

Case Scenario: Confidential Data of Offenders who did Sexual grooming of a Child.
Suspect: "Lord Bouse"
Victim Name: "Nuria Lora"

A forensic image of Lord Bouse's computer has been provided to you. A group of people grooms a child sexually. To get a youngster ready for eventual sexual involvement, they participate in predatory behavior. They interact with the child in an effort to become friends and build a bond through shared emotional experiences. In this instance, a person engages in predatory behavior to set up a youngster to become her friend, emotionally attach to her, and/or systematically take her social media account information. Social networking websites were used to establish their relationship. For the grooming of a child, he has partners.

1. OVERVIEW OF THE CASE	3
1.1 NARRATIVE OF THE CASE	3
1.2 TIMELINE OF KEY EVIDENCE.....	3
1.3 DETAILS OF THE OFFENDERS, VICTIMS AND WITNESSES	3
1.4 PHOTOGRAPHS OF ANY PHYSICAL EVIDENCE, CLUES OR SUPPLEMENTAL MATERIAL	3
1.5 SCENARIO RULES.....	4
2. LEGISLATION ANALYSIS	5
2.1 LEGISLATION	5
2.2 POINTS TO PROVE.....	5
2.3 WHAT THE DIGITAL FORENSICS CASE CAN PROVE	5
2.4 WHAT THE DIGITAL FORENSICS CASE WILL NOT PROVE.....	5
2.5 HIGHLIGHT ANY ARTEFACTS THAT UNDERMINE THE PROSECUTION’S CASE.....	5
3. EVIDENCE FILE	7
3.1 DETAILS OF THE EVIDENCE FILE	7
3.2 HASH VALUE OF THE EVIDENCE FILE.....	8
4. ARTEFACTS	10
4.1 SUMMARY OF ARTEFACTS	10
4.2 DATA RECOVERY ARTEFACTS.....	14
4.3 DATA HIDING ARTEFACTS	22
5. SUPPORTING MATERIAL	41
6. PERSONAL REFLECTION	42
6.1 STUDENT 1.....	42

1. Overview of the Case

1.1 Narrative of the case

A Group of Persons do Sexual grooming of a Child. To get a youngster ready for eventual sexual involvement, they participate in predatory behavior. They interact with the child in an effort to become friends and build a bond through shared emotional experiences. In this instance, a person engages in predatory behavior to set up a youngster to become her friend, emotionally attach to her, and/or systematically take her social media account information. 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: Thu Nov 10 19:07:21 2022

Acquisition finished: Thu Nov 10 19:36:54 2022

Segment list:

E:\Mensil.E01

E:\Mensil.E02

E:\Mensil.E03

Image Verification Results:

Verification started: Thu Nov 10 19:36:54 2022

Verification finished: Thu Nov 10 19:49:49 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

Detailed information on all types of child sexual exploitation and abuse was gathered. The opinions of children and young people are taken into account as a crucial component in the creation of legislation pertaining 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: 957

Evidence Number: 567

Unique Description:

Examiner: Mensil N

Notes: Child Protection in the Digital Age

Information for E:\Mensil:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 6,527

Tracks per Cylinder: 255

Sectors per Track: 63

Bytes per Sector: 512

Sector Count: 104,857,600

[Physical Drive Information]

Drive Model: VBOX HARDDISK

Drive Serial Number: VB58036779-832520e8

Drive Interface Type: IDE

Removable drive: False

Source data size: 51200 MB

Sector count: 104857600

Image Information:

Acquisition started: Thu Nov 10 19:07:21 2022

Acquisition finished: Thu Nov 10 19:36:54 2022

Segment list:

E:\Mensil.E01

E:\Mensil.E02

E:\Mensil.E03

Image Verification Results:

Verification started: Thu Nov 10 19:36:54 2022

Verification finished: Wed Nov 10 19:49:49 2022

3.2 Hash value of the Evidence File

[Computed Hashes]

MD5 checksum: 1d3faa7b469bf864264cabe01a899f32 : verified

SHA1 checksum: 2dc7043a37c44219f3c0f676468c31101957e73 : verified

Created By AccessData® FTK® Imager 4.5.0.3

Case Information:

Acquired using: ADI4.5.0.3

Case Number: 957

Evidence Number: 567

Unique Description:

Examiner: Mensil N

Notes: Child Protection in the Digital Age

Information for E:\Mensil:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 6,527

Tracks per Cylinder: 255

Sectors per Track: 63

Bytes per Sector: 512

Sector Count: 104,857,600

[Physical Drive Information]

Drive Model: VBOX HARDDISK

Drive Serial Number: VB58036779-832520e8

Drive Interface Type: IDE

Removable drive: False

Source data size: 51200 MB

Sector count: 104857600

[Computed Hashes]

MD5 checksum: 1d3faa7b469bf864264cabe01a899f32

SHA1 checksum: 2dc7043a37c44219f3c0f676468c31101957e73

Image Information:

Acquisition started: Thu Nov 10 19:07:21 2022

Acquisition finished: Thu Nov 10 19:36:54 2022

Segment list:

E:\Mensil.E01

E:\Mensil.E02

E:\Mensil.E03

Image Verification Results:

Verification started: Thu Nov 10 19:36:54 2022

Verification finished: Thu Nov 10 19:49:49 2022

MD5 checksum: 1d3faa7b469bf864264cabe01a899f32 : verified

SHA1 checksum: 2dc7043a37c44219f3c0f676468c31101957e73 : 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	Item NO.	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.
DR0S	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.wav	File Containing ethical consideration message for child protection.
DH0S	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	Lourd bouse.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

Table of Evidence Items

Item no.	Grade (1-5 in ascending order) / Row No in CSV File	Description of Evidence Item and its significance to the case.	Provenance Block	Method of Hiding	Password (if any) required to access this item	Method to be used by examiner to find
4.2.1	219721 & 219736	Files containing the victim child image & Clarification.	Info. Located on CSV File by Row no.	Victim info in pdf document	N/A	In Documents file found the project_1.pdf file & info from pdf that is related to name then keyword search by name.
4.2.2	219777	File containing some social media chat logs between victim & offender.	Info. Located on CSV File by Row no.	N/A	N/A	Manual Findings in Pictures section.
4.2.3	185	File containing the information about offender edited the victim image for sexually Abuse. Like tools and file.	Info. Located on CSV File by Row no.	N/A	N/A	Software_Hive useful for data editing.
4.2.4	219735	Files containing information about child protection research article by UNICEF.	Info. Located on CSV File by Row no.	N/A	N/A	Recycle Bin for windows so its found from Deleted files section
4.3.1	219737	Contains information about sexual abused images goes to online.	Info. Located on CSV File by Row no.	In White Background using White text	N/A	Manual findings in metadata
4.3.2	219759	File Containing ethical consideration message for child protection.	Info. Located on CSV File by Row no.	In Morse Code Audio	N/A	In Audio section also in metadata
4.3.3	219739	File containing Data secret data hiding by changing the file extension	Info. Located on CSV	Change extension	N/A	Extension Mismatched detection

			File by Row no.			
4.3.4	219763	File containing offender real image information.	Info. Located on CSV File by Row no.	Check header signature and correct with matching by extension signature	N/A	Image Gallery in Autopsy
4.3.5	219734	File Containing the victim child abused image.	Info. Located on CSV File by Row no.	Password protected zip	Pass : tort oise 123	Metadata section
4.3.6	219732	File Containing the information of offender partners.	Info. Located on CSV File by Row no.	Encoded message in American sign language	N/A	Metadata section
4.3.7	219730	File containing information on a article related with online child sexual exploitation and abuse	Info. Located on CSV File by Row no.	In Binary Value	N/A	Manual Findings in Documents section
4.3.8	219725	Here is Some secret string under this image. Containing information about victim real name.	Info. Located on CSV File by Row no.	In image String with base64 hash	N/A	Metadata and pictures section or Image gallery

4.2 Data Recovery Artefacts

4.2.1 Category DRF

Screenshot of the artefact:

Item Number	Description
4.2.1	Files containing the victim child image & Clarification.
Location on Stick	Partition 2\NONAME [NTFS]\[root]\Users\Mensil N\Desktop\Project_1.pdf\

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
<div>< <div></div> ></div>										
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences										
Result: 1 of 1 Result <div>< ></div> Metadata										
Type	Value		Source(s)							
Version	1.4		org.sleuthkit.autopsy.keywordsearch.KeywordSearchIngestModule							
Source File Path	/img_Mensil.E01/ef/microsoft/Project_1.pdf									
Artifact ID	-9223372036854775743									

Its me



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

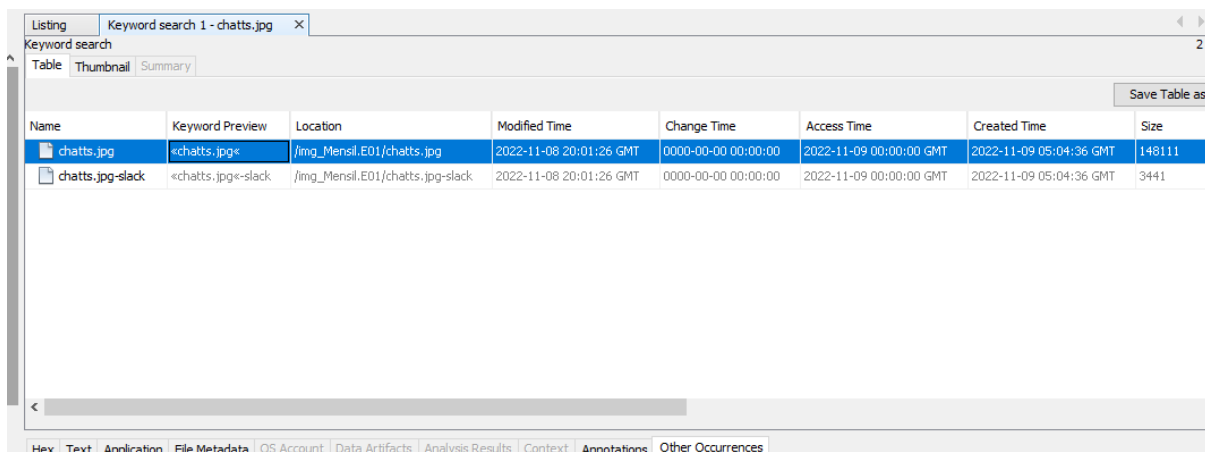
Description and implications of the artefact:

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:

Item Number	Description
4.2.2	File containing some social media chat logs between victim & offender.
Location on Stick	Partition 2\NONAME [NTFS]\[root]\Users\Mensil N\Pictures\Saved Pictures\chatts.jpg\



The screenshot shows a 'Keyword search 1 - chatts.jpg' window. It contains a table with the following data:

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

At the bottom of the window, there is a navigation bar with the following tabs: Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences.



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

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

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:

Item Number	Description
4.2.3	File containing the information about offender edited the victim image for sexually Abuse. Like tools and file.
Location on Stick	Partition 2\NONAME [NTFS]\[root]\Software_Hive\

Listing
/img_Mensil.E01/Software_Hive 5 Results

Table Thumbnail Summary

Save Table as CSV

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	/
[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	/
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	/
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	/
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	/

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

A screenshot of artefact evidence details:

Listing
/img_Mensil.E01/Software_Hive

Table Thumbnail Summary

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

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

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 abuse image edited by paint software & the files hives saved.

4.2.4 Category DRFS

Screenshot of the artefact:

Item Number	Description
4.2.4	Files containing information about child protection research article by UNICEF.
Location on Stick	Partition 2\NONAME [NTFS]\[root]\Users\Mensil N\Documents\Deleted Files\

Child_Protection - Autopsy 4.19.3

Case View Tools Window Help

+ Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Keyword Lists Keyword Search

Listing /img_Mensil.E01/Deleted Files 5 Results

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

Save Table as CSV

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

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Result: 1 of 1 Result									Metadata
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:

Listing

/img_Mensil.E01/Deleted Files

Table

Thumbnail

Summary

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 00:00:00
[parent folder]				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 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 00:00:00
ict_eng.pdf			0	2022-11-08 20:37:36 GMT	0000-00-00 00:00:00	2022-11-09 00:00:00
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 00:00:00

<

Hex

Text

Application

File Metadata

OS Account

Data Artifacts

Analysis Results

Context

Annotations

Other Occurrences

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

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Metadata									
Name:	/img_Mensil.E01/Deleted Files/Legislatng 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:

Item Number	Description
4.3.1	Contains information about sexual abused images goes to online.
Location on Stick	Partition 2\NONAME [NTFS]\[root]\Users\Mensil N\Documents\Something_Bookmark.docx\

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

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: 1 of 1 Match
100%
Reset
Text Source: Search Results

something_bookmark.docx Q2hpbGQgc2V4dWFsIGV4cGxvaXRhdGlvb2ZlcnMgdG8gdGhIHNleHVhbCBhYnVzZSBvZiBhI
HBlcnNvb2ZlcnMgdG8gdGhIHNleHVhbCBhYnVzZSBvZiBhIHB1cnNvb2ZlcnMgdG8gdGhIHNleHVhbCBhYnVzZSBvZiBhI
9mIGltYWdlcyBvZiBzdWN0IGFidXNlIGFuZCB0aGUgc2hhcmLuZyBvZiB0aG9zZSBpbWFnZXMgb25saW5l

Base64 Decode and Encode - Online

METADATA

Content:

Q2hpbGQgc2V4dWFsIGV4cGxvaXRhdGlvb2ZlcnMgdG8gdGhIHNleHVhbCBhYnVzZSBvZiBhI
HBlcnNvb2ZlcnMgdG8gdGhIHNleHVhbCBhYnVzZSBvZiBhIHB1cnNvb2ZlcnMgdG8gdGhIHNleHVhbCBhYnVzZSBvZiBhI
9mIGltYWdlcyBvZiBzdWN0IGFidXNlIGFuZCB0aGUgc2hhcmLuZyBvZiB0aG9zZSBpbWFnZXMgb25saW5l

[Base64 Decode and Encode - Online](#)

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/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.

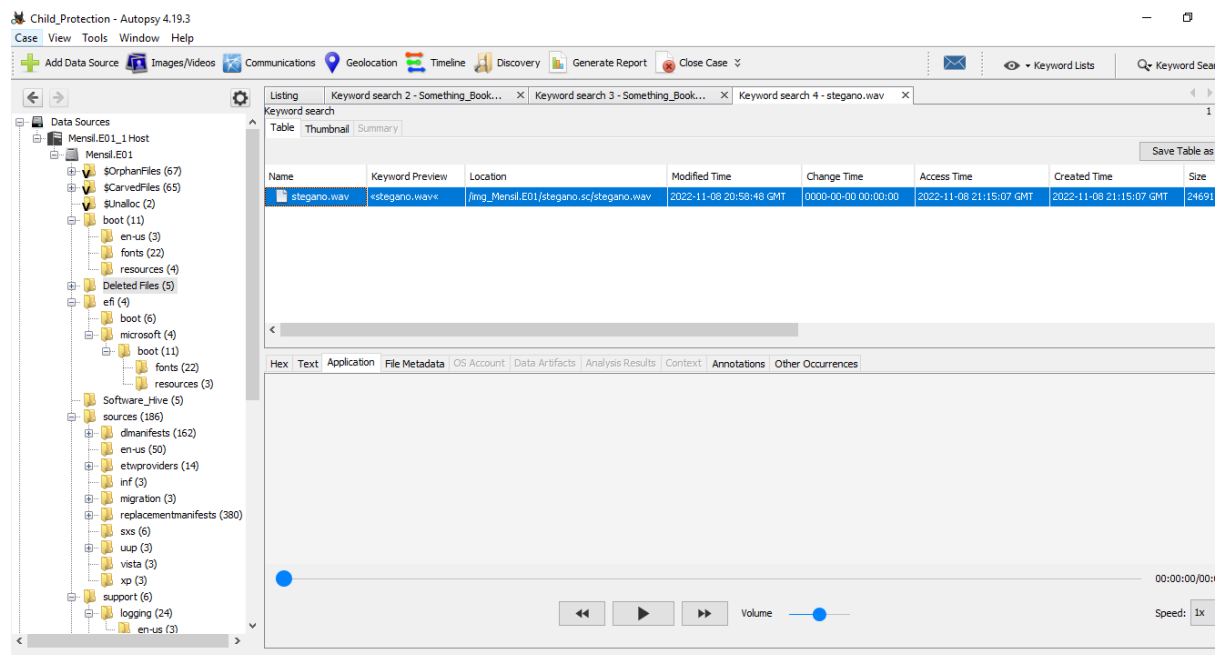
Description of the hiding/unhiding process:

Hide the characters in a docs file by a white background. Essentially, when it is opened, it can show a blank page, but mark it and change the color to reveal the text that has a hash value similar to base64. We decode from base64 decoder.

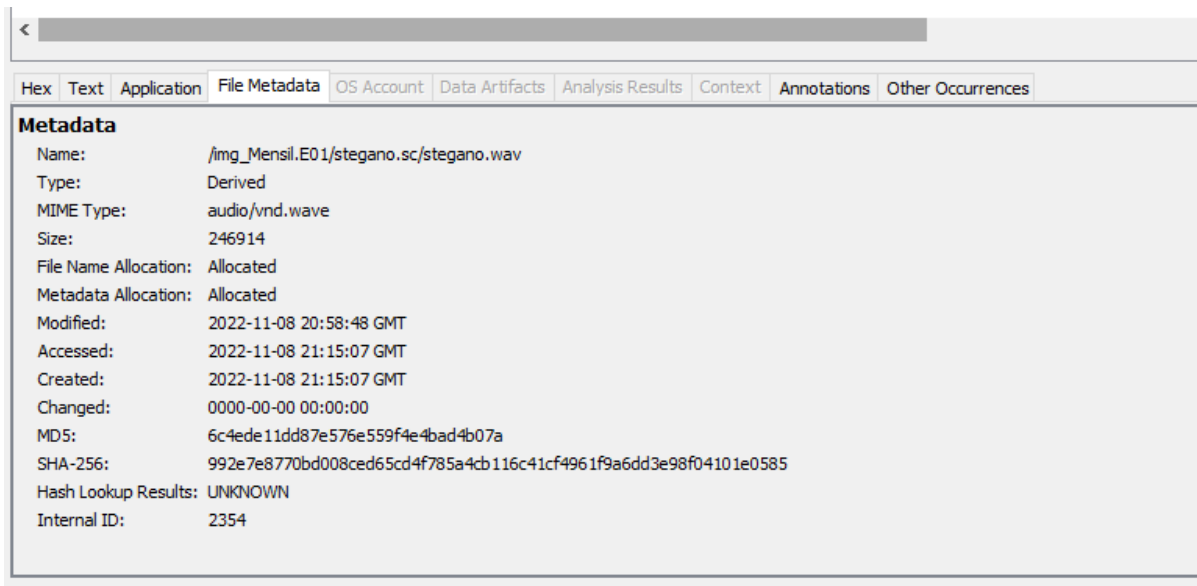
4.3.2 Category DHA

Screenshot of the artefact:

Item Number	Description
4.3.2	File Containing ethical consideration message for child protection.
Location on Stick	Partition 2\NONAME [NTFS]\[root]\Users\Mensil N\Music\stegano.wav\



A screenshot of artefact evidence details:



Description and implications of the artefact:

Offender Used the steganography technique for hide some secret data that is related to Grooming of a child & Abuselement. The extracted message will shown here.

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
<input checked="" type="radio"/>	Morse	20	-100	-30	700	700	200	256
<input type="radio"/>	Alphabet	30	-100	-30	600	600	200	256
<input type="radio"/>	Alphabet	40	-60	-30	700	700	200	256
<input type="radio"/>	Fox (via mic)	23	-60	-30	600	700	225	256
<input type="radio"/>	Inspector Morse	10	-60	-30	1313	1358	25	1024
<input type="radio"/>	Two Tone	20	-60	-30	300	300	200	1024
<input type="radio"/>	Two Tone	20	-60	-30	700	700	200	1024

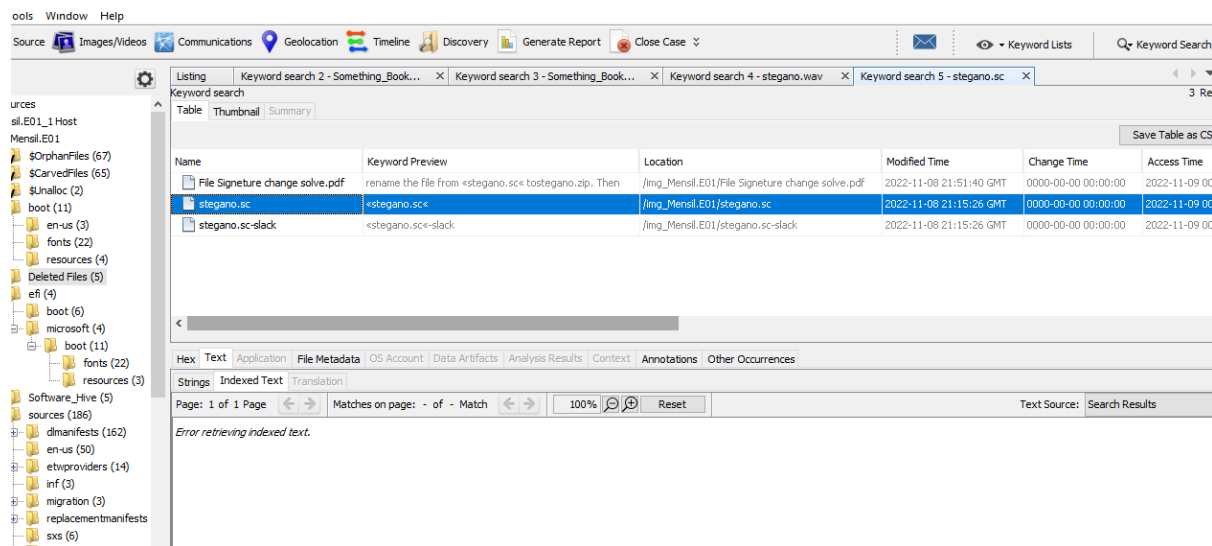
Use the "Apply" button to change the parameters to those selected in the table. The "Play" button will play the selected file regardless.

4.3.3 Category DHOS

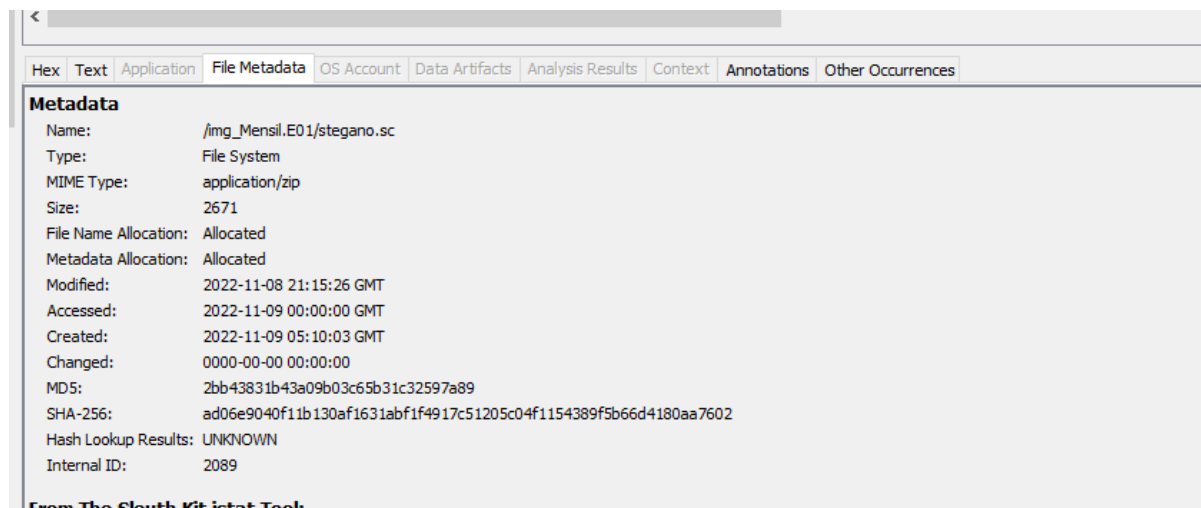
Screenshot of the artefact:

Item Number	Description
-------------	-------------

4.3.3	File containing Data secret data hiding by changing the file extension
Location on Stick	Partition 2\NONAME [NTFS]\[root]\Users\Mensil N\Documents\stegano.sc



A screenshot of artefact evidence details:

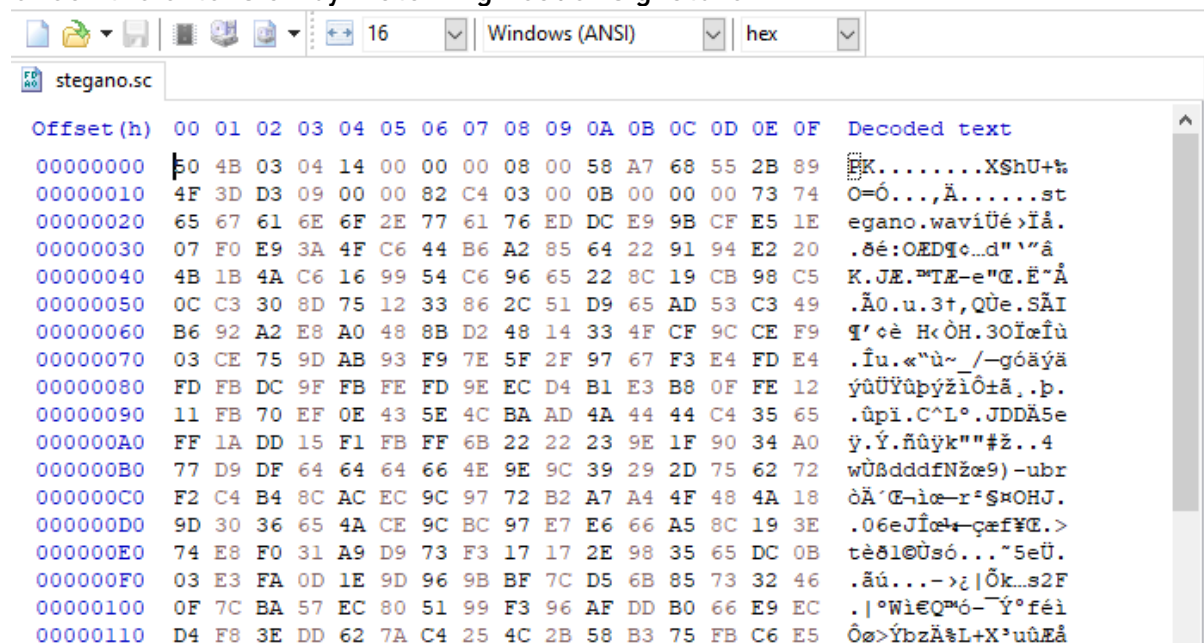


Description and implications of the artefact:

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 matching header signature.



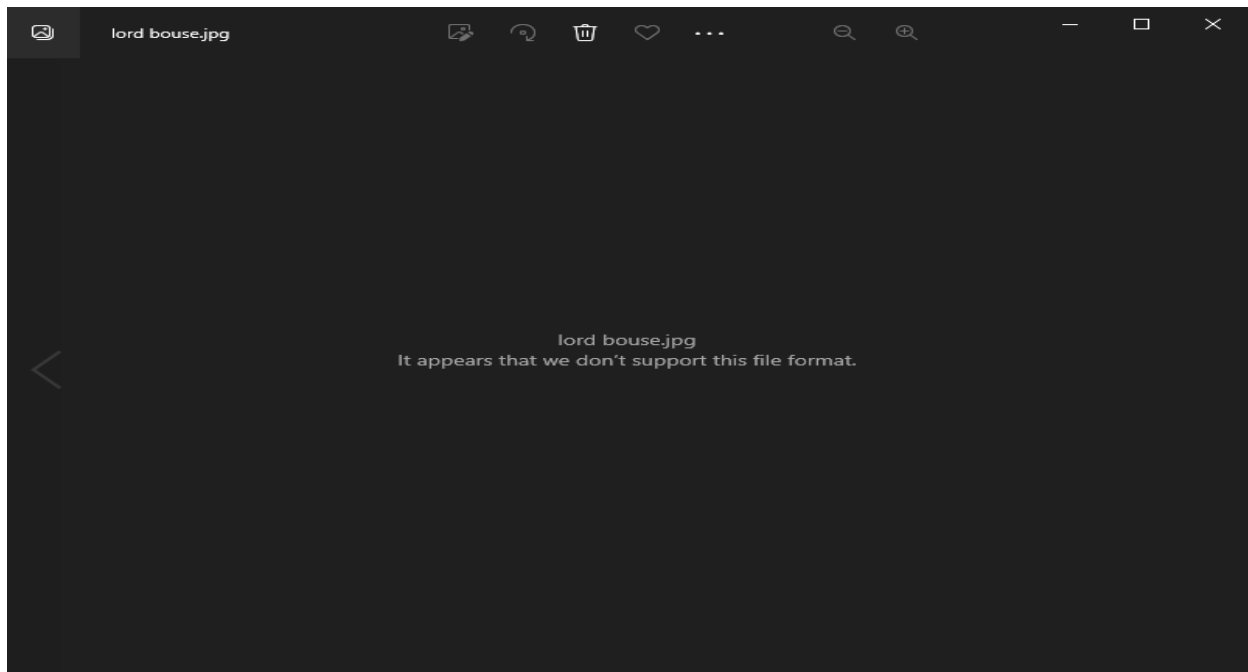
```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
00000000 50 4B 03 04 14 00 00 00 08 00 58 A7 68 55 2B 89 PK.....XShU+%
00000010 4F 3D D3 09 00 00 82 C4 03 00 0B 00 00 00 73 74 O=Ó...,Ä.....st
00000020 65 67 61 6E 6F 2E 77 61 76 ED DC E9 9B CF E5 1E egano.waviÜé>IÄ.
00000030 07 F0 E9 3A 4F C6 44 B6 A2 85 64 22 91 94 E2 20 .8é:OEDqco...d"\'ä
00000040 4B 1B 4A C6 16 99 54 C6 96 65 22 8C 19 CB 98 C5 K.JÆ."TÆ-e"Æ.Ë~Å
00000050 0C C3 30 8D 75 12 33 86 2C 51 D9 65 AD 53 C3 49 .Ä0.u.3+,QÜe.SÄI
00000060 B6 92 A2 E8 A0 48 8B D2 48 14 33 4F CF 9C CE F9 q'cè H<ÖH.3Oiafù
00000070 03 CE 75 9D AB 93 F9 7E 5F 2F 97 67 F3 E4 FD E4 .ïu.«"ù~/--góäyã
00000080 FD FB DC 9F FB FE FD 9E EC D4 B1 E3 B8 0F FE 12 ýÜÜýÜpýžĩô±ã,.p.
00000090 11 FB 70 EF 0E 43 5E 4C BA AD 4A 44 44 C4 35 65 .ûpĩ.C^L°.JDDÄ5e
000000A0 FF 1A DD 15 F1 FB FF 6B 22 22 23 9E 1F 90 34 A0 ý.Ý.ñúyk""#ž..4
000000B0 77 D9 DF 64 64 64 66 4E 9E 9C 39 29 2D 75 62 72 wÜBdddfNžæ9)-ubr
000000C0 F2 C4 B4 8C AC EC 9C 97 72 B2 A7 A4 4F 48 4A 18 òÄ'Æ-ia-r²$=OHJ.
000000D0 9D 30 36 65 4A CE 9C BC 97 E7 E6 66 A5 8C 19 3E .06eJia-çaf¥Æ.>
000000E0 74 E8 F0 31 A9 D9 73 F3 17 17 2E 98 35 65 DC 0B tè8l@Üsó...~5eÜ.
000000F0 03 E3 FA 0D 1E 9D 96 9B BF 7C D5 6B 85 73 32 46 .äú...->¿|Ök...s2F
00000100 0F 7C BA 57 EC 80 51 99 F3 96 AF DD B0 66 E9 EC .|°WiEQ"ó-~Ý°féi
00000110 D4 F8 3E DD 62 7A C4 25 4C 2B 58 B3 75 FB C6 E5 Ôø>ÝbzÄ%L+X³uûÄÄ
```

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

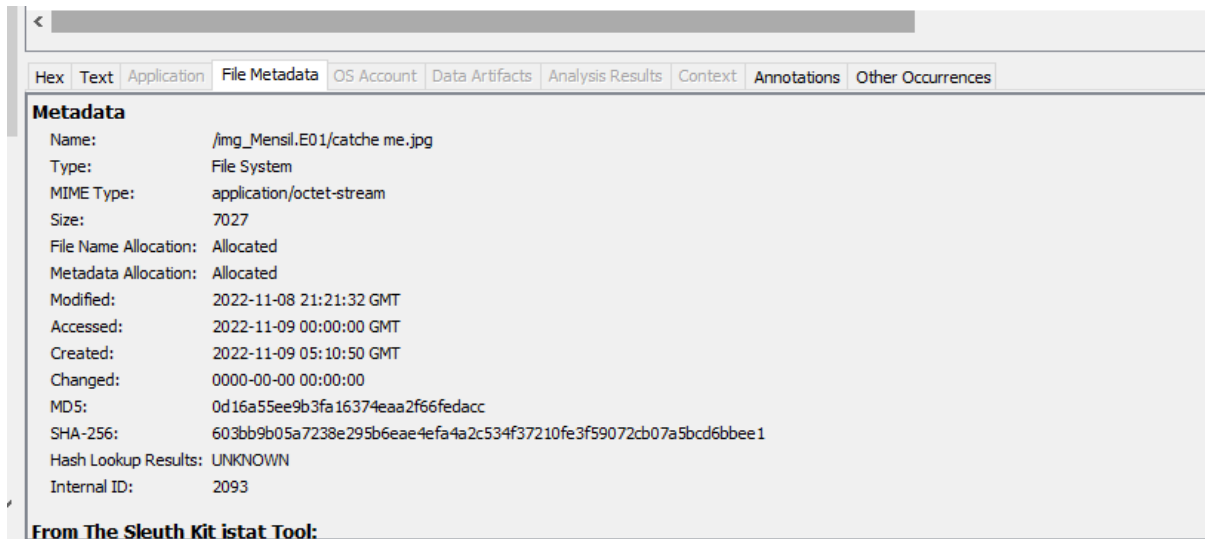
4.3.4 Category DHFS

Screenshot of the artefact:

Item Number	Description
4.3.4	File containing offender real image information.
Location on Stick	Partition 2\NONAME [NTFS]\[root]\Users\Mensil N\Pictures\lord bouse.jpg\



A screenshot of artefact evidence details:



“Catche me.jpg” replace by “lord bouse.jpg”

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 “lord bouse” 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 file 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.

And start with some wrong hex like this

00001B00	00	1F	51	F9	7F	F0	35	F9	BF	F8	AA	28	AE	FC	0B	B6	..Qù.85ùgø*(@ü.¶
00001B10	22	16	38	31	B1	52	C3	CE	E6	BF	C6	ED	23	CB	92	C7	".81±RÄîæ;Æi#È'Ç
00001B20	54	54	EF	F6	79	3F	F4	24	FF	00	D9	AB	CB	B9	A2	8A	TTiöy?ô\$ÿ.Û«Ë¹cŠ
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	c¼sØ.hæŠ(.æŽhc€.
00001B50	68	E6	8A	28	00	E6	8E	68	A2	80	0E	68	E6	8A	28	00	hæŠ(.æŽhc€..hæŠ(.æŽhc€.
00001B60	E6	8E	68	A2	80	0E	68	E6	8A	28	00	E6	8E	68	A2	80	æŽhc€..hæŠ(.æŽhc€
00001B70	3F	FF	D9														?ÿÜ

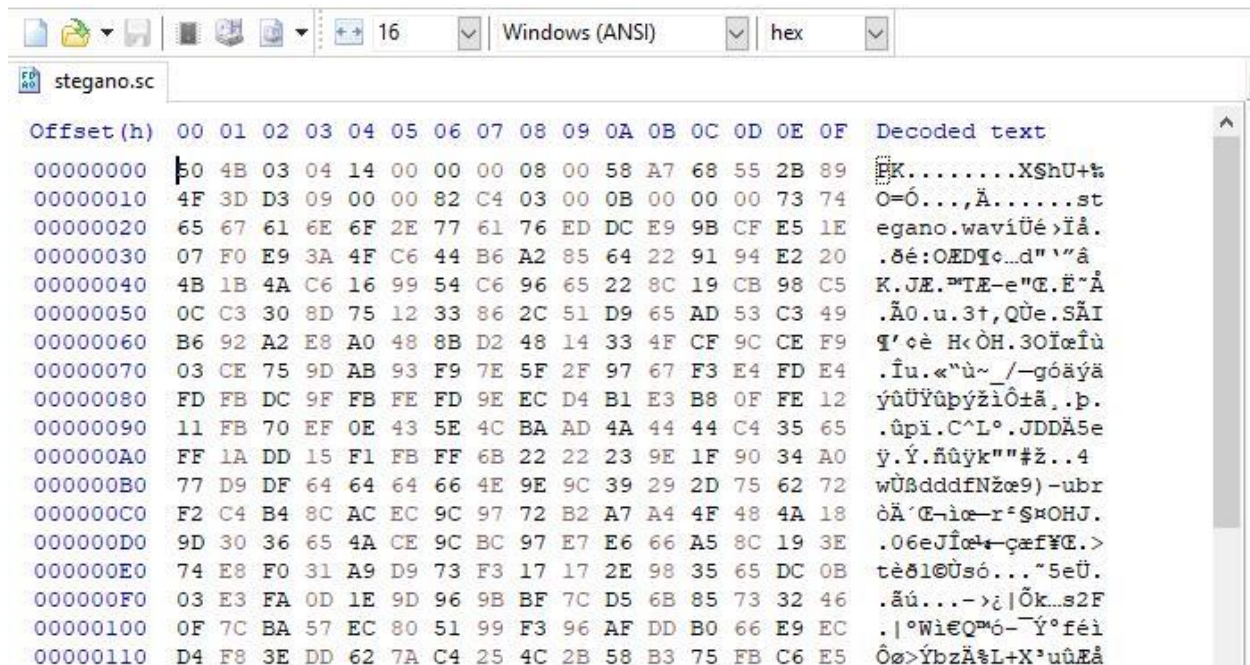
lord bouse.jpg																	
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	EF	D0	EF	E2	00	10	4A	46	49	46	00	01	01	01	00	60	iDlâ..JFIF.....`
00000010	00	60	00	00	FF	DB	00	43	00	03	02	02	03	02	02	03	..ÿÜ.C.....
00000020	03	03	03	04	03	03	04	05	08	05	05	04	04	05	0A	07
00000030	07	06	08	0C	0A	0C	0C	0B	0A	0B	0B	0D	0E	12	10	0D
00000040	0E	11	0E	0B	0B	10	16	10	11	13	14	15	15	15	0C	0F
00000050	17	18	16	14	18	12	14	15	14	FF	DB	00	43	01	03	04ÿÜ.C...
00000060	04	05	04	05	09	05	05	09	14	0D	0B	0D	14	14	14	14
00000070	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14

But we can also see that it begins with JFIF in the ascii portion and ends with hex FF D9. It is a jpeg fle, then. Extension fits the bill. But because of the mismatched signature, this cannot be opened.

We know that the Jpg file 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.



Hex starts from 50 4B 03 04 that means it's a zip fle. Zip file 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:

Item Number	Description
4.3.5	File Containing the victim child abused image.
Location on Stick	Partition 2\NONAME [NTFS]\[root]\Users\Mensil N\Documents\child_abused_Image.zip

...k... Keyword search 4 - stegano.wav X Keyword search 5 - stegano.sc X Keyword search 6 - catche me X Keyword search 7 - catche me.jpg X 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

<

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% [icon] [icon] Reset Text Source: Search

Error retrieving indexed text.

...sc Keyword search 6 - catche me X Keyword search 7 - catche me.jpg X Keyword search 8 - child_abused_I... X Keyword search 9 - child_abused_I... X Keyword search 10 - notes X 19

Keyword search

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-(

<

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: 1 of 1 Match < > 100% [icon] [icon] Reset Text Source: Search Results

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

-----METADATA-----

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/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:									

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
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:	bc8f83071d036ef18c783931fca3aeea35ae609c101dbe9618ee2c8fc1a650f3								
Hash Lookup Results:	UNKNOWN								
Internal ID:	2115								

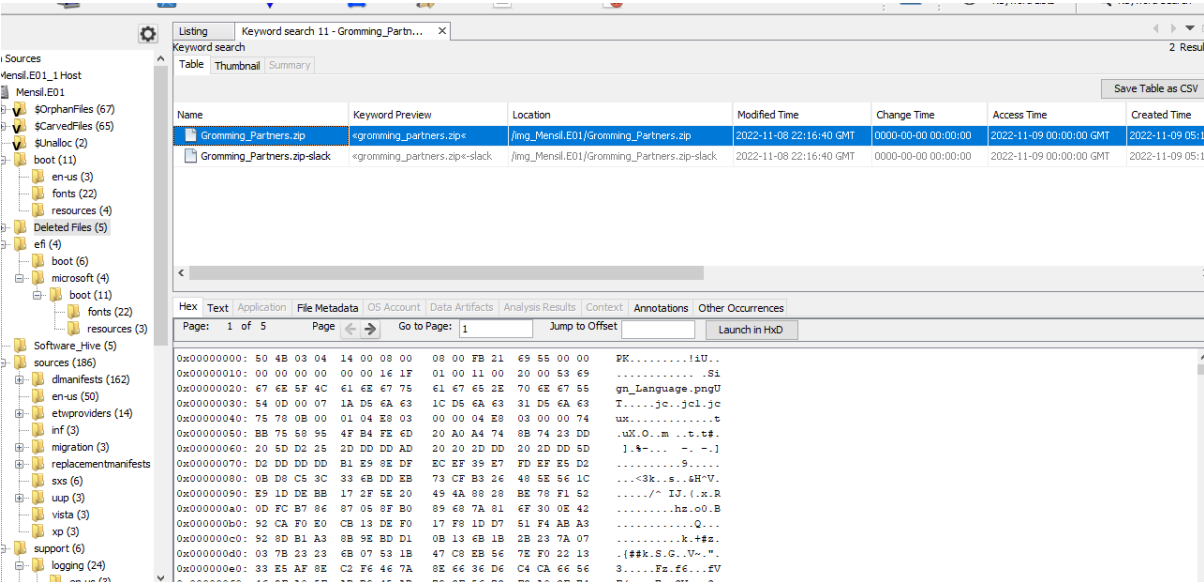
Description and implications of the artefact:

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:

Item Number	Description
4.3.6	File Containing the information of offender partners.
Location on Stick	Partition 2\NONAME [NTFS]\[root]\Users\Mensil N\Documents\Gromming_Partners.zip



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/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:		6baf5069001c194d8fb8223fadb77acd							
SHA-256:		ac1ad976bbc9e28612e6b651741ef41777fb81a96f92bd3ab42fbe4e40a75719							
Hash Lookup Results:		UNKNOWN							
Internal ID:		2109							

Description and implications of the artefact:

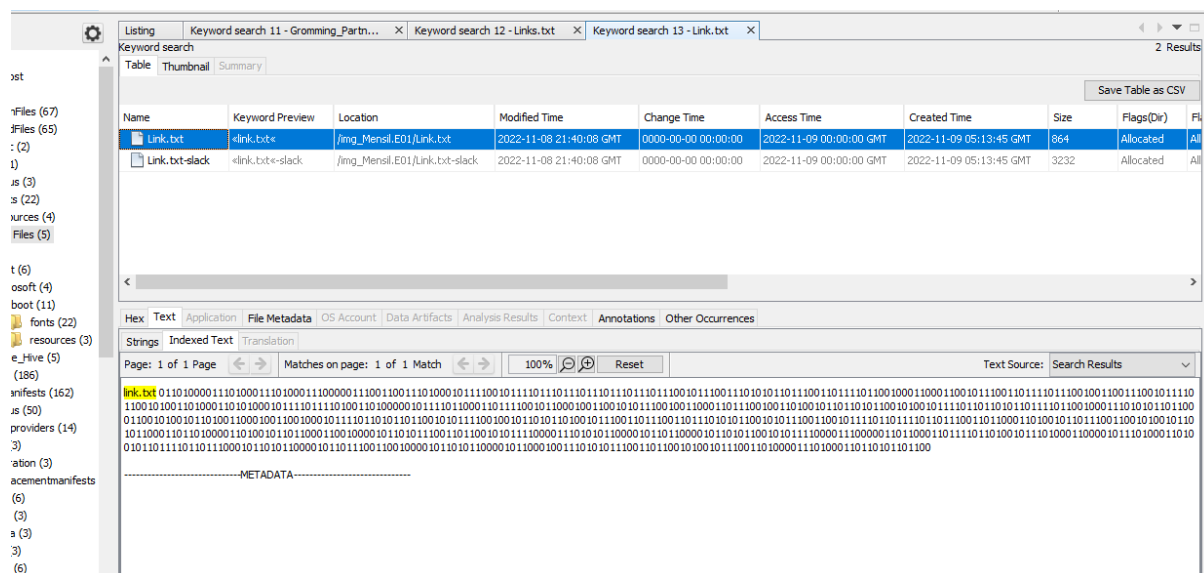
In this section, after extracted the zip file we found a image that is related to sign language. That means another some secret message encoded in sign language. Using

<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:

Item Number	Description
4.3.7	File containing information on a article related with online child sexual exploitation and abuse
Location on Stick	Partition 2\NONAME [NTFS]\[root]\Users\Mensil N\Documents\Link.txt



A screenshot of artefact evidence details:



Description and implications of the artefact:

In this section we found a link.txt file that is binary text. We will use an online decoder for this binary then we found a link that is related with Online child sexual exploitation and abuse. After extraction and decode the link will be shown.

4.3.8 Category DR_1

Screenshot of the artefact:

Item Number	Description
4.3.8	Here is Some secret string under this image. Containing information about victim real name.
Location on Stick	Partition 2\NONAME [NTFS]\[root]\Users\Mensil N\Documents\victim.png

Table Thumbnail Summary							
Save Table as							
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

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Page: 1 of 1	Page	Go to Page: 1	Jump to Offset	Launch in HxD					

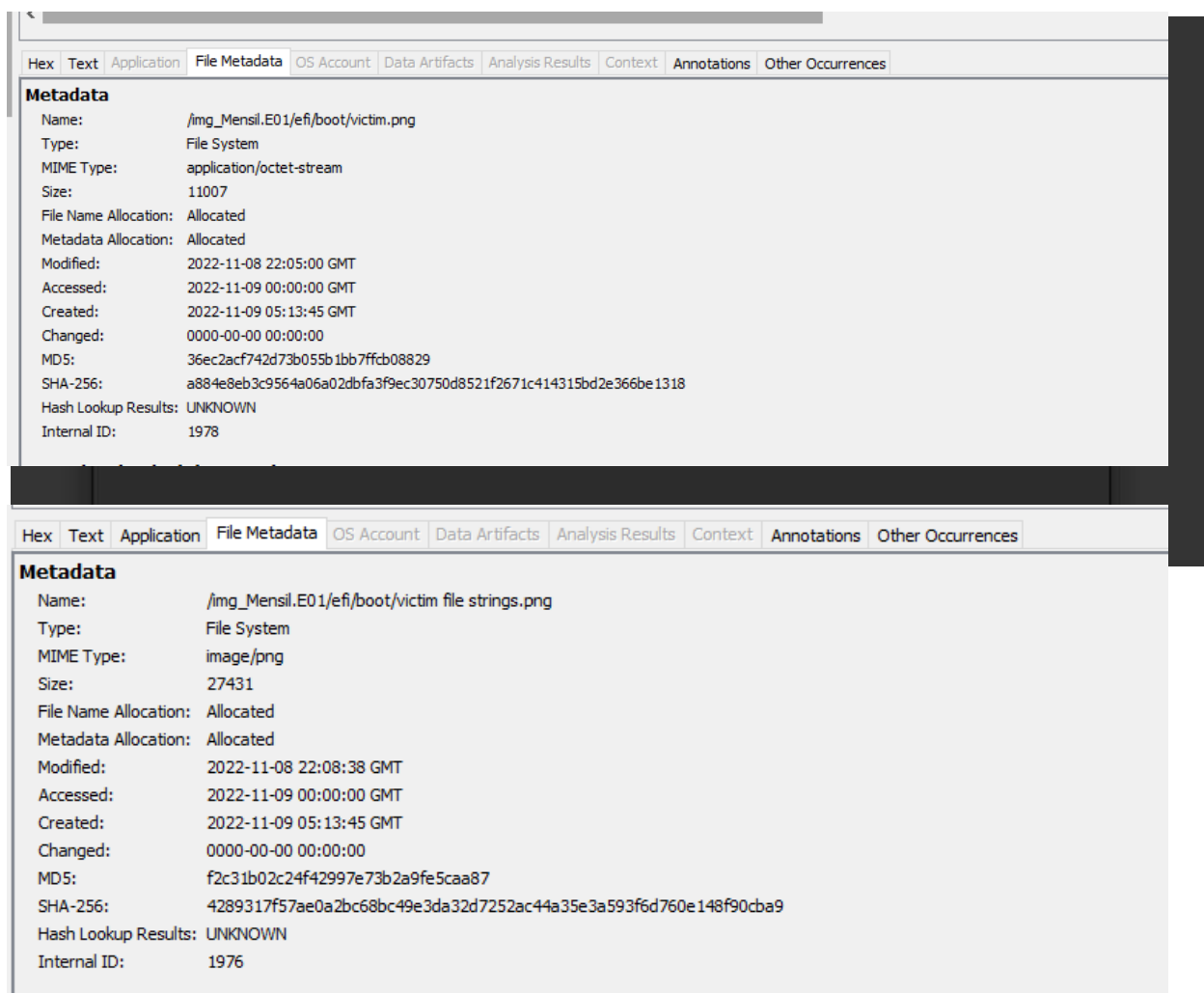
0x00000000: 89 50 4E 47 0D 0A 1A 0D 0A 00 00 00 0D 49 48 44 .PNG.....IHD	
0x00000010: 52 00 00 02 80 00 00 01 25 08 06 00 00 00 74 F4 R.....t.	
0x00000020: 53 E3 00 00 00 04 73 42 49 54 08 08 08 08 7C 08 S.....sBIT....l.	
0x00000030: 64 88 00 00 00 19 74 45 58 74 53 6F 66 74 77 61 d.....tEXtSoftwa	
0x00000040: 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 re.gnome-screens	
0x00000060: 72 65 61 74 69 6F 6E 20 54 69 6D 65 00 00 00 00 hot....giTxC	
0x00000070: 00 E0 A6 AC E0 A7 81 E0 A6 A7 E0 A6 AC E0 A6 BE reation Time....	
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/.....ID	
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 S1 0C 22 53 \$!...!...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 00:00:00
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 00:00:00
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 00:00:00
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 00:00:00

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
0°	49%	Reset							

<pre> -]...+ {h1Ge Tfd RRL 0x23 Tfd ++23 00-e ffff 0000 2Ten Vh1ydgGltEShbuGtCJ0K3pyrSMB3h3w== JELT00Q WNo) 0aBP tttUv\\ t233 JKKC 0u0h Vya 2kMy--- zUPP C++ -si] +==] s106 +77 +88U p1306V 218k -B </pre>	
--	--

A screenshot of artefact evidence details:



Description and implications of the artefact:

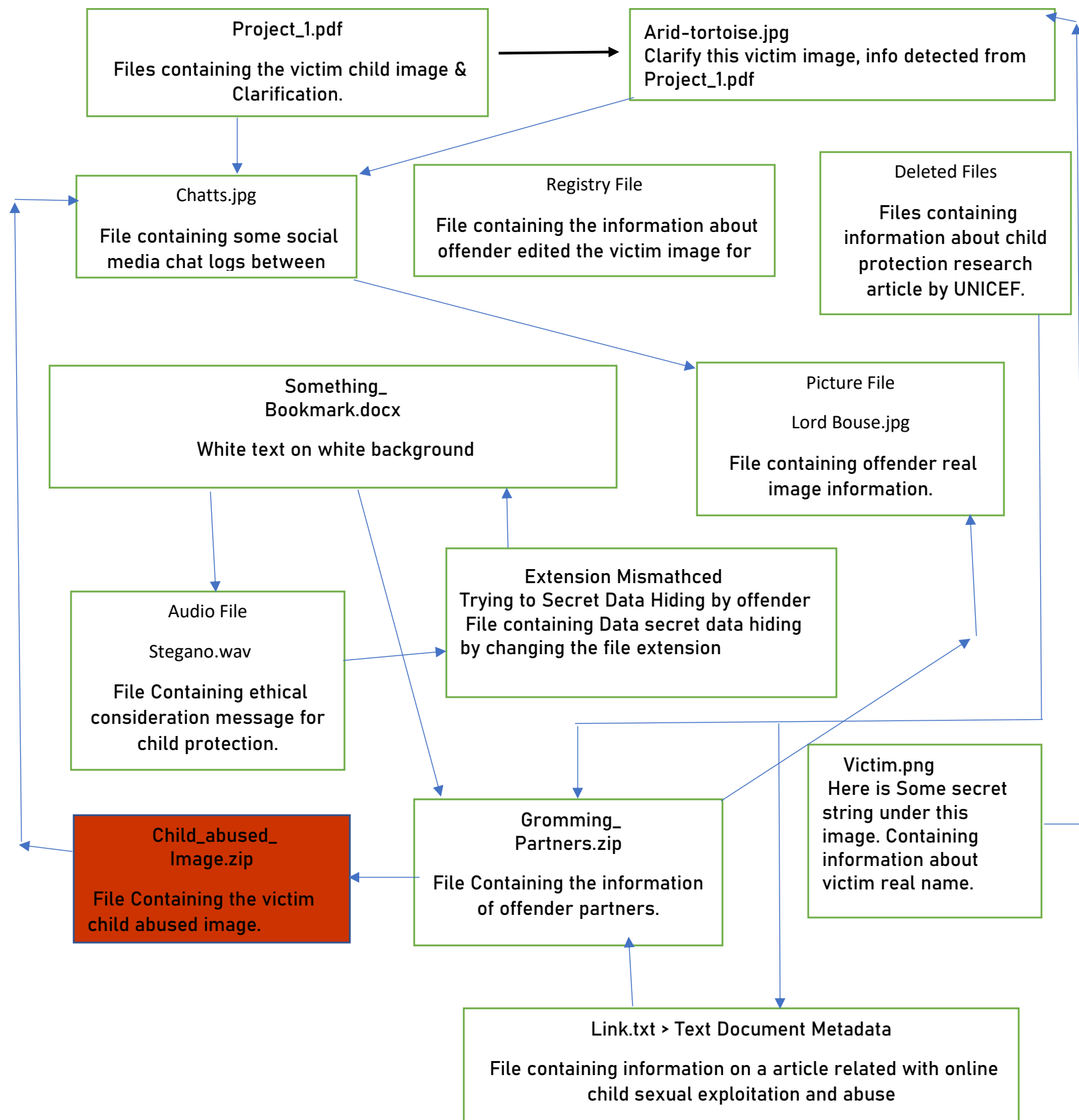
In this section we will find the victim's original name. We located a victim.png image file, however it cannot be opened either. However, we also discovered another picture file that is connected to the victim.png file. We discovered that this technique compromised the victim.png file string. So, we see that the base64 hash text is present in the strings area. We gather it and decode it using the same process as before. The victim's original name was then ultimately discovered. The extracted name or test is: "Victim Name: Nuria Lora"

Description of the hiding/unhiding process:

The victim.png file is corrupted by ASCII conversion. That means we need to check its strings.

```
>},++  
[n1I6e  
_TTd  
RRRL  
6m23  
SI6d  
+++33  
SO=e  
////  
b%%~  
2I6n  
VmLjdGltIE5hbWU6ICJ0dXJpYSBMb3JhJw==  
GEEYQQQ  
%%6j  
0aBP  
iiV\\  
h233  
JKKC  
4W4h  
YYYa  
zkHy~~  
zUPP  
G+**  
_%I]  
,=]  
ai7R  
*??_  
%%U  
p!366V  
233k  
~8
```

Evidence Map:



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

Hash: VmljdGltIE5hbWU6ICJ0dXJpYSBMb3JhJw==

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://meridianoutpost.com/convert-text-to-audio-morse-code/)
 - <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 Signature Mismatch 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.