Digital Forensics: CMP020N210S
Portfolio 1 – Analysing Forensic Images

STUDENT NAME: Sawsan Mounes
STUDENT ID: Mou23620003

BSc. CYBER SECURITY

Table of Contents

Introduction

Investigator(s): Sawsan Mounes
Date of Report 12/02/25

A client reported an incident where one of their employees is suspected of committing a crime related to digital piracy. Following this report, our digital forensics team conducted a thorough search of the suspect's office, carefully examining all potential evidence. During the investigation, several items were seized that could serve as crucial evidence to confirm whether the suspect was indeed involved in piracy. Among the collected digital evidence, two forensic disk images were obtained: USB image (E_01_Physical_Image_yourname) and USB_03.E01. Our team is investigating multiple aspects, including verifying image integrity by comparing computed hash values with stored hashes, recovering deleted files by extracting and analysing hidden or deleted data, and examining file signatures to identify file types, formats, and metadata. Additionally, we are investigating encrypted data to detect and attempt decryption of hidden files and analysing digital artifacts using forensic tools such as FTK Imager, Autopsy, HxD, and VeraCrypt to examine file system structures, logs, and timestamps. By referring to Appendix A, the Chain of Custody details for all seized evidence, including the forensic images, have been documented and preserved to ensure the integrity of the investigation.

Recovering Files from a Forensic Image eo01_Sawsan.E01

Identification of the Person Who Added the Files?

Even after careful analysis of the USB drive's digital evidence, we couldn't figure out who added the files. There were no text files, metadata, or user information that clearly showed who handled the data. However, there might be a clue: the name 'Oitaclh' is written on a label on the USB drive, which could hint at the owner or user but there was an image found saying anonymous therefore suspect may want to stay anonymous and not known .

Evidence of files found in eo01_Sawsan.E01 ?

File name	File signature	File extension	File size (KB)
!.E01	45 56 46	EVF	12,269
XIC_20200701 - Financial Crimes in the Era of Dark Web - Assessment Report	25 50 44 46	PDF	3,327
150803-silk-road-1126.jpg	4A 46 49 46	JPG	196
C_01_PHYSICAL_EVIDANCE.E01	4A 46 49 46	E01	12,269
IC_20200701 - Financial Crimes in the Era of Dark Web - Assessment Report Final.pdf	25 50 44 46	PDF	3,327
thumb-1920-423529.jpg	4A 46 49 46	JPG	409
building-9340309_1280.jpg	4A 46 49 46	JPG	387
1000_F_36415952_fElBKJYoUfJLzbbHRJo2oleleNxGuU9Q.jpg	4A 46 49 46	JPG	196
150803-silk-road-1126.jpg	4A 46 49 46	JPG	196
drug-alcohol-test.jpg	4A 46 49 46	JFIF	123
Cyber-security-threat.jpg.webp	57 45 42 50	WEBP	77
Digital_Forensics_Investigation_Report_Template.docx	CA A2 F7 30 B6 DB 71 E8 E1 04 07 34 D4 7D C2 96	DOC.X(error not docx)	68
birds-8554199_1280.jpg	7E 40 DC A9 C1 CB E4 F4 0D E6 FD 3E 0F F7 8C F9	Jpg(not a jpg file error)	41
v4-460px-Pass-a-Drug-Test-Step-3-Version-3.jpg.jfif	57 45 42 50	.WEBP	21
b71ad530-5b13-11ef-8f0f-0577398c3339.jpg.webp	57 45 42 50	WEBP	20
v4-460px-Pass-a-Drug-Test-Step-23.jpg.jfif	57 45 42 50	WEBP	15
images.jfif	4A 46 49 46	JFIF	14
C_01_PHYSICAL_EVIDANCE.E01.txt	EF BB BF 4E 4F 54 49 43 45 3A 20 54 68 65 20 69	The image doesn't work it's a notice	2
TEST-FILE.txt	F9 2B EF 41 FF D5 6E 84 57 BE 1D 6B A3 60 61 C4	.TXT	1
New Text Document.txt	0	0	0

(Kessler, 2019)
(Duttke, n.d.)

Digital_Forensics_In...	383 (1 KB)	File Slack	
C_01_PHYSICAL_EVI...	46,077,007 (44,998 KB)	Regular File	1/27/2025 11:37:42 AM
!.E01	12,563,127 (12,269 KB)	Regular File	1/27/2025 11:44:42 AM
IC_20200701 - Fina...	3,406,351 (3,327 KB)	Regular File	1/29/2025 11:25:08 AM
thumb-1920-42352...	418,645 (409 KB)	Regular File	1/29/2025 11:21:22 AM
building-9340309_...	396,253 (387 KB)	Regular File	1/27/2025 11:19:00 AM
1000_F_36415952_f...	200,676 (196 KB)	Regular File	1/29/2025 11:20:02 AM
150803-silk-road-1...	199,803 (196 KB)	Regular File	1/29/2025 11:24:38 AM
woman-9227532_1...	159,016 (156 KB)	Regular File	1/27/2025 11:17:42 AM
highland-cow-8972...	157,662 (154 KB)	Regular File	1/27/2025 11:15:42 AM
drug-alcohol-test.jpg	125,341 (123 KB)	Regular File	1/29/2025 11:23:34 AM
Cyber-security-thre...	78,054 (77 KB)	Regular File	1/29/2025 11:19:46 AM
drink-9295840_128...	70,222 (69 KB)	Regular File	1/27/2025 11:18:08 AM
Digital_Forensics_In...	69,249 (68 KB)	Regular File	1/27/2025 10:59:30 AM
birds-8554199_128...	41,836 (41 KB)	Regular File	1/27/2025 11:18:46 AM
v4-460px-Pass-a-Dr...	21,450 (21 KB)	Regular File	1/29/2025 11:21:52 AM
b71ad530-5b13-11...	20,394 (20 KB)	Regular File	1/29/2025 11:21:36 AM
v4-460px-Pass-a-Dr...	15,056 (15 KB)	Regular File	1/29/2025 11:22:44 AM
images.jfif	14,277 (14 KB)	Regular File	1/29/2025 11:19:54 AM
C_01_PHYSICAL_EVI...	1,192 (2 KB)	Regular File	1/27/2025 11:37:42 AM
TEST-FILE.txt	28 (1 KB)	Regular File	1/27/2025 11:20:00 AM
New Text Documen...	0 (0 KB)	Regular File	1/27/2025 11:19:36 AM

Evidence from E01 image found.

Storage Capacity Analysis

Observation: The USB drive's total storage capacity is recorded as 3840 MB. This measurement was confirmed by examining the device's properties in the system's storage information section, accessible through the download area of the USB.

Evidence:

```
Created By AccessData® FTK® Imager 4.7.1.2

Case Information:
Acquired using: ADI4.7.1.2
Case Number: Case 1
Evidence Number: 1
Unique Description:
Examiner:
Notes:

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

Information for D:\sawsan\eo01_sawsan:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 489
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 7,864,320
[Physical Drive Information]
 Drive Model: General UDisk USB Device
 Drive Serial Number:
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 3840 MB
 Sector count:    7864320
[Computed Hashes]
 MD5 checksum:    993132cd38f7bfe2622ce1d40f548474
 SHA1 checksum:   ab751828a31fbae8bdb84ae0c3c0eb8085d753a7

Image Information:
 Acquisition started:   Wed Feb 12 11:58:00 2025
 Acquisition finished:  Wed Feb 12 12:00:36 2025
 Segment list:
  D:\sawsan\eo01_sawsan.E01

Image Verification Results:
 Verification started:  Wed Feb 12 12:00:36 2025
 Verification finished: Wed Feb 12 12:01:24 2025
 MD5 checksum:    993132cd38f7bfe2622ce1d40f548474 : verified
 SHA1 checksum:   ab751828a31fbae8bdb84ae0c3c0eb8085d753a7 : verified
```

USB device confiscated during the investigation.

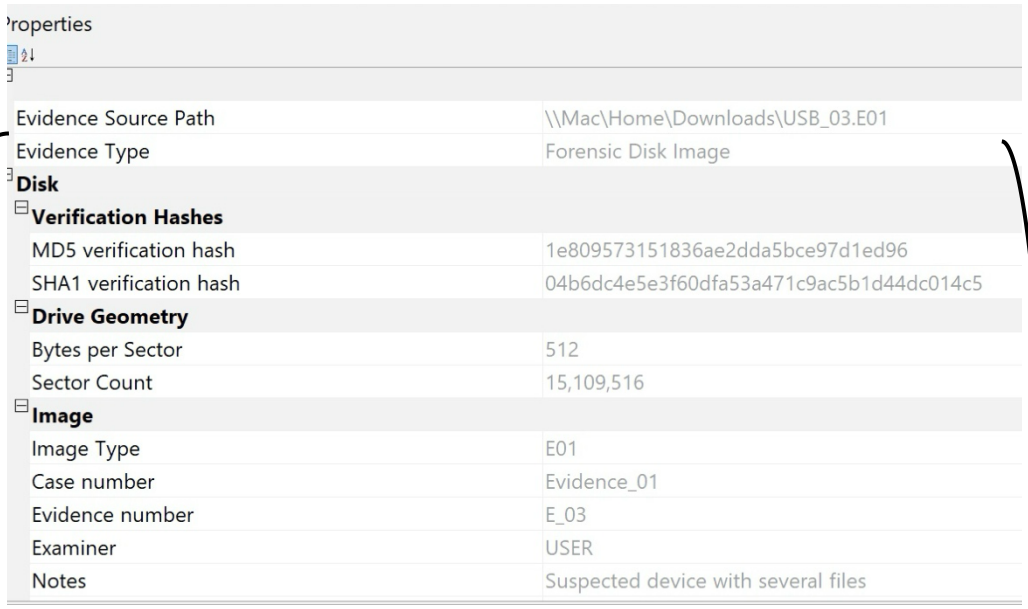
Evidence from E01 image found.

File Signature Investigations – Analysing the USB_03_E01 image.

Verification of a Downloaded Hash Against the Original Hash

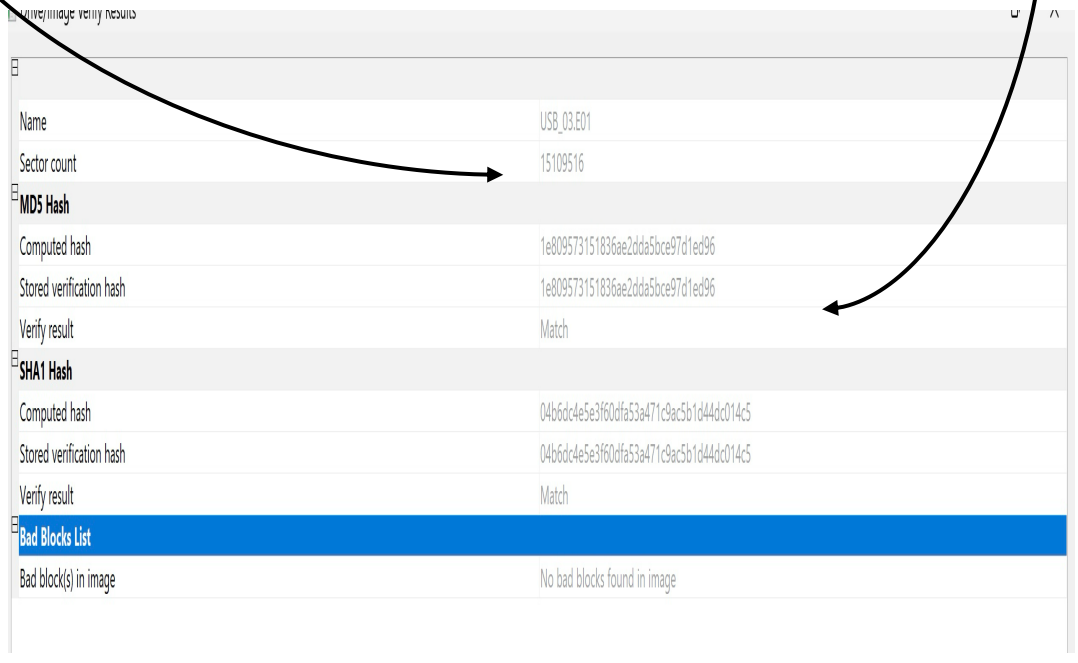
In Source 1, the original image is displayed, containing both the MD5 verification hash and SHA-1 hash. Source 2 presents the downloaded image, showing the computed hash values after undergoing the verification process.

Evidence



Properties	
Evidence Source Path	\\Mac\Home\Downloads\USB_03.E01
Evidence Type	Forensic Disk Image
Disk	
Verification Hashes	
MD5 verification hash	1e809573151836ae2dda5bce97d1ed96
SHA1 verification hash	04b6dc4e5e3f60dfa53a471c9ac5b1d44dc014c5
Drive Geometry	
Bytes per Sector	512
Sector Count	15,109,516
Image	
Image Type	E01
Case number	Evidence_01
Evidence number	E_03
Examiner	USER
Notes	Suspected device with several files

Source 1



Name	USB_03.E01
Sector count	15109516
MD5 Hash	
Computed hash	1e809573151836ae2dda5bce97d1ed96
Stored verification hash	1e809573151836ae2dda5bce97d1ed96
Verify result	Match
SHA1 Hash	
Computed hash	04b6dc4e5e3f60dfa53a471c9ac5b1d44dc014c5
Stored verification hash	04b6dc4e5e3f60dfa53a471c9ac5b1d44dc014c5
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Source 2

Explanation

After going through the verification of the original image in Source A, Source B confirms that both MD5 and SHA-1 hash values match. MD5 Hash: 1e809573151836ae2dda5bce97d1ed96

SHA-1 Hash: 04b6dc4e5e3f60dfa53a471c9ac5b1d44dc014c5. This result indicates that no modifications have been made to the original file and that the files have not been tampered with. Furthermore, since hash values are unique identifiers, they ensure the integrity and authenticity of the forensic image.

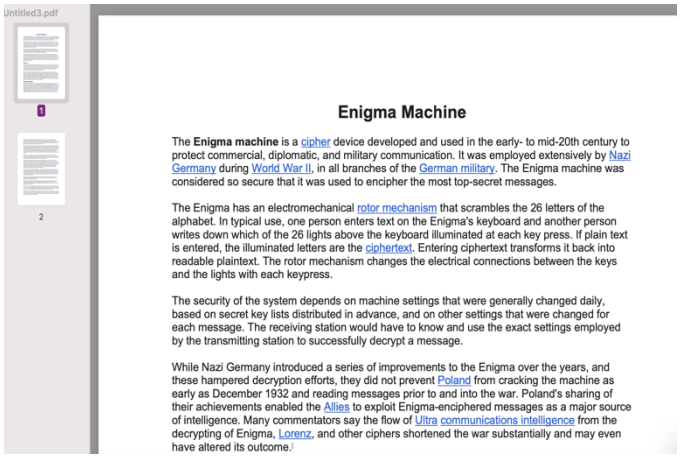
File Format Identification from HEX in FTK Imager

Below is a table containing the file signature, file extension, and file size for each file (file01 – file07) identified using the HEX format tab in FTK Imager in USB_03.E01 .

File name	File signature	File extension	File sizes
FILE 1	25 50 44 46	.PDF	126 KB
FILE 2	50 4B 03 04	.ZIP	13,214 KB
FILE 3	41 72 73 65 6E 61 6C	.txt	3KB
FILE 4	31 21 44 4F 43 54 59 50 45	.html	79KB
FILE 5	37 7A BC AF 27 1C	.7z	1,643KB
FILE 6	47 49 46 38 39 61	.GIF	1,688KB
FILE 7	FF FB 90 44	MP3	53KB

(Wikipedia Contributors, 2019)
(Kessler, 2019)

Evidence of files 1-7



Enigma Machine

The **Enigma machine** is a cipher device developed and used in the early- to mid-20th century to protect commercial, diplomatic, and military communication. It was employed extensively by Nazi Germany during World War II, in all branches of the German military. The Enigma machine was considered so secure that it was used to encipher the most top-secret messages.

The Enigma has an electromechanical rotor mechanism that scrambles the 26 letters of the alphabet. In typical use, one person enters text on the Enigma's keyboard and another person writes down which of the 26 lights above the keyboard illuminated at each key press. If plain text is entered, the illuminated letters are the ciphertext. Entering ciphertext transforms it back into readable plaintext. The rotor mechanism changes the electrical connections between the keys and the lights with each keypress.

The security of the system depends on machine settings that were generally changed daily, based on secret key lists distributed in advance, and on other settings that were changed for each message. The receiving station would have to know and use the exact settings employed by the transmitting station to successfully decrypt a message.

While Nazi Germany introduced a series of improvements to the Enigma over the years, and these hampered decryption efforts, they did not prevent Poland from cracking the machine as early as December 1932 and reading messages prior to and into the war. Poland's sharing of their achievements enabled the Allies to exploit Enigma-enciphered messages as a major source of intelligence. Many commentators say the flow of Ultra communications intelligence from the decrypting of Enigma, Lorenz, and other ciphers shortened the war substantially and may even have altered its outcome.

File 1

File 1

```
Arsenal
Arsenal Football Club is a professional football club based in Islington, London, England, that plays in the Premier League, the top flight of English fo
Arsenal was the first club from the South of England to join The Football League, in 1893, and they reached the First Division in 1904. Relegated only on
Herbert Chapman won Arsenal's first national trophies, but died prematurely. He helped introduce the WM formation, floodlights, and shirt numbers,[7] and
In 1886, Woolwich munitions workers founded the club as Dial Square. In 1913, the club crossed the city to Arsenal Stadium in Highbury, becoming close ne
```

File 2

Manga & Anime Favorites

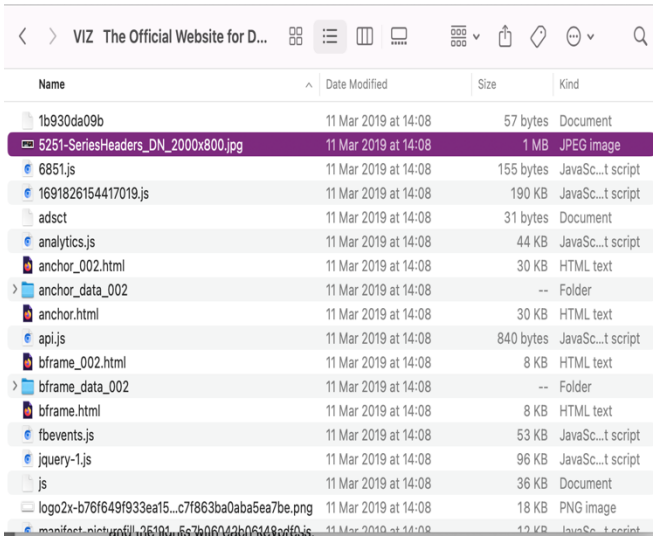
- Sailor Moon
- Boruto
- Naruto
- One-Punch Man
- My Hero Academia
- Tokyo Ghoul
- Pokémon
- VIZ's First Video Game!

VIZ Media: The world's most popular anime, manga and

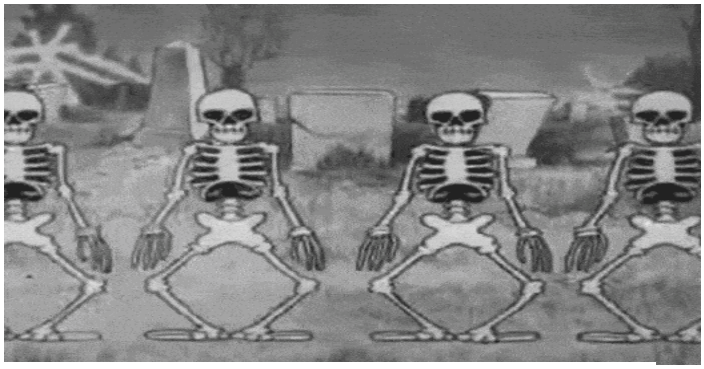
Menu Dismiss

- Read
- Watch
- Shonen Jump
- Community
- Calendar

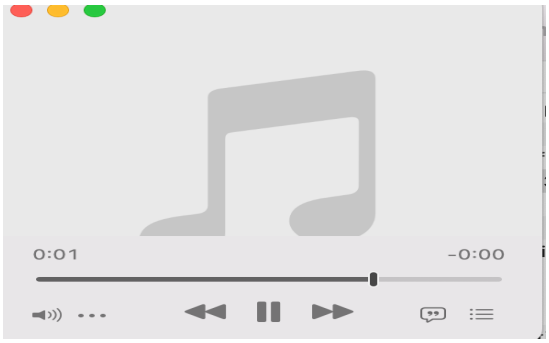
File 3



File 4



File 6

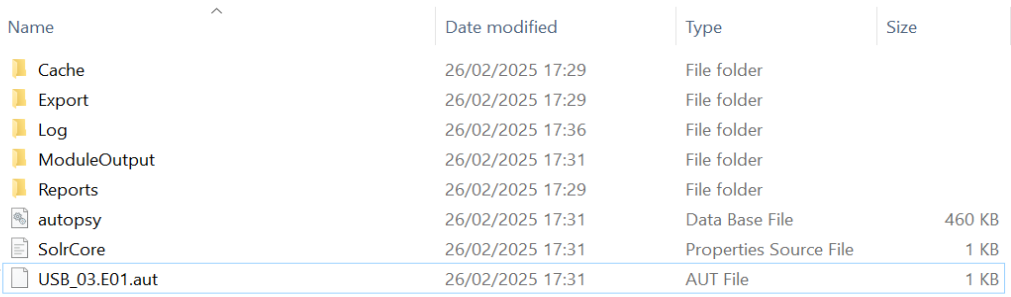


File 7

(Duttke, n.d.)

Analysing USB_03.E01 Forensic Image with Autopsy

What is the extension of an Autopsy case file?



Name	Date modified	Type	Size
Cache	26/02/2025 17:29	File folder	
Export	26/02/2025 17:29	File folder	
Log	26/02/2025 17:36	File folder	
ModuleOutput	26/02/2025 17:31	File folder	
Reports	26/02/2025 17:29	File folder	
autopsy	26/02/2025 17:31	Data Base File	460 KB
SolrCore	26/02/2025 17:31	Properties Source File	1 KB
USB_03.E01.aut	26/02/2025 17:31	AUT File	1 KB

Extension file name: Aut file it In Autopsy, an "aut" file is used to automate tasks like data parsing and report generation, streamlining digital forensic investigations.

What is the Device Model used to create the image called?

Sword.Art.Online.full.1189342.jpg?

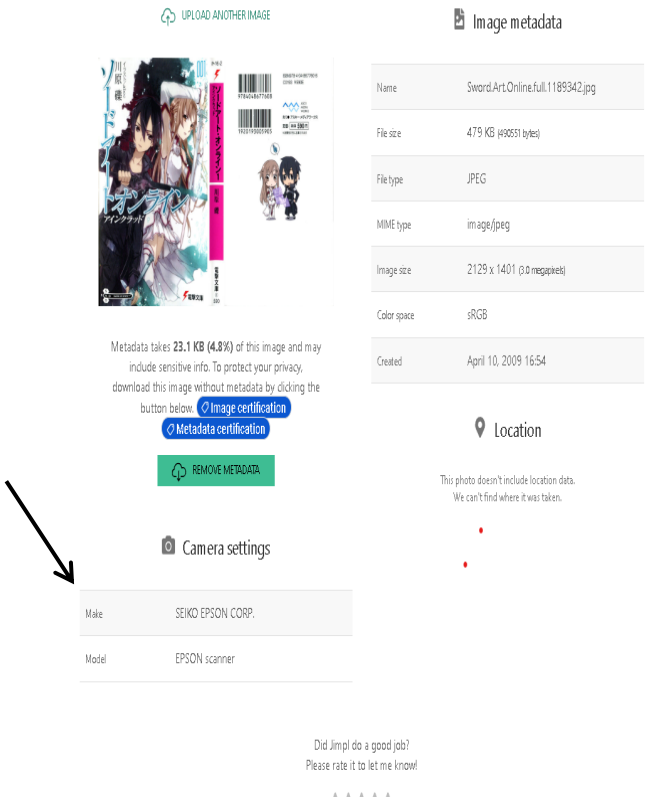
Item: Sword.Art.Online.full.1189342.jpg
Aggregate Score: Not Notable

Analysis Result 1
Score: Not Notable
Type: EXIF Metadata
Configuration:
Conclusion:
Date Created: 2009-04-10 16:54:02 BST
Device Make: SEIKO EPSON CORP.
Device Model: EPSON scanner

Analysis Result 2
Score: Likely Notable
Type: Keyword Hits
Configuration:
Conclusion:
Keyword: Sword.Art.Online.full.1189342.jpg
Keyword Preview: «sword.art.online.full.1189342.jpg«
Keyword Search Type: 0

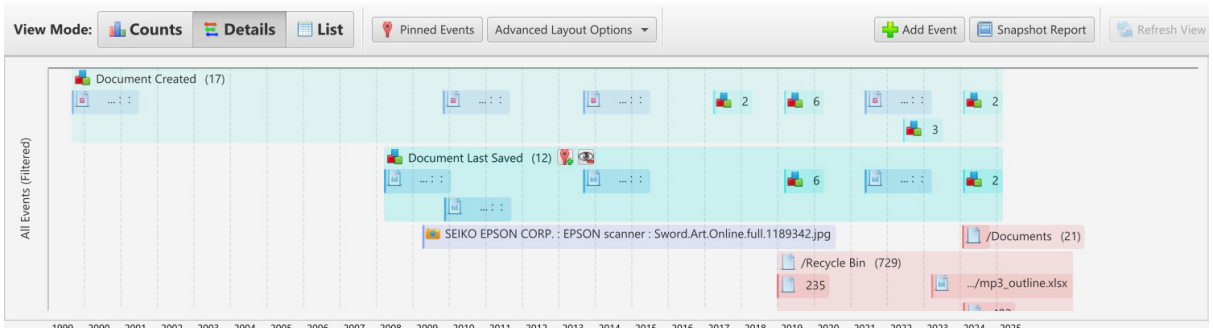
Analysis Result 3
Score: Likely Notable
Type: Keyword Hits
Configuration:
Conclusion:
Keyword: Sword.Art.Online.full.1189342.jpg
Keyword Preview: «sword.art.online.full.1189342.jpg«
Keyword Search Type: 0

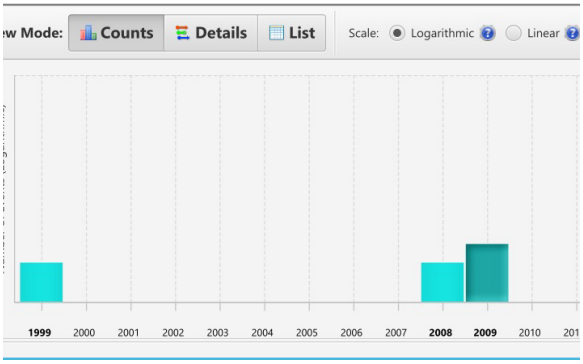
Analysis Result 4
Score: Unknown
Type: User Content Suspected
Configuration:
Conclusion:
Comment: EXIF metadata data exists for this file.



Based on analysing the metadata, it was determined that an Epson scanner was used to digitise the document in the file named 'sword.art.online.full'. To confirm the scanner model, additional verification was carried out using both autopsy analysis and online tools, which also indicated that an Epson scanner was utilised.

Within the Autopsy Timeline view, how many event types occurred in 2009?

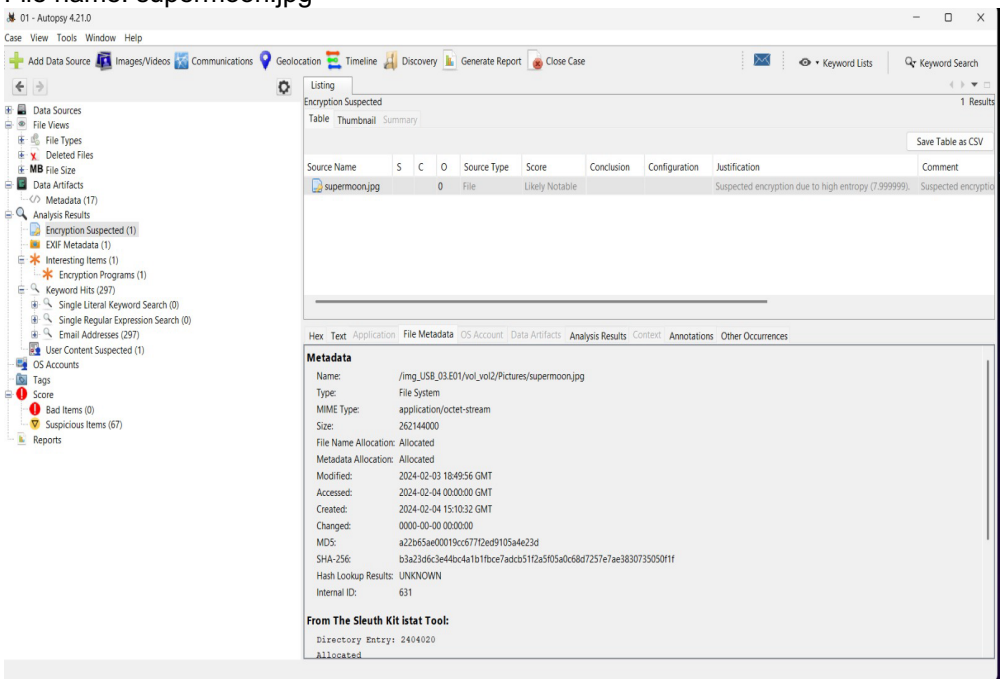




In 2009, three key events were recorded: the creation of files, the addition of the 'sword.art.online.full.jpg', and the last save of a file. The detailed timeline reveals that the document in question was first created in 1999 and continued to be relevant up to 2024. It was last saved multiple times between 2009 and 2024. Specifically, the 'sword.art.online.full.jpg' file underwent modifications starting from 2009 and continued to be modified until its last recorded save in 2024. The first image in the timeline shows the creation of files, while the bar chart and the detailed timeline indicate the periods of modification, marking the start and end dates of the file's activity.

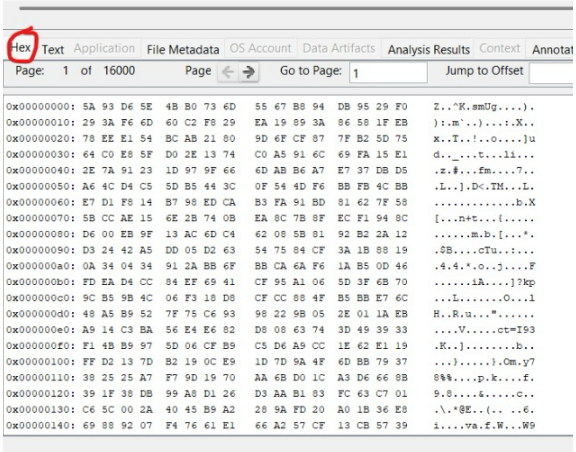
Consider USB_03.E01 image and based on your investigation with Autopsy which file. (including the name and extension) is possibly encrypted?

File name: supermoon.jpg



File Size: The 'supermoon.jpg' file is unusually large for a JPEG image, at 2.6 GB. Typically, JPEG files are much smaller, even at high resolutions. This disproportionate file size raises suspicions about the content of the file, suggesting that it might not just contain image data.

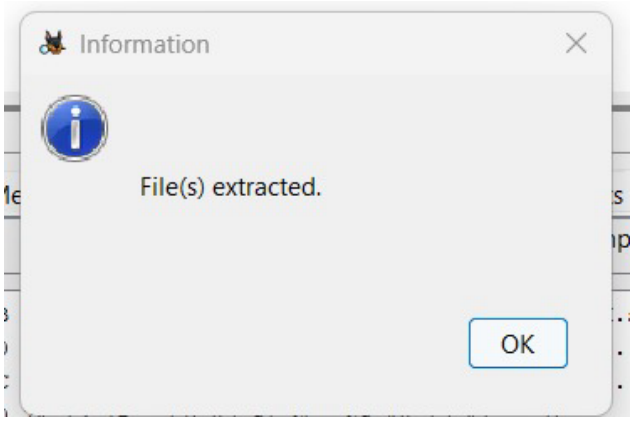
High Entropy: The entropy value of 7.999999 is extremely high. In data analysis, entropy is used to measure randomness. Files with high entropy are often encrypted because encryption algorithms aim to make the data appear as random as possible to secure its contents against unauthorized access.



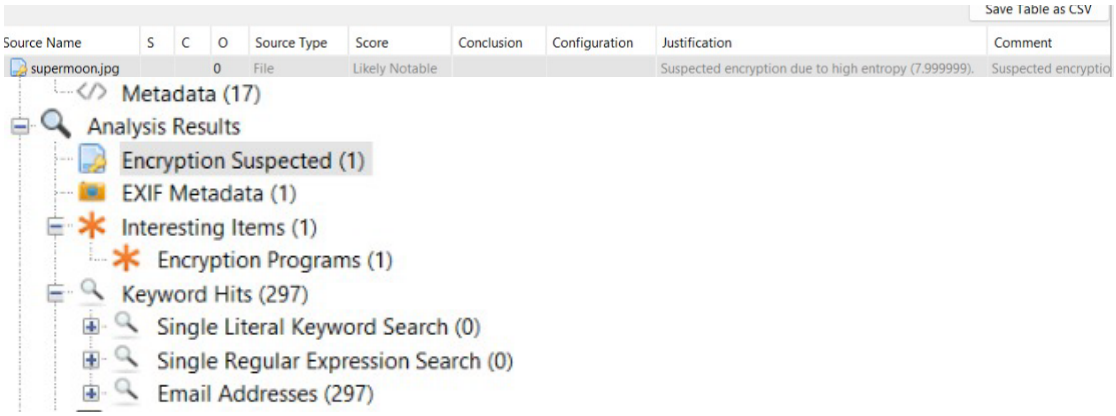
Hash Recognition: The SHA-256 hash of the file does not match any known patterns for standard JPEG files. This anomaly could be indicative of altered content, such as encryption furthermore the image meta data suggests that the hash is UNKNOWN.

Analysing USB_03.E01 Forensic Image

Supermoon,jpg has been extracted from autopsy

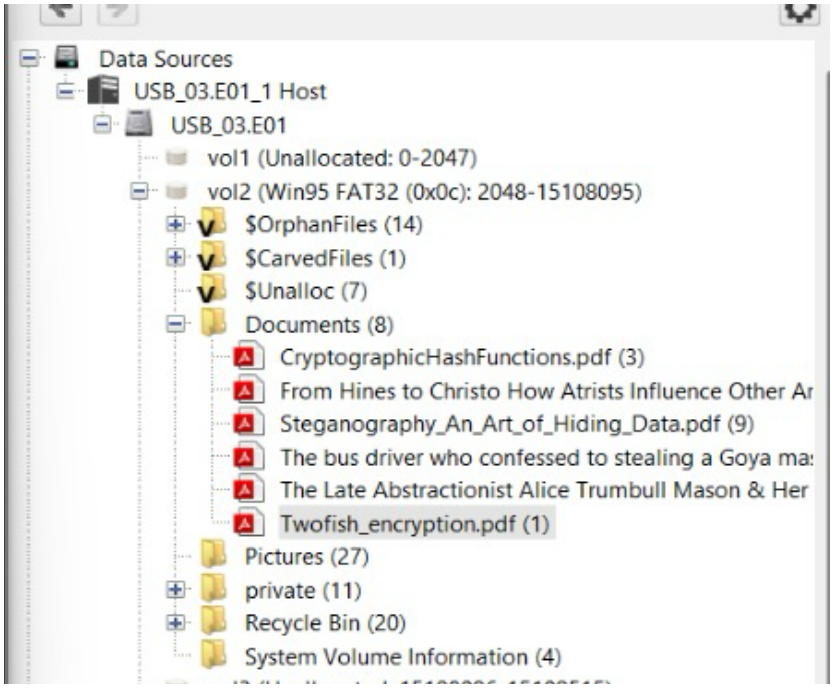


Which file (including the extension) will give access to the VeraCrypt container?

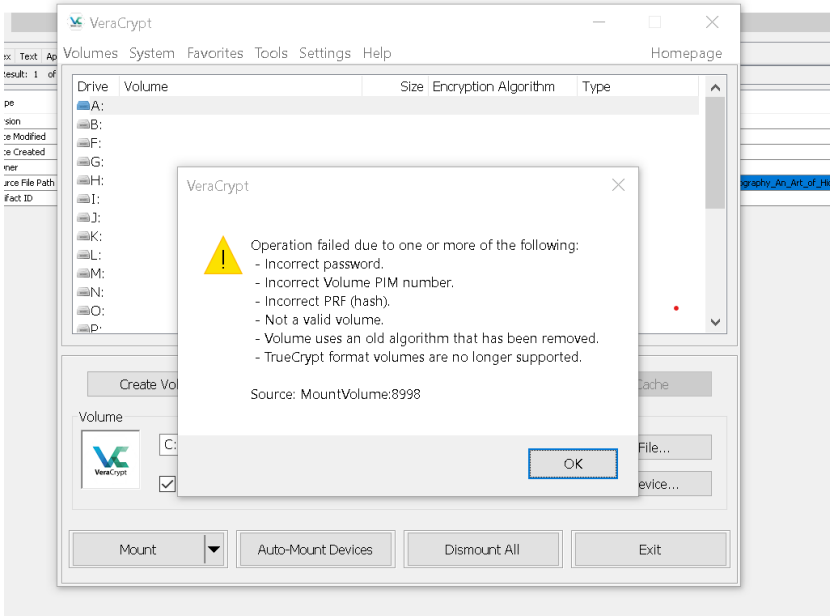


The file "supermoon.jpg" is suspected to be encrypted, and encryption activity has been detected. Given this, it is likely that "supermoon.jpg" contains the necessary data or key to access the VeraCrypt container.

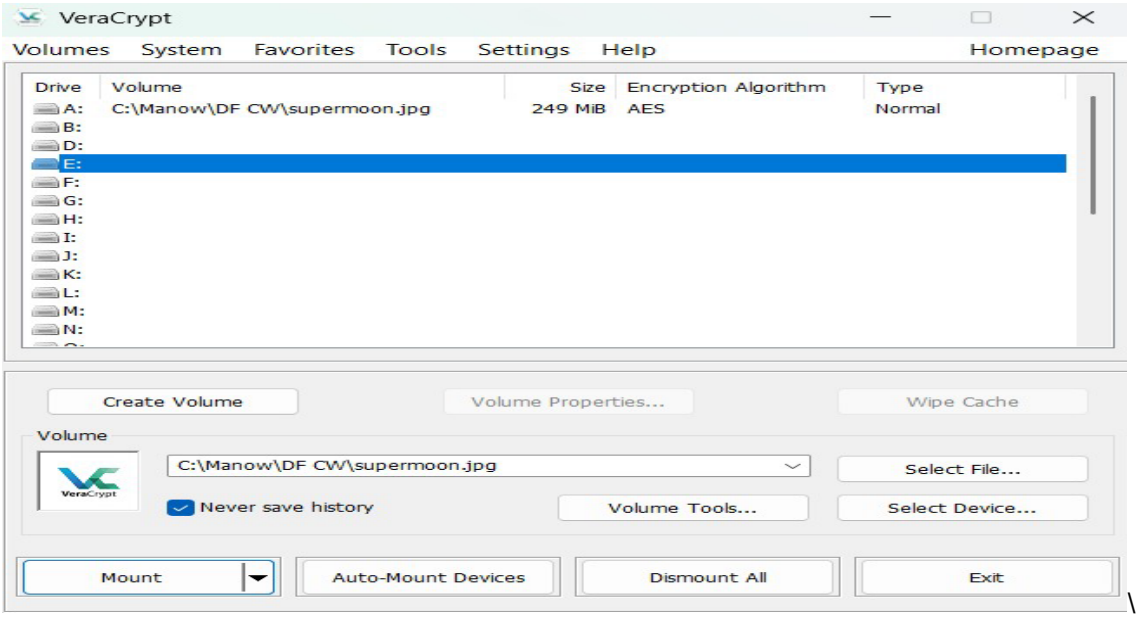
What is SHA256 hash that you generated to access the VeraCrypt container?



Within the vol2 directory, there is a folder named Documents containing six PDF files. Among these files, one holds the password in the form of a SHA-256 hash, which is used to access the VeraCrypt container.



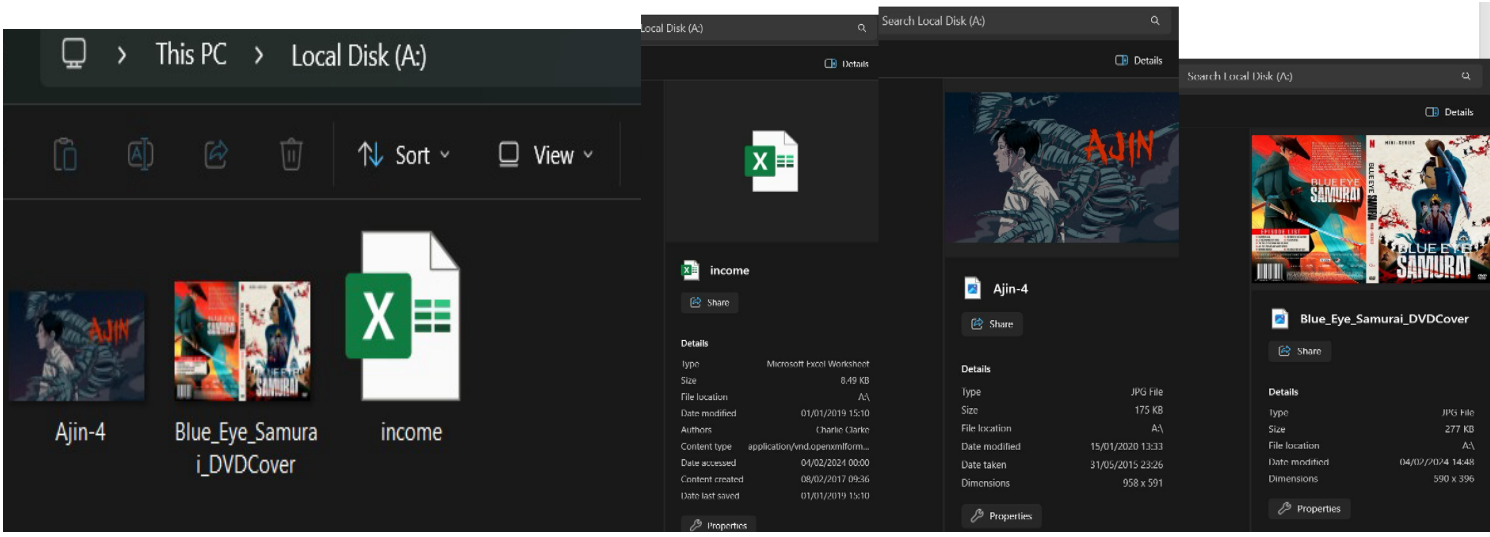
We initially generated a SHA-256 hash for the file "Steganography_An_Art_of_Hiding_Data.pdf", resulting in: 86348a07558bce3208ab3bc1ab7f3fa03345aad6856a7e10bd9f7beae867adc6 However, this hash did not grant access.



\

Next, we hashed "Twofish_encryption.pdf", obtaining:
cbca79cfd838aaae8b21f3df724fde090de17cb276dd82d78adfb48d984a36ae
This hash successfully unlocked the VeraCrypt container.

How many files found within the VeraCrypt container? Please write filename and file sizes for each file.



I found 3 files an excel sheet and 2 jpg files.

File Name	File size (KB)
Blue_Eye_Samurai_DVDCover	277
Ajin-4	175
income	8.49

How many collectors can be found in the income.xlsx file?

	A	B	C	D	E
1	**Collector**	**Years as client**	**Number of anime sales**	**Average sale price**	**Total income**
2	Jerry Dyson	1	81	£12	£972.00
3	Nancy Logan	1	12	£21	£252.00
4	Chris Deyl	2	67	£11	£737.00
5	Jodi S. Boling	2	79	£9	£711.00
6	Ermias Adonay	1	11	£20	£220.00
7	Norm Rico	1	4	£30	£120.00
8	Haddas Michael	1	12	£25	£300.00
9	Al Taiqraa	1	1	£60	£60.00
10	Vin Alvaro	2	87	£9	£783.00
11	Faye Fraser	1	8	£25	£200.00
12	Divya Jatin	2	71	£20	£1,420.00
13	Hirato kausaki	1	2	£56	£112.00
14	Galra Etik	1	15	£25	£375.00
15	Riya Naveen	1	9	£34	£306.00
16	Yi Wei	3	122	£8	£976.00
17	Manuela Klein	1	22	£24	£528.00
18	Abu Kalkalakh	1	12	£36	£432.00
19	Sabina Lovrić	1	32	£28	£896.00
20	Xiu Juan Jen	3	99	£12	£1,188.00
21	Rajesh Singh	2	43	£18	£774.00
22	Elliot Bould	2	69	£24	£1,656.00
23	**TOTALS**				**£11.362.00**

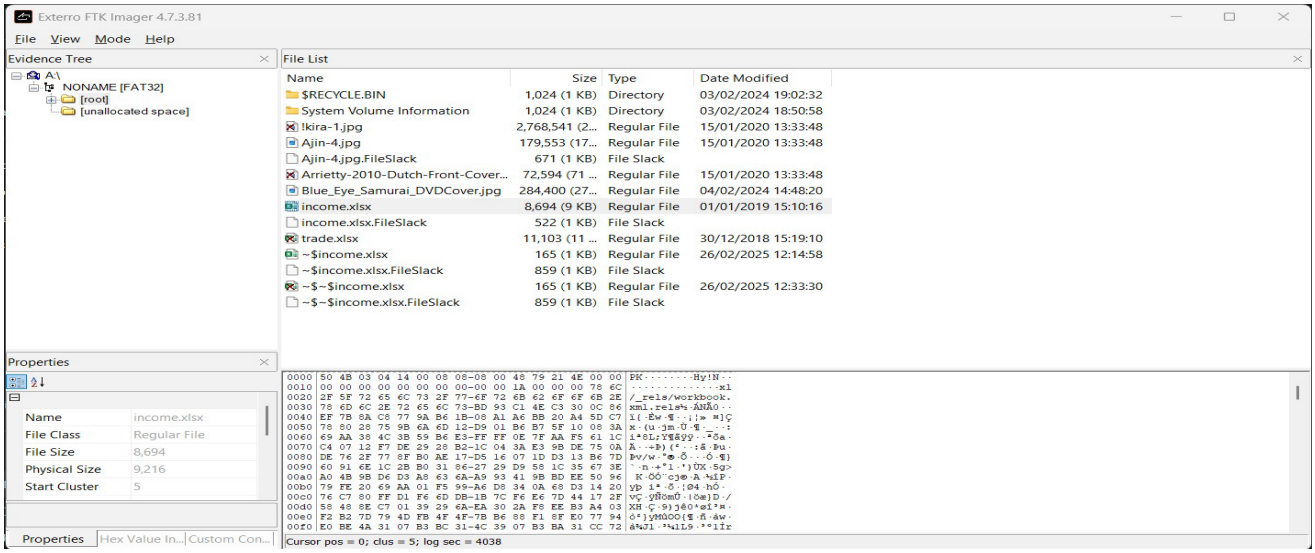
The number of collectors in the income.xlsx file is 21.

How many movie titles are listed in the second Excel file. How did you find this file?

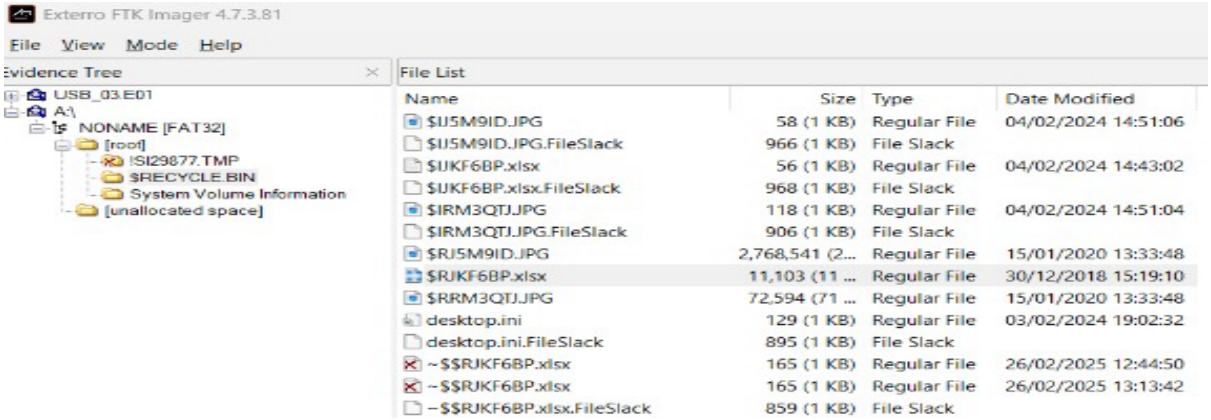
Since there is no second Excel file visible on the local disk and only three were originally present, it indicates that a hidden file is mounted on the disk. Additionally, by checking the properties of the Supermoon JPEG, we can confirm that the hidden file is not protected, making it easily accessible.

Property	Value
Location	C:\Manow\DF CW\supermoon.jpg
Size	261881856 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	5.9 MiB
Data Written since Mount	53 KiB

Furthermore, there are two ways to locate the hidden file: first, by extracting the contents of the Supermoon.jpg folder and then mounting it onto FDK Imager.



By mounting the image onto FTK Imager, we discovered 12 files, including two folders: $RECYCLE.BIN and System Volume Information. Additionally, we identified corrupted files, such as trade.xlsx. Inside the recycle bin folder is the movie titles file.

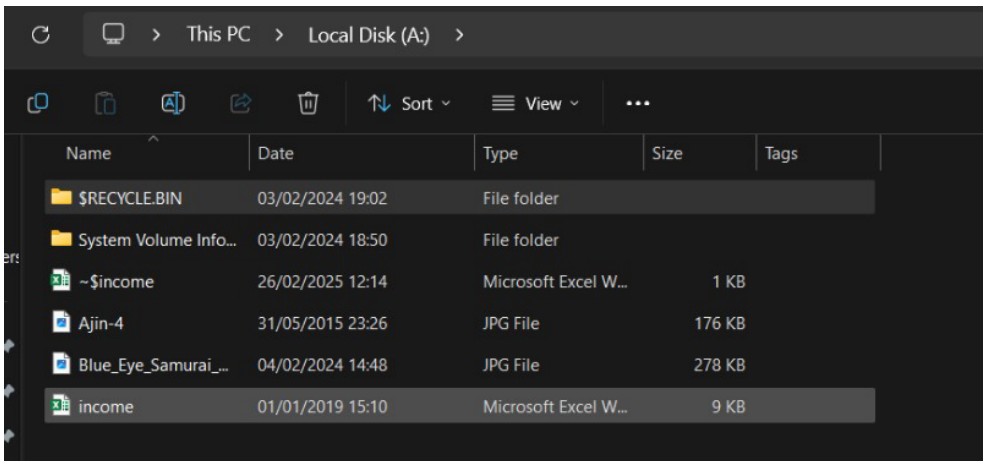


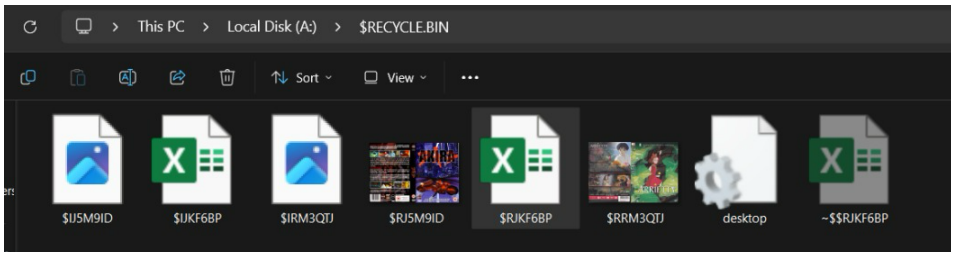
Another Excel file ($RJKF6BP.xlsx) in the Recycle Bin, suggesting an attempt to delete or conceal data.

Another way we also unreleased the hidden file sis using the terminal by inserting attrib -h -r -s /s /d A:\ .
(Fredrick, 2020)

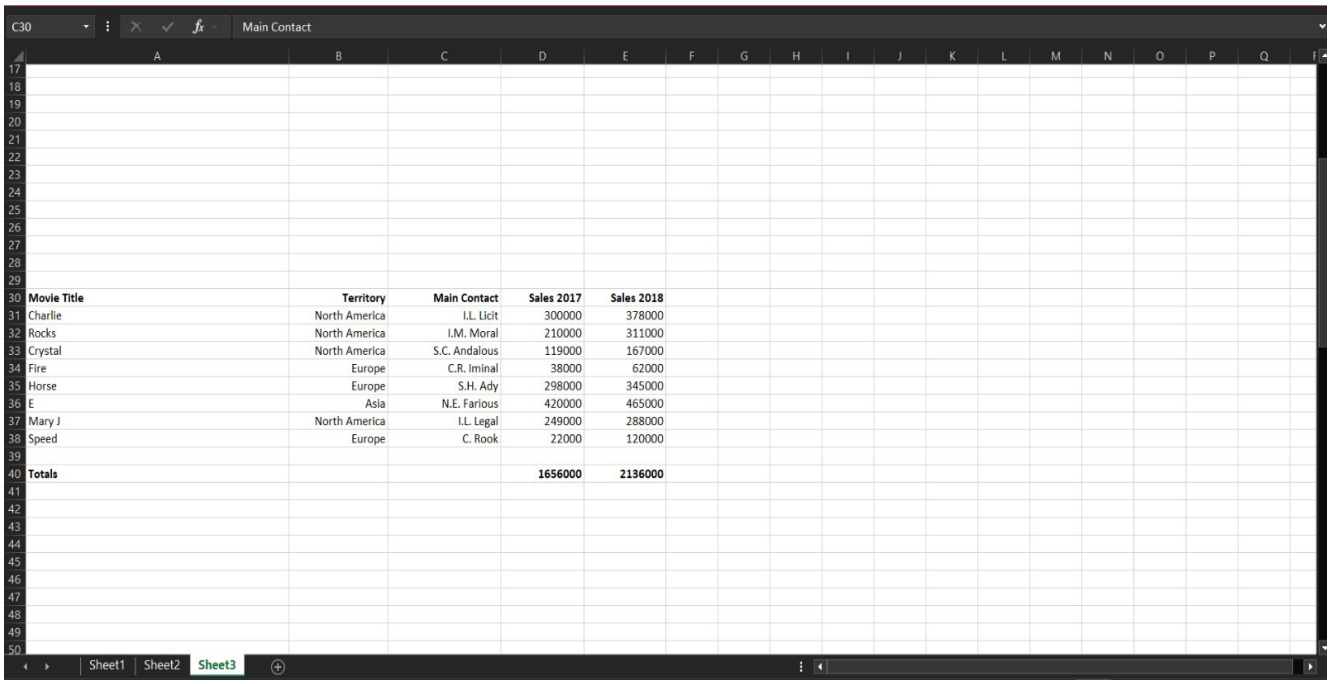
```
Last login: Fri Feb 28 17:49:50 on ttys002
(base) sawsanmounes@ABZ ~ % attrib -h -r -s /s /d A:\.
```

After entering this command into the terminal and pressing Enter, the hidden files became visible on the local disk.





By selecting the recycle bin as the victim could have potentially binned the excel sheet into there, we found a excel sheet called $RJKF6BP.



When the Excel sheet was opened, the movie titles were found hidden on page 3, line 30. These titles may potentially be linked to piracy.

Based on your investigation of the USB_03.E01 image and VeraCrypt contents, is there evidence of any crime? What evidence do you have?

The forensic investigation uncovered several indicators that may suggest piracy, though no definitive conclusions can be drawn.

Key findings:

- The forensic analysis suggests signs of potential piracy during the investigation, though no definitive conclusions can be drawn.
- A hidden Excel file ($RJKF6BP) found in the Recycle Bin contained movie titles placed on page 3, line 30, indicating an effort to obscure relevant information.
- Additionally, the file "supermoon.jpg" (2.6 GB) displayed extremely high entropy (7.999999), suggesting it was likely an encrypted container used to store concealed data, which was later accessed via VeraCrypt.
- Inside the decrypted VeraCrypt container, three notable files were found:
- A DVD cover (Blue_Eye_Samurai_DVDCover).
- An anime-related file (Ajin-4).
- An income spreadsheet listing 21 collectors, possibly indicating organized data tracking.
- Furthermore, a corrupted file named "trade.xlsx" was discovered, which could suggest an attempt to hide or remove information, whether intentional or accidental.
- Lastly, metadata analysis revealed that an Epson scanner was used to create "sword.art.online.full.jpg", raising the possibility that physical media, such as DVD covers or lists, were digitized.

The findings indicate possible attempts to store, encrypt, and track digital media, which may be relevant to piracy. However, the investigation cannot definitively confirm piracy based on the available evidence.

Conclusion

The forensic analysis of the seized USB images uncovered key findings, including encrypted files, hidden data, and suspicious activity. Hash verification confirmed the integrity of forensic images, while file signature analysis and metadata examination helped identify concealed information. The eo01_Sawsan.E01 image did not provide any conclusive evidence regarding the identity of the person who added the files, leaving the user anonymous. Meanwhile, USB_03.E01 contained an encrypted file (supermoon.jpg), hidden spreadsheets, and deleted data in the Recycle Bin, suggesting deliberate file concealment. While the investigation identified various digital artifacts and storage behaviours, additional analysis is needed to fully understand their relevance. This case underscores the importance of digital forensics in detecting hidden data, validating file authenticity, and preserving evidence integrity This case highlights the crucial role of digital forensics in uncovering concealed data, verifying file authenticity, and ensuring the integrity of evidence.

Appendix A

Evidence Chain of Custody Tracking Form

Case Number: 001

Offense: Digital Piracy

Submitting Officer: (Name/ID#) Sawsan MOUNES/Mou23620003

Victim: The Movie company

Suspect: Anonymous

Date/Time Seized: 9/02/25.

Location of Seizure: The movie company headquarters

Chain of Custody

Item	Date/Time	Released by	Received by	Comments/Location
USB_03.E01	9/02/25	James McCall	Sawsan MOUNES	Seized from the suspect's office, stored in a secured evidence locker.
eo01_Sawsan.E01	9/02/25	James McCall	Sawsan MOUNES	Captured forensic image of suspect's USB device, stored for analysis.

References

Duttke, J. (n.d.). *HexEd.it - Browser-based Online and Offline Hex Editing*. [online] HexEd.it. Available at: https://hexed.it/.

Fredrick, S. (2020). *What is the terminal command to view hidden folders in a git repo on VSCode?* [online] Stack Overflow. Available at: https://stackoverflow.com/questions/62107456/what-is-the-terminal-command-to-view-hidden-folders-in-a-git-repo-on-vscode.

Kessler, G. (2019). *File Signatures*. [online] Garykessler.net. Available at: https://www.garykessler.net/library/file_sigs.html.

Wikipedia Contributors (2019). *List of file signatures*. [online] Wikipedia. Available at: https://en.wikipedia.org/wiki/List_of_file_signatures.

.