions in the **'Key to decode.png**' file, both hidden in the '**Secret**' folder (**Artefact 10**), outlined the decryption method using **Base64** and **Vigenère**

ciphers key is the name of the encrypted file named ‘**Heaven**’ (More on **Artefact 11**). Decoding the '**£ncr1pt3d c0d3.jpg**' file revealed it to contain the pin for Mr. Tsuyoshi's door, showcasing a deliberate strategy to shield this sensitive information.



Vigenère Decode
Key: heaven

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

```
VXM1Inp0
```

```
935674
```

The type of Artefact

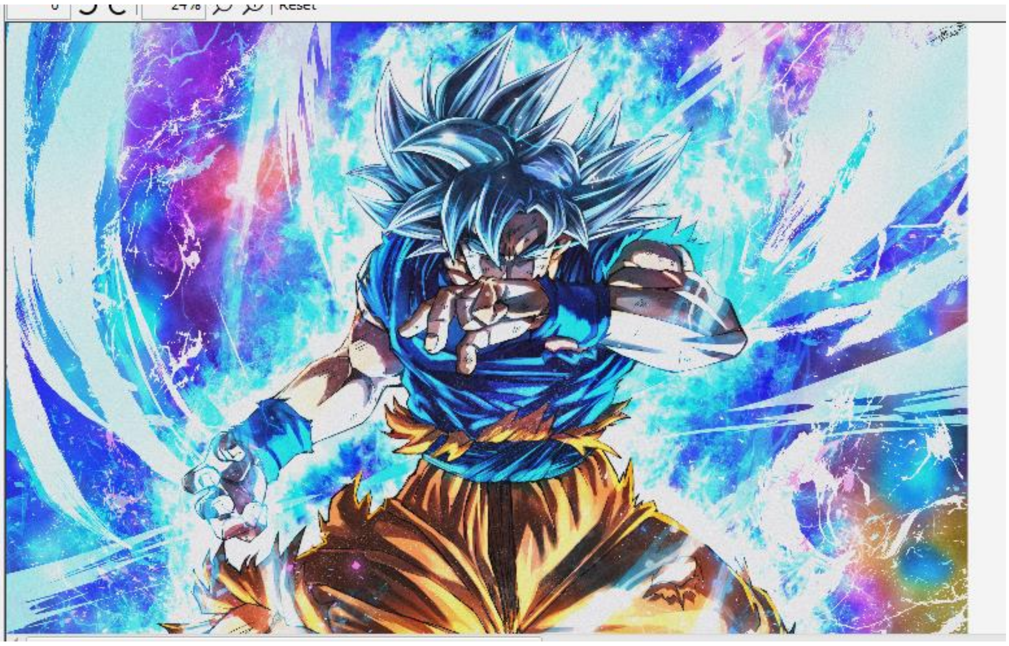
Encoded Text

Artefact Detail Table

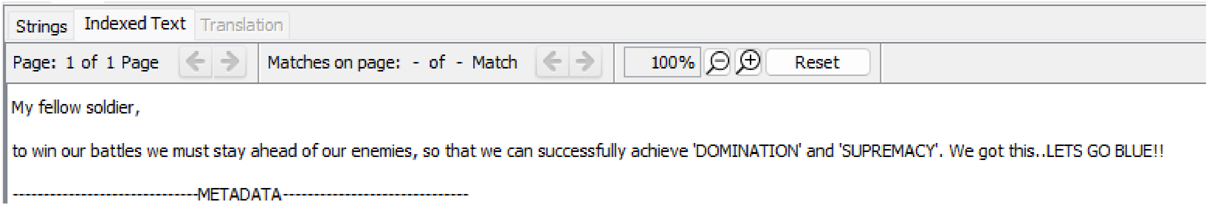
Artefact is	**Tick Appropriate**
Application Level	✓
OS Level	
File System Level	
Reconnaissance / Research phase	✓
Recording phase	
Result / Aftermath phase	

Artefact 13: LETS GO BLUE

LETS GO BLUE.jpg



Heaven.txt



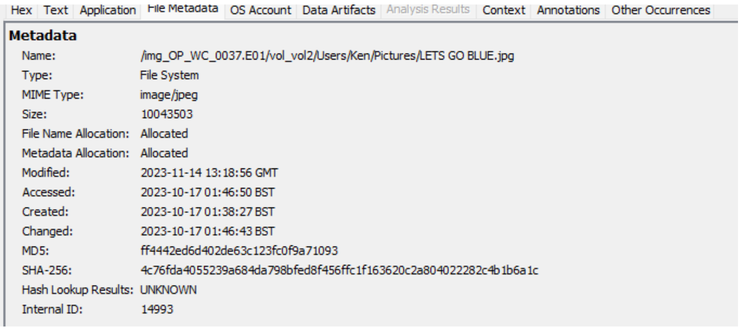
My fellow soldier,

to win our battles we must stay ahead of our enemies, so that we can successfully achieve 'DOMINATION' and 'SUPREMACY'. We got this..LETS GO BLUE!!

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

Meta-Data of the artefact:

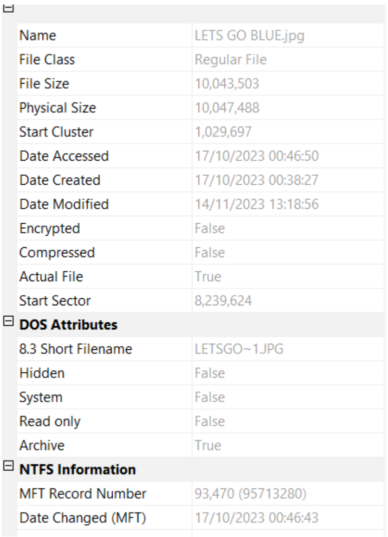
Meta-Data of LETS GO BLUE.jpg from Autopsy:



Metadata

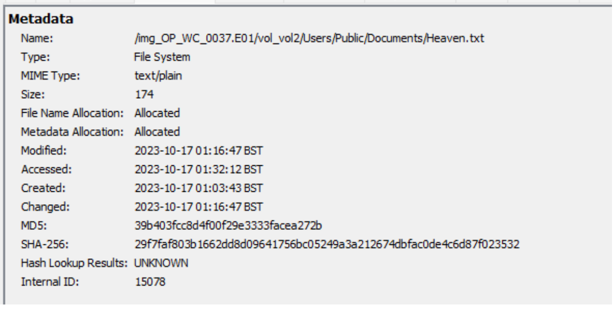
```
Name:                  /img_OP_WC_0037.E01/vol_vol2/Users/Ken/Pictures/LETS GO BLUE.jpg
Type:                  File System
MIME Type:             image/jpeg
Size:                  10043503
File Name Allocation:  Allocated
Metadata Allocation:   Allocated
Modified:              2023-11-14 13:18:56 GMT
Accessed:              2023-10-17 01:46:50 BST
Created:               2023-10-17 01:38:27 BST
Changed:               2023-10-17 01:46:43 BST
MD5:                   ff4442ed6d402de63c123fc0f9a71093
SHA-256:               4c76fda4055239a684da798bfed8f456ffc1f163620c2a804022282c4b1b6a1c
Hash Lookup Results:   UNKNOWN
Internal ID:           14993
```

Meta-Data of LETS GO BLUE.jpg from FTK Imager:



Name	LETS GO BLUE.jpg
File Class	Regular File
File Size	10,043,503
Physical Size	10,047,488
Start Cluster	1,029,697
Date Accessed	17/10/2023 00:46:50
Date Created	17/10/2023 00:38:27
Date Modified	14/11/2023 13:18:56
Encrypted	False
Compressed	False
Actual File	True
Start Sector	8,239,624
DOS Attributes	
8.3 Short Filename	LETSGO~1.JPG
Hidden	False
System	False
Read only	False
Archive	True
NTFS Information	
MFT Record Number	93,470 (95713280)
Date Changed (MFT)	17/10/2023 00:46:43

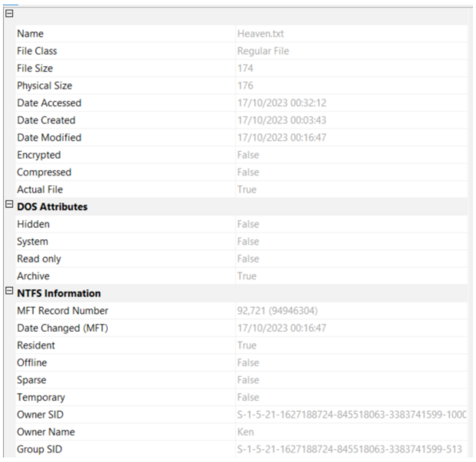
Meta-Data of Heaven.txt from Autopsy:



Metadata

Name:	/img_OP_WC_0037.E01/vol_vol2/Users/Public/Documents/Heaven.txt
Type:	File System
MIME Type:	text/plain
Size:	174
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2023-10-17 01:16:47 BST
Accessed:	2023-10-17 01:32:12 BST
Created:	2023-10-17 01:03:43 BST
Changed:	2023-10-17 01:16:47 BST
MD5:	39b403fcc8d4f00f29e3333facea272b
SHA-256:	29f7faf803b1662dd8d09641756bc05249a3a212674dbfac0de4c6d87f023532
Hash Lookup Results:	UNKNOWN
Internal ID:	15078

Meta-Data of Heaven.txt from FTK Imager:



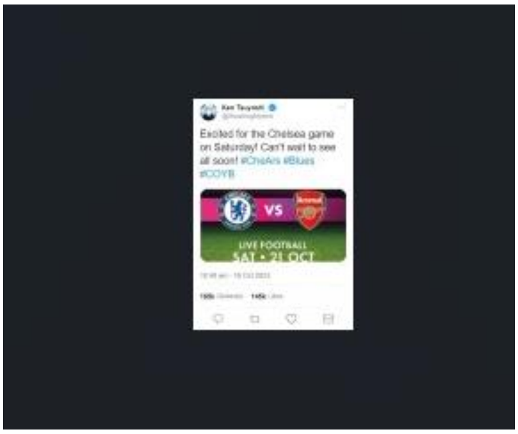
Name	Heaven.txt
File Class	Regular File
File Size	174
Physical Size	176
Date Accessed	17/10/2023 00:32:12
Date Created	17/10/2023 00:03:43
Date Modified	17/10/2023 00:16:47
Encrypted	False
Compressed	False
Actual File	True
DOS Attributes	
Hidden	False
System	False
Read only	False
Archive	True
NTFS Information	
MFT Record Number	92,721 (94946304)
Date Changed (MFT)	17/10/2023 00:16:47
Resident	True
Offline	False
Sparse	False
Temporary	False
Owner SID	S-1-5-21-1627188724-845518063-3383741599-100C
Owner Name	Ken
Group SID	S-1-5-21-1627188724-845518063-3383741599-513

Implications of the Artefact:

Artefact 13 is associated with a '**heaven.txt**' file that contains the phrase '**LETS GO BLUE!!!**' and capitalized words '**DOMINATION**' and '**SUPREMACY**'. This 'txt' file led to the discovery of a 'jpg' file named '**LETS GO BLUE.JPG**', which was flagged for modification. OpenPuff, a steganography software found installed on the system, suggests the 'jpg' file may contain hidden data. The emphasis on the two capitalized words hints they may serve as passwords for revealing the concealed content. This is particularly relevant to the investigation as it ties to Mr. Tsuyoshi's intended attendance at a Premier League match and the date of the burglary.

Method to hide/unhide artefact:

The artefact involved concealing a Twitter post inside '**LETS GO BLUE.JPG**' using steganography via OpenPuff, with '**DOMINATION**' and '**SUPREMACY**' as passwords. This method was sophisticated yet traceable through the associated '**heaven.txt**' file and the OpenPuff software, linking digital traces to the physical crime.



Ken Tsuyoshi

Excited for the Chelsea game on Saturday! Can't wait to see all soon! #CheArs #Blues #COYB

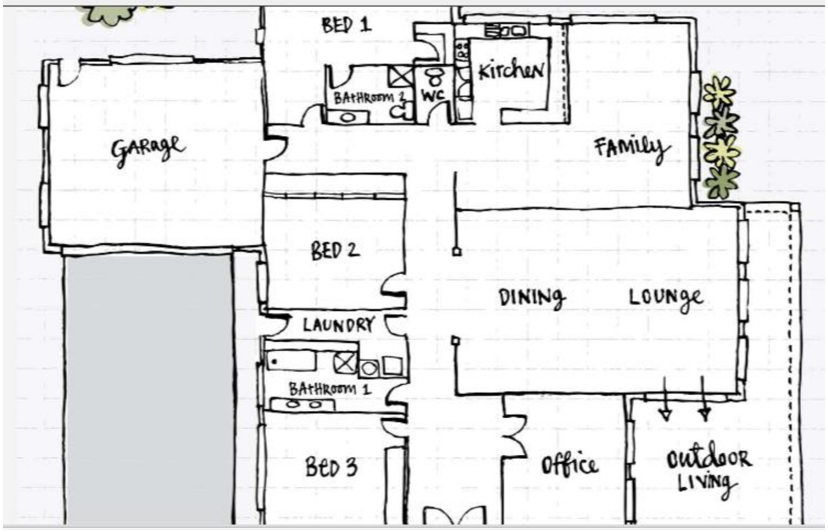
The type of Artefact

Steg of Pictures

Artefact Detail Table

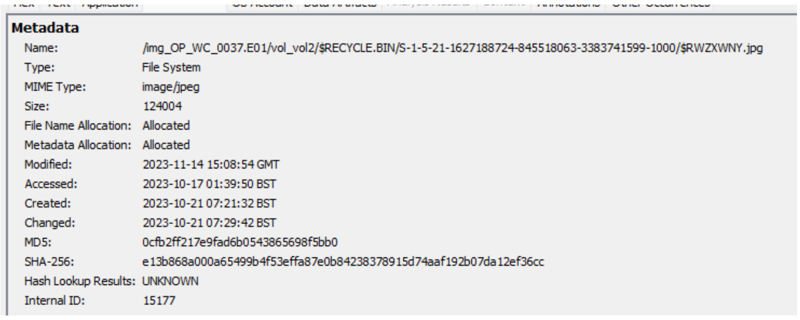
Artefact is	Tick Appropriate
Application Level	✓
OS Level	
File System Level	
Reconnaissance / Research phase	✓
Recording phase	✓
Result / Aftermath phase	

Artefact 14: $RWZXWNY.jpg



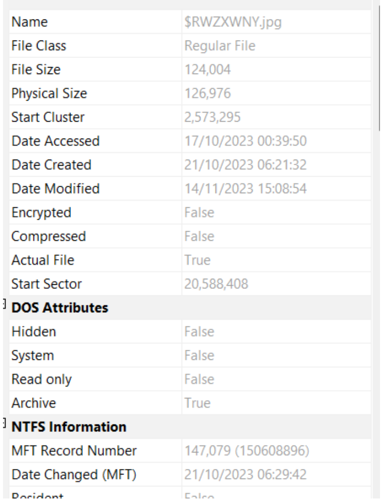
Meta-Data of the artefact:

Mega-Data from Autopsy:



```
Metadata
  Name:                   /img_OP_WC_0037.E01/vol_vol2/$RECYCLE.BIN/S-1-5-21-1627188724-845518063-3383741599-1000/$RWZXWNY.jpg
  Type:                   File System
  MIME Type:              image/jpeg
  Size:                   124004
  File Name Allocation:   Allocated
  Metadata Allocation:    Allocated
  Modified:               2023-11-14 15:08:54 GMT
  Accessed:               2023-10-17 01:39:50 BST
  Created:                2023-10-21 07:21:32 BST
  Changed:                2023-10-21 07:29:42 BST
  MD5:                    0cfb2ff217e9fad6b0543865698f5bb0
  SHA-256:                e13b868a000a65499b4f53effa87e0b84238378915d74aaf192b07da12ef36cc
  Hash Lookup Results:    UNKNOWN
  Internal ID:            15177
```

Mega-Data from FTK Imager:



Name	$RWZXWNY.jpg
File Class	Regular File
File Size	124,004
Physical Size	126,976
Start Cluster	2,573,295
Date Accessed	17/10/2023 00:39:50
Date Created	21/10/2023 06:21:32
Date Modified	14/11/2023 15:08:54
Encrypted	False
Compressed	False
Actual File	True
Start Sector	20,588,408
DOS Attributes	
Hidden	False
System	False
Read only	False
Archive	True
NTFS Information	
MFT Record Number	147,079 (150608896)
Date Changed (MFT)	21/10/2023 06:29:42
Resident	False

Implications of the Artefact:

Artefact 14, an image file found in the **Recycle Bin**, is a sketch of Mr. Tsuyoshi's house layout. The file's recovery from the Recycle Bin is significant, as it appears to be a premeditated plan of the house, potentially used by the burglar to determine an entry point. The details of the house map and the fact that it was discarded after the burglary suggest it was used in the planning of the crime.

Method to hide/unhide artefact:

Not hidden but it discovered in the **Recycle Bin**, indicating it was deleted, possibly in an attempt to eliminate evidence.

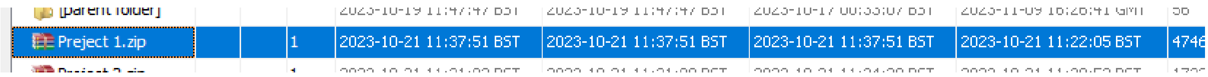
The type of Artefact

Deleted files (Recycle Bin)

Artefact Detail Table

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

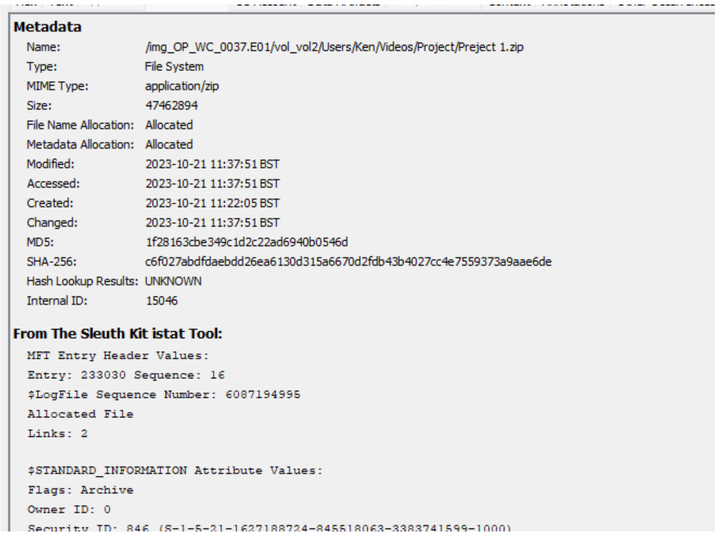
Artefact 15: Preject 1. zip



[parent folder]			2023-10-19 11:47:47 BST	2023-10-19 11:47:47 BST	2023-10-17 00:33:07 BST	2023-11-09 16:26:41 GMT	56
Preject 1.zip		1	2023-10-21 11:37:51 BST	2023-10-21 11:37:51 BST	2023-10-21 11:37:51 BST	2023-10-21 11:22:05 BST	4746

Meta-Data of the artefact:

Mega-Data from Autopsy:



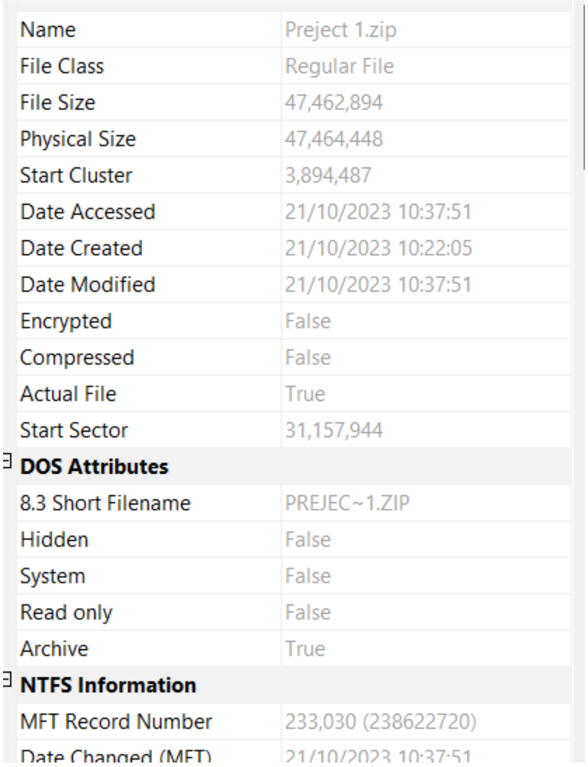
Metadata

Name:	/img_OP_WC_0037.E01/vol_vol2/Users/Ken/Videos/Project/Preject 1.zip
Type:	File System
MIME Type:	application/zip
Size:	47462894
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2023-10-21 11:37:51 BST
Accessed:	2023-10-21 11:37:51 BST
Created:	2023-10-21 11:22:05 BST
Changed:	2023-10-21 11:37:51 BST
MD5:	1f28163cbe349c1d2c22ad6940b0546d
SHA-256:	c6f027abdfdaebdd26ea6130d315a6670d2fdb43b4027cc4e7559373a9aae6de
Hash Lookup Results:	UNKNOWN
Internal ID:	15046

From The Sleuth Kit istat Tool:

```
MFT Entry Header Values:
Entry: 233030 Sequence: 16
$LogFile Sequence Number: 6087194995
Allocated File
Links: 2

$STANDARD_INFORMATION Attribute Values:
Flags: Archive
Owner ID: 0
Security ID: 846 (S-1-5-21-1627188724-845518063-3383741599-1000)
```

Mega-Data from FTK Imager:



Name	Preject 1.zip
File Class	Regular File
File Size	47,462,894
Physical Size	47,464,448
Start Cluster	3,894,487
Date Accessed	21/10/2023 10:37:51
Date Created	21/10/2023 10:22:05
Date Modified	21/10/2023 10:37:51
Encrypted	False
Compressed	False
Actual File	True
Start Sector	31,157,944
DOS Attributes	
8.3 Short Filename	PREJEC~1.ZIP
Hidden	False
System	False
Read only	False
Archive	True
NTFS Information	
MFT Record Number	233,030 (238622720)
Date Changed (MFT)	21/10/2023 10:37:51

Implications of the Artefact:

Artefact 15, a zip file named '**Preject 1.zip**', was found to contain nested zip folders, suggesting an intentional obfuscation of the file contents and/or path name. This could indicate an effort to hide sensitive information by making it harder to reach or recognize the true contents without multiple levels of extraction.

Method to hide/unhide artefact:

The method of hiding this artefact involved multiple layers of zipping, which serves as a rudimentary way of obfuscating the file path and contents.

The type of Artefact

Obfuscation of file path and contents

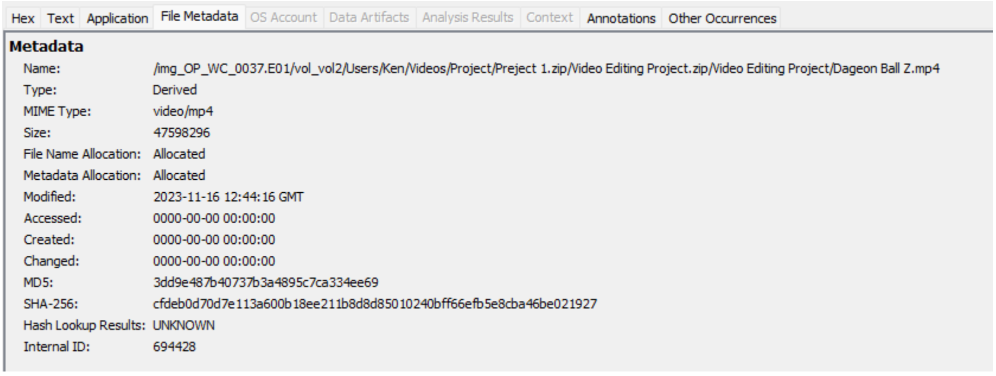
Artefact Detail Table

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

Artefact 16: Dragon Ball Z.mp4

Meta-Data of the artefact:

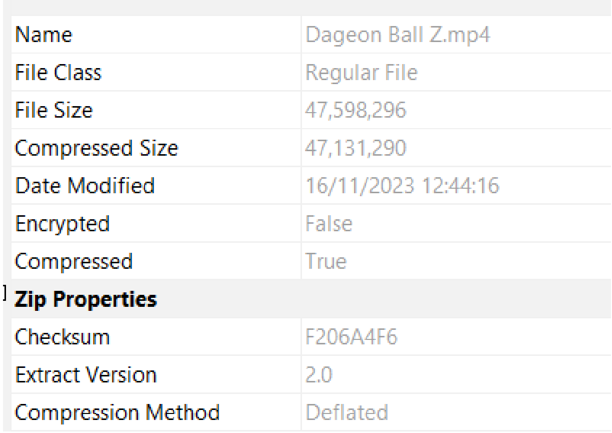
Meta-Data from Autopsy:



Metadata

Name:	/img_OP_WC_0037.E01/vol_vol2/Users/Ken/Videos/Project/Preject 1.zip/Video Editing Project.zip/Video Editing Project/Dageon Ball Z.mp4
Type:	Derived
MIME Type:	video/mp4
Size:	47598296
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2023-11-16 12:44:16 GMT
Accessed:	0000-00-00 00:00:00
Created:	0000-00-00 00:00:00
Changed:	0000-00-00 00:00:00
MD5:	3dd9e487b40737b3a4895c7ca334ee69
SHA-256:	cfdeb0d70d7e113a600b18ee211b8d8d85010240bff66efb5e8cba46be021927
Hash Lookup Results:	UNKNOWN
Internal ID:	694428

Meta-Data from FTK Imager:



Name	Dageon Ball Z.mp4
File Class	Regular File
File Size	47,598,296
Compressed Size	47,131,290
Date Modified	16/11/2023 12:44:16
Encrypted	False
Compressed	True
Zip Properties	
Checksum	F206A4F6
Extract Version	2.0
Compression Method	Deflated

Implications of the Artefact:

Artefact 16, a video file named '**Dragon Ball Z.mp4**', was located deep within a nested zip file structure (as noted in **Artefact 15**), suggesting a deliberate attempt to conceal it. The title of the video is significant because it directly references the item reported as stolen from Mr. Tsuyoshi's house, indicating a potential link to the crime.

Method to hide/unhide artefact:

The video file was obscured through multiple layers of zipping, a method used to obfuscate the file path and make it difficult to ascertain the content without unpacking all layers.

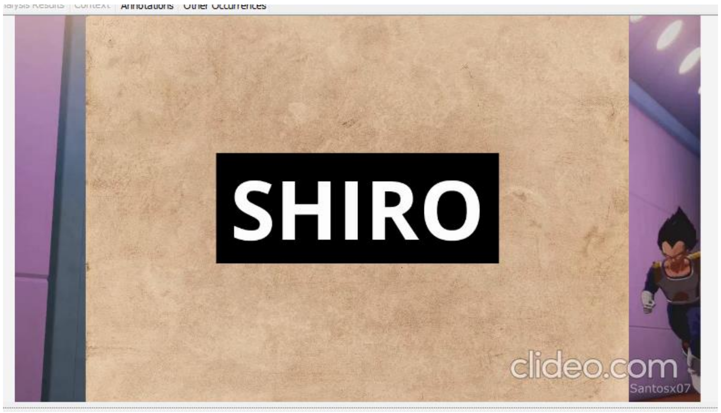
The type of Artefact

A video

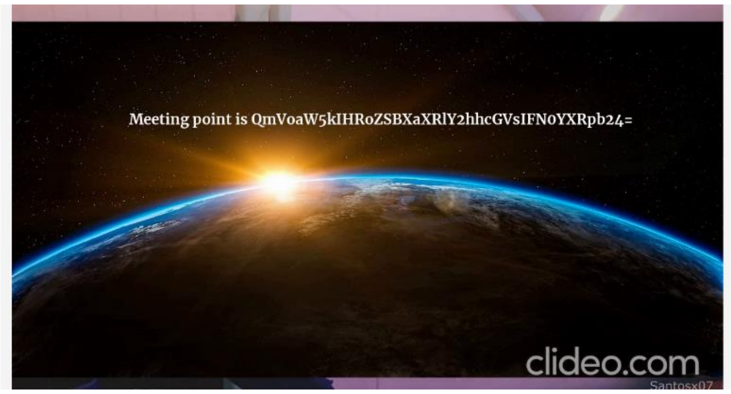
Artefact Detail Table

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

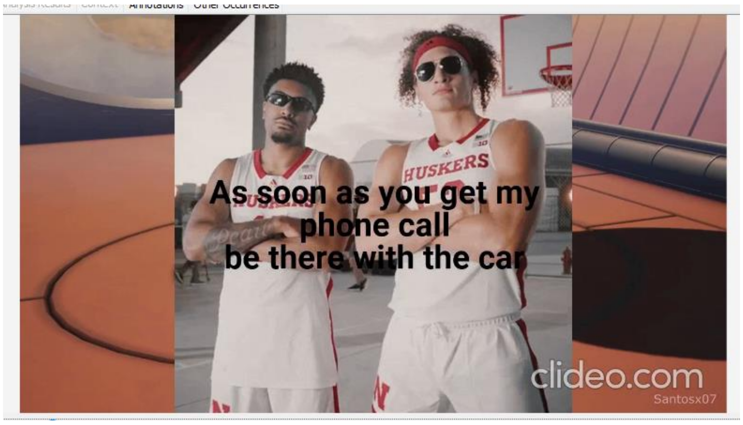
Artefact 17: Dragon Ball Z.mp4



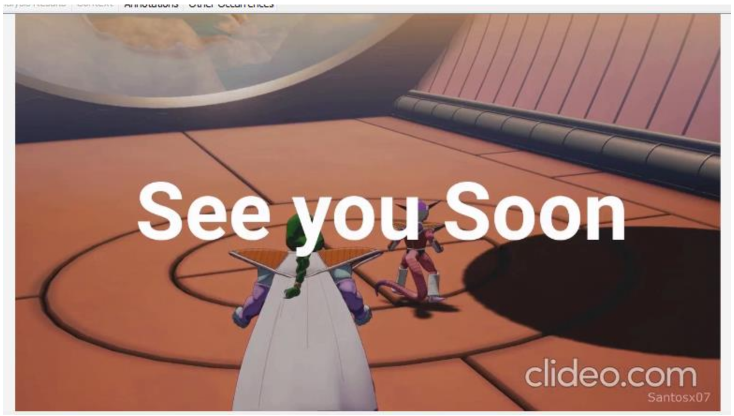
SHIRO



Meeting point is QmVoaW5kIHRoZSBXaXRlY2hhcGVsIFN0YXRpb24=



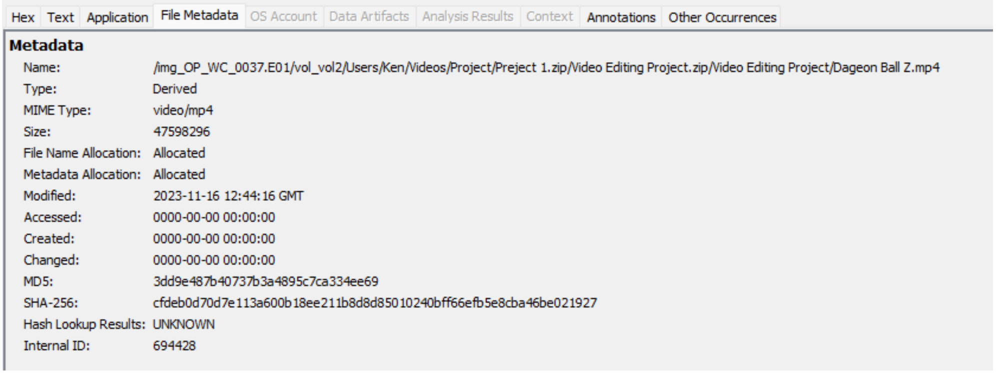
As soon as you get my phone call be there with the car



See you Soon

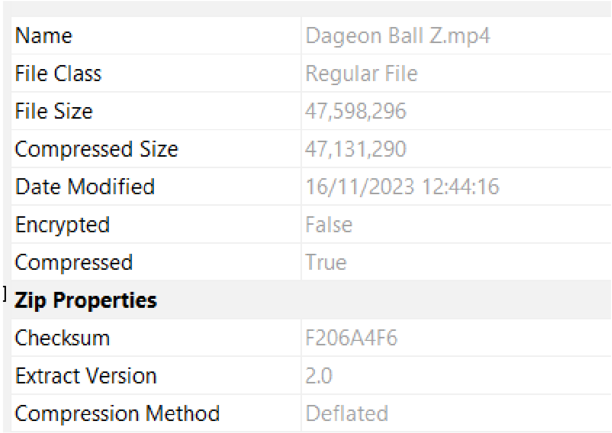
Meta-Data of the artefact:

Meta-Data from Autopsy:



```
Metadata
  Name:                   /img_OP_WC_0037.E01/vol_vol2/Users/Ken/Videos/Project/Preject 1.zip/Video Editing Project.zip/Video Editing Project/Dageon Ball Z.mp4
  Type:                   Derived
  MIME Type:              video/mp4
  Size:                   47598296
  File Name Allocation:   Allocated
  Metadata Allocation:    Allocated
  Modified:               2023-11-16 12:44:16 GMT
  Accessed:               0000-00-00 00:00:00
  Created:                0000-00-00 00:00:00
  Changed:                0000-00-00 00:00:00
  MD5:                    3dd9e487b40737b3a4895c7ca334ee69
  SHA-256:                cfdeb0d70d7e113a600b18ee211b8d8d85010240bff66efb5e8cba46be021927
  Hash Lookup Results:    UNKNOWN
  Internal ID:            694428
```

Meta-Data from FTK Imager:



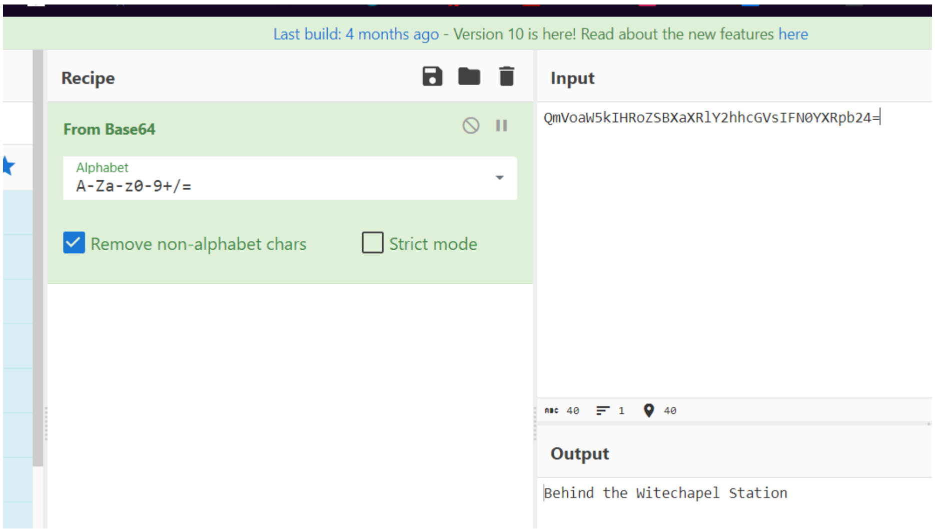
Name	Dageon Ball Z.mp4
File Class	Regular File
File Size	47,598,296
Compressed Size	47,131,290
Date Modified	16/11/2023 12:44:16
Encrypted	False
Compressed	True
Zip Properties	
Checksum	F206A4F6
Extract Version	2.0
Compression Method	Deflated

Implications of the Artefact:

Artefact 17 is a video file that contains critical information pertaining to the case and also uses a software '**clideo.com**' as the watermark showed in the video. The mention of the name '**Shiro**' in the video links it to a suspect in the crime. The video includes a coded message about a meeting point, indicating communication and coordination between accomplices. The phrase '**As soon as you get my phone call be there with the car**' implies the planning of a getaway vehicle, and '**See you soon**' suggests the video was created shortly before the burglary took place. The coded message '**QmVoaW5kHRoZSBXaXRlY2hhcGVsIFNoYXRpb24=**' appears to be Base64 encoded and could potentially reveal further details about the meeting location when decoded.

Method to hide/unhide artefact:

The video was likely sent discreetly to accomplices and may have been hidden within multiple zip files (as indicated by the context of **Artefact 15**) to avoid easy detection. The use of an encoded message within the video adds an additional layer of secrecy, requiring decryption to understand the full implications of the content. The video's discovery is crucial as it contains direct references to the suspects and their planned actions related to the crime.



Last build: 4 months ago - Version 10 is here! Read about the new features here

Recipe

From Base64

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

☑ Remove non-alphabet chars ☐ Strict mode

Input

```
QmVoaW5kIHRoZSBXaXRlY2hhcGVsIFN0YXRpb24=
```

Output

```
Behind the Witechapel Station
```

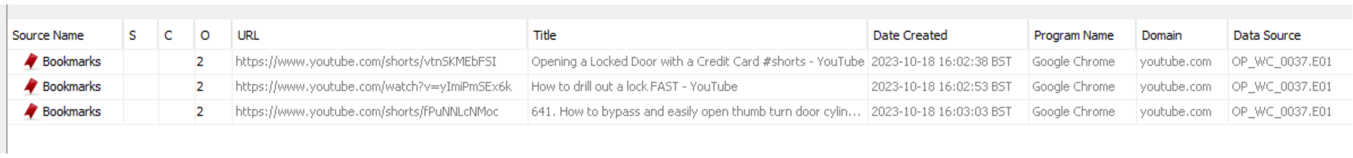
The type of Artefact

Splicing – using the software to edit video

Artefact Detail Table

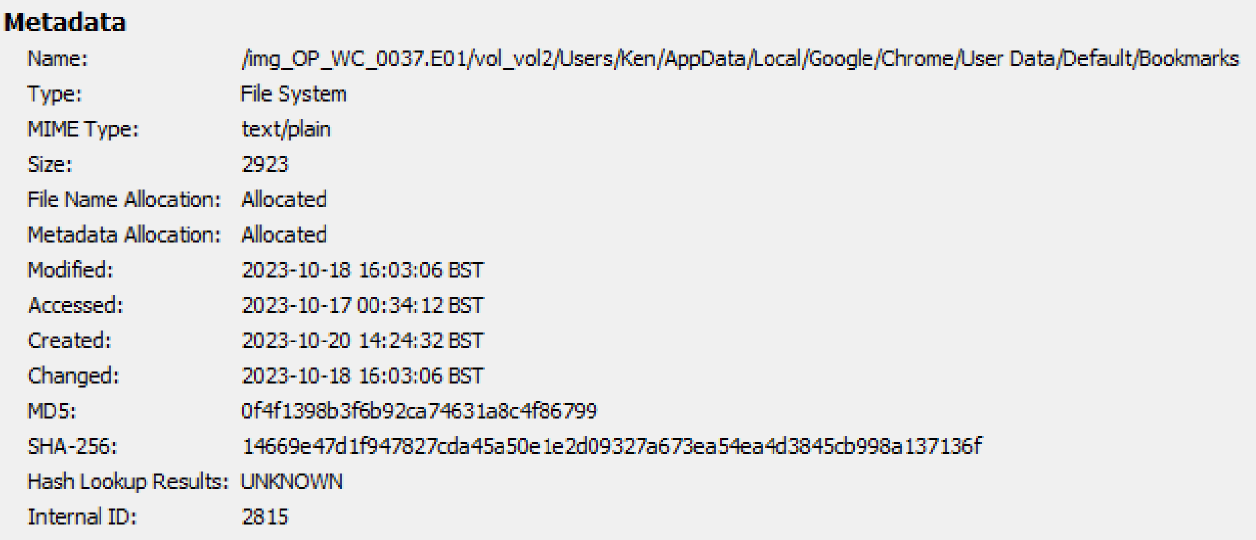
Artefact is	Tick Appropriate
Application Level	✓
OS Level	
File System Level	
Reconnaissance / Research phase	✓
Recording phase	
Result / Aftermath phase	✓

Artefact 18: Bookmarks



Source Name	S	C	O	URL	Title	Date Created	Program Name	Domain	Data Source
Bookmarks			2	https://www.youtube.com/shorts/vtnSKMEbFSI	Opening a Locked Door with a Credit Card #shorts - YouTube	2023-10-18 16:02:38 BST	Google Chrome	youtube.com	OP_WC_0037.E01
Bookmarks			2	https://www.youtube.com/watch?v=yImiPmSEx6k	How to drill out a lock FAST - YouTube	2023-10-18 16:02:53 BST	Google Chrome	youtube.com	OP_WC_0037.E01
Bookmarks			2	https://www.youtube.com/shorts/fPuNNLcNMoc	641. How to bypass and easily open thumb turn door cylin...	2023-10-18 16:03:03 BST	Google Chrome	youtube.com	OP_WC_0037.E01

Meta-Data of the artefact:



Metadata

Name:	/img_OP_WC_0037.E01/vol_vol2/Users/Ken/AppData/Local/Google/Chrome/User Data/Default/Bookmarks
Type:	File System
MIME Type:	text/plain
Size:	2923
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2023-10-18 16:03:06 BST
Accessed:	2023-10-17 00:34:12 BST
Created:	2023-10-20 14:24:32 BST
Changed:	2023-10-18 16:03:06 BST
MD5:	0f4f1398b3f6b92ca74631a8c4f86799
SHA-256:	14669e47d1f947827cda45a50e1e2d09327a673ea54ea4d3845cb998a137136f
Hash Lookup Results:	UNKNOWN
Internal ID:	2815

Implications of the Artefact:

Artefact 18 consists of bookmarks found on the suspect's **Google Chrome** browser, with each bookmark directing to **YouTube** videos on how to unlock doors without keys, including using credit cards and lock picking. The dates and times of the bookmarks' creation and modification suggest that the suspect researched these methods close to the date of the burglary, which implies a direct connection to the crime. This evidence indicates premeditation and an intent to gain unauthorized entry.

Method to hide/unhide artefact:

The bookmarks were not hidden, being saved directly within the browser's bookmark folder.

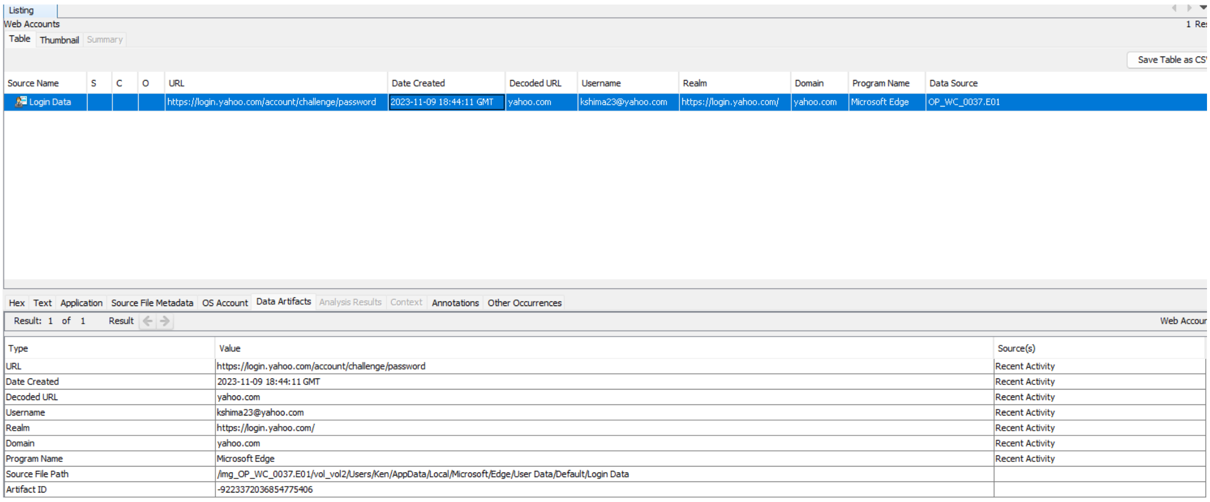
The type of Artefact

Internet history records showing searches of relevant terms

Artefact Detail Table

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

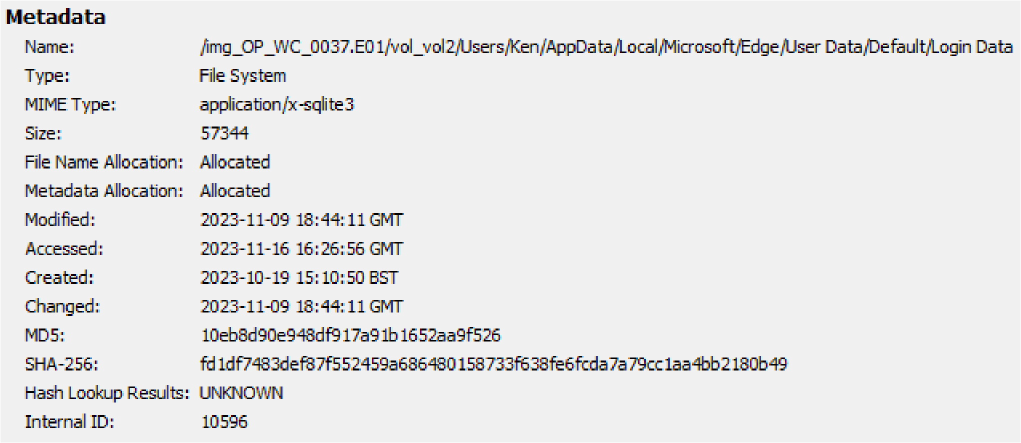
Artefact 19: Yahoo Login Data



Source Name	S	C	O	URL	Date Created	Decoded URL	Username	Realm	Domain	Program Name	Data Source
Login Data				https://login.yahoo.com/account/challenge/password	2023-11-09 18:44:11 GMT	yahoo.com	kshima23@yahoo.com	https://login.yahoo.com/	yahoo.com	Microsoft Edge	OP_WC_0037.E01

Type	Value	Source(s)
URL	https://login.yahoo.com/account/challenge/password	Recent Activity
Date Created	2023-11-09 18:44:11 GMT	Recent Activity
Decoded URL	yahoo.com	Recent Activity
Username	kshima23@yahoo.com	Recent Activity
Realm	https://login.yahoo.com/	Recent Activity
Domain	yahoo.com	Recent Activity
Program Name	Microsoft Edge	Recent Activity
Source File Path	/img_OP_WC_0037.E01/vol_vol2/Users/Ken/AppData/Local/Microsoft/Edge/User Data/Default/Login Data	
Artifact ID	-9223372036854775406	

Meta-Data of the artefact:



Metadata

Name:	/img_OP_WC_0037.E01/vol_vol2/Users/Ken/AppData/Local/Microsoft/Edge/User Data/Default/Login Data
Type:	File System
MIME Type:	application/x-sqlite3
Size:	57344
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2023-11-09 18:44:11 GMT
Accessed:	2023-11-16 16:26:56 GMT
Created:	2023-10-19 15:10:50 BST
Changed:	2023-11-09 18:44:11 GMT
MD5:	10eb8d90e948df917a91b1652aa9f526
SHA-256:	fd1df7483def87f552459a686480158733f638fe6fcda7a79cc1aa4bb2180b49
Hash Lookup Results:	UNKNOWN
Internal ID:	10596

Implications of the Artefact:

Artefact 19 is the login data which indicates recent activity on a **Yahoo account potentially linked to the suspect, Ken Shima**. The accessed URL suggests the account was used for checking emails or general activity, which may include communication with the other suspect known as Shiro. The timing of this activity in relation to the events of the case could be significant and may provide insight into the suspect's actions and intentions around the time of the alleged crime.

Method to hide/unhide artefact:

Given that the file was located in the user's AppData directory, it may not have been explicitly hidden but is not easily accessible to an average user without knowledge of the file system.

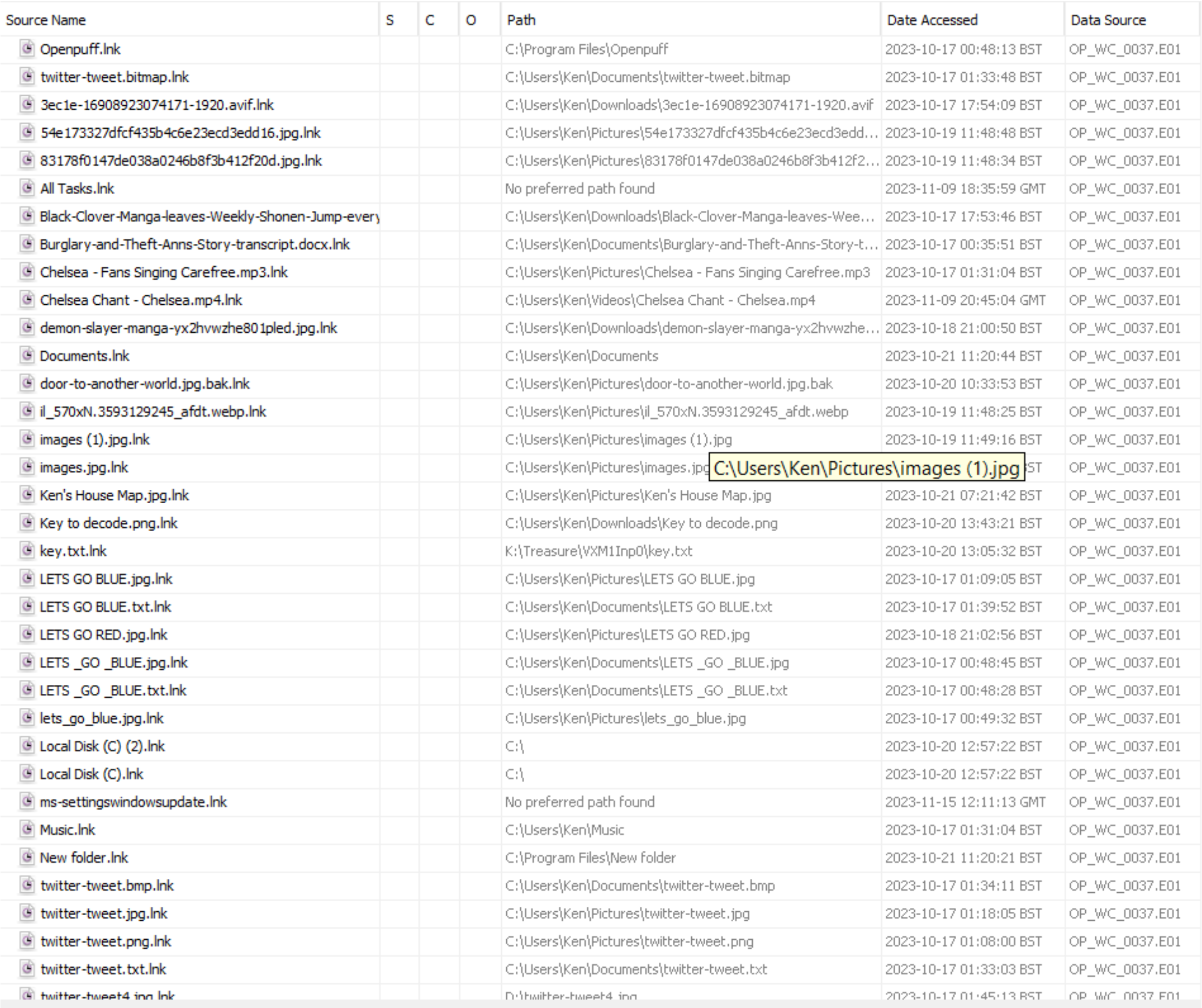
The type of Artefact

Registry Information - Username

Artefact Detail Table

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

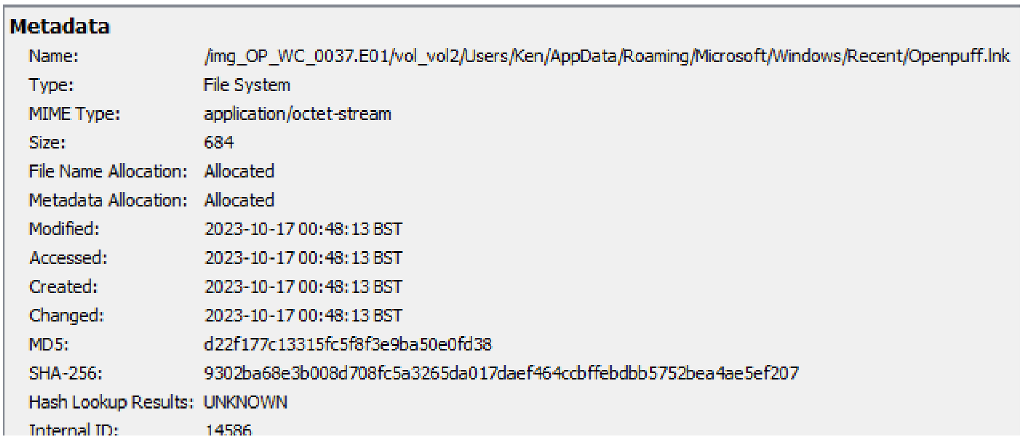
Artefact 20: Most Recently Used (MRU)



Source Name	S	C	O	Path	Date Accessed	Data Source
Openpuff.lnk				C:\Program Files\Openpuff	2023-10-17 00:48:13 BST	OP_WC_0037.E01
twitter-tweet.bitmap.lnk				C:\Users\Ken\Documents\twitter-tweet.bitmap	2023-10-17 01:33:48 BST	OP_WC_0037.E01
3ec1e-16908923074171-1920.avif.lnk				C:\Users\Ken\Downloads\3ec1e-16908923074171-1920.avif	2023-10-17 17:54:09 BST	OP_WC_0037.E01
54e173327dfcf435b4c6e23ecd3edd16.jpg.lnk				C:\Users\Ken\Pictures\54e173327dfcf435b4c6e23ecd3edd…	2023-10-19 11:48:48 BST	OP_WC_0037.E01
83178f0147de038a0246b8f3b412f20d.jpg.lnk				C:\Users\Ken\Pictures\83178f0147de038a0246b8f3b412f2…	2023-10-19 11:48:34 BST	OP_WC_0037.E01
All Tasks.lnk				No preferred path found	2023-11-09 18:35:59 GMT	OP_WC_0037.E01
Black-Clover-Manga-leaves-Weekly-Shonen-Jump-every				C:\Users\Ken\Downloads\Black-Clover-Manga-leaves-Wee…	2023-10-17 17:53:46 BST	OP_WC_0037.E01
Burglary-and-Theft-Anns-Story-transcript.docx.lnk				C:\Users\Ken\Documents\Burglary-and-Theft-Anns-Story-t…	2023-10-17 00:35:51 BST	OP_WC_0037.E01
Chelsea - Fans Singing Carefree.mp3.lnk				C:\Users\Ken\Pictures\Chelsea - Fans Singing Carefree.mp3	2023-10-17 01:31:04 BST	OP_WC_0037.E01
Chelsea Chant - Chelsea.mp4.lnk				C:\Users\Ken\Videos\Chelsea Chant - Chelsea.mp4	2023-11-09 20:45:04 GMT	OP_WC_0037.E01
demon-slayer-manga-yx2hvwzhe801pled.jpg.lnk				C:\Users\Ken\Downloads\demon-slayer-manga-yx2hvwzhe…	2023-10-18 21:00:50 BST	OP_WC_0037.E01
Documents.lnk				C:\Users\Ken\Documents	2023-10-21 11:20:44 BST	OP_WC_0037.E01
door-to-another-world.jpg.bak.lnk				C:\Users\Ken\Pictures\door-to-another-world.jpg.bak	2023-10-20 10:33:53 BST	OP_WC_0037.E01
il_570xN.3593129245_afdt.webp.lnk				C:\Users\Ken\Pictures\il_570xN.3593129245_afdt.webp	2023-10-19 11:48:25 BST	OP_WC_0037.E01
images (1).jpg.lnk				C:\Users\Ken\Pictures\images (1).jpg	2023-10-19 11:49:16 BST	OP_WC_0037.E01
images.jpg.lnk				C:\Users\Ken\Pictures\images.jpg	ST	OP_WC_0037.E01
Ken's House Map.jpg.lnk				C:\Users\Ken\Pictures\Ken's House Map.jpg	2023-10-21 07:21:42 BST	OP_WC_0037.E01
Key to decode.png.lnk				C:\Users\Ken\Downloads\Key to decode.png	2023-10-20 13:43:21 BST	OP_WC_0037.E01
key.txt.lnk				K:\Treasure\VXM1Inp0\key.txt	2023-10-20 13:05:32 BST	OP_WC_0037.E01
LETS GO BLUE.jpg.lnk				C:\Users\Ken\Pictures\LETS GO BLUE.jpg	2023-10-17 01:09:05 BST	OP_WC_0037.E01
LETS GO BLUE.txt.lnk				C:\Users\Ken\Documents\LETS GO BLUE.txt	2023-10-17 01:39:52 BST	OP_WC_0037.E01
LETS GO RED.jpg.lnk				C:\Users\Ken\Pictures\LETS GO RED.jpg	2023-10-18 21:02:56 BST	OP_WC_0037.E01
LETS _GO _BLUE.jpg.lnk				C:\Users\Ken\Documents\LETS _GO _BLUE.jpg	2023-10-17 00:48:45 BST	OP_WC_0037.E01
LETS _GO _BLUE.txt.lnk				C:\Users\Ken\Documents\LETS _GO _BLUE.txt	2023-10-17 00:48:28 BST	OP_WC_0037.E01
lets_go_blue.jpg.lnk				C:\Users\Ken\Pictures\lets_go_blue.jpg	2023-10-17 00:49:32 BST	OP_WC_0037.E01
Local Disk (C) (2).lnk				C:\	2023-10-20 12:57:22 BST	OP_WC_0037.E01
Local Disk (C).lnk				C:\	2023-10-20 12:57:22 BST	OP_WC_0037.E01
ms-settingswindowsupdate.lnk				No preferred path found	2023-11-15 12:11:13 GMT	OP_WC_0037.E01
Music.lnk				C:\Users\Ken\Music	2023-10-17 01:31:04 BST	OP_WC_0037.E01
New folder.lnk				C:\Program Files\New folder	2023-10-21 11:20:21 BST	OP_WC_0037.E01
twitter-tweet.bmp.lnk				C:\Users\Ken\Documents\twitter-tweet.bmp	2023-10-17 01:34:11 BST	OP_WC_0037.E01
twitter-tweet.jpg.lnk				C:\Users\Ken\Pictures\twitter-tweet.jpg	2023-10-17 01:18:05 BST	OP_WC_0037.E01
twitter-tweet.png.lnk				C:\Users\Ken\Pictures\twitter-tweet.png	2023-10-17 01:08:00 BST	OP_WC_0037.E01
twitter-tweet.txt.lnk				C:\Users\Ken\Documents\twitter-tweet.txt	2023-10-17 01:33:03 BST	OP_WC_0037.E01
twitter-tweet4.jpg.lnk				D:\twitter-tweet4.jpg	2023-10-17 01:45:13 BST	OP_WC_0037.E01

Meta-Data of the artefact:

This is one of the Meta-Data of the files called ‘OpenPuff.lnk’



Metadata

Name:	/img_OP_WC_0037.E01/vol_vol2/Users/Ken/AppData/Roaming/Microsoft/Windows/Recent/Openpuff.lnk
Type:	File System
MIME Type:	application/octet-stream
Size:	684
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2023-10-17 00:48:13 BST
Accessed:	2023-10-17 00:48:13 BST
Created:	2023-10-17 00:48:13 BST
Changed:	2023-10-17 00:48:13 BST
MD5:	d22f177c13315fc5f8f3e9ba50e0fd38
SHA-256:	9302ba68e3b008d708fc5a3265da017daef464ccbffebdbb5752bea4ae5ef207
Hash Lookup Results:	UNKNOWN
Internal ID:	14586

Implications of the Artefact:

Artefact 20 is the **MRU paths** which suggest that the user accessed a variety of files and applications, which may give insights into their recent activities and interests. The presence of various image files and documents could indicate the transfer of information or concealment of evidence.

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

6. Supporting Material

6.1 Use of Software

The software utilised during the project were the following:

- **OpenPuff** - The use of the OpenPuff allowed to hide a crucial information in form of ‘jpg’ file into another ‘jpg’ file by using the steganography technique.
- **HxD Hex Editor** – By utilising the software HxD Hex Editor, a file containing important details regarding a crime got destroyed by manipulating the headers of the file, which was later recoverable by retrieving the correct Hex of the file.
- **VeraCrypt** – The software VeraCrypt was utilised to create a password protected container, in order to make it difficult for the investigators to retrieve key details of the crime.
- **Notepad** – The software notepad was used to plan the evidence in ‘txt’ files.

6.3 Use of Website

- **PRANKSHIT**– This website provided with social media posts and messages templates from different social media platforms, this website has been used to develop a tweet from our victim as an artefact.
- **Browsers** – To gather all the necessary and unnecessary files to fill the storage of the operating system and some artefacts such as some ‘jpg’ file.