COMP1812: Coursework 1 - 2022/2023

Operation Oval: Child Protection

Group: Student 1

1. Overview of the Case

1.1 Narrative of the case

A Group of Persons do Sexual grooming of a Child. They engages in predatory conduct to prepare a child person for sexual activity at a later time. They communicate to befriend and establish a relationship by emotional connection with the child. In this case A person engages in predatory conduct to prepare a child person to befriend and attach with her and emotionally or systematically capture her social media id. Their connection was established via social media platforms. He has partners for grooming of a child.

1.2 Timeline of key evidence

```
Image Information:
 Acquisition started:   Wed Nov  9 05:19:45 2022
 Acquisition finished:  Wed Nov  9 05:25:36 2022
 Segment list:
  F:\Hamidemon705\Evidence Files download\Mensil.E01
  F:\Hamidemon705\Evidence Files download\Mensil.E02
  F:\Hamidemon705\Evidence Files download\Mensil.E03

Image Verification Results:
 Verification started:  Wed Nov  9 05:25:37 2022
 Verification finished: Wed Nov  9 05:27:07 2022
```

1.3 Details of the offenders, victims and witnesses

A targeted child name arid tortoise sexually abused by offenders. Witness is child image & Project_1.pdf file collected from seizure device of offender.

1.4 Photographs of any physical evidence, clues or supplemental material

1.5 Scenario Rules

A tortoise represent a victim child image. Flag represent the Offender image. Sample Pendrive represent the seizure device from the offenders.

2. Legislation Analysis

2.1 Legislation

High quality and disaggregated data on all forms of child sexual exploitation and abuse collected. children and young people’s views are considered as a key element of the development of legislation related to online child sexual exploitation and abuse.

2.2 Points to prove

A Child emotionally abused by a grooming person & the person have partners for child sexual exploitation.

2.3 What the Digital Forensics case can prove

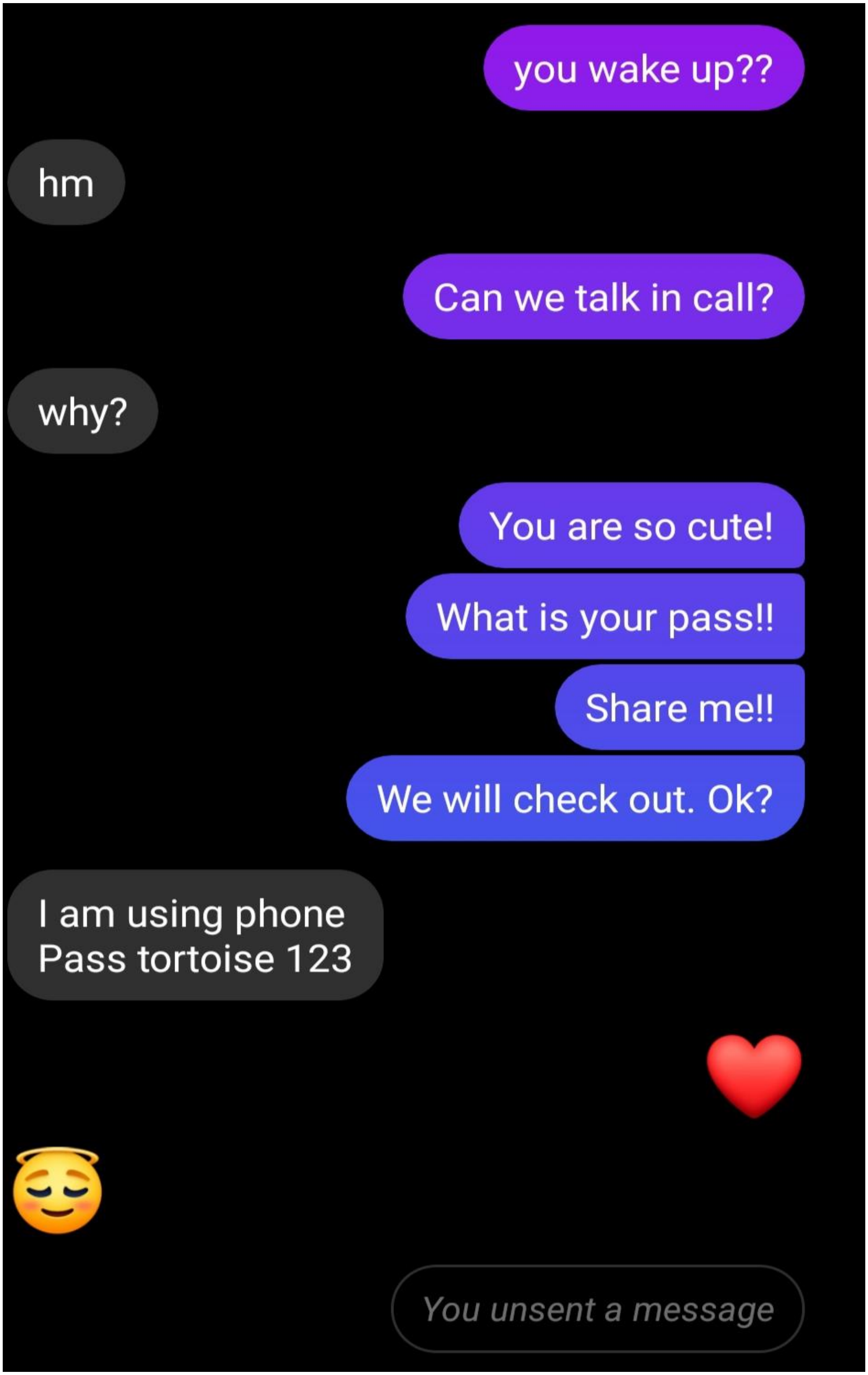
This Digital Forensics case can prove that who is the child, who is the offender & which member included with real offender.

2.4 What the Digital Forensics case will not prove

This Digital Forensics Case does not prove the exact location address of the offenders.

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

Here is social media chat between victim & offender that can prove, child emotionally attached with offender & offender treated her by like this and also the child social media id password collected by the offender. Attachment Below:



you wake up??

hm

Can we talk in call?

why?

You are so cute!

What is your pass!!

Share me!!

We will check out. Ok?

I am using phone
Pass tortoise 123

❤️

😇

You unsent a message

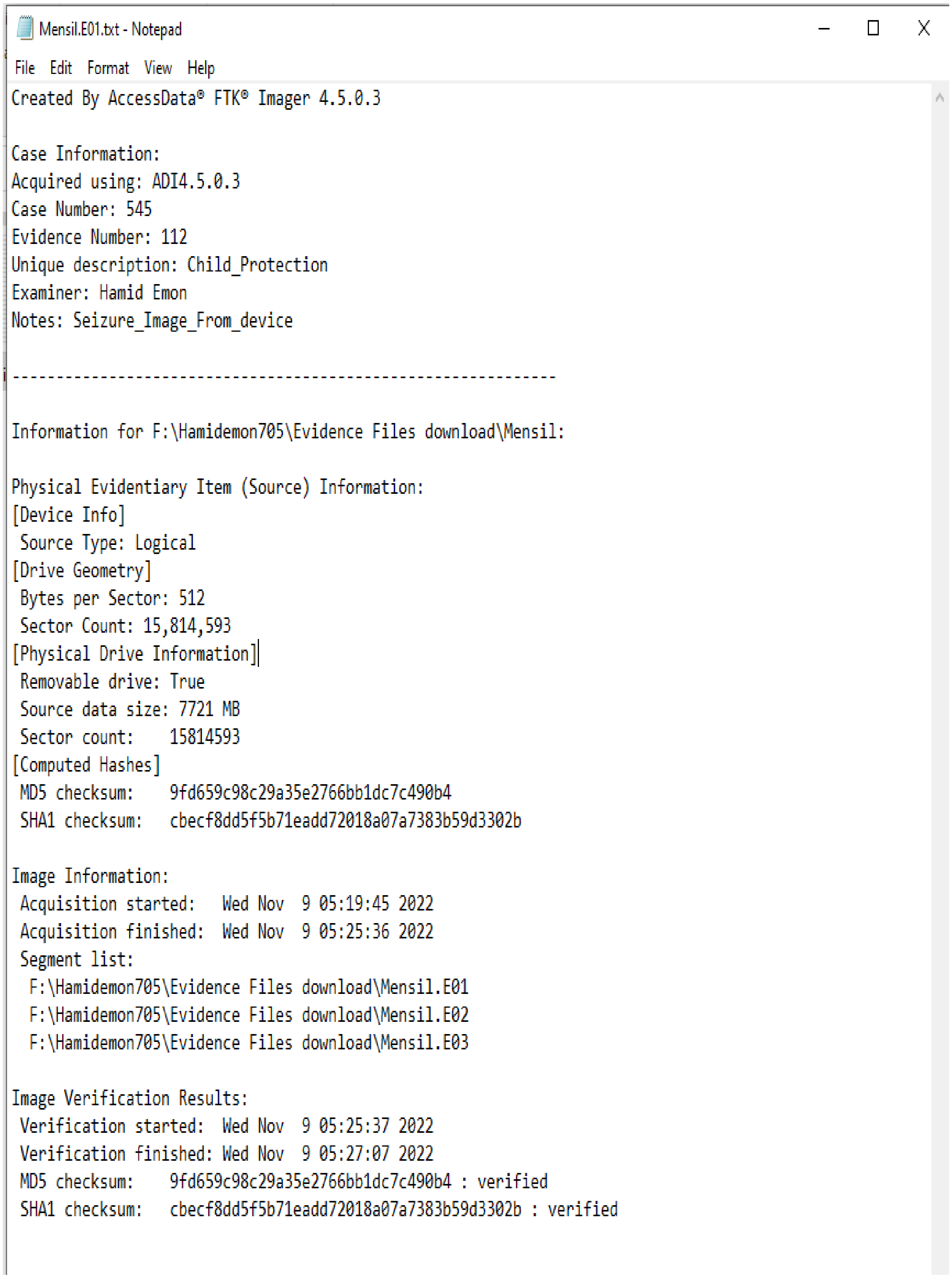
3. Evidence File

3.1 Details of the Evidence File

```
Created By AccessData® FTK® Imager 4.5.0.3

Case Information:
Acquired using: ADI4.5.0.3
Case Number: 545
Evidence Number: 112
Unique description: Child_Protection
Examiner: Hamid Emon
Notes: Seizure_Image_From_device

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

Information for F:\Hamidemon705\Evidence Files download\Mensil:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Logical
[Drive Geometry]
 Bytes per Sector: 512
 Sector Count: 15,814,593
[Physical Drive Information]
 Removable drive: True
 Source data size: 7721 MB
 Sector count:    15814593
Image Information:
 Acquisition started:   Wed Nov  9 05:19:45 2022
 Acquisition finished:  Wed Nov  9 05:25:36 2022
 Segment list:
  F:\Hamidemon705\Evidence Files download\Mensil.E01
  F:\Hamidemon705\Evidence Files download\Mensil.E02
  F:\Hamidemon705\Evidence Files download\Mensil.E03

Image Verification Results:
 Verification started:  Wed Nov  9 05:25:37 2022
 Verification finished: Wed Nov  9 05:27:07 2022
```

3.2 Hash value of the Evidence File

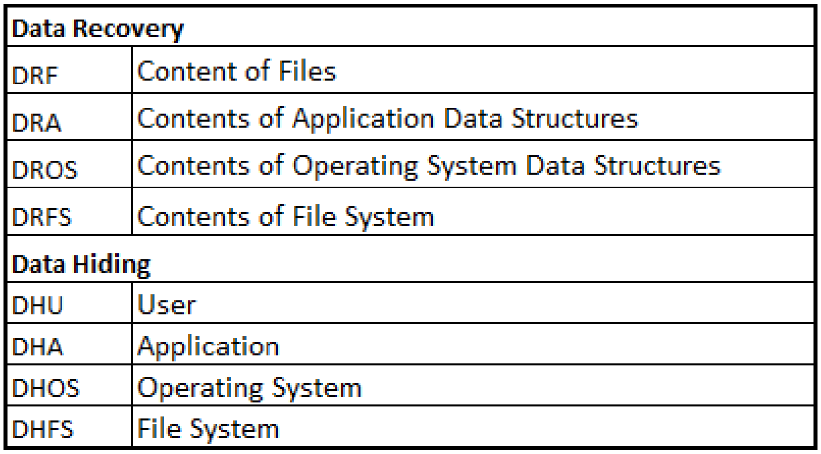
```
[Computed Hashes]
MD5 checksum:    9fd659c98c29a35e2766bb1dc7c490b4 : verified
 SHA1 checksum:   cbecf8dd5f5b71eadd72018a07a7383b59d3302b : verified
```



```
Created By AccessData® FTK® Imager 4.5.0.3

Case Information:
Acquired using: ADI4.5.0.3
Case Number: 545
Evidence Number: 112
Unique description: Child_Protection
Examiner: Hamid Emon
Notes: Seizure_Image_From_device


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


Information for F:\Hamidemon705\Evidence Files download\Mensil:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Logical
[Drive Geometry]
 Bytes per Sector: 512
 Sector Count: 15,814,593
[Physical Drive Information]
 Removable drive: True
 Source data size: 7721 MB
 Sector count:    15814593
[Computed Hashes]
 MD5 checksum:    9fd659c98c29a35e2766bb1dc7c490b4
 SHA1 checksum:   cbecf8dd5f5b71eadd72018a07a7383b59d3302b

Image Information:
 Acquisition started:   Wed Nov  9 05:19:45 2022
 Acquisition finished:  Wed Nov  9 05:25:36 2022
 Segment list:
  F:\Hamidemon705\Evidence Files download\Mensil.E01
  F:\Hamidemon705\Evidence Files download\Mensil.E02
  F:\Hamidemon705\Evidence Files download\Mensil.E03

Image Verification Results:
 Verification started:  Wed Nov  9 05:25:37 2022
 Verification finished: Wed Nov  9 05:27:07 2022
 MD5 checksum:    9fd659c98c29a35e2766bb1dc7c490b4 : verified
 SHA1 checksum:   cbecf8dd5f5b71eadd72018a07a7383b59d3302b : verified
```

4. Artefacts

4.1 Summary of Artefacts



Data Recovery	
DRF	Content of Files
DRA	Contents of Application Data Structures
DROS	Contents of Operating System Data Structures
DRFS	Contents of File System
Data Hiding	
DHU	User
DHA	Application
DHOS	Operating System
DHFS	File System

Figure 4.1 – Key for table 4.2

Category	Type	Number	Filename or Data Structure	Comment
DRF	Document File & Picture File	4.2.1	Project_1.pdf Arid-tortoise.jpg	Files containing the victim child image & Clarification.
DRA	Picture File	4.2.2	Chats.jpg	File containing some social media chat logs between victim & offender.
DROS	Registry File	4.2.3	.img_Mensil.E01/ Software_Hive	File containing the information about offender edited the victim image for sexually Abuse. Like tools and file.
DRFS	Document File	4.2.4	.img_Mensil.E01/ Deleted Files	Files containing information about child protection research article by UNICEF.
DHU	White text on white background	4.3.1	Something_ Bookmark.docx	Contains information about sexual abused images goes to online.
DHA	Audio file	4.3.2	Stegano.pdf	File Containing ethical consideration message for child protection.
DHOS	Unknown File(.sc)	4.3.3	Stegano.sc	File containing Data secret data hiding by changing the file extension
DHFS	Picture File	4.3.4	Catch me.jpg	File containing offender real image information.
DHU_1	Compressed File	4.3.5	Child_abused_ Image.zip	File Containing the victim child abused image.
DHU_2	Compressed File with Picture File	4.3.6	Gromming_ Partners.zip	File Containing the information of offender partners.
DHU_3	Text File	4.3.7	Link.txt	File containing information on a article related with online child sexual exploitation and abuse
DR_1	Image File	4.3.8	Victim.png	Here is Some secret string under this image. Containing information about victim real name.

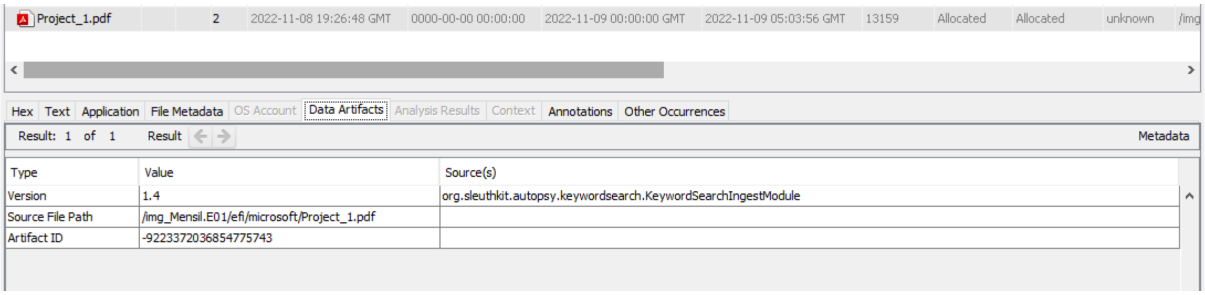
Table 4.2 – Summary Table of Artefacts

4.2 Data Recovery Artefacts

4.2.1 Category DRF

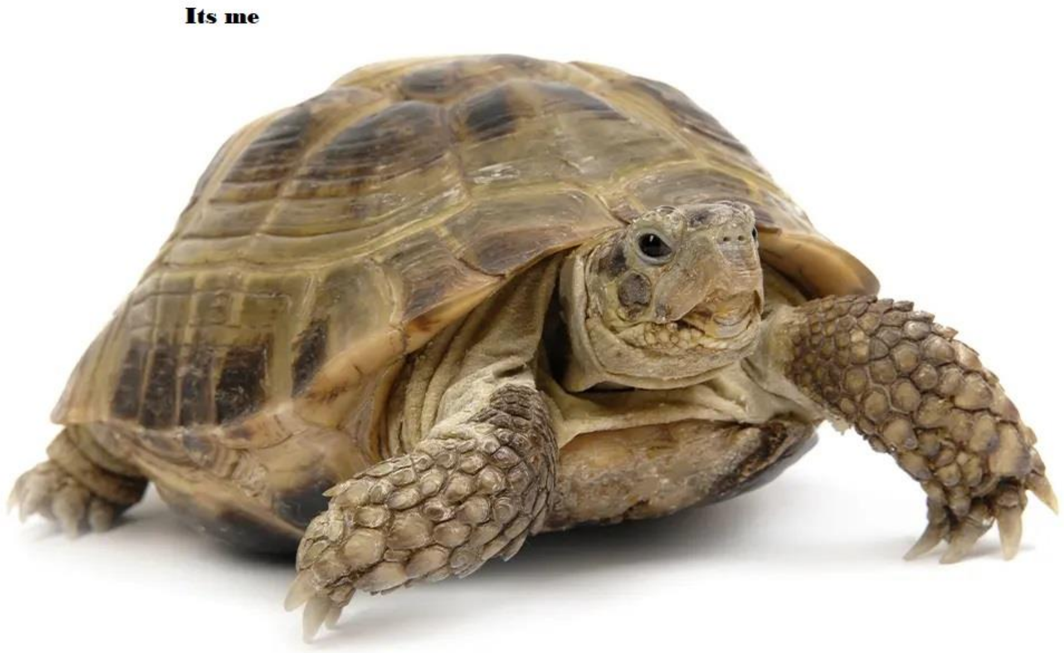
Screenshot of the artefact:

Content- Abusement– A tortoise we found from social media emotionally. We need to continue chatting with his favorite social media platform.



Project_1.pdf		2	2022-11-08 19:26:48 GMT	0000-00-00 00:00:00	2022-11-09 00:00:00 GMT	2022-11-09 05:03:56 GMT	13159	Allocated	Allocated	unknown	/img

Type	Value	Source(s)
Version	1.4	org.sleuthkit.autopsy.keywordsearch.KeywordSearchIngestModule
Source File Path	/img_Mensil.E01/efi/microsoft/Project_1.pdf	
Artifact ID	-9223372036854775743	



A screenshot of artefact evidence details:

Metadata

Name:	/img_Mensil.E01/efi/microsoft/Project_1.pdf
Type:	File System
MIME Type:	application/pdf
Size:	13159
File Name Allocation:	Allocated

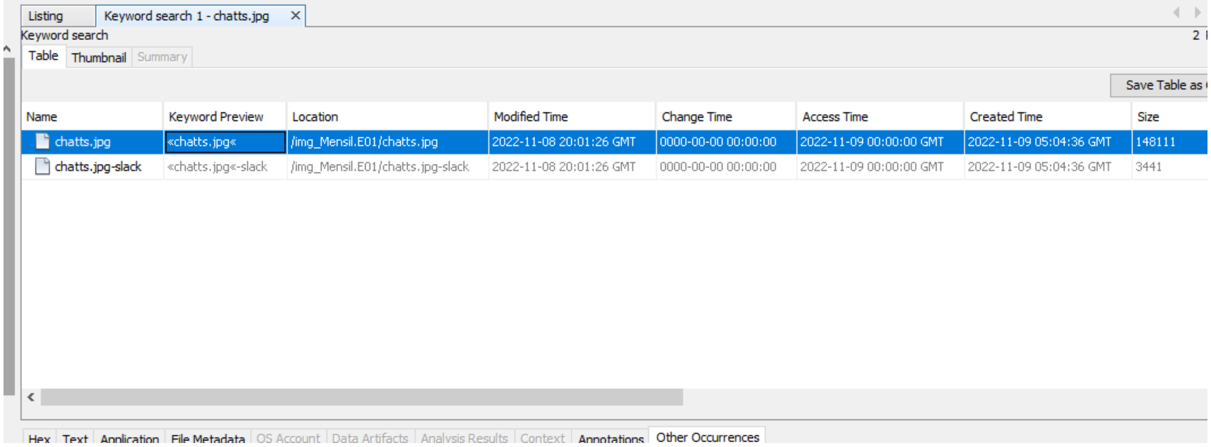
Metadata Allocation:	Allocated
Modified:	2022-11-08 19:26:48 GMT
Accessed:	2022-11-09 00:00:00 GMT
Created:	2022-11-09 05:03:56 GMT
Changed:	0000-00-00 00:00:00
MD5:	ff711451343cb686d9910b5c3d94a077
SHA-256:	7afd65bee62d08e5bfb4996e387fd134591a54f27db56c16a2f8a3901176ac3d
Hash Lookup Results:	UNKNOWN
Internal ID:	1969

Description and implications of the artefact:

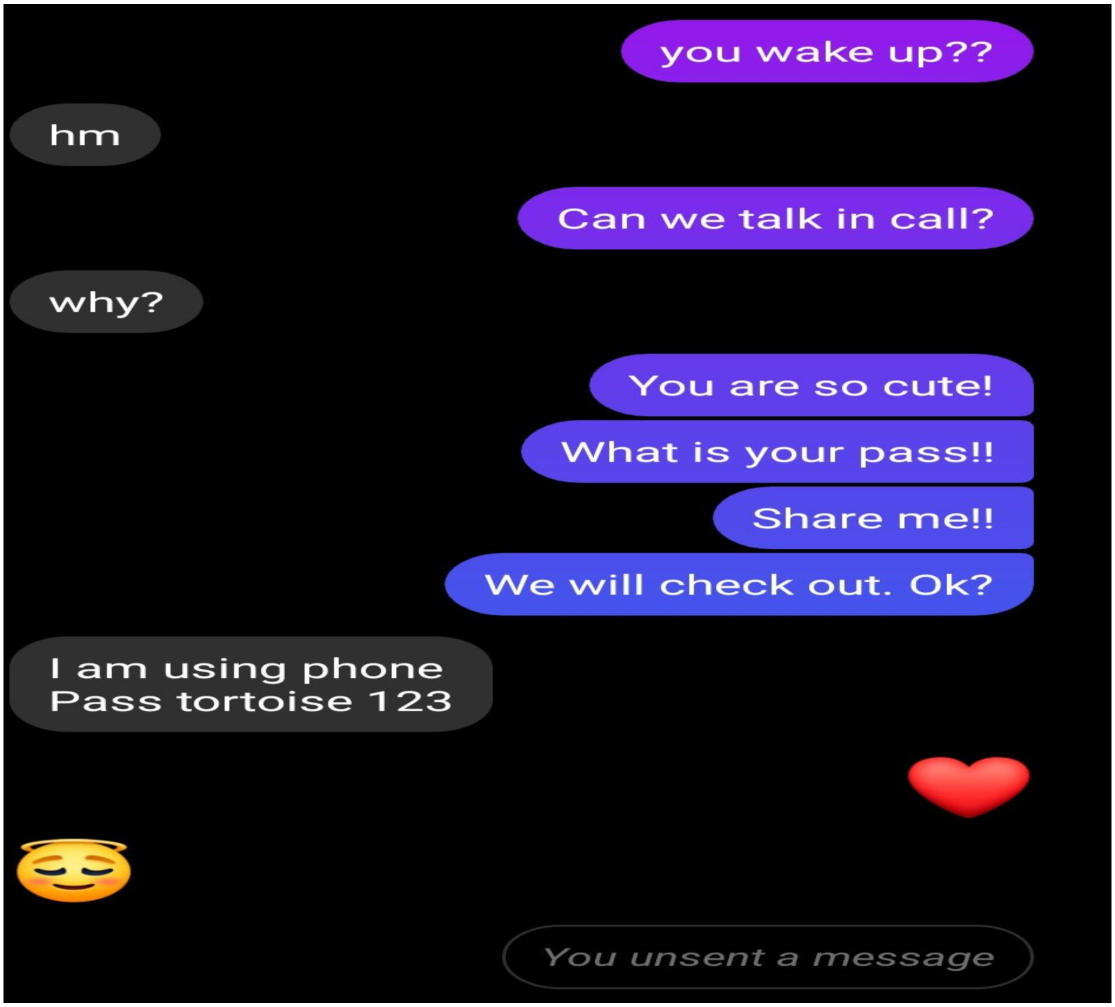
This Document ensure that offender found a child person from social media by contacting emotionally. They planned for continue the chat in social media platform with her. They mentioned her name & we found the named picture. So that is relevant that the victim.

4.2.2 Category DRA

Screenshot of the artefact:



Name	Keyword Preview	Location	Modified Time	Change Time	Access Time	Created Time	Size
chatts.jpg	«chatts.jpg«	/img_Mensil.E01/chatts.jpg	2022-11-08 20:01:26 GMT	0000-00-00 00:00:00	2022-11-09 00:00:00 GMT	2022-11-09 05:04:36 GMT	148111
chatts.jpg-slack	«chatts.jpg«-slack	/img_Mensil.E01/chatts.jpg-slack	2022-11-08 20:01:26 GMT	0000-00-00 00:00:00	2022-11-09 00:00:00 GMT	2022-11-09 05:04:36 GMT	3441



you wake up??

hm

Can we talk in call?

why?

You are so cute!

What is your pass!!

Share me!!

We will check out. Ok?

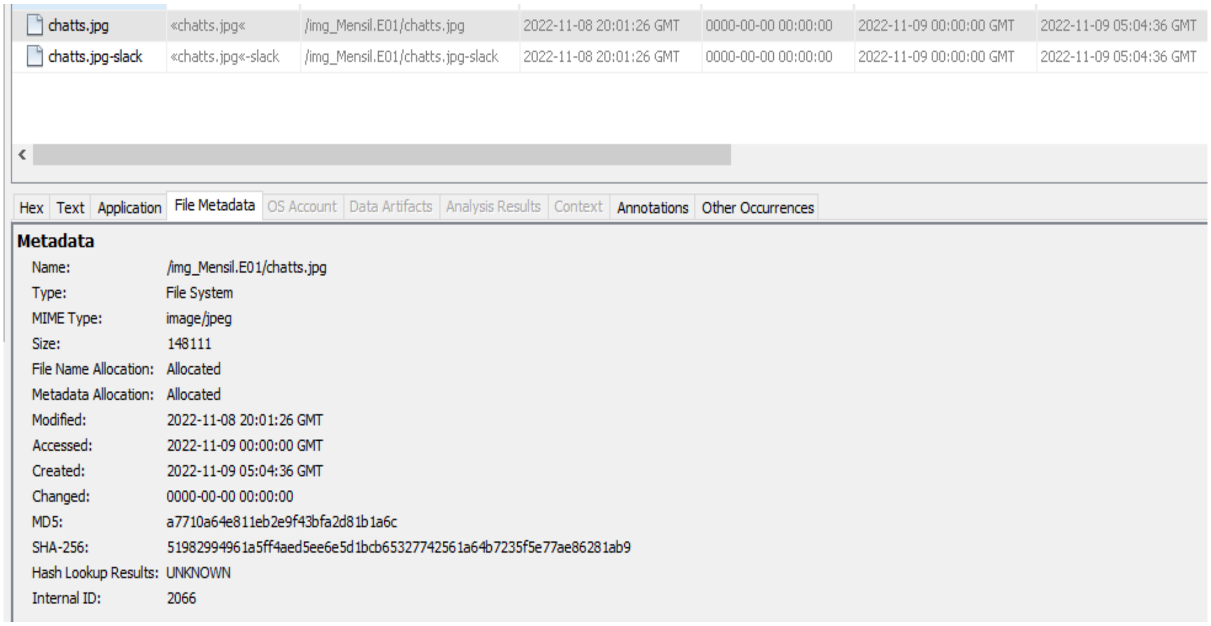
I am using phone
Pass tortoise 123

❤️

😇

You unsent a message

A screenshot of artefact evidence details:



chatts.jpg	«chatts.jpg«	/img_Mensil.E01/chatts.jpg	2022-11-08 20:01:26 GMT	0000-00-00 00:00:00	2022-11-09 00:00:00 GMT	2022-11-09 05:04:36 GMT
chatts.jpg-slack	«chatts.jpg«-slack	/img_Mensil.E01/chatts.jpg-slack	2022-11-08 20:01:26 GMT	0000-00-00 00:00:00	2022-11-09 00:00:00 GMT	2022-11-09 05:04:36 GMT

Metadata

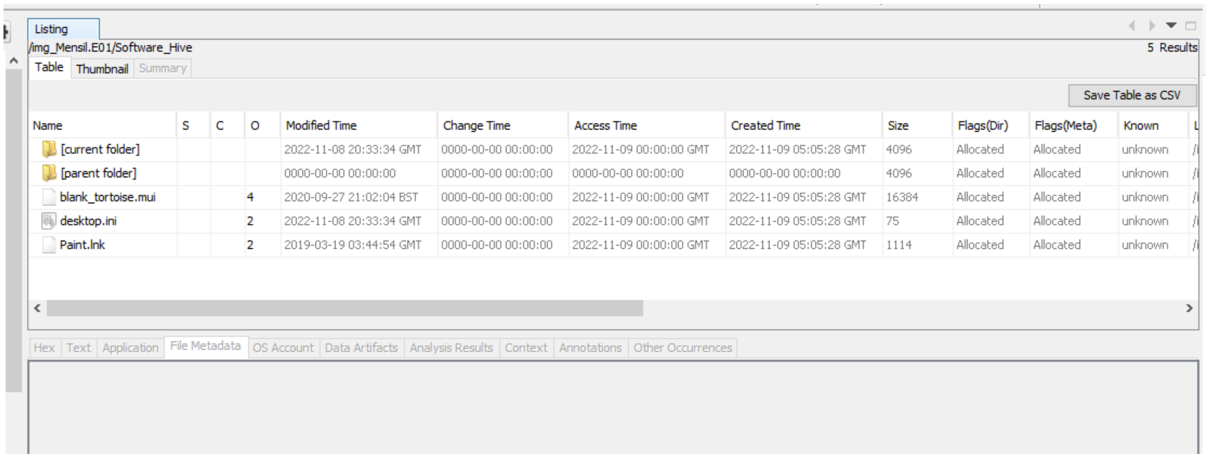
```
Name:                  /img_Mensil.E01/chatts.jpg
Type:                  File System
MIME Type:             image/jpeg
Size:                  148111
File Name Allocation:  Allocated
Metadata Allocation:   Allocated
Modified:              2022-11-08 20:01:26 GMT
Accessed:              2022-11-09 00:00:00 GMT
Created:               2022-11-09 05:04:36 GMT
Changed:               0000-00-00 00:00:00
MD5:                   a7710a64e811eb2e9f43bfa2d81b1a6c
SHA-256:               51982994961a5ff4aed5ee6e5d1bcb65327742561a64b7235f5e77ae86281ab9
Hash Lookup Results:   UNKNOWN
Internal ID:           2066
```

Description and implications of the artefact:

Here is social media chat between victim & offender that can prove, child emotionally attached with offender & offender treated her by like this and also the child social media id password collected by the offender.

4.2.3 Category DROS

Screenshot of the artefact:

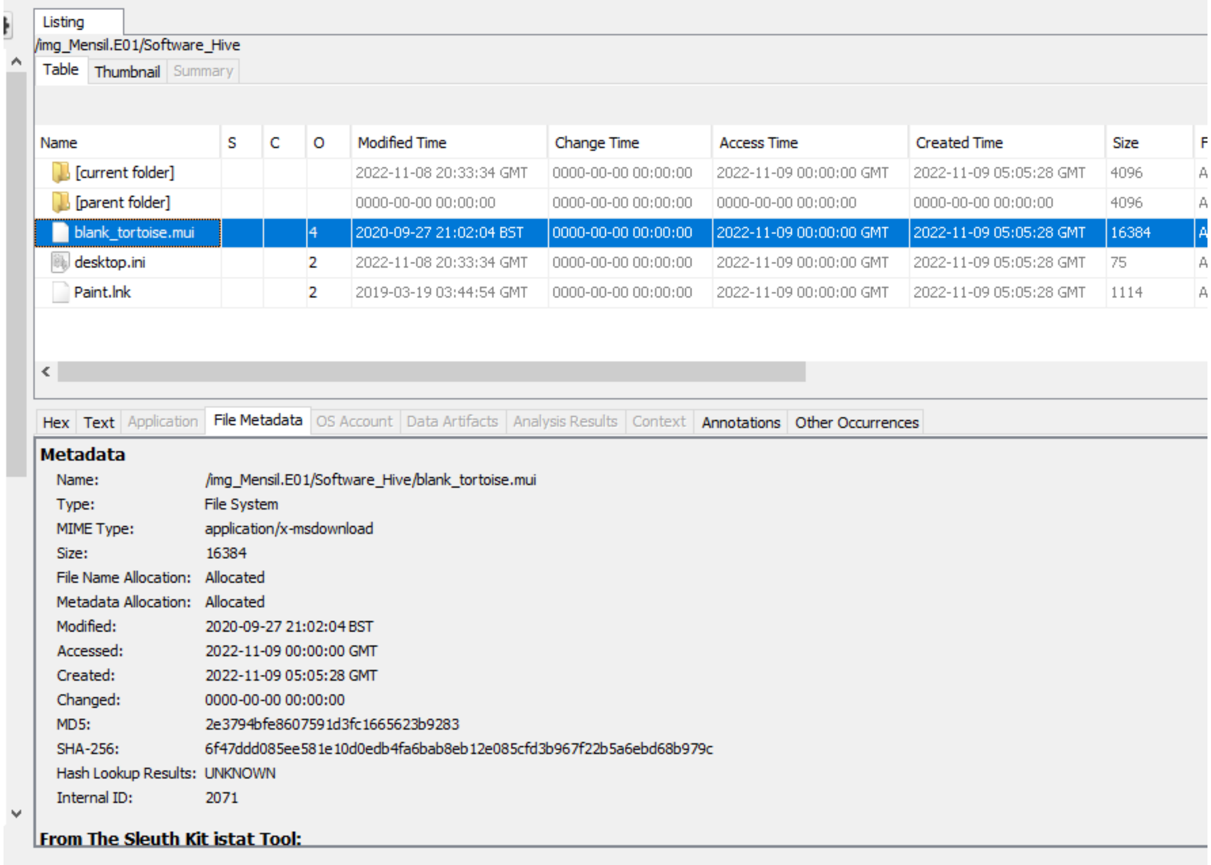


/img_Mensil.E01/Software_Hive

5 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	L
[current folder]				2022-11-08 20:33:34 GMT	0000-00-00 00:00:00	2022-11-09 00:00:00 GMT	2022-11-09 05:05:28 GMT	4096	Allocated	Allocated	unknown	/i
[parent folder]				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4096	Allocated	Allocated	unknown	/i
blank_tortoise.mui			4	2020-09-27 21:02:04 BST	0000-00-00 00:00:00	2022-11-09 00:00:00 GMT	2022-11-09 05:05:28 GMT	16384	Allocated	Allocated	unknown	/i
desktop.ini			2	2022-11-08 20:33:34 GMT	0000-00-00 00:00:00	2022-11-09 00:00:00 GMT	2022-11-09 05:05:28 GMT	75	Allocated	Allocated	unknown	/i
Paint.lnk			2	2019-03-19 03:44:54 GMT	0000-00-00 00:00:00	2022-11-09 00:00:00 GMT	2022-11-09 05:05:28 GMT	1114	Allocated	Allocated	unknown	/i

A screenshot of artefact evidence details:



/img_Mensil.E01/Software_Hive

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	F
[current folder]				2022-11-08 20:33:34 GMT	0000-00-00 00:00:00	2022-11-09 00:00:00 GMT	2022-11-09 05:05:28 GMT	4096	A
[parent folder]				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4096	A
blank_tortoise.mui			4	2020-09-27 21:02:04 BST	0000-00-00 00:00:00	2022-11-09 00:00:00 GMT	2022-11-09 05:05:28 GMT	16384	A
desktop.ini			2	2022-11-08 20:33:34 GMT	0000-00-00 00:00:00	2022-11-09 00:00:00 GMT	2022-11-09 05:05:28 GMT	75	A
Paint.lnk			2	2019-03-19 03:44:54 GMT	0000-00-00 00:00:00	2022-11-09 00:00:00 GMT	2022-11-09 05:05:28 GMT	1114	A

Metadata

Name:	/img_Mensil.E01/Software_Hive/blank_tortoise.mui
Type:	File System
MIME Type:	application/x-msdownload
Size:	16384
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2020-09-27 21:02:04 BST
Accessed:	2022-11-09 00:00:00 GMT
Created:	2022-11-09 05:05:28 GMT
Changed:	0000-00-00 00:00:00
MD5:	2e3794bfe8607591d3fc1665623b9283
SHA-256:	6f47ddd085ee581e10d0edb4fa6bab8eb12e085cfd3b967f22b5a6ebd68b979c
Hash Lookup Results:	UNKNOWN
Internal ID:	2071

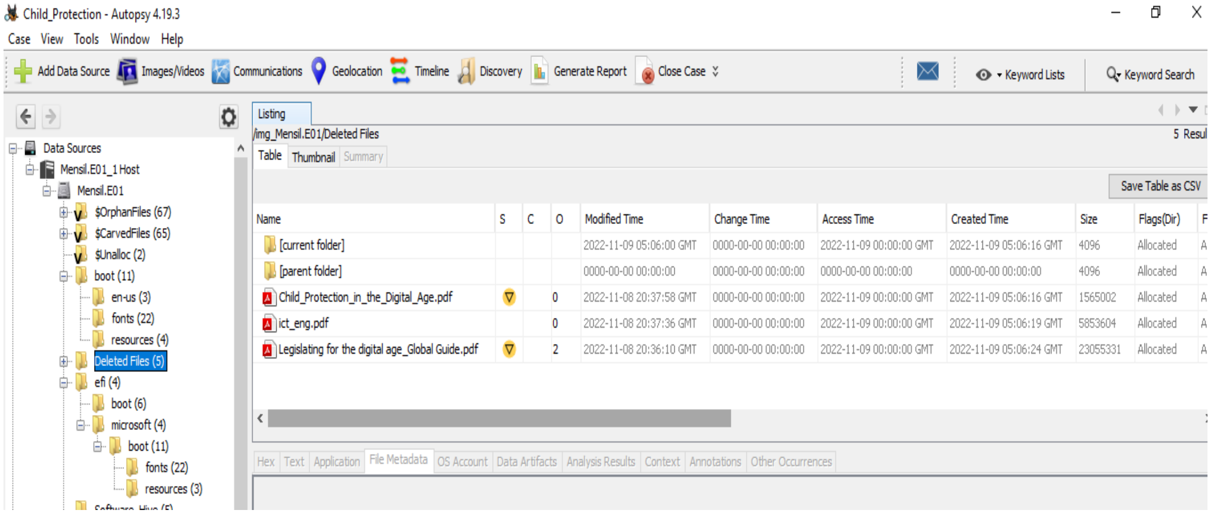
From The Sleuth Kit istat Tool:

Description and implications of the artefact:

Victim Image edited by this software. For make sexual abusement image edited by paint software & the files hives saved.

4.2.4 Category DRFS

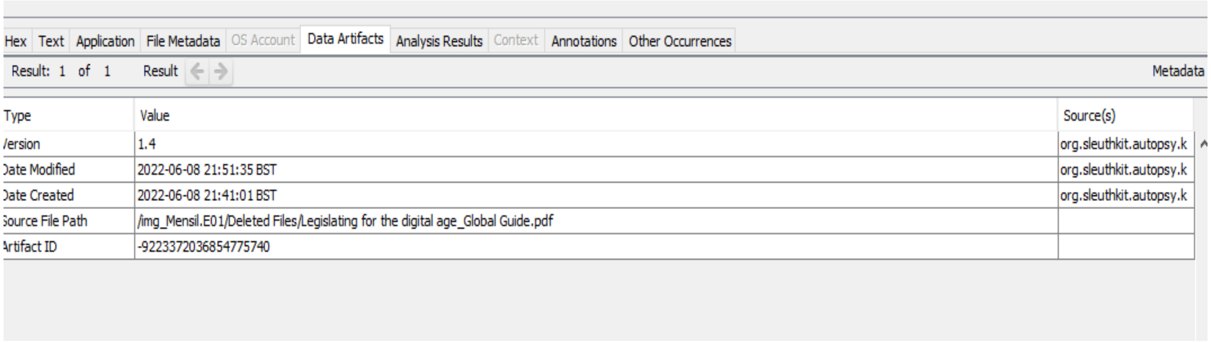
Screenshot of the artefact:



/img_Mensil.E01/Deleted Files

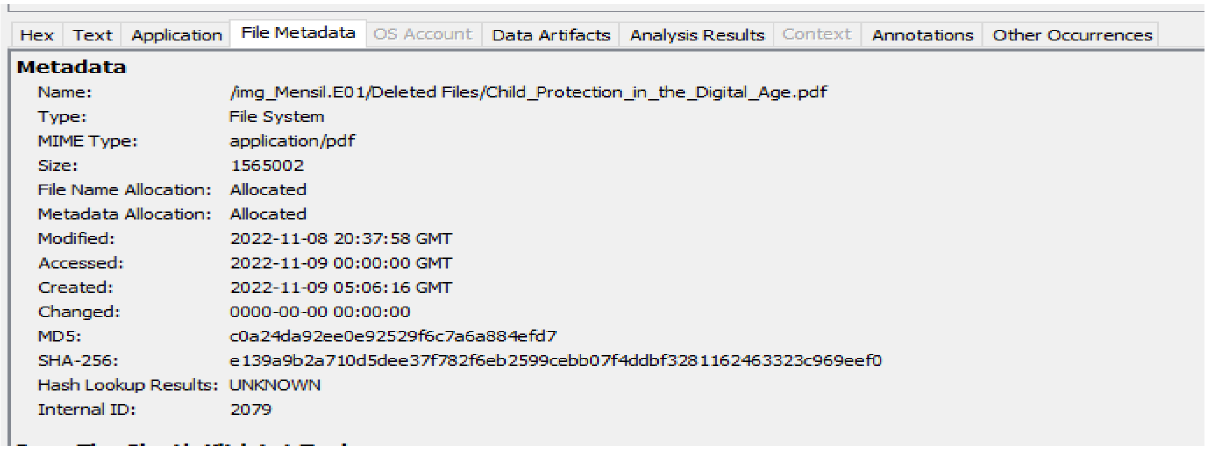
5 Resul

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	F
[current folder]				2022-11-09 05:06:00 GMT	0000-00-00 00:00:00	2022-11-09 00:00:00 GMT	2022-11-09 05:06:16 GMT	4096	Allocated	A
[parent folder]				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4096	Allocated	A
Child_Protection_in_the_Digital_Age.pdf	▽		0	2022-11-08 20:37:58 GMT	0000-00-00 00:00:00	2022-11-09 00:00:00 GMT	2022-11-09 05:06:16 GMT	1565002	Allocated	A
ict_eng.pdf			0	2022-11-08 20:37:36 GMT	0000-00-00 00:00:00	2022-11-09 00:00:00 GMT	2022-11-09 05:06:19 GMT	5853604	Allocated	A
Legislating for the digital age_Global Guide.pdf	▽		2	2022-11-08 20:36:10 GMT	0000-00-00 00:00:00	2022-11-09 00:00:00 GMT	2022-11-09 05:06:24 GMT	23055331	Allocated	A



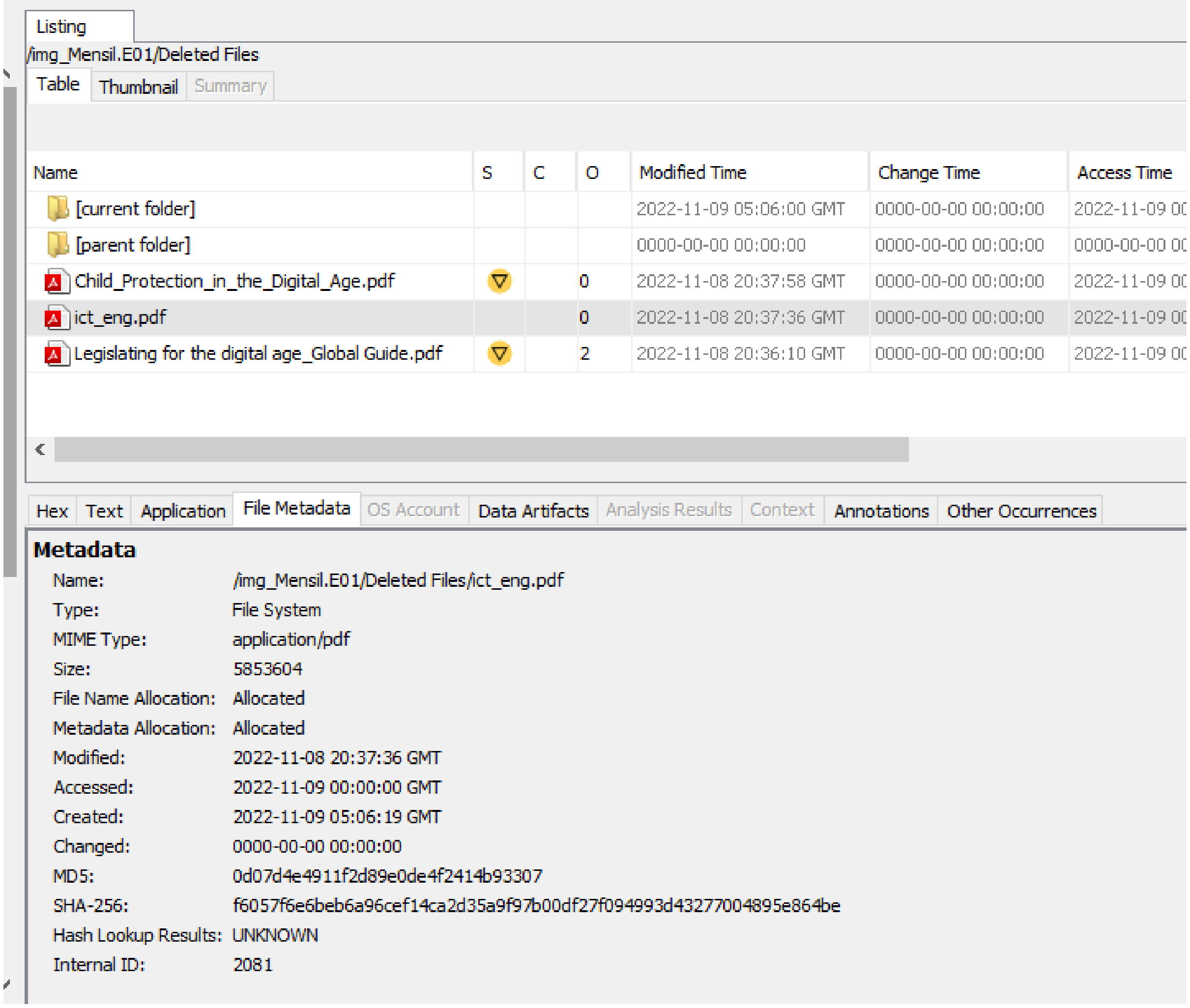
Type	Value	Source(s)
Version	1.4	org.sleuthkit.autopsy.k
Date Modified	2022-06-08 21:51:35 BST	org.sleuthkit.autopsy.k
Date Created	2022-06-08 21:41:01 BST	org.sleuthkit.autopsy.k
Source File Path	/img_Mensil.E01/Deleted Files/Legislating for the digital age_Global Guide.pdf	
Artifact ID	-9223372036854775740	

A screenshot of artefact evidence details:



Metadata

```
Name:                   /img_Mensil.E01/Deleted Files/Child_Protection_in_the_Digital_Age.pdf
Type:                   File System
MIME Type:              application/pdf
Size:                   1565002
File Name Allocation:   Allocated
Metadata Allocation:    Allocated
Modified:               2022-11-08 20:37:58 GMT
Accessed:               2022-11-09 00:00:00 GMT
Created:                2022-11-09 05:06:16 GMT
Changed:                0000-00-00 00:00:00
MD5:                    c0a24da92ee0e92529f6c7a6a884efd7
SHA-256:                e139a9b2a710d5dee37f782f6eb2599cebb07f4ddbf3281162463323c969eef0
Hash Lookup Results:    UNKNOWN
Internal ID:            2079
```

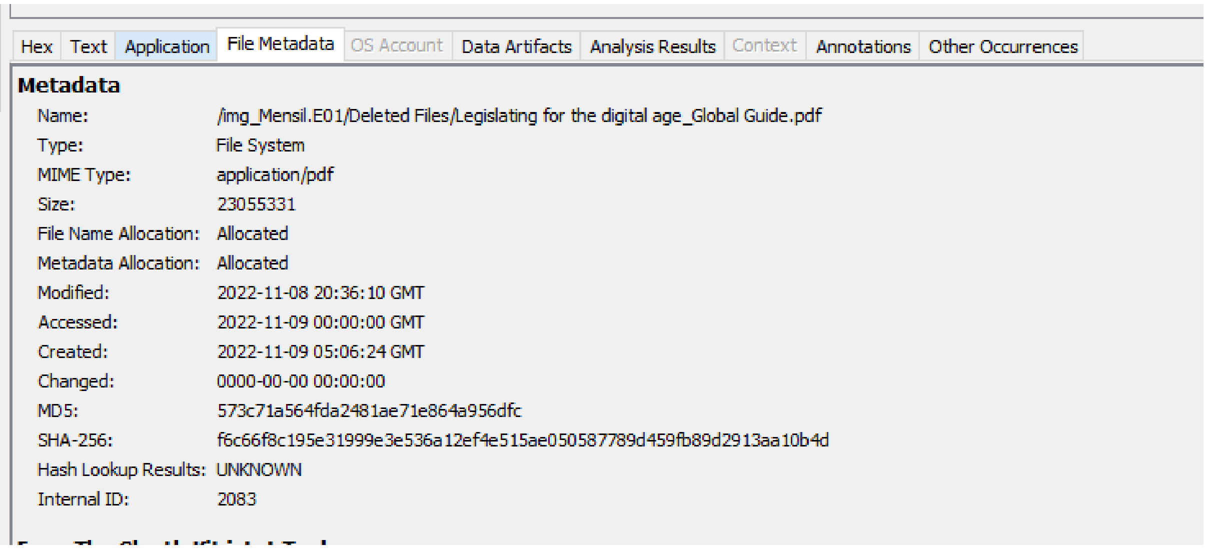


/img_Mensil.E01/Deleted Files

Name	S	C	O	Modified Time	Change Time	Access Time
[current folder]				2022-11-09 05:06:00 GMT	0000-00-00 00:00:00	2022-11-09 00
[parent folder]				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00
Child_Protection_in_the_Digital_Age.pdf	▽		0	2022-11-08 20:37:58 GMT	0000-00-00 00:00:00	2022-11-09 00
ict_eng.pdf			0	2022-11-08 20:37:36 GMT	0000-00-00 00:00:00	2022-11-09 00
Legislating for the digital age_Global Guide.pdf	▽		2	2022-11-08 20:36:10 GMT	0000-00-00 00:00:00	2022-11-09 00

Metadata

```
Name:                   /img_Mensil.E01/Deleted Files/ict_eng.pdf
Type:                   File System
MIME Type:              application/pdf
Size:                   5853604
File Name Allocation:   Allocated
Metadata Allocation:    Allocated
Modified:               2022-11-08 20:37:36 GMT
Accessed:               2022-11-09 00:00:00 GMT
Created:                2022-11-09 05:06:19 GMT
Changed:                0000-00-00 00:00:00
MD5:                    0d07d4e4911f2d89e0de4f2414b93307
SHA-256:                f6057f6e6beb6a96cef14ca2d35a9f97b00df27f094993d43277004895e864be
Hash Lookup Results:    UNKNOWN
Internal ID:            2081
```



Metadata

Name:	/img_Mensil.E01/Deleted Files/Legislating for the digital age_Global Guide.pdf
Type:	File System
MIME Type:	application/pdf
Size:	23055331
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-11-08 20:36:10 GMT
Accessed:	2022-11-09 00:00:00 GMT
Created:	2022-11-09 05:06:24 GMT
Changed:	0000-00-00 00:00:00
MD5:	573c71a564fda2481ae71e864a956dfc
SHA-256:	f6c66f8c195e31999e3e536a12ef4e515ae050587789d459fb89d2913aa10b4d
Hash Lookup Results:	UNKNOWN
Internal ID:	2083

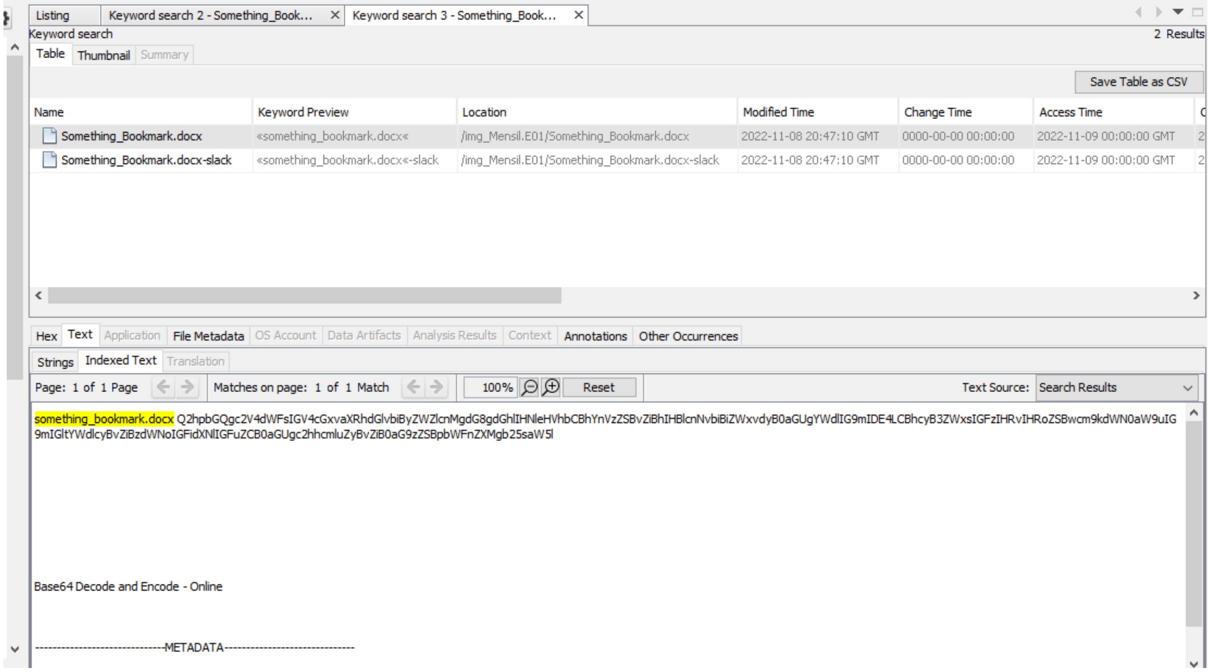
Description and implications of the artefact:

This Section clarify that offenders analysis the article on Child protection in the digital age & legislation on Global Guidance. Thinking to bypass the Digital law inforcement.

4.3 Data Hiding Artefacts

4.3.1 Category DHU

Screenshot of the artefact:



Listing
Keyword search 2 - Something_Book...
Keyword search 3 - Something_Book...
Keyword search
2 Results
Table
Thumbnail
Summary
Save Table as CSV

Name	Keyword Preview	Location	Modified Time	Change Time	Access Time
Something_Bookmark.docx	«something_bookmark.docx«	/img_Mensil.E01/Something_Bookmark.docx	2022-11-08 20:47:10 GMT	0000-00-00 00:00:00	2022-11-09 00:00:00 GMT
Something_Bookmark.docx-slack	«something_bookmark.docx«-slack	/img_Mensil.E01/Something_Bookmark.docx-slack	2022-11-08 20:47:10 GMT	0000-00-00 00:00:00	2022-11-09 00:00:00 GMT

something_bookmark.docx Q2hpbGQgc2V4dWFsIGV4cGxvaXRhdGlvbiByZWZlcnMgdG8gdGhlIHNleHVhbCBhYnVzZSBvZiBhIHBlcnNvbiBiZWxvdyB0aGUgYWdlIG9mIDE4LCBhcyB3ZWxsIGFzIHRvIHRoZSBwcm9kdWN0aW9uIG
9mIGltYWdlcyBvZiBzdWNoIGFidXNlIGFuZCB0aGUgc2hhcmluZyBvZiB0aG9zZSBpbWFnZXMgb25saW5l

Base64 Decode and Encode - Online

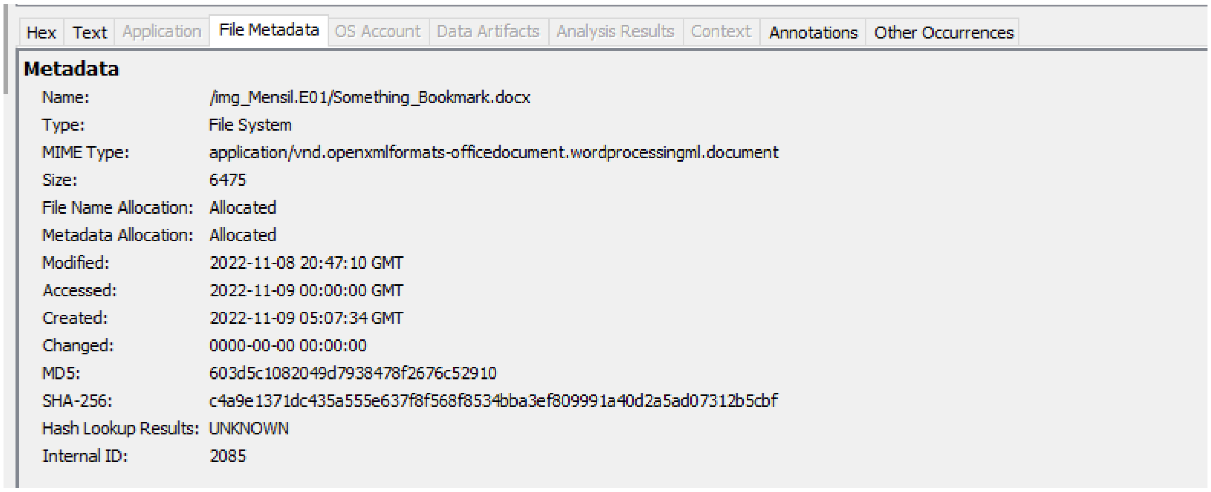
----------------------------METADATA----------------------------

Content:

Q2hpbGQgc2V4dWFsIGV4cGxvaXRhdGlvbiByZWZlcnMgdG8gdGhlIHNleHVhbCBhYnVzZSBvZiBhIHBlcn
NvbiBiZWxvdyB0aGUgYWdlIG9mIDE4LCBhcyB3ZWxsIGFzIHRvIHRoZSBwcm9kdWN0aW9uIG9mIGltYW
dlcyBvZiBzdWNoIGFidXNlIGFuZCB0aGUgc2hhcmluZyBvZiB0aG9zZSBpbWFnZXMgb25saW5l

Base64 Decode and Encode - Online

A screenshot of artefact evidence details:



Metadata

```
Name:                   /img_Mensil.E01/Something_Bookmark.docx
Type:                   File System
MIME Type:              application/vnd.openxmlformats-officedocument.wordprocessingml.document
Size:                   6475
File Name Allocation:   Allocated
Metadata Allocation:    Allocated
Modified:               2022-11-08 20:47:10 GMT
Accessed:               2022-11-09 00:00:00 GMT
Created:                2022-11-09 05:07:34 GMT
Changed:                0000-00-00 00:00:00
MD5:                    603d5c1082049d7938478f2676c52910
SHA-256:                c4a9e1371dc435a555e637f8f568f8534bba3ef809991a40d2a5ad07312b5cbf
Hash Lookup Results:    UNKNOWN
Internal ID:            2085
```

Description and implications of the artefact:

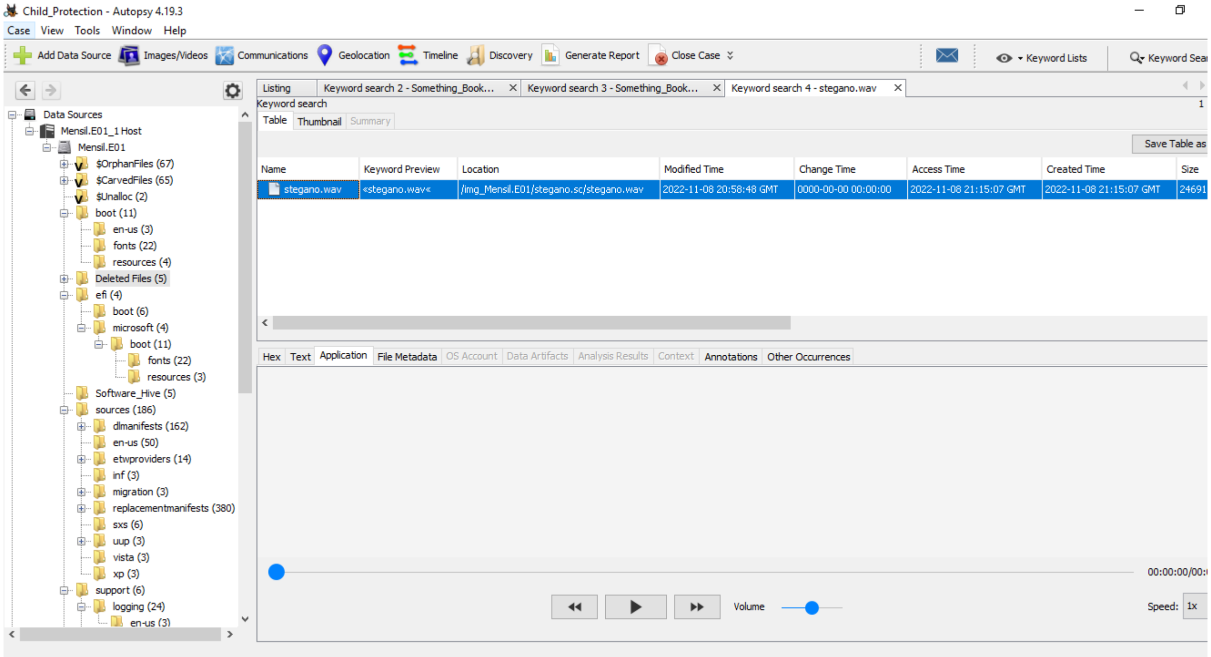
Offender Hide some secret data in a docx file by encrypting to a hash code like base64 format. After decode the hash found that text “Child sexual exploitation refers to the sexual abuse of a person below the age of 18, as well as to the production of images of such abuse and the sharing of those images online”. We clarify that they are planning to share the abuse images of a child to social media platform.

Description of the hiding/unhiding process:

Hide the characters in a docs file by a white background. Basically when it is opened then it can view by blank but mark the page and change the colour then we found the text that is hash value like base64. We decode from base64 decoder.

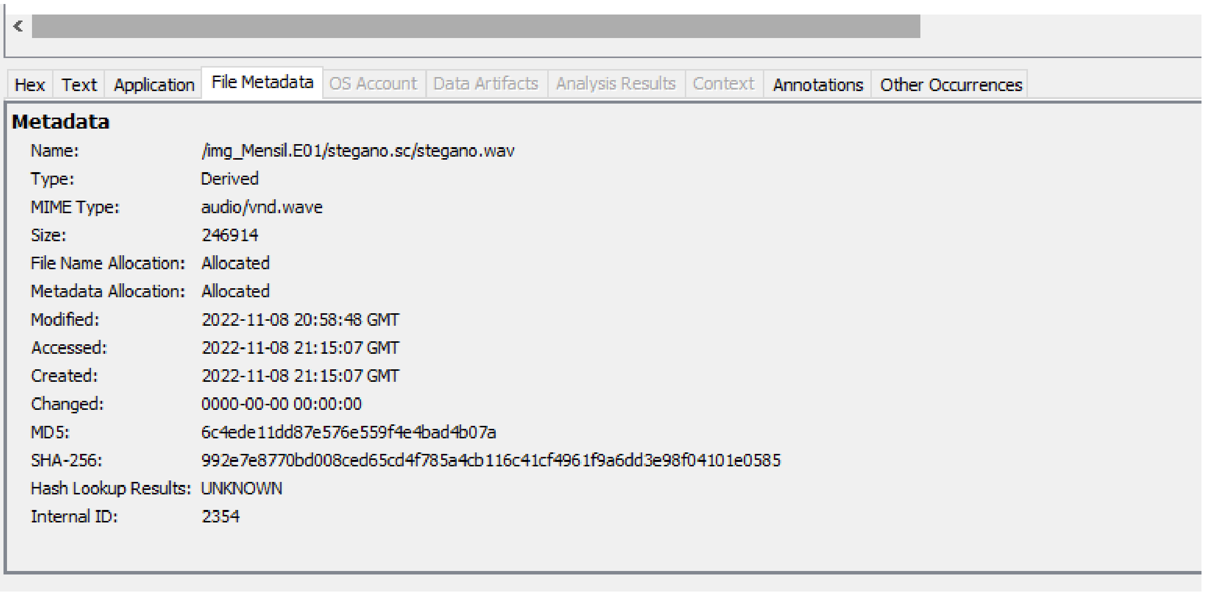
4.3.2 Category DHA

Screenshot of the artefact:



Name	Keyword Preview	Location	Modified Time	Change Time	Access Time	Created Time	Size
stegano.wav	«stegano.wav«	/img_Mensil.E01/stegano.sc/stegano.wav	2022-11-08 20:58:48 GMT	0000-00-00 00:00:00	2022-11-08 21:15:07 GMT	2022-11-08 21:15:07 GMT	24691

A screenshot of artefact evidence details:



Metadata

Name:	/img_Mensil.E01/stegano.sc/stegano.wav
Type:	Derived
MIME Type:	audio/vnd.wave
Size:	246914
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-11-08 20:58:48 GMT
Accessed:	2022-11-08 21:15:07 GMT
Created:	2022-11-08 21:15:07 GMT
Changed:	0000-00-00 00:00:00
MD5:	6c4ede11dd87e576e559f4e4bad4b07a
SHA-256:	992e7e8770bd008ced65cd4f785a4cb116c41cf4961f9a6dd3e98f04101e0585
Hash Lookup Results:	UNKNOWN
Internal ID:	2354

Description and implications of the artefact:

Offender Used the steganography technique for hide some secret data that is related to Grooming of a child & Abusement. The extracted message is **WEWILLSAFEOURCHILDFROMSEXUALABUSEMENT**

They used Morse Code Adaptive audio for hide the text.

Description of the hiding/unhiding process:

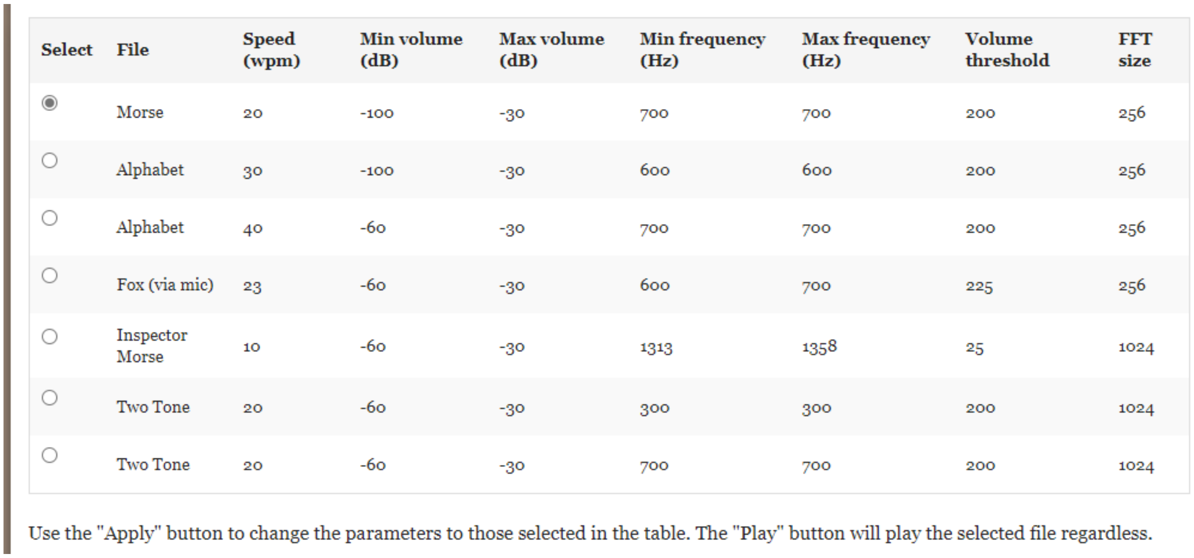
Data Hiding in Application section Like Steganography

This is a morse code adaptive audio for some plain text messages. We hide a readable message in audio via morse code. You can extract the plain text by decode the morse code adaptive audio using a suitable decoder. We used an online site to make the file [link.]()

Decode the file using Morse code Adaptive audio decoder site. Link:
[Morse Code Audio Decoder | Morse Code World]()

Step-1: go to the link and upload the audio file.

Step-2: Set the morse speed 20 WPM & Minimum,maximum frequency is 700 HZ. Screenshot below

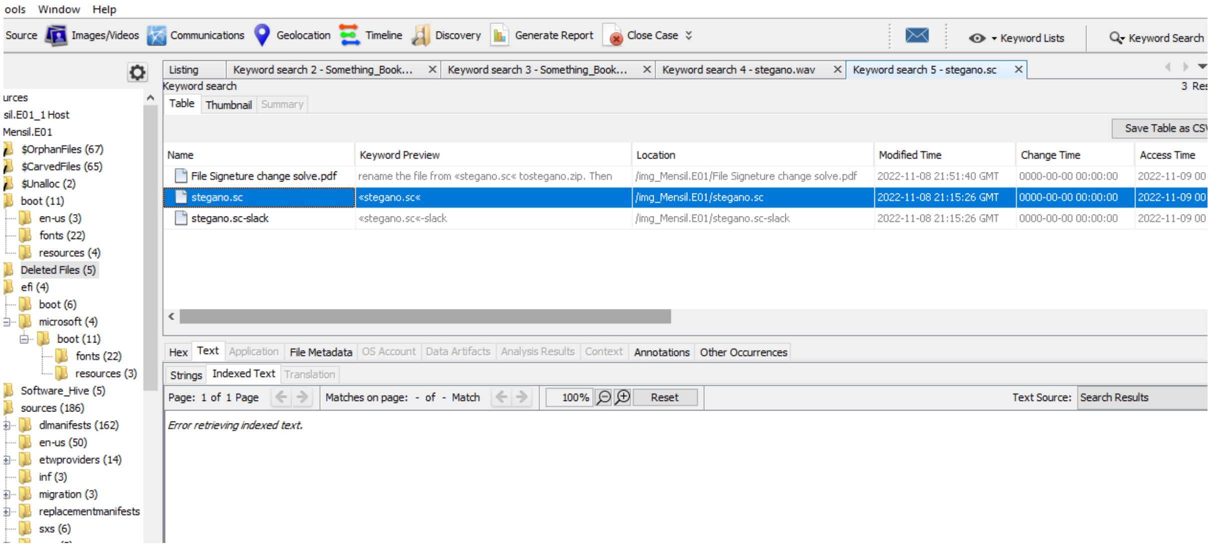


Select	File	Speed (wpm)	Min volume (dB)	Max volume (dB)	Min frequency (Hz)	Max frequency (Hz)	Volume threshold	FFT size
●	Morse	20	-100	-30	700	700	200	256
○	Alphabet	30	-100	-30	600	600	200	256
○	Alphabet	40	-60	-30	700	700	200	256
○	Fox (via mic)	23	-60	-30	600	700	225	256
○	Inspector Morse	10	-60	-30	1313	1358	25	1024
○	Two Tone	20	-60	-30	300	300	200	1024
○	Two Tone	20	-60	-30	700	700	200	1024

Use the "Apply" button to change the parameters to those selected in the table. The "Play" button will play the selected file regardless.

4.3.3 Category DHOS

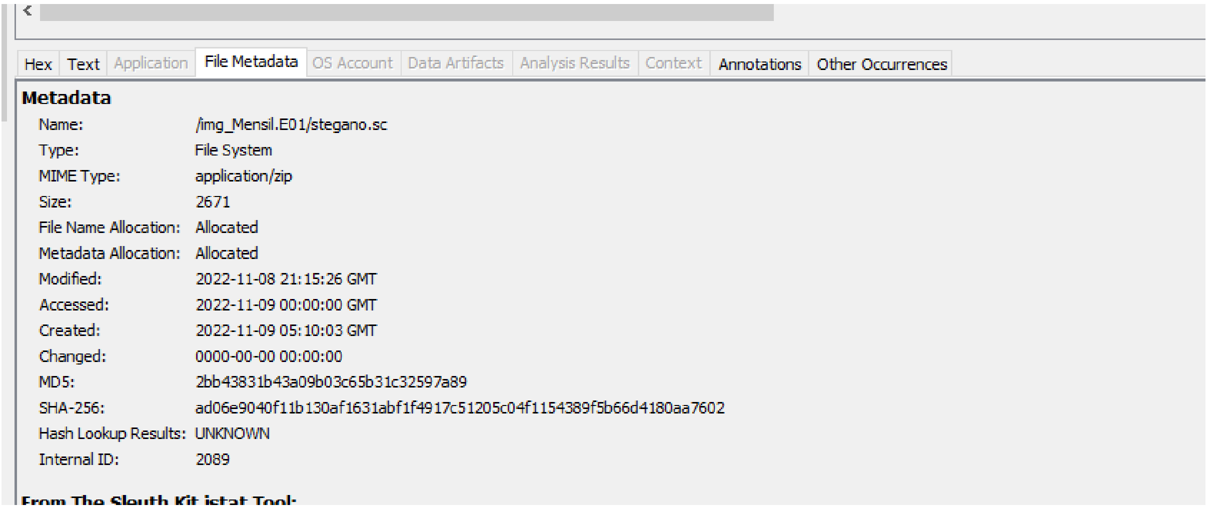
Screenshot of the artefact:


ools Window Help
Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Listing
Keyword search 2 - Something_Book...
Keyword search 3 - Something_Book...
Keyword search 4 - stegano.wav
Keyword search 5 - stegano.sc
Keyword search
3 Res
Table Thumbnail Summary
Save Table as CSV
urces
sil.E01_1 Host
Mensil.E01
$OrphanFiles (67)
$CarvedFiles (65)
$Unalloc (2)
boot (11)
en-us (3)
fonts (22)
resources (4)
Deleted Files (5)
efi (4)
boot (6)
microsoft (4)
boot (11)
fonts (22)
resources (3)
Software_Hive (5)
sources (186)
dlmanifests (162)
en-us (50)
etwproviders (14)
inf (3)
migration (3)
replacementmanifests
sxs (6)
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Strings Indexed Text Translation
Page: 1 of 1 Page Matches on page: - of - Match 100% Reset
Text Source: Search Results

Name	Keyword Preview	Location	Modified Time	Change Time	Access Time
File Signeture change solve.pdf	rename the file from «stegano.sc« tostegano.zip. Then	/img_Mensil.E01/File Signeture change solve.pdf	2022-11-08 21:51:40 GMT	0000-00-00 00:00:00	2022-11-09 00
stegano.sc	«stegano.sc«	/img_Mensil.E01/stegano.sc	2022-11-08 21:15:26 GMT	0000-00-00 00:00:00	2022-11-09 00
stegano.sc-slack	«stegano.sc«-slack	/img_Mensil.E01/stegano.sc-slack	2022-11-08 21:15:26 GMT	0000-00-00 00:00:00	2022-11-09 00

Error retrieving indexed text.

A screenshot of artefact evidence details:


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

Metadata

Name:	/img_Mensil.E01/stegano.sc
Type:	File System
MIME Type:	application/zip
Size:	2671
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-11-08 21:15:26 GMT
Accessed:	2022-11-09 00:00:00 GMT
Created:	2022-11-09 05:10:03 GMT
Changed:	0000-00-00 00:00:00
MD5:	2bb43831b43a09b03c65b31c32597a89
SHA-256:	ad06e9040f11b130af1631abf1f4917c51205c04f1154389f5b66d4180aa7602
Hash Lookup Results:	UNKNOWN
Internal ID:	2089

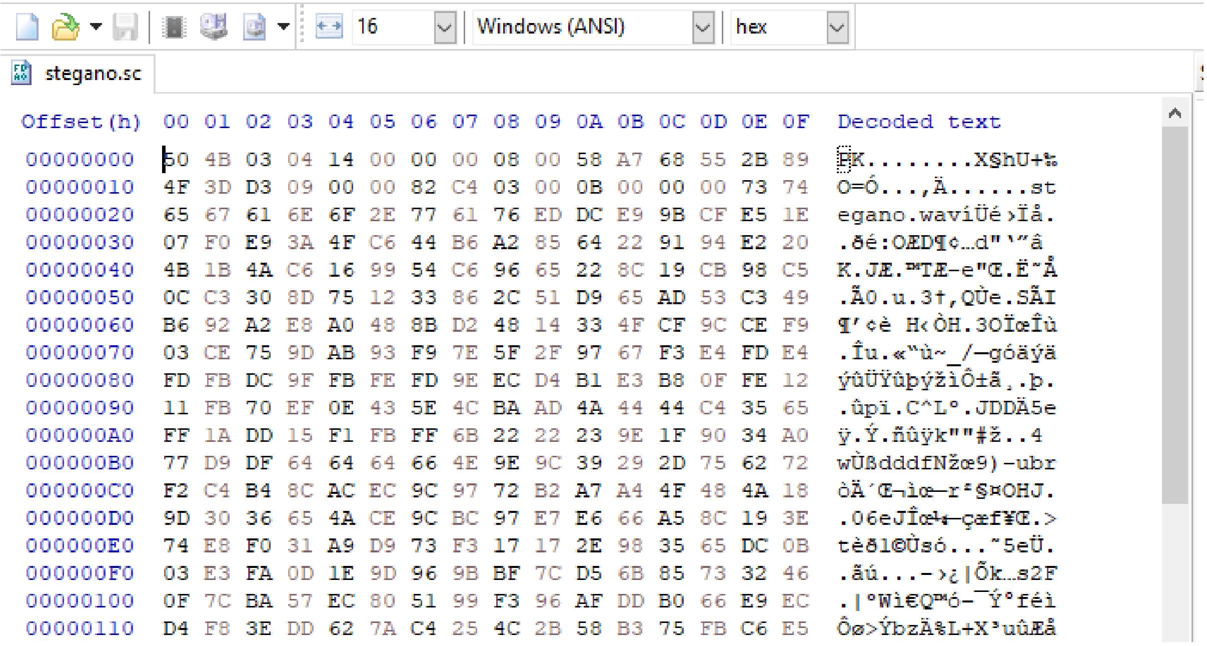
From The Sleuth Kit istat Tool:

Description and implications of the artefact:

In this section Offender Make corrupt the file by change the extension of the previous section file Compressed like Stegano.zip to stegano.sc

Description of the hiding/unhiding process:

Check the extension by matchinfg header signature.

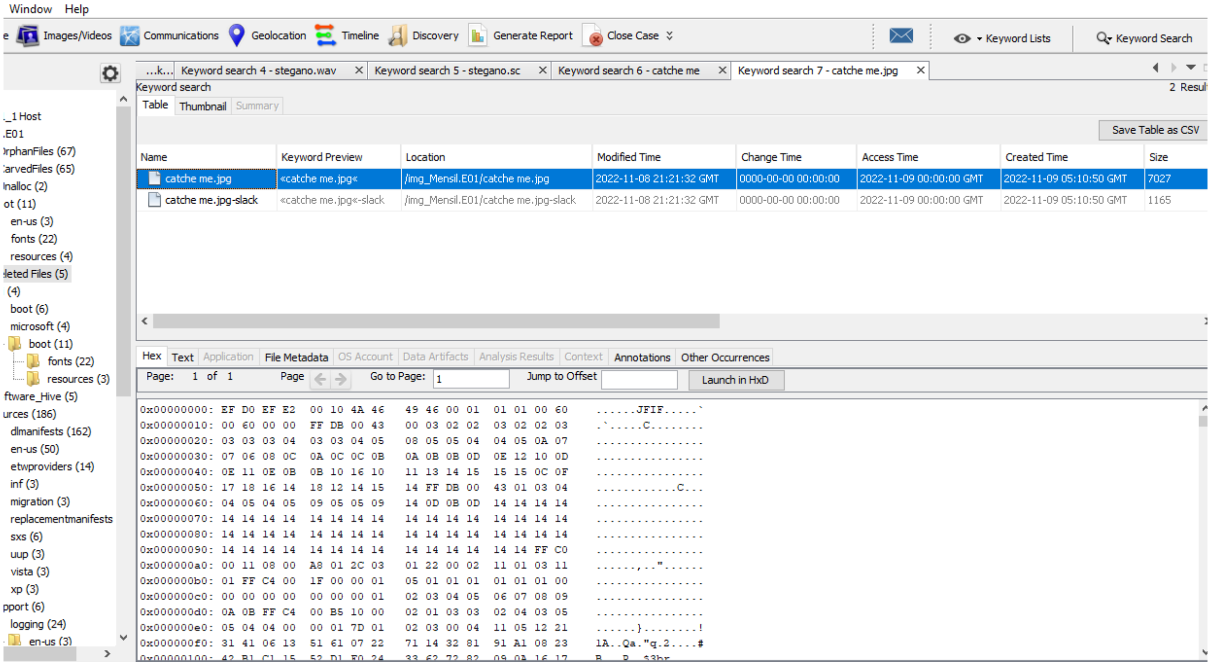


```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00000000  50 4B 03 04 14 00 00 00 08 00 58 A7 68 55 2B 89  PK........X§hU+‰
00000010  4F 3D D3 09 00 00 82 C4 03 00 0B 00 00 00 73 74  O=Ó...‚Ä......st
00000020  65 67 61 6E 6F 2E 77 61 76 ED DC E9 9B CF E5 1E  egano.waviÜé›Ïå.
00000030  07 F0 E9 3A 4F C6 44 B6 A2 85 64 22 91 94 E2 20  .ðé:OÆD¶¢…d"'"â 
00000040  4B 1B 4A C6 16 99 54 C6 96 65 22 8C 19 CB 98 C5  K.JÆ.™TÆ–e"Œ.Ë˜Å
00000050  0C C3 30 8D 75 12 33 86 2C 51 D9 65 AD 53 C3 49  .Ã0.u.3†,QÙe.SÃI
00000060  B6 92 A2 E8 A0 48 8B D2 48 14 33 4F CF 9C CE F9  ¶'¢è H‹ÒH.3OÏœÎù
00000070  03 CE 75 9D AB 93 F9 7E 5F 2F 97 67 F3 E4 FD E4  .Îu.«"ù~_/—góäýä
00000080  FD FB DC 9F FB FE FD 9E EC D4 B1 E3 B8 0F FE 12  ýûÜŸûþýžìÔ±ã¸.þ.
00000090  11 FB 70 EF 0E 43 5E 4C BA AD 4A 44 44 C4 35 65  .ûpï.C^Lº.JDDÄ5e
000000A0  FF 1A DD 15 F1 FB FF 6B 22 22 23 9E 1F 90 34 A0  ÿ.Ý.ñûÿk""#ž..4 
000000B0  77 D9 DF 64 64 64 4E 9E 9C 39 29 2D 75 62 72     wÙßdddNžœ9)-ubr
000000C0  F2 C4 B4 8C AC EC 9C 97 72 B2 A7 A4 4F 48 4A 18  òÄ´Œ¬ìœ—r²§¤OHJ.
000000D0  9D 30 36 65 4A CE 9C BC 97 E7 E6 66 A5 8C 19 3E  .06eJÎœ¼—çæf¥Œ.>
000000E0  74 E8 F0 31 A9 D9 73 F3 17 17 2E 98 35 65 DC 0B  tèð1©Ùsó...˜5eÜ.
000000F0  03 E3 FA 0D 1E 9D 96 9B BF 7C D5 6B 85 73 32 46  .ãú...–›¿|Õk…s2F
00000100  0F 7C BA 57 EC 80 51 99 F3 96 AF DD B0 66 E9 EC  .|ºWì€Q™ó–¯Ý°féì
00000110  D4 F8 3E DD 62 7A C4 25 4C 2B 58 B3 75 FB C6 E5  Ôø>ÝbzÄ%L+X³uûÆå
```

Hex start from “50 4B 03 04” that is Related to zip file. Rename the file from stegano.sc to stegano.zip.

4.3.4 Category DHFS

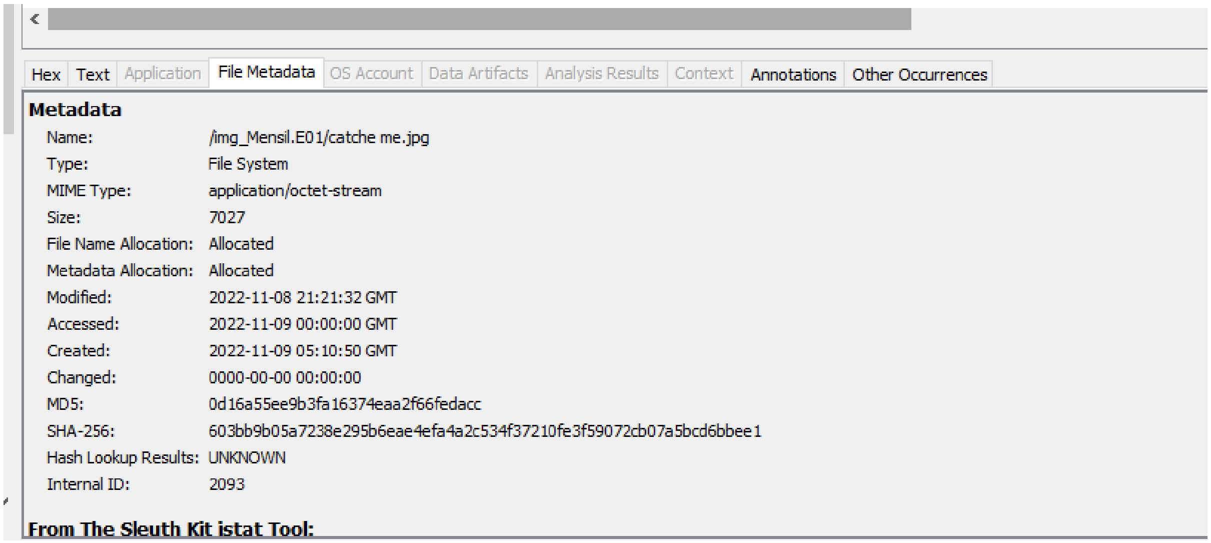
Screenshot of the artefact:



Name	Keyword Preview	Location	Modified Time	Change Time	Access Time	Created Time	Size
catche me.jpg	«catche me.jpg«	/img_Mensil.E01/catche me.jpg	2022-11-08 21:21:32 GMT	0000-00-00 00:00:00	2022-11-09 00:00:00 GMT	2022-11-09 05:10:50 GMT	7027
catche me.jpg-slack	«catche me.jpg«-slack	/img_Mensil.E01/catche me.jpg-slack	2022-11-08 21:21:32 GMT	0000-00-00 00:00:00	2022-11-09 00:00:00 GMT	2022-11-09 05:10:50 GMT	1165

```
0x00000000: EF D0 EF E2  00 10 4A 46  49 46 00 01  01 01 00 60   ......JFIF.....`
0x00000010: 00 60 00 00  FF DB 00 43  00 03 02 02  03 02 02 03   .`.....C........
0x00000020: 03 03 03 04  03 03 04 05  08 05 05 04  04 05 0A 07   ................
0x00000030: 07 06 08 0C  0A 0C 0C 0B  0A 0B 0B 0D  0E 12 10 0D   ................
0x00000040: 0E 11 0E 0B  0B 10 16 10  11 13 14 15  15 15 0C 0F   ................
0x00000050: 17 18 16 14  18 12 14 15  14 FF DB 00  43 01 03 04   ............C...
0x00000060: 04 05 04 05  09 05 05 09  14 0D 0B 0D  14 14 14 14   ................
0x00000070: 14 14 14 14  14 14 14 14  14 14 14 14  14 14 14 14   ................
0x00000080: 14 14 14 14  14 14 14 14  14 14 14 14  14 14 14 14   ................
0x00000090: 14 14 14 14  14 14 14 14  14 14 14 14  14 14 FF C0   ................
0x000000a0: 00 11 08 00  A8 01 2C 03  01 22 00 02  11 01 03 11   ......,.."......
0x000000b0: 01 FF C4 00  1F 00 00 01  05 01 01 01  01 01 01 00   ................
0x000000c0: 00 00 00 00  00 00 00 01  02 03 04 05  06 07 08 09   ................
0x000000d0: 0A 0B FF C4  00 B5 10 00  02 01 03 03  02 04 03 05   ................
0x000000e0: 05 04 04 00  00 01 7D 01  02 03 00 04  11 05 12 21   ......}........!
0x000000f0: 31 41 06 13  51 61 07 22  71 14 32 81  91 A1 08 23   1A..Qa."q.2....#
0x00000100: 42 B1 C1 15  52 D1 F0 24  33 62 72 82  09 0A 16 17   B...R..$3br....
```

A screenshot of artefact evidence details:



```
Metadata
  Name:                   /img_Mensil.E01/catche me.jpg
  Type:                   File System
  MIME Type:              application/octet-stream
  Size:                   7027
  File Name Allocation:   Allocated
  Metadata Allocation:    Allocated
  Modified:               2022-11-08 21:21:32 GMT
  Accessed:               2022-11-09 00:00:00 GMT
  Created:                2022-11-09 05:10:50 GMT
  Changed:                0000-00-00 00:00:00
  MD5:                    0d16a55ee9b3fa16374eaa2f66fedacc
  SHA-256:                603bb9b05a7238e295b6eae4efa4a2c534f37210fe3f59072cb07a5bcd6bbee1
  Hash Lookup Results:    UNKNOWN
  Internal ID:            2093

From The Sleuth Kit istat Tool:
```

Description and implications of the artefact:

Finally we noticed that this is the offender image and information. But the image is being corrupted. We need to correct it. Here is, they do the file signature change for hide the real image. This is a offenders jpg image but not opened. So after correct the header signature of jpg file then it will opened. And we got it our offenders image.

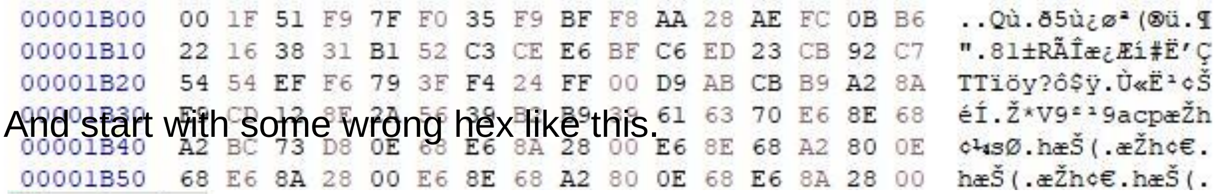
Description of the hiding/unhiding process:

File Signature Correction

For the “Catch me” jpg fle, we showed that the fle does not open due to a signature or extension mismatched. This image extension we show that it's a jpg fle but not opened. Using HxD tools, we can open it to check the signature with a detailed hex view with ascii value. After Open in HxD,

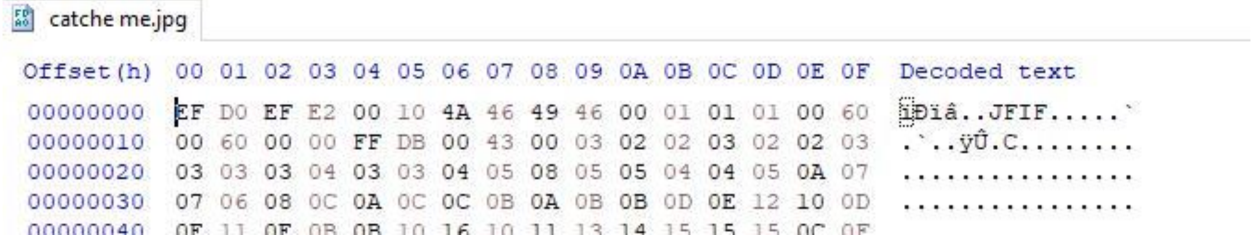
Check the fle header signature.

We noticed that the hex value ended with FF D9.



```
00001B00  00 1F 51 F9 7F F0 35 F9 BF F8 AA 28 AE FC 0B B6  ..Qù.ð5ù¿ø ª(®ü.¶
00001B10  22 16 38 31 B1 52 C3 CE E6 BF C6 ED 23 CB 92 C7  ".81±RÃÎæ¿Æí#Ë’Ç
00001B20  54 54 EF F6 79 3F F4 24 FF 00 D9 AB CB B9 A2 8A  TTïöy?ô$ÿ.Ù«Ë¹¢Š
00001B30  E9 CD 12 8E 2A 56 39 B2 B9 39 61 63 70 E6 8E 68  éÍ.Ž*V9²¹9acpæŽh
00001B40  A2 BC 73 D8 0E 68 E6 8A 28 00 E6 8E 68 A2 80 0E  ¢¼sØ.hæŠ(.æŽh¢€.
00001B50  68 E6 8A 28 00 E6 8E 68 A2 80 0E 68 E6 8A 28 00  hæŠ(.æŽh¢€.hæŠ(.
```

And start with some wrong hex like this.



catche me.jpg

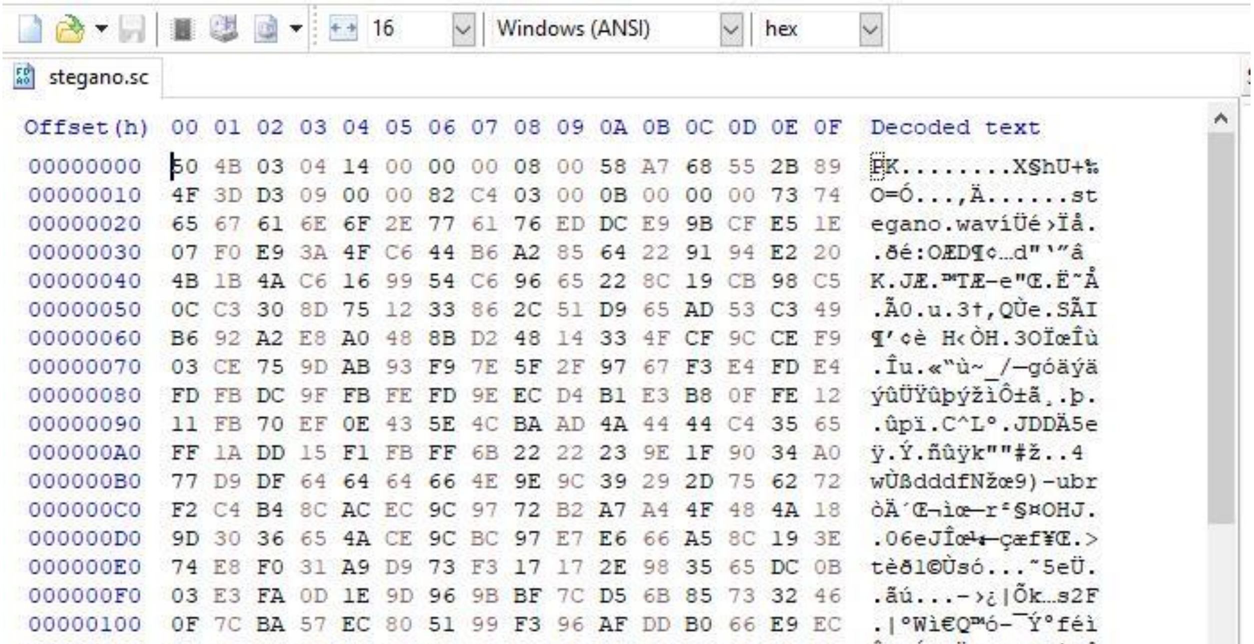
```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00000000  EF D0 EF E2 00 10 4A 46 49 46 00 01 01 01 00 60  ïÐïâ..JFIF.....`
00000010  00 60 00 00 FF DB 00 43 00 03 02 02 03 02 02 03  .`..ÿÛ.C........
00000020  03 03 03 04 03 03 04 05 08 05 05 04 04 05 0A 07  ................
00000030  07 06 08 0C 0A 0C 0C 0B 0A 0B 0B 0D 0E 12 10 0D  ................
00000040  0F 11 0F 0B 0B 10 16 10 11 13 14 15 15 15 0C 0F
```

But also we can see that its start JFIF in ascii section & ended by hex FF D9. That means it's a jpg fle. Extension is correct. But the signature is incorrect, that's why this is not open.

We know that the Jpg fle header signature starts from **FF D8 FF E0** sequence. So we will correct from the beginning. And save it. Then it will be open.

File Extension Correction

For stegano fle we can see that it's an unknown fle. By open in HxD.



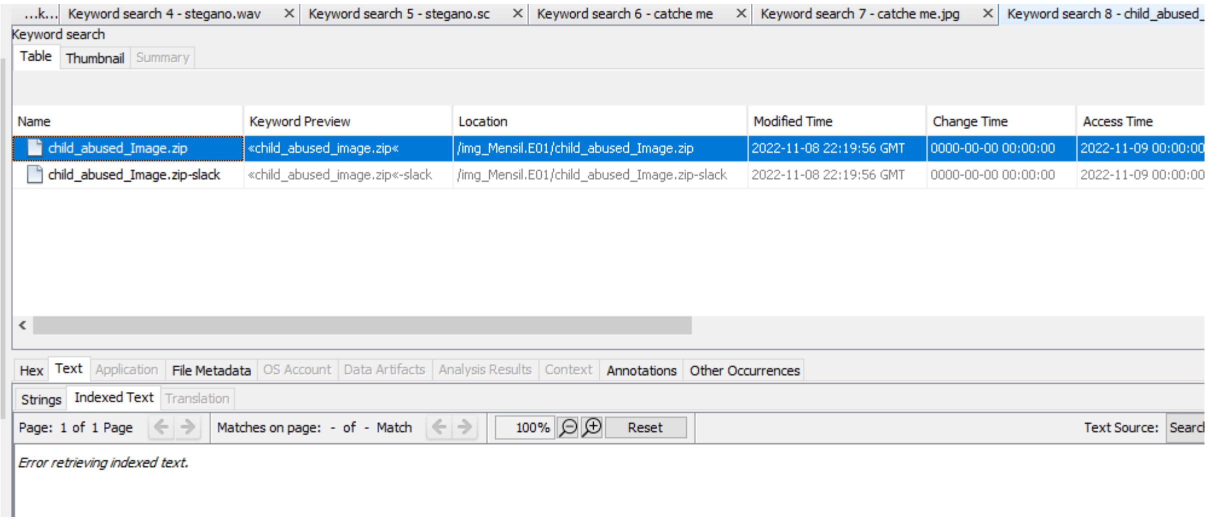
stegano.sc

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

00000000  50 4B 03 04 14 00 00 00 08 00 58 A7 68 55 2B 89  PK........X§hU+‰
00000010  4F 3D D3 09 00 00 82 C4 03 00 0B 00 00 00 73 74  O=Ó...‚Ä......st
00000020  65 67 61 6E 6F 2E 77 61 76 ED DC E9 9B CF E5 1E  egano.wavíÜé›Ïå.
00000030  07 F0 E9 3A 4F C6 44 B6 A2 85 64 22 91 94 E2 20  .ðé:OÆD¶¢…d"‘”â 
00000040  4B 1B 4A C6 16 99 54 C6 96 65 22 8C 19 CB 98 C5  K.JÆ.™TÆ–e"Œ.Ë˜Å
00000050  0C C3 30 8D 75 12 33 86 2C 51 D9 65 AD 53 C3 49  .Ã0.u.3†,QÙe.SÃI
00000060  B6 92 A2 E8 A0 48 8B D2 48 14 33 4F CF 9C CE F9  ¶’¢è H‹ÒH.3OÏœÎù
00000070  03 CE 75 9D AB 93 F9 7E 5F 2F 97 67 F3 E4 FD E4  .Îu.«“ù~_/—góäýä
00000080  FD FB DC 9F FB FE FD 9E EC D4 B1 E3 B8 0F FE 12  ýûÜŸûþýžìÔ±ã¸.þ.
00000090  11 FB 70 EF 0E 43 5E 4C BA AD 4A 44 44 C4 35 65  .ûpï.C^Lº.JDDÄ5e
000000A0  FF 1A DD 15 F1 FB FF 6B 22 22 23 9E 1F 90 34 A0  ÿ.Ý.ñûÿk""#ž..4 
000000B0  77 D9 DF 64 64 64 66 4E 9E 9C 39 29 2D 75 62 72  wÙßdddfNžœ9)-ubr
000000C0  F2 C4 B4 8C AC EC 9C 97 72 B2 A7 A4 4F 48 4A 18  òÄ´Œ¬ìœ—r²§¤OHJ.
000000D0  9D 30 36 65 4A CE 9C BC 97 E7 E6 66 A5 8C 19 3E  .06eJÎœ¼—çæf¥Œ.>
000000E0  74 E8 F0 31 A9 D9 73 F3 17 17 2E 98 35 65 DC 0B  tèð1©Ùsó...˜5eÜ.
000000F0  03 E3 FA 0D 1E 9D 96 9B BF 7C D5 6B 85 73 32 46  .ãú...–›¿|Õk…s2F
00000100  0F 7C BA 57 EC 80 51 99 F3 96 AF DD B0 66 E9 EC  .|ºWì€Q™ó–¯Ý°féì
```

Hex starts from 50 4B 03 04 that means it's a zip fle. Zip fle header is 50 4B 03 04. so , we need to rename the fle from stegano.sc to stegano.zip. Then it will be corrected and will open.

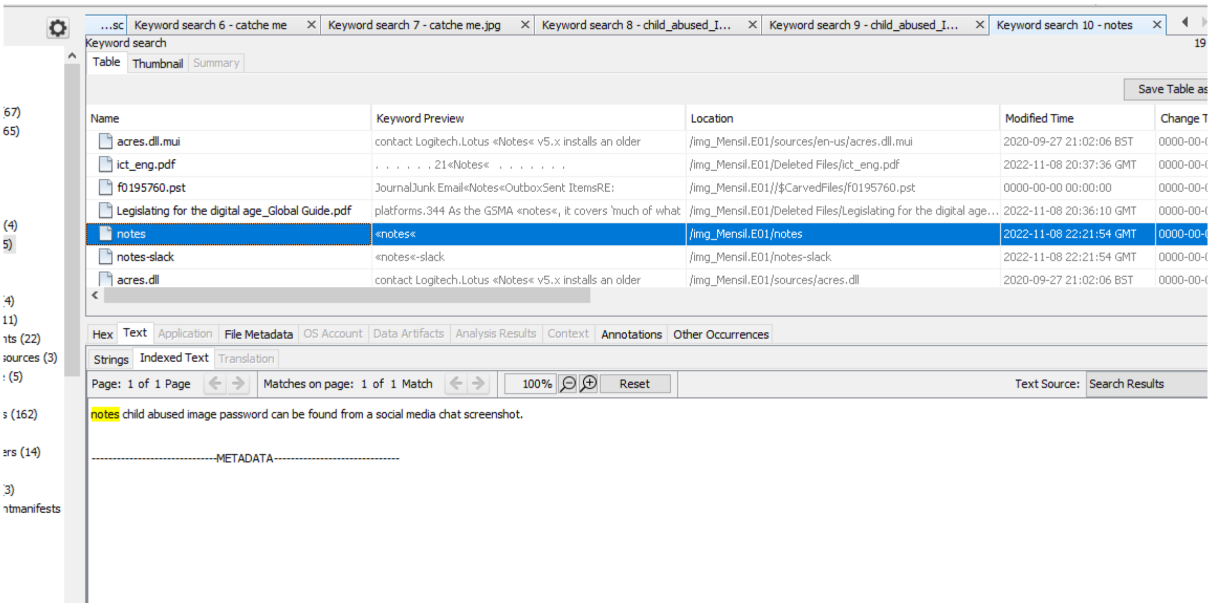
4.3.5 Category DHU_1

Screenshot of the artefact:


...k...
Keyword search 4 - stegano.wav
Keyword search 5 - stegano.sc
Keyword search 6 - catche me
Keyword search 7 - catche me.jpg
Keyword search 8 - child_abused_
Keyword search
Table
Thumbnail
Summary

Name	Keyword Preview	Location	Modified Time	Change Time	Access Time
child_abused_Image.zip	«child_abused_image.zip«	/img_Mensil.E01/child_abused_Image.zip	2022-11-08 22:19:56 GMT	0000-00-00 00:00:00	2022-11-09 00:00:00
child_abused_Image.zip-slack	«child_abused_image.zip«-slack	/img_Mensil.E01/child_abused_Image.zip-slack	2022-11-08 22:19:56 GMT	0000-00-00 00:00:00	2022-11-09 00:00:00

Error retrieving indexed text.

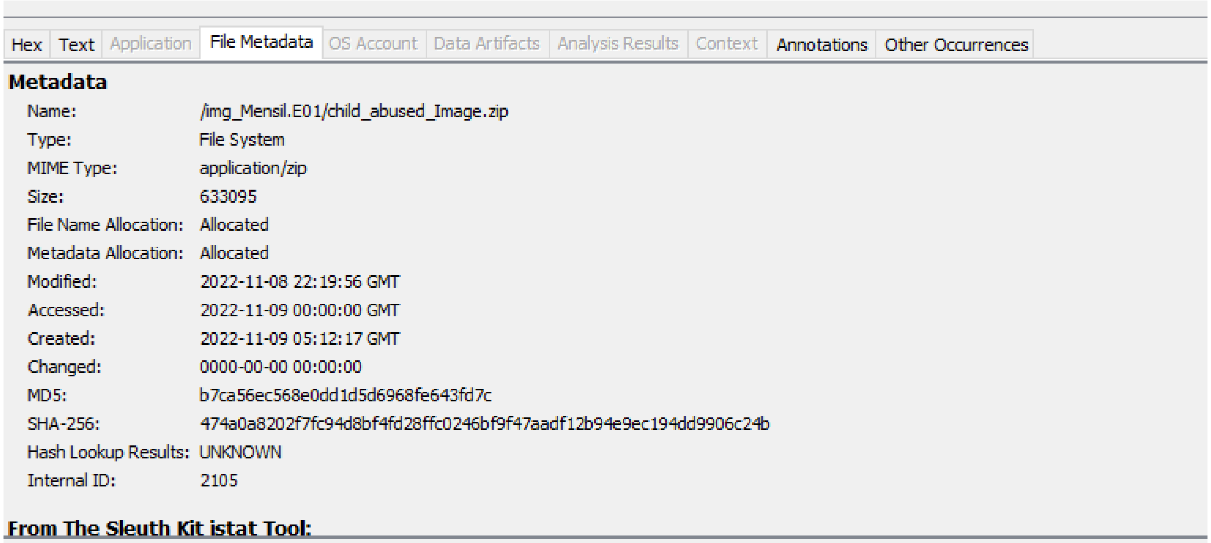

...sc
Keyword search 6 - catche me
Keyword search 7 - catche me.jpg
Keyword search 8 - child_abused_I...
Keyword search 9 - child_abused_I...
Keyword search 10 - notes
Keyword search
19
Table
Thumbnail
Summary
Save Table as

Name	Keyword Preview	Location	Modified Time	Change T
acres.dll.mui	contact Logitech.Lotus «Notes« v5.x installs an older	/img_Mensil.E01/sources/en-us/acres.dll.mui	2020-09-27 21:02:06 BST	0000-00-
ict_eng.pdf	. . . . 21«Notes«	/img_Mensil.E01/Deleted Files/ict_eng.pdf	2022-11-08 20:37:36 GMT	0000-00-
f0195760.pst	JournalJunk Email«Notes«OutboxSent ItemsRE:	/img_Mensil.E01//$CarvedFiles/f0195760.pst	0000-00-00 00:00:00	0000-00-
Legislating for the digital age_Global Guide.pdf	platforms.344 As the GSMA «notes«, it covers 'much of what	/img_Mensil.E01/Deleted Files/Legislating for the digital age...	2022-11-08 20:36:10 GMT	0000-00-
notes	«notes«	/img_Mensil.E01/notes	2022-11-08 22:21:54 GMT	0000-00-
notes-slack	«notes«-slack	/img_Mensil.E01/notes-slack	2022-11-08 22:21:54 GMT	0000-00-
acres.dll	contact Logitech.Lotus «Notes« v5.x installs an older	/img_Mensil.E01/sources/acres.dll	2020-09-27 21:02:06 BST	0000-00-

notes child abused image password can be found from a social media chat screenshot.

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

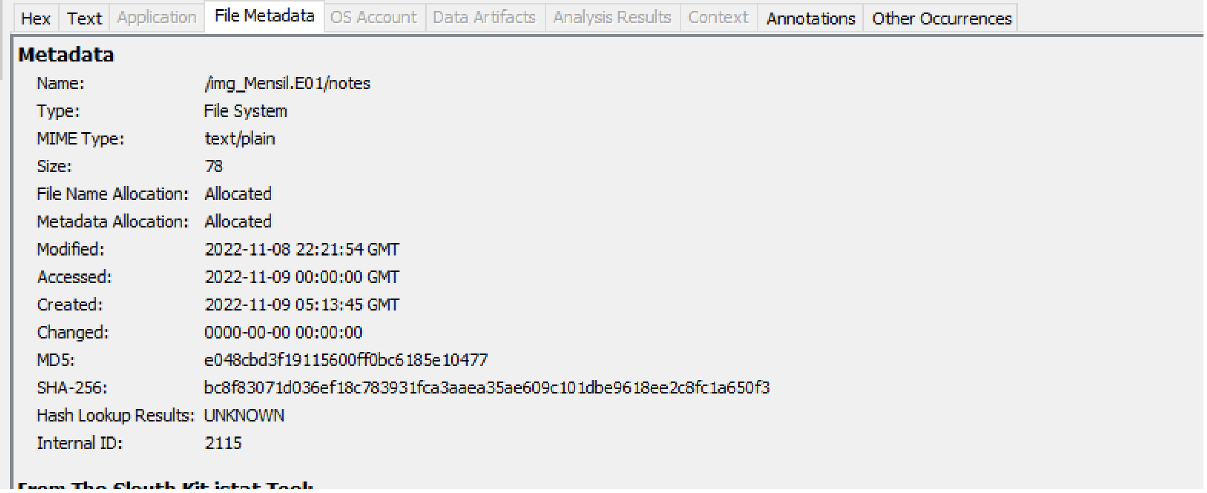
A screenshot of artefact evidence details:



Metadata

Name:	/img_Mensil.E01/child_abused_Image.zip
Type:	File System
MIME Type:	application/zip
Size:	633095
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-11-08 22:19:56 GMT
Accessed:	2022-11-09 00:00:00 GMT
Created:	2022-11-09 05:12:17 GMT
Changed:	0000-00-00 00:00:00
MD5:	b7ca56ec568e0dd1d5d6968fe643fd7c
SHA-256:	474a0a8202f7fc94d8bf4fd28ffc0246bf9f47aadf12b94e9ec194dd9906c24b
Hash Lookup Results:	UNKNOWN
Internal ID:	2105

From The Sleuth Kit istat Tool:



Metadata

Name:	/img_Mensil.E01/notes
Type:	File System
MIME Type:	text/plain
Size:	78
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-11-08 22:21:54 GMT
Accessed:	2022-11-09 00:00:00 GMT
Created:	2022-11-09 05:13:45 GMT
Changed:	0000-00-00 00:00:00
MD5:	e048cbd3f19115600ff0bc6185e10477
SHA-256:	bc8f83071d036ef18c783931fca3aaea35ae609c101dbe9618ee2c8fc1a650f3
Hash Lookup Results:	UNKNOWN
Internal ID:	2115

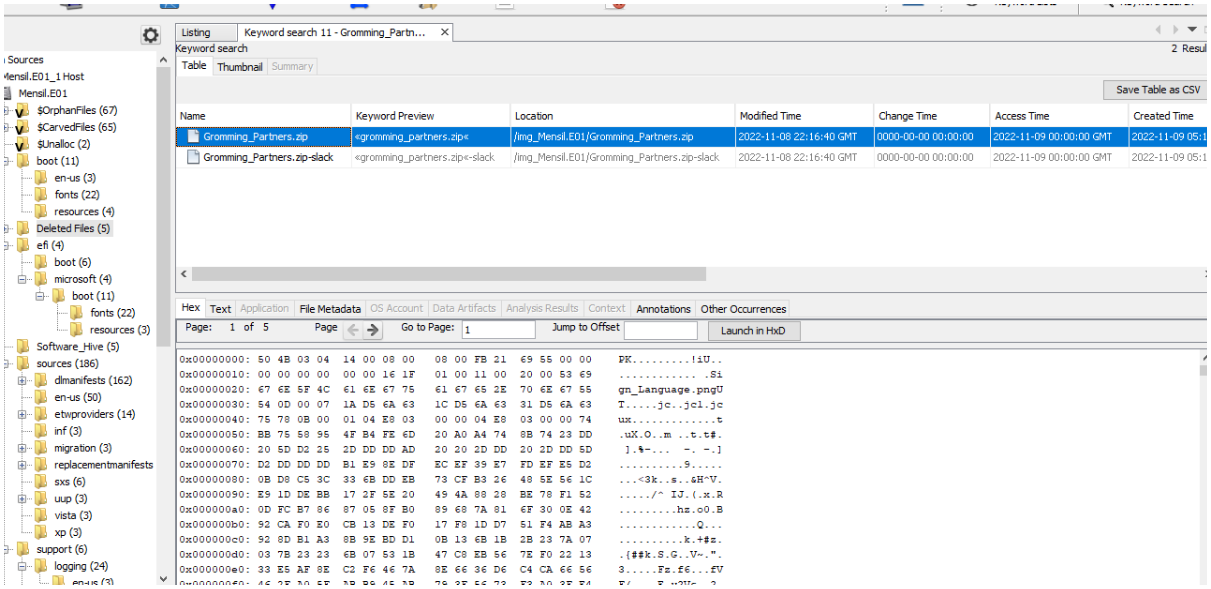
From The Sleuth Kit istat Tool:

Description and implications of the artefact:

In this section we found a notes text file that is define that a child abused image have in offender. We found the image zip file that is password protected. Offender hide the image in a zip file by password protect. Notes file define us that the zip file password can be found from chats. So from the leaked social media chats section we found the pass and using this password we extracted the image files. That can prove against offender by a strong proof.

4.3.6 Category DHU_2

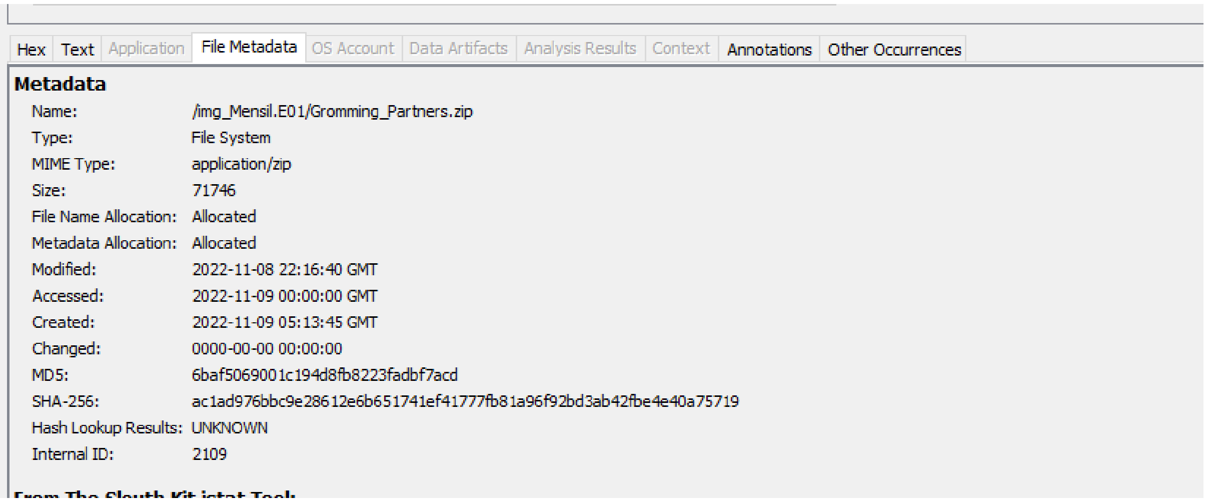
Screenshot of the artefact:



Name	Keyword Preview	Location	Modified Time	Change Time	Access Time	Created Time
Gromming_Partners.zip	«gromming_partners.zip«	/img_Mensil.E01/Gromming_Partners.zip	2022-11-08 22:16:40 GMT	0000-00-00 00:00:00	2022-11-09 00:00:00 GMT	2022-11-09 05:1
Gromming_Partners.zip-slack	«gromming_partners.zip«-slack	/img_Mensil.E01/Gromming_Partners.zip-slack	2022-11-08 22:16:40 GMT	0000-00-00 00:00:00	2022-11-09 00:00:00 GMT	2022-11-09 05:1

```
0x00000000: 50 4B 03 04  14 00 08 00   08 00 FB 21  69 55 00 00    PK.........!iU..
0x00000010: 00 00 00 00  00 00 16 1F   01 00 11 00  20 00 53 69    ............ .Si
0x00000020: 67 6E 5F 4C  61 6E 67 75   61 67 65 2E  70 6E 67 55    gn_Language.pngU
0x00000030: 54 0D 00 07  1A D5 6A 63   1C D5 6A 63  31 D5 6A 63    T.....jc..jc1.jc
0x00000040: 75 78 0B 00  01 04 E8 03   00 00 04 E8  03 00 00 74    ux.............t
0x00000050: BB 75 58 95  4F B4 FE 6D   20 A0 A4 74  8B 74 23 DD    .uX.O..m ..t.t#.
0x00000060: 20 5D D2 25  2D DD DD AD   20 20 2D DD  20 2D DD 5D     ].%-...  -. -.]
0x00000070: D2 DD DD DD  B1 E9 8E DF   EC EF 39 E7  FD EF E5 D2    ..........9.....
0x00000080: 0B D8 C5 3C  33 6B DD EB   73 CF B3 26  48 5E 56 1C    ...<3k..s..&H^V.
0x00000090: E9 1D DE BB  17 2F 5E 20   49 4A 88 28  BE 78 F1 52    ...../^ IJ.(.x.R
0x000000a0: 0D FC B7 86  87 05 8F B0   89 68 7A 81  6F 30 0E 42    .........hz.o0.B
0x000000b0: 92 CA F0 E0  CB 13 DE F0   17 F8 1D D7  51 F4 AB A3    ............Q...
0x000000c0: 92 8D B1 A3  8B 9E BD D1   0B 13 6B 1B  2B 23 7A 07    ..........k.+#z.
0x000000d0: 03 7B 23 23  6B 07 53 1B   47 C8 EB 56  7E F0 22 13    .{##k.S.G..V~.".
0x000000e0: 33 E5 AF 8E  C2 F6 46 7A   8E 66 36 D6  C4 CA 66 56    3.....Fz.f6...fV
```

A screenshot of artefact evidence details:



Metadata

Name:	/img_Mensil.E01/Gromming_Partners.zip
Type:	File System
MIME Type:	application/zip
Size:	71746
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-11-08 22:16:40 GMT
Accessed:	2022-11-09 00:00:00 GMT
Created:	2022-11-09 05:13:45 GMT
Changed:	0000-00-00 00:00:00
MD5:	6baf5069001c194d8fb8223fadbf7acd
SHA-256:	ac1ad976bbc9e28612e6b651741ef41777fb81a96f92bd3ab42fbe4e40a75719
Hash Lookup Results:	UNKNOWN
Internal ID:	2109

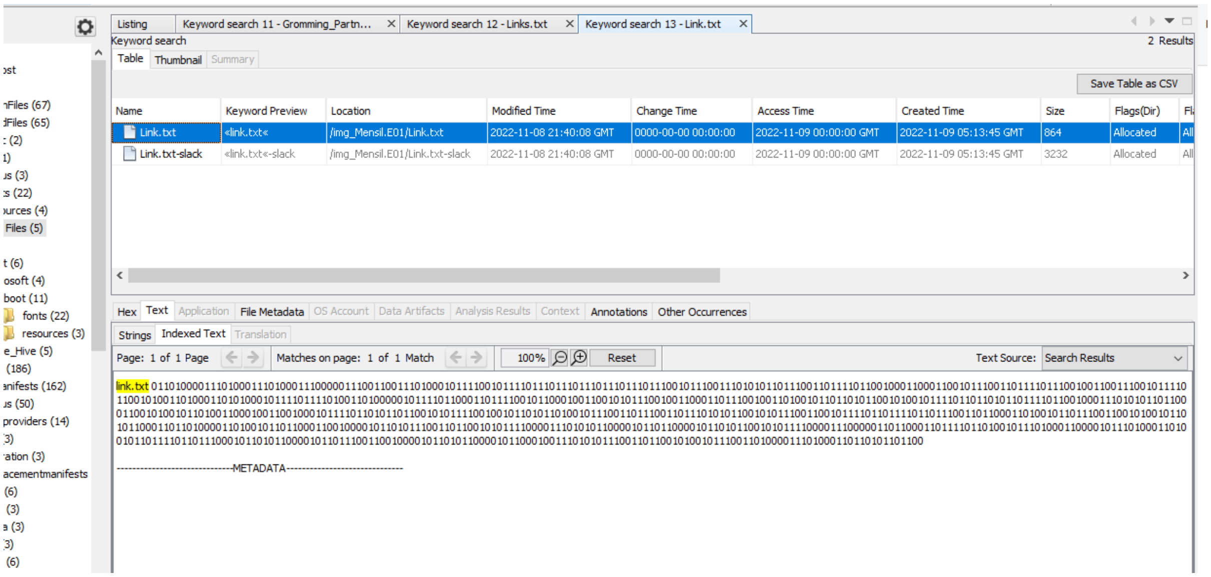
From The Sleuth Kit istat Tool:

Description and implications of the artefact:

In this section, after extracted the zip file we found a image that is related to sign language. That means another some secret message encoded in sign language. Using https://www.dcode.fr/american-sign-language this site we convert the sign language to plain text.

4.3.7 Category DHU_3

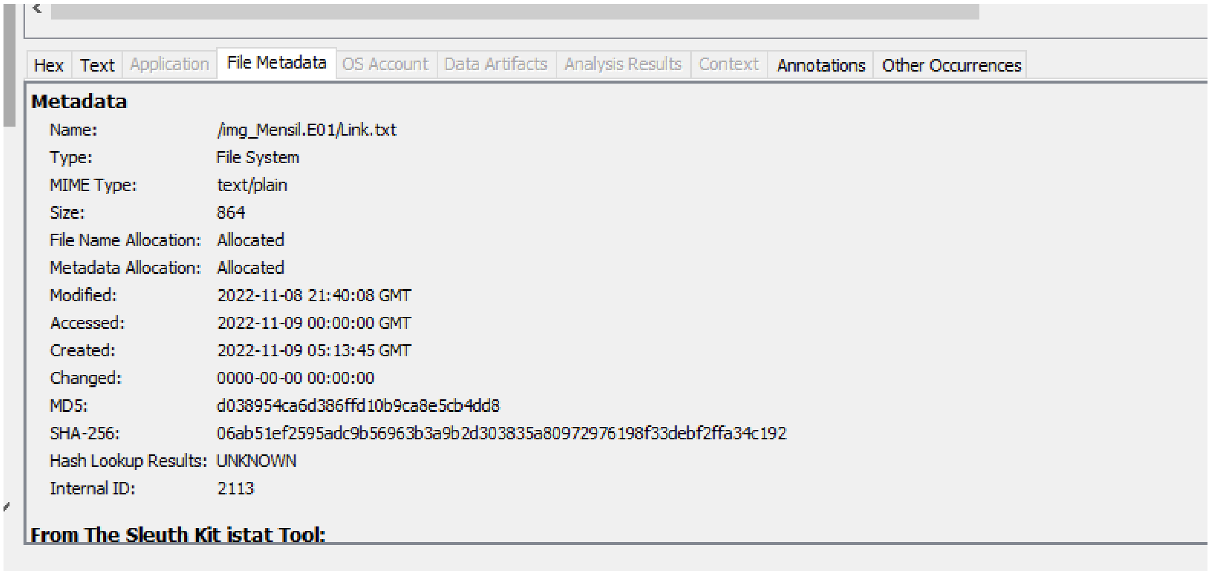
Screenshot of the artefact:



Name	Keyword Preview	Location	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Fl
Link.txt	«link.txt«	/img_Mensil.E01/Link.txt	2022-11-08 21:40:08 GMT	0000-00-00 00:00:00	2022-11-09 00:00:00 GMT	2022-11-09 05:13:45 GMT	864	Allocated	All
Link.txt-slack	«link.txt«-slack	/img_Mensil.E01/Link.txt-slack	2022-11-08 21:40:08 GMT	0000-00-00 00:00:00	2022-11-09 00:00:00 GMT	2022-11-09 05:13:45 GMT	3232	Allocated	All

```
link.txt 011010000111010001110100011100000111001100111010001011110010111101110111011101110111011100101110011101010110111001101111011001000110001100101110011011110111001001100111001011110
1100101001101000110101000101111011110100110100000101111011000110111100101100010011001010111001001100011011100100110100101101101011001010010111101101101011011110110010001110101011011000
0110010100101101001100010011001000101111011010110110010101111001001011010110100101110011011100110111010101100101011100110010111101101111011011100110110001101001011011100110010100101100
1011000110110100001101001011011000110010000101101011100110110010101111000011101010110000101101100001011010110010101111000011100000110110001101111011010010111010001100001011101000110100
0101101111011011100010110101100001011011100110010000101101011000010110001001110101011100110110010100101110011010000111010001101101011011000

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

A screenshot of artefact evidence details:



Metadata

Name:	/img_Mensil.E01/Link.txt
Type:	File System
MIME Type:	text/plain
Size:	864
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-11-08 21:40:08 GMT
Accessed:	2022-11-09 00:00:00 GMT
Created:	2022-11-09 05:13:45 GMT
Changed:	0000-00-00 00:00:00
MD5:	d038954ca6d386ffd10b9ca8e5cb4dd8
SHA-256:	06ab51ef2595adc9b56963b3a9b2d303835a80972976198f33debf2ffa34c192
Hash Lookup Results:	UNKNOWN
Internal ID:	2113

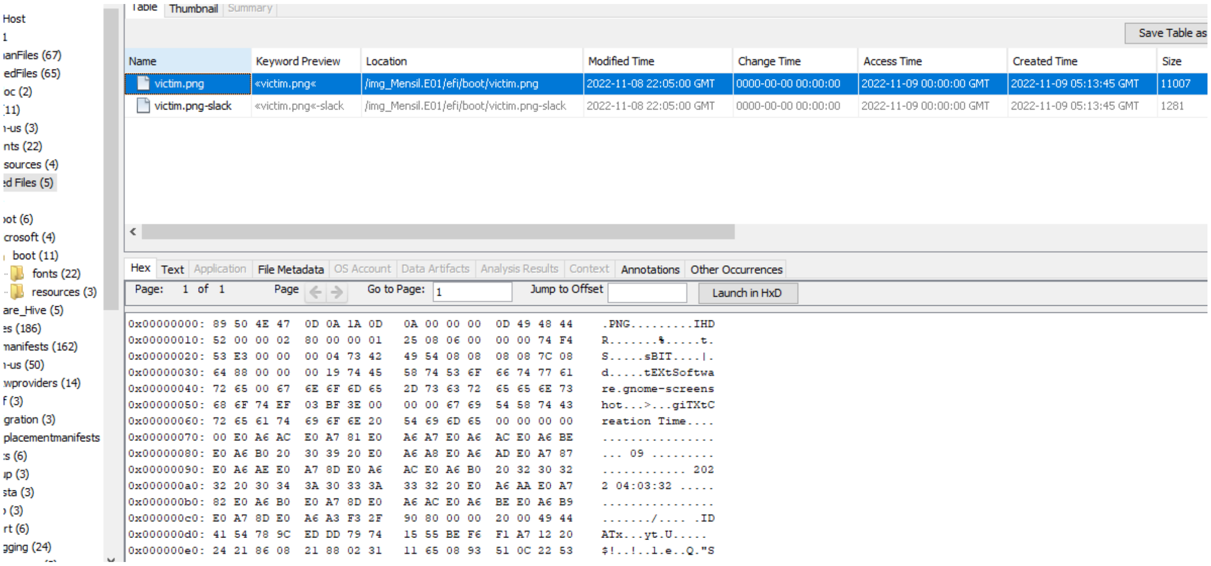
From The Sleuth Kit istat Tool:

Description and implications of the artefact:

In this section we dounf a link.txt file that is binary text. We will use a online decoder for this binary then we found a link that is related with Online child sexual exploitation and abuse. The link is: https://www.unodc.org/e4j/zh/cybercrime/module-12/key-issues/online-child-sexual-exploitation-and-abuse.html

4.3.8 Category DR_1

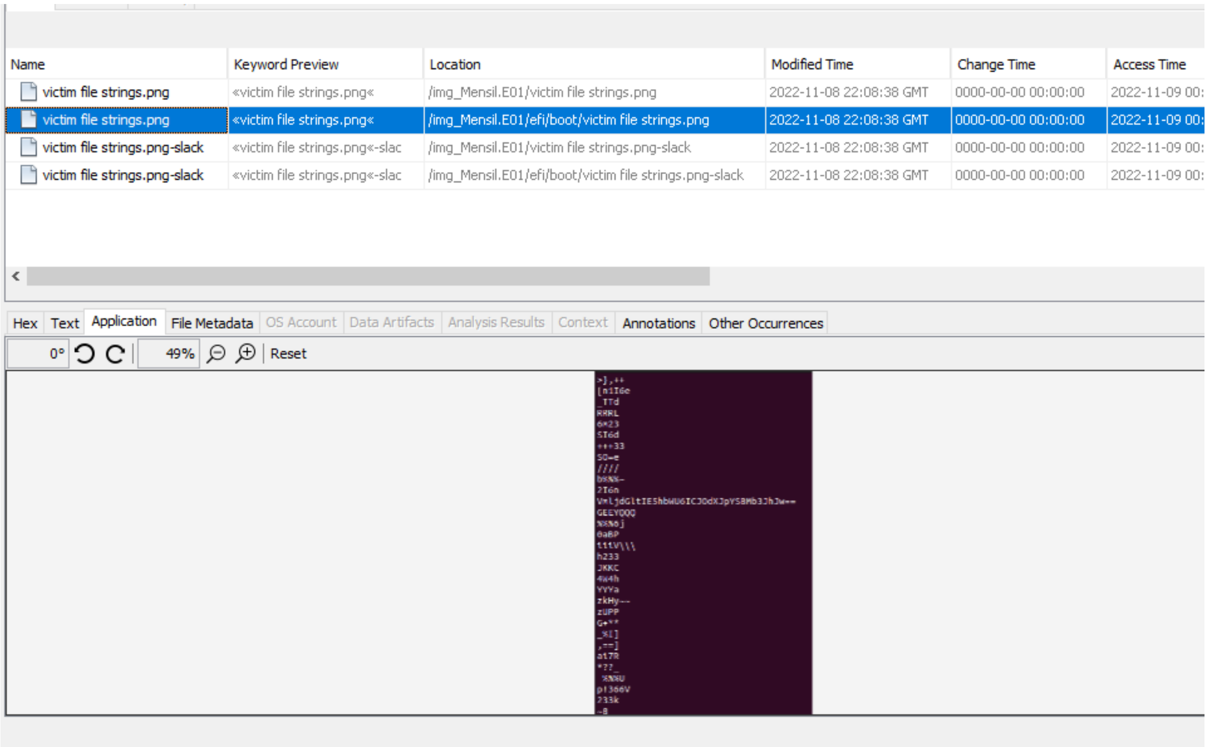
Screenshot of the artefact:



Name	Keyword Preview	Location	Modified Time	Change Time	Access Time	Created Time	Size
victim.png	«victim.png«	/img_Mensil.E01/efi/boot/victim.png	2022-11-08 22:05:00 GMT	0000-00-00 00:00:00	2022-11-09 00:00:00 GMT	2022-11-09 05:13:45 GMT	11007
victim.png-slack	«victim.png«-slack	/img_Mensil.E01/efi/boot/victim.png-slack	2022-11-08 22:05:00 GMT	0000-00-00 00:00:00	2022-11-09 00:00:00 GMT	2022-11-09 05:13:45 GMT	1281

Page: 1 of 1 Page Go to Page: 1 Jump to Offset

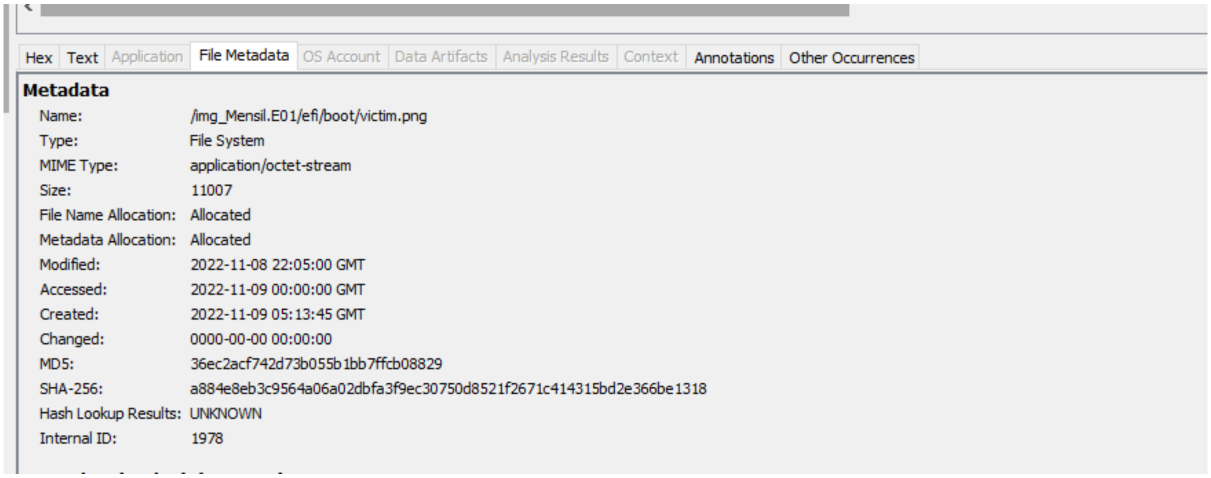
```
0x00000000: 89 50 4E 47  0D 0A 1A 0D  0A 00 00 00  0D 49 48 44   .PNG.........IHD
0x00000010: 52 00 00 02  80 00 00 01  25 08 06 00  00 00 74 F4   R.......%.....t.
0x00000020: 53 E3 00 00  00 04 73 42  49 54 08 08  08 08 7C 08   S.....sBIT....|.
0x00000030: 64 88 00 00  00 19 74 45  58 74 53 6F  66 74 77 61   d.....tEXtSoftwa
0x00000040: 72 65 00 67  6E 6F 6D 65  2D 73 63 72  65 65 6E 73   re.gnome-screens
0x00000050: 68 6F 74 EF  03 BF 3E 00  00 00 67 69  54 58 74 43   hot...>...giTXtC
0x00000060: 72 65 61 74  69 6F 6E 20  54 69 6D 65  00 00 00 00   reation Time....
0x00000070: 00 E0 A6 AC  E0 A7 81 E0  A6 A7 E0 A6  AC E0 A6 BE   ................
0x00000080: E0 A6 B0 20  30 39 20 E0  A6 A8 E0 A6  AD E0 A7 87   ... 09 .........
0x00000090: E0 A6 AE E0  A7 8D E0 A6  AC E0 A6 B0  20 32 30 32   ............ 202
0x000000a0: 32 20 30 34  3A 30 33 3A  33 32 20 E0  A6 AA E0 A7   2 04:03:32 .....
0x000000b0: 82 E0 A6 B0  E0 A7 8D E0  A6 AC E0 A6  BE E0 A6 B9   ................
0x000000c0: E0 A7 8D E0  A6 A3 F3 2F  90 80 00 00  20 00 49 44   ......./.... .ID
0x000000d0: 41 54 78 9C  ED DD 79 74  15 55 BE F6  F1 A7 12 20   ATx...yt.U.....
0x000000e0: 24 21 86 08  21 88 02 31  11 65 08 93  51 0C 22 53   $!..!..1.e..Q."S
```



Name	Keyword Preview	Location	Modified Time	Change Time	Access Time
victim file strings.png	«victim file strings.png«	/img_Mensil.E01/victim file strings.png	2022-11-08 22:08:38 GMT	0000-00-00 00:00:00	2022-11-09 00:
victim file strings.png	«victim file strings.png«	/img_Mensil.E01/efi/boot/victim file strings.png	2022-11-08 22:08:38 GMT	0000-00-00 00:00:00	2022-11-09 00:
victim file strings.png-slack	«victim file strings.png«-slac	/img_Mensil.E01/victim file strings.png-slack	2022-11-08 22:08:38 GMT	0000-00-00 00:00:00	2022-11-09 00:
victim file strings.png-slack	«victim file strings.png«-slac	/img_Mensil.E01/efi/boot/victim file strings.png-slack	2022-11-08 22:08:38 GMT	0000-00-00 00:00:00	2022-11-09 00:

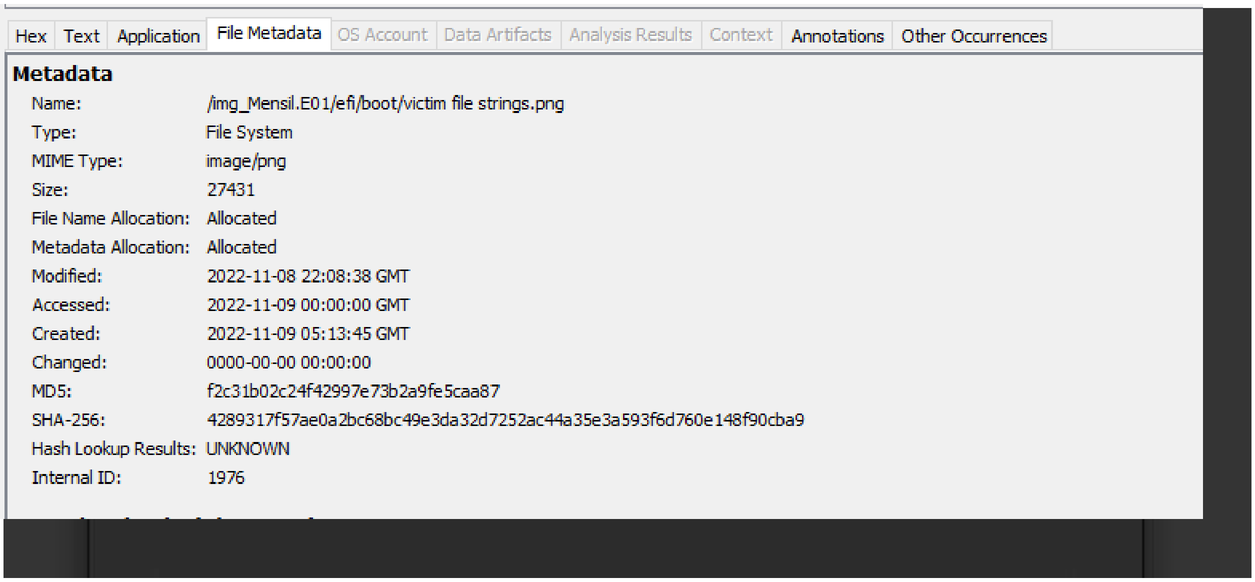
```
>},++
[n1I6e
_TTd
RRRL
6*23
SI6d
+++33
SO=e
////
b%%%-
2T6n
VmljdGltIE5hbWU6ICJOdXJpYSBMb3JhJw==
GEEYQQQ
%%%6j
0aBP
ttLV\\\
h233
JKKC
4W4h
YYYa
zkHy---
zUPP
G+**
_%I]
,==]
a17R
*??_
 %%%U
p!366V
233k
-8
```

A screenshot of artefact evidence details:



Metadata

Name:	/img_Mensil.E01/efi/boot/victim.png
Type:	File System
MIME Type:	application/octet-stream
Size:	11007
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-11-08 22:05:00 GMT
Accessed:	2022-11-09 00:00:00 GMT
Created:	2022-11-09 05:13:45 GMT
Changed:	0000-00-00 00:00:00
MD5:	36ec2acf742d73b055b1bb7ffcb08829
SHA-256:	a884e8eb3c9564a06a02dbfa3f9ec30750d8521f2671c414315bd2e366be1318
Hash Lookup Results:	UNKNOWN
Internal ID:	1978



Metadata

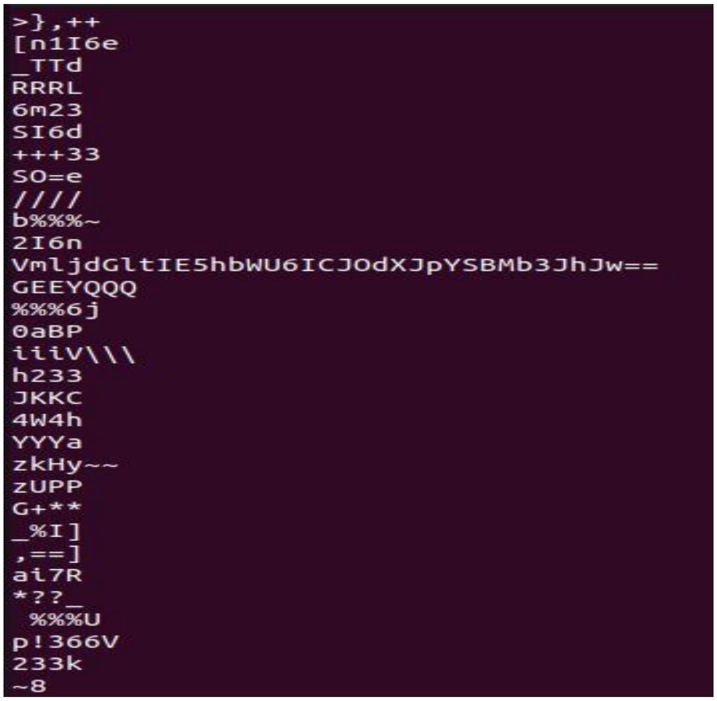
Name: /img_Mensil.E01/efi/boot/victim file strings.png
Type: File System
MIME Type: image/png
Size: 27431
File Name Allocation: Allocated
Metadata Allocation: Allocated
Modified: 2022-11-08 22:08:38 GMT
Accessed: 2022-11-09 00:00:00 GMT
Created: 2022-11-09 05:13:45 GMT
Changed: 0000-00-00 00:00:00
MD5: f2c31b02c24f42997e73b2a9fe5caa87
SHA-256: 4289317f57ae0a2bc68bc49e3da32d7252ac44a35e3a593f6d760e148f90cba9
Hash Lookup Results: UNKNOWN
Internal ID: 1976

Description and implications of the artefact:

In this section we will found victim original name. we found a image file named victim.png but its also not opened. But here we found a another image file that is related to this victim.png file. We noticed that victim.png file string compromised by this encase. So we notice that in the strings section have some hash txt like base64. We collect it and decode as same method as followed in previous. Then finally we found the victim original name. The extracted name or test is: “ Victim Name: Nuria Lora”

Description of the hiding/unhiding process:

Victim.png file corrupted by ASCII conversion. That means we need to check its strings.



```
>},++
[n1I6e
_TTd
RRRL
6m23
SI6d
+++33
SO=e
////
b%%%~
2I6n
VmljdGltIE5hbWU6ICJOdXJpYSBMb3JhJw==
GEEYQQQ
%%%6j
0aBP
iiiV\\\
h233
JKKC
4W4h
YYYa
zkHy~~
zUPP
G+**
_%I]
,==]
ai7R
*??_
 %%%U
p!366V
233k
~8
```

We can see that here is a hash value. Collect this hash and decode it. Then we found the text.

Hash: VmljdGltIE5hbWU6ICJOdXJpYSBMb3JhJw==

Decode site link: https://www.base64decode.org/

5. Supporting Material

Tools:

- Autopsy
- Access Data FTK Imager
- HXD

Site:

- https://www.base64decode.org/
- https://gchq.github.io/CyberChef/
- https://morsecode.world/international/decoder/audio-decoder-adaptive.html
- Convert Text to Audio Morse Code [Downloadable Audio] (meridianoutpost.com)
- https://www.dcode.fr/american-sign-language

6. Personal Reflection

6.1 Student 1

6.1.1 Reflection

Child Protection Policy is very need in this time. Digital crime is the most common factors for this time & child can easily the target by the social media.

6.1.2 Strengths/major contributions to the group

Completed the full Project on Child Protection Digital Crime Scenario make and Investigation on this.

6.1.3 What you found enjoyable

Data Encryption for Data Hiding. Most of Steganography Techniques Like morse and the other section is sign language.

6.1.4 What was challenging

File Signeture Mismathce checking and Correction.

6.1.5 Technical challenges and outcomes

Encase Forensics Imager is not free version, is premium. I am use Access Data FTK Imager for create the crime scenario evidence .E01 file. That was techniqal challenge for me. The outcome is it can be done easily by Encase Forensics but that is not available in every section like Not Open Source. So Its need to be Open source file.